VCE4Plus

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **AWS-Solutions-Architect-Professional-KR**

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

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
회사에는 애플리케이션 데이터베이스로 Amazon Aurora PostgreSQL DB 클러스터를 사용하는 애플리케이션이 있습니다. DB 클러스터에는 하나의 작은 기본 인스턴스와 세 개의 큰 복제본 인스턴스가 포함되어 있습니다. 애플리케이션은 AWS Lambda 함수에서 실행됩니다. 애플리케이션은 읽기 전용 작업을 수행하기 위해 데이터베이스의 복제본 인스턴스에 대한 단기 연결을 여러 개 만듭니다.
트래픽이 많은 기간에는 애플리케이션이 불안정해지고 데이터베이스에서 너무 많은 연결이 설정되고 있다고 보고합니다. 트래픽이 많은 기간의 빈도는 예측할 수 없습니다.
애플리케이션의 안정성을 향상시키는 솔루션은 무엇입니까?
A. Amazon RDS 프록시를 사용하여 DB 클러스터에 대한 프록시를 생성합니다. 프록시에 대한 읽기 전용 끝점을 구성합니다. 프록시 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
B. DB 클러스터의 파라미터 그룹에서 max_connections 설정을 늘립니다. DB 클러스터의 모든 인스턴스를 재부팅합니다. DB 클러스터 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
C. DatabaseConnections 지표가 max _connections 설정에 가까울 때 발생하도록 DB 클러스터에 대한 인스턴스 조정을 구성합니다. Aurora 리더 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
D. Amazon RDS 프록시를 사용하여 DB 클러스터에 대한 프록시를 생성합니다. 프록시에서 Aurora 데이터 API에 대한 읽기 전용 엔드포인트를 구성합니다. 프록시 엔드포인트에 연결하도록 Lambda 함수를 업데이트합니다.
Answer: A

QUESTION NO: 2
회사는 전자 상거래 웹 사이트를 위한 DR(재해 복구) 솔루션을 구축해야 합니다. 웹 애플리케이션은 t3.large Amazon EC2 인스턴스 플릿에서 호스팅되며 Amazon RDS for MySQL DB 인스턴스를 사용합니다. EC2 인스턴스는 여러 가용 영역에 걸쳐 확장되는 Auto Scaling 그룹에 있습니다.
재해 발생 시 웹 애플리케이션은 RPO가 30초이고 R TO가 10분인 보조 환경으로 장애 조치해야 합니다.
이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?
A. 코드형 인프라(IaC)를 사용하여 DR 지역에서 새 인프라를 프로비저닝합니다. DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. AWS Backup에서 백업 계획을 설정하여 EC2 인스턴스 및 DB 인스턴스에 대한 교차 리전 백업을 생성합니다. EC2 인스턴스와 DB 인스턴스를 30초마다 DR 지역에 백업하는 cron 표현식을 생성합니다. 최신 EC2 백업에서 EC2 인스턴스를 복구합니다. Amazon Route 53 지리적 위치 라우팅 정책을 사용하여 재해 발생 시 자동으로 DR 리전으로 장애 조치합니다.
B. 코드형 인프라(IaC)를 사용하여 DR 지역에서 새 인프라를 프로비저닝합니다. DB 인스턴스에 대한 리전 간 읽기 전용 복제본을 생성합니다. EC2 인스턴스를 DR 지역에 지속적으로 복제하도록 AWS Elastic Disaster Recovery를 설정합니다. DR 지역에서 최소 용량으로 EC2 인스턴스 실행 Amazon Route 53 장애 조치 라우팅 정책을 사용하여 재해 발생 시 자동으로 DR 지역으로 장애 조치합니다. Auto Scaling 그룹의 원하는 용량을 늘립니다.
C. AWS Backup에서 백업 계획을 설정하여 EC2 인스턴스 및 DB 인스턴스에 대한 교차 리전 백업을 생성합니다. EC2 인스턴스와 DB 인스턴스를 30초마다 DR 지역에 백업하는 cron

표현식을 생성합니다. 코드형 인프라(IaC)를 사용하여 DR 리전에서 새 인프라를 프로비저닝합니다.
새 인스턴스에서 백업된 데이터를 수동으로 복원합니다. 재해 발생 시 Amazon Route 53 단순 라우팅 정책을 사용하여 DR 리전으로 자동 장애 조치합니다.
D. 코드형 인프라(IaC)를 사용하여 DR 지역에서 새 인프라를 프로비저닝합니다. Amazon Aurora 글로벌 데이터베이스를 생성합니다. EC2 인스턴스를 DR 지역에 지속적으로 복제하도록 AWS Elastic Disaster Recovery를 설정합니다. DR 지역에서 전체 용량으로 EC2 인스턴스의 Auto Scaling 그룹을 실행합니다. Amazon Route 53 장애 조치 라우팅 정책을 사용하여 재해 발생 시 자동으로 DR 리전으로 장애 조치합니다.

Answer: B

Explanation:

The company should use infrastructure as code (IaC) to provision the new infrastructure in the DR Region.

The company should create a cross-Region read replica for the DB instance. The company should set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. The company should run the EC2 instances at the minimum capacity in the DR Region. The company should use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. The company should increase the desired capacity of the Auto Scaling group. This solution will meet the requirements most cost-effectively because AWS Elastic Disaster Recovery (AWS DRS) is a service that minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. AWS DRS enables RPOs of seconds and RTOs of minutes1.

AWS DRS continuously replicates data from the source servers to a staging area subnet in the DR Region, where it uses low-cost storage and minimal compute resources to maintain ongoing replication. In the event of a disaster, AWS DRS automatically converts the servers to boot and run natively on AWS and launches recovery instances on AWS within minutes2.

By using AWS DRS, the company can save costs by removing idle recovery site resources and paying for the full disaster recovery site only when needed. By creating a cross-Region read replica for the DB instance, the company can have a standby copy of its primary database in a different AWS Region3. By using infrastructure as code (IaC), the company can provision the new infrastructure in the DR Region in an automated and consistent way4.

By using an Amazon Route 53 failover routing policy, the company can route traffic to a resource that is healthy or to another resource when the first resource becomes unavailable.

The other options are not correct because:

Using AWS Backup to create cross-Region backups for the EC2 instances and the DB instance would not meet the RPO and RTO requirements. AWS Backup is a service that enables you to centralize and automate data protection across AWS services. You can use AWS Backup to back up your application data across AWS services in your account and across accounts. However, AWS Backup does not provide continuous replication or fast recovery; it creates backups at scheduled intervals and requires manual restoration. Creating backups every 30 seconds would also incur high costs and network bandwidth.

Creating an Amazon API Gateway Data API service integration with Amazon Redshift would not help with disaster recovery. The Data API is a feature that enables you to query your Amazon Redshift cluster using HTTP requests, without needing a persistent connection or a

SQL client. It is useful for building applications that interact with Amazon Redshift, but not for replicating or recovering data.
Creating an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster would not help with disaster recovery. AWS Data Exchange is a service that makes it easy for AWS customers to exchange data in the cloud. You can use AWS Data Exchange to subscribe to a diverse selection of third-party data products or offer your own data products to other AWS customers. A datashare is a feature that enables you to share live and secure access to your Amazon Redshift data across your accounts or with third parties without copying or moving the underlying data. It is useful for sharing query results and views with other users, but not for replicating or recovering data.
References:
https://aws.amazon.com/disaster-recovery/
https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.XR
https://aws.amazon.com/cloudformation/
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html
https://aws.amazon.com/backup/
https://docs.aws.amazon.com/redshift/latest/mgmt/data-api.html
https://aws.amazon.com/data-exchange/
https://docs.aws.amazon.com/redshift/latest/dg/datashare-overview.html

QUESTION NO: 3
한 회사가 레거시 애플리케이션을 AWS 클라우드로 마이그레이션했습니다. 애플리케이션은 3개의 가용 영역에 분산된 3개의 Amazon EC2 인스턴스에서 실행됩니다. 각 가용 영역에는 하나의 EC2 인스턴스가 있습니다. EC2 인스턴스는 VPC의 프라이빗 서브넷 3개에서 실행 중이며 퍼블릭 서브넷 3개와 연결된 ALB(Application Load Balancer)의 대상으로 설정됩니다. 애플리케이션은 온프레미스 시스템과 통신해야 합니다. 회사의 IP 주소 범위에 있는 IP 주소의 트래픽만 온프레미스 시스템에 액세스할 수 있습니다. 회사의 보안팀은 내부 IP 주소 범위에서 IP 주소 하나만 클라우드로 가져오고 있습니다. 회사는 이 IP 주소를 회사 방화벽의 허용 목록에 추가했습니다. 회사에서는 이 IP 주소에 대한 탄력적 IP 주소도 생성했습니다.
솔루션 설계자는 애플리케이션이 온프레미스 시스템과 통신할 수 있는 기능을 제공하는 솔루션을 만들어야 합니다. 또한 솔루션은 오류를 자동으로 완화할 수 있어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. 각 퍼블릭 서브넷에 하나씩 3개의 NAT 게이트웨이를 배포합니다. NAT 게이트웨이에 탄력적 IP 주소를 할당합니다. NAT 게이트웨이에 대한 상태 확인을 활성화합니다. NAT 게이트웨이가 상태 확인에 실패하면 NAT 게이트웨이를 다시 생성하고 탄력적 IP 주소를 새 NAT 게이트웨이에 할당합니다.
B. ALB를 NLB(Network Load Balancer)로 교체합니다. NLB에 탄력적 IP 주소를 할당합니다. NLB에 대한 상태 확인을 켭니다. 상태 확인에 실패한 경우 NLB를 다른 서브넷에 다시 배포합니다.
C. 퍼블릭 서브넷에 단일 NAT 게이트웨이를 배포합니다. NAT 게이트웨이에 탄력적 IP 주소를 할당합니다.
사용자 지정 지표와 함께 Amazon CloudWatch를 사용하여 다음을 수행합니다.
NAT 게이트웨이를 모니터링합니다. NAT 게이트웨이가 비정상인 경우 AWS Lambda 함수를

호출하여 다른 서브넷에 새 NAT 게이트웨이를 생성하십시오. 새 NAT 게이트웨이에 탄력적 IP 주소를 할당합니다.
D. 탄력적 IP 주소를 ALB에 할당합니다. 탄력적 IP 주소를 값으로 사용하여 Amazon Route 53 단순 레코드를 생성합니다. Route 53 상태 확인을 생성합니다. 상태 확인에 실패한 경우 다른 서브넷에 ALB를 다시 생성하십시오.
Answer: C
Explanation:
to connect out from the private subnet you need an NAT gateway and since only one Elastic IP whitelisted on firewall its one NATGateway at time and if AZ failure happens Lambda creates a new NATGATEWAY in a different AZ using the Same Elastic IP ,dont be tempted to select D since application that needs to connect is on a private subnet whose outbound connections use the NATGateway Elastic IP

QUESTION NO: 4
금융 회사는 Amazon S3에서 데이터 레이크를 호스팅합니다. 회사는 여러 제3자로부터 매일 밤 SFTP를 통해 재무 데이터 기록을 수신합니다. 이 회사는 VPC의 퍼블릭 서브넷에 있는 Amazon EC2 인스턴스에서 자체 SFTP 서버를 실행합니다. 업로드된 파일은 동일한 인스턴스에서 실행되는 cron 작업에 의해 데이터 레이크로 이동됩니다. Amazon Route를 사용하여 DNS sftp.examWe.com에서 SFTP 서버에 연결할 수 있습니다.
53.
솔루션 설계자는 SFTP 솔루션의 안정성과 확장성을 개선하기 위해 무엇을 해야 합니까?
A. EC2 인스턴스를 Auto Scaling 그룹으로 이동합니다. ALB(Application Load Balancer) 뒤에 EC2 인스턴스를 배치합니다. ALB를 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
B. SFTP 서버를 SFTP용 AWS Transfer로 마이그레이션합니다. Route에서 DNS 레코드 sftp.example.com 업데이트
53은 서버 끝점 호스트 이름을 가리킵니다.
C. SFTP 서버를 AWS Storage Gateway의 파일 게이트웨이로 마이그레이션합니다. 파일 게이트웨이 엔드포인트를 가리키도록 Route 53의 DNS 레코드 sflp.example.com을 업데이트합니다.
D. EC2 인스턴스를 NLB(Network Load Balancer) 뒤에 배치합니다. NLB를 가리키도록 Route 53의 DNS 레코드 sftp.example.com을 업데이트합니다.
Answer: B
Explanation:
https://aws.amazon.com/aws-transfer-family/faqs/
https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html
https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/?nc1=h_

QUESTION NO: 5
대기업은 수백 개의 AWS 계정에 배포된 VPC에서 워크로드를 실행합니다. 각 VPC는 여러 가용 영역에 걸쳐 있는 퍼블릭 서브넷과 프라이빗 서브넷으로 구성됩니다. NAT 게이트웨이는 퍼블릭 서브넷에 배포되며 프라이빗 서브넷에서 인터넷으로의 아웃바운드 연결을 허용합니다.
솔루션 설계자는 허브 앤 스포크 설계를 진행 중입니다. 스포크 VPC의 모든 프라이빗

서브넷은 송신 VPC를 통해 트래픽을 인터넷으로 라우팅해야 합니다. 솔루션 아키텍트는 이미 중앙 AWS 계정의 송신 VPC에 NAT 게이트웨이를 배포했습니다.
이러한 요구 사항을 충족하기 위해 솔루션 설계자가 수행해야 하는 추가 단계는 무엇입니까?

A. 송신 VPC와 스포크 VPC 간에 피어링 연결을 생성합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.

B. 전송 게이트웨이를 생성하고 이를 기존 AWS 계정과 공유합니다. Transit Gateway에 기존 VPC를 연결합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.

C. 모든 계정에 전송 게이트웨이를 생성합니다. NAT 게이트웨이를 전송 게이트웨이에 연결합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.

D. 송신 VPC와 스포크 VPC 사이에 AWS PrivateLink 연결을 생성합니다. 인터넷 액세스를 허용하도록 필요한 라우팅을 구성합니다.

Answer: B

Explanation:
https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/NAT-gateway-centralized-egress-ra.pdf?d

QUESTION NO: 6

한 회사는 Oracle 데이터베이스용 Amazon RDS를 다른 AWS 계정의 PostgreSQL용 RDS DB 인스턴스로 마이그레이션할 계획입니다. 솔루션 설계자는 가동 중지 시간이 필요하지 않고 마이그레이션을 완료하는 데 필요한 시간을 최소화하는 마이그레이션 전략을 설계해야 합니다. 마이그레이션 전략은 모든 기존 데이터와 마이그레이션 중에 생성된 모든 새 데이터를 복제해야 합니다. 대상 데이터베이스는 마이그레이션 프로세스 완료 시 원본 데이터베이스와 동일해야 합니다. 모든 애플리케이션은 현재 Amazon Route 53 CNAME 레코드를 통신용 엔드포인트로 사용합니다. Oracle DB 인스턴스용 RDS Oracle DB 인스턴스용 RDS는 프라이빗 서브넷에 있습니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 수행해야 합니까? (3개 선택)

A. 대상 계정에서 PostgreSQL DB 인스턴스용 새 RDS를 생성합니다. AWS Schema Conversion Tool(AWS SCT)을 사용하여 소스 데이터베이스에서 대상 데이터베이스로 데이터베이스 스키마를 마이그레이션합니다.

B. AWS Schema Conversion Tool(AWS SCT)을 사용하여 소스 데이터베이스의 스키마 및 초기 데이터를 사용하여 대상 계정에 PostgreSQL용 새 RDS DB 인스턴스를 생성합니다.

C. 두 AWS 계정의 VPC 간에 VPC 피어링을 구성하여 대상 계정에서 두 DB 인스턴스 모두에 대한 연결을 제공합니다. 대상 계정의 VPC에서 데이터베이스 포트의 트래픽을 허용하도록 각 DB 인스턴스에 연결된 보안 그룹을 구성합니다.

D. 대상 계정의 VPC에서 연결을 제공하기 위해 원본 DB 인스턴스에 일시적으로 공개적으로 액세스할 수 있도록 허용합니다. 대상의 VPC에서 데이터베이스 포트의 트래픽을 허용하도록 각 DB 인스턴스에 연결된 보안 그룹을 구성합니다. 계정.

E. 대상 계정에서 AWS Database Migration Service(AWS DMS)를 사용하여 소스 데이터베이스에서 대상 데이터베이스로 전체 로드 및 변경 데이터 캡처(CDC) 마이그레이션을 수행합니다. 마이그레이션이 완료되면 CNAME 레코드를 변경합니다. 대상 DB 인스턴스 엔드포인트를 가리킵니다.

F. 대상 계정에서 AWS Database Migration Service(AWS DMS)를 사용하여 원본 데이터베이스에서 대상 데이터베이스로 변경 데이터 캡처(CDC) 마이그레이션을 수행합니다.

마이그레이션이 완료되면 CNAME 레코드가 다음을 가리키도록 변경합니다. 대상 DB 인스턴스 엔드포인트.

Answer: A C E

QUESTION NO: 7

회사에는 AWS Organizations의 조직에 속한 AWS 계정이 있습니다. 회사는 Amazon EC2 사용량을 지표로 추적하려고 합니다. 회사의 아키텍처 팀은 EC2 사용량이 지난 30일 동안의 평균 EC2 사용량보다 10% 이상 높은 경우 매일 알림을 받아야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 조직의 마스터 계정에서 AWS 예산을 구성합니다. EC2 실행 시간의 사용 유형을 지정합니다. 일일 기간을 지정합니다. AWS Cost Explorer에서 지난 30일 동안 보고된 평균 사용량보다 10% 더 높게 예산 금액을 설정합니다. 사용량 임계값이 충족되면 아키텍처 팀에 알리도록 경고를 구성합니다.

B. 조직의 마스터 계정에서 AWS 비용 이상 탐지를 구성합니다. AWS 서비스의 모니터 유형을 구성합니다. Amazon EC2 필터를 적용합니다. 사용량이 지난 30일 동안의 평균 사용량보다 10% 많은 경우 아키텍처 팀에 알리도록 경고 구독을 구성합니다.

C. 조직의 마스터 계정에서 AWS Trusted Advisor를 활성화합니다. EC2 사용량이 지난 30일 동안 보고된 평균 사용량보다 10% 더 많은 경우 아키텍처 팀에 알리도록 비용 최적화 권고 경고를 구성합니다.

D. 조직의 마스터 계정에서 Amazon Detective를 구성합니다. Detective가 10%가 넘는 사용 이상을 식별한 경우 아키텍처 팀에 알리도록 EC2 사용 이상 경고를 구성합니다.

Answer: B

Explanation:

AWS Cost Anomaly Detection is a feature of the AWS Cost Management suite that leverages machine learning to enable continuous monitoring of your AWS costs and usage, allowing you to identify unexpected and abnormal spending1. You can create cost monitors that evaluate specific AWS services, member accounts, cost allocation tags, or cost categories based on your AWS account structure2. You can also configure alert subscriptions that notify you when a cost monitor detects an anomaly that meets your threshold2. In this case, you can create a cost monitor with a monitor type of AWS Service and apply a filter of Amazon EC2 to track the EC2 usage as a metric. You can then configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days, which is the anomaly detection period used by AWS Cost Anomaly Detection3.

QUESTION NO: 8

회사는 AWS에서 많은 워크로드를 실행하고 AWS Organizations를 사용하여 계정을 관리합니다. 워크로드는 Amazon EC2에서 호스팅됩니다. AWS 파게이트. 그리고 AWS 람다.
일부 워크로드에는 예측할 수 없는 수요가 있습니다. 계정에서 어떤 달에는 높은 사용량이 기록되고 다른 달에는 낮은 사용량이 기록됩니다.
회사는 향후 3년 동안 컴퓨팅 비용을 최적화하려고 합니다. 솔루션 설계자는 사용량을 계산하기 위한 조직 전체의 각 계정에 대한 6개월 평균입니다.
조직의 모든 컴퓨팅 사용량에 대해 가장 많은 비용 절감 효과를 제공하는 솔루션은 무엇입니까?

A. 멤버 계정에서 가장 일반적인 EC2 인스턴스의 크기 및 수와 일치하도록 조직의 예약 인스턴스를 구매합니다.

B. 마스터 계정 수준의 권장 사항을 사용하여 마스터 계정에서 조직을 위한 Compute Savings Plan을 구매합니다.
C. 지난 6개월 동안의 데이터에 따라 EC2 사용량이 높은 각 멤버 계정에 대해 예약 인스턴스를 구매합니다.
D. 지난 6개월 동안의 EC2 사용 데이터를 기반으로 마스터 계정에서 각 멤버 계정에 대한 EC2 Instance Savings Plan을 구매합니다.
Answer: B

QUESTION NO: 9
솔루션 아키텍트는 Auto Scaling 그룹의 Amazon EC2 인스턴스에 배포된 운영 워크로드를 가지고 있습니다. VPC 아키텍처는 두 개의 가용 영역(AZ)에 걸쳐 있으며 각 가용 영역에는 Auto Scaling 그룹이 대상으로 하는 서브넷이 있습니다. VPC는 온프레미스 환경에 연결되어 있으며 연결을 중단할 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 해당 지역에서 세 번째 AZ를 사용할 수 있게 되었습니다. 솔루션 설계자는 추가 IPv4 주소 공간을 추가하지 않고 서비스 가동 중지 시간 없이 새 AZ를 채택하려고 합니다. 어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. AZ2 서브넷만 사용하도록 Auto Scaling 그룹 업데이트 이전 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 생성 새 AZI 서브넷도 사용하도록 Auto Scaling 그룹 조정 인스턴스가 정상이면 조정 AZ1 서브넷만 사용하도록 Auto Scaling 그룹 현재 AZ2 서브넷 제거 원래 AZ1 서브넷 주소 공간의 후반부를 사용하여 새 AZ2 서브넷을 생성합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 생성한 다음 업데이트합니다. 세 개의 새 서브넷을 모두 대상으로 하는 Auto Scaling 그룹.
B. AZ1 서브넷에서 EC2 인스턴스를 종료합니다. 주소 공간 홀을 사용하여 AZ1 서브넷을 삭제하고 다시 생성합니다. 이 새 서브넷을 사용하도록 Auto Scaling 그룹을 업데이트합니다. 두 번째 AZ에 대해 이를 반복합니다.
AZ3에서 새 서브넷을 정의한 다음 세 개의 새 서브넷을 모두 대상으로 지정하도록 Auto Scaling 그룹을 업데이트합니다.
C. 동일한 IPv4 주소 공간을 사용하여 새 VPC를 생성하고 각 AZ마다 하나씩 3개의 서브넷을 정의합니다. 새 VPC의 새 서브넷을 대상으로 하도록 기존 Auto Scaling 그룹을 업데이트합니다.
D. AZ2 서브넷만 사용하도록 Auto Scaling 그룹을 업데이트합니다. 이전 주소 공간을 중지하도록 AZ1 서브넷을 업데이트합니다. AZ1 서브넷도 다시 사용하도록 Auto Scaling 그룹을 조정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 Auto Seating 그룹을 조정합니다. 현재 AZ2 서브넷을 업데이트하고 원래 AZ1 서브넷에서 주소 공간의 나머지 절반을 할당합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 생성한 다음 세 개의 새 서브넷을 모두 대상으로 지정하도록 Auto Scaling 그룹을 업데이트합니다.
Answer: A
Explanation:
https://repost.aws/knowledge-center/vpc-ip-address-range

QUESTION NO: 10

한 회사가 AWS에서 SaaS(Software as a Service) 솔루션을 호스팅합니다. 솔루션에는 HTTPS 엔드포인트를 제공하는 Amazon API Gateway API가 있습니다. API는 컴퓨팅을 위해 AWS Lambda 함수를 사용합니다. Lambda 함수는 Amazon Aurora Serverless VI 데이터베이스에 데이터를 저장합니다.
이 회사는 AWS Serverless Application Model(AWS SAM)을 사용하여 솔루션을 배포했습니다. 이 솔루션은 여러 가용 영역에 걸쳐 확장되며 재해 복구(DR) 계획이 없습니다. 솔루션 아키텍트는 다른 AWS 리전에서 솔루션을 복구할 수 있는 DR 전략을 설계해야 합니다. 이 솔루션의 R TO는 5분, RPO는 1분입니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. 대상 리전에 Aurora Serverless VI 데이터베이스의 읽기 전용 복제본을 생성합니다. AWS SAM을 사용하여 Runbook을 생성하여 대상 리전에 솔루션을 배포합니다. 재해 발생 시 읽기 전용 복제본을 기본 복제본으로 승격합니다.

B. Aurora Serverless VI 데이터베이스를 소스 리전과 대상 리전에 걸쳐 확장되는 표준 Aurora MySQL 글로벌 데이터베이스로 변경합니다. AWS SAM을 사용하여 Runbook을 생성하여 대상 리전에 솔루션을 배포합니다.

C. 대상 리전에 여러 라이터 인스턴스가 있는 Aurora Serverless VI DB 클러스터를 생성합니다.
대상 지역에서 솔루션을 시작합니다. 활성-수동 구성에서 작동하도록 두 지역 솔루션을 구성합니다.

D. Aurora Serverless VI 데이터베이스를 소스 리전과 대상 리전에 걸쳐 확장되는 표준 Aurora MySQL 글로벌 데이터베이스로 변경합니다. 대상 지역에서 솔루션을 시작합니다. 활성-수동 구성에서 작동하도록 두 지역 솔루션을 구성합니다.

Answer: D

Explanation: This option allows the solutions architect to use Aurora global database to replicate data across multiple AWS Regions with low latency and high availability1. By launching the solution in the target Region, the solutions architect can ensure that the API Gateway, Lambda functions, and other resources are ready to serve traffic in case of a disaster in the source Region. By configuring the two Regional solutions to work in an active-passive configuration, the solutions architect can minimize costs and avoid data conflicts by having only one primary Region that accepts write operations and one secondary Region that serves as a standby2. The RTO and RPO requirements can be met by using Aurora global database, which supports sub-second failover times and near real-time replication1.
References:
Working with Amazon Aurora global database
Active-passive failover

QUESTION NO: 11

한 회사에서 AWS Organizations의 조직을 사용하여 수백 개의 AWS 계정을 관리하고 있습니다. 솔루션 설계자는 OWASP(Open Web Application Security Project) 상위 10개 웹 애플리케이션 취약성에 대한 기본 보호를 제공하는 솔루션을 개발하고 있습니다. 솔루션 설계자는 조직 내에 배포된 모든 기존 및 신규 Amazon CloudFront 배포에 AWS WAF를 사용하고 있습니다.
솔루션 설계자가 기본 보호를 제공하기 위해 수행해야 하는 단계의 조합은 무엇입니까? (3개를 선택하세요.)

A. 모든 계정에서 AWS Config를 활성화합니다.

B. 모든 계정에서 Amazon GuardDuty를 활성화합니다.
C. 조직의 모든 기능을 활성화합니다.
D. AWS Firewall Manager를 사용하여 모든 CloudFront 배포의 모든 계정에 AWS WAF 규칙을 배포합니다.
E. AWS Shield Advanced를 사용하여 모든 CloudFront 배포의 모든 계정에 AWS WAF 규칙을 배포합니다.
F. AWS Security Hub를 사용하여 모든 CloudFront 배포의 모든 계정에 AWS WAF 규칙을 배포합니다.
Answer: C D E
Explanation:
Enabling all features for the organization will enable using AWS Firewall Manager to centrally configure and manage firewall rules across multiple AWS accounts1. Using AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions will enable providing baseline protection for the OWASP top 10 web application vulnerabilities2. AWS Firewall Manager supports AWS WAF rules that can help protect against common web exploits such as SQL injection and cross-site scripting3. Configuring redirection of HTTP requests to HTTPS requests in CloudFront will enable encrypting the data in transit using SSL/TLS.

QUESTION NO: 12
회사에는 AWS Organizations에 많은 AWS 계정이 있는 조직이 있습니다. 솔루션 설계자는 회사가 조직의 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 새 IP CIDR 범위를 추가할 책임이 있습니다. 보안 팀에는 자체 AWS 계정이 있습니다. 현재 보안 팀은 허용 목록이 변경되면 다른 AWS 계정의 소유자에게 알립니다.
솔루션 설계자는 CIDR 범위의 공통 집합을 모든 계정에 배포하는 솔루션을 설계해야 합니다. 최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. 보안 팀의 AWS 계정에서 Amazon Simple Notification Service(Amazon SNS) 주제를 설정합니다. 각 AWS 계정에 AWS Lambda 함수를 배포합니다. SNS 주제가 메시지를 수신할 때마다 실행되도록 Lambda 함수를 구성합니다. IP 주소를 입력으로 받아 계정의 보안 그룹 목록에 추가하도록 Lambda 함수를 구성합니다. SNS 주제에 메시지를 게시하여 변경 사항을 배포하도록 보안 팀에 지시합니다.
B. 조직 내의 각 AWS 계정에 새로운 고객 관리 접두사 목록을 만듭니다. 모든 내부 CIDR 범위로 각 계정의 접두사 목록을 채웁니다. 보안 그룹의 계정에서 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다. 각 AWS 계정 소유자와 업데이트를 공유하도록 보안 팀에 지시합니다.
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 관리 접두사 목록을 조직과 공유하십시오. 보안 그룹에서 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다.
D. 조직의 각 계정에서 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 계정에서 역할을 수임하고, 각 계정의 보안 그룹에 IP 주소 목록을 추가하도록 Lambda 함수를 구성합니다.

Answer: C

Explanation:

Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups. This solution meets the requirements with the least amount of operational overhead as it requires the security team to create and maintain a single customer-managed prefix list, and share it with the organization using AWS Resource Access Manager. The owners of each AWS account are then responsible for allowing the prefix list in their security groups, which eliminates the need for the security team to manually notify each account owner when changes are made. This solution also eliminates the need for a separate AWS Lambda function in each account, reducing the overall complexity of the solution.

QUESTION NO: 13

한 회사가 AWS에서 SaaS(Software-as-a-Service) 솔루션을 구축하고 있습니다. 이 회사는 여러 AWS 리전과 동일한 프로덕션 계정에 AWS Lambda 통합과 함께 Amazon API Gateway REST API를 배포했습니다.

이 회사는 고객이 초당 특정 수의 API 호출을 할 수 있는 용량에 대해 비용을 지불할 수 있는 계층형 가격을 제공합니다. 프리미엄 계층은 초당 최대 3,000개의 호출을 제공하며 고객은 고유한 API 키로 식별됩니다. 다양한 리전의 여러 프리미엄 계층 고객은 사용량이 가장 많은 시간 동안 여러 API 메서드에서 429개의 너무 많은 요청 오류 응답을 받았다고 보고합니다. 로그는 Lambda 함수가 호출되지 않았음을 나타냅니다.

이러한 고객에게 표시되는 오류 메시지의 원인은 무엇입니까?

A. Lambda 함수가 동시성 제한에 도달했습니다.

B. Lambda는 동시성에 대한 리전 제한 기능을 합니다.

C. 회사가 API 게이트웨이 계정의 초당 호출 한도에 도달했습니다.

D. 회사는 초당 호출에 대한 API 게이트웨이 기본 메서드별 제한에 도달했습니다.

Answer: C

Explanation:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-reques

QUESTION NO: 14

회사는 고객 거래 데이터베이스를 온프레미스에서 AWS로 마이그레이션해야 합니다. 데이터베이스는 Linux 서버에서 실행되는 Oracle DB 인스턴스에 상주합니다. 새로운 보안 요구 사항에 따라 회사는 매년 데이터베이스 비밀번호를 교체해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Schema Conversion Tool(AWS SCT)을 사용하여 데이터베이스를 Amazon DynamoDB로 변환합니다.

AWS Systems Manager Parameter Store에 암호를 저장합니다. 연간 암호 교체를 위해 AWS Lambda 함수를 호출하는 Amazon CloudWatch 경보를 생성합니다.

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

QUESTION NO: 15
회사는 AWS 클라우드에서 여러 프로젝트를 개발하고 호스팅하고 있습니다. 프로젝트는 AWS Organizations의 동일한 조직에 속한 여러 AWS 계정에서 개발됩니다. 회사는 소유 프로젝트에 비용 또는 클라우드 인프라를 할당해야 합니다. 모든 AWS 계정을 담당하는 팀은 여러 Amazon EC2 인스턴스에 비용 할당에 사용되는 프로젝트 태그가 없음을 발견했습니다. 솔루션 설계자는 문제를 해결하고 미래에 문제가 발생하지 않도록 어떤 조치를 취해야 합니까? (3개를 선택합니다.)
A. 각 계정에서 AWS Config 규칙을 생성하여 태그가 누락된 리소스를 찾습니다.
B. 프로젝트 태그가 누락된 경우 ec2:RunInstances에 대한 거부 작업으로 조직에 SCP를 만듭니다.
C. 조직에서 Amazon Inspector를 사용하여 태그가 누락된 리소스를 찾습니다.
D. 프로젝트 태그가 누락된 경우 ec2:RunInstances에 대한 거부 작업을 사용하여 각 계정에 IAM 정책을 생성합니다.
E. 조직에서 누락된 Project 태그가 있는 EC2 인스턴스 목록을 수집할 AWS Config 수집기를 생성합니다.
F. AWS Security Hub를 사용하여 누락된 Project 태그가 있는 EC2 인스턴스 목록을 집계합니다.
Answer: A B E
Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/config-rule-multi-account-deployment.html
https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html

QUESTION NO: 16
회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 핵심 비즈니스 로직은 Auto Scaling 그룹의 Amazon EC2 인스턴스 세트에서 실행됩니다. ALB(Application Load Balancer)는 EC2 인스턴스에 트래픽을 분산합니다. Amazon Route 53 레코드 api.example.com이 ALB를 가리키고 있습니다.
회사의 개발 팀은 비즈니스 논리를 크게 업데이트합니다. 회사에는 변경 사항이 배포되면 테스트 기간 동안 고객의 10%만 새로운 논리를 받을 수 있다는 규칙이 있습니다. 고객은 테스트 기간 동안 동일한 버전의 비즈니스 로직을 사용해야 합니다.

회사는 이러한 요구 사항을 충족하기 위해 업데이트를 어떻게 배포해야 합니까?

A. 두 번째 ALB를 생성하고 새 Auto Scaling 그룹의 EC2 인스턴스 집합에 새 논리를 배포합니다.
EC2 인스턴스에 트래픽을 분산하도록 ALB를 구성합니다. 가중치 기반 라우팅을 사용하도록 Route 53 레코드를 업데이트하고 레코드가 두 ALB를 가리키도록 합니다.

B. ALB에서 참조하는 두 번째 대상 그룹을 생성합니다. 이 새 대상 그룹의 EC2 인스턴스에 새 논리를 배포합니다. 가중 대상 그룹을 사용하도록 ALB 리스너 규칙을 업데이트합니다. ALB 대상 그룹 고정성을 구성합니다.

C. Auto Scaling 그룹에 대한 새 시작 구성을 생성합니다. AutoScalingRollingUpdate 정책을 사용하도록 시작 구성을 지정하고 MaxBatchSize 옵션을 10으로 설정합니다. Auto Scaling 그룹에서 시작 구성을 교체합니다. 변경 사항을 배포합니다.

D. ALB에서 참조하는 두 번째 Auto Scaling 그룹을 생성합니다. 이 새 Auto Scaling 그룹의 EC2 인스턴스 집합에 새 논리를 배포합니다. ALB 라우팅 알고리즘을 최소 미해결 요청(LOR)으로 변경합니다. ALB 세션 고정성을 구성합니다.

Answer: B

Explanation:

The company should create a second target group that is referenced by the ALB. The company should deploy the new logic to EC2 instances in this new target group. The company should update the ALB listener rule to use weighted target groups. The company should configure ALB target group stickiness. This solution will meet the requirements because weighted target groups are a feature that enables you to distribute traffic across multiple target groups using a single listener rule. You can specify a weight for each target group, which determines the percentage of requests that are routed to that target group. For example, if you specify two target groups, each with a weight of 10, each target group receives half the requests1. By creating a second target group and deploying the new logic to EC2 instances in this new target group, the company can have two versions of its business logic running in parallel. By updating the ALB listener rule to use weighted target groups, the company can control how much traffic is sent to each version. By configuring ALB target group stickiness, the company can ensure that a customer uses the same version of the business logic during the testing window. Target group stickiness is a feature that enables you to bind a user's session to a specific target within a target group for the duration of the session2.

The other options are not correct because:

Creating a second ALB and deploying the new logic to a set of EC2 instances in a new Auto Scaling group would not be as cost-effective or simple as using weighted target groups. A second ALB would incur additional charges and require more configuration and management. Updating the Route 53 record to use weighted routing would not ensure that a customer uses the same version of the business logic during the testing window, as DNS caching could affect how requests are routed.

Creating a new launch configuration for the Auto Scaling group and replacing it on the Auto Scaling group would not allow for gradual traffic shifting between versions. A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. You can specify information such as the AMI ID, instance type, key pair, security groups, and block device mapping for your instances3.

However, replacing the launch configuration on an Auto Scaling group would affect all

instances in that group, not just 10% of customers.
Creating a second Auto Scaling group and changing the ALB routing algorithm to least outstanding requests (LOR) would not allow for controlled traffic shifting between versions. A second Auto Scaling group would require more configuration and management. The LOR routing algorithm is a feature that enables you to route traffic based on how quickly targets respond to requests. The load balancer selects a target from the target group with the fewest outstanding requests4. However, this algorithm does not take into account customer sessions or weights.
References:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#listener-
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#rou

QUESTION NO: 17
한 회사가 us-east-1 리전의 Amazon RDS for MySQL DB 인스턴스에 데이터베이스를 배포했습니다.
회사는 유럽의 고객이 데이터를 사용할 수 있도록 해야 합니다. 유럽의 고객은 미국(US)의 고객과 동일한 데이터에 액세스할 수 있어야 하며 높은 애플리케이션 대기 시간 또는 오래된 데이터를 허용하지 않습니다. 유럽 고객과 미국 고객은 데이터베이스에 기록해야 합니다. 두 고객 그룹 모두 다른 그룹의 업데이트를 실시간으로 확인해야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. RDS for MySQL DB 인스턴스의 Amazon Aurora MySQL 복제본을 생성합니다. RDS DB 인스턴스에 대한 애플리케이션 쓰기를 일시 중지합니다. Aurora 복제본을 독립 실행형 DB 클러스터로 승격합니다. Aurora 데이터베이스를 사용하도록 애플리케이션을 재구성하고 쓰기를 재개하십시오. eu-west-1을 보조 리전으로 추가합니다.
06 클러스터. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 Aurora MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
B. RDS for MySQL DB 인스턴스에 대해 eu-west-1에 교차 리전 복제본을 추가합니다. 쓰기 쿼리를 다시 기본 DB 인스턴스로 복제하도록 복제본을 구성합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 RDS for MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
C. RDS for MySQL DB 인스턴스에서 eu-west-1로 가장 최근 스냅샷을 복사합니다. 스냅샷에서 eu-west-1에 새 RDS for MySQL DB 인스턴스를 생성합니다. us-east-1에서 eu-west-1로 MySQL 논리적 복제를 구성합니다. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-west-1에 애플리케이션을 배포합니다.
eu-west-1에서 RDS for MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
D. RDS for MySQL DB 인스턴스를 Amazon Aurora MySQL DB 클러스터로 변환합니다. eu-west-1을 DB 클러스터에 보조 리전으로 추가합니다. DB 클러스터에서 쓰기 전달을 활성화합니다. eu-west-1에 애플리케이션을 배포합니다. eu-west-1에서 Aurora MySQL 엔드포인트를 사용하도록 애플리케이션을 구성합니다.
Answer: D

Explanation:
The company should use AWS Amplify to create a static website for uploads of media files. The company should use Amplify Hosting to serve the website through Amazon CloudFront. The company should use Amazon S3 to store the uploaded media files. The company should use Amazon Cognito to authenticate users.
This solution will meet the requirements with the least operational overhead because AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS, with the flexibility to leverage the breadth of AWS services as use cases evolve. No cloud expertise needed1. By using AWS Amplify, the company can refactor the application to a serverless architecture that reduces operational complexity and costs. AWS Amplify offers the following features and benefits:
Amplify Studio: A visual interface that enables you to build and deploy a full-stack app quickly, including frontend UI and backend.
Amplify CLI: A local toolchain that enables you to configure and manage an app backend with just a few commands.
Amplify Libraries: Open-source client libraries that enable you to build cloud-powered mobile and web apps.
Amplify UI Components: Open-source design system with cloud-connected components for building feature-rich apps fast.
Amplify Hosting: Fully managed CI/CD and hosting for fast, secure, and reliable static and server-side rendered apps.
By using AWS Amplify to create a static website for uploads of media files, the company can leverage Amplify Studio to visually build a pixel-perfect UI and connect it to a cloud backend in clicks. By using Amplify Hosting to serve the website through Amazon CloudFront, the company can easily deploy its web app or website to the fast, secure, and reliable AWS content delivery network (CDN), with hundreds of points of presence globally. By using Amazon S3 to store the uploaded media files, the company can benefit from a highly scalable, durable, and cost-effective object storage service that can handle any amount of data2. By using Amazon Cognito to authenticate users, the company can add user sign-up, sign-in, and access control to its web app with a fully managed service that scales to support millions of users3.
The other options are not correct because:
Using AWS Application Migration Service to migrate the application server to Amazon EC2 instances would not refactor the application or accelerate development. AWS Application Migration Service (AWS MGN) is a service that enables you to migrate physical servers, virtual machines (VMs), or cloud servers from any source infrastructure to AWS without requiring agents or specialized tools. However, this would not address the challenges of overutilization and data uploads failures. It would also not reduce operational overhead or costs compared to a serverless architecture.
Creating a static website for uploads of media files and using AWS AppSync to create an API would not be as simple or fast as using AWS Amplify. AWS AppSync is a service that enables you to create flexible APIs for securely accessing, manipulating, and combining data from one or more data sources.
However, this would require more configuration and management than using Amplify Studio and Amplify Hosting. It would also not provide authentication features like Amazon Cognito.

Setting up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application would not be as suitable as using Amazon Cognito. AWS Single Sign-On (AWS SSO) is a service that enables you to centrally manage SSO access and user permissions across multiple AWS accounts and business applications. However, this service is designed for enterprise customers who need to manage access for employees or partners across multiple resources. It is not intended for authenticating end users of web or mobile apps.
References:
https://aws.amazon.com/amplify/
https://aws.amazon.com/s3/
https://aws.amazon.com/cognito/
https://aws.amazon.com/mgn/
https://aws.amazon.com/appsync/
https://aws.amazon.com/single-sign-on/

QUESTION NO: 18
회사는 사용자에게 맞춤형 애플리케이션에서 이미지를 업로드할 수 있는 기능을 제공합니다. 업로드 프로세스는 Amazon S3 버킷에서 이미지를 처리하고 저장하는 AWS Lambda 함수를 호출합니다. 애플리케이션은 특정 함수 버전 ARN을 사용하여 Lambda 함수를 호출합니다. Lambda 함수는 환경 변수를 사용하여 이미지 처리 매개변수를 수락합니다. 회사는 종종 최적의 이미지 처리 출력을 얻기 위해 Lambda 함수의 환경 변수를 조정합니다.
회사는 다양한 매개변수를 테스트하고 결과를 확인한 후 업데이트된 환경 변수로 새 기능 버전을 게시합니다. 또한 이 업데이트 프로세스에서는 새 기능 버전 ARN을 호출하기 위해 사용자 지정 애플리케이션을 자주 변경해야 합니다. 이러한 변경 사항은 사용자에게 방해가 됩니다.
솔루션 설계자는 이 프로세스를 단순화하여 사용자의 혼란을 최소화해야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. 게시된 Lambda 함수 버전의 환경 변수를 직접 수정합니다. SLATEST 버전을 사용하여 이미지 처리 매개변수를 테스트합니다.
B. 이미지 처리 매개변수를 저장할 Amazon DynamoDB 테이블을 생성합니다. DynamoDB 테이블에서 이미지 처리 매개변수를 검색하도록 Lambda 함수를 수정합니다.
C. Lambda 함수 내에서 이미지 처리 매개변수를 직접 코딩하고 환경 변수를 제거합니다. 회사에서 매개변수를 업데이트하면 새 기능 버전을 게시합니다.
D. Lambda 함수 별칭을 생성합니다. 함수 별칭 ARN을 사용하도록 클라이언트 애플리케이션을 수정합니다.
회사에서 테스트를 완료하면 함수의 새 버전을 가리키도록 Lambda 별칭을 재구성합니다.
Answer: D
Explanation:
A Lambda function alias allows you to point to a specific version of a function and also can be updated to point to a new version of the function without modifying the client application. This way, the company can test different versions of the function with different environment variables and, once the optimal parameters are found, update the alias to point to the new version, without the need to update the client application.
By using this approach, the company can simplify the process of updating the environment variables, minimize disruption to users, and reduce the operational overhead.

Reference:
AWS Lambda documentation: https://aws.amazon.com/lambda/
AWS Lambda Aliases documentation:
https://docs.aws.amazon.com/lambda/latest/dg/aliases-intro.html AWS Lambda versioning and aliases documentation:
https://aws.amazon.com/blogs/compute/versioning-aliases-in-aws-lambda/

QUESTION NO: 19
최근 대규모 급여 회사가 소규모 채용 회사와 합병되었습니다. 이제 통합된 회사에는 여러 사업부가 있으며 각 사업부는 자체 기존 AWS 계정을 가지고 있습니다.
솔루션 아키텍트는 회사가 모든 AWS 계정에 대한 청구 및 액세스 정책을 중앙에서 관리할 수 있는지 확인해야 합니다. 솔루션 아키텍트는 중앙 집중식 마스터 계정에서 회사의 모든 회원 계정에 초대를 보내 AWS Organizations를 구성합니다.
이러한 요구 사항을 충족하려면 솔루션 설계자가 다음에 무엇을 해야 합니까?
A. 각 회원 계정에 OrganizationAccountAccess IAM 그룹을 생성합니다. 각 관리자에게 필요한 IAM 역할을 포함합니다.
B. 각 회원 계정에서 OrganizationAccountAccessPolicy IAM 정책을 생성합니다. 교차 계정 액세스를 사용하여 회원 계정을 마스터 계정에 연결합니다.
C. 각 회원 계정에서 OrganizationAccountAccessRole IAM 역할을 생성합니다. IAM 역할을 맡을 수 있는 권한을 마스터 계정에 부여하십시오.
D. 마스터 계정에서 OrganizationAccountAccessRole IAM 역할을 생성합니다. AdministratorAccess AWS 관리형 정책을 IAM 역할에 연결합니다. 각 회원 계정의 관리자에게 IAM 역할을 할당합니다.
Answer: C

QUESTION NO: 20
한 회사가 Amazon EC2 인스턴스 집합에 분산된 인 메모리 데이터베이스를 배포하고 있습니다. 플릿은 기본 노드 1개와 작업자 노드 8개로 구성됩니다. 기본 노드는 클러스터 상태를 모니터링하고, 사용자 요청을 수락하고, 사용자 요청을 작업자 노드에 배포하고, 집계 응답을 클라이언트에 다시 보내는 일을 담당합니다. 작업자 노드는 서로 통신하여 데이터 파티션을 복제합니다.
회사는 최대 성능을 달성하기 위해 가능한 가장 낮은 네트워킹 대기 시간을 요구합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. 파티션 배치 그룹에서 메모리 최적화 EC2 인스턴스를 시작합니다.
B. 파티션 배치 그룹에서 컴퓨팅 최적화 EC2 인스턴스를 시작합니다.
C. 클러스터 배치 그룹에서 메모리 최적화 EC2 인스턴스 시작
D. 분산 배치 그룹에서 컴퓨팅 최적화 EC2 인스턴스를 시작합니다.
Answer: C

QUESTION NO: 21
소프트웨어 회사는 개발 프로세스의 일부로 풀 요청을 테스트하기 위해 단기 테스트 환경을 만들어야 합니다. 각 테스트 환경은 Auto Scaling 그룹에 있는 단일 Amazon EC2 인스턴스로 구성됩니다.
테스트 환경은 테스트 결과를 보고하기 위해 중앙 서버와 통신할 수 있어야 합니다. 중앙 서버는 온프레미스 데이터 센터에 있습니다. 솔루션 아키텍트는 회사가 수동 개입 없이

테스트 환경을 생성하고 삭제할 수 있도록 솔루션을 구현해야 합니다. 회사는 온프레미스 네트워크에 대한 VPN 연결을 사용하여 전송 게이트웨이를 만들었습니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 전송 게이트웨이 연결 및 관련 라우팅 구성이 포함된 AWS CloudFormation 템플릿을 생성합니다. 이 템플릿을 포함하는 CloudFormation 스택 세트를 생성합니다. CloudFormation StackSets를 사용하여 계정의 각 VPC에 대해 새 스택을 배포합니다. 각 테스트 환경에 대해 새 VPC를 배포합니다.

B. 테스트 환경을 위한 단일 VPC를 생성합니다. Transit Gateway 연결 및 관련 라우팅 구성을 포함합니다. AWS CloudFormation을 사용하여 모든 테스트 환경을 VPC에 배포합니다.

C. 테스트를 위해 AWS Organizations에 새 OU를 생성합니다. VPC, 필요한 네트워킹 리소스, 전송 게이트웨이 연결 및 관련 라우팅 구성이 포함된 AWS CloudFormation 템플릿을 생성합니다. 이 템플릿을 포함하는 CloudFormation 스택 세트를 생성합니다. 테스트 01.1에서 각 계정에 배포하려면 CloudFormation StackSets를 사용하세요. 각 테스트 환경에 대해 새 계정을 만듭니다.

D. 테스트 환경 EC2 인스턴스를 Docker 이미지로 변환합니다. AWS CloudFormation을 사용하여 새 VPC에서 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 구성하고, 전송 게이트웨이 연결을 생성하고, 관련 라우팅 구성을 생성합니다. Kubernetes를 사용하여 테스트 환경의 배포 및 수명 주기를 관리하세요.

Answer: B

Explanation: This option allows the company to use a single VPC to host multiple test environments that are isolated from each other by using different subnets and security groups1. By including a transit gateway attachment and related routing configurations, the company can enable the test environments to communicate with the central server in the on-premises data center through a VPN connection2. By using AWS CloudFormation to deploy all test environments into the VPC, the company can automate the creation and deletion of test environments without any manual intervention3. This option also minimizes the operational overhead by reducing the number of VPCs, accounts, and resources that need to be managed.

References:

Working with VPCs and subnets

Working with transit gateways

Working with AWS CloudFormation stacks

QUESTION NO: 22

회사는 소스라는 AWS 계정에 애플리케이션을 가지고 있습니다. 계정은 AWS Organizations의 조직에 있습니다. 애플리케이션 중 하나는 AWS Lambda 기능을 사용하고 인벤토리 데이터를 Amazon Aurora 데이터베이스에 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 다운타임을 최소화해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 소스 계정에서 Lambda 함수 배포 패키지를 다운로드합니다. 배포 패키지를 사용하고 Target 계정에서 새 Lambda 함수를 생성합니다. 자동화된 Aurora DB 클러스터 스냅샷을 대상

계정과 공유합니다.

B. 소스 계정에서 Lambda 함수 배포 패키지를 다운로드합니다. 배포 패키지를 사용하고 대상 계정에서 새 Lambda 함수를 생성합니다. AWS Resource Access Manager(AWS RAM)를 사용하여 Aurora DB 클러스터를 대상 계정과 공유합니다. 대상 계정에 Aurora DB 클러스터를 복제할 수 있는 권한을 부여합니다.

C. AWS Resource Access Manager(AWS RAM)를 사용하여 대상 계정과 Lambda 함수 및 Aurora DB 클러스터를 공유합니다. 대상 계정에 Aurora DB 클러스터를 복제할 수 있는 권한을 부여합니다.

D. AWS Resource Access Manager(AWS RAM)를 사용하여 대상 계정과 Lambda 함수를 공유합니다. 자동화된 Aurora DB 클러스터 스냅샷을 대상 계정과 공유합니다.

Answer: C

Explanation:

This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime. In this solution, the Lambda function deployment package is downloaded from the Source account and used to create new Lambda functions in the Target account. The Aurora DB cluster is shared with the Target account using AWS RAM and the Target account is granted permission to clone the Aurora DB cluster, allowing for a new copy of the Aurora database to be created in the Target account. This approach allows for the data to be migrated to the Target account while minimizing downtime, as the Target account can use the cloned Aurora database while the original Aurora database continues to be used in the Source account.

QUESTION NO: 23

한 회사에서 Amazon EC2 Auto Scaling 그룹에 대한 애플리케이션의 CI/CD에 AWS CodePipeline을 사용하고 있습니다. 모든 AWS 리소스는 AWS CloudFormation 템플릿에 정의됩니다. 애플리케이션 아티팩트는 Amazon S3 버킷에 저장되고 인스턴스 사용자 데이터 스크립트를 사용하여 Auto Scaling 그룹에 배포됩니다.

애플리케이션이 더욱 복잡해짐에 따라 CloudFormation 템플릿의 최근 리소스 변경으로 인해 계획되지 않은 가동 중지 시간이 발생했습니다.

솔루션 설계자는 템플릿 변경으로 인해 가동 중지 시간이 발생할 가능성을 줄이기 위해 CI/CD 파이프라인을 어떻게 개선해야 합니까?

A. 배포를 수행할 때 CloudFormation 오류 조건을 감지하고 보고하도록 배포 스크립트를 조정합니다. 프로덕션 변경을 승인하기 전에 테스트 팀이 비프로덕션 환경에서 실행할 테스트 계획을 작성합니다.

B. 테스트 환경에서 AWS CodeBuild를 사용하여 자동화된 테스트를 구현합니다. CloudFormation 변경 세트를 사용하여 배포 전에 변경 사항을 평가합니다. AWS CodeDeploy를 사용하면 블루/그린 배포 패턴을 활용하여 필요한 경우 평가 및 변경 사항을 되돌릴 수 있습니다.

C. IDE(통합 개발 환경)용 플러그인을 사용하여 템플릿에 오류가 있는지 확인하고 AWS CLI를 사용하여 템플릿이 올바른지 확인합니다. 오류 조건을 확인하고 오류에 대한 알림을 생성하도록 배포 코드를 조정합니다. 프로덕션 변경을 승인하기 전에 테스트 환경에 배포하고 수동 테스트 계획을 실행하십시오.

D. AWS CodeDeploy 및 CloudFormation과 함께 블루/그린 배포 패턴을 사용하여 사용자 데이터 배포 스크립트를 대체합니다. 운영자가 실행 중인 인스턴스에 로그인하고 수동 테스트

계획을 통해 애플리케이션이 예상대로 실행되고 있는지 확인하도록 합니다.
Answer: B

QUESTION NO: 24
한 회사에 데이터 계층이 단일 AWS 리전에 배포된 중요한 애플리케이션이 있습니다. 데이터 계층은 Amazon DynamoDB 테이블과 Amazon Aurora MySQL DB 클러스터를 사용합니다. 현재 Aurora MySQL 엔진 버전은 글로벌 데이터베이스를 지원합니다. 애플리케이션 계층은 이미 두 지역에 배포되었습니다.
회사 정책에 따르면 중요한 애플리케이션에는 애플리케이션 계층 구성 요소와 데이터 계층 구성 요소가 두 지역에 걸쳐 배포되어야 합니다. RTO 및 RPO는 각각 몇 분을 넘지 않아야 합니다. 솔루션 설계자는 데이터 계층이 회사 정책을 준수하도록 하는 솔루션을 권장해야 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (두 가지를 선택하세요.)
A. Aurora MySQL DB 클러스터에 다른 리전 추가
B. Aurora MySQL DB 클러스터의 각 테이블에 다른 리전 추가
C. DynamoDB 테이블 및 Aurora MySQL DB 클러스터에 대한 예약된 교차 리전 백업 설정
D. 구성에 다른 리전을 추가하여 기존 DynamoDB 테이블을 전역 테이블로 변환
E. Amazon Route 53 애플리케이션 복구 컨트롤러를 사용하여 보조 리전으로 데이터베이스 백업 및 복구 자동화
Answer: A D
Explanation:
The company should use Amazon Aurora global database and Amazon DynamoDB global table to deploy the data tier components across two Regions. Amazon Aurora global database is a feature that allows a single Aurora database to span multiple AWS Regions, enabling low-latency global reads and fast recovery from Region-wide outages1. Amazon DynamoDB global table is a feature that allows a single DynamoDB table to span multiple AWS Regions, enabling low-latency global reads and writes and fast recovery from Region-wide outages2.
References:
https://aws.amazon.com/rds/aurora/global-database/
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/globaltables_HowItWorks.html
https://aws.amazon.com/route53/application-recovery-controller/

QUESTION NO: 25
한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 AWS Fargate 기술을 기본 컴퓨팅으로 실행하는 AWS Lambda 함수와 Amazon Elastic Container Service(Amazon ECS) 컨테이너를 사용합니다. 애플리케이션의 로드가 불규칙합니다. 애플리케이션이 장기간 사용되지 않은 후 갑자기 트래픽이 크게 증가하거나 감소합니다. 이 애플리케이션은 쓰기 집약적이며 Amazon Aurora MySQL 데이터베이스에 데이터를 저장합니다. 데이터베이스는 로드를 처리할 수 없는 Amazon RDS 메모리 최적화 DB 인스턴스에서 실행됩니다.
회사가 갑작스럽고 중대한 트래픽 변화를 처리할 수 있는 가장 비용 효과적인 방법은 무엇입니까?
A. 데이터베이스에 읽기 전용 복제본을 추가합니다. 인스턴스 Savings Plan과 RDS 예약

인스턴스를 구매하세요.
B. 데이터베이스를 Aurora 멀티 마스터 DB 클러스터로 마이그레이션합니다. 인스턴스 절약 플랜을 구매하세요.
C. 데이터베이스를 Aurora 글로벌 데이터베이스로 마이그레이션합니다. Compute Savings Plan 및 RDS 예약 인스턴스를 구매하세요.
D. 데이터베이스를 Aurora Serverless v1로 마이그레이션합니다. Compute Savings Plan을 구매하세요.
Answer: D

QUESTION NO: 26
글로벌 사무소가 있는 회사에는 단일 AWS 리전에 대한 단일 1Gbps AWS Direct Connect 연결이 있습니다.
회사의 온프레미스 네트워크는 연결을 사용하여 AWS 클라우드에 있는 회사 리소스와 통신합니다. 연결에는 단일 VPC에 연결하는 단일 프라이빗 가상 인터페이스가 있습니다.
솔루션 설계자는 동일한 지역에 중복 Direct Connect 연결을 추가하는 솔루션을 구현해야 합니다. 또한 솔루션은 회사가 다른 지역으로 확장할 때 동일한 Direct Connect 연결 쌍을 통해 다른 지역에 대한 연결을 제공해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. Direct Connect 게이트웨이를 프로비저닝합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다. 두 번째 Direct Connect 연결을 만듭니다. 각 연결에서 새 개인 가상 인터레이스를 만들고 두 개인 가상 인터페이스를 Direct Connect 게이트웨이에 연결합니다. Direct Connect 게이트웨이를 단일 VPC에 연결합니다.
B. 기존 개인 가상 인터페이스를 유지합니다. 두 번째 Direct Connect 연결을 만듭니다. 새 연결에서 새 프라이빗 가상 인터페이스를 생성하고 새 프라이빗 가상 인터페이스를 단일 VPC에 연결합니다.
C. 기존 개인 가상 인터페이스를 유지합니다. 두 번째 Direct Connect 연결을 만듭니다. 새 연결에서 새 퍼블릭 가상 인터페이스를 생성하고 새 퍼블릭 가상 인터페이스를 단일 VPC에 연결합니다.
D. 전송 게이트웨이를 제공합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다.
두 번째 Direct Connect 연결을 만듭니다. 각 연결에서 새 프라이빗 가상 인터페이스를 만들고 두 프라이빗 가상 인터페이스를 전송 게이트웨이에 연결합니다. Transit Gateway를 단일 VPC와 연결합니다.
Answer: A
Explanation:
A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

QUESTION NO: 27
한 회사가 AWS 클라우드의 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 복제본 세트를 데이터 계층으로 사용하는 MongoDB 데이터베이스를 사용하고 있습니다. MongoDB 데이터베이스는 회사의 온프레미스 데이터 센터 시스템에

설치되며 데이터 센터 환경에 대한 AWS Direct Connect 연결을 통해 액세스할 수 있습니다.
솔루션 설계자는 온프레미스 MongoDB 데이터베이스를 Amazon DocumentDB(MongoDB와 호환 가능)로 마이그레이션해야 합니다.
솔루션 설계자는 이 마이그레이션을 수행하기 위해 어떤 전략을 선택해야 합니까?

A. EC2 인스턴스 집합을 생성합니다. EC2 인스턴스에 MongoDB Community Edition을 설치하고 데이터베이스를 생성합니다. 온프레미스 데이터 센터에서 실행 중인 데이터베이스를 사용하여 연속 동기 복제를 구성합니다.

B. AWS Database Migration Service(AWS DMS) 복제 인스턴스를 생성합니다. 변경 데이터 캡처(CDC)를 사용하여 온프레미스 MongoDB 데이터베이스에 대한 소스 엔드포인트를 만듭니다. Amazon DocumentDB 데이터베이스에 대한 대상 엔드포인트를 생성합니다. DMS 마이그레이션 작업을 생성하고 실행합니다.

C. AWS Data Pipeline을 사용하여 데이터 마이그레이션 파이프라인을 생성합니다. 온프레미스 MongoDB 데이터베이스 및 Amazon DocumentDB 데이터베이스에 대한 데이터 노드를 정의합니다. 데이터 파이프라인을 실행하기 위한 예약된 작업을 만듭니다.

D. AWS Glue 크롤러를 사용하여 온프레미스 MongoDB 데이터베이스에 대한 소스 엔드포인트를 생성합니다.
MongoDB 데이터베이스와 Amazon DocumentDB 데이터베이스 간의 연속 비동기 복제를 구성합니다.

Answer: B

Explanation:
https://aws.amazon.com/getting-started/hands-on/move-to-managed/migrate-mongodb-to-documentdb/

QUESTION NO: 28

솔루션 설계자는 기존 VPC에 대한 DNS 전략을 결정하고 있습니다. VPC는 다음을 사용하도록 프로비저닝됩니다.
10.24.34.0/24 CIDR 블록. VPC는 DNS용 Amazon Route 53 Resolver도 사용합니다. 새로운 요구 사항에 따라 DNS 쿼리는 프라이빗 호스팅 영역을 사용해야 합니다. 또한 퍼블릭 IP 주소가 있는 인스턴스는 해당 퍼블릭 호스트 이름을 받아야 합니다.
VPC 내에서 도메인 이름이 올바르게 확인되도록 하기 위해 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 프라이빗 호스팅 영역을 생성합니다. VPC에 대한 활성화DnsSupport 속성 및 활성화DnsHostnames 속성을 활성화합니다. domain-name-servers-10.24.34.2를 포함하도록 VPC DHCP 옵션 세트를 업데이트합니다.

B. 프라이빗 호스팅 영역을 생성합니다. 프라이빗 호스팅 영역을 VPC와 연결합니다. VPC에 대한 활성화DnsSupport 속성 및 활성화DnsHostnames 속성을 활성화합니다. 새 VPC DHCP 옵션 세트를 생성하고 domain-name-servers=AmazonProvidedDNS를 구성합니다. 새 DHCP 옵션 세트를 VPC와 연결합니다.

C. VPC에 대한 활성화DnsSupport 속성을 비활성화합니다. VPC에 대한 활성화DnsHostnames 속성을 활성화합니다. 새 VPC DHCP 옵션 세트를 생성하고 domain-name-servers=10.24.34.2를 구성합니다.
새 DHCP 옵션 세트를 VPC와 연결합니다.

D. 프라이빗 호스팅 영역을 생성합니다. 프라이빗 호스팅 영역을 VPC와 연결합니다. VPC에 대한 활성화DnsSupport 속성을 활성화합니다. VPC에 대한 활성화DnsHostnames 속성을

비활성화합니다.
domain-name-servers=AmazonProvidedDNS를 포함하도록 VPC DHCP 옵션 세트를 업데이트합니다.

Answer: B

Explanation: This option allows the solutions architect to use a private hosted zone to host DNS records that are only accessible within the VPC1. By associating the private hosted zone with the VPC, the solutions architect can ensure that DNS queries from the VPC are routed to the private hosted zone2. By activating the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC, the solutions architect can enable DNS resolution and hostname assignment for instances in the VPC3. By creating a new VPC DHCP options set, and configuring domain-name-servers=AmazonProvidedDNS, the solutions architect can use Amazon-provided DNS servers to resolve DNS queries from instances in the VPC4. By associating the new DHCP options set with the VPC, the solutions architect can apply the DNS settings to all instances in the VPC5.

References:

What is Amazon Route 53 Resolver?

Associating a private hosted zone with your VPC

Using DNS with your VPC

DHCP options sets

Modifying your DHCP options

QUESTION NO: 29

한 회사가 수천 개의 Amazon EC2 인스턴스로 구성된 워크로드를 실행하고 있습니다. 워크로드는 여러 퍼블릭 서브넷과 프라이빗 서브넷이 포함된 VPC에서 실행 중입니다. 퍼블릭 서브넷에는 다음 경로가 있습니다.
0.0.0.0/0을 기존 인터넷 게이트웨이에 연결합니다. 프라이빗 서브넷에는 기존 NAT 게이트웨이에 대한 0.0.0.0/0 경로가 있습니다.
솔루션 아키텍트는 IPv6를 사용하기 위해 전체 EC2 인스턴스 플릿을 마이그레이션해야 합니다. 프라이빗 서브넷에 있는 EC2 인스턴스는 퍼블릭 인터넷에서 액세스할 수 없어야 합니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. 기존 VPC를 업데이트하고 사용자 지정 IPv6 CIDR 블록을 VPC 및 모든 서브넷과 연결합니다.
모든 VPC 라우팅 테이블을 업데이트하고 ::/0에 대한 경로를 인터넷 게이트웨이에 추가합니다.

B. 기존 VPC를 업데이트하고 Amazon 제공 IPv6 CIDR 블록을 VPC 및 모든 서브넷과 연결합니다. 모든 프라이빗 서브넷의 VPC 라우팅 테이블을 업데이트하고 NAT 게이트웨이에 ::/0에 대한 경로를 추가합니다.

C. 기존 VPC를 업데이트하고 Amazon 제공 IPv6 CIDR 블록을 VPC 및 모든 서브넷과 연결합니다. 외부 전용 인터넷 게이트웨이를 만듭니다. 모든 프라이빗 서브넷의 VPC 라우팅 테이블을 업데이트하고 외부 전용 인터넷 게이트웨이에 ::/0에 대한 경로를 추가합니다.

D. 기존 VPC를 업데이트하고 사용자 지정 IPv6 CIDR 블록을 VPC 및 모든 서브넷과 연결합니다. 새 NAT 게이트웨이를 생성하고 IPv6 지원을 활성화합니다. 모든 프라이빗 서브넷의 VPC 라우팅 테이블을 업데이트하고 IPv6 지원 NAT 게이트웨이에 ::/0에 대한 경로를 추가합니다.

Answer: C

QUESTION NO: 30
회사는 Amazon RDS for MySQL 데이터베이스를 사용하여 데이터를 저장하는 중요한 애플리케이션을 실행하고 있습니다. RDS DB 인스턴스는 다중 AZ 모드로 배포됩니다. 최근의 RDS 데이터베이스 장애 조치 테스트로 인해 애플리케이션이 40초 동안 중단되었습니다. 솔루션 설계자는 중단 시간을 20초 미만으로 줄이는 솔루션을 설계해야 합니다.
솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계 조합을 취해야 합니까? (3개를 선택합니다.)
A. 데이터베이스 앞에서 Memcached용 Amazon ElastiCache 사용
B. 데이터베이스 앞에서 Redis용 Amazon ElastiCache를 사용합니다.
C. 데이터베이스 앞에서 RDS Proxy 사용
D. 데이터베이스를 Amazon Aurora MySQL로 마이그레이션
E. Amazon Aurora 복제본 생성
F. MySQL 읽기 전용 복제본용 RDS 생성
Answer: C D E
Explanation:
Migrate the database to Amazon Aurora MySQL. - Create an Amazon Aurora Replica. - Use RDS Proxy in front of the database. - These options are correct because they address the requirement of reducing the failover time to less than 20 seconds. Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time. Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure. Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

QUESTION NO: 31
회사는 ALB(Application Load Balancer) 뒤에 있는 Amazon EC2 인스턴스에서 인트라넷 웹 애플리케이션을 호스팅합니다. 현재 사용자는 내부 사용자 데이터베이스에 대해 애플리케이션을 인증합니다.
회사는 기존 Microsoft Active Directory용 AWS Directory Service 디렉터리를 사용하여 애플리케이션에 대해 사용자를 인증해야 합니다. 디렉터리에 계정이 있는 모든 사용자는 애플리케이션에 액세스할 수 있어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. 디렉터리에 새 앱 클라이언트를 만듭니다. ALB에 대한 리스너 규칙을 생성합니다. 리스너 규칙에 대한 authenticate-oidc 작업을 지정합니다. Active Directory 서비스에 대한 적절한 발급자, 클라이언트 ID 및 암호, 끝점 세부 정보를 사용하여 수신기 규칙을 구성합니다. ALB가 제공하는 콜백 URL을 사용하여 새 앱 클라이언트를 구성하십시오.
B. Amazon Cognito 사용자 풀을 구성합니다. 디렉터리의 메타데이터가 있는 연합 IdP(ID 공급자)로 사용자 풀을 구성합니다. 앱 클라이언트를 만듭니다. 앱 클라이언트를 사용자 풀과 연결합니다. ALB에 대한 리스너 규칙을 생성합니다. 리스너 규칙에 대한 authenticate-cognito

작업을 지정합니다.
사용자 풀과 앱 클라이언트를 사용하도록 리스너 규칙을 구성합니다.
C. 디렉터리를 새로운 1AM ID 공급자(IdP)로 추가합니다. SAML 2.0 페더레이션의 엔터티 유형을 가진 새로운 1AM 역할을 생성합니다. ALB에 대한 액세스를 허용하는 역할 정책을 구성합니다. 새 역할을 IdP에 대한 기본 인증 사용자 역할로 구성합니다. ALB에 대한 리스너 규칙을 생성합니다. 리스너 규칙에 대한 authenticate-oidc 작업을 지정합니다.
D. AWS 1AM Identity Center(AWS Single Sign-On)를 활성화합니다. SAML을 사용하는 외부 ID 공급자(IdP)로 디렉터리를 구성합니다. 자동 프로비저닝 방법을 사용합니다. SAML 2.0 페더레이션의 엔터티 유형을 가진 새로운 1AM 역할을 생성합니다. ALB에 대한 액세스를 허용하는 역할 정책을 구성합니다.
모든 그룹에 새 역할을 연결합니다. ALB에 대한 리스너 규칙을 생성합니다. 리스너 규칙에 대한 authenticate-cognito 작업을 지정합니다.

Answer: A

Explanation:

The correct solution is to use the authenticate-oidc action for the ALB listener rule and configure it with the details of the AWS Directory Service for Microsoft Active Directory directory. This way, the ALB can use OpenID Connect (OIDC) to authenticate users against the directory and grant them access to the intranet web application. The app client in the directory is used to register the ALB as an OIDC client and provide the necessary credentials and endpoints. The callback URL is the URL that the ALB redirects the user to after a successful authentication. This solution does not require any additional services or roles, and it leverages the existing directory accounts for all users.

The other solutions are incorrect because they either use the wrong action for the ALB listener rule, or they involve unnecessary or incompatible services or roles. For example:

Solution B is incorrect because it uses Amazon Cognito user pool, which is a separate user directory service that does not integrate with AWS Directory Service for Microsoft Active Directory. To use this solution, the company would have to migrate or synchronize their users from the directory to the user pool, which is not required by the question. Moreover, the authenticate-cognito action for the ALB listener rule only works with Amazon Cognito user pools, not with federated identity providers (IdPs) that have metadata from the directory.

Solution C is incorrect because it uses IAM as an identity provider (IdP), which is not compatible with AWS Directory Service for Microsoft Active Directory. IAM can only be used as an IdP for web identity federation, which allows users to sign in with social media or other third-party IdPs, not with Active Directory. Moreover, the authenticate-oidc action for the ALB listener rule requires an OIDC IdP, not a SAML 2.0 federation IdP, which is what IAM provides.

Solution D is incorrect because it uses AWS IAM Identity Center (AWS Single Sign-On), which is a service that simplifies the management of SSO access to multiple AWS accounts and business applications. This service is not needed for the scenario in the question, which only involves a single intranet web application. Moreover, the authenticate-cognito action for the ALB listener rule does not work with external IdPs that use SAML, such as AWS IAM Identity Center.

References:

Authenticate users using an Application Load Balancer

What is AWS Directory Service for Microsoft Active Directory?

Using OpenID Connect for user authentication

QUESTION NO: 32
한 회사에서 웹 사이트를 온프레미스 데이터 센터에서 AWS로 마이그레이션하려고 합니다. 동시에 가용성과 비용 효율성을 개선하기 위해 웹사이트를 컨테이너화된 마이크로서비스 기반 아키텍처로 마이그레이션하려고 합니다. 회사의 보안 정책에는 권한과 네트워크 권한이 모범 사례에 따라 최소 권한을 사용하여 구성되어야 한다고 명시되어 있습니다.
Solutions Architect는 보안 요구 사항을 충족하고 Amazon ECS 클러스터에 애플리케이션을 배포한 컨테이너화된 아키텍처를 생성해야 합니다.
요구 사항을 충족하려면 배포 후 어떤 단계가 필요합니까? (2개를 선택하세요.)
A. 브리지 네트워크 모드를 사용하여 작업을 생성합니다.
B. awsvpc 네트워크 모드를 사용하여 작업을 생성합니다.
C. Amazon EC2 인스턴스에 보안 그룹을 적용하고 EC2 인스턴스에 대한 IAM 역할을 사용하여 다른 리소스에 액세스합니다.
D. 작업에 보안 그룹을 적용하고 시작 시 IAM 자격 증명을 컨테이너에 전달하여 다른 리소스에 액세스합니다.
E. 작업에 보안 그룹을 적용하고 작업에 대한 IAM 역할을 사용하여 다른 리소스에 액세스합니다.
Answer: B E
Explanation: The awsvpc network mode provides each task with its own elastic network interface (ENI) and a primary private IP address1. By using this network mode, the solutions architect can isolate the tasks from each other and apply security groups to the tasks directly2. This way, the solutions architect can control the inbound and outbound traffic at the task level and enforce the least privilege principle3. IAM roles for tasks allow the solutions architect to assign permissions to each task separately, so that they can access other AWS resources that they need4. By using IAM roles for tasks, the solutions architect can avoid passing IAM credentials into the container at launch time, which is less secure and more prone to errors5.
References:
awsvpc network mode
Task networking with the awsvpc network mode
Security groups for your VPC
IAM roles for tasks
Best practices for managing AWS access keys

QUESTION NO: 33
스마트 자동차를 제조하는 회사입니다. 회사는 맞춤형 애플리케이션을 사용하여 차량 데이터를 수집합니다. 차량은 MQTT 프로토콜을 사용하여 애플리케이션에 연결합니다. 회사는 5분 간격으로 데이터를 처리합니다. 그런 다음 회사는 차량 텔레매틱스 데이터를 온프레미스 스토리지에 복사합니다. 맞춤형 애플리케이션은 이 데이터를 분석하여 이상을 감지합니다.
데이터를 전송하는 차량의 수는 지속적으로 증가하고 있습니다. 최신 차량은 많은 양의 데이터를 생성합니다. 온프레미스 스토리지 솔루션은 피크 트래픽에 맞게 확장할 수 없으므로 데이터 손실이 발생합니다. 회사는 솔루션을 현대화하고 솔루션을 AWS로 마이그레이션하여 확장 문제를 해결해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS IOT Greengrass를 사용하여 차량 데이터를 Amazon Managed Streaming for Apache Kafka(Amazon MSK)로 보냅니다. Amazon S3에 데이터를 저장할 Apache Kafka 애플리케이션을 생성합니다. Amazon SageMaker에서 사전 훈련된 모델을 사용하여 이상을 감지합니다.

B. AWS IOT Core를 사용하여 차량 데이터를 수신합니다. Amazon S3에 데이터를 저장하는 Amazon Kinesis Data Firehose 전송 스트림으로 데이터를 라우팅하도록 규칙을 구성합니다. 이상을 감지하기 위해 전송 스트림에서 읽는 Amazon Kinesis Data Analytics 애플리케이션을 생성합니다.

C. AWS IOT FleetWise를 사용하여 차량 데이터를 수집합니다. 데이터를 Amazon Kinesis 데이터 스트림으로 보냅니다.
Amazon Kinesis Data Firehose 전송 스트림을 사용하여 Amazon S3에 데이터를 저장합니다. AWS Glue에 내장된 기계 학습 변환을 사용하여 이상을 감지합니다.

D. RabbitMQ용 Amazon MQ를 사용하여 차량 데이터를 수집합니다. 데이터를 Amazon Kinesis Data Firehose 전송 스트림으로 보내 Amazon S3에 데이터를 저장합니다. Amazon Lookout for Metrics를 사용하여 이상 징후를 탐지하십시오.

Answer: B

Explanation:

Using AWS IoT Core to receive the vehicle data will enable connecting the smart vehicles to the cloud using the MQTT protocol1. AWS IoT Core is a platform that enables you to connect devices to AWS Services and other devices, secure data and interactions, process and act upon device data, and enable applications to interact with devices even when they are offline2. Configuring rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3 will enable processing and storing the vehicle data in a scalable and reliable way3. Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3. Creating an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies will enable analyzing the vehicle data using SQL queries or Apache Flink applications. Amazon Kinesis Data Analytics is a fully managed service that enables you to process and analyze streaming data using SQL or Java.

QUESTION NO: 34

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: 35
한 회사가 인프라를 AWS 클라우드로 마이그레이션하고 있습니다. 회사는 다양한 프로젝트에 대한 다양한 규제 표준을 준수해야 합니다. 회사에는 다중 계정 환경이 필요합니다.
솔루션 아키텍트는 기본 인프라를 준비해야 합니다. 솔루션은 일관된 관리 및 보안 기준을 제공해야 하지만 다양한 AWS 계정 내의 다양한 규정 준수 요구 사항에 대한 유연성을 허용해야 합니다. 또한 솔루션은 기존 온-프레미스 AD FS(Active Directory Federation Services) 서버와 통합되어야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. AWS Organizations에서 조직을 생성합니다. 모든 계정에 대한 최소 권한 액세스를 위해 단일 SCP를 만듭니다. 모든 계정에 대해 단일 OU를 만듭니다. 온프레미스 AD FS 서버와의 연동을 위해 IAM ID 공급자를 구성합니다. 로그 이벤트를 중앙 계정으로 보내려면 로그 생성 서비스에 대해 정의된 프로세스로 중앙 로깅 계정을 구성합니다. 모든 계정에 대한 적합성 팩을 사용하여 중앙 계정에서 AWS Config를 활성화합니다.
B. AWS Organizations에서 조직을 생성합니다. 조직에서 AWS Control Tower를 활성화합니다. SCP에 포함된 제어(가드레일)를 검토합니다. 추가가 필요한 영역은 AWS Config를 확인하세요. 필요에 따라 OUS를 추가합니다. AWS IAM Identity Center(AWS Single Sign-On)를 온프레미스 AD FS 서버에 연결합니다.
C. AWS Organizations에서 조직을 생성합니다. 최소 권한 액세스를 위해 SCP를 생성합니다. OU 구조를 생성하고 이를 사용하여 AWS 계정을 그룹화합니다. AWS IAM Identity Center(AWS Single Sign-On)를 온프레미스 AD FS 서버에 연결합니다. 로그 이벤트를 중앙 계정으로 보내려면 로그 생성 서비스에 대해 정의된 프로세스로 중앙 로깅 계정을 구성합니다. 집계자 및 적합성 팩을 사용하여 중앙 계정에서 AWS Config를 활성화합니다.
D. AWS Organizations에서 조직을 생성합니다. 조직에서 AWS Control Tower를 활성화합니다. SCP에 포함된 제어(가드레일)를 검토합니다. 추가가 필요한 영역은 AWS Config를 확인하세요. 온프레미스 AD FS 서버와의 연동을 위해 IAM ID 공급자를 구성합니다.
Answer: B