001 (고민석) 4회차 完

◆ | **Q#0001.** | **Ref#0001.**
회사는 하이브리드 DNS 솔루션을 설계해야 합니다. 이 솔루션은 Amazon Route 53의 프라이빗 호스팅 존을 사용하여 VPC 내에 저장된 리소스를 위한 도메인 cloud.example.com을 사용할 것입니다.
회사에는 다음과 같은 DNS 해석 요구사항이 있습니다.
온프레미스 시스템은 cloud.example.com을 해석하고 연결할 수 있어야 합니다.
모든 VPC는 cloud.example.com을 해석할 수 있어야 합니다.
이미 온프레미스 기업 네트워크와 AWS Transit Gateway 사이에 AWS Direct Connect 연결이 있습니다.
이러한 요구사항을 가장 높은 성능으로 충족하기 위한 아키텍처는 무엇입니까?

> **A.** 프라이빗 호스팅 존을 모든 VPC에 연결합니다. 공유 서비스 VPC에 Route 53 인바운드 리졸버를 생성합니다. 모든 VPC를 Transit Gateway에 연결하고 온프레미스 DNS 서버에 대한 cloud.example.com에 대한 포워딩 규칙을 인바운드 리졸버를 가리키도록 설정합니다.
> **B.** 프라이빗 호스팅 존을 모든 VPC에 연결합니다. 공유 서비스 VPC에 Amazon EC2 조건부 포워더를 배포합니다. 모든 VPC를 Transit Gateway에 연결하고 온프레미스 DNS 서버에 대한 cloud.example.com에 대한 포워딩 규칙을 조건부 포워더를 가리키도록 설정합니다.
> **C.** 프라이빗 호스팅 존을 공유 서비스 VPC에 연결합니다. 공유 서비스 VPC에 Route 53 아웃바운드 리졸버를 생성합니다. 모든 VPC를 Transit Gateway에 연결하고 온프레미스 DNS 서버에 대한 cloud.example.com에 대한 포워딩 규칙을 아웃바운드 리졸버를 가리키도록 설정합니다.
> **D.** 프라이빗 호스팅 존을 공유 서비스 VPC에 연결합니다. 공유 서비스 VPC에 Route 53 인바운드 리졸버를 생성합니다. 공유 서비스 VPC를 Transit Gateway에 연결하고 온프레미스 DNS 서버에 대한 cloud.example.com에 대한 포워딩 규칙을 인바운드 리졸버를 가리키도록 설정합니다.
>
> 해설
> 정답: A
> 설명: 모든 VPC에 프라이빗 호스티드 존을 연결하여 VPC 내에 저장된 리소스에 대한 DNS 해석을 제공합니다.
> 공유 서비스 VPC에 Route 53 인바운드 리졸버를 생성하여 온프레미스 시스템이 VPC의 리소스를 해석할 수 있도록 합니다.
> 모든 VPC를 Transit Gateway에 연결하여 VPC 간 통신을 효율적으로 라우팅합니다.
> 온프레미스 DNS 서버에는 cloud.example.com에 대한 포워딩 규칙을 인바운드 리졸버를 가리키도록 설정하여 온프레미스 시스템이 VPC의 리소스를 해석할 수 있도록 합니다.

◆ | **Q#0002.** | **Ref#0002.**
한 회사가 REST 기반 API를 통해 여러 고객에게 날씨 데이터를 제공하고 있습니다. API는 Amazon API Gateway에서 호스팅되며 각 API 작업에 대해 다양한 AWS Lambda 함수와 통합됩니다. 이 회사는 DNS에 Amazon Route 53을 사용하고 Weather.example.com이라는 리소스 레코드를 생성했습니다. 회사는 API에 대한 데이터를 Amazon DynamoDB 테이블에 저장합니다. 회사에는 API에 다른 AWS 리전으로 장애 조치할 수 있는 기능을 제공하는 솔루션이 필요합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 새 지역에 새로운 Lambda 함수 세트를 배포합니다. 두 리전의 Lambda 함수를 대상으로 하여 엣지 최적화 API 엔드포인트를 사용하도록 API Gateway API를 업데이트합니다. DynamoDB 테이블을 전역 테이블로 변환합니다.
> **B.** 다른 지역에 새로운 API Gateway API 및 Lambda 함수를 배포합니다. Route 53 DNS 레코드를 다중값 응답으로 변경합니다. 답변에 두 API 게이트웨이 API를 모두 추가합니다. 대상 상태 모니터링을 활성화합니다. DynamoDB 테이블을 전역 테이블로 변환합니다.
> **C.** 다른 지역에 새로운 API Gateway API 및 Lambda 함수를 배포합니다. Route 53 DNS 레코드를 장애 조치 레코드로 변경합니다. 대상 상태 모니터링을 활성화합니다. DynamoDB 테이블을 전역 테이블로 변환합니다.

D. 새 지역에 새 API 게이트웨이 API를 배포합니다. Lambda 함수를 전역 함수로 변경합니다. Route 53 DNS 레코드를 다중값 응답으로 변경합니다. 답변에 두 API 게이트웨이 API를 모두 추가합니다. 대상 상태 모니터링을 활성화합니다. DynamoDB 테이블을 전역 테이블로 변환합니다.

해설
정답: C
설명: 회사가 API의 다른 AWS 리전으로의 장애 조치 기능을 필요로 하는 경우, 다음과 같은 단계를 따라야 합니다.
새로운 AWS 리전에 새로운 API Gateway API 및 Lambda 함수를 배포합니다.
Route 53 DNS 레코드를 장애 조치(failover) 레코드로 변경합니다.
대상 상태 모니터링을 활성화하여 각 리전의 API Gateway와 Lambda 함수가 작동하는지 모니터링 합니다.
DynamoDB 테이블을 글로벌 테이블로 변환하여 여러 리전 간에 데이터를 동기화합니다.
이러한 단계를 따르면 API가 한 리전에서의 장애 시에 다른 리전으로 자동으로 전환되어 안정적으로 운영될 수 있습니다. 따라서 옵션 C가 이 요구사항을 충족하는 가장 적절한 솔루션입니다.

◆ | **Q#0003.** | **Ref#0003.**
회사는 Production이라는 단일 OU가 있는 AWS Organizations를 사용하여 여러 계정을 관리합니다. 모든 계정은 Production OU의 구성원입니다. 관리자는 조직 루트의 거부 목록 SCP를 사용하여 제한된 서비스에 대한 액세스를 관리합니다.
회사는 최근 새로운 사업부를 인수하고 새 사업부의 기존 AWS 계정을 조직에 초대했습니다. 온보딩 후 새 사업부의 관리자는 회사 정책을 충족하도록 기존 AWS Config 규칙을 업데이트할 수 없다는 사실을 발견했습니다.
관리자가 추가 장기 유지 관리를 도입하지 않고도 현재 정책을 변경하고 계속 시행할 수 있게 해주는 옵션은 무엇입니까?

A. AWS Config에 대한 액세스를 제한하는 조직의 루트 SCP를 제거하십시오. 회사의 표준 AWS Config 규칙에 대한 AWS Service Catalog 제품을 생성하고 새 계정을 포함하여 조직 전체에 배포합니다.
B. 새 계정에 대해 Onboarding이라는 임시 OU를 만듭니다. AWS Config 작업을 허용하려면 온보딩 OU에 SCP를 적용하세요. AWS Config 조정이 완료되면 새 계정을 프로덕션 OU로 이동합니다.
C. 조직의 루트 SCP를 거부 목록 SCP에서 변환하여 필요한 서비스만 허용하도록 목록 SCP를 허용합니다. 새 계정의 보안 주체에 대해서만 AWS Config 작업을 허용하는 SCP를 조직의 루트에 임시로 적용합니다.
D. 새 계정을 위한 임시 Onboarding OU를 생성합니다. Onboarding OU에 AWS Config 작업을 허용하는 SCP를 적용합니다. 회사의 루트 SCP를 Production OU로 이동합니다. AWS Config의 조정이 완료되면 새 계정을 Production OU로 이동합니다.

해설
정답: D
설명: 이 옵션은 새로운 비즈니스 계정을 임시 OU로 이동하여 새로운 계정이 AWS Config 규칙을 업데이트할 수 있도록 허용하는 것입니다
이를 통해 새로운 계정은 새로운 설정을 수행할 수 있게 되지만, 동시에 기존의 회사 정책에 영향을 주지 않습니다.
이후에는 루트 SCP를 Production OU로 이동시킵니다. 이렇게 하면 새로운 계정은 이전에 적용된 정책에 영향을 받지 않으면서도 새로운 AWS Config 규칙을 업데이트할 수 있게 됩니다.
이것은 임시적으로 새로운 계정에 대한 규칙을 완화하고, 이후에는 이를 Production OU로 이동하여 전체 조직의 정책을 유지하는 방법입니다.

◆ | **Q#0004.** | **Ref#0004.**
회사는 온프레미스 데이터 센터에서 2계층 웹 기반 애플리케이션을 실행하고 있습니다. 애플리케이션 계층은 상태 저장 애플리케이션을 실행하는 단일 서버로 구성됩니다. 애플리케이션은 별도의 서버에서 실행되는 PostgreSQL 데이터베이스에 연결됩니다. 애플리케이션의 사용자 기반이 크게 성장할 것으로 예상되므로 회사는 애플리케이션과 데이터베이스를 AWS로 마이그레이션하고 있습니다. 이 솔루션은 Amazon Aurora PostgreSQL,

Amazon EC2 Auto Scaling 및 Elastic Load Balancing을 사용합니다.
애플리케이션 및 데이터베이스 계층의 확장을 허용하는 일관된 사용자 경험을 제공하는 솔루션은 무엇입니까?

A. Aurora 복제본에 대해 Aurora Auto Scaling을 활성화합니다. 미해결 요청 라우팅 알고리즘이 가장 적고 고정 세션이 활성화된 Network Load Balancer를 사용합니다.
B. Aurora 작성자에 대해 Aurora Auto Scaling을 활성화합니다. 라운드 로빈 라우팅 알고리즘과 고정 세션이 활성화된 Application Load Balancer를 사용합니다.
C. Aurora 복제본에 대해 Aurora Auto Scaling을 활성화합니다. 라운드 로빈 라우팅 및 고정 세션이 활성화된 Application Load Balancer를 사용합니다.
D. Aurora 작성자에 대해 Aurora Scaling을 활성화합니다. 미해결 요청 라우팅 알고리즘이 가장 적고 고정 세션이 활성화된 Network Load Balancer를 사용합니다.

해설
정답: C.
C는 Aurora Replicas를 위해 Aurora Auto Scaling을 활성화하고, 라운드 로빈 라우팅 알고리즘과 스티키 세션을 활성화한 Application Load Balancer를 사용합니다.
이렇게 하면 일관된 사용자 경험을 제공하면서 애플리케이션 및 데이터베이스 계층을 확장하는 데 가장 적합합니다.
A, B, D 옵션은 Aurora Auto Scaling을 Aurora Replicas가 아닌 다른 대상에 적용하거나 잘못된 로드 밸런싱 알고리즘을 선택하고 있습니다.

◆ | **Q#0005.** | **Ref#0005.**
회사는 서비스를 사용하여 회사가 온프레미스에서 호스팅하는 애플리케이션에서 메타데이터를 수집합니다. TV 및 인터넷 라디오와 같은 소비자 장치는 애플리케이션에 액세스합니다. 많은 구형 장치는 특정 HTTP 헤더를 지원하지 않으며 이러한 헤더가 응답에 있을 때 오류를 표시합니다. 회사는 User-Agent 헤더로 식별한 이전 장치로 전송된 응답에서 지원되지 않는 헤더를 제거하도록 온프레미스 로드 밸런서를 구성했습니다.
회사는 서비스를 AWS로 마이그레이션하고, 서버리스 기술을 채택하고, 이전 장치를 지원하는 기능을 유지하기를 원합니다. 회사는 이미 애플리케이션을 AWS Lambda 함수 세트로 마이그레이션했습니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 메타데이터 서비스용 Amazon CloudFront 배포를 생성합니다. ALB(Application Load Balancer)를 생성합니다. ALB에 요청을 전달하도록 CloudFront 배포를 구성합니다. 각 요청 유형에 대해 올바른 Lambda 함수를 호출하도록 ALB를 구성합니다. User-Agent 헤더 값을 기반으로 문제가 있는 헤더를 제거하는 CloudFront 함수를 생성합니다.
B. 메타데이터 서비스용 Amazon API Gateway REST API를 생성합니다. 각 요청 유형에 대해 올바른 Lambda 함수를 호출하도록 API 게이트웨이를 구성합니다. User-Agent 헤더 값을 기반으로 문제가 있는 헤더를 제거하도록 기본 게이트웨이 응답을 수정합니다.
C. 메타데이터 서비스를 위한 Amazon API Gateway HTTP API를 생성합니다. 각 요청 유형에 대해 올바른 Lambda 함수를 호출하도록 API 게이트웨이를 구성합니다. User-Agent의 값을 기반으로 문제가 있는 헤더를 제거하는 응답 매핑 템플릿을 만듭니다. 응답 데이터 매핑을 HTTP API와 연결합니다.
D. 메타데이터 서비스용 Amazon CloudFront 배포를 생성합니다. ALB(Application Load Balancer)를 생성합니다. ALB에 요청을 전달하도록 CloudFront 배포를 구성합니다. 각 요청 유형에 대해 올바른 Lambda 함수를 호출하도록 ALB를 구성합니다. User-Agent 헤더 값을 기반으로 최종 사용자 요청에 대한 응답으로 문제가 있는 헤더를 제거하는 Lambda@Edge 함수를 생성합니다.

해설
정답: D
A와 D 옵션 모두 CloudFront, ALB, Lambda 함수를 활용하고 있습니다.
그러나 문제에서 언급된 '회사는 User-Agent 헤더로 식별한 이전 장치로 전송된 응답에서 지원되지 않는 헤더를 제거하도록' 요구사항을 고려할 때 올바른 답은 D입니다.
B 및 C 옵션은 Amazon API Gateway를 사용하여 Lambda 함수에 요청을 전달하고 응답을 처리하는 방법을 기반으로 합니다.

그러나 이러한 옵션들은 User-Agent 헤더를 기반으로 특정 헤더를 제거하는 기능을 제공하지 않습니다

◆ | **Q#0006.** | **Ref#0006.**
소매 회사는 비즈니스 파트너인 다른 회사에 일련의 데이터 파일을 제공해야 합니다. 이러한 파일은 소매 회사에 속한 계정 A의 Amazon S3 버킷에 저장됩니다. 비즈니스 파트너 회사는 IAM 사용자 중 한 명인 User_DataProcessor가 자체 AWS 계정(계정 B)에서 파일에 액세스하기를 원합니다.
User_DataProcessor가 S3 버킷에 성공적으로 액세스할 수 있도록 회사는 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

A. 계정 A의 S3 버킷에 대한 CORS(교차 원본 리소스 공유) 기능을 활성화합니다.
B. 계정 A에서 S3 버킷 정책을 다음과 같이 설정합니다.

```
{
   "Effect": "Allow",
   "Action": [
       "s3:GetObject",
       "s3:ListBucket"
   ],
   "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

C. 계정 A에서 S3 버킷 정책을 다음과 같이 설정합니다.

```
{
   "Effect": "Allow",
   "Principal": {
       "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
   },
   "Action": [
       "s3:GetObject",
       "s3:ListBucket"
   ],
   "Resource": [
       "arn:aws:s3:::AccountABucketName/*"
   ]
}
```

D. 계정 B에서 User_DataProcessor의 권한을 다음과 같이 설정합니다.

```
{
   "Effect": "Allow",
   "Action": [
       "s3:GetObject",
       "s3:ListBucket"
   ],
   "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

E. 계정 B에서 User_DataProcessor의 권한을 다음과 같이 설정합니다.

```
{
   "Effect": "Allow",
   "Principal": {
       "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
   },
   "Action": [
       "s3:GetObject",
       "s3:ListBucket"
   ],
   "Resource": [
       "arn:aws:s3:::AccountABucketName/*"
   ]
}
```

해설

정답: C, D
Account B의 IAM 사용자가 Account A의 S3 버킷에 액세스할 수 있도록 하려면 다음 단계를 수행해야 합니다
Account A에서 IAM 사용자 B에서 S3 버킷에 필요한 작업(GetObject 및 ListBucket)을 수행할 수 있도록 Bucket 정책을 설정해야 합니다.
이는 Account B의 IAM 사용자에게 Bucket 및 그 내용에 대한 필요한 작업을 수행할 수 있도록 하는 Bucket 정책에 명령문을 추가하여 수행됩니다.
Account B에서 IAM 사용자인 User_DataProcessor가 S3 버킷 및 해당 내용에 대해 필요한 작업(GetObject 및 ListBucket)을 수행할 수 있도록 하는 IAM 정책을 생성해야 합니다.
이 정책은 IAM 사용자가 수행할 수 있는 작업 및 S3 버킷의 ARN을 참조해야 합니다.
참고: Account A의 S3 버킷에서 Cross-Origin Resource Sharing (CORS) 기능을 활성화할 필요가 없습니다. CORS는 일반적으로 웹 브라우저가 서로 다른 도메인의 리소스에 액세스할 수 있도록 하는 데 사용됩니다.

◆ | **Q#0007.** | **Ref#0007.**
한 회사가 Amazon EC2 인스턴스에서 기존 웹 애플리케이션을 실행하고 있습니다. 회사는 애플리케이션을 컨테이너에서 실행되는 마이크로서비스로 리팩터링해야 합니다. 별도의 애플리케이션 버전이 프로덕션과 테스트라는 두 가지 서로 다른 환경에 존재합니다. 애플리케이션 부하는 가변적이지만 최소 부하와 최대 부하가 알려져 있습니다. 솔루션 설계자는 운영 복잡성을 최소화하는 서버리스 아키텍처로 업데이트된 애플리케이션을 설계해야 합니다.
이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 컨테이너 이미지를 AWS Lambda에 함수로 업로드합니다. 예상되는 최대 로드를 처리하기 위해 연결된 Lambda 함수에 대한 동시성 제한을 구성합니다. Amazon API Gateway 내에서 두 개의 개별 Lambda 통합을 구성합니다. 하나는 프로덕션용이고 다른 하나는 테스트용입니다.
B. 컨테이너 이미지를 Amazon Elastic Container Registry(Amazon ECR)에 업로드합니다. 예상 로드를 처리하기 위해 Fargate 시작 유형을 사용하여 자동 확장된 Amazon Elastic Container Service(Amazon ECS) 클러스터 2개를 구성합니다. ECR 이미지에서 작업을 배포합니다. 트래픽을 ECS 클러스터로 전달하도록 두 개의 별도 Application Load Balancer를 구성합니다.
C. 컨테이너 이미지를 Amazon Elastic Container Registry(Amazon ECR)에 업로드합니다. 예상 로드를 처리하기 위해 Fargate 시작 유형을 사용하여 자동 확장된 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터 2개를 구성합니다. ECR 이미지에서 작업을 배포합니다. 트래픽을 EKS 클러스터로 전달하도록 두 개의 별도 Application Load Balancer를 구성합니다.
D. 컨테이너 이미지를 AWS Elastic Beanstalk에 업로드합니다. Elastic Beanstalk에서는 프로덕션 및 테스트를 위해 별도의 환경과 배포를 생성합니다. 트래픽을 Elastic Beanstalk 배포로 전달하도록 두 개의 별도 Application Load Balancer를 구성합니다.

해설
정답: B
이 옵션은 Amazon Elastic Container Registry (Amazon ECR)에 컨테이너 이미지를 업로드하고, 예상되는 부하를 처리하기 위해 Fargate 로케이션 유형과 함께 두 개의 자동 확장 Amazon Elastic Container Service (Amazon ECS) 클러스터를 구성합니다.
Amazon ECS에서 ECR 이미지를 통해 작업을 배포하고, 두 개의 별도 Application Load Balancer를 구성하여 트래픽을 ECS 클러스터로 전달합니다.
이 방법은 서비스 아키텍처를 사용하면서 비용을 최소화하고 운영 복잡성을 최소화할 수 있는 방법입니다.

◆ | **Q#0008.** | **Ref#0008.**
한 회사에는 ALB(Application Load Balancer) 뒤에 있는 Amazon EC2 인스턴스 집합에서 실행되는 다중 계층 웹 애플리케이션이 있습니다. 인스턴스는 Auto Scaling 그룹에 있습니다. ALB 및 Auto Scaling 그룹은 백업 AWS 지역에 복제됩니다. Auto Scaling 그룹의 최소값과 최대값은 0으로 설정됩니다. Amazon RDS 다중 AZ DB 인스턴스는 애플리케이션의 데이터를 저장합니다. DB 인스턴스의 백업 리전에 읽기 전용 복제본이 있습니다. 애플리케이션은

Amazon Route 53 레코드를 사용하여 최종 사용자에게 엔드포인트를 제공합니다.
회사는 애플리케이션에 백업 리전으로 자동 장애 조치하는 기능을 제공하여 RTO를 15분 미만으로 줄여야 합니다.
회사는 액티브-액티브 전략을 수행할 만큼 충분한 예산을 갖고 있지 않습니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 권장해야 합니까?

> **A.** 두 ALB 간에 트래픽을 로드 밸런싱하는 지연 시간 기반 라우팅 정책을 사용하여 애플리케이션의 Route 53 레코드를 재구성합니다. 백업 리전에서 AWS Lambda 함수를 생성하여 읽기 전용 복제본을 승격하고 Auto Scaling 그룹 값을 수정합니다. 기본 리전의 ALB에 대한 HTTPCode_Target_5XX_Count 지표를 기반으로 Amazon CloudWatch 경보를 생성합니다. Lambda 함수를 호출하도록 CloudWatch 경보를 구성합니다.
> **B.** 백업 리전에서 AWS Lambda 함수를 생성하여 읽기 전용 복제본을 승격하고 Auto Scaling 그룹 값을 수정합니다. 웹 애플리케이션을 모니터링하고 상태 확인 상태가 비정상일 때 Amazon Simple 알림 서비스(Amazon SNS) 알림을 Lambda 함수에 보내는 상태 확인으로 Route 53을 구성합니다. 상태 확인 실패가 발생할 경우 백업 리전의 ALB로 트래픽을 라우팅하는 장애 조치 정책으로 애플리케이션의 Route 53 레코드를 업데이트합니다.
> **C.** 백업 리전의 Auto Scaling 그룹이 기본 리전의 Auto Scaling 그룹과 동일한 값을 갖도록 구성합니다. 두 ALB 간에 트래픽을 로드 밸런싱하는 지연 시간 기반 라우팅 정책을 사용하여 애플리케이션의 Route 53 레코드를 재구성합니다. 읽기 복제본을 제거합니다. 읽기 전용 복제본을 독립형 RDS DB 인스턴스로 교체합니다. 스냅샷과 Amazon S3를 사용하여 RDS DB 인스턴스 간에 교차 리전 복제를 구성합니다.
> **D.** 두 개의 ALB를 동일한 가중치 대상으로 사용하여 AWS Global Accelerator에서 엔드포인트를 구성합니다. 백업 리전에서 AWS Lambda 함수를 생성하여 읽기 전용 복제본을 승격하고 Auto Scaling 그룹 값을 수정합니다. 기본 리전의 ALB에 대한 HTTPCode_Target_5XX_Count 지표를 기반으로 Amazon CloudWatch 경보를 생성합니다. Lambda 함수를 호출하도록 CloudWatch 경보를 구성합니다.
>
> 해설
> 정답: B
> 이 옵션은 백업 리전에 있는 AWS Lambda 함수를 사용하여 읽기 전용 레플리카를 프로모션하고 Auto Scaling 그룹 값을 수정합니다.
> Route 53을 웹 애플리케이션을 모니터하는 health check과 Amazon SNS 알림을 지원하는 Health Check을 만들고 Health Check 상태가 비정상일 경우 Amazon SNS 알림을 Lambda 함수에 전송하도록 구성합니다.
> Web 애플리케이션의 Route 53 레코드를 변경하여 건강 검사 실패시 트래픽을 백업 리전의 ALB로 전송하는 페일오버 정책을 사용합니다.
> 이 방법을 통해 솔루션아키텍트는 회사가 RTO를 줄이고 자동화된 백업 리전 페일오버 기능을 도입할 수 있게 됩니다.

◆ | Q#0009. | Ref#0009.
한 회사가 단일 Amazon EC2 인스턴스에서 중요한 애플리케이션을 호스팅하고 있습니다. 애플리케이션은 인 메모리 데이터 스토어를 위해 Redis 단일 노드 클러스터용 Amazon ElastiCache를 사용합니다. 애플리케이션은 관계형 데이터베이스에 MariaDB DB 인스턴스용 Amazon RDS를 사용합니다. 애플리케이션이 작동하려면 인프라의 각 부분이 정상이어야 하며 활성 상태여야 합니다.
솔루션 설계자는 가동 중지 시간을 최소화하면서 인프라가 오류로부터 자동으로 복구될 수 있도록 애플리케이션의 아키텍처를 개선해야 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽을 분산시킵니다. EC2 인스턴스가 최소 2개의 인스턴스 용량을 갖는 Auto Scaling 그룹의 일부인지 확인하십시오.
> **B.** Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽을 분산시킵니다. EC2 인스턴스가 무제한 모드로 구성되어 있는지 확인하십시오.
> **C.** 동일한 가용 영역에 읽기 전용 복제본을 생성하도록 DB 인스턴스를 수정합니다. 장애 시나리오

에서 읽기 전용 복제본을 기본 DB 인스턴스로 승격합니다.
D. DB 인스턴스를 수정하여 두 개의 가용 영역에 걸쳐 확장되는 다중 AZ 배포를 생성합니다.
E. Redis용 ElastiCache 클러스터에 대한 복제 그룹을 생성합니다. 최소 2개의 인스턴스 용량이 있는 Auto Scaling 그룹을 사용하도록 클러스터를 구성합니다.
F. Redis용 ElastiCache 클러스터에 대한 복제 그룹을 생성합니다. 클러스터에서 다중 AZ를 활성화합니다.

해설
정답:
A는 여러 EC2 인스턴스 간에 트래픽을 분산하기 위해 Elastic Load Balancer를 사용하고, EC2 인스턴스가 최소 두 개의 인스턴스로 구성된 Auto Scaling 그룹의 일부임을 확인합니다.
D는 DB 인스턴스를 수정하여 두 개의 가용 영역을 확장하는 Multi-AZ 배포를 생성합니다.
F는 ElastiCache for Redis 클러스터에 Multi-AZ를 활성화 하는 것은 Redis 클러스터의 가용성을 향상시키는 좋은 방법 중 하나입니다.
Multi-AZ 설정은 Redis 클러스터의 보다 안정적인 운영을 지원하고, 장애 발생 시 클러스터의 가용성을 확보할 수 있습니다.

따라서 A, D, F의 조합이 가용성을 향상시키고 자동화된 장애 복구 기능을 제공하는데 가장 효과적입니다.

◆ | **Q#0010.** | **Ref#0010.**
한 소매 회사가 AWS에서 전자상거래 애플리케이션을 운영하고 있습니다. 애플리케이션은 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스에서 실행됩니다. 회사는 Amazon RDS DB 인스턴스를 데이터베이스 백엔드로 사용합니다. Amazon CloudFront는 ALB를 가리키는 하나의 오리진으로 구성됩니다. 정적 콘텐츠가 캐시됩니다. Amazon Route 53은 모든 공개 영역을 호스팅하는 데 사용됩니다.
애플리케이션 업데이트 후 ALB는 때때로 502 상태 코드(잘못된 게이트웨이) 오류를 반환합니다. 근본 원인은 ALB에 반환되는 잘못된 HTTP 헤더입니다. 오류가 발생한 직후 솔루션 설계자가 웹 페이지를 다시 로드하면 웹 페이지가 성공적으로 반환됩니다.
회사가 문제를 해결하는 동안 솔루션 설계자는 방문자에게 표준 ALB 오류 페이지 대신 사용자 정의 오류 페이지를 제공해야 합니다.
최소한의 운영 오버헤드로 이 요구 사항을 충족하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. Amazon S3 버킷을 생성합니다. 정적 웹페이지를 호스팅하도록 S3 버킷을 구성합니다. 사용자 정의 오류 페이지를 Amazon S3에 업로드합니다.
B. ALB 상태 확인 응답 Target.FailedHealthChecks가 0보다 큰 경우 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다. 공개적으로 액세스 가능한 웹 서버를 가리키도록 ALB에서 전달 규칙을 수정하도록 Lambda 함수를 구성합니다.
C. 상태 확인을 추가하여 기존 Amazon Route 53 레코드를 수정합니다. 상태 확인에 실패할 경우 대체 대상을 구성합니다. 공개적으로 액세스할 수 있는 웹페이지를 가리키도록 DNS 레코드를 수정합니다.
D. ALB 상태 확인 응답 Elb.InternalError가 0보다 큰 경우 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다. 공개 액세스 가능한 웹 서버를 가리키도록 ALB에서 전달 규칙을 수정하도록 Lambda 함수를 구성합니다.
E. CloudFront 사용자 지정 오류 페이지를 구성하여 사용자 지정 오류 응답을 추가합니다. 공개적으로 액세스할 수 있는 웹 페이지를 가리키도록 DNS 레코드를 수정합니다.

해설
정답: A,E
A는 502 상태 코드(장애 게이트웨이) 오류가 발생할 때 사용자 정의 오류 페이지를 제공하기 위해 Amazon S3 버킷을 생성하고 정적 웹페이지를 호스팅하여 운영 오버헤드를 최소화하면서 사용자 정의 오류 페이지를 쉽게 제공할 수 있습니다.
E는 CloudFront를 사용하여 사용자 정의 오류 페이지를 구성하고, DNS 레코드를 수정하여 이 페이

지로 이용자를 리디렉션하는 방법입니다. 이 방법 역시 운영 오버헤드를 최소화하면서 사용자 정의 오류 페이지를 빠르게 제공할 수 있는 방법 중 하나입니다
이 두 가지 단계를 조합하여 사용자 정의 오류 페이지를 제공하면서 최소한의 운영 오버헤드로 경고 페이지 관리 문제를 해결할 수 있습니다.

011 (김성원) 4회차 完

◆ | **Q#0011.** | **Ref#0011.**
회사에는 많은 AWS 계정이 있으며 AWS Organizations를 사용하여 모든 계정을 관리합니다. 솔루션 설계자는 회사가 여러 계정에서 공통 네트워크를 공유하는 데 사용할 수 있는 솔루션을 구현해야 합니다.
회사의 인프라 팀에는 VPC가 있는 전용 인프라 계정이 있습니다. 인프라 팀은 이 계정을 사용하여 네트워크를 관리해야 합니다. 개인 계정은 자신의 네트워크를 관리할 수 없습니다. 그러나 개별 계정은 서브넷 내에서 AWS 리소스를 생성할 수 있어야 합니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 작업 조합을 수행해야 합니까? (2개를 선택하세요.)

A. 인프라 계정에 전송 게이트웨이를 생성합니다.
B. AWS Organizations 마스터 계정에서 리소스 공유를 활성화합니다.
C. AWS Organizations의 조직 내 각 AWS 계정에 VPC를 생성합니다. 인프라 계정의 VPC와 동일한 CIDR 범위 및 서브넷을 공유하도록 VPC를 구성합니다. 각 개별 계정의 VPC를 인프라 계정의 VPC와 피어링합니다.
D. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다. 공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다. 리소스 공유와 연결할 각 서브넷을 선택합니다.
E. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다. 공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다. 리소스 공유와 연결할 각 접두사 목록을 선택합니다.

해설
정답: B,D

B는 조직이 계정 간에 리소스를 공유할 수 있도록 하기 때문에 필요합니다.
D는 인프라 계정이 조직의 다른 계정과 특정 서브넷을 공유할 수 있도록 허용하여 다른 계정이 자체 네트워크를 관리할 필요 없이 해당 서브넷 내에 리소스를 생성할 수 있도록 하기 때문에 필요합니다.

-참고-
A - 고객은 VPC가 1개뿐이므로 TGW가 필요하지 않습니다.
C - CIDR이 겹치는 경우에는 불가능하고 VPC가 1개이므로 이 솔루션에는 필요하지 않음
E - 접두사 목록을 사용하여 RAM을 통해 리소스를 공유할 수 없습니다.

◆ | **Q#0012.** | **Ref#0012.**
회사에서는 타사 SaaS(Software-as-a-Service) 애플리케이션을 사용하려고 합니다. 타사 SaaS 애플리케이션은 여러 API 호출을 통해 사용됩니다. 타사 SaaS 애플리케이션도 VPC 내부의 AWS에서 실행됩니다.
회사는 VPC 내부에서 타사 SaaS 애플리케이션을 사용합니다. 회사에는 인터넷을 통과하지 않는 개인 연결의 사용을 의무화하는 내부 보안 정책이 있습니다. 회사 VPC에서 실행되는 리소스는 회사 VPC 외부에서 액세스할 수 없습니다. 모든 권한은 최소 권한의 원칙을 준수해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS PrivateLink 인터페이스 VPC 엔드포인트를 생성합니다. 이 끝점을 타사 SaaS 애플리케이션이 제공하는 끝점 서비스에 연결합니다. 엔드포인트에 대한 액세스를 제한하려면 보안 그룹을 생성하십시오. 보안 그룹을 엔드포인트와 연결합니다.
B. 타사 SaaS 애플리케이션과 회사 VPC 간에 AWS Site-to-Site VPN 연결을 생성합니다. VPN 터널

전반에 걸쳐 액세스를 제한하도록 네트워크 ACL을 구성합니다.
C. 피어링 연결에 필요한 경로를 추가하여 타사 SaaS 애플리케이션과 회사 VPUpdate 라우팅 테이블 간에 VPC 피어링 연결을 생성합니다.
D. AWS PrivateLink 엔드포인트 서비스를 생성합니다. 타사 SaaS 공급자에게 이 엔드포인트 서비스에 대한 인터페이스 VPC 엔드포인트를 생성하도록 요청하세요. 타사 SaaS 공급자의 특정 계정에 엔드포인트 서비스에 대한 권한을 부여합니다.

해설
정답: A

인터넷을 통하지 않고 비공개로 모든 서비스에 액세스할 수 있는 VPC 인터페이스 엔드포인트입니다.
인터넷을 통과하는 트래픽 없이 회사의 VPC와 타사 SaaS 애플리케이션 VPC 간에 안전한 비공개 연결을 생성하는 AWS PrivateLink를 사용합니다.
보안 그룹을 사용하고 엔드포인트 서비스에 대한 액세스를 제한하는 것은 최소 권한의 원칙을 따릅니다.

◆ | **Q#0013.** | **Ref#0013.**
회사에서는 서버에 대한 패치 프로세스를 구현해야 합니다. 온프레미스 서버와 Amazon EC2 인스턴스는 다양한 도구를 사용하여 패치를 수행합니다. 관리에는 모든 서버와 인스턴스의 패치 상태를 보여주는 단일 보고서가 필요합니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 조치를 취해야 합니까?

A. AWS Systems Manager를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리하십시오. Systems Manager를 사용하여 패치 규정 준수 보고서를 생성하세요.
B. AWS OpsWorks를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리합니다. OpsWorks와 Amazon QuickSight 통합을 사용하여 패치 규정 준수 보고서를 생성합니다.
C. Amazon EventBridge 규칙을 사용하여 AWS Systems Manager 패치 수정 작업을 예약하여 패치를 적용합니다. Amazon Inspector를 사용하여 패치 규정 준수 보고서를 생성합니다.
D. AWS OpsWorks를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리합니다. AWS X-Ray를 사용하여 패치 상태를 AWS Systems Manager OpsCenter에 게시하여 패치 규정 준수 보고서를 생성합니다.

해설
정답: A

AWS OpsWorks는 EC2 인스턴스에서 애플리케이션의 배포, 구성 및 관리를 자동화하는 방법을 제공하는 구성 관리 서비스입니다.
이는 애플리케이션의 전체 수명주기를 관리하는 데 도움이 되도록 설계되었습니다.

◆ | **Q#0014.** | **Ref#0014.**
한 회사가 Application Load Balancer 뒤에 있는 Auto Scaling 그룹의 여러 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 애플리케이션의 로드는 하루 종일 다양하며 EC2 인스턴스는 정기적으로 확장 및 축소됩니다. EC2 인스턴스의 로그 파일은 15분마다 중앙 Amazon S3 버킷에 복사됩니다. 보안팀은 종료된 일부 EC2 인스턴스에서 로그 파일이 누락된 것을 발견했습니다.
로그 파일이 종료된 EC2 인스턴스에서 중앙 S3 버킷으로 복사되도록 보장하는 작업 세트는 무엇입니까?

A. 로그 파일을 Amazon S3에 복사하는 스크립트를 생성하고 EC2 인스턴스의 파일에 스크립트를 저장합니다. Auto Scaling 수명 주기 후크와 Amazon EventBridge 규칙을 생성하여 Auto Scaling 그룹에서 수명 주기 이벤트를 감지합니다. autoscaling:EC2_INSTANCE_TERMINATING 전환에서 AWS Lambda 함수를 호출하여 ABANDON을 Auto Scaling 그룹에 보내 종료를 방지하고, 스크립트를 실행하여 로그 파일을 복사하고, AWS SDK를 사용하여 인스턴스를 종료합니다.

B. 로그 파일을 Amazon S3에 복사하는 스크립트가 포함된 AWS 시스템 관리자 문서를 생성합니다. Auto Scaling 수명 주기 후크와 Amazon EventBridge 규칙을 생성하여 Auto Scaling 그룹에서 수명 주기 이벤트를 감지합니다. autoscaling:EC2_INSTANCE_TERMINATING 전환에서 AWS Lambda 함수를 호출하여 AWS 시스템 관리자 API SendCommand 작업을 호출하여 문서를 실행하여 로그 파일을 복사하고 CONTINUE를 Auto Scaling 그룹에 보내 인스턴스를 종료합니다.
C. 로그 전달 속도를 5분 간격으로 변경합니다. 로그 파일을 Amazon S3에 복사하는 스크립트를 생성하고 EC2 인스턴스 사용자 데이터에 스크립트를 추가합니다. EC2 인스턴스 종료를 감지하는 Amazon EventBridge 규칙을 생성합니다. AWS CLI를 사용하는 EventBridge 규칙에서 AWS Lambda 함수를 호출하여 사용자 데이터 스크립트를 실행하여 로그 파일을 복사하고 인스턴스를 종료합니다.
D. 로그 파일을 Amazon S3에 복사하는 스크립트를 사용하여 AWS 시스템 관리자 문서를 생성합니다. Amazon Simple 알림 서비스(Amazon SNS) 주제에 메시지를 게시하는 Auto Scaling 수명 주기 후크를 생성합니다. SNS 알림에서 AWS Systems Manager API SendCommand 작업을 호출하여 문서를 실행하여 로그 파일을 복사하고 ABANDON을 Auto Scaling 그룹에 보내 인스턴스를 종료합니다.

해설
정답: B

SM이 포함된 문서는 다른 인스턴스에서도 다시 활용할 수 있기 때문에 B가 더 나은 솔루션입니다.

-참고-
A- 종료 방지가 필요하지 않기 때문에 X
C- 5분 간격으로 인해 오버헤드나 지연이 발생하므로 X. 스크립트에 사용자 데이터를 사용하면 복잡해집니다.
D- SNS 때문에 X.

◆ | **Q#0015.** | **Ref#0015.**
회사에서 여러 AWS 계정을 사용하고 있습니다. DNS 레코드는 계정 A의 Amazon Route 53에 대한 프라이빗 호스팅 영역에 저장됩니다. 회사의 애플리케이션과 데이터베이스는 계정 B에서 실행됩니다.
솔루션 아키텍트는 새 VPC에 2계층 애플리케이션을 배포합니다. 구성을 단순화하기 위해 Amazon RDS 엔드포인트에 대한 db.example.com CNAME 레코드 세트가 Amazon Route 53의 프라이빗 호스팅 영역에 생성되었습니다.
배포 중에 애플리케이션을 시작하지 못했습니다. 문제 해결 결과 Amazon EC2 인스턴스에서 db.example.com을 확인할 수 없는 것으로 나타났습니다. 솔루션 설계자는 Route 53에서 레코드 세트가 올바르게 생성되었음을 확인했습니다.
이 문제를 해결하려면 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. 새 VPC의 별도 EC2 인스턴스에 데이터베이스를 배포합니다. 프라이빗 호스팅 영역에서 인스턴스의 프라이빗 IP에 대한 레코드 세트를 생성합니다.
B. SSH를 사용하여 애플리케이션 계층 EC2 인스턴스에 연결합니다. /etc/resolv.conf 파일에 RDS 엔드포인트 IP 주소를 추가합니다.
C. 계정 A의 프라이빗 호스팅 영역을 계정 B의 새 VPC와 연결하기 위한 권한 부여를 생성합니다.
D. 계정 B에서 예제 com 도메인에 대한 프라이빗 호스팅 영역을 생성합니다. AWS 계정 간에 Route 53 복제를 구성합니다.
E. 계정 B의 새 VPC를 계정 A의 호스팅 영역과 연결합니다. 계정 A의 연결 인증을 삭제합니다.

해설
정답: C,E

C : 다중 계정 AWS 설정에서 다른 계정의 VPC(계정 B)에 있는 한 계정(계정 A)의 Route 53 프라이빗 호스팅 영역을 사용하려면 먼저 권한 부여를 생성해야 하며 이 인증은 한 계정의 프라이빗 호스팅 영역을 다른 계정의 VPC와 연결하도록 허용하는 데 필요합니다. 이 단계를 통해 계정 전체의 프라이

빗 호스팅 영역에 저장된 DNS 레코드를 확인할 수 있습니다.

E : 옵션 C에서 생성된 권한 부여에 대한 후속 조치 입니다. 권한 부여가 완료되면 계정 B의 새 VPC를 계정 A의 프라이빗 호스팅 영역과 연결할 수 있으며, 이 연결을 통해 실제로 계정 B의 VPC 내의 EC2 인스턴스는 계정 A의 프라이빗 호스팅 영역을 사용하여 DNS 쿼리를 확인하여 db.example.com이 의도한 대로 확인될 수 있도록 합니다.

◆ | **Q#0016.** | **Ref#0016.**
한 회사는 Amazon EC2 인스턴스를 사용하여 블로그 사이트를 호스팅하기 위한 웹 집합을 배포했습니다. EC2 인스턴스는 ALB(Application Load Balancer) 뒤에 있으며 Auto Scaling 그룹에서 구성됩니다. 웹 애플리케이션은 모든 블로그 콘텐츠를 Amazon EFS 볼륨에 저장합니다.
회사는 최근 블로거가 자신의 게시물에 동영상을 추가할 수 있는 기능을 추가하여 이전 사용자 트래픽의 10배를 유치했습니다. 하루 중 사용량이 많은 시간대에 사용자는 사이트에 접속하거나 비디오를 시청하려고 할 때 버퍼링 및 시간 초과 문제를 보고합니다.
사용자의 문제를 해결하는 가장 비용 효율적이고 확장 가능한 배포는 무엇입니까?

A. 최대 I/O를 활성화하도록 Amazon EFS를 재구성합니다.
B. 인스턴스 스토어 볼륨을 저장용으로 사용하도록 블로그 사이트를 업데이트합니다. 사이트 콘텐츠를 시작 시 볼륨에 복사하고 종료 시 Amazon S3에 복사합니다.
C. Amazon CloudFront 배포를 구성합니다. 배포를 S3 버킷으로 지정하고 비디오를 EFS에서 Amazon S3로 마이그레이션합니다.
D. 모든 사이트 콘텐츠에 대해 Amazon CloudFront 배포를 설정하고 ALB에서 배포를 지정합니다.

해설
정답: C

C와 D는 모두 실행 가능합니다. 그러나 비용효율적인 면에서는 C가 유리합니다.

◆ | **Q#0017.** | **Ref#0017.**
글로벌 사무소가 있는 회사는 단일 AWS 리전에 대한 단일 1Gbps AWS Direct Connect 연결을 보유합니다. 회사의 온프레미스 네트워크는 연결을 사용하여 AWS 클라우드에 있는 회사 리소스와 통신합니다. 연결에는 단일 VPC에 연결되는 단일 프라이빗 가상 인터페이스가 있습니다.
솔루션 아키텍트는 동일한 리전에 중복 Direct Connect 연결을 추가하는 솔루션을 구현해야 합니다. 또한 솔루션은 회사가 다른 지역으로 확장함에 따라 동일한 Direct Connect 연결 쌍을 통해 다른 지역에 대한 연결을 제공해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Direct Connect 게이트웨이를 프로비저닝합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다. 두 번째 Direct Connect 연결을 생성합니다. 각 연결마다 새 프라이빗 가상 인터페이스를 생성하고 두 프라이빗 가상 인터페이스를 모두 Direct Connect 게이트웨이에 연결합니다. Direct Connect 게이트웨이를 단일 VPC에 연결합니다.
B. 기존 개인 가상 인터페이스를 유지합니다. 두 번째 Direct Connect 연결을 생성합니다. 새 연결에 새 프라이빗 가상 인터페이스를 생성하고 새 프라이빗 가상 인터페이스를 단일 VPC에 연결합니다.
C. 기존 프라이빗 가상 인터페이스를 유지합니다. 두 번째 Direct Connect 연결을 생성합니다. 새 연결에 새 퍼블릭 가상 인터페이스를 생성하고 새 퍼블릭 가상 인터페이스를 단일 VPC에 연결합니다.
D. 전송 게이트웨이를 프로비저닝합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다. 두 번째 Direct Connect 연결을 생성합니다. 각 연결마다 새 프라이빗 가상 인터페이스를 생성하고 두 프라이빗 가상 인터페이스를 모두 Transit Gateway에 연결합니다. 전송 게이트웨이를 단일 VPC와 연결합니다.

해설

정답: A

DCGW는 DC 연결을 모두 지원하고 다른 지역으로의 확장을 허용하므로 여기서 유일한 옵션입니다.
TGW는 여러 지역에 걸쳐 있지 않습니다.

◆ | **Q#0018.** | **Ref#0018.**
한 회사에 사용자가 짧은 동영상을 업로드할 수 있는 웹 애플리케이션이 있습니다. 비디오는 Amazon EBS 볼륨에 저장되고 분류를 위해 사용자 정의 인식 소프트웨어로 분석됩니다.
웹사이트에는 특정 달에 트래픽이 가장 많이 발생하는 가변적인 트래픽이 있는 정적 콘텐츠가 포함되어 있습니다.
아키텍처는 웹 애플리케이션용 Auto Scaling 그룹에서 실행되는 Amazon EC2 인스턴스와 Amazon SQS 대기열을 처리하기 위해 Auto Scaling 그룹에서 실행되는 EC2 인스턴스로 구성됩니다. 회사는 가능한 경우 AWS 관리형 서비스를 사용하여 운영 오버헤드를 줄이고 타사 소프트웨어에 대한 종속성을 제거하기 위해 애플리케이션을 재설계하려고 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 웹 애플리케이션에는 Amazon ECS 컨테이너를 사용하고 SQS 대기열을 처리하는 Auto Scaling 그룹에는 스팟 인스턴스를 사용하십시오. 사용자 지정 소프트웨어를 Amazon Rekognition으로 교체하여 비디오를 분류합니다.
B. 업로드된 비디오를 Amazon EFS에 저장하고 웹 애플리케이션용 EC2 인스턴스에 파일 시스템을 탑재합니다. Amazon Rekognition API를 호출하여 비디오를 분류하는 AWS Lambda 함수로 SQS 대기열을 처리합니다.
C. Amazon S3에서 웹 애플리케이션을 호스팅합니다. 업로드된 비디오를 Amazon S3에 저장합니다. S3 이벤트 알림을 사용하여 SQS 대기열에 이벤트를 게시합니다. Amazon Rekognition API를 호출하여 비디오를 분류하는 AWS Lambda 함수로 SQS 대기열을 처리합니다.
D. AWS Elastic Beanstalk를 사용하여 웹 애플리케이션용 Auto Scaling 그룹에서 EC2 인스턴스를 시작하고 SQS 대기열을 처리하기 위한 작업자 환경을 시작합니다. 사용자 지정 소프트웨어를 Amazon Rekognition으로 교체하여 비디오를 분류합니다.

해설
정답: C

서버리스 접근 방식을 다루는 Lambda, S3는 EFS보다 훨씬 우수하고 SQS는 S3의 이벤트를 처리합니다.

◆ | **Q#0019.** | **Ref#0019.**
회사에는 Amazon CloudFront, Amazon API Gateway 및 AWS Lambda 기능으로 구성된 서버리스 애플리케이션이 있습니다. 애플리케이션 코드의 현재 배포 프로세스는 Lambda 함수의 새 버전 번호를 생성하고 AWS CLI 스크립트를 실행하여 업데이트하는 것입니다. 새 함수 버전에 오류가 있는 경우 다른 CLI 스크립트는 함수의 이전 작업 버전을 배포하여 되돌립니다. 회사는 Lambda 함수가 제공하는 애플리케이션 로직의 새 버전을 배포하는 시간을 줄이고, 오류가 식별될 때 감지하고 되돌리는 시간도 줄이고자 합니다.
이것이 어떻게 이루어질 수 있습니까?

A. AWS CloudFront 배포 및 API 게이트웨이로 구성된 상위 스택과 Lambda 함수가 포함된 하위 스택을 사용하여 중첩된 AWS CloudFormation 스택을 생성하고 배포합니다. Lambda를 변경하려면 AWS CloudFormation 변경 세트를 생성하고 배포하세요. 오류가 발생하면 AWS CloudFormation 변경 세트를 이전 버전으로 되돌립니다.
B. AWS SAM 및 내장된 AWS CodeDeploy를 사용하여 새 Lambda 버전을 배포하고, 점차적으로 트래픽을 새 버전으로 이동하고, 트래픽 전 및 트래픽 후 테스트 기능을 사용하여 코드를 확인합니다. Amazon CloudWatch 경보가 트리거되면 롤백합니다.
C. AWS CLI 스크립트를 새 Lambda 버전을 배포하는 단일 스크립트로 리팩터링합니다. 배포가 완료되면 스크립트 테스트가 실행됩니다. 오류가 감지되면 이전 Lambda 버전으로 되돌립니다.

D. 새로운 Lambda 버전을 참조하는 새로운 API 게이트웨이 엔드포인트로 구성된 AWS CloudFormation 스택을 생성하고 배포합니다. CloudFront 오리진을 새 API 게이트웨이 엔드포인트로 변경하고, 오류를 모니터링하고, 감지되면 AWS CloudFront 오리진을 이전 API 게이트웨이 엔드포인트로 변경합니다.

해설
정답: B

AWS SAM은 CodeDeploy와 함께 내장되어 점진적인 제공을 제공합니다. AWS Lambda 배포. 몇 줄의 구성만으로 AWS SAM은 다음 작업을 수행합니다.
Lambda 함수의 새 버전을 배포하고 새 버전을 가리키는 별칭을 자동으로 생성합니다.
고객 트래픽이 예상대로 작동한다는 점에 만족할 때까지 점차적으로 새 버전으로 이동합니다. 업데이트가 제대로 작동하지 않으면 변경 사항을 롤백할 수 있습니다.
새로 배포된 코드가 올바르게 구성되었는지, 애플리케이션이 예상대로 작동하는지 확인하기 위해 트래픽 전 및 트래픽 후 테스트 기능을 정의합니다.
CloudWatch 경보가 트리거되면 배포를 자동으로 롤백합니다.

◆ | **Q#0020.** | **Ref#0020.**
한 회사에서는 대량의 보관 문서를 저장하고 회사 인트라넷을 통해 직원들이 해당 문서를 사용할 수 있도록 할 계획입니다. 직원은 VPC에 연결된 클라이언트 VPN 서비스를 통해 연결하여 시스템에 액세스합니다. 데이터는 대중이 접근할 수 없어야 합니다.
회사가 저장하고 있는 문서는 다른 곳의 물리적 매체에 보관된 데이터의 복사본입니다. 요청 횟수가 적습니다. 가용성과 검색 속도는 회사의 관심사가 아닙니다.
가장 저렴한 비용으로 이러한 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. Amazon S3 버킷을 생성합니다. S3 One Zone-IA(S3 One Zone-IA) 스토리지 클래스를 기본으로 사용하도록 S3 버킷을 구성합니다. 웹사이트 호스팅을 위해 S3 버킷을 구성합니다. S3 인터페이스 엔드포인트를 생성합니다. 해당 엔드포인트를 통해서만 액세스를 허용하도록 S3 버킷을 구성합니다.
B. 웹 서버를 실행하는 Amazon EC2 인스턴스를 시작합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 연결하여 EFS One Zone-Infrequent Access(EFS One Zone-IA) 스토리지 클래스에 보관된 데이터를 저장합니다. 프라이빗 네트워크에서만 액세스를 허용하도록 인스턴스 보안 그룹을 구성합니다.
C. 웹 서버를 실행하는 Amazon EC2 인스턴스를 시작합니다. Amazon Elastic Block Store(Amazon EBS) 볼륨을 연결하여 보관된 데이터를 저장합니다. Cold HDD(sc1) 볼륨 유형을 사용합니다. 프라이빗 네트워크에서만 액세스를 허용하도록 인스턴스 보안 그룹을 구성합니다.
D. Amazon S3 버킷을 생성합니다. S3 Glacier Deep Archive 스토리지 클래스를 기본값으로 사용하도록 S3 버킷을 구성합니다. 웹사이트 호스팅을 위해 S3 버킷을 구성합니다. S3 인터페이스 엔드포인트를 생성합니다. 해당 엔드포인트를 통해서만 액세스를 허용하도록 S3 버킷을 구성합니다.

해설
정답: A

A와D 중 답을 골라야 하는데 D는 더 저렴하지만 실행 가능하지 않습니다. 웹 호스팅에는 Deep Glacier 클래스의 S3 버킷을 사용할 수 없습니다.
그래서 정답은 A 입니다.

021 (나권서) 4회차 完

◆ | **Q#0021.** | **Ref#0021.**
회사는 사용자 인증을 위해 온프레미스 Active Directory 서비스를 사용하고 있습니다. 회사는 동일한 인증 서비스

를 사용하여 AWS Organizations를 사용하는 회사의 AWS 계정에 로그인하려고 합니다. 온프레미스 환경과 회사의 모든 AWS 계정 간에 AWS Site-to-Site VPN 연결이 이미 존재합니다.
회사의 보안 정책에 따라 사용자 그룹 및 역할을 기반으로 계정에 대한 조건부 액세스가 필요합니다. 사용자 ID는 단일 위치에서 관리되어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** SAML 2.0을 사용하여 Active Directory에 연결하도록 AWS IAM Identity Center(AWS Single Sign-On)를 구성합니다. SCIM(System for Cross-domain Identity Management) v2.0 프로토콜을 사용하여 자동 프로비저닝을 활성화합니다. ABAC(속성 기반 액세스 제어)를 사용하여 AWS 계정에 대한 액세스 권한을 부여합니다.
> **B.** IAM 자격 증명 센터를 자격 증명 소스로 사용하여 AWS IAM 자격 증명 센터(AWS Single Sign-On)를 구성합니다. SCIM(System for Cross-domain Identity Management) v2.0 프로토콜을 사용하여 자동 프로비저닝을 활성화합니다. IAM Identity Center 권한 세트를 사용하여 AWS 계정에 대한 액세스 권한을 부여합니다.
> **C.** 회사의 AWS 계정 중 하나에서 SAML 2.0 자격 증명 공급자를 사용하도록 AWS Identity and Access Management(IAM)를 구성합니다. 연합된 사용자에 매핑된 IAM 사용자를 프로비저닝합니다. Active Directory의 적절한 그룹에 해당하는 액세스 권한을 부여합니다. 교차 계정 IAM 사용자를 사용하여 필요한 AWS 계정에 대한 액세스 권한을 부여합니다.
> **D.** 회사의 AWS 계정 중 하나에서 OpenID Connect(OIDC) 자격 증명 공급자를 사용하도록 AWS Identity and Access Management(IAM)를 구성합니다. Active Directory의 적절한 그룹에 해당하는 연동 사용자에게 AWS 계정에 대한 액세스 권한을 부여하는 IAM 역할을 프로비저닝합니다. 교차 계정 IAM 역할을 사용하여 필요한 AWS 계정에 대한 액세스 권한을 부여합니다.
>
> 해설
> 정답: A
> IAM Identity Center(AWS Single Sign-On)을 사용하여 Active Directory와의 연결을 설정하고 단일 위치에서 사용자 ID를 관리할 수 있고
> SCIM 프로토콜을 사용하여 자동 프로비저닝을 활성화하여 사용자 관리를 자동화할 수 있으며
> ABAC을 사용하여 사용자 그룹과 역할에 기반한 조건부 액세스를 설정할 수 있어 회사의 보안 정책을 준수할 수 있음

◆ | **Q#0022.** | **Ref#0022.**
한 소프트웨어 회사가 Amazon API Gateway, AWS Lambda 함수 및 Amazon DynamoDB 테이블을 사용하여 REST API를 사용하는 애플리케이션을 배포했습니다. 애플리케이션은 PUT 요청 중에 오류 수가 증가하는 것을 보여줍니다. 대부분의 PUT 호출은 특정 API 키로 인증된 소수의 클라이언트에서 발생합니다.
솔루션 설계자는 다수의 PUT 요청이 하나의 클라이언트에서 발생한다는 것을 확인했습니다. API는 중요하지 않으며 클라이언트는 실패한 호출의 재시도를 허용할 수 있습니다. 그러나 이러한 오류는 고객에게 표시되며 API의 평판에 손상을 입히고 있습니다.
고객 경험을 개선하기 위해 솔루션 아키텍트가 권장해야 할 것은 무엇입니까?

> **A.** 클라이언트 애플리케이션에서 지수 백오프 및 불규칙 변형을 사용하여 재시도 논리를 구현합니다. 오류를 포착하고 설명적인 오류 메시지로 처리하는지 확인하세요.
> **B.** API 게이트웨이 수준에서 사용량 계획을 통해 API 조절을 구현합니다. 클라이언트 애플리케이션이 오류 없이 코드 429 응답을 처리하는지 확인하십시오.
> **C.** API 캐싱을 활성화하여 프로덕션 단계의 응답성을 향상시킵니다. 10분 동안 부하 테스트를 실행합니다. 캐시 용량이 워크로드에 적합한지 확인하십시오.
> **D.** 트래픽이 갑자기 증가하는 동안 필요한 리소스를 제공하기 위해 Lambda 함수 수준에서 예약된 동시성을 구현합니다.
>
> 해설
> 정답:B
> 클라이언트 응용 프로그램에서 API를 호출할 때 발생하는 PUT 요청 오류 문제를 해결하기 위해 API Gateway에서

API 쓰로틀링을 구현하는 것이 가장 적합하고 API 쓰로틀링을 통해 코드 429 응답을 보낼 수 있어 클라이언트가 요청을 조절할 수 있으며,
이를 통해 너무 많은 요청을 방지하고 과부하를 제어할 수 있음

◆ | **Q#0023.** | **Ref#0023.**
한 회사가 AWS에서 데이터 집약적인 애플리케이션을 실행하고 있습니다. 애플리케이션은 수백 개의 Amazon EC2 인스턴스 클러스터에서 실행됩니다. 공유 파일 시스템은 200TB의 데이터를 저장하는 여러 EC2 인스턴스에서도 실행됩니다. 애플리케이션은 공유 파일 시스템의 데이터를 읽고 수정하고 보고서를 생성합니다. 작업은 한 달에 한 번씩 실행되고, 공유 파일 시스템에서 파일의 하위 집합을 읽고, 완료하는 데 약 72시간이 걸립니다. 컴퓨팅 인스턴스는 Auto Scaling 그룹에서 확장되지만 공유 파일 시스템을 호스팅하는 인스턴스는 지속적으로 실행됩니다. 컴퓨팅 및 스토리지 인스턴스는 모두 동일한 AWS 리전에 있습니다.
솔루션 설계자는 공유 파일 시스템 인스턴스를 교체하여 비용을 절감해야 합니다. 파일 시스템은 72시간 실행 기간 동안 필요한 데이터에 대한 고성능 액세스를 제공해야 합니다.
이러한 요구 사항을 충족하면서 가장 큰 전체 비용 절감 효과를 제공하는 솔루션은 무엇입니까?

A. 기존 공유 파일 시스템의 데이터를 S3 Intelligent-Tiering 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업이 실행되기 전에 Lustre용 Amazon FSx를 사용하여 지연 로딩을 통해 Amazon S3의 데이터로 새 파일 시스템을 생성합니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.
B. 다중 연결이 활성화된 기존 공유 파일 시스템의 데이터를 대규모 Amazon Elastic Block Store(Amazon EBS) 볼륨으로 마이그레이션합니다. Auto Scaling 그룹 시작 템플릿의 사용자 데이터 스크립트를 사용하여 각 인스턴스에 EBS 볼륨을 연결합니다. 작업 기간 동안 EBS 볼륨을 공유 스토리지로 사용합니다. 작업이 완료되면 EBS 볼륨 분리
C. 기존 공유 파일 시스템의 데이터를 S3 Standard 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업이 실행되기 전에 Amazon FSx for Lustre를 사용하여 일괄 로드를 통해 Amazon S3의 데이터로 새 파일 시스템을 생성합니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.
D. 기존 공유 파일 시스템의 데이터를 Amazon S3 버킷으로 마이그레이션합니다. 매달 작업이 실행되기 전에 AWS Storage Gateway를 사용하여 Amazon S3의 데이터로 파일 게이트웨이를 생성합니다. 파일 게이트웨이를 작업의 공유 스토리지로 사용합니다. 작업이 완료되면 파일 게이트웨이를 삭제합니다.

해설
정답:A
Amazon S3 Intelligent-Tiering 스토리지 클래스를 사용하는 S3 버킷으로 데이터를 이관하여 비용을 절감할 수 있음
- 매월 작업 실행 전에 Amazon FSx for Lustre를 사용하여 필요한 데이터로 새 파일 시스템을 생성하고 작업 동안에만
해당 파일 시스템을 공유 저장소로 사용함으로써 원하는 성능을 제공하고 작업이 완료되면 파일 시스템을 삭제하여
추가 비용을 절감

◆ | **Q#0024.** | **Ref#0024.**
한 회사가 정적 포트에서 TCP를 사용하여 액세스할 새로운 서비스를 개발 중입니다. 솔루션 설계자는 서비스의 가용성이 높고, 가용성 영역 전체에 중복성이 있으며, 공개적으로 액세스할 수 있는 DNS 이름 my.service.com을 사용하여 액세스할 수 있는지 확인해야 합니다. 서비스는 다른 회사가 허용 목록에 주소를 추가할 수 있도록 고정 주소 할당을 사용해야 합니다.
리소스가 단일 지역의 여러 가용 영역에 배포된다고 가정하면 어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 각 인스턴스에 대해 탄력적 IP 주소를 사용하여 Amazon EC2 인스턴스를 생성합니다.
NLB(Network Load Balancer)를 생성하고 정적 TCP 포트를 노출합니다. NLB에 EC2 인스턴스를 등록합니다. my.service.com이라는 새 이름 서버 레코드 세트를 생성하고 EC2 인스턴스의 탄력적 IP 주소를 레코드 세트에 할당합니다. 허용 목록에 추가할 EC2 인스턴스의 탄력적 IP 주소를 다른 회사에

제공합니다.
B. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다. ECS 클러스터에 대한 공용 IP 주소를 생성하고 할당합니다. NLB(Network Load Balancer)를 생성하고 TCP 포트를 노출합니다. 대상 그룹을 생성하고 ECS 클러스터 이름을 NL에 할당합니다. my.service.com이라는 새 A 레코드 세트를 생성하고 ECS 클러스터의 퍼블릭 IP 주소를 레코드 세트에 할당합니다. 허용 목록에 추가할 ECS 클러스터의 공용 IP 주소를 다른 회사에 제공합니다.
C. 서비스용 Amazon EC2 인스턴스를 생성합니다. 각 가용 영역마다 하나의 탄력적 IP 주소를 생성합니다. NLB(Network Load Balancer)를 생성하고 할당된 TCP 포트를 노출합니다. 각 가용 영역의 NLB에 탄력적 IP 주소를 할당합니다. 대상 그룹을 생성하고 EC2 인스턴스를 NLB에 등록합니다. my.service.com이라는 새 A(별칭) 레코드 세트를 생성하고 NLB DNS 이름을 레코드 세트에 할당합니다.
D. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다. 클러스터의 각 호스트에 대한 공용 IP 주소를 생성하고 할당합니다. ALB(Application Load Balancer)를 생성하고 정적 TCP 포트를 노출합니다. 대상 그룹을 생성하고 ECS 서비스 정의 이름을 ALB에 할당합니다. 새 CNAME 레코드 세트를 생성하고 퍼블릭 IP 주소를 레코드 세트에 연결합니다. Amazon EC2 인스턴스의 탄력적 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

해설
정답:C
다중 Availability Zone에 걸쳐서 가용성 및 탐욕성을 보장하려면 EC2 인스턴스를 각 Availability Zone에 생성하고,
NLB를 사용하여 인스턴스를 연결하는 것이 좋음
Elastic IP 주소를 사용하여 고정 주소 할당을 유지하고 다른 회사들이 allow 목록에 주소를 추가할 수 있도록 할 수 있고,
NLB를 통해 한 가용 영역에 있는 EC2 인스턴스를 능동적으로 관리하고, DNS 이름을 사용하여 고도의 가용성을 유지할 수 있음

◆ | **Q#0025.** | **Ref#0025.**
회사는 온프레미스 데이터 분석 플랫폼을 사용합니다. 이 시스템은 회사 데이터 센터의 12개 서버에 걸쳐 완전히 중복된 구성으로 가용성이 높습니다.
시스템은 사용자의 일회성 요청 외에도 매시간 및 매일 예약된 작업을 실행합니다. 예약된 작업은 실행을 완료하는 데 20분에서 2시간 정도 걸릴 수 있으며 엄격한 SLA가 적용됩니다. 예약된 작업은 시스템 사용량의 65%를 차지합니다. 사용자 작업은 일반적으로 5분 이내에 실행이 완료되며 SLA가 없습니다. 사용자 작업은 시스템 사용량의 35%를 차지합니다. 시스템 오류가 발생하는 동안 예약된 작업은 SLA를 계속 충족해야 합니다. 그러나 사용자 작업이 지연될 수 있습니다.
솔루션 아키텍트는 시스템을 Amazon EC2 인스턴스로 이동하고 소비 기반 모델을 채택하여 장기 약정 없이 비용을 절감해야 합니다. 솔루션은 고가용성을 유지해야 하며 SLA에 영향을 주어서는 안 됩니다.
이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 선택한 AWS 지역의 두 가용 영역에 걸쳐 12개의 인스턴스를 분할합니다. 용량 예약을 통해 각 가용 영역에서 2개의 인스턴스를 온디맨드 인스턴스로 실행합니다. 각 가용 영역에서 4개의 인스턴스를 스팟 인스턴스로 실행합니다.
B. 선택한 AWS 지역의 3개 가용 영역에 걸쳐 12개의 인스턴스를 분할합니다. 가용 영역 중 하나에서 4개의 인스턴스를 모두 용량 예약이 포함된 온디맨드 인스턴스로 실행합니다. 나머지 인스턴스를 스팟 인스턴스로 실행합니다.
C. 선택한 AWS 지역의 3개 가용 영역에 걸쳐 12개의 인스턴스를 분할합니다. Savings Plan을 통해 각 가용 영역에서 2개의 인스턴스를 온디맨드 인스턴스로 실행합니다. 각 가용 영역에서 두 개의 인스턴스를 스팟 인스턴스로 실행합니다.
D. 선택한 AWS 지역의 3개 가용 영역에 12개의 인스턴스를 분할합니다. 용량 예약을 통해 각 가용 영역에서 3개의 인스턴스를 온디맨드 인스턴스로 실행합니다. 각 가용 영역에서 하나의 인스턴스를 스팟 인스턴스로 실행합니다.

해설
정답: D
On-Demand Instances와 Capacity Reservations을 사용하여 사용자들의 SLA에 영향을 끼치지 않으면서 예약된 용량을 활용할 수 있음
스팟 인스턴스를 통해 비용을 절감하고, 시스템 가용성을 유지할 수 있고 세 가용 영역을 활용하여 고가용성을 유지하면서 비용을 효율적으로 관리

◆ | **Q#0026.** | **Ref#0026.**
보안 엔지니어는 기존 애플리케이션이 Amazon S3의 암호화된 파일에서 MySQL용 Amazon RDS 데이터베이스에 대한 자격 증명을 검색한다는 사실을 확인했습니다. 애플리케이션의 다음 버전에서 보안 엔지니어는 보안을 강화하기 위해 다음과 같은 애플리케이션 설계 변경을 구현하려고 합니다.
데이터베이스는 안전한 AWS 관리형 서비스에 저장된 무작위로 생성된 강력한 암호를 사용해야 합니다.
애플리케이션 리소스는 AWS CloudFormation을 통해 배포되어야 합니다.
애플리케이션은 90일마다 데이터베이스에 대한 자격 증명을 교체해야 합니다.
솔루션 설계자는 애플리케이션을 배포하기 위해 CloudFormation 템플릿을 생성합니다.
CloudFormation 템플릿에 지정된 리소스는 최소한의 운영 오버헤드로 보안 엔지니어의 요구 사항을 충족합니까?

A. AWS Secrets Manager를 사용하여 데이터베이스 비밀번호를 비밀 리소스로 생성합니다. 데이터베이스 암호를 교체하기 위한 AWS Lambda 함수 리소스를 생성합니다. 90일마다 데이터베이스 암호를 교체하려면 Secrets Manager RotationSchedule 리소스를 지정합니다.
B. AWS Systems Manager Parameter Store를 사용하여 SecureString 매개변수 유형으로 데이터베이스 비밀번호를 생성합니다. 데이터베이스 암호를 교체하기 위한 AWS Lambda 함수 리소스를 생성합니다. 90일마다 데이터베이스 암호를 교체하려면 Parameter Store RotationSchedule 리소스를 지정하십시오.
C. AWS Secrets Manager를 사용하여 데이터베이스 비밀번호를 비밀 리소스로 생성합니다. 데이터베이스 암호를 교체하기 위한 AWS Lambda 함수 리소스를 생성합니다. 90일마다 Lambda 함수 암호 교체를 트리거하는 Amazon EventBridge 예약 규칙 리소스를 생성합니다.
D. AWS Systems Manager Parameter Store를 사용하여 SecureString 매개변수 유형으로 데이터베이스 비밀번호를 생성합니다. 90일마다 데이터베이스 암호를 자동으로 교체하도록 AWS AppSync DataSource 리소스를 지정합니다.

해설
정답: A
AWS Secrets Manager는 안전하게 비밀을 저장하고 회전시키는 데 사용할 수 있는 AWS 관리 서비스임.
AWS Lambda 함수를 사용하여 데이터베이스 암호를 주기적으로 회전시키는 것이 보안을 향상하고, Secrets Manager의 RotationSchedule 리소스를 사용하여 데이터베이스 암호를 매 90일마다 회전시키는 스케줄을 설정할 수 있음

◆ | **Q#0027.** | **Ref#0027.**
한 회사가 여러 Amazon DynamoDB 테이블에 데이터를 저장하고 있습니다. 솔루션 설계자는 서버리스 아키텍처를 사용하여 HTTPS를 통한 간단한 API를 통해 데이터에 공개적으로 액세스할 수 있도록 해야 합니다. 솔루션은 수요에 따라 자동으로 확장되어야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까? (2개를 선택하세요.)

A. Amazon API Gateway REST API를 생성합니다. API Gateway의 AWS 통합 유형을 사용하여 DynamoDB에 직접 통합되도록 이 API를 구성합니다.
B. Amazon API Gateway HTTP API를 생성합니다. API Gateway의 AWS 통합 유형을 사용하여 Dynamo DB에 직접 통합되도록 이 API를 구성합니다.
C. Amazon API Gateway HTTP API를 생성합니다. DynamoDB 테이블에서 데이터를 반환하는 AWS Lambda 함수에 대한 통합으로 이 API를 구성합니다.
D. AWS Global Accelerator에서 액셀러레이터를 생성합니다. DynamoDB 테이블에서 데이터를 반환하는 AWS Lambda@Edge 함수 통합으로 이 액셀러레이터를 구성합니다.

E. 네트워크 로드 밸런서를 생성합니다. 요청을 적절한 AWS Lambda 함수로 전달하도록 리스너 규칙을 구성합니다.

해설
정답: AC
A-이것은 데이터베이스에 대한 직접 통합을 통해 데이터에 대한 액세스를 가능하게 하며, Serverless 아키텍처를 사용하여 요구 사항에 적합
C-데이터에 대한 액세스를 가능하게하고 서버리스 아키텍처를 사용하여 스케일링이 가능

◆ | **Q#0028.** | **Ref#0028.**
한 회사가 10개의 새로운 도메인 이름을 등록했습니다. 회사는 온라인 마케팅을 위해 도메인을 사용합니다. 회사에는 온라인 방문자를 각 도메인의 특정 URL로 리디렉션하는 솔루션이 필요합니다. 모든 도메인과 대상 URL은 JSON 문서에 정의됩니다. 모든 DNS 레코드는 Amazon Route 53에서 관리됩니다.
솔루션 아키텍트는 HTTP 및 HTTPS 요청을 수락하는 리디렉션 서비스를 구현해야 합니다.
솔루션 설계자는 최소한의 운영 노력으로 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (3개를 선택하세요.)

A. Amazon EC2 인스턴스에서 실행되는 동적 웹 페이지를 만듭니다. 이벤트 메시지와 함께 JSON 문서를 사용하여 리디렉션 URL을 조회하고 응답하도록 웹페이지를 구성합니다.
B. HTTP 및 HTTPS 리스너를 포함하는 Application Load Balancer를 생성합니다.
C. 이벤트 메시지와 함께 JSON 문서를 사용하여 리디렉션 URL을 조회하고 응답하는 AWS Lambda 함수를 생성합니다.
D. 사용자 지정 도메인과 함께 Amazon API Gateway API를 사용하여 AWS Lambda 함수를 게시합니다.
E. Amazon CloudFront 배포판을 생성합니다. Lambda@Edge 함수를 배포합니다.
F. ACM(AWS Certificate Manager)을 사용하여 SSL 인증서를 생성합니다. 도메인을 주체 대체 이름으로 포함합니다.

해설
정답: CEF
아래와 같이하면 운영 노력을 줄일 수 있음
C-SON 문서 및 이벤트 메시지를 사용하여 각 도메인의 대상 URL을 조회하고 리디렉션 URL로 응답하는 AWS Lambda 함수를 생성하고
웹 서버를 사용하여 리디렉션을 처리하기 위해 Lambda 함수를 만듬
E-Lambda@Edge 함수를 배포하여 각 도메인의 대상 URL을 조회하고 적절한 리디렉션 URL로 응답할 수 있도록
클라우드 프론트(CF) 배포를 생성하고 CloudFront는 리디렉션 처리를 실행
F-ACM을 사용하여 SSL 인증서를 생성하고 도메인을 Subject Alternative Names로 포함시켜 HTTPS 요청을 처리할 수 있도록 함

◆ | **Q#0029.** | **Ref#0029.**
여러 AWS 계정을 보유한 회사가 AWS Organizations를 사용하고 있습니다. 회사의 AWS 계정은 VPC, Amazon EC2 인스턴스 및 컨테이너를 호스팅합니다.
회사의 규정 준수 팀은 회사가 배포한 각 VPC에 보안 도구를 배포했습니다. 보안 도구는 EC2 인스턴스에서 실행되며 규정 준수 팀 전용 AWS 계정으로 정보를 보냅니다. 회사는 "costCenter" 키와 값 또는 "compliance"를 사용하여 모든 규정 준수 관련 리소스에 태그를 지정했습니다.
회사는 규정 준수 팀의 AWS 계정에 비용을 청구할 수 있도록 EC2 인스턴스에서 실행되는 보안 도구의 비용을 식별하려고 합니다. 비용 계산은 최대한 정확해야 합니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. 조직의 마스터 계정에서 costCenter 사용자 정의 태그를 활성화합니다. 월별 AWS 비용 및 사용 보고서를 구성하여 마스터 계정의 Amazon S3 버킷에 저장합니다. 보고서의 태그 분석을 사용하여 CostCenter 태그가 지정된 리소스에 대한 총 비용을 확인하세요.

B. 조직의 회원 계정에서 CostCenter 사용자 정의 태그를 활성화합니다. 월별 AWS 비용 및 사용 보고서를 구성하여 마스터 계정의 Amazon S3 버킷에 저장합니다. 보고서를 검색하고 costCenter 태그가 지정된 리소스에 대한 총 비용을 계산하도록 월별 AWS Lambda 함수를 예약합니다.
C. 조직의 회원 계정에서 costCenter 사용자 정의 태그를 활성화합니다. 마스터 계정에서 월별 AWS 비용 및 사용 보고서를 예약합니다. 보고서의 태그 분석을 사용하여 CostCenter 태그가 지정된 리소스의 총 비용을 계산합니다.
D. AWS Trusted Advisor의 조직 보기에서 사용자 지정 보고서를 생성합니다. 규정 준수 팀의 AWS 계정에서 costCenter 태그가 지정된 리소스에 대한 월별 결제 요약을 생성하도록 보고서를 구성합니다.

해설
정답: A
조직의 관리 계정을 사용하여 모든 계정의 비용 및 사용량 정보를 중앙 집중화할 수 있고,
사용자 정의 태그를 활성화하여 비용을 태그별로 분류하고 Amazon S3 버킷에 보고서를 저장하여 필요할 때 접근할 수 있으며.
태그 분석을 통해 costCenter로 태그가 지정된 리소스의 비용을 정확하게 계산할 수 있음

◆ | **Q#0030.** | **Ref#0030.**
회사에는 AWS Organizations 조직의 구성원인 AWS 계정이 50개 있습니다. 각 계정에는 여러 VPC가 포함되어 있습니다. 회사는 AWS Transit Gateway를 사용하여 각 회원 계정의 VPC 간에 연결을 설정하려고 합니다. 새 멤버 계정이 생성될 때마다 회사는 새 VPC 및 전송 게이트웨이 연결을 생성하는 프로세스를 자동화하려고 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. 마스터 계정에서 AWS Resource Access Manager를 사용하여 전송 게이트웨이를 회원 계정과 공유하십시오.
B. 마스터 계정에서 AWS Organizations SCP를 사용하여 전송 게이트웨이를 회원 계정과 공유합니다.
C. 회원 계정에 새 VPC와 VPC 전송 게이트웨이 연결을 자동으로 생성하는 마스터 계정에서 AWS CloudFormation 스택 세트를 시작합니다. 전송 게이트웨이 ID를 사용하여 마스터 계정의 전송 게이트웨이와 연결을 연결합니다.
D. 회원 계정에 새 VPC와 피어링 전송 게이트웨이 연결을 자동으로 생성하는 마스터 계정에서 AWS CloudFormation 스택 세트를 시작합니다. 전송 게이트웨이 서비스 연결 역할을 사용하여 마스터 계정의 전송 게이트웨이와 연결을 공유합니다.
E. 마스터 계정에서 AWS Service Catalog를 사용하여 전송 게이트웨이를 회원 계정과 공유합니다.

해설
정답: AC
아래의 절차로 새로운 계정이 생성될 때마다 VPC와 트랜지트 게이트웨이 어태치먼트를 자동화하여 효율적으로 관리할 수 있음
트랜지트 게이트웨이의 공유를 통해 여러 계정 간의 연결성을 확보하고
CloudFormation 스택 세트를 통해 새 VPC 생성과 트랜지트 게이트웨이 어태치먼트 설정을 자동화하여 효율적으로 운영
Resource Access Manager를 사용하여 트랜지트 게이트웨이를 여러 회원 계정과 공유함으로써 연결성을 유지

031 (노종옥) 4회차 完

◆ | **Q#0031.** | **Ref#0031.**
한 엔터프라이즈 회사에서는 개발자가 AWS Marketplace를 통해 타사 소프트웨어를 구매할 수 있도록 허용하려고 합니다. 회사는 모든 기능이 활성화된 AWS Organizations 계정 구조를 사용하며, 조달 관리자가 사용할 각 조직 단위(OU)에 공유 서비스 계정을 가지고 있습니다. 조달 팀의 정책에 따르면 개발자는 승인된 목록에서만 타사 소프트웨어를 얻을 수 있어야 하며 AWS Marketplace의 Private Marketplace를 사용하여 이 요구 사항을 충족할 수 있

어야 합니다. 조달 팀은 Private Marketplace의 관리가 조달 관리자가 맡을 수 있는 조달-관리자-역할이라는 역할로 제한되기를 원합니다. 회사의 다른 IAM 사용자, 그룹, 역할 및 계정 관리자는 Private Marketplace 관리 액세스가 거부되어야 합니다.
이러한 요구 사항을 충족하도록 아키텍처를 설계하는 가장 효율적인 방법은 무엇입니까?

> **A.** 조직의 모든 AWS 계정에 procurement-manager-role이라는 IAM 역할을 생성합니다. PowerUserAccess 관리형 정책을 역할에 추가합니다. 모든 AWS 계정의 모든 IAM 사용자 및 역할에 인라인 정책을 적용하여 AWSPrivateMarketplaceAdminFullAccess 관리형 정책에 대한 권한을 거부합니다.
> **B.** 조직의 모든 AWS 계정에 procurement-manager-role이라는 IAM 역할을 생성합니다. 역할에 AdministratorAccess 관리형 정책을 추가합니다. AWSPrivateMarketplaceAdminFullAccess 관리형 정책을 사용하여 권한 경계를 정의하고 이를 모든 개발자 역할에 연결합니다.
> **C.** 조직의 모든 공유 서비스 계정에 procurement-manager-role이라는 IAM 역할을 생성합니다. 역할에 AWSPrivateMarketplaceAdminFullAccess 관리형 정책을 추가합니다. Procurement-manager-role이라는 역할을 제외한 모든 사람에게 Private Marketplace를 관리할 수 있는 권한을 거부하는 조직 루트 수준 SCP를 만듭니다. 다른 조직 루트 수준 SCP를 생성하여 조직의 모든 사람에게 procurement-manager-role이라는 IAM 역할을 생성할 수 있는 권한을 거부합니다.
> **D.** 개발자가 사용할 모든 AWS 계정에 procurement-manager-role이라는 IAM 역할을 생성합니다. 역할에 AWSPrivateMarketplaceAdminFullAccess 관리형 정책을 추가합니다. 조달 관리자 역할이라는 역할을 제외한 모든 사람에게 Private Marketplace를 관리할 수 있는 권한을 거부하려면 조직에서 SCP를 만듭니다. 조직의 모든 공유 서비스 계정에 SCP를 적용합니다.
>
> 해설
> 정답:C
> 질문포인트:Private Marketplace의 관리가 procurement-manager-role 역할로 제한되고, 그 외는 액세스가 거부되어야 함
> A와 B는 모든 AWS 계정에 해당 역할을 생성하는 것을 요구하며, 이는 중복성과 관리에 불필요한 복잡성을 추가합니다.
> D는 특정 권한을 모든 개발자 계정에 할당하려 하지만, 이는 회사의 요구사항인 Private Marketplace 관리 권한을 조달 관리자에게 한정하는 것에 어긋납니다.

◆ | **Q#0032.** | **Ref#0032.**
한 회사는 개발자가 Amazon EC2, Amazon S3 및 Amazon DynamoDB만 사용하도록 제한하기 위해 AWS Organizations를 구현하는 중입니다. 개발자 계정은 전용 조직 단위(OU)에 있습니다. 솔루션스 아키텍트는 개발자 계정에 다음 SCP를 구현했습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "AllowDynamoDB",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "*"
        },
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
```

```
            }
        ]
    }
```

이 정책이 배포되면 개발자 계정의 IAM 사용자는 정책에 나열되지 않은 AWS 서비스를 계속 사용할 수 있습니다. 개발자가 이 정책의 범위를 벗어나는 서비스를 사용할 수 없도록 솔루션 설계자는 어떻게 해야 합니까?

> **A.** 제한해야 하는 각 AWS 서비스에 대해 명시적인 거부 문을 생성합니다.
> **B.** 개발자 계정의 OU에서 FullAWSAccess SCP를 제거합니다.
> **C.** 모든 서비스를 명시적으로 거부하도록 FullAWSAccess SCP를 수정합니다.
> **D.** SCP 끝에 와일드카드를 사용하여 명시적인 거부 문을 추가합니다.
>
> 해설
> 정답:B
> B. 개발자 계정의 OU에서 FullAWSAccess SCP를 제거합니다.
> 기본적으로 FullAWSAccess 정책이 모든 OU에 연결되어 있음
> D는 모든 서비스를 이용할 수 없음

◆ | **Q#0033.** | **Ref#0033.**
한 회사가 VPC의 퍼블릭 서브넷에 있는 5개의 Amazon EC2 인스턴스에서 모바일 앱용 모놀리식 REST 기반 API를 호스팅하고 있습니다. 모바일 클라이언트는 Amazon Route 53에서 호스팅되는 도메인 이름을 사용하여 API에 연결합니다. 회사는 모든 EC2 인스턴스의 IP 주소를 사용하여 Route 53 다중 응답 라우팅 정책을 생성했습니다. 최근 앱 트래픽이 대규모로 급증하면서 과부하가 걸렸습니다. 앱이 트래픽을 따라잡지 못했습니다.
솔루션 설계자는 앱이 새롭고 다양한 부하를 처리할 수 있도록 솔루션을 구현해야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** API를 개별 AWS Lambda 함수로 분리합니다. 백엔드에 대한 Lambda 통합을 통해 Amazon API Gateway REST API를 구성합니다. API Gateway API를 가리키도록 Route 53 레코드를 업데이트합니다.
> **B.** API 로직을 컨테이너화합니다. Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 생성합니다. Amazon EC2를 사용하여 클러스터에서 컨테이너를 실행합니다. Kubernetes 수신을 만듭니다. Kubernetes 수신을 가리키도록 Route 53 레코드를 업데이트합니다.
> **C.** Auto Scaling 그룹을 생성합니다. 모든 EC2 인스턴스를 Auto Scaling 그룹에 배치합니다. CPU 사용률을 기반으로 조정 작업을 수행하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹 변경 사항에 반응하고 Route 53 레코드를 업데이트하는 AWS Lambda 함수를 생성합니다.
> **D.** API 앞에 ALB(Application Load Balancer)를 생성합니다. EC2 인스턴스를 VPC의 프라이빗 서브넷으로 이동합니다. EC2 인스턴스를 ALB의 대상으로 추가합니다. ALB를 가리키도록 Route 53 레코드를 업데이트합니다.
>
> 해설
> 정답:A
> 질문포인트:EC2인스턴스에소 Rest기반 API, Route53에서 호스팅, 큰 규모의 로드 처리, 최소한의 운영 오버헤드
> A. API를 개별 AWS Lambda 함수로 분리합니다. 백엔드에 대한 Lambda 통합을 통해 Amazon API Gateway REST API를 구성합니다. API Gateway API를 가리키도록 Route 53 레코드를 업데이트합니다.
> D는 대규모 트래픽 처리에 대한 솔루션이 없음

◆ | **Q#0034.** | **Ref#0034.**
한 회사가 각 엔지니어링 팀을 위해 AWS Organizations에 OU를 생성했습니다. 각 OU는 여러 AWS 계정을 소유합니다. 조직에는 수백 개의 AWS 계정이 있습니다.
솔루션 아키텍트는 각 OU가 AWS 계정 전체의 사용 비용 분석을 볼 수 있도록 솔루션을 설계해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Resource Access Manager를 사용하여 각 OU에 대한 AWS 비용 및 사용 보고서(CUR)를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.
B. AWS Organizations 마스터 계정에서 AWS 비용 및 사용 보고서(CUR)를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.
C. 각 AWS Organizations 회원 계정에서 AWS 비용 및 사용 보고서(CUR)를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.
D. AWS 시스템 관리자를 사용하여 AWS 비용 및 사용 보고서(CUR)를 생성합니다. 각 팀이 Systems Manager OpsCenter 대시보드를 통해 CUR을 시각화할 수 있습니다.

해설
정답:B
질문포인트:계정 전체의 사용 비용 분석을 볼수 있도록.
마스터 계정은 조직의 모든 소유한 계정에 대한 비용 보고서를 생성할 수 있습니다.
QuickSight는 이 보고서를 시각화하는 데 사용될 수 있습니다

◆ | **Q#0035.** | **Ref#0035.**
회사는 Windows 파일 서버에 온프레미스로 데이터를 저장하고 있습니다. 회사는 매일 5GB의 새로운 데이터를 생성합니다.
회사는 Windows 기반 워크로드의 일부를 AWS로 마이그레이션했으며 클라우드의 파일 시스템에서 데이터를 사용할 수 있어야 합니다. 회사는 이미 온프레미스 네트워크와 AWS 간에 AWS Direct Connect 연결을 설정했습니다.
회사는 어떤 데이터 마이그레이션 전략을 사용해야 합니까?

A. AWS Storage Gateway의 파일 게이트웨이 옵션을 사용하여 기존 Windows 파일 서버를 교체하고 기존 파일 공유가 새 파일 게이트웨이를 가리키도록 하십시오.
B. AWS DataSync를 사용하여 온프레미스 Windows 파일 서버와 Amazon FSx 간에 데이터를 복제하는 일일 작업을 예약합니다.
C. AWS Data Pipeline을 사용하여 온프레미스 Windows 파일 서버와 Amazon Elastic File System(Amazon EFS) 간에 데이터를 복제하는 일일 작업을 예약합니다.
D. AWS DataSync를 사용하여 온프레미스 Windows 파일 서버와 Amazon Elastic File System(Amazon EFS) 간에 데이터를 복제하는 일일 작업을 예약합니다.

해설
정답:B
AWS DataSync는 온프레미스 시스템과 AWS 스토리지 서비스 간에 데이터를 쉽게 이동, 복제 및 동기화할 수 있는 온라인 데이터 이전 서비스입니다.
Amazon FSx는 Windows에서 실행되는 워크로드를 위해 최적화된 파일 시스템을 제공함.

◆ | **Q#0036.** | **Ref#0036.**
한 회사의 솔루션 아키텍트가 AWS에서 실행되는 웹 애플리케이션을 검토하고 있습니다. 애플리케이션은 us-east-1 지역의 Amazon S3 버킷에 있는 정적 자산을 참조합니다. 회사는 여러 AWS 리전에 걸친 복원력이 필요합니다.
회사는 이미 두 번째 리전에 S3 버킷을 생성했습니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 각 객체를 두 S3 버킷 모두에 쓰도록 애플리케이션을 구성합니다. 각 S3 버킷에 가중치 기반 라우팅 정책을 사용하여 레코드 세트로 Amazon Route 53 퍼블릭 호스팅 영역을 설정합니다. Route 53 DNS 이름을 사용하여 객체를 참조하도록 애플리케이션을 구성합니다.
B. us-east-1의 S3 버킷에서 두 번째 리전의 S3 버킷으로 객체를 복사하는 AWS Lambda 함수를 생성합니다. us-east-1의 S3 버킷에 객체가 기록될 때마다 Lambda 함수를 호출합니다. 두 개의 S3 버킷을 오리진으로 포함하는 오리진 그룹을 사용하여 Amazon CloudFront 배포를 설정합니다.
C. us-east-1의 S3 버킷에 복제를 구성하여 두 번째 리전의 S3 버킷에 객체를 복제합니다. 두 개의 S3 버킷을 오리진으로 포함하는 오리진 그룹을 사용하여 Amazon CloudFront 배포를 설정합니다.
D. us-east-1의 S3 버킷에 복제를 구성하여 두 번째 리전의 S3 버킷에 객체를 복제합니다. 장애 조치

가 필요한 경우 애플리케이션 코드를 업데이트하여 두 번째 리전의 S3 버킷에서 S3 객체를 로드합니다.

해설
정답:C
질문포인트:정적자원참조, 여러 리전에 걸치 복원력 필요. 최소한의 운영 오버헤드
S3의 교차 리전 복제(Cross-Region Replication, CRR) 기능을 사용하여 복제 가능->복원력 향상
CloudFront를 사용하여 기존 S3 버킷 및 복제된 S3 버킷을 오리진으로 설정하면, 사용자는 가장 가까운 엣지 로케이션에서 콘텐츠를 빠르게 받을 수 있습니다

◆ | **Q#0037.** | **Ref#0037.**
회사는 온프레미스 환경에서 3계층 웹 애플리케이션을 호스팅하고 있습니다. 최근 트래픽 급증으로 인해 가동 중단 시간이 발생하고 재정적으로 막대한 영향을 미치게 되면서 회사 경영진은 애플리케이션을 AWS로 이전하도록 명령했습니다. 애플리케이션은 .NET으로 작성되었으며 MySQL 데이터베이스에 종속됩니다. 솔루션 설계자는 매일 200,000명의 사용자 수요를 충족할 수 있는 확장 가능하고 가용성이 높은 솔루션을 설계해야 합니다.
솔루션 아키텍트는 적절한 솔루션을 설계하기 위해 어떤 단계를 수행해야 합니까?

A. AWS Elastic Beanstalk를 사용하여 웹 서버 환경과 Amazon RDS MySQL 다중 AZ DB 인스턴스로 새 애플리케이션을 생성하십시오. 환경은 여러 가용 영역의 Amazon EC2 Auto Scaling 그룹 앞에서 Network Load Balancer(NLB)를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 NLB로 트래픽을 라우팅합니다.
B. AWS CloudFormation을 사용하여 3개의 가용 영역에 걸쳐 있는 Amazon EC2 Auto Scaling 그룹 앞에 Application Load Balancer(ALB)가 포함된 스택을 시작합니다. 스택은 보존 삭제 정책을 사용하여 Amazon Aurora MySQL DB 클러스터의 다중 AZ 배포를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 ALB로 트래픽을 라우팅합니다.
C. AWS Elastic Beanstalk를 사용하여 각 지역에 ALB(Application Load Balancer)가 있는 두 개의 개별 지역에 걸쳐 자동으로 확장되는 웹 서버 환경을 생성합니다. 리전 간 읽기 전용 복제본을 사용하여 Amazon Aurora MySQL DB 클러스터의 다중 AZ 배포를 생성합니다. 지리 근접 라우팅 정책과 함께 Amazon Route 53을 사용하여 두 지역 간에 트래픽을 라우팅합니다.
D. AWS CloudFormation을 사용하여 3개의 가용 영역에 걸쳐 있는 스팟 인스턴스의 Amazon ECS 클러스터 앞에 Application Load Balancer(ALB)가 포함된 스택을 시작합니다. 스택은 스냅샷 삭제 정책을 사용하여 Amazon RDS MySQL DB 인스턴스를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 ALB로 트래픽을 라우팅합니다.

해설
정답:B
질문포인트:3계층 웹 온프레미스에서 AWS로 이전계획, MySQL종속, 매일 20만명 사용자 수요를 충족할 수 있는 확장 가능하고, 가용성이 높은 솔루션은?
3개의 가용영역에 걸쳐 있는 Amazon EC2 Auto Scaling 그룹->확장성을 제공
Application Load Balancer(ALB)는 복수의 가용 영역에 분산된 인스턴스를 자동으로 감지하므로 고가용성 환경에 적합
Amazon Aurora MySQL -> 우수한 성능과 적은 운영 오버헤드로 고 가용성 제공

◆ | **Q#0038.** | **Ref#0038.**
한 회사에서 AWS Organizations를 사용하여 여러 AWS 계정을 관리하고 있습니다. 보안을 위해 회사에서는 모든 조직 회원 계정에서 타사 알림 시스템과 통합할 수 있는 Amazon Simple 알림 서비스(Amazon SNS) 주제를 생성해야 합니다.
솔루션 아키텍트는 AWS CloudFormation 템플릿을 사용하여 CloudFormation 스택 배포를 자동화하기 위한 SNS 주제와 스택 세트를 생성했습니다. 조직에서 신뢰할 수 있는 액세스가 활성화되었습니다.
모든 AWS 계정에 CloudFormation StackSets를 배포하려면 솔루션 아키텍트가 무엇을 해야 합니까?

A. 조직 회원 계정에 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다. 조직에 배포하기 위한 배포 옵션을 설정합니다. CloudFormation StackSets 드리프트 감지를 사용합니다.

B. 조직 회원 계정에 스택을 생성합니다. 셀프 서비스 권한을 사용합니다. 조직에 배포하기 위한 배포 옵션을 설정합니다. CloudFormation StackSets 자동 배포를 활성화합니다.
C. 조직 마스터 계정에 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다. 조직에 배포할 배포 옵션을 설정합니다. CloudFormation StackSets 자동 배포를 활성화합니다.
D. 조직 마스터 계정에 스택을 생성합니다. 서비스 관리 권한을 사용합니다. 조직에 배포할 배포 옵션을 설정합니다. CloudFormation StackSets 드리프트 감지를 활성화합니다.

해설
정답:C
질문포인트:CloudFormation 스택 배포를 자동화하기 위한 SNS 주제와 스택 세트를 생성, 모든 AWS 계정에 CloudFormation StackSets를 배포 요구
조직의 마스터 계정에서 스택 세트를 생성하고 서비스 관리 권한을 사용하는 것이 필요하며, 조직에 배포할 배포 옵션을 설정해야 합니다.
CloudFormation StackSets 자동 배포 기능을 활성화하면, 조직의 새로운 계정이 자동으로 스택 세트를 받습니다.

◆ | **Q#0039.** | **Ref#0039.**
회사는 워크로드를 온프레미스에서 AWS로 마이그레이션하려고 합니다. 워크로드는 Linux 및 Windows에서 실행됩니다. 이 회사는 수많은 애플리케이션을 호스팅하는 VM과 물리적 머신으로 구성된 대규모 온프레미스 인프라를 보유하고 있습니다.

회사는 온프레미스 워크로드의 시스템 구성, 시스템 성능, 실행 중인 프로세스 및 네트워크 연결에 대한 세부 정보를 캡처해야 합니다. 또한 회사는 AWS 마이그레이션을 위해 온프레미스 애플리케이션을 그룹으로 나누어야 합니다. 회사는 가장 비용 효과적인 방식으로 AWS에서 워크로드를 실행할 수 있도록 Amazon EC2 인스턴스 유형에 대한 권장 사항이 필요합니다.

이러한 요구 사항을 충족하려면 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. 물리적 시스템과 VM에 AWS Application Discovery Agent를 설치하여 기존 애플리케이션을 평가합니다.
B. 물리적 시스템과 VM에 AWS Systems Manager 에이전트를 설치하여 기존 애플리케이션을 평가합니다.
C. AWS Systems Manager Application Manager를 사용하여 마이그레이션할 애플리케이션으로 서버를 그룹화합니다.
D. AWS Migration Hub를 사용하여 마이그레이션할 애플리케이션으로 서버를 그룹화합니다.
E. AWS Migration Hub를 사용하여 권장 인스턴스 유형 및 관련 비용을 생성합니다.
F. 서버 크기에 대한 데이터를 AWS Trusted Advisor로 가져옵니다. 비용 최적화를 위한 권장 사항을 따르십시오.

해설
정답:ADE
AWS Application Discovery Agent는 마이그레이션할 때 AWS 장치 크기를 예상하고 비용을 예측하는 데 도와줍니다.
AWS Migration Hub는 마이그레이션할 애플리케이션으로 서버를 그룹화하고, 권장 인스턴스 유형 및 관련 비용을 생성하는데 도와줌.

◆ | **Q#0040.** | **Ref#0040.**
한 회사가 VPC의 AWS에서 이미지 처리 서비스를 호스팅하고 있습니다. VPC는 두 개의 가용 영역으로 확장됩니다. 각 가용 영역에는 퍼블릭 서브넷 1개와 프라이빗 서브넷 1개가 포함되어 있습니다.

이 서비스는 프라이빗 서브넷의 Amazon EC2 인스턴스에서 실행됩니다. 퍼블릭 서브넷의 Application Load Balancer는 서비스 앞에 있습니다. 서비스는 인터넷과 통신해야 하며 두 개의 NAT 게이트웨이를 통해 통신합니다.

이 서비스는 이미지 저장을 위해 Amazon S3를 사용합니다. EC2 인스턴스는 매일 S3 버킷에서 약 1TB의 데이터를 검색합니다.

회사는 이 서비스를 매우 안전하다고 홍보했습니다. 솔루션 설계자는 서비스의 보안 상태를 손상시키거나 지속적인 운영에 소요되는 시간을 늘리지 않으면서 클라우드 비용을 최대한 줄여야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** NAT 게이트웨이를 NAT 인스턴스로 교체합니다. VPC 라우팅 테이블에서 프라이빗 서브넷에서 NAT 인스턴스로의 경로를 생성합니다.
> **B.** EC2 인스턴스를 퍼블릭 서브넷으로 이동합니다. NAT 게이트웨이를 제거합니다.
> **C.** VPA에서 S3 게이트웨이 VPC 엔드포인트를 설정합니다. 엔드포인트 정책을 엔드포인트에 연결하여 S3 버킷에 필요한 작업을 허용합니다.
> **D.** Amazon Elastic File System(Amazon EFS) 볼륨을 EC2 인스턴스에 연결합니다. EFS 볼륨에 이미지를 호스팅합니다.
>
> 해설
> 정답:C
> S3 게이트웨이 VPC 엔드포인트를 설정하면 회사는 VPC내에서 Amazon S3로 트래픽을 보낼 때 요금을 지불하지 않아도 됩니다
> 이는 데이터 전송 비용을 크게 줄여주는 중요한 비용 절감 기법입니다.
> 엔드포인트 정책은 사용자가 S3 버킷에 필요한 작업을 실행할 수 있도록 허용하고, 보안 상태가 손상되지 않도록 합니다.

041 (박지수) 4회차 完

◆ | **Q#0041.** | **Ref#0041.**
한 회사는 최근 AWS에 애플리케이션을 배포했습니다. 애플리케이션은 Amazon DynamoDB를 사용합니다. 회사는 애플리케이션 로드를 측정하고 예상되는 최대 로드와 일치하도록 DynamoDB 테이블의 RCU 및 WCU를 구성했습니다. 최대 부하는 일주일에 한 번 4시간 동안 발생하며 평균 부하의 두 배입니다. 애플리케이션 부하는 이번 주의 나머지 기간 동안의 평균 부하에 가깝습니다. 액세스 패턴에는 테이블 읽기보다 테이블에 대한 쓰기가 더 많이 포함됩니다.

솔루션 설계자는 테이블 비용을 최소화하는 솔루션을 구현해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 피크 기간 동안 용량을 늘리려면 AWS Application Auto Scaling을 사용하십시오. 평균 부하에 맞게 예약된 RCU 및 WCU를 구매하세요.
> **B.** 테이블에 대한 주문형 용량 모드를 구성합니다.
> **C.** 테이블 앞에 DynamoDB Accelerator(DAX)를 구성합니다. 테이블의 새로운 최대 로드에 맞춰 프로비저닝된 읽기 용량을 줄입니다.
> **D.** 테이블 앞에 DynamoDB Accelerator(DAX)를 구성합니다. 테이블에 대한 주문형 용량 모드를 구성합니다.
>
> 해설
> 정답: A
> Application Auto Scaling을 사용해서 피크 시간 동안에만 용량을 증설하고, 평상시에는 에약된 (Reserved) RCU(읽기용량유닛), WCU(쓰기용량유닛) 구매해서 비용 절감
> ※ Application Auto Scaling에는 DynamoDB Auto Scaling도 포함됨
> DAX는 읽기 성능 향상을 위한 것이므로, 문제에서는 쓰기가 더 많다고 했기때문에 오답 : C,D 오답
> On-Demand(주문형 용량 모드)는 사용량 예측할 수 없을때 사용하는 거싱고 비용도 비쌈 : B,D 오답

◆ | **Q#0042.** | **Ref#0042.**
솔루션 아키텍트는 회사에 온프레미스 데이터 처리 애플리케이션을 AWS 클라우드로 마이그레이션하는 방법에 대해 조언해야 합니다. 현재 사용자는 웹 포털을 통해 입력 파일을 업로드합니다. 그런 다음 웹 서버는 업로드된 파일을 NAS에 저장하고 메시지 대기열을 통해 처리 서버에 메시지를 보냅니다. 각 미디어 파일을 처리하는 데 최대 1시간이 걸릴 수 있습니다. 회사에서는 처리 대기 중인 미디어 파일의 수가 업무 시간 중에 훨씬 더 많고, 업무 시간 이후에는 파일 수가 급격하게 감소한다는 사실을 확인했습니다.

가장 비용 효율적인 마이그레이션 권장 사항은 무엇입니까?

> **A.** Amazon SQS를 사용하여 대기열을 생성합니다. 새 큐에 게시하도록 기존 웹 서버를 구성합니다. 대기열에 메시지가 있으면 AWS Lambda 함수를 호출하여 대기열에서 요청을 가져와 파일을 처리합니다. 처리된 파일을 Amazon S3 버킷에 저장합니다.
> **B.** Amazon MQ를 사용하여 대기열을 생성합니다. 새 큐에 게시하도록 기존 웹 서버를 구성합니다. 대기열에 메시지가 있으면 새 Amazon EC2 인스턴스를 생성하여 대기열에서 요청을 가져와 파일을 처리합니다. 처리된 파일을 Amazon EFS에 저장합니다. 작업이 완료된 후 EC2 인스턴스를 종료합니다.
> **C.** Amazon MQ를 사용하여 대기열을 생성합니다. 새 큐에 게시하도록 기존 웹 서버를 구성합니다. 대기열에 메시지가 있으면 AWS Lambda 함수를 호출하여 대기열에서 요청을 가져와 파일을 처리합니다. 처리된 파일을 Amazon EFS에 저장합니다.
> **D.** Amazon SQS를 사용하여 대기열을 생성합니다. 새 큐에 게시하도록 기존 웹 서버를 구성합니다. EC2 Auto Scaling 그룹의 Amazon EC2 인스턴스를 사용하여 대기열에서 요청을 가져와 파일을 처리합니다. SQS 대기열 길이를 기준으로 EC2 인스턴스를 확장합니다. 처리된 파일을 Amazon S3 버킷에 저장합니다.
>
> 해설
> 정답: D
> EC2 인스턴스는 SQS 대기열 길이에 따라 확장될 수 있으므로 사용량이 가장 많은 시간에 리소스를 사용할 수 있고 사용량이 많지 않은 시간에는 비용을 절감할 수 있다.
> S3는 처리된 미디어 파일을 저장하기 위한 내구성이 뛰어나고 비용 효율적인 솔루션이다.
> Lambda는 최대 실행시간이 15분이므로 최대 1시간 소요되는 작업 처리 불가 : A,C 오답
> EFS는 S3에 비해 고비용으로 비효율적 : B,C 오답
> MQ 대기열의 각 메시지에 대해 새 EC2 인스턴스를 생성하는 것은 비용 효율적이지 않음 : B 오답

◆ | **Q#0043.** | **Ref#0043.**
한 회사에서 Amazon OpenSearch Service를 사용하여 데이터를 분석하고 있습니다. 이 회사는 S3 Standard 스토리지를 사용하는 Amazon S3 버킷에서 10개의 데이터 노드가 있는 OpenSearch Service 클러스터에 데이터를 로드합니다. 데이터는 읽기 전용 분석을 위해 1개월 동안 클러스터에 보관됩니다. 1개월 후 회사는 해당 데이터가 포함된 인덱스를 클러스터에서 삭제합니다. 규정 준수를 위해 회사는 모든 입력 데이터의 사본을 보관해야 합니다.

회사는 지속적인 비용을 우려하고 솔루션 설계자에게 새로운 솔루션을 추천해 달라고 요청합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** 예상 용량을 처리하려면 모든 데이터 노드를 UltraWarm 노드로 교체하십시오. 회사가 데이터를 클러스터에 로드할 때 입력 데이터를 S3 Standard에서 S3 Glacier Deep Archive로 전환합니다.
> **B.** 클러스터의 데이터 노드 수를 2개로 줄입니다. UltraWarm 노드를 추가하여 예상 용량을 처리합니다. OpenSearch 서비스가 데이터를 수집할 때 UltraWarm으로 전환되도록 인덱스를 구성합니다. S3 수명 주기 정책을 사용하여 1개월 후에 입력 데이터를 S3 Glacier Deep Archive로 전환합니다.
> **C.** 클러스터의 데이터 노드 수를 2로 줄입니다. UltraWarm 노드를 추가하여 예상 용량을 처리합니다. OpenSearch 서비스가 데이터를 수집할 때 UltraWarm으로 전환되도록 인덱스를 구성합니다. 클러스터에 콜드 스토리지 노드를 추가합니다. 인덱스를 UltraWarm에서 콜드 스토리지로 전환합니다. S3 수명 주기 정책을 사용하여 1개월 후에 S3 버킷에서 입력 데이터를 삭제합니다.
> **D.** 클러스터의 데이터 노드 수를 2로 줄입니다. 인스턴스 지원 데이터 노드를 추가하여 예상 용량을

처리합니다. 회사가 데이터를 클러스터에 로드할 때 입력 데이터를 S3 Standard에서 S3 Glacier Deep Archive로 전환합니다.

해설
정답: B
데이터 입력 1개월 후에 클러스터에서 삭제하고 사본을 보관하는 요건 충족하기위해, 1개월 후에 S3 Glacier Deep Archive로 전환하는 것이 적절한 방법임
데이터를 로드할 때 S3 Glacier Deep Archive로 전환하는 것은 오답 : A,D 오답
1개월 후에 S3 버킷에서 데이터를 삭제하는 것은 사본 보관 요건 불충족 : C 오답
모든 데이터 노드를 UltraWarm으로 교체할 수 없음 : A 오답

◆ | **Q#0044.** | **Ref#0044.**
회사에는 AWS Organizations의 조직에 속하는 10개의 계정이 있습니다. AWS Config는 각 계정에서 구성됩니다. 모든 계정은 Prod OU 또는 NonProd OU에 속합니다.

회사는 0.0.0.0/0을 소스로 사용하여 Amazon EC2 보안 그룹 인바운드 규칙이 생성될 때 Amazon Simple 알림 서비스(Amazon SNS) 주제에 알리도록 각 AWS 계정에 Amazon EventBridge 규칙을 설정했습니다. 회사 보안팀이 SNS 주제를 구독하고 있습니다.

NonProd OU의 모든 계정에 대해 보안 팀은 0.0.0.0/0을 소스로 포함하는 보안 그룹 인바운드 규칙을 생성하는 기능을 제거해야 합니다.

최소한의 운영 오버헤드로 이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Lambda 함수를 호출하여 보안 그룹 인바운드 규칙을 제거하고 SNS 주제에 게시하도록 EventBridge 규칙을 수정합니다. NonProd OU에 업데이트된 규칙을 배포합니다.
B. vpc-sg-open-only-to-authorized-ports AWS Config 관리형 규칙을 NonProd OU에 추가합니다.
C. aws:SourceIp 조건 키의 값이 0.0.0.0/0이 아닐 때 ec2:AuthorizeSecurityGroupIngress 작업을 허용하도록 SCP를 구성합니다. NonProd OU에 SCP를 적용합니다.
D. aws:SourceIp 조건 키의 값이 0.0.0.0/0일 때 ec2:AuthorizeSecurityGroupIngress 작업을 거부하도록 SCP를 구성합니다. NonProd OU에 SCP를 적용합니다.

해설
정답: D
목표는 최소한의 운영 오버헤드로 NonProd 조직 단위(OU)의 모든 계정에 대한 소스로 0.0.0.0/0을 포함하는 Amazon EC2 보안 그룹 인바운드 규칙이 생성되지 않도록 방지하는 것입니다. 옵션 D는 최소한의 운영 오버헤드로 요구 사항을 충족하는 가장 간단하고 효과적인 솔루션입니다.
aws:SourceIp 조건 키가 0.0.0.0/0일 때 ec2:AuthorizeSecurityGroupIngress 작업을 거부하도록 서비스 제어 정책(SCP)을 구성하고 이 정책을 NonProd OU에 적용함으로써 회사는 이 OU 내의 어떤 계정도 보안 그룹 인바운드 규칙을 생성할 수 없도록 보장할 수 있습니다.
EventBridge 규칙을 수정하거나 Config 규칙을 추가하는 것, 특정 IP로 허용하는 것보다 운영 오버헤드가 적음

◆ | **Q#0045.** | **Ref#0045.**
회사는 온프레미스 데이터 센터에서 Git 저장소를 호스팅합니다. 회사는 웹훅을 사용하여 AWS 클라우드에서 실행되는 기능을 호출합니다. 회사는 회사가 ALB(Application Load Balancer)의 대상으로 설정한 Auto Scaling 그룹의 Amazon EC2 인스턴스 세트에서 웹후크 로직을 호스팅합니다. Git 서버는 구성된 웹후크에 대해 ALB를 호출합니다. 회사는 솔루션을 서버리스 아키텍처로 이동하려고 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 각 웹후크에 대해 AWS Lambda 함수 URL을 생성하고 구성합니다. 개별 Lambda 함수 URL을 호출하도록 Git 서버를 업데이트합니다.
B. Amazon API Gateway HTTP API를 생성합니다. 별도의 AWS Lambda 함수에서 각 웹훅 로직을 구

현합니다. API 게이트웨이 엔드포인트를 호출하도록 Git 서버를 업데이트합니다.
C. AWS App Runner에 웹훅 로직을 배포합니다. ALB를 생성하고 App Runner를 대상으로 설정합니다. ALB 엔드포인트를 호출하도록 Git 서버를 업데이트합니다.
D. 웹훅 로직을 컨테이너화합니다. Amazon Elastic Container Service(Amazon ECS) 클러스터를 생성하고 AWS Fargate에서 웹후크 로직을 실행하십시오. Amazon API Gateway REST API를 생성하고 Fargate를 대상으로 설정합니다. API 게이트웨이 엔드포인트를 호출하도록 Git 서버를 업데이트합니다.

해설
정답: B
Lambda 함수는 웹훅 로직을 구현하는 가장 쉬운 방법이며,
API 게이트웨이가 포함된 AWS Lambda 함수를 사용하는 것이 운영 오버헤드가 가장 적은 방법임

◆ | **Q#0046.** | **Ref#0046.**
한 회사가 1,000개의 온프레미스 서버를 AWS로 마이그레이션할 계획입니다. 서버는 회사 데이터 센터의 여러 VMware 클러스터에서 실행됩니다. 마이그레이션 계획의 일환으로 회사는 CPU 세부 정보, RAM 사용량, 운영 체제 정보, 실행 중인 프로세스 등의 서버 측정항목을 수집하려고 합니다. 그런 다음 회사는 데이터를 쿼리하고 분석하려고 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 온프레미스 호스트에 AWS Agentless Discovery Connector 가상 어플라이언스를 배포하고 구성합니다. AWS Migration Hub에서 데이터 탐색을 구성합니다. AWS Glue를 사용하여 데이터에 대해 ETL 작업을 수행합니다. Amazon S3 Select를 사용하여 데이터를 쿼리합니다.
B. 온프레미스 호스트의 VM 성능 정보만 내보냅니다. 필요한 데이터를 AWS Migration Hub로 직접 가져옵니다. Migration Hub에서 누락된 정보를 업데이트하세요. Amazon QuickSight를 사용하여 데이터를 쿼리합니다.
C. 온프레미스 호스트에서 서버 정보를 자동으로 수집하는 스크립트를 만듭니다. AWS CLI를 사용하여 put-resource-attributes 명령을 실행하여 AWS Migration Hub에 세부 서버 데이터를 저장합니다. Migration Hub 콘솔에서 직접 데이터를 쿼리합니다.
D. AWS Application Discovery Agent를 각 온프레미스 서버에 배포합니다. AWS Migration Hub에서 데이터 탐색을 구성합니다. Amazon Athena를 사용하여 Amazon S3의 데이터에 대해 사전 정의된 쿼리를 실행합니다.

해설
정답: D
각 온프레미스 서버에 AWS Application Discovery Agent를 배포하면 CPU 사용량, RAM 사용량, 운영체제 세부 정보, 실행 중인 프로세스 등 서버 지표를 자세히 수집할 수 있습니다.
AWS Migration Hub에서 데이터 탐색을 구성하면 수집된 데이터를 효과적으로 분석하고 쿼리할 수 있습니다.
쿼리에 Amazon Athena를 사용하면 S3에 저장된 데이터에 대한 강력한 SQL 기반 탐색이 가능해지며, 마이그레이션 준비 상태와 계획 데이터를 분석하는 유연하고 확장 가능한 방법을 제공합니다.
Agentless Discovery Connector는 VM 내부 접근이 불가하여 프로세스 정보 수집하지 못함 : A 오답

◆ | **Q#0047.** | **Ref#0047.**
한 회사가 VPC에 연결된 AWS Lambda 함수에서 실행되는 서버리스 애플리케이션을 구축하고 있습니다. 회사는 애플리케이션을 외부 공급자의 새로운 서비스와 통합해야 합니다. 외부 공급자는 허용 목록에 있는 공용 IPv4 주소에서 오는 요청만 지원합니다.

회사는 애플리케이션이 새로운 서비스를 사용하기 시작하기 전에 외부 공급자에게 단일 공용 IP 주소를 제공해야 합니다.

애플리케이션에 새로운 서비스에 액세스할 수 있는 기능을 제공하는 솔루션은 무엇입니까?

A. NAT 게이트웨이를 배포합니다. 탄력적 IP 주소를 NAT 게이트웨이와 연결합니다. NAT 게이트웨이를 사용하도록 VPC를 구성합니다.
B. 외부 전용 인터넷 게이트웨이를 배포합니다. 탄력적 IP 주소를 외부 전용 인터넷 게이트웨이와 연결합니다. 외부 전용 인터넷 게이트웨이를 사용하도록 Lambda 함수에서 탄력적 네트워크 인터페이스를 구성합니다.
C. 인터넷 게이트웨이를 배포합니다. 탄력적 IP 주소를 인터넷 게이트웨이와 연결합니다. 인터넷 게이트웨이를 사용하도록 Lambda 함수를 구성합니다.
D. 인터넷 게이트웨이를 배포합니다. 탄력적 IP 주소를 인터넷 게이트웨이와 연결합니다. 인터넷 게이트웨이를 사용하도록 퍼블릭 VPC 라우팅 테이블에서 기본 경로를 구성합니다.

해설
정답: A
이 솔루션은 퍼블릭 탄력적 IP 주소가 있는 NAT 게이트웨이를 통해 아웃바운드 트래픽을 라우팅하여 Lambda 함수에 인터넷에 대한 액세스를 제공합니다. 이를 통해 외부 공급자는 NAT 게이트웨이와 연결된 단일 공용 IP 주소를 화이트리스트에 추가하고 애플리케이션이 새 서비스에 액세스할 수 있습니다.
외부 전용 인터넷 게이트웨이는 IPv6 전용 : B 오답
탄력적(Elastic) IP를 인터넷 게이트웨이에 연결할 수 없음 : C,D 오답

◆ | **Q#0048.** | **Ref#0048.**
솔루션 아키텍트는 Amazon API Gateway 지역 엔드포인트와 AWS Lambda 함수를 사용하는 웹 애플리케이션을 개발했습니다. 웹 애플리케이션의 소비자는 모두 애플리케이션이 배포될 AWS 리전에 가깝습니다. Lambda 함수는 Amazon Aurora MySQL 데이터베이스만 쿼리합니다. 솔루션 설계자는 3개의 읽기 복제본을 갖도록 데이터베이스를 구성했습니다.

테스트 중에 애플리케이션이 성능 요구 사항을 충족하지 않습니다. 로드가 높을 때 애플리케이션은 많은 수의 데이터베이스 연결을 엽니다. 솔루션 아키텍트는 애플리케이션의 성능을 개선해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 조치를 취해야 합니까? (2개를 선택하세요.)

A. Aurora 데이터베이스의 클러스터 엔드포인트를 사용하십시오.
B. RDS Proxy를 사용하여 Aurora 데이터베이스의 리더 엔드포인트에 대한 연결 풀을 설정합니다.
C. Lambda 프로비저닝 동시성 기능을 사용하십시오.
D. 이벤트 핸들러 외부의 Lambda 함수에서 데이터베이스 연결을 여는 코드를 이동합니다.
E. API 게이트웨이 엔드포인트를 엣지 최적화 엔드포인트로 변경합니다.

해설
정답: B,D
B. RDS Proxy를 사용하여 Aurora 데이터베이스의 리더 엔드포인트에 대한 연결 풀을 설정하면 데이터베이스에 열려 있는 연결 수를 줄여 애플리케이션 성능을 향상시키는 데 도움이 될 수 있습니다. RDS Proxy는 연결 풀을 관리하고 들어오는 연결을 사용 가능한 읽기 전용 복제본으로 라우팅합니다. 이는 연결 관리에 도움이 되고 열고 닫아야 하는 연결 수를 줄일 수 있습니다.
D. 이벤트 핸들러 외부의 Lambda 함수에서 데이터베이스 연결을 열기 위한 코드를 이동하면 여러 요청에서 데이터베이스 연결을 재사용할 수 있으므로 애플리케이션 성능을 향상시키는데 도움이 될 수 있습니다. 이렇게 하면 각 요청에 대해 새 연결을 열고 닫는 오버헤드를 줄일 수 있습니다.

◆ | **Q#0049.** | **Ref#0049.**
한 회사가 AWS에서 웹 애플리케이션을 호스팅할 계획이며 Amazon EC2 인스턴스 그룹 전체에 트래픽 로드 밸런싱을 원합니다. 보안 요구 사항 중 하나는 클라이언트와 웹 서버 간 전송 시 end-to-end 암호화를 활성화하는 것입니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. ALB(Application Load Balancer) 뒤에 EC2 인스턴스를 배치합니다. AWS Certificate Manager(ACM)을 사용하여 SSL 인증서를 프로비저닝하고 SSL 인증서를 ALB와 연결합니다. SSL 인증서를 내보내고 각 EC2 인스턴스에 설치합니다. 포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 ALB를 구성합니다.
B. EC2 인스턴스를 대상 그룹과 연결합니다. AWS Certificate Manager(ACM)를 사용하여 SSL 인증서를 프로비저닝합니다. Amazon CloudFront 배포를 생성하고 SSL 인증서를 사용하도록 구성합니다. 대상 그룹을 오리진 서버로 사용하도록 CloudFront를 설정합니다.
C. ALB(Application Load Balancer) 뒤에 EC2 인스턴스를 배치합니다. ACM(AWS Certificate Manager)을 사용하여 SSL 인증서를 프로비저닝하고 SSL 인증서를 ALB와 연결합니다. 타사 SSL 인증서를 프로비저닝하고 각 EC2 인스턴스에 설치합니다. 포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 ALB를 구성합니다.
D. NLB(Network Load Balancer) 뒤에 EC2 인스턴스를 배치합니다. 타사 SSL 인증서를 프로비저닝하고 NLB와 각 EC2 인스턴스에 설치합니다. 포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 NLB를 구성합니다.

해설
정답: C (D라는 의견도 있음)
end-to-end 암호화를 활성화하려면 타사 SSL 인증서를 사용해야 합니다. AWS 인증서 사용 불가 : A,B 오답
C,D 중 정답은 EC2 인스턴스를 ALB 뒤에 배치할지, NLB 뒤에 배치할지의 문제인데,
NLB와 ALB 모두 SSL/TLS 오프로딩/종료를 처리할 수 있지만 여기서 핵심은 웹 트래픽(HTTP)을 가리키고 ALB는 웹 트래픽을 처리하고 NLB는 TCP 트래픽을 처리하므로 C를 선택
그러나 완전한 end-to-end 암호화를 위해서는 NLB를 사용해야 한다는 의견도 있는데, D의 경우 NLB에 인증서를 설치하는 것은 불필요하다는 것이 대다수 의견임

◆ | **Q#0050.** | **Ref#0050.**
한 회사에서 데이터 분석 환경을 온프레미스에서 AWS로 마이그레이션하려고 합니다. 환경은 두 개의 간단한 Node.js 애플리케이션으로 구성됩니다. 애플리케이션 중 하나는 센서 데이터를 수집하여 MySQL 데이터베이스에 로드합니다. 다른 애플리케이션은 데이터를 보고서로 집계합니다. 집계 작업이 실행되면 일부 로드 작업이 올바르게 실행되지 않습니다.

회사는 데이터 로딩 문제를 해결해야 합니다. 또한 회사는 회사 고객을 위해 중단이나 변경 없이 마이그레이션을 수행해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. Amazon Aurora MySQL 데이터베이스를 온프레미스 데이터베이스의 복제 대상으로 설정합니다. Aurora MySQL 데이터베이스용 Aurora 복제본을 생성하고 Aurora 복제본에 대해 실행할 집계 작업을 이동합니다. NLB(Network Load Balancer) 뒤에 있는 AWS Lambda 함수로 수집 엔드포인트를 설정하고 Amazon RDS 프록시를 사용하여 Aurora MySQL 데이터베이스에 씁니다. 데이터베이스가 동기화되면 복제 작업을 비활성화하고 Aurora 복제본을 기본 인스턴스로 다시 시작합니다. 수집기 DNS 레코드가 NLB를 가리키도록 합니다.
B. Amazon Aurora MySQL 데이터베이스를 설정합니다. AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스 데이터베이스에서 Aurora로 지속적인 데이터 복제를 수행합니다. Aurora MySQL 데이터베이스에 대해 실행할 집계 작업을 이동합니다. Auto Scaling 그룹의 Amazon EC2 인스턴스로 Application Load Balancer(ALB) 뒤의 수집 엔드포인트를 설정합니다. 데이터베이스가 동기화되면 수집기 DNS 레코드가 온프레미스에서 AWS로 컷오버된 후 AWS DMS 동기화 작업을 ALDisable로 지정합니다.
C. Amazon Aurora MySQL 데이터베이스를 설정합니다. AWS Database Migration Service(AWS DMS)를 사용하여 온프레미스 데이터베이스에서 Aurora로 지속적인 데이터 복제를 수행합니다. Aurora MySQL 데이터베이스용 Aurora 복제본을 생성하고 Aurora 복제본에 대해 실행할 집계 작업을 이동합니다. Application Load Balancer(ALB) 뒤에 있는 AWS Lambda 함수로 수집 엔드포인트를 설정하고 Amazon RDS 프록시를 사용하여 Aurora MySQL 데이터베이스에 씁니다. 데이터베이스가

동기화되면 콜렉터 DNS 레코드가 ALB를 가리키도록 하십시오. 온프레미스에서 AWS로 전환한 후 AWS DMS 동기화 작업을 비활성화합니다.
D. Amazon Aurora MySQL 데이터베이스를 설정합니다. Aurora MySQL 데이터베이스용 Aurora 복제본을 생성하고 Aurora 복제본에 대해 실행할 집계 작업을 이동합니다. 수집 엔드포인트를 Amazon Kinesis 데이터 스트림으로 설정합니다. Amazon Kinesis Data Firehose를 사용하여 데이터를 Aurora MySQL 데이터베이스에 복제합니다. 데이터베이스가 동기화되면 복제 작업을 비활성화하고 Aurora 복제본을 기본 인스턴스로 다시 시작합니다. 수집기 DNS 레코드가 Kinesis 데이터 스트림을 가리키도록 합니다.

해설
정답: C
Aurora MySQL을 생성하고 Migration 위한 데이터 복제는 DMS(Database Migration Service) 사용한다.
Aurora 복제본(Replica) 생성하여 데이터 보고서 집계 작업수행함으로써, 집계하는 동안 데이터 수집/로드 정상처리할 수 있다.
ALB 뒤에 있는 Lambda 함수로 수집 엔드포인트를 설정하면 클라이언트 측에 영향을 미치지 않고 작업할 수 있다.

051 (백은희) 4회차 完

◆ | **Q#0051.** | **Ref#0051.**
건강 보험 회사는 개인 식별 정보(PII)를 Amazon S3 버킷에 저장하고 있습니다. 회사는 S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화를 사용하여 객체를 암호화하고 있습니다. 새로운 요구 사항에 따라 S3 버킷의 현재 및 미래 모든 객체는 회사 보안 팀이 관리하는 키로 암호화되어야 합니다. S3 버킷에는 버전 관리가 활성화되어 있지 않습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. S3 버킷 속성에서 고객 관리형 키를 사용하여 기본 암호화를 SSE-S3으로 변경합니다. AWS CLI를 사용하여 S3 버킷의 모든 객체를 다시 업로드합니다. 암호화되지 않은 PutObject 요청을 거부하도록 S3 버킷 정책을 설정합니다.
B. S3 버킷 속성에서 기본 암호화를 AWS KMS 관리형 암호화 키(SSE-KMS)를 사용한 서버 측 암호화로 변경합니다. 암호화되지 않은 PutObject 요청을 거부하도록 S3 버킷 정책을 설정합니다. AWS CLI를 사용하여 S3 버킷의 모든 객체를 다시 업로드합니다.
C. S3 버킷 속성에서 기본 암호화를 AWS KMS 관리형 암호화 키(SSE-KMS)를 사용한 서버 측 암호화로 변경합니다. GetObject 및 PutObject 요청 시 객체를 자동으로 암호화하도록 S3 버킷 정책을 설정합니다.
D. S3 버킷 속성에서 고객 관리형 키를 사용하여 기본 암호화를 AES-256으로 변경합니다. S3 버킷에 액세스하는 모든 엔터티에 대한 암호화되지 않은 PutObject 요청을 거부하는 정책을 연결합니다. AWS CLI를 사용하여 S3 버킷의 모든 객체를 다시 업로드합니다.

해설
정답: B
새로운 요구사항에 따라, S3 버킷의 기본 암호화를 고객 관리 키로 변경해야 하며, 기존 객체를 새로운 암호화 방식으로 다시 업로드해야 하고, 앞으로 암호화되지 않은 객체가 업로드되지 않도록 S3 버킷 정책을 설정합니다.
(참고) https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html

◆ | **Q#0052.** | **Ref#0052.**
한 회사가 AWS 클라우드에서 웹 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon EC2 인스턴스 세트

에서 생성된 동적 콘텐츠로 구성됩니다. EC2 인스턴스는 ALB(Application Load Balancer)의 대상 그룹으로 구성된 Auto Scaling 그룹에서 실행됩니다.

이 회사는 Amazon CloudFront 배포를 사용하여 애플리케이션을 전 세계적으로 배포하고 있습니다. CloudFront 배포판은 ALB를 오리진(원본)으로 사용합니다. 이 회사는 DNS에 Amazon Route 53을 사용하고 CloudFront 배포를 위해 www.example.com이라는 A 레코드를 생성했습니다.

솔루션 설계자는 가용성이 높고 내결함성이 있도록 애플리케이션을 구성해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 다른 AWS 리전에서 전체 보조 애플리케이션 배포를 프로비저닝합니다. Route 53 A 레코드를 장애 조치 레코드로 업데이트합니다. 두 CloudFront 배포를 모두 값으로 추가합니다. Route 53 상태 확인을 생성합니다.
> **B.** 다른 AWS 리전에 ALB, Auto Scaling 그룹 및 EC2 인스턴스를 프로비저닝합니다. CloudFront 배포를 업데이트하고 새 ALB에 대한 두 번째 오리진을 생성합니다. 두 오리진에 대한 오리진 그룹을 생성합니다. 하나의 오리진을 기본(primary)으로 구성하고 다른 하나의 오리진을 보조(secondary)로 구성합니다.
> **C.** 다른 AWS 리전에 Auto Scaling 그룹과 EC2 인스턴스를 프로비저닝합니다. ALB에서 새 Auto Scaling 그룹에 대한 두 번째 대상을 생성합니다. ALB에서 장애 조치 라우팅 알고리즘을 설정합니다.
> **D.** 다른 AWS 리전에 전체 보조 애플리케이션 배포를 프로비저닝합니다. 두 번째 CloudFront 배포를 생성하고 새 애플리케이션 설정을 오리진으로 추가합니다. AWS Global Accelerator 액셀러레이터를 생성합니다. 두 CloudFront 배포를 모두 엔드포인트로 추가합니다.
>
> 해설
> 정답: B
> 다른 AWS 리전의 ALB, Auto Scaling 그룹 및 EC2 인스턴스를 프로비저닝하면 애플리케이션에 대한 중복성 및 장애 조치 기능이 제공됩니다. CloudFront 배포는 두 번째 리전에 새 ALB에 대한 두 번째 오리진을 생성함으로써 기본 오리진에 문제가 있는 경우 트래픽을 정상 오리진으로 자동 라우팅할 수 있습니다. 이렇게 하면 애플리케이션의 가용성과 내결함성이 유지됩니다
> (참고)
> A : 옵션 A는 Route 53 장애 조치 레코드를 사용하므로 올바르지 않습니다. 이로 인해 클라이언트의 지연 시간과 DNS 확인 시간이 늘어날 수 있습니다.
> C : 애플리케이션의 중요한 구성 요소인 로드 밸런서에 대한 중복성을 제공하지 않기 때문에 올바르지 않습니다.
> D : 첫 번째 리전의 기본 원본에 문제가 있는 경우 애플리케이션에 대한 중복성을 제공하지 않으므로 올바르지 않습니다.

◆ | **Q#0053.** | **Ref#0053.**
회사에는 AWS 계정이 많은 AWS Organizations 조직이 있습니다. AWS 계정 중 하나가 Transit(전송) 계정으로 지정되고 다른 모든 AWS 계정과 공유되는 Transit(전송) 게이트웨이가 있습니다. 모든 글로벌 오피스와 트랜짓 계정 간에 AWS Site-to-Site VPN 연결이 구성되어 있습니다. 회사는 모든 계정에서 AWS Config를 활성화했습니다.

회사의 네트워킹 팀은 글로벌 사무소에 속한 내부 IP 주소 범위 목록을 중앙에서 관리해야 합니다. 개발자는 이 목록을 참조하여 애플리케이션에 안전하게 액세스할 수 있어야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** Amazon S3에서 호스팅되고 모든 내부 IP 주소 범위를 나열하는 JSON 파일을 생성합니다. JSON 파일이 업데이트될 때 호출할 수 있는 각 계정에서 Amazon Simple Notification Service (Amazon SNS) 주제를 구성합니다. AWS Lambda 함수를 SNS 주제에 구독하여 관련 보안 그룹 규칙을 업데이트합니다.
> **B.** 모든 내부 IP 주소 범위를 포함하는 새로운 AWS Config 관리형 규칙을 생성합니다. 규칙을 사용하여 각 계정의 보안 그룹을 확인하여 IP 주소 범위 목록을 준수하는지 확인합니다. 감지된 모든 비

준수 보안 그룹을 자동으로 교정하도록 규칙을 구성합니다.
C. 전송 계정(transit account)에서 모든 내부 IP 주소 범위가 포함된 VPC Prefix 목록을 생성합니다. AWS Resource Access Manager를 사용하여 Prefix 목록을 다른 모든 계정과 공유합니다. 공유된 Prefix 목록을 사용하여 다른 계정의 보안 그룹 규칙을 구성합니다.
D. 전송 계정(transit account)에서 모든 내부 IP 주소 범위를 포함하는 보안 그룹을 생성합니다. 다른 계정들의 보안 그룹이 전송 계정의 보안 그룹을 참조하도록 구성하며, 이때 "/sg-1a2b3c4d" 와 같은 중첩 보안 그룹 참조(nested security group reference)를 사용합니다.

해설
정답: C
모든 내부 IP 주소 범위가 포함된 VPC Prefix 리스트가 Transit 계정에서 생성되고, AWS Resource Access Manager를 사용하여 다른 모든 계정과 공유됩니다. 이를 통해 IP 주소 범위를 중앙에서 관리할 수 있으며 각 계정의 보안 그룹 규칙을 수동으로 업데이트할 필요가 없습니다. 솔루션은 AWS Config를 사용하여 준수 여부를 확인하고, 비준수 보안 그룹을 자동으로 교정할 수 있게 합니다.

◆ | **Q#0054.** | **Ref#0054.**
회사는 Amazon S3에서 정적 웹 사이트로 새 애플리케이션을 실행합니다. 회사는 프로덕션 AWS 계정에 애플리케이션을 배포하고 Amazon CloudFront를 사용하여 웹 사이트를 제공합니다. 웹사이트는 Amazon API Gateway REST API를 호출합니다. 각 API 메서드는 AWS Lambda 함수에 의해 지원됩니다.

회사는 각 API Lambda 함수의 권장 구성 메모리, 권장 비용, 현재 구성과 권장 사항 간의 가격 차이를 표시하기 위해 2주마다 CSV 보고서를 생성하려고 합니다. 회사는 보고서를 S3 버킷에 저장합니다.

가장 짧은 개발 시간으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 2주 동안 Amazon CloudWatch Logs에서 각 API Lambda 함수에 대한 지표 데이터를 추출하는 Lambda 함수를 생성합니다. 데이터를 표 형식으로 대조합니다. 데이터를 S3 버킷에 .csv 파일로 저장합니다. Amazon EventBridge 규칙을 생성하여 Lambda 함수가 2주마다 실행되도록 예약합니다.
B. AWS Compute Optimizer를 선택합니다. ImportLambdaFunctionRecommendations 작업을 호출하는 Lambda 함수를 생성합니다. .csv 파일을 S3 버킷으로 내보냅니다. Amazon EventBridge 규칙을 생성하여 Lambda 함수가 2주마다 실행되도록 예약합니다.
C. AWS Compute Optimizer를 선택합니다. 향상된 인프라 측정항목을 설정하세요. Compute Optimizer 콘솔 내에서 Lambda 권장 사항을 .csv 파일로 내보내는 작업을 예약합니다. 2주마다 S3 버킷에 파일을 저장합니다.
D. 프로덕션 계정에 대한 AWS Business Support 플랜을 구매합니다. AWS Trusted Advisor 점검을 위해 AWS Compute Optimizer를 선택합니다. Trusted Advisor 콘솔에서 비용 최적화 검사를 .csv 파일로 내보내는 작업을 예약합니다. 2주마다 S3 버킷에 파일을 저장합니다.

해설
정답: B
AWS Compute Optimizer : AWS 리소스(예: EC2 인스턴스, Lambda 함수, ECS 태스크) 사용을 분석하고 최적화 권장 사항을 제공하는 서비스입니다. 이 서비스는 사용 패턴을 분석하여 리소스가 과도하게 프로비저닝되었거나 과소 프로비저닝된 경우 최적의 리소스 유형 및 구성을 추천합니다.
ExportLambdaFunctionRecommendations : AWS Compute Optimizer API의 작업 중 하나입니다. 이 작업을 사용하면 Compute Optimizer가 제공하는 Lambda 함수에 대한 권장 사항을 CSV 파일 형식으로 내보낼 수 있습니다.
Amazon EventBridge : AWS에서 이벤트를 생성하고 라우팅하는 서버리스 이벤트 버스입니다. EventBridge는 AWS 서비스, 통합 애플리케이션 및 자체 애플리케이션에서 발생하는 이벤트를 캡처하고 필터링할 수 있습니다. EventBridge를 사용하면 이벤트 기반 애플리케이션을 손쉽게 구축할 수 있으며, 특정 이벤트가 발생할 때 Lambda 함수, Step Functions, SNS, SQS 등 다양한 AWS 서비스로

이벤트를 전송할 수 있습니다.

◆ | **Q#0055.** | **Ref#0055.**
회사의 공장 및 자동화 애플리케이션이 단일 VPC에서 실행되고 있습니다. Amazon EC2, Amazon Elastic Container Service(Amazon ECS) 및 Amazon RDS의 조합에서 20개 이상의 애플리케이션이 실행됩니다.

이 회사에는 세 팀에 소프트웨어 엔지니어가 분산되어 있습니다. 세 팀 중 하나가 각 애플리케이션을 소유하며, 매번 모든 애플리케이션의 비용과 성능을 책임집니다. 팀 리소스에는 해당 애플리케이션과 팀을 나타내는 태그가 있습니다. 팀은 일상 활동에 IAM 액세스를 사용합니다.

회사는 월별 AWS 청구서에서 각 애플리케이션이나 팀에 발생한 비용을 확인해야 합니다. 또한 회사는 지난 12개월의 비용을 비교하고 향후 12개월의 비용을 예측하는 데 도움이 되는 보고서를 작성할 수 있어야 합니다. 솔루션 아키텍트는 이러한 비용 보고서를 제공하는 AWS Billing and Cost Management 솔루션을 권장해야 합니다.

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

A. 애플리케이션과 팀을 나타내는 사용자 정의 비용 할당 태그를 활성화합니다.
B. 애플리케이션과 팀을 나타내는 AWS 생성 비용 할당 태그를 활성화합니다.
C. Billing and Cost Management에서 각 애플리케이션에 대한 비용 범주를 생성합니다.
D. Billing and Cost Management에 대한 IAM 액세스를 활성화합니다.
E. 비용 예산을 수립합니다.
F. 비용 탐색기를 활성화합니다.

해설
정답: A C F (A D F 논란)
A : 사용자 정의 비용 할당 태그를 활성화하여 각 애플리케이션 및 팀을 나타내는 태그를 사용하면 비용 보고서에서 태그를 기준으로 비용을 추적할 수 있습니다.
C : 비용 및 관리에서 각 애플리케이션에 대한 비용 카테고리를 생성하면 애플리케이션별로 비용을 그룹화할 수 있습니다.
F : Cost Explorer를 활성화하면 비용 데이터를 시각화하고 분석할 수 있는 도구를 사용할 수 있습니다. Cost Explorer는 지난 12개월 동안의 비용을 비교하고 향후 12개월 동안의 비용을 예측하는 데 도움이 됩니다.
D : 팀이 비용 및 청구 관리 콘솔에 액세스하여 비용 보고서를 보고 분석할 수 있으려면, IAM 액세스를 활성화해야 합니다.
팀이 비용을 직접 관리하고 접근해야 한다면 ADF가 적절하고, 단순히 비용을 분석하고 보고서를 생성하는 것이 목표라면 ACF가 적절합니다.

◆ | **Q#0056.** | **Ref#0056.**
AWS 고객은 온프레미스에서 실행되는 웹 애플리케이션을 보유하고 있습니다. 웹 애플리케이션은 방화벽 뒤에 있는 서드파티 API에서 데이터를 가져옵니다. 서드파티는 각 클라이언트의 허용 목록에서 단 하나의 공개 CIDR 블록만 허용합니다.

고객은 웹 애플리케이션을 AWS 클라우드로 마이그레이션하려고 합니다. 애플리케이션은 VPC의 ALB(Application Load Balancer) 뒤의 Amazon EC2 인스턴스 세트에서 호스팅됩니다. ALB는 퍼블릭 서브넷에 있습니다. EC2 인스턴스는 프라이빗 서브넷에 있습니다. NAT 게이트웨이는 프라이빗 서브넷에 대한 인터넷 액세스를 제공합니다.

솔루션 설계자는 마이그레이션 후에도 웹 애플리케이션이 계속해서 서드파티 API를 호출할 수 있도록 어떻게 보장해야 합니까?

A. 고객 소유의 퍼블릭 IP 주소 블록을 VPC에 연결합니다. VPC의 퍼블릭 서브넷에 대한 퍼블릭 IP 주소 지정을 활성화합니다.
B. AWS 계정에 고객 소유의 퍼블릭 IP 주소 블록을 등록합니다. 주소 블록에서 Elastic IP 주소를 생성하고 이를 VPC의 NAT 게이트웨이에 할당합니다.

C. 고객 소유 IP 주소 블록에서 Elastic IP 주소를 생성합니다. ALB에 고정 Elastic IP 주소를 할당합니다.
D. AWS 계정에 고객 소유의 퍼블릭 IP 주소 블록을 등록합니다. 주소 블록의 Elastic IP 주소를 사용하도록 AWS Global Accelerator를 설정합니다. ALB를 가속기 엔드포인트로 설정하십시오.

해설
정답: B
NAT 게이트웨이에 할당된 고객 소유 퍼블릭 IP 주소를 사용하여 마이그레이션 후에도 계속해서 서드파티 API를 호출할 수 있습니다. 이렇게 하면 서드파티 API가 허용 목록에 있는 고객 소유 IP 주소에서 들어오는 트래픽만 허용할 수 있습니다.
(참고) https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html
EIP : Elastic IP는 AWS에서 제공하는 정적인 공용 IP 주소입니다. 주로 AWS 리소스인 EC2 인스턴스, NAT 게이트웨이, Application Load Balancer 등에 할당하여 사용됩니다.
Elastic IP는 생성 후에 변경되지 않는 고정 IP 주소입니다. 이는 IP 주소가 변경되는 일반적인 경우와 달리, 유지보수 및 관리 측면에서 편리성을 제공합니다.
Elastic IP 주소는 EC2 인스턴스, NAT 게이트웨이, ALB 등의 AWS 리소스에 직접 연결할 수 있습니다. 이를 통해 해당 리소스가 공용 인터넷을 통해 접근 가능하게 할 수 있습니다.
EC2 인스턴스의 경우, 인스턴스를 중지하고 다시 시작하더라도 할당된 Elastic IP는 유지됩니다. 이는 인스턴스의 재부팅이나 이전과 동일한 IP 주소로의 접근을 보장합니다.

◆ | **Q#0057.** | **Ref#0057.**
여러 AWS 계정을 보유한 회사가 AWS Organizations 및 서비스 제어 정책(SCP)을 사용하고 있습니다. 관리자가 다음 SCP를 생성하여 AWS 계정 1111-1111-1111이 포함된 조직 단위(OU)에 연결했습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyCloudTrail",
            "Effect": "Deny",
            "Action": "cloudtrail:*",
            "Resource": "*"
        }
    ]
}
```

계정 1111-1111-1111에서 작업하는 개발자는 Amazon S3 버킷을 생성할 수 없다고 불평합니다. 관리자는 이 문제를 어떻게 해결해야 합니까?

A. SCP에 s3:CreateBucket을 "Allow" 효과로 추가합니다.
B. 해당 계정을 OU에서 제거하고, SCP를 계정 1111-1111-1111에 직접 연결합니다.
C. 개발자들에게 그들의 IAM 엔티티에 Amazon S3 권한을 추가하라고 지시합니다.
D. SCP를 계정 1111-1111-1111에서 제거합니다.

해설
정답: C
주어진 SCP는 기본적으로 모든 액션을 허용합니다(Allow), 단 cloudtrail 관련 액션만 명시적으로 금지하고 있습니다(Deny). SCP 자체에는 S3 버킷 생성(s3:CreateBucket)을 금지하는 내용이 없습니다. SCP에서 모든 액션을 허용했지만, 개발자들이 S3 버킷을 생성할 수 없는 이유는 IAM 권한이 충분하

지 않기 때문입니다.
SCP는 계정 전체의 정책을 설정하지만, 각 사용자나 역할에 부여된 IAM 권한이 실제 작업 수행 여부를 결정합니다. 따라서 IAM 권한을 조정하여 문제를 해결해야 합니다.

◆ | **Q#0058.** | **Ref#0058.**
회사에는 회사 비즈니스에 중요한 모놀리식 애플리케이션이 있습니다. 회사는 Amazon Linux 2를 실행하는 Amazon EC2 인스턴스에서 애플리케이션을 호스팅합니다. 회사의 애플리케이션 팀은 법무 부서로부터 인스턴스의 암호화된 Amazon Elastic Block Store(Amazon EBS) 볼륨의 데이터를 Amazon S3 버킷에 백업하라는 지시를 받습니다. 애플리케이션 팀에는 인스턴스에 대한 관리 SSH 키 쌍이 없습니다. 애플리케이션은 계속해서 사용자에게 서비스를 제공해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon S3에 쓸 수 있는 권한이 있는 인스턴스에 역할을 연결합니다. AWS Systems Manager Session Manager 옵션을 사용하여 인스턴스에 액세스하고 명령을 실행하여 Amazon S3에 데이터를 복사합니다.
B. 재부팅 옵션이 활성화된 인스턴스의 이미지를 생성합니다. 이미지에서 새 EC2 인스턴스를 시작합니다. Amazon S3에 쓰기 권한이 있는 새 인스턴스에 역할을 연결합니다. Amazon S3에 데이터를 복사하는 명령을 실행합니다.
C. Amazon Data Lifecycle Manager (Amazon DLM)를 사용하여 EBS 볼륨의 스냅샷을 만듭니다. 데이터를 Amazon S3에 복사합니다.
D. 인스턴스의 이미지를 생성합니다. 이미지에서 새 EC2 인스턴스를 시작합니다. Amazon S3에 쓰기 권한이 있는 새 인스턴스에 역할을 연결합니다. Amazon S3에 데이터를 복사하는 명령을 실행합니다.

해설
정답: C (A 논란, voting 비중 유사함)
C(x): AWS는 루트 볼륨 스냅샷을 생성하기 위해 EC2 인스턴스를 중지할 것을 권장합니다. 루트 디바이스 역할을 하는 EBS 볼륨에 대한 스냅샷을 생성하는 경우 스냅샷을 생성하기 전에 인스턴스를 중지하는 것이 좋습니다.
C : Amazon Data Lifecycle Manager (DLM)을 사용하여 EBS 볼륨의 스냅샷을 찍는 것은 인스턴스 또는 SSH 키 쌍에 접근할 필요 없이 볼륨의 백업을 만들 수 있기 때문에 요구 사항을 충족합니다. 또한 DLM을 사용하면 특정 간격으로 백업을 예약할 수 있으며, 스냅샷을 S3 버킷으로 복사할 수도 있습니다. 이 방법은 EBS 볼륨 레벨에서 백업이 수행되기 때문에 실행 중인 애플리케이션에 영향을 미치지 않습니다.
A : 이 옵션은 SSH 키 쌍을 요구하지 않고 EC2 인스턴스에 대한 안전한 접근을 허용합니다. IAM 역할을 인스턴스에 연결하여 S3 쓰기 권한을 부여함으로써 세션 관리자를 사용하여 데이터 복사 명령을 직접 S3로 실행할 수 있습니다. 이 방법은 실행 중인 애플리케이션에 영향을 주지 않으므로 지속적인 운영 요구 사항을 충족합니다.
직접 S3로 복사하는 경우 A, 스냅샷을 활용하여 백업 받는 경우 C를 선택할 수 있습니다. 백업 정책에 있어서는 C가 더 안정적입니다.

◆ | **Q#0059.** | **Ref#0059.**
솔루션 아키텍트는 AWS 계정의 Amazon S3 버킷에서 새 AWS 계정의 새 S3 버킷으로 데이터를 복사해야 합니다. 솔루션 아키텍트는 AWS CLI를 사용하는 솔루션을 구현해야 합니다.

데이터를 성공적으로 복사하려면 어떤 단계를 조합해야 합니까? (3개를 선택하세요.)

A. 원본 버킷이 해당 콘텐츠를 나열하고 대상 버킷에 객체를 배치하고 객체 ACL을 설정할 수 있도록 버킷 정책을 생성합니다. 버킷 정책을 대상 버킷에 연결합니다.
B. 대상 계정의 사용자가 원본 버킷의 콘텐츠를 나열하고 원본 버킷의 객체를 읽을 수 있도록 허용

하는 버킷 정책을 만듭니다. 버킷 정책을 원본 버킷에 연결합니다.
C. 원본 계정에서 IAM 정책을 생성합니다. 원본 계정의 사용자가 원본 버킷에서 콘텐츠를 나열하고 객체를 가져올 수 있도록 허용하고, 대상 버킷에서 콘텐츠를 나열하고 객체를 넣고 객체 ACL을 설정할 수 있도록 정책을 구성합니다. 정책을 사용자에게 연결합니다.
D. 대상 계정에 IAM 정책을 생성합니다. 대상 계정의 사용자가 원본 버킷에서 콘텐츠를 나열하고 객체를 가져올 수 있도록 허용하고, 대상 버킷에서 콘텐츠를 나열하고 객체를 넣고 objectACL을 설정할 수 있도록 정책을 구성합니다. 정책을 사용자에게 연결합니다.
E. 원본 계정의 사용자로 aws s3 sync 명령을 실행합니다. 데이터를 복사할 소스 및 대상 버킷을 지정합니다.
F. 대상 계정의 사용자로 aws s3 sync 명령을 실행합니다. 데이터를 복사할 소스 및 대상 버킷을 지정합니다.

해설
정답: B D F
B: 원본 버킷에 대해 대상 계정 사용자가 필요한 읽기 권한을 갖도록 설정합니다.
D: 대상 버킷에 대해 대상 계정 사용자가 필요한 모든 권한을 갖도록 설정합니다.
F: aws s3 sync 명령어를 대상 계정의 사용자로 실행함으로써, 복사된 객체가 대상 버킷에서 적절한 권한을 갖도록 보장합니다.
대상 계정의 사용자가 모든 권한을 가지고 작업을 수행할 수 있어야 합니다.

◆ | **Q#0060.** | **Ref#0060.**
한 회사는 AWS CloudFormation 스택에 배포된 AWS Lambda를 기반으로 애플리케이션을 구축했습니다. 웹 애플리케이션의 마지막 프로덕션 릴리스에서는 몇 분 동안 중단이 발생하는 문제가 발생했습니다. 솔루션 설계자는 카나리아 릴리스(cananry release)를 지원하도록 배포 프로세스를 조정해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 새로 배포된 모든 버전의 Lambda 함수에 대한 별칭을 생성합니다. AWS CLI update-alias 명령을 Routing-config 파라미터와 함께 사용하여 로드를 분산하십시오.
B. 애플리케이션을 새로운 CloudFormation 스택에 배포합니다. 부하를 분산하려면 Amazon Route 53 가중치 기반 라우팅 정책을 사용하십시오.
C. 새로 배포된 모든 Lambda 함수에 대한 버전을 생성합니다. AWS CLI update-function-configuration 명령을 Routing-config 파라미터와 함께 사용하여 로드를 분산하십시오.
D. AWS CodeDeploy를 구성하고 배포 구성에서 CodeDeployDefault.OneAtATime을 사용하여 로드를 분산시킵니다.

해설
정답: A
A : Lambda 함수의 새 버전에 대해 별칭(alias)을 만들고, update-alias 명령과 routing-config 매개변수를 사용하여 트래픽을 새 버전으로 점진적으로 전환할 수 있습니다.
별칭 생성: Lambda 함수의 모든 새 버전에 대해 별칭을 생성합니다. 별칭을 사용하면 사용자에게 친숙한 이름을 특정 버전의 함수와 연결할 수 있습니다. 라우팅 구성: AWS Lambda는 트래픽을 한 별칭에서 다른 별칭으로 점진적으로 이동할 수 있는 라우팅 구성을 지원합니다.
D : AWS CodeDeploy는 다양한 배포 전략을 지원하여, 동시 배포, 일괄 배포, 롤링 배포 등을 선택할 수 있습니다. 그렇지만 CodeDeployDefault.OneAtATime은 EC2/온프레미스용 CodeDeploy 옵션인 반면, 이 시나리오에서는 CodeDeployDefault.LambdaCanary10Percent5Minutes와 같은 Lambda용 카나리아 옵션이 필요합니다.
(참고)
카나리아 릴리스는 소프트웨어 개발에서 사용되는 개발 및 배포 전략 중 하나입니다. 이 전략은 새로운 기능이나 업데이트를 포함한 소프트웨어를 일찍이 제한된 사용자 집단에게 먼저 배포하고, 사용자들이 이를 테스트하고 피드백을 제공하도록 하는 것을 의미합니다. 이 초기 사용자 집단은 '카나리아'로 비유되며, 일종의 '실험실' 역할을 합니다. 이 과정을 통해 개발자는 잠재적인 버그나 문제

점을 신속히 발견하고 수정할 수 있습니다.

061 (송희성) 4회차 完

◆ | **Q#0061.** | **Ref#0061.**
금융 회사는 Amazon S3에서 데이터 레이크를 호스팅합니다. 회사는 매일 밤 여러 제3자로부터 SFTP를 통해 금융 데이터 기록을 받습니다. 이 회사는 VPC의 퍼블릭 서브넷에 있는 Amazon EC2 인스턴스에서 자체 SFTP 서버를 실행합니다. 파일이 업로드된 후 동일한 인스턴스에서 실행되는 크론 작업을 통해 데이터 레이크로 이동됩니다. SFTP 서버는 Amazon Route 53을 사용하여 DNS sftp.example.com에 연결할 수 있습니다.

SFTP 솔루션의 안정성과 확장성을 향상하려면 솔루션 설계자가 무엇을 해야 합니까?

> **A.** EC2 인스턴스를 Auto Scaling 그룹으로 이동합니다. Application Load Balancer(ALB) 뒤에 EC2 인스턴스를 배치합니다. ALB를 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
> **B.** SFTP 서버를 AWS Transfer for SFTP로 마이그레이션합니다. 서버 엔드포인트 호스트 이름을 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
> **C.** SFTP 서버를 AWS Storage Gateway의 파일 게이트웨이로 마이그레이션합니다. 파일 게이트웨이 엔드포인트를 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
> **D.** NLB(Network Load Balancer) 뒤에 EC2 인스턴스를 배치합니다. NLB를 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
>
> 해설
> 정답: B
> AWS Transfer for SFTP는 다양한 리전의 데이터를 주고받을 수 있으며, 서버 관리와 확장성을 자동으로 aws에서 관리해준다.
>
> ALB의 경우는 HTTP/HTTPS에 최적화 되어있다. 이에 반해 NLB는 TCP최적화이지만, 추가적 관리 소요 및 새로운 SFTP용 서버를 한대 더 파야 한다.
>
> AWS Transfer Family Features

◆ | **Q#0062.** | **Ref#0062.**
회사는 온프레미스 데이터 센터에서 실행되는 VMware 인프라에서 Amazon EC2로 애플리케이션을 마이그레이션하려고 합니다. 솔루션 설계자는 마이그레이션 중에 소프트웨어 및 구성 설정을 보존해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** 데이터 저장소를 Amazon FSx for Windows File Server로 복제하기 시작하도록 AWS DataSync 에이전트를 구성합니다. SMB 공유를 사용하여 VMware 데이터 저장소를 호스팅합니다. VM Import/Export를 사용하여 VM을 Amazon EC2로 이동합니다.
> **B.** VMware vSphere 클라이언트를 사용하여 애플리케이션을 OVF(Open Virtualization Format) 형식의 이미지로 내보냅니다. 대상 AWS 리전에 이미지를 저장할 Amazon S3 버킷을 생성합니다. VM Import를 위한 IAM 역할을 생성하고 적용합니다. AWS CLI를 사용하여 EC2 가져오기 명령을 실행합니다.
> **C.** CIFS(Common Internet File System) 공유를 내보내도록 파일 서비스용 AWS Storage Gateway를 구성합니다. 공유 폴더에 백업 복사본을 만듭니다. AWS Management Console에 로그인하고 백업 복사본에서 AMI를 생성합니다. AMI를 기반으로 하는 EC2 인스턴스를 시작합니다.
> **D.** AWS 시스템 관리자에서 하이브리드 환경을 위한 관리형 인스턴스 활성화를 생성합니다. 온프레미스 VM에 Systems Manager 에이전트를 다운로드하고 설치합니다. VM을 Systems Manager에 등

록하여 관리형 인스턴스로 만듭니다. AWS Backup을 사용하여 VM의 스냅샷을 생성하고 AMI를 생성합니다. AMI를 기반으로 하는 EC2 인스턴스를 시작합니다.

해설
정답: B
OVF 형식의 이미지를 사용하여 VM의 설정을 그대로 유지하면서 EC2로 마이그레이션 할 수 있다.
VMware vSphere를 활용하여, OVF형식으로 내보내고 이를 Amazon S3버킷에 저장 후, VM Import를 사용한다.

◆ | **Q#0063.** | **Ref#0063.**
비디오 처리 회사에는 Amazon S3 버킷에서 이미지를 다운로드하고, 이미지를 처리하고, 변환된 이미지를 두 번째 S3 버킷에 저장하고, Amazon DynamoDB 테이블의 이미지에 대한 메타데이터를 업데이트하는 애플리케이션이 있습니다. 애플리케이션은 Node.js로 작성되었으며 AWS Lambda 함수를 사용하여 실행됩니다. 새로운 이미지가 Amazon S3에 업로드되면 Lambda 함수가 호출됩니다.

한동안 문제 없이 애플리케이션이 실행되었습니다. 그러나 이미지의 크기가 크게 늘어났습니다. 이제 Lambda 함수가 시간 초과 오류로 인해 자주 실패합니다. 함수 시간 초과는 최대값으로 설정됩니다. 솔루션 설계자는 호출 실패를 방지하기 위해 애플리케이션의 아키텍처를 리팩터링해야 합니다. 회사는 기본 인프라를 관리하고 싶지 않습니다.

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

A. 애플리케이션 코드가 포함된 Docker 이미지를 구축하여 애플리케이션 배포를 수정합니다. Amazon Elastic Container Registry(Amazon ECR)에 이미지를 게시합니다.
B. 호환성 유형이 AWS Fargate인 새로운 Amazon Elastic Container Service(Amazon ECS) 작업 정의를 생성합니다. Amazon Elastic Container Registry(Amazon ECR)에서 새 이미지를 사용하도록 작업 정의를 구성합니다. 새 파일이 Amazon S3에 도착하면 ECS 작업 정의를 사용하여 ECS 작업을 호출하도록 Lambda 함수를 조정합니다.
C. 병렬 상태로 AWS Step Functions 상태 머신을 생성하여 Lambda 함수를 호출합니다. Lambda 함수의 프로비저닝된 동시성을 높입니다.
D. Amazon EC2의 호환성 유형을 사용하여 새로운 Amazon Elastic Container Service(Amazon ECS) 작업 정의를 생성합니다. Amazon Elastic Container Registry(Amazon ECR)에서 새 이미지를 사용하도록 작업 정의를 구성합니다. 새 파일이 Amazon S3에 도착하면 ECS 작업 정의를 사용하여 ECS 작업을 호출하도록 Lambda 함수를 조정합니다.
E. Amazon Elastic File System(Amazon EFS)에 이미지를 저장하고 Amazon RDS DB 인스턴스에 메타데이터를 저장하도록 애플리케이션을 수정합니다. EFS 파일 공유를 탑재하도록 Lambda 함수를 조정합니다.

해설
정답: AB
Docker 이미지를 사용하여 어플리케이션을 컨테이너 이미지로 만들고 AWS Fargate를 활용하여 인프라 관리 없이 14일까지는 작업을 수행할 수 있다.
Lambda는 timeout이 15분이므로 Fargate가 좋은 해결책이 될 수 있다.
C의 경우 이미지 크기 증가로 각각의 lambda가 느려졌으므로, 병렬 수행으로 Timeout문제를 해결할 수 없다.
D의 경우 EC2인프라를 관리해야하는 소요가 생긴다.

◆ | **Q#0064.** | **Ref#0064.**
회사는 AWS Organizations에 조직을 가지고 있습니다. 회사는 AWS Control Tower를 사용하여 조직의 랜딩 존을 배포하고 있습니다. 회사는 거버넌스 및 정책 시행을 구현하기를 원합니다. 회사는 회사의 프로덕션 OU에 저장되어 있는 암호화되지 않은 Amazon RDS DB 인스턴스를 감지하는 정책을 구현해야 합니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Control Tower에서 필수 가드레일을 활성화합니다. 프로덕션 OU에 필수 가드레일을 적용합니다.
B. AWS Control Tower의 강력 권장 가드레일 목록에서 적절한 가드레일을 활성화합니다. 프로덕션 OU에 가드레일을 적용합니다.
C. AWS Config를 사용하여 새로운 필수 가드레일을 생성합니다. 프로덕션 OU의 모든 계정에 규칙을 적용합니다.
D. AWS Control Tower에서 사용자 지정 SCP를 생성합니다. 프로덕션 OU에 SCP를 적용합니다.

해설
정답: B
참조 링크에 나타난 대로 강력권장 가드레일 목록에 있으니, 적용하면 된다.
A와 C는 Owner가 AWS Control Tower라 수정할 수 없다.
D의경우는 SCP는 특정 리소스를 검사하는 것이 아니고, 서비스의 사용과 관련된 정책을 포함한다.

unencrypted RDS

◆ | **Q#0065.** | **Ref#0065.**
한 스타트업 회사는 최신 Amazon Linux 2 AMI를 사용하여 프라이빗 서브넷에서 Amazon EC2 인스턴스 플릿을 호스팅합니다. 회사의 엔지니어들은 문제 해결을 위해 인스턴스에 대한 SSH 액세스에 크게 의존하고 있습니다.

회사의 기존 아키텍처에는 다음이 포함됩니다.

• 프라이빗 및 퍼블릭 서브넷이 있는 VPC와 NAT 게이트웨이.
• 온프레미스 환경과의 연결을 위한 사이트 간 VPN.
• 온프레미스 환경에서 직접 SSH에 액세스할 수 있는 EC2 보안 그룹.

회사는 SSH 액세스에 대한 보안 제어를 강화하고 엔지니어가 실행하는 명령에 대한 감사를 제공해야 합니다.

솔루션 아키텍트는 어떤 전략을 사용해야 합니까?

A. EC2 인스턴스 집합에 EC2 Instance Connect를 설치하고 구성합니다. 포트 22에서 인바운드 TCP를 허용하는 EC2 인스턴스에 연결된 모든 보안 그룹 규칙을 제거합니다. 엔지니어에게 EC2 Instance Connect CLI를 사용하여 인스턴스에 원격으로 액세스하도록 조언하십시오.
B. 엔지니어 장치의 IP 주소에 대한 포트 22의 인바운드 TCP만 허용하도록 EC2 보안 그룹을 업데이트합니다. 모든 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치하고 운영 체제 감사 로그를 CloudWatch Logs로 보냅니다.
C. 엔지니어 장치의 IP 주소에 대한 포트 22의 인바운드 TCP만 허용하도록 EC2 보안 그룹을 업데이트합니다. EC2 보안 그룹 리소스 변경을 위해 AWS Config를 활성화합니다. AWS Firewall Manager를 활성화하고 규칙 변경 사항을 자동으로 해결하는 보안 그룹 정책을 적용합니다.
D. AmazonSSMManagedInstanceCore 관리형 정책이 연결된 IAM 역할을 생성합니다. 모든 EC2 인스턴스에 IAM 역할을 연결합니다. 포트 22에서 인바운드 TCP를 허용하는 EC2 인스턴스에 연결된 모든 보안 그룹 규칙을 제거합니다. 엔지니어가 장치에 AWS Systems Manager Session Manager 플러그인을 설치하고 Systems Manager의 시작 세션 API 호출을 사용하여 인스턴스에 원격으로 액세스하도록 합니다.

해설
정답: D
Session Manager을 활용하여 명령어 감사 지원이 되며, SSH대신 SSM 을 활용하여 HTTP연결을 하므로, Key Pair, 포트 허용을 위한 보안 그룹을 만들 필요도 없다.
A,B,C의 경우는 명령어 감사 기능이 제한적이거나 제공되지 않는다.

◆ | **Q#0066.** | **Ref#0066.**
AWS Organizations를 사용하는 회사에서는 개발자가 AWS를 실험할 수 있습니다. 회사가 배포한 랜딩 존의 일부로 개발자는 회사 이메일 주소를 사용하여 계정을 요청합니다. 회사는 개발자가 비용이 많이 드는 서비스를 출시

하거나 불필요하게 서비스를 실행하지 않도록 하고 싶어합니다. 회사는 AWS 비용을 제한하기 위해 개발자에게 고정된 월별 예산을 제공해야 합니다.

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

> **A.** 고정된 월간 계정 사용 제한을 설정하려면 SCP를 생성하십시오. 개발자 계정에 SCP를 적용합니다.
> **B.** AWS 예산을 사용하여 계정 생성 프로세스의 일부로 각 개발자 계정에 대한 고정 월 예산을 생성합니다.
> **C.** 비용이 많이 드는 서비스 및 구성 요소에 대한 액세스를 거부하는 SCP를 만듭니다. 개발자 계정에 SCP를 적용합니다.
> **D.** 비용이 많이 드는 서비스 및 구성 요소에 대한 액세스를 거부하는 IAM 정책을 만듭니다. 개발자 계정에 IAM 정책을 적용합니다.
> **E.** 예산 금액에 도달하면 서비스를 종료하는 AWS 예산 알림 작업을 생성합니다. 모든 서비스를 종료하는 작업을 구성합니다.
> **F.** 예산 금액에 도달하면 Amazon Simple 알림 서비스(Amazon SNS) 알림을 보내는 AWS 예산 알림 작업을 생성합니다. AWS Lambda 함수를 호출하여 모든 서비스를 종료합니다.
>
> 해설
> 정답: BCF
> AWS Budget을 통해 계정의 월별 비용 모니터링 몇 Instance연계가 가능하다. 추가적으로 SCP를 통해 특정 고가 서비스 제한으로 비용통제가 가능해진다.
> Lambda함수를 통해 필요없는 서비스를 종료할 수 있습니다.
>
> A의 경우는 SCP는 비용 단위가 아니라, 정책 단위이므로, 부적절하다.
> D의 경우 SCP보다 더 공수가 많다고 이야기 한다.(여러 사람들이)

◆ | **Q#0067.** | **Ref#0067.**
회사에는 Source라는 AWS 계정에 애플리케이션이 있습니다. 계정이 AWS Organizations의 조직에 있습니다. 애플리케이션 중 하나는 AWS Lambda 함수를 사용하고 Amazon Aurora 데이터베이스에 인벤토리 데이터를 저장합니다. 애플리케이션은 배포 패키지를 사용하여 Lambda 함수를 배포합니다. 회사는 Aurora에 대한 자동 백업을 구성했습니다.

회사는 Lambda 함수와 Aurora 데이터베이스를 Target이라는 새 AWS 계정으로 마이그레이션하려고 합니다. 애플리케이션은 중요한 데이터를 처리하므로 회사는 가동 중지 시간을 최소화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 소스 계정에서 Lambda 함수 배포 패키지를 다운로드합니다. 배포 패키지를 사용하고 Target 계정에서 새 Lambda 함수를 생성합니다. 자동화된 Aurora DB 클러스터 스냅샷을 Target 계정과 공유합니다.
> **B.** 소스 계정에서 Lambda 함수 배포 패키지를 다운로드합니다. 배포 패키지를 사용하고 Target 계정에서 새 Lambda 함수를 생성합니다. AWS Resource Access Manager (AWS RAM)을 사용하여 Aurora DB 클러스터를 대상 계정과 공유합니다. Aurora DB 클러스터를 복제할 수 있는 대상 계정 권한을 부여합니다.
> **C.** AWS Resource Access Manager(AWS RAM)를 사용하여 Lambda 함수와 Aurora DB 클러스터를 Target 계정과 공유합니다. Aurora DB 클러스터를 복제할 수 있는 대상 계정 권한을 부여합니다.
> **D.** AWS Resource Access Manager(AWS RAM)를 사용하여 Lambda 기능을 Target 계정과 공유합니다. 자동화된 Aurora DB 클러스터 스냅샷을 Target 계정과 공유합니다.
>
> 해설
> 정답: B
> RAM은 Lambda 기능을 Share할 수 없다. (C,D Out)

A와 B의 차이는 RAM인데 RAM은 계정 간 DB Cluster를 공유할 수 있으므로 A보다 더 빠르다. 따라서 B가 정답이다.

◆ | **Q#0068.** | **Ref#0068.**
회사는 Amazon EC2 인스턴스에서 Python 스크립트를 실행하여 데이터를 처리합니다. 스크립트는 10분마다 실행됩니다. 스크립트는 Amazon S3 버킷에서 파일을 수집하고 파일을 처리합니다. 평균적으로 스크립트는 각 파일을 처리하는 데 약 5분 정도 걸립니다. 스크립트는 스크립트가 이미 처리한 파일을 다시 처리하지 않습니다.

회사는 Amazon CloudWatch 지표를 검토한 결과 파일 처리 속도로 인해 EC2 인스턴스가 약 40%의 시간 동안 유휴 상태임을 확인했습니다. 회사는 워크로드의 가용성과 확장성을 높이려고 합니다. 또한 회사는 장기적인 관리 오버헤드를 줄이고 싶어합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 데이터 처리 스크립트를 AWS Lambda 함수로 마이그레이션합니다. 회사가 객체를 업로드할 때 S3 이벤트 알림을 사용하여 Lambda 함수를 호출하여 객체를 처리합니다.
B. Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. SQS 대기열에 이벤트 알림을 보내도록 Amazon S3를 구성합니다. 최소 1개의 인스턴스 크기로 EC2 Auto Scaling 그룹을 생성합니다. SQS 대기열을 폴링하도록 데이터 처리 스크립트를 업데이트합니다. SQS 메시지가 식별하는 S3 객체를 처리합니다.
C. 데이터 처리 스크립트를 컨테이너 이미지로 마이그레이션합니다. EC2 인스턴스에서 데이터 처리 컨테이너를 실행합니다. 새 객체에 대해 S3 버킷을 폴링하고 결과 객체를 처리하도록 컨테이너를 구성합니다.
D. 데이터 처리 스크립트를 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS)에서 실행되는 컨테이너 이미지로 마이그레이션합니다. 컨테이너가 파일을 처리할 때 Fargate RunTaskAPI 작업을 호출하는 AWS Lambda 함수를 생성합니다. S3 이벤트 알림을 사용하여 Lambda 함수를 호출합니다.

해설
정답: A
Lambda를 활용하여 서버리스로 관리 소요를 줄이고, 15분이 최대 timeout이므로 5분은 Timeout문제 없이 수행될 수 있으며,
컨테이너화 하여 Fargate를 사용하는 것보다 비용 효율적이다.

◆ | **Q#0069.** | **Ref#0069.**
북미의 한 금융 서비스 회사는 AWS 고객에게 새로운 온라인 웹 애플리케이션을 출시할 계획입니다. 회사는 Amazon EC2 인스턴스의 us-east-1 지역에서 애플리케이션을 시작할 예정입니다. 애플리케이션은 가용성이 높아야 하며 사용자 트래픽에 맞게 동적으로 확장되어야 합니다. 또한 회사는 활성-수동 장애 조치를 사용하여 us-west-1 지역의 애플리케이션에 대한 재해 복구 환경을 구현하려고 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. us-east-1에 VPC를 생성하고 us-west-1에 VPC를 생성합니다. VPC 피어링을 구성합니다. us-east-1 VPC에서 두 VPC 모두의 여러 가용 영역으로 확장되는 ALB(Application Load Balancer)를 생성합니다. 두 VPC의 여러 가용 영역에 걸쳐 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. ALB 뒤에 Auto Scaling 그룹을 배치합니다.
B. us-east-1에 VPC를 생성하고 us-west-1에 VPC를 생성합니다. us-east-1 VPC에서 해당 VPC의 여러 가용 영역으로 확장되는 ALB(Application Load Balancer)를 생성합니다. us-east-1 VPC의 여러 가용 영역에 걸쳐 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. us-west-1 VPC에서 동일한 구성으로 ALSet 뒤에 Auto Scaling 그룹을 배치합니다. Amazon Route 53 호스팅 영역을 생성합니다. 각 ALEnable 상태 확인에 대해 별도의 레코드를 생성하여 리전 간 고가용성을 보장합니다.
C. us-east-1에 VPC를 생성하고 us-west-1에 VPC를 생성합니다. us-east-1 VPC에서 해당 VPC의 여러 가용 영역에 걸쳐 확장되는 ALB(Application Load Balancer)를 생성합니다. us-east-1 VPP의 여러 가용 영역에 걸쳐 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. ALB 뒤의 스케일링 그

룹. us-west-1 VPC에서 동일한 구성을 설정하고 Amazon Route 53 호스팅 영역을 생성합니다. 각 ALB에 대해 별도의 레코드를 생성합니다. 상태 확인을 활성화하고 각 레코드에 대한 장애 조치 라우팅 정책을 구성합니다.
D. us-east-1에 VPC를 생성하고 us-west-1에 VPC를 생성합니다. VPC 피어링을 구성합니다. us-east-1 VPC에서 두 VPC 모두의 여러 가용 영역으로 확장되는 ALB(Application Load Balancer)를 생성합니다. 두 VPC의 여러 가용 영역에 걸쳐 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. ALB 뒤에 Auto Scaling 그룹을 배치합니다. Amazon Route 53 호스팅 영역을 생성합니다. ALB에 대한 레코드를 만듭니다.

해설
정답: C
이 문제는 고가용성과 장애 복구를 제공하기 위해 두 개의 AWS 리전(us-east-1과 us-west-1)에 걸친 애플리케이션 배포를 설계하는 것입니다.
각 리전에서 애플리케이션을 운영하며, 하나의 리전이 장애가 발생할 경우 다른 리전으로 자동으로 장애 조치가 이뤄져야 합니다.

VPC와 ALB 생성: 각 리전(us-east-1, us-west-1)에 VPC와 ALB를 생성하고, 여러 가용 영역에 걸쳐 EC2 인스턴스를 배포합니다.
Route 53 설정: Route 53을 사용해 각 리전의 ALB에 대해 DNS 레코드를 만들고, 상태 확인과 장애 조치 라우팅을 설정합니다.
이 설정은 고가용성을 유지하면서 리전 간 장애가 발생할 경우 자동으로 트래픽을 다른 리전으로 전환할 수 있는 최적의 솔루션을 제공합니다.

◆ | **Q#0070.** | **Ref#0070.**
회사에는 단일 AWS 계정이 있는 환경이 있습니다. 솔루션 아키텍트는 AWS Management Console에 대한 액세스 측면에서 회사가 구체적으로 개선할 수 있는 사항을 권장하기 위해 환경을 검토하고 있습니다. 회사의 IT 지원 작업자는 현재 관리 작업을 위해 콘솔에 액세스하여 해당 직무에 매핑된 명명된 IAM 사용자를 인증합니다.

IT 지원 작업자는 더 이상 Active Directory와 IAM 사용자 계정을 모두 유지하기를 원하지 않습니다. 그들은 기존 Active Directory 자격 증명을 사용하여 콘솔에 액세스할 수 있기를 원합니다. 솔루션 아키텍트는 AWS IAM Identity Center(AWS Single Sign-On)를 사용하여 이 기능을 구현합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. AWS Organizations에서 조직을 생성합니다. 조직에서 IAM ID 센터 기능을 활성화합니다. 회사의 온프레미스 Active Directory에 대한 양방향 신뢰를 사용하여 Microsoft Active Directory용 AWS 디렉터리 서비스(AWS Managed Microsoft AD)에서 디렉터리를 생성하고 구성합니다. IAM 자격 증명 센터를 구성하고 AWS Managed Microsoft AD 디렉터리를 자격 증명 소스로 설정합니다. 권한 세트를 생성하고 이를 AWS Managed Microsoft AD 디렉터리 내의 기존 그룹에 매핑합니다.
B. AWS Organizations에서 조직을 생성합니다. 조직에서 IAM ID 센터 기능을 활성화합니다. 회사의 온프레미스 Active Directory에 연결하기 위한 AD 커넥터를 생성하고 구성합니다. IAM ID 센터를 구성하고 AD 커넥터를 ID 소스로 선택합니다. 권한 집합을 만들고 이를 회사 Active Directory 내의 기존 그룹에 매핑합니다.
C. AWS Organizations에서 조직을 생성합니다. 조직의 모든 기능을 활성화합니다. 회사의 온프레미스 Active Directory에 대한 양방향 신뢰를 사용하여 Microsoft Active Directory용 AWS 디렉터리 서비스(AWS Managed Microsoft AD)에서 디렉터리를 생성하고 구성합니다. IAM 자격 증명 센터를 구성하고 AWS Managed Microsoft AD 디렉터리를 자격 증명 소스로 선택합니다. 권한 세트를 생성하고 이를 AWS Managed Microsoft AD 디렉터리 내의 기존 그룹에 매핑합니다.
D. AWS Organizations에서 조직을 생성합니다. 조직의 모든 기능을 활성화합니다. 회사의 온프레미스 Active Directory에 연결하기 위한 AD 커넥터를 생성하고 구성합니다. IAM ID 센터를 구성하고 AD 커넥터를 ID 소스로 설정합니다. 권한 집합을 만들고 이를 회사 Active Directory 내의 기존 그룹에 매핑합니다.

해설
정답: D
AD 커넥터를 활용하는 것이 AWS Managed Microsoft AD를 사용하는 것보다 비용 효율적이다.
AWS IAM Identity Center SSO를 사용하기 위해서는 조직의 모든 기능을 활성화 해야한다.

B is wrong 모든 기능 활성화 필요

071 (신재경) 4회차 完

◆ | **Q#0071.** | **Ref#0071.**
한 비디오 스트리밍 회사는 최근 비디오 공유를 위한 모바일 앱을 출시했습니다. 앱은 us-east-1 리전의 Amazon S3 버킷에 다양한 파일을 업로드합니다. 파일 크기는 1GB에서 10GB까지입니다.

호주에서 앱에 액세스하는 사용자는 업로드에 오랜 시간이 걸리는 경험을 했습니다. 때때로 이러한 사용자에 대한 파일이 완전히 업로드되지 않습니다. 솔루션 설계자는 이러한 업로드에 대한 앱 성능을 개선해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까? (2개를 선택하세요.)

A. S3 버킷에서 S3 Transfer Acceleration을 활성화합니다. 업로드에 Transfer Acceleration 엔드포인트를 사용하도록 앱을 구성합니다.
B. 업로드를 수신하도록 각 지역의 S3 버킷을 구성합니다. S3 교차 리전 복제를 사용하여 파일을 배포 S3 버킷에 복사합니다.
C. 가장 가까운 S3 버킷 리전으로 업로드를 라우팅하도록 지연 시간 기반 라우팅을 사용하여 Amazon Route 53을 설정합니다.
D. 비디오 파일을 청크로 나누도록 앱을 구성합니다. 멀티파트 업로드를 사용하여 파일을 Amazon S3로 전송합니다.
E. 업로드하기 전에 파일에 임의의 접두사를 추가하도록 앱을 수정합니다.

해설
정답: A, D

A: Transfer Accelerator를 사용하는게 업로드에 성능 향상 됨
D: 다중 업로드(멀티)를 이용하여 S3로 전송하는게 성능 개선

◆ | **Q#0072.** | **Ref#0072.**
애플리케이션은 us-east-1 리전에서 MySQL 다중 AZ DB 인스턴스용 Amazon RDS를 사용하고 있습니다. 장애 조치 테스트 후 애플리케이션에서 데이터베이스에 대한 연결이 끊어지고 연결을 다시 설정할 수 없습니다. 애플리케이션을 다시 시작한 후 애플리케이션이 연결을 다시 설정했습니다.

솔루션 설계자는 애플리케이션을 다시 시작할 필요 없이 데이터베이스에 대한 연결을 다시 설정할 수 있도록 솔루션을 구현해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon Aurora MySQL Serverless v1 DB 인스턴스를 생성하십시오. RDS DB 인스턴스를 Aurora Serverless v1 DB 인스턴스로 마이그레이션합니다. Aurora 리더 엔드포인트를 가리키도록 애플리케이션의 연결 설정을 업데이트합니다.
B. RDS 프록시를 생성합니다. 기존 RDS 엔드포인트를 대상으로 구성합니다. RDS 프록시 엔드포인트를 가리키도록 애플리케이션의 연결 설정을 업데이트합니다.
C. 2노드 Amazon Aurora MySQL DB 클러스터를 생성합니다. RDS DB 인스턴스를 Aurora DB 클러스터로 마이그레이션합니다. RDS 프록시를 생성합니다. 기존 RDS 엔드포인트를 대상으로 구성합니다. RDS 프록시 엔드포인트를 가리키도록 애플리케이션의 연결 설정을 업데이트합니다.
D. Amazon S3 버킷을 생성합니다. AWS Database Migration Service(AWS DMS)를 사용하여 데이터

베이스를 Amazon S3로 내보냅니다. S3 버킷을 데이터 스토어로 사용하도록 Amazon Athena를 구성합니다. 애플리케이션에 대한 최신 ODBC(Open Database Connectivity) 드라이버를 설치하십시오. Athena 엔드포인트를 가리키도록 애플리케이션의 연결 설정을 업데이트합니다.

해설
정답: B

RDS 프록시는 풀링 연결 외에도 대기 인스턴스에 자동으로 연결하여 데이터베이스 오류에 대한 애플리케이션의 복원력 상승

◆ | **Q#0073.** | **Ref#0073.**
한 회사가 AWS 클라우드에 솔루션을 구축하고 있습니다. 수천 대의 장치가 솔루션에 연결되어 데이터를 보냅니다. 각 장치는 MQTT 프로토콜을 통해 실시간으로 데이터를 보내고 받을 수 있어야 합니다. 각 장치는 고유한 X.509 인증서를 사용하여 인증해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS IoT Core를 설정합니다. 각 디바이스에 대해 해당 Amazon MQ 대기열을 생성하고 인증서를 프로비저닝합니다. 각 디바이스를 Amazon MQ에 연결합니다.
B. NLB(Network Load Balancer)를 생성하고 AWS Lambda 권한 부여자로 구성합니다. Auto Scaling 그룹의 Amazon EC2 인스턴스에서 MQTT 브로커를 실행합니다. Auto Scaling 그룹을 NLConnect 각 디바이스의 대상으로 NLB로 설정합니다.
C. AWS IoT Core를 설정합니다. 각 디바이스에 대해 해당 AWS IoT 사물을 생성하고 인증서를 프로비저닝합니다. 각 장치를 AWS IoT Core에 연결합니다.
D. Amazon API Gateway HTTP API 및 NLB(Network Load Balancer)를 설정합니다. API 게이트웨이와 NLB 간의 통합을 만듭니다. HTTP API에 상호 TLS 인증서 권한 부여자를 구성합니다. NLB가 대상으로 하는 Amazon EC2 인스턴스에서 MQTT 브로커를 실행합니다. 각 장치를 NLB에 연결합니다.

해설
정답: C

AWS IoT Core 설정. 각 디바이스에 대해 해당 AWS IoT 사물을 생성하고 인증서를 프로비저닝합니다. 각 장치를 AWS IoT Core에 연결합니다. AWS IoT Core는 인터넷에 연결된 장치와 AWS 클라우드 간의 안전한 양방향 통신을 지원하는 완전관리형 서비스입니다. MQTT 프로토콜을 지원하며 내장된 장치 인증 및 액세스 제어를 포함합니다. 회사는 AWS IoT Core를 사용하여 각 디바이스에 대한 X.509 인증서를 쉽게 프로비저닝 및 관리하고, 운영 오버헤드를 최소화하면서 디바이스를 서비스에 연결할 수 있습니다.

◆ | **Q#0074.** | **Ref#0074.**
회사는 단일 AWS 계정에서 여러 워크로드를 실행하고 있습니다. 새로운 회사 정책에는 엔지니어가 승인된 리소스만 프로비저닝할 수 있으며 엔지니어가 이러한 리소스를 프로비저닝하려면 AWS CloudFormation을 사용해야 한다고 명시되어 있습니다. 솔루션 아키텍트는 엔지니어가 액세스에 사용하는 IAM 역할에 새로운 제한을 적용하는 솔루션을 생성해야 합니다.

솔루션 설계자는 솔루션을 만들기 위해 무엇을 해야 합니까?

A. 승인된 리소스가 포함된 AWS CloudFormation 템플릿을 Amazon S3 버킷에 업로드합니다. Amazon S3 및 AWS CloudFormation에 대한 액세스만 허용하도록 엔지니어의 IAM 역할에 대한 IAM 정책을 업데이트합니다. AWS CloudFormation 템플릿을 사용하여 리소스를 프로비저닝합니다.
B. 승인된 리소스 및 AWS CloudFormation의 프로비저닝만 허용하는 권한으로 엔지니어의 IAM 역할에 대한 IAM 정책을 업데이트합니다. AWS CloudFormation 템플릿을 사용하여 승인된 리소스로 스택을 생성합니다.

C. AWS CloudFormation 작업만 허용하는 권한으로 엔지니어의 IAM 역할에 대한 IAM 정책을 업데이트합니다. 승인된 리소스를 프로비저닝할 수 있는 권한이 있는 새 IAM 정책을 생성하고 해당 정책을 새 IAM 서비스 역할에 할당합니다. 스택 생성 중에 AWS CloudFormation에 IAM 서비스 역할을 할당합니다.
D. AWS CloudFormation 스택에 리소스를 프로비저닝합니다. 엔지니어의 IAM 역할에 대한 IAM 정책을 업데이트하여 자신의 AWS CloudFormation 스택에 대한 액세스만 허용합니다.

해설
정답: C

AWS CloudFormation과 관련된 작업만 허용하도록 엔지니어의 IAM 역할을 업데이트하여 CloudFormation 외부에서 AWS 리소스를 직접 프로비저닝하거나 수정하는 것을 효과적으로 방지하는 작업이 포함됩니다. 템플릿을 실행할 때 CloudFormation이 가정하는 서비스 역할(승인된 리소스를 프로비저닝할 수 있는 권한 포함)을 생성하면 CloudFormation을 통해 승인된 리소스만 프로비저닝하도록 적용

◆ | **Q#0075.** | **Ref#0075.**
솔루션 설계자는 회사에서 곧 출시할 새 애플리케이션을 위한 데이터 저장 및 검색 아키텍처를 설계하고 있습니다. 이 애플리케이션은 전 세계 장치에서 분당 수백만 개의 작은 레코드를 수집하도록 설계되었습니다. 각 레코드의 크기는 4KB 미만이며 짧은 대기 시간으로 검색할 수 있는 내구성 있는 위치에 저장되어야 합니다. 데이터는 일시적이며 회사는 120일 동안만 데이터를 저장해야 하며 그 이후에는 데이터가 삭제될 수 있습니다.

솔루션 설계자는 1년 동안 스토리지 요구 사항이 약 10~15TB가 될 것으로 계산합니다.

가장 비용 효율적이고 설계 요구 사항을 충족하는 스토리지 전략은 무엇입니까?

A. 인덱싱된 검색을 허용하기 위해 각 수신 레코드를 Amazon S3 버킷에 단일 .csv 파일로 저장하도록 애플리케이션을 설계합니다. 120일이 지난 데이터를 삭제하도록 수명 주기 정책을 구성합니다.
B. 규모에 맞게 적절하게 구성된 Amazon DynamoDB 테이블에 각 수신 레코드를 저장하도록 애플리케이션을 설계합니다. 120일보다 오래된 레코드를 삭제하도록 DynamoDB TTL(Time to Live) 기능을 구성합니다.
C. 각 수신 레코드를 Amazon RDS MySQL 데이터베이스의 단일 테이블에 저장하도록 애플리케이션을 설계합니다. 120일보다 오래된 레코드를 삭제하는 쿼리를 실행하는 야간 크론 작업을 실행합니다.
D. 수신 레코드를 Amazon S3 버킷에 쓰기 전에 일괄 처리하도록 애플리케이션을 설계합니다. 배치의 레코드 목록을 포함하도록 객체의 메타데이터를 업데이트하고 Amazon S3 메타데이터 검색 기능을 사용하여 데이터를 검색합니다. 120일 후에 데이터를 삭제하도록 수명 주기 정책을 구성합니다.

해설
정답: B

Amazon DynamoDB는 높은 처리량과 낮은 지연 시간을 제공하며, Time to Live(TTL) 기능을 사용하여 120일이 지난 데이터를 자동으로 삭제할 수 있습니다. 이는 대규모 데이터 수집 요구 사항에 적합하고 비용 효율적입니다.

◆ | **Q#0076.** | **Ref#0076.**
한 소매 회사가 여러 AWS 리전에 걸쳐 AWS에서 전자 상거래 웹 사이트를 호스팅하고 있습니다. 회사는 온라인 구매를 위해 웹사이트가 항상 운영되기를 원합니다. 웹 사이트는 MySQL DB 인스턴스용 Amazon RDS에 데이터를 저장합니다.

어떤 솔루션이 데이터베이스에 가장 높은 가용성을 제공합니까?

A. Amazon RDS에서 자동 백업을 구성합니다. 중단이 발생하는 경우 자동 백업을 독립형 DB 인스턴스로 승격하세요. 승격된 DB 인스턴스로 데이터베이스 트래픽을 전달합니다. 승격된 DB 인스턴스를 소스로 포함하는 대체 읽기 전용 복제본을 생성합니다.
B. Amazon RDS에서 글로벌 테이블과 읽기 전용 복제본을 구성합니다. 지역 간 범위를 활성화합니다. 중단이 발생하는 경우 AWS Lambda를 사용하여 한 지역에서 다른 지역으로 읽기 전용 복제본을 복사하세요.
C. Amazon RDS에서 글로벌 테이블과 자동 백업을 구성합니다. 중단이 발생하는 경우 AWS Lambda를 사용하여 한 지역에서 다른 지역으로 읽기 전용 복제본을 복사하세요.
D. Amazon RDS에서 읽기 전용 복제본을 구성합니다. 중단이 발생하는 경우 교차 리전 및 읽기 전용 복제본을 독립형 DB 인스턴스로 승격하세요. 승격된 DB 인스턴스로 데이터베이스 트래픽을 전달합니다. 승격된 DB 인스턴스를 소스로 포함하는 대체 읽기 전용 복제본을 생성합니다.

해설
정답: D
Amazon RDS에서 읽기 복제본을 사용하여 교차 리전 복제를 구성하고, 장애 발생 시 교차 리전 읽기 복제본을 독립형 DB 인스턴스로 승격시키는 방법이 가장 높은 가용성을 제공합니다. 이를 통해 데이터베이스가 항상 이용 가능하도록 보장할 수 있습니다.

◆ | **Q#0077.** | **Ref#0077.**
example Corp.에는 온프레미스 데이터 센터가 있고, example Corp. AWS 계정에 VPC A라는 이름의 VPC가 있습니다. 온프레미스 네트워크는 AWS Site-To-Site VPN을 통해 VPC A에 연결됩니다. 온프레미스 서버는 VPC A에 올바르게 액세스할 수 있습니다. 예시 회사는 방금 VPC B라는 VPC가 있는 AnyCompany를 인수했습니다. 이러한 네트워크 간에는 IP 주소가 중복되지 않습니다. example Corp.는 VPC A와 VPC B를 피어링했습니다.

example Corp.는 온프레미스 서버에서 VPC B로 연결하려고 합니다. example Corp.는 네트워크 ACL과 보안 그룹을 올바르게 설정했습니다.

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

A. 전송 게이트웨이를 생성합니다. Site-to-Site VPN, VPC A 및 VPC B를 전송 게이트웨이에 연결합니다. 모든 네트워크의 전송 게이트웨이 라우팅 테이블을 업데이트하여 다른 모든 네트워크에 대한 IP 범위 경로를 추가합니다.
B. 전송 게이트웨이를 생성합니다. 온프레미스 네트워크와 VPC B 사이에 Site-to-Site VPN 연결을 생성하고 VPN 연결을 Transit Gateway에 연결합니다. 피어링된 VPC로 트래픽을 전달하는 경로를 추가하고, 클라이언트에게 VPC A와 B에 대한 액세스 권한을 부여하는 권한 부여 규칙을 추가합니다.
C. 세 네트워크 모두에 대해 Site-to-Site VPN과 두 VPC의 라우팅 테이블을 업데이트합니다. 세 네트워크 모두에 대해 BGP 전파를 구성합니다. BGP 전파가 완료될 때까지 최대 5분 동안 기다립니다.
D. VPC A와 VPC B를 포함하도록 Site-to-Site VPN의 가상 프라이빗 게이트웨이 정의를 수정합니다. 두 VPC 간에 가상 프라이빗 게이트웨이의 두 라우터를 분할합니다.

해설
정답: A

전송 게이트웨이를 생성하고 Site-to-Site VPN, VPC A 및 VPC B를 전송 게이트웨이에 연결하면 온프레미스 서버가 최소한의 운영 노력으로 VPC B에 액세스할 수 있습니다. VPC와 온프레미스 서버 간의 통신을 활성화하려면 Transit Gateway 라우팅 테이블을 다른 모든 네트워크에 대한 IP 범위 경로로 업데이트해야 합니다.

◆ | **Q#0078.** | **Ref#0078.**
한 회사는 최근 플랫폼 변경 전략을 사용하여 온프레미스 데이터 센터에서 AWS 클라우드로의 마이그레이션을 완료했습니다. 마이그레이션된 서버 중 하나는 중요한 애플리케이션이 의존하는 기존 SMTP(Simple Mail Transfer Protocol) 서비스를 실행하고 있습니다. 애플리케이션은 회사 고객에게 아웃바운드 이메일 메시지를 보냅니다. 레

거시 SMTP 서버는 TLS 암호화를 지원하지 않으며 TCP 포트 25를 사용합니다. 애플리케이션은 SMTP만 사용할 수 있습니다.

회사는 Amazon Simple Email Service(Amazon SES)를 사용하고 기존 SMTP 서버를 폐기하기로 결정했습니다. 회사는 SES 도메인을 생성하고 검증했습니다. 회사는 SES 제한을 해제했습니다.

Amazon SES에서 이메일 메시지를 보내도록 애플리케이션을 수정하려면 회사는 어떻게 해야 합니까?

> **A.** TLS 래퍼를 사용하여 Amazon SES에 연결하도록 애플리케이션을 구성합니다. ses:SendEmail 및 ses:SendRawEmail 권한이 있는 IAM 역할을 생성합니다. IAM 역할을 Amazon EC2 인스턴스에 연결합니다.
> **B.** STARTTLS를 사용하여 Amazon SES에 연결하도록 애플리케이션을 구성합니다. Amazon SES SMTP 자격 증명을 얻습니다. 자격 증명을 사용하여 Amazon SES에 인증합니다.
> **C.** SES API를 사용하여 이메일 메시지를 보내도록 애플리케이션을 구성합니다. ses:SendEmail 및 ses:SendRawEmail 권한이 있는 IAM 역할을 생성합니다. IAM 역할을 Amazon SES의 서비스 역할로 사용합니다.
> **D.** AWS SDK를 사용하여 이메일 메시지를 보내도록 애플리케이션을 구성합니다. Amazon SES용 IAM 사용자를 생성합니다. API 액세스 키를 생성합니다. 액세스 키를 사용하여 Amazon SES에 인증합니다.
>
> 해설
> 정답: B
>
> STARTTLS 연결을 설정하기 위해 SMTP 클라이언트는 포트 25, 587 또는 2587에서 Amazon SES SMTP 엔드포인트에 연결하고 EHLO 명령을 실행한 다음 서버가 STARTTLS SMTP 확장을 지원한다고 발표할 때까지 기다립니다. 그런 다음 클라이언트는 STARTTLS 명령을 실행하여 TLS 협상을 시작합니다. 협상이 완료되면 클라이언트는 암호화된 새 연결을 통해 EHLO 명령을 실행하고 SMTP 세션은 정상적으로 진행됩니다. TLS 래퍼 연결을 설정하기 위해 SMTP 클라이언트는 포트 465 또는 2465에서 Amazon SES SMTP 엔드포인트에 연결합니다. 서버는 해당 인증서가 있으면 클라이언트는 EHLO 명령을 발행하고 SMTP 세션은 정상적으로 진행됩니다.

◆ | **Q#0079.** | **Ref#0079.**
한 회사가 최근 다른 여러 회사를 인수했습니다. 각 회사에는 청구 및 보고 방법이 다른 별도의 AWS 계정이 있습니다. 인수 회사는 모든 계정을 AWS Organizations의 하나의 조직으로 통합했습니다. 그러나 인수 회사는 모든 팀에 의미 있는 그룹이 포함된 비용 보고서를 생성하는 데 어려움을 겪었습니다.

인수 회사의 재무팀에는 자체 관리 애플리케이션을 통해 모든 회사의 비용을 보고할 수 있는 솔루션이 필요합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 조직에 대한 AWS 비용 및 사용 보고서를 생성합니다. 보고서에서 태그와 비용 범주를 정의합니다. Amazon Athena에서 테이블을 생성합니다. Athena 테이블을 기반으로 Amazon QuickSight 데이터세트를 생성합니다. 데이터세트를 재무팀과 공유하세요.
> **B.** 조직에 대한 AWS 비용 및 사용 보고서를 생성합니다. 보고서에서 태그와 비용 범주를 정의합니다. 재무 부서에서 보고서를 작성하는 데 사용할 특수 템플릿을 AWS Cost Explorer에서 생성합니다.
> **C.** AWS Price List Query API로부터 지출 정보를 수신하는 Amazon QuickSight 데이터세트를 생성합니다. 데이터세트를 재무팀과 공유하세요.
> **D.** AWS Price List Query API를 사용하여 계정 지출 정보를 수집합니다. 재무 부서에서 보고서를 작성하는 데 사용할 특수 템플릿을 AWS Cost Explorer에서 생성합니다.
>
> 해설
> 정답: A

조직에 대한 AWS 비용 및 사용 보고서를 생성하고 보고서에서 태그와 비용 범주를 정의하면 하나의 조직으로 통합된 여러 회사에 대한 자세한 비용 보고가 가능합니다.
Amazon Athena에 테이블을 생성하고 Athena 테이블을 기반으로 하는 Amazon QuickSight 데이터 세트를 생성하면 재무팀에서 모든 회사의 비용에 대한 보고서를 쉽게 쿼리하고 생성할 수 있습니다. 그런 다음 재무팀이 보고 요구 사항에 사용할 수 있도록 데이터세트를 재무팀과 공유할 수 있습니다.
B(x): 모든 회사의 비용에 대한 보고서를 쿼리하고 생성하는 방법을 제공하지 않으므로 올바르지 않습니다.
C(x): AWS Price List Query API의 지출 정보만 제공하고 다른 회사에 대한 자세한 비용 보고를 제공하지 않기 때문에 올바르지 않습니다.
D(x): AWS Price List Query API만 사용하고 모든 회사의 비용에 대한 보고서를 쿼리하고 생성하는 방법을 제공하지 않기 때문에 올바르지 않습니다.

◆ | **Q#0080.** | **Ref#0080.**
한 회사가 AWS에서 IoT 플랫폼을 운영하고 있습니다. 다양한 위치에 있는 IoT 센서는 Application Load Balancer 뒤에서 실행되는 Amazon EC2 인스턴스에 있는 회사의 Node.js API 서버로 데이터를 보냅니다. 데이터는 4TB 범용 SSD 볼륨을 사용하는 Amazon RDS MySQL DB 인스턴스에 저장됩니다.

회사가 현장에 배치한 센서의 수는 시간이 지남에 따라 증가했으며 크게 증가할 것으로 예상됩니다. API 서버는 지속적으로 과부하되고 RDS 측정항목은 높은 쓰기 대기 시간을 나타냅니다.

다음 중 이 플랫폼을 비용 효율적으로 유지하면서 문제를 영구적으로 해결하고 새로운 센서가 프로비저닝됨에 따라 성장을 가능하게 하는 단계는 무엇입니까? (2개를 선택하세요.)

A. 볼륨의 IOPS를 향상시키려면 MySQL 범용 SSD 스토리지의 크기를 6TB로 조정하십시오.
B. RDS MySQL DB 인스턴스 대신 Amazon Aurora를 사용하도록 데이터베이스 계층을 재설계하고 읽기 전용 복제본을 추가합니다.
C. Amazon Kinesis Data Streams 및 AWS Lambda를 활용하여 원시 데이터를 수집하고 처리합니다.
D. AWS X-Ray를 사용하여 애플리케이션 문제를 분석 및 디버깅하고 로드에 맞게 더 많은 API 서버를 추가합니다.
E. RDS MySQL DB 인스턴스 대신 Amazon DynamoDB를 사용하도록 데이터베이스 계층을 재설계합니다.

해설
정답: C, E

C: Amazon Kinesis Data Streams 및 AWS Lambda를 활용하여 원시 데이터를 수집하고 처리하면 API 서버가 지속적으로 과부하되는 문제를 해결하는 데 도움이 됩니다. Kinesis를 사용하면 데이터가 실시간으로 수집 및 처리되므로 API 서버가 증가된 로드를 처리할 수 있습니다. Lambda를 사용하여 데이터를 처리하면 플랫폼의 전반적인 성능과 확장성을 개선하는 데도 도움이 될 수 있습니다.
E:RDS MySQL DB 인스턴스 대신 Amazon DynamoDB를 사용하도록 데이터베이스 계층을 재설계하면 쓰기 지연 시간이 긴 문제를 해결하는 데 도움이 됩니다. DynamoDB는 고성능과 확장성을 위해 설계된 NoSQL 데이터베이스이므로 이 사용 사례에 매우 적합

081 (박지형) 4회차 完

◆ | **Q#0081.** | **Ref#0081.**
한 회사에서 사용자가 문서를 업로드하는 전자 문서 관리 시스템을 구축하고 있습니다. 애플리케이션 스택은 완전히 서버리스이며 eu-central-1 지역의 AWS에서 실행됩니다. 시스템에는 Amazon S3를 원본으로하여 제공하기 위해 Amazon CloudFront 배포를 사용하는 웹 애플리케이션이 포함되어 있습니다. 웹 애플리케이션은 Amazon API Gateway 지역 엔드포인트와 통신합니다. API Gateway API는 Amazon Aurora Serverless 데이터베이스에 메타데이터를 저장하고 문서를 S3 버킷에 저장하는 AWS Lambda 함수를 호출합니다.

회사는 꾸준히 성장하고 있으며 최대 고객과의 개념 증명을 완료했습니다. 회사는 유럽 이외의 지역에서 대기 시간을 개선해야 합니다.

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

> **A.** S3 버킷에서 S3 Transfer Acceleration을 활성화합니다. 웹 애플리케이션이 Transfer Acceleration 서명된 URL을 사용하는지 확인하십시오.
> **B.** AWS Global Accelerator에서 액셀러레이터를 생성합니다. CloudFront 배포판에 액셀러레이터를 연결합니다.
> **C.** API Gateway 지역 엔드포인트를 엣지 최적화 엔드포인트로 변경합니다.
> **D.** 전 세계에 분산된 다른 두 위치에 전체 스택을 프로비저닝합니다. Aurora Serverless 클러스터에서 글로벌 데이터베이스를 사용합니다.
> **E.** Lambda 함수와 Aurora Serverless 데이터베이스 사이에 Amazon RDS 프록시를 추가합니다.
>
> 해설
> 정답: A, C
> 이 질문은 AWS에서 제공하는 서버리스 애플리케이션의 성능을 향상 시키는 방법에 대한 것입니다.
> A. S3 Transfer Acceleration을 활성화하면 사용자가 문서를 업로드할 때 S3 버킷까지의 전송 속도를 향상시킵니다. 이는 유럽 외의 사용자들의 대기 시간을 줄일 수 있습니다.
> C. API Gateway의 지역 엔드포인트를 엣지 최적화 엔드포인트로 변경하면 API Gateway의 응답을 사용자에게 더 가까운 위치에 캐싱함으로써 대기 시간을 개선할 수 있습니다.

◆ | **Q#0082.** | **Ref#0082.**
모험 회사가 모바일 앱에 새로운 기능을 출시했습니다. 사용자는 이 기능을 사용하여 언제든지 하이킹 및 래프팅 사진과 비디오를 업로드할 수 있습니다. 사진과 비디오는 S3 버킷의 Amazon S3 Standard 스토리지에 저장되며 Amazon CloudFront를 통해 제공됩니다.

회사는 스토리지 비용을 최적화해야 합니다. 솔루션 설계자는 업로드된 사진과 비디오의 대부분이 30일 이후에 자주 액세스되지 않는다는 사실을 발견했습니다. 하지만 업로드된 사진과 동영상 중 일부는 30일 이후에도 자주 액세스됩니다. 솔루션 설계자는 가능한 최저 비용으로 사진과 비디오의 검색 가용성을 밀리초 단위로 유지하는 솔루션을 구현해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** S3 버킷에 S3 Intelligent-Tiering을 구성합니다.
> **B.** 30일 후에 이미지 객체와 비디오 객체를 S3 Standard에서 S3 Glacier Deep Archive로 전환하도록 S3 수명 주기 정책을 구성합니다.
> **C.** Amazon S3를 Amazon EC2 인스턴스에 탑재된 Amazon Elastic File System(Amazon EFS) 파일 시스템으로 교체합니다.
> **D.** S3 이미지 개체 및 S3 비디오 개체에 Cache-Control: max-age 헤더를 추가합니다. 헤더를 30일로 설정합니다.
>
> 해설
> 정답: A
> S3 Intelligent-Tiering은 일부 파일이 자주 접근되고, 일부는 거의 사용되지 않는 시나리오에 최적화되어 있습니다.
> 이 서비스는 자동으로 객체를 액세스 패턴에 따라 다른 계층으로 이동시킵니다. 이로써 빈번하게 접근되지 않는 객체에 대해서는 저장 비용을 줄일 수 있고, 그럼에도 불구하고 필요할 때는 항상 객체를 검색할 수 있습니다.

◆ | **Q#0083.** | **Ref#0083.**
한 회사는 Amazon S3를 사용하여 다양한 스토리지 클래스에 파일과 이미지를 저장합니다. 회사의 S3 비용은 지난 한 해 동안 크게 증가했습니다.

솔루션 설계자는 지난 12개월 동안의 데이터 추세를 검토하고 개체에 적합한 스토리지 클래스를 식별해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 지난 12개월간 S3 사용에 대한 AWS 비용 및 사용 보고서를 다운로드하세요. 비용 절감을 위한 AWS Trusted Advisor 권장 사항을 검토하십시오.
> **B.** S3 스토리지 클래스 분석을 사용하십시오. 데이터 추세를 Amazon QuickSight 대시보드로 가져와 스토리지 추세를 분석합니다.
> **C.** Amazon S3 스토리지 렌즈를 사용하십시오. 스토리지 추세에 대한 고급 측정항목을 포함하도록 기본 대시보드를 업그레이드하세요.
> **D.** S3용 액세스 분석기를 사용합니다. 지난 12개월 동안의 S3용 액세스 분석기 보고서를 다운로드하세요. .csv 파일을 Amazon QuickSight 대시보드로 가져옵니다.
>
> 해설
> 정답: C
> Amazon S3 Storage Lens는 S3 사용에 대한 조직 전체의 통찰력을 제공하는 고객의 클라우드 스토리지 관리를 위한 기본적인 분석 기능입니다.
> 이를 통해 사용자는 사용 패턴과 비용의 트렌드를 확인하고 스토리지를 최적화하는 데 도움이 됩니다. 따라서, 스토리지 사용 트렌드 및 비용을 분석하고 최적화하는데 필요한 요구사항을 충족시킵니다.
> 이와 반면 다른 옵션들은 S3 비용 및 사용량 자체에 관한 분석이나 접근 분석에 초점을 맞추고 있습니다. 이 중에서는 S3 Storage Lens가 비용 및 스토리지 사용 트렌드 분석에 가장 적합합니다.

◆ | **Q#0084.** | **Ref#0084.**
회사는 AWS에 클라우드 인프라를 보유하고 있습니다. 솔루션 설계자는 인프라를 코드로 정의해야 합니다. 인프라는 현재 하나의 AWS 지역에 배포되어 있습니다. 회사의 비즈니스 확장 계획에는 여러 AWS 계정에 걸쳐 여러 지역에 배포하는 것이 포함됩니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** AWS CloudFormation 템플릿을 사용하십시오. IAM 정책을 추가하여 다양한 계정을 제어하고 여러 지역에 템플릿을 배포합니다.
> **B.** AWS 조직을 사용하십시오. 마스터 계정에서 AWS CloudFormation 템플릿 배포 AWS Control Tower를 사용하여 계정 전체의 배포를 관리합니다.
> **C.** AWS Organizations 및 AWS CloudFormation StackSets를 사용하십시오. 필요한 IAM 권한이 있는 계정에서 Cloud Formation 템플릿을 배포합니다.
> **D.** AWS CloudFormation 템플릿과 함께 중첩 스택을 사용합니다. 중첩 스택을 사용하여 지역을 변경합니다.
>
> 해설
> 정답: C
> 여러 AWS 계정과 지역에서 인프라를 배포하려면 AWS CloudFormation StackSets와 AWS Organizations를 함께 사용하는 것이 가장 효과적입니다. AWS CloudFormation StackSets는 한 번에 여러 AWS 계정 및 지역에 걸쳐 AWS CloudFormation을 사용하여 스택을 생성하고 관리하는 기능을 제공합니다.
> 따라서, 이 옵션은 서로 다른 계정과 지역 간에 인프라를 배포하는 요구사항을 충족시킵니다.
> 다른 옵션들에 비해, CloudFormation StackSets와 AWS Organizations 조합이 여러 계정과 지역에서 인프라 배포를 처리하는 과정을 더 단순화할 수 있기 때문에 이 옵션이 가장 적합합니다. AWS Organizations는 AWS 리소스의 정책 기반 관리와 AWS 계정 관리를 단일 AWS 계정에서 가능하게 합니다.
> 다른 옵션들은 다중 계정 및 지역 배포 요구사항을 완벽하게 충족시키지 못합니다. AWS CloudFormation 템플릿만 사용하거나 AWS Control Tower를 사용하거나 중첩 스텍을 사용하는 옵션은 StackSets와 Organizations의 조합만큼 효과적으로 여러 리전과 계정을 관리할 수 없습니다.

◆ | **Q#0085.** | **Ref#0085.**
회사는 AWS에 클라우드 인프라를 보유하고 있습니다. 솔루션 설계자는 인프라를 코드로 정의해야 합니다. 인프라는 현재 하나의 AWS 지역에 배포되어 있습니다. 회사의 비즈니스 확장 계획에는 여러 AWS 계정에 걸쳐 여러 지역에 배포하는 것이 포함됩니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** AWS CloudFormation 템플릿을 사용하십시오. IAM 정책을 추가하여 다양한 계정을 제어하고 여러 지역에 템플릿을 배포합니다.
> **B.** AWS 조직을 사용하십시오. 마스터 계정에서 AWS CloudFormation 템플릿 배포 AWS Control Tower를 사용하여 계정 전체의 배포를 관리합니다.
> **C.** AWS Organizations 및 AWS CloudFormation StackSets를 사용하십시오. 필요한 IAM 권한이 있는 계정에서 Cloud Formation 템플릿을 배포합니다.
> **D.** AWS CloudFormation 템플릿과 함께 중첩 스택을 사용합니다. 중첩 스택을 사용하여 지역을 변경합니다.
>
> 해설
> 정답:C
> 여러 계정과 지역에서 여러 번의 클라우드 인프라를 쉽게 배포하고 관리하려면 AWS Organizations와 AWS CloudFormation StackSets를 함께 사용하는 것이 가장 효율적입니다.
> AWS CloudFormation StackSets은 단일 AWS CloudFormation 템플릿을 사용하여 선택한 여러 AWS 계정과 지역에 걸쳐 스택의 생성, 업데이트 또는 삭제를 자동화할 수 있습니다.
> 이는 효과적으로 여러 계정 및 리전에서 인프라를 일관되게 배포하고 관리할 수 있게 해주므로, 이는 여러 리전과 AWS 계정에서의 배포를 포함하는 비즈니스 확장 계획을 수행하기에 적합한 솔루션이 될 것입니다.

◆ | **Q#0086.** | **Ref#0086.**
한 회사는 모놀리식 애플리케이션을 AWS에 배포된 최신 애플리케이션 디자인으로 리팩터링할 계획입니다. CI/CD 파이프라인은 다음 요구 사항에 따라 애플리케이션에 대한 현대적인 디자인을 지원하도록 업그레이드되어야 합니다.

• 변경 사항이 매시간 여러 번 릴리스될 수 있어야 합니다.
• 변경 사항을 최대한 빨리 롤백할 수 있어야 합니다.

어떤 디자인이 이러한 요구 사항을 충족합니까?

> **A.** 애플리케이션과 해당 구성을 포함하기 위해 AMI를 통합하는 CI/CD 파이프라인을 배포합니다. Amazon EC2 인스턴스를 교체하여 애플리케이션을 배포합니다.
> **B.** 애플리케이션의 CI/CD 파이프라인 배포 대상으로 보조 환경에서 준비할 AWS Elastic Beanstalk를 지정합니다. 배포하려면 스테이징 환경과 프로덕션 환경 URL을 바꾸세요.
> **C.** AWS 시스템 관리자를 사용하여 각 배포에 대한 인프라를 다시 프로비저닝합니다. Amazon EC2 사용자 데이터를 업데이트하여 Amazon S3에서 최신 코드 아티팩트를 가져오고 Amazon Route 53 가중치 라우팅을 사용하여 새 환경을 가리킵니다.
> **D.** 사전 구축된 AMI를 사용하여 Auto Scaling 이벤트의 일부로 애플리케이션 업데이트를 롤아웃합니다. 새 버전의 AMI를 사용하여 인스턴스를 추가하세요. 배포 이벤트 중에 구성된 종료 정책과 함께 이전 AMI 버전을 사용하는 모든 인스턴스를 단계적으로 중단합니다.
>
> 해설
> 정답: B
> Elastic Beanstalk는 AWS에서 제공하는 PaaS(Platform as a Service)로, 개발자가 인프라에 대한 걱정 없이 오직 애플리케이션 개발에만 집중할 수 있게 해주는 서비스입니다.
> 스테이징 환경은 실제 제품 환경에서 실행되는 애플리케이션의 복제본을 가지고 있고, CI/CD 파이프라인의 일부로 사용되어 새로운 코드 변경 사항을 테스트하는 데 사용됩니다.
> Elastic Beanstalk는 '환경 URL 교환' 기능도 제공하는데, 이를 통해 스테이징 환경과 프로덕션 환경

의 URL을 바로 교환할 수 있습니다. 즉, 새롭게 배포 준비가 완료된 스테이징 환경을 실제 사용자에게 노출시키고, 이전 프로덕션 환경은 스테이징 환경으로 전환시킬 수 있습니다.
따라서, 이 방식을 사용하면 하루에 여러 번 소프트웨어 변경 사항을 배포할 수 있으며, 만약 문제가 발생하면 빠르게 이전 환경으로 롤백하는 것도 가능합니다. 이런 이유로 선택지 B가 이 문제에 가장 적합한 해답입니다.

◆ | **Q#0087.** | **Ref#0087.**
회사에 Amazon EC2 인스턴스에서 실행되는 애플리케이션이 있습니다. 솔루션 아키텍트는 애플리케이션이 Amazon Aurora DB 클러스터에 액세스해야 하는 AWS 리전에서 VPC 인프라를 설계하고 있습니다. EC2 인스턴스는 모두 동일한 보안 그룹과 연결되어 있습니다. DB 클러스터는 자체 보안 그룹과 연결되어 있습니다.

솔루션 설계자는 애플리케이션에 DB 클러스터에 대한 최소 권한 액세스를 제공하기 위해 보안 그룹에 규칙을 추가해야 합니다.

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

A. EC2 인스턴스의 보안 그룹에 인바운드 규칙을 추가합니다. DB 클러스터의 보안 그룹을 기본 Aurora 포트를 통한 소스로 지정합니다.
B. EC2 인스턴스의 보안 그룹에 아웃바운드 규칙을 추가합니다. DB 클러스터의 보안 그룹을 기본 Aurora 포트를 통한 대상으로 지정합니다.
C. DB 클러스터의 보안 그룹에 인바운드 규칙을 추가합니다. EC2 인스턴스의 보안 그룹을 기본 Aurora 포트를 통한 소스로 지정합니다.
D. DB 클러스터의 보안 그룹에 아웃바운드 규칙을 추가합니다. EC2 인스턴스의 보안 그룹을 기본 Aurora 포트를 통한 대상으로 지정합니다.
E. DB 클러스터의 보안 그룹에 아웃바운드 규칙을 추가합니다. 임시 포트를 통한 대상으로 EC2 인스턴스의 보안 그룹을 지정합니다.

해설
정답: B,C
EC2 인스턴스는 DB 클러스터에 액세스하는 데 필요하므로 EC2 인스턴스의 보안 그룹에 아웃바운드 규칙을 추가해야 합니다. 그래서 EC2 인스턴스를 대상으로 하여 DB 클러스터의 보안 그룹을 지정하므로 선택지 B가 필요합니다.
DB 클러스터는 EC2 인스턴스로부터 연결을 허용해야 하므로 DB 클러스터의 보안 그룹에 인바운드 규칙을 추가해야 합니다. 따라서 DB 클러스터를 대상으로 하여 EC2 인스턴스의 보안 그룹을 지정하므로 선택지 C가 필요합니다.

◆ | **Q#0088.** | **Ref#0088.**
회사에서는 각 사업부에 대한 내부 클라우드 청구 전략을 변경하려고 합니다. 현재 클라우드 거버넌스팀은 전체 클라우드 지출에 대한 보고서를 각 사업부 책임자와 공유하고 있습니다. 회사는 AWS Organizations를 사용하여 각 사업부에 대한 별도의 AWS 계정을 관리합니다. 조직의 기존 태그 지정 표준에는 애플리케이션, 환경 및 소유자가 포함됩니다. 클라우드 거버넌스 팀은 각 사업부가 클라우드 지출에 대한 월간 보고서를 받을 수 있는 중앙 집중식 솔루션을 원합니다. 또한 솔루션은 설정된 임계값을 초과하는 클라우드 지출에 대한 알림을 보내야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 방법은 무엇입니까?

A. 각 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 알림에 대한 Amazon SNS 주제에 각 사업부를 추가합니다. 각 계정에서 Cost Explorer를 사용하여 각 사업부에 대한 월별 보고서를 생성합니다.
B. 조직의 마스터 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 알림에 대한 Amazon SNS 주제에 각 사업부를 추가합니다. 조직의 마스터 계정에서 Cost Explorer를 사용하여 각 사업부에 대한 월별 보고서를 생성합니다.
C. 각 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 알림에 대한 Amazon SNS 주제에 각 사업부를 추가합니다. 각 계정의 AWS Billing and Cost Management 대시보드를 사용하여 각 사업부에 대한 월별 보고서를 생성합니다.

D. 조직의 마스터 계정에서 AWS 비용 및 사용 보고서를 활성화하고 애플리케이션, 환경별로 그룹화된 보고서를 구성합니다. 그리고 주인. AWS 비용 및 사용 보고서를 처리하고, 예산 알림을 보내고, 각 사업부의 이메일 목록에 월별 보고서를 보내는 AWS Lambda 함수를 생성합니다.

해설
정답: B
AWS Budgets는 AWS비용에 대한 예산을 설정하고 이를 기반으로 알림을 받을 수 있는 서비스입니다. Budgets를 조직의 관리 계정에서 설정하면, 모든 계정에 대한 중앙에서의 비용 관리가 가능해집니다.
그리고 AWS 리소스에 대한 태그 (애플리케이션, 환경, 소유자)를 활용하여 예산 알림을 그룹화합니다. 이는 예산을 상세하게 나눠서, 특정 리소스가 예상 비용을 초과했을 때, 알림을 받을 수 있게 해줍니다.
Simple Notification Service (SNS)라는 AWS 서비스를 이용하여 알림을 받습니다. SNS는 Pub/Sub 메시징 프레임워크로서, 구독자에게 알림을 통보하는 데 사용됩니다. 여기에서는 각 사업부를 SNS 토픽에 추가하여, 예산 초과 알림을 사업부별로 받을 수 있습니다.
AWS Cost Explorer를 사용하여 각 사업 부문에 대한 월간 비용 보고서를 작성하는데 사용합니다.
AWS Cost Explorer는 AWS 비용 및 사용량 데이터에 대한 시각적 단면을 제공하는 서비스로, 조직의 관리 계정에서 사용하면 모든 계정의 비용을 볼 수 있게 됩니다.

◆ | **Q#0089.** | **Ref#0089.**
한 회사가 AWS CloudFormation을 사용하여 인프라를 배포하고 있습니다. 회사는 프로덕션 CloudFormation 스택이 삭제되면 Amazon RDS 데이터베이스 또는 Amazon EBS 볼륨에 저장된 중요한 데이터도 삭제될 수 있다는 점을 우려하고 있습니다.

회사는 사용자가 이런 방식으로 실수로 데이터를 삭제하는 것을 어떻게 방지할 수 있나요?

A. CloudFormation 템플릿을 수정하여 RDS 및 EBS 리소스에 DeletionPolicy 속성을 추가합니다.
B. RDS 및 EBS 리소스 삭제를 허용하지 않는 스택 정책을 구성합니다.
C. IAM 정책을 수정하여 "aws:cloudformation:stack-name" 태그가 지정된 RDS 및 EBS 리소스 삭제를 거부합니다.
D. AWS Config 규칙을 사용하여 RDS 및 EBS 리소스 삭제를 방지합니다.

해설
정답: A
CloudFormation 템플릿 내의 리소스에 DeletionPolicy 속성을 추가하면, 리소스가 CloudFormation에서 삭제되더라도 리소스 자체가 보존되게 할 수 있습니다. 이는 실수로 중요한 데이터를 포함하는 리소스를 삭제하는 것을 막아줍니다.
특히 RDS와 EBS의 경우에는 DeletionPolicy를 "Retain"으로 설정하여 스택 삭제 시 해당 리소스가 삭제되지 않도록 할 수 있습니다. 이러한 이유로 A 선택지가 가장 적절한 방법입니다.

◆ | **Q#0090.** | **Ref#0090.**
회사의 NAT 게이트웨이에 대해 활성화된 VPC 흐름 로그가 있습니다. 회사에는 프라이빗 Amazon EC2 인스턴스로 향하는 퍼블릭 IP 주소 198.51.100.2에서 들어오는 인바운드 트래픽에 대해 Action = ACCEPT가 표시됩니다.

솔루션 설계자는 트래픽이 인터넷에서 원치 않는 인바운드 연결을 나타내는지 여부를 확인해야 합니다. VPC CIDR 블록의 처음 두 옥텟은 203.0입니다.

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

A. AWS CloudTrail 콘솔을 엽니다. NAT 게이트웨이의 탄력적 네트워크 인터페이스와 프라이빗 인스턴스의 탄력적 네트워크 인터레이스가 포함된 로그 그룹을 선택합니다. 쿼리를 실행하여 "like 203.0"으로 설정된 대상 주소와 "like 198.51.100.2"로 설정된 소스 주소로 필터링합니다. stats 명령을 실행하여 소스 주소와 대상 주소로 전송된 바이트의 합계를 필터링합니다.
B. Amazon CloudWatch 콘솔을 엽니다. NAT 게이트웨이의 탄력적 네트워크 인터페이스와 프라이

빗 인스턴스의 탄력적 네트워크 인터페이스가 포함된 로그 그룹을 선택합니다. 쿼리를 실행하여 "like 203.0"으로 설정된 대상 주소와 "like 198.51.100.2"로 설정된 소스 주소로 필터링합니다. stats 명령을 실행하여 소스 주소와 대상 주소로 전송된 바이트의 합계를 필터링합니다.
C. AWS CloudTrail 콘솔을 엽니다. NAT 게이트웨이의 탄력적 네트워크 인터페이스와 프라이빗 인스턴스의 탄력적 네트워크 인터페이스가 포함된 로그 그룹을 선택합니다. 쿼리를 실행하여 "like 198.51.100.2"로 설정된 대상 주소와 "like 203.0"으로 설정된 소스 주소로 필터링합니다. stats 명령을 실행하여 소스 주소와 대상 주소로 전송된 바이트의 합계를 필터링합니다.
D. Amazon CloudWatch 콘솔을 엽니다. NAT 게이트웨이의 탄력적 네트워크 인터페이스와 프라이빗 인스턴스의 탄력적 네트워크 인터페이스가 포함된 로그 그룹을 선택합니다. 쿼리를 실행하여 "like 198.51.100.2"로 설정된 대상 주소와 "like 203.0"으로 설정된 소스 주소로 필터링합니다. stats 명령을 실행하여 소스 주소와 대상 주소로 전송된 바이트의 합계를 필터링합니다.

해설
정답: B
VPC Flow Logs는 Amazon Virtual Private Cloud (Amazon VPC)에서 네트워크 인터페이스를 통해 전송되는 IP 트래픽 정보를 포착하고 로그로 저장합니다. 이 포착된 로그들은 공개되지 않은 연결이 의심될 때 요청하지 않은 인바운드 연결이 있는지 확인하는데 사용될 수 있습니다.
Amazon CloudWatch는 AWS 리소스 및 애플리케이션에서 수집한 데이터를 모니터링하고 분석할 수 있는 서비스입니다. 로그 그룹에는 같은 유형의 로그 데이터를 모아놓을 수 있기 때문에 로그를 분석할 때 굉장히 편리하게 쓰입니다.
문제에서 목적지 주소를 "like 203.0"으로 설정하고 출처 주소를 "like 198.51.100.2"로 설정하여 필터링한다는 설명은 로그 데이터에서 198.51.100.2로 시작하는 IP 주소에서 발송된 패킷과 VPC의 CIDR 블록이 203.0으로 시작하는 프라이빗 EC2 인스턴스로 수신되는 패킷들만 필터링하겠다는 의미입니다.
stats 명령을 실행하는 것은 필터링된 패킷들이 얼마나 많은 데이터를 통신하였는지 합계를 내보겠다는 의미입니다. 이를 통해 실질적으로 데이터가 얼마나 통신되었는지를 파악하여, 활동이 실제로 일어났는지 파악할 수 있습니다.

091 (최정현) 4회차 完

◆ | **Q#0091.** | **Ref#0091.**
회사는 두 개의 별도 사업 단위로 구성됩니다. 각 사업부는 AWS Organizations의 단일 조직 내에 자체 AWS 계정을 가지고 있습니다. 각 사업부는 정기적으로 중요한 문서를 서로 공유합니다. 공유를 용이하게 하기 위해 회사는 각 계정에 Amazon S3 버킷을 생성하고 S3 버킷 간에 저방향 복제를 구성했습니다. S3 버킷에는 수백만 개의 객체가 있습니다.

최근 보안 감사를 통해 S3 버킷 모두 저장 시 암호화가 활성화되어 있지 않은 것으로 확인되었습니다. 회사 정책에 따라 모든 문서는 암호화된 상태로 저장되어야 합니다. 회사는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 서버 측 암호화를 구현하려고 합니다.

이러한 요구 사항을 충족하는 가장 운영 효율적인 솔루션은 무엇입니까?

A. 두 S3 버킷 모두에서 SSE-S3을 켭니다. S3 배치 작업을 사용하여 동일한 위치에 객체를 복사하고 암호화합니다.
B. 각 계정에 AWS Key Management Service(AWS KMS) 키를 생성합니다. 해당 AWS 계정의 해당 KMS 키를 사용하여 각 S3 버킷에서 AWS KMS 키(SSE-KMS)로 서버 측 암호화를 활성화합니다. AWS CLI에서 S3 복사 명령을 사용하여 기존 객체를 암호화합니다.
C. 두 S3 버킷 모두에서 SSE-S3을 켭니다. AWS CLI에서 S3 복사 명령을 사용하여 기존 객체를 암호화합니다.
D. 각 계정에 AWS Key Management Service(AWS KMS) 키를 생성합니다. 해당 AWS 계정의 해당 KMS 키를 사용하여 각 S3 버킷에서 AWS KMS 키(SSE-KMS)로 서버 측 암호화를 활성화합니다. S3 배치 작업을 사용하여 객체를 동일한 위치에 복사합니다.

해설
정답: A

기존 Amazon S3 개체를 암호화하려면 Amazon S3 Batch Operations를 사용하면 됩니다. S3 Batch Operations에 작업할 개체 목록을 제공하고 Batch Operations는 지정된 작업을 수행하기 위해 해당 API를 호출합니다. Batch Operations Copy 작업을 사용하여 암호화되지 않은 기존 개체를 복사하고 암호화된 개체와 동일한 버킷에 다시 쓸 수 있습니다. 한 개의 Batch Operations 작업으로 수십억 개의 개체에 대해 지정된 작업을 수행할 수 있습니다.

B: SSE-S3 방식의 암호화를 사용한다고 했으니, KMS 방식은 틀림
C: CLI 방식은 배치 방식 보다 효율적이지 않다.
D: B와 같은 이유

◆ | **Q#0092.** | **Ref#0092.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon S3 버킷에 대량의 구조화되지 않은 데이터를 수집하고 저장합니다. S3 버킷에는 수 테라바이트의 데이터가 포함되어 있으며 S3 Standard 스토리지 클래스를 사용합니다. 데이터 크기는 매일 수 기가바이트씩 증가합니다.

회사는 데이터를 쿼리하고 분석해야 합니다. 회사는 1년이 넘은 데이터에 접근하지 않습니다. 그러나 회사는 규정 준수를 위해 모든 데이터를 무기한 보관해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. S3 Select를 사용하여 데이터를 쿼리합니다. 1년이 넘은 데이터를 S3 Glacier Deep Archive로 전환하는 S3 수명 주기 정책을 생성합니다.
B. Amazon Redshift Spectrum을 사용하여 데이터를 쿼리합니다. 1년이 넘은 10 S3 Glacier Deep Archive 데이터를 전환하는 S3 수명 주기 정책을 생성합니다.
C. AWS Glue 데이터 카탈로그와 Amazon Athena를 사용하여 데이터를 쿼리합니다. 1년이 넘은 데이터를 S3 Glacier Deep Archive로 전환하는 S3 수명 주기 정책을 생성합니다.
D. Amazon Redshift Spectrum을 사용하여 데이터를 쿼리합니다. 1년이 넘은 데이터를 S3 Intelligent-Tiering으로 전환하는 S3 수명 주기 정책을 생성합니다.

해설
정답: C

C 솔루션을 사용하면 아마존 아테나와 AWS 글루 데이터 카탈로그를 사용하여 S3 버킷에 데이터를 쿼리하고 분석할 수 있습니다. 아마존 아테나는 서버리스 대화형 쿼리 서비스로 SQL을 사용하여 S3에서 데이터를 분석할 수 있습니다. AWS 글루 데이터 카탈로그는 관리되는 메타데이터 저장소로 S3에 저장된 데이터에 대한 테이블 정의를 저장하고 검색하는 데 사용할 수 있습니다. 이 서비스들은 함께 많은 양의 비정형 데이터를 쿼리하고 분석하는 비용 효율적인 방법을 제공할 수 있습니다. 또한 S3 라이프사이클 정책을 사용하여 1년 이상 된 데이터를 S3 Glacier Deep Archive로 전환함으로써 규정 준수를 이유로 데이터를 무기한 유지하는 동시에 스토리지 비용을 절감할 수 있습니다.

A: S3 Select를 사용하는 것은 S3에서 데이터를 필터링하는 데는 좋지만, 대량의 데이터를 조회하고 분석하는 데는 적합하지 않은 솔루션일 수 있습니다.
B: Amazon Redshift Spectrum은 S3에 저장된 데이터를 쿼리하는 데 사용할 수 있지만 비정형 데이터를 쿼리하는 데 Amazon Athena를 사용하는 것만큼 비용 효율적이지 않을 수 있습니다.
D: Amazon Redshift Spectrum을 S3 Intelligent-Tiering과 함께 사용하는 것이 좋은 해결책이 될 수 있지만, S3 Intelligent-Tiering은 액세스 패턴에 따라 스토리지 비용을 최적화하도록 설계되었으며, 액세스 패턴에 따라 데이터를 다른 스토리지 클래스로 이동하기 때문에 규정 준수를 위한 최선의 해결책이 될 수 없습니다.

◆ | **Q#0093.** | **Ref#0093.**
비디오 처리 회사는 회사의 온프레미스 네트워크 연결 스토리지 시스템에 수천 개의 파일로 저장되어 있는 600TB의 압축 데이터를 사용하여 기계 학습(ML) 모델을 구축하려고 합니다. 회사는 ML 실험에 필요한 컴퓨팅 리소스를 사내에 보유하고 있지 않으며 AWS를 사용하려고 합니다.

회사는 3주 이내에 AWS로의 데이터 전송을 완료해야 합니다. 데이터 전송은 일회성 전송입니다. 데이터는 전송 중에 암호화되어야 합니다. 회사 인터넷 연결의 측정된 업로드 속도는 100Mbps입니다. 여러 부서가 연결을 공유합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** AWS Management Console을 사용하여 여러 AWS Snowball Edge Storage Optimized 디바이스를 주문하십시오. 대상 S3 버킷으로 장치를 구성합니다. 데이터를 장치에 복사합니다. 디바이스를 AWS로 다시 배송합니다.
> **B.** 회사 위치와 가장 가까운 AWS 지역 간에 10Gbps AWS Direct Connect 연결을 설정합니다. VPN 연결을 통해 데이터를 지역으로 전송하여 Amazon S3에 데이터를 저장합니다.
> **C.** 온프레미스 네트워크 연결 스토리지와 가장 가까운 AWS 리전 간에 VPN 연결을 생성합니다. VPN 연결을 통해 데이터를 전송합니다.
> **D.** 온프레미스에 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 대상 S3 버킷으로 파일 게이트웨이를 구성합니다. 데이터를 파일 게이트웨이에 복사합니다.
>
> 해설
> 정답: A
>
> 스노우볼 엣지(Snowball Edge Storage Optimized) 기기가 많은 양의 데이터를 빠르고 안전하게 전송할 수 있기 때문에 이 옵션은 3주 이내에 데이터 전송을 완료해야 하는 요구 사항을 충족합니다. 데이터는 전송 중 및 정지 상태에서 암호화됩니다. 회사의 인터넷 연결 속도는 인터넷이 아닌 기기에서 데이터 전송이 이루어지기 때문에 병목 현상이 발생하지 않습니다.
>
> B: 10Gbps 다이렉트 커넥트 연결을 설정하고 유지하는 데 비용이 상당히 많이 들 수 있기 때문에 비용 효율적인 솔루션이 아닙니다. 특히 일회성 데이터 전송에만 필요한 경우에는 더욱 그렇습니다.
> C: 온프레미스 스토리지와 가장 가까운 AWS 영역 간에 VPN 연결을 생성하려면 상당한 네트워킹 구성 및 유지보수가 필요하고 Snowball Edge 장치를 사용하는 것보다 비용이 더 많이 들기 때문에 비용 효율적인 솔루션이 아닙니다.
> D: 비용 효율적인 솔루션이 아닙니다. AWS Storage Gateway 파일 게이트웨이를 사내에 구축하려면 추가 하드웨어 및 지속적인 유지보수 비용이 필요하고 일회성 데이터 전송이 필요하지 않을 수 있습니다.

◆ | **Q#0094.** | **Ref#0094.**
한 회사가 양식 처리 애플리케이션을 AWS로 마이그레이션했습니다. 사용자는 애플리케이션과 상호 작용할 때 웹 애플리케이션을 통해 스캔한 양식을 파일로 업로드합니다. 데이터베이스는 사용자 메타데이터와 Amazon S3에 저장된 파일에 대한 참조를 저장합니다. 웹 애플리케이션은 Amazon EC2 인스턴스와 PostgreSQL용 Amazon RDS 데이터베이스에서 실행됩니다.

양식이 업로드되면 애플리케이션은 Amazon Simple 알림 서비스(Amazon SNS)를 통해 팀에 알림을 보냅니다. 그러면 팀원이 로그인하여 각 양식을 처리합니다. 팀 구성원은 API를 사용하는 다른 시스템에 정보를 입력하기 전에 양식에 대한 데이터 유효성 검사를 수행하고 관련 데이터를 추출합니다.

솔루션 설계자는 양식의 수동 처리를 자동화해야 합니다. 솔루션은 정확한 양식 추출을 제공해야 합니다. 시장 출시 시간을 최소화하고, 장기적인 운영 오버헤드를 최소화합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 양식에서 광학 문자 인식(OCR)을 수행하기 위한 사용자 정의 라이브러리를 개발합니다. 라이브러리를 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 애플리케이션 계층으로 배포합니다. 양식이 업로드될 때 양식을 처리하려면 이 계층을 사용합니다. 출력을 Amazon S3에 저장합니다. 데이터를 Amazon DynamoDB 테이블로 추출하여 이 출력을 구문 분석합니다. 데이터를 대상 시스템의 APL에 제출합니다. EC2 인스턴스에 새 애플리케이션 계층을 호스팅합니다.
B. AWS Step Functions 및 AWS Lambda를 사용하는 애플리케이션 계층으로 시스템을 확장합니다. 양식이 업로드될 때 양식에서 광학 문자 인식(OCR)을 수행하기 위해 EC2 인스턴스에서 훈련되고 호스팅되는 인공 지능 및 기계 학습(AI/ML) 모델을 사용하도록 이 계층을 구성합니다. 출력을 Amazon S3에 저장합니다. 애플리케이션 계층 내에서 필요한 데이터를 추출하여 이 출력을 구문 분석합니다. 대상 시스템의 API에 데이터를 제출합니다.
C. EC2 인스턴스에 새로운 애플리케이션 계층을 호스팅합니다. 양식에서 광학 문자 인식(OCR)을 수행하기 위해 Amazon SageMaker에서 교육 및 호스팅되는 인공 지능 및 기계 팀 구성(AI/ML) 모델을 호스팅하는 엔드포인트를 호출하려면 이 계층을 사용합니다. 출력을 Amazon ElastiCache에 저장합니다. 애플리케이션 계층 내에서 필요한 데이터를 추출하여 이 출력을 구문 분석합니다. 대상 시스템의 API에 데이터를 제출합니다.
D. AWS Step Functions 및 AWS Lambda를 사용하는 애플리케이션 계층으로 시스템을 확장합니다. 양식이 업로드될 때 양식에서 광학 문자 인식(OCR)을 수행하기 위해 Amazon Textract 및 Amazon Comprehend를 사용하도록 이 계층을 구성합니다. 출력을 Amazon S3에 저장합니다. 애플리케이션 계층 내에서 필요한 데이터를 추출하여 이 출력을 구문 분석합니다. 대상 시스템의 API에 데이터를 제출합니다.

해설
정답: D

D 솔루션은 정확한 양식 추출, 최소 시장 출시 시간 및 최소 장기 운영 오버헤드의 요구 사항을 충족합니다. Amazon Textract와 Amazon Comprehend는 OCR을 수행하고 양식에서 관련 데이터를 추출할 수 있는 완벽하게 관리되고 서버가 없는 서비스이므로 맞춤형 라이브러리를 개발하거나 모델을 훈련하고 호스트할 필요가 없습니다. AWS Step Functions와 Lambda를 사용하면 프로세스를 쉽게 자동화하고 필요에 따라 확장할 수 있습니다.

A: 이 옵션을 사용하려면 상당한 개발 및 유지보수 작업이 필요하고 완전히 관리되는 서비스를 활용하지 못해 운영 오버헤드가 증가합니다.
B: 이 옵션은 모델을 교육하고 호스팅하는 데 상당한 개발 및 유지보수 노력이 필요하고, 완전히 관리된 서비스를 활용하지 못해 운영 오버헤드가 증가한다는 점에서 옵션 A와 유사합니다.
C: 이 옵션은 모델을 교육하고 호스팅하는 데 상당한 개발 및 유지보수 노력이 필요하고, 완전히 관리되는 서비스를 활용하지 못해 운영 오버헤드가 증가한다는 점에서 옵션 B와 유사합니다.

◆ | **Q#0095.** | **Ref#0095.**
한 회사가 AWS 클라우드에서 온프레미스 주문 처리 플랫폼을 리팩터링하고 있습니다. 플랫폼에는 여러 VM에서 호스팅되는 웹 프런트 엔드, 프런트 엔드를 백엔드에 연결하는 RabbitMQ, 주문을 처리하기 위해 컨테이너화된 백엔드 시스템을 실행하는 Kubernetes 클러스터가 포함되어 있습니다. 회사는 애플리케이션에 큰 변경을 원하지 않습니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 웹 서버 VM의 AMI를 생성합니다. AMI와 Application Load Balancer를 사용하는 Amazon EC2 Auto Scaling 그룹을 생성합니다. 온프레미스 메시징 대기열을 대체하도록 Amazon MQ를 설정합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service(Amazon EKS)를 구성합니다.
B. 웹 서버 환경을 모방하는 사용자 지정 AWS Lambda 런타임을 생성합니다. 프런트엔드 웹 서버를 대체할 Amazon API Gateway API를 생성합니다. 온프레미스 메시징 대기열을 대체하도록 Amazon

MQ를 설정합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service(Amazon EKS)를 구성합니다.
C. 웹 서버 VM의 AMI를 생성합니다. AMI와 Application Load Balancer를 사용하는 Amazon EC2 Auto Scaling 그룹을 생성합니다. 온프레미스 메시징 대기열을 대체하도록 Amazon MQ를 설정합니다. 다양한 EC2 인스턴스 집합에 Kubernetes를 설치하여 주문 처리 백엔드를 호스팅합니다.
D. 웹 서버 VM의 AMI를 생성합니다. AMI와 Application Load Balancer를 사용하는 Amazon EC2 Auto Scaling 그룹을 생성합니다. 온프레미스 메시징 대기열을 대체할 Amazon Simple Queue Service(Amazon SQS) 대기열을 설정합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service(Amazon EKS)를 구성합니다.

해설
정답: A

A 솔루션에서 회사는 웹 서버 VM의 Amazon Machine Image (AMI)를 만들고, 이는 온프레미스 웹 서버와 동일한 EC2 인스턴스를 시작하는 데 사용할 수 있습니다. 그런 다음 회사는 AMI와 ALB(Application Load Balancer)를 사용하여 웹 프론트 엔드에 자동 확장 및 고가용성을 제공하는 EC2 자동 확장 그룹을 만듭니다. 회사는 또한 온프레미스 메시징 큐(RabbitMQ)를 RabbitMQ와 완벽하게 호환되는 관리형 메시지 브로커 서비스인 Amazon MQ로 대체합니다. 마지막으로 회사는 Amazon Elastic Kubernetes Service(EKS)를 사용하여 주문 처리 백엔드를 호스팅하여 애플리케이션에 큰 변경을 가하지 않고 기존 Kubernetes 클러스터를 AWS 클라우드에서 실행할 수 있습니다. 이 접근 방식은 회사가 운영 오버헤드를 최소화하면서 기존 플랫폼을 들어올리고 이동할 수 있도록 합니다.

B: 사용자 지정 AWS Lambda 런타임 및 Amazon API Gateway를 사용하면 응용 프로그램을 크게 변경해야 하며 현재 코드베이스와 호환되지 않을 수 있습니다.
C: 다양한 EC2 인스턴스의 함대에 Kubernetes를 설치하는 것으로 응용 프로그램을 크게 변경해야 하며 현재 코드베이스와 호환되지 않을 수 있습니다.
D: Amazon MQ 대신 Amazon Simple Queue Service(Amazon SQS)를 사용하면 Amazon MQ와 동일한 수준의 메시징 기능을 제공하지 못할 뿐만 아니라 주문 처리 플랫폼의 요구 사항에 충분하지 않을 수 있습니다.

◆ | **Q#0096.** | **Ref#0096.**
솔루션 아키텍트는 새로운 Amazon S3 버킷에 저장될 객체에 대해 클라이언트 측 암호화 메커니즘을 구현해야 합니다. 솔루션 아키텍트는 이러한 목적으로 AWS Key Management Service(AWS KMS)에 저장되는 CMK를 생성했습니다.

솔루션 설계자는 다음 IAM 정책을 생성하여 IAM 역할에 연결했습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadUpload",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::BucketName/*"
        },
        {
            "Sid": "KMSAccess",
```

```
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:kms:Region:Account:key/Key ID"
        }
    ]
}
```

테스트 중에 솔루션 설계자는 S3 버킷에서 기존 테스트 개체를 성공적으로 가져올 수 있었습니다. 그러나 새 개체를 업로드하려고 하면 오류 메시지가 발생했습니다. 오류 메시지에는 작업이 금지되었다고 명시되어 있습니다.

모든 요구 사항을 충족하려면 솔루션 설계자가 IAM 정책에 어떤 작업을 추가해야 합니까?

> **A.** kms:GenerateDataKey
> **B.** kms:GetKeyPolicy
> **C.** kms:GetPublicKey
> **D.** kms:Sign
>
> 해설
> 정답: A
>
> 클라이언트 측 암호화를 위한 데이터 키를 생성하기 위해 "kms:GenerateDataKey" 작업을 IAM 정책에 추가해야 합니다. 이 작업이 없으면 IAM 역할에 데이터 키를 생성하는 데 필요한 권한이 없으므로 새 개체를 업로드하려고 할 때 오류 메시지가 표시됩니다.
>
> kms:GetKeyPolicy 는 CMK에 대한 키 정책을 검색할 수 있지만 S3 개체의 클라이언트 측 암호화와 관련이 없으며
> kms:GetPublicKey에서는 CMK의 공개 키를 검색할 수 있지만 S3 개체의 클라이언트 측 암호화와 관련이 없으며
> kms:Sign에서는 CMK를 사용하여 메시지에 서명할 수 있지만 S3 개체의 클라이언트 측 암호화와는 관련이 없습니다.

◆ | **Q#0097.** | **Ref#0097.**
한 회사에서 웹 애플리케이션을 개발했습니다. 이 회사는 Application Load Balancer 뒤에 있는 Amazon EC2 인스턴스 그룹에서 애플리케이션을 호스팅하고 있습니다. 회사는 애플리케이션의 보안 상태를 개선하기를 원하며 AWS WAF 웹 ACL을 사용할 계획입니다. 솔루션은 애플리케이션에 대한 합법적인 트래픽에 부정적인 영향을 주어서는 안 됩니다.

솔루션 설계자는 이러한 요구 사항을 충족하도록 웹 ACL을 어떻게 구성해야 합니까?

> **A.** 웹 ACL 규칙의 작업을 개수로 설정합니다. AWS WAF 로깅을 활성화합니다. 오탐지 요청을 분석합니다. 잘못된 긍정을 방지하려면 규칙을 수정하세요. 시간이 지남에 따라 웹 ACL 규칙의 작업을 개수에서 차단으로 변경합니다.
> **B.** 웹 ACL에서는 속도 기반 규칙만 사용하고 제한을 최대한 높게 설정합니다. 한도를 초과하는 모든 요청을 일시적으로 차단합니다. 요율 추적 범위를 좁히려면 중첩 규칙을 정의하세요.
> **C.** 웹 ACL 규칙의 동작을 차단으로 설정합니다. 웹 ACL에는 AWS 관리형 규칙 그룹만 사용하십시오. AWS WAF 샘플링 요청 또는 AWS WAF 로그와 함께 Amazon CloudWatch 지표를 사용하여 규칙 그룹을 평가합니다.
> **D.** 웹 ACL에서는 사용자 지정 규칙 그룹만 사용하고 작업을 허용으로 설정합니다. AWS WAF 로깅을 활성화합니다. 오탐지 요청을 분석합니다. 잘못된 긍정을 방지하려면 규칙을 수정하세요. 시간이 지남에 따라 웹 ACL 규칙의 작업을 허용에서 차단으로 변경합니다.

해설
정답: A

웹 ACL 규칙의 동작을 Count로 설정합니다. AWS WAF 로깅을 활성화합니다. false positive 요청을 분석합니다. false positive를 방지하도록 규칙을 수정합니다. 시간이 지남에 따라 웹 ACL 규칙의 동작을 Count에서 Block으로 변경합니다.
이 접근 방식은 합법적인 트래픽에 영향을 미칠 수 있는 조치를 취하기 전에 들어오는 트래픽과 그 행동을 모니터링할 수 있게 합니다. 조치를 카운트로 설정함으로써, 웹 ACL은 규칙의 조건과 일치하는 요청만 기록할 뿐 그것들을 차단하지는 않습니다. 이러한 방식으로, 회사는 요청을 분석하고 거짓 긍정을 확인할 수 있습니다. 일단 그들이 거짓 긍정을 식별하고 수정하면, 그들은 웹 ACL 규칙의 조치를 카운트에서 블록으로 점진적으로 변경할 수 있고, 따라서 합법적인 트래픽에 악영향을 미치지 않고 응용 프로그램의 보안 자세를 개선할 수 있습니다.
B: Rate-based rules 만 사용하면 오탐이 발생하고 합법적인 트래픽이 차단될 수 있다.
C: AWS 관리 규칙 그룹만 사용하면 웹 ACL의 유연성과 특수성이 제한될 수 있다.
D: 사용자 지정 규칙 그룹만 사용하고 작업을 허용으로 설정을 하면 보안 취약점이 발생할 수 있다.

◆ | **Q#0098.** | **Ref#0098.**
회사에는 AWS Organizations에 많은 AWS 계정이 있는 조직이 있습니다. 솔루션 아키텍트는 회사가 조직 내 AWS 계정에 대한 공통 보안 그룹 규칙을 관리하는 방법을 개선해야 합니다.

회사는 회사의 온프레미스 네트워크에 대한 액세스를 허용하기 위해 각 AWS 계정의 허용 목록에 공통 IP CIDR 범위 세트를 가지고 있습니다. 각 계정 내의 개발자는 보안 그룹에 새로운 IP CIDR 범위를 추가할 책임이 있습니다. 보안팀에는 자체 AWS 계정이 있습니다. 현재 보안 팀은 허용 목록이 변경되면 다른 AWS 계정 소유자에게 알립니다.

솔루션 설계자는 모든 계정에 공통 CIDR 범위 집합을 배포하는 솔루션을 설계해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 보안 팀의 AWS 계정에 Amazon Simple 알림 서비스(Amazon SNS) 주제를 설정합니다. 각 AWS 계정에 AWS Lambda 함수를 배포합니다. SNS 주제가 메시지를 수신할 때마다 실행되도록 Lambda 함수를 구성합니다. IP 주소를 입력으로 사용하고 이를 계정의 보안 그룹 목록에 추가하도록 Lambda 함수를 구성합니다. 보안팀에 SNS 주제에 메시지를 게시하여 변경 사항을 배포하도록 지시하세요.
B. 조직 내의 각 AWS 계정에 새로운 고객 관리 접두사 목록을 생성합니다. 모든 내부 CIDR 범위로 각 계정의 접두사 목록을 채웁니다. 보안 그룹의 계정에 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다. 각 AWS 계정 소유자와 업데이트를 공유하도록 보안팀에 지시하십시오.
C. 보안 팀의 AWS 계정에 새로운 고객 관리 접두사 목록을 생성합니다. 모든 내부 CIDR 범위로 고객 관리 접두사 목록을 채웁니다. AWS Resource Access Manager를 사용하여 고객 관리형 접두사 목록을 조직과 공유합니다. 보안 그룹에서 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다.
D. 조직의 각 계정에 IAM 역할을 생성합니다. 보안 그룹을 업데이트할 수 있는 권한을 부여합니다. 보안 팀의 AWS 계정에 AWS Lambda 함수를 배포합니다. 내부 IP 주소 목록을 입력으로 사용하고, 각 조직 계정의 역할을 맡고, 각 계정의 보안 그룹에 IP 주소 목록을 추가하도록 Lambda 함수를 구성합니다.

해설
정답: C

C 솔루션은 보안 팀이 단일 고객 관리 접두사 목록을 생성 및 유지 관리하고 AWS 리소스 액세스 매니저를 사용하여 조직과 공유해야 하므로 운영 오버헤드가 가장 적은 요구 사항을 충족합니다. 그러

면 각 AWS 계정의 소유자는 보안 그룹에서 접두사 목록을 허용해야 하므로 변경 사항이 발생할 때 보안 팀이 각 계정 소유자에게 수동으로 통지할 필요가 없습니다. 또한 이 솔루션은 각 계정에서 별도의 AWS Lambda 기능이 필요하지 않으므로 솔루션의 전반적인 복잡성이 줄어듭니다.
A: 보안팀 AWS 계정에 SNS 토픽을 설정하고 각 AWS 계정에 AWS 람다 기능을 배치해야 하기 때문에 맞지 않습니다. 이는 SNS 토픽 설정 및 유지보수, 각 계정에 람다 기능을 배치 및 구성해야 하기 때문에 운영 오버헤드가 증가합니다.
B: 조직 내 각 AWS 계정에 고객 관리 접두사 목록을 새로 만들어야 하므로 맞지 않으며, 이는 보안 팀이 여러 접두사 목록을 만들고 유지 관리해야 하므로 운영 오버헤드가 증가합니다.
D: 조직의 각 계정에 IAM 역할을 생성해야 하므로 맞지 않으며, 이는 보안 팀이 여러 역할을 설정하고 유지해야 하므로 운영 오버헤드가 증가합니다. 또한 보안 팀의 AWS 계정에 AWS Lambda 기능을 배치하여 복잡성과 운영 오버헤드가 증가합니다.

◆ | **Q#0099.** | **Ref#0099.**
한 회사는 직원들이 VPN을 사용하여 연결하면 집에서 원격으로 근무할 수 있도록 허용하는 새로운 정책을 도입했습니다. 회사는 여러 AWS 계정의 VPC를 사용하여 내부 애플리케이션을 호스팅하고 있습니다. 현재 애플리케이션은 AWS Site-to-Site VPN 연결을 통해 회사의 온프레미스 사무실 네트워크에서 액세스할 수 있습니다. 회사의 기본 AWS 계정에 있는 VPC에는 다른 AWS 계정에 있는 VPC와 피어링 연결이 설정되어 있습니다.

솔루션 아키텍트는 직원이 재택근무하는 동안 사용할 수 있도록 확장 가능한 AWS 클라이언트 VPN 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 솔루션은 무엇입니까?

A. 각 AWS 계정에 클라이언트 VPN 엔드포인트를 생성합니다. 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.
B. 기본 AWS 계정에 클라이언트 VPN 엔드포인트를 생성합니다. 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.
C. 기본 AWS 계정에 클라이언트 VPN 엔드포인트를 생성합니다. 각 AWS 계정에 연결된 전송 게이트웨이를 프로비저닝합니다. 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.
D. 기본 AWS 계정에 클라이언트 VPN 엔드포인트를 생성합니다. 클라이언트 VPN 엔드포인트와 AWS Site-to-Site VPN 간의 연결을 설정합니다.

해설
정답: C

확장 가능한 것을 설계하라는 질문이며, C에서는 Transit Gateway가 network transit hub 역할을 하여 VPN 연결이 서로 다른 AWS 계정에 있는 여러 VPC를 통해 리소스에 액세스할 수 있도록 합니다. VPC 피어링 연결은 전환적 피어링 관계를 지원하지 않습니다. 즉, 사용자가 AWS Client VPN을 통해 하나의 VPC에 연결된 경우 피어링 연결을 통해 연결된 다른 VPC의 리소스에 액세스할 수 없습니다.

◆ | **Q#0100.** | **Ref#0100.**
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 최근 애플리케이션 지표에 따르면 응답 시간이 일관되지 않고 오류율이 크게 증가한 것으로 나타났습니다. 타사 서비스에 대한 호출로 인해 지연이 발생합니다. 현재 애플리케이션은 AWS Lambda 함수를 직접 호출하여 타사 서비스를 동기식으로 호출합니다.

솔루션 설계자는 타사 서비스 호출을 분리하고 모든 호출이 최종적으로 완료되도록 해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon Simple Queue Service(Amazon SQS) 대기열을 사용하여 이벤트를 저장하고 Lambda 함수를 호출합니다.

B. AWS Step Functions 상태 시스템을 사용하여 이벤트를 Lambda 함수에 전달합니다.
C. Amazon EventBridge 규칙을 사용하여 이벤트를 Lambda 함수에 전달합니다.
D. Amazon Simple 알림 서비스(Amazon SNS) 주제를 사용하여 이벤트를 저장하고 Lambda 함수를 호출합니다.

해설
정답: A

SQS는 애플리케이션이 분산 구성 요소 간에 메시지를 보내고, 저장하고, 받을 수 있도록 하는 완벽하게 관리되고 안정적이며 확장성이 뛰어난 메시지 대기열 서비스입니다. 타사 서비스 호출을 SQS 대기열로 보내면 타사 서비스가 응답할 때까지 기다리지 않고 애플리케이션이 계속 처리할 수 있으므로 응답 시간이 빨라지고 오류율이 낮아질 수 있습니다.

AWS Step Functions는 시각적 워크플로우를 사용하여 분산된 애플리케이션과 마이크로서비스의 구성 요소를 쉽게 조정할 수 있는 서비스입니다.
Amazon EventBridge는 서버가 없는 이벤트 버스로 자신의 애플리케이션, 통합 SaaS 애플리케이션 및 AWS 서비스의 데이터를 사용하여 애플리케이션을 쉽게 연결할 수 있습니다.
Amazon SNS는 애플리케이션 대 애플리케이션 및 애플리케이션 대 개인(A2P) 통신 모두를 위한 완전히 관리되는 메시징 서비스입니다. 이러한 서비스는 메시지 큐를 제공하는 데 중점을 두지 않으며 이 사용 사례에 가장 적합하지 않습니다.