# AWS문제풀이

기업의 데이터 계층은 PostgreSQL 데이터베이스용 Amazon RDS를 기반으로 합니다. 조직은 데이터베이스 비밀번호 순환을 채택해야 합니다.

다음 중 운영 오버헤드가 가장 적은 이 기준을 충족하는 옵션은 무엇입니까?

A. AWS Secrets Manager에 암호를 저장합니다. 보안 비밀에 대한 자동 순환을 활성화합니다.

B. AWS Systems Manager Parameter Store에 암호를 저장합니다. 매개변수에서 자동 회전을 활성화합니다.

C. AWS Systems Manager Parameter Store에 암호를 저장합니다. 암호를 교체하는 AWS Lambda 함수를 작성합니다.

D. AWS Key Management Service(AWS KMS)에 암호를 저장합니다. 고객 마스터 키(CMK)에서 자동 교체를 활성화합니다.

**AWS Secret Manager**

**보안 비밀에 대한 자동 순환**

틀림

**AWS Systems Manager Parameter Store**

**AWS Key Management Service (AWS KMS)**

**고객 마스터키 (CMK)**

참고

AWS KMS에서는 *고객 마스터 키(CMK)*라는 용어가 *AWS KMS key*와 *KMS 키*로 바뀌었습니다. 단, 개념은 바뀌지 않았습니다. 호환성에 영향을 미치는 변경 사항이 발생하지 않도록 AWS KMS에서는 이 용어의 일부 변형된 형태를 그대로 사용합니다.

## 기존 보안 파일 관리 방법

DB등 다른 곳으로 액세스 하기위해 필요한 값을 로컬 파일 .env에 저장하고 그 값을 사용

.env 파일

video_rank_db > .env.prod

```
HOST=keyt-db.cufestxiukhf.ap-northeast-2.rds.amazonaws.com
USER=admin
PASSWORD=dpszhdk#22
DATABASE=video_rank
```

.env의 값을 Config에 설정

video_rank_db > src > config > TS env_db.ts > dbconfig > port

You, 1 second ago | 2 authors (haraaaaaa and others)

```
import dotenv from "dotenv";
dotenv.config();

export const dbconfig = {
    host: process.env.HOST || '',
    user: process.env.USER || '',
    password: process.env.PASSWORD || '',
    database: process.env.DATABASE || '',
    port: Number(process.env.DATABASE) || 3306
};
```

Config의 정보를 가져와서 DB와 연결

video_rank_db > src > TS db.ts > connection

You, last week | 2 authors (haraaaaaa and others)

```
import mysql from 'mysql';
import { dbconfig }from "./config/env_db";
import { logger } from './log/winston';

const connection = mysql.createConnection(dbconfig);
```

## 기존 보안 파일 관리 방법

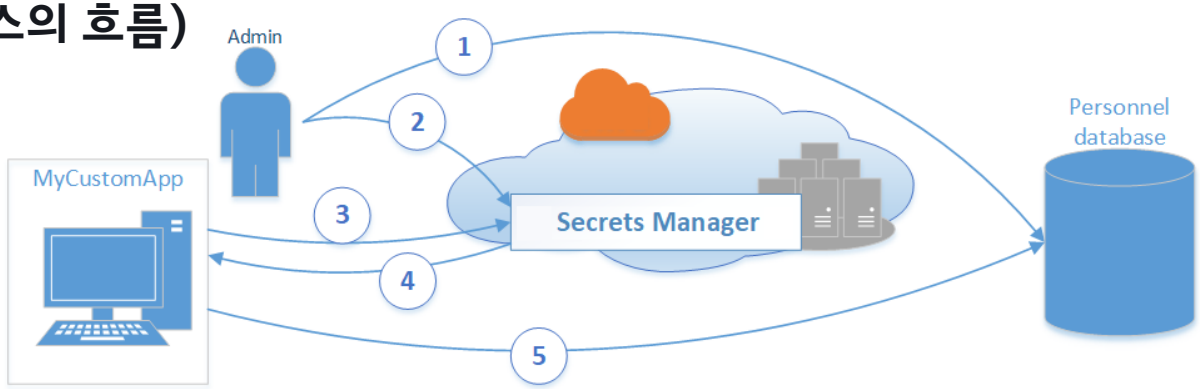
### ec2에서 환경변수를 .env로 관리 시 단점

1. aws에서 codedeploy나 autoscale group을 자주 이용하면 서버 인스턴스를 생성하고 지우는 과정에서 .env파일이 삭제되어 다시 설정해야 하는 번거로움이 있다.
2. 누군가가 ec2 인스턴스에 접속하면 해당 .env파일을 열람할 수 있어 보안적인 면에서 안심이 되지 않는다.

# AWS Secret Manager

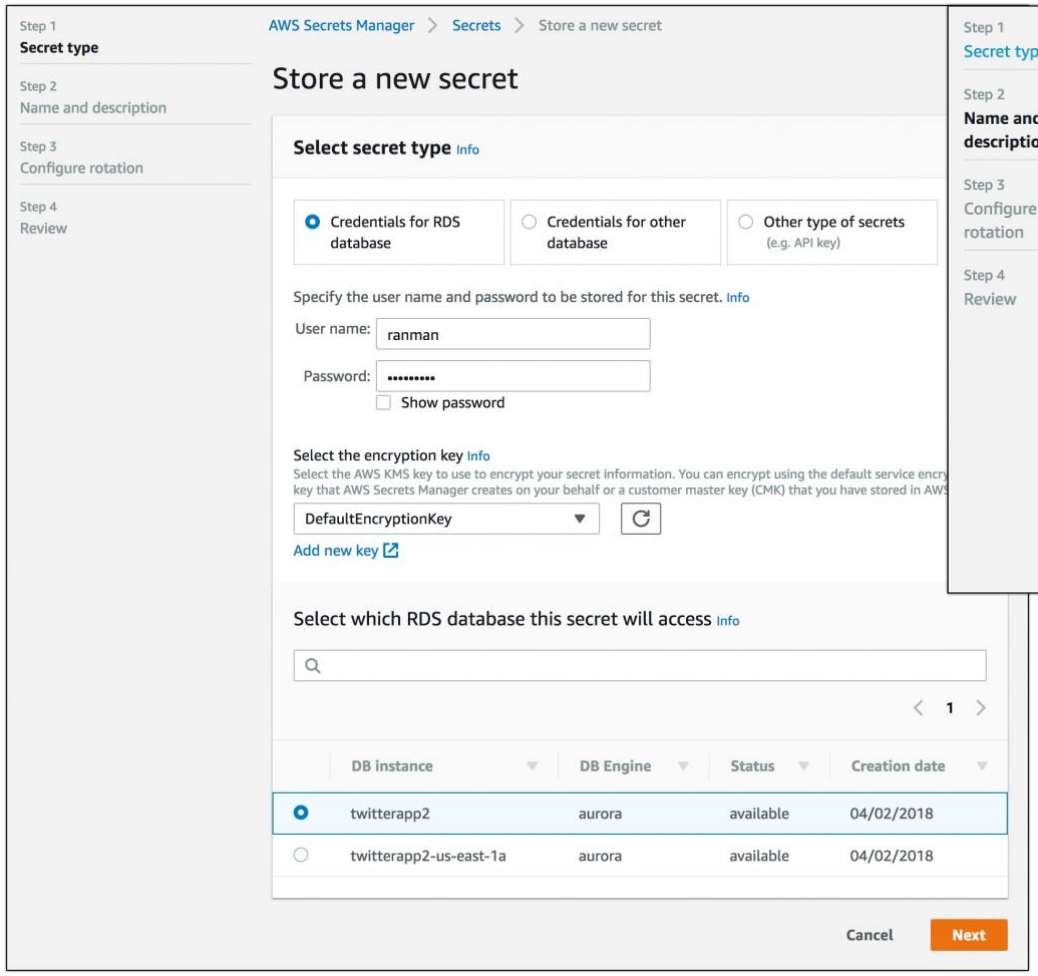
- Secrets Manager는 AWS에서 제공하는 Secret (보안 비밀) 관리 서비스
- Secret 값들을 저장해두고 어플리케이션에서 AWS의 API를 호출해서 받아가 사용하는 방식

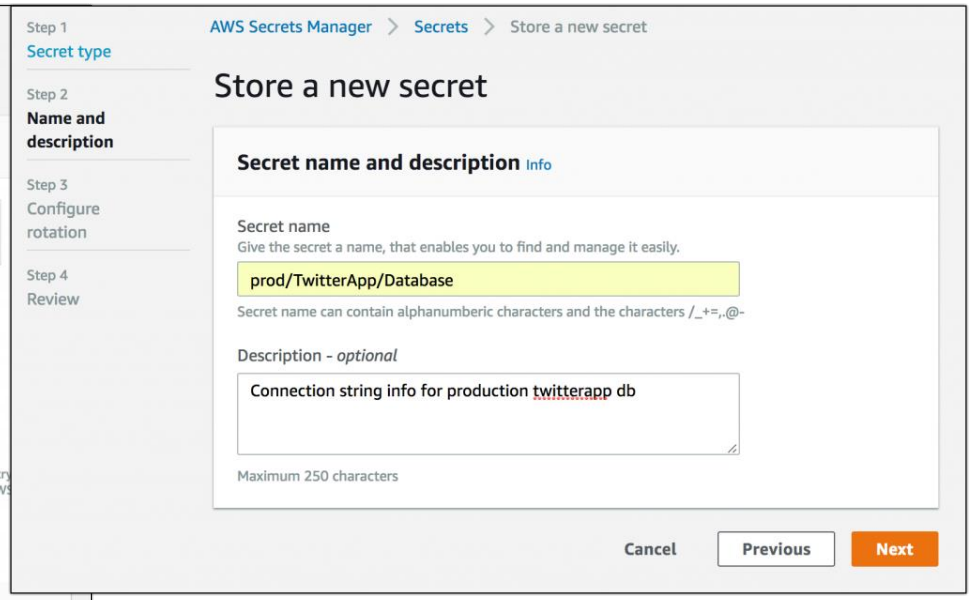
## 예시 (서비스의 흐름)




1. Admin이 MyCustomApp 애플리케이션에서 DB에 액세스 할 때 사용할 수 있도록 Personal DB에 대한 자격 증명을 생성
2. Admin이 Secrets Manager에서 자격 증명을 MyCustomAppCreds(Secret)으로 저장 하면,
   Secrets Manager는 자격 증명을 암호화하여 텍스트로 저장
3. MyCustomApp에서 DB에 액세스 할 때, 이 애플리케이션은 Secrets Manager에 MyCustomAppCreds 를 요청
4. Secrets Manager는 Secret을 검색하고 Secret 텍스트의 암호를 해독해
   보안(TLS를 통한 HTTPS) 채널을 통해 MyCustomApp 애플리케이션에 Secret 을 반환
5. MyCustomApp 애플리케이션은 응답에서 자격 증명, 연결 문자열 및 기타 필요한 정보를 구문 분석한 다음
   분석한 정보를 사용해 DB 서버에 액세스

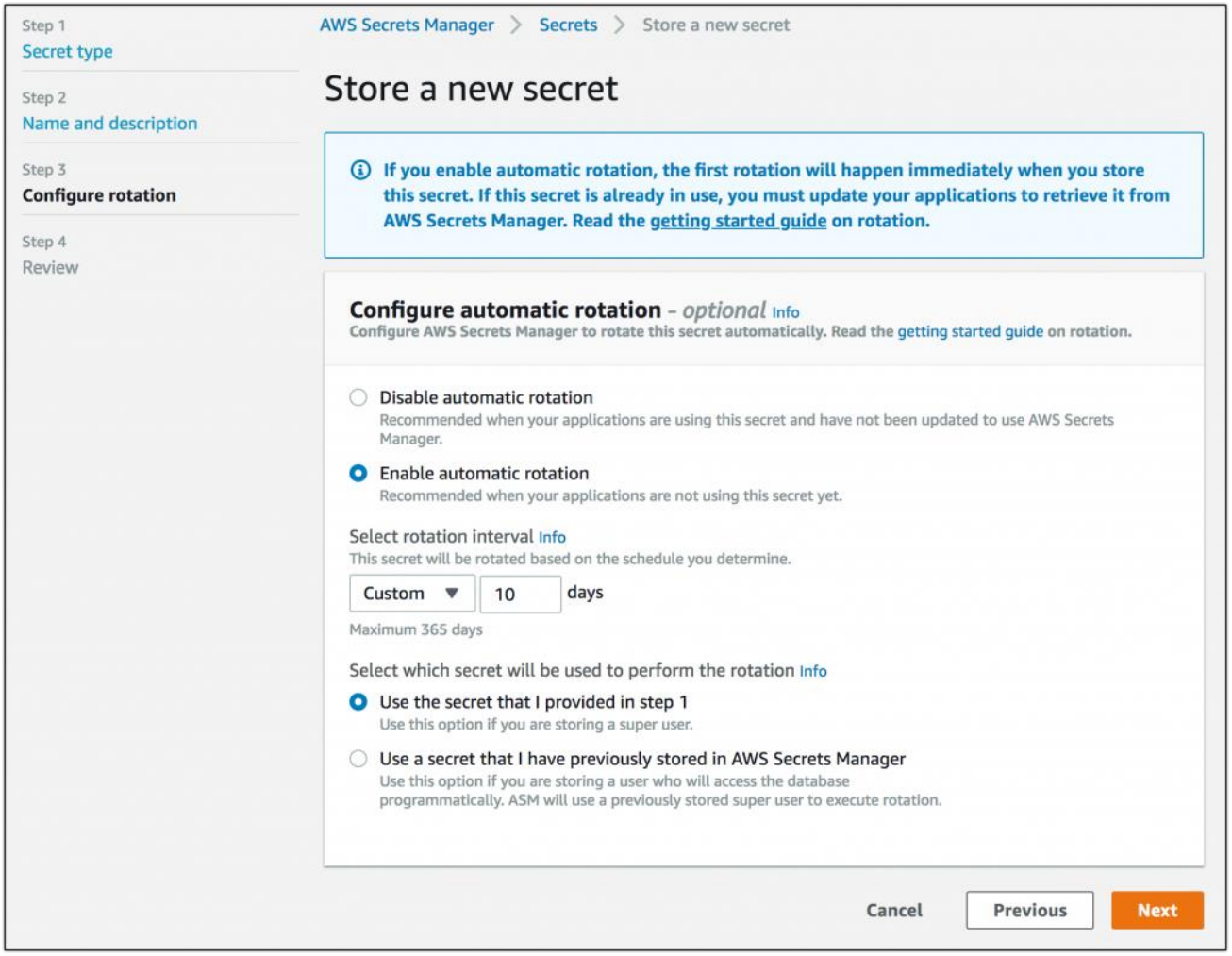
# User가 애플리케이션에서 DB에 액세스 할 때 사용할 수 있도록 DB에 대한 자격 증명을 생성



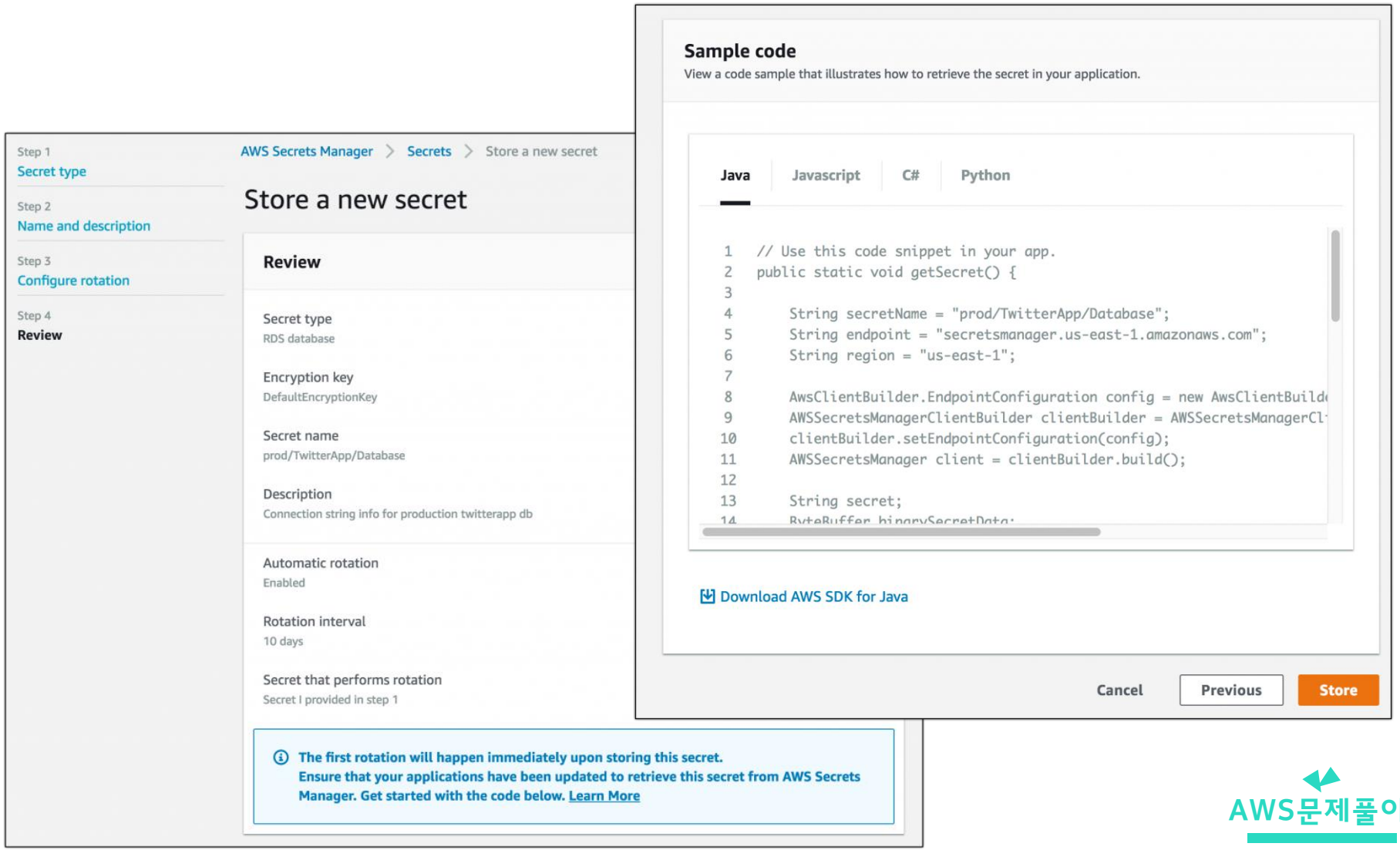

AWS문제풀이

# 보안 비밀에 대한 자동 순환

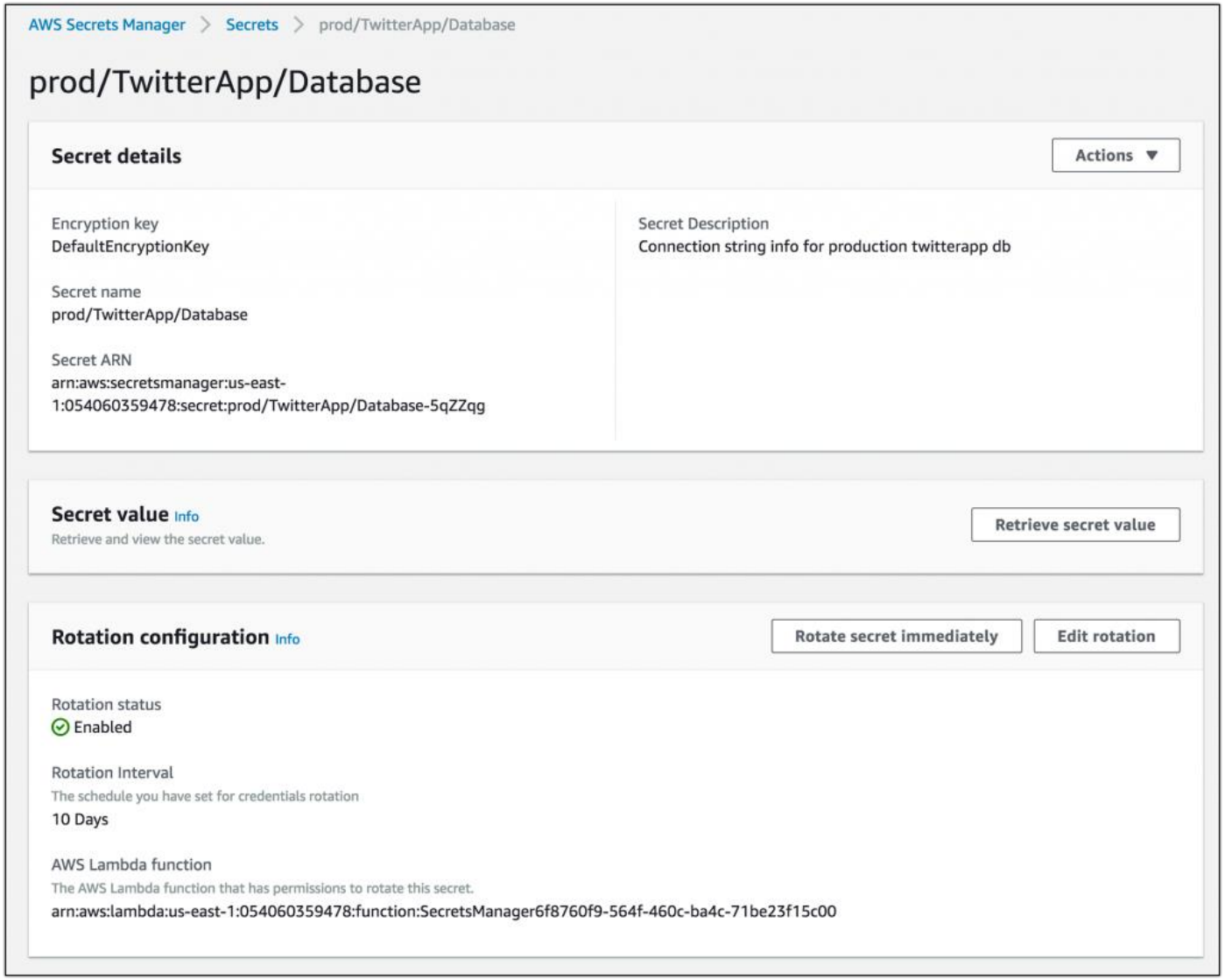



Secrets Manager에서 제공하는 Lambda 함수를 사용하여 10일마다 암호를 교체하도록 교체 설정을 구성

# 세부 정보 검토 및 Secret을 저장 / 검색하는 샘플 코드 확인



# 생성 완료 (AWS 콘솔에서 관리 가능)



# DB 등으로 액세스가 필요할 때 API호출

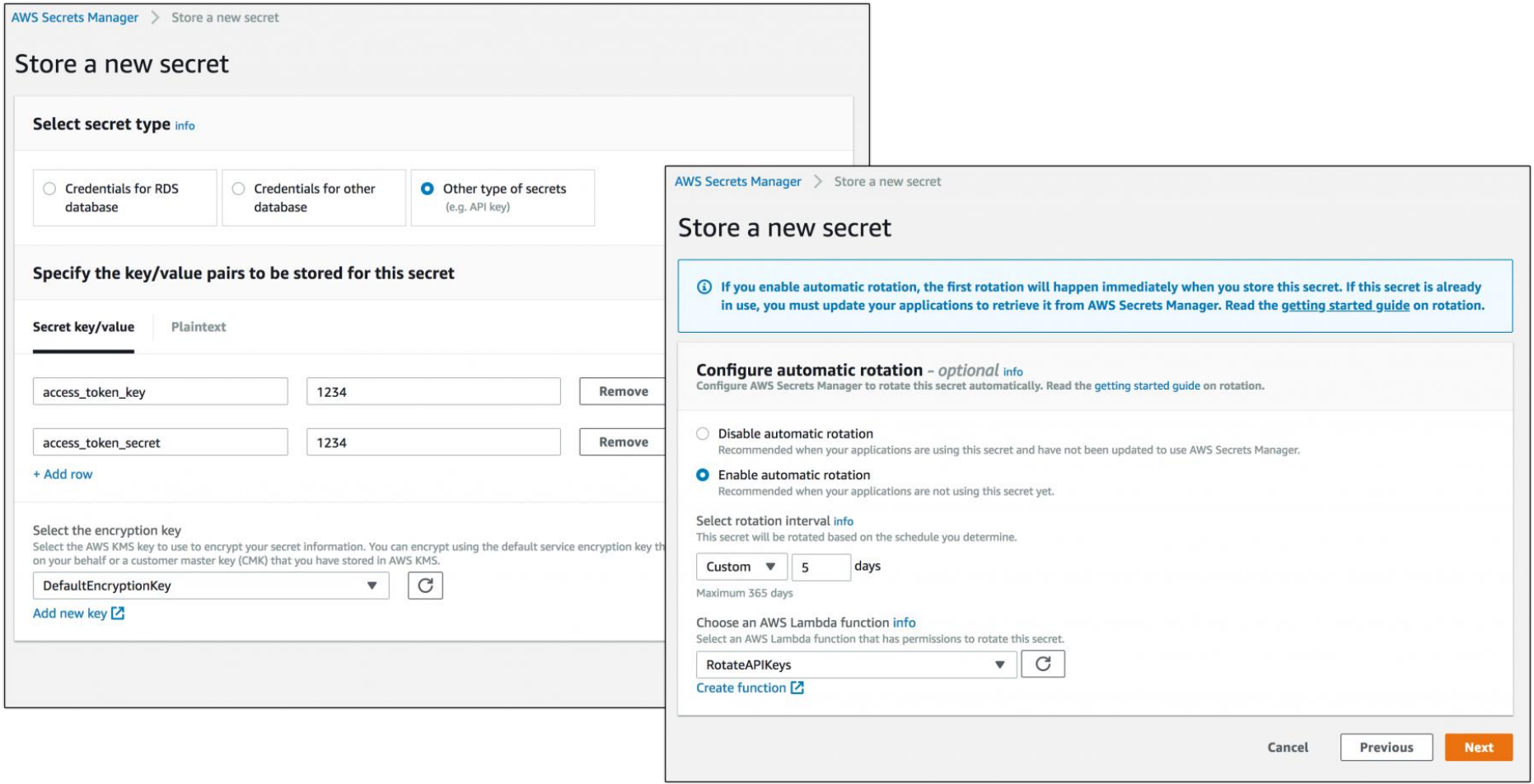
```python
import json
import boto3
secrets = boto3.client("secretsmanager")
rds = json(sm.get_secrets_value("prod/TwitterApp/Database")['SecretString'])
print(rds)
```

호출한 결과 값

```python
{'engine': 'mysql',
 'host': 'twitterapp2.abcdefg.us-east-1.rds.amazonaws.com',
 'password': '-)Kw>THISISAFAKEPASSWORD:lg{&sad+Canr',
 'port': 3306,
 'username': 'ranman'}
```

# 다양한 값을 Secret으로 저장 가능

- 단순한 password 뿐 만 아니라 Oauth 자격 증명, 이진 데이터 등을 저장 가능
- AWS Lambda 함수를 사용하여 이러한 타사(Twitter) OAuth 자격 증명의 교체도 정의 가능



# AWS Systems Manager Parameter Store

## Systems Manager Parameter Store 이란?

- AWS Systems Manager 서비스 중 하나로, 데이터 관리 및 암호 관리를 위한 안전한 계층적 스토리지를 제공하는 서비스
- 암호, 데이터베이스 문자열, Amazon Machine Image(AMI) ID 및 라이센스 코드를 파라미터 값으로 지정 가능
- 값을 일반 텍스트 또는 암호화된 데이터로도 저장 가능
- 파라미터를 생성할 때 지정한 고유 이름을 사용하여 스크립트, 명령, SSM 문서 및 구성 및 자동화 워크플로우에서 Systems Manager 파라미터 참조 가능
- Parameter Store는 Secrets Manager와도 통합되어 있음
  (EC2, ECS, Lambda, Cloud Formation, Code Build, Code Deploy 등 다른 AWS 서비스에 대한 Secret을 사용하는 경우만)

## Systems Manager Parameter Store 의 장점

- 안전하고 확장 가능한 호스팅 방식 암호 관리 서비스이기 때문에 개발자가 따로 서버를 관리할 필요가 없음
- 데이터를 코드와 격리하여 보안 개선
- 구성 데이터 및 암호화된 문자열을 계층으로 저장하고 버전을 추적 가능
- 세분화된 수준에서 액세스를 제어하고 감시
- Parameter Store는 AWS 리전의 여러 가용 영역에서 호스팅되기 때문에 파라미터를 안정적으로 저장 가능

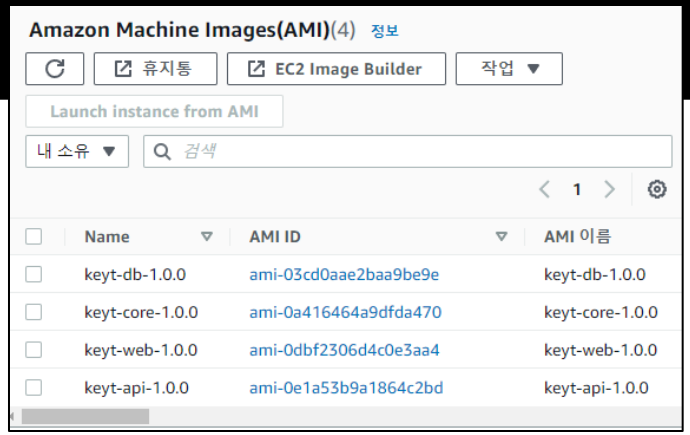
# AWS Systems Manager Parameter Store

## Systems Manager Parameter Store 의 기능

- 변경 알림
- 액세스 구성 및 제어
    - 특정 환경, 부서, 사용자, 그룹 또는 기간의 파라미터에 태그 지정
    - 지정된 태그를 통해 IAM로 액세스 제한 가능

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:ListGroupsForUser",
            "Resource": "arn:aws:iam::111222333444:user/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
            }
        }]
}
```

- 레이블(Label) 버전
    - 레이블로 버전관리가 가능
- 데이터 유효성 검사
    - 예상 리소스 유형을 참조하는지, 리소스가 존재하는지, 리소스 사용 권한이 있는지 확인 가능



# AWS Systems Manager Parameter Store

## Systems Manager Parameter Store 의 기능

- 참고 보안 암호
    - 다른 AWS 서비스를 사용할 때 Secrets Manager 암호를 검색할 수 있도록 AWS Secrets Manager와 통합
- Parameter를 사용하는 다른 AWS 서비스에서 액세스 가능
    - Amazon Elastic Compute Cloud(Amazon EC2)
    - Amazon Elastic Container Service(Amazon ECS)
    - AWS Secrets Manager
    - AWS Lambda
    - AWS CloudFormation
    - AWS CodeBuild
    - AWS CodePipeline
    - AWS CodeDeploy
- 암호화, 알림, 모니터링 및 감사 기능을 하는 다른 AWS 서비스와 연계 가능
    - AWS Key Management Service (AWS KMS)
    - Amazon Simple Notification Service (Amazon SNS)
    - Amazon CloudWatch
    - Amazon EventBridge
    - AWS CloudTrail

# AWS Systems Manager Parameter Store

## Systems Manager Parameter Store 사용 예시 흐름

1. AWS 콘솔에서 파라미터 생성 (이름/유형/값 입력)
2. 사용할 EC2에 자격 증명 생성

```
AWS Access Key ID [None]: # 입력 후 엔터
AWS Secret Access Key [None]: # 입력 후 엔터
Default region name [None]: # 입력 후 엔터
Default output format [None]: json # 공백으로 하고 엔터를 해도 무관하다.
```

3. IAM설정

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath",
        "ssm:GetParameter"
      ],
      "Resource": "arn:aws:ssm:본인의 region:aws 계정 번호:parameter/*"
    }
  ]
}
```

4. 코드로 파라미터 가져오기

```
const awsParamStore = require( 'aws-param-store' );
const paramName = "config"; // parameter store에서 추가한 파라미터의 이름
const region = 'ap-northeast-2';

const parameter = awsParamStore.getParameterSync(paramName, { region });

module.exports = JSON.parse(parameter.Value);
```

## 차이점

| | Systems Manager Parameter Store | Secret Manager |
|---|---|---|
| 비밀번호 생성 | X | AWS CLI 또는 SDK를 통해 임의의 문자열(암호) 생성 가능 |
| 자동 순환 | X | AWS Lambda를 이용하여 자동 변경 가능 |
| 비용 | 추가비용은 없지만<br>계정당 10,000개로 제한 | 저장된 Secret당 0.40 USD의 비용이 들며,<br>10,000번의 API 호출에 대해 0.05 USD의 추가 비용 있음 |
| 교차 계정 액세스 | X | Secret을 다른 계정과 공유 가능 |

## 결론

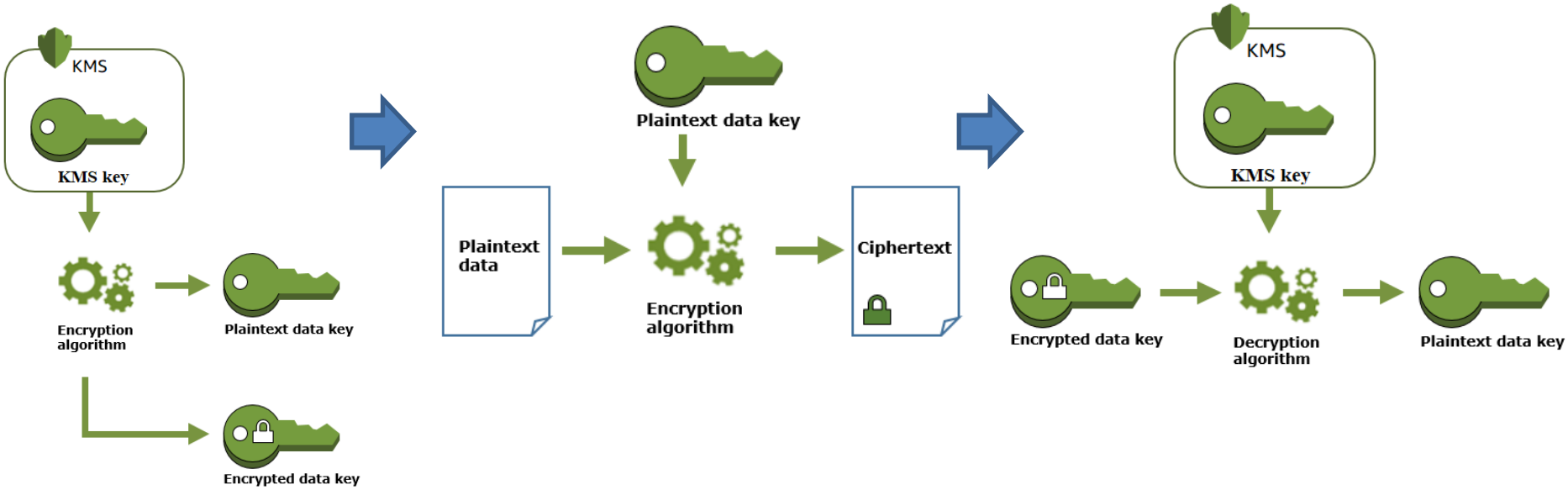
**보안에서는 Secret Manager가 안전, 금액에서는 Systems Manager Parameter Store이 저렴하기 때문에 유리**

# AWS Key Management Service (AWS KMS)

암호화 키의 라이프사이클을 관리하는 전용 시스템으로 암호화 키의 생성, 저장, 백업, 복구, 파기 등의 기능을 제공하는 시스템

## 데이터 키 사용 흐름

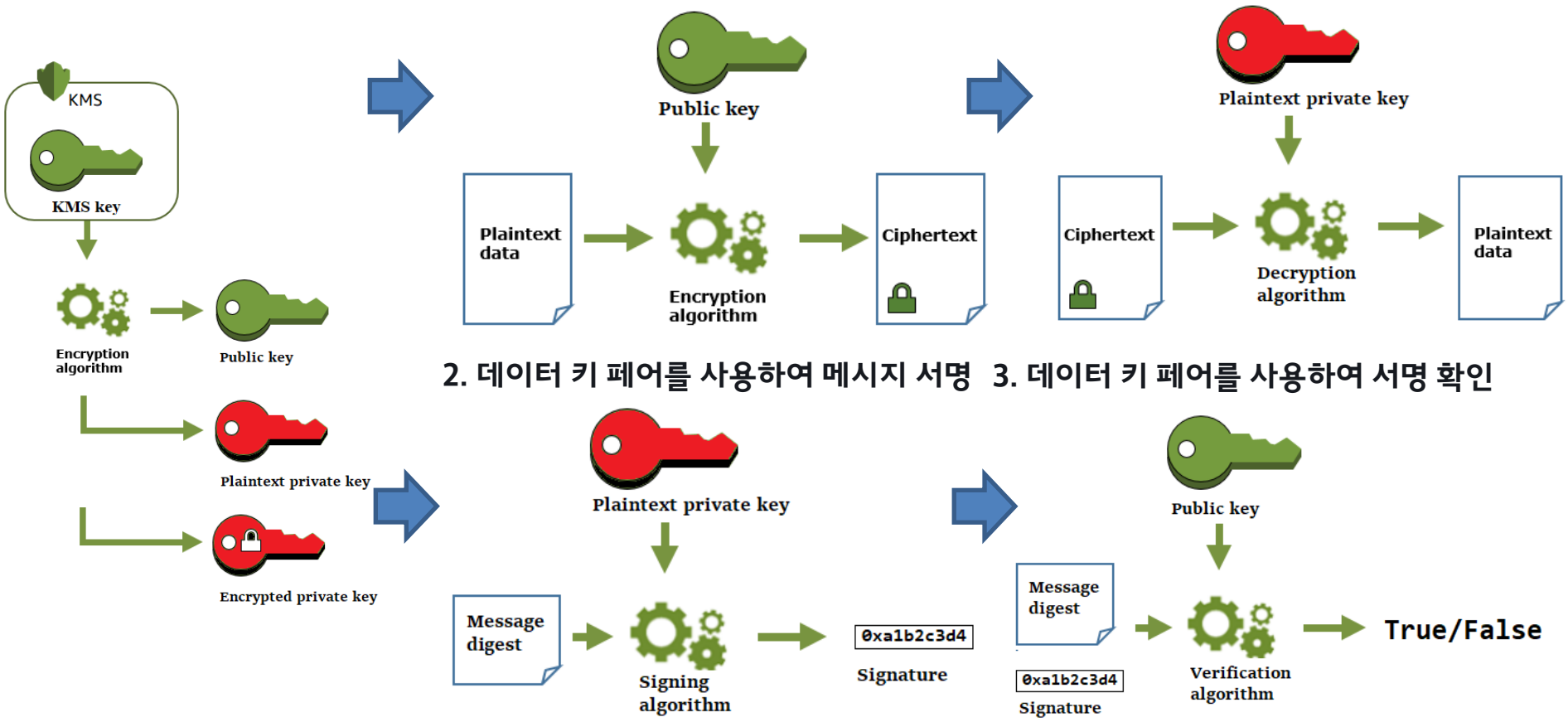
1. 데이터 키 생성
2. 데이터 키로 데이터 암호화
3 .데이터 키로 데이터



# AWS Key Management Service (AWS KMS)

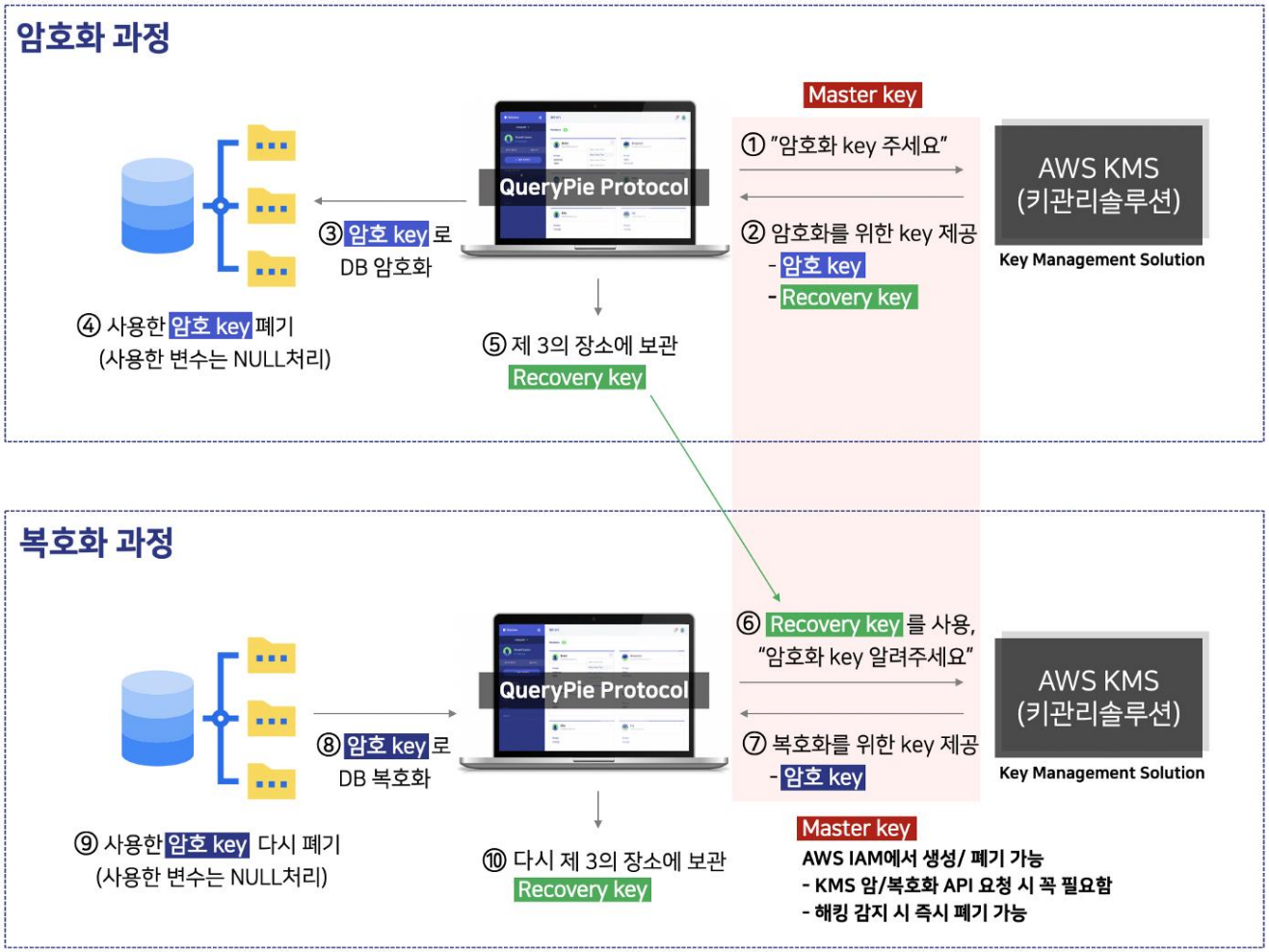
## 데이터 키 페어흐름

1. 데이터 키 페어 생성
2. 데이터 키페어로 데이터 암호화
3 . 데이터 키 페어로 데이터 암호 해독



# AWS Key Management Service (AWS KMS)

## 사용 예)



기업의 데이터 계층은 PostgreSQL 데이터베이스용 Amazon RDS를 기반으로 합니다. 조직은 데이터베이스 비밀번호 순환을 채택해야 합니다.

다음 중 운영 오버헤드가 가장 적은 이 기준을 충족하는 옵션은 무엇입니까?

A. AWS Secrets Manager에 암호를 저장합니다. 보안 비밀에 대한 자동 순환을 활성화합니다.

B. AWS Systems Manager Parameter Store에 암호를 저장합니다. 매개변수에서 자동 회전을 활성화합니다.

C. AWS Systems Manager Parameter Store에 암호를 저장합니다. 암호를 교체하는 AWS Lambda 함수를 작성합니다.

D. AWS Key Management Service(AWS KMS)에 암호를 저장합니다. 고객 마스터 키(CMK)에서 자동 교체를 활성화합니다.

틀림

**B: Parameter Store은 매개변수 자동회전 불가**

**C: Parameter Store은 암호 교체 AWS Lambda 불가**

**D: KMS는 암호 저장 서비스가 아님**

## 참고 사이트

https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/tagging-opsitems.html

https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/systems-manager-parameter-store.html

https://fgh0296.tistory.com/51

https://www.1strategy.com/blog/2019/02/28/aws-parameter-store-vs-aws-secrets-manager/

기업의 온프레미스 데이터 센터가 스토리지 한도에 도달했습니다. 조직은 대역폭 비용을 가능한 한 낮게 유지하면서 스토리지 시스템을 AWS로 전환하기를 원합니다. 솔루션은 빠르고 비용 없는 데이터 검색을 가능하게 해야 합니다.

이러한 조건은 어떻게 충족되어야 합니까?

A. Amazon S3 Glacier Vault를 배포하고 신속 검색을 활성화합니다. 워크로드에 대해 프로비저닝된 검색 용량을 활성화합니다.

B. 캐시된 볼륨을 사용하여 AWS Storage Gateway를 배포합니다. Storage Gateway를 사용하여 Amazon S3에 데이터를 저장하는 동시에 자주 액세스하는 데이터 하위 집합의 복사본을 로컬에 유지합니다.

C. 저장된 볼륨을 사용하여 AWS Storage Gateway를 배포하여 데이터를 로컬에 저장합니다. Storage Gateway를 사용하여 데이터의 특정 시점 스냅샷을 Amazon S3에 비동기식으로 백업합니다.

D. AWS Direct Connect를 배포하여 온프레미스 데이터 센터에 연결합니다. 데이터를 로컬에 저장하도록 AWS Storage Gateway를 구성합니다. Storage Gateway를 사용하여 데이터의 특정 시점 스냅샷을 Amazon S3에 비동기식으로 백업합니다.

틀림

# 02
04/04

기업의 온프레미스 데이터 센터가 스토리지 한도에 도달했습니다. 조직은 대역폭 비용을 가능한 한 낮게 유지하면서 스토리지 시스템을 AWS로 전환하기를 원합니다. 솔루션은 빠르고 비용 없는 데이터 검색을 가능하게 해야 합니다.

이러한 조건은 어떻게 충족되어야 합니까?

A. Amazon S3 Glacier Vault를 배포하고 신속 검색을 활성화합니다. 워크로드에 대해 프로비저닝된 검색 용량을 활성화합니다.

B. 캐시된 볼륨을 사용하여 AWS Storage Gateway를 배포합니다. Storage Gateway를 사용하여 Amazon S3에 데이터를 저장하는 동시에 자주 액세스하는 데이터 하위 집합의 복사본을 로컬에 유지합니다.

C. 저장된 볼륨을 사용하여 AWS Storage Gateway를 배포하여 데이터를 로컬에 저장합니다. Storage Gateway를 사용하여 데이터의 특정 시점 스냅샷을 Amazon S3에 비동기식으로 백업합니다.

D. AWS Direct Connect를 배포하여 온프레미스 데이터 센터에 연결합니다. 데이터를 로컬에 저장하도록 AWS Storage Gateway를 구성합니다. Storage Gateway를 사용하여 데이터의 특정 시점 스냅샷을 Amazon S3에 비동기식으로 백업합니다.

**A: 신속검색 활성화 → 검색 비용 추가**

**C: 비동기식 백업 → 비용 없는 검색을 위해 S3 어떤 서비스를 사용할지에 대한 언급 없음**

**D: AWS Direct Connect → 대역폭 비용이 비싼 편**

**틀림**

AWS문제풀이

# 03
04/04

온프레미스 애플리케이션을 보유한 기업이 애플리케이션의 유연성과 가용성을 높이기 위해 AWS로 전환하고 있습니다. 현재 설계에서는 Microsoft SQL Server 데이터베이스를 많이 사용합니다. 회사는 다른 데이터베이스 솔루션을 조사하고 필요한 경우 데이터베이스 엔진을 마이그레이션하려고 합니다.
개발 팀은 테스트 데이터베이스를 만들기 위해 4시간마다 프로덕션 데이터베이스의 전체 복사본을 만듭니다. 이 기간 동안 사용자는 지연이 발생합니다.

솔루션 설계자는 대체 데이터베이스로 어떤 데이터베이스를 제안해야 합니까?

A. 다중 AZ Aurora 복제본과 함께 Amazon Aurora를 사용하고 테스트 데이터베이스에 대해 mysqldump에서 복원합니다.

B. 다중 AZ Aurora 복제본과 함께 Amazon Aurora를 사용하고 테스트 데이터베이스에 대해 Amazon RDS에서 스냅샷을 복원합니다.

C. 다중 AZ 배포 및 읽기 전용 복제본과 함께 MySQL용 Amazon RDS를 사용하고 테스트 데이터베이스에 대기 인스턴스를 사용합니다.

D. 다중 AZ 배포 및 읽기 전용 복제본과 함께 SQL Server용 Amazon RDS를 사용하고 테스트 데이터베이스용으로 RDS에서 스냅샷을 복원합니다.

틀림

온프레미스 애플리케이션을 보유한 기업이 애플리케이션의 유연성과 가용성을 높이기 위해 AWS로 전환하고 있습니다. 현재 설계에서는 Microsoft SQL Server 데이터베이스를 많이 사용합니다. 회사는 다른 데이터베이스 솔루션을 조사하고 필요한 경우 데이터베이스 엔진을 마이그레이션하려고 합니다.
개발 팀은 테스트 데이터베이스를 만들기 위해 4시간마다 프로덕션 데이터베이스의 전체 복사본을 만듭니다. 이 기간 동안 사용자는 지연이 발생합니다.

솔루션 설계자는 대체 데이터베이스로 어떤 데이터베이스를 제안해야 합니까?

A. 다중 AZ Aurora 복제본과 함께 Amazon Aurora를 사용하고 테스트 데이터베이스에 대해 mysqldump에서 복원합니다.

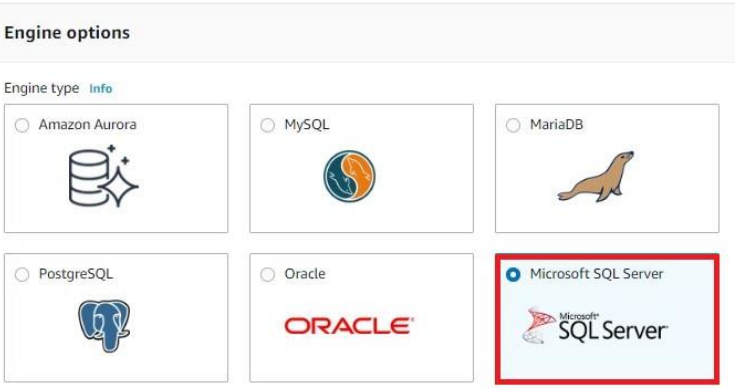
B. 다중 AZ Aurora 복제본과 함께 Amazon Aurora를 사용하고 테스트 데이터베이스에 대해 Amazon RDS에서 스냅샷을 복원합니다.

C. 다중 AZ 배포 및 읽기 전용 복제본과 함께 MySQL용 Amazon RDS를 사용하고 테스트 데이터베이스에 대기 인스턴스를 사용합니다.

D. 다중 AZ 배포 및 읽기 전용 복제본과 함께 SQL Server용 Amazon RDS를 사용하고 테스트 데이터베이스용으로 RDS에서 스냅샷을 복원합니다.

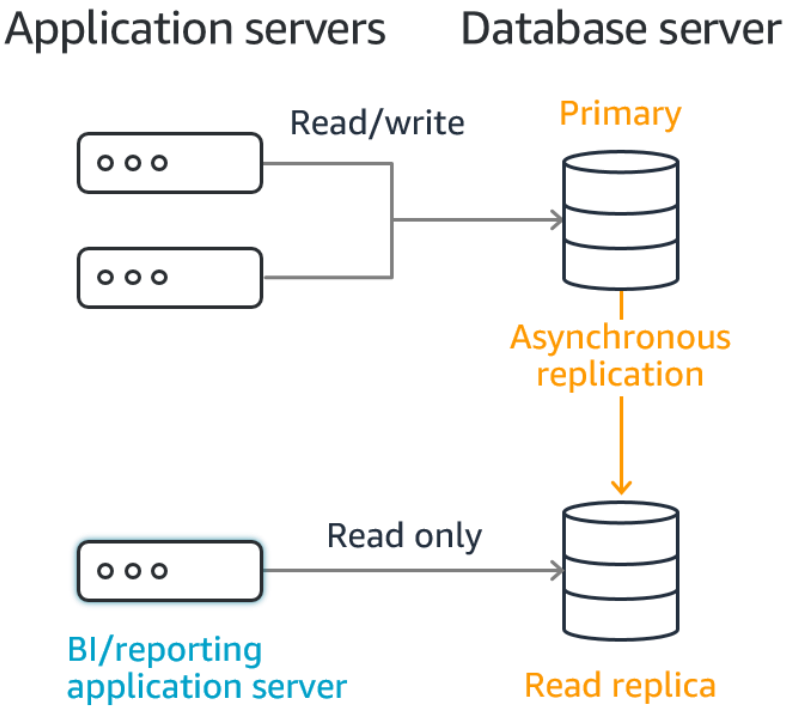
**mysqldump → MySQL의 대표적인 백업 프로그램**

**Amazon RDS 읽기 전용 복제본**



## Amazon RDS 읽기 전용 복제본

1. Amazon RDS에서 소스 DB 인스턴스의 스냅샷을 사용해 두 번째 DB 인스턴스를 생성
2. 엔진의 기본 비동기식 복제 기능을 사용해 소스 DB 인스턴스가 변경될 때마다 읽기 전용 복제본을 업데이트




틀림

Amazon Elastic Container Service(Amazon ECS) 컨테이너 인스턴스는 ALB(Application Load Balancer) 뒤에 전자 상거래 웹 사이트의 웹 애플리케이션을 설치하는 데 사용됩니다. 사용량이 많은 순간에는 웹 사이트 속도가 느려지고 가용성이 감소합니다. 솔루션 설계자는 Amazon CloudWatch 경보를 활용하여 가용성 문제가 발생할 때 알림을 받고 리소스를 확장할 수 있습니다. 비즈니스 경영진은 이러한 상황에 자동으로 대응하는 시스템을 원합니다.

어떤 솔루션이 이러한 기준을 충족합니까?

A. ALB에 시간 초과가 있을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

B. ALB CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

C. 서비스의 CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

D. ALB 대상 그룹 CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

틀림

# 01
04/11

Amazon Elastic Container Service(Amazon ECS) 컨테이너 인스턴스는 ALB(Application Load Balancer) 뒤에 전자 상거래 웹 사이트의 웹 애플리케이션을 설치하는 데 사용됩니다. 사용량이 많은 순간에는 웹 사이트 속도가 느려지고 가용성이 감소합니다. 솔루션 설계자는 Amazon CloudWatch 경보를 활용하여 가용성 문제가 발생할 때 알림을 받고 리소스를 확장할 수 있습니다. 비즈니스 경영진은 이러한 상황에 자동으로 대응하는 시스템을 원합니다.

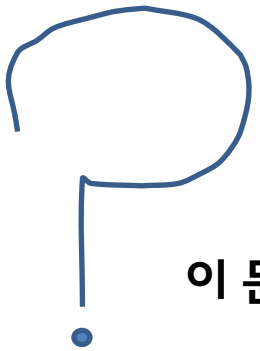
어떤 솔루션이 이러한 기준을 충족합니까?

A. ALB에 시간 초과가 있을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

B. ALB CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

C. 서비스의 CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.

D. ALB 대상 그룹 CPU 사용률이 너무 높을 때 ECS 서비스를 확장하도록 AWS Auto Scaling을 설정합니다. CPU 또는 메모리 예약이 너무 높을 때 ECS 클러스터를 확장하도록 AWS Auto Scaling을 설정합니다.



**이 문제는 같이 이야기 해보고 싶습니다**

틀림

AWS문제풀이

Amazon EC2 인스턴스 집합에서 기업은 교육 사이트를 제공합니다. 이 회사는 웹에서 수백 개의 교육 비디오를 포함하는 새로운 과정이 일주일 안에 제공되면 엄청난 인기를 얻을 것으로 예측합니다.

솔루션 설계자는 예측된 서버 로드를 최소로 유지하기 위해 무엇을 해야 합니까?

A. Redis용 Amazon ElastiCache에 비디오를 저장합니다. ElastiCache API를 사용하여 비디오를 제공하도록 웹 서버를 업데이트하십시오.

B. 비디오를 Amazon Elastic File System(Amazon EFS)에 저장합니다. 웹 서버가 EFS 볼륨을 탑재할 사용자 데이터 스크립트를 생성합니다.

C. 비디오를 Amazon S3 버킷에 저장합니다. 해당 S3 버킷의 원본 액세스 ID(OAI)를 사용하여 Amazon CloudFront 배포를 생성합니다. OAI에 대한 Amazon S3 액세스를 제한합니다.

D. 비디오를 Amazon S3 버킷에 저장합니다. S3 버킷에 액세스할 AWS Storage Gateway 파일 게이트웨이를 생성합니다. 파일 게이트웨이를 탑재할 웹 서버용 사용자 데이터 스크립트를 생성합니다.

맞음

Amazon EC2 인스턴스 집합에서 기업은 교육 사이트를 제공합니다. 이 회사는 웹에서 수백 개의 교육 비디오를 포함하는 새로운 과정이 일주일 안에 제공되면 엄청난 인기를 얻을 것으로 예측합니다.

솔루션 설계자는 예측된 서버 로드를 최소로 유지하기 위해 무엇을 해야 합니까?

A. Redis용 Amazon ElastiCache에 비디오를 저장합니다. ElastiCache API를 사용하여 비디오를 제공하도록 웹 서버를 업데이트하십시오.

B. 비디오를 Amazon Elastic File System(Amazon EFS)에 저장합니다. 웹 서버가 EFS 볼륨을 탑재할 사용자 데이터 스크립트를 생성합니다.

C. 비디오를 Amazon S3 버킷에 저장합니다. 해당 S3 버킷의 원본 액세스 ID(OAI)를 사용하여 Amazon CloudFront 배포를 생성합니다. OAI에 대한 Amazon S3 액세스를 제한합니다.

D. 비디오를 Amazon S3 버킷에 저장합니다. S3 버킷에 액세스할 AWS Storage Gateway 파일 게이트웨이를 생성합니다. 파일 게이트웨이를 탑재할 웹 서버용 사용자 데이터 스크립트를 생성합니다.

비디오 (콘텐츠), 서버로드 최소 → Cloud Front

맞음

AWS문제풀이

# 03
04/11

기업은 3계층 웹 애플리케이션을 온프레미스에서 AWS 클라우드로 전환하기로 선택합니다. 새 데이터베이스는 저장 용량을 동적으로 확장하고 테이블 조인을 수행할 수 있어야 합니다.

이 기준을 충족하는 AWS 서비스는 무엇입니까?

A. 아마존 오로라

B. SqlServer용 Amazon RDS

C. Amazon DynamoDB 스트림

D. Amazon DynamoDB 온디맨드

맞음

AWS문제풀이

기업은 3계층 웹 애플리케이션을 온프레미스에서 AWS 클라우드로 전환하기로 선택합니다. 새 데이터베이스는 저장 용량을 동적으로 확장하고 테이블 조인을 수행할 수 있어야 합니다.

이 기준을 충족하는 AWS 서비스는 무엇입니까?

A. 아마존 오로라

B. SqlServer용 Amazon RDS 저장용량 동적 할당 X

C. Amazon DynamoDB 스트림 ] 테이블 X

D. Amazon DynamoDB 온디맨드 ]

맞음

# 01
04/12

다음 정책은 Amazon EC2 관리자가 개발했으며 수많은 사용자를 포함하는 IAM 그룹에 할당되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

맞음

이 정책은 어떤 영향을 미칩니까?

A. 사용자는 us-east-1을 제외한 모든 AWS 리전에서 EC2 인스턴스를 종료할 수 있습니다.

B. 사용자는 us-east-1 리전에서 IP 주소가 10.100.100.1인 EC2 인스턴스를 종료할 수 있습니다.

C. 사용자의 소스 IP가 10.100.100.254인 경우 사용자는 us-east-1 리전에서 EC2 인스턴스를 종료할 수 있습니다.

D. 사용자의 소스 IP가 10.100.100.254인 경우 사용자는 us-east-1 리전에서 EC2 인스턴스를 종료할 수 없습니다.

# 01
04/12

다음 정책은 Amazon EC2 관리자가 개발했으며 수많은 사용자를 포함하는 IAM 그룹에 할당되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

10.100.100.0 네트워크 내의 IP 주소는 ec2를 종료할 수 있음

us-east-1이 아니면 모든 ec2에서 거부
→ us-east-1만 가능

맞음

이 정책은 어떤 영향을 미칩니까?

A. 사용자는 us-east-1을 제외한 모든 AWS 리전에서 EC2 인스턴스를 종료할 수 있습니다.

B. 사용자는 us-east-1 리전에서 IP 주소가 10.100.100.1인 EC2 인스턴스를 종료할 수 있습니다.

C. 사용자의 소스 IP가 10.100.100.254인 경우 사용자는 us-east-1 리전에서 EC2 인스턴스를 종료할 수 있습니다.

D. 사용자의 소스 IP가 10.100.100.254인 경우 사용자는 us-east-1 리전에서 EC2 인스턴스를 종료할 수 없습니다.

비즈니스는 Amazon EC2 인스턴스를 사용하여 API 기반 인벤토리 보고 애플리케이션을 운영합니다. 이 프로그램은 Amazon DynamoDB 데이터베이스를 사용하여 데이터를 저장합니다. 회사의 유통 센터는 API와 통신하는 온프레미스 배송 애플리케이션을 사용하여 배송 라벨을 생성하기 전에 인벤토리를 업데이트합니다. 매일 조직은 애플리케이션 중단으로 인해 트랜잭션이 누락되는 것을 목격했습니다.

솔루션 설계자는 애플리케이션의 탄력성을 높이기 위해 무엇을 제안해야 합니까?

A. 로컬 데이터베이스에 쓰도록 배송 애플리케이션을 수정합니다.

B. AWS Lambda를 사용하여 서버리스를 실행하도록 애플리케이션 API 수정

C. EC2 인벤토리 애플리케이션 API를 호출하도록 Amazon API Gateway를 구성합니다.

D. Amazon Simple Queue Service(Amazon SQS)를 사용하여 인벤토리 업데이트를 보내도록 애플리케이션을 수정합니다.

맞음

비즈니스는 Amazon EC2 인스턴스를 사용하여 API 기반 인벤토리 보고 애플리케이션을 운영합니다. 이 프로그램은 Amazon DynamoDB 데이터베이스를 사용하여 데이터를 저장합니다. 회사의 유통 센터는 API와 통신하는 온프레미스 배송 애플리케이션을 사용하여 배송 라벨을 생성하기 전에 인벤토리를 업데이트합니다. 매일 조직은 애플리케이션 중단으로 인해 트랜잭션이 누락되는 것을 목격했습니다.

솔루션 설계자는 애플리케이션의 탄력성을 높이기 위해 무엇을 제안해야 합니까?

A. 로컬 데이터베이스에 쓰도록 배송 애플리케이션을 수정합니다.

B. AWS Lambda를 사용하여 서버리스를 실행하도록 애플리케이션 API 수정

C. EC2 인벤토리 애플리케이션 API를 호출하도록 Amazon API Gateway를 구성합니다.

D. Amazon Simple Queue Service(Amazon SQS)를 사용하여 인벤토리 업데이트를 보내도록 애플리케이션을 수정합니다.

누락되는 것을 피하기 위해서 AWS SQS를 사용

맞음

# 03
04/12

Amazon Aurora에서 기업은 데이터베이스를 운영하고 있습니다. 매일 밤 데이터베이스는 비활성화됩니다. 사용자 트래픽이 이른 시간에 급증하면 데이터베이스에서 많은 양의 읽기를 수행하는 애플리케이션이 성능 문제에 직면하게 됩니다. 이러한 피크 시간 동안 데이터베이스에서 읽을 때 프로그램에서 시간 초과 문제가 발생합니다. 전담 운영 인력이 없기 때문에 조직은 성능 문제를 해결하기 위한 자동화된 솔루션이 필요합니다.

데이터베이스가 증가하는 읽기 로드에 자동으로 조정되도록 솔루션 설계자가 취해야 하는 활동은 무엇입니까? (2개를 선택하세요.)

A. 데이터베이스를 Aurora Serverless로 마이그레이션합니다.

B. Aurora 데이터베이스의 인스턴스 크기를 늘립니다.

C. Aurora 복제본을 사용하여 Aurora Auto Scaling을 구성합니다.

D. 데이터베이스를 Aurora 멀티 마스터 클러스터로 마이그레이션합니다.

E. 데이터베이스를 Amazon RDS for MySQL 다중 AZ 배포로 마이그레이션합니다.

틀림

# 03
04/12

Amazon Aurora에서 기업은 데이터베이스를 운영하고 있습니다. 매일 밤 데이터베이스는 비활성화됩니다. 사용자 트래픽이 이른 시간에 급증하면 데이터베이스에서 많은 양의 읽기를 수행하는 애플리케이션이 성능 문제에 직면하게 됩니다. 이러한 피크 시간 동안 데이터베이스에서 읽을 때 프로그램에서 시간 초과 문제가 발생합니다. 전담 운영 인력이 없기 때문에 조직은 성능 문제를 해결하기 위한 자동화된 솔루션이 필요합니다.

데이터베이스가 증가하는 읽기 로드에 자동으로 조정되도록 솔루션 설계자가 취해야 하는 활동은 무엇입니까? (2개를 선택하세요.)

A. 데이터베이스를 Aurora Serverless로 마이그레이션합니다.

B. Aurora 데이터베이스의 인스턴스 크기를 늘립니다. 인스턴스의 크기면 메모리? CPU 업그레이드?

C. Aurora 복제본을 사용하여 Aurora Auto Scaling을 구성합니다.

D. 데이터베이스를 Aurora 멀티 마스터 클러스터로 마이그레이션합니다. 쓰기 능력 ↑

E. 데이터베이스를 Amazon RDS for MySQL 다중 AZ 배포로 마이그레이션합니다. 데이터 손실 ↓

틀림

## Aurora Serverless

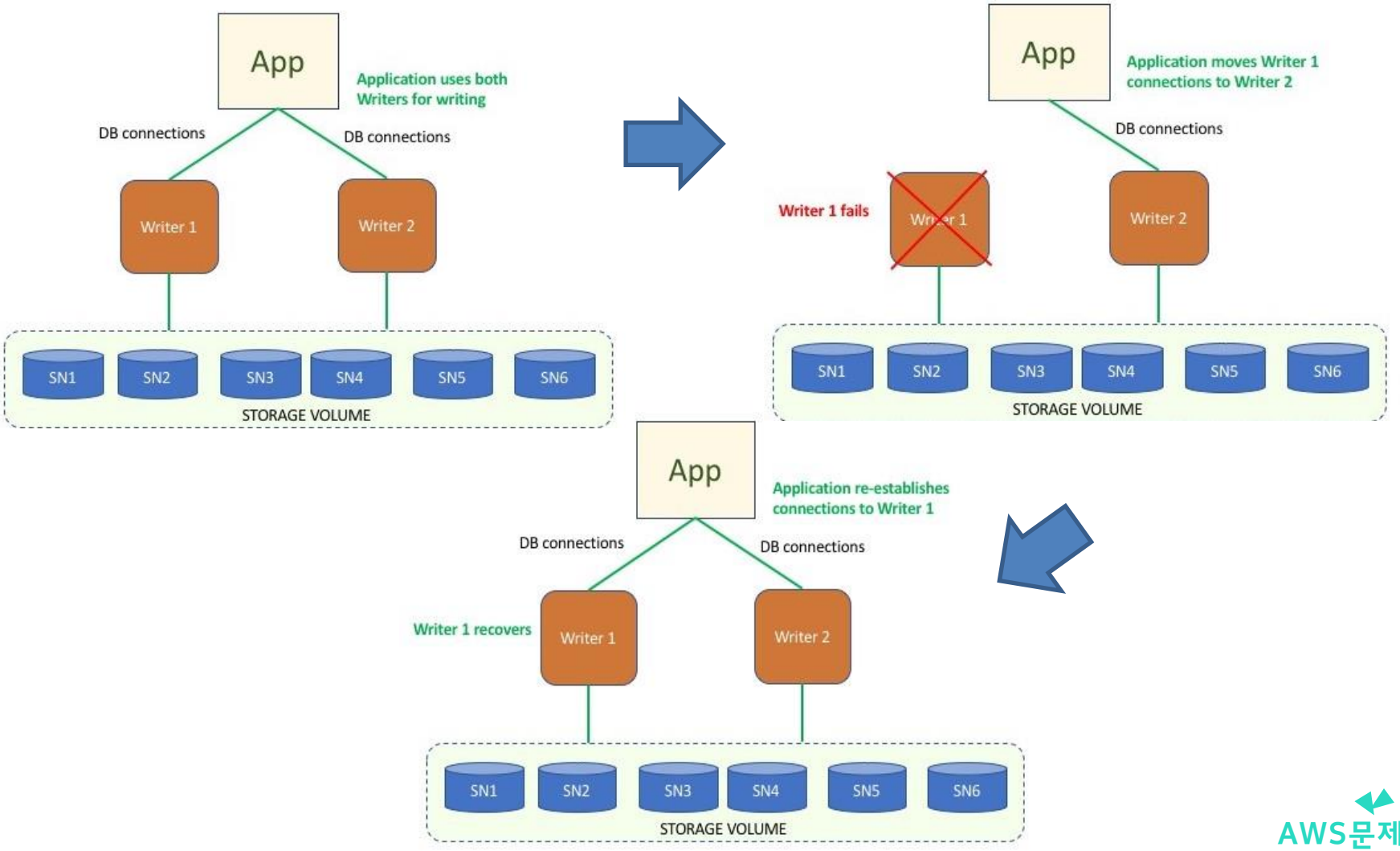
Amazon Aurora의 온디맨드 Auto Scaling 구성

→ 어플리케이션 요구 사항을 기반으로 자동으로 시작 및 종료하고 용량을 확장 또는 축소

## Aurora 멀티 마스터 클러스터

- 여러 가용 영역에 걸쳐 복수의 쓰기 인스턴스를 생성
- 지속적인 쓰기 가용성을 달성
- 인스턴스 또는 가용 영역 장애가 발생하는 경우,
  다운 타임 없이 읽기 및 쓰기 가용성을 유지할 수 있으며, 별도의 DB 장애 조치가 필요 없음

# Aurora 멀티 마스터 클러스터



기업은 느슨하게 결합되도록 밀접하게 연결된 애플리케이션을 재설계하고 있습니다. 이전에는 프로그램이 요청/응답 패턴을 통해 계층 간에 통신했습니다. 조직은 Amazon Simple Queue Service(Amazon SQS)를 사용하여 이를 수행하려고 합니다. 첫 번째 아키텍처는 요청 큐와 응답 큐를 포함합니다. 그러나 프로그램이 커질 때 이 전략은 모든 메시지를 처리하지 않습니다.

솔루션 아키텍트가 이 문제를 해결하기 위해 취해야 할 가장 좋은 조치는 무엇입니까?

A. SQS 대기열의 ReceiveMessage API 작업에서 배달 못한 편지 대기열을 구성합니다.

B. FIFO 대기열을 구성하고 메시지 중복 제거 ID 및 메시지 그룹 ID를 사용합니다.

C. 각 응답 메시지를 수신할 임시 대기열 클라이언트를 사용하여 임시 대기열을 만듭니다.

D. 각 생산자에 대한 시작 시 각 요청 및 응답에 대한 대기열을 만들고 상관 ID 메시지 속성을 사용합니다.

맞음

# 01
04/13

기업은 느슨하게 결합되도록 밀접하게 연결된 애플리케이션을 재설계하고 있습니다. 이전에는 프로그램이 요청/응답 패턴을 통해 계층 간에 통신했습니다. 조직은 Amazon Simple Queue Service(Amazon SQS)를 사용하여 이를 수행하려고 합니다. 첫 번째 아키텍처는 요청 큐와 응답 큐를 포함합니다. 그러나 프로그램이 커질 때 이 전략은 모든 메시지를 처리하지 않습니다.

솔루션 아키텍트가 이 문제를 해결하기 위해 취해야 할 가장 좋은 조치는 무엇입니까?

누락되는 것을 피하기 위해서 AWS SQS를 사용

A. SQS 대기열의 ReceiveMessage API 작업에서 배달 못한 편지 대기열을 구성합니다.

B. FIFO 대기열을 구성하고 메시지 중복 제거 ID 및 메시지 그룹 ID를 사용합니다.

C. 각 응답 메시지를 수신할 임시 대기열 클라이언트를 사용하여 임시 대기열을 만듭니다.

D. 각 생산자에 대한 시작 시 각 요청 및 응답에 대한 대기열을 만들고 상관 ID 메시지 속성을 사용합니다.

맞음

AWS문제풀이

기업의 데이터 웨어하우스는 Amazon Redshift를 기반으로 합니다. 이 회사는 구성 요소 오류 발생 시 데이터의 장기적인 생존 가능성을 보장하기를 원합니다.

솔루션 설계자는 어떤 권장 사항을 제시해야 합니까?

A. 동시성 확장을 활성화합니다.

B. 교차 리전 스냅샷을 활성화합니다.

C. 데이터 보유 기간을 늘립니다.

D. 다중 AZ에 Amazon Redshift를 배포합니다.

**데이터 웨어하우스**

**Amazon Redshift**

**동시성 확장의 의미**

**교차 리전 스냅샷의 의미**

**다중 AZ에 배포의 의미**

틀림

## 데이터 웨어 하우스란?

데이터 웨어하우스는 POS 트랜잭션, 마케팅 자동화, 고객 관계 관리 시스템 등의 여러 소스에서 가져온 구조화된 데이터와 반구조화된 데이터를 분석하고 보고하는 데 사용되는 엔터프라이즈 시스템

**즉, 수많은 데이터를 관리하고 분석하기 위한 솔루션**

## Amazon Redshift

클라우드에서 완벽하게 관리되는 페타바이트급 데이터 웨어하우스 서비스

## Amazon Redshift 동시성 확장(Concurrent Scaling)

Redshift는 클러스터에서 충분한 컴퓨팅 리소스를 사용할 수 있을 때까지 쿼리를 대기열에 배치 하기 때문에 사용자 피크 시간에 동시 쿼리의 수가 증가할 때 성능 저하 발생

- 필요에 따라 Redshift 클러스터 성능을 확장
- 추가 처리 성능은 몇 초 내에 준비되며 사전 준비 또는 사전 프로비저닝이 필요하지 않음
- 초당 청구 금액으로 사용한 만큼만 요금을 지불
- 추가 처리 성능은 더 이상 필요하지 않은 경우 제거

## 교차 리전 스냅샷을 찍는다의 의미는?

- 어플리케이션의 지리적 확장
- 데이터 센터 마이그레이션
- 재해 복구

## 다중 AZ에 배포한다의 의미는?

데이터 내구성 및 가용성 향상을 위해 다중 AZ에 배포합니다. 하지만 Redshift는 단일 AZ만 지원합니다.

**Q: Amazon Redshift는 다중 AZ 배포를 지원하나요?**

현재 Amazon Redshift는 단일 리전 배포만 지원합니다. 재해 복구(DR) 구성을 설정하려면 클러스터에서 교차 리전 스냅샷 복사를 활성화합니다. 이렇게 하면 클러스터의 모든 스냅샷이 다른 AWS 리전으로 복제됩니다. DR 사건이 발생하면 복제 리전의 스냅샷을 복원하여 새 클러스터를 만들 수 있습니다. Amazon Redshift는 교차 리전 데이터 공유도 지원합니다. 이를 통해 고객 클러스터가 다른 리전의 생산자 클러스터에 있는 라이브 데이터에 액세스할 수 있습니다. 이 기능은 Amazon Redshift Serverless 및 RA3에서만 지원됩니다.

# 02
04/13

기업의 데이터 웨어하우스는 Amazon Redshift를 기반으로 합니다. 이 회사는 구성 요소 오류 발생 시 데이터의 장기적인 생존 가능성을 보장하기를 원합니다.

솔루션 설계자는 어떤 권장 사항을 제시해야 합니까?

A. 동시성 확장을 활성화합니다.

B. 교차 리전 스냅샷을 활성화합니다.

C. 데이터 보유 기간을 늘립니다.

D. 다중 AZ에 Amazon Redshift를 배포합니다.

틀림

AWS문제풀이

# 03
04/13

Amazon S3는 기업에서 개인 감사 기록을 저장하는 데 사용됩니다. 최소 권한 개념에 따라 S3 버킷은 버킷 제한을 구현하여 감사 팀 IAM 사용자 자격 증명에 대한 액세스를 제한합니다. 회사 경영진은 S3 버킷에서 의도하지 않은 문서 파괴에 대해 우려하고 있으며 보다 안전한 솔루션이 필요합니다.

솔루션 설계자는 감사 문서의 보안을 보장하기 위해 어떤 단계를 수행해야 합니까?

A. S3 버킷에서 버전 관리 및 MFA 삭제 기능을 활성화합니다.

B. 각 감사 팀 IAM 사용자 계정의 IAM 사용자 자격 증명에 대해 다단계 인증(MFA)을 활성화합니다.

C. 감사 날짜 동안 s3:DeleteObject 작업을 거부하려면 감사 팀의 IAM 사용자 계정에 S3 수명 주기 정책을 추가합니다.

D. AWS Key Management Service(AWS KMS)를 사용하여 S3 버킷을 암호화하고 감사 팀 IAM 사용자 계정이 KMS 키에 액세스하지 못하도록 제한합니다.

맞음

# 03
04/13

Amazon S3는 기업에서 개인 감사 기록을 저장하는 데 사용됩니다. 최소 권한 개념에 따라 S3 버킷은 버킷 제한을 구현하여 감사 팀 IAM 사용자 자격 증명에 대한 액세스를 제한합니다. 회사 경영진은 S3 버킷에서 의도하지 않은 문서 파괴에 대해 우려하고 있으며 보다 안전한 솔루션이 필요합니다.

솔루션 설계자는 감사 문서의 보안을 보장하기 위해 어떤 단계를 수행해야 합니까?

A. S3 버킷에서 버전 관리 및 MFA 삭제 기능을 활성화합니다.

B. 각 감사 팀 IAM 사용자 계정의 IAM 사용자 자격 증명에 대해 다단계 인증(MFA)을 활성화합니다.

C. 감사 날짜 동안 s3:DeleteObject 작업을 거부하려면 감사 팀의 IAM 사용자 계정에 S3 수명 주기 정책을 추가합니다.

D. AWS Key Management Service(AWS KMS)를 사용하여 S3 버킷을 암호화하고 감사 팀 IAM 사용자 계정이 KMS 키에 액세스하지 못하도록 제한합니다.

**B: 의도하지 않은 문서 파괴에 대한 대책이 없음**

**C: 수명주기 정책은 현재 문제와 관련이 없음**

**D: 의도하지 않은 문서 파괴에 대한 대책이 없음**

맞음