AWS Key Management Service 모범 사례

AWS 권장 가이드

AWS 권장 가이드: AWS Key Management Service 모범 사례

Table of Contents

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 분산형 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 분산형 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 분산 접근 방식으로, 각 계정에서 해당 키를 사용하는 키를 생성합니다. 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 중앙 집중식 접근 방식으로, KMS 키를 하나 또는 몇 개의 지정된에 유지합니다 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 때 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. 하지만 키를 사용할 수 있는 IAM 역할 및 사용자 권한은 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 사용하면 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 키

는 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 대한 제한인 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 사용에 대한 요금 부과	키 존재에 대한 요금 없음, 호출자에게 API 사용에 대한 요금 부과	고객에게 부과되는 요금 없음

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)이라고 하는 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 여부를 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 해독할 수 없습니다. 삭제된 키는 삭제된 후 복구할 수 AWS 없습니다. 의 다른 중요한 작업과 마찬가지로 AWS삭제를 위해 키를 예약하고 키 삭제를 위해 다중 인증(MFA)이 필요한 사용자를 제한하는 정책을 적용해야 합니다.

실수로 인한 키 삭제를 방지하기 위해는 `DeleteKey` 호출 실행 후 키를 삭제하기 전에 기본 최소 대기 기간인 7일을 AWS KMS 적용합니다. 대기 기간을 최대 30 일로 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 중 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 업로드하고 있습니다. 객체를 버킷에 업로드하기 전에 재료를 키로 가져옵니다. 객체가 업로드되면 해당 키에서 가져온 키 구성 요소를 삭제합니다. 객체는 암호화된 상태로 버킷에 남아 있지만 삭제된 키 구성 요소를 키로 다시 가져올 때까지는 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 주요 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
- AWS KMS 및 영향 범위에 대한 키 교체
- 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 (AWS KMS) 키가 있어야 합니다. 예를 들어 기밀, 내부 전용 및 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 특정 분류의 데이터를 저장하는 AWS 서비스 또는 자체 애플리케이션의 모든 조합에서 사용할 수 있습니다. 여러 워크로드에서 키를 사용할 때 제한 요인 AWS 서비스 은 사용자 집합에서 데이터에 대한 액세스를 제어하는 데 사용 권한이 얼마나 복잡해야 하는지입니다. AWS KMS 키 정책 JSON 문서는 32 KB 미만이어야 합니다. 이 크기 제한이

제한이 될 경우 권한 AWS KMS 부여를 사용하거나 여러 키를 생성하여 키 정책 문서의 크기를 최소화하는 것이 좋습니다.

KMS 키를 분할하기 위해 데이터 분류에만 의존하는 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 암호화해야 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 필

요한 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 암호화되지 않은 볼륨 또는 암호화를 지원하지 않는 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 `GenerateDataKey` 및가 `Decrypt` 호출됩니다 AWS KMS. 이렇게 하면 AWS KMS 사용량에 따른 요금이 증가할 수 있습니다. Amazon S3 버킷 키를 구성하여 AWS KMS 비용을 크게 줄일 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 암호화할 때는 고객 관리형 키를 사용하는 것이 좋습니다. 이 접근 방식을 사용하면 AWS KMS 키 정책에서 특정

IAM 사용자 및 역할을 대상으로 지정하여 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 보호(데이터가 클라이언트에 일반 텍스트로만 표시되어야 함)가 필요한 데이터의 경우 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 테이블을 열 때(및 복호화할 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 모두 사이퍼텍스트만 볼 수 있음을 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 사용하기로 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. 클라이언트 측 암호화를 사용할 때는 SQL 쿼리 내 조인 또는 인덱스 생성과 같이 데이터베이스 액세스에 미치는 영향을 고려해야 합니다.

를 사용한 PCI DSS 데이터 암호화 AWS KMS

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

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 사용을 감사 AWS CloudTrail할 수 있습니다. 그러나 Amazon S3 버킷 키를 사용하는 경우 모든 Amazon S3 작업에 해당하는 항목은 없습니다. 이는 버킷 키가 Amazon S3의 객체를 암호화하는 데 사용하는 데이터 키를 암호화하기 때문입니다. 버킷 키를 사용하면에 대한 모든 API 호출이 제거되지는 않지만 그 수는 AWS KMS줄어듭니다. 따라서 더 이상 Amazon S3 객체 액세스 시도와 API 호출 간에 one-to-one 일치가 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 대한 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 작업에

서 KMS 키를 사용하도록 허용해야 합니다. AWS KMS 키 정책이 작업을 수행하는 IAM 보안 주체에게 작업을 수행할 권한을 부여하지 않으면 해당 작업이 거부됩니다. 키 정책에서 액세스 허용 권한을 올바르게 적용하는 방법에 대한 자세한 내용은 Amazon EC2 Auto Scaling 설명서의 Amazon EC2 Auto Scaling의 데이터 보호를 참조하세요. Amazon EC2 Auto Scaling

AWS KMS 및 영향 범위에 대한 키 교체

규정 준수를 위해 키를 교체해야 하는 경우가 아니면 키 교체 AWS Key Management Service (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. 새 볼륨을 원래 볼륨과 동일한 인스턴스 또는 컨테이너에 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. 원본 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. 암호화에 새 KMS 키를 지정합니다. 지침은 Amazon RDS용 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 해당 데이터베이스의 데이터가 작동하는지 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 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 독립형 SDK로 사용할 수도 있습니다.

이 도구 사용에 대한 권장 사례에는 애플리케이션의 요구 사항을 신중하게 고려하는 것이 포함됩니다. 애플리케이션에 키 캐싱을 도입하는 등 특정 구성으로 인해 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 서비스와의 서버 측 암호화로는 충족할 수 없는 클라이언트 측 암호화 요구 사항이 있나요 AWS KMS?
- 클라이언트 측에서 데이터를 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 등을 AWS KMS 기준으로에 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 작업을 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 90 일간 기록된 관리-이벤트 API 활동에 대한 보기, 검색, 다운로드 및 변경 불가능한 레코드를 제공합니다 AWS 리전. 90 일 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 들면, 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. 를 AWS Config 확인하여 필요한 관리형 규칙이 해당 리전에서 지원되는지 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 준수 여부를 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 컨트롤로 구현할 수도 있습니다AWS Security Hub CSPM. Security Hub CSPM은에 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 구성되

어 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 Config시작
- 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 실행 중인 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 Hub CSPM에서 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 캐싱과 같은 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 에 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 교체에 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 권장됩니다 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 요금을 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 테스트한 다음 원하는 결과를 생성하는 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 로깅할 데이터 이벤트를 제한하도록 고급 이벤트 선택기를 구성하여 CloudTrail AWS KMS및 Amazon S3에 대한 비용을 절감하도록 로깅을 최적화할 수 있습니다. 자세한 내용은 고급 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

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