Kontrol keamanan yang disarankan untuk menerapkan AWS kemampuan keamanan CAF

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Kontrol keamanan yang disarankan untuk menerapkan AWS kemampuan keamanan CAF

Table of Contents

Pengantar 1
Identitas dan kontrol akses 3
Aktivitas pengguna root 3
Kunci akses untuk pengguna root 4
MFA untuk pengguna root 4
Praktik terbaik IAM 5
Keistimewaan paling sedikit 5
Pagar pembatas pada tingkat beban kerja 6
Putar tombol akses IAM 7
Sumber daya yang dibagikan secara eksternal 7
Kontrol pencatatan dan pemantauan 8
CloudTrail Jejak multi-wilayah 8
Layanan dan pencatatan aplikasi 9
Penebangan terpusat 9
Akses ke file CloudTrail log 10
Peringatan untuk grup keamanan atau perubahan ACL jaringan 10
Peringatan untuk alarm CloudWatch 11
Kontrol infrastruktur 12
CloudFront objek root default 12
Pindai kode aplikasi 13
Buat lapisan jaringan 13
Gunakan hanya port resmi 14
Akses publik ke dokumen Systems Manager 14
Akses publik ke fungsi Lambda 15
Perbarui grup keamanan default 15
Memindai kerentanan dan eksposur jaringan 16
Mengatur AWS WAF 17
Perlindungan lanjutan terhadap serangan DDo S 17
Mengendalikan lalu lintas jaringan 18
Kontrol data 19
Klasifikasi data pada tingkat beban kerja 19
Menetapkan kontrol untuk setiap tingkat klasifikasi data 20
Enkripsi data saat istirahat 21
Enkripsi data dalam perjalanan 21

Akses publik ke snapshot Amazon EBS 22
Akses publik ke snapshot Amazon RDS 22
Akses publik ke Amazon RDS, Amazon Redshift, dan sumber daya AWS DMS 23
Akses publik ke ember S3 24
Memerlukan MFA untuk menghapus data bucket S3 24
OpenSearch Domain layanan di VPCs 25
Peringatan untuk penghapusan kunci KMS 25
Akses publik ke kunci KMS 26
Pendengar menggunakan protokol aman 26
Rekomendasi respons insiden 28
Rencana respons insiden 28
Runbook dan buku pedoman 29
Otomatisasi berbasis peristiwa 29
Dukungan proses 30
Peringatan untuk acara keamanan 30
Langkah selanjutnya 32
Riwayat dokumen 33
Glosarium 34
..... 34
A 35
B 38
C 40
D 43
E 47
F 49
G 51
H 52
I 53
L 56
M 57
O 62
P 64
Q 67
R 68
D 71
T 75

U 76
V 77
W 77
Z 78
..... lxxx

Kontrol keamanan yang disarankan untuk menerapkan AWS kemampuan keamanan CAF

Rishi Singla dan Rovan Omar, Amazon Web Services ()AWS

November 2023 (riwayat dokumen)

Keamanan adalah prioritas utama di AWS. Untuk membantu meringankan beban operasional Anda, Anda berbagi tanggung jawab atas keamanan dan kepatuhan cloud AWS. AWS bertanggung jawab atas keamanan cloud, yang berarti melindungi infrastruktur yang menjalankan layanan yang ditawarkan di AWS Cloud. Anda bertanggung jawab atas keamanan di cloud, seperti data dan aplikasi Anda. Panduan ini menyediakan kontrol keamanan yang dapat membantu Anda memenuhi tanggung jawab keamanan Anda di AWS Cloud.

AWS Cloud Adoption Framework (AWS CAF) menyediakan praktik terbaik yang dirancang untuk meningkatkan kesiapan cloud Anda. AWS CAF mengkategorikan praktik terbaik tersebut ke dalam enam perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Panduan ini berfokus pada kemampuan berikut dalam perspektif keamanan:

- Manajemen identitas dan akses - Kelola identitas manusia dan mesin serta izinnya dalam skala besar.
- Deteksi ancaman — Konfigurasikan pencatatan dan pemantauan untuk mendeteksi dan menyelidiki potensi kesalahan konfigurasi keamanan, ancaman, atau perilaku tak terduga.
- Melindungi infrastruktur — Melindungi sistem dan layanan dari akses yang tidak diinginkan atau tidak sah dan potensi kerentanan.
- Melindungi data — Mengkategorikan data berdasarkan tingkat sensitivitas. Pertahankan visibilitas dan kontrol atas data dan bagaimana data tersebut diakses dan digunakan di organisasi Anda.
- Respon insiden — Menetapkan mekanisme untuk menanggapi dan mengurangi dampak potensial dari insiden keamanan.

Kegagalan untuk menerapkan kontrol keamanan preventif, detektif, dan responsif untuk kemampuan keamanan AWS CAF ini dapat menimbulkan risiko penting bagi lingkungan cloud Anda, dan itu dapat mengganggu bisnis Anda. Menerapkan kontrol keamanan dalam panduan ini dapat membantu organisasi Anda melindungi lingkungan cloud-nya.

> **Note**
>
> AWS menyediakan layanan, alat, dan kerangka kerja yang dapat membantu Anda beroperasi dengan aman di. AWS Cloud Panduan ini selaras dengan dan melengkapi AWS Well-Architected Framework AWS , Cloud Adoption Framework AWS (CAF), Security Reference Architecture AWS (SRA),AWS dan rekomendasi keamanan lainnya yang diterbitkan oleh. AWS Kontrol dalam panduan ini tidak komprehensif dari semua pertimbangan keamanan cloud, dan panduan ini tidak dimaksudkan untuk menggantikan kerangka kerja ini.

Rekomendasi kontrol keamanan untuk mengelola identitas dan akses

Anda dapat membuat identitas di AWS, atau Anda dapat menghubungkan sumber identitas eksternal. Melalui kebijakan AWS Identity and Access Management (IAM), Anda memberi pengguna izin yang diperlukan sehingga mereka dapat mengakses atau mengelola AWS sumber daya dan aplikasi terintegrasi. Manajemen identitas dan akses yang efektif membantu memvalidasi bahwa orang dan mesin yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. The AWS Well-Architected Framework menyediakan praktik terbaik untuk mengelola identitas dan izinnya. Contoh praktik terbaik termasuk mengandalkan penyedia identitas terpusat dan menggunakan mekanisme masuk yang kuat, seperti otentikasi multi-faktor (MFA). Kontrol keamanan di bagian ini dapat membantu Anda menerapkan praktik terbaik ini.

Kontrol di bagian ini:

- Pantau dan konfigurasikan notifikasi untuk aktivitas pengguna root
- Jangan membuat kunci akses untuk pengguna root
- Aktifkan MFA untuk pengguna root
- Ikuti praktik terbaik keamanan untuk IAM
- Berikan izin hak istimewa paling sedikit
- Tentukan pagar pembatas izin di tingkat beban kerja
- Putar tombol akses IAM secara berkala
- Identifikasi sumber daya yang dibagikan dengan entitas eksternal

Pantau dan konfigurasikan notifikasi untuk aktivitas pengguna root

Saat pertama kali membuat Akun AWS, Anda mulai dengan identitas masuk tunggal yang disebut pengguna root. Secara default, pengguna root memiliki akses penuh ke semua Layanan AWS dan sumber daya di akun. Anda harus mengontrol dan memantau pengguna root dengan ketat, dan Anda harus menggunakannya hanya untuk tugas-tugas yang memerlukan kredenal pengguna root.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Berikan akses hak istimewa paling sedikit dalam Kerangka Well-Architected AWS
- Pantau aktivitas pengguna root IAM dalam Panduan AWS Preskriptif

Jangan membuat kunci akses untuk pengguna root

Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. Menonaktifkan akses terprogram ke pengguna root membantu mengurangi risiko paparan kredenal pengguna yang tidak disengaja dan kompromi lingkungan cloud selanjutnya. Kami menyarankan Anda membuat dan menggunakan peran IAM sebagai kredensi sementara untuk mengakses sumber daya dan sumber daya Anda. Akun AWS

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Kunci akses pengguna root IAM seharusnya tidak ada dalam dokumentasi AWS Security Hub
- Menghapus kunci akses untuk pengguna root dalam dokumentasi IAM
- Peran IAM dalam dokumentasi IAM

Aktifkan MFA untuk pengguna root

Kami menyarankan Anda mengaktifkan beberapa perangkat otentikasi multi-faktor (MFA) untuk pengguna Akun AWS root dan pengguna IAM. Ini meningkatkan bilah keamanan Akun AWS dan dapat menyederhanakan manajemen akses. Karena pengguna root adalah pengguna yang sangat istimewa yang dapat melakukan tindakan istimewa, sangat penting untuk meminta MFA untuk pengguna root. Anda dapat menggunakan perangkat MFA perangkat keras yang menghasilkan kode numerik berdasarkan algoritma kata sandi satu kali berbasis waktu (TOTP), kunci keamanan perangkat keras FIDO, atau aplikasi otentikator virtual.

Pada tahun 2024, MFA akan diminta untuk mengakses pengguna root apa pun. Akun AWS Untuk informasi lebih lanjut, lihat Aman menurut Desain: AWS untuk meningkatkan persyaratan MFA pada tahun 2024 di Blog Keamanan. AWS Kami sangat menganjurkan Anda untuk memperluas praktik keamanan ini dan mewajibkan MFA untuk semua jenis pengguna di lingkungan Anda AWS .

Jika memungkinkan, kami menyarankan Anda menggunakan perangkat MFA perangkat keras untuk pengguna root. MFA virtual mungkin tidak memberikan tingkat keamanan yang sama dengan perangkat MFA perangkat keras. Anda dapat menggunakan MFA virtual sambil menunggu persetujuan atau pengiriman pembelian perangkat keras.

Dalam situasi di mana Anda mengelola ratusan akun AWS Organizations, tergantung pada toleransi risiko organisasi Anda, mungkin tidak dapat diskalakan untuk menggunakan MFA berbasis perangkat keras untuk pengguna root dari setiap akun di unit organisasi (OU). Dalam hal ini, Anda dapat

memilih satu akun di OU yang bertindak sebagai akun manajemen OU, dan kemudian menonaktifkan pengguna root untuk akun lain di OU itu. Secara default, akun manajemen OU tidak memiliki akses ke akun lain. Dengan mengatur akses lintas akun terlebih dahulu, Anda dapat mengakses akun lain dari akun manajemen OU dalam keadaan darurat. Untuk mengatur akses lintas akun, Anda membuat peran IAM di akun anggota, dan Anda menentukan kebijakan sehingga hanya pengguna root di akun manajemen OU yang dapat mengambil peran ini. Untuk informasi selengkapnya, lihat Tutorial: Mendelegasikan akses Akun AWS menggunakan peran IAM dalam dokumentasi IAM.

Kami menyarankan Anda mengaktifkan beberapa perangkat MFA untuk kredensi pengguna root Anda. Anda dapat mendaftarkan hingga delapan perangkat MFA dari kombinasi apa pun.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengaktifkan token TOTP perangkat keras dalam dokumentasi IAM
- Mengaktifkan perangkat otentikasi multi-faktor virtual (MFA) dalam dokumentasi IAM
- Mengaktifkan kunci keamanan FIDO dalam dokumentasi IAM
- Amankan login pengguna root Anda dengan otentikasi multi-faktor (MFA) dalam dokumentasi IAM

Ikuti praktik terbaik keamanan untuk IAM

Dokumentasi IAM mencakup daftar praktik terbaik yang dirancang untuk membantu Anda mengamankan sumber daya Akun AWS dan sumber daya Anda. Ini termasuk rekomendasi untuk mengonfigurasi akses dan izin sesuai dengan prinsip hak istimewa paling sedikit. Contoh praktik terbaik keamanan IAM termasuk mengonfigurasi federasi identitas, mewajibkan MFA, dan menggunakan kredensil sementara.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Praktik terbaik keamanan di IAM dalam dokumentasi IAM
- Menggunakan kredensi sementara dengan AWS sumber daya dalam dokumentasi IAM

Berikan izin hak istimewa paling sedikit

Keistimewaan paling sedikit adalah praktik pemberian hanya izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu.

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut, seperti tag mereka. Anda dapat menggunakan atribut grup, identitas, dan sumber daya untuk menentukan izin secara dinamis dalam skala besar, daripada menentukan izin untuk pengguna individual. Misalnya, Anda dapat menggunakan ABAC untuk mengizinkan sekelompok pengembang mengakses hanya sumber daya yang memiliki tag tertentu yang terkait dengan proyek mereka.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Terapkan izin hak istimewa paling sedikit dalam dokumentasi IAM
- Untuk apa ABAC AWS dalam dokumentasi IAM

Tentukan pagar pembatas izin di tingkat beban kerja

Ini adalah praktik terbaik untuk menggunakan strategi multi-akun karena memberikan fleksibilitas untuk menentukan pagar pembatas pada tingkat beban kerja. Arsitektur Referensi AWS Keamanan menawarkan panduan preskriptif tentang cara menyusun akun Anda. Akun-akun ini dikelola sebagai organisasi di AWS Organizations, dan akun dikelompokkan ke dalam unit organisasi (OUs).

Layanan AWS, seperti AWS Control Tower, dapat membantu Anda mengelola kontrol secara terpusat di seluruh organisasi. Kami menyarankan Anda menentukan tujuan yang jelas untuk setiap akun atau OU dalam organisasi, dan menerapkan kontrol sesuai dengan tujuan itu. AWS Control Tower menerapkan kontrol preventif, detektif, dan proaktif yang membantu Anda mengatur sumber daya dan memantau kepatuhan. Kontrol preventif dirancang untuk mencegah suatu peristiwa terjadi. Kontrol detektif dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol proaktif dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai dengan memindai sumber daya sebelum disediakan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Pisahkan beban kerja menggunakan akun di AWS Well-Architected Framework
- AWS Arsitektur Referensi Keamanan (AWS SRA) dalam Panduan AWS Preskriptif
- Tentang kontrol AWS Control Tower di dalam AWS Control Tower dokumentasi
- Menerapkan kontrol keamanan di AWS dalam Panduan AWS Preskriptif
- Gunakan kebijakan kontrol layanan untuk menetapkan pagar pembatas izin di seluruh akun di AWS Organisasi Anda di Blog Keamanan AWS

Putar tombol akses IAM secara berkala

Ini adalah praktik terbaik untuk memperbarui kunci akses untuk kasus penggunaan yang memerlukan kredensi jangka panjang. Kami merekomendasikan memutar kunci akses setiap 90 hari atau kurang. Memutar kunci akses mengurangi risiko bahwa kunci akses yang terkait dengan akun yang disusupi atau dihentikan digunakan. Ini juga mencegah akses dengan menggunakan kunci lama yang mungkin telah hilang, disusupi, atau dicuri. Selalu perbarui aplikasi setelah memutar tombol akses.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Perbarui kunci akses bila diperlukan untuk kasus penggunaan yang memerlukan kredensi jangka panjang dalam dokumentasi IAM
- Secara otomatis memutar kunci akses pengguna IAM pada skala besar dengan AWS Organizations dan AWS Secrets Manager dalam Panduan AWS Preskriptif
- Memperbarui kunci akses dalam dokumentasi IAM

Identifikasi sumber daya yang dibagikan dengan entitas eksternal

Entitas eksternal adalah sumber daya, aplikasi, layanan, atau pengguna yang berada di luar AWS organisasi Anda, seperti pengguna lain Akun AWS, pengguna root, pengguna atau peran IAM, pengguna federasi, atau pengguna anonim (atau tidak diautentikasi). Layanan AWS Merupakan praktik keamanan terbaik untuk menggunakan IAM Access Analyzer untuk mengidentifikasi sumber daya di organisasi dan akun Anda, seperti bucket Amazon Simple Storage Service (Amazon S3) atau peran IAM, yang dibagikan dengan entitas eksternal. Ini membantu Anda mengidentifikasi akses yang tidak diinginkan ke sumber daya dan data, yang merupakan risiko keamanan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Verifikasi akses publik dan lintas akun ke sumber daya dengan IAM Access Analyzer dalam dokumentasi IAM
- Menganalisis akses publik dan lintas akun di AWS Well-Architected Framework
- Menggunakan AWS Identity and Access Management Access Analyzer dalam dokumentasi IAM

Rekomendasi kontrol keamanan untuk pencatatan dan pemantauan

Penebangan dan pemantauan adalah aspek penting dari deteksi ancaman. Deteksi ancaman adalah salah satu kemampuan perspektif keamanan dalam AWS Cloud Adoption Framework (AWS CAF). Dengan menggunakan data log, organisasi Anda dapat memantau lingkungan Anda untuk memahami dan mengidentifikasi potensi kesalahan konfigurasi keamanan, ancaman, dan perilaku tak terduga. Memahami potensi ancaman dapat membantu organisasi Anda memprioritaskan kontrol keamanan, dan deteksi ancaman yang efektif dapat membantu Anda merespons ancaman dengan lebih cepat.

Kontrol di bagian ini:

- Konfigurasikan setidaknya satu jejak Multi-wilayah di CloudTrail
- Konfigurasikan logging di tingkat layanan dan aplikasi
- Menetapkan lokasi terpusat untuk menganalisis log dan menanggapi peristiwa keamanan
- Mencegah akses tidak sah ke bucket S3 yang berisi file log CloudTrail
- Konfigurasikan peringatan untuk perubahan pada grup keamanan atau jaringan ACLs
- Konfigurasikan peringatan untuk CloudWatch alarm yang masuk ke status ALARM

Konfigurasikan setidaknya satu jejak Multi-wilayah di CloudTrail

AWS CloudTrailmembantu Anda mengaudit tata kelola, kepatuhan, dan risiko operasional Anda Akun AWS. Tindakan yang diambil oleh pengguna, peran, atau Layanan AWS direkam sebagai peristiwa di CloudTrail. Peristiwa termasuk tindakan yang diambil dalam AWS Management Console, AWS Command Line Interface (AWS CLI), dan AWS SDKs dan APIs. Riwayat acara ini membantu Anda menganalisis postur keamanan, melacak perubahan sumber daya, dan kepatuhan audit.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, Anda harus membuat jejak. Setiap jejak harus dikonfigurasi untuk mencatat peristiwa di semua Wilayah AWS. Dengan mencatat peristiwa di semua Wilayah AWS, Anda memastikan bahwa semua peristiwa yang terjadi di Akun AWS Anda dicatat, terlepas dari mana peristiwa Wilayah AWS itu terjadi. Jejak multi-wilayah memastikan bahwa peristiwa layanan global dicatat.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- CloudTrail praktik terbaik keamanan detektif dalam dokumentasi CloudTrail
- Mengonversi jejak yang berlaku untuk satu Wilayah untuk diterapkan ke semua Wilayah dalam dokumentasi CloudTrail
- Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global dalam dokumentasi CloudTrail

Konfigurasikan logging di tingkat layanan dan aplikasi

AWS Well-Architected Framework merekomendasikan agar Anda menyimpan log peristiwa keamanan dari layanan dan aplikasi. Ini adalah prinsip dasar keamanan untuk audit, investigasi, dan kasus penggunaan operasional. Penyimpanan log layanan dan aplikasi adalah persyaratan keamanan umum yang didorong oleh standar, kebijakan, dan prosedur tata kelola, risiko, dan kepatuhan (GRC).

Tim operasi keamanan mengandalkan log dan alat pencarian untuk menemukan potensi peristiwa menarik yang mungkin menunjukkan aktivitas yang tidak sah atau perubahan yang tidak disengaja. Anda dapat mengaktifkan pencatatan untuk berbagai layanan, tergantung pada kasus penggunaan. Misalnya, Anda dapat mencatat akses bucket Amazon S3, lalu lintas ACL AWS WAF web, lalu lintas Amazon API Gateway di lapisan jaringan, atau distribusi Amazon. CloudFront

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Streaming Amazon CloudWatch Logs ke akun terpusat untuk audit dan analisis di Blog AWS Arsitektur
- Konfigurasikan pencatatan layanan dan aplikasi di AWS Well-Architected Framework

Menetapkan lokasi terpusat untuk menganalisis log dan menanggapi peristiwa keamanan

Menganalisis log secara manual dan memproses informasi tidak cukup untuk mengikuti volume informasi yang terkait dengan arsitektur yang kompleks. Analisis dan pelaporan saja tidak memfasilitasi penugasan acara ke sumber daya yang benar secara tepat waktu. AWS Well-Architected Framework merekomendasikan agar Anda AWS mengintegrasikan peristiwa dan temuan keamanan ke dalam sistem notifikasi dan alur kerja, seperti sistem tiket, bug, atau informasi keamanan dan manajemen acara (SIEM). Sistem ini membantu Anda menetapkan, merutekan, dan mengelola peristiwa keamanan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Menganalisis log, temuan, dan metrik secara terpusat di AWS Well-Architected Framework
- Menganalisis keamanan, kepatuhan, dan aktivitas operasional menggunakan CloudTrail Amazon Athena di AWS Blog Keamanan
- AWS Mitra yang menyediakan layanan deteksi dan respons ancaman dalam Portofolio AWS Mitra

Mencegah akses tidak sah ke bucket S3 yang berisi file log CloudTrail

Secara default, file CloudTrail log disimpan di bucket Amazon S3. Ini adalah praktik terbaik keamanan untuk mencegah akses tidak sah ke bucket Amazon S3 apa pun yang CloudTrail berisi file log. Ini membantu Anda menjaga integritas, kelengkapan, dan ketersediaan log ini, yang sangat penting untuk tujuan forensik dan audit. Jika Anda ingin mencatat peristiwa data untuk bucket S3 yang berisi file CloudTrail log, Anda dapat membuat CloudTrail jejak untuk tujuan ini.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengonfigurasi blokir setelan akses publik untuk bucket S3 Anda dalam dokumentasi Amazon S3
- CloudTrail praktik terbaik keamanan preventif dalam dokumentasi CloudTrail
- Membuat jejak dalam CloudTrail dokumentasi

Konfigurasikan peringatan untuk perubahan pada grup keamanan atau jaringan ACLs

Grup keamanan di Amazon Virtual Private Cloud (Amazon VPC) mengontrol lalu lintas yang diizinkan untuk mencapai dan meninggalkan sumber daya yang terkait dengannya. Daftar kontrol akses jaringan (ACL) memungkinkan atau menolak lalu lintas masuk atau keluar tertentu pada tingkat subnet VPC. Sumber daya ini sangat penting untuk mengelola akses di AWS lingkungan Anda.

Buat dan konfigurasikan CloudWatch alarm Amazon yang memberi tahu Anda jika grup keamanan atau konfigurasi ACL jaringan berubah. Konfigurasikan alarm ini untuk mengingatkan Anda setiap kali panggilan AWS API dilakukan untuk memperbarui grup keamanan. Anda juga dapat menggunakan layanan, seperti Amazon EventBridge dan AWS Config, untuk secara otomatis menanggapi jenis peristiwa keamanan ini.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Secara otomatis mengembalikan dan menerima pemberitahuan tentang perubahan pada grup keamanan Amazon VPC Anda di AWS Blog Keamanan
- Menggunakan CloudWatch alarm Amazon dalam dokumentasi CloudWatch
- Menerapkan peristiwa keamanan yang dapat ditindaklanjuti dalam Kerangka Well-Architected AWS
- Otomatiskan respons terhadap peristiwa di AWS Well-Architected Framework

Konfigurasikan peringatan untuk CloudWatch alarm yang masuk ke status ALARM

Di CloudWatch, Anda dapat menentukan tindakan apa yang dilakukan alarm saat mengubah status antara`OK`,`ALARM`, dan `INSUFFICIENT_DATA` status. Jenis tindakan alarm yang paling umum adalah memberi tahu satu atau lebih orang dengan mengirim pesan ke topik Amazon Simple Notification Service (Amazon SNS). Anda juga dapat mengonfigurasi alarm untuk membuat OpsItemsatau insiden di. AWS Systems Manager

Kami menyarankan Anda mengaktifkan tindakan alarm untuk memperingatkan secara otomatis jika metrik yang dipantau berada di luar ambang batas yang ditentukan. Memantau alarm membantu Anda mengidentifikasi aktivitas yang tidak biasa dan dengan cepat menanggapi masalah keamanan dan operasional.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Menerapkan peristiwa keamanan yang dapat ditindaklanjuti dalam Kerangka Well-Architected AWS
- Tindakan alarm dalam CloudWatch dokumentasi

Rekomendasi kontrol keamanan untuk melindungi infrastruktur

Perlindungan infrastruktur adalah bagian penting dari program keamanan apa pun. Ini mencakup metodologi kontrol yang membantu Anda melindungi jaringan dan menghitung sumber daya. Contoh perlindungan infrastruktur termasuk batas kepercayaan, defense-in-depth pendekatan, pengerasan keamanan, manajemen patch, dan otentikasi dan otorisasi sistem operasi. Untuk informasi lebih lanjut, lihat Perlindungan infrastruktur di AWS Well-Architected Framework. Kontrol keamanan di bagian ini dapat membantu Anda menerapkan praktik terbaik untuk perlindungan infrastruktur.

Kontrol di bagian ini:

- Tentukan objek root default untuk CloudFront distribusi
- Pindai kode aplikasi untuk mengidentifikasi masalah keamanan umum
- Buat layer jaringan dengan menggunakan dedicated VPCs dan subnet
- Batasi lalu lintas masuk hanya ke port resmi
- Blokir akses publik ke dokumen Systems Manager
- Blokir akses publik ke fungsi Lambda
- Batasi lalu lintas masuk dan keluar di grup keamanan default
- Memindai kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan
- Mengatur AWS WAF
- Konfigurasikan perlindungan lanjutan terhadap serangan DDo S
- Gunakan defense-in-depth pendekatan untuk mengontrol lalu lintas jaringan

Tentukan objek root default untuk CloudFront distribusi

Amazon CloudFront mempercepat distribusi konten web Anda dengan mengirimkannya melalui jaringan pusat data di seluruh dunia, yang menurunkan latensi dan meningkatkan kinerja. Jika Anda tidak menentukan objek akar default, mintalah akar pas distribusi Anda ke server asal Anda. Jika Anda menggunakan asal Amazon Simple Storage Service (Amazon S3), permintaan tersebut dapat menampilkan daftar konten di bucket S3 atau daftar konten pribadi asal Anda. Menentukan objek root default membantu Anda menghindari mengekspos konten distribusi Anda.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Menentukan objek root default dalam dokumentasi CloudFront

Pindai kode aplikasi untuk mengidentifikasi masalah keamanan umum

The AWS Well-Architected Framework merekomendasikan agar Anda memindai pustaka dan dependensi untuk masalah dan cacat. Ada banyak alat analisis kode sumber yang dapat Anda gunakan untuk memindai kode sumber. Misalnya, Amazon CodeGuru dapat memindai masalah keamanan umum di Java atau Python aplikasi dan memberikan rekomendasi untuk remediasi.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- CodeGuru dokumentasi
- Alat analisis kode sumber di OWASP Foundation situs web
- Lakukan manajemen kerentanan dalam AWS Well-Architected Framework

Buat layer jaringan dengan menggunakan dedicated VPCs dan subnet

AWS Well-Architected Framework merekomendasikan agar Anda mengelompokkan komponen yang berbagi persyaratan sensitivitas ke dalam lapisan. Ini meminimalkan potensi ruang lingkup dampak akses yang tidak sah. Misalnya, cluster database yang tidak memerlukan akses internet harus ditempatkan di subnet pribadi VPC-nya untuk memastikan bahwa tidak ada rute ke atau dari internet.

AWS menawarkan banyak layanan yang dapat membantu Anda menguji dan mengidentifikasi jangkauan publik. Misalnya, Reachability Analyzer adalah alat analisis konfigurasi yang membantu Anda menguji konektivitas antara sumber dan sumber daya tujuan di situs Anda. VPCs Selain itu, Network Access Analyzer dapat membantu Anda mengidentifikasi akses jaringan yang tidak diinginkan ke sumber daya.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Buat layer jaringan di AWS Well-Architected Framework

- Dokumentasi Reachability Analyzer
- Dokumentasi Network Access Analyzer
- Buat subnet di dokumentasi Amazon Virtual Private Cloud (Amazon VPC)

Batasi lalu lintas masuk hanya ke port resmi

Akses tidak terbatas, seperti lalu lintas dari alamat IP `0.0.0.0/0` sumber, meningkatkan risiko aktivitas berbahaya, seperti peretasan, serangan (denial-of-serviceDoS), dan hilangnya data. Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port terkenal, seperti SSH dan Windows protokol desktop jarak jauh (RDP). Untuk lalu lintas masuk, di grup keamanan Anda, izinkan hanya koneksi TCP atau UDP pada port resmi. Untuk menghubungkan ke instans Amazon Elastic Compute Cloud (Amazon EC2), gunakan Session Manager atau Run Command alih-alih akses SSH atau RDP langsung.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Bekerja dengan grup keamanan dalam EC2 dokumentasi Amazon
- Kontrol lalu lintas ke AWS sumber daya Anda menggunakan grup keamanan dalam dokumentasi Amazon VPC

Blokir akses publik ke dokumen Systems Manager

Kecuali kasus penggunaan Anda mengharuskan berbagi publik diaktifkan, praktik AWS Systems Manager terbaik menyarankan Anda memblokir berbagi publik untuk dokumen Systems Manager. Berbagi publik dapat memberikan akses yang tidak diinginkan ke dokumen. Dokumen Systems Manager publik dapat mengekspos informasi berharga dan sensitif tentang akun, sumber daya, dan proses internal Anda.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Praktik terbaik untuk dokumen Systems Manager bersama dalam dokumentasi Systems Manager
- Memodifikasi izin untuk dokumen Systems Manager bersama dalam dokumentasi Systems Manager

Blokir akses publik ke fungsi Lambda

AWS Lambdaadalah layanan komputasi yang membantu Anda menjalankan kode tanpa perlu menyediakan atau mengelola server. Fungsi Lambda tidak boleh diakses publik karena ini memungkinkan akses yang tidak diinginkan ke kode fungsi.

Kami menyarankan Anda mengonfigurasi kebijakan berbasis sumber daya untuk fungsi Lambda untuk menolak akses dari luar akun Anda. Anda dapat mencapai ini dengan menghapus izin atau dengan menambahkan `AWS:SourceAccount` kondisi ke pernyataan yang memungkinkan akses. Anda dapat memperbarui kebijakan berbasis sumber daya untuk fungsi Lambda melalui API Lambda atau (). AWS Command Line Interface AWS CLI

Kami juga menyarankan agar Anda mengaktifkan kebijakan fungsi Lambda [Lambda.1] harus melarang kontrol akses publik. AWS Security Hub Kontrol ini memvalidasi bahwa kebijakan berbasis sumber daya untuk fungsi Lambda melarang akses publik.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- AWS Lambda kontrol dalam dokumentasi Security Hub
- Menggunakan kebijakan berbasis sumber daya untuk Lambda dalam dokumentasi Lambda
- Sumber daya dan kondisi untuk tindakan Lambda dalam dokumentasi Lambda

Batasi lalu lintas masuk dan keluar di grup keamanan default

Jika Anda tidak mengaitkan grup keamanan khusus saat menyediakan AWS sumber daya, sumber daya tersebut dikaitkan dengan grup keamanan default VPC. Aturan default untuk grup keamanan ini memungkinkan semua lalu lintas masuk dari semua sumber daya yang ditetapkan ke grup keamanan ini, dan mereka mengizinkan semua keluar IPv4 dan IPv6 lalu lintas. Ini mungkin memungkinkan lalu lintas yang tidak diinginkan ke sumber daya.

AWS merekomendasikan agar Anda tidak menggunakan grup keamanan default. Sebagai gantinya, buat grup keamanan khusus untuk sumber daya atau grup sumber daya tertentu.

Karena grup keamanan default tidak dapat dihapus, sebaiknya Anda mengubah aturan grup keamanan default untuk membatasi lalu lintas masuk dan keluar. Saat mengonfigurasi aturan grup keamanan, ikuti prinsip hak istimewa paling sedikit.

Kami juga menyarankan agar Anda mengaktifkan grup keamanan default VPC [EC2.2] tidak boleh mengizinkan kontrol lalu lintas masuk atau keluar di Security Hub. Kontrol ini memvalidasi bahwa grup keamanan default VPC menolak lalu lintas masuk dan keluar.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Kontrol lalu lintas ke AWS sumber daya Anda menggunakan grup keamanan dalam dokumentasi Amazon VPC
- Grup keamanan default untuk VPCs dokumentasi Amazon VPC Anda
- EC2Kontrol Amazon dalam dokumentasi Security Hub

Memindai kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan

Kami menyarankan Anda mengaktifkan Amazon Inspector di semua akun Anda. Amazon Inspector adalah layanan manajemen kerentanan yang terus-menerus memindai instans Amazon Anda, gambar wadah Amazon Elastic Container Registry (Amazon ECR) Registry (Amazon ECR) EC2 , dan fungsi Lambda untuk mencari kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan. Ini juga mendukung inspeksi mendalam dari EC2 instans Amazon. Ketika Amazon Inspector mengidentifikasi kerentanan atau jalur jaringan terbuka, Amazon Inspector menghasilkan temuan yang dapat Anda selidiki. Jika Amazon Inspector dan Security Hub disiapkan di akun Anda, Amazon Inspector secara otomatis mengirimkan temuan keamanan ke Security Hub untuk pengelolaan terpusat.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memindai sumber daya dengan Amazon Inspector dalam dokumentasi Amazon Inspector
- Inspektur Amazon Inspeksi mendalam untuk Amazon EC2 dalam dokumentasi Amazon Inspector
- Pindai EC2 AMIs menggunakan Amazon Inspector di Blog Keamanan AWS
- Membangun program manajemen kerentanan yang dapat diskalakan di AWS dalam AWS Panduan Preskriptif
- Mengotomatiskan perlindungan jaringan di AWS Well-Architected Framework
- Mengotomatiskan perlindungan komputasi di AWS Well-Architected Framework

Mengatur AWS WAF

AWS WAFadalah firewall aplikasi web yang membantu Anda memantau dan memblokir permintaan HTTP atau HTTPS yang diteruskan ke sumber daya aplikasi web Anda yang dilindungi, seperti Amazon API Gateway, CloudFront distribusi APIs Amazon, atau Application Load Balancers. Berdasarkan kriteria yang Anda tentukan, layanan merespons permintaan baik dengan konten yang diminta, dengan kode status HTTP 403 (Terlarang), atau dengan respons khusus. AWS WAF dapat membantu melindungi aplikasi web atau APIs terhadap eksploitasi web umum yang dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. Pertimbangkan untuk menyiapkan AWS WAF Akun AWS dan menggunakan kombinasi aturan AWS terkelola, aturan khusus, dan integrasi mitra untuk membantu melindungi aplikasi Anda dari serangan lapisan aplikasi (lapisan 7).

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memulai dengan AWS WAF dalam AWS WAF dokumentasi
- AWS WAF mitra pengiriman di situs AWS web
- Otomatisasi keamanan untuk AWS WAF di Perpustakaan AWS Solusi
- Menerapkan inspeksi dan perlindungan dalam Kerangka AWS Well-Architected

Konfigurasikan perlindungan lanjutan terhadap serangan DDo S

AWS Shieldmemberikan perlindungan terhadap serangan penolakan layanan terdistribusi (DDoS) untuk AWS sumber daya di jaringan dan lapisan transport (lapisan 3 dan 4) dan lapisan aplikasi (lapisan 7). Layanan ini tersedia dalam dua opsi: AWS Shield Standard dan AWS Shield Advanced. Shield Standard secara otomatis melindungi AWS sumber daya yang didukung, tanpa biaya tambahan.

Kami menyarankan Anda berlangganan Shield Advanced, yang menyediakan perlindungan serangan DDo S yang diperluas untuk sumber daya yang dilindungi. Perlindungan yang Anda terima dari Shield Advanced bervariasi tergantung pada pilihan arsitektur dan konfigurasi Anda. Pertimbangkan untuk menerapkan perlindungan Shield Advanced untuk aplikasi di mana Anda memerlukan salah satu dari berikut ini:

- Ketersediaan terjamin untuk pengguna aplikasi.
- Akses cepat ke ahli mitigasi DDo S jika aplikasi dipengaruhi oleh serangan DDo S.

- Kesadaran AWS bahwa aplikasi mungkin terpengaruh oleh serangan DDo S dan pemberitahuan serangan dari AWS dan eskalasi ke tim keamanan atau operasi Anda.
- Prediktabilitas dalam biaya cloud Anda, termasuk ketika serangan DDo S memengaruhi penggunaan Anda. Layanan AWS

Untuk informasi selengkapnya, lihat sumber daya berikut:

- AWS Shield Advanced ikhtisar dalam dokumentasi Shield
- AWS Shield Advanced sumber daya yang dilindungi dalam dokumentasi Shield
- AWS Shield Advanced kemampuan dan opsi dalam dokumentasi Shield
- Menanggapi peristiwa DDo S dalam dokumentasi Shield
- Menerapkan inspeksi dan perlindungan dalam Kerangka AWS Well-Architected

Gunakan defense-in-depth pendekatan untuk mengontrol lalu lintas jaringan

AWS Network Firewall adalah firewall jaringan stateful, dikelola, dan layanan deteksi dan pencegahan intrusi untuk cloud pribadi virtual () VPCs di. AWS Cloud Ini membantu Anda menerapkan perlindungan jaringan penting di perimeter VPC. Ini termasuk memfilter lalu lintas yang pergi dan datang dari gateway internet, gateway NAT, atau melalui VPN atau. AWS Direct Connect Network Firewall mencakup fitur yang membantu melindungi terhadap ancaman jaringan umum. Firewall stateful di Network Firewall dapat menggabungkan konteks dari arus lalu lintas, seperti koneksi dan protokol, untuk menegakkan kebijakan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- AWS Network Firewall dokumentasi
- Kontrol lalu lintas di semua lapisan dalam Kerangka AWS Well-Architected

Rekomendasi kontrol keamanan untuk melindungi data

AWS Well-Architected Framework mengelompokkan praktik terbaik untuk melindungi data ke dalam tiga kategori: klasifikasi data, melindungi data saat istirahat, dan melindungi data saat transit. Kontrol keamanan di bagian ini dapat membantu Anda menerapkan praktik terbaik untuk perlindungan data. Praktik terbaik dasar ini harus ada sebelum Anda merancang beban kerja apa pun di cloud. Mereka mencegah kesalahan penanganan data, dan membantu Anda memenuhi kewajiban organisasi, peraturan, dan kepatuhan. Gunakan kontrol keamanan di bagian ini untuk menerapkan praktik terbaik untuk perlindungan data.

Kontrol di bagian ini:

- Mengidentifikasi dan mengklasifikasikan data pada tingkat beban kerja
- Menetapkan kontrol untuk setiap tingkat klasifikasi data
- Enkripsi data saat istirahat
- Enkripsi data dalam perjalanan
- Blokir akses publik ke snapshot Amazon EBS
- Blokir akses publik ke snapshot Amazon RDS
- Blokir akses publik ke Amazon RDS, Amazon Redshift, dan sumber daya AWS DMS
- Blokir akses publik ke bucket Amazon S3
- Memerlukan MFA untuk menghapus data di bucket Amazon S3 yang penting
- Konfigurasikan domain OpenSearch Layanan Amazon di VPC
- Konfigurasikan peringatan untuk penghapusan AWS KMS key
- Blokir akses publik ke AWS KMS keys
- Konfigurasikan pendengar penyeimbang beban untuk menggunakan protokol aman

Mengidentifikasi dan mengklasifikasikan data pada tingkat beban kerja

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 sering mengurangi frekuensi duplikasi data. Ini dapat mengurangi biaya penyimpanan dan cadangan dan mempercepat pencarian.

Kami menyarankan Anda memahami jenis dan klasifikasi data yang diproses oleh beban kerja Anda, proses bisnis terkait, tempat data disimpan, dan siapa yang memiliki data tersebut. Klasifikasi data membantu pemilik beban kerja untuk mengidentifikasi lokasi yang menyimpan data sensitif dan menentukan bagaimana data tersebut harus diakses dan dibagikan. Tag adalah pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya. AWS Tag dapat membantu mengelola, mengidentifikasi, mengatur, mencari, dan memfilter sumber daya.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Klasifikasi data dalam AWS Whitepaper
- Identifikasi data dalam beban kerja Anda di AWS Well-Architected Framework

Menetapkan kontrol untuk setiap tingkat klasifikasi data

Tentukan kontrol perlindungan data untuk setiap tingkat klasifikasi. Misalnya, gunakan kontrol yang disarankan untuk mengamankan data yang diklasifikasikan sebagai publik, dan melindungi data sensitif dengan kontrol tambahan. Gunakan mekanisme dan alat yang mengurangi atau menghilangkan kebutuhan untuk langsung mengakses atau memproses data secara manual. Otomatisasi identifikasi dan klasifikasi data mengurangi risiko kesalahan klasifikasi, kesalahan penanganan, modifikasi, atau kesalahan manusia.

Misalnya, pertimbangkan untuk menggunakan Amazon Macie untuk memindai bucket Amazon Simple Storage Service (Amazon S3) untuk mencari data sensitif, seperti informasi identitas pribadi (PII). Selain itu, Anda dapat mengotomatiskan deteksi akses data yang tidak diinginkan dengan menggunakan VPC Flow Logs di Amazon Virtual Private Cloud (Amazon VPC).

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Tentukan kontrol perlindungan data dalam AWS Well-Architected Framework
- Mengotomatiskan identifikasi dan klasifikasi dalam AWS Well-Architected Framework
- AWS Arsitektur Referensi Privasi (AWS PRA) dalam Panduan AWS Preskriptif
- Menemukan data sensitif dengan Amazon Macie dalam dokumentasi Macie
- Mencatat lalu lintas IP menggunakan VPC Flow Logs dalam dokumentasi Amazon VPC

- Teknik umum untuk mendeteksi data PHI dan PII yang digunakan Layanan AWS di blog AWS for Industries

Enkripsi data saat istirahat

Data saat istirahat adalah data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan. Menerapkan enkripsi dan kontrol akses yang tepat untuk data saat istirahat membantu mengurangi risiko akses yang tidak sah. Enkripsi adalah proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext. Anda memerlukan kunci enkripsi untuk mendekripsi konten kembali ke teks biasa sehingga dapat digunakan. Di dalam AWS Cloud, Anda dapat menggunakan AWS Key Management Service (AWS KMS) untuk membuat dan mengontrol kunci kriptografi yang membantu melindungi data Anda.

Sebagaimana dibahas dalamMenetapkan kontrol untuk setiap tingkat klasifikasi data, kami menyarankan untuk membuat kebijakan yang menentukan jenis data apa yang memerlukan enkripsi. Sertakan kriteria bagaimana menentukan data mana yang harus dienkripsi dan data mana yang harus dilindungi dengan teknik lain, seperti tokenisasi atau hashing.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengkonfigurasi enkripsi default dalam dokumentasi Amazon S3
- Enkripsi secara default untuk volume EBS baru dan salinan snapshot dalam dokumentasi Amazon EC2
- Mengenkripsi sumber daya Amazon Aurora dalam dokumentasi Amazon Aurora
- Pengantar rincian kriptografi AWS KMS dalam dokumentasi AWS KMS
- Membuat strategi enkripsi perusahaan untuk data saat istirahat di Panduan AWS Preskriptif
- Menerapkan enkripsi saat istirahat di AWS Well-Architected Framework
- Untuk informasi selengkapnya tentang enkripsi secara spesifik Layanan AWS, lihat AWS dokumentasi untuk layanan tersebut

Enkripsi data dalam perjalanan

Data dalam transit adalah data yang secara aktif bergerak melalui jaringan Anda, seperti antar sumber daya jaringan. Enkripsi semua data dalam perjalanan dengan menggunakan protokol TLS aman dan cipher suite. Lalu lintas jaringan antara sumber daya dan internet harus dienkripsi

untuk membantu mencegah akses tidak sah ke data. Jika memungkinkan, gunakan TLS untuk mengenkripsi lalu lintas jaringan dalam lingkungan internal AWS Anda.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memerlukan HTTPS untuk komunikasi antara CloudFront pemirsa dan dalam CloudFront dokumentasi Amazon
- Dokumentasi AWS PrivateLink
- Menerapkan enkripsi dalam perjalanan di Kerangka AWS Well-Architected
- Untuk informasi selengkapnya tentang enkripsi secara spesifik Layanan AWS, lihat AWS dokumentasi untuk layanan tersebut

Blokir akses publik ke snapshot Amazon EBS

Amazon Elastic Block Store (Amazon EBS) menyediakan volume penyimpanan tingkat blok untuk digunakan dengan instans Amazon Elastic Compute Cloud (Amazon). EC2 Anda dapat mencadangkan data pada volume Amazon EBS Anda ke Amazon S3 dengan point-in-time mengambil snapshot. Anda dapat berbagi snapshot secara publik dengan semua yang lain Akun AWS, atau Anda dapat membagikannya secara pribadi dengan individu Akun AWS yang Anda tentukan.

Kami menyarankan Anda untuk tidak membagikan snapshot Amazon EBS secara publik. Ini mungkin secara tidak sengaja mengekspos data sensitif. Saat Anda membagikan snapshot, Anda memberi orang lain akses ke data dalam snapshot. Bagikan snapshot hanya dengan orang yang Anda percayai dengan semua data ini.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Bagikan snapshot di dokumentasi Amazon EC2
- Snapshot Amazon EBS tidak boleh dipulihkan secara publik dalam dokumentasi AWS Security Hub
- ebs-snapshot-public-restorable-periksa di dokumentasi AWS Config

Blokir akses publik ke snapshot Amazon RDS

Amazon Relational Database Service (Amazon RDS) membantu Anda menyiapkan, mengoperasikan, dan menskalakan database relasional di. AWS Cloud Amazon RDS membuat dan

menyimpan pencadangan otomatis instans database (DB) atau cluster DB multi-AZ selama jendela pencadangan instans DB Anda. Amazon RDS membuat cuplikan volume penyimpanan instans basis data Anda, sehingga mencadangkan seluruh instans basis data dan bukan hanya masing-masing basis data. Anda dapat membagikan snapshot manual untuk tujuan menyalin snapshot atau memulihkan instans DB darinya.

Jika Anda membagikan snapshot sebagai publik, pastikan tidak ada data dalam snapshot yang bersifat pribadi atau sensitif. Ketika snapshot dibagikan secara publik, itu memberikan semua Akun AWS izin untuk mengakses data. Hal ini dapat mengakibatkan eksposur data yang tidak diinginkan dalam instans Amazon RDS Anda.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Berbagi snapshot DB dalam dokumentasi Amazon RDS
- rds-snapshots-public-prohibiteddalam AWS Config dokumentasi
- Snapshot RDS harus bersifat pribadi dalam dokumentasi Security Hub

Blokir akses publik ke Amazon RDS, Amazon Redshift, dan sumber daya AWS DMS

Anda dapat mengonfigurasi instans Amazon RDS DB, kluster Amazon Redshift, AWS Database Migration Service dan instans replikasi AWS DMS() agar dapat diakses publik. Jika nilai `publiclyAccessible` bidangnya`true`, maka sumber daya ini dapat diakses publik. Memungkinkan akses publik dapat mengakibatkan lalu lintas, paparan, atau kebocoran data yang tidak perlu. Kami menyarankan Anda untuk tidak mengizinkan akses publik ke sumber daya ini.

Sebaiknya aktifkan AWS Config aturan atau kontrol Security Hub untuk mendeteksi apakah instans Amazon RDS DB, instans AWS DMS replikasi, atau kluster Amazon Redshift mengizinkan akses publik.

> **Note**
>
> Pengaturan akses publik untuk instance AWS DMS replikasi tidak dapat dimodifikasi setelah instance disediakan. Untuk mengubah pengaturan akses publik, hapus instance saat ini dan kemudian buat ulang. Saat Anda membuatnya ulang, jangan pilih opsi yang dapat diakses publik.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- AWS DMS instance replikasi tidak boleh bersifat publik dalam dokumentasi Security Hub
- Instans RDS DB harus melarang akses publik dalam dokumentasi Security Hub
- Cluster Amazon Redshift harus melarang akses publik dalam dokumentasi Security Hub
- rds-instance-public-access-periksa di dokumentasi AWS Config
- dms-replication-not-publicdalam AWS Config dokumentasi
- redshift-cluster-public-access-periksa di dokumentasi AWS Config
- Memodifikasi instans Amazon RDS DB dalam dokumentasi Amazon RDS
- Memodifikasi cluster dalam dokumentasi Amazon Redshift

Blokir akses publik ke bucket Amazon S3

Ini adalah praktik terbaik keamanan Amazon S3 untuk memastikan bahwa bucket Anda tidak dapat diakses publik. Kecuali Anda secara eksplisit mengharuskan siapa pun di internet untuk dapat membaca atau menulis ke ember Anda, pastikan ember Anda tidak publik. Ini membantu melindungi integritas dan keamanan data. Anda dapat menggunakan AWS Config aturan dan kontrol Security Hub untuk mengonfirmasi bahwa bucket Amazon S3 Anda sesuai dengan praktik terbaik ini.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Praktik terbaik keamanan Amazon S3 dalam dokumentasi Amazon S3
- Pengaturan Akses Publik Blok S3 harus diaktifkan dalam dokumentasi Security Hub
- Bucket S3 harus melarang akses baca publik dalam dokumentasi Security Hub
- Bucket S3 harus melarang akses tulis publik dalam dokumentasi Security Hub
- s3- bucket-public-read-prohibited aturan dalam dokumentasi AWS Config
- s3- bucket-public-write-prohibited dalam dokumentasi AWS Config

Memerlukan MFA untuk menghapus data di bucket Amazon S3 yang penting

Saat bekerja dengan Penentuan Versi S3 di bucket Amazon S3, Anda dapat secara opsional menambahkan lapisan keamanan lainnya dengan mengonfigurasi bucket untuk mengaktifkan Penghapusan MFA (autentikasi multi-faktor). Saat melakukannya, pemilik bucket harus menyertakan

dua bentuk autentikasi dalam setiap permintaan untuk menghapus sebuah versi atau mengubah status Penentuan Versi bucket. Kami menyarankan Anda mengaktifkan fitur ini untuk bucket yang berisi data yang penting bagi organisasi Anda. Ini dapat mencegah penghapusan bucket dan data yang tidak disengaja.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengkonfigurasi penghapusan MFA dalam dokumentasi Amazon S3

Konfigurasikan domain OpenSearch Layanan Amazon di VPC

Amazon OpenSearch Service adalah layanan terkelola yang membantu Anda menerapkan, mengoperasikan, dan menskalakan OpenSearch cluster di. AWS Cloud OpenSearch Layanan Amazon mendukung OpenSearch dan warisan Elasticsearch perangkat lunak sumber terbuka (OSS). Domain OpenSearch Layanan Amazon yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan Anda dengan membatasi akses ke data dalam perjalanan. Kami menyarankan agar Anda tidak melampirkan domain OpenSearch Layanan Amazon ke subnet publik dan VPC dikonfigurasi sesuai dengan praktik terbaik.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC di dokumentasi Layanan Amazon OpenSearch
- opensearch-in-vpc-onlydalam AWS Config dokumentasi
- OpenSearch domain harus dalam VPC dalam dokumentasi Security Hub

Konfigurasikan peringatan untuk penghapusan AWS KMS key

AWS Key Management Service (AWS KMS) kunci tidak dapat dipulihkan setelah dihapus. Jika kunci KMS dihapus, data yang masih dienkripsi di bawah kunci itu tidak dapat dipulihkan secara permanen. Jika Anda perlu mempertahankan akses ke data, sebelum Anda menghapus kunci, Anda harus mendekripsi data atau mengenkripsi ulang dengan kunci KMS baru. Anda harus menghapus kunci KMS hanya ketika Anda yakin bahwa Anda tidak perlu menggunakannya lagi.

Kami menyarankan Anda mengonfigurasi CloudWatch alarm Amazon yang memberi tahu Anda jika seseorang memulai penghapusan kunci KMS. Karena merusak dan berpotensi berbahaya

untuk menghapus kunci KMS, AWS KMS mengharuskan Anda menetapkan masa tunggu dan menjadwalkan penghapusan dalam 7-30 hari. Ini memberikan kesempatan untuk meninjau penghapusan yang dijadwalkan dan membatalkannya, jika perlu.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Menjadwalkan dan membatalkan penghapusan kunci dalam dokumentasi AWS KMS
- Membuat alarm yang mendeteksi penggunaan kunci KMS tertunda penghapusan dalam dokumentasi AWS KMS
- AWS KMS keys tidak boleh dihapus secara tidak sengaja dalam dokumentasi Security Hub

Blokir akses publik ke AWS KMS keys

Kebijakan utama adalah cara utama untuk mengontrol akses ke AWS KMS keys. Setiap kunci KMS memiliki persis satu kebijakan utama. Mengizinkan akses anonim ke kunci KMS dapat menyebabkan kebocoran data sensitif. Kami menyarankan Anda mengidentifikasi kunci KMS yang dapat diakses publik dan memperbarui kebijakan aksesnya untuk mencegah permintaan yang tidak ditandatangani yang dibuat untuk sumber daya ini.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Praktik terbaik keamanan untuk AWS Key Management Service dalam AWS KMS dokumentasi
- Mengubah kebijakan utama dalam AWS KMS dokumentasi
- Menentukan akses ke AWS KMS keys dalam AWS KMS dokumentasi

Konfigurasikan pendengar penyeimbang beban untuk menggunakan protokol aman

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas aplikasi yang masuk ke beberapa target. Anda mengkonfigurasi load balncer Anda untuk menerima lalu lintas masuk dengan menentukan satu atau lebihpendengar. Listener adalah proses yang memeriksa permintaan koneksi, menggunakan protokol dan port yang Anda konfigurasikan. Setiap jenis load balancer mendukung protokol dan port yang berbeda:

- Application Load Balancers membuat keputusan routing di lapisan aplikasi dan menggunakan protokol HTTP atau HTTPS.

- Network Load Balancers membuat keputusan routing di lapisan transport dan menggunakan protokol TCP, TLS, UDP, atau TCP_UDP.
- Classic Load Balancer membuat keputusan routing baik pada lapisan transport (dengan menggunakan protokol TCP atau SSL) atau pada lapisan aplikasi (dengan menggunakan protokol HTTP atau HTTPS).

Kami menyarankan Anda selalu menggunakan protokol HTTPS atau TLS. Protokol ini memastikan bahwa penyeimbang beban bertanggung jawab untuk mengenkripsi dan mendekripsi lalu lintas antara klien dan target.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Listener untuk Application Load Balancers Anda dalam dokumentasi Elastic Load Balancing
- Pendengar untuk Classic Load Balancer Anda dalam dokumentasi Elastic Load Balancing
- Pendengar untuk Network Load Balancer Anda dalam dokumentasi Elastic Load Balancing
- Pastikan penyeimbang AWS beban menggunakan protokol pendengar yang aman di Panduan Preskriptif AWS
- elb-tls-https-listeners-hanya dalam dokumentasi AWS Config
- Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS dalam dokumentasi Security Hub
- Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS dalam dokumentasi Security Hub

Rekomendasi keamanan untuk menanggapi insiden

Ketika peristiwa keamanan terjadi di organisasi Anda, pengguna Anda harus siap untuk menanggapi masalah tersebut. Semua pengguna harus memiliki pemahaman dasar tentang proses respons keamanan organisasi Anda. Perencanaan, pelatihan, dan pengalaman sangat penting untuk program respons insiden yang sukses. Idealnya, Anda mempersiapkan organisasi Anda sebelum peristiwa keamanan potensial terjadi. AWS Well-Architected Framework mengidentifikasi tiga fondasi yang diperlukan untuk program respons insiden yang sukses di cloud: persiapan, operasi, dan aktivitas pasca-insiden. Untuk informasi lebih lanjut, lihat Aspek respons AWS insiden dalam Kerangka AWS Well-Architected.

Dengan pengecualian kontrol keamanan yang memberi tahu Anda tentang peristiwa atau meresponsnya secara otomatis, ada kontrol terbatas yang dapat Anda buat untuk respons insiden. Postur respons insiden yang kuat terutama dibuat melalui rencana, proses, runbook, buku pedoman, dan program pelatihan yang Anda gunakan dalam organisasi Anda. Anda dapat menggunakan kontrol dan rekomendasi di bagian ini untuk menerapkan praktik terbaik untuk program respons insiden Anda. Untuk informasi lebih lanjut tentang praktik terbaik untuk respons insiden dan panduan implementasi, lihat Respons insiden dalam Kerangka Kerja AWS Well-Architected.

Rekomendasi di bagian ini:

- Tentukan rencana respons insiden
- Membuat dan memelihara runbook dan buku pedoman respons insiden
- Menerapkan otomatisasi keamanan berbasis peristiwa
- Dokumentasikan bagaimana tim operasional harus terlibat Dukungan
- Konfigurasikan peringatan untuk acara keamanan

Tentukan rencana respons insiden

Buat rencana respons insiden (IRP) yang terdefinisi dengan baik. Rencana respons insiden dirancang untuk menjadi dasar bagi program respons insiden Anda. Rencana ini harus disesuaikan untuk memenuhi kebutuhan masing-masing organisasi.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Kembangkan dan uji rencana respons insiden di Panduan Respons Insiden AWS Keamanan

- Mengembangkan rencana manajemen insiden dalam AWS Well-Architected Framework
- Identifikasi personel kunci dan sumber daya eksternal dalam AWS Well-Architected Framework

Membuat dan memelihara runbook dan buku pedoman respons insiden

Bagian penting dari mempersiapkan proses respons insiden adalah mengembangkan buku pedoman. Buku pedoman respons insiden menyediakan serangkaian langkah yang direkomendasikan yang diikuti pengguna saat peristiwa keamanan terjadi. Memiliki struktur dan langkah yang jelas menyederhanakan respons dan mengurangi kemungkinan kesalahan manusia.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Untuk apa membuat buku pedoman di Panduan Respons Insiden AWS Keamanan
- AWS contoh pedoman respons insiden pada GitHub
- Mengembangkan dan menguji pedoman respons insiden keamanan di AWS Well-Architected Framework

Menerapkan otomatisasi keamanan berbasis peristiwa

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

Banyak yang Layanan AWS mendukung tanggapan otomatis. Misalnya, Anda dapat mengonfigurasi CloudWatch alarm Amazon untuk metrik tertentu, dan alarm dapat memulai tindakan saat alarm berubah status. Melalui Amazon EventBridge, Anda juga dapat mengonfigurasi respons dan remediasi otomatis untuk temuan di AWS Security Hub dan Amazon Inspector.

Untuk informasi lebih lanjut, silakan lihat sumber daya di bawah ini:

- Memulihkan temuan keamanan Amazon Inspector secara otomatis di AWS Blog Keamanan
- Memulai otomatisasi respons keamanan AWS di Blog AWS Keamanan
- Respons keamanan otomatis AWS aktif di Perpustakaan AWS Solusi

- Menggunakan CloudWatch alarm Amazon dalam dokumentasi CloudWatch
- Respons dan remediasi otomatis dalam dokumentasi Security Hub
- Membuat tanggapan khusus terhadap temuan Amazon Inspector dengan Amazon EventBridge dalam dokumentasi Amazon Inspector

Dokumentasikan bagaimana tim operasional harus terlibat Dukungan

Untuk Anda Akun AWS, Anda dapat menentukan kontak utama dan tiga kontak alternatif. Kami menyarankan Anda memberikan kontak keamanan untuk masing-masing Akun AWS atau untuk organisasi Anda.

AWS Dukungan menawarkan berbagai rencana yang menyediakan akses ke alat dan keahlian yang dapat mendukung keberhasilan dan kesehatan operasional AWS solusi. Juga, pertimbangkan apakah organisasi Anda akan mendapat manfaat dari menggunakan AWS Managed Services alih-alih Dukungan rencana. AWS Managed Services (AMS) membantu Anda beroperasi lebih efisien dan aman dengan menyediakan pengelolaan AWS infrastruktur yang berkelanjutan, termasuk pemantauan, manajemen insiden, panduan keamanan, dukungan patch, dan pencadangan untuk beban AWS kerja. Model dukungan AMS dapat lebih cocok untuk organisasi yang memiliki sumber daya terbatas pada tim operasi cloud mereka. Kami menyarankan Anda membandingkan model dan rencana ini untuk memilih yang paling sesuai untuk kasus penggunaan organisasi dan tingkat kematangan cloud Anda.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memahami tim AWS respons dan dukungan dalam Panduan Respons Insiden AWS Keamanan
- Perbarui kontak alternatif untuk Anda Akun AWS di Panduan Manajemen AWS Akun
- Bandingkan Dukungan Paket di situs AWS web
- Strategi penggunaan AWS Managed Services untuk mencapai target hasil bisnis dalam Panduan AWS Preskriptif

Konfigurasikan peringatan untuk acara keamanan

Mendeteksi kelainan sama pentingnya dengan tindakan yang diterapkan untuk mengendalikan kelainan itu. Peringatan adalah komponen utama dari fase deteksi. Ini menghasilkan pemberitahuan

untuk memulai proses respons insiden berdasarkan Akun AWS aktivitas yang menarik. Pastikan bahwa peringatan menyertakan informasi yang relevan bagi tim untuk mengambil tindakan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Deteksi dalam Panduan Respons Insiden AWS Keamanan
- Mempersiapkan kemampuan forensik dalam AWS Well-Architected Framework
- Menerapkan peristiwa keamanan yang dapat ditindaklanjuti dalam Kerangka Well-Architected AWS

Langkah selanjutnya

Saat Anda melanjutkan perjalanan cloud Anda, penting untuk menerapkan kontrol, panduan, dan opsi remediasi yang terdokumentasi ini. Rekomendasi ini membantu meningkatkan postur keamanan cloud Anda dan membantu Anda memenuhi tanggung jawab keamanan Anda di AWS Cloud, sebagaimana didefinisikan dalam model tanggung jawab AWS bersama.

Untuk langkah selanjutnya, kami merekomendasikan yang berikut:

- Untuk informasi lebih lanjut tentang praktik terbaik dan panduan implementasi, tinjau enam pilar Kerangka Kerja AWS Well-Architected.
- Untuk Layanan AWS yang digunakan organisasi Anda, tinjau daftar AWS Security Hub kontrol yang tersedia dan evaluasi apakah Anda harus mengaktifkan salah satu kontrol ini di lingkungan Anda.
- Untuk Layanan AWS yang digunakan organisasi Anda, tinjau daftar aturan AWS Config terkelola yang tersedia dan evaluasi apakah Anda harus mengaktifkan salah satu aturan ini di lingkungan Anda.

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
MFA untuk pengguna root	Kami memperbarui rekomendasi dan memberikan informasi lebih lanjut di MFA untuk bagian pengguna root.	9 November 2023
Publikasi awal	—	Oktober 27, 2023

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan 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.

Pusat Keunggulan Cloud (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

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

FM

Lihat model pondasi.

model pondasi (FM)

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

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

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

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

data penahanan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet 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 lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. 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 dengan jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

ketekunan poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

Teknik 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 berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

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

publish/subscribe (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

LAP

Lihat Retrieval Augmented Generation.

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Wilayah

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan 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). Tipe dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

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

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

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

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

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

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

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS 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 jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

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

tugas yang tidak terdiferensiasi

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

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

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

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

data hangat

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

fungsi jendela

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

bisikan zero-shot

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

aplikasi zombie

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

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