201 (나권서) 2회차 完

◆ | **Q#0201.** | **Ref#0201.**
솔루션 아키텍트는 AWS 클라우드에 호스팅되는 애플리케이션을 개선해야 합니다. 애플리케이션이 연결 과부하가 발생하는 Amazon Aurora MySQL DB 인스턴스를 사용합니다. 대부분의 애플리케이션 작업은 데이터베이스에 레코드를 삽입합니다. 애플리케이션은 현재 텍스트 기반 구성 파일에 자격 증명을 저장합니다.

솔루션 설계자는 애플리케이션이 현재 연결 로드를 처리할 수 있도록 솔루션을 구현해야 합니다. 솔루션은 자격 증명을 안전하게 유지해야 하며 정기적으로 자격 증명을 자동으로 교체하는 기능을 제공해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** Amazon RDS 프록시 계층을 배포합니다. DB 인스턴스 앞. 연결 자격 증명을 AWS Secrets Manager에 비밀로 저장합니다.
> **B.** DB 인스턴스 앞에 Amazon RDS 프록시 계층을 배포합니다. AWS Systems Manager Parameter Store에 연결 자격 증명을 저장합니다.
> **C.** Aurora 복제본을 생성합니다. AWS Secrets Manager에 연결 자격 증명을 비밀로 저장
> **D.** Aurora 복제본을 생성합니다. AWS Systems Manager Parameter Store에 연결 자격 증명을 저장합니다.
>
> 해설
> 정답: A
> Amazon RDS Proxy를 사용하여 연결 풀링을 제공하고 데이터베이스 연결을 효율적으로 관리하여 과부하된 연결 문제를 직접 해결할 수 있음.
> 또한, AWS Secrets Manager에 자격 증명을 저장하면 자격 증명이 안전하게 보관되고 정기적으로 자동 회전이 가능.
> B(x), D(x): AWS Systems Manager Parameter Store는 데이터베이스 자격 증명의 자동 회전을 기본적으로 지원하지 않음.
> C(x), D(x): Aurora Replica를 생성하면 읽기 확장은 가능하지만, 레코드 삽입 작업의 연결 과부하 문제를 직접 해결하지는 못함.

◆ | **Q#0202.** | **Ref#0202.**
회사는 전자상거래 웹사이트를 위한 재해 복구(DR) 솔루션을 구축해야 합니다. 웹 애플리케이션은 t3.large Amazon EC2 인스턴스 집합에서 호스팅되며 MySQL DB 인스턴스용 Amazon RDS를 사용합니다. EC2 인스턴스는 여러 가용 영역에 걸쳐 확장되는 Auto Scaling 그룹에 있습니다.

재해가 발생하는 경우 웹 애플리케이션은 RPO 30초, RTO 10분을 사용하여 보조 환경으로 장애 조치해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** IaC(Infrastructure as Code)를 사용하여 DR 지역에 새 인프라를 프로비저닝합니다. DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. AWS Backup에서 백업 계획을 설정하여 EC2 인스턴스 및 DB 인스턴스에 대한 리전 간 백업을 생성합니다. EC2 인스턴스와 DB 인스턴스를 30초마다 DR 리전에 백업하는 cron 표현식을 생성합니다. 최신 EC2 백업에서 EC2 인스턴스를 복구합니다. 재해 발생 시 자동으로 DR 지역으로 장애 조치하려면 Amazon Route 53 지리적 위치 라우팅 정책을 사용하십시오.
> **B.** IaC(Infrastructure as Code)를 사용하여 DR 지역에 새 인프라를 프로비저닝합니다. DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. EC2 인스턴스를 DR 지역에 지속적으로 복제하도록 AWS Elastic Disaster Recovery를 설정합니다. DR 지역의 최소 용량으로 EC2 인스턴스를 실행합니다. 재해 발생 시 자동으로 DR 지역으로 장애 조치하려면 Amazon Route 53 장애 조치 라우팅 정책을 사용하십시오. Auto Scaling 그룹의 원하는 용량을 늘립니다.
> **C.** AWS Backup에서 백업 계획을 설정하여 EC2 인스턴스 및 DB 인스턴스에 대한 지역 간 백업을 생

성합니다. EC2 인스턴스와 DB 인스턴스를 30초마다 DR 리전에 백업하는 cron 표현식을 생성합니다. IaC(Infrastructure as Code)를 사용하여 DR 지역에 새 인프라를 프로비저닝합니다. 새 인스턴스에서 백업된 데이터를 수동으로 복원합니다. 재해 발생 시 자동으로 DR 지역으로 장애 조치하려면 Amazon Route 53 단순 라우팅 정책을 사용하십시오.
D. IaC(Infrastructure as Code)를 사용하여 DR 지역에 새 인프라를 프로비저닝합니다. Amazon Aurora 글로벌 데이터베이스를 생성합니다. EC2 인스턴스를 DR 지역에 지속적으로 복제하도록 AWS Elastic Disaster Recovery를 설정합니다. DR 지역에서 전체 용량으로 EC2 인스턴스의 Auto Scaling 그룹을 실행합니다. 재해 발생 시 자동으로 DR 지역으로 장애 조치하려면 Amazon Route 53 장애 조치 라우팅 정책을 사용하십시오.

해설
정답: B
B: 지속적인 복제를 제공하고 DR 리전에서 최소 용량으로 EC2 인스턴스를 실행하여 비용 효율적, RPO와 RTO를 충족하면서도 비용을 절감
A(x): 비용이 많이 들고, EC2 인스턴스를 30초마다 백업하는 것은 비현실적
C(x): 백업 주기와 수동 복구가 RPO와 RTO 요구 사항을 충족하지 못할 수 있음.
D(x): DR 리전에서 EC2 인스턴스를 전체 용량으로 실행하는 것은 비용이 많이 들며, 불필요한 리소스 사용을 초래함

◆ | **Q#0203.** | **Ref#0203.**
회사는 온프레미스 MySQL 데이터베이스를 us-east-1 리전의 Amazon Aurora MySQL로 일회적으로 마이그레이션할 계획입니다. 회사의 현재 인터넷 연결에는 대역폭이 제한되어 있습니다. 온프레미스 MySQL 데이터베이스의 크기는 60TB입니다. 회사에서는 현재 인터넷 연결을 통해 데이터를 AWS로 전송하는 데 한 달이 걸릴 것으로 추정합니다. 회사에는 데이터베이스를 더 빠르게 마이그레이션할 마이그레이션 솔루션이 필요합니다.

가장 짧은 시간 내에 데이터베이스를 마이그레이션하는 솔루션은 무엇입니까?

A. 온프레미스 데이터 센터와 AWS 간에 1Gbps AWS Direct Connect 연결을 요청합니다. AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스 MySQL 데이터베이스를 Aurora MySQL로 마이그레이션합니다.
B. 현재 인터넷 연결과 함께 AWS DataSync를 사용하여 온프레미스 데이터 센터와 AWS 간의 데이터 전송을 가속화합니다. AWS Application Migration Service를 사용하여 온프레미스 MySQL 데이터베이스를 Aurora MySQL로 마이그레이션합니다.
C. AWS Snowball Edge 디바이스를 주문합니다. S3 인터페이스를 사용하여 Amazon S3 버킷에 데이터를 로드합니다. AWS Database Migration Service(AWS DMS)를 사용하여 Amazon S3에서 Aurora MySQL로 데이터를 마이그레이션합니다.
D. AWS Snowball 디바이스를 주문합니다. Snowball용 S3 어댑터를 사용하여 Amazon S3 버킷에 데이터를 로드합니다. AWS Application Migration Service를 사용하여 Amazon S3에서 Aurora MySQL로 데이터를 마이그레이션합니다.

해설
정답: C
AWS Snowball Edge 장치를 사용하여 데이터를 S3로 로드하고, AWS DMS를 통해 Aurora MySQL로 마이그레이션하는 것이 가장 빠름.
이 방법은 물리적인 장치를 사용해 데이터를 빠르게 전송할 수 있으며, 인터넷 대역폭의 제한을 피할 수 있음.
A(x): 1Gbps DX 연결은 빠르고 안정적인 전송 속도를 제공하지만, 설치 및 구성에 1개월 가량 오랜 시간이 걸릴 수 있음.

◆ | **Q#0204.** | **Ref#0204.**
회사는 AWS 클라우드에 애플리케이션을 가지고 있습니다. 이 애플리케이션은 20개의 Amazon EC2 인스턴스 집합에서 실행됩니다. EC2 인스턴스는 지속적이며 연결된 여러 Amazon Elastic Block Store(Amazon EBS) 볼륨에 데이터를 저장합니다.

회사는 별도의 AWS 리전에서 백업을 유지해야 합니다. 회사는 영업일 기준 1일 이내에 EC2 인스턴스와 해당 구성을 복구할 수 있어야 하며 최대 1일 분량의 데이터가 손실되어서는 안 됩니다. 회사에는 제한된 직원이 있으며 운영 효율성과 비용을 최적화하는 백업 솔루션이 필요합니다. 회사는 보조 리전에 필요한 네트워크 구성을 배포할 수 있는 AWS CloudFormation 템플릿을 이미 생성했습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 보조 지역에서 EC2 인스턴스를 다시 생성할 수 있는 두 번째 CloudFormation 템플릿을 생성합니다. AWS Systems Manager Automation Runbook을 사용하여 매일 다중 볼륨 스냅샷을 실행합니다. 스냅샷을 보조 리전에 복사합니다. CloudFormation 템플릿 실행에 실패할 경우 스냅샷에서 EBS 볼륨을 복원하고 사용량을 보조 리전으로 전송합니다.
> **B.** Amazon Data Lifecycle Manager(Amazon DLM)를 사용하여 EBS 볼륨의 일일 다중 볼륨 스냅샷을 생성합니다. 오류가 발생하는 경우 CloudFormation 템플릿을 시작하고 Amazon DLM을 사용하여 EBS 볼륨을 복원하고 사용량을 보조 리전으로 전송합니다.
> **C.** AWS Backup을 사용하여 EC2 인스턴스에 대한 예약된 일일 백업 계획을 생성합니다. 보조 지역의 볼트에 백업을 복사하도록 백업 작업을 구성합니다. 오류가 발생하면 CloudFormation 템플릿을 시작하고 백업 저장소에서 인스턴스 볼륨과 구성을 복원한 다음 사용량을 보조 지역으로 이전하세요.
> **D.** 동일한 크기와 구성의 EC2 인스턴스를 보조 지역에 배포합니다. 기본 리전에서 보조 리전으로 데이터를 복사하도록 AWS DataSync를 매일 구성합니다. 오류가 발생하면 CloudFormation 템플릿을 시작하고 사용량을 보조 지역으로 이전하세요.
>
> 해설
> 정답: C
> AWS Backup을 사용하여 정기적인 일일 백업 계획을 생성하고, 이를 보조 리전으로 복사하여,
> 장애 시 CloudFormation을 통해 인스턴스와 데이터를 빠르게 복원할 수 있음.
> B(x): AWS 백업은 복원을 지원하지만 DLM은 복원을 지원하지 않음.

◆ | **Q#0205.** | **Ref#0205.**
한 회사가 정적 콘텐츠를 호스팅하는 새로운 웹사이트를 디자인하고 있습니다. 이 웹사이트는 사용자에게 대용량 파일을 업로드하고 다운로드할 수 있는 기능을 제공합니다. 회사 요구 사항에 따라 모든 데이터는 전송 중 및 저장 중 암호화되어야 합니다. 솔루션 설계자는 Amazon S3 및 Amazon CloudFront를 사용하여 솔루션을 구축하고 있습니다.

암호화 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** 웹 애플리케이션이 사용하는 S3 버킷에 대해 S3 서버 측 암호화를 활성화합니다.
> **B.** S3 ACL의 읽기 및 쓰기 작업에 대해 "aws:SecureTransport": "true" 정책 속성을 추가합니다.
> **C.** 웹 애플리케이션이 사용하는 S3 버킷에서 암호화되지 않은 작업을 거부하는 버킷 정책을 생성합니다.
> **D.** AWS KMS 키(SSE-KMS)를 사용한 서버 측 암호화를 사용하여 CloudFront에서 저장 중 암호화를 구성합니다.
> **E.** CloudFront에서 HTTP 요청을 HTTPS 요청으로 리디렉션하도록 구성합니다.
> **F.** 웹 애플리케이션이 사용하는 S3 버킷에 대해 미리 서명된 URL을 생성할 때 RequireSSL 옵션을 사용합니다.
>
> 해설
> 정답: ACE
> A: S3 서버 측 암호화(서버 측에서 데이터를 자동으로 암호화) 기능을 활성화하여 저장 시 데이터 암호화를 보장
> C: S3 버킷 정책을 생성하여 암호화되지 않은 모든 작업을 거부함으로써 암호화되지 않은 데이터 전송을 방지
> E: CloudFront에서 HTTP 요청을 HTTPS 요청으로 리디렉션하도록 설정하여 전송 중 데이터 암호화

를 보장
이렇게 하면 전송 중과 저장 시 모두 데이터가 암호화되어 회사 요구 사항을 충족.

◆ | **Q#0206.** | **Ref#0206.**
한 회사는 Amazon RDS의 Microsoft SQL Server DB 인스턴스에 액세스하는 데 필요한 AWS Lambda 함수를 사용하여 서버리스 아키텍처를 구현하고 있습니다. 회사는 데이터베이스 시스템 복제를 포함하여 개발 및 생산을 위한 별도의 환경을 보유하고 있습니다.

회사의 개발자는 개발 데이터베이스에 대한 자격 증명에 액세스할 수 있습니다. 그러나 프로덕션 데이터베이스에 대한 자격 증명은 IT 보안 팀의 IAM 사용자 그룹 구성원만 액세스할 수 있는 키로 암호화되어야 합니다. 이 키는 정기적으로 순환되어야 합니다.

이러한 요구 사항을 충족하려면 솔루션 설계자가 프로덕션 환경에서 무엇을 해야 합니까?

A. AWS KMS(AWS Key Management Service) 고객 관리형 키로 암호화된 SecureString 파라미터를 사용하여 AWS Systems Manager Parameter Store에 데이터베이스 자격 증명을 저장합니다. SecureString 파라미터에 대한 액세스를 제공하려면 각 Lambda 함수에 역할을 연결하세요. IT 보안 팀만 매개변수와 키에 액세스할 수 있도록 SecureString 매개변수와 고객 관리 키에 대한 액세스를 제한합니다.
B. AWS Key Management Service(AWS KMS) 기본 Lambda 키를 사용하여 데이터베이스 자격 증명을 암호화합니다. 각 Lambda 함수의 환경 변수에 자격 증명을 저장합니다. Lambda 코드의 환경 변수에서 자격 증명을 로드합니다. IT 보안 팀만 키에 액세스할 수 있도록 KMS 키에 대한 액세스를 제한합니다.
C. 각 Lambda 함수의 환경 변수에 데이터베이스 자격 증명을 저장합니다. AWS Key Management Service(AWS KMS) 고객 관리형 키를 사용하여 환경 변수를 암호화합니다. IT 보안 팀만 키에 액세스할 수 있도록 고객 관리 키에 대한 액세스를 제한합니다.
D. AWS Secrets Manager에 데이터베이스 자격 증명을 AWS Key Management Service(AWS KMS) 고객 관리형 키와 연결된 비밀로 저장합니다. 보안 암호에 대한 액세스를 제공하려면 각 Lambda 함수에 역할을 연결하세요. IT 보안 팀만 비밀 및 키에 액세스할 수 있도록 비밀 및 고객 관리형 키에 대한 액세스를 제한합니다.

해설
정답: D
AWS Secrets Manager: 데이터베이스 자격 증명을 안전하게 저장하고 관리하며, 주기적으로 자격 증명을 자동으로 회전시킬 수 있음.
AWS KMS 고객 관리형 키: 자격 증명을 암호화하며, 이 키에 대한 접근을 IT 보안 팀으로 제한할 수 있음.
Lambda 역할: 각 Lambda 함수에 역할을 부여하여 해당 함수가 보안암호에 접근할 수 있도록 함.
이 방식은 자격 증명의 안전한 저장과 주기적인 회전, 그리고 접근 권한 관리를 모두 충족
D Rotation = Secret Manager(Parameter Store 아님)

◆ | **Q#0207.** | **Ref#0207.**
한 온라인 소매 회사가 기존 온프레미스 .NET 애플리케이션을 AWS로 마이그레이션하고 있습니다. 애플리케이션은 부하 분산된 프런트엔드 웹 서버, 부하 분산된 애플리케이션 서버 및 Microsoft SQL Server 데이터베이스에서 실행됩니다.

회사는 가능한 경우 AWS 관리형 서비스를 사용하기를 원하며 애플리케이션을 다시 작성하고 싶지 않습니다. 솔루션 설계자는 확장 문제를 해결하고 애플리케이션 확장에 따른 라이선스 비용을 최소화하기 위한 솔루션을 구현해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 웹 계층과 애플리케이션 계층을 위해 Application Load Balancer 뒤의 Auto Scaling 그룹에 Amazon EC2 인스턴스를 배포합니다. SQL Server 데이터베이스를 다시 플랫폼화하려면 Babelfish가

활성화된 Amazon Aurora PostgreSQL을 사용하십시오.
B. AWS Database Migration Service(AWS DMS)를 사용하여 모든 서버의 이미지를 생성합니다. 온프레미스 가져오기를 기반으로 Amazon EC2 인스턴스를 배포합니다. 웹 계층과 애플리케이션 계층에 대해 Network Load Balancer 뒤의 Auto Scaling 그룹에 인스턴스를 배포합니다. Amazon DynamoDB를 데이터베이스 계층으로 사용합니다.
C. 웹 프런트엔드 계층과 애플리케이션 계층을 컨테이너화합니다. Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 프로비저닝합니다. 웹 계층과 애플리케이션 계층에 대해 Network Load Balancer 뒤에 Auto Scaling 그룹을 생성합니다. SQL Server용 Amazon RDS를 사용하여 데이터베이스를 호스팅합니다.
D. 애플리케이션 기능을 AWS Lambda 기능으로 분리합니다. 웹 프런트엔드 계층과 애플리케이션 계층에 Amazon API Gateway를 사용합니다. 데이터를 Amazon S3로 마이그레이션합니다. Amazon Athena를 사용하여 데이터를 쿼리합니다.

해설
정답: A
Amazon Aurora PostgreSQL with Babelfish:
- SQL Server 데이터베이스를 Amazon Aurora PostgreSQL로 재플랫폼화하여 라이선스 비용을 절감
- Babelfish를 사용하면 기존 SQL Server 애플리케이션을 최소한의 변경으로 PostgreSQL에서 실행할 수 있음.
- Babelfish는 PostgreSQL에 대한 SQL Server 호환성을 제공하여 코드 변경 없이 애플리케이션을 실행할 수 있게 함.
기존 애플리케이션을 크게 변경하지 않으면서도 AWS 관리형 서비스를 활용하여 비용을 절감하고 확장성을 확보할 수 있음.
B(x): DynamoDB는 SQL Server와 데이터 모델이 다르기 때문에 애플리케이션을 많이 변경해야 함.
C(x): 컨테이너화 및 Amazon EKS 사용은 관리 복잡성을 증가시킬 수 있으며, 기존 애플리케이션을 컨테이너로 변환하는 과정에서 추가 작업 필요
D(x): 애플리케이션을 Lambda 함수로 분리하고 API Gateway를 사용하는 것은 기존 애플리케이션을 재설계하는 방식, 비용과 시간이 많이 소요

◆ | **Q#0208.** | **Ref#0208.**
SaaS(Software-as-a-Service) 공급자는 ALB(Application Load Balancer)를 통해 API를 노출합니다. ALB는 us-east-1 지역에 배포된 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 연결됩니다. 노출된 API에는 LINK, UNLINK, LOCK 및 UNLOCK과 같은 몇 가지 비표준 REST 메서드의 사용이 포함되어 있습니다.

미국 이외의 사용자는 이러한 API에 대한 응답 시간이 길고 일관성이 없다고 보고하고 있습니다. 솔루션 설계자는 운영 오버헤드를 최소화하는 솔루션으로 이 문제를 해결해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon CloudFront 배포를 추가합니다. ALB를 오리진으로 구성합니다.
B. Amazon API Gateway 엣지 최적화 API 엔드포인트를 추가하여 API를 노출합니다. ALB를 대상으로 구성하십시오.
C. AWS Global Accelerator에 액셀러레이터를 추가합니다. ALB를 오리진으로 구성합니다.
D. 두 개의 추가 AWS 지역인 eu-west-1 및 ap-southeast-2에 API를 배포합니다. Amazon Route 53에 지연 시간 기반 라우팅 레코드를 추가합니다.

해설
정답: C
외국 사용자들의 응답 시간 문제를 해결하기 위해 AWS Global Accelerator를 사용하여 가속기를 추가하고 ALB를 원본으로 구성
AWS Global Accelerator는 글로벌 사용자를 위해 애플리케이션의 가용성과 성능을 향상시키는 서비스
Global Accelerator를 사용하여 여러 국가의 인스턴스와 단일 위치의 데이터베이스 서버 간의 통신

속도를 높입니다.
A(x): CloudFront는 LINK, UNLINK, LOCK, UNLOCK을 지원하지 않습니다 B(x): API Gateway는 LINK, UNLINK, LOCK, UNLOCK을 지원하지 않습니다

◆ | **Q#0209.** | **Ref#0209.**
한 회사가 AWS 클라우드에서 IoT 애플리케이션을 실행하고 있습니다. 이 회사는 미국 내 주택에서 데이터를 수집하는 수백만 개의 센서를 보유하고 있습니다. 센서는 MQTT 프로토콜을 사용하여 사용자 정의 MQTT 브로커에 연결하고 데이터를 보냅니다. MQTT 브로커는 단일 Amazon EC2 인스턴스에 데이터를 저장합니다. 센서는 iot.example.com이라는 도메인을 통해 브로커에 연결됩니다. 이 회사는 DNS 서비스로 Amazon Route 53을 사용합니다. 회사는 Amazon DynamoDB에 데이터를 저장합니다.

여러 경우에 데이터 양으로 인해 MQTT 브로커가 과부하되어 센서 데이터가 손실되었습니다. 회사는 솔루션의 신뢰성을 향상시켜야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. ALB(Application Load Balancer)와 MQTT 브로커용 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 ALB의 대상으로 사용합니다. Route 53의 DNS 레코드를 별칭 레코드로 업데이트합니다. 별칭 레코드가 ALB를 가리키도록 합니다. MQTT 브로커를 사용하여 데이터를 저장합니다.
B. 센서 데이터를 수신하도록 AWS IoT Core를 설정합니다. AWS IoT Core에 연결할 사용자 지정 도메인을 생성하고 구성합니다. AWS IoT Core Data-ATS 엔드포인트를 가리키도록 Route 53의 DNS 레코드를 업데이트합니다. 데이터를 저장하도록 AWS IoT 규칙을 구성합니다.
C. 네트워크 로드 밸런서(NLB)를 생성합니다. MQTT 브로커를 대상으로 설정합니다. AWS Global Accelerator 액셀러레이터를 생성합니다. NLB를 가속기의 끝점으로 설정합니다. Route 53의 DNS 레코드를 다중값 응답 레코드로 업데이트합니다. Global Accelerator IP 주소를 값으로 설정합니다. MQTT 브로커를 사용하여 데이터를 저장합니다.
D. 센서 데이터를 수신하도록 AWS IoT Greengrass를 설정합니다. AWS IoT Greengrass 엔드포인트를 가리키도록 Route 53의 DNS 레코드를 업데이트합니다. 데이터를 저장하기 위해 AWS Lambda 함수를 호출하도록 AWS IoT 규칙을 구성합니다.

해설
정답: B
모든 IoT를 위한 IoT Core
AWS IoT Core는 확장성과 신뢰성을 제공하는 관리형 서비스로, 수백만 개의 디바이스를 쉽게 연결하고 데이터를 수집할 수 있음.
*AWS IoT Greengrass는 클라우드 기능을 로컬 디바이스로 확장하는 소프트웨어로 오프라인 작업지원이 가능한 IOT 솔루션.

◆ | **Q#0210.** | **Ref#0210.**
회사에 Linux 기반 Amazon EC2 인스턴스가 있습니다. 사용자는 EC2 SSH 키 페어와 함께 SSH를 사용하여 인스턴스에 액세스해야 합니다. 각 머신에는 고유한 EC2 키 쌍이 필요합니다.

회사는 요청 시 모든 EC2 키 쌍을 자동으로 교체하고 키를 안전하게 암호화된 장소에 보관하는 키 교체 정책을 구현하려고 합니다. 회사는 키 순환 중에 1분 미만의 가동 중지 시간을 허용합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Secrets Manager에 모든 키를 저장하십시오. AWS Lambda 함수를 호출하여 새 키 쌍을 생성하도록 Secrets Manager 교체 일정을 정의합니다. EC2 인스턴스의 공개 키를 교체합니다. Secrets Manager에서 개인 키를 업데이트합니다.
B. AWS 시스템 관리자의 기능인 Parameter Store에 모든 키를 문자열로 저장합니다. AWS Lambda 함수를 호출하여 새 키 쌍을 생성하도록 Systems Manager 유지 관리 기간을 정의합니다. EC2 인스턴스의 공개 키를 교체합니다. Parameter Store에서 프라이빗 키를 업데이트합니다.
C. EC2 키 쌍을 AWS Key Management Service(AWS KMS)로 가져옵니다. 이러한 키 쌍에 대해 자동

키 순환을 구성합니다. AWS KMS에서 키 교체를 시작하기 위해 AWS Lambda 함수를 호출하는 Amazon EventBridge 예약 규칙을 생성합니다.
D. AWS Systems Manager의 기능인 Fleet Manager에 모든 EC2 인스턴스를 추가합니다. Systems Manager 유지 관리 기간을 정의하여 Systems Manager Run Command 문서를 발행하여 새로운 키 쌍을 생성하고 Fleet Manager의 모든 인스턴스에 대한 공개 키를 순환시킵니다.

해설
정답: A
모든 키를 AWS Secrets Manager에 저장하고, Secrets Manager 회전 일정을 정의하여 AWS Lambda 함수를 호출하여
새로운 키 쌍을 생성한 후 EC2 인스턴스에 있는 공개 키를 교체하고, Secrets Manager에 있는 개인 키를 업데이트하면
회전 과정을 자동화하고, downtime이 1분 미만이됨

211 (송희성) 2회차 完

◆ | **Q#0211.** | **Ref#0211.**
회사에서 AWS로 마이그레이션하려고 합니다. 이 회사는 VMware ESXi 환경에서 수천 개의 VM을 실행하고 있습니다. 이 회사에는 구성 관리 데이터베이스가 없으며 VMware 포트폴리오 활용에 대한 지식도 거의 없습니다.

솔루션 설계자는 회사가 비용 효율적인 마이그레이션을 계획할 수 있도록 정확한 인벤토리를 회사에 제공해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Systems Manager Patch Manager를 사용하여 Migration Evaluator를 각 VM에 배포하십시오. Amazon QuickSight에서 수집된 데이터를 검토합니다. 활용도가 높은 서버를 식별합니다. 마이그레이션 목록에서 활용도가 높은 서버를 제거합니다. 데이터를 AWS Migration Hub로 가져옵니다.
B. VMware 포트폴리오를 .csv 파일로 내보냅니다. 각 서버의 디스크 활용도를 확인하세요. 활용도가 높은 서버를 제거합니다. 데이터를 AWS Application Migration Service로 내보냅니다. AWS Server Migration Service(AWS SMS)를 사용하여 나머지 서버를 마이그레이션합니다.
C. Migration Evaluator 에이전트 없는 수집기를 ESXi 하이퍼바이저에 배포합니다. Migration Evaluator에서 수집된 데이터를 검토합니다. 비활성 서버를 식별합니다. 마이그레이션 목록에서 비활성 서버를 제거합니다. 데이터를 AWS Migration Hub로 가져옵니다.
D. AWS Application Migration Service 에이전트를 각 VM에 배포합니다. 데이터가 수집되면 Amazon Redshift를 사용하여 데이터를 가져오고 분석합니다. 데이터 시각화를 위해 Amazon QuickSight를 사용하십시오.

해설
정답: C
Agentless collector를 통해 VM에 설치 없이 데이터 수집이 가능하여, 운영 부담을 줄여줄 수 있다.
또한 수집된 VM데이터를 Migration Evaluator를 통해 인벤토리 파악
그리고 효율적인 이관 전략을 수립할 수 있습니다.
Migration Evaluator

◆ | **Q#0212.** | **Ref#0212.**
회사에서는 AWS Lambda 함수로 마이크로서비스를 실행합니다. 마이크로서비스는 제한된 수의 동시 연결을 지원하는 온프레미스 SQL 데이터베이스에 데이터를 씁니다. Lambda 함수 호출 수가 너무 많으면 데이터베이스가 충돌하고 애플리케이션 가동 중지 시간이 발생합니다. 회사는 회사의 VPC와 온프레미스 데이터 센터 간에 AWS Direct Connect 연결을 보유하고 있습니다. 회사는 충돌로부터 데이터베이스를 보호하려고 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon Simple Queue Service(Amazon SQS) 대기열에 데이터를 씁니다. 대기열에서 읽고 기존 데이터베이스에 쓰도록 Lambda 함수를 구성합니다. 데이터베이스가 지원하는 연결 수보다 적은 수로 Lambda 함수에 대해 예약된 동시성 제한을 설정합니다.
B. 새로운 Amazon Aurora Serverless DB 클러스터를 생성합니다. AWS DataSync를 사용하여 기존 데이터베이스의 데이터를 Aurora Serverless로 마이그레이션합니다. Aurora에 쓰도록 Lambda 함수를 재구성합니다.
C. Amazon RDS 프록시 DB 인스턴스를 생성합니다. RDS Proxy DB 인스턴스를 Amazon RDS DB 인스턴스에 연결합니다. RDS Proxy DB 인스턴스에 쓰도록 Lambda 함수를 재구성합니다.
D. Amazon Simple 알림 서비스(Amazon SNS) 주제에 데이터를 씁니다. 주제가 새 메시지를 수신하면 Lambda 함수를 호출하여 기존 데이터베이스에 씁니다. 데이터베이스가 지원하는 연결 수와 동일하도록 Lambda 함수에 대한 프로비저닝된 동시성을 구성합니다.

해설
정답: A
RDS 프록시 DB인스턴스는 On-prem 환경의 DB를 지원할 수 없다.
SQS를 사용함으로써 Lambda함수의 동시 실행 수를 제어하여 어플리케이션 다운타임 없이 운영 가능합니다.

◆ | **Q#0213.** | **Ref#0213.**
회사는 단일 Amazon EC2 인스턴스에서 실행되는 Grafana 데이터 시각화 솔루션을 사용하여 회사의 AWS 워크로드 상태를 모니터링합니다. 회사는 회사가 보존하고 싶은 대시보드를 만들기 위해 시간과 노력을 투자했습니다. 대시보드는 가용성이 높아야 하며 10분 이상 종료될 수 없습니다. 회사에서는 지속적인 유지 관리를 최소화해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon CloudWatch 대시보드로 마이그레이션하십시오. 기존 Grafana 대시보드와 일치하도록 대시보드를 다시 만듭니다. 가능하면 자동 대시보드를 사용하세요.
B. Amazon Managed Grafana 작업 공간을 생성합니다. 새로운 Amazon CloudWatch 데이터 소스를 구성합니다. 기존 Grafana 인스턴스에서 대시보드를 내보냅니다. 대시보드를 새 작업 영역으로 가져옵니다.
C. Grafana가 사전 설치된 AMI를 생성합니다. Amazon Elastic File System(Amazon EFS)에 기존 대시보드를 저장합니다. 새 AMI를 사용하는 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹의 최소, 원하는, 최대 인스턴스 수를 1로 설정합니다. 2개 이상의 가용 영역을 제공하는 Application Load Balancer를 생성합니다.
D. 매 시간마다 Grafana를 실행하는 EC2 인스턴스를 백업하도록 AWS Backup을 구성합니다. 필요한 경우 대체 가용 영역의 최신 스냅샷에서 EC2 인스턴스를 복원합니다.

해설
정답: B
A의 경우 CloudWatch에 대한 대시보드를 다시 만든다는 말이 기존의 쏟아 부은 노력을 부정하며
B의 경우 AWS가 관리 주체로, 운영 부담이 적고, 고가용성을 제공한다.
기존 대시보드를 내보내고 가져오는 과정이 간단하므로 B가 정답이다.

◆ | **Q#0214.** | **Ref#0214.**
회사는 고객 거래 데이터베이스를 온프레미스에서 AWS로 마이그레이션해야 합니다. 데이터베이스는 Linux 서버에서 실행되는 Oracle DB 인스턴스에 상주합니다. 새로운 보안 요구 사항에 따라 회사는 매년 데이터베이스 비밀번호를 교체해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS SCT(AWS Schema Conversion Tool)를 사용하여 데이터베이스를 Amazon DynamoDB로 변환합니다. AWS Systems Manager Parameter Store에 암호를 저장합니다. 연간 패스타드 교체를 위해 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다.

B. 데이터베이스를 Oracle용 Amazon RDS로 마이그레이션합니다. AWS Secrets Manager에 비밀번호를 저장합니다. 자동 회전을 켭니다. 연간 순환 일정을 구성합니다.
C. 데이터베이스를 Amazon EC2 인스턴스로 마이그레이션합니다. AWS Systems Manager Parameter Store를 사용하면 연간 일정에 따라 AWS Lambda 함수를 사용하여 연결 문자열을 유지하고 교체할 수 있습니다.
D. AWS SCT(AWS Schema Conversion Tool)를 사용하여 데이터베이스를 Amazon Neptune으로 마이그레이션합니다. 연간 암호 교체를 위해 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다.

해설
정답: B
오라클 DB를 호환하고, 운영 부담을 줄이는 솔루션은 Amazon RDS for Oracle이다.
Dynamo DB 및 Neptune은 아키텍처가 달라서 이관에 노력이 필요하고, AWS Secrets Manager를 사용하여 자동으로 비밀번호를 교체할 수 있다.

AWS Secrets Manager

◆ | **Q#0215.** | **Ref#0215.**
솔루션 아키텍트는 여러 팀으로 구성된 회사의 AWS 계정 구조를 설계하고 있습니다. 모든 팀은 동일한 AWS 리전에서 작업합니다. 회사에는 온프레미스 네트워크에 연결된 VPC가 필요합니다. 회사에서는 온프레미스 네트워크를 오가는 총 트래픽이 50Mbps 미만일 것으로 예상합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. VPC와 필수 서브넷을 프로비저닝하는 AWS CloudFormation 템플릿을 생성합니다. 각 AWS 계정에 템플릿을 배포합니다.
B. VPC와 필수 서브넷을 프로비저닝하는 AWS CloudFormation 템플릿을 생성합니다. 공유 서비스 계정에 템플릿을 배포합니다. AWS Resource Access Manager를 사용하여 서브넷을 공유합니다.
C. 온프레미스 네트워크에 연결하려면 AWS Site-to-Site VPN과 함께 AWS Transit Gateway를 사용하십시오. AWS Resource Access Manager를 사용하여 전송 게이트웨이를 공유합니다.
D. 온프레미스 네트워크에 연결하려면 AWS Site-to-Site VPN을 사용하십시오.
E. 온프레미스 네트워크에 연결하려면 AWS Direct Connect를 사용하십시오.

해설
정답: BD
Site to Site VPN은 최대 대역폭이 1.25Gbps이며, 50Mbps는 충분하다.
따라서 Direct Connect보다는 비용 효율적이다.
여러 VPC에 대한 언급이 없으므로, Transit GateWay는 굳이.

AWS RAM

◆ | **Q#0216.** | **Ref#0216.**
대기업의 솔루션 아키텍트는 AWS Organizations의 조직 내 모든 AWS 계정에서 인터넷으로의 아웃바운드 트래픽에 대한 네트워크 보안을 설정해야 합니다. 조직에는 100개 이상의 AWS 계정이 있으며, 계정은 중앙 집중식 AWS Transit Gateway를 사용하여 서로 라우팅됩니다. 각 계정에는 인터넷으로의 아웃바운드 트래픽을 위한 인터넷 게이트웨이와 NAT 게이트웨이가 모두 있습니다. 회사는 단일 AWS 리전에만 리소스를 배포합니다.

회사는 조직 내 모든 AWS 계정에 대해 인터넷으로의 모든 아웃바운드 트래픽에 대해 중앙에서 관리되는 규칙 기반 필터링을 추가할 수 있는 기능이 필요합니다. 아웃바운드 트래픽의 최대 로드는 각 가용 영역에서 25Gbps를 초과하지 않습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 인터넷으로의 아웃바운드 트래픽을 위한 새 VPC를 생성하십시오. 기존 Transit Gateway를 새 VPC에 연결합니다. 새 NAT 게이트웨이를 구성합니다. 리전의 모든 가용 영역에서 규칙 기반 필터링을 위해 오픈 소스 인터넷 프록시를 실행하는 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 프록시의 Auto Scaling 그룹을 가리키도록 모든 기본 경로를 수정합니다.
B. 인터넷으로의 아웃바운드 트래픽을 위한 새 VPC를 생성합니다. 기존 Transit Gateway를 새 VPC에 연결합니다. 새 NAT 게이트웨이를 구성합니다. 규칙 기반 필터링에는 AWS 네트워크 방화벽 방화벽을 사용합니다. 각 가용 영역에 네트워크 방화벽 엔드포인트를 생성합니다. 네트워크 방화벽 끝점을 가리키도록 모든 기본 경로를 수정합니다.
C. 각 AWS 계정에서 규칙 기반 필터링을 위한 AWS 네트워크 방화벽 방화벽을 생성합니다. 각 계정의 네트워크 방화벽 방화벽을 가리키도록 모든 기본 경로를 수정합니다.
D. 각 AWS 계정에서 규칙 기반 필터링을 위해 오픈 소스 인터넷 프록시를 실행하는 네트워크 최적화 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 프록시의 Auto Scaling 그룹을 가리키도록 모든 기본 경로를 수정합니다.

해설
정답: B
VPC를 별도 구성함으로써 outbound traffic을 다른 리소스와 분리하여 관리할 수 있습니다.
기존 트랜짓 게이트웨이와 연결하여 새 VPC와 연결하고,
규칙 기반 필터링을 위해 Network FireWall을 사용시 VPC에서 나가는 트래픽에 대한 사용자 지정 규칙을 정의하고 적용할 수 있습니다.

◆ | **Q#0217.** | **Ref#0217.**
회사는 로드 밸런서를 사용하여 단일 가용 영역의 Amazon EC2 인스턴스에 트래픽을 분산합니다. 회사는 보안에 대해 우려하고 있으며 솔루션 설계자가 다음 요구 사항을 충족하도록 솔루션을 다시 설계하기를 원합니다.

• 일반적인 취약성 공격에 대해 인바운드 요청을 필터링해야 합니다.
• 거부된 요청은 타사 감사 응용 프로그램으로 전송되어야 합니다.
• 모든 리소스는 가용성이 높아야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 애플리케이션의 AMI를 사용하여 다중 AZ Auto Scaling 그룹을 구성합니다. Application Load Balancer(ALB)를 생성하고 이전에 생성된 Auto Scaling 그룹을 대상으로 선택합니다. Amazon Inspector를 사용하여 ALB 및 EC2 인스턴스에 대한 트래픽을 모니터링합니다. WAF에서 웹 ACL을 생성합니다. 웹 ACL 및 ALB를 사용하여 AWS WAF를 생성합니다. AWS Lambda 함수를 사용하여 Amazon Inspector 보고서를 타사 감사 애플리케이션에 자주 푸시합니다.
B. ALB(Application Load Balancer)를 구성하고 EC2 인스턴스를 대상으로 추가합니다. WAF에서 웹 ACL을 생성합니다. 웹 ACL 및 ALB 이름을 사용하여 AWS WAF를 생성하고 Amazon CloudWatch Logs로 로깅을 활성화합니다. AWS Lambda 함수를 사용하여 로그를 타사 감사 애플리케이션에 자주 푸시합니다.
C. EC2 인스턴스를 대상으로 추가하는 대상 그룹과 함께 Application Load Balancer(ALB)를 구성합니다. 타사 감사 애플리케이션의 대상을 사용하여 Amazon Kinesis Data Firehose를 생성합니다. WAF에서 웹 ACL을 생성합니다. 웹 ACL 및 ALB를 사용하여 AWS WAF를 생성한 다음 Kinesis Data Firehose를 대상으로 선택하여 로깅을 활성화합니다. AWS Marketplace에서 AWS 관리형 규칙을 구독하고 WAF를 구독자로 선택합니다.
D. 애플리케이션의 AMI를 사용하여 다중 AZ Auto Scaling 그룹을 구성합니다. Application Load Balancer(ALB)를 생성하고 이전에 생성된 Auto Scaling 그룹을 대상으로 선택합니다. 타사 감사 애플리케이션의 대상을 사용하여 Amazon Kinesis Data Firehose를 생성합니다. WAF에서 웹 ACL을 생성합니다. WebACL 및 ALB를 사용하여 AWS WAF를 생성한 다음 Kinesis Data Firehose를 대상으로 선택하여 로깅을 활성화합니다. AWS Marketplace에서 AWS 관리형 규칙을 구독하고 WAF를 구독자로 선택합니다.

해설

정답: D
Multy-AZ Auto Scaling 그룹을 사용하여 고가용성을 보장하고,
WAF를 활용하여 공격을 필터링할 수 있다. Kinesis Data Firehose를 통해 3rd-party솔루션으로 전송이 가능합니다.
B와 C는 고가용성 전략 설명이 부족합니다. A의 Amazon Inspector는
트래픽 모니터링 도구이지 실시간 필터링 도구가 아닙니다.

◆ | **Q#0218.** | **Ref#0218.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 Application Load Balancer 뒤의 여러 가용 영역에 있는 Amazon EC2 인스턴스 집합에서 실행되는 마이크로서비스로 구성됩니다. 이 회사는 최근 Amazon API Gateway에 구현된 새로운 REST API를 추가했습니다. EC2 인스턴스에서 실행되는 일부 이전 마이크로서비스는 이 새로운 API를 호출해야 합니다.

회사는 공용 인터넷에서 API에 액세스하는 것을 원하지 않으며 독점 데이터가 공용 인터넷을 통과하는 것을 원하지 않습니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. VPC와 API 게이트웨이 사이에 AWS Site-to-Site VPN 연결을 생성합니다. API 게이트웨이를 사용하여 각 마이크로서비스에 대한 고유한 API 키를 생성하세요. 키를 요구하도록 API 메서드를 구성합니다.
B. API 게이트웨이용 인터페이스 VPC 엔드포인트를 생성하고 특정 API에 대한 액세스만 허용하도록 엔드포인트 정책을 설정합니다. VPC 엔드포인트에서의 액세스만 허용하도록 API 게이트웨이에 리소스 정책을 추가합니다. API 게이트웨이 엔드포인트 유형을 프라이빗으로 변경합니다.
C. IAM 인증을 사용하도록 API 게이트웨이를 수정합니다. API 게이트웨이에 대한 액세스를 허용하도록 EC2 인스턴스에 할당된 IAM 역할에 대한 IAM 정책을 업데이트합니다. API 게이트웨이를 새 VP로 이동하고 전송 게이트웨이를 배포하고 VPC를 연결합니다.
D. AWS Global Accelerator에서 액셀러레이터를 생성하고 액셀러레이터를 API 게이트웨이에 연결합니다. 생성된 Global Accelerator 엔드포인트 IP 주소에 대한 경로를 사용하여 모든 VPC 서브넷의 라우팅 테이블을 업데이트합니다. 인증에 사용할 서비스별로 API 키를 추가하세요.

해설
정답: B
VPC엔드포인트를 생성하여 인터넷 통신 없이 Private한 통신 환경을 구축하고, 엔드포인트 정책 및 API 게이트웨이 정책을 수정함으로 문제의 요구사항을 이행할 수 있습니다.

◆ | **Q#0219.** | **Ref#0219.**
한 회사가 AWS에 전체 인프라를 설정했습니다. 이 회사는 Amazon EC2 인스턴스를 사용하여 전자상거래 웹사이트를 호스팅하고 Amazon S3를 사용하여 정적 데이터를 저장합니다. 회사의 엔지니어 3명이 하나의 AWS 계정을 통해 클라우드 관리 및 개발을 처리합니다. 때때로 엔지니어가 다른 엔지니어의 EC2 보안 그룹 구성을 변경하여 환경에 규정 준수 문제가 발생하는 경우가 있습니다.

솔루션 아키텍트는 엔지니어의 변경 사항을 추적하는 시스템을 설정해야 합니다. 엔지니어가 EC2 인스턴스의 보안 설정을 비준수로 변경하면 시스템에서 경고를 보내야 합니다.

솔루션 설계자가 이러한 요구 사항을 충족하는 가장 빠른 방법은 무엇입니까?

A. 회사를 위한 AWS Organizations를 설정합니다. SCP를 적용하여 AWS 계정에 대한 비준수 보안 그룹 변경 사항을 관리하고 추적합니다.
B. AWS CloudTrail을 활성화하여 EC2 보안 그룹에 대한 변경 사항을 캡처합니다. 비준수 보안 설정이 감지되면 알림을 제공하도록 Amazon CloudWatch 규칙을 활성화합니다.
C. 환경에 비준수 보안 그룹 변경이 있을 때 경고를 제공하도록 AWS 계정의 SCP를 활성화합니다.
D. EC2 보안 그룹에서 AWS Config를 활성화하여 비준수 변경 사항을 추적합니다. Amazon Simple Notification Service(Amazon SNS) 주제를 통해 변경 사항을 알림으로 보냅니다.

해설
정답: D
AWS Config 사용: AWS Config는 AWS 리소스의 구성을 지속적으로 모니터링하고 기록하는 서비스입니다. 보안 그룹 변경 사항을 추적하고 이러한 변경 사항이 설정된 규칙을 준수하는지 평가할 수 있습니다.
알림 전송: Amazon SNS를 사용하여 비규격 변경이 감지될 때마다 엔지니어에게 알림을 보낼 수 있습니다. 이를 통해 비규격 변경이 발생했을 때 즉각적인 대응이 가능합니다.
빠른 구현: 이 솔루션은 AWS Config를 활성화하고 SNS 주제를 설정하는 것만으로 구성되므로 빠르게 구현할 수 있습니다. 이는 SCP 또는 CloudTrail을 사용하여 비규격 변경을 추적하고 경고를 생성하는 것보다 빠르고 간단한 방법입니다.

◆ | **Q#0220.** | **Ref#0220.**
한 회사에는 대도시 전체의 교통 패턴을 모니터링하는 IoT 센서가 있습니다. 회사는 센서에서 데이터를 읽고 수집하고 데이터 집계를 수행하려고 합니다.

솔루션 아키텍트는 IoT 장치가 Amazon Kinesis Data Streams로 스트리밍되는 솔루션을 설계합니다. 여러 애플리케이션이 스트림에서 읽고 있습니다. 그러나 여러 소비자가 제한을 겪고 있으며 정기적으로 ReadProvisionedThroughputExceeded 오류가 발생하고 있습니다.

이 문제를 해결하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까? (3개를 선택하세요.)

A. 스트림을 다시 샤딩하여 스트림의 샤드 수를 늘립니다.
B. KPL(Kinesis 생산자 라이브러리)을 사용합니다. 폴링 빈도를 조정합니다.
C. 향상된 팬아웃 기능을 갖춘 소비자를 사용합니다.
D. 스트림을 다시 샤딩하여 스트림의 샤드 수를 줄입니다.
E. 소비자 논리에서 오류 재시도 및 지수 백오프 메커니즘을 사용합니다.
F. 동적 파티셔닝을 사용하도록 스트림을 구성합니다.

해설
정답: ACE
A: 샤드 수를 늘리면 스트림의 처리 용량이 증가하여 읽기 Throughput 초과 오류를 줄일 수 있습니다.
C: 향상된 팬아웃(Enhanced fan-out) 기능을 사용하면 각 Consumer가 독립적으로 데이터를 처리할 수 있어 Consumer 간의 리소스 경쟁이 줄어듭니다.
E: Error retry 및 지수 백오프(Exponential backoff) 메커니즘을 Consumer Logic에 적용하면 일시적인 Throughput 초과 오류를 효과적으로 처리할 수 있습니다.

221 (최정현) 2회차 完

◆ | **Q#0221.** | **Ref#0221.**
회사는 AWS Organizations를 사용하여 AWS 계정을 관리합니다. 회사에는 CPU 또는 메모리 사용량이 부족한 모든 Amazon EC2 인스턴스 목록이 필요합니다. 또한 회사는 활용도가 낮은 인스턴스의 크기를 줄이는 방법에 대한 권장 사항도 필요합니다.

최소한의 노력으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 모든 EC2 인스턴스에 AWS Marketplace의 CPU 및 메모리 모니터링 도구를 설치합니다. 결과를 Amazon S3에 저장합니다. 활용도가 낮은 인스턴스를 식별하는 Python 스크립트를 구현합니다. 축소 옵션에 대한 권장 사항은 EC2 인스턴스 요금 정보를 참조하세요.
B. AWS 시스템 관리자를 사용하여 모든 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다. 조직 마스터 계정의 AWS Cost Explorer에서 리소스 최적화 권장 사항을 검색합니다. 권장 사항을 사용하여 조직의 모든 계정에서 활용률이 낮은 인스턴스의 크기를 줄입니다.
C. AWS 시스템 관리자를 사용하여 모든 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니

다. 조직의 각 계정에 있는 AWS Cost Explorer에서 리소스 최적화 권장 사항을 검색합니다. 권장 사항을 사용하여 조직의 모든 계정에서 활용률이 낮은 인스턴스의 크기를 줄입니다.
D. AWS 시스템 관리자를 사용하여 모든 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다. 모든 EC2 인스턴스에서 CPU 및 메모리 사용량을 추출하는 AWS Lambda 함수를 생성합니다. 결과를 Amazon S3에 파일로 저장합니다. Amazon Athena를 사용하여 활용도가 낮은 인스턴스를 찾으세요. 축소 옵션에 대한 권장 사항은 EC2 인스턴스 요금 정보를 참조하세요.

해설
정답: B
AWS Cost Explorer는 과거 사용량 데이터를 기반으로 EC2 인스턴스 크기를 조정하는 등 리소스 최적화 권장 사항을 제공.
이러한 권장 사항은 조직 마스터 계정의 각 계정에 대해 생성되므로 모든 계정에 대한 인사이트를 중앙에서 얻을 수 있음.

A: 타사 솔루션(Marketplace) 설치와 별도의 스크립트(Python) 개발은 복잡함
C: 조직 내의 각 계정에 대해 별도로 권장 사항을 검색해야 하므로 중앙 집중식 관리 접근 방식에 비해 관리 오버헤드가 늘어남
D: CloudWatch와 AWS Cost Explorer 조합 보다 Lambda,Athena 사용은 복잡함

◆ | **Q#0222.** | **Ref#0222.**
회사에서는 트래픽이 VPC를 떠나고 들어갈 때 트래픽을 검사하기 위해 사용자 정의 네트워크 분석 소프트웨어 패키지를 실행하려고 합니다. 이 회사는 Auto Scaling 그룹의 Amazon EC2 인스턴스 3개에 AWS CloudFormation을 사용하여 솔루션을 배포했습니다. 트래픽을 EC2 인스턴스로 전달하기 위해 모든 네트워크 라우팅이 설정되었습니다.

분석 소프트웨어가 작동을 멈출 때마다 Auto Scaling 그룹은 인스턴스를 교체합니다. 인스턴스 교체가 발생하면 네트워크 경로가 업데이트되지 않습니다.

이 문제를 해결하려면 어떤 단계를 조합해야 합니까? (3개를 선택하세요.)

A. Auto Scaling 그룹이 실패한 인스턴스를 교체하게 하는 EC2 상태 확인 지표를 기반으로 경보를 생성합니다.
B. CloudFormation 템플릿을 업데이트하여 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다. 애플리케이션에 대한 프로세스 지표를 보내도록 CloudWatch 에이전트를 구성합니다.
C. CloudFormation 템플릿을 업데이트하여 EC2 인스턴스에 AWS Systems Manager 에이전트를 설치하십시오. 애플리케이션에 대한 프로세스 지표를 보내도록 Systems Manager 에이전트를 구성합니다.
D. 실패 시나리오에 대해 Amazon CloudWatch에서 사용자 지정 지표에 대한 경보를 생성합니다. Amazon Simple 알림 서비스(Amazon SNS) 주제에 메시지를 게시하도록 경보를 구성합니다.
E. Amazon Simple 알림 서비스(Amazon SNS) 메시지에 응답하여 인스턴스 서비스를 중단하는 AWS Lambda 함수를 생성합니다. 대체 인스턴스를 가리키도록 네트워크 경로를 업데이트합니다.
F. CloudFormation 템플릿에서 대체 인스턴스가 시작될 때 네트워크 경로를 업데이트하는 조건을 작성합니다.

해설
정답: BDE
-VPC 트래픽 검사 위해 사용자 정의 네트워크 분석 소프트웨어 패키지 실행 하려고 함
-Auto Scaling 그룹의 EC2 인스턴스 3개에 CloudFormation 으로 솔루션 배포
-분석 S/W가 멈출 때마다 Auto Scaling 그룹은 인스턴스를 교체 하지만, 네트워크 경로가 업데이트 되지 않음
문제 해결 방법은??

아래 절차로 해결한다.

CloudWatch Agent 설치 -> 경보 생성/구성 -> Amazon SNS(Simple Notification Service) 메시지에 응답하는 Lambda 함수 생성(네트워크 경로 업데이트)

◆ | **Q#0223.** | **Ref#0223.**
한 회사가 마이크로서비스를 기반으로 하는 새로운 주문형 비디오 애플리케이션을 개발하고 있습니다. 이 애플리케이션은 출시 시점에 500만 명의 사용자를 확보하고 6개월 후에는 3000만 명의 사용자를 확보하게 됩니다. 이 회사는 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)에 애플리케이션을 배포했습니다. 회사는 HTTPS 프로토콜을 사용하는 ECS 서비스를 사용하여 애플리케이션을 개발했습니다.

솔루션 설계자는 블루/그린 배포를 사용하여 애플리케이션에 대한 업데이트를 구현해야 합니다. 솔루션은 로드 밸런서를 통해 각 ECS 서비스에 트래픽을 분산해야 합니다. 애플리케이션은 Amazon CloudWatch 경보에 응답하여 작업 수를 자동으로 조정해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 블루/그린 배포 유형과 Network Load Balancer를 사용하도록 ECS 서비스를 구성합니다. 수요를 충족하기 위해 서비스당 작업에 대한 서비스 할당량을 요청합니다.
B. 블루/그린 배포 유형과 Network Load Balancer를 사용하도록 ECS 서비스를 구성합니다. Cluster Autoscaler를 사용하여 각 ECS 서비스에 대한 Auto Scaling 그룹을 구현합니다.
C. 블루/그린 배포 유형과 Application Load Balancer를 사용하도록 ECS 서비스를 구성합니다. Cluster Autoscaler를 사용하여 각 ECS 서비스에 대한 Auto Scaling 그룹을 구현합니다.
D. 블루/그린 배포 유형과 Application Load Balancer를 사용하도록 ECS 서비스를 구성합니다. 각 ECS 서비스에 대해 서비스 자동 조정을 구현합니다.

해설
정답: D
(상황)
-Microservice 기반의 VOD App 개발중
-사용자 증가 : 500만 -> 3,000만
-Farget의 Amazon Elastic Container Service(ECS)에 App 배포
-HTTPS 프로토콜 사용
(솔루션은?)
-솔루션 설계자는 블루/그린 배포 방식으로 App 업데이트 해야 함
-솔루션은 로드 밸런서를 통해 각 ECS 서비스에 트래픽 분산 해야 함
-App은 CloudWatch 경보에 응답하여 작업(tasks) 수를 자동 조정 해야 함

A,B: HTTPS를 사용한다고 했으니, Network Load Balancer 사용은 오답
C: Fargate에는 Cluster Auto Scaling이 없으므로 오답

*Amazon Elastic Container Service(Amazon ECS)?
컨테이너 애플리케이션을 쉽게 배포, 관리 및 확대할 수 있도록 도와주는 완전 관리형 컨테이너 오케스트레이션 서비스
*AWS Fargate?
-사용량에 따라 요금이 부과되는 서버리스 컴퓨팅 엔진
-서버를 관리할 필요가 없기 때문에 애플리케이션 구축에 집중할 수 있다.

◆ | **Q#0224.** | **Ref#0224.**
한 회사가 AWS 클라우드에서 컨테이너화된 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon EC2 인스턴스 세트에서 Amazon Elastic Container Service(Amazon ECS)를 사용하여 실행됩니다. EC2 인스턴스는 Auto Scaling 그룹에서 실행됩니다.

이 회사는 Amazon Elastic Container Registry(Amazon ECR)를 사용하여 컨테이너 이미지를 저장합니다. 새 이미지 버전이 업로드되면 새 이미지 버전은 고유한 태그를 받습니다.

회사에는 일반적인 취약점과 노출이 있는지 새 이미지 버전을 검사하는 솔루션이 필요합니다. 솔루션은 심각도 또는 높음 심각도 결과가 있는 새 이미지 태그를 자동으로 삭제해야 합니다. 또한 솔루션은 그러한 삭제가 발생하는 경우 개발팀에 알려야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 리포지토리에서 푸시 시 스캔(scan)을 구성합니다. 위험 또는 높음 심각도 결과가 있는 이미지에 대한 스캔이 완료되면 Amazon EventBridge를 사용하여 AWS Step Functions 상태 시스템을 호출합니다. Step Functions 상태 시스템을 사용하여 해당 이미지에 대한 이미지 태그를 삭제하고 Amazon Simple 알림 서비스(Amazon SNS)를 통해 개발 팀에 알립니다.
> **B.** 리포지토리에서 푸시 시 스캔(scan)을 구성합니다. Amazon Simple Queue Service(Amazon SQS) 대기열에 푸시되도록 스캔 결과를 구성합니다. SQS 대기열에 새 메시지가 추가되면 AWS Lambda 함수를 호출합니다. 심각도 또는 높음 심각도 결과가 있는 이미지의 이미지 태그를 삭제하려면 Lambda 함수를 사용하십시오. Amazon Simple Email Service(Amazon SES)를 사용하여 개발 팀에 알립니다.
> **C.** 매시간 수동 이미지 스캔을 시작하도록 AWS Lambda 함수를 예약합니다. 스캔이 완료되면 다른 Lambda 함수를 호출하도록 Amazon EventBridge를 구성합니다. 두 번째 Lambda 함수를 사용하여 심각도 또는 높음 심각도 결과가 있는 이미지의 이미지 태그를 삭제합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 개발팀에 알립니다.
> **D.** 리포지토리에서 정기적인 이미지 검색을 구성합니다. Amazon Simple Queue Service(Amazon SQS) 대기열에 추가되도록 스캔 결과를 구성합니다. SQS 대기열에 새 메시지가 추가되면 AWS Step Functions 상태 시스템을 호출합니다. 심각도 또는 높음 심각도 결과가 있는 이미지에 대한 이미지 태그를 삭제하려면 Step Functions 상태 시스템을 사용하십시오. Amazon Simple Email Service(Amazon SES)를 사용하여 개발 팀에 알립니다.
>
> 해설
> 정답: A
> (상황)
> -AWS에서 컨테이너화된 App 실행 중
> -App은 Amazon Elastic Container Service(Amazon ECS)를 사용
> -EC2 인스턴스는 Auto Scaling 그룹에서 실행
> -Amazon Elastic Container Registry(Amazon ECR)를 사용하여 컨테이너 이미지를 저장
> -새 이미지 버전이 업로드 될때, Unique tag를 받음
>
> (솔루션?)
> -새 이미지에 취약점이 있는지 검사하는 솔루션 필요
> -Critical or High severity 있는 새 이미지 태그는 자동 삭제
> -자동 삭제시 개발팀에 알려야 함
>
> Amazon ECR 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 된다.
> 주기적으로 스캔하는것은 충분하지 않기에 새 이미지 업로드시 스캔하는 "푸시 스캔" 솔루션을 찾는다.
>
> B: SES는 일반적으로 대량/마케팅 이메일 발송시 사용
> C: 주기적(매시간) 스캔은 좋은 방법이 아님
> D: B와 같은 이유로 제외
>
> *EventBridge
> -AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에

자동으로 대응할 수 있다.
-AWS 서비스에서 발생하는 이벤트는 거의 EventBridge 실시간으로 전송된다.
-관심 있는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동 작업을 포함할 수 있다.

*AWS Step Functions
-시각적 워크플로우를 사용해 분산 애플리케이션 및 마이크로서비스의 구성 요소를 손쉽게 조정하도록 해주는 웹 서비스
-AWS의 여러 컴퓨팅 자원들의 수행 순서를 설정할 수 있는 서비스

◆ | **Q#0225.** | **Ref#0225.**
회사는 AWS에서 많은 워크로드를 실행하고 AWS Organizations를 사용하여 계정을 관리합니다. 워크로드는 Amazon EC2,AWS Fargate,AWS Lambda에서 호스팅됩니다. 일부 워크로드에는 예측할 수 없는 수요가 있습니다. 계정은 어떤 달에는 높은 사용량을 기록하고 다른 달에는 낮은 사용량을 기록합니다.

회사는 향후 3년 동안 컴퓨팅 비용을 최적화하려고 합니다. 솔루션 설계자는 사용량을 계산하기 위해 조직 전체의 각 계정에 대해 6개월 평균을 얻습니다.

조직의 모든 컴퓨팅 사용량에 대해 가장 많은 비용 절감 효과를 제공하는 솔루션은 무엇입니까?

A. 회원 계정에서 가장 일반적인 EC2 인스턴스의 크기와 수에 맞게 조직의 예약 인스턴스를 구매하십시오.
B. 마스터 계정 수준의 권장 사항을 사용하여 마스터 계정에서 조직을 위한 Compute Savings Plan을 구매합니다.
C. 지난 6개월 동안의 데이터에 따라 EC2 사용량이 높은 각 멤버 계정에 대해 예약 인스턴스를 구매합니다.
D. 지난 6개월 동안의 EC2 사용 데이터를 기반으로 마스터 계정에서 각 멤버 계정에 대한 EC2 Instance Savings Plan을 구매합니다.

해설
정답: B
-AWS에서 많은 워크로드 실행 -> AWS Organizations로 계정 관리
-워크로드는 EC2, Fargate, Lambda에서 호스팅
-예측할 수 없는 수요가 있다.

-3년 동안 컴퓨팅 비용 최적화 예정
-설계자는 사용량을 계산하기 위해 조직 전체의 각 계정에 대해 6개월 평균을 얻는다.
-비용 절감 효과 제공하는 솔루션은?

A: RI(Reserved Instances,예약 인스턴스)는 EC2 만 지원
B: Compute Savings Plan은 마스터 계정에 적용 되며, EC2,Fargate,Lambda 지원
C: RI는 EC2 및 조직 마스커 계정에 적용 되는 변경 사항만 지원
D: EC2 Instance Savings Plan은 EC2만 지원

◆ | **Q#0226.** | **Ref#0226.**
회사에는 수백 개의 AWS 계정이 있습니다. 회사는 AWS Organizations의 조직을 사용하여 모든 계정을 관리합니다. 회사는 모든 기능을 켰습니다.

재무팀은 AWS 비용에 대한 일일 예산을 할당했습니다. 조직의 AWS 비용이 할당된 예산의 80%를 초과하는 경우 재무팀은 이메일 알림을 받아야 합니다. 솔루션 설계자는 비용을 추적하고 알림을 전달하는 솔루션을 구현해야 합

니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 조직의 마스터 계정에서 AWS 예산을 사용하여 일일 기간이 있는 예산을 생성합니다. 경고 임계값을 추가하고 값을 80%로 설정합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 재무팀에 알립니다.
> **B.** 조직의 마스터 계정에서 AWS Trusted Advisor에 대한 조직 보기 기능을 설정합니다. 비용 최적화를 위한 조직 보기 보고서를 만듭니다. 경고 임계값을 80%로 설정합니다. 알림 기본 설정을 구성합니다. 재무팀의 이메일 주소를 추가하세요.
> **C.** AWS Control Tower에 조직을 등록합니다. 선택적 비용 관리(가드레일)를 활성화합니다. 제어(가드레일) 매개변수를 80%로 설정합니다. 제어(가드레일) 알림 기본 설정을 구성합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 재무팀에 알립니다.
> **D.** 일일 AWS 비용 및 사용 보고서를 조직의 Amazon S3 버킷에 저장하도록 회원 계정을 구성합니다. 마스터 계정. Amazon EventBridge를 사용하여 일일 Amazon Athena 쿼리를 예약하여 조직의 비용을 계산합니다. 총 비용이 할당된 예산의 80%를 초과하는 경우 Amazon CloudWatch 알림을 보내도록 Athena를 구성합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 재무팀에 알립니다.
>
> 해설
> 정답: A
>
> -회사에는 수백 개의 AWS 계정이 있음
> -AWS Organizations 으로 계정 관리
> -재무팀은 비용에 대해 일일 예산 할당
> -80% 초과시 이메일 알림 필요
>
> A: 마스터 계정에서 일일 예산 생성, 임계치 설정하고, SNS 서비스로 알림
> B,C,D: 불필요한 방법(Trusted Advisor,Control Tower,예산은 Mgmt 계정 자체에서 관리)

◆ | **Q#0227.** | **Ref#0227.**
한 회사에서 미술품 경매 서비스를 제공하고 북미와 유럽 전역에 사용자를 보유하고 있습니다. 이 회사는 us-east-1 지역의 Amazon EC2 인스턴스에서 애플리케이션을 호스팅합니다. 아티스트는 자신의 작품 사진을 대형 사이즈로 업로드합니다. 휴대폰의 고해상도 이미지 파일을 us-east-1 리전에서 생성된 중앙 집중식 Amazon S3 버킷으로 보냅니다. 유럽 사용자들은 이미지 업로드 성능이 저하되고 있다고 보고하고 있습니다.

솔루션 설계자는 이미지 업로드 프로세스의 성능을 어떻게 향상시킬 수 있습니까?

> **A.** S3 멀티파트 업로드를 사용하려면 애플리케이션을 재배포하세요.
> **B.** Amazon CloudFront 배포판을 생성하고 애플리케이션을 사용자 지정 원본으로 지정합니다.
> **C.** S3 Transfer Acceleration을 사용하도록 버킷을 구성합니다.
> **D.** EC2 인스턴스에 대한 Auto Scaling 그룹을 생성하고 조정 정책을 생성합니다.
>
> 해설
> 정답: C
>
> -미술품 경매 서비스 제공, 북미와 유럽에 사용자 있음
> -us-east-1 Region의 EC2 에서 App 호스팅
> -아티스트는 작품 사진을 대형 사이즈로 업로드(휴대폰)
> -작품 이미지는 중앙 집중식 Amazon S3 버킷으로 보내짐
> -유럽 사용자는 성능 저하 => 성능 향상 방법??

S3 Transfer Acceleration은 Amazon CloudFront 글로벌 엣지 로케이션 네트워크를 활용하여 S3 버킷과의 데이터 전송을 가속화 한다.
중앙 집중식 S3 버킷에서 S3 Transfer Acceleration을 활성화하면 유럽 사용자는 데이터가 가장 가까운 CloudFront 엣지 위치를 통해 라우팅되므로 업로드가 더 빨라진다.
https://aws.amazon.com/s3/transfer-acceleration/

S3 멀티파트 업로드는 북미/유럽 사용자 모두 빨라짐. 문제는 유럽 사용자들 성능 향상이기에 제외됨

◆ | **Q#0228.** | **Ref#0228.**
한 회사는 다중 계층 웹 애플리케이션을 컨테이너화하고 애플리케이션을 온프레미스 데이터 센터에서 AWS로 이동하려고 합니다. 응용 프로그램에는 웹이 포함되어 있습니다. 애플리케이션 및 데이터베이스 계층. 회사는 애플리케이션의 내결함성과 확장성을 높여야 합니다. 자주 액세스하는 일부 데이터는 애플리케이션 서버 전체에서 항상 사용할 수 있어야 합니다. 프런트엔드 웹 서버에는 세션 지속성이 필요하며 트래픽 증가에 맞춰 확장해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)에서 애플리케이션을 실행하십시오. 웹 계층과 애플리케이션 계층 간에 자주 액세스되는 데이터에는 Amazon Elastic File System(Amazon EFS)을 사용합니다. Amazon Simple Queue Service(Amazon SQS)에 프런트엔드 웹 서버 세션 데이터를 저장합니다.
B. Amazon EC2의 Amazon Elastic Container Service(Amazon ECS)에서 애플리케이션을 실행합니다. Redis용 Amazon ElastiCache를 사용하여 프런트엔드 웹 서버 세션 데이터를 캐시합니다. 여러 가용 영역에 분산된 EC2 인스턴스에서 다중 연결 기능이 있는 Amazon Elastic Block Store(Amazon EBS)를 사용하세요.
C. Amazon Elastic Kubernetes Service(Amazon EKS)에서 애플리케이션을 실행합니다. 관리형 노드 그룹을 사용하도록 Amazon EKS를 구성합니다. ReplicaSets를 사용하여 웹 서버와 애플리케이션을 실행합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. 모든 EKS 포드에 EFS 파일 시스템을 탑재하여 프런트엔드 웹 서버 세션 데이터를 저장합니다.
D. Amazon Elastic Kubernetes Service(Amazon EKS)에 애플리케이션을 배포합니다. 관리형 노드 그룹을 사용하도록 Amazon EKS를 구성합니다. EKS 클러스터에서 웹 서버와 애플리케이션을 Kubernetes 배포로 실행합니다. 프런트엔드 웹 서버 세션 데이터를 Amazon DynamoDB 테이블에 저장합니다. 배포 시 모든 애플리케이션이 탑재될 Amazon Elastic File System(Amazon EFS) 볼륨을 생성합니다.

해설
정답: D
Amazon EKS를 사용하면 애플리케이션의 확장성이 용이
DynamoDB에 세션 데이터를 저장하면 데이터의 고가용성과 내구성이 보장
EKS, DynamoDB 및 EFS와 같은 관리형 서비스는 인프라 관리 작업을 처리하여 지속적인 운영 오버헤드를 줄이는 데 도움이 됨

◆ | **Q#0229.** | **Ref#0229.**
솔루션 아키텍트는 중요한 Microsoft SQL Server 데이터베이스를 AWS로 마이그레이션할 계획입니다. 데이터베이스는 레거시 시스템이므로 솔루션 설계자는 데이터베이스를 최신 데이터 아키텍처로 이동합니다. 솔루션 설계자는 가동 중지 시간이 거의 없이 데이터베이스를 마이그레이션해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Application Migration Service 및 AWS Schema Conversion Tool(AWS SCT)을 사용하십시오. 마이그레이션 전에 전체 업그레이드를 수행합니다. 컷오버 후 마이그레이션된 데이터를 Amazon Aurora Serverless로 내보냅니다. 애플리케이션을 Amazon Aurora로 다시 지정합니다.
B. AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 다시 호스팅합니다. Amazon S3를 대상으로 설정합니다. 변경 데이터 캡처(CDC) 복제를 설정합니다. 원본과 대상이 완전히 동기화되면 Amazon S3의 데이터를 Microsoft SQL Server DB 인스턴스용 Amazon RDS로 로드합니다.
C. 기본 데이터베이스 고가용성 도구를 사용하십시오. 소스 시스템을 Microsoft SQL Server DB 인스턴스용 Amazon RDS에 연결합니다. 이에 따라 복제를 구성하십시오. 데이터 복제가 완료되면 워크로드를 Microsoft SQL Server DB 인스턴스용 Amazon RDS로 전환합니다.
D. AWS 애플리케이션 마이그레이션 서비스를 사용하십시오. Amazon EC2에서 데이터베이스 서버를 다시 호스팅합니다. 데이터 복제가 완료되면 데이터베이스를 분리하고 데이터베이스를 Microsoft SQL Server DB 인스턴스용 Amazon RDS로 이동합니다. 데이터베이스를 다시 연결한 다음 모든 네트워킹을 차단합니다.

해설
정답: C

(문제)
-Microsoft SQL Server 데이터베이스 -> AWS로 마이그레이션할 계획
-데이터베이스를 최신 데이터 아키텍처로 변경
-가동 중지 시간이 거의 없이 데이터베이스를 마이그레이션 방법?

네이티브 데이터베이스 고가용성 도구(Native Database High Availability Tools): AWS는 데이터베이스 미러링, Always On Availability Groups, 트랜잭션 복제와 같은 MS-SQL 서버용 네이티브 고가용성 도구를 제공
이러한 도구는 마이그레이션 프로세스 중 다운타임을 최소화하고 데이터 일관성과 무결성을 보장하도록 설계되었음

https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/always-on.html

◆ | **Q#0230.** | **Ref#0230.**
한 회사의 솔루션 설계자가 다중 애플리케이션 환경의 비용을 분석하고 있습니다. 환경은 단일 AWS 리전의 여러 가용 영역에 배포됩니다. 최근 인수 후 회사는 AWS Organizations에서 두 개의 조직을 관리합니다. 회사는 하나의 조직에서 AWS PrivateLink 기반 VPC 엔드포인트 서비스로 여러 서비스 공급자 애플리케이션을 만들었습니다. 회사는 다른 조직에서 여러 서비스 소비자 애플리케이션을 만들었습니다.

데이터 전송 비용은 회사가 예상한 것보다 훨씬 높으며, 솔루션 아키텍트는 비용을 줄여야 합니다. 솔루션 설계자는 개발자가 서비스를 배포할 때 따라야 할 지침을 권장해야 합니다. 이러한 지침은 전체 환경에 대한 데이터 전송 비용을 최소화해야 합니다.

이러한 요구 사항을 충족하는 지침은 무엇입니까? (2개를 선택하세요.)

A. AWS Resource Access Manager를 사용하여 서비스 공급자 애플리케이션을 호스팅하는 서브넷을 조직의 다른 계정과 공유하십시오.
B. 동일한 조직의 AWS 계정에 서비스 공급자 애플리케이션과 서비스 소비자 애플리케이션을 배치합니다.
C. 모든 서비스 제공업체 애플리케이션 배포에서 Network Load Balancer에 대한 교차 영역 로드 밸런싱을 해제합니다.
D. 엔드포인트의 로컬 DNS 이름을 사용하여 서비스 소비자 컴퓨팅 리소스가 가용 영역별 엔드포인트 서비스를 사용하는지 확인합니다.

E. 조직의 계획된 가용 영역 간 데이터 전송 사용량에 대해 적절한 적용 범위를 제공하는 절약 계획을 만듭니다.

해설
정답: CD

(문제)
-다중 App 환경의 비용 분석 중
-환경은 단일 AWS Region의 여러 가용 영역(AZ)에 배포
-최근 인수 후 회사는 AWS Organizations에서 두 개의 조직을 관리
-회사는 한 조직에서 AWS PrivateLink 기반 VPC 엔드포인트 서비스로 여러 서비스 공급자 App 제작
-회사는 다른 조직에서 여러 서비스 소비자 App 제작
-데이터 전송 비용은 회사가 예상한 것보다 훨씬 높으며, 비용 절감이 필요

A. AWS Resource Access Manager를 사용하여 서브넷을 공유하는 것은 데이터 전송 비용을 줄이는 직접적인 방법이 아닙니다.
B. 동일한 조직 내에 애플리케이션을 배치하는 것은 데이터 전송 비용에 큰 영향을 미치지 않습니다.
C. 크로스 존 로드 밸런싱을 끄면 가용 영역 간 데이터 전송 비용을 줄일 수 있습니다.
D. 로컬 DNS 이름을 사용하여 가용 영역 간 데이터 전송을 피할 수 있습니다.
E. Savings Plan은 비용 절감에 도움이 되지만, 데이터 전송 비용과는 직접적인 관련이 없습니다.
따라서, C와 D가 데이터 전송 비용을 줄이는데 가장 효과적인 가이드라인입니다.

231 (김성원) 2회차 完

◆ | **Q#0231.** | **Ref#0231.**
회사에는 야간에 로컬 드라이브에 200GB 내보내기를 쓰는 온프레미스 Microsoft SQL Server 데이터베이스가 있습니다. 회사는 백업을 Amazon S3의 더욱 강력한 클라우드 스토리지로 옮기기를 원합니다. 회사는 온프레미스 데이터 센터와 AWS 간에 10Gbps AWS Direct Connect 연결을 설정했습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 새 S3 버킷을 생성합니다. Direct Connect 연결에 연결된 VPC 내에 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 새 SMB 파일 공유를 만듭니다. 야간 데이터베이스 내보내기를 새 SMB 파일 공유에 기록합니다.
B. Direct Connect 연결에 연결된 VPC 내에 Windows 파일 서버 단일 AZ 파일 시스템용 Amazon FSx를 생성합니다. 새 SMB 파일 공유를 만듭니다. Amazon FSx 파일 시스템의 SMB 파일 공유에 야간 데이터베이스 내보내기를 기록합니다. 야간 백업을 활성화합니다.
C. Direct Connect 연결에 연결된 VPC 내에서 Windows 파일 서버 다중 AZ 파일 시스템용 Amazon FSx를 생성합니다. 새 SMB 파일 공유를 만듭니다. Amazon FSx 파일 시스템의 SMB 파일 공유에 야간 데이터베이스 내보내기를 기록합니다. 야간 백업을 활성화합니다.
D. 새 S3 버킷을 생성합니다. Direct Connect 연결에 연결된 VPC 내에 AWS Storage Gateway 볼륨 게이트웨이를 배포합니다. 새 SMB 파일 공유를 만듭니다. 볼륨 게이트웨이의 새 SMB 파일 공유에 야간 데이터베이스 내보내기를 작성하고 이 데이터를 S3 버킷에 자동으로 복사합니다.

해설
정답: A

AWS Storage Gateway 파일 게이트웨이를 사용하면 온프레미스에서 S3의 견고한 클라우드 스토리지로 손쉽게 데이터를 백업할 수 있습니다. 이 방법은 비용도 절약하고 운영 효율성도 향상시킵니다.

◆ | **Q#0232.** | **Ref#0232.**
회사는 온프레미스 데이터 센터에서 AWS로 연결을 설정해야 합니다. 회사는 VPC 네트워크 간의 전이적 라우팅 기능을 사용하여 다양한 AWS 지역에 있는 모든 VPC를 연결해야 합니다. 또한 회사는 네트워크 아웃바운드 트래픽 비용을 줄이고, 대역폭 처리량을 늘리며, 최종 사용자에게 일관된 네트워크 경험을 제공해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 온프레미스 데이터 센터와 새로운 중앙 VPC 간에 AWS Site-to-Site VPN 연결을 생성합니다. 중앙 VPC에서 다른 모든 VPC로 시작되는 VPC 피어링 연결을 생성합니다.
> **B.** 온프레미스 데이터 센터와 AWS 간에 AWS Direct Connect 연결을 생성합니다. 전송 VIF를 프로비저닝하고 이를 Direct Connect 게이트웨이에 연결합니다. 각 리전의 전송 게이트웨이를 사용하여 Direct Connect 게이트웨이를 다른 모든 VPC에 연결합니다.
> **C.** 온프레미스 데이터 센터와 새로운 중앙 VP 간에 AWS Site-to-Site VPN 연결을 생성합니다. 동적 라우팅이 포함된 전송 게이트웨이를 사용합니다. Transit Gateway를 다른 모든 VPC에 연결합니다.
> **D.** 온프레미스 데이터 센터와 AWS 간에 AWS Direct Connect 연결을 생성합니다. 각 리전의 모든 VPC 간에 AWS Site-to-Site VPN 연결을 설정합니다. 중앙 VPC에서 다른 모든 VPC로 시작되는 VPC 피어링 연결을 생성합니다.
>
> 해설
> 정답: B
>
> AWS Direct Connect는 사설 연결을 통해 온프레미스 환경과 AWS를 연결합니다. 그리고 각 리전의 트랜짓 게이트웨이를 사용하여 Direct Connect 게이트웨이를 모든 다른 VPC에 연결함으로써, 트래픽 비용을 줄이고 대역폭 처리량을 늘리며 일관된 네트워크를 제공할 수 있습니다.

◆ | **Q#0233.** | **Ref#0233.**
한 회사가 개발 및 생산 워크로드를 AWS Organizations의 새로운 조직으로 마이그레이션하고 있습니다. 회사는 개발용 회원계정과 제작용 회원계정을 별도로 개설하였습니다. 통합결제는 마스터 계정에 연결됩니다. 마스터 계정에서 솔루션 아키텍트는 두 멤버 계정 모두에서 리소스를 중지하거나 종료할 수 있는 IAM 사용자를 생성해야 합니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 마스터 계정에서 IAM 사용자 및 교차 계정 역할을 생성합니다. 멤버 계정에 대한 최소 권한 액세스로 교차 계정 역할을 구성합니다.
> **B.** 각 회원 계정에 IAM 사용자를 생성합니다. 마스터 계정에서 최소 액세스 권한이 있는 교차 계정 역할을 생성합니다. 신뢰 정책을 사용하여 IAM 사용자에게 교차 계정 역할에 대한 액세스 권한을 부여합니다.
> **C.** 마스터 계정에서 IAM 사용자를 생성합니다. 회원 계정에서 최소 액세스 권한이 있는 IAM 그룹을 생성합니다. 마스터 계정의 IAM 사용자를 멤버 계정의 각 IAM 그룹에 추가합니다.
> **D.** 마스터 계정에서 IAM 사용자를 생성합니다. 멤버 계정에서 최소 액세스 권한이 있는 교차 계정 역할을 생성합니다. 신뢰 정책을 사용하여 IAM 사용자에게 역할에 대한 액세스 권한을 부여합니다.
>
> 해설
> 정답: D
>
> 관리 계정에 IAM 사용자를 생성하고, 각 멤버 계정에서 해당 사용자를 위한 크로스-어카운트 역할을 생성합니다. 이 역할은 최소 권한으로 설정되어야 하며, 이 사용자가 해당 역할에 접근할 수 있도록 신뢰 정책이 필요합니다. 이렇게 하면 사용자는 각 멤버 계정에서 리소스를 중지하거나 종료할 수 있는 권한을 얻게 됩니다.
> - 교차 계정 역할: 한 AWS 계정의 사용자 또는 서비스가 다른 계정의 리소스에 액세스할 수 있는 안전하고 관리되는 방법을 제공합니다.

- 최소 권한 액세스: 멤버 계정의 리소스를 중지하거나 종료하는 데 필요한 최소 권한으로 교차 계정 역할을 구성하여 잠재적인 보안 위험을 최소화합니다.
- 중앙 집중식 제어: 마스터 계정에서 사용자 자격 증명 및 액세스를 유지하면 중앙 집중식 관리 및 감사가 단순화됩니다.

◆ | **Q#0234.** | **Ref#0234.**
회사에서는 온프레미스 애플리케이션의 재해 복구를 위해 AWS를 사용하려고 합니다. 이 회사는 애플리케이션을 실행하는 수백 대의 Windows 기반 서버를 보유하고 있습니다. 모든 서버는 공통 공유를 마운트합니다.

이 회사의 RTO는 15분, RPO는 5분입니다. 솔루션은 기본 장애 조치 및 대체 기능을 지원해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. AWS Storage Gateway 파일 게이트웨이를 생성합니다. 매일 Windows 서버 백업을 예약합니다. 데이터를 Amazon S3에 저장합니다. 재해 발생 시 백업에서 온프레미스 서버를 복구합니다. 테일백 중에 Amazon EC2 인스턴스에서 온프레미스 서버를 실행합니다.
B. AWS CloudFormation 템플릿 세트를 생성하여 인프라를 생성합니다. AWS DataSync를 사용하여 모든 데이터를 Amazon Elastic File System(Amazon EFS)에 복제합니다. 재해 발생 시 AWS CodePipeline을 사용하여 온프레미스 서버를 복원하는 템플릿을 배포합니다. DataSync를 사용하여 데이터를 장애 복구합니다.
C. AWS CDK(AWS Cloud Development Kit) 파이프라인을 생성하여 AWS에서 다중 사이트 Active-Active 환경을 구축합니다. s3 sync 명령을 사용하여 데이터를 Amazon S3에 복제합니다. 재해가 발생하면 DNS 엔드포인트를 AWS를 가리키도록 교체하세요. s3 sync 명령을 사용하여 데이터를 장애 복구합니다.
D. AWS Elastic Disaster Recovery를 사용하여 온프레미스 서버를 복제합니다. AWS DataSync를 사용하여 Amazon FSx for Windows File Server 파일 시스템에 데이터를 복제합니다. 파일 시스템을 AWS 서버에 탑재합니다. 재해 발생 시 온프레미스 서버를 AWS로 장애 조치합니다. Elastic Disaster Recovery를 사용하여 신규 또는 기존 서버로 장애 복구합니다.

해설
정답: D

AWS Elastic Disaster Recovery를 사용하면 온프레미스 서버를 AWS에 복제하고, AWS DataSync를 사용하여 Amazon FSx for Windows File Server 파일 시스템에 데이터를 복제할 수 있습니다. 재해 발생 시에는 온프레미스 서버를 AWS로 장애 전환하고 이후 재해 복구를 위해 Elastic Disaster Recovery를 사용하여 새로운 서버나 기존 서버로 복제하면 됩니다. 이 방법이 가장 비용 효율적이며 요구사항을 충족시킵니다.

◆ | **Q#0235.** | **Ref#0235.**
한 회사는 Amazon EFS에 저장된 대량의 공유 파일을 생성하는 긴밀하게 결합된 워크로드를 위해 AWS에 고성능 컴퓨팅(HPC) 클러스터를 구축했습니다. 클러스터의 Amazon EC2 인스턴스 수가 100개일 때는 클러스터 성능이 좋았습니다. 그러나 회사가 클러스터 크기를 EC2 인스턴스 1,000개로 늘렸을 때 전체 성능은 기대보다 훨씬 낮았습니다.

솔루션 아키텍트는 HPC 클러스터에서 최대 성능을 달성하기 위해 어떤 디자인 선택을 해야 합니까? (3개를 선택하세요.)

A. HPC 클러스터가 단일 가용 영역 내에서 시작되는지 확인하세요.
B. EC2 인스턴스를 시작하고 탄력적 네트워크 인터페이스를 4의 배수로 연결합니다.
C. EFA(Elastic Fabric Adapter)가 활성화된 EC2 인스턴스 유형을 선택합니다.
D. 클러스터가 여러 가용 영역에서 시작되는지 확인합니다.
E. Amazon EFS를 RAID 어레이의 여러 Amazon EBS 볼륨으로 교체합니다.
F. Amazon EFS를 Lustre용 Amazon FSx로 교체합니다.

해설
정답: A,C,F

- A. 클러스터의 EC2 인스턴스가 동일한 데이터 센터 내에 위치하므로 네트워크 지연 시간이 짧고 대역폭이 높습니다
- C. EFA는 EC2 인스턴스 간에 지연 시간이 짧고 고대역폭 통신을 제공하는 네트워크 인터페이스입니다. EFA가 활성화된 인스턴스 유형을 선택하면 클러스터는 향상된 인스턴스 간 통신의 이점을 누릴 수 있습니다.
- F. Lustre용 Amazon FSx는 HPC 워크로드에 최적화된 고성능 파일 시스템입니다. Amazon EFS 대신 FSx for Lustre를 사용하면 클러스터는 워크로드에서 생성된 많은 수의 공유 파일에 대해 더 나은 성능을 얻을 수 있습니다.

◆ | **Q#0236.** | **Ref#0236.**
한 회사가 AWS Organizations 구조를 설계하고 있습니다. 회사는 전체 조직에 태그를 적용하는 프로세스를 표준화하려고 합니다. 회사에서는 사용자가 새 리소스를 생성할 때 특정 값이 포함된 태그를 요구합니다. 회사의 각 OU에는 고유한 태그 값이 있습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 필수 태그가 없는 리소스 생성을 거부하려면 SCP를 사용하십시오. 회사가 각 OU에 할당한 태그 값을 포함하는 태그 정책을 생성합니다. 태그 정책을 OU에 연결합니다.
B. SCP를 사용하여 필수 태그가 없는 리소스 생성을 거부합니다. 회사가 각 OU에 할당한 태그 값을 포함하는 태그 정책을 생성합니다. 태그 정책을 조직의 마스터 계정에 연결합니다.
C. SCP를 사용하여 리소스에 필수 태그가 있는 경우에만 리소스 생성을 허용합니다. 회사가 각 OU에 할당한 태그 값을 포함하는 태그 정책을 생성합니다. 태그 정책을 OU에 연결합니다.
D. SCP를 사용하여 필수 태그가 없는 리소스 생성을 거부합니다. 태그 목록을 정의합니다. SCP를 OU에 연결합니다.

해설
정답: A
필요한 태그가 없는 리소스 생성을 거부하는 서비스 제어 정책(Service Control Policy, SCP)을 사용하고, 회사에서 각 조직 단위(OU)에 할당한 태그 값이 포함된 태그 정책을 만든 후 이를 해당 조직 단위에 첨부하면 됩니다. 이렇게 하면 필요한 태그와 값을 모든 리소스 생성에 적용하는 데 필요한 표준화를 달성할 수 있습니다.

◆ | **Q#0237.** | **Ref#0237.**
한 회사에는 MQTT(Message Queuing Telemetry Transport) 프로토콜을 사용하여 온프레미스 Apache Kafka 서버에 데이터를 보내는 10,000개 이상의 센서가 있습니다. 온프레미스 Kafka 서버는 데이터를 변환한 다음 결과를 Amazon S3 버킷에 객체로 저장합니다.

최근 Kafka 서버가 다운되었습니다. 서버를 복원하는 동안 회사에서 센서 데이터가 손실되었습니다. 솔루션 아키텍트는 유사한 발생을 방지하기 위해 가용성과 확장성이 뛰어난 새로운 설계를 AWS에서 생성해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 두 개의 Amazon EC2 인스턴스를 시작하여 두 개의 가용 영역에 걸쳐 활성/대기 구성으로 Kafka 서버를 호스팅합니다. Amazon Route 53에서 도메인 이름을 생성합니다. Route 53 장애 조치 정책을 생성합니다. 데이터를 도메인 이름으로 보내도록 센서를 라우팅합니다.
B. 온프레미스 Kafka 서버를 Amazon Managed Streaming for Apache Kafka(Amazon MSK)로 마이그레이션합니다. Amazon MSK 브로커를 가리키는 NLB(Network Load Balancer)를 생성합니다. NLB 상태 확인을 활성화합니다. 데이터를 NLB로 보내도록 센서를 라우팅합니다.
C. AWS IoT Core를 배포하고 Amazon Kinesis Data Firehose 전송 스트림에 연결합니다. AWS Lambda 함수를 사용하여 데이터 변환을 처리합니다. 데이터를 AWS IoT Core로 보내도록 센서를 라

우팅합니다.
D. AWS IoT Core를 배포하고 Amazon EC2 인스턴스를 시작하여 Kafka 서버를 호스팅합니다. 데이터를 EC2 인스턴스로 보내도록 AWS IoT Core를 구성합니다. 데이터를 AWS IoT Core로 보내도록 센서를 라우팅합니다.

해설
정답: C

데이터를 실시간으로 수집, 변환 및 이동시키는 과정을 단순화하는 Kinesis Data Firehose와 함께 AWS IoT Core를 사용합니다. 센서 데이터는 AWS IoT Core를 통해 전송되고, Kinesis Data Firehose를 통해 어디에서나 안전하게 저장 및 분석할 수 있습니다. AWS Lambda는 실시간 데이터 변환을 처리하고 결과를 S3 버킷에 즉시 저장할 수 있습니다. 이 방법은 높은 가용성과 확장성을 제공합니다.

◆ | **Q#0238.** | **Ref#0238.**
한 회사는 최근 AWS 클라우드에서 새로운 애플리케이션 워크로드를 호스팅하기 시작했습니다. 이 회사는 Amazon EC2 인스턴스, Amazon Elastic File System (Amazon EFS) 파일 시스템, 그리고 Amazon RDS DB 인스턴스를 사용하고 있습니다.

규정 및 비즈니스 요구 사항을 충족하기 위해 회사는 데이터 백업에 대해 다음과 같은 변경을 수행해야 합니다.

• 백업은 사용자 지정 일일, 주간 및 월간 요구 사항에 따라 유지되어야 합니다.
• 백업은 캡처 후 즉시 하나 이상의 다른 AWS 리전에 복제되어야 합니다.
• 백업 솔루션은 AWS 환경 전반에 걸쳐 백업 상태에 대한 단일 소스를 제공해야 합니다.
• 백업 솔루션은 리소스 백업 실패 시 즉시 알림을 보내야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. 각 보존 요구 사항에 대한 백업 규칙을 사용하여 AWS 백업 계획을 생성합니다.
B. 백업을 다른 지역으로 복사하도록 AWS 백업 계획을 구성합니다.
C. 백업을 다른 리전에 복제하고 오류가 발생하면 알림을 보내는 AWS Lambda 함수를 생성합니다.
D. BACKUP_JOB_COMPLETED를 제외한 모든 상태의 완료된 작업에 대한 알림을 보내려면 백업 계획에 Amazon Simple 알림 서비스(Amazon SNS) 주제를 추가합니다.
E. 각 보존 요구 사항에 대한 Amazon Data Lifecycle Manager(Amazon DLM) 스냅샷 수명 주기 정책을 생성합니다.
F. 각 데이터베이스에 RDS 스냅샷을 설정합니다.

해설
정답: A,B,D

- A를 통해, 회사는 일일, 주간, 월간 보존 요구사항별로 백업 계획을 만들 수 있습니다.
- B는 백업을 다른 AWS 리전으로 즉시 복제하는 것을 가능하게 합니다. 이는 회사가 데이터를 백업한 후에 신속하게 복제를 수행해야 할 때 특히 유용합니다.
- D는 백업 작업의 완료를 알려주고, BACKUP_JOB_COMPLETED라는 상태 외의 모든 상태에 대해 알림을 보냅니다. 이것은 백업 실패에 대한 즉각적인 알림을 보장하는 데 도움이 됩니다.

◆ | **Q#0239.** | **Ref#0239.**
한 회사는 연구자들이 다양한 집단으로부터 대량의 데이터 샘플을 수집하는 데 도움이 되도록 게놈 정보를 수집하는 유전자 보고 장치를 개발하고 있습니다. 이 장치는 데이터를 처리 및 분석하고 연구자들에게 정보를 다시 제공해야 하는 데이터 플랫폼에 매초 8KB의 게놈 데이터를 푸시합니다. 데이터 플랫폼은 다음 요구 사항을 충족해야 합니다.

• 인바운드 게놈 데이터에 대한 거의 실시간 분석 제공
• 데이터의 유연성, 병렬성 및 내구성 보장
• 처리 결과를 데이터 웨어하우스에 전달

이 요구 사항을 충족하기 위해 솔루션 아키텍트가 사용할 전략은 무엇입니까?

> **A.** Amazon Kinesis Data Firehose를 사용하여 인바운드 센서 데이터를 수집하고, Kinesis 클라이언트로 데이터를 분석하고, 결과를 Amazon RDS 인스턴스에 저장합니다.
> **B.** Amazon Kinesis Data Streams를 사용하여 인바운드 센서 데이터를 수집하고, Kinesis 클라이언트로 데이터를 분석하고, Amazon EMR을 사용하여 Amazon Redshift 클러스터에 결과를 저장합니다.
> **C.** Amazon S3를 사용하여 인바운드 장치 데이터를 수집하고, Kinesis를 사용하여 Amazon SQS에서 데이터를 분석하고, 결과를 Amazon Redshift 클러스터에 저장합니다.
> **D.** Amazon API Gateway를 사용하여 Amazon SQS 대기열에 요청을 넣고, AWS Lambda 함수로 데이터를 분석하고, Amazon EMR을 사용하여 Amazon Redshift 클러스터에 결과를 저장합니다.
>
> 해설
> 정답: B
>
> Amazon Kinesis Data Streams는 실시간으로 들어오는 데이터를 수집하고 병렬로 처리하는 데 적합합니다. 이는 거의 실시간 분석을 제공해야 하는 요구 사항을 충족합니다.
> Kinesis 클라이언트는 데이터를 유연하고 병렬적으로 처리할 수 있으며, 내구성 있는 데이터 스트림을 지원합니다.
> Amazon EMR은 대규모 데이터를 처리하는 데 유용하며, 데이터를 분석한 결과를 Amazon Redshift 클러스터로 전달하여 데이터를 저장하고 분석할 수 있습니다.
>
> A(x): Kinesis Data Firehose는 실시간 처리보다는 데이터 스트림을 안정적으로 전달하는 데 더 적합합니다. 실시간 분석에는 적합하지 않을 수 있습니다.
> C(x): Amazon S3와 SQS를 사용하는 방식은 실시간 처리보다는 배치 처리에 더 적합하며, 실시간 분석 요구 사항을 충족하기 어렵습니다.
> D(x): API Gateway와 SQS를 사용하는 방식은 데이터를 실시간으로 처리하기보다는 요청 기반으로 큐에 저장하므로 실시간 분석 요구 사항을 충족하지 못할 수 있습니다.

◆ | **Q#0240.** | **Ref#0240.**
솔루션 설계자는 웹, 애플리케이션, NoSQL 데이터 계층을 포함한 3계층 애플리케이션을 위한 참조 아키텍처를 정의해야 합니다. 참조 아키텍처는 다음 요구 사항을 충족해야 합니다:

• AWS 리전 내 고가용성
• 재해 복구를 위해 1분 안에 다른 AWS 리전으로 장애 조치 가능
• 사용자 경험에 미치는 영향을 최소화하면서 가장 효율적인 솔루션 제공

이 요구 사항을 충족하려면 어떤 조합의 단계를 수행해야 합니까? (3개를 선택하세요.)

> **A.** 선택한 두 리전에서 100/0으로 설정된 Amazon Route 53 가중치 라우팅 정책을 사용하십시오. TTL(Time to Live)을 1시간으로 설정합니다.
> **B.** 기본 지역에서 재해 복구 지역으로의 장애 조치를 위해 Amazon Route 53 장애 조치 라우팅 정책을 사용합니다. TTL(Time to Live)을 30초로 설정합니다.
> **C.** 선택한 두 리전에서 데이터에 액세스할 수 있도록 Amazon DynamoDB 내의 글로벌 테이블을 사용합니다.
> **D.** 60분마다 기본 리전의 Amazon DynamoDB 테이블에서 데이터를 백업한 다음 Amazon S3에 데이터를 씁니다. S3 교차 리전 복제를 사용하여 기본 리전의 데이터를 재해 복구 리전으로 복사합니다. 재해 복구 시나리오에서 스크립트를 통해 데이터를 DynamoDB로 가져오도록 합니다.
> **E.** 지역의 여러 가용 영역에 걸쳐 웹 및 애플리케이션 계층에 대한 Auto Scaling 그룹을 사용하여 상시 대기 모델을 구현합니다. 최소 서버 수에는 영역 예약 인스턴스를 사용하고 추가 리소스에는 온

디맨드 인스턴스를 사용합니다.
F. 리전의 여러 가용 영역에 걸쳐 웹 및 애플리케이션 계층에 Auto Scaling 그룹을 사용합니다. 필요한 리소스에 스팟 인스턴스를 사용하십시오.

해설
정답: B,C,E

B: 1분 안에 다른 AWS 지역으로 장애를 넘길 수 있는 Amazon Route 53 장애 조치 라우팅 정책을 사용하게 됩니다.
C: 글로벌 테이블 Amazon DynamoDB는 데이터를 두 선택한 지역에서 동일하게 복제하므로 데이터 고가용성이 보장됩니다.
E: 가용 영역간에 오토 스케일링 그룹을 사용하여 웹 및 애플리케이션 계층의 고가용성을 보장하며, 센터 비용을 최소화하는 동시에 서비스 수준의 유연성이 증가합니다.

241 (고민석) 2회차 完

◆ | **Q#0241.** | **Ref#0241.**
스마트 자동차를 제조하는 회사입니다. 회사는 맞춤형 애플리케이션을 사용하여 차량 데이터를 수집합니다. 차량은 MQTT 프로토콜을 사용하여 애플리케이션에 연결합니다. 회사는 5분 간격으로 데이터를 처리합니다. 그런 다음 회사는 차량 텔레매틱스 데이터를 온프레미스 스토리지에 복사합니다. 맞춤형 애플리케이션은 이 데이터를 분석하여 이상 징후를 탐지합니다.

데이터를 전송하는 차량의 수는 지속적으로 증가하고 있습니다. 최신 차량은 대량의 데이터를 생성합니다. 온프레미스 스토리지 솔루션은 최대 트래픽에 맞게 확장할 수 없으므로 데이터 손실이 발생합니다. 회사는 확장 문제를 해결하기 위해 솔루션을 현대화하고 솔루션을 AWS로 마이그레이션해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS IoT Greengrass를 사용하여 차량 데이터를 Apache Kafka용 Amazon Managed Streaming(Amazon MSK)으로 보냅니다. Amazon S3에 데이터를 저장할 Apache Kafka 애플리케이션을 생성합니다. Amazon SageMaker에서 사전 훈련된 모델을 사용하여 이상 징후를 탐지합니다.
B. AWS IoT Core를 사용하여 차량 데이터를 수신합니다. Amazon S3에 데이터를 저장하는 Amazon Kinesis Data Firehose 전송 스트림으로 데이터를 라우팅하는 규칙을 구성합니다. 이상을 탐지하기 위해 전송 스트림에서 읽는 Amazon Kinesis Data Analytics 애플리케이션을 생성합니다.
C. AWS IoT FleetWise를 사용하여 차량 데이터를 수집합니다. Amazon Kinesis 데이터 스트림으로 데이터를 보냅니다. Amazon Kinesis Data Firehose 전송 스트림을 사용하여 Amazon S3에 데이터를 저장합니다. AWS Glue에 내장된 기계 학습 변환을 사용하여 이상 현상을 탐지합니다.
D. RabbitMQ용 Amazon MQ를 사용하여 차량 데이터를 수집합니다. Amazon Kinesis Data Firehose 전송 스트림으로 데이터를 전송하여 Amazon S3에 데이터를 저장합니다. Amazon Lookout for Metrics를 사용하여 이상 징후를 탐지하십시오.

해설
정답: B
B의 AWS IoT Core는 MQTT 프로토콜을 지원하므로 차량에서 데이터를 안전하게 수신하는 데 이상적입니다
Amazon Kinesis Data Firehose는 IoT Core에서 수신한 데이터를 적절한 대상으로 안전하게 전달하고 데이터를 대용량의 데이터를 효율적이고 실시간으로 처리할 수 있습니다
Amazon Kinesis Data Analytics는 실시간으로 스트리밍 데이터를 분석하며 이 데이터를 기반으로 이상 징후를 감지할 수 있습니다.
따라서 가장 적은 운영 부담으로 요구사항을 충족시킬 수 있습니다
나머지 옵션들은 모두 운영 부하를 더 많이 발생시킵니다. 이들은 추가적인 서비스 이용, 설정 및 관리가 필요하며, 이로 인해 운영 부담이 증가합니다.

◆ | **Q#0242.** | **Ref#0242.**
감사 중에 보안 팀은 개발 팀이 IAM 사용자 보안 액세스 키를 코드에 넣은 다음 이를 AWS CodeCommit 리포지토리에 커밋하고 있음을 발견했습니다. 보안 팀은 이 보안 취약점의 인스턴스를 자동으로 찾아서 해결하려고 합니다.

자격 증명이 자동으로 적절하게 보호되도록 보장하는 솔루션은 무엇입니까?

> **A.** AWS Systems Manager Run Command를 사용하여 야간에 스크립트를 실행하여 개발 인스턴스에서 자격 증명을 검색합니다. 찾은 경우 AWS Secrets Manager를 사용하여 자격 증명을 교체하세요.
> **B.** 예약된 AWS Lambda 함수를 사용하여 CodeCommit에서 애플리케이션 코드를 다운로드하고 스캔합니다. 자격 증명이 발견되면 새 자격 증명을 생성하여 AWS KMS에 저장합니다.
> **C.** CodeCommit 리포지토리에서 자격 증명을 검색하도록 Amazon Macie를 구성합니다. 자격 증명이 발견되면 AWS Lambda 함수를 트리거하여 자격 증명을 비활성화하고 사용자에게 알립니다.
> **D.** 새로운 코드 제출에서 자격 증명을 검색하기 위해 AWS Lambda 함수를 호출하도록 CodeCommit 트리거를 구성합니다. 자격 증명이 발견되면 AWS IAM에서 자격 증명을 비활성화하고 사용자에게 알립니다.
>
> 해설
> 정답: D
> D는 AWS CodeCommit 트리거를 이용해 코드의 신규 제출이 발생할 때마다 AWS Lambda 함수를 호출하게 설정하여, IAM 사용자의 비밀 액세스 키와 같은 인증 정보를 찾게됩니다
> 만약 인증 정보가 발견되면 AWS IAM에서 해당 인증 정보를 비활성화하고 AWS 자원에 대한 액세스가 즉시 차단되어 이후 보안 위협을 예방할 수 있습니다
> 따라서 D는 실시간으로 보안 문제를 자동으로 탐지하고 해결하는데 가장 효과적입니다.

◆ | **Q#0243.** | **Ref#0243.**
한 회사의 Amazon S3에 여러 AWS 계정에 걸쳐 수백 개의 애플리케이션이 액세스해야 하는 데이터 레이크가 있습니다. 회사의 정보 보안 정책에는 S3 버킷이 공용 인터넷을 통해 액세스되어서는 안 되며 각 애플리케이션이 작동하는 데 필요한 최소한의 권한이 있어야 한다고 명시되어 있습니다.

이러한 요구 사항을 충족하기 위해 솔루션 아키텍트는 각 애플리케이션에 대해 특정 VPC로 제한된 S3 액세스 포인트를 사용할 계획입니다.

솔루션 아키텍트는 이 솔루션을 구현하기 위해 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

> **A.** S3 버킷을 소유한 AWS 계정의 각 애플리케이션에 대해 S3 액세스 포인트를 생성합니다. 애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다. 액세스 포인트에서 액세스를 요구하도록 버킷 정책을 업데이트합니다.
> **B.** 각 애플리케이션의 VPC에서 Amazon S3에 대한 인터페이스 엔드포인트를 생성합니다. S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다. S3 엔드포인트에 대한 VPC 게이트웨이 연결을 생성합니다.
> **C.** 각 애플리케이션의 VPC에서 Amazon S3에 대한 게이트웨이 엔드포인트를 생성합니다. S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다. 액세스 포인트에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.
> **D.** 각 AWS 계정의 각 애플리케이션에 대한 S3 액세스 포인트를 생성하고 액세스 포인트를 S3 버킷에 연결합니다. 애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다. 액세스 포인트에서 액세스를 요구하도록 버킷 정책을 업데이트합니다.
> **E.** 데이터 레이크의 VPC에 Amazon S3용 게이트웨이 엔드포인트를 생성합니다. S3 버킷에 대한 액세스를 허용하려면 엔드포인트 정책을 연결하세요. 버킷에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.
>
> 해설

정답: A,C
A : 각 애플리케이션의 VPC는 해당 애플리케이션만을 위한 지정된 이름(name)과 연결된 접근 지점을 통해 S3 버킷에 대한 접근을 얻게 됩니다. 이후, S3 버킷 정책을 업데이트하여 액세스 지점을 통한 접근만을 허용하도록 합니다.
C : 애플리케이션의 네트워크 트래픽이 인터넷을 거치지 않도록 하며, S3와 통신하는데 있어 추가적인 데이터 전송 비용이나 대역폭 제한을 없애줍니다.

2가지 설정을 통해 퍼블릭 인터넷을 통한 S3 버킷 접근을 막고, 각 애플리케이션의 VPC에서 최소한의 권한으로 작동할 수 있습니다, 만약 특정 애플리케이션이 S3 버킷에 접근해야 할 경우, 해당 애플리케이션의 VPC에서 액세스 지점과 S3 게이트웨이 엔드포인트를 통해 접근할 수 있습니다

◆ | **Q#0244.** | **Ref#0244.**
한 회사가 데이터 센터와 AWS 간의 하이브리드 솔루션을 개발했습니다. 이 회사는 애플리케이션 로그를 Amazon CloudWatch로 보내는 Amazon VPC 및 Amazon EC2 인스턴스를 사용합니다. EC2 인스턴스는 온프레미스에서 호스팅되는 여러 관계형 데이터베이스에서 데이터를 읽습니다.

회사는 데이터베이스에 연결된 EC2 인스턴스를 거의 실시간으로 모니터링하려고 합니다. 이 회사는 이미 온프레미스에서 Splunk를 사용하는 모니터링 솔루션을 보유하고 있습니다. 솔루션 아키텍트는 네트워킹 트래픽을 Splunk로 보내는 방법을 결정해야 합니다.

솔루션 설계자는 이러한 요구 사항을 어떻게 충족해야 합니까?

A. VPC 흐름 로그를 활성화하고 CloudWatch로 보냅니다. 사전 정의된 내보내기 기능을 사용하여 CloudWatch 로그를 Amazon S3 버킷으로 주기적으로 내보내는 AWS Lambda 함수를 생성합니다. ACCESS_KEY 및 SECRET_KEY AWS 자격 증명을 생성합니다. 해당 자격 증명을 사용하여 S3 버킷에서 로그를 가져오도록 Splunk를 구성합니다.
B. Splunk를 대상으로 하여 Amazon Kinesis Data Firehose 전송 스트림을 생성합니다. CloudWatch Logs 구독 필터가 전송한 레코드에서 개별 로그 이벤트를 추출하는 Kinesis Data Firehose 스트림 프로세서를 사용하여 사전 처리 AWS Lambda 함수를 구성합니다. VPC 흐름 로그를 활성화하고 CloudWatch로 보냅니다. Kinesis Data Firehose 전송 스트림으로 로그 이벤트를 보내는 CloudWatch Logs 구독을 생성합니다.
C. EC2 인스턴스 IP 주소와 함께 데이터베이스에 대한 모든 요청을 기록하도록 회사에 요청하십시오. CloudWatch 로그를 Amazon S3 버킷으로 내보냅니다. Amazon Athena를 사용하여 데이터베이스 이름별로 그룹화된 로그를 쿼리합니다. Athena 결과를 다른 S3 버킷으로 내보냅니다. AWS Lambda 함수를 호출하여 S3 버킷에 있는 새 파일을 Splunk에 자동으로 보냅니다.
D. SQL 애플리케이션용 Amazon Kinesis Data Analytics를 사용하여 CloudWatch 로그를 Amazon Kinesis 데이터 스트림으로 보냅니다. 이벤트를 수집하기 위해 1분 슬라이딩 기간을 구성합니다. 이상 탐지 템플릿을 사용하여 거의 실시간으로 네트워킹 트래픽 이상을 모니터링하는 SQL 쿼리를 만듭니다. Splunk를 대상으로 하여 Amazon Kinesis Data Firehose 전송 스트림으로 결과를 보냅니다.

해설
정답: B
B는 VPC 플로우 로그를 활성화하여 모든 네트워크 트래픽을 CloudWatch로 전송하고, 이 로그를 Kinesis Data Firehose를 통해 실시간으로 Splunk로 전송하는 방법을 제안합니다.
이렇게 하면 AWS에서 발생하는 모든 트래픽이 실질적으로 사내의 Splunk로 전송되어 사내에서 원하는 모든 분석을 수행할 수 있게 됩니다.
또한, Kinesis Data Firehose는 대량의 스트리밍 데이터를 수집하고, 변환한 후, 지정된 대상으로 데이터를 로드하는 기능을 제공하므로 거의 실시간 모니터링이 가능하여 EC2 인스턴스에서 발생하는 모든 네트워크 트래픽, 즉 데이터베이스 연결도 로그를 통해 실시간으로 로깅되고 모니터링될 수 있다는 점입니다.

◆ | **Q#0245.** | **Ref#0245.**
회사에는 애플리케이션을 개발하고 호스팅하기 위해 각각 5개의 AWS 계정을 생성한 5개의 개발 팀이 있습니다.

지출을 추적하기 위해 개발 팀은 매달 각 계정에 로그인하고 AWS Billing and Cost Management 콘솔에서 현재 비용을 기록한 다음 해당 정보를 회사의 재무 팀에 제공합니다.

회사는 엄격한 규정 준수 요구 사항을 갖고 있으며 리소스가 미국의 AWS 리전에서만 생성되도록 해야 합니다. 그러나 일부 리소스는 다른 리전에서 생성되었습니다.

솔루션 설계자는 재무팀이 모든 계정에 대한 지출을 추적하고 통합할 수 있는 기능을 제공하는 솔루션을 구현해야 합니다. 또한 솔루션은 회사가 미국 지역에서만 리소스를 생성할 수 있도록 보장해야 합니다.

가장 운영상 효율적인 방식으로 이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** 마스터 계정으로 사용할 새 계정을 생성합니다. 재무팀을 위한 Amazon S3 버킷을 생성합니다. AWS 비용 및 사용 보고서를 사용하여 월별 보고서를 생성하고 재무팀의 S3 버킷에 데이터를 저장합니다.
> **B.** 마스터 계정으로 사용할 새 계정을 생성합니다. 모든 기능이 활성화된 AWS Organizations에 조직을 배포합니다. 기존 계정을 모두 조직에 초대합니다. 각 계정이 초대를 수락하는지 확인하세요.
> **C.** 모든 개발팀을 포함하는 OU를 생성합니다. 미국에 있는 리전에서만 리소스 생성을 허용하는 SCP를 생성합니다. SCP를 OU에 적용합니다.
> **D.** 모든 개발팀을 포함하는 OU를 만듭니다. 미국 이외 지역의 리소스 생성을 거부하는 SCP를 생성합니다. SCP를 OU에 적용합니다.
> **E.** 마스터 계정에서 IAM 역할을 생성합니다. Billing and Cost Management 콘솔을 볼 수 있는 권한이 포함된 정책을 연결합니다. 재무팀 사용자가 역할을 맡도록 허용합니다. AWS Cost Explorer와 Billing and Cost Management 콘솔을 사용하여 비용을 분석하세요.
> **F.** 각 AWS 계정에 IAM 역할을 생성합니다. Billing and Cost Management 콘솔을 볼 수 있는 권한이 포함된 정책을 연결합니다. 재무팀 사용자가 역할을 맡도록 허용합니다.
>
> 해설
> 정답: B,D,E
> B : 관리 계정을 생성하고, 모든 AWS 계정을 AWS 조직에 추가하면 AWS 계정들을 기능별로 분류하고, 중앙에서 관리가 가능해집니다. 이로 인해 효율적인 작업 관리 및 비용 추적이 가능하게 됩니다.
> D : 리소스가 미국 외부 지역에서 생성되는 것을 거부하는 정책을 적용하면, 회사의 엄격한 준수 요구사항을 만족시킬 수 있습니다. 이 정책은 회사가 미국 지역에서만 AWS 리소스를 생성하도록 보장하는데 도움이 됩니다.
> E :관리 계정에 IAM 역할을 만들고, 이 역할에 권한을 부여하면, 재무팀은 AWS 비용 탐색기와 비용 관리 콘솔에 접근하여 계정 비용을 분석하고 관리할 수 있습니다. 이로써 회사의 재무팀이 모든 AWS 계정의 지출을 효과적으로 추적하고 합칠 수 있게 됩니다.
>
> 이러한 요소들을 결합하면, 회사는 비용을 효과적으로 추적하고 미국 내에서만 AWS 리소스를 생성하도록 강제함으로써 기업의 요구사항을 충족시킬 수 있습니다

◆ | **Q#0246.** | **Ref#0246.**
회사는 중앙 위치에서 여러 부서에 대한 여러 AWS 계정을 생성하고 관리해야 합니다. 보안 팀에는 자체 AWS 계정에서 모든 계정에 대한 읽기 전용 액세스 권한이 필요합니다. 회사는 AWS Organizations를 사용하고 있으며 보안 팀용 계정을 만들었습니다.

솔루션 아키텍트는 이러한 요구 사항을 어떻게 충족해야 합니까?

> **A.** OrganizationAccountAccessRole IAM 역할을 사용하여 각 회원 계정에 읽기 전용 액세스 권한이 있는 새 IAM 정책을 생성합니다. 각 회원 계정의 IAM 정책과 보안 계정 간의 신뢰 관계를 설정합니다. 보안팀에 IAM 정책을 사용하여 액세스 권한을 부여해 달라고 요청하세요.
> **B.** OrganizationAccountAccessRole IAM 역할을 사용하여 각 회원 계정에 읽기 전용 액세스 권한이 있는 새 IAM 역할을 생성합니다. 각 구성원 계정의 IAM 역할과 보안 계정 간에 신뢰 관계를 설정합니다. 보안팀에 IAM 역할을 사용하여 액세스 권한을 얻으라고 요청하세요.
> **C.** 보안 팀에 AWS Security Token Service(AWS STS)를 사용하여 보안 계정의 마스터 계정에서

OrganizationAccountAccessRole IAM 역할에 대한 AssumeRole API를 호출하도록 요청하십시오. 생성된 임시 자격 증명을 사용하여 액세스하세요.
D. 보안 팀에 AWS Security Token Service(AWS STS)를 사용하여 보안 계정에서 멤버 계정의 OrganizationAccountAccessRole IAM 역할에 대한 AssumeRole API를 호출하도록 요청하세요. 생성된 임시 자격 증명을 사용하여 액세스하세요.

해설
정답: B
AWS Organizations를 사용하면 회사는 중앙에서 여러 AWS 계정을 생성하고 관리할 수 있습니다.
이 경우, 각 계정에는 자동으로 'OrganizationAccountAccessRole'이라는 IAM 역할이 생성됩니다.
이 역할에는 원칙적으로 조직의 관리 계정에서 해당 멤버 계정으로 스위칭하는 권한이 부여됩니다.
하지만, 이 문제에서는 보안 팀이 자신의 계정에서 모든 계정에 대한 읽기 전용 액세스 권한을 필요로 합니다.
따라서 OrganizationAccountAccessRole IAM 역할을 사용하여, 각 회원 계정에서 읽기 전용 액세스 권한을 가진 새로운 IAM 역할을 생성하고,각 회원 계정의 IAM 역할과 보안 계정 간에 신뢰 관계를 수립합니다.
이렇게 하면, 보안 팀이 IAM 역할을 통해 읽기 전용 액세스를 얻을 수 있게 됩니다

◆ | **Q#0247.** | **Ref#0247.**
대기업은 수백 개의 AWS 계정에 배포된 VPC에서 워크로드를 실행합니다. 각 VPC는 여러 가용 영역에 걸쳐 있는 퍼블릭 서브넷과 프라이빗 서브넷으로 구성됩니다. NAT 게이트웨이는 퍼블릭 서브넷에 배포되며 프라이빗 서브넷에서 인터넷으로의 아웃바운드 연결을 허용합니다.

솔루션 설계자는 허브 앤 스포크 설계를 진행 중입니다. 스포크 VPC의 모든 프라이빗 서브넷은 송신 VPC를 통해 트래픽을 인터넷으로 라우팅해야 합니다. 솔루션 아키텍트는 이미 중앙 AWS 계정의 송신 VPC에 NAT 게이트웨이를 배포했습니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자가 수행해야 하는 추가 단계는 무엇입니까?

A. 송신 VPC와 스포크 VPC 간에 피어링 연결을 생성합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.
B. 전송 게이트웨이를 생성하고 이를 기존 AWS 계정과 공유합니다. 기존 VPC를 Transit Gateway에 연결합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.
C. 모든 계정에 전송 게이트웨이를 생성합니다. NAT 게이트웨이를 전송 게이트웨이에 연결합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.
D. 송신 VPC와 스포크 VPC 사이에 AWS PrivateLink 연결을 생성합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.

해설
정답: B
B는 공유된 트랜짓 게이트웨이를 생성하고, 모든 VPC를 이 트랜짓 게이트웨이에 연결하여 필요한 인터넷 액세스를 허용하는 라우팅을 설정하는 전략을 제시합니다.
이 방식은 모든 VPC가 중앙의 송신 VPC를 통해 인터넷으로 라우팅되도록 구성할 수 있게 해주므로, 이 문제의 요구사항을 만족시킵니다.

◆ | **Q#0248.** | **Ref#0248.**
한 교육회사에서 전 세계 대학생들이 사용하는 웹 애플리케이션을 운영하고 있습니다. 애플리케이션은 ALB(Application Load Balancer) 뒤의 Auto Scaling 그룹에 있는 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 실행됩니다. 시스템 관리자는 애플리케이션의 인증 서비스를 압도하는 로그인 시도 실패 횟수가 매주 급증하는 것을 감지했습니다. 실패한 모든 로그인 시도는 매주 변경되는 약 500개의 서로 다른 IP 주소에서 발생합니다. 솔루션 설계자는 로그인 시도 실패로 인해 인증 서비스가 과부하되는 것을 방지해야 합니다.

가장 높은 운영 효율성으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Firewall Manager를 사용하여 IP 주소의 액세스를 거부하는 보안 그룹 및 보안 그룹 정책을 생성하십시오.
B. 비율 기반 규칙을 사용하여 AWS WAF 웹 ACL을 생성하고 규칙 작업을 차단으로 설정합니다. 웹 ACL을 ALB에 연결합니다.
C. AWS Firewall Manager를 사용하여 특정 CIDR 범위에만 액세스를 허용하는 보안 그룹 및 보안 그룹 정책을 생성합니다.
D. IP 세트 일치 규칙을 사용하여 AWS WAF 웹 ACL을 생성하고 규칙 작업을 차단으로 설정합니다. 웹 ACL을 ALB에 연결합니다.

해설
정답: B
B는 AWS WAF 웹 ACL을 만들고, 그 안에 비율 기반의 규칙을 생성하고 이를 ALB에 연결하는 방법을 제시하고 있습니다.
비율 기반 규칙은 특정 시간 동안의 요청 수를 기반으로 IP 주소를 차단하기 때문에, 지속적으로 로그인을 시도하는 IP 주소를 자동으로 차단해주는 방법입니다.
이 방법은 로그인 요청이 많은 IP 주소를 알아서 찾아내고 차단하므로, 매주 바뀌는 로그인 시도 IP 주소를 수동으로 관리하는 수고를 덜어줍니다.
이로 인하여 가장 운영 효율이 높은 방법이라고 할 수 있습니다.

◆ | **Q#0249.** | **Ref#0249.**
회사는 매일 여러 파일을 수집하는 온프레미스 SaaS(Software-as-a-Service) 솔루션을 운영합니다. 회사는 파일 전송을 용이하게 하기 위해 고객에게 여러 공용 SFTP 엔드포인트를 제공합니다. 고객은 아웃바운드 트래픽에 대한 방화벽 허용 목록에 SFTP 끝점 IP 주소를 추가합니다. SFTP 엔드포인트 IP 주소에 대한 변경은 허용되지 않습니다.

회사는 SaaS 솔루션을 AWS로 마이그레이션하고 파일 전송 서비스의 운영 오버헤드를 줄이고 싶어합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 회사의 AWS 계정에 고객이 소유한 IP 주소 블록을 등록합니다. 주소 풀에서 탄력적 IP 주소를 생성하고 SFTP용 AWS 전송 엔드포인트에 할당합니다. AWS Transfer를 사용하여 Amazon S3에 파일을 저장합니다.
B. 고객 소유의 IP 주소 블록을 포함하는 서브넷을 VPC에 추가합니다. 주소 풀에서 탄력적 IP 주소를 생성하고 이를 ALB(Application Load Balancer)에 할당합니다. 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨에 파일을 ALStore 뒤의 Auto Scaling 그룹에서 FTP 서비스를 호스팅하는 EC2 인스턴스를 시작합니다.
C. 고객 소유 IP 주소 블록을 Amazon Route 53에 등록합니다. Route 53에서 NLB(Network Load Balancer)를 가리키는 별칭 레코드를 생성합니다. NLB 뒤에 있는 Auto Scaling 그룹에서 FTP 서비스를 호스팅하는 EC2 인스턴스를 시작합니다. Amazon S3에 파일을 저장합니다.
D. 회사의 AWS 계정에 고객 소유 IP 주소 블록을 등록합니다. 주소 풀에서 탄력적 IP 주소를 생성하고 이를 Amazon S3 VPC 엔드포인트에 할당합니다. S3 버킷에서 SFTP 지원을 활성화합니다.

해설
정답: A
A는 기존 SFTP 엔드포인트 IP 주소의 변동없이 기능을 AWS로 이전할 수 있으며, 서비스 운영 부담도 줄일 수 있습니다.
AWS Transfer for SFTP 서비스는 완전 관리형 서비스로, 서버 구성 및 관리를 필요로하지 않습니다.
B는 SFTP가 아닌 FTP 서비스를 사용하고 있어서, 요구 사항을 충족시키지 못합니다.
C는 문제의 요구사항을 충족하기 위해 필요한 SFTP 기능을 제공하지 않습니다.
D의 Amazon S3 VPC 엔드포인트에서 SFTP 지원을 활성화하는 것은 현재 AWS에서 지원하지 않는 기능입니다.

◆ | **Q#0250.** | **Ref#0250.**
한 회사에 단일 AWS 리전의 5개 Amazon EC2 인스턴스에서 실행해야 하는 새로운 애플리케이션이 있습니다. 애

플리케이션에는 애플리케이션이 실행될 모든 EC2 인스턴스 간에 처리량이 높고 지연 시간이 짧은 네트워크 연결이 필요합니다. 애플리케이션이 내결함성이 있어야 한다는 요구 사항은 없습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 5개의 새로운 EC2 인스턴스를 클러스터 배치 그룹으로 시작합니다. EC2 인스턴스 유형이 향상된 네트워킹을 지원하는지 확인하세요.
> **B.** 동일한 가용 영역에 있는 Auto Scaling 그룹에 5개의 새로운 EC2 인스턴스를 시작합니다. 각 EC2 인스턴스에 추가 탄력적 네트워크 인터페이스를 연결합니다.
> **C.** 5개의 새로운 EC2 인스턴스를 파티션 배치 그룹으로 시작합니다. EC2 인스턴스 유형이 향상된 네트워킹을 지원하는지 확인하세요.
> **D.** 5개의 새로운 EC2 인스턴스를 분산 배치 그룹으로 시작합니다. 각 EC2 인스턴스에 추가 탄력적 네트워크 인터페이스를 연결합니다.
>
> 해설
> 정답: A
> A: 클러스터 배치 그룹은 같은 가용 영역에서 EC2 인스턴스를 그룹화합니다.
> 이렇게 함으로써 인스턴스간에 높은 네트워크 처리량과 낮은 지연 시간을 제공할 수 있어, 그룹에 속한 인스턴스 사이에서의 통신이 강화되고 고성능 네트워킹을 필요로 하는 어플리케이션에 이상적입니다.
> 문제에서의 애플리케이션은 고장 감내력(fault tolerant)이 필요하지 않고, 오직 높은 성능의 네트워크 통신을 요구하므로, 클러스터 배치 그룹이 이를 충족시키는 가장 효율적인 방법입니다

251 (신재경) 2회차 完

◆ | **Q#0251.** | **Ref#0251.**
한 회사가 미국에 있는 6개 파트너와 정보를 공유하기 위해 REST API를 만들고 있습니다. 회사는 Amazon API Gateway 지역 엔드포인트를 생성했습니다. 6개 파트너는 각각 하루에 한 번씩 API에 액세스하여 일일 판매 수치를 게시합니다.

초기 배포 후 회사는 전 세계 500개의 서로 다른 IP 주소에서 발생하는 초당 1,000개의 요청을 관찰합니다. 회사는 이 트래픽이 봇넷에서 발생한다고 믿고 비용을 최소화하면서 API를 보호하기를 원합니다.

API를 보호하기 위해 회사는 어떤 접근 방식을 취해야 합니까?

> **A.** API를 원본으로 사용하여 Amazon CloudFront 배포를 생성합니다. 하루에 5개 이상의 요청을 제출하는 클라이언트를 차단하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 CloudFront 배포와 연결합니다. OAI(원본 액세스 ID)로 CloudFront를 구성하고 이를 배포와 연결합니다. OAI만 POST 메서드를 실행할 수 있도록 API 게이트웨이를 구성합니다.
> **B.** API를 원본으로 사용하여 Amazon CloudFront 배포판을 생성합니다. 하루에 5개 이상의 요청을 제출하는 클라이언트를 차단하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 CloudFront 배포와 연결합니다. API 키로 채워진 CloudFront 배포에 사용자 지정 헤더를 추가합니다. POST 메서드에 API 키가 필요하도록 API를 구성합니다.
> **C.** 6개 파트너가 사용하는 IP 주소에 대한 액세스를 허용하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 API와 연결합니다. 요청 제한이 있는 리소스 정책을 생성하고 이를 API와 연결합니다. POST 메서드에 API 키가 필요하도록 API를 구성합니다.
> **D.** 6개 파트너가 사용하는 IP 주소에 대한 액세스를 허용하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 API와 연결합니다. 요청 제한이 있는 사용량 계획을 생성하고 이를 API와 연결합니다. API 키를 생성하여 사용량 계획에 추가하세요.
>
> 해설
> 정답: D
> AWS WAF를 사용하여 지정된 IP 주소만 허용하면 신뢰할 수 있는 파트너만 API에 접근할 수 있습니

다.
Usage Plan을 통해 요청 한도를 설정하면 API에 대한 과도한 요청을 방지할 수 있습니다.
API 키를 사용하여 인증을 강화할 수 있습니다.

◆ | **Q#0252.** | **Ref#0252.**
회사는 단일 AWS 리전의 애플리케이션에 Amazon Aurora PostgreSQL DB 클러스터를 사용합니다. 회사의 데이터베이스 팀은 모든 데이터베이스의 모든 데이터 활동을 모니터링해야 합니다.

이 목표를 달성할 솔루션은 무엇입니까?

A. AWS Database Migration Service(AWS DMS) 변경 데이터 캡처(CDC) 작업을 설정합니다. Aurora DB 클러스터를 소스로 지정합니다. Amazon Kinesis Data Firehose를 대상으로 지정합니다. 추가 분석을 위해 Kinesis Data Firehose를 사용하여 Amazon OpenSearch Service 클러스터에 데이터를 업로드합니다.
B. Amazon EventBridge에서 활동 스트림을 캡처하려면 Aurora DB 클러스터에서 데이터베이스 활동 스트림을 시작하십시오. EventBridge의 대상으로 AWS Lambda 함수를 정의합니다. EventBridge의 메시지를 해독하고 추가 분석을 위해 모든 데이터베이스 활동을 Amazon S3에 게시하도록 Lambda 함수를 프로그래밍합니다.
C. Aurora DB 클러스터에서 데이터베이스 활동 스트림을 시작하여 활동 스트림을 Amazon Kinesis 데이터 스트림으로 푸시합니다. Kinesis 데이터 스트림을 사용하고 추가 분석을 위해 Amazon S3에 데이터를 전송하도록 Amazon Kinesis Data Firehose를 구성합니다.
D. AWS Database Migration Service(AWS DMS) 변경 데이터 캡처(CDC) 작업을 설정합니다. Aurora DB 클러스터를 소스로 지정합니다. Amazon Kinesis Data Firehose를 대상으로 지정합니다. Kinesis Data Firehose를 사용하여 Amazon Redshift 클러스터에 데이터를 업로드합니다. Amazon Redshift 데이터에 대한 쿼리를 실행하여 Aurora 데이터베이스의 데이터베이스 활동을 확인합니다.

해설
정답: C
Amazon RDS Aurora의 데이터베이스 활동 스트림은 데이터 변경이 이벤트로 발생할 때 이벤트를 알립니다.
이 스트림은 Amazon Kinesis Data Streams나 Amazon Kinesis Data Firehose로 전송될 수 있습니다.
따라서, 데이터베이스 팀이 모든 데이터 활동을 모니터링할 수 있는 솔루션으로
Amazon Aurora PostgreSQL DB 클러스터와 함께 Amazon Kinesis Data Streams나 Amazon Kinesis Data Firehose를 이용하는 것이 적합할 것으로 보입니다.
A(x), D(x): AWS DMS의 변경 데이터 캡처(CDC) 기능은 데이터베이스 수준에서 이루어진 변경 사항을 캡처하기 때문에 모든 데이터 활동을 모니터링할 수 없음.

◆ | **Q#0253.** | **Ref#0253.**
최근 한 엔터테인먼트 회사에서 새로운 게임을 출시했습니다. 출시 기간 동안 플레이어에게 좋은 경험을 보장하기 위해 회사는 Network Load Balancer 뒤에 12개의 r6g.16xlarge(메모리 최적화) Amazon EC2 인스턴스를 정적으로 배포했습니다. 회사의 운영 팀은 Amazon CloudWatch 에이전트와 사용자 지정 지표를 사용하여 모니터링 전략에 메모리 사용률을 포함시켰습니다.

출시 기간의 CloudWatch 지표를 분석한 결과 회사가 예상한 CPU 및 메모리의 약 4분의 1 정도의 소비가 나타났습니다. 게임에 대한 초기 수요가 줄어들고 변동성이 더욱 커졌습니다. 회사는 인스턴스 집합을 동적으로 확장하기 위해 CPU 및 메모리 소비를 모니터링하는 Auto Scaling 그룹을 사용하기로 결정했습니다. 솔루션 아키텍트는 가장 비용 효율적인 방법으로 수요를 충족하도록 Auto Scaling 그룹을 구성해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. c6g.4xlarge(컴퓨팅 최적화) 인스턴스를 배포하도록 Auto Scaling 그룹을 구성합니다. 최소 용량 3, 원하는 용량 3, 최대 용량 12를 구성합니다.
B. m6g.4xlarge(범용) 인스턴스를 배포하도록 Auto Scaling 그룹을 구성합니다. 최소 용량 3, 원하는 용량 3, 최대 용량 12를 구성합니다.

C. r6g.4xlarge(메모리 최적화) 인스턴스를 배포하도록 Auto Scaling 그룹을 구성합니다. 최소 용량 3, 원하는 용량 3, 최대 용량 12를 구성합니다.
D. r6g.8xlarge(메모리 최적화) 인스턴스를 배포하도록 Auto Scaling 그룹을 구성합니다. 최소 용량 2, 원하는 용량 2, 최대 용량 6을 구성합니다.

해설
정답: C
새로운 게임은 메모리 최적화 인스턴스(r6g.16xlarge)에서 실행되고 있지만 CPU와 메모리의 약 1/4만 활용하고 있습니다.
따라서 r6g.16xlarge 인스턴스의 1/4을 제공하는 더 작은 인스턴스(r6g.4xlarge)를 사용하는 것이 비용 효율적입니다.

◆ | **Q#0254.** | **Ref#0254.**
금융 서비스 회사는 수백만 건의 과거 주식 거래를 Amazon DynamoDB 테이블에 로드했습니다. 테이블은 주문형 용량 모드를 사용합니다. 매일 자정에 한 번씩 수백만 개의 새로운 레코드가 테이블에 로드됩니다. 테이블에 대한 애플리케이션 읽기 활동은 하루 종일 폭발적으로 발생합니다. 제한된 키 세트가 반복적으로 조회됩니다. 회사는 DynamoDB와 관련된 비용을 절감해야 합니다.

이 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 전략을 권장해야 합니까?

A. DynamoDB 테이블 앞에 Amazon ElastiCache 클러스터 배포
B. DynamoDB Accelerator(DAX)를 배포합니다. DynamoDB Auto Scaling을 구성합니다. Cost Explorer에서 Savings Plan을 구매하세요.
C. 프로비저닝된 용량 모드를 사용합니다. Cost Explorer에서 Savings Plan을 구매하세요.
D. DynamoDB Accelerator(DAX)를 배포합니다. 프로비저닝된 용량 모드를 사용합니다. DynamoDB Auto Scaling을 구성합니다.

해설
정답: D
반복 조회 = DAX 버스트 방지 = 프로비저닝된 용량
DynamoDB Accelerator(DAX): Amazon DynamoDB의 성능을 향상시키기 위한 AWS에서 제공하는 인 메모리 캐싱 서비스, 읽기 지연 시간을 줄이고 자주 액세스하는 데이터에 대한 읽기 처리량을 향상시킴.
이는 애플리케이션과 DynamoDB 간의 캐싱 계층 역할을 하여 자주 액세스하는 데이터에 대해 DynamoDB 서비스에 직접 액세스할 필요성을 줄여 읽기 비용을 줄일 수 있음.
프로비저닝된 용량 모드: 주문형 용량 모드를 사용하면 사전 계획이 필요하지 않지만 예측 가능한 워크로드가 있는 애플리케이션의 경우 비용이 많이 들 수 있습니다.
프로비저닝된 용량을 사용하면 하루 동안 필요한 최소 및 최대 용량을 지정하여 더 나은 비용 최적화 및 예측 가능성을 얻을 수 있습니다.
DynamoDB Auto Scaling: 실제 사용 패턴에 따라 프로비저닝된 용량을 자동으로 조정하여 사용량이 많은 시간에는 테이블의 용량이 충분하고 사용량이 적은 시간에는 리소스 낭비를 방지하여 비용을 절감할 수 있음.

◆ | **Q#0255.** | **Ref#0255.**
한 회사는 수백 개의 AWS 계정에서 로그를 수신하고 분석하는 Amazon EC2에서 실행되는 중앙 집중식 로깅 서비스를 만들고 있습니다. AWS PrivateLink는 클라이언트 서비스와 로깅 서비스 간의 연결을 제공하는 데 사용됩니다.

클라이언트가 있는 각 AWS 계정에는 로깅 서비스를 위한 인터페이스 엔드포인트가 생성되어 사용할 수 있습니다. NLB(Network Load Balancer)를 사용하여 EC2 인스턴스에서 실행되는 로깅 서비스는 다른 서브넷에 배포됩니다. 클라이언트는 VPC 엔드포인트를 사용하여 로그를 제출할 수 없습니다.

이 문제를 해결하기 위해 솔루션 아키텍트가 수행해야 하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. NLB 서브넷과의 통신을 허용하려면 NACL이 로깅 서비스 서브넷에 연결되어 있는지 확인하십시오. EC2 인스턴스에서 실행되는 로깅 서비스 서브넷과의 통신을 허용하려면 NACL이 NLB 서브넷에 연결되어 있는지 확인하십시오.
B. NACL이 로깅 서비스 서브넷에 연결되어 인터페이스 엔드포인트 서브넷과의 통신을 허용하는지 확인합니다. EC2 인스턴스에서 실행되는 로깅 서비스 서브넷과의 통신을 허용하려면 인터페이스 엔드포인트 서브넷에 NACL이 연결되어 있는지 확인하세요.
C. EC2 인스턴스에서 실행 중인 로깅 서비스에 대한 보안 그룹을 확인하여 NLB 서브넷으로부터의 수신을 허용하는지 확인합니다.
D. EC2 인스턴스에서 실행되는 로깅 서비스의 보안 그룹을 확인하여 클라이언트로부터의 수신을 허용하는지 확인하세요.
E. NLB의 보안 그룹을 확인하여 인터페이스 엔드포인트 서브넷으로부터의 수신을 허용하는지 확인하십시오.

해설
정답: A,C

A. 로깅 서비스 서브넷에 NACL이 NLB 서브넷과 통신을 허용하도록 구성되어야 하며, NLB 서브넷에 NACL이 로깅 서비스 EC2 인스턴스 서브넷과 통신을 허용하도록 구성되어야 합니다.
이 조치는 서브넷 간의 통신을 보장하기 위해 필요합니다.
C. EC2 인스턴스에서 실행 중인 로깅 서비스의 보안 그룹을 확인하여 NLB 서브넷으로부터의 인바운드를 허용하는지 확인해야 합니다. 이 조치는 NLB 네트워크 통신을 허용하기 위해 필요합니다.
따라서, A와 C 조치 조합이 필요한 이유는 서브넷 간의 통신 및 네트워크 보안을 강화하여 문제를 해결하기 위해서입니다.

◆ | **Q#0256.** | **Ref#0256.**
한 회사의 Amazon S3 버킷에 수백만 개의 객체가 있습니다. 객체는 S3 Standard 스토리지 클래스에 있습니다. 모든 S3 객체는 자주 액세스됩니다. 개체에 액세스하는 사용자와 애플리케이션의 수가 빠르게 증가하고 있습니다. 객체는 AWS KMS 키(SSE-KMS)를 사용한 서버 측 암호화로 암호화됩니다.

솔루션 아키텍트는 회사의 월별 AWS 송장을 검토한 후 Amazon S3의 요청 수가 많아 AWS KMS 비용이 증가하고 있음을 확인했습니다. 솔루션 설계자는 애플리케이션 변경을 최소화하면서 비용을 최적화해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 고객 제공 키(SSE-C)를 암호화 유형으로 사용하여 서버 측 암호화를 사용하는 새 S3 버킷을 생성합니다. 기존 객체를 새 S3 버킷에 복사합니다. SSE-C를 지정합니다.
B. Amazon S3 관리형 키(SSE-S3)를 암호화 유형으로 사용하여 서버 측 암호화를 사용하는 새 S3 버킷을 생성합니다. S3 배치 작업을 사용하여 기존 객체를 새 S3 버킷에 복사합니다. SSE-S3을 지정합니다.
C. AWS CloudHSM을 사용하여 암호화 키를 저장합니다. 새 S3 버킷을 생성합니다. S3 배치 작업을 사용하여 기존 객체를 새 S3 버킷에 복사합니다. CloudHSM의 키를 사용하여 객체를 암호화합니다.
D. S3 버킷에는 S3 Intelligent-Tiering 스토리지 클래스를 사용하십시오. 90일 동안 액세스하지 않은 객체를 S3 Glacier Deep Archive로 전환하려면 S3 Intelligent-Tiering 아카이브 구성을 생성하세요.

해설
정답: B

암호화 방법을 AWS Key Management Service(AWS KMS) 사용에서 S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화 사용으로 전환합니다.
AWS KMS는 API 요청당 요금을 부과하는 반면, SSE-S3에는 S3 사용량 외에 API 요청당 추가 요금이 부과되지 않으므로 이러한 변경으로 인해 비용이 크게 절감될 수 있습니다.

◆ | **Q#0257.** | **Ref#0257.**
미디어 스토리지 애플리케이션은 AWS Lambda 함수에서 처리할 수 있도록 사용자 사진을 Amazon S3에 업로드합니다. 애플리케이션 상태는 Amazon DynamoDB 테이블에 저장됩니다. 업로드된 일부 사진이 제대로 처리되지 않는다는 사용자들의 신고가 접수되었습니다. 애플리케이션 개발자는 로그를 추적하여 수천 명의 사용자가 동시에 사진을 업로드할 때 Lambda에 사진 처리 문제가 발생하고 있음을 발견했습니다. 문제는 Lambda 동시성 제한과 데이터 저장 시 DynamoDB의 성능으로 인해 발생합니다.

솔루션 아키텍트는 애플리케이션의 성능과 안정성을 높이기 위해 어떤 조치 조합을 취해야 합니까? (2개를 선택하세요.)

> **A.** DynamoDB 테이블의 RCU를 평가하고 조정합니다.
> **B.** DynamoDB 테이블의 WCU를 평가하고 조정합니다.
> **C.** Amazon ElastiCache 계층을 추가하여 Lambda 함수의 성능을 높입니다.
> **D.** Amazon S3와 Lambda 함수 사이에 Amazon Simple Queue Service(Amazon SQS) 대기열 및 재처리 로직을 추가합니다.
> **E.** S3 Transfer Acceleration을 사용하여 사용자에게 더 짧은 지연 시간을 제공합니다.
>
> 해설
> 정답: B,D
>
> B. DynamoDB 테이블의 WCU를 평가하고 조정하면 데이터 저장 시 DynamoDB 테이블의 성능을 향상시키는 데 도움이 됩니다.
> D. Amazon S3와 Lambda 함수 사이에 Amazon SQS 대기열을 추가하고 실패시 재처리 로직을 추가하면 S3 이벤트 발생시 Lambda 함수가 사진을 안정적으로 처리할 수 있게 됩니다.
> 이는 Lambda 기능의 성능을 향상시키고 사진이 제대로 처리되지 않을 위험을 줄이는 데 도움이 됩니다.

◆ | **Q#0258.** | **Ref#0258.**
회사는 온프레미스 데이터 센터에서 애플리케이션을 실행합니다. 이 애플리케이션은 사용자에게 미디어 파일을 업로드할 수 있는 기능을 제공합니다. 파일은 파일 서버에 유지됩니다. 웹 애플리케이션에는 많은 사용자가 있습니다. 애플리케이션 서버가 과도하게 사용되어 가끔 데이터 업로드가 실패합니다. 회사에서는 파일 서버에 새로운 스토리지를 자주 추가합니다. 회사는 애플리케이션을 AWS로 마이그레이션하여 이러한 문제를 해결하려고 합니다.

미국과 캐나다 전역의 사용자가 애플리케이션에 액세스합니다. 인증된 사용자만 애플리케이션에 액세스하여 파일을 업로드할 수 있어야 합니다. 회사는 애플리케이션을 리팩터링하는 솔루션을 고려할 것이며 회사는 애플리케이션 개발을 가속화해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** AWS Application Migration Service를 사용하여 애플리케이션 서버를 Amazon EC2 인스턴스로 마이그레이션하십시오. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. Application Load Balancer를 사용하여 요청을 분산합니다. Amazon S3를 사용하여 파일을 유지하도록 애플리케이션을 수정합니다. Amazon Cognito를 사용하여 사용자를 인증합니다.
> **B.** AWS Application Migration Service를 사용하여 애플리케이션 서버를 Amazon EC2 인스턴스로 마이그레이션합니다. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. Application Load Balancer를 사용하여 요청을 분산합니다. 사용자가 애플리케이션에 로그인할 수 있도록 AWS IAM Identity Center(AWS Single Sign-On)를 설정합니다. Amazon S3를 사용하여 파일을 유지하도록 애플리케이션을 수정합니다.
> **C.** 미디어 파일 업로드를 위한 정적 웹사이트를 만듭니다. Amazon S3에 정적 자산을 저장합니다. AWS AppSync를 사용하여 API를 생성합니다. AWS Lambda 해석기를 사용하여 미디어 파일을 Amazon S3에 업로드합니다. Amazon Cognito를 사용하여 사용자를 인증합니다.
> **D.** AWS Amplify를 사용하여 미디어 파일 업로드를 위한 정적 웹사이트를 생성합니다. Amplify

Hosting을 사용하여 Amazon CloudFront를 통해 웹 사이트를 제공하십시오. Amazon S3를 사용하여 업로드된 미디어 파일을 저장합니다. Amazon Cognito를 사용하여 사용자를 인증합니다.

해설
정답: D

Amplify는 더 쉬운 개발 환경을 제공하고 파일 저장을 위한 Amazon S3 및 사용자 인증을 위한 Amazon Cognito와의 통합을 지원합니다.
확장성, 안정성 및 사용자 인증을 보장하면서 간소화된 개발 프로세스를 제공
AWS Amplify는 프런트엔드 웹 및 모바일 개발자가 AWS에서 풀 스택 애플리케이션을 쉽게 구축, 제공 및 호스팅할 수 있게 해주는 완벽한 솔루션

◆ | **Q#0259.** | **Ref#0259.**
회사에는 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스에 배포된 애플리케이션이 있습니다. 인스턴스는 Auto Scaling 그룹의 일부입니다. 애플리케이션에는 예측할 수 없는 워크로드가 있고 확장 및 축소가 자주 발생합니다. 회사의 개발 팀은 애플리케이션 로그를 분석하여 애플리케이션 성능을 향상시킬 수 있는 방법을 찾으려고 합니다. 그러나 인스턴스 축소 후에는 더 이상 로그를 사용할 수 없습니다.

축소 이벤트 후 개발 팀이 애플리케이션 로그를 볼 수 있는 기능을 제공하는 솔루션은 무엇입니까?

A. ALB에 대한 액세스 로그를 활성화합니다. Amazon S3 버킷에 로그를 저장합니다.
B. 통합 CloudWatch 에이전트를 사용하여 Amazon CloudWatch Logs에 로그를 게시하도록 EC2 인스턴스를 구성합니다.
C. 단계 조정 정책을 사용하도록 Auto Scaling 그룹을 수정합니다.
D. AWS X-Ray 추적을 사용하여 애플리케이션을 계측합니다.

해설
정답: B

질문에는 개발 팀이 애플리케이션 로그를 분석하려고 하는데 EC2 인스턴스가 축소된 후에 이러한 로그가 사라진다는 내용이 나와 있습니다. 이 문제를 해결하려면 통합 CloudWatch 에이전트를 사용하여 로그를 Amazon CloudWatch Logs로 보내도록 EC2 인스턴스를 구성할 수 있습니다. 이를 통해 로그를 장기간 보관할 수 있으며 개발팀은 인스턴스가 종료된 후에도 언제든지 로그를 분석할 수 있습니다.

◆ | **Q#0260.** | **Ref#0260.**
한 회사에서 사용자 등록 양식이 포함된 인증되지 않은 정적 웹사이트(www.example.com)를 운영하고 있습니다. 웹 사이트는 호스팅에 Amazon S3를 사용하고 AWS WAF가 구성된 콘텐츠 전송 네트워크로 Amazon CloudFront를 사용합니다. 등록 양식이 제출되면 웹 사이트는 AWS Lambda 함수를 호출하여 페이로드를 처리하고 페이로드를 외부 API 호출로 전달하는 Amazon API Gateway API 엔드포인트를 호출합니다.

테스트 중에 솔루션 설계자에게 CORS(교차 원본 리소스 공유) 오류가 발생했습니다. 솔루션 설계자는 CloudFront 배포 오리진에 www.example.com으로 설정된 Access-Control-Allow-Origin 헤더가 있는지 확인합니다.

솔루션 설계자는 오류를 해결하기 위해 무엇을 해야 합니까?

A. S3 버킷의 CORS 구성을 변경합니다. www.example.com의 AllowedOrigin 요소에 CORS에 대한 규칙을 추가합니다.
B. AWS WAF에서 CORS 설정을 활성화합니다. Access-Control-Allow-Origin 헤더가 www.example.com으로 설정된 웹 ACL 규칙을 생성합니다.
C. API 게이트웨이 API 엔드포인트에서 CORS 설정을 활성화합니다. Access-Control-Allow-Origin 헤더가 www.example.com으로 설정된 모든 응답을 반환하도록 API 엔드포인트가 구성되어 있는지 확인하세요.

D. Lambda 함수에서 CORS 설정을 활성화합니다. 함수의 반환 코드에 Access-Control-Allow-Origin 헤더가 www.example.com으로 설정되어 있는지 확인하세요.

해설
정답: C

다른 원본에서 API 게이트웨이 엔드포인트를 호출하면 API 게이트웨이는 요청이 확인된 원본에서 오는지 확인할 수 있어야 하므로 API 게이트웨이에서 CORS를 활성화하고 웹사이트 원본을 확인된 원본 목록에 추가해야 합니다.

261 (황호실) 2회차 完

◆ | **Q#0261.** | **Ref#0261.**
회사에는 별도의 AWS 계정이 많이 있으며 중앙 청구 또는 관리를 사용하지 않습니다. 각 AWS 계정은 회사의 다양한 부서를 위한 서비스를 호스팅합니다. 회사에는 배포된 Microsoft Azure Active Directory가 있습니다.

솔루션 아키텍트는 회사의 AWS 계정에 대한 청구 및 관리를 중앙 집중화해야 합니다. 회사는 수동 사용자 관리 대신 ID 페더레이션을 사용하기를 원합니다. 또한 회사는 수명이 긴 액세스 키 대신 임시 자격 증명을 사용하려고 합니다.

이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. 마스터 계정 역할을 할 새 AWS 계정을 생성합니다. AWS Organizations에 조직을 배포합니다. 각 기존 AWS 계정을 초대하여 조직에 가입하십시오. 각 계정이 초대를 수락하는지 확인하세요.
B. 각 AWS 계정의 이메일 주소를 aws+로 구성합니다.@example.com을 사용하면 계정 관리 이메일 메시지와 청구서가 같은 곳으로 전송됩니다.
C. 마스터 계정에 AWS IAM Identity Center(AWS Single Sign-On)를 배포합니다. IAM ID 센터를 Azure Active Directory에 연결합니다. 사용자 및 그룹의 자동 동기화를 위해 IAM ID 센터를 구성합니다.
D. 마스터 계정에 AWS Managed Microsoft AD 디렉터리를 배포합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 조직의 다른 모든 계정과 디렉터리를 공유합니다.
E. AWS IAM Identity Center(AWS Single Sign-On) 권한 세트를 생성합니다. 적절한 IAM Identity Center 그룹 및 AWS 계정에 권한 세트를 연결합니다.
F. 인증 및 승인을 위해 AWS Managed Microsoft AD를 사용하도록 각 AWS 계정에서 AWS Identity and Access Management(IAM)를 구성합니다.

해설
정답: ACE
A: 새로운 AWS 계정을 생성하여 마스터 계정으로 설정, AWS Organizations 에서 조직을 배포하고 각 기존 계정들을 초대하여 조직에 가입, 초대수락 확인.
C: AWS IAM Identity Center(AWS Single Sign-On)를 Azure Active Directory에 연결하고, 사용자와 그룹의 자동 동기화 설정.
E: AWS IAM Identity Center(AWS Single Sign-On) 권한 세트 생성, 적절한 AWS IAM IC그룹과 AWS 계정에 권한세트 연결.

◆ | **Q#0262.** | **Ref#0262.**
한 회사는 자주 사용되지 않지만 여전히 비즈니스에 중요한 애플리케이션 20개 그룹과 관련된 비용을 AWS로 마이그레이션하여 관리하려고 합니다. 애플리케이션은 다양한 인스턴스 클러스터에 분산된 Java와 Node.js가 혼합되어 있습니다. 회사는 단일 배포 방법을 사용하여 표준화하는 동시에 비용을 최소화하려고 합니다.

대부분의 애플리케이션은 동시 사용자 수가 적은 월말 처리 루틴의 일부이지만 가끔 다른 시간에 실행됩니다. 평균 애플리케이션 메모리 소비량은 1GB 미만입니다. 일부 응용 프로그램은 최대 처리 중에 최대 2.5GB의 메모리를

사용합니다. 그룹에서 가장 중요한 애플리케이션은 여러 데이터 소스에 액세스하고 종종 몇 시간 동안 실행되는 Java로 작성된 청구 보고서입니다.

가장 비용 효율적인 솔루션은 무엇입니까?

> **A.** 각 애플리케이션에 대해 별도의 AWS Lambda 함수를 배포하십시오. AWS CloudTrail 로그와 Amazon CloudWatch 경보를 사용하여 중요한 작업의 완료를 확인하세요.
> **B.** 75%의 메모리 사용률로 구성된 Auto Scaling을 사용하여 Amazon EC2에 Amazon ECS 컨테이너를 배포합니다. ECS 작업 확장을 통해 마이그레이션되는 각 애플리케이션에 대해 ECS 작업을 배포합니다. Amazon CloudWatch를 사용하여 서비스와 호스트를 모니터링합니다.
> **C.** Auto Scaling을 사용하여 각 애플리케이션에 대해 AWS Elastic Beanstalk를 배포하여 모든 요청에 충분한 리소스가 있는지 확인합니다. CloudWatch 경보를 사용하여 각 AWS Elastic Beanstalk 배포를 모니터링합니다.
> **D.** EC2 Auto Scaling 및 Application Load Balancer를 사용하여 모든 애플리케이션을 공동 호스팅하는 새로운 Amazon EC2 인스턴스 클러스터를 배포합니다. 인스턴스 메모리 사용률에 설정된 사용자 지정 지표를 기반으로 클러스터 크기를 확장합니다. Auto Scaling 그룹의 GroupMaxSize 파라미터와 동일한 3년 예약 인스턴스 예약을 구매합니다.
>
> 해설
> 정답: B
> B: 메모리 사용률을 기준으로 Auto Scaling을 설정하여 사용량에 따라 동적으로 리소스를 할당하여 필요할 때만 리소스를 사용하게 하여 비용을 절감
> ECS 작업을 사용하여 각 애플리케이션을 개별적으로 관리할 수 있으며, Amazon CloudWatch를 통해 서비스와 호스트를 모니터링하여 성능을 유지할 수 있음.
> A(x): 실행 시간이 긴 애플리케이션(예: 청구 보고서)에 Lambda는 적합하지 않음.
> C(x): Elastic Beanstalk을 사용하여 Application을 독립적으로 배포하고 모니터링 하는 것은 관리의 복잡성 및 비용 증가.
> D(x): 새로운 EC2 인스턴스 클러스터를 사용하여 모든 애플리케이션을 호스팅 => 전체 클러스터 크기를 미리 정해야 하므로 비효율적인 리소스 사용과 높은 비용 발생.
> B: Auto Scaling을 사용하여 리소스를 효율적으로 활용하고, Amazon ECS를 사용하여 컨테이너화된 애플리케이션을 관리하며,
> CloudWatch를 사용하여 모니터링하므로 비용을 최소화하면서 효율적인 운영이 가능합니다.
>
> 메모리 사용률에 기반한 Auto Scaling과 ECS 작업 확장을 사용하는 옵션 B가 가장 비용 효율적인 솔루션

◆ | Q#0263. | Ref#0263.
솔루션 아키텍트는 EMRFS(EMR 파일 시스템)를 사용하는 Amazon EMR 클러스터의 설계를 검토해야 합니다. 클러스터는 비즈니스 요구에 중요한 작업을 수행합니다. 클러스터는 모든 작업, 기본 및 코어 노드에 대해 항상 Amazon EC2 온디맨드 인스턴스를 실행하고 있습니다. EMR 작업은 매일 아침 오전 1시부터 실행됩니다. 실행을 완료하는 데 6시간이 걸립니다. 하루 늦게까지 데이터가 참조되지 않기 때문에 처리를 완료하는 데 걸리는 시간은 우선순위가 아닙니다.

솔루션 설계자는 아키텍처를 검토하고 컴퓨팅 비용을 최소화할 수 있는 솔루션을 제안해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 솔루션을 권장해야 합니까?

> **A.** 인스턴스 집합의 스팟 인스턴스에서 모든 작업, 기본 및 코어 노드를 시작합니다. 처리가 완료되면 모든 인스턴스를 포함하여 클러스터를 종료합니다.
> **B.** 온디맨드 인스턴스에서 기본 및 핵심 노드를 시작합니다. 인스턴스 집합의 스팟 인스턴스에서 작업 노드를 시작합니다. 처리가 완료되면 모든 인스턴스를 포함하여 클러스터를 종료합니다. 온디맨드 인스턴스 사용량을 충당하려면 Compute Savings Plan을 구매하세요.
> **C.** 온디맨드 인스턴스에서 모든 노드를 계속 시작합니다. 처리가 완료되면 모든 인스턴스를 포함하

여 클러스터를 종료합니다. 온디맨드 인스턴스 사용량을 충당하려면 Compute Savings Plan을 구매하세요.
D. 온디맨드 인스턴스에서 기본 및 핵심 노드를 시작합니다. 인스턴스 집합의 스팟 인스턴스에서 작업 노드를 시작합니다. 처리가 완료되면 작업 노드 인스턴스만 종료합니다. 온디맨드 인스턴스 사용량을 충당하려면 Compute Savings Plan을 구매하세요.

해설
정답: D
D: 비용 절감을 위해 작업 노드를 Spot 인스턴스로 시작하면서도, 기본 및 코어 노드를 On-Demand 인스턴스로 유지하여 안정성을 보장
On-Demand 인스턴스 사용량을 커버하기 위해 Compute Savings Plans를 구매하여 추가적인 비용 절감
B(x): 이미 저축 플랜을 구매했다면 기본 인스턴스를 종료하는 것은 의미가 없습니다. 전체 스택을 종료하더라도 요금이 청구됩니다.

◆ | **Q#0264.** | **Ref#0264.**
한 회사가 레거시 애플리케이션을 AWS 클라우드로 마이그레이션했습니다. 애플리케이션은 3개의 가용 영역에 분산된 3개의 Amazon EC2 인스턴스에서 실행됩니다. 각 가용 영역에는 하나의 EC2 인스턴스가 있습니다. EC2 인스턴스는 VPC의 프라이빗 서브넷 3개에서 실행 중이며 퍼블릭 서브넷 3개와 연결된 ALB(Application Load Balancer)의 대상으로 설정됩니다.

애플리케이션은 온프레미스 시스템과 통신해야 합니다. 회사의 IP 주소 범위에 있는 IP 주소의 트래픽만 온프레미스 시스템에 액세스할 수 있습니다. 회사의 보안팀은 내부 IP 주소 범위에서 IP 주소 하나만 클라우드로 가져오고 있습니다. 회사는 이 IP 주소를 회사 방화벽의 허용 목록에 추가했습니다. 회사에서는 이 IP 주소에 대한 탄력적 IP 주소도 생성했습니다.

솔루션 설계자는 애플리케이션이 온프레미스 시스템과 통신할 수 있는 기능을 제공하는 솔루션을 만들어야 합니다. 또한 솔루션은 오류를 자동으로 완화할 수 있어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 각 퍼블릭 서브넷에 하나씩 세 개의 NAT 게이트웨이를 배포합니다. NAT 게이트웨이에 탄력적 IP 주소를 할당합니다. NAT 게이트웨이에 대한 상태 확인을 활성화합니다. NAT 게이트웨이가 상태 확인에 실패하면 NAT 게이트웨이를 다시 생성하고 탄력적 IP 주소를 새 NAT 게이트웨이에 할당합니다.
B. ALB를 NLB(Network Load Balancer)로 교체합니다. NL에 대한 상태 확인 켜기에 탄력적 IP 주소를 할당합니다. 상태 확인이 실패한 경우 NLB를 다른 서브넷에 다시 배포합니다.
C. 퍼블릭 서브넷에 단일 NAT 게이트웨이를 배포합니다. NAT 게이트웨이에 탄력적 IP 주소를 할당합니다. 사용자 지정 지표와 함께 Amazon CloudWatch를 사용하여 NAT 게이트웨이를 모니터링합니다. NAT 게이트웨이가 비정상인 경우 AWS Lambda 함수를 호출하여 다른 서브넷에 새 NAT 게이트웨이를 생성하십시오. 새 NAT 게이트웨이에 탄력적 IP 주소를 할당합니다.
D. 탄력적 IP 주소를 ALB에 할당합니다. 탄력적 IP 주소를 값으로 사용하여 Amazon Route 53 단순 레코드를 생성합니다. Route 53 상태 확인을 생성합니다. 상태 확인에 실패한 경우 다른 서브넷에 ALB를 다시 생성하십시오.

해설
정답: C
하나의 NAT 게이트웨이를 사용하여 Elastic IP 주소를 할당하면 비용을 절감할 수 있음.
또한, Amazon CloudWatch와 사용자 지정 메트릭을 사용하여 NAT 게이트웨이를 모니터링하고, 문제가 발생할 경우 AWS Lambda 함수를 통해 다른 서브넷에 새로운 NAT 게이트웨이를 생성하고 Elastic IP 주소를 할당하면 자동으로 장애를 완화할 수 있음.
이 방식은 관리 효율성과 자동 복구 기능을 모두 갖추고 있습니다.

◆ | **Q#0265.** | **Ref#0265.**
한 회사는 AWS Organizations를 사용하여 1,000개가 넘는 AWS 계정을 관리합니다. 회사는 새로운 개발자 조직을 만들었습니다. 새로운 개발자 조직으로 이동해야 하는 개발자 회원 계정은 540개입니다. 모든 계정은 각 계정이 독립형 계정으로 운영될 수 있도록 필요한 모든 정보로 설정됩니다.

모든 개발자 계정을 새로운 개발자 조직으로 이동하려면 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** 이전 조직의 마스터 계정에서 Organizations API의 MoveAccount 작업을 호출하여 개발자 계정을 새 개발자 조직으로 마이그레이션합니다.
> **B.** 마스터 계정에서 조직 API의 RemoveAccountFromOrganization 작업을 사용하여 이전 조직에서 각 개발자 계정을 제거합니다.
> **C.** 각 개발자 계정에서 Organizations API의 RemoveAccountFromOrganization 작업을 사용하여 이전 조직에서 계정을 제거합니다.
> **D.** 새로운 개발자 조직의 마스터 계정에 로그인하고 개발자 계정 마이그레이션의 대상 역할을 하는 자리 표시자 회원 계정을 생성합니다.
> **E.** 새로운 개발자 조직의 마스터 계정에서 Organizations API의 InviteAccountToOrganization 작업을 호출하여 개발자 계정에 초대를 보냅니다.
> **F.** 각 개발자가 자신의 계정에 로그인하고 새 개발자 조직에 가입했는지 확인하도록 합니다.
>
> 해설
> 정답: BEF
> B: 이전 조직의 마스터 계정에서 RemoveAccountFromOrganization 작업을 호출하여 개발자 계정을 이전 조직에서 제거하면 개발자 계정이 독립적인 상태가 됨.
> E: 새로운 개발자 조직의 관리 계정에서 InviteAccountToOrganization 작업을 호출하여 개발자 계정으로 초대장을 보냄.
> F: 각 개발자가 자신의 계정에 로그인하여 새로운 조직에 가입하는 초대를 수락하고 확인.

◆ | **Q#0266.** | **Ref#0266.**
회사의 대화형 웹 애플리케이션은 Amazon CloudFront 배포를 사용하여 Amazon S3 버킷의 이미지를 제공합니다. 때때로 타사 도구가 손상된 이미지를 S3 버킷으로 수집합니다. 이러한 이미지 손상으로 인해 나중에 애플리케이션에서 사용자 경험이 저하됩니다. 회사는 손상된 이미지를 감지하기 위해 Python 논리를 성공적으로 구현하고 테스트했습니다.

솔루션 설계자는 수집과 제공 사이의 대기 시간을 최소화하면서 감지 논리를 통합하는 솔루션을 권장해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 최종 사용자 응답 이벤트에 의해 호출되는 Lambda@Edge 함수를 사용하십시오.
> **B.** 오리진-응답 이벤트에 의해 호출되는 Lambda@Edge 함수를 사용하십시오.
> **C.** AWS Lambda 함수를 호출하는 S3 이벤트 알림을 사용하십시오.
> **D.** AWS Step Functions 상태 시스템을 호출하는 S3 이벤트 알림을 사용하십시오.
>
> 해설
> 정답: C
> S3 이벤트 알림을 사용하여 객체가 S3 버킷에 업로드될 때 AWS Lambda 함수를 호출할 수 있음.
> 이를 통해 이미지가 업로드될 때마다 손상 여부를 즉시 검사할 수 있으며, 지연을 최소화하면서 손상된 이미지를 감지.
> Lambda 함수는 이미지가 손상된 경우 적절한 조치를 취할 수 있음.

◆ | **Q#0267.** | **Ref#0267.**
회사에는 Amazon EC2 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 실행되는 애플리케이션이 있습니다. 회사는 AWS CodePipeline을 사용하여 애플리케이션을 배포합니다. Auto Scaling 그룹에서 실행되는 인스턴스는 조정 이벤트로 인해 지속적으로 변경됩니다.

회사가 새 애플리케이션 코드 버전을 배포할 때 회사는 새 대상 EC2 인스턴스에 AWS CodeDeploy 에이전트를 설치하고 인스턴스를 CodeDeploy 배포 그룹과 연결합니다. 애플리케이션은 앞으로 24시간 이내에 게시되도록 설정되어 있습니다.

최소한의 운영 오버헤드로 애플리케이션 배포 프로세스를 자동화하기 위해 솔루션 설계자가 권장해야 하는 것은 무엇입니까?

> **A.** 새로운 EC2 인스턴스가 Auto Scaling 그룹으로 시작될 때 AWS Lambda 함수를 호출하도록 Amazon EventBridge를 구성합니다. EC2 인스턴스를 CodeDeploy 배포 그룹과 연결하도록 Lambda 함수를 코딩합니다.
> **B.** 새 코드를 배포하기 전에 Amazon EC2 Auto Scaling 작업을 일시 중지하는 스크립트를 작성합니다. 배포가 완료되면 새 AMI를 생성하고 새 시작에 새 AMI를 사용하도록 Auto Scaling 그룹의 시작 템플릿을 구성합니다. Amazon EC2 Auto Scaling 작업을 재개합니다.
> **C.** 새 코드가 포함된 새 AMI를 생성하는 새 AWS CodeBuild 프로젝트를 생성합니다. Auto Scaling 그룹의 시작 템플릿을 새 AMI로 업데이트하도록 CodeBuild를 구성합니다. Amazon EC2 Auto Scaling 인스턴스 새로 고침 작업을 실행합니다.
> **D.** CodeDeploy 에이전트가 설치된 새 AMI를 생성합니다. 새 AMI를 사용하도록 Auto Scaling 그룹의 시작 템플릿을 구성합니다. CodeDeploy 배포 그룹을 EC2 인스턴스 대신 Auto Scaling 그룹과 연결합니다.
>
> 해설
> 정답: D
> 핵심 요구사항:
> 변경 이벤트로 인해 EC2 인스턴스가 자주 바뀌는 Auto Scaling 그룹에서 새로운 애플리케이션 코드 버전을 자동으로 배포해야 합니다.
> 최소한의 운영 오버헤드로 이를 자동화할 수 있는 솔루션을 추천해야 합니다.
>
> CodeDeploy 에이전트가 사전 설치된 새로운 AMI를 생성하고, Auto Scaling 그룹의 시작 템플릿을 이 AMI로 구성하면 새로운 인스턴스가 자동으로 배포 그룹에 포함될 수 있음.
> 이 방법은 운영 오버헤드를 최소화하며, 새로운 코드 배포를 간소화합니다.
> CodeDeploy 배포 그룹을 Auto Scaling 그룹과 연결하면 CodeDeploy는 Auto Scaling 그룹에서 시작한 모든 새 인스턴스에 애플리케이션을 자동으로 배포합니다.

◆ | **Q#0268.** | **Ref#0268.**
ALB(Application Load Balancer) 뒤에 있는 4개의 Amazon EC2 인스턴스에서 실행되는 웹 사이트가 있는 회사가 있습니다. ALB가 EC2 인스턴스를 더 이상 사용할 수 없음을 감지하면 Amazon CloudWatch 경보가 ALARM 상태로 전환됩니다. 그런 다음 회사 운영 팀의 구성원이 ALB 뒤에 새 EC2 인스턴스를 수동으로 추가합니다.

솔루션 아키텍트는 EC2 인스턴스 교체를 자동으로 처리하는 고가용성 솔루션을 설계해야 합니다. 회사는 새로운 솔루션으로 전환하는 동안 가동 중지 시간을 최소화해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 수행해야 합니까?

> **A.** 기존 ALB를 삭제합니다. 웹 애플리케이션 트래픽을 처리하도록 구성된 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹에 새 시작 템플릿을 연결합니다. 새 ALB를 생성합니다. Auto Scaling 그룹을 새 ALB에 연결합니다. 기존 EC2 인스턴스를 Auto Scaling 그룹에 연결합니다.
> **B.** 웹 애플리케이션 트래픽을 처리하도록 구성된 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹에 새 시작 템플릿을 연결합니다. Auto Scaling 그룹을 기존 ALA에 연결합니다. 기존 EC2 인스턴스를 Auto Scaling 그룹에 연결합니다.
> **C.** 기존 ALB 및 EC2 인스턴스를 삭제합니다. 웹 애플리케이션 트래픽을 처리하도록 구성된 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹에 새 시작 템플릿을 연결합니다. 새 ALB를 생성합니다. Auto Scaling 그룹을 새 ALB에 연결합니다. Auto Scaling 그룹이 최소 수의 EC2 인스턴스를 시작

할 때까지 기다립니다.
D. 웹 애플리케이션 트래픽을 처리하도록 구성된 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹에 새 시작 템플릿을 연결합니다. 기존 ALB에 Auto Scaling 그룹을 연결합니다. 기존 ALB가 기존 EC2 인스턴스를 Auto Scaling 그룹에 등록할 때까지 기다립니다.

해설
정답: B
새로운 Auto Scaling 그룹을 생성하고, 웹 애플리케이션 트래픽을 처리하도록 설정합니다.
새로운 시작 템플릿을 Auto Scaling 그룹에 연결하고, Auto Scaling 그룹을 기존 ALB에 연결합니다.
기존 EC2 인스턴스를 Auto Scaling 그룹에 연결합니다.
이 방식은 최소한의 다운타임으로 고가용성 솔루션을 제공합니다. 기존 ALB와 인스턴스를 유지하면서 Auto Scaling 그룹을 구성할 수 있습니다.

◆ | **Q#0269.** | **Ref#0269.**
회사는 AWS Organizations의 회사 조직 내 개발자 계정 전체에서 AWS 데이터 전송 비용과 컴퓨팅 비용을 최적화하려고 합니다. 개발자는 단일 AWS 리전에서 VPC를 구성하고 Amazon EC2 인스턴스를 시작할 수 있습니다. EC2 인스턴스는 Amazon S3에서 매일 약 1TB의 데이터를 검색합니다.

개발자 활동으로 인해 EC2 인스턴스와 S3 버킷 간의 과도한 월별 데이터 전송 요금과 NAT 게이트웨이 처리 요금이 발생하고 컴퓨팅 비용도 높아집니다. 회사는 개발자가 AWS 계정 내에 배포하는 모든 EC2 인스턴스 및 VPC 인프라에 대해 승인된 아키텍처 패턴을 사전에 적용하기를 원합니다. 회사는 이러한 시행이 개발자가 작업을 수행할 수 있는 속도에 부정적인 영향을 미치는 것을 원하지 않습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 개발자가 승인되지 않은 EC2 인스턴스 유형을 시작하지 못하도록 SCP를 생성하십시오. 개발자에게 AWS CloudFormation 템플릿을 제공하여 S3 인터페이스 엔드포인트와 함께 승인된 VPC 구성을 배포합니다. 개발자가 CloudFormation을 통해서만 VPC 리소스를 시작할 수 있도록 개발자의 IAM 권한 범위를 지정합니다.
B. AWS 예산을 사용하여 일일 예측 예산을 생성하여 개발자 계정 전체의 EC2 컴퓨팅 비용과 S3 데이터 전송 비용을 모니터링합니다. 예상 비용이 실제 예산 비용의 75%이면 개발자팀에 알림을 보냅니다. 실제 예산 비용이 100%인 경우 개발자의 EC2 인스턴스 및 VPC 인프라를 종료하는 예산 작업을 생성합니다.
C. 사용자가 S3 게이트웨이 엔드포인트 및 승인된 EC2 인스턴스로 승인된 VPC 구성을 생성하는 데 사용할 수 있는 AWS Service Catalog 포트폴리오를 생성합니다. 개발자 계정과 포트폴리오를 공유하세요. 승인된 IAM 역할을 사용하도록 AWS Service Catalog 시작 제약 조건을 구성합니다. AWS Service Catalog에 대한 액세스만 허용하도록 개발자의 IAM 권한 범위를 지정합니다.
D. 개발자 AWS 계정에서 EC2 및 VPC 리소스의 규정 준수를 모니터링하기 위해 AWS Config 규칙을 생성하고 배포합니다. 개발자가 승인되지 않은 EC2 인스턴스를 시작하거나 개발자가 S3 게이트웨이 엔드포인트 없이 VPC를 생성하는 경우 수정 작업을 수행하여 승인되지 않은 리소스를 종료하십시오.

해설
핵심 요구사항:
- AWS 데이터 전송 및 컴퓨트 비용 최적화
- 승인된 아키텍처 패턴을 EC2 인스턴스와 VPC 인프라에 강제 적용
- 개발자 작업 속도에 부정적인 영향을 미치지 않도록 할 것

정답: C
서비스 카탈로그는 모든 문제를 해결합니다. S3 게이트웨이 엔드포인트는 AWS의 VPC에서 데이터를 전송하여 더욱 비용이 효율적입니다.
AWS 서비스 카탈로그를 통해 개발자에게 승인된 구성을 제공하면서 아키텍처 패턴을 강제하는 것

을 보장합니다.
또한 IAM 권한은 AWS 서비스 카탈로그에만 액세스할 수 있도록 제한되어 의도하지 않은 리소스 배포 가능성을 최소화합니다.
C는 개발자 생산성에 지장을 최소화하는 옵션

◆ | **Q#0270.** | **Ref#0270.**
회사가 확장되고 있습니다. 이 회사는 리소스를 여러 AWS 리전에 있는 수백 개의 서로 다른 AWS 계정으로 분리할 계획입니다. 솔루션 설계자는 특별히 지정된 지역 외부의 모든 작업에 대한 액세스를 거부하는 솔루션을 권장해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 각 계정에 대한 IAM 역할을 생성합니다. 계정에 대해 승인된 리전만 포함하는 조건부 허용 권한이 있는 IAM 정책을 생성합니다.
B. AWS Organizations에서 조직을 생성합니다. 각 계정에 대해 IAM 사용자를 생성합니다. 계정이 인프라를 배포할 수 없는 지역에 대한 액세스를 차단하려면 각 사용자에게 정책을 연결하세요.
C. AWS Control Tower 랜딩 존을 시작합니다. OU를 생성하고 승인된 지역 외부의 서비스 실행에 대한 액세스를 거부하는 SCP를 연결합니다.
D. 각 계정에서 AWS Security Hub를 활성화합니다. 계정이 인프라를 배포할 수 있는 지역을 지정하는 컨트롤을 만듭니다.

해설
정답:C
AWS Control Tower를 사용하면 승인된 리전 외의 서비스 실행 액세스를 거부하는 SCP를 사용하여 리전별 제한을 설정할 수 있습니다.
이는 회사가 다양한 AWS 리전과 계정을 관리하는 데 도움이 될 것입니다.
AWS Control Tower를 사용하여 SCP를 사용하여 리전별 액세스 제어를 강제함으로써 조직의 AWS 환경에서 리전 기반 권한 정책을 준수합니다.

271 (노종옥) 2회차 完

◆ | **Q#0271.** | **Ref#0271.**
한 회사는 현재 웹 호스팅, 데이터베이스 API 서비스 및 비즈니스 로직을 위해 로드 밸런싱된 Amazon EC2 인스턴스 집합이 있는 소매 주문 웹 애플리케이션을 리팩터링하려고 합니다. 회사는 실패한 주문을 유지하는 동시에 운영 비용을 최소화하기 위한 메커니즘을 갖춘 분리되고 확장 가능한 아키텍처를 만들어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 데이터베이스 API 서비스용 Amazon API Gateway를 사용한 웹 호스팅에는 Amazon S3를 사용하십시오. 주문 대기열에는 Amazon Simple Queue Service(Amazon SQS)를 사용합니다. 실패한 주문을 유지하기 위해 Amazon SQS 장기 폴링이 포함된 비즈니스 로직에 Amazon Elastic Container Service(Amazon ECS)를 사용하십시오.
B. 데이터베이스 API 서비스를 위해 Amazon API Gateway를 사용하여 웹 호스팅에 AWS Elastic Beanstalk를 사용하십시오. 주문 대기열에는 Amazon MQ를 사용합니다. 실패한 주문을 보관하려면 Amazon S3 Glacier Deep Archive와 함께 비즈니스 로직에 AWS Step Functions를 사용하세요.
C. 데이터베이스 API 서비스용 AWS AppSync를 사용한 웹 호스팅에 Amazon S3를 사용합니다. 주문 대기열에는 Amazon Simple Queue Service(Amazon SQS)를 사용합니다. 실패한 주문을 보관하기 위해 Amazon SQS 배달 못한 편지 대기열과 함께 비즈니스 로직에 AWS Lambda를 사용하십시오.
D. 데이터베이스 API 서비스를 위해 AWS AppSync를 사용한 웹 호스팅에 Amazon Lightsail을 사용하십시오. 주문 대기열에는 Amazon Simple Email Service(Amazon SES)를 사용하십시오. 실패한 주

문을 유지하려면 Amazon OpenSearch Service의 비즈니스 로직에 Amazon Elastic Kubernetes Service(Amazon EKS)를 사용하십시오.

해설
정답: C
Amazon S3는 정적 콘텐츠 호스팅에 매우 저렴하고 확장 가능한 옵션입니다.
AWS AppSync은 GraphQL API를 위한 완전히 관리되는 서비스입니다. 이는 데이터베이스 API 서비스에 적합한 선택입니다.
Amazon SQS 배달 못한 편지 대기열은 처리되지 않은 또는 배달 실패한 메시지를 저장하는 데 사용됩니다. 이 기능을 사용하여 나중에 다시 처리할 수 있습니다.
AWS Lambda는 코드를 실행하는 데 사용되는 완전히 관리되는 서버리스 컴퓨팅 서비스입니다. 주문 처리, 실패한 주문 처리 및 기타 비즈니스 로직을 구현하는 데 사용할 수 있습니다.

◆ | **Q#0272.** | **Ref#0272.**
회사는 us-east-1 지역의 AWS에서 웹 애플리케이션을 호스팅합니다. 애플리케이션 서버는 Application Load Balancer 뒤의 3개 가용 영역에 분산되어 있습니다. 데이터베이스는 Amazon EC2 인스턴스의 MySQL 데이터베이스에서 호스팅됩니다. 솔루션 아키텍트는 AWS 서비스를 사용하여 RTO가 5분 미만, RPO가 1분 미만인 교차 리전 데이터 복구 솔루션을 설계해야 합니다. 솔루션 설계자는 us-west-2에 애플리케이션 서버를 배포하고 있으며 Amazon Route 53 상태 확인 및 us-west-2에 대한 DNS 장애 조치를 구성했습니다.

솔루션 설계자는 어떤 추가 단계를 수행해야 합니까?

A. us-west-2에 교차 리전 읽기 전용 복제본이 있는 Amazon RDS for MySQL 인스턴스로 데이터베이스를 마이그레이션합니다.
B. 기본 데이터베이스가 us-east-1에 있고 보조 데이터베이스가 us-west-2에 있는 Amazon Aurora 글로벌 데이터베이스로 데이터베이스를 마이그레이션합니다.
C. 다중 AZ 배포를 통해 데이터베이스를 MySQL용 Amazon RDS 인스턴스로 마이그레이션합니다.
D. us-west-2의 Amazon EC2 인스턴스에 MySQL 대기 데이터베이스를 생성합니다.

해설
정답: B
RTO 5분 미만, RPO 1분 미만이라는 요구 사항을 충족하기 위해서는 지역 간 데이터 복제 솔루션이 필요합니다.
Amazon Aurora 글로벌 데이터베이스는 지역간 데이터복제, 자동 페일오버, RPO 1분 미만을 달성할 수 있습니다.

◆ | **Q#0273.** | **Ref#0273.**
한 회사가 AWS Organizations를 사용하여 여러 계정을 관리하고 있습니다. 규제 요구 사항으로 인해 회사는 특정 회원 계정을 리소스 배포가 허용되는 특정 AWS 지역으로 제한하려고 합니다. 계정의 리소스에는 태그를 지정하고 그룹 표준에 따라 적용하며 최소한의 구성으로 중앙에서 관리해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. 특정 회원 계정에서 AWS Config 규칙을 생성하여 리전을 제한하고 태그 정책을 적용하십시오.
B. AWS Billing and Cost Management 콘솔의 마스터 계정에서 특정 회원 계정에 대한 지역을 비활성화하고 루트에 태그 정책을 적용합니다.
C. 특정 회원 계정을 루트와 연결합니다. 지역을 제한하는 조건을 사용하여 태그 정책과 SCP를 적용합니다.
D. 특정 회원 계정을 새 OU와 연결합니다. 지역을 제한하는 조건을 사용하여 태그 정책과 SCP를 적용합니다.

해설

문제의 핵심 요구사항:

특정 멤버 계정을 특정 AWS 리전으로 제한
계정 내 자원에 태그를 그룹 표준에 따라 적용 및 강제
최소한의 구성으로 중앙 관리

정답: D

D: 조직 단위(OU)를 사용하여 특정 멤버 계정을 중앙에서 관리하고 태그 정책과 SCP를 적용하여 리전 제한을 강제하는 최적의 해결책.

조직 단위 (OU) 사용: 특정 멤버 계정을 새로운 OU에 연결함으로써 그룹 내에서 계정을 중앙에서 관리 가능. 이는 계정에 대한 정책을 일괄적으로 적용하기에 적합.
태그 정책 적용: OU 수준에서 태그 정책을 적용하면 해당 OU에 속한 모든 계정에 일관된 태그 관리가 가능. 이는 그룹 표준에 따라 태그를 강제할 수 있음.
서비스 제어 정책(SCP) 사용: SCP를 사용하여 조건을 설정하고 특정 리전에서만 자원을 배포할 수 있도록 제한. 이는 특정 멤버 계정을 특정 리전으로 제한하는 요구사항을 충족.

◆ | **Q#0274.** | **Ref#0274.**
한 회사에 보고서를 생성하고 이를 Amazon S3 버킷에 저장하는 애플리케이션이 있습니다. 사용자가 보고서에 액세스하면 애플리케이션은 사용자가 보고서를 다운로드할 수 있도록 서명된 URL을 생성합니다. 회사 보안팀은 해당 파일이 공개되어 있어 누구나 인증 없이 다운로드할 수 있다는 사실을 발견했습니다. 회사는 문제가 해결될 때까지 새로운 보고서 생성을 중단했습니다.

애플리케이션의 일반적인 작업 흐름에 영향을 주지 않고 보안 문제를 즉시 해결하는 조치 세트는 무엇입니까?

A. 인증되지 않은 사용자에 대해 모두 거부 정책을 적용하는 AWS Lambda 함수를 생성합니다. Lambda 함수를 호출하는 예약된 이벤트를 생성합니다.
B. AWS Trusted Advisor 버킷 권한 확인을 검토하고 권장 조치를 구현합니다.
C. 버킷의 모든 객체에 프라이빗 ACL을 배치하는 스크립트를 실행합니다.
D. Amazon S3의 공개 액세스 차단 기능을 사용하여 버킷에서 IgnorePublicAcls 옵션을 TRUE로 설정합니다.

해설
문제의 핵심 요구사항:

파일을 비공개로 만들어야 함 (인증 없이 다운로드 불가)
애플리케이션의 정상적인 워크플로우에 영향을 주지 않아야 함
즉각적인 문제 해결 필요

정답: D

Amazon S3의 Block Public Access 기능을 사용하면 버킷과 객체에 대해 퍼블릭 액세스를 즉시 차단 가능. 이 옵션은 기존의 퍼블릭 액세스 설정을 무시하고, 모든 퍼블릭 액세스를 차단.
즉각적 효과: Block Public Access 기능은 설정 즉시 적용되므로, 파일이 더 이상 공개되지 않도록 즉각적인 효과를 발휘함.
이 설정은 퍼블릭 액세스만 차단하며, 애플리케이션이 생성하는 서명된 URL을 통한 접근에는 영향을 주지 않아 애플리케이션의 정상적인 워크플로우에 영향을 미치지 않음.

◆ | **Q#0275.** | **Ref#0275.**
한 회사는 Oracle 데이터베이스용 Amazon RDS를 다른 AWS 계정의 PostgreSQL용 RDS DB 인스턴스로 마이그레이션할 계획입니다. 솔루션 설계자는 가동 중지 시간이 필요하지 않고 마이그레이션을 완료하는 데 필요한 시간을 최소화하는 마이그레이션 전략을 설계해야 합니다. 마이그레이션 전략은 모든 기존 데이터와 마이그레이션 중에

생성된 모든 새 데이터를 복제해야 합니다. 마이그레이션 프로세스가 완료되면 대상 데이터베이스는 원본 데이터베이스와 동일해야 합니다.

현재 모든 애플리케이션은 Oracle DB 인스턴스용 RDS와의 통신을 위한 엔드포인트로 Amazon Route 53 CNAME 레코드를 사용합니다. Oracle DB 인스턴스용 RDS는 프라이빗 서브넷에 있습니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (3개를 선택하세요.)

> **A.** 대상 계정에 새로운 PostgreSQL DB 인스턴스용 RDS를 생성합니다. AWS Schema Conversion Tool(AWS SCT)을 사용하여 소스 데이터베이스에서 대상 데이터베이스로 데이터베이스 스키마를 마이그레이션합니다.
> **B.** AWS SCT(AWS Schema Conversion Tool)를 사용하여 소스 데이터베이스의 스키마 및 초기 데이터를 사용하여 대상 계정에 PostgreSQL DB 인스턴스용 새 RDS를 생성합니다.
> **C.** 두 AWS 계정의 VPC 간에 VPC 피어링을 구성하여 대상 계정에서 두 DB 인스턴스 모두에 대한 연결을 제공합니다. 대상 계정의 VPC에서 데이터베이스 포트의 트래픽을 허용하도록 각 DB 인스턴스에 연결된 보안 그룹을 구성합니다.
> **D.** 대상 계정의 VPC에서 연결을 제공하기 위해 원본 DB 인스턴스에 일시적으로 공개적으로 액세스할 수 있도록 허용합니다. 대상 계정의 VPC에서 데이터베이스 포트의 트래픽을 허용하도록 각 DB 인스턴스에 연결된 보안 그룹을 구성합니다.
> **E.** 대상 계정에서 AWS Database Migration Service(AWS DMS)를 사용하여 소스 데이터베이스에서 대상 데이터베이스로 전체 로드 및 변경 데이터 캡처(CDC) 마이그레이션을 수행합니다. 마이그레이션이 완료되면 대상 DB 인스턴스 엔드포인트를 가리키도록 CNAME 레코드를 변경합니다.
> **F.** 대상 계정에서 AWS Database Migration Service(AWS DMS)를 사용하여 원본 데이터베이스에서 대상 데이터베이스로 변경 데이터 캡처(CDC) 마이그레이션을 수행합니다. 마이그레이션이 완료되면 대상 DB 인스턴스 엔드포인트를 가리키도록 CNAME 레코드를 변경합니다.
>
> 해설
> 문제의 핵심 요구사항:
>
> 다운타임 없이 RDS for Oracle 데이터베이스를 RDS for PostgreSQL DB 인스턴스로 마이그레이션
> 기존 데이터와 마이그레이션 중 생성된 새 데이터 모두 복제
> 마이그레이션 완료 시 타겟 데이터베이스가 소스 데이터베이스와 동일해야 함
>
> 정답: ACE
>
> 새 RDS for PostgreSQL 인스턴스 생성, AWS SCT(AWS Schema Conversion Tool)를 사용하여 소스 데이터베이스의 스키마를 타겟 데이터베이스로 마이그레이션
> VPC 피어링 설정: 두 AWS 계정의 VPC 간에 피어링을 설정하여 두 데이터베이스 인스턴스 간에 연결성을 제공. 또한, 각 DB 인스턴스에 연결된 보안 그룹을 구성하여 타겟 계정의 VPC에서 데이터베이스 포트로의 트래픽을 허용합니다. 이는 안전한 데이터 전송을 보장
> AWS DMS를 사용하여 전체 로드와 변경 데이터 캡처(CDC) 수행: AWS DMS를 사용하여 전체 데이터를 로드하고, 이후 변경된 데이터를 캡처합니다. 마이그레이션이 완료되면, Route 53의 CNAME 레코드를 타겟 DB 인스턴스의 엔드포인트로 변경합니다. 이는 데이터가 지속적으로 동기화되도록 보장하며, 다운타임 없이 마이그레이션을 완료할 수 있게 합니다.
> B: AWS SCT는 RDS를 생성할 수 없습니다
> D: 원본 데이터베이스를 공개적으로 노출하는 것은 보안 위험입니다.
> F: 단순한 변경이 아닌 초기 데이터도 필요합니다.

◆ | **Q#0276.** | **Ref#0276.**
한 회사는 이벤트 중심 아키텍처를 사용하여 주문 시스템을 구현했습니다. 초기 테스트 중에 시스템이 주문 처리를 중단했습니다. 추가 로그 분석에 따르면 Amazon Simple Queue Service(Amazon SQS) 표준 대기열의 한 주문 메시지가 백엔드에 오류를 일으키고 모든 후속 주문 메시지를 차단하고 있는 것으로 나타났습니다. 대기열의 표시

제한 시간은 30초로 설정되고 백엔드 처리 시간 제한은 10초로 설정됩니다. 솔루션 아키텍트는 잘못된 주문 메시지를 분석하고 시스템이 후속 메시지를 계속 처리하는지 확인해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 수행해야 합니까?

> **A.** 가시성 시간 초과와 일치하도록 백엔드 처리 시간 초과를 30초로 늘립니다.
> **B.** 대기열의 표시 시간 제한을 줄여 잘못된 메시지를 자동으로 제거합니다.
> **C.** 새로운 SQS FIFO 대기열을 배달 못한 편지 대기열로 구성하여 잘못된 메시지를 격리합니다.
> **D.** 새로운 SQS 표준 대기열을 배달 못한 편지 대기열로 구성하여 잘못된 메시지를 격리합니다.
>
> 해설
> 정답: D
> C(x): 대기열이 표준 대기열이므로 FIFO 대기열일 수 없습니다.
> B(x): 잘못된 메시지를 제거하는 데 도움이 될 수 있지만 유효한 메시지 손실 위험도 있습니다.
> A(x): 근본적인 문제를 해결하지 못하고 시스템 성능 저하를 초래할 수 있습니다

◆ | Q#0277. | Ref#0277.
한 회사는 AWS Step Functions를 사용하여 기계 학습 모델의 야간 재교육을 자동화했습니다. 워크플로는 AWS Lambda를 사용하는 여러 단계로 구성됩니다. 각 단계는 다양한 이유로 실패할 수 있으며, 실패하면 전체 워크플로가 실패하게 됩니다.

검토 결과 회사가 이를 인지하지 못한 채 여러 밤 연속으로 재교육이 실패한 것으로 나타났습니다. 솔루션 설계자는 재교육 프로세스의 모든 유형의 실패에 대해 알림이 전송되도록 워크플로를 개선해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (3개를 선택하세요.)

> **A.** 팀의 메일링 목록을 대상으로 하는 "이메일" 유형의 구독을 사용하여 Amazon Simple 알림 서비스(Amazon SNS) 주제를 생성합니다.
> **B.** 입력 인수를 SNS 주제에 전달하는 "이메일"이라는 작업을 생성합니다.
> **C.** "ErrorEquals": ["States.ALL"] 및 "Next": "Email" 문이 있는 모든 작업, 맵 및 병렬 상태에 Catch 필드를 추가합니다.
> **D.** Amazon Simple Email Service(Amazon SES)에 새 이메일 주소를 추가합니다. 이메일 주소를 확인하세요.
> **E.** 입력 인수를 SES 이메일 주소로 전달하는 "Email"이라는 작업을 만듭니다.
> **F.** "ErrorEquals": ["States.Runtime"] 및 "Next": "Email" 문이 있는 모든 작업, 맵 및 병렬 상태에 Catch 필드를 추가합니다.
>
> 해설
> 정답: ABC
> A: Amazon SNS 주제를 생성하여 팀의 메일링 리스트로 이메일 알림을 보냅니다. 이는 오류 발생 시 신속한 알림을 위해 필수적입니다.
> B: "Email"이라는 태스크를 만들어 입력 인수를 SNS 주제로 전달합니다. 이 작업은 오류 발생 시 알림을 트리거합니다.
> C: 모든 Task, Map, Parallel 상태에 "ErrorEquals": ["States.ALL"] 및 "Next": "Email"을 포함하는 Catch 필드를 추가하여 모든 유형의 오류를 포착하고 알림을 보냅니다.
>
> D(x),E(x): Amazon SES는 알림용이 아님.
> F(x): 모든 유형의 오류가 아닌 특정 오류만 감지하기 때문에 올바른 선택이 아님.

◆ | Q#0278. | Ref#0278.
한 회사는 VPC 내부의 Amazon EC2 인스턴스에 새로운 프라이빗 인트라넷 서비스를 배포할 계획입니다. AWS Site-to-Site VPN은 VPC를 회사의 온프레미스 네트워크에 연결합니다. 새 서비스는 기존 온프레미스 서비스와 통신해야 합니다. 온프레미스 서비스는 company.example DNS 영역에 있는 호스트 이름을 사용하여 액세스할 수 있습니다. 이 DNS 영역은 전적으로 온프레미스에서 호스팅되며 회사의 개인 네트워크에서만 사용할 수 있습니다.

솔루션 설계자는 새 서비스가 company.example 도메인의 호스트 이름을 확인하여 기존 서비스와 통합할 수 있는지 확인해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** Amazon Route 53에서 company.example에 대해 빈 프라이빗 영역을 생성합니다. Route 53의 새로운 프라이빗 영역에 대한 권한 있는 이름 서버를 가리키는 회사의 온프레미스 company.example 영역에 추가 NS 레코드를 추가합니다.
> **B.** VPC에 대한 DNS 호스트 이름을 활성화합니다. Amazon Route 53 Resolver를 사용하여 새로운 아웃바운드 엔드포인트를 구성합니다. company.example에 대한 요청을 온프레미스 이름 서버로 전달하는 확인자 규칙을 만듭니다.
> **C.** Amazon Route 53 Resolver를 사용하여 새로운 인바운드 확인자 엔드포인트를 구성하는 VPC에 대한 DNS 호스트 이름을 켭니다. company.example에 대한 요청을 새 확인자로 전달하도록 온프레미스 DNS 서버를 구성합니다.
> **D.** AWS 시스템 관리자를 사용하여 필수 호스트 이름이 포함된 호스트 파일을 설치할 실행 문서를 구성합니다. 인스턴스가 실행 상태로 전환될 때 Amazon EventBridge 규칙을 사용하여 문서를 실행합니다.
>
> 해설
> 핵심 요구사항:
> 회사의 새로 배포된 서비스가 사내 네트워크의 company.example 도메인에 있는 호스트 이름을 해결할 수 있어야 합니다.
>
> 정답: B
> B: VPC에서 DNS 호스트 이름을 활성화하고, Amazon Route 53 Resolver를 사용해 아웃바운드 엔드포인트를 구성한 후,
> company.example 도메인의 요청을 온프레미스 네임 서버로 전달하는 Resolver 규칙을 생성.
> 이 설정은 VPC 내 서비스가 사내 네트워크에 있는 도메인 이름을 정확하게 해결할 수 있도록 보장
>
> A: 빈 프라이빗 영역만 생성하면 company.example 도메인에 대한 DNS 요청을 해결할 수 없습니다.
> C: 인바운드 확인자 엔드포인트를 사용하는 것은 추가적인 복잡성을 야기할 수 있습니다.
> D: 호스트 파일을 사용하는 것은 비효율적이고 관리하기 어려울 수 있습니다.

◆ | **Q#0279.** | **Ref#0279.**
회사는 AWS CloudFormation을 사용하여 전송 게이트웨이에 모두 연결된 여러 VPC 내에 애플리케이션을 배포합니다. 공용 인터넷으로 트래픽을 전송하는 각 VPC는 공유 서비스 VPC를 통해 트래픽을 전송해야 합니다. VPC 내의 각 서브넷은 기본 VPC 라우팅 테이블을 사용하고 트래픽은 전송 게이트웨이로 라우팅됩니다. Transit Gateway는 모든 VPC 연결에 대해 기본 라우팅 테이블을 사용합니다.

보안 감사 결과, VPC 내에 배포된 Amazon EC2 인스턴스가 회사의 다른 VPC에 배포된 EC2 인스턴스와 통신할 수 있는 것으로 나타났습니다. 솔루션 아키텍트는 VPC 간의 트래픽을 제한해야 합니다. 각 VPC는 사전 정의되고 제한된 승인된 VPC 집합과만 통신할 수 있어야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** 승인된 VPC로만 아웃바운드 트래픽을 허용하도록 VPC 내 각 서브넷의 네트워크 ACL을 업데이트합니다. 기본 거부 규칙을 제외한 모든 거부 규칙을 제거합니다.
> **B.** 승인되지 않은 VPC 내에서 사용되는 보안 그룹에 대한 아웃바운드 트래픽을 거부하려면 VPC 내에서 사용되는 모든 보안 그룹을 업데이트하십시오.
> **C.** 각 VPC 연결에 대한 전용 전송 게이트웨이 라우팅 테이블을 생성합니다. 승인된 VPC로만 트래픽을 라우팅합니다.
> **D.** Transit Gateway를 통해 승인된 VPC로만 트래픽을 라우팅하도록 각 VPC의 기본 라우팅 테이블을 업데이트합니다.

해설
핵심 요구사항:
각 VPC는 사전 정의된 특정 VPC들과만 통신해야 하며, 나머지 VPC들과의 통신은 제한되어야 합니다.

정답: C
C: 각 VPC 연결에 대해 전용 전송 게이트웨이 라우트 테이블을 생성하여, 트래픽이 승인된 VPC로만 라우팅되도록 합니다.
이를 통해 트래픽 흐름을 세밀하게 제어할 수 있어 보안 요구사항을 충족시킬 수 있습니다.

A: 네트워크 ACL은 상태 비저장이라서 양방향 트래픽을 제어하기 어렵습니다.
B: 보안 그룹은 상태 저장이라서 더 세밀한 제어가 가능하지만, VPC 간의 트래픽 제어보다는 인스턴스 간의 트래픽 제어에 더 적합합니다.
D: 이 방법도 가능하지만, 기본 라우팅 테이블을 업데이트하는 것은 다소 복잡할 수 있고, 실수로 인해 잘못된 라우팅 설정이 될 위험이 있습니다.

◆ | **Q#0280.** | **Ref#0280.**
회사에는 사용자의 Windows 컴퓨터에 패키지되어 배포되는 Windows 기반 데스크톱 응용 프로그램이 있습니다. 이 회사는 최근 Linux 운영 체제가 설치된 컴퓨터를 주로 사용하는 직원이 있는 다른 회사를 인수했습니다. 인수 회사는 Windows 기반 데스크톱 애플리케이션을 AWS로 마이그레이션하고 다시 호스팅하기로 결정했습니다.

모든 직원은 애플리케이션을 사용하기 전에 인증을 받아야 합니다. 인수 회사는 온프레미스에서 Active Directory를 사용하지만 모든 직원의 AWS 애플리케이션에 대한 액세스를 관리하는 단순화된 방법을 원합니다.

최소한의 개발 노력으로 AWS에서 애플리케이션을 다시 호스팅할 솔루션은 무엇입니까?

A. 모든 직원을 위해 Amazon Workspaces 가상 데스크톱을 설정하고 프로비저닝합니다. Amazon Cognito 자격 증명 풀을 사용하여 인증을 구현합니다. 직원들에게 프로비저닝된 Workspaces 가상 데스크탑에서 애플리케이션을 실행하도록 지시하십시오.
B. Windows 기반 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 각 EC2 인스턴스를 회사의 Active Directory 도메인에 가입시킵니다. 온프레미스에서 실행되는 Active Directory를 사용하여 인증을 구현합니다. 직원들에게 Windows 원격 데스크톱을 사용하여 애플리케이션을 실행하도록 지시합니다.
C. Amazon AppStream 2.0 이미지 빌더를 사용하여 애플리케이션과 필수 구성이 포함된 이미지를 생성합니다. 이미지 실행을 위한 동적 플릿 Auto Scaling 정책을 사용하여 AppStream 2.0 온디맨드 플릿을 프로비저닝합니다. AppStream 2.0 사용자 풀을 사용하여 인증을 구현합니다. 직원들에게 브라우저 기반 AppStream 2.0 스트리밍 세션을 시작하여 애플리케이션에 액세스하도록 지시합니다.
D. 웹 기반 애플리케이션으로 실행되도록 애플리케이션을 리팩터링하고 컨테이너화합니다. 단계 조정 정책을 사용하여 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)에서 애플리케이션을 실행합니다. Amazon Cognito 사용자 풀을 사용하여 인증을 구현합니다. 직원들에게 브라우저에서 애플리케이션을 실행하도록 지시합니다.

해설
정답: C
Amazon AppStream 2.0 사용: 이 방법은 최소한의 개발 노력을 요구하면서도 Linux 사용자와 Windows 사용자 모두가 브라우저 기반 스트리밍을 통해 애플리케이션에 접근가능.
AppStream 2.0 사용자 풀을 통해 인증을 구현하므로, Active Directory와의 복잡한 통합 없이 쉽게 접근 관리가 가능합니다.
이 방법은 최소한의 개발 노력으로 AWS에서 Windows 기반 데스크톱 애플리케이션을 빠르고 쉽게 마이그레이션하고 다시 호스팅하는 가장 간편하고 효율적인 방법입니다.

A: Amazon Workspaces는 데스크톱 환경을 제공하지만, 별도의 라이선스 비용이 발생하고 관리가 복잡해질 수 있습니다.

B: Windows EC2 인스턴스는 유연성을 제공하지만, Active Directory 통합, 인증 및 관리가 복잡해질 수 있습니다.
D: 애플리케이션 리팩터링은 개발 노력이 많이 필요하고 시간이 오래 걸릴 수 있습니다.

281 (황호실) 3회차 完

◆ | **Q#0281.** | **Ref#0281.**
한 회사가 다양한 IoT 장치에서 대량의 데이터를 수집하고 있습니다. 데이터는 영구 Amazon EMR 클러스터의 HDFS(하둡 분산 파일 시스템)에 ORC(Optimized Row Columnar) 파일로 저장됩니다. 회사의 데이터 분석 팀은 동일한 EMR 클러스터에 배포된 Apache Presto의 SQL을 사용하여 데이터를 쿼리합니다. 쿼리는 대량의 데이터를 검색하고 항상 15분 미만 동안 실행되며 오후 5시에서 오후 10시 사이에만 실행됩니다.

회사는 현재 솔루션과 관련된 높은 비용을 우려하고 있습니다. 솔루션 설계자는 SQL 데이터 쿼리를 허용하는 가장 비용 효율적인 솔루션을 제안해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon S3에 데이터를 저장합니다. Amazon Redshift Spectrum을 사용하여 데이터를 쿼리합니다.
B. Amazon S3에 데이터를 저장합니다. AWS Glue 데이터 카탈로그와 Amazon Athena를 사용하여 데이터를 쿼리합니다.
C. EMRFS(EMR 파일 시스템)에 데이터를 저장합니다. Amazon EMR에서 Presto를 사용하여 데이터를 쿼리합니다.
D. Amazon Redshift에 데이터를 저장합니다. Amazon Redshift를 사용하여 데이터를 쿼리합니다.

해설
정답: B
데이터를 Amazon S3에 저장하고 AWS Glue Data Catalog와 Amazon Athena를 사용하여 데이터를 쿼리하는 것입니다.
S3에 데이터를 저장하면 HDFS로 영구 EMR 클러스터를 실행하는 것에 비해 저렴하게 보관할 수 있으며, Athena를 사용하면 서버리스 환경에서 SQL 쿼리를 실행할 수 있어 비용 절감 가능.
Athena는 사용한 만큼만 비용이 청구되므로, 특정 시간대에만 쿼리가 실행되는 상황에 적합합니다.
AWS Glue 데이터 카탈로그는 S3에서 데이터를 구성하고 분류하기 위한 중앙 집중식 메타데이터 저장소를 제공함.

◆ | **Q#0282.** | **Ref#0282.**
한 대기업은 최근 Amazon RDS 및 Amazon DynamoDB 비용이 예기치 않게 증가하는 것을 경험했습니다. 회사는 AWS Billing and Cost Management의 세부 정보에 대한 가시성을 높여야 합니다. 많은 개발 및 프로덕션 계정을 포함하여 AWS Organizations와 연결된 다양한 계정이 있습니다. 조직 전체에 일관된 태그 지정 전략은 없지만 일관된 태그 지정과 함께 AWS CloudFormation을 사용하여 모든 인프라를 배포하도록 요구하는 지침이 있습니다. 관리에는 기존 및 향후의 모든 DynamoDB 테이블과 RDS 인스턴스에 대해 비용 센터 번호와 프로젝트 ID 번호가 필요합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 전략을 제공해야 합니까?

A. 기존 리소스에 태그를 지정하려면 Tag Editor를 사용하세요. 비용 할당 태그를 생성하여 비용 센터와 프로젝트 ID를 정의하고 태그가 기존 리소스에 전파되는 데 24시간을 허용합니다.
B. AWS Config 규칙을 사용하여 태그가 지정되지 않은 리소스를 재무팀에 알립니다. 교차 계정 역할을 사용하여 매시간 태그가 지정되지 않은 RDS 데이터베이스 및 DynamoDB 리소스에 태그를 지정하는 중앙 집중식 AWS Lambda 기반 솔루션을 만듭니다.
C. 태그 편집기를 사용하여 기존 리소스에 태그를 지정합니다. 비용 할당 태그를 생성하여 비용 센터 및 프로젝트 ID를 정의합니다. SCP를 사용하면 리소스에 비용 센터 및 프로젝트 ID가 없는 리소스 생성을 제한할 수 있습니다.

D. 비용 할당 태그를 생성하여 비용 센터와 프로젝트 ID를 정의하고 태그가 기존 리소스에 전파되는 데 24시간을 허용합니다. 리소스에 비용 센터 및 프로젝트 ID가 포함되지 않은 리소스를 프로비저닝하는 권한을 제한하려면 기존 연합 역할을 업데이트하세요.

해설
정답: C
C는 기존 리소스에 대한 Tagging과 미래 리소스 생성을 위한 Tagging 정책의 시행 모두를 해결합니다. Tag Editor를 사용하면 기존 리소스를 신속하게 태그할 수 있으며,
SCP(서비스 제어 정책)를 통해 조직 전체에 정책을 적용하여 비태그된 리소스의 생성을 방지할 수 있습니다.
Tag Editor를 사용하여 기존 리소스에 태그를 추가합니다. 비용 센터 및 프로젝트 ID를 정의하는 비용 할당 태그를 생성합니다. 비용 센터 및 프로젝트 ID가 리소스에 없는 경우
리소스 생성을 제한하는 SCP를 사용합니다.이 솔루션은 비용 센터와 프로젝트 ID 태그가 기존 및 미래의 모든 리소스에 일관되게 적용되도록 하여, 경영진의 가시성과 통제 요구 사항을 충족합니다.

◆ | **Q#0283.** | **Ref#0283.**
회사는 온프레미스 시스템에서 Amazon S3 버킷으로 데이터를 전송하려고 합니다. 회사는 세 가지 다른 계정에 S3 버킷을 생성했습니다. 회사는 데이터가 인터넷을 통해 이동하지 않고 비공개로 데이터를 전송해야 합니다. 회사에는 AWS에 대한 기존 전용 연결이 없습니다.

이러한 요구 사항을 충족하려면 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. AWS 클라우드에 네트워킹 계정을 설정하십시오. 네트워킹 계정에 프라이빗 VPC를 생성합니다. 온프레미스 환경과 프라이빗 VPC 간에 프라이빗 VIF를 사용하여 AWS Direct Connect 연결을 설정합니다.
B. AWS 클라우드에 네트워킹 계정을 설정합니다. 네트워킹 계정에 프라이빗 VPC를 생성합니다. 온프레미스 환경과 프라이빗 VPC 간에 퍼블릭 VIF를 사용하여 AWS Direct Connect 연결을 설정합니다.
C. 네트워킹 계정에 Amazon S3 인터페이스 엔드포인트를 생성합니다.
D. 네트워킹 계정에 Amazon S3 게이트웨이 엔드포인트를 생성합니다.
E. AWS 클라우드에 네트워킹 계정을 설정합니다. 네트워킹 계정에 프라이빗 VPC를 생성합니다. 네트워크 계정의 VPC를 사용하여 S3 버킷을 호스팅하는 계정의 피어 VPC.

해설
정답: AC
A: 네트워킹 계정을 AWS 클라우드에 설정하고, 전용 VPC를 만든 후 온프레미스 환경과 이 VPC 간에 프라이빗 VIF(가상 인터페이스)를 사용하여 AWS Direct Connect 연결을 설정함.
C: Amazon S3 인터페이스 엔드포인트를 사용하면 S3 버킷에 대한 액세스를 인터넷을 거치지 않고 프라이빗하게 수행할 수 있음. 이 두 단계를 함께 사용하여 요구사항을 충족.

◆ | **Q#0284.** | **Ref#0284.**
한 회사에서 퀵서비스 레스토랑을 운영하고 있습니다. 레스토랑은 매일 4시간 동안 판매 트래픽이 높은 예측 가능한 모델을 따릅니다. 피크 시간대 외에는 판매 트래픽이 더 적습니다.

POS 및 관리 플랫폼은 AWS 클라우드에 배포되며 Amazon DynamoDB를 기반으로 하는 백엔드를 갖추고 있습니다. 데이터베이스 테이블은 알려진 최대 리소스 소비량과 일치하도록 100,000개의 RCU 및 80,000개의 WCU가 있는 프로비저닝된 처리량 모드를 사용합니다.

회사는 DynamoDB 비용을 줄이고 IT 직원의 운영 오버헤드를 최소화하려고 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 프로비저닝된 RCU 및 WCU를 줄입니다.
B. 온디맨드 용량을 사용하도록 DynamoDB 테이블을 변경합니다.

C. 테이블에 대해 Dynamo DB Auto Scaling을 활성화합니다.
D. 매일 4시간 동안 최대 부하를 처리하기에 충분한 1년 예약 용량을 구매합니다.

해설
정답: C
DynamoDB 자동 확장을 활성화하는 것이 회사의 요구에 가장 비용 효율적인 솔루션입니다. 자동 확장은 실제 워크로드에 맞춰 프로비저닝된 처리 용량을 자동으로 조정하여,
높은 트래픽 시간에는 용량을 증가시키고 낮은 트래픽 시간에는 용량을 줄입니다. 이를 통해 불필요한 용량 과잉 프로비저닝을 피하고 사용한 만큼만 비용을 지불하여 비용을
절감하고 운영 부담을 최소화할 수 있습니다.

◆ | **Q#0285.** | **Ref#0285.**
한 회사는 Amazon API Gateway, Amazon DynamoDB 및 AWS Lambda를 사용하여 AWS에서 블로그 게시물 애플리케이션을 호스팅합니다. 애플리케이션은 현재 요청을 승인하기 위해 API 키를 사용하지 않습니다. API 모델은 다음과 같습니다:

GET /posts/{postId}: 게시물 세부 정보 가져오기
GET /users/{userId}: 사용자 세부 정보 가져오기
GET /comments/{commentId}: 댓글 세부 정보 가져오기

회사는 사용자가 적극적으로 댓글 섹션에서 주제에 대해 논의하고 있으며 회사는 댓글이 실시간으로 표시되도록 하여 사용자 참여를 늘리기를 원합니다.

댓글 대기 시간을 줄이고 사용자 경험을 개선하려면 어떤 디자인을 사용해야 합니까?

A. Amazon CloudFront와 함께 엣지 최적화 API를 사용하여 API 응답을 캐시합니다.
B. 10초마다 GET/comments/{commentId}를 요청하도록 블로그 애플리케이션 코드를 수정합니다.
C. AWS AppSync를 사용하고 WebSocket을 활용하여 의견을 전달합니다.
D. API 응답 시간을 낮추기 위해 Lambda 함수의 동시성 제한을 변경합니다.

해설
정답: C
AWS AppSync와 WebSockets를 사용하면 실시간 댓글 업데이트를 효율적으로 제공할 수 있습니다. WebSockets는 지속적인 연결을 통해 새로운 댓글이 있을 때마다 클라이언트에
즉시 전달할 수 있으므로 사용자 경험이 크게 향상됩니다. 이는 저지연 및 실시간성을 모두 확보할 수 있는 최적의 솔루션입니다.

◆ | **Q#0286.** | **Ref#0286.**
회사는 AWS Organizations에 속한 조직의 중앙에서 수백 개의 AWS 계정을 관리합니다. 회사는 최근 제품 팀이 자신의 계정에서 자체 S3 액세스 포인트를 생성하고 관리할 수 있도록 허용하기 시작했습니다. S3 액세스 포인트는 인터넷이 아닌 VPC 내에서만 액세스할 수 있습니다.

이 요구 사항을 시행하는 가장 운영상 효율적인 방법은 무엇입니까?

A. s3:AccessPointNetworkOrigin 조건 키가 VPC로 평가되지 않는 한 s3:CreateAccessPoint 작업을 거부하도록 S3 액세스 포인트 리소스 정책을 설정합니다.
B. s3:AccessPointNetworkOrigin 조건 키가 VPC로 평가되지 않는 한 s3:CreateAccessPoint 작업을 거부하도록 조직의 루트 수준에서 SCP를 생성합니다.
C. AWS CloudFormation StackSets를 사용하여 s3:AccessPointNetworkOrigin 조건 키가 VPC로 평가되는 경우에만 s3:CreateAccessPoint 작업을 허용하는 각 AWS 계정에 새 IAM 정책을 생성합니다.

D. s3:AccessPointNetworkOrigin 조건 키가 VPC로 평가되지 않는 한 s3:CreateAccessPoint 작업을 거부하도록 S3 버킷 정책을 설정합니다.

해설
정답: B
SCP는 조직의 권한을 관리하는 데 사용할 수 있는 정책 유형으로, 여러 AWS 계정에 걸쳐 AWS 서비스 작업을 제어할 수 있습니다.
루트 수준에서 SCP를 생성하면 조직 내의 모든 계정에 이 정책이 적용됩니다. 이는 모든 계정에서 단일 정책 변경이 적용되므로 모든 계정에 요구 사항을 적용하는 효율적인 방법.
조직의 루트 수준에서 SCP를 사용하여 s3 작업을 VPC로 제한하는 조건을 설정하는 것이 가장 운영 효율적인 방법.
이는 조직 내 모든 계정에 중앙에서 일관된 정책을 적용할 수 있어 관리가 용이하고, 각 계정이나 버킷마다 개별 정책을 설정할 필요가 없어 운영 오버헤드를 줄일 수 있음.

◆ | **Q#0287.** | **Ref#0287.**
솔루션 아키텍트는 블루/그린 배포 방법을 사용하여 AWS Elastic Beanstalk 내의 애플리케이션 환경을 업데이트해야 합니다. 솔루션 아키텍트는 기존 애플리케이션 환경과 동일한 환경을 생성하고 애플리케이션을 새 환경에 배포합니다.

업데이트를 완료하려면 다음에 무엇을 해야 합니까?

A. Amazon Route 53을 사용하여 새로운 환경으로 리디렉션합니다.
B. 환경 URL 교환 옵션을 선택합니다.
C. Auto Scaling 시작 구성을 교체합니다.
D. 녹색 환경을 가리키도록 DNS 레코드를 업데이트합니다.

해설
정답:B
AWS Elastic Beanstalk는 블루/그린 배포를 수행하기 위한 환경 URL 교체 옵션을 제공합니다. 이 작업은 두 환경의 CNAME 레코드를 교환하여 원래 환경(파란색)에서
새 환경(녹색)으로 트래픽을 다시 라우팅합니다.

◆ | **Q#0288.** | **Ref#0288.**
한 회사에서 사용자가 임의의 사진을 업로드하고 검색할 수 있는 이미지 서비스를 웹에 구축하고 있습니다. 사용량이 가장 많을 때는 전 세계적으로 최대 10,000명의 사용자가 이미지를 업로드합니다. 그러면 업로드된 이미지에 텍스트가 오버레이되어 회사 웹사이트에 게시됩니다.

솔루션 아키텍트는 어떤 디자인을 구현해야 합니까?

A. 업로드된 이미지를 Amazon Elastic File System(Amazon EFS)에 저장합니다. 각 이미지에 대한 애플리케이션 로그 정보를 Amazon CloudWatch Logs로 보냅니다. CloudWatch Logs를 사용하여 처리해야 할 이미지를 결정하는 Amazon EC2 인스턴스 플릿을 생성합니다. 처리된 이미지를 Amazon EFS의 다른 디렉터리에 배치합니다. Amazon CloudFront를 활성화하고 플릿의 EC2 인스턴스 중 하나가 되도록 오리진을 구성합니다.
B. 업로드된 이미지를 Amazon S3 버킷에 저장하고 Amazon Simple 알림 서비스(Amazon SNS)에 메시지를 보내도록 S3 버킷 이벤트 알림을 구성합니다. ALB(Application Load Balancer) 뒤에 Amazon EC2 인스턴스 플릿을 생성하여 Amazon SNS에서 메시지를 가져와 이미지를 처리하고 Amazon Elastic File System(Amazon EFS)에 배치합니다. SNS 메시지 볼륨에 대한 Amazon CloudWatch 지표를 사용하여 EC2 인스턴스를 확장합니다. Amazon CloudFront를 활성화하고 오리진을 EC2 인스턴스 앞의 ALB로 구성합니다.
C. 업로드된 이미지를 Amazon S3 버킷에 저장하고 Amazon Simple Queue Service(Amazon SQS) 대

기열에 메시지를 보내도록 S3 버킷 이벤트 알림을 구성합니다. Amazon EC2 인스턴스 집합을 생성하여 SQS 대기열에서 메시지를 가져와 이미지를 처리하고 다른 S3 버킷에 배치합니다. 대기열 깊이에 대한 Amazon CloudWatch 지표를 사용하여 EC2 인스턴스를 확장합니다. Amazon CloudFront를 활성화하고 원본이 처리된 이미지가 포함된 S3 버킷이 되도록 구성합니다.
D. 업로드된 이미지를 Amazon EC2 스팟 인스턴스 집합에 탑재된 공유 Amazon Elastic Block Store(Amazon EBS) 볼륨에 저장합니다. 업로드된 각 이미지에 대한 정보와 처리 여부를 포함하는 Amazon DynamoDB 테이블을 생성합니다. Amazon EventBridge 규칙을 사용하여 EC2 인스턴스를 확장합니다. Amazon CloudFront를 활성화하고 EC2 인스턴스 집합 앞에서 Elastic Load Balancer를 참조하도록 오리진을 구성합니다.

해설
정답: C
업로드된 이미지를 S3 버킷에 저장하고 SQS 대기열과 함께 S3 이벤트 알림 사용이 가장 적합한 설계입니다. Amazon S3는 업로드된 이미지를 위한 확장성과 내구성이 뛰어난 스토리지를제공합니다. SQS 대기열로 메시지를 보내도록 S3 이벤트 알림을 구성하면 업로드 프로세스에서 이미지 처리를 분리할 수 있습니다. EC2 인스턴스 집합은 SQS 대기열에서 메시지를 가져와 이미지를 처리하고 다른 S3 버킷에 저장할 수 있습니다. CloudWatch 지표를 사용하여 SQS 대기열 깊이를 기반으로 EC2 인스턴스를 확장하면 리소스를 효율적으로 활용할 수 있습니다. 처리된 이미지가 포함된 S3 버킷으로 설정된 원본으로 Amazon CloudFront를 활성화하면 이미지 전송의 글로벌 가용성과 성능이 향상됩니다.

◆ | **Q#0289.** | **Ref#0289.**
한 회사가 us-east-1 지역의 MySQL DB 인스턴스용 Amazon RDS에 데이터베이스를 배포했습니다. 회사는 유럽 고객에게 데이터를 제공해야 합니다. 유럽 고객은 미국(US) 고객과 동일한 데이터에 액세스할 수 있어야 하며 높은 애플리케이션 대기 시간이나 오래된 데이터를 용납하지 않습니다. 유럽 고객과 미국 고객은 데이터베이스에 기록해야 합니다. 두 고객 그룹 모두 다른 그룹의 업데이트를 실시간으로 확인해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. RDS for MySQL DB 인스턴스의 Amazon Aurora MySQL 복제본을 생성합니다. RDS DB 인스턴스에 대한 애플리케이션 쓰기를 일시 중지합니다. Aurora 복제본을 독립형 DB 클러스터로 승격합니다. Aurora 데이터베이스를 사용하고 쓰기를 재개하도록 애플리케이션을 재구성하십시오. eu-west-1을 DB 클러스터에 보조 리전으로 추가합니다. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 Aurora MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
B. RDS for MySQL DB 인스턴스에 대해 eu-west-1에 교차 리전 복제본을 추가합니다. 기본 DB 인스턴스에 쓰기 쿼리를 다시 복제하도록 복제본을 구성합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 RDS for MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
C. RDS for MySQL DB 인스턴스의 최신 스냅샷을 eu-west-1로 복사합니다. 스냅샷에서 eu-west-1에 새로운 MySQL용 RDS DB 인스턴스를 생성합니다. us-east-1에서 eu-west-1로 MySQL 논리적 복제를 구성합니다. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-wes&1에 애플리케이션을 배포합니다. eu-west-1에서 RDS for MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
D. RDS for MySQL DB 인스턴스를 Amazon Aurora MySQL DB 클러스터로 변환합니다. eu-west-1을 DB 클러스터에 보조 리전으로 추가합니다. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 Aurora MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.

해설
정답:A
기본적으로 RDS MySQL을 Aurora MySQL로 변환할 수 없습니다. 먼저 Aurora 읽기 전용 복제본을 생성한 후 독립 DB 클러스터로 승격해야 합니다.

고객들에게 유럽에서 데이터를 제공하고, 저 애플리케이션 지연 시간과 미국과 유럽 고객 간 실시간 업데이트를 보장하기 위한 요구 사항을 충족시키기 위해 최선의 해결책은
RDS for MySQL DB 인스턴스의 Amazon Aurora MySQL 복제본을 생성하는 것입니다.
Amazon Aurora는 다중 리전 복제를 지원하여 RDS for MySQL DB 인스턴스의 복제본을 다른 AWS 리전 (이 경우 eu-west-1)에 생성할 수 있습니다.
Aurora 복제본은 승격하여 독립형 DB 클러스터로 제공되며, 고가용성과 읽기 확장성을 제공합니다.
DB 클러스터에서 쓰기 전달을 활성화하면, 미국과 유럽 모두에서의 쓰기 쿼리를 주요 DB 인스턴스 (us-east-1 지역)로 전달할 수 있습니다.
이로써 미국과 유럽 고객 모두가 데이터베이스에 쓰기를 할 수 있고 실시간으로 업데이트를 볼 수 있습니다.
응용 프로그램은 유럽 고객을 위해 eu-west-1의 Aurora MySQL 엔드포인트를 사용하도록 다시 구성되어야 합니다.

◆ | **Q#0290.** | **Ref#0290.**
회사는 인터넷을 통해 액세스할 수 있는 SFTP 서버를 통해 고객에게 파일을 제공하고 있습니다. SFTP 서버는 탄력적 IP 주소가 연결된 단일 Amazon EC2 인스턴스에서 실행됩니다. 고객은 탄력적 IP 주소를 통해 SFTP 서버에 연결하고 SSH를 사용하여 인증합니다. EC2 인스턴스에는 모든 고객 IP 주소의 액세스를 허용하는 연결된 보안 그룹도 있습니다.

솔루션 설계자는 가용성을 향상시키고, 인프라 관리의 복잡성을 최소화하며, 파일에 액세스하는 고객의 업무 중단을 최소화하는 솔루션을 구현해야 합니다. 솔루션은 고객이 연결하는 방식을 변경해서는 안 됩니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS Transfer Family 서버를 생성합니다. 공개적으로 액세스 가능한 엔드포인트로 Transfer Family 서버를 구성합니다. SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. Transfer Family 서버를 S3 버킷으로 지정합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.
B. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS Transfer Family 서버를 생성합니다. VPC 호스팅, 인터넷 연결 엔드포인트로 Transfer Family 서버를 구성합니다. SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. 고객 IP 주소가 포함된 보안 그룹을 새 엔드포인트에 연결합니다. Transfer Family 서버를 S3 버킷으로 지정합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.
C. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 새로운 Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. SFTP 서버를 실행하기 위한 AWS Fargate 작업 정의를 생성합니다. 작업 정의에서 EFS 파일 시스템을 탑재로 지정합니다. 작업 정의를 사용하여 Fargate 서비스를 생성하고 서비스 앞에 NLB(Network Load Balancer)를 배치합니다. 서비스를 구성할 때 고객 IP 주소가 포함된 보안 그룹을 SFTP 서버를 실행하는 작업에 연결하세요. 탄력적 IP 주소를 NLB와 연결합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.
D. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 다중 연결 Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성합니다. 탄력적 IP 주소가 연결된 NLB(Network Load Balancer)를 생성합니다. SFTP 서버를 실행하는 EC2 인스턴스로 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹에서 시작되는 인스턴스가 새로운 다중 연결 EBS 볼륨을 연결해야 함을 정의합니다. NLB 뒤에 인스턴스를 자동으로 추가하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹이 시작하는 EC2 인스턴스에 대해 고객 IP 주소를 허용하는 보안 그룹을 사용하도록 Auto Scaling 그룹을 구성합니다. SFTP 서버의 모든 파일을 새로운 다중 연결 EBS 볼륨으로 동기화합니다.

해설
정답:B
옵션 B는 EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제하고 SFTP 파일 호스팅을 위한 Amazon

S3 버킷을 생성할 것을 제안합니다.
그런 다음 AWS Transfer Family 서버가 생성되고 VPC 호스팅 >인터넷 연결 엔드포인트로 구성됩니다. SFTP 탄력적 IP 주소는 새 엔드포인트와 연결되고,
고객 IP 주소가 있는 보안 그룹은 엔드포인트에 연결됩니다. Transfer Family 서버는 S3 버킷을 가리키고 SFTP 서버의 모든 파일은 S3 버킷에 동기화됩니다.

IP를 화이트리스트에 추가하려면 SG(보안그룹)가 필요합니다.
B 질문은 "EC2 인스턴스에는 모든 고객 IP 주소의 액세스를 허용하는 보안 그룹도 연결되어 있습니다."라고 말합니다. B는 "고객 IP 주소가 포함된 보안 그룹을 새 엔드포인트에 연결합니다"라고 말합니다. 고객을 위한 보안 작업을 위한 보안 그룹이어야 합니다.

291 (김지형) 3회차 完

◆ | **Q#0291.** | **Ref#0291.**
회사는 스트리밍 시장 데이터를 수집하고 처리합니다. 데이터 속도는 일정합니다. 집계 통계를 계산하는 야간 프로세스는 완료하는 데 4시간이 걸립니다. 통계 분석은 비즈니스에 중요하지 않으며 특정 실행이 실패하면 다음 반복 중에 데이터 포인트가 처리됩니다.

현재 아키텍처는 1년 예약이 포함된 Amazon EC2 예약 인스턴스 풀을 사용합니다. 이러한 EC2 인스턴스는 풀타임으로 실행되어 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨에 스트리밍 데이터를 수집하고 저장합니다. 예약된 스크립트는 매일 밤 EC2 온디맨드 인스턴스를 시작하여 야간 처리를 수행합니다. 인스턴스는 수집 서버의 NFS 공유에 저장된 데이터에 액세스합니다. 처리가 완료되면 스크립트는 인스턴스를 종료합니다.

예약 인스턴스 예약이 만료됩니다. 회사는 새로운 예약을 구매할지 아니면 새로운 디자인을 구현할지 결정해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. Amazon Kinesis Data Firehose를 사용하여 Amazon S3에 데이터를 저장하도록 수집 프로세스를 업데이트합니다. 예약된 스크립트를 사용하여 매일 밤 EC2 온디맨드 인스턴스 집합을 시작하여 S3 데이터의 일괄 처리를 수행합니다. 처리가 완료되면 인스턴스를 종료하도록 스크립트를 구성합니다.
B. Amazon Kinesis Data Firehose를 사용하여 Amazon S3에 데이터를 저장하도록 수집 프로세스를 업데이트합니다. 스팟 인스턴스와 함께 AWS Batch를 사용하면 온디맨드 가격의 50%에 해당하는 최대 스팟 가격으로 야간 처리를 수행할 수 있습니다.
C. Network LoadBalancer 뒤에 3년 예약이 포함된 EC2 예약 인스턴스 집합을 사용하도록 수집 프로세스를 업데이트합니다. 스팟 인스턴스와 함께 AWS Batch를 사용하면 온디맨드 가격의 50%에 해당하는 최대 스팟 가격으로 야간 처리를 수행할 수 있습니다.
D. Amazon Kinesis Data Firehose를 사용하여 Amazon Redshift에 데이터를 저장하도록 수집 프로세스를 업데이트합니다. Amazon EventBridge를 사용하면 AWS Lambda 함수가 야간에 실행되어 Amazon Redshift에 쿼리하여 일일 통계를 생성하도록 예약할 수 있습니다.

해설
정답: B
Amazon Kinesis Data Firehose를 사용하여 데이터를 실시간으로 캡처하고 저장할 수 있어 데이터 스트리밍에 적합.
Spot Instances를 사용하여 야간에 비용 절감하며 배치 작업을 수행 가능해 비용 효율성 증대.
AWS Batch를 통해 효과적으로 배치 컴퓨팅 작업 실행 가능하며 인스턴스를 자동으로 선택하고 큐를 스케일링하여 적합.

◆ | **Q#0292.** | **Ref#0292.**
회사는 온프레미스 SFTP 사이트를 AWS로 마이그레이션해야 합니다. SFTP 사이트는 현재 Linux VM에서 실행됩니

다. 업로드된 파일은 NFS 공유를 통해 다운스트림 애플리케이션에서 사용할 수 있습니다.

AWS로 마이그레이션하는 과정에서 솔루션 아키텍트는 고가용성을 구현해야 합니다. 솔루션은 공급업체가 허용할 수 있는 고정 공용 IP 주소 집합을 외부 공급업체에 제공해야 합니다. 회사는 온프레미스 데이터 센터와 VPC 간에 AWS Direct Connect 연결을 설정했습니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** AWS Transfer Family 서버를 생성합니다. Transfer Family 서버에 대한 인터넷 연결 VPC 엔드포인트를 구성합니다. 각 서브넷에 대해 탄력적 IP 주소를 지정합니다. 여러 가용 영역에 배포된 Amazon Elastic File System(Amazon EFS) 파일 시스템에 파일을 배치하도록 Transfer Family 서버를 구성합니다. 대신 EFS 엔드포인트를 탑재하도록 기존 NFS 공유에 액세스하는 다운스트림 애플리케이션의 구성을 수정합니다.
> **B.** AWS Transfer Family 서버를 생성합니다. Transfer Family 서버에 대해 공개적으로 액세스 가능한 엔드포인트를 구성합니다. 여러 가용 영역에 배포된 Amazon Elastic File System(Amazon EFS) 파일 시스템에 파일을 배치하도록 Transfer Family 서버를 구성합니다. 대신 EFS 엔드포인트를 탑재하도록 기존 NFS 공유에 액세스하는 다운스트림 애플리케이션의 구성을 수정합니다.
> **C.** AWS Application Migration Service를 사용하여 기존 Linux VM을 Amazon EC2 인스턴스로 마이그레이션합니다. EC2 인스턴스에 탄력적 IP 주소를 할당합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 EC2 인스턴스에 탑재합니다. EFS 파일 시스템에 파일을 배치하도록 SFTP 서버를 구성합니다. 대신 EFS 엔드포인트를 탑재하도록 기존 NFS 공유에 액세스하는 다운스트림 애플리케이션의 구성을 수정합니다.
> **D.** AWS Application Migration Service를 사용하여 기존 Linux VM을 AWS Transfer Family 서버로 마이그레이션합니다. Transfer Family 서버에 대해 공개적으로 액세스 가능한 엔드포인트를 구성합니다. 여러 가용 영역에 배포되는 Amazon FSx for Lustre 파일 시스템에 파일을 배치하도록 Transfer Family 서버를 구성합니다. 대신 기존 NFS 공유에 액세스하는 다운스트림 애플리케이션의 구성을 수정하여 FSx for Lustre 엔드포인트를 탑재합니다.
>
> 해설
> 정답: A
> AWS 전송 패밀리는 외부 공급 업체가 현재 사용 중인 SFTP를 교체하는 가장 쉬운 방법입니다. 이 도구는 SFTP, FTPS, FTP를 지원하므로 기존 사용자가 방해를 받지 않고 작동을 계속할 수 있습니다.
> 확장 가능한 저장소를 위해 Amazon EFS를 선택하면 모든 에플리케이션이 저장소를 공유할 수 있고, 다른 가용 영역에서도 동시에 파일에 액세스할 수 있습니다. 이로 인해 고가용성이 제공됩니다.
> 여러 가용 영역에 배포되어 있는 탄력적인 IP 주소를 설정하면 업체가 이러한 IP 주소를 허용 리스트에 추가할 수 있게 됩니다.

◆ | **Q#0293.** | **Ref#0293.**
솔루션 아키텍트에는 Auto Scaling 그룹의 Amazon EC2 인스턴스에 배포된 운영 워크로드가 있습니다. VPC 아키텍처는 Auto Scaling 그룹이 대상으로 삼는 각각의 서브넷이 있는 두 개의 가용 영역(AZ)에 걸쳐 있습니다. VPC는 온프레미스 환경에 연결되어 있으며 연결이 중단될 수 없습니다. Auto Scaling 그룹의 최대 크기는 서비스 중인 인스턴스 20개입니다. VPC IPv4 주소 지정은 다음과 같습니다.

VPC CIDR: 10.0.0.0/23 -

AZ1 서브넷 CIDR: 10.0.0.0/24 -

AZ2 서브넷 CIDR: 10.0.1.0/24 -

배포 이후 세 번째 AZ를 해당 지역에서 사용할 수 있게 되었습니다. 솔루션 설계자는 추가 IPv4 주소 공간을 추가하지 않고 서비스 가동 중지 시간 없이 새 AZ를 채택하기를 원합니다. 어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** AZ2 서브넷만 사용하도록 Auto Scaling 그룹을 업데이트합니다. 이전 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 생성합니다. 새 AZ1 서브넷도 사용하도록 Auto Scaling 그룹을 조

정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 Auto Scaling 그룹을 조정합니다. 현재 AZ2 서브넷을 제거합니다. 원래 AZ1 서브넷 주소 공간의 후반부를 사용하여 새 AZ2 서브넷을 생성합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 생성한 다음 세 개의 새 서브넷을 모두 대상으로 지정하도록 Auto Scaling 그룹을 업데이트합니다.
B. AZ1 서브넷에서 EC2 인스턴스를 종료합니다. 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 생성합니다. 이 새 서브넷을 사용하도록 Auto Scaling 그룹을 업데이트합니다. 두 번째 AZ에 대해 이를 반복합니다. AZ3에서 새 서브넷을 정의한 다음 세 개의 새 서브넷을 모두 대상으로 지정하도록 Auto Scaling 그룹을 업데이트합니다.
C. 동일한 IPv4 주소 공간으로 새 VPC를 생성하고 각 AZ마다 하나씩 3개의 서브넷을 정의합니다. 새 VPC의 새 서브넷을 대상으로 지정하도록 기존 Auto Scaling 그룹을 업데이트합니다.
D. AZ2 서브넷만 사용하도록 Auto Scaling 그룹을 업데이트합니다. 이전 주소 공간의 절반을 갖도록 AZ1 서브넷을 업데이트합니다. AZ1 서브넷도 다시 사용하도록 Auto Scaling 그룹을 조정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 Auto Scaling 그룹을 조정합니다. 현재 AZ2 서브넷을 업데이트하고 원래 AZ1 서브넷에서 주소 공간의 두 번째 절반을 할당합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 생성한 다음 세 개의 새 서브넷을 모두 대상으로 지정하도록 Auto Scaling 그룹을 업데이트합니다.

해설
정답: A
되도록 연결이 끊어지지 않고 추가적인 IPv4 주소 공간을 사용하지 않으면서 세 번째 가용 영역을 적용하고자 하는 이 회사의 요구사항을 가장 효과적으로 만족시키는 해결 방안은 옵션 A입니다.
Auto Scaling 그룹에서 한 번에 한 AZ의 인스턴스를 제거하고 새 서브넷에 대한 조정을 진행하는 방식으로 예비 AZ의 연결성은 유지되고 간헐적으로 끊어지지 않습니다.
서브넷을 반으로 나누고 반은 새 AZ에 할당함으로써 추가적인 IP 주소 공간을 필요로 하지 않습니다.

◆ | **Q#0294.** | **Ref#0294.**
회사는 AWS Organizations의 조직을 사용하여 회사의 AWS 계정을 관리합니다. 회사는 AWS CloudFormation을 사용하여 모든 인프라를 배포합니다. 재무팀에서 지불 거절 모델을 구축하려고 합니다. 재무팀은 각 사업부에게 사전 정의된 프로젝트 값 목록을 사용하여 리소스에 태그를 지정하도록 요청했습니다.

재무팀은 AWS Cost Explorer에서 AWS 비용 및 사용 보고서를 사용하고 프로젝트를 기준으로 필터링했을 때 규정을 준수하지 않는 프로젝트 값을 발견했습니다. 회사는 새 리소스에 대해 프로젝트 태그 사용을 시행하려고 합니다.

최소한의 노력으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 조직의 마스터 계정에 허용된 프로젝트 태그 값을 포함하는 태그 정책을 생성합니다. 프로젝트 태그가 추가되지 않는 한 cloudformation:CreateStack API 작업을 거부하는 SCP를 생성합니다. SCP를 각 OU에 연결합니다.
B. 각 OU에 허용되는 프로젝트 태그 값을 포함하는 태그 정책을 생성합니다. 프로젝트 태그가 추가되지 않는 한 cloudformation:CreateStack API 작업을 거부하는 SCP를 생성합니다. SCP를 각 OU에 연결합니다.
C. AWS 마스터 계정에서 허용되는 프로젝트 태그 값을 포함하는 태그 정책을 생성합니다. 프로젝트 태그가 추가되지 않는 한 cloudformation:CreateStack API 작업을 거부하는 IAM 정책을 생성합니다. 각 사용자에게 정책을 할당합니다.
D. AWS Service Catalog를 사용하여 CloudFormation 스택을 제품으로 관리합니다. TagOptions 라이브러리를 사용하여 프로젝트 태그 값을 제어합니다. 조직에 있는 모든 OU와 포트폴리오를 공유합니다.

해설
정답: A
AWS Organizations에서 태그 정책을 생성하여 조직의 모든 계정에 적용할 수 있습니다. 이렇게 하

면 효율적으로 모든 계정에서 태그를 관리하고 통제할 수 있습니다.
SCP는 특정 조직 계층 구조 내의 모든 AWS 계정에 권한을 부여하거나 거부할 수 있습니다. AWS Organizations에서 SCP를 사용하면 조직의 모든 계정에서 cloudformation:CreateStack API 작업을 통제할 수 있습니다.

◆ | **Q#0295.** | **Ref#0295.**
Auto Scaling 그룹에서 실행되는 Amazon EC2 인스턴스에 애플리케이션이 배포됩니다. Auto Scaling 그룹 구성은 한 가지 유형의 인스턴스만 사용합니다.

CPU 및 메모리 사용률 지표는 인스턴스의 사용률이 낮은 것으로 나타났습니다. 솔루션 아키텍트는 EC2 비용을 영구적으로 줄이고 활용도를 높이는 솔루션을 구현해야 합니다.

앞으로 최소한의 구성 변경으로 이러한 요구 사항을 충족할 솔루션은 무엇입니까?

A. 현재 인스턴스의 속성과 유사한 속성을 가진 인스턴스 유형을 나열합니다. 목록에 있는 여러 인스턴스 유형을 사용하도록 Auto Scaling 그룹의 시작 템플릿 구성을 수정합니다.
B. 애플리케이션의 CPU 및 메모리 사용률에 대한 정보를 사용하여 요구 사항에 맞는 인스턴스 유형을 선택합니다. 새 인스턴스 유형을 추가하여 Auto Scaling 그룹의 구성을 수정합니다. 구성에서 현재 인스턴스 유형을 제거합니다.
C. 애플리케이션의 CPU 및 메모리 사용률에 대한 정보를 사용하여 Auto Scaling 그룹 시작 템플릿의 새 개정판에서 CPU 및 메모리 요구 사항을 지정합니다. 구성에서 현재 인스턴스 유형을 제거합니다.
D. AWS Price List Bulk API에서 적절한 인스턴스 유형을 선택하는 스크립트를 생성합니다. 선택한 인스턴스 유형을 사용하여 Auto Scaling 그룹 시작 템플릿의 새 개정판을 생성합니다.

해설
정답: C B(x)
C: ASG가 아닌 시작 템플릿에서 인스턴스 유형/크기를 변경합니다. ASG는 인스턴스 유형이 아닌 최소/최대 크기를 변경할 수 있습니다.
답변의 핵심은 "수정". 런치 템플릿을 만든 후에는 수정할 수 없습니다. 대신 필요한 변경 사항을 포함하는 새 버전의 런치 템플릿을 만들 수 있습니다.
우리는 시작 구성이나 시작 템플릿을 변경/수정할 수 없습니다.

정답: B
시작 템플릿에서는 하나의 인스턴스 유형만 선택할 수 있습니다. 그러나 ASG 구성에서 시작 템플릿을 재정의하고 여러 인스턴스 유형을 지정할 수 있습니다.
AWS 콘솔에서 직접 테스트해보았는데 정답은 "B"입니다. 인스턴스 유형을 변경하려면 3가지 옵션이 있으며 모든 옵션에는 ASG 구성을 수정해야 합니다.
1. 현재 시작 템플릿의 새 개정판을 생성한 다음 이를 사용하도록 ASG 구성을 변경합니다.
2. 새 시작 템플릿을 생성한 다음 이를 사용하도록 ASG 구성을 변경합니다.
3. ASG 구성에서 "시작 템플릿 재정의" 옵션을 사용합니다.
시작 템플릿의 새 개정판만 생성하는 경우 ASG는 이전 개정판을 계속 사용합니다.
ASG 구성에서 인스턴스 유형을 변경할 수 없는 상태는 사실이 아니며 누구나 AWS 콘솔에서 이를 확인할 수 있습니다.
인스턴스가 활용되지 않고 있다는 지표를 고려하여 요구사항에 맞는 새로운 인스턴스 유형을 선택하고, 이를 Auto Scaling 그룹에 추가하며, 기존의 활용도가 낮은 인스턴스 유형은 제거하는 방안을 제시하고 있습니다. 이렇게 하면 EC2 비용을 줄일 수 있으며, 구성 변경도 최소화할 수 있습니다.
시작 구성 또는 시작 템플릿을 변경/수정할 수 없기 때문에 C라는 의견들이 있으나 사용자가 AWS Console에 실제로 로그인해서 ASG(오토 스케일링 그룹) 구성을 변경해볼 수 있다는 사실을 확인하여 B로 결정

◆ | **Q#0296.** | **Ref#0296.**
회사는 Amazon Elastic Container Service(Amazon ECS) 및 Amazon API Gateway를 사용하여 컨테이너화된 애플리케이션을 구현합니다. 애플리케이션 데이터는 Amazon Aurora 데이터베이스 및 Amazon DynamoDB 데이터베이

스에 저장됩니다. 회사는 AWS CloudFormation을 사용하여 인프라 프로비저닝을 자동화합니다. 회사는 AWS CodePipeline을 사용하여 애플리케이션 배포를 자동화합니다.

솔루션 아키텍트는 2시간의 RPO와 4시간의 RTO를 충족하는 재해 복구(DR) 전략을 구현해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** 데이터베이스를 보조 AWS 리전에 복제하도록 Aurora 글로벌 데이터베이스와 DynamoDB 글로벌 테이블을 설정합니다. 기본 리전과 보조 리전에서 리전 엔드포인트를 사용하여 API Gateway API를 구성합니다. DR 시나리오 중에 트래픽을 보조 리전으로 라우팅하기 위해 오리진 장애 조치가 포함된 Amazon CloudFront를 구현합니다.
> **B.** AWS DMS(AWS Database Migration Service), Amazon EventBridge 및 AWS Lambda를 사용하여 Aurora 데이터베이스를 보조 AWS 지역에 복제합니다. DynamoDB 스트림, EventBridge를 사용합니다. DynamoDB 데이터베이스를 보조 리전에 복제하는 Lambda. 기본 리전과 보조 리전에서 리전 엔드포인트를 사용하여 API Gateway API를 구성합니다. Amazon Route 53 장애 조치 라우팅을 구현하여 기본 지역에서 보조 지역으로 트래픽을 전환합니다.
> **C.** AWS 백업을 사용하여 보조 AWS 리전에 Aurora 데이터베이스 및 DynamoDB 데이터베이스의 백업을 생성하십시오. 기본 리전과 보조 리전에서 리전 엔드포인트를 사용하여 API Gateway API를 구성합니다. Amazon Route 53 장애 조치 라우팅을 구현하여 기본 지역에서 보조 지역으로 트래픽을 전환합니다.
> **D.** 데이터베이스를 보조 AWS 리전에 복제하도록 Aurora 글로벌 데이터베이스와 DynamoDB 글로벌 테이블을 설정합니다. 기본 리전과 보조 리전에서 리전 엔드포인트를 사용하여 API Gateway API를 구성합니다. Amazon Route 53 장애 조치 라우팅을 구현하여 기본 지역에서 보조 지역으로 트래픽을 전환합니다.
>
> 해설
> 정답: D
> Aurora 및 DynamoDB의 글로벌 테이블 설정이 실시간 데이터 복제를 가능하게 하므로 RPO와 RTO를 만족시키고, 이는 AWS 백업에서 제공하는 백업 복원 방식보다 신속하고 효과적이라는 점입니다. 그러나, 몇몇 의견은 C가 더 비용 효율적이고 AWS 백업을 사용하는 것이 글로벌 데이터베이스를 구성하는 것보다 저렴하다고 주장합니다. 이러한 의견은 AWS 백업을 통해 RPO와 RTO 목표를 달성할 수 있다는 가정 하에 성립합니다.
> 가장 비용효율적인건 여러 가지 요소에 좌우되며 특히 데이터의 크기, 변동률, 예상 복구 시간 등이 결정적인 역할을 합니다. 이러한 정보가 없는 경우 각 솔루션의 비용을 비교하기 어려우며, 따라서 D 옵션은 가장 일반적으로 적용할 수 있는 옵션이고 특정 시나리오에서는 C가 더 비용 효율적일 수 있습니다.

◆ | **Q#0297.** | **Ref#0297.**
한 회사에는 글로벌 확장성과 성능을 위해 Amazon CloudFront를 활용하는 복잡한 웹 애플리케이션이 있습니다. 시간이 지나면서 사용자들은 웹 애플리케이션 속도가 느려지고 있다고 보고합니다.

회사 운영 팀은 CloudFront 캐시 적중률이 꾸준히 감소하고 있다고 보고합니다. 캐시 지표 보고서는 일부 URL의 쿼리 문자열이 일관되지 않게 정렬되어 있으며 때로는 대소문자가 혼합되어 지정되거나 소문자로 지정된다는 것을 나타냅니다.

캐시 적중률을 최대한 빨리 높이기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?

> **A.** 매개변수를 이름별로 정렬하고 소문자로 강제 지정하려면 Lambda@Edge 함수를 배포하세요. CloudFront 뷰어 요청 트리거를 선택하여 함수를 호출합니다.
> **B.** 쿼리 문자열 매개변수를 기반으로 캐싱을 비활성화하도록 CloudFront 배포를 업데이트합니다.
> **C.** 로드 밸런서 뒤에 역방향 프록시를 배포하여 애플리케이션에서 내보낸 URL을 사후 처리하여 URL 문자열을 소문자로 만듭니다.
> **D.** 대소문자를 구분하지 않는 쿼리 문자열 처리를 지정하도록 CloudFront 배포를 업데이트합니다.

해설
정답: A
캐시 히트 비율이 감소하는 문제를 해결하기 위해 솔루션 아키텍트는 Lambda@Edge 함수를 배포하여 요청의 파라미터를 이름순으로 정렬하고 소문자로 강제해야 합니다. 이는 CloudFront의 뷰어 요청 트리거를 사용하여 함수를 호출함으로써 실행됩니다.
B는 캐싱을 아예 비활성화하는 것이므로 성능 저하를 초래하고, C는 URL의 캡처와 처리를 위해 추가적인 컴포넌트인 역방향 프록시를 요구하므로 비효율적입니다. 그리고 D는 CloudFront에 존재하지 않는 기능을 구현하려는 것으로 실행이 불가능합니다.

◆ | **Q#0298.** | **Ref#0298.**
회사는 단일 AWS 리전에서 전자상거래 애플리케이션을 실행합니다. 이 애플리케이션은 5노드 Amazon Aurora MySQL DB 클러스터를 사용하여 고객 및 고객의 최근 주문에 대한 정보를 저장합니다. DB 클러스터에서는 하루 종일 많은 수의 쓰기 트랜잭션이 발생합니다.

회사는 재해 복구 요구 사항을 충족하기 위해 Aurora 데이터베이스의 데이터를 다른 지역으로 복제해야 합니다. 회사의 RPO는 1시간입니다.

가장 저렴한 비용으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. Aurora 데이터베이스를 Aurora 글로벌 데이터베이스로 수정하십시오. 다른 리전에 두 번째 Aurora 데이터베이스를 생성합니다.
B. Aurora 데이터베이스에 대한 역추적 기능을 활성화합니다. 데이터베이스의 스냅샷을 백업 리전에 복사하기 위해 매일 실행되는 AWS Lambda 함수를 생성합니다.
C. AWS Database Migration Service(AWS DMS)를 사용한다. Aurora 데이터베이스에서 다른 리전의 Amazon S3 버킷으로 진행 중인 변경 사항을 복제하는 DMS 변경 데이터 캡처(CDC) 작업을 생성합니다.
D. 자동화된 Aurora 백업을 끄십시오. 1시간의 백업 빈도로 Aurora 백업을 구성하십시오. 다른 지역을 대상 지역으로 지정하세요. 리소스 할당으로 Aurora 데이터베이스를 선택합니다.

해설
정답: C
변동 데이터 캡처 (CDC) 작업을 사용하여 Aurora 데이터베이스의 지속적인 변경 사항을 복제하는 AWS Database Migration Service (DMS)를 사용하는 것이 비용이 가장 적게 듭니다.
데이터 동기화 작업을 통해 기본 데이터베이스의 변경 사항을 실시간으로 추적하고, 이 변경 사항들을 사용자가 지정한 빈도로 다른 리전의 S3 버킷에 복제합니다.
이 방법으로 회사의 RPO 요구 사항인 1시간을 충족시킬 수 있습니다.

◆ | **Q#0299.** | **Ref#0299.**
한 회사의 솔루션 아키텍트가 몇 년 전에 배포된 AWS 워크로드를 평가하고 있습니다. 애플리케이션 계층은 상태 비저장이며 AMI에서 시작된 단일 대규모 Amazon EC2 인스턴스에서 실행됩니다. 애플리케이션은 단일 EC2 인스턴스에서 실행되는 MySQL 데이터베이스에 데이터를 저장합니다.

애플리케이션 서버 EC2 인스턴스의 CPU 사용률이 100%에 도달하는 경우가 많아 애플리케이션이 응답을 중지합니다. 회사는 인스턴스에 패치를 수동으로 설치합니다. 과거에는 패치 적용으로 인해 다운타임이 발생했습니다. 회사는 애플리케이션의 가용성을 높여야 합니다.

최소한의 개발로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 애플리케이션 계층을 기존 VPC의 AWS Lambda 함수로 이동합니다. Lambda 함수 전체에 트래픽을 분산시키기 위해 Application Load Balancer를 생성합니다. Amazon GuardDuty를 사용하여 Lambda 함수를 스캔합니다. 데이터베이스를 Amazon DocumentDB로 마이그레이션합니다 (MongoDB와 호환됩니다.
B. EC2 인스턴스 유형을 더 작은 Graviton 기반 인스턴스 유형으로 변경합니다. 기존 AMI를 사용하여 Auto Scaling 그룹에 대한 시작 템플릿을 생성합니다. Auto Scaling 그룹의 인스턴스 전체에 트래

픽을 분산시키기 위해 Application Load Balancer를 생성합니다. CPU 사용률에 따라 조정되도록 Auto Scaling 그룹을 설정합니다. 데이터베이스를 Amazon DynamoDB로 마이그레이션합니다.
C. Docker를 사용하여 애플리케이션 계층을 컨테이너로 이동합니다. EC2 인스턴스를 사용하여 Amazon Elastic Container Service(Amazon ECS)에서 컨테이너를 실행합니다. ECS 클러스터 전체에 트래픽을 분산시키기 위해 Application Load Balancer를 생성합니다. CPU 사용률에 따라 확장되도록 ECS 클러스터를 구성합니다. 데이터베이스를 Amazon Neptune으로 마이그레이션합니다.
D. AWS 시스템 관리자 에이전트(SSM 에이전트)로 구성된 Now AMI를 생성합니다. 새 AMI를 사용하여 Auto Scaling 그룹에 대한 시작 템플릿을 생성합니다. Auto Scaling 그룹에서 더 작은 인스턴스를 사용합니다. Auto Scaling 그룹의 인스턴스 전체에 트래픽을 분산시키기 위해 Application Load Balancer를 생성합니다. CPU 사용률에 따라 조정되도록 Auto Scaling 그룹을 설정합니다. 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다.

해설
정답: D
AWS Systems Manager를 이용하면 패치 설치를 자동화하여 장애를 줄일 수 있고, EC2 인스턴스 크기를 축소하고 Auto Scaling을 적용하여 CPU 과부하를 관리할 수 있습니다.
또한, 아마존 Aurora MySQL을 사용하게 되면 아마존의 고가용성이 제공하는 데이터베이스를 지원할 수 있어서 위의 요구사항을 모두 충족시킬 수 있습니다.
다른 해결책들은 람다 함수 또는 도커와 같은 새로운 기술을 도입하거나, 기존의 MySQL에서 DynamoDB나 Neptune과 같은 완전히 다른 종류의 데이터베이스 시스템으로 마이그레이션하는 것을 필요로 합니다. 이 작업들은 개발자들이 새로운 기술을 배우고 기존 코드를 크게 수정해야 하기 때문에 많은 개발 비용이 소요됩니다.

◆ | **Q#0300.** | **Ref#0300.**
한 회사에서 여러 애플리케이션을 AWS로 마이그레이션할 계획입니다. 회사는 전체 애플리케이션 자산을 제대로 이해하지 못하고 있습니다. 자산은 물리적 머신과 VM의 혼합으로 구성됩니다.

회사가 마이그레이션할 한 애플리케이션에는 대기 시간에 민감한 종속성이 많이 있습니다. 회사는 모든 종속성이 무엇인지 확신하지 못합니다. 그러나 회사는 지연 시간이 짧은 통신이 포트 1000에서 실행되는 사용자 지정 IP 기반 프로토콜을 사용한다는 것을 알고 있습니다. 회사는 애플리케이션과 이러한 종속성을 함께 마이그레이션하여 지연 시간이 짧은 모든 인터페이스를 동시에 AWS로 이동하려고 합니다.

회사는 AWS Application Discovery Agent를 설치하고 몇 달 동안 데이터를 수집해 왔습니다.

애플리케이션과 동일한 단계에서 마이그레이션해야 하는 종속성을 식별하려면 회사는 무엇을 해야 합니까?

A. AWS Migration Hub를 사용하고 애플리케이션을 호스팅하는 서버를 선택하십시오. 네트워크 그래프를 시각화하여 애플리케이션과 상호 작용하는 서버를 찾으세요. Amazon Athena에서 데이터 탐색을 활성화합니다. 서버 간에 전송되는 데이터를 쿼리하여 포트 1000에서 통신하는 서버를 식별합니다. Migration Hub로 돌아갑니다. Athena 쿼리 결과를 기반으로 이동 그룹을 만듭니다.
B. AWS Application Migration Service를 사용하고 애플리케이션을 호스팅하는 서버를 선택합니다. 네트워크 그래프를 시각화하여 애플리케이션과 상호 작용하는 서버를 찾으세요. 애플리케이션과 상호 작용하는 모든 서버에 대해 테스트 인스턴스를 시작하도록 Application Migration Service를 구성합니다. 테스트 인스턴스에 대한 승인 테스트를 수행합니다. 문제가 식별되지 않으면 테스트된 서버를 기반으로 이동 그룹을 만듭니다.
C. AWS Migration Hub를 사용하고 애플리케이션을 호스팅하는 서버를 선택합니다. 네트워크 액세스 분석기에서 데이터 탐색을 활성화합니다. 네트워크 액세스 분석기 콘솔을 사용하여 애플리케이션을 호스팅하는 서버를 선택합니다. 포트 1000의 네트워크 액세스 범위를 선택하고 일치하는 서버를 기록해 둡니다. 마이그레이션 허브로 돌아갑니다. Network Access Analyser의 결과를 기반으로 이동 그룹을 만듭니다.
D. AWS Migration Hub를 사용하고 애플리케이션을 호스팅하는 서버를 선택합니다. AWS Application Discovery Agent를 사용하여 Amazon CloudWalch 에이전트를 식별된 서버로 푸시합니다. 에이전트가 수집하는 CloudWatch 로그를 Amazon S3로 내보냅니다. Amazon Athena를 사용하

여 로그를 쿼리하여 포트 1000에서 통신하는 서버를 찾습니다. Migration Hub로 돌아가기 Athena 쿼리 결과를 기반으로 이동 그룹을 생성합니다.

해설
정답: A
회사는 몇달 동안 AWS Application Discovery Agent로 데이터를 수집한 상황이며, 애플리케이션과 함께 마이그레이션해야 하는 종속성을 식별해야 합니다.
AWS Migration Hub를 사용하여 애플리케이션을 호스팅하는 서버를 선택하고 네트워크 그래프를 시각화하여 상호 작용하는 서버를 찾습니다.
그리고 Amazon Athena를 사용하여 데이터를 쿼리하여 포트 1000에서 통신하는 서버를 확인하고, Migration Hub로 돌아가서 Athena 쿼리 결과를 기반으로 이동 그룹을 생성합니다. 이를 통해 애플리케이션과 함께 마이그레이션해야 하는 모든 종속성을 식별할 수 있습니다.
아키텍처 패턴은 데이터 탐색을 위한 Discovery Service + Migration Hub + Athena입니다.
B(x): AWS Application Migration Service는 리프트 앤 시프트용, 종속성 매핑용 아님
C(x): 온프레미스용이 아닌 AWS 리소스 전용 네트워크 액세스 분석기
D(x): CloudWatch 사용 사례 아님.