101 (황호실) 4회차 完

◆ | **Q#0101.** | **Ref#0101.**
한 회사가 다중 계정 환경의 AWS에서 애플리케이션을 실행하고 있습니다. 회사의 영업팀과 마케팅팀은 AWS Organizations에서 별도의 AWS 계정을 사용합니다.

영업팀은 Amazon S3 버킷에 페타바이트 규모의 데이터를 저장합니다. 마케팅 팀은 데이터 시각화를 위해 Amazon QuickSight를 사용합니다. 마케팅 팀은 상태 팀이 S3 버킷에 저장하는 데이터에 액세스해야 합니다. 회사는 AWS KMS(AWS Key Management Service) 키를 사용하여 S3 버킷을 암호화했습니다. 마케팅 팀은 마케팅 AWS 계정에 QuickSight 액세스를 제공하기 위해 QuickSight에 대한 IAM 서비스 역할을 이미 생성했습니다. 회사에는 AWS 계정 전체에서 S3 버킷의 데이터에 대한 보안 액세스를 제공하는 솔루션이 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 마케팅 계정에 새 S3 버킷을 생성합니다. 판매 계정에서 S3 복제 규칙을 생성하여 마케팅 계정의 새 S3 버킷에 객체를 복사합니다. 새 S3 버킷에 대한 액세스 권한을 부여하려면 마케팅 계정의 QuickSight 권한을 업데이트하세요.
> **B.** SCP를 생성하여 마케팅 계정에 S3 버킷에 대한 액세스 권한을 부여합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 sates 계정의 KMS 키를 마케팅 계정과 공유합니다. S3 버킷에 대한 액세스 권한을 부여하려면 마케팅 계정의 QuickSight 권한을 업데이트하세요.
> **C.** 마케팅 계정의 S3 버킷 정책을 업데이트하여 QuickSight 역할에 대한 액세스 권한을 부여합니다. S3 버킷에 사용되는 암호화 키에 대한 KMS 권한을 생성합니다. QuickSight 역할에 암호 해독 액세스 권한을 부여합니다. S3 버킷에 대한 액세스 권한을 부여하려면 마케팅 계정의 QuickSight 권한을 업데이트하세요.
> **D.** 판매 계정에 IAM 역할을 생성하고 S3 버킷에 대한 액세스 권한을 부여합니다. 마케팅 계정에서 판매 계정의 IAM 역할을 맡아 S3 버킷에 액세스합니다. QuickSight 루트를 업데이트하여 영업 계정의 새 IAM 역할과 신뢰 관계를 생성합니다.
>
> 해설
> 정답:D
> 이 문제의 핵심 요구 사항은 판매 팀의 S3 버킷에 저장된 암호화된 데이터를 마케팅 팀이 최소한의 운영 오버헤드로 접근할 수 있게 하는 것.
> 판매 계정에 IAM 역할을 생성하고 S3 버킷에 대한 액세스를 부여합니다. 마케팅 계정에서는 이 IAM 역할을 수임하여 S3 버킷에 접근합니다.
> 이 방법은 다른 계정에서 이미 설정된 QuickSight 역할과의 신뢰 관계를 통해 작업을 수행할 수 있으므로 운영 오버헤드가 적습니다.
>
> 이 접근 방식은 S3 버킷에 직접 접근할 수 있고, 추가적인 복사나 설정 없이 간단하게 마케팅 팀이 데이터를 활용할 수 있게 해줍니다.

◆ | **Q#0102.** | **Ref#0102.**
한 회사가 비즈니스에 중요한 애플리케이션을 온프레미스 데이터 센터에서 AWS로 마이그레이션할 계획입니다. 회사에는 Microsoft SQL Server Always On 클러스터가 온프레미스에 설치되어 있습니다. 회사는 AWS 관리형 데이터베이스 서비스로 마이그레이션하려고 합니다. 솔루션 아키텍트는 AWS에서 이기종 데이터베이스 마이그레이션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 백업 및 복원 유틸리티를 사용하여 SQL Server 데이터베이스를 MySQL용 Amazon RDS로 마이그레이션합니다.
> **B.** AWS Snowball Edge Storage Optimized 디바이스를 사용하여 Amazon S3로 데이터를 전송합니다. MySQL용 Amazon RDS를 설정합니다. BULK INSERT와 같은 SQL Server 기능과 S3 통합을 사용합

니다.
C. AWS Schema Conversion Tool을 사용하여 데이터베이스 스키마를 MySQL용 Amazon RDS로 변환합니다. 그런 다음 AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스 데이터베이스의 데이터를 Amazon RDS로 마이그레이션합니다.
D. AWS DataSync를 사용하여 온프레미스 스토리지와 Amazon S3 간에 네트워크를 통해 데이터를 마이그레이션합니다. MySQL용 Amazon RDS를 설정합니다. BULK INSERT와 같은 SQL Server 기능과 S3 통합을 사용합니다.

해설
정답:C
핵심은 회사의 온프레미스 Microsoft SQL Server Always On 클러스터를 AWS의 관리형 데이터베이스 서비스로 이기종 데이터베이스 마이그레이션 하는 것.
C: AWS Schema Conversion Tool을 사용하여 SQL Server의 데이터베이스 스키마를 Amazon RDS for MySQL로 변환한 후,
AWS Database Migration Service (AWS DMS)를 사용하여 온프레미스 데이터베이스에서 Amazon RDS로 데이터를 마이그레이션합니다.
이 접근법은 이기종 데이터베이스 마이그레이션을 효율적으로 수행할 수 있도록 도와줍니다.

◆ | **Q#0103.** | **Ref#0103.**
출판사의 디자인 팀은 전자상거래 웹 애플리케이션에서 사용하는 아이콘과 기타 정적 자산을 업데이트합니다. 회사는 회사의 프로덕션 계정에서 호스팅되는 Amazon S3 버킷의 아이콘과 자산을 제공합니다. 회사에서는 디자인 팀 구성원이 액세스할 수 있는 개발 계정도 사용합니다.

디자인 팀이 개발 계정의 정적 자산을 테스트한 후 디자인 팀은 프로덕션 계정의 S3 버킷에 자산을 로드해야 합니다. 솔루션 설계자는 원치 않는 변경 위험에 웹 애플리케이션의 다른 부분을 노출시키지 않고 디자인 팀에게 프로덕션 계정에 대한 액세스 권한을 제공해야 합니다.

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

A. 프로덕션 계정에서 S3 버킷에 대한 읽기 및 쓰기 액세스를 허용하는 새로운 IAM 정책을 생성하십시오.
B. 개발 계정에서 S3 버킷에 대한 읽기 및 쓰기 액세스를 허용하는 새로운 IAM 정책을 생성합니다.
C. 프로덕션 계정에서 역할을 생성하고 새 정책을 역할에 연결합니다. 개발 계정을 신뢰할 수 있는 엔터티로 정의합니다.
D. 개발 계정에서 역할을 생성합니다. 역할에 새 정책을 연결합니다. 프로덕션 계정을 신뢰할 수 있는 엔터티로 정의합니다.
E. 개발 계정에서 디자인 팀의 모든 IAM 사용자를 포함하는 그룹을 생성합니다. 프로덕션 계정의 역할에 대한 sts:AssumeRole 작업을 허용하도록 그룹에 다른 IAM 정책을 연결합니다.
F. 개발 계정에서 디자인 팀의 모든 IAM 사용자를 포함하는 그룹을 생성합니다. 개발 계정의 역할에 대해 sts:AssumeRole 작업을 허용하도록 그룹에 다른 IAM 정책을 연결합니다.

해설
정답: ACE
A 단계는 프로덕션 계정에서 S3 버킷에 대한 적절한 권한을 설정합니다.
C 단계는 개발 계정의 사용자가 프로덕션 계정의 역할을 맡을 수 있도록 설정합니다.
E 단계는 디자인 팀이 프로덕션 계정의 역할을 맡을 수 있도록 합니다.

◆ | **Q#0104.** | **Ref#0104.**
한 회사에서 AWS Elastic Beanstalk 및 Java를 사용하여 파일럿 애플리케이션을 개발했습니다. 개발 중 비용을 절감하기 위해 회사의 개발 팀은 애플리케이션을 단일 인스턴스 환경에 배포했습니다. 최근 테스트에 따르면 애플리케

이션이 예상보다 더 많은 CPU를 소비하는 것으로 나타났습니다. CPU 사용률은 정기적으로 85%를 초과하므로 일부 성능 병목 현상이 발생합니다.

솔루션 설계자는 회사가 애플리케이션을 프로덕션에 출시하기 전에 성능 문제를 완화해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 새로운 Elastic Beanstalk 애플리케이션을 생성합니다. 로드 밸런싱된 환경 유형을 선택합니다. 모든 가용 영역을 선택합니다. 최대 CPU 사용률이 5분 동안 85%를 초과하는 경우 실행되는 확장 규칙을 추가합니다.
> **B.** 두 번째 Elastic Beanstalk 환경을 생성합니다. 트래픽 분할 배포 정책을 적용합니다. 평균 CPU 사용률이 5분 동안 85%를 초과하는 경우 새 환경으로 전달할 수신 트래픽의 비율을 지정합니다.
> **C.** 로드 밸런싱된 환경 유형을 사용하도록 기존 환경의 용량 구성을 수정합니다. 모든 가용 영역을 선택합니다. 평균 CPU 사용률이 5분 동안 85%를 초과하는 경우 실행되는 확장 규칙을 추가합니다.
> **D.** 로드 밸런싱 옵션을 사용하여 환경 재구축 작업을 선택합니다. 가용성 영역을 선택합니다. 총 CPU 사용률이 5분 동안 85%를 초과하는 경우 실행되는 확장 규칙을 추가합니다.
>
> 해설
> 정답:C
> 기존 환경의 용량 구성을 수정하여 로드 밸런싱 환경 유형을 사용하도록 설정합니다. 모든 가용 영역을 선택합니다.
> 평균 CPU 사용률이 5분 동안 85%를 초과할 경우 자동으로 확장되는 규칙을 추가합니다.
> 이 솔루션은 기존 Elastic Beanstalk 환경을 로드 밸런싱 구성으로 변경하여 성능 문제를 최소한의 운영 부담으로 해결합니다.
> CPU 사용률이 85%를 초과할 경우 자동으로 인스턴스가 확장되며, 이를 통해 부하를 여러 인스턴스로 분산시켜 성능을 개선할 수 있습니다.

◆ | **Q#0105.** | **Ref#0105.**
한 금융 회사가 현재 세대의 Linux EC2 인스턴스에서 비즈니스 크리티컬 애플리케이션을 실행하고 있습니다. 이 애플리케이션에는 과도한 I/O 작업을 수행하는 자체 관리형 MySQL 데이터베이스가 포함되어 있습니다. 해당 애플리케이션은 해당 달 동안 적당한 양의 트래픽을 처리하기 위해 잘 작동하고 있습니다. 그러나 회사가 증가된 수요를 충족하기 위해 인프라 내에서 Elastic Load Balancer 및 Auto Scaling을 사용하고 있음에도 불구하고 월말 보고로 인해 매월 마지막 3일 동안 속도가 느려집니다.

다음 중 데이터베이스가 성능에 가장 적은 영향을 미치면서 월말 로드를 처리할 수 있도록 하는 작업은 무엇입니까?

> **A.** 더 큰 인스턴스 유형을 사용하여 Elastic Load Balancer를 예열하고 모든 Amazon EBS 볼륨을 GP2 볼륨으로 변경합니다.
> **B.** 데이터베이스 클러스터를 Amazon RDS로 일회성 마이그레이션을 수행하고, 월말 동안 로드를 처리하기 위해 여러 개의 추가 읽기 전용 복제본을 생성합니다.
> **C.** AWS Lambda와 함께 Amazon CloudWatch를 사용하여 특정 CloudWatch 지표를 기반으로 클러스터에 있는 Amazon EBS 볼륨의 유형, 크기 또는 IOPS를 변경합니다.
> **D.** 월말 전에 스냅샷을 찍고 나중에 되돌려 기존의 모든 Amazon EBS 볼륨을 사용 가능한 최대 스토리지 크기와 초당 I/O를 갖춘 새로운 PIOPS 볼륨으로 교체합니다.
>
> 해설
> 정답:B
> 데이터베이스 클러스터를 Amazon RDS로 일회성 마이그레이션을 수행하고, 월말 동안 로드를 처리하기 위해 여러 개의 추가 읽기 전용 복제본을 생성합니다.
> 데이터베이스를 Amazon RDS로 >마이그레이션하면 월말에 증가된 읽기 트래픽을 처리하기 위해 읽기 복제본을 쉽게 확장할 수 있는 기능이 제공되므로 이는 최적의 솔루션입니다.
> 또한 RDS는 기본 인프라를 관리하고 자동 백업,소프트웨어 패치 및 모니터링을 제공하여 회사의 운영 오버헤드를 줄여줍니다.

옵션 A는 도움이 될 수 있지만 무거운 부하를 처리하기에는 충분하지 않습니다. 옵션 C와 D는 효율적인 솔루션이 아닙니다.

◆ | **Q#0106.** | **Ref#0106.**
회사는 회사 데이터 센터에 있는 VM에 대해 복잡한 종속성을 갖는 Java 애플리케이션을 실행합니다. 응용 프로그램이 안정적입니다. 하지만 회사는 기술 스택을 현대화하고 싶어합니다. 회사는 애플리케이션을 AWS로 마이그레이션하고 서버 유지 관리에 드는 관리 오버헤드를 최소화하려고 합니다.

최소한의 코드 변경으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS App2Container를 사용하여 애플리케이션을 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)로 마이그레이션합니다. 컨테이너 이미지를 Amazon Elastic Container Registry(Amazon ECR)에 저장합니다. ECS 작업 실행 역할에 ECR 이미지 리포지토리에 액세스할 수 있는 권한을 부여합니다. Amazon ECS를 구성하여 Application Load Balancer(ALB)를 사용합니다. ALB를 사용하여 애플리케이션과 상호 작용합니다.
B. 애플리케이션 코드를 AWS Lambda에서 실행되는 컨테이너로 마이그레이션합니다. Lambda 통합을 통해 Amazon API Gateway REST API를 구축하세요. API 게이트웨이를 사용하여 애플리케이션과 상호 작용합니다.
C. AWS App2Container를 사용하여 EKS 관리형 노드 그룹의 Amazon Elastic Kubernetes Service(Amazon EKS)로 애플리케이션을 마이그레이션합니다. Amazon Elastic Container Registry(Amazon ECR)에 컨테이너 이미지를 저장합니다. ECR 이미지 저장소에 액세스할 수 있는 권한을 EKS 노드에 부여하십시오. Amazon API Gateway를 사용하여 애플리케이션과 상호 작용합니다.
D. 애플리케이션 코드를 AWS Lambda에서 실행되는 컨테이너로 마이그레이션합니다. Application Load Balancer(ALB)를 사용하도록 Lambda를 구성합니다. ALB를 사용하여 애플리케이션과 상호작용합니다.

해설
정답:A
AWS App2Container를 사용하여 애플리케이션을 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)로 마이그레이션하고
Amazon Elastic Container Registry(Amazon ECR)에 컨테이너 이미지를 저장하면 코드 변경과 필요한 관리 오버헤드가 최소화됩니다.
B(x): 애플리케이션 코드를 AWS Lambda에서 실행되는 컨테이너로 마이그레이션해야 하며, 이를 위해서는 더 많은 코드 변경이 필요합니다.
C(x): 더 많은 관리 오버헤드가 필요한 Amazon Elastic Kubernetes Service(Amazon EKS)로 애플리케이션을 마이그레이션해야 합니다.
D(x): Lambda의 기본 기능이 아닌 ALB(Application Load Balancer)를 사용하도록 Lambda를 구성해야 합니다.

◆ | **Q#0107.** | **Ref#0107.**
회사에는 AWS Lambda 함수로 호스팅되는 비동기 HTTP 애플리케이션이 있습니다. 퍼블릭 Amazon API Gateway 엔드포인트는 Lambda 함수를 호출합니다. Lambda 함수와 API 게이트웨이 엔드포인트는 us-east-1 리전에 있습니다. 솔루션 아키텍트는 다른 AWS 리전으로의 장애 조치를 지원하도록 애플리케이션을 재설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. us-west-2 지역에 API 게이트웨이 엔드포인트를 생성하여 us-east-1의 Lambda 함수로 트래픽을 보냅니다. 장애 조치 라우팅 정책을 사용하여 두 개의 API 게이트웨이 엔드포인트에 대한 트래픽을 라우팅하도록 Amazon Route 53을 구성합니다.

B. Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. Lambda 함수 대신 SQS 대기열로 트래픽을 전달하도록 API 게이트웨이를 구성합니다. 처리를 위해 대기열에서 메시지를 가져오도록 Lambda 함수를 구성합니다.
C. us-west-2 지역에 Lambda 함수를 배포합니다. us-west-2에 API Gateway 엔드포인트를 생성하여 us-west-2의 Lambda 함수로 트래픽을 보냅니다. 두 개의 API 게이트웨이 엔드포인트에서 트래픽을 관리하도록 AWS Global Accelerator와 Application Load Balancer를 구성합니다.
D. us-west-2 지역에 Lambda 함수와 API 게이트웨이 엔드포인트를 배포합니다. 장애 조치 라우팅 정책을 사용하여 두 개의 API 게이트웨이 엔드포인트에 대한 트래픽을 라우팅하도록 Amazon Route 53을 구성합니다.

해설
정답: D
Lambda 함수와 API Gateway 엔드포인트를 us-west-2 리전에 배포합니다.
Amazon Route 53을 구성하여 두 API Gateway 엔드포인트에 대한 트래픽을 라우팅하기 위해 장애 조치 라우팅 정책을 사용합니다.
이 솔루션은 Lambda 함수와 API Gateway 엔드포인트를 추가적인 리전에 배포하고, Route 53을 사용하여 두 리전 간의 트래픽을 라우팅하여 한 리전에서 문제가 발생할 경우 자동으로 다른 리전으로 트래픽을 전환할 수 있습니다. 이는 높은 가용성을 보장하고 장애에 대한 대응력을 강화합니다.

◆ | **Q#0108.** | **Ref#0108.**
한 소매 회사가 AWS 계정을 AWS Organizations 조직의 일부로 구성했습니다. 회사는 통합 청구를 설정하고 부서를 재무, 영업, 인사(HR), 마케팅 및 운영 OU에 매핑했습니다. 각 OU에는 부서 내 환경마다 하나씩 여러 개의 AWS 계정이 있습니다. 이러한 환경은 개발, 테스트, 사전 프로덕션 및 프로덕션입니다.

HR 부서에서는 3개월 후에 출시될 새로운 시스템을 출시할 예정입니다. 준비 과정에서 HR 부서는 프로덕션 AWS 계정에서 여러 예약 인스턴스(RI)를 구입했습니다. HR 부서에서는 이 계정에 새 애플리케이션을 설치합니다. HR 부서에서는 다른 부서가 RI 할인을 공유할 수 없도록 하려고 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. HR 부서 프로덕션 계정의 AWS Billing and Cost Management 콘솔에서 RI 공유를 끕니다.
B. 조직에서 HR 부서의 프로덕션 AWS 계정을 제거합니다. 통합 청구 구성에만 계정을 추가합니다.
C. AWS Billing and Cost Management 콘솔에서 조직의 관리 계정을 사용하여 HR 부서 프로덕션 AWS 계정에 대한 RI 공유를 끕니다.
D. 조직 내에 SCP를 생성하여 RI에 대한 접근을 제한합니다. SCP를 다른 부서의 OU에 적용합니다.

해설
정답: C
AWS는 조직 내 모든 계정이 RI 할인 혜택을 공유할 수 있도록 허용합니다.
이는 통합 청구(consolidated billing)를 통해 구매한 RI를 최대한 활용하고 비용을 절감하는 데 도움이 됩니다.
관리 계정을 통해 RI 공유 설정을 조정하면 특정 계정에 대한 RI 할인 혜택의 공유를 제어할 수 있습니다.
이 방법은 HR 부서의 생산 계정에 대한 RI 할인 혜택이 다른 부서와 공유되지 않도록 하는 데 효과적입니다.

◆ | **Q#0109.** | **Ref#0109.**
한 대기업에서 인기 있는 웹 애플리케이션을 실행하고 있습니다. 애플리케이션은 프라이빗 서브넷의 Auto Scaling 그룹에 있는 여러 Amazon EC2 Linux 인스턴스에서 실행됩니다. Application Load Balancer는 프라이빗 서브넷의 Auto Scaling 그룹에 있는 인스턴스를 대상으로 합니다. AWS Systems Manager Session Manager가 구성되었으며 AWS Systems Manager 에이전트가 모든 EC2 인스턴스에서 실행되고 있습니다.

회사는 최근 새로운 버전의 애플리케이션을 출시했습니다. 일부 EC2 인스턴스가 현재 비정상으로 표시되어 종료되고 있습니다. 결과적으로 애플리케이션은 감소된 용량으로 실행됩니다. 솔루션 설계자는 애플리케이션에서 수집된 Amazon CloudWatch 로그를 분석하여 근본 원인을 파악하려고 시도하지만 로그로는 결론을 내리지 못합니다.

문제를 해결하려면 솔루션 설계자가 EC2 인스턴스에 어떻게 액세스해야 합니까?

> **A.** Auto Scaling 그룹의 HealthCheck 조정 프로세스를 일시 중단합니다. 비정상으로 표시된 인스턴스에 로그인하려면 세션 관리자를 사용하십시오.
> **B.** EC2 인스턴스 종료 보호를 활성화합니다. 비정상으로 표시된 인스턴스에 로그인하려면 세션 관리자를 사용하십시오.
> **C.** Auto Scaling 그룹의 종료 정책을 OldestInstance로 설정합니다. 비정상으로 표시된 인스턴스에 로그인하려면 세션 관리자를 사용하십시오.
> **D.** Auto Scaling 그룹의 종료 프로세스를 일시 중단합니다. 비정상으로 표시된 인스턴스에 로그인하려면 세션 관리자를 사용하십시오.
>
> 해설
> 정답:D
> D: Auto Scaling 그룹의 Terminate 프로세스를 일시 중지하면 Auto Scaling이 비정상 상태로 표시된 인스턴스를 즉시 종료하지 않도록 할 수 있습니다.
> 이렇게 하면 비정상 상태의 인스턴스에 Session Manager를 통해 접근하여 문제를 직접 진단하고 해결할 수 있습니다.
> Auto Scaling 그룹의 Terminate 프로세스를 일시 중지함으로써 인스턴스가 자동으로 종료되지 않게 하고,
> Session Manager를 사용하여 인스턴스에 로그인하여 문제를 분석할 수 있습니다.

◆ | **Q#0110.** | **Ref#0110.**
한 회사에서 여러 AWS 계정에 걸쳐 AWS WAF 규칙을 관리하기 위해 AWS WAF 솔루션을 배포하려고 합니다. 계정은 AWS Organizations의 다양한 OU에서 관리됩니다.

관리자는 필요에 따라 관리형 AWS WAF 규칙 세트에서 계정이나 OU를 추가하거나 제거할 수 있어야 합니다. 또한 관리자는 모든 계정에서 규정을 준수하지 않는 AWS WAF 규칙을 자동으로 업데이트하고 해결할 수 있는 능력도 있어야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** AWS Firewall Manager를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리하십시오. AWS Systems Manager Parameter Store 매개변수를 사용하여 관리할 계정 번호와 OU를 저장합니다. 계정이나 OU를 추가하거나 제거하려면 필요에 따라 매개변수를 업데이트하세요. Amazon EventBridge 규칙을 사용하여 매개변수에 대한 변경 사항을 식별하고 AWS Lambda 함수를 호출하여 Firewall Manager 관리 계정의 보안 정책을 업데이트합니다.
> **B.** 선택한 OU의 모든 리소스가 AWS WAF 규칙을 연결하도록 요구하는 조직 전체에 AWS Config 규칙을 배포합니다. AWS Lambda를 사용하여 자동화된 수정 작업을 배포하여 규정을 준수하지 않는 리소스를 수정합니다. AWS Config 규칙이 적용되는 동일한 OU를 대상으로 하는 AWS CloudFormation 스택 세트를 사용하여 AWS WAF 규칙을 배포합니다.
> **C.** 조직의 마스터 계정에 AWS WAF 규칙을 생성합니다. AWS Lambda 환경 변수를 사용하여 관리할 계정 번호와 OU를 저장합니다. 계정이나 OU를 추가하거나 제거하려면 필요에 따라 환경 변수를 업데이트하세요. 회원 계정에서 교차 계정 IAM 역할을 생성합니다. Lambda 함수에서 AWS Security Token Service(AWS STS)를 사용하여 역할을 맡아 멤버 계정에서 AWS WAF 규칙을 생성하고 업데이트합니다.
> **D.** AWS Control Tower를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리합니다. AWS Key Management Service(AWS KMS)를 사용하여 관리할 계정 번호와 OU를 저장합니다. 계정이나 OU를

추가하거나 제거하려면 필요에 따라 AWS KMS를 업데이트하세요. 회원 계정에 IAM 사용자를 생성합니다. 허용 AWS Control Tower 마스터 계정 액세스 키 및 보안 액세스 키를 사용하여 회원 계정에서 AWS WAF 규칙을 생성하고 업데이트합니다.

해설
정답:A
AWS Firewall Manager는 여러 AWS 계정에서 AWS WAF 규칙을 중앙에서 관리할 수 있는 서비스입니다.
AWS Systems Manager Parameter Store를 사용하여 계정 번호와 OU를 관리하고 필요에 따라 업데이트할 수 있습니다.
Amazon EventBridge 규칙을 사용하여 파라미터 변경을 감지하고 AWS Lambda를 호출하여 Firewall Manager의 보안 정책을 업데이트하는 방식은 자동화된 관리와 비준수 수정 기능을 제공하며, 운영 오버헤드를 최소화할 수 있습니다.

111 (박지수) 3회차 完

◆ | **Q#0111.** | **Ref#0111.**
솔루션 아키텍트는 회사의 보안 설정 또는 AWS Lambda 기능을 감사하고 있습니다. Lambda 함수는 Amazon Aurora 데이터베이스에서 최신 변경 사항을 검색합니다. Lambda 함수와 데이터베이스는 동일한 VPC에서 실행됩니다. Lambda 환경 변수는 Lambda 함수에 데이터베이스 자격 증명을 제공합니다.

Lambda 함수는 데이터를 집계하고 AWS KMS 관리형 암호화 키(SSE-KMS)를 사용한 서버 측 암호화용으로 구성된 Amazon S3 버킷에서 데이터를 사용할 수 있도록 합니다. 데이터는 인터넷을 통해 이동해서는 안 됩니다. 데이터베이스 자격 증명이 손상되면 회사에는 손상의 영향을 최소화하는 솔루션이 필요합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 권장해야 합니까?

A. Aurora DB 클러스터에서 IAM 데이터베이스 인증을 활성화합니다. IAM 데이터베이스 인증을 사용하여 함수가 데이터베이스에 액세스할 수 있도록 Lambda 함수에 대한 IAM 역할을 변경합니다. VPC에 Amazon S3용 게이트웨이 VPC 엔드포인트를 배포합니다.
B. Aurora DB 클러스터에서 IAM 데이터베이스 인증을 활성화합니다. IAM 데이터베이스 인증을 사용하여 함수가 데이터베이스에 액세스할 수 있도록 Lambda 함수에 대한 IAM 역할을 변경합니다. 데이터 전송 중 Amazon S3 연결에 HTTPS를 적용합니다.
C. AWS Systems Manager Parameter Store에 데이터베이스 자격 증명을 저장합니다. Parameter Store의 자격 증명에 대한 암호 교체를 설정합니다. 함수가 Parameter Store에 액세스할 수 있도록 Lambda 함수의 IAM 역할을 변경합니다. Parameter Store에서 자격 증명을 검색하도록 Lambda 함수를 수정합니다. VPC에 Amazon S3용 게이트웨이 VPC 엔드포인트를 배포합니다.
D. AWS Secrets Manager에 데이터베이스 자격 증명을 저장합니다. Secrets Manager에서 자격 증명에 대한 비밀번호 교체를 설정합니다. 함수가 Secrets Manager에 액세스할 수 있도록 Lambda 함수의 IAM 역할을 변경합니다. Secrets Manager에서 자격 증명을 검색하도록 Lambda 함수를 수정합니다. 데이터 전송 중 Amazon S3 연결에 HTTPS를 적용합니다.

해설
정답: A
Aurora DB 클러스터에 대한 IAM 데이터베이스 인증을 통해 데이터베이스에 대한 액세스를 중앙 집중식으로 안전하게 관리할 수 있으며 데이터베이스에 사용자 자격 증명을 저장할 필요가 없습니다.
Lambda 함수에 대한 IAM 역할을 변경하면 IAM 데이터베이스 인증을 통해 데이터베이스에 안전하게 액세스할 수 있습니다.
Amazon S3용 게이트웨이 VPC 엔드포인트를 배포하면 데이터가 인터넷을 통해 이동하지 않고 VPC 보안으로 보호됩니다.

◆ | **Q#0112.** | **Ref#0112.**
대규모 모바일 게임 회사는 모든 온프레미스 인프라를 AWS 클라우드로 성공적으로 마이그레이션했습니다. 솔루션 설계자는 환경이 설계에 따라 구축되었는지, Well-Architected 프레임워크에 맞춰 실행되는지 확인하기 위해 환경을 검토하고 있습니다.

비용 탐색기에서 이전 월별 비용을 검토하는 동안 솔루션 설계자는 여러 대규모 인스턴스 유형의 생성 및 후속 종료가 비용의 높은 부분을 차지한다는 사실을 발견했습니다. 솔루션 설계자는 회사 개발자가 테스트의 일부로 새로운 Amazon EC2 인스턴스를 시작하고 있으며 개발자가 적절한 인스턴스 유형을 사용하고 있지 않다는 사실을 발견했습니다.

솔루션 아키텍트는 개발자만 시작할 수 있는 인스턴스 유형을 제한하는 제어 메커니즘을 구현해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** AWS Config에서 원하는 인스턴스 유형 관리형 규칙을 생성합니다. 허용되는 인스턴스 유형으로 규칙을 구성합니다. 새 EC2 인스턴스가 시작될 때마다 실행되도록 이벤트에 규칙을 연결합니다.
> **B.** EC2 콘솔에서 허용되는 인스턴스 유형을 지정하는 시작 템플릿을 생성합니다. 개발자의 IAM 계정에 시작 템플릿을 할당합니다.
> **C.** 새로운 IAM 정책을 생성합니다. 허용되는 인스턴스 유형을 지정합니다. 개발자용 IAM 계정이 포함된 IAM 그룹에 정책을 연결합니다.
> **D.** EC2 이미지 빌더를 사용하여 개발자를 위한 이미지 파이프라인을 생성하고 골든 이미지 생성을 지원합니다.
>
> 해설
> 정답: C
> 허용되는 인스턴스 유형을 지정하는 새로운 IAM 정책을 생성하고 개발자의 IAM 계정이 포함된 IAM 그룹에 연결하면, 개발자가 지정된 유형의 인스턴스만 시작할 수 있으므로 대규모 인스턴스 생성 및 종료와 관련된 비용을 제한할 수 있다.

◆ | **Q#0113.** | **Ref#0113.**
한 회사가 AWS 클라우드에서 여러 프로젝트를 개발하고 호스팅하고 있습니다. 프로젝트는 AWS Organizations의 동일한 조직에 속한 여러 AWS 계정에 걸쳐 개발됩니다. 회사는 클라우드 인프라 비용을 소유 프로젝트에 할당해야 합니다. 모든 AWS 계정을 담당하는 팀은 여러 Amazon EC2 인스턴스에 비용 할당에 사용되는 프로젝트 태그가 부족하다는 사실을 발견했습니다.

문제를 해결하고 향후 이러한 문제가 발생하지 않도록 방지하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까? (3개를 선택하세요.)

> **A.** 각 계정에 AWS Config 규칙을 생성하여 태그가 누락된 리소스를 찾으십시오.
> **B.** 프로젝트 태그가 누락된 경우 ec2:RunInstances에 대한 거부 작업을 사용하여 조직에 SCP를 생성합니다.
> **C.** 조직에서 Amazon Inspector를 사용하여 태그가 누락된 리소스를 찾습니다.
> **D.** 프로젝트 태그가 누락된 경우 ec2:RunInstances에 대한 거부 작업을 사용하여 각 계정에 IAM 정책을 생성합니다.
> **E.** 조직이 프로젝트 태그가 누락된 EC2 인스턴스 목록을 수집할 수 있도록 AWS Config 수집기를 생성합니다.
> **F.** AWS Security Hub를 사용하여 프로젝트 태그가 누락된 EC2 인스턴스 목록을 집계합니다.
>
> 해설
> 정답: A,B,E
> A. AWS Config는 AWS 리소스의 구성을 평가하고 특정 태그 누락과 같이 지정된 요구 사항을 준수하지 않는 리소스를 식별할 수 있습니다. 이는 문제가 있는 기존 리소스를 식별하는 데 도움이 됩니

다.
B. SCP(서비스 제어 정책)는 조직의 모든 계정에 권한을 적용할 수 있습니다. 필수 프로젝트 태그 없이 EC2 인스턴스 시작을 거부하는 SCP를 생성하면 향후 조직 수준에서 문제가 발생하는 것을 방지할 수 있습니다.
E. AWS Config 수집기는 여러 계정 및 지역에서 규정 준수 데이터를 집계할 수 있습니다. 이를 통해 필수 태그가 부족한 인스턴스를 중앙 집중식으로 볼 수 있으므로 조직 전체에서 문제를 더 쉽게 해결하고 관리할 수 있습니다.

◆ | **Q#0114.** | **Ref#0114.**
회사에는 이벤트 지속성을 위해 PostgreSQL 데이터베이스를 사용하는 온프레미스 모니터링 솔루션이 있습니다. 과도한 수집으로 인해 데이터베이스를 확장할 수 없으며 스토리지가 부족해지는 경우가 많습니다.

회사는 하이브리드 솔루션을 만들고 싶어하며 이미 네트워크와 AWS 간에 VPN 연결을 설정했습니다. 솔루션에는 다음 속성이 포함되어야 합니다.
• 운영 복잡성을 최소화하는 관리형 AWS 서비스.
• 데이터 처리량에 맞춰 자동으로 확장되며 지속적인 관리가 필요 없는 버퍼입니다.
• 거의 실시간으로 이벤트를 관찰하기 위한 대시보드를 생성하는 시각화 도구입니다.
• 반구조화된 JSON 데이터 및 동적 스키마를 지원합니다.

회사에서 이러한 요구 사항을 충족하는 모니터링 솔루션을 만들 수 있는 구성 요소 조합은 무엇입니까? (2개를 선택하세요.)

A. Amazon Kinesis Data Firehose를 사용하여 이벤트를 버퍼링하세요. 이벤트를 처리하고 변환하는 AWS Lambda 함수를 생성합니다.
B. 이벤트를 버퍼링하기 위해 Amazon Kinesis 데이터 스트림을 생성합니다. 이벤트를 처리하고 변환하는 AWS Lambda 함수를 생성합니다.
C. 이벤트를 수신하도록 Amazon Aurora PostgreSQL DB 클러스터를 구성합니다. Amazon QuickSight를 사용하여 데이터베이스에서 읽고 거의 실시간 시각화 및 대시보드를 생성합니다.
D. 이벤트를 수신하도록 Amazon Elasticsearch Service(Amazon ES)를 구성합니다. Amazon ES와 함께 배포된 Kibana 엔드포인트를 사용하여 거의 실시간 시각화 및 대시보드를 생성합니다.
E. 이벤트를 수신하도록 Amazon Neptune DB 인스턴스를 구성합니다. Amazon QuickSight를 사용하여 데이터베이스에서 읽고 거의 실시간 시각화 및 대시보드를 생성합니다.

해설
정답: A,D
A. Amazon Kinesis Data Firehose는 스트리밍 데이터를 Amazon S3, Amazon Redshift, Amazon Elasticsearch Service 및 Splunk와 같은 AWS 서비스에 손쉽게 로드하기 위한 완전관리형 서비스를 제공합니다. 데이터 처리량에 맞춰 자동으로 확장되며 지속적인 관리가 필요하지 않습니다. AWS Lambda를 Kinesis Data Firehose와 함께 사용하면 데이터가 대상에 로드되기 전에 데이터를 처리하고 변환하여 동적 스키마와 반구조화된 JSON 데이터를 지원할 수 있습니다. 또한 Amazon Kinesis Data Firehose에는 버퍼링 기능이 내장되어 있으며 거의 실시간으로 이벤트를 관찰하는 데 사용할 수 있으므로 특정 시나리오에 더 적합한 선택입니다.
D. Amazon Elasticsearch Service(Amazon ES)는 Elasticsearch를 쉽게 배포, 보호, 운영 및 확장하여 실시간으로 데이터를 검색, 분석 및 시각화할 수 있게 해주는 관리형 서비스입니다. Kibana는 Elasticsearch와 함께 작동하도록 설계된 오픈 소스 시각화 도구로, 거의 실시간으로 데이터를 시각화할 수 있는 대시보드를 생성할 수 있는 강력하고 사용하기 쉬운 기능을 제공합니다.

◆ | **Q#0115.** | **Ref#0115.**
팀은 회사 전체의 행동 데이터를 수집하고 전달합니다. 이 회사는 퍼블릭 서브넷, 프라이빗 서브넷 및 인터넷 게이트웨이를 갖춘 다중 AZ VPC 환경을 실행합니다. 각 퍼블릭 서브넷에는 NAT 게이트웨이도 포함되어 있습니다. 대부분의 회사 애플리케이션은 Amazon Kinesis Data Streams에서 읽고 씁니다. 대부분의 워크로드는 프라이빗 서브넷에서 실행됩니다.

솔루션 설계자는 인프라를 검토해야 합니다. 솔루션 설계자는 비용을 절감하고 애플리케이션의 기능을 유지해야 합니다. 솔루션 설계자는 Cost Explorer를 사용하여 EC2-기타 범주의 비용이 지속적으로 높다는 사실을 확인합니다. 추가 검토에 따르면 NatGateway-Bytes 요금으로 인해 EC2-기타 범주의 비용이 증가하는 것으로 나타났습니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** VPC 흐름 로그를 활성화합니다. Amazon Athena를 사용하여 제거할 수 있는 트래픽에 대한 로그를 분석합니다. 보안 그룹이 높은 비용을 초래하는 트래픽을 차단하고 있는지 확인하십시오.
> **B.** Kinesis Data Streams용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. 애플리케이션에 인터페이스 VPC 엔드포인트를 사용할 수 있는 올바른 IAM 권한이 있는지 확인하십시오.
> **C.** VPC 흐름 로그 및 Amazon Detective를 활성화합니다. Kinesis Data Streams와 관련되지 않은 트래픽에 대한 탐지 결과를 검토합니다. 해당 트래픽을 차단하도록 보안 그룹을 구성하십시오.
> **D.** Kinesis Data Streams용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. VPC 엔드포인트 정책이 애플리케이션의 트래픽을 허용하는지 확인하십시오.
>
> 해설
> 정답: D
> Kinesis Data Streams용 인터페이스 VPC 엔드포인트를 VPC에 추가하면 NAT 게이트웨이 없이도 애플리케이션이 서비스에 액세스할 수 있습니다. 이렇게하면 EC2-기타 범주의 비용을 증가시키는 NatGateway-Bytes 요금과 관련된 비용이 줄어듭니다.
> 엔드포인트를 통해 서비스를 사용하는 데는 IAM 권한이 필요하지 않습니다. 해당 엔드포인트에 대한 적절한 라우팅만 설정하면 됩니다.

◆ | **Q#0116.** | **Ref#0116.**
한 소매 회사가 유럽에 온프레미스 데이터 센터를 보유하고 있습니다. 또한 이 회사는 eu-west-1 및 us-east-1 지역을 포함하는 다중 리전 AWS를 보유하고 있습니다. 회사는 온프레미스 인프라에서 해당 리전 중 하나의 VPC로 네트워크 트래픽을 라우팅할 수 있기를 원합니다. 또한 회사는 해당 리전의 VPC 간에 직접 라우팅되는 트래픽을 지원해야 합니다. 네트워크에는 단일 실패 지점이 존재할 수 없습니다.

이 회사는 이미 온프레미스 데이터 센터에서 2개의 1Gbps AWS Direct Connect 연결을 생성했습니다. 고가용성을 위해 각 연결은 유럽의 별도 Direct Connect 위치로 이동됩니다. 이 두 위치의 이름은 각각 DX-A 및 DX-B입니다. 각 리전에는 해당 리전 내의 모든 VPC 간 트래픽을 라우팅하도록 구성된 단일 AWS Transit Gateway가 있습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** DX-A 연결에서 Direct Connect 게이트웨이로 프라이빗 VIF를 생성합니다. 고가용성을 위해 DX-B 연결에서 동일한 Direct Connect 게이트웨이로 프라이빗 VIF를 생성합니다. eu-west-1 및 us-east-1 전송 게이트웨이를 모두 Direct Connect 게이트웨이와 연결합니다. 지역 간 라우팅을 지원하려면 전송 게이트웨이를 서로 피어링하세요.
> **B.** DX-A 연결에서 Direct Connect 게이트웨이로의 전송 VIF를 생성합니다. eu-west-1 전송 게이트웨이를 이 Direct Connect 게이트웨이와 연결합니다. DX-B 연결에서 별도의 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. us-east-1 전송 게이트웨이를 이 별도의 Direct Connect 게이트웨이와 연결합니다. 고가용성 및 지역 간 라우팅을 지원하려면 Direct Connect 게이트웨이를 서로 피어링하세요.
> **C.** DX-A 연결에서 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. 고가용성을 위해 DX-B 연결에서 동일한 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. eu-west-1 및 us-east-1 전송 게이트웨이를 모두 이 Direct Connect 게이트웨이와 연결합니다. 전송 게이트웨이 간에 트래픽을 라우팅하도록 Direct Connect 게이트웨이를 구성합니다.
> **D.** DX-A 연결에서 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. 고가용성을 위해 DX-B 연결에서 동일한 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. eu-west-1 및 us-east-1 전송

게이트웨이를 모두 이 Direct Connect 게이트웨이와 연결합니다. 지역 간 라우팅을 지원하려면 전송 게이트웨이를 서로 피어링하세요.

해설
정답: D
Transit 게이트웨이에 연결하려면 Transit VIF가 필요하고, 지역 간 라우팅을 허용하려면 Transit 게이트웨이 피어링이 필요하다.

AWS Direct Connect + AWS Transit Gateway
AWS DX – DXGW with AWS Transit Gateway, Multi-Regions, and AWS Public Peering

◆ | **Q#0117.** | **Ref#0117.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 회사의 보안 팀은 모든 신규 IAM 사용자 생성을 승인해야 합니다. 새로운 IAM 사용자가 생성되면 해당 사용자에 대한 모든 액세스 권한이 자동으로 제거되어야 합니다. 그런 다음 보안 팀은 사용자를 승인하라는 알림을 받아야 합니다. 회사는 AWS 계정에 다중 리전 AWS CloudTrail 추적을 보유하고 있습니다.

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

A. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 생성합니다. CloudTrail을 통한 AWS API 호출로 설정된 세부 유형 값과 CreateUser의 eventName을 사용하여 패턴을 정의합니다.
B. CreateUser 이벤트에 대한 알림을 Amazon SNS(Amazon SNS) 주제로 보내도록 CloudTrail을 구성합니다.
C. AWS Fargate 기술을 사용하여 Amazon Elastic Container Service(Amazon ECS)에서 실행되는 컨테이너를 호출하여 액세스를 제거합니다.
D. AWS Step Functions 상태 시스템을 호출하여 액세스를 제거합니다.
E. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 보안팀에 알립니다.
F. Amazon Pinpoint를 사용하여 보안 팀에 알립니다.

해설
정답: A,D,E
A: 첫 번째 단계는 CreateUser 이벤트를 감지하도록 EventBridge 규칙을 생성하는 것입니다.
D: 다음 단계는 AWS Step Functions 상태 시스템을 사용하여 새 IAM 사용자에 대한 액세스 권한을 제거하는 것입니다. 이렇게 하면 보안 팀의 요구에 따라 액세스 권한이 자동으로 제거됩니다.
E: 마지막으로 Amazon SNS를 사용하여 새 사용자가 생성되었고 액세스 권한이 제거되었음을 보안 팀에 알립니다.

◆ | **Q#0118.** | **Ref#0118.**
회사에서 AWS로 마이그레이션하려고 합니다. 회사는 모든 계정과 애플리케이션에 대한 액세스를 중앙에서 관리하는 다중 계정 구조를 사용하려고 합니다. 또한 회사는 트래픽을 개인 네트워크에 유지하려고 합니다. 로그인 시 MFA(Multi-Factor Authentication)가 필요하며, 사용자 그룹에는 특정 역할이 할당됩니다.

회사는 개발을 위해 별도의 계정을 만들어야 합니다. 스테이징, 프로덕션 및 공유 네트워크. 프로덕션 계정과 공유 네트워크 계정은 모든 계정에 연결되어 있어야 합니다. 개발 계정과 스테이징 계정은 서로에게만 액세스할 수 있어야 합니다.

솔루션 설계자가 이러한 요구 사항을 충족하려면 어떤 단계 조합을 거쳐야 합니까? (3개를 선택하세요.)

A. AWS Control Tower를 사용하여 랜딩 존 환경을 배포합니다. 계정을 등록하고 기존 계정을 AWS Organizations의 결과 조직에 초대합니다.
B. 모든 계정에서 AWS Security Hub를 활성화하여 교차 계정 액세스를 관리합니다. AWS CloudTrail을 통해 결과를 수집하여 MFA 로그인을 강제합니다.
C. 각 계정에 전송 게이트웨이 및 전송 게이트웨이 VPC 연결을 생성합니다. 적절한 라우팅 테이블을 구성합니다.

D. AWS IAM Identity Center(AWS Single Sign-On)를 설정하고 활성화합니다. 기존 계정에 필요한 MFA를 사용하여 적절한 권한 집합을 만듭니다.
E. 모든 계정에서 AWS Control Tower를 활성화하여 계정 간 라우팅을 관리합니다. AWS CloudTrail을 통해 결과를 수집하여 MFA 로그인을 강제합니다.
F. IAM 사용자 및 그룹을 생성합니다. 모든 사용자에 대해 MFA를 구성합니다. Amazon Cognoto 사용자 풀과 자격 증명 풀을 설정하여 계정에 대한 액세스 및 계정 간 액세스를 관리합니다.

해설
정답: A,C,D
A: AWS Control Tower를 사용하여 랜딩 존 환경을 배포하고 AWS Organizations의 조직에 계정을 등록하면 모든 계정과 애플리케이션에 대한 액세스를 중앙 집중식으로 관리할 수 있습니다.
C: 각 계정에 전송 게이트웨이 및 전송 게이트웨이 VPC 연결을 생성하고 적절한 라우팅 테이블을 구성하면 프라이빗 네트워크 트래픽이 허용되고, 프로덕션 계정과 공유 네트워크 계정이 모든 계정에 연결되는 반면 개발 및 스테이징 계정은 서로에게만 액세스할 수 있습니다.
D: AWS IAM Identity Center(AWS Single Sign-On)를 설정 및 활성화하고 기존 계정에 필요한 MFA를 사용하여 적절한 권한 세트를 생성하면 로그인 시 다단계 인증이 가능하고 특정 역할을 사용자 그룹에 할당할 수 있습니다.
AWS IAM Identity Center는 중앙 집중식 인증 및 권한 관리를 제공하며, MFA를 포함하여 특정 사용자 그룹에 적합한 권한을 할당할 수 있습니다. 이를 통해 여러 계정에 대한 중앙 관리 접근을 효과적으로 설정할 수 있습니다.

◆ | **Q#0119.** | **Ref#0119.**
회사는 eu-west-1 지역에서 애플리케이션을 실행하고 개발, 테스트, 프로덕션 등 각 환경에 대해 하나의 계정을 갖습니다. 모든 환경은 상태 저장 Amazon EC2 인스턴스와 MySQL용 Amazon RDS 데이터베이스를 사용하여 연중무휴 24시간 실행됩니다. 데이터베이스 크기는 500GB에서 800GB 사이입니다.

개발팀과 테스트팀은 업무시간 중 영업일에 근무하지만, 프로덕션 환경은 연중무휴 24시간 운영됩니다. 회사는 비용을 절감하고 싶어합니다. 모든 리소스에는 개발, 테스트 또는 프로덕션을 핵심으로 하는 환경 태그가 지정됩니다.

최소한의 운영 노력으로 비용을 절감하려면 솔루션 설계자가 무엇을 해야 합니까?

A. 매일 한 번 실행되는 Amazon EventBridge 규칙을 만듭니다. 태그, 요일, 시간에 따라 인스턴스를 시작하거나 중지하는 AWS Lambda 함수 하나를 호출하도록 규칙을 구성합니다.
B. 매일 저녁에 실행되는 Amazon EventBridge 규칙을 만듭니다. 태그를 기반으로 인스턴스를 중지하는 AWS Lambda 함수를 호출하도록 규칙을 구성합니다. 매일 아침에 실행되는 두 번째 EventBridge 규칙을 생성합니다. 두 번째 규칙을 구성하여 태그를 기반으로 인스턴스를 시작하는 다른 Lambda 함수를 호출합니다.
C. 매일 저녁에 실행되는 Amazon EventBridge 규칙을 생성하고, 지연을 기반으로 인스턴스를 종료하는 AWS Lambda 함수를 호출하도록 규칙을 구성합니다. 매일 아침에 실행되는 두 번째 EventBridge 규칙을 생성합니다. 두 번째 규칙을 구성하면 태그를 기반으로 마지막 백업에서 인스턴스를 복원하는 다른 Lambda 함수를 호출합니다.
D. 매시간 실행되는 Amazon EventBridge 규칙을 생성합니다. 태그를 기반으로 마지막 백업에서 인스턴스를 종료하거나 복원하는 하나의 AWS Lambda 함수를 호출하도록 규칙을 구성합니다. 요일, 시간.

해설
정답: B
업무 외 시간에 사용하지 않는 인스턴스를 중지하고 아침에 다시 시작하도록 구현
매일 저녁 실행되는 EventBridge 규칙 생성, 태그 기반으로 인스턴스를 중지하는 Lambda 함수 호출
매일 아침 실행되는 EventBridge 규칙 생성, 태그 기반으로 인스턴스를 시작하는 Lambda 함수 호출

◆ | **Q#0120.** | **Ref#0120.**
한 회사가 AWS에서 SaaS(Software-as-a-Service) 솔루션을 구축하고 있습니다. 이 회사는 여러 AWS 지역과 동일한 프로덕션 계정에 AWS Lambda 통합을 통해 Amazon API Gateway REST API를 배포했습니다.

이 회사는 고객이 초당 특정 수의 API 호출을 수행할 수 있는 용량에 대해 비용을 지불할 수 있는 계층화된 가격을 제공합니다. 프리미엄 계층은 초당 최대 3,000개의 호출을 제공하며 고객은 고유한 API 키로 식별됩니다. 다양한 지역의 몇몇 프리미엄 등급 고객은 사용량이 가장 많은 시간 동안 여러 API 메서드로부터 429 요청이 너무 많다는 오류 응답을 받았다고 보고합니다. 로그에는 Lambda 함수가 호출되지 않았음을 나타냅니다.

이러한 고객에게 나타나는 오류 메시지의 원인은 무엇입니까?

> **A.** Lambda 함수가 동시성 제한에 도달했습니다.
> **B.** Lambda 함수의 동시성 지역 제한.
> **C.** 회사가 API Gateway 계정의 초당 호출 한도에 도달했습니다.
> **D.** 회사는 초당 호출에 대한 API 게이트웨이 기본 메서드별 제한에 도달했습니다.
>
> 해설
> 정답: C
> "429 Too Many Request" 에러는 초당 API 호출이 초과되었음을 나타냅니다.
> API Gateway에는 계정당, 리전당 초당 10,000개의 요청 제한이 있습니다
> Amazon API Gateway quotas and important notes

121 (고민석) 3회차 完

◆ | **Q#0121.** | **Ref#0121.**
한 금융 회사가 웹 애플리케이션을 온프레미스에서 AWS로 마이그레이션할 계획입니다. 회사는 타사 보안 도구를 사용하여 애플리케이션에 대한 인바운드 트래픽을 모니터링합니다. 회사는 지난 15년 동안 보안 도구를 사용해 왔으며 이 도구에는 해당 공급업체에서 제공하는 클라우드 솔루션이 없습니다. 회사의 보안팀은 보안 도구를 AWS 기술과 통합하는 방법에 대해 고민하고 있습니다.

회사는 Amazon EC2 인스턴스를 통해 AWS로 애플리케이션 마이그레이션을 배포할 계획입니다. EC2 인스턴스는 전용 VPC의 Auto Scaling 그룹에서 실행됩니다. 회사는 보안 도구를 사용하여 VPC에 들어오고 나가는 모든 패킷을 검사해야 합니다. 이 검사는 실시간으로 이루어져야 하며 애플리케이션 성능에 영향을 주어서는 안 됩니다. 솔루션 아키텍트는 AWS 리전 내에서 가용성이 높은 AWS 대상 아키텍처를 설계해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

> **A.** 기존 VPC의 새로운 Auto Scaling 그룹에 EC2 인스턴스에 보안 도구를 배포합니다.
> **B.** Network Load Balancer 뒤에 웹 애플리케이션 배포
> **C.** 보안 도구 인스턴스 앞에 Application Load Balancer를 배포합니다.
> **D.** 각 가용 영역에 대해 게이트웨이 로드 밸런서를 프로비저닝하여 트래픽을 보안 도구로 리디렉션합니다.
> **E.** VPC 간 통신을 용이하게 하기 위해 전송 게이트웨이를 프로비저닝합니다.
>
> 해설
> 정답: D,E
> D: Gateway Load Balancer (GWLB)는 네트워크 트래픽을 특정 보안 장비로 리디렉션하기 위한 도구로, 보안 도구가 모든 패킷을 검사할 수 있도록 합니다. 이 선택은 요구 사항을 충족하는 데 적합합니다.
> A: 보안 도구를 기존 VPC 내의 EC2 인스턴스에 배포하고 Auto Scaling 그룹을 사용하여 필요에 따라 인스턴스를 확장함으로써, 트래픽 증가 시에도 높은 가용성을 유지할 수 있습니다. 이 두 가지 조합은 실시간 패킷 검사 요구 사항을 충족하면서 AWS 환경에서 높은 가용성을 유지할 수 있도록 도와

줍니다.
E: Transit Gateway는 여러 VPC 간의 네트워크 트래픽을 효율적으로 라우팅할 수 있는 서비스입니다. 이 문제의 시나리오에서는 VPC와 다른 네트워크 간의 트래픽을 보안 도구로 라우팅하기 위해 Transit Gateway를 활용할 수 있습니다. 이는 보안 도구가 여러 VPC에서 발생하는 트래픽을 모니터링할 수 있도록 도와줍니다.
A(x): 웹 애플리케이션이 전용 VPC에 있어야 하므로 A는 유효하지 않습니다.
웹 애플리케이션은 전용 VPC에 배포됩니다. 이는 보안 모니터링 도구가 웹 애플리케이션의 VPC 외부, 즉 다른 VPC에 배포되어야 함을 의미합니다.
보안 모니터링은 웹 애플리케이션의 성능에 영향을 주어서는 안 됩니다. 간단해야 합니다. 자연스러운 적합성은 Gateway Load Balancer를 사용하는 것입니다.
GWLB 및 TGW "EC2 인스턴스는 전용 VPC의 Auto Scaling 그룹에서 실행됩니다." 따라서 VPC가 두 개 이상 있습니다. 이는 옵션 A를 배제합니다. 또한 이는 VPC 간 통신(E)에 전송 게이트웨이가 필요하다는 의미이기도 합니다.

◆ | **Q#0122.** | **Ref#0122.**
한 회사가 여러 공급업체로부터 가전제품을 구입했습니다. 가전제품에는 모두 IoT 센서가 있습니다. 센서는 정보를 JSON으로 구문 분석하는 레거시 애플리케이션에 공급업체의 독점 형식으로 된 상태 정보를 보냅니다. 구문 분석은 간단하지만 각 공급업체마다 고유한 형식이 있습니다. 매일 한 번씩 애플리케이션은 모든 JSON 레코드를 구문 분석하고 분석을 위해 관계형 데이터베이스에 레코드를 저장합니다.

회사는 더 빠르게 제공하고 비용을 최적화할 수 있는 새로운 데이터 분석 솔루션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. IoT 센서를 AWS IoT Core에 연결합니다. AWS Lambda 함수를 호출하여 정보를 구문 분석하고 .csv 파일을 Amazon에 저장하는 규칙을 설정합니다. S3 AWS Glue를 사용하여 파일을 카탈로그화합니다. 분석에는 Amazon Athena 및 Amazon QuickSight를 사용하십시오.
B. IoT 센서로부터 정보를 수신하고 정보를 관계형 형식으로 구문 분석하는 AWS Fargate로 애플리케이션 서버를 마이그레이션합니다. 분석을 위해 구문 분석된 정보를 Amazon RedshIft에 저장합니다.
C. SFTP용 AWS 전송 서버를 생성합니다. IoT 센서 코드를 업데이트하여 정보를 SFTP를 통해 .csv 파일로 서버에 보냅니다. AWS Glue를 사용하여 파일을 카탈로그화합니다. 분석에는 Amazon Athena를 사용하세요.
D. AWS Snowball Edge를 사용하여 IoT 센서에서 직접 데이터를 수집하여 로컬 분석을 수행합니다. 정기적으로 데이터를 Amazon Redshift로 수집하여 글로벌 분석을 수행합니다.

해설
정답: A
이 문제는 IoT 센서로부터 데이터를 신속하게 수집하고 다양한 형식의 데이터를 효과적으로 변환하며, 빠른 데이터 분석을 가능하게 하는 솔루션을 구현해야 합니다.
A : AWS IoT Core는 대규모의 IoT 디바이스 네트워크를 안전하게 연결하고 관리하고 데이터를 수집하는 기능을 제공합니다.
AWS Lambda는 서버를 관리하지 않고도 코드를 실행할 수 있게 해주는 이벤트 중심의 서비스입니다.
마지막으로 Amazon Athena를 이용해서 S3에 저장된 데이터를 분석하고 Amazon QuickSight를 이용해서 그들의 데이터를 시각화하게 됩니다.
위의 기능으로 서버를 직접 관리하거나 유지보수할 필요가 없고 이로 인해 회사는 속도를 높이고 비용을 최적화하는 데에 초점을 맞출 수 있습니다.
C는 비용 및 복잡성 측면에서 문제를 야기할 수 있습니다. 각 IoT 센서의 코드를 업데이트 해야하고, SFTP 서버를 생성해야 합니다.

◆ | **Q#0123.** | **Ref#0123.**
한 회사가 일부 애플리케이션을 AWS로 마이그레이션하고 있습니다. 회사는 네트워킹 및 보안 전략을 확정한 후

신속하게 애플리케이션을 마이그레이션하고 현대화하기를 원합니다. 회사는 중앙 네트워크 계정에 AWS Direct Connect 연결을 설정했습니다.

회사는 가까운 시일 내에 수백 개의 AWS 계정과 VPC를 보유할 것으로 예상합니다. 기업 네트워크는 AWS의 리소스에 원활하게 액세스할 수 있어야 하며 모든 VPC와 통신할 수도 있어야 합니다. 또한 회사는 온프레미스 데이터 센터를 통해 클라우드 리소스를 인터넷으로 라우팅하려고 합니다.

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

> **A.** 중앙 계정에 Direct Connect 게이트웨이를 생성합니다. 각 계정에서 Direct Connect 게이트웨이와 모든 가상 프라이빗 게이트웨이의 계정 ID를 사용하여 연결 제안을 생성합니다.
> **B.** 중앙 네트워크 계정에 Direct Connect 게이트웨이와 전송 게이트웨이를 생성합니다. 전송 VIF를 사용하여 전송 게이트웨이를 Direct Connect 게이트웨이에 연결합니다.
> **C.** 인터넷 게이트웨이를 프로비저닝합니다. 인터넷 게이트웨이를 서브넷에 연결합니다. 게이트웨이를 통한 인터넷 트래픽을 허용합니다.
> **D.** Transit Gateway를 다른 계정과 공유합니다. Transit Gateway에 VPC를 연결합니다.
> **E.** 필요에 따라 VPC 피어링을 프로비저닝합니다.
> **F.** 프라이빗 서브넷만 프로비저닝합니다. AWS의 아웃바운드 인터넷 트래픽이 데이터 센터에서 실행되는 NAT 서비스를 통해 흐를 수 있도록 전송 게이트웨이 및 고객 게이트웨이에서 필요한 경로를 엽니다.
>
> 해설
> 정답: B,D,F
> B: Direct Connect 게이트웨이를 통해 여러 VPC와 온프레미스 네트워크 간의 연결을 중앙에서 관리할 수 있습니다. 트랜싯 게이트웨이를 Direct Connect 게이트웨이에 연결함으로써 수백 개의 계정과 VPC에 대해 확장 가능한 네트워크 구조를 설정할 수 있습니다.
> D: Transit 게이트웨이는 여러 계정과 VPC를 중앙에서 연결하고, 네트워크 트래픽을 관리할 수 있는 핵심 역할을 합니다. 이를 공유함으로써 모든 계정과 VPC 간의 통신을 원활하게 할 수 있습니다.
> F: 온프레미스 데이터 센터를 통해 모든 클라우드 리소스의 인터넷 트래픽을 라우팅하려면 프라이빗 서브넷을 사용하고, 트랜싯 게이트웨이와 고객 게이트웨이의 라우팅 테이블을 적절히 구성해야 합니다. 이를 통해 인터넷 트래픽이 온프레미스 네트워크를 경유하도록 설정할 수 있습니다.

◆ | Q#0124. | Ref#0124.
회사에는 수백 개의 AWS 계정이 있습니다. 회사는 최근 새로운 예약 인스턴스를 구매하고 기존 예약 인스턴스를 수정하기 위한 중앙 집중식 내부 프로세스를 구현했습니다. 이 프로세스에서는 예약 인스턴스를 구매하거나 수정하려는 모든 사업 단위가 조달을 위해 전담 팀에 요청을 제출해야 합니다. 이전에는 사업부가 각자의 AWS 계정에서 예약 인스턴스를 자율적으로 직접 구매하거나 수정했습니다.

솔루션 설계자는 가능한 가장 안전한 방식으로 새로운 프로세스를 시행해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

> **A.** 모든 AWS 계정이 모든 기능이 활성화된 AWS Organizations의 조직에 속해 있는지 확인하십시오.
> **B.** AWS Config를 사용하여 ec2:PurchaseReservedInstancesOffering 작업 및 ec2:ModifyReservedInstances 작업에 대한 액세스를 거부하는 IAM 정책 첨부를 보고합니다.
> **C.** 각 AWS 계정에서 ec2:PurchaseReservedInstancesOffering 작업과 ec2:ModifyReservedInstances 작업을 거부하는 IAM 정책을 생성합니다.
> **D.** ec2:PurchaseReservedInstancesOffering 작업 및 ec2:ModifyReservedInstances 작업을 거부하는 SCP를 생성합니다. SCP를 조직의 각 OU에 연결합니다.
> **E.** 모든 AWS 계정이 통합 결제 기능을 사용하는 AWS Organizations 조직의 일부인지 확인하십시오.
>
> 해설

정답:A,D
A: AWS Organizations를 사용하면 중앙에서 여러 AWS 계정을 관리할 수 있으며, 모든 기능을 활성화하면 서비스 제어 정책(SCP)과 같은 고급 관리 기능을 사용할 수 있습니다. 이 기능을 통해 여러 계정에서 일관된 보안 정책을 강제로 적용할 수 있습니다.
D: 서비스 제어 정책(SCP)은 조직 내 모든 계정에 대한 특정 작업을 허용하거나 거부할 수 있는 정책입니다. 이를 사용하여 모든 비즈니스 유닛이 직접 예약 인스턴스를 구매하거나 수정하는 것을 막고, 중앙 팀을 통해서만 해당 작업을 수행할 수 있도록 강제할 수 있습니다.

◆ | **Q#0125.** | **Ref#0125.**
한 회사에서 Amazon RDS for MySQL 데이터베이스를 사용하여 데이터를 저장하는 중요한 애플리케이션을 실행하고 있습니다. RDS DB 인스턴스는 다중 AZ 모드로 배포됩니다.

최근 RDS 데이터베이스 장애 조치 테스트로 인해 애플리케이션이 40초 동안 중단되었습니다. 솔루션 설계자는 중단 시간을 20초 미만으로 줄이는 솔루션을 설계해야 합니다.

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

A. 데이터베이스 앞에 Memcached용 Amazon ElastiCache를 사용합니다.
B. 데이터베이스 앞에 Redis용 Amazon ElastiCache 사용
C. 데이터베이스 앞에 RDS Proxy를 사용하십시오.
D. 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다.
E. Amazon Aurora 복제본을 생성합니다.
F. MySQL용 RDS 읽기 전용 복제본 생성

해설
정답: C,D,E
C : RDS 프록시는 데이터베이스 커넥션을 관리하여 애플리케이션 패일오버 시간을 줄입니다
D : Amazon Aurora는 MySQL과 호환되며, 높은 내구성과 가용성을 위해 설계되었습니다. Amazon Aurora는 빠른 패일오버 시간을 가지고 있습니다
E: Amazon Aurora 복제본은 추가적인 가용성을 제공하고, 읽기 트래픽을 분산하여 성능을 향상시킵니다. 이는 패일오버 시간을 더욱 줄이는 데 도움이 됩니다

◆ | **Q#0126.** | **Ref#0126.**
AWS 파트너 회사는 org1이라는 조직을 사용하여 AWS Organizations에 서비스를 구축하고 있습니다. 이 서비스를 이용하려면 파트너 회사가 org2라는 별도의 조직에 있는 고객 계정의 AWS 리소스에 액세스할 수 있어야 합니다. 회사는 API 또는 명령줄 도구를 사용하여 고객 계정에 대한 최소 권한 보안 액세스를 설정해야 합니다.

org1이 org2의 리소스에 액세스하도록 허용하는 가장 안전한 방법은 무엇입니까?

A. 고객은 로그인하고 필요한 작업을 수행하기 위해 파트너사에 AWS 계정 액세스 키를 제공해야 합니다.
B. 고객은 IAM 사용자를 생성하고 IAM 사용자에게 필요한 권한을 할당해야 합니다. 그러면 고객은 로그인하고 필요한 작업을 수행할 수 있도록 파트너 회사에 자격 증명을 제공해야 합니다.
C. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위해 액세스를 요청할 때 IAM 역할의 Amazon 리소스 이름(ARN)을 사용해야 합니다.
D. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위해 액세스를 요청할 때 IAM 역할의 신뢰 정책에 있는 외부 ID를 포함하여 IAM 역할의 Amazon 리소스 이름(ARN)을 사용해야 합니다.

해설
정답:D
D: 가장 안전한 방법. 고객은 IAM 역할을 생성하고 필요한 권한을 할당한 후, 파트너 회사가 접근 요청 시 외부 ID를 포함한 IAM 역할의 ARN을 사용하도록 함.

외부 ID는 파트너 회사가 악의적인 사용자로 가장하지 않도록 추가적인 보안 계층을 제공하며, 교차 계정 역할을 안전하게 사용할 수 있게 합니다.
A(x), B(x): 각각 액세스 키 또는 IAM 사용자 자격 증명을 외부 파트너에게 제공하는 방식으로 보안상 매우 위험한 방식. 액세스 키나 사용자 자격 증명이 유출되면 계정 전체가 위협에 노출될 수 있음.
C(x) IAM 역할을 사용하여 접근 권한을 제공하는 방법을 제안하지만, 외부 ID를 사용하지 않음. 외부 ID를 사용하지 않으면 "중간자 공격"의 위험에 노출됨.

◆ | **Q#0127.** | **Ref#0127.**
배송 회사는 타사 경로 계획 애플리케이션을 AWS로 마이그레이션해야 합니다. 타사는 공개 레지스트리에서 지원되는 Docker 이미지를 제공합니다. 이미지는 경로 맵을 생성하는 데 필요한 만큼 많은 컨테이너에서 실행될 수 있습니다.

회사는 배송 지역을 공급 허브로 구분해 배송 기사가 허브에서 고객까지 최단 거리를 이동할 수 있도록 했다. 경로 맵을 생성하는 데 필요한 시간을 줄이기 위해 각 섹션에서는 섹션 영역에서만 주문을 처리하는 사용자 지정 구성이 포함된 자체 Docker 컨테이너 세트를 사용합니다.

회사는 실행 중인 컨테이너 수에 따라 비용 효율적으로 리소스를 할당할 수 있는 능력이 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon EC2에 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 생성합니다. Amazon EKS CLI를 사용하면 --tags 옵션을 사용하여 포드에 사용자 지정 태그를 할당함으로써 포드에서 계획 애플리케이션을 시작할 수 있습니다.
B. AWS Fargate에 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 생성합니다. Amazon EKS CLI를 사용하여 계획 애플리케이션을 시작합니다. AWS CLI 태그 리소스 API 호출을 사용하여 포드에 사용자 지정 태그를 할당합니다.
C. Amazon EC2에 Amazon Elastic Container Service(Amazon ECS) 클러스터를 생성합니다. run-tasks가 true로 설정된 AWS CLI를 사용하면 --tags 옵션을 사용하여 작업에 사용자 지정 태그를 할당함으로써 계획 애플리케이션을 시작할 수 있습니다.
D. AWS Fargate에 Amazon Elastic Container Service(Amazon ECS) 클러스터를 생성합니다. AWS CLI run-task 명령을 사용하고 활성화ECSManagedTags를 true로 설정하여 계획 애플리케이션을 시작합니다. --tags 옵션을 사용하여 작업에 사용자 정의 태그를 할당합니다.

해설
정답:D
D는 AWS Fargate를 사용하여 시스템을 간단하게 관리하고 컨테이너를 실행하는 비용을 최적화하게 해줍니다.
실행 중인 컨테이너 수에 따라 리소스를 동적으로 할당하며, 더 많은 운영 오버헤드 없이 사용자 정의 태그를 할당함으로써 각 섹션에 대한 사용자 정의 구성을 활용할 수 있습니다.
enableECSManagedTags의 동작은 Amazon ECS가 사용자 지정 태그를 ECS 관련 리소스에 자동으로 붙이도록 합니다.

◆ | **Q#0128.** | **Ref#0128.**
소프트웨어 회사는 여러 AWS 계정 및 리전의 리소스를 사용하여 AWS에서 애플리케이션을 호스팅합니다. 애플리케이션은 IPv4 CIDR 블록이 10.10.0.0/16인 us-east-1 리전에 위치한 애플리케이션 VPC의 Amazon EC2 인스턴스 그룹에서 실행됩니다. 다른 AWS 계정에서 공유 서비스 VPC는 IPv4 CIDR 블록이 10.10.10.0/24인 us-east-2 리전에 있습니다. 클라우드 엔지니어가 AWS CloudFormation을 사용하여 애플리케이션 VPC를 공유 서비스 VPC와 피어링하려고 시도하면 피어링 실패를 나타내는 오류 메시지가 나타납니다.

어떤 요인으로 인해 이 오류가 발생할 수 있나요? (2개를 선택하세요.)

A. 두 VPC의 IPv4 CIDR 범위가 겹칩니다.
B. VPC가 동일한 리전에 있지 않습니다.

C. 하나 또는 두 계정 모두 인터넷 게이트웨이에 액세스할 수 없습니다.
D. VPC 중 하나가 AWS Resource Access Manager를 통해 공유되지 않았습니다.
E. 피어 수락자 계정의 IAM 역할에 올바른 권한이 없습니다.

해설
정답: A,E
A : VPC 피어링은 겹치지 않는 CIDR 블록을 가진 VPC간에서 가능합니다. 두 CIDR 범위가 중첩되면 피어링을 설정할 수 없습니다.
E : 피어링을 수락하는 계정의 IAM 역할이 필요한 권한을 갖고 있지 않으면, VPC 피어링 요청을 수락할 수 없어서 오류가 발생합니다.

◆ | **Q#0129.** | **Ref#0129.**
한 회사의 서버리스 애플리케이션에 대한 외부 감사 결과 너무 많은 권한을 부여하는 IAM 정책이 드러났습니다. 이러한 정책은 회사의 AWS Lambda 실행 역할에 연결됩니다. 수백 개의 회사 Lambda 함수에는 Amazon S3 버킷 및 Amazon DynamoDB 테이블에 대한 전체 액세스와 같은 광범위한 액세스 권한이 있습니다. 회사는 각 기능이 해당 작업을 완료하는 데 필요한 최소한의 권한만 갖기를 원합니다.

솔루션 아키텍트는 각 Lambda 함수에 필요한 권한을 결정해야 합니다.

최소한의 노력으로 이 요구 사항을 충족하려면 솔루션 설계자가 무엇을 해야 합니까?

A. Amazon CodeGuru를 설정하여 Lambda 함수를 프로파일링하고 AWS API 호출을 검색하십시오. 각 Lambda 함수에 필요한 API 호출 및 리소스의 인벤토리를 생성합니다. 각 Lambda 함수에 대해 새로운 IAM 액세스 정책을 생성합니다. 새 정책을 검토하여 회사의 비즈니스 요구 사항을 충족하는지 확인하세요.
B. AWS 계정에 대해 AWS CloudTrail 로깅을 활성화합니다. AWS Identity and Access Management 액세스 분석기를 사용하여 CloudTrail 로그에 기록된 활동을 기반으로 IAM 액세스 정책을 생성합니다. 생성된 정책을 검토하여 회사의 비즈니스 요구 사항을 충족하는지 확인하세요.
C. AWS 계정에 대해 AWS CloudTrail 로깅을 활성화합니다. CloudTrail 로그를 구문 분석하고, Lambda 실행 역할별로 AWS API 호출을 검색하고, 요약 보고서를 생성하는 스크립트를 생성합니다. 보고서를 검토하세요. 각 Lambda 함수에 대해 더 제한적인 권한을 제공하는 IAM 액세스 정책을 생성합니다.
D. AWS 계정에 대해 AWS CloudTrail 로깅을 활성화합니다. CloudTrail 로그를 Amazon S3로 내보냅니다. Amazon EMR을 사용하여 Amazon S3에서 CloudTrail 로그를 처리하고 각 실행 역할에서 사용하는 API 호출 및 리소스에 대한 보고서를 생성합니다. 각 역할에 대해 새로운 IAM 액세스 정책을 생성합니다. 생성된 역할을 S3 버킷으로 내보냅니다. 생성된 정책을 검토하여 회사의 비즈니스 요구 사항을 충족하는지 확인하세요.

해설
정답: B
AWS Lambda 함수에 할당된 IAM 정책이 과도하게 권한을 부여하고 있어, 최소 권한 원칙(Least Privilege Principle)에 따라 각 Lambda 함수에 필요한 최소한의 권한만 부여하고자 하는 상황입니다. 이를 위해서는 각 Lambda 함수가 실제로 사용하는 권한을 파악한 후, 그에 따라 제한된 권한의 IAM 정책을 생성해야 합니다.
CloudTrail을 사용하여 모든 API 호출을 기록하고, IAM Access Analyzer를 사용해 기록된 활동을 기반으로 필요한 IAM 정책을 생성하는 방법입니다.
이는 자동화된 방식으로 IAM 정책을 생성할 수 있으며, 최소한의 노력으로 정책을 효율적으로 관리할 수 있습니다. 또한, 생성된 정책을 검토하여 비즈니스 요구사항에 부합하는지 확인할 수 있습니다.
Access Analyser는 자동화된 추론을 사용하여 리소스 정책을 분석하고 과도한 액세스 허용 또는 조직 보안 정책 위반과 같은 문제를 감지합니다. S3 버킷, IAM 역할, KMS 키 등 AWS 리소스에 연결된 정책을 검사하고 잠재적인 보안 위험이나 정책 위반을 식별하는 방식으로 작동합니다.

◆ | **Q#0130.** | **Ref#0130.**
솔루션 아키텍트는 회사의 Amazon EC2 인스턴스와 Amazon Elastic Block Store(Amazon EBS) 볼륨을 분석하여 회사가 리소스를 효율적으로 사용하고 있는지 확인해야 합니다. 이 회사는 활성/수동 구성으로 배포되는 데이터베이스 클러스터를 호스팅하기 위해 여러 개의 대규모 고용량 EC2 인스턴스를 실행하고 있습니다. 이러한 EC2 인스턴스의 활용도는 데이터베이스를 사용하는 애플리케이션에 따라 다르며 회사에서는 패턴을 식별하지 못했습니다.

솔루션 설계자는 환경을 분석하고 결과에 따라 조치를 취해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** AWS Systems Manager OpsCenter를 사용하여 대시보드를 생성하십시오. EC2 인스턴스 및 해당 EBS 볼륨과 연결된 Amazon CloudWatch 지표에 대한 시각화를 구성합니다. 대시보드를 주기적으로 검토하고 사용 패턴을 파악하세요. 지표의 최고치를 기준으로 EC2 인스턴스의 크기를 조정합니다.
> **B.** EC2 인스턴스 및 해당 EBS 볼륨에 대한 Amazon CloudWatch 세부 모니터링을 활성화합니다. 측정항목을 기반으로 대시보드를 만들고 검토하세요. 사용 패턴을 식별합니다. 지표의 최고치를 기준으로 EC2 인스턴스의 크기를 조정합니다.
> **C.** 각 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다. AWS Compute Optimizer를 켜고 최소 12시간 동안 실행해 보세요. Compute Optimizer의 권장 사항을 검토하고 지시에 따라 EC2 인스턴스 크기를 조정합니다.
> **D.** AWS Enterprise Support 플랜에 가입하세요. AWS Trusted Advisor를 활성화합니다. 12시간을 기다리세요. Trusted Advisor의 권장 사항을 검토하고 지시에 따라 EC2 인스턴스 크기를 조정합니다.
>
> 해설
> 정답: C
> C: AWS Compute Optimizer는 EC2 인스턴스 및 Auto Scaling 그룹과 같은 AWS 리소스의 사용 패턴을 분석하고 기계 학습 알고리즘을 사용하여 성능 및 비용을 최적화하는 방법에 대한 권장 사항을 제공합니다. 그런 다음 인스턴스 유형을 조정하는 데 사용할 수 있는 권장 사항을 생성합니다. Compute Optimizer는 메모리, CPU, 스토리지 등에 대한 사용 패턴을 분석하고, 가장 효과적인 구성을 제안해주어 비용 효율적입니다
>
> A, B는 EC2 인스턴스 및 EBS 볼륨의 CloudWatch 지표를 분석하고 최적화 방안을 수동으로 찾아야 합니다. 이러한 접근법은 수동 작업을 필요로 하기 때문에, 효율적이지 않습니다
> D는 AWS Enterprise Support 계획이 추가 비용을 발생시킵니다

131 (신재경) 3회차 完

◆ | **Q#0131.** | **Ref#0131.**
회사는 AWS 클라우드에서 다중 계정 설정을 위해 AWS Organizations를 사용합니다. 회사는 거버넌스를 위해 AWS Control Tower를 사용하고 계정 간 VPC 연결을 위해 AWS Transit Gateway를 사용합니다.

AWS 애플리케이션 계정에서 회사의 애플리케이션 팀은 AWS Lambda 및 Amazon RDS를 사용하는 웹 애플리케이션을 배포했습니다. 회사의 데이터베이스 관리자는 별도의 DBA 계정을 가지고 있으며 해당 계정을 사용하여 조직 전체의 모든 데이터베이스를 중앙에서 관리합니다. 데이터베이스 관리자는 DBA 계정에 배포된 Amazon EC2 인스턴스를 사용하여 애플리케이션 계정에 배포된 RDS 데이터베이스에 액세스합니다.

애플리케이션 팀은 애플리케이션 계정의 AWS Secrets Manager에 데이터베이스 자격 증명을 비밀로 저장했습니다. 애플리케이션 팀은 데이터베이스 관리자와 비밀을 수동으로 공유하고 있습니다. 비밀은 애플리케이션 계정의 Secrets Manager에 대한 기본 AWS 관리형 키로 암호화됩니다. 솔루션 설계자는 데이터베이스 관리자에게 데이터베이스에 대한 액세스 권한을 제공하고 비밀을 수동으로 공유할 필요가 없는 솔루션을 구현해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Resource Access Manager(AWS RAM)를 사용하여 애플리케이션 계정의 비밀을 DBA 계정과 공유하십시오. DBA 계정에서 DBA-Admin이라는 IAM 역할을 생성합니다. 공유 암호에 액세스하는 데 필요한 권한을 역할에 부여합니다. 교차 계정 암호에 액세스하려면 DBA-Admin 역할을 EC2 인스턴스에 연결하세요.
B. 애플리케이션 계정에서 DBA-Secret이라는 IAM 역할을 생성합니다. 비밀에 액세스하는 데 필요한 권한을 역할에 부여합니다. DBA 계정에서 DBA-Admin이라는 IAM 역할을 생성합니다. 애플리케이션 계정에서 DBA-Secret 역할을 맡는 데 필요한 권한을 DBA-Admin 역할에 부여합니다. 교차 계정 암호에 액세스하려면 DBA-Admin 역할을 EC2 인스턴스에 연결하세요.
C. DBA 계정에서 DBA-Admin이라는 IAM 역할을 생성합니다. 애플리케이션 계정의 암호 및 기본 AWS 관리형 키에 액세스하는 데 필요한 권한을 역할에 부여합니다. 애플리케이션 계정에서 리소스 기반 정책을 키에 연결하여 DBA 계정의 액세스를 허용합니다. 교차 계정 암호에 액세스하려면 DBA-Admin 역할을 EC2 인스턴스에 연결하세요.
D. DBA 계정에서 DBA-Admin이라는 IAM 역할을 생성합니다. 애플리케이션 계정의 비밀에 액세스하는 데 필요한 권한을 역할에 부여합니다. DBA 계정의 비밀에 대한 액세스를 허용하려면 애플리케이션 계정에 SCP를 연결하세요. 교차 계정 암호에 액세스하려면 DBA-Admin 역할을 EC2 인스턴스에 연결하세요.

해설
정답: B
B: 교차 계정 간 비밀을 안전하고 자동으로 접근할 수 있는 방법을 제공합니다.
먼저, 애플리케이션 계정에서 비밀에 접근할 수 있는 DBA-Secret 역할을 생성하고,
DBA 계정에서 DBA-Admin 역할을 생성하여 애플리케이션 계정의 DBA-Secret 역할을 가정(assume)할 수 있는 권한을 부여합니다.
이를 통해 DBA 계정의 EC2 인스턴스가 애플리케이션 계정의 비밀에 접근할 수 있으며, 비밀을 수동으로 공유할 필요가 없어집니다.

A(x): AWS RAM은 주로 리소스 공유에 사용되지만, Secrets Manager의 비밀을 직접 공유하기에는 적절하지 않습니다.
C(x): 관리 키에 대한 리소스 기반 정책을 적용하는 복잡한 접근 방식이 필요하며, 효율적인 솔루션이 아닙니다.
D(x): SCP(서비스 제어 정책)는 조직 수준에서 특정 서비스에 대한 접근을 제한하거나 허용하는 데 사용되지만, 이 시나리오에서는 필요하지 않음.

◆ | **Q#0132.** | **Ref#0132.**
회사는 AWS Organizations를 사용하여 여러 AWS 계정을 관리합니다. 루트 OU 아래에 회사에는 Research와 DataOps라는 두 개의 OU가 있습니다.

규제 요구 사항으로 인해 회사가 조직에 배포하는 모든 리소스는 ap-northeast-1 지역에 있어야 합니다. 또한 회사가 DataOps OU에 배포하는 EC2 인스턴스는 사전 정의된 인스턴스 유형 목록을 사용해야 합니다.

솔루션 설계자는 이러한 제한 사항을 적용하는 솔루션을 구현해야 합니다. 솔루션은 운영 효율성을 극대화하고 지속적인 유지 관리를 최소화해야 합니다.

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

A. DataOps OU 아래의 한 계정에 IAM 역할을 생성합니다. 특정 인스턴스 유형에 대한 액세스를 제한하려면 역할에 대한 인라인 정책에서 ec2:InstanceType 조건 키를 사용하십시오.
B. 루트 OU 아래의 모든 계정에 IAM 사용자를 생성합니다. ap-northeast-1을 제외한 모든 AWS 리전에 대한 액세스를 제한하려면 각 사용자의 인라인 정책에 aws:RequestedRegion 조건 키를 사용하십시오.
C. SCP를 생성합니다. aws:RequestedRegion 조건 키를 사용하여 ap-northeast-1을 제외한 모든 AWS 리전에 대한 액세스를 제한합니다. 루트 OU에 SCP를 적용합니다.
D. SCP를 생성합니다. ec2:Region 조건 키를 사용하여 ap-northeast-1을 제외한 모든 AWS 리전에

대한 액세스를 제한합니다. 루트 OU, DataOps OU 및 연구 OU에 SCP를 적용합니다.
E. SCP를 생성합니다. 특정 인스턴스 유형에 대한 액세스를 제한하려면 ec2:InstanceType 조건 키를 사용하세요. DataOps OU에 SCP를 적용합니다.

해설
정답: C,E
C: SCP를 루트 OU에 적용하여 리전 접근 제한: aws:RequestedRegion 조건 키를 사용하여 ap-northeast-1을 제외한 모든 AWS 리전에 대한 접근을 제한하는 SCP를 생성하고, 이를 루트 OU에 적용하면, 조직의 모든 계정이 이 리전 내에서만 리소스를 배포할 수 있게 됩니다. 이 방법은 중앙 집중식으로 관리가 가능하며, 유지보수 비용을 줄여줍니다.
E: SCP를 DataOps OU에 적용하여 인스턴스 유형 제한: ec2:InstanceType 조건 키를 사용하여 특정 인스턴스 유형에 대한 접근을 제한하는 SCP를 생성하고, 이를 DataOps OU에 적용하면, 이 OU에 있는 모든 계정에서 인스턴스 유형이 제한됩니다. 이렇게 하면 DataOps OU의 규제 요구 사항을 충족하면서 관리가 간편해집니다.

◆ | **Q#0133.** | **Ref#0133.**
회사는 단일 AWS 리전에서 서버리스 애플리케이션을 실행합니다. 애플리케이션은 외부 URL에 액세스하고 해당 사이트에서 메타데이터를 추출합니다. 이 회사는 Amazon Simple 알림 서비스(Amazon SNS) 주제를 사용하여 Amazon Simple Queue Service(Amazon SQS) 대기열에 URL을 게시합니다. AWS Lambda 함수는 대기열을 이벤트 소스로 사용하고 대기열의 URL을 처리합니다. 결과는 Amazon S3 버킷에 저장됩니다.

회사는 다른 리전에서도 각 URL을 처리하여 사이트의 지역화 차이를 비교하고 싶어 합니다. URL은 기존 리전에서 게시되어야 하며, 결과는 현재 리전의 기존 S3 버킷에 작성되어야 합니다.

이러한 요구 사항을 충족하는 다중 지역 배포를 생성하는 변경 사항 조합은 무엇입니까? (2개를 선택하세요.)

A. Lambda 함수를 사용하여 SQS 대기열을 다른 리전에 배포합니다.
B. 각 지역의 SNS 주제를 SQS 대기열에 등록합니다.
C. 각 리전의 SQS 대기열에서 SNS 주제를 구독합니다.
D. 각 지역의 SNS 주제에 URL을 게시하도록 SQS 대기열을 구성합니다.
E. SNS 주제와 Lambda 기능을 다른 지역에 배포합니다.

해설
정답: A,C
A: 다른 리전에 SQS 큐와 Lambda 함수를 배포: 다른 리전에서도 URL을 처리하기 위해서는 각 리전에 SQS 큐와 Lambda 함수를 배포해야 합니다. 이렇게 하면 각 리전에서 동일한 Lambda 함수가 실행되어 URL을 처리할 수 있습니다.
C: 각 리전의 SQS 큐를 SNS 주제에 구독시킴: 기존 리전의 SNS 주제에 각 리전의 SQS 큐를 구독시키면, 하나의 SNS 주제에서 게시된 URL이 여러 리전의 SQS 큐에 전달됩니다. 이렇게 하면 각 리전에서 동일한 URL을 처리할 수 있습니다.
SNS는 게시자이고 SQS는 구독자입니다.
A: Lambda 함수를 사용하여 SQS 대기열을 다른 지역에 배포하면 애플리케이션이 해당 지역의 URL을 처리하고 사이트 현지화의 차이점을 비교할 수 있음.
C: 각 지역의 SQS 대기열을 기존 지역의 SNS 주제에 구독하면 애플리케이션이 기존 SNS 주제에 URL을 게시하고 해당 URL을 다른 지역에서 처리할 수 있기 때문입니다.
B(x): 각 지역의 SNS 주제를 기존 지역의 SQS 대기열에 구독하면 다른 지역에서 URL을 처리할 수 없음.
D(x): 각 지역의 SNS 주제에 URL을 게시하도록 SQS 대기열을 구성하면 URL이 해당 지역에서 처리되는 것을 보장할 수 없음.
E(x): SQS 대기열 없이 SNS 주제와 Lambda 함수를 다른 지역에 배포하면 애플리케이션이 해당 지역의 URL을 처리할 수 없음.

◆ | **Q#0134.** | **Ref#0134.**
회사는 Amazon EC2 Linux 인스턴스에서 독점적인 상태 비저장 ETL 애플리케이션을 실행합니다. 해당 애플리케이션은 Linux 바이너리이므로 소스 코드를 수정할 수 없습니다. 이 애플리케이션은 단일 스레드이고 2GB RAM을 사용하며 CPU 집약적입니다. 애플리케이션은 4시간마다 실행되도록 예약되어 있으며 최대 20분 동안 실행됩니다. 솔루션 설계자는 솔루션의 아키텍처를 수정하려고 합니다.

솔루션 설계자는 어떤 전략을 사용해야 합니까?

> **A.** AWS Lambda를 사용하여 애플리케이션을 실행하십시오. Amazon CloudWatch Logs를 사용하여 4시간마다 Lambda 함수를 호출합니다.
> **B.** AWS Batch를 사용하여 애플리케이션을 실행합니다. AWS Step Functions 상태 시스템을 사용하여 4시간마다 AWS Batch 작업을 호출합니다.
> **C.** AWS Fargate를 사용하여 애플리케이션을 실행합니다. Amazon EventBridge(Amazon CloudWatch Events)를 사용하여 4시간마다 Fargate 작업을 호출합니다.
> **D.** Amazon EC2 스팟 인스턴스를 사용하여 애플리케이션을 실행합니다. AWS CodeDeploy를 사용하여 4시간마다 애플리케이션을 배포하고 실행합니다.
>
> 해설
> 정답: C
> AWS Fargate는 기본 EC2 인스턴스를 관리하지 않고도 컨테이너화된 워크로드를 실행할 수 있는 컨테이너용 서버리스 컴퓨팅 엔진입니다. 이렇게 하면 컨테이너를 실행하기 위해 가상 머신 클러스터를 프로비저닝, 구성 및 확장할 필요가 없습니다.
> C: EventBridge만 예약된 작업을 실행할 수 있습니다.
> A(x): Amazon CloudWatch Logs는 4시간마다 람다를 호출할 수 없습니다.
> B(x): Step Function은 4시간마다 일괄 작업을 호출할 수 없습니다. Step Function에는 스케줄러로 EventBridge가 필요합니다.
> D(x): CodeDeploy는 4시간마다 애플리케이션을 실행할 수 없습니다.

◆ | **Q#0135.** | **Ref#0135.**
한 회사에서 인기 온라인 게임의 속편을 만들고 있습니다. 출시 후 첫 주 이내에 전 세계의 수많은 사용자가 게임을 플레이하게 됩니다. 현재 게임은 단일 AWS 리전에 배포된 다음 구성 요소로 구성됩니다.

• 게임 자산을 저장하는 Amazon S3 버킷
• 플레이어 점수를 저장하는 Amazon DynamoDB 테이블

솔루션 아키텍트는 지연 시간을 줄이고 안정성을 향상시키는 다중 리전 솔루션을 설계해야 합니다. , 구현하는 데 최소한의 노력이 필요합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** S3 버킷의 자산을 제공하기 위해 Amazon CloudFront 배포를 생성합니다. S3 교차 리전 복제를 구성합니다. 새 리전에 새 DynamoDB 테이블을 생성합니다. 새 테이블을 DynamoDB 전역 테이블의 복제본 대상으로 사용합니다.
> **B.** S3 버킷의 자산을 제공하기 위해 Amazon CloudFront 배포판을 생성합니다. S3 동일 리전 복제를 구성합니다. 새 리전에 새 DynamoDB 테이블을 생성합니다. 변경 데이터 캡처(CDC)와 함께 AWS Database Migration Service(AWS DMS)를 사용하여 DynamoDB 테이블 간의 비동기식 복제를 구성합니다.
> **C.** 새 리전에 또 다른 S3 버킷을 생성하고 버킷 간에 S3 교차 리전 복제를 구성합니다. Amazon CloudFront 배포를 생성하고 각 리전의 S3 버킷에 액세스하는 두 개의 오리진으로 오리진 장애 조치를 구성합니다. Amazon DynamoDB 스트림을 활성화하여 DynamoDB 전역 테이블을 구성하고 새 리전에 복제본 테이블을 추가합니다.
> **D.** 사인 리전에 또 다른 S3 버킷을 생성하고 버킷 간에 S3 동일 리전 복제를 구성합니다. Amazon CloudFront 배포를 생성하고 S3 버킷에 액세스하는 두 개의 오리진으로 오리진 장애 조치를 구성합

니다. 새 리전에 새 DynamoDB 테이블을 생성합니다. 새 테이블을 DynamoDB 전역 테이블의 복제본 대상으로 사용합니다.

해설
정답: C
DynamoDB 전역 테이블 + S3 복제 + Cloudfront
A(x): "S3 교차 리전 복제 구성"이지만 다른 리전에 새 버킷을 생성하지 않습니다.
B(x): "S3 동일 리전 복제 구성"이 아닌 리전 간 복제여야 함. CDC가 포함된 AWS DMS는 적합하지 않음. 전역 테이블이 올바른 옵션.
D(x): 다른 지역에 새 버킷이 필요합니다.

◆ | **Q#0136.** | **Ref#0136.**
회사에는 잠재적 임차인 및 구매자에게 부동산 정보를 제공하는 온프레미스 웹 사이트 애플리케이션이 있습니다. 이 웹사이트는 Java 백엔드와 NoSQL MongoDB 데이터베이스를 사용하여 구독자 데이터를 저장합니다.

회사는 전체 애플리케이션을 유사한 구조의 AWS로 마이그레이션해야 합니다. 고가용성을 위해서는 애플리케이션을 배포해야 하며 회사는 애플리케이션을 변경할 수 없습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon Aurora DB 클러스터를 구독자 데이터용 데이터베이스로 사용하십시오. Java 백엔드 애플리케이션을 위해 여러 가용 영역에 걸쳐 Auto Scaling 그룹에 Amazon EC2 인스턴스를 배포합니다.
B. Amazon EC2 인스턴스의 MongoDB를 구독자 데이터의 데이터베이스로 사용하십시오. Java 백엔드 애플리케이션을 위한 단일 가용 영역의 Auto Scaling 그룹에 EC2 인스턴스를 배포합니다.
C. 여러 가용 영역에서 적절한 크기의 인스턴스를 사용하여 구독자 데이터용 데이터베이스로 Amazon DocumentDB(MongoDB 호환)를 구성합니다. Java 백엔드 애플리케이션을 위해 여러 가용 영역에 걸쳐 Auto Scaling 그룹에 Amazon EC2 인스턴스를 배포합니다.
D. 여러 가용 영역에서 온디맨드 용량 모드로 Amazon DocumentDB(MongoDB 호환)를 구독자 데이터용 데이터베이스로 구성합니다. Java 백엔드 애플리케이션을 위해 여러 가용 영역에 걸쳐 Auto Scaling 그룹에 Amazon EC2 인스턴스를 배포합니다.

해설
정답: C
A(x): Aurora는 MongoDB가 아닌 MySQL과 PostgreSQL을 지원합니다. 앱 변경은 허용되지 않음.
B(x): 작동할 수 있지만 DocumentDB는 선호되는 관리형 MongoDB 인스턴스를 제공함.
D(x): AWS DocumentDB에는 온디맨드 인스턴스만 있고 온디맨드 용량 모드는 없음. 모드는 DynamoDB용

◆ | **Q#0137.** | **Ref#0137.**
디지털 마케팅 회사에는 다양한 팀에 속한 여러 AWS 계정이 있습니다. 크리에이티브 팀은 AWS 계정의 Amazon S3 버킷을 사용하여 회사의 마케팅 캠페인 콘텐츠로 사용되는 이미지와 미디어 파일을 안전하게 저장합니다. 크리에이티브 팀은 전략 팀이 객체를 볼 수 있도록 S3 버킷을 전략 팀과 공유하려고 합니다.

솔루션 설계자가 전략 계정에 strategy_reviewer라는 IAM 역할을 생성했습니다. 또한 솔루션 아키텍트는 Creative 계정에 사용자 지정 AWS Key Management Service(AWS KMS) 키를 설정하고 해당 키를 S3 버킷과 연결했습니다. 그러나 전략 계정의 사용자가 IAM 역할을 맡고 S3 버킷의 객체에 액세스하려고 하면 액세스 거부 오류가 발생합니다.

솔루션 설계자는 전략 계정의 사용자가 S3 버킷에 액세스할 수 있는지 확인해야 합니다. 솔루션은 이러한 사용자에게 필요한 최소한의 권한만 제공해야 합니다.

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

A. S3 버킷에 대한 읽기 권한을 포함하는 버킷 정책을 생성합니다. 버킷 정책의 주체를 전략 계정의 계정 ID로 설정합니다.
B. strategy_reviewer IAM 역할을 업데이트하여 S3 버킷에 대한 전체 권한을 부여하고 사용자 지정 KMS 키에 대한 암호 해독 권한을 부여합니다.
C. Creative 계정의 사용자 지정 KMS 키 정책을 업데이트하여 strategy_reviewer IAM 역할에 암호 해독 권한을 부여합니다.
D. S3 버킷에 대한 읽기 권한을 포함하는 버킷 정책을 생성합니다. 버킷 정책의 주체를 익명 사용자로 설정합니다.
E. Creative 계정에서 사용자 지정 KMS 키 정책을 업데이트하여 strategy_reviewer IAM 역할에 암호화 권한을 부여합니다.
F. strategy_reviewer IAM 역할을 업데이트하여 S3 버킷에 대한 읽기 권한을 부여하고 사용자 지정 KMS 키에 대한 암호 해독 권한을 부여합니다.

해설
정답: A,C,F
S3 버킷 접근 권한 설정:
A. 버킷 정책 생성: strategy_reviewer 역할이 S3 버킷의 객체를 읽을 수 있도록 허용하기 위해 버킷 정책을 생성해야 합니다. 이 정책에서 Principal을 Strategy 계정의 계정 ID로 설정합니다.

KMS 키 접근 권한 설정:
C. KMS 키 정책 업데이트: strategy_reviewer 역할이 S3 버킷의 객체를 읽을 때 데이터 복호화를 할 수 있도록 KMS 키 정책을 업데이트해야 합니다. strategy_reviewer 역할에 KMS 키에 대한 복호화 권한(kms:Decrypt)을 부여해야 합니다.

IAM 역할에 필요한 권한 부여:
F. IAM 역할 업데이트: strategy_reviewer IAM 역할에 S3 버킷에 대한 읽기 권한과 KMS 키에 대한 복호화 권한을 부여해야 합니다. 이로 인해 Strategy 계정의 사용자는 이 역할을 가정한 후 S3 객체를 안전하게 읽을 수 있습니다.

B(x): 전체 권한을 부여하는 것은 최소 권한 원칙에 어긋납니다.
D(x): 익명 사용자에게 접근 권한을 부여하는 것은 보안 위험이 있습니다.
E(x): Encrypt 권한은 이 시나리오에서 필요하지 않으며, 주어진 요구 사항에 맞지 않습니다.

◆ | **Q#0138.** | **Ref#0138.**
한 생명 과학 회사는 데이터 분석 워크플로를 관리하기 위한 오픈 소스 도구와 온프레미스 데이터 센터의 서버에서 실행되는 Docker 컨테이너를 조합하여 사용하여 유전체학 데이터를 처리하고 있습니다. 시퀀싱 데이터가 생성되어 로컬 SAN(Storage Area Network)에 저장된 후 처리됩니다. 연구 개발 팀은 용량 문제에 직면해 있으며 워크로드 수요에 따라 확장하고 처리 시간을 몇 주에서 며칠로 단축하기 위해 AWS에서 게놈 분석 플랫폼을 다시 설계하기로 결정했습니다.

회사는 고속 AWS Direct Connect 연결을 보유하고 있습니다. 시퀀서는 각 게놈에 대해 약 200GB의 데이터를 생성하며 개별 작업은 이상적인 컴퓨팅 용량으로 데이터를 처리하는 데 몇 시간이 걸릴 수 있습니다. 최종 결과는 Amazon S3에 저장됩니다. 회사에서는 매일 10~15개의 작업 요청을 예상하고 있습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 정기적으로 예약된 AWS Snowball Edge 디바이스를 사용하여 시퀀싱 데이터를 AWS로 전송합니다. AWS가 Snowball Edge 디바이스를 수신하고 데이터가 Amazon S3에 로드되면 S3 이벤트를 사용하여 AWS Lambda 함수를 트리거하여 데이터를 처리합니다.
B. AWS Data Pipeline을 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하면 Amazon EC2 Auto Scaling 그룹을 트리거하여 Docker 컨테이너를 실행하는 사용자 지정 AMI EC2 인스턴스를 시작하여 데이터를 처리할 수 있습니다.
C. AWS DataSync를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여

AWS Step Functions 워크플로를 시작하는 AWS Lambda 함수를 트리거합니다. Amazon Elastic Container Registry(Amazon ECR)에 Docker 이미지를 저장하고 AWS Batch를 트리거하여 컨테이너를 실행하고 시퀀싱 데이터를 처리합니다.
D. AWS Storage Gateway 파일 게이트웨이를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 Docker 컨테이너를 실행하는 Amazon EC2 인스턴스에서 실행되는 AWS Batch 작업을 트리거하여 데이터를 처리합니다.

해설
정답: C
AWS DataSync는 온프레미스 데이터를 AWS로 신속하게 전송하는 데 적합한 서비스로, 대규모 데이터를 효율적으로 전송할 수 있습니다. 이는 200GB의 데이터를 정기적으로 전송해야 하는 이 시나리오에 잘 맞습니다.
S3 이벤트를 사용하여 데이터를 전송한 후 자동으로 다음 워크플로우를 시작할 수 있습니다.
AWS Step Functions는 여러 AWS 서비스 간의 복잡한 워크플로우를 오케스트레이션하는 데 사용되며, 여기서 데이터 처리 작업의 흐름을 관리할 수 있습니다.
AWS Batch는 컴퓨팅 리소스를 동적으로 프로비저닝하여 Docker 컨테이너에서 데이터를 처리하는 데 사용될 수 있으며, 이는 이 작업의 병렬 처리 요구에 적합합니다.

◆ | **Q#0139.** | **Ref#0139.**
회사는 개발 환경의 단일 Windows Amazon EC2 인스턴스에서 콘텐츠 관리 애플리케이션을 실행합니다. 애플리케이션은 인스턴스에 루트 디바이스로 연결된 2TB Amazon Elastic Block Store(Amazon EBS) 볼륨에 정적 콘텐츠를 읽고 씁니다. 회사는 여러 가용 영역에 걸쳐 최소 3개의 EC2 인스턴스에서 실행되는 고가용성 및 내결함성 솔루션으로 이 애플리케이션을 프로덕션에 배포할 계획입니다.

솔루션 설계자는 애플리케이션을 실행하는 모든 인스턴스를 Active Directory 도메인에 연결하는 솔루션을 설계해야 합니다. 또한 솔루션은 파일 콘텐츠에 대한 액세스를 제어하기 위해 Windows ACL을 구현해야 합니다. 애플리케이션은 항상 특정 시점에 실행 중인 모든 인스턴스에서 정확히 동일한 콘텐츠를 유지해야 합니다.

최소한의 관리 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon Elastic File System(Amazon EFS) 파일 공유를 생성합니다. 3개의 가용 영역에 걸쳐 확장되고 최소 3개의 인스턴스 크기를 유지하는 Auto Scaling 그룹을 생성합니다. 사용자 데이터 스크립트를 구현하여 애플리케이션을 설치하고, 인스턴스를 AD 도메인에 조인하고, EFS 파일 공유를 탑재합니다.
B. 실행 중인 현재 EC2 인스턴스에서 새 AMI를 생성합니다. Lustre 파일 시스템용 Amazon FSx를 생성합니다. 3개의 가용 영역에 걸쳐 확장되고 최소 3개의 인스턴스 크기를 유지하는 Auto Scaling 그룹을 생성합니다. 인스턴스를 AD 도메인에 조인하고 FSx for Lustre 파일 시스템을 탑재하는 사용자 데이터 스크립트를 구현합니다.
C. Windows 파일 서버용 Amazon FSx 파일 시스템을 생성합니다. 3개의 가용 영역에 걸쳐 확장되고 최소 3개의 인스턴스 크기를 유지하는 Auto Scaling 그룹을 생성합니다. 사용자 데이터 스크립트를 구현하여 애플리케이션을 설치하고 FSx for Windows File Server 파일 시스템을 탑재합니다. 원활한 도메인 조인을 수행하여 인스턴스를 AD 도메인에 조인합니다.
D. 현재 실행 중인 EC2 인스턴스에서 새 AMI를 생성합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. 3개의 가용 영역에 걸쳐 확장되고 최소 3개의 인스턴스 크기를 유지하는 Auto Scaling 그룹을 생성합니다. 원활한 도메인 조인을 수행하여 인스턴스를 AD 도메인에 조인합니다.

해설
정답: C
Amazon FSx for Windows File Server는 Windows 환경에서 파일 시스템을 관리하는 데 최적화된 솔루션으로, Windows ACL을 지원하여 파일 접근 제어를 할 수 있습니다.
C: 모든 인스턴스에서 동일한 파일 콘텐츠를 유지하기 위해 중앙 집중식 파일 시스템을 사용하며, Auto Scaling 그룹을 통해 고가용성을 보장합니다. 또한 AD 도메인 가입을 자동화하여 관리 오버헤

드를 최소화합니다.
Windows 환경에 최적화된 FSx for Windows File Server를 사용하여 AD 통합 및 ACL 관리가 용이하며, 고가용성을 유지하면서 모든 인스턴스에서 동일한 데이터를 사용할 수 있는 가장 적합한 솔루션입니다.

A(x), D(x): Amazon EFS는 Linux 기반에서 주로 사용되며, Windows ACL을 제대로 지원하지 않으므로 Windows 환경에는 적합하지 않습니다.
B(x): Amazon FSx for Lustre는 고성능 컴퓨팅에 적합하지만, Windows ACL을 지원하지 않으며, 이 경우에 비효율적입니다.

◆ | **Q#0140.** | **Ref#0140.**
SaaS(Software as a Service) 기반 회사는 솔루션의 일부인 A3 고객에게 사례 관리 솔루션을 제공합니다. 회사는 독립형 SMTP(Simple Mail Transfer Protocol) 서버를 사용하여 애플리케이션에서 이메일 메시지를 보냅니다. 또한 애플리케이션은 고객에게 이메일 메시지를 보내기 전에 고객 데이터를 채우는 승인 이메일 메시지용 이메일 템플릿을 저장합니다.

회사는 이 메시징 기능을 AWS 클라우드로 마이그레이션할 계획이며 운영 오버헤드를 최소화해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. AWS Marketplace의 AMI를 사용하여 Amazon EC2 인스턴스에 SMTP 서버를 설정하십시오. Amazon S3 버킷에 이메일 템플릿을 저장합니다. S3 버킷에서 템플릿을 검색하고 애플리케이션의 고객 데이터를 템플릿과 병합하는 AWS Lambda 함수를 생성합니다. Lambda 함수에서 SDK를 사용하여 이메일 메시지를 보냅니다.
B. 이메일 메시지를 보내도록 Amazon Simple Email Service(Amazon SES)를 설정합니다. Amazon S3 버킷에 이메일 템플릿을 저장합니다. S3 버킷에서 템플릿을 검색하고 애플리케이션의 고객 데이터를 템플릿과 병합하는 AWS Lambda 함수를 생성합니다. Lambda 함수에서 SDK를 사용하여 이메일 메시지를 보냅니다.
C. AWS Marketplace의 AMI를 사용하여 Amazon EC2 인스턴스에 SMTP 서버를 설정합니다. 고객 데이터에 대한 매개변수를 사용하여 Amazon Simple Email Service(Amazon SES)에 이메일 템플릿을 저장합니다. SES 템플릿을 호출하고 고객 데이터를 전달하여 매개변수를 대체하는 AWS Lambda 함수를 생성합니다. AWS Marketplace SMTP 서버를 사용하여 이메일 메시지를 보냅니다.
D. 이메일 메시지를 보내도록 Amazon Simple Email Service(Amazon SES)를 설정합니다. 고객 데이터에 대한 매개변수와 함께 이메일 템플릿을 Amazon SES에 저장합니다. SendTemplateEmail API 작업을 호출하고 매개변수와 이메일 대상을 대체하기 위해 고객 데이터를 전달하는 AWS Lambda 함수를 생성합니다.

해설
정답: D
Amazon SES는 AWS에서 관리되는 이메일 발송 서비스로, SMTP 서버를 직접 설정할 필요가 없기 때문에 운영 오버헤드를 크게 줄여줍니다.
D: 이메일 템플릿을 SES에 직접 저장하고, SES의 SendTemplatedEmail API를 사용하여 고객 데이터를 파라미터로 전달해 템플릿을 채워서 이메일을 발송합니다.
이 방법은 AWS의 관리형 서비스인 SES를 최대한 활용하여 운영 부담을 최소화하고 비용을 절감할 수 있는 가장 효율적인 방법입니다.

A(x): 직접 SMTP 서버를 운영해야 하므로 운영 오버헤드가 크고, SES를 사용하는 것보다 비용이 더 많이 들 수 있습니다.
B(x): SES를 사용하지만, 이메일 템플릿을 SES에 저장하지 않고 S3에서 가져오는 방법이기 때문에 추가적인 스텝이 필요합니다.
C(x): SMTP 서버를 직접 운영해야 하기 때문에 운영 부담이 크며, SES를 완전히 활용하지 못합니다.

141 (송희성) 3회차 完

◆ | **Q#0141.** | **Ref#0141.**
한 회사가 Auto Scaling 그룹의 Amazon EC2 인스턴스를 사용하여 AWS 클라우드에서 비디오를 처리하고 있습니다. 비디오를 처리하는 데 30분이 소요됩니다. 여러 EC2 인스턴스는 Amazon Simple Queue Service(Amazon SQS) 대기열의 비디오 수에 따라 확장 및 축소됩니다.

회사는 대상 배달 못한 편지 대기열과 maxReceiveCount를 1로 지정하는 리드라이브 정책을 사용하여 SQS 대기열을 구성했습니다. 회사는 SQS 대기열에 대한 표시 제한 시간을 1시간으로 설정했습니다. 회사는 배달 못한 편지 대기열에 메시지가 있을 때 개발 팀에 알리기 위해 Amazon CloudWatch 경보를 설정했습니다.

하루에도 여러 번. 개발팀은 메시지가 배달 못한 편지 대기열에 있고 비디오가 처리되지 않았다는 알림을 받습니다. 조사 결과 애플리케이션 로그에서 오류가 발견되지 않았습니다.

회사는 이 문제를 어떻게 해결할 수 있나요?

> **A.** EC2 인스턴스에 대한 종료 방지 기능을 활성화합니다.
> **B.** SQS 대기열의 제한 시간 초과를 3시간으로 업데이트합니다.
> **C.** 처리 중 인스턴스에 대한 축소 보호 구성
> **D.** 리드라이브 정책을 업데이트하고 maxReceiveCount를 0으로 설정합니다.
>
> 해설
> 정답: C
> 처리되지 않은 비디오는 처리 중 인스턴스의 종료로 중단된 것으로 이는 Auto-Scaling의 Scale-in 문제로 보여진다.
> 이를 해결하기 위해서는 C가 적합하다.
>
> A(x): Auto-Scaling에 의한 종료를 막을 수 없으며
> B(x): 비디오의 처리시간이 30분이라 1시간도 적합하다.
> D(x): maxReceiveCount는 양의 정수로 설정해야 한다.

◆ | **Q#0142.** | **Ref#0142.**
한 회사가 지역 엔드포인트와 함께 Amazon API Gateway를 사용하는 API를 개발했습니다. API는 API 게이트웨이 인증 메커니즘을 사용하는 AWS Lambda 함수를 호출합니다. 설계 검토 후 솔루션 설계자는 공개 액세스가 필요하지 않은 API 세트를 식별합니다.

솔루션 아키텍트는 VPC에서만 API 세트에 액세스할 수 있도록 솔루션을 설계해야 합니다. 모든 API는 인증된 사용자를 통해 호출해야 합니다.

최소한의 노력으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

> **A.** 내부 ALB(Application Load Balancer)를 생성합니다. 대상 그룹을 만듭니다. 호출할 Lambda 함수를 선택합니다. ALB DNS 이름을 사용하여 VPC에서 API를 호출합니다.
> **B.** API Gateway에서 API와 연결된 DNS 항목을 제거합니다. Amazon Route 53에서 호스팅 영역을 생성합니다. 호스팅 영역에 CNAME 레코드를 생성합니다. CNAME 레코드를 사용하여 API Gateway의 API를 업데이트합니다. CNAME 레코드를 사용하여 VPC에서 API를 호출합니다.
> **C.** API 게이트웨이에서 API 엔드포인트를 지역에서 프라이빗으로 업데이트합니다. VPC에서 인터페이스 VPC 엔드포인트를 생성합니다. 리소스 정책을 생성하고 이를 API에 연결합니다. VPC 엔드포인트를 사용하여 VPC에서 API를 호출합니다.
> **D.** VPC 내부에 Lambda 함수를 배포합니다. EC2 인스턴스를 프로비저닝하고 Apache 서버를 설치합니다. Apache 서버에서 Lambda 함수를 호출합니다. EC2 인스턴스의 내부 CNAME 레코드를 사용하여 VPC에서 API를 호출합니다.

해설
정답: C
C: 가장 적은 노력으로 요구 사항을 충족할 수 있는 방법.
API Gateway 엔드포인트를 Regional에서 프라이빗으로 업데이트하고, VPC 내에서 API에 접근할 수 있도록 인터페이스 VPC 엔드포인트를 생성합니다.
또한 리소스 정책을 사용해 API 접근을 제어할 수 있습니다.
이를 통해 VPC 내에서만 API에 접근할 수 있게 하며, 인증된 사용자만 접근할 수 있도록 설정할 수 있습니다.

A와 D는 간접적이고 복잡한 방식이며, B는 VPC내부에서만 접근하도록 하지 않는다.

◆ | **Q#0143.** | **Ref#0143.**
날씨 서비스는 eu-west-1 지역의 AWS에 호스팅된 웹 애플리케이션에서 고해상도 날씨 지도를 제공합니다. 날씨 지도는 자주 업데이트되며 정적 HTML 콘텐츠와 함께 Amazon S3에 저장됩니다. 웹 애플리케이션 앞에는 Amazon CloudFront가 있습니다.

회사는 최근 us-east-1 지역의 사용자에게 서비스를 제공하도록 확장했으며 이러한 신규 사용자는 각자의 날씨 지도를 보는 것이 때때로 느리다고 보고합니다.

us-east-1 성능 문제를 해결하려면 어떤 단계를 조합해야 합니까? (2개를 선택하세요.)

A. eu-west-1의 S3 버킷에 대한 AWS Global Accelerator 엔드포인트를 구성합니다. us-east-1에서 TCP 포트 80 및 443에 대한 엔드포인트 그룹을 구성합니다.
B. us-east-1에 새 S3 버킷을 생성합니다. eu-west-1의 S3 버킷에서 동기화하도록 S3 교차 리전 복제를 구성합니다.
C. Lambda@Edge를 사용하여 us-east-1에서 S3 Transfer Acceleration 엔드포인트를 사용하도록 북미의 요청을 수정합니다.
D. Lambda@Edge를 사용하여 us-east-1의 S3 버킷을 사용하도록 북미의 요청을 수정합니다.
E. us-east-1에 대한 AWS Global Accelerator 엔드포인트를 CloudFront 배포의 오리진으로 구성합니다. Lambda@Edge를 사용하여 새 오리진을 사용하도록 북미의 요청을 수정합니다.

해설
정답: BD
B: us-east-1 리전에 새로운 S3 버킷을 생성하고, 크로스 리전 복제를 통해 eu-west-1의 S3 버킷과 동기화하여 콘텐츠를 복제합니다. 이렇게 하면 us-east-1 리전의 사용자들이 더 빠르게 콘텐츠에 접근할 수 있습니다.
D: Lambda@Edge를 사용하여 북미 사용자들이 us-east-1의 S3 버킷에서 데이터를 요청하도록 요청을 수정합니다. 이렇게 하면 사용자의 위치에 따라 가장 가까운 리전에서 콘텐츠를 제공받을 수 있어 성능이 개선됩니다.

◆ | **Q#0144.** | **Ref#0144.**
솔루션 아키텍트는 회사가 Amazon Workspaces에서 새 세션을 설정할 수 없는 문제를 조사하고 있습니다. 초기 분석에 따르면 문제에 사용자 프로필이 관련되어 있는 것으로 나타났습니다. Amazon Workspaces 환경은 Amazon FSx for Windows File Server를 프로필 공유 스토리지로 사용하도록 구성되어 있습니다. FSx for Windows File Server 파일 시스템은 10TB의 스토리지로 구성됩니다.

솔루션 설계자는 파일 시스템이 최대 용량에 도달했음을 발견합니다. 솔루션 설계자는 사용자가 다시 액세스할 수 있도록 해야 합니다. 또한 솔루션은 문제가 다시 발생하는 것을 방지해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 이전 사용자 프로필을 제거하여 공간을 만듭니다. 사용자 프로필을 Amazon FSx for Lustre 파일 시스템으로 마이그레이션합니다.
B. update-file-system 명령을 사용하여 용량을 늘립니다. 여유 공간을 모니터링하는 Amazon

CloudWatch 지표를 구현합니다. Amazon EventBridge를 사용하여 AWS Lambda 함수를 호출하여 필요에 따라 용량을 늘립니다.
C. Amazon CloudWatch에서 FreeStorageCapacity 지표를 사용하여 파일 시스템을 모니터링합니다. AWS Step Functions를 사용하여 필요에 따라 용량을 늘립니다.
D. 이전 사용자 프로필을 제거하여 공간을 만듭니다. Windows 파일 서버 파일 시스템용 추가 FSx를 생성합니다. 사용자 중 50%가 새 파일 시스템을 사용하도록 사용자 프로필 리디렉션을 업데이트합니다.

해설
정답: B

기존의 프로필을 제거하는 것보다 용량을 늘리는 방안이 더 효과적이며, CloudWatch와 EventBridge를 사용하여 Storage 부족 시 증설을 자동화 할 수 있다.
C(x): Step Function을 활용해서는 인스턴스 용량을 늘릴 수 없다.

◆ | **Q#0145.** | **Ref#0145.**
국제 배송 회사는 AWS에서 배송 관리 시스템을 호스팅합니다. 운전자는 시스템을 사용하여 배송 확인을 업로드합니다. 확인에는 수령인의 서명이나 수령인이 찍힌 패키지 사진이 포함됩니다. 운전자의 휴대용 장치는 FTP를 통해 단일 Amazon EC2 인스턴스에 서명과 사진을 업로드합니다. 각 휴대용 장치는 로그인한 사용자를 기반으로 하는 디렉터리에 파일을 저장하며 파일 이름은 배달 번호와 일치합니다. 그런 다음 EC2 인스턴스는 중앙 데이터베이스에 쿼리하여 배달 정보를 가져온 후 파일에 메타데이터를 추가합니다. 그런 다음 파일은 보관을 위해 Amazon S3에 배치됩니다.

회사가 확장됨에 따라 운전자는 시스템이 연결을 거부하고 있다고 보고합니다. FTP 서버는 이러한 문제에 대한 응답으로 연결 끊김 및 메모리 문제로 인해 문제를 겪고 있습니다. 시스템 엔지니어는 30분마다 EC2 인스턴스를 재부팅하도록 cron 작업을 예약합니다. 청구팀에서는 파일이 항상 아카이브에 있는 것은 아니며 중앙 시스템이 항상 업데이트되지는 않는다고 보고합니다.

솔루션 설계자는 아카이브가 항상 파일을 수신하고 시스템이 항상 업데이트되도록 확장성을 최대화하는 솔루션을 설계해야 합니다. 휴대용 장치는 수정할 수 없으므로 회사에서는 새 애플리케이션을 배포할 수 없습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 기존 EC2 인스턴스의 AMI를 생성합니다. Application Load Balancer 뒤에 EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 최소 3개의 인스턴스를 갖도록 Auto Scaling 그룹을 구성합니다.
B. AWS Transfer Family를 사용하여 Amazon Elastic File System(Amazon EFS)에 파일을 저장하는 FTP 서버를 생성합니다. EFS 볼륨을 기존 EC2 인스턴스에 탑재합니다. EC2 인스턴스가 파일 처리를 위한 새 경로를 가리키도록 합니다.
C. AWS Transfer Family를 사용하여 Amazon S3에 파일을 배치하는 FTP 서버를 생성합니다. Amazon Simple 알림 서비스(Amazon SNS)를 통해 S3 이벤트 알림을 사용하여 AWS Lambda 함수를 호출합니다. 메타데이터를 추가하고 전달 시스템을 업데이트하도록 Lambda 함수를 구성합니다.
D. 파일을 Amazon S3에 직접 배치하려면 휴대용 장치를 업데이트하십시오. Amazon Simple Queue Service(Amazon SQS)를 통해 S3 이벤트 알림을 사용하여 AWS Lambda 함수를 호출합니다. 메타데이터를 추가하고 전달 시스템을 업데이트하도록 Lambda 함수를 구성합니다.

해설
정답: C
A와 B는 기존의 EC2인스턴스에서 S3으로 Archive하는데 기존의 메모리 이슈가 우려된다.
따라서 별도의 FTP인스턴스를 생성하여, S3에 데이터가 적재되면, 알람을 통해 중앙 시스템을 업데이트 하는 것이 적절하다.

◆ | **Q#0146.** | **Ref#0146.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon Elastic Container Service(Amazon ECS) 클러스터의 컨테이너에서 실행됩니다. ECS 작업은 Fargate 시작 유형을 사용합니다. 애플리

케이션의 데이터는 관계형이며 Amazon Aurora MySQL에 저장됩니다. 규제 요구 사항을 충족하려면 애플리케이션 오류가 발생할 경우 애플리케이션을 별도의 AWS 리전으로 복구할 수 있어야 합니다. 장애가 발생하더라도 데이터는 손실되지 않습니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 다른 리전에 Aurora 복제본을 프로비저닝하십시오.
> **B.** 데이터를 다른 지역으로 지속적으로 복제하도록 AWS DataSync를 설정합니다.
> **C.** 다른 지역으로 데이터를 지속적으로 복제하도록 AWS Database Migration Service(AWS DMS)를 설정합니다.
> **D.** Amazon Data Lifecycle Manager(Amazon DLM)를 사용하여 5분마다 스냅샷을 예약합니다.
>
> 해설
> 정답: A
> 다른 리전에 Aurora replica를 프로비저닝 함으로써, 장애 발생 시 해당 replica로 fail-over하여 데이터 손실 없이 서비스 할 수 있다.
>
> B, C는 별도의 추가 구성 관리가 필요하다. D는 스냅샷의 경우 장애 시 데이터 손실이 발생할 수 있다.

◆ | **Q#0147.** | **Ref#0147.**
금융 서비스 회사는 신용 카드 서비스 파트너로부터 정기적인 데이터 피드를 받습니다. 약 5,000개의 레코드가 15분마다 일반 텍스트로 전송되며 서버 측 암호화를 통해 HTTPS를 통해 Amazon S3 버킷으로 직접 전달됩니다. 이 피드에는 민감한 신용카드 기본 계좌 번호(PAN) 데이터가 포함되어 있습니다. 회사는 추가 내부 처리를 위해 데이터를 다른 S3 버킷으로 보내기 전에 PAN을 자동으로 마스킹해야 합니다. 또한 회사는 특정 필드를 제거하고 병합한 다음 레코드를 JSON 형식으로 변환해야 합니다. 또한 향후 추가 피드가 추가될 가능성이 높으므로 모든 디자인은 쉽게 확장 가능해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 각 레코드를 추출하여 Amazon SQS 대기열에 쓰는 파일 전송 시 AWS Lambda 함수를 호출합니다. 새 메시지가 SQS 대기열에 도착하면 다른 Lambda 함수를 호출하여 레코드를 처리하고 결과를 Amazon S3의 임시 위치에 씁니다. SQS 대기열이 비어 있으면 최종 Lambda 함수를 호출하여 레코드를 JSON 형식으로 변환하고 내부 처리를 위해 결과를 다른 S3 버킷으로 보냅니다.
> **B.** 각 레코드를 추출하여 Amazon SQS 대기열에 쓰는 파일 전송 시 AWS Lambda 함수를 호출합니다. SQS 대기열에 메시지가 포함된 경우 단일 인스턴스로 자동 확장되도록 AWS Fargate 컨테이너 애플리케이션을 구성합니다. 애플리케이션에서 각 레코드를 처리하고 레코드를 JSON 형식으로 변환하도록 합니다. 대기열이 비어 있으면 내부 처리를 위해 결과를 다른 S3 버킷으로 보내고 AWS Fargate 인스턴스를 축소합니다.
> **C.** 데이터 피드 형식을 기반으로 AWS Glue 크롤러 및 사용자 지정 분류자를 생성하고 일치하는 테이블 정의를 구축합니다. 파일 전송 시 AWS Lambda 함수를 호출하여 처리 및 변환 요구 사항에 따라 전체 레코드를 변환하는 AWS Glue ETL 작업을 시작합니다. 출력 형식을 JSON으로 정의합니다. 완료되면 ETL 작업이 내부 처리를 위해 결과를 다른 S3 버킷으로 보내도록 합니다.
> **D.** 데이터 피드 형식을 기반으로 AWS Glue 크롤러 및 사용자 지정 분류자를 생성하고 일치하는 테이블 정의를 구축합니다. 파일 전송에 대해 Amazon Athena 쿼리를 수행하여 처리 및 변환 요구 사항에 따라 전체 레코드를 변환하는 Amazon EMR ETL 작업을 시작합니다. 출력 형식을 JSON으로 정의합니다. 완료되면 내부 처리를 위해 결과를 다른 S3 버킷으로 보내고 EMR 클러스터를 축소합니다.
>
> 해설
> 정답: C
> AWS Glue를 사용하여 데이터를 추출, 변환 및 로드(ETL)할 수 있습니다.
> AWS Glue 크롤러와 사용자 정의 분류자를 사용하여 데이터 형식을 식별하고,

AWS Glue ETL 작업을 통해 데이터를 마스킹, 필드 병합 및 JSON 형식으로 변환할 수 있습니다.
AWS Lambda는 파일 전달 시 ETL 작업을 자동으로 시작하며, 이 솔루션은 확장 가능하고 추가 작업이 필요할 경우 쉽게 확장할 수 있습니다.
C 선택지는 관리 오버헤드가 적고, 추가 피드가 추가될 경우 확장성 면에서도 우수합니다.

◆ | **Q#0148.** | **Ref#0148.**
회사에서는 회사의 주요 온프레미스 애플리케이션이 실패할 경우를 대비해 AWS를 사용하여 비즈니스 연속성 솔루션을 만들고 싶어합니다. 애플리케이션은 다른 애플리케이션도 실행하는 물리적 서버에서 실행됩니다. 회사에서 마이그레이션할 계획인 온프레미스 애플리케이션은 MySQL 데이터베이스를 데이터 저장소로 사용합니다. 회사의 모든 온프레미스 애플리케이션은 Amazon EC2와 호환되는 운영 체제를 사용합니다.

최소한의 운영 오버헤드로 회사의 목표를 달성할 수 있는 솔루션은 무엇입니까?

A. MySQL 서버를 포함한 소스 서버에 AWS 복제 에이전트를 설치합니다. 모든 서버에 대한 복제를 설정합니다. 정기 훈련을 위한 테스트 인스턴스를 시작합니다. 오류 이벤트가 발생할 경우 워크로드를 장애 조치하기 위해 테스트 인스턴스로 전환합니다.
B. MySQL 서버를 포함한 소스 서버에 AWS 복제 에이전트를 설치합니다. 대상 AWS 리전에서 AWS Elastic Disaster Recovery를 초기화합니다. 시작 설정을 정의합니다. 가장 최근 시점부터 장애 조치(failover) 및 대체(fallback)를 자주 수행합니다.
C. AWS DMS(AWS Database Migration Service) 복제 서버와 대상 Amazon Aurora MySQL DB 클러스터를 생성하여 데이터베이스를 호스팅합니다. 기존 데이터를 대상 DB 클러스터에 복사하는 DMS 복제 작업을 생성합니다. 로컬 AWS Schema Conversion Tool(AWS SCT) 변경 데이터 캡처(CDC) 작업을 생성하여 데이터 동기화를 유지합니다. 호환되는 기본 AMI로 시작하여 EC2 인스턴스에 나머지 소프트웨어를 설치합니다.
D. 온프레미스에 AWS Storage Gateway 볼륨 게이트웨이를 배포합니다. 모든 온프레미스 서버에 볼륨을 탑재합니다. 새 볼륨에 애플리케이션과 MySQL 데이터베이스를 설치합니다. 정기적으로 스냅샷을 찍으세요. 호환되는 기본 AMI로 시작하여 EC2 인스턴스에 모든 소프트웨어를 설치합니다. EC2 인스턴스에서 볼륨 게이트웨이를 시작합니다. 최신 스냅샷에서 볼륨을 복원합니다. 오류가 발생하는 경우 EC2 인스턴스에 새 볼륨을 탑재합니다.

해설
정답: B
가장 적은 운영 오버헤드를 지원하기 위해서는 B가 적합하다.
EDR(Elastic Disaster Recovery)은 Fail-over와 Fail-back을 자동으로 지원한다.
A는 regular drill을 위해 테스트 인스턴스를 생성하므로 운영 소요가 있다.
C는 DB중심적이며, app을 EC2인스턴스에 수동설치 해야한다.
D는 정기적으로 스냅샷을 찍고 복원을 해야하므로 운영 소요가 있다.

◆ | **Q#0149.** | **Ref#0149.**
회사는 재무 정보에 대한 규제 감사를 받습니다. 단일 AWS 계정을 사용하는 외부 감사자는 회사의 AWS 계정에 액세스해야 합니다. 솔루션 아키텍트는 감사자에게 회사의 AWS 계정에 대한 안전한 읽기 전용 액세스 권한을 제공해야 합니다. 솔루션은 AWS 보안 모범 사례를 준수해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 회사의 AWS 계정에서 계정의 모든 리소스에 대한 리소스 정책을 생성하여 감사자의 AWS 계정에 대한 액세스 권한을 부여합니다. 리소스 정책에 고유한 외부 ID를 할당합니다.
B. 회사의 AWS 계정에서 감사자의 AWS 계정을 신뢰하는 IAM 역할을 생성합니다. 필요한 권한이 있는 IAM 정책을 생성합니다. 정책을 역할에 연결합니다. 역할의 신뢰 정책에 고유한 외부 ID를 할당합니다.
C. 회사의 AWS 계정에서 IAM 사용자를 생성합니다. 필요한 IAM 정책을 IAM 사용자에게 연결합니다. IAM 사용자에 대한 API 액세스 키를 생성합니다. 감사자와 액세스 키를 공유합니다.

D. 회사의 AWS 계정에서 필요한 권한이 있는 IAM 그룹을 생성합니다. 각 감사자에 대해 회사 계정에 IAM 사용자를 생성합니다. IAM 그룹에 IAM 사용자를 추가합니다.

해설
정답: B

IAM role에 정책을 할당하여 외부 감사인이 회사 내부 자료에 대한 적절한 권한을 가질 수 있도록 설정할 수 있다.
A(x): 외부 감사인의 권한을 제한할 수 있는 방법을 제공하지 않음.
C(x): 경우 감사자와 API 액세스 키를 공유하므로, 안전하지 않음.
D(x): 경우 감사인마다 개별 계정을 생성해야하므로 비효율적이다.

◆ | **Q#0150.** | **Ref#0150.**
한 회사에는 Amazon DynamoDB를 스토리지 백엔드로 사용하는 지연 시간에 민감한 거래 플랫폼이 있습니다. 회사는 온디맨드 용량 모드를 사용하도록 DynamoDB 테이블을 구성했습니다. 솔루션 설계자는 거래 플랫폼의 성능을 향상시키기 위한 솔루션을 설계해야 합니다. 새로운 솔루션은 거래 플랫폼의 고가용성을 보장해야 합니다.

가장 짧은 대기 시간으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 2노드 DynamoDB Accelerator(DAX) 클러스터를 생성합니다. DAX를 사용하여 데이터를 읽고 쓰도록 애플리케이션을 구성합니다.
B. 3노드 DynamoDB Accelerator(DAX) 클러스터를 생성합니다. DAX를 사용하여 데이터를 읽고 DynamoDB 테이블에 직접 데이터를 쓰도록 애플리케이션을 구성합니다.
C. 3노드 DynamoDB Accelerator(DAX) 클러스터를 생성합니다. DynamoDB 테이블에서 직접 데이터를 읽고 DAX를 사용하여 데이터를 쓰도록 애플리케이션을 구성합니다.
D. 단일 노드 DynamoDB Accelerator(DAX) 클러스터를 생성합니다. DAX를 사용하여 데이터를 읽고 DynamoDB 테이블에 직접 데이터를 쓰도록 애플리케이션을 구성합니다.

해설
정답: B

고가용성: 단일노드 2노드보다는 3노드
DAX의 최적 사용 방식은 쓰기는 Direct로 DynamoDB에 읽기는 DAX를 활용하는 것이다.

151 (최정현) 3회차 完

◆ | **Q#0151.** | **Ref#0151.**
한 회사가 애플리케이션을 온프레미스에서 AWS로 마이그레이션했습니다. 애플리케이션 프런트엔드는 Application Load Balancer(ALB) 뒤에 있는 두 개의 Amazon EC2 인스턴스에서 실행되는 정적 웹 사이트입니다. 애플리케이션 백엔드는 다른 ALB 뒤에 있는 3개의 EC2 인스턴스에서 실행되는 Python 애플리케이션입니다. EC2 인스턴스는 애플리케이션의 최대 사용량에 대한 온프레미스 사양을 충족하도록 크기가 조정된 대규모 범용 온디맨드 인스턴스입니다.

이 애플리케이션은 매월 평균 수십만 건의 요청을 처리합니다. 그러나 애플리케이션은 주로 점심 시간에 사용되며 나머지 시간에는 트래픽이 최소화됩니다.

솔루션 설계자는 애플리케이션 가용성에 부정적인 영향을 주지 않고 애플리케이션의 인프라 비용을 최적화해야 합니다.

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

A. 기존 EC2 인스턴스와 동일한 수의 코어를 가진 최적화된 인스턴스를 컴퓨팅하도록 모든 EC2 인스턴스를 변경합니다.
B. 애플리케이션 프런트엔드를 Amazon S3에서 호스팅되는 정적 웹 사이트로 이동합니다.

C. AWS Elastic Beanstalk를 사용하여 애플리케이션 프런트엔드를 배포합니다. 노드에 동일한 인스턴스 유형을 사용합니다.
D. 모든 백엔드 EC2 인스턴스를 스팟 인스턴스로 변경합니다.
E. 기존 EC2 인스턴스와 코어 수가 동일한 범용 버스트 가능 EC2 인스턴스에 백엔드 Python 애플리케이션을 배포합니다.

해설
정답: BE

-S3가 EC2 보다 저렴한 스토리지로 Frontend 비용 절감
-Burstable instances 는 CPU 부하가 변화하는 워크로드에 적합하며, 비용 절약 (https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/burstable-credits-baseline-concepts.html)
-Spot Instances 는 가용성 저하 됨(Batch 처리,데이터분석,이미지/비디오 처리등 중단될 수 있는 워크로드에 적합)
-컴퓨팅 최적화 인스턴스가 버스트 가능 인스턴스보다 비쌈

◆ | **Q#0152.** | **Ref#0152.**
한 회사가 AWS에서 이벤트 티켓팅 플랫폼을 운영하고 있으며 플랫폼의 비용 효율성을 최적화하려고 합니다. 이 플랫폼은 Amazon EC2와 함께 Amazon Elastic Kubernetes Service(Amazon EKS)에 배포되며 MySQL DB 인스턴스용 Amazon RDS의 지원을 받습니다. 이 회사는 AWS Fargate를 사용하여 Amazon EKS에서 실행할 수 있는 새로운 애플리케이션 기능을 개발하고 있습니다.

플랫폼은 드물게 높은 수요 피크를 경험합니다. 수요 급증은 이벤트 날짜에 따라 다릅니다.

플랫폼에 가장 비용 효율적인 설정을 제공하는 솔루션은 무엇입니까?

A. EKS 클러스터가 기준 로드에 사용하는 EC2 인스턴스에 대한 표준 예약 인스턴스를 구매하십시오. 피크를 처리하려면 스팟 인스턴스로 클러스터를 확장하세요. 해당 연도의 예상 최대 로드를 충족하려면 데이터베이스에 대한 1년 전체 선결제 예약 인스턴스를 구매하세요.
B. EKS 클러스터의 예상 중간 로드에 대한 Compute Savings Plan을 구매합니다. 피크 이벤트 날짜를 기준으로 온디맨드 용량 예약을 통해 클러스터를 확장합니다. 예측된 기본 로드를 충족하려면 데이터베이스에 대한 '1년 선결제 없음(1-year No Upfront Reserved Instances)' 예약 인스턴스를 구매하세요. 피크 기간 동안 데이터베이스 읽기 복제본을 일시적으로 확장합니다.
C. EKS 클러스터의 예상 기본 로드에 대한 EC2 Instance Savings Plan을 구매합니다. 피크를 처리하려면 스팟 인스턴스로 클러스터를 확장하세요. 예상 기본 로드를 충족하려면 데이터베이스에 대한 1년 전체 선결제 예약 인스턴스를 구매하세요. 피크 기간 동안 일시적으로 DB 인스턴스를 수동으로 확장합니다.
D. EKS 클러스터의 예상 기본 로드에 대한 Compute Savings Plan을 구매합니다. 피크를 처리하려면 스팟 인스턴스로 클러스터를 확장하세요. 예상 기본 로드를 충족하려면 데이터베이스에 대한 1년 전체 선결제 예약 인스턴스를 구매하세요. 피크 기간 동안 일시적으로 DB 인스턴스를 수동으로 확장합니다.

해설
정답: B

Fargate를 사용하여 EKS 실행 App 개발시의 비용 효율화이기 때문에 Fargate를 절약하는 Compute Savings Plan 을 선택

A,C : Sopt 인스턴스는 Production 서버에 부적합
C,D : DB 수동 확장은 불가(peak는 불규칙적이라고 했음)

*Savings Plans 이란?
-1/3년 기간의 사용량 약정(EC2,Lambda,Fargate)
-유형 : Compute Savings Plans, EC2 Instance Savings Plans
.Compute Savings Plans : 최대 66% 절감, 가장 유연한 요금 모델,
Instance Family,Size,AZ,Region,OS,Tenancy 관계 없이 EC2/Lambda,Fargate 사용량에 적용
.EC2 Instance Savings Plans : 한 지역의 개별 인스턴스 패밀리 사용 약정, 최대 72% 절감

*Fargate 란?
-사용량에 따라 요금이 부과되는 서버리스 컴퓨팅 엔진, 서버를 관리할 필요가 없기 때문에 애플리케이션 구축에 집중
-ECS,EKS 호환

◆ | **Q#0153.** | **Ref#0153.**
한 회사가 AWS Elastic Beanstalk에 애플리케이션을 배포했습니다. 애플리케이션은 데이터베이스 계층에 Amazon Aurora를 사용합니다. Amazon CloudFront 배포는 웹 요청을 처리하고 Elastic Beanstalk 도메인 이름을 오리진(Origin) 서버로 포함합니다. 배포는 방문자가 애플리케이션에 액세스할 때 사용하는 대체 도메인 이름으로 구성됩니다.

매주 회사는 정기 유지 관리를 위해 애플리케이션 서비스를 중단합니다. 애플리케이션을 사용할 수 없는 동안 회사에서는 방문자가 CloudFront 오류 메시지 대신 정보 메시지를 받기를 원합니다.

솔루션 아키텍트는 프로세스의 첫 번째 단계로 Amazon S3 버킷을 생성합니다.

솔루션 설계자가 요구 사항을 충족하기 위해 다음에 수행해야 하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. S3 버킷에 정적 정보 콘텐츠를 업로드합니다.
B. 새로운 CloudFront 배포판을 생성합니다. S3 버킷을 원본으로 설정합니다.
C. S3 버킷을 원래 CloudFront 배포의 두 번째 오리진으로 설정합니다. OAI(원본 액세스 ID)를 사용하도록 배포 및 S3 버킷을 구성합니다.
D. 주간 유지 관리 중에 S3 오리진을 사용하도록 기본 캐시 동작을 편집합니다. 유지 관리가 완료되면 변경 사항을 되돌립니다.
E. 주간 유지 관리 중에 새 배포에서 S3 원본에 대한 캐시 동작을 만듭니다. 경로 패턴을 \로 설정합니다. 우선 순위를 0으로 설정합니다. 유지 관리가 완료되면 캐시 동작을 삭제합니다.
F. 주간 유지 관리 중에 S3 버킷의 트래픽을 제공하도록 Elastic Beanstalk를 구성합니다.

해설
정답: ACD

App 사용할 수 없는 동안 방문자가 CloudFront 오류 메시지 대신 정보 메시지를 보여주려 할때는??

-1단계: 정적 정보 콘텐츠를 S3 버킷에 업로드
-2단계: S3 버킷을 원래 CloudFront 배포의 두 번째 오리진으로 설정
S3 버킷을 안전하게 유지하려면 원본 액세스 ID(OAI)를 사용하도록 배포 및 S3 버킷을 구성
이렇게 하면 CloudFront만 S3 버킷에 액세스할 수 있다.
-3단계: 주간 유지 관리 중에 솔루션 설계자는 S3 원본을 사용하도록 CloudFront 배포의 기본 캐시 동작을 편집해야 한다.
이렇게 하면 들어오는 모든 트래픽이 S3 버킷으로 리디렉션되고 정적 정보 콘텐츠가 사용자에게 표시 된다.

*Elastic Beanstalk 이란?
-App 신속 배포/관리
-용량 프로비저닝,로그 밸런싱,조정,모니터링

-GO,Java,.NET,Node.js,PHP,Python 개발 App 지원

*CloudFront 란?
-.html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹 서비스

◆ | **Q#0154.** | **Ref#0154.**
회사는 사용자에게 맞춤형 애플리케이션에서 이미지를 업로드할 수 있는 기능을 제공합니다. 업로드 프로세스는 Amazon S3 버킷에서 이미지를 처리하고 저장하는 AWS Lambda 함수를 호출합니다. 애플리케이션은 특정 함수 버전 ARN을 사용하여 Lambda 함수를 호출합니다.

Lambda 함수는 환경 변수를 사용하여 이미지 처리 매개변수를 허용합니다. 회사에서는 최적의 이미지 처리 출력을 얻기 위해 Lambda 함수의 환경 변수를 조정하는 경우가 많습니다. 회사는 다양한 매개변수를 테스트하고 결과를 검증한 후 업데이트된 환경 변수를 사용하여 새 기능 버전을 게시합니다. 또한 이 업데이트 프로세스에서는 새 기능 버전 ARN을 호출하기 위해 사용자 지정 애플리케이션을 자주 변경해야 합니다. 이러한 변경으로 인해 사용자가 중단될 수 있습니다.

솔루션 설계자는 사용자의 업무 중단을 최소화하기 위해 이 프로세스를 단순화해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 게시된 Lambda 함수 버전의 환경 변수를 직접 수정합니다. SLAEST 버전을 사용하여 이미지 처리 매개변수를 테스트하세요.
B. 이미지 처리 매개변수를 저장할 Amazon DynamoDB 테이블을 생성합니다. DynamoDB 테이블에서 이미지 처리 매개변수를 검색하도록 Lambda 함수를 수정합니다.
C. Lambda 함수 내에서 이미지 처리 매개변수를 직접 코딩하고 환경 변수를 제거합니다. 회사에서 매개변수를 업데이트하면 새 기능 버전을 게시합니다.
D. Lambda 함수 별칭을 생성합니다. 함수 별칭 ARN을 사용하도록 클라이언트 애플리케이션을 수정합니다. 회사에서 테스트가 완료되면 함수의 새 버전을 가리키도록 Lambda 별칭을 재구성합니다.

해설
정답: D

함수 별칭을 사용하면 사용자 지정 App은 회사에서 이미지 처리 매개 변수를 업데이트할 때마다 App 코드 수정 없이 최신 버전의 Lambda 함수 호출 한다.
(https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html)

◆ | **Q#0155.** | **Ref#0155.**
글로벌 미디어 회사가 애플리케이션을 여러 AWS 리전에 배포하려고 합니다. 사용자의 경험을 두 대륙에서 일관되게 유지하기 위해 Amazon DynamoDB 글로벌 테이블을 사용할 예정입니다. 각 배포는 퍼블릭 애플리케이션 로드 밸런서(ALB)를 갖게 되며, 회사는 퍼블릭 DNS를 내부적으로 관리하고 있습니다. 회사는 애플리케이션을 Apex 도메인을 통해 사용할 수 있도록 하고 싶습니다.

최소한의 노력으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 퍼블릭 DNS를 Amazon Route 53으로 마이그레이션합니다. ALB를 가리키도록 apex 도메인에 대한 CNAME 레코드를 생성합니다. 지리적 위치 라우팅 정책을 사용하여 사용자 위치에 따라 트래픽을 라우팅합니다.
B. ALB 앞에 네트워크 로드 밸런서(NLB)를 배치합니다. 퍼블릭 DNS를 Amazon Route 53으로 마이그레이션합니다. Apex 도메인이 NLB의 정적 IP 주소를 가리키도록 CNAME 레코드를 생성합니다. Geolocation 라우팅 정책을 사용하여 사용자 위치에 따라 트래픽을 라우팅합니다.

C. 여러 엔드포인트 그룹을 타겟으로 하는 AWS Global Accelerator를 생성합니다. Global Accelerator의 정적 IP 주소를 사용하여 퍼블릭 DNS에서 Apex 도메인의 레코드를 생성합니다.
D. AWS 지역 중 하나에서 AWS Lambda가 지원하는 Amazon API Gateway API를 생성합니다. 라운드 로빈 방법을 사용하여 애플리케이션 배포로 트래픽을 라우팅하도록 Lambda 함수를 구성합니다. API의 URL을 가리키도록 apex 도메인에 대한 CNAME 레코드를 생성합니다.

해설
정답: C

AWS Global Accelerator를 사용하면 여러 리전에서 애플리케이션의 엔드포인트를 지정하고, 사용자에게 가장 가까운 리전으로 트래픽을 라우팅할 수 있음.
또한 Global Accelerator의 정적 IP 주소를 사용하여 Apex 도메인에 대한 퍼블릭 DNS 레코드를 생성할 수 있음.
이 방법은 지리적 위치 기반 라우팅을 자동으로 처리하고, 퍼블릭 DNS를 Route 53으로 마이그레이션할 필요 없이 쉽게 설정할 수 있음.

◆ | **Q#0156.** | **Ref#0156.**
한 회사가 Amazon API Gateway와 AWS Lambda를 사용하여 새로운 서버리스 API를 개발하고 있습니다. 회사는 여러 공유 라이브러리와 사용자 지정 클래스를 사용하기 위해 Lambda 기능을 API 게이트웨이와 통합했습니다.

솔루션 설계자는 솔루션 배포를 단순화하고 코드 재사용을 최적화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 공유 라이브러리와 사용자 정의 클래스를 Docker 이미지에 배포합니다. 이미지를 S3 버킷에 저장합니다. Docker 이미지를 소스로 사용하는 Lambda 계층을 생성합니다. API의 Lambda 함수를 Zip 패키지로 배포합니다. Lambda 계층을 사용하도록 패키지를 구성합니다.
B. 공유 라이브러리와 사용자 정의 클래스를 Docker 이미지에 배포합니다. Amazon Elastic Container Registry(Amazon ECR)에 이미지를 업로드합니다. Docker 이미지를 소스로 사용하는 Lambda 계층을 생성합니다. API의 Lambda 함수를 Zip 패키지로 배포합니다. Lambda 계층을 사용하도록 패키지를 구성합니다.
C. AWS Fargate 시작 유형을 사용하여 Amazon Elastic Container Service(Amazon ECS)의 Docker 컨테이너에 공유 라이브러리 및 사용자 지정 클래스를 배포합니다. API의 Lambda 함수를 Zip 패키지로 배포합니다. 배포된 컨테이너를 Lambda 계층으로 사용하도록 패키지를 구성합니다.
D. API의 Lambda 함수에 대한 공유 라이브러리, 사용자 지정 클래스 및 코드를 Docker 이미지에 배포합니다. Amazon Elastic Container Registry(Amazon ECR)에 이미지를 업로드합니다. Docker 이미지를 배포 패키지로 사용하도록 API의 Lambda 함수를 구성합니다.

해설
정답: D

AWS Lambda 계층은 Docker 이미지 또는 배포된 컨테이너를 소스로 지원하지 않기에 ABC는 불가
(https://docs.aws.amazon.com/lambda/latest/dg/configuration-layers.html)

◆ | **Q#0157.** | **Ref#0157.**
한 제조 회사가 공장용 검사 솔루션을 구축하고 있습니다. 이 회사는 각 조립 라인 끝에 IP 카메라를 설치했습니다. 이 회사는 Amazon SageMaker를 사용하여 기계 학습(ML) 모델을 훈련하여 정지 이미지에서 일반적인 결함을 식별했습니다.

회사에서는 결함이 발견되면 공장 작업자에게 현지 피드백을 제공하려고 합니다. 회사는 공장의 인터넷 연결이 끊어진 경우에도 이러한 피드백을 제공할 수 있어야 합니다. 회사에는 작업자에게 로컬 피드백을 제공하는 API를 호

스팅하는 로컬 Linux 서버가 있습니다.

회사는 이러한 요구 사항을 충족하기 위해 ML 모델을 어떻게 배포해야 합니까?

> **A.** 각 IP 카메라에서 AWS로 Amazon Kinesis 비디오 스트림을 설정합니다. Amazon EC2 인스턴스를 사용하여 스트림의 정지 이미지를 찍습니다. Amazon S3 버킷에 이미지를 업로드합니다. ML 모델을 사용하여 SageMaker 엔드포인트를 배포합니다. 새 이미지가 업로드되면 AWS Lambda 함수를 호출하여 추론 엔드포인트를 호출합니다. 결함이 감지되면 로컬 API를 호출하도록 Lambda 함수를 구성합니다.
> **B.** 로컬 서버에 AWS IoT Greengrass를 배포합니다. ML 모델을 Greengrass 서버에 배포합니다. Greengrass 구성 요소를 생성하여 카메라에서 스틸 이미지를 가져와 추론을 실행합니다. 결함이 감지되면 로컬 API를 호출하도록 구성 요소를 구성합니다.
> **C.** AWS Snowball 디바이스를 주문합니다. SageMaker 엔드포인트, ML 모델 및 Amazon EC2 인스턴스를 Snowball 디바이스에 배포합니다. 카메라에서 정지 이미지를 가져옵니다. EC2 인스턴스에서 추론을 실행합니다. 결함이 감지되면 로컬 API를 호출하도록 인스턴스를 구성합니다.
> **D.** 각 IP 카메라에 Amazon Monitron 장치를 배포합니다. Amazon Monitron Gateway를 온프레미스에 배포합니다. ML 모델을 Amazon Monitron 디바이스에 배포합니다. 결함이 감지되면 Amazon Monitron 상태 경보를 사용하여 AWS Lambda 함수에서 로컬 API를 호출합니다.
>
> 해설
> 정답: B
>
> 오프라인 작업 지원이 가능한 방법을 찾는 문제로 "IoT Greengrass" 을 선택
>
> *AWS IoT Greengrass는 클라우드 기능을 로컬 디바이스로 확장하는 소프트웨어입니다.
> 이를 통해 장치는 정보 소스에 더 가까운 데이터를 수집 및 분석하고, 로컬 이벤트에 자율적으로 반응하고,로컬 네트워크에서 서로 안전하게 통신할 수 있습니다. 로컬 장치는 AWS IoT Core와 안전하게 통신하고 IoT 데이터를 AWS 클라우드로 내보낼 수도 있습니다.
> AWS IoT Greengrass 개발자는 AWS Lambda 함수와 사전 구축된 커넥터를 사용하여 로컬 실행을 위해 디바이스에 배포되는 서버리스 애플리케이션을 생성할 수 있습니다.

◆ | **Q#0158.** | **Ref#0158.**
솔루션 아키텍트는 회사의 온프레미스 데이터 센터를 AWS 클라우드로 마이그레이션하기 위한 비즈니스 사례를 만들어야 합니다. 솔루션 설계자는 회사의 모든 서버에 대한 CMDB(구성 관리 데이터베이스) 내보내기를 사용하여 사례를 생성합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** AWS Well-Architected Tool을 사용하여 CMDB 데이터를 가져와 분석을 수행하고 권장 사항을 생성합니다.
> **B.** 마이그레이션 평가기(Migration Evaluator)를 사용하여 분석을 수행합니다. 데이터 가져오기 템플릿을 사용하여 CMDB 내보내기에서 데이터를 업로드합니다.
> **C.** 자원 일치 규칙을 구현합니다. CMDB 내보내기 및 AWS Price List Bulk API를 사용하여 AWS 서비스에 대한 CMDB 데이터를 대량으로 쿼리합니다.
> **D.** AWS Application Discovery Service를 사용하여 CMDB 데이터를 가져와 분석을 수행합니다.
>
> 해설
> 정답: B
>
> AWS Migration Evaluator는 서버, 스토리지, 네트워킹, 애플리케이션을 포함한 현재 온프레미스 환경에 대한 데이터를 분석하여 작동.
> 그런 다음 기존 인프라 및 애플리케이션에 가장 잘 맞는 권장 AWS 서비스 및 구성을 간략하게 설명

하는 보고서를 제공.
이 보고서에는 AWS 클라우드에서 애플리케이션을 실행하는데 드는 총 비용을 추정하는 자세한 비용 분석이 포함되어 있음.

A: AWS 아키텍처를 평가하는 데 사용되는 설문지 도구
C: 복잡한 애플리케이션을 생성해야 함
D: Application Discovery는 무료이며 CMDB 가져오기를 지원하지만 계획만 제공할 수 있고 비즈니스 사용 사례는 제공할 수 없음
B: 무료이며 비즈니스 사용 사례를 만드는 데 도움이 됨

◆ | **Q#0159.** | **Ref#0159.**
ALB(Application Load Balancer) 뒤에 Amazon EC2 인스턴스에서 실행되는 웹 사이트가 있는 회사가 있습니다. 인스턴스는 Auto Scaling 그룹에 있습니다. ALB는 AWS WAF 웹 ACL과 연결되어 있습니다.

웹사이트는 애플리케이션 계층에서 공격을 받는 경우가 많습니다. 공격으로 인해 애플리케이션 서버의 트래픽이 갑자기 크게 증가합니다. 액세스 로그는 각 공격이 서로 다른 IP 주소에서 시작되었음을 보여줍니다. 솔루션 설계자는 이러한 공격을 완화하기 위한 솔루션을 구현해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 서버 액세스를 모니터링하는 Amazon CloudWatch 경보를 생성하십시오. IP 주소별 액세스를 기반으로 임계값을 설정합니다. 웹 ACL의 거부 목록에 IP 주소를 추가하는 경보 작업을 구성합니다.
B. AWS WAF 외에 AWS Shield Advanced를 배포합니다. ALB를 보호된 리소스로 추가합니다.
C. 사용자 IP 주소를 모니터링하는 Amazon CloudWatch 경보를 생성합니다. IP 주소별 액세스를 기반으로 임계값을 설정합니다. AWS Lambda 함수를 호출하여 경보를 활성화하는 모든 IP 주소에 대해 애플리케이션 서버의 서브넷 라우팅 테이블에 거부 규칙을 추가하도록 경보를 구성합니다.
D. 액세스 로그를 검사하여 공격을 시작한 IP 주소의 패턴을 찾습니다. Amazon Route 53 지리적 위치 라우팅 정책을 사용하여 해당 IP 주소를 호스팅하는 국가의 트래픽을 거부합니다.

해설
정답: B

AWS Shield Advanced는 DDoS 공격으로부터 보호하는 데 중점을 두고 있는 반면, AWS WAF는 웹 공격으로부터 보호하는 데 중점을 두고 있다.
두 서비스를 함께 사용하면 애플리케이션에 대한 포괄적인 보호를 할수 있다.
(https://docs.aws.amazon.com/waf/latest/developerguide/ddos-app-layer-protections.html)

◆ | **Q#0160.** | **Ref#0160.**
회사에는 데이터 계층이 단일 AWS 지역(single AWS Region)에 배포되는 중요한 애플리케이션이 있습니다. 데이터 계층은 Amazon DynamoDB 테이블과 Amazon Aurora MySQL DB 클러스터를 사용합니다. 현재 Aurora MySQL 엔진 버전은 글로벌 데이터베이스를 지원합니다. 애플리케이션 계층은 이미 두 리전에 배포되었습니다.

회사 정책에 따르면 중요한 애플리케이션에는 애플리케이션 계층 구성 요소와 데이터 계층 구성 요소가 두 Regions에 걸쳐 배포되어야 합니다. RTO 및 RPO는 각각 몇 분 이하여야 합니다. 솔루션 설계자는 데이터 계층이 회사 정책을 준수하도록 하는 솔루션을 권장해야 합니다.

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

A. Aurora MySQL DB 클러스터에 다른 리전 추가
B. Aurora MySQL DB 클러스터의 각 테이블에 다른 리전을 추가합니다.
C. DynamoDB 테이블 및 Aurora MySQL DB 클러스터에 대한 예약된 교차 리전 백업 설정
D. 구성에 다른 리전을 추가하여 기존 DynamoDB 테이블을 글로벌 테이블로 변환합니다.

E. Amazon Route 53 애플리케이션 복구 컨트롤러를 사용하여 데이터베이스 백업 및 보조 지역으로의 복구를 자동화합니다.

해설
정답: A,D

데이터와 애플리케이션 서버 모두 두개 Regions에 배포 되고 RTO/RPO가 몇분이내여야 한다.
이 구성을 위해서는 DynamoDB의 경우는 전역 테이블(Global Table) 사용하고,
Aurora는 Region간 읽기 전용 복제본을 사용한다.

*Amazon DynamoDB 글로벌 테이블은 완전관리형 다중 리전 다중 활성 데이터베이스 옵션으로, 대규모로 확장되는 글로벌 애플리케이션에 빠른 로컬 읽기 및 쓰기 성능을 지원
글로벌 테이블은 복제 솔루션을 직접 구축하여 관리하지 않고도 다중 리전의 다중 활성 데이터베이스를 배포할 수 있는 완전관리형 솔루션을 제공
(https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html)
(https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html)

161 (김성원) 3회차 完

◆ | **Q#0161.** | **Ref#0161.**
한 통신회사가 AWS에서 애플리케이션을 실행하고 있습니다. 회사는 회사의 온프레미스 데이터 센터와 AWS 간에 AWS Direct Connect 연결을 설정했습니다. 이 회사는 내부 ALB(Application Load Balancer) 뒤의 여러 가용 영역에 있는 Amazon EC2 인스턴스에 애플리케이션을 배포했습니다. 회사의 클라이언트는 HTTPS를 사용하여 온프레미스 네트워크에서 연결합니다. TLS(Transport Layer Security 전송계층 보안)는 ALB에서 종료됩니다. 회사에는 여러 대상 그룹이 있으며 경로 기반 라우팅을 사용하여 URL 경로를 기반으로 요청을 전달합니다.

회사는 IP 주소를 기반으로 하는 허용 목록을 사용하여 온프레미스 방화벽 어플라이언스를 배포할 계획입니다. 솔루션 아키텍트는 클라이언트가 애플리케이션에 계속 액세스할 수 있도록 온프레미스 네트워크에서 AWS로의 트래픽 흐름을 허용하는 솔루션을 개발해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 고정 IP 주소를 사용하도록 기존 ALB를 구성합니다. 여러 가용 영역의 IP 주소를 ALB에 할당합니다. ALB IP 주소를 방화벽 어플라이언스에 추가하십시오.
B. 네트워크 로드 밸런서(NLB)를 생성합니다. NLB를 여러 가용 영역에 있는 하나의 고정 IP 주소와 연결합니다. NLB에 대한 ALB 유형 대상 그룹을 생성하고 기존 ALB를 추가합니다. 방화벽 어플라이언스에 NLB IP 주소를 추가합니다. NLB에 연결하도록 클라이언트를 업데이트합니다.
C. 네트워크 로드 밸런서(NLB)를 생성합니다. NLB를 여러 가용 영역에 있는 하나의 고정 IP 주소와 연결합니다. NLB에 기존 대상 그룹을 추가합니다. NLB에 연결하도록 클라이언트를 업데이트합니다. ALB 삭제 방화벽 어플라이언스에 NLB IP 주소를 추가합니다.
D. 게이트웨이 로드 밸런서(GWLB)를 생성합니다. 여러 가용 영역의 GWLB에 고정 IP 주소를 할당합니다. GWLB에 대한 ALB 유형 대상 그룹을 생성하고 기존 ALB를 추가합니다. 방화벽 어플라이언스에 GWLB IP 주소를 추가합니다. GWLB에 연결하도록 클라이언트를 업데이트합니다.

해설
정답: B

내부 어플리케이션 로드 밸런서를 사용하는 경우, 고정 IP를 사용할 수 없습니다.
ALB를 사용하던 애플리케이션을 유지하면서 고정 IP가 필요한 경우 네트워크 로드 밸런서(NLB)를

생성하고 이에 대한 고정 IP를 할당해야 합니다.
그런 다음, NLB의 대상 그룹을 ALB 타입으로 생성하고, 기존 ALB를 추가합니다.
이렇게 하면 온프레미스 네트워크에서의 트래픽이 NLB를 거쳐 ALB로 이동하고, 여기서 요청은 경로 기반 라우팅 규칙을 따라 적절한 대상 그룹으로 전달됩니다.
마지막으로 방화벽 장비에 NLB의 IP 주소를 추가하고, 클라이언트에게 NLB로의 연결을 업데이트하면 됩니다.

◆ | **Q#0162.** | **Ref#0162.**
회사는 인터넷 연결 ALB(Application Load Balancer) 뒤의 프라이빗 서브넷에 있는 Amazon EC2 인스턴스 집합에서 애플리케이션을 실행합니다. ALB는 Amazon CloudFront 배포의 오리진입니다. 다양한 AWS 관리형 규칙을 포함하는 AWS WAF 웹 ACL은 CloudFront 배포와 연결됩니다.

회사에는 인터넷 트래픽이 ALB에 직접 액세스하는 것을 방지하는 솔루션이 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 기존 웹 ACL에 포함된 것과 동일한 규칙을 포함하는 새 웹 ACL을 생성합니다. 새 웹 ACL을 ALB와 연결합니다.
B. 기존 웹 ACL을 ALB와 연결합니다.
C. CloudFront에 대해서만 AWS 관리형 접두사 목록의 트래픽을 허용하도록 ALB에 보안 그룹 규칙을 추가합니다.
D. 다양한 CloudFront IP 주소 범위만 허용하도록 ALB에 보안 그룹 규칙을 추가합니다.

해설
정답: C

Internet-facing ALB를 개방하지 않기 위한 가장 적절하고 운영적 오버헤드가 작은 방법은 ALB에 보안 그룹(Security Group) 규칙을 추가하여 CloudFront에서만 트래픽을 허용하는 것입니다.
이렇게 하면 직접 ALB로의 인터넷 접근을 차단하고, CloudFront를 통해서만 해당 서비스에 접근할 수 있도록 할 수 있습니다.
AWS 관리형 CloudFront 접두사 목록은 CloudFront 엣지 위치의 IP 주소 범위를 포함하고 있으며, 이를 이용하면 간단하게 CloudFront 에서만 트래픽을 허용하는 보안 그룹 규칙을 생성할 수 있습니다.

◆ | **Q#0163.** | **Ref#0163.**
한 회사에서 Redis용 Amazon ElastiCache 클러스터를 캐싱 계층으로 사용하는 애플리케이션을 실행하고 있습니다. 최근 보안 감사에서 회사가 ElastiCache에 대해 저장 암호화를 구성한 것으로 나타났습니다. 그러나 회사에서는 전송 중 암호화를 사용하도록 ElastiCache를 구성하지 않았습니다. 또한 사용자는 인증 없이 캐시에 액세스할 수 있습니다.

솔루션 설계자는 사용자 인증을 요구하고 회사가 종단 간 암호화를 사용하도록 변경해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AUTH 토큰을 생성합니다. AWS System Manager Parameter Store에 토큰을 암호화된 파라미터로 저장합니다. AUTH를 사용하여 새 클러스터를 생성하고 전송 중 암호화를 구성합니다. 필요한 경우 Parameter Store에서 AUTH 토큰을 검색하고 인증에 AUTH 토큰을 사용하도록 애플리케이션을 업데이트합니다.
B. AUTH 토큰을 생성합니다. AWS Secrets Manager에 토큰을 저장합니다. AUTH 토큰을 사용하도록 기존 클러스터를 구성하고 전송 중 암호화를 구성합니다. 필요한 경우 Secrets Manager에서 AUTH 토큰을 검색하고 인증에 AUTH 토큰을 사용하도록 애플리케이션을 업데이트합니다.
C. SSL 인증서를 생성합니다. AWS Secrets Manager에 인증서를 저장합니다. 새 클러스터를 생성하고 전송 중 암호화를 구성합니다. 필요한 경우 Secrets Manager에서 SSL 인증서를 검색하고 인증에 인증서를 사용하도록 애플리케이션을 업데이트합니다.

D. SSL 인증서를 생성합니다. 암호화된 고급 파라미터로 AWS Systems Manager Parameter Store에 인증서를 저장합니다. 전송 중 암호화를 구성하려면 기존 클러스터를 업데이트하세요. 필요한 경우 Parameter Store에서 SSL 인증서를 검색하고 인증에 인증서를 사용하도록 애플리케이션을 업데이트합니다.

해설
정답: B

AUTH 토큰 생성 및 저장: 이 옵션은 Redis AUTH 토큰을 생성하고 AWS Secrets Manager에 안전하게 저장합니다. Secrets Manager는 보안 자격 증명을 관리하고 필요할 때 이를 안전하게 검색할 수 있는 서비스입니다.
기존 클러스터 구성: 기존 ElastiCache 클러스터를 수정하여 AUTH 토큰을 사용하도록 설정하고 전송 중 암호화를 활성화할 수 있습니다. 클러스터를 재생성하지 않고도 이러한 보안 설정을 추가할 수 있어 운영 부담을 줄입니다.
Secrets Manager 통합: 애플리케이션은 필요할 때 Secrets Manager에서 토큰을 안전하게 검색하여 인증에 사용할 수 있습니다. 이는 보안과 관리 편의성을 높여줍니다.

◆ | **Q#0164.** | **Ref#0164.**
회사는 Auto Scaling 그룹에 속한 Amazon EC2 스팟 인스턴스를 사용하여 컴퓨팅 워크로드를 실행하고 있습니다. 시작 템플릿은 두 개의 배치 그룹과 단일 인스턴스 유형을 사용합니다.

최근 모니터링 시스템에서는 시스템 사용자의 대기 시간이 길어지는 것과 관련된 Auto Scaling 인스턴스 시작 실패를 보고했습니다. 회사는 워크로드의 전반적인 안정성을 개선해야 합니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 속성 기반 인스턴스 유형 선택을 사용하는 Auto Scaling 그룹을 사용하려면 시작 템플릿을 시작 구성으로 바꾸십시오.
B. 속성 기반 인스턴스 유형 선택을 사용하는 새로운 시작 템플릿 버전을 생성합니다. 새로운 시작 템플릿 버전을 사용하도록 Auto Scaling 그룹을 구성합니다.
C. 시작 템플릿 Auto Scaling 그룹을 업데이트하여 배치 그룹 수를 늘립니다.
D. 더 큰 인스턴스 유형을 사용하도록 시작 템플릿을 업데이트합니다.

해설
정답: B

Auto Scaling 그룹이 인스턴스 시작에 실패하면 신뢰성 있는 플랫폼을 제공하기 위해 인스턴스 타입 선택을 개선해야 합니다. AWS에서는 속성 기반의 인스턴스 타입 선택을 사용하는 것을 추천하며, 이를 사용하면 CPU, 메모리, 스토리지 등의 특성에 따라 인스턴스 타입을 선택할 수 있습니다. 이를 위해서는 기존의 런치 템플릿을 수정하는 대신 새로운 런치 템플릿 버전을 생성하고, Auto Scaling 그룹이 이 새로운 버전의 런치 템플릿을 사용하도록 설정해야 합니다.

◆ | **Q#0165.** | **Ref#0165.**
한 회사가 문서 처리 워크로드를 AWS로 마이그레이션하고 있습니다. 이 회사는 기본적으로 Amazon S3 API를 사용하여 처리 서버가 초당 약 5개의 문서를 생성하는 문서를 저장, 검색 및 수정하도록 많은 애플리케이션을 업데이트했습니다. 문서 처리가 완료된 후 고객은 Amazon S3에서 직접 문서를 다운로드할 수 있습니다.

마이그레이션 중에 회사는 S3 API를 지원하기 위해 많은 문서를 생성하는 처리 서버를 즉시 업데이트할 수 없다는 사실을 발견했습니다. 서버는 Linux에서 실행되며 서버가 생성하고 수정하는 파일에 대한 빠른 로컬 액세스가 필요합니다. 서버가 처리를 마치면 30분 이내에 파일을 대중이 다운로드할 수 있어야 합니다.

최소한의 노력으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 애플리케이션을 AWS Lambda 함수로 마이그레이션합니다. Java용 AWS SDK를 사용하면 회사가 Amazon S3에 직접 저장하는 파일을 생성, 수정 및 액세스할 수 있습니다.
B. Amazon S3 파일 게이트웨이를 설정하고 문서 저장소에 연결된 파일 공유를 구성합니다. NFS를 사용하여 Amazon EC2 인스턴스에 파일 공유를 탑재합니다. Amazon S3에서 변경 사항이 발생하면 RefreshCache API 호출을 시작하여 S3 파일 게이트웨이를 업데이트합니다.
C. 가져오기 및 내보내기 정책을 사용하여 Lustre용 Amazon FSx를 구성합니다. 새 파일 시스템을 S3 버킷에 연결합니다. Lustre 클라이언트를 설치하고 NFS를 사용하여 Amazon EC2 인스턴스에 문서 저장소를 탑재합니다.
D. Amazon EC2 인스턴스에 연결하도록 AWS DataSync를 구성합니다. 생성된 파일을 Amazon S3와 동기화하는 작업을 구성합니다.

해설
정답: B

A(x): Lambda로 마이그레이션하려면 많은 작업이 필요하며 파일에 대한 빠른 액세스 요구가 해결되지 않습니다.
C(x): Lustre용 FSx는 NFS를 지원하지 않습니다.
D(x): DataSynch는 매시간, 매일 또는 매주 전송을 예약할 수 있지만 시간당 한 번보다 빠르게 실행할 수 없습니다.
B: Amazon S3 파일 게이트웨이는 현재 구성된 서버 환경에 S3와의 간단한 통합을 제공하는 서비스입니다.
이는 기존 서버 구성에 별다른 변경 없이 Amazon S3와의 연동을 가능케 하며, 이후 S3에서 직접 파일을 제공할 수 있게 됩니다.

◆ | **Q#0166.** | **Ref#0166.**
배송 회사가 AWS 클라우드에서 서버리스 솔루션을 실행하고 있습니다. 사용자 데이터, 배송정보, 과거 구매내역 등을 관리하는 솔루션입니다. 솔루션은 여러 마이크로서비스로 구성됩니다. 중앙 사용자 서비스는 중요한 데이터를 Amazon DynamoDB 테이블에 저장합니다. 다른 마이크로서비스 중 일부는 민감한 데이터의 일부 복사본을 다른 스토리지 서비스에 저장합니다.

회사는 요청 시 사용자 정보를 삭제할 수 있는 권한이 필요합니다. 중앙 사용자 서비스가 사용자를 삭제하자마자 다른 모든 마이크로서비스도 해당 데이터 사본을 즉시 삭제해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. DynamoDB 테이블에서 DynamoDB 스트림을 활성화합니다. Amazon Simple Queue Service(Amazon SQS) 대기열의 사용자 삭제에 대한 이벤트를 게시하는 DynamoDB 스트림에 대한 AWS Lambda 트리거를 생성합니다. 대기열을 폴링하고 DynamoDB 테이블에서 사용자를 삭제하도록 각 마이크로서비스를 구성합니다.
B. DynamoDB 테이블에 DynamoDB 이벤트 알림을 설정합니다. DynamoDB 이벤트 알림의 대상으로 Amazon Simple 알림 서비스(Amazon SNS) 주제를 생성합니다. SNS 주제를 구독하고 DynamoDB 테이블에서 사용자를 삭제하도록 각 마이크로서비스를 구성합니다.
C. 회사가 사용자를 삭제할 때 사용자 지정 Amazon EventBridge 이벤트 버스에 이벤트를 게시하도록 중앙 사용자 서비스를 구성합니다. 사용자 삭제 이벤트 패턴과 일치하도록 각 마이크로서비스에 대한 EventBridge 규칙을 생성하고 마이크로서비스에서 로직을 호출하여 DynamoDB 테이블에서 사용자를 삭제합니다.
D. 회사가 사용자를 삭제할 때 Amazon Simple Queue Service(Amazon SQS) 대기열에 메시지를 게시하도록 중앙 사용자 서비스를 구성합니다. SQS 대기열에 이벤트 필터를 생성하고 DynamoDB 테이블에서 사용자를 삭제하도록 각 마이크로서비스를 구성합니다.

해설

정답: C

Amazon EventBridge는 AWS, 장외 서비스, 어플리케이션에서 발생하는 모든 종류의 이벤트를 함께 처리하기 위한 서버 리스 이벤트 버스입니다. EventBridge를 사용하면, 특정 이벤트 패턴에 일치하는 규칙을 사용하여 로직을 처리할 수 있습니다. 중앙 사용자 서비스에서 사용자 정보를 삭제할 때마다 이를 EventBridge에서 디텍팅하고, 해당 이벤트가 발생했음을 모든 마이크로서비스에 알릴 수 있습니다. 이 방법은 사용자 데이터의 삭제를 신속하게 동기화하는데 가장 효과적입니다.

◆ | **Q#0167.** | **Ref#0167.**
회사가 VPC에서 웹 애플리케이션을 실행하고 있습니다. 웹 애플리케이션은 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스 그룹에서 실행됩니다. ALB는 AWS WAF를 사용하고 있습니다.

외부 고객이 웹 애플리케이션에 연결해야 합니다. 회사는 모든 외부 고객에게 IP 주소를 제공해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. ALB를 NLB(Network Load Balancer)로 교체합니다. NLB에 탄력적 IP 주소를 할당합니다.
B. 탄력적 IP 주소를 할당합니다. 탄력적 IP 주소를 ALP에 할당합니다. 탄력적 IP 주소를 고객에게 제공합니다.
C. AWS Global Accelerator 표준 액셀러레이터를 생성합니다. ALB를 가속기의 엔드포인트로 지정합니다. 고객에게 가속기의 IP 주소를 제공합니다.
D. Amazon CloudFront 배포를 구성합니다. ALB를 원점으로 설정합니다. 배포의 공용 IP 주소를 확인하려면 배포의 DNS 이름을 핑합니다. 고객에게 IP 주소를 제공합니다.

해설
정답: C

A(x): AWS WAF는 NLB와의 연결을 지원하지 않습니다.
B(x): ALB는 탄력적 IP를 연결할 수 없으며, ALB는 고정 IP를 전혀 가질 수 없습니다.
D(x): CloudFront 배포판은 많은 IP에서 응답하며, AWS는 이에 대한 접두사 목록을 관리합니다. 고객 측에서 구성하기 쉽지 않음
C: AWS Global Accelerator는 고객에게 두 개의 정적 IP 주소를 제공합니다. 이를 통해 외부 고객은 웹 애플리케이션에 연결할 수 있습니다.
이는 로드 밸런서나 EC2 인스턴스에 직접적으로 Elastic IP를 할당하는 것보다 운영 부하를 줄여줍니다.
Global Accelerator는 또한 높은 가용성 및 안정성을 제공하는 AWS의 전 세계적인 네트워크를 활용합니다.

◆ | **Q#0168.** | **Ref#0168.**
회사에는 개발용 AWS 계정이 몇 개 있고 프로덕션 애플리케이션을 AWS로 이전하려고 합니다. 회사는 미사용 중인 현재 프로덕션 계정과 향후 프로덕션 계정에만 Amazon Elastic Block Store(Amazon EBS) 암호화를 적용해야 합니다. 회사에는 기본 제공 청사진과 가드레일이 포함된 솔루션이 필요합니다.

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

A. AWS CloudFormation StackSets를 사용하여 프로덕션 계정에 AWS Config 규칙을 배포하십시오.
B. 기존 개발자 계정에 새로운 AWS Control Tower 랜딩 존을 생성합니다. 계정을 위한 조직 단위(OUs)를 만듭니다. 프로덕션 계정과 개발 계정을 각각 프로덕션 및 개발 조직 단위(OUs)에 추가합니다.
C. 회사의 관리 계정에 새로운 AWS Control Tower 랜딩 존을 만듭니다. 프로덕션 및 개발 계정을 각각 프로덕션 및 개발 조직 단위(OUs)에 추가합니다.
D. 기존 계정을 초대하여 AWS Organizations의 조직에 가입합니다. 규정 준수를 보장하기 위해 SCP

를 생성하세요.
E. EBS 암호화를 탐지하기 위해 마스터 계정에서 가드레일을 생성합니다.
F. EBS 암호화를 감지하기 위해 프로덕션 OU에 대한 가드레일을 생성합니다.

해설
정답: C,D,F

AWS Control Tower: AWS Control Tower는 계정 설정과 보안 규칙(guardrails)을 설정하기 위한 기본적인 관리 도구입니다. 관리 계정에 새로운 AWS Control Tower 랜딩 존을 생성하고, 프로덕션 및 개발 계정을 각각의 조직 단위(OU)에 추가하면 보안과 관리가 일관되게 유지됩니다.
SCP (Service Control Policies): AWS Organizations에서 SCP를 사용하여 프로덕션 계정에서 특정 규칙을 강제할 수 있습니다. SCP는 계정에 적용되는 제어 정책으로, 모든 EBS 볼륨이 암호화되도록 보장할 수 있습니다.
Guardrails 설정: 프로덕션 OU에 대해 EBS 암호화를 감지하는 guardrail을 설정하면 EBS 볼륨이 암호화되지 않았을 때 알림을 받을 수 있습니다. 이는 보안 규칙을 준수하는 데 도움이 됩니다.

◆ | **Q#0169.** | **Ref#0169.**
한 회사는 MySQL용 Amazon RDS 데이터베이스가 있는 ALB(Application Load Balancer) 뒤에 있는 두 개의 Linux Amazon EC2 인스턴스에서 중요한 상태 저장 웹 애플리케이션을 실행하고 있습니다. 회사는 Amazon Route 53에서 애플리케이션에 대한 DNS 레코드를 호스팅합니다. 솔루션 설계자는 애플리케이션의 복원력을 향상시키기 위한 솔루션을 권장해야 합니다.

솔루션은 다음 목표를 충족해야 합니다.

• 애플리케이션 계층: RPO 2분. RTO 30분
• 데이터베이스 계층: RPO 5분. 30분의 RTO

회사는 기존 애플리케이션 아키텍처를 크게 변경하고 싶지 않습니다. 회사는 장애 조치 후 최적의 대기 시간을 보장해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Elastic Disaster Recovery를 사용하도록 EC2 인스턴스를 구성합니다. RDS DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. 두 번째 AWS 지역에 ALB를 생성합니다. AWS Global Accelerator 엔드포인트를 생성하고 엔드포인트를 ALB와 연결합니다. Global Accelerator 엔드포인트를 가리키도록 DNS 레코드를 업데이트합니다.
B. Amazon Data Lifecycle Manager(Amazon DLM)를 사용하여 EBS 볼륨의 스냅샷을 찍도록 EC2 인스턴스를 구성합니다. RDS 자동 백업을 구성합니다. 두 번째 AWS 리전에 대한 백업 복제를 구성합니다. 두 번째 리전에 ALB를 생성합니다. AWS Global Accelerator 엔드포인트를 생성하고 엔드포인트를 ALB와 연결합니다. Global Accelerator 엔드포인트를 가리키도록 DNS 레코드를 업데이트합니다.
C. AWS Backup에서 EC2 인스턴스 및 RDS DB 인스턴스에 대한 백업 계획을 생성합니다. 두 번째 AWS 리전에 대한 백업 복제를 구성합니다. 두 번째 리전에 ALB를 생성합니다. ALB 앞에 Amazon CloudFront 배포를 구성합니다. CloudFront를 가리키도록 DNS 레코드를 업데이트합니다.
D. Amazon Data Lifecycle Manager(Amazon DLM)를 사용하여 EBS 볼륨의 스냅샷을 찍도록 EC2 인스턴스를 구성합니다. RDS DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. 두 번째 AWS 지역에 ALB를 생성합니다. AWS Global Accelerator 엔드포인트를 생성하고 엔드포인트를 ALB와 연결합니다.

해설
정답: A

AWS Elastic Disaster Recovery를 사용하여 EC2 인스턴스를 구성하면 RPO를 2분, RTO를 30분으로

만족시킵니다. RDS DB 인스턴스의 크로스 리전 읽기 복제본은 데이터베이스 계층의 복원 시간 목표(RTO) 및 복원 지점 목표(RPO)를 만족시킵니다. 글로벌 가속기는 장애 전환 후에 최적의 지연 시간을 보장합니다.

◆ | **Q#0170.** | **Ref#0170.**
솔루션 아키텍트는 단일 AWS 계정에서 Amazon EC2 인스턴스의 비용을 최적화하고 적절하게 크기를 조정하려고 합니다. 솔루션 설계자는 인스턴스가 CPU, 메모리 및 네트워크 지표를 기반으로 최적화되기를 원합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

A. 해당 계정에 대해 AWS Business Support 또는 AWS Enterprise Support를 구매하십시오.
B. AWS Trusted Advisor를 켜고 "낮은 활용도 Amazon EC2 인스턴스" 권장 사항을 검토합니다.
C. Amazon CloudWatch 에이전트를 설치하고 EC2 인스턴스에 메모리 지표 수집을 구성합니다.
D. 결과 및 최적화 권장 사항을 수신하려면 AWS 계정에서 AWS Compute Optimizer를 구성하십시오.
E. 관심 있는 AWS 지역, 인스턴스 패밀리 및 운영 체제에 대한 EC2 인스턴스 절감 계획을 생성합니다.

해설
정답: C,D

Compute Optimizer가 인스턴스의 메모리 사용률 지표를 분석하도록 하려면 인스턴스에 CloudWatch 에이전트를 설치하십시오.
Compute Optimizer를 활성화하여 인스턴스의 메모리 사용률 데이터를 분석하면 Compute Optimizer의 권장 사항을 더욱 향상시키는 추가 데이터 측정이 제공됩니다.
AWS Compute Optimizer는 기계 학습을 사용하여 과거 사용률 지표를 분석함으로써 비용을 절감하고 성능을 향상시키기 위해 워크로드에 최적의 AWS 리소스를 권장합니다.

171 (나권서) 3회차 完

◆ | **Q#0171.** | **Ref#0171.**
회사는 AWS CodeCommit 리포지토리를 사용합니다. 회사는 두 번째 AWS 지역의 리포지토리에 있는 데이터의 백업 복사본을 저장해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. CodeCommit 리포지토리 데이터를 두 번째 리전에 복제하도록 AWS Elastic Disaster Recovery를 구성합니다.
B. AWS Backup을 사용하여 시간별 일정에 따라 CodeCommit 리포지토리를 백업합니다. 두 번째 리전에 교차 리전 복사본을 생성합니다.
C. 회사가 리포지토리에 코드를 푸시할 때 AWS CodeBuild를 호출하는 Amazon EventBridge 규칙을 생성합니다. CodeBuild를 사용하여 리포지토리를 복제합니다. 콘텐츠의 .zip 파일을 만듭니다. 두 번째 리전의 S3 버킷에 파일을 복사합니다.
D. CodeCommit 리포지토리의 스냅샷을 찍기 위해 매 시간마다 AWS Step Functions 워크플로를 생성합니다. 두 번째 리전의 S3 버킷에 스냅샷을 복사하도록 워크플로를 구성합니다.

해설
정답: C
AWS Backup를 사용하여 CodeCommit 저장소를 시간당 일정 스케줄로 백업하고 두 번째 리전에 교차 리전 복사본을 생성함으로써
요구 사항을 충족시킴

◆ | **Q#0172.** | **Ref#0172.**
회사에는 AWS에 각각 별도의 계정이 있는 여러 사업부가 있습니다. 각 사업부는 CIDR 범위가 겹치는 여러 VPC로 자체 네트워크를 관리합니다. 회사의 마케팅 팀은 새로운 내부 애플리케이션을 생성했으며 다른 모든 사업부에서 이 애플리케이션에 액세스할 수 있도록 하려고 합니다. 솔루션은 개인 IP 주소만 사용해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 각 사업부에 고유한 보조 CIDR 범위를 사업부의 VPC에 추가하도록 지시합니다. VPC를 피어링하고 보조 범위의 개인 NAT 게이트웨이를 사용하여 트래픽을 마케팅 팀으로 라우팅합니다.
> **B.** 마케팅 계정의 VPC에서 가상 어플라이언스 역할을 할 Amazon EC2 인스턴스를 생성합니다. 마케팅 팀과 각 사업부의 VPC 간에 AWS Site-to-Site VPN 연결을 생성합니다. 필요한 경우 NAT를 수행합니다.
> **C.** 마케팅 애플리케이션을 공유하기 위해 AWS PrivateLink 엔드포인트 서비스를 생성합니다. 특정 AWS 계정에 서비스에 연결할 수 있는 권한을 부여합니다. 프라이빗 IP 주소를 사용하여 애플리케이션에 액세스하려면 다른 계정에 인터페이스 VPC 엔드포인트를 생성하세요.
> **D.** 프라이빗 서브넷의 마케팅 애플리케이션 앞에 NLB(Network Load Balancer)를 생성합니다. API 게이트웨이 API를 생성합니다. Amazon API Gateway 프라이빗 통합을 사용하여 API를 NLB에 연결합니다. API에 대한 IAM 승인을 활성화합니다. 다른 사업부의 계정에 대한 액세스 권한을 부여합니다.
>
> 해설
> 정답: C
> AWS PrivateLink 엔드포인트 서비스를 사용하여 마케팅 응용프로그램을 공유하고 특정 AWS 계정에 서비스에 연결할 수 있는 권한을 부여하고
> 다른 계정의 인터페이스 VPC 엔드포인트를 생성하여 개인 IP 주소를 사용하여 어플리케이션에 액세스할 수 있도록 하면 다른 비즈니스 유닛들이
> 마케팅 응용프로그램에 접근할 수 있으면서 운영 부담을 최소화할 수 있음

◆ | **Q#0173.** | **Ref#0173.**
회사는 새로 취득한 AWS 계정의 보안 상태를 감사해야 합니다. 회사의 데이터 보안 팀은 Amazon S3 버킷이 공개적으로 노출되는 경우에만 알림을 요구합니다. 회사는 이미 데이터 보안 팀의 이메일 주소를 구독하는 Amazon Simple 알림 서비스(Amazon SNS) 주제를 설정했습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** isPublic 이벤트에 대해 모든 S3 버킷에 S3 이벤트 알림을 생성합니다. 이벤트 알림 대상으로 SNS 주제를 선택합니다.
> **B.** AWS Identity and Access Management Access Analyser에서 분석기를 생성합니다. "isPublic: true"에 대한 필터를 사용하여 이벤트 유형 "액세스 분석기 찾기"에 대한 Amazon EventBridge 규칙을 생성합니다. EventBridge 규칙 대상으로 SNS 주제를 선택합니다.
> **C.** "PutBucketPolicy"에 대한 필터를 사용하여 "CloudTrail을 통한 버킷 수준 API 호출" 이벤트 유형에 대한 Amazon EventBridge 규칙을 생성합니다. EventBridge 규칙 대상으로 SNS 주제를 선택합니다.
> **D.** AWS Config를 활성화하고 cloudtrail-s3-dataevents-enabled 규칙을 추가합니다. "NON_COMPLIANT" 필터를 사용하여 이벤트 유형 "구성 규칙 재평가 상태"에 대한 Amazon EventBridge 규칙을 생성합니다. EventBridge 규칙 대상으로 SNS 주제를 선택합니다.
>
> 해설
> 정답: B
> IAM Access Analyzer를 사용하여 S3 버킷의 외부 또는 다른 AWS 계정에 액세스를 허용하도록 구성된 버킷에 대해 경고를 받을 수 있음

◆ | **Q#0174.** | **Ref#0174.**
솔루션 설계자는 새로 인수한 회사의 애플리케이션 및 데이터베이스 포트폴리오를 평가해야 합니다. 솔루션 아키텍트는 포트폴리오를 AWS로 마이그레이션하기 위한 비즈니스 사례를 생성해야 합니다. 새로 인수된 회사는 온프

레미스 데이터 센터에서 애플리케이션을 실행합니다. 데이터 센터에 대한 문서화가 잘 되어 있지 않습니다. 솔루션 설계자는 얼마나 많은 애플리케이션과 데이터베이스가 존재하는지 즉시 확인할 수 없습니다. 애플리케이션의 트래픽은 가변적입니다. 일부 애플리케이션은 매월 말에 실행되는 일괄 프로세스입니다.

솔루션 아키텍트는 AWS로의 마이그레이션을 시작하기 전에 포트폴리오를 더 잘 이해해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** AWS Server Migration Service(AWS SMS) 및 AWS Database Migration Service(AWS DMS)를 사용하여 마이그레이션을 평가합니다. AWS Service Catalog를 사용하여 애플리케이션 및 데이터베이스 종속성을 이해합니다.
> **B.** AWS 애플리케이션 마이그레이션 서비스를 사용하십시오. 온프레미스 인프라에서 에이전트를 실행합니다. AWS Migration Hub를 사용하여 에이전트를 관리합니다. AWS Storage Gateway를 사용하여 로컬 스토리지 요구 사항과 데이터베이스 종속성을 평가합니다.
> **C.** 마이그레이션 평가기를 사용하여 서버 목록을 생성합니다. 비즈니스 사례에 대한 보고서를 작성하세요. AWS Migration Hub를 사용하여 포트폴리오를 확인하세요. AWS Application Discovery Service를 사용하여 애플리케이션 종속성을 이해하십시오.
> **D.** 대상 계정에서 AWS Control Tower를 사용하여 애플리케이션 포트폴리오를 생성합니다. AWS Server Migration Service(AWS SMS)를 사용하여 심층적인 보고서와 비즈니스 사례를 생성하십시오. 핵심 계정 및 리소스에 대한 랜딩 존을 사용하십시오.
>
> 해설
> 정답: C
> Migration Evaluator를 사용하여 서버 목록을 생성하고 비즈니스 케이스를 작성할 수 있고 AWS Migration Hub를 사용하여
> 포트폴리오를 확인하고 AWS Application Discovery Service를 사용하여 애플리케이션 의존성을 이해할 수 있음

◆ | **Q#0175.** | **Ref#0175.**
회사에는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에서 여러 포드의 ReplicaSet으로 실행되는 애플리케이션이 있습니다. EKS 클러스터에는 여러 가용 영역에 노드가 있습니다. 애플리케이션은 실행 중인 모든 애플리케이션 인스턴스에서 액세스할 수 있어야 하는 많은 작은 파일을 생성합니다. 회사는 해당 파일을 백업하고, 백업본을 1년간 보관해야 합니다.

가장 빠른 스토리지 성능을 제공하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** EKS 클러스터의 노드가 포함된 각 서브넷에 대해 Amazon Elastic File System(Amazon EFS) 파일 시스템과 탑재 대상을 생성합니다. 파일 시스템을 마운트하도록 ReplicaSet를 구성합니다. 파일 시스템에 파일을 저장하도록 애플리케이션에 지시합니다. 1년 동안 데이터 복사본을 백업하고 보관하도록 AWS Backup을 구성합니다.
> **B.** Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성합니다. EBS 다중 연결 기능을 활성화합니다. EBS 볼륨을 마운트하도록 ReplicaSet를 구성합니다. EBS 볼륨에 파일을 저장하도록 애플리케이션에 지시합니다. 1년 동안 데이터 복사본을 백업하고 보관하도록 AWS Backup을 구성합니다.
> **C.** Amazon S3 버킷을 생성합니다. S3 버킷을 마운트하도록 ReplicaSet를 구성합니다. 애플리케이션이 S3 버킷에 파일을 저장하도록 지시합니다. 데이터 복사본을 유지하도록 S3 버전 관리를 구성합니다. 1년 후에 객체를 삭제하도록 S3 수명 주기 정책을 구성합니다.
> **D.** 실행 중인 각 애플리케이션 포드에서 사용 가능한 스토리지를 사용하여 파일을 로컬에 저장하도록 ReplicaSet를 구성합니다. 타사 도구를 사용하여 EKS 클러스터를 1년 동안 백업합니다.
>
> 해설
> 정답: A
> Amazon Elastic File System (Amazon EFS) 파일 시스템을 생성하고 EKS 클러스터 노드가 있는 각 서브넷에 대한 마운트 타겟을 만들 수 있고
> ReplicaSet을 구성하여 파일 시스템을 마운트하고 애플리케이션에 파일을 저장하도록 지시할 수 있

고
AWS Backup을 구성하여 데이터를 백업하고 1년간 유지할 수 있음

◆ | **Q#0176.** | **Ref#0176.**
한 회사는 전화를 받고 모든 고객에게 문자 메시지를 통해 관리되는 대화형 양방향 경험 설문조사를 자동으로 보내는 고객 서비스 센터를 운영하고 있습니다. 고객 서비스 센터를 지원하는 애플리케이션은 회사가 온프레미스 데이터 센터에서 호스팅하는 시스템에서 실행됩니다. 회사에서 사용하는 하드웨어가 오래되어 회사 시스템에 다운타임이 발생하고 있습니다. 회사는 안정성을 향상하기 위해 시스템을 AWS로 마이그레이션하려고 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon Connect를 사용하여 기존 콜센터 하드웨어를 교체하십시오. Amazon Pinpoint를 사용하여 고객에게 문자 메시지 설문조사를 보냅니다.
B. Amazon Connect를 사용하여 기존 콜센터 하드웨어를 교체하십시오. Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 고객에게 문자 메시지 설문조사를 보냅니다.
C. 콜센터 소프트웨어를 Auto Scaling 그룹에 있는 Amazon EC2 인스턴스로 마이그레이션합니다. EC2 인스턴스를 사용하여 고객에게 문자 메시지 설문조사를 보냅니다.
D. Amazon Pinpoint를 사용하여 기존 콜센터 하드웨어를 교체하고 고객에게 문자 메시지 설문조사를 보냅니다.

해설
정답: A
가장 낮은 운영 오버헤드로 충족하기 위해서는 Amazon Connect를 사용하여 오래된 콜센터 하드웨어를 대체하고,
Amazon Pinpoint를 사용하여 고객에게 문자 메시지 형식의 설문 조사를 전송해야 합

◆ | **Q#0177.** | **Ref#0177.**
한 회사에서 Amazon Connect를 사용하여 콜센터를 구축하고 있습니다. 회사의 운영 팀은 AWS 지역 전반에 걸쳐 재해 복구(DR) 전략을 정의하고 있습니다. 연락 센터에는 수십 개의 연락 흐름, 수백 명의 사용자, 수십 개의 청구된 전화 번호가 있습니다.

DR에 가장 낮은 RTO를 제공하는 솔루션은 무엇입니까?

A. Amazon Connect 인스턴스의 가용성을 확인하고 사용할 수 없는 경우 운영 팀에 알림을 보내는 AWS Lambda 함수를 생성하십시오. 5분마다 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. 알림을 받은 후 운영 팀에 AWS Management Console을 사용하여 두 번째 지역에 새 Amazon Connect 인스턴스를 프로비저닝하도록 지시하십시오. AWS CloudFormation 템플릿을 사용하여 고객 응대 흐름, 사용자 및 청구된 전화번호를 배포합니다.
B. 두 번째 지역의 모든 기존 사용자와 함께 새로운 Amazon Connect 인스턴스를 프로비저닝합니다. Amazon Connect 인스턴스의 가용성을 확인하는 AWS Lambda 함수를 생성합니다. 5분마다 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. 문제가 발생하는 경우 두 번째 지역에서 고객 응대 흐름 및 청구 번호를 프로비저닝하는 AWS CloudFormation 템플릿을 배포하도록 Lambda 함수를 구성합니다.
C. 두 번째 지역에서 모든 기존 고객 응대 흐름과 청구된 전화번호를 사용하여 새로운 Amazon Connect 인스턴스를 프로비저닝합니다. Amazon Connect 인스턴스의 URL에 대한 Amazon Route 53 상태 확인을 생성합니다. 상태 확인 실패에 대한 Amazon CloudWatch 경보를 생성합니다. 모든 사용자를 프로비저닝하는 AWS CloudFormation 템플릿을 배포하는 AWS Lambda 함수를 생성합니다. Lambda 함수를 호출하도록 경보를 구성합니다.
D. 두 번째 지역의 모든 기존 사용자 및 고객 응대 흐름을 사용하여 새로운 Amazon Connect 인스턴스를 프로비저닝합니다. Amazon Connect 인스턴스의 URL에 대한 Amazon Route 53 상태 확인을 생성합니다. 상태 확인 실패에 대한 Amazon CloudWatch 경보를 생성합니다. 청구된 전화번호를 프로비저닝하는 AWS CloudFormation 템플릿을 배포하는 AWS Lambda 함수를 생성합니다. Lambda 함수를 호출하도록 경보를 구성합니다.

해설
정답: D
필요한 모든 구성 요소가 이미 두 번째 리전에 프로비저닝되어있고, 재해 발생 시 실패한 헬스 체크가 클레임된 전화 번호를
프로비저닝하는 AWS CloudFormation 템플릿을 실행하는 Lambda 함수가 트리거되면 가장 빠른 복구 시간을 제공하며,
필요한 모든 구성 요소가 이미 두 번째 지역에 준비되어 있으므로 가장 낮은 RTO를 제공할 수 있음

◆ | **Q#0178.** | **Ref#0178.**
한 회사가 AWS에서 애플리케이션을 실행하고 있습니다. 회사는 다양한 소스로부터 데이터를 선별합니다. 회사는 독점 알고리즘을 사용하여 데이터 변환 및 집계를 수행합니다. 회사는 ETL 프로세스를 수행한 후 결과를 Amazon Redshift 테이블에 저장합니다. 회사는 이 데이터를 다른 회사에 판매합니다. 회사는 Amazon Redshift 테이블에서 데이터를 파일로 다운로드하고 FTP를 사용하여 여러 데이터 고객에게 파일을 전송합니다. 데이터 고객 수가 크게 늘어났습니다. 데이터 고객 관리가 어려워졌습니다.

회사는 AWS Data Exchange를 사용하여 회사가 고객과 데이터를 공유하는 데 사용할 수 있는 데이터 제품을 만들 것입니다. 회사는 데이터를 공유하기 전에 고객의 신원을 확인하기를 원합니다. 또한 고객은 회사가 데이터를 게시할 때 최신 데이터에 액세스해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. API용 AWS Data Exchange를 사용하여 고객과 데이터를 공유하십시오. 구독 확인을 구성합니다. 데이터를 생산하는 회사의 AWS 계정에서 Amazon Redshift와 Amazon API Gateway 데이터 API 서비스 통합을 생성합니다. 데이터 고객에게 데이터 제품을 구독하도록 요구합니다.
B. 데이터를 생산하는 회사의 AWS 계정에서 AWS Data Exchange를 Redshift 클러스터에 연결하여 AWS Data Exchange 데이터 공유를 생성합니다. 구독 확인을 구성합니다. 데이터 고객에게 데이터 제품을 구독하도록 요구합니다.
C. Amazon Redshift 테이블의 데이터를 주기적으로 Amazon S3 버킷으로 다운로드합니다. S3용 AWS Data Exchange를 사용하여 고객과 데이터를 공유하십시오. 구독 확인을 구성합니다. 데이터 고객에게 데이터 제품을 구독하도록 요구합니다.
D. Amazon Redshift 데이터를 AWS Data Exchange의 개방형 데이터에 게시합니다. 고객에게 AWS Data Exchange의 데이터 제품을 구독하도록 요구합니다. 데이터를 생산하는 회사의 AWS 계정에서 IAM 리소스 기반 정책을 Amazon Redshift 테이블에 연결하여 확인된 AWS 계정에만 액세스를 허용합니다.

해설
정답: B
가장 낮은 운영 오버헤드로 충족하기 위해서는 AWS 계정에서 데이터를 생성하는 회사가 AWS Data Exchange를 사용하여 데이터 공유를 위해
데이터 제품에 가입할 것을 요구하고 데이터 고객들은 최신 데이터에 액세스해야 하므로 Redshift를 통해 데이터에 직접 액세스할 수 있어야 함

◆ | **Q#0179.** | **Ref#0179.**
솔루션 설계자는 이벤트를 처리하기 위한 솔루션을 설계하고 있습니다. 솔루션에는 솔루션이 수신하는 이벤트 수에 따라 규모를 확대 및 축소할 수 있는 기능이 있어야 합니다. 처리 오류가 발생하는 경우 이벤트는 검토를 위해 별도의 대기열로 이동해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon SNS(Amazon SNS) 주제로 이벤트 세부 정보를 보냅니다. 이벤트를 처리하려면 AWS Lambda 함수를 SNS 주제의 구독자로 구성하세요. 실패 시 대상을 함수에 추가합니다. Amazon Simple Queue Service(Amazon SQS) 대기열을 대상으로 설정합니다.
B. Amazon Simple Queue Service(Amazon SQS) 대기열에 이벤트를 게시합니다. Amazon EC2 Auto Scaling 그룹을 생성합니다. 대기열의 ApproximateAgeOfOldestMessage 지표를 기반으로 확장 및

축소하도록 Auto Scaling 그룹을 구성합니다. 실패한 메시지를 배달 못한 편지 대기열에 쓰도록 애플리케이션을 구성합니다.
C. Amazon DynamoDB 테이블에 이벤트를 씁니다. 테이블에 대한 DynamoDB 스트림을 구성합니다. AWS Lambda 함수를 호출하도록 스트림을 구성합니다. 이벤트를 처리하도록 Lambda 함수를 구성합니다.
D. Amazon EventBndge 이벤트 버스에 이벤트를 게시합니다. Application Load Balancer(ALB) 뒤에 있는 Auto Scaling 그룹을 사용하여 Amazon EC2 인스턴스에서 애플리케이션을 생성하고 실행합니다. ALB를 이벤트 버스 대상으로 설정합니다. 이벤트를 재시도하도록 이벤트 버스를 구성합니다. 애플리케이션이 메시지를 처리할 수 없는 경우 배달 못한 편지 대기열에 메시지를 씁니다.

해설
정답: B
이벤트를 Amazon Simple Queue Service (Amazon SQS) 큐에 발행하고, 큐의
ApproximateAgeOfOldestMessage 메트릭을 기반으로
Amazon EC2 Auto Scaling 그룹을 만들어야하고 응용 프로그램을 구성하여 실패한 메시지를 데드레터 큐에 쓸 수 있어야 함

◆ | **Q#0180.** | **Ref#0180.**
회사는 AWS 클라우드에서 처리 엔진을 실행합니다. 엔진은 물류센터의 환경 데이터를 처리하여 지속가능성 지수를 계산합니다. 이 회사는 유럽 전역에 분산된 물류 센터에 수백만 대의 장치를 보유하고 있습니다. 장치는 RESTful API를 통해 처리 엔진에 정보를 보냅니다.

API에서 예측할 수 없는 트래픽 급증이 발생합니다. 회사는 장치가 처리 엔진으로 보내는 모든 데이터를 처리하는 솔루션을 구현해야 합니다. 데이터 손실은 용납될 수 없습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. RESTful API용 ALB(Application Load Balancer)를 생성합니다. Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. ALB에 대한 리스너 및 대상 그룹을 생성합니다. SQS 대기열을 대상으로 추가합니다. Fargate 시작 유형과 함께 Amazon Elastic Container Service(Amazon ECS)에서 실행되는 컨테이너를 사용하여 대기열의 메시지를 처리합니다.
B. RESTful API를 구현하는 Amazon API Gateway HTTP API를 생성합니다. Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. SQS 대기열과 API Gateway 서비스 통합을 생성합니다. SQS 대기열의 메시지를 처리하는 AWS Lambda 함수를 생성합니다.
C. RESTful API를 구현하는 Amazon API Gateway REST API를 생성합니다. Auto Scaling 그룹에 Amazon EC2 인스턴스 플릿을 생성합니다. API Gateway Auto Scaling 그룹 프록시 통합을 생성합니다. EC2 인스턴스를 사용하여 수신 데이터를 처리합니다.
D. RESTful API용 Amazon CloudFront 배포판을 생성합니다. Amazon Kinesis Data Streams에서 데이터 스트림을 생성합니다. 데이터 스트림을 배포 원본으로 설정합니다. 데이터 스트림의 데이터를 소비하고 처리하는 AWS Lambda 함수를 생성합니다.

해설
정답: B
Amazon API Gateway HTTP API를 생성하여 RESTful API를 구현하고, Amazon Simple Queue Service (Amazon SQS) 큐를 생성한 다음
API Gateway 서비스 통합과 SQS 큐를 생성하고, 메시지를 처리할 AWS Lambda 함수를 만들어야 함

181 (노종옥) 3회차 完

◆ | **Q#0181.** | **Ref#0181.**
한 회사가 AWS 클라우드에서 네트워크 구성을 설계하고 있습니다. 회사는 AWS Organizations를 사용하여 다중

계정 설정을 관리합니다. 회사에는 3개의 OU가 있습니다. 각 OU에는 100개 이상의 AWS 계정이 포함되어 있습니다. 각 계정에는 단일 VPC가 있으며 각 OU의 모든 VPC는 동일한 AWS 리전에 있습니다.

모든 AWS 계정의 CIDR 범위는 겹치지 않습니다. 회사는 동일한 OU에 있는 VPC가 서로 통신할 수 있지만 다른 OU에 있는 VPC와는 통신할 수 없는 솔루션을 구현해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 각 OU의 계정 간에 VPC 피어링을 설정하는 AWS CloudFormation 스택 세트를 생성합니다. 각 OU에 스택 세트를 프로비저닝합니다.
> **B.** 각 OU에서 단일 VPC가 있는 전용 네트워킹 계정을 생성합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 이 VPC를 OU의 다른 모든 계정과 공유합니다. 네트워킹 계정과 OU의 각 계정 간에 VPC 피어링 연결을 생성합니다.
> **C.** 각 OU의 계정에 전송 게이트웨이를 프로비저닝합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 조직 전체에서 전송 게이트웨이를 공유합니다. 각 VPC에 대해 Transit Gateway VPC 연결을 생성합니다.
> **D.** 각 OU에서 단일 VPC가 있는 전용 네트워킹 계정을 생성합니다. 네트워킹 계정과 OU의 다른 계정 간에 VPN 연결을 설정합니다. 타사 라우팅 소프트웨어를 사용하여 VPC 간에 전이적 트래픽을 라우팅합니다.
>
> 해설
> 정답:C
> 각 OU마다 전송 게이트웨이를 프로비저닝하고, AWS Resource Access Manager(AWS RAM)를 이용하여 조직 전체에서 전송 게이트웨이를 공유하면,
> 각 VPC에 대하여 Transit Gateway VPC 연결을 생성할 수 있고, 이를 통해 동일한 OU내의 VPC들은 서로 통신이 가능하지만, 다른 OU의 VPC와의 통신은 막을 수 있습니다.

◆ | **Q#0182.** | **Ref#0182.**
한 회사가 애플리케이션을 AWS로 마이그레이션하고 있습니다. 마이그레이션 중에 완전 관리형 서비스를 최대한 많이 사용하려고 합니다. 회사는 다음 요구 사항에 따라 대용량 중요 문서를 애플리케이션 내에 저장해야 합니다.

. 1. 데이터의 내구성과 가용성이 높아야 합니다
. 2. 데이터는 저장 및 전송 중에 항상 암호화되어야 합니다
. 3. 암호화 키는 회사에서 관리해야 합니다. 주기적으로 교체됩니다.

다음 중 솔루션 설계자가 권장해야 하는 솔루션은 무엇입니까?

> **A.** 파일 게이트웨이 모드로 스토리지 게이트웨이를 AWS에 배포합니다. AWS KMS 키를 사용하여 Amazon EBS 볼륨 암호화를 사용하여 스토리지 게이트웨이 볼륨을 암호화합니다.
> **B.** 버킷 정책과 함께 Amazon S3를 사용하여 버킷 연결에 HTTPS를 적용하고 객체 암호화를 위해 서버 측 암호화 및 AWS KMS를 적용합니다.
> **C.** SSL과 함께 Amazon DynamoDB를 사용하여 DynamoDB에 연결합니다. AWS KMS 키를 사용하여 저장 중인 DynamoDB 객체를 암호화합니다.
> **D.** 이 데이터를 저장하기 위해 Amazon EBS 볼륨이 연결된 인스턴스를 배포합니다. AWS KMS 키를 사용하여 EBS 볼륨 암호화를 사용하여 데이터를 암호화합니다.
>
> 해설
> 정답:B
> 높은 내구성과 가용성, 그리고 항상 암호화된 데이터를 포함하고 있는데, 이러한 요구사항은 Amazon S3를 사용할 때 가장 잘 충족됩니다.
> 또한, Amazon S3는 데이터를 서버 측에서 암호화 할 수 있으며, AWS Key Management Service(KMS)를 사용하여 암호화 키를 회사가 관리할 수 있습니다.

◆ | **Q#0183.** | **Ref#0183.**
회사의 공개 API는 Amazon Elastic Container Service(Amazon ECS)에서 작업으로 실행됩니다. 작업은 ALB(Application Load Balancer) 뒤의 AWS Fargate에서 실행되며 CPU 사용률을 기반으로 작업을 위해 서비스 자동 조정으로 구성됩니다. 이 서비스는 몇 달 동안 잘 운영되어 왔습니다.

최근 API 성능이 저하되어 애플리케이션을 사용할 수 없게 되었습니다. 회사는 API에 대해 상당수의 SQL 주입 공격이 발생했으며 API 서비스가 최대 수준으로 확장되었음을 발견했습니다.

솔루션 설계자는 SQL 주입 공격이 ECS API 서비스에 도달하는 것을 방지하는 솔루션을 구현해야 합니다. 솔루션은 합법적인 트래픽을 허용해야 하며 운영 효율성을 극대화해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 새로운 AWS WAF 웹 ACL을 생성하여 ECS 작업 이전에 ALB로 전달되는 HTTP 요청 및 HTTPS 요청을 모니터링합니다.
> **B.** 새로운 AWS WAF 봇 제어 구현을 생성합니다. AWS WAF Bot Control 관리형 규칙 그룹에 규칙을 추가하여 트래픽을 모니터링하고 ECS 작업 이전에 ALB에 대한 합법적인 트래픽만 허용합니다.
> **C.** 새로운 AWS WAF 웹 ACL을 생성합니다. SQL 데이터베이스 규칙 그룹과 일치하는 요청을 차단하는 새 규칙을 추가합니다. 해당 규칙과 일치하지 않는 다른 모든 트래픽을 허용하도록 웹 ACL을 설정합니다. ECS 작업 앞의 ALB에 웹 ACL을 연결합니다.
> **D.** 새로운 AWS WAF 웹 ACL을 생성합니다. AWS WAF에서 새로운 빈 IP 세트를 생성합니다. 새 IP 세트의 IP 주소에서 시작되는 요청을 차단하려면 웹 ACL에 새 규칙을 추가합니다. SQL 주입 공격을 보내는 IP 주소에 대한 API 로그를 스크랩하고 해당 IP 주소를 IP 세트에 추가하는 AWS Lambda 함수를 생성합니다. ECS 작업 앞의 ALB에 웹 ACL을 연결합니다.
>
> 해설
> 정답:C
> AWS WAF는 SQL 주입 공격을 필터링하고 차단하기 위해 사용할 수 있는 웹 애플리케이션 방화벽(WAF)입니다.
> 웹 ACL을 생성하고, 그 규칙 안에서 SQL 주입을 감지하여 이를 차단할 수 있는 규칙을 설정하는 것이 필요합니다.
> 그리고 이 웹 ACL을 ECS 작업 앞의 ALB에 연결하면, SQL 주입 공격을 방지하면서 합법적인 트래픽은 허용할 수 있게 됩니다.

◆ | **Q#0184.** | **Ref#0184.**
한 환경 회사가 공기 질을 측정하기 위해 전국 주요 도시에 센서를 배치하고 있습니다. 센서는 AWS IoT Core에 연결하여 시계열 데이터 판독값을 수집합니다. 회사는 Amazon DynamoDB에 데이터를 저장합니다.

비즈니스 연속성을 위해 회사는 두 개의 AWS 리전에서 데이터를 수집하고 저장할 수 있어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 두 리전의 AWS IoT Core 데이터 엔드포인트에 대한 값을 사용하여 Amazon Route 53 별칭 장애 조치 라우팅 정책을 생성합니다. 데이터를 Amazon Aurora 글로벌 테이블로 마이그레이션합니다.
> **B.** 각 리전에서 AWS IoT Core에 대한 도메인 구성을 생성합니다. Amazon Route 53 지연 시간 기반 라우팅 정책을 생성합니다. 두 리전 모두에서 AWS IoT Core 데이터 엔드포인트를 값으로 사용합니다. 데이터를 Redis용 Amazon MemoryDB로 마이그레이션하고 리전 간 복제를 구성합니다.
> **C.** 각 리전에서 AWS IoT Core에 대한 도메인 구성을 생성합니다. 도메인 구성 상태를 평가하는 Amazon Route 53 상태 확인을 생성합니다. AWS IoT Core 도메인 구성의 도메인 이름 값을 사용하여 장애 조치 라우팅 정책을 생성합니다. DynamoDB 테이블을 전역 테이블로 업데이트합니다.
> **D.** Amazon Route 53 지연 시간 기반 라우팅 정책을 생성합니다. 두 리전 모두에서 AWS IoT Core 데이터 엔드포인트를 값으로 사용합니다. DynamoDB 스트림과 리전 간 데이터 복제를 구성합니다.
>
> 해설

정답:C
AWS IoT Core는 완벽하게 관리되는 서비스이며, 이를 사용하면 인터넷에 연결된 디바이스에 연결하고 상호 작용할 수 있게 됩니다.
DynamoDB는 전역 테이블 기능을 지원하므로 이를 통해 다른 리전에 자동으로 복제할 수 있습니다.

◆ | **Q#0185.** | **Ref#0185.**
회사는 AWS 클라우드에서 다중 계정 설정을 위해 AWS Organizations를 사용합니다. 회사의 재무팀에는 AWS Lambda 및 Amazon DynamoDB를 사용하는 데이터 처리 애플리케이션이 있습니다. 회사의 마케팅 팀은 DynamoDB 테이블에 저장된 데이터에 액세스하려고 합니다.

DynamoDB 테이블에는 기밀 데이터가 포함되어 있습니다. 마케팅 팀은 DynamoDB 테이블에 있는 데이터의 특정 속성에만 액세스할 수 있습니다. 재무팀과 마케팅팀은 별도의 AWS 계정을 가지고 있습니다.

마케팅 팀에 DynamoDB 테이블에 대한 적절한 액세스 권한을 제공하려면 솔루션 아키텍트가 무엇을 해야 합니까?

A. 마케팅 팀의 AWS 계정에 DynamoDB 테이블의 특정 속성에 대한 액세스 권한을 부여하려면 SCP를 생성하십시오. 재무팀의 OU에 SCP를 연결합니다.
B. 특정 DynamoDB 속성(세분화된 액세스 제어)에 대한 IAM 정책 조건을 사용하여 재무팀의 계정에 IAM 역할을 생성합니다. 마케팅팀의 계정에 대한 신뢰를 구축하세요. 마케팅팀 계정에서 재무팀 계정의 IAM 역할을 맡을 수 있는 권한이 있는 IAM 역할을 생성합니다.
C. 특정 DynamoDB 속성(세분화된 액세스 제어)에 대한 조건을 포함하는 리소스 기반 IAM 정책을 생성합니다. DynamoDB 테이블에 정책을 연결합니다. 마케팅 팀 계정에서 재무 팀 계정의 DynamoDB 테이블에 액세스할 수 있는 권한이 있는 IAM 역할을 생성합니다.
D. 재무팀의 계정에 IAM 역할을 생성하여 DynamoDB 테이블에 액세스합니다. IAM 권한 경계를 사용하여 특정 속성에 대한 액세스를 제한합니다. 마케팅팀 계정에서 재무팀 계정의 IAM 역할을 맡을 수 있는 권한이 있는 IAM 역할을 생성합니다.

해설
정답:B
마케팅 팀에게 DynamoDB 테이블의 특정 속성에만 대한 액세스 권한을 제공하려면, IAM 역할과 그 역할에 연결된 IAM 정책을 설정하는 것이 필요합니다.
이때, 정책에서는 DynamoDB 테이블의 특정 속성에 대한 액세스를 허용하도록 세분화된 액세스 제어를 구성해야 합니다.
마케팅 팀 계정에서 재무팀 계정의 IAM 역할을 맡을 수 있는 권한을 가진 IAM 역할을 마케팅 팀 계정에 생성해야 합니다.

◆ | **Q#0186.** | **Ref#0186.**
솔루션 아키텍트는 Amazon S3 버킷에 객체를 저장하는 애플리케이션을 생성하고 있습니다. 솔루션 아키텍트는 동시에 사용될 두 개의 AWS 지역에 애플리케이션을 배포해야 합니다. 두 S3 버킷의 객체는 서로 동기화된 상태를 유지해야 합니다.

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

A. S3 다중 지역 액세스 포인트 생성 다중 지역 액세스 포인트를 참조하도록 애플리케이션 변경
B. 두 S3 버킷 간에 양방향 S3 교차 리전 복제(CRR) 구성
C. 각 S3 버킷에 객체를 저장하도록 애플리케이션을 수정합니다.
D. 각 S3 버킷에 대해 S3 수명 주기 규칙을 생성하여 한 S3 버킷에서 다른 S3 버킷으로 객체를 복사합니다.
E. 각 S3 버킷에 대해 S3 버전 관리를 활성화합니다.
F. 한 S3 버킷에서 다른 S3 버킷으로 객체를 복사하는 AWS Lambda 함수를 호출하도록 각 S3 버킷에 대한 이벤트 알림을 구성합니다.

해설
정답:ABE
질문포인트 : 두 개의 S3 버킷이 서로 동기화 상태를 유지하면서 최소한의 운영 오버헤드를 가져야 함
B. 두 S3 버킷 간에 양방향 S3 교차 리전 복제(CRR) 구성
A. S3 다중 지역 액세스 포인트 생성, 다중 지역 액세스 포인트를 참조하도록 애플리케이션 변경: 사용자의 애플리케이션에 가장 가까운 지역에서 S3 객체를 자동으로 읽고 쓸 수 있는 기능을 제공합니다.
E. 각 S3 버킷에 대해 S3 버전 관리를 활성화: 모든 버전의 모든 객체를 추적하고 복원할 수 있습니다. 이렇게 함으로써 데이터 손실을 방지하며 복구를 용이하게 합니다.

◆ | **Q#0187.** | **Ref#0187.**
회사에는 온프레미스 환경에서 실행되는 IoT 플랫폼이 있습니다. 플랫폼은 MQTT 프로토콜을 사용하여 IoT 장치에 연결하는 서버로 구성됩니다. 플랫폼은 적어도 5분마다 한 번씩 장치로부터 원격 측정 데이터를 수집합니다. 플랫폼은 또한 MongoDB 클러스터에 장치 메타데이터를 저장합니다.

온프레미스 머신에 설치된 애플리케이션은 정기적인 작업을 실행하여 원격 분석 및 장치 메타데이터를 집계하고 변환합니다. 애플리케이션은 동일한 온프레미스 컴퓨터에서 실행되는 다른 웹 애플리케이션을 사용하여 사용자가 볼 수 있는 보고서를 생성합니다. 정기 작업을 실행하는 데 120~600초가 걸립니다. 그러나 웹 애플리케이션은 항상 실행 중입니다.

회사는 플랫폼을 AWS로 이전하고 있으며 스택의 운영 오버헤드를 줄여야 합니다.

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

A. AWS Lambda 함수를 사용하여 IoT 장치에 연결
B. AWS IoT Core에 게시할 IoT 장치를 구성합니다.
C. Amazon EC2 인스턴스의 자체 관리형 MongoDB 데이터베이스에 메타데이터 쓰기
D. Amazon DocumentDB에 메타데이터 쓰기(MongoDB 호환)
E. AWS Lambda 작업과 함께 AWS Step Functions 상태 시스템을 사용하여 보고서를 준비하고 Amazon S3에 보고서를 작성합니다. S3 오리진과 함께 Amazon CloudFront를 사용하여 보고서 제공
F. Amazon EC2 인스턴스와 함께 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 사용하여 보고서를 준비합니다. EKS 클러스터의 수신 컨트롤러를 사용하여 보고서 제공

해설
정답:BDE
질문키워드:최소한의 운영오버헤드, IoT, MongoDB, 보고서생성
B. AWS IoT Core는 IoT 장치와 클라우드 간 통신을 관리하고, 장치 데이터를 수집하고 처리하는 데 사용됩니다. MQTT 프로토콜을 사용하여 IoT 장치에 연결하는 과정을 단순화합니다.
D. DocumentDB는 완전 관리형 MongoDB 호환 데이터베이스로, 운영 부담을 줄이는 데 이상적입니다.
E. 이 조합은 처리 및 보고 작업을 자동화하는 데 이상적입니다. S3는 보고서 저장소로 사용되며, CloudFront는 이들 보고서를 효과적으로 배포하기 위한 CDN 서비스를 제공합니다.

◆ | **Q#0188.** | **Ref#0188.**
한 글로벌 제조 회사는 대부분의 애플리케이션을 AWS로 마이그레이션할 계획입니다. 그러나 회사에서는 데이터 규제 요구 사항이나 1000분의 1초의 대기 시간 요구 사항으로 인해 특정 국가 또는 회사의 중앙 온프레미스 데이터 센터에 남아 있어야 하는 애플리케이션에 대해 우려하고 있습니다. 또한 회사는 제한된 네트워크 인프라가 존재하는 일부 공장 현장에서 호스팅하는 애플리케이션에 대해서도 우려하고 있습니다.

회사는 개발자가 애플리케이션을 한 번 구축하고 온프레미스, 클라우드 또는 하이브리드 아키텍처에 배포할 수 있도록 일관된 개발자 환경을 원합니다. 개발자는 자신에게 익숙한 동일한 도구, API 및 서비스를 사용할 수 있어야 합니다.

이러한 요구 사항을 충족하기 위해 일관된 하이브리드 환경을 제공하는 솔루션은 무엇입니까?

> **A.** 모든 애플리케이션을 규정을 준수하는 가장 가까운 AWS 리전으로 마이그레이션하십시오. 중앙 온프레미스 데이터 센터와 AWS 간에 AWS Direct Connect 연결을 설정합니다. Direct Connect 게이트웨이를 배포합니다.
> **B.** 데이터 규제 요구 사항이나 한 자릿수 밀리초의 지연 시간 요구 사항이 있는 애플리케이션에는 AWS Snowball Edge Storage Optimized 디바이스를 사용하십시오. 장치를 온프레미스에 보관하세요. AWS Wavelength를 배포하여 공장 현장에서 워크로드를 호스팅합니다.
> **C.** 데이터 규제 요구 사항이나 한 자릿수 밀리초의 지연 시간 요구 사항이 있는 애플리케이션을 위해 AWS Outpost를 설치합니다. AWS Snowball Edge Compute Optimized 디바이스를 사용하여 공장 현장에서 워크로드를 호스팅합니다.
> **D.** 데이터 규제 요구 사항 또는 한 자릿수 밀리초의 지연 시간 요구 사항이 있는 애플리케이션을 AWS 로컬 영역으로 마이그레이션합니다. AWS Wavelength를 배포하여 공장 현장에서 워크로드를 호스팅합니다.
>
> 해설
> 정답:C
> 질문포인트:밀리초 지연시간, 제한된 네트워크
> AWS Outposts는 사용자의 온프레미스 환경에 도입될 수 있는 완전 관리형 서비스로, 사이트에서 데이터를 저장하고 처리하면서도 AWS 서비스에 접근하는 데 필요한 지연 시간을 최소화할 수 있습니다.
> Snowball Edge는 제한된 네트워크 용량을 가진 장소에서 워크로드 처리가 필요한 공장과 같은 곳에 이상적입니다. 이러한 디바이스는 기능, 데이터 전송 및 저장을 결합하여 필요한 워크로드를 처리할 수 있게 합니다.

◆ | **Q#0189.** | **Ref#0189.**
한 회사에서 고객이 온라인 주문에 사용하는 애플리케이션을 업데이트하고 있습니다. 최근 악의적인 행위자에 의한 애플리케이션 공격이 증가했습니다.

회사는 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 업데이트된 애플리케이션을 호스팅할 예정입니다. 회사는 Amazon DynamoDB를 사용하여 애플리케이션 데이터를 저장할 것입니다. 공용 ALB(Application Load Balancer)는 최종 사용자에게 애플리케이션에 대한 액세스를 제공합니다. 회사는 공격이 진행되는 동안 서비스 중단을 최소화하여 공격을 방지하고 비즈니스 연속성을 보장해야 합니다.

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

> **A.** ALB를 오리진으로 사용하여 Amazon CloudFront 배포판을 생성합니다. CloudFront 도메인에 사용자 지정 헤더와 임의의 값을 추가합니다. 헤더와 값이 일치하는 경우 조건부로 트래픽을 전달하도록 ALB를 구성합니다.
> **B.** 두 개의 AWS 지역에 애플리케이션을 배포합니다. 동일한 가중치를 갖는 두 지역으로 라우팅하도록 Amazon Route 53을 구성합니다.
> **C.** Amazon ECS 작업에 대한 자동 조정 구성 DynamoDB Accelerator(DAX) 클러스터를 생성합니다.
> **D.** DynamoDB의 오버헤드를 줄이도록 Amazon ElastiCache를 구성합니다.
> **E.** 적절한 규칙 그룹을 포함하는 AWS WAF 웹 ACL을 배포합니다. 웹 ACL을 Amazon CloudFront 배포와 연결합니다.
>
> 해설
> 정답:AE
> AWS WAF는 애플리케이션에 대한 웹 공격을 차단하여 보호를 유지하는 데 사용할 수 있는 웹 애플리케이션 방화벽 서비스이며, CloudFront와 함께 사용하면 훨씬 더 강력한 보호를 제공합니다.
> CloudFront를 사용하는 것은 보안과 성능 모두 향상됩니다. 사용자 지정 헤더를 통해 사용자 트래픽을 보다 세밀하게 관리할 수 있습니다.

◆ | **Q#0190.** | **Ref#0190.**
한 회사가 AWS에서 웹 애플리케이션을 실행하고 있습니다. 웹 애플리케이션은 Amazon CloudFront 배포 뒤에 있는 Amazon S3 버킷에서 정적 콘텐츠를 제공합니다. 애플리케이션은 Auto Scaling 그룹의 Amazon EC2 인스턴스 집합에 요청을 배포하는 ALB(Application Load Balancer)를 사용하여 동적 콘텐츠를 제공합니다. 애플리케이션은 Amazon Route 53의 도메인 이름 설정을 사용합니다.

일부 사용자는 피크 시간대에 웹 사이트에 액세스하려고 할 때 가끔 문제가 발생한다고 보고했습니다. 운영팀은 ALB가 때때로 HTTP 503 서비스를 사용할 수 없음 오류를 반환한다는 사실을 발견했습니다. 회사에서는 이러한 오류가 발생할 때 사용자 정의 오류 메시지 페이지를 표시하려고 합니다. 이 오류 코드에 대해 페이지가 즉시 표시되어야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** Route 53 장애 조치 라우팅 정책을 설정하십시오. ALB 엔드포인트의 상태를 확인하고 장애 조치 S3 버킷 엔드포인트로 장애 조치하도록 상태 확인을 구성합니다.
> **B.** 두 번째 CloudFront 배포판과 S3 정적 웹 사이트를 생성하여 사용자 지정 오류 페이지를 호스팅합니다. Route 53 장애 조치 라우팅 정책을 설정합니다. 두 배포판 간에 활성-수동 구성을 사용합니다.
> **C.** 두 개의 오리진이 있는 CloudFront 오리진 그룹을 생성합니다. ALB 엔드포인트를 기본 원본으로 설정합니다. 보조 오리진의 경우 정적 웹 사이트를 호스팅하도록 구성된 S3 버킷을 설정합니다. CloudFront 배포에 대한 오리진 장애 조치를 설정합니다. 사용자 정의 오류 페이지를 통합하도록 S3 정적 웹 사이트를 업데이트하십시오.
> **D.** ALB가 반환하는 각 HTTP 응답 코드를 검증하는 CloudFront 함수를 생성합니다. S3 버킷에 S3 정적 웹 사이트를 생성합니다. 사용자 정의 오류 페이지를 S3 버킷에 장애 조치로 업로드합니다. S3 버킷을 읽고 최종 사용자에게 오류 페이지를 제공하도록 함수를 업데이트합니다.
>
> 해설
> 정답:C
> 질문포인트 : 사용자 정의 오류 페이지를 최소한의 운영 오버헤드로 표시하는 방법
> 사용자 정의 오류 페이지를 표시하려면 CloudFront 오리진 그룹 기능을 사용할 수 있습니다.
> C 옵션은 CloudFront와 S3 사이에 내결함성을 제공하며, ALB에서 오류가 발생할 경우 S3에서 호스팅된 사용자 정의 오류 페이지를 사용자에게 표시합니다. 이렇게 하면 고객에게 간편하게 사용자 정의 오류 페이지를 제공하는 동시에 피크 시간에도 서비스를 지속적으로 제공하는 데 도움이 됩니다.

191 (백은희) 3회차 完

◆ | **Q#0191.** | **Ref#0191.**
한 회사에서 애플리케이션을 AWS로 마이그레이션할 계획입니다. 애플리케이션은 Docker 컨테이너로 실행되며 NFS 버전 4 파일 공유를 사용합니다.

솔루션 설계자는 기본 인프라의 프로비저닝이나 관리가 필요하지 않은 안전하고 확장 가능한 컨테이너형 솔루션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** Fargate 시작 유형과 함께 Amazon Elastic Container Service(Amazon ECS)를 사용하여 애플리케이션 컨테이너를 배포합니다. 공유 스토리지에는 Amazon Elastic File System(Amazon EFS)을 사용합니다. ECS 작업 정의에서 EFS 파일 시스템 ID, 컨테이너 마운트 포인트 및 EFS 인증 IAM 역할을 참조합니다.
> **B.** Fargate 시작 유형과 함께 Amazon Elastic Container Service(Amazon ECS)를 사용하여 애플리케이션 컨테이너를 배포합니다. 공유 스토리지에는 Amazon FSx for Lustre를 사용합니다. ECS 작업 정의에서 FSx for Lustre 파일 시스템 ID, 컨테이너 마운트 포인트 및 FSx for Lustre 인증 IAM 역할을 참조합니다.

C. Amazon EC2 시작 유형 및 Auto Scaling이 활성화된 Amazon Elastic Container Service(Amazon ECS)를 사용하여 애플리케이션 컨테이너를 배포합니다. 공유 스토리지에는 Amazon Elastic File System(Amazon EFS)을 사용합니다. ECS 컨테이너 인스턴스에 EFS 파일 시스템을 마운트합니다. EC2 인스턴스 프로필에 EFS 인증 IAM 역할을 추가합니다.
D. Amazon EC2 시작 유형 및 Auto Scaling이 활성화된 Amazon Elastic Container Service(Amazon ECS)를 사용하여 애플리케이션 컨테이너를 배포합니다. 공유 스토리지에 대해 다중 연결이 활성화된 Amazon Elastic Block Store(Amazon EBS) 볼륨을 사용합니다. EBS 볼륨을 ECS 컨테이너 인스턴스에 연결합니다. EC2 인스턴스 프로필에 EBS 인증 IAM 역할을 추가합니다.

해설
정답: A
Fargate를 사용하면 기본 인프라를 관리할 필요가 없어 서버리스 인프라를 제공합니다. EFS는 NFS 버전 4를 지원하며, ECS 작업 정의에서 EFS 파일 시스템을 마운트하여 사용할 수 있습니다.
참고) FSx for Lustre는 고성능 파일 시스템이지만, NFS가 아닌 Lustre 파일 시스템을 사용합니다.
EC2 시작 유형을 사용하면 기본 인프라를 관리해야 합니다.
EBS는 블록 스토리지로, NFS 파일 시스템을 지원하지 않습니다.

◆ | **Q#0192.** | **Ref#0192.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 핵심 비즈니스 로직은 Auto Scaling 그룹의 여러 Amazon EC2 인스턴스에서 실행됩니다. Application Load Balancer(ALB)는 트래픽을 EC2 인스턴스에 분산합니다. Amazon Route 53 레코드 api.example.com이 ALB를 가리키고 있습니다.

회사의 개발 팀은 비즈니스 로직의 주요 업데이트를 수행합니다. 회사에는 변경 사항이 배포되면 테스트 기간 동안 고객 중 10%만 새 로직을 받을 수 있다는 규칙이 있습니다. 고객은 테스트 기간 동안 동일한 버전의 비즈니스 로직을 사용해야 합니다.

회사는 이러한 요구 사항을 충족하기 위해 업데이트를 어떻게 배포해야 합니까?

A. 두 번째 ALB를 생성하고 새 Auto Scaling 그룹의 EC2 인스턴스 세트에 새 로직을 배포합니다. EC2 인스턴스에 트래픽을 분산하도록 ALB를 구성합니다. 가중치 기반 라우팅을 사용하도록 Route 53 레코드를 업데이트하고 레코드가 두 ALB를 모두 가리키도록 합니다.
B. ALB에서 참조하는 두 번째 타겟 그룹을 생성합니다. 이 새 타겟 그룹의 EC2 인스턴스에 새 로직을 배포합니다. 가중치가 적용된 타겟 그룹을 사용하도록 ALB 리스너 규칙을 업데이트합니다. ALB 타겟 그룹 고정성(Stickiness)을 구성합니다.
C. Auto Scaling 그룹에 대한 새로운 시작 구성을 생성합니다. AutoScalingRollingUpdate 정책을 사용하도록 시작 구성을 지정하고 MaxBatchSize 옵션을 10으로 설정합니다. Auto Scaling 그룹에서 시작 구성을 바꿉니다. 변경 사항을 배포합니다.
D. ALB에서 참조하는 두 번째 Auto Scaling 그룹을 생성합니다. 이 새로운 Auto Scaling 그룹의 EC2 인스턴스 세트에 새 로직을 배포합니다. ALB 라우팅 알고리즘을 LOR(최소 미해결 요청)로 변경합니다. ALB 세션 고정성(Stickiness)을 구성합니다.

해설
정답: B
트래픽의 10%만 새 버전으로 라우팅되어야 하며, 고객은 테스트 기간 동안 동일한 버전의 비즈니스 로직을 사용하기 위해 Stickiness를 구성해야 합니다.
ALB는 가중 대상 그룹(weighted target group)을 지원하여 트래픽을 여러 타겟 그룹 간에 분배할 수 있습니다 . 이를 통해 트래픽의 일정 비율(예: 10%)을 새 버전의 로직으로 라우팅할 수 있습니다.
ALB는 대상 그룹 고정성(target group stickiness)을 지원하여, 한 번 연결된 클라이언트가 동일한 대상 그룹에 지속적으로 연결되도록 할 수 있습니다.

◆ | **Q#0193.** | **Ref#0193.**
한 대규모 교육 회사는 최근 여러 대학에서 내부 애플리케이션에 대한 액세스를 제공하기 위해 Amazon Workspaces를 도입했습니다. 회사는 Windows 파일 서버용 Amazon FSx 파일 시스템에 사용자 프로필을 저장하고 있습니다. 파일 시스템은 DNS 별칭으로 구성되고 자체 관리형 Active Directory에 연결됩니다. 사용자가 증가함에 따라 로그인 시간이 불만족스러울 정도로 길어졌습니다.

조사 결과 파일 시스템의 성능 저하가 드러났습니다. 회사는 16MBps의 처리량으로 HDD 스토리지에 파일 시스템을 만들었습니다. 솔루션 설계자는 정의된 유지 관리 기간 동안 파일 시스템의 성능을 개선해야 합니다.

최소한의 관리 노력으로 이러한 요구 사항을 충족하려면 솔루션 설계자가 무엇을 해야 합니까?

> **A.** AWS Backup을 사용하여 파일 시스템의 특정 시점 백업을 생성하십시오. 백업을 새로운 FSx for Windows File Server 파일 시스템으로 복원합니다. 스토리지 유형으로 SSD를 선택합니다. 처리량 용량으로 32MBps를 선택합니다. 백업 및 복원 프로세스가 완료되면 그에 따라 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.
> **B.** 파일 시스템에서 사용자 연결을 끊습니다. Amazon FSx 콘솔에서 처리량 용량을 32MBps로 업데이트합니다. 스토리지 유형을 SSD로 업데이트합니다. 사용자를 파일 시스템에 다시 연결합니다.
> **C.** AWS DataSync 에이전트를 새로운 Amazon EC2 인스턴스에 배포합니다. 작업을 만듭니다. 기존 파일 시스템을 소스 위치로 구성합니다. SSD 스토리지와 32MBps의 처리량을 대상 위치로 사용하여 Windows 파일 서버 파일 시스템용 새 FSx를 구성합니다. 작업을 예약합니다. 작업이 완료되면 그에 따라 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.
> **D.** Windows PowerShell 명령을 사용하여 기존 파일 시스템에서 섀도 복사본을 활성화합니다. 파일 시스템의 특정 시점 백업을 생성하도록 섀도 복사본 작업을 예약합니다. 이전 버전을 복원하려면 선택하세요. SSD 스토리지와 32MBps의 처리량을 갖춘 새로운 FSx for Windows File Server 파일 시스템을 생성합니다. 복사 작업이 완료되면 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.
>
> 해설
> 정답: B (A 논란)
> Amazon FSx 콘솔에서 직접 스토리지 유형과 처리량을 변경할 수 있습니다. 사용자의 연결이 끊어지는 문제가 있지만 최소한의 관리 노력으로 해결할 수 있습니다.
> https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-type.html
> FSx 콘솔 또는 FSx API에서 스토리지 유형을 변경할 수 있습니다.
> AWS Backup을 사용하여 백업을 생성하고 복원하는 방식으로도 유형과 처리량을 변경 할 수 있습니다. 옵션 B가 직접 콘솔에서 설정을 변경하는 것이라면, 옵션 A는 백업과 복원을 통해 안전하게 새 스토리지로 전환하는 접근법을 사용합니다. A는 용량이 제시되지 않았기 때문에 작업 시간을 예상할 수 없으며 DNS 별칭 조정 작업이 동반되며, 사용자 연결 단절도 동반되기 대문에 B 옵션이 정답이라는 의견이 우세합니다.

◆ | **Q#0194.** | **Ref#0194.**
한 회사가 AWS에서 애플리케이션을 호스팅합니다. 애플리케이션은 단일 Amazon S3 버킷에 저장된 객체를 읽고 씁니다. 회사는 애플리케이션을 두 개의 AWS 리전으로 배포하도록 수정해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** S3 버킷을 오리진으로 사용하여 Amazon CloudFront 배포를 설정합니다. 두 번째 지역에 애플리케이션 배포 CloudFront 배포를 사용하도록 애플리케이션을 수정합니다. AWS Global Accelerator를 사용하여 S3 버킷의 데이터에 액세스합니다.
> **B.** 두 번째 지역에 새 S3 버킷을 생성합니다. 원래 S3 버킷과 새 S3 버킷 간에 양방향 S3 교차 리전 복제(CRR)를 설정합니다. 두 S3 버킷을 모두 사용하는 S3 다중 지역 액세스 포인트를 구성합니다. 수정된 애플리케이션을 두 지역 모두에 배포합니다.
> **C.** 두 번째 지역에 새 S3 버킷을 생성합니다. 두 번째 지역에 애플리케이션을 배포합니다. 새 S3 버킷을 사용하도록 애플리케이션을 구성합니다. 원래 S3 버킷에서 새 S3 버킷으로 S3 교차 리전 복제

(CRR)를 설정합니다.
D. S3 버킷을 원본으로 사용하여 S3 게이트웨이 엔드포인트를 설정합니다. 두 번째 지역에 애플리케이션을 배포합니다. 새 S3 게이트웨이 엔드포인트를 사용하도록 애플리케이션을 수정합니다. S3 버킷에서 S3 Intelligent-Tiering을 사용하십시오.

해설
정답: B
양방향 S3 교차 리전 복제(CRR)를 사용하면 데이터의 일관성을 유지할 수 있고, 두 리전 모두에서 데이터를 읽고 쓸 수 있습니다.
S3 다중 리전 액세스 포인트(S3 Multi-Region Access Point)를 사용하면 S3 버킷을 한 지점처럼 사용할 수 있어 애플리케이션이 간단히 두 리전에서 데이터를 접근할 수 있습니다.
B : Set up "bidirectional" S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. (양방향)
C : Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket. (단방향)

◆ | **Q#0195.** | **Ref#0195.**
온라인 게임 회사는 AWS에서 게임 플랫폼을 다시 호스팅해야 합니다. 이 회사의 게임 애플리케이션에는 고성능 컴퓨팅(HPC) 처리가 필요하며 리더보드(순위표)가 자주 변경됩니다. 컴퓨팅 생성에 최적화된 Ubuntu 인스턴스는 게임 디스플레이용 Node.js 애플리케이션을 호스팅합니다. 게임 상태는 온프레미스 Redis 인스턴스에서 추적됩니다.

회사에는 애플리케이션 성능을 최적화하는 마이그레이션 전략이 필요합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Application Load Balancer 뒤에 m5.large Amazon EC2 스팟 인스턴스의 Auto Scaling 그룹을 생성합니다. Redis 클러스터용 Amazon ElastICache를 사용하여 순위표를 유지합니다.
B. Application Load Balancer 뒤에 c5.large Amazon EC2 스팟 인스턴스의 Auto Scaling 그룹을 생성합니다. Amazon OpenSearch Service 클러스터를 사용하여 순위표를 유지합니다.
C. Application Load Balancer 뒤에 c5.large Amazon EC2 온디맨드 인스턴스의 Auto Scaling 그룹을 생성합니다. Redis 클러스터용 Amazon ElastiCache를 사용하여 순위표를 유지합니다.
D. Application Load Balancer 뒤에 m5.large Amazon EC2 온디맨드 인스턴스의 Auto Scaling 그룹을 생성합니다. Amazon DynamoDB 테이블을 사용하여 순위표를 유지합니다.

해설
정답: C
c5.large 인스턴스는 컴퓨팅 최적화된 인스턴스로, 고성능 컴퓨팅에 적합합니다. ElastiCache for Redis는 높은 읽기/쓰기 성능을 제공하여 자주 변경되는 리더보드를 유지하는 데 적합합니다.
m5.large 인스턴스는 메모리 및 네트워크 성능이 균형 잡혀 있지만, 컴퓨팅 최적화가 아니므로 고성능 컴퓨팅에 적합하지 않습니다.
OpenSearch는 로그 분석, 실시간 애플리케이션 모니터링 등에 적합하지만, Redis만큼 빠른 읽기/쓰기 성능을 제공하지 않습니다.

◆ | **Q#0196.** | **Ref#0196.**
솔루션 설계자는 직원들의 모바일 기기에서 근태 기록을 수집하는 애플리케이션을 설계 중입니다. Timesheet(근태기록,시간표)는 매주 제출되며 대부분의 제출은 금요일에 이루어집니다. 데이터는 급여 관리자가 월별 보고서를 실행할 수 있는 형식으로 저장되어야 합니다. 인프라는 가용성이 높아야 하며 수신 데이터 및 보고 요청의 속도에 맞게 확장되어야 합니다.

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

A. 여러 가용 영역에 걸친 로드 밸런싱을 통해 Amazon EC2 온디맨드 인스턴스에 애플리케이션을 배포합니다. 금요일에 제출량이 많아지기 전에 예약된 Amazon EC2 Auto Scaling을 사용하여 용량을 추가합니다.
B. 여러 가용 영역에 걸쳐 로드 밸런싱을 수행하는 Amazon Elastic Container Service(Amazon ECS)를 사용하여 컨테이너에 애플리케이션을 배포합니다.
금요일에 제출량이 많아지기 전에 예약된 서비스 Auto Scaling을 사용하여 용량을 추가합니다.
C. Amazon CloudFront에서 제공하는 Amazon S3 버킷에 애플리케이션 프론트엔드를 배포합니다. AWS Lambda 프록시 통합과 함께 Amazon API Gateway를 사용하여 애플리케이션 백엔드를 배포합니다.
D. 근태 기록 제출 데이터를 Amazon Redshift에 저장합니다. Amazon QuickSight를 사용하면 Amazon Redshift를 데이터 소스로 사용하여 보고서를 생성할 수 있습니다.
E. 근태 기록 제출 데이터를 Amazon S3에 저장합니다. Amazon Athena 및 Amazon QuickSight를 사용하면 Amazon S3를 데이터 소스로 사용하여 보고서를 생성할 수 있습니다.

해설
정답: C E (B E 논란)
C : Amazon S3, CloudFront, API Gateway, Lambda를 사용하면 완전히 관리형 서버리스 아키텍처가 됩니다. 이는 최소한의 운영 오버헤드를 제공하며, 고가용성과 확장성을 보장합니다.
E : Amazon S3에 데이터를 저장하고, Amazon Athena와 QuickSight를 사용하여 보고서를 생성하는 것은 매우 효율적이고 운영 오버헤드가 적습니다. S3는 높은 가용성과 확장성을 제공하며, Athena는 서버리스로 데이터를 쿼리할 수 있습니다.
B : ECS와 Service Auto Scaling을 사용하는 것은 컨테이너 관리를 필요로 하며, 예약된 Scaling이 어느 정도 목적에 부합합니다.

◆ | **Q#0197.** | **Ref#0197.**
한 회사가 민감한 데이터를 Amazon S3 버킷에 저장하고 있습니다. 회사는 S3 버킷의 객체에 대한 모든 활동을 기록해야 하며 해당 로그를 5년 동안 보관해야 합니다. 또한 회사의 보안 팀은 S3 버킷의 데이터를 삭제하려고 시도할 때마다 이메일 알림을 받아야 합니다.

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

A. S3 데이터 이벤트를 기록하도록 AWS CloudTrail을 구성합니다.
B. S3 버킷에 대한 S3 서버 액세스 로깅을 구성합니다.
C. Amazon Simple Email Service(Amazon SES)에 객체 삭제 이벤트를 보내도록 Amazon S3를 구성합니다.
D. Amazon SNS(Amazon SNS) 주제에 게시되는 Amazon EventBridge 이벤트 버스로 객체 삭제 이벤트를 보내도록 Amazon S3를 구성합니다.
E. 데이터 스토리지 계층화를 통해 로그를 Amazon Timestream으로 보내도록 Amazon S3를 구성합니다.
F. S3 수명 주기 정책에 따라 로그를 저장하도록 새 S3 버킷을 구성합니다.

해설
정답: A D F
A : CloudTrail은 S3 데이터 이벤트를 로깅할 수 있으며, 이를 통해 S3 객체에 대한 모든 활동을 기록할 수 있습니다.
D : EventBridge를 사용하여 S3 객체 삭제 이벤트를 캡처하고, 이를 SNS 주제로 게시하여 이메일 알림을 받을 수 있습니다.
F : S3 수명 주기 정책(S3 Lifecycle policy)을 통해 5년 동안 로그를 보관할 수 있습니다.

◆ | **Q#0198.** | **Ref#0198.**
한 회사가 온프레미스 데이터 센터와 AWS 클라우드에 서버를 포함하는 하이브리드 환경을 구축하고 있습니다. 이

회사는 세 개의 VPC에 Amazon EC2 인스턴스를 배포했습니다. 각 VPC는 서로 다른 AWS 리전에 있습니다. 회사는 데이터 센터에서 가장 가까운 리전에 AWS Direct Connect 연결을 설정했습니다.

회사는 온프레미스 데이터 센터의 서버가 세 개의 VPC의 EC2 인스턴스에 접근할 수 있어야 하며, AWS 퍼블릭 서비스에도 접근할 수 있어야 합니다.

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

> **A.** 데이터 센터에 가장 가까운 리전에 Direct Connect 게이트웨이를 생성합니다. Direct Connect 게이트웨이에 Direct Connect 연결을 첨부(attach)합니다. Direct Connect 게이트웨이를 사용하여 다른 두 리전의 VPC를 연결합니다.
> **B.** 온프레미스 데이터 센터에서 다른 두 리전으로의 추가 Direct Connect 연결을 설정합니다.
> **C.** 프라이빗 VIF를 생성합니다. 프라이빗 VIF를 통해 다른 두 리전의 VPC에 대한 AWS Site-to-Site VPN 연결을 설정합니다.
> **D.** 퍼블릭 VIF를 생성합니다. 퍼블릭 VIF를 통해 다른 두 리전의 VPC에 대한 AWS Site-to-Site VPN 연결을 설정합니다.
> **E.** VPC 피어링을 사용하여 리전 전체에 걸쳐 VPC 간 연결을 설정합니다. 기존 Direct Connect 연결을 사용하여 프라이빗 VIF를 생성하여 피어링된 VPC에 연결합니다.
>
> 해설
> 정답: A D
> A : Direct Connect 게이트웨이를 사용하면 여러 리전의 VPC를 하나의 Direct Connect 연결을 통해 접근할 수 있습니다. 이는 추가 Direct Connect 연결을 설정하는 것보다 비용 효율적입니다.
> D : 퍼블릭 VIF를 사용하여 AWS 퍼블릭 서비스에 접근할 수 있으며, 이를 통해 다른 두 리전의 VPC에도 접근할 수 있습니다.

◆ | **Q#0199.** | **Ref#0199.**
한 회사가 AWS Organizations를 사용하여 수백 개의 AWS 계정을 관리하고 있습니다. 솔루션 설계자는 OWASP(Open Web Application Security Project) 상위 10개 웹 애플리케이션 취약점에 대한 기본 보호를 제공하는 솔루션을 개발 중입니다. 솔루션 아키텍트는 조직 내에 배포된 모든 기존 및 신규 Amazon CloudFront 배포에 AWS WAF를 사용하고 있습니다.

솔루션 설계자는 기본 보호를 제공하기 위해 어떤 단계 조합을 수행해야 합니까? (3개를 선택하세요.)

> **A.** 모든 계정에서 AWS Config 활성화
> **B.** 모든 계정에서 Amazon GuardDuty 활성화
> **C.** 조직의 모든 기능을 활성화합니다.
> **D.** AWS Firewall Manager를 사용하여 모든 CloudFront 배포에 대한 모든 계정에 AWS WAF 규칙을 배포합니다.
> **E.** AWS Shield Advanced를 사용하여 모든 CloudFront 배포에 대한 모든 계정에 AWS WAF 규칙을 배포합니다.
> **F.** AWS Security Hub를 사용하여 모든 CloudFront 배포에 대한 모든 계정에 AWS WAF 규칙을 배포합니다.
>
> 해설
> 정답: A C D
> A : AWS Config는 리소스 구성 변경 사항을 추적하고 규정 준수 상태를 모니터링할 수 있어 추가적인 보안 관리에 도움이 됩니다.
> C : 모든 기능을 활성화하면 조직 전체의 리소스를 중앙에서 관리할 수 있으며, AWS Firewall Manager를 포함한 다양한 보안 기능을 사용할 수 있습니다.
> D : Firewall Manager는 여러 계정에서 보안 정책을 중앙에서 관리하고 배포할 수 있는 도구로, OWASP 상위 10개 취약점을 보호하는 데 유용합니다.
> 참고 : - GuardDuty는 악의적인 활동을 감지하는 데 도움을 주지만, 직접적인 OWASP 취약점 보호

기능은 아닙니다.
- AWS Shield Advanced는 DDoS 보호를 제공하지만, WAF 규칙을 배포하는 기능과는 직접적인 관련이 없습니다.
- Security Hub는 보안 상태를 모니터링하고 보고하는 도구로, 직접적인 WAF 규칙 배포 기능은 제공하지 않습니다.

◆ | **Q#0200.** | **Ref#0200.**
솔루션 아키텍트는 AWS 환경에 대한 사용자 액세스를 인증하기 위해 회사의 온프레미스 ID 공급자(IdP)와 함께 SAML 2.0 통합 ID 솔루션을 구현했습니다. 솔루션 아키텍트가 federated identity web portal(연합 ID 웹 포털)을 통해 인증을 테스트하면 AWS 환경에 대한 액세스 권한이 부여됩니다. 그러나 테스트 사용자가 federated identity web portal을 통해 인증을 시도하면 AWS 환경에 액세스할 수 없습니다.

ID 페더레이션이 올바르게 구성되었는지 확인하기 위해 솔루션 설계자가 확인해야 하는 항목은 무엇입니까? (3개를 선택하세요.)

A. IAM 사용자의 권한 정책에 따라 해당 사용자에 대한 SAML 연동 사용이 허용되었습니다. (The IAM user's permissions policy has allowed the use of SAML federation for that user.)
B. 연합 사용자 또는 연합 그룹의 신뢰 정책을 위해 생성된 IAM 역할은 SAML 공급자를 주체로 설정했습니다. (The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.)
C. 테스트 사용자는 회사 IdP의 AWSFederatedUsers 그룹에 속하지 않습니다.
D. 웹 포털은 SAML 공급자의 ARN, IAM 역할의 ARN 및 IdP의 SAML 어설션을 사용하여 AWS STS AssumeRoleWithSAML API를 호출합니다.
E. 온프레미스 IdP의 DNS 호스트 이름은 AWS 환경 VPC에서 연결할 수 있습니다.
F. 회사의 IdP가 적절한 권한이 있는 IAM 역할에, 회사의 사용자 또는 그룹을 올바르게 매핑하는 SAML 어서션을 정의했습니다. (The company's IdP defines SAML assertions that properly map users or groups in the company to IAM roles with appropriate permissions.)

해설
정답: B D F
B : SAML 공급자가 신뢰 정책의 주체로 설정되어 있는지 확인하는 것이 중요합니다. 이것이 없으면 역할이 SAML 인증을 신뢰하지 않습니다.
D : 웹 포털이 올바르게 AWS STS AssumeRoleWithSAML API를 호출하여 SAML 인증이 작동하는지 확인해야 합니다.
F : IdP가 사용자 또는 그룹을 적절한 권한이 있는 IAM 역할에 올바르게 매핑하는지 확인하는 것이 중요합니다.
SAML 2.0 연동 | 동일문제 참고