



Encryption and Data Protection

박병화

Sr. Security Consultant (bhpark@amazon.com)

AWS Proserve

Agenda

1. 데이터 암호화

2. 전송 중 암호화

Q&A

목표

- AWS의 데이터에 대한 고객의 책임 이해
- AWS에서 암호화가 수행되는 방법 알아보기
- 자체 암호화 요구 사항 고려
- 데이터 보호 관련 AWS 서비스 알아보기

의사결정 사항

1. 데이터 저장소에 대한 암호화
(S3, EBS, RDS)
2. 전송 중 암호화 결정, TLS 종단
3. 위 사항에 대한 주요 관리 책임자

클라우드에서의 암호화

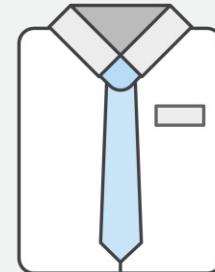
- 규제 준수를 위해
- 보안 모범사례를 따르기 위해
- 클라우드 사업자에게서 내 데이터를 보호하기 위해
- 클라우드 사업자의 다른 고객으로부터 내 데이터를 보호하기 위해



IT 보안 인력
키 접근 정책



소프트웨어 개발자
암호키 사용



규제 준수팀
암호화 구성 및 이력

전송 중 및 미사용 데이터 보호

전송 중인 암호화

SSL/TLS

SSH

VPN/IPSEC

데이터 암호화

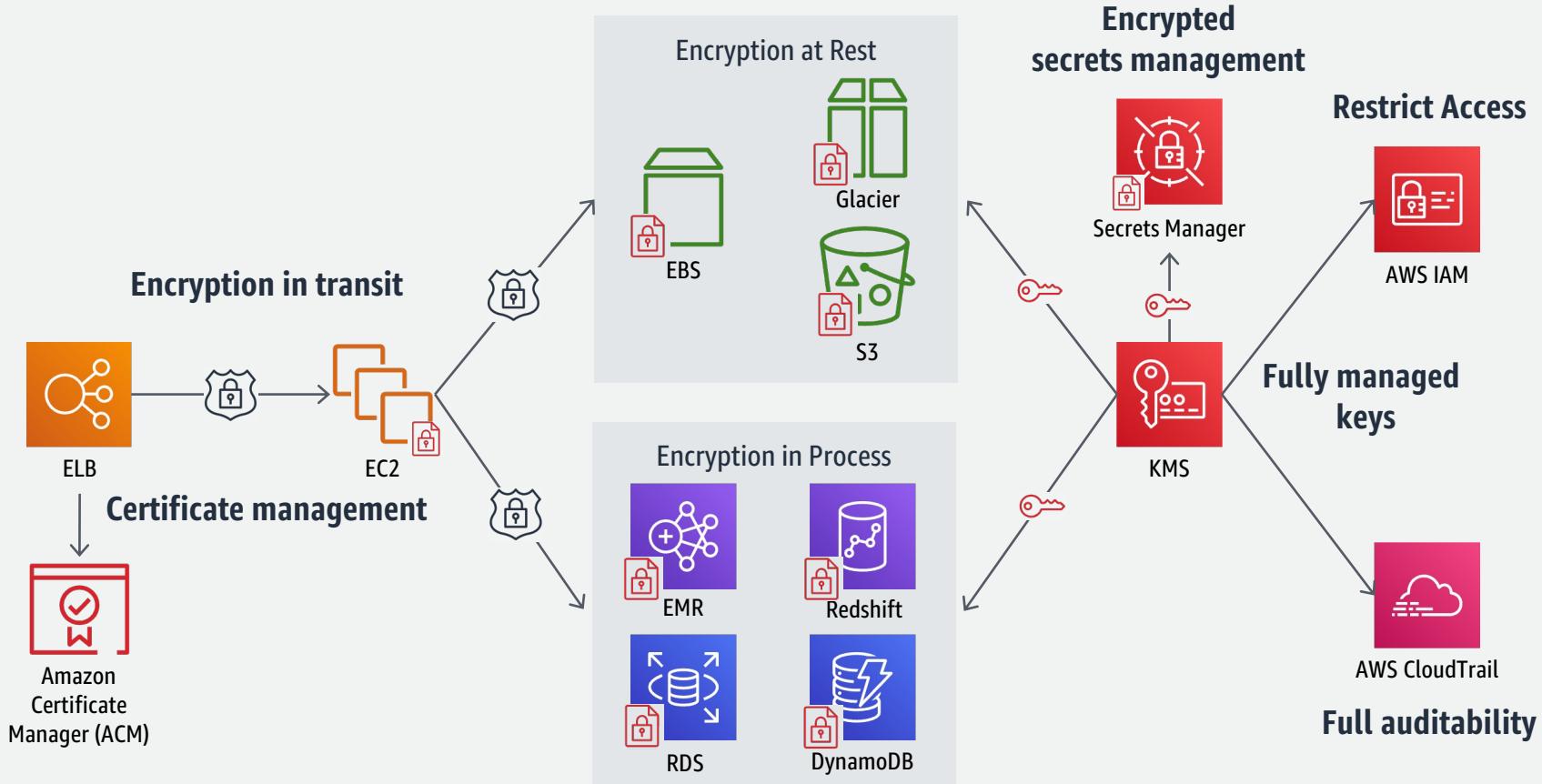
객체

데이터베이스

파일 시스템

디스크

유비쿼터스(어디에나 있는) 암호화

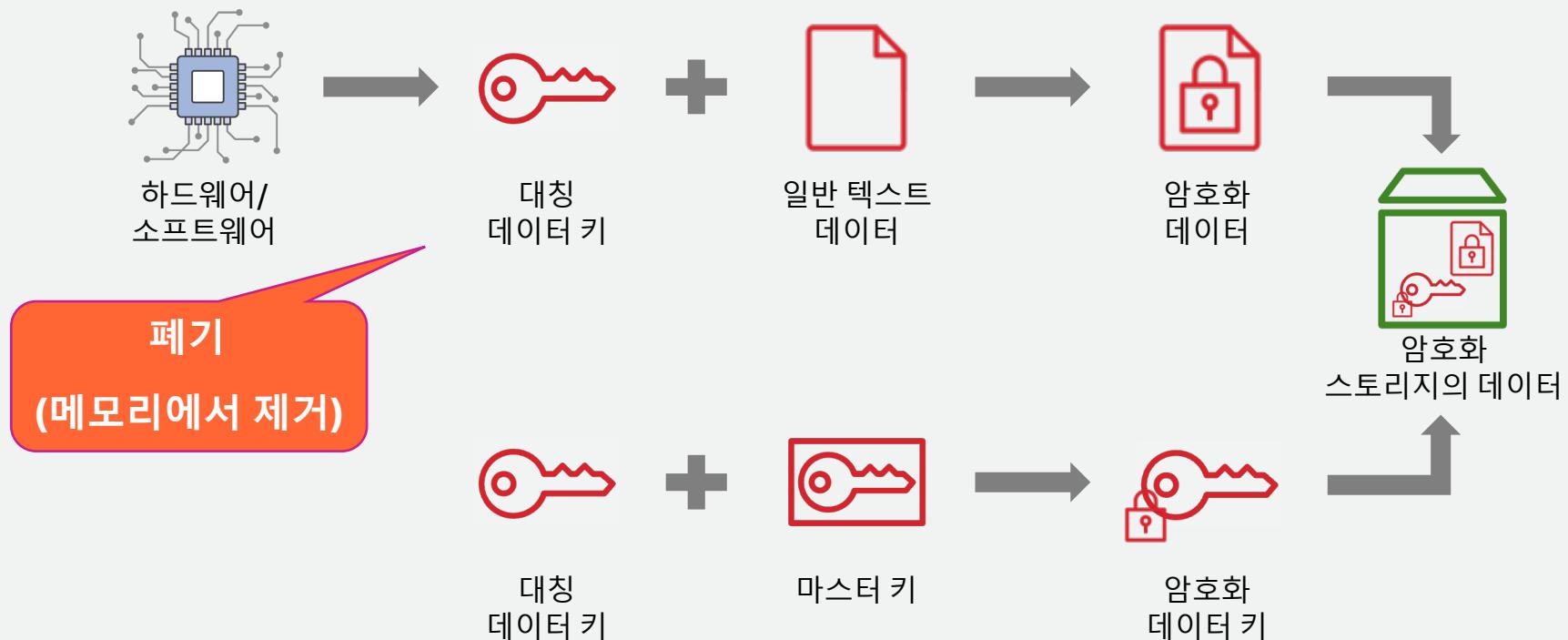


데이터 암호화

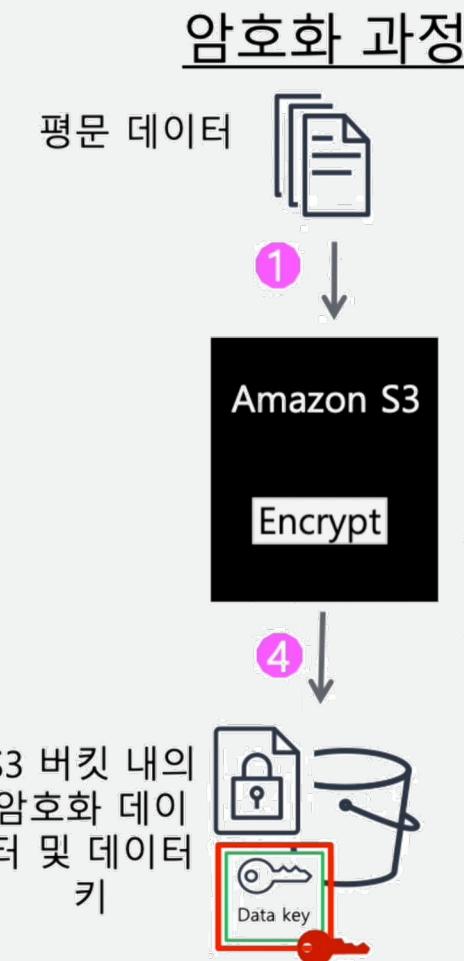


© 2022, Amazon Web Services, Inc. or its affiliates.

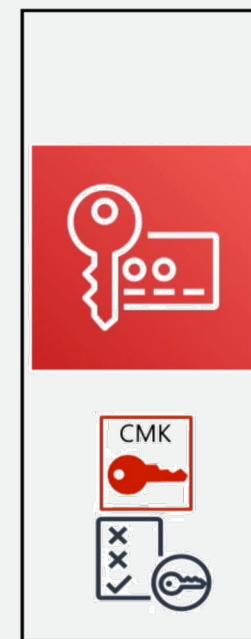
데이터 암호화 - 봉투 암호화 입문서



데이터 암호화 - 봉투 암호화 입문서



예제: S3 서버 측 암호화

복호화 과정

5. 암호화된 데이터키 (Encrypted data key) is sent to Amazon S3.

6. Data key is decrypted using another Data key.

7. The decrypted Data key is used to decrypt the encrypted data.

8. The final decrypted data (Plain text data) is output.

© 2022, Amazon Web Services, Inc. or its affiliates.

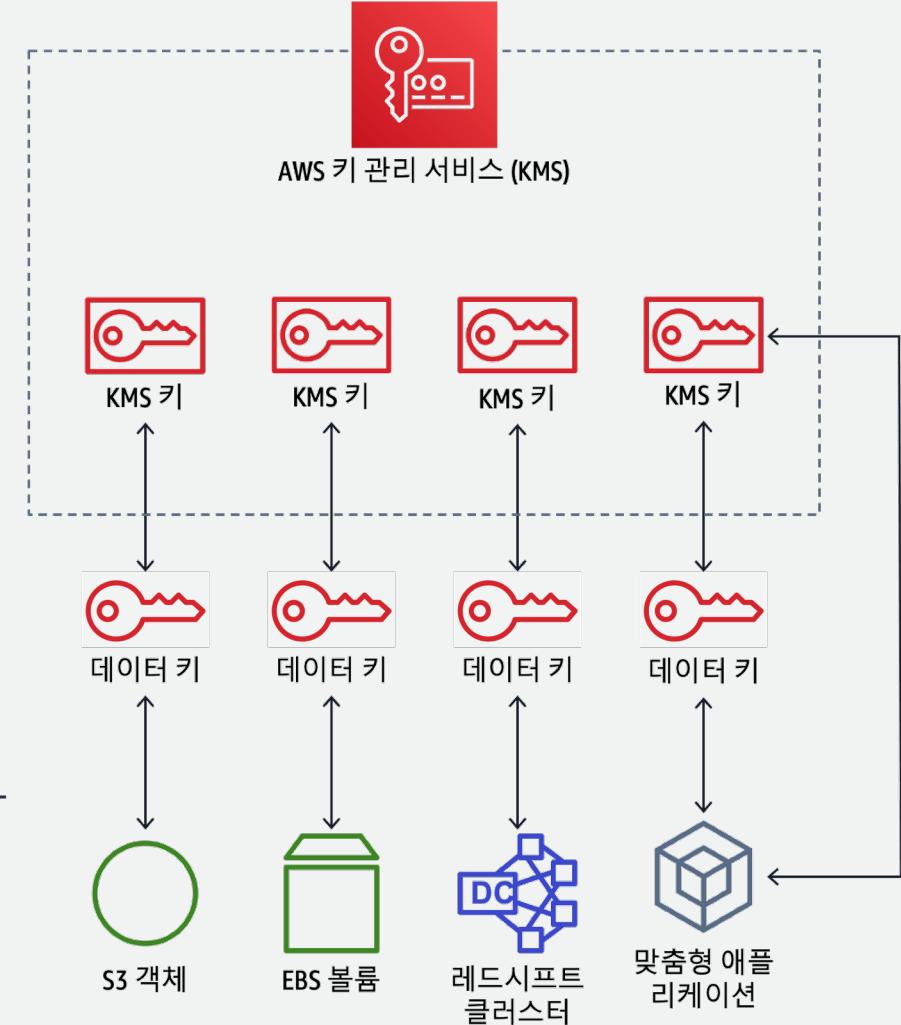
AWS KMS(Key Management Service)

AWS 키 관리 서비스 계층

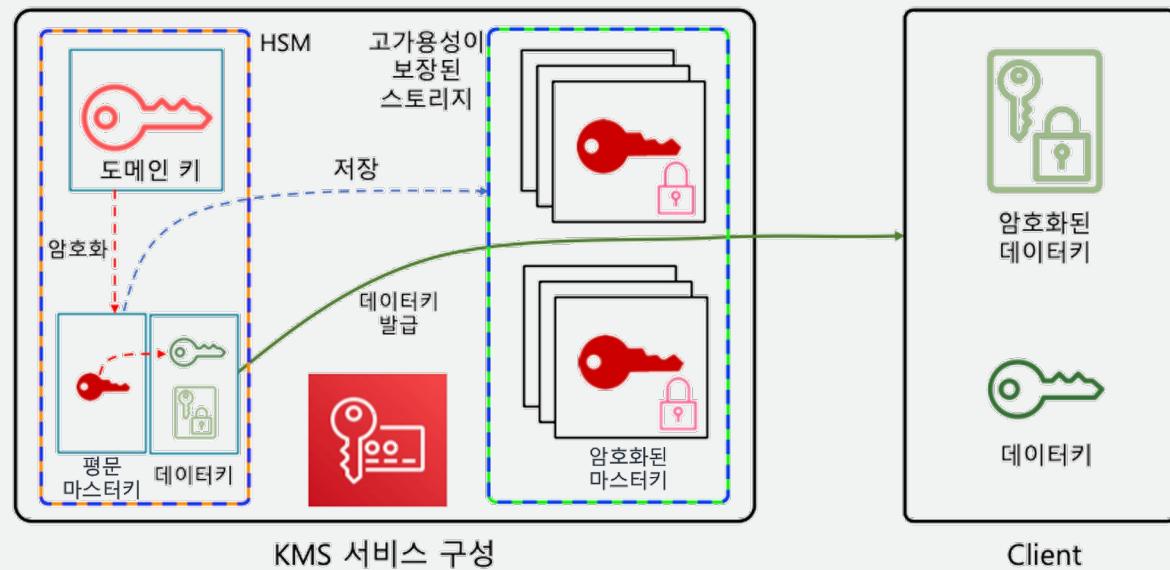
- 봉투 암호화를 사용한 2계층 키 계층
- 고유한 데이터 키로 고객 데이터 암호화
- KMS 키는 데이터 키를 암호화합니다.

장점

- 데이터 키 손상 위험 제한
- 대용량 데이터 암호화를 위한 성능 향상
- 수백만 개의 데이터 키보다 적은 수의 KMS 키 관리가 쉬움
- 중앙 집중식 액세스 및 주요 활동 감사



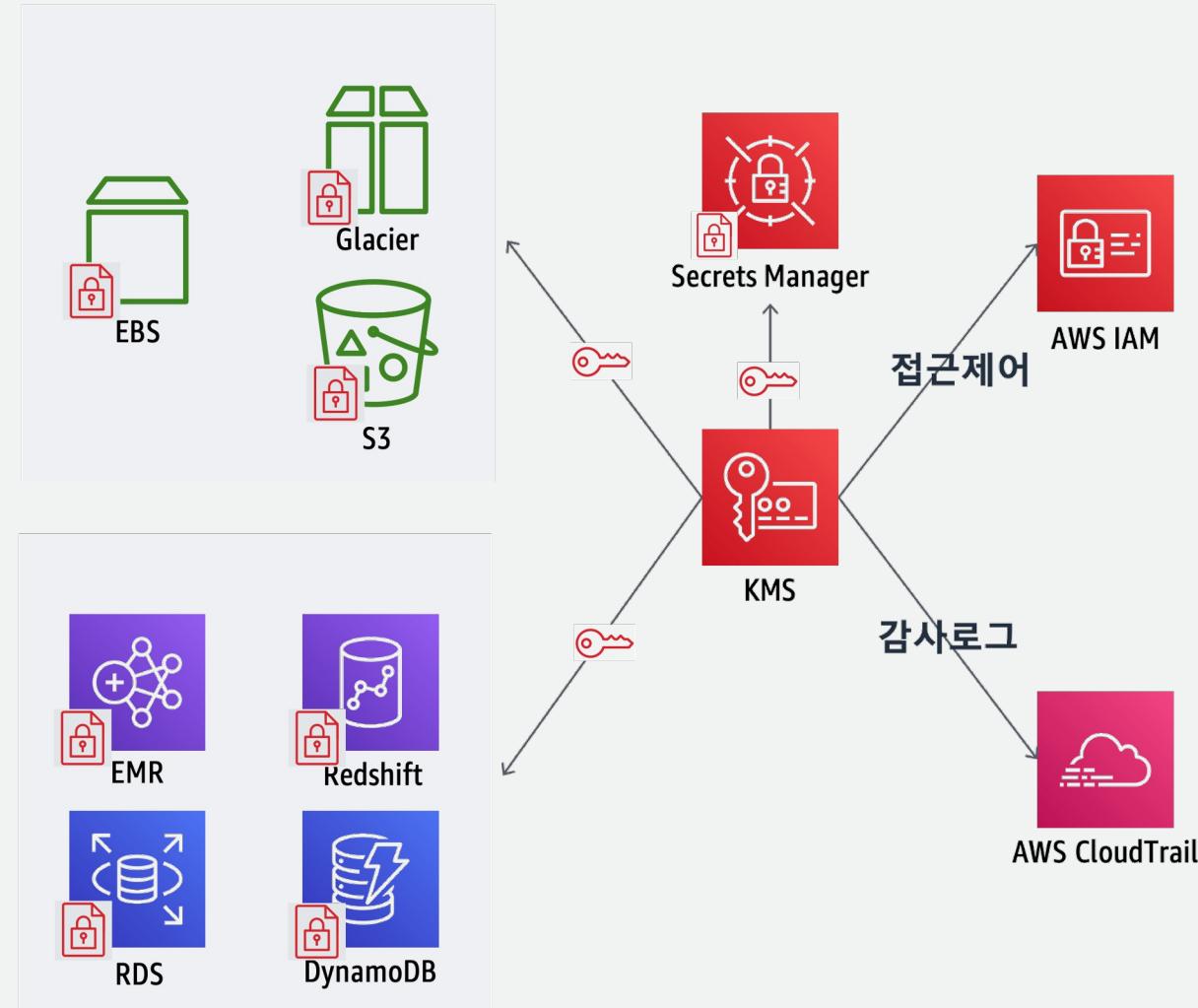
AWS KMS(Key Management Service)



1. 마스터키(KMS 내부의 HSM에서 생성)는 절대 평문 형태로 HSM을 벗어나지 않는다.
2. 마스터키는 HSM에 저장된 도메인 키로 암호화되며 암호화된 상태로 KMS 내부의 별도 저장공간(KMS Host)에 저장된다.
3. 데이터키는 KMS 내부의 HSM에서 생성된다.
4. 생성된 데이터키는 CMK로 암호화하여 평문 데이터키와 함께 전달된다.

**KMS에 암/복호화를 요청하는 경우 HSM에 의해 암/복호화가 수행되며 원본 데이터의 사이즈는 4KB로 제한된다

AWS KMS(Key Management Service)



AWS KMS 키 유형

	AWS KMS 키 유형
갯수	Amazon S3-managed keys (SSE-S3)
생성	고객 AWS KMS 키
교체	3년
삭제	삭제
AWS 계정 내에서 표시	예
사용 범위	Amazon S3-managed keys (SSE-S3)

Default encryption
Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

Disable
 Enable

Encryption key type
To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

Amazon S3-managed keys (SSE-S3)
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

AWS Key Management Service key (SSE-KMS)
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

AWS managed key (aws/s3)
arn:aws:kms:ap-northeast-2:611984617746:alias/aws/s3

Choose from your AWS KMS keys

Enter AWS KMS key ARN

AWS KMS key

Choose AWS KMS key ▾

Bucket Key
Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. Use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)

Disable
 Enable

arn:aws:kms:ap-northeast-2:611984617746:key/1ffc93fd-cc92-48d2-9deb-e1efd8b8cb80

arn:aws:kms:ap-northeast-2:611984617746:key/21335c95-fd34-4f97-bb27-dd6342855ddc FirstCMK

arn:aws:kms:ap-northeast-2:611984617746:key/5e059bff-fc0e-49a8-99bc-cde6a67a23df

arn:aws:kms:ap-northeast-2:611984617746:key/6b6e1970-31bb-421f-8eb7-54860f0bd1f3

데이터 암호화 – AWS의 옵션

클라이언트 측 암호화

- 데이터를 서비스에 제출하기 전에 데이터를 암호화합니다.
- AWS 계정에서 암호화 키를 제공하거나 키를 사용합니다.
- 사용 가능한 클라이언트:
- S3, EMR 파일 시스템 (EMRFS), DynamoDB, AWS Encryption SDK

서버 측 암호화

- AWS는 서비스를 통해 데이터를 수신한 후 사용자를 대신하여 데이터를 암호화합니다.
- 통합 암호화를 사용하는 서비스에는 S3, 스노우볼, EBS, RDS, 아마존 레드시프트, 워크스페이스, 아마존 키네시스 파이어호스, 클라우드트레일, EMR, DynamoDB, 코드 파이프라인, AWS 비밀 관리자, AWS 백업 등이 포함됩니다.
- 고객 관리 통제 하에 AWS KMS에 암호화키(CMK) 보관

클라이언트 측 암호화 - AWS Encryption SDK

- 암호화 작업에서, 개발자는 다음 2개의 사항만 고려
 - ✓ 암호화 할 메세지/파일/데이터스트림
 - ✓ 마스터 키들을 리턴하는 마스터 키 제공자(key provider)
- SDK를 다양한 방식으로 커스터마이징해서 사용
 - ✓ 복수 리전에서 복수개의 키를 활용하여 암호화
 - ✓ 성능향상이나 KMS Limit을 회피하기 위해 데이터 키 캐싱 기능을 이용하여 KMS로의 요청을 절감
- 현재 C, Java, Python, JavaScript, CLI 버전 제공
 - ✓ <http://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html>

AWS 서비스에서 KMS를 활용하는 방식

- **EC2/EBS 모델**
 - ✓ EBS 볼륨 별로 데이터 키를 생성하고, CMK로 암호화한 뒤 볼륨 메타데이터에 저장
 - ✓ 고객의 EBS 리소스가 EC2에 붙어 있는 동안, 해당 EBS 볼륨을 암호화하는데 사용되는 평문
 - ✓ 데이터 키는 하이퍼바이저의 휘발성 메모리 상에 보관 > 볼륨, I/O, 스냅샷을 암호화
 - ✓ 해당 서비스: EBS, RDS, Redshift, WorkSpaces, Amazon Lightsail
- **S3 모델**
 - ✓ S3의 3가지 서버 측 암호화 중 SSE-KMS 방식
 - ✓ 객체 별로 데이터 키를 생성하고, CMK로 암호화한 뒤, 객체 메타데이터에 저장
 - ✓ 객체에 대한 암호화는 S3 호스트의 휘발성 메모리 상에서 진행되고 평문 데이터 키는 작업 후 바로 삭제됨.
 - ✓ 비정기적인 Get 요청에 대해 S3는 KMS 쪽으로 암호화된 데이터 키와 CMK를 지정하여 복호화
 - ✓ 요청하고, 복호화된 데이터 키를 받아서 타겟 객체를 복호화 한 뒤, 작업 후 삭제됨.
 - ✓ 해당 서비스: S3, EMR, CloudTrail, Amazon Athena, Amazon Kinesis, Amazon SQS, Amazon CloudWatch

AWS 서비스에서 KMS를 활용하는 방식

- 고객은 직접 CMK 사용 조건에 대한 권한설정을 키 정책(CMK Policy)으로 정의
- 키 정책 사례:
 - ✓ <지정된 어카운트>의 <지정된 사용자와 Role>만이 암/복호화 수행
 - ✓ 어플리케이션 A에서만 데이터를 암호화하고, 어플리케이션 B에서만 그 데이터를 복호화 할 수 있다.
 - ✓ 지정된 관리 그룹 혹은 Role에 의해 관리가능함.
 - ✓ <지정된 어카운트>만이 암/복호화 작업을 수행할 수 있으나, 다른 관리작업(생성/삭제/정책관리/위임 등)은 불가.
- AWS Identity and Access Management과 연계

데이터 암호화 - AWS 키 관리 서비스

AWS CloudTrail을 활용한 키 사용 감사

```
"EventName": "DecryptResult",           This KMS API action was called ...  
"EventTime": "2021-08-18T18:13:07Z",      ... at this time  
"RequestParameters":  
    "{\"keyId\": \"2b42x363-1911-4e3a-8321-6b67329025ex\"}", ... in reference to this key  
"EncryptionContext": "volumeid-12345",       ... to protect this AWS resource  
"SourceIPAddress": "203.0.113.113",          ... from this IP address  
"UserIdentity":  
    "{\"arn\": \"arn:aws:iam:: 111122223333:user/User123\"} ... by this AWS user in this account
```

데이터 암호화 – S3

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#) 

Server-side encryption

- Disable
- Enable

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

Amazon S3-managed keys (SSE-S3)

An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#) 

AWS Key Management Service key (SSE-KMS)

An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#) 

데이터 암호화 - EBS

Encryption [Info](#)
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

KMS key [Info](#)

Select a KMS key

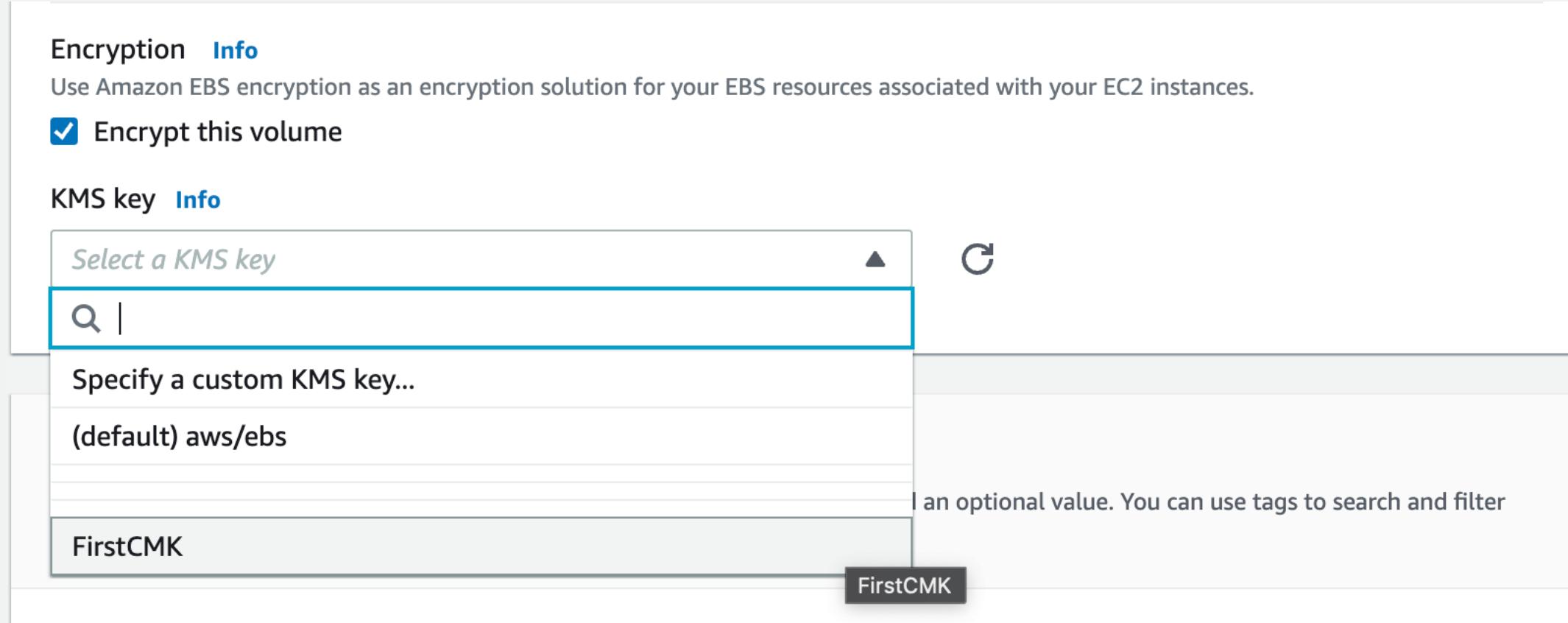
|

Specify a custom KMS key...
(default) aws/ebs

FirstCMK

I an optional value. You can use tags to search and filter

FirstCMK



데이터 암호화 – Database

Encryption

Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

AWS KMS Key [Info](#)

(default) aws/rds



Account

(default) aws/rds



(default) aws/rds

KMS key ID

arn:aws:kms:ap-northeast-2:611984617746:key/1ffc93fd-cc92-48d2-9deb-e1efd8b8cb80

alias/aws/rds

FirstCMK

arn:aws:kms:ap-northeast-2:611984617746:key/5e059bff-fc0e-49a8-99bc-cde6a67a23df

arn:aws:kms:ap-northeast-2:611984617746:key/6b6e1970-31bb-421f-8eb7-54860f0bd1f3

Enter a key ARN



전송 중 암호화



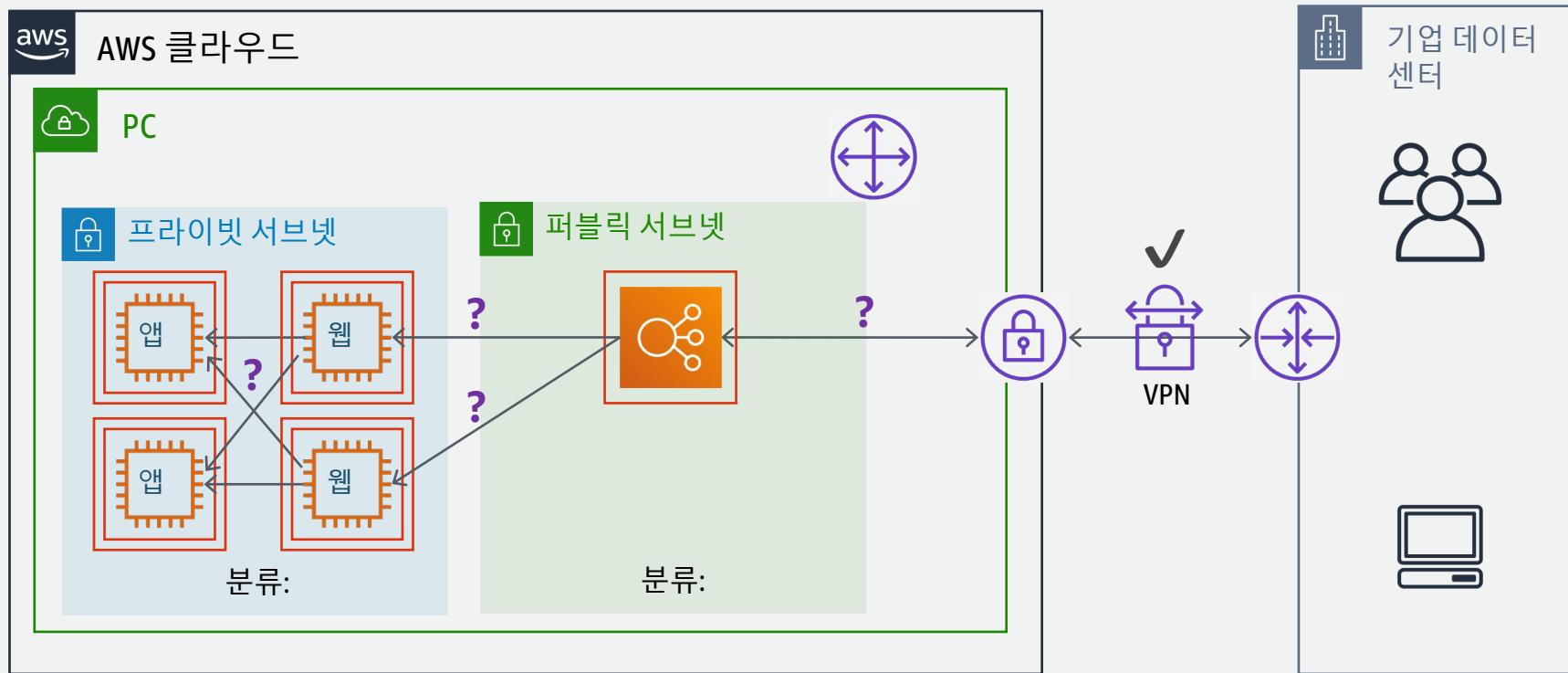
© 2022, Amazon Web Services, Inc. or its affiliates.

전송 중 암호화 – **VPC** 내부

VPC란 무엇입니까?

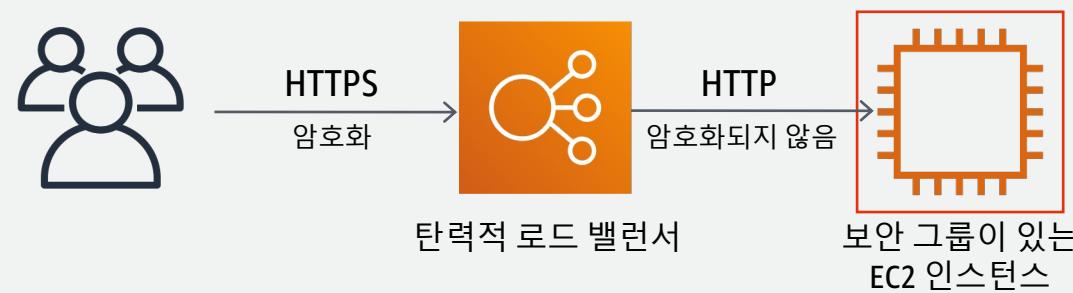
- 가상 **프라이빗** 클라우드
- AWS 인프라의 **논리적으로 격리된 부분**
- 기존 데이터 센터 네트워크를 클라우드로 확장할 수 있습니다.
- PCI 규정 준수에 의해 **사설 네트워크로 간주** 될 수 있습니다.
- SOC1/2, ISO27001, FedRAMP, HIPAA BAA, PCI에서 **감사 및 인증**
- 대부분의 L2/L3 공격으로부터 보호 (**멀티캐스트, IP/MAC/ARP 스폐핑, 스니핑**)

전송 중 암호화 - VPC 내부

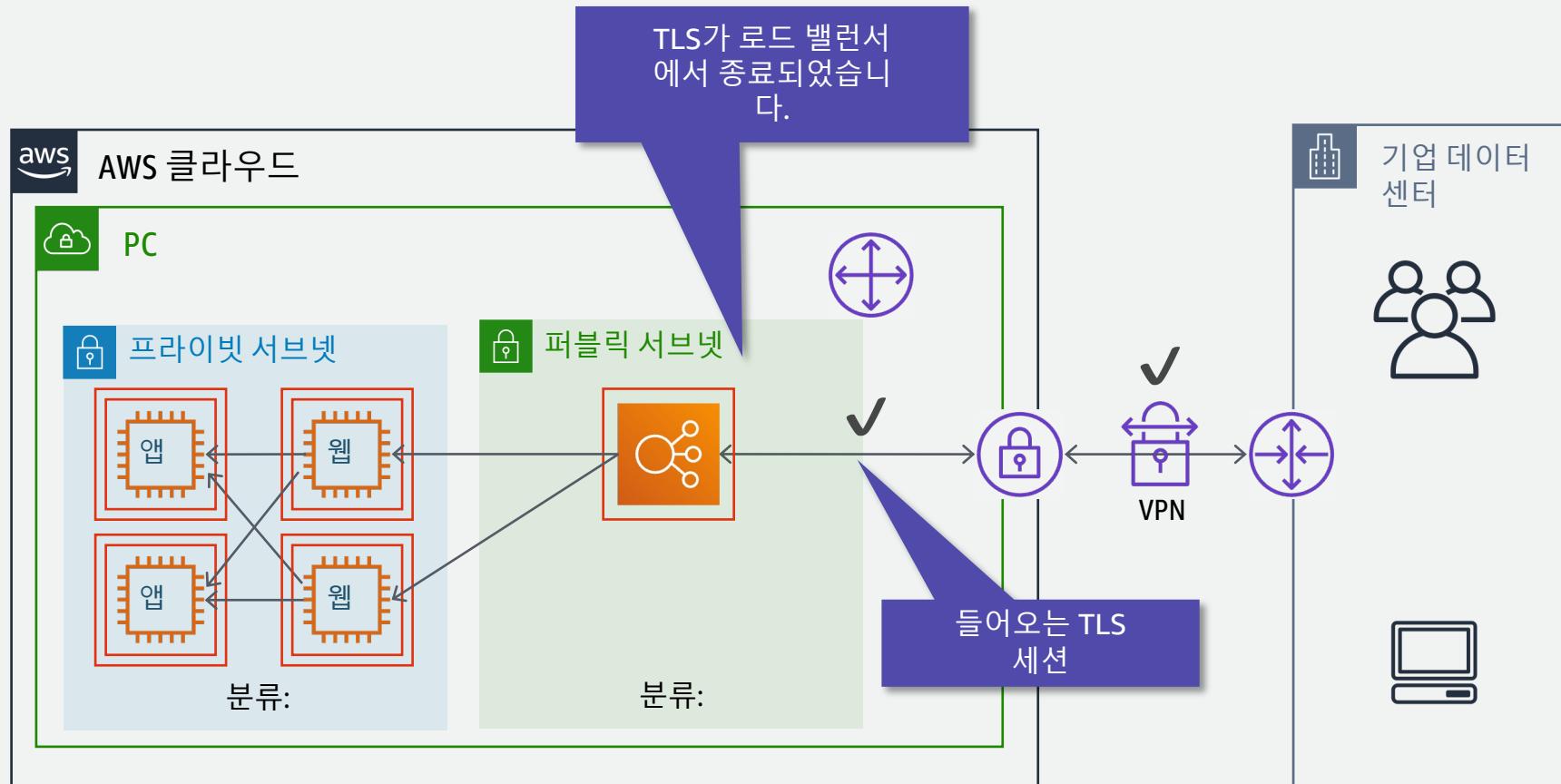


전송 중 암호화 – Amazon ELB를 사용하는 TLS

HTTPS 종료에 ELB를 사용하여 포트 80의 백엔드 인스턴스에 대한 암호화되지 않은 통신과 함께 사용할 수 있습니다.

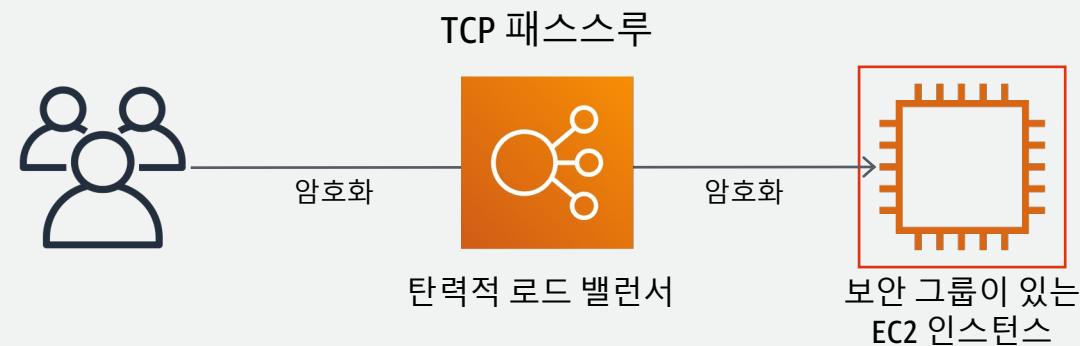


전송 중 암호화 - VPC 내부

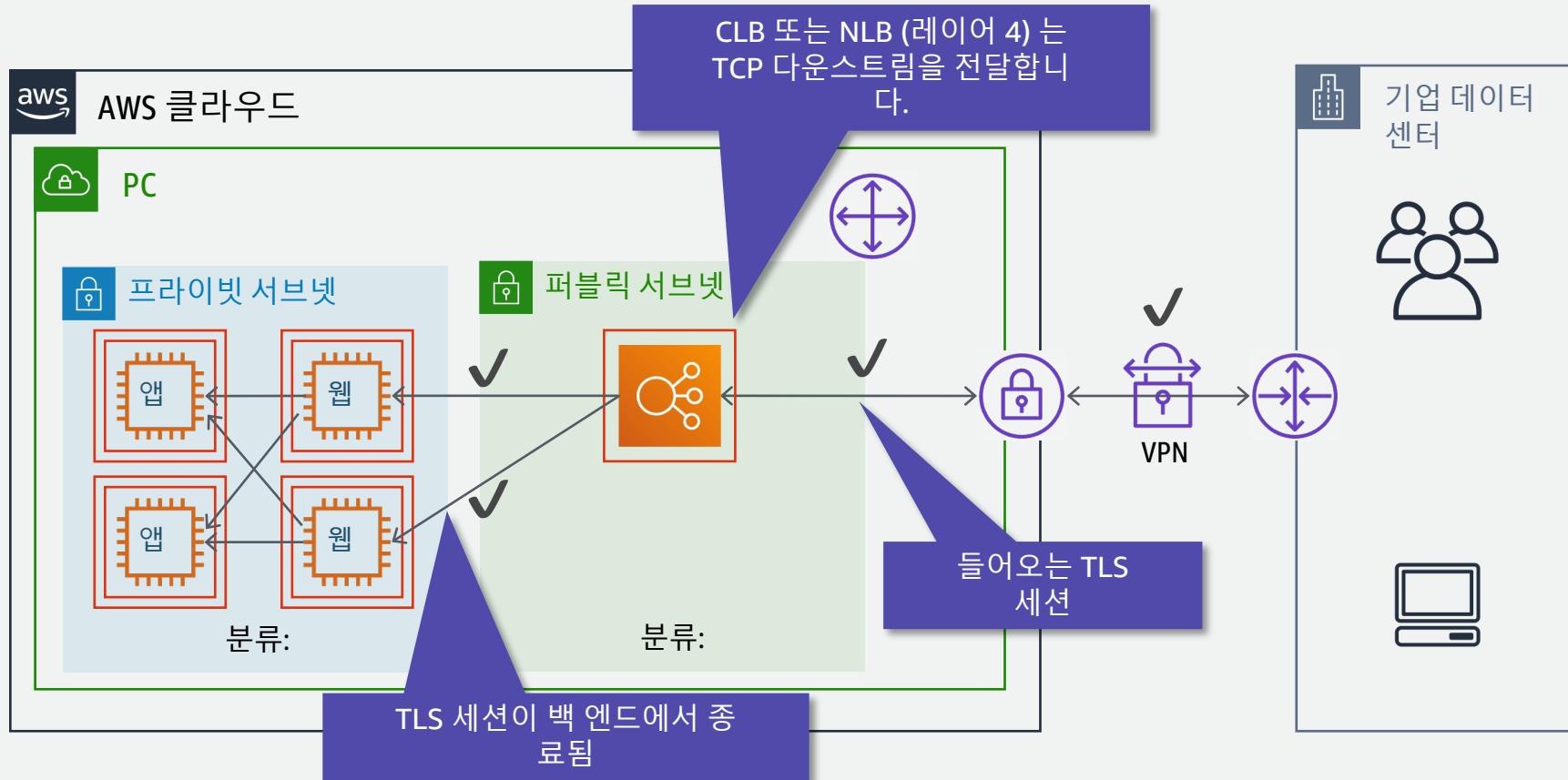


전송 중 암호화 – **Amazon ELB**를 사용하는 TLS

또는 TCP 패스스루 모드에서 클래식 로드 밸런서 및 네트워크 로드 밸런서를 사용하여 EC2 인스턴스에서 TLS 연결을 종료할 수 있습니다.



전송 중 암호화 - VPC 내부



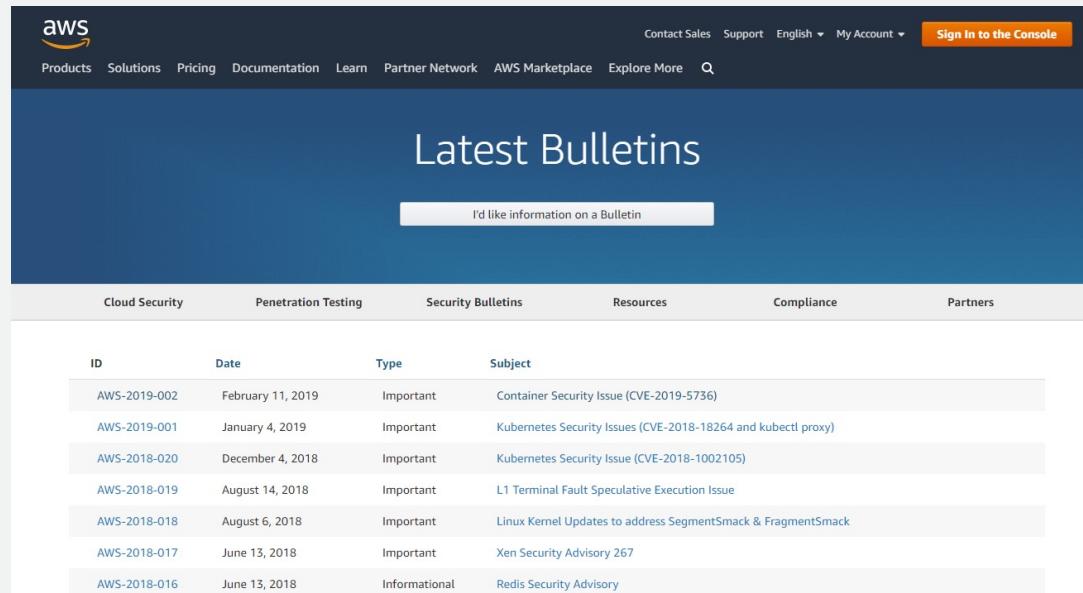
전송 중 암호화 - **ELB** 옵션

	클래식 로드 밸런서	애플리케이션 로드 밸런서	네트워크 로드 밸런서
프로토콜	TCP, SSL/TLS, HTTP, HTTPS	HTTP, HTTPS	TCP, TLS
네트워크 계층	L4 — L7	L7	L4
ACM과의 통합	✓	✓	✓
공개 키를 기반으로 하는 백엔드 TLS 인증	✓	✗	✗
서버 이름 표시 (SNI)	✗	✓	✗
여러 보안 정책	✓	✓	✓
사용자 지정 보안 정책	✓	✗	✗

전송 중 암호화 - **ELB** 옵션

아마존은 다음 사항에 대해 당일 완화를 제공할 수 있습니다.

- 하트블리드
- 푸들
- 로그잼

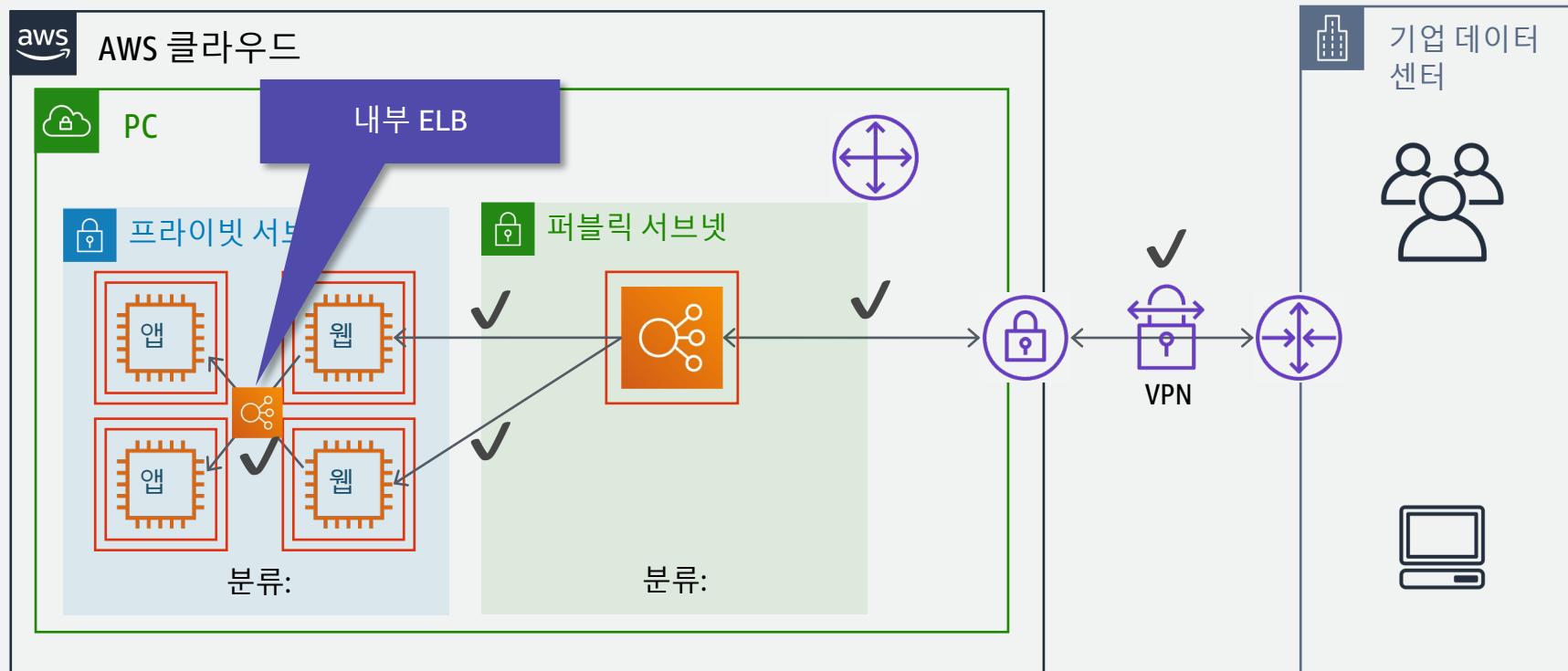


The screenshot shows the AWS Security Bulletins page. At the top, there's a navigation bar with links for Contact Sales, Support, English, My Account, and Sign in to the Console. Below the navigation is a dark blue header with the text "Latest Bulletins". A button labeled "I'd like information on a Bulletin" is visible. The main content area features a table with columns for Cloud Security, Penetration Testing, Security Bulletins, Resources, Compliance, and Partners. The table lists seven security bulletins, each with a unique ID, date, type, and subject. The subjects include Container Security Issue (CVE-2019-5736), Kubernetes Security Issues (CVE-2018-18264 and kubectl proxy), Kubernetes Security Issue (CVE-2018-1002105), L1 Terminal Fault Speculative Execution Issue, Linux Kernel Updates to address SegmentSmack & FragmentSmack, Xen Security Advisory 267, and Redis Security Advisory.

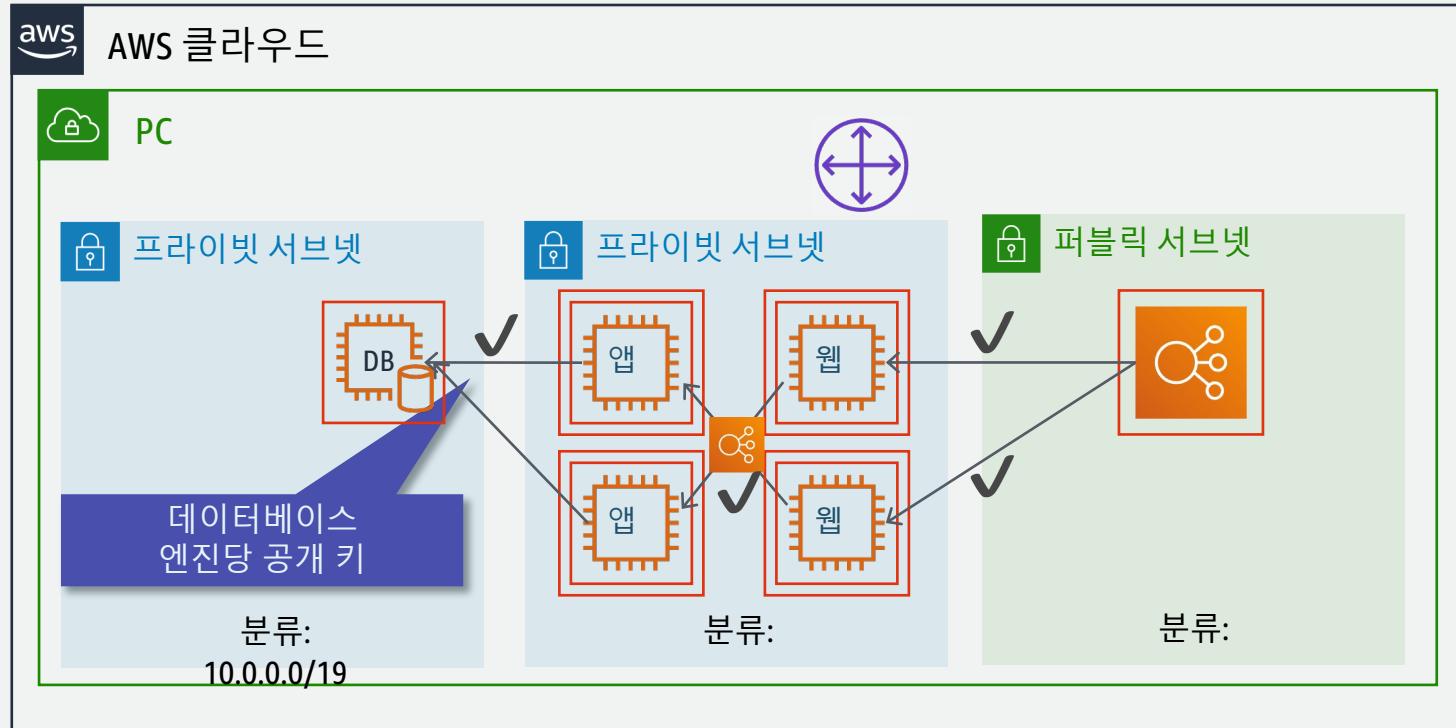
ID	Date	Type	Subject
AWS-2019-002	February 11, 2019	Important	Container Security Issue (CVE-2019-5736)
AWS-2019-001	January 4, 2019	Important	Kubernetes Security Issues (CVE-2018-18264 and kubectl proxy)
AWS-2018-020	December 4, 2018	Important	Kubernetes Security Issue (CVE-2018-1002105)
AWS-2018-019	August 14, 2018	Important	L1 Terminal Fault Speculative Execution Issue
AWS-2018-018	August 6, 2018	Important	Linux Kernel Updates to address SegmentSmack & FragmentSmack
AWS-2018-017	June 13, 2018	Important	Xen Security Advisory 267
AWS-2018-016	June 13, 2018	Informational	Redis Security Advisory

<https://aws.amazon.com/security/security-bulletins/>

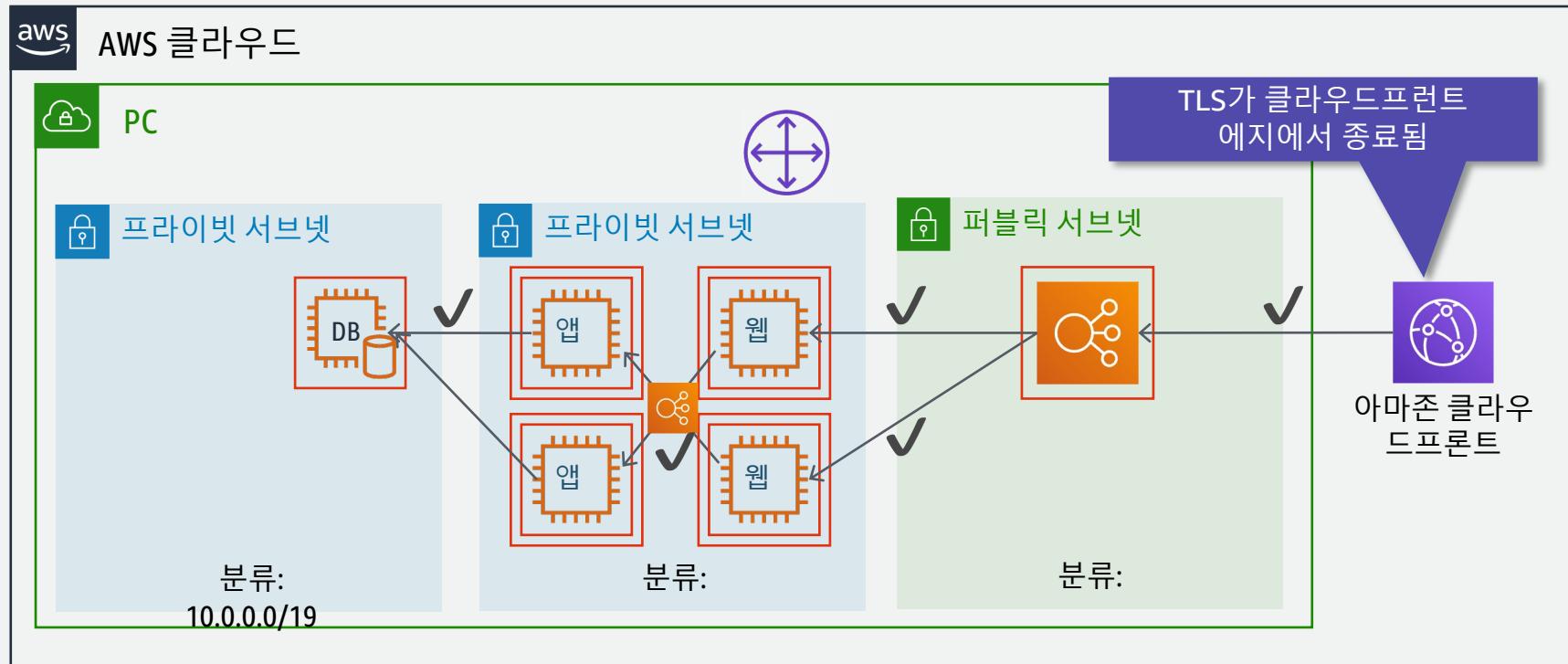
전송 중 암호화 - VPC 내부



전송 중 암호화 - VPC 내부



전송 중 암호화 - VPC 내부



전송 중 암호화 – **AMAZON** 인증서 관리자(ACM)

- AWS 리소스에서 사용할 수 있도록 AWS에서 신뢰할 수 있는 SSL/TLS 인증서를
프로비저닝합니다.
 - Elastic Loadbalancing (ALB / CLB)
 - Amazon CloudFront
 - Amazon API Gateway
 - AWS Elastic Beanstalk
- AWS가 수고를 처리합니다.
 - 키 쌍 및 CSR 생성
 - 갱신 및 배포 관리
- 이메일 또는 DNS (Route 53) 를 통한 DV (도메인 유효성 검사)
- AWS 관리 콘솔, AWS 명령줄 인터페이스 (AWS CLI) 또는 API를 통해 사용 가능



전송 중 암호화 – ACM Private Certificate Authority

사설 SSL/TLS 인증서 발급기관(CA)을 관리형으로 제공

- 기업 내부의 웹서버, API G/W, SSL VPN, IoT 환경 등

지원되는 개인키 알고리즘

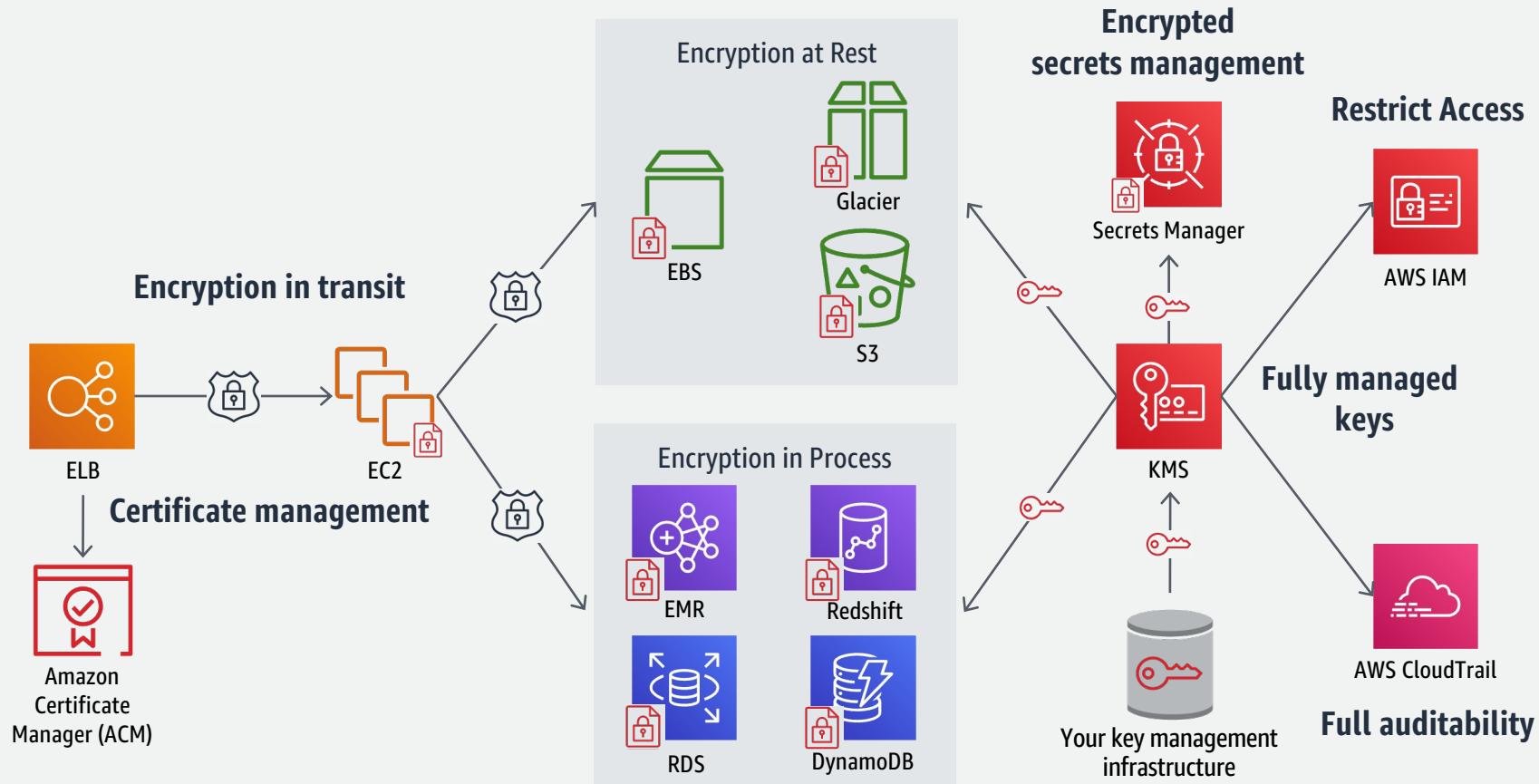
- RSA 2048 / RSA 4096 / ECDSA P256 / ECDSA P384

관리가 까다로운 PKI 영역을 AWS가 대신함

- 사설CA 인프라의 안정적인 관리
- 인증서의 안전한 보관(FIPS 140-2 Level 3를 지원하는 HSM)
- 인증서 폐기 목록(CRL) 배포 관리



데이터 암호화 - 유비쿼터스 암호화



Q & A



Thank you!