AWS Key Management Service 모범 사례

# AWS 권장 가이드

# AWS 권장 가이드: AWS Key Management Service 모범 사례

# Table of Contents

소개 ..... 1
목표 비즈니스 성과 ..... 1
정보 AWS KMS keys ..... 2
키 관리 ..... 3
관리 모델 선택 ..... 3
키 유형 선택 ..... 4
키 스토어 선택 ..... 6
KMS 키 삭제 및 비활성화 ..... 6
데이터 보호 ..... 8
암호화 ..... 8
로그 데이터 암호화 ..... 9
암호화 기본 제공 ..... 10
데이터베이스 암호화 ..... 11
PCI DSS 데이터 암호화 ..... 12
Amazon EC2 Auto Scaling에서 KMS 키 사용 ..... 12
키 교체 ..... 13
대칭 키 교체 ..... 13
Amazon EBS의 키 교체 ..... 13
Amazon RDS의 키 교체 ..... 15
Amazon S3의 키 교체 ..... 15
가져온 구성 요소로 키 교체 ..... 16
AWS Encryption SDK사용 ..... 16
자격 증명 및 액세스 관리 ..... 17
키 정책 및 IAM 정책 ..... 17
최소 권한 ..... 19
역할 기반 액세스 제어 ..... 20
속성 기반 액세스 제어 ..... 21
암호화 컨텍스트 ..... 22
권한 문제 해결 ..... 23
탐지 및 모니터링 ..... 24
모니터링 AWS KMS 작업 ..... 24
키 액세스 모니터링 ..... 25
암호화 설정 모니터링 ..... 26
CloudWatch 경보 구성 ..... 27

응답 자동화 ..... 27
비용 및 결제 ..... 29
키 스토리지 비용 ..... 29
Amazon S3 버킷 키 ..... 29
데이터 키 캐싱 ..... 30
대안 ..... 30
로깅 비용 관리 ..... 30
리소스 ..... 32
AWS KMS 설명서 ..... 32
도구 ..... 32
AWS 권장 가이드 ..... 32
전략 ..... 32
가이드 ..... 32
패턴 ..... 32
기여자 ..... 33
작성 ..... 33
검토 ..... 33
기술 작성 ..... 33
문서 기록 ..... 34
용어집 ..... 35
# ..... 35
A ..... 36
B ..... 38
C ..... 40
D ..... 43
E ..... 47
F ..... 49
G ..... 50
H ..... 51
정보 ..... 53
L ..... 55
M ..... 56
O ..... 60
P ..... 62
Q ..... 65
R ..... 65

S ..... 68
T ..... 71
U ..... 73
V ..... 73
W ..... 74
Z ..... 75
..... lxxvi

# AWS Key Management Service 모범 사례

Amazon Web Services(기여자)

2025년 3월(문서 기록)

AWS Key Management Service (AWS KMS)는 데이터를 보호하는 데 사용하는 암호화 키를 쉽게 생성하고 제어할 수 있게 해주는 관리형 서비스입니다. 이 가이드에서는를 효과적으로 사용하는 방법을 설명하고 모범 사례를 AWS KMS 제공합니다. 이를 통해 구성 옵션을 비교하고 필요에 가장 적합한 세트를 선택할 수 있습니다.

이 가이드에는 조직에서 민감한 정보를 보호하고 여러 사용 사례에 대한 서명을 구현 AWS KMS 하는 데를 사용하는 방법에 대한 권장 사항이 포함되어 있습니다. 다음 차원을 사용하는 현재 권장 사항을 고려합니다.

- 키 관리 - 관리 및 키 스토리지 선택에 대한 위임 옵션
- 데이터 보호 - 자체 애플리케이션 내에서 데이터를 암호화하는 것과 사용자를 대신하여 AWS 서비스 데이터를 암호화하는 것
- 액세스 관리 - AWS KMS 키 정책 및 AWS Identity and Access Management (IAM) 정책을 사용하여 역할 기반 액세스 제어(RBAC) 또는 속성 기반 액세스 제어(ABAC)를 구현합니다.
- 다중 계정 및 다중 리전 아키텍처 - 대규모 배포를 위한 권장 사항입니다.
- 결제 및 비용 관리 - 비용 및 사용량과 비용 절감 방법에 대한 권장 사항을 이해합니다.
- 탐지 제어 - KMS 키, 암호화 설정 및 암호화된 데이터의 상태를 모니터링합니다.
- 인시던트 대응 - 데이터 보호 정책을 준수하지 않는 잘못된 구성을 수정합니다.

## 목표 비즈니스 성과

데이터는 비즈니스에 중요하고 민감한 자산입니다. 를 사용하면 데이터를 보호하고 확인하는 데 사용되는 암호화 키를 AWS KMS관리할 수 있습니다. 데이터 사용 방법, 데이터에 액세스할 수 있는 사용자, 데이터 암호화 방법을 제어합니다. 이 가이드는 개발자, 시스템 관리자 및 보안 전문가가 저장되거나 전송되는 민감한 데이터를 보호하는 데 도움이 되는 암호화 모범 사례를 구현하는 데 도움을 주기 위한 것입니다 AWS 서비스. 이 가이드의 권장 사항을 이해하고 구현하면 AWS 환경 전체에서 데이터 기밀성과 무결성을 높일 수 있습니다. 데이터 보호 요구 사항이 내부적으로 작성되었는지 또는 규정 준수 또는 검증 프로그램과 관련된 요구 사항이 있는지 여부에 관계없이 데이터 보호 요구 사항을 충족할 수 있습니다. AWS KMS 가 AWS 환경에서 데이터를 보호하는 데 도움이 되는 방법에 대한 자세한 내용은 AWS KMS 설명서의 에서 AWS KMS 암호화 사용을 AWS 서비스 참조하세요.

# 정보 AWS KMS keys

AWS Key Management Service (AWS KMS)를 사용하면 서비스에 전달하는 데이터에 사용할 수 있는 암호화 키를 생성할 수 있습니다. 기본 리소스 유형은 KMS 키이며, 그 중 세 가지 유형이 있습니다.

- 고급 암호화 표준(AES) 대칭 키 - AES의 Galois Counter Mode(GCM) 모드에서 사용되는 256비트 키입니다. 이러한 키는 크기가 4KB 미만인 데이터의 인증된 암호화 및 복호화를 제공합니다. 가장 일반적인 유형의 키입니다. 애플리케이션에서 사용하거나 사용자를 대신하여 데이터를 AWS 서비스 암호화하는에서 사용하는 것과 같은 다른 데이터 키를 보호하는 데 사용됩니다.
- RSA 또는 타원 곡선 비대칭 키 "" - 이러한 키는 다양한 크기로 사용할 수 있으며 많은 알고리즘을 지원합니다. 알고리즘에 따라 암호화 및 복호화와 서명 및 확인 작업에 사용할 수 있습니다.
- 해시 기반 메시지 인증 코드(HMAC) 작업을 수행하기 위한 대칭 키 - 이러한 키는 서명 및 확인 작업에 사용되는 256비트 키입니다.

KMS 키는 서비스에서 일반 텍스트로 내보낼 수 없습니다. KMS 키는 서비스에서 사용하는 하드웨어 보안 모듈(HSM)에 의해 생성되고 해당 보안 모듈 내에서만 사용될 수 있습니다. 이는 키 손상을 방지하기 AWS KMS 위한의 기본 보안 속성입니다. 중국(베이징) 및 중국(닝샤) 리전에서는 이러한 HSMs OSCCA의 인증을 받았습니다. 다른 모든 리전에서는에 사용되는 HSMs 보안 수준 3의 NIST 내에서 FIPS 140 프로그램에 따라 검증 AWS KMS 됩니다. 키를 보호하는 데 도움이 AWS KMS 되는의 설계 및 제어에 대한 자세한 내용은 AWS Key Management Service 암호화 세부 정보를 참조하세요.

KMS 키를 사용하여 암호화, 복호화, 서명 또는 확인 작업을 수행하기 위해 다양한 암호화 APIs를 AWS KMS 사용하여에 데이터를 제출할 수 있습니다. KMS 키가 데이터 키라는 키 유형을 보호하는 키 암호화 키처럼 작동하도록 선택할 수도 있습니다. 로컬 애플리케이션 또는 사용자를 대신하여 데이터를 AWS 서비스 보호하는 내에서 사용하기 AWS KMS 위해에서 데이터 키를 내보낼 수 있습니다. 데이터 키의 사용은 모든 키 관리 시스템에서 일반적이며 봉투 암호화라고도 합니다. 봉투 암호화를 사용하면 KMS 키 아래에서 직접 AWS KMS 암호화를 위해 민감한 데이터를 로 보내는 대신 민감한 데이터를 처리하는 원격 시스템에서 데이터 키를 사용할 수 있습니다.

자세한 내용은 AWS KMS 설명서의 AWS KMS keys 및 AWS KMS 암호화 필수 항목을 참조하세요.

# 에 대한 키 관리 모범 사례 AWS KMS

AWS Key Management Service (AWS KMS)를 사용할 때는 몇 가지 기본적인 설계 결정을 내려야 합니다. 여기에는 키 관리 및 액세스를 위해 중앙 집중식 모델을 사용할지 아니면 분산식 모델을 사용할지 여부, 사용할 키 유형, 사용할 키 스토어 유형이 포함됩니다. 다음 섹션에서는 조직 및 사용 사례에 적합한 결정을 내리는 데 도움이 됩니다. 이 섹션에서는 데이터 및 키를 보호하기 위해 수행해야 하는 작업을 포함하여 KMS 키 비활성화 및 삭제에 대한 중요한 고려 사항으로 마무리합니다.

이 섹션은 다음 주제를 포함합니다:

- 중앙 집중식 또는 분산식 모델 선택
- 고객 관리형 키, AWS 관리형 키 또는 AWS 소유 키 선택
- AWS KMS 키 스토어 선택
- KMS 키 삭제 및 비활성화

## 중앙 집중식 또는 분산식 모델 선택

AWS 에서는 여러를 사용하고 해당 계정을에서 단일 조직으로 AWS 계정 관리할 것을 권장합니다AWS Organizations. 다중 계정 환경에서를 관리하는 데는 두 가지 광범위한 접근 방식이 AWS KMS keys 있습니다.

첫 번째 접근 방식은 각 계정에서 해당 키를 사용하는 키를 생성하는 분산 접근 방식입니다. KMS 키를 보호하는 리소스와 동일한 계정에 저장하는 경우 AWS 보안 주체 및 키에 대한 액세스 요구 사항을 이해하는 로컬 관리자에게 권한을 위임하는 것이 더 쉽습니다. 키 정책만 사용하여 키 사용을 승인하거나 AWS Identity and Access Management (IAM)에서 키 정책과 자격 증명 기반 정책을 결합할 수 있습니다.

두 번째 접근 방식은 KMS 키를 하나 또는 몇 개의 지정된에 유지하는 중앙 집중식 접근 방식입니다 AWS 계정. 다른 계정이 암호화 작업에만 키를 사용하도록 허용합니다. 중앙 집중식 계정에서 키, 수명 주기 및 권한을 관리합니다. 다른 AWS 계정 사용자가 키를 사용하도록 허용하지만 다른 권한은 허용하지 않습니다. 외부 계정은 키의 수명 주기 또는 액세스 권한에 대한 어떤 것도 관리할 수 없습니다. 이 중앙 집중식 모델은 위임된 관리자 또는 사용자의 의도하지 않은 키 삭제 또는 권한 에스컬레이션 위험을 최소화하는 데 도움이 될 수 있습니다.

선택하는 옵션은 여러 요인에 따라 달라집니다. 접근 방식을 선택할 때는 다음 사항을 고려하세요.

1. 키 및 리소스 액세스를 프로비저닝하기 위한 자동 또는 수동 프로세스가 있습니까? 여기에는 배포 파이프라인 및 코드형 인프라(IaC) 템플릿과 같은 리소스가 포함됩니다. 이러한 도구는 여러에 리

소스(예: KMS 키, 키 정책, IAM 역할 및 IAM 정책)를 배포하고 관리하는 데 도움이 될 수 있습니다 AWS 계정. 이러한 배포 도구가 없는 경우 키 관리에 대한 중앙 집중식 접근 방식이 비즈니스에 더 적합할 수 있습니다.

2. KMS 키를 사용하는 리소스 AWS 계정 가 포함된 모든에 대한 관리 제어 권한이 있습니까? 그렇다면 중앙 집중식 모델을 사용하면 관리를 간소화하고 키를 관리하기 AWS 계정 위해 전환할 필요가 없습니다. 그러나 키를 사용할 수 있는 IAM 역할 및 사용자 권한은 여전히 계정별로 관리해야 합니다.
3. 자체 AWS 계정 및 리소스가 있는 고객 또는 파트너에게 KMS 키를 사용할 수 있는 액세스 권한을 제공해야 합니까? 이러한 키의 경우 중앙 집중식 접근 방식을 통해 고객과 파트너의 관리 부담을 줄일 수 있습니다.
4. 중앙 집중식 또는 로컬 액세스 접근 방식을 통해 더 잘 해결되는 AWS 리소스에 액세스하기 위한 권한 부여 요구 사항이 있습니까? 예를 들어, 서로 다른 애플리케이션 또는 사업부가 자체 데이터의 보안을 관리하는 역할을 하는 경우 키 관리에 대한 분산형 접근 방식이 더 좋습니다.
5. 에 대한 서비스 리소스 할당량을 초과하고 있습니까 AWS KMS? 이러한 할당량은 당 설정되므로 AWS 계정분산 모델은 계정 간에 로드를 분산하여 서비스 할당량을 효과적으로 곱합니다.

> **Note**
>
> 키 관리 모델은 요청 할당량을 고려할 때 관련이 없습니다. 이러한 할당량은 키를 소유하거나 관리하는 계정이 아니라 키에 대해 요청하는 계정 보안 주체에 적용되기 때문입니다.

일반적으로 중앙 집중식 KMS 키 모델의 필요성을 명확히 설명할 수 없는 한 분산형 접근 방식으로 시작하는 것이 좋습니다.

## 고객 관리형 키, AWS 관리형 키 또는 AWS 소유 키 선택

자체 암호화 애플리케이션에서 사용하기 위해 생성하고 관리하는 KMS 키를 고객 관리형 키라고 합니다.는 고객 관리형 키를 사용하여 서비스가 사용자를 대신하여 저장하는 데이터를 암호화할 AWS 서비스 수 있습니다. 수명 주기와 키 사용을 완전히 제어하려면 고객 관리형 키를 사용하는 것이 좋습니다. 계정에 고객 관리형 키를 보유하는 데는 월별 비용이 발생합니다. 또한 키 사용 또는 관리 요청에는 사용 비용이 발생합니다. 자세한 내용은 AWS KMS 요금을 참조하십시오.

AWS 서비스 에서 데이터를 암호화하지만 키 관리의 오버헤드나 비용을 원하지 않는 경우 AWS 관리형 키를 사용할 수 있습니다. 이러한 유형의 키는 계정에 존재하지만 특정 상황에서만 사용할 수 있습니다. 운영 중인의 컨텍스트에서만 사용할 수 있으며 키 AWS 서비스 가 포함된 계정 내의 보안 주체만

사용할 수 있습니다. 이러한 키의 수명 주기 또는 권한은 관리할 수 없습니다. 일부는 AWS 관리형 키를 AWS 서비스 사용합니다. AWS 관리형 키 별칭의 형식은 입니다`aws/<service code>`. 예를 들어 키는 `aws/ebs` 키와 동일한 계정의 Amazon Elastic Block Store(Amazon EBS) 볼륨을 암호화하는 데만 사용할 수 있으며 해당 계정의 IAM 보안 주체만 사용할 수 있습니다. AWS 관리형 키는 해당 계정의 사용자와 해당 계정의 리소스에 대해서만 사용할 수 있습니다. AWS 관리형 키로 암호화된 리소스는 다른 계정과 공유할 수 없습니다. 사용 사례에 제한이 있는 경우 대신 고객 관리형 키를 사용하는 것이 좋습니다. 해당 키의 사용을 다른 계정과 공유할 수 있습니다. 계정에 AWS 관리형 키가 있는 경우 요금이 부과되지 않지만 키에 AWS 서비스 할당된에서이 키 유형을 사용하는 경우 요금이 부과됩니다.

AWS 관리형 키는 2021 AWS 서비스 년부터 새에 대해 더 이상 생성되지 않는 레거시 키 유형입니다. 대신 새 키(및 레거시 키) AWS 서비스 는 AWS 소유 키를 사용하여 기본적으로 데이터를 암호화합니다. AWS 소유 키는가 여러에서 사용하기 위해 AWS 서비스 소유하고 관리하는 KMS 키 모음입니다 AWS 계정. 이러한 키는에 없지만 AWS 계정는 키를 사용하여 계정의 리소스를 보호할 AWS 서비스 수 있습니다.

세분화된 제어가 가장 중요한 경우 고객 관리형 키를 사용하고 편의성이 가장 중요한 경우 AWS 소유 키를 사용하는 것이 좋습니다.

다음 표에서는 각 키 유형 간의 키 정책, 로깅, 관리 및 요금 차이를 설명합니다. 키 유형에 대한 자세한 내용은 AWS KMS 개념을 참조하세요.

| 고려 사항 | 고객 관리형 키 | AWS 관리형 키 | AWS 소유 키 |
| --- | --- | --- | --- |
| 키 정책 | 고객이 독점적으로 제어 | 서비스에서 제어, 고객이 볼 수 있음 | 데이터를 암호화하는 AWS 서비스 에서만 독점적으로 제어되고 볼 수 있음 |
| 로깅 | AWS CloudTrail 고객 추적 또는 이벤트 데이터 스토어 | CloudTrail 고객 추적 또는 이벤트 데이터 저장소 | 고객이 볼 수 없음 |
| 수명 주기 관리 | 고객이 교체, 삭제 및 관리 AWS 리전 | AWS 서비스 는 교체(연간), 삭제 및 리전을 관리합니다. | AWS 서비스 는 교체(연간), 삭제 및 리전을 관리합니다. |
| 요금 | 키 존재에 대한 월별 요금(시간당 비례 할당), 호출자에게 API | 키 존재에 대한 요금 없음, 호출자에게 API 사용에 대한 요금 부과 | 고객에게 부과되는 요금 없음 |

| 고려 사항 | 고객 관리형 키 | AWS 관리형 키 | AWS 소유 키 |
| --- | --- | --- | --- |
| | 사용 요금이 청구됩니다. | | |

## AWS KMS 키 스토어 선택

키 스토어는 암호화 키 구성 요소를 저장하고 사용하기 위한 안전한 위치입니다. 키 스토어의 업계 모범 사례는 보안 수준 3의 NIST Federal Information Processing Standards(FIPS) 140 암호화 모듈 검증 프로그램에 따라 검증된 하드웨어 보안 모듈(HSM)이라는 디바이스를 사용하는 것입니다. 결제를 처리하는 데 사용되는 키 스토어를 지원하는 다른 프로그램이 있습니다. AWS Payment Cryptography는 결제 워크로드와 관련된 데이터를 보호하는 데 사용할 수 있는 서비스입니다.

AWS KMS 는를 사용하여 암호화 키를 생성하고 관리할 때 키 구성 요소를 보호하는 AWS KMS 데 도움이 되는 여러 키 스토어 유형을 지원합니다. 에서 제공하는 모든 키 스토어 옵션은 보안 수준 3의 FIPS 140에 따라 지속적으로 검증 AWS KMS 됩니다. 연 AWS 산자를 포함한 모든 사용자가 권한 없이 일반 텍스트 키에 액세스하거나 사용하지 못하도록 설계되었습니다. 사용 가능한 키 스토어 유형에 대한 자세한 내용은 AWS KMS 설명서의 키 스토어를 참조하세요.

AWS KMS 표준 키 스토어는 대부분의 워크로드에 가장 적합합니다. 다른 유형의 키 스토어를 선택해야 하는 경우 규제 또는 기타 요구 사항(예: 내부)에서 이러한 선택을 요구하는지 신중하게 고려하고 비용과 이점을 신중하게 고려하세요.

## KMS 키 삭제 및 비활성화

KMS 키를 삭제하면 상당한 영향을 미칠 수 있습니다. 더 이상 사용하지 않을 KMS 키를 삭제하기 전에 키 상태를 비활성화됨으로 설정하는 것이 적절한지 고려합니다. 키가 비활성화된 동안에는 암호화 작업에 사용할 수 없습니다. 여전히에 있으며 필요한 경우 나중에 다시 활성화 AWS할 수 있습니다. 비활성화된 키에는 계속 스토리지 요금이 발생합니다. 키가 데이터 또는 데이터 키를 보호하지 않는다고 확신할 때까지 키를 삭제하는 대신 비활성화하는 것이 좋습니다.

> **Important**
>
> 키 삭제는 신중하게 계획해야 합니다. 해당 키가 삭제된 경우 데이터를 복호화할 수 없습니다. AWS 는 삭제된 키를 삭제한 후 복구할 방법이 없습니다. 의 다른 중요한 작업과 마찬가지로 AWS삭제를 위해 키를 예약하고 키 삭제를 위해 다중 인증(MFA)을 요구할 수 있는 사용자를 제한하는 정책을 적용해야 합니다.

우발적인 키 삭제를 방지하기 위해는 `DeleteKey` 호출 실행 후 7일의 기본 최소 대기 기간을 AWS KMS 적용한 후 키를 삭제합니다. 대기 기간을 최대 30일로 설정할 수 있습니다. 대기 기간 동안 키는 여전히 삭제 보류 중 상태로 AWS KMS 에 저장됩니다. 암호화 또는 복호화 작업에 사용할 수 없습니다. 암호화 또는 복호화를 위해 삭제 보류 중 상태인 키를 사용하려는 모든 시도는에 기록됩니다 AWS CloudTrail. CloudTrail 로그에서 이러한 이벤트에 대한 Amazon CloudWatch 경보를 설정할 수 있습니다. 이러한 이벤트에 대한 경보를 수신하는 경우 필요한 경우 삭제 프로세스를 취소하도록 선택할 수 있습니다. 대기 기간이 만료될 때까지 삭제 보류 상태에서 키를 복구하고 비활성화됨 또는 활성화됨 상태로 복원할 수 있습니다.

다중 리전 키를 삭제하려면 원본 복사 전에 복제본을 삭제해야 합니다. 자세한 내용은 다중 리전 키 삭제를 참조하세요.

가져온 키 구성 요소가 있는 키를 사용하는 경우 가져온 키 구성 요소를 즉시 삭제할 수 있습니다. 이는 여러 가지 방법으로 KMS 키를 삭제하는 것과 다릅니다. `DeleteImportedKeyMaterial` 작업을 수행하면가 키 구성 요소를 AWS KMS 삭제하고 키 상태가 가져오기 보류 중으로 변경됩니다. 키 구성 요소를 삭제하면 키를 즉시 사용할 수 없습니다. 대기 기간은 없습니다. 키 사용을 다시 활성화하려면 동일한 키 구성 요소를 다시 가져와야 합니다. KMS 키 삭제 대기 기간은 가져온 키 구성 요소가 있는 KMS 키에도 적용됩니다.

데이터 키가 KMS 키로 보호되고에서 적극적으로 사용 중인 경우 연결된 KMS 키가 비활성화되거나 가져온 키 구성 요소가 삭제되더라도 데이터 키는 즉시 영향을 AWS 서비스받지 않습니다. 예를 들어 가져온 구성 요소가 있는 키를 사용하여 SSE-KMS로 객체를 암호화했다고 가정해 보겠습니다. Amazon Simple Storage Service(Amazon S3) 버킷에 객체를 업로드하는 중입니다. 버킷에 객체를 업로드하기 전에 구성 요소를 키로 가져옵니다. 객체가 업로드되면 해당 키에서 가져온 키 구성 요소를 삭제합니다. 객체는 암호화된 상태로 버킷에 남아 있지만 삭제된 키 구성 요소가 키로 다시 가져오기 전까지는 아무도 객체에 액세스할 수 없습니다. 이 흐름에는 키에서 키 구성 요소를 가져오고 삭제하기 위한 정확한 자동화가 필요하지만, 환경 내에서 추가 수준의 제어를 제공할 수 있습니다.

AWS 는 KMS 키의 예약된 삭제를 모니터링하고 수정(필요한 경우)하는 데 도움이 되는 규범적 지침을 제공합니다. 자세한 내용은 AWS KMS 키의 예약된 삭제 모니터링 및 수정을 참조하세요.

# 에 대한 데이터 보호 모범 사례 AWS KMS

이 섹션에서는 각 데이터 유형에 사용할 키와 같이 데이터 보호를 위한 AWS Key Management Service (AWS KMS) 키 사용에 대해 선택할 수 있습니다. 또한를 다른 AWS KMS 와 함께 사용하는 구체적인 예제도 제공합니다 AWS 서비스. 이러한 권장 사항 및 예제는 필요한 키 수와 이러한 키를 사용하기 위해 권한이 필요한 보안 주체를 이해하는 데 도움이 됩니다.

이 섹션에서는 키 교체에 대해서도 설명합니다. 키 교체는 기존 KMS 키를 새 키로 교체하거나 기존 KMS 키와 연결된 암호화 구성 요소를 새 구성 요소로 교체하는 방법입니다. 이 가이드에서는 일반적으로 사용되는 KMS 키를 교체하는 방법에 대한 예제와 지침을 제공합니다 AWS 서비스. 권장 사항 및 예제는 키 교체 전략에 대해 정보에 입각한 선택을 하는 데 도움이 되도록 설계되었습니다.

마지막으로이 섹션에서는 애플리케이션에서 클라이언트 측 암호화를 구현하기 위한 도구 AWS Encryption SDK인를 사용하는 방법에 대한 권장 사항을 제공합니다. 이 섹션에는의 기능 세트와 기능을 기반으로 수행할 수 있는 설계 선택 사항이 포함되어 있습니다 AWS Encryption SDK.

이 섹션에서는 다음 암호화 주제에 대해 설명합니다.

- 를 사용한 암호화 AWS KMS
- 영향의 키 교체 AWS KMS 및 범위
- 사용에 대한 권장 사항 AWS Encryption SDK

## 를 사용한 암호화 AWS KMS

암호화는 민감한 정보의 기밀성과 무결성을 보호하는 일반적인 모범 사례입니다. 기존 데이터 분류 수준을 사용해야 하며 수준당 하나 이상의 AWS Key Management Service 키(AWS KMS)가 있어야 합니다. 예를 들어 기밀, 내부 전용, 중요로 분류된 데이터에 대해 KMS 키를 정의할 수 있습니다. 이렇게 하면 권한이 부여된 사용자만 각 분류 수준과 연결된 키를 사용할 수 있는 권한을 갖도록 할 수 있습니다.

> **Note**
>
> 단일 고객 관리형 KMS 키는 AWS 서비스 또는 특정 분류의 데이터를 저장하는 자체 애플리케이션의 모든 조합에서 사용할 수 있습니다. 여러 워크로드에서 키를 사용할 때 제한 요인 AWS 서비스 은 사용자 집합에서 데이터에 대한 액세스를 제어하기 위해 사용 권한이 얼마나 복잡해야 하는지입니다. AWS KMS 키 정책 JSON 문서는 32KB 미만이어야 합니다. 이 크기 제한이 제한이 되는 경우 권한 AWS KMS 부여를 사용하거나 여러 키를 생성하여 키 정책 문서의 크기를 최소화하는 것이 좋습니다.

데이터 분류에만 의존하여 KMS 키를 분할하는 대신 단일 내에서 데이터 분류에 사용할 KMS 키를 할당하도록 선택할 수도 있습니다 AWS 서비스. 예를 들어 Amazon Simple Storage Service(Amazon S3)`Sensitive`에 태그가 지정된 모든 데이터는와 같은 이름의 KMS 키로 암호화되어야 합니다`S3-Sensitive`. 정의된 데이터 분류 및 AWS 서비스 /또는 애플리케이션 내에서 여러 KMS 키에 데이터를 추가로 배포할 수 있습니다. 예를 들어 특정 기간의 일부 데이터 세트를 삭제하고 다른 기간의 다른 데이터 세트를 삭제할 수 있습니다. 리소스 태그를 사용하여 특정 KMS 키로 암호화된 데이터를 식별하고 정렬할 수 있습니다.

KMS 키에 대한 분산 관리 모델을 선택하는 경우 가드레일을 적용하여 지정된 분류의 새 리소스가 생성되고 올바른 권한이 있는 예상 KMS 키를 사용해야 합니다. 자동화를 사용하여 리소스 구성을 적용, 감지 및 관리하는 방법에 대한 자세한 내용은이 가이드의 탐지 및 모니터링 섹션을 참조하세요.

이 섹션에서는 다음 암호화 주제에 대해 설명합니다.

- 를 사용한 로그 데이터 암호화 AWS KMS
- 암호화 기본 제공
- 를 사용한 데이터베이스 암호화 AWS KMS
- 를 사용한 PCI DSS 데이터 암호화 AWS KMS
- Amazon EC2 Auto Scaling에서 KMS 키 사용

## 를 사용한 로그 데이터 암호화 AWS KMS

Amazon GuardDuty 및와 AWS 서비스같은 많은는 Amazon S3로 전송되는 로그 데이터를 암호화하는 옵션을 AWS CloudTrail제공합니다. GuardDuty에서 Amazon S3로 결과를 내보낼 때는 KMS 키를 사용해야 합니다. 모든 로그 데이터를 암호화하고 보안 팀, 인시던트 대응 담당자, 감사자와 같은 승인된 보안 주체에게만 복호화 액세스 권한을 부여하는 것이 좋습니다.

AWS 보안 참조 아키텍처는 로깅을 AWS 계정 위한 중앙를 생성할 것을 권장합니다. 이렇게 하면 키 관리 오버헤드를 줄일 수도 있습니다. 예를 들어 CloudTrail을 사용하면 조직 추적 또는 이벤트 데이터 스토어를 생성하여 조직 전체의 이벤트를 로깅할 수 있습니다. 조직 추적 또는 이벤트 데이터 스토어를 구성할 때 지정된 로깅 계정에서 단일 Amazon S3 버킷과 KMS 키를 지정할 수 있습니다. 이 구성은 조직의 모든 멤버 계정에 적용됩니다. 그런 다음 모든 계정은 CloudTrail 로그를 로깅 계정의 Amazon S3 버킷으로 전송하고 로그 데이터는 지정된 KMS 키로 암호화됩니다. CloudTrail에 키를 사용하는 데 필요한 권한을 부여하려면이 KMS 키에 대한 키 정책을 업데이트해야 합니다. 자세한 내용은 CloudTrail 설명서의 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.

GuardDuty 및 CloudTrail 로그를 보호하려면 Amazon S3 버킷과 KMS 키가 동일해야 합니다 AWS 리전. AWS 보안 참조 아키텍처는 로깅 및 다중 계정 아키텍처에 대한 지침도 제공합니다. 여러 리전 및

계정에서 로그를 집계할 때는 CloudTrail 설명서의 조직에 대한 추적 생성을 검토하여 옵트인 리전에 대해 자세히 알아보고 중앙 집중식 로깅이 설계된 대로 작동하는지 확인하세요.

## 암호화 기본 제공

AWS 서비스 는 일반적으로 저장 데이터 암호화를 제공합니다. 이 보안 기능은 데이터를 사용하지 않을 때 암호화하여 데이터를 보호하는 데 도움이 됩니다. 권한 있는 사용자는 필요할 때도 여전히 액세스할 수 있습니다.

구현 및 암호화 옵션은 서로 다릅니다 AWS 서비스. 많은가 기본적으로 암호화를 제공합니다. 사용하는 각 서비스에 대해 암호화가 작동하는 방식을 이해하는 것이 중요합니다. 다음은 몇 가지 예시입니다.

- Amazon Elastic Block Store(Amazon EBS) - 기본적으로 암호화를 활성화하면 모든 새 Amazon EBS 볼륨 및 스냅샷 복사본이 암호화됩니다. AWS Identity and Access Management (IAM) 역할 또는 사용자는 암호화를 지원하지 않는 암호화되지 않은 볼륨으로 인스턴스를 시작할 수 없습니다. 이 기능은 Amazon EBS 볼륨에 저장된 모든 데이터가 암호화되도록 하여 보안, 규정 준수 및 감사를 지원합니다. 이 서비스의 암호화에 대한 자세한 내용은 Amazon EBS 설명서의 Amazon EBS 암호화를 참조하세요.
- Amazon Simple Storage Service(Amazon S3) - 모든 새 객체는 기본적으로 암호화됩니다. Amazon S3는 다른 암호화 옵션을 지정하지 않는 한 각 새 객체에 대해 Amazon S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화를 자동으로 적용합니다. IAM 보안 주체는 API 호출에서 명시적으로 명시하여 암호화되지 않은 객체를 Amazon S3에 업로드할 수 있습니다. Amazon S3에서 SSE-KMS 암호화를 적용하려면 암호화가 필요한 조건이 있는 버킷 정책을 사용해야 합니다. 샘플 정책은 Amazon S3 S3 설명서의 버킷에 기록된 모든 객체에 대해 SSE-KMS 요구하기를 참조하세요. 일부 Amazon S3 버킷은 많은 수의 객체를 수신하고 제공합니다. 이러한 객체가 KMS 키로 암호화된 경우 많은 수의 Amazon S3 작업으로 인해 및가 `GenerateDataKey` `Decrypt` 호출됩니다 AWS KMS. 이렇게 하면 AWS KMS 사용량에 대해 발생하는 요금이 증가할 수 있습니다. Amazon S3 버킷 키를 구성하여 AWS KMS 비용을 크게 절감할 수 있습니다. 이 서비스의 암호화에 대한 자세한 내용은 Amazon S3 설명서의 암호화로 데이터 보호를 참조하세요.
- Amazon DynamoDB – DynamoDB는 기본적으로 서버 측 저장 데이터 암호화를 활성화하고 비활성화할 수 없는 완전 관리형 NoSQL 데이터베이스 서비스입니다. DynamoDB 테이블을 암호화하려면 고객 관리형 키를 사용하는 것이 좋습니다. 이 접근 방식을 사용하면 AWS KMS 키 정책에서 특정 IAM 사용자 및 역할을 대상으로 하여 세분화된 권한과 업무 분리를 통해 최소 권한을 구현할 수 있습니다. DynamoDB 테이블에 대한 암호화 설정을 구성할 때 AWS 관리형 키 또는 AWS 소유 키를 선택할 수도 있습니다. 높은 수준의 보호가 필요한 데이터의 경우(데이터가 클라이언트에 일반 텍스트로만 표시되어야 함) AWS Database Encryption SDK와 함께 클라이언트 측 암호화를 사용하는 것이

좋습니다. 이 서비스의 암호화에 대한 자세한 내용은 DynamoDB 설명서의 데이터 보호를 참조하세요.

## 를 사용한 데이터베이스 암호화 AWS KMS

암호화를 구현하는 수준은 데이터베이스 기능에 영향을 미칩니다. 다음은 고려해야 할 장단점입니다.

- AWS KMS 암호화만 사용하는 경우 테이블을 지원하는 스토리지는 DynamoDB 및 Amazon Relational Database Service(RDS)에 대해 암호화됩니다. DynamoDB Amazon Relational Database Service 즉, 데이터베이스를 실행하는 운영 체제는 스토리지의 콘텐츠를 일반 텍스트로 봅니다. 인덱스 생성 및 일반 텍스트 데이터에 액세스해야 하는 기타 상위 함수를 포함한 모든 데이터베이스 함수는 예상대로 계속 작동합니다.
- Amazon RDS는 Amazon Elastic Block Store(Amazon EBS) 암호화를 기반으로 구축되어 데이터베이스 볼륨에 대한 전체 디스크 암호화를 제공합니다. Amazon RDS를 사용하여 암호화된 데이터베이스 인스턴스를 생성하면 Amazon RDS는 사용자를 대신하여 암호화된 Amazon EBS 볼륨을 생성하여 데이터베이스를 저장합니다. 볼륨, 데이터베이스 스냅샷, 자동 백업 및 읽기 전용 복제본에 저장된 데이터는 모두 데이터베이스 인스턴스를 생성할 때 지정한 KMS 키로 암호화됩니다.
- Amazon Redshift는와 통합 AWS KMS 되고 데이터 수준을 통해 클러스터 수준을 암호화하는 데 사용되는 4계층 키 계층 구조를 생성합니다. 클러스터를 시작할 때 AWS KMS 암호화를 사용하도록 선택할 수 있습니다. Amazon Redshift 애플리케이션과 적절한 권한이 있는 사용자만 메모리에서 테이블이 열릴 때(및 해독될 때) 일반 텍스트를 볼 수 있습니다. 이는 일부 상용 데이터베이스에서 사용할 수 있는 투명 또는 테이블 기반 데이터 암호화(TDE) 기능과 매우 유사합니다. 즉, 인덱스 생성 및 일반 텍스트 데이터에 액세스해야 하는 기타 상위 함수를 포함한 모든 데이터베이스 함수는 예상대로 계속 작동합니다.
- AWS Database Encryption SDK(및 유사한 도구)를 통해 구현된 클라이언트 측 데이터 수준 암호화는 운영 체제와 데이터베이스 모두에 사이퍼텍스트만 표시됨을 의미합니다. 사용자는 AWS Database Encryption SDK가 설치된 클라이언트에서 데이터베이스에 액세스하고 관련 키에 액세스할 수 있는 경우에만 일반 텍스트를 볼 수 있습니다. 인덱스 생성과 같이 일반 텍스트에 대한 액세스가 의도한 대로 작동해야 하는 고차 데이터베이스 함수는 암호화된 필드에서 작동하도록 지시하면 작동하지 않습니다. 클라이언트 측 암호화를 사용하도록 선택할 때는 암호화된 데이터에 대한 일반적인 공격을 방지하는 데 도움이 되는 강력한 암호화 메커니즘을 사용해야 합니다. 여기에는 강력한 암호화 알고리즘과 솔트와 같은 적절한 기술을 사용하여 사이퍼텍스트 공격을 완화하는 것이 포함됩니다.

AWS 데이터베이스 서비스에 AWS KMS 통합 암호화 기능을 사용하는 것이 좋습니다. 민감한 데이터를 처리하는 워크로드의 경우 민감한 데이터 필드에 대해 클라이언트 측 암호화를 고려해야 합니다. 클

라이언트 측 암호화를 사용할 때는 SQL 쿼리 내 조인 또는 인덱스 생성과 같은 데이터베이스 액세스에 미치는 영향을 고려해야 합니다.

## 를 사용한 PCI DSS 데이터 암호화 AWS KMS

의 보안 및 품질 제어는 PCI DSS(지불 카드 산업 데이터 보안 표준)의 요구 사항을 충족하도록 검증되고 인증 AWS KMS 되었습니다. 즉, KMS 키로 기본 계정 번호(PAN) 데이터를 암호화할 수 있습니다. KMS 키를 사용하여 데이터를 암호화하면 암호화 라이브러리 관리의 일부 부담이 줄어듭니다. 또한 KMS 키를 내보낼 수 없으므로 암호화 키가 안전하지 않은 방식으로 저장되는 것에 대한 우려가 AWS KMS줄어듭니다.

PCI DSS 요구 사항을 충족하는 AWS KMS 데 사용할 수 있는 다른 방법이 있습니다. 예를 들어 Amazon S3와 AWS KMS 함께를 사용하는 경우 각 서비스의 액세스 제어 메커니즘이 다른 서비스와 다르기 때문에 Amazon S3에 PAN 데이터를 저장할 수 있습니다.

항상 그렇듯이 규정 준수 요구 사항을 검토할 때 적절한 경험과 자격을 갖춘 검증된 당사자로부터 조언을 얻어야 합니다. 키를 직접 사용하여 PCI DSS 범위에 속하는 카드 트랜잭션 데이터를 보호하는 애플리케이션을 설계할 때는 AWS KMS 요청 할당량에 유의하세요.

모든 AWS KMS 요청이 로그인되어 있으므로 CloudTrail 로그를 검토하여 키 사용량을 감사 AWS CloudTrail할 수 있습니다. 그러나 Amazon S3 버킷 키를 사용하는 경우 모든 Amazon S3 작업에 해당하는 항목은 없습니다. 이는 버킷 키가 Amazon S3에서 객체를 암호화하는 데 사용하는 데이터 키를 암호화하기 때문입니다. 버킷 키를 사용하면에 대한 모든 API 호출이 제거되지는 않지만 그 수가 AWS KMS줄어듭니다. 따라서 Amazon S3 객체 액세스 시도와 API 호출 간에 one-to-one 일치가 더 이상 발생하지 않습니다 AWS KMS.

## Amazon EC2 Auto Scaling에서 KMS 키 사용

Amazon EC2 Auto Scaling은 Amazon EC2 인스턴스의 규모 조정을 자동화하는 데 권장되는 서비스입니다. 이를 통해 애플리케이션의 로드를 처리하는 데 사용할 수 있는 인스턴스 수가 올바른지 확인할 수 있습니다. Amazon EC2 Auto Scaling은 서비스에 적절한 권한을 제공하고 계정 내에서 활동을 승인하는 서비스 연결 역할을 사용합니다. Amazon EC2 Auto Scaling에서 KMS 키를 사용하려면 자동화가 유용하려면 AWS KMS 키 정책`Decrypt`에서 서비스 연결 역할이와 같은 일부 API 작업에서 KMS 키를 사용하도록 허용해야 합니다. AWS KMS 키 정책이 작업을 수행하는 IAM 보안 주체에게 작업을 수행할 권한을 부여하지 않으면 해당 작업이 거부됩니다. 키 정책에서 권한을 올바르게 적용하여 액세스를 허용하는 방법에 대한 자세한 내용은 Amazon EC2 Auto Scaling 설명서의 Amazon EC2 Auto Scaling의 데이터 보호를 참조하세요. Amazon EC2 Auto Scaling

# 영향의 키 교체 AWS KMS 및 범위

규정 준수를 위해 키를 교체해야 하는 경우가 아니면 AWS Key Management Service 키 교체(AWS KMS)를 권장하지 않습니다. 예를 들어 비즈니스 정책, 계약 규칙 또는 정부 규정으로 인해 KMS 키를 교체해야 할 수 있습니다. 의 설계는 일반적으로 키 교체가 완화하는 데 사용되는 위험 유형을 AWS KMS 크게 줄입니다. KMS 키를 교체해야 하는 경우 자동 키 교체를 사용하고 자동 키 교체가 지원되지 않는 경우에만 수동 키 교체를 사용하는 것이 좋습니다.

이 섹션에서는 다음 주요 교체 주제에 대해 설명합니다.

- AWS KMS 대칭 키 교체
- Amazon EBS 볼륨의 키 교체
- Amazon RDS의 키 교체
- Amazon S3 및 동일 리전 복제의 키 교체
- 가져온 구성 요소로 KMS 키 교체

## AWS KMS 대칭 키 교체

AWS KMS 는가 AWS KMS 생성하는 키 구성 요소가 있는 대칭 암호화 KMS 키에 대해서만 자동 키 교체를 지원합니다. 고객 관리형 KMS 키의 경우 자동 교체는 선택 사항입니다. 는 매년 AWS 관리형 KMS 키의 키 구성 요소를 AWS KMS 교체합니다.는 암호화 구성 요소의 모든 이전 버전을 영구적으로 AWS KMS 저장하므로 해당 KMS 키로 암호화된 데이터를 해독할 수 있습니다.는 KMS 키를 삭제할 때까지 교체된 키 구성 요소를 삭제하지 AWS KMS 않습니다. 또한를 사용하여 객체를 복호화하면 서비스가 AWS KMS복호화 작업에 사용할 올바른 백업 구성 요소를 결정하므로 추가 입력 파라미터를 제공할 필요가 없습니다.

는 암호화 키 구성 요소의 이전 버전을 AWS KMS 유지하고 해당 구성 요소를 사용하여 데이터를 복호화할 수 있으므로 키 교체는 추가 보안 이점을 제공하지 않습니다. 키 교체 메커니즘은 규제 또는 기타 요구 사항에서 요구하는 컨텍스트에서 워크로드를 운영하는 경우 키를 더 쉽게 교체할 수 있도록 하기 위해 존재합니다.

## Amazon EBS 볼륨의 키 교체

다음 방법 중 하나를 사용하여 Amazon Elastic Block Store(Amazon EBS) 데이터 키를 교체할 수 있습니다. 접근 방식은 워크플로, 배포 방법 및 애플리케이션 아키텍처에 따라 달라집니다. 관리형 키에서 고객 관리형 키로 AWS 변경할 때이 작업을 수행할 수 있습니다.

운영 체제 도구를 사용하여 한 볼륨에서 다른 볼륨으로 데이터를 복사하려면

1. 새 KMS 키를 생성합니다. 지침은 KMS 키 생성을 참조하세요.
2. 원본과 크기가 같거나 더 큰 새 Amazon EBS 볼륨을 생성합니다. 암호화의 경우 생성한 KMS 키를 지정합니다. 지침은 Amazon EBS 볼륨 생성을 참조하세요.
3. 원래 볼륨과 동일한 인스턴스 또는 컨테이너에 새 볼륨을 마운트합니다. 지침은 Amazon EC2 인스턴스에 Amazon EBS 볼륨 연결을 참조하세요.
4. 원하는 운영 체제 도구를 사용하여 기존 볼륨의 데이터를 새 볼륨으로 복사합니다.
5. 동기화가 완료되면 사전 예약된 유지 관리 기간 동안 인스턴스에 대한 트래픽을 중지합니다. 지침은 인스턴스 수동 중지 및 시작을 참조하세요.
6. 원래 볼륨의 탑재를 해제합니다. 지침은 Amazon EC2 인스턴스에서 Amazon EBS 볼륨 분리를 참조하세요.
7. 새 볼륨을 원래 탑재 지점에 탑재합니다.
8. 새 볼륨이 올바르게 작동하는지 확인합니다.
9. 원래 볼륨을 삭제합니다. 지침은 Amazon EBS 볼륨 삭제를 참조하세요.

Amazon EBS 스냅샷을 사용하여 한 볼륨에서 다른 볼륨으로 데이터를 복사하려면

1. 새 KMS 키를 생성합니다. 지침은 KMS 키 생성을 참조하세요.
2. 원래 볼륨의 Amazon EBS 스냅샷을 생성합니다. 지침은 Amazon EBS 스냅샷 생성을 참조하세요.
3. 스냅샷에서 새 볼륨을 생성합니다. 암호화의 경우 생성한 새 KMS 키를 지정합니다. 지침은 Amazon EBS 볼륨 생성을 참조하세요.

   > **Note**
   >
   > 워크로드에 따라 Amazon EBS 빠른 스냅샷 복원을 사용하여 볼륨의 초기 지연 시간을 최소화할 수 있습니다.

4. 새 Amazon EC2 인스턴스를 생성합니다. 지침은 Amazon EC2 인스턴스 시작을 참조하세요.
5. 생성한 볼륨을 Amazon EC2 인스턴스에 연결합니다. 지침은 Amazon EC2 인스턴스에 Amazon EBS 볼륨 연결을 참조하세요.
6. 새 인스턴스를 프로덕션 환경으로 전환합니다.
7. 원래 인스턴스를 프로덕션 환경에서 교체하고 삭제합니다. 지침은 Amazon EBS 볼륨 삭제를 참조하세요.

> **Note**
>
> 스냅샷을 복사하고 대상 복사에 사용되는 암호화 키를 수정할 수 있습니다. 스냅샷을 복사하고 원하는 KMS 키로 암호화한 후 스냅샷에서 Amazon Machine Image(AMI)를 생성할 수도 있습니다. 자세한 내용은 Amazon EC2 설명서의 Amazon EBS 암호화를 참조하세요. Amazon EC2

## Amazon RDS의 키 교체

Amazon Relational Database Service(RDS)와 같은 일부 서비스의 경우 데이터 암호화는 서비스 내에서 수행되며에서 제공됩니다 AWS KMS. 다음 지침에 따라 Amazon RDS 데이터베이스 인스턴스의 키를 교체합니다.

Amazon RDS 데이터베이스의 KMS 키를 교체하려면

1. 암호화된 원본 데이터베이스의 스냅샷을 생성합니다. 지침은 Amazon RDS 설명서의 수동 백업 관리를 참조하세요.
2. 스냅샷을 새 스냅샷에 복사합니다. 암호화의 경우 새 KMS 키를 지정합니다. 지침은 Amazon RDS 용 DB 스냅샷 복사를 참조하세요.
3. 새 스냅샷을 사용하여 새 Amazon RDS 클러스터를 생성합니다. 지침은 Amazon RDS 설명서의 DB 인스턴스로 복원을 참조하세요. 기본적으로 클러스터는 새 KMS 키를 사용합니다.
4. 새 데이터베이스와 그 안에 있는 데이터의 작업을 확인합니다.
5. 새 데이터베이스를 프로덕션으로 전환합니다.
6. 이전 데이터베이스를 프로덕션 환경에서 교체하고 삭제합니다. 지침은 DB 인스턴스 삭제를 참조하세요.

## Amazon S3 및 동일 리전 복제의 키 교체

Amazon Simple Storage Service(Amazon S3)의 경우 객체의 암호화 키를 변경하려면 객체를 읽고 다시 작성해야 합니다. 객체를 다시 작성할 때 쓰기 작업에서 새 암호화 키를 명시적으로 지정합니다. 이렇게 하려면 Amazon S3 배치 작업을 사용하면 됩니다. 작업 설정 내에서 복사 작업에 대해 새 암호화 설정을 지정합니다. 예를 들어 SSE-KMS를 선택하고 keyId를 입력할 수 있습니다.

또는 Amazon S3 동일 리전 복제(SRR)를 사용할 수 있습니다. SSR은 전송 중인 객체를 다시 암호화할 수 있습니다.

## 가져온 구성 요소로 KMS 키 교체

AWS KMS 는 가져온 키 구성 요소를 복구하거나 교체하지 않습니다. 가져온 키 구성 요소가 있는 KMS 키를 교체하려면 키를 수동으로 교체해야 합니다.

# 사용에 대한 권장 사항 AWS Encryption SDK

AWS Encryption SDK는 애플리케이션에서 클라이언트 측 암호화를 구현하기 위한 강력한 도구입니다. 라이브러리는 Java, JavaScript, C, Python 및 기타 프로그래밍 언어에서 사용할 수 있습니다. ()와 통합됩니다 AWS Key Management Service AWS KMS. KMS 키를 참조하지 않고 독립 실행형 SDK로 사용할 수도 있습니다.

이 도구를 사용하는 권장 사례에는 애플리케이션의 요구 사항을 신중하게 고려하는 것이 포함됩니다. 애플리케이션에 키 캐싱을 도입하는 등 특정 구성에서 발생할 수 있는 위험과 이러한 요구 사항의 균형을 맞춥니다. 데이터 키 캐싱에 대한 자세한 내용은 AWS Encryption SDK 설명서의 데이터 키 캐싱을 참조하세요.

를 사용할지 여부를 결정할 때 AWS Encryption SDK다음 질문을 고려하세요.

- 와 통합되는 서비스를 사용한 서버 측 암호화로는 충족할 수 없는 클라이언트 측 암호화 요구 사항이 있나요 AWS KMS?
- 데이터 클라이언트 측을 암호화하는 데 사용되는 키를 적절하게 보호할 수 있습니까? 어떻게 해야 합니까?
- 사용 사례에 더 적합할 수 있는 다른 fit-for-purpose 암호화 라이브러리가 있나요? Amazon S3 클라이언트 측 암호화 및 AWS Database Encryption SDK와 같은 대체 AWS 제품을 고려합니다.

사용 사례에 적합한 서비스를 선택하는 방법에 대한 자세한 내용은 AWS Crypto 도구 설명서를 참조하세요.

# 에 대한 자격 증명 및 액세스 관리 모범 사례 AWS KMS

AWS Key Management Service (AWS KMS)를 사용하려면가 요청을 인증하고 승인하는 데 사용할 AWS 수 있는 자격 증명이 있어야 합니다. 명시적으로 제공되고 거부되지 않는 한 보안 AWS 주체는 KMS 키에 대한 권한이 없습니다. KMS 키를 사용하거나 관리할 수 있는 암시적 또는 자동 권한은 없습니다. 이 섹션의 주제에서는 인프라를 보호하는 데 사용해야 하는 AWS KMS 액세스 관리 제어를 결정하는 데 도움이 되는 보안 모범 사례를 정의합니다.

이 섹션에서는 다음 자격 증명 및 액세스 관리 주제에 대해 설명합니다.

- AWS KMS 키 정책 및 IAM 정책
- 에 대한 최소 권한 AWS KMS
- 에 대한 역할 기반 액세스 제어 AWS KMS
- 에 대한 속성 기반 액세스 제어 AWS KMS
- 에 대한 암호화 컨텍스트 AWS KMS
- AWS KMS 권한 문제 해결

## AWS KMS 키 정책 및 IAM 정책

AWS KMS 리소스에 대한 액세스를 관리하는 주요 방법은 정책을 사용하는 것입니다. 정책은 어떤 보안 주체가 어떤 리소스에 액세스 할 수 있는지를 설명하는 문서입니다. AWS Identity and Access Management (IAM) 자격 증명(사용자, 사용자 그룹 또는 역할)에 연결된 정책을 자격 증명 기반 정책이라고 합니다. 리소스에 연결하는 IAM 정책을 리소스 기반 정책이라고 합니다. KMS 키에 대한 AWS KMS 리소스 정책을 키 정책이라고 합니다. 는 IAM 정책 및 AWS KMS 키 정책 AWS KMS 외에도 권한 부여를 지원합니다. 권한 부여는 권한을 위임하는 유연하고 강력한 방법을 제공합니다. 권한 부여를 사용하여 AWS 계정 또는 다른의 IAM 보안 주체에 시간 제한 KMS 키 액세스 권한을 부여할 수 있습니다 AWS 계정.

모든 KMS 키에는 키 정책이 있습니다. 제공하지 않으면 AWS KMS 에서 자동으로 생성합니다. 에서 AWS KMS 사용하는 기본 키 정책은 AWS KMS 콘솔을 사용하여 키를 생성하는지 아니면 AWS KMS API를 사용하는지에 따라 다릅니다. 조직의 최소 권한 요구 사항에 맞게 기본 키 정책을 편집하는 것이 좋습니다. 또한 이는 IAM 정책을 키 정책과 함께 사용하기 위한 전략과 일치해야 합니다. 에서 IAM 정책을 사용하는 방법에 대한 자세한 권장 사항은 AWS KMS 설명서의 IAM 정책 모범 사례를 AWS KMS 참조하세요.

키 정책을 사용하여 IAM 보안 주체에 대한 권한 부여를 자격 증명 기반 정책에 위임할 수 있습니다. 키 정책을 사용하여 자격 증명 기반 정책과 함께 권한 부여를 세분화할 수도 있습니다. 어느 경우든 서비

스 제어 정책(SCPs), 리소스 제어 정책(RCPs) 또는 권한 경계와 같이 액세스 범위를 지정하는 기타 적용 가능한 정책과 함께 키 정책 및 자격 증명 기반 정책 모두 액세스를 결정합니다. 보안 주체가 KMS 키와 다른 계정에 있는 경우 기본적으로 암호화 및 권한 부여 작업만 지원됩니다. 이 교차 계정 시나리오에 대한 자세한 내용은 설명서의 다른 계정의 사용자가 KMS 키를 사용하도록 허용을 참조하세요 AWS KMS .

KMS 키에 대한 액세스를 제어하려면 IAM 자격 증명 기반 정책을 키 정책과 함께 사용해야 합니다. 권한 부여는 이러한 정책과 함께 사용하여 KMS 키에 대한 액세스를 제어할 수도 있습니다. 자격 증명 기반 정책을 사용하여 KMS 키에 대한 액세스를 제어하려면 키 정책에서 계정이 자격 증명 기반 정책을 사용하도록 허용해야 합니다. IAM 정책을 활성화하는 키 정책 문을 지정하거나 키 정책에서 허용되는 위탁자를 명시적으로 지정할 수 있습니다.

정책을 작성할 때는 다음 작업을 수행할 수 있는 사용자를 제한하는 강력한 제어가 있어야 합니다.

- IAM 정책 및 KMS 키 정책 업데이트, 생성 및 삭제
- 사용자, 역할 및 그룹에서 자격 증명 기반 정책 연결 및 분리
- KMS AWS KMS 키에서 키 정책 연결 및 분리
- KMS 키에 대한 권한 부여 생성 - 키 정책을 통해서만 KMS 키에 대한 액세스를 제어하든 IAM 정책과 키 정책을 결합하든 정책을 수정할 수 있는 기능을 제한해야 합니다. 기존 정책을 변경하기 위한 승인 프로세스를 구현합니다. 승인 프로세스는 다음을 방지하는 데 도움이 될 수 있습니다.
  - 우발적인 IAM 보안 주체 권한 손실 - IAM 보안 주체가 키를 관리하거나 암호화 작업에 사용할 수 없도록 변경할 수 있습니다. 극단적인 시나리오에서는 모든 사용자의 키 관리 권한을 취소할 수 있습니다. 이 경우에 문의하여 키에 AWS Support 다시 액세스해야 합니다.
  - KMS 키 정책에 대한 승인되지 않은 변경 사항 - 승인되지 않은 사용자가 키 정책에 액세스할 수 있는 경우 의도하지 않은 AWS 계정 또는 보안 주체에게 권한을 위임하도록 수정할 수 있습니다.
  - IAM 정책에 대한 승인되지 않은 변경 사항 - 권한이 없는 사용자가 그룹 멤버십을 관리할 수 있는 권한이 있는 자격 증명 세트를 획득하면 자신의 권한을 높이고 IAM 정책, 키 정책, KMS 키 구성 또는 기타 AWS 리소스 구성을 변경할 수 있습니다.

KMS 키 관리자로 지정된 IAM 보안 주체와 연결된 IAM 역할 및 사용자를 주의 깊게 검토합니다. 이렇게 하면 무단 삭제 또는 변경을 방지하는 데 도움이 될 수 있습니다. KMS 키에 액세스할 수 있는 보안 주체를 변경해야 하는 경우 새 관리자 보안 주체가 모든 필수 키 정책에 추가되었는지 확인합니다. 이전 관리 보안 주체를 삭제하기 전에 권한을 테스트합니다. 모든 IAM 보안 모범 사례를 따르고 장기 자격 증명 대신 임시 자격 증명을 사용하는 것이 좋습니다.

정책이 생성될 때 보안 주체의 이름을 모르거나 액세스가 필요한 보안 주체가 자주 변경되는 경우 권한 부여를 통해 시간 제한 액세스 권한을 부여하는 것이 좋습니다. 피부여자 보안 주체는 KMS 키와 동일

한 계정 또는 다른 계정에 있을 수 있습니다. 보안 주체 키와 KMS 키가 서로 다른 계정에 있는 경우 권한 부여 외에 자격 증명 기반 정책을 지정해야 합니다. API를 직접 호출하여 권한 부여를 생성하고 더 이상 필요하지 않을 때 권한 부여를 사용 중지하거나 취소해야 하기 때문에 권한 부여에는 추가 관리가 필요합니다.

계정 루트 사용자 또는 키 생성자를 포함한 보안 AWS 주체는 키 정책, IAM 정책 또는 권한 부여에서 명시적으로 허용되고 명시적으로 거부되지 않는 한 KMS 키에 대한 권한이 없습니다. 확장을 통해 사용자가 KMS 키를 사용하기 위해 의도하지 않은 액세스 권한을 얻는 경우 발생할 수 있는 상황과 그 영향을 고려해야 합니다. 이러한 위험을 완화하려면 다음을 고려하세요.

- 데이터 범주마다 다른 KMS 키를 유지할 수 있습니다. 이렇게 하면 키를 분리하고 해당 데이터 범주에 대한 보안 주체 액세스를 특별히 대상으로 하는 정책 설명이 포함된 보다 간결한 키 정책을 유지할 수 있습니다. 또한 관련 IAM 자격 증명에 의도하지 않게 액세스하는 경우 해당 액세스에 연결된 자격 증명은 IAM 정책에 지정된 키에만 액세스할 수 있으며 키 정책이 해당 보안 주체에 대한 액세스를 허용하는 경우에만 액세스할 수 있습니다.
- 의도하지 않은 키 액세스 권한이 있는 사용자가 데이터에 액세스할 수 있는지 평가할 수 있습니다. 예를 들어 Amazon Simple Storage Service(Amazon S3)를 사용하면 사용자에게 Amazon S3의 암호화된 객체에 액세스할 수 있는 적절한 권한도 있어야 합니다. 또는 사용자에게 KMS 키로 암호화된 볼륨이 있는 Amazon EC2 인스턴스에 대한 의도하지 않은 액세스 권한(RDP 또는 SSH 사용)이 있는 경우 사용자는 운영 체제 도구를 사용하여 데이터에 액세스할 수 있습니다.

> **Note**
>
> AWS 서비스 를 사용하는는 사용자에게 사이퍼텍스트를 노출하지 AWS KMS 않습니다(암호 분석에 대한 최신 접근 방식에는 사이퍼텍스트에 대한 액세스 권한이 필요합니다). 또한 AWS 데이터 센터 외부의 물리적 검사에는 사이퍼텍스트를 사용할 수 없습니다. NIST SP800-88 요구 사항에 따라 모든 스토리지 미디어가 폐기될 때 물리적으로 파괴되기 때문입니다.

## 에 대한 최소 권한 AWS KMS

KMS 키는 민감한 정보를 보호하므로 최소 권한 액세스 원칙을 따르는 것이 좋습니다. 키 정책을 정의할 때 작업을 수행하는 데 필요한 최소 권한을 위임합니다. 추가 자격 증명 기반 정책으로 권한을 추가로 제한하려는 경우에만 KMS 키 정책에 대한 모든 작업(`kms:*`)을 허용합니다. 자격 증명 기반 정책을 사용하여 권한을 관리하려는 경우 IAM 정책을 생성하여 IAM 보안 주체에 연결하고 정책 변경을 모니터링할 수 있는 사용자를 제한합니다.

키 정책과 자격 증명 기반 정책 모두에서 모든 작업(`kms:*`)을 허용하는 경우 보안 주체는 KMS 키에 대한 관리 및 사용 권한을 모두 갖습니다. 보안 모범 사례로 이러한 권한을 특정 보안 주체에게만 위임하는 것이 좋습니다. 키를 관리할 보안 주체와 키를 사용할 보안 주체에 권한을 할당하는 방법을 고려합니다. 키 정책에서 보안 주체의 이름을 명시적으로 지정하거나 자격 증명 기반 정책이 연결되는 보안 주체를 제한하여이 작업을 수행할 수 있습니다. 조건 키를 사용하여 권한을 제한할 수도 있습니다. 예를 들어 API 호출을 수행하는 보안 주체에 조건 규칙에 지정된 태그가 있는 경우 aws:PrincipalTag를 사용하여 모든 작업을 허용할 수 있습니다.

정책 설명이 평가되는 방식을 이해하는 데 도움이 필요하면 IAM 설명서의 정책 평가 로직을 AWS참조하세요. 정책을 작성하기 전에이 주제를 검토하여 액세스 권한이 없는 보안 주체에게 액세스 권한을 제공하는 등 정책에 의도하지 않은 영향이 있을 가능성을 줄이는 것이 좋습니다.

> **Tip**
>
> 비프로덕션 환경에서 애플리케이션을 테스트할 때는 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)를 사용하여 IAM 정책에 최소 권한 권한을 적용할 수 있습니다.

IAM 역할 대신 IAM 사용자를 사용하는 경우 장기 자격 증명의 취약성을 완화하기 위해 AWS 다중 인증(MFA)을 사용하는 것이 좋습니다. MFA를 사용하여 다음을 수행할 수 있습니다.

- 사용자에게 키 삭제 예약과 같은 권한 있는 작업을 수행하기 전에 MFA를 사용하여 자격 증명을 검증하도록 요구합니다.
- 관리자 계정 암호 및 MFA 디바이스의 소유권을 개인 간에 분할하여 분할 권한 부여를 구현합니다.

최소 권한 구성에 도움이 되는 샘플 정책은 AWS KMS 설명서의 IAM 정책 예제를 참조하세요.

## 에 대한 역할 기반 액세스 제어 AWS KMS

역할 기반 액세스 제어(RBAC)는 사용자에게 직무 수행에 필요한 권한만 제공하는 권한 부여 전략입니다. 최소 권한 원칙을 구현하는 데 도움이 되는 접근 방식입니다.

AWS KMS 는 RBAC를 지원합니다. 이를 통해 키 정책 내에서 세분화된 권한을 지정하여 키에 대한 액세스를 제어할 수 있습니다. 키 정책은 키에 대한 액세스 권한을 부여하는 리소스, 작업, 효과, 위탁자 및 선택적 조건을 지정합니다. 에서 RBAC를 구현하려면 키 사용자와 키 관리자에 대한 권한을 분리하는 AWS KMS것이 좋습니다.

키 사용자의 경우 사용자에게 필요한 권한만 할당합니다. 다음 질문을 사용하면 권한을 더욱 구체화하는 데 도움이 됩니다.

- 어떤 IAM 보안 주체가 키에 액세스해야 합니까?
- 각 위탁자가 키로 수행해야 하는 작업은 무엇인가요? 예를 들어 보안 주체에게 `Encrypt` 및 `Sign` 권한만 필요합니까?
- 보안 주체가 액세스해야 하는 리소스는 무엇입니까?
- 개체가 인간입니까, 아니면 입니까 AWS 서비스? 서비스인 경우 kms:ViaService 조건 키를 사용하여 키 사용을 특정 서비스로 제한할 수 있습니다.

키 관리자의 경우 관리자에게 필요한 권한만 할당합니다. 예를 들어 관리자의 권한은 키가 테스트 환경에서 사용되는지 프로덕션 환경에서 사용되는지에 따라 달라질 수 있습니다. 특정 비프로덕션 환경에서 덜 제한적인 권한을 사용하는 경우 정책을 프로덕션으로 릴리스하기 전에 테스트하는 프로세스를 구현합니다.

키 사용자 및 관리자에 대한 역할 기반 액세스 제어를 구성하는 데 도움이 되는 샘플 정책은 RBAC for AWS KMS 섹션을 참조하세요.

## 에 대한 속성 기반 액세스 제어 AWS KMS

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. RBAC와 마찬가지로 최소 권한 원칙을 구현하는 데 도움이 되는 접근 방식입니다.

AWS KMS 는 KMS 키와 같은 대상 리소스와 연결된 태그 및 API 호출을 수행하는 보안 주체와 연결된 태그를 기반으로 권한을 정의할 수 있도록 하여 ABAC를 지원합니다. 에서는 태그와 AWS KMS별칭을 사용하여 고객 관리형 키에 대한 액세스를 제어할 수 있습니다. 예를 들어, 보안 주체의 태그가 KMS 키와 연결된 태그와 일치할 때 작업을 허용하는 태그 조건 키를 사용하는 IAM 정책을 정의할 수 있습니다. 자습서는 설명서의 태그를 기반으로 AWS 리소스에 액세스할 수 있는 권한 정의를 참조하세요 AWS KMS .

가장 좋은 방법은 ABAC 전략을 사용하여 IAM 정책 관리를 간소화하는 것입니다. ABAC를 사용하면 관리자는 태그를 사용하여 기존 정책을 업데이트하는 대신 새 리소스에 대한 액세스를 허용할 수 있습니다. 다양한 직무에 대해 다른 정책을 생성할 필요가 없으므로 ABAC에는 더 적은 정책이 필요합니다. 자세한 내용은 IAM 설명서의 기존 RBAC 모델과 ABAC 비교를 참조하세요.

최소 권한의 모범 사례를 ABAC 모델에 적용합니다. IAM 보안 주체에게 작업을 수행하는 데 필요한 권한만 제공합니다. 사용자가 역할 및 리소스의 태그를 수정할 수 있도록 태깅 APIs에 대한 액세스를 신

중하게 제어합니다. 키 별칭 조건 키를 사용하여에서 ABAC를 지원하는 경우 키를 생성하고 별칭을 수정할 수 있는 사용자를 제한하는 강력한 제어 기능 AWS KMS도 있어야 합니다.

태그를 사용하여 특정 키를 비즈니스 범주에 연결하고 특정 작업에 올바른 키가 사용되고 있는지 확인할 수도 있습니다. 예를 들어 AWS CloudTrail 로그를 사용하여 특정 AWS KMS 작업을 수행하는 데 사용되는 키가 사용 중인 리소스와 동일한 비즈니스 범주에 속하는지 확인할 수 있습니다.

> **Warning**
>
> 태그 키 또는 태그 값에 기밀 또는 민감한 정보를 포함하지 마세요. 태그는 암호화되지 않습니다. 결제를 AWS 서비스포함하여 많은 사용자가 액세스할 수 있습니다.

액세스 제어에 대한 ABAC 접근 방식을 구현하기 전에 사용하는 다른 서비스가이 접근 방식을 지원하는지 고려하세요. ABAC를 지원하는 서비스를 결정하는 데 도움이 필요하면 AWS 서비스 IAM 설명서에서 IAM으로 작업하는를 참조하세요.

용 ABAC 구현 AWS KMS 및 정책 구성에 도움이 될 수 있는 조건 키에 대한 자세한 내용은 ABAC for AWS KMS 섹션을 참조하세요.

## 에 대한 암호화 컨텍스트 AWS KMS

대칭 AWS KMS 암호화 KMS 키를 사용하는 모든 암호화 작업은 암호화 컨텍스트를 허용합니다. 암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함할 수 있는 비밀이 아닌 키-값 페어의 선택적 집합입니다. 가장 좋은 방법은의 `Encrypt` 작업에 암호화 컨텍스트를 삽입 AWS KMS 하여에 대한 복호화 API 호출의 권한 부여 및 감사 가능성을 개선할 수 있습니다 AWS KMS.는 암호화 컨텍스트를 인증된 암호화를 지원하기 위한 추가 인증 데이터(AAD)로 AWS KMS 사용합니다. 암호화 컨텍스트는 사이퍼텍스트에 암호적으로 바인딩되므로 데이터를 복호화하는 데 동일한 암호화 컨텍스트가 필요합니다.

암호화 컨텍스트는 암호가 아니며 암호화되지 않습니다. AWS CloudTrail 로그에 일반 텍스트로 표시되므로 이를 사용하여 암호화 작업을 식별하고 분류할 수 있습니다. 암호화 컨텍스트는 비밀이 아니므로 승인된 보안 주체만 CloudTrail 로그 데이터에 액세스하도록 허용해야 합니다.

또한 kms:EncryptionContext:context-key 및 kms:EncryptionContextKeys 조건 키를 사용하여 암호화 컨텍스트를 기반으로 대칭 암호화 KMS 키에 대한 액세스를 제어할 수 있습니다. 또한 이러한 조건 키를 사용하여 암호화 작업에 암호화 컨텍스트를 사용하도록 요구할 수 있습니다. 이러한 조건 키의 경우 정책이 의도한 권한을 반영하는지 확인하기 위해의 사용에 대한 지침을 검토`ForAnyValue`하거나 연산자를 `ForAllValues` 설정합니다.

# AWS KMS 권한 문제 해결

KMS 키에 대한 액세스 제어 정책을 작성할 때는 IAM 정책과 키 정책이 어떻게 함께 작동하는지 고려합니다. 보안 주체에 대한 유효 권한은 모든 유효 정책에 의해 부여(명시적으로 거부되지 않음)되는 권한입니다. 계정 내에서 KMS 키에 대한 권한은 IAM 자격 증명 기반 정책, 키 정책, 권한 경계, 서비스 제어 정책 또는 세션 정책의 영향을 받을 수 있습니다. 예를 들어 자격 증명 기반 정책과 키 정책을 모두 사용하여 KMS 키에 대한 액세스를 제어하는 경우 보안 주체 및 리소스와 관련된 모든 정책을 평가하여 지정된 작업을 수행할 수 있는 보안 주체의 권한을 결정합니다. 자세한 내용은 IAM 설명서의 정책 평가 로직을 참조하세요.

키 액세스 문제 해결을 위한 자세한 내용과 흐름도는 AWS KMS 설명서의 키 액세스 문제 해결을 참조하세요.

액세스 거부 오류 메시지 문제를 해결하려면

1. IAM 자격 증명 기반 정책 및 KMS 키 정책이 액세스를 허용하는지 확인합니다.
2. IAM의 권한 경계가 액세스를 제한하지 않는지 확인합니다.
3. 의 서비스 제어 정책(SCP) 또는 리소스 제어 정책(RCP) AWS Organizations 이 액세스를 제한하지 않는지 확인합니다.
4. VPC 엔드포인트를 사용하는 경우 엔드포인트 정책이 올바른지 확인합니다.
5. 자격 증명 기반 정책 및 키 정책에서 키에 대한 액세스를 제한하는 조건 또는 리소스 참조를 제거합니다. 이러한 제한을 제거한 후 보안 주체가 이전에 실패한 API를 성공적으로 호출할 수 있는지 확인합니다. 성공한 경우 조건과 리소스 참조를 한 번에 하나씩 다시 적용하고 그 후에 보안 주체가 여전히 액세스할 수 있는지 확인합니다. 이렇게 하면 오류를 일으키는 조건 또는 리소스 참조를 식별하는 데 도움이 됩니다.

자세한 내용은 IAM 설명서의 액세스 거부 오류 메시지 문제 해결을 참조하세요.

# 에 대한 탐지 및 모니터링 모범 사례 AWS KMS

탐지 및 모니터링은 AWS Key Management Service (AWS KMS) 키의 가용성, 상태 및 사용량을 이해하는 데 중요한 부분입니다. 모니터링은 AWS 솔루션의 보안, 신뢰성, 가용성 및 성능을 유지하는 데 도움이 됩니다.는 KMS 키 및 AWS KMS 작업을 모니터링하기 위한 여러 도구를 AWS 제공합니다. 이 섹션에서는 이러한 도구를 구성하고 사용하여 환경에 대한 가시성을 높이고 KMS 키 사용을 모니터링하는 방법을 설명합니다.

이 섹션에서는 다음 탐지 및 모니터링 주제에 대해 설명합니다.

- 를 사용하여 AWS KMS 작업 모니터링 AWS CloudTrail
- IAM Access Analyzer를 사용하여 KMS 키에 대한 액세스 모니터링
- 를 AWS 서비스 사용하여 다른의 암호화 설정 모니터링 AWS Config
- Amazon CloudWatch 경보를 사용하여 KMS 키 모니터링
- Amazon EventBridge를 사용하여 응답 자동화

## 를 사용하여 AWS KMS 작업 모니터링 AWS CloudTrail

AWS KMS 는 사용자, 역할 및 기타에 AWS KMS 의해에 대한 모든 호출을 기록할 수 있는 서비스AWS CloudTrail인와 통합됩니다 AWS 서비스. CloudTrail은 AWS KMS 콘솔, API, AWS Command Line Interface (AWS CLI) 및의 호출을 포함하여 AWS CloudFormation에 대한 모든 AWS KMS APIs 호출을 이벤트 AWS KMS 로 캡처합니다 AWS Tools for PowerShell.

CloudTrail은 `ListAliases` 및와 같은 읽기 전용 AWS KMS 작업을 포함한 모든 작업을 로깅합니다`GetKeyRotationStatus`. 또한 `CreateKey` `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey` 및와 같은 KMS 키를 관리하는 작업도 로깅합니다`Decrypt`. 또한 `DeleteExpiredKeyMaterial`, , 및와 같이 `DeleteKey`가 자동으로 AWS KMS 호출하는 내부 작업을 로깅`SynchronizeMultiRegionKey`합니다`RotateKey`.

CloudTrail은 생성할 AWS 계정 때에서 활성화됩니다. 기본적으로 이벤트 기록은에서 지난 90일간 기록된 관리-이벤트 API 활동을 보고, 검색하고, 다운로드하고, 변경할 수 없는 레코드를 제공합니다 AWS 리전. 90일 이상 KMS 키 사용을 모니터링하거나 감사하려면에 대한 CloudTrail 추적을 생성하는 것이 좋습니다 AWS 계정. 에서 조직을 생성한 경우 AWS Organizations조직 추적 또는 해당 조직의 모든 AWS 계정 에 대한 이벤트를 로깅하는 이벤트 데이터 스토어를 생성할 수 있습니다.

계정 또는 조직에 대한 추적을 설정한 후 다른 AWS 서비스 를 사용하여 추적에 로깅된 이벤트를 저장, 분석 및 자동으로 응답할 수 있습니다. 예를 들어, 다음을 수행할 수 있습니다.

- 추적의 특정 이벤트를 알리는 Amazon CloudWatch 경보를 설정할 수 있습니다. 자세한 내용은 이 안내서의 Amazon CloudWatch 경보를 사용하여 KMS 키 모니터링 섹션을 참조하세요.
- 추적에서 이벤트가 발생할 때 작업을 자동으로 수행하는 Amazon EventBridge 규칙을 생성할 수 있습니다. 자세한 내용은이 가이드의 Amazon EventBridge를 사용한 응답 자동화를 참조하세요.
- Amazon Security Lake를 사용하여 CloudTrail을 AWS 서비스포함한 여러에서 로그를 수집하고 저장할 수 있습니다. 자세한 내용은 Amazon Security Lake 설명서 AWS 서비스 의 Security Lake에서 데이터 수집을 참조하세요.
- 운영 활동 분석을 개선하기 위해 Amazon Athena를 사용하여 CloudTrail 로그를 쿼리할 수 있습니다. 자세한 내용은 Amazon Athena 설명서의 쿼리 AWS CloudTrail 로그를 참조하세요.

CloudTrail을 사용한 AWS KMS 모니터링 작업에 대한 자세한 내용은 다음을 참조하세요.

- 를 사용하여 API 호출 로깅 AWS KMSAWS CloudTrail
- AWS KMS 로그 항목의 예
- Amazon EventBridge를 사용하여 KMS 키 모니터링
- Amazon EventBridge와 CloudTrail 통합

## IAM Access Analyzer를 사용하여 KMS 키에 대한 액세스 모니터링

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)를 사용하면 외부 엔터티와 공유되는 조직 및 계정의 리소스(예: KMS 키)를 식별할 수 있습니다. 이 서비스는 리소스 및 데이터에 대한 의도하지 않거나 지나치게 광범위한 액세스를 식별하는 데 도움이 될 수 있으며, 이는 보안 위험입니다. IAM Access Analyzer는 로직 기반 추론을 사용하여 AWS 환경의 리소스 기반 정책을 분석하여 외부 보안 주체와 공유되는 리소스를 식별합니다.

IAM Access Analyzer를 사용하여 KMS 키에 액세스할 수 있는 외부 엔터티를 식별할 수 있습니다. IAM Access Analyzer를 활성화하면 전체 조직 또는 대상 계정에 대한 분석기를 생성합니다. 선택한 조직 또는 계정을 분석기의 신뢰 영역이라고 합니다. 분석기는 신뢰 영역 내에서 지원되는 리소스를 모니터링합니다. 신뢰 영역 내의 보안 주체가 리소스에 액세스하는 것은 신뢰할 수 있는 것으로 간주됩니다.

KMS 키의 경우 IAM Access Analyzer는 키에 적용된 키 정책 및 권한 부여를 분석합니다. 키 정책 또는 권한 부여가 외부 엔터티가 키에 액세스하도록 허용하는 경우 결과를 생성합니다. IAM Access Analyzer를 사용하여 외부 엔터티가 KMS 키에 액세스할 수 있는지 확인한 다음 해당 엔터티에 액세스 권한이 있는지 확인합니다.

IAM Access Analyzer를 사용하여 KMS 키 액세스를 모니터링하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- AWS Identity and Access Management Access Analyzer사용
- 외부 액세스를 위한 IAM Access Analyzer 리소스 유형
- IAM Access Analyzer 리소스 유형: AWS KMS keys
- 외부 및 미사용 액세스에 대한 조사 결과

## 를 AWS 서비스 사용하여 다른의 암호화 설정 모니터링 AWS Config

AWS Config는의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다 AWS 계정. AWS Config 를 사용하여 KMS 키를 AWS 서비스 사용하는에 암호화 설정이 적절하게 구성되어 있는지 확인할 수 있습니다. 예를 들어 암호화된 볼륨 AWS Config 규칙을 사용하여 Amazon Elastic Block Store(Amazon EBS) 볼륨이 암호화되었는지 확인할 수 있습니다.

AWS Config 에는 리소스를 평가할 규칙을 빠르게 선택하는 데 도움이 되는 관리형 규칙이 포함되어 있습니다. 에서 필요한 관리형 규칙이 해당 리전에서 지원되는지 AWS Config AWS 리전 확인합니다. 사용 가능한 관리형 규칙에는 Amazon Relational Database Service(RDS) 스냅샷 구성, CloudTrail 추적 암호화, Amazon Simple Storage Service(Amazon S3) 버킷의 기본 암호화, Amazon DynamoDB 테이블 암호화 등에 대한 검사가 포함됩니다.

사용자 지정 규칙을 생성하고 비즈니스 로직을 적용하여 리소스가 요구 사항을 준수하는지 확인할 수도 있습니다. 여러 관리형 규칙의 오픈 소스 코드는 GitHub의 AWS Config 규칙 리포지토리에서 사용할 수 있습니다. 이는 사용자 지정 규칙을 개발하는 데 유용한 출발점이 될 수 있습니다.

리소스가 규칙을 준수하지 않는 경우 대응 작업을 시작할 수 있습니다. AWS Config 에는 AWS Systems Manager 자동화가 수행하는 문제 해결 작업이 포함되어 있습니다. 예를 들어 cloud-trail-encryption-enabled 규칙을 적용하고 규칙이 `NON_COMPLIANT` 결과를 반환하는 경우 AWS Config 는 CloudTrail 로그를 암호화하여 문제를 해결하는 자동화 문서를 시작할 수 있습니다.

AWS Config 를 사용하면 리소스를 프로비저닝하기 전에 AWS Config 규칙 준수를 사전에 확인할 수 있습니다. 사전 예방적 모드에서 규칙을 적용하면 클라우드 리소스가 생성되거나 업데이트되기 전에 구성을 평가하는 데 도움이 됩니다. 배포 파이프라인의 일부로 사전 예방적 모드에서 규칙을 적용하면 리소스를 배포하기 전에 리소스 구성을 테스트할 수 있습니다.

를 통해 AWS Config 규칙을 제어로 구현할 수도 있습니다AWS Security Hub. Security Hub는에 적용할 수 있는 보안 표준을 제공합니다 AWS 계정. 이러한 표준은 권장 사례를 기준으로 환경을 평가하는

데 도움이 됩니다. AWS 기본 보안 모범 사례 표준에는 저장 데이터 암호화가 구성되어 있고 KMS 키 정책이 권장 사례를 따르는지 확인하기 위한 보호 제어 범주 내의 제어가 포함되어 있습니다.

를 사용하여의 암호화 설정을 모니터링하는 AWS Config 방법에 대한 자세한 내용은 다음을 AWS 서비스참조하세요.

- AWS Config시작하기
- AWS Config 관리형 규칙
- AWS Config 사용자 지정 규칙
- 를 사용하여 규정 미준수 리소스 문제 해결 AWS Config

## Amazon CloudWatch 경보를 사용하여 KMS 키 모니터링

Amazon CloudWatch는 AWS 리소스와 AWS 에서 실행하는 애플리케이션을 실시간으로 모니터링합니다. CloudWatch를 사용하여 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.

가져온 키 구성 요소의 만료 또는 키 삭제는 의도하지 않거나 제대로 계획되지 않은 경우 잠재적으로 치명적인 이벤트입니다. 이러한 이벤트가 발생하기 전에 알리도록 CloudWatch 경보를 구성하는 것이 좋습니다. 또한 중요한 키가 삭제되지 않도록 AWS Identity and Access Management (IAM) 정책 또는 AWS Organizations 서비스 제어 정책(SCPs)을 구성하는 것이 좋습니다.

CloudWatch 경보는 키 삭제 취소와 같은 수정 조치 또는 삭제되거나 만료된 키 구성 요소 다시 가져오기와 같은 수정 조치를 취하는 데 도움이 됩니다.

## Amazon EventBridge를 사용하여 응답 자동화

Amazon EventBridge를 사용하여 KMS 키에 영향을 미치는 중요한 이벤트를 알릴 수도 있습니다. EventBridge는 AWS 리소스에 대한 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 AWS 서비스 제공하는 입니다. EventBridge는 CloudTrail 및 Security Hub에서 이벤트를 자동으로 수신합니다. EventBridge에서는 CloudTrail에서 기록한 이벤트에 응답하는 규칙을 생성할 수 있습니다.

AWS KMS 이벤트에는 다음이 포함됩니다.

- KMS 키의 키 구성 요소가 자동으로 교체되었습니다.
- KMS 키에서 가져온 키 구성 요소가 만료됨
- 삭제가 예약된 KMS 키가 삭제되었습니다.

이러한 이벤트는에서 추가 작업을 시작할 수 있습니다 AWS 계정. 이러한 작업은 이벤트가 발생한 후에만 조치를 취할 수 있으므로 이전 섹션에 설명된 CloudWatch 경보와 다릅니다. 예를 들어 해당 키가 삭제된 후 특정 키에 연결된 리소스를 삭제하거나 규정 준수 또는 감사 팀에 키가 삭제되었음을 알릴 수 있습니다.

EventBridge를 사용하여 CloudTrail에 로깅된 다른 API 이벤트를 필터링할 수도 있습니다. 즉, 주요 정책 관련 API 작업이 특별히 우려되는 경우 이를 필터링할 수 있습니다. 예를 들어 EventBridge에서 `PutKeyPolicy` API 작업을 필터링할 수 있습니다. 보다 광범위하게 또는 로 시작하는 API 작업을 필터링`Disable*Delete*`하여 자동 응답을 시작할 수 있습니다.

EventBridge를 사용하면 (감지 제어)를 모니터링하고 (응답 제어)를 조사하여 예기치 않거나 선택한 이벤트에 대응할 수 있습니다. 예를 들어 IAM 사용자 또는 역할이 생성되거나 KMS 키가 생성되거나 키 정책이 변경될 경우 보안 팀에 알리고 특정 조치를 취할 수 있습니다. 지정한 API 작업을 필터링한 다음 대상을 규칙에 연결하는 EventBridge 이벤트 규칙을 생성할 수 있습니다. 대상의 예로는 AWS Lambda 함수, Amazon Simple Notification Service(Amazon SNS) 알림, Amazon Simple Queue Service(Amazon SQS) 대기열 등이 있습니다. 대상으로 이벤트를 보내는 방법에 대한 자세한 내용은 Amazon EventBridge의 이벤트 버스 대상을 참조하세요.

EventBridge를 AWS KMS 사용한 모니터링 및 응답 자동화에 대한 자세한 내용은 AWS KMS 설명서의 Amazon EventBridge를 사용한 KMS 키 모니터링을 참조하세요.

# 에 대한 비용 및 결제 관리 모범 사례 AWS KMS

폭과 깊이를 통해 비즈니스 요구 사항을 충족하면서 비용을 관리할 수 있는 유연성을 AWS 서비스 제공합니다. 이 섹션에서는 (AWS KMS)의 AWS Key Management Service 키 스토리지 요금을 다루며, 키 캐싱을 통한 비용 절감을 위한 권장 사항을 제공합니다. KMS 키 사용량을 검토하여 비용을 절감할 추가 기회가 있는지 확인할 수도 있습니다.

이 섹션에서는 다음 비용 및 결제 관리 주제에 대해 설명합니다.

- AWS KMS 키 스토리지 요금
- 기본 암호화를 사용하는 Amazon S3 버킷 키
- 를 사용하여 데이터 키 캐싱 AWS Encryption SDK
- 키 캐싱 및 Amazon S3 버킷 키의 대안
- KMS 키 사용에 대한 로깅 비용 관리

## AWS KMS 키 스토리지 요금

에서 AWS KMS key 생성하는 각 AWS KMS 에는 요금이 부과됩니다. 대칭 키, 비대칭 키, HMAC 키, 다중 리전 키(각 기본 및 각 복제본 다중 리전 키), 가져온 키 구성 요소가 있는 키, 키 오리진이 AWS CloudHSM 또는 외부 키 스토어인 KMS 키에 대한 월별 요금은 동일합니다.

자동 또는 온디맨드 방식으로 교체하는 KMS 키의 경우 키의 첫 번째 및 두 번째 교체 시 추가 월별 요금(시간당 비례 배분)이 추가됩니다. 두 번째 교체 후에는 해당 월의 후속 교체에 대한 요금이 청구되지 않습니다. 최신 AWS KMS 요금 정보는 요금을 참조하세요.

AWS Budgets를 사용하여 사용량 예산을 구성할 수 있습니다. AWS Budgets 는 계정 내 지출이 특정 임계값을 초과할 때 알림을 보낼 수 있습니다. 관련 비용의 경우 KMS 키 또는 요청에 따라 알림을 보낼 사용 예산을 생성할 AWS KMS수 있습니다. 이렇게 하면 AWS KMS 키 스토리지 및 사용 비용에 대한 가시성을 높일 수 있습니다.

## 기본 암호화를 사용하는 Amazon S3 버킷 키

일부 사용 사례에서는 Amazon Simple Storage Service(Amazon S3)에서 많은 수의 객체에 액세스하거나 생성하는 워크로드가 대량의 요청을 생성하여 비용을 높 AWS KMS일 수 있습니다. Amazon S3 버킷 키를 구성하면 비용을 최대 99% 절감할 수 있습니다. 이는 관련 비용을 줄이기 위해 암호화를 비활성화하는 대신 권장되는 대안입니다 AWS KMS.

# 를 사용하여 데이터 키 캐싱 AWS Encryption SDK

를 사용하여 클라이언트 측 암호화AWS Encryption SDK를 수행할 때 데이터 키 캐싱은 애플리케이션의 성능을 개선하고, 애플리케이션의 요청 AWS KMS 제한이 발생할 위험을 줄이고, 비용을 줄이는 데 도움이 될 수 있습니다. 시작하는 방법에 대한 자세한 내용은 데이터 키 캐싱을 사용하는 방법을 참조하세요.

# 키 캐싱 및 Amazon S3 버킷 키의 대안

데이터 처리 요구 사항으로 인해 키 캐싱이 옵션이 아닌 경우 AWS Management Console 또는 Service Quotas API를 사용하여 AWS KMS 할당량 증가를 요청할 수도 있습니다. 수행할 수 있는 API 호출의 양을 고려합니다. API 직접 호출 횟수는 AWS KMS 요금의 중요한 요소입니다. 요청 속도 할당량을 늘려 성능을 확장하면에 대한 요청 수가 증가하면 추가 비용이 AWS KMS 발생합니다.

# KMS 키 사용에 대한 로깅 비용 관리

모든 AWS KMS API 호출이에 기록됩니다 AWS CloudTrail. 애플리케이션 및 서비스는 대량의 AWS KMS API 호출(예: 암호화 및 복호화를 포함한 암호화 작업)을 생성할 수 있습니다. 해당 데이터를 구성하고, 추세를 조사하고, 비정상적인 API 활동을 검색하는 데 도움이 되는 도구 없이 CloudTrail 로그를 검토하는 것은 어려울 수 있습니다. Amazon Athena는 CloudTrail 로그에 대한 테이블을 빠르게 설정하고 로그 데이터 분석을 시작하는 데 도움이 되는 사전 정의된 데이터 구조를 제공합니다. 이는 인시던트 대응 중에 임시 분석 또는 추가 조사에 특히 유용합니다. 자세한 내용은 Athena 설명서의 쿼리 AWS CloudTrail 로그를 참조하세요.

Athena에 대해 쿼리별로 비용을 지불하므로 무료로 테이블을 미리 설정할 수 있습니다. 데이터 정의 언어 문에는 요금이 부과되지 않습니다. 인시던트에 대응할 때 많은 사전 조건이 이미 충족되었는지 확인하는 데 도움이 됩니다. 준비하는 데 도움이 되도록 테이블을 생성한 후 쿼리를 작성하고 테스트하고 원하는 결과를 생성하고 있는지 확인하는 것이 가장 좋습니다. 나중에 사용할 수 있도록 Athena에 쿼리를 저장할 수 있습니다. Athena를 시작하는 방법에 대한 자세한 내용은 Amazon Athena 시작하기를 참조하세요.

데이터 이벤트는 리소스에서 또는 리소스 내에서 수행되는 작업에 대한 가시성을 제공합니다. 이를 데이터 영역 작업이라고도 합니다. 예를 들어 Amazon S3 `PutObject` 이벤트 또는 Lambda 함수 작업 API 호출이 있습니다. 데이터 이벤트는 대용량 활동인 경우가 많으며 로깅에 대한 요금이 발생합니다. CloudTrail의 추적 또는 이벤트 데이터 스토어에 로깅되는 데이터 이벤트의 양을 제어하는 데 도움이 되도록 CloudTrail에 로그인할 데이터 이벤트를 제한하도록 고급 이벤트 선택기를 구성하여 CloudTrail AWS KMS및 Amazon S3에 대한 비용을 절감하도록 로깅을 최적화할 수 있습니다. 자세한 내용은 고

급 이벤트 선택기를 사용하여 AWS CloudTrail 비용을 최적화하는 방법(블로그 게시물)을 참조하세요.AWS

# 리소스

## AWS Key Management Service (AWS KMS) 설명서

- AWS KMS 개발자 안내서
- AWS KMS API 레퍼런스
- AWS KMS 참조의 AWS CLI

## 도구

- AWS Encryption SDK

## AWS 권장 가이드

### 전략

- 저장 데이터에 대한 암호화 전략 생성

### 가이드

- 에 대한 암호화 모범 사례 및 기능 AWS 서비스
- AWS 프라이버시 참조 아키텍처(AWS PRA)

### 패턴

- Amazon EBS 볼륨 자동 암호화
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- 의 예약된 삭제 모니터링 및 수정 AWS KMS keys

# 기여자

## 작성

- Frank Phillis, Senior GTM Specialist Solutions Architect AWS
- Ken Beer, AWS KMS 및 Crypto 라이브러리 책임자, AWS
- Michael Miller, Senior Solutions Architect AWS
- Jeremy Stieglitz, Principal Product Manager AWS
- Zach Miller, Principal Solutions Architect, AWS
- Peter M. O'Donnell, Principal Solutions Architect AWS
- Patrick Palmer, Principal Solutions Architect, AWS
- Dave Walker, Principal Solutions Architect, AWS

## 검토

- Manigandan Shri, Senior Delivery Consultant, AWS

## 기술 작성

- GxP AbouHarb, Senior Technical Writer, AWS
- Kimberly Garmoe, Senior Technical Writer, AWS

# 문서 기록

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

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 최초 게시 | — | 2025년 3월 24일 |

# 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 데이터가 대상 데이터베이스에 복제되는 동안 소스 데이터베이스만 애플리케이션 연결의 트랜잭션을 처리하는 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 전환하기 위한 효율적이고 효과적인 계획을 개발하는 AWS 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 감염되고 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 스키마에서 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 참조하십시오.

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)

기업의 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

별표 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 빈번한 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 LLM에 작업과 원하는 출력을 보여주는 몇 가지 예제를 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 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(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 실행 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 및 관련 모범 사례 체크리스트입니다. 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

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 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)

제조 분야에서는 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

검색 증강 생성을 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 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.

secret

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 Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?를 참조하세요.

설계를 통한 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 측면 측정.

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)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에 장애가 발생한 경우.

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 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 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 보고 많이 읽습니다.

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.