Membuat strategi enkripsi perusahaan untuk data saat istirahat

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Membuat strategi enkripsi perusahaan untuk data saat istirahat

Table of Contents

Membuat strategi enkripsi perusahaan untuk data saat istirahat

Venki Srivatsav, Andrea Di Fabio, dan Vikramaditya Bhatnagar, Amazon Web Services ()AWS

September 2022 (sejarah dokumen)

Banyak perusahaan khawatir tentang ancaman keamanan siber dari pelanggaran data. Ketika pelanggaran data terjadi, orang yang tidak berwenang mendapatkan akses ke jaringan Anda dan mencuri data perusahaan. Firewall dan layanan anti-malware dapat membantu melindungi dari ancaman ini. Perlindungan lain yang dapat Anda terapkan adalah enkripsi data. Di bagian Tentang enkripsi data panduan ini, Anda dapat mempelajari lebih lanjut tentang cara kerja enkripsi data dan jenis yang tersedia.

Ketika Anda mendiskusikan enkripsi, secara umum, ada dua jenis data. Data dalam transit adalah data yang secara aktif bergerak melalui jaringan Anda, seperti antar sumber daya jaringan. Data saat istirahat adalah data yang stasioner dan tidak aktif, seperti data yang ada dalam penyimpanan. Strategi ini berfokus pada data saat istirahat. Untuk informasi selengkapnya tentang mengenkripsi data dalam perjalanan, lihat Melindungi data dalam perjalanan (Well-Architected AWS Framework).

Strategi enkripsi terdiri dari empat bagian yang Anda kembangkan dalam fase berurutan. Kebijakan enkripsi ditentukan oleh manajemen senior dan menguraikan peraturan, kepatuhan, dan persyaratan bisnis untuk enkripsi. Standar enkripsi membantu mereka yang menerapkan kebijakan untuk memahaminya dan mematuhinya. Standar dapat berupa teknologi atau prosedural. Kerangka kerja adalah prosedur operasi standar, struktur, dan pagar pembatas yang mendukung penerapan standar. Akhirnya, arsitektur adalah implementasi teknis dari standar enkripsi Anda, seperti lingkungan, layanan, dan alat yang Anda gunakan. Tujuan dari dokumen ini adalah untuk membantu Anda membuat strategi enkripsi yang sesuai dengan kebutuhan bisnis, keamanan, dan kepatuhan Anda. Ini mencakup rekomendasi tentang cara meninjau dan menerapkan standar keamanan untuk data saat istirahat sehingga Anda dapat memenuhi kepatuhan dan kebutuhan bisnis Anda secara holistik.

Strategi ini menggunakan AWS Key Management Service (AWS KMS) untuk membantu Anda membuat dan mengelola kunci kriptografi yang membantu melindungi data Anda. AWS KMS terintegrasi dengan banyak AWS layanan untuk mengenkripsi semua data Anda saat istirahat. Bahkan jika Anda memilih layanan enkripsi yang berbeda, Anda masih dapat mengadopsi rekomendasi dan fase dalam panduan ini.

Audiens yang dituju

Strategi ini dirancang untuk menangani audiens berikut:

- Pejabat eksekutif yang merumuskan kebijakan untuk perusahaan mereka, seperti CEOs, kepala petugas teknologi (CTOs), kepala petugas informasi (CIOs), dan kepala petugas keamanan informasi (CISOs)
- Petugas teknologi yang bertanggung jawab untuk menetapkan standar teknis, seperti wakil presiden dan direktur teknis
- Petugas kepatuhan dan tata kelola yang bertugas memantau kepatuhan terhadap kebijakan kepatuhan, termasuk rezim kepatuhan hukum dan sukarela

Hasil bisnis yang ditargetkan

- Data-at-rest kebijakan enkripsi — Pembuat keputusan dan kebijakan dapat membuat kebijakan enkripsi dan memahami faktor-faktor penting yang mempengaruhi kebijakan.
- Data-at-rest Standar enkripsi — Pemimpin teknis dapat mengembangkan standar enkripsi yang didasarkan pada kebijakan enkripsi.
- Kerangka kerja untuk enkripsi — Pemimpin teknis dan pelaksana dapat membuat kerangka kerja yang bertindak sebagai jembatan antara mereka yang menentukan kebijakan dan mereka yang membuat standar. Kerangka kerja, dalam konteks ini, berarti mengidentifikasi proses dan alur kerja yang sesuai yang membantu Anda menerapkan standar dalam batas-batas kebijakan. Kerangka kerja mirip dengan prosedur operasi standar atau proses manajemen perubahan untuk mengubah kebijakan atau standar.
- Arsitektur dan implementasi teknis — Pelaksana langsung, seperti pengembang dan arsitek, menyadari referensi arsitektur yang tersedia yang dapat membantu mereka menerapkan strategi enkripsi.

Batasan

Dokumen ini dimaksudkan untuk membantu Anda merumuskan strategi enkripsi khusus yang paling sesuai dengan kebutuhan perusahaan Anda. Ini bukan strategi enkripsi itu sendiri, dan itu bukan daftar periksa kepatuhan. Topik berikut tidak termasuk dalam dokumen ini:

- Mengenkripsi data dalam perjalanan

- Tokenisasi
- Hashing
- Kepatuhan dan tata kelola data
- Penganggaran untuk program enkripsi Anda

Untuk informasi lebih lanjut tentang beberapa topik ini, lihat Sumber daya bagian.

Tentang enkripsi data

Bagian ini berisi ikhtisar tingkat tinggi tentang konsep dan terminologi enkripsi. Enkripsi data membantu Anda menegakkan kerahasiaan data. Dengan menerapkan enkripsi dan kontrol akses, Anda dapat membantu melindungi data di perusahaan Anda.

Tentang kunci enkripsi

Layanan enkripsi menggunakan kunci enkripsi untuk mengenkripsi data. Kunci enkripsi adalah string kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik. Kekuatan enkripsi biasanya tergantung pada dua faktor: panjang kunci dan algoritma yang digunakan. Secara umum, kunci yang lebih panjang memberikan enkripsi yang lebih kuat.

Tentang algoritma enkripsi

Ada dua jenis algoritma untuk menghasilkan kunci enkripsi, simetris dan asimetris.

Enkripsi simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Jenis enkripsi ini biasanya lebih cepat dan, oleh karena itu, efisien untuk sejumlah besar data. Jenis enkripsi ini banyak digunakan dan diterima secara umum untuk aman. Karena satu kunci digunakan untuk enkripsi dan dekripsi, praktik terbaik adalah sering mengubah kunci untuk mencegah orang yang tidak berwenang mendapatkannya. Untuk informasi selengkapnya tentang kapan enkripsi simetris direkomendasikan, lihat Kapan saya membutuhkan enkripsi simetris? di bagian FAQ.

Enkripsi asimetris 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. Enkripsi asimetris umumnya dianggap lebih aman daripada enkripsi simetris, tetapi lebih lambat karena menggunakan panjang kunci yang lebih panjang dan memerlukan perhitungan enkripsi yang lebih kompleks. Untuk informasi selengkapnya tentang kapan enkripsi asimetris direkomendasikan, lihat Kapan saya membutuhkan enkripsi asimetris? di bagian FAQ.

Tentang enkripsi amplop

Ketika Anda mengenkripsi data Anda, itu dilindungi hanya selama kunci enkripsi Anda tetap rahasia. Kunci yang digunakan untuk mengenkripsi data dikenal sebagai kunci data. Enkripsi amplop adalah

praktik mengenkripsi kunci data Anda dengan kunci enkripsi lain, yang disebut kunci enkripsi kunci. Anda bahkan dapat mengenkripsi kunci itu dengan kunci enkripsi lain, dan seterusnya. Akhirnya, satu kunci harus tetap dalam plaintext sehingga Anda dapat mendekripsi kunci dan data Anda. Kunci enkripsi kunci plaintext tingkat atas ini dikenal sebagai kunci root.

Enkripsi amplop menawarkan beberapa manfaat:

- Kenyamanan — Karena kunci data Anda dienkripsi, Anda dapat menyimpannya dengan data terenkripsi.
- Efisiensi — Operasi enkripsi dapat memakan waktu, terutama ketika itu sejumlah besar data. Alih-alih mengenkripsi ulang data mentah beberapa kali dengan kunci yang berbeda, Anda dapat mengenkripsi ulang hanya kunci data yang melindungi data mentah. Ini memungkinkan Anda untuk menyediakan dua atau lebih lapisan perlindungan enkripsi tanpa mengenkripsi ulang data.
- Kinerja - Anda dapat menggabungkan algoritma enkripsi. Misalnya, Anda dapat menggunakan enkripsi simetris untuk data mentah tetapi menggunakan enkripsi asimetris untuk kunci data, yang menggabungkan kekuatan kedua algoritma enkripsi.

Untuk informasi selengkapnya tentang enkripsi amplop, lihat Enkripsi amplop (AWS Key Management Service dokumentasi). Untuk informasi selengkapnya tentang memutuskan apakah Anda memerlukan enkripsi amplop, lihat Kapan saya membutuhkan enkripsi amplop? di bagian FAQ.

Fase membangun strategi enkripsi

Membangun strategi enkripsi tingkat perusahaan membutuhkan pendekatan multi-fase. Setiap fase mendefinisikan satu set kontrol untuk membantu Anda mencapai hasil yang diinginkan dan nyata. Dokumen ini memandu Anda melalui fase-fase ini dan mengajukan pertanyaan spesifik untuk membantu Anda menyesuaikan strategi enkripsi Anda.

Membangun strategi enkripsi untuk data saat istirahat terdiri dari fase berurutan berikut:

1. Kebijakan enkripsi— Bangun kebijakan yang menentukan tujuan data-at-rest enkripsi untuk perusahaan Anda.
2. Standar enkripsi— Tentukan standar teknis dan prosedural yang membantu Anda mewujudkan kebijakan bisnis Anda.
3. Kerangka enkripsi— Bangun kerangka kerja yang membantu semua pemangku kepentingan memahami, mengubah, dan menerapkan standar enkripsi Anda.
4. Implementasi— Menyebarkan infrastruktur enkripsi Anda.

Kebijakan enkripsi

Tujuan dari kebijakan enkripsi adalah untuk menetapkan, pada tingkat manajemen senior, harapan bisnis dan kepatuhan yang perlu dipenuhi organisasi. Kebijakan ini berfungsi sebagai titik awal untuk menentukan strategi enkripsi yang sesuai. Kebijakan harus cukup abstrak untuk memberikan kebebasan dan fleksibilitas untuk implementasi. Pada saat yang sama, itu harus cukup spesifik untuk menentukan batas-batas implementasi yang dapat diterima yang memenuhi tujuan organisasi. Secara umum, kebijakan bersifat teknologi-agnostik dan sangat jarang diubah karena mereka menentukan karakteristik dasar dari strategi enkripsi perusahaan Anda.

Biasanya, kebijakan enkripsi mengandung, tetapi tidak terbatas pada, hal-hal berikut:

- Rezim peraturan atau kepatuhan apa pun yang harus dipenuhi perusahaan Anda
- Komitmen atau harapan bisnis apa pun untuk enkripsi data
- Jenis data yang harus dienkripsi
- Kriteria kapan harus menggunakan teknik perlindungan data selain enkripsi, seperti hashing atau tokenisasi

Tingkat manajemen tertinggi organisasi, seperti CIO, CTO, dan CISO, biasanya mendefinisikan dan menyetujui kebijakan enkripsi.

Pertimbangkan hal berikut saat membuat kebijakan enkripsi Anda:

- Lini bisnis Anda menentukan kepatuhan dan rezim peraturan yang harus Anda patuhi. Rezim ini menentukan persyaratan enkripsi data. Keputusan tingkat eksekutif untuk memperluas bisnis ke wilayah baru atau memperluas penawaran produk dapat memengaruhi peraturan mana yang berlaku untuk data Anda. Misalnya, jika bank memutuskan untuk menawarkan kartu kredit kepada pelanggannya, mereka mungkin harus mematuhi Standar Keamanan Data industri kartu pembayaran (PCI-DSS), yang memerlukan enkripsi data.
- Kebijakan Anda harus menentukan jenis data apa yang perlu dienkripsi. Ini bervariasi berdasarkan persyaratan kepatuhan dan tujuan penanganan data perusahaan Anda. Misalnya, kebijakan Anda mungkin menyatakan bahwa data apa pun yang ditangkap atau dimiliki bisnis harus dienkripsi saat istirahat.
- Kebijakan enkripsi Anda harus selaras dengan standar kategorisasi data internal Anda. Untuk merumuskan kebijakan enkripsi yang efektif, penentuan kategori data pada tingkat metadata diperlukan. Misalnya, kategori Anda mungkin mencakup data publik, internal, rahasia, rahasia, atau pelanggan.
- Sertakan kriteria bagaimana menentukan data mana yang harus dienkripsi dan data mana yang harus dilindungi dengan teknik lain, seperti tokenisasi atau hashing. Misalnya, kebijakan Anda mungkin menyatakan Informasi Identifikasi Pribadi (PII) apa pun yang masuk ke audit, jejak, atau log aplikasi harus diberi token.

Standar enkripsi

Standar berasal dari kebijakan Anda. Ini lebih sempit dalam lingkup dan membantu mendefinisikan kerangka kerja dan arsitektur untuk implementasi. Misalnya, jika kebijakan organisasi Anda adalah mengenkripsi data Anda saat istirahat, maka standar akan menentukan jenis enkripsi apa yang diperlukan dan memberikan arahan umum tentang cara mematuhi kebijakan tersebut.

Standar enkripsi biasanya menentukan yang berikut:

- Jenis enkripsi yang harus digunakan
- Spesifikasi minimum untuk kunci enkripsi
- Siapa yang memiliki akses ke kunci enkripsi
- Dimana kunci enkripsi harus disimpan

- Kriteria untuk memilih kekuatan kunci yang tepat saat memilih teknik enkripsi atau hashing
- Frekuensi rotasi kunci

Meskipun Anda jarang perlu memperbarui kebijakan enkripsi, standar enkripsi dapat berubah. Industri keamanan siber terus berkembang untuk memenuhi lanskap ancaman yang terus berubah. Dengan demikian, standar Anda harus berubah untuk mengadopsi teknologi terbaru dan praktik terbaik untuk memberikan perlindungan terbaik untuk data perusahaan Anda.

Dalam organisasi perusahaan, wakil presiden, direktur, atau pengelola data biasanya menentukan standar enkripsi, dan petugas kepatuhan biasanya meninjau dan menyetujuinya.

Pertimbangkan kategori faktor berikut saat menentukan dan memelihara standar enkripsi di organisasi Anda:

- Pertimbangan biaya dan kinerja
- Kontrol akses kunci
- Jenis enkripsi
- Spesifikasi kunci enkripsi
- Lokasi penyimpanan kunci

Pertimbangan biaya dan kinerja

Pertimbangkan faktor operasional berikut saat menentukan standar enkripsi untuk data saat istirahat:

- Sumber daya perangkat keras yang tersedia harus dapat mendukung standar Anda dalam skala besar.
- Biaya enkripsi bervariasi berdasarkan panjang kunci, jumlah data, dan waktu yang diperlukan untuk melakukan enkripsi. Misalnya, jika dibandingkan dengan enkripsi simetris, enkripsi asimetris menggunakan kunci yang lebih panjang dan membutuhkan lebih banyak waktu.
- Pertimbangkan persyaratan kinerja aplikasi perusahaan Anda. Jika aplikasi Anda memerlukan latensi rendah dan throughput tinggi, maka Anda mungkin ingin menggunakan enkripsi simetris.

Kontrol akses kunci

Identifikasi kebijakan kontrol akses untuk kunci enkripsi Anda berdasarkan prinsip hak istimewa paling sedikit. Keistimewaan paling sedikit adalah praktik keamanan terbaik untuk memberikan

pengguna akses minimum yang mereka butuhkan untuk menjalankan fungsi pekerjaan mereka. Dalam standar Anda, tentukan kebijakan kontrol akses yang:

- Mengidentifikasi peran yang mengelola kunci enkripsi kunci dan kunci data.
- Mendefinisikan dan memetakan izin kunci untuk peran. Misalnya, mendefinisikan siapa yang memiliki hak istimewa admin utama dan siapa yang memiliki dan hak istimewa pengguna utama. Admin kunci dapat membuat atau memodifikasi kunci enkripsi kunci, dan pengguna kunci dapat mengenkripsi dan mendekripsi data dan menghasilkan kunci data.

Jenis enkripsi

Dalam standar Anda, tentukan jenis dan fitur enkripsi mana yang cocok untuk organisasi Anda:

- Dokumentasikan kapan harus menggunakan algoritma enkripsi simetris dan asimetris. Untuk informasi lebih lanjut, lihat Kapan saya membutuhkan enkripsi simetris? dan Kapan saya membutuhkan enkripsi asimetris? di bagian FAQ.
- Putuskan apakah Anda harus menggunakan enkripsi amplop, dan tentukan situasinya. Untuk informasi lebih lanjut, lihat Kapan saya membutuhkan enkripsi amplop? di bagian FAQ.
- Tentukan kriteria kapan harus menggunakan alternatif enkripsi, seperti tokenisasi dan hashing.

Spesifikasi kunci enkripsi

Tentukan spesifikasi yang diperlukan untuk kunci enkripsi Anda, seperti kekuatan kunci dan algoritme. Spesifikasi ini harus mematuhi rezim peraturan dan kepatuhan yang ditentukan dalam kebijakan. Pertimbangkan untuk mendefinisikan spesifikasi berikut:

- Tentukan kekuatan kunci minimum dan algoritma untuk jenis enkripsi simetris dan asimetris. Faktor-faktor kekuatan kunci termasuk panjang, keacakan, dan keunikan.
- Tentukan kapan Anda ingin menerapkan versi baru algoritma enkripsi. Misalnya, standar Anda mungkin menyatakan Implementasikan versi terbaru algoritme dalam waktu 30 hari setelah rilis atau Selalu gunakan satu versi yang lebih lama dari rilis terbaru.
- Tentukan interval untuk memutar kunci enkripsi Anda.

Lokasi penyimpanan kunci

Dalam standar Anda, pertimbangkan hal berikut saat memutuskan tempat menyimpan kunci enkripsi Anda:

- Kepatuhan dan persyaratan peraturan mungkin menentukan di mana kunci enkripsi Anda dapat disimpan.
- Putuskan apakah Anda ingin menyimpan kunci di lokasi terpusat atau dengan data yang sesuai. Untuk informasi lebih lanjut, lihat Mengapa saya harus mengelola kunci enkripsi secara terpusat? di bagian FAQ.
- Jika Anda memilih penyimpanan terpusat, putuskan apakah akan menyimpan kunci dalam infrastruktur yang dikelola perusahaan, seperti modul keamanan perangkat keras (HSM), atau penyedia layanan terkelola, seperti. AWS Key Management Service Untuk informasi lebih lanjut, lihat Kapan saya harus menggunakan modul keamanan perangkat keras (HSM)? di bagian FAQ.

Kerangka enkripsi

Kerangka kerja, dalam konteks ini, mengacu pada seperangkat prosedur operasi standar yang perlu diikuti ketika Anda memodifikasi standar atau kebijakan enkripsi. Kerangka kerja adalah perancah yang membantu Anda menerapkan standar. Ini membantu mengubah kata-kata menjadi tindakan. Kerangka kerja menghubungkan orang-orang yang mendefinisikan standar dengan orang-orang yang menerapkannya.

Kerangka kerja biasanya mencakup topik-topik berikut:

- Klasifikasi data
- Klasifikasi lingkungan
- Ubah peristiwa dan proses

Klasifikasi data

Klasifikasi data memainkan peran penting dalam menciptakan strategi enkripsi. Klasifikasi data adalah proses penetapan data ke kategori berdasarkan sensitivitas data. Berikut ini adalah kategori klasifikasi data umum, dalam urutan sensitivitas yang meningkat: publik, pribadi, internal, rahasia, dan terbatas.

Kerangka enkripsi Anda harus menyertakan informasi berikut tentang klasifikasi data:

- Kategori klasifikasi data untuk perusahaan Anda.
- Kriteria klasifikasi yang digunakan untuk mengklasifikasikan data ke dalam kategori yang sesuai. Misalnya, resep perdagangan perusahaan dapat diklasifikasikan sebagai dibatasi, PII karyawan dapat bersifat rahasia, dan komunikasi internal antara karyawan melalui saluran resmi mungkin bersifat internal.
- Proses yang digunakan untuk mempromosikan dan menurunkan data antar kategori.
- Kriteria akses untuk setiap kategori klasifikasi data.
- Jenis kunci enkripsi yang diperlukan untuk setiap kategori.

Klasifikasi lingkungan

Perusahaan Anda mungkin memiliki beberapa lingkungan, seperti pengembangan, pengujian, kotak pasir, praproduksi, dan produksi. Setiap lingkungan dapat berisi berbagai jenis data dan memiliki persyaratan enkripsi yang berbeda.

Kerangka enkripsi Anda harus menyertakan informasi berikut tentang lingkungan Anda:

- Tentukan lingkungan perusahaan Anda.
- Tentukan persyaratan enkripsi untuk setiap lingkungan. Misalnya, Anda mungkin menggunakan kunci enkripsi tunggal untuk semua kategori data di lingkungan pengembangan Anda, dan di lingkungan produksi Anda, Anda mungkin menggunakan kunci enkripsi yang berbeda untuk setiap aplikasi bisnis atau kategori klasifikasi data.

Ubah peristiwa dan proses

Standar enkripsi dapat sering berubah sehingga Anda dapat mengikuti teknologi terbaru, praktik terbaik, dan inovasi. Berikut ini adalah peristiwa perubahan umum yang mungkin memulai revisi standar enkripsi Anda:

- Perubahan panjang minimum kunci enkripsi
- Perubahan kekuatan algoritma enkripsi
- Perubahan pada siapa yang dapat mengakses kunci enkripsi atau caranya
- Perubahan interval rotasi untuk kunci Anda
- Perubahan pada proses untuk menghapus kunci
- Perubahan pada lokasi penyimpanan utama atau kebijakan

- Perubahan pada proses pencadangan dan pemulihan kunci

Kerangka kerja enkripsi Anda harus mencakup hal-hal berikut untuk membantu mempersiapkan organisasi Anda mengelola, menerapkan, dan mengkomunikasikan perubahan pada standar atau kebijakan enkripsi:

- Proses kontrol perubahan — Tujuan dari proses ini adalah untuk merencanakan dan mempersiapkan perubahan yang akan datang. Saat Anda perlu mengubah standar atau kebijakan enkripsi, proses yang dapat diulang dan dapat diskalakan ini dirancang untuk menentukan:
  - Bagaimana organisasi Anda menilai dampak perubahan
  - Siapa yang bisa memulai perubahan
  - Siapa yang bertanggung jawab untuk menerapkan perubahan
  - Siapa yang bertanggung jawab untuk menyetujui perubahan
  - Bagaimana organisasi Anda akan mengembalikan perubahan, jika perlu
- Ubah proses auditabilitas dan keterlacakan — Proses ini mendefinisikan bagaimana organisasi Anda mengaudit dan melacak perubahan, baik di tingkat metadata maupun di tingkat data. Ini harus menentukan bagaimana Anda menyimpan dan mengakses catatan:
  - Apa yang berubah
  - Ketika itu diubah
  - Siapa yang memprakarsai, menyetujui, dan menerapkan perubahan

  Misalnya, jika organisasi Anda mengubah kekuatan kunci enkripsi minimum, Anda harus dapat menentukan persyaratan asli dan baru, kapan perubahan itu efektif, dan siapa yang terlibat dalam proses perubahan.
- Proses peluncuran perubahan — Tujuan dari proses ini adalah untuk menentukan bagaimana organisasi Anda menerapkan perubahan setelah Anda memutuskan untuk membuatnya. Proses ini mendefinisikan:
  - Siapa pemangku kepentingan
  - Apakah Anda harus menyelesaikan pilot atau bukti konsep
  - Bagaimana dan kapan Anda harus mengomunikasikan status perubahan
  - Cara memutar kembali perubahan, jika perlu.
  - Berapa periode pengamatan yang seharusnya setelah menerapkan perubahan.
  - Apa proses observasi untuk memantau dampak perubahan, termasuk bagaimana mengumpulkan umpan balik tentang perubahan dan menilai efektivitas

- Proses pensiun — Tujuan dari proses ini adalah untuk menentukan bagaimana organisasi Anda menangani pensiun sumber daya dan informasi terkait enkripsi. Ini termasuk instruksi untuk pensiun yang sebenarnya serta proses komunikasi untuk pensiun.

Implementasi

Dalam strategi ini, arsitektur mengacu pada implementasi teknis standar enkripsi Anda. Bagian ini mencakup informasi tentang bagaimana Layanan AWS, seperti AWS Key Management Service (AWS KMS) dan AWS CloudHSM, dapat membantu Anda menerapkan strategi data-at-rest enkripsi sesuai dengan kebijakan dan standar Anda.

AWS KMS adalah layanan terkelola yang membantu Anda membuat dan mengontrol kunci kriptografi yang digunakan untuk melindungi data Anda. Kunci KMS tidak pernah meninggalkan layanan tidak terenkripsi. Untuk menggunakan atau mengelola kunci KMS Anda, Anda berinteraksi dengan AWS KMS, dan banyak Layanan AWS yang terintegrasi dengannya AWS KMS.

AWS CloudHSM adalah layanan kriptografi untuk membuat dan memelihara modul keamanan perangkat keras (HSMs) di AWS lingkungan Anda. HSMs adalah perangkat komputasi yang memproses operasi kriptografi dan menyediakan penyimpanan yang aman untuk kunci kriptografi. Jika standar Anda mengharuskan Anda untuk menggunakan perangkat keras yang divalidasi FIPS 140-2 Level 3, atau jika standar Anda menentukan penggunaan standar industri, seperti PKCS #11 APIs, Java Cryptography Extensions (JCE), dan Microsoft CryptOong (CNG), maka Anda dapat mempertimbangkan untuk menggunakannya. AWS CloudHSM

Anda dapat mengonfigurasi AWS CloudHSM sebagai toko kunci khusus untuk AWS KMS. Solusi ini menggabungkan kenyamanan dan integrasi layanan AWS KMS dengan kontrol tambahan dan manfaat kepatuhan menggunakan AWS CloudHSM cluster di Anda Akun AWS. Untuk informasi selengkapnya, lihat Toko kunci khusus (AWS KMS dokumentasi).

Dokumen ini membahas AWS KMS fitur pada tingkat tinggi dan menjelaskan bagaimana AWS KMS dapat mengatasi kebijakan dan standar Anda.

Biaya, kenyamanan, dan kontrol

AWS KMS menawarkan berbagai jenis kunci. Beberapa dimiliki atau dikelola oleh AWS, dan yang lainnya dibuat dan dikelola oleh pelanggan. Anda dapat memilih di antara opsi-opsi ini berdasarkan tingkat kontrol yang ingin Anda miliki atas pertimbangan kunci dan biaya:

- AWS kunci yang AWS dimiliki — memiliki dan mengelola kunci ini, dan mereka digunakan dalam beberapa Akun AWS. Beberapa kunci Layanan AWS dukungan AWS yang dimiliki. Anda dapat menggunakan kunci ini tanpa biaya. Jenis kunci ini membebaskan Anda dari biaya dan overhead administratif untuk mengelola siklus hidup kunci dan akses ke sana. Untuk informasi selengkapnya tentang jenis kunci ini, lihat kunci yang AWS dimiliki (AWS KMS dokumentasi).
- AWS kunci terkelola — Jika terintegrasi Layanan AWS dengan AWS KMS, ia dapat membuat, mengelola, dan menggunakan jenis kunci ini atas nama Anda, untuk melindungi sumber daya Anda dalam layanan itu. Kunci ini dibuat di Anda Akun AWS, dan hanya Layanan AWS dapat menggunakannya. Tidak ada biaya bulanan untuk kunci yang AWS dikelola. Mereka dapat dikenakan biaya untuk penggunaan melebihi tingkat gratis, tetapi beberapa Layanan AWS menutupi biaya ini untuk Anda. Anda dapat menggunakan kebijakan identitas untuk mengontrol tampilan dan mengaudit akses untuk kunci ini, tetapi AWS mengelola siklus hidup kunci. Untuk informasi selengkapnya tentang jenis kunci ini, lihat kunci AWS terkelola (AWS KMS dokumentasi). Untuk daftar lengkap Layanan AWS yang terintegrasi dengan AWS KMS, lihat Layanan AWS integrasi (AWS pemasaran).
- Kunci terkelola pelanggan — Anda membuat, memiliki, dan mengelola jenis kunci ini, dan Anda memiliki kontrol penuh atas siklus hidup kunci. Untuk pemisahan tugas, Anda dapat menggunakan kebijakan berbasis identitas dan sumber daya untuk mengontrol akses ke kunci. Anda juga dapat mengatur rotasi kunci otomatis. Kunci yang dikelola pelanggan dikenakan biaya bulanan, dan jika Anda melebihi tingkat gratis, mereka juga dikenakan biaya untuk digunakan. Untuk informasi selengkapnya tentang jenis kunci ini, lihat Kunci terkelola pelanggan (AWS KMS dokumentasi).

Untuk informasi selengkapnya tentang penyimpanan dan penggunaan kunci, lihat AWS Key Management Service harga (AWS pemasaran).

Jenis kinerja dan enkripsi

Berdasarkan jenis enkripsi yang dipilih dalam standar, Anda dapat menggunakan dua jenis kunci KMS.

- Simetris — Semua AWS KMS key jenis mendukung enkripsi simetris. Saat mengenkripsi kunci yang dikelola pelanggan, Anda dapat menggunakan kunci kekuatan tunggal untuk enkripsi dan dekripsi dengan AES-256-GCM.
- Asimetris - Kunci yang dikelola pelanggan mendukung enkripsi asimetris. Anda dapat memilih antara kekuatan kunci dan algoritma yang berbeda, berdasarkan tujuan penggunaan Anda. Kunci asimetris dapat mengenkripsi dan mendekripsi dengan RSA dan dapat menandatangani

dan memverifikasi operasi dengan RSA atau ECC. Algoritma kunci asimetris secara inheren memberikan pemisahan peran dan menyederhanakan manajemen kunci. Saat menggunakan enkripsi asimetris dengan AWS KMS, beberapa operasi tidak didukung, seperti memutar kunci dan mengimpor materi kunci eksternal.

Untuk informasi selengkapnya tentang AWS KMS operasi yang didukung kunci simetris dan asimetris, lihat Referensi tipe kunci (AWS KMS dokumentasi).

Enkripsi amplop

Enkripsi amplop dibangun ke dalam AWS KMS. Di AWS KMS, Anda menghasilkan kunci data dalam format teks biasa atau terenkripsi. Kunci data terenkripsi dienkripsi dengan kunci KMS. Anda dapat menyimpan kunci KMS di toko kunci khusus dalam sebuah AWS CloudHSM cluster. Untuk informasi lebih lanjut tentang manfaat enkripsi amplop, lihatTentang enkripsi amplop.

Lokasi penyimpanan kunci

Anda menggunakan kebijakan untuk mengelola akses ke AWS KMS sumber daya. Kebijakan menggambarkan siapa yang dapat mengakses sumber daya mana. Kebijakan yang dilampirkan pada prinsipal AWS Identity and Access Management (IAM) disebut kebijakan berbasis identitas atau kebijakan IAM. Kebijakan yang melekat pada jenis sumber daya lain disebut kebijakan sumber daya. AWS KMS kebijakan sumber daya untuk AWS KMS keys disebut kebijakan kunci. Setiap kunci KMS memiliki kebijakan kunci.

Kebijakan utama memberikan fleksibilitas untuk menyimpan kunci enkripsi di lokasi pusat atau menyimpannya lebih dekat ke data, secara terdistribusi. Pertimbangkan AWS KMS fitur-fitur berikut saat Anda memutuskan tempat menyimpan kunci KMS di: Akun AWS

- Dukungan infrastruktur Single-Region - Secara default, kunci KMS bersifat spesifik Wilayah, dan tidak pernah dibiarkan tidak terenkripsi. AWS KMS Jika standar Anda memiliki persyaratan ketat untuk mengontrol kunci di lokasi geografis tertentu, jelajahi menggunakan kunci Wilayah tunggal.
- Dukungan infrastruktur Multi-Region — AWS KMS juga mendukung tipe kunci tujuan khusus yang disebut Multi-region keys. Menyimpan data dalam beberapa Wilayah AWS adalah konfigurasi umum untuk pemulihan bencana. Dengan menggunakan kunci Multi-region, Anda dapat mentransfer data antar Wilayah tanpa mengenkripsi ulang, dan Anda dapat mengelola data seolah-olah Anda memiliki kunci yang sama di setiap Wilayah. Fungsionalitas ini sangat berguna jika standar Anda mengharuskan infrastruktur enkripsi Anda mencakup beberapa Wilayah dalam

konfigurasi aktif-aktif. Untuk informasi selengkapnya, lihat Kunci Multi-Wilayah (AWS KMS dokumentasi).

- Manajemen terpusat — Jika standar Anda mengharuskan Anda menyimpan kunci di lokasi terpusat, Anda dapat menggunakannya AWS KMS untuk menyimpan semua kunci enkripsi Anda dalam satu. Akun AWS Anda menggunakan kebijakan utama untuk memberikan akses ke aplikasi lain, yang dapat berada di akun berbeda di Wilayah yang sama. Manajemen kunci terpusat dapat mengurangi overhead administratif untuk mengelola siklus hidup kunci dan kontrol akses kunci.
- Materi kunci eksternal - Anda dapat mengimpor materi kunci yang dihasilkan secara eksternal ke dalam. AWS KMS Support untuk fungsi ini tersedia untuk kunci simetris tunggal dan Multi-wilayah. Karena bahan kunci simetris dihasilkan secara eksternal, Anda bertanggung jawab untuk melindungi bahan kunci yang dihasilkan. Untuk informasi selengkapnya, lihat Materi kunci yang diimpor (AWS KMS dokumentasi).

Kontrol akses

Di AWS KMS, Anda dapat menerapkan kontrol akses tingkat terperinci dengan menggunakan mekanisme kebijakan berikut: kebijakan utama, kebijakanIAM, dan hibah. Dengan menggunakan kontrol ini, Anda dapat mengatur pemisahan tugas berdasarkan peran, seperti administrator, pengguna kunci yang dapat mengenkripsi data, pengguna kunci yang dapat mendekripsi data, dan pengguna kunci yang dapat mengenkripsi dan mendekripsi data. Untuk informasi selengkapnya, lihat Otentikasi dan kontrol akses (AWS KMS dokumentasi).

Audit dan pencatatan

AWS KMS terintegrasi dengan AWS CloudTrail dan Amazon EventBridge untuk tujuan pencatatan dan pemantauan. Semua operasi AWS KMS API dicatat dan dapat diaudit dalam CloudTrail log. Anda dapat menggunakan Amazon CloudWatch, EventBridge, dan AWS Lambda menyiapkan solusi pemantauan khusus untuk mengonfigurasi notifikasi dan remediasi otomatis. Untuk informasi selengkapnya, lihat Pencatatan dan pemantauan (AWS KMS dokumentasi).

Pertanyaan yang Sering Diajukan

Bagian ini memberikan jawaban atas pertanyaan yang sering diajukan saat menentukan standar enkripsi Anda atau saat membuat infrastruktur enkripsi Anda dalam fase implementasi.

Kapan saya membutuhkan enkripsi simetris?

Anda dapat menggunakan enkripsi simetris saat:

- Kecepatan, biaya, dan overhead komputasi yang lebih rendah adalah prioritas.
- Anda perlu mengenkripsi sejumlah besar data.
- Data terenkripsi tidak meninggalkan batas-batas jaringan organisasi.

Kapan saya membutuhkan enkripsi asimetris?

Anda dapat menggunakan enkripsi asimetris saat:

- Anda perlu berbagi data di luar organisasi.
- Peraturan atau tata kelola melarang berbagi kunci.
- Diperlukan nonrepudiation. (Nonrepudiation mencegah pengguna menyangkal komitmen atau tindakan sebelumnya.)
- Anda perlu memisahkan akses ke kunci enkripsi secara ketat berdasarkan peran organisasi.

Kapan saya membutuhkan enkripsi amplop?

Anda perlu mendukung dan menerapkan enkripsi amplop jika kebijakan enkripsi Anda memerlukan rotasi kunci. Beberapa rezim tata kelola dan kepatuhan memerlukan rotasi kunci, atau kebijakan Anda mungkin mengamanatkannya untuk memenuhi kebutuhan bisnis.

Kapan saya harus menggunakan modul keamanan perangkat keras (HSM)?

Anda mungkin memerlukan HSM jika kebijakan Anda menentukan kepatuhan terhadap:

- Standar Pengolahan Informasi Federal (FIPS) 140-2 level 3 standar enkripsi. Untuk informasi selengkapnya, lihat validasi FIPS (AWS CloudHSM dokumentasi).
- Standar industri APIs, seperti PKCS #11, Java Cryptography Extension (JCE), atau Microsoft Cryptography API: Next Generation (CNG)

Mengapa saya harus mengelola kunci enkripsi secara terpusat?

Berikut ini adalah manfaat umum dari manajemen kunci terpusat:

- Karena kunci digunakan dan dikelola di lokasi yang berbeda, Anda dapat menggunakan kembali kunci, yang dapat mengurangi biaya.
- Anda memiliki kontrol lebih besar atas akses ke kunci enkripsi.
- Menyimpan kunci di satu lokasi memudahkan untuk melihat, mengaudit, dan memperbarui kunci jika terjadi perubahan standar.

Apakah saya perlu menggunakan infrastruktur enkripsi yang dibuat khusus untuk data saat istirahat?

Perusahaan Anda memerlukan infrastruktur enkripsi jika salah satu dari berikut ini benar:

- Perusahaan Anda menangani dan menyimpan data klasifikasi apa pun selain publik.
- Perusahaan Anda menangkap dan menyimpan data tentang karyawan atau pelanggan.
- Perusahaan Anda menangani data PII.
- Perusahaan Anda harus mematuhi rezim peraturan atau tata kelola yang memerlukan data untuk dienkripsi.
- Kepemimpinan eksekutif perusahaan Anda telah mengamanatkan enkripsi semua data saat istirahat.

Bagaimana dapat AWS KMS membantu organisasi saya memenuhi tujuan enkripsi untuk data saat istirahat?

Selain banyak fitur lainnya, AWS Key Management Service dapat membantu Anda:

- Gunakan enkripsi amplop.

- Kontrol akses kunci enkripsi, seperti memisahkan administrasi kunci dari penggunaan kunci.
- Bagikan kunci di beberapa Wilayah AWS dan Akun AWS.
- Memusatkan administrasi kunci.
- Otomatiskan dan mandat rotasi kunci.

Sumber daya

Layanan AWS dokumentasi

- AWS KMS Detail Kriptografi
- Panduan Developer AWS KMS
  - AWS KMS konsep
  - Kunci tujuan khusus
  - Otentikasi dan kontrol akses untuk AWS KMS
  - Keamanan AWS KMS
  - Bagaimana Layanan AWS menggunakan AWS KMS
- AWS CloudHSM Panduan Pengguna

AWS pemasaran

- AWS KMS harga
- AWS KMS Integrasi dengan yang lain Layanan AWS

AWS Kerangka Well-Architected

- Melindungi data dalam perjalanan
- Melindungi data saat istirahat

Hashing dan tokenisasi

- Cara menggunakan tokenisasi untuk meningkatkan keamanan data dan mengurangi lingkup audit (AWS posting blog)
- Rekomendasi untuk aplikasi yang menggunakan algoritma hash yang disetujui (publikasi NIST)

Video

- Bagaimana enkripsi bekerja di AWS
- Mengamankan penyimpanan blok Anda AWS
- Mencapai tujuan keamanan dengan AWS CloudHSM
- Praktik terbaik untuk mengimplementasikan AWS Key Management Service
- Menyelam jauh ke dalam layanan AWS enkripsi

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	15 September 2022

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: 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 membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

Dengan 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 is commonly described as a pipeline. CI/CDdapat membantu

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur, gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan

adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet 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 file. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta

jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

ketekunan poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona 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 prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

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

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). 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 kredensi 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.