Panduan pencatatan dan pemantauan untuk pemilik aplikasi

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Panduan pencatatan dan pemantauan untuk pemilik aplikasi

Table of Contents

Panduan pencatatan dan pemantauan untuk pemilik aplikasi

John Buckley, Layanan Web Amazon (AWS)

Januari 2023(sejarah dokumen)

SEBUAHbeban kerjaadalah kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend. Beban kerja mungkin terdiri dari subset sumber daya dalam satuAkun AWS, atau mungkin menjangkau beberapaAkun AWS. Di awan, sebuahpenerapanadalah jenis beban kerja. Ini mungkin diterapkan secara eksklusif di lingkungan cloud, atau mungkin juga didukung oleh perangkat keras lokal lokal. Banyak publikasi berfokus pada pencatatan dan pemantauan infrastruktur cloud dan ditujukan untuk tim keamanan. Panduan ini ditujukan untuk pemilik aplikasi dan berfokus pada pendekatan yang efektif dan efisien untuk pencatatan dan pemantauan aplikasi diAWS Cloud.

Panduan ini membantu Anda mengatur pencatatan dan pemantauan pada tingkat yang sesuai sehingga Anda dapat mengidentifikasi dan merespons anomali dengan cepat. Ini juga membantu Anda memastikan bahwa log aplikasi Anda mendukung analisis terperinci dan penyelesaian masalah apa pun.

Meskipun panduan ini ditulis denganAWS Cloudpenerapan dalam pikiran, Anda dapat menerapkan prinsip-prinsip ini ke aplikasi yang berjalan di tempat atau di infrastruktur penyedia cloud lainnya.

Hasil bisnis yang ditargetkan

Setelah membaca panduan ini, Anda harus dapat memahami:

- Jenis peristiwa yang biasa dicatat untuk aplikasi
- Atribut event (seperti siapa, apa, dan kapan) yang harus Anda pertimbangkan untuk masuk
- Jenis data yang harus Anda pertimbangkan untuk dikecualikan dari log, seperti data yang mungkin membahayakan postur keamanan Anda atau informasi yang dapat diidentifikasi secara pribadi
- Cara mengatur pencatatan dan pemantauan pada tingkat yang sesuai untuk aplikasi Anda
- Siapa yang seharusnya dapat mengelola dan mengakses log aplikasi Anda
- TheAWS layanandan fitur yang dapat Anda konfigurasikan untuk memantau dan mencatat aplikasi Anda diAWS Cloud
- Cara menggunakan data log dari aplikasi Anda danAWS layanandan fitur untuk triase masalah dan mendiagnosis masalah

Tentang pencatatan dan pemantauan untuk aplikasi

Pencatatan, pemantauan, peringatan, dan pelaporan adalah proses keamanan berbeda yang bekerja sama untuk memberikan visibilitas ke dalam kesehatan dan kinerja aplikasi Anda. Sangat penting bahwa Anda membuat dan memelihara catatan rinci tindakan dan peristiwa untuk aplikasi Anda sehingga Anda dapat memantau, memperingatkan, dan melaporkan berdasarkan aktivitas yang direkam.

Pencatatan aplikasiadalah proses mengumpulkan peristiwa yang dihasilkan oleh aplikasi Anda dan merekamnya dalam satu atau lebih file log. Riwayat peristiwa ini dapat membantu Anda melakukan analisis keamanan dan kinerja, melacak perubahan sumber daya, dan memecahkan masalah aplikasi.

Pemantauan aplikasiadalah proses menilai kinerja dan kesehatan aplikasi Anda secara keseluruhan. Anda harus dapat memantau frontend dan backend aplikasi secara konstan. Karena aplikasi yang di-host di cloud sangat terdistribusi, alat pencatatan dan pemantauan dapat membantu Anda memecahkan masalah kinerja dengan cepat atau mengidentifikasi dan memulihkan ancaman keamanan secara real time. Data log adalah input penting untuk pemantauan.

Observabilitasmirip dengan pemantauan, tetapi memperkenalkan cara untuk mengukur perilaku aplikasi menggunakan parameter yang berbeda, dan memungkinkan korelasi yang kompleks. Contohnya adalah mengukur tingkat keberhasilan HTTP pada hari tertentu, untuk sekumpulan pengguna di wilayah geografis tertentu. Untuk informasi lebih lanjut, lihatPemantauan dan Observabilitas(AWSpemasaran).

Pada akhirnya, tujuan pemilik aplikasi adalah untuk menjaga aplikasi yang aman, sehat, dan pengalaman pengguna yang positif dengan aplikasi tersebut. Dengan menerapkan pencatatan dan pemantauan, pengembang dan tim operasi Anda dapat merencanakan dan memecahkan masalah aplikasi dengan lebih cepat.

Tingkat pencatatan dan pemantauan yang diperlukan bervariasi untuk setiap aplikasi. Faktor-faktor yang dapat mempengaruhi tingkat pemantauan dan pencatatan termasuk kebijakan dan prosedur organisasi, tingkat risiko keamanan yang ditimbulkan aplikasi, kekritisan aplikasi untuk operasi bisnis, dan sensitivitas data yang dikelola oleh aplikasi. Secara umum, aplikasi yang bersifat publik atau pelanggan memerlukan tingkat pemantauan dan pencatatan yang lebih tinggi daripada aplikasi yang digunakan secara internal dalam organisasi. Panduan ini mencakup informasi umum dan rekomendasi, dan Anda harus menyesuaikan pendekatan Anda berdasarkan persyaratan aplikasi Anda.

> **Note**
>
> Standar atau prosedur dalam organisasi Anda mungkin mengamanatkan atribut pencatatan dan pemantauan tertentu. Contohnya adalah meneruskan izin pengguna ke dalam sistem peninjauan hak perusahaan. Pastikan bahwa rencana pencatatan dan pemantauan Anda memenuhi persyaratan organisasi Anda.

Logging untuk aplikasi diAWS Cloud

Untuk aplikasi logging diAWS Cloud, tinjau jenis acara umum, atribut acara, dan praktik terbaik.

Bagian ini mencakup topik-topik berikut:

Tipe peristiwa

Salah satu pertimbangan terpenting saat membuat strategi pencatatan aplikasi adalah memutuskan peristiwa dan tindakan mana yang akan dicatat. Meskipun persyaratan organisasi dan aplikasi Anda dapat memengaruhi keputusan ini, kami menyarankan Anda untuk selalu mencatat hal-hal berikut jika berlaku untuk aplikasi Anda:

- Kegagalan validasi masukanContohnya termasuk pelanggaran protokol, pengkodean yang tidak dapat diterima, dan nama dan nilai parameter yang tidak valid.
- Kegagalan validasi keluaran— Contohnya termasuk ketidakcocokan kumpulan catatan database dan pengkodean data yang tidak valid.
- Keberhasilan dan kegagalan otentikasi identitas— Aktivitas otentikasi log, tetapi jangan mencatat nama pengguna dan kata sandi. Karena pengguna dapat secara tidak sengaja mengetikkan kata sandi mereka ke dalam bidang nama pengguna, sebaiknya Anda tidak mencatat nama pengguna. Ini mungkin secara tidak sengaja mengekspos kredensil dan mengakibatkan akses resmi. Menerapkan kontrol keamanan untuk setiap log yang berisi data otentikasi.
- Kegagalan otorisasi (kontrol akses)— Untuk sistem otorisasi terkait, log upaya akses gagal. Anda dapat memantau data log ini untuk pola yang mungkin menunjukkan serangan atau masalah dengan sistem otorisasi dalam aplikasi.
- Kegagalan manajemen sesi— Contohnya termasuk memodifikasi cookie sesi atau token. Aplikasi sering menggunakan cookie atau token untuk mengelola status pengguna. Pengguna jahat dapat mencoba mengubah nilai cookie untuk mendapatkan akses yang tidak sah. Mencatat token sesi yang dirusak menyediakan cara untuk mendeteksi perilaku ini.
- Kesalahan aplikasi dan peristiwa sistemContohnya termasuk kesalahan sintaks dan runtime, masalah konektivitas, masalah kinerja, pesan kesalahan dari layanan pihak ketiga, kesalahan sistem file, deteksi virus untuk unggahan file, dan perubahan konfigurasi.

- Status aplikasiMemulai atau menghentikan aplikasi dan sumber daya terkaitnya.
- Status logging— Memulai, menghentikan, atau menjeda logging.
- Penggunaan fungsionalitas berisiko tinggi— Contohnya termasuk perubahan koneksi jaringan, menambah atau menghapus pengguna, mengubah hak istimewa, menugaskan pengguna ke token, menambah atau menghapus token, menggunakan hak administratif sistem, akses oleh administrator aplikasi, semua tindakan yang dilakukan oleh pengguna dengan hak administratif, mengakses data pemegang kartu pembayaran, menggunakan kunci enkripsi data, mengubah kunci enkripsi, membuat dan menghapus objek tingkat sistem, mengirimkan konten yang dibuat pengguna (terutama unggahan file), dan mengimpor dan mengekspor data (termasuk laporan).
- Legal dan opt-in lainnyaContohnya termasuk izin untuk kemampuan ponsel, syarat penggunaan, syarat dan ketentuan, persetujuan penggunaan data pribadi, dan izin untuk menerima komunikasi pemasaran.

Selain atribut yang disarankan, untuk aplikasi Anda, pertimbangkan atribut tambahan apa yang mungkin menyediakan data berguna untuk pemantauan, peringatan, dan pelaporan. Contohnya termasuk:

- Kegagalan pengurutan
- Atribut yang membantu Anda menilai perilaku pengguna yang melanggar kebijakan penggunaan yang dapat diterima organisasi Anda
- Perubahan data
- Atribut yang diperlukan untuk mematuhi standar atau peraturan, seperti mencegah kejahatan keuangan, membatasi perdagangan ekuitas, atau mengumpulkan kesehatan atau informasi pribadi lainnya.
- Atribut yang membantu Anda mengidentifikasi perilaku mencurigakan atau tidak terduga, seperti upaya untuk melakukan tindakan yang tidak sah
- Perubahan konfigurasi
- File kode aplikasi atau perubahan memori

Atribut acara

Setiap entri log perlu menyertakan informasi yang cukup rinci untuk pemantauan dan analisis. Anda dapat mencatat data konten lengkap, tetapi lebih efisien untuk mencatat properti ekstrak atau ringkasan. Log aplikasi harus mencatatketika,di mana,yang,apa, danyang manadari setiap event.

Properti untuk ini akan berbeda tergantung pada arsitektur, kelas aplikasi, dan sistem host atau perangkat.

Saat mencatat stempel tanggal dan waktu, gunakan Waktu Universal Terkoordinasi (UTC) dan format tanggal dan waktu yang diakui secara internasionalISO 8601(Situs web ISO).

> **Note**
>
> Pertimbangkan untuk menggunakan layanan sinkronisasi waktu jaringan untuk membantu memastikan stempel waktu yang akurat. Amazon menyediakan Layanan Sinkronisasi Waktu Amazon, yang digunakan oleh banyak orangAWS layanan, termasuk Amazon Elastic Compute Cloud (Amazon EC2). Amazon Time Sync Service menggunakan armada jam referensi atom dan satelit yang terhubung di masing-masingWilayah AWSuntuk memberikan pembacaan waktu yang akurat saat ini dari standar global UTC melalui Network Time Protocol (NTP). Untuk informasi lebih lanjut, lihatMenjaga Waktu dengan Layanan Sinkronisasi Waktu Amazon(AWSposting blog).

Atribut peristiwa berikut biasanya disertakan dalam log.

Kategori atribut	Atribut acara	Deskripsi
Saat	Tanggal dan waktu pencatatan	Catat tanggal dan waktu acara ditambahkan ke log.
	Tanggal dan waktu acara	Catat tanggal dan waktu peristiwa itu terjadi. Ini mungkin berbeda dari catatan logging, seperti saat pencatata n tertunda karena aplikasi klien di-host di perangkat jarak jauh yang secara berkala atau sebentar-sebentar online.
	Pengidentifikasi acara	Log nama pengguna, nomor akun, atau atribut unik lainnya yang memastikan acara selalu dapat diidentifikasi.

Di mana	Pengidentifikasi aplikasi	Log nama dan versi aplikasi.
	Alamat aplikasi	Log cluster atau nama host, alamat server IPv4 atau IPv6, nomor port, identitas workstation, dan pengenal perangkat lokal.
	Layanan	Log nama layanan dan protokol.
	Geolokasi	Log lokasi geografis pengguna.
	Jendela, formulir, atau halaman	Log URL titik masuk, metode HTTP untuk aplikasi web, atau nama kotak dialog tempat tindakan diambil.
	Lokasi kode	Catat skrip atau nama modul.
Siapa (pengguna manusia atau mesin)	Alamat sumber	Catat pengenal perangkat pengguna, alamat IP, ID menara frekuensi seluler atau radio (RF), atau nomor telepon seluler.
	Identitas pengguna	Jika pengguna diautentikasi atau diketahui, catat nilai kunci primer tabel basis data pengguna, nama pengguna, atau nomor lisensi.

	Klasifikasi tipe pengguna	Log jenis pengguna, seperti publik, otentikasi, CMS, mesin pencari, penguji penetrasi resmi, atau monitor uptime. Untuk informasi selengkap nya tentang monitor uptime, lihatPeringatan dan pengecual iandalam panduan ini.
	Minta header HTTP atau agen pengguna HTTP	(Hanya aplikasi web) Log informasi header permintaan HTTP, termasuk string agen pengguna HTTP, karena nilai-nilai ini memengaruhi informasi yang dikirim klien ke server.
Apa	Jenis acara	Catat apakah acara tersebut bersifat informasi, peringatan, atau kesalahan.
	Tingkat keparahan peristiwa	Klasifikasi tingkat keparahan peristiwa, seperti tinggi, sedang, dan rendah.
	Bendera acara keamanan	Jika log berisi data yang tidak terkait dengan peristiwa keamanan, buat tanda untuk peristiwa terkait keamanan untuk membantu Anda mengidentifikasinya.
	Deskripsi acara	(Opsional) Sertakan deskripsi singkat tentang acara tersebut.

	Tindakan atau niat	Catat tujuan asli yang dimaksudkan dari permintaan, seperti masuk, menyegarkan ID sesi, keluar, atau memperbarui profil.
	Respons pengguna atau aplikasi	Log respons pengguna atau aplikasi ke acara tersebut, seperti kode status, pesan teks khusus, penghentian sesi, atau peringatan administrator.
	Status hasil	Catat apakah tindakan itu berhasil, seperti sukses, gagal, atau menunda.
	Alasan hasil	Catat alasan status terjadi. Misalnya, permintaan masuk mungkin gagal karena pengguna tidak diautentikasi dalam database.
	Detail diperpanjang	Log informasi tambahan apa pun yang terkait dengan peristiwa, seperti jejak tumpukan, pesan kesalahan sistem, informasi debug, dan badan permintaan HTTP.
	Kode status respons HTTP	(Hanya aplikasi web) Log kode status respons HTTP yang dikembalikan ke pengguna, seperti `200` atau `301`. Untuk informasi lain, lihat Tingkat pencatatan dalam panduan ini.
Yang mana	Sumber daya terpengaruh	Catat sumber daya mana yang ditindaklanjuti.

	Objek	Log komponen yang terpengaruh atau objek lain, seperti akun pengguna, sumber daya data, file, URL, atau ID sesi.
	Nama sumber daya	Catat nama sumber daya yang terpengaruh.
	Tanda sumber daya	Log tag yang ditetapkan ke sumber daya yang terpengaruh. Untuk informasi selengkapnya tentang tag, lihatMenandaiAWSsumber daya(AWSReferensi Umum).
Lainnya	Keyakinan analitis	Catat kepercayaan layanan logging dalam deteksi peristiwa, seperti menetapkan peringkat rendah, sedang, atau tinggi atau nilai numerik.
	Klasifikasi internal	Catat klasifikasi internal apa pun untuk standar atau kepatuhan kepatuhan.
	Klasifikasi eksternal	Catat klasifikasi eksternal apa pun untuk standar atau kepatuhan kepatuhan, seperti NIST Security Content Automation Protocol (SCAP).

Praktik terbaik pencatatan

Tingkat pencatatan

Berhati-hatilah untuk tidak mencatat jumlah data yang berlebihan. Log harus menangkap data yang berguna dan dapat ditindaklanjuti. Penebangan yang berlebihan dapat berdampak negatif pada

kinerja, dan juga dapat meningkatkan biaya penyimpanan dan pemrosesan logging. Pencatatan yang berlebihan juga dapat mengakibatkan masalah dan peristiwa keamanan tidak terdeteksi.

Mencatat kode status respons HTTP dapat menghasilkan sejumlah besar data log, terutama kode status 200 tingkat (sukses) dan 300 tingkat (pengalihan). Kami menyarankan Anda mempertimbangkan untuk mencatat hanya kode status 400 tingkat (kesalahan sisi klien) dan 500 tingkat (kesalahan sisi server).

Kerangka kerja logging aplikasi menyediakan tingkat logging yang berbeda, sepertiinfo,awakutu, ataukesalahan. Untuk lingkungan pengembangan, Anda mungkin ingin menggunakan pencatatan verbose, seperti menyertakaninfodanawakutuuntuk membantu pengembang Anda. Namun, kami menyarankan Anda menonaktifkaninfodanawakututingkat untuk lingkungan produksi karena ini dapat menghasilkan data logging yang berlebihan.

Peringatan dan pengecualian

- Pastikan bahwa data yang Anda catat diizinkan secara hukum, terutama di yurisdiksi tempat organisasi Anda beroperasi.
- Jangan mengecualikan peristiwa apa pun dari pengguna yang dikenal (seperti sistem internal lainnya), pihak ketiga tepercaya, robot mesin pencari, uptime atau monitor proses, dan sistem pemantauan jarak jauh lainnya. Namun, Anda dapat menyertakan bendera klasifikasi untuk masing-masing dalam data yang direkam. Pertimbangkan bahwa file log yang dihasilkan oleh aplikasi Anda mungkin digunakan oleh pihak-pihak, seperti solusi pemantauan log pihak ketiga atau penyedia layanan eksternal, yang tidak berwenang untuk melihat data sensitif apa pun yang diproses aplikasi.
- Atribut berikut tidak boleh direkam langsung di log. Hapus, tutupi, sanitasi, hash, atau enkripsi yang berikut ini:
  - Kode sumber aplikasi
  - Nilai identifikasi sesi (pertimbangkan untuk mengganti ini dengan nilai hash jika Anda perlu melacak peristiwa khusus sesi)
  - Token akses
  - Data pribadi sensitif dan beberapa bentuk informasi identitas pribadi (PII), seperti informasi kesehatan atau pengenal yang dikeluarkan pemerintah
  - Kata sandi otentikasi
  - String koneksi database
  - Kunci enkripsi dan rahasia utama lainnya

- Rekening bank atau data pemegang kartu pembayaran
- Data dengan klasifikasi keamanan yang lebih tinggi daripada sistem logging diizinkan untuk disimpan
- Informasi yang sensitif secara komersial
- Informasi yang ilegal untuk dikumpulkan di yurisdiksi yang relevan
- Informasi bahwa pengguna telah memilih keluar dari atau belum secara eksplisit menyetujui pengumpulan
- Informasi yang persetujuan untuk dikumpulkan telah kedaluwarsa

Tipe data khusus

Terkadang, data berikut juga dapat direkam dalam log. Meskipun dapat berguna untuk tujuan investigasi dan pemecahan masalah, ini dapat mengungkapkan informasi sensitif tentang sistem. Anda mungkin perlu menganonimkan, hash, atau mengenkripsi tipe data ini sebelum acara direkam:

- Jalur file
- Nama dan alamat jaringan internal
- Data pribadi yang tidak sensitif, seperti nama pribadi, nomor telepon, dan alamat email

Gunakan anonimisasi data jika identitas asli individu tidak diperlukan dalam log atau jika risikonya dianggap terlalu besar.

Akses dan manajemen perubahan

- Pengguna non-administratif seharusnya tidak dapat menonaktifkan pencatatan peristiwa, terutama yang diperlukan untuk memenuhi persyaratan kepatuhan.
- Hanya pengguna administratif yang dapat menjeda atau menghentikan layanan logging atau memodifikasi konfigurasi.
- Jika layanan logging Anda memiliki fitur validasi integritas file log, aktifkan. Ini membantu Anda mendeteksi modifikasi, penghapusan, atau penempaan file log. Untuk informasi lebih lanjut tentang fitur ini diAWS layanan, lihatMenggunakan CloudTraildalam panduan ini.
- Perubahan logging harus intrinsik untuk aplikasi, seperti dibuat secara otomatis oleh aplikasi berdasarkan algoritma yang disetujui, atau mengikuti proses manajemen perubahan yang disetujui, seperti ketika Anda mengubah data konfigurasi atau memodifikasi kode sumber.

AWS layananuntuk pencatatan dan pemantauan

Panduan ini berfokus pada pencatatan dan pemantauan aplikasi yang digunakan diAWS Cloud. Anda dapat menggunakanAWS layananuntuk mengimplementasikan rencana pencatatan dan pemantauan Anda, atau Anda dapat menggunakannya untuk menambah solusi Anda saat ini. Misalnya, jika Anda memecahkan masalah dengan aplikasi Anda, Anda dapat:

- Lakukan triase log aplikasi dengan fitur VPC Flow Logs di Amazon Virtual Private Cloud (Amazon VPC) dan lihat lalu lintas jaringan yang sesuai dengan masalah tersebut.
- GunakanAWS CloudTrailuntuk melihat panggilan API yang sesuai dengan waktu peristiwa masalah.
- Tinjau log di AmazonCloudWatchLog untuk memeriksa lonjakan CPU yang sesuai dengan waktu peristiwa masalah.

Anda dapat menerapkan yang berikutAWS layanandan fitur untuk pencatatan dan pemantauan aplikasi Anda:

- AWS CloudTrailmembantu Anda mengaudit tata kelola, kepatuhan, dan risiko operasional AndaAkun AWSdengan merekam tindakan yang diambil oleh pengguna, peran, atauAWS layanan. Untuk informasi selengkapnya tentang penggunaan layanan ini untuk mencatat atau memantau peristiwa untuk aplikasi Anda, lihatCloudTraildalam panduan ini.
- AmazonCloudWatchmembantu Anda menganalisis log dan, secara real time, memantau metrik AndaAWSsumber daya dan aplikasi yang dihosting. Anda juga dapat menggunakanServiceLensfitur untuk memantau kesehatan aplikasi Anda atau menggunakan fitur Synthetics untuk membuat kenari yang memantau titik akhir dan API Anda. Untuk informasi selengkapnya tentang penggunaan layanan ini untuk memantau aplikasi Anda, lihatCloudWatchdalam panduan ini.
- AmazonCloudWatchLogmembantu Anda memusatkan log dari semua sistem, aplikasi, danAWS layanansehingga Anda dapat memonitor mereka dan mengarsipkannya dengan aman. Untuk informasi selengkapnya tentang menggunakan layanan ini untuk mencatat peristiwa untuk aplikasi Anda, lihatCloudWatch Logdalam panduan ini.
- TheLog Aliran VPCFitur Amazon Virtual Private Cloud (Amazon VPC) menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di VPC Anda. Untuk informasi selengkapnya tentang menggunakan layanan ini untuk mencatat peristiwa untuk aplikasi Anda, lihatLog Alur VPCdalam panduan ini.

- AWS X-Raymengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan ini membantu Anda melihat, memfilter, dan mendapatkan wawasan tentang data tersebut untuk mengidentifikasi masalah dan peluang pengoptimalan. Untuk informasi selengkapnya tentang penggunaan layanan ini untuk memantau aplikasi Anda, lihatX-Raydalam panduan ini.

Pencatatan dan pemantauan aplikasi menggunakanAWS CloudTrail

AWS CloudTrailadalah sebuahAWS layananyang membantu Anda mengaktifkan audit operasional dan risiko, tata kelola, dan kepatuhan AndaAkun AWS. Tindakan yang diambil oleh pengguna, peran, atauAWS layanandicatat sebagaiacaradiCloudTrail. Peristiwa dapat mencakup tindakan yang diambil dalamAWS Management Console,AWS Command Line Interface(AWS CLI), danAWSSDK dan API.

Menggunakan CloudTrail

CloudTraildiaktifkan pada AndaAkun AWSketika Anda membuatnya. Ketika aktivitas terjadi diAkun AWSKegiatan tersebut dicatat dalamCloudTrailacara. Anda dapat dengan mudah melihat peristiwa terbaru diCloudTrailkonsol dengan pergi keRiwayat acara.

Untuk catatan aktivitas dan acara yang sedang berlangsung diAkun AWS, Anda membuatjejak. Anda dapat membuat jalur untuk satuWilayah AWSatau untuk semua wilayah. Trails merekam file log di setiap Wilayah, danCloudTraildapat mengirimkan file log ke satu bucket Amazon Simple Storage Service (Amazon S3) yang terkonsolidasi.

Anda dapat mengonfigurasi beberapa jejak secara berbeda sehingga jejak memproses dan hanya mencatat peristiwa yang Anda tentukan. Ini dapat berguna ketika Anda ingin melakukan triase peristiwa yang terjadi di AndaAkun AWSdengan peristiwa yang terjadi dalam aplikasi Anda.

> **Note**
>
> CloudTrailmemiliki fitur validasi yang dapat Anda gunakan untuk menentukan apakah file log diubah, dihapus, atau tidak berubah setelahnyaCloudTrailmengirimkannya. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukanCloudTraillog file tanpa deteksi. Anda dapat menggunakanAWS CLIuntuk memvalidasi file di lokasi di manaCloudTrailmengantarkan

mereka. Untuk informasi selengkapnya tentang fitur ini dan cara mengaktifkannya, lihatMemvalidasiCloudTrailintegritas file log(CloudTraildokumentasi).

Kasus penggunaan untuk CloudTrail

- Bantuan kepatuhan— MenggunakanCloudTraildapat membantu Anda mematuhi kebijakan internal dan standar peraturan dengan memberikan riwayat peristiwa diAkun AWS.
- Analisis keamanan— Anda dapat melakukan analisis keamanan dan mendeteksi pola perilaku pengguna dengan menelanCloudTraillog file ke manajemen log dan solusi analitik, sepertiCloudWatchLog, AmazonEventBridge, Amazon Athena, AmazonOpenSearchLayanan, atau solusi pihak ketiga lainnya.
- Eksfiltrasi data— Anda dapat mendeteksi eksfiltrasi data dengan mengumpulkan data aktivitas pada objek Amazon S3 melalui peristiwa API tingkat objek yang direkamCloudTrail. Setelah data aktivitas dikumpulkan, Anda dapat menggunakan yang lainAWS layanan, sepertiEventBridgedanAWS Lambda, untuk memicu respons otomatis.
- Pemecahan masalah operasional— Anda dapat memecahkan masalah operasional dengan menggunakanCloudTrailfile log. Misalnya, Anda dapat dengan cepat mengidentifikasi perubahan terbaru yang dibuat pada sumber daya di lingkungan Anda, termasuk pembuatan, modifikasi, dan penghapusanAWSsumber daya.

Praktik terbaik untuk CloudTrail

- AktifkanCloudTraildalam semuaWilayah AWS.
- Aktifkan validasi integritas file log.
- Enkripsi log.
- TertelanCloudTraillog file keCloudWatchLog.
- Memusatkan log dari semuaAkun AWSdan Wilayah.
- Terapkan kebijakan siklus hidup ke bucket S3 yang berisi file log.
- Mencegah pengguna agar tidak dapat menonaktifkan loginCloudTrail. Terapkan yang berikut inikebijakan kontrol layanan(SCP) diAWS Organizations. SCP ini menetapkan aturan penolakan eksplisit untuk`StopLogging`dan`DeleteTrail`tindakan di seluruh organisasi.

```
{
"Version": "2012-10-17",
```

```
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

Pencatatan dan pemantauan aplikasi menggunakan AmazonCloudWatch

AmazonCloudWatchmemonitor AndaAWSsumber daya dan aplikasi yang Anda jalankanAWSsecara real time. Anda dapat menggunakanCloudWatchuntuk mengumpulkan dan melacakmetrik, yang merupakan variabel yang dapat Anda ukur untuk sumber daya dan aplikasi Anda.

Menggunakan CloudWatch

CloudWatchPada dasarnya, adalah repositori metrik. SebuahAWS layanan, seperti Amazon EC2, menempatkan metrik ke dalam repositori, dan Anda mengambil statistik berdasarkan metrik tersebut. Jika Anda memasukkan metrik kustom Anda sendiri ke dalam repositori, Anda juga dapat mengambil statistik pada metrik ini. Untuk informasi lebih lanjut, lihatMenggunakanCloudWatchmetrik(CloudWatchdokumentasi).

Anda juga dapat mengkonfigurasialarm, yang secara otomatis memulai tindakan atas nama Anda. Alarm mengawasi metrik tunggal selama periode waktu tertentu dan melakukan satu atau lebih tindakan tertentu, berdasarkan nilai metrik relatif terhadap ambang batas dari waktu ke waktu. Misalnya, alarm mungkin mengirim pemberitahuan ke topik Amazon Simple Notification Service (Amazon SNS). Anda juga dapat menambahkan alarm ke dasbor. Untuk informasi lebih lanjut, lihatMenggunakanCloudWatchalarm(CloudWatchdokumentasi).

TheCloudWatchkonsol secara otomatis menampilkan metrik tentang setiapAWS layananAnda menggunakan. Anda dapat membuat dasbor khusus tambahan untuk menampilkan metrik dan alarm untuk aplikasi Anda. Untuk informasi lebih lanjut, lihatMenggunakanCloudWatchdasbor(CloudWatchdokumentasi).

CloudWatchsecara otomatis mendukung fungsionalitas lintas wilayah. Anda tidak perlu mengambil langkah tambahan untuk menampilkan metrik dari yang berbedaWilayah AWSdalam satu akun pada grafik atau dasbor yang sama. Anda dapat mencapai fungsionalitas lintas akun dengan menerapkanobservabilitas lintas akun(CloudWatchdokumentasi).

Untuk informasi lebih lanjut dan panduan rinci tentang penggunaanCloudWatchuntuk mencatat dan memantau beban kerja diAWS Cloud, lihatMerancang dan menerapkan pencatatan dan pemantauan dengan AmazonCloudWatch(AWSPanduan Preskriptif).

Kasus penggunaan untuk CloudWatch

- Pemantauan kesehatan aplikasi—CloudWatch ServiceLensmeningkatkan observabilitas layanan dan aplikasi Anda dengan memungkinkan Anda mengintegrasikan jejak, metrik, log, alarm, dan informasi kesehatan sumber daya lainnya ke satu tempat. ServiceLensterintegrasiCloudWatchbersamaAWS X-Rayuntuk memberikan tampilan end-to-end dari aplikasi Anda untuk membantu Anda lebih efisien menentukan kemacetan kinerja dan mengidentifikasi pengguna yang terkena dampak. Untuk informasi lebih lanjut, lihatMenggunakanServiceLensuntuk memantau kesehatan aplikasi Anda(CloudWatchdokumentasi).
- Pemantauan sintetis— Anda dapat menggunakanCloudWatchSintetis untuk membuat kenari, skrip yang dapat dikonfigurasi yang berjalan sesuai jadwal, untuk memantau titik akhir dan API Anda. Canary mengikuti rute yang sama dan melakukan tindakan yang sama sebagai pelanggan, sehingga memungkinkan Anda untuk terus memverifikasi pengalaman pelanggan bahkan ketika Anda tidak memiliki lalu lintas pelanggan pada aplikasi Anda. Canary memeriksa ketersediaan dan latensi titik akhir Anda dan dapat menyimpan data waktu pemuatan dan tangkapan layar UI. Mereka memantau REST API, URL, dan konten situs web Anda, dan mereka dapat memeriksa perubahan yang tidak sah dari phishing, injeksi kode, dan skrip lintas situs. Untuk informasi lebih lanjut, lihatMenggunakan pemantauan sintetis(CloudWatchdokumentasi).
- Pemantauan pengguna— DenganCloudWatchRUM, Anda dapat melakukan pemantauan pengguna nyata untuk mengumpulkan dan melihat data sisi klien tentang kinerja aplikasi web Anda. Data mencakup waktu pemuatan halaman, kesalahan sisi klien, dan perilaku pengguna. Anda dapat menggunakan data yang dikumpulkan untuk mengidentifikasi dan men-debug masalah kinerja sisi klien dengan cepat. Untuk informasi lebih lanjut, lihatMenggunakanCloudWatchRUM(CloudWatchdokumentasi).
- Deteksi perilaku anomali— Saat Anda mengaktifkandeteksi anomaliuntuk metrik,CloudWatchmenerapkan algoritma statistik dan pembelajaran mesin. Algoritma ini terus menganalisis metrik sistem dan aplikasi, menentukan garis dasar normal, dan

anomali permukaan. Untuk informasi lebih lanjut, lihatMenggunakanCloudWatchdeteksi anomali(CloudWatchdokumentasi).

- Validasi fitur dan eksperimen A/BAnda dapat menggunakan AmazonCloudWatchTerbukti untuk memvalidasi fitur-fitur baru dengan aman dengan menyajikannya ke persentase tertentu dari pengguna Anda saat Anda meluncurkan fitur tersebut. Anda juga dapat melakukan eksperimen A/B untuk membuat keputusan desain fitur berdasarkan bukti dan data. Untuk informasi lebih lanjut, lihatLakukan peluncuran dan eksperimen A/B denganCloudWatchTerbukti(CloudWatchdokumentasi).

Pencatatan dan pemantauan aplikasi menggunakan AmazonCloudWatchLog

AmazonCloudWatchLogmemungkinkan Anda untuk memusatkan log dari semua sistem, aplikasi, danAWS layananyang Anda gunakan, dalam satu layanan yang sangat skalabel. Anda kemudian dapat dengan mudah melihat log, mencari adanya kode atau pola kesalahan tertentu, memfilter berdasarkan bidang tertentu, atau mengarsipkannya dengan aman untuk analisis pada masa mendatang. Anda dapat melihat semua peristiwa log Anda, terlepas dari sumbernya, sebagai aliran peristiwa tunggal dan konsisten yang diurutkan berdasarkan waktu. Anda dapat menanyakan dan mengurutkannya, mengelompokkannya berdasarkan bidang tertentu, membuat perhitungan khusus, dan memvisualisasikan data log di dasbor.

MenggunakanCloudWatchLog

DiCloudWatchLog, peristiwa log diatur ke dalam aliran log dan grup log. Pengaliran log adalah urutan log acara yang berbagi sumber yang sama. Lebih khusus lagi, pengaliran log umumnya dimaksudkan untuk mewakili urutan kejadian yang berasal dari instans aplikasi atau sumber daya yang dipantau. Grup logtentukan satu atau beberapa aliran log yang berbagi pengaturan retensi, pemantauan, dan kontrol akses yang sama. Setiap aliran log harus dimiliki setidaknya satu grup log. Untuk informasi lebih lanjut, lihatBekerja dengan grup log dan aliran log(CloudWatchDokumentasi log).

Anda dapat menggunakanCloudWatchLog Wawasan untuk mencari dan menganalisis data log Anda di AmazonCloudWatchLog. Anda dapat melakukan kueri untuk membantu Anda agar lebih efisien dan efektif dalam menanggapi masalah operasional. Jika terjadi masalah, Anda dapat menggunakanCloudWatchLog Wawasan untuk mengidentifikasi penyebab potensial dan memvalidasi perbaikan yang diterapkan. Untuk informasi lebih lanjut, lihatMenganalisis data log denganCloudWatchWawasan Log(CloudWatchDokumentasi log).

Anda dapat mencari dan memfilter data log yang masukCloudWatchLog dengan membuat satu atau lebihfilter metrik. Filter metrik menentukan istilah dan pola yang akan dicari dalam data log saat dikirim keCloudWatchLog. CloudWatchLog menggunakan filter metrik ini untuk mengubah data log menjadi numerikCloudWatchmetrik yang dapat Anda buat grafik atau nyalakan alarm. Untuk informasi lebih lanjut, lihatMembuat metrik dari peristiwa log menggunakan filter(CloudWatchDokumentasi log).

Gunakan kasus untukCloudWatchLog

- PemantauanCloudTraillog— Anda dapat membuat alarm diCloudWatchdan menerima pemberitahuan aktivitas API tertentu, seperti yang ditangkap olehCloudTrail, dan gunakan notifikasi untuk melakukan pemecahan masalah. Untuk informasi lebih lanjut, lihatMengirimCloudTrailAcara keCloudWatchLog(CloudTraildokumentasi).
- PenebanganAWSPanggilan API— Jika Anda memiliki solusi pemantauan pihak ketiga, Anda dapat menggunakanCloudWatchLog untuk logAWSPanggilan API. Anda menyiapkan layanan pemantauan pihak ketiga untuk mengevaluasi log ini dan API tingkat aplikasi.
- Mengkonfigurasi retensi log— Secara default, log inCloudWatchLog disimpan tanpa batas waktu dan tidak pernah kedaluwarsa. Anda dapat menyesuaikan kebijakan retensi untuk setiap grup log, menjaga retensi tidak terbatas, atau memilih periode retensi antara satu hari dan 10 tahun.
- Mengarsipkan dan menyimpan log— Anda dapat menggunakanCloudWatchLog untuk menyimpan data log Anda dalam penyimpanan yang sangat tahan lama. TheCloudWatchAgen log mengirimkan data log yang diputar dan tidak diputar ke dalam layanan log. Anda kemudian dapat mengakses data log mentah ketika dibutuhkannya.

Pencatatan dan pemantauan aplikasi menggunakan VPC Flow Logs

Log Aliran VPCadalah fitur Amazon Virtual Private Cloud (Amazon VPC) yang membantu Anda menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di VPC Anda.

Menggunakan VPC Flow Logs

Anda dapat membuat log aliran untuk virtual private cloud (VPC), subnet, atau antarmuka jaringan. Jika Anda membuat log alur untuk subnet atau VPC, setiap antarmuka jaringan di subnet atau VPC dipantau. Untuk informasi lebih lanjut, lihatBekerja dengan log aliran(Dokumentasi Amazon VPC).

Data log aliran untuk antarmuka jaringan yang dipantau dicatat sebagai catatan log aliran. SEBUAHcatatan log aliranmewakili aliran jaringan di VPC Anda. Secara default, setiap catatan menangkap arus lalu lintas IP jaringan yang terjadi dalam interval agregasi. Setiap catatan adalah string dengan bidang yang dipisahkan oleh spasi. Sebuah catatan termasuk nilai-nilai untuk komponen yang berbeda dari aliran IP, misalnya, sumber, tujuan, dan protokol. Ketika Anda membuat log alur, Anda dapat menggunakan format default untuk catatan log alur, atau Anda dapat menentukan format kustom. Untuk informasi lebih lanjut, lihatContoh catatan log aliran(Dokumentasi Amazon VPC).

Log aliran tidak menangkap informasi berikut:

- Lalu lintas yang dihasilkan oleh instance ketika mereka menghubungi server Amazon Domain Name System (DNS). Jika Anda menggunakan server DNS Anda sendiri, maka semua lalu lintas ke server DNS tersebut dicatat.
- Lalu lintas yang dihasilkan oleh instans Windows untuk aktivasi lisensi Amazon Windows.
- Lalu lintas ke dan dari`254.169.254`Misalnya metadata.
- Lalu lintas ke dan dari`254.169.123`, untuk Layanan Sinkronisasi Waktu Amazon.
- Lalu lintas Dynamic Host Configuration Protocol (DHCP).
- Lalu lintas ke alamat IP yang dipesan untuk router VPC default.
- Lalu lintas antara antarmuka jaringan titik akhir dan antarmuka jaringan Penyeimbang Beban Jaringan.

Data log aliran dapat dipublikasikan ke beberapaAWS layanan, termasuk AmazonCloudWatchLog. Setelah Anda membuat log aliran, Anda dapat mengambil dan melihat catatan log aliran diCloudWatchLog di grup log yang Anda konfigurasikan. Untuk informasi lebih lanjut, lihatPublikasikan log aliran keCloudWatchLog(Dokumentasi Amazon VPC).

Data log alur dikumpulkan di luar jalur lalu lintas jaringan Anda, dan oleh karena itu tidak mempengaruhi throughput atau latensi jaringan. Anda dapat membuat atau menghapus log alur tanpa risiko dampak terhadap kinerja jaringan.

Kasus penggunaan untuk VPC Flow Logs

- Mendiagnosis aturan kelompok keamanan yang terlalu ketat
- Pantau lalu lintas yang mencapai instance aplikasi Anda
- Tentukan arah lalu lintas

Pencatatan dan pemantauan aplikasi menggunakanAWS X-Ray

AWS X-Raymengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan ini membantu Anda melihat, memfilter, dan mendapatkan wawasan tentang data tersebut untuk mengidentifikasi masalah dan peluang pengoptimalan.

Menggunakan X-Ray

AWS X-Raymenerima jejak dari aplikasi Anda dan, jika mereka terintegrasi dengan X-Ray, dariAWS layananyang digunakan aplikasi Anda. Sampel X-Ray dan memvisualisasikan permintaan padagrafik layananketika mereka mengalir melalui komponen aplikasi Anda. X-Ray menghasilkan pengidentifikasi jejak sehingga Anda dapat mengkorelasikan permintaan saat mengalir melalui beberapa komponen, yang membantu Anda melihat permintaan dari ujung ke ujung. Anda dapat lebih menyempurnakannya dengan menyertakan anotasi dan metadata untuk membantu mencari dan mengidentifikasi karakteristik permintaan secara unik.

Kami menyarankan Anda mengonfigurasi setiap server atau titik akhir dalam aplikasi Anda dengan X-Ray. X-Ray diimplementasikan dalam kode aplikasi Anda dengan melakukan panggilan ke layanan X-Ray. X-Ray juga menyediakanAWSSDK untuk berbagai bahasa, termasuk klien berinstrumen yang secara otomatis mengirim data ke X-Ray. X-Ray SDK menyediakan tambalan ke pustaka umum yang digunakan untuk melakukan panggilan ke layanan lain (misalnya, HTTP, MySQL, PostgreSQL, atau MongoDB).

Untuk informasi lebih lanjut, lihatMenelusuri aplikasi denganAWS X-Ray(AWSPanduan Preskriptif).

Gunakan kasus untuk X-Ray

- Analisis aplikasi dan debug— Melacak data dapat membantu Anda men-debug aplikasi dengan memberikan tampilan permintaan dari ujung ke ujung sehingga Anda dapat mengidentifikasi kemacetan dan memecahkan masalah. X-Raypeta layananadalah alat visual yang membantu Anda mengidentifikasi di mana kesalahan terjadi, koneksi dengan latensi tinggi, atau jejak untuk permintaan yang gagal.
- Analisis kinerja—Konsol Analyticsadalah alat interaktif untuk menafsirkan data jejak untuk memahami dengan cepat bagaimana kinerja aplikasi Anda dan layanan yang mendasarinya. Konsol membantu Anda menjelajahi, menganalisis, dan memvisualisasikan jejak. Anda juga dapat membandingkan set jejak dengan kondisi yang berbeda, untuk analisis akar penyebab.

Pertanyaan umum

Dapatkah saya menggunakan layanan pemantauan saya saat ini?

AmazonCloudWatchadalah layanan pemantauan dan observabilitas yang dibangun untukDevOpsinsinyur, pengembang, insinyur keandalan situs (SRE), manajer TI, dan pemilik aplikasi. Ini memberikan data dan wawasan yang dapat ditindaklanjuti untuk membantu Anda memantau aplikasi Anda, menanggapi perubahan kinerja di seluruh sistem, dan mengoptimalkan pemanfaatan sumber daya. Namun, jika Anda memiliki layanan pemantauan yang mapan, Anda tidak perlu menggantinya.

Bagaimana cara menghentikan file log agar tidak dirusak?

Anda dapat mengaktifkan validasi integritas file log. Ini adalah praktik yang baik untuk mengelola dan menyimpan log Anda di tempat khususAkun AWSdan membatasi akses ke akun tersebut. Untuk informasi lain, lihat Menggunakan CloudTrail dalam panduan ini.

Apakah saya harus memelihara file log terpisah untuk setiap aplikasi?

Tidak, Anda dapat mengkonsolidasikan data log dari beberapa aplikasi ke dalam file log yang sama. Namun, pastikan bahwa pengidentifikasi unik untuk setiap aplikasi direkam dalam aliran log.

Sumber daya

Dokumentasi AWS

- AWS CloudTraildokumentasi
- AWS CloudTonton dokumentasi
- AWS CloudTonton dokumentasi Log
- Dokumentasi Amazon VPC Flow Logs
- AWS X-Raydokumentasi
- Merancang dan menerapkan pencatatan dan pemantauan dengan AmazonCloudWatch(AWSBimbingan Preskriptif)

AWSpemasaran

- AWS CloudTrail
- AmazonCloudWatch
- Logging TerpusatAWS(AWSSolusi)
- Pemantauan dan Observabilitas(AWS CloudOperasi)
- Cara Memantau Aplikasi Anda Secara Efektif(AWSStartup)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan di masa mendatang, Anda dapat berlanggananUmpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Januari 6, 2023

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

Cloud Center of Excellence (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme pemrosesan gambar untuk CV.

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi database.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

komputasi tepi

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin

kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

G

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

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

layanan mikro

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

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase

ini menggunakan praktik terbaik dan pelajaran yang dipetik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi,

dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

persistensi poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

Privasi oleh Desain

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

zona host pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

pseudonimisasi

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

terbitkan/berlangganan (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Wilayah

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke AWS Management Console atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk

semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

PENIPUAN

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh

tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans Amazon EC2, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh AWS layanan yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

T

tag

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

variabel target

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

daftar tugas

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

lingkungan uji

Lihat lingkungan.

pelatihan

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

gerbang transit

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

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

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

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

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

data hangat

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

fungsi jendela

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat Kerangka Kualifikasi Beban Kerja AWS.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

aplikasi zombie

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

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