AWS Kerangka Migrasi Aman: Memobilisasi keamanan dan kepatuhan

AWS Panduan Preskriptif

AWS Panduan Preskriptif: AWS Kerangka Migrasi Aman: Memobilisasi keamanan dan kepatuhan

Table of Contents

AWS Secure Migrations Framework: Memobilisasi keamanan dan kepatuhan

Amazon Web Services (kontributor)

Maret 2024 (sejarah dokumen)

Migrasi cloud perusahaan dapat menjadi kompleks, menghasilkan tantangan dan risiko jika tidak direncanakan secara memadai dari sudut pandang bisnis dan teknis. Keamanan dan kepatuhan memerlukan perencanaan terperinci selama perjalanan migrasi dan modernisasi. Banyak organisasi menganggap keamanan dan kepatuhan sebagai hambatan untuk adopsi cloud. Chief Information Security Officers (CISO) dan tim keamanan sering mengutip tantangan umum berikut ketika membuat keputusan adopsi cloud: ketidakpastian kemampuan keamanan cloud, kepatuhan terhadap persyaratan kepatuhan, kesulitan pemetaan kebijakan keamanan, kurangnya keterampilan keamanan cloud, dan selera risiko yang rendah.

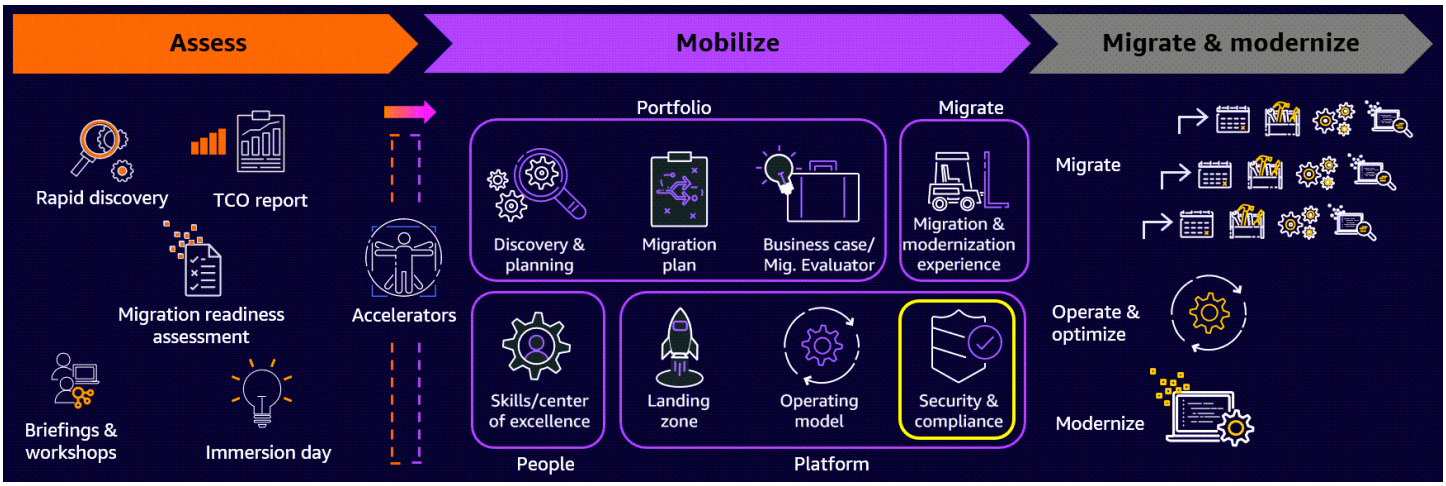
Untuk mengatasi tantangan tersebut, AWS Secure Migrations Framework menyoroti aktivitas utama yang harus Anda rencanakan dan kelola selama fase mobilisasi proyek migrasi. Panduan ini membantu Anda menyelaraskan proses migrasi, metodologi, dan pendekatan untuk menyertakan praktik terbaik ini.

Audiens yang dituju

Kerangka kerja ini ditujukan bagi mereka yang melakukan migrasi dan modernisasi ke AWS Cloud, dan juga ditujukan untuk pihak ketiga yang mendukung migrasi klien mereka.

Alur kerja keamanan dan kepatuhan serta struktur tim

AWS menawarkan AWS Migration Acceleration Program. Program ini memisahkan proses migrasi menjadi tiga fase: menilai, memobilisasi, dan bermigrasi dan memodernisasi. Sebagai bagian dari fase mobilisasi, Anda membuat rencana migrasi dan menyempurnakan kasus bisnis Anda. Anda mengatasi kesenjangan dalam kesiapan organisasi Anda yang terungkap dalam fase penilaian. Anda juga fokus untuk membangun landing zone, mendorong kesiapan operasional, dan mengembangkan keterampilan cloud. Bagian penting dari fase mobilisasi adalah menciptakan alur kerja keamanan dan kepatuhan yang merencanakan dan menangani persyaratan keamanan, risiko, dan kepatuhan untuk migrasi. Seperti yang ditunjukkan pada gambar berikut, alur kerja keamanan dan kepatuhan adalah bagian dari perspektif platform metodologi migrasi ini.



Selama fase mobilisasi, penting untuk menemukan dan merencanakan persyaratan keamanan dan kepatuhan Anda. Evaluasi kebutuhan Anda melalui lensa alat, orang, dan proses. Ada lima domain utama untuk alur kerja keamanan dan kepatuhan selama fase mobilisasi:

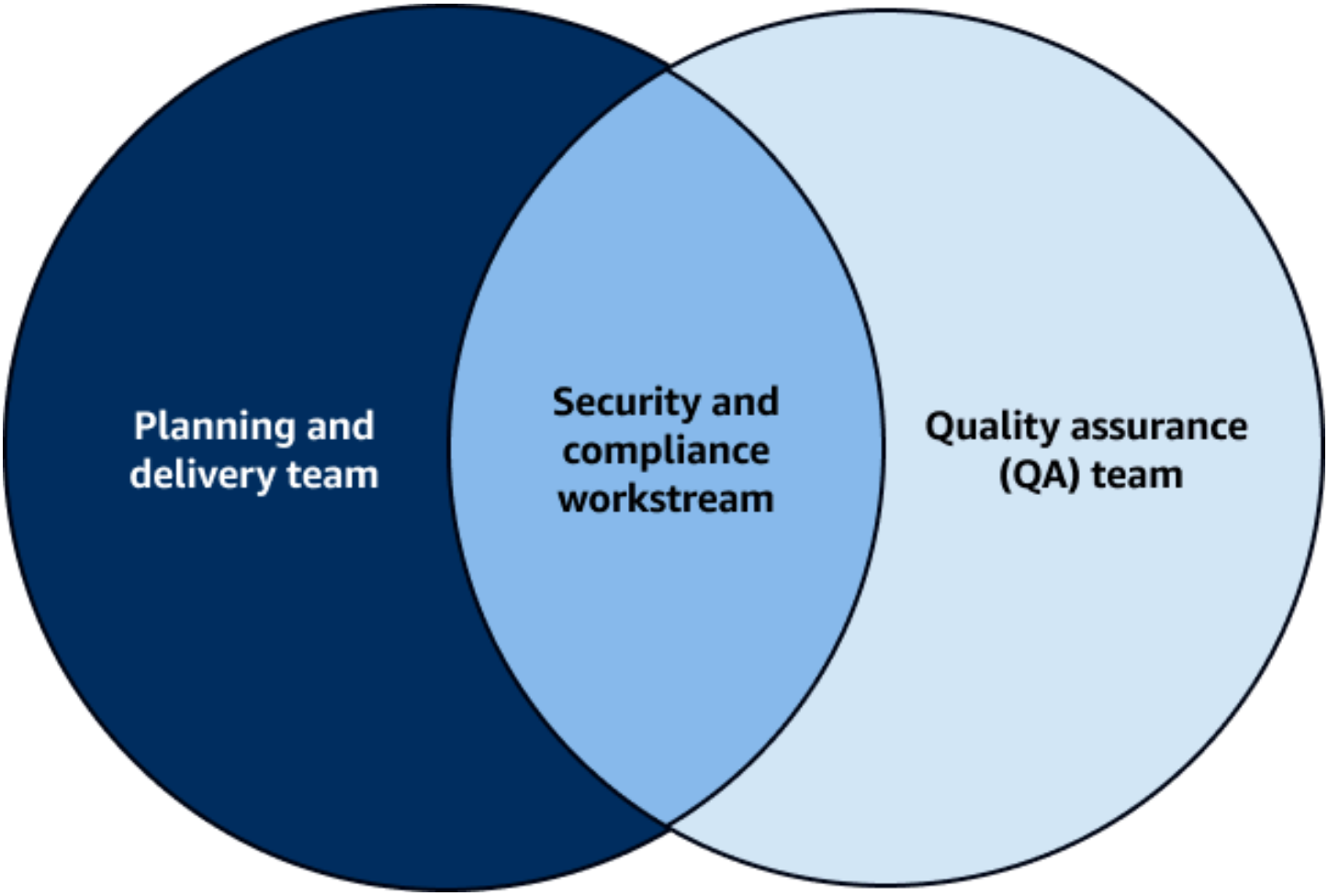
- Penemuan dan penyelarasan keamanan
- Pemetaan kerangka keamanan
- Implementasi keamanan, integrasi, validasi
- Dokumentasi keamanan
- Keamanan dan kepatuhan operasi cloud

Kegiatan-kegiatan ini dibahas secara rinci Domain dari alur kerja keamanan dan kepatuhan dalam bagian panduan ini. Pertama, penting untuk memahami komposisi dan struktur tim yang mendukung

alur kerja keamanan dan kepatuhan. Tim-tim ini melakukan atau memfasilitasi kegiatan dalam alur kerja keamanan dan kepatuhan.

Struktur tim keamanan dan kepatuhan

Langkah pertama untuk mobilisasi keamanan dan kepatuhan yang efektif adalah membentuk atau membentuk dua tim yang dapat mendukung, menyelesaikan, dan mengatur lima kegiatan utama dalam kerangka kerja. Gambar berikut menunjukkan struktur tim yang direkomendasikan dan persyaratan sumber daya. Alur kerja keamanan dan kepatuhan terutama terdiri dari individu-individu dari tim jaminan kualitas (QA) dan tim perencanaan dan pengiriman.



Tim perencanaan dan pengiriman bertanggung jawab atas hal-hal berikut dalam alur kerja keamanan dan kepatuhan:

- Memahami model tanggung jawab AWS bersama
- Memahami layanan AWS keamanan dan kepatuhan pada tingkat 300-400

- Memahami desain dan pengaturan arsitektur kepatuhan AWS
- Mengumpulkan persyaratan keamanan dan kepatuhan dengan menggunakan perkakas atau mekanisme yang ditentukan
- Memetakan persyaratan keamanan, kebijakan, konfigurasi, kontrol, dan pagar pembatas ke konfigurasi layanan AWS (Ini dikenal sebagai pemetaan kerangka kerja keamanan)
- Menyediakan setidaknya dua individu yang disertifikasi dalam AWS keamanan
- Membuat dokumentasi keamanan

Tim QA bertanggung jawab atas hal-hal berikut dalam alur kerja keamanan dan kepatuhan:

- Menyediakan total 3-5 individu, dan setidaknya dua dari mereka harus memiliki sertifikasi keamanan AWS
- Memahami desain dan pengaturan arsitektur kepatuhan AWS
- Memahami dan pengalaman menyelesaikan lima atau lebih ulasan AWS Well-Architected
- Memvalidasi bahwa AWS infrastruktur dan sumber daya mematuhi praktik terbaik AWS keamanan dan kepatuhan
- Membuat dan menyajikan laporan validasi keamanan

Persyaratan untuk setiap tim bervariasi tergantung pada ukuran migrasi dan keamanan serta kompleksitas kepatuhan. Penting juga untuk dicatat bahwa struktur dan persyaratan tim terbatas pada ruang lingkup berikut:

- Pengoperasian alur kerja keamanan dan kepatuhan dalam fase mobilisasi
- Validasi keamanan dan kepatuhan migrasi dan modernisasi

Setelah migrasi, kami menyarankan Anda untuk mendirikan Pusat Operasi Keamanan (SOC) khusus untuk terus memantau dan mengatur keamanan dan kepatuhan di. AWS Cloud

Domain dari alur kerja keamanan dan kepatuhan

Bagian ini menjelaskan, secara rinci, domain yang menjadi tanggung jawab alur kerja keamanan dan kepatuhan. Selama fase mobilisasi proyek migrasi Anda, domain ini membantu mempercepat perencanaan dan implementasi keamanan dan kepatuhan pada: AWS

- Penemuan dan penyelarasan keamanan
- Pemetaan kerangka kerja keamanan
- Implementasi keamanan, integrasi, dan validasi
- Dokumentasi keamanan
- Keamanan dan kepatuhan operasi cloud

Penting untuk mengatasi domain ini selama fase mobilisasi untuk mengamankan aktivitas migrasi selama fase migrasi berikutnya dan memodernisasi.

Penemuan dan penyelarasan keamanan

Saat memobilisasi proyek migrasi, domain pertama untuk alur kerja keamanan dan kepatuhan adalah penemuan dan penyelarasan keamanan. Domain ini dimaksudkan untuk membantu organisasi Anda mencapai tujuan berikut:

- Melatih alur kerja keamanan dan kepatuhan tentang layanan AWS keamanan, kemampuan, dan kepatuhan kepatuhan
- Temukan persyaratan keamanan dan kepatuhan Anda serta praktik terkini. Pertimbangkan persyaratan ini dari sudut pandang infrastruktur dan operasi, termasuk:
  - Tantangan keamanan dan driver untuk status akhir target
  - Keterampilan tim keamanan cloud
  - Kebijakan, konfigurasi, kontrol, dan pagar pembatas risiko keamanan dan kepatuhan
  - Nafsu dan baseline risiko keamanan
  - Perkakas keamanan yang ada dan prospektif

Lokakarya hari perendaman

Untuk menyelaraskan tujuan ini, gunakan hari pencelupan keamanan dan kepatuhan. Immersion days adalah lokakarya yang mencakup berbagai topik terkait keamanan, seperti:

- AWS model tanggung jawab bersama
- AWS layanan keamanan
- AWS Arsitektur Referensi Keamanan (AWS SRA)
- AWS kepatuhan
- Pilar Keamanan Kerangka AWS Well-Architected

Lokakarya hari imersi membantu menetapkan dasar pengetahuan untuk tim keamanan Anda. Ini melatih mereka tentang layanan AWS keamanan dan praktik terbaik keamanan dan kepatuhan. AWS Arsitek Solusi, Layanan AWS Profesional, dan AWS Mitra dapat membantu Anda melakukan lokakarya interaktif ini. Mereka menggunakan dek presentasi standar, laboratorium AWS, dan aktivitas papan tulis untuk membantu mempersiapkan tim Anda.

Lokakarya penemuan

Setelah lokakarya hari imersi, Anda melakukan beberapa lokakarya penemuan keamanan dan kepatuhan mendalam. Ini membantu tim Anda menemukan persyaratan keamanan, risiko, dan kepatuhan (SRC) saat ini dari infrastruktur, aplikasi, dan operasi. Anda menganalisis persyaratan ini melalui perspektif berikut: orang, proses, dan teknologi. Berikut ini adalah bidang penemuan untuk setiap perspektif.

Perspektif orang

- Struktur organisasi - Memahami struktur dan tanggung jawab arus kerja keamanan dan kepatuhan saat ini.
- Kemampuan dan keahlian — Memiliki pengetahuan dan keahlian praktis untuk dan untuk keamanan cloud Layanan AWS dan kemampuan kepatuhan. Ini termasuk penemuan, perencanaan, implementasi, dan operasi.
- Matriks yang bertanggung jawab, akuntabel, konsultasi, informasi (RACI) - Tentukan peran dan tanggung jawab untuk kegiatan keamanan dan kepatuhan saat ini dalam organisasi.
- Budaya — Memahami budaya keamanan dan kepatuhan saat ini. Prioritaskan keamanan dan kepatuhan sebagai bagian dari fase pembangunan, desain, implementasi, dan operasi.

Memperkenalkan Operasi Keamanan Pengembangan (DevSecOps) ke dalam budaya keamanan dan kepatuhan cloud.

Perspektif proses

- Praktik — Menentukan dan mendokumentasikan proses keamanan dan kepatuhan saat ini untuk membangun, merancang, mengimplementasikan, dan mengoperasikan. Proses meliputi:
  - Akses dan manajemen identitas
  - Kontrol dan respons deteksi insiden
  - Infrastruktur dan keamanan jaringan
  - Perlindungan data
  - Kepatuhan
  - Kelangsungan dan pemulihan bisnis
- Dokumentasi implementasi — Kebijakan keamanan dan kepatuhan dokumen, konfigurasi kontrol, dokumentasi perkakas, dan dokumentasi arsitektur. Dokumen-dokumen ini diperlukan untuk mencakup keamanan dan kepatuhan dari infrastruktur, jaringan, aplikasi, database, dan area penyebaran.
- Dokumentasi risiko — Buat dokumentasi risiko keamanan informasi yang menguraikan selera risiko dan ambang batas.
- Validasi — Membuat validasi keamanan internal dan eksternal dan persyaratan audit.
- Runbook — Mengembangkan runbook operasional yang mencakup implementasi standar dan proses tata kelola saat ini untuk keamanan dan kepatuhan.

Perspektif teknologi

- Layanan dan alat — Gunakan alat untuk memvalidasi postur keamanan dan kepatuhan Anda serta untuk menegakkan dan mengatur lanskap TI saat ini. Tetapkan perkakas untuk kategori berikut:
  - Akses dan manajemen identitas
  - Kontrol dan respons deteksi insiden
  - Infrastruktur dan keamanan jaringan
  - Perlindungan data
  - Kepatuhan
  - Kelangsungan dan pemulihan bisnis

Selama lokakarya penemuan AWS keamanan, Anda menggunakan templat pengumpulan data standar dan kuesioner untuk mengumpulkan data. Dalam skenario di mana Anda tidak dapat memberikan informasi karena kurangnya kejelasan data atau data usang, Anda dapat menggunakan alat penemuan migrasi untuk mengumpulkan informasi keamanan tingkat aplikasi dan infrastruktur. Untuk daftar alat penemuan yang dapat Anda gunakan, lihat Alat migrasi penemuan, perencanaan, dan rekomendasi di Panduan AWS Preskriptif. Daftar ini memberikan rincian tentang kemampuan dan penggunaan penemuan setiap alat. Ini juga membandingkan alat untuk membantu Anda memilih alat terbaik untuk memenuhi persyaratan dan kendala lanskap TI Anda.

Selama penilaian keamanan awal, kami sangat menyarankan Anda memulai dengan pemodelan ancaman. Ini membantu Anda mengidentifikasi kemungkinan ancaman dan tindakan yang ada yang ada. Mungkin juga ada persyaratan yang telah ditentukan dan didokumentasikan untuk keamanan, kepatuhan, dan risiko. Untuk informasi lebih lanjut, lihat lokakarya Pemodelan ancaman untuk pembangun (AWS pelatihan) dan lihat Cara mendekati pemodelan ancaman (posting AWS blog). Pendekatan ini membantu Anda mempertimbangkan kembali strategi keamanan dan kepatuhan Anda untuk penerapan, implementasi, dan tata kelola di. AWS Cloud

Pemetaan kerangka kerja keamanan

Setelah menyelesaikan domain penemuan dan penyelarasan keamanan, langkah selanjutnya adalah menyelesaikan domain pemetaan kerangka keamanan. Domain ini adalah proses lokakarya yang memetakan persyaratan keamanan dan kepatuhan yang ditemukan ke layanan AWS Cloud keamanan. Ini juga menyelaraskan arsitektur dan operasi Anda dengan praktik terbaik AWS keamanan dan kepatuhan. Lokakarya memetakan semua persyaratan dari perspektif orang, proses dan teknologi untuk mencakup hal-hal berikut:

- AWS Infrastruktur
  - Akun AWS, infrastruktur, dan perlindungan jaringan
  - Perlindungan data
  - Kepatuhan
  - Deteksi dan respons insiden
  - Manajemen identitas dan akses
  - Kelangsungan dan pemulihan bisnis
- Aplikasi pada AWS
  - Mengikuti praktik terbaik Layanan AWS untuk membantu melindungi aplikasi Anda
  - Kontrol akses untuk aplikasi, database, sistem operasi, dan data

- Perlindungan sistem operasi
- Aplikasi, basis data, dan perlindungan data
- Deteksi dan respons insiden
- Kepatuhan
- Kelangsungan dan pemulihan bisnis aplikasi

Saat Anda menyelesaikan domain pemetaan kerangka kerja keamanan, pertimbangkan selera risiko yang ditentukan, struktur tim, keahlian dan kemampuan tim, proses keamanan, kebijakan keamanan, kontrol keamanan, perkakas, operasi keamanan, serta persyaratan dan kendala keamanan lainnya. Secara keseluruhan, pemetaan kerangka kerja keamanan memberi organisasi pendekatan sistematis untuk mengelola risiko keamanan, menjaga kepatuhan, dan terus meningkatkan postur keamanan mereka, sesuai dengan standar industri dan praktik terbaik.

Proses pemetaan kerangka keamanan menggunakan Arsitektur Referensi AWS Keamanan (AWS SRA), Pilar Keamanan Kerangka Well-Architected, Lensa Migrasi Kerangka AWSAWS Well-Architected, dan whitepaper Pengantar Keamanan. AWS Dokumen-dokumen ini bertindak sebagai referensi panduan untuk membantu Anda mengikuti praktik AWS terbaik untuk keamanan dan kepatuhan cloud.

Dengan menggunakan templat pemetaan standar di bengkel, Anda memetakan persyaratan ke status akhir target. Anda menyoroti alat Layanan AWS, proses, kebijakan, kontrol, dan perubahan yang diperlukan untuk mencapai status akhir target.

Saat menjalankan lokakarya pemetaan kerangka kerja keamanan, Anda dapat menggunakan Layanan AWS Profesional, Arsitek Solusi AWS Keamanan, atau AWS Mitra. Sumber daya ini dapat membantu Anda mempercepat dan memfasilitasi lokakarya. Lokakarya pemetaan kerangka kerja keamanan dapat dimasukkan sebagai bagian dari pihak Experience-Based Acceleration (EBA), yang dipimpin oleh AWS Solution Architects, Customer Solution Manager, AWS atau Partners. AWS Partai EBA bertindak sebagai akselerator untuk membantu Anda membangun AWS Cloud fondasi yang kuat yang mengikuti praktik terbaik AWS migrasi dan modernisasi.

Implementasi keamanan, integrasi, dan validasi

Setelah memetakan persyaratan keamanan, risiko, dan kepatuhan Anda, domain berikutnya adalah implementasi keamanan, integrasi, dan validasi. Berdasarkan persyaratan yang teridentifikasi, pilih kontrol dan tindakan keamanan yang tepat untuk mengurangi risiko secara efektif. Ini mungkin

termasuk enkripsi, kontrol akses, sistem deteksi intrusi, atau firewall. Integrasikan solusi keamanan, seperti sistem deteksi dan pencegahan intrusi, perlindungan titik akhir, dan manajemen identitas, ke dalam infrastruktur TI yang ada untuk memberikan cakupan keamanan yang komprehensif. Melakukan penilaian keamanan rutin, termasuk pemindaian kerentanan, pengujian penetrasi, dan tinjauan kode, untuk memvalidasi efektivitas kontrol keamanan dan mengidentifikasi kelemahan atau kesenjangan. Dengan berfokus pada implementasi keamanan, integrasi, dan validasi, organisasi dapat memperkuat postur keamanan mereka, mengurangi kemungkinan pelanggaran keamanan, dan menunjukkan kepatuhan terhadap persyaratan peraturan dan standar industri.

Implementasi

Pertama, perbarui dokumentasi untuk ambang batas keamanan, risiko, dan kepatuhan Anda saat ini. Ini memungkinkan Anda untuk menerapkan persyaratan keamanan dan kepatuhan yang direncanakan, kontrol, kebijakan, dan perkakas di cloud. Langkah ini diperlukan hanya jika Anda memiliki daftar risiko dan selera yang sudah ditentukan, yang akan diidentifikasi selama lokakarya penemuan.

Selanjutnya, Anda menerapkan persyaratan keamanan dan kepatuhan yang direncanakan, kontrol, kebijakan, dan perkakas di cloud. Kami menyarankan Anda menerapkan ini dalam urutan berikut: infrastruktur, Layanan AWS, sistem operasi, dan kemudian aplikasi atau database. Gunakan informasi dalam tabel berikut untuk memastikan bahwa Anda telah menangani semua bidang keamanan dan kepatuhan yang diperlukan.

Luas	Persyaratan keamanan dan kepatuhan

Infrastruktur	• Akun AWS
	• Zona pendaratan
	  • Kontrol pencegahan
	  • Kontrol detektif
	• Segmentasi jaringan
	• Kontrol akses
	• Enkripsi

	• Pencatatan, pemantauan, dan peringatan

Layanan AWS	• Layanan AWS konfigurasi
	• Contoh
	  • Penyimpanan
	  • Jaringan
	• Kontrol akses
	• Enkripsi
	• Pembaruan dan tambalan
	• Pencatatan, pemantauan, dan peringatan

Sistem operasi	• Antivirus • Perlindungan malware dan worm • Konfigurasi • Perlindungan jaringan • Kontrol akses • Enkripsi • Pembaruan dan tambalan • Pencatatan, pemantauan, dan peringatan

Aplikasi atau database	• Konfigurasi • Kode dan skema • Kontrol akses • Enkripsi • Pembaruan dan tambalan • Pencatatan, pemantauan, dan peringatan

Integrasi

Implementasi keamanan seringkali membutuhkan integrasi dengan yang berikut:

- Jaringan — Jaringan di dalam dan di luar AWS Cloud
- Lanskap TI hibrida — Lingkungan TI selain AWS Cloud, seperti di tempat, awan publik, awan pribadi, dan kolokasi
- Perangkat lunak atau layanan eksternal — Perangkat lunak dan layanan yang dikelola oleh vendor perangkat lunak independen (ISVs) dan tidak dihosting di lingkungan Anda.
- Layanan model operasi AWS cloud — layanan model operasi cloud yang menyediakan DevSecOps kemampuan.

Selama fase penilaian proyek migrasi Anda, gunakan alat penemuan, dokumentasi yang ada, atau lokakarya wawancara aplikasi untuk mengidentifikasi dan mengonfirmasi titik integrasi keamanan ini. Saat merancang dan menerapkan beban kerja di AWS Cloud, buat integrasi ini sesuai dengan kebijakan dan proses keamanan dan kepatuhan yang Anda tentukan selama lokakarya pemetaan.

Validasi

Setelah implementasi dan integrasi, kegiatan selanjutnya adalah memvalidasi implementasi. Anda memastikan bahwa pengaturan selaras dengan praktik AWS terbaik untuk keamanan dan kepatuhan. Kami menyarankan Anda memvalidasi keamanan dari dua area cakupan:

- Penilaian kerentanan khusus beban kerja dan pengujian penetrasi - Validasi sistem operasi, aplikasi, database, atau keamanan jaringan beban kerja yang berjalan. Layanan AWS Untuk melakukan validasi ini, gunakan alat dan skrip pengujian yang ada. Penting untuk mematuhi kebijakan dukungan pelanggan pengujian AWS penetrasi saat melakukan penilaian ini.
- AWSvalidasi praktik terbaik keamanan - Validasi apakah AWS implementasi Anda sesuai AWS dengan Well Architected Framework dan tolok ukur terpilih lainnya, seperti Center for Internet Security (CIS). Untuk validasi ini, Anda dapat menggunakan alat dan layanan seperti, Prowler (GitHub) AWS Trusted Advisor, AWS Service Screener (), atau AWS Self-Service Security GitHub Assessment (). GitHub

Penting untuk mendokumentasikan dan mengkomunikasikan semua temuan keamanan dan kepatuhan kepada tim keamanan dan pemimpin. Standarisasi templat pelaporan dan gunakan untuk memfasilitasi komunikasi kepada pemangku kepentingan keamanan masing-masing. Dokumentasikan semua pengecualian yang dibuat selama menemukan remediasi dan pastikan bahwa masing-masing pemangku kepentingan keamanan menandatangani.

Dokumentasi keamanan

Saat memobilisasi keamanan dan kepatuhan selama migrasi, penting untuk menentukan dan mendokumentasikan bagaimana Anda menerapkan keamanan dan kepatuhan di cloud. Dokumentasi harus mencakup yang berikut:

- Dokumentasi implementasi keamanan dan kepatuhan — Buat satu atau beberapa dokumen yang merinci definisi, proses, kebijakan, kontrol, konfigurasi, dan alat keamanan dan kepatuhan Anda. Pastikan dokumen-dokumen ini membahas aspek-aspek ini dari AWS Cloud perspektif. Sertakan yang berikut ini dalam dokumentasi ini:
  - Akses dan manajemen identitas
  - Kontrol dan respons deteksi insiden
  - Infrastruktur dan keamanan jaringan
  - Perlindungan data
  - Kepatuhan
  - Kelangsungan dan pemulihan bisnis
- Runbook keamanan dan kepatuhan — Buat runbook operasional keamanan dan kepatuhan yang memandu tim operasi cloud. Mereka harus merinci cara menyelesaikan tugas, aktivitas, dan perubahan keamanan dan kepatuhan di cloud sebagai bagian dari persyaratan operasional. Ini

termasuk pemantauan keamanan dan kepatuhan, manajemen insiden, validasi, dan peningkatan berkelanjutan. Pastikan bahwa runbook Anda memenuhi persyaratan yang Anda identifikasi selama penemuan keamanan dan domain penyelarasan.

- Matriks RACI keamanan cloud - Buat matriks yang bertanggung jawab, akuntabel, konsultasi, informasi (RACI) yang mendefinisikan tanggung jawab keamanan dan kepatuhan serta pemangku kepentingan untuk bidang-bidang berikut:
  - Desain dan pengembangan
  - Penerapan dan implementasi
  - Operasi

Keamanan dan kepatuhan operasi cloud

Domain terakhir adalah keamanan dan kepatuhan operasi cloud. Ini adalah aktivitas berkelanjutan di mana Anda menggunakan runbook operasional keamanan dan kepatuhan yang ditentukan untuk mengatur operasi cloud. Anda juga membangun model operasi cloud keamanan untuk menentukan tanggung jawab atas keamanan dan kepatuhan di organisasi Anda.

Model operasi cloud keamanan dan kepatuhan

Di domain ini, Anda menentukan model operasi cloud untuk keamanan. Model operasi cloud Anda harus memenuhi persyaratan yang Anda identifikasi selama lokakarya penemuan dan kemudian didefinisikan sebagai runbook. Anda dapat merancang model operasi cloud keamanan dan kepatuhan dengan salah satu dari tiga cara:

- Terpusat — Model yang lebih tradisional, di mana SecOps bertanggung jawab untuk mengidentifikasi dan memulihkan peristiwa keamanan di seluruh bisnis. Ini dapat mencakup meninjau temuan postur keamanan umum untuk bisnis, seperti masalah tambalan dan konfigurasi keamanan.
- Desentralisasi — Tanggung jawab untuk menanggapi dan memulihkan peristiwa keamanan di seluruh bisnis telah didelegasikan kepada pemilik aplikasi dan unit bisnis individu, dan tidak ada fungsi operasi pusat. Biasanya, masih ada fungsi tata kelola keamanan menyeluruh yang mendefinisikan kebijakan dan prinsip.
- Hybrid — Campuran dari kedua pendekatan, di mana SecOps masih memiliki tingkat tanggung jawab dan kepemilikan untuk mengidentifikasi dan mengatur respons terhadap peristiwa keamanan dan tanggung jawab untuk remediasi dimiliki oleh pemilik aplikasi dan unit bisnis individu.

Penting untuk memilih model operasi yang tepat berdasarkan persyaratan keamanan dan kepatuhan Anda, kematangan organisasi, dan kendala. Persyaratan dan kendala keamanan dan kepatuhan diidentifikasi selama lokakarya penemuan. Kematangan organisasi, di sisi lain, mendefinisikan tingkat praktik keamanan operasional. Berikut ini adalah contoh rentang jatuh tempo:

- Rendah — Logging bersifat lokal, dan beberapa atau tindakan sporadis diambil.
- Intermediate — Log dari berbagai sumber berkorelasi, dan peringatan otomatis dibuat.
- Tinggi - Buku pedoman terperinci ada dan berisi detail tentang respons proses standar. Secara operasional dan teknis, sebagian besar respons peringatan otomatis.

Untuk lebih memahami model operasi cloud keamanan dan kepatuhan dan membantu dalam pemilihan desain yang sesuai, lihat Pertimbangan untuk operasi keamanan di cloud (posting AWS blog). Dalam skenario di mana tidak ada persyaratan yang telah ditentukan sebelumnya, sebaiknya Anda menyiapkan Security Operations Center (SOC) sebagai bagian dari model operasi cloud. Ini biasanya merupakan praktik model operasi terpusat. Dengan pendekatan ini, Anda dapat mengarahkan peristiwa dari berbagai sumber ke tim terpusat, yang kemudian dapat memicu tindakan dan tanggapan. Ini menstandarisasi tata kelola keamanan melalui operasi cloud. AWS dan AWS Mitra memiliki kemampuan yang dapat membantu Anda membangun SOC dan menentukan serta menerapkan Security Orchestration, Automation, and Response (SOAR). AWS dan AWS Mitra menggunakan konsultasi layanan profesional, templat yang ditentukan Layanan AWS, dan alat pihak ketiga dari AWS Mitra.

Operasi keamanan yang sedang berlangsung

Di domain ini, lakukan tugas-tugas berikut secara berkelanjutan dengan menggunakan runbook operasi keamanan dan kepatuhan yang Anda tentukan:

- Pemantauan keamanan dan kepatuhan — Lakukan pemantauan terpusat terhadap peristiwa dan ancaman keamanan dengan menggunakan perangkat Layanan AWS, alat, metrik, kriteria, dan frekuensi yang Anda tentukan. Tim operasi atau SOC mengelola pemantauan berkelanjutan ini, tergantung pada struktur organisasi Anda. Pemantauan keamanan melibatkan analisis dan korelasi sejumlah besar log dan data. Data log berasal dari titik akhir, jaringan, infrastruktur Layanan AWS, dan aplikasi dan disimpan dalam repositori terpusat, seperti Amazon Security Lake atau sistem manajemen informasi dan peristiwa keamanan (SIEM). Penting untuk mengonfigurasi peringatan sehingga Anda dapat merespons peristiwa secara manual atau otomatis secara tepat waktu.
- Manajemen insiden — Tentukan postur keamanan dasar Anda. Ketika penyimpangan dari garis dasar yang telah ditetapkan terjadi, baik melalui kesalahan konfigurasi atau faktor eksternal, catat

suatu insiden. Pastikan bahwa tim yang ditugaskan menanggapi insiden ini. Fondasi dari program respons insiden yang sukses di cloud adalah agar orang, proses, dan perkakas terintegrasi ke dalam setiap tahap program respons insiden (persiapan, operasi, dan aktivitas pasca-insiden). Pendidikan, pelatihan, dan pengalaman sangat penting untuk program respons insiden cloud yang sukses. Idealnya, ini diterapkan dengan baik sebelum harus menangani kemungkinan insiden keamanan. Untuk informasi selengkapnya tentang menyiapkan program respons insiden keamanan yang efektif, lihat Panduan Respons Insiden AWS Keamanan.

- Validasi keamanan — Validasi keamanan melibatkan menjalankan penilaian kerentanan, pengujian penetrasi, dan pengujian peristiwa simulasi keamanan kekacauan. Validasi keamanan harus terus dijalankan secara berkala, terutama untuk skenario berikut:
  - Pembaruan dan rilis perangkat lunak
  - Ancaman yang baru diidentifikasi, seperti malware, virus, atau worm
  - Persyaratan audit internal dan eksternal
  - Pelanggaran keamanan

  Penting untuk mendokumentasikan proses validasi keamanan dan menyoroti orang, proses, jadwal, perkakas, dan templat untuk pengumpulan dan pelaporan data. Ini menstandarisasi validasi keamanan. Terus patuhi kebijakan dukungan AWS pelanggan untuk pengujian penetrasi saat menjalankan validasi keamanan di cloud.
- Audit internal dan eksternal — Melakukan audit internal dan eksternal untuk memvalidasi bahwa konfigurasi keamanan dan kepatuhan memenuhi persyaratan peraturan atau kebijakan internal. Lakukan audit secara berkala berdasarkan jadwal yang telah ditentukan. Audit internal biasanya dilakukan oleh tim keamanan dan risiko internal. Audit eksternal dilakukan oleh lembaga terkait atau pejabat standar. Anda dapat menggunakan Layanan AWS, seperti AWS Audit Managerdan AWS Artifact, untuk memfasilitasi proses audit. Layanan ini dapat memberikan bukti yang relevan runtuk laporan audit TI keamanan. Mereka juga dapat menyederhanakan manajemen risiko dan kepatuhan dengan standar peraturan dan industri dengan mengotomatiskan pengumpulan bukti. Ini membantu Anda menilai apakah kebijakan, prosedur, dan aktivitas yang dikenal sebagai kontrol beroperasi secara efektif. Penting juga untuk menyelaraskan persyaratan audit dengan mitra layanan terkelola Anda untuk memastikan kepatuhan.

Tinjauan arsitektur keamanan — Selesaikan tinjauan berkala dan pembaruan AWS arsitektur Anda dari sudut pandang keamanan dan kepatuhan. Tinjau arsitektur setiap triwulanan atau ketika ada perubahan arsitektur. AWS terus merilis pembaruan dan peningkatan fitur dan layanan keamanan dan kepatuhan. Gunakan Arsitektur Referensi AWS Keamanan dan Alat Arsitek AWS Baik untuk

memfasilitasi tinjauan arsitektur ini. Penting untuk mendokumentasikan implementasi keamanan dan kepatuhan Anda dan perubahan yang disarankan setelah proses peninjauan.

AWS layanan keamanan untuk operasi

Anda berbagi tanggung AWS jawab dengan keamanan dan kepatuhan dalam AWS Cloud. Hubungan ini dijelaskan secara rinci dalam model tanggung jawab AWS bersama. Saat AWS mengelola keamanan cloud, Anda bertanggung jawab atas keamanan di cloud. Anda bertanggung jawab untuk melindungi konten, infrastruktur, aplikasi, sistem, dan jaringan Anda sendiri, tidak berbeda dengan yang Anda lakukan untuk pusat data lokal. Tanggung jawab Anda untuk keamanan dan kepatuhan AWS Cloud bervariasi tergantung pada layanan yang Anda gunakan, bagaimana Anda mengintegrasikan layanan tersebut ke dalam lingkungan TI Anda, dan hukum dan peraturan yang berlaku.

Keuntungannya AWS Cloud adalah memungkinkan Anda untuk menskalakan dan berinovasi dengan menggunakan praktik AWS terbaik dan layanan keamanan dan kepatuhan. Ini membantu Anda menjaga lingkungan yang aman sambil membayar hanya untuk layanan yang Anda gunakan. Anda juga memiliki akses ke layanan AWS keamanan dan kepatuhan yang sama yang digunakan organisasi perusahaan yang sangat aman untuk mengamankan lingkungan cloud mereka.

Membangun arsitektur cloud di atas fondasi yang sehat dan aman adalah langkah pertama dan terbaik untuk memastikan keamanan dan kepatuhan cloud. Namun, AWS sumber daya Anda hanya seaman Anda mengonfigurasinya. Postur keamanan dan kepatuhan yang efektif dicapai hanya melalui kepatuhan yang terus-menerus dan ketat pada tingkat operasional. Operasi keamanan dan kepatuhan dapat dikelompokkan secara luas menjadi lima kategori:

- Perlindungan data
- Akses dan manajemen identitas
- Perlindungan jaringan dan aplikasi
- Deteksi ancaman dan pemantauan berkelanjutan
- Kepatuhan dan privasi data

AWS Layanan keamanan dan kepatuhan dipetakan ke kategori ini untuk membantu Anda memenuhi serangkaian persyaratan yang komprehensif. Dikelompokkan ke dalam kategori ini, berikut ini adalah layanan inti AWS keamanan dan kepatuhan serta kemampuannya. Layanan ini dapat membantu Anda membangun dan menegakkan tata kelola keamanan cloud.

Perlindungan data

AWS menyediakan layanan berikut yang dapat membantu Anda melindungi data, akun, dan beban kerja Anda dari akses yang tidak sah:

- AWS Certificate Manager— Menyediakan, mengelola, dan menyebarkan SSL/TLS sertifikat untuk digunakan dengan Layanan AWS.
- AWS CloudHSM— Kelola modul keamanan perangkat keras Anda (HSMs) di AWS Cloud.
- AWS Key Management Service (AWS KMS) — Buat dan kendalikan kunci yang digunakan untuk mengenkripsi data Anda.
- Amazon Macie — Temukan, klasifikasikan, dan bantu lindungi data sensitif dengan fitur keamanan yang didukung pembelajaran mesin.
- AWS Secrets Manager— Putar, kelola, dan ambil kredenal basis data, kunci API, dan rahasia lainnya melalui siklus hidupnya.

Manajemen identitas dan akses

Layanan AWS identitas berikut membantu Anda mengelola identitas, sumber daya, dan izin secara aman dalam skala besar:

- Amazon Cognito — Tambahkan pendaftaran pengguna, masuk, dan kontrol akses ke web dan aplikasi seluler Anda.
- AWS Directory Service— Gunakan Microsoft Active Directory yang dikelola di AWS Cloud.
- AWS IAM Identity Center— Kelola akses masuk tunggal (SSO) secara terpusat ke beberapa Akun AWS aplikasi bisnis.
- AWS Identity and Access Management (IAM) - Kontrol akses Layanan AWS dan sumber daya dengan aman.
- AWS Organizations— Menerapkan manajemen berbasis kebijakan untuk beberapa. Akun AWS
- AWS Resource Access Manager (AWS RAM) — Bagikan AWS sumber daya di seluruh akun Anda.

Perlindungan jaringan dan aplikasi

Kategori layanan ini membantu Anda menegakkan kebijakan keamanan berbutir halus di titik kontrol jaringan di seluruh organisasi Anda. Berikut ini Layanan AWS membantu Anda memeriksa dan memfilter lalu lintas untuk membantu mencegah akses sumber daya yang tidak sah di batas tingkat host, tingkat jaringan, dan tingkat aplikasi:

- AWS Firewall Manager— Konfigurasikan dan kelola AWS WAF aturan di seluruh Akun AWS dan aplikasi dari lokasi pusat.
- AWS Network Firewall— Menyebarkan perlindungan jaringan penting untuk awan pribadi virtual Anda ()VPCs.
- Amazon Route 53 Resolver DNS Firewall — Membantu melindungi permintaan DNS keluar Anda dari Anda. VPCs
- AWS Shield— Lindungi aplikasi web Anda dengan perlindungan S terkelola DDo.
- AWS Systems Manager— Konfigurasikan dan kelola Amazon Elastic Compute Cloud (Amazon EC2) dan sistem lokal untuk menerapkan patch OS, membuat image sistem yang aman, dan mengonfigurasi sistem operasi.
- Amazon Virtual Private Cloud (Amazon VPC) - Menyediakan bagian yang terisolasi secara logis AWS tempat Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan.
- AWS WAF— Membantu melindungi aplikasi web Anda dari eksploitasi web umum.

Deteksi ancaman dan pemantauan berkelanjutan

Layanan AWS pemantauan dan deteksi berikut membantu Anda mengidentifikasi potensi insiden keamanan di AWS lingkungan Anda:

- AWS CloudTrail— Lacak aktivitas pengguna dan penggunaan API untuk memungkinkan tata kelola dan audit operasional dan risiko Anda. Akun AWS
- AWS Config— Rekam dan evaluasi konfigurasi AWS sumber daya Anda untuk membantu Anda mengaudit kepatuhan, melacak perubahan sumber daya, dan menganalisis keamanan sumber daya.
- AWS Config aturan — Buat aturan yang secara otomatis bertindak sebagai respons terhadap perubahan di lingkungan Anda, seperti mengisolasi sumber daya, memperkaya peristiwa dengan data tambahan, atau memulihkan konfigurasi ke status yang diketahui baik.
- Amazon Detective — Menganalisis dan memvisualisasikan data keamanan untuk dengan cepat sampai ke akar penyebab masalah keamanan potensial.
- Amazon GuardDuty — Bantu lindungi beban kerja Anda Akun AWS dengan deteksi ancaman cerdas dan pemantauan berkelanjutan.
- Amazon Inspector — Mengotomatiskan penilaian keamanan untuk membantu meningkatkan keamanan dan kepatuhan aplikasi yang digunakan. AWS

- AWS LambdaJalankan kode tanpa menyediakan atau mengelola server sehingga Anda dapat menskalakan respons terprogram dan otomatis terhadap insiden.
- AWS Security Hub CSPM— Lihat dan kelola peringatan keamanan dan otomatiskan pemeriksaan kepatuhan dari lokasi pusat.

Kepatuhan dan privasi data

Berikut ini Layanan AWS memberikan pandangan komprehensif tentang status kepatuhan Anda. Mereka terus memantau lingkungan Anda dengan menggunakan pemeriksaan kepatuhan otomatis yang didasarkan pada praktik AWS terbaik dan standar industri:

- AWS Artifact— Dapatkan akses sesuai permintaan ke laporan AWS keamanan dan kepatuhan dan pilih perjanjian online.
- AWS Audit Manager— Terus audit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan menjaga kepatuhan terhadap peraturan dan standar industri.

Kesimpulan

Keamanan dan kepatuhan cloud sangat penting untuk keberhasilan dan pertumbuhan perjalanan adopsi cloud organisasi. Persyaratan keamanan dan kepatuhan harus dikumpulkan dan dianalisis. Dari perspektif kesiapan cloud, sangat penting untuk mengidentifikasi kesenjangan di awal perjalanan migrasi Anda. Fase mobilisasi Program Percepatan AWS Migrasi merekomendasikan agar Anda membuat alur kerja keamanan dan kepatuhan untuk tujuan ini. Ketika alur kerja ini bekerja secara efektif, ini menciptakan fondasi cloud yang kuat dan aman untuk perjalanan migrasi dan modernisasi cloud yang sukses. Kami menyarankan Anda untuk merujuk dan menggabungkan pendekatan dan proses yang dirinci dalam kerangka kerja ini ke dalam praktik migrasi dan modernisasi Anda untuk merencanakan dan mengimplementasikan fondasi cloud yang aman secara memadai.

Sumber daya

AWS dokumentasi

- AWS Panduan Respons Insiden Keamanan (AWS whitepaper)
- AWS Arsitektur Referensi Keamanan (AWS SRA) (PanduanAWS Preskriptif)
- Pengantar AWS Keamanan (AWS whitepaper)
- Lensa Migrasi (Kerangka AWS Well-Architected)
- Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar (Panduan AWS Preskriptif)
- Pilar Keamanan (KerangkaAWS Well-Architected)

AWS Sumber daya lainnya

- AWS Kebijakan Customer Support untuk Penetration Testing
- AWS Manajer Insiden - Otomatiskan respons insiden terhadap peristiwa keamanan (AWS lokakarya)
- AWS Model Tanggung Jawab Bersama
- Pertimbangan untuk operasi keamanan di cloud (posting AWS blog)

Kontributor

Mengotorisasi

- Ahilan Thiagarajah, Arsitek Solusi Mitra Utama, AWS
- Rishi Singla, Arsitek Solusi Mitra Senior, AWS
- Venkatesh Krishnan, Arsitek Solusi Mitra Senior, AWS

Meninjau

- Magesh Dhanasekaran, Arsitek Keamanan, AWS
- Wana Tun, Arsitek Solusi Senior, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Maret 11, 2024

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau menyebabkan kerugian bagi individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

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 penyimpanan atau kelas yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-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 CSPM, 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 AWS dengan Layanan Migrasi Aplikasi.

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

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

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan 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.

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

Proses penggantian pengidentifikasi 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.

Region

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 Konsol Manajemen AWS atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

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

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations 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 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 terkini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

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

fungsi jendela

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat 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.