여러 로 전환 AWS 계정

AWS 권장 가이드

AWS 권장 가이드: 여러 로 전환 AWS 계정

Table of Contents

여러 로 전환 AWS 계정

Amazon Web Services(기여자)

2024년 11월(문서 기록)

많은 기업이 단일 Amazon Web Services(AWS) 계정을 사용하여 여정을 시작합니다. 회사 내 여러 역할이 이 계정을 사용하여 비즈니스를 운영합니다. 엔지니어는 코드를 개발하고, 개발 및 테스트 환경에 배포하고, 프로덕션 변경을 촉진합니다. 제품 관리자는 데이터 소스를 쿼리하여 비즈니스 성과에 대한 인사이트를 수집합니다. 영업 팀은 신규 고객을 유치하기 위해 프로덕션 환경에서 데모를 진행하고 있습니다. 재무 팀은 AWS Billing 콘솔에서 클라우드 지출을 모니터링하고 있습니다.

이러한 모든 개별 역할이 단일 역할을 사용하는 경우 최소 권한 적용이라는 보안 모범 사례를 적용하기 어려울 수 있습니다. 즉 AWS 계정, 작업을 수행하는 데 필요한 최소 권한만 부여해야 합니다. 스타트업 개발의 특정 단계에서 누군가 '모든 엔지니어가 프로덕션에 액세스해야 합니까?'라고 질문할 것입니다. 답은 거의 항상 '아니요'지만 많은 기업들은 비즈니스 속도를 늦추지 않으면서 기존의 단일 계정 환경을 다중 계정 환경으로 전환하는 방법을 고심하고 있습니다.

이 가이드에는 단일 계정 환경에서 다중 계정 환경으로 전환하는 데 도움이 되는 모범 사례가 포함되어 있습니다. 그리고 계정 마이그레이션, 사용자 관리, 네트워킹, 보안 및 아키텍처와 관련하여 내려야 할 결정을 설명합니다. 이 제품은 비즈니스 및 일상 업무를 위해 가동 중지를 방지하거나 최소화하는 데 도움이 되도록 설계되었습니다. 이 가이드는 단일 계정 환경에서 AWS 계정 다중 계정 환경으로 전환할 때 다음 기능에 중점을 둡니다.

- ID 관리 및 액세스 제어
- 권한 및 액세스 관리
- 네트워크 연결
- 보안 인시던트 대응
- 백업
- 계정 마이그레이션
- 리소스 마이그레이션
- 청구 고려 사항

기능에 대한 자세한 내용은 의 Cloud Foundation AWS 섹션을 참조하세요.

이 가이드는 AWS 시작 보안 기준(AWS SSB), 여러 계정을 사용하여 AWS 환경 구성 백서, AWS 보안 참조 아키텍처(AWS SRA) 및 백서 기반 클라우드 기반 구축을 포함하여이 주제와 관련된 기존 리소스

에 맞춰져 있습니다 AWS. 이 가이드에서 다루지 않은 보다 구체적인 지침을 보려면 이들 리소스를 계속 사용해야 합니다.

수강 대상

이 가이드는 여러 AWS 계정으로 전환하기를 원하거나 전환해야 하는 회사에 가장 적합합니다. 스타트업의 경우 이러한 요구는 일반적으로 제품 시장 적합성을 찾고, 자금을 조달하고, 인프라, 개발 운영(DevOps) 또는 보안과 같은 고유한 엔지니어링 분야를 고용하기 시작할 때 발생합니다.

회사가 아직 이러한 전환을 수행할 준비가 되지 않았더라도 이 가이드를 사용하여 전환 중에 내려야 할 결정을 이해하고 준비를 시작할 수 있습니다.

다중 계정 아키텍처로 전환하기 위한 목표

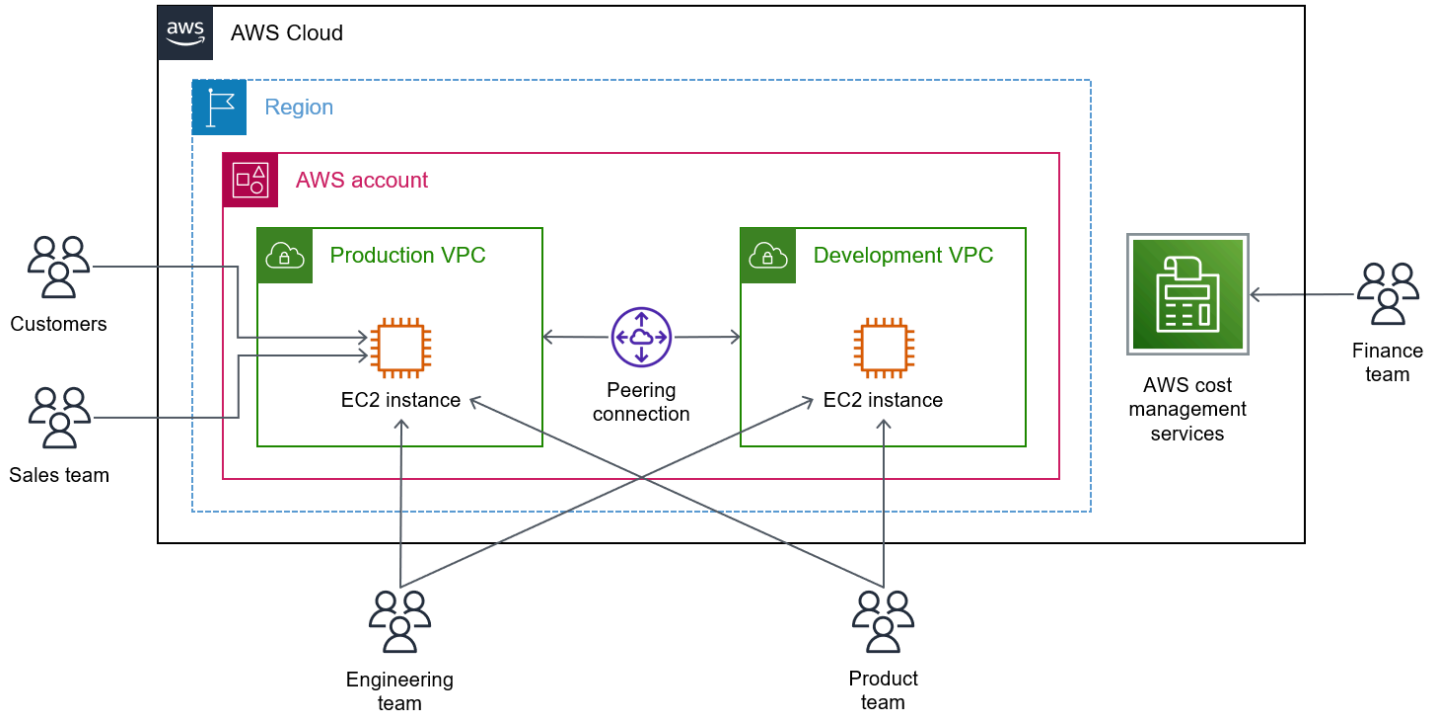
다중 계정 아키텍처로 전환은 일반적으로 다음 이점 중 하나 이상에 대한 비즈니스 요구에 의해 이루어집니다.

- 비즈니스 목적 또는 소유권을 기준으로 워크로드 그룹화
- 환경별로 다른 보안 제어 적용
- 민감한 데이터에 대한 액세스 제한
- 혁신 및 민첩성 증진
- 부작용으로 인한 영향 범위 제한
- 다양한 IT 운영 모델 지원
- 비용 관리
- 할당 AWS 서비스 량 및 API 요청 속도 제한 배포

다중 계정 아키텍처 사용의 다양한 이점에 대한 자세한 내용은 여러 계정을 사용하여 AWS 환경 구성(AWS 백서) 및 잘 설계된 환경을 설정하기 위한 지침(AWS Control Tower 설명서)을 참조하세요.

샘플 단일 계정 아키텍처

우선 스타트업이나 소규모 회사에서는 단일 AWS 리전 을 사용하고 VPC 피어링으로 연결된 2개의 Virtual Private Cloud(VPC)를 보유하는 것이 일반적입니다. 각 VPC에는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 같은 컴퓨팅 리소스가 포함되어 있습니다. 엔지니어링 팀이 직접 개발 VPC에서 코드를 개발하고 제품 팀이 변경 사항을 검토한 후 엔지니어링 팀이 직접 변경 사항을 프로덕션 VPC로 승격합니다. 재무 팀은 AWS 결제 및 비용 관리 콘솔을 검토할 수 AWS 계정 있도록에 액세스할 수 있습니다.



다음은 이 환경에서 기업이 겪을 수 있는 문제의 몇 가지 예입니다.

- 한 엔지니어가 개발 데이터베이스에 액세스하고 있다고 생각하여 실수로 프로덕션 데이터를 삭제했습니다.
- 프로덕션 배포가 예상보다 오래 걸려 영업 데모가 영향을 받았습니다.
- 개발 코드에 대해 부하 테스트를 수행할 때 프로덕션 VPC가 느려지고 제한에 대한 오류 메시지가 생성되었습니다.
- 재무 팀은 프로덕션 환경과 개발 환경에 대한 비용을 구분할 수 없습니다.
- CEO는 새로 고용된 해외 계약업체 중 일부가 프로덕션 VPC를 통해 고객 데이터에 액세스할 수 있다는 점을 우려합니다.
- 재무 팀은 높은 비용이 발생할 수 AWS 서비스 있는 특정에 대한 액세스를 허용할 수 없습니다.

다중 계정 전략을 채택하면 워크로드와 액세스를 구분 AWS 계정 하기 위해 세분화된를 사용하여 이러한 모든 문제를 해결할 수 있습니다.

다중 계정 아키텍처로 전환을 위한 기본 프레임워크 및 보안 책임

이 가이드의 정보와 모범 사례는 인프라 및 보안에 대한 기존 AWS 권장 사항을 보완하도록 설계되었습니다. 단일 AWS 계정 계정에서 여러 계정으로 전환할 때 새로운 다중 계정 아키텍처가 AWS Well-Architected Framework 및 Cloud Foundation 원칙과 일치하는지 확인하는 AWS 계정것이 중요합니다. 이를 통해 거버넌스 요구 사항 및 AWS 모범 사례를 준수하면서 보안, 성능 및 복원력을 위해 설계된 환경을 구축하고 운영할 수 있습니다.

AWS Well-Architected 프레임워크

AWS Well-Architected Framework를 사용하면 애플리케이션 및 워크로드를 위한 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 인프라를 구축할 수 있습니다. 이 가이드는 이 프레임워크의 운영 우수성, 보안 및 신뢰성 원칙에 부합하며, 이를 통해 현재 AWS 권장 사항에 따라 비즈니스 및 규제 요구 사항을 충족할 수 있습니다.

AWS 계정에서 AWS Well-Architected Tool을 사용하여 잘 설계된 모범 사례를 준수하는지 평가할 수 있습니다.

의 Cloud Foundation AWS

(AWS 화이트페이퍼)에서 클라우드 기반 구축 AWS은 비즈니스 요구 사항에 맞게 AWS 환경을 조정하는 데 도움이 되는 지침을 제공합니다. 기능 기반 접근 방식을 사용하여 워크로드를 배포, 운영 및 관리할 환경을 생성할 수 있습니다. 또한 요구 사항이 발전하고 클라우드에 추가 워크로드를 배포함에 따라 환경을 확장하는 기능을 개선할 수 있습니다. 에서 정의한 30가지 기능에 대한 자세한 내용은 기능을 AWS참조하세요. 이 가이드에는 초기 기능을 의도한 순서대로 구현하기 위한 모범 사례가 포함되어 있습니다.

운영 및 거버넌스 요구 사항에 따라 기능을 채택하고 구현할 수 있습니다. 비즈니스 요구 사항이 성숙해지면 기능 기반 접근 방식을 클라우드 환경이 워크로드를 지원하고 필요에 따라 확장할 준비가 되었는지 확인하는 메커니즘으로 사용할 수 있습니다. 이 접근 방식을 사용하면 빌더와 비즈니스를 위한 클라우드 환경을 자신 있게 구축할 수 있습니다.

다중 계정 아키텍처로 전환을 위한 ID 관리 및 액세스 제어

다중 계정 아키텍처로 전환하는 첫 단계는 조직 내에 새 계정 구조를 설정하는 것입니다. 그런 다음 사용자를 추가하고 계정에 대한 액세스를 구성할 수 있습니다. 이 섹션에서는 여러 AWS 계정에 대한 사용자 액세스를 관리하는 접근 방식을 설명합니다.

이 섹션은 다음 작업으로 구성됩니다.

- 조직 설정
- 랜딩 존 생성
- 조직 단위 추가
- 초기 사용자 추가
- 멤버 계정 관리

조직 설정

여러 계정이 있는 경우의 조직을 통해 이러한 계정을 논리적으로 관리할 AWS 계정수 있습니다AWS Organizations. 의 계정 AWS Organizations 은 리소스와 해당 AWS 리소스에 액세스할 수 있는 자격 증명을 AWS 계정 포함하는 표준입니다. 조직은 단일 단위로 관리할 수 AWS 계정 있도록를 통합하는 엔터티입니다.

계정을 사용하여 조직을 생성하면 계정이 조직의 관리 계정(지급인 계정 또는 루트 계정이라고도 함)이 됩니다. 조직에 관리 계정은 하나만 있을 수 있습니다. AWS 계정 조직에 추가하면 멤버 계정이 됩니다.

> **Note**
>
> AWS 계정 또한 각 에는 루트 사용자라는 단일 자격 증명이 있습니다. 계정을 생성할 때 사용한 이메일 주소와 암호를 사용하여 루트 사용자로 로그인할 수 있습니다. 그러나 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않는 것이 좋습니다. 자세한 내용은 AWS 계정 루트 사용자를 참조하세요.
> 또한 멤버 계정에 대한 루트 액세스를 중앙 집중화하고 조직의 멤버 계정에서 루트 사용자 자격 증명을 제거하는 것이 좋습니다.

조직 루트, 조직 단위(OU) 및 멤버 계정으로 구성된 계층적 트리 구조로 계정을 구성합니다.
루트는 조직의 모든 계정에 대한 상위 컨테이너입니다. 조직 단위(OU)는 루트 내의 https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#account계

정에 대한 컨테이너입니다. OU에는 다른 OU 또는 멤버 계정이 포함될 수 있습니다. OU에는 상위 항목이 하나만 있을 수 있으며 각 계정은 하나의 OU에만 속할 수 있습니다. 자세한 내용은 용어 및 개념(AWS Organizations 문서)을 참조하세요.

서비스 제어 정책(SCP)은 사용자와 역할이 사용할 수 있는 서비스와 작업을 지정합니다. SCPs는 권한을 부여하지 않는다는 점을 제외하면 AWS Identity and Access Management (IAM) 권한 정책과 유사합니다. 대신 SCP는 최대 권한을 정의합니다. 계층의 노드 중 하나에 정책을 연결하면 해당 노드 내의 모든 OU 및 계정에 정책이 적용됩니다. 예를 들어, 루트에 정책을 적용하면 조직의 모든 OU와 계정에 정책이 적용되고 OU에 정책을 적용하면 대상 OU의 OU 및 계정에만 정책이 적용됩니다.

리소스 제어 정책(RCP)은 조직 내 리소스에 사용 가능한 최대 권한을 중앙에서 제어합니다. RCPs 계정의 리소스가 조직의 액세스 제어 지침 내에 있도록 하는 데 도움이 됩니다.

AWS Organizations 콘솔을 사용하여 조직 내 모든 계정을 중앙에서 보고 관리할 수 있습니다. 조직 사용의 이점 중 하나는 관리 및 멤버 계정과 관련된 모든 요금이 표시된 통합 청구서를 받을 수 있다는 것입니다. 자세한 내용은 통합 결제(AWS Organizations 문서)를 참조하세요.

모범 사례

- 기존를 사용하여 조직을 AWS 계정 생성하지 마세요. 조직의 관리 계정이 되는 새 계정으로 시작합니다. 권한 있는 작업은 조직의 관리 계정 내에서 수행할 수 있으며 SCPs 및 RCPs 관리 계정에 적용되지 않습니다. 그러므로 관리 계정에 포함된 클라우드 리소스와 데이터는 관리 계정에서 관리해야 하는 항목으로만 제한해야 합니다.
- 관리 계정에 대한 액세스를 새를 프로비저닝 AWS 계정 하고 조직을 관리해야 하는 개인으로만 제한합니다.
- SCP를 사용하여 루트, 조직 단위 및 멤버 계정에 대한 최대 권한을 정의합니다. 관리 계정에 SCP를 직접 적용할 수는 없습니다.
- RCPs 사용하여 멤버 계정의 리소스에 대한 최대 권한을 정의합니다. RCPs 관리 계정에 직접 적용할 수 없습니다.
- (AWS Organizations 문서) 모범 사례를 AWS Organizations 준수합니다.

랜딩 존 생성

랜딩 존은 워크로드와 애플리케이션을 배포할 수 있는 출발점인 잘 설계된 다중 계정 AWS 환경입니다. 다중 계정 아키텍처, ID 및 액세스 관리, 거버넌스, 데이터 보안, 네트워크 설계 및 로깅을 시작할 수 있는 기준선을 제공합니다. AWS Control Tower는 자동화된 가드레일을 제공하여 다중 계정 환경의 유지 및 거버넌스를 단순화하는 서비스입니다. 일반적으로 계정 AWS 서비스 내 다른를 오케스트레

이션하여 all AWS 리전. AWS Control Tower works에서 환경을 관리하는 단일 AWS Control Tower 랜딩 존을 프로비저닝합니다. 자세한 내용은 랜딩 존을 설정할 때 발생하는 일(문서)을 참조하세요.AWS Control Tower

로 랜딩 존을 설정할 때 관리 계정 AWS Control Tower, 로그 아카이브 계정, 감사 계정의 세 가지 공유 계정을 식별합니다. 자세한 내용은 공유 계정이란 무엇입니까(AWS Control Tower 문서)를 참조하세요. 관리 계정의 경우 워크로드를 호스팅하지 않는 기존 계정을 사용하여 랜딩 존을 설정해야 합니다. 로그 아카이브 및 감사 계정의 경우 기존 계정을 재사용 AWS 계정하거나 자동으로 생성할 AWS Control Tower 수 있습니다.

AWS Control Tower 랜딩 존을 설정하는 방법에 대한 지침은 시작하기(AWS Control Tower 문서)를 참조하세요.

모범 사례

- 다중 계정 전략에 대한 설계 원칙의 모범 사례를 준수합니다(AWS 화이트페이퍼).
- 관리자 모범 사례 AWS Control Tower(AWS Control Tower 문서)를 준수합니다.
- 대부분의 워크로드를 호스팅 AWS 리전 하는에서 랜딩 존을 생성합니다.

> **Important**
>
> 랜딩 존을 배포한 후이 리전을 변경하기로 결정한 경우의 도움이 필요하며 AWS Support랜딩 존을 폐기해야 합니다. 이 방법은 권장되지 않습니다.

- 어떤 리전을 관리할 AWS Control Tower 지 결정할 때는 워크로드를 즉시 배포할 것으로 예상되는 리전만 선택합니다. 이러한 리전을 변경하거나 나중에 더 추가할 수 있습니다. 가 리전을 AWS Control Tower 관리하는 경우 해당 리전에 탐지 가드레일을 로 배포합니다AWS Config 규칙.
- 어떤 리전을 관리할 AWS Control Tower 지 결정한 후 관리되지 않는 모든 리전에 대한 액세스를 거부합니다. 그러면 워크로드 및 개발자가 승인된 AWS 리전만 사용할 수 있습니다. 이는 조직의 서비스 제어 정책(SCP)으로 구현됩니다. 자세한 내용은 AWS 리전 거부 제어 구성(AWS Control Tower 문서)을 참조하세요.
- 에서 랜딩 존을 설정할 때 다음 OUs 및 계정의 이름을 바꾸는 AWS Control Tower것이 좋습니다.
  - Security OU의 이름을 Security_Prod로 변경하여 이 OU가 프로덕션 보안 관련 AWS 계정에 사용됨을 나타내는 것이 좋습니다.
  - AWS Control Tower 에서 추가 OU를 생성한 다음 샌드박스에서 워크로드로 이름을 변경하는 것이 좋습니다. 다음 섹션에서는 AWS 계정을 구성하는 데 사용하는 Workloads OU 내에 추가 OU를 생성합니다.

  - 중앙 집중식 로깅의 이름을 로그 아카이브 AWS 계정 에서 log-archive-prod로 변경하는 것이 좋습니다.
  - 감사 계정의 이름을 Audit에서 security-tooling-prod로 바꾸는 것이 좋습니다.
- 사기를 방지하려면가 사용 기록이 AWS 계정 있는를 AWS AWS Control Tower 랜딩 존에 추가해야 합니다. 사용 기록 AWS 계정 없이 새를 사용하는 경우 새 계정에서 AWS 프리 티어에 없는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작할 수 있습니다. 인스턴스를 몇 분 동안 실행한 후 종료합니다.

조직 단위 추가

다중 계정 환경을 설정하려면 적절한 조직 구조를 구축하는 것이 중요합니다. 서비스 제어 정책(SCP)을 사용하여 OU와 그 안의 계정에 대한 최대 권한을 정의하므로 조직 구조는 관리, 권한 및 재무 보고 관점에서 논리적이어야 합니다. 조직 단위(OUs)를 포함한 조직의 구조에 대한 자세한 내용은 용어 및 개념(AWS Organizations 문서)을 참조하세요.

이 섹션에서는 프로덕션, 비 프로덕션 등의 환경을 세분화하고 구조화하는 데 도움이 되는 중첩된 OU를 생성하여 랜딩 영역을 사용자 지정합니다. 이러한 권장 모범 사례는 랜딩 존을 세분화하여 프로덕션 및 비 프로덕션 리소스를 분리하고 인프라를 워크로드와 분리하도록 설계되었습니다.

OUs를 생성하는 방법에 대한 자세한 내용은 조직 단위 관리(AWS Organizations 문서)를 참조하세요.

모범 사례

- 랜딩 존 생성에서 생성한 Workloads OU 내에 다음과 같은 중첩 OU를 생성합니다.
  - Prod – 고객 데이터를 포함한 프로덕션 데이터를 저장하고 액세스하는 AWS 계정 에 이 OU를 사용합니다.
  - NonProd – 개발, 스테이징, 테스트 환경 등의 비 프로덕션 데이터를 저장하는 AWS 계정 에 이 OU를 사용합니다.

조직 루트 아래에 Infrastructure_Prod OU를 생성합니다. 이 OU를 사용하여 중앙 집중식 네트워킹 계정을 호스팅할 수 있습니다.

초기 사용자 추가

사용자에게 AWS 계정에 대한 액세스 권한을 부여하는 방법은 두 가지입니다.

- IAM 보안 인증(예: 사용자, 그룹 및 역할)
- 를 사용한 것과 같은 자격 증명 페더레이션 AWS IAM Identity Center

소규모 회사와 단일 계정 환경에서는 신규 직원이 입사할 때 관리자가 IAM 사용자를 생성하는 것이 일반적입니다. IAM 사용자에게 연결된 액세스 키와 시크릿 키 보안 인증 정보는 만료되지 않기 때문에 장기 보안 인증 정보라고 합니다. 그러나 공격자가 해당 보안 인증 정보를 손상시킨 경우 사용자에 대한 새로운 보안 인증 정보 세트를 생성해야 하므로 이는 권장되는 보안 모범 사례가 아닙니다. 액세스에 대한 또 다른 접근 방식은 IAM 역할을 통 AWS 계정 하는 것입니다. AWS Security Token Service(AWS STS)를 사용하여 구성 가능한 시간이 지나면 만료되는 단기 보안 인증 정보를 일시적으로 요청할 수도 있습니다.

IAM Identity Center를 AWS 계정 통해에 대한 사용자 액세스를 관리할 수 있습니다. 각 직원 또는 계약자에 대한 개별 사용자 계정을 생성할 수 있으며, 이들은 자신의 암호와 다중 인증(MFA) 솔루션을 관리하고 그룹화하여 액세스를 관리할 수 있습니다. MFA를 구성할 때 인증자 애플리케이션과 같은 소프트웨어 토큰을 사용하거나 YubiKey 디바이스와 같은 하드웨어 토큰을 사용할 수 있습니다.

또한 IAM Identity Center는 Okta, JumpCloud, Ping Identity와 같은 외부 ID 제공업체(idP)와의 페더레이션을 지원합니다. 자세한 내용은 Supported identity providers(IAM Identity Center 설명서)를 참조하세요. 외부 IdP와 페더레이션하면 애플리케이션 간에 사용자 인증을 관리한 다음 IAM Identity Center를 사용하여 특정에 대한 액세스를 승인할 수 있습니다 AWS 계정.

모범 사례

- 사용자 액세스 구성에 대한 보안 모범 사례(IAM 설명서)를 준수합니다.
- 개별 사용자가 아닌 그룹별로 계정 액세스를 관리합니다. IAM Identity Center에서 각 비즈니스 기능을 나타내는 새 그룹을 생성합니다. 예를 들어, 엔지니어링, 재무, 영업, 제품 관리를 위한 그룹을 생성할 수 있습니다.
- 모든 AWS 계정 에 액세스(대개 읽기 전용 액세스)해야 하는 사용자와 단일 AWS 계정에 액세스해야 하는 사용자를 구분하여 그룹을 정의하는 경우가 많습니다. 그룹과 연결된 AWS 계정 및 권한을 쉽게 식별할 수 있도록 그룹에 다음 이름 지정 규칙을 사용하는 것이 좋습니다.

  `<prefix>-<account name>-<permission set>`
- 예를 들어, `AWS-A-dev-nonprod-DeveloperAccess` 그룹의 경우 `AWS-A`는 단일 계정에 대한 액세스를 나타내는 접두사이고, `dev-nonprod`는 계정 이름이고, `DeveloperAccess`는 그룹에 할당된 권한 세트입니다. `AWS-O-BillingAccess` 그룹의 경우 `AWS-O` 접두사는 전체 조직에 대한 액세스를 나타내고 `BillingAccess`는 그룹에 대한 권한 세트를 나타냅니다. 이 예시에서는 그룹이 전체 조직에 액세스할 수 있기 때문에 그룹 이름에 계정 이름이 표시되지 않습니다.

- 외부 SAML 기반 IdP와 함께 IAM Identity Center를 사용하고 있고 MFA를 요구하려는 경우 ABAC(속성 기반 액세스 제어)를 사용하여 IdP에서 IAM Identity Center로 인증 방법을 전달할 수 있습니다. 속성은 SAML 어설션을 통해 전송됩니다. 자세한 내용은 Enable and configure attributes for access control(IAM Identity Center 설명서)을 참조하세요.

  Microsoft Azure Active Directory 및 Okta와 같은 많은 IdP는 SAML 어설션 내의 `amr`(Authentication Method Reference) 클레임을 사용하여 사용자의 MFA 상태를 IAM Identity Center에 전달할 수 있습니다. MFA 상태를 확인하는 데 사용되는 클레임과 해당 형식은 IdP에 따라 다릅니다. 자세한 내용은 IdP 설명서를 참조하세요.

  그런 다음 IAM Identity Center에서 AWS 리소스에 액세스할 수 있는 사용자를 결정하는 권한 세트 정책을 생성할 수 있습니다. ABAC를 활성화하고 속성을 지정하면 IAM Identity Center가 정책 평가에 사용할 인증된 사용자의 속성 값을 IAM으로 전달합니다. 자세한 내용은 Create permission policies for ABAC(IAM Identity Center 설명서)를 참조하세요. 다음 예와 같이 `aws:PrincipalTag` 조건 키를 사용하여 MFA에 대한 액세스 제어 규칙을 생성합니다.

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

멤버 계정 관리

이 섹션에서는 기존 계정을 조직에 초대하고 조직 내에 새 계정을 생성하기 시작합니다. 이 프로세스에서 중요한 부분은 새 계정을 프로비저닝해야 하는지 여부를 결정하는 데 사용할 기준을 정의하는 것입니다.

이 섹션은 다음 작업으로 구성됩니다.

- 기존 계정 초대
- 에서 VPC 설정 사용자 지정 AWS Control Tower
- 범위 기준 정의

기존 계정 초대

내에서 회사의 기존 계정을 새 조직에 초대할 AWS Organizations수 있습니다. 조직의 관리 계정만 다른 계정을 가입하도록 초대할 수 있습니다. 초대받은 계정의 관리자가 수락하면 계정은 즉시 조직에 가입하고 새 멤버 계정에 의해 발생한 모든 경비를 조직의 관리 계정이 책임지게 됩니다. 자세한 내용은

조직에 가입하도록 AWS 계정 초대와 조직에서 보낸 초대 수락 또는 거부(AWS Organizations 설명서)를 참조하세요.

> **Note**
>
> 현재 다른 조직에 속해 있지 않은 계정만 조직에 가입하도록 초대할 수 있습니다. 계정이 기존 조직의 멤버인 경우 조직에서 해당 계정을 제거해야 합니다. 계정이 실수로 생성된 다른 조직의 관리 계정인 경우 해당 조직을 삭제해야 합니다.

> **Important**
>
> 기존 계정의 과거 비용 또는 사용 정보에 액세스해야 하는 경우 AWS Cost and Usage Report를 사용하여 해당 정보를 Amazon Simple Storage Service(Amazon S3) 버킷으로 내보낼 수 있습니다. 조직 가입 초대를 수락하기 전에 이 작업을 수행하세요. 계정이 조직에 가입하면 해당 계정의 이 기록 데이터에 액세스할 수 없게 됩니다. 자세한 내용은 Setting up an Amazon S3 bucket for Cost and Usage Reports(AWS Cost and Usage Report documentation)를 참조하세요.

모범 사례

- 조직 단위 추가 에서 생성한 워크로드 > Prod 조직 단위에 프로덕션 워크로드를 포함할 가능성이 높은 기존 계정을 추가하는 것이 좋습니다.
- 기본적으로 조직의 관리 계정은 조직에 초대된 멤버 계정에 대한 관리 액세스 권한이 없습니다. 관리 계정이 관리 제어 권한을 갖도록 하려면 멤버 계정에서 OrganizationAccountAccessRole IAM 역할을 생성하고, 관리 계정에게 해당 역할을 수임할 권한을 부여해야 합니다. 자세한 내용은 초대된 멤버 계정에서 OrganizationAccountAccessRole 생성(AWS Organizations 문서)을 참조하세요.
- 조직에 초대한 기존 계정의 경우 멤버 계정에 대한 모범 사례(AWS Organizations 문서)를 검토하고 계정이 이러한 권장 사항을 준수하는지 확인합니다.

에서 VPC 설정 사용자 지정 AWS Control Tower

의 Account Factory를 AWS 계정 통해 새로 프로비저닝하는 것이 좋습니다 AWS Control Tower. Account Factory를 AWS Control Tower 사용하면 Amazon EventBridge와의 통합을 사용하여 계정이 생성되는 AWS 계정 즉시 리소스를 새로 프로비저닝할 수 있습니다.

새를 설정하면 AWS 계정기본 Virtual Private Cloud(VPC)가 자동으로 프로비저닝됩니다. 그러나 Account Factory를 통해 새 계정을 설정하면 AWS Control Tower 가 자동으로 추가 VPC를 프로비저닝합니다. 자세한 내용은 AWS Control Tower 및 VPCs.AWS Control Tower 즉, 기본적으로 AWS Control Tower 는 모든 새 계정에 2개의 기본 VPC를 프로비저닝합니다.

기업에서는 계정 내 VPC에 대한 통제력을 강화하고자 하는 경우가 많습니다. 많은 사용자가 AWS CloudFormation Hashicorp Terraform 또는 Pulumi와 같은 다른 서비스를 사용하여 VPCs. AWS Control Tower에서 프로비저닝한 추가 VPC 생성을 방지하려면 Account Factory 설정을 사용자 지정해야 합니다. 지침은 Amazon VPC 설정 구성(AWS Control Tower 문서)을 참조하고 다음 설정을 적용합니다.

1. 인터넷 액세스가 가능한 서브넷 옵션을 비활성화합니다.
2. 최대 프라이빗 서브넷 수에서 0을 선택합니다.
3. VPC 생성용 리전에서 모든 리전을 지웁니다.
4. 가용 영역에서 3을 선택합니다.

모범 사례

- 모든 새 계정에서 자동으로 프로비저닝되는 기본 VPC를 삭제합니다. 이렇게 하면 사용자가 전용 VPC를 명시적으로 생성하지 않고 계정에서 퍼블릭 EC2 인스턴스를 시작할 수 없습니다. 자세한 내용은 기본 서브넷과 기본 VPC 삭제(Amazon Virtual Private Cloud 설명서)를 참조하세요. 새로 생성된 계정에서 기본 VPC를 자동으로 삭제하도록 AWS Control Tower Account Factory for Terraform(AFT)을 구성할 수도 있습니다.
- dev-nonprod AWS 계정 라는 새를 워크로드 > NonProd 조직 단위로 프로비저닝합니다. 개발 환경에 이 계정을 사용합니다. 지침은 를 사용하여 계정 팩토리 계정 프로비저닝 AWS Service Catalog(AWS Control Tower 문서)을 참조하세요.

범위 기준 정의

새를 프로비저닝할지 여부를 결정할 때 회사에서 사용할 기준을 선택해야 합니다 AWS 계정. 사업부별로 계정을 프로비저닝하거나 프로덕션, 테스트, QA 등의 환경에 따라 계정을 프로비저닝하기로 결정할 수 있습니다. 모든 회사에는 얼마나 커야 하는지 또는 작아 AWS 계정 야 하는지에 대한 자체 요구 사항이 있습니다. 일반적으로 계정 규모 조정 방법을 결정할 때 다음 세 가지 요소를 평가합니다.

- 서비스 할당량 밸런싱 - 서비스 할당량은 AWS 서비스 내의 각에 대한 리소스, 작업 및 항목 수의 최대값입니다 AWS 계정. 많은 워크로드가 동일한 계정을 공유하고 한 워크로드가 서비스 할당량의 대부분 또는 전부를 소비하는 경우 동일한 계정의 다른 워크로드에 부정적인 영향을 미칠 수 있습니다.

이러한 경우 해당 워크로드들을 서로 다른 계정으로 분리해야 할 수 있습니다. 자세한 내용은 AWS 서비스 quotas(AWS 일반 참조)를 참조하세요.

- 비용 보고 - 워크로드를 별도의 계정으로 격리하면 비용 및 사용 보고서에서 계정 수준의 비용을 확인할 수 있습니다. 여러 워크로드에 동일한 계정을 사용하는 경우 태그를 사용하면 리소스를 관리하고 식별하는 데 도움이 됩니다. 태그 지정에 대한 자세한 내용은 AWS 리소스 태그 지정()을 참조하세요AWS 일반 참조.
- 액세스 제어 - 워크로드가 계정을 공유하는 경우 사용자가 필요 없는 워크로드에 액세스하지 못하도록 계정 리소스에 대한 액세스를 제한하도록 IAM 정책을 구성하는 방법을 고려해야 합니다. 또는 IAM Identity Center에서 여러 계정과 권한 세트를 사용하여 개별 계정에 대한 액세스를 관리할 수도 있습니다.

모범 사례

- AWSAWS Control Tower 랜딩 존에 대한 다중 계정 전략의 모범 사례를 준수합니다(AWS Control Tower 설명서).
- AWS 리소스를 식별하고 관리하는 데 도움이 되는 효과적인 태깅 전략을 수립합니다. 태그를 사용하여 용도, 사업부, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 자세한 내용은 태깅 모범 사례(AWS 일반 참조 문서화)를 참조하세요.
- 워크로드가 너무 많아 계정이 오버로드되지 않도록 합니다. 워크로드 수요가 서비스 할당량을 초과하는 경우 성능 문제가 발생할 수 있습니다. 경쟁 워크로드를 다른 워크로드로 분리 AWS 계정 하거나 서비스 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Requesting a quota increase(Service Quotas 문서)를 참조하세요.

다중 계정 아키텍처에 대한 권한 및 액세스 관리

이 섹션은 다음 주제로 구성됩니다.

- 엔지니어링 문화적 고려 사항
- 권한 세트 생성
- 권한 경계 생성
- 개인의 권한 관리

엔지니어링 문화적 고려 사항

AWS Well-Architected 프레임워크의 원칙 중 하나는 운영 우수성입니다. 팀은 비즈니스 성과를 달성하는 데 있어 운영 모델과 역할을 이해해야 합니다. 팀은 맡은 책임을 이해하고, 주인의식을 갖고, 의사결정 방식을 파악하면 공동의 목표를 달성하는 데 집중할 수 있습니다.

빠르게 성장하고 있는 초기 단계의 회사에서는 팀원 모두가 여러 역할을 수행합니다. 이러한 사용자가 전체 AWS 계정에 대해 높은 액세스 권한을 갖는 것은 드문 일이 아닙니다. 회사가 성장함에 따라 최소 권한의 원칙을 따르고 사용자가 업무를 수행하는 데 필요한 권한만 부여하려는 경우가 많습니다. 범위를 제한하는 데 도움이 되도록 AWS Identity and Access Management Access Analyzer를 사용하여 사용자 또는 IAM 역할이 실제로 사용하고 있는 권한을 확인하여 초과 권한을 제거할 수 있습니다.

회사에서 IAM 역할을 생성할 권한이 있는 사용자를 결정하는 것은 어려울 수 있습니다. 이는 일반적으로 권한 에스컬레이션의 원인입니다. 사용자가 자신의 권한이나 액세스 범위를 확장할 수 있는 경우 권한 에스컬레이션이 가능합니다. 예를 들어, 사용자가 제한된 권한을 가지고 있지만 새 IAM 역할을 생성할 수 있는 경우 `AdministratorAccess` 관리형 정책이 적용된 새 IAM 역할을 생성하고 수임하여 권한을 에스컬레이션할 수 있습니다.

일부 회사는 IAM 역할 프로비저닝을 신뢰할 수 있는 개인으로 구성된 중앙 팀으로 제한합니다. 이 접근 방식의 단점은 거의 모두 IAM 역할이 AWS 서비스 필요하기 때문에이 팀이 빠르게 병목 현상이 될 수 있다는 것입니다. 또는 권한 경계를 사용하여 클라우드 인프라를 개발, 테스트, 시작 및 관리하는 사용자에게만 IAM 액세스를 위임할 수 있습니다. 정책 예시는 Example Permission Boundaries(GitHub)를 참조하세요.

플랫폼 팀이라고도 하는 개발 운영(DevOps) 팀은 여러 내부 개발 팀의 셀프 서비스 기능과 애플리케이션 운영 안정성을 조정해야 하는 경우가 많습니다. 업무 공간에서 자율성, 숙달, 목적을 포용하는 엔지니어링 문화를 조성하면 팀에 동기를 부여하는 데 도움이 될 수 있습니다. 엔지니어는 다른 사람에게

의존하지 않고 자기 주도적으로 작업하기를 원합니다. DevOps 팀이 셀프 서비스 솔루션을 구현할 수 있다면 다른 사람들이 작업을 완료하기 위해 DevOps 팀에 의존하는 시간도 줄어듭니다.

권한 세트 생성

에서 권한 세트를 사용하여 AWS 계정 액세스를 관리할 수 있습니다 AWS IAM Identity Center. 권한 세트는 하나 이상의 IAM 정책을 여러 AWS 계정에 배포하는 데 사용할 수 있는 템플릿입니다. AWS 계정에 권한 세트를 할당하면 IAM Identity Center는 IAM 역할을 생성하고 IAM 정책을 해당 역할에 연결합니다. 자세한 내용은 Create and manage permission sets(IAM Identity Center 문서)를 참조하세요.

AWS 는 비즈니스의 다양한 페르소나에 매핑되는 권한 세트를 생성할 것을 권장합니다.

예를 들어, 다음과 같은 권한 세트를 생성할 수 있습니다.

- 결제 권한 세트
- 개발자 권한 세트
- 프로덕션 권한 세트

다음 권한 세트는 AWS CloudFormation 템플릿의 코드 조각입니다. 이 코드를 시작점으로 사용하여 비즈니스에 맞게 사용자 지정의해야 합니다. CloudFormation 템플릿에 대한 자세한 내용은 Learn template basics(CloudFormation 설명서)를 참조하세요.

결제 권한 세트

재무 팀은 BillingAccessPermissionSet를 사용하여 각 계정 AWS Cost Explorer 의 AWS Billing 콘솔 대시보드 및를 봅니다.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

개발자 권한 세트

엔지니어링 팀은 DeveloperAccessPermissionSet를 사용하여 비 프로덕션 계정에 액세스합니다.

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

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

프로덕션 권한 세트

엔지니어링 팀은 ProductionPermissionSet를 사용하여 프로덕션 계정에 액세스합니다. 이 권한 세트에는 제한된 읽기 전용 액세스 권한이 있습니다.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
```

```
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

권한 경계 생성

권한 세트를 배포한 후 권한 경계를 설정합니다. 이 권한 경계는 클라우드 인프라를 개발, 테스트, 시작 및 관리하는 사용자에게만 IAM 액세스를 위임하는 메커니즘입니다. 이러한 사용자는 정책과 권한 경계에서 허용하는 작업만 수행할 수 있습니다.

AWS CloudFormation 템플릿에서 권한 경계를 정의한 다음 CloudFormation StackSets를 사용하여 템플릿을 여러 계정에 배포할 수 있습니다. 이렇게 하면 단일 작업으로 조직 전체에 표준화된 정책을 수립하고 유지할 수 있습니다. 자세한 내용과 지침은 Working with AWS CloudFormation StackSets(CloudFormation 설명서)를 참조하세요.

다음 CloudFormation 템플릿은 IAM 역할을 프로비저닝하고 권한 경계 역할을 하는 IAM 정책을 생성합니다. 스택 세트를 사용하면 이 템플릿을 조직의 모든 멤버 계정에 배포할 수 있습니다.

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

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
```

```
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
        - Sid: OverlyPermissiveAllowedServices
          Effect: Allow
          Action:
            - "lambda:*"
            - "apigateway:*"
            - "events:*"
            - "s3:*"
            - "logs:*"
          Resource: "*"
```

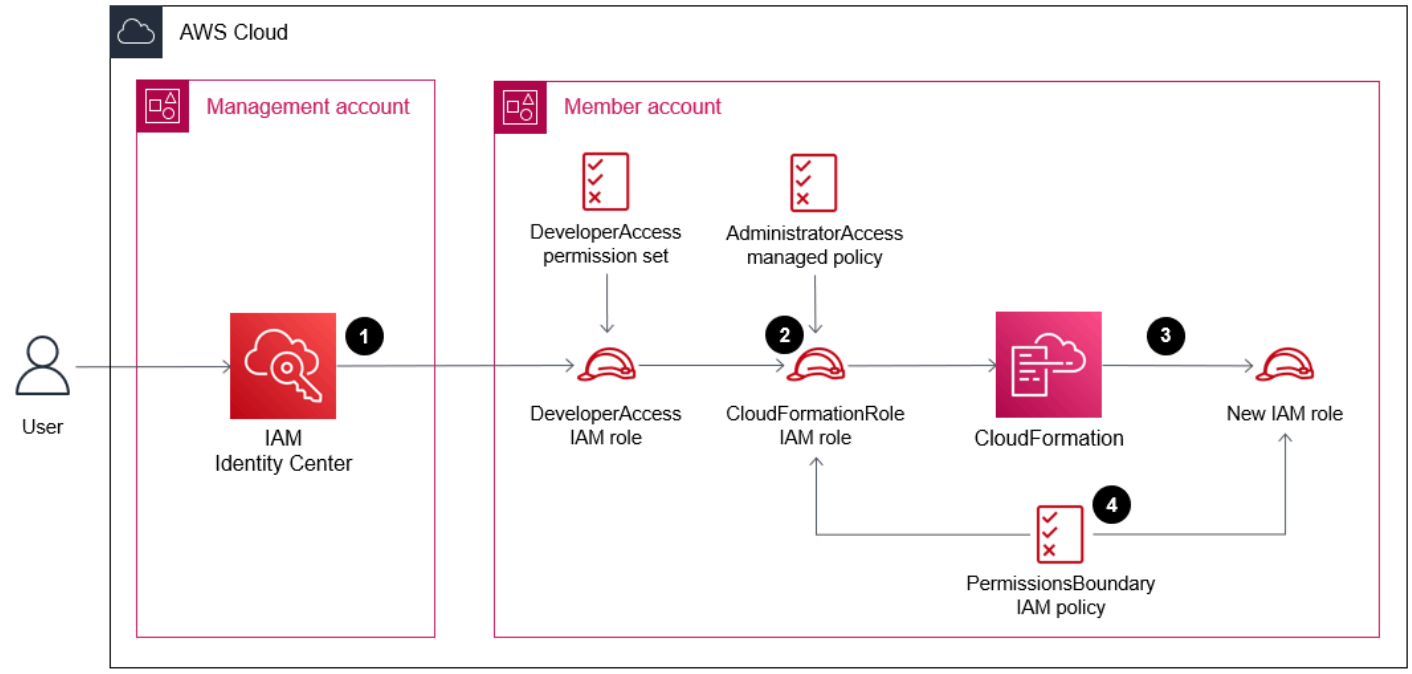
CloudFormationRole 역할, PermissionsBoundary 정책 및 DeveloperAccess 권한 세트가 함께 작동하여 다음 권한을 부여합니다.

- 사용자는 ReadOnlyAccess AWS 관리형 정책을 AWS 서비스통해 대부분의에 대한 읽기 전용 액세스 권한을 가집니다.
- 사용자는 AWSSupportAccess AWS 관리형 정책을 통해 열린 지원 사례에 액세스할 수 있습니다.
- 사용자는 AWSBillingReadOnlyAccess AWS 관리형 정책을 통해 AWS Billing 콘솔 대시보드에 대한 읽기 전용 액세스 권한을 가집니다.

- 사용자는 AWSProtonDeveloperAccess AWS 관리형 정책을 AWS Proton통해에서 새 환경을 프로비저닝할 수 있습니다.
- 사용자는 AWSServiceCatalogEndUserFullAccess AWS 관리형 정책을 통해 Service Catalog에서 제품을 프로비저닝할 수 있습니다.
- 사용자는 인라인 정책을 통해 모든 CloudFormation 템플릿의 비용을 검증하고 추정할 수 있습니다.
- 사용자는 CloudFormationRole IAM 역할을 사용하여 app/로 시작하는 CloudFormation 스택을 생성, 업데이트 또는 삭제할 수 있습니다.
- 사용자는 CloudFormation을 사용하여 app/로 시작하는 IAM 역할을 생성, 업데이트 또는 삭제할 수 있습니다. PermissionsBoundary IAM 정책은 사용자가 권한을 에스컬레이션하는 것을 방지합니다.
- 사용자는 CloudFormation을 사용해야만 AWS Lambda Amazon EventBridge, Amazon CloudWatch, Amazon Simple Storage Service(Amazon S3) 및 Amazon API Gateway 리소스를 프로비저닝할 수 있습니다.

다음 이미지는 개발자와 같은 권한 있는 사용자가 이 가이드에 설명된 권한 세트, IAM 역할 및 권한 경계를 사용하여 멤버 계정에서 새 IAM 역할을 생성하는 방법을 보여줍니다.

1. 사용자가 IAM Identity Center에서 인증하고 DeveloperAccess IAM 역할을 수임합니다.
2. 사용자가 `cloudformation:CreateStack` 작업을 시작하고 CloudFormationRole IAM 역할을 수임합니다.
3. 사용자가 `iam:CreateRole` 작업을 시작하고 CloudFormation을 사용하여 새 IAM 역할을 생성합니다.
4. PermissionsBoundary IAM 정책이 새 IAM 역할에 적용됩니다.



CloudFormationRole 역할에는 AdministratorAccess 관리형 정책이 연결되어 있지만 PermissionsBoundary IAM 정책으로 인해 CloudFormationRole 역할의 유효 권한은 PermissionsBoundary 정책과 동일해집니다. PermissionsBoundary 정책은 `iam:CreateRole` 작업을 허용할 때 자체적으로 참조하므로 권한 경계가 적용된 경우에만 역할이 생성될 수 있습니다.

개인의 권한 관리

권한 세트, 권한 경계 및 CloudFormationRole IAM 역할을 사용하여 개별 보안 주체에게 직접 할당해야 하는 권한의 양을 제한할 수 있습니다. 이를 통해 회사가 성장함에 따라 액세스를 관리하고 최소 권한을 부여하는 보안 모범 사례를 적용할 수 있습니다.

또한 사용자를 대신하여 리소스를 프로비저닝할 수 있도록 AWS 서비스에 권한을 부여하는 서비스 연결 역할을 사용할 수도 있습니다. IAM 보안 주체(사용자, 사용자 그룹 또는 역할)에게 권한을 부여하는 대신 서비스에 권한을 부여할 수 있습니다. 예를 들어, AWS Proton과 AWS Service Catalog의 서비스 연결 역할을 사용하면 IAM 보안 주체에게 권한을 할당하지 않고도 자체 템플릿, 리소스 및 환경을 프로비저닝할 수 있습니다. 자세한 내용은 AWS IAM으로 작업하는AWS 서비스와 서비스 연결 역할 사용(IAM 설명서)을 참조하세요.

또 다른 모범 사례는 개인이 AWS Management Console에 액세스할 수 있는 양을 제한하는 것입니다. 콘솔에 대한 액세스를 제한함으로써 개인이 AWS CloudFormation, HashiCorp Terraform 또는 Pulumi와 같은 코드형 인프라(IaC) 기술을 사용하여 리소스를 프로비저닝하도록 할 수 있습니다. IaC

를 통해 인프라를 관리하면 시간 경과에 따른 리소스 변경 사항을 추적하고 GitHub 풀 요청과 같은 변경 사항을 승인하는 메커니즘을 도입할 수 있습니다.

다중 계정 아키텍처를 위한 네트워크 연결

VPC 연결

많은 회사가 Amazon Virtual Private Cloud(VPC)에서 VPC 피어링을 사용하여 개발 및 프로덕션 VPC를 연결합니다. VPC 피어링 연결을 사용하면 프라이빗 IP 주소 지정을 사용하여 두 VPC 간에 트래픽을 라우팅할 수 있습니다. 연결된 VPCs는 서로 다르 AWS 계정 고 서로 다른에 있을 수 있습니다 AWS 리전. 자세한 내용은 VPC 피어링이란(Amazon VPC 설명서)을 참조하세요. 회사가 성장하고 VPC 수가 증가함에 따라 모든 VPC 간의 피어링 연결을 유지하는 것이 유지 관리 부담이 될 수 있습니다. 또한 VPC당 최대 VPC 피어링 연결 수에 따른 제한을 받을 수도 있습니다. 자세한 내용은 VPC 피어링 연결 할당량(Amazon VPC 설명서)을 참조하세요.

여러에 걸쳐 비프로덕션 데이터를 호스팅하는 개발, 테스트 및 스테이징 환경이 여러 개 AWS 계정있는 경우 이러한 모든 VPCs 간에 네트워크 연결을 제공하지만 프로덕션 환경에 대한 액세스는 허용하지 않을 수 있습니다. AWS Transit Gateway를 사용하여 여러 계정에 걸쳐 여러 VPC를 연결할 수 있습니다. 개발 VPC가 중앙 집중식 라우터 역할을 하는 전송 게이트웨이를 통해 프로덕션 VPC와 통신하지 못하도록 라우팅 테이블을 분리할 수 있습니다. 자세한 내용은 중앙 집중식 라우터(Transit Gateway 설명서)를 참조하세요.

Transit Gateway는 다른 AWS 계정 또는 AWS 리전에 있는 Transit Gateway를 포함한 다른 Transit Gateway와의 피어링을 지원합니다. Transit Gateway는 완전관리형 고가용성 서비스이므로 각 리전에 대해 하나의 Transit Gateway만 프로비저닝하면 됩니다.

자세한 내용과 자세한 네트워크 아키텍처는 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축(AWS 백서)을 참조하세요.

애플리케이션 연결

동일한 환경(예: 프로덕션)의 다른 AWS 계정 에 있는 애플리케이션 간에 통신을 설정해야 하는 경우 다음 옵션 중 하나를 사용할 수 있습니다.

- 여러 IP 주소 및 포트에 대한 광범위한 액세스를 열려는 경우 VPC 피어링 또는 AWS Transit Gateway가 네트워크 수준에서 연결을 제공할 수 있습니다.
- AWS PrivateLink는 VPC의 프라이빗 서브넷에 엔드포인트를 생성하고 이러한 엔드포인트는 Amazon Route 53 Resolver에 DNS 항목으로 등록됩니다. 애플리케이션은 DNS를 사용하여 VPC의 NAT 게이트웨이 또는 인터넷 게이트웨이 없이도 엔드포인트를 확인하고 등록된 서비스에 연결할 수 있습니다.

- Amazon VPC Lattice는 여러 계정과 VPC에서 애플리케이션과 같은 서비스를 연결하고 서비스 네트워크로 수집합니다. 서비스 네트워크와 연결된 VPC의 클라이언트는 동일한 계정에 있는지 여부에 관계없이 서비스 네트워크와 연결된 다른 모든 서비스로 요청을 전송할 수 있습니다. VPC Lattice는 AWS Resource Access Manager (AWS RAM)와 통합되어 다른 계정 또는를 통해 리소스를 공유할 수 있습니다 AWS Organizations. VPC는 하나의 서비스 네트워크와만 연결할 수 있습니다. 이 솔루션은 계정 간 통신을 위해 VPC 피어링 또는 AWS Transit Gateway 를 사용할 필요가 없습니다.

네트워크 연결 모범 사례

- 중앙 집중식 네트워킹에 사용하는 AWS 계정 를 생성합니다. 이 계정의 이름을 network-prod로 지정하고 AWS Transit Gateway 및 Amazon VPC IP Address Manager(IPAM)에 사용합니다. Infrastructure_Prod 조직 단위에 이 계정을 추가합니다.
- AWS Resource Access Manager(AWS RAM)를 사용하여 전송 게이트웨이, VPC Lattice 서비스 네트워크 및 IPAM 풀을 나머지 조직과 공유합니다. 이를 통해 조직 AWS 계정 내 모든가 이러한 서비스와 상호 작용할 수 있습니다.
- IPAM 풀로 IPv4 및 IPv6 주소 할당을 중앙에서 관리하여 최종 사용자가 AWS Service Catalog로 VPC를 자체 프로비저닝하도록 할 수 있습니다. 이를 통해 VPC 크기를 적절하게 조정하고 IP 주소 공간이 겹치는 것을 방지할 수 있습니다.
- 인터넷으로 향하는 트래픽에는 중앙 집중식 송신 접근 방식을 사용하고, 인터넷에서 환경으로 들어오는 트래픽에는 분산 수신 접근 방식을 사용합니다. 자세한 내용은 중앙 집중식 송신 및 분산 수신 섹션을 참조하세요.

중앙 집중식 송신

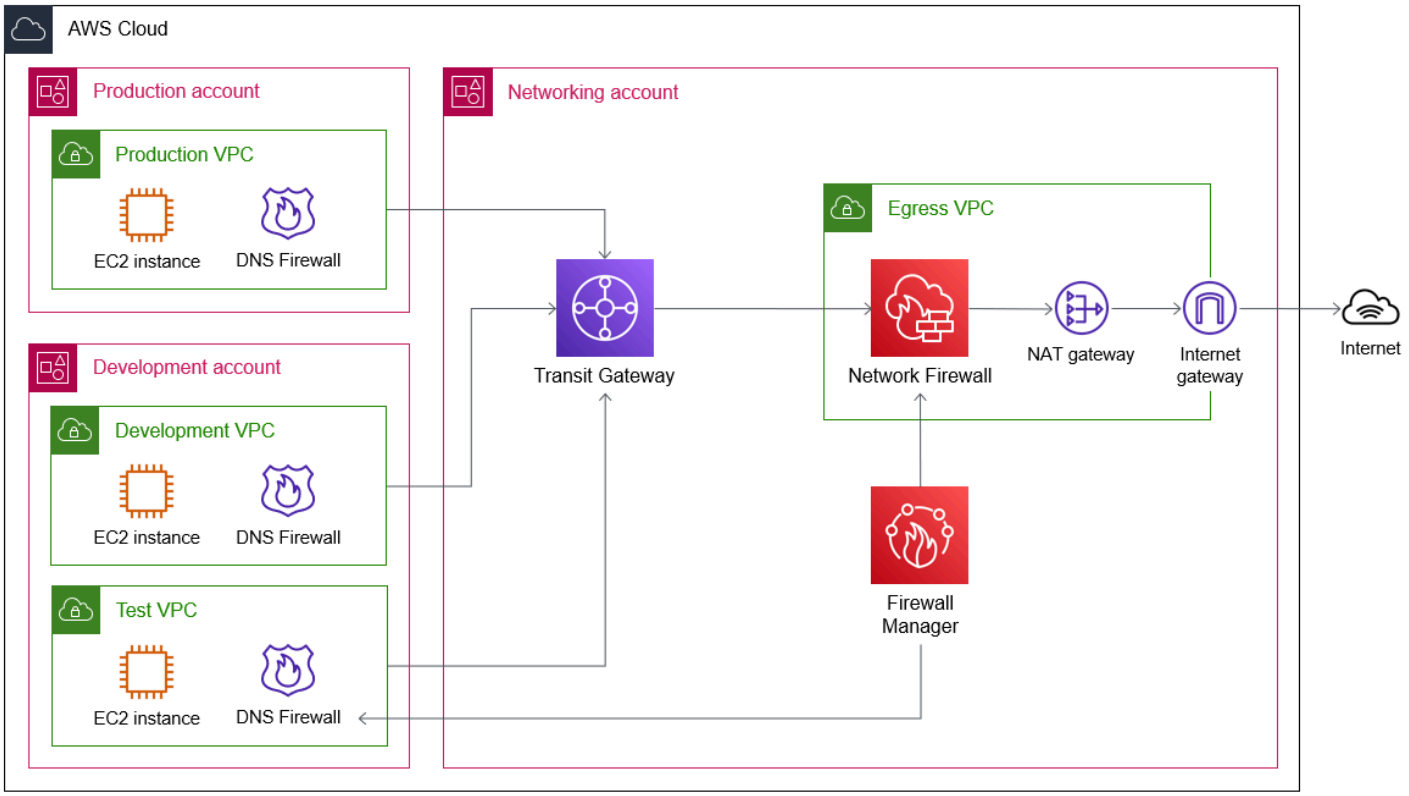
중앙 집중식 송신은 인터넷으로 향하는 모든 네트워크 트래픽에 대해 단일 공통 검사 지점을 사용하는 원칙입니다. 이 검사 지점에서는 지정된 도메인으로만 트래픽을 허용하거나 지정된 포트나 프로토콜을 통해서만 트래픽을 허용할 수 있습니다. 또한 송신을 중앙 집중화하면 인터넷에 연결하기 위해 각 VPC에 NAT 게이트웨이를 배포할 필요가 없으므로 비용을 절감할 수 있습니다. 이는 맬웨어 명령 및 제어(C&C) 인프라와 같이 외부에서 액세스 가능한 악성 리소스에 대한 노출을 제한하므로 보안 관점에서 유익합니다. 중앙 집중식 송신에 대한 자세한 내용과 아키텍처 옵션은 중앙 집중식 송신에서 인터넷으로(백서)를 참조하세요.AWS

관리형 상태 저장 Network Firewall이자 침입 탐지 및 방지 서비스인 AWS Network Firewall을 송신 트래픽의 중앙 검사 지점으로 사용할 수 있습니다. 송신 트래픽을 위한 전용 VPC에서 이 방화벽을 설정

합니다. Network Firewall은 특정 도메인에 대한 인터넷 액세스를 제한하는 데 사용할 수 있는 상태 저장 규칙을 지원합니다. 자세한 내용은 Domain filtering(Network Firewall 설명서)을 참조하세요.

Amazon Route 53 Resolver DNS 방화벽을 사용하면 송신 트래픽을 특정 도메인 이름으로 제한하여 주로 데이터의 무단 유출을 방지할 수도 있습니다. DNS 방화벽 규칙에서는 지정된 도메인에 대한 액세스를 허용하거나 거부하는 도메인 목록(Route 53 설명서)을 적용할 수 있습니다. 악의적인 활동 또는 기타 잠재적 위협과 관련된 도메인 이름이 포함된 AWS 관리형 도메인 목록을 사용하거나 사용자 지정 도메인 목록을 생성할 수 있습니다. DNS 방화벽 규칙 그룹을 생성한 다음 VPC에 적용합니다. 아웃바운드 DNS 요청은 도메인 이름 확인을 위해 VPC의 Resolver를 통해 라우팅되며, DNS 방화벽은 VPC에 적용된 규칙 그룹을 기반으로 요청을 필터링합니다. Resolver로 가는 재귀적 DNS 요청은 전송 게이트웨이와 Network Firewall 경로를 통해 흐르지 않습니다. Route 53 Resolver와 DNS 방화벽은 VPC에서 나가는 별도의 송신 경로로 간주해야 합니다.

다음 이미지는 중앙 집중식 송신을 위한 샘플 아키텍처를 보여줍니다. 네트워크 통신이 시작되기 전에 DNS 요청이 Route 53 Resolver로 전송됩니다. 여기서 DNS 방화벽은 통신에 사용되는 IP 주소의 확인을 허용하거나 거부합니다. 인터넷으로 향하는 트래픽은 중앙 집중식 네트워킹 계정의 전송 게이트웨이로 라우팅됩니다. 전송 게이트웨이는 검사를 위해 트래픽을 Network Firewall에 전달합니다. 방화벽 정책이 송신 트래픽을 허용하는 경우 트래픽은 NAT 게이트웨이, 인터넷 게이트웨이 및 인터넷을 통해 라우팅됩니다. AWS Firewall Manager 를 사용하여 다중 계정 인프라에서 DNS 방화벽 규칙 그룹 및 네트워크 방화벽 정책을 중앙에서 관리할 수 있습니다.



송신 트래픽 보안 모범 사례

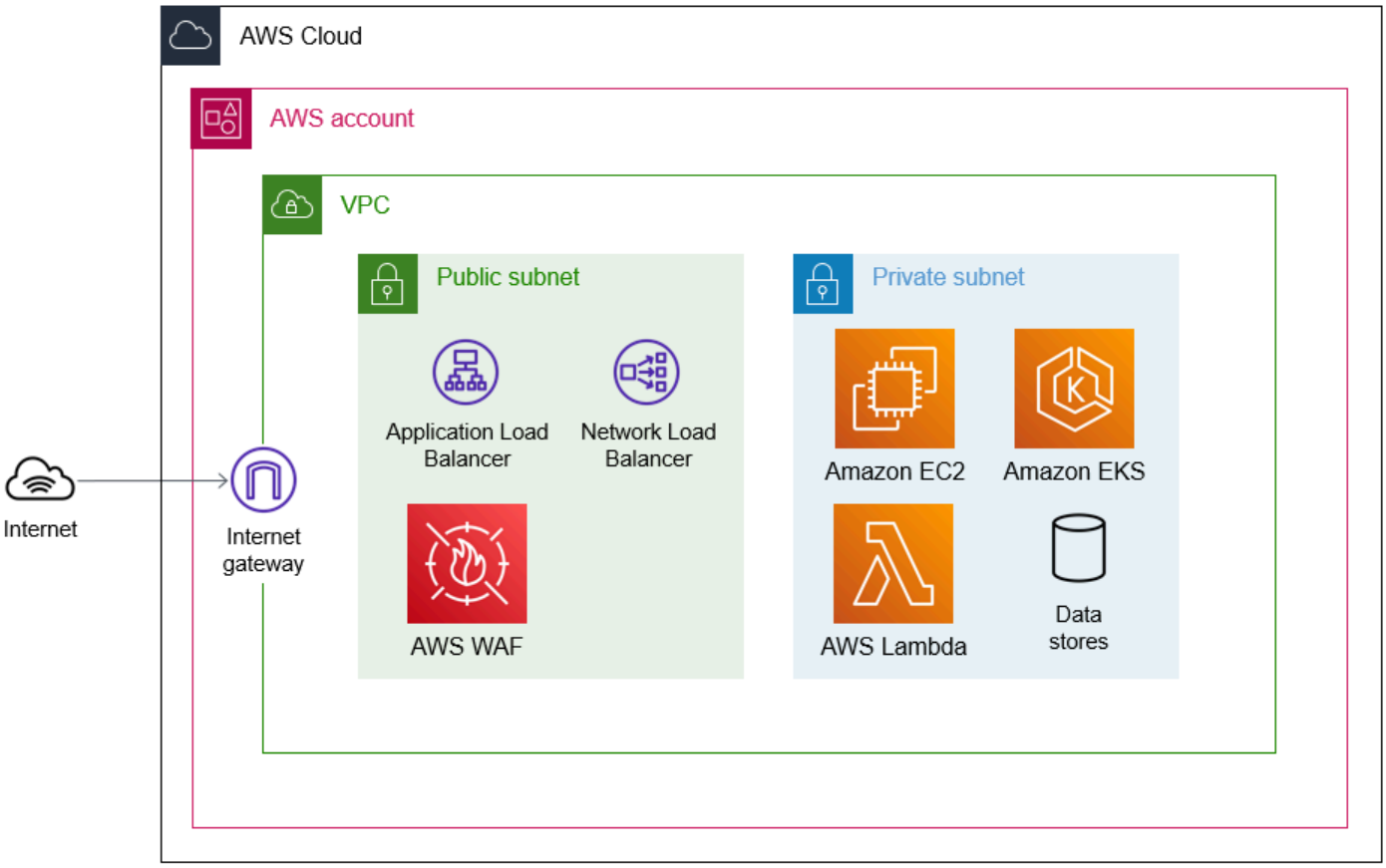
- 로깅 전용 모드(Route 53 설명서)에서 시작합니다. 합법적인 트래픽이 영향을 받지 않는지 확인한 후 차단 모드로 변경합니다.
- AWS Firewall Manager 네트워크 액세스 제어 목록에 대한 정책을 사용하거나를 사용하여 인터넷으로 가는 DNS 트래픽을 차단합니다 AWS Network Firewall. 모든 DNS 쿼리는 Route 53 Resolver를 통해 라우팅되어야 합니다. 여기서 Amazon GuardDuty(활성화된 경우)를 사용하여 모니터링하고 Route 53 Resolver DNS 방화벽(활성화된 경우)을 사용하여 필터링할 수 있습니다. 자세한 내용은 Resolving DNS queries between VPCs and your network(Route 53 설명서)를 참조하세요.
- DNS 방화벽과 Network Firewall에서 AWS 관리형 도메인 목록(Route 53 설명서)을 사용합니다.
- .info, .top, .xyz 또는 일부 국가 코드 도메인과 같이 위험도가 높고 사용되지 않는 최상위 도메인을 차단하는 것을 고려합니다.
- 포트 1389, 4444, 3333, 445, 135, 139 또는 53과 같이 위험도가 높고 사용되지 않는 포트를 차단하는 것을 고려합니다.
- 시작점으로 AWS 관리형 규칙이 포함된 거부 목록을 사용할 수 있습니다. 그런 다음 시간이 지남에 따라 허용 목록 모델을 구현할 수 있습니다. 예를 들어 허용 목록에 정규화된 도메인 이름의 엄격한 목록만 포함하는 대신 *.example.com 같은 일부 와일드카드를 사용하는 것으로 시작합니다. 예상한 최상위 도메인만 허용하고 다른 도메인은 모두 차단할 수도 있습니다. 그런 다음 시간이 지남에 따라 범위를 좁힙니다.
- Route 53 Profiles(Route 53 설명서)를 사용하여 여러 VPCs AWS 계정.
- 이러한 모범 사례에 대한 예외를 처리하는 프로세스를 정의합니다.

분산 수신

분산 수신은 개별 계정 수준에서 인터넷 트래픽이 해당 계정의 워크로드에 도달하는 방식을 정의하는 원칙입니다. 다중 계정 아키텍처에서 분산 수신의 이점 중 하나는 각 계정이 해당 워크로드에 가장 적합한 수신 서비스 또는 리소스(예: Application Load Balancer, Amazon API Gateway 또는 Network Load Balancer)를 사용할 수 있다는 것입니다.

분산 수신은 각 계정을 개별적으로 관리해야 함을 의미하지만 AWS Firewall Manager를 통해 구성을 중앙에서 관리하고 유지할 수 있습니다. Firewall Manager는 AWS WAF 및 Amazon VPC 보안 그룹과 같은 보호를 지원합니다. Application Load Balancer, Amazon CloudFront, API Gateway 또는 AWS WAF 에 연결할 수 있습니다 AWS AppSync. 중앙 집중식 송신에 설명된 대로 송신 VPC와 전송 게이트웨이를 사용하는 경우 각 스포크 VPC에는 퍼블릭 및 프라이빗 서브넷이 포함됩니다. 그러나 트래픽은 네트워킹 계정의 송신 VPC를 통해 라우팅되므로 NAT 게이트웨이를 배포할 필요가 없습니다.

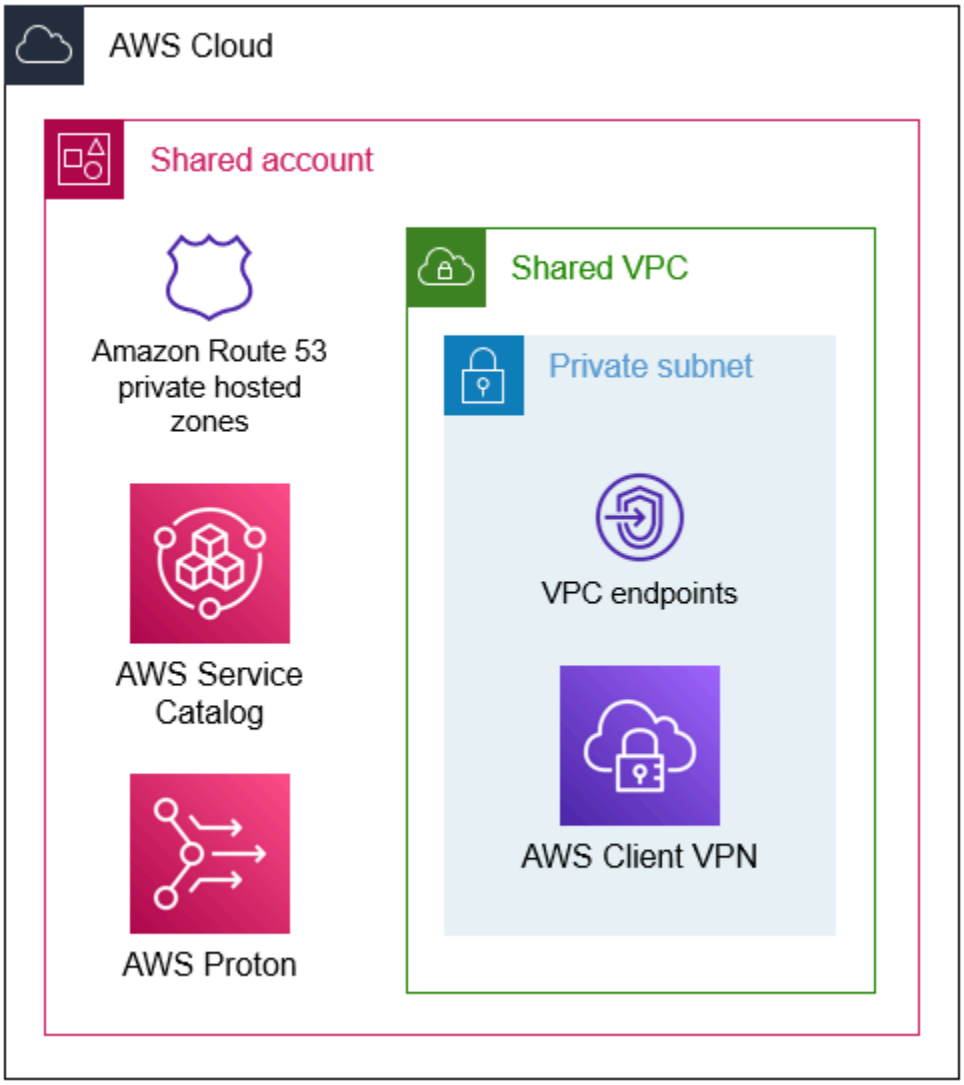
다음 이미지는 인터넷에 액세스할 수 AWS 계정 있는 워크로드가 포함된 단일 VPC가 있는 개인의 예를 보여줍니다. 인터넷의 트래픽은 인터넷 게이트웨이를 통해 VPC에 액세스하고 퍼블릭 서브넷에서 호스팅되는 로드 밸런싱 및 보안 서비스에 도달합니다. 퍼블릭 서브넷에는 인터넷 게이트웨이에 대한 기본 경로가 포함되어 있습니다. 로드 밸런서를 퍼블릭 서브넷에 배포하고 AWS WAF 액세스 제어 목록(ACLs)을 연결하여 교차 사이트 스크립팅과 같은 악성 트래픽으로부터 보호합니다. 인터넷에 직접 액세스할 수 없는 프라이빗 서브넷에 애플리케이션을 호스팅하는 워크로드를 배포합니다.



조직에 VPC가 많은 경우 전용 공유 AWS 계정에 인터페이스 VPC 엔드포인트 또는 프라이빗 호스팅 영역을 생성하여 공통 AWS 서비스 를 공유할 수 있습니다. 자세한 내용은 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스(AWS PrivateLink 문서화) 및 프라이빗 호스팅 영역 작업(Route 53 설명서)을 참조하세요.

다음 이미지는 조직 전체에서 공유할 수 있는 리소스를 호스팅 AWS 계정 하는의 예를 보여줍니다. 전용 VPC에서 VPC 엔드포인트를 생성하여 여러 계정에서 공유할 수 있습니다. VPC 엔드포인트를 생성할 때 AWS 가 엔드포인트에 대한 DNS 항목을 관리하도록 할 수도 있습니다. 엔드포인트를 공유하려면 이 옵션을 선택 취소하고 별도의 Route 53 프라이빗 호스팅 영역(PHZ)에 DNS 항목을 생성합니다. 그런 다음 VPC 엔드포인트의 중앙 집중식 DNS 확인을 위해 PHZ를 조직의 모든 VPC에 연결할 수 있

습니다. 또한 전송 게이트웨이 라우팅 테이블에 공유 VPC에서 다른 VPC로의 경로가 포함되어 있는지 확인해야 합니다. 자세한 내용은 인터페이스 VPC 엔드포인트에 대한 중앙 집중식 액세스(AWS 백서)를 참조하세요.



공유는 AWS Service Catalog 포트폴리오를 호스팅하기에 AWS 계정 좋은 장소이기도 합니다. 포트폴리오는 배포에 사용할 수 있게 하려는 IT 서비스의 모음이며 AWS포트폴리오에는 해당 서비스에 대한 구성 정보가 포함되어 있습니다. 공유 계정에서 포트폴리오를 생성하고 조직에 공유한 다음 각 멤버 계정이 포트폴리오를 자체 리전 Service Catalog 인스턴스로 가져올 수 있습니다. 자세한 내용은 Sharing with AWS Organizations(Service Catalog 설명서)를 참조하세요.

마찬가지로를 사용하면 공유 계정을 사용하여 환경 및 서비스 템플릿을 중앙에서 관리한 다음 조직 멤버 계정과 계정 연결을 설정할 AWS Proton수 있습니다. 자세한 내용은 환경 계정 연결(AWS Proton 문서)을 참조하세요.

다중 계정 아키텍처에 대한 보안 인시던트 대응

여러 로 전환할 때 조직 내에서 발생할 수 있는 보안 이벤트에 대한 가시성을 유지하는 AWS 계정것이 중요합니다. ID 관리 및 액세스 제어에서는 AWS Control Tower 를 사용하여 랜딩 존을 설정했습니다. 이 설정 프로세스 중에 보안을 AWS 계정 위해를 AWS Control Tower 지정했습니다. 보안 서비스 관리를 security-tooling-prod 계정에 위임하고 이 계정을 사용하여 중앙에서 서비스를 관리해야 합니다.

이 가이드에서는 AWS 계정 와 조직을 보호하기 AWS 서비스 위해 다음의 사용을 검토합니다.

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty는 AWS CloudTrail 이벤트 로그와 같은 데이터 소스를 분석하는 지속적인 보안 모니터링 서비스입니다. 지원되는 데이터 소스의 전체 목록은 How Amazon GuardDuty uses its data sources(GuardDuty 설명서)를 참조하세요. 악성 IP 주소 및 도메인 목록 등 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경에서 예기치 않게 발생하는 잠재적 무단 활동과 악의적 활동을 찾아냅니다.

GuardDuty AWS Organizations를와 함께 사용하는 경우 조직의 관리 계정은 조직의 모든 계정을 GuardDuty 위임된 관리자로 지정할 수 있습니다. 위임된 관리자가 해당 리전의 GuardDuty 관리자 계정이 됩니다. GuardDuty는 해당 :에서 자동으로 활성화되며AWS 리전, 위임된 관리자 계정에는 해당 리전 내 조직의 모든 계정에 대해 GuardDuty를 활성화하고 관리할 수 있는 권한이 있습니다. 자세한 내용은 Managing GuardDuty accounts with AWS Organizations를 참조하세요.

GuardDuty는 리전 서비스입니다. 즉, 모니터링하려는 각 리전에서 GuardDuty를 활성화해야 합니다.

모범 사례

- 지원되는 모든에서 GuardDuty를 활성화합니다 AWS 리전. GuardDuty는 현재 활발히 사용하고 있지 않은 리전에서도 비정상적인 활동이나 허가되지 않은 활동에 대한 조사 결과를 생성할 수 있습니다. GuardDuty 요금은 분석된 이벤트 수를 기준으로 책정됩니다. 워크로드를 운영하지 않는 리전에서도 GuardDuty를 활성화하면 잠재적으로 악의적인 활동을 알릴 수 있는 효과적이고 비용 효율적인 탐지 도구로 활용할 수 있습니다. GuardDuty를 사용할 수 있는 리전에 대한 자세한 내용은 Amazon GuardDuty service endpoints(AWS 일반 참조)를 참조하세요.

- 모든 리전 내에서 security-tooling-prod 계정을 위임하여 조직의 GuardDuty를 관리합니다. 자세한 내용은 Designating a GuardDuty delegated administrator(GuardDuty 설명서)를 참조하세요.
- 조직에 추가될 AWS 계정 때 자동으로 새를 등록하도록 GuardDuty를 구성합니다. 자세한 내용은 Managing accounts with AWS Organizations(GuardDuty documentation)의 Step 3 - automate the addition of new organization accounts as members를 참조하세요.

Amazon Macie

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 Amazon Simple Storage Service(S3)에서 민감한 데이터를 검색, 모니터링, 보호하는 데 도움이 되는 완전관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다. Amazon Relational Database Service(RDS) 및 Amazon DynamoDB에서 S3 버킷으로 데이터를 내보낸 다음 Macie를 사용하여 데이터를 스캔할 수 있습니다.

Macie AWS Organizations를와 함께 사용하는 경우 조직의 관리 계정은 조직의 모든 계정을 Macie 관리자 계정으로 지정할 수 있습니다. 관리자 계정은 조직의 멤버 계정에 대해 Macie를 활성화 및 관리하고, Amazon S3 인벤토리 데이터에 액세스하고, 계정에 대해 민감한 데이터 검색 작업을 실행할 수 있습니다. 자세한 내용은 Managing accounts with AWS Organizations(Macie 설명서)를 참조하세요.

Macie는 리전 서비스입니다. 즉, 모니터링하려는 각 리전에서 Macie를 활성화해야 하며 Macie 관리자 계정은 동일한 리전 내에서만 멤버 계정을 관리할 수 있습니다.

모범 사례

- Considerations and recommendations for using Macie with AWS Organizations(Macie 설명서)를 준수합니다.
- 모든 리전 내에서 security-tooling-prod 계정을 위임하여 조직의 Macie를 관리합니다. 여러에서 Macie 계정을 중앙에서 관리하려면 AWS 리전관리 계정이 조직이 현재 Macie를 사용하거나 사용할 각 리전에 로그인한 다음 각 리전에서 Macie 관리자 계정을 지정해야 합니다. 그러면 Macie 관리자 계정이 해당 리전 각각에서 조직을 구성할 수 있습니다. 자세한 내용은 Integrating and configuring an organization(Macie 설명서)을 참조하세요.
- Macie는 민감한 데이터 검색 작업을 위한 월간 프리 티어를 제공합니다. Amazon S3에 민감한 데이터가 저장되어 있는 경우 Macie를 사용하여 월간 프리 티어의 일부로 S3 버킷을 분석하세요. 프리 티어를 초과하면 계정에 민감한 데이터 검색 요금이 발생하기 시작합니다.

AWS Security Hub

AWS Security Hub는의 보안 상태를 포괄적으로 보여줍니다 AWS. 이를 사용하면 환경에서 보안 업계 표준 및 모범 사례를 준수하는지 확인할 수 있습니다. Security Hub는 모든 AWS 계정서비스 (GuardDuty 및 Macie 포함) 및 지원되는 타사 파트너 제품에서 보안 데이터를 수집합니다. Security Hub는 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다. Security Hub는 각 AWS 계정에서 규정 준수 검사를 수행하기 위해 활성화할 수 있는 다양한 보안 표준을 제공합니다.

Security Hub AWS Organizations를와 함께 사용하는 경우 조직의 관리 계정은 조직의 모든 계정을 Security Hub 관리자 계정으로 지정할 수 있습니다. 그러면 Security Hub 관리자 계정이 조직의 다른 멤버 계정을 활성화하고 관리할 수 있습니다. 자세한 내용은 AWS Organizations 를 사용하여 계정 관리(Security Hub 설명서)를 참조하세요.

Security Hub는 리전 서비스입니다. 즉, 분석하려는 각 리전에서 Security Hub를 활성화하고 AWS Organizations에서 각 리전에 대해 위임된 관리자를 정의해야 합니다.

모범 사례

- Prerequisites and recommendations(Security Hub 설명서)를 준수합니다.
- 모든 리전 내에서 security-tooling-prod 계정을 위임하여 조직의 Security Hub를 관리합니다. 자세한 내용은 Designating a Security Hub administrator account(Security Hub 설명서)를 참조하세요.
- 조직에 추가될 AWS 계정 때 새를 자동으로 등록하도록 Security Hub를 구성합니다.
- AWS Foundational Security Best Practices 표준(Security Hub 설명서)을 활성화하여 리소스가 보안 모범 사례에서 벗어나는 경우를 탐지합니다.
- 단일 리전에서 모든 Security Hub 조사 결과를 보고 관리할 수 있도록 크로스 리전 집계(Security Hub 설명서)를 활성화합니다.

다중 계정 아키텍처에 대한 백업 구성

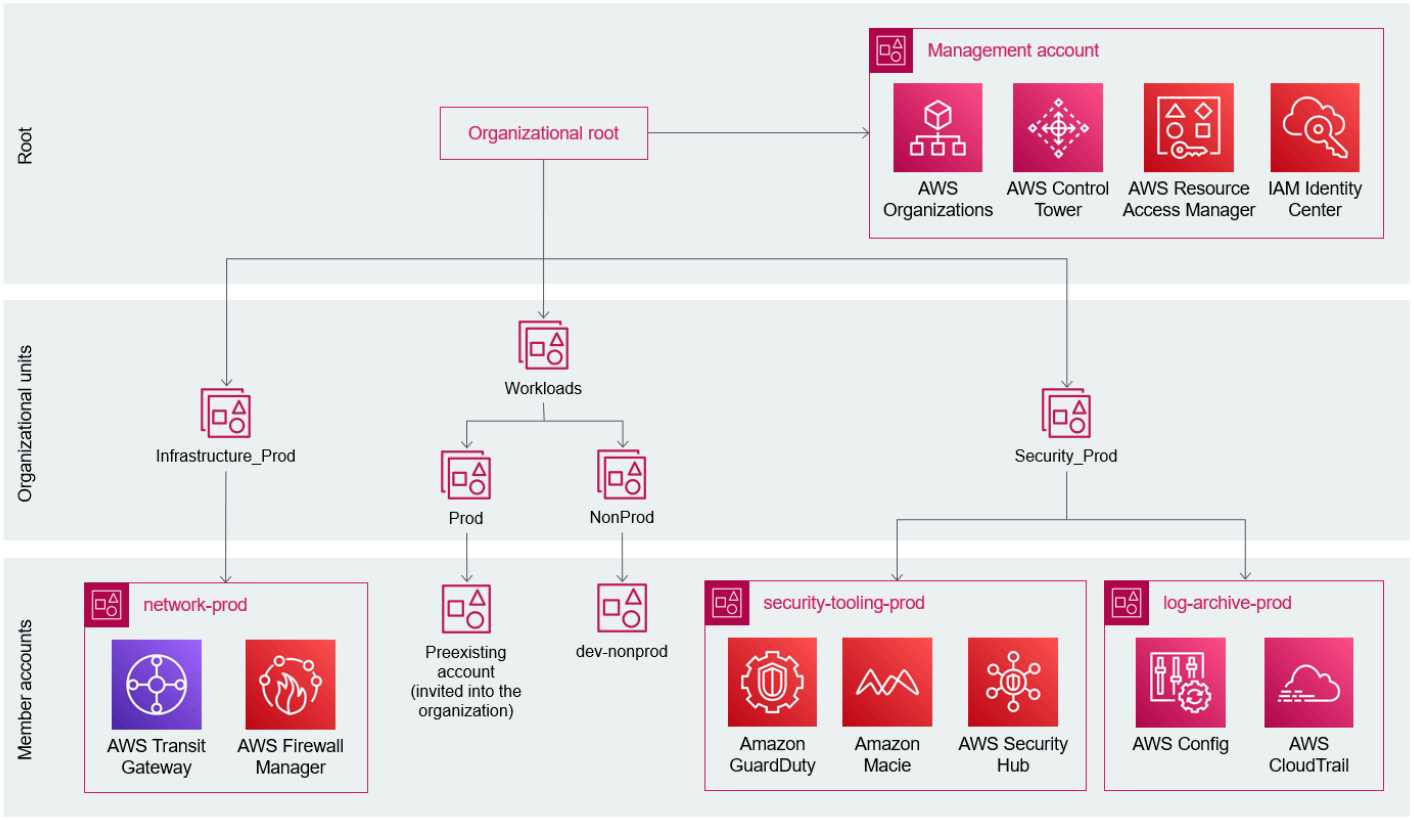
포괄적인 백업 전략은 보안 이벤트로 인해 지속될 수 있는 영향을 견디고, 복구하고, 줄이기 위한 기업 데이터 보호 계획의 필수적인 부분입니다. 조직의 모든 계정에서 리소스에 대한 백업 전략을 표준화하고 구현하는 데 도움이 되는 백업 정책입니다. 백업 정책에서 리소스에 대한 백업 계획을 구성하고 배포할 수 있습니다. 자세한 내용은 백업 정책(AWS Organizations 문서)을 참조하세요. 자세한 내용은 의 백업 보안을 위한 상위 10가지 보안 모범 사례(예비 지침)를 참조하세요 AWS.AWS

다중 계정 아키텍처로 전환 시 계정 마이그레이션

기존 계정 초대에서 워크로드 > Prod 조직 단위에 가입하도록 기존 계정을 초대하였습니다. 이 계정은 이제 조직의 일부로 관리됩니다.

또한 워크로드 > NonProd 조직 단위에서 새 dev-nonprod 계정을 프로비저닝했습니다. 이제 팀원은 를 통해 적절한 계정에 액세스할 수 있습니다 AWS IAM Identity Center. AWS Identity and Access Management (IAM)에서 개별 사용자 계정을 제거합니다.

이 가이드의 권장 사항을 따랐다면 이제 조직의 구조는 다음과 같습니다.



기존 계정 내에서 실행 중인 워크로드가 있는 경우 이제 범위 기준 정의에서 설정한 기준에 따라 이러한 워크로드를 독립 계정으로 마이그레이션합니다. 비 프로덕션 워크로드를 새로운 dev-nonprod 조직 단위로 마이그레이션하고 프로덕션 워크로드를 network-prod 계정으로 마이그레이션합니다. 공통 AWS 리소스 마이그레이션에 대한 자세한 내용은이 가이드의 다음 섹션인 섹션을 참조하세요리소스 마이그레이션.

AWS 계정간 리소스 복제 또는 마이그레이션

단일 계정 아키텍처에서 AWS 계정 다중 계정 아키텍처로 마이그레이션한 후 기존 계정에서 프로덕션 및 비프로덕션 워크로드를 실행하는 것이 일반적입니다. 이러한 리소스를 전용 프로덕션 및 비 프로덕션 계정 또는 조직 단위로 마이그레이션하면 이러한 워크로드에 대한 액세스와 네트워킹을 관리할 수 있습니다. 다음은 공통 AWS 리소스를 다른 리소스로 마이그레이션하는 몇 가지 옵션입니다 AWS 계정.

이 섹션에서는 AWS 계정간 데이터 복제 전략에 중점을 둡니다. 계정 간에 컴퓨팅 리소스를 복제할 필요가 없게 워크로드를 최대한 상태 비저장으로 만들어야 합니다. 별도의 AWS 계정에서 환경을 다시 프로비저닝할 수 있도록 코드형 인프라(IaC)를 통해 리소스를 관리하는 것도 도움이 됩니다.

이 섹션에서는 다음 데이터 리소스를 마이그레이션하는 옵션을 검토합니다.

- AWS AppConfig 구성 및 환경
- AWS Certificate Manager 인증서
- Amazon CloudFront 배포
- AWS CodeArtifact 도메인 및 리포지토리
- Amazon DynamoDB 테이블
- Amazon EBS 볼륨
- Amazon EC2 인스턴스 또는 AMI
- Amazon ECR 레지스트리
- Amazon EFS 파일 시스템
- Amazon ElastiCache(Redis OSS) 클러스터
- AWS Elastic Beanstalk 환경
- 탄력적 IP 주소
- AWS Lambda 계층
- Amazon Lightsail 인스턴스
- Amazon Neptune 클러스터
- Amazon OpenSearch Service 도메인
- Amazon RDS 스냅샷
- Amazon Redshift 클러스터
- Amazon Route 53 도메인 및 호스팅 영역

- Amazon S3 버킷
- Amazon SageMaker AI 모델
- AWS WAF 웹 ACLs

AWS AppConfig 구성 및 환경

AWS AppConfig 는 구성을 다른에 직접 복사하는 것을 지원하지 않습니다 AWS 계정. 그러나 환경을 호스팅 AWS 계정 하는와 별도로 AWS AppConfig 구성 및 환경을 관리하는 것이 가장 좋습니다. 자세한 내용은 를 사용한 교차 계정 구성 AWS AppConfig(AWS 블로그 게시물)을 참조하세요.

AWS Certificate Manager 인증서

인증서의 프라이빗 키를 암호화하는 데 사용되는 AWS Certificate Manager () 키는 각 AWS 리전 및 계정에 고유하기 때문에 한 계정에서 다른 계정으로 AWS Key Management Service (ACM AWS KMS) 인증서를 직접 내보낼 수 없습니다. 그러나 여러 계정과 리전에서 동일한 도메인 이름을 가진 여러 인증서를 동시에 프로비저닝할 수 있습니다. ACM은 DNS(권장) 또는 이메일을 사용한 도메인 소유권 검증을 지원합니다. DNS 검증을 사용하고 새 인증서를 생성하면 ACM은 인증서의 모든 도메인에 대해 고유한 CNAME 레코드를 생성합니다. CNAME 레코드는 계정마다 고유하며 올바른 인증서 검증을 위해 72시간 내에 Amazon Route 53 호스팅 영역 또는 DNS 공급자에게 추가해야 합니다.

Amazon CloudFront 배포

Amazon CloudFront는 배포를 한에서 다른 로 마이그레이션 AWS 계정 하는 것을 지원하지 않습니다 AWS 계정. 그러나 CloudFront는 한 배포판에서 다른 배포판으로의 대체 도메인 이름(CNAME이라고도 함) 마이그레이션을 지원합니다. 자세한 내용은 CloudFront 배포(Knowledge Center)에 대한 CNAME 별칭을 설정할 때 CNAMEAlreadyExists 오류를 해결하려면 어떻게 해야 합니까?를 참조하세요.AWS

AWS CodeArtifact 도메인 및 리포지토리

조직에 여러 도메인이 있을 수 있지만 게시된 아티팩트를 모두 포함하는 단일 프로덕션 도메인이 있는 것이 좋습니다. 이를 통해 개발 팀은 조직 전체에서 패키지를 찾고 공유할 수 있습니다. 도메인을 소유 AWS 계정 한는 도메인과 연결된 리포지토리를 소유한 계정과 다를 수 있습니다. 리포지토리 간에 패키지를 복사할 수 있지만 해당 리포지토리가 동일한 도메인에 속해야 합니다. 자세한 내용은 Copy packages between repositories(CodeArtifact 설명서)를 참조하세요.

Amazon DynamoDB 테이블

다음 서비스 중 하나를 사용하여 다른 AWS 계정으로 Amazon DynamoDB 테이블을 마이그레이션할 수 있습니다.

- AWS Backup
- DynamoDB 가져오기 및 Amazon S3로 내보내기
- Amazon S3 및 AWS Glue
- AWS Data Pipeline
- Amazon EMR

자세한 내용은 Amazon DynamoDB 테이블을 한 테이블에서 다른 테이블 AWS 계정 로 마이그레이션 하려면 어떻게 해야 합니까(AWS 지식 센터)를 참조하세요.

Amazon EBS 볼륨

기존 Amazon Elastic Block Store(Amazon EBS) 볼륨의 스냅샷을 생성하고 해당 스냅샷을 대상 계정과 공유한 다음 대상 계정에 볼륨 복사본을 생성할 수 있습니다. 이렇게 하면 볼륨이 한 계정에서 다른 계정으로 효과적으로 마이그레이션됩니다. 자세한 내용은 암호화된 Amazon EBS 스냅샷 또는 볼륨을 다른와 공유하려면 어떻게 해야 합니까 AWS 계정(AWS 지식 센터)를 참조하세요.

Amazon EC2 인스턴스 또는 AMI

기존 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스나 Amazon Machine Image(AMI)를 다른 AWS 계정으로 직접 전송할 수는 없습니다. 대신 소스 계정에서 사용자 지정 AMI를 생성하고, 대상 계정과 AMI를 공유하고, 대상 계정의 공유 AMI에서 새 EC2 인스턴스를 시작한 다음 공유 AMI를 등록 취소할 수 있습니다.

Amazon ECR 레지스트리

Amazon Elastic Container Registry(Amazon ECR)는 크로스 계정 복제와 크로스 리전 복제를 모두 지원합니다. 소스 레지스트리에서 복제를 구성하고 대상 레지스트리에서 레지스트리 권한 정책을 구성합니다. 자세한 내용은 교차 계정 복제 구성(Amazon ECR 설명서)과 소스 계정의 루트 사용자가 모든 리포지토리를 복제하도록 허용(Amazon ECR 설명서)을 참조하세요.

Amazon EFS 파일 시스템

Amazon Elastic File System(Amazon EFS)은 교차 계정 및 교차 리전 복제를 지원합니다. 소스 파일 시스템에서 복제를 구성할 수 있습니다. 자세한 내용은 파일 시스템 복제(Amazon EFS 설명서)를 참조하세요.

Amazon ElastiCache(Redis OSS) 클러스터

Amazon ElastiCache(Redis OSS) 데이터베이스 클러스터의 백업을 사용하여 다른 계정으로 마이그레이션할 수 있습니다. 자세한 내용은 ElastiCache(Redis OSS) 클러스터 마이그레이션 모범 사례(AWS 지식 센터)를 참조하세요.

AWS Elastic Beanstalk 환경

의 AWS Elastic Beanstalk경우 저장된 구성(Elastic Beanstalk 설명서)을 사용하여 환경을 다른 로 마이그레이션할 수 있습니다 AWS 계정. 자세한 내용은 Elastic Beanstalk 환경을 한 환경에서 다른 환경으로 마이그레이션하려면 어떻게 AWS 계정 해야 하나요 AWS 계정(AWS 지식 센터)를 참조하세요.

탄력적 IP 주소

동일한에 AWS 계정 있는 간에 탄력적 IP 주소를 전송할 수 있습니다 AWS 리전. 자세한 내용은 탄력적 IP 주소 전송(Amazon VPC 설명서)을 참조하세요.

AWS Lambda 계층

기본적으로 생성하는 AWS Lambda 계층은에 비공개입니다 AWS 계정. 그러나 선택적으로 계층을 다른와 공유 AWS 계정 하거나 퍼블릭으로 설정할 수 있습니다. 계층을 복사하려면 다른 계층에서 다시 프로비저닝합니다 AWS 계정. 자세한 내용은 Lambda 계층 작업(Lambda 설명서)을 참조하세요.

Amazon Lightsail 인스턴스

Amazon Lightsail 인스턴스의 스냅샷을 생성하고 해당 스냅샷을 Amazon Machine Image(AMI)와 Amazon EBS 볼륨의 암호화된 스냅샷으로 내보낼 수 있습니다. 자세한 내용은 Amazon EC2로 Amazon Lightsail 스냅샷 내보내기(Lightsail 설명서)를 참조하세요. 기본적으로 스냅샷은 AWS Key Management Service ()에서 생성된 AWS 관리형 키로 암호화됩니다AWS KMS. 그러나이 유형의 KMS 키는 간에 공유할 수 없습니다 AWS 계정. 대신 대상 계정에서 사용할 수 있는 고객 관리형 키로 AMI 사본을 수동으로 암호화합니다. 자세한 내용은 다른 계정의 사용자가 KMS 키를 사용하도록 허

용(AWS KMS 문서)을 참조하세요. 그런 다음 복사된 AMI를 대상과 공유하고 복사된 AMILightsail에서 에 대한 새 EC2 인스턴스를 AWS 계정 시작할 수 있습니다. 자세한 내용은 새 인스턴스 시작 마법사를 사용하여 인스턴스 시작(Amazon EC2 문서)을 참조하세요.

Amazon Neptune 클러스터

Amazon Neptune 데이터베이스 클러스터의 자동 스냅샷을 다른 AWS 계정에 복사할 수 있습니다. 자세한 내용은 Copying a database (DB) cluster snapshot(Neptune 설명서)을 참조하세요.

또한 스냅샷에서 DB 클러스터를 직접 복원할 수 있는 최대 20개의AWS 계정 과 수동 스냅샷을 공유할 수도 있습니다. 자세한 내용은 Sharing a DB Cluster Snapshot(Neptune 설명서)을 참조하세요.

Amazon OpenSearch Service 도메인

Amazon OpenSearch Service 도메인 간에 데이터를 복사하려면 Amazon S3를 사용하여 소스 도메인의 스냅샷을 생성한 다음 다른 AWS 계정의 대상 도메인으로 해당 스냅샷을 복원합니다. 자세한 내용은 다른 (AWS 지식 센터)의 Amazon OpenSearch Service 도메인에서 데이터를 복원하는 방법을 참조하세요 AWS 계정.

간에 네트워크 연결이 있는 경우 OpenSearch Service의 클러스터 간 복제(OpenSearch Service 설명서) 기능을 사용할 수도 AWS 계정있습니다.OpenSearch

Amazon RDS 스냅샷

Amazon Relational Database Service(RDS)의 경우 DB 인스턴스 또는 클러스터의 수동 스냅샷을 최대 20개의AWS 계정과 공유할 수 있습니다. 그런 다음 공유 스냅샷에서 DB 인스턴스나 DB 클러스터를 복원할 수 있습니다. 자세한 내용은 수동 Amazon RDS DB 스냅샷 또는 Aurora DB 클러스터 스냅샷을 다른와 공유하려면 어떻게 해야 합니까 AWS 계정(AWS 지식 센터)를 참조하세요.

AWS Database Migration Service (AWS DMS)를 사용하여 다른 계정의 데이터베이스 인스턴스 간에 연속 복제를 구성할 수도 있습니다. 그러나 이를 위해서는 VPC 피어링 또는 전송 게이트웨이와 같은 계정 간의 네트워크 연결이 필요합니다.

Amazon Redshift 클러스터

Amazon Redshift 클러스터를 다른 로 마이그레이션하려면 소스 계정에서 클러스터의 수동 스냅샷을 AWS 계정생성하고 대상과 스냅샷을 공유한 AWS 계정다음 스냅샷에서 클러스터를 복원합니다. 자세한 내용은 Amazon Redshift 프로비저닝된 클러스터를 다른에 복사하는 방법 AWS 계정(AWS 지식 센터)을 참조하세요.

Amazon Route 53 도메인 및 호스팅 영역

AWS 계정간에 Amazon Route 53 도메인을 이전할 수 있습니다. 자세한 내용은 Transfer a domain to a different AWS 계정(Route 53 설명서)를 참조하세요.

Route 53 호스팅 영역을 다른 로 마이그레이션할 수도 있습니다 AWS 계정. 이것이 권장되거나 필요한 경우에 대한 자세한 내용은 Migrate a hosted zone to a different AWS 계정(Route 53 설명서)를 참조하세요. 호스팅 영역을 마이그레이션할 때 대상 AWS 계정에서 해당 영역을 재생성합니다. 지침은 Migrating a hosted zone to a different AWS 계정(Route 53 설명서)를 참조하세요.

Amazon S3 버킷

Amazon Simple Storage Service(Amazon S3) 동일 리전 복제를 사용하여 동일한 AWS 리전의 S3 버킷 간에 객체를 복사할 수 있습니다. 자세한 내용은 객체 복제(Amazon S3 설명서)를 참조하세요. 다음 사항에 유의하세요.

- 복제본 소유권을 대상 버킷을 소유 AWS 계정 한 로 변경합니다. 자세한 내용은 복제본 소유권 변경(Amazon S3 설명서)을 참조하세요.
- 대상 버킷의 AWS 계정 ID를 반영하도록 버킷 소유자 조건을 업데이트합니다. 자세한 내용은 버킷 소유자 조건을 사용하여 버킷 소유권 확인(Amazon S3 사용 설명서)을 참조하세요.
- 2023년 4월 현재 버킷 소유자 적용 설정이 새로 생성된 버킷에 대해 활성화되어 있어 버킷 액세스 제어 목록(ACL)과 객체 ACL이 효과적이지 않습니다. 자세한 내용은 Amazon S3 보안 변경 예정(블로그 게시물)을 참조하세요.AWS
- S3 배치 복제(Amazon S3 설명서)를 사용하여 복제가 구성되기 전에 존재했던 객체를 복제할 수 있습니다.

Amazon SageMaker AI 모델

SageMaker AI 모델은 훈련 중에 Amazon S3 버킷에 저장됩니다. 대상 계정에서 S3 버킷에 대한 액세스 권한을 부여하면 소스 계정에 저장된 모델을 대상 계정에 배포할 수 있습니다. 자세한 내용은 Amazon SageMaker AI 모델을 다른에 배포하는 방법(지식 센터)을 참조하세요 AWS 계정.AWS

AWS WAF 웹 ACLs

AWS WAF 웹 액세스 제어 목록(웹 ACLs)은 Amazon CloudFront 배포, Application Load Balancer, Amazon API Gateway REST APIs 및 AWS AppSync GraphQL APIs와 같이 연결된 리소스와 동일한

계정에 있어야 합니다. AWS Firewall Manager 를 사용하여의 전체 조직 AWS Organizations 과 리전에서 AWS WAF 웹 ACLs을 중앙에서 관리할 수 있습니다. 자세한 내용은 Getting started with AWS Firewall Manager AWS WAF policies(Firewall Manager 설명서)를 참조하세요.

다중 계정 아키텍처로 전환할 때의 결제 고려 사항

AWS Organizations 를 사용하여 여러 로 전환하는 경우 통합 결제 기능(AWS Organizations 문서)을 사용할 AWS 계정수 있습니다. 이 기능은 여러 계정의 요금을 보여주는 결합된 단일 청구서를 제공합니다.

다음은 여러 계정으로 전환하기 위한 결제 모범 사례 및 권장 사항입니다.

- 과거 결제 데이터에 액세스해야 하는 경우 조직 가입 초대를 수락하기 전에 비용 및 사용 보고서(AWS Cost and Usage Report 문서)를 생성하여 계정의 과거 결제 데이터를 Amazon Simple Storage Service(Amazon S3) 버킷으로 내보냅니다. 조직 가입 초대를 수락하면 계정의 과거 결제 데이터에 더 이상 액세스할 수 없습니다.
- 합병 또는 인수와 같이 두 조직을 결합해야 하는 경우, Account Assessment for AWS Organizations (AWS Solutions Library)를 사용하여 각 조직의 리소스 기반 정책을 평가하고 잠재적 문제를 결합하기 전에 식별할 수 있습니다.

결론

단일 계정에서 AWS 계정 여러 계정으로 전환하면 채택 전략 없이 처음에는 부담스러울 수 있습니다. 다중 계정 전략을 실행하면 회사가 단일 AWS 계정을 사용할 때 직면하는 다음과 같은 많은 문제를 해결할 수 있습니다.

- 개발 데이터에 대한 프로덕션 데이터 모방 - 별도의 권한 세트 프로덕션 및 비프로덕션 조직 단위와 AWS IAM Identity Center 함께를 사용하여 다양한 권한과 액세스 권한을 부여할 수 있습니다. 높은 권한을 가진 사용자만 프로덕션 데이터베이스에 액세스할 수 있어야 하며, 해당 액세스는 제한된 기간 동안만 허용되고 감사를 받아야 합니다.
- 다른 비즈니스 운영에 영향을 미치는 프로덕션 배포 - 여러 계정과 환경을 사용하여 이해관계자를 분리할 수 있습니다. 예를 들어, 데모가 진행되지 않을 때 배포 및 릴리스를 계획할 수 있도록 비 프로덕션 계정 내에 전용 영업 데모 환경을 생성할 수 있습니다.
- 개발 워크로드를 테스트할 때 프로덕션 워크로드 성능 저하 - 각 AWS 계정 에는 각 서비스를 관리하는 독립적인 서비스 할당량이 있습니다. 여러 계정을 사용하여 한 환경이 다른 환경에 미치는 영향 범위를 제한할 수 있습니다.
- 프로덕션 비용과 개발 비용 구별 – 조직에 대한 통합 결제는 AWS 계정 수준에서 모든 비용을 합산하므로 재무 팀은 개발, 테스트, 데모 환경 등의 비 프로덕션 환경과 비교하여 생산 비용이 얼마나 되는지 확인할 수 있습니다. 태그와 태그 지정 정책을 사용하여 계정 내의 비용을 구분할 수도 있습니다.
- 민감한 데이터에 대한 액세스 제한 – IAM Identity Center를 사용하면 특정 계정에 연결된 사용자 그룹에 대해 별도의 액세스 정책을 설정할 수 있습니다.
- 비용 제어 – 다중 계정 아키텍처에서 서비스 제어 정책(SCP)을 사용하면 조직에 높은 비용이 발생할 수 있는 특정 AWS 서비스 에 대한 액세스를 허용하지 않을 수 있습니다. SCP는 특정 서비스에 대한 모든 액세스를 거부하거나 생성할 수 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 유형을 제한하는 등 특정 유형으로 서비스 사용을 제한할 수 있습니다.

기여자

다음은 이 문서의 기여자입니다.

- Justin Plock, Principal Solutions Architect, AWS (주요 작성자)
- Emily Arnautovic, 보안 주체 아키텍트, AWS
- Jason DiDomenico, Senior Solutions Architect, AWS
- Michael Leighty, 선임 보안 전문가 솔루션 아키텍트, AWS
- Jesse Lepich, 선임 보안 전문가 솔루션 아키텍트, AWS
- Rodney Lester, Principal Solutions Architect, AWS
- 이스라엘 Lopez Moriano, 솔루션 아키텍트, AWS
- George Rolston, Senior Solutions Architect, AWS
- Alex Torres, Senior Solutions Architect, AWS
- Dave Walker, Principal Solutions Architect, AWS

리소스

AWS 규범적 지침

- AWS 시작 보안 기준(AWS SSB)
- AWS 보안 참조 아키텍처(AWS SRA)
- 에서 백업을 보호하기 위한 상위 10가지 보안 모범 사례 AWS

AWS 블로그 게시물

- How Setting Up IAM Users and IAM Roles Can Help Keep Your Startup Secure
- How to let builders create IAM resources while improving security and agility for your organization

AWS 백서

- 여러 계정을 사용하여 AWS 환경 구성
- 에서 Cloud Foundation 설정 AWS
- 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축

AWS 코드 샘플

- Automate the setup of security services with AWS Control Tower(GitHub)

문서 기록

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

변경 사항	설명	날짜
리소스 제어 정책	리소스 제어 정책에 대한 정보를 조직 설정 섹션에 추가했습니다.	2024년 11월 20일
중앙 집중식 송신 모범 사례	송신 트래픽 보안을 위한 모범 사례를 업데이트했습니다.	2024년 5월 6일
조직 모범 사례	AWS Organizations에서 조직 생성의 모범 사례를 업데이트했습니다.	2023년 12월 4일
청구 고려 사항	청구 고려 사항 섹션을 추가했습니다.	2023년 9월 20일
리소스 마이그레이션, 애플리케이션 연결, Amazon VPC Lattice	리소스 마이그레이션 및 애플리케이션 연결 섹션을 추가했습니다. 새로운 AWS 서비스인 Amazon Virtual Private Cloud(VPC) Lattice에 대한 정보도 추가했습니다.	2023년 4월 27일
계정 기록 및 ABAC	새에 AWS 계정 사용 기록이 있는지 확인하는 방법에 대한 정보를 추가하여 랜딩 존에 추가할 수 있도록 랜딩 존 생성 섹션을 수정했습니다. AWS Control Tower 또한 초기 사용자 추가 섹션을 수정해 속성 기반 액세스 제어(ABAC)를 사용하여 외부 SAML 기반 IdP에서 AWS IAM Identity Center로 인증 방	2023년 1월 6일

	법을 전달하는 방법에 대한 정보를 추가했습니다.	
송신 트래픽 네트워킹	Amazon Route 53 Resolver DNS 방화벽을 사용하여 송신 트래픽을 특정 도메인 이름으로 제한하는 방법에 대한 정보를 추가하도록 중앙 집중식 송신 섹션을 수정했습니다.	2022년 10월 13일
송신 트래픽의 보안	송신 트래픽 보안 모범 사례를 추가했습니다.	2022년 10월 6일
권한 경계	권한 경계의 정의를 개선하고 리소스 섹션에서 이 주제와 관련된 자세한 정보에 대한 새 링크를 추가했습니다.	2022년 9월 22일
최초 게시	—	2022년 9월 6일

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 버전으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예:에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(RDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예:의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 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, 격리, 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 예로는 `SUM` 및 `MAX`가 있습니다.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 작업을 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 사용할 수 있는 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 검색 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 웹 사이트와 AWS CAF 백서를 참조하십시오.

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

잘못된 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 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. Endianness도 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

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

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇이라고 하는 일부 다른 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 것입니다.

봇넷

맬웨어에 감염되어 있고 봇 셰이더 또는 봇 운영자라고 하는 단일 당사자가 제어하는 봇 네트워크입니다. Botnet은 봇과 봇의 영향을 확장하는 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.

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 깨진 절차 구현 표시기를 AWS 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 클라우드 채택 프레임워크를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 드는 경우 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

Cloud Center of Excellence를 참조하세요.

CDC

변경 데이터 캡처를 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 장애 또는 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 전달을 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 기술과 연결됩니다.

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 로 마이그레이션할 때 일반적으로 거치는 4단계: AWS 클라우드

- 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 리포지토리에는 GitHub 또는가 포함됩니다Bitbucket Cloud. 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 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며, 일반적으로 점진적이고 의도하지 않습니다.

구성 관리 데이터베이스(CMDB)

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

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 문제 해결 작업의 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 Framework에서 보안 원칙의 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 분산된 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 일반적으로 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

데이터베이스 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 컨트롤을 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 Implementing security controls on AWS의 Detective controls를 참조하십시오.

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 스키마에서는 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 일반적으로 쿼리 제약, 필터링 및 결과 집합 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 시간과 데이터 손실을 최소화하는 데 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

기준 구성과의 편차 추적. 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 값 스트림 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 클라우드 컴퓨팅과 비교할 때 엣지 컴퓨팅은 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간의 비즈니스 문서 자동 교환. 자세한 내용은 전자 데이터 교환이란 무엇입니까?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 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외래 키가 포함된 열의 두 가지 유형이 포함됩니다.

빠른 실패

개발 수명 주기를 줄이기 위해 자주 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

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.

몇 장의 샷 프롬프트

유사한 작업을 수행하도록 요청하기 전에 작업과 원하는 출력을 보여주는 몇 가지 예제를 LLM에 제공합니다. 이 기법은 컨텍스트 내 학습을 적용하여 모델이 프롬프트에 포함된 예제(샷)에서 학습합니다. 퓨샷 프롬프트는 특정 형식 지정, 추론 또는 도메인 지식이 필요한 작업에 효과적일 수 있습니다. 제로샷 프롬프트도 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 연속 데이터 복제를 사용하여 최대한 짧은 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화 및 레이블 지정되지 않은 데이터의 대규모 데이터 세트에 대해 훈련된 대규모 딥 러닝 신경망입니다. FMs은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 작업을 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란 무엇입니까?를 참조하세요.

G

생성형 AI

대량의 데이터에 대해 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트 및 오디오와 같은 새 콘텐츠 및 아티팩트를 생성할 수 있는 AI 모델의 하위 집합입니다. 자세한 내용은 생성형 AI란 무엇입니까?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 현대적이고 선호하는 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조업에서는 골든 이미지를 사용하여 여러 디바이스에 소프트웨어를 프로비저닝할 수 있으며 디바이스 제조 작업의 속도, 확장성 및 생산성을 개선하는 데 도움이 됩니다.

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, , 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 데이터 세트에서 보류된 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교하여 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.

정보

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 참조하십시오.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 적용 또는 수정하는 대신 프로덕션 워크로드를 위한 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 사용한 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 참조하기 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 VPCs. 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(TIL)

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

IT 서비스 관리(TSM)

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 데이터를 기반으로 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문 답변, 문서 요약, 텍스트를 다른 언어로 변환, 문장 완성과 같은 여러 작업을 수행할 수 있습니다. 자세한 내용은 LLMs 참조하십시오.

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. Endianness도 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 개인 정보 보호를 손상하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 중단하거나, 민감한 정보를 유출하거나, 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

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

제조 실행 시스템(MES)

원재료를 작업 현장의 완성된 제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

마이그레이션 가속화 프로그램을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동 시 자체를 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 대기열 원격 측정 전송(MQTT)

리소스가 제한된 IoT 디바이스에 대한 게시/구독 패턴을 기반으로 하는 경량 M2M(machine-to-machine) 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)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. 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 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은이 용어집의 7R 항목을 참조하고 대규모 마이그레이션을 가속화하기 위해 조직 동원을 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 의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드.

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 의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드.

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

마이그레이션 포트폴리오 평가를 참조하세요.

MQTT

메시지 대기열 원격 측정 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 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 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

작업 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 Architecture를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 M2M(Machinemachine-to-machine) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 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 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 혁신의 핵심 초점입니다.

운영 통합(OI)

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

조직 트레일

조직의 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는 AWS 계정 에서 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 가능한 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한을 정의하거나(자격 증명 기반 정책 참조), 액세스 조건을 지정하거나(리소스 기반 정책 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체 AWS Organizations 입니다(서비스 제어 정책 참조).

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 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 마이크로서비스에서 데이터 지속성 활성화를 참조하십시오.

포트폴리오 평가

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

조건자

`false`일반적으로 `WHERE` 절에 있는 `true` 또는를 반환하는 쿼리 조건입니다.

조건자 푸시다운

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

설계에 따른 개인 정보 보호

전체 개발 프로세스를 통해 개인 정보를 고려하는 시스템 엔지니어링 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.

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 리소스를 스캔합니다. 리소스가 컨트롤을 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 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

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

프롬프트 체인

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 작업을 하위 작업으로 나누거나 예비 응답을 반복적으로 구체화하거나 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)

마이크로서비스 간의 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 지침과 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

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RAG

Retrieval Augmented Generation을 참조하세요.

랜섬웨어

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

RASCI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 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.

재설계

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 지정을 참조 AWS 리전 하세요.

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.

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 고가용성 및 재해 복구가 일반적인 고려 사항입니다 AWS 클라우드. 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 Implementing security controls on AWS의 Responsive controls를 참조하십시오.

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 의미 검색을 수행할 수 있습니다. 자세한 내용은 RAG란 무엇입니까?를 참조하십시오.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 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

복구 시점 목표를 참조하세요.

RTO

복구 시간 목표를 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 조직 내 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.

secret

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 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 Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?를 참조하세요.

설계별 보안

전체 개발 프로세스를 통해 보안을 고려하는 시스템 엔지니어링 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 예방, 탐지, 대응 및 사전 예방의 네 가지 주요 유형이 있습니다.

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

서버 측 암호화

데이터를 AWS 서비스 수신하는가 대상에서 데이터를 암호화합니다.

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 표시기(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 대상 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 장애 지점(SPOF)

애플리케이션의 중요한 단일 구성 요소에 장애가 발생하여 시스템이 중단될 수 있습니다.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 표시기를 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 에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드.

SPOF

단일 장애 지점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스 또는 비즈니스 인텔리전스용으로 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 압도

하고 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)

제조에서 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 시스템을 테스트합니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 지침 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 및 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.

전송 게이트웨이

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 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 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대 위치를 기반으로 행 값에 액세스하는 등의 작업을 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

쓰기를 한 번, 많이 읽기를 참조하세요.

WQF

AWS 워크로드 검증 프레임워크를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

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

Z

제로데이 익스플로잇

[제로데이 취약성](#)을 활용하는 공격, 일반적으로 맬웨어입니다.

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 프롬프트

[LLM](#)에 작업을 수행하기 위한 지침을 제공하지만 작업에 도움이 될 수 있는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 작업을 처리해야 합니다. 제로샷 프롬프트의 효과는 작업의 복잡성과 프롬프트의 품질에 따라 달라집니다. [스크린샷이 거의 없는 프롬프트도 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.