AWS 결정 가이드

AWS 암호화 서비스 선택

AWS 암호화 서비스 선택: AWS 결정 가이드

Table of Contents

AWS 암호화 서비스 선택

첫 번째 단계 수행

용도	조직에 가장 적합한 AWS 암호화 서비스를 결정하는 데 도움이 됩니다.
최종 업데이트 날짜	2025년 1월 31일
적용 대상 서비스	• AWS Certificate Manager • AWS CloudHSM • AWS 데이터베이스 암호화 SDK • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
관련 가이드	AWS 보안, 자격 증명 및 거버넌스 서비스 선택

소개

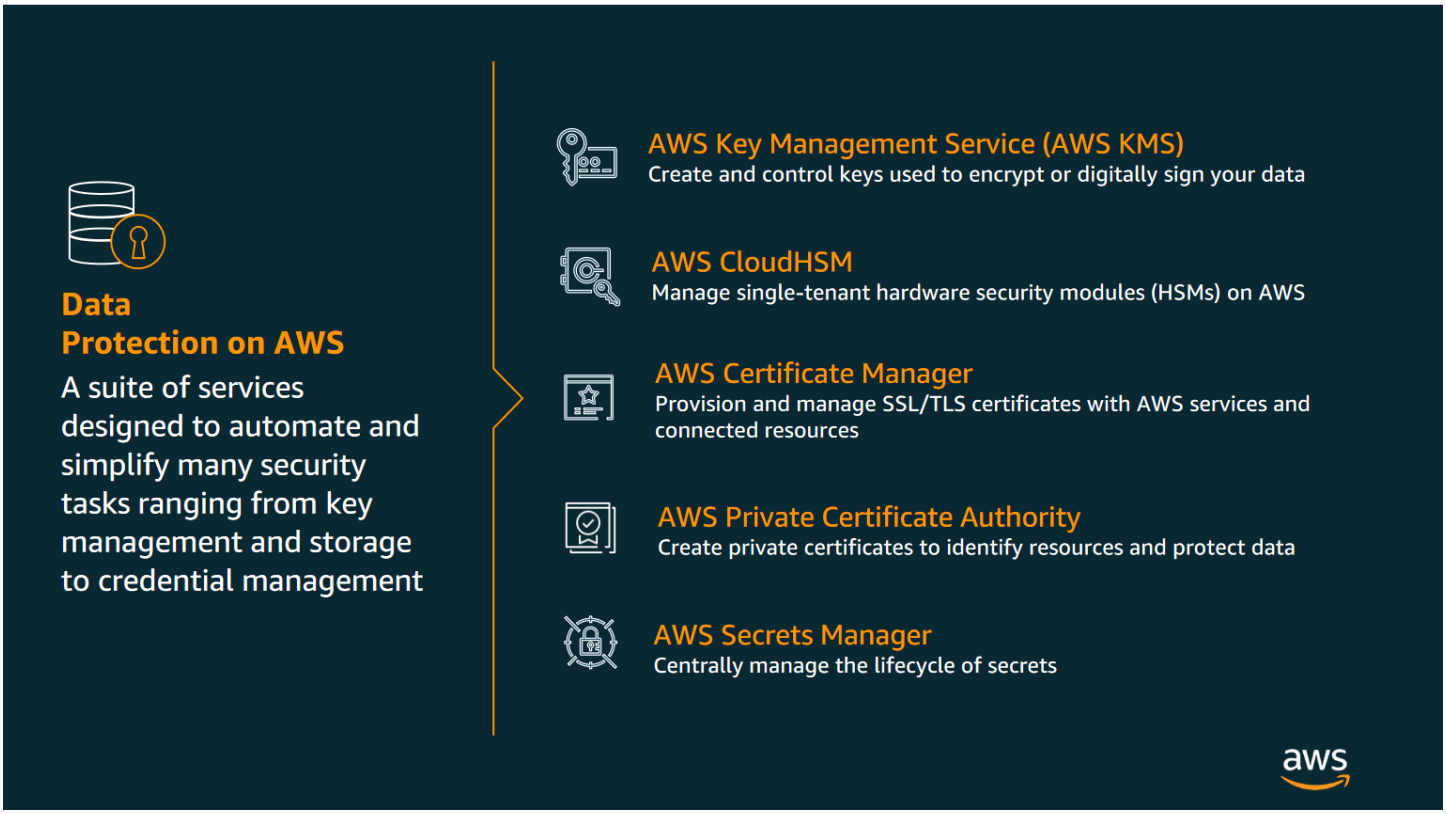
암호화는 클라우드 컴퓨팅에서 보안의 초석으로, 데이터 기밀성, 무결성 및 신뢰성을 보장하는 데 도움이 됩니다. 클라우드 환경에서는 민감한 데이터가 퍼블릭 네트워크를 통과하고 공유 인프라에 상주할 수 있으므로 무단 액세스 또는 변조로부터 보호하는 데 필요한 강력한 암호화 조치를 취할 수 있습니다.

AWS 는 데이터를 보호하고 암호화 키를 관리하며 민감한 정보를 보호하기 위한 포괄적인 암호화 서비스를 제공합니다. 여기에는 중앙 집중식 키 관리, AWS CloudHSM PKCS11 애플리케이션 및 전용 하드웨어 보안 모듈, 클라이언트 측 암호화 AWS Encryption SDK 를 위한 AWS Key Management Service (KMS)가 포함됩니다. AWS Secrets Manager 는 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 암호와 같은 민감한 정보를 안전하게 저장, 관리 및 검색할 수 있는 서비스입니다. AWS Certificate Manager (ACM)은와 함께 사용할 공개적으로 신뢰할 수 있는 전송 계층 보안(TLS) 인증서를 프로비저닝, 관리 및 배포하는 프로세스를 간소화합니다 AWS 서비스. AWS Private Certificate Authority (PCA)를 사용하면 내부 리소스에 대한 x509 인증서를 생성하고 배포할 수 있습니다.

이 가이드는 요구 사항과 조직에 가장 적합한 AWS 암호화 서비스 및 도구를 선택하는 데 도움이 되도록 설계되었습니다.

다음 동영상은 암호화 모범 사례를 소개하는 프레젠테이션의 2분 세그먼트입니다.

이해



올바른 AWS 암호화 서비스 선택은 다음 표에 설명된 특정 사용 사례, 데이터 보안 요구 사항, 규정 준수 의무 및 운영 기본 설정에 따라 달라집니다.

Key management

암호화 키를 안전하게 관리해야 하는 경우 AWS Key Management Service(KMS)를 고려하세요. 이를 통해 다른와 통합된 암호화 키를 생성, 교체 및 관리할 수 있습니다 AWS 서비스. KMS는 FIPS 검증 HSMs 사용하여 규정 준수 방식을 충족하고 KMS에서 노출되는 암호화 프리미티브 구현의 정확성을 보장하는 데 도움이 됩니다. 일부 애플리케이션에는 기존 HSM에서만 사용할 수 있고 클라우드에서 전용 하드웨어 보안 모듈(HSMs)을 AWS CloudHSM 제공하여 암호화 키 및 작업을 완벽하게 제어할 수 있는 특정 암호화 함수 또는 애플리케이션 인터페이스가 필요합니다.

Data encryption

고객 세부 정보 또는 지적 재산과 같은 민감한 데이터를 암호화하기 위해 AWS KMS 는 스토리지, 데이터베이스 및 메시징 서비스(예: S3, RDS 또는 EBS)와 긴밀하게 통합 AWS 됩니다. 클라이언트 측 암호화가 필요한 경우 AWS Encryption SDK 는 애플리케이션 내에서 데이터를 클라우드로 전송하기 전에 쉽게 암호화할 수 있는 오픈 소스 라이브러리입니다.

Secure communications

전송 중 데이터를 보호하기 위해 AWS Certificate Manager (ACM)은 공개적으로 신뢰할 수 있는 TLS 인증서의 관리를 간소화합니다. 이를 사용하여 인증서 갱신에 대한 걱정 없이 인터넷 연결 애플리케이션의 ID를 어설션하고 애플리케이션, 사용자 및 클라우드 서비스 간의 통신을 쉽게 암호화할 수 있습니다. 내부 애플리케이션의 경우 AWS 프라이빗 인증 기관(PCA)을 사용하여 클라이언트와 서버를 모두 포함한 내부 리소스에 대한 x509 인증서를 생성하고 배포할 수 있습니다.

Secrets and credentials management

데이터베이스 자격 증명, API 키 또는 인증서와 같은 애플리케이션 보안 암호를 안전하게 저장하고 검색하려면를 고려하세요 AWS Secrets Manager. 자동 보안 암호 교체 및 세분화된 액세스 제어를 제공합니다. 또는 AWS Systems Manager Parameter Store는 민감하지 않은 구성을 관리하기 위한 저렴한 옵션이며와 통합할 수 있습니다 AWS Secrets Manager.

Compliance and auditing

규정 준수 작업의 경우 암호화 표준을 충족하는 AWS CloudHSM 데 도움이 되도록 AWS KMS 및를 고려하세요. AWS Artifact는 ISO 인증 및 SOC 보고서와 같은 AWS보안 및 규정 준수 보고서에 대한 온디맨드 액세스 권한과 Business Associate Addendum(BAA)과 같은 계약을 검토하고 수락할 수 있는 기능을 제공하는 셀프 서비스 포털입니다. 또한 및 AWS Config AWS Security Hub와 같은 서비스를 사용하여 규정 준수를 AWS Audit Manager 모니터링하고 자체적으로 사용하거나 이해관계자가 사용할 수 있도록 적절한 아티팩트를 생성할 수 있습니다.

AWS 암호화 서비스 중에서 선택할 때는 다음 요구 사항을 고려하세요.

요구 사항	서비스:
적은 노력, 완전 관리형	AWS KMS 또는 AWS Secrets Manager
KMS에서 지원하지 않는 특정 애플리케이션 인터페이스 또는 암호화 알고리즘 필요	AWS CloudHSM
애플리케이션에서 데이터 암호화/암호 해독	AWS Encryption SDK

요구 사항	서비스:
간소화된 퍼블릭 TLS 인증서 관리	AWS Certificate Manager
보안 암호 관리	AWS Secrets Manager

요구 사항을 이러한 옵션에 맞게 조정하여 보안 및 운영 요구 사항에 맞는 암호화 솔루션을 구현할 수 있습니다.

고려 사항

올바른 암호화 서비스를 선택하려면 특정 보안, 운영 및 규정 준수 요구 사항을 이해해야 합니다. AWS AWS 는 키 관리부터 데이터 암호화 및 보안 통신에 이르기까지 다양한 사용 사례를 해결하도록 설계된 다양한 암호화 서비스를 제공합니다. 정보에 입각한 결정을 내리려면 사용 사례, 제어 및 유연성 요구 사항, 규정 준수 의무, 비용 고려 사항, 와의 통합 등 몇 가지 중요한 기준에 따라 요구 사항을 평가해야 합니다 AWS 서비스. 이러한 기준은 조직의 보안 목표 및 운영 워크플로에 맞게 선택을 조정하는 데 도움이 됩니다.

Use case

데이터 암호화, 키 관리, 보안 통신 또는 보안 암호 관리를 위해 필요한 암호화 서비스를 고려합니다. 예를 들어 AWS 서비스, AWS KMS 는에 통합된 암호화에 이상적이며,는 종종 엄격한 규정 준수 또는 특정 애플리케이션 요구 사항으로 인해 특정 암호화 기능, 애플리케이션 인터페이스 또는 단일 테넌트 HSM이 필요한 조직에 AWS CloudHSM 적합합니다. 목적을 명확히 하면 요구 사항에 적합한 서비스를 선택하여 기능과 비용을 모두 최적화할 수 있습니다.

Control and flexibility

암호화 작업에 필요한 제어 수준을 평가합니다. 와 같은 관리형 서비스는 키 구성 요소를 완벽하게 제어하면서 다중 테넌트 HSM을 통해 관리 오버헤드를 최소화하면서 사용 편의성을 AWS KMS 제공합니다. 반대로는 특정 애플리케이션, 암호화 또는 규정 준수 요구 사항에 맞는 단일 테넌트 모델을 AWS CloudHSM 제공합니다.

Compliance requirements

규제 산업에서 운영하는 경우 서비스가 GDPR, PCI DSS 또는 HIPAA와 같은 표준에 부합 AWS KMS 하고 둘 다 FIPS 140-2 레벨 3 인증을 받았 AWS CloudHSM 는지 확인합니다. 비기능적 요구 사항을 충족하는 서비스를 선택하면 신뢰를 유지하는 데 도움이 되며 잠재적인 법적 또는 재정적 처벌을 피할 수 있습니다.

Cost considerations

서비스의 요금 모델을 기준으로 예산을 평가합니다. AWS KMS 는 일반적인 암호화 요구 사항에 대해 비용 효율적이지만 전용 하드웨어로 인해 더 많은 비용이 AWS CloudHSM 발생합니다. 비용 영향을 이해하면 보안 지출을 최적화하는 데 도움이 됩니다.

Integration with AWS ecosystem

를 많이 사용하는 경우 S3 AWS 서비스, RDS 또는 Lambda와 원활하게 통합되는 AWS KMS 또는 ACM과 같은 암호화 솔루션의 우선 순위를 지정합니다. 이렇게 하면 워크플로가 더 매끄러워지고 개발 작업이 줄어듭니다. 통합 기능은 운영 효율성을 크게 향상시킬 수 있습니다.

선택

올바른 암호화 서비스를 선택하려면 특정 보안, 운영 및 규정 준수 요구 사항을 이해해야 합니다. AWS AWS 는 키 관리부터 데이터 암호화 및 보안 통신에 이르기까지 다양한 사용 사례를 해결하도록 설계된 다양한 암호화 서비스를 제공합니다. 정보에 입각한 결정을 내리려면 사용 사례, 제어 및 유연성 요구 사항, 규정 준수 의무, 비용 고려 사항, 와의 통합 등 몇 가지 중요한 기준에 따라 요구 사항을 평가해야 합니다 AWS 서비스. 이러한 기준은 조직의 보안 목표 및 운영 워크플로에 맞게 선택을 조정하는 데 도움이 됩니다.

대상 사용 사례	언제 사용하나요?	권장 서비스
키 관리	다른와 통합된 암호화 키를 안전하게 생성, 교체 및 관리하려면 AWS 서비스	AWS KMS
키 관리	특정 애플리케이션 통합 또는 암호화 프리미티브의 경우	AWS CloudHSM
데이터 암호화	클라이언트 측 암호화를 구현하여 고객 세부 정보 또는 지적 재산과 같은 민감한 데이터를 보호합니다.	AWS Encryption SDK AWS 데이터베이스 암호화 SDK
통신 보안	전송 중인 데이터를 보호하고 SSL/TLS 인증서 관리를 간소화합니다.	AWS Certificate Manager AWS Private CA

대상 사용 사례	언제 사용하나요?	권장 서비스
보안 암호 및 자격 증명 관리	데이터베이스 자격 증명, API 키 또는 인증서와 같은 애플리케이션 보안 암호를 안전하게 저장하고 검색합니다.	AWS Secrets Manager AWS 파라미터 스토어

사용

이제 각 AWS 암호화 서비스가 수행하는 작업과 사용자에게 적합할 수 있는 작업을 명확하게 이해할 수 있습니다.

사용 가능한 AWS 각 암호화 서비스를 사용하고 자세히 알아보는 방법을 알아보기 위해 각 암호화 서비스의 작동 방식을 탐색하는 경로를 제공했습니다. 다음 섹션에서는 시작하는 데 도움이 되는 심층 설명서, 실습 자습서 및 기타 리소스에 대한 링크를 제공합니다.

AWS Certificate Manager

- 시작하기 AWS Certificate Manager

  퍼블릭 인증서와 프라이빗 인증서 작업을 모두 AWS Certificate Manager포함하여 사용을 시작합니다.

  가이드 살펴보기
- 모범 사례 AWS Certificate Manager

  보다 효과적으로 사용하는 AWS Certificate Manager 데 도움이 되는 권장 사항을 검토합니다.

  가이드 살펴보기
- AWS Certificate Manager FAQ

  AWS Certificate Manager (ACM) FAQ 페이지에서 ACM의 기능 및 사용에 대한 일반적인 질문에 대한 자세한 답변을 확인하세요. ACM이 관리하는 인증서 유형, 다른 와의 통합 AWS 서비스, SSL/TLS 인증서 프로비저닝 및 관리에 대한 지침과 같은 주제를 다룹니다.

  FAQs 살펴보기

AWS CloudHSM

- 시작하기 AWS CloudHSM

  에서 클러스터를 생성, 초기화 및 활성화하는 방법을 알아봅니다 AWS CloudHSM. 이러한 절차를 완료하면 사용자를 관리하고 클러스터를 관리하며 포함된 소프트웨어 라이브러리를 사용하여 암호화 작업을 수행할 수 있습니다.

  가이드 살펴보기

- 의 모범 사례 AWS CloudHSM

  클러스터 관리 및 모니터링을 AWS CloudHSM 위한 모범 사례를 살펴봅니다.

  가이드 살펴보기

- AWS CloudHSM 요금

  요금 페이지를 검토하여 AWS CloudHSM 요금에 대해 알아봅니다. AWS CloudHSM사용에 따른 선결제 비용은 없습니다. 를 사용하면 HSM을 종료할 때까지 시작하는 각 HSM에 대해 시간당 요금을 AWS CloudHSM지불합니다. 이 가이드에서는 각 AWS 리전의 시간당 요금을 제공합니다.

  요금 페이지 살펴보기

- AWS CloudHSM FAQ

  AWS CloudHSM FAQ 페이지를 검토하여 기능 AWS CloudHSM, 요금, 프로비저닝, 보안, 규정 준수, 성능, 타사 애플리케이션과의 통합 등에 대한 일반적인 질문에 대한 자세한 답변을 확인하세요.

  FAQs 살펴보기

AWS Encryption SDK

- 시작하기 AWS Encryption SDK

  를와 AWS Encryption SDK 함께 사용하는 방법을 알아봅니다 AWS KMS.

  가이드 살펴보기

- 의 모범 사례 AWS Encryption SDK

를 효과적으로 활용하여 데이터를 보호하는 AWS Encryption SDK 방법에 대한 지침은 AWS Encryption SDK 모범 사례 페이지를 검토하세요. 이러한 모범 사례를 준수하면 암호화된 데이터의 기밀성과 무결성을 보장하는 데 도움이 됩니다.

가이드 살펴보기

- AWS Encryption SDK FAQ

  AWS Encryption SDK FAQ 페이지에서 기능 AWS Encryption SDK, 지원되는 프로그래밍 언어 및 구현 모범 사례를 포함하여에 대한 일반적인 질문에 대한 답변을 검토하세요.

  FAQ 살펴보기

AWS Database Encryption SDK

- AWS Database Encryption SDK 시작하기

  AWS Database Encryption SDK를와 함께 사용하는 방법을 알아봅니다 AWS KMS.

  가이드 살펴보기
- AWS Database Encryption SDK 구성

  프로그래밍 언어 선택 및 래핑 키 선택을 포함하여 AWS Database Encryption SDK를 구성하는 방법을 알아봅니다.

  가이드 살펴보기

AWS KMS

- 시작하기 AWS KMS

  대칭 및 비대칭 암호화 키를 포함하여 KMS 키를 생성하는 방법을 알아봅니다.

  가이드 살펴보기
- 에 대한 모범 사례 AWS KMS

  에 대한 암호화 모범 사례를 알아봅니다 AWS KMS.

  가이드 살펴보기
- AWS KMS 요금

AWS Key Management Service (KMS) 요금 페이지를 검토하여 키 스토리지 AWS KMS, API 요청 및 사용자 지정 키 스토어와 같은 선택적 기능에 대한 요금을 포함하여 사용과 관련된 비용에 대해 알아봅니다.

요금 페이지 살펴보기

- AWS KMS FAQ

  AWS Key Management Service (KMS) FAQ 페이지에서는 기능 AWS KMS, 보안 조치, 결제 관행, 키 관리 옵션, 기타와의 통합 등에 대한 일반적인 질문에 대한 자세한 답변을 제공합니다 AWS 서비스.

  FAQs 살펴보기

AWS Private CA

- 에 대한 모범 사례 AWS Private CA

  를 효과적으로 사용하는 AWS Private CA 데 도움이 되는 권장 사항을 검토합니다.

  가이드 살펴보기

- 시작하기 AWS Private CA

  프로그래밍 방식으로 루트 CA를 생성하고 활성화하는 방법을 알아봅니다.

  가이드 살펴보기

- AWS Private CA 요금

  프라이빗 CAs 운영 및 프라이빗 인증서 발급과 관련된 비용을 검토합니다.

  요금 페이지 살펴보기

- AWS Private CA FAQ

  기능 AWS Private CA, 요금, 프로비저닝, 보안, 규정 준수, 성능, 다른 와의 통합 등에 대한 일반적인 질문에 대한 자세한 답변을 얻을 수 있습니다 AWS 서비스.

  FAQs 살펴보기

AWS Secrets Manager

- 시작하기 AWS Secrets Manager

  AWS Secrets Manager 보안 암호를 생성하는 방법을 알아봅니다.

  가이드 살펴보기
- 에 대한 모범 사례 AWS Secrets Manager

  사용 시 고려해야 할 모범 사례에 대해 알아봅니다 AWS Secrets Manager.

  가이드 살펴보기
- AWS Secrets Manager 요금

  AWS Secrets Manager 요금 페이지를 검토하여 데이터베이스 자격 증명 및 API 키와 같은 보안 암호의 안전한 저장, 관리 및 검색과 관련된 비용에 대해 알아봅니다.

  요금 페이지 살펴보기
- AWS Secrets Manager FAQ

  AWS Secrets Manager FAQ 페이지를 검토하여 기능 AWS Secrets Manager, 보안 조치, 요금 및 통합 기능을 포함하여에 대한 일반적인 질문에 대한 자세한 답변을 확인하세요.

  FAQs 살펴보기

탐색

- 연구 및 리소스

  암호화에 대한 AWS 블로그, 비디오 및 도구를 살펴봅니다.

  리소스 검토
- 비디오

  YouTube의 AWS 개발자 채널에서이 동영상을 시청하여 암호화 전략을 더욱 개발하고 구체화하세요.

  암호화 비디오 살펴보기

문서 이력

다음 표에서는이 결정 가이드의 중요한 변경 사항에 대해 설명합니다. 이 가이드의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
최초 게시	가이드가 처음 게시되었습니다.	2025년 1월 31일

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