401 (정창화) 1회차 完

◆ | **Q#0401.** | **Ref#0401.**
회사는 회사 데이터 센터에서 실행되는 애플리케이션에 대한 재해 복구(DR) 솔루션을 설계하려고 합니다. 애플리케이션은 SMB 파일 공유에 쓰고 두 번째 파일 공유에 복사본을 만듭니다. 두 파일 공유는 모두 데이터 센터에 있습니다. 애플리케이션은 메타데이터 파일과 이미지 파일이라는 두 가지 유형의 파일을 사용합니다.

회사는 복사본을 AWS에 저장하려고 합니다. 회사는 재해가 발생할 경우 SMB를 사용하여 데이터 센터나 AWS의 데이터에 액세스할 수 있는 능력이 필요합니다. 데이터 사본은 거의 액세스되지 않지만 5분 이내에 사용 가능해야 합니다.

> **A.** Amazon S3 스토리지를 사용하여 AWS Outposts를 배포합니다. Outposts에서 Windows Amazon EC2 인스턴스를 파일 서버로 구성합니다.
> **B.** Amazon FSx 파일 게이트웨이를 배포합니다. SSD 스토리지를 사용하는 Windows 파일 서버 다중 AZ 파일 시스템용 Amazon FSx를 구성합니다.
> **C.** Amazon S3 파일 게이트웨이를 배포합니다. 메타데이터 파일에 Amazon S3 Standard-Infrequent Access(S3 Standard-IA)를 사용하고 이미지 파일에 S3 Glacier Deep Archive를 사용하도록 S3 파일 게이트웨이를 구성합니다.
> **D.** Amazon S3 파일 게이트웨이를 배포합니다. 메타데이터 파일 및 이미지 파일에 Amazon S3 Standard-Infrequent Access(S3 Standard-IA)를 사용하도록 S3 파일 게이트웨이를 구성합니다.
>
> 해설
> 정답: D
> Amazon S3 File Gateway는 온프레미스에서 NFS 또는 SMB 파일 공유로 접근할 수 있도록 제공. 5분 이내 접근 보장을 위해 S3 Standard-IA에 저장하는 것이 더 적합. 빈도는 낮지만 필요할 때 빠른 액세스 가능
> AWS Outposts는 매우 높은 비용이 들며 재해복구용으로 맞지 않음.
> Amazon FSx for Windows File Server는 고성능과 고가용성을 제공하며 재해복구용으로 맞지 않음.
> S3 Glacier Deep Archive는 복구 시간이 최대 12시간까지 걸릴 수 있음.

◆ | **Q#0402.** | **Ref#0402.**
한 회사에서는 예상치 못한 재해가 발생할 경우 400명의 직원을 원격 근무 환경으로 이동할 수 있는 솔루션을 만들고 있습니다. 사용자 데스크탑에는 Windows와 Linux 운영 체제가 혼합되어 있습니다. 웹 브라우저, 메일 클라이언트 등 다양한 유형의 소프트웨어가 각 데스크톱에 설치됩니다.

솔루션 설계자는 직원이 기존 ID 자격 증명을 사용할 수 있도록 회사의 온프레미스 Active Directory와 통합할 수 있는 솔루션을 구현해야 합니다. 솔루션은 다중 인증(MFA)을 제공해야 하며 기존 데스크탑의 사용자 경험을 복제해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 클라우드 데스크톱 서비스에는 Amazon WorkSpaces를 사용하십시오. 온프레미스 네트워크에 대한 VPN 연결을 설정합니다. AD 커넥터를 생성하고 온프레미스 Active Directory에 연결합니다. AWS Management Console을 사용하여 Amazon WorkSpaces에 대한 MFA를 활성화합니다.
> **B.** Amazon AppStream 2.0을 애플리케이션 스트리밍 서비스로 사용하십시오. 직원을 위한 데스크탑 보기를 구성하십시오. 온프레미스 네트워크에 대한 VPN 연결을 설정합니다. 온프레미스에 AD FS(Active Directory Federation Services)를 설정합니다. VPN 연결을 통해 VPC 네트워크를 AD FS에 연결합니다.
> **C.** 클라우드 데스크톱 서비스에는 Amazon WorkSpaces를 사용하십시오. 온프레미스 네트워크에 대한 VPN 연결을 설정합니다. AD 커넥터를 생성하고 온프레미스 Active Directory에 연결합니다. MFA용 RADIUS 서버를 구성합니다.
> **D.** Amazon AppStream 2.0을 애플리케이션 스트리밍 서비스로 사용하십시오. 온프레미스에 Active

Directory Federation Services를 설정합니다. AppStream 2.0에 대한 사용자 액세스 권한을 부여하도록 MFA를 구성합니다.

해설
정답: C
Amazon WorkSpaces: 사용자가 원격에서 데스크톱을 사용할 수 있게 하는 클라우드 데스크톱 서비스.
AD Connector를 통해 온프레미스 Active Directory에 연결하여 기존 자격 증명을 사용할 수 있게 함.
RADIUS(Remote Authentication Dial-In User Service) 서버를 사용하여 다중 인증(MFA)을 구성할 수 있고, VPN 연결을 통해 온프레미스 네트워크와의 보안을 유지할 수 있음.

◆ | **Q#0403.** | **Ref#0403.**
회사는 Amazon Connect 컨택트 센터를 배포했습니다. 컨택트 센터 상담원은 컴퓨터에서 생성된 수많은 통화를 보고하고 있습니다. 회사는 이러한 통화로 인한 비용 및 생산성 영향을 우려하고 있습니다. 회사는 상담원이 해당 통화를 스팸으로 표시하고 향후 상담원에게 전달되는 번호를 자동으로 차단할 수 있는 솔루션을 원합니다.

이러한 요구 사항을 충족하는 가장 운영 효율적인 솔루션은 무엇입니까?

A. Contact Control Panel (CCP)을 사용자 지정하여 호출 플래그 버튼을 추가하고, 이 버튼이 AWS Lambda 함수를 호출하여 UpdateContactAttributes API를 호출하도록 합니다. 스팸 번호를 저장하는 Amazon DynamoDB 테이블을 사용합니다. 연락처 흐름을 수정하여 업데이트된 속성을 확인하고, Lambda 함수를 사용하여 DynamoDB 테이블을 읽고 쓰도록 합니다.
B. Contact Lens for Amazon Connect 규칙을 사용하여 스팸 전화를 확인합니다. 스팸 번호를 저장하는 Amazon DynamoDB 테이블을 사용합니다. 연락처 흐름을 수정하여 규칙을 확인하고, AWS Lambda 함수를 호출하여 DynamoDB 테이블을 읽고 쓰도록 합니다.
C. 스팸 번호를 저장하는 Amazon DynamoDB 테이블을 사용합니다. 에이전트가 Contact Control Panel (CCP)에서 스팸 전화를 전달할 수 있는 빠른 연결을 만듭니다. 빠른 연결 연락처 흐름을 수정하여 AWS Lambda 함수를 호출하여 DynamoDB 테이블에 기록하도록 합니다.
D. 초기 연락처 흐름을 수정하여 호출자 입력을 요청합니다. 에이전트가 입력을 받지 못하면, 에이전트는 호출자를 스팸으로 표시해야 합니다. 스팸 번호를 저장하는 Amazon DynamoDB 테이블을 사용합니다. AWS Lambda 함수를 사용하여 DynamoDB 테이블을 읽고 쓰도록 합니다.

해설
정답: A
CCP(Contact Control Panel) 사용자 지정을 통해 에이전트가 스팸 전화를 직접 플래그할 수 있어 간편하게 관리할 수 있음.
Lambda 함수를 사용하여 스팸 전화 속성을 업데이트하고 DynamoDB 테이블에 저장할 수 있으며 실시간 처리 및 저장이 가능.

◆ | **Q#0404.** | **Ref#0404.**
회사는 모든 공장에서 습도 및 조명과 같은 환경 매개 변수를 수집하는 센서를 설치했습니다. 회사는 AWS 클라우드에서 실시간으로 데이터를 스트리밍하고 분석해야 합니다. 매개 변수가 허용 범위를 벗어나면 공장 운영 팀이 즉시 알림을 받아야 합니다.

요구 사항을 충족하는 솔루션은 무엇입니까?

A. 데이터를 Amazon Kinesis Data Firehose 전송 스트림으로 스트리밍합니다. AWS Step Functions를 사용하여 Kinesis Data Firehose 전송 스트림의 데이터를 사용하고 분석합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 운영팀에 알립니다.
B. 데이터를 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 클러스터로 스트리밍합니다. Amazon MSK에서 트리거를 설정하여 AWS Fargate 작업을 호출하여 데이터를 분석합니다. Amazon Simple Email Service(Amazon SES)를 사용하여 운영 팀에 알립니다.
C. 데이터를 Amazon Kinesis 데이터 스트림으로 스트리밍합니다. Kinesis 데이터 스트림을 사용하고 데이터를 분석하는 AWS Lambda 함수를 생성합니다. Amazon Simple 알림 서비스(Amazon SNS)를

사용하여 운영팀에 알립니다.
D. 데이터를 Amazon Kinesis Data Analytics 애플리케이션으로 스트리밍합니다. Amazon Elastic Container Service(Amazon ECS)에서 자동으로 확장되고 컨테이너화된 서비스를 사용하여 데이터를 사용하고 분석합니다. Amazon Simple Email Service(Amazon SES)를 사용하여 운영 팀에 알립니다.

해설
정답: C
Amazon Kinesis 데이터 스트림은 고속 데이터 스트리밍을 처리할 수 있으며, AWS Lambda 함수는 실시간으로 데이터를 처리하고 분석하는 데 최적화됨.
Amazon SNS는 운영 팀에 신속하게 실시간 알림을 보낼 수 있음.
이 솔루션은 간단하고 효율적이며, 실시간 데이터 분석 및 알림에 적합.

◆ | **Q#0405.** | **Ref#0405.**
회사는 작업 부하를 지원하기 위해 Amazon Elastic Kubernetes Service (Amazon EKS) 클러스터를 배포할 준비를 하고 있습니다. 회사는 클러스터가 예측할 수 없는 수의 상태 비저장 포드를 지원할 것으로 예상하고 있습니다. 많은 포드가 짧은 시간 동안 생성될 것이며, 이는 작업 부하가 사용하는 복제본 수를 자동으로 조정함에 따라 발생합니다.

노드 탄력성을 최대화하는 솔루션은 무엇입니까?

A. 별도의 시작 템플릿을 사용하여 워크로드 노드 그룹과 별개인 두 번째 클러스터에 EKS 제어 플레인을 배포합니다.
B. 워크로드 노드 그룹을 업데이트합니다. 더 적은 수의 노드 그룹과 더 큰 인스턴스를 노드 그룹에 사용하세요.
C. 워크로드 노드 그룹의 컴퓨팅 용량이 부족하게 프로비저닝되도록 Kubernetes Cluster Autoscaler를 구성합니다.
D. 가용 영역을 기반으로 하는 토폴로지 분산 제약 조건을 사용하도록 워크로드를 구성합니다.

해설
정답: D
토폴로지 분산 제약 조건을 사용하여 여러 가용 영역에 걸쳐 포드를 분산시키는 것은 클러스터의 고가용성과 노드 탄력성을 극대화하는 데 중요한 역할을 함.
A(x): 제어 플레인을 별도의 클러스터에 배포하는 것은 보안 및 관리의 측면에서 유용할 수 있지만, 노드 탄력성 문제를 해결하지 못함.
B(x): 더 큰 인스턴스 사용은 오히려 노드 탄력성을 감소시킬 수 있음.
C(x): 컴퓨팅 용량이 부족하게 구성하는 것은 리소스가 부족하게 유지될 수 있어 실질적으로 클러스터의 탄력성을 감소시킬 수 있음.

◆ | **Q#0406.** | **Ref#0406.**
회사는 웹 애플리케이션에 대한 재해 복구(DR) 계획을 구현해야 합니다. 애플리케이션은 단일 AWS 리전에서 실행됩니다.

애플리케이션은 컨테이너에서 실행되는 마이크로서비스를 사용합니다. 컨테이너는 Amazon Elastic Container Service(Amazon ECS)의 AWS Fargate에서 호스팅됩니다. 애플리케이션에는 데이터 계층으로 MySQL용 Amazon RDS DB 인스턴스가 있고 DNS 확인을 위해 Amazon Route 53을 사용합니다. 애플리케이션에 오류가 발생하면 Amazon CloudWatch 경보는 Amazon EventBridge 규칙을 호출합니다.

솔루션 설계자는 별도의 지역에 애플리케이션 복구를 제공하도록 DR 솔루션을 설계해야 합니다. 솔루션은 오류로부터 복구하는 데 필요한 시간을 최소화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 별도 리전의 Fargate에 두 번째 ECS 클러스터와 ECS 서비스를 설정합니다. 다음 작업을 수행하는 AWS Lambda 함수를 생성합니다. RDS DB 인스턴스의 스냅샷 생성, 스냅샷을 별도의 리전에 복사, 스냅샷에서 새 RDS DB 인스턴스 생성, Route 53을 업데이트하여 트래픽을 두 번째 ECS 클러스터로

라우팅. EventBridge 규칙을 업데이트하여 Lambda 함수를 호출할 대상을 추가합니다.
B. 별도의 리전에 두 번째 ECS 클러스터와 ECS 서비스를 생성하는 AWS Lambda 함수를 생성합니다. 다음 작업을 수행하도록 Lambda 함수를 구성합니다. RDS DB 인스턴스의 스냅샷을 만들고, 스냅샷을 별도의 리전에 복사하고, 스냅샷에서 새 RDS DB 인스턴스를 생성하고, Route 53을 업데이트하여 두 번째 ECS 클러스터로 트래픽을 라우팅합니다. EventBridge 규칙을 업데이트하여 Lambda 함수를 호출할 대상을 추가합니다.
C. 별도 리전의 Fargate에 두 번째 ECS 클러스터와 ECS 서비스를 설정합니다. 별도의 리전에서 RDS DB 인스턴스의 리전 간 읽기 전용 복제본을 생성합니다. 읽기 전용 복제본을 기본 데이터베이스로 승격하는 AWS Lambda 함수를 생성합니다. Route 53을 업데이트하여 두 번째 ECS 클러스터로 트래픽을 라우팅하도록 Lambda 함수를 구성합니다. EventBridge 규칙을 업데이트하여 Lambda 함수를 호출할 대상을 추가합니다.
D. 별도 리전의 Fargate에 두 번째 ECS 클러스터와 ECS 서비스를 설정합니다. RDS DB 인스턴스의 스냅샷을 찍습니다. 스냅샷을 Amazon DynamoDB 전역 테이블로 변환합니다. 두 번째 ECS 클러스터로 트래픽을 라우팅하도록 Route 53을 업데이트하는 AWS Lambda 함수를 생성합니다. EventBridge 규칙을 업데이트하여 Lambda 함수를 호출할 대상을 추가합니다.

해설
정답: C
C: RDS 읽기전용 복제본 승격 및 Route 53 업데이트에 소요되는 시간이 훨씬 짧으며, 요구 사항을 충족함.
A(x), B(x): 스냅샷을 통해 RDS DB 생성은 비교적 시간이 오래 걸리는 프로세스, DR에서 빠른 회복이 필요하므로 이 솔루션은 적합하지 않음.
D(x): 스냅샷은 A,B 와 동일한 단점을 가지며, 요구사항을 충족하지 않음.

◆ | **Q#0407.** | **Ref#0407.**
회사에는 AWS Organizations의 조직에 속한 AWS 계정이 있습니다. 회사는 Amazon EC2 사용량을 지표로 추적하려고 합니다. 회사의 아키텍처 팀은 EC2 사용량(Usage)이 지난 30일 동안의 평균 EC2 사용량보다 10% 이상 높은 경우 매일 알림을 받아야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 조직의 마스터 계정에서 AWS Budgets을 구성합니다. EC2 실행 시간의 사용 유형을 지정합니다. 일일 기간을 지정합니다. AWS Cost Explorer에서 지난 30일 동안 보고된 평균 사용량보다 10% 더 높게 예산 금액을 설정합니다. 사용량 임계값이 충족되면 아키텍처 팀에 알리도록 경고를 구성합니다.
B. 조직의 마스터 계정에서 AWS Cost Anomaly Detection을 구성합니다. AWS 서비스의 모니터 유형을 구성합니다. Amazon EC2 필터를 적용합니다. 사용량이 지난 30일 동안의 평균 사용량보다 10% 많은 경우 아키텍처 팀에 알리도록 경고 구독을 구성합니다.
C. 조직의 마스터 계정에서 AWS Trusted Advisor를 활성화합니다. EC2 사용량이 지난 30일 동안 보고된 평균 사용량보다 10% 더 많은 경우 아키텍처 팀에 알리도록 비용 최적화 권고 경고를 구성합니다.
D. 조직의 마스터 계정에서 Amazon Detective를 구성합니다. Detective가 10%가 넘는 사용 이상을 식별한 경우 아키텍처 팀에 알리도록 EC2 사용 이상 경고를 구성합니다.

해설
정답: A
AWS Budgets은 AWS 비용 및 사용량을 추적하고 조치를 취할 수 있도록 합니다.
EC2 실행 시간과 같은 사용 유형을 지정하고, 지난 30일 동안의 평균 사용량보다 10% 더 높은 일일 예산을 설정, EC2 사용이 10% 이상 증가하면 아키텍처 팀에 즉시 알림을 보내도록 설정.
B: AWS 비용 이상 탐지(AWS Cost Anomaly Detection)는 AWS 비용 및 사용량 패턴의 이상을 모니터링하는 데 사용, 특정 EC2 사용 지표를 추적하고 특정 임계값에 따라 경고를 생성하는 데에는 부적합.

◆ | **Q#0408.** | **Ref#0408.**
한 전자 상거래 회사는 IT 인프라를 개편하고 있으며 AWS 서비스를 사용할 계획입니다. 회사의 CIO는 솔루션 설계자에게 간단하고 가용성이 높으며 느슨하게 결합된 주문 처리 애플리케이션을 설계해 달라고 요청했습니다. 애플리케이션은 주문을 Amazon DynamoDB 테이블에 저장하기 전에 수신하고 처리하는 역할을 담당합니다. 애플리케이션에는 산발적인 트래픽 패턴이 있으며 마케팅 캠페인 중에 확장하여 지연을 최소화하면서 주문을 처리할 수 있어야 합니다.

다음 중 요구 사항을 충족하기 위한 가장 신뢰할 수 있는 접근 방식은 무엇입니까?

> **A.** Amazon EC2 호스팅 데이터베이스에서 주문을 받고 EC2 인스턴스를 사용하여 처리합니다.
> **B.** Amazon SQS 대기열에서 주문을 받고 AWS Lambda 함수를 호출하여 처리합니다.
> **C.** AWS Step Functions 프로그램을 사용하여 주문을 받고 Amazon ECS 컨테이너를 시작하여 처리합니다.
> **D.** Amazon Kinesis Data Streams에서 주문을 받고 Amazon EC2 인스턴스를 사용하여 처리합니다.
>
> 해설
> 정답: B
> Amazon SQS 대기열에서 주문을 수신하고 AWS Lambda 함수를 호출하여 처리합니다.
> Amazon SQS는 간단한 대기열 서비스이며, 높은 가용성을 제공, 복잡한 구성 없이 신속하게 구현할 수 있음.
> AWS Lambda를 사용하면 서버리스 아키텍처를 구축하여 응용 프로그램을 느슨하게 결합할 수 있음.
> 주문량이 증가할 때 AWS Lambda는 자동으로 스케일링되어 요청을 처리하는 데 필요한 컴퓨팅 리소스를 제공하여 마케팅 캠페인과 같은 주문이 증가하는 이벤트에 대비가능.

◆ | **Q#0409.** | **Ref#0409.**
한 회사가 PostgreSQL용 Amazon RDS 데이터베이스에 액세스하는 AWS Lambda 함수를 배포하고 있습니다. 회사는 QA 환경과 프로덕션 환경에서 Lambda 기능을 시작해야 합니다.

회사는 애플리케이션 코드 내에서 자격 증명을 노출해서는 안 되며 비밀번호를 자동으로 교체해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 양 환경에 대한 데이터베이스 자격 증명을 AWS Systems Manager Parameter Store에 저장합니다. AWS Key Management Service (AWS KMS) 키를 사용하여 자격 증명을 암호화합니다. Lambda 함수의 응용 프로그램 코드 내에서 AWS SDK for Python (Boto3)를 사용하여 Parameter Store 매개변수에서 자격 증명을 가져옵니다. Lambda 함수에 역할을 추가하여 Parameter Store 매개변수에 액세스합니다.
> **B.** 양 환경에 대한 데이터베이스 자격 증명을 AWS Secrets Manager에 저장하고 QA 환경과 프로덕션 환경에 대해 별도의 키 항목을 사용합니다. 회전을 켭니다. Lambda 함수에 대한 환경 변수로 Secrets Manager 키에 대한 참조를 제공합니다.
> **C.** 양 환경에 대한 데이터베이스 자격 증명을 AWS Key Management Service (AWS KMS)에 저장합니다. 회전을 켭니다. Lambda 함수에 대한 환경 변수로 AWS KMS에 저장된 자격 증명에 대한 참조를 제공합니다.
> **D.** QA 환경과 프로덕션 환경에 대해 별도의 S3 버킷을 만듭니다. S3 버킷에 AWS KMS 키 (SSE-KMS)로 서버 측 암호화를 켭니다. Lambda 함수의 응용 프로그램 코드가 해당 환경에 해당하는 함수의 올바른 자격 증명을 가져올 수 있도록 객체 이름 패턴을 사용합니다. 각 Lambda 함수의 실행 역할에 Amazon S3 액세스 권한을 부여합니다.
>
> 해설
> 정답: B
> AWS Secrets Manager는 안전한 방법으로 자격 증명을 저장하고 회전시킬 수 있는 서비스.
> 암호 자동 교체 -> AWS Secrets Manager
> Lambda 함수는 환경 변수를 통해 Secrets Manager에 저장된 자격 증명을 손쉽게 액세스 가능.

◆ | **Q#0410.** | **Ref#0410.**
한 회사가 AWS Control Tower를 사용하여 AWS Organizations에 속한 조직의 AWS 계정을 관리하고 있습니다. 회사에는 계정이 포함된 조직 단위(OU)가 있습니다. 회사는 OU의 계정에서 새로운 또는 기존의 Amazon EC2 인스턴스가 Public IP 주소를 획득하는 것을 방지해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** AWS 시스템 관리자를 사용하도록 OU의 각 계정에 있는 모든 인스턴스를 구성합니다. 시스템 관리자 자동화 Runbook을 사용하여 Public IP 주소가 인스턴스에 연결되는 것을 방지합니다.
> **B.** OU 계정의 인스턴스에 Public IP 주소가 있는지 확인하기 위해 AWS Control Tower 사전 제어를 구현합니다. AssociatePublicIpAddress 속성을 False로 설정합니다. OU에 사전 제어를 연결합니다.
> **C.** Public IP 주소가 있는 인스턴스의 시작을 방지하는 SCP를 생성합니다. 또한 기존 인스턴스에 Public IP 주소가 연결되지 않도록 SCP를 구성합니다. SCP를 OU에 연결합니다.
> **D.** Public IP 주소가 있는 인스턴스를 감지하는 AWS Config 사용자 지정 규칙을 생성합니다. AWS Lambda 함수를 사용하여 인스턴스에서 Public IP 주소를 분리하는 해결 작업을 구성합니다.
>
> 해설
> 정답: C
> Public IP 주소가 있는 인스턴스의 시작을 방지하는 SCP(Service Control Policies)를 사용하면 조직 단위 또는 계정 전체에 정책을 적용할 수 있으며,
> OU에 SCP를 연결하여 EC2 인스턴스에서 Public IP 주소의 획득을 제어할 수 있음.
> AWS Control Tower를 사용하여 조직을 관리하는 경우, 조직 단위(OU)를 사용하여 정책을 적용할 수 있음.

411 (정창화) 2회차 完

◆ | **Q#0411.** | **Ref#0411.**
한 회사가 AWS에 타사 웹 애플리케이션을 배포하고 있습니다. 애플리케이션은 Docker 이미지로 패키지됩니다. 회사는 Docker 이미지를 Amazon Elastic Container Service(Amazon ECS)에 AWS Fargate 서비스로 배포했습니다. ALB(Application Load Balancer)는 트래픽을 애플리케이션으로 전달합니다.

회사는 특정 사용자 목록에만 인터넷에서 애플리케이션에 액세스할 수 있는 기능을 제공해야 합니다. 회사는 애플리케이션을 변경할 수 없으며 애플리케이션을 ID 공급자와 통합할 수도 없습니다. 모든 사용자는 다단계 인증(MFA)을 통해 인증되어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** Amazon Cognito에서 사용자 풀을 생성합니다. 애플리케이션에 대한 풀을 구성합니다. 필요한 사용자로 풀을 채웁니다. MFA를 요구하도록 풀을 구성합니다. Amazon Cognito 호스팅 UI를 통해 인증을 요구하도록 ALB에서 리스너 규칙을 구성합니다.
> **B.** AWS Identity and Access Management(IAM)에서 사용자를 구성합니다. 사용자가 MFA를 사용하도록 요구하려면 Fargate 서비스에 리소스 정책을 연결합니다. IAM을 통한 인증을 요구하도록 ALB에서 리스너 규칙을 구성합니다.
> **C.** AWS Identity and Access Management(IAM)에서 사용자를 구성합니다. AWS IAM ID 센터(AWS Single Sign-On)를 활성화합니다. ALB에 대한 리소스 보호를 구성합니다. 사용자가 MFA를 사용하도록 요구하는 리소스 보호 규칙을 만듭니다.
> **D.** AWS Amplify에서 사용자 풀을 생성합니다. 애플리케이션에 대한 풀을 구성합니다. 필요한 사용자로 풀을 채웁니다. MFA를 요구하도록 풀을 구성합니다. Amplify 호스팅 UI를 통해 인증을 요구하도록 ALB에서 리스너 규칙을 구성합니다.
>
> 해설
> 정답: A
> Amazon Cognito는 사용자 인증 및 권한 부여를 위한 완전 관리형 서비스.

Amazon Cognito를 사용하여 사용자 풀을 생성하고, 해당 풀을 MFA를 필요로 하도록 구성 가능.
그런 다음 ALB에 대한 리스너 규칙을 구성하여 요청된 사용자에 대해서만 Amazon Cognito 호스팅 UI를 통해 인증을 요구할 수 있도록 함.

◆ | **Q#0412.** | **Ref#0412.**
솔루션 아키텍트는 이전에 사용되지 않았던 여러 AWS 리전에 새 보안 도구를 배포할 예정입니다. 솔루션 아키텍트는 AWS CloudFormation 스택 세트를 사용하여 도구를 배포할 것입니다. 스택 세트의 템플릿에는 사용자 지정 이름을 가진 IAM 역할이 포함되어 있습니다. 스택 세트를 생성하면 스택 인스턴스가 성공적으로 생성되지 않습니다.

스택을 성공적으로 배포하려면 솔루션 설계자가 무엇을 해야 합니까?

A. 모든 관련 계정에서 새 리전을 활성화합니다. 스택 세트 생성 중에 CAPABILITY_NAMED_IAM 기능을 지정합니다.
B. Service Quotas 콘솔을 사용하여 모든 관련 계정에서 새 리전에 대한 CloudFormation 스택 수 증가를 요청하십시오. 스택 세트 생성 중에 CAPABILITY_IAM 기능을 지정합니다.
C. 스택 세트 생성 중에 CAPABILITY_NAMED_IAM 기능과 SELF_MANAGED 권한 모델을 지정합니다.
D. 스택 세트 생성 중에 관리 역할 ARN 및 CAPABILITY_IAM 기능을 지정합니다.

해설
정답: A
솔루션 아키텍트는 모든 관련 계정에서 새로운 리전을 활성화해야 합니다.
또한 사용자 정의 이름을 가진 IAM에 대한 CAPABILITY_NAMED_IAM 기능을 스택 세트 생성 중에 지정해야 합니다.
이렇게 하면 CloudFormation이 사용자 지정 IAM 역할을 생성할 수 있습니다.

◆ | **Q#0413.** | **Ref#0413.**
회사에는 애플리케이션 데이터베이스로 Amazon Aurora PostgreSQL DB 클러스터를 사용하는 애플리케이션이 있습니다. DB 클러스터에는 하나의 작은 기본 인스턴스와 세 개의 큰 복제본 인스턴스가 포함되어 있습니다. 애플리케이션은 AWS Lambda 함수에서 실행됩니다. 애플리케이션은 읽기 전용 작업을 수행하기 위해 데이터베이스의 복제본 인스턴스에 대한 단기 연결을 여러 개 만듭니다.

트래픽이 많은 기간에는 애플리케이션이 불안정해지고 데이터베이스에서 너무 많은 연결이 설정되고 있다고 보고합니다. 트래픽이 많은 기간의 빈도는 예측할 수 없습니다.

애플리케이션의 안정성을 향상시키는 솔루션은 무엇입니까?

A. Amazon RDS 프록시를 사용하여 DB 클러스터용 프록시를 생성합니다. 프록시에 대한 읽기 전용 엔드포인트를 구성합니다. 프록시 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
B. DB 클러스터의 파라미터 그룹에서 max_connections 설정을 늘립니다. DB 클러스터의 모든 인스턴스를 재부팅합니다. DB 클러스터 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
C. DatabaseConnections 지표가 최대 연결 설정에 가까울 때 발생하도록 DB 클러스터에 대한 인스턴스 조정을 구성합니다. Aurora 리더 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
D. Amazon RDS 프록시를 사용하여 DB 클러스터용 프록시를 생성합니다. 프록시에서 Aurora 데이터 API에 대한 읽기 전용 엔드포인트를 구성합니다. 프록시 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.

해설
정답: A
Lambda -> rds-proxy -> Aurora 복제본 읽기 전용 엔드포인트 Amazon RDS Proxy를 사용하면 DB 연결을 관리하고 최적화할 수 있어 Lambda 함수가 DB 연결을 보다 효율적으로 관리가능.
RDS Proxy는 연결 풀링을 제공하므로 너무 많은 연결이 동시에 설정되는 문제를 해결.
RDS Proxy에 대한 읽기 전용 엔드포인트를 구성함으로써, Lambda 함수는 복제본 인스턴스에 효과적으로 접근하여 애플리케이션 안정성 향상됨.

◆ | **Q#0414.** | **Ref#0414.**
한 소매업체가 전 세계 모든 매장에 IoT 센서를 탑재하고 있습니다. 각 센서를 제조하는 동안 회사의 사설 인증 기관(CA)은 고유 일련 번호가 포함된 X.509 인증서를 발급합니다. 그런 다음 회사는 각 인증서를 해당 센서에 배포합니다.

솔루션 아키텍트는 센서가 설치된 후 AWS로 데이터를 전송할 수 있는 기능을 센서에 부여해야 합니다. 센서는 설치될 때까지 AWS로 데이터를 보낼 수 없어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 일련번호를 검증할 수 있는 AWS Lambda 함수를 생성합니다. AWS IoT Core 프로비저닝 템플릿을 생성합니다. 매개변수 섹션에 SerialNumber 매개변수를 포함합니다. Lambda 함수를 사전 프로비저닝 후크로 추가합니다. 제조 중에 RegisterThing API 작업을 호출하고 템플릿과 매개변수를 지정합니다.
> **B.** 일련 번호를 확인할 수 있는 AWS Step Functions 상태 머신을 생성합니다. AWS IoT Core 프로비저닝 템플릿을 생성합니다. 매개변수 섹션에 SerialNumber 매개변수를 포함합니다. 매개변수를 검증하려면 Step Functions 상태 시스템을 지정하세요. 설치 중에 StartThingRegistrationTask API 작업을 호출합니다.
> **C.** 일련번호를 검증할 수 있는 AWS Lambda 함수를 생성합니다. AWS IoT Core 프로비저닝 템플릿을 생성합니다. 매개변수 섹션에 SerialNumber 매개변수를 포함합니다. Lambda 함수를 사전 프로비저닝 후크로 추가합니다. AWS IoT Core에 CA를 등록하고, 프로비저닝 템플릿을 지정하고, Allow-auto-registration 매개변수를 설정합니다.
> **D.** AWS IoT Core 프로비저닝 템플릿을 생성합니다. 매개변수 섹션에 SerialNumber 매개변수를 포함합니다. 템플릿에 매개변수 검증을 포함합니다. CA를 사용하는 각 장치에 대해 청구 인증서와 개인 키를 프로비저닝합니다. 프로비저닝 중에 AWS IoT 사물을 업데이트할 수 있는 AWS IoT Core 서비스 권한을 부여합니다.
>
> 해설
> 정답: C
> AWS IoT Core의 사전 프로비저닝 후크(pre-provisioning hook) 기능을 사용하여 일련 번호를 검증할 수 있는 Lambda 함수를 만들고, 이를 통해 각 센서가 설치될 때까지 AWS에 데이터를 전송할 수 없도록 설정.
> Lambda 함수를 사전 프로비저닝 후크로 추가하여 센서가 설치되기 전에는 AWS IoT Core에 등록되지 않도록 할 수 있음.
> CA를 AWS IoT Core에 등록하고 프로비저닝 템플릿을 지정함으로써, 센서의 인증서가 신뢰할 수 있는 CA에 의해 발급되었음을 보장할 수 있음.
> allow-auto-registration 매개변수를 설정하여 인증서가 유효하고 설치가 완료된 센서만 자동으로 등록되도록 할 수 있음.

◆ | **Q#0415.** | **Ref#0415.**
한 스타트업 회사는 최근 대규모 전자 상거래 웹사이트를 AWS로 마이그레이션했습니다. 웹사이트 매출이 70% 증가했습니다. 소프트웨어 엔지니어는 개인 GitHub 저장소를 사용하여 코드를 관리하고 있습니다. DevOps 팀은 빌드 및 단위 테스트에 Jenkins를 사용하고 있습니다. 엔지니어는 배포 중에 잘못된 빌드와 가동 중지 시간에 대한 알림을 받아야 합니다. 또한 엔지니어는 프로덕션 변경 사항이 사용자에게 원활하게 전달되고 중대한 문제가 발생할 경우 롤백될 수 있는지 확인해야 합니다.

소프트웨어 엔지니어는 AWS CodePipeline을 사용하여 빌드 및 배포 프로세스를 관리하기로 결정했습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** GitHub 웹소켓을 사용하여 CodePipeline 파이프라인을 트리거하십시오. AWS CodeBuild용 Jenkins 플러그인을 사용하여 단위 테스트를 수행합니다. 잘못된 빌드에 대해 Amazon SNS 토픽에 알림을 보냅니다. AWS CodeDeploy를 사용하여 전체 동시 배포 구성으로 배포합니다.
> **B.** GitHub 웹훅을 사용하여 CodePipeline 파이프라인을 트리거합니다. AWS CodeBuild용 Jenkins 플

러그인을 사용하여 단위 테스트를 수행합니다. 잘못된 빌드에 대해 Amazon SNS 토픽에 알림을 보냅니다. AWS CodeDeploy를 사용하여 블루/그린 배포로 배포합니다.
C. GitHub 웹소켓을 사용하여 CodePipeline 파이프라인을 트리거합니다. 단위 테스트 및 정적 코드 분석에 AWS X-Ray를 사용하십시오. 잘못된 빌드에 대해 Amazon SNS 토픽에 알림을 보냅니다. AWS CodeDeploy를 사용하여 블루/그린 배포로 배포합니다.
D. GitHub 웹훅을 사용하여 CodePipeline 파이프라인을 트리거합니다. 단위 테스트 및 정적 코드 분석에 AWS X-Ray를 사용하십시오. 잘못된 빌드에 대해 Amazon SNS 토픽에 알림을 보냅니다. AWS CodeDeploy를 사용하여 전체 동시 배포 구성으로 배포합니다.

해설
정답: B
GitHub 웹훅을 사용하여 코드 변경 사항이 있을 때마다 CodePipeline을 트리거할 수 있으며, 웹소켓보다 설정이 더 간단하고 안정적임.
Jenkins 플러그인을 사용하여 AWS CodeBuild에서 단위 테스트를 수행.
빌드 실패 시 알림을 받기 위해 Amazon SNS를 사용.
AWS CodeDeploy를 사용하여 블루/그린 배포를 수행하면 배포 중에 다운타임이 발생하지 않으며, 문제가 발생할 경우 쉽게 롤백가능. 이는 제로 다운타임 배포와 롤백 요구 사항을 충족.
AWS X-Ray는 단위 테스트가 아닌 디버깅을 위한 것

◆ | **Q#0416.** | **Ref#0416.**
소프트웨어 서비스(SaaS) 회사가 다중 테넌트 환경을 개발했습니다. 회사는 스토리지 계층에 대해 테넌트가 공유하는 Amazon DynamoDB 테이블을 사용합니다. 회사는 애플리케이션 서비스를 위해 AWS Lambda 함수를 사용합니다.

회사는 각 테넌트의 리소스 소비를 기반으로 한 계층형 구독 모델을 제공하고자 합니다. 각 테넌트는 Lambda 함수에 요청의 일부로 전송되는 고유한 테넌트 ID로 식별됩니다. 회사는 AWS 계정에서 AWS Cost and Usage Report(AWS CUR)를 생성했습니다. 회사는 각 테넌트의 리소스 소비에 맞춰 DynamoDB 비용을 각 테넌트에 할당하고자 합니다.

가장 적은 운영 노력으로 각 테넌트에 대한 DynamoDB 비용을 세밀하게 파악할 수 있는 솔루션은 무엇입니까?

A. DynamoDB의 각 테이블에 테넌트 ID라는 새 태그를 연결합니다. AWS Billing and Cost Management 콘솔에서 비용 할당 태그로 태그를 활성화합니다. 테넌트 ID를 Amazon CloudWatch Logs에 기록하도록 새 Lambda 함수 코드를 배포합니다. AWS CUR을 사용하여 각 테넌트 ID에 대한 DynamoDB 소비 비용을 분리합니다.
B. Lambda 함수가 각 트랜잭션에 대해 테넌트 ID와 DynamoDB에서 소비된 RCU 및 WCU를 Amazon CloudWatch Logs에 기록하도록 구성합니다. 로깅된 용량 단위와 AWS Cost Explorer API의 전체 DynamoDB 비용을 사용하여 테넌트 비용을 계산하는 또 다른 Lambda 함수를 배포합니다. Amazon EventBridge 규칙을 생성하여 일정에 따라 계산 Lambda 함수를 호출합니다.
C. DynamoDB 항목을 개별 테넌트와 연결하는 새 파티션 키를 생성합니다. 각 트랜잭션의 일부로 새 열을 채우기 위해 Lambda 함수를 배포합니다. Amazon Athena를 사용하여 DynamoDB의 테넌트 항목 수와 AWS CUR의 전체 DynamoDB 비용을 계산하는 또 다른 Lambda 함수를 배포합니다. Amazon EventBridge 규칙을 생성하여 일정에 따라 계산 Lambda 함수를 호출합니다.
D. 테넌트 ID, 각 응답의 크기 및 트랜잭션 호출 시간을 사용자 정의 메트릭으로 Amazon CloudWatch Logs에 기록하는 Lambda 함수를 배포합니다. CloudWatch Logs Insights를 사용하여 각 테넌트에 대한 사용자 정의 메트릭을 쿼리합니다. AWS Pricing Calculator를 사용하여 전체 DynamoDB 비용을 얻고 테넌트 비용을 계산합니다.

해설
정답: B
테넌트 ID와 각 트랜잭션에서 소비된 RCU 및 WCU를 Amazon CloudWatch Logs에 기록하도록 Lambda 함수를 구성합니다.
그런 다음, 기록된 용량 단위와 AWS Cost Explorer API를 사용하여 전체 DynamoDB 비용을 계산하

는 Lambda 함수를 배포합니다.
이 솔루션은 DynamoDB 비용을 세밀하게 추적하고 할당할 수 있고, 추가적인 수동 작업이 필요하지 않기 때문에 운영 노력이 최소화됨.
옵션 B는 DynamoDB 비용을 각 테넌트에 정확하게 할당하고 AWS 비용 관리 도구와의 통합을 통해 비용 할당 프로세스를 자동화하는 데 가장 적합.

◆ | **Q#0417.** | **Ref#0417.**
한 회사가 데이터를 단일 Amazon S3 버킷에 저장하는 애플리케이션을 가지고 있습니다. 회사는 모든 데이터를 1년 동안 보관해야 합니다. 회사의 보안 팀은 장기 자격 증명이 유출되어 공격자가 AWS 계정에 접근할 수 있다는 점을 우려하고 있습니다.

기존 및 향후 S3 버킷의 객체를 보호할 수 있는 솔루션은 무엇입니까?

A. 위임된 역할을 통해 보안 팀만 액세스할 수 있는 새 AWS 계정을 생성합니다. 새로운 계정에서 S3 버킷을 생성하고 S3 Versioning 및 S3 Object Lock을 활성화합니다. 기본 보존 기간을 1년으로 설정합니다. 기존 S3 버킷에서 새로운 S3 버킷으로 복제를 설정합니다. 모든 기존 데이터를 복사하기 위해 S3 Batch Replication 작업을 생성합니다.
B. 3-bucket-versioning-enabled AWS Config 관리 규칙을 사용합니다. 비준수 리소스에 대해 S3 Versioning 및 MFA Delete를 활성화하는 AWS Lambda 함수를 사용하는 자동 수정 작업을 구성합니다. 1년 후에 객체를 삭제하는 S3 Lifecycle 규칙을 추가합니다.
C. 모든 사용자 및 역할이 S3 버킷 생성을 명시적으로 거부하고 AWS Service Catalog 런치 제약 역할만 예외로 설정합니다. S3 버킷 생성 시 S3 Versioning 및 MFA Delete를 강제로 활성화하는 Service Catalog 제품을 정의합니다. 사용자가 S3 버킷을 생성할 때 제품을 시작하도록 승인합니다.
D. 계정 및 AWS 리전에서 S3 보호 기능이 포함된 Amazon GuardDuty를 활성화합니다. 1년 후에 객체를 삭제하는 S3 Lifecycle 규칙을 추가합니다.

해설
정답: A
A는 새로운 AWS 계정을 생성하고, 이 계정에서 S3 Versioning 및 S3 Object Lock을 활성화하여 기본 보존 기간을 1년으로 설정하는 방식.
이렇게 하면 장기 자격 증명이 유출되더라도 중요한 데이터가 보호됩니다.
또한, S3 복제를 설정하여 기존 데이터를 새로운 S3 버킷으로 복사하고, S3 Batch Replication 작업을 통해 모든 기존 데이터를 복사합니다.
이 방법은 데이터의 무결성을 유지하고, 데이터 손실이나 무단 변경을 방지하는 데 효과적.
A는 가장 강력한 데이터 보호를 제공하며, 장기 자격 증명 유출로 인한 보안 위협을 최소화함. S3 Versioning과 S3 Object Lock을 함께 사용하여 데이터의 보호 수준을 높일 수 있음.

◆ | **Q#0418.** | **Ref#0418.**
회사는 AWS에서 웹 기반 애플리케이션의 보안을 개선해야 합니다. 애플리케이션은 두 개의 사용자 지정 오리진과 함께 Amazon CloudFront를 사용합니다. 첫 번째 사용자 지정 오리진은 요청을 Amazon API Gateway HTTP API로 라우팅합니다. 두 번째 사용자 지정 원본은 트래픽을 ALB(Application Load Balancer)로 라우팅합니다. 이 애플리케이션은 사용자 관리를 위해 OIDC(OpenID Connect) ID 공급자(IdP)와 통합됩니다.

보안 감사에 따르면 JWT(JSON Web Token) 권한 부여자가 API에 대한 액세스를 제공하는 것으로 나타났습니다. 또한 보안 감사는 ALB가 인증되지 않은 사용자의 요청을 수락한다는 것을 보여줍니다.

솔루션 설계자는 모든 백엔드 서비스가 인증된 사용자에게만 응답하도록 솔루션을 설계해야 합니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. ALB를 IdP와 통합하여 인증 및 권한 부여를 시행하도록 ALB를 구성합니다. 인증된 사용자만 백엔드 서비스에 액세스하도록 허용합니다.
B. 서명된 URL을 사용하도록 CloudFront 구성을 수정합니다. 모든 요청이 백엔드 서비스에 액세스하도록 허용하는 허용적 서명 정책을 구현합니다.

C. ALB 수준에서 인증되지 않은 요청을 필터링하는 AWS WAF 웹 ACL을 생성합니다. 인증된 트래픽만 백엔드 서비스에 도달하도록 허용합니다.
D. AWS CloudTrail을 활성화하여 ALB에 들어오는 모든 요청을 기록합니다. 로그를 분석하고 인증되지 않은 사용자로부터 오는 모든 요청을 차단하는 AWS Lambda 함수를 생성합니다.

해설
정답: A
A: ALB를 IdP와 통합하여 인증 및 권한 부여를 강제하는 방법.
이 방법은 ALB가 모든 요청을 수신할 때 인증 여부를 확인하고, 인증된 사용자만이 백엔드 서비스에 접근할 수 있도록 함.
ALB는 OIDC IdP와 직접 통합할 수 있어 사용자 인증을 중앙에서 관리할 수 있으며, 클라우드 기반 애플리케이션에서 보안성을 높이는 데 효과적.
Application Load Balancer를 사용하여 사용자 인증

◆ | **Q#0419.** | **Ref#0419.**
회사는 다중 계정 AWS 환경을 관리하고 통제하기 위해 AWS Control Tower 랜딩 존을 생성합니다. 회사의 보안 팀은 예방 제어 및 탐지 제어를 배포하여 모든 계정에서 AWS 서비스를 모니터링합니다. 보안 팀은 모든 계정의 보안 상태를 중앙 집중식으로 볼 수 있어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Control Tower 관리 계정에서 AWS CloudFormation StackSets를 사용하여 조직의 모든 계정에 AWS Config 적합성 팩을 배포합니다.
B. AWS Organizations의 조직에 대해 Amazon Detective를 활성화합니다. 하나의 AWS 계정을 Detective의 위임된 관리자로 지정합니다.
C. AWS Control Tower 관리 계정에서 자동 배포 옵션을 사용하여 조직에 대해 Amazon Detective를 활성화하는 AWS CloudFormation 스택 세트를 배포합니다.
D. AWS Organizations의 조직에 대해 AWS Security Hub를 활성화합니다. 하나의 AWS 계정을 Security Hub의 위임된 관리자로 지정합니다.

해설
정답: D
중앙 집중식 보기 == AWS Security Hub
Security Hub를 활성화하고 중앙에서 모든 계정의 보안 상태를 모니터링할 수 있는 완전한 솔루션을 제공.
Security Hub를 통해 보안 기준 및 규정 준수를 지속적으로 모니터링하고 자동화된 보안 검사를 수행할 수 있음.
위임 관리자 계정을 지정하면 중앙 계정에서 모든 계정의 보안 상태를 쉽게 관리할 수 있음.

◆ | **Q#0420.** | **Ref#0420.**
유럽과 아시아에 사무실을 두고 가전 제품을 개발하는 회사는 유럽의 온프레미스에 60TB의 소프트웨어 이미지를 저장했습니다. 회사는 ap-northeast-1 리전의 Amazon S3 버킷으로 이미지를 전송하려고 합니다. 새로운 소프트웨어 이미지는 매일 생성되며 전송 중에 암호화되어야 합니다. 이 회사에는 모든 기존 소프트웨어 이미지와 새 소프트웨어 이미지를 Amazon S3로 자동 전송하기 위해 사용자 지정 개발이 ??필요하지 않은 솔루션이 필요합니다.

이전 프로세스의 다음 단계는 무엇입니까?

A. AWS DataSync 에이전트를 배포하고 이미지를 S3 버킷으로 전송하는 작업을 구성합니다.
B. S3 Transfer Acceleration을 사용하여 이미지를 전송하도록 Amazon Kinesis Data Firehose를 구성합니다.
C. AWS Snowball 디바이스를 사용하여 S3 버킷을 대상으로 하는 이미지를 전송합니다.
D. 멀티파트 업로드가 포함된 S3 API를 사용하여 Site-to-Site VPN 연결을 통해 이미지를 전송합니다.

해설
정답: A
AWS DataSync는 데이터 전송을 자동화하고 가속화하는 서비스로, 대량의 데이터를 안정적으로 전송하는 데 매우 적합.
DataSync는 이미지를 전송하는 동안 데이터를 암호화하며, 온프레미스 스토리지에서 Amazon S3 버킷으로 데이터를 이동할 수 있음.
또한, DataSync는 사용하기 쉽고, 맞춤형 개발이 필요 없으며, 기존 데이터와 새로운 데이터를 자동으로 전송할 수 있는 기능을 제공.

421 (백은희) 1회차 完

◆ | **Q#0421.** | **Ref#0421.**
한 회사가 Amazon API Gateway, AWS Lambda, 및 Amazon DynamoDB를 사용하는 웹 애플리케이션을 운영하고 있습니다. 최근 마케팅 캠페인으로 인해 수요가 증가했습니다. 모니터링 소프트웨어는 많은 요청의 응답 시간이 마케팅 캠페인 이전보다 상당히 길어졌다고 보고하고 있습니다.

솔루션 아키텍트가 API Gateway에 대해 Amazon CloudWatch Logs를 활성화했을 때, 요청의 20%에서 오류가 발생하고 있음을 확인했습니다. CloudWatch에서 Lambda 함수의 Throttles 메트릭은 요청의 1%를 나타내고, Errors 메트릭은 요청의 10%를 나타냅니다. 애플리케이션 로그는 오류가 발생할 때 DynamoDB에 호출이 있음을 나타냅니다.

웹 애플리케이션이 대중화됨에 따라 현재 응답 시간을 개선하기 위해 솔루션 설계자는 어떤 변화를 취해야 합니까?

A. Lambda 함수의 동시성 제한을 늘립니다.
B. DynamoDB 테이블의 자동 스케일링을 구현합니다.
C. API 게이트웨이 제한 한도를 늘립니다.
D. 더 잘 분할된 기본 인덱스를 사용하여 DynamoDB 테이블을 다시 생성합니다.

해설
정답: B
Amazon API Gateway: API Gateway는 요청을 받아들이고 다른 AWS 서비스로 라우팅하는 역할을 합니다.
에러가 발생하는 비율이 20%로 높습니다. 에러가 발생할 때 DynamoDB를 호출하고 있음을 알 수 있습니다.
트래픽이 급증할 때 DynamoDB의 throughput을 늘리기 위해 autoscaling 을 구성하는 것은 성능 향상에 도움이 됩니다.
Throttles(제한) ? 동시성 한도로 인해 호출에 실패한 횟수. Throttles 지표를 살펴보고 동시성 문제를 식별.

◆ | **Q#0422.** | **Ref#0422.**
회사에 웹 프런트엔드가 있는 애플리케이션이 있습니다. 애플리케이션은 회사의 온프레미스 데이터 센터에서 실행되며 중요한 데이터를 위한 파일 스토리지에 대한 액세스가 필요합니다. 애플리케이션은 무중단 운영을 위해 (for redundancy) 3개의 Linux VM에서 실행됩니다. 아키텍처에는 HTTP 요청 기반 라우팅을 갖춘 로드 밸런서가 포함되어 있습니다.

회사는 가능한 한 빨리 애플리케이션을 AWS로 마이그레이션해야 합니다. AWS의 아키텍처는 가용성이 높아야 합니다.

아키텍처를 가장 적게 변경하여 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 3개의 가용 영역에서 Fargate 시작 유형을 사용하는 Amazon Elastic Container Service(Amazon ECS) 컨테이너로 애플리케이션을 마이그레이션합니다. Amazon S3를 사용하여 세 가지 컨테이너 모

두에 파일 스토리지를 제공합니다. Network Load Balancer를 사용하여 트래픽을 컨테이너로 전달합니다.
B. 3개의 가용 영역에 있는 Amazon EC2 인스턴스로 애플리케이션을 마이그레이션합니다. 파일 저장에는 Amazon Elastic File System(Amazon EFS)을 사용합니다. 세 개의 EC2 인스턴스 모두에 파일 스토리지를 탑재합니다. Application Load Balancer를 사용하여 트래픽을 EC2 인스턴스로 전달합니다.
C. 3개의 가용 영역에서 Fargate 시작 유형을 사용하는 Amazon Elastic Kubernetes Service(Amazon EKS) 컨테이너로 애플리케이션을 마이그레이션합니다. Lustre용 Amazon FSx를 사용하여 세 가지 컨테이너 모두에 파일 스토리지를 제공합니다. Network Load Balancer를 사용하여 트래픽을 컨테이너로 전달합니다.
D. 3개 AWS 지역의 Amazon EC2 인스턴스로 애플리케이션을 마이그레이션합니다. 파일 저장에는 Amazon Elastic Block Store(Amazon EBS)를 사용하십시오. 세 개의 EC2 인스턴스 모두에 대해 교차 리전 복제(CRR)를 활성화합니다. Application Load Balancer를 사용하여 트래픽을 EC2 인스턴스로 전달합니다.

해설
정답: B
Amazon EC2를 사용하여 애플리케이션을 호스팅하고, Amazon EFS를 사용하여 파일 저장소를 제공합니다.
Application Load Balancer(ALB)를 사용하여 트래픽을 EC2 인스턴스로 라우팅하므로 현재 아키텍처와 비슷한 방식으로 트래픽을 관리할 수 있음.

◆ | **Q#0423.** | **Ref#0423.**
한 회사가 온프레미스 데이터 센터를 AWS로 마이그레이션할 계획입니다. 이 회사는 현재 Linux 기반 VMware VM에서 데이터 센터를 호스팅하고 있습니다. 솔루션 설계자는 VM 간의 네트워크 종속성에 대한 정보를 수집해야 합니다. 정보는 호스트 IP 주소, 호스트 이름 및 네트워크 연결 정보를 자세히 설명하는 다이어그램 형식이어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS 애플리케이션 검색 서비스를 사용하세요. AWS Migration Hub 홈 AWS 지역을 선택합니다. 데이터 수집을 위해 온프레미스 서버에 AWS Application Discovery Agent를 설치합니다. Migration Hub 네트워크 다이어그램을 사용할 수 있도록 Application Discovery Service에 권한을 부여합니다.
B. 서버 데이터 수집을 위해 AWS Application Discovery Service Agentless Collector를 사용하십시오. AWS Migration Hub에서 네트워크 다이어그램을 .png 형식으로 내보냅니다.
C. 데이터 수집을 위해 온프레미스 서버에 AWS Application Migration Service 에이전트를 설치합니다. AWS의 Workload Discovery에서 AWS Migration Hub 데이터를 사용하여 네트워크 다이어그램을 생성합니다.
D. 데이터 수집을 위해 온프레미스 서버에 AWS Application Migration Service 에이전트를 설치합니다. AWS Migration Hub의 데이터를 .csv 형식으로 Amazon CloudWatch 대시보드로 내보내 네트워크 다이어그램을 생성합니다.

해설
정답: A
AWS Application Discovery Service는 온프레미스 데이터 센터의 서버와 애플리케이션에 대한 정보를 수집하는 도구.
Application Discovery Agent를 서버에 설치하여 네트워크 종속성, 호스트 IP 주소, 호스트 이름 및 네트워크 연결 정보를 포함한 세부 데이터 수집.
AWS Migration Hub는 여러 AWS 및 타사 마이그레이션 도구를 한곳에서 관리할 수 있는 중앙 허브. 수집된 데이터를 기반으로 네트워크 다이어그램을 생성하고 시각화.
"A" 이 모든 단계를 포함하고 있으며, 네트워크 다이어그램 생성에 필요한 정보를 수집하고 AWS Migration Hub를 통해 이를 시각화하는 데 필요한 권한을 부여하는 작업까지 명시하고 있습니다
참고: Prerequisites for using the network diagram in Migration Hub

◆ | **Q#0424.** | **Ref#0424.**
한 회사가 AWS에서 SaaS(Software-as-a-Service) 애플리케이션을 실행합니다. 애플리케이션은 AWS Lambda 함수와 MySQL 다중 AZ 데이터베이스용 Amazon RDS로 구성됩니다. 시장 이벤트 중에 애플리케이션의 작업량은 평소보다 훨씬 높습니다. 사용자는 많은 데이터베이스 연결로 인해 피크 기간 동안 응답 시간이 느려지는 것을 발견합니다. 회사는 데이터베이스의 확장 가능한 성능과 가용성을 개선해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 리소스 사용률이 임계값에 도달할 때 MySQL용 Amazon RDS 읽기 전용 복제본을 추가하기 위해 Lambda 함수를 트리거하는 Amazon CloudWatch 경보 작업을 생성합니다.
> **B.** 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Lambda 핸들러 함수 외부에 데이터베이스 연결 풀을 추가합니다.
> **C.** 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Amazon Route 53 가중치 기반 레코드를 사용합니다.
> **D.** 데이터베이스를 Amazon Aurora로 마이그레이션하고 Aurora 복제본을 추가합니다. 데이터베이스 connection pool을 관리하도록 Amazon RDS 프록시를 구성합니다.
>
> 해설
> 정답: D
> Amazon Aurora는 MySQL과 호환되는 고성능 데이터베이스 서비스로, 특히 읽기 복제본을 추가하여 읽기 작업을 분산하고 성능을 향상시킬 수 있습니다.
> Aurora Replica는 데이터베이스의 가용성과 확장성을 높이는 데 도움을 줍니다.
> Amazon RDS Proxy는 데이터베이스 연결 풀을 관리하여 Lambda 함수가 데이터베이스에 대한 연결을 보다 효율적으로 사용할 수 있도록 합니다.
> 이는 DB 연결 초과 문제를 완화하고 데이터베이스 성능을 최적화하는 데 중요한 역할을 합니다.
> 참고: Using Amazon RDS Proxy for Aurora

◆ | **Q#0425.** | **Ref#0425.**
한 회사가 애플리케이션을 온프레미스에서 AWS 클라우드로 마이그레이션할 계획입니다. 회사는 애플리케이션의 기본 데이터 스토리지를 AWS로 이동하여 마이그레이션을 시작합니다. 애플리케이션 데이터는 온프레미스 공유 파일 시스템에 저장되고, 애플리케이션 서버는 SMB를 통해 공유 파일 시스템에 연결됩니다.

솔루션 아키텍트는 공유 스토리지에 Amazon S3 버킷을 사용하는 솔루션을 구현해야 합니다. 애플리케이션이 완전히 마이그레이션되고 기본 Amazon S3 API를 사용하도록 코드가 다시 작성될 때까지 애플리케이션은 SMB를 통해 데이터에 계속 액세스할 수 있어야 합니다. 솔루션 아키텍트는 온프레미스 애플리케이션이 데이터에 액세스할 수 있도록 허용하면서 애플리케이션 데이터를 AWS의 새로운 위치로 마이그레이션해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 새로운 Amazon FSx for Windows File Server 파일 시스템을 생성합니다. 온프레미스 파일 공유를 위한 위치 하나와 새로운 Amazon FSx 파일 시스템을 위한 위치 하나를 사용하여 AWS DataSync를 구성합니다. 온프레미스 파일 공유 위치에서 Amazon FSx 파일 시스템으로 데이터를 복사하는 새 DataSync 작업을 생성합니다.
> **B.** 애플리케이션용 S3 버킷을 생성합니다. 온프레미스 스토리지의 데이터를 S3 버킷으로 복사합니다.
> **C.** AWS SMS(AWS Server Migration Service) VM을 온프레미스 환경에 배포합니다. AWS SMS를 사용하여 파일 스토리지 서버를 온프레미스에서 Amazon EC2 인스턴스로 마이그레이션합니다.
> **D.** 애플리케이션용 S3 버킷을 생성합니다. 온프레미스 VM에 새로운 AWS Storage Gateway 파일 게이트웨이를 배포합니다. S3 버킷에 데이터를 저장하고 파일 게이트웨이와 연결된 새 파일 공유를 생성합니다. 온프레미스 스토리지에서 새로운 파일 게이트웨이 엔드포인트로 데이터를 복사합니다.
>
> 해설

정답: D
AWS Storage Gateway의 파일 게이트웨이는 온프레미스 애플리케이션이 SMB 또는 NFS를 통해 Amazon S3에 저장된 데이터에 접근할 수 있도록 합니다.
이 접근 방식은 애플리케이션이 완전히 마이그레이션되고 코드가 S3 API를 사용할 수 있도록 다시 작성될 때까지 온프레미스에서 계속해서 데이터를 액세스할 수 있도록 합니다.
S3 버킷에 데이터를 저장하면 비용 효율적인 저장소를 제공하며, 나중에 애플리케이션 코드를 변경하여 S3 API를 직접 사용할 수 있도록 할 수 있습니다.
이 솔루션은 기존의 데이터 접근 방법(SMB)을 유지하면서 데이터를 AWS로 마이그레이션하고, 점진적으로 애플리케이션을 클라우드로 전환하는 데 이상적입니다.

◆ | **Q#0426.** | **Ref#0426.**
한 글로벌 기업이 티켓 바코드를 표시하는 모바일 앱을 보유하고 있습니다. 고객은 모바일 앱의 티켓을 사용하여 라이브 이벤트에 참석합니다. 이벤트 스캐너는 티켓 바코드를 읽고 백엔드 API를 호출하여 데이터베이스의 데이터와 비교하여 바코드 데이터의 유효성을 검사합니다. 바코드가 스캔된 후 백엔드 로직은 데이터베이스의 단일 테이블에 기록하여 바코드가 사용된 것으로 표시합니다.

회사는 api.example.com이라는 DNS 이름을 사용하여 AWS에 앱을 배포해야 합니다. 회사는 전 세계 3개 AWS 지역에서 데이터베이스를 호스팅할 예정입니다.

회사의 요구사항을 최저 지연 시간으로 충족할 솔루션은 무엇입니까?

A. Amazon Aurora 글로벌 데이터베이스 클러스터에서 데이터베이스를 호스팅합니다. 데이터베이스와 동일한 리전에 있는 3개의 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 백엔드를 호스팅합니다. AWS Global Accelerator에서 액셀러레이터를 생성하여 요청을 가장 가까운 ECS 클러스터로 라우팅합니다. api.example.com을 액셀러레이터 엔드포인트에 매핑하는 Amazon Route 53 레코드를 생성합니다.
B. Amazon Aurora 글로벌 데이터베이스 클러스터에서 데이터베이스를 호스팅합니다. 데이터베이스와 동일한 리전에 있는 3개의 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에서 백엔드를 호스팅합니다. 3개의 클러스터를 오리진으로 사용하여 Amazon CloudFront 배포를 생성합니다. 가장 가까운 EKS 클러스터로 요청을 라우팅합니다. api.example.com을 CloudFront 배포에 매핑하는 Amazon Route 53 레코드를 생성합니다.
C. Amazon DynamoDB 글로벌 테이블에서 데이터베이스를 호스팅합니다. Amazon CloudFront 배포를 생성합니다. CloudFront 배포를 바코드 검증을 위한 백엔드 로직이 포함된 CloudFront 함수와 연결합니다. api.example.com을 CloudFront 배포에 매핑하는 Amazon Route 53 레코드를 생성합니다.
D. Amazon DynamoDB 글로벌 테이블에서 데이터베이스를 호스팅합니다. Amazon CloudFront 배포를 생성합니다. CloudFront 배포를 바코드 검증을 위한 백엔드 로직이 포함된 Lambda@Edge 함수와 연결합니다. api.example.com을 CloudFront 배포에 매핑하는 Amazon Route 53 레코드를 생성합니다.

해설
정답: D
Amazon DynamoDB 글로벌 테이블은 여러 리전에 걸쳐 데이터를 복제하여 글로벌 사용자에게 낮은 지연 시간으로 일관된 데이터를 제공합니다.
Amazon CloudFront는 전 세계에 분산된 엣지 로케이션을 통해 낮은 지연 시간으로 콘텐츠를 제공할 수 있습니다.
Lambda@Edge를 사용하면 CloudFront 엣지 로케이션에서 코드를 실행할 수 있어 사용자와 가장 가까운 곳에서 백엔드 로직을 처리할 수 있습니다.
이는 지연 시간을 최소화하는 데 매우 효과적입니다.
Amazon Route 53을 사용하여 api.example.com을 CloudFront 배포에 매핑하면 DNS 이름을 통해 전 세계에서 요청을 CloudFront로 라우팅할 수 있습니다.

◆ | **Q#0427.** | **Ref#0427.**
의료 회사는 Amazon EC2 인스턴스 세트에서 REST API를 실행하고 있습니다. EC2 인스턴스는 Application Load Balancer (ALB) 뒤에서 Auto Scaling 그룹으로 실행됩니다. ALB는 세 개의 퍼블릭 서브넷에서 실행되며, EC2 인스턴스는 세 개의 프라이빗 서브넷에서 실행됩니다. 회사는 ALB를 유일한 오리진으로 하는 Amazon CloudFront 배포판을 배포했습니다.

솔루션 아키텍트가 오리진 보안을 강화하기 위해 권장해야 할 솔루션은 무엇입니까?

> **A.** AWS Secrets Manager에 랜덤 문자열을 저장합니다. 자동 비밀 교체(automatic secret rotation)를 위한 AWS Lambda 함수를 생성합니다. CloudFront가 오리진 요청에 대한 커스텀 HTTP 헤더로 랜덤 문자열을 주입하도록 구성합니다. 커스텀 헤더에 대한 문자열 매치 규칙이 포함된 AWS WAF 웹 ACL 규칙을 생성합니다. 웹 ACL을 ALB에 연결합니다.
> **B.** CloudFront 서비스 IP 주소 범위의 IP 매치 조건을 사용하여 AWS WAF 웹 ACL 규칙을 생성합니다. 웹 ACL을 ALB에 연결하고 ALB를 세 개의 프라이빗 서브넷으로 이동합니다.
> **C.** AWS Systems Manager Parameter Store에 랜덤 문자열을 저장합니다. 문자열의 자동 회전을 위한 Parameter Store를 구성합니다. CloudFront가 오리진 요청에 대한 커스텀 HTTP 헤더로 랜덤 문자열을 주입하도록 구성합니다. 커스텀 HTTP 헤더의 값을 검사하고, ALB에서 접근을 차단합니다.
> **D.** AWS Shield Advanced 구성 CloudFront 서비스 IP 주소 범위에서의 연결을 허용하는 보안 그룹 정책을 생성합니다. AWS Shield Advanced에 정책을 추가하고 ALB에 정책을 연결합니다.
>
> 해설
> 정답: A
> AWS Secrets Manager를 사용하여 랜덤 문자열을 저장하고, 자동 비밀 교체을 통해 주기적으로 문자열을 갱신하면 보안성이 강화.
> CloudFront는 오리진 요청 시 커스텀 HTTP 헤더로 랜덤 문자열을 주입할 수 있으며, 이를 통해 요청이 CloudFront를 통해 온 것임을 확인가능.
> AWS WAF 웹 ACL 규칙을 사용하여 커스텀 헤더의 값을 검사하면, CloudFront 외부에서 오는 요청을 차단할 수 있음.
> (참고)AWS Shield Advanced는 주로 DDoS 공격 방어에 중점을 두고 있으며, 특정 IP 주소 범위를 통한 접근 제어에는 최적화되지 않음.
> AWS WAF 및 AWS Secrets Manager를 사용하여 Amazon CloudFront 오리진 보안을 강화하는 방법

◆ | **Q#0428.** | **Ref#0428.**
업계 규정을 준수하기 위해 솔루션 아키텍트는 회사 본사가 위치한 미국을 포함하여 여러 Public AWS 지역에 회사의 중요 데이터를 저장할 솔루션을 설계해야 합니다. 솔루션 아키텍트는 AWS에 저장된 데이터에 대한 액세스를 회사의 글로벌 WAN 네트워크에 제공해야 합니다. 보안 팀은 이 데이터에 액세스하는 트래픽이 공용 인터넷을 통과해서는 안 된다고 규정하고 있습니다.

솔루션 아키텍트가 요구 사항을 충족하면서도 고가용성을 갖추고 비용 효율적인 솔루션을 설계하려면 어떻게 해야 합니까?

> **A.** 본사에서 모든 AWS 리전으로 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 본사로 트래픽을 전송한 다음, 해당 DX 연결을 통해 데이터를 액세스합니다.
> **B.** 본사에서 한 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다. 다른 AWS 리전의 데이터를 액세스하기 위해 리전 간 VPC peering을 사용합니다.
> **C.** 본사에서 한 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다. 다른 AWS 리전의 데이터를 액세스하기 위해 AWS Transit VPC 솔루션을 사용합니다.
> **D.** 본사에서 한 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다. 다른 AWS 리전의 데이터를 액세스하기 위해 Direct Connect Gateway를 사용합니다.

해설
정답: D
Direct Connect Gateway는 AWS Direct Connect(DX) 연결을 통해 여러 AWS 리전의 VPC에 액세스할 수 있는 기능을 제공합니다. 이를 통해 단일 Direct Connect 연결을 통해 여러 리전의 데이터를 액세스할 수 있어 비용 효율적입니다.
본사에서 AWS 리전으로 두 개의 Direct Connect 연결을 설정하여 고가용성을 보장합니다.
회사 WAN을 사용하여 Direct Connect 연결을 통해 트래픽을 전송함으로써 공용 인터넷을 사용하지 않고 보안 요구 사항을 충족할 수 있습니다.
Direct Connect Gateway는 여러 리전에 걸쳐 데이터를 안전하게 액세스할 수 있도록 해주며, 각 리전에 별도의 Direct Connect 연결을 설정할 필요가 없으므로 비용 효율적입니다.

◆ | **Q#0429.** | **Ref#0429.**
한 회사가 온프레미스에서 호스팅하는 VMware vSphere VM에서 Windows Server를 실행하는 애플리케이션을 개발했습니다. 애플리케이션 데이터는 애플리케이션을 통해서만 읽을 수 있는 독점 형식으로 저장됩니다. 회사는 서버와 애플리케이션을 수동으로 프로비저닝했습니다.

재해 복구 계획의 일환으로 회사는 회사의 온프레미스 환경을 사용할 수 없게 되는 경우 일시적으로 AWS에서 애플리케이션을 호스팅할 수 있는 기능을 원합니다. 회사는 재해 복구 이벤트가 완료된 후 애플리케이션이 온프레미스 호스팅으로 돌아가기를 원합니다. RPO는 5분입니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS DataSync를 구성합니다. 데이터를 Amazon Elastic Block Store(Amazon EBS) 볼륨에 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 AWS CloudFormation 템플릿을 사용하여 Amazon EC2 인스턴스를 프로비저닝하고 EBS 볼륨을 연결합니다.
B. AWS Elastic Disaster Recovery를 구성합니다. Amazon Elastic Block Store(Amazon EBS) 볼륨에 연결된 복제 Amazon EC2 인스턴스에 데이터를 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 Elastic Disaster Recovery를 사용하여 복제된 볼륨을 사용하는 EC2 인스턴스를 시작합니다.
C. AWS Storage Gateway 파일 게이트웨이를 프로비저닝합니다. 데이터를 Amazon S3 버킷에 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 AWS Backup을 사용하여 데이터를 Amazon Elastic Block Store(Amazon EBS) 볼륨으로 복원하고 이러한 EBS 볼륨에서 Amazon EC2 인스턴스를 시작합니다.
D. AWS에서 Windows 파일 서버용 Amazon FSx 파일 시스템을 프로비저닝합니다. 데이터를 파일 시스템에 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 AWS CloudFormation 템플릿을 사용하여 Amazon EC2 인스턴스를 프로비저닝하고 AWS::CloudFormation::Init 명령을 사용하여 Amazon FSx 파일 공유를 탑재합니다.

해설
정답: B
AWS Elastic Disaster Recovery는 기존 온프레미스 워크로드를 AWS로 효율적으로 복제하고 재해 복구 상황에서 신속하게 EC2 인스턴스를 시작할 수 있도록 지원하는 서비스.
Elastic Disaster Recovery를 통해 자동으로 데이터를 Amazon EC2 인스턴스와 연결된 Amazon EBS 볼륨으로 복제할 수 있으며, 재해 복구 상황에서는 손쉽게 EC2 인스턴스를 시작할 수 있습니다.
다른 옵션들도 재해 복구를 가능하게 하지만, 운영 오버헤드 측면에서 Elastic Disaster Recovery가 가장 적합합니다.
AWS Elastic Disaster Recovery는 낮은 운영 오버헤드와 5분 RPO에 맞춰 조정됨.

◆ | **Q#0430.** | **Ref#0430.**
회사는 eu-north-1 지역의 Amazon EC2에서 고가용성 데이터 수집 애플리케이션을 실행합니다. 애플리케이션은 최종 사용자 장치에서 데이터를 수집하고 Amazon Kinesis 데이터 스트림과 레코드를 처리하는 일련의 AWS Lambda 함수에 레코드를 씁니다. 회사는 레코드 처리 결과를 eu-north-1의 Amazon S3 버킷에 유지합니다. 회사는 S3 버킷의 데이터를 Amazon Athena의 데이터 소스로 사용합니다.

회사는 글로벌 입지를 확대하고자 합니다. 솔루션 아키텍트는 sa-east-1 및 ap-northeast-1 지역에서 데이터 수집 기능을 시작해야 합니다. 솔루션 아키텍트는 두 개의 새로운 리전에 애플리케이션, Kinesis 데이터 스트림 및 Lambda 함수를 배포합니다. 솔루션 아키텍트는 데이터 분석을 중앙 집중화하기 위한 요구 사항을 충족하기 위해 S3 버킷을 eu-north-1에 유지합니다.

새로운 설정을 테스트하는 동안 솔루션 아키텍트는 새 리전에서 S3 버킷으로 데이터가 도착할 때 상당한 지연이 있음을 발견했습니다.

이 지연 시간을 가장 많이 개선할 수 있는 솔루션은 무엇입니까?

> **A.** 두 개의 새로운 리전 각각에서 VPC에서 실행되도록 Lambda 함수를 설정하십시오. 해당 VPC에 S3 게이트웨이 엔드포인트를 설정합니다.
> **B.** eu-north-1의 S3 버킷에서 S3 Transfer Acceleration을 켭니다. 애플리케이션이 S3 버킷에 데이터를 업로드할 때 새로운 S3 가속 엔드포인트를 사용하도록 애플리케이션을 변경합니다.
> **C.** 두 개의 새로운 리전 각각에 S3 버킷을 생성합니다. 각 새 리전의 애플리케이션을 해당 S3 버킷에 업로드하도록 설정합니다. eu-north-1의 S3 버킷에 데이터를 복제하도록 S3 교차 리전 복제(Cross-Region Replication)를 설정합니다.
> **D.** 여러 코어를 사용할 수 있도록 Lambda 함수의 메모리 요구 사항을 늘립니다. 애플리케이션이 Lambda에서 Amazon S3로 데이터를 업로드할 때 멀티파트 업로드 기능을 사용합니다.
>
> 해설
> 정답: C (B와 정답 논란)
> 교차 리전 복제(Cross-Region Replication)는 S3 버킷 간의 데이터를 자동으로 복제하여, 원격지 리전에서도 데이터를 중앙 집중화된 S3 버킷으로 전송할 수 있습니다.
> 이를 통해 데이터를 각 리전에서 가까운 S3 버킷으로 먼저 업로드한 후, 자동으로 중앙 S3 버킷(eu-north-1)으로 복제합니다.
> 각 리전에서 데이터 전송 지연을 줄이면서, 중앙 S3 버킷에서 데이터를 분석할 수 있는 설정이 가능합니다.
>
> (참고) S3 Transfer Acceleration은 글로벌 액세스 지점 네트워크를 사용하여 데이터를 S3 버킷으로 더 빠르게 전송할 수 있도록 도와줍니다.
> 애플리케이션이 S3 가속화 엔드포인트를 사용하여 데이터를 업로드하도록 변경하면, 새로운 리전에서의 데이터 전송 속도가 개선될 수 있습니다.
> 그러나 eu-north-1 리전에서는 S3 Transfer Acceleration이 지원되지 않기 때문에 B를 선택할 수 없습니다.

431 (김지형) 1회차 完

◆ | **Q#0431.** | **Ref#0431.**
회사는 단일 공유 VPC에서 호스팅되는 중앙 집중식 Amazon EC2 애플리케이션을 제공합니다. 중앙 집중식 애플리케이션은 다른 사업부의 VPC에서 실행되는 클라이언트 애플리케이션에서 액세스할 수 있어야 합니다. 중앙 집중식 애플리케이션 프런트 엔드는 확장성을 위해 NLB(Network Load Balancer)로 구성됩니다.

최대 10개의 사업부 VPC를 공유 VPC에 연결해야 합니다. 비즈니스 단위 VPC CIDR 블록 중 일부는 공유 VPC와 겹치고 일부는 서로 겹칩니다. 공유 VPC의 중앙 집중식 애플리케이션에 대한 네트워크 연결은 승인된 비즈니스 단위 VPC에서만 허용되어야 합니다.

솔루션 아키텍트는 사업부 VPC의 클라이언트 애플리케이션에서 공유 VPC의 중앙 집중식 애플리케이션으로 연결을 제공하기 위해 어떤 네트워크 구성을 사용해야 합니까?

> **A.** AWS Transit Gateway를 생성합니다. 공유 VPC와 승인된 사업부 VPC를 Transit Gateway에 연결합니다. 단일 Transit Gateway 라우팅 테이블을 생성하고 이를 연결된 모든 VPC와 연결합니다. 첨부 파일의 경로가 경로 테이블로 자동 전파되도록 허용합니다. Transit Gateway로 트래픽을 보내도록

VPC 라우팅 테이블을 구성합니다.
B. 중앙 집중식 애플리케이션 NLB를 사용하여 VPC 엔드포인트 서비스를 생성하고 엔드포인트 승인을 요구하는 옵션을 활성화합니다. 엔드포인트 서비스의 서비스 이름을 사용하여 각 사업부 VPC에 VPC 엔드포인트를 생성합니다. 엔드포인트 서비스 콘솔에서 승인된 엔드포인트 요청을 수락합니다.
C. 각 사업부 VPC에서 공유 VPC로의 VPC 피어링 연결을 생성합니다. 공유 VPC 콘솔에서 VPC 피어링 연결을 수락합니다. 트래픽을 VPC 피어링 연결로 보내도록 VPC 라우팅 테이블을 구성합니다.
D. 공유 VPC에 대한 가상 프라이빗 게이트웨이를 구성하고 승인된 각 사업부 VPC에 대해 고객 게이트웨이를 생성합니다. 사업부 VPC에서 공유 VPC로 Site-to-Site VPN 연결을 설정합니다. VPN 연결로 트래픽을 보내도록 VPC 라우팅 테이블을 구성합니다.

해설
정답: **B**
VPC 엔드포인트 서비스를 사용하면 CIDR 블록이 겹치는 문제를 해결할 수 있으며, 승인된 사업부 VPC에서만 접근을 허용할 수 있음.
Transit Gateway는 네트워크 연결을 관리하는 효과적인 방법이지만, CIDR 블록이 겹치는 문제를 해결하지 못함.
VPC Peering 연결은 CIDR 블록이 겹치는 문제를 해결하지 못함.
가상 프라이빗 게이트웨이는 복잡하고 관리 오버헤드가 높으며, CIDR 블록이 겹치는 문제를 해결하지 못함.

◆ | **Q#0432.** | **Ref#0432.**
한 회사에서 웹사이트를 AWS로 마이그레이션하려고 합니다. 웹사이트는 마이크로서비스를 사용하며 온프레미스 자체 관리형 Kubernetes 클러스터에 배포된 컨테이너에서 실행됩니다. Kubernetes 배포의 컨테이너 배포를 정의하는 모든 매니페스트는 소스 제어에 있습니다.

웹사이트의 모든 데이터는 PostgreSQL 데이터베이스에 저장됩니다. 오픈 소스 컨테이너 이미지 저장소는 온프레미스 환경과 함께 실행됩니다.

솔루션 아키텍트는 회사가 AWS의 웹 사이트에 사용할 아키텍처를 결정해야 합니다.

최소한의 마이그레이션 노력으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS App Runner 서비스를 생성합니다. App Runner 서비스를 오픈 소스 컨테이너 이미지 저장소에 연결합니다. 온프레미스에서 App Runner 서비스로 매니페스트를 배포합니다. PostgreSQL 데이터베이스용 Amazon RDS를 생성합니다.
B. 관리형 노드 그룹이 있는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 생성합니다. 애플리케이션 컨테이너를 새로운 Amazon Elastic Container Registry(Amazon ECR) 리포지토리에 복사합니다. 온프레미스에서 EKS 클러스터로 매니페스트를 배포합니다. Amazon Aurora PostgreSQL DB 클러스터를 생성합니다.
C. Amazon EC2 용량 풀이 있는 Amazon Elastic Container Service(Amazon ECS) 클러스터를 생성합니다. 애플리케이션 컨테이너를 새로운 Amazon Elastic Container Registry(Amazon ECR) 리포지토리에 복사합니다. 각 컨테이너 이미지를 새 작업 정의로 등록합니다. 원래 Kubernetes 배포와 일치하도록 각 작업 정의에 대한 ECS 서비스를 구성합니다. Amazon Aurora PostgreSQL DB 클러스터를 생성합니다.
D. Amazon EC2 인스턴스에서 클러스터를 호스팅하여 온프레미스 Kubernetes 클러스터를 재구축합니다. 오픈 소스 컨테이너 이미지 저장소를 EC2 인스턴스로 마이그레이션합니다. 온프레미스에서 AWS의 새 클러스터로 매니페스트를 배포합니다. 새 클러스터에 오픈 소스 PostgreSQL 데이터베이스를 배포합니다.

해설
정답: B
Amazon EKS는 Kubernetes와 완벽하게 호환되며, 기존의 Kubernetes 매니페스트를 그대로 사용할

수 있음.
ECR을 사용하여 컨테이너 이미지를 저장하고, Aurora PostgreSQL은 고가용성과 성능을 제공하는 관리형 데이터베이스 서비스.
따라서 이 옵션은 애플리케이션은 변경할 필요 없이 최소한의 노력으로 마이그레이션을 할 수 있음.
A(x): App Runner는 단순한 웹 애플리케이션 배포에 적합, 마이크로서비스 아키텍처에는 적절하지 않음,
C(x): ECS는 Docker 기반 컨테이너 서비스, Kubernetes 매니페스트와의 호환성이 낮아 매니페스트를 ECS 태스크 정의로 변환해야 하는 추가 작업이 필요,
D(x): EC2 인스턴스에서 Kubernetes 클러스터를 운영하는 것은 복잡도가 높음.

◆ | **Q#0433.** | **Ref#0433.**
한 회사는 AWS의 모바일 앱을 사용하여 온라인 콘테스트를 운영합니다. 회사는 각 콘테스트가 끝날 때 무작위로 우승자를 선택합니다. 콘테스트는 다양한 기간 동안 진행됩니다. 회사는 콘테스트가 끝난 후 콘테스트의 데이터를 보관할 필요가 없습니다.

이 회사는 Amazon EC2 인스턴스에 호스팅된 사용자 지정 코드를 사용하여 콘테스트 데이터를 처리하고 우승자를 선택합니다. EC2 인스턴스는 Application Load Balancer 뒤에서 실행되며 Amazon RDS DB 인스턴스에 콘테스트 항목을 저장합니다. 회사는 콘테스트 운영 비용을 줄이기 위해 새로운 아키텍처를 설계해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 컨테스트 참가작의 스토리지를 Amazon DynamoDB로 마이그레이션합니다. DynamoDB Accelerator(DAX) 클러스터를 생성합니다. Fargate 시작 유형을 사용하는 Amazon Elastic Container Service(Amazon ECS) 컨테이너로 실행되도록 코드를 다시 작성합니다. 콘테스트가 끝나면 DynamoDB 테이블을 삭제합니다.
B. 콘테스트 참가작의 스토리지를 Amazon Redshift로 마이그레이션합니다. 코드를 AWS Lambda 함수로 다시 작성합니다. 콘테스트가 끝나면 Redshift 클러스터를 삭제합니다.
C. RDS DB 인스턴스 앞에 Redis용 Amazon ElastiCache 클러스터를 추가하여 콘테스트 항목을 캐시합니다. Fargate 시작 유형을 사용하는 Amazon Elastic Container Service(Amazon ECS) 컨테이너로 실행되도록 코드를 다시 작성합니다. 콘테스트 종료 시 각 항목이 만료되도록 각 항목의 ElastiCache TTL 속성을 설정합니다.
D. 콘테스트 참가작의 스토리지를 Amazon DynamoDB로 마이그레이션합니다. 코드를 AWS Lambda 함수로 다시 작성합니다. 콘테스트 종료 시 각 항목이 만료되도록 각 항목의 DynamoDB TTL 속성을 설정합니다.

해설
정답: D
DynamoDB와 Lambda의 조합은 매우 비용 효율적임. DynamoDB의 TTL 기능을 사용하여 데이터를 자동으로 만료시킬 수 있으므로 데이터 관리가 용이함.
Lambda는 사용한 만큼만 비용을 지불하므로, 가변적인 콘테스트 기간 동안 비용을 최적화할 수 있음.

◆ | **Q#0434.** | **Ref#0434.**
회사에서 새로운 보안 요구 사항을 구현했습니다. 새로운 요구 사항에 따라 회사는 회사 VPC에 있는 회사 AWS 인스턴스의 모든 트래픽에서 회사 보안 정책 위반 여부를 검사해야 합니다. 이러한 스캔 결과, 회사는 특정 IP 주소에 대한 접근을 차단할 수 있습니다.

새로운 요구 사항을 충족하기 위해 회사는 프라이빗 서브넷에 Amazon EC2 인스턴스 세트를 배포하여 투명한 프록시 역할을 합니다. 회사는 이러한 EC2 인스턴스에 승인된 프록시 서버 소프트웨어를 설치합니다. 회사는 프록시 소프트웨어가 포함된 해당 EC2 인스턴스를 기본 경로로 사용하도록 모든 서브넷의 경로 테이블을 수정합니다. 또한 회사는 보안 정책을 준수하는 보안 그룹을 생성하고 이러한 보안 그룹을 EC2 인스턴스에 할당합니다.

이러한 구성에도 불구하고 프라이빗 서브넷의 EC2 인스턴스 트래픽이 인터넷으로 제대로 전달되지 않습니다.

이 문제를 해결하려면 솔루션 설계자가 무엇을 해야 합니까?

> **A.** 프록시 소프트웨어를 실행하는 EC2 인스턴스에서 소스/대상 확인을 비활성화합니다.
> **B.** 이 보안 그룹이 있는 인스턴스 간의 모든 트래픽을 허용하도록 프록시 EC2 인스턴스에 할당된 보안 그룹에 규칙을 추가합니다. 이 보안 그룹을 VPC의 모든 EC2 인스턴스에 할당합니다.
> **C.** VPC DHCP 옵션 세트를 변경합니다. 프록시 EC2 인스턴스의 주소를 가리키도록 DNS 서버 옵션을 설정합니다.
> **D.** 각 프록시 EC2 인스턴스에 하나의 추가 탄력적 네트워크 인터페이스를 할당합니다. 이러한 네트워크 인터페이스 중 하나에 프라이빗 서브넷에 대한 경로가 있는지 확인하세요. 다른 네트워크 인터페이스에 인터넷으로의 경로가 있는지 확인하십시오.
>
> 해설
> 정답: A
> 프라이빗 서브넷의 EC2 인스턴스의 트래픽이 올바르게 인터넷으로 전달되지 않는 문제를 해결해야 합니다.
> A: NAT와 같은 프록시는 소스/대상 확인(SrcDestCheck)을 비활성화해야 합니다.
> 소스/대상 확인은 네트워크 트래픽의 출발지 및 목적지를 확인하는 기능으로, 프록시 인스턴스에서 이를 비활성화함으로써 트래픽이 프록시를 통해 올바르게 전달될 수 있습니다.

◆ | **Q#0435.** | **Ref#0435.**
회사는 수동으로 생성된 VPC의 AWS에서 솔루션을 실행하고 있습니다. 회사는 AWS CloudFormation을 사용하여 인프라의 다른 부분을 프로비저닝하고 있습니다. 새로운 요구 사항에 따라 회사는 모든 인프라를 자동으로 관리해야 합니다.

최소한의 노력으로 이 새로운 요구 사항을 충족하려면 회사는 무엇을 해야 합니까?

> **A.** 기존 VPC 리소스 및 구성을 엄격하게 프로비저닝하는 새로운 AWS Cloud Development Kit(AWS CDK) 스택을 생성합니다. AWS CDK를 사용하여 VPC를 스택으로 가져오고 VPC를 관리합니다.
> **B.** VPC를 생성하는 CloudFormation 스택 세트를 생성합니다. 스택 세트를 사용하여 VPC를 스택으로 가져옵니다.
> **C.** 기존 VPC 리소스 및 구성을 엄격하게 프로비저닝하는 새 CloudFormation 템플릿을 생성합니다. CloudFormation 콘솔에서 기존 리소스를 가져와 새 스택을 생성합니다.
> **D.** VPC를 생성하는 새로운 CloudFormation 템플릿을 생성합니다. AWS Serverless Application Model(AWS SAM) CLI를 사용하여 VPC를 가져옵니다.
>
> 해설
> 정답: C
> CloudFormation을 이미 사용 중이므로 새로운 요구 사항을 충족시키기 위해 기존 VPC를 가져와 새로운 CloudFormation 템플릿을 만들고 기존 리소스를 가져오는 것이 가장 적은 노력을 필요로 할 것으로 보입니다.
> CloudFormation 콘솔을 통해 기존 VPC 리소스를 쉽게 가져와서 자동으로 관리할 수 있음.
> A(x): AWS CDK는 인프라 관리에 강력하지만, 기존 VPC를 직접 가져오고 관리하는 작업이 CloudFormation만큼 간단하지 않음.
> B(x): 스택 세트는 여러 계정 및 리전에 걸친 리소스 관리를 용이하게 하지만, 단일 VPC를 가져오는 데는 과도한 선택.
> D(x): AWS SAM은 주로 서버리스 애플리케이션에 사용되며, 기존 VPC를 가져오는 데는 적합하지 않음.

◆ | **Q#0436.** | **Ref#0436.**
한 회사에서 인기 비디오 게임의 새 릴리스를 개발하여 공개 다운로드할 수 있도록 하려고 합니다. 새 릴리스 패키지의 크기는 약 5GB입니다. 회사는 온프레미스 데이터 센터에 호스팅된 Linux 기반의 공개 FTP 사이트에서 기존 릴리스에 대한 다운로드를 제공합니다. 회사는 전 세계 사용자가 새 릴리스를 다운로드할 것으로 예상하고 있습니다. 회사는 사용자의 위치에 관계없이 향상된 다운로드 성능과 낮은 전송 비용을 제공하는 솔루션을 원합니다.

A. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 탑재된 Amazon EBS 볼륨에 게임 파일을 저장합니다. EC2 인스턴스에서 FTP 서비스를 구성합니다. Auto Scaling 그룹 앞에 Application Load Balancer를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.
B. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 연결된 Amazon EFS 볼륨에 게임 파일을 저장합니다. 각 EC2 인스턴스에 FTP 서비스를 구성합니다. Auto Scaling 그룹 앞에 Application Load Balancer를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.
C. 웹 사이트 호스팅을 위해 Amazon Route 53 및 Amazon S3 버킷을 구성합니다. 게임 파일을 S3 버킷에 업로드합니다. 웹 사이트에는 Amazon CloudFront를 사용하십시오. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.
D. 웹 사이트 호스팅을 위해 Amazon Route 53 및 Amazon S3 버킷을 구성합니다. 게임 파일을 S3 버킷에 업로드합니다. S3 버킷에 대한 요청자 지불을 설정합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.

해설
정답: C
전 세계적으로 콘텐츠를 캐시하고 제공하는 CloudFront를 사용하므로 향상된 다운로드 성능과 낮은 전송 비용을 제공함.
S3와 CloudFront는 데이터를 에지 위치에 캐시하여 사용자의 위치에 관계없이 전 세계적으로 빠른 다운로드를 지원.

◆ | **Q#0437.** | **Ref#0437.**
회사는 데이터베이스와 웹 사이트로 구성된 클라우드에서 애플리케이션을 실행합니다. 사용자는 웹사이트에 데이터를 게시하고, 데이터를 처리하고, 데이터를 이메일로 다시 전송할 수 있습니다. 데이터는 Amazon EC2 인스턴스에서 실행되는 MySQL 데이터베이스에 저장됩니다. 데이터베이스는 2개의 프라이빗 서브넷이 있는 VPC에서 실행되고 있습니다. 웹 사이트는 하나의 퍼블릭 서브넷이 있는 다른 VPC에 있는 단일 EC2 인스턴스의 Apache Tomcat에서 실행되고 있습니다. 데이터베이스와 웹사이트 VPC 사이에는 단일 VPC 피어링 연결이 있습니다.

지난 한 달 동안 트래픽 폭주로 인해 웹사이트가 여러 차례 중단되었습니다.

솔루션 설계자는 애플리케이션의 안정성을 높이기 위해 어떤 조치를 취해야 합니까? (3개를 선택하세요.)

A. Application Load Balancer 뒤에 여러 EC2 인스턴스가 있는 Auto Scaling 그룹에 Tomcat 서버를 배치합니다.
B. 추가 VPC 피어링 연결을 프로비저닝합니다.
C. 하나의 Aurora 복제본을 사용하여 MySQL 데이터베이스를 Amazon Aurora로 마이그레이션합니다.
D. 데이터베이스 VPC에 두 개의 NAT 게이트웨이를 프로비저닝합니다.
E. Tomcat 서버를 데이터베이스 VPC로 이동합니다.
F. 웹사이트 VPC의 다른 가용 영역에 추가 퍼블릭 서브넷을 생성합니다.

해설
정답: A,C,F
A. Tomcat 서버를 Auto Scaling 그룹으로 배치하고 Application Load Balancer 뒤에 배치하여 자동으로 스케일링되고 고가용성을 제공할 수 있습니다. 이것은 고트래픽에 대응하기 위한 좋은 방법입니다.
C. MySQL 데이터베이스를 Amazon Aurora로 이전하고 Aurora Replica를 만들면 데이터베이스의 가용성이 향상됩니다. Aurora는 자동 장애 조치 및 자동 스케일링을 지원하여 신뢰성을 높일 수 있습니다.
F. 추가 퍼블릭 서브넷을 다른 가용 영역에 생성하면 웹 사이트의 가용성이 향상됩니다. 이렇게 하면 단일 가용 영역의 장애로부터 보호받을 수 있습니다.

◆ | **Q#0438.** | **Ref#0438.**
한 소매 회사가 AWS에서 전자상거래 애플리케이션을 운영하고 있습니다. 애플리케이션은 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스에서 실행됩니다. 회사는 Amazon RDS DB 인스턴스를 데이터베이스 백엔드로 사용합니다. Amazon CloudFront는 ALB를 가리키는 하나의 오리진으로 구성됩니다. 정적 콘텐츠가 캐시됩니다. Amazon Route 53은 모든 공개 영역을 호스팅하는 데 사용됩니다.

애플리케이션 업데이트 후 ALB는 때때로 502 상태 코드(잘못된 게이트웨이) 오류를 반환합니다. 근본 원인은 ALB에 반환되는 잘못된 HTTP 헤더입니다. 오류가 발생한 직후 솔루션 설계자가 웹 페이지를 다시 로드하면 웹 페이지가 성공적으로 반환됩니다.

회사가 문제를 해결하는 동안 솔루션 설계자는 방문자에게 표준 ALB 오류 페이지 대신 사용자 정의 오류 페이지를 제공해야 합니다.

최소한의 운영 오버헤드로 이 요구 사항을 충족하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

> **A.** Amazon S3 버킷을 생성합니다. 정적 웹페이지를 호스팅하도록 S3 버킷을 구성합니다. 사용자 정의 오류 페이지를 Amazon S3에 업로드합니다.
> **B.** ALB 상태 확인 응답 Target.FailedHealthChecks가 0보다 큰 경우 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다. 공개적으로 액세스 가능한 웹 서버를 가리키도록 ALB에서 전달 규칙을 수정하도록 Lambda 함수를 구성합니다.
> **C.** 상태 확인을 추가하여 기존 Amazon Route 53 레코드를 수정합니다. 상태 확인에 실패할 경우 대체 대상을 구성합니다. 공개적으로 액세스할 수 있는 웹페이지를 가리키도록 DNS 레코드를 수정합니다.
> **D.** ALB 상태 확인 응답 Elb.InternalError가 0보다 큰 경우 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다. 공개 액세스 가능한 웹 서버를 가리키도록 ALB에서 전달 규칙을 수정하도록 Lambda 함수를 구성합니다.
> **E.** CloudFront 사용자 지정 오류 페이지를 구성하여 사용자 지정 오류 응답을 추가합니다. 공개적으로 액세스할 수 있는 웹 페이지를 가리키도록 DNS 레코드를 수정합니다.
>
> 해설
> 정답: A,E
> 이 요구 사항을 가장 적은 운영 오버헤드로 충족하는 두 가지 단계 조합은 A와 E입니다.
> 사용자 지정 오류 페이지를 제공하기 위해 S3 버킷에 정적 웹 페이지를 호스팅하고, CloudFront를 사용하여 사용자 지정 오류 응답을 추가하는 것이 간단하고 효율적입니다.

◆ | **Q#0439.** | **Ref#0439.**
회사에서는 Amazon Aurora MySQL DB 클러스터를 기존 AWS 계정에서 동일한 AWS 리전의 새 AWS 계정으로 마이그레이션하려고 합니다. 두 계정 모두 AWS Organizations에서 동일한 조직의 구성원입니다.

회사는 새 데이터베이스에 대한 DNS 컷오버를 수행하기 전에 데이터베이스 서비스 중단을 최소화해야 합니다.

이 요구 사항을 충족하는 마이그레이션 전략은 무엇입니까? (2개를 선택하세요.)

> **A.** 기존 Aurora 데이터베이스의 스냅샷을 찍습니다. 새 AWS 계정과 스냅샷을 공유합니다. 스냅샷의 새 계정에 Aurora DB 클러스터를 생성합니다.
> **B.** 새 AWS 계정에 Aurora DB 클러스터를 생성합니다. AWS Database Migration Service(AWS DMS)를 사용하여 두 Aurora DB 클러스터 간에 데이터를 마이그레이션합니다.
> **C.** AWS 백업을 사용하여 기존 AWS 계정의 Aurora 데이터베이스 백업을 새 AWS 계정으로 공유합니다. 스냅샷에서 새 AWS 계정에 Aurora DB 클러스터를 생성합니다.
> **D.** 새 AWS 계정에 Aurora DB 클러스터를 생성합니다. AWS Application Migration Service를 사용하여 두 Aurora DB 클러스터 간에 데이터를 마이그레이션합니다.
>
> 해설
> 정답: A,B
> A: 기존 Aurora 데이터베이스의 스냅샷을 찍고 이를 새로운 AWS 계정과 공유한 다음, 새 계정에서

스냅샷을 사용하여 Aurora DB 클러스터를 생성합니다. 이 방법은 데이터베이스 서비스 중단을 최소화하면서 마이그레이션을 수행할 수 있음.
B: 새로운 AWS 계정에서 Aurora DB 클러스터를 생성하고, AWS 데이터베이스 마이그레이션 서비스(AWS DMS)를 사용하여 두 Aurora DB 클러스터 간에 데이터를 마이그레이션합니다.
AWS DMS를 사용하면 데이터베이스 서비스가 실행 중인 상태에서 데이터를 이동할 수 있으므로 서비스 중단 시간을 최소화할 수 있음.
C(x): AWS Backup은 다른 AWS 계정과 공유할 수는 없음.

◆ | **Q#0440.** | **Ref#0440.**
SaaS(Software as a Service) 회사는 고객에게 미디어 소프트웨어 솔루션을 제공합니다. 이 솔루션은 다양한 AWS 리전 및 AWS 계정에 걸쳐 50개의 VPC에서 호스팅됩니다. VPC 중 하나가 관리 VPC로 지정됩니다. VPC의 컴퓨팅 리소스는 독립적으로 작동합니다.

이 회사는 50개 VPC 모두가 서로 통신할 수 있어야 하는 새로운 기능을 개발했습니다. 또한 새로운 기능을 사용하려면 각 고객의 VPC에서 회사의 관리 VPC로 단방향 액세스가 필요합니다. 관리 VPC는 ??미디어 소프트웨어 솔루션에 대한 라이선스를 검증하는 컴퓨팅 리소스를 호스팅합니다.

회사가 솔루션을 호스팅하는 데 사용할 VPC의 수는 솔루션이 성장함에 따라 계속해서 늘어날 것입니다.

최소한의 운영 오버헤드로 필요한 VPC 연결을 제공하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. 전송 게이트웨이를 생성합니다. 모든 회사의 VPC 및 관련 서브넷을 Transit Gateway에 연결합니다.
B. 회사의 모든 VPC 간에 VPC 피어링 연결을 생성합니다.
C. 라이선스 검증을 위해 컴퓨팅 리소스를 가리키는 NLB(Network Load Balancer)를 생성합니다. 각 고객의 VPC가 사용할 수 있는 AWS PrivateLink 엔드포인트 서비스를 생성합니다. 엔드포인트 서비스를 NLB와 연결합니다.
D. 각 고객의 VPC에 VPN 어플라이언스를 생성합니다. AWS Site-to-Site VPN을 사용하여 회사의 관리 VPC를 각 고객의 VPC에 연결합니다.
E. 회사의 관리 VPC와 각 고객의 VPC 간에 VPC 피어링 연결을 생성합니다.

해설
정답: A,C
A: Transit Gateway는 중앙 허브 역할을 하여 VPC 간 통신을 단순화하고 VPC의 수가 증가함에 따라 잘 확장됩니다.
C: AWS PrivateLink는 각 고객 VPC에서 회사의 관리 VPC로의 단방향 액세스가 가능하게 합니다. 이 방법은 각 고객 VPC에서 특정 서비스에 대한 액세스를 제어하므로 보안적인 측면에서 유리합니다. 또한 각 VPC 간의 라우팅이 필요하지 않으므로 관리적인 부담이 적습니다.
B: VPC 피어링 연결은 각 회사의 VPC 간에 직접 연결을 설정하여 모든 VPC 간의 통신을 용이하게 합니다. 이것은 비교적 간단하고 효율적인 방법이지만, 여러 VPC 간의 라우팅이 복잡해질 수 있습니다.
A가 틀린 이유는 한 지역의 VPC를 다른 지역의 TGW에 연결할 수 없습니다. 동일한 리전의 TGW에만 VPC를 연결할 수 있기 때문입니다.
Transit Gateway Peering

441 (박지수) 1회차 完

◆ | **Q#0441.** | **Ref#0441.**
한 회사에 여러 사업부(LOB)가 있으며, 이들은 모회사에 속해 있습니다. 회사는 솔루션 아키텍트에게 다음 요구 사항을 충족하는 솔루션을 개발하도록 요청했습니다:

- LOB에서 사용하는 모든 AWS 계정에 대해 단일 AWS 청구서를 생성합니다.
- 청구서에서 각 LOB 계정의 비용을 구분하여 표시합니다.

- 회사의 거버넌스 정책에 따라 LOB 계정에서 서비스와 기능을 제한할 수 있는 기능을 제공합니다.
- 각 LOB 계정은 거버넌스 정책에 상관없이 전체 관리자 권한을 위임받아야 합니다.

솔루션 아키텍트가 이 요구 사항을 충족하기 위해 취해야 할 단계의 조합은 무엇입니까? (두 가지를 선택하십시오.)

> **A.** AWS Organizations를 사용하여 각 LOB의 상위 계정에 조직을 생성하십시오. 그런 다음 각 LOB 계정을 적절한 조직에 초대합니다.
> **B.** AWS Organizations를 사용하여 상위 계정에 단일 조직을 생성하십시오. 그런 다음 각 LOB의 AWS 계정을 초대하여 조직에 가입합니다.
> **C.** 서비스 할당량을 구현하여 허용되는 서비스와 기능을 정의하고 할당량을 적절하게 각 LOB에 적용합니다.
> **D.** 승인된 서비스 및 기능만 허용하는 SCP를 생성한 다음 LOB 계정에 정책을 적용합니다.
> **E.** 상위 계정의 결제 콘솔에서 통합 청구를 활성화하고 LOB 계정을 연결합니다.
>
> 해설
> 정답: B,E
> B: AWS Organizations를 사용하여 모계정에 단일 조직을 생성하고, 각 LOB 계정을 조직에 초대함으로써 중앙에서 계정을 관리할 수 있습니다. 이를 통해 통합된 청구서와 계정 관리가 용이해집니다.
> E: AWS Organizations에서 통합 청구 기능을 활성화하면 모든 LOB 계정의 비용이 모계정으로 집계되며, 청구서에서 각 계정의 비용이 구분되어 표시됩니다. D(x): 서비스 제한을 위한 SCP를 적용하는 것은 LOB 계정에 전체 관리자 권한을 부여하려는 요구 사항과 상충됨.

◆ | **Q#0442.** | **Ref#0442.**
솔루션 아키텍트는 사용자 지정 도메인 아래 두 AWS 리전의 사용자에게 서비스를 제공하는 웹 애플리케이션을 배포했습니다. 애플리케이션은 Amazon Route 53 지연 시간 기반 라우팅을 사용합니다. 솔루션 아키텍트는 각 지역에 대해 별도의 가용 영역에 있는 웹 서버 쌍과 가중치 기반 레코드 세트를 연결했습니다.

솔루션 설계자는 재해 복구 시나리오를 실행합니다. 한 리전의 모든 웹 서버가 중지되었을 때, Route 53은 자동으로 사용자를 다른 리전으로 리디렉션하지 않았습니다.

다음 중 이 문제의 근본 원인은 무엇입니까? (2개를 선택하세요.)

> **A.** 웹 서버가 중지된 지역의 가중치는 다른 지역의 가중치보다 높습니다.
> **B.** 보조 지역의 웹 서버 중 하나가 HTTP 상태 확인을 통과하지 못했습니다.
> **C.** 지연 리소스 레코드 세트는 가중치 리소스 레코드 세트와 함께 사용할 수 없습니다.
> **D.** 웹 서버가 중지된 리전의 도메인과 연결된 지연 시간 별칭 리소스 레코드 세트에 대해 대상 상태를 평가하는 설정이 켜져 있지 않습니다.
> **E.** 중지된 웹 서버와 연결된 하나 이상의 가중치 기반 리소스 레코드 세트에 대해 HTTP 상태 확인이 설정되지 않았습니다.
>
> 해설
> 정답: D, E
> D: "Evaluate Target Health" 설정이 활성화되어 있어야 Route 53이 리소스의 상태를 평가하고, 리소스가 비정상이면 대체 리소스를 선택할 수 있음.
> 상태 평가 설정이 켜져 있지 않으면 상태에 따라 트래픽이 자동으로 다른 리전으로 리디렉션되지 않음.
> E: HTTP 상태 검사가 설정되지 않은 경우, Route 53은 리소스가 비정상인지 알 수 없으므로 트래픽을 계속해서 중지된 서버로 보낼 수 있음.
> HTTP 상태 검사가 있어야 리소스가 비정상일 때 트래픽을 다른 리소스로 리디렉션할 수 있습니다.

◆ | **Q#0443.** | **Ref#0443.**
홍수 모니터링 기관은 10,000개 이상의 수위 모니터링 센서를 배치했습니다. 센서는 지속적인 데이터 업데이트를

보내며 각 업데이트의 크기는 1MB 미만입니다. 이 기관은 온프레미스 애플리케이션 서버를 보유하고 있습니다. 이러한 서버는 센서로부터 업데이트를 수신하고, 원시 데이터를 사람이 읽을 수 있는 형식으로 변환하고, 결과를 온프레미스 관계형 데이터베이스 서버에 기록합니다. 그런 다음 데이터 분석가는 간단한 SQL 쿼리를 사용하여 데이터를 모니터링합니다.

기관에서는 전반적인 애플리케이션 가용성을 높이고 유지 관리 작업을 수행하는 데 필요한 노력을 줄이고 싶어합니다. 애플리케이션 서버에 대한 업데이트 및 패치를 포함하는 이러한 유지 관리 작업으로 인해 가동 중지 시간이 발생합니다. 애플리케이션 서버가 다운되면 나머지 서버가 전체 작업 부하를 처리할 수 없기 때문에 센서의 데이터가 손실됩니다.

기관에서는 운영 오버헤드와 비용을 최적화하는 솔루션을 원합니다. 솔루션 아키텍트는 AWS IoT Core를 사용하여 센서 데이터를 수집할 것을 권장합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 또 무엇을 권장해야 합니까?

> **A.** 센서 데이터를 Amazon Kinesis Data Firehose로 보냅니다. AWS Lambda 함수를 사용하여 Kinesis Data Firehose 데이터를 읽고 .csv 형식으로 변환한 후 Amazon Aurora MySQL DB 인스턴스에 삽입합니다. 데이터 분석가에게 DB 인스턴스에서 직접 데이터를 쿼리하도록 지시합니다.
> **B.** 센서 데이터를 Amazon Kinesis Data Firehose로 보냅니다. AWS Lambda 함수를 사용하여 Kinesis Data Firehose 데이터를 읽고 이를 Apache Parquet 형식으로 변환한 후 Amazon S3 버킷에 저장합니다. 데이터 분석가에게 Amazon Athena를 사용하여 데이터를 쿼리하도록 지시합니다.
> **C.** 센서 데이터를 Apache Flink용 Amazon Managed Service(이전의 Amazon Kinesis Data Analytics) 애플리케이션으로 보내 데이터를 .csv 형식으로 변환하고 Amazon S3 버킷에 저장합니다. 데이터를 Amazon Aurora MySQL DB 인스턴스로 가져옵니다. 데이터 분석가에게 DB 인스턴스에서 직접 데이터를 쿼리하도록 지시합니다.
> **D.** 센서 데이터를 Apache Flink용 Amazon Managed Service(이전의 Amazon Kinesis Data Analytics) 애플리케이션으로 보내 데이터를 Apache Parquet 형식으로 변환하고 Amazon S3 버킷에 저장합니다. 데이터 분석가에게 Amazon Athena를 사용하여 데이터를 쿼리하도록 지시합니다.
>
> 해설
> 정답: B (or D?)
> 문제에서 요구하는대로 데이터를 처리하고 기존의 유지 보수 문제를 해결하기 위해 서버리스 및 관리형 서비스를 사용해야 합니다.
> AWS Lambda를 사용하여 Kinesis Data Firehose의 데이터를 Parquet 형식으로 변환한 후 S3에 저장하면(서버리스 방식) 기존 서버 관리와 관련된 유지 관리 노력이 줄어듭니다. Lambda는 들어오는 워크로드에 따라 자동으로 확장되어 가동 중지 없이 지속적인 데이터 처리를 보장합니다.
> B: 데이터 수집, 변환 및 저장을 자동화하여 운영 오버헤드를 줄입니다. AWS Lambda는 Kinesis Data Firehose에서 데이터를 읽어 효율적인 저장 형식인 Apache Parquet으로 변환합니다.
> 변환된 데이터는 Amazon S3에 저장되고, 데이터 분석가는 Amazon Athena를 사용하여 SQL 쿼리를 통해 데이터를 쉽게 분석할 수 있음.
>
> D: Apache flink는 스트리밍 및 변환을 위한 관리형 서비스이므로 일을 더 단순하게 만든다.
> 데이터 변환을 위해 관리형 서비스를 사용하면 운영 오버헤드가 최적화됩니다.
> Amazon Managed Service for Apache Flink는 실시간 데이터 스트리밍 처리를 위해 설계된 관리형 서비스입니다.
> Apache Flink를 사용하면 복잡한 데이터 처리 논리를 구현할 수 있으며, 대용량 데이터를 효율적으로 변환할 수 있음.
> B와 D 모두 유사한 방식으로 데이터를 처리하고 저장하지만, Amazon Managed Service for Apache Flink는 실시간 데이터 처리를 위한 더 강력한 기능을 제공합니다. 이는 대규모 데이터 스트리밍 환경에서 특히 중요합니다. 따라서, 더 강력하고 실시간 처리가 가능한 D가 더 적합한 선택입니다.

◆ | **Q#0444.** | **Ref#0444.**
공개 소매 웹 애플리케이션은 여러 가용 영역(AZ)에 걸쳐 실행되는 Amazon EC2 인스턴스 앞에 Application Load

Balancer (ALB)를 사용하며, Amazon RDS MySQL Multi-AZ 배포를 백엔드로 사용합니다. 타겟 그룹 health check는 HTTP를 사용하도록 구성되고 제품 카탈로그 페이지를 가리킵니다. Auto Scaling은 ALB 상태 확인을 기반으로 웹 플릿 크기를 유지하도록 구성됩니다.

최근 애플리케이션이 중단되었습니다. Auto Scaling은 중단 중에 인스턴스를 지속적으로 교체했습니다. 후속 조사에서는 웹 서버 지표가 정상 범위 내에 있었지만 데이터베이스 계층에 높은 로드가 발생하여 쿼리 응답 시간이 심각하게 늘어난 것으로 확인되었습니다.

다음 중 향후 성장을 위해 전체 애플리케이션 스택의 가용성 및 기능에 대한 모니터링 기능을 개선하는 동시에 이러한 문제를 해결하는 변경 사항은 무엇입니까? (2개를 선택하세요.)

> **A.** Amazon RDS MySQL에 대한 읽기 전용 복제본을 구성하고 웹 애플리케이션에서 단일 리더 엔드포인트를 사용하여 백엔드 데이터베이스 계층의 로드를 줄입니다.
> **B.** 제품 카탈로그 페이지 대신 간단한 HTML 페이지를 가리키도록 대상 그룹 상태 확인을 구성하고 제품 페이지에 대한 Amazon Route 53 상태 확인을 구성하여 전체 애플리케이션 기능을 평가합니다. 사이트에 장애가 발생하면 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.
> **C.** Amazon EC2 웹 서버의 TCP 확인과 제품 페이지에 대한 Amazon Route 53 상태 확인을 사용하여 전체 애플리케이션 기능을 평가하도록 대상 그룹 상태 확인을 구성합니다. 사이트에 장애가 발생하면 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.
> **D.** 데이터베이스 계층에서 로드가 높고 손상된 RDS 인스턴스를 복구하는 작업을 사용하여 Amazon RDS에 대한 Amazon CloudWatch 경보를 구성합니다.
> **E.** Amazon ElastiCache 클러스터를 구성하고 이를 웹 애플리케이션과 RDS MySQL 인스턴스 사이에 배치하여 백엔드 데이터베이스 계층의 로드를 줄입니다.
>
> 해설
> 정답: B,E
> Health Check를 단순 HTML 페이지로 변경하면 ALB는 기본적인 웹 서버 가용성을 확인할 수 있습니다. Route 53 건강 체크는 전체 애플리케이션 기능(제품 페이지)을 평가하는 데 사용됩니다. 이렇게 하면 데이터베이스 부하로 인해 제품 페이지 로드가 실패할 경우를 감지할 수 있습니다.
> CloudWatch 알람은 사이트가 실패할 때 관리자가 신속히 대응할 수 있도록 도와줍니다.
> 대상 그룹 헬스 체크를 간단한 HTML 페이지로 지정하고 Amazon Route 53 헬스 체크를 사용하여 전체 애플리케이션 기능을 평가하도록 구성합니다. 이렇게 하면 데이터베이스 티어를 헬스 체크 중에 우회할 수 있습니다.
> ElastiCache는 자주 조회되는 데이터를 캐시하여 RDS에 대한 읽기 요청을 줄여줌. 이는 데이터베이스의 부하를 줄이고, 성능과 응답 시간을 개선

◆ | **Q#0445.** | **Ref#0445.**
한 회사는 온프레미스 데이터 센터를 보유하고 있으며 Kubernetes를 사용하여 AWS에서 새로운 솔루션을 개발하고 있습니다. 이 회사는 개발 및 테스트 환경에 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 사용합니다.

프로덕션 워크로드를 위한 EKS 제어 플레인과 데이터 플레인은 온프레미스에 있어야 합니다. 회사에는 Kubernetes 관리를 위한 AWS 관리형 솔루션이 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 온프레미스 데이터 센터에 AWS Outposts 서버를 설치합니다. 프로덕션 워크로드를 위해 Outposts 서버에서 로컬 클러스터 구성을 사용하여 Amazon EKS를 배포합니다.
> **B.** 온프레미스 데이터 센터에 있는 회사 하드웨어에 Amazon EKS Anywhere를 설치합니다. EKS Anywhere 클러스터에 프로덕션 워크로드를 배포합니다.
> **C.** 온프레미스 데이터 센터에 AWS Outposts 서버를 설치합니다. 프로덕션 워크로드를 위해 Outposts 서버에서 확장된 클러스터 구성을 사용하여 Amazon EKS를 배포합니다.
> **D.** 온프레미스 데이터 센터에 AWS Outposts 서버를 설치합니다. Outposts 서버에 Amazon EKS Anywhere를 설치합니다. EKS Anywhere 클러스터에 프로덕션 워크로드를 배포합니다.

해설
정답: A
Outposts 서버에서 로컬 클러스터 구성을 사용하여 EKS 배포하면 제어 플레인과 데이터 플레인이 모두 온프레미스에 있음
Outposts 서버에서 확장된 클러스터 구성을 사용하여 EKS 배포하면 제어 플레인은 AWS, 데이터 플레인은 온프레미스에 있음
EKS Anywhere는 고객이 관리하는 것이므로 AWS 관리형 솔루션이 아님
D(x): Amazon EKS Anywhere는 AWS Outposts에서 지원되지 않습니다.
B(x): Amazon EKS Anywhere는 AWS가 구축한 컨테이너 관리 소프트웨어로 오픈 소스이며 무료로 사용가능, 고객이 직접 관리하고 단독 사용가능
Amazon EKS Anywhere는 인프라 설정 및 Kubernetes 클러스터 수명 주기 작업과 같은 획일적이고 힘든 작업을 자동화하여 온프레미스 Kubernetes 클러스터 관리를 간소화
Outposts의 Amazon EKS : AWS Outposts는 온프레미스 시설의 기본 AWS 서비스, 인프라 및 운영 모델을 지원합니다. Outposts의 Amazon EKS를 사용하면 확장 또는 로컬 클러스터를 실행하도록 선택할 수 있습니다. 확장 클러스터를 사용하면 Kubernetes 컨트롤 플레인이 AWS 리전에서 실행되고 노드가 Outposts에서 실행됩니다. 로컬 클러스터를 사용하면 Kubernetes 컨트롤 플레인과 노드를 모두 포함하여 전체 Kubernetes 클러스터가 Outposts에서 로컬로 실행됩니다.
C(x): 확장 클러스터는 컨트롤 플레인이 AWS 리전에서 실행 Compare EKS Anywhere and EKS | Amazon EKS 배포 옵션

◆ | **Q#0446.** | **Ref#0446.**
회사는 AWS Organizations를 사용하여 개발 환경을 관리합니다. 회사의 각 개발 팀에는 자체 AWS 계정이 있습니다. 각 계정에는 겹치지 않는 단일 VPC 및 CIDR 블록이 있습니다.

회사는 공유 서비스 계정에 Amazon Aurora DB 클러스터를 보유하고 있습니다. 모든 개발팀은 DB 클러스터의 실시간 데이터로 작업해야 합니다.

최소한의 운영 오버헤드로 DB 클러스터에 필요한 연결을 제공하는 솔루션은 무엇입니까?

A. DB 클러스터에 대한 AWS Resource Access Manager(AWS RAM) 리소스 공유를 생성합니다. 모든 개발 계정과 DB 클러스터를 공유합니다.
B. 공유 서비스 계정에 전송 게이트웨이를 생성합니다. Transit Gateway에 대한 AWS Resource Access Manager(AWS RAM) 리소스 공유를 생성합니다. 모든 개발 계정과 전송 게이트웨이를 공유합니다. 개발자에게 리소스 공유를 수락하도록 지시합니다. 네트워킹을 구성합니다.
C. DB 클러스터의 IP 주소를 가리키는 ALB(Application Load Balancer)를 생성합니다. ALB를 사용하는 AWS PrivateLink 엔드포인트 서비스를 생성합니다. 각 개발 계정이 엔드포인트 서비스에 연결할 수 있도록 권한을 추가하세요.
D. 공유 서비스 계정에서 AWS Site-to-Site VPN 연결을 생성합니다. 네트워킹을 구성합니다. 각 개발 계정에서 AWS Marketplace VPN 소프트웨어를 사용하여 Site-to-Site VPN 연결에 연결합니다.

해설
정답: B
전송 게이트웨이는 VPC 간 및 온프레미스 네트워크 간에 쉽게 연결할 수 있는 중앙 허브로 여러 VPC와 계정을 간단히 연결할 수 있음.
AWS RAM을 사용하여 전송 게이트웨이를 공유하면 각 개발 팀이 자신의 계정에서 네트워크를 쉽게 연결할 수 있어 운영 오버헤드가 적고, 스케일링이 쉽고, 중앙 집중식 관리를 가능.
A(x): AWS RAM을 사용하여 Aurora DB 클러스터를 공유할 수 있지만 실시간이 아닌 복제본으로 공유가능.
C(x): PrivateLink에는 ALB가 아닌 NLB가 필요함.
D(x): 각 개발 계정에 VPN 연결을 설정하고 유지 관리하는 데 많은 노력이 필요함.

◆ | **Q#0447.** | **Ref#0447.**
한 회사는 AWS CloudFormation을 사용하여 AWS 회원 계정에 새로운 인프라를 모두 생성했습니다. 리소스는 거

의 변경되지 않으며 예상 로드에 맞게 크기가 적절하게 조정됩니다. 월별 AWS 청구서는 일관됩니다.

개발자가 테스트를 위해 새 리소스를 생성하고 테스트가 완료되면 리소스를 제거하는 것을 잊어버리는 경우가 있습니다. 이러한 테스트의 대부분은 리소스가 더 이상 필요하지 않을 때까지 며칠 동안 지속됩니다.

회사는 사용되지 않은 리소스를 찾는 프로세스를 자동화하려고 합니다. 솔루션 아키텍트는 AWS 청구서 비용이 증가하는지 여부를 결정하는 솔루션을 설계해야 합니다. 솔루션은 비용 증가를 유발하는 리소스를 식별하는 데 도움이 되어야 하며 회사 운영 팀에 자동으로 알려야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 청구 알림을 켜십시오. AWS Cost Explorer를 사용하여 지난달 비용을 확인합니다. 총 예상 요금에 대한 Amazon CloudWatch 경보를 생성합니다. Cost Explorer에서 결정한 비용보다 높은 비용 임계값을 지정합니다. 경보 임계값이 위반되면 운영팀에 알리는 알림을 추가합니다.
> **B.** 청구 알림을 켜십시오. AWS Cost Explorer를 사용하여 지난 3개월 동안의 월 평균 비용을 확인하세요. 총 예상 요금에 대한 Amazon CloudWatch 경보를 생성합니다. Cost Explorer에서 결정한 비용보다 높은 비용 임계값을 지정합니다. 경보 임계값이 위반되면 운영팀에 알리는 알림을 추가합니다.
> **C.** AWS 비용 이상 탐지를 사용하여 연결된 계정 모니터 유형이 있는 비용 모니터를 생성합니다. 일일 AWS 비용 요약을 운영 팀에 보내려면 구독을 생성하세요. 비용 차이에 대한 임계값을 지정합니다.
> **D.** AWS 비용 이상 탐지를 사용하여 모니터 유형이 AWS 서비스인 비용 모니터를 생성합니다. 일일 AWS 비용 요약을 운영 팀에 보내려면 구독을 생성하세요. 비용 차이에 대한 임계값을 지정합니다.
>
> 해설
> 정답: D
> 연결된 계정의 서비스 모니터는 해당 연결된 계정의 각 서비스에 대한 개별 지출을 모니터링하므로 비정상적인 서비스 비용 급증을 감지합니다.
> A(x), B(x)청구 알림은 지난달 비용, 지난 3개월 비용을 확인하므로 실시간 비용 증가를 감지할 수 없음
> C(x): 연결된 계정(Linkde Account) 모니터는 해당 연결된 계정에 대한 모든 서비스의 총 지출을 모니터링 하므로 개별 서비스 비용의 이상을 감지하지 못함.

◆ | **Q#0448.** | **Ref#0448.**
한 회사에서 새로운 웹 기반 애플리케이션을 배포하고 있으며 Linux 애플리케이션 서버용 스토리지 솔루션이 필요합니다. 회사는 모든 인스턴스에 대한 애플리케이션 데이터 업데이트를 위한 단일 위치를 생성하려고 합니다. 활성 데이터 세트의 크기는 최대 100GB입니다. 솔루션 설계자는 최대 작업이 매일 3시간 동안 발생하며 총 225MiBps의 읽기 처리량이 필요하다고 결정했습니다.

솔루션 아키텍트는 재해 복구(DR)를 위해 다른 AWS 리전에서 사용할 수 있는 데이터 복사본을 만드는 다중 AZ 솔루션을 설계해야 합니다. DR 복사본의 RPO는 1시간 미만입니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 새로운 Amazon Elastic File System(Amazon EFS) 다중 AZ 파일 시스템을 배포합니다. 75MiBps의 프로비저닝된 처리량을 위해 파일 시스템을 구성합니다. DR 지역의 파일 시스템에 대한 복제를 구현합니다.
> **B.** Lustre 파일 시스템용 새 Amazon FSx를 배포합니다. 파일 시스템에 대한 버스팅 처리량 모드를 구성합니다. AWS Backup을 사용하여 파일 시스템을 DR 지역에 백업합니다.
> **C.** 처리량이 225MiBps인 범용 SSD(gp3) Amazon Elastic Block Store(Amazon EBS) 볼륨을 배포합니다. EBS 볼륨에 대해 다중 연결을 활성화합니다. AWS Elastic Disaster Recovery를 사용하여 EBS 볼륨을 DR 지역에 복제합니다.
> **D.** 프로덕션 지역과 DR 지역 모두에 Amazon FSx for OpenZFS 파일 시스템을 배포합니다. 10분마다 프로덕션 파일 시스템에서 DR 파일 시스템으로 데이터를 복제하는 AWS DataSync 예약 작업을 생성합니다.

해설
정답: A
Amazon EFS는 여러 AZ에 걸쳐 데이터를 저장하여 고가용성을 제공. DR 지역에 데이터를 복제할 수 있으며, 1시간 이내의 RPO를 달성함.
EFS의 프로비저닝된 처리량 옵션을 사용하여 필요한 75 MiBps의 처리량을 설정하면 피크 시간 동안의 총 읽기 처리량 요구 사항인 225 MiBps를 충족.
B(x): AWS Backup은 백업주기 1시간 미만으로 설정 불가하므로 1시간 RPO 충족 못함
C(x): EBS는 기본적으로 다른 지역 간의 실시간 복제를 지원하지 않음.
D(x): Data Sync 작업은 1시간보다 더 자주 예약할 수 없으므로 데이터 동기화 작업을 10분마다 수행하도록 예약할 수 없음.

◆ | **Q#0449.** | **Ref#0449.**
회사는 인터넷에 연결되지 않은 원격 위치에서 실험을 통해 데이터를 수집해야 합니다. 실험 동안 로컬 네트워크에 연결된 센서는 1주일에 걸쳐 독점 형식으로 6TB의 데이터를 생성합니다. 데이터 파일을 FTP 서버에 주기적으로 업로드하도록 센서를 구성할 수 있지만 센서에는 자체 FTP 서버가 없습니다. 센서는 다른 프로토콜도 지원하지 않습니다. 회사는 실험 후 최대한 빨리 데이터를 중앙에서 수집하고 데이터를 AWS 클라우드의 객체 스토리지로 이동해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Snowball Edge Compute Optimized 디바이스를 주문하십시오. 장치를 로컬 네트워크에 연결하십시오. 대상 버킷 이름으로 AWS DataSync를 구성하고 NFS를 통해 데이터를 디바이스로 언로드합니다. 실험 후에는 데이터가 Amazon S3에 로드될 수 있도록 디바이스를 AWS로 반환합니다.
B. Amazon Linux 2 AMI를 포함한 AWS Snowcone 디바이스를 주문합니다. 장치를 로컬 네트워크에 연결하십시오. 디바이스에서 Amazon EC2 인스턴스를 시작합니다. 각 센서에서 주기적으로 데이터를 다운로드하는 셸 스크립트를 만듭니다. 실험 후에는 데이터를 Amazon Elastic Block Store(Amazon EBS) 볼륨으로 로드할 수 있도록 디바이스를 AWS로 반환합니다.
C. Amazon Linux 2 AMI를 포함한 AWS Snowcone 디바이스를 주문합니다. 장치를 로컬 네트워크에 연결하십시오. 디바이스에서 Amazon EC2 인스턴스를 시작합니다. EC2 인스턴스에 FTP 서버를 설치하고 구성합니다. EC2 인스턴스에 데이터를 업로드하도록 센서를 구성합니다. 실험 후에는 데이터가 Amazon S3에 로드될 수 있도록 디바이스를 AWS로 반환합니다.
D. AWS Snowcone 디바이스를 주문합니다. 장치를 로컬 네트워크에 연결하십시오. Amazon FSx를 사용하도록 장치를 구성합니다. 장치에 데이터를 업로드하도록 센서를 구성합니다. 업로드된 데이터를 Amazon S3 버킷과 동기화하도록 디바이스에서 AWS DataSync를 구성합니다. 데이터를 Amazon Elastic Block Store(Amazon EBS) 볼륨으로 로드할 수 있도록 디바이스를 AWS로 반환합니다.

해설
정답: C
AWS Snowcone는 연결이 거의 또는 전혀 없는 열악한 환경에서 엣지 컴퓨팅, 데이터 스토리지, 이동 중 데이터 전송을 제공하는 견고하고 안전한 소형 디바이스입니다.
데이터를 FTP 서버에 업로드하기 위해 FTP 서버 구성
Snowcone 엣지 컴퓨팅 + FTP 데이터 전송

◆ | **Q#0450.** | **Ref#0450.**
여러 사업부를 보유한 회사는 모든 기능이 활성화된 AWS Organizations를 사용하고 있습니다. 회사는 각 사업부가 자체 AWS 계정을 갖는 계정 구조를 구현했습니다. 각 AWS 계정의 관리자는 Amazon Athena를 사용하여 해당 계정에 대한 자세한 비용 및 사용률 데이터를 확인해야 합니다.

각 사업부는 자체 비용 및 활용 데이터에만 액세스할 수 있습니다. AWS 비용 및 사용 보고서 설정 기능을 관리하는 IAM 정책이 마련되어 있습니다. 조직의 모든 데이터가 포함된 중앙 비용 및 사용 보고서는 이미 Amazon S3 버킷에서 사용할 수 있습니다.

운영 복잡성을 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 조직의 마스터 계정에서 AWS Resource Access Manager(AWS RAM)를 사용하여 비용 및 사용 보고서 데이터를 각 회원 계정과 공유합니다.
> **B.** 조직의 마스터 계정에서 중앙 비용 및 사용 보고서가 포함된 S3 버킷에 새 파일이 도착할 때마다 AWS Lambda 함수를 호출하도록 S3 이벤트를 구성합니다. 각 회원 계정의 데이터를 추출하고 해당 데이터를 Amazon S3의 별도 접두사 아래에 배치하도록 Lambda 함수를 구성합니다. 각 회원 계정이 자체 접두사에 액세스할 수 있도록 S3 버킷 정책을 수정합니다.
> **C.** 각 회원 계정에서 AWS Cost Explorer에 액세스합니다. 계정에 대한 관련 비용 정보가 포함된 새 보고서를 만듭니다. Cost Explorer에 보고서를 저장합니다. 계정 관리자가 저장된 보고서에 액세스하는 데 사용할 수 있는 지침을 제공하십시오.
> **D.** 각 회원 계정에서 비용 및 사용 보고서 데이터를 저장할 새 S3 버킷을 생성합니다. 비용 및 사용 보고서를 설정하여 데이터를 새 S3 버킷으로 전달합니다.
>
> 해설
> 정답: B
> 이 방법은 중앙화된 Cost and Usage Report 데이터를 사용하여 각 비즈니스 단위의 계정에 액세스하는 데 가장 적합한 방법입니다. 각 구성원 계정에 대해 추가 S3 버킷을 생성하고 보고서를 설정할 필요가 없으며, Lambda 함수를 사용하여 데이터를 추출하고 처리하는 방법을 통해 운영 복잡성을 최소화할 수 있습니다.
> B: 버킷에서 이미 보고서를 사용할 수 있다는 점을 고려하면 운영 복잡성이 가장 낮습니다. 초기 설정 후 프로세스는 완전 자동으로 이루어집니다. 즉, 계정 관리자의 별도 작업과 관련된 운영 복잡성이 필요하지 않습니다.

451 (송희성) 1회차 完

◆ | **Q#0451.** | **Ref#0451.**
한 회사가 제조 애플리케이션을 위한 AWS 환경을 설계하고 있습니다. 애플리케이션은 고객에게 성공적이었으며 애플리케이션의 사용자 기반이 증가했습니다. 회사는 1Gbps AWS Direct Connect 연결을 통해 AWS 환경을 회사의 온프레미스 데이터 센터에 연결했습니다. 회사는 연결을 위해 BGP를 구성했습니다.

회사는 솔루션의 가용성, 내결함성, 보안을 보장하기 위해 기존 네트워크 연결 솔루션을 업데이트해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** 동적 프라이빗 IP AWS Site-to-Site VPN을 보조 경로로 추가하여 전송 중인 데이터를 보호하고 Direct Connect 연결에 대한 복원력을 제공합니다. Direct Connect 연결 내부의 트래픽을 암호화하도록 MACsec을 구성합니다.
> **B.** 회사의 온프레미스 데이터 센터와 AWS 간에 또 다른 Direct Connect 연결을 프로비저닝하여 전송 속도를 높이고 복원력을 제공합니다. Direct Connect 연결 내부의 트래픽을 암호화하도록 MACsec을 구성합니다.
> **C.** 여러 프라이빗 VIF를 구성합니다. 복원력을 제공하기 위해 온프레미스 데이터 센터와 AWS 사이의 VIF에 걸쳐 데이터 로드 밸런싱을 수행합니다.
> **D.** 전송 중인 데이터를 보호하고 Direct Connect 연결에 대한 복원력을 제공하기 위해 정적 AWS Site-to-Site VPN을 보조 경로로 추가합니다.
>
> 해설
> 정답: D
> 비용 효율성: Site-to-Site VPN을 보조 경로로 추가하는 것은 비용 효율적인 방법. VPN은 직접적인 추가 Direct Connect 연결보다 저렴하며, 탄력성과 보안을 제공.
> 탄력성: VPN 보조 경로로 설정하면 Direct Connect 연결이 실패할 경우 자동으로 VPN 경로로 전환

되어 고가용성과 내결함성을 제공합니다.
보안: VPN을 사용하면 데이터 전송 중 암호화를 제공하여 보안을 강화할 수 있습니다.
A(x), B(x): MACsec은 10Gbps, 100Gbps 에서만 지원되고 1Gbps Direct Connect 미지원. MACsec는 비용과 복잡성을 초래함.
C(x): 프라이빗 VIF를 사용하여 로드 밸런싱을 제공할 수 있지만, 이는 Direct Connect의 기본 연결 수를 증가시키지 않으며, 내결함성을 위한 추가 경로를 제공하지 않음.
MacSec reference

◆ | **Q#0452.** | **Ref#0452.**
회사는 애플리케이션을 현대화하고 해당 애플리케이션을 AWS로 마이그레이션해야 합니다. 애플리케이션은 사용자 프로필 데이터를 온프레미스 MySQL 데이터베이스의 단일 테이블에 텍스트로 저장합니다.

현대화 후에 사용자는 애플리케이션을 사용하여 최대 4GB 크기의 비디오 파일을 업로드하게 됩니다. 다른 사용자는 애플리케이션에서 비디오 파일을 다운로드할 수 있어야 합니다. 회사에는 신속한 확장을 제공하는 비디오 스토리지 솔루션이 필요합니다. 솔루션은 애플리케이션 성능에 영향을 주어서는 안 됩니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 Amazon Aurora PostgreSQL로 마이그레이션합니다. 비디오를 데이터베이스의 TEXT 열에 base64로 인코딩된 문자열로 저장합니다.
B. AWS Schema Conversion Tool(AWS SCT)과 함께 AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 Amazon DynamoDB로 마이그레이션합니다. 비디오를 Amazon S3에 객체로 저장합니다. 해당 DynamoDB 항목에 S3 키를 저장합니다.
C. AWS Schema Conversion Tool(AWS SCT)과 함께 AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 Amazon Keyspaces(Apache Cassandra용)로 마이그레이션합니다. 비디오를 Amazon S3에 객체로 저장합니다. 해당 Amazon Keyspaces 항목에 S3 객체 식별자를 저장합니다.
D. AWS Schema Conversion Tool(AWS SCT)과 함께 AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 Amazon DynamoDB로 마이그레이션합니다. 해당 DynamoDB 항목에 비디오를 base64로 인코딩된 문자열로 저장합니다.

해설
정답: B
비디오를 S3의 객체로 저장하면 대용량 파일을 저장하는 데 확장 가능하고 비용 효율적
DynamoDB는 비디오 메타데이터(S3 키 포함)를 저장할 수 있으므로 비디오를 효율적으로 검색하고 관리할 수 있음.
A(x), D(x): 비디오를 base64로 인코딩하여 저장하는 것은 비효율적임.
C(x): Apache Cassandra는 운영 및 유지관리가 어려우며, S3는 많은 Site에서 DynamoDB와 연결되며, 문서화도 잘 되어있음.
large object best pratice

◆ | **Q#0453.** | **Ref#0453.**
회사는 Amazon Elastic File System(Amazon EFS) 파일 시스템에 문서를 저장하고 관리합니다. 파일 시스템은 AWS Key Management Service(AWS KMS) 키로 암호화됩니다. 파일 시스템은 독점 소프트웨어를 실행하는 Amazon EC2 인스턴스에 탑재됩니다.

회사는 파일 시스템에 대한 자동 백업을 활성화했습니다. 자동 백업은 AWS Backup 기본 백업 계획을 사용합니다.

솔루션 설계자는 삭제된 문서를 RPO 100분 이내에 복구할 수 있는지 확인해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 새로운 IAM 역할을 생성합니다. 새 백업 계획을 만듭니다. 새로운 IAM 역할을 사용하여 백업을 생성합니다. 새 IAM 역할이 키를 사용할 수 있도록 KMS 키 정책을 업데이트합니다. 파일 시스템에

대해 시간별 백업 일정을 구현합니다.
B. 새로운 백업 계획을 생성합니다. AWSServiceRoleForBackup IAM 역할이 키를 사용할 수 있도록 KMS 키 정책을 업데이트합니다. 30분마다 파일 시스템 백업을 실행하려면 사용자 정의 cron 표현식을 구현하십시오.
C. 새로운 IAM 역할을 생성합니다. 기존 백업 계획을 사용합니다. 새 IAM 역할이 키를 사용할 수 있도록 KMS 키 정책을 업데이트합니다. 특정 시점 복구를 위해 지속적인 백업을 활성화합니다.
D. 기존 백업 계획을 사용합니다. AWSServiceRoleForBackup IAM 역할이 키를 사용할 수 있도록 KMS 키 정책을 업데이트합니다. 파일 시스템에 대해 교차 지역 복제를 활성화합니다.

해설
정답: A
C(x), D(x): 기존의 기본 백업 계획은 1일 1회 백업으로 RPO 100분 보장불가
B(x): EFS의 백업 주기는 최소 1시간으로 30분 마다 백업실행은 불가능
EFS Backup

◆ | **Q#0454.** | **Ref#0454.**
솔루션 아키텍트는 클라우드 엔지니어 팀이 AWS CLI를 사용하여 Amazon S3 버킷에 객체를 업로드할 수 있는 안전한 방법을 제공해야 합니다. 각 클라우드 엔지니어에는 IAM 사용자, IAM 액세스 키 및 가상 다단계 인증(MFA) 디바이스가 있습니다. 클라우드 엔지니어의 IAM 사용자는 S3-access라는 그룹에 있습니다. 클라우드 엔지니어는 MFA를 사용하여 Amazon S3에서 작업을 수행해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. IAM 사용자가 S3 버킷에서 작업을 수행할 때 IAM 사용자에게 MFA 코드를 묻는 메시지를 표시하도록 S3 버킷에 정책을 연결합니다. AWS CLI와 함께 IAM 액세스 키를 사용하여 Amazon S3를 호출합니다.
B. 주체가 그룹을 맡을 때 주체가 MFA를 사용하도록 요구하도록 S3 액세스 그룹에 대한 신뢰 정책을 업데이트합니다. AWS CLI와 함께 IAM 액세스 키를 사용하여 Amazon S3를 호출합니다.
C. MFA가 존재하지 않는 한 모든 S3 작업을 거부하도록 S3 액세스 그룹에 정책을 연결합니다. AWS CLI와 함께 IAM 액세스 키를 사용하여 Amazon S3를 호출합니다.
D. MFA가 존재하지 않는 한 모든 S3 작업을 거부하도록 S3 액세스 그룹에 정책을 연결합니다. AWS Security Token Service(AWS STS)에서 임시 자격 증명을 요청합니다. 사용자가 Amazon S3에서 작업을 수행할 때 Amazon S3가 참조할 프로필에 임시 자격 증명을 연결합니다.

해설
정답: D
D: MFA를 강제하기 위해서는 AWS Security Token Service(AWS STS)가 필수.
A(x), C(x): AWS CLI와 함께 IAM Access Key를 사용하면 MFA를 건너뛰게 되어 강제할 수 없음.
B(x): MFA는 역할이나 그룹을 맡을 때뿐만 아니라 특정 작업에도 필요함.

◆ | **Q#0455.** | **Ref#0455.**
회사는 60개의 온프레미스 레거시 애플리케이션을 AWS로 마이그레이션해야 합니다. 응용 프로그램은 .NET Framework를 기반으로 하며 Windows에서 실행됩니다.

회사에는 마이그레이션 시간을 최소화하고 애플리케이션 코드 변경이 필요하지 않은 솔루션이 필요합니다. 회사는 또한 인프라 관리를 원하지 않습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Toolkit for NET Refactoring을 사용하여 애플리케이션을 리팩터링하고 컨테이너화합니다. Fargate 시작 유형과 함께 Amazon Elastic Container Service(Amazon ECS)를 사용하여 컨테이너화된 애플리케이션을 호스팅합니다.

B. Windows Web Application Migration Assistant를 사용하여 애플리케이션을 AWS Elastic Beanstalk로 마이그레이션합니다. Elastic Beanstalk를 사용하여 애플리케이션을 배포하고 관리하세요.
C. Windows Web Application Migration Assistant를 사용하여 애플리케이션을 Amazon EC2 인스턴스로 마이그레이션합니다. EC2 인스턴스를 사용하여 애플리케이션을 배포하고 관리합니다.
D. AWS Toolkit for NET Refactoring을 사용하여 애플리케이션을 리팩터링하고 컨테이너화합니다. Fargate 시작 유형과 함께 Amazon Elastic Kubernetes Service(Amazon EKS)를 사용하여 컨테이너화된 애플리케이션을 호스팅합니다.

해설
정답: B
Elastic Beanstalk는 Go, Java, .NET, Node.js, PHP, Python 및 Ruby에서 개발된 애플리케이션을 지원합니다.
A(x), D(x): 어플리케이션 소스 변경을 하지 않는 것이 요구사항이므로 애플리케이션 리팩터링은 탈락
C(x): EC2 인스턴스를 활용 시 인프라 관리 주체가 사용자가 됨
Elastic Beanstalk에서 Windows .NET 시작하기

◆ | **Q#0456.** | **Ref#0456.**
회사는 Amazon S3 버킷에 저장된 데이터에 대해 대규모 일괄 처리 작업을 실행해야 합니다. 작업은 시뮬레이션을 수행합니다. 작업 결과는 시간에 민감하지 않으며 프로세스는 중단을 견딜 수 있습니다.

데이터가 S3 버킷에 저장될 때 각 작업은 15~20GB의 데이터를 처리해야 합니다. 회사는 추가 분석을 위해 작업의 출력을 다른 Amazon S3 버킷에 저장합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 서버리스 데이터 파이프라인을 생성합니다. 오케스트레이션을 위해 AWS Step Functions를 사용하세요. 프로비저닝된 용량과 함께 AWS Lambda 함수를 사용하여 데이터를 처리합니다.
B. Amazon EC2 스팟 인스턴스를 포함하는 AWS Batch 컴퓨팅 환경을 생성합니다. SPOT_CAPACITY_OPTIMIZED 할당 전략을 지정합니다.
C. Amazon EC2 온디맨드 인스턴스 및 스팟 인스턴스를 포함하는 AWS Batch 컴퓨팅 환경을 생성합니다. 스팟 인스턴스에 대한 SPOT_CAPACITY_OPTIMIZED 할당 전략을 지정합니다.
D. Amazon Elastic Kubernetes Service(Amazon EKS)를 사용하여 처리 작업을 실행합니다. Amazon EC2 온디맨드 인스턴스와 스팟 인스턴스의 조합이 포함된 관리형 노드 그룹을 사용합니다.

해설
정답: B
시간에 민감하지 않으며 프로세스가 중단을 견딜 수 있음" -> 스팟
시간에 민감하지 않은 스팟 인스턴스가 포함된 AWS Batch
C(x), D(x): 온디맨드와 스팟 인스턴스를 함께 포함하므로 B가 더 비용 효율적
A(x): AWS Lambda 함수는 15분 제한이 있다. 15~20GB를 처리하기엔 짧은 시간이며 데이터 처리를 위해 프로비저닝된 용량 사용은 서버리스 아키텍처와는 상반된 내용
SPOT Instance AWS

◆ | **Q#0457.** | **Ref#0457.**
회사에는 온프레미스에서 이미지 데이터를 분석하고 저장하는 애플리케이션이 있습니다. 이 애플리케이션은 매일 수백만 개의 새로운 이미지 파일을 받습니다. 파일 크기는 평균 1MB입니다. 파일은 1GB 단위로 분석됩니다. 애플리케이션이 배치를 분석할 때 애플리케이션은 이미지를 함께 압축합니다. 그런 다음 애플리케이션은 장기 저장을 위해 이미지를 온프레미스 NFS 서버에 단일 파일로 보관합니다.

회사는 온프레미스에 Microsoft Hyper-V 환경을 보유하고 있으며 사용 가능한 컴퓨팅 용량을 보유하고 있습니다. 회사는 스토리지 용량이 없어 AWS에 이미지를 보관하려고 합니다. 회사는 요청 후 1주일 이내에 보관된 데이터를

검색할 수 있는 능력이 필요합니다.

이 회사는 온프레미스 데이터 센터와 AWS 간에 10Gbps AWS Direct Connect 연결을 보유하고 있습니다. 회사는 대역폭 제한을 설정하고 업무 시간 외에 보관된 이미지가 AWS에 복사되도록 예약해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** 새로운 GPU 기반 Amazon EC2 인스턴스에 AWS DataSync 에이전트를 배포합니다. NFS 온프레미스 서버에서 Amazon S3 Glacier Instant Retrieval로 파일 배치를 복사하도록 DataSync 에이전트를 구성합니다. 복사가 성공한 후 온프레미스 스토리지에서 데이터를 삭제합니다.
> **B.** AWS DataSync 에이전트를 온프레미스에 Hyper-V VM으로 배포합니다. NFS 온프레미스 서버에서 Amazon S3 Glacier Deep Archive로 파일 배치를 복사하도록 DataSync 에이전트를 구성합니다. 복사가 성공한 후 온프레미스 스토리지에서 데이터를 삭제합니다.
> **C.** 새로운 범용 Amazon EC2 인스턴스에 AWS DataSync 에이전트를 배포합니다. NFS 온프레미스 서버에서 Amazon S3 Standard로 파일 배치를 복사하도록 DataSync 에이전트를 구성합니다. 복사가 성공한 후 온프레미스 스토리지에서 데이터를 삭제합니다. 1일 후에 객체를 S3 Standard에서 S3 Glacier Deep Archive로 전환하는 S3 수명 주기 규칙을 생성합니다.
> **D.** Hyper-V 환경의 온프레미스에 AWS Storage Gateway 테이프 게이트웨이를 배포합니다. 테이프 게이트웨이를 AWS에 연결합니다. 자동 테이프 생성을 사용합니다. Amazon S3 Glacier Deep Archive 풀을 지정합니다. 이미지 배치가 복사된 후 테이프를 꺼냅니다.
>
> 해설
> 정답: B
> Hyper-V 환경에 AWS DataSync를 배포하고 S3 Glacier Deep Archive를 더 비용 효율적으로 사용
> A(x): 이미지 복사와 압축에는 GPU의 처리 능력이 필요하지 않다.
> C(x): Hyper-V환경이 있는데 새로운 범용 EC2를 사용하는 것은 비용 비효율
> D(x): DataSync를 사용하는 것이 테이프보다는 일주일 내에 검색할 수 있어야 한다는 비즈니스 요구에 조금 더 적합하고 비용 효율적.

◆ | **Q#0458.** | **Ref#0458.**
회사에서는 사용자 기반 라이선스 스키마로 전환하기 위한 전략의 일환으로 애플리케이션의 핵심성과지표(KPI)를 기록하려고 합니다. 이 애플리케이션은 웹 기반 UI를 갖춘 다중 계층 애플리케이션입니다. 회사는 CloudWatch 에이전트를 사용하여 모든 로그 파일을 Amazon CloudWatch에 저장합니다. 애플리케이션에 대한 모든 로그인은 로그 파일에 저장됩니다.

새로운 라이센스 스키마의 일부로 회사는 각 클라이언트의 일일, 주간, 월간 고유 사용자 수를 파악해야 합니다.

애플리케이션을 최소한으로 변경하면서 이 정보를 제공하는 솔루션은 무엇입니까?

> **A.** 성공한 각 로그인을 지표로 저장하는 Amazon CloudWatch Logs 지표 필터를 구성합니다. 사용자 이름과 클라이언트 이름을 메트릭에 대한 차원으로 구성합니다.
> **B.** 로그인이 성공할 때마다 AWS SDK에 대한 호출을 생성하여 CloudWatch에서 사용자 이름과 클라이언트 이름 차원을 기록하는 사용자 지정 지표를 증가시키도록 애플리케이션 로직을 변경합니다.
> **C.** 로그에서 성공적인 로그인 지표를 추출하도록 CloudWatch 에이전트를 구성합니다. 또한 성공적인 로그인 지표를 지표의 차원으로 사용자 이름과 클라이언트 이름을 사용하는 사용자 지정 지표로 저장하도록 CloudWatch 에이전트를 구성합니다.
> **D.** 애플리케이션 로그의 Amazon CloudWatch Logs 스트림을 사용하도록 AWS Lambda 함수를 구성합니다. 또한 사용자 이름과 클라이언트 이름을 지표의 차원으로 사용하는 CloudWatch에서 사용자 지정 지표를 증가시키도록 Lambda 함수를 구성합니다.
>
> 해설
> 정답: A
> CloudWatch Logs 메트릭 필터를 사용하면 애플리케이션 코드를 변경할 필요 없이 로그 데이터를

분석하고 메트릭으로 변환할 수 있음.
B(x), D(x): 어플리케이션 로직을 변경하는 것과 lambda 함수를 구성하는 행위는 필터링 조건을 구현하는 것보다는 변경 소요가 많음
C(x): 이미 모든 로그 파일을 저장하도록 CloudWatch Agent를 구성하였는데, 추가적인 CloudWatch Agent를 구성하는 것도 소스 변경 소요가 있어 비효율적
CloudWatch Log Filtering

◆ | **Q#0459.** | **Ref#0459.**
한 회사는 GitHub Actions를 사용하여 AWS의 리소스에 액세스하는 CI/CD 파이프라인을 실행하고 있습니다. 회사에는 AWS에 인증하기 위해 파이프라인의 비밀 키를 사용하는 IAM 사용자가 있습니다. 정책이 연결된 기존 IAM 역할은 리소스 배포에 필요한 권한을 부여합니다.

회사의 보안 팀은 파이프라인이 더 이상 수명이 긴 비밀 키를 사용할 수 없다는 새로운 요구 사항을 구현합니다. 솔루션 설계자는 비밀 키를 단기 솔루션으로 교체해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Identity and Access Management(IAM)에서 IAM SAML 2.0 자격 증명 공급자(IdP)를 생성합니다. sts:AssumeRole API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 기존 IAM 정책을 새 IAM 역할에 연결합니다. 파이프라인에 SAML 인증을 사용하도록 GitHub를 업데이트하세요.
B. AWS Identity and Access Management(IAM)에서 IAM OpenID Connect(OIDC) 자격 증명 공급자(IdP)를 생성합니다. GitHub OIDC IdP에서 sts:AssumeRoleWithWebIdentity API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 파이프라인에 대한 역할을 맡도록 GitHub를 업데이트하세요.
C. Amazon Cognito 자격 증명 풀을 생성합니다. GitHub를 사용하도록 인증 공급자를 구성합니다. GitHub 인증 공급자의 sts:AssumeRoleWithWebIdentity API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. Cognito를 인증 공급자로 사용하도록 파이프라인을 구성합니다.
D. AWS 사설 인증 기관에 대한 트러스트 앵커를 생성합니다. AWS IAM Roles Anywhere에 사용할 클라이언트 인증서를 생성합니다. sts:AssumeRole API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 기존 IAM 정책을 새 IAM 역할에 연결합니다. 자격 증명 도우미 도구를 사용하고 클라이언트 인증서 공개 키를 참조하여 새 IAM 역할을 맡도록 파이프라인을 구성합니다.

해설
정답: B
OIDC를 사용하여 GitHub Actions와의 통합을 통해 GitHub에서 AWS로의 안전한 단기 인증을 제공 가능
A(x), D(x): sts:AssumeRole API 호출은 AWS 내에서 역할 위임할 때 사용. 외부와의 통합에는 AssumeRoleWithWebIdentity API 호출이 적합.
GitHub을 통해 인증된 사용자가 IAM 역할을 가정하도록 설정해야 함.
A(x): GitHub은 SAML 프로토콜을 지원하지 않음.
C(x): Cognito를 사용하는 것은 가능하지만, OIDC IdP를 사용하는 것이 더 직접적이고 간단함.

◆ | **Q#0460.** | **Ref#0460.**
한 회사는 기계 학습 훈련 알고리즘에 대한 훈련 문서를 얻기 위해 대상 URL 목록에서 웹 크롤링 프로세스를 실행하고 있습니다. Amazon EC2 t2.micro 인스턴스 집합은 Amazon Simple Queue Service(Amazon SQS) 대기열에서 대상 URL을 가져옵니다. 그런 다음 인스턴스는 크롤링 알고리즘의 결과를 Amazon Elastic File System(Amazon EFS) 볼륨에 .csv 파일로 기록합니다. EFS 볼륨은 플릿의 모든 인스턴스에 탑재됩니다.

별도의 시스템이 드물게 SQS 대기열에 URL을 추가합니다. 인스턴스는 10초 이내에 각 URL을 크롤링합니다.

지표는 SQS 대기열에 URL이 없을 때 일부 인스턴스가 유휴 상태임을 나타냅니다. 솔루션 설계자는 비용을 최적화하기 위해 아키텍처를 재설계해야 합니다.

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

> **A.** 웹 크롤링 프로세스에는 t2.micro 인스턴스 대신 m5.8xlarge 인스턴스를 사용하십시오. 플릿의 인스턴스 수를 50% 줄입니다.
> **B.** 웹 크롤링 프로세스를 AWS Lambda 함수로 변환합니다. SQS 대기열에서 URL을 가져오도록 Lambda 함수를 구성합니다.
> **C.** 결과를 Amazon Neptune에 저장하도록 웹 크롤링 프로세스를 수정합니다.
> **D.** Amazon Aurora Serverless MySQL 인스턴스에 결과를 저장하도록 웹 크롤링 프로세스를 수정합니다.
> **E.** 결과를 Amazon S3에 저장하도록 웹 크롤링 프로세스를 수정합니다.
>
> 해설
> 정답: BE
> EC2 대신 Lambda를 사용하고 비용 효율적인 S3에 저장.
> A(x), C(x): m5.8xlarge와 Amazon Neptune은 고가의 솔루션.
> D(x): SQS대기열에 드물게 URL이 추가되므로, Aurora Serverless는 실행되는 시간에 따라 과금되므로, 드물게 발생할 때 역시 활성화 상태이므로 과금됨.
> Amazon Neptune은 그래프 데이터베이스 서비스

461 (최정현) 1회차 完

◆ | **Q#0461.** | **Ref#0461.**
회사는 웹사이트를 온프레미스 데이터 센터에서 AWS로 마이그레이션해야 합니다. 이 웹 사이트는 로드 밸런서, Linux 운영 체제에서 실행되는 콘텐츠 관리 시스템(CMS) 및 MySQL 데이터베이스로 구성됩니다.

CMS에는 파일 시스템용 영구 NFS 호환 스토리지가 필요합니다. AWS의 새로운 솔루션은 예측할 수 없는 트래픽 증가에 대응하여 Amazon EC2 인스턴스 2개에서 EC2 인스턴스 30개로 확장할 수 있어야 합니다. 또한 새로운 솔루션은 웹사이트를 변경할 필요가 없어야 하며 데이터 손실을 방지해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. Application Load Balancer 및 Auto Scaling 그룹을 사용하여 CMS를 AWS Elastic Beanstalk에 배포합니다. .ebextensions를 사용하여 EFS 파일 시스템을 EC2 인스턴스에 탑재합니다. Elastic Beanstalk 환경과 별도로 Amazon Aurora MySQL 데이터베이스를 생성합니다.
> **B.** Amazon Elastic Block Store(Amazon EBS) 다중 연결 볼륨을 생성합니다. Network Load Balancer 및 Auto Scaling 그룹을 사용하여 CMS를 AWS Elastic Beanstalk에 배포합니다. .ebextensions를 사용하여 EBS 볼륨을 EC2 인스턴스에 탑재합니다. Elastic Beanstalk 환경에서 MySQL용 Amazon RDS 데이터베이스를 생성합니다.
> **C.** Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. CMS를 지원하기 위해 EC2 인스턴스를 시작하기 위한 시작 템플릿과 Auto Scaling 그룹을 생성합니다. 트래픽을 분산하기 위해 Network Load Balancer를 생성합니다. Amazon Aurora MySQL 데이터베이스를 생성합니다. EC2 Auto Scaling 축소 수명 주기 후크를 사용하여 EFS 파일 시스템을 EC2 인스턴스에 탑재합니다.
> **D.** Amazon Elastic Block Store(Amazon EBS) 다중 연결 볼륨을 생성합니다. CMS를 지원하기 위해 EC2 인스턴스를 시작하기 위한 시작 템플릿과 Auto Scaling 그룹을 생성합니다. 트래픽을 분산시키기 위해 Application Load Balancer를 생성합니다. MySQL 데이터베이스를 지원하기 위해 Redis용 Amazon ElastiCache 클러스터를 생성합니다. EC2 사용자 데이터를 사용하여 EBS 볼륨을 EC2 인스턴스에 연결합니다.

해설
정답: A
B(x),D(x): EBS는 NFS와 호환 불가
C(x): 축소 수명 주기(scale-in lifecycle)시에는 EFS Mount 불가, 확장 수명 주기(scale-out)시에 Mount 가능

◆ | **Q#0462.** | **Ref#0462.**
회사는 단일 AWS 리전에서 실행되는 중요한 애플리케이션에 대한 재해 복구를 구현해야 합니다. 애플리케이션 사용자는 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스에서 호스팅되는 웹 프런트엔드와 상호 작용합니다. 애플리케이션은 MySQL DB 인스턴스용 Amazon RDS에 씁니다. 또한 애플리케이션은 Amazon S3 버킷에 저장된 처리된 문서를 출력합니다.

회사의 재무팀은 보고서를 실행하기 위해 데이터베이스를 직접 쿼리합니다. 바쁜 기간 동안 이러한 쿼리는 리소스를 소비하고 애플리케이션 성능에 부정적인 영향을 미칩니다.

솔루션 설계자는 재해 발생 시 복원력을 제공할 솔루션을 설계해야 합니다. 솔루션은 데이터 손실을 최소화하고 재무팀의 쿼리로 인해 발생하는 성능 문제를 해결해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 데이터베이스를 Amazon DynamoDB로 마이그레이션하고 DynamoDB 글로벌 테이블을 사용하십시오. 별도의 리전에서 글로벌 테이블을 쿼리하도록 재무팀에 지시합니다. 원래 S3 버킷의 콘텐츠를 별도 리전의 새 S3 버킷에 주기적으로 동기화하는 AWS Lambda 함수를 생성합니다. EC2 인스턴스를 시작하고 별도의 리전에 ALB를 생성합니다. 새 S3 버킷을 가리키도록 애플리케이션을 구성합니다.
B. 별도의 지역에서 애플리케이션을 호스팅하는 추가 EC2 인스턴스를 시작합니다. 기존 AL에 추가 인스턴스를 추가합니다. 별도의 리전에서 RDS DB 인스턴스의 읽기 전용 복제본을 생성합니다. 읽기 전용 복제본에 대해 쿼리를 실행하도록 재무팀에 지시합니다. 원래 S3 버킷에서 별도 리전의 새 S3 버킷으로 S3 교차 리전 복제(CRR)를 사용합니다. 재해 발생 시 읽기 전용 복제본을 독립형 DB 인스턴스로 승격합니다. 새 S3 버킷과 새로 승격된 읽기 전용 복제본을 가리키도록 애플리케이션을 구성합니다.
C. 별도의 리전에 RDS DB 인스턴스의 읽기 전용 복제본을 생성합니다. 읽기 전용 복제본에 대해 쿼리를 실행하도록 재무팀에 지시합니다. 애플리케이션 프런트엔드를 호스팅하는 EC2 인스턴스의 AMI를 생성합니다. AMI를 별도의 리전에 복사합니다. 원래 S3 버킷에서 별도 리전의 새 S3 버킷으로 S3 교차 리전 복제(CRR)를 사용합니다. 재해 발생 시 읽기 전용 복제본을 독립형 DB 인스턴스로 승격합니다. AMI에서 EC2 인스턴스를 시작하고 ALB를 생성하여 최종 사용자에게 애플리케이션을 제공합니다. 새 S3 버킷을 가리키도록 애플리케이션을 구성합니다.
D. RDS DB 인스턴스의 시간별 스냅샷을 생성합니다. 스냅샷을 별도의 리전에 복사합니다. 기존 RDS 데이터베이스 앞에 Amazon ElastiCache 클러스터를 추가합니다. 애플리케이션 프런트엔드를 호스팅하는 EC2 인스턴스의 AMI를 생성합니다. AMI를 별도의 리전에 복사합니다. 원래 S3 버킷에서 별도 리전의 새 S3 버킷으로 S3 교차 리전 복제(CRR)를 사용합니다. 재해 발생 시 최신 RDS 스냅샷에서 데이터베이스를 복원하세요. AMI에서 EC2 인스턴스를 시작하고 ALB를 생성하여 최종 사용자에게 애플리케이션을 제공합니다. 새 S3 버킷을 가리키도록 애플리케이션을 구성합니다.

해설
정답: C
재무팀의 보고서용 쿼리 부하 분산과 재해 대비를 위해서는 RDS 읽기 전용 복제본을 생성하여 제공하고, 재해 발생시 읽기 전용 인스턴스를 standalone DB(Read/Write)로 전환한다.

A(x): DynamoDB는 Nosql DB로 불가
B(x): EC2 DR 요구 사항이 없음

D(x): Snapshot 사용은 데이터 손실 가능

◆ | **Q#0463.** | **Ref#0463.**
회사에는 온프레미스 데이터 센터에서 실행되는 많은 서비스가 있습니다. 데이터 센터는 AWS Direct Connect(DX) 및 IPSec VPN을 사용하여 AWS에 연결됩니다. 서비스 데이터는 중요하므로 연결이 인터넷을 통과할 수 없습니다. 회사는 새로운 시장 부문으로 확장하고 AWS를 사용하는 다른 회사에 서비스를 제공하기를 원합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. TCP 트래픽을 허용하는 VPC Endpoint 서비스를 생성하고 이를 Network Load Balancer 뒤에서 호스팅하고 DX를 통해 서비스를 사용할 수 있도록 합니다.
B. HTTP 또는 HTTPS 트래픽을 허용하는 VPC 엔드포인트 서비스를 생성하고, 이를 Application Load Balancer 뒤에서 호스팅하고, DX를 통해 서비스를 사용할 수 있도록 합니다.
C. 인터넷 게이트웨이를 VPC에 연결하고 네트워크 액세스 제어 및 보안 그룹 규칙이 관련 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다.
D. NAT 게이트웨이를 VPC에 연결하고 네트워크 액세스 제어 및 보안 그룹 규칙이 관련 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다.

해설
정답: A

A: VPC 엔드포인트 + NLB = PrivateLink
B(x): 많은 서비스를 이용하기에 HTTP/HTTPS로 한정은 불가
C(x),D(x): 인터넷 연결이 안 되어야 하기에 불가

◆ | **Q#0464.** | **Ref#0464.**
회사는 AWS Organizations를 사용하여 AWS 계정을 관리합니다. 솔루션 설계자는 관리자 역할만 IAM 작업을 사용할 수 있도록 허용되는 솔루션을 설계해야 합니다. 그러나 솔루션 아키텍트는 회사 전체의 모든 AWS 계정에 액세스할 수 없습니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 관리자 역할에 대해서만 IAM 작업을 허용하려면 모든 AWS 계정에 적용되는 SCP를 생성하십시오. 루트 OU에 SCP를 적용합니다.
B. IAM 작업과 관련된 각 이벤트에 대해 AWS Lambda 함수를 호출하도록 AWS CloudTrail을 구성합니다. 작업을 호출한 사용자가 관리자가 아닌 경우 작업을 거부하도록 기능을 구성합니다.
C. 모든 AWS 계정에 적용되는 SCP를 생성하여 관리자 역할이 있는 사용자를 제외한 모든 사용자에 대한 IAM 작업을 거부합니다. 루트 OU에 SCP를 적용합니다.
D. IAM 작업을 허용하는 IAM 권한 경계를 설정합니다. 모든 AWS 계정의 모든 관리자 역할에 권한 경계를 연결합니다.

해설
정답: C
지정된 거부 규칙을 사용하여 root OU에 SCP 적용

A(x): SCP를 사용하여 관리자외 다른 사람은 거부를 해야 하나 그러지 못함.
B(x): CloudTrail과 Lambda를 사용하는 것은 실시간으로 작업을 모니터링하고 차단해야 하므로 복잡도가 증가
D(x): 모든 관리자 역할에 권한 경계를 개별적으로 설정해야 하므로 운영 오버헤드가 크다.

SCP (Serive Control Policy)
-SCP는 OU 또는 AWS account 를 대상으로 적용이 가능하다.

-SCP는 하위 OU에 상속이 된다.
-SCP는 OU들에 다르게 적용 가능하다.

OU (Organization Unit)
-OU는 AWS Account 들의 그룹 단위이다.
-OU는 하위 OU를 가질 수 있다. 회사 구조를 반영할 수 있다.
-하나의 AWS 계정은 오직 하나의 OU에 속할 수 있다. 다른 OU에는 속할 수 없다.
-OU는 5단계 계층적 구조를 가질 수 있다.

◆ | **Q#0465.** | **Ref#0465.**
회사는 AWS Organizations의 조직을 사용하여 여러 AWS 계정을 관리합니다. 회사는 회사 공유 서비스 계정의 VPC에서 일부 애플리케이션을 호스팅합니다.

회사는 공유 서비스 계정의 VPC에 전송 게이트웨이를 연결했습니다.

회사는 새로운 기능을 개발 중이며 공유 서비스 계정에 있는 애플리케이션에 액세스해야 하는 개발 환경을 만들었습니다. 회사에서는 개발 계정의 리소스를 자주 삭제하고 다시 생성할 예정입니다. 또한 회사에서는 필요에 따라 공유 서비스 계정에 대한 팀 연결을 다시 생성할 수 있는 기능을 개발 팀에 제공하려고 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 개발 계정에 전송 게이트웨이를 생성하십시오. 공유 서비스 계정에 대한 전송 게이트웨이 피어링 요청을 생성합니다. 피어링 연결을 자동으로 수락하도록 공유 서비스 전송 게이트웨이를 구성합니다.
B. 공유 서비스 계정에서 전송 게이트웨이에 대한 자동 수락을 활성화합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 공유 서비스 계정의 전송 게이트웨이 리소스를 개발 계정과 공유합니다. 개발 계정에서 리소스를 수락합니다. 개발 계정에 전송 게이트웨이 연결을 생성합니다.
C. 공유 서비스 계정에서 전송 게이트웨이에 대한 자동 수락을 켭니다. VPC 엔드포인트를 생성합니다. 엔드포인트 정책을 사용하여 개발 계정에 대한 VPC 엔드포인트에 대한 권한을 부여합니다. 연결 요청을 자동으로 수락하도록 엔드포인트 서비스를 구성합니다. 개발팀에 엔드포인트 세부정보를 제공하세요.
D. 개발 계정이 연결 요청을 할 때 전송 게이트웨이 연결을 수락하는 AWS Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. AWS Network Manager를 사용하여 공유 서비스 계정의 전송 게이트웨이를 개발 계정과 공유합니다. 개발 계정에서 전송 게이트웨이를 수락합니다.

해설
정답: B
개발팀이 공유 서비스 계정에 대한 연결을 다시 만드는 데 필요한 유연성을 제공
개발 계정은 연결이 생성될 때마다 수동 개입 없이 전송 게이트웨이 연결을 생성할 수 있습니다.

A(x): Transit Gateway는 계정이 아닌 지역간에 이루어지기 때문에 오답
C(x): VPC 엔드포인트의 사용 사례가 아님. VPC 엔드포인트는 일반적으로 공용 인터넷을 통과하지 않고 AWS 서비스에 비공개로 연결하는 데 사용
D(x): 과도한 구성

Transit Gateway(TGW)란?
-VPC 와 VPC, VPC와 온프레미스간에 네트워크를 상호 연결 할 수 있도록 만들어주는 네트워크 전송 허브
-TGW에 여러 네트워크들을 연결하여 각 네트워크간 통신을 시켜주는 일종의 라우터

AWS Resource Access Manager(RAM) 이란?
-리소스 유형에 대해 AWS 계정 간, 조직 또는 조직 단위(OU) 내에서, 그리고 AWS Identity and

Access Management(IAM) 역할 및 사용자와 리소스를 안전하게 공유할 수 있다.
-AWS 계정이 여러 개 있는 경우 리소스를 한 번 생성한 후 AWS RAM을 사용하여 다른 계정에서 해당 리소스를 사용할 수 있도록 설정할 수 있다.

Network Manager 란?
Network Manager를 사용하면 전체 AWS 계정, 리전 및 온프레미스 위치에서 AWS Cloud WAN 코어 네트워크와 AWS Transit Gateway 네트워크를 중앙에서 관리할 수 있습니다.
다중 계정 지원을 통해 모든 AWS 계정의 단일 글로벌 네트워크를 생성하고, Network Manager 콘솔을 사용하여 여러 계정의 Transit Gateway를 글로벌 네트워크에 등록할 수 있습니다.

◆ | **Q#0466.** | **Ref#0466.**
회사는 온프레미스 데이터 센터에서 AWS로 가상 Microsoft 워크로드를 마이그레이션하려고 합니다. 이 회사는 AWS에서 몇 가지 샘플 워크로드를 성공적으로 테스트했습니다. 또한 회사는 VPC에 대한 AWS Site-to-Site VPN 연결을 생성했습니다. 솔루션 설계자는 데이터 센터의 모든 워크로드 마이그레이션에 대한 총 소유 비용(TCO) 보고서를 생성해야 합니다.

데이터 센터의 각 VM에서 SNMP(Simple Network Management Protocol)가 활성화되었습니다. 회사는 데이터 센터에 VM을 더 추가할 수 없으며 VM에 추가 소프트웨어를 설치할 수도 없습니다. 검색 데이터는 자동으로 AWS Migration Hub로 가져와야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Application Migration Service 에이전트 없는 서비스와 AWS Migration Hub 전략 권장 사항을 사용하여 TCO 보고서를 생성하십시오.
B. Windows Amazon EC2 인스턴스를 시작합니다. EC2 인스턴스에 Migration Evaluator 에이전트 없는 수집기를 설치합니다. TCO 보고서를 생성하도록 Migration Evaluator를 구성합니다.
C. Windows Amazon EC2 인스턴스를 시작합니다. EC2 인스턴스에 Migration Evaluator 에이전트 없는 수집기를 설치합니다. TCO 보고서를 생성하도록 Migration Hub를 구성합니다.
D. VPC 내부에서 AWS 마이그레이션 준비 평가 도구를 사용하십시오. TCO 보고서를 생성하도록 마이그레이션 평가기를 구성합니다.

해설
정답: B
Migration Evaluator를 통해 TCO 보고서를 생성할수 있다.

A,C: Migration Hub로는 TCO 보고서를 생성할 수 없다. TCO 이해를 할수 있게 도움만
(AWS Migration Hub는 검색, 평가, 계획 및 실행을 통한 전체 마이그레이션 및 현대화 여정을 안내)
D: Migration Readiness Assessment는 Migration 준비 상태를 Business/Technical 관점에서의 진단이지 TCO 보고서를 생성하지 않음

◆ | **Q#0467.** | **Ref#0467.**
모바일 게임을 개발하는 회사는 두 개의 AWS 리전에서 게임 자산을 사용할 수 있도록 만들고 있습니다. 게임 자산은 각 지역의 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스 세트에서 제공됩니다. 회사에서는 가장 가까운 지역에서 게임 자산을 가져와야 합니다. 가장 가까운 지역에서 게임 자산을 사용할 수 없게 되면 다른 지역에서 가져와야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. Amazon CloudFront 배포판을 생성합니다. 각 ALB에 대해 하나의 원본이 있는 원본 그룹을 만듭니다. 원본 중 하나를 기본으로 설정합니다.
B. 각 ALB에 대한 Amazon Route 53 상태 확인을 생성합니다. 두 개의 ALB를 가리키는 Route 53 장애 조치 라우팅 레코드를 생성합니다. 대상 상태 평가 값을 예로 설정합니다.

C. 각각 하나의 ALB를 오리진으로 사용하는 두 개의 Amazon CloudFront 배포판을 생성합니다. 두 CloudFront 배포를 가리키는 Amazon Route 53 장애 조치 라우팅 레코드를 생성합니다. 대상 상태 평가 값을 예로 설정합니다.
D. 각 ALB에 대해 Amazon Route 53 상태 확인을 생성합니다. 두 개의 ALB를 가리키는 Route 53 지연 별칭 레코드를 생성합니다. 대상 상태 평가 값을 예로 설정합니다.

해설
정답: D

A: 다른 원본에 대한 캐시 동작을 설정해야 함
B: 장애 조치 라우팅 레코드가 2개의 ALB를 가리킬 수 없음
C: 작동하지만 요구 사항을 충족하지 않음
D: 지연시간(latency) 기반 라우팅은 가장 가까운 지역이 비정상이 되지 않는 한 가장 가까운 지역으로 트래픽을 보냄

Amazon CloudFront란
-html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹 서비스

ALB(Application Load Balancer)란
-L7단의 로드 밸런서를 지원
-HTTP/HTTPS 프로토콜의 헤더를 보고 적절한 패킷으로 전송
-IP주소 + 포트번호 + 패킷 내용을 보고 스위칭
-IP 주소가 변동되기 때문에 Client에서 Access 할 ELB의 DNS Name을 이용
-L7단을 지원하기 때문에 SSL 적용이 가능

Amazon Route 53 이란?
-도메인 이름 시스템(DNS) 웹 서비스
-사용자 요청을 AWS 또는 온프레미스에서 실행되는 인터넷 애플리케이션에 연결

◆ | **Q#0468.** | **Ref#0468.**
회사는 여러 AWS 계정에 워크로드를 배포합니다. 각 계정에는 중앙 집중식 Amazon S3 버킷에 텍스트 로그 형식으로 게시된 VPC 흐름 로그가 있는 VPC가 있습니다. 각 로그 파일은 gzip 압축으로 압축됩니다. 회사는 로그 파일을 무기한 보관해야 합니다.

보안 엔지니어는 때때로 Amazon Athena를 사용하여 VPC 흐름 로그를 쿼리하여 로그를 분석합니다. 수집된 로그 수가 증가함에 따라 시간이 지남에 따라 쿼리 성능이 저하됩니다. 솔루션 아키텍트는 로그 분석 성능을 향상하고 VPC 흐름 로그가 사용하는 저장 공간을 줄여야 합니다.

가장 큰 성능 개선으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. gzip 파일의 압축을 풀고 bzip2 압축으로 파일을 압축하는 AWS Lambda 함수를 생성합니다. S3 버킷에 대한 s3:ObjectCreated:Put S3 이벤트 알림에 대한 Lambda 함수를 구독합니다.
B. S3 버킷에 대해 S3 Transfer Acceleration을 활성화합니다. 파일이 업로드되는 즉시 S3 Intelligent-Tiering 스토리지 클래스로 파일을 이동하도록 S3 수명 주기 구성을 생성합니다.
C. 파일을 Apache Parquet 형식으로 저장하도록 VPC 흐름 로그 구성을 업데이트합니다. 로그 파일의 시간별 파티션을 지정합니다.
D. 데이터 사용량 제어 제한 없이 새로운 Athena 작업 그룹을 생성합니다. Athena 엔진 버전 2를 사용하세요.

해설

정답: C
Apache Parquet 형식을 사용하여 고도로 최적화된 컬럼형 스토리지 형식과 시간별 파티셔닝을 통해 Athena 쿼리 성능 향상

◆ | **Q#0469.** | **Ref#0469.**
회사는 온프레미스 인프라와 AWS 간에 전용 연결을 설정하려고 합니다. 회사는 계정 VPC에 대한 1Gbps AWS Direct Connect 연결을 설정하고 있습니다. 아키텍처에는 여러 VPC와 온프레미스 인프라를 연결하기 위한 전송 게이트웨이와 Direct Connect 게이트웨이가 포함되어 있습니다.

회사는 Direct Connect 연결을 사용하여 전송 VIF를 통해 VPC 리소스에 연결해야 합니다.

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

A. 1Gbps Direct Connect 연결을 10Gbps로 업데이트합니다.
B. 전송 VIF를 통해 온프레미스 네트워크 접두사를 알립니다(Advertise).
C. 전송 VIF를 통해 Direct Connect 게이트웨이의 VPC 접두사를 온프레미스 네트워크에 알립니다.
D. Direct Connect 연결의 MACsec 암호화 모드 속성을 must_encrypt로 업데이트합니다.
E. MACsec 연결 키 이름/연결 연관 키(CKN/CAK) 쌍을 Direct Connect 연결과 연결합니다.

해설
정답: BC

On-premises와 VPC가 연결될 수 있도록 VPC Prefix와 On-premises Prefix를 알려야(Advertise) 함
D(x),E(x): MACsec은 10Gbps가 필요하므로 제외
Transit Gateway 연결
Prefix 목록 참조

가상 인터페이스(VIF)란?
-AWS 서비스에 액세스하는 데 필요하며 퍼블릭 또는 프라이빗입니다. 퍼블릭 가상 인터페이스를 사용하면 Amazon S3와 같은 퍼블릭 서비스에 액세스할 수 있고, 프라이빗 가상 인터페이스를 통해 VPC에 액세스할 수 있습니다.

◆ | **Q#0470.** | **Ref#0470.**
한 회사에서 Amazon WorkSpaces를 씬 클라이언트 디바이스와 함께 사용하여 노후된 데스크톱을 교체하려고 합니다. 직원들은 데스크톱을 사용하여 임상 시험 데이터를 다루는 애플리케이션에 액세스합니다. 기업 보안 정책에 따르면 애플리케이션에 대한 액세스는 회사 지점으로만 제한되어야 합니다. 회사는 향후 6개월 내에 지점을 추가로 추가하는 것을 고려하고 있습니다.

가장 효율적인 운영 효율성으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 지점의 공용 주소 목록을 사용하여 IP 액세스 제어 그룹 규칙을 만듭니다. IP 액세스 제어 그룹을 WorkSpaces 디렉터리와 연결합니다.
B. AWS Firewall Manager를 사용하여 지점 위치의 공용 주소 목록이 포함된 IPSet가 포함된 웹 ACL 규칙을 생성합니다. 웹 ACL을 WorkSpaces 디렉터리와 연결합니다.
C. ACM(AWS Certificate Manager)을 사용하여 지사 위치에 배포된 시스템에 신뢰할 수 있는 장치 인증서를 발급합니다. WorkSpaces 디렉터리에 대해 제한된 액세스를 활성화합니다.
D. 지점의 공용 주소에 대한 액세스를 제한하도록 구성된 Windows 방화벽을 사용하여 사용자 지정 WorkSpace 이미지를 생성합니다. 이미지를 사용하여 WorkSpaces를 배포합니다.

해설
정답: A

지점에서만 접속을 제한하려면 지점에 공용 IP를 추가해야 함.
IP 접근 제어 그룹을 사용하므로 운영상 가장 효율적
WorkSpaces의 IP 액세스 제어 그룹
IP 액세스 제어 그룹은 사용자가 WorkSpaces에 액세스할 수 있는 IP 주소를 제어하는 가상 방화벽의 역할을 합니다.

471 (정창화) 4회차 完

◆ | **Q#0471.** | **Ref#0471.**
회사는 AWS Organizations를 사용합니다. 회사는 중앙 네트워킹 계정에서 두 개의 방화벽 어플라이언스를 실행합니다. 각 방화벽 어플라이언스는 수동으로 구성된 고가용성 Amazon EC2 인스턴스에서 실행됩니다. 전송 게이트웨이는 중앙 집중식 네트워킹 계정의 VPC를 회원 계정의 VPC에 연결합니다. 각 방화벽 어플라이언스는 회원 계정에서 인터넷으로 트래픽을 라우팅하는 데 사용되는 고정 사설 IP 주소를 사용합니다.

최근 사건 중에 잘못 구성된 스크립트로 인해 두 방화벽 장비가 모두 종료되었습니다. 방화벽 장비를 재구축하는 동안 회사는 시작 시 방화벽 장비를 구성하기 위한 새로운 스크립트를 작성했습니다.

회사는 방화벽 어플라이언스 배포를 현대화하려고 합니다. 방화벽 어플라이언스는 네트워크 확장 시 증가된 트래픽을 처리하기 위해 수평으로 확장할 수 있는 기능이 필요합니다. 회사는 회사 정책을 준수하기 위해 방화벽 장비를 계속 사용해야 합니다. 방화벽 어플라이언스 공급자는 최신 버전의 방화벽 코드가 모든 AWS 서비스에서 작동함을 확인했습니다.

솔루션 설계자는 이러한 요구 사항을 가장 비용 효율적으로 충족하기 위해 어떤 단계 조합을 권장해야 합니까? (3개를 선택하세요.)

A. 중앙 네트워킹 계정에 게이트웨이 Load Balancer를 배포합니다. AWS PrivateLink를 사용하는 엔드포인트 서비스를 설정합니다.
B. 중앙 네트워킹 계정에 Network Load Balancer를 배포합니다. AWS PrivateLink를 사용하는 엔드포인트 서비스를 설정합니다.
C. 방화벽 어플라이언스를 구성하기 위해 새 스크립트를 사용자 데이터로 사용하는 Auto Scaling 그룹과 시작 템플릿을 생성합니다. 인스턴스 대상 유형을 사용하는 대상 그룹을 생성합니다.
D. Auto Scaling 그룹을 생성합니다. 새 스크립트를 사용자 데이터로 사용하여 방화벽 어플라이언스를 구성하는 AWS Launch Wizard 배포를 구성합니다. IP 대상 유형을 사용하는 대상 그룹을 생성합니다.
E. 각 회원 계정에 VPC 엔드포인트를 생성합니다. VPC 엔드포인트를 가리키도록 라우팅 테이블을 업데이트합니다.
F. 중앙 네트워킹 계정에 VPC 엔드포인트를 생성합니다. VPC 엔드포인트를 가리키도록 각 멤버 계정의 라우팅 테이블을 업데이트합니다.

해설
정답: A, C, F
A. Gateway Load Balancer 배포: Gateway Load Balancer는 방화벽 어플라이언스를 포함한 네트워크 어플라이언스를 확장하고 관리하는 데 유용함. 이 설정을 통해 트래픽을 방화벽 인스턴스로 효과적으로 분산.
C. Auto Scaling 그룹 및 시작 템플릿 생성: Auto Scaling 그룹과 시작 템플릿을 사용하여 방화벽 어플라이언스를 자동으로 배포하고 확장할 수 있음. 시작 템플릿에 새 스크립트를 사용자 데이터로 포함시켜 인스턴스 시작 시 자동으로 구성되도록 함.
F. 중앙 네트워킹 계정에 VPC 엔드포인트 생성: 중앙 네트워킹 계정에 VPC 엔드포인트를 생성하고, 회원 계정의 라우팅 테이블을 업데이트하여 트래픽이 VPC 엔드포인트로 라우팅되도록 함. 이를 통해 중앙에서 네트워크 트래픽을 관리하고 방화벽 어플라이언스로 라우팅할 수 있음.

◆ | **Q#0472.** | **Ref#0472.**
솔루션 아키텍트는 웹 애플리케이션을 지원하는 PostgreSQL용 Amazon RDS 데이터베이스에 대한 다중 리전 아키텍처를 구현해야 합니다. 데이터베이스는 기본 및 보조 리전에 모두 존재하는 AWS 서비스 및 기능을 포함하는 AWS CloudFormation 템플릿에서 시작됩니다.

데이터베이스는 자동 백업을 위해 구성되었으며 RTO는 15분, RPO는 2시간입니다. 웹 애플리케이션은 Amazon Route 53 레코드를 사용하여 트래픽을 데이터베이스로 라우팅하도록 구성됩니다.

모든 요구 사항을 충족하는 고가용성 아키텍처를 구현하려면 어떤 단계를 조합해야 합니까? (2개를 선택하세요.)

> **A.** 보조 리전에 데이터베이스의 리전 간 읽기 전용 복제본을 생성합니다. 장애 조치 이벤트 중에 읽기 전용 복제본을 승격하도록 보조 리전에 AWS Lambda 함수를 구성합니다.
> **B.** 기본 리전에서 오류가 감지되면 AWS Lambda 함수를 호출하는 데이터베이스에 대한 상태 확인을 생성합니다. 보조 리전의 최신 데이터베이스 스냅샷에서 데이터베이스를 다시 생성하고 데이터베이스에 대한 Route 53 호스트 레코드를 업데이트하도록 Lambda 기능을 프로그래밍합니다.
> **C.** 2시간마다 최신 자동 백업을 보조 리전에 복사하는 AWS Lambda 함수를 생성합니다.
> **D.** Route 53에서 데이터베이스 DNS 레코드에 대한 장애 조치 라우팅 정책을 생성합니다. 기본 및 보조 엔드포인트를 각 리전의 엔드포인트로 설정합니다.
> **E.** 보조 지역에 상시 대기 데이터베이스를 생성합니다. 기본 데이터베이스에 오류가 발생할 경우 AWS Lambda 함수를 사용하여 보조 데이터베이스를 최신 RDS 자동 백업으로 복원합니다.
>
> 해설
> 정답: A, D
> A. 크로스 리전 읽기 복제를 사용하면 보조 리전에 데이터베이스의 최신 복제본을 유지할 수 있음. 장애 발생 시 Lambda 함수를 사용해 읽기 복제를 승격하면 빠르게 장애 복구가 가능
> D. Route 53의 장애 조치 라우팅 정책을 사용하면 주요 리전의 데이터베이스가 실패할 경우 트래픽을 자동으로 보조 리전으로 전환할 수 있음. 이는 RTO와 RPO 요구사항을 충족하는 데 매우 유용함.

◆ | **Q#0473.** | **Ref#0473.**
전자상거래 회사가 AWS에서 애플리케이션을 실행하고 있습니다. 애플리케이션에는 AWS Lambda 함수를 호출하는 Amazon API Gateway API가 있습니다. 데이터는 PostgreSQL DB 인스턴스용 Amazon RDS에 저장됩니다.

회사의 가장 최근 플래시 세일 기간 동안 API 호출이 갑자기 증가하여 애플리케이션 성능에 부정적인 영향을 미쳤습니다. 솔루션 설계자는 해당 기간 동안 Amazon CloudWatch 지표를 검토한 결과 Lambda 호출 및 데이터베이스 연결이 크게 증가한 것을 발견했습니다. DB 인스턴스에서도 CPU 사용률이 높았습니다.

솔루션 설계자는 애플리케이션 성능을 최적화하기 위해 무엇을 권장해야 합니까?

> **A.** Lambda 함수의 메모리를 늘리십시오. 데이터가 검색될 때 데이터베이스 연결을 닫도록 Lambda 함수를 수정합니다.
> **B.** Redis용 Amazon ElastiCache 클러스터를 추가하여 RDS 데이터베이스에서 자주 액세스하는 데이터를 저장합니다.
> **C.** Lambda 콘솔을 사용하여 RDS 프록시를 생성합니다. 프록시 엔드포인트를 사용하도록 Lambda 함수를 수정합니다.
> **D.** 함수 핸들러 외부의 데이터베이스에 연결하도록 Lambda 함수를 수정합니다. 새 연결을 만들기 전에 기존 데이터베이스 연결을 확인하세요.
>
> 해설
> 정답: C
> RDS 프록시는 Lambda 함수와 RDS 간의 데이터베이스 연결을 효율적으로 관리하여 데이터베이스 연결 수를 줄이고, Lambda 호출 시 새로운 연결을 만드는 오버헤드를 줄여줌. 이는 높은 동시성 처리에 효과적임.
> A: CPU 및 메모리 사용을 줄일 수 있지만, 데이터베이스 연결 수를 관리하는 문제를 해결하지 못함.
> B: 캐싱을 통해 데이터베이스 부하를 줄일 수 있지만, 이 문제의 주요 원인인 데이터베이스 연결 관

리를 해결하지 못함.
D: Lambda 함수의 실행 중 연결을 재사용하여 연결 오버헤드를 줄일 수 있지만, RDS 프록시만큼 효율적이지는 않음.

◆ | **Q#0474.** | **Ref#0474.**
한 소매 회사에서 애플리케이션 아키텍처를 개선하려고 합니다. 회사의 애플리케이션은 새로운 주문을 등록하고 상품 반품을 처리하며 분석을 제공합니다. 애플리케이션은 MySQL 데이터베이스와 Oracle OLAP 분석 데이터베이스에 소매 데이터를 저장합니다. 모든 애플리케이션과 데이터베이스는 Amazon EC2 인스턴스에서 호스팅됩니다.

각 애플리케이션은 주문 프로세스의 다양한 부분을 처리하는 여러 구성 요소로 구성됩니다. 이러한 구성 요소는 다양한 소스에서 들어오는 데이터를 사용합니다. 별도의 ETL 작업이 매주 실행되어 각 애플리케이션의 데이터를 분석 데이터베이스에 복사합니다.

솔루션 설계자는 서버리스 서비스를 사용하는 이벤트 기반 솔루션으로 아키텍처를 재설계해야 합니다. 솔루션은 거의 실시간으로 업데이트된 분석을 제공해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 개별 애플리케이션을 마이크로서비스로 AWS Fargate를 사용하는 Amazon Elastic Container Service(Amazon ECS) 컨테이너로 마이그레이션합니다. 소매 MySQL 데이터베이스를 Amazon EC2에 보관하세요. 분석 데이터베이스를 Amazon Neptune으로 이동합니다. Amazon Simple Queue Service(Amazon SQS)를 사용하여 수신되는 모든 데이터를 마이크로서비스 및 분석 데이터베이스로 보냅니다.
B. 각 애플리케이션에 대해 Auto Scaling 그룹을 생성합니다. 각 Auto Scaling 그룹에 필요한 EC2 인스턴스 수를 지정합니다. 소매 MySQL 데이터베이스와 분석 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 들어오는 모든 데이터를 올바른 EC2 인스턴스와 분석 데이터베이스로 보냅니다.
C. 개별 애플리케이션을 마이크로서비스로 AWS Fargate를 사용하는 Amazon Elastic Kubernetes Service(Amazon EKS) 컨테이너로 마이그레이션합니다. 소매 MySQL 데이터베이스를 Amazon Aurora Serverless MySQL로 마이그레이션합니다. 분석 데이터베이스를 Amazon Redshift Serverless로 마이그레이션합니다. Amazon EventBridge를 사용하여 수신되는 모든 데이터를 마이크로서비스 및 분석 데이터베이스로 보냅니다.
D. 개별 애플리케이션을 마이크로서비스로 Amazon AppStream 2.0으로 마이그레이션합니다. 소매 MySQL 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다. 분석 데이터베이스를 Amazon Redshift Serverless로 마이그레이션합니다. AWS IoT Core를 사용하여 수신되는 모든 데이터를 마이크로서비스 및 분석 데이터베이스로 보냅니다.

해설
정답: C
애플리케이션을 마이크로서비스로 분할하여 Amazon EKS와 Fargate를 사용하여 관리하며, 데이터베이스를 서버리스 옵션(Aurora Serverless 및 Redshift Serverless)으로 마이그레이션.
EventBridge는 다양한 소스에서 데이터를 수집하고 이를 마이크로서비스 및 분석 데이터베이스로 전송하는 데 적합하며, 거의 실시간으로 데이터를 처리하고 분석할 수 있는 구조를 제공.
A(x): SQS는 거의 실시간이 아님. EC2의 MySQL은 서버리스가 아님.
B(x): 서버리스가 아님.
D(x): AppStream 2.0은 데스크탑 애플리케이션 스트리밍 서비스, IoT Core는 IoT 장치에서 데이터 수집용

◆ | **Q#0475.** | **Ref#0475.**
한 회사가 온프레미스 데이터 센터에서 AWS 클라우드로 마이그레이션을 계획하고 있습니다. 회사는 AWS Organizations의 조직에서 관리되는 여러 AWS 계정을 사용할 계획입니다. 회사는 처음에 소수의 계정을 생성하고 필요에 따라 계정을 추가합니다. 솔루션 아키텍트는 모든 AWS 계정에서 AWS CloudTrail을 활성화하는 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하는 가장 운영 효율적인 솔루션은 무엇입니까?

> **A.** 조직의 모든 AWS 계정에 새로운 CloudTrail 추적을 생성하는 AWS Lambda 함수를 생성하십시오. Amazon EventBridge에서 예약된 작업을 사용하여 매일 Lambda 함수를 호출합니다.
> **B.** 조직의 마스터 계정에 새 CloudTrail 추적을 생성합니다. 조직의 모든 AWS 계정에 대한 모든 이벤트를 기록하도록 추적을 구성합니다.
> **C.** 조직의 모든 AWS 계정에 새로운 CloudTrail 추적을 생성합니다. 새 계정이 생성될 때마다 새 트레일을 생성합니다. 트레일의 삭제 또는 수정을 방지하는 SCP를 정의합니다. 루트 OU에 SCP를 적용합니다.
> **D.** 조직의 모든 AWS 계정에서 CloudTrail 추적을 생성하는 AWS 시스템 관리자 자동화 Runbook을 생성합니다. Systems Manager State Manager를 사용하여 자동화를 호출합니다.
>
> 해설
> 정답: B
> 가장 간단하고 효율적임. 마스터 계정에서 조직 전체의 모든 이벤트를 기록하도록 설정할 수 있어 단일 지점에서 중앙 집중식 로그 관리가 가능.
> 운영 오버헤드가 최소화되며 모든 계정이 자동으로 포함. 가장 운영효율성이 높은 솔루션

◆ | **Q#0476.** | **Ref#0476.**
소프트웨어 개발 회사에는 원격으로 작업하는 여러 엔지니어가 있습니다. 이 회사는 Amazon EC2 인스턴스에서 AD DS(Active Directory Domain Services)를 실행하고 있습니다. 회사의 보안 정책에는 VPC에 배포된 모든 내부 비공개 서비스가 VPN을 통해 액세스할 수 있어야 한다고 명시되어 있습니다. VPN에 액세스하려면 다중 요소 인증(MFA)을 사용해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** AWS Site-to-Site VPN 연결을 생성합니다. VPN과 AD DS 간의 통합을 구성합니다. VPN 연결을 설정하려면 MFA 지원이 활성화된 Amazon WorkSpaces 클라이언트를 사용하십시오.
> **B.** AWS 클라이언트 VPN 엔드포인트를 생성합니다. AD DS와의 통합을 위한 AD Connector 디렉터리를 만듭니다. AD 커넥터에 대해 MFA를 활성화합니다. AWS 클라이언트 VPN을 사용하여 VPN 연결을 설정합니다.
> **C.** AWS VPN CloudHub를 사용하여 여러 AWS Site-to-Site VPN 연결을 생성합니다. AWS VPN CloudHub와 AD DS 간의 통합을 구성합니다. AWS Copilot을 사용하여 VPN 연결을 설정합니다.
> **D.** Amazon WorkLink 엔드포인트를 생성합니다. Amazon WorkLink와 AD DS 간의 통합을 구성합니다. Amazon WorkLink에서 MFA를 활성화합니다. AWS 클라이언트 VPN을 사용하여 VPN 연결을 설정합니다.
>
> 해설
> 정답: B
> AWS Client VPN은 AWS Directory Service와 통합하여 Active Directory 지원을 제공하며, AWS Managed Microsoft AD 또는 AD Connector에 대해 활성화된 경우 멀티 팩터 인증(MFA)을 지원합니다.이 방식은 원격 근무 엔지니어가 Client VPN을 통해 AD DS에 접근할 수 있도록 함.
> AD Connector는 AD DS와의 통합을 제공하며, MFA를 통해 보안을 강화할 수 있음.

◆ | **Q#0477.** | **Ref#0477.**
회사는 온프레미스 데이터 센터에서 3계층 웹 애플리케이션을 실행하고 있습니다. 프런트엔드는 Apache 웹 서버에서 제공되고, 중간 계층은 모놀리식 Java 애플리케이션이며, 스토리지 계층은 PostgreSQL 데이터베이스입니다.

최근 마케팅 프로모션 중에 애플리케이션이 다운되어 고객이 애플리케이션을 통해 주문할 수 없었습니다. 분석 결과 세 계층 모두 과부하가 발생한 것으로 나타났습니다. 애플리케이션이 응답하지 않게 되었고, 읽기 작업으로 인해 데이터베이스가 용량 제한에 도달했습니다. 회사는 가까운 시일 내에 이미 여러 가지 유사한 프로모션을 계획하고 있습니다.

솔루션 아키텍트는 이러한 문제를 해결하기 위해 AWS로 마이그레이션하기 위한 계획을 개발해야 합니다. 솔루션은 확장성을 극대화하고 운영 노력을 최소화해야 합니다.

어떤 단계 조합이 이러한 요구 사항을 충족합니까? (3개를 선택하세요.)

> **A.** 정적 자산이 Amazon S3에서 호스팅될 수 있도록 프런트엔드를 리팩터링합니다. Amazon CloudFront를 사용하여 고객에게 프런트엔드를 제공합니다. 프런트엔드를 Java 애플리케이션에 연결합니다.
> **B.** Auto Scaling 그룹에 있는 Amazon EC2 인스턴스에서 프런트엔드의 Apache 웹 서버를 다시 호스팅합니다. Auto Scaling 그룹 앞에 로드 밸런서를 사용합니다. Amazon Elastic File System(Amazon EFS)을 사용하여 Apache 웹 서버에 필요한 정적 자산을 호스팅합니다.
> **C.** Auto Scaling이 포함된 AWS Elastic Beanstalk 환경에서 Java 애플리케이션을 다시 호스팅합니다.
> **D.** Java 애플리케이션을 리팩터링하고, Java 애플리케이션을 실행하기 위한 Docker 컨테이너를 개발합니다. AWS Fargate를 사용하여 컨테이너를 호스팅합니다.
> **E.** AWS Database Migration Service(AWS DMS)를 사용하여 PostgreSQL 데이터베이스를 Amazon Aurora PostgreSQL 데이터베이스로 플랫폼을 변경합니다. 읽기 복제본에는 Aurora Auto Scaling을 사용합니다.
> **F.** 온프레미스 서버보다 메모리가 두 배 많은 Amazon EC2 인스턴스에 PostgreSQL 데이터베이스를 다시 호스팅합니다.
>
> 해설
> 정답: A, C, E
> A: 정적 콘텐츠를 S3와 CloudFront로 제공하면 확장성과 성능이 크게 향상됨. 이는 프론트엔드 서버의 부하를 줄이고 고객에게 더 빠른 응답 시간을 제공
> C: Elastic Beanstalk는 Java 애플리케이션을 자동으로 관리하고 확장할 수 있는 환경을 제공함. 이는 운영 노력을 최소화하면서도 애플리케이션의 가용성과 확장성을 보장
> E: Amazon Aurora는 고성능, 고가용성 데이터베이스 솔루션을 제공함. Auto Scaling 기능을 통해 읽기 부하를 효과적으로 처리할 수 있음. 이는 데이터베이스의 확장성과 성능을 최적화함.
> B(x): EC2 인스턴스와 EFS 사용은 운영 부담을 증가시킴
> D(x): Docker 컨테이너 사용은 Elastic Beanstalk 환경에 비해 운영 부담 증가
> F(x): EC2를 사용하는 것은 데이터베이스의 확장성을 제한

◆ | **Q#0478.** | **Ref#0478.**
한 회사가 AWS에 새로운 애플리케이션을 배포하고 있습니다. 애플리케이션은 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터와 Amazon Elastic Container Registry(Amazon ECR) 리포지토리로 구성됩니다. EKS 클러스터에는 AWS 관리형 노드 그룹이 있습니다.

회사의 보안 지침에는 AWS의 모든 리소스에 보안 취약성이 있는지 지속적으로 검사해야 한다고 명시되어 있습니다.

최소한의 운영 오버헤드로 이 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** AWS 보안 허브를 활성화합니다. EKS 노드와 ECR 리포지토리를 스캔하도록 Security Hub를 구성합니다.
> **B.** Amazon Inspector를 활성화하여 EKS 노드와 ECR 저장소를 스캔합니다.
> **C.** 새로운 Amazon EC2 인스턴스를 시작하고 AWS Marketplace에서 취약점 검색 도구를 설치합니다. EKS 노드를 스캔하도록 EC2 인스턴스를 구성합니다. 푸시 시 기본 스캔을 수행하도록 Amazon ECR을 구성합니다.
> **D.** EKS 노드에 Amazon CloudWatch 에이전트를 설치합니다. 지속적으로 검색하도록 CloudWatch 에이전트를 구성합니다. 푸시 시 기본 스캔을 수행하도록 Amazon ECR을 구성합니다.
>
> 해설
> 정답: B
> Amazon Inspector는 AWS에서 관리되는 보안 서비스로, EC2 인스턴스, 컨테이너 이미지 및 서버리

스 애플리케이션을 스캔하여 보안 취약성을 탐지함.
EKS 노드와 ECR 리포지토리를 지속적으로 스캔할 수 있으며, 운영 오버헤드를 최소화하면서 보안 지침을 준수할 수 있음.
A(x): AWS Security Hub는 보안 상태를 모니터링하고 중앙 집중식 보안 대시보드를 제공하지만, 직접적으로 취약성 스캔을 수행하지 않음.
C(x): 새로운 EC2 인스턴스를 관리하고 취약성 스캐닝 도구를 유지보수해야 하므로 운영 오버헤드가 큼.
D(x): CloudWatch 에이전트는 주로 로그 및 메트릭 수집을 위한 도구

◆ | **Q#0479.** | **Ref#0479.**
회사는 티켓팅 애플리케이션의 신뢰성을 향상시켜야 합니다. 애플리케이션은 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 실행됩니다. 회사는 Amazon CloudFront를 사용하여 애플리케이션을 제공합니다. ECS 클러스터의 단일 ECS 서비스는 CloudFront 배포의 오리진입니다.

이 애플리케이션에서는 특정 수의 활성 사용자만 티켓 구매 흐름에 참여할 수 있습니다. 이러한 사용자는 JWT(JSON 웹 토큰)의 암호화된 속성으로 식별됩니다. 다른 모든 사용자는 구매할 수 있는 용량이 확보될 때까지 대기실 모듈로 리디렉션됩니다.

애플리케이션에 높은 부하가 발생하고 있습니다. 대기실 모듈은 설계된 대로 작동하지만 대기실의 부하로 인해 애플리케이션 가용성이 저하됩니다.
이러한 중단은 애플리케이션의 티켓 판매 거래에 부정적인 영향을 미치고 있습니다.

부하가 높은 기간 동안 티켓 판매 거래에 가장 높은 신뢰성을 제공하는 솔루션은 무엇입니까?

A. 대기실을 위해 ECS 클러스터에 별도의 서비스를 생성합니다. 별도의 스케일링 구성을 사용하세요. 티켓팅 서비스가 JWT 정보를 사용하여 요청을 대기실 서비스로 적절하게 전달하도록 합니다.
B. 애플리케이션을 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터로 이동합니다. 대기실 모듈을 발권 포드와 별도의 포드로 분할합니다. 티켓팅 포드를 StatefulSet의 일부로 만듭니다. 발권 포드가 JWT 정보를 사용하고 요청을 대기실 포드에 적절하게 전달하는지 확인하세요.
C. 대기실을 위해 ECS 클러스터에 별도의 서비스를 생성합니다. 별도의 스케일링 구성을 사용하세요. CloudFront 함수를 만들어 JWT 정보를 검사하고 요청을 티켓팅 서비스 또는 대기실 서비스로 적절하게 전달하도록 합니다.
D. 애플리케이션을 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터로 이동합니다. 대기실 모듈을 발권 포드와 별도의 포드로 분할합니다. Kubernetes용 App Mesh 컨트롤러를 프로비저닝하여 AWS App Mesh를 사용하세요. 티켓팅 포드와 대기실 포드 간의 통신을 위해 mTLS 인증 및 서비스 간 인증을 활성화합니다. 발권 포드가 JWT 정보를 사용하고 요청을 대기실 포드에 적절하게 전달하는지 확인하세요.

해설
정답: C
대기실 모듈을 별도의 서비스로 분리하고 이를 독립적으로 스케일링할 수 있도록 설정하는 것이 높은 부하 동안 애플리케이션의 안정성을 향상시키는 데 도움이 됨.
CloudFront 함수를 사용하여 JWT 정보를 검사하고 요청을 적절한 서비스로 전달함으로써, 대기실 서비스의 부하가 티켓팅 서비스에 영향을 미치지 않도록 함.
B(x): EKS 클러스터로 이동하는 것은 필요 이상의 복잡성을 초래

◆ | **Q#0480.** | **Ref#0480.**
솔루션 아키텍트는 기존의 수동으로 생성된 비프로덕션 AWS 환경에서 AWS CloudFormation 템플릿을 만들고 있습니다. CloudFormation 템플릿은 필요에 따라 삭제하고 다시 생성할 수 있습니다. 이 환경에는 Amazon EC2 인스턴스가 포함되어 있으며, 해당 인스턴스는 상위 계정의 역할을 맡기 위해 인스턴스 프로필을 사용합니다.

솔루션 아키텍트는 CloudFormation 템플릿에서 동일한 역할 이름을 사용하여 역할을 다시 생성했습니다. 그러나 CloudFormation 템플릿이 하위 계정에서 실행될 때, EC2 인스턴스는 상위 계정에서 역할을 맡을 수 없게 되었습니다. 이는 권한 부족 때문입니다.

이 문제를 해결하려면 솔루션 설계자가 어떻게 해야 합니까?

> **A.** 상위 계정에서 EC2 인스턴스가 맡아야 하는 역할에 대한 신뢰 정책을 편집하십시오. sts:AssumeRole 작업을 허용하는 기존 구문의 대상 역할 ARN이 올바른지 확인하십시오. 신뢰 정책을 저장합니다.
> **B.** 상위 계정에서 EC2 인스턴스가 맡아야 하는 역할에 대한 신뢰 정책을 편집하십시오. 하위 계정의 루트 주체에 대해 sts:AssumeRole 작업을 허용하는 문을 추가합니다. 신뢰 정책을 저장합니다.
> **C.** CloudFormation 스택을 다시 업데이트합니다. CAPABILITY_NAMED_IAM 기능만 지정하세요.
> **D.** CloudFormation 스택을 다시 업데이트합니다. CAPABILITY_IAM 기능 및 CAPABILITY_NAMED_IAM 기능을 지정합니다.
>
> 해설
> 정답: A
> 이 문제는 상위 계정의 역할에 대한 신뢰 정책이 올바르게 설정되지 않았기 때문에 발생.
> 이는 ARN은 다르지만 역할 이름은 동일하게 생성할 때 발생할 수 있어 올바른 ARN을 반영하도록 신뢰 정책을 업데이트해야 함.
> 옵션 A는 상위 계정의 신뢰 정책에 하위 계정의 역할에 대한 올바른 ARN이 포함되어 있는지 확인하고 sts:AssumeRole 작업을 허용함으로써 이 문제를 해결
> B(x): 루트 주체가 역할을 맡도록 허용하는 것은 위험하므로 보안 문제로 인해 피해야 함.

481 (백은희,고민석) 5회차 完

◆ | **Q#0481.** | **Ref#0481.**
회사의 웹 애플리케이션에 안정성 문제가 있습니다. 이 응용 프로그램은 전 세계 고객에게 서비스를 제공합니다. 애플리케이션은 단일 Amazon EC2 인스턴스에서 실행되며 Amazon RDS for MySQL 데이터베이스에서 읽기 집약적인 작업을 수행합니다.

부하가 높으면 애플리케이션이 응답하지 않게 되며 EC2 인스턴스를 수동으로 다시 시작해야 합니다. 솔루션 설계자는 애플리케이션의 안정성을 향상해야 합니다.

최소한의 개발 노력으로 이 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

> **A.** Amazon CloudFront 배포판을 생성합니다. EC2 인스턴스를 배포 원본으로 지정합니다. RDS for MySQL 데이터베이스에 대한 다중 AZ 배포를 구성합니다. 읽기 집약적인 작업에는 대기 DB 인스턴스를 사용합니다.
> **B.** Auto Scaling 그룹에 있는 EC2 인스턴스에서 애플리케이션을 실행합니다. ELB(Elastic Load Balancing) 로드 밸런서 뒤에 EC2 인스턴스를 배치합니다. 데이터베이스 서비스를 Amazon Aurora로 교체합니다. 읽기 집약적인 작업에는 Aurora 복제본을 사용하십시오.
> **C.** AWS Global Accelerator를 배포합니다. RDS for MySQL 데이터베이스에 대한 다중 AZ 배포를 구성합니다. 읽기 집약적인 작업에는 대기 DB 인스턴스를 사용합니다.
> **D.** 애플리케이션을 AWS Lambda 함수로 마이그레이션합니다. RDS for MySQL 데이터베이스에 대한 읽기 전용 복제본을 생성합니다. 읽기 집약적인 작업에는 읽기 전용 복제본을 사용하세요.
>
> 해설
> 정답: B
> Auto Scaling 그룹을 사용하여 EC2 인스턴스를 배치하고, ELB 로드 밸런서 뒤에 놓고, Amazon Aurora로 데이터베이스를 교체하고,
> Aurora Replicas를 읽기 집중 작업에 사용하는 옵션 B가 가장 적은 개발 노력으로 문제를 해결함.
> D(x): Lambda 마이그레이션은 최소한의 개발 노력이 아님.

◆ | **Q#0482.** | **Ref#0482.**
회사에서는 Amazon S3 버킷이 있는 AWS Transfer Family SFTP 지원 서버를 사용하여 타사 데이터 공급업체로부터 업데이트를 받아야 합니다. 데이터는 Pretty Good Privacy(PGP) 암호화로 암호화됩니다. 회사에서는 데이터를

수신한 후 자동으로 데이터를 복호화하는 솔루션이 필요합니다. 솔루션 아키텍트는 Transfer Family 관리 워크플로를 사용합니다. 회사에서는 AWS Secrets Manager와 S3 버킷에 액세스할 수 있는 IAM 정책을 사용하여 IAM 서비스 역할을 만들었습니다. 역할의 신뢰 관계를 통해 transfer amazonaws.com 서비스가 역할을 맡을 수 있습니다.

솔루션 아키텍트는 자동 복호화를 위한 솔루션을 완료하기 위해 다음에 무엇을 해야 합니까?

> **A.** Secrets Manager에 PGP 공개 키를 저장합니다. Transfer Family 관리 워크플로에 명목 단계를 추가하여 파일을 암호 해독합니다. 명목 단계에서 PGP 암호화 매개변수를 구성합니다. 워크플로를 Transfer Family 서버와 연결합니다.
> **B.** Secrets Manager에 PGP 개인 키를 저장합니다. Transfer Family 관리 워크플로에 예외 처리 단계를 추가하여 파일을 암호 해독합니다. 예외 처리기에서 PGP 암호화 매개변수를 구성합니다. 워크플로를 SFTP 사용자와 연결합니다.
> **C.** Secrets Manager에 PGP 개인 키를 저장합니다. Transfer Family 관리 워크플로에 명목 단계를 추가하여 파일을 암호 해독합니다. 명목 단계에서 PGP 암호 해독 매개변수를 구성합니다. 워크플로를 Transfer Family 서버와 연결합니다.
> **D.** Secrets Manager에 PGP 공개 키를 저장합니다. Transfer Family 관리 워크플로에 예외 처리 단계를 추가하여 파일을 암호 해독합니다. 예외 처리기에서 PGP 암호 해독 매개변수를 구성합니다. 워크플로를 SFTP 사용자와 연결합니다.
>
> 해설
> 정답: C
> 이 방법은 PGP 개인 키를 사용하여 데이터를 복호화하는 과정을 정의합니다.
> Secrets Manager에 저장된 키를 사용해 Transfer Family 관리 워크플로우에서 데이터를 복호화하고, 워크플로우를 Transfer Family 서버와 연결하여 자동으로 데이터를 복호화할 수 있습니다.

◆ | **Q#0483.** | **Ref#0483.**
한 회사가 대규모 멀티플레이어 게임을 위한 인프라를 AWS로 이전하고 있습니다. 이 게임의 애플리케이션에는 플레이어가 실시간으로 순위를 볼 수 있는 리더보드가 있습니다. 리더보드에는 마이크로초 단위의 읽기와 1자리 밀리초 단위의 쓰기 지연 시간이 필요합니다. 데이터 세트는 1자리 테라바이트 크기이며 기본 노드에 장애가 발생하면 1분 이내에 쓰기를 허용할 수 있어야 합니다.

이 회사에는 데이터 파이프라인을 통해 추가 분석 처리를 위해 데이터를 유지할 수 있는 솔루션이 필요합니다.

어떤 솔루션이 이러한 요구 사항을 가장 적은 운영 오버헤드로 충족할까요?

> **B.** 읽기 복제본이 있는 Amazon RDS 데이터베이스를 만듭니다. 쓰기를 작성자 엔드포인트로 가리키도록 애플리케이션을 구성합니다. 읽기를 리더 엔드포인트로 가리키도록 애플리케이션을 구성합니다.
> **C.** Muit-AZ 모드에서 Redis용 Amazon MemoryDB 클러스터를 만듭니다. 애플리케이션이 기본 노드와 상호 작용하도록 구성합니다.
> **D.** 여러 가용성 영역에 걸쳐 분산된 Amazon EC2 인스턴스에 여러 Redis 노드를 만듭니다. Amazon S3에 대한 백업을 구성합니다.
>
> 해설
> 정답: C
> Multi-AZ 모드로 Amazon MemoryDB for Redis 클러스터를 생성하고, 애플리케이션이 주 노드와 상호작용하도록 구성합니다.
> 이 방법은 Microsecond reads와 single-digit-millisecond write latencies를 제공하는 Redis 기반의 데이터베이스를 사용합니다.
> 장점으로는 Multi-AZ 모드를 통한 고가용성을 제공하여, 주요 노드 실패 시 데이터를 수 분 내에 복구할 수 있습니다.
> 관리형 서비스인 Amazon MemoryDB for Redis를 사용하면 최소한의 운영 오버헤드를 유지할 수 있습니다.

데이터가 지속적으로 저장되어 데이터 파이프라인을 통한 추가적인 분석 처리에 사용할 수 있습니다.

◆ | **Q#0484.** | **Ref#0484.**
한 회사가 AWS 클라우드에서 여러 애플리케이션을 실행하고 있습니다. 애플리케이션은 회사의 별도 사업부에 특화되어 있습니다. 회사는 AWS Organizations의 조직에 있는 여러 AWS 계정에서 애플리케이션의 구성 요소를 실행하고 있습니다.

회사 조직의 모든 클라우드 리소스에는 BusinessUnit이라는 태그가 있습니다. 모든 태그에는 이미 사업부 이름의 적절한 값이 있습니다.

회사는 클라우드 비용을 여러 사업부에 할당해야 합니다. 회사는 또한 각 사업부의 클라우드 비용을 시각화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. 조직의 관리 계정에서 BusinessUnit이라는 이름의 비용 할당 태그를 만듭니다. 또한 관리 계정에서 Amazon S3 버킷과 AWS 비용 및 사용 보고서(AWS CUR)를 만듭니다. S3 버킷을 AWS CUR의 대상으로 구성합니다. 관리 계정에서 Amazon Athena를 사용하여 AWS CUR 데이터를 쿼리합니다. 시각화를 위해 Amazon QuickSight를 사용합니다.
B. 각 멤버 계정에서 BusinessUnit이라는 이름의 비용 할당 태그를 만듭니다. 조직의 관리 계정에서 Amazon S3 버킷과 AWS 비용 및 사용 보고서(AWS CUR)를 만듭니다. S3 버킷을 AWS CUR의 대상으로 구성합니다. 시각화를 위한 Amazon CloudWatch 대시보드를 만듭니다.
C. 조직의 관리 계정에서 BusinessUnit이라는 이름의 비용 할당 태그를 만듭니다. 각 멤버 계정에서 Amazon S3 버킷과 AWS 비용 및 사용 보고서(AWS CUR)를 만듭니다. 각 S3 버킷을 해당 AWS CUR의 대상으로 구성합니다. 관리 계정에서 시각화를 위한 Amazon CloudWatch 대시보드를 만듭니다.
D. 각 멤버 계정에서 BusinessUnit이라는 이름의 비용 할당 태그를 만듭니다. 또한 각 멤버 계정에서 Amazon S3 버킷과 AWS 비용 및 사용 보고서(AWS CUR)를 만듭니다. 각 S3 버킷을 해당 AWS CUR의 대상으로 구성합니다. 관리 계정에서 Amazon Athena를 사용하여 AWS CUR 데이터를 쿼리합니다. 시각화를 위해 Amazon QuickSight를 사용합니다.

해설
정답: A
이 솔루션은 아래와 같은 장점이 있습니다
중앙 집중식 관리: 모든 비용 관리와 보고서를 중앙에서 관리 계정에서 처리합니다. 이를 통해 관리가 더 단순해지고 효율적이 됩니다.
비용 할당 태그 적용: 비용 할당 태그는 중앙 관리 계정에서 한 번만 생성하면 되므로 이를 중심으로 모든 태그를 일관되게 관리할 수 있습니다.
강력한 데이터 분석 및 시각화: Amazon Athena와 Amazon QuickSight를 사용하여 AWS CUR 데이터를 쿼리하고 시각화할 수 있습니다. 이는 데이터 분석 및 시각화를 위한 효율적이고 강력한 도구입니다.

◆ | **Q#0485.** | **Ref#0485.**
유틸리티 회사가 스마트 미터에서 5분마다 사용 데이터를 수집하여 사용 시간 측정을 용이하게 하려고 합니다. 미터가 AWS로 데이터를 보내면 데이터가 Amazon API Gateway로 전송되고 AWS Lambda 함수에서 처리되어 Amazon DynamoDB 테이블에 저장됩니다. 파일럿 단계에서는 Lambda 함수가 완료되는 데 3~5초가 걸렸습니다.

더 많은 스마트 미터가 배포됨에 따라 엔지니어는 Lambda 함수가 완료되는 데 1~2분이 걸린다는 것을 알게 되었습니다. 장치에서 새로운 유형의 메트릭이 수집됨에 따라 함수의 지속 시간도 길어지고 있습니다. DynamoDB에서 PUT 작업을 수행하는 동안 많은 ProvisionedThroughputExceededException 오류가 발생하고 Lambda에서 많은 TooManyRequestsException 오류도 발생합니다.

어떤 변경 조합이 이러한 문제를 해결할까요? (두 가지를 선택하세요.)

A. DynamoDB 테이블에 대한 쓰기 용량 단위를 늘립니다.
B. 람다 함수에 사용할 수 있는 메모리를 늘립니다.
C. 더 많은 데이터를 전송하기 위해 스마트 미터의 탑재량 크기를 늘립니다.
D. API Gateway에서 Amazon Kinesis 데이터 스트림으로 데이터를 스트리밍하고 일괄 처리하여 데이터를 처리합니다.
E. Amazon SQS FIFO 대기열에서 데이터를 수집하여 각 메시지를 처리하기 위한 Lambda 함수를 트리거합니다.

해설
정답: A, D
A는 DynamoDB 테이블의 쓰기 용량 단위를 증가시킵니다.DynamoDB 테이블이 너무 많은 쓰기 요청을 처리하고 있는 경우, 쓰기 용량 단위를 늘려 더 많은 쓰기 요청을 처리할 수 있도록 합니다.
D는 데이터를 Amazon Kinesis 데이터 스트림으로 스트리밍하고, 데이터를 배치로 처리합니다.
이 접근 방식은 데이터를 실시간으로 스트리밍하고, 람다 함수가 데이터를 배치로 처리하도록 하여 더 효율적으로 데이터를 처리할 수 있게 합니다.

◆ | **Q#0486.** | **Ref#0486.**
한 회사가 최근 Amazon WorkSpaces의 성공적인 개념 증명을 완료했습니다. 솔루션 아키텍트는 두 AWS 지역에서 솔루션을 고가용성으로 만들어야 합니다. Amazon WorkSpaces는 장애 조치 지역(fail-over region)에 배포되고 호스팅된 영역은 Amazon Route 53에 배포됩니다.

솔루션 아키텍트는 솔루션에 대한 고가용성을 구성하기 위해 무엇을 해야 합니까?

A. 기본 지역과 장애 조치 지역에 연결 별칭(Connection Alias)을 만듭니다. 연결 별칭을 각 지역의 디렉토리와 연결합니다. Route 53 장애 조치 라우팅 정책(failover routing policy)을 만듭니다. Evaluate Target Health를 Yes로 설정합니다.
B. 기본 지역과 장애 조치 지역에 연결 별칭을 만듭니다. 연결 별칭을 기본 지역의 디렉토리와 연결합니다. Route 53 다중값 응답 라우팅 정책을 만듭니다.
C. 기본 리전에서 연결 별칭을 만듭니다. 연결 별칭을 기본 리전의 디렉토리와 연결합니다. Route 53 가중 라우팅 정책을 만듭니다.
D. 기본 지역에서 연결 별칭을 만듭니다. 연결 별칭을 장애 조치 지역의 디렉토리와 연결합니다. Route 53 장애 조치 라우팅 정책을 만듭니다. Evaluate Target Health를 Yes로 설정합니다.

해설
정답: A
페일오버 라우팅 정책(failover routing policy)은 주 리전의 WorkSpaces가 장애가 발생할 경우, 자동으로 대체 리전으로 트래픽을 전환할 수 있게 해줍니다.
Route 53의 페일오버 라우팅 정책을 설정하여 주 리전의 WorkSpaces가 장애가 발생할 경우 대체 리전으로 자동 전환되도록 구성합니다. Evaluate Target Health를 'Yes'로 설정하면, 헬스 체크를 통해 주 리전의 상태를 확인하여 고가용성을 보장할 수 있습니다.

◆ | **Q#0487.** | **Ref#0487.**
한 회사가 온프레미스 환경에서 AWS로 많은 VM을 마이그레이션할 계획입니다. 이 회사는 마이그레이션 전에 온프레미스 환경에 대한 초기 평가, VM에서 실행되는 애플리케이션 간의 종속성에 대한 시각화, 온프레미스 환경에 대한 평가를 제공하는 보고서가 필요합니다.

이 정보를 얻기 위해 이 회사는 Migration Evaluator 평가 요청을 시작했습니다. 이 회사는 제약 없이 온프레미스 환경에 수집기 소프트웨어를 설치할 수 있습니다.

어떤 솔루션이 회사에 필요한 정보를 최소한의 운영 오버헤드로 제공할까요?

A. 온프레미스 VM마다 AWS 애플리케이션 검색 에이전트를 설치합니다. 데이터 수집 기간이 끝나면 AWS 마이그레이션 허브를 사용하여 애플리케이션 종속성을 확인합니다. 마이그레이션 허브에서 빠른 인사이트 평가 보고서를 다운로드합니다.

B. 온프레미스 VM마다 Migration Evaluator Collector를 설치합니다. 데이터 수집 기간이 끝나면 Migration Evaluator를 사용하여 애플리케이션 종속성을 확인합니다. Migration Evaluator에서 발견된 서버 목록을 다운로드하여 내보냅니다. Amazon QuickSight에 목록을 업로드합니다. QuickSight 보고서가 생성되면 Quick Insights 평가 보고서를 다운로드합니다.
C. 온프레미스 환경에서 AWS Application Discovery Service Agentless Collector를 설정합니다. 데이터 수집 기간이 끝나면 AWS Migration Hub를 사용하여 애플리케이션 종속성을 확인합니다. Application Discovery Service에서 발견된 서버 목록을 내보냅니다. 목록을 Migration Evaluator에 업로드합니다. Migration Evaluator 보고서가 생성되면 Quick Insights 평가를 다운로드합니다.
D. 온프레미스 환경에서 Migration Evaluator Collector를 설정합니다. 각 VM에 AWS Application Discovery Agent를 설치합니다. 데이터 수집 기간이 끝나면 AWS Migration Hub를 사용하여 애플리케이션 종속성을 확인합니다. Migration Evaluator에서 Quick Insights 평가 보고서를 다운로드합니다.

해설
정답: C
에이전트리스 수집기(Agentless Collector)를 사용해 데이터를 수집하므로, 각 VM에 별도의 소프트웨어를 설치할 필요가 없으며, 운영 오버헤드를 최소화할 수 있습니다. 이후, Migration Hub를 통해 애플리케이션 종속성을 시각화하고, Migration Evaluator에서 평가 보고서를 생성할 수 있습니다. 이 방법은 최소한의 운영 오버헤드로 요구된 정보를 제공합니다.
다른 선택지들은 각 VM에 에이전트를 설치하거나, 여러 도구를 활용해야 하므로 운영 오버헤드가 더 크기 때문에 최적의 선택이 아닙니다.

◆ | **Q#0488.** | **Ref#0488.**
한 회사는 API 메서드의 로직을 포함하는 Amazon API Gateway API와 AWS Lambda 함수를 사용하여 AWS에서 기본 API를 호스팅합니다. 회사의 내부 애플리케이션은 핵심 기능과 비즈니스 로직에 API를 사용합니다. 회사의 고객은 API를 사용하여 계정의 데이터에 액세스합니다. 여러 고객은 단일 독립형 Amazon EC2 인스턴스에서 실행되는 레거시 API에도 액세스할 수 있습니다.

이 회사는 이러한 API의 보안을 강화하여 서비스 거부(DoS) 공격을 더 잘 방지하고, 취약성을 확인하고, 일반적인 악용을 방지하고자 합니다.

솔루션 아키텍트는 이러한 요구 사항을 충족하기 위해 무엇을 해야 할까요?

A. AWS WAF를 사용하여 두 API를 보호합니다. Amazon Inspector를 구성하여 레거시 API를 분석합니다. Amazon GuardDuty를 구성하여 API에 대한 악의적인 액세스 시도를 모니터링합니다.
B. AWS WAF를 사용하여 API Gateway API를 보호합니다. Amazon Inspector를 구성하여 두 API를 모두 분석합니다. Amazon GuardDuty를 구성하여 API에 대한 악의적인 액세스 시도를 차단합니다.
C. AWS WAF를 사용하여 API Gateway API를 보호합니다. Amazon Inspector를 구성하여 레거시 API를 분석합니다. Amazon GuardDuty를 구성하여 API에 액세스하려는 악의적인 시도를 모니터링합니다.
D. AWS WAF를 사용하여 API Gateway API를 보호하세요! Amazon Inspector를 구성하여 레거시 API를 보호하세요. Amazon GuardDuty를 구성하여 API에 액세스하려는 악의적인 시도를 차단합니다.

해설
정답: C
회사는 두 개의 API를 사용하고 있습니다. (Amazon API Gateway와 AWS Lambda로 구성된 API. 단일 Amazon EC2 인스턴스에서 실행 중인 레거시 API)
* AWS WAF는 API Gateway API를 보호하여 일반적인 웹 공격으로부터 방어할 수 있습니다.
* Amazon Inspector는 EC2환경인 레거시 API를 분석하여 보안 취약점을 검사하는 데 적합합니다.
* Amazon GuardDuty는 악의적인 접근 시도를 모니터링할 수 있으며, 두 API에 대한 모니터링을 제공할 수 있습니다.(차단기능을 제공하지 않습니다.)

◆ | **Q#0489.** | **Ref#0489.**
한 회사가 AWS에서 서버리스 전자상거래 애플리케이션을 실행하고 있습니다. 이 애플리케이션은 Amazon API Gateway를 사용하여 AWS Lambda Java 함수를 호출합니다. Lambda 함수는 Amazon RDS for MySQL 데이터베이스에 연결하여 데이터를 저장합니다.

최근 세일 이벤트 중에 웹 트래픽이 갑자기 증가하여 API 성능이 저하되고 데이터베이스 연결에 오류가 발생했습니다. 이 회사는 Lambda 함수의 지연 시간을 최소화하고 트래픽 급증을 지원하는 솔루션을 구현해야 합니다.

어떤 솔루션이 애플리케이션에 최소한의 변경으로 이러한 요구 사항을 충족할까요?

> **A.** Lambda 함수의 코드를 업데이트하여 Lambda 함수가 함수 핸들러 외부에서 데이터베이스 연결을 열도록 합니다. Lambda 함수에 대한 프로비저닝된 동시성을 증가시킵니다.
> **B.** 데이터베이스에 대한 RDS 프록시 엔드포인트를 만듭니다. AWS Secrets Manager에 데이터베이스 비밀을 저장합니다. 필요한 IAM 권한을 설정합니다. Lambda 함수를 업데이트하여 RDS 프록시 엔드포인트에 연결합니다. Lambda 함수에 대한 프로비저닝된 동시성을 늘립니다.
> **C.** 사용자 지정 매개변수 그룹을 만듭니다. max_connections 매개변수의 값을 늘립니다. 사용자 지정 매개변수 그룹을 RDS DB 인스턴스와 연결하고 재부팅을 예약합니다. Lambda 함수에 대한 예약된 동시성을 늘립니다.
> **D.** 데이터베이스에 대한 RDS 프록시 엔드포인트를 만듭니다. AWS Secrets Manager에 데이터베이스 비밀을 저장합니다. 필요한 IAM 권한을 설정합니다. Lambda 함수를 업데이트하여 RDS 프록시 엔드포인트에 연결합니다. Lambda 함수에 대한 예약된 동시성을 늘립니다.
>
> 해설
> 정답: B
> RDS Proxy 생성: RDS Proxy는 데이터베이스 연결 풀링을 제공하여, 많은 Lambda 함수 호출로 인해 발생할 수 있는 데이터베이스 연결 문제를 해결할 수 있습니다.
> Secrets Manager를 사용해 데이터베이스 자격 증명 관리: 안전한 자격 증명 관리를 위해 필요합니다.
> IAM 권한 설정 및 Lambda 함수 업데이트: Lambda 함수가 RDS Proxy를 통해 연결되도록 코드 변경이 필요합니다.
> 프로비저닝된 동시성 증가: 트래픽 폭증 시 성능을 유지하는 데 도움이 됩니다.

◆ | **Q#0490.** | **Ref#0490.**
어떤 회사에서는 모든 내부 애플리케이션 연결에 프라이빗 IP 주소를 사용하도록 요구합니다. 이 정책을 용이하게 하기 위해 솔루션 아키텍트가 AWS Public 서비스에 연결하는 인터페이스 엔드포인트(interface endpoints)를 만들었습니다. 테스트 결과, 솔루션 아키텍트는 서비스 이름이 퍼블릭 IP 주소로 확인되고 내부 서비스가 인터페이스 엔드포인트에 연결할 수 없다는 것을 알아챘습니다.

솔루션 아키텍트는 이 문제를 해결하기 위해 어떤 단계를 거쳐야 할까요?

> **A.** 인터페이스 엔드포인트에 대한 경로로 서브넷 경로 테이블을 업데이트합니다.
> **B.** VPC 속성에서 프라이빗 DNS 옵션을 활성화합니다.
> **C.** AWS 서비스에 대한 연결을 허용하도록 인터페이스 엔드포인트에서 보안 그룹을 구성합니다.
> **D.** 내부 애플리케이션에 대한 조건부 포워더를 사용하여 Amazon Route 53 개인 호스팅 영역을 구성합니다.
>
> 해설
> 정답: B
> 인터페이스 엔드포인트를 사용하여 내부 애플리케이션이 AWS 퍼블릭 서비스에 연결할 때, 퍼블릭 IP 주소 대신 프라이빗 IP 주소를 사용하도록 해야 합니다.
> 프라이빗 DNS 옵션을 활성화하면, 해당 서비스의 DNS 이름이 프라이빗 IP 주소로 해석되며, 내부 애플리케이션이 프라이빗 IP를 사용하여 서비스에 연결할 수 있습니다.

491 (김성원,송희성) 5회차 完

◆ | **Q#0491.** | **Ref#0491.**
한 회사가 지연에 민감한 애플리케이션을 개발하고 있습니다. 애플리케이션의 일부에는 가능한 한 빨리 초기화해야 하는 여러 AWS Lambda 함수가 포함되어 있습니다. Lambda 함수는 Java로 작성되었으며 라이브러리를 로드하고, 클래스를 초기화하고, 고유 ID를 생성하기 위한 핸들러 외부의 초기화 코드가 포함되어 있습니다.

어떤 솔루션이 가장 비용 효율적으로 시작 성능 요구 사항을 충족할까요?

> **A.** 모든 초기화 코드를 각 Lambda 함수의 핸들러로 옮깁니다. 각 Lambda 함수에 대해 Lambda SnapStart를 활성화합니다. SnapStart를 구성하여 각 Lambda 함수의 $LATEST 버전을 참조합니다.
> **B.** 각 Lambda 함수의 버전을 게시합니다. 각 Lambda 함수에 대한 별칭을 만듭니다. 각 별칭이 해당 버전을 가리키도록 구성합니다. 각 Lambda 함수에 대한 프로비저닝된 동시성 구성을 설정하여 해당 별칭을 가리킵니다.
> **C.** 각 Lambda 함수의 버전을 게시합니다. 각 Lambda 함수에 대해 프로비저닝된 동시성 구성을 설정하여 해당 버전을 가리킵니다. Lambda 함수의 게시된 버전에 대해 Lambda SnapStar를 활성화합니다.
> **D.** Lambda 함수를 업데이트하여 사전 스냅샷 후크를 추가합니다. 고유 ID를 생성하는 코드를 핸들러로 이동합니다. 각 Lambda 함수의 버전을 게시합니다. Lambda 함수의 게시된 버전에 대해 Lambda SnapStart를 활성화합니다.
>
> 해설
> 정답: D
>
> 사전 스냅샷 훅을 사용하여 초기화 작업을 효율적으로 처리하고, 고유 ID 생성 코드를 핸들러로 이동하여 SnapStart의 효과를 극대화하는 방법이 가장 비용 효율적입니다.
> SnapStart를 사용하면 Lambda 함수의 초기화 시간을 단축할 수 있으며, 특히 지연에 민감한 애플리케이션의 요구 사항을 충족할 수 있습니다.

◆ | **Q#0492.** | **Ref#0492.**
솔루션 아키텍트가 AWS Import/Export의 Amazon EC2 VM Import 기능을 사용하여 온프레미스 환경에서 VM을 가져오고 있습니다. 솔루션 아키텍트는 AMI를 생성하고 해당 AMI를 기반으로 하는 Amazon EC2 인스턴스를 프로비저닝했습니다. EC2 인스턴스는 VPC의 퍼블릭 서브넷 내부에서 실행되며 퍼블릭 IP 주소가 할당됩니다.

EC2 인스턴스는 AWS Systems Manager 콘솔에서 관리형 인스턴스로 나타나지 않습니다.

솔루션 아키텍트는 이 문제를 해결하기 위해 어떤 단계 조합을 취해야 합니까? (두 가지를 선택하세요.)

> **A.** 인스턴스에 Systems Manager Agent가 설치되어 실행 중인지 확인합니다.
> **B.** 인스턴스에 Systems Manager에 대한 적절한 IAM 역할이 할당되었는지 확인합니다.
> **C.** VPC에 VPC 엔드포인트가 있는지 확인합니다.
> **D.** AWS Application Discovery Agent가 구성되었는지 확인하세요.
> **E.** Systems Manager에 대한 서비스 연결 역할의 올바른 구성을 확인합니다.
>
> 해설
> 정답: A,B
>
> AWS Systems Manager가 EC2 인스턴스를 관리하려면 인스턴스에 Systems Manager Agent가 설치되어 실행 중이어야 하며, 인스턴스가 적절한 IAM 역할을 가져야 합니다.

◆ | **Q#0493.** | **Ref#0493.**
한 회사가 모든 애플리케이션에 대한 배포 도구로 AWS CloudFormation을 사용하고 있습니다. 버전 관리가 활성화된 Amazon S3 버킷 내에서 모든 애플리케이션 바이너리와 템플릿을 스테이징합니다. 개발자는 통합 개발 환경

(IDE)을 호스팅하는 Amazon EC2 인스턴스에 액세스할 수 있습니다. 개발자는 Amazon S3에서 EC2 인스턴스로 애플리케이션 바이너리를 다운로드하고 변경한 다음 로컬에서 단위 테스트를 실행한 후 바이너리를 S3 버킷에 업로드합니다. 개발자는 기존 배포 메커니즘을 개선하고 AWS CodePipeline을 사용하여 CI/CD를 구현하려고 합니다.

개발자는 다음과 같은 요구 사항을 가지고 있습니다.

- 소스 제어에 AWS CodeCommit을 사용합니다.
- 단위 테스트와 보안 스캐닝을 자동화합니다.
- 단위 테스트가 실패하면 개발자에게 알립니다.
- 애플리케이션 기능을 켜고 끄고 CI/CD의 일부로 배포를 동적으로 사용자 지정합니다.
- 애플리케이션을 배포하기 전에 수석 개발자에게 승인을 받습니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

> **A.** AWS CodeBuild를 사용하여 단위 테스트와 보안 스캔을 실행합니다. Amazon EventBridge 규칙을 사용하여 단위 테스트가 실패하면 개발자에게 Amazon SNS 알림을 보냅니다. 다양한 솔루션 기능에 대한 AWS Cloud Development Kit(AWS CDK) 구문을 작성하고 매니페스트 파일을 사용하여 AWS CDK 애플리케이션에서 기능을 켜고 끕니다. 파이프라인에서 수동 승인 단계를 사용하여 리드 개발자가 애플리케이션을 승인할 수 있도록 합니다.
> **B.** AWS Lambda를 사용하여 단위 테스트와 보안 스캔을 실행합니다. 파이프라인의 후속 단계에서 Lambda를 사용하여 단위 테스트가 실패하면 개발자에게 Amazon SNS 알림을 보냅니다. 다양한 솔루션 기능에 대한 AWS Amplify 플러그인을 작성하고 사용자 프롬프트를 사용하여 기능을 켜고 끕니다. 파이프라인에서 Amazon SES를 사용하여 리드 개발자가 애플리케이션을 승인할 수 있도록 합니다.
> **C.** Jenkins를 사용하여 단위 테스트와 보안 스캔을 실행합니다. 파이프라인에서 Amazon EventBridge 규칙을 사용하여 단위 테스트가 실패하면 개발자에게 Amazon SES 알림을 보냅니다. 다양한 솔루션 기능 및 매개변수에 AWS CloudFormation 중첩 스택을 사용하여 기능을 켜고 끕니다. 파이프라인에서 AWS Lambda를 사용하여 리드 개발자가 애플리케이션을 승인할 수 있도록 합니다.
> **D.** AWS CodeDeploy를 사용하여 단위 테스트와 보안 스캔을 실행합니다. 파이프라인에서 Amazon CloudWatch 알람을 사용하여 단위 테스트가 실패하면 개발자에게 Amazon SNS 알림을 보냅니다. 다양한 솔루션 기능에 Docker 이미지를 사용하고 AWS CLI를 사용하여 기능을 켜고 끕니다. 파이프라인에서 수동 승인 단계를 사용하여 리드 개발자가 애플리케이션을 승인할 수 있도록 합니다.
>
> 해설
> 정답: A
>
> AWS CodeBuild를 사용하여 단위 테스트와 보안 스캔을 실행할 수 있습니다.
> Amazon EventBridge 규칙을 사용하여 단위 테스트 실패 시 Amazon SNS 알림을 개발자에게 보낼 수 있습니다.
> AWS CDK를 사용하여 다양한 솔루션 기능에 대해 CDK Constructs를 작성하고, 매니페스트 파일을 사용하여 CI/CD 과정에서 기능을 동적으로 켜고 끌 수 있습니다.
> 파이프라인에 수동 승인 단계를 추가하여 리드 개발자가 애플리케이션을 승인할 수 있게 합니다.

◆ | Q#0494. | Ref#0494.
글로벌 전자상거래 회사는 전 세계에 많은 데이터 센터를 보유하고 있습니다. 저장된 데이터가 증가함에 따라 이 회사는 레거시 온프레미스 파일 애플리케이션에 확장 가능한 스토리지를 제공하는 솔루션을 설정해야 합니다. 이 회사는 AWS Backup을 사용하여 볼륨의 시점 복사본을 가져와야 하며 자주 액세스하는 데이터에 대한 저지연 액세스를 유지해야 합니다. 이 회사는 또한 회사의 온프레미스 애플리케이션 서버에서 iSCSI(Internet Small Computer System Interface) 장치로 마운트할 수 있는 스토리지 볼륨이 필요합니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. AWS Storage Gateway 테이프 게이트웨이를 프로비저닝합니다. 테이프 게이트웨이를 구성하여 Amazon S3 버킷에 데이터를 저장합니다. AWS Backup을 배포하여 볼륨의 특정 시점 복사본을 가져옵니다.
B. Amazon FSx 파일 게이트웨이와 Amazon S3 파일 게이트웨이를 프로비저닝합니다. AWS Backup을 배포하여 데이터의 특정 시점 복사본을 가져옵니다.
C. 캐시 모드에서 AWS Storage Gateway 볼륨 게이트웨이를 프로비저닝합니다. AWS Backup으로 온프레미스 Storage Gateway 볼륨을 백업합니다.
D. 캐시 모드에서 AWS Storage Gateway 파일 게이트웨이를 프로비저닝합니다. AWS Backup을 배포하여 볼륨의 특정 시점 복사본을 가져옵니다.

해설
정답: C

AWS Storage Gateway의 **Volume Gateway (Cache 모드)**는 온프레미스 애플리케이션 서버에서 iSCSI 장치로 마운트할 수 있는 스토리지 볼륨을 제공합니다.
이 모드에서는 자주 액세스하는 데이터가 로컬 캐시에 저장되어 저지연 액세스를 제공합니다.
AWS Backup을 사용하여 Storage Gateway 볼륨의 시점 복사본을 생성할 수 있습니다. 확장 가능한 스토리지, 저지연 액세스, 특정 시점 백업 및 iSCSI 장치 지원에 대한 모든 요구 사항을 위한 포괄적인 솔루션.

◆ | **Q#0495.** | **Ref#0495.**
한 회사에는 AWS Key Management Service(AWS KMS)를 사용하여 데이터를 암호화하고 복호화하는 애플리케이션이 있습니다. 이 애플리케이션은 AWS 지역의 Amazon S3 버킷에 데이터를 저장합니다. 회사 보안 정책에 따라 데이터를 S3 버킷에 넣기 전에 데이터를 암호화해야 합니다. 애플리케이션은 S3 버킷에서 파일을 읽을 때 데이터를 복호화해야 합니다.

회사는 S3 버킷을 다른 지역에 복제합니다. 솔루션 아키텍트는 애플리케이션이 여러 지역에서 데이터를 암호화하고 복호화할 수 있도록 솔루션을 설계해야 합니다. 애플리케이션은 동일한 키를 사용하여 각 지역의 데이터를 복호화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. KMS 다중 지역 기본 키를 만듭니다. KMS 다중 지역 기본 키를 사용하여 애플리케이션이 실행 중인 각 추가 지역에서 KMS 다중 지역 복제 키를 만듭니다. 각 지역에서 특정 복제 키를 사용하도록 애플리케이션 코드를 업데이트합니다.
B. 애플리케이션이 실행 중인 각 추가 지역에서 새로운 고객 관리 KMS 키를 만듭니다. 각 지역에서 특정 KMS 키를 사용하도록 애플리케이션 코드를 업데이트합니다.
C. AWS Private Certificate Authority를 ??사용하여 기본 리전에 새 인증 기관(CA)을 만듭니다. CA에서 애플리케이션의 웹사이트 URL에 대한 새 개인 인증서를 발급합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 추가 리전과 CA를 공유합니다. 각 리전에서 공유된 CA 인증서를 사용하도록 애플리케이션 코드를 업데이트합니다.
D. AWS Systems Manager Parameter Store를 사용하여 애플리케이션이 실행 중인 각 추가 리전에 매개변수를 만듭니다. 기본 리전의 KMS 키에서 키 자료를 내보냅니다. 각 리전의 매개변수에 키 자료를 저장합니다. 각 리전의 매개변수에서 키 데이터를 사용하도록 애플리케이션 코드를 업데이트합니다.

해설
정답: A

KMS Multi-Region Primary Key와 Replica Key는 여러 리전에서 동일한 암호화 키를 사용할 수 있도록 해줍니다. 이 솔루션을 사용하면 애플리케이션은 각 리전에서 데이터를 암호화하고 복호화할 때 동일한 키를 사용할 수 있습니다.

KMS 멀티 리전 기본 키를 생성하고 각 추가 리전에 멀티 리전 복제 키를 생성한 후 애플리케이션 코드가 해당 리전의 복제 키를 사용하도록 업데이트하면 요구 사항을 충족할 수 있습니다.

◆ | **Q#0496.** | **Ref#0496.**
한 회사가 Application Load Balancer(ALB) 뒤의 Auto Scaling 그룹에서 여러 Amazon EC2 인스턴스를 사용하는 애플리케이션을 호스팅합니다. EC2 인스턴스의 초기 시작 중에 EC2 인스턴스는 사용자 데이터 스크립트를 실행하여 Amazon S3 버킷에서 애플리케이션의 중요한 콘텐츠를 다운로드합니다.

EC2 인스턴스는 올바르게 시작됩니다. 그러나 일정 시간 후 EC2 인스턴스는 다음과 같은 오류 메시지와 함께 종료됩니다. "ELB 시스템 상태 검사 실패에 대한 응답으로 인스턴스가 서비스에서 제외되었습니다." EC2 인스턴스는 무한 루프에서 Auto Scaling 이벤트로 인해 계속 시작되고 종료됩니다.

배포에 대한 최근의 유일한 변경 사항은 회사가 S3 버킷에 많은 양의 중요한 콘텐츠를 추가했다는 것입니다. 회사는 프로덕션에서 사용자 데이터 스크립트를 변경하고 싶어하지 않습니다.

프로덕션 환경에서 성공적으로 배포할 수 있도록 솔루션 아키텍트는 무엇을 해야 합니까?

A. EC2 인스턴스의 크기를 늘립니다.
B. ALB에 대한 상태 점검 시간 제한을 늘립니다.
C. ALB에 대한 상태 검사 경로를 변경합니다.
D. 자동 크기 조정 그룹의 상태 검사 유예 기간을 늘립니다.

해설
정답: D
EC2인스턴스가 시작되고 나서 중요한 컨텐츠를 S3에서 로드하는 데 시간이 걸리므로, 인스턴스가 아직 준비되지 않은 상태에서 ALB 헬스체크에 실패하고 있다. 이로 인해 오토 스케일링 그룹은 인스턴스를 계속 시작하고 종료하는 과정을 반복하고 있다. 따라서 오토스케일링 그룹이 인스턴스 헬스체크 시간을 연장하는 것이 정답이 된다.

◆ | **Q#0497.** | **Ref#0497.**
회사에서 온프레미스 Oracle 데이터베이스를 AWS로 옮겨야 합니다. 이 회사는 비즈니스 규정 준수를 위해 일부 데이터베이스를 온프레미스에 유지하기로 했습니다.

온프레미스 데이터베이스에는 공간 데이터가 포함되어 있으며 유지 관리를 위해 크론 작업이 실행됩니다. 이 회사는 AWS에서 온프레미스 시스템에 직접 연결하여 데이터를 외래 테이블로 쿼리해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 자동 스케일링이 활성화된 Amazon DynamoDB 글로벌 테이블을 만듭니다. AWS Schema Conversion Tool(AWS SCT) 및 AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스에서 DynamoDB로 데이터를 이동합니다. AWS Lambda 함수를 만들어 공간 데이터를 Amazon S3로 이동합니다. Amazon Athena를 사용하여 데이터를 쿼리합니다. Amazon EventBridge를 사용하여 유지 관리를 위해 DynamoDB에서 작업을 예약합니다. Amazon API Gateway를 사용하여 외래 테이블 지원을 수행합니다.
B. Microsoft SQL Server DB 인스턴스용 Amazon RDS를 만듭니다. 네이티브 복제를 사용하여 온프레미스에서 DB 인스턴스로 데이터를 이동합니다. AWS Schema Conversion Tool(AWS SCT)을 사용하여 복제 후 필요에 따라 SQL Server 스키마를 수정합니다. 공간 데이터를 Amazon Redshift로 이동합니다. 시스템 유지 관리를 위해 저장 프로시저를 사용합니다. AWS Glue 크롤러를 만들어 외래 테이블 지원을 위해 온프레미스 Oracle 데이터베이스에 연결합니다.
C. Oracle 데이터베이스를 호스팅하기 위해 Amazon EC2 인스턴스를 시작합니다. EC2 인스턴스를 Auto Scaling 그룹에 배치합니다. AWS Application Migration Service를 사용하여 온프레미스에서 EC2 인스턴스로 데이터를 이동하고 실시간 양방향 변경 데이터 캡처(CDC) 동기화를 수행합니다. Oracle 네이티브 공간 데이터 지원을 사용합니다. AWS Step Functions 워크플로의 일부로 유지 관리 작업을 실행하는 AWS Lambda 함수를 만듭니다. 외래 테이블 지원을 위한 인터넷 게이트웨이를 만듭니다.

D. Amazon RDS for PostgreSQL DB 인스턴스를 만듭니다. AWS Schema Conversion Tool(AWS SCT) 및 AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스에서 DB 인스턴스로 데이터를 이동합니다. PostgreSQL 네이티브 공간 데이터 지원을 사용합니다. 유지 관리를 위해 DB 인스턴스에서 cron 작업을 실행합니다. AWS Direct Connect를 사용하여 DB 인스턴스를 온프레미스 환경에 연결하여 외래 테이블 지원을 제공합니다.

해설
정답: D
PostgreSql은 오라클과 유사한 Spacial data처리를 지원하며, AWS SCT, DMS를 사용해 데이터를 RDS로 Migration이 가능하다.
반면 DynamoDB와 SQL Server는 Spacial data(공간 데이터)를 효율적으로 지원하지 않으며
C의 경우 인터넷 게이트웨이를 사용하는 것은 보안 및 성능 문제를 야기 할 수 있다.

◆ | **Q#0498.** | **Ref#0498.**
Accompany는 Amazon EC2와 AWS Lambda에서 애플리케이션을 실행합니다. 이 애플리케이션은 Amazon S3에 임시 데이터를 저장합니다. S3 객체는 24시간 후에 삭제됩니다.

이 회사는 AWS CloudFormation 스택을 실행하여 애플리케이션의 새 버전을 배포합니다. 스택은 필요한 리소스를 만듭니다. 새 버전을 검증한 후 이 회사는 이전 스택을 삭제합니다. 이전 개발 스택을 삭제하는 데 최근에 실패했습니다. 솔루션 아키텍트는 주요 아키텍처 변경 없이 이 문제를 해결해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. S3 버킷에서 객체를 삭제하는 Lambda 함수를 만듭니다. S3 버킷 리소스를 가리키는 DependsOn 속성이 있는 CloudFormation 스택에 Lambda 함수를 사용자 지정 리소스로 추가합니다.
B. CloudFormation 스택을 수정하여 S3 버킷에 Delete 값이 있는 DeletionPolicy 속성을 연결합니다.
C. S3 버킷 리소스에 대한 스냅샷 값을 갖는 DeletionPolicy 속성을 추가하기 위해 CloudFormation 스택을 업데이트합니다.
D. CloudFormation 템플릿을 업데이트하여 Amazon S3 대신 임시 파일을 저장하는 Amazon Elastic File System(Amazon EFS) 파일 시스템을 만듭니다. Lambda 함수를 EFS 파일 시스템과 동일한 VPC에서 실행되도록 구성합니다.

해설
정답: A
S3 버킷에 저장된 임시 데이터들 중 이전 스택과 의존된 상태여서 의존 스택을 삭제하는 데 실패하였다.
따라서 S3 버킷에서 임시 데이터를 삭제한 후 이전 스택을 삭제하도록 합니다.

◆ | **Q#0499.** | **Ref#0499.**
한 회사에는 S3 Standard 스토리지를 사용하는 Amazon S3 버킷에 사용자가 업로드한 비디오를 저장하는 애플리케이션이 있습니다. 사용자는 비디오가 업로드된 후 처음 180일 동안 비디오에 자주 액세스합니다. 180일 후에 액세스하는 경우는 드뭅니다. 명명된 사용자와 익명 사용자가 비디오에 액세스합니다.

대부분의 비디오는 크기가 100MB가 넘습니다. 사용자는 비디오를 업로드할 때 인터넷 연결이 좋지 않아 업로드가 실패하는 경우가 많습니다. 이 회사는 비디오에 다중 파트 업로드를 사용합니다.

솔루션 아키텍트는 애플리케이션의 S3 비용을 최적화해야 합니다.

이러한 요구 사항을 충족하는 작업의 조합은 무엇입니까? (두 가지를 선택하십시오.)

A. S3 버킷을 요청자 지불 버킷으로 구성합니다.
B. S3 전송 가속을 사용하여 비디오를 S3 버킷에 업로드합니다.
C. 불완전한 멀티파트 업로드를 시작한 후 7일이 지나면 업로드가 만료되도록 S3 라이프사이클 구성을 생성합니다.
D. 1일 후 객체를 S3 Glacier Instant Retrieval로 전환하기 위한 S3 수명 주기 구성을 생성합니다.

E. 180일 후에 객체를 S3 Standard-Infrequent Access(S3 Standard-IA)로 전환하기 위한 S3 수명 주기 구성을 생성합니다.

해설
정답: CE
미완성 multipart 업로드는 저장 공간을 차지하므로, 7일 후에 만료되도록 S3 라이프사이클 구성을 설정하면 비용을 절감할 수 있습니다.
비디오가 처음 180일 동안 자주 접근되지만 이후에는 접근이 드물기 때문에, 180일 후에 S3 Standard-IA로 전환하면 저장 비용을 절감할 수 있습니다.
S3 Standard-IA는 저렴한 비용으로 비정기적으로 접근하는 데이터를 저장하는 데 적합합니다.
A(x): 전체적인 비용 절감은 되나, 사용자에게 비용이 부과되어 적합하지 않다.
B(x): S3에 추가적인 비용을 발생시킨다.
D(x): 180일의 자주 액세스되는 기간동안 Glacier로 접근하게 되며, 접근 시 복구 비용이 발생된다. 따라서 추가 비용 발생될 수 있음.

◆ | **Q#0500.** | **Ref#0500.**
한 회사가 AWS에서 전자상거래 웹 애플리케이션을 실행합니다. 웹 애플리케이션은 콘텐츠 전송을 위해 Amazon CloudFront가 있는 Amazon S3에서 정적 웹사이트로 호스팅됩니다. Amazon API Gateway API는 AWS Lambda 함수를 호출하여 웹 애플리케이션에 대한 사용자 요청과 주문 처리를 처리합니다. Lambda 함수는 온디맨드 인스턴스를 사용하는 Amazon RDS for MySQL DB 클러스터에 데이터를 저장합니다. DB 클러스터 사용은 지난 12개월 동안 일관적이었습니다.

최근에 웹사이트에서 SQL 주입 및 웹 악용 시도가 발생했습니다. 고객들은 또한 사용량이 가장 많은 기간 동안 주문 처리 시간이 증가했다고 보고합니다. 이러한 기간 동안 Lambda 함수는 종종 콜드 스타트를 수행합니다. 회사가 성장함에 따라 회사는 트래픽이 가장 많은 기간 동안 확장성과 저지연 액세스를 보장해야 합니다. 회사는 또한 데이터베이스 비용을 최적화하고 SQL 주입 및 웹 악용 시도에 대한 보호 기능을 추가해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Lambda 함수가 피크 기간 동안 시간 초과 값을 늘리도록 구성합니다. 데이터베이스에 RDS 예약 인스턴스를 사용합니다. CloudFront를 사용하고 AWS Shield Advanced에 가입하여 SQL 주입 및 웹 익스플로잇 시도로부터 보호합니다.
B. Lambda 함수의 메모리를 늘리고, 데이터베이스를 위해 Amazon Redshift로 전환합니다. Amazon Inspector를 CloudFront와 통합하여 SQL 주입 및 웹 익스플로잇 시도로부터 보호합니다.
C. 피크 기간 동안 컴퓨팅을 위해 프로비저닝된 동시성을 갖춘 Lambda 함수를 사용하고, 데이터베이스의 경우 Amazon Aurora Serverless로 전환합니다. CloudFront를 사용하고 AWS Shield Advanced에 가입하여 SQL 주입 및 웹 익스플로잇 시도로부터 보호합니다.
D. 피크 기간 동안 컴퓨팅을 위해 프로비저닝된 동시성을 갖춘 Lambda 함수를 사용합니다. 데이터베이스에는 RDS 예약 인스턴스를 사용합니다. SQL 주입 및 웹 익스플로잇 시도로부터 보호하기 위해 AWS WAF를 CloudFront와 통합합니다.

해설
정답: D
Provisioned Concurrency는 피크 기간 동안 Lambda 함수의 콜드 스타트 문제를 줄여주며, 사전 초기화된 Lambda 인스턴스를 제공하여 요청 처리 시간을 단축시킵니다.
예약 인스턴스는 데이터베이스 사용량이 일관된 경우 비용을 절감할 수 있는 옵션입니다.
AWS WAF를 CloudFront와 통합하면 SQL 인젝션 및 웹 악용 시도로부터 보호할 수 있습니다.
WAF는 특정 웹 애플리케이션 공격에 대한 필터링 및 보호를 제공하여 보안을 강화합니다.