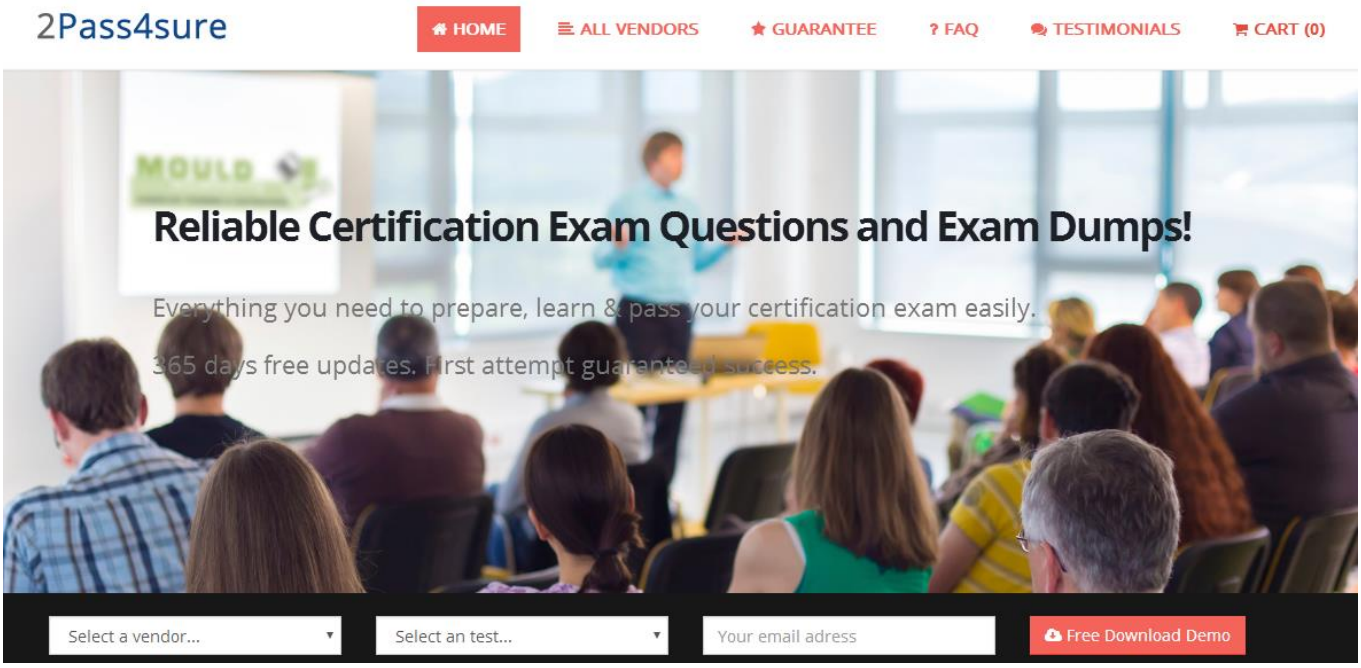
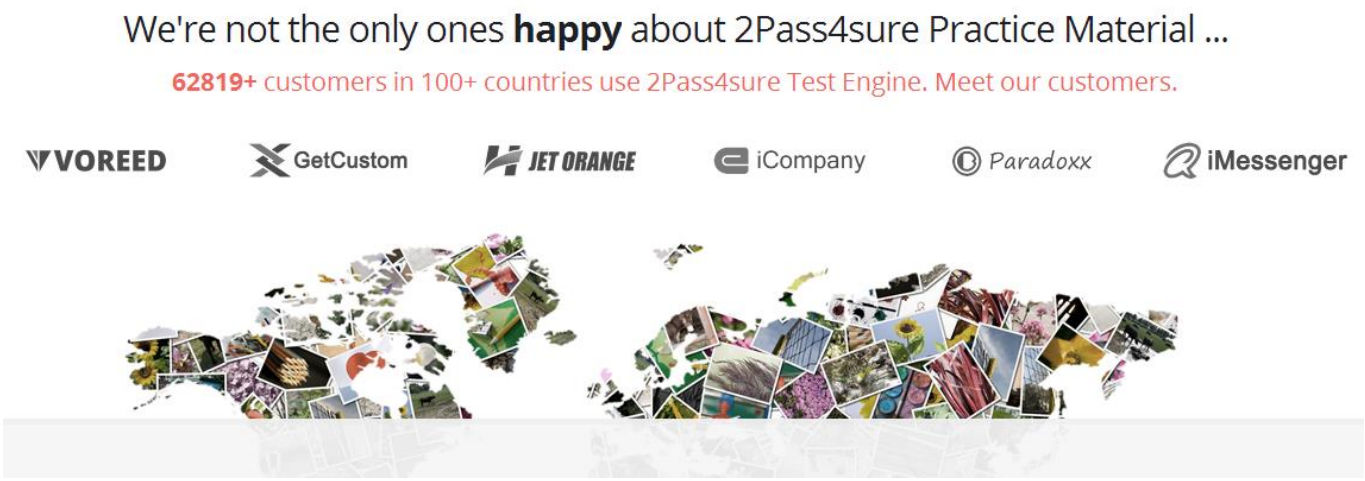
2Pass4sure





http://www.2pass4sure.com/

Reliable Certification Exam Questions and Exam Dumps - 2Pass4sure

Exam : **SAP-C02-KR**

Title : AWS Certified Solutions Architect - Professional (SAP-C02 Korean Version)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
회사에서 정적 콘텐츠를 호스팅하는 새 웹 사이트를 디자인하고 있습니다. 이 웹사이트는 사용자에게 대용량 파일을 업로드하고 다운로드할 수 있는 기능을 제공합니다. 회사 요구 사항에 따라 모든 데이터는 전송 중 및 유휴 상태에서 암호화되어야 합니다. 솔루션 설계자는 Amazon S3 및 Amazon CloudFront를 사용하여 솔루션을 구축하고 있습니다.
어떤 단계 조합이 암호화 요구 사항을 충족합니까? (3개를 선택하세요.)
A. 웹 애플리케이션이 사용하는 S3 버킷에 대해 S3 서버 측 암호화를 켭니다.
B. S3 ACL의 읽기 및 쓰기 작업에 대해 "aws:SecureTransport": "true" 정책 속성을 추가합니다.
C. 웹 애플리케이션이 사용하는 S3 버킷에서 암호화되지 않은 작업을 거부하는 버킷 정책을 생성합니다.
D. AWS KMS 키(SSE-KMS)로 서버 측 암호화를 사용하여 CloudFront에서 유휴 암호화를 구성합니다.
E. CloudFront에서 HTTP 요청의 HTTPS 요청으로의 리디렉션을 구성합니다.
F. 웹 애플리케이션이 사용하는 S3 버킷에 대해 미리 서명된 URL을 생성할 때 RequireSSL 옵션을 사용하십시오.
Answer: A C E
Explanation:
Turning on S3 server-side encryption for the S3 bucket that the web application uses will enable encrypting the data at rest using Amazon S3 managed keys (SSE-S3)1. Creating a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses will enable enforcing encryption for all requests to the bucket2. Configuring redirection of HTTP requests to HTTPS requests in CloudFront will enable encrypting the data in transit using SSL/TLS3.

QUESTION NO: 2
한 유틸리티 회사가 스마트 미터에서 5분마다 사용량 데이터를 수집합니다. 수집된 데이터는 API 게이트웨이로 전송되어 Lambda 함수에서 처리된 후 DynamoDB에 저장됩니다. 사용량이 증가함에 따라 Lambda 함수 실행 시간이 늘어나고 DynamoDB PUT 요청이 ProvisionedThroughputExceededException 오류와 함께 실패했습니다. 또한 Lambda 함수에서 TooManyRequestsException 오류도 발생했습니다.
어떤 변경 사항 조합이 이러한 문제를 해결할 수 있을까요? (두 가지를 선택하세요.)
A. 스마트 미터의 페이로드 크기를 늘립니다.
B. Amazon SQS FIFO 큐에 데이터를 수집하고, 각 메시지가 전송될 때마다 Lambda 함수가 실행되어 처리합니다.
C. API Gateway에서 Amazon Kinesis 데이터 스트림으로 데이터를 스트리밍하고 데이터를 일괄 처리합니다.
D. DynamoDB 테이블의 쓰기 용량 단위를 늘립니다.
E. Lambda 함수에 사용 가능한 메모리를 늘리세요.
Answer: C,D

QUESTION NO: 3
애플리케이션이 us-east-1 리전의 Amazon RDS for MySQL Multi-AZ DB 인스턴스를 사용하고 있습니다. 장애 조치 테스트 후 애플리케이션이 데이터베이스 연결이 끊어졌고 다시

연결할 수 없었습니다.
애플리케이션을 재시작한 후, 애플리케이션이 연결을 다시 설정했습니다.
솔루션 설계자는 애플리케이션이 재시작 없이 데이터베이스와의 연결을 다시 설정할 수 있도록 솔루션을 구현해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. 2노드 Amazon Aurora MySQL DB 클러스터를 생성합니다. RDS DB 인스턴스를 Aurora DB 클러스터로 마이그레이션합니다. RDS 프록시를 생성합니다. 기존 RDS 엔드포인트를 대상으로 구성합니다. 애플리케이션의 연결 설정을 RDS 프록시 엔드포인트를 가리키도록 업데이트합니다.

B. Amazon S3 버킷을 생성합니다. AWS Database Migration Service(AWS DMS)를 사용하여 데이터베이스를 Amazon S3로 내보냅니다. Amazon Athena가 S3 버킷을 데이터 저장소로 사용하도록 구성합니다. 애플리케이션에 최신 ODBC(Open Database Connectivity) 드라이버를 설치합니다. 애플리케이션의 연결 설정을 업데이트하여 Athena 엔드포인트를 가리키도록 합니다.

C. Amazon Aurora MySQL Serverless v1 DB 인스턴스를 생성합니다. RDS DB 인스턴스를 Aurora Serverless v1 DB 인스턴스로 마이그레이션합니다. 애플리케이션의 연결 설정을 Aurora 리더 엔드포인트를 가리키도록 업데이트합니다.

D. RDS 프록시를 생성합니다. 기존 RDS 엔드포인트를 대상으로 구성합니다. 애플리케이션의 연결 설정을 업데이트하여 RDS 프록시 엔드포인트를 가리키도록 합니다.

Answer: D

QUESTION NO: 4

한 회사가 AWS에서 데이터 집약적 애플리케이션을 실행하고 있습니다. 이 애플리케이션은 수백 개의 Amazon EC2 인스턴스 클러스터에서 실행됩니다. 공유 파일 시스템도 200TB의 데이터를 저장하는 여러 EC2 인스턴스에서 실행됩니다.
이 애플리케이션은 공유 파일 시스템의 데이터를 읽고 수정하고 보고서를 생성합니다. 이 작업은 한 달에 한 번 실행되고 공유 파일 시스템에서 파일의 하위 집합을 읽고 완료하는 데 약 72시간이 걸립니다.
컴퓨트 인스턴스는 Auto Scaling 그룹에서 확장되지만 공유 파일 시스템을 호스팅하는 인스턴스는 지속적으로 실행됩니다. 컴퓨트 및 스토리지 인스턴스는 모두 동일한 AWS 지역에 있습니다.
솔루션 아키텍트는 공유 파일 시스템 인스턴스를 교체하여 비용을 절감해야 합니다. 파일 시스템은 72시간 실행 기간 동안 필요한 데이터에 대한 고성능 액세스를 제공해야 합니다.
이러한 요구 사항을 충족하는 동시에 전체 비용을 가장 크게 절감할 수 있는 솔루션은 무엇입니까?

A. 기존 공유 파일 시스템의 데이터를 S3 Intelligent-Tiering 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업을 실행하기 전에 Amazon FSx for Lustre를 사용하여 지연 로딩을 사용하여 Amazon S3의 데이터로 새 파일 시스템을 만듭니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.

B. 기존 공유 파일 시스템에서 Multi-Attach가 활성화된 대규모 Amazon Elastic Block Store(Amazon EBS) 볼륨으로 데이터를 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 볼륨을 분리합니다.

C. 기존 공유 파일 시스템의 데이터를 S3 Standard 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업을 실행하기 전에 Amazon FSx for Lustre를 사용하여 일괄 로딩을 사용하여 Amazon S3의 데이터로 새 파일 시스템을 만듭니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.

D. 기존 공유 파일 시스템에서 Amazon S3 버킷으로 데이터를 마이그레이션합니다. 매월 작업을 실행하기 전에 AWS Storage Gateway를 사용하여 Amazon S3의 데이터로 파일 게이트웨이를 만듭니다. 파일 게이트웨이를 작업의 공유 스토리지로 사용합니다. 작업이 완료되면 파일 게이트웨이를 삭제합니다.

Answer: A

Explanation:

https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre- and-amazon-s3/

QUESTION NO: 5

솔루션 아키텍트는 Auto Scaling Group의 Amazon EC2 인스턴스에 배포된 운영 워크로드를 가지고 있습니다. VPC 아키텍처는 Auto Scaling 그룹이 타겟팅하는 각각에 서브넷이 있는 두 개의 가용성 영역(AZ)에 걸쳐 있습니다. VPC는 온프레미스 환경에 연결되어 있으며 연결이 중단될 수 없습니다. Auto Scaling 그룹의 최대 크기는 서비스 중인 인스턴스 20개입니다. VPC IPv4 주소 지정은 다음과 같습니다.

VPCCIDR 10 0 0 0/23

AZ1 서브넷 CIDR: 10 0 0 0724

AZ2 서브넷 CIDR: 10.0.1 0724

배포 이후, 세 번째 AZ가 지역에서 사용 가능해졌습니다. 솔루션 아키텍트는 추가 IPv4 주소 공간을 추가하지 않고 서비스 다운타임 없이 새로운 AZ를 채택하고자 합니다. 어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. AZ2 서브넷만 사용하도록 자동 확장 그룹을 업데이트합니다. 이전 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 만듭니다. 새 AZI 서브넷도 사용하도록 자동 확장 그룹을 조정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 자동 확장 그룹을 조정합니다. 현재 AZ2 서브넷을 제거합니다. 원래 AZ1 서브넷의 주소 공간의 두 번째 절반을 사용하여 새 AZ2 서브넷을 만듭니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 만든 다음, 세 개의 새 서브넷을 모두 대상으로 자동 확장 그룹을 업데이트합니다.

B. AZ1 서브넷에서 EC2 인스턴스를 종료합니다. 주소 공간을 사용하여 AZ1 서브넷을 삭제하고 다시 만듭니다. 이 새로운 서브넷을 사용하도록 자동 확장 그룹을 업데이트합니다. 두 번째 AZ에 대해 이를 반복합니다.

AZ3에 새 서브넷을 정의한 다음 자동 크기 조정 그룹을 업데이트하여 세 개의 새 서브넷을 모두 대상으로 지정합니다.

C. 동일한 IPv4 주소 공간을 사용하여 새 VPC를 생성하고 각 AZ에 대해 하나씩 총 세 개의 서브넷을 정의합니다. 새 VPC의 새 서브넷을 대상으로 기존 자동 확장 그룹을 업데이트합니다.

D. AZ2 서브넷만 사용하도록 자동 확장 그룹을 업데이트합니다. 이전 주소 공간을 중단하도록 AZ1 서브넷을 업데이트합니다. 자동 확장 그룹을 조정하여 AZ1 서브넷도 다시 사용합니다. 인스턴스가 정상이면 자동 좌석 그룹을 조정하여 AZ1 서브넷만 사용합니다. 현재 AZ2 서브넷을 업데이트하고 원래 AZ1 서브넷에서 주소 공간의 두 번째 절반을 할당합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 만든 다음 자동 확장 그룹을

업데이트하여 세 개의 새 서브넷을 모두 대상으로 합니다.

Answer: A

Explanation:

https://repost.aws/knowledge-center/vpc-ip-address-range

QUESTION NO: 6

한 의료 회사가 아마존 베드락(Amazon Bedrock) 플랫폼을 기반으로 채팅형 사용자 지원 도우미를 개발하고 있습니다. 사용자들은 개인 정보가 포함될 수 있는 건강 관련 질문을 할 것입니다.

솔루션 설계자는 다음과 같은 기능을 수행할 수 있는 솔루션을 구성해야 합니다.

* 보조자가 의료 진단 조언을 제공하는 것을 방지하십시오.
* 사용자 입력과 모델 응답 모두에서 개인 식별 정보(PII)를 삭제합니다.
* 회사가 나중에 기본 모델(FM)을 변경하더라도 동일한 통제를 시행해야 합니다.
* 불필요한 추론 비용을 방지하기 위해 위험한 사용자 프롬프트를 모델에 전송하기 전에 평가하십시오.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. 승인된 건강 지원 지침을 Amazon Bedrock 지식 기반에 저장합니다. 모델이 진단 조언을 제공하지 않도록 시스템 프롬프트를 구성합니다. 추론 후 AWS Lambda 함수를 사용하여 모델 응답에서 개인 식별 정보(PII)를 제거한 후 사용자에게 응답을 반환합니다.

B. 승인된 지원 대화에 대한 FM을 세밀하게 조정합니다. 진단 조언을 금지하는 프롬프트 템플릿을 추가합니다. 대화가 종료된 후 금지된 주제 및 민감한 정보가 있는지 대화를 스캔하는 별도의 검토 프로세스를 실행합니다.

C. 애플리케이션 내에 사용자 지정 검토 계층을 구축하여 금지된 주제를 검사하고 사용자 입력에서 민감한 정보를 삭제합니다. Converse API를 통해 해당 모델을 호출합니다. 응답을 사용자에게 표시하기 전에 별도의 후처리 로직을 사용하여 응답에서 민감한 정보를 삭제합니다.

D. Amazon Bedrock 가드레일을 생성합니다. 의료 진단 조언에 대한 접근 금지 토픽을 구성합니다. 개인 식별 정보(PII)를 마스킹하기 위해 민감 정보 필터를 구성합니다. 콘텐츠 필터를 구성합니다. 추론 전에 사용자 프롬프트에서 ApplyGuardrail API를 호출합니다. 모델 응답을 평가하기 위해 Converse API에도 동일한 가드레일을 포함합니다.

Answer: D

Explanation:

Amazon Bedrock Guardrails are the correct managed control plane for this scenario. A guardrail can combine denied topics, content filters, and sensitive information filters, and it can be applied to prompts and responses across supported foundation models. The ApplyGuardrail API can evaluate text independently before invoking a foundation model, which helps reject or mask risky prompts before incurring model inference cost.

The Converse API also supports guardrail configuration so the same policy can evaluate conversational model responses. Option A relies on prompts and post-processing only, so it does not evaluate risky prompts before inference and does not protect inputs. Option B is retrospective and model-specific. Option C could work technically but creates custom moderation and response-filtering code, which is higher operational overhead than Bedrock Guardrails.

QUESTION NO: 7

회사에 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 함수에서 제공하는 애플리케이션 로직의 새 버전을 배포하는 시간을 줄이고 오류가 식별되었을 때 이를 감지하고 되돌리는 시간도 줄이고자 합니다. 이것이 어떻게 이루어질 수 있습니까?

A. AWS CloudFront 배포 및 API Gateway로 구성된 상위 스택과 Lambda 함수를 포함하는 하위 스택으로 중첩된 AWS CloudFormation 스택을 생성하고 배포합니다. Lambda를 변경하려면 AWS CloudFormation 변경 세트를 생성하고 배포하십시오. 오류가 트리거되면 AWS CloudFormation 변경 세트를 이전 버전으로 되돌립니다.

B. AWS SAM 및 기본 제공 AWS CodeDeploy를 사용하여 새 Lambda 버전을 배포하고 트래픽을 새 버전으로 점진적으로 전환하고 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. 새 Lambda 버전을 참조하는 새 API 게이트웨이 엔드포인트로 구성된 AWS CloudFormation 스택을 생성하고 배포합니다. CloudFront 오리진을 새 API 게이트웨이 엔드포인트로 변경하고 오류를 모니터링하며 감지된 경우 AWS CloudFront 오리진을 이전 API 게이트웨이 엔드포인트로 변경합니다.

Answer: B

Explanation:

https://aws.amazon.com/about-aws/whats-new/2017/11/aws-lambda-supports-traffic-shifting-and-phased- deployments-with-aws-codedeploy/

QUESTION NO: 8

회사에서 애플리케이션을 AWS로 마이그레이션하고 있습니다. 마이그레이션하는 동안 최대한 완전 관리형 서비스를 사용하고자 합니다. 회사는 다음 요구 사항을 충족하는 대규모 중요 문서를 애플리케이션 내에 저장해야 합니다.

1. 데이터는 내구성이 뛰어나고 가용성이 높아야 합니다.
2. 데이터는 저장 중 및 전송 중에 항상 암호화되어야 합니다.
3 암호화 키는 회사에서 관리해야 하며 주기적으로 교체해야 합니다. 솔루션 아키텍트는 다음 중 어떤 솔루션을 권장해야 합니까?

A. 파일 게이트웨이 모드에서 AWS에 스토리지 게이트웨이 배포 AWS KMS 키를 사용하여 Amazon EBS 볼륨 암호화를 사용하여 스토리지 게이트웨이 볼륨을 암호화합니다.

B. 버킷 정책과 함께 Amazon S3를 사용하여 버킷에 대한 연결에 HTTPS를 적용하고 객체 암호화에 서버 측 암호화와 AWS KMS를 적용합니다.

C. SSL을 사용하여 Amazon DynamoDB를 사용하여 DynamoDB에 연결합니다. AWS KMS 키를 사용하여 저장 중인 DynamoDB 객체를 암호화합니다.

D. 이 데이터를 저장하기 위해 Amazon EBS 볼륨이 연결된 인스턴스를 배포합니다. AWS KMS 키를 사용하여 EBS 볼륨 암호화를 사용하여 데이터를 암호화합니다.

Answer: B

QUESTION NO: 9
한 회사가 단일 Amazon EC2 인스턴스에서 중요한 애플리케이션을 호스팅하고 있습니다. 이 애플리케이션은 인 메모리 데이터 스토어를 위해 Redis 단일 노드 클러스터용 Amazon ElastiCache를 사용합니다. 이 애플리케이션은 관계형 데이터베이스에 Amazon RDS for MariaDB DB 인스턴스를 사용합니다. 애플리케이션이 작동하려면 인프라의 각 부분이 정상이어야 하고 활성 상태여야 합니다.
솔루션 설계자는 애플리케이션의 아키텍처를 개선하여 인프라가 가동 중지 시간을 최소화하면서 장애로부터 자동으로 복구할 수 있도록 해야 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)
A. Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽을 분산합니다. EC2 인스턴스가 최소 용량이 인스턴스 2개인 Auto Scaling 그룹의 일부인지 확인합니다.
B. Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽 분산 EC2 인스턴스가 무제한 모드로 구성되었는지 확인합니다.
C. 동일한 가용 영역에 읽기 전용 복제본을 생성하도록 DB 인스턴스를 수정합니다. 장애 시나리오에서 읽기 전용 복제본을 기본 DB 인스턴스로 승격합니다.
D. 두 가용 영역에 걸쳐 확장되는 다중 AZ 배포를 생성하도록 DB 인스턴스를 수정합니다.
E. Redis 클러스터용 ElastiCache에 대한 복제 그룹을 생성합니다. 최소 용량이 인스턴스 2개인 Auto Scaling 그룹을 사용하도록 클러스터를 구성합니다.
F. Redis 클러스터용 ElastiCache에 대한 복제 그룹을 생성합니다. 클러스터에서 다중 AZ를 활성화합니다.
Answer: A D F
Explanation:
Option A is correct because using an Elastic Load Balancer and an Auto Scaling group with a minimum capacity of two instances can improve the availability and scalability of the EC2 instances that host the application. The load balancer can distribute traffic across multiple instances and the Auto Scaling group can replace any unhealthy instances automatically1 Option D is correct because modifying the DB instance to create a Multi-AZ deployment that extends across two Availability Zones can improve the availability and durability of the RDS for MariaDB database. Multi- AZ deployments provide enhanceddata protection and minimize downtime by automatically failing over to astandby replica in another Availability Zone in case of a planned or unplanned outage4 Option F is correct because creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ on the cluster can improve the availability and fault tolerance of the in-memory data store. A replication group consists of a primary node and up to five read-only replica nodes that are synchronized with the primary node using asynchronous replication. Multi-AZ allows automatic failover to one of the replicas if the primary node fails or becomes unreachable6 References: 1: https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing- works.html 2: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances- unlimited-mode.html 3: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html 4: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html 5: https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoScaling.html 6: https://docs.aws.amazon.com /AmazonElastiCache/latest/red-ug/Replication.Redis.Groups.html

QUESTION NO: 10
한 회사가 온프레미스 인프라와 AWS 간에 전용 연결을 설정하려고 합니다. 이 회사는 계정 VPC에 1Gbps AWS Direct Connect 연결을 설정하고 있습니다. 이 아키텍처에는 여러 VPC와 온프레미스 인프라를 연결하는 전송 게이트웨이와 Direct Connect 게이트웨이가 포함됩니다. 회사는 Direct Connect 연결을 사용하여 전송 VIF를 통해 VPC 리소스에 연결해야 합니다.
이러한 요구 사항을 충족하려면 어떤 단계 조합이 필요합니까? (두 가지를 선택하세요.)
A. 1Gbps 직접 연결 연결을 10Gbps로 업데이트합니다.
B. 전송 VIF를 통해 온프레미스 네트워크 접두사를 광고합니다.
C. 전송 VIF를 통해 Direct Connect 게이트웨이에서 온프레미스 네트워크로 VPC 접두사를 변경합니다.
D. Direct Connect 연결의 MACsec 암호화 모드 속성을 반드시 암호화하도록 업데이트합니다.
E. MACsec 연결 키 이름-연결 연관 키(CKN/CAK) 쌍을 직접 연결 연결과 연결합니다.
Answer: B C
Explanation:
To connect VPC resources over a transit Virtual Interface (VIF) using a Direct Connect connection, the company should advertise the on-premises network prefixes over the transit VIF and advertise the VPC prefixes from the Direct Connect gateway to the on-premises network over the same VIF. This configuration ensures seamless connectivity between the on-premises infrastructure and the AWS VPCs through the transit gateway, facilitating efficient and secure communication across the network.
AWS Documentation on AWS Direct Connect and transit gateways provides detailed instructions on configuring transit VIFs and routing for Direct Connect connections. This setup is recommended in AWS best practices for establishing dedicated network connections between on-premises environments and AWS to achieve low-latency, high-throughput, and secure connectivity.

QUESTION NO: 11
한 회사가 VPC 내부의 Amazon EC2 인스턴스에 새로운 프라이빗 인트라넷 서비스를 배포할 계획입니다. AWS 사이트 간 VPN은 VPC를 회사의 온프레미스 네트워크에 연결합니다.
새로운 서비스는 기존 온프레미스 서비스와 통신해야 합니다. 온프레미스 서비스는 회사 예제 DNS 영역에 있는 호스트 이름을 사용하여 액세스할 수 있습니다. 이 DNS 영역은 전적으로 온프레미스에서 호스팅되며 회사의 프라이빗 네트워크에서만 사용할 수 있습니다.
솔루션 아키텍트는 새로운 서비스가 기존 서비스와 통합되기 위해 회사 예시 도메인의 호스트 이름을 확인할 수 있는지 확인해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. 회사 예제를 위한 Amazon Route 53에 빈 개인 영역 만들기 Route 53의 새 개인 영역에 대한 권한 있는 이름 서버를 가리키는 회사의 온프레미스 회사 예제 영역에 추가 NS 레코드를 추가합니다.
B. VPC에 대한 DNS 호스트 이름 켜기 Amazon Route 53 Resolver로 새 아웃바운드 엔드포인트 구성. 회사 예제에 대한 요청을 온프레미스 이름 서버로 전달하기 위한 Resolver 규칙 생성
C. VPC에 대한 DNS 호스트 이름 켜기 Amazon Route를 사용하여 새로운 인바운드 리졸버 엔드포인트 구성
53 Resolver. 온프레미스 DNS 서버를 구성하여 회사 예제에 대한 요청을 새 Resolver로

전달합니다.

D. AWS Systems Manager를 사용하여 필요한 호스트 이름이 포함된 호스트 파일을 설치하는 실행 문서를 구성합니다. Amazon EventBndge 규칙을 사용하여 인스턴스가 실행 상태로 전환될 때 문서를 실행합니다.

Answer: B

Explanation:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html

QUESTION NO: 12

한 회사가 AWS 클라우드에서 워크로드를 실행하고 있습니다. 이 회사는 애플리케이션 데이터를 이전 버전의 Amazon DocumentDB에 저장합니다. 여러 백엔드 서비스가 24시간 내내 데이터베이스에서 데이터를 지속적으로 읽고 씁니다. 모든 서비스는 Amazon Route 53에 DNS 레코드로 등록된 Amazon DocumentDB 클러스터 엔드포인트를 사용하여 데이터베이스에 연결합니다.

해당 회사는 데이터 손실 없이 데이터베이스를 최신 버전의 Amazon DocumentDB로 업그레이드해야 합니다. 또한, 백엔드 서비스에서 업그레이드된 버전을 사용하기 전에 업그레이드 테스트 및 검증을 완료해야 합니다. 회사는 이미 변경 스트림을 활성화하고 24시간의 보존 기간을 설정했습니다.

어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. 최신 버전의 Amazon DocumentDB 클러스터를 새로 생성합니다. Amazon DocumentDB 인덱스 도구를 사용하여 기존 인덱스를 내보내고 새 클러스터로 가져옵니다. 새 AWS DMS 인스턴스와 소스 및 대상 엔드포인트를 생성합니다. '마이그레이션 및 복제' 마이그레이션 유형을 사용하여 데이터를 마이그레이션하는 DMS 작업을 생성합니다. 새 클러스터를 테스트하고 확인합니다. Route 53 레코드를 업데이트하여 새 클러스터를 가리키도록 합니다.

B. 최신 버전의 Amazon DocumentDB 클러스터를 새로 생성합니다. Amazon EC2 인스턴스에 MongoDB 명령줄 인터페이스(CLI) 데이터베이스 도구를 설치합니다. MongoDB CLI를 사용하여 바이너리 내보내기를 생성하고 새 Amazon DocumentDB 클러스터로 데이터를 가져옵니다. 새 클러스터를 테스트하고 검증합니다. Route 53 레코드를 업데이트하여 새 클러스터를 가리키도록 합니다.

C. 기존 Amazon DocumentDB 클러스터의 스냅샷을 생성합니다. 제자리에서 주요 버전 업그레이드를 수행합니다. 기존 클러스터를 최신 버전 및 최신 클러스터 파라미터 그룹으로 수정합니다. 수정 사항을 즉시 적용합니다. 업그레이드를 테스트하고 확인합니다.

D. 최신 버전의 Amazon DocumentDB 클러스터를 새로 생성합니다. AWS DataSync 에이전트를 Amazon EC2 인스턴스에 배포하고 활성화합니다. 향상된 모드로 AWS DataSync 작업을 새로 생성합니다. 전송 작업을 시작하여 데이터를 새 클러스터로 복사합니다. 새 클러스터를 테스트하고 확인합니다. Route 53 레코드를 업데이트하여 새 클러스터를 가리키도록 합니다.

Answer: A

Explanation:

The company needs to upgrade DocumentDB to the latest version with no data loss while allowing continuous reads and writes. The company also must be able to test and verify the upgrade before switching production traffic. This is a classic requirement for performing an upgrade using a blue/green approach: build a new target environment on the new version, keep it in sync with the source, validate it, and then cut over by changing the endpoint (here, Route 53 DNS).

Option A implements this pattern using a new DocumentDB cluster running the latest version and AWS DMS to continuously migrate and replicate changes from the old cluster to the new cluster. Because the workload is continuously changing, a one-time export/import is insufficient; continuous replication is needed to keep the target cluster current during the test period. AWS DMS supports a "migrate and replicate" style of task that performs a full load and then applies ongoing changes (CDC) so the target stays synchronized. The question also states that change streams are enabled with a 24-hour retention period, which supports capturing and applying changes during migration/validation and helps ensure the replication stream can be maintained while testing.
Option A also addresses indexes by using the DocumentDB Index Tool to export and import indexes, which is important because indexes can affect query performance and behavior. After the company validates the new cluster, the cutover is done by updating the Route 53 record to point to the new cluster endpoint, switching all backend services without changing application configuration beyond DNS resolution.
Option B uses MongoDB CLI tools to export/import. This is not suitable for continuous write workloads because export/import is a point-in-time operation and would require downtime or risk data divergence during the test period. It also adds more operational overhead and does not provide continuous replication for the duration of validation.
Option C performs an in-place major version upgrade. That does not satisfy the requirement to test and verify the upgrade before backend services use the upgraded version because the upgrade happens directly on the production cluster. Even though a snapshot exists for rollback, production is still exposed to the upgrade immediately, which violates the requirement for pre-cutover verification.
Option D is incorrect because AWS DataSync transfers files between storage systems such as NFS/SMB and AWS storage services. It is not a database migration or replication service and cannot copy a DocumentDB database in a way that preserves database semantics and supports continuous replication.
Therefore, creating a new DocumentDB cluster, keeping it synchronized using AWS DMS (supported by change stream retention), validating it, and then cutting over via Route 53 DNS update (option A) meets all requirements.
References:
AWS documentation on blue/green style database upgrades by migrating to a new cluster and cutting over via DNS.
AWS documentation on AWS DMS full load plus ongoing replication (CDC) patterns for minimizing downtime and maintaining target synchronization during validation.
AWS documentation on Amazon DocumentDB change streams and retention considerations for capturing ongoing changes during migration windows.

QUESTION NO: 13
회사에서 AWS로 마이그레이션하려고 합니다. 이 회사는 VMware ESXi 환경에서 수천 개의 VM을 실행하고 있습니다. 이 회사는 구성 관리 데이터베이스가 없으며 VMware 포트폴리오 활용에 대한 지식이 거의 없습니다.
솔루션 설계자는 회사가 비용 효율적인 마이그레이션을 계획할 수 있도록 회사에 정확한 인벤토리를 제공해야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Systems Manager Patch Manager를 사용하여 Migration Evaluator를 각 VM에 배포합니다. Amazon QuickSight에서 수집된 데이터를 검토합니다. 사용률이 높은 서버를 식별합니다. 마이그레이션 목록에서 사용률이 높은 서버를 제거합니다. 데이터를 AWS Migration Hub로 가져옵니다.

B. VMware 포트폴리오를 csv 파일로 내보냅니다. 각 서버의 디스크 사용률을 확인하십시오. 사용률이 높은 서버를 제거합니다. 데이터를 AWS Application Migration Service로 내보냅니다. AWS Server Migration Service(AWS SMS)를 사용하여 나머지 서버를 마이그레이션합니다.

C. Migration Evaluator 에이전트 없는 수집기를 ESXi 하이퍼바이저에 배포합니다. Migration Evaluator에서 수집된 데이터를 검토합니다. 비활성 서버를 식별합니다. 마이그레이션 목록에서 비활성 서버를 제거하십시오. 데이터를 AWS Migration Hub로 가져옵니다.

D. 각 VM에 AWS Application Migration Service 에이전트를 배포합니다. 데이터가 수집되면 Amazon Redshift를 사용하여 데이터를 가져와 분석합니다. 데이터 시각화를 위해 Amazon QuickSight를 사용하십시오.

Answer: C

Explanation:

https://aws.amazon.com/migration-evaluator/features/

QUESTION NO: 14

솔루션 아키텍트가 기존에 수동으로 생성한 비프로덕션 AWS 환경에서 AWS CloudFormation 템플릿을 만들고 있습니다. CloudFormation 템플릿은 필요에 따라 폐기하고 다시 생성할 수 있습니다. 해당 환경에 Amazon EC2 인스턴스가 포함되어 있습니다. EC2 인스턴스에는 EC2 인스턴스가 부모 계정에서 역할을 맡는 데 사용하는 인스턴스 프로필이 있습니다. 솔루션 아키텍트가 CloudFormation 템플릿에서 역할을 다시 생성하고 동일한 역할 이름을 사용합니다. 자식 계정에서 CloudFormation 템플릿이 시작되면 EC2 인스턴스는 권한이 부족하여 더 이상 부모 계정에서 역할을 맡을 수 없습니다. 솔루션 아키텍트는 이 문제를 해결하기 위해 무엇을 해야 합니까?

A. 부모 계정에서 EC2 인스턴스가 가정해야 하는 역할에 대한 신뢰 정책을 편집합니다. sts AssumeRole 작업을 허용하는 기존 명령문의 대상 역할 ARN이 올바른지 확인합니다. 신뢰 정책을 저장합니다.

B. 부모 계정에서 EC2 인스턴스가 가정해야 하는 역할에 대한 신뢰 정책을 편집합니다. 자식 계정의 루트 주체에 대해 sts AssumeRole 작업을 허용하는 명령문을 추가합니다. 신뢰 정책을 저장합니다.

C. CloudFormation 스택을 다시 업데이트합니다. CAPABILITY_NAMED_IAM 기능만 지정합니다.

D. CloudFormation 스택을 다시 업데이트합니다. CAPABIUTYJAM 기능과 CAPABILITY_NAMEDJAM 기능을 지정합니다.

Answer: A

Explanation:

Edit the Trust Policy:

Go to the IAM console in the parent account and locate the role that the EC2 instance needs to assume.

Edit the trust policy of the role to ensure that it correctly allows the sts action for the role ARN in the child account.

Update the Role ARN:
Verify that the target role ARN specified in the trust policy matches the role ARN created by the CloudFormation stack in the child account.
If necessary, update the ARN to reflect the correct role in the child account.
Save and Test:
Save the updated trust policy and ensure there are no syntax errors.
Test the setup by attempting to assume the role from the EC2 instance in the child account.
Verify that the instance can successfully assume the role and perform the required actions.
This ensures that the EC2 instance in the child account can assume the role in the parent account, resolving the permission issue.
References
AWS IAM Documentation on Trust Policies#51#.

QUESTION NO: 15
한 회사가 대도시 전역의 교통 패턴을 모니터링하는 IoT 센서를 보유하고 있습니다. 이 회사는 센서에서 데이터를 읽고 수집하여 데이터에 대한 집계를 수행하려고 합니다.
솔루션 아키텍트는 IoT 기기가 Amazon Kinesis Data Streams로 스트리밍되는 솔루션을 설계합니다. 여러 애플리케이션이 스트림에서 읽고 있습니다. 그러나 여러 소비자가 제한을 겪고 있으며 주기적으로 RealProvisioned Throughput Exceeded 오류가 발생합니다.
이 문제를 해결하기 위해 솔루션 아키텍트는 어떤 조치를 취해야 합니까? (3가지를 선택하세요.)
A. 스트림을 재분할하여 스트림의 샤드 수를 늘립니다.
B. Kinesis Producer Library KPL을 사용합니다. 폴링 빈도를 조정합니다.
C. 향상된 팬아웃 기능을 갖춘 소비자를 활용하세요.
D. 스트림을 재분할하여 스트림의 샤드 수를 줄입니다.
E. 소비자 로직에서 오류 재시도 및 지수 백오프 메커니즘을 사용합니다.
F. 동적 분할을 사용하도록 스트림을 구성합니다.
Answer: A C E
Explanation:
https://repost.aws/knowledge-center/kinesis-readprovisionedthroughputexceeded Follow Data Streams best practices To mitigate ReadProvisionedThroughputExceeded exceptions, apply these best practices:
* Reshard your stream to increase the number of shards in the stream.
* Use consumers with enhanced fan-out. For more information about enhanced fan-out, see Developing custom consumers with dedicated throughput (enhanced fan-out).
* Use an error retry and exponential backoff mechanism in the consumer logic if ReadProvisionedThroughputExceeded exceptions are encountered. For consumer applications that use an AWS SDK, the requests are retried by default.

QUESTION NO: 16
질문:
한 회사가 Amazon EC2와 AWS Lambda에서 애플리케이션을 실행합니다. 이 애플리케이션은 Amazon S3에 임시 데이터를 저장합니다. S3 객체는 24시간 후에 삭제됩니다.
회사는 AWS CloudFormation 스택을 실행하여 새 버전의 애플리케이션을 배포합니다. 스택은 필요한 리소스를 생성합니다. 새 버전의 유효성을 검사한 후 회사는 이전 스택을 삭제합니다.

최근 이전 개발 스택을 삭제하는 데 실패했습니다.
솔루션 아키텍트는 주요 아키텍처 변경 없이 이 문제를 해결해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. S3 버킷에서 객체를 삭제하는 Lambda 함수를 생성합니다. Lambda 함수를 CloudFormation 스택에 사용자 지정 리소스로 추가하고, S3 버킷 리소스를 가리키는 DependsOn 속성을 추가합니다.

B. CloudFormation 스택을 수정하여 S3 버킷에 Delete 값을 갖는 DeletionPolicy 속성을 연결합니다.

C. S3 버킷 리소스에 대한 스냅샷 값을 갖는 DeletionPolicy 속성을 추가하기 위해 CloudFormation 스택을 업데이트합니다.

D. CloudFormation 템플릿을 업데이트하여 Amazon S3 대신 임시 파일을 저장하는 Amazon EFS 파일 시스템을 생성합니다. Lambda 함수가 EFS 파일 시스템과 동일한 VPC에서 실행되도록 구성합니다.

Answer: A

Explanation:
CloudFormation cannot delete non-empty S3 buckets. OptionAallows you to create acustom Lambda resourcethat deletes all objects in the S3 bucket before the stack deletes it. The DependsOn ensures the bucket deletion occurs only after the Lambda has completed.
B: Adding DeletionPolicy: Delete does not resolve the issue if the bucket still contains objects.
C: Snapshot doesn ' t apply to S3 and won ' t help here.
D: Changing to Amazon EFS would require architectural changes, which are not allowed per requirements.
Reference:https://aws.amazon.com/blogs/devops/safely-delete-s3-buckets-using-aws-cloudformation/https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute- deletionpolicy.html

QUESTION NO: 17
한 회사에 여러 AWS 계정이 있습니다. 개발 팀은 클라우드 거버넌스 및 문제 해결 프로세스를 위한 자동화 프레임워크를 구축하고 있습니다. 자동화 프레임워크는 중앙 집중식 계정에서 AWS Lambda 함수를 사용합니다. 솔루션 설계자는 Lambda 함수가 회사의 각 AWS 계정에서 실행될 수 있도록 허용하는 최소 권한 정책을 구현해야 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (두 가지를 선택하세요.)

A. 중앙 집중식 계정에서 Lambda 서비스를 신뢰할 수 있는 엔터티로 포함하는 IAM 역할을 생성합니다. 다른 AWS 계정의 역할을 맡도록 인라인 정책을 추가합니다.

B. 다른 AWS 계정에서 최소 권한을 가진 IAM 역할을 생성합니다. 중앙 집중식 계정의 Lambda IAM 역할을 신뢰할 수 있는 엔터티로 추가합니다.

C. 중앙 집중식 계정에서 다른 계정의 역할을 신뢰할 수 있는 엔터티로 갖는 IAM 역할을 생성합니다. 최소한의 권한을 제공합니다.

D. 다른 AWS 계정에서 중앙 집중식 계정의 역할을 맡을 수 있는 권한이 있는 IAM 역할을 생성합니다. Lambda 서비스를 신뢰할 수 있는 엔터티로 추가합니다.

E. 다른 AWS 계정에서 최소 권한이 있는 IAM 역할을 생성합니다. Lambda 서비스를 신뢰할 수 있는 엔터티로 추가합니다.

Answer: A B

Explanation:
https://medium.com/@it.melnichenko/invoke-a-lambda-across-multiple-aws-accounts-8c094b2e70be

QUESTION NO: 18
질문:
한 회사에는 사용자가 업로드한 비디오를 S3 Standard 스토리지를 사용하여 Amazon S3 버킷에 저장하는 애플리케이션이 있습니다. 사용자는 처음 180일 동안은 자주 비디오를 보지만 그 이후로는 거의 보지 않습니다. 대부분의 비디오는 100MB가 넘습니다. 사용자의 인터넷 연결 상태가 좋지 않은 경우가 많고, 회사는 멀티파트 업로드를 사용합니다.
솔루션 아키텍트는 S3 스토리지 비용을 최적화해야 합니다.
이러한 요구 사항을 충족하는 조치의 조합은 무엇입니까? (두 가지를 선택하세요.)
A. S3 버킷을 요청자 지불 버킷으로 구성합니다.
B. S3 전송 가속을 사용하여 비디오를 업로드합니다.
C. 완료되지 않은 멀티파트 업로드를 7일 후에 만료시키는 수명 주기 규칙을 만듭니다.
D. 1일 후 객체를 S3 Glacier Instant Retrieval로 전환하는 수명 주기 규칙을 만듭니다.
E. 180일 후에 객체를 S3 Standard-IA로 전환하는 수명 주기 규칙을 만듭니다.
Answer: C E
Explanation:
C: Multipart uploads can leave incomplete parts behind, which incur storage costs. Expiring them after 7 days minimizes waste and saves cost.
E: Since objects are infrequently accessed after 180 days, transitioning toS3 Standard-IAis cost-effective, especially for large files > 128 KB (your 100 MB+ files qualify).
Ais for shifting download cost, not reducing your S3 storage expenses.
Bhelps with upload speed butincreases cost.
Dis too aggressive; Glacier is not suited for access patterns within the first few days.
Reference:https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-configuration-examples.
htmlhttps://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html

QUESTION NO: 19
한 회사가 온 프레미스 데이터 센터를 AWS로
마이그레이션할 계획입니다 . 이 회사는 현재 Linux 기반 VMware VM에서 데이터 센터를 호스팅하고 있습니다. 솔루션 설계자는 VM 간의 네트워크 종속성에 대한 정보를 수집해야 합니다. 정보는 호스트 IP 주소, 호스트 이름 및 네트워크 연결 정보를 자세히 설명하는 다이어그램 형식이어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. AWS 애플리케이션 검색 서비스를 사용합니다. AWS Migration Hub 홈 AWS 지역을 선택합니다. 데이터 수집을 위해 온프레미스 서버에 AWS Application Discovery Agent를 설치합니다. Migration Hub 네트워크 다이어그램을 사용할 수 있도록 Application Discovery Service에 권한을 부여합니다.
B. 서버 데이터 수집을 위해 AWS Application Discovery Service Agentless Collector를 사용합니다. AWS Migration Hub에서 네트워크 다이어그램을 .png 형식으로 내보냅니다.
C. 데이터 수집을 위해 온프레미스 서버에 AWS Application Migration Service 에이전트를 설치합니다. AWS의 Workload Discovery에서 AWS Migration Hub 데이터를 사용하여

네트워크 다이어그램을 생성합니다.
D. 데이터 수집을 위해 온프레미스 서버에 AWS Application Migration Service 에이전트를 설치합니다. AWS Migration Hub의 데이터를 .csv 형식으로 Amazon CloudWatch 대시보드로 내보내 네트워크 다이어그램을 생성합니다.
Answer: A
Explanation:
To effectively gather information about network dependencies between VMs in an on-premises data center for migration to AWS, it ' s crucial to use tools that can capture detailed application and server dependencies. The AWS Application Discovery Service is designed for this purpose, particularly when migrating from environments like Linux-based VMware VMs. By installing the AWS Application Discovery Agent on the on- premises servers, the service can collect necessary data such as host IP addresses, hostnames, and network connection information. This data is crucial for creating a comprehensive network diagram that outlines the interactions and dependencies between various components of the on-premises infrastructure. The integration with AWS Migration Hub enhances this process by allowing the visualization of these dependencies in a network diagram format, aiding in the planning and execution of the migration process. This approach ensures a thorough understanding of the on-premises environment, which is essential for a successful migration to AWS.
References:
AWS Documentation on Application Discovery Service: This provides detailed guidance on how to use the Application Discovery Service, including the installation and configuration of the Discovery Agent.
AWS Migration Hub User Guide: Offers insights on how to integrate Application Discovery Service data with Migration Hub for comprehensive migration planning and tracking.
AWS Solutions Architect Professional Learning Path: Contains advanced topics and best practices for migrating complex on-premises environments to AWS, emphasizing the use of AWS services and tools for effective migration planning and execution.

QUESTION NO: 20
한 회사가 향후 3년간 진행될 프로젝트를 위해 AWS에서 애플리케이션을 호스팅하고 있습니다. 이 애플리케이션은 네트워크 로드 밸런싱(NLB) 대상 그룹에 등록된 20개의 Amazon EC2 온디맨드 인스턴스로 구성됩니다. 인스턴스는 두 개의 가용 영역에 분산되어 있습니다. 이 애플리케이션은 상태 비저장 방식이며, AWS에서 실행됩니다.
하루 24시간, 일주일 내내.
해당 회사는 사용자들이 애플리케이션 응답 속도가 느리다고 호소하는 보고를 받았습니다. 성능 지표에 따르면 일반적인 애플리케이션 사용 시 인스턴스의 CPU 사용률은 10%입니다. 하지만 사용량이 많은 시간대에는 CPU 사용률이 100%까지 치솟는데, 이러한 시간대는 보통 몇 시간 동안 지속됩니다.
회사는 애플리케이션 응답 속도 저하 문제를 해결하기 위해 새로운 아키텍처가 필요합니다.
어떤 솔루션이 이러한 요구 사항을 가장 비용 효율적으로 충족할까요?
A. 자동 스케일링 그룹을 생성합니다. 생성된 자동 스케일링 그룹을 NLB의 대상 그룹에 연결합니다. 최소 용량을 20으로, 원하는 용량을 28로 설정합니다. 예약 인스턴스를 20개 구매합니다.
B. 요청 유형이 요청인 스팟 플릿을 생성합니다. TotalTargetCapacity 매개변수를 20으로

설정합니다. DefaultTargetCapacityType 매개변수를 온디맨드로 설정합니다. 스팟 플릿을 생성할 때 NLB를 지정합니다.

C. 요청 유형이 유지 관리인 스팟 플릿을 생성합니다. TotalTargetCapacity 매개변수를 20으로 설정합니다. DefaultTargetCapacityType 매개변수를 Spot으로 설정합니다. NLB를 애플리케이션 로드 밸런서로 교체합니다.

D. 자동 스케일링 그룹을 생성합니다. 생성된 자동 스케일링 그룹을 NLB의 대상 그룹에 연결합니다. 최소 용량을 4, 최대 용량을 28로 설정합니다. 예약 인스턴스를 4개 구매합니다.

Answer: D

QUESTION NO: 21

한 회사가 자체 데이터 센터와 AWS 간의 하이브리드 솔루션을 개발했습니다. 이 회사는 Amazon VPC와 Amazon EC2 인스턴스를 사용하여 애플리케이션 로그를 Amazon CloudWatch로 전송합니다. EC2 인스턴스는 온프레미스에 호스팅된 여러 관계형 데이터베이스에서 데이터를 읽어옵니다.

이 회사는 EC2 인스턴스가 데이터베이스에 연결된 상태를 거의 실시간으로 모니터링하고자 합니다. 이미 온프레미스 Splunk를 사용하는 모니터링 솔루션을 보유하고 있으며, 솔루션 아키텍트는 네트워크 트래픽을 Splunk로 전송하는 방법을 결정해야 합니다.

솔루션 설계자는 이러한 요구 사항을 어떻게 충족해야 할까요?

A. VPC 흐름 로그를 활성화하고 CloudWatch로 전송합니다. 사전 정의된 내보내기 함수를 사용하여 CloudWatch 로그를 주기적으로 Amazon S3 버킷으로 내보내는 AWS Lambda 함수를 생성합니다. ACCESS_KEY 및 SECRET_KEY AWS 자격 증명을 생성합니다. 해당 자격 증명을 사용하여 Splunk가 S3 버킷에서 로그를 가져오도록 구성합니다.

B. Splunk를 대상으로 하는 Amazon Data Firehose 전송 스트림을 생성합니다. CloudWatch Logs 구독 필터에서 전송된 레코드에서 개별 로그 이벤트를 추출하는 Firehose 스트림 프로세서를 사용하는 사전 처리 AWS Lambda 함수를 구성합니다. VPC 흐름 로그를 활성화하고 CloudWatch로 전송합니다. Firehose 전송 스트림으로 로그 이벤트를 전송하는 CloudWatch Logs 구독을 생성합니다.

C. 회사에 데이터베이스에 대한 모든 요청과 EC2 인스턴스 IP 주소를 로그에 기록하도록 요청합니다. CloudWatch 로그를 Amazon S3 버킷으로 내보냅니다. Amazon Athena를 사용하여 데이터베이스 이름별로 그룹화된 로그를 쿼리합니다. Athena 결과를 다른 S3 버킷으로 내보냅니다. AWS Lambda 함수를 호출하여 S3 버킷에 새 파일이 추가될 때마다 Splunk로 자동으로 전송합니다.

D. CloudWatch 로그를 Amazon Managed Service for Apache Flink(이전 명칭: Amazon Kinesis Data Analytics)를 사용하여 Amazon Kinesis 데이터 스트림으로 전송합니다. 이벤트를 수집하기 위해 1분 슬라이딩 윈도우를 구성합니다. 이상 탐지 템플릿을 사용하는 SQL 쿼리를 생성하여 네트워크 트래픽 이상을 거의 실시간으로 모니터링합니다. 결과를 Splunk를 대상으로 하는 Amazon Data Firehose 전송 스트림으로 보냅니다.

Answer: B

Explanation:

The company needs near-real-time visibility into which EC2 instances are connecting to on-premises databases. The correct telemetry source for network connection metadata at the VPC level is VPC Flow Logs.

VPC Flow Logs capture information about IP traffic going to and from network interfaces in a VPC, including source/destination IPs, ports, protocol, and accept/reject decisions. This data can be used to infer which EC2 instance IPs are connecting to database IPs.

The company already uses Splunk on premises, so the solution should deliver these logs to Splunk with minimal delay and operational overhead. Amazon Data Firehose provides a fully managed way to deliver streaming data to supported destinations, including Splunk, with buffering and retry handling. CloudWatch Logs subscription filters can stream log events in near real time from CloudWatch Logs to destinations such as Firehose.
Option B uses the standard pattern: enable VPC Flow Logs to CloudWatch Logs, then create a CloudWatch Logs subscription filter that streams the flow logs to a Firehose delivery stream configured with Splunk as the destination. Because CloudWatch Logs subscription deliveries can batch log events, using a Firehose preprocessing Lambda to extract individual log events is a common approach to format records in a way that Splunk ingests cleanly. This yields near-real-time delivery with low operational overhead.
Option A introduces delay because it exports CloudWatch logs periodically to S3 and requires Splunk to poll S3. It also requires long-lived access keys and periodic batch exports, which is not near real time.
Option C relies on application-level logging changes and batch analytics with Athena, which is not near real time and requires substantial changes and additional pipelines.
Option D is over-engineered for the stated requirement. Using Flink and anomaly detection focuses on anomalies rather than simply identifying connections, and it adds significant operational complexity compared to direct delivery of flow logs to Splunk via Firehose.
Therefore, streaming VPC Flow Logs from CloudWatch Logs to Splunk using a Firehose delivery stream and a subscription filter is the best approach.
References:AWS documentation on VPC Flow Logs and the metadata they provide for network connection visibility.AWS documentation on CloudWatch Logs subscription filters for near-real-time streaming of log events.AWS documentation on Amazon Data Firehose delivery to Splunk and optional Lambda transformations for record formatting.

QUESTION NO: 22
한 회사가 Amazon Workspaces 개념 증명을 성공적으로 완료했습니다. 이제 두 AWS 지역에서 Workspaces를 매우 쉽게 사용할 수 있도록 하려고 합니다. Workspaces는 장애 조치 지역에 배포됩니다. 호스팅된 영역은 Amazon Route 53에서 사용할 수 있습니다.
솔루션 아키텍트는 무엇을 해야 하나요?
A. 기본 지역과 장애 조치 지역에 연결 별칭을 만듭니다. 각각을 해당 지역의 디렉토리와 연결합니다. Evaluate Target Health = Yes로 Route 53 장애 조치 라우팅 정책을 만듭니다.
B. 두 지역에 연결 별칭을 만듭니다. 둘 다 기본 지역의 디렉토리와 연결합니다. Route 53 다중값 답변 라우팅 정책을 사용합니다.
C. 기본 지역에서 연결 별칭을 만듭니다. 기본 지역의 디렉토리와 연결합니다.
53번 도로의 가중치가 적용된 경로를 사용하세요.
D. 기본 지역에서 연결 별칭을 만듭니다. 이를 장애 조치 지역의 디렉토리와 연결합니다.
Evaluate Target Health = Yes로 Route 53 장애 조치 라우팅을 사용합니다.
Answer: A
Explanation:
A is correct because AWS recommends using oneconnection alias per Region, associated witheach directory.
Then, configure a Route 53 failover policy so that if the primary Region becomes unhealthy, users are directed to the failover Region automatically. "Evaluate Target Health" ensures

automatic detection and failover.
References:
Amazon Workspaces Cross-Region Resilience
Route 53 Failover Routing

QUESTION NO: 23
회사에는 AWS Organizations에 조직이 있습니다. 이 회사는 AWS Control Tower를 사용하여 조직의 랜딩 존을 배포하고 있습니다. 회사는 거버넌스 및 정책 집행을 구현하려고 합니다. 회사는 회사의 프로덕션 OU에서 유휴 상태에서 암호화되지 않은 Amazon RDS DB 인스턴스를 감지하는 정책을 구현해야 합니다.
이 요구 사항을 충족하는 솔루션은 무엇입니까?
A. AWS Control Tower에서 필수 가드레일을 켭니다. 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.
Answer: B
Explanation:
AWS Control Tower provides a set of " strongly recommended guardrails " that can be enabled to implement governance and policy enforcement. One of these guardrails is " Encrypt Amazon RDS instances " which will detect RDS DB instances that are not encrypted at rest. By enabling this guardrail and applying it to the production OU, the company will be able to enforce encryption for RDS instances in the production environment.

QUESTION NO: 24
모험 회사가 모바일 앱에 새로운 기능을 출시했습니다. 사용자는 이 기능을 사용하여 언제든지 하이킹 및 래팅 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 후에 드물게 액세스된다는 것을 발견했습니다. 다만, 업로드된 사진과 영상 중 일부는 30일 이후에 자주 접속되는 경우가 있습니다. 솔루션 설계자는 가능한 가장 낮은 비용으로 사진 및 비디오의 밀리초 검색 가용성을 유지하는 솔루션을 구현해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. S3 버킷에서 S3 Intelligent-Tiering을 구성합니다.
B. 30일 후에 S3 Standard에서 S3 Glacier Deep Archive로 이미지 객체 및 비디오 객체를 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 객체 및 S3 비디오 객체에 Cache-Control: max-age 헤더를 추가합니다. 헤더를 30일로 설정합니다.
Answer: A
Explanation:

Amazon S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers based on changing access patterns. Objects that are accessed frequently are stored in the frequent access tier and objects that are accessed infrequently are stored in the infrequent access tier. This allows for cost optimization without requiring manual intervention. This makes it an ideal solution for the scenario described, as it can automatically move objects that are infrequently accessed after 30 days to a lower-cost storage tier while still maintaining millisecond retrieval availability.

QUESTION NO: 25
한 회사에서 인기 비디오 게임의 새 릴리스를 개발하여 공개 다운로드할 수 있도록 하려고 합니다. 새 릴리스 패키지의 크기는 약 5GB입니다. 회사는 온프레미스 데이터 센터에서 호스팅되는 Linux 기반 공개 FTP 사이트에서 기존 릴리스에 대한 다운로드를 제공합니다. 회사는 새 릴리스가 전 세계 사용자가 다운로드할 것으로 예상합니다. 회사는 향상된 다운로드 성능과 낮은 전송 비용을 제공하는 솔루션을 원합니다. 사용자의 위치에 관계없이 어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 탑재된 Amazon EBS 볼륨에 게임 파일을 저장합니다. EC2 인스턴스에 FTP 서비스를 구성합니다. Auto Scaling 그룹 앞에 Application Load Balancer를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시하세요.
B. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 연결된 Amazon EFS 볼륨에 게임 파일을 저장합니다. 각 EC2 인스턴스에 FTP 서비스를 구성합니다. Auto Scaling 그룹 앞에 Application Load Balancer를 사용합니다. 사용자가 패키지를 다운로드할 수 있는 게임 다운로드 URL
C. 웹 사이트 호스팅을 위해 Amazon Route 53 및 Amazon S3 버킷 구성 S3 버킷에 게임 파일 업로드 웹 사이트에 Amazon CloudFront 사용 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL 게시
D. 웹 사이트 호스팅을 위해 Amazon Route 53 및 Amazon S3 버킷 구성 S3 버킷에 게임 파일 업로드 S3 버킷에 대해 요청자 지불 설정 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL 게시
Answer: C
Explanation:
Create an S3 Bucket:
Navigate to Amazon S3 in the AWS Management Console and create a new S3 bucket to store the game files.
Enable static website hosting on this bucket.
Upload Game Files:
Upload the 5 GB game release package to the S3 bucket. Ensure that the files are publicly accessible if required for download.
Configure Amazon Route 53:
Set up a new domain or subdomain in Amazon Route 53 and point it to the S3 bucket. This allows users to access the game files using a custom URL.
Use Amazon CloudFront:
Create a CloudFront distribution with the S3 bucket as the origin. CloudFront is a content delivery network (CDN) that caches content at edge locations worldwide, improving download performance and reducing latency for users regardless of their location.

Publish the Download URL:
Use the CloudFront distribution URL as the download link for users to access the game files. CloudFront will handle the efficient distribution and caching of the content.
This solution leverages the scalability of Amazon S3 and the performance benefits of CloudFront to provide an optimal download experience for users globally while minimizing costs.
References
Amazon CloudFront Documentation
Amazon S3 Static Website Hosting

QUESTION NO: 26
AWS 계정이 여러 개인 회사에서 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 가능한 한 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 분류를 사용하여 costCenter 태그가 지정된 리소스에 대한 총 비용을 얻으십시오.
B. 조직의 회원 계정에서 costCenter 사용자 정의 태그를 활성화합니다. 월별 AWS 비용 및 사용 보고서를 구성하여 마스터 계정의 Amazon S3 버킷에 저장합니다. 월별 AWS Lambda 함수를 예약하여 보고서를 검색하고 costCenter 태그가 지정된 리소스의 총 비용을 계산합니다.
C. 조직의 구성원 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 청구 요약을 생성하도록 보고서를 구성합니다.
Answer: A
Explanation:
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.htmlhttps://docs.aws.amazon.com
/awsaccountbilling/latest/aboutv2/configurecostallocreport.html

QUESTION NO: 27
한 회사가 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 클러스터에서 메시지를 소비하는 지연 시간에 민감한 애플리케이션을 운영하고 있습니다. 이 MSK 클러스터는 세 개의 가용 영역에 걸쳐 실행됩니다.
현재 MSK 클러스터는 각 가용 영역에 두 개의 표준 대형 인스턴스를 사용하는 표준 브로커를 사용합니다.

이 회사는 브로커와 동일한 가용 영역에 배포된 Apache Kafka 클라이언트 간의 지연 시간을 최소화하고자 합니다. 또한 가용 대역폭을 늘리고 클러스터의 확장 속도를 향상시키고자 합니다. 현재 클라이언트는 기본 설정을 사용하고 있습니다. 솔루션 구현 과정에서 일시적인 다운타임은 허용됩니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?

A. 예측 스케일링 정책을 구성하고 MSK 클러스터를 대상으로 설정합니다. 대상 값을 80으로 설정하고 스케줄링 버퍼 크기를 0으로 설정합니다. Kafka 클라이언트용 배치 그룹을 구성하고 MSK 호스트를 해당 배치 그룹과 연결합니다.

B. MSK 클러스터에서 크루즈 컨트롤을 구성하고 대역폭 제어 및 재조정을 활성화합니다. 지연 시간 기반 라우팅을 사용하는 Amazon MSK Connect 프록시 계층을 배포합니다. Kafka 클라이언트가 프록시 엔드포인트를 사용하도록 재구성합니다.

C. 표준 브로커를 Express 대형 인스턴스를 사용하는 Express 브로커로 교체하십시오. Kafka 클라이언트의 client.rack 속성을 az_id로 설정하십시오.

D. 브로커 크기를 표준 xlarge 인스턴스로 조정합니다. 각 가용 영역에 MSK PrivateLink 엔드포인트를 생성합니다. 각 Kafka 클라이언트가 클라이언트와 동일한 가용 영역에 있는 엔드포인트를 사용하도록 재구성합니다.

Answer: C

Explanation:

The company wants three things: minimize client-to-broker latency within the same Availability Zone, increase available bandwidth, and increase the scaling speed of the MSK cluster. The current brokers are Standard brokers (two per AZ). Clients use default settings, which means they are not explicitly configured for rack awareness or AZ affinity.

A common way to reduce latency in multi-AZ Kafka deployments is to enable rack awareness on clients and brokers so clients prefer brokers in the same "rack," which can map to an Availability Zone. In Kafka, the client.rack setting allows the client to include rack information so the broker can return metadata that helps the client select replicas that are closest, reducing cross-AZ traffic and improving latency.

To increase bandwidth and improve scaling speed, the most direct approach in the choices is to move from Standard brokers to Express brokers. Express brokers are designed to provide higher throughput and faster scaling characteristics compared to standard broker types. Since the question explicitly calls out increasing available bandwidth and scaling speed, the broker type change is the key lever, and it can be combined with client.rack configuration to minimize cross-AZ latency.

Option C matches these requirements: it replaces Standard brokers with Express brokers (to improve throughput/bandwidth and scaling speed) and sets client.rack to the Availability Zone identifier (az_id) to improve locality and reduce latency between clients and brokers in the same AZ.

Option A is not appropriate because MSK does not use EC2 Auto Scaling predictive scaling in that manner, and Kafka clients/brokers are not "associated" with an EC2 placement group as a primary latency solution in MSK. Placement groups are for EC2 instance placement; MSK broker placement is managed by the service.

Option B introduces a proxy layer and MSK Connect in a way that increases complexity and does not directly guarantee lower latency or higher bandwidth. MSK Connect is for Kafka Connect workloads, not as a general- purpose low-latency routing proxy for Kafka clients. Cruise Control is used for partition rebalancing and cluster optimization, but it does not

replace the benefits of higher-throughput broker types and client rack awareness for AZ locality.
Option D increases broker size and introduces PrivateLink endpoints. PrivateLink is about private connectivity from VPCs to services and does not inherently ensure AZ-local broker selection or reduce latency between clients and brokers in the same AZ. Also, resizing to xlarge increases capacity but does not address scaling speed and locality as directly as express brokers plus rack configuration.
Therefore, option C best meets all requirements.
References:AWS documentation on Amazon MSK broker types, including performance and scaling characteristics of Standard and Express brokers.Apache Kafka concepts and AWS guidance on rack awareness and using client.rack to reduce cross-AZ traffic and latency in multi-AZ Kafka deployments.

QUESTION NO: 28
회사가 환경 데이터를 처리합니다. 도시의 여러 지역에서 연속적인 데이터 스트림을 제공하기 위해 센서를 설정했습니다. 데이터는 JSON 형식으로 제공됩니다.
이 회사는 AWS 솔루션을 사용하여 고정된 저장 스키마가 필요 없는 데이터베이스로 데이터를 전송하려고 합니다. 데이터는 실시간으로 전송되어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족시킬까요?
A. Amazon Kinesis Data Firehouse를 사용하여 Amazon Redshift로 데이터를 전송합니다.
B. Amazon Kinesis Data 스트림을 사용하여 데이터를 Amazon DynamoDB로 전송합니다.
C. Amazon Managed Streaming for Apache Kafka(Amazon MSK)를 사용하여 데이터를 Amazon Aurora로 전송합니다.
D. Amazon Kinesis Data Firehouse를 사용하여 Amazon Keyspaces(Apache Cassandra용)로 데이터를 전송합니다.
Answer: B
Explanation:
Amazon Kinesis Data Streams is a service that enables real-time data ingestion and processing. Amazon DynamoDB is a NoSQL database that does not require fixed schemas for storage. By using Kinesis Data Streams and DynamoDB, the company can send the JSON data to a database that can handle schemaless data in real time. References:
https://docs.aws.amazon.com/streams/latest/dev/introduction.html
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

QUESTION NO: 29
한 회사가 GitHub Actions를 사용하여 AWS 리소스에 액세스하는 CI/CD 파이프라인을 운영하고 있습니다. 이 회사에는 파이프라인에서 비밀 키를 사용하여 AWS에 인증하는 IAM 사용자가 있습니다. 연결된 정책이 있는 기존 IAM 역할은 리소스 배포에 필요한 권한을 부여합니다.
회사 보안팀은 파이프라인에서 장기 보안 키를 더 이상 사용할 수 없도록 하는 새로운 요구 사항을 구현했습니다. 솔루션 설계자는 해당 보안 키를 단기 보안 솔루션으로 교체해야 합니다.
어떤 솔루션이 운영 비용을 최소화하면서 이러한 요구 사항을 충족할 수 있을까요?
A. IAM에서 IAM SAML 2.0 ID 공급자(IdP)를 생성합니다. sts:AssumeRole API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 기존 IAM 정책을 새 IAM

역할에 연결합니다. 파이프라인에 SAML 인증을 사용하도록 GitHub을 업데이트합니다.

B. IAM에서 IAM OpenID Connect(OIDC) ID 공급자(IdP)를 생성합니다. GitHub OIDC IdP에서 sts:AssumeRoleWithWebIdentity API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 파이프라인에 대한 역할을 맡도록 GitHub을 업데이트합니다.

C. Amazon Cognito 자격 증명 풀을 생성합니다. GitHub을 사용하도록 인증 공급자를 구성합니다. GitHub 인증 공급자의 sts:AssumeRoleWithWebIdentity API 호출을 허용하는 적절한 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다. 파이프라인이 Cognito를 인증 공급자로 사용하도록 구성합니다.

D. AWS Private CA에 대한 트러스트 앵커를 생성합니다. AWS IAM Roles Anywhere에서 사용할 클라이언트 인증서를 생성합니다. sts:AssumeRole API 호출을 허용하는 적절한 트러스트 정책을 사용하여 새 IAM 역할을 생성합니다. 기존 IAM 정책을 새 IAM 역할에 연결합니다. 자격 증명 도우미 도구를 사용하고 클라이언트 인증서 공개 키를 참조하여 새 IAM 역할을 위임하도록 파이프라인을 구성합니다.

Answer: B

Explanation:

This explanation is based on AWS documentation and best practices but is paraphrased, not a literal extract.

The current CI/CD pipeline uses an IAM user with long-lived access keys stored in GitHub Actions. The new requirement is that pipelines must not use long-lived secret keys. Instead, the solution should provide short- lived credentials with minimal operational overhead.

GitHub Actions natively supports integration with cloud providers using OpenID Connect (OIDC). With OIDC, GitHub acts as an identity provider that can issue OIDC tokens to workflows. On the AWS side, IAM supports configuring an OIDC identity provider and roles that can be assumed by principals presenting valid OIDC tokens through the sts:AssumeRoleWithWebIdentity API. This pattern enables short-lived, automatically rotated credentials for CI/CD jobs without storing long-lived secrets.

In the correct solution (option B), you configure an IAM OIDC identity provider for GitHub in the AWS account. You then create a new IAM role with a trust policy that allows the Github OIDC provider to call sts:

AssumeRoleWithWebIdentity, with conditions that restrict which repositories or workflows can assume the role. The existing IAM policy that grants deployment permissions is attached to that role. In GitHub Actions, you update the pipeline configuration to request an OIDC token and assume the IAM role at runtime. Each workflow run receives short-lived credentials without storing static keys, and AWS automatically handles the token verification and temporary credential issuance. This approach is the AWS-recommended pattern for integrating GitHub Actions with AWS without long-lived secrets and has low operational overhead once configured.

Option A uses SAML 2.0, which is typically used for enterprise single sign-on for users, not for GitHub Actions workflows. GitHub does not natively use SAML to obtain AWS credentials for CI/CD pipelines in the same streamlined way as OIDC, and implementing a SAML-based integration would add unnecessary complexity.

Option C introduces Amazon Cognito as an indirection layer. Although Cognito can federate with external identity providers, including social providers, using it as an intermediary to obtain temporary AWS credentials for a machine-to-machine CI/CD pipeline is not necessary when IAM OIDC federation with GitHub is directly supported. This adds additional

configuration and operational overhead.
Option D uses IAM Roles Anywhere with client certificates from AWS Private CA. Roles Anywhere is designed for workloads running outside AWS that need to assume IAM roles using X.509 certificates instead of access keys. While technically possible, it requires managing private certificates, trust anchors, and a credential helper tool, which is more complex and operationally heavier than the direct OIDC integration specifically designed for GitHub Actions.
Therefore, configuring an IAM OIDC identity provider for GitHub and creating an IAM role to be assumed via sts:AssumeRoleWithWebIdentity (option B) meets the requirement to replace long-lived secret keys with short-lived credentials with the least operational overhead .
References:AWS documentation on configuring IAM OpenID Connect identity providers and roles for GitHub Actions integration.AWS security best practices recommending federation and temporary credentials over long-lived IAM user access keys for CI/CD pipelines.

QUESTION NO: 30
회사에서 다른 공급업체로부터 가전제품을 구입했습니다. 어플라이언스에는 모두 IoT 센서가 있습니다. 센서는 정보를 JSON으로 구문 분석하는 레거시 응용 프로그램에 공급업체의 독점 형식으로 상태 정보를 보냅니다. 구문 분석은 간단하지만 각 공급업체마다 고유한 형식이 있습니다. 애플리케이션은 매일 한 번 모든 JSON 레코드를 구문 분석하고 분석을 위해 레코드를 관계형 데이터베이스에 저장합니다.
회사는 더 빠르게 제공하고 비용을 최적화할 수 있는 새로운 데이터 분석 솔루션을 설계해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. IoT 센서를 AWS IoT Core에 연결합니다. AWS Lambda 함수를 호출하여 정보를 구문 분석하고 .csv 파일을 Amazon S3에 저장하는 규칙을 설정합니다. AWS Glue를 사용하여 파일을 분류합니다. 분석을 위해 Amazon Athena 및 Amazon QuickSight를 사용합니다.
B. 애플리케이션 서버를 AWS Fargate로 마이그레이션하면 IoT 센서에서 정보를 수신하고 정보를 관계형 형식으로 구문 분석합니다. 분석을 위해 구문 분석된 정보를 Amazon Redshift에 저장합니다.
C. SFTP 서버용 AWS 전송을 생성합니다. SFTP를 통해 정보를 .csv 파일로 서버에 전송하도록 IoT 센서 코드를 업데이트합니다. AWS Glue를 사용하여 파일을 분류합니다. Amazon Athena를 사용하여 분석하십시오.
D. AWS Snowball Edge를 사용하여 IoT 센서에서 직접 데이터를 수집하여 로컬 분석을 수행합니다. 정기적으로 데이터를 Amazon Redshift로 수집하여 글로벌 분석을 수행합니다.
Answer: A
Explanation:
Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis. This solution meets the requirement of faster analysis and cost optimization by using AWS IoT Core to collect data from the IoT sensors in real-time and then using AWS Glue and Amazon Athena for efficient data analysis.
This solution involves connecting the IoT sensors to the AWS IoT Core, setting a rule to invoke an AWS Lambda function to parse the information, and saving a .csv file to Amazon

S3. AWS Glue can be used to catalog the files and Amazon Athena and Amazon QuickSight can be used for analysis. This solution will enable faster and more cost-effective data analysis.
This solution is in line with the official Amazon Textbook and Resources for the AWS Certified Solutions Architect - Professional certification. In particular, the book states that: "AWS IoT Core can be used to ingest and process the data, AWS Lambda can be used to process and transform the data, and Amazon S3 can be used to store the data. AWS Glue can be used to catalog and access the data, Amazon Athena can be used to query the data, and Amazon QuickSight can be used to visualize the data." (Source:https://d1.awsstatic.com /training-and-certification/docs-sa-pro /AWS_Certified_Solutions_Architect_Professional_Exam_Guide_EN_v1.5.pdf)

QUESTION NO: 31
회사에서 각 사업부에 대한 내부 클라우드 청구 전략을 변경하려고 합니다. 현재 클라우드 거버넌스팀은 전체 클라우드 지출에 대한 보고서를 각 사업부장과 공유하고 있다. 회사는 각 사업부에 대해 별도의 AWS 계정을 관리하기 위해 AWS Organizations를 사용합니다. 조직의 기존 태깅 표준에는 애플리케이션, 환경 및 소유자가 포함됩니다. 클라우드 거버넌스 팀은 각 사업부가 클라우드 지출에 대한 월별 보고서를 받을 수 있도록 중앙 집중식 솔루션을 원합니다. 또한 솔루션은 설정된 임계값을 초과하는 모든 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 비용 탐색기를 사용하여 각 비즈니스 단위에 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 비용 탐색기를 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 계정에서 AWS Billing and Cost Management 대시보드를 사용하여 각 비즈니스 단위에 대한 월별 보고서를 생성합니다.
D. 조직의 마스터 계정에서 AWS 비용 및 사용 보고서를 활성화하고 애플리케이션, 환경 및 소유자별로 그룹화된 보고서를 구성합니다. AWS 비용 및 사용 보고서를 처리하고, 예산 알림을 보내고, 각 사업부의 이메일 목록에 월별 보고서를 보내는 AWS Lambda 함수를 생성합니다.
Answer: B
Explanation:
Configure AWS Budgets in the organization # €™s master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization # €™s master account to create monthly reports for each business unit.
https://aws.amazon.com/about-aws/whats-new/2019/07/introducing-aws-budgets-reports/#:~:text=AWS% 20Budgets%20gives%20you%20the,below%20the%20threshold%20you%20define

QUESTION NO: 32
회사에서 새로운 웹 기반 애플리케이션을 배포하고 있으며 Linux 애플리케이션 서버용 스토리지 솔루션이 필요합니다. 회사는 모든 인스턴스에 대한 애플리케이션 데이터 업데이트를 위한 단일 위치를 생성하려고 합니다. 활성 데이터 세트의 크기는 최대 100GB입니다. 솔루션 설계자는 매일 3시간 동안 최대 작업이 발생하고 총 225MiBps의 읽기 처리량이 필요하다고 결정했습니다.
솔루션 설계자는 재해 복구(DR)를 위해 다른 AWS 리전에서 사용할 수 있는 데이터 사본을 만드는 다중 AZ 솔루션을 설계해야 합니다. DR 사본의 RPO는 1시간 미만입니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. 새로운 Amazon Elastic File System(Amazon EFS) 다중 AZ 파일 시스템을 배포합니다. 프로비저닝된 처리량의 75MiBps에 대해 파일 시스템을 구성합니다. DR 지역의 파일 시스템에 대한 복제를 구현합니다.
B. 새로운 Amazon FSx for Lustre 파일 시스템을 배포합니다. 파일 시스템에 대한 버스팅 처리량 모드를 구성합니다. AWS Backup을 사용하여 파일 시스템을 DR 리전에 백업합니다.
C. 처리량이 225MiBps인 범용 SSD(gp3) Amazon Elastic Block Store(Amazon EBS) 볼륨을 배포합니다. EBS 볼륨에 대해 다중 연결을 활성화합니다. AWS Elastic Disaster Recovery를 사용하여 EBS 볼륨을 DR 리전에 복제합니다.
D. 프로덕션 리전과 DR 리전 모두에 Amazon FSx for OpenZFS 파일 시스템을 배포합니다. 10분마다 프로덕션 파일 시스템에서 DR 파일 시스템으로 데이터를 복제하는 AWS DataSync 예약 작업을 생성합니다.
Answer: A
Explanation:
The company should deploy a new Amazon Elastic File System (Amazon EFS) Multi-AZ file system. The company should configure the file system for 75 MiBps of provisioned throughput. The company should implement replication to a file system in the DR Region. This solution will meet the requirements because Amazon EFS is a serverless, fully elastic file storage service that lets you share file data without provisioning or managing storage capacity and performance. Amazon EFS is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files1. By deploying a new Amazon EFS Multi-AZ file system, the company can create a single location for updates to application data for all instances. A Multi-AZ file system replicates data across multiple Availability Zones (AZs) within a Region, providing high availability and durability2. By configuring the file system for 75 MiBps of provisioned throughput, the company can ensure that it meets the peak operations requirement of 225 MiBps of read throughput. Provisioned throughput is a feature that enables you to specify a level of throughput that the file system can drive independent of the file system's size or burst credit balance3. By implementing replication to a file system in the DR Region, the company can make a copy of the data available in another AWS Region for disaster recovery. Replication is a feature that enables you to replicate data from one EFS file system to another EFS file system across AWS Regions. The replication process has an RPO of less than 1 hour.
The other options are not correct because:
Deploying a new Amazon FSx for Lustre file system would not provide a single location for updates to application data for all instances. Amazon FSx for Lustre is a fully managed

service that provides cost- effective, high-performance storage for compute workloads. However, it does not support concurrent write access from multiple instances. Using AWS Backup to back up the file system to the DR Region would not provide real-time replication of data. AWS Backup is a service that enables you to centralize and automate data protection across AWS services. However, it does not support continuous data replication or cross-Region disaster recovery.
Deploying a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume with 225 MiBps of throughput would not provide a single location for updates to application data for all instances.
Amazon EBS is a service that provides persistent block storage volumes for use with Amazon EC2 instances.
However, it does not support concurrent access from multiple instances, unless Multi-Attach is enabled.
Enabling Multi-Attach for the EBS volume would not provide Multi-AZ resilience or cross-Region replication. Multi-Attach is a feature that enables you to attach an EBS volume to multiple EC2 instances within the same Availability Zone. Using AWS Elastic Disaster Recovery to replicate the EBS volume to the DR Region would not provide real-time replication of data. AWS Elastic Disaster Recovery (AWS DRS) is a service that enables you to orchestrate and automate disaster recovery workflows across AWS Regions.
However, it does not support continuous data replication or sub-hour RPOs.
Deploying an Amazon FSx for OpenZFS file system in both the production Region and the DR Region would not be as simple or cost-effective as using Amazon EFS. Amazon FSx for OpenZFS is a fully managed service that provides high-performance storage with strong data consistency and advanced data management features for Linux workloads. However, it requires more configuration and management than Amazon EFS, which is serverless and fully elastic. Creating an AWS DataSync scheduled task to replicate the data from the production file system to the DR file system every 10 minutes would not provide real-time replication of data.
AWS DataSync is a service that enables you to transfer data between on-premises storage and AWS services, or between AWS services. However, it does not support continuous data replication or sub-minute RPOs.
References:
https://aws.amazon.com/efs/
https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-azs
https://docs.aws.amazon.com/efs/latest/ug/performance.html#provisioned-throughput
https://docs.aws.amazon.com/efs/latest/ug/replication.html
https://aws.amazon.com/fsx/lustre/
https://aws.amazon.com/backup/
https://aws.amazon.com/ebs/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html

QUESTION NO: 33
한 회사의 웹 애플리케이션은 Amazon API Gateway API, AWS Lambda 함수, Amazon DynamoDB 글로벌 테이블을 사용하여 백엔드 요청을 처리합니다. 이 웹 애플리케이션은 액티브-패시브 모델로 두 개의 AWS 리전에 배포됩니다. 회사는 DNS를 위해 Amazon Route 53을 사용합니다. 웹 애플리케이션은 보조 리전으로 장애 조치(failover)하기 위해 수동 DNS

업데이트가 필요합니다. 분석 Lambda 함수는 동일한 AWS 계정에서 실행됩니다. 이 함수로 인해 Lambda 동시성이 평균적으로 현재 할당량의 90%에 도달했습니다. 최근 분석 워크로드 트래픽이 급증하여 Lambda 요청이 제한되고 웹 애플리케이션 사용자에게 열악한 사용자 환경이 발생했습니다. 솔루션 아키텍트는 웹 애플리케이션의 안정성을 높여야 합니다. 솔루션은 Lambda 동시성이 특정 사용률 임계값에 도달하면 Amazon CloudWatch 알람을 사용하여 Amazon SNS 알림을 전송해야 합니다. 운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇일까요?

A. 웹 애플리케이션 Lambda 함수에 예약된 동시성을 설정합니다. Route 53 상태 확인 및 장애 조치 레코드를 구현하여 트래픽을 보조 리전으로 라우팅합니다. AWS Trusted Advisor ServiceLimitUsage 지표를 사용하고 SNS 알림을 전송하도록 CloudWatch 알람을 구성합니다.

B. 웹 애플리케이션 Lambda 함수에 예약된 동시성을 설정합니다. Route 53 상태 확인 및 지연 시간 레코드를 구현하여 트래픽을 보조 리전으로 라우팅합니다. CloudWatch 알람이 AWS Trusted Advisor ServiceLimitUsage 지표를 사용하고 SNS 알림을 전송하도록 구성합니다.

C. 웹 애플리케이션 Lambda 함수에 프로비저닝된 동시성을 설정합니다. Route 53 상태 확인 및 장애 조치 레코드를 구현하여 트래픽을 보조 리전으로 라우팅합니다. Lambda ConcurrentExecutions 지표를 사용하고 SNS 알림을 전송하도록 CloudWatch 알람을 구성합니다.

D. 웹 애플리케이션 Lambda 함수에 프로비저닝된 동시성을 설정합니다. Route 53 상태 확인 및 지리적 위치 기록을 구현하여 트래픽을 보조 리전으로 라우팅합니다. Lambda ProvisionedConcurrencyInvocations 지표를 사용하고 SNS 알림을 전송하도록 CloudWatch 알람을 구성합니다.

Answer: C

Explanation:

The use of provisioned concurrency ensures the web application's Lambda functions have pre-initialized execution environments, removing cold start latency and maintaining performance during high-traffic periods.

Route 53 health checks and failover records automate DNS failover to the secondary Region, improving application availability and reliability.

The CloudWatch alarm is configured to monitor the Lambda ConcurrentExecutions metric and send an SNS notification if concurrency usage nears the limit, enabling quick operational response.

This approach minimizes manual management, ensuring reliability and performance during peak traffic while meeting best practices for AWS Lambda and Route 53 failover.

QUESTION NO: 34

회사에서 여러 Amazon DynamoDB 테이블에 데이터를 저장하고 있습니다. 솔루션 설계자는 서버리스 아키텍처를 사용하여 HTTPS를 통한 간단한 API를 통해 공개적으로 데이터에 액세스할 수 있도록 해야 합니다. 솔루션은 수요에 따라 자동으로 확장되어야 합니다. 어떤 솔루션이 이러한 요구 사항을 충족합니까? (두 가지를 선택하세요.)

A. Amazon API Gateway REST API를 생성합니다. API Gateway의 AWS 통합 유형을 사용하여 DynamoDB에 대한 직접 통합으로 이 API를 구성합니다.

B. Amazon API Gateway HTTP API를 생성합니다. API Gateway의 AWS 통합 유형을 사용하여 Dynamo DB에 대한 직접 통합으로 이 API를 구성합니다.

C. Amazon API Gateway HTTP API를 생성합니다. DynamoDB 테이블에서 데이터를

반환하는 AWS Lambda 함수와의 통합으로 이 API를 구성합니다.
D. AWS Global Accelerator에서 액셀러레이터를 생성합니다. DynamoDB 테이블에서 데이터를 반환하는 AWS Lambda@Edge 함수 통합으로 이 액셀러레이터를 구성합니다.
E. Network Load Balancer를 생성합니다. 요청을 적절한 AWS Lambda 함수로 전달하도록 리스너 규칙 구성
Answer: A C
Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-overview-developer-experience.
html

QUESTION NO: 35
한 회사가 AWS에서 컨테이너화된 워크로드를 실행하고 있습니다. 이 워크로드는 여러 데이터 처리 서비스로 구성되어 있으며, 이 서비스들은 아마존 EC2 인스턴스 그룹에서 실행됩니다.
이 회사는 매일 밤 새로운 데이터를 Amazon S3 버킷에 업로드합니다. 각 EC2 인스턴스에서 실행되는 cron 작업이 매일 밤 데이터 처리를 시작합니다. 업로드되는 데이터 양은 변동이 심하며, 데이터 처리 작업은 완료하는 데 몇 시간이 걸릴 수 있습니다. 데이터 처리가 완료되면 서비스는 다음 날 밤 다음 처리 시간이 될 때까지 유휴 상태로 유지됩니다. 이 회사는 아키텍처를 현대화하고 운영 오버헤드를 줄일 수 있는 솔루션이 필요합니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?
A. 컨테이너 이미지를 실행하는 AWS Lambda 함수로 워크로드를 마이그레이션합니다. Amazon EventBridge 규칙을 구성하여 S3 이벤트를 필터링하고 데이터가 S3 버킷에 업로드될 때 Lambda 함수를 호출합니다.
B. 워크로드를 AWS Fargate에서 실행되는 Amazon ECS 클러스터의 태스크로 마이그레이션합니다. Fargate 태스크를 호출하는 AWS Step Functions 상태 머신을 생성합니다. 데이터가 S3 버킷에 업로드될 때 상태 머신 태스크가 호출되도록 S3 이벤트 알림을 구성합니다.
C. 워크로드를 AWS Fargate에서 실행되는 Amazon ECS 클러스터의 태스크로 마이그레이션합니다. Fargate 태스크를 호출하는 AWS Step Functions 상태 머신을 생성합니다. 데이터가 S3 버킷에 업로드될 때 상태 머신을 호출하도록 Amazon EventBridge 규칙을 구성합니다.
D. 컨테이너 이미지를 Lambda 레이어로 패키징하여 워크로드를 AWS Lambda 함수로 마이그레이션합니다. 데이터가 S3 버킷에 업로드될 때 Lambda 함수가 호출되도록 S3 이벤트 알림을 구성합니다.
Answer: C
Explanation:
The workload is containerized, runs for hours, and is event-driven by nightly data arrival in Amazon S3. The current architecture uses EC2 instances and cron jobs, which results in operational overhead (managing instances, patching, scaling, scheduling) and idle compute between processing windows.
A key constraint is that the processing tasks can take hours. AWS Lambda has maximum execution duration limits that make it unsuitable for multi-hour batch processing. Even though Lambda can run container images, it still must complete within Lambda's runtime limit. Packaging container images as Lambda layers is also not an appropriate pattern for long-

running container workloads and adds complexity.
A modern, low-ops approach for long-running, containerized batch jobs is to run containers on AWS Fargate.
Fargate removes the need to manage EC2 instances and allows tasks to run for extended periods as needed, scaling based on demand. Because the workload is composed of several data-processing services that likely need orchestration (for example, fan-out, sequencing, retries, parallelism), AWS Step Functions is well suited to coordinate the workflow and invoke the appropriate ECS tasks.
For triggering based on new S3 data, Amazon EventBridge provides a managed, scalable event bus for AWS service events, including S3 object events, and can route events to targets such as Step Functions state machines. Using EventBridge reduces the need for direct point-to-point notification wiring and provides centralized event routing, filtering, and monitoring.
Option C combines all the right elements: it runs the containers as ECS tasks on Fargate to eliminate EC2 management and idle capacity, uses Step Functions to orchestrate tasks that can run for hours, and uses EventBridge to trigger the state machine when new data is uploaded to S3. This replaces the per-instance cron scheduling with an event-driven serverless orchestration model and significantly reduces operational overhead.
Option B is close but is less appropriate as written because S3 Event Notifications are typically configured to send to Amazon SQS, Amazon SNS, or AWS Lambda. Triggering Step Functions directly is more naturally handled through EventBridge rules. EventBridge is also the recommended event routing layer for integrating service events into workflows.
Option A is not suitable because Lambda is not designed for multi-hour processing jobs due to runtime limits.
Option D is incorrect because Lambda layers are for sharing libraries and runtime dependencies, not for packaging multi-hour container workloads. It also still depends on Lambda runtime limits and does not match the operational model for long-running batch processing.
Therefore, option C is the best modernization approach with the least operational overhead.
References:AWS documentation on AWS Fargate for running container workloads without managing EC2 instances and supporting long-running tasks.AWS documentation on AWS Step Functions for orchestrating long-running workflows, retries, parallelism, and service integrations including Amazon ECS.AWS documentation on Amazon EventBridge for routing Amazon S3 object events to targets such as Step Functions state machines for event-driven architectures.