

Encryption and Data Protection 2

서버측 암호화 비교

박병화

Security Risk & Compliance

AWS Proserve

Agenda

1. 서버측 암호화 종류 및 CloudTrail 로그
2. KMS 활용방식 및 비용
3. 서버측 암호화 - Key 비교
4. 주요 Q&A
5. KMS Best Practices

서버측 암호화

Amazon S3 > Buckets > test-bhpark-s3 > Edit default encryption

Edit default encryption [Info](#)

Default encryption

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

Server-side encryption

- ☒ Disable
☐ Enable

서버측 암호화 여부

Cancel

Save changes

- ✓ Amazon S3에서 데이터 센터의 디스크에 데이터를 쓰면서 객체 수준에서 데이터를 암호화하고, 사용자가 해당 데이터에 액세스할 때 자동으로 암호를 복호화합니다.
- ✓ 동일한 객체에 서로 다른 서버측 암호화 유형을 동시에 적용할 수는 없습니다.
- ✓ 서버 측 암호화는 객체 메타데이터가 아니라 객체 데이터만 암호화합니다.



서버측 암호화 종류

Amazon S3 > Buckets > test-bhpark-s3 > Edit default encryption

Edit default encryption [Info](#)

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](#)

Cancel

Save changes

Amazon S3-managed Key (SSE-S3)

- AWS Owned Key
- AES-256 GCM을 사용하여 암호화
- SSE-S3암호화에 추가 요금 없음
- 1년의 자동 키 교환 주기(May 2022~)

AWS Key Management Service Key (SSE-KMS)

- 객체에 대한 무단 액세스에 대해 추가적인 보호 제공(KMS 키 사용 권한 필요)
- KMS 키 사용 일시 및 주체를 기록하는 감사 추적 기능 (w/ CloudTrail)
- AMK / CMK

서버측 암호화 종류

Amazon S3 > Buckets > test-bhnpark-s3 > Edit default encryption

Edit default encryption [Info](#)

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-2:341155410232:alias/aws/s3

☐ Choose from your AWS KMS keys

☐ Enter AWS KMS key ARN

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

☐ Disable

☒ Enable

[Cancel](#) [Save changes](#)

AWS Managed Key 사용 또는 Customer Managed Key 사용

- AMK :
 - 객체를 처음으로 추가할 때, AMK 키가 자동 생성(default)
 - 다른 S3 버킷에서 KMS-AMK를 사용할 경우, 동일 키를 사용
- CMK :
 - 보다 유연한 컨트롤 가능(생성, 로테이션, 비활성화, 권한, 감사 등)
 - S3의 경우, KMS-CMK 생성시 대칭키만(symmetrical) 지원

Bucket Key

- Amazon S3에서 AWS KMS로의 요청 트래픽을 줄여 AWS KMS 요청 비용 최대 99%까지 감소

KMS

- CloudTrail Log



CloudTrail



Dashboard

Event history

Insights

Lake [New](#)

Trails

Pricing

Documentation

Forums

FAQs

Event record [Info](#)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAU63TSOE4IB2IZXNDB",
    "arn": "arn:aws:iam::341155410232:user/admin",
    "accountId": "341155410232",
    "accessKeyId": "ASIAIUK7RH7Q7FCBTZJQ",
    "userName": "admin",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-05-26T01:19:44Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "invokedBy": "AWS Internal"
},
{
  "eventTime": "2022-05-26T07:51:34Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "ap-northeast-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "encryptionContext": {
      "aws:s3:arn": "arn:aws:s3:::test-bhpark-s3-2"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "d820b5c5-3a16-4ac8-8802-4936ecd8d3cf",
  "eventID": "7eff9840-d703-4085-abf8-9b6a8b8156e3",
  "readOnly": true,
  "resources": [
    {
      "accountId": "341155410232",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:ap-northeast-2:341155410232:key/bde655df-a644-4281-b8c4-950655645575"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "341155410232",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": true
}
```

사용자

일시/이벤트

리소스

KMS Key

AWS 서비스에서 KMS를 활용하는 방식

- EC2/EBS 모델

- ✓ EBS 볼륨 별로 데이터 키를 생성하고, CMK로 암호화한 뒤 볼륨 메타데이터에 저장
- ✓ 고객의 EBS리소스가 EC2에 붙어 있는 동안, 해당 EBS볼륨을 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 Get요청에 대해 S3는 KMS쪽으로 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 CMK Policy로 정의
- Key Policy 사례:
 - ✓ <지정된 Account>의 <지정된 User와 Role>만, 암호/복호화 수행한다.
 - ✓ 어플리케이션 A에서만 데이터를 암호화하고, 어플리케이션 B에서만 그 데이터를 복호화 할 수 있다.
 - ✓ 지정된 관리 그룹 혹은 Role에 의해 키 관리 가능하다.
 - ✓ <지정된 Account>만이 암호/복호화 작업을 수행할 수 있으나, 다른 키 관리작업(생성/삭제/정책관리/위임 등)은 불가하다.

AWS 서비스에서 KMS를 활용하는 방식 예제

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-2",
  "Statement": [
```

111122223333 Account에 KMS
Key의 모든 액세스 권한 부여

```
{
  "Sid": "Enable IAM policies",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
},
```

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KMSAdminUser",
    "arn:aws:iam::111122223333:role/KMSAdminRole"
  ]},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
},
```

IAM 사용자 KMSAdminUser 및 IAM Role
KMSAdminRole이 Key 관리하도록 허용

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/ExampleUser",
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/ExampleUser",
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
}
}
```

IAM 사용자 KMSAdminUser 및 IAM Role
KMSAdminRole 그리고 444455556666
Account가 Key 관리하도록 허용

AWS KMS 비용 예제 (Free tier 월 20,000건)

- AMAZON EBS

- 1개의 KMS Key 사용 : 1 USD
- 250개의 볼륨에 데이터 암호화 Key를 생성 및 프로비저닝을 위한 API 3 호출(총 3 x 250 : 750 API) : 0 USD

** 결과 : 1.00 USD / Month

- AMAZON S3

- 1개의 KMS Key 사용 : 1 USD
- 월 10,000개의 오브젝트 암호화 요청 (10,000건의 암호화 요청 API)
- 월 2,000,000회 액세스 (2,000,000 건의 복호화 요청 API)

** 결과 : 1.00 USD + 5.97 USD $\{(2,010,000 - 20,000) \times 0.03 \text{ USD} / 10,000\} = 6.97 \text{ USD} / \text{Month}$

Free Tier : 20,000 Request

\$0.03 per 10,000 requests

\$0.03 per 10,000 requests involving RSA 2048 keys

\$0.10 per 10,000 ECC GenerateDataKeyPair requests

\$0.15 per 10,000 asymmetric requests except RSA 2048

\$12.00 per 10,000 RSA GenerateDataKeyPair requests

https://docs.cloudera.com/HDPDocuments/HDP3/HDP-3.1.5/bk_cloud-data-access/content/S3-encryption-performance.html



서버측 암호화 - Key 비교

	AWS Owned Key	AWS Managed Key	Customer Managed Key
생성 주체	AWS에서 생성한 키	고객을 대신하여 생성된 AWS	고객이 생성됨
자동 키 교체	1 년에 한번 자동으로	1 년에 한번 자동으로	선택적 (수동 또는 일 년에 한번 자동)
키 삭제	삭제 불가	삭제 불가	삭제 가능
AWS 계정에서 KMS Key 메타 데이터를 볼 수 있는지	불가	가능	가능
나의 AWS 계정만을 위해 사용되는지	특정 계정에만 국한되지 않음	<ul style="list-style-type: none"> AWS 계정내의 특정 AWS 서비스로 제한 	<ul style="list-style-type: none"> AWS 계정내의 특정 AWS 서비스로 제한 KMS/IAM 정책을 통해 제어

* KMS 메타데이터 : 데이터를 암호화하고 복호화하는 데 사용되는 키 구성 요소 외에도 키 ID, 생성 날짜, 설명 및 키 상태



주요 Q&A

<https://aws.amazon.com/ko/kms/faqs/>

Q: 자체 키를 AWS KMS로 가져올 수 있습니까?

예. 자체 키 관리 인프라에서 키 사본을 AWS KMS로 가져와서 통합된 다른 AWS 서비스에서 사용하거나 자체 애플리케이션 내에서 사용할 수 있습니다. **비대칭 KMS 키는 AWS KMS로 가져올 수 없습니다.**

Q: 자동으로 키를 교체할 수 있습니까?

예. **AWS KMS HSM 내에서 생성된 키에 한해 AWS KMS가 KMS 키를 매년 자동으로 교체하도록 선택할 수 있습니다.** 키를 가져왔거나, 키가 비대칭이거나, AWS CloudHSM 클러스터에서 KMS 사용자 지정 키 스토어 기능을 사용해 키를 생성했다면 자동 키 교체 기능이 지원되지 않습니다.

Q: AWS KMS의 키가 교체된 후 내 데이터를 다시 암호화해야 합니까?

키를 AWS KMS에서 자동으로 교체하도록 선택한 경우 데이터를 다시 암호화할 필요가 없습니다. AWS KMS가 자동으로 키의 이전 버전을 보관하여 이전 버전의 키로 암호화된 데이터의 복호화에 사용합니다. AWS KMS의 키에 대한 모든 새 암호화 요청은 최신 버전의 키로 암호화됩니다.

Q: AWS KMS에 만들 수 있는 키 개수에 제한이 있습니까?

리전별로 계정마다 최대 10,000개의 KMS 키를 생성할 수 있습니다.

Q: AWS KMS에서 내 키 구성을 누가 사용하고 변경했는지 어떻게 알 수 있습니까?

AWS CloudTrail의 로그에는 관리 요청(예: 생성, 교체, 비활성화, 정책 편집)과 암호화 요청(예: 암호화/복호화)을 비롯하여 모든 AWS KMS API 요청이 표시됩니다.

Q: AWS KMS는 서비스 수준 계약(SLA)을 제공합니까?

예. AWS KMS SLA는 고객의 월간 가동률이 월별 결제 주기 동안 서비스 약정보다 낮을 경우 서비스 크레딧을 제공합니다.



KMS Best Practices

<https://d1.awsstatic.com/whitepapers/aws-kms-best-practices.pdf>

- AWS KMS, IAM Policy, Key Policy – Least Privilege / Separation of Duties
- CMK Auditing – CloudTrail + S3 bucket
- Encrypting PCI Data Using AWS KMS
- Secret Management Using AWS KMS and Amazon S3
- Encrypting Lambda Environment Variables
- Enforcing Data at Rest Encryption within AWS Services – S3, EBS, RDS



Q & A



Thank you!

데이터 암호화 - 봉투 암호화 입문서

