Transisi ke beberapa Akun AWS

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Transisi ke beberapa Akun AWS

Table of Contents

Transisi ke beberapa Akun AWS

Amazon Web Services (kontributor)

Mei 2024 (riwayat dokumen)

Banyak perusahaan memulai perjalanan mereka dengan menggunakan satu akun Amazon Web Services (AWS). Beberapa peran dalam perusahaan menggunakan akun ini untuk mengoperasikan bisnis. Insinyur mengembangkan kode, menyebarkan ke lingkungan pengembangan dan pengujian, dan mempromosikan perubahan pada produksi. Manajer produk meminta sumber data untuk mengumpulkan wawasan tentang kinerja bisnis. Tim penjualan sedang melakukan demo dari lingkungan produksi untuk menarik pelanggan baru. Tim keuangan memantau pengeluaran cloud dari AWS Billing konsol.

Ketika semua peran terpisah ini menggunakan satu Akun AWS, akan menjadi sulit untuk menerapkan praktik terbaik keamanan Menerapkan izin hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin minimum yang diperlukan untuk melakukan pekerjaan itu. Pada tahap tertentu dalam pengembangan startup, seseorang akan mengajukan pertanyaan Apakah semua teknisi kami membutuhkan akses ke produksi? Jawabannya hampir selalu tidak, tetapi banyak perusahaan berjuang dengan cara melepas lingkungan akun tunggal mereka yang ada ke dalam lingkungan multi-akun tanpa memperlambat bisnis.

Panduan ini mencakup praktik terbaik untuk membantu Anda beralih dari lingkungan akun tunggal ke lingkungan multi-akun. Ini membahas keputusan yang perlu Anda buat tentang migrasi akun, manajemen pengguna, jaringan, keamanan, dan arsitektur. Ini dirancang untuk membantu Anda sukses dengan downtime minimal atau tanpa waktu henti untuk bisnis dan operasi harian Anda. Panduan ini berfokus pada kemampuan berikut saat Anda beralih dari satu Akun AWS ke lingkungan multi-akun:

- Manajemen identitas dan kontrol akses
- Mengelola izin dan akses
- Konektivitas jaringan
- Respon insiden keamanan
- Backup
- Migrasi akun
- Migrasi sumber daya

- Pertimbangan penagihan

Untuk informasi selengkapnya tentang kemampuan, lihatCloud Foundation di AWS.

Panduan ini disejajarkan dengan sumber daya yang ada terkait dengan topik ini, termasuk AWS Startup Security Baseline (AWS SSB), whitepaper Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun, Arsitektur Referensi AWS Keamanan (AWS SRA) dan Establishing Your Cloud Foundation di whitepaper. AWS Anda harus terus menggunakan sumber daya tersebut untuk panduan yang lebih spesifik yang tidak tercakup dalam panduan ini.

Audiens yang dituju

Panduan ini paling cocok untuk perusahaan yang ingin atau perlu beralih ke beberapa Akun AWS. Untuk startup, kebutuhan ini biasanya muncul ketika Anda telah menemukan kecocokan pasar produk, mengumpulkan putaran pendanaan, dan mulai menyewa disiplin teknik yang berbeda, seperti infrastruktur, operasi pengembangan ()DevOps, atau keamanan.

Bahkan jika perusahaan Anda belum siap untuk melakukan transisi ini, Anda masih dapat menggunakan panduan ini untuk memahami keputusan yang perlu dibuat selama transisi dan mulai mempersiapkan.

Tujuan untuk transisi ke arsitektur multi-akun

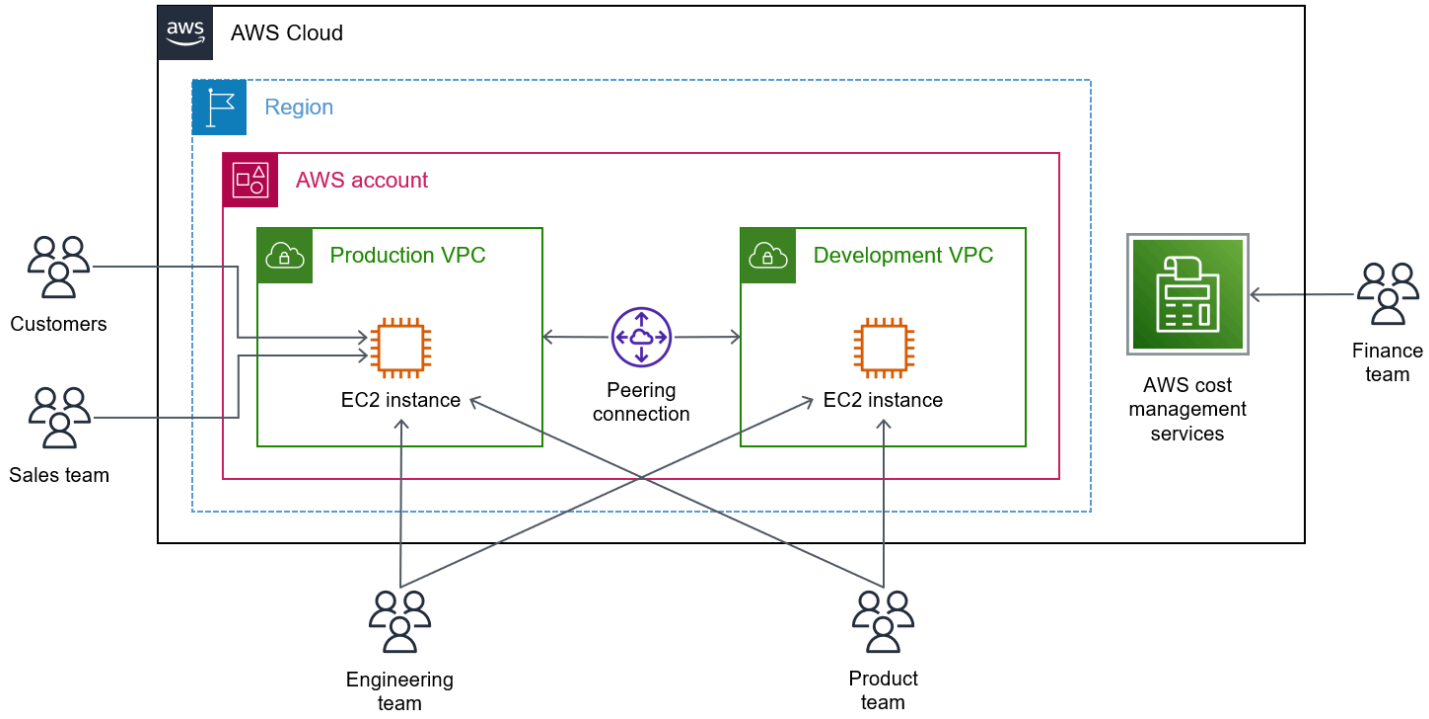
Transisi ke arsitektur multi-akun biasanya didorong oleh kebutuhan bisnis untuk satu atau lebih manfaat berikut:

- Mengelompokkan beban kerja berdasarkan tujuan bisnis atau kepemilikan
- Menerapkan kontrol keamanan yang berbeda menurut lingkungan
- Membatasi akses ke data sensitif
- Mempromosikan inovasi dan kelincahan
- Membatasi ruang lingkup dampak dari efek samping
- Mendukung beberapa model operasi TI
- Mengelola biaya
- Mendistribusikan Layanan AWS kuota dan batas tingkat permintaan API

Untuk informasi selengkapnya tentang banyak manfaat menggunakan arsitektur multi-akun, lihat Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun (AWSwhitepaper) dan Pedoman untuk menyiapkan lingkungan yang dirancang dengan baik (dokumentasi). AWS Control Tower

Contoh arsitektur akun tunggal

Sebagai titik awal, adalah umum bagi startup atau perusahaan kecil untuk menggunakan satu Wilayah AWS dan memiliki dua virtual private cloud (VPC) yang dihubungkan oleh peering VPC. Setiap VPC berisi sumber daya komputasi, seperti instans Amazon Elastic Compute Cloud (Amazon EC2). Tim teknik mengembangkan kode langsung di VPC Pengembangan. Tim produk meninjau perubahan, dan kemudian tim teknik secara manual mempromosikan perubahan pada VPC Produksi. Tim keuangan memiliki akses ke Akun AWS sehingga mereka dapat meninjau AWS Billing and Cost Management konsol.



Berikut ini adalah beberapa contoh tantangan yang mungkin dialami perusahaan dengan lingkungan ini:

- Seorang insinyur secara keliru menghapus data produksi ketika mereka mengira mereka mengakses database pengembangan.
- Demo penjualan terpengaruh ketika penyebaran produksi memakan waktu lebih lama dari yang diharapkan.
- Ketika kode pengembangan sedang diuji beban, VPC Produksi menjadi lambat dan menghasilkan pesan kesalahan tentang pelambatan.
- Tim keuangan tidak dapat membedakan biaya untuk lingkungan produksi dan pengembangan.
- CEO khawatir bahwa beberapa kontraktor lepas pantai yang baru dipekerjakan memiliki akses ke data pelanggan melalui VPC Produksi.
- Tim keuangan tidak dapat melarang akses ke spesifik Layanan AWS yang mungkin menimbulkan biaya tinggi.

Mengadopsi strategi multi-akun mengatasi semua tantangan ini dengan menggunakan kotak-kotak untuk memisahkan beban kerja dan Akun AWS akses.

Kerangka dasar dan tanggung jawab keamanan untuk transisi ke arsitektur multi-akun

Informasi dan praktik terbaik dalam panduan ini dirancang untuk melengkapi AWS rekomendasi yang ada untuk infrastruktur dan keamanan. Saat Anda bertransisi dari satu Akun AWS ke beberapaAkun AWS, penting untuk memastikan bahwa arsitektur multi-akun baru Anda konsisten dengan prinsip AWS Well-Architected Framework dan Cloud Foundation. Ini membantu Anda membangun dan mengoperasikan lingkungan yang dirancang untuk keamanan, kinerja, dan ketahanan, sambil mematuhi persyaratan tata kelola dan praktik terbaik. AWS

AWSKerangka Well-Architected

AWSWell-Architected Framework membantu Anda membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja. Panduan ini sejalan dengan pilar Keunggulan Operasional, Keamanan, dan Keandalan kerangka kerja ini. Ini membantu Anda memenuhi persyaratan bisnis dan peraturan Anda dengan mengikuti AWS rekomendasi saat ini.

Anda dapat menilai kepatuhan Anda terhadap praktik terbaik yang dirancang dengan baik dengan menggunakan dalam AWS Well-Architected ToolAnda. Akun AWS

Cloud Foundation di AWS

Membangun Yayasan Cloud Anda di AWS (AWSWhitepaper) memberikan panduan yang membantu Anda menyesuaikan AWS lingkungan Anda untuk memenuhi kebutuhan bisnis Anda. Dengan menggunakan pendekatan berbasis kemampuan, Anda dapat membuat lingkungan untuk menyebarkan, mengoperasikan, dan mengelola beban kerja Anda. Anda juga dapat meningkatkan kemampuan untuk memperluas lingkungan Anda saat kebutuhan Anda berkembang dan Anda menyebarkan beban kerja tambahan ke cloud. Untuk informasi selengkapnya tentang 30 kemampuan yang ditentukan olehAWS, lihat Kemampuan. Panduan ini mencakup praktik terbaik untuk menerapkan kemampuan awal dalam urutan yang dimaksudkan.

Anda dapat mengadopsi dan menerapkan kemampuan sesuai dengan kebutuhan operasional dan tata kelola Anda. Saat kebutuhan bisnis Anda matang, pendekatan berbasis kemampuan dapat digunakan sebagai mekanisme untuk memverifikasi bahwa lingkungan cloud Anda siap mendukung beban kerja dan skala sesuai kebutuhan. Pendekatan ini memungkinkan Anda untuk dengan percaya diri membangun lingkungan cloud Anda untuk pembangun dan bisnis Anda.

Manajemen identitas dan kontrol akses untuk transisi ke arsitektur multi-akun

Langkah pertama saat beralih ke arsitektur multi-akun adalah menyiapkan struktur akun baru Anda dalam suatu organisasi. Kemudian Anda dapat menambahkan pengguna dan mengonfigurasi akses mereka ke akun. Bagian ini menjelaskan pendekatan untuk mengelola akses manusia ke beberapaAkun AWS.

Bagian ini terdiri dari tugas-tugas berikut:

- Menyiapkan organisasi
- Buat landing zone
- Tambahkan unit organisasi
- Tambahkan pengguna awal
- Kelola akun anggota

Menyiapkan organisasi

Ketika Anda memiliki beberapaAkun AWS, Anda dapat secara logis mengelola akun tersebut melalui organisasi di AWS Organizations. Akun di AWS Organizations adalah standar Akun AWS yang berisi AWS sumber daya Anda dan identitas yang dapat mengakses sumber daya tersebut. Organisasi adalah entitas yang mengkonsolidasikan Anda Akun AWS sehingga Anda dapat mengelolanya sebagai satu unit.

Ketika Anda menggunakan akun untuk membuat organisasi, akun itu menjadi akun manajemen (juga dikenal sebagai akun pembayar atau akun root) untuk organisasi. Sebuah organisasi hanya dapat memiliki satu akun manajemen. Ketika Anda menambahkan tambahan Akun AWS ke organisasi, mereka menjadi akun anggota.

> **Note**
>
> Masing-masing Akun AWS juga memiliki identitas tunggal yang disebut pengguna root. Anda dapat masuk sebagai pengguna root dengan menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Namun, kami sangat menyarankan agar Anda

tidak menggunakan pengguna root untuk tugas sehari-hari, bahkan yang administratif. Untuk informasi selengkapnya, lihat pengguna Akun AWS root.

Anda mengatur akun dalam struktur seperti pohon hierarkis yang terdiri dari akar organisasi, unit organisasi (OU), dan akun anggota. Root adalah wadah induk untuk semua akun di organisasi Anda. Unit organisasi (OU) adalah wadah untuk akun di dalam root. OU dapat berisi akun OU atau anggota lainnya. OU hanya dapat memiliki satu orang tua, dan setiap akun dapat menjadi anggota hanya satu OU. Untuk informasi lebih lanjut, lihat Terminologi dan konsep (AWS Organizationsdokumentasi).

Kebijakan kontrol layanan (SCP) menentukan layanan dan tindakan yang dapat digunakan pengguna dan peran. SCP mirip dengan kebijakan izin AWS Identity and Access Management (IAM) kecuali bahwa mereka tidak memberikan izin. Sebagai gantinya, SCP menentukan izin maksimum. Ketika Anda melampirkan kebijakan ke salah satu node dalam hierarki, itu berlaku untuk semua OU dan akun dalam node tersebut. Misalnya, jika Anda menerapkan kebijakan ke root, itu berlaku untuk semua OU dan akun di organisasi, dan jika Anda menerapkan kebijakan ke OU, itu hanya berlaku untuk OU dan akun di OU target.

Anda dapat menggunakan AWS Organizations konsol untuk melihat dan mengelola semua akun Anda secara terpusat dalam suatu organisasi. Salah satu manfaat menggunakan organisasi adalah Anda dapat menerima tagihan konsolidasi yang menunjukkan semua biaya yang terkait dengan akun manajemen dan anggota. Untuk informasi selengkapnya, lihat Penagihan konsolidasi (AWS Organizationsdokumentasi).

Praktik terbaik

- Jangan gunakan yang sudah ada Akun AWS untuk membuat organisasi. Mulailah dengan akun baru, yang menjadi akun manajemen Anda untuk organisasi. Operasi istimewa dapat dilakukan dalam akun manajemen organisasi, dan SCP tidak berlaku untuk akun manajemen. Itu sebabnya Anda harus membatasi sumber daya cloud dan data yang terkandung dalam akun manajemen hanya untuk yang harus dikelola di akun manajemen.
- Batasi akses ke akun manajemen hanya untuk individu-individu yang perlu menyediakan yang baru Akun AWS dan untuk mengelola organisasi.
- Gunakan SCP untuk menentukan izin maksimum untuk root, unit organisasi, dan akun anggota. SCP tidak dapat langsung diterapkan ke akun manajemen.
- Patuhi Praktik terbaik untuk AWS Organizations (AWS Organizationsdokumentasi).

Buat landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang merupakan titik awal dari mana Anda dapat menyebarkan beban kerja dan aplikasi. Ini memberikan dasar untuk memulai dengan arsitektur multi-akun, identitas dan manajemen akses, tata kelola, keamanan data, desain jaringan, dan logging. AWS Control Toweradalah layanan yang menyederhanakan pemeliharaan dan tata kelola lingkungan multi-akun dengan menyediakan pagar pembatas otomatis. Biasanya, Anda menyediakan satu AWS Control Tower landing zone yang mengelola lingkungan Anda di semuaWilayah AWS. AWS Control Towerbekerja dengan mengatur orang lain Layanan AWS dalam akun Anda. Untuk informasi selengkapnya, lihat Apa yang terjadi saat Anda menyiapkan landing zone (AWS Control Towerdokumentasi).

Saat menyiapkan landing zoneAWS Control Tower, Anda mengidentifikasi tiga akun bersama: akun manajemen, akun arsip log, dan akun audit. Untuk informasi selengkapnya, lihat Apa itu akun bersama (AWS Control Towerdokumentasi). Untuk akun manajemen, Anda harus menggunakan akun yang sudah ada yang tidak menghosting beban kerja apa pun untuk mengatur landing zone. Untuk arsip log dan akun audit, Anda dapat memilih untuk menggunakan kembali yang sudah adaAkun AWS, atau AWS Control Tower dapat membuatnya untuk Anda.

Untuk petunjuk tentang cara mengatur AWS Control Tower landing zone, lihat Memulai (AWS Control Towerdokumentasi).

Praktik terbaik

- Patuhi praktik terbaik dalam prinsip-prinsip Desain untuk strategi multi-akun Anda (AWSWhitepaper).
- Patuhi Praktik terbaik untuk AWS Control Tower administrator (AWS Control Towerdokumentasi).
- Buat landing zone Anda di tempat Wilayah AWS yang menampung sebagian besar beban kerja Anda.

> **Important**
>
> Jika Anda memutuskan untuk mengubah Wilayah ini setelah menerapkan landing zone Anda, Anda memerlukan bantuanAWS Support, dan Anda harus menonaktifkan landing zone. Praktek ini tidak dianjurkan.

- Saat menentukan Wilayah mana yang AWS Control Tower akan diatur, pilih hanya Wilayah yang Anda harapkan untuk segera menerapkan beban kerja. Anda dapat mengubah Wilayah ini atau

menambahkan lebih banyak lagi nanti. Jika AWS Control Tower memerintah suatu Wilayah, ia akan mengerahkan pagar pembatas detektifnya ke Wilayah itu sebagai. Aturan AWS Config

- Setelah menentukan Wilayah mana yang AWS Control Tower akan memerintah, tolak akses ke semua Wilayah yang tidak diatur. Ini membantu memastikan bahwa beban kerja dan pengembang Anda hanya dapat menggunakan disetujuiWilayah AWS. Ini diimplementasikan sebagai kebijakan kontrol layanan (SCP) dalam organisasi. Untuk informasi selengkapnya, lihat Wilayah AWSMengonfigurasi kontrol penolakan (AWS Control Towerdokumentasi).
- Saat menyiapkan landing zone diAWS Control Tower, kami sarankan Anda mengganti nama OU dan akun berikut:
  - Kami menyarankan Anda mengganti nama Security OU menjadi Security_Prod untuk menandakan bahwa OU ini akan digunakan untuk keamanan produksi terkait. Akun AWS
  - Kami menyarankan Anda mengizinkan AWS Control Tower untuk membuat OU tambahan dan kemudian mengganti namanya dari Sandbox ke Workloads. Di bagian berikutnya, Anda membuat OU tambahan dalam Workloads OU, yang Anda gunakan untuk mengatur. Akun AWS
  - Kami menyarankan Anda mengganti nama logging terpusat Akun AWS dari Log Archive menjadi. log-archive-prod
  - Kami menyarankan Anda mengganti nama akun audit dari Audit menjadi security-tooling-prod.
- Untuk membantu mencegah penipuan, AWS diperlukan yang Akun AWS memiliki riwayat penggunaan sebelum dapat ditambahkan ke AWS Control Tower landing zone. Jika Anda menggunakan yang baru Akun AWS tanpa riwayat penggunaan apa pun, di akun baru, Anda dapat meluncurkan instans Amazon Elastic Compute Cloud (Amazon EC2) yang tidak ada di Tingkat Gratis. AWS Biarkan instance berjalan selama beberapa menit dan kemudian hentikan.

Tambahkan unit organisasi

Menetapkan struktur organisasi yang tepat sangat penting untuk menyiapkan lingkungan multi-akun. Karena Anda menggunakan kebijakan kontrol layanan (SCP) untuk menentukan izin maksimum untuk OU dan akun di dalamnya, struktur organisasi Anda harus logis dari perspektif manajemen, izin, dan pelaporan keuangan. Untuk informasi lebih lanjut tentang struktur organisasi, termasuk unit organisasi (OU), lihat Terminologi dan konsep (AWS Organizationsdokumentasi).

Di bagian ini, Anda menyesuaikan landing zone dengan membuat OU bersarang yang membantu Anda mengelompokkan dan menyusun lingkungan Anda, seperti produksi dan non-produksi. Praktik terbaik yang direkomendasikan ini dirancang untuk mengelompokkan landing zone Anda untuk

memisahkan sumber daya produksi dan non-produksi serta memisahkan infrastruktur dari beban kerja.

Untuk informasi selengkapnya tentang cara membuat OU, lihat Mengelola unit organisasi (AWS Organizationsdokumentasi).

Praktik terbaik

- Dalam Workloads OU yang Anda buatBuat landing zone, buat OU bersarang berikut:
  - Prod - Gunakan OU ini untuk Akun AWS menyimpan dan mengakses data produksi, termasuk data pelanggan.
  - NonProd— Gunakan OU ini untuk Akun AWS menyimpan data non-produksi, seperti lingkungan pengembangan, pementasan, atau pengujian

Di bawah root organisasi, buat Infrastructure_Prod OU. Gunakan OU ini untuk meng-host akun jaringan terpusat.

Tambahkan pengguna awal

Ada dua cara untuk memberi orang akses keAkun AWS:

- Identitas IAM, seperti pengguna, grup, dan peran
- Federasi identitas, seperti dengan menggunakan AWS IAM Identity Center

Di perusahaan yang lebih kecil dan lingkungan akun tunggal, adalah umum bagi administrator untuk membuat pengguna IAM ketika orang baru bergabung dengan perusahaan. Kunci akses dan kredenal kunci rahasia yang terkait dengan pengguna IAM dikenal sebagai kredensi jangka panjang karena tidak kedaluwarsa. Namun, ini bukan praktik terbaik keamanan yang direkomendasikan karena jika penyerang mengkompromikan kredensil tersebut, Anda harus menghasilkan satu set kredensil baru untuk pengguna. Pendekatan lain untuk mengakses Akun AWS adalah melalui peran IAM. Anda juga dapat menggunakan AWS Security Token Service(AWS STS) untuk meminta sementara kredensi jangka pendek, yang kedaluwarsa setelah jangka waktu yang dapat dikonfigurasi.

Anda dapat mengelola akses orang ke Anda Akun AWS melalui IAM Identity Center. Anda dapat membuat akun pengguna individual untuk setiap karyawan atau kontraktor Anda, mereka dapat

mengelola kata sandi dan solusi otentikasi multi-faktor (MFA) mereka sendiri, dan Anda dapat mengelompokkannya untuk mengelola akses. Saat mengonfigurasi MFA, Anda dapat menggunakan token perangkat lunak, seperti aplikasi autentikator, atau Anda dapat menggunakan token perangkat keras, seperti perangkat. YubiKey

IAM Identity Center juga mendukung federasi dari penyedia identitas eksternal (IdPs) seperti Okta, JumpCloud, dan Ping Identity. Untuk informasi selengkapnya, lihat Penyedia identitas yang didukung (dokumentasi Pusat Identitas IAM). Dengan berfederasi dengan iDP eksternal, Anda dapat mengelola otentikasi pengguna di seluruh aplikasi dan kemudian menggunakan IAM Identity Center untuk mengotorisasi akses ke spesifik. Akun AWS

Praktik terbaik

- Patuhi praktik terbaik Keamanan (dokumentasi IAM) untuk mengonfigurasi akses pengguna.
- Kelola akses akun berdasarkan grup, bukan oleh pengguna individu. Di IAM Identity Center, buat grup baru yang mewakili setiap fungsi bisnis Anda. Misalnya, Anda dapat membuat grup untuk teknik, keuangan, penjualan, dan manajemen produk.
- Seringkali, grup didefinisikan dengan memisahkan mereka yang membutuhkan akses ke semua Akun AWS (seringkali akses hanya-baca) dan mereka yang membutuhkan akses ke satu. Akun AWS Kami menyarankan Anda menggunakan konvensi penamaan berikut untuk grup sehingga mudah untuk mengidentifikasi Akun AWS dan izin yang terkait dengan grup.

  `<prefix>-<account name>-<permission set>`
- Misalnya, untuk grup`AWS-A-dev-nonprod-DeveloperAccess`, `AWS-A` adalah awalan yang menunjukkan akses ke satu akun, `dev-nonprod` adalah nama akun, dan `DeveloperAccess` merupakan set izin yang ditetapkan ke grup. Untuk grup`AWS-O-BillingAccess`, `AWS-O` awalan menunjukkan akses ke seluruh organisasi, dan `BillingAccess` menunjukkan izin yang ditetapkan untuk grup. Dalam contoh ini, karena grup memiliki akses ke seluruh organisasi, nama akun tidak direpresentasikan dalam nama grup.
- Jika Anda menggunakan IAM Identity Center dengan IDP berbasis SAML eksternal dan ingin meminta MFA, Anda dapat menggunakan kontrol akses berbasis atribut (ABAC) untuk meneruskan metode otentikasi dari IDP ke IAM Identity Center. Atribut dikirim melalui pernyataan SAMP. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses (dokumentasi Pusat Identitas IAM).

  Banyak IdPs, seperti Microsoft Azure Active Directory dan Okta, dapat menggunakan klaim Authentication Method Reference (`amr`) di dalam pernyataan SAMP untuk meneruskan status

MFA pengguna ke IAM Identity Center. Klaim yang digunakan untuk menegaskan status MFA dan formatnya bervariasi menurut IDP. Untuk informasi selengkapnya, lihat dokumentasi untuk IDP Anda.

Di Pusat Identitas IAM, Anda kemudian dapat membuat kebijakan set izin yang menentukan siapa yang dapat mengakses AWS sumber daya Anda. Saat Anda mengaktifkan ABAC dan menentukan atribut, Pusat Identitas IAM meneruskan nilai atribut pengguna yang diautentikasi ke IAM untuk digunakan dalam evaluasi kebijakan. Untuk informasi selengkapnya, lihat Membuat kebijakan izin untuk ABAC (dokumentasi Pusat Identitas IAM). Seperti yang ditunjukkan pada contoh berikut, Anda menggunakan tombol `aws:PrincipalTag` kondisi untuk membuat aturan kontrol akses untuk MFA.

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Kelola akun anggota

Di bagian ini, Anda mengundang akun yang sudah ada sebelumnya ke organisasi dan Anda mulai membuat akun baru dalam organisasi Anda. Bagian penting dari proses ini adalah mendefinisikan kriteria yang Anda gunakan untuk menentukan apakah Anda perlu menyediakan akun baru.

Bagian ini terdiri dari tugas-tugas berikut:

- Undang akun Anda yang sudah ada sebelumnya
- Sesuaikan pengaturan VPC di AWS Control Tower
- Tentukan kriteria pelingkupan

Undang akun Anda yang sudah ada sebelumnya

Di dalamnyaAWS Organizations, Anda dapat mengundang akun perusahaan Anda yang sudah ada sebelumnya ke organisasi baru Anda. Hanya akun manajemen di organisasi yang dapat mengundang akun lain untuk bergabung. Ketika administrator akun yang diundang menerima, akun segera bergabung dengan organisasi, dan akun manajemen organisasi menjadi bertanggung jawab atas semua biaya yang timbul oleh akun anggota baru. Untuk informasi selengkapnya, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda dan Menerima atau menolak undangan dari organisasi (AWS Organizationsdokumentasi).

> **Note**
>
> Anda dapat mengundang akun untuk bergabung dengan organisasi hanya jika akun tersebut saat ini tidak berada di organisasi lain. Jika akun tersebut adalah anggota organisasi yang ada, Anda harus menghapusnya dari organisasi. Jika akun tersebut adalah akun manajemen untuk organisasi lain yang dibuat karena kesalahan, Anda harus menghapus organisasi.

> **Important**
>
> Jika Anda memerlukan akses ke informasi biaya atau penggunaan historis dari akun yang sudah ada sebelumnya, Anda dapat menggunakannya AWS Cost and Usage Report untuk mengekspor informasi tersebut ke bucket Amazon Simple Storage Service (Amazon S3). Lakukan ini sebelum menerima undangan untuk bergabung dengan organisasi. Saat akun bergabung dengan organisasi, Anda kehilangan akses ke data historis ini untuk akun tersebut. Untuk informasi selengkapnya, lihat Menyiapkan bucket Amazon S3 untuk Laporan Biaya dan Penggunaan (AWS Cost and Usage Reportdokumentasi).

Praktik terbaik

- Kami menyarankan Anda menambahkan akun yang sudah ada sebelumnya, yang kemungkinan berisi beban kerja produksi, ke unit organisasi Beban Kerja > Prod yang Anda buat. Tambahkan unit organisasi
- Secara default, akun manajemen organisasi tidak memiliki akses administratif atas akun anggota yang diundang ke organisasi. Jika Anda ingin akun manajemen memiliki kontrol administratif, Anda harus membuat peran OrganizationAccountAccessRoleIAM di akun anggota dan memberikan izin ke akun manajemen untuk mengambil peran tersebut. Untuk informasi selengkapnya, lihat Membuat akun anggota yang diundang (AWS Organizationsdokumentasi). OrganizationAccountAccessRole
- Untuk akun yang sudah ada sebelumnya yang Anda undang ke organisasi, tinjau Praktik terbaik untuk akun anggota (AWS Organizationsdokumentasi) dan konfirmasikan bahwa akun tersebut mematuhi rekomendasi ini.

Sesuaikan pengaturan VPC di AWS Control Tower

Kami menyarankan Anda untuk menyediakan yang baru Akun AWS melalui Account Factory diAWS Control Tower. Dengan menggunakan Account Factory, Anda dapat menggunakan AWS Control Tower integrasi dengan Amazon EventBridge untuk menyediakan sumber daya baru Akun AWS segera setelah akun dibuat.

Saat Anda menyiapkan yang baruAkun AWS, virtual private cloud (VPC) default secara otomatis disediakan. Namun, ketika Anda menyiapkan akun baru melalui Account Factory, AWS Control Tower secara otomatis memberikan VPC tambahan. Untuk informasi selengkapnya, lihat Ikhtisar AWS Control Tower dan VPC (AWS Control Towerdokumentasi). Ini berarti bahwa, secara default, AWS Control Tower menyediakan dua VPC default di setiap akun baru.

Adalah umum bagi perusahaan untuk menginginkan kontrol lebih besar atas VPC dalam akun mereka. Banyak yang lebih suka menggunakan layanan lain, sepertiAWS CloudFormation, Hashicorp Terraform, atau Pulumi, untuk mengatur dan mengelola VPC mereka. Anda harus menyesuaikan pengaturan Account Factory untuk mencegah pembuatan VPC tambahan yang disediakan oleh. AWS Control Tower Untuk petunjuknya, lihat Mengonfigurasi setelan Amazon VPC (AWS Control Towerdokumentasi), dan menerapkan setelan berikut:

1. Nonaktifkan opsi subnet yang dapat diakses Internet.
2. Dalam jumlah maksimum subnet pribadi, pilih 0.
3. Di Wilayah untuk pembuatan VPC, hapus semua Wilayah.
4. Di Availability Zones, pilih 3.

Praktik terbaik

- Hapus VPC default yang secara otomatis disediakan di setiap akun baru. Ini mencegah pengguna meluncurkan instans EC2 publik di akun tanpa secara eksplisit membuat VPC khusus. Untuk informasi selengkapnya, lihat Menghapus subnet default dan VPC default (dokumentasi Amazon Virtual Private Cloud). Anda juga dapat mengonfigurasi AWS Control TowerAccount Factory for Terraform (AFT) untuk secara otomatis menghapus VPC default di akun yang baru dibuat.
- Menyediakan yang baru Akun AWS disebut dev-nonprod ke dalam Workloads > unit organisasi. NonProd Gunakan akun ini untuk lingkungan pengembangan Anda. Untuk petunjuk, lihat Menyediakan akun Account Factory dengan AWS Service Catalog (AWS Control Towerdokumentasi).

Tentukan kriteria pelingkupan

Anda perlu memilih kriteria yang akan digunakan perusahaan Anda ketika memutuskan apakah akan menyediakan yang baruAkun AWS. Anda mungkin memutuskan untuk menyediakan akun untuk setiap unit bisnis, atau Anda mungkin memutuskan untuk menyediakan akun berdasarkan lingkungan, seperti produksi, pengujian, atau QA. Setiap perusahaan memiliki persyaratan sendiri untuk seberapa besar atau kecil mereka Akun AWS seharusnya. Umumnya, Anda mengevaluasi tiga faktor berikut saat memutuskan cara mengukur akun Anda:

- Kuota layanan penyeimbangan — Kuota layanan adalah nilai maksimum untuk jumlah sumber daya, tindakan, dan item untuk masing-masing Layanan AWS dalam file. Akun AWS Jika banyak beban kerja berbagi akun yang sama dan satu beban kerja menghabiskan sebagian besar atau seluruh kuota layanan, itu mungkin berdampak negatif pada beban kerja lain di akun yang sama. Jika demikian, Anda mungkin perlu memisahkan beban kerja tersebut ke dalam akun yang berbeda. Untuk informasi selengkapnya, lihat Layanan AWSkuota (Referensi Umum AWS).
- Pelaporan biaya - Mengisolasi beban kerja ke dalam akun terpisah memungkinkan Anda melihat biaya pada tingkat akun dalam laporan biaya dan penggunaan. Saat menggunakan akun yang sama untuk beberapa beban kerja, Anda dapat menggunakan tag untuk membantu mengelola dan mengidentifikasi sumber daya. Untuk informasi selengkapnya tentang penandaan, lihat Menandai AWS resource ()Referensi Umum AWS.
- Mengontrol akses - Saat beban kerja berbagi akun, Anda perlu mempertimbangkan cara mengonfigurasi kebijakan IAM untuk membatasi akses ke sumber daya akun sehingga pengguna tidak memiliki akses ke beban kerja yang tidak mereka butuhkan. Sebagai alternatif, Anda dapat menggunakan beberapa akun dan set izin di Pusat Identitas IAM untuk mengelola akses ke akun individual.

Praktik terbaik

- Patuhi praktik terbaik dalam strategi AWS multi-akun untuk AWS Control Tower landing zone Anda (AWS Control Towerdokumentasi).
- Tetapkan strategi penandaan yang efektif yang membantu Anda mengidentifikasi dan mengelola AWS sumber daya. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, unit bisnis, lingkungan, atau kriteria lainnya. Untuk informasi selengkapnya, lihat Praktik terbaik untuk penandaan (Referensi Umum AWSdokumentasi).
- Jangan membebani akun dengan terlalu banyak beban kerja. Jika permintaan beban kerja melebihi kuota layanan, ini dapat menyebabkan masalah kinerja. Anda dapat memisahkan beban kerja yang

bersaing menjadi berbeda Akun AWS atau Anda dapat meminta peningkatan kuota layanan. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota (Dokumentasi Service Quotas).

Mengelola izin dan akses untuk arsitektur multi-akun

Bagian ini terdiri dari topik-topik berikut:

- Pertimbangan budaya rekayasa
- Membuat set izin
- Membuat batas izin
- Mengelola izin untuk individu

Pertimbangan budaya rekayasa

Salah satu pilar dari AWS Well-Architected Framework adalah Operational Excellence. Tim harus memahami model operasi dan peran mereka dalam mencapai hasil bisnis Anda. Tim dapat fokus pada pencapaian tujuan bersama ketika mereka memahami tanggung jawab mereka, dapat mengambil kepemilikan, dan mengetahui bagaimana keputusan dibuat.

Dengan perusahaan tahap awal yang membangun dengan cepat, semua orang di tim melakukan banyak peran. Tidak jarang bagi pengguna ini untuk memiliki akses yang sangat istimewa ke keseluruhan. Akun AWS Seiring pertumbuhan perusahaan, mereka sering ingin mengikuti prinsip hak istimewa paling sedikit dan hanya memberikan izin yang diperlukan bagi pengguna untuk melakukan pekerjaan mereka. Untuk membantu Anda membatasi cakupan, Anda dapat menggunakan AWS Identity and Access Management Access Analyzeruntuk melihat izin apa yang sebenarnya digunakan oleh pengguna atau peran IAM, sehingga Anda dapat menghapus izin berlebih.

Mungkin sulit untuk memutuskan siapa di perusahaan Anda yang memiliki izin untuk membuat peran IAM. Ini biasanya merupakan vektor untuk meningkatkan hak istimewa. Meningkatnya hak istimewa adalah ketika pengguna dapat memperluas izin atau cakupan akses mereka sendiri. Misalnya, jika pengguna memiliki izin terbatas tetapi dapat membuat peran IAM baru, pengguna tersebut dapat meningkatkan hak istimewa mereka dengan membuat dan mengasumsikan peran IAM baru yang menerapkan kebijakan terkelola. `AdministratorAccess`

Beberapa perusahaan membatasi penyediaan peran IAM ke tim individu tepercaya yang terpusat. Kelemahan dari pendekatan ini adalah bahwa tim ini dapat dengan cepat menjadi hambatan karena hampir semua Layanan AWS memerlukan peran IAM untuk beroperasi. Sebagai alternatif, Anda dapat menggunakan batas izin untuk mendelegasikan akses IAM hanya kepada pengguna yang mengembangkan, menguji, meluncurkan, dan mengelola infrastruktur cloud Anda. Misalnya kebijakan, lihat Contoh Batas Izin (GitHub).

Tim operasi pengembangan (DevOps), juga dikenal sebagai tim platform, sering perlu menyeimbangkan kemampuan layanan mandiri untuk beberapa tim pengembangan internal terhadap stabilitas operasional aplikasi. Membina budaya teknik yang mencakup otonomi, penguasaan, dan tujuan di tempat kerja dapat membantu memotivasi tim. Insinyur ingin melakukan pekerjaan mereka dengan cara yang diarahkan sendiri, tanpa bergantung pada orang lain untuk melakukan sesuatu untuk mereka. Jika DevOps tim dapat menerapkan solusi swalayan, ini juga mengurangi jumlah waktu orang lain bergantung pada mereka untuk menyelesaikan sesuatu.

Membuat set izin

Anda dapat mengelola Akun AWS akses dengan menggunakan set izin diAWS IAM Identity Center. Kumpulan izin adalah templat yang membantu Anda menerapkan satu atau beberapa kebijakan IAM ke beberapa. Akun AWS Saat Anda menetapkan izin yang disetel keAkun AWS, Pusat Identitas IAM akan membuat peran IAM dan melampirkan kebijakan IAM Anda ke peran tersebut. Untuk informasi selengkapnya, lihat Membuat dan mengelola set izin (dokumentasi Pusat Identitas IAM).

AWSmerekomendasikan membuat set izin yang memetakan ke persona yang berbeda dalam bisnis Anda.

Misalnya, Anda dapat membuat set izin berikut:

- Izin penagihan ditetapkan
- Set izin pengembang
- Set izin produksi

Set izin berikut adalah cuplikan dari template. AWS CloudFormation Anda harus menggunakan kode ini sebagai titik awal dan menyesuaikannya untuk bisnis Anda. Untuk informasi selengkapnya tentang CloudFormation templat, lihat Pelajari dasar-dasar templat (CloudFormation dokumentasi).

Izin penagihan ditetapkan

Tim keuangan menggunakan BillingAccessPermissionSetuntuk melihat dasbor AWS Billing konsol dan AWS Cost Explorer di setiap akun.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
```

```
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

Set izin pengembang

Tim teknik menggunakan DeveloperAccessPermissionSetuntuk mengakses akun non-produksi.

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
```

```
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

Set izin produksi

Tim teknik menggunakan ProductionPermissionSetuntuk mengakses akun produksi. Set izin ini memiliki akses terbatas hanya lihat.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
```

```
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

Membuat batas izin

Setelah Anda menerapkan set izin, Anda menetapkan batas izin. Batas izin ini adalah mekanisme untuk mendelegasikan akses IAM hanya kepada pengguna yang mengembangkan, menguji, meluncurkan, dan mengelola infrastruktur cloud Anda. Pengguna tersebut hanya dapat melakukan tindakan yang diizinkan oleh kebijakan dan batas izin.

Anda dapat menentukan batas izin dalam AWS CloudFormation template dan kemudian menggunakan CloudFormation StackSets untuk menyebarkan template ke beberapa akun. Ini membantu Anda menetapkan dan memelihara kebijakan standar di seluruh organisasi Anda dengan satu operasi. Untuk informasi dan petunjuk selengkapnya, lihat Bekerja dengan AWS CloudFormation StackSets (CloudFormation dokumentasi).

CloudFormation Template berikut menyediakan peran IAM dan membuat kebijakan IAM yang bertindak sebagai batas izin. Dengan menggunakan kumpulan tumpukan, Anda dapat menerapkan template ini ke semua akun anggota di organisasi Anda.

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
```

```
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
        - Sid: OverlyPermissiveAllowedServices
          Effect: Allow
          Action:
            - "lambda:*"
            - "apigateway:*"
            - "events:*"
            - "s3:*"
            - "logs:*"
```

```
            Resource: "*"
```

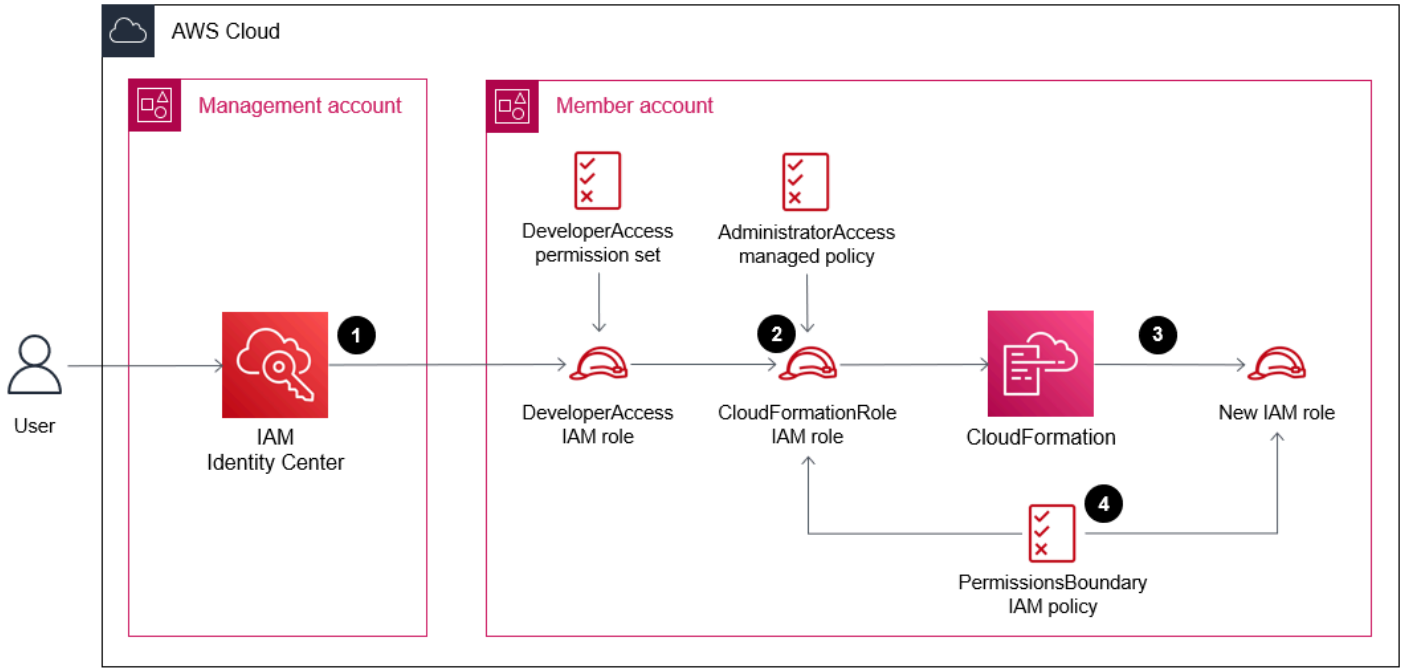
CloudFormationRolePeran, PermissionsBoundarykebijakan, dan set DeveloperAccessizin bekerja sama untuk memberikan izin berikut:

- Pengguna memiliki akses hanya-baca ke sebagian besarLayanan AWS, melalui kebijakan ReadOnlyAccessAWSterkelola.
- Pengguna memiliki akses ke kasus dukungan terbuka, melalui kebijakan AWSSupportAccessAWSterkelola.
- Pengguna memiliki akses hanya-baca ke dasbor AWS Billing konsol, melalui kebijakan AWSBillingReadOnlyAccessAWSterkelola.
- Pengguna dapat menyediakan lingkungan baru dariAWS Proton, melalui kebijakan AWSProtonDeveloperAccessAWSterkelola.
- Pengguna dapat menyediakan produk dari Service Catalog, melalui kebijakan yang AWSServiceCatalogEndUserFullAccessAWSdikelola.
- Pengguna dapat memvalidasi dan memperkirakan biaya CloudFormation template apa pun, melalui kebijakan inline.
- Dengan menggunakan peran CloudFormationRoleIAM, pengguna dapat membuat, memperbarui, atau menghapus CloudFormation tumpukan apa pun yang dimulai dengan app/.
- Pengguna dapat menggunakan CloudFormation untuk membuat, memperbarui, atau menghapus peran IAM yang dimulai dengan app/. Kebijakan PermissionsBoundaryIAM mencegah pengguna meningkatkan hak istimewa mereka.
- Pengguna dapat menyediakan sumber daya Amazon AWS Lambda EventBridge, Amazon CloudWatch, Amazon Simple Storage Service (Amazon S3), dan Amazon API Gateway hanya dengan menggunakan. CloudFormation

Gambar berikut menunjukkan bagaimana pengguna yang berwenang, seperti pengembang, dapat membuat peran IAM baru di akun anggota dengan menggunakan set izin, peran IAM, dan batas izin yang dijelaskan dalam panduan ini:

1. Pengguna mengautentikasi di IAM Identity Center dan mengasumsikan peran IAM. DeveloperAccess
2. Pengguna memulai `cloudformation:CreateStack` tindakan dan mengasumsikan peran CloudFormationRoleIAM.

3. Pengguna memulai `iam:CreateRole` tindakan dan menggunakan CloudFormation untuk membuat peran IAM baru.
4. Kebijakan PermissionsBoundaryIAM diterapkan pada peran IAM yang baru.



CloudFormationRolePeran tersebut memiliki kebijakan AdministratorAccessterkelola yang dilampirkan, tetapi karena kebijakan PermissionsBoundaryIAM, izin efektif CloudFormationRoleperan menjadi sama dengan kebijakan. PermissionsBoundary PermissionsBoundaryKebijakan mereferensikan dirinya sendiri saat mengizinkan `iam:CreateRole` tindakan, yang memastikan bahwa peran hanya dapat dibuat jika batas izin diterapkan.

Mengelola izin untuk individu

Dengan menggunakan set izin, batas izin, dan peran CloudFormationRoleIAM, Anda dapat membatasi jumlah izin yang perlu Anda tetapkan langsung ke masing-masing kepala sekolah. Ini membantu Anda mengelola akses saat perusahaan Anda tumbuh dan membantu Anda menerapkan praktik terbaik keamanan untuk memberikan hak istimewa paling sedikit.

Anda juga dapat menggunakan peran terkait layanan, yang memberikan izin ke AWS layanan untuk menyediakan sumber daya atas nama Anda. Alih-alih memberikan izin kepada prinsipal IAM (pengguna, grup pengguna, atau peran), Anda dapat memberikan izin ke layanan. Misalnya, peran terkait layanan untuk AWS Protondan AWS Service Catalogmemungkinkan Anda menyediakan

templat, sumber daya, dan lingkungan Anda sendiri, tanpa menetapkan izin ke prinsipal IAM. Untuk informasi selengkapnya, lihat Layanan AWSyang bekerja dengan IAM dan Menggunakan peran terkait layanan (dokumentasi IAM).

Praktik terbaik lainnya adalah membatasi jumlah akses yang dimiliki individu keAWS Management Console. Dengan membatasi akses ke konsol, Anda dapat meminta individu untuk menyediakan sumber daya dengan menggunakan teknologi infrastruktur sebagai kode (IAc), seperti, HashiCorp Terraform AWS CloudFormation, atau Pulumi. Mengelola infrastruktur melalui IAc Anda untuk melacak perubahan sumber daya dari waktu ke waktu dan memperkenalkan mekanisme untuk menyetujui perubahan, seperti permintaan GitHub tarik.

Konektivitas jaringan untuk arsitektur multi-akun

Menghubungkan VPC

Banyak perusahaan menggunakan VPC peering di Amazon Virtual Private Cloud (Amazon VPC) untuk menghubungkan pengembangan dan produksi VPC. Menggunakan koneksi peering VPC, Anda dapat merutekan lalu lintas antara dua VPC dengan menggunakan alamat IP pribadi. VPC yang terhubung dapat berbeda Akun AWS dan berbeda Wilayah AWS. Untuk informasi selengkapnya, lihat Apa itu peering VPC (dokumentasi Amazon VPC). Seiring pertumbuhan perusahaan dan jumlah VPC meningkat, menjaga koneksi peering antara semua VPC dapat menjadi beban pemeliharaan. Anda mungkin juga dibatasi oleh jumlah maksimum koneksi peering VPC per VPC. Untuk informasi selengkapnya, lihat kuota koneksi peering VPC (dokumentasi Amazon VPC).

Jika Anda memiliki beberapa lingkungan pengembangan, pengujian, dan pementasan yang meng-host data non-produksi di beberapa Akun AWS, Anda mungkin ingin menyediakan konektivitas jaringan di antara semua VPC tersebut tetapi tidak mengizinkan akses apa pun ke lingkungan produksi. Anda dapat menggunakan AWS Transit Gatewayuntuk menghubungkan beberapa VPC di beberapa akun. Anda dapat memisahkan tabel rute untuk mencegah pengembangan VPC berkomunikasi ke VPC produksi melalui gateway transit, yang bertindak sebagai router terpusat. Untuk informasi selengkapnya, lihat Router terpusat (dokumentasi Transit Gateway).

Transit Gateway juga mendukung peering dengan gateway transit lainnya, termasuk yang berbeda atau. Akun AWS Wilayah AWS Karena Transit Gateway adalah layanan yang dikelola sepenuhnya dan sangat tersedia, Anda hanya perlu menyediakan satu gateway transit untuk setiap Wilayah.

Untuk informasi selengkapnya dan arsitektur jaringan terperinci, lihat Membangun Infrastruktur AWS Jaringan Multi-VPC (Whitepaper) yang Dapat Diskalakan dan Aman.AWS

Menghubungkan aplikasi

Jika Anda perlu menjalin komunikasi antar aplikasi di lingkungan yang berbeda Akun AWS (seperti produksi), Anda dapat menggunakan salah satu opsi berikut:

- VPC mengintip atau AWS Transit Gatewaydapat menyediakan konektivitas di tingkat jaringan jika Anda ingin membuka akses luas ke beberapa alamat IP dan port.
- AWS PrivateLinkmembuat titik akhir di subnet pribadi VPC, dan titik akhir ini terdaftar sebagai entri DNS di. Amazon Route 53 Resolver Dengan menggunakan DNS, aplikasi dapat menyelesaikan

titik akhir dan terhubung ke layanan terdaftar, tanpa memerlukan gateway NAT atau gateway internet di VPC.

- Amazon VPC Lattice mengaitkan layanan, seperti aplikasi, di beberapa akun dan VPC dan mengumpulkannya ke dalam jaringan layanan. Klien di VPC yang terkait dengan jaringan layanan dapat mengirim permintaan ke semua layanan lain yang terkait dengan jaringan layanan, terlepas dari apakah mereka berada di akun yang sama. VPC Lattice terintegrasi dengan AWS Resource Access Manager (AWS RAM) sehingga Anda dapat berbagi sumber daya dengan akun lain atau melalui. AWS Organizations Anda dapat mengaitkan VPC hanya dengan satu jaringan layanan. Solusi ini tidak memerlukan penggunaan VPC peering atau AWS Transit Gateway untuk berkomunikasi lintas akun.

Praktik terbaik untuk konektivitas jaringan

- Buat Akun AWS yang Anda gunakan untuk jaringan terpusat. Beri nama akun ini network-prod, dan gunakan untuk dan AWS Transit Gateway Amazon VPC IP Address Manager (IPAM). Tambahkan akun ini ke unit organisasi Infrastructure_Prod.
- Gunakan AWS Resource Access Manager(AWS RAM) untuk berbagi gateway transit, jaringan layanan VPC Lattice, dan kolam IPAM dengan seluruh organisasi. Ini memungkinkan siapa pun Akun AWS di dalam organisasi Anda untuk berinteraksi dengan layanan ini.
- Dengan menggunakan kolam IPAM untuk mengelola alokasi alamat IPv4 dan IPv6 secara terpusat, Anda dapat mengizinkan pengguna akhir Anda untuk menyediakan VPC sendiri dengan menggunakan. AWS Service Catalog Ini membantu Anda mengukur VPC dengan tepat dan mencegah spasi alamat IP yang tumpang tindih.
- Gunakan pendekatan jalan keluar terpusat untuk lalu lintas yang terikat ke internet, dan gunakan pendekatan masuk terdesentralisasi untuk lalu lintas yang masuk ke lingkungan Anda dari internet. Untuk informasi selengkapnya, lihat Jalan keluar terpusat dan Masuknya terdesentralisasi.

Jalan keluar terpusat

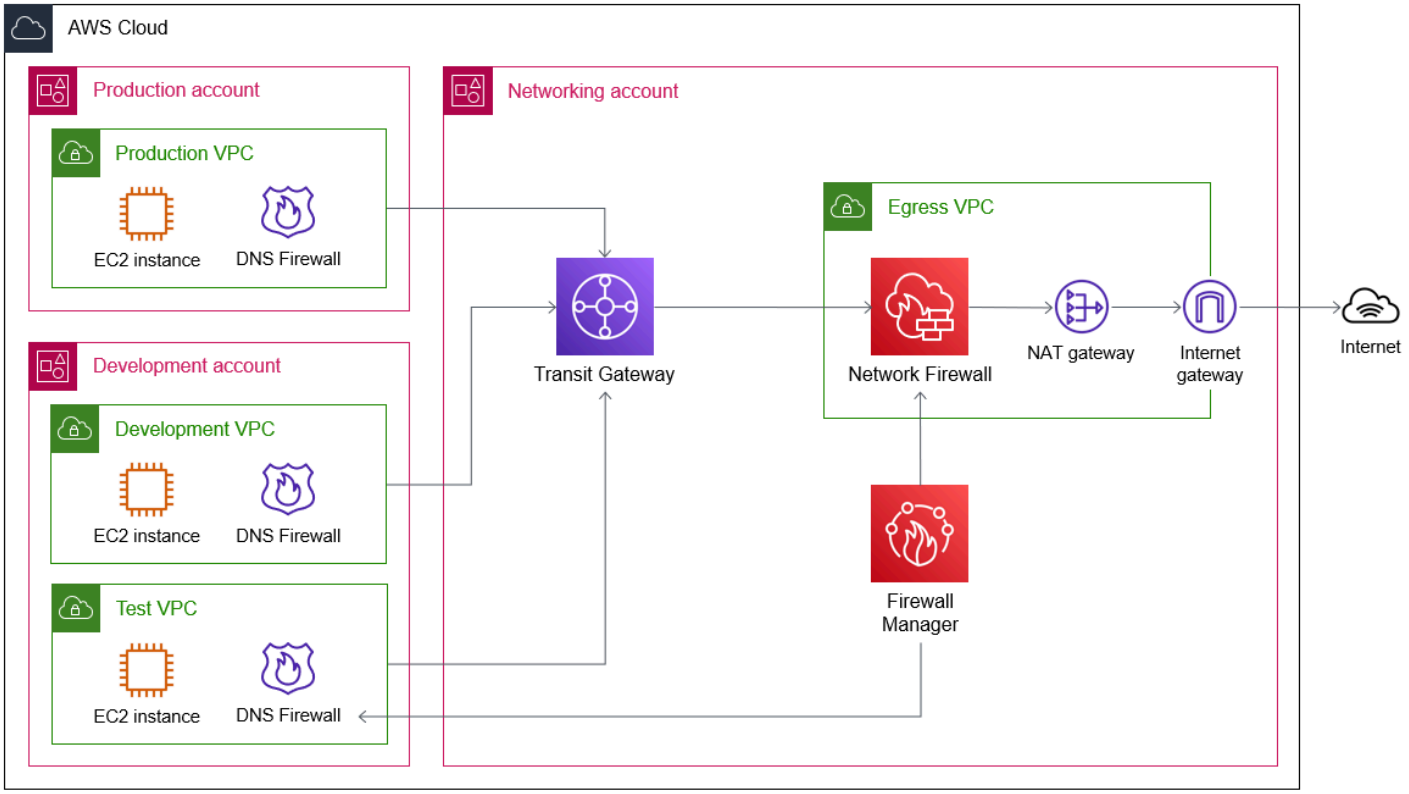
Jalan keluar terpusat adalah prinsip menggunakan satu titik inspeksi umum untuk semua lalu lintas jaringan yang ditujukan ke internet. Pada titik pemeriksaan ini, Anda dapat mengizinkan lalu lintas hanya ke domain tertentu atau hanya melalui port atau protokol tertentu. Memusatkan jalan keluar juga dapat membantu Anda mengurangi biaya dengan menghilangkan kebutuhan untuk menyebarkan gateway NAT di setiap VPC Anda untuk menjangkau internet. Ini bermanfaat dari perspektif keamanan karena membatasi paparan sumber daya berbahaya yang dapat diakses

secara eksternal, seperti infrastruktur perintah dan kontrol malware (C&C). Untuk informasi selengkapnya dan opsi arsitektur untuk jalan keluar terpusat, lihat Jalan keluar terpusat ke internet (Whitepaper).AWS

Anda dapat menggunakan AWS Network Firewall, yang merupakan firewall jaringan stateful, dikelola, dan layanan deteksi dan pencegahan intrusi, sebagai titik inspeksi pusat untuk lalu lintas jalan keluar. Anda mengatur firewall ini di VPC khusus untuk lalu lintas keluar. Network Firewall mendukung aturan stateful yang dapat Anda gunakan untuk membatasi akses internet ke domain tertentu. Untuk informasi selengkapnya, lihat Pemfilteran domain (dokumentasi Network Firewall).

Anda juga dapat menggunakan Amazon Route 53 Resolver DNS Firewall untuk membatasi lalu lintas keluar ke nama domain tertentu, terutama untuk mencegah eksfiltrasi data Anda yang tidak sah. Dalam aturan DNS Firewall, Anda dapat menerapkan daftar domain (dokumentasi Route 53), yang mengizinkan atau menolak akses ke domain tertentu. Anda dapat menggunakan daftar domain AWS terkelola, yang berisi nama domain yang terkait dengan aktivitas berbahaya atau potensi ancaman lainnya, atau Anda dapat membuat daftar domain khusus. Anda membuat grup aturan DNS Firewall dan kemudian menerapkannya ke VPC Anda. Permintaan DNS keluar rute melalui Resolver di VPC untuk resolusi nama domain, dan DNS Firewall memfilter permintaan berdasarkan grup aturan yang diterapkan ke VPC. Permintaan DNS rekursif yang masuk ke Resolver tidak mengalir melalui gateway transit dan jalur Network Firewall. Route 53 Resolver dan DNS Firewall harus dianggap sebagai jalur keluar terpisah dari VPC.

Gambar berikut menunjukkan contoh arsitektur untuk jalan keluar terpusat. Sebelum komunikasi jaringan dimulai, permintaan DNS dikirim ke Resolver Route 53, di mana firewall DNS memungkinkan atau menolak resolusi alamat IP yang digunakan untuk komunikasi. Lalu lintas yang ditujukan ke internet diarahkan ke gateway transit di akun jaringan terpusat. Gateway transit meneruskan lalu lintas ke Network Firewall untuk diperiksa. Jika kebijakan firewall mengizinkan lalu lintas keluar, lalu lintas rute melalui gateway NAT, melalui gateway internet, dan ke internet. Anda dapat menggunakannya AWS Firewall Manager untuk mengelola grup aturan DNS Firewall dan kebijakan Firewall Jaringan secara terpusat di seluruh infrastruktur multi-akun Anda.



Praktik terbaik untuk mengamankan lalu lintas jalan keluar

- Mulai dalam mode logging-only (dokumentasi Route 53). Ubah ke mode blokir setelah Anda memvalidasi bahwa lalu lintas yang sah tidak terpengaruh.
- Blokir lalu lintas DNS yang masuk ke internet dengan menggunakan AWS Firewall Manager kebijakan untuk daftar kontrol akses jaringan atau dengan menggunakan AWS Network Firewall. Semua kueri DNS harus dirutekan melalui Resolver Route 53, di mana Anda dapat memantaunya dengan Amazon GuardDuty (jika diaktifkan) dan memfilternya dengan Route 53 Resolver DNS Firewall (jika diaktifkan). Untuk informasi selengkapnya, lihat Menyelesaikan kueri DNS antara VPC dan jaringan Anda (dokumentasi Rute 53).
- Gunakan Daftar Domain AWS Terkelola (dokumentasi Route 53) di DNS Firewall dan Network Firewall.
- Pertimbangkan untuk memblokir domain tingkat atas yang berisiko tinggi dan tidak terpakai, seperti.info, .top, .xyz, atau beberapa domain kode negara.
- Pertimbangkan untuk memblokir port berisiko tinggi dan tidak terpakai, seperti port 1389, 4444, 3333, 445, 135, 139, atau 53.

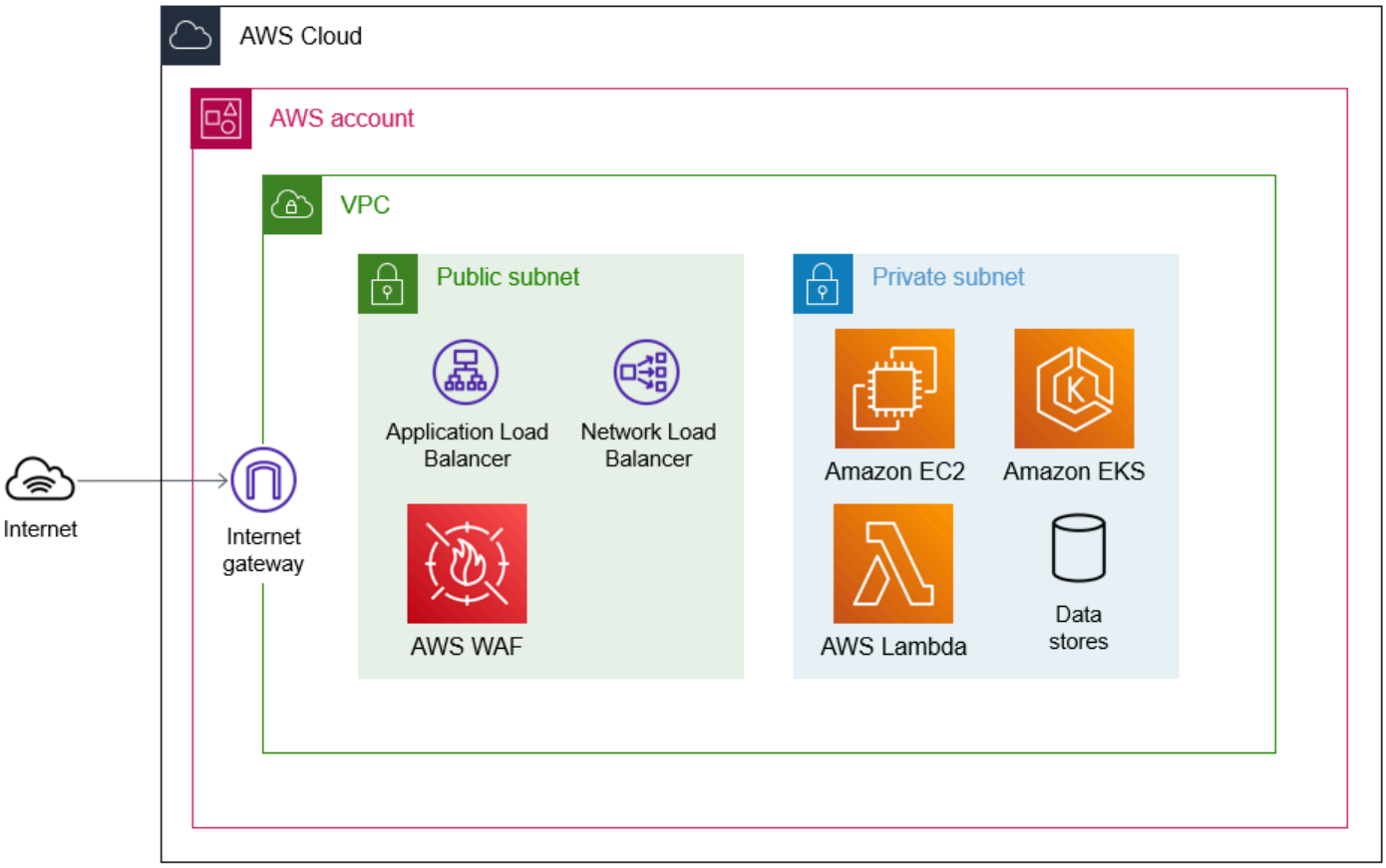
- Sebagai titik awal, Anda dapat menggunakan daftar tolak yang menyertakan aturan AWS terkelola. Anda kemudian dapat bekerja dari waktu ke waktu untuk menerapkan model daftar izin. Misalnya, alih-alih hanya menyertakan daftar ketat nama domain yang sepenuhnya memenuhi syarat dalam daftar izinkan, mulailah dengan menggunakan beberapa wildcard, seperti *.example.com. Anda bahkan dapat mengizinkan hanya domain tingkat atas yang Anda harapkan dan memblokir semua domain lainnya. Kemudian, seiring waktu, persempit juga.
- Gunakan Profil Route 53 (dokumentasi Rute 53) untuk menerapkan konfigurasi Route 53 terkait DNS di banyak VPC dan berbeda. Akun AWS
- Tentukan proses untuk menangani pengecualian terhadap praktik terbaik ini.

Masuknya terdesentralisasi

Ingress terdesentralisasi adalah prinsip mendefinisikan, pada tingkat akun individu, bagaimana lalu lintas dari internet mencapai beban kerja di akun itu. Dalam arsitektur multi-akun, salah satu manfaat dari ingress terdesentralisasi adalah bahwa setiap akun dapat menggunakan layanan ingress atau sumber daya yang paling tepat untuk beban kerjanya, seperti Application Load Balancer, Amazon API Gateway, atau Network Load Balancer.

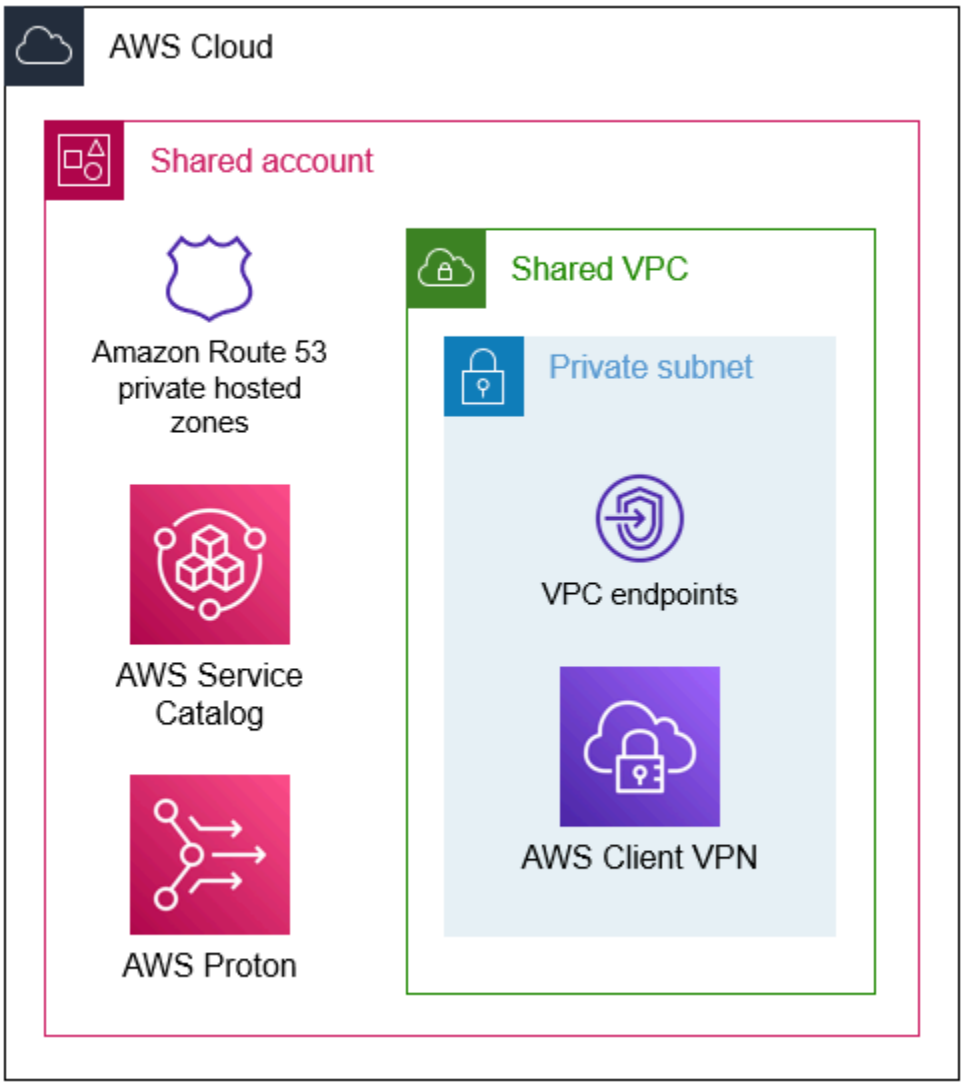
Meskipun ingress terdesentralisasi berarti Anda harus mengelola setiap akun secara individual, Anda dapat mengelola dan mempertahankan konfigurasi secara terpusat. AWS Firewall Manager Firewall Manager mendukung perlindungan seperti AWS WAFdan grup keamanan Amazon VPC. Anda dapat mengaitkan AWS WAF ke Application Load Balancer CloudFront, Amazon, API Gateway, atau. AWS AppSync Jika Anda menggunakan VPC jalan keluar dan gateway transit, seperti yang dijelaskan dalam, Jalan keluar terpusat setiap VPC spoke berisi subnet publik dan pribadi. Namun, tidak perlu menggunakan gateway NAT karena rute lalu lintas melalui VPC jalan keluar di akun jaringan.

Gambar berikut menunjukkan contoh individu Akun AWS yang memiliki satu VPC yang berisi beban kerja yang dapat diakses internet. Lalu lintas dari internet mengakses VPC melalui gateway internet dan mencapai penyeimbangan beban dan layanan keamanan yang dihosting di subnet publik. (Subnet publik berisi rute default ke gateway internet). Menyebarkan penyeimbang beban ke subnet publik, dan lampirkan daftar kontrol AWS WAF akses (ACL) untuk membantu melindungi dari lalu lintas berbahaya, seperti skrip lintas situs. Menyebarkan beban kerja yang meng-host aplikasi ke subnet pribadi, yang tidak memiliki akses langsung ke dan dari internet.



Jika Anda memiliki banyak VPC di organisasi Anda, Anda mungkin ingin berbagi kesamaan Layanan AWS dengan membuat titik akhir VPC antarmuka atau zona host pribadi di dedicated dan shared. Akun AWS Untuk informasi selengkapnya, lihat Mengakses titik akhir VPC antarmuka (AWS PrivateLink dokumentasi) dan Bekerja dengan zona yang dihosting pribadi (dokumentasi Rute 53). Layanan AWS

Gambar berikut menunjukkan contoh sumber daya host Akun AWS yang dapat dibagikan di seluruh organisasi. Titik akhir VPC dapat dibagikan di beberapa akun dengan membuatnya di VPC khusus. Saat membuat titik akhir VPC, Anda dapat AWS mengelola entri DNS untuk titik akhir secara opsional. Untuk berbagi titik akhir, hapus opsi ini, dan buat entri DNS di zona host pribadi Route 53 (PHZ) terpisah. Anda kemudian dapat mengaitkan PHZ ke semua VPC di organisasi Anda untuk resolusi DNS terpusat dari titik akhir VPC. Anda juga perlu memastikan bahwa tabel rute gateway transit menyertakan rute untuk VPC bersama ke VPC lainnya. Untuk informasi selengkapnya, lihat Akses terpusat ke titik akhir AWS VPC antarmuka (Whitepaper).



Shared juga Akun AWS merupakan tempat yang baik untuk meng-host AWS Service Catalog portofolio. Portofolio adalah kumpulan layanan TI yang ingin Anda sediakan untuk penyebaran AWS, dan portofolio berisi informasi konfigurasi untuk layanan tersebut. Anda dapat membuat portofolio di akun bersama, membagikannya ke organisasi, dan kemudian setiap akun anggota mengimpor portofolio ke instance Service Catalog regionalnya sendiri. Untuk informasi selengkapnya, lihat Berbagi dengan AWS Organizations (Dokumentasi Service Catalog).

Demikian pula AWS Proton, dengan, Anda dapat menggunakan akun bersama untuk mengelola lingkungan dan templat layanan Anda secara terpusat, lalu mengatur koneksi akun dengan akun anggota organisasi. Untuk informasi selengkapnya, lihat Koneksi akun lingkungan (AWS Proton dokumentasi).

Respons insiden keamanan untuk arsitektur multi-akun

Saat Anda beralih ke beberapa Akun AWS, penting bagi Anda untuk menjaga visibilitas ke peristiwa keamanan yang mungkin terjadi dalam organisasi Anda. DiManajemen identitas dan kontrol akses, Anda biasa AWS Control Tower mengatur landing zone Anda. Selama proses penyiapan itu, AWS Control Tower ditunjuk Akun AWS untuk keamanan. Anda harus mendelegasikan administrasi layanan keamanan ke dalam security-tooling-prodakun dan menggunakan akun ini untuk mengelola layanan ini secara terpusat.

Panduan ini mengulas penggunaan berikut ini Layanan AWS untuk membantu melindungi Anda Akun AWS dan organisasi:

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis sumber data, seperti log AWS CloudTrail peristiwa. Untuk daftar lengkap sumber data yang didukung, lihat Cara Amazon GuardDuty menggunakan sumber datanya (GuardDuty dokumentasi). Aplikasi ini menggunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, dan machine learning untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam lingkungan AWS .

Saat Anda menggunakannya GuardDuty AWS Organizations, akun manajemen di organisasi dapat menunjuk akun apa pun di organisasi untuk menjadi administrator yang GuardDuty didelegasikan. Administrator yang didelegasikan menjadi akun GuardDuty administrator untuk Wilayah. GuardDuty diaktifkan secara otomatis dalam:Wilayah AWS, dan akun administrator yang didelegasikan memiliki izin untuk mengaktifkan dan mengelola GuardDuty semua akun di organisasi dalam Wilayah tersebut. Untuk informasi selengkapnya, lihat Mengelola GuardDuty akun dengan AWS Organizations (GuardDuty dokumentasi).

GuardDuty adalah layanan regional. Ini berarti Anda harus mengaktifkan GuardDuty di setiap Wilayah yang ingin Anda pantau.

Praktik terbaik

- Aktifkan GuardDuty di semua yang didukung Wilayah AWS. GuardDuty dapat menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa, bahkan di Wilayah yang tidak Anda gunakan secara aktif. Penetapan harga GuardDuty didasarkan pada jumlah peristiwa yang dianalisis. Bahkan di Wilayah di mana Anda tidak mengoperasikan beban kerja, mengaktifkan GuardDuty adalah alat deteksi yang efektif dan hemat biaya untuk mengingatkan Anda tentang aktivitas yang berpotensi berbahaya. Untuk informasi selengkapnya tentang Wilayah yang GuardDuty tersedia, lihat titik akhir GuardDuty layanan Amazon (Referensi Umum AWS).
- Di setiap Wilayah, delegasikan security-tooling-prodakun GuardDuty untuk dikelola organisasi Anda. Untuk informasi selengkapnya, lihat Menunjuk administrator yang GuardDuty didelegasikan (GuardDuty dokumentasi).
- Konfigurasikan GuardDuty untuk secara otomatis mendaftarkan baru Akun AWS saat ditambahkan ke organisasi. Untuk informasi selengkapnya, lihat Langkah 3 - mengotomatiskan penambahan akun organisasi baru sebagai anggota di Mengelola akun dengan AWS Organizations (GuardDuty dokumentasi).

Amazon Macie

Amazon Macie adalah layanan keamanan data dan privasi data yang dikelola sepenuhnya yang menggunakan pembelajaran mesin dan pencocokan pola untuk membantu Anda menemukan, memantau, dan melindungi data sensitif di Amazon Simple Storage Service (Amazon S3). Anda dapat mengekspor data dari Amazon Relational Database Service (Amazon RDS) dan Amazon DynamoDB ke bucket S3 dan kemudian menggunakan Macie untuk memindai data.

Saat Anda menggunakan Macie dengan AWS Organizations, akun manajemen di organisasi dapat menunjuk akun apa pun di organisasi untuk menjadi akun administrator Macie. Akun administrator dapat mengaktifkan dan mengelola Macie untuk akun anggota di organisasi, dapat mengakses data inventaris Amazon S3, dan dapat menjalankan pekerjaan penemuan data sensitif untuk akun tersebut. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations (dokumentasi Macie).

Macie adalah layanan regional. Ini berarti bahwa Anda harus mengaktifkan Macie di setiap Wilayah yang ingin Anda pantau dan bahwa akun administrator Macie dapat mengelola akun anggota hanya dalam Wilayah yang sama.

Praktik terbaik

- Patuhi Pertimbangan dan rekomendasi untuk menggunakan Macie dengan AWS Organizations (dokumentasi Macie).
- Di setiap Wilayah, delegasikan security-tooling-prodakun untuk mengelola Macie untuk organisasi Anda. Untuk mengelola akun Macie secara terpusat dalam beberapa Wilayah AWS, akun manajemen harus masuk ke setiap Wilayah tempat organisasi saat ini menggunakan atau akan menggunakan Macie, dan kemudian menunjuk akun administrator Macie di masing-masing Wilayah tersebut. Akun administrator Macie kemudian dapat mengonfigurasi organisasi di masing-masing Wilayah tersebut. Untuk informasi selengkapnya, lihat Mengintegrasikan dan mengonfigurasi organisasi (dokumentasi Macie).
- Macie menyediakan tingkat gratis bulanan untuk pekerjaan penemuan data sensitif. Jika Anda mungkin memiliki data sensitif yang disimpan di Amazon S3, gunakan Macie untuk menganalisis bucket S3 Anda sebagai bagian dari tingkat gratis bulanan. Jika Anda melebihi tingkat gratis, biaya penemuan data sensitif mulai bertambah untuk akun Anda.

AWS Security Hub

AWS Security Hubmemberi Anda pandangan komprehensif tentang keadaan keamanan Anda di AWS. Anda dapat menggunakannya untuk memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan data keamanan dari seluruh layanan Anda Akun AWS(termasuk GuardDuty dan Macie), dan produk mitra pihak ketiga yang didukung. Security Hub membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi. Security Hub menyediakan berbagai standar keamanan yang dapat Anda aktifkan untuk melakukan pemeriksaan kepatuhan di masing-masing Akun AWS.

Saat Anda menggunakan Security Hub AWS Organizations, akun manajemen di organisasi dapat menetapkan akun apa pun di organisasi sebagai akun administrator Security Hub. Akun administrator Security Hub kemudian dapat mengaktifkan dan mengelola akun anggota lain di organisasi. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations untuk mengelola akun (Dokumentasi Security Hub).

Security Hub adalah layanan regional. Ini berarti Anda harus mengaktifkan Security Hub di setiap Wilayah yang ingin Anda analisis, dan di AWS Organizations, Anda harus menentukan administrator yang didelegasikan untuk setiap Wilayah.

Praktik terbaik

- Patuhi Prasyarat dan rekomendasi (dokumentasi Security Hub).
- Di setiap Wilayah, delegasikan security-tooling-prodakun untuk mengelola Security Hub untuk organisasi Anda. Untuk informasi selengkapnya, lihat Menetapkan akun administrator Security Hub (dokumentasi Security Hub).
- Konfigurasikan Security Hub untuk mendaftarkan yang baru secara otomatis Akun AWS saat ditambahkan ke organisasi.
- Aktifkan standar Praktik Terbaik Keamanan AWS Dasar (dokumentasi Security Hub) untuk mendeteksi kapan sumber daya menyimpang dari praktik terbaik keamanan.
- Aktifkan agregasi Lintas Wilayah (dokumentasi Security Hub) sehingga Anda dapat melihat dan mengelola semua temuan Security Hub dari satu Wilayah.

Mengkonfigurasi cadangan untuk arsitektur multi-akun

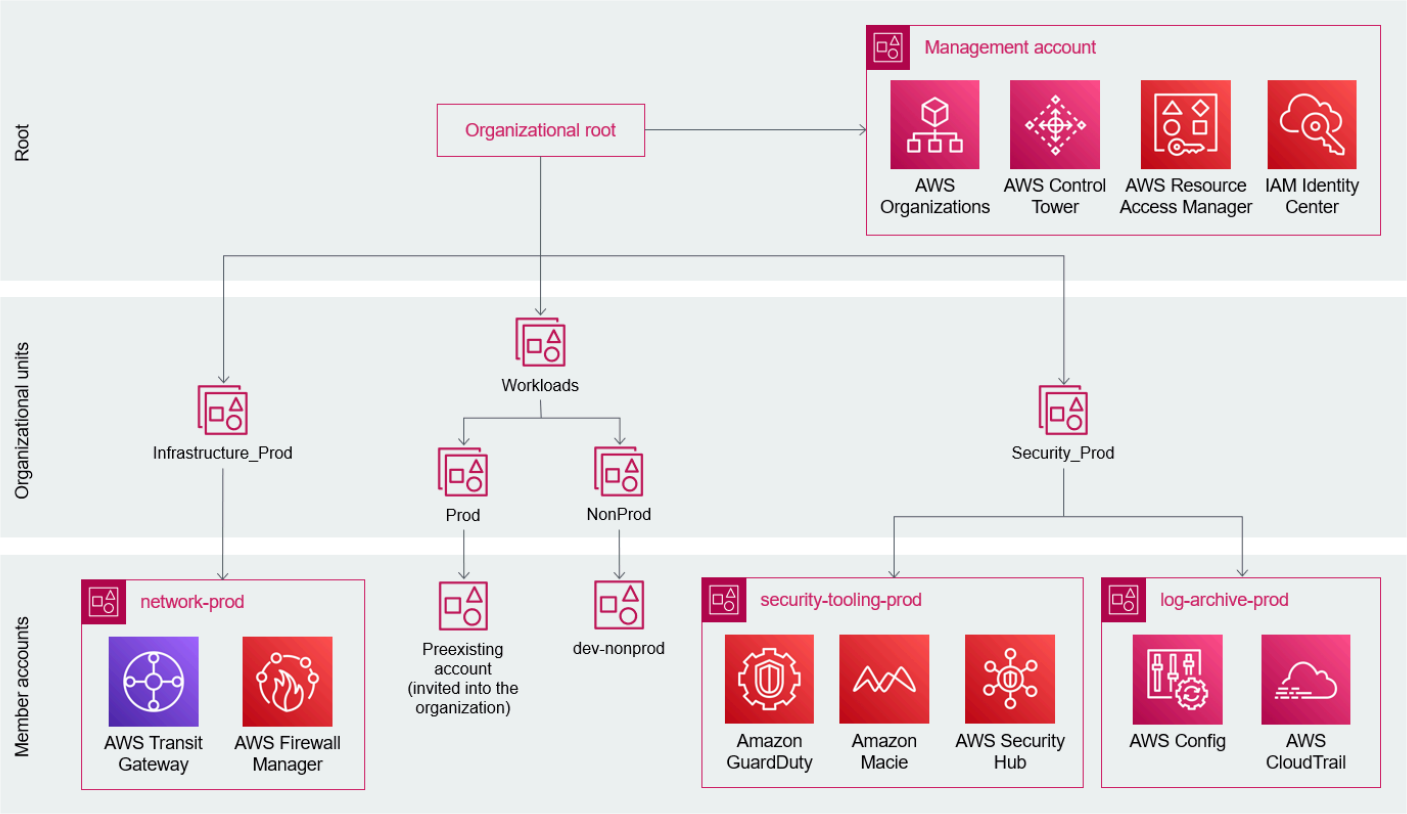
Strategi pencadangan yang komprehensif adalah bagian penting dari rencana perlindungan data perusahaan untuk menahan, memulihkan, dan mengurangi dampak apa pun yang mungkin dipertahankan karena peristiwa keamanan. Kebijakan pencadangan membantu Anda menstandarisasi dan menerapkan strategi cadangan untuk sumber daya di semua akun di organisasi Anda. Dalam Kebijakan backup, Anda dapat mengkonfigurasi dan menyebarkan rencana cadangan untuk sumber daya Anda. Untuk informasi lebih lanjut, lihatKebijakan pencadangan(AWS Organizationsdokumentasi). Untuk informasi lebih lanjut, lihat10 praktik terbaik keamanan teratas untuk mengamankan cadanganAWS(AWSBimbingan Preskriptif).

Migrasi akun saat beralih ke arsitektur multi-akun

DiUndang akun Anda yang sudah ada sebelumnya, Anda mengundang akun Anda yang sudah ada sebelumnya untuk bergabung denganBeban Kerja > Produnit organisasi. Akun ini sekarang dikelola sebagai bagian dari organisasi Anda.

Anda juga menyediakan yang barudev-nonprodakun diBeban kerja >NonProdunit organisasi. Anggota tim sekarang harus dapat mengakses akun yang sesuai melaluiAWS IAM Identity Center. Hapus setiap akun pengguna individu diAWS Identity and Access Management(IAM).

Jika Anda telah mengikuti rekomendasi dalam panduan ini, organisasi Anda sekarang memiliki struktur berikut.



Jika ada beban kerja yang berjalan di dalam akun yang sudah ada sebelumnya, Anda sekarang memigrasikan beban kerja ini ke akun independen, sesuai dengan kriteria yang Anda buatTentukan kriteria pelingkupan. Migrasikan beban kerja non-produksi ke yang barudev-nonprodunit organisasi, dan memigrasikan beban kerja produksi kejaringan-prodakun. Untuk informasi lebih lanjut tentang migrasi umumAWSsumber daya, lihat bagian berikut dari panduan ini,Migrasi sumber daya.

Replikasi sumber daya atau migrasi antara Akun AWS

Setelah bermigrasi dari arsitektur tunggal Akun AWS ke multi-akun, biasanya beban kerja produksi dan non-produksi berjalan di akun yang sudah ada sebelumnya. Migrasi sumber daya ini ke akun produksi dan non-produksi khusus atau unit organisasi membantu Anda mengelola akses dan jaringan untuk beban kerja ini. Berikut ini adalah beberapa opsi untuk memigrasikan AWS sumber daya umum ke sumber daya lain Akun AWS.

Bagian ini berfokus pada strategi untuk mereplikasi data antara Akun AWS. Anda harus berusaha agar beban kerja Anda menjadi tanpa kewarganegaraan mungkin untuk menghindari kebutuhan untuk mereplikasi sumber daya komputasi antar akun. Ini juga bermanfaat untuk mengelola sumber daya Anda melalui infrastruktur sebagai kode (IAc) sehingga Anda dapat menyediakan kembali lingkungan secara terpisah. Akun AWS

Bagian ini mengulas opsi untuk memigrasikan sumber data berikut:

- AWS AppConfig konfigurasi dan lingkungan
- AWS Certificate Manager sertifikat
- CloudFront Distribusi Amazon
- AWS CodeArtifact domain dan repositori
- Tabel Amazon DynamoDB
- EBSVolume Amazon
- EC2Contoh Amazon atau AMIs
- ECRPendaftaran Amazon
- Sistem EFS file Amazon
- ElastiCache Cluster Amazon (RedisOSS)
- AWS Elastic Beanstalk lingkungan
- Alamat IP elastis
- AWS Lambda lapisan
- Contoh Amazon Lightsail
- Cluster Amazon Neptunus
- Domain OpenSearch Layanan Amazon
- RDSCuplikan Amazon
- Cluster Amazon Redshift

- Amazon Route 53 domain dan zona yang dihosting
- Bucket Amazon S3
- SageMaker Model Amazon
- AWS WAF web ACLs

AWS AppConfig konfigurasi dan lingkungan

AWS AppConfig tidak mendukung penyalinan konfigurasinya secara langsung ke yang lain Akun AWS. Namun, ini adalah praktik terbaik untuk mengelola AWS AppConfig konfigurasi dan lingkungan secara terpisah dari Akun AWS yang menghosting lingkungan. Untuk informasi selengkapnya, lihat Konfigurasi lintas akun dengan AWS AppConfig (posting AWS blog).

AWS Certificate Manager sertifikat

Anda tidak dapat langsung mengekspor sertifikat AWS Certificate Manager (ACM) dari satu akun ke akun lainnya karena kunci AWS Key Management Service (AWS KMS) yang digunakan untuk mengenkripsi kunci pribadi sertifikat unik untuk masing-masing akun Wilayah AWS dan akun. Namun, Anda dapat secara bersamaan menyediakan beberapa sertifikat dengan nama domain yang sama di beberapa akun dan Wilayah. ACMmendukung validasi kepemilikan domain dengan menggunakan DNS (disarankan) atau email. Saat Anda menggunakan DNS validasi dan membuat sertifikat baru, ACM buat CNAME catatan unik untuk setiap domain pada sertifikat. CNAMECatatan unik untuk setiap akun, dan harus ditambahkan ke zona atau DNS penyedia yang dihosting Amazon Route 53 dalam waktu 72 jam agar sertifikat divalidasi dengan benar.

CloudFront Distribusi Amazon

Amazon CloudFront tidak mendukung migrasi distribusi dari satu Akun AWS ke yang lain Akun AWS. Namun, CloudFront mendukung migrasi nama domain alternatif, juga dikenal sebagai CNAME, dari satu distribusi ke distribusi lainnya. Untuk informasi selengkapnya, lihat Bagaimana cara mengatasi CNAMEAlreadyExists kesalahan saat menyiapkan CNAME alias untuk CloudFront distribusi saya (Pusat AWS Pengetahuan).

AWS CodeArtifact domain dan repositori

Meskipun sebuah organisasi dapat memiliki beberapa domain, rekomendasinya adalah memiliki domain produksi tunggal yang berisi semua artefak yang diterbitkan. Ini membantu tim

pengembangan menemukan dan berbagi paket di seluruh organisasi. Akun AWS Yang memiliki domain dapat berbeda dari akun yang memiliki repositori apa pun yang terkait dengan domain. Anda dapat menyalin paket antar repositori, tetapi mereka harus milik domain yang sama. Untuk informasi selengkapnya, lihat Menyalin paket antar repositori (CodeArtifact dokumentasi).

Tabel Amazon DynamoDB

Anda dapat menggunakan salah satu layanan berikut untuk memigrasikan tabel Amazon DynamoDB ke tabel lain: Akun AWS

- AWS Backup
- DynamoDB impor dan ekspor ke Amazon S3
- Amazon S3 dan AWS Glue
- AWS Data Pipeline
- Amazon EMR

Untuk informasi selengkapnya, lihat Bagaimana cara memigrasikan tabel Amazon DynamoDB saya Akun AWS dari satu ke yang AWS lain (Pusat Pengetahuan).

EBSVolume Amazon

Anda dapat mengambil snapshot dari volume Amazon Elastic Block Store (AmazonEBS) yang ada, membagikan snapshot dengan akun target, dan kemudian membuat salinan volume di akun target. Ini secara efektif memigrasikan volume dari satu akun ke akun lainnya. Untuk informasi selengkapnya, lihat Bagaimana cara membagikan EBS snapshot atau volume Amazon terenkripsi dengan yang lain Akun AWS (Pusat AWS Pengetahuan).

EC2Contoh Amazon atau AMIs

Tidak mungkin mentransfer instans Amazon Elastic Compute Cloud (AmazonEC2) atau Amazon Machine Images (AMIs) secara langsung ke instans lain. Akun AWS Sebagai gantinya, Anda dapat membuat kustom AMI di akun sumber, membagikannya AMI dengan akun target, meluncurkan EC2 instance baru dari yang dibagikan AMI di akun target, lalu membatalkan pendaftaran yang dibagikan. AMI Untuk informasi selengkapnya, lihat Bagaimana cara mentransfer EC2 instans Amazon atau AMI ke Akun AWS(Pusat AWS Pengetahuan) yang berbeda.

ECRPendaftaran Amazon

Amazon Elastic Container Registry (AmazonECR) mendukung replikasi lintas akun dan lintas wilayah. Anda mengonfigurasi replikasi pada registri sumber dan kebijakan izin registri pada registri target. Untuk informasi selengkapnya, lihat Mengonfigurasi replikasi lintas akun (ECRdokumentasi Amazon) dan Mengizinkan pengguna root akun sumber mereplikasi semua repositori (dokumentasi Amazon). ECR

Sistem EFS file Amazon

Untuk Amazon Elastic File System (AmazonEFS), Anda dapat menggunakannya AWS DataSync untuk menyalin data dari sistem file sumber ke sistem file tujuan di sistem file lain Akun AWS. DataSync Agen harus dibuat sama Wilayah AWS dan Akun AWS sebagai sistem file sumber. Untuk informasi selengkapnya, lihat Mentransfer data dari sistem file cloud ke sistem file cloud lain (DataSyncdokumentasi). Saat menyalin antara dua sistem EFS file Amazon secara berbeda Akun AWS, kami sarankan Anda menggunakan transfer NFS (sumber) ke EFS (tujuan). Untuk informasi dan petunjuk selengkapnya, lihat Membuat tugas untuk mentransfer data dari Amazon EFS (DataSync dokumentasi).

ElastiCache Cluster Amazon (RedisOSS)

Anda dapat menggunakan cadangan kluster database Amazon ElastiCache (RedisOSS) untuk memigrasikannya ke akun lain. Untuk informasi selengkapnya, lihat Apa praktik terbaik untuk memigrasi klaster ElastiCache (RedisOSS) saya (Pusat AWS Pengetahuan).

AWS Elastic Beanstalk lingkungan

Untuk AWS Elastic Beanstalk, Anda dapat menggunakan konfigurasi tersimpan (dokumentasi Elastic Beanstalk) untuk memigrasikan lingkungan ke lingkungan yang berbeda. Akun AWS Untuk informasi lebih lanjut, lihat Bagaimana cara memigrasikan lingkungan Elastic Beanstalk saya Akun AWS dari satu Akun AWS ke yang lain (Pusat Pengetahuan).AWS

Alamat IP elastis

Anda dapat mentransfer alamat IP Elastis antara Akun AWS yang sama Wilayah AWS. Untuk informasi selengkapnya, lihat Mentransfer alamat IP Elastis (VPCdokumentasi Amazon).

AWS Lambda lapisan

Secara default, AWS Lambda lapisan yang Anda buat bersifat pribadi untuk Anda Akun AWS. Namun, Anda dapat secara opsional berbagi layer dengan yang lain Akun AWS atau menjadikannya publik. Untuk menyalin lapisan, Anda menyediakannya kembali di lapisan lain Akun AWS. Untuk informasi selengkapnya, lihat Mengonfigurasi izin lapisan (dokumentasi Lambda).

Contoh Amazon Lightsail

Anda dapat membuat snapshot instance Amazon Lightsail dan mengekspor snapshot ke Amazon Machine AMI Image () dan snapshot terenkripsi dari volume Amazon. EBS Untuk informasi selengkapnya, lihat Mengekspor snapshot Amazon Lightsail ke EC2 Amazon (dokumentasi Lightsail). Secara default, snapshot dienkripsi dengan kunci AWS terkelola yang dibuat di AWS Key Management Service ().AWS KMS Namun, jenis KMS kunci ini tidak dapat dibagi antara Akun AWS. Sebagai gantinya, Anda secara manual mengenkripsi salinan AMI dengan kunci yang dikelola pelanggan yang dapat digunakan dari akun target. Untuk informasi selengkapnya, lihat Mengizinkan pengguna di akun lain menggunakan KMS kunci (AWS KMS dokumentasi). Anda kemudian dapat membagikan salinan AMI dengan target Akun AWS dan meluncurkan EC2 instance baru untuk Lightsail dari yang disalin. AMI Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan wizard instans peluncuran baru (EC2dokumentasi Amazon).

Cluster Amazon Neptunus

Anda dapat menyalin snapshot otomatis dari cluster database Amazon Neptunus ke yang lain. Akun AWS Untuk informasi selengkapnya, lihat Menyalin snapshot cluster database (DB) (dokumentasi Neptunus).

Anda juga dapat membagikan snapshot manual hingga 20 Akun AWS yang dapat langsung mengembalikan cluster DB dari snapshot. Untuk informasi selengkapnya, lihat Berbagi Snapshot Cluster DB (dokumentasi Neptunus).

Domain OpenSearch Layanan Amazon

Untuk menyalin data antara domain OpenSearch Layanan Amazon, Anda dapat menggunakan Amazon S3 untuk membuat snapshot dari domain sumber dan kemudian mengembalikan snapshot ke domain target yang berbeda. Akun AWS Untuk informasi selengkapnya, lihat Bagaimana cara

memulihkan data dari domain OpenSearch Layanan Amazon di domain lain Akun AWS (Pusat AWS Pengetahuan).

Jika Anda memiliki konektivitas jaringan antara Akun AWS, Anda juga dapat menggunakan replikasi lintas cluster (Dokumentasi OpenSearch layanan) fitur di OpenSearch Layanan.

RDSCuplikan Amazon

Untuk Amazon Relational Database Service (RDSAmazon), Anda dapat membagikan snapshot manual instans atau cluster DB hingga 20.Akun AWS Anda kemudian dapat memulihkan instans DB atau cluster DB dari snapshot bersama. Untuk informasi selengkapnya, lihat Bagaimana cara membagikan snapshot Amazon RDS DB manual atau snapshot klaster Aurora DB dengan yang Akun AWS lain AWS (Pusat Pengetahuan).

Anda juga dapat menggunakan AWS Database Migration Service (AWS DMS) untuk mengonfigurasi replikasi berkelanjutan antara instance database di akun yang berbeda. Namun, ini membutuhkan konektivitas jaringan antar akun, seperti VPC peering atau gateway transit.

Cluster Amazon Redshift

Untuk memigrasikan cluster Amazon Redshift ke cluster Akun AWS lain, Anda membuat snapshot manual cluster di akun sumber, membagikan snapshot dengan Akun AWS target, lalu memulihkan cluster dari snapshot. Untuk informasi selengkapnya, lihat Bagaimana cara menyalin klaster yang disediakan Amazon Redshift ke Akun AWS(AWS Pusat Pengetahuan) yang berbeda.

Amazon Route 53 domain dan zona yang dihosting

Anda dapat mentransfer domain Amazon Route 53 antara Akun AWS. Untuk informasi selengkapnya, lihat Mentransfer domain ke domain lain Akun AWS (dokumentasi Route 53).

Anda juga dapat memigrasikan zona yang dihosting Route 53 ke zona lain Akun AWS. Untuk informasi selengkapnya tentang kapan ini direkomendasikan atau diperlukan, lihat Memigrasi zona yang dihosting ke zona lain Akun AWS (dokumentasi Rute 53). Saat memigrasikan zona yang dihosting, Anda membuatnya ulang di target. Akun AWS Untuk petunjuk, lihat Memigrasi zona yang dihosting ke zona lain Akun AWS (dokumentasi Rute 53).

Bucket Amazon S3

Anda dapat menggunakan Amazon Simple Storage Service (Amazon S3) Simple Storage Service S3) Same-Region Replication untuk menyalin objek antara bucket S3 di Wilayah yang sama. AWS Untuk informasi selengkapnya, lihat Mereplikasi objek (dokumentasi Amazon S3). Perhatikan hal berikut:

- Ubah kepemilikan replika ke Akun AWS bucket yang memiliki tujuan. Untuk petunjuk, lihat Mengubah pemilik replika (dokumentasi Amazon S3).
- Perbarui kondisi pemilik bucket untuk mencerminkan Akun AWS ID bucket target. Untuk informasi selengkapnya, lihat Memverifikasi kepemilikan bucket dengan kondisi pemilik bucket (dokumentasi Amazon S3).
- Mulai April 2023, pengaturan yang diberlakukan pemilik Bucket diaktifkan untuk bucket yang baru dibuat, membuat daftar kontrol akses bucket (ACLs) dan objek tidak efektif. ACLs Untuk informasi selengkapnya, lihat Perubahan Keamanan Amazon S3 Akan Datang (posting AWS blog).
- Anda dapat menggunakan Replikasi Batch S3 (dokumentasi Amazon S3) untuk mereplikasi objek yang ada sebelum replikasi dikonfigurasi.

SageMaker Model Amazon

SageMaker model disimpan dalam ember Amazon S3 selama pelatihan. Dengan memberikan akses ke bucket S3 dari akun target, Anda dapat menerapkan model yang disimpan di akun sumber ke akun target. Untuk informasi selengkapnya, lihat Bagaimana cara menerapkan SageMaker model Amazon ke Akun AWS(Pusat AWS Pengetahuan) yang berbeda.

AWS WAF web ACLs

AWS WAF Daftar kontrol akses web (webACLs) harus berada di akun yang sama dengan sumber daya yang terkait dengannya, seperti CloudFront distribusi Amazon, Application Load Balancers, Amazon Gateway RESTAPIs, dan API GraphQL. AWS AppSync APIs Anda dapat menggunakan AWS Firewall Manager untuk mengelola AWS WAF web secara terpusat ACLs di seluruh organisasi Anda di AWS Organizations dan di seluruh Wilayah. Untuk informasi selengkapnya, lihat Memulai AWS Firewall ManagerAWS WAF kebijakan (dokumentasi Firewall Manager).

Pertimbangan penagihan saat beralih ke arsitektur multi-akun

Jika Anda menggunakan AWS Organizations untuk transisi ke beberapaAkun AWS, Anda dapat menggunakan fitur penagihan konsolidasi (AWS Organizationsdokumentasi). Fitur ini menyediakan tagihan gabungan tunggal yang menunjukkan tagihan di beberapa akun.

Berikut ini adalah praktik terbaik penagihan dan rekomendasi untuk transisi ke beberapa akun:

- Jika Anda memerlukan akses ke data penagihan historis, sebelum menerima undangan untuk bergabung dengan organisasi, buat Laporan Biaya dan Penggunaan (AWS Cost and Usage Reportdokumentasi) untuk mengekspor data penagihan historis akun ke bucket Amazon Simple Storage Service (Amazon S3). Setelah Anda menerima undangan untuk bergabung dengan organisasi, data tagihan historis akun tidak lagi dapat diakses.
- Jika Anda perlu menggabungkan dua organisasi, seperti untuk merger atau akuisisi, Anda dapat menggunakan Account Assessment for AWS Organizations (AWSSolutions Library) untuk mengevaluasi kebijakan berbasis sumber daya di setiap organisasi dan mengidentifikasi potensi masalah sebelum menggabungkannya.

Kesimpulan

Transisi dari satuAkun AWSke beberapa akun bisa terasa luar biasa pada awalnya tanpa strategi adopsi. Dengan menerapkan strategi multi-akun, Anda dapat mengatasi banyak tantangan yang dihadapi perusahaan saat menggunakan satu akun.Akun AWS:

- Salah mengira data produksi sebagai data pengembangan— Anda dapat memberikan izin dan akses yang berbeda dengan menggunakanAWS IAM Identity Centerdengan izin terpisah menetapkan unit organisasi produksi dan non-produksi. Hanya pengguna yang memiliki hak istimewa yang harus memiliki akses ke basis data produksi, dan akses itu harus untuk jangka waktu terbatas dan diaudit.
- Penyebaran produksi mempengaruhi operasi bisnis lainnya— Anda dapat memisahkan pemangku kepentingan dengan menggunakan beberapa akun dan beberapa lingkungan. Misalnya, Anda dapat membuat lingkungan demo penjualan khusus, dalam akun non-produksi, sehingga Anda dapat merencanakan penerapan dan rilis saat demo tidak terjadi.
- Performa beban kerja produksi lambat saat menguji beban kerja pengembangan— Masing-masingAkun AWSmemiliki kuota layanan independen yang mengatur setiap layanan. Dengan menggunakan beberapa akun, Anda dapat membatasi ruang lingkup satu lingkungan yang memengaruhi lingkungan lain.
- Membedakan biaya produksi dari biaya pengembangan— Tagihan konsolidasi untuk organisasi menggulung semua biaya diAkun AWStingkat sehingga tim keuangan dapat melihat berapa banyak biaya produksi dibandingkan dengan lingkungan non-produksi, seperti pengembangan, pengujian, dan lingkungan demo. Anda juga dapat menggunakan tag dan kebijakan penandaan untuk memisahkan biaya dalam akun.
- Membatasi akses ke data sensitif— Pusat Identitas IAM memungkinkan Anda memiliki kebijakan akses terpisah untuk sekelompok orang yang terkait dengan akun tertentu.
- Mengontrol biaya— Dengan menggunakan kebijakan kontrol layanan (SCP) dalam arsitektur multi-akun, Anda dapat melarang akses ke spesifikLayanan AWSyang mungkin menimbulkan biaya tinggi untuk organisasi Anda. SCP dapat menolak semua akses ke layanan tertentu atau dapat membatasi penggunaan layanan ke jenis tertentu, seperti membatasi jenis instans Amazon Elastic Compute Cloud (Amazon EC2) yang dapat dibuat.

Kontributor

Kontributor dokumen ini meliputi:

- Justin Plock, Arsitek Solusi Utama, AWS (penulis utama)
- Emily Arnautovic, Arsitek Utama, AWS
- Jason DiDomenico, Arsitek Solusi Senior, AWS
- Michael Leighty, Sr. Arsitek Solusi Spesialis Keamanan, AWS
- Jesse Lepich, Sr. Arsitek Solusi Spesialis Keamanan, AWS
- Rodney Lester, Arsitek Solusi Utama, AWS
- Israel Lopez Moriano, Arsitek Solusi, AWS
- George Rolston, Arsitek Solusi Senior, AWS
- Alex Torres, Arsitek Solusi Senior, AWS
- Dave Walker, Arsitek Solusi Utama, AWS

Sumber daya

AWSBimbingan Preskriptif

- AWSDasar Keamanan Startup(AWSSSB)
- AWSArsitektur Referensi Keamanan(AWSSRA)
- 10 praktik terbaik keamanan teratas untuk mengamankan cadangan diAWS

AWSposting blog

- Bagaimana Menyiapkan Pengguna IAM dan Peran IAM Dapat Membantu Menjaga Startup Anda Aman
- Cara membiarkan pembangun membuat sumber daya IAM sambil meningkatkan keamanan dan kelincahan untuk organisasi Anda

AWSWhitepaper

- Mengatur AndaAWSLingkungan Menggunakan Beberapa Akun
- Membangun Cloud Foundation Anda diAWS
- Membangun Multi-VPC yang Dapat Diskalakan dan AmanAWSInfrastruktur Jaringan

AWScontoh kode

- Mengotomatiskan pengaturan layanan keamanan dengan AWS Control Tower(GitHub)

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Praktik terbaik jalan keluar terpusat	Kami memperbarui praktik terbaik untuk mengamankan lalu lintas jalan keluar.	6 Mei 2024
Praktik terbaik organisasi	Kami memperbarui praktik terbaik untuk membuat organisasi di AWS Organizations.	Desember 4, 2023
Pertimbangan penagihan	Kami menambahkan bagian Pertimbangan Penagihan.	20 September 2023
Migrasi sumber daya, konektivitas aplikasi, dan Amazon VPC Lattice	Kami menambahkan bagian migrasi Sumber Daya dan Menghubungkan aplikasi. Kami juga menambahkan informasi tentang Kisi Amazon Virtual Private Cloud (Amazon VPC) baru Layanan AWS.	27 April 2023
Riwayat akun dan ABAC	Kami merevisi bagian Create a landing zone untuk menambahkan informasi tentang cara memastikan riwayat penggunaan baru Akun AWS Anda sehingga Anda dapat menambahkannya ke AWS Control Tower landing zone Anda. Kami juga merevisi bagian	Januari 6, 2023

	Tambahkan pengguna awal untuk menambahkan informasi tentang bagaimana Anda dapat menggunakan kontrol akses berbasis atribut (ABAC) untuk meneruskan metode otentikasi dari IDP berbasis SAML eksternal ke. AWS IAM Identity Center	
Jaringan lalu lintas keluar	Kami merevisi bagian jalan keluar terpusat untuk menambahkan informasi tentang penggunaan Amazon Route 53 Resolver DNS Firewall untuk membatasi lalu lintas keluar ke nama domain tertentu.	13 Oktober 2022
Keamanan lalu lintas jalan keluar	Kami menambahkan Praktik terbaik untuk mengamankan lalu lintas jalan keluar.	6 Oktober 2022
Batas izin	Kami meningkatkan definisi batas izin, dan di bagian Sumber Daya, kami menambahkan tautan baru untuk informasi lebih lanjut tentang topik ini.	September 22, 2022
Publikasi awal	—	September 6, 2022

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ACID

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

SQLFungsi 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 AWS di 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 pemrosesan atau modifikasi 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 CAFMengatur panduan ke dalam enam bidang 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 berikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs AWS CAFweb dan AWS CAFwhitepaper.

AWS Kerangka Kualifikasi Beban Kerja ()AWS WQF

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

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, API panggilan 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

CAF

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat CCoEposting 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, mendefinisikanCCoE, 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. YAML 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 di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi database (DML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan () DVSM

Proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang berdampak buruk pada kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSMmemperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik manufaktur

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani 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 bagaimana Anda dapat menggunakan desain berbasis domain dengan pola ara pencekik, lihat Memodernisasi Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer 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 to AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir antarmuka. VPC Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (AmazonVPC).

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 AWS CAF keamanan termasuk 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. EDAdilakukan 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 ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas IAM izin. 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 untuk 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 IAM prinsip yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki rata-rata CPU dan penggunaan memori 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, a VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretasi

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITILmenyediakan fondasi untukITSM.

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 ITSM alat, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label () LBAC

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

landing zone

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

MAP

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

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi () MRA

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana tindakan untuk menutup kesenjangan yang diidentifikasi, menggunakan. AWS CAF Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRAIni 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 mengklarifikasi apa yang dijanjikan oleh 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 AWS Well-Architected.

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. OCMmembantu 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 OCMpanduannya.

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakanOAI, 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, a VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

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

Informasi Identifikasi Pribadi () PII

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contohnya 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 optimasi kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol pencegahan

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, IAM peran, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam IAM dokumentasi.

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 DNS kueri untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

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

manajemen siklus hidup produk () PLM

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram () PLC

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

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 layanan mikro berbasis MES, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan oleh 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 SQL relasional.

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

RACImatriks

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

ransomware

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

RASCImatriks

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Wilayah

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

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 SQL ekspresi dasar dan fleksibel yang telah menetapkan aturan akses. RCACterdiri 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 (SSO) gabungan, sehingga pengguna dapat masuk ke AWS Management Console atau memanggil AWS API operasi tanpa Anda harus membuat pengguna untuk semua

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

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

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.

informasi keamanan dan manajemen acara (SIEM) sistem

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen peristiwa keamanan (SEM). Sebuah SIEM sistem 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 VPC keamanan, menambal EC2 instans Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan () SLA

Perjanjian yang menjelaskan apa yang dijanjikan oleh tim TI untuk diberikan kepada pelanggan mereka, seperti uptime 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.

satu titik kegagalan (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 Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer dan Amazon API Gateway.

subnet

Berbagai alamat IP di AndaVPC. 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 jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

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

tugas yang tidak terdiferensiasi

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

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

VPCmengintip

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

SQLFungsi 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.

WORM

Lihat menulis sekali, baca banyak.

WQF

Lihat AWSKerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

aplikasi zombie

Aplikasi yang memiliki rata-rata CPU 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.