AWS Arsitektur Referensi Privasi

AWS Panduan Preskriptif

AWS Panduan Preskriptif: AWS Arsitektur Referensi Privasi

Table of Contents

AWS Arsitektur Referensi Privasi

Amazon Web Services (kontributor)

September 2025 (riwayat dokumen)

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Pemberitahuan

Panduan ini disediakan untuk tujuan informasi saja. Ini bukan nasihat hukum dan tidak boleh diandalkan sebagai nasihat hukum. AWS mendorong pelanggannya untuk mendapatkan saran yang tepat tentang penerapan lingkungan privasi dan perlindungan data mereka, dan secara lebih umum, hukum yang berlaku yang relevan dengan bisnis mereka.

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat.

Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Pengantar

Arsitektur Referensi AWS Privasi (AWS PRA) menyediakan seperangkat pedoman khusus untuk desain dan konfigurasi kontrol pendukung privasi di. Layanan AWS Panduan ini dapat membantu Anda membuat keputusan tentang orang, proses, dan teknologi yang membantu mendukung privasi di dalamnya AWS Cloud.

Model tanggung jawab AWS bersama dan privasi

Dalam AWS Cloud, Anda berbagi tanggung jawab untuk keamanan dan kepatuhan dengan AWS. AWS bertanggung jawab atas keamanan cloud, yang berarti AWS bertanggung jawab melindungi infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud. Anda bertanggung jawab atas keamanan di cloud, yang berarti Anda bertanggung jawab untuk mengonfigurasi dan mengelola Layanan AWS sesuai dengan persyaratan keamanan dan privasi. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Layanan AWS menyediakan kemampuan yang memungkinkan Anda menerapkan kontrol privasi Anda sendiri di cloud untuk mendukung persyaratan privasi Anda. Tanggung jawab privasi Anda bervariasi berdasarkan banyak faktor, termasuk Layanan AWS dan yang Wilayah AWS Anda pilih, integrasi layanan tersebut ke dalam lingkungan TI Anda, dan undang-undang dan peraturan yang berlaku untuk organisasi dan beban kerja Anda.

Saat menggunakan Layanan AWS, Anda mempertahankan kontrol atas konten Anda. Secara khusus, konten pelanggan didefinisikan sebagai perangkat lunak (termasuk gambar mesin), data, teks, audio, video, atau gambar yang Anda atau pengguna akhir transfer kepada kami untuk diproses, disimpan, atau dihosting Layanan AWS sehubungan dengan akun Anda. Ini juga mencakup hasil komputasi apa pun yang Anda atau pengguna akhir dapatkan dengan menggunakan. Layanan AWS Anda bertanggung jawab untuk mengelola keputusan berikut, yang berada di bawah kendali Anda:

- Data yang Anda pilih untuk dikumpulkan, disimpan, atau diproses AWS
- Yang Layanan AWS Anda gunakan dengan data
- AWS Region Tempat Anda mengumpulkan, menyimpan, atau memproses data
- Format dan struktur data Anda dan apakah itu bertopeng, dianonimkan, atau dienkripsi
- Bagaimana Anda mendefinisikan, menyimpan, memutar, dan mengoperasikan kunci kriptografi Anda untuk enkripsi
- Siapa yang memiliki akses dan kapan mereka memiliki akses ke data Anda, dan bagaimana hak akses tersebut diberikan, dikelola, dan dicabut

Setelah Anda memahami model tanggung jawab AWS bersama dan bagaimana hal itu umumnya berlaku untuk beroperasi di cloud, Anda harus menentukan bagaimana hal itu berlaku untuk kasus penggunaan Anda. Layanan AWS Yang Anda pilih untuk digunakan menentukan jumlah konfigurasi yang harus Anda lakukan sebagai bagian dari tanggung jawab privasi organisasi Anda.

Misalnya, layanan seperti Amazon Elastic Compute Cloud (Amazon EC2) dikategorikan sebagai infrastruktur sebagai layanan (IaaS). Dengan demikian, jika Anda menggunakan Amazon EC2, Anda harus melakukan semua konfigurasi privasi yang diperlukan untuk sistem operasi tamu dan untuk perangkat lunak aplikasi atau utilitas yang Anda instal pada instans EC2 Anda. Saat Anda menggunakan layanan abstrak, seperti Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB, bertanggung jawab atas lapisan infrastruktur AWS , sistem operasi, dan platform. Tanggung jawab Anda adalah mengelola dan mengklasifikasikan data (konten pelanggan) dan mengonfigurasi kebijakan yang digunakan untuk mengakses titik akhir untuk menyimpan dan mengambil data. Untuk informasi selengkapnya tentang cara AWS membantu Anda melindungi data dan privasi, lihat Perlindungan dan privasi data di AWS.

Memahami AWS PRA

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Bagian ini menjelaskan hubungan antara Arsitektur Referensi AWS Privasi (AWS PRA) dan AWS panduan lainnya. Bagian ini juga mengulas tata letak umum dan struktur lingkungan AWS multi-akun contoh di AWS PRA.

Bagian ini berisi topik berikut:

- Menggunakan AWS PRA dan SRA AWS
- AWS Organizations dan struktur akun khusus
- Operasionalisasi layanan privasi AWS

Menggunakan AWS PRA dan SRA AWS

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

AWS PRA menyediakan pola yang menurut pelanggan bermanfaat dalam merencanakan kontrol privasi tingkat dasar dan aplikasi untuk infrastruktur dan beban kerja mereka. AWSAWS Security Reference Architecture (AWS SRA) menyediakan seperangkat pedoman untuk membangun arsitektur yang mengimplementasikan dan mendukung rangkaian kontrol keamanan yang tepat di seluruh AWS landing zone dan aplikasi Anda. Untuk menetapkan kontrol privasi yang dirinci dalam panduan ini, AWS PRA mengasumsikan banyak pedoman dasar dan struktur akun yang sama yang dijelaskan dalam SRA. AWS AWS PRA dan AWS SRA merinci banyak kunci yang sama. Layanan AWS Panduan ini hanya mencakup deskripsi singkat tentang layanan ini. Anda dapat mempelajari lebih lanjut tentang layanan ini dan bagaimana mereka digunakan dalam konteks keamanan di AWS SRA.

AWS SRA dapat membantu Anda merancang, menerapkan, dan mengelola layanan AWS keamanan sehingga selaras dengan praktik yang AWS direkomendasikan. Anda dapat menggunakan AWS SRA sebagai panduan mandiri, atau Anda dapat menggunakan AWS SRA dan AWS PRA sebagai panduan pendamping. Banyak pedoman keamanan yang dirinci dalam AWS SRA dapat diikuti bersama-sama dengan kontrol privasi yang dirinci dalam PRA. AWS Mirip dengan keamanan, ada pertimbangan privasi dasar yang dapat membantu untuk dilakukan di awal AWS Cloud perjalanan Anda karena keputusan ini dapat memengaruhi desain struktur akun organisasi. Misalnya, beberapa pertanyaan yang mungkin Anda pertimbangkan meliputi:

- Bagaimana organisasi saya mendefinisikan data pribadi?
- Apakah organisasi saya mendukung aplikasi yang memproses data pribadi?
- Bagaimana dengan aplikasi yang memproses jenis data lain yang diatur?
- Kontrol tingkat organisasi apa yang dapat saya terapkan untuk menjaga pengembang dan teknisi cloud saya sejauh mungkin dari data pribadi?
- Bagaimana cara memisahkan data pribadi dari jenis data lain?
- Apa persyaratan transfer data lintas batas organisasi saya?

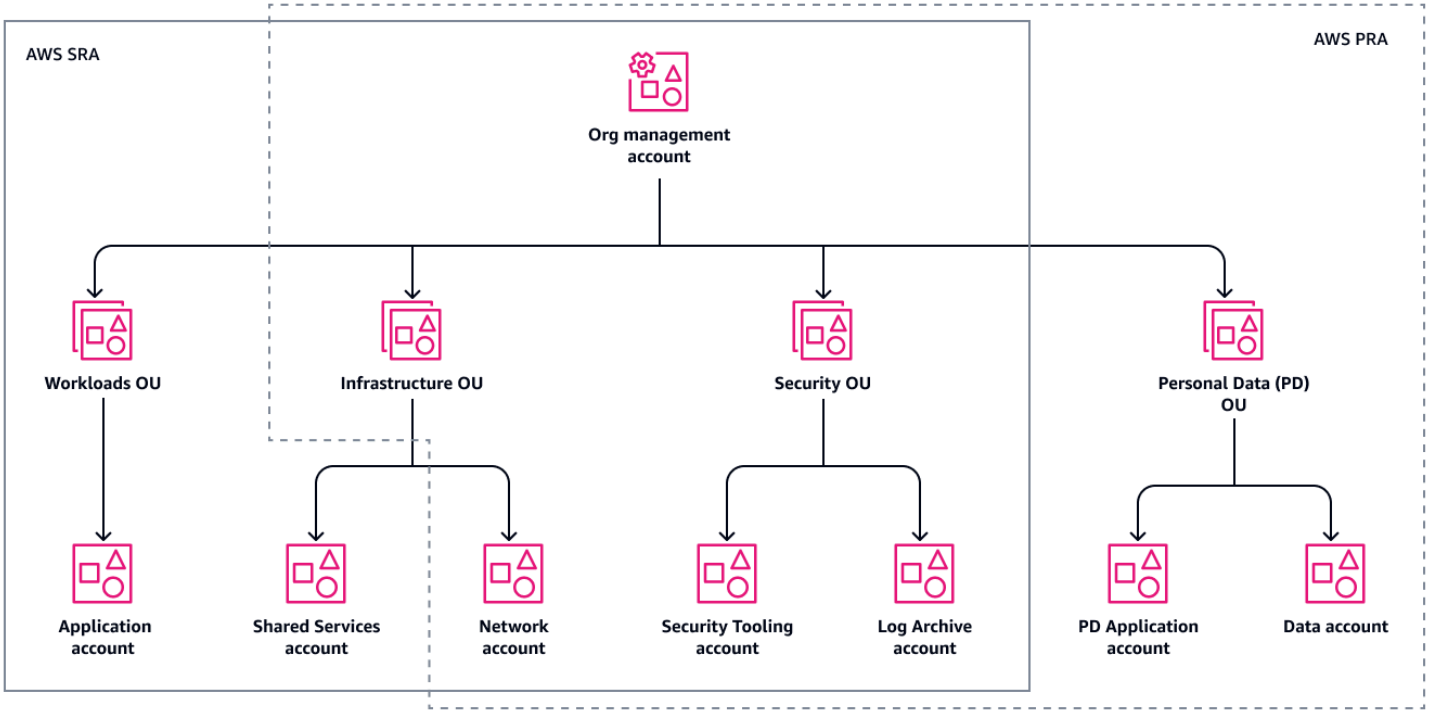
Jawaban atas banyak pertanyaan ini dapat berimplikasi pada desain lingkungan cloud Anda, seperti Akun AWS struktur Anda, kebijakan kontrol layanan, dan peran AWS Identity and Access Management (IAM).

AWS Organizations dan struktur akun khusus

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

AWS Organizationsadalah layanan manajemen akun yang membantu Anda mengelola dan mengatur beberapa secara terpusat. Akun AWS Penggunaan AWS Organizations adalah dasar dari lingkungan AWS multi-akun yang dirancang dengan baik. Untuk informasi selengkapnya, lihat Membangun AWS lingkungan praktik terbaik Anda.

Diagram berikut menunjukkan akun tingkat tinggi dan struktur unit organisasi (OU) dari AWS PRA. Sebagian besar, struktur organisasi AWS PRA cocok dengan struktur organisasi AWS SRA.



Penyimpangan dari organisasi AWS SRA meliputi:

- AWS PRA menambahkan Data Pribadi (PD) OU, yang didedikasikan untuk mengumpulkan, menyimpan, dan memproses data pribadi. Pemisahan struktural ini memberikan fleksibilitas sehingga Anda dapat menentukan kontrol spesifik dan berbutir halus untuk membantu melindungi data pribadi dari pengungkapan yang tidak diinginkan.
- Dalam Infrastruktur OU, AWS PRA saat ini tidak menyertakan panduan tambahan untuk akun Layanan Bersama yang dijelaskan dalam AWS SRA.
- AWS PRA saat ini tidak menyertakan panduan tambahan untuk Beban Kerja OU yang dijelaskan dalam SRA. AWS Aplikasi yang mengumpulkan atau memproses data pribadi terletak di akun khusus di PD OU.

Anda dapat menggunakan tata kelola dasar AWS Control Towersecara keseluruhan dan penerapan otomatis kontrol keamanan dan privasi di seluruh organisasi Anda. Jika AWS Control Tower tidak digunakan hari ini di organisasi Anda, Anda masih dapat menerapkan banyak kontrol keamanan dan privasi di AWS Control Tower, seperti kebijakan dan AWS Config aturan kontrol layanan, di layanan masing-masing.

Anda mungkin merasa terbantu untuk mempertimbangkan pemrosesan data pribadi saat merencanakan akun dan struktur OU Anda, termasuk strategi segmentasi akun. Anda mungkin

perlu mempertimbangkan jenis data yang Anda proses untuk kasus penggunaan unik mereka dan hukum dan peraturan yang berlaku. Misalnya, data pemegang kartu dilindungi berdasarkan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), dan informasi kesehatan yang dilindungi mungkin tunduk pada Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA). Anda mungkin ingin meninjau lingkungan mana yang berisi data pribadi dan merencanakan strategi segmentasi Anda untuk itu. Strategi segmentasi akun tipikal dapat mencakup dedicated Akun AWS yang selaras dengan siklus hidup pengembangan perangkat lunak (SDLC), seperti akun khusus untuk pengembangan, pementasan atau jaminan kualitas (QA), dan produksi. Strategi segmentasi seperti ini dapat menjadi komponen penting dalam diskusi desain keseluruhan, dan Anda OUs mungkin perlu menyelaraskan dengan persyaratan peraturan khusus Anda.

Beberapa AWS lingkungan multi-akun memerlukan akun aplikasi khusus per AWS Region, atau mereka mungkin memerlukan zona pendaratan multi-akun. Dalam hal ini, Anda memerlukan segmentasi tambahan untuk memenuhi persyaratan kedaulatan data unik untuk pelanggan dan regulator Anda. Untuk informasi selengkapnya, lihat Strategi untuk ekspansi global dalam panduan ini.

Operasionalisasi layanan privasi AWS

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Bagi banyak orang, privasi bersifat lintas sektoral. Banyak tim yang berbeda memiliki peran untuk dimainkan, termasuk tim regulasi, kepatuhan, dan teknik. Ketika organisasi Anda telah mulai menentukan orang-orang kunci dan komponen kebijakan dari program privasi Anda, Anda dapat memetakan kontrol terhadap kerangka kepatuhan privasi untuk operasi yang konsisten. Kerangka kerja dapat berfungsi sebagai rubrik untuk menerapkan kontrol privasi dasar dan khusus aplikasi untuk data pribadi di lingkungan Anda. AWS

Terlepas dari kerangka kerja yang digunakan pelanggan untuk mengkategorikan persyaratan privasi mereka, kepatuhan privasi, rekayasa privasi, dan tim aplikasi sering kali perlu bekerja sama untuk mencapai tujuan implementasi. Misalnya, tim regulasi dan kepatuhan mungkin menyediakan persyaratan tingkat tinggi, dan tim teknik dan aplikasi mengonfigurasi Layanan AWS dan fitur untuk menyelaraskan dengan persyaratan ini. Dimulai dengan kerangka kerja kontrol dapat membantu Anda menentukan kontrol organisasi dan teknis yang lebih preskriptif.

Ketika mendefinisikan kontrol teknis Layanan AWS dan fitur, keputusan kunci lainnya adalah apakah kontrol harus berlaku untuk seluruh organisasi, OU, akun, atau sumber daya tertentu. Beberapa layanan dan fitur sangat cocok untuk menerapkan kontrol di seluruh AWS organisasi Anda. Misalnya, memblokir akses publik ke bucket Amazon S3 adalah kontrol khusus yang sebaiknya dikonfigurasi di root organisasi daripada secara individual untuk setiap akun. Namun, kebijakan retensi Anda mungkin berbeda dari satu aplikasi ke aplikasi lainnya, yang berarti Anda dapat menerapkan kontrol di tingkat sumber daya.

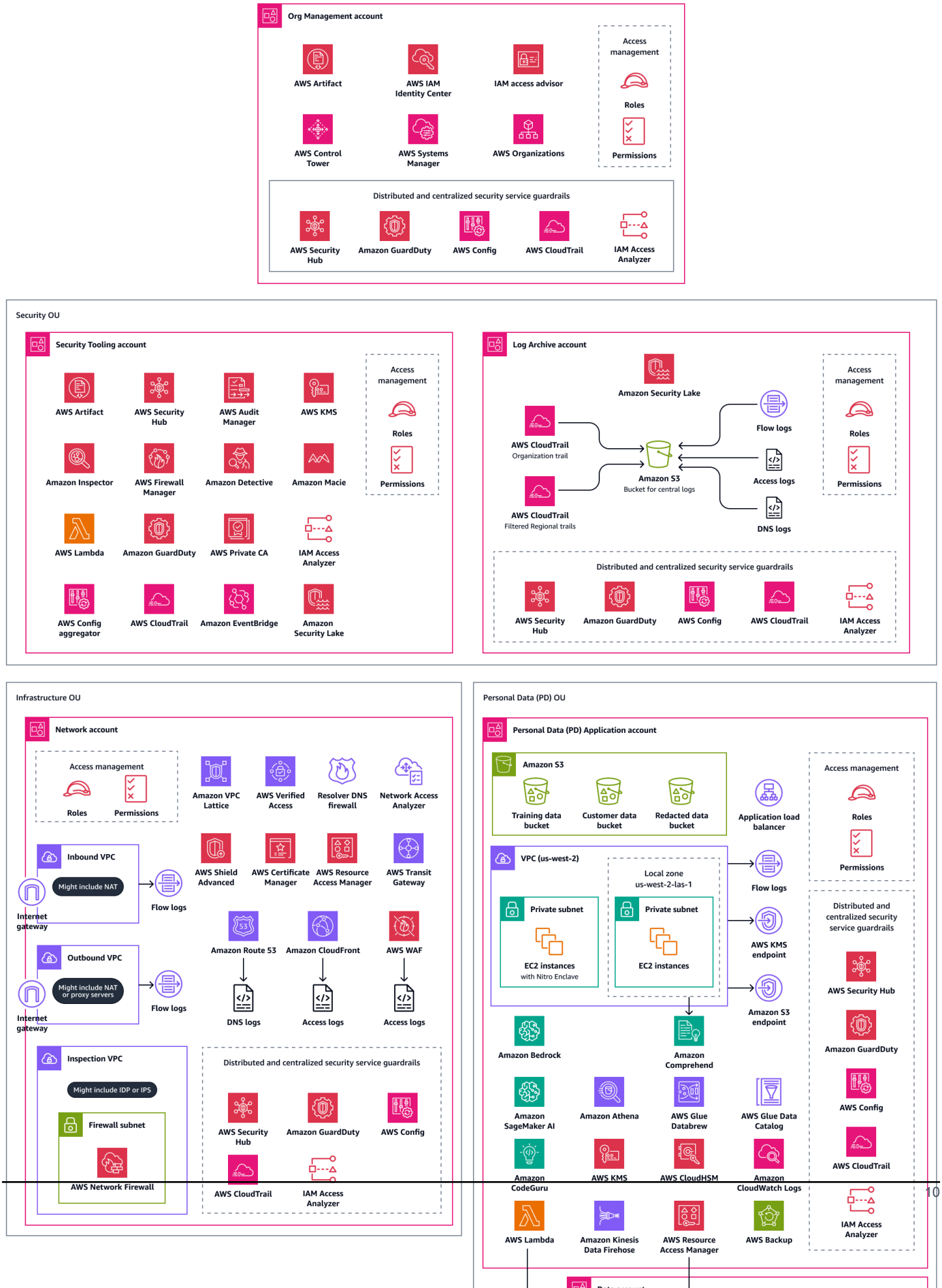
Untuk membantu Anda mempercepat operasionalisasi privasi di organisasi Anda, AWS menawarkan layanan konsultasi audit dan kepatuhan untuk beban kerja Anda. AWS Untuk informasi lebih lanjut, hubungi AWS SAS.

Arsitektur Referensi AWS Privasi

Survei

Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Diagram berikut menggambarkan Arsitektur Referensi AWS Privasi (AWS PRA). Ini adalah contoh arsitektur yang menghubungkan banyak fitur dan terkait privasi Layanan AWS . Arsitektur ini dibangun di atas landing zone yang diatur oleh AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Access logs
Amazon S3
Bucket for central logs
AWS CloudTrail
Filtered Regional trails
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

AWS PRA mencakup arsitektur web tanpa server yang di-host di akun Aplikasi Data Pribadi (PD). Arsitektur dalam akun ini adalah contoh beban kerja yang mengumpulkan data pribadi langsung dari konsumen. Dalam beban kerja ini, pengguna terhubung melalui tingkat web. Tingkat web berinteraksi dengan tingkat aplikasi. Tingkat ini menerima input dari tingkat web, memproses dan menyimpan data, memungkinkan tim internal yang berwenang dan pihak ketiga untuk mengakses data, dan akhirnya mengarsipkan dan menghapus data ketika tidak lagi diperlukan. Arsitekturnya sengaja modular dan didorong oleh peristiwa untuk menunjukkan banyak teknik rekayasa privasi dasar tanpa mempelajari kasus penggunaan tertentu, seperti data lake, container, compute, atau Internet of Things (IoT).

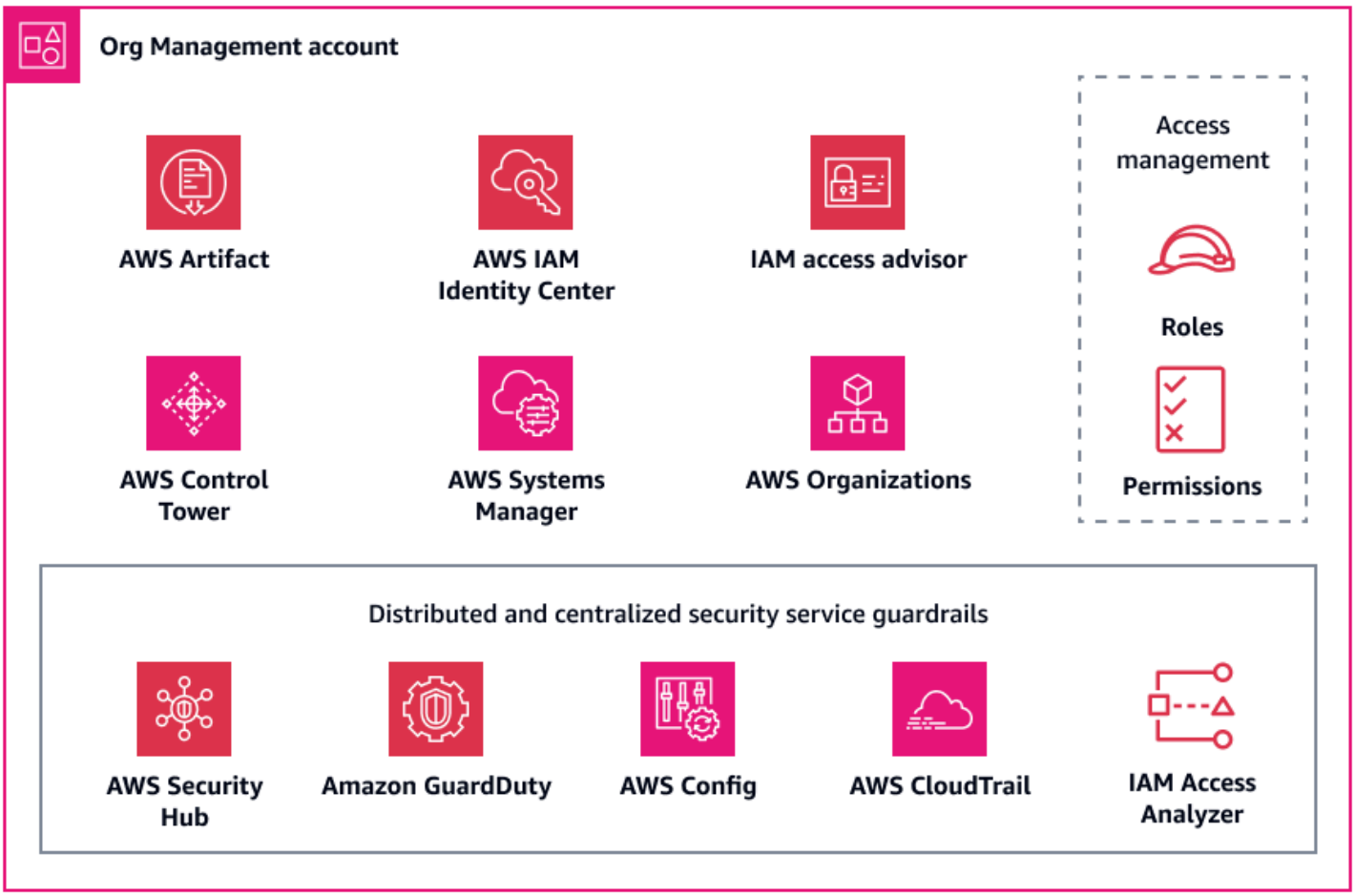
Selanjutnya, panduan ini menjelaskan setiap akun dalam organisasi secara rinci. Ini membahas layanan dan fitur terkait privasi, pertimbangan dan rekomendasi, dan diagram untuk masing-masing akun berikut:

- Akun Manajemen Org
- Security OU - Akun Perkakas Keamanan
- Keamanan OU - Akun Arsip Log
- Infrastruktur OU - Akun jaringan
- Data Pribadi OU - Akun Aplikasi PD

Akun Manajemen Org

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Akun Manajemen Org terutama digunakan untuk mengelola penyimpangan konfigurasi sumber daya untuk kontrol privasi dasar di semua akun di organisasi Anda, yang dikelola oleh. AWS Organizations Akun ini juga merupakan tempat Anda dapat menyebarkan akun anggota baru secara konsisten, dengan banyak kontrol keamanan dan privasi yang sama. Untuk informasi selengkapnya tentang akun ini, lihat Arsitektur Referensi AWS Keamanan (AWS SRA). Diagram berikut menggambarkan layanan AWS keamanan dan privasi yang dikonfigurasi di akun Manajemen Org.



Bagian ini memberikan informasi lebih rinci tentang hal-hal berikut Layanan AWS yang digunakan dalam akun ini:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifactdapat membantu Anda dengan audit dengan menyediakan unduhan sesuai permintaan dokumen AWS keamanan dan kepatuhan. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Ini Layanan AWS membantu Anda memahami kontrol yang Anda warisi AWS dan menentukan kontrol apa yang mungkin tersisa untuk Anda terapkan di lingkungan Anda. AWS Artifact menyediakan akses ke laporan AWS keamanan dan kepatuhan, seperti laporan Sistem dan Kontrol

Organisasi (SOC) dan laporan industri kartu pembayaran (PCI). Ini juga menyediakan akses ke sertifikasi dari badan akreditasi di seluruh geografi dan vertikal kepatuhan yang memvalidasi implementasi dan efektivitas operasi kontrol. AWS Dengan menggunakan AWS Artifact, Anda dapat memberikan artefak AWS audit kepada auditor atau regulator Anda sebagai bukti kontrol AWS keamanan dan privasi. Laporan berikut mungkin berguna untuk menunjukkan efektivitas kontrol AWS privasi:

- Laporan Privasi SOC 2 Tipe 2 — Laporan ini menunjukkan efektivitas AWS kontrol untuk bagaimana data pribadi dikumpulkan, digunakan, disimpan, diungkapkan, dan dibuang. Ada juga laporan Privasi SOC 3, yang merupakan deskripsi yang kurang rinci tentang kontrol privasi SOC 2. Untuk informasi lebih lanjut, lihat SOC FAQ.
- Cloud Computing Compliance Controls Catalog (C5) — Laporan ini dibuat oleh otoritas keamanan siber nasional Jerman, Bundesamt für Sicherheit in der Informationstechnik (BSI). Ini merinci kontrol keamanan yang AWS diterapkan untuk memenuhi persyaratan C5. Ini juga mencakup persyaratan kontrol tambahan untuk privasi yang berkaitan dengan lokasi data, penyediaan layanan, tempat yurisdiksi, dan kewajiban pengungkapan informasi.
- Laporan sertifikasi ISO/IEC 27701:2019 — ISO/IEC 27701:2019 menjelaskan persyaratan dan pedoman untuk menetapkan dan terus meningkatkan sistem manajemen informasi privasi (PIMS). Laporan ini merinci ruang lingkup sertifikasi ini dan dapat berfungsi sebagai bukti AWS sertifikasi. Untuk informasi lebih lanjut tentang standar ini, lihat ISO/IEC 27701:2019 (situs web ISO).

AWS Control Tower

AWS Control Towermembantu Anda mengatur dan mengatur lingkungan AWS multi-akun yang mengikuti praktik yang direkomendasikan keamanan preskriptif. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Di AWS Control Tower, Anda juga dapat mengotomatiskan penyebaran banyak kontrol proaktif, preventif, dan detektif, juga dikenal sebagai pagar pembatas, yang selaras dengan persyaratan privasi data Anda, khusus untuk residensi dan kedaulatan data. Misalnya, Anda dapat menentukan pagar pembatas yang membatasi transfer data hanya disetujui. Wilayah AWSUntuk kontrol yang lebih terperinci, Anda dapat memilih dari lebih dari 17 pagar pembatas yang dirancang untuk mengontrol residensi data, seperti Larang koneksi Jaringan Pribadi Virtual Amazon (VPN), Larang akses internet untuk instance VPC Amazon, dan Tolak akses berdasarkan permintaan. AWS AWS Region Pagar pembatas ini terdiri dari sejumlah AWS CloudFormation kait, kebijakan kontrol layanan, dan AWS Config aturan yang dapat diterapkan secara seragam di seluruh organisasi Anda. Untuk

informasi selengkapnya, lihat Kontrol yang meningkatkan perlindungan residensi data dalam AWS Control Tower dokumentasi.

Untuk kedaulatan data, AWS Control Tower saat ini menyediakan kontrol pencegahan, seperti Mengharuskan volume Amazon EBS terlampir dikonfigurasi untuk mengenkripsi data saat istirahat dan Memerlukan kebijakan AWS KMS utama untuk memiliki pernyataan yang membatasi pembuatan hibah. AWS KMS Layanan AWS Kontrol kedaulatan lebih luas dari sekedar kontrol residensi data. Mereka membantu mencegah tindakan yang mungkin melanggar residensi data, pembatasan akses terperinci, enkripsi, dan persyaratan ketahanan. Untuk informasi lebih lanjut, lihat Kontrol pencegahan yang membantu kedaulatan digital dalam dokumentasi. AWS Control Tower

Jika Anda perlu menerapkan pagar pembatas privasi di luar kontrol residensi dan kedaulatan data, sertakan sejumlah kontrol wajib. AWS Control Tower Kontrol ini diterapkan secara default di setiap OU saat Anda mengatur landing zone. Banyak di antaranya adalah kontrol pencegahan yang dirancang untuk melindungi log, seperti Larang Penghapusan Arsip Log dan Aktifkan Validasi Integritas untuk File Log. CloudTrail

AWS Control Tower juga terintegrasi dengan AWS Security Hub CSPM untuk menyediakan kontrol detektif. Kontrol ini dikenal sebagai Standar yang Dikelola Layanan:. AWS Control Tower Anda dapat menggunakan kontrol ini untuk memantau penyimpangan konfigurasi kontrol pendukung privasi, seperti enkripsi saat istirahat untuk instans database Amazon Relational Database Service (Amazon RDS).

AWS Organizations

AWS PRA menggunakan AWS Organizations untuk mengelola semua akun dalam arsitektur secara terpusat. Untuk informasi selengkapnya, lihat AWS Organizations dan struktur akun khusus dalam panduan ini. Di AWS Organizations, Anda dapat menggunakan kebijakan kontrol layanan (SCPs) dan kebijakan manajemen untuk membantu melindungi data pribadi dan privasi.

Kebijakan kontrol layanan (SCPs)

Kebijakan kontrol layanan (SCPs) adalah jenis kebijakan organisasi yang dapat Anda gunakan untuk mengelola izin di organisasi Anda. Mereka memberikan kontrol terpusat atas izin maksimum yang tersedia untuk peran AWS Identity and Access Management (IAM) dan pengguna di akun target, unit organisasi (OU), atau seluruh organisasi. Anda dapat membuat dan mendaftar SCPs dari akun Manajemen Org.

Anda dapat menggunakan AWS Control Tower untuk menyebarkan SCPs secara seragam di seluruh akun Anda. Untuk informasi lebih lanjut tentang kontrol residensi data yang dapat Anda

terapkan AWS Control Tower, lihat AWS Control Tower di panduan ini. AWS Control Tower termasuk pelengkap penuh pencegahan SCPs. Jika saat ini AWS Control Tower tidak digunakan di organisasi, Anda juga dapat menerapkan kontrol ini secara manual.

Menggunakan SCPs untuk mengatasi persyaratan residensi data

Adalah umum untuk mengelola persyaratan residensi data pribadi dengan menyimpan dan memproses data dalam wilayah geografis tertentu. Untuk memverifikasi bahwa persyaratan residensi data unik yurisdiksi terpenuhi, kami menyarankan Anda bekerja sama dengan tim pengatur Anda untuk mengonfirmasi persyaratan Anda. Ketika persyaratan ini telah ditentukan, ada sejumlah kontrol privasi AWS dasar yang dapat membantu mendukung. Misalnya, Anda dapat menggunakan SCPs untuk membatasi yang Wilayah AWS dapat digunakan untuk memproses dan menyimpan data. Untuk contoh kebijakan, lihat Batasi transfer data di seluruh Wilayah AWS di panduan ini.

Menggunakan SCPs untuk membatasi panggilan API berisiko tinggi

Penting untuk memahami kontrol keamanan dan privasi mana yang AWS bertanggung jawab atas dan mana yang menjadi tanggung jawab Anda. Misalnya, Anda bertanggung jawab atas hasil panggilan API yang dapat dilakukan terhadap Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab untuk memahami panggilan mana yang dapat mengakibatkan perubahan pada postur keamanan atau privasi Anda. Jika Anda khawatir tentang mempertahankan postur keamanan dan privasi tertentu, Anda dapat SCPs mengaktifkannya menolak panggilan API tertentu. Panggilan API ini mungkin memiliki implikasi, seperti pengungkapan data pribadi yang tidak diinginkan atau pelanggaran transfer data lintas batas tertentu. Misalnya, Anda mungkin ingin melarang panggilan API berikut:

- Mengaktifkan akses publik ke bucket Amazon Simple Storage Service (Amazon S3)
- Menonaktifkan Amazon GuardDuty atau membuat aturan penekanan untuk temuan eksfiltrasi data, seperti temuan Trojan: EC2/Ekfiltrasi DNSData
- Menghapus aturan AWS WAF eksfiltrasi data
- Berbagi snapshot Amazon Elastic Block Store (Amazon EBS) secara publik
- Menghapus akun anggota dari organisasi
- Memisahkan Amazon CodeGuru Reviewer dari repositori

Kebijakan pengelolaan

Kebijakan manajemen AWS Organizations dapat membantu Anda mengonfigurasi Layanan AWS dan mengelola secara terpusat serta fitur-fiturnya. Jenis kebijakan manajemen yang Anda pilih

menentukan bagaimana kebijakan memengaruhi OUs dan akun yang mewarisinya. Kebijakan tag adalah contoh kebijakan manajemen AWS Organizations yang berhubungan langsung dengan privasi.

Menggunakan kebijakan tag

Tag adalah pasangan nilai kunci yang membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter AWS sumber daya. Hal ini dapat berguna untuk menerapkan tag yang membedakan sumber daya di organisasi Anda yang menangani data pribadi. Penggunaan tag mendukung banyak solusi privasi dalam panduan ini. Misalnya, Anda mungkin ingin menerapkan tag yang menunjukkan klasifikasi data umum dari data yang sedang diproses atau disimpan dalam sumber daya. Anda dapat menulis kebijakan kontrol akses berbasis atribut (ABAC) yang membatasi akses ke sumber daya yang memiliki tag atau kumpulan tag tertentu. Misalnya, kebijakan Anda mungkin menentukan bahwa `SysAdmin` peran tidak dapat mengakses sumber daya yang memiliki `dataclassification:4` tag. Untuk informasi selengkapnya dan tutorial, lihat Menentukan izin untuk mengakses AWS sumber daya berdasarkan tag dalam dokumentasi IAM. Selain itu, jika organisasi Anda menggunakan AWS Backupuntuk menerapkan kebijakan penyimpanan data secara luas di seluruh pencadangan di banyak akun, Anda dapat menerapkan tag yang menempatkan sumber daya tersebut dalam cakupan kebijakan pencadangan tersebut.

Kebijakan tag membantu Anda mempertahankan tag yang konsisten di seluruh organisasi Anda. Dalam kebijakan tag, Anda menentukan aturan yang berlaku untuk sumber daya saat diberi tag. Misalnya, Anda dapat meminta sumber daya untuk diberi tag dengan kunci tertentu, seperti `DataClassification` atau`DataSteward`, dan Anda dapat menentukan perlakuan kasus atau nilai yang valid untuk kunci. Anda juga dapat menggunakan penegakan hukum untuk mencegah permintaan penandaan yang tidak sesuai selesai.

Saat menggunakan tag sebagai komponen inti dari strategi kontrol privasi Anda, pertimbangkan hal berikut:

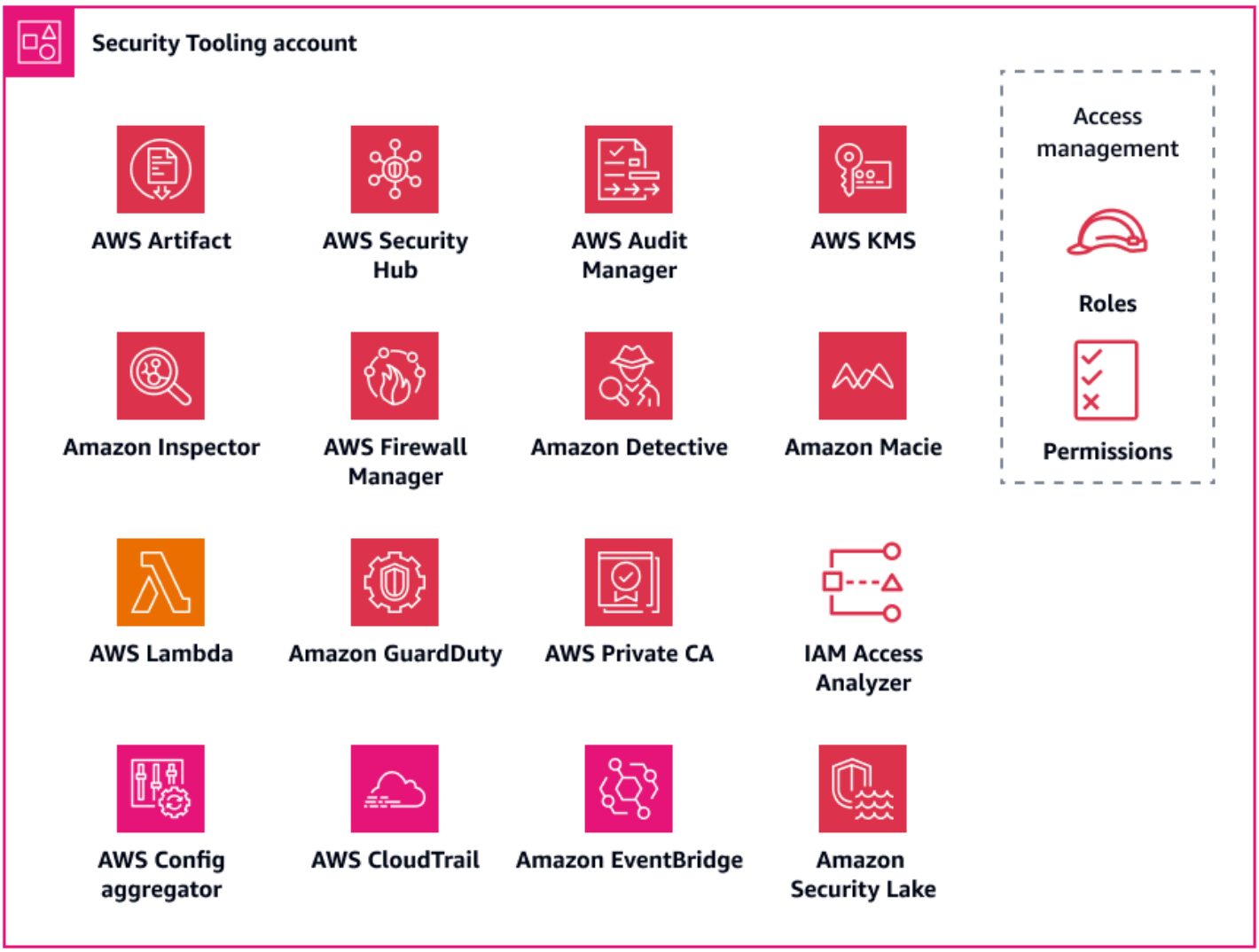
- Pertimbangkan implikasi penempatan data pribadi atau jenis data sensitif lainnya dalam kunci atau nilai tag. Ketika Anda menghubungi AWS untuk bantuan teknis, AWS mungkin menganalisis tag dan pengenal sumber daya lainnya untuk membantu menyelesaikan masalah. Data tag tidak dienkripsi, dan, seperti Layanan AWS AWS Manajemen Penagihan dan Biaya, dapat membacanya. Oleh karena itu, Anda mungkin ingin membatalkan identifikasi nilai tag dan kemudian mengidentifikasinya kembali dengan menggunakan sistem yang Anda kontrol, seperti sistem manajemen layanan TI (ITSM). AWS merekomendasikan untuk tidak memasukkan informasi yang dapat diidentifikasi secara pribadi dalam tag.

- Pertimbangkan bahwa beberapa nilai tag perlu dibuat tidak berubah (tidak dapat dimodifikasi) untuk mencegah pengelakan kontrol teknis, seperti kondisi ABAC yang bergantung pada tag.

Security OU - Akun Perkakas Keamanan

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Akun Security Tooling didedikasikan untuk mengoperasikan layanan dasar keamanan dan privasi, pemantauan Akun AWS, dan otomatisasi peringatan dan respons keamanan dan privasi. Untuk informasi selengkapnya tentang akun ini, lihat Arsitektur Referensi AWS Keamanan (AWS SRA). Diagram berikut menggambarkan layanan AWS keamanan dan privasi yang dikonfigurasi di akun Security Tooling.



Bagian ini memberikan informasi lebih rinci tentang hal-hal berikut di akun ini:

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrailmembantu Anda mengaudit aktivitas API secara keseluruhan di Anda Akun AWS. Mengaktifkan CloudTrail semua Akun AWS penyimpanan, proses, atau pengiriman data

pribadi dapat membantu Anda melacak penggunaan dan pengungkapan data ini. Wilayah AWS Arsitektur Referensi AWS Keamanan merekomendasikan untuk mengaktifkan jejak organisasi, yang merupakan jejak tunggal yang mencatat semua peristiwa untuk semua akun di organisasi. Namun, mengaktifkan jejak organisasi ini menggabungkan data log Multi-wilayah ke dalam satu bucket Amazon Simple Storage Service (Amazon S3) di akun Arsip Log. Untuk akun yang menangani data pribadi, ini dapat membawa beberapa pertimbangan desain tambahan. Catatan log mungkin berisi beberapa referensi ke data pribadi. Untuk memenuhi persyaratan residensi data dan transfer data, Anda mungkin perlu mempertimbangkan kembali penggabungan data log Lintas wilayah ke dalam satu Wilayah tempat bucket S3 berada. Organisasi Anda mungkin mempertimbangkan beban kerja regional mana yang harus dimasukkan atau dikecualikan dari jejak organisasi. Untuk beban kerja yang Anda putuskan untuk dikecualikan dari jejak organisasi, Anda dapat mempertimbangkan untuk mengonfigurasi jejak khusus Wilayah yang menutupi data pribadi. Untuk informasi selengkapnya tentang menutupi data pribadi, lihat Amazon Data Firehose bagian panduan ini. Pada akhirnya, organisasi Anda mungkin memiliki kombinasi jejak organisasi dan jalur regional yang digabungkan ke dalam akun Arsip Log terpusat.

Untuk informasi selengkapnya tentang mengonfigurasi jejak wilayah Tunggal, lihat petunjuk penggunaan AWS Command Line Interface (AWS CLI) atau konsol. Saat membuat jejak organisasi, Anda dapat menggunakan setelan keikutsertaan AWS Control Tower, atau Anda dapat membuat jejak langsung di CloudTrail konsol.

Untuk informasi lebih lanjut tentang pendekatan keseluruhan dan cara mengelola sentralisasi log dan persyaratan transfer data, lihat Penyimpanan log terpusat bagian dalam panduan ini. Konfigurasi apa pun yang Anda pilih, Anda mungkin ingin memisahkan manajemen jejak di akun Security Tooling dari penyimpanan log di akun Arsip Log, menurut AWS SRA. Desain ini membantu Anda membuat kebijakan akses hak istimewa paling sedikit bagi mereka yang perlu mengelola log dan mereka yang perlu menggunakan data log.

AWS Config

AWS Configmemberikan tampilan rinci tentang sumber daya di Anda Akun AWS dan bagaimana mereka dikonfigurasi. Ini membantu Anda mengidentifikasi bagaimana sumber daya berhubungan satu sama lain dan bagaimana konfigurasi mereka telah berubah dari waktu ke waktu. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Di AWS Config, Anda dapat menerapkan paket kesesuaian, yang merupakan seperangkat AWS Config aturan dan tindakan remediasi. Paket kesesuaian menyediakan kerangka kerja tujuan umum

yang dirancang untuk memungkinkan pemeriksaan tata kelola privasi, keamanan, operasional, dan pengoptimalan biaya dengan menggunakan aturan terkelola atau khusus. AWS Config Anda dapat menggunakan alat ini sebagai bagian dari seperangkat alat otomatisasi yang lebih besar untuk melacak apakah konfigurasi AWS sumber daya Anda sesuai dengan persyaratan kerangka kerja kontrol Anda sendiri.

Paket kesesuaian Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0 diselaraskan dengan sejumlah kontrol terkait privasi dalam Kerangka Privasi NIST. Setiap AWS Config aturan berlaku untuk jenis AWS sumber daya tertentu, dan ini terkait dengan satu atau lebih kontrol Kerangka Privasi NIST. Anda dapat menggunakan paket kesesuaian ini untuk melacak kepatuhan berkelanjutan terkait privasi di seluruh sumber daya di akun Anda. Berikut ini adalah beberapa aturan yang termasuk dalam paket kesesuaian ini:

- `no-unrestricted-route-to-igw`— Aturan ini membantu mencegah eksfiltrasi data pada bidang data dengan terus memantau tabel rute VPC untuk rute default `0.0.0.0/0` atau jalan keluar ke `::/0` gateway internet. Ini membantu Anda membatasi di mana lalu lintas internet dapat dikirim, terutama jika ada rentang CIDR yang diketahui berbahaya.
- `encrypted-volumes`— Aturan ini memeriksa apakah volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) dienkripsi. Jika organisasi Anda memiliki persyaratan kontrol khusus yang berkaitan dengan penggunaan kunci AWS Key Management Service (AWS KMS) untuk perlindungan data pribadi, Anda dapat menentukan kunci tertentu IDs sebagai bagian dari aturan untuk memeriksa apakah volume dienkripsi dengan kunci tertentu. AWS KMS
- `restricted-common-ports`— Aturan ini memeriksa apakah grup keamanan Amazon EC2 mengizinkan lalu lintas TCP yang tidak dibatasi ke port tertentu. Grup keamanan dapat membantu Anda mengelola akses jaringan dengan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Memblokir lalu lintas masuk dari `0.0.0.0/0` port umum, seperti TCP 3389 dan TCP 21, pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

AWS Config dapat digunakan untuk pemeriksaan kepatuhan proaktif dan reaktif sumber daya Anda AWS . Selain mempertimbangkan aturan yang ditemukan dalam paket kesesuaian, Anda dapat memasukkan aturan ini dalam mode evaluasi detektif dan proaktif. Ini membantu menerapkan pemeriksaan privasi sebelumnya dalam siklus hidup pengembangan perangkat lunak Anda karena pengembang aplikasi dapat mulai memasukkan pemeriksaan predeployment. Misalnya, mereka dapat menyertakan kait dalam AWS CloudFormation templat mereka yang memeriksa sumber

daya yang dideklarasikan dalam templat terhadap semua AWS Config aturan terkait privasi yang mengaktifkan mode proaktif. Untuk informasi selengkapnya, lihat AWS Config Aturan Sekarang Mendukung Kepatuhan Proaktif (posting AWS blog).

Amazon GuardDuty

AWS menawarkan beberapa layanan yang mungkin digunakan untuk menyimpan atau memproses data pribadi, seperti Amazon S3, Amazon Relational Database Service (Amazon RDS), atau Amazon EC2 dengan Kubernetes. Amazon GuardDuty menggabungkan visibilitas cerdas dengan pemantauan berkelanjutan untuk mendeteksi indikator yang mungkin terkait dengan pengungkapan data pribadi yang tidak diinginkan. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Dengan GuardDuty, Anda dapat mengidentifikasi aktivitas yang berpotensi berbahaya dan terkait privasi di seluruh siklus hidup serangan. Misalnya, GuardDuty dapat mengingatkan Anda tentang koneksi ke situs yang masuk daftar hitam, lalu lintas port jaringan atau volume lalu lintas yang tidak biasa, eksfiltrasi DNS, peluncuran instans EC2 yang tidak terduga, dan penelepon ISP yang tidak biasa. Anda juga dapat mengonfigurasi GuardDuty untuk menghentikan peringatan untuk alamat IP tepercaya dari daftar IP tepercaya Anda sendiri dan memberi tahu alamat IP berbahaya yang diketahui dari daftar ancaman Anda sendiri.

Seperti yang direkomendasikan dalam AWS SRA, Anda dapat mengaktifkan GuardDuty untuk semua Akun AWS di organisasi Anda dan mengonfigurasi akun Security Tooling sebagai administrator yang GuardDuty didelegasikan. GuardDutymengumpulkan temuan dari seluruh organisasi ke dalam akun tunggal ini. Untuk informasi selengkapnya, lihat Mengelola GuardDuty akun dengan AWS Organizations. Anda juga dapat mempertimbangkan untuk mengidentifikasi semua pemangku kepentingan terkait privasi dalam proses respons insiden, mulai dari deteksi dan analisis hingga penahanan dan pemberantasan, dan melibatkan mereka dalam insiden apa pun yang mungkin melibatkan eksfiltrasi data.

IAM Access Analyzer

Banyak pelanggan menginginkan jaminan terus-menerus bahwa data pribadi dibagikan secara tepat dengan pemroses pihak ketiga yang telah disetujui sebelumnya dan dimaksudkan dan tidak ada entitas lain. Perimeter data adalah seperangkat pagar pembatas pencegahan yang dirancang untuk memungkinkan hanya identitas tepercaya dari jaringan yang diharapkan untuk mengakses sumber daya tepercaya di lingkungan Anda. AWS Saat Anda menentukan kontrol untuk pengungkapan data pribadi yang tidak diinginkan dan dimaksudkan, Anda dapat menentukan identitas tepercaya, sumber daya tepercaya, dan jaringan yang diharapkan.

Dengan AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), organisasi dapat menentukan Akun AWS zona kepercayaan dan mengonfigurasi peringatan untuk pelanggaran terhadap zona kepercayaan tersebut. IAM Access Analyzer menganalisis kebijakan IAM untuk membantu mengidentifikasi dan menyelesaikan akses publik atau lintas akun yang tidak diinginkan ke sumber daya yang berpotensi sensitif. IAM Access Analyzer menggunakan logika matematika dan inferensi untuk menghasilkan temuan komprehensif untuk sumber daya yang dapat diakses dari luar. Akun AWS Terakhir, untuk menanggapi dan memulihkan kebijakan IAM yang terlalu permisif, Anda dapat menggunakan IAM Access Analyzer untuk memvalidasi kebijakan yang ada terhadap praktik yang direkomendasikan IAM dan memberikan saran. IAM Access Analyzer dapat menghasilkan kebijakan IAM dengan hak istimewa paling sedikit yang didasarkan pada aktivitas akses sebelumnya oleh kepala sekolah IAM. Ini menganalisis CloudTrail log dan menghasilkan kebijakan yang hanya memberikan izin yang diperlukan untuk terus melakukan tugas tersebut.

Untuk informasi selengkapnya tentang cara IAM Access Analyzer digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Amazon Macie

Amazon Macie adalah layanan yang menggunakan pembelajaran mesin dan pencocokan pola untuk menemukan data sensitif, memberikan visibilitas terhadap risiko keamanan data, dan membantu Anda mengotomatiskan perlindungan terhadap risiko tersebut. Macie menghasilkan temuan saat mendeteksi potensi pelanggaran kebijakan atau masalah dengan keamanan atau privasi bucket Amazon S3 Anda. Macie adalah alat lain yang dapat digunakan organisasi untuk menerapkan otomatisasi guna mendukung upaya kepatuhan. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Macie dapat mendeteksi daftar tipe data sensitif yang besar dan terus bertambah, termasuk informasi identitas pribadi (PII), seperti nama, alamat, dan atribut lain yang dapat diidentifikasi. Anda bahkan dapat membuat pengidentifikasi data khusus untuk menentukan kriteria deteksi yang mencerminkan definisi data pribadi organisasi Anda.

Saat organisasi Anda menetapkan kontrol pencegahan untuk bucket Amazon S3 Anda yang berisi data pribadi, Anda dapat menggunakan Macie sebagai mekanisme validasi untuk memberikan jaminan berkelanjutan tentang tempat data pribadi Anda berada dan bagaimana data tersebut dilindungi. Untuk memulai, aktifkan Macie dan konfigurasikan penemuan data sensitif otomatis. Macie terus menganalisis objek di semua bucket S3 Anda, di seluruh akun dan. Wilayah AWS Macie menghasilkan dan memelihara peta panas interaktif yang menggambarkan di mana data pribadi berada. Fitur penemuan data sensitif otomatis dirancang untuk mengurangi biaya dan

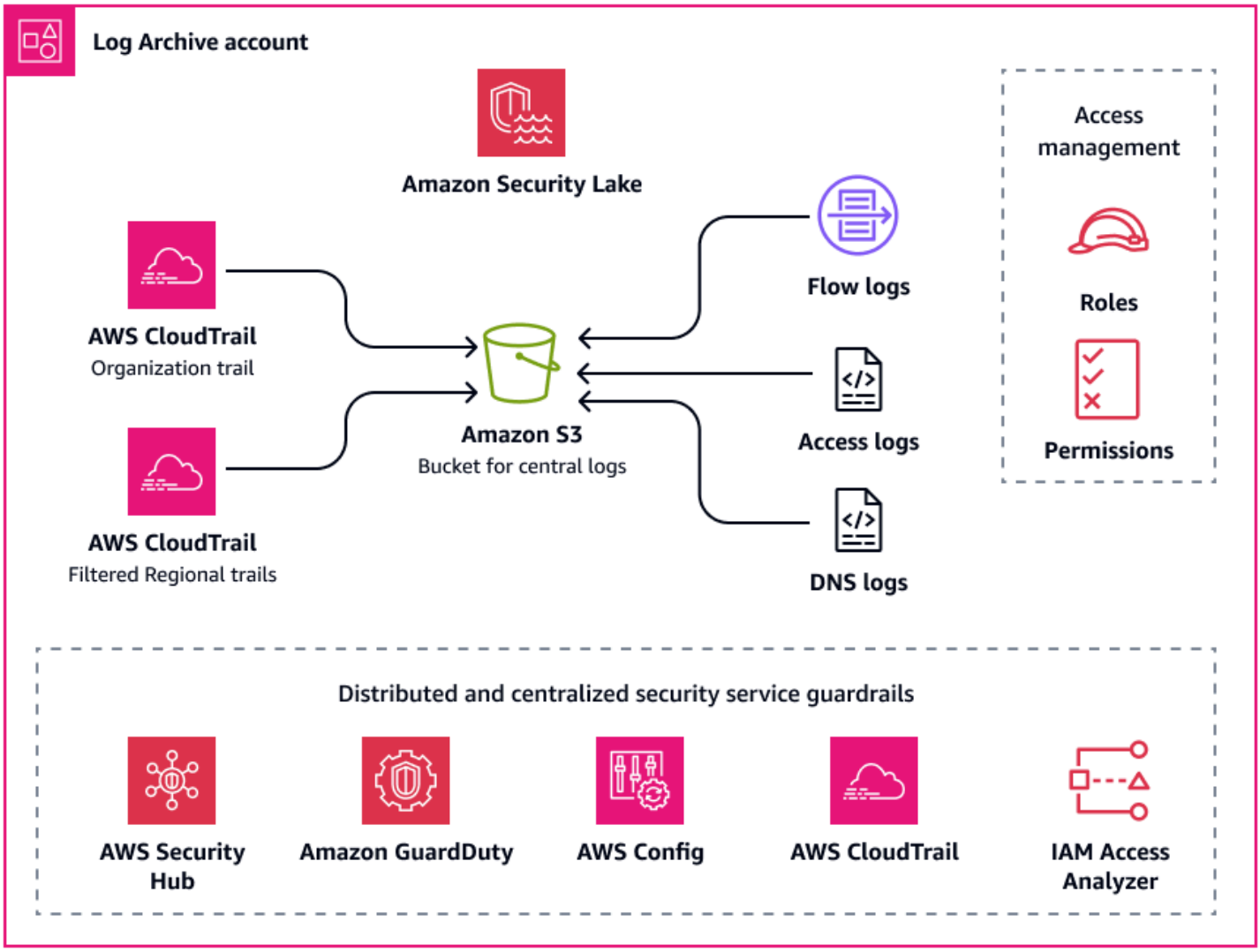
meminimalkan kebutuhan untuk mengonfigurasi pekerjaan penemuan secara manual. Anda dapat membangun di atas fitur penemuan data sensitif otomatis dan menggunakan Macie untuk secara otomatis mendeteksi bucket baru atau data baru di bucket yang ada dan kemudian memvalidasi data terhadap tag klasifikasi data yang ditetapkan. Konfigurasikan arsitektur ini untuk memberi tahu tim pengembangan dan privasi yang sesuai tentang bucket yang salah diklasifikasikan atau tidak diklasifikasikan secara tepat waktu.

Anda dapat mengaktifkan Macie untuk setiap akun di organisasi Anda dengan menggunakan AWS Organizations. Untuk informasi selengkapnya, lihat Mengintegrasikan dan mengonfigurasi organisasi di Amazon Macie.

Keamanan OU - Akun Arsip Log

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Akun Log Archive adalah tempat Anda memusatkan infrastruktur, layanan, dan jenis log aplikasi. Untuk informasi selengkapnya tentang akun ini, lihat Arsitektur Referensi AWS Keamanan (AWS SRA). Dengan akun khusus untuk log, Anda dapat menerapkan peringatan yang konsisten di semua jenis log dan untuk mengonfirmasi bahwa responden insiden dapat mengakses agregat log ini dari satu tempat. Anda dapat mengatur kontrol keamanan dan kebijakan penyimpanan data dari satu tempat juga, yang dapat menyederhanakan overhead operasional privasi. Diagram berikut menggambarkan layanan AWS keamanan dan privasi yang dikonfigurasi di akun Arsip Log.



Penyimpanan log terpusat

File log (seperti AWS CloudTrail log) mungkin berisi informasi yang dapat dianggap sebagai data pribadi. Beberapa organisasi memilih untuk menggunakan jejak organisasi untuk mengumpulkan CloudTrail log di seluruh Wilayah AWS dan di seluruh akun ke dalam satu lokasi pusat, untuk tujuan visibilitas. Untuk informasi selengkapnya, lihat AWS CloudTrail dalam panduan ini. Saat menerapkan sentralisasi CloudTrail log, log biasanya disimpan dalam bucket Amazon Simple Storage Service (Amazon S3) di satu Wilayah.

Bergantung pada definisi data pribadi organisasi Anda, kewajiban kontraktual Anda kepada pelanggan Anda, dan peraturan privasi regional yang berlaku, Anda mungkin perlu mempertimbangkan transfer data lintas batas dalam hal agregasi log. Tentukan apakah data pribadi dalam berbagai jenis log termasuk dalam batasan ini. Misalnya, CloudTrail log mungkin berisi data

karyawan organisasi Anda, tetapi mungkin tidak berisi data pribadi pelanggan Anda. Jika organisasi Anda perlu mematuhi persyaratan transfer data terbatas, opsi berikut dapat membantu mendukung:

- Jika organisasi Anda menyediakan layanan AWS Cloud untuk subjek data di beberapa negara, Anda dapat memilih untuk menggabungkan semua log di negara yang memiliki persyaratan residensi data paling ketat. Misalnya, jika Anda beroperasi di Jerman dan memiliki persyaratan paling ketat, Anda dapat menggabungkan data dalam bucket S3 agar data yang dikumpulkan `eu-central-1` AWS Region di Jerman tidak meninggalkan perbatasan Jerman. Untuk opsi ini, Anda dapat mengonfigurasi jejak organisasi tunggal di log agregat CloudTrail tersebut dari seluruh akun dan Wilayah AWS ke Wilayah target.
- Menyunting data pribadi yang perlu disimpan AWS Region sebelum data disalin dan dikumpulkan ke wilayah lain. Misalnya, Anda dapat menutupi data pribadi di Wilayah host aplikasi sebelum Anda mentransfer log ke Wilayah yang berbeda. Untuk informasi selengkapnya tentang menutupi data pribadi, lihat Amazon Data Firehose bagian panduan ini.
- Jika Anda memiliki masalah kedaulatan data yang ketat, Anda dapat mempertahankan landing zone multi-akun terpisah yang memberlakukan persyaratan ini. AWS Region Dengan cara ini, Anda dapat menyederhanakan konfigurasi landing zone di Region untuk logging terpusat. Ini juga memberikan manfaat segregasi infrastruktur tambahan dan membantu menjaga log lokal ke Wilayah mereka sendiri. Bekerja dengan penasihat hukum Anda untuk menentukan data pribadi mana yang ada dalam cakupan dan Region-to-Region transfer mana yang diizinkan. Untuk informasi selengkapnya, lihat Strategi untuk ekspansi global dalam panduan ini.

Melalui log layanan, log aplikasi, dan log sistem operasi (OS), Anda dapat menggunakan Amazon CloudWatch untuk memantau Layanan AWS atau sumber daya di akun dan Wilayah yang sesuai secara default. Banyak yang memilih untuk memusatkan log dan metrik ini dari beberapa akun dan Wilayah ke dalam satu akun. Secara default, log ini tetap ada di akun terkait dan Wilayah tempat asalnya. Untuk sentralisasi, Anda dapat menggunakan filter langganan dan tugas ekspor Amazon S3 untuk berbagi data ke lokasi terpusat. Mungkin penting untuk menyertakan filter yang tepat dan tugas ekspor saat menggabungkan log dari beban kerja yang memiliki persyaratan transfer data lintas batas. Jika log akses beban kerja berisi data pribadi, Anda mungkin perlu memastikan bahwa log tersebut ditransfer atau disimpan di akun dan Wilayah tertentu.

Amazon Security Lake

Seperti yang direkomendasikan di AWS SRA, Anda mungkin ingin menggunakan akun Arsip Log sebagai akun administrator yang didelegasikan untuk Amazon Security Lake. Saat Anda melakukan

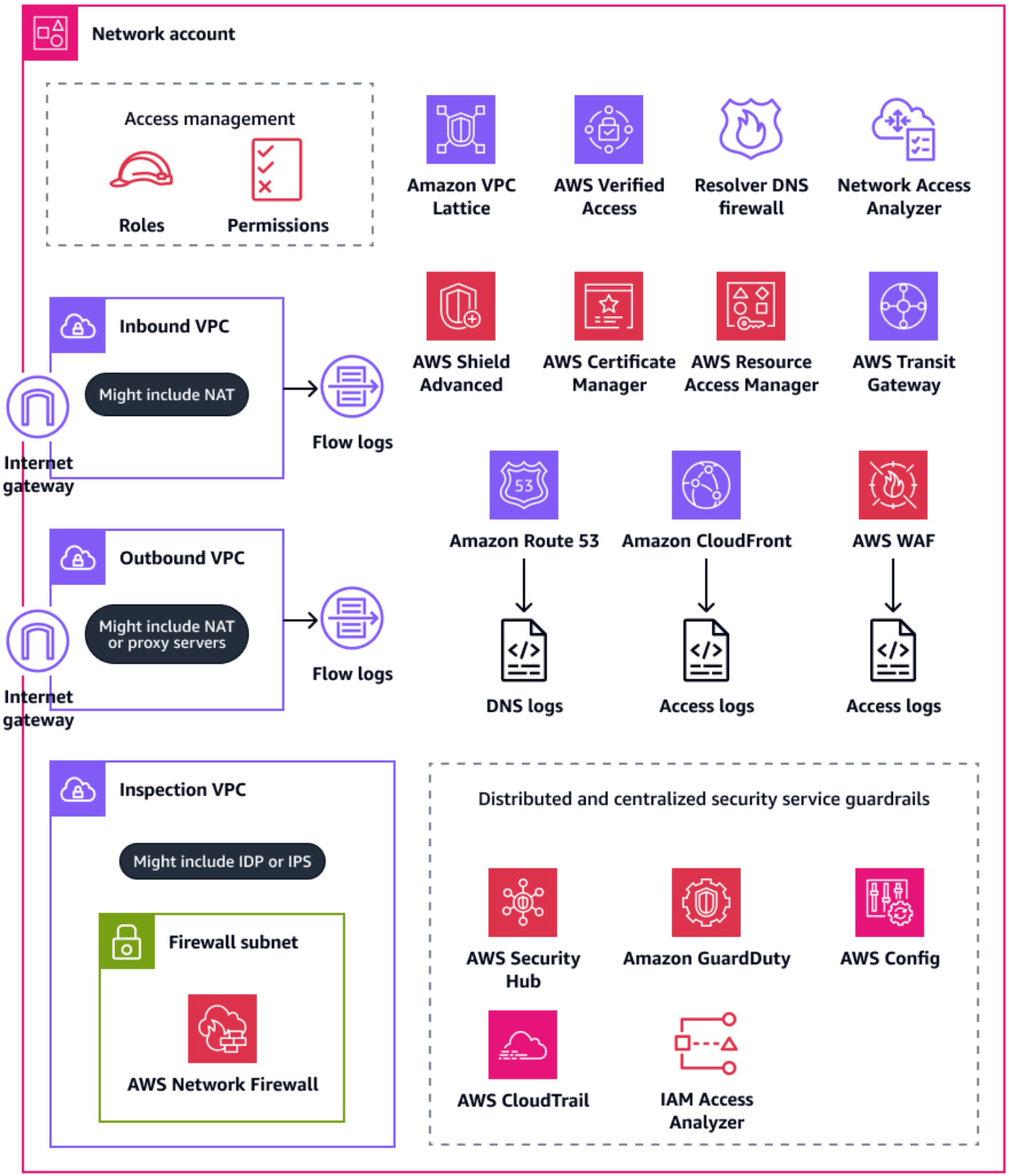
ini, Security Lake mengumpulkan log yang didukung di bucket Amazon S3 khusus di akun yang sama dengan log keamanan yang direkomendasikan SRA lainnya.

Dari perspektif privasi, penting bagi responden insiden Anda untuk memiliki akses ke log dari AWS lingkungan Anda, penyedia SaaS, di tempat, sumber cloud, dan sumber pihak ketiga. Ini membantu mereka lebih cepat memblokir dan memulihkan akses tidak sah ke data pribadi. Pertimbangan yang sama untuk penyimpanan log kemungkinan besar berlaku untuk residensi log dan pergerakan Regional dalam Amazon Security Lake. Ini karena Security Lake mengumpulkan log keamanan dan peristiwa dari Wilayah AWS tempat Anda mengaktifkan layanan. Untuk mematuhi persyaratan residensi data, pertimbangkan konfigurasi Wilayah rollup Anda.Wilayah rollup adalah Wilayah tempat Security Lake mengkonsolidasikan data dari satu atau lebih Wilayah yang berkontribusi, yang Anda pilih. Organisasi Anda mungkin perlu menyelaraskan persyaratan kepatuhan Regional Anda untuk residensi data sebelum Anda dapat mengonfigurasi Security Lake dan rollup Regions.

Infrastruktur OU - Akun jaringan

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Di akun Jaringan, Anda mengelola jaringan antara awan pribadi virtual Anda (VPCs) dan internet yang lebih luas. Di akun ini, Anda dapat menerapkan mekanisme kontrol pengungkapan luas dengan menggunakan AWS WAF, use AWS Resource Access Manager (AWS RAM) untuk berbagi subnet AWS Transit Gateway dan lampiran VPC, dan menggunakan CloudFront Amazon untuk mendukung penggunaan layanan yang ditargetkan. Untuk informasi selengkapnya tentang akun ini, lihat Arsitektur Referensi AWS Keamanan (AWS SRA). Diagram berikut menggambarkan layanan AWS keamanan dan privasi yang dikonfigurasi di akun Jaringan.


Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Bagian ini memberikan informasi lebih rinci tentang hal-hal berikut Layanan AWS yang digunakan dalam akun ini:

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront mendukung pembatasan geografis untuk aplikasi frontend dan hosting file. CloudFrontdapat mengirimkan konten melalui jaringan pusat data di seluruh dunia yang disebut lokasi tepi. Saat pengguna meminta konten yang Anda sajikan CloudFront, permintaan tersebut dirutekan ke lokasi tepi yang memberikan latensi terendah. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Program privasi Anda saat ini mungkin mendukung kepatuhan terhadap undang-undang regional tertentu. Jika beban kerja Anda dicakup untuk menyediakan layanan hanya kepada pelanggan yang hanya tinggal di wilayah ini, Anda dapat menerapkan langkah-langkah teknis yang mencegah penggunaan dari wilayah lain. Anda dapat menggunakan batasan CloudFront geografis untuk mencegah pengguna di lokasi geografis tertentu mengakses konten yang Anda distribusikan melalui distribusi. CloudFront Untuk informasi selengkapnya dan opsi konfigurasi untuk pembatasan geografis, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Anda juga dapat mengonfigurasi CloudFront untuk menghasilkan log akses yang berisi informasi terperinci tentang setiap permintaan pengguna yang CloudFront diterima. Untuk informasi selengkapnya, lihat Mengkonfigurasi dan menggunakan log standar (log akses) dalam CloudFront dokumentasi. Terakhir, jika CloudFront dikonfigurasi untuk menyimpan konten di serangkaian lokasi tepi, Anda dapat mempertimbangkan di mana caching terjadi. Untuk beberapa organisasi, caching lintas wilayah mungkin tunduk pada persyaratan transfer data lintas batas.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) membantu Anda berbagi sumber daya dengan aman Akun AWS untuk mengurangi overhead operasional dan memberikan visibilitas dan auditabilitas. Dengan AWS RAM, organisasi dapat membatasi AWS sumber daya mana yang dapat dibagikan dengan orang lain Akun AWS di organisasi mereka atau dengan akun pihak ketiga. Untuk informasi

selengkapnya, lihat AWS Sumber daya yang dapat dibagikan. Di akun Jaringan, Anda dapat menggunakan AWS RAM untuk berbagi subnet VPC dan koneksi gateway transit. Jika Anda menggunakan AWS RAM untuk berbagi koneksi pesawat data dengan yang lain Akun AWS, Anda dapat mempertimbangkan untuk membuat proses untuk memeriksa apakah koneksi dibuat untuk disetujui sebelumnya Wilayah AWS dan mematuhi persyaratan residensi data Anda.

Selain koneksi gateway berbagi VPCs dan transit, AWS RAM dapat digunakan untuk berbagi sumber daya yang tidak mendukung kebijakan berbasis sumber daya IAM. Untuk beban kerja yang dihosting di Data Pribadi OU, Anda dapat menggunakan AWS RAM untuk mengakses data pribadi yang terletak di tempat terpisah Akun AWS. Untuk informasi selengkapnya, lihat AWS Resource Access Manager di bagian Akun Aplikasi OU — PD Data Pribadi.

AWS Transit Gateway

Jika Anda ingin menyebarkan AWS sumber daya yang mengumpulkan, menyimpan, atau memproses data pribadi Wilayah AWS yang sesuai dengan persyaratan residensi data organisasi Anda dan Anda memiliki perlindungan teknis yang sesuai, pertimbangkan untuk menerapkan pagar pembatas untuk mencegah aliran data lintas batas yang tidak disetujui pada bidang kontrol dan data. Pada bidang kontrol, Anda dapat membatasi penggunaan Wilayah dan, sebagai hasilnya, aliran data lintas wilayah menggunakan IAM dan kebijakan kontrol layanan.

Ada beberapa opsi untuk mengontrol aliran data lintas wilayah pada bidang data. Misalnya, Anda dapat menggunakan tabel rute, peering VPC, dan lampiran. AWS Transit Gateway AWS Transit Gatewayadalah hub pusat yang menghubungkan virtual private cloud (VPCs) dan jaringan lokal. Sebagai bagian dari AWS landing zone Anda yang lebih besar, Anda dapat mempertimbangkan berbagai cara data dapat melintasi Wilayah AWS, termasuk melalui gateway internet, melalui pengintipan langsung, dan melalui VPC-to-VPC pengintipan antar wilayah. AWS Transit Gateway Misalnya, Anda dapat melakukan hal berikut di AWS Transit Gateway:

- Konfirmasikan bahwa koneksi timur-barat dan utara-selatan antara lingkungan Anda VPCs dan lokal selaras dengan persyaratan privasi Anda.
- Konfigurasikan pengaturan VPC sesuai dengan persyaratan privasi Anda.
- Gunakan kebijakan kontrol layanan dalam AWS Organizations dan kebijakan IAM untuk membantu mencegah modifikasi pada konfigurasi Amazon Virtual Private Cloud (Amazon VPC) Anda AWS Transit Gateway dan Amazon. Untuk contoh kebijakan kontrol layanan, lihat Batasi perubahan pada konfigurasi VPC di panduan ini.

AWS WAF

Untuk membantu mencegah pengungkapan data pribadi yang tidak diinginkan, Anda dapat menerapkan defense-in-depth pendekatan untuk aplikasi web Anda. Anda dapat membangun validasi input dan pembatasan tarif ke dalam aplikasi Anda, tetapi AWS WAF dapat berfungsi sebagai garis pertahanan lain. AWS WAFadalah firewall aplikasi web yang membantu Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke sumber daya aplikasi web Anda yang dilindungi. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

Dengan AWS WAF, Anda dapat menentukan dan menerapkan aturan yang memeriksa kriteria tertentu. Kegiatan berikut mungkin terkait dengan pengungkapan data pribadi yang tidak diinginkan:

- Lalu lintas dari alamat IP atau lokasi geografis yang tidak dikenal atau berbahaya
- Open Worldwide Application Security Project (OWASP) 10 serangan teratas, termasuk serangan terkait eksfiltrasi seperti injeksi SQL
- Tingkat permintaan yang tinggi
- Lalu lintas bot umum
- Pengikis konten

Anda dapat menerapkan grup AWS WAF aturan yang dikelola oleh AWS. Beberapa grup aturan terkelola untuk AWS WAF dapat digunakan untuk mendeteksi ancaman terhadap privasi dan data pribadi, misalnya:

- Database SQL — Grup aturan ini berisi aturan yang dirancang untuk memblokir pola permintaan yang terkait dengan eksploitasi database SQL, seperti serangan injeksi SQL. Pertimbangkan grup aturan ini jika aplikasi Anda berinteraksi dengan database SQL.
- Masukan buruk yang diketahui - Grup aturan ini berisi aturan yang dirancang untuk memblokir pola permintaan yang diketahui tidak valid dan terkait dengan eksploitasi atau penemuan kerentanan.
- Kontrol Bot — Grup aturan ini berisi aturan yang dirancang untuk mengelola permintaan dari bot, yang dapat mengkonsumsi sumber daya berlebih, mengubah metrik bisnis, menyebabkan downtime, dan melakukan aktivitas berbahaya.
- Pencegahan pengambilalihan akun (ATP) - Grup aturan ini berisi aturan yang dirancang untuk mencegah upaya pengambilalihan akun berbahaya. Grup aturan ini memeriksa upaya login yang dikirim ke titik akhir login aplikasi Anda.

Data Pribadi OU - Akun Aplikasi PD

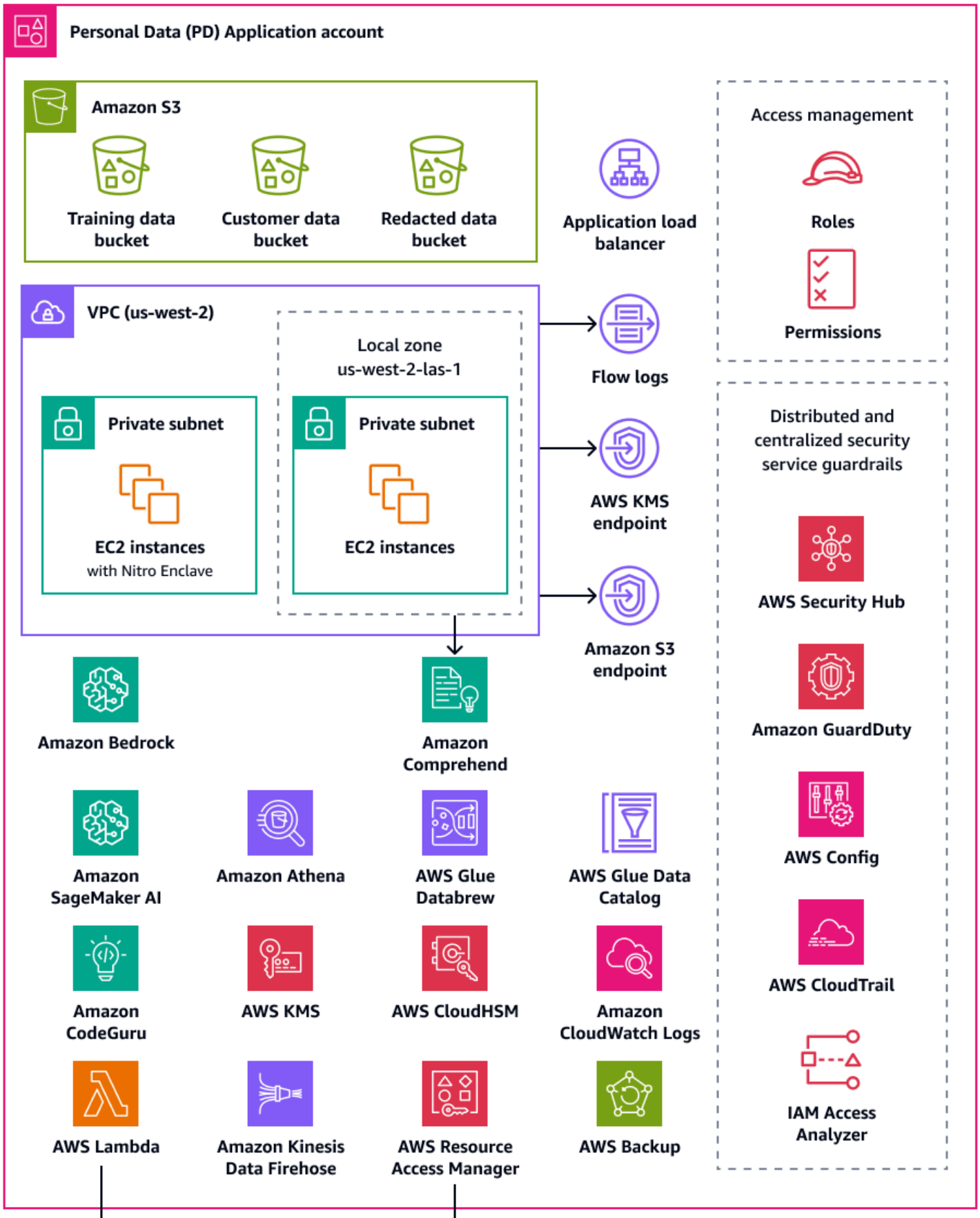
> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Akun Aplikasi Data Pribadi (PD) adalah tempat organisasi Anda menyelenggarakan layanan yang mengumpulkan dan memproses data pribadi. Secara khusus, Anda dapat menyimpan apa yang Anda definisikan sebagai data pribadi di akun ini. AWS PRA menunjukkan sejumlah contoh konfigurasi privasi melalui arsitektur web tanpa server multi-tier. Ketika menyangkut beban kerja pengoperasian di seluruh AWS landing zone, konfigurasi privasi tidak boleh dianggap sebagai one-size-fits-all solusi. Misalnya, tujuan Anda mungkin untuk memahami konsep yang mendasarinya, bagaimana mereka dapat meningkatkan privasi, dan bagaimana organisasi Anda dapat menerapkan solusi untuk kasus penggunaan dan arsitektur khusus Anda.

Karena Akun AWS di organisasi Anda yang mengumpulkan, menyimpan, atau memproses data pribadi, Anda dapat menggunakan AWS Organizations dan AWS Control Tower menerapkan pagar pembatas dasar dan berulang. Menetapkan unit organisasi khusus (OU) untuk akun ini sangat penting. Misalnya, Anda mungkin ingin menerapkan pagar pembatas residensi data hanya pada sebagian akun di mana residensi data merupakan pertimbangan desain inti. Bagi banyak organisasi, ini adalah akun yang menyimpan dan memproses data pribadi.

Organisasi Anda mungkin mempertimbangkan untuk mendukung akun Data khusus, yang merupakan tempat Anda menyimpan sumber otoritatif kumpulan data pribadi Anda. Sumber data otoritatif adalah lokasi tempat Anda menyimpan versi data utama, yang mungkin dianggap sebagai versi data yang paling andal dan akurat. Misalnya, Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain, seperti bucket Amazon Simple Storage Service (Amazon S3) di akun Aplikasi PD yang digunakan untuk menyimpan data pelatihan, subset data pelanggan, dan data yang disunting. Dengan mengambil pendekatan multi-akun ini untuk memisahkan kumpulan data pribadi yang lengkap dan definitif di akun Data dari beban kerja konsumen hilir di akun Aplikasi PD, Anda dapat mengurangi cakupan dampak jika terjadi akses tidak sah ke akun Anda.

Diagram berikut menggambarkan layanan AWS keamanan dan privasi yang dikonfigurasi dalam akun Aplikasi dan Data PD.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management
Log archive

Bagian ini memberikan informasi lebih rinci tentang hal-hal berikut Layanan AWS yang digunakan dalam akun ini:

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- CloudWatch Log Amazon
- CodeGuru Peninjau Amazon
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- AWS Local Zones
- AWS Enklaf Nitro
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS fitur yang membantu mengelola siklus hidup data
- Layanan AWS dan fitur yang membantu mengelompokkan data
- Layanan AWS dan fitur yang membantu menemukan, mengklasifikasikan, atau membuat katalog data

Amazon Athena

Anda dapat mempertimbangkan kontrol pembatasan kueri data untuk memenuhi tujuan privasi Anda. Amazon Athena adalah layanan kueri interaktif yang membantu Anda menganalisis data secara langsung di Amazon S3 dengan menggunakan SQL standar. Anda tidak perlu memuat data ke Athena; ini bekerja langsung dengan data yang disimpan dalam ember S3.

Kasus penggunaan umum untuk Athena adalah menyediakan kumpulan data yang disesuaikan dan disanitasi kepada tim analitik data. Jika kumpulan data berisi data pribadi, Anda dapat membersihkan

kumpulan data dengan menutupi seluruh kolom data pribadi yang memberikan sedikit nilai bagi tim analitik data. Untuk informasi selengkapnya, lihat Menganonimkan dan mengelola data di danau data Anda dengan Amazon Athena dan AWS Lake Formation (posting blog).AWS

Jika pendekatan transformasi data Anda memerlukan fleksibilitas tambahan di luar fungsi yang didukung di Athena, Anda dapat menentukan fungsi kustom, yang disebut fungsi yang ditentukan pengguna (UDF). Anda dapat memanggil UDFs dalam kueri SQL yang dikirimkan ke Athena, dan mereka berjalan. AWS Lambda Anda dapat menggunakan UDFs dalam `SELECT` dan `FILTER SQL` kueri, dan Anda dapat memanggil beberapa UDFs dalam kueri yang sama. Untuk privasi, Anda dapat membuat UDFs yang melakukan jenis penyembunyian data tertentu, seperti hanya menampilkan empat karakter terakhir dari setiap nilai dalam kolom.

Amazon Bedrock

Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang menyediakan akses ke model foundation dari perusahaan AI terkemuka seperti AI21 Labs, Anthropic, Meta, Mistral AI, dan Amazon. Ini membantu organisasi untuk membangun dan menskalakan aplikasi AI generatif. Apa pun platform yang digunakan, saat menggunakan AI generatif, organisasi dapat menghadapi risiko privasi, termasuk potensi paparan data pribadi, akses data yang tidak sah, dan pelanggaran kepatuhan lainnya.

Amazon Bedrock Guardrails dirancang untuk membantu mengurangi risiko ini dengan menerapkan praktik terbaik keamanan dan kepatuhan di seluruh beban kerja AI generatif Anda di Amazon Bedrock. Penyebaran dan penggunaan sumber daya AI mungkin tidak selalu selaras dengan persyaratan privasi dan kepatuhan organisasi. Organizations dapat berjuang dengan menjaga privasi data saat menggunakan model AI generatif karena model ini berpotensi menghafal atau mereproduksi informasi sensitif. Amazon Bedrock Guardrails membantu melindungi privasi dengan mengevaluasi input pengguna dan respons model. Secara keseluruhan, jika data input berisi data pribadi, mungkin ada risiko informasi ini terpapar dalam output model.

Amazon Bedrock Guardrails menyediakan mekanisme untuk menegakkan kebijakan perlindungan data dan membantu mencegah paparan data yang tidak sah. Ini menawarkan kemampuan penyaringan konten untuk mendeteksi dan memblokir data pribadi dalam input, pembatasan topik untuk membantu mencegah akses ke materi pelajaran yang tidak pantas atau berisiko, dan filter kata untuk menutupi atau menyunting istilah sensitif dalam permintaan dan tanggapan model. Kemampuan ini membantu mencegah peristiwa yang dapat menyebabkan pelanggaran privasi, seperti tanggapan bias, atau erosi kepercayaan pelanggan. Fitur-fitur ini dapat membantu Anda memastikan bahwa data pribadi tidak diproses atau diungkapkan secara tidak sengaja oleh model

AI Anda. Amazon Bedrock Guardrails mendukung evaluasi input dan tanggapan di luar Amazon Bedrock juga. Untuk informasi selengkapnya, lihat Menerapkan langkah-langkah keamanan independen model dengan Amazon Bedrock Guardrails (posting blog).AWS

Dengan Amazon Bedrock Guardrails, Anda dapat membatasi risiko halusinasi model dengan menggunakan pemeriksaan pentanahan kontekstual, yang mengevaluasi landasan faktual dan relevansi respons. Contohnya adalah menerapkan aplikasi generatif AI yang menghadap pelanggan yang menggunakan sumber data pihak ketiga dalam aplikasi Retrieval Augmented Generation (RAG). Pemeriksaan grounding kontekstual dapat digunakan untuk memvalidasi respons model terhadap sumber data ini dan menyaring tanggapan yang tidak akurat. Dalam konteks AWS PRA, Anda dapat menerapkan Amazon Bedrock Guardrails di seluruh akun beban kerja, yang memberlakukan pagar pembatas privasi tertentu yang disesuaikan dengan setiap persyaratan beban kerja.

AWS Clean Rooms

Ketika organisasi mencari cara untuk berkolaborasi satu sama lain melalui analisis kumpulan data sensitif yang berpotongan atau tumpang tindih, menjaga keamanan dan privasi data bersama itu menjadi perhatian. AWS Clean Roomsmembantu Anda menyebarkan ruang bersih data, yang merupakan lingkungan yang aman dan netral tempat organisasi dapat menganalisis kumpulan data gabungan tanpa membagikan data mentah itu sendiri. Ini juga dapat menghasilkan wawasan unik dengan menyediakan akses ke organisasi lain AWS tanpa memindahkan atau menyalin data dari akun mereka sendiri dan tanpa mengungkapkan kumpulan data yang mendasarinya. Semua data tetap berada di lokasi sumber. Aturan analisis bawaan membatasi output dan membatasi kueri SQL. Semua kueri dicatat, dan anggota kolaborasi dapat melihat bagaimana data mereka ditanyakan.

Anda dapat membuat AWS Clean Rooms kolaborasi dan mengundang AWS pelanggan lain untuk menjadi anggota kolaborasi itu. Anda memberikan satu anggota kemampuan untuk menanyakan kumpulan data anggota, dan Anda dapat memilih anggota tambahan untuk menerima hasil kueri tersebut. Jika lebih dari satu anggota perlu menanyakan kumpulan data, Anda dapat membuat kolaborasi tambahan dengan sumber data yang sama dan pengaturan anggota yang berbeda. Setiap anggota dapat memfilter data yang dibagikan dengan anggota kolaborasi, dan Anda dapat menggunakan aturan analisis khusus untuk menetapkan batasan tentang bagaimana data yang mereka berikan kepada kolaborasi dapat dianalisis.

Selain membatasi data yang disajikan untuk kolaborasi dan bagaimana hal itu dapat digunakan oleh anggota lain, AWS Clean Rooms menyediakan kemampuan berikut yang dapat membantu Anda melindungi privasi:

- Privasi diferensial adalah teknik matematika yang meningkatkan privasi pengguna dengan menambahkan jumlah noise yang dikalibrasi dengan hati-hati ke data. Ini membantu mengurangi risiko identifikasi ulang pengguna individu dalam kumpulan data tanpa mengaburkan nilai-nilai yang diminati. Menggunakan Privasi AWS Clean Rooms Diferensial tidak memerlukan keahlian privasi diferensial.
- AWS Clean Rooms ML memungkinkan dua atau lebih pihak untuk mengidentifikasi pengguna serupa dalam data mereka tanpa langsung berbagi data satu sama lain. Ini mengurangi risiko serangan inferensi keanggotaan, di mana anggota kolaborasi dapat mengidentifikasi individu dalam kumpulan data anggota lain. Dengan membuat model yang mirip dan menghasilkan segmen yang mirip, AWS Clean Rooms ML membantu Anda membandingkan kumpulan data tanpa mengekspos data asli. Ini tidak mengharuskan salah satu anggota untuk memiliki keahlian ML atau melakukan pekerjaan apa pun di luar AWS Clean Rooms. Anda mempertahankan kendali penuh dan kepemilikan model terlatih.
- Cryptographic Computing for Clean Rooms (C3R) dapat digunakan dengan aturan analisis untuk memperoleh wawasan dari data sensitif. Ini secara kriptografis membatasi apa yang dapat dipelajari oleh pihak lain untuk kolaborasi. Dengan menggunakan klien enkripsi C3R, data dienkripsi di klien sebelum diberikan. AWS Clean Rooms Karena tabel data dienkripsi menggunakan alat enkripsi sisi klien sebelum diunggah ke Amazon S3, data tetap dienkripsi dan bertahan melalui pemrosesan.

Di AWS PRA, kami menyarankan Anda membuat AWS Clean Rooms kolaborasi di akun Data. Anda dapat menggunakannya untuk berbagi data pelanggan terenkripsi dengan pihak ketiga. Gunakan hanya jika ada tumpang tindih dalam kumpulan data yang disediakan. Untuk informasi selengkapnya tentang cara menentukan tumpang tindih, lihat Aturan analisis daftar dalam AWS Clean Rooms dokumentasi.

CloudWatch Log Amazon

Amazon CloudWatch Logs membantu Anda memusatkan log dari semua sistem, aplikasi, Layanan AWS sehingga Anda dapat memantau dan mengarsipkannya dengan aman. Di CloudWatch Log, Anda dapat menggunakan kebijakan perlindungan data untuk grup log baru atau yang sudah ada untuk membantu meminimalkan risiko pengungkapan data pribadi. Kebijakan perlindungan data dapat mendeteksi data sensitif, seperti data pribadi, di log Anda. Kebijakan perlindungan data dapat menutupi data tersebut ketika pengguna mengakses log melalui file Konsol Manajemen AWS. Ketika pengguna memerlukan akses langsung ke data pribadi, sesuai dengan spesifikasi tujuan keseluruhan untuk beban kerja Anda, Anda dapat menetapkan `logs:Unmask` izin untuk pengguna tersebut.

Anda juga dapat membuat kebijakan perlindungan data di seluruh akun dan menerapkan kebijakan ini secara konsisten di semua akun di organisasi Anda. Ini mengonfigurasi masking secara default untuk semua grup log saat ini dan masa depan di CloudWatch Log. Kami juga menyarankan Anda mengaktifkan laporan audit dan mengirimkannya ke grup log lain, bucket Amazon S3, atau Amazon Data Firehose. Laporan ini berisi catatan rinci temuan perlindungan data di setiap grup log.

CodeGuru Peninjau Amazon

Untuk privasi dan keamanan, sangat penting bagi banyak organisasi bahwa mereka mendukung kepatuhan berkelanjutan selama fase penerapan dan pasca-penyebaran. AWS PRA mencakup kontrol proaktif dalam pipeline penyebaran untuk aplikasi yang memproses data pribadi. Amazon CodeGuru Reviewer dapat mendeteksi potensi cacat yang mungkin mengekspos data pribadi di Jawa, JavaScript, dan kode Python. Ini menawarkan saran kepada pengembang untuk meningkatkan kode. CodeGuru Peninjau dapat mengidentifikasi cacat di berbagai keamanan, privasi, dan praktik umum yang direkomendasikan. Ini dirancang untuk bekerja dengan beberapa penyedia sumber, termasuk, Bitbucket AWS CodeCommit, GitHub, dan Amazon S3. Beberapa cacat terkait privasi yang dapat dideteksi oleh CodeGuru Reviewer meliputi:

- Injeksi SQL
- Cookie tanpa jaminan
- Otorisasi hilang
- Enkripsi ulang sisi klien AWS KMS

Untuk daftar lengkap apa yang dapat dideteksi oleh CodeGuru Reviewer, lihat Amazon CodeGuru Detector Library.

Amazon Comprehend

Amazon Comprehend adalah layanan pemrosesan bahasa alami (NLP) yang menggunakan pembelajaran mesin untuk mengungkap wawasan dan koneksi berharga dalam dokumen teks bahasa Inggris. Amazon Comprehend dapat mendeteksi dan menyunting data pribadi dalam dokumen teks terstruktur, semi-terstruktur, atau tidak terstruktur. Untuk informasi selengkapnya, lihat Informasi identitas pribadi (PII) di dokumentasi Amazon Comprehend.

Karena Amazon Comprehend memiliki banyak opsi untuk AWS SDKs integrasi aplikasi, Anda dapat menggunakan Amazon Comprehend untuk mengidentifikasi data pribadi di berbagai tempat di mana Anda mengumpulkan, menyimpan, dan memproses data. Anda dapat menggunakan kemampuan Amazon Comprehend MLuntuk mendeteksi dan menyunting data pribadi diAWS log aplikasi (posting

blog), email pelanggan, tiket dukungan, dan banyak lagi. Diagram arsitektur untuk akun Aplikasi PD menunjukkan bagaimana Anda dapat melakukan fungsi ini untuk log aplikasi di Amazon EC2. Amazon Comprehend menawarkan dua mode redaksi:

- `REPLACE_WITH_PII_ENTITY_TYPE`menggantikan setiap entitas PII dengan tipenya. Misalnya, Jane Doe akan diganti dengan NAME.
- `MASK`menggantikan karakter dalam entitas PII dengan karakter pilihan Anda (! , #, $,%, &,, atau @). Misalnya, Jane Doe dapat diganti dengan **** ***.

Amazon Data Firehose

Amazon Data Firehose dapat digunakan untuk menangkap, mengubah, dan memuat data streaming ke layanan hilir, seperti Amazon Managed Service untuk Apache Flink atau Amazon S3. Firehose sering digunakan untuk mengangkut data streaming dalam jumlah besar, seperti log aplikasi, tanpa harus membangun pipa pemrosesan dari bawah ke atas.

Anda dapat menggunakan fungsi Lambda untuk melakukan pemrosesan khusus atau bawaan sebelum data dikirim ke hilir. Untuk privasi, kemampuan ini mendukung minimalisasi data dan persyaratan transfer data lintas batas. Misalnya, Anda dapat menggunakan Lambda dan Firehose untuk mengubah data log Multi-wilayah sebelum terpusat di akun Arsip Log. Untuk informasi selengkapnya, lihat Biogen: Solusi Pencatatan Terpusat untuk Multi Akun (YouTube video). Di akun Aplikasi PD, Anda mengonfigurasi Amazon CloudWatch dan AWS CloudTrail mendorong log ke aliran pengiriman Firehose. Fungsi Lambda mengubah log dan mengirimkannya ke bucket S3 pusat di akun Arsip Log. Anda dapat mengonfigurasi fungsi Lambda untuk menutupi bidang tertentu yang berisi data pribadi. Ini membantu mencegah transfer data pribadi Wilayah AWS. Dengan menggunakan pendekatan ini, data pribadi disembunyikan sebelum transfer dan sentralisasi, bukan setelahnya. Untuk aplikasi di yurisdiksi yang tidak tunduk pada persyaratan transfer lintas batas, biasanya lebih efisien secara operasional dan hemat biaya untuk mengumpulkan log melalui jejak organisasi di. CloudTrail Untuk informasi selengkapnya, lihat AWS CloudTrail di bagian Security OU — Security Tooling account dari panduan ini.

Amazon DataZone

Ketika organisasi menskalakan pendekatan mereka untuk berbagi data melalui Layanan AWS seperti itu AWS Lake Formation, mereka ingin memastikan bahwa akses diferensial dikendalikan oleh mereka yang paling akrab dengan data: pemilik data. Namun, pemilik data ini mungkin mengetahui persyaratan privasi, seperti persetujuan atau pertimbangan transfer data lintas batas. Amazon

DataZone membantu pemilik data dan tim tata kelola data berbagi dan mengkonsumsi data di seluruh organisasi sesuai dengan kebijakan tata kelola data Anda. Di Amazon DataZone, lini bisnis (LOBs) mengelola data mereka sendiri, dan katalog melacak kepemilikan ini. Pihak yang tertarik dapat menemukan dan meminta akses ke data sebagai bagian dari tugas bisnis mereka. Selama mematuhi kebijakan yang ditetapkan oleh penerbit data, pemilik data dapat memberikan akses ke tabel yang mendasarinya, tanpa administrator atau memindahkan data.

Dalam konteks privasi, Amazon DataZone dapat membantu dalam contoh kasus penggunaan berikut:

- Aplikasi yang dihadapi pelanggan menghasilkan data penggunaan yang dapat dibagikan dengan LOB pemasaran terpisah. Anda perlu memastikan bahwa hanya data untuk pelanggan yang telah memilih untuk pemasaran yang dipublikasikan ke katalog.
- Data pelanggan Eropa dipublikasikan tetapi hanya dapat berlangganan oleh LOBs lokal ke Wilayah Ekonomi Eropa (EEA). Untuk informasi selengkapnya, lihat Meningkatkan keamanan data dengan kontrol akses berbutir halus di Amazon. DataZone

Di AWS PRA, Anda dapat menghubungkan data di bucket Amazon S3 bersama ke DataZone Amazon sebagai produsen data.

AWS Glue

Mempertahankan kumpulan data yang berisi data pribadi adalah komponen kunci dari Privacy by Design. Data organisasi mungkin ada dalam bentuk terstruktur, semi-terstruktur, atau tidak terstruktur. Kumpulan data pribadi tanpa struktur dapat menyulitkan untuk melakukan sejumlah operasi peningkatan privasi, termasuk meminimalkan data, melacak data yang dikaitkan dengan subjek data tunggal sebagai bagian dari permintaan subjek data, memastikan kualitas data yang konsisten, dan segmentasi kumpulan data secara keseluruhan. AWS Glueadalah layanan ekstrak, transformasi, dan beban (ETL) yang dikelola sepenuhnya. Ini dapat membantu Anda mengkategorikan, membersihkan, memperkaya, dan memindahkan data antara penyimpanan data dan aliran data. AWS Glue fitur dirancang untuk membantu Anda menemukan, menyiapkan, menyusun, dan menggabungkan kumpulan data untuk analitik, pembelajaran mesin, dan pengembangan aplikasi. Anda dapat menggunakan AWS Glue untuk membuat struktur yang dapat diprediksi dan umum di atas kumpulan data yang ada. AWS Glue Data Catalog, AWS Glue DataBrew, dan Kualitas AWS Glue Data adalah AWS Glue fitur yang dapat membantu mendukung persyaratan privasi organisasi Anda.

AWS Glue Data Catalog

AWS Glue Data Catalogmembantu Anda membuat kumpulan data yang dapat dipelihara. Katalog Data berisi referensi ke data yang digunakan sebagai sumber dan target untuk mengekstrak, mengubah, dan memuat (ETL) pekerjaan di AWS Glue. Informasi dalam Katalog Data disimpan sebagai tabel metadata, dan setiap tabel menentukan penyimpanan data tunggal. Anda menjalankan AWS Glue crawler untuk mengambil inventaris data dalam berbagai jenis penyimpanan data. Anda menambahkan pengklasifikasi bawaan dan kustom ke crawler, dan pengklasifikasi ini menyimpulkan format data dan skema data pribadi. Crawler kemudian menulis metadata ke Katalog Data. Tabel metadata terpusat dapat memudahkan untuk menanggapi permintaan subjek data (seperti hak untuk menghapus) karena menambahkan struktur dan prediktabilitas di berbagai sumber data pribadi di lingkungan Anda. AWS Untuk contoh komprehensif tentang cara menggunakan Katalog Data untuk merespons permintaan ini secara otomatis, lihat Menangani permintaan penghapusan data di data lake Anda dengan Amazon S3 Find and Forget AWS (posting blog). Terakhir, jika organisasi Anda menggunakan AWS Lake Formationuntuk mengelola dan menyediakan akses berbutir halus di seluruh database, tabel, baris, dan sel, Katalog Data adalah komponen kunci. Data Catalog menyediakan berbagi data lintas akun dan membantu Anda menggunakan kontrol akses berbasis tag untuk mengelola data lake Anda dalam skala besar (posting AWS blog). Untuk informasi lebih lanjut, lihat AWS Lake Formation di bagian ini.

AWS Glue DataBrew

AWS Glue DataBrewmembantu Anda membersihkan dan menormalkan data, dan dapat melakukan transformasi pada data, seperti menghapus atau menutupi informasi yang dapat diidentifikasi secara pribadi dan mengenkripsi bidang data sensitif dalam jaringan data. Anda juga dapat memetakan garis keturunan data Anda secara visual untuk memahami berbagai sumber data dan langkah-langkah transformasi yang telah dilalui data. Fitur ini menjadi semakin penting karena organisasi Anda bekerja untuk lebih memahami dan melacak asal data pribadi. DataBrew membantu Anda menutupi data pribadi selama persiapan data. Anda dapat mendeteksi data pribadi sebagai bagian dari pekerjaan pembuatan profil data dan mengumpulkan statistik, seperti jumlah kolom yang mungkin berisi data pribadi dan kategori potensial. Anda kemudian dapat menggunakan teknik transformasi data reversibel atau ireversibel bawaan, termasuk substitusi, hashing, enkripsi, dan dekripsi, semuanya tanpa menulis kode apa pun. Anda kemudian dapat menggunakan kumpulan data yang dibersihkan dan disamarkan di hilir untuk tugas analitik, pelaporan, dan pembelajaran mesin. Beberapa teknik masking data yang tersedia di DataBrew antaranya:

- Hashing - Terapkan fungsi hash ke nilai kolom.
- Substitusi — Ganti data pribadi dengan nilai lain yang tampak otentik.

- Nulling out atau penghapusan - Ganti bidang tertentu dengan nilai null, atau hapus kolom.
- Masking out — Gunakan karakter scrambling, atau menutupi bagian-bagian tertentu dalam kolom.

Berikut ini adalah teknik enkripsi yang tersedia:

- Enkripsi deterministik — Menerapkan algoritma enkripsi deterministik ke nilai kolom. Enkripsi deterministik selalu menghasilkan ciphertext yang sama untuk suatu nilai.
- Enkripsi probabilistik — Menerapkan algoritma enkripsi probabilistik ke nilai kolom. Enkripsi probabilistik menghasilkan ciphertext yang berbeda setiap kali diterapkan.

Untuk daftar lengkap resep transformasi data pribadi yang disediakan DataBrew, lihat langkah-langkah resep Informasi Identifikasi Pribadi (PII).

AWS Glue Kualitas Data

AWS Glue Kualitas Data membantu Anda mengotomatiskan dan mengoperasionalkan pengiriman data berkualitas tinggi di seluruh jalur data, secara proaktif, sebelum dikirimkan ke konsumen data Anda. AWS Glue Kualitas Data menyediakan analisis statistik masalah kualitas data di seluruh jalur data Anda, dapat memicu peringatan di Amazon EventBridge, dan dapat membuat rekomendasi aturan kualitas untuk perbaikan. AWS Glue Kualitas Data juga mendukung pembuatan aturan dengan bahasa khusus domain sehingga Anda dapat membuat aturan kualitas data khusus.

AWS Key Management Service

AWS Key Management Service (AWS KMS) membantu Anda membuat dan mengontrol kunci kriptografi untuk membantu melindungi data Anda. AWS KMS menggunakan modul keamanan perangkat keras untuk melindungi dan memvalidasi AWS KMS keys di bawah Program Validasi Modul Kriptografi FIPS 140-2. Untuk informasi selengkapnya tentang cara layanan ini digunakan dalam konteks keamanan, lihat Arsitektur Referensi AWS Keamanan.

AWS KMS terintegrasi dengan sebagian besar Layanan AWS yang menawarkan enkripsi, dan Anda dapat menggunakan kunci KMS dalam aplikasi Anda yang memproses dan menyimpan data pribadi. Anda dapat menggunakan AWS KMS untuk membantu mendukung berbagai persyaratan privasi Anda dan melindungi data pribadi, termasuk:

- Menggunakan kunci yang dikelola pelanggan untuk kontrol yang lebih besar atas kekuatan, rotasi, kedaluwarsa, dan opsi lainnya.

- Menggunakan kunci terkelola pelanggan khusus untuk melindungi data pribadi dan rahasia yang memungkinkan akses ke data pribadi.
- Mendefinisikan tingkat klasifikasi data dan menunjuk setidaknya satu kunci yang dikelola pelanggan khusus per level. Misalnya, Anda mungkin memiliki satu kunci untuk mengenkripsi data operasional dan yang lain untuk mengenkripsi data pribadi.
- Mencegah akses lintas akun yang tidak diinginkan ke kunci KMS.
- Menyimpan kunci KMS dalam Akun AWS sama dengan sumber daya yang akan dienkripsi.
- Menerapkan pemisahan tugas untuk administrasi dan penggunaan kunci KMS. Untuk informasi selengkapnya, lihat Cara menggunakan KMS dan IAM untuk mengaktifkan kontrol keamanan independen untuk data terenkripsi di S3 (posting blog).AWS
- Menegakkan rotasi kunci otomatis melalui pagar pembatas preventif dan reaktif.

Secara default, kunci KMS disimpan dan hanya dapat digunakan di Wilayah tempat mereka dibuat. Jika organisasi Anda memiliki persyaratan khusus untuk residensi dan kedaulatan data, pertimbangkan apakah kunci KMS Multi-wilayah sesuai untuk kasus penggunaan Anda. Tombol Multi-Region adalah kunci KMS tujuan khusus yang berbeda Wilayah AWS yang dapat digunakan secara bergantian. Proses pembuatan kunci Multi-wilayah memindahkan materi utama Anda melintasi AWS Region batas-batas di dalamnya AWS KMS, sehingga kurangnya isolasi regional ini mungkin tidak sesuai dengan tujuan kedaulatan dan residensi organisasi Anda. Salah satu cara untuk mengatasinya adalah dengan menggunakan jenis kunci KMS yang berbeda, seperti kunci yang dikelola pelanggan khusus Wilayah.

Toko kunci eksternal

Bagi banyak organisasi, penyimpanan AWS KMS kunci default di AWS Cloud dapat memenuhi kedaulatan data dan persyaratan peraturan umum mereka. Tetapi beberapa mungkin mengharuskan kunci enkripsi dibuat dan dipelihara di luar lingkungan cloud dan Anda memiliki jalur otorisasi dan audit independen. Dengan penyimpanan kunci eksternal AWS KMS, Anda dapat mengenkripsi data pribadi dengan materi utama yang dimiliki dan dikendalikan organisasi Anda di luar. AWS Cloud Anda masih berinteraksi dengan AWS KMS API seperti biasa, tetapi hanya AWS KMS berinteraksi dengan perangkat lunak proxy penyimpanan kunci eksternal (proxy XKS) yang Anda sediakan. Proxy penyimpanan kunci eksternal Anda kemudian memediasi semua komunikasi antara AWS KMS dan manajer kunci eksternal Anda.

Saat menggunakan penyimpanan kunci eksternal untuk enkripsi data, penting bagi Anda untuk mempertimbangkan overhead operasional tambahan dibandingkan dengan mempertahankan kunci

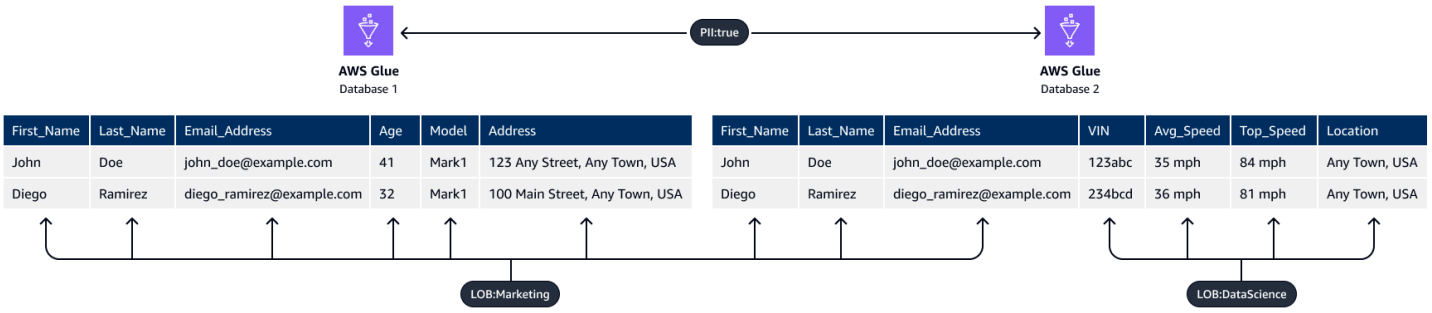
masuk AWS KMS. Dengan penyimpanan kunci eksternal, Anda harus membuat, mengkonfigurasi, dan memelihara penyimpanan kunci eksternal. Juga, jika ada kesalahan dalam infrastruktur tambahan yang harus Anda pertahankan, seperti proxy XKS, dan konektivitas hilang, pengguna mungkin untuk sementara tidak dapat mendekripsi dan mengakses data. Bekerja sama dengan pemangku kepentingan kepatuhan dan peraturan Anda untuk memahami kewajiban hukum dan kontrak untuk enkripsi data pribadi dan perjanjian tingkat layanan Anda untuk ketersediaan dan ketahanan.

AWS Lake Formation

Banyak organisasi yang membuat katalog dan mengkategorikan kumpulan data mereka melalui katalog metadata terstruktur ingin membagikan kumpulan data tersebut di seluruh organisasi mereka. Anda dapat menggunakan kebijakan izin AWS Identity and Access Management (IAM) untuk mengontrol akses ke seluruh kumpulan data, tetapi kontrol yang lebih terperinci sering diperlukan untuk kumpulan data yang berisi data pribadi dengan sensitivitas yang berbeda-beda. Misalnya, spesifikasi tujuan dan batasan penggunaan (situs web FPC) mungkin menunjukkan bahwa tim pemasaran memerlukan akses ke alamat pelanggan, tetapi tim ilmu data tidak.

Ada juga tantangan privasi yang terkait dengan data lake, yang memusatkan akses ke sejumlah besar data sensitif dalam format aslinya. Sebagian besar data organisasi dapat diakses secara terpusat di satu tempat, sehingga pemisahan data yang logis, terutama yang berisi data pribadi, dapat menjadi yang terpenting. AWS Lake Formationdapat membantu Anda mengatur tata kelola dan pemantauan saat berbagi data, apakah itu dari satu sumber atau banyak sumber yang terkandung dalam danau data. Di AWS PRA, Anda dapat menggunakan Lake Formation untuk memberikan kontrol akses berbutir halus ke data di bucket data bersama di akun Data.

Anda dapat menggunakan fitur kontrol akses berbasis tag di Lake Formation. Kontrol akses berbasis tag adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam Lake Formation, atribut ini disebut LF-tag. Dengan menggunakan LF-tag, Anda dapat melampirkan tag ini ke database, tabel, dan kolom Katalog Data dan memberikan tag yang sama ke prinsipal IAM. Lake Formation memungkinkan operasi pada sumber daya tersebut ketika prinsipal telah diberikan akses ke nilai tag yang cocok dengan nilai tag sumber daya. Gambar berikut menunjukkan bagaimana Anda dapat menetapkan LF-tag dan izin untuk memberikan akses berbeda ke data pribadi.



Contoh ini menggunakan sifat hierarki tag. Kedua database berisi informasi yang dapat diidentifikasi secara pribadi (`PII:true`), tetapi tag pada tingkat kolumnar membatasi kolom tertentu untuk tim yang berbeda. Dalam contoh ini, prinsipal IAM yang memiliki `PII:true` LF-tag dapat mengakses sumber daya AWS Glue database yang memiliki tag ini. Prinsipal dengan `LOB:DataScience` LF-tag dapat mengakses kolom tertentu yang memiliki tag ini, dan prinsipal dengan `LOB:Marketing` LF-tag hanya dapat mengakses kolom yang memiliki tag ini. Pemasaran hanya dapat mengakses PII yang relevan dengan kasus penggunaan pemasaran, dan tim ilmu data hanya dapat mengakses PII yang relevan dengan kasus penggunaannya.

AWS Local Zones

Jika Anda perlu mematuhi persyaratan residensi data, Anda dapat menyebarkan sumber daya yang menyimpan dan memproses data pribadi secara khusus Wilayah AWS untuk mendukung persyaratan ini. Anda juga dapat menggunakan AWS Local Zones, yang membantu Anda menempatkan komputasi, penyimpanan, database, dan AWS sumber daya pilihan lainnya dekat dengan populasi besar dan pusat industri. Zona Lokal adalah perpanjangan dari AWS Region yang berada dalam kedekatan geografis dengan wilayah metropolitan yang besar. Anda dapat menempatkan jenis sumber daya tertentu dalam Zona Lokal, di dekat Wilayah yang sesuai dengan Zona Lokal. Local Zones dapat membantu Anda memenuhi persyaratan residensi data ketika suatu Wilayah tidak tersedia dalam yurisdiksi hukum yang sama. Saat Anda menggunakan Local Zones, pertimbangkan kontrol residensi data yang diterapkan dalam organisasi Anda. Misalnya, Anda mungkin memerlukan kontrol untuk mencegah transfer data dari Zona Lokal tertentu ke Wilayah lain. Untuk informasi selengkapnya tentang SCPs cara menggunakan pagar pembatas transfer data lintas batas, lihat Praktik Terbaik untuk mengelola residensi data dalam menggunakan kontrol landing AWS Local Zones zone (AWS posting blog).

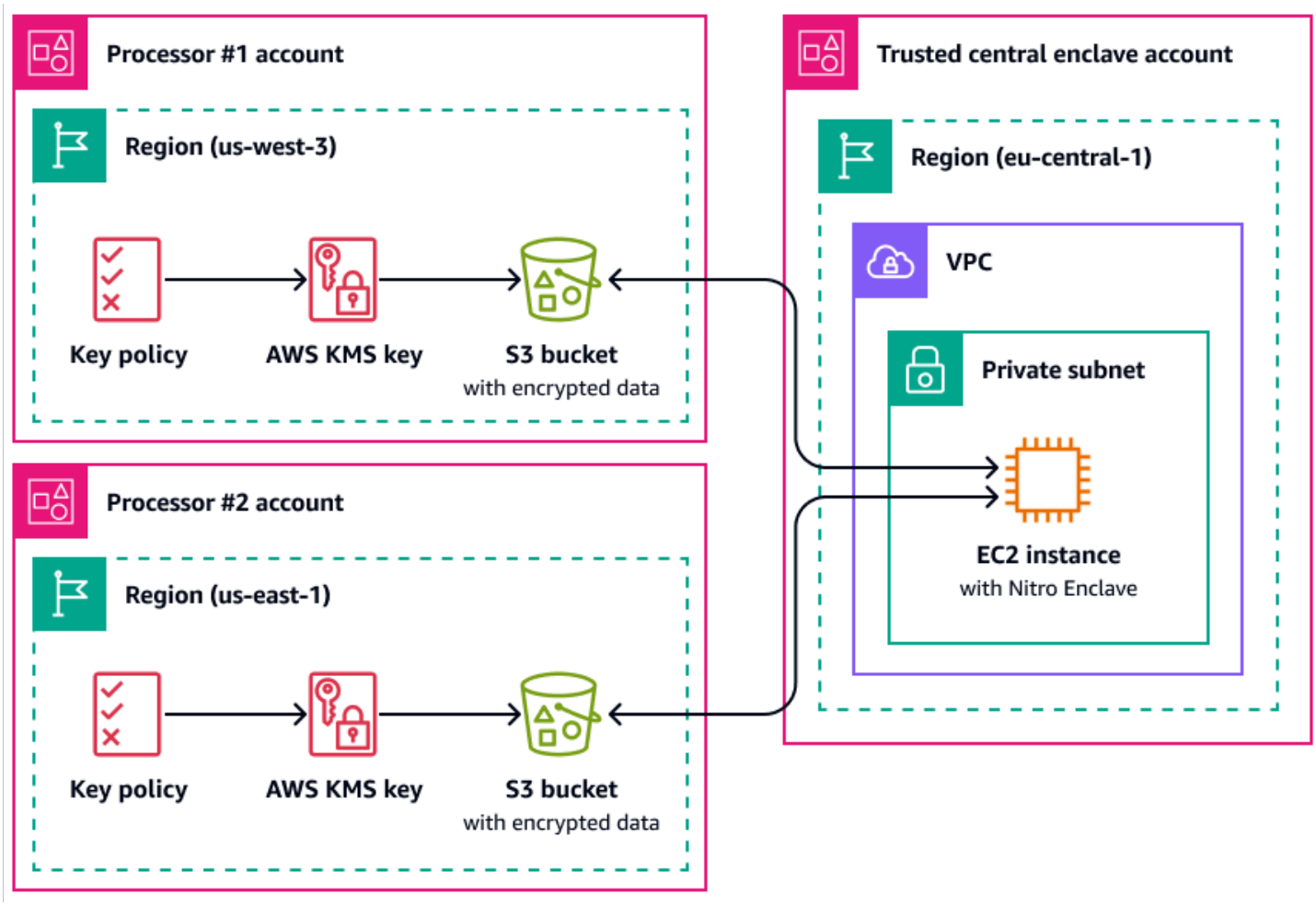
AWS Enklaf Nitro

Pertimbangkan strategi segmentasi data Anda dari perspektif pemrosesan, seperti memproses data pribadi dengan layanan komputasi seperti Amazon Elastic Compute Cloud (Amazon EC2). Komputasi

rahasia sebagai bagian dari strategi arsitektur yang lebih besar dapat membantu Anda mengisolasi pemrosesan data pribadi dalam kantong CPU yang terisolasi, terlindungi, dan tepercaya. Enklave adalah mesin virtual yang terpisah, mengeras, dan sangat dibatasi. AWS Nitro Enclave adalah fitur Amazon EC2 yang dapat membantu Anda membuat lingkungan komputasi yang terisolasi ini. Untuk informasi selengkapnya, lihat Desain Keamanan Sistem AWS Nitro (AWS whitepaper).

Nitro Enclave menyebarkan kernel yang dipisahkan dari kernel instance induk. Kernel instance induk tidak memiliki akses ke enklave. Pengguna tidak dapat SSH atau mengakses data dan aplikasi dari jarak jauh di enclave. Aplikasi yang memproses data pribadi dapat disematkan di kantong dan dikonfigurasi untuk menggunakan Vsock enklave, soket yang memfasilitasi komunikasi antara enclave dan instance induk.

Salah satu kasus penggunaan di mana Nitro Enclave dapat berguna adalah pemrosesan bersama antara dua prosesor data yang terpisah Wilayah AWS dan yang mungkin tidak saling percaya. Gambar berikut menunjukkan bagaimana Anda dapat menggunakan enklaf untuk pemrosesan pusat, kunci KMS untuk mengenkripsi data pribadi sebelum dikirim ke enklaf, dan AWS KMS key kebijakan yang memverifikasi bahwa enklaf yang meminta dekripsi memiliki pengukuran unik dalam dokumen pengesahan. Untuk informasi dan petunjuk selengkapnya, lihat Menggunakan pengesahan kriptografi dengan. AWS KMS Untuk contoh kebijakan kunci, lihat Memerlukan pengesahan untuk menggunakan kunci AWS KMS di panduan ini.



Dengan implementasi ini, hanya pengolah data masing-masing dan enklave yang mendasarinya yang memiliki akses ke data pribadi plaintext. Satu-satunya tempat data diekspos, di luar lingkungan masing-masing prosesor data, adalah di kantong itu sendiri, yang dirancang untuk mencegah akses dan gangguan.

AWS PrivateLink

Banyak organisasi ingin membatasi paparan data pribadi ke jaringan yang tidak tepercaya. Misalnya, jika Anda ingin meningkatkan privasi desain arsitektur aplikasi Anda secara keseluruhan, Anda dapat mengelompokkan jaringan berdasarkan sensitivitas data (mirip dengan pemisahan logis dan fisik kumpulan data yang dibahas di Layanan AWS dan fitur yang membantu mengelompokkan data bagian ini). AWS PrivateLinkmembantu Anda membuat koneksi pribadi searah dari cloud pribadi virtual Anda (VPCs) ke layanan di luar VPC. Dengan menggunakan AWS PrivateLink, Anda dapat mengatur koneksi pribadi khusus ke layanan yang menyimpan atau memproses data pribadi di lingkungan Anda; tidak perlu terhubung ke titik akhir publik dan mentransfer data ini melalui jaringan publik yang tidak tepercaya. Saat Anda mengaktifkan titik akhir AWS PrivateLink layanan untuk

layanan dalam lingkup, tidak perlu gateway internet, perangkat NAT, alamat IP publik, AWS Direct Connect koneksi, atau AWS Site-to-Site VPN koneksi untuk berkomunikasi. Saat Anda menggunakan AWS PrivateLink untuk menyambung ke layanan yang menyediakan akses ke data pribadi, Anda dapat menggunakan kebijakan titik akhir VPC dan grup keamanan untuk mengontrol akses, sesuai dengan definisi perimeter data organisasi Anda. Untuk contoh kebijakan titik akhir VPC yang hanya mengizinkan prinsip dan AWS sumber daya IAM di organisasi tepercaya untuk mengakses titik akhir layanan, lihat di panduan ini. Memerlukan keanggotaan organisasi untuk mengakses sumber daya VPC

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) membantu Anda berbagi sumber daya dengan aman Akun AWS untuk mengurangi overhead operasional dan memberikan visibilitas dan auditabilitas. Saat Anda merencanakan strategi segmentasi multi-akun Anda, pertimbangkan AWS RAM untuk menggunakan untuk berbagi penyimpanan data pribadi yang Anda simpan di akun terpisah dan terisolasi. Anda dapat membagikan data pribadi tersebut dengan akun tepercaya lainnya untuk keperluan pemrosesan. Di AWS RAM, Anda dapat mengelola izin yang menentukan tindakan apa yang dapat dilakukan pada sumber daya bersama. Semua panggilan API ke AWS RAM login CloudTrail. Selain itu, Anda dapat mengonfigurasi CloudWatch Acara Amazon untuk memberi tahu Anda secara otomatis tentang peristiwa tertentu AWS RAM, seperti saat perubahan dilakukan pada pembagian sumber daya.

Meskipun Anda dapat berbagi banyak jenis AWS sumber daya dengan orang lain Akun AWS dengan menggunakan kebijakan berbasis sumber daya di IAM atau kebijakan bucket di Amazon S3, AWS RAM memberikan beberapa manfaat tambahan untuk privasi. AWS memberi pemilik data visibilitas tambahan tentang bagaimana dan dengan siapa data dibagikan di seluruh Anda Akun AWS, termasuk:

- Mampu berbagi sumber daya dengan seluruh OU alih-alih memperbarui daftar akun secara manual IDs
- Penegakan proses undangan untuk inisiasi berbagi jika akun konsumen bukan bagian dari organisasi Anda
- Visibilitas ke mana prinsipal IAM tertentu memiliki akses ke setiap sumber daya individu

Jika sebelumnya Anda telah menggunakan kebijakan berbasis sumber daya untuk mengelola pembagian sumber daya dan ingin menggunakannya, AWS RAM gunakan operasi API. PromoteResourceShareCreatedFromPolicy

Amazon SageMaker AI

Amazon SageMaker AI adalah layanan pembelajaran mesin terkelola (ML) yang membantu Anda membangun dan melatih model ML, lalu menerapkannya ke lingkungan host yang siap produksi. SageMaker AI dirancang untuk mempermudah persiapan data pelatihan dan membuat fitur model.

Monitor SageMaker Model Amazon

Banyak organisasi mempertimbangkan penyimpangan data saat melatih model ML. Data drift adalah 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. Jika sifat statistik dari data yang diterima model ML dalam produksi menjauh dari sifat data dasar yang dilatihnya, keakuratan prediksi mungkin menurun. Amazon SageMaker Model Monitor dapat terus memantau kualitas model pembelajaran mesin Amazon SageMaker AI dalam produksi dan memantau kualitas data. Deteksi drift data secara dini dan proaktif dapat membantu Anda menerapkan tindakan korektif, seperti melatih ulang model, mengaudit sistem hulu, atau memperbaiki masalah kualitas data. Model Monitor dapat meringankan kebutuhan untuk memantau model secara manual atau membangun perkakas tambahan.

Amazon SageMaker Klarifikasi

Amazon SageMaker Clarify memberikan wawasan tentang bias model dan penjelasan. SageMaker Clarify biasanya digunakan selama persiapan data model ML dan fase pengembangan secara keseluruhan. Pengembang dapat menentukan atribut yang menarik, seperti jenis kelamin atau usia, dan SageMaker Clarify menjalankan serangkaian algoritme untuk mendeteksi adanya bias pada atribut tersebut. Setelah algoritme berjalan, SageMaker Clarify memberikan laporan visual dengan deskripsi sumber dan pengukuran kemungkinan bias sehingga Anda dapat mengidentifikasi langkah-langkah untuk memulihkan bias. Misalnya, dalam kumpulan data keuangan yang hanya berisi beberapa contoh pinjaman bisnis untuk satu kelompok umur dibandingkan dengan yang lain, SageMaker dapat menandai ketidakseimbangan sehingga Anda dapat menghindari model yang tidak menyukai kelompok usia tersebut. Anda juga dapat memeriksa model bias yang sudah terlatih dengan meninjau prediksinya dan dengan terus memantau model MLnya untuk bias. Terakhir, SageMaker Clarify terintegrasi dengan Amazon SageMaker AI Experiments untuk memberikan grafik yang menjelaskan fitur mana yang paling berkontribusi pada proses pembuatan prediksi model secara keseluruhan. Informasi ini dapat berguna untuk memenuhi hasil penjelasan, dan ini dapat membantu Anda menentukan apakah input model tertentu memiliki pengaruh lebih besar daripada yang seharusnya pada perilaku model secara keseluruhan.

Kartu SageMaker Model Amazon

Kartu SageMaker Model Amazon dapat membantu Anda mendokumentasikan detail penting tentang model ML Anda untuk tujuan tata kelola dan pelaporan. Rincian ini dapat mencakup pemilik model, tujuan umum, kasus penggunaan yang dimaksudkan, asumsi yang dibuat, peringkat risiko model, detail dan metrik pelatihan, dan hasil evaluasi. Untuk informasi lebih lanjut, lihat Model Explainability with AWS Artificial Intelligence and Machine Learning Solutions (AWS whitepaper).

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler adalah alat pembelajaran mesin yang membantu merampingkan persiapan data dan proses rekayasa fitur. Ini menyediakan antarmuka visual yang membantu ilmuwan data dan insinyur pembelajaran mesin untuk dengan cepat dan mudah mempersiapkan dan mengubah data untuk digunakan dalam model pembelajaran mesin. Dengan Data Wrangler, Anda dapat mengimpor data dari berbagai sumber, seperti Amazon S3, Amazon Redshift, dan Amazon Athena. Kemudian, Anda dapat menggunakan lebih dari 300 transformasi data bawaan untuk membersihkan, menormalkan, dan menggabungkan fitur tanpa harus menulis kode apa pun.

Data Wrangler dapat digunakan sebagai bagian dari persiapan data dan proses rekayasa fitur di PRA. AWS Ini mendukung enkripsi data saat istirahat dan dalam perjalanan dengan menggunakan AWS KMS, dan menggunakan peran dan kebijakan IAM untuk mengontrol akses ke data dan sumber daya. Ini mendukung penyembunyian data melalui AWS Glue atau Amazon SageMaker Feature Store. Jika Anda mengintegrasikan Data Wrangler AWS Lake Formation, Anda dapat menerapkan kontrol dan izin akses data berbutir halus. Anda bahkan dapat menggunakan Data Wrangler dengan Amazon Comprehend untuk secara otomatis menyunting data pribadi dari data tabular sebagai bagian dari alur kerja MLOps Anda yang lebih luas. Untuk informasi selengkapnya, lihat Menyunting PII secara otomatis untuk pembelajaran mesin menggunakan Amazon SageMaker Data Wrangler (AWS posting blog).

Fleksibilitas Data Wrangler membantu Anda menutupi data sensitif untuk banyak industri, seperti nomor rekening, nomor kartu kredit, nomor jaminan sosial, nama pasien, dan catatan medis dan militer. Anda dapat membatasi akses ke data sensitif apa pun atau memilih untuk menyuntingnya.

AWS fitur yang membantu mengelola siklus hidup data

Ketika data pribadi tidak lagi diperlukan, Anda dapat menggunakan siklus hidup dan time-to-live kebijakan untuk data di banyak penyimpanan data yang berbeda. Saat mengonfigurasi kebijakan penyimpanan data, pertimbangkan lokasi berikut yang mungkin berisi data pribadi:

- Database, seperti Amazon DynamoDB dan Amazon Relational Database Service (Amazon RDS)
- Bucket Amazon S3
- Log dari CloudWatch dan CloudTrail
- Data cache dari migrasi di AWS Database Migration Service (AWS DMS) dan proyek AWS Glue DataBrew
- Cadangan dan snapshot

Fitur Layanan AWS dan fitur berikut dapat membantu Anda mengonfigurasi kebijakan penyimpanan data di AWS lingkungan Anda:

- Siklus Hidup Amazon S3 — Seperangkat aturan yang menentukan tindakan yang diterapkan Amazon S3 pada sekelompok objek. Dalam konfigurasi Amazon S3 Lifecyle, Anda dapat membuat tindakan kedaluwarsa, yang menentukan kapan Amazon S3 menghapus objek kedaluwarsa atas nama Anda. Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan Anda.
- Amazon Data Lifecycle Manager — Di Amazon EC2, buat kebijakan yang mengotomatiskan pembuatan, penyimpanan, dan penghapusan snapshot Amazon Elastic Block Store (Amazon EBS) dan Amazon Machine Images () yang didukung EBS (). AMIs
- DynamoDB Time to Live (TTL) - Tentukan stempel waktu per item yang menentukan kapan item tidak lagi diperlukan. Tak lama setelah tanggal dan waktu stempel waktu yang ditentukan, DynamoDB menghapus item dari tabel Anda.
- Pengaturan penyimpanan CloudWatch log di Log — Anda dapat menyesuaikan kebijakan penyimpanan untuk setiap grup log dengan nilai antara 1 hari dan 10 tahun.
- AWS Backup— Terapkan kebijakan perlindungan data secara terpusat untuk mengonfigurasi, mengelola, dan mengatur aktivitas pencadangan Anda di berbagai AWS sumber daya, termasuk bucket S3, instance database RDS, tabel DynamoDB, volume EBS, dan banyak lagi. Terapkan kebijakan pencadangan ke AWS sumber daya Anda dengan menentukan jenis sumber daya atau memberikan perincian tambahan dengan menerapkan berdasarkan tag sumber daya yang ada. Audit dan laporkan aktivitas pencadangan dari konsol terpusat untuk membantu memenuhi persyaratan kepatuhan cadangan.

Layanan AWS dan fitur yang membantu mengelompokkan data

Segmentasi data adalah proses dimana Anda menyimpan data dalam wadah terpisah. Ini dapat membantu Anda memberikan langkah-langkah keamanan dan otentikasi yang berbeda untuk setiap kumpulan data dan untuk mengurangi cakupan dampak paparan untuk kumpulan data Anda secara

keseluruhan. Misalnya, alih-alih menyimpan semua data pelanggan dalam satu database besar, Anda dapat mengelompokkan data ini menjadi grup yang lebih kecil dan lebih mudah dikelola.

Anda dapat menggunakan pemisahan fisik dan logis untuk mengelompokkan data pribadi:

- Pemisahan fisik — Tindakan menyimpan data di penyimpanan data terpisah atau mendistribusikan data Anda ke AWS sumber daya yang terpisah. Meskipun data dipisahkan secara fisik, kedua sumber daya mungkin dapat diakses oleh prinsip yang sama. Inilah sebabnya mengapa kami merekomendasikan menggabungkan pemisahan fisik dengan pemisahan logis.
- Pemisahan logis — Tindakan mengisolasi data dengan menggunakan kontrol akses. Fungsi pekerjaan yang berbeda memerlukan tingkat akses yang berbeda ke himpunan bagian data pribadi. Untuk contoh kebijakan yang menerapkan pemisahan logis, lihat Berikan akses ke atribut Amazon DynamoDB tertentu di panduan ini.

Kombinasi pemisahan logis dan fisik memberikan fleksibilitas, kesederhanaan, dan perincian saat menulis kebijakan berbasis identitas dan sumber daya untuk mendukung akses yang berbeda di seluruh fungsi pekerjaan. Misalnya, dapat menjadi kompleks secara operasional untuk membuat kebijakan yang secara logis memisahkan klasifikasi data yang berbeda dalam satu bucket S3. Menggunakan bucket S3 khusus untuk setiap klasifikasi data menyederhanakan konfigurasi dan manajemen kebijakan.

Layanan AWS dan fitur yang membantu menemukan, mengklasifikasikan, atau membuat katalog data

Beberapa organisasi belum mulai menggunakan alat ekstrak, muat, dan transformasi (ELT) di lingkungan mereka untuk secara proaktif membuat katalog data mereka. Pelanggan ini mungkin berada pada tahap penemuan data awal, di mana mereka ingin lebih memahami data yang mereka simpan dan proses AWS dan bagaimana itu terstruktur dan diklasifikasikan. Anda dapat menggunakan Amazon Macie untuk lebih memahami data PII Anda di Amazon S3. Namun, Amazon Macie tidak dapat membantu Anda menganalisis sumber data lain, seperti Amazon Relational Database Service (Amazon RDS) dan Amazon Redshift. Anda dapat menggunakan dua pendekatan untuk mempercepat penemuan awal di awal latihan pemetaan data yang lebih besar:

- Pendekatan manual — Buat tabel dengan dua kolom dan baris sebanyak yang Anda butuhkan. Di kolom pertama, tulis karakterisasi data (seperti nama pengguna, alamat, atau jenis kelamin) yang mungkin ada di header atau badan paket jaringan atau dalam layanan apa pun yang Anda berikan. Mintalah tim kepatuhan Anda untuk menyelesaikan kolom kedua. Di kolom kedua, masukkan “ya”

jika data dianggap pribadi dan “tidak” jika tidak. Tunjukkan semua jenis data pribadi yang dianggap sangat sensitif, seperti denominasi agama atau data kesehatan.

- Pendekatan otomatis — Gunakan perkakas yang disediakan melalui AWS Marketplace. Salah satu alat tersebut adalah Securiti. Solusi ini menawarkan integrasi yang memungkinkan mereka memindai dan menemukan data di berbagai jenis AWS sumber daya, serta aset di platform layanan cloud lainnya. Banyak dari solusi yang sama ini dapat terus mengumpulkan dan memelihara inventaris aset data dan aktivitas pemrosesan data dalam katalog data terpusat. Jika Anda mengandalkan alat untuk melakukan klasifikasi otomatis, mungkin diperlukan penyetelan aturan penemuan dan klasifikasi untuk menyelaraskan dengan definisi data pribadi organisasi Anda.

Contoh kebijakan terkait privasi

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Banyak organisasi yang menangani data sensitif mengambil pendekatan preventif-maju, dengan lapisan kontrol detektif dan reaktif diterapkan secara keseluruhan. Bagian ini memberikan contoh kebijakan terkait privasi untuk AWS Identity and Access Management (IAM), AWS Organizations, dan (). AWS Key Management Service AWS KMS Kebijakan ini dapat membantu organisasi Anda memenuhi berbagai penggunaan, batasan pengungkapan, dan tujuan privasi transfer data lintas batas dengan menggunakan pendekatan pencegahan. Banyak dari kebijakan ini direferensikan di bagian sebelumnya dalam panduan ini.

Bagian ini berisi contoh kebijakan berikut:

- Memerlukan akses dari alamat IP tertentu
- Memerlukan keanggotaan organisasi untuk mengakses sumber daya VPC
- Batasi transfer data di seluruh Wilayah AWS
- Berikan akses ke atribut Amazon DynamoDB tertentu
- Batasi perubahan pada konfigurasi VPC
- Memerlukan pengesahan untuk menggunakan kunci AWS KMS

Memerlukan akses dari alamat IP tertentu

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Kebijakan ini memungkinkan `john_stiles` pengguna untuk mengambil peran IAM hanya jika panggilan berasal dari alamat IP dalam rentang `192.0.2.0/24` atau`203.0.113.0/24`. Kebijakan

ini dapat membantu mencegah pengungkapan data pribadi yang tidak diinginkan dan transfer data lintas batas yang tidak diinginkan. Misalnya, jika organisasi Anda memiliki staf dukungan pelanggan yang memerlukan akses ke data pribadi, Anda mungkin ingin staf pendukung tersebut mengakses data tersebut hanya dari kantor yang terletak di subset spesifik Wilayah AWS. Selain itu, verifikasi definisi PII organisasi Anda karena beberapa kebijakan mungkin memerlukan `Condition` atau `Principal` bagian yang membatasi akses ke pengguna atau alamat IP tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Memerlukan keanggotaan organisasi untuk mengakses sumber daya VPC

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Kebijakan titik akhir VPC ini hanya mengizinkan prinsipal dan sumber daya AWS Identity and Access Management (IAM) dari organisasi untuk `o-1abcde123` mengakses titik akhir Amazon Personalize (Amazon S3). Kontrol pencegahan ini membantu membangun zona kepercayaan dan menentukan perimeter data pribadi. Untuk informasi selengkapnya tentang bagaimana kebijakan ini dapat membantu melindungi privasi dan data pribadi di organisasi Anda, lihat AWS PrivateLink di panduan ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Batasi transfer data di seluruh Wilayah AWS

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Dengan pengecualian dua peran AWS Identity and Access Management (IAM), kebijakan kontrol layanan ini menolak panggilan API ke regional Layanan AWS Wilayah AWS selain `eu-west-1` dan. `eu-central-1` SCP ini dapat membantu mencegah pembuatan layanan AWS penyimpanan dan pemrosesan di Wilayah yang tidak disetujui. Ini dapat membantu mencegah data pribadi ditangani oleh Layanan AWS di Wilayah tersebut sama sekali. Kebijakan ini menggunakan `NotAction` parameter karena menyumbang global Layanan AWS, seperti IAM, dan layanan yang terintegrasi dengan layanan global, seperti AWS Key Management Service (AWS KMS) dan Amazon CloudFront. Dalam nilai parameter, Anda dapat menentukan layanan global dan layanan lain yang tidak berlaku sebagai pengecualian. Untuk informasi selengkapnya tentang bagaimana kebijakan ini dapat membantu melindungi privasi dan data pribadi di organisasi Anda, lihat AWS Organizations di panduan ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
```

```
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
```

```
        }
    ]
}
```

Berikan akses ke atribut Amazon DynamoDB tertentu

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Saat organisasi Anda mendiskusikan strategi untuk memisahkan data pribadi secara fisik dan logis, pertimbangkan layanan AWS penyimpanan mana yang mendukung kebijakan kontrol akses berbutir halus di AWS Identity and Access Management (IAM). Kebijakan berbasis identitas berikut memungkinkan pengambilan hanya `LastLoggedIn` atribut`UserID`,`SignUpTime`, dan dari tabel Amazon DynamoDB bernama. `Users` Misalnya, Anda dapat melampirkan kebijakan ini ke peran dukungan pelanggan alih-alih memberikan akses peran ini ke kumpulan data pribadi lengkap. Untuk informasi selengkapnya tentang bagaimana kebijakan ini dapat membantu melindungi privasi dan data pribadi di organisasi Anda, lihat Layanan AWS dan fitur yang membantu mengelompokkan data di panduan ini.

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
```

```
                "SignUpTime",
                "LastLoggedIn"
            ]
         },
         "StringEquals":{
            "dynamodb:Select":[
               "SPECIFIC_ATTRIBUTES"
            ]
         }
      }
   ]
}
```

Batasi perubahan pada konfigurasi VPC

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Setelah merancang dan menerapkan AWS infrastruktur yang mendukung persyaratan transfer data lintas batas, yang mencakup aliran data jaringan, Anda mungkin ingin mencegah modifikasi. Kebijakan kontrol layanan berikut membantu mencegah penyimpangan konfigurasi VPC atau modifikasi yang tidak disengaja. Ini menyangkal lampiran gateway internet baru, koneksi peering VPC, lampiran gateway transit, dan koneksi VPN baru. Untuk informasi selengkapnya tentang bagaimana kebijakan ini dapat membantu melindungi privasi dan data pribadi di organisasi Anda, lihat AWS Transit Gateway di panduan ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
```

```
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Memerlukan pengesahan untuk menggunakan kunci AWS KMS

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Kebijakan kunci berikut AWS Key Management Service (AWS KMS) memungkinkan instance AWS Nitro Enclave menggunakan kunci KMS hanya jika dokumen pengesahan enclave dalam permintaan cocok dengan pengukuran dalam pernyataan kondisi. Kebijakan ini hanya mengizinkan enklaf tepercaya untuk mendekripsi data. Untuk informasi selengkapnya tentang bagaimana kebijakan ini dapat membantu melindungi privasi dan data pribadi di organisasi Anda, lihat AWS Enklaf Nitro di panduan ini. Untuk daftar lengkap kunci AWS KMS kondisi yang dapat digunakan dalam kebijakan

utama dan kebijakan AWS Identity and Access Management (IAM), lihat Kunci kondisi untuk AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
               "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
               "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

Strategi untuk ekspansi global

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

AWS Layanan Jaminan Keamanan sering menerima pertanyaan mengenai arsitektur privasi AWS saat memperluas secara global. Pertanyaan berkisar pada kekhawatiran dengan menjaga kepatuhan terhadap persyaratan privasi yang unik, seperti kewajiban kedaulatan data atau kontrak pelanggan, sambil menghindari biaya tambahan dan overhead operasional. Pertimbangan desain sering kali mencakup residensi data, pembatasan akses operator, ketahanan dan kemampuan bertahan hidup, dan kemandirian secara keseluruhan. Untuk informasi lebih lanjut, lihat Memenuhi persyaratan kedaulatan digital pada AWS (AWS re:Invent 2022 presentation).

Pertanyaan-pertanyaan berikut adalah umum, dan hanya Anda yang dapat menjawabnya untuk kasus penggunaan Anda:

- Di mana data pribadi pelanggan saya harus berada?
- Di mana data pelanggan saya disimpan?
- Bagaimana dan di mana data pribadi dapat melintasi batas?
- Apakah akses manusia atau layanan ke data lintas wilayah merupakan transfer?
- Bagaimana saya bisa yakin bahwa tidak ada pemerintah asing yang mengakses data pribadi pelanggan saya?
- Di mana saya dapat menyimpan cadangan dan situs panas atau dingin saya?
- Untuk menjaga data lokal, haruskah saya mempertahankan AWS landing zone di setiap wilayah tempat saya menyediakan layanan? Atau bisakah saya menggunakan AWS Control Tower landing zone yang sudah ada?

Untuk persyaratan residensi data, penerapan arsitektur yang berbeda mungkin bekerja lebih baik untuk organisasi yang berbeda. Beberapa organisasi mungkin memiliki persyaratan bahwa data pribadi pelanggan mereka tetap berada dalam wilayah tertentu. Jika demikian, Anda mungkin khawatir dengan cara mematuhi peraturan secara umum sambil menegakkan kewajiban ini. Apa pun situasinya, ada beberapa pertimbangan saat memilih strategi penyebaran multi-akun.

Untuk menentukan komponen desain arsitektur utama, bekerja sama dengan tim kepatuhan dan kontrak Anda untuk mengonfirmasi persyaratan di mana, kapan, dan bagaimana data pribadi dapat melintas Wilayah AWS. Tentukan apa yang memenuhi syarat sebagai transfer data, seperti memindahkan, menyalin, atau melihat. Selain itu, pahami apakah ada ketahanan khusus dan kontrol perlindungan data yang harus diterapkan. Apakah strategi pencadangan dan pemulihan bencana memerlukan failover lintas wilayah? Jika demikian, tentukan Wilayah mana yang dapat Anda gunakan untuk menyimpan data cadangan Anda. Tentukan apakah ada persyaratan untuk enkripsi data, seperti algoritma enkripsi khusus atau modul keamanan perangkat keras khusus untuk pembuatan kunci. Setelah Anda menyelaraskan dengan pemangku kepentingan kepatuhan pada topik ini, mulailah mempertimbangkan pendekatan desain untuk lingkungan multi-akun Anda.

Berikut ini adalah tiga pendekatan yang dapat Anda gunakan untuk merencanakan strategi AWS multi-akun Anda, dalam urutan pemisahan infrastruktur yang meningkat:

- Central landing zone dengan Wilayah terkelola
- Zona pendaratan regional
- AWS Awan Berdaulat Eropa

Penting juga untuk diingat bahwa kepatuhan privasi mungkin tidak berhenti hanya pada kedaulatan data. Tinjau sisa panduan ini untuk memahami solusi yang mungkin untuk banyak tantangan lain, seperti manajemen persetujuan, permintaan subjek data, tata kelola data, dan bias AI.

Central landing zone dengan Wilayah terkelola

Jika Anda ingin memperluas secara global tetapi telah membuat arsitektur multi-akun di AWS, biasanya ingin menggunakan landing zone multi-akun (MALZ) yang sama untuk mengelola tambahan. Wilayah AWS Dalam konfigurasi ini, Anda akan terus mengoperasikan layanan infrastruktur seperti logging, pabrik akun, dan administrasi umum dari AWS Control Tower landing zone yang ada, di Wilayah tempat Anda membuatnya.

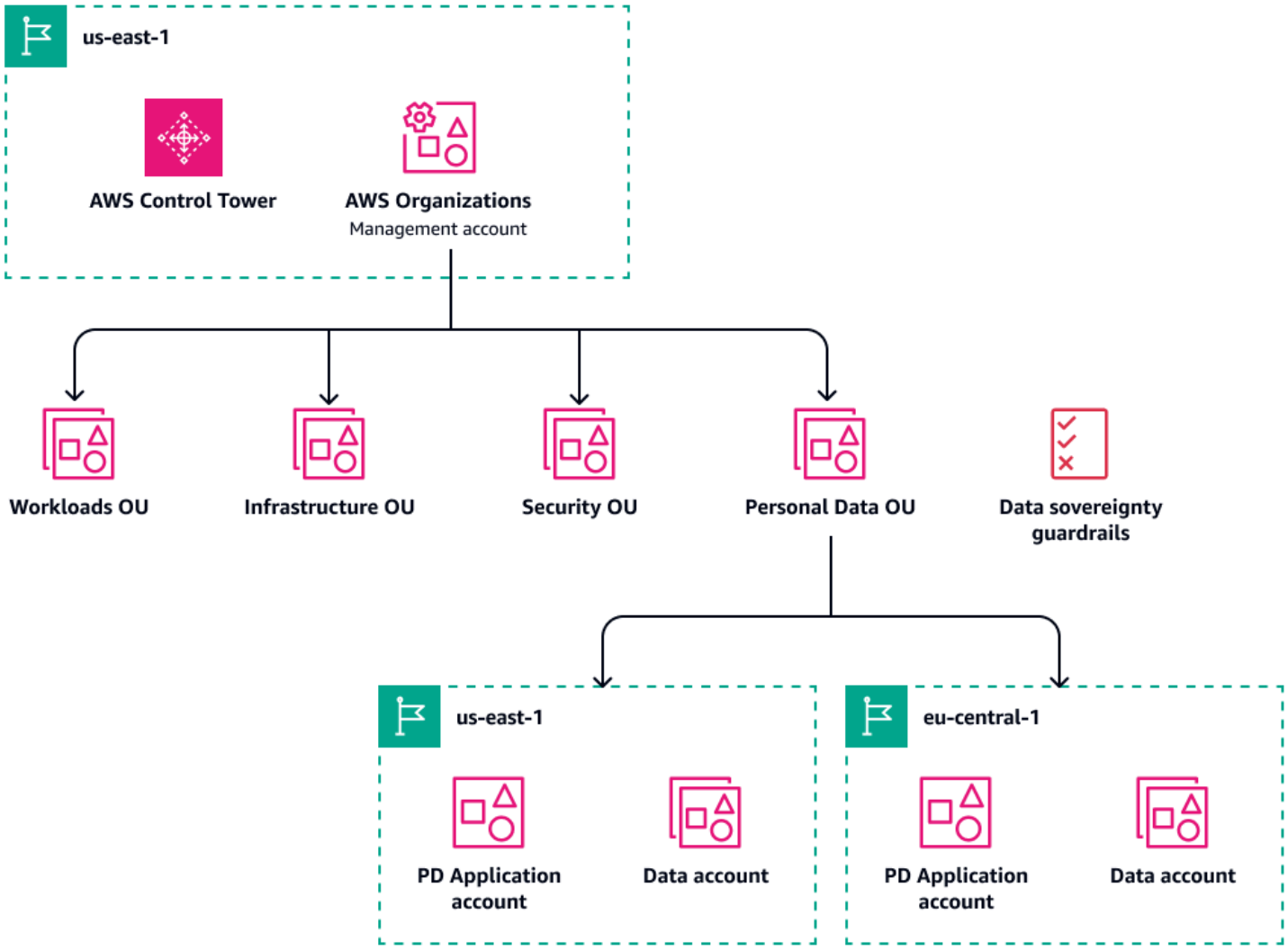
Untuk beban kerja produksi, Anda dapat mengoperasikan penyebaran Regional dengan memperluas AWS Control Tower landing zone ke Wilayah baru. Dengan melakukan ini, Anda dapat memperluas AWS Control Tower tata kelola ke Wilayah baru. Dengan cara ini, Anda dapat menyimpan penyimpanan data pribadi dalam Wilayah tertentu yang dikelola, data masih berada di akun yang mendapat manfaat dari layanan infrastruktur dan AWS Control Tower tata kelola. Di AWS Organizations, akun yang berisi data pribadi masih digulung di bawah OU Data Pribadi khusus, di mana semua pagar pembatas kedaulatan data diimplementasikan. AWS Control Tower Selain itu,

beban kerja khusus Wilayah terkandung dalam akun khusus, daripada membuat akun produksi yang mungkin berisi beban kerja yang sama di beberapa Wilayah.

Penyebaran ini dapat menjadi yang paling hemat biaya, tetapi pertimbangan tambahan diperlukan untuk mengendalikan aliran data pribadi melintasi Akun AWS dan batas-batas Regional. Pertimbangkan hal berikut:

- Log mungkin berisi data pribadi, sehingga beberapa konfigurasi tambahan mungkin diperlukan untuk memuat atau menyunting bidang sensitif untuk mencegah transfer lintas wilayah selama agregasi. Untuk informasi selengkapnya dan praktik yang direkomendasikan untuk mengontrol agregasi log di seluruh Wilayah, lihat Penyimpanan log terpusat di panduan ini.
- Akun untuk isolasi VPCs dan arus lalu lintas jaringan dua arah yang sesuai dalam desain. AWS Transit Gateway Anda dapat membatasi lampiran Transit Gateway mana yang diizinkan dan disetujui, dan Anda dapat membatasi siapa atau apa yang dapat mengubah tabel rute VPC.
- Anda mungkin perlu mencegah anggota tim operasi cloud Anda mengakses data pribadi. Misalnya, log aplikasi yang berisi data transaksi pelanggan dapat dianggap memiliki sensitivitas yang lebih tinggi daripada sumber log lainnya. Persetujuan tambahan dan pagar pembatas teknis mungkin diperlukan, seperti kontrol akses berbasis peran dan kontrol akses berbasis atribut. Selain itu, data mungkin tunduk pada batasan tempat tinggal dalam hal akses. Misalnya, data di satu Wilayah A hanya dapat diakses dari dalam Wilayah tersebut.

Diagram berikut menunjukkan landing zone terpusat dengan penyebaran Regional.



Zona pendaratan regional

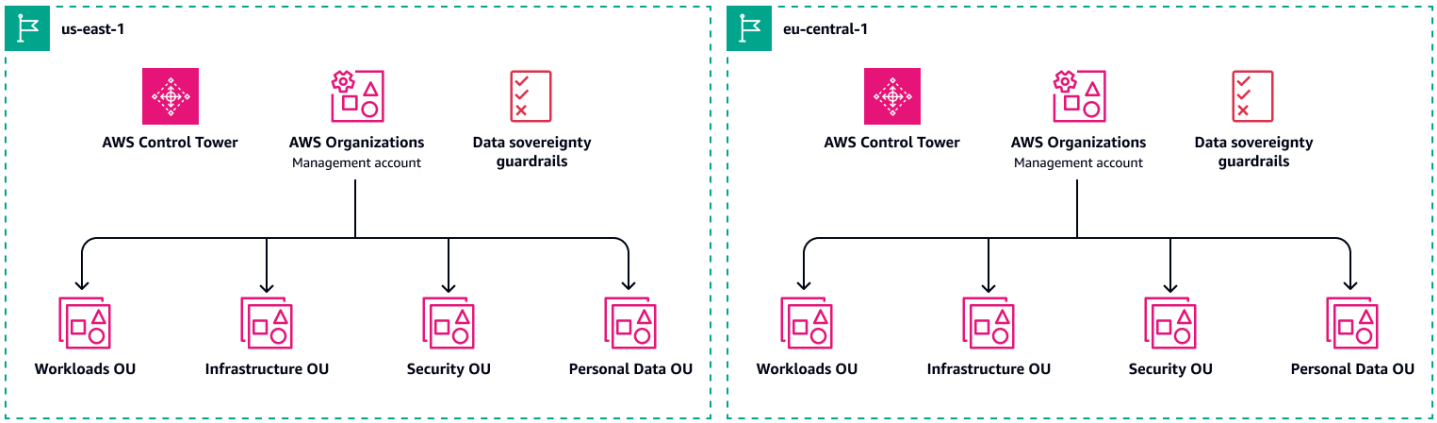
Memiliki lebih dari satu MALZ dapat membantu Anda mencapai persyaratan kepatuhan yang lebih ketat dengan sepenuhnya mengisolasi beban kerja yang memproses data pribadi dibandingkan dengan beban kerja non-material. AWS Control Tower agregasi logging terpusat dapat dikonfigurasi secara default dan karenanya disederhanakan. Dengan pendekatan ini, Anda tidak perlu mempertahankan pengecualian untuk logging dengan aliran log terpisah yang memerlukan redaksi. Anda bahkan dapat memiliki tim operasi cloud lokal dan khusus untuk setiap MALZ, yang membatasi akses operator ke residensi lokal.

Banyak organisasi memiliki penyebaran landing zone berbasis AS dan Uni Eropa yang terpisah. Setiap landing zone regional memiliki postur keamanan tunggal dan tata kelola terkait untuk akun di

Wilayah. Misalnya, enkripsi data pribadi menggunakan dedicated HSMs mungkin tidak diperlukan dalam beban kerja di satu MALZ, tetapi mungkin diperlukan di MALZ lain.

Meskipun strategi ini dapat disesuaikan untuk memenuhi banyak persyaratan saat ini dan masa depan, penting untuk memahami biaya tambahan dan overhead operasional yang terkait dengan pemeliharaan beberapa MALZs. Untuk informasi selengkapnya, lihat harga AWS Control Tower.

Diagram berikut menunjukkan zona pendaratan terpisah di dua Wilayah.



AWS Awan Berdaulat Eropa

Beberapa organisasi memerlukan pemisahan menyeluruh dari beban kerja mereka yang beroperasi di Wilayah Ekonomi Eropa (EEA) dan beban kerja yang beroperasi di tempat lain. Dalam situasi ini, pertimbangkan AWS European Sovereign Cloud. AWS European Sovereign Cloud adalah cloud independen baru untuk Eropa, yang dirancang untuk membantu pelanggan memenuhi kebutuhan kedaulatan kawasan yang terus berkembang, termasuk residensi data yang ketat, otonomi operasional, dan persyaratan ketahanan.

AWS European Sovereign Cloud secara fisik dan logis terpisah dari yang ada Wilayah AWS, semuanya menawarkan keamanan, ketersediaan, dan kinerja yang sama. Hanya AWS karyawan yang berlokasi di UE yang memiliki kendali atas operasi dan dukungan untuk AWS European Sovereign Cloud. Jika Anda memiliki persyaratan residensi data yang ketat, AWS European Sovereign Cloud menyimpan semua metadata yang Anda buat (seperti peran, izin, label sumber daya, dan konfigurasi yang digunakan untuk dijalankan) di UE. AWS AWS European Sovereign Cloud juga memiliki sistem penagihan dan pengukuran penggunaannya sendiri.

Untuk pendekatan ini, Anda akan menggunakan pola yang sama seperti pada bagian sebelumnya, zona pendaratan Regional. Namun, untuk layanan yang Anda berikan kepada pelanggan Eropa, Anda dapat menggunakan MALZ khusus di AWS European Sovereign Cloud.

Sumber daya

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

AWS Bimbingan Preskriptif

- AWS Arsitektur Referensi Keamanan (AWS SRA)

AWS dokumentasi

- Perlindungan data (AWS Well-Architected Framework)
- Klasifikasi data (AWS whitepaper)
- Amazon Web Services: Risiko dan Kepatuhan (AWS whitepaper)
- Arsitektur hybrid untuk memenuhi persyaratan pemrosesan data pribadi (AWS whitepaper)
- Menavigasi Kepatuhan GDPR di AWS (whitepaper)AWS
- Membangun perimeter data pada AWS (AWS whitepaper)
- AWS Dokumentasi Keamanan

AWS Sumber daya lainnya

- AWS Program Kepatuhan
- AWS Model Tanggung Jawab Bersama
- FAQ Privasi Data
- AWS Layanan Jaminan Keamanan
- AWS Ikrar Kedaulatan Digital: Kontrol tanpa kompromi (posting blog)AWS
- AWS Pembelajaran Keamanan

Kontributor

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

Panduan ini ditulis oleh tim AWS Security Assurance Services. Untuk mendukung penerapan rekomendasi dalam panduan ini dan mengoperasionalkan beban kerja Anda, hubungi tim Layanan AWS Jaminan Keamanan.

Penulis utama

- Amber Welch, Konsultan Privasi AWS Senior
- Daniel Nieters, Konsultan Privasi AWS Utama
- Robert Carter, Manajer Program AWS Teknis

Kontributor

- Avik Mukherjie, Konsultan Keamanan Senior AWS
- David Bounds, Arsitek Solusi AWS Senior
- Jeff Lombardo, Arsitek Solusi Keamanan AWS Senior
- Ram Ramani, AWS Arsitek Solusi Keamanan Utama
- Vanessa Jacobs, Konsultan Keamanan Senior AWS
- Thomas Nicholson, Konsultan Privasi AWS Senior
- Jose DeJesus, Konsultan AWS Jaminan Senior
- Doug Pardue, Manajer Arsitek AWS Solusi

Penulis teknis

- Lilly AbouHarb, Penulis Teknis AWS Senior

Riwayat dokumen

> **Survei**
>
> Kami akan senang mendengar dari Anda. Harap berikan umpan balik tentang AWS PRA dengan mengikuti survei singkat.

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
Pembaruan signficant	Kami menambahkan Cloud Computing Compliance Controls Catalog (C5) ke AWS Artifactbagian tersebut. Kami menambahkan Amazon Security Lake ke akun Log Archive. Kami menambahk an Amazon Bedrock, Amazon AWS Clean Rooms, DataZone AWS Lake Formation, Amazon SageMaker AI, Layanan AWS dan fitur yang membantu menemukan, mengklasi fikasikan, atau membuat katalog data ke akun Aplikasi PD. Kami menambahkan bagian Strategi untuk ekspansi global.	September 16, 2025
Pembaruan signficant	Kami membuat pembaruan yang signifikan di seluruh.	26 Maret 2024
Publikasi awal	—	2 Oktober 2023

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

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

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

FM

Lihat model pondasi.

model pondasi (FM)

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

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

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

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

data penahanan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

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

layanan mikro

Layanan kecil dan independen yang berkomunikasi dengan jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk

informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

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

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

ketekunan poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

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

publish/subscribe (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

LAP

Lihat Retrieval Augmented Generation.

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Region

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM merujuk sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan

pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

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

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

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

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

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

T

tag

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

variabel target

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

daftar tugas

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

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang

memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

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

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan

ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

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

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

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

data hangat

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

fungsi jendela

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

bisikan zero-shot

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

aplikasi zombie

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

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