AWS 프라이버시 참조 아키텍처

AWS 권장 가이드

AWS 권장 가이드: AWS 프라이버시 참조 아키텍처

Table of Contents

AWS 프라이버시 참조 아키텍처

Amazon Web Services(기여자)

2025년 9월(문서 기록)

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

Notices

이 가이드는 정보 목적으로만 제공됩니다. 이는 법적 조언이 아니며 법률 조언으로 의존해서는 안 됩니다.는 고객이 개인 정보 보호 및 데이터 보호 환경의 구현에 대한 적절한 조언과 보다 일반적으로 비즈니스와 관련된 관련 법률을 얻을 것을 AWS 권장합니다.

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 (a) 정보 제공 목적으로만 사용되며, (b) 예고 없이 변경될 수 있는 현재 AWS 제품 제공 및 관행을 나타내며, (c) AWS 및 그 계열사, 공급업체 또는 라이센서로부터 어떠한 약정 또는 보증도 생성하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 표현 또는 조건 없이 "있는 그대로" 제공됩니다.

고객에 AWS 대한의 책임과 책임은 계약에 의해 AWS 관리되며,이 문서는 AWS 와 고객 간의 계약의 일부이거나 수정하지 않습니다.

소개

개인 AWS 정보 보호 참조 아키텍처(AWS PRA)는에서 개인 정보 보호 지원 제어의 설계 및 구성과 관련된 일련의 지침을 제공합니다 AWS 서비스. 이 가이드는 AWS 클라우드에서 개인 정보 보호를 지원하는 데 도움이 되는 사람, 프로세스 및 기술에 대한 결정을 내리는 데 도움이 될 수 있습니다.

AWS 공동 책임 모델 및 개인 정보 보호

에서는 보안 및 규정 준수에 대한 책임을 AWS 클라우드공유합니다 AWS. AWS 는 클라우드의 보안을 담당합니다. 즉, AWS 는에서 제공되는 모든 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. 클라우드의 보안에 대한 책임은 사용자에게 있습니다. 즉, 보안 및 개인 정보 보호 요구

사항에 AWS 서비스 따라를 구성하고 관리할 책임은 사용자에게 있습니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

AWS 서비스 는 개인 정보 요구 사항을 지원하기 위해 클라우드에서 자체 개인 정보 제어를 구현할 수 있는 기능을 제공합니다. 개인 정보 보호 책임은 AWS 리전 선택한 AWS 서비스 및 , 해당 서비스를 IT 환경에 통합, 조직 및 워크로드에 적용되는 법률과 규정을 비롯한 여러 요인에 따라 달라집니다.

를 사용할 때 콘텐츠에 대한 제어를 AWS 서비스유지합니다. 특히 고객 콘텐츠는 사용자 또는 최종 사용자가 계정과 관련하여에서 처리, 저장 또는 호스팅하기 위해 당사 AWS 서비스 로 전송하는 소프트웨어(기계 이미지 포함), 데이터, 텍스트, 오디오, 비디오 또는 이미지로 정의됩니다. 또한 사용자 또는 최종 사용자가를 사용하여 도출하는 모든 계산 결과도 포함됩니다 AWS 서비스. 사용자는 다음 결정을 관리할 책임이 있으며 이는 사용자가 제어합니다.

- 에서 수집, 저장 또는 처리하도록 선택한 데이터 AWS
- 데이터와 함께 AWS 서비스 사용하는
- 데이터를 수집, 저장 또는 처리하는 AWS 리전
- 데이터의 형식 및 구조와 마스킹, 익명화 또는 암호화 여부
- 암호화를 위한 암호화 키를 정의, 저장, 교체 및 운영하는 방법
- 액세스 권한이 있는 사용자 및 데이터에 대한 액세스 권한을 보유하는 시점 그리고 이러한 액세스 권한이 부여, 관리 및 취소되는 방법

AWS 공동 책임 모델과 클라우드 운영에 일반적으로 적용되는 방식을 이해한 후에는 사용 사례에 적용되는 방법을 결정해야 합니다. 사용하기로 AWS 서비스 선택한에 따라 조직의 개인 정보 보호 책임의 일부로 수행해야 하는 구성의 양이 결정됩니다. 예를 들어 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 서비스는 서비스형 인프라(IaaS)로 분류됩니다. 따라서 Amazon EC2를 사용하는 경우 게스트 운영 체제와 EC2 인스턴스에 설치하는 애플리케이션 소프트웨어 또는 유틸리티에 필요한 모든 개인 정보 보호 구성을 수행해야 합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB와 같은 추상화된 서비스를 사용하는 경우 인프라 계층, 운영 체제 및 플랫폼을 AWS 담당합니다. 데이터(고객 콘텐츠)를 관리 및 분류하고 데이터를 저장 및 검색하기 위해 엔드포인트에 액세스하는 데 사용되는 정책을 구성하는 것은 사용자의 책임입니다. AWS 가 데이터 및 개인 정보 보호를 지원하는 방법에 대한 자세한 내용은 의 데이터 보호 및 개인 정보 AWS 보호를 참조하세요.

AWS PRA 이해

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

이 섹션에서는 AWS 프라이버시 참조 아키텍처(AWS PRA)와 기타 AWS 지침 간의 관계를 설명합니다. 또한이 섹션에서는 AWS PRA의 예제 AWS 다중 계정 환경의 일반적인 레이아웃과 구조를 검토합니다.

이 섹션은 다음 주제를 포함합니다:

- AWS PRA 및 AWS SRA 사용
- AWS Organizations 및 전용 계정 구조
- AWS 개인 정보 보호 서비스 운영

AWS PRA 및 AWS SRA 사용

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

AWS PRA는 고객이 인프라 및 워크로드에 대한 기본 및 애플리케이션 수준 프라이버시 제어를 계획하는 데 도움이 되는 패턴을 제공합니다 AWS. AWS 보안 참조 아키텍처(AWS SRA)는 AWS 랜딩 존 및 애플리케이션 전반에서 적절한 보안 제어 세트를 구현하고 지원하는 아키텍처를 구축하기 위한 일련의 지침을 제공합니다. 이 가이드에 자세히 설명된 개인 정보 보호 제어를 설정하기 위해 AWS PRA는 AWS SRA에 설명된 것과 동일한 기본 지침 및 계정 구조를 다수 가정합니다. AWS PRA와 AWS SRA는 많은 동일한 키를 자세히 설명합니다 AWS 서비스. 이 가이드에는 이러한 서비스에 대한 간략한 설명만 포함되어 있습니다. 이러한 서비스와 AWS SRA의 보안 컨텍스트에서 사용되는 방법에 대해 자세히 알아볼 수 있습니다.

AWS SRA는 AWS 권장 사례에 맞게 AWS 보안 서비스를 설계, 구현 및 관리하는 데 도움이 될 수 있습니다. AWS SRA를 독립 실행형 가이드로 사용하거나 AWS SRA 및 AWS PRA를 컴패니언 가이드

로 사용할 수 있습니다. AWS SRA에 자세히 설명된 많은 보안 지침을 AWS PRA에 자세히 설명된 개인 정보 보호 제어와 함께 따를 수 있습니다. 보안과 마찬가지로 AWS 클라우드 여정 초기에 수행하는 데 도움이 될 수 있는 기본적인 개인 정보 보호 고려 사항이 있습니다. 이러한 결정은 조직의 계정 구조 설계에 영향을 미칠 수 있기 때문입니다. 예를 들어 고려할 수 있는 몇 가지 질문은 다음과 같습니다.

- 조직에서 개인 데이터를 어떻게 정의하나요?
- 내 조직은 개인 데이터를 처리하는 애플리케이션을 지원하나요?
- 다른 유형의 규제 데이터를 처리하는 애플리케이션은 어떤가요?
- 개발자와 클라우드 엔지니어가 개인 데이터로부터 최대한 멀리 떨어져 있도록 하기 위해 어떤 조직 수준의 제어를 구현할 수 있나요?
- 개인 데이터를 다른 유형의 데이터와 분리하려면 어떻게 해야 하나요?
- 내 조직의 국가 간 데이터 전송 요구 사항은 무엇인가요?

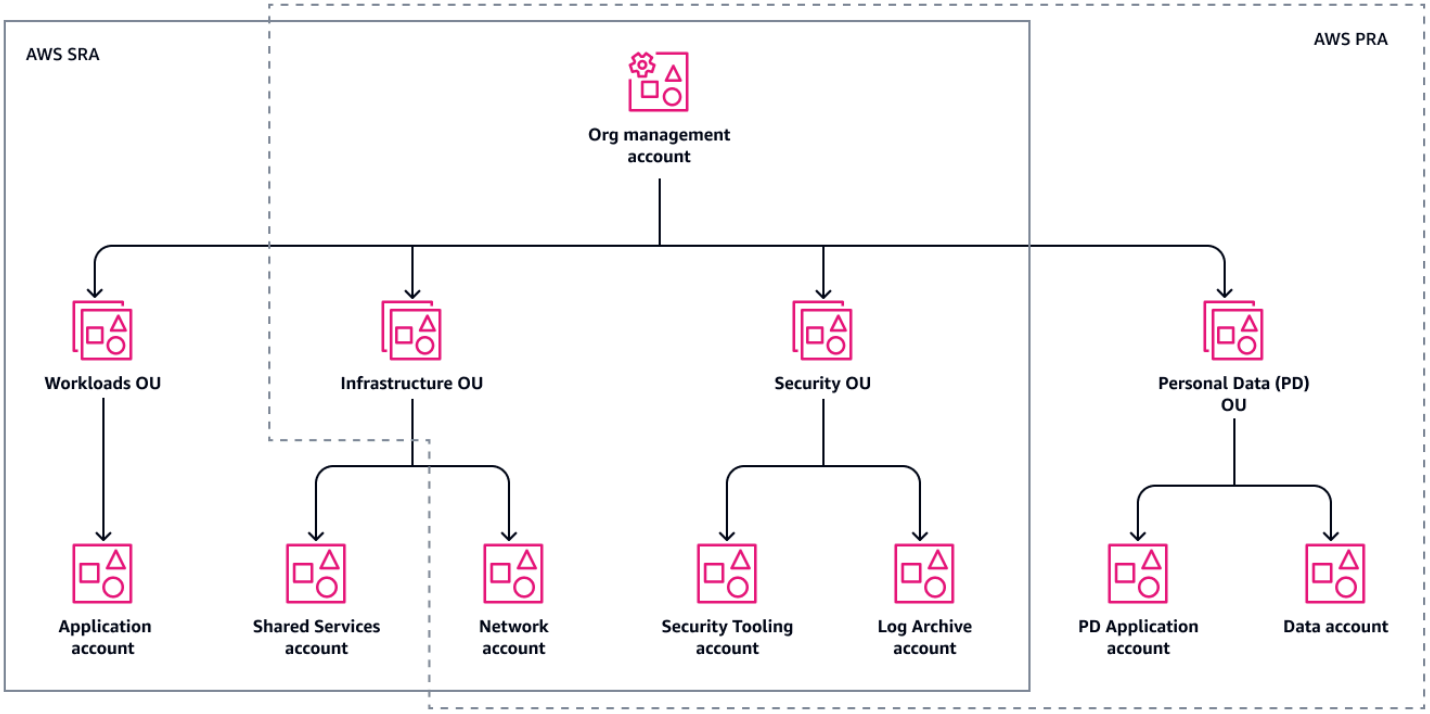
이러한 많은 질문에 대한 답변은 AWS 계정 구조, 서비스 제어 정책 및 AWS Identity and Access Management (IAM) 역할과 같은 클라우드 환경 설계에 영향을 미칠 수 있습니다.

AWS Organizations 및 전용 계정 구조

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

AWS Organizations는 여러 AWS 계정을 중앙에서 관리하고 관리하는 데 도움이 되는 계정 관리 서비스입니다. 의 사용은 잘 설계된 다중 계정 AWS 환경의 기반 AWS Organizations 입니다. 자세한 내용은 Establishing your best practice AWS environment를 참조하세요.

다음 다이어그램은 AWS PRA의 상위 수준 계정 및 조직 단위(OU) 구조를 보여줍니다. 대부분의 경우, PRA의 AWS 조직 구조는 AWS SRA의 조직 구조와 일치합니다.



AWS SRA 조직과의 편차는 다음과 같습니다.

- AWS 개인 데이터 수집, 저장 및 처리 전용 개인 데이터(PD) OU가 추가됩니다. 이러한 구조적 분리는 유연성을 제공하므로 개인 데이터가 의도치 않게 공개되지 않도록 보호하는 데 도움이 되는 구체적이고 세분화된 제어를 정의할 수 있습니다.
- 인프라 OU에서 AWS 현재 PRA는 AWS SRA에 설명된 공유 서비스 계정에 대한 추가 지침을 포함하지 않습니다.
- 현재 AWS PRA에는 AWS SRA에 설명된 워크로드 OU에 대한 추가 지침이 포함되어 있지 않습니다. 개인 데이터를 수집하거나 처리하는 애플리케이션은 PD OU의 전용 계정에 있습니다.

AWS Control Tower를 사용하여 조직 전체에 보안 및 개인 정보 보호 제어의 전반적인 기본 거버넌스와 자동화된 배포를 수행할 수 있습니다. AWS Control Tower 가 현재 조직에서 사용되지 않는 경우에도 서비스 제어 정책 및 AWS Config 규칙 AWS Control Tower과 같은 많은 보안 및 개인 정보 보호 제어를 해당 서비스에 배포할 수 있습니다.

계정 세분화 전략을 포함하여 계정 및 OU 구조를 계획할 때 개인 데이터 처리를 고려하는 것이 도움이 될 수 있습니다. 고유한 사용 사례와 관련 법률 및 규정에 대해 처리 중인 데이터 유형을 고려해야 할 수 있습니다. 예를 들어 카드 소지자 데이터는 Payment Card Industry Data Security Standard(PCI DSS)에 따라 보호되며, 보호 대상 건강 정보는 미국 건강 보험 양도 및 책임에 관한 법(HIPAA)의 적용을 받을 수 있습니다. 개인 데이터가 포함된 환경을 검토하고 이를 기반으로 세분화 전략을 계획하려고 할

수도 있습니다. 일반적인 계정 세분화 전략에는 개발, 스테이징 또는 품질 보증(QA) 및 프로덕션을 위한 전용 계정과 같이 소프트웨어 개발 수명 주기(SDLC)에 맞는 전용 AWS 계정 이 포함될 수 있습니다. 이와 같은 세분화 전략은 전반적인 설계 논의에서 중요한 구성 요소일 수 있으며 OU가 특정 규제 요구 사항에 부합해야 할 수 있습니다.

일부 다중 계정 AWS 환경에는 당 전용 애플리케이션 계정이 AWS 리전필요하거나 다중 계정 랜딩 존이 필요할 수 있습니다. 이 경우 고객과 규제 기관의 고유한 데이터 주권 요구 사항을 충족하기 위해 추가 세분화가 필요합니다. 자세한 내용은 이 안내서의 글로벌 확장을 위한 전략 수립 섹션을 참조하세요.

AWS 개인 정보 보호 서비스 운영

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

많은 경우 개인 정보 보호는 교차 절단입니다. 규제 팀, 규정 준수 팀, 엔지니어링 팀 등 많은 여러 팀이 맡아야 할 역할이 있습니다. 조직에서 개인 정보 보호 프로그램의 주요 인물 및 정책 구성 요소를 정의하기 시작하면 일관된 운영을 위해 개인 정보 보호 규정 준수 프레임워크에 대한 제어를 매핑할 수 있습니다. 프레임워크는 AWS 환경의 개인 데이터에 대한 기본 및 애플리케이션별 프라이버시 제어를 구현하기 위한 규정 역할을 할 수 있습니다.

고객이 개인 정보 보호 요구 사항을 분류하는 데 사용하는 프레임워크에 관계없이 개인 정보 보호 규정 준수, 개인 정보 보호 엔지니어링 및 애플리케이션 팀은 종종 구현 목표를 달성하기 위해 협력하곤 합니다. 예를 들어 규제 및 규정 준수 팀은 높은 수준의 요구 사항을 제공할 수 있으며, 엔지니어링 및 애플리케이션 팀은 이러한 요구 사항에 맞게 AWS 서비스 및 기능을 구성합니다. 제어 프레임워크를 시작하면 보다 규범적인 조직 및 기술 제어를 정의하는 데 도움이 될 수 있습니다.

AWS 서비스 및 기능의 기술적 제어를 정의할 때 또 다른 주요 결정은 제어가 전체 조직, OU, 계정 또는 특정 리소스에 적용되어야 하는지 여부입니다. 일부 서비스 및 기능은 전체 AWS 조직에서 제어를 구현하는 데 매우 적합합니다. 예를 들어 Amazon S3 버킷에 대한 퍼블릭 액세스를 차단하는 것은 각 계정에 대해 개별적으로 구성하지 않고 조직 루트에서 구성하는 것이 좋습니다. 그러나 보존 정책은 애플리케이션에 따라 다를 수 있습니다. 즉, 리소스 수준에서 제어를 적용할 수 있습니다.

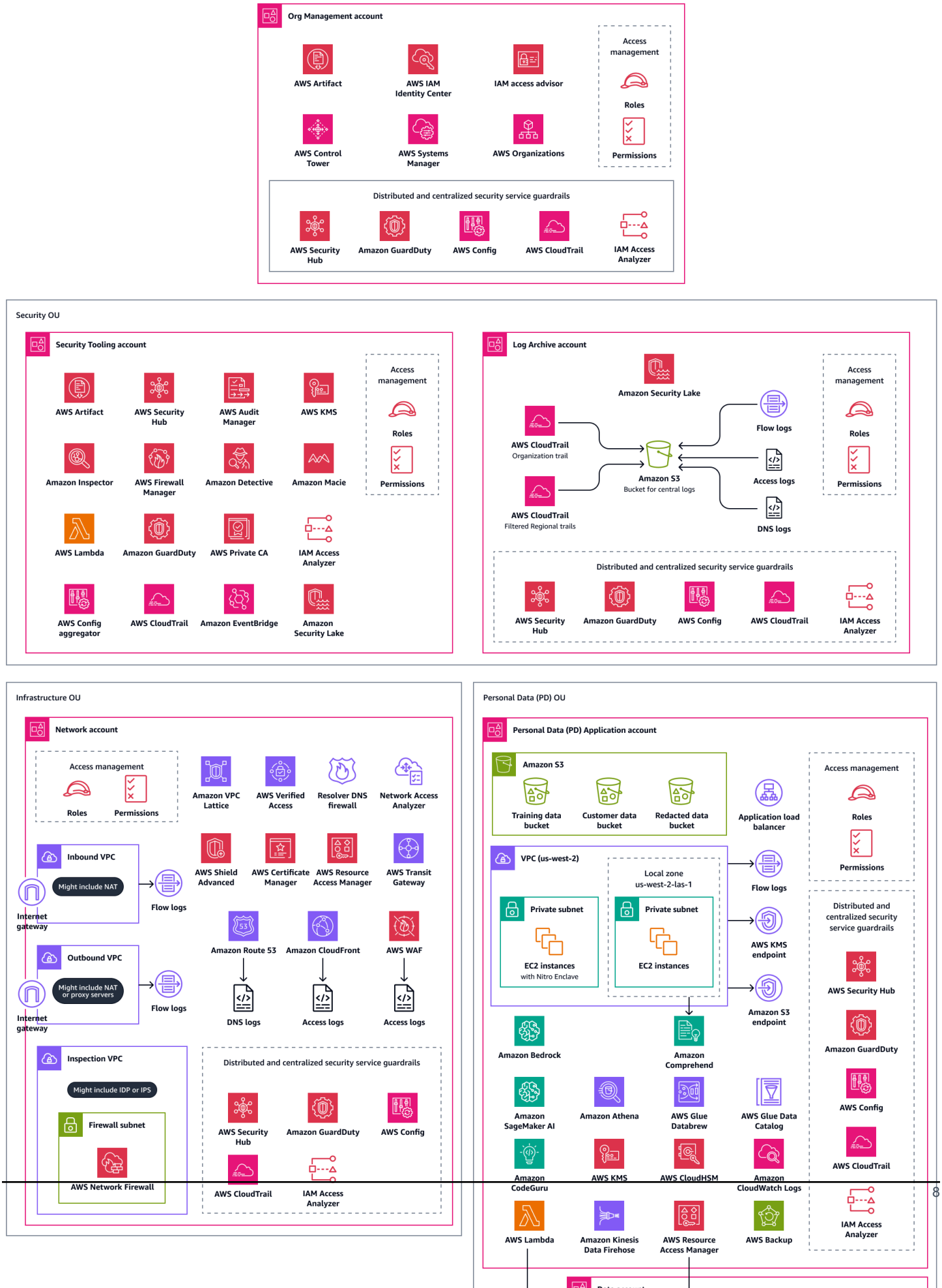
는 조직의 개인 정보 보호를 신속하게 운영할 수 있도록 AWS 워크로드에 대한 감사 및 규정 준수 자문 서비스를 AWS 제공합니다. 자세한 내용은 AWS SAS에 문의하십시오.

AWS 프라이버시 참조 아키텍처

설문 조사

여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

다음 다이어그램은 AWS 프라이버시 참조 아키텍처(AWS PRA)를 보여줍니다. 다음은 많은 개인 정보 보호 관련 AWS 서비스 및 기능을 연결하는 아키텍처의 예입니다. 이 아키텍처는 AWS Control Tower에서 규제하는 랜딩 존을 기반으로 합니다.


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 PRA에는 개인 데이터(PD) 애플리케이션 계정에서 호스팅되는 서버리스 웹 아키텍처가 포함되어 있습니다. 이 계정의 아키텍처는 소비자로부터 직접 개인 데이터를 수집하는 워크로드에 대한 예제입니다. 이 워크로드에서 사용자는 웹 티어를 통해 연결됩니다. 웹 티어는 애플리케이션 티어와 상호 작용합니다. 이 계층은 웹 계층으로부터 입력을 수신하고, 데이터를 처리 및 저장하며, 승인된 내부 팀과 서드 파티가 데이터에 액세스할 수 있도록 허용하고, 결국 더 이상 필요하지 않을 때 데이터를 아카이브하고 삭제합니다. 이 아키텍처는 데이터 레이크, 컨테이너, 컴퓨팅 또는 사물 인터넷(IoT)과 같은 특정 사용 사례를 살펴보지 않고 많은 기본 프라이버시 엔지니어링 기술을 보여주기 위해 의도적으로 모듈화된 이벤트 중심 아키텍처입니다.

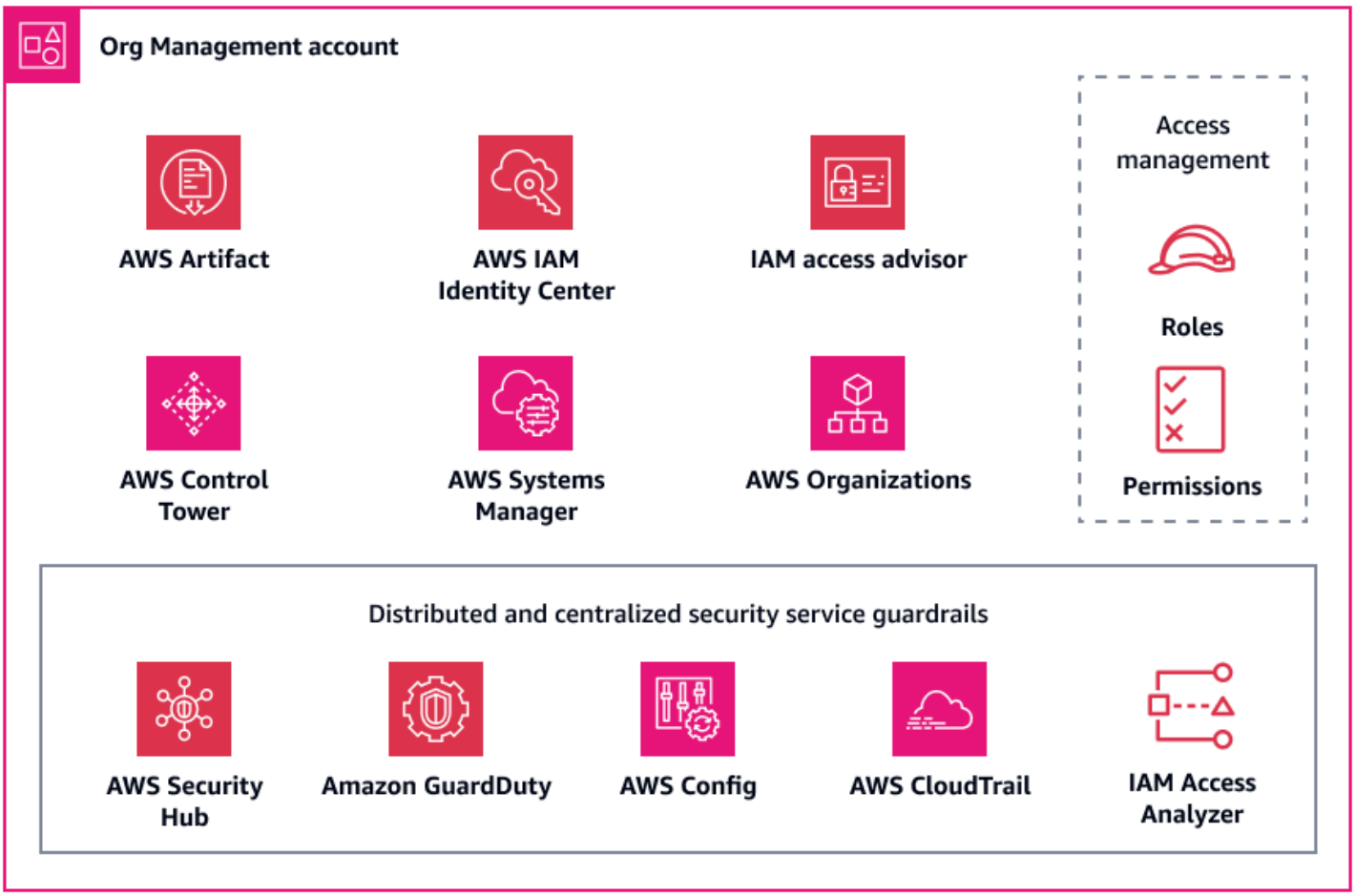
다음으로 이 가이드에서는 조직의 각 계정을 자세히 설명합니다. 다음 각 계정의 개인 정보 보호와 관련된 서비스 및 기능, 고려 사항 및 권장 사항, 다이어그램에 대해 설명합니다.

- 조직 관리 계정
- 보안 OU - 보안 도구 계정
- 보안 OU - 로그 아카이브 계정
- 인프라 OU - Network 계정
- 개인 데이터 OU - PD 애플리케이션 계정

조직 관리 계정

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

조직 관리 계정은 기본적으로 AWS Organizations에서 관리하는 조직의 모든 계정에서 기본 개인 정보 보호 제어를 위한 리소스 구성 드리프트를 관리하는 데 사용됩니다. 또한 이 계정에서는 동일한 보안 및 개인 정보 보호 제어를 통해 새 멤버 계정을 일관된 방식으로 배포할 수 있습니다. 이 계정에 대한 자세한 내용은 AWS 보안 참조 아키텍처(AWS SRA)를 참조하세요. 다음 다이어그램은 조직 관리 계정에 구성된 AWS 보안 및 개인 정보 보호 서비스를 보여줍니다.



이 섹션에서는 이 계정에서 사용되는 다음 AWS 서비스 에 대한 자세한 정보를 제공합니다.

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact는 AWS 보안 및 규정 준수 문서의 온디맨드 다운로드를 제공하여 감사를 지원할 수 있습니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

이를 AWS 서비스 통해 상속 AWS 받은 제어를 이해하고 환경에서 구현할 수 있는 컨트롤을 결정할 수 있습니다.는 SOC(System and Organization Controls) 보고서 및 PCI(Payment Card Industry) 보고서와 같은 AWS 보안 및 규정 준수 보고서에 대한 액세스를 AWS Artifact 제공합니다. 또한 AWS 제어의 구현 및 운영 효율성을 검증하는 여러 지역 및 규정 준수 수직 부문의 인증 기관의 인증에 대한 액세

스를 제공합니다. 를 사용하면 감사자 또는 규제 기관에 AWS 보안 및 개인 정보 보호 제어의 증거로 AWS 감사 아티팩트를 제공할 AWS Artifact 수 있습니다. 다음 보고서는 AWS 개인 정보 보호 제어의 효과를 입증하는 데 유용할 수 있습니다.

- SOC 2 유형 2 개인 정보 보호 보고서 -이 보고서는 개인 데이터가 수집, 사용, 보존, 공개 및 폐기되는 방식에 대한 AWS 제어의 효과를 보여줍니다. SOC 3 개인 정보 보호 보고서도 있는데, 이는 SOC 2 개인 정보 보호 제어에 대해 덜 상세한 설명을 제공합니다. 자세한 내용은 SOC FAQ를 참조하세요.
- 클라우드 컴퓨팅 규정 준수 제어 카탈로그(C5) - 이 보고서는 독일의 국가 사이버 보안 기관인 Informationstechnik(BSI)의 Bundesamt für Sicherheit에서 작성했습니다. C5 요구 사항을 충족하기 위해 AWS 가 구현한 보안 제어를 자세히 설명합니다. 또한 데이터 위치, 서비스 프로비저닝, 관할 구역 및 정보 공개 의무와 관련된 개인 정보 보호에 대한 추가 제어 요구 사항도 포함됩니다.
- ISO/IEC 27701:2019 인증 보고서 – ISO/IEC 27701:2019에서는 개인 정보 보호 관리 시스템(PIMS)을 설정하고 지속적으로 개선하기 위한 요구 사항과 지침을 설명합니다. 이 보고서는이 인증의 범위를 자세히 설명하고 AWS 인증 증명 역할을 할 수 있습니다. 이 표준에 대한 자세한 내용은 ISO/IEC 27701:2019(ISO 웹 사이트)를 참조하세요.

AWS Control Tower

AWS Control Tower는 규범적 보안 권장 사례를 따르는 AWS 다중 계정 환경을 설정하고 관리하는 데 도움이 됩니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

에서는 데이터 프라이버시 요구 사항, 특히 데이터 레지던시 및 주권에 맞는 가드레일이라고도 하는 많은 선제적, 예방적 및 탐지 제어의 배포를 자동화 AWS Control Tower할 수도 있습니다. 예를 들어 데이터 전송을 승인된 AWS 리전으로만 제한하는 가드레일을 지정할 수 있습니다. 보다 세분화된 제어를 위해 Amazon Virtual Private Network(VPN) 연결 허용 안 함, Amazon VPC 인스턴스에 대한 인터넷 액세스 허용 안 함, 요청된에 따라에 대한 액세스 거부 등 데이터 레지던시를 제어하도록 설계된 17개 이상의 가드레일 중에서 선택할 수 있습니다. AWS AWS 리전 이러한 가드레일은 조직 전체에 균일하게 배포할 수 있는 여러 AWS CloudFormation 후크, 서비스 제어 정책 및 AWS Config 규칙으로 구성됩니다. 자세한 내용은 AWS Control Tower 설명서의 데이터 레지던시 보호를 강화하는 제어를 참조하세요.

데이터 주권의 경우 AWS Control Tower 현재는 연결된 Amazon EBS 볼륨이 유휴 데이터를 암호화하도록 구성되어 있어야 함, AWS KMS 권한 부여 생성을 제한하는 문이 있어야 AWS KMS 함 AWS 서비스과 같은 예방 제어를 제공합니다. 주권 제어는 단순한 데이터 레지던시 제어보다 광범위합니다. 이를 통해 데이터 레지던시, 세분화된 액세스 제한, 암호화 및 복원력 요구 사항을 위반할 수 있는 작업을

방지할 수 있습니다. 자세한 내용은 AWS Control Tower 설명서의 Preventive controls that assist with digital sovereignty를 참조하세요.

데이터 레지던시 및 주권 제어를 넘어 프라이버시 가드레일을 배포해야 하는 경우 에는 여러 가지 필수 제어가 AWS Control Tower 포함됩니다. 이러한 제어는 랜딩 존을 설정할 때 기본적으로 모든 OU에 배포됩니다. 이러한 대부분은 로그 아카이브 삭제 허용 안 함 및 CloudTrail 로그 파일에 대한 무결성 검증 활성화와 같이 로그를 보호하도록 설계된 예방적 제어입니다.

AWS Control Tower 또한는와 통합되어 탐지 제어를 AWS Security Hub CSPM 제공합니다. 이러한 제어를 서비스 관리형 표준 AWS Control Tower이라고 합니다. 이러한 제어를 사용하여 Amazon Relational Database Service(Amazon RDS) 데이터베이스 인스턴스에 대한 저장 데이터 암호화와 같은 개인 정보 보호 지원 제어의 구성 드리프트를 모니터링할 수 있습니다.

AWS Organizations

AWS PRA는 AWS Organizations 를 사용하여 아키텍처 내의 모든 계정을 중앙에서 관리합니다. 자세한 내용은 이 안내서의 AWS Organizations 및 전용 계정 구조 섹션을 참조하세요. 에서는 서비스 제어 정책(SCPs) 및 관리 정책을 사용하여 개인 데이터와 개인 정보를 보호할 AWS Organizations수 있습니다.

서비스 제어 정책(SCP)

서비스 제어 정책(SCP)은 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. 이를 통해 대상 계정, 조직 단위 AWS Identity and Access Management (OU) 또는 전체 조직의 (IAM) 역할 및 사용자에 대해 사용 가능한 최대 권한을 중앙 집중식으로 제어할 수 있습니다. 조직 관리 계정에서 SCP를 생성하고 적용할 수 있습니다.

AWS Control Tower 를 사용하여 계정 전체에 SCPs 균일하게 배포할 수 있습니다. 적용할 수 있는 데이터 레지던시 제어에 대한 자세한 내용은이 가이드AWS Control Tower의 섹션을 AWS Control Tower 참조하세요. 예방 SCPs의 전체 보완을 AWS Control Tower 포함합니다. AWS Control Tower 가 현재 조직에서 사용되지 않는 경우 이러한 제어를 수동으로 배포할 수도 있습니다.

SCP를 사용하여 데이터 레지던시 요구 사항 해결

특정 지리적 리전 내에 데이터를 저장하고 처리하여 개인 데이터 레지던시 요구 사항을 관리하는 것이 일반적입니다. 관할 구역의 고유한 데이터 레지던시 요구 사항이 충족되는지 확인하려면 규제 팀과 긴밀히 협력하여 요구 사항을 확인하는 것이 좋습니다. 이러한 요구 사항이 결정되면 지원에 도움이 될 수 있는 여러 AWS 가지 기본 개인 정보 보호 제어가 있습니다. 예를 들어 SCPs 사용하여 데이터를 처리하고 저장하는 데 사용할 수 있는를 제한할 AWS 리전 수 있습니다. 정책 샘플은 이 가이드의 간 데이터 전송 제한 AWS 리전 섹션을 참조하세요.

SCP를 사용하여 고위험 API 직접 호출 제한

어떤 보안 및 개인 정보 보호 제어 AWS 에 책임이 있고 어떤 보안 및 개인 정보 보호 제어에 책임이 있는지 이해하는 것이 중요합니다. 예를 들어 사용하는 AWS 서비스 에 대해 발생할 수 있는 API 직접 호출 결과에 대한 책임은 사용자에게 있습니다. 또한 보안 또는 개인 정보 보호 태세를 변경할 수 있는 직접 호출을 파악하는 것도 사용자의 책임입니다. 특정 보안 및 개인 정보 보호 태세의 유지 관리와 관련해 우려 사항이 있는 경우 특정 API 직접 호출을 거부하는 SCP를 활성화할 수 있습니다. 이러한 API 직접 호출은 의도하지 않은 개인 데이터 공개 또는 특정 국가 간 데이터 전송 위반과 같은 영향을 미칠 수 있습니다. 예를 들어 다음 API 직접 호출을 금지할 수 있습니다.

- Amazon Simple Storage Service(Amazon S3) 버킷에 대한 퍼블릭 액세스 활성화
- Amazon GuardDuty 비활성화 또는 Trojan:EC2/DNSDataExfiltration 조사 결과와 같은 데이터 유출 조사 결과에 대한 억제 규칙 생성
- AWS WAF 데이터 유출 규칙 삭제
- Amazon Elastic Block Store(Amazon EBS) 스냅샷 퍼블릭 공유
- 조직에서 멤버 계정 제거
- 리포지토리에서 Amazon CodeGuru Reviewer 연결 해제

관리 정책

의 관리 정책은 AWS 서비스 및 해당 기능을 중앙에서 구성하고 관리하는 데 도움이 될 AWS Organizations 수 있습니다. 선택한 관리 정책 유형에 따라 정책이 정책을 상속하는 OU 및 계정에 미치는 영향이 달라집니다. 태그 정책은 개인 정보 보호와 AWS Organizations 직접 관련된의 관리 정책의 예입니다.

태그 정책 사용

태그는 AWS 리소스를 관리, 식별, 구성, 검색 및 필터링하는 데 도움이 되는 키 값 페어입니다. 개인 데이터를 처리하는 조직의 리소스를 구별하는 태그를 적용하는 방법이 유용할 수 있습니다. 태그 사용은 이 가이드의 많은 개인 정보 보호 솔루션을 지원합니다. 예를 들어 리소스 내에서 처리되거나 저장되는 데이터의 일반적인 데이터 분류를 나타내는 태그를 적용할 수 있습니다. 특정 태그 또는 태그 세트가 있는 리소스에 대한 액세스를 제한하는 속성 기반 액세스 제어(ABAC) 정책을 작성할 수 있습니다. 예를 들어 정책에서 `SysAdmin` 역할이 `dataclassification:4` 태그가 있는 리소스에 액세스할 수 없도록 지정할 수 있습니다. 자세한 내용과 자습서는 IAM 설명서의 태그를 기반으로 AWS 리소스에 액세스할 수 있는 권한 정의를 참조하세요. 또한 조직에서 AWS Backup을 사용하여 여러 계정의 백업에 데이터 보존 정책을 광범위하게 적용하는 경우 해당 리소스를 해당 백업 정책의 범위 내에 배치하는 태그를 적용할 수 있습니다.

태그 정책은 조직 전체에서 일관된 태그를 유지하는 데 도움이 됩니다. 태그 정책에서 리소스에 태그를 지정할 때 리소스에 적용할 규칙을 지정합니다. 예를 들어 리소스에 `DataClassification` 또는 `DataSteward`와 같은 특정 키로 태그를 지정하도록 요구할 수 있으며 키에 유효한 대소문자 처리 또는 값을 지정할 수 있습니다. 또한 적용을 사용하여 규정 미준수 태그 지정 요청이 완료되지 않도록 할 수 있습니다.

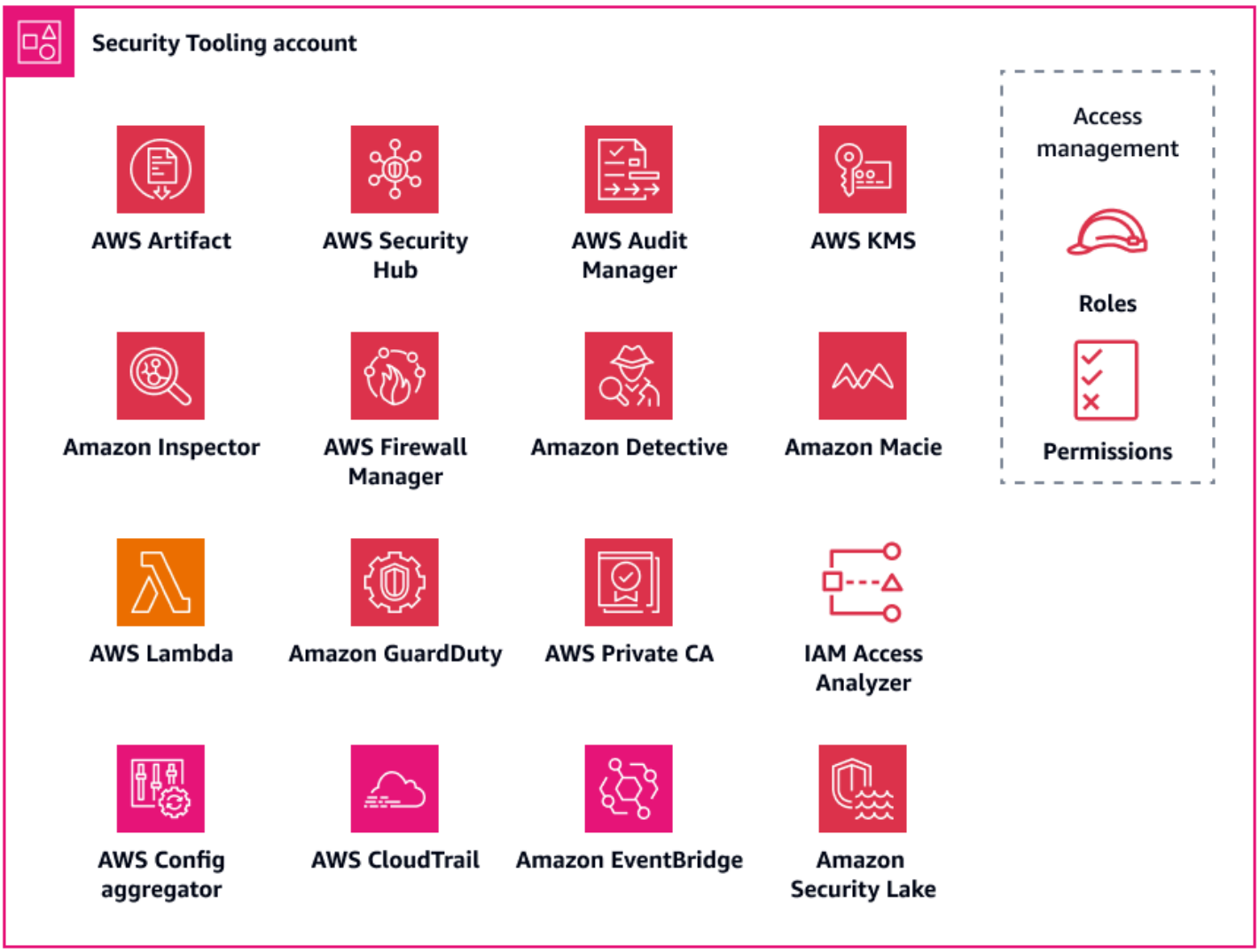
태그를 개인 정보 보호 제어 전략의 핵심 구성 요소로 사용하는 경우 다음 사항을 고려합니다.

- 태그 키 또는 값 내에 개인 데이터 또는 기타 유형의 민감한 데이터를 배치할 경우 관련 영향을 고려합니다. 기술 지원을 위해에 문의 AWS 하면 AWS 에서 태그 및 기타 리소스 식별자를 분석하여 문제를 해결할 수 있습니다. 태그 데이터는 암호화되지 않으며 AWS 서비스와 같이가 데이터를 읽을 AWS 결제 및 비용 관리수 있습니다. 따라서 태그에 개인 식별 정보를 포함하지 않는 IT 서비스 관리(ITSM) system. AWS recommds와 같이 제어하는 시스템을 사용하여 태그 값을 비식별화한 다음 다시 식별할 수 있습니다.
- 태그에 의존하는 ABAC 조건과 같은 기술 제어의 우회를 방지하려면 일부 태그 값을 변경할 수 없는 항목(수정 불가)으로 설정해야 합니다.

보안 OU - 보안 도구 계정

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

Security Tooling 계정은 보안 및 개인 정보 보호 기본 서비스 운영, 보안 AWS 계정및 개인 정보 보호 알림 및 응답 모니터링 및 자동화를 전담합니다. 이 계정에 대한 자세한 내용은 AWS 보안 참조 아키텍처(AWS SRA)를 참조하세요. 다음 다이어그램은 AWS Security Tooling 계정에 구성된 보안 및 개인 정보 보호 서비스를 보여줍니다.



이 섹션에서는 이 계정의 다음 사항에 대한 자세한 정보를 제공합니다.

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

AWS CloudTrail

AWS CloudTrail는의 전체 API 활동을 감사하는 데 도움이 됩니다 AWS 계정. 개인 데이터를 저장, 처리 또는 전송하는 모든 AWS 계정 및에서 CloudTrail을 활성화하면이 데이터의 사용 및 공개를 추적

AWS 리전 하는 데 도움이 될 수 있습니다. AWS Security Reference Architecture는 조직의 모든 계정에 대한 모든 이벤트를 로깅하는 단일 추적에 해당하는 조직 추적을 활성화할 것을 권장합니다. 그러나 이 조직 추적을 활성화하면 다중 리전 로그 데이터가 로그 아카이브 계정의 단일 Amazon Simple Storage Service(Amazon S3) 버킷으로 집계됩니다. 개인 데이터를 처리하는 계정의 경우 이로 인해 몇 가지 추가 설계 고려 사항이 발생할 수 있습니다. 로그 레코드에는 개인 데이터에 대한 일부 참조가 포함될 수 있습니다. 데이터 레지던시 및 데이터 전송 요구 사항을 충족하려면 교차 리전 로그 데이터를 S3 버킷이 위치한 단일 리전으로 집계하는 방식을 다시 고려해야 할 수 있습니다. 조직은 조직 추적에 포함하거나 제외해야 하는 리전별 워크로드를 고려할 수 있습니다. 조직 추적에서 제외하기로 결정한 워크로드의 경우 개인 데이터를 마스킹하는 리전별 추적을 구성하는 방법을 고려할 수 있습니다. 개인 데이터 마스킹에 대한 자세한 내용은 이 가이드의 Amazon Data Firehose 섹션을 참조하세요. 궁극적으로 조직은 중앙 집중식 로그 아카이브 계정으로 집계되는 조직 추적과 리전 추적을 조합할 수 있습니다.

단일 리전 추적 구성에 대한 자세한 내용은 AWS Command Line Interface (AWS CLI) 또는 콘솔 사용 지침을 참조하세요. 조직 추적을 생성하는 경우 AWS Control Tower에서 옵트인 설정을 사용하거나 CloudTrail 콘솔에서 직접 추적을 생성할 수 있습니다.

전반적인 접근 방식과 로그 및 데이터 전송 요구 사항의 중앙 집중화를 관리하는 방법에 대한 자세한 내용은 이 가이드의 중앙 집중식 로그 스토리지 섹션을 참조하세요. 어떤 구성을 선택하든 AWS SRA에 따라 보안 도구 계정의 추적 관리를 로그 아카이브 계정의 로그 스토리지와 분리할 수 있습니다. 이 설계는 로그를 관리해야 하는 사용자와 로그 데이터를 사용해야 하는 사용자를 위한 최소 권한 액세스 정책을 생성하는 데 도움이 됩니다.

AWS Config

AWS Config에서는 AWS 계정 에 있는 리소스와 해당 구성 방식을 자세히 보여줍니다. 이 정보는 리소스가 서로 관련되는 방식과 리소스의 구성이 시간이 지남에 따라 변경된 방식을 식별하는 데 도움이 됩니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

에서는 AWS Config 규칙 및 문제 해결 작업 세트인 적합성 팩 AWS Config을 배포할 수 있습니다. 적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙을 사용하여 개인 정보 보호, 보안, 운영 및 비용 최적화 거버넌스 검사를 지원하도록 설계된 범용 프레임워크를 제공합니다. 이 도구를 더 큰 자동화 도구 세트의 일부로 사용하여 AWS 리소스 구성이 자체 제어 프레임워크 요구 사항을 준수하는지 여부를 추적할 수 있습니다.

Operational Best Practices for NIST Privacy Framework v1.0 적합성 팩은 NIST Privacy Framework의 여러 개인 정보 보호 관련 제어에 부합됩니다. 각 AWS Config 규칙은 특정 AWS 리소스 유형에 적용되며 하나 이상의 NIST 프라이버시 프레임워크 제어와 관련이 있습니다. 이 적합성 팩을 사용하여 계정

의 리소스 전반에서 개인 정보 보호와 관련된 지속적 규정 준수를 추적할 수 있습니다. 다음은 이 적합성 팩에 포함된 몇 가지 규칙입니다.

- `no-unrestricted-route-to-igw` - 이 규칙은 VPC 라우팅 테이블에서 인터넷 게이트웨이로의 기본 `0.0.0.0/0` 또는 `::/0` 송신 경로를 지속적으로 모니터링하여 데이터 플레인의 데이터 유출을 방지하는 데 도움이 됩니다. 이를 통해 특히 악의적인 것으로 알려진 CIDR 범위가 있는 경우 인터넷 바운드 트래픽을 전송할 수 있는 위치를 제한할 수 있습니다.
- `encrypted-volumes` - 이 규칙은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨이 암호화되었는지 확인합니다. 조직에 개인 데이터 보호를 위한 AWS Key Management Service (AWS KMS) 키 사용과 관련된 특정 제어 요구 사항이 있는 경우 규칙의 일부로 특정 키 IDs를 지정하여 볼륨이 특정 AWS KMS 키로 암호화되었는지 확인할 수 있습니다.
- `restricted-common-ports` - 이 규칙은 Amazon EC2 보안 그룹이 지정된 포트에 대한 무제한 TCP 트래픽을 허용하는지 확인합니다. 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. `0.0.0.0/0`에서 TCP 3389 및 TCP 21과 같은 공통 포트로의 수신 트래픽을 차단하면 원격 액세스를 제한하는 데 도움이 됩니다.

AWS Config 는 리소스의 사전 및 사후 규정 준수 검사에 모두 사용할 수 있습니다 AWS . 적합성 팩에 있는 규칙을 고려하는 것 외에도 이러한 규칙을 감지 및 선제적 평가 모드 모두에 통합할 수 있습니다. 이렇게 하면 애플리케이션 개발자가 배포 전 검사를 통합하기 시작할 수 있으므로 소프트웨어 개발 수명 주기 초기에 개인 정보 보호 검사를 구현하는 데 도움이 됩니다. 예를 들어 사전 예방적 모드가 활성화된 모든 개인 정보 보호 관련 AWS Config 규칙에 대해 AWS CloudFormation 템플릿에서 선언된 리소스를 확인하는 후크를 템플릿에 포함할 수 있습니다. 자세한 내용은 AWS Config Rules Now Support Proactive Compliance(AWS 블로그 게시물)를 참조하세요.

Amazon GuardDuty

AWS 는 Amazon S3, Amazon Relational Database Service(RDS) 또는 Amazon EC2 with Kubernetes와 같이 개인 데이터를 저장하거나 처리하는 데 사용할 수 있는 여러 서비스를 제공합니다. Amazon GuardDuty는 지능형 가시성과 지속적인 모니터링을 결합하여 의도하지 않은 개인 데이터 공개와 관련되었을 수 있는 지표를 감지합니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

GuardDuty를 사용하면 공격 수명 주기 전반에 걸쳐 잠재적으로 악의적인 개인 정보 보호 관련 활동을 식별할 수 있습니다. 예를 들어 GuardDuty는 블랙리스트에 등록된 사이트에 대한 연결, 비정상적인 네트워크 포트 트래픽 또는 트래픽 볼륨, DNS 유출, 예상치 못한 EC2 인스턴스 시작 및 비정상적인 ISP

직접 호출자를 알릴 수 있습니다. 신뢰할 수 있는 IP 목록에서 신뢰할 수 있는 IP에 대한 알림과 자체 위협 목록의 알려진 악성 IP의 알림을 중지하도록 GuardDuty를 구성할 수 있습니다.

AWS SRA에서 권장하는 대로 조직의 모든 AWS 계정 에 대해 GuardDuty를 활성화하고 보안 도구 계정을 GuardDuty 위임된 관리자로 구성할 수 있습니다. GuardDuty는 조직 전체의 조사 결과를 이 단일 계정으로 집계합니다. 자세한 내용은 로 GuardDuty 계정 관리를 참조하세요 AWS Organizations. 또한 감지 및 분석부터 격리 및 근절까지 인시던트 대응 프로세스에서 모든 개인 정보 보호 관련 이해관계자를 식별하고 데이터 유출과 관련되었을 수 있는 모든 인시던트에 참여시키는 방법을 고려할 수 있습니다.

IAM Access Analyzer

많은 고객이 개인 데이터가 사전 승인되고 의도된 서드 파티 프로세서와 적절하게 공유되고 있으며 다른 엔터티와는 공유되지 않는다는 지속적인 보장을 원합니다. 데이터 경계는 AWS 환경의 신뢰할 수 있는 리소스에 예상되는 네트워크의 신뢰할 수 있는 ID만 액세스할 수 있도록 설계된 예방적 가드레일입니다. 개인 데이터의 의도하지 않은 공개 및 의도된 공개에 대한 제어를 정의할 때 신뢰할 수 있는 ID, 신뢰할 수 있는 리소스 및 예상되는 네트워크를 정의할 수 있습니다.

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)를 사용하면 조직은 신뢰 AWS 계정 영역을 정의하고 해당 신뢰 영역에 대한 위반에 대한 알림을 구성할 수 있습니다. IAM Access Analyzer는 IAM 정책을 분석하여 잠재적으로 민감한 리소스에 대한 의도하지 않은 퍼블릭 또는 교차 계정 액세스를 식별하고 해결하는 데 도움이 됩니다. IAM Access Analyzer는 수학 로직과 추론을 사용하여 AWS 계정외부에서 액세스할 수 있는 리소스에 대한 포괄적인 조사 결과를 생성합니다. 마지막으로 지나치게 허용적인 IAM 정책에 대응하고 관련 문제를 해결하려면 IAM Access Analyzer를 사용하여 IAM 권장 사례를 기준으로 기존 정책을 검증하고 제안을 제공할 수 있습니다. IAM Access Analyzer는 IAM 위탁자의 이전 액세스 활동을 기반으로 최소 권한 IAM 정책을 생성할 수 있습니다. CloudTrail 로그를 분석하고 해당 작업을 계속 수행하는 데 필요한 권한만 부여하는 정책을 생성합니다.

보안 컨텍스트에서 IAM Access Analyzer를 사용하는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

Amazon Macie

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험에 대한 보호를 자동화할 수 있는 서비스입니다. Macie는 Amazon S3 버킷의 보안 또는 개인 정보 보호와 관련하여 잠재적 정책 위반 또는 문제를 감지하면 조사 결과를 생성합니다. Macie는 조직이 규정 준수 노력을 지원하기 위해 자동화를 구현하는 데 사용

할 수 있는 또 다른 도구입니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

Macie는 이름, 주소 및 신분을 식별할 수 있는 기타 속성과 같은 개인 식별 정보(PII)를 포함하여 점점 증가하는 대규모 민감한 데이터 유형 목록을 감지할 수 있습니다. 조직의 개인 데이터 정의를 반영하는 감지 기준을 정의하기 위해 사용자 지정 데이터 식별자를 생성할 수도 있습니다.

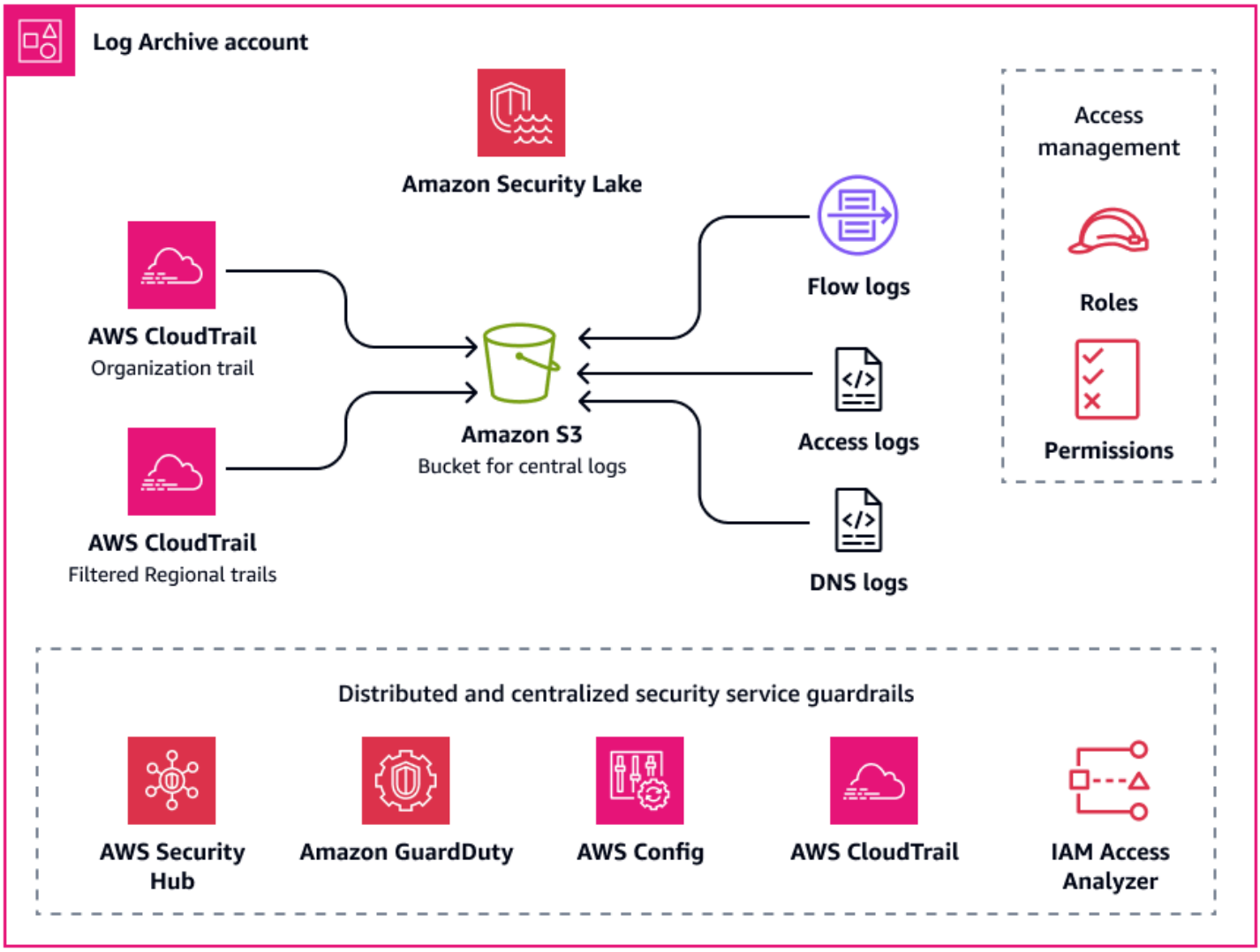
조직에서 개인 데이터가 포함된 Amazon S3 버킷에 대한 예방적 제어를 정의하면 Macie를 검증 메커니즘으로 사용하여 개인 데이터가 있는 위치를 지속적으로 재확인하고 개인 데이터를 보호하는 방법을 제공할 수 있습니다. 시작하려면 Macie를 활성화하고 자동화된 민감한 데이터 검색을 구성합니다. Macie는 계정 및 간에 모든 S3 버킷의 객체를 지속적으로 분석합니다 AWS 리전. Macie는 개인 데이터가 상주하는 위치를 나타내는 대화형 히트 맵을 생성하고 유지 관리합니다. 자동화된 민감한 데이터 검색 기능은 비용을 절감하고 검색 작업을 수동으로 구성할 필요성을 최소화하도록 설계되었습니다. 자동화된 민감한 데이터 검색 기능을 기반으로 빌드하고 Macie를 사용하여 새 버킷 또는 기존 버킷의 새 데이터를 자동으로 감지한 다음 할당된 데이터 분류 태그와 비교하여 데이터를 검증할 수 있습니다. 적절한 개발 및 개인 정보 보호 팀에 잘못 분류되거나 분류되지 않은 버킷을 적시에 알리도록 이 아키텍처를 구성합니다.

를 사용하여 조직의 모든 계정에 대해 Macie를 활성화할 수 있습니다 AWS Organizations. 자세한 내용은 Integrating and configuring an organization in Amazon Macie를 참조하세요.

보안 OU - 로그 아카이브 계정

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

로그 아카이브 계정은 인프라, 서비스 및 애플리케이션 로그 유형을 중앙 집중화하는 위치입니다. 이 계정에 대한 자세한 내용은 AWS 보안 참조 아키텍처(AWS SRA)를 참조하세요. 로그 전용 계정을 사용하면 모든 로그 유형에서 일관된 알림을 적용하고 인시던트 대응 담당자가 한 곳에서 이러한 로그의 집계에 액세스할 수 있는지 확인할 수 있습니다. 한 곳에서 보안 제어 및 데이터 보존 정책도 설정할 수 있으므로 개인 정보 보호 운영 오버헤드를 단순화할 수 있습니다. 다음 다이어그램에서는 로그 아카이브 계정에 구성된 AWS 보안 및 개인 정보 보호 서비스를 보여줍니다.



중앙 집중식 로그 스토리지

로그 파일(예: AWS CloudTrail 로그)에는 개인 데이터로 간주될 수 있는 정보가 포함될 수 있습니다. 일부 조직은 가시성을 위해 조직 추적을 사용하여 계정 간 AWS 리전 및 계정 간 CloudTrail 로그를 하나의 중앙 위치로 집계하기로 선택합니다. 자세한 내용은 이 안내서의 AWS CloudTrail 섹션을 참조하세요. CloudTrail 로그의 중앙 집중화를 구현할 때 로그는 일반적으로 단일 리전의 Amazon Simple Storage Service(Amazon S3) 버킷에 저장됩니다.

조직의 개인 데이터 정의, 고객에 대한 계약 의무 및 관련 리전 개인 정보 보호 규정에 따라 로그 집계와 관련하여 국가 간 데이터 전송을 고려해야 할 수도 있습니다. 다양한 로그 유형 내 개인 데이터가 이러한 제한 사항에 부합되는지 확인합니다. 예를 들어 CloudTrail 로그에는 조직의 직원 데이터가 포함될 수 있지만 고객의 개인 데이터는 포함되지 않을 수 있습니다. 조직에서 제한된 데이터 전송 요구 사항을 준수해야 하는 경우 다음 옵션을 통해 지원할 수 있습니다.

- 조직에서 여러 국가의 데이터 주체 AWS 클라우드 에게의 서비스를 제공하는 경우 가장 엄격한 데이터 레지던시 요구 사항이 있는 국가의 모든 로그를 집계하도록 선택할 수 있습니다. 예를 들어 독일에서 운영 중이고 요구 사항이 가장 엄격한 경우 독일에서 수집된 데이터가 독일 국경을 벗어나지 `eu-central-1` AWS 리전 않도록의 S3 버킷에 데이터를 집계할 수 있습니다. 이 옵션의 경우 모든 계정에서 대상 리전으로 로그를 집계하는 단일 조직 추적을 CloudTrail AWS 리전 에서 구성할 수 있습니다.
- 데이터를 복사하여 다른 리전으로 집계하기 AWS 리전 전에에 유지해야 하는 개인 데이터를 수정합니다. 예를 들어 로그를 다른 리전으로 전송하기 전에 애플리케이션의 호스트 리전에 있는 개인 데이터를 마스킹할 수 있습니다. 개인 데이터 마스킹에 대한 자세한 내용은 이 가이드의 Amazon Data Firehose 섹션을 참조하세요.
- 엄격한 데이터 주권 문제가 있는 경우 이러한 요구 사항을 AWS 리전 적용하는에서 별도의 다중 계정 랜딩 존을 유지할 수 있습니다. 이 경우 중앙 집중식 로깅을 위해 리전의 랜딩 존 구성을 단순화할 수 있습니다. 또한 추가 인프라 분리 이점을 제공하고 로그를 자체 리전에 로컬로 유지하는 데 도움이 됩니다. 법률 고문과 협력하여 범위 내에 있는 개인 데이터와 허용되는 리전 간 전송을 결정합니다. 자세한 내용은 이 안내서의 글로벌 확장을 위한 전략 수립 섹션을 참조하세요.

서비스 로그, 애플리케이션 로그 및 운영 체제(OS) 로그를 통해 Amazon CloudWatch를 사용하여 기본적으로 해당 계정 및 리전의 AWS 서비스 또는 리소스를 모니터링할 수 있습니다. 많은 사용자가 여러 계정 및 리전의 이러한 로그와 지표를 단일 계정으로 중앙 집중화하기로 선택합니다. 기본적으로 이러한 로그는 해당 계정 및 로그가 시작된 리전에 유지됩니다. 중앙 집중화를 위해 구독 필터와 Amazon S3 내보내기 태스크를 사용하여 데이터를 중앙 위치로 공유할 수 있습니다. 국가 간 데이터 전송 요구 사항이 있는 워크로드에서 로그를 집계할 때 적절한 필터와 내보내기 태스크를 포함하는 것이 중요할 수 있습니다. 워크로드의 액세스 로그에 개인 데이터가 포함된 경우 이러한 데이터가 특정 계정 및 리전으로 전송되거나 보존되는지 확인해야 할 수도 있습니다.

Amazon Security Lake

AWS SRA에서 권장하는 대로 로그 아카이브 계정을 Amazon Security Lake의 위임된 관리자 계정으로 사용할 수 있습니다. 이렇게 하면 Security Lake는 다른 SRA 권장 보안 로그와 동일한 계정의 전용 Amazon S3 버킷에서 지원되는 로그를 수집합니다.

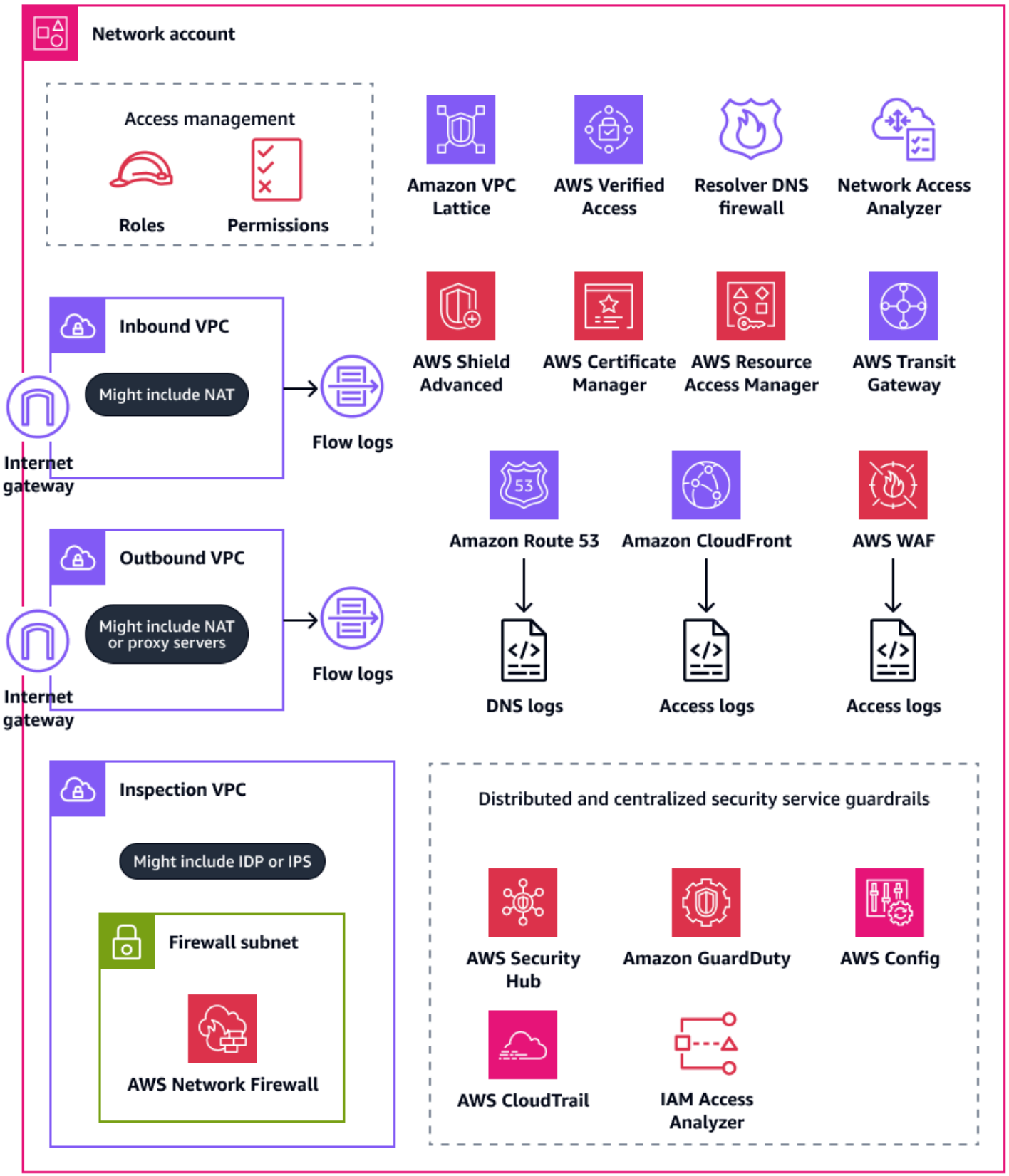
개인 정보 보호 관점에서 인시던트 대응 담당자는 AWS 환경, SaaS 공급자, 온프레미스, 클라우드 소스 및 타사 소스의 로그에 액세스할 수 있어야 합니다. 그러면 개인 데이터에 대한 무단 액세스를 더 빠르게 차단하고 해결할 수 있습니다. Amazon Security Lake 내 로그 레지던시 및 리전 이동에도 로그 스토리지에 대한 동일한 고려 사항이 적용될 가능성이 큽니다. 이는 Security Lake가 서비스를 활성화한 AWS 리전 에서 보안 로그 및 이벤트를 수집하기 때문입니다. 데이터 레지던시 요구 사항을 준수하려면 롤업 리전 구성을 고려합니다. 롤업 리전은 Security Lake가 선택한 하나 이상의 기여 리전의 데이터

를 통합하는 리전으로, 사용자가 선택합니다. Security Lake 및 롤업 리전을 구성하기 전에 조직에서 데이터 레지던시에 대한 리전 규정 준수 요구 사항을 조정해야 할 수도 있습니다.

인프라 OU - Network 계정

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

네트워크 계정에서는 가상 프라이빗 클라우드(VPC) 및 더 광범위한 인터넷 사이에서 네트워킹을 관리합니다. 이 계정에서는를 사용하고 AWS WAF, AWS Resource Access Manager (AWS RAM)를 사용하여 VPC 서브넷 및 AWS Transit Gateway 연결을 공유하고, Amazon CloudFront를 사용하여 대상 서비스 사용을 지원하여 광범위한 공개 제어 메커니즘을 구현할 수 있습니다. 이 계정에 대한 자세한 내용은 AWS 보안 참조 아키텍처(AWS SRA)를 참조하세요. 다음 다이어그램은 네트워크 계정에 구성된 AWS 보안 및 개인 정보 보호 서비스를 보여줍니다.



이 섹션에서는 이 계정에서 사용되는 다음 AWS 서비스 에 대한 자세한 정보를 제공합니다.

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

Amazon CloudFront

Amazon CloudFront는 프론트엔드 애플리케이션 및 파일 호스팅에 대한 지리적 제한을 지원합니다. CloudFront는 엣지 로케이션이라고 하는 데이터 센터의 전 세계 네트워크를 통해 콘텐츠를 전달할 수 있습니다. CloudFront를 통해 제공하는 콘텐츠를 사용자가 요청하면 지연 시간이 가장 낮은 엣지 로케이션으로 요청이 라우팅됩니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

개인 정보 보호 프로그램은 현재 특정 리전 법률 준수를 지원할 수 있습니다. 이러한 리전 내에만 상주하는 고객에게만 서비스를 제공하도록 워크로드 범위가 지정된 경우 다른 리전에서의 사용을 방지하는 기술적 조치를 구현할 수 있습니다. CloudFront 지리적 제한을 사용하여 특정 지리적 위치에 있는 사용자가 CloudFront 배포를 통해 배포한 콘텐츠에 액세스하는 것을 차단할 수 있습니다. 지리적 제한에 대한 구성 옵션과 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하세요.

CloudFront에서 수신하는 모든 사용자 요청에 대한 세부 정보가 포함된 액세스 로그를 생성하도록 CloudFront를 구성할 수도 있습니다. 자세한 내용은 CloudFront 설명서의 표준 로그(액세스 로그) 구성 및 사용을 참조하세요. 마지막으로 CloudFront가 일련의 엣지 로케이션에서 콘텐츠를 캐싱하도록 구성된 경우 캐싱이 발생하는 위치를 고려할 수 있습니다. 일부 조직의 경우 교차 리전 캐싱에 국가 간 데이터 전송 요구 사항이 적용될 수 있습니다.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM)를 사용하면에서 리소스를 안전하게 공유 AWS 계정 하여 운영 오버헤드를 줄이고 가시성 및 감사 가능성을 제공할 수 있습니다. AWS RAM를 사용하면 조직은 조직 AWS 계정 내 다른 나 타사 계정과 공유할 수 있는 AWS 리소스를 제한할 수 있습니다. 자세한 내용은 공유 가능한 AWS 리소스를 참조하세요. 네트워크 계정에서 AWS RAM 를 사용하여 VPC 서브넷과 전송 게이트웨이 연결을 공유할 수 있습니다. AWS RAM 를 사용하여 다른와 데이터 영역 연결을 공유하는 경우 AWS 계정사전 승인 AWS 리전 되고 데이터 레지던시 요구 사항을 준수하는 연결인지 확인하는 프로세스를 설정하는 것이 좋습니다.

VPCs 및 전송 게이트웨이 연결을 공유하는 것 외에도를 사용하여 IAM 리소스 기반 정책을 지원하지 않는 리소스를 공유할 수 AWS RAM 있습니다. 개인 데이터 OU에서 호스팅되는 워크로드의 경우

AWS RAM 를 사용하여 별도의에 있는 개인 데이터에 액세스할 수 있습니다 AWS 계정. 자세한 내용은 개인 데이터 OU – PD 애플리케이션 계정 섹션의 AWS Resource Access Manager를 참조하세요.

AWS Transit Gateway

조직 데이터 레지던시 요구 사항에 AWS 리전 따라에서 개인 데이터를 수집, 저장 또는 처리하는 AWS 리소스를 배포하려는 경우 적절한 기술적 보호 조치가 있는 경우 가드레일을 구현하여 제어 및 데이터 영역에서 승인되지 않은 국가 간 데이터 흐름을 방지하는 것이 좋습니다. 컨트롤 플레인에서 IAM 및 서비스 제어 정책을 사용하여 리전 사용량을 제한하고 결과적으로 교차 리전 데이터 흐름을 제한할 수 있습니다.

데이터 플레인에서 교차 리전 데이터 흐름을 제어하는 여러 옵션이 있습니다. 예를 들어 라우팅 테이블, VPC 피어링 및 AWS Transit Gateway 연결을 사용할 수 있습니다. AWS Transit Gateway는 가상 프라이빗 클라우드(VPC)와 온프레미스 네트워크를 연결하는 중앙 허브입니다. 더 큰 AWS 랜딩 존의 일부로 인터넷 게이트웨이, 직접 VPC-to-VPC 피어링, 리전 간 피어링을 AWS 리전통해 데이터를 탐색할 수 있는 다양한 방법을 고려할 수 있습니다 AWS Transit Gateway. 예를 들어 AWS Transit Gateway에서 다음을 수행할 수 있습니다.

- VPC와 온프레미스 환경 간 동서 및 남북 연결이 개인 정보 보호 요구 사항에 부합하는지 확인합니다.
- 개인 정보 보호 요구 사항에 따라 VPC 설정을 구성합니다.
- AWS Organizations 및 IAM 정책에서 서비스 제어 정책을 사용하여 AWS Transit Gateway 및 Amazon Virtual Private Cloud(VPC) 구성의 수정을 방지할 수 있습니다. 서비스 제어 정책 샘플은 이 가이드의 VPC 구성에 대한 변경 제한 섹션을 참조하세요.

AWS WAF

개인 데이터의 의도하지 않은 공개를 방지하기 위해 웹 애플리케이션에 심층 방어 접근 방식을 배포할 수 있습니다. 애플리케이션에 입력 검증 및 속도 제한을 구축할 수 있지만 다른 방어선 역할을 할 AWS WAF 수 있습니다. AWS WAF는 보호된 웹 애플리케이션 리소스로 전달되는 HTTP 및 HTTPS 요청을 모니터링하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

를 사용하면 특정 기준을 검사하는 규칙을 정의하고 배포할 AWS WAF수 있습니다. 다음 활동은 의도하지 않은 개인 데이터 공개와 관련이 있을 수 있습니다.

- 알 수 없거나 악의적인 IP 주소 또는 지리적 위치의 트래픽

- SQL 주입과 같은 유출 관련 공격을 포함한 Open Worldwide Application Security Project(OWASP) 상위 10개 공격
- 높은 요청 속도
- 일반 봇 트래픽
- 콘텐츠 스크레이퍼

에서 관리하는 AWS WAF 규칙 그룹을 배포할 수 있습니다 AWS. 에 대한 일부 관리형 규칙 그룹을 사용하여 개인 정보 보호 및 개인 데이터에 대한 위협을 탐지할 AWS WAF 수 있습니다. 예를 들면 다음과 같습니다.

- SQL 데이터베이스 - 이 규칙 그룹에는 SQL 인젝션 공격과 같은 SQL 데이터베이스 도용과 관련된 요청 패턴을 차단하도록 설계된 규칙이 포함되어 있습니다. 애플리케이션이 SQL 데이터베이스와 접속하는 경우 이 규칙 그룹을 고려합니다.
- 알려진 잘못된 입력 - 이 규칙 그룹에는 유효하지 않은 것으로 알려져 있으며 취약성의 도용 또는 발견과 관련된 요청 패턴을 차단하도록 설계된 규칙이 포함되어 있습니다.
- 봇 컨트롤 - 이 규칙 그룹에는 과도한 리소스를 소비하고, 비즈니스 지표를 왜곡하며, 가동 중지 시간을 유발하고, 악의적인 활동을 수행할 수 있는 봇의 요청을 관리하도록 설계된 규칙이 포함되어 있습니다.
- 계정 탈취 방지(ATP) - 이 규칙 그룹에는 악의적인 계정 탈취 시도를 방지하도록 설계된 규칙이 포함되어 있습니다. 이 규칙 그룹은 애플리케이션의 로그인 엔드포인트로 전송된 로그인 시도를 검사합니다.

개인 데이터 OU - PD 애플리케이션 계정

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

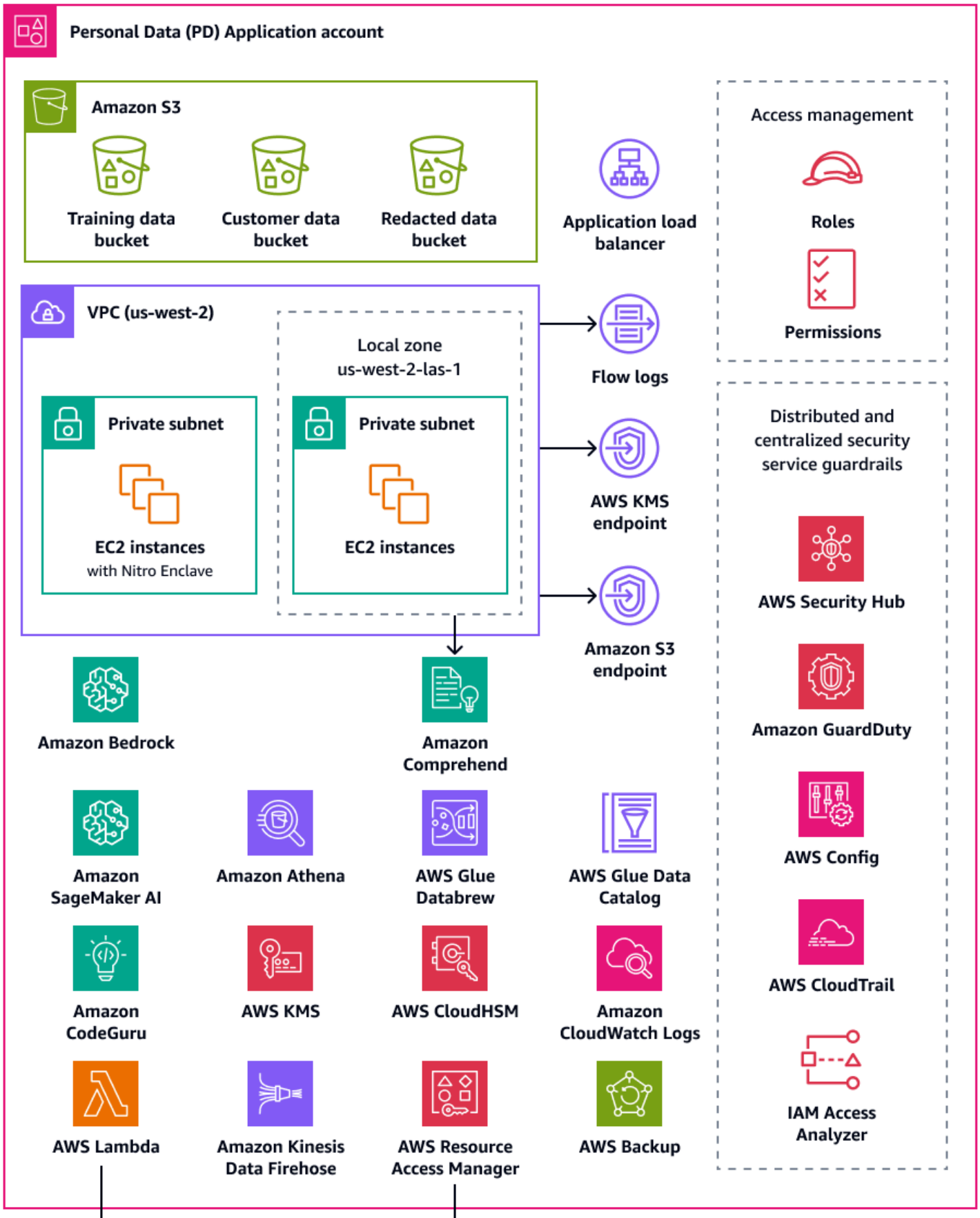
개인 데이터(PD) 애플리케이션 계정은 조직에서 개인 데이터를 수집하고 처리하는 서비스를 호스팅하는 위치입니다. 특히 이 계정에서 개인 데이터로 정의한 내용을 저장할 수 있습니다. AWS PRA는 다중 계층 서버리스 웹 아키텍처를 통해 여러 예제 프라이버시 구성을 보여줍니다. AWS 랜딩 존에서 워크로드를 운영할 때 개인 정보 보호 구성을 one-size-fits-all 솔루션으로 간주해서는 안 됩니다. 예를 들어

기본 개념, 개인 정보 보호를 강화하는 방법, 조직에서 특정 사용 사례 및 아키텍처에 솔루션을 적용하는 방법을 이해하는 것이 목표일 수 있습니다.

개인 데이터를 수집, 저장 또는 처리하는 조직의 AWS 계정 에 AWS Organizations 및 AWS Control Tower 를 사용하여 기본적이고 반복 가능한 가드레일을 배포할 수 있습니다. 이러한 계정에 대한 전용 조직 단위(OU)를 설정하는 것이 중요합니다. 예를 들어 데이터 레지던시가 핵심 설계 고려 사항인 계정의 하위 세트에만 데이터 레지던시 가드레일을 적용할 수 있습니다. 많은 조직의 경우 개인 데이터를 저장하고 처리하는 계정이 이에 해당됩니다.

조직은 개인 데이터세트의 신뢰할 수 있는 소스를 저장하는 위치인 전용 데이터 계정을 지원하는 것을 고려할 수 있습니다. 신뢰할 수 있는 데이터 소스는 가장 신뢰할 수 있고 정확한 버전의 데이터로 간주될 수 있는 기본 버전의 데이터를 저장하는 위치입니다. 예를 들어 신뢰할 수 있는 데이터 소스의 데이터를 훈련 데이터, 고객 데이터의 하위 세트 및 수정된 데이터를 저장하는 데 사용되는 PD 애플리케이션 계정의 Amazon Simple Storage Service(Amazon S3) 버킷과 같은 다른 위치로 복사할 수 있습니다. 이 다중 계정 접근 방식을 사용하여 데이터 계정의 완전하고 확정적인 개인 데이터세트를 PD 애플리케이션 계정의 다운스트림 소비자 워크로드와 분리하면 계정에 대한 무단 액세스가 발생할 경우 영향 범위를 줄일 수 있습니다.

다음 다이어그램은 PD 애플리케이션 및 데이터 계정에 구성된 AWS 보안 및 개인 정보 보호 서비스를 보여줍니다.


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

이 섹션에서는 이 계정에서 사용되는 다음 AWS 서비스 에 대한 자세한 정보를 제공합니다.

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- Amazon CloudWatch Logs
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- AWS 로컬 영역
- AWS Nitro Enclaves
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS 데이터 수명 주기를 관리하는 데 도움이 되는 기능
- AWS 서비스 및 데이터를 세그먼트화하는 데 도움이 되는 기능
- AWS 서비스 데이터 검색, 분류 또는 카탈로그 작성에 도움이 되는 및 기능

Amazon Athena

개인 정보 보호 목표를 충족하기 위해 데이터 쿼리 제한 제어를 고려할 수 있습니다. Amazon Athena는 표준 SQL을 사용하여 Amazon S3에 있는 데이터를 직접 분석할 수 있는 대화형 쿼리 서비스입니다. 데이터를 Athena에 로드할 필요가 없습니다. S3 버킷에 저장된 데이터를 직접 사용합니다.

Athena의 일반적인 사용 사례는 데이터 분석 팀에 맞춤형 데이터세트와 보안 삭제 처리된 데이터세트를 제공하는 것입니다. 데이터세트에 개인 데이터가 포함된 경우 데이터 분석 팀에 거의 가치를 제공하지 않는 개인 데이터의 전체 열을 마스킹하여 데이터세트를 보안 삭제 처리할 수 있습니다. 자세한 내용은 Amazon Athena를 사용하여 데이터 레이크의 데이터 익명화 및 관리를 참조하세요 AWS Lake Formation(AWS 블로그 게시물).

데이터 변환 접근 방식에 Athena에서 지원되는 함수 이외의 추가 유연성이 필요한 경우 사용자 정의 함수(UDF)라고 하는 사용자 지정 함수를 정의할 수 있습니다. Athena에 제출된 SQL 쿼리에서 UDF를 간접 호출할 수 있으며 AWS Lambda에서 실행됩니다. `SELECT` 및 `FILTER` SQL 쿼리에서 UDF를 사용할 수 있으며 동일한 쿼리에서 여러 UDF를 간접 호출할 수 있습니다. 개인 정보 보호를 위해 열의 모든 값에서 마지막 4자만 표시하는 등 특정 유형의 데이터 마스킹을 수행하는 UDF를 생성할 수 있습니다.

Amazon Bedrock

Amazon Bedrock은 AI21 Labs, Anthropic, Meta, Mistral AI, Amazon과 같은 선도적인 AI 회사의 파운데이션 모델에 대한 액세스를 제공하는 완전관리형 서비스입니다. 이를 통해 조직은 생성형 AI 애플리케이션을 빌드하고 규모를 조정할 수 있습니다. 어떤 플랫폼을 사용하든 생성형 AI를 사용하는 경우 조직은 개인 데이터의 잠재적 노출, 무단 데이터 액세스 및 기타 규정 준수 위반을 포함한 개인 정보 보호 위험에 직면할 수 있습니다.

Amazon Bedrock Guardrails는 Amazon Bedrock의 생성형 AI 워크로드에서 보안 및 규정 준수 모범 사례를 적용하여 이러한 위험을 완화하도록 설계되었습니다. AI 리소스의 배포 및 사용이 조직의 개인 정보 보호 및 규정 준수 요구 사항에 항상 부합되는 것은 아닙니다. 조직은 생성형 AI 모델을 사용하는 경우 데이터 개인 정보 보호를 유지 관리하는 데 어려움을 겪을 수 있습니다. 이러한 모델은 잠재적으로 민감한 정보를 기억하거나 재현할 수 있기 때문입니다. Amazon Bedrock Guardrails는 사용자 입력 및 모델 응답을 평가하여 개인 정보를 보호하는 데 도움이 됩니다. 전반적으로 입력 데이터에 개인 데이터가 포함된 경우 이 정보가 모델의 출력에 노출될 위험이 있습니다.

Amazon Bedrock Guardrails는 데이터 보호 정책을 적용하고 무단 데이터 노출을 방지하기 위한 메커니즘을 제공합니다. 여기에서는 입력에서 개인 데이터를 감지하고 차단하는 콘텐츠 필터링 기능, 부적절하거나 위험한 주제에 대한 액세스를 방지하는 데 도움이 되는 주제 제한, 모델 프롬프트 및 응답에서 민감한 용어를 마스킹하거나 수정하는 단어 필터를 제공합니다. 이러한 기능은 편향된 응답 또는 고객 신뢰 저하와 같이 개인 정보 보호 위반으로 이어질 수 있는 이벤트를 방지하는 데 도움이 됩니다. 이러한 기능을 사용하면 AI 모델에서 개인 데이터가 실수로 처리되거나 공개되지 않도록 할 수 있습니다. Amazon Bedrock Guardrails는 Amazon Bedrock 외부의 입력 및 응답 평가도 지원합니다. 자세한 내용은 Implement model-independent safety measures with Amazon Bedrock Guardrails(AWS 블로그 게시물)를 참조하세요.

Amazon Bedrock Guardrails를 사용하면 사실적 근거와 응답의 관련성을 평가하는 컨텍스트 근거 검사를 사용하여 모델 할루시네이션의 위험을 제한할 수 있습니다. 검색 증강 생성(RAG) 애플리케이션에서 서드 파티 데이터 소스를 사용하는 생성형 AI 고객 대면 애플리케이션을 배포하는 경우를 예로 들 수 있습니다. 컨텍스트 근거 검사를 사용하여 이러한 데이터 소스에 대한 모델 응답을 검증하고 부정확한 응답을 필터링할 수 있습니다. AWS PRA의 맥락에서는 워크로드 계정 전체에서 Amazon Bedrock

가드레일을 구현하여 각 워크로드의 요구 사항에 맞는 특정 프라이버시 가드레일을 적용할 수 있습니다.

AWS Clean Rooms

조직은 교차하거나 중첩되는 민감한 데이터세트를 분석하여 서로 협업할 방법을 찾고 있으므로 해당 공유 데이터의 보안 및 개인 정보 보호를 유지 관리하는 것이 중요합니다. AWS Clean Rooms는 조직이 원시 데이터 자체를 공유하지 않고 결합된 데이터세트를 분석할 수 있는 안전한 중립 환경인 데이터 클린 룸을 배포하는 데 도움이 됩니다. 또한 자신의 계정에서 데이터를 이동하거나 복사 AWS 하지 않고 기본 데이터 세트를 공개하지 않고도의 다른 조직에 대한 액세스를 제공하여 고유한 인사이트를 생성할 수 있습니다. 모든 데이터는 소스 위치에 남아 있습니다. 기본 제공 분석 규칙은 출력을 제한하고 SQL 쿼리를 제한합니다. 모든 쿼리가 로깅되고 협업 멤버는 데이터가 쿼리되는 방식을 볼 수 있습니다.

AWS Clean Rooms 공동 작업을 생성하고 다른 AWS 고객을 해당 공동 작업의 구성원으로 초대할 수 있습니다. 한 멤버에게 멤버 데이터세트를 쿼리할 수 있는 권한을 부여하고 추가 멤버를 선택하여 해당 쿼리의 결과를 받도록 선택할 수 있습니다. 둘 이상의 멤버가 데이터세트를 쿼리해야 하는 경우 동일한 데이터 소스와 다른 멤버 설정으로 추가 협업을 생성할 수 있습니다. 각 멤버는 협업 멤버와 공유되는 데이터를 필터링할 수 있으며, 사용자 지정 분석 규칙을 사용하여 협업에 제공하는 데이터를 분석할 수 있는 방법에 대한 제한을 설정할 수 있습니다.

공동 작업에 제공되는 데이터와 다른 구성원이 데이터를 사용하는 방법을 제한하는 것 외에도는 프라이버시를 보호하는 데 도움이 되는 다음과 같은 기능을 AWS Clean Rooms 제공합니다.

- 차등 프라이버시는 데이터에 신중하게 보정된 양의 노이즈를 추가하여 사용자 개인 정보 보호를 개선하는 수학 기법입니다. 이를 통해 관심 값을 가리지 않고 데이터세트 내에서 개별 사용자 재식별 위험을 줄일 수 있습니다. AWS Clean Rooms 차등 프라이버시를 사용하는 경우 차등 프라이버시에 대한 전문 지식은 필요하지 않습니다.
- AWS Clean Rooms ML을 사용하면 둘 이상의 당사자가 데이터를 직접 서로 공유할 필요 없이 데이터에서 유사한 사용자를 식별할 수 있습니다. 이렇게 하면 협업 멤버가 다른 멤버의 데이터세트에서 개인을 식별할 수 있는 멤버십 추론 공격의 위험이 줄어듭니다. 유사 모델을 생성하고 유사 세그먼트를 생성하면 AWS Clean Rooms ML은 원본 데이터를 노출하지 않고 데이터 세트를 비교하는 데 도움이 됩니다. 이렇게 하면 멤버가 ML 전문 지식을 보유하거나 외부에서 작업을 수행할 필요가 없습니다 AWS Clean Rooms. 훈련된 모델의 전체 제어 및 소유권을 유지합니다.
- Cryptographic Computing for Clean Rooms(C3R)를 분석 규칙과 함께 사용하여 민감한 데이터에서 인사이트를 도출할 수 있습니다. 협업의 다른 당사자가 학습할 수 있는 내용을 암호화된 방식으로 제한합니다. C3R 암호화 클라이언트를 사용하면 데이터가 제공되기 전에 클라이언트에서 암호화됩니다 AWS Clean Rooms. 데이터 테이블은 Amazon S3에 업로드되기 전에 클라이언트 측 암호화 도구

를 사용하여 암호화되므로 데이터는 암호화된 상태로 유지되며 처리 과정에서 해당 상태가 유지됩니다.

AWS PRA에서는 데이터 계정에서 AWS Clean Rooms 공동 작업을 생성하는 것이 좋습니다. 이를 사용하여 암호화된 고객 데이터를 서드 파티와 공유할 수 있습니다. 제공된 데이터세트에 중복이 있는 경우에만 사용합니다. 중복을 확인하는 방법에 대한 자세한 내용은 AWS Clean Rooms 설명서의 분석 규칙 나열을 참조하세요.

Amazon CloudWatch Logs

Amazon CloudWatch Logs는 모든 시스템, 애플리케이션 및 AWS 서비스 의 로그를 중앙 집중화하여 모니터링하고 안전하게 보관할 수 있도록 도와줍니다. CloudWatch Logs에서는 신규 또는 기존 로그 그룹에 대한 데이터 보호 정책을 사용하여 개인 데이터의 공개 위험을 최소화할 수 있습니다. 데이터 보호 정책은 로그에서 개인 데이터와 같은 민감한 데이터를 감지할 수 있습니다. 데이터 보호 정책은 사용자가 AWS Management Console을 통해 로그에 액세스할 때 해당 데이터를 마스킹할 수 있습니다. 사용자가 워크로드의 전반적인 용도 사양에 따라 개인 데이터에 직접 액세스해야 하는 경우 해당 사용자에게 `logs:Unmask` 권한을 할당할 수 있습니다. 또한 계정 전체의 데이터 보호 정책을 생성하고 조직의 모든 계정에 이 정책을 일관되게 적용할 수 있습니다. 이 경우 CloudWatch Logs의 모든 현재 및 미래 로그 그룹에 대해 마스킹이 기본적으로 구성됩니다. 또한 감사 보고서를 활성화하고 다른 로그 그룹, Amazon S3 버킷 또는 Amazon Data Firehose로 전송하는 것이 좋습니다. 이러한 보고서에는 각 로그 그룹의 데이터 보호 조사 결과에 대한 자세한 레코드가 포함되어 있습니다.

Amazon CodeGuru Reviewer

개인 정보 보호와 보안 모두의 차원에서 많은 조직이 배포 및 배포 후 단계 모두에서 지속적인 규정 준수를 지원하는 것이 중요합니다. AWS PRA에는 개인 데이터를 처리하는 애플리케이션의 배포 파이프라인에 선제적 제어가 포함되어 있습니다. Amazon CodeGuru Reviewer는 Java, JavaScript 및 Python 코드에서 개인 데이터를 노출할 수 있는 잠재적 결함을 감지할 수 있습니다. 그리고 개발자에게 코드 개선을 위한 제안을 제공합니다. CodeGuru Reviewer는 광범위한 보안, 개인 정보 보호 및 일반적인 권장 사례에서 결함을 식별할 수 있습니다. 이 기능은 AWS CodeCommit, Bitbucket, GitHub 및 Amazon S3를 비롯한 여러 소스 제공업체와 함께 작동하도록 설계되었습니다. CodeGuru Reviewer가 감지할 수 있는 일부 개인 정보 보호 관련 결함은 다음과 같습니다.

- SQL 인젝션
- 보안되지 않은 쿠키
- 누락된 권한 부여
- 클라이언트 측 AWS KMS 재암호화

CodeGuru Reviewer가 감지할 수 있는 항목의 전체 목록은 Amazon CodeGuru Detector Library를 참조하세요.

Amazon Comprehend

Amazon Comprehend는 영어 텍스트 문서에서 인사이트 및 관계를 찾기 위해 기계 학습을 사용하는 자연어 처리(NLP) 서비스입니다. Amazon Comprehend는 정형, 반정형 또는 비정형 텍스트 문서에서 개인 데이터를 감지하고 수정할 수 있습니다. 자세한 내용은 Amazon Comprehend 설명서의 Personally identifiable information (PII)을 참조하세요.

Amazon Comprehend에는 AWS SDKs 통한 애플리케이션 통합을 위한 다양한 옵션이 있으므로 Amazon Comprehend를 사용하여 데이터를 수집, 저장 및 처리하는 다양한 위치에서 개인 데이터를 식별할 수 있습니다. Amazon Comprehend ML 기능을 사용하여 애플리케이션 로그(AWS 블로그 게시물), 고객 이메일, 지원 티켓 등의 개인 데이터를 감지하고 수정할 수 있습니다. PD 애플리케이션 계정의 아키텍처 다이어그램에서는 Amazon EC2의 애플리케이션 로그에 대해 이 함수를 수행하는 방법을 보여줍니다. Amazon Comprehend는 다음과 같은 두 가지 수정 모드를 제공합니다.

- `REPLACE_WITH_PII_ENTITY_TYPE`은 각 PII 엔터티를 해당 유형으로 바꿉니다. 예를 들어 Jane Doe는 NAME으로 대체됩니다.
- `MASK`는 PII 엔터티의 문자를 원하는 문자(!, #, $, %, &, 또는 @)로 바꿉니다. 예를 들어 Jane Doe를 **** ***로 바꿀 수 있습니다.

Amazon Data Firehose

Amazon Data Firehose는 스트리밍 데이터를 캡처 및 변환하고 Amazon Managed Service for Apache Flink 또는 Amazon S3와 같은 다운스트림 서비스로 로드하는 데 사용할 수 있습니다. Firehose는 처음부터 처리 파이프라인을 빌드할 필요 없이 애플리케이션 로그와 같은 대량의 스트리밍 데이터를 전송하는 데 자주 사용됩니다.

Lambda 함수를 사용하여 데이터를 다운스트림으로 전송하기 전에 사용자 지정 또는 기본 제공 처리를 수행할 수 있습니다. 개인 정보 보호를 위해 이 기능은 데이터 최소화 및 국가 간 데이터 전송 요구 사항을 지원합니다. 예를 들어 Lambda 및 Firehose를 사용하여 로그 아카이브 계정에서 중앙 집중화하기 전에 다중 리전 로그 데이터를 변환할 수 있습니다. 자세한 내용은 Biogen: Centralized Logging Solution for Multi Accounts(YouTube 비디오)를 시청하세요. PD 애플리케이션 계정에서 Firehose 전송 스트림으로 로그를 푸시 AWS CloudTrail 하도록 Amazon CloudWatch 및를 구성합니다. Lambda 함수는 로그를 변환하여 로그 아카이브 계정의 중앙 S3 버킷으로 전송합니다. 개인 데이터가 포함된 특정 필드를 마스킹하도록 Lambda 함수를 구성할 수 있습니다. 그러면 AWS 리전에서 개인 데이터의

전송을 방지할 수 있습니다. 이 접근 방식을 사용하면 사후가 아니라 전송 및 중앙 집중화 이전에 개인 데이터가 마스킹됩니다. 국가 간 전송 요구 사항이 적용되지 않는 관할 구역의 애플리케이션의 경우 일반적으로 CloudTrail의 조직 추적을 통해 로그를 집계하는 것이 더 운영 효율적이고 비용 효율적입니다. 자세한 내용은 이 가이드의 보안 OU - 보안 도구 계정 섹션에서 AWS CloudTrail을 참조하세요.

Amazon DataZone

조직은 AWS 서비스 와 같은를 통해 데이터를 공유하는 접근 방식을 확장함에 따라 데이터 소유자라는 데이터에 가장 익숙한 사람이 차등 액세스를 제어하도록 AWS Lake Formation하려고 합니다. 그러나 이러한 데이터 소유자는 동의 또는 국가 간 데이터 전송 고려 사항과 같은 개인 정보 보호 요구 사항을 알고 있을 수 있습니다. Amazon DataZone은 데이터 소유자와 데이터 거버넌스 팀이 데이터 거버넌스 정책에 따라 조직 전체에서 데이터를 공유하고 소비할 수 있도록 지원합니다. Amazon DataZone에서 사업부(LOB)는 자체 데이터를 관리하며 카탈로그를 통해 이 소유권을 추적합니다. 이해 당사자는 비즈니스 작업의 일부로 데이터를 찾고 데이터에 대한 액세스를 요청할 수 있습니다. 데이터 게시자가 설정한 정책을 준수하는 한, 데이터 소유자는 관리자나 데이터 이동 없이 기본 테이블에 대한 액세스 권한을 부여할 수 있습니다.

개인 정보 보호 컨텍스트에서 Amazon DataZone은 다음 사용 사례 예제에서 유용할 수 있습니다.

- 고객 대면 애플리케이션은 별도의 마케팅 LOB와 공유할 수 있는 사용량 데이터를 생성합니다. 마케팅을 옵트인한 고객의 데이터만 카탈로그에 게시되도록 해야 합니다.
- 유럽 고객 데이터는 게시되지만 유럽 경제 지역(EEA)의 LOB에서만 이를 구독할 수 있습니다. 자세한 내용은 Enhance data security with fine-grained access controls in Amazon DataZone을 참조하세요.

AWS PRA에서는 공유 Amazon S3 버킷의 데이터를 데이터 생산자인 Amazon DataZone에 연결할 수 있습니다.

AWS Glue

개인 데이터가 포함된 데이터세트를 유지 관리하는 작업은 개인 정보 보호 중심 설계의 주요 구성 요소입니다. 조직의 데이터는 정형, 반정형 또는 비정형 형태로 존재할 수 있습니다. 구조가 없는 개인 데이터세트에서는 데이터 최소화, 데이터 주체 요청의 일부로 단일 데이터 주체에 귀속된 데이터 추적, 일관된 데이터 품질 보장, 데이터세트의 전체 세분화 등 여러 개인 정보 보호 개선 작업을 수행하기 어려울 수 있습니다. AWS Glue는 완전관리형 추출, 전환, 적재(ETL) 서비스입니다. 데이터 스토어와 데이터 스트림 간에 데이터를 분류, 정리, 보강 및 이동하는 데 도움이 될 수 있습니다. AWS Glue 기능은 분석, 기계 학습 및 애플리케이션 개발을 위한 데이터 세트를 검색, 준비, 구조화 및 결합하는 데 도움이 되도록 설계되었습니다. AWS Glue 를 사용하여 기존 데이터 세트를 기반으로 예측 가능하고 일반적인

구조를 생성할 수 있습니다. AWS Glue Data Catalog AWS Glue DataBrew및 AWS Glue Data Quality는 조직의 개인 정보 보호 요구 사항을 지원하는 데 도움이 되는 AWS Glue 기능입니다.

AWS Glue Data Catalog

AWS Glue Data Catalog는 유지 관리 가능한 데이터세트를 설정하는 데 도움이 됩니다. 데이터 카탈로그에는 추출, 변환 및 로드(ETL) 작업의 소스 및 대상으로 사용되는 데이터에 대한 참조가 포함되어 있습니다 AWS Glue. Data Catalog의 정보는 메타데이터 테이블로 저장되며, 각 테이블은 단일 데이터 저장소를 지정합니다. AWS Glue 크롤러를 실행하여 다양한 데이터 저장소 유형으로 데이터 인벤토리를 가져옵니다. 기본 제공 분류자와 사용자 지정 분류자를 크롤러에 추가합니다. 그러면 이러한 분류자가 개인 데이터의 데이터 형식과 스키마를 추론합니다. 크롤러는 메타데이터를 Data Catalog에 작성합니다. 중앙 집중식 메타데이터 테이블은 AWS 환경의 서로 다른 개인 데이터 소스에 구조와 예측 가능성을 추가하므로 데이터 주체 요청(예: 삭제 권한)에 더 쉽게 응답할 수 있습니다. Data Catalog를 사용하여 이러한 요청에 자동으로 응답하는 방법에 대한 포괄적인 예는 Amazon S3 Find and Forget을 사용하여 데이터 레이크에서 데이터 삭제 요청 처리(블로그 게시물)를 참조하세요.AWS 마지막으로 조직에서 AWS Lake Formation을 사용하여 데이터베이스, 테이블, 행 및 셀에 대한 세분화된 액세스를 관리하고 제공하는 경우 Data Catalog는 주요 구성 요소입니다. 데이터 카탈로그는 교차 계정 데이터 공유를 제공하며 태그 기반 액세스 제어를 사용하여 데이터 레이크를 대규모로 관리하는 데 도움이 됩니다(AWS 블로그 게시물). 자세한 내용은 이 섹션의 AWS Lake Formation을 참조하세요.

AWS Glue DataBrew

AWS Glue DataBrew는 데이터를 정리하고 정규화하는 데 도움이 되며, 개인 식별 정보를 제거 또는 마스킹하고 데이터 파이프라인의 민감한 데이터 필드를 암호화하는 등 데이터에 대한 변환을 수행할 수 있습니다. 또한 데이터 리니지를 시각적으로 매핑하여 데이터가 거친 다양한 데이터 소스 및 변환 단계를 이해할 수 있습니다. 조직이 개인 데이터 출처를 더 잘 이해하고 추적하기 위해 노력함에 따라 이 기능은 점점 더 중요해지고 있습니다. DataBrew는 데이터 준비 중에 개인 데이터를 마스킹하는 데 도움이 됩니다. 데이터 프로파일링 작업 중에 개인 데이터를 감지하고 개인 데이터가 포함될 수 있는 열의 번호 및 잠재적 범주와 같은 통계를 수집할 수 있습니다. 그런 다음 코드를 작성하지 않고도 대체, 해싱, 암호화 및 암호 해독을 포함하여 기본 제공 가역 또는 비가역 데이터 변환 기술을 사용할 수 있습니다. 그런 다음 정리 및 마스킹 처리된 데이터세트를 분석, 보고 및 기계 학습 태스크에 대한 다운스트림으로 사용할 수 있습니다. DataBrew에서 사용할 수 있는 몇 가지 데이터 마스킹 기법은 다음과 같습니다.

- 해싱 - 열 값에 해시 함수를 적용합니다.
- 대체 - 개인 데이터를 다른 사실적인 값으로 바꿉니다.
- Null 처리 또는 삭제 - 특정 필드를 null 값으로 바꾸거나 열을 삭제합니다.
- 마스킹 - 문자 스크램블링 기법을 사용하거나 열의 특정 부분을 마스킹합니다.

사용 가능한 암호화 기법은 다음과 같습니다.

- 결정적 암호화 - 열 값에 결정적 암호화 알고리즘을 적용합니다. 결정적 암호화는 항상 값에 대해 동일한 사이퍼텍스트를 생성합니다.
- 확률적 암호화 - 열 값에 확률적 암호화 알고리즘을 적용합니다. 확률적 암호화는 적용될 때마다 다른 사이퍼텍스트를 생성합니다.

DataBrew에서 제공된 개인 데이터 변환 레시피의 전체 목록은 Personally identifiable information (PII) recipe steps를 참조하세요.

AWS Glue 데이터 품질

AWS Glue 데이터 품질은 데이터 파이프라인 간에 고품질 데이터를 데이터 소비자에게 전달하기 전에 사전에 데이터 파이프라인 간에 전송을 자동화하고 운영할 수 있도록 지원합니다. AWS Glue 데이터 품질은 데이터 파이프라인 전반의 데이터 품질 문제에 대한 통계 분석을 제공하고, Amazon EventBridge에서 알림을 트리거하고, 문제 해결을 위한 품질 규칙 권장 사항을 제공할 수 있습니다. AWS Glue 데이터 품질은 또한 도메인별 언어로 규칙 생성을 지원하므로 사용자 지정 데이터 품질 규칙을 생성할 수 있습니다.

AWS Key Management Service

AWS Key Management Service (AWS KMS)를 사용하면 암호화 키를 생성하고 제어하여 데이터를 보호할 수 있습니다.는 하드웨어 보안 모듈을 AWS KMS 사용하여 FIPS 140-2 암호화 모듈 검증 프로그램에 AWS KMS keys 따라 보호하고 검증합니다. 이 서비스가 보안 컨텍스트에서 사용되는 방법에 대한 자세한 내용은 AWS Security Reference Architecture를 참조하세요.

AWS KMS 는 암호화 AWS 서비스 를 제공하는 대부분의와 통합되며 개인 데이터를 처리하고 저장하는 애플리케이션에서 KMS 키를 사용할 수 있습니다. AWS KMS 를 사용하여 다음을 비롯해 다양한 개인 정보 보호 요구 사항을 지원하고 개인 데이터를 보호할 수 있습니다.

- 강도, 교체, 만료 및 기타 옵션을 더 잘 제어하기 위해 고객 관리형 키 사용.
- 전용 고객 관리형 키를 사용하여 개인 데이터 및 개인 데이터에 대한 액세스를 허용하는 보안 암호 보호.
- 데이터 분류 수준을 정의하고 수준당 하나 이상의 전용 고객 관리형 키 지정. 예를 들어 운영 데이터를 암호화하는 키 하나와 개인 데이터를 암호화하는 다른 키 하나가 있을 수 있습니다.
- KMS 키에 대한 의도하지 않은 교차 계정 액세스 방지.
- 암호화할 리소스 AWS 계정 와 동일한 내에 KMS 키 저장.

- KMS 키 관리 및 사용에 대한 업무 분리 구현. 자세한 내용은 KMS 및 IAM을 사용하여 S3의 암호화된 데이터에 대한 독립적인 보안 제어를 활성화하는 방법(AWS 블로그 게시물)을 참조하세요.
- 예방 및 사후 대응 가드레일을 통해 자동 키 교체 적용.

기본적으로 KMS 키는 저장되며 키가 생성된 리전에서만 사용할 수 있습니다. 조직에 데이터 레지던시 및 주권에 대한 특정 요구 사항이 있는 경우 다중 리전 KMS 키가 사용 사례에 적합한지 고려합니다. 다중 리전 키는 서로 바꿔서 사용할 수 AWS 리전 있는 다양한의 특수 목적 KMS 키입니다. 다중 리전 키를 생성하는 프로세스는 내 AWS 리전 경계를 넘어 키 구성 요소를 이동 AWS KMS하므로 이러한 리전 격리 부족은 조직의 주권 및 레지던시 목표와 호환되지 않을 수 있습니다. 이를 해결하는 한 가지 방법은 리전별 고객 관리형 키와 같은 서로 다른 유형의 KMS 키를 사용하는 것입니다.

외부 키 스토어

많은 조직의 경우의 기본 AWS KMS 키 스토어는 데이터 주권 및 일반 규제 요구 사항을 충족할 AWS 클라우드 수 있습니다. 그러나 드물지만 암호화 키가 클라우드 환경 외부에서 생성 및 유지 관리되고 사용자에게 독립적인 권한 부여 및 감사 경로가 있어야 하는 경우가 있을 수 있습니다. 의 외부 키 스토어를 사용하면 조직이 외부에서 소유하고 제어하는 키 구성 요소로 개인 데이터를 암호화 AWS KMS 할 수 있습니다 AWS 클라우드. 여전히 평소와 같이 AWS KMS API와 상호 작용하지만는 사용자가 제공하는 외부 키 스토어 프록시(XKS 프록시) 소프트웨어와만 AWS KMS 상호 작용합니다. 그러면 외부 키 스토어 프록시가 AWS KMS 와 외부 키 관리자 간의 모든 통신을 중재합니다.

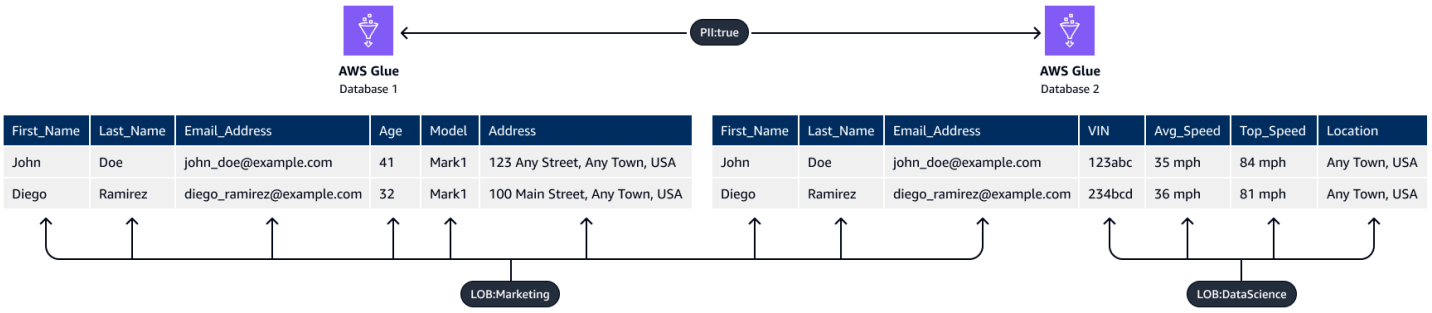
데이터 암호화에 외부 키 저장소를 사용하는 경우 AWS KMS에서 키를 유지 관리하는 방식과 비교했을 때 추가 운영 오버헤드를 고려하는 것이 중요합니다. 외부 키 저장소를 사용하는 경우 사용자가 외부 키 저장소를 생성, 구성 및 유지 관리해야 합니다. 또한 XKS 프록시와 같이 유지 관리해야 하는 추가 인프라에 오류가 있고 연결이 끊어지면 사용자가 일시적으로 데이터를 해독하고 액세스하지 못할 수 있습니다. 규정 준수 및 규제 이해관계자와 긴밀히 협력하여 개인 데이터 암호화에 대한 법적 및 계약상의 의무와 가용성 및 복원력에 대한 서비스 수준 계약을 이해합니다.

AWS Lake Formation

정형 메타데이터 카탈로그를 통해 데이터세트를 카탈로그화하고 분류하는 많은 조직이 조직 전체에서 해당 데이터세트를 공유하려고 합니다. AWS Identity and Access Management (IAM) 권한 정책을 사용하여 전체 데이터 세트에 대한 액세스를 제어할 수 있지만 민감도가 다양한 개인 데이터가 포함된 데이터 세트에는 더 세분화된 제어가 필요한 경우가 많습니다. 예를 들어 용도 사양 및 사용 제한(FPC 웹사이트)에서는 마케팅 팀이 고객 주소에 액세스해야 하지만 데이터 과학 팀은 액세스해서는 안 된다는 점을 표시할 수 있습니다.

데이터 레이크와 관련된 개인 정보 보호 문제도 있으며, 이는 원본 형식으로 대량의 민감한 데이터에 대한 액세스를 중앙 집중화합니다. 조직의 데이터 대부분은 한 곳에서 중앙 집중식으로 액세스할 수 있으므로 데이터세트, 특히 개인 데이터가 포함된 데이터세트의 논리적 분리가 가장 중요할 수 있습니다. AWS Lake Formation은 단일 소스에서든 데이터 레이크에 포함된 많은 소스에서든 데이터를 공유할 때 거버넌스 및 모니터링을 설정하는 데 도움이 될 수 있습니다. AWS PRA에서는 Lake Formation을 사용하여 데이터 계정의 공유 데이터 버킷에 있는 데이터에 대한 세분화된 액세스 제어를 제공할 수 있습니다.

Lake Formation에서 태그 기반 액세스 제어 기능을 사용할 수 있습니다. 태그 기반 액세스 제어는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. Lake Formation에서는 이러한 속성을 LF 태그라고 합니다. LF 태그를 사용하면 이러한 태그를 데이터 카탈로그 데이터베이스, 테이블 및 열에 연결하고 IAM 위탁자에게 동일한 태그를 부여할 수 있습니다. 위탁자에게 리소스 태그 값과 일치하는 태그 값에 대한 액세스 권한이 부여되면 Lake Formation에서 해당 리소스에서의 작업을 허용합니다. 다음 이미지에서는 LF 태그 및 권한을 할당하여 개인 데이터에 대한 차별화된 액세스를 제공하는 방법을 보여줍니다.



이 예제에서는 태그의 계층 특성을 사용합니다. 두 데이터베이스 모두 개인 식별 정보(`PII:true`)를 포함하지만 열 수준의 태그는 특정 열을 서로 다른 팀으로 제한합니다. 이 예제에서는 `PII:true` LF 태그가 있는 IAM 보안 주체가이 태그가 있는 AWS Glue 데이터베이스 리소스에 액세스할 수 있습니다. `LOB:DataScience` LF 태그가 있는 위탁자는 이 태그가 있는 특정 열에 액세스할 수 있고, `LOB:Marketing` LF 태그가 있는 위탁자는 이 태그가 있는 열에만 액세스할 수 있습니다. 마케팅은 마케팅 사용 사례와 관련된 PII에만 액세스할 수 있으며 데이터 과학 팀은 사용 사례와 관련된 PII에만 액세스할 수 있습니다.

AWS 로컬 영역

데이터 레지던시 요구 사항을 준수해야 하는 경우 이러한 요구 사항을 지원하기 AWS 리전 위해 특정에 개인 데이터를 저장하고 처리하는 리소스를 배포할 수 있습니다. 컴퓨팅, 스토리지AWS 로컬 영역, 데이터베이스 및 기타 일부 AWS 리소스를 대규모 인구 및 산업 센터와 가까운 곳에 배치하는 데 도움이 되는를 사용할 수도 있습니다. 로컬 영역은 대규모 대도시 지역과 지리적으로 가까운 AWS 리전 의 확장 기능입니다. 로컬 영역이 대응되는 리전 근처에서 로컬 영역 내에 특정 유형의 리소스를 배치할

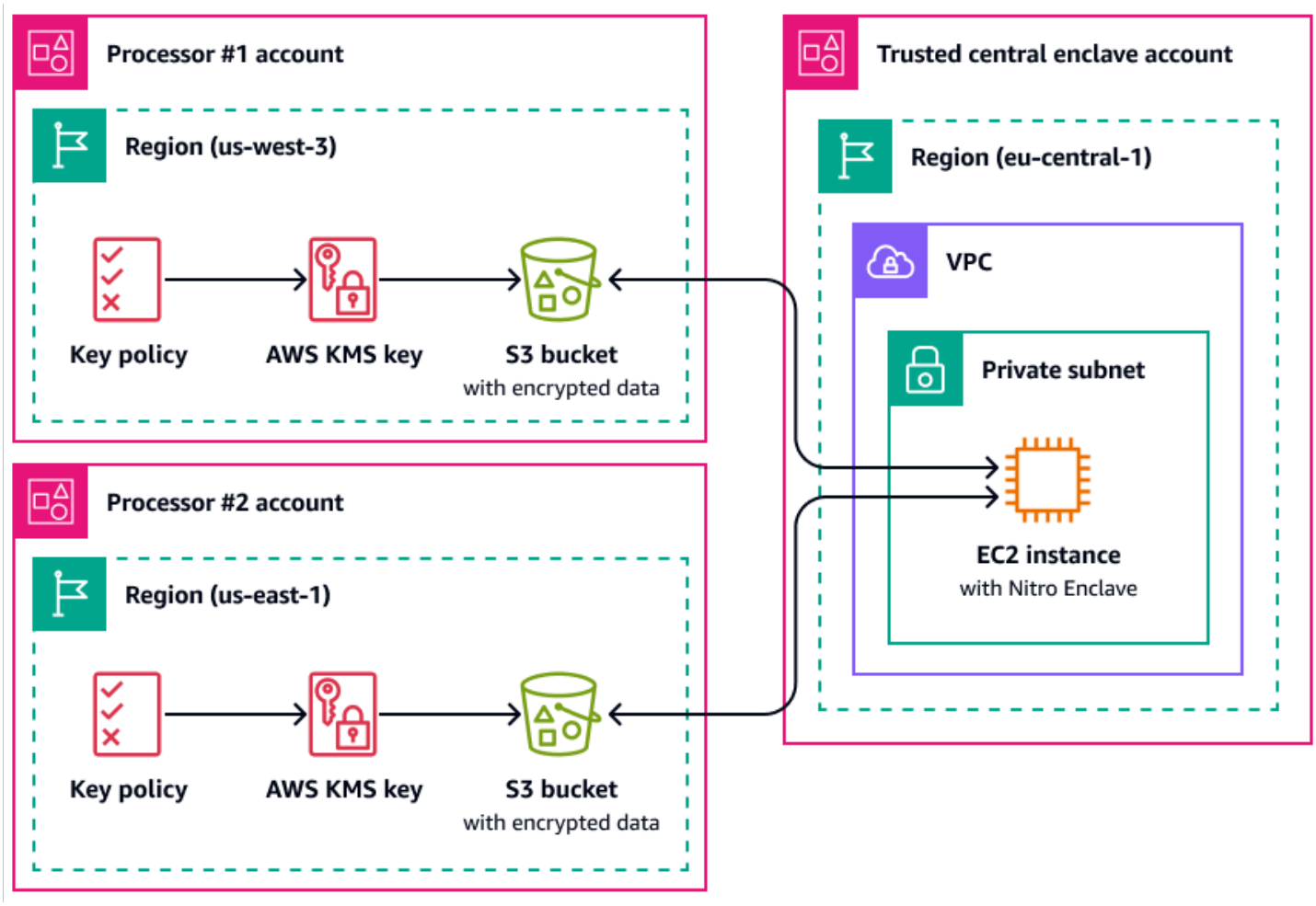
수 있습니다. 로컬 영역은 동일한 법적 관할 구역 내에서 리전을 사용할 수 없는 경우 데이터 레지던시 요구 사항을 충족하는 데 도움이 될 수 있습니다. 로컬 영역을 사용하는 경우 조직 내에 배포된 데이터 레지던시 제어를 고려합니다. 예를 들어 특정 로컬 영역에서 다른 리전으로의 데이터 전송을 방지하기 위한 제어가 필요할 수 있습니다. SCPs를 사용하여 국가 간 데이터 전송 가드레일을 유지하는 방법에 대한 자세한 내용은 랜딩 존 제어를 AWS 로컬 영역 사용하여에서 데이터 레지던시를 관리하는 모범 사례(AWS 블로그 게시물)를 참조하세요.

AWS Nitro Enclaves

Amazon Elastic Compute Cloud(Amazon EC2)와 같은 컴퓨팅 서비스를 사용하여 개인 데이터를 처리하는 등 처리 관점에서 데이터 세분화 전략을 고려합니다. 대규모 아키텍처 전략의 일환으로 기밀 컴퓨팅을 사용하면 격리되고 보호되며 신뢰할 수 있는 CPU 엔클레이브에서 개인 데이터 처리를 격리할 수 있습니다. 엔클레이브는 별도의 강화되고 고도로 제한된 가상 머신입니다. AWS Nitro Enclaves는 이러한 격리된 컴퓨팅 환경을 생성하는 데 도움이 되는 Amazon EC2 기능입니다. 자세한 내용은 AWS Nitro 시스템의 보안 설계(AWS 백서)를 참조하세요.

Nitro Enclaves는 상위 인스턴스의 커널과 분리된 커널을 배포합니다. 상위 인스턴스의 커널은 엔클레이브에 액세스할 수 없습니다. 사용자는 엔클레이브의 데이터 및 애플리케이션에 SSH 또는 원격으로 액세스할 수 없습니다. 개인 데이터를 처리하는 애플리케이션을 엔클레이브에 임베드하고 엔클레이브와 상위 인스턴스 간 통신을 용이하게 하는 소켓인 엔클레이브의 Vsock를 사용하도록 구성할 수 있습니다.

Nitro Enclaves가 유용할 수 있는 사용 사례 중 하나는 별도의에 AWS 리전 있고 서로 신뢰하지 않을 수 있는 두 데이터 프로세서 간의 공동 처리입니다. 다음 이미지에서는 중앙 처리에 엔클레이브를 사용하는 방법, 엔클레이브로 전송되기 전에 개인 데이터를 암호화하기 위한 KMS 키, 암호 해독을 요청하는 엔클레이브가 증명 문서에 고유한 측정값을 보유하는지를 확인하는 AWS KMS key 정책을 보여줍니다. 자세한 내용과 지침은 에서 암호화 증명 사용을 참조하세요 AWS KMS. 키 정책 샘플은 이 가이드의 AWS KMS 키를 사용하려면 증명이 필요합니다. 섹션을 참조하세요.



이 구현에서는 각 데이터 프로세서와 기본 엔클레이브만 일반 텍스트 개인 데이터에 액세스할 수 있습니다. 각 데이터 프로세서 환경 외부에서 데이터가 노출되는 유일한 위치는 액세스 및 변조를 방지하도록 설계된 엔클레이브 자체에 있습니다.

AWS PrivateLink

많은 조직이 신뢰할 수 없는 네트워크에 개인 데이터가 노출되지 않도록 제한하려고 합니다. 예를 들어 전체 애플리케이션 아키텍처 설계의 개인 정보 보호를 개선하려는 경우 데이터 민감도(AWS 서비스 및 데이터를 세그먼트화하는 데 도움이 되는 기능 섹션에서 논의한 데이터세트의 논리적 및 물리적 분리와 유사)를 기반으로 네트워크를 세분화할 수 있습니다. AWS PrivateLink는 가상 프라이빗 클라우드(VPC)에서 VPC 외부의 서비스에 대한 단방향 프라이빗 연결을 생성하는 데 도움이 됩니다. AWS PrivateLink를 사용하면 환경에서 개인 데이터를 저장하거나 처리하는 서비스에 대한 전용 프라이빗 연결을 설정할 수 있습니다. 이 경우 퍼블릭 엔드포인트에 연결하고 신뢰할 수 없는 퍼블릭 네트워크를 통해 이 데이터를 전송할 필요가 없습니다. 범위 내 서비스에 대해 AWS PrivateLink 서비스 엔드포인트를 활성화하면 통신하기 위해 인터넷 게이트웨이, NAT 디바이스, 퍼블릭 IP 주소, AWS Direct Connect 연결 또는 AWS Site-to-Site VPN 연결이 필요하지 않습니다. AWS PrivateLink 를 사용하여

개인 데이터에 대한 액세스를 제공하는 서비스에 연결하는 경우 조직의 데이터 경계 정의에 따라 VPC 엔드포인트 정책 및 보안 그룹을 사용하여 액세스를 제어할 수 있습니다. 신뢰할 수 있는 조직의 IAM 원칙 및 AWS 리소스만 서비스 엔드포인트에 액세스할 수 있도록 허용하는 샘플 VPC 엔드포인트 정책은이 가이드VPC 리소스에 액세스하려면 조직 멤버십 필요의 섹션을 참조하세요.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM)를 사용하면에서 리소스를 안전하게 공유 AWS 계정 하여 운영 오버헤드를 줄이고 가시성 및 감사 가능성을 제공할 수 있습니다. 다중 계정 세분화 전략을 계획할 때는 AWS RAM 를 사용하여 별도의 격리된 계정에 저장하는 개인 데이터 스토어를 공유하는 것이 좋습니다. 처리를 목적으로 해당 개인 데이터를 신뢰할 수 있는 다른 계정과 공유할 수 있습니다. 에서는 공유 리소스에서 수행할 AWS RAM수 있는 작업을 정의하는 권한을 관리할 수 있습니다. 에 대한 모든 API 호출 AWS RAM 은 CloudTrail에 로깅됩니다. 또한 리소스 공유가 변경되는 경우 AWS RAM 와 같은의 특정 이벤트에 대해 자동으로 알리도록 Amazon CloudWatch Events를 구성할 수 있습니다.

IAM의 AWS 리소스 기반 정책 또는 Amazon S3의 버킷 정책을 AWS 계정 사용하여 다양한 유형의 리소스를 다른와 공유할 수 있지만,는 프라이버시에 대한 몇 가지 추가 이점을 AWS RAM 제공합니다.는 데이터 소유자에게 다음을 AWS 계정포함하여에서 데이터가 공유되는 방식과 대상에 대한 추가 가시성을 AWS 제공합니다.

- 계정 ID 목록을 수동으로 업데이트하는 대신, 전체 OU와 리소스 공유 가능
- 소비자 계정이 조직에 속하지 않은 경우 공유 시작을 위해 초대 프로세스 적용
- 각 개별 리소스에 액세스할 수 있는 특정 IAM 위탁자에 대한 가시성

이전에 리소스 기반 정책을 사용하여 리소스 공유를 관리하고 AWS RAM 대신를 사용하려면 PromoteResourceShareCreatedFromPolicy API 작업을 사용합니다.

Amazon SageMaker AI

Amazon SageMaker AI는 ML 모델을 빌드하고 훈련시킨 후 모델을 프로덕션 지원 호스팅 환경에 배포할 수 있는 관리형 기계 학습(ML) 서비스입니다. SageMaker AI는 훈련 데이터를 더 쉽게 준비하고 모델 기능을 생성할 수 있도록 설계되었습니다.

Amazon SageMaker Model Monitor

많은 조직에서 ML 모델을 훈련할 때 데이터 드리프트를 고려합니다. 데이터 드리프트는 프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화입니다. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습

니다. 프로덕션 환경에서 ML 모델이 수신하는 데이터의 통계적 속성이 훈련 받은 기준 데이터의 속성과 멀어지면 모델의 예측 정확도가 떨어질 수 있습니다. Amazon SageMaker Model Monitor는 프로덕션에서 Amazon SageMaker AI 기계 학습 모델의 품질을 지속적으로 모니터링하고 데이터 품질을 모니터링합니다. 데이터 드리프트를 조기에 선제적으로 감지하면 모델 재훈련, 업스트림 시스템 감사 또는 데이터 품질 문제 수정과 같은 수정 조치를 구현하는 데 도움이 될 수 있습니다. Model Monitor를 사용하면 모델을 수동으로 모니터링하거나 추가 도구를 빌드가 필요성이 줄어듭니다.

Amazon SageMaker Clarify

Amazon SageMaker Clarify는 모델 편향과 설명 가능성에 대한 인사이트를 제공합니다. SageMaker Clarify는 ML 모델 데이터 준비 및 전반적인 개발 단계에서 일반적으로 사용됩니다. 개발자는 성별이나 연령과 같은 관심 속성을 지정할 수 있으며, SageMaker Clarify는 알고리즘 세트를 실행하여 해당 속성에 편향이 있는지를 감지합니다. 알고리즘이 실행된 후 SageMaker Clarify는 잠재적 편향의 가능한 원인 및 관련 측정값에 대한 설명이 포함된 시각적 보고서를 제공해주므로 사용자는 편향을 해결하기 위한 단계를 식별할 수 있습니다. 다른 연령대에 비해 특정 연령대에 대해서는 사업자 대출 사례가 몇 건밖에 없는 금융 데이터세트를 예로 들면, SageMaker는 여기에 불균형 플래그를 지정하여 모델이 해당 연령대에 불리하게 작동하는 상황을 방지할 수 있도록 합니다. 예측을 검토하고 해당 ML 모델의 편향을 지속적으로 모니터링하여 이미 훈련된 모델의 편향을 확인할 수도 있습니다. 마지막으로 SageMaker Clarify는 Amazon SageMaker AI Experiments와 통합되어 모델의 전반적인 예측 생성 프로세스에 가장 많이 기여한 기능을 설명하는 그래프를 제공합니다. 이 정보는 설명 가능성 성과를 충족하는 데 유용할 수 있으며, 특정 모델 입력이 전반적인 모델 동작에서 원래보다 더 많은 영향을 주는지 확인하는 데 도움이 될 수 있습니다.

Amazon SageMaker Model Card

Amazon SageMaker Model Card를 사용하면 거버넌스 및 보고 목적으로 기계 학습(ML) 모델에 대한 중요한 세부 정보를 문서화할 수 있습니다. 이러한 세부 정보에는 모델 소유자, 범용, 의도한 사용 사례, 가정, 모델의 위험 등급, 훈련 세부 정보 및 지표, 평가 결과가 포함될 수 있습니다. 자세한 내용은 AWS 인공 지능 및 Machine Learning 솔루션을 사용한 모델 설명 가능성(AWS 백서)을 참조하세요.

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler는 데이터 준비 및 특성 엔지니어링 프로세스를 간소화하는 데 도움이 되는 기계 학습 도구입니다. 데이터 과학자와 기계 학습 엔지니어가 기계 학습 모델에 사용할 데이터를 빠르고 쉽게 준비하고 변환할 수 있는 시각적 인터페이스를 제공합니다. Data Wrangler를 사용하면 Amazon S3, Amazon Redshift, Amazon Athena와 같은 다양한 소스에서 데이터를 가져올 수 있습니다. 그런 다음 코드를 작성하지 않고도 300개가 넘는 기본 제공 데이터 변환을 사용하여 기능을 정리, 정규화 및 결합할 수 있습니다.

Data Wrangler는 AWS PRA의 데이터 준비 및 기능 엔지니어링 프로세스의 일부로 사용할 수 있습니다. 를 사용하여 저장 및 전송 중 데이터 암호화 AWS KMS를 지원하고 IAM 역할 및 정책을 사용하여 데이터 및 리소스에 대한 액세스를 제어합니다. AWS Glue 또는 Amazon SageMaker 특성 저장소를 통한 데이터 마스킹을 지원합니다. Data Wrangler를와 통합하면 세분화된 데이터 액세스 제어 및 권한을 적용할 AWS Lake Formation수 있습니다. Amazon Comprehend와 함께 Data Wrangler를 사용하여 광범위한 ML Ops 워크플로의 일부로 테이블 형식 데이터에서 개인 데이터를 자동으로 수정할 수도 있습니다. 자세한 내용은 Amazon SageMaker Data Wrangler를 사용하여 기계 학습을 위한 PII 자동 수정(AWS 블로그 게시물)을 참조하세요.

Data Wrangler의 다재다능한 기능은 계정 번호, 신용 카드 번호, 주민등록번호, 환자 이름, 의료 및 군사 기록 등 많은 산업에 민감한 데이터를 마스킹하는 데 도움이 됩니다. 민감한 데이터에 대한 액세스를 제한하거나 수정하도록 선택할 수 있습니다.

AWS 데이터 수명 주기를 관리하는 데 도움이 되는 기능

개인 데이터가 더 이상 필요하지 않은 경우 많은 데이터 저장소의 데이터에 대해 수명 주기 및 유지 시간 정책을 사용할 수 있습니다. 데이터 보존 정책을 구성할 경우 개인 데이터가 포함될 수 있는 다음 위치를 고려합니다.

- Amazon DynamoDB 및 Amazon Relational Database Service(Amazon RDS)와 같은 데이터베이스
- Amazon S3 버킷
- CloudWatch 및 CloudTrail의 로그
- AWS Database Migration Service (AWS DMS) 및 AWS Glue DataBrew 프로젝트의 마이그레이션에서 캐시된 데이터
- 백업 및 스냅샷

다음 AWS 서비스 및 기능은 AWS 환경에서 데이터 보존 정책을 구성하는 데 도움이 될 수 있습니다.

- Amazon S3 수명 주기 - Amazon S3가 객체 그룹에 적용하는 작업을 정의하는 일련의 규칙. Amazon S3 수명 주기 구성에서 사용자를 대신해 Amazon S3가 만료된 객체를 삭제하는 시점을 정의하는 만료 작업을 생성할 수 있습니다. 자세한 내용은 스토리지 수명 주기 관리를 참조하세요.
- Amazon Data Lifecycle Manager - Amazon EC2에서 Amazon Elastic Block Store(Amazon EBS) 스냅샷 및 EBS 지원 Amazon Machine Image(AMI)의 생성, 보존 및 삭제를 자동화하는 정책을 생성합니다.
- Amazon DynamoDB 유지 시간(TTL) - 항목이 더 이상 필요하지 않은 시점을 결정하는 항목별 타임스탬프를 정의합니다. 지정된 타임스탬프 날짜 및 시간이 지나면 바로 DynamoDB는 테이블에서 항목을 삭제합니다.

- CloudWatch Logs의 로그 보존 설정 - 각 로그 그룹의 보존 정책을 1일에서 10년 사이의 값으로 조정할 수 있습니다.
- AWS Backup - 데이터 보호 정책을 중앙에서 배포하여 S3 버킷, RDS 데이터베이스 인스턴스, DynamoDB 테이블, EBS 볼륨 등 다양한 AWS 리소스에서 백업 활동을 구성, 관리 및 관리합니다. AWS 리소스 유형을 지정하여 리소스에 백업 정책을 적용하거나 기존 리소스 태그를 기반으로를 적용하여 추가 세부 수준을 제공합니다. 중앙 집중식 콘솔에서 백업 활동을 감사하고 보고하여 백업 규정 준수 요구 사항을 충족할 수 있습니다.

AWS 서비스 및 데이터를 세그먼트화하는 데 도움이 되는 기능

데이터 세분화는 별도의 컨테이너에 데이터를 저장하는 프로세스입니다. 이를 통해 각 데이터세트에 차별화된 보안 및 인증 조치를 제공하고 전체 데이터세트에 대한 노출의 영향 범위를 줄일 수 있습니다. 예를 들어 모든 고객 데이터를 하나의 대규모 데이터베이스에 저장하는 대신 이 데이터를 더 작고 관리 가능한 그룹으로 세분화할 수 있습니다.

물리적 및 논리적 분리를 사용하여 개인 데이터를 세분화할 수 있습니다.

- 물리적 분리 - 데이터를 별도의 데이터 저장소에 저장하거나 데이터를 별도의 AWS 리소스에 배포하는 작업. 데이터가 물리적으로 분리되어 있지만 동일한 위탁자가 두 리소스에 모두 액세스할 수 있습니다. 따라서 물리적 분리와 논리적 분리를 결합하는 것이 좋습니다.
- 논리적 분리 - 액세스 제어를 사용하여 데이터를 격리하는 작업. 직무에 따라 개인 데이터의 하위 세트에 대한 다양한 수준의 액세스가 필요합니다. 논리적 분리를 구현하는 정책 샘플은 이 가이드의 Amazon DynamoDB의 특정 속성에 대한 액세스 권한 부여 섹션을 참조하세요.

논리적 및 물리적 분리의 조합은 직무 전반의 차별화된 액세스를 지원하기 위해 ID 기반 및 리소스 기반 정책을 작성할 때 유연성, 단순성 및 세분성을 제공합니다. 예를 들어 단일 S3 버킷에서 서로 다른 데이터 분류를 논리적으로 분리하는 정책을 생성하는 방법은 운영상 복잡할 수 있습니다. 각 데이터 분류에 전용 S3 버킷을 사용하면 정책 구성 및 관리가 단순해집니다.

AWS 서비스 데이터 검색, 분류 또는 카탈로그 작성에 도움이 되는 및 기능

일부 조직에서는 환경에서 추출, 적재, 변환(ELT) 도구를 사용하여 데이터의 선제적 카탈로그 작성을 시작하지 않았습니다. 이러한 고객은 초기 데이터 검색 단계에 있을 수 있습니다.이 단계에서는 고객이 저장하고 처리하는 데이터와 그 구조 및 분류 AWS 방식을 더 잘 이해하고 싶을 수 있습니다. Amazon Macie를 사용하여 Amazon S3에서 PII 데이터를 더 잘 이해할 수 있습니다. 그러나 Amazon Macie는 Amazon Relational Database Service(Amazon RDS) 및 Amazon Redshift와 같은 다른 데이터 소스를

분석하는 데 도움을 줄 수 없습니다. 더 큰 데이터 매핑 연습을 시작할 때 두 가지 접근 방식을 사용하여 초기 검색을 가속화할 수 있습니다.

- 수동 접근 방식 - 두 개의 열과 필요한 만큼의 행으로 테이블을 만듭니다. 첫 번째 열에서는 네트워크 패킷의 헤더 또는 본문이나 사용자가 제공하는 서비스에 존재할 수 있는 데이터 특성(예: 사용자 이름, 주소 또는 성별)을 작성합니다. 규정 준수 팀에 두 번째 열을 작성하도록 요청합니다. 두 번째 열에서는 데이터가 개인 데이터로 간주되는 경우 '예'를 입력하고 그렇지 않은 경우 '아니요'를 입력합니다. 종파 또는 의료 데이터와 같이 특히 민감한 정보로 간주되는 모든 유형의 개인 데이터를 표시합니다.
- 자동화된 접근 방식 - AWS Marketplace를 통해 제공되는 도구를 사용합니다. 이러한 도구 중 하나가 Securiti입니다. 이러한 솔루션은 다른 클라우드 서비스 플랫폼의 자산뿐만 아니라 여러 AWS 리소스 유형의 데이터를 스캔하고 검색할 수 있는 통합을 제공합니다. 이러한 동일한 솔루션 중 상당수는 중앙 집중식 데이터 카탈로그에서 데이터 자산 및 데이터 처리 활동의 인벤토리를 지속적으로 수집하고 유지 관리할 수 있습니다. 도구를 사용하여 자동화된 분류를 수행하는 경우 조직의 개인 데이터 정의에 맞게 검색 및 분류 규칙을 조정해야 할 수도 있습니다.

개인 정보 보호 관련 정책 샘플

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

민감한 데이터를 처리하는 많은 조직은 감지 및 대응적 제어 계층을 전체적으로 구현하여 예방 중심의 접근 방식을 취합니다. 이 섹션에서는 AWS Identity and Access Management (IAM), AWS Organizations및 AWS Key Management Service ()에 대한 개인 정보 보호 관련 정책의 예를 제공합니다AWS KMS. 이러한 정책은 예방 접근 방식을 사용하여 조직이 다양한 사용, 공개 제한 사항 및 국가 간 데이터 전송 개인 정보 보호 목표를 충족하는 데 도움이 될 수 있습니다. 이러한 다수의 정책은 이 가이드의 이전 섹션에서 언급됩니다.

이 섹션에는 다음 정책 샘플이 포함되어 있습니다.

- 특정 IP 주소의 액세스 필요
- VPC 리소스에 액세스하려면 조직 멤버십 필요
- 간 데이터 전송 제한 AWS 리전
- Amazon DynamoDB의 특정 속성에 대한 액세스 권한 부여
- VPC 구성에 대한 변경 제한
- AWS KMS 키를 사용하려면 증명이 필요합니다.

특정 IP 주소의 액세스 필요

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

이 정책은 `192.0.2.0/24` 또는 `203.0.113.0/24` 범위의 IP 주소에서 통화가 수신되는 경우에만 `john_stiles` 사용자가 IAM 역할을 수임하도록 허용합니다. 이 정책은 개인 데이터의 의도하지 않은 공개와 원치 않는 국가 간 데이터 전송을 방지하는 데 도움이 됩니다. 예를 들어 조직에 개인 데이터에

액세스해야 하는 고객 지원 직원이 있는 경우 해당 지원 직원이 특정의 하위 집합에 있는 사무실에서만 해당 데이터에 액세스하도록 할 수 있습니다 AWS 리전. 또한 일부 정책에는 특정 사용자 또는 IP 주소에 대한 액세스를 제한하는 Condition 또는 Principal 섹션이 필요할 수 있으므로 조직의 PII 정의를 확인합니다.

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

VPC 리소스에 액세스하려면 조직 멤버십 필요

설문 조사

여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

이 VPC 엔드포인트 정책은 o-1abcde123 조직의 AWS Identity and Access Management (IAM) 보안 주체 및 리소스만 Personalize(Amazon S3) 엔드포인트에 액세스할 수 있도록 허용합니다. 이러한 예방적 제어는 신뢰 영역을 설정하고 개인 데이터 경계를 정의하는 데 도움이 됩니다. 이 정책이 조직의 개인 정보 보호 및 개인 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 이 가이드의 AWS PrivateLink 섹션을 참조하세요.

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

간 데이터 전송 제한 AWS 리전

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

두 개의 AWS Identity and Access Management (IAM) 역할을 제외하고이 서비스 제어 정책은 eu-west-1 및 AWS 리전 이외의 리전 AWS 서비스에 대한 API 호출을 거부합니다eu-central-1. 이 SCP는 승인되지 않은 리전에서 AWS 스토리지 및 처리 서비스가 생성되는 것을 방지하는 데 도움이 될 수 있습니다. 이렇게 하면 해당 리전 AWS 서비스 에서가 개인 데이터를 처리하는 것을 방지할 수 있습니다. 이 정책은 IAM과 같은 글로벌 및 AWS 서비스 AWS Key Management Service (AWS KMS) 및 Amazon CloudFront와 같은 글로벌 서비스와 통합되는 서비스를 고려하기 때문에 NotAction 파라미

터를 사용합니다. 파라미터 값에서 이러한 글로벌 및 기타 적용되지 않는 서비스를 예외로 지정할 수 있습니다. 이 정책이 조직의 개인 정보 보호 및 개인 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 이 가이드의 AWS Organizations 섹션을 참조하세요.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Amazon DynamoDB의 특정 속성에 대한 액세스 권한 부여

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

조직에서 개인 데이터를 물리적 및 논리적으로 분리하는 전략을 논의할 때 AWS Identity and Access Management (IAM)에서 세분화된 액세스 제어 정책을 지원하는 AWS 스토리지 서비스를 고려합니다. 다음 ID 기반 정책은 `Users`라는 Amazon DynamoDB 테이블에서 `UserID`, `SignUpTime` 및 `LastLoggedIn` 속성만 검색할 수 있도록 허용합니다. 예를 들어 이 역할에 전체 개인 데이터세트에

대한 액세스 권한을 부여하는 대신 이 정책을 고객 지원 역할에 연결할 수 있습니다. 이 정책이 조직의 개인 정보 보호 및 개인 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 이 가이드의 AWS 서비스 및 데이터를 세그먼트화하는 데 도움이 되는 기능 섹션을 참조하세요.

```
{
   "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"
               ]
            }
         }
      }
   ]
}
```

VPC 구성에 대한 변경 제한

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

네트워크 데이터 흐름을 포함하는 국가 간 데이터 전송 요구 사항을 지원하는 AWS 인프라를 설계하고 배포한 후에는 수정을 방지할 수 있습니다. 다음 서비스 제어 정책은 VPC 구성 드리프트 또는 의도하지 않은 수정을 방지하는 데 도움이 됩니다. 새 인터넷 게이트웨이 연결, VPC 피어링 연결, Transit Gateway Attachment 및 새 VPN 연결을 거부합니다. 이 정책이 조직의 개인 정보 보호 및 개인 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 이 가이드의 AWS Transit Gateway 섹션을 참조하세요.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

AWS KMS 키를 사용하려면 증명이 필요합니다.

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

다음 AWS Key Management Service (AWS KMS) 키 정책은 요청의 엔클레이브 증명 문서가 조건문의 측정값과 일치하는 경우에만 AWS Nitro Enclave 인스턴스가 KMS 키를 사용하도록 허용합니다. 이 정책은 신뢰할 수 있는 엔클레이브만 데이터를 해독하도록 허용합니다. 이 정책이 조직의 개인 정보 보호 및 개인 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 이 가이드의 AWS Nitro Enclaves 섹션을 참조하세요. 키 정책 및 AWS Identity and Access Management (IAM) 정책에 사용할 수 있는 조건 키의 AWS KMS 전체 목록은 조건 키를 참조하세요 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
            }
         }
      }
   ]
}
```

글로벌 확장을 위한 전략 수립

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주십시오.

AWS Security Assurance Services는 전 세계로 확장할 AWS 때의 개인 정보 보호 설계와 관련된 질문을 자주 받습니다. 질문은 추가 비용 및 운영 오버헤드를 피하면서 데이터 주권 의무 또는 고객 계약과 같은 고유한 개인 정보 보호 요구 사항의 준수와 관련된 사안에 기반합니다. 설계 고려 사항에는 종종 데이터 레지던시, 운영자 액세스 제한, 복원력 및 지속 가능성, 전반적인 독립성이 포함됩니다. 자세한 내용은 의 디지털 주권 요구 사항 충족 AWS(AWS re:Invent 2022 프레젠테이션)을 참조하세요.

다음은 일반적인 질문으로, 사용자만 사용 사례에 맞게 답할 수 있습니다.

- 고객의 개인 데이터는 어디에 상주해야 하나요?
- 고객 데이터는 어디에 저장되나요?
- 개인 데이터가 국경을 넘어갈 수 있는 경우와 그 방법은 무엇인가요?
- 여러 리전에서 데이터에 대한 인적 액세스 또는 서비스 액세스에 전송이 포함되나요?
- 고객의 개인 데이터에 액세스하는 외국 정부가 없는지 확인하려면 어떻게 해야 하나요?
- 백업과 핫 사이트 또는 콜드 사이트를 어디에 저장할 수 있나요?
- 데이터를 로컬로 유지하려면 서비스를 제공하는 모든 리전에서 AWS 랜딩 존을 유지해야 합니까? 아니면 기존 AWS Control Tower 랜딩 존을 사용할 수 있나요?

데이터 레지던시 요구 사항의 경우 여러 조직에서 적합한 아키텍처 배포가 서로 다를 수 있습니다. 일부 조직에는 고객의 개인 데이터가 특정 리전 내에 있어야 하는 요구 사항이 있을 수 있습니다. 이 경우 이러한 의무 사항을 지키면서 일반적으로 규정을 준수하는 방법에 대해 걱정할 수 있습니다. 상황에 관계없이 다중 계정 배포 전략을 선택할 경우 여러 고려 사항이 있습니다.

주요 아키텍처 설계 구성 요소를 정의하려면 규정 준수 및 계약 팀과 긴밀히 협력하여 개인 데이터가 AWS 리전을 통과할 수 있는 위치, 시기 및 방법에 대한 요구 사항을 확인합니다. 이동, 복사 또는 보기와 같이 데이터 전송에 적합한 항목을 결정합니다. 또한 구현해야 하는 특정 복원력 및 데이터 보호 제어가 있는지 이해합니다. 백업 및 재해 복구 전략에 교차 리전 장애 조치가 필요하나요? 그렇다면 백업 데이터를 저장하는 데 사용할 수 있는 리전을 결정합니다. 키 생성을 위한 특정 암호화 알고리즘 또는

전용 하드웨어 보안 모듈과 같은 데이터 암호화에 대한 요구 사항이 있는지 확인합니다. 이러한 주제에서 규정 준수 이해관계자와 조율한 후 다중 계정 환경의 설계 접근 방식을 고려하기 시작합니다.

다음은 인프라 분리의 오름차순으로 AWS 다중 계정 전략을 계획하는 데 사용할 수 있는 세 가지 접근 방식입니다.

- 관리형 리전이 있는 중앙 랜딩 존
- 리전별 랜딩 존
- AWS European Sovereign Cloud

또한 개인 정보 보호 규정 준수는 데이터 주권에서만 그치지 않는다는 점을 명심해야 합니다. 이 가이드의 나머지 부분을 검토하여 동의 관리, 데이터 주체 요청, 데이터 거버넌스, AI 편향과 같은 다른 여러 문제에 대한 가능한 솔루션을 파악합니다.

관리형 리전이 있는 중앙 랜딩 존

전역적으로 확장하고 싶지만에서 이미 다중 계정 아키텍처를 설정한 경우 동일한 다중 계정 랜딩 존(MALZ)을 사용하여 추가를 관리하는 AWS것이 일반적입니다 AWS 리전. 이 구성에서는 로깅, 계정 팩토리, 기존 AWS Control Tower 랜딩 존의 일반 관리와 같은 인프라 서비스를 생성한 리전에서 계속 운영합니다.

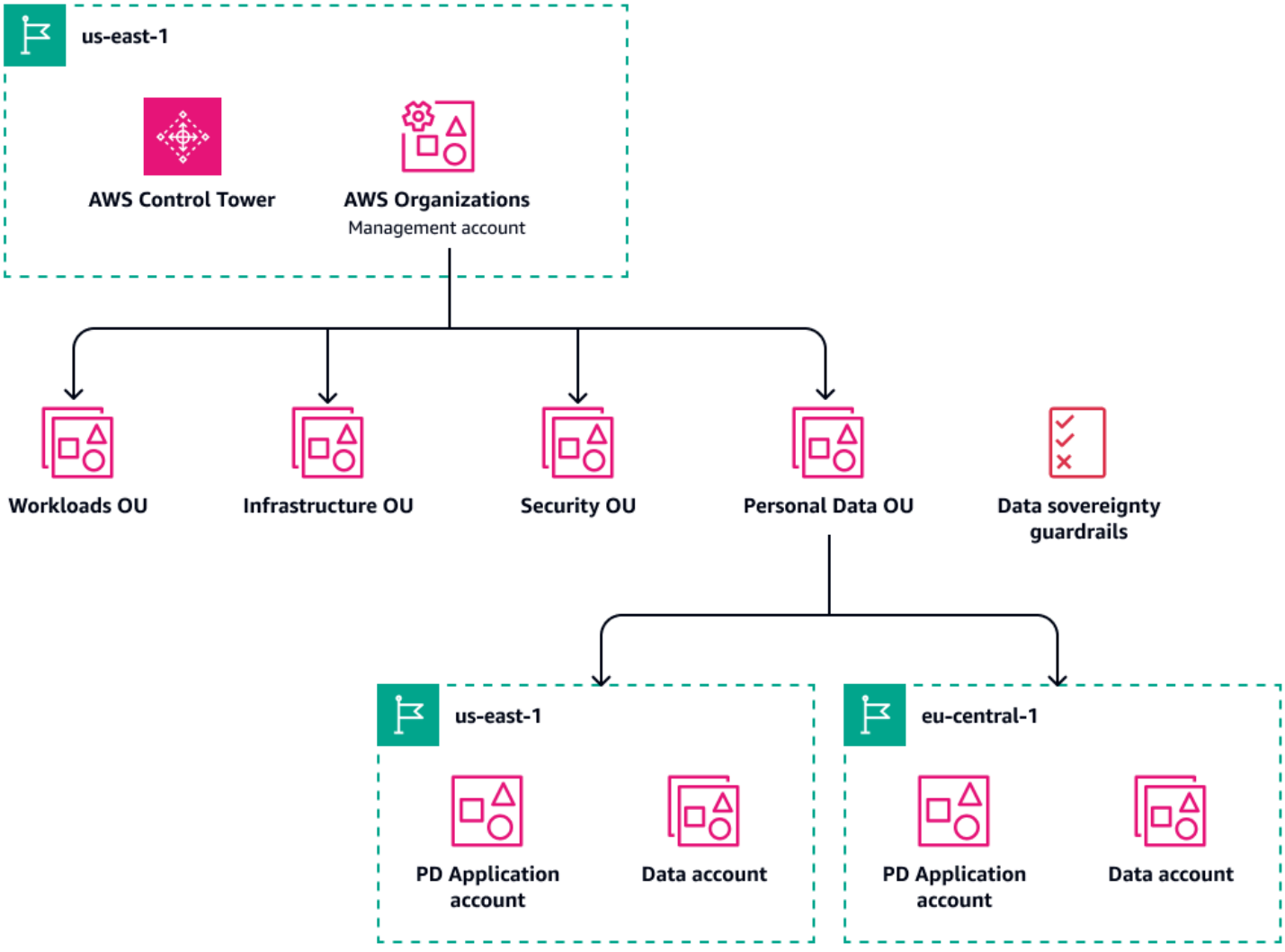
프로덕션 워크로드의 경우 AWS Control Tower 랜딩 존을 새 리전으로 확장하여 리전 배포를 운영할 수 있습니다. 이렇게 하면 AWS Control Tower 거버넌스를 새 리전으로 확장할 수 있습니다. 이렇게 하면 특정 관리형 리전 내에 개인 데이터 스토어를 유지할 수 있으며, 데이터는 여전히 인프라 서비스 및 AWS Control Tower 거버넌스의 이점을 활용하는 계정에 상주합니다. 에서 개인 데이터가 포함된 AWS Organizations계정은의 모든 데이터 주권 가드레일이 구현되는 전용 개인 데이터 OU 아래에 계속 롤업 AWS Control Tower 됩니다. 또한 리전별 워크로드는 여러 리전에서 동일한 워크로드를 포함할 수 있는 프로덕션 계정을 설정하는 대신 전용 계정에 포함됩니다.

이 배포는 가장 비용 효율적일 수 있지만, AWS 계정 및 리전 경계를 넘어 개인 데이터의 흐름을 제어하려면 추가 고려 사항이 필요합니다. 다음을 고려하세요.

- 로그에는 개인 데이터가 포함될 수 있으므로 집계 중에 교차 리전 전송을 방지하기 위해 민감한 필드를 포함하거나 수정하려면 일부 추가 구성이 필요할 수 있습니다. 여러 리전에서 로그 집계를 제어하는 방법에 대한 자세한 내용과 권장 사례는 이 가이드의 중앙 집중식 로그 스토리지 섹션을 참조하세요.

- AWS Transit Gateway 설계에서 VPCs 격리 및 적절한 양방향 네트워크 트래픽 흐름을 고려합니다. 허용 및 승인되는 Transit Gateway Attachment를 제한할 수 있으며 VPC 라우팅 테이블을 변경할 수 있는 사용자 또는 대상을 제한할 수 있습니다.
- 클라우드 운영 팀의 멤버가 개인 데이터에 액세스하지 못하도록 해야 할 수 있습니다. 예를 들어 고객 트랜잭션 데이터가 포함된 애플리케이션 로그는 다른 로그 소스보다 민감도가 높은 것으로 간주될 수 있습니다. 역할 기반 액세스 제어 및 속성 기반 액세스 제어와 같은 추가 승인 및 기술 가드레일이 필요할 수 있습니다. 또한 데이터에 액세스할 때 레지던시 제한 사항이 적용될 수 있습니다. 예를 들어 한 리전 A의 데이터는 해당 리전 내에서만 액세스할 수 있습니다.

다음 다이어그램에서는 리전 배포가 있는 중앙 집중식 랜딩 존을 보여줍니다.



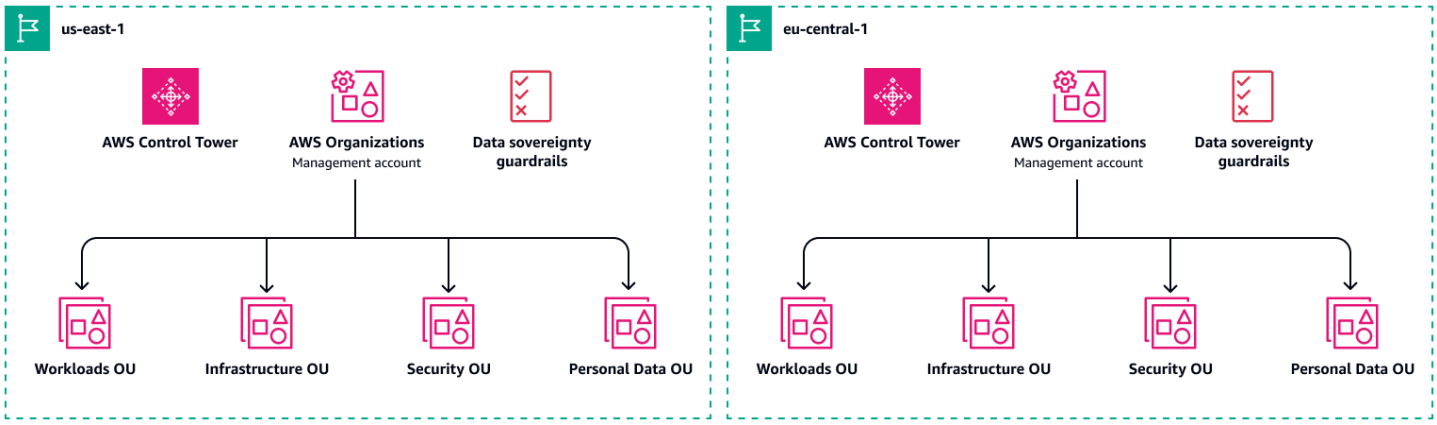
리전별 랜딩 존

MALZ가 두 개 이상 있으면 중요하지 않은 워크로드에 비해 개인 데이터를 처리하는 워크로드를 완전히 격리하여 더 엄격한 규정 준수 요구 사항을 달성하는 데 도움이 될 수 있습니다. AWS Control Tower 중앙 집중식 로깅 집계는 기본적으로 구성하여 간소화할 수 있습니다. 이 접근 방식을 사용하면 수정이 필요한 별도의 로그 스트림으로 로깅하기 위해 예외를 유지 관리할 필요가 없습니다. 운영자 액세스를 로컬 레지던시로 제한하는 각 MALZ에 대한 로컬 및 전용 클라우드 운영 팀이 있을 수도 있습니다.

많은 조직에 별도의 미국 및 EU 기반 랜딩 존 배포가 있습니다. 각 리전의 랜딩 존에는 리전의 계정에 대한 하나의 포괄적인 보안 태세와 관련 거버넌스가 있습니다. 예를 들어 전용 HSM을 사용하는 개인 데이터 암호화는 하나의 MALZ에 있는 워크로드에서 필요하지 않을 수 있지만 다른 MALZ에는 필요할 수 있습니다.

이 전략은 현재와 미래의 여러 요구 사항을 충족하도록 확장할 수 있지만 여러 MALZ 유지 관리와 관련된 추가 비용과 운영 오버헤드를 이해하는 것이 중요합니다. 자세한 내용은 AWS Control Tower 요금을 참조하십시오.

다음 다이어그램에서는 두 리전에 있는 별도의 랜딩 존을 보여줍니다.



AWS European Sovereign Cloud

일부 조직에서는 유럽 경제 지역(EEA)에서 운영하는 워크로드와 다른 지역에서 운영하는 워크로드를 철저히 분리해야 합니다. 이러한 상황에서는 AWS European Sovereign Cloud를 고려합니다. AWS European Sovereign Cloud는 유럽을 위한 새로운 독립 클라우드로, 고객이 엄격한 데이터 레지던시, 운영 자율성 및 복원력 요구 사항을 포함하여 리전의 진화하는 주권 요구 사항을 충족할 수 있도록 설계되었습니다.

AWS European Sovereign Cloud는 기존와 물리적 및 논리적으로 분리되는 동시에 동일한 보안 AWS 리전, 가용성 및 성능을 제공합니다. EU에 위치한 AWS 직원만 AWS 유럽 서버린 클라우드에 대한

운영 및 지원을 제어할 수 있습니다. 엄격한 데이터 레지던시 요구 사항이 있는 경우 AWS European Sovereign Cloud는 사용자가 생성하는 모든 메타데이터(예: 실행하는 데 사용하는 역할, 권한, 리소스 레이블 및 구성 AWS)를 EU에 보관합니다. AWS European Sovereign Cloud에는 자체 결제 및 사용량 측정 시스템도 있습니다.

이 접근 방식의 경우 이전 섹션인 리전 랜딩 존과 유사한 패턴을 사용합니다. 그러나 유럽 고객에게 제공하는 서비스의 경우 AWS European Sovereign Cloud에 전용 MALZ를 배포할 수 있습니다.

리소스

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주세요.

AWS 권장 가이드

- AWS Security Reference ArchitectureAWS(SRA)

AWS 설명서

- Data protection(AWS Well-Architected Framework)
- Data classification(AWS 백서)
- Amazon Web Services: 위험 및 규정 준수(AWS 백서)
- Hybrid architectures to address personal data processing requirements(AWS 백서)
- AWS에서 GDPR 규정 준수 탐색(AWS 백서)
- Building a data perimeter on AWS(AWS 백서)
- AWS 보안 설명서

기타 AWS 리소스

- AWS 규정 준수 프로그램
- AWS 공동 책임 모델
- 데이터 프라이버시 FAQ
- AWS Security Assurance Services
- AWS Digital Sovereignty Pledge: Control without compromise(AWS 블로그 게시물)
- AWS 보안 학습

기여자

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주세요.

이 가이드는 AWS Security Assurance Services 팀에서 작성했습니다. 이 가이드의 권장 사항을 구현하고 워크로드를 운영하도록 지원하려면 AWS Security Assurance Services 팀에 문의하세요.

주요 작성자

- Amber Welch, AWS Senior Privacy Consultant
- Daniel Nieters, AWS Principal Privacy Consultant
- Robert Carter, AWS Technical Program Manager

기여자

- Avik Mukherjee, AWS Senior Security Consultant
- David Bounds, AWS Senior Solutions Architect
- Jeff Lombardo, AWS Senior Security Solutions Architect
- Ram Ramani, AWS Principal Security Solutions Architect
- Vanessa Jacobs, AWS Senior Security Consultant
- Thomas Nicholson, AWS Senior Privacy Consultant
- Jose DeJesus, AWS Senior Assurance Consultant
- Doug Pardue, AWS Solutions Architect Manager

기술 작성자

- Lilly AbouHarb, AWS Senior Technical Writer

문서 기록

> **설문 조사**
>
> 여러분의 의견을 듣고 싶습니다. 간단한 설문 조사에 참여하여 AWS PRA에 대한 피드백을 제공해 주세요.

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
중요한 업데이트	AWS Artifact 섹션에 클라우드 컴퓨팅 규정 준수 제어 카탈로그(C5)를 추가했습니다. 로그 아카이브 계정에 Amazon Security Lake를 추가했습니다. PD 애플리케이션 계정에 Amazon Bedrock, AWS Clean Rooms, Amazon DataZone, AWS Lake Formation, Amazon SageMaker AI 그리고 카탈로그 데이터를 검색, 분류 또는 카탈로그화하는 데 도움이 되는 AWS 서비스 및 기능을 추가했습니다. 글로벌 확장을 위한 전략 수립 섹션을 추가했습니다.	2025년 9월 16일
중요한 업데이트	전반적으로 중요한 업데이트를 수행했습니다.	2024년 3월 26일
최초 게시	—	2023년 10월 2일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 에디션으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 Amazon Relational Database Service(Amazon RDS) for Oracle로 마이그레이션합니다.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com으로 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드클라우드의 EC2 인스턴스에 있는 Oracle로 마이그레이션합니다.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

속성 기반 액세스 제어를 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리성, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 액티브 패시브 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로 `SUM` 및 `MAX`가 있습니다.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 운영을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용하도록 허용하는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 탐색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 용 ABAC AWS를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환 AWS 하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹사이트와 AWS CAF 백서를 참조하세요.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

악성 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 직접 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

동일하지만 별개의 두 환경을 생성하는 배포 전략입니다. 하나의 환경(파란색)에서 현재 애플리케이션 버전을 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 신속하게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 태스크를 실행하고 인적 활동이나 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같이 유용하거나 이로운 봇도 있습니다. 악성 봇이라고 하는 다른 일부 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

봇넷

맬웨어에 감염되고 봇 허더 또는 봇 운영자와 같은 단일 당사자가 제어하는 봇 네트워크입니다. 봇넷은 봇의 규모와 봇의 영향 범위를 확대하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 About branches(GitHub 설명서)를 참조하십시오.

긴급 액세스 권한

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 AWS Well-Architected 지침의 Implement break-glass procedures 지표를 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

AWS Cloud Adoption Framework를 참조하세요.

카나리 배포

최종 사용자에게 제공하는 느린 증분 릴리스 버전입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

클라우드 혁신 센터를 참조하세요.

CDC

데이터 캡처 변경을 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애나 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전송을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술에 연결되어 있습니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 AWS 클라우드로 마이그레이션할 때 일반적으로 거치는 4단계는 다음과 같습니다.

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 – 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리로 GitHub 또는 Bitbucket Cloud가 포함됩니다. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상되는 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며, 이는 일반적으로 점진적이고 의도되지 않은 작업입니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 탐색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 탈중앙화된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 보통 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터 정의 언어를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 제어를 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 AWS에서 보안 제어 구현의 탐지 제어를 참조하세요.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블을 말합니다. 차원 테이블 속성은 일반적으로 텍스트 필드나 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 보통 쿼리 제약, 필터링 및 결과 세트 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간 및 데이터 손실을 최소화하기 위해 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준이 되는 구성과의 편차 추적을 말합니다. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 가치 흐름 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 엣지 컴퓨팅은 클라우드 컴퓨팅에 비해 보다 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간 비즈니스 문서의 자동화된 교환을 나타냅니다. 자세한 내용은 전자 데이터 교환(EDI)이란 무엇인가요?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

스타 스키마의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블은 측정값이 있는 열 및 차원 테이블에 대한 외래 키가 있는 열과 같이 두 가지 열 유형을 포함합니다.

빠른 실패

개발 수명 주기를 줄이기 위해 빈번한 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 핵심입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용

할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

퓨샷 프롬프팅

유사한 태스크를 수행하도록 요청하기 전에 LLM에 태스크와 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 모델이 프롬프트에 포함된 예제(샷)에서 학습하는 컨텍스트 내 학습을 적용합니다. 퓨샷 프롬프팅은 특정 형식 지정, 추론 또는 분야별 지식이 필요한 태스크에 효과적일 수 있습니다. 제로샷 프롬프팅도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 지속적 데이터 복제를 사용하여 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화되고 레이블이 지정되지 않은 데이터의 대규모 데이터세트에서 훈련된 대규모 딥 러닝 신경망입니다. FM은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 태스크를 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란?을 참조하세요.

G

생성형 AI

대량의 데이터에서 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트, 오디오와 같은 새 콘텐츠와 아티팩트를 생성할 수 있는 AI 모델의 하위 세트입니다. 자세한 내용은 생성형 AI란 무엇인가요?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 선호되는 현대적 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 해당 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조 분야에서는 골든 이미지를 사용하여 여러 디바이스에서 소프트웨어를 프로비저닝할 수 있으며 이를 통해 딥이스 제조 작업의 속도, 확장성 및 생산성을 개선할 수 있습니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub CSPM, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터세트에서 보류되는 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교해 모델 성능을 평가할 수 있습니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

I

IaC

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하세요.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드에 대한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용하여 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 나타내기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷(IoT) 디지털 트랜스포메이션 전략 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(ITIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(ITSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터에서 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문에 대한 답변, 문서 요약, 텍스트를 다른 언어로 번역, 문장 완성과 같은 여러 태스크를 수행할 수 있습니다. 자세한 내용은 대규모 언어 모델(LLM)이란 무엇인가요?를 참조하세요.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 프라이버시를 위협하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 방해하거나 민감한 정보를 유출하거나 무단 액세스 권한을 확보할 수 있습니다. 맬웨어의 예로 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하고, 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로 Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB가 있습니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원자재를 생산 현장에서 완제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

Migration Acceleration Program을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 조정을 위해 결과를 검사하는 전체 프로세스입니다. 메커니즘은 작동 시 자체적으로 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 큐 원격 분석 전송(MQTT)

리소스 제약이 있는 IoT 디바이스에 대한 게시 및 구독 패턴을 기반으로 하는 경량 Machine-to-Machine(M2M) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

AWS 클라우드로 마이그레이션하는 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 행동 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 AWS 클라우드로 마이그레이션하는 데 사용되는 접근 방식입니다. 자세한 내용은 이 용어집의 7R 항목과 조직을 동원하여 대규모 마이그레이션 가속화를 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 전략을 참조하세요.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션의 현대화 준비 상태 평가를 참조하세요.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

Migration Portfolio Assessment를 참조하세요.

MQTT

메시지 큐 원격 분석 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드에 대한 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework에서는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

운영 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

Open Process Communications - Unified Architecture(OPC-UA)를 참조하세요.

Open Process Communications - Unified Architecture(OPC-UA)

산업 자동화를 위한 Machine-to-Machine(M2M) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계에 관한 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 잠재적 장애의 범위를 이해, 평가 또는 예방하거나 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 상태 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경에서 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조 분야에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 트랜스포메이션의 주요 중점 사항입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

개인 식별 정보를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한 정의(ID 기반 정책 참조), 액세스 조건 지정(리소스 기반 정책 참조), AWS Organizations 내 조직의 모든 계정에 대한 최대 권한 정의(서비스 제어 정책 참조)와 같은 작업을 수행할 수 있는 객체입니다.

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 저장소를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

보통 `WHERE` 절에 있는 `true` 또는 `false`를 반환하는 쿼리 조건입니다.

푸시다운 조건자

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

개인 정보 보호 중심 설계

전체 개발 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

선제적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 제어를 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도를 거쳐 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리를 나타냅니다.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능 로직 컨트롤러(PLC)

제조 분야에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체이닝

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 태스크를 하위 태스크로 나누거나 예비 응답을 반복적으로 세부 조정하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

여러 마이크로서비스에서 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 명령어와 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RAG

검색 증강 생성을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

리아키텍팅

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 AWS 리전 지정을 참조하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7R을 참조하세요.

릴리스

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 중단을 복구할 수 있는 애플리케이션의 기능입니다. 고가용성 및 재해 복구는 AWS 클라우드에서 복원력을 계획할 때 일반적인 고려 사항입니다. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 AWS에서 보안 제어 구현의 대응 제어를 참조하세요.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 시맨틱 검색을 수행할 수 있습니다. 자세한 내용은 검색 증강 생성(RAG)이란 무엇인가요?를 참조하세요.

교체

공격자가 자격 증명에 액세스하는 것을 더욱 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

목표 복구 시점(RPO)을 참조하세요.

RTO

목표 복구 시간(RTO)을 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

보안 암호

에는 암호화된 형식으로 저장하는 암호 또는 사용자 자격 증명과 같은 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 AWS Secrets Manager 설명서의 Secrets Manager 보안 암호란 무엇인가요?를 참조하세요.

보안 중심 설계

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어는 예방, 감지, 대응, 선제적과 같은 기본적인 네 가지 보안 제어 유형으로 구분됩니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 이를 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동화된 응답 작업의 예로 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

대상에서 데이터를 수신하는 AWS 서비스 에 의한 데이터 암호화.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 지표(SLI)

오류 발생률, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정값입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 목표 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 발생하는 장애입니다.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 지표를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 단계별 접근 방식을 참조하세요.

SPOF

단일 장애점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 더 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스에서 또는 비즈니스 인텔리전스 목적으로 사용하도록 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조 분야에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 진행되는 시스템 테스트입니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 명령 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색, 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

Transit Gateway

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 대한 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 Quantifying uncertainty in deep learning systems 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란?을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에서 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 태스크를 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

Write Once, Read Many(WORM)를 참조하세요.

WQF

AWS Workload Qualification Framework를 참조하세요.

Write Once Read Many(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 여러 번 데이터를 읽을 수 있지만 데이터를 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경 불가능한 항목으로 간주됩니다.

Z

제로데이 익스플로잇

제로데이 취약성을 악용하는 공격(일반적으로 맬웨어)입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프팅

태스크를 수행하기 위해 LLM에 명령을 제공하지만 안내에 도움이 되는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 태스크를 처리해야 합니다. 제로샷 프롬프팅의 효과는 태스크의 복잡성과 프롬프트의 품질에 따라 달라집니다. 퓨샷 프롬프팅도 참조하세요.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.