301 (고민석) 1회차 完

◆ | **Q#0301.** | **Ref#0301.**
한 회사가 AWS Lambda 함수에서 실행될 애플리케이션을 구축하고 있습니다. 수백 명의 고객이 응용 프로그램을 사용합니다. 회사는 각 고객에게 특정 기간 동안 요청 할당량을 제공하려고 합니다. 할당량은 고객 사용 패턴과 일치해야 합니다. 일부 고객은 더 짧은 기간 동안 더 높은 할당량을 받아야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 프록시 통합을 통해 Amazon API Gateway REST API를 생성하여 Lambda 함수를 호출합니다. 각 고객에 대해 적절한 요청 할당량이 포함된 API Gateway 사용 계획을 구성합니다. 고객이 필요로 하는 사용자별 사용량 계획에서 API 키를 생성합니다.
> **B.** 프록시 통합을 통해 Amazon API Gateway HTTP API를 생성하여 Lambda 함수를 호출합니다. 각 고객에 대해 적절한 요청 할당량이 포함된 API Gateway 사용 계획을 구성합니다. 각 사용 계획에 대한 경로 수준 조절을 구성합니다. 고객이 필요로 하는 사용자별 사용량 계획에서 API Key를 생성합니다.
> **C.** 각 고객에 대한 Lambda 함수 별칭을 생성합니다. 적절한 요청 할당량과 함께 동시성 제한을 포함합니다. 각 함수 별칭에 대한 Lambda 함수 URL을 생성합니다. 관련 고객과 각 별칭에 대한 Lambda 함수 URL을 공유합니다.
> **D.** VPC에 ALB(Application Load Balancer)를 생성합니다. Lambda 함수를 ALB의 대상으로 구성합니다. ALB에 대한 AWS WAF 웹 ACL을 구성합니다. 각 고객에 대해 적절한 요청 할당량이 포함된 규칙 기반 규칙을 구성합니다.
>
> 해설
> 정답: A
> Amazon API Gateway REST API: 이 API를 사용하면 RESTful 서비스를 손쉽게 설정하고 관리할 수 있으며, Lambda 함수와의 프록시 통합을 통해 유연한 백엔드 서비스 호출이 가능합니다.
> 사용량 계획: API Gateway 사용량 계획을 통해 각 고객의 요청 할당량을 관리할 수 있습니다.
> API 키: 고객별로 API 키를 생성하여 사용량 계획을 적용함으로써, 각 고객의 사용량을 개별적으로 추적하고 관리할 수 있습니다.

◆ | **Q#0302.** | **Ref#0302.**
한 회사는 120개의 VM으로 구성된 온프레미스 VMware 클러스터를 AWS로 마이그레이션할 계획입니다. VM에는 다양한 운영 체제와 다양한 맞춤형 소프트웨어 패키지가 설치되어 있습니다. 이 회사에는 크기가 10TB인 온프레미스 NFS 서버도 있습니다. 회사는 마이그레이션을 위해 AWS에 10Gbps AWS Direct Connect 연결을 설정했습니다.

가장 짧은 시간 내에 AWS로의 마이그레이션을 완료할 솔루션은 무엇입니까?

> **A.** 온프레미스 VM을 내보내고 Amazon S3 버킷에 복사합니다. VM Import/Export를 사용하여 Amazon S3에 저장된 VM 이미지에서 AMI를 생성합니다. AWS Snowball Edge 디바이스를 주문하세요. NFS 서버 데이터를 장치에 복사합니다. NFS가 구성된 Amazon EC2 인스턴스로 NFS 서버 데이터를 복원합니다.
> **B.** VMware 클러스터에 연결하여 AWS Application Migration Service를 구성합니다. VMS에 대한 복제 작업을 생성합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. Direct Connect 연결을 통해 NFS 서버 데이터를 EFS 파일 시스템에 복사하도록 AWS DataSync를 구성합니다.
> **C.** AWS에서 VM을 Amazon EC2 인스턴스로 다시 생성합니다. 필요한 모든 소프트웨어 패키지를 설치합니다. Lustre 파일 시스템용 Amazon FSx를 생성합니다. Direct Connect 연결을 통해 NFS 서버 데이터를 FSx for Lustre 파일 시스템에 복사하도록 AWS DataSync를 구성합니다.
> **D.** AWS Snowball Edge 디바이스 2개를 주문합니다. VM 및 NFS 서버 데이터를 디바이스에 복사합

니다. 디바이스의 데이터가 Amazon S3 버킷에 로드된 후 VM Import/Export를 실행합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. Amazon S3의 NFS 서버 데이터를 EFS 파일 시스템에 복사합니다.

해설
정답: B
AWS Application Migration Service는 온프레미스의 VMware VM의 상태를 지속적으로 추적하고 (AWS 클라우드로) 중앙집중식으로 복제하는 서비스입니다. 이로 인해 VM이 점진적으로 이동되어 마이그레이션 시 필요한 다운타임이 최소화됩니다
또한 AWS DataSync는 온프레미스 서버에서 AWS로 데이터를 신속하게 및 안전하게 전송할 수 있습니다. 회사가 10 Gbps의 AWS Direct Connect을 설정한 데 따라 이 서비스는 온프레미스 NFS 서버의 데이터를 빠르게 AWS로 이동시킵니다
A: 이 선택지는 VM을 내보내고 다시 가져와야 하며 시간이 오래 걸립니다. C: VM을 AWS에서 새로 생성하고 모든 필요한 소프트웨어 패키지를 설치하면 시간이 많이 소요됩니다.D: Snowball Edge를 사용해서 VM과 NFS 서버 데이터를 복사하면 시간이 오래걸리고, 데이터를 S3 버킷으로 마이그레이션하고 나서 VM Import/Export를 실행해야 하므로 추가 시간이 소요됩니다

◆ | **Q#0303.** | **Ref#0303.**
온라인 설문 조사 회사는 AWS 클라우드에서 애플리케이션을 실행합니다. 애플리케이션은 분산되어 있으며 자동으로 확장되는 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 실행되는 마이크로서비스로 구성됩니다. ECS 클러스터는 ALB(Application Load Balancer)의 대상입니다. ALB는 Amazon CloudFront 배포의 사용자 지정 오리진입니다.

회사에는 민감한 데이터가 포함된 설문조사가 있습니다. 민감한 데이터는 애플리케이션을 통해 이동할 때 암호화되어야 합니다. 애플리케이션의 데이터 처리 마이크로서비스는 데이터를 해독할 수 있는 유일한 마이크로서비스입니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 데이터 처리 마이크로서비스 전용 대칭 AWS Key Management Service(AWS KMS) 키를 생성합니다. 필드 수준 암호화 프로필 및 구성을 만듭니다. KMS 키와 구성을 CloudFront 캐시 동작과 연결합니다.
B. 데이터 처리 마이크로서비스 전용 RSA 키 쌍을 생성합니다. CloudFront 배포에 퍼블릭 키를 업로드합니다. 필드 수준 암호화 프로필 및 구성을 만듭니다. CloudFront 캐시 동작에 구성을 추가합니다.
C. 데이터 처리 마이크로서비스 전용 대칭 AWS Key Management Service(AWS KMS) 키를 생성합니다. Lambda@Edge 함수를 생성합니다. KMS 키를 사용하여 민감한 데이터를 암호화하는 기능을 프로그래밍하세요.
D. 데이터 처리 마이크로서비스 전용 RSA 키 쌍을 생성합니다. Lambda@Edge 함수를 생성합니다. RSA 키 쌍의 개인 키를 사용하여 민감한 데이터를 암호화하는 기능을 프로그래밍합니다.

해설
정답: B
CloudFront 필드 수준 암호화를 사용하면 CloudFront에서 민감한 데이터를 암호화하고 오직 데이터 핸들링 마이크로서비스에서만 복호화할 수 있도록 RSA 키 페어를 사용합니다
데이터를 처리하는 마이크로서비스만이 데이터를 복호화 할 수 있어야 하므로, 답은 B입니다. AWS KMS(A,C) 키나 Lambda@Edge 함수(C,D)를 사용하는 선택지는 복호화가 가능한 위치를 제한하지 않습니다.

◆ | **Q#0304.** | **Ref#0304.**
솔루션 설계자는 기존 VPC에 대한 DNS 전략을 결정하고 있습니다. VPC는 10.24.34.0/24 CIDR 블록을 사용하도록 프로비저닝됩니다. 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 활성화 DnsHostnames 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.** VPA의 활성화DnsSupport 속성을 비활성화합니다. VPC의 활성화DnsHostnames 속성을 활성화하고 새 VPC DHCP 옵션 세트를 생성하고 doman-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.
>
> 해설
> 정답: B
> 프라이빗 호스티드 존 생성: 프라이빗 호스티드 존을 생성하고 VPC에 연결하여 프라이빗 DNS 쿼리를 지원합니다.
> VPC 속성 활성화: enableDnsSupport와 enableDnsHostnames 속성을 활성화하여 인스턴스가 DNS를 사용할 수 있도록 합니다.
> DHCP 옵션 세트 구성: Amazon 제공 DNS를 사용하는 새 DHCP 옵션 세트를 생성하고 VPC에 연결하여 공용 IP 주소를 가진 인스턴스가 공용 호스트 이름을 받을 수 있도록 합니다.

◆ | **Q#0305.** | **Ref#0305.**
데이터 분석 회사에는 여러 예약 노드로 구성된 Amazon Redshift 클러스터가 있습니다. 직원 팀이 심층 감사 분석 보고서를 작성하고 있기 때문에 클러스터에서 예상치 못한 사용량 급증이 발생하고 있습니다. 보고서를 생성하는 쿼리는 복잡한 읽기 쿼리이며 CPU를 많이 사용합니다.

비즈니스 요구 사항에 따라 클러스터는 항상 쿼리 읽기 및 쓰기 서비스를 제공할 수 있어야 합니다. 솔루션 설계자는 급증하는 사용량을 수용할 수 있는 솔루션을 고안해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** Amazon EMR 클러스터 프로비저닝 복잡한 데이터 처리 작업을 오프로드합니다.
> **B.** Amazon CloudWatch의 클러스터 CPU 지표가 80%에 도달하면 클래식 크기 조정 작업을 사용하여 Amazon Redshift 클러스터에 용량을 추가하는 AWS Lambda 함수를 배포합니다.
> **C.** Amazon CloudWatch의 클러스터 CPU 지표가 80%에 도달하면 탄력적 크기 조정 작업을 사용하여 Amazon Redshift 클러스터에 용량을 추가하는 AWS Lambda 함수를 배포합니다.
> **D.** Amazon Redshift 클러스터에 대한 동시성 확장 기능을 활성화합니다.
>
> 해설
> 정답:D
> 동시성 확장 기능은 사용량이 많을 때 추가 용량을 제공하여 사용량의 급증을 처리할 수 있도록 합니다. 일관되게 빠른 쿼리 성능으로 수천 0 동시 사용자와 동시 쿼리를 지원할 수 있어 단기적인 사용량 증가 처리에 적합하고, Amazon Redshift은 매달 일정 시간 동안 무료 크레딧을 제공하여 비용적인 면에서 효율적입니다

◆ | **Q#0306.** | **Ref#0306.**
한 연구 센터가 AWS 클라우드로 마이그레이션하고 있으며 온프레미스 1PB 객체 스토리지를 Amazon S3 버킷으로 이동했습니다. 100명의 과학자들이 이 객체 스토리지를 사용하여 업무 관련 문서를 저장하고 있습니다. 각 과학자는 개체 저장소에 개인 폴더를 가지고 있습니다. 모든 과학자는 단일 IAM 사용자 그룹의 구성원입니다.

연구 센터의 규정 준수 담당자는 과학자들이 서로의 작업에 접근할 수 있을지 걱정하고 있습니다. 연구 센터는 어떤 과학자가 어떤 문서에 접근하는지 보고할 엄격한 의무가 있습니다. 이러한 보고서를 담당하는 팀은 AWS 경험이 거의 없으며 운영 오버헤드를 최소화하는 즉시 사용 가능한 솔루션을 원합니다.

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

> **A.** 사용자에게 읽기 및 쓰기 액세스 권한을 부여하는 ID 정책을 만듭니다. S3 경로 앞에 $(aws:username)이 붙어야 함을 지정하는 조건을 추가합니다. 과학자의 IAM 사용자 그룹에 정책을 적용합니다.
> **B.** S3 버킷의 모든 객체 수준 이벤트를 캡처하도록 AWS CloudTrail을 사용하여 추적을 구성합니다. 트레일 출력을 다른 S3 버킷에 저장합니다. Amazon Athena를 사용하여 로그를 쿼리하고 보고서를 생성합니다.
> **C.** S3 서버 액세스 로깅을 활성화합니다. 로그 전송 대상으로 다른 S3 버킷을 구성합니다. Amazon Athena를 사용하여 로그를 쿼리하고 보고서를 생성합니다.
> **D.** 과학자의 IAM 사용자 그룹에 속한 사용자에게 읽기 및 쓰기 액세스 권한을 부여하는 S3 버킷 정책을 생성합니다.
> **E.** S3 버킷의 모든 객체 수준 이벤트를 캡처하고 Amazon CloudWatch에 이벤트를 기록하도록 AWS CloudTrail을 사용하여 추적을 구성합니다. Amazon Athena CloudWatch 커넥터를 사용하여 로그를 쿼리하고 보고서를 생성합니다.
>
> 해설
> 정답: A,B
> A: 여기에서는 $(aws:username)으로 시작하는 S3 경로를 사용하는 조건이 설정된 IAM 정책을 작성하고, 이를 과학자들의 IAM 사용자 그룹에 적용하여 과학자들이 서로의 작업에 접근하는 것을 방지할 수 있습니다.
> B: AWS CloudTrail은 사용자 활동과 API 사용에 대한 세부 정보를 기록하고 로깅하는 서비스입니다. Amazon Athena는 대규모 데이터 세트를 분석하고 쿼리할 수 있는 대화식 쿼리 서비스입니다. CloudTrail을 사용하여 S3 버킷에서 발생하는 모든 객체 레벨 이벤트를 캡처하고, Amazon Athena를 사용해서 로그를 쿼리하고 보고서를 생성하게 합니다
> 이 방법으로, 연구소는 과학자가 어떤 문서에 접근했는지에 대한 엄밀한 보고를 만들 수 있습니다0

◆ | **Q#0307.** | **Ref#0307.**
회사는 AWS Organizations를 사용하여 다중 계정 구조를 관리합니다. 이 회사는 수백 개의 AWS 계정을 보유하고 있으며 계정 수가 더 늘어날 것으로 예상하고 있습니다. 회사는 Docker 이미지를 사용하는 새로운 애플리케이션을 구축하고 있습니다. 회사는 Docker 이미지를 Amazon Elastic Container Registry(Amazon ECR)로 푸시합니다. 회사 조직 내의 계정만 이미지에 액세스할 수 있어야 합니다.

회사에는 자주 실행되는 CI/CD 프로세스가 있습니다. 회사는 태그가 지정된 모든 이미지를 유지하려고 합니다. 그러나 회사는 태그가 지정되지 않은 가장 최근의 5개 이미지만 유지하려고 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** Amazon ECR에 프라이빗 리포지토리를 생성합니다. 필수 ECR 작업만 허용하는 저장소에 대한 권한 정책을 생성합니다. aws:PrincipalOrgID 조건 키의 값이 회사 조직의 ID와 동일한 경우 ECR 작업을 허용하는 조건을 포함합니다. 5개 이상의 태그가 지정되지 않은 이미지를 모두 삭제하는 수명 주기 규칙을 ECR 저장소에 추가합니다.
> **B.** Amazon ECR에 퍼블릭 리포지토리를 생성합니다. ECR 계정에 IAM 역할을 생성합니다. aws:PrincipalOrgID 조건 키의 값이 회사 조직의 ID와 동일한 경우 모든 계정이 역할을 맡을 수 있도록 권한을 설정합니다. 5개가 넘는 태그가 지정되지 않은 이미지를 모두 삭제하는 수명 주기 규칙을

ECR 저장소에 추가합니다.
C. Amazon ECR에 프라이빗 리포지토리를 생성합니다. 필수 ECR 작업만 포함하는 저장소에 대한 권한 정책을 생성합니다. 조직의 모든 계정 ID에 대해 ECR 작업을 허용하는 조건을 포함합니다. 5개 이상의 태그가 지정되지 않은 모든 이미지를 삭제하는 AWS Lambda 함수를 호출하도록 일일 Amazon EventBridge 규칙을 예약합니다.
D. Amazon ECR에 퍼블릭 리포지토리를 생성합니다. 회사가 가져와야 하는 이미지에 대한 필수 권한이 포함된 엔드포인트 정책과 함께 인터페이스 VPC 엔드포인트를 사용하도록 Amazon ECR을 구성합니다. 회사 조직의 모든 계정 ID에 대해 ECR 작업을 허용하는 조건을 포함합니다. 5개 이상의 태그가 지정되지 않은 이미지를 모두 삭제하는 AWS Lambda 함수를 호출하도록 일일 Amazon EventBridge 규칙을 예약합니다.

해설
정답: A
A 솔루션이 AWS 조직 내의 계정들만이 이미지에 접근할 수 있도록 하고, 이미지 관리를 위한 라이프사이클 규칙을 설정하여 작업 부하를 최소화합니다. 필요한 ECR 작업들만을 포함하는 정책을 설정함으로써, 보안 요구사항도 충족시키는 방법입니다
나머지 선택지들은 불필요한 추가적인 작업을 필요로 하거나, 보안 요구사항을 충족시키지 못합니다.

◆ | **Q#0308.** | **Ref#0308.**
솔루션 아키텍트는 Amazon RDS DB 인스턴스의 스냅샷을 생성하는 회사의 프로세스를 검토하고 있습니다. 회사는 매일 자동 스냅샷을 촬영하고 해당 스냅샷을 7일 동안 보관합니다.

솔루션 설계자는 6시간마다 스냅샷을 생성하고 30일 동안 스냅샷을 유지하는 솔루션을 권장해야 합니다. 회사는 AWS Organizations를 사용하여 모든 AWS 계정을 관리합니다. 회사에는 RDS 스냅샷 상태에 대한 통합 보기가 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Backup에서 교차 계정 관리 기능을 활성화합니다. 빈도 및 보존 요구 사항을 지정하는 백업 계획을 만듭니다. DB 인스턴스에 태그를 추가합니다. 태그를 사용하여 백업 계획을 적용합니다. AWS Backup을 사용하여 백업 상태를 모니터링합니다.
B. Amazon RDS에서 교차 계정 관리 기능을 활성화합니다. 빈도 및 보존 요구 사항을 지정하는 스냅샷 글로벌 정책을 만듭니다. 백업 상태를 모니터링하려면 마스터 계정의 RDS 콘솔을 사용하십시오.
C. AWS CloudFormation에서 교차 계정 관리 기능을 활성화합니다. 마스터 계정에서 빈도 및 보존 요구 사항을 지정하는 AWS Backup의 백업 계획이 포함된 CloudFormation 스택 세트를 배포합니다. 백업 상태를 모니터링하려면 마스터 계정에서 AWS Lambda 함수를 생성하세요. 일정에 따라 Lambda 함수를 실행하려면 각 계정에 Amazon EventBridge 규칙을 생성하세요.
D. 각 계정에서 AWS Backup을 구성합니다. 빈도 및 보존 요구 사항을 지정하는 Amazon Data Lifecycle Manager 수명 주기 정책을 생성합니다. DB 인스턴스를 대상 리소스로 지정 각 멤버 계정의 Amazon Data Lifecycle Manager 콘솔을 사용하여 백업 상태를 모니터링합니다.

해설
정답: A
AWS Backup은 중앙에서 백업 정책을 설정하고, 관리하고, 구동하며, 사용할 수 있다는 장점이 있습니다. 백업 작업의 상태도 AWS Backup에서 볼 수 있기 때문에 실질적인 작업 부하를 최소화하는데 도움이 됩니다. 이 방법은 각각의 AWS 계정마다 개별 설정을 하는 것보다 훨씬 운영 부하를 줄일 수 있습니다

◆ | **Q#0309.** | **Ref#0309.**
회사는 다중 계정 아키텍처로 AWS Organizations를 사용하고 있습니다. 계정 아키텍처에 대한 회사의 현재 보안 구성에는 SCP, 리소스 기반 정책, ID 기반 정책, 신뢰 정책 및 세션 정책이 포함됩니다.

솔루션 아키텍트는 계정 A의 IAM 사용자가 계정 B의 역할을 맡도록 허용해야 합니다.

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

> **A.** 작업을 허용하도록 계정 A에 대한 SCP를 구성합니다.
> **B.** 해당 작업을 허용하도록 리소스 기반 정책을 구성합니다.
> **C.** 작업을 허용하도록 계정 A의 사용자에 대한 자격 증명 기반 정책을 구성합니다.
> **D.** 작업을 허용하도록 계정 B의 사용자에 대한 자격 증명 기반 정책을 구성합니다.
> **E.** 작업을 허용하도록 계정 B의 대상 역할에 대한 신뢰 정책을 구성합니다.
> **F.** 작업을 허용하고 GetSessionToken API 작업을 통해 프로그래밍 방식으로 전달되도록 세션 정책을 구성합니다.
>
> 해설
> 정답: A,C,E
> 먼저, AWS Organizations에서 SCP(Service Control Policy)는 조직 내에서 멤버 AWS 계정이 수행할 수 있는 작업을 정의합니다.(A)
> 둘째, 사용자에 대한 신원 기반 정책은 특정 사용자가 수행할 수 있는 작업과 그 작업을 수행할 수 있는 리소스를 허용하거나 거부합니다.(C)0
> 마지막으로, 계정 B의 대상 역할에 대한 신뢰 정책(Trust Policy)은 특정 계정, 서비스, 사용자가 이 역할을 가정할 수 있음을 명시합니다.(E)0
> 이 세 가지 설정을 통해 IAM 사용자는 계정 A에서 계정 B의 역할을 가정하고, 계정 B의 AWS 리소스에 대한 작업을 수행할 수 있게 됩니다.

◆ | **Q#0310.** | **Ref#0310.**
한 회사에서 Amazon S3를 사용하여 온프레미스 파일 스토리지 솔루션을 백업하려고 합니다. 회사의 온프레미스 파일 스토리지 솔루션은 NFS를 지원하며 회사는 NFS를 지원하는 새로운 솔루션을 원합니다. 회사에서는 5일 후에 백업 파일을 보관하려고 합니다. 회사에 재해 복구를 위해 보관된 파일이 필요한 경우 회사는 해당 파일을 검색할 때까지 며칠 정도 기다릴 의향이 있습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** S3 버킷과 연결된 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 온프레미스 파일 스토리지 솔루션에서 파일 게이트웨이로 파일을 이동합니다. 5일 후에 파일을 S3 Standard-Infrequent Access(S3 Standard-IA)로 이동하는 S3 수명 주기 규칙을 생성합니다.
> **B.** S3 버킷과 연결된 AWS Storage Gateway 볼륨 게이트웨이를 배포합니다. 온프레미스 파일 스토리지 솔루션에서 볼륨 게이트웨이로 파일을 이동합니다. 5일 후에 파일을 S3 Glacier Deep Archive로 이동하는 S3 수명 주기 규칙을 생성합니다.
> **C.** S3 버킷과 연결된 AWS Storage Gateway 테이프 게이트웨이를 배포합니다. 온프레미스 파일 스토리지 솔루션에서 테이프 게이트웨이로 파일을 이동합니다. 5일 후에 파일을 S3 Standard-Infrequent Access(S3 Standard-IA)로 이동하는 S3 수명 주기 규칙을 생성합니다.
> **D.** S3 버킷과 연결된 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 온프레미스 파일 스토리지 솔루션에서 파일 게이트웨이로 파일을 이동합니다. 5일 후에 파일을 S3 Glacier Deep Archive로 이동하는 S3 수명 주기 규칙을 생성합니다.
>
> 해설
> 정답: D
> 파일 게이트웨이는 가상의 온프레미스 파일 서버를 제공하며, 이를 통해 NFS와 같은 표준 파일 저장 프로토콜을 통해 Amazon S3 객체를 저장하고 검색할 수 있습니다. 또한, S3 Glacier Deep Archive는 몇 일 동안의 검색 시간이 허용되는 Amazon S3의 가장 저렴한 저장소 클래스입니다. 이러한 측면들이 온프레미스 환경에서 장기적인 보관, 재해 복구를 매우 비용 효율적으로 만듭니다.

311 (신재경) 1회차 完

◆ | **Q#0311.** | **Ref#0311.**
회사는 Amazon EC2 인스턴스와 AWS Lambda 함수에서 애플리케이션을 실행합니다. EC2 인스턴스는 지속적이고 안정적인 로드를 경험합니다. Lambda 함수는 다양하고 예측할 수 없는 로드를 경험합니다. 애플리케이션에는 Amazon MemoryDB for Redis 클러스터를 사용하는 캐싱 계층이 포함되어 있습니다.

솔루션 설계자는 회사의 전체 월별 비용을 최소화할 수 있는 솔루션을 권장해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** EC2 인스턴스를 보장하려면 EC2 인스턴스 Savings Plan을 구매하세요. Lambda 함수의 최소 예상 소비량을 충당하려면 Lambda용 컴퓨팅 절감 플랜을 구매하세요. MemoryDB 캐시 노드를 포함하려면 예약 노드를 구매하세요.
> **B.** EC2 인스턴스를 포함하는 Compute Savings Plan을 구매하세요. 예상되는 Lambda 사용량을 처리하려면 Lambda 예약 동시성을 구매하세요. MemoryDB 캐시 노드를 포함하려면 예약 노드를 구매하세요.
> **C.** EC2 인스턴스, Lambda 함수 및 MemoryDB 캐시 노드의 전체 예상 비용을 충당하려면 Compute Savings Plan을 구매하세요.
> **D.** EC2 인스턴스와 MemoryDB 캐시 노드를 포함하는 Compute Savings Plan을 구매하세요. 예상되는 Lambda 사용량을 처리하려면 Lambda 예약 동시성을 구매하세요.
>
> 해설
> 정답: A
>
> EC2 - Instance Saving Plan, MemoryDB - Reserved Node, Lambda - Compute Saving Plan
> Lambda Compute Saving Plans은 MemoryDB를 커버하지 않음.
> B(x), D(x): Lambda의 예약 동시성(Reserved Concurrency)은 비용 절약을 제공하지 않음. => Lambda용 Compute Saving Plan

◆ | **Q#0312.** | **Ref#0312.**
한 회사가 Amazon EC2 인스턴스에서 새로운 온라인 게임을 출시하고 있습니다. 게임은 전 세계적으로 이용 가능해야 합니다. 회사는 us-east-1, eu-west-1 및 ap-southeast-1의 3개 AWS 리전에서 게임을 실행할 계획입니다. 게임의 순위표, 플레이어 인벤토리 및 이벤트 상태는 여러 지역에서 사용할 수 있어야 합니다.

솔루션 설계자는 모든 지역의 로드를 처리할 수 있도록 확장할 수 있는 기능을 모든 지역에 제공하는 솔루션을 설계해야 합니다. 또한 사용자는 지연 시간이 가장 짧은 지역에 자동으로 연결해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** EC2 스팟 집합을 생성합니다. 각 리전의 NLB(Network Load Balancer)에 스팟 집합을 연결합니다. NLB를 가리키는 AWS Global Accelerator IP 주소를 생성합니다. Global Accelerator IP 주소에 대한 Amazon Route 53 지연 시간 기반 라우팅 항목을 생성합니다. 각 리전의 MySQL용 Amazon RDS DB 인스턴스에 게임 메타데이터를 저장합니다. 다른 리전에 읽기 전용 복제본을 설정하세요.
> **B.** EC2 인스턴스용 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 각 리전의 NLB(Network Load Balancer)에 연결합니다. 각 지역에 대해 지리 근접 라우팅을 사용하고 해당 지역의 NLB를 가리키는 Amazon Route 53 항목을 생성합니다. 각 지역의 EC2 인스턴스에 있는 MySQL 데이터베이스에 게임 메타데이터를 저장합니다. 각 리전의 데이터베이스 EC2 인스턴스 간 복제를 설정합니다.
> **C.** EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 각 리전의 Network Load Balancer(NLB)에 연결합니다. 각 지역에 대해 지연 시간 기반 라우팅을 사용하고 해당 지역의

NLB를 가리키는 Amazon Route 53 항목을 생성합니다. 게임 메타데이터를 Amazon DynamoDB 전역 테이블에 저장합니다.
D. EC2 글로벌 뷰를 사용하세요. 각 지역에 EC2 인스턴스를 배포합니다. 인스턴스를 Network Load Balancer(NLB)에 연결합니다. 각 리전의 EC2 인스턴스에 DNS 서버를 배포합니다. 각 DNS 서버에 사용자 지정 논리를 설정하여 사용자를 가장 짧은 지연 시간을 제공하는 지역으로 리디렉션합니다. 게임 메타데이터를 Amazon Aurora 글로벌 데이터베이스에 저장합니다.

해설
정답: C

latency-based routing과 DynamoDB global table이라는 키워드가 나타나며, 이 두 가지 요구사항은 옵션 C에만 포함되어 있습니다.
latency-based routing은 사용자가 자동으로 가장 낮은 지연 시간을 제공하는 지역에 연결되도록 하고, DynamoDB global table은 게임의 리더보드, 플레이어 인벤토리, 이벤트 상태 등의 정보를 전역적으로 사용 가능하게 함으로써,
모든 지역이 부하를 처리할 수 있게 합니다.

◆ | **Q#0313.** | **Ref#0313.**
회사는 회사의 AWS 환경에서 나가는 트래픽을 모니터링하고 보호하기 위해 AWS Marketplace의 타사 방화벽 어플라이언스 솔루션을 배포하고 있습니다. 회사는 이 어플라이언스를 공유 서비스 VPC에 배포하고 모든 아웃바운드 인터넷 바인딩 트래픽을 어플라이언스를 통해 라우팅하려고 합니다.

솔루션 아키텍트는 안정성을 우선시하고 단일 AWS 리전 내 방화벽 어플라이언스 간의 장애 조치 시간을 최소화하는 배포 방법을 권장해야 합니다. 회사는 공유 서비스 VPC에서 다른 VPC로의 라우팅을 설정했습니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 단계를 권장해야 합니까? (3개를 선택하세요.)

A. 두 개의 방화벽 어플라이언스를 각각 별도의 가용 영역에 있는 공유 서비스 VPC에 배포합니다.
B. 공유 서비스 VPC에 새 Network Load Balancer를 생성합니다. 새 대상 그룹을 생성하고 이를 새 Network Load Balancer에 연결합니다. 각 방화벽 어플라이언스 인스턴스를 대상 그룹에 추가합니다.
C. 공유 서비스 VPC에서 새 게이트웨이 로드 밸런서를 생성합니다. 새 대상 그룹을 생성하고 이를 새 게이트웨이 로드 밸런서에 연결합니다. 각 방화벽 어플라이언스 인스턴스를 대상 그룹에 추가합니다.
D. VPC 인터페이스 엔드포인트를 생성합니다. 공유 서비스 VPC의 라우팅 테이블에 경로를 추가합니다. 다른 VPC에서 공유 서비스 VPC로 들어오는 트래픽에 대한 다음 홉으로 새 엔드포인트를 지정합니다.
E. 각각 동일한 가용 영역에 있는 두 개의 방화벽 어플라이언스를 공유 서비스 VPC에 배포합니다.
F. VPC 게이트웨이 로드 밸런서 엔드포인트를 생성합니다. 공유 서비스 VPC의 라우팅 테이블에 경로를 추가합니다. 다른 VPC에서 공유 서비스 VPC로 들어오는 트래픽에 대한 다음 홉으로 새 엔드포인트를 지정합니다.

해설
정답: A,C,F

A: 높은 가용성(High Availability)을 위해 두 개의 방화벽을 두 개의 가용 영역에 분산 배치하고 NLB로 균형을 맞춘 후,
C: 게이트웨이 로드 밸런서를 사용하여 NLB를 통해 가상 서드파티 네트워크 방화벽과 연결하고,
F: 공유 GLB + 방화벽으로 트래픽을 가져오는 경로가 있는 고객 VPC의 Gateway Load Balancer Endpoint 가 필요.
Gateway Load Balancer 시작하기

◆ | **Q#0314.** | **Ref#0314.**
솔루션 아키텍트는 온프레미스 레거시 애플리케이션을 AWS로 마이그레이션해야 합니다. 애플리케이션은 로드 밸런서 뒤의 두 서버에서 실행됩니다. 응용 프로그램에는 서버 네트워크 어댑터의 MAC 주소와 연결된 라이센스 파일이 필요합니다. 소프트웨어 공급업체에서 새 라이센스 파일을 보내는 데 12시간이 걸립니다. 또한 애플리케이션은 고정 IP 주소가 포함된 구성 파일을 사용하여 데이터베이스 서버에 액세스하며 호스트 이름은 지원되지 않습니다.

이러한 요구 사항을 고려할 때 AWS의 애플리케이션 서버에 대한 고가용성 아키텍처를 구현하려면 어떤 단계 조합을 수행해야 합니까? (2개를 선택하세요.)

> **A.** ENI 풀을 생성합니다. 풀 공급업체에 라이선스 파일을 요청하고 라이선스 파일을 Amazon S3에 저장합니다. 부트스트랩 자동화 스크립트를 생성하여 라이선스 파일을 다운로드하고 해당 ENI를 Amazon EC2 인스턴스에 연결합니다.
> **B.** ENI 풀을 생성합니다. 풀 공급업체에 라이선스 파일을 요청하고 Amazon EC2 인스턴스에 라이선스 파일을 저장합니다. 인스턴스에서 AMI를 생성하고 향후 모든 EC2 인스턴스에 이 AMI를 사용합니다.
> **C.** 공급업체로부터 새 라이선스 파일을 요청하는 부트스트랩 자동화 스크립트를 생성합니다. 응답을 받으면 라이선스 파일을 Amazon EC2 인스턴스에 적용합니다.
> **D.** 부트스트랩 자동화 스크립트를 편집하여 AWS 시스템 관리자 매개 변수 저장소에서 데이터베이스 서버 IP 주소를 읽고 해당 값을 로컬 구성 파일에 삽입합니다.
> **E.** 구성 파일에 데이터베이스 서버 IP 주소를 포함하도록 Amazon EC2 인스턴스를 편집하고 향후 모든 EC2 자세에 사용할 AMI를 다시 생성합니다.
>
> 해설
> 정답: A,D
>
> A: ENI(Elastic Network Interface) 풀을 생성하고 풀에 대한 라이선스 파일을 요청한 후, 이 파일들을 Amazon S3에 저장하는 것이다. 그런 다음 해당 ENI를 Amazon EC2 인스턴스에 연결하고 라이센스 파일을 다운로드하는 부트스트랩 자동화 스크립트를 생성합니다. 이 과정은 라이선스 요건을 충족시킵니다.
> D: 부트스트랩 자동화 스크립트를 편집하여, 데이터베이스 서버의 IP 주소를 AWS Systems Manager Parameter Store에서 읽고, 이 값을 로컬 구성 파일에 저장
> EC2 인스턴스에서 IP 주소를 분리하여 ENI(탄력적 네트워크 인터페이스)객체로 정의 가능. 추가 ENI를 생성하고 두 번째 ENI를 EC2 인스턴스에 연결할 수 있는 기능을 제공합니다.

◆ | **Q#0315.** | **Ref#0315.**
한 회사가 미국 AWS 리전에서 판매 보고 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon API Gateway 지역 API 및 AWS Lambda 함수를 사용하여 Amazon RDS for MySQL 데이터베이스의 데이터에서 온디맨드 보고서를 생성합니다. 애플리케이션의 프런트엔드는 Amazon S3에서 호스팅되며 Amazon CloudFront 배포를 통해 사용자가 액세스합니다. 회사는 도메인의 DNS 서비스로 Amazon Route 53을 사용하고 있습니다. Route 53은 트래픽을 API Gateway API로 라우팅하기 위한 간단한 라우팅 정책으로 구성됩니다.

향후 6개월 내에 회사는 유럽으로 사업을 확장할 계획입니다. 데이터베이스 트래픽의 90% 이상이 읽기 전용 트래픽입니다. 회사는 이미 새 지역에 API Gateway API 및 Lambda 기능을 배포했습니다.

솔루션 설계자는 보고서를 다운로드하는 사용자의 대기 시간을 최소화하는 솔루션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 전체 로드가 포함된 AWS Database Migration Service(AWS DMS) 작업을 사용하여 원래 리전의 기본 데이터베이스를 새 리전의 데이터베이스로 복제합니다. API Gateway API에 연결하려면 Route 53 레코드를 지연 시간 기반 라우팅으로 변경하세요.
> **B.** 전체 로드와 변경 데이터 캡처(CDC)가 포함된 AWS Database Migration Service(AWS DMS) 작업을 사용하여 원래 리전의 기본 데이터베이스를 새 리전의 데이터베이스로 복제합니다. API Gateway

API에 연결하려면 Route 53 레코드를 지리적 위치 라우팅으로 변경하세요.
C. 새 리전에서 RDS 데이터베이스에 대한 리전 간 읽기 전용 복제본을 구성합니다. Route 53 레코드를 지연 시간 기반 라우팅으로 변경하여 API Gateway API에 연결합니다.
D. 새 리전의 RDS 데이터베이스에 대한 리전 간 읽기 전용 복제본을 구성합니다. API Gateway API에 연결하려면 Route 53 레코드를 지리적 위치 라우팅으로 변경하세요.

해설
정답: C

데이터베이스 트래픽의 90%가 읽기 전용으로 사용자가 보고서를 다운로드할때 지연 시간을 최소화 할 수 있는 방법은 latency-based routing이 유일한 방법이다.
교차 리전 읽기 복제본: 새로운 리전에 데이터베이스의 읽기 복제본을 구성하여 읽기 전용 트래픽을 현지화. 이는 유럽 사용자가 보고서를 생성할 때 지연 시간을 줄임.
지연 시간 기반 라우팅: Route 53의 지연 시간 기반 라우팅 정책을 사용하여 가장 낮은 지연 시간으로 API Gateway API에 연결되도록 함.
기술적 단순성: 이 접근 방식은 비교적 구현이 간단하며 운영 오버헤드가 낮습니다.

◆ | **Q#0316.** | **Ref#0316.**
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 CioudFormation 템플릿을 생성합니다. 이 템플릿을 포함하는 CloudFormation 스택 세트를 생성합니다. 테스트 OU의 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.

해설
정답: B

B: 단일 VPC를 사용하여 모든 테스트 환경을 관리하므로 운영 오버헤드가 가장 적다.
Transit Gateway 연결 및 관련 라우팅 구성을 포함하고 CloudFormation을 사용하여 모든 테스트 환경을 VPC에 배포하면 됨.
이는 새로운 테스트 환경이 생성되고 삭제될 때마다 별도의 네트워크 구성이 필요 없어 관리가 단순.
A(x): 각 테스트 환경마다 새 VPC를 배포하는 것은 운영 오버헤드가 크고 복잡성 증가.
C(x): 각 테스트 환경마다 새 계정을 생성하는 것은 관리 오버헤드가 매우 큼.
D(x): Docker 및 Kubernetes를 사용하여 복잡성을 증가시키며 운영 오버헤드가 증가.

◆ | **Q#0317.** | **Ref#0317.**
한 회사가 AWS에 새로운 API를 배포하고 있습니다. API는 호스팅을 위해 지역 API 엔드포인트 및 AWS Lambda 함수와 함께 Amazon API Gateway를 사용합니다. API는 외부 공급업체 API에서 데이터를 검색하고, Amazon DynamoDB 글로벌 테이블에 데이터를 저장하고, DynamoDB 글로벌 테이블에서 데이터를 검색합니다. 공급업체 API의 API 키는 AWS Secrets Manager에 저장되어 있으며 AWS Key Management Service (AWS KMS)의 고객 관리 키로 암호화되어 있습니다. 회사는 단일 AWS 리전에 자체 API를 배포했습니다.

솔루션 설계자는 회사 API의 API 구성 요소를 변경하여 구성 요소가 Active-Active 구성의 여러 지역에서 실행될 수 있도록 해야 합니다.

최소한의 운영 오버헤드로 이 요구 사항을 충족하는 변경 사항 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** API를 여러 지역에 배포합니다. 각 지역 API 엔드포인트로 트래픽을 라우팅하는 사용자 지정 도메인 이름으로 Amazon Route 53을 구성합니다. Route 53 다중 응답 라우팅 정책을 구현합니다.
> **B.** 새로운 KMS 다중 지역 고객 관리형 키를 생성합니다. 각 범위 내 리전에서 새 KMS 고객 관리형 복제본 키를 생성합니다.
> **C.** 기존 Secrets Manager 비밀을 다른 리전에 복제합니다. 각 범위 내 리전의 복제된 암호에 대해 적절한 KMS 키를 선택합니다.
> **D.** 각 범위 내 지역에서 새로운 AWS 관리형 KMS 키를 생성합니다. 기존 키를 multiRegion 키로 변환합니다. 다른 리전에서는 다중 리전 키를 사용하세요.
> **E.** 각 범위 내 지역에서 새로운 Secrets Manager 비밀을 생성합니다. 기존 리전의 비밀 값을 각 범위 내 리전의 새 비밀로 복사합니다.
> **F.** 범위 내 지역 전체에 걸쳐 배포를 반복하도록 Lambda 함수의 배포 프로세스를 수정합니다. 기존 API에 대해 다중 리전 옵션을 활성화합니다. 다중 지역 API의 백엔드로 각 지역에 배포되는 Lambda 함수를 선택합니다.
>
> 해설
> 정답: A,B,C
>
> A: 여러 리전에 API를 배포하고 Route 53을 사용하여 트래픽을 각 리전의 API 엔드포인트로 라우팅함으로써 Active-Active 구성이 가능.
> B: KMS 키를 다중 리전으로 설정하면 여러 리전에서 동일한 암호화 키를 사용할 수 있어 보안과 일관성을 유지 가능.
> C: Secrets Manager secret을 다른 리전으로 복제하고 각 리전에서 적절한 KMS 키를 선택하면, 다중 리전에서 동일한 보안 정보를 사용 가능.

◆ | **Q#0318.** | **Ref#0318.**
온라인 소매 회사는 단일 서버의 온프레미스 데이터 센터에서 상태 저장 웹 기반 애플리케이션과 MySQL 데이터베이스를 호스팅합니다. 회사는 더 많은 마케팅 캠페인과 프로모션을 실시하여 고객 기반을 확대하려고 합니다. 준비 과정에서 회사는 아키텍처의 안정성을 높이기 위해 애플리케이션과 데이터베이스를 AWS로 마이그레이션하려고 합니다.

가장 높은 수준의 안정성을 제공해야 하는 솔루션은 무엇입니까?

> **A.** 데이터베이스를 Amazon RDS MySQL 다중 AZ DB 인스턴스로 마이그레이션합니다. Application Load Balancer 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Amazon Neptune에 세션 저장
> **B.** 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다. Application Load Balancer 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Redis용 Amazon ElastiCache 복제 그룹에 세션을 저장합니다.
> **C.** 데이터베이스를 Amazon DocumentDB(MongoDB와 호환)로 마이그레이션합니다. Amazon Kinesis Data Firehose의 Network Load Balancer Store 세션 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다.

D. 데이터베이스를 Amazon RDS MariaDB 다중 AZ DB 인스턴스로 마이그레이션합니다. Application Load Balancer 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Memcached용 Amazon ElastiCache에 세션을 저장합니다.

해설
정답: B

Amazon Aurora MySQL: Aurora는 고가용성과 내구성을 제공하는 고성능 관계형 데이터베이스 서비스. 다중 AZ를 통해 높은 안정성을 보장.
Application Load Balancer와 Auto Scaling 그룹: EC2 인스턴스에 대한 자동 확장 및 부하 분산을 통해 애플리케이션의 가용성과 확장성을 극대화.
Amazon ElastiCache for Redis: Redis는 세션 저장에 적합한 인메모리 데이터 구조 저장소.

◆ | **Q#0319.** | **Ref#0319.**
회사의 솔루션 아키텍트는 VPC에서 호스팅되는 Amazon EC2 Windows 인스턴스의 사용자에게 안전한 원격 데스크톱 연결을 제공해야 합니다. 솔루션은 중앙 집중식 사용자 관리를 회사의 온프레미스 Active Directory와 통합해야 합니다. VPC에 대한 연결은 인터넷을 통해 이루어집니다. 회사에는 AWS Site-to-Site VPN 연결을 설정하는 데 사용할 수 있는 하드웨어가 있습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. Microsoft Active Directory용 AWS Directory Service를 사용하여 관리형 Active Directory를 배포합니다. 온프레미스 Active Directory와 신뢰를 설정합니다. EC2 인스턴스를 VPC의 배스천 호스트로 배포합니다. EC2 인스턴스가 도메인에 가입되어 있는지 확인하세요. 배스천 호스트를 사용하여 RDP를 통해 대상 인스턴스에 액세스합니다.
B. Microsoft Active Directory AD Connector용 AWS 디렉터리 서비스를 사용하여 온프레미스 Active Directory와 통합하도록 AWS IAM Identity Center(AWS Single Sign-On)를 구성합니다. AWS 시스템 관리자에 액세스하기 위해 사용자 그룹에 대한 권한 세트를 구성합니다. RDP를 통해 대상 인스턴스에 액세스하려면 Systems Manager Fleet Manager를 사용하십시오.
C. 온프레미스 환경과 대상 VPC 간에 VPN을 구현합니다. 대상 인스턴스가 VPN 연결을 통해 온프레미스 Active Directory 도메인에 연결되어 있는지 확인합니다. VPN을 통해 RDP 액세스를 구성합니다. 회사 네트워크에서 대상 인스턴스로 연결합니다.
D. Microsoft Active Directory용 AWS Directory Service를 사용하여 관리형 Active Directory를 배포합니다. 온프레미스 Active Directory와 신뢰를 설정합니다. AWS Quick Start를 사용하여 AWS에 원격 데스크톱 게이트웨이를 배포합니다. 원격 데스크톱 게이트웨이가 도메인에 가입되어 있는지 확인하세요. 원격 데스크톱 게이트웨이를 사용하여 RDP를 통해 대상 인스턴스에 액세스합니다.

해설
정답: C

VPN을 통해 on-premise 환경과 VPC를 연결한 뒤, 대상 EC2 인스턴스를 on-premise Active Directory 도메인에 가입시키고 RDP 액세스를 구성
가장 비용 효율적인 방법은 기존 하드웨어를 사용하여 온프레미스 환경과 AWS VPC 간에 VPN을 설정하는 것입니다.

◆ | **Q#0320.** | **Ref#0320.**
한 회사의 규정 준수 감사 결과 AWS 계정에서 생성된 일부 Amazon Elastic Block Store(Amazon EBS) 볼륨이 암호화되지 않은 것으로 나타났습니다. 솔루션 설계자는 저장 중인 모든 새로운 EBS 볼륨을 암호화하는 솔루션을 구현해야 합니다.

최소한의 노력으로 이 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. 암호화되지 않은 EBS 볼륨 생성을 감지하는 Amazon EventBridge 규칙을 생성합니다. AWS Lambda 함수를 호출하여 비준수 볼륨을 삭제합니다.

B. 데이터 암호화와 함께 AWS Audit Manager를 사용하십시오.
C. 새로운 EBS 볼륨 생성을 감지하는 AWS Config 규칙을 생성합니다. AWS 시스템 관리자 자동화를 사용하여 볼륨을 암호화합니다.
D. 모든 AWS 리전에서 기본적으로 EBS 암호화를 활성화합니다.

해설
정답: D

새로운 EBS 볼륨을 자동으로 암호화하여 모든 새 볼륨이 추가적인 구성 없이 자동으로 암호화되도록 하는 것
AWS Management Console에서 간단히 설정을 켜는 것만으로 모든 새로운 EBS 볼륨이 자동으로 암호화되도록 할 수 있습니다.

321 (황호실) 1회차 完

◆ | **Q#0321.** | **Ref#0321.**
한 연구 회사는 높은 수요를 충족하기 위해 AWS 클라우드에서 매일 시뮬레이션을 실행하고 있습니다. 시뮬레이션은 Amazon Linux 2를 기반으로 하는 수백 개의 Amazon EC2 인스턴스에서 실행됩니다. 때때로 시뮬레이션이 중단되고 클라우드 운영 엔지니어가 SSH를 통해 EC2 인스턴스에 연결하여 문제를 해결해야 합니다.

회사 정책에 따르면 EC2 인스턴스는 동일한 SSH 키를 사용할 수 없으며 모든 연결은 AWS CloudTrail에 기록되어야 합니다.

솔루션 설계자는 이러한 요구 사항을 어떻게 충족할 수 있습니까?

A. 새로운 EC2 인스턴스를 시작하고 각 인스턴스에 대해 개별 SSH 키를 생성하십시오. AWS Secrets Manager에 SSH 키를 저장합니다. 새 IAM 정책을 생성하고 GetSecretValue 작업에 대한 Allow 문을 사용하여 이를 엔지니어의 IAM 역할에 연결합니다. SSH 클라이언트를 통해 연결할 때 Secrets Manager에서 SSH 키를 가져오도록 엔지니어에게 지시합니다.
B. EC2 인스턴스에서 명령을 실행하여 새로운 고유 SSH 키를 설정하는 AWS 시스템 관리자 문서를 생성합니다. 새 IAM 정책을 생성하고 이를 엔지니어의 IAM 역할에 연결하여 시스템 관리자 문서를 실행하도록 허용합니다. 엔지니어에게 문서를 실행하여 SSH 키를 설정하고 SSH 클라이언트를 통해 연결하도록 지시하십시오.
C. 인스턴스에 대한 SSH 키를 설정하지 않고 새 EC2 인스턴스를 시작합니다. 각 인스턴스에 EC2 Instance Connect를 설정합니다. 새 IAM 정책을 생성하고 SendSSHPublicKey 작업에 대한 Allow 문을 사용하여 이를 엔지니어의 IAM 역할에 연결합니다. EC2 콘솔에서 브라우저 기반 SSH 클라이언트를 사용하여 인스턴스에 연결하도록 엔지니어에게 지시합니다.
D. EC2 SSH 키를 저장하도록 AWS Secrets Manager를 설정합니다. 새 AWS Lambda 함수를 생성하여 새 SSH 키를 생성하고 AWS Systems Manager Session Manager를 호출하여 EC2 인스턴스에 SSH 키를 설정합니다. 매일 한 번씩 자동 교체를 위해 Lambda 함수를 사용하도록 Secrets Manager를 구성합니다. SSH 클라이언트를 통해 연결할 때 Secrets Manager에서 SSH 키를 가져오도록 엔지니어에게 지시합니다.

해설
정답: C
SSH 키를 설정하지 않고 EC2 인스턴스를 시작하고 EC2 Instance Connect를 사용하여 엔지니어들이 브라우저 기반 SSH 클라이언트를 통해 EC2 콘솔에서 인스턴스에 연결할 수 있도록 함.
이 방법은 엔지니어가 개별 SSH 키를 사용할 필요가 없으며, 모든 연결이 AWS CloudTrail에 기록됨.
또한, IAM 정책을 통해 SendSSHPublicKey 작업을 허용함으로써 보안 관리도 간편해짐.

◆ | **Q#0322.** | **Ref#0322.**
회사가 모바일 뱅킹 애플리케이션을 Amazon EC2 인스턴스에서 실행하기 위해 VPC로 마이그레이션하고 있습니

다. 백엔드 서비스 애플리케이션은 온프레미스 데이터 센터에서 실행됩니다. 데이터 센터는 AWS로의 AWS Direct Connect 연결을 가지고 있습니다. VPC에서 실행되는 애플리케이션은 데이터 센터에서 실행되는 온프레미스 Active Directory 도메인에 대한 DNS 요청을 해결해야 합니다.

최소한의 관리 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** VPC 내 애플리케이션 서버의 DNS 쿼리를 해결하기 위해 캐싱 DNS 서버로 VPC의 두 가용 영역에 걸쳐 EC2 인스턴스 세트를 프로비저닝합니다.
> **B.** Amazon Route 53 프라이빗 호스팅 영역을 프로비저닝합니다. 온프레미스 DNS 서버를 가리키는 NS 레코드를 구성합니다.
> **C.** Amazon Route 53 Resolver를 사용하여 DNS 엔드포인트를 생성합니다. 온프레미스 데이터 센터와 VPC 간의 DNS 네임스페이스를 확인하기 위한 조건부 전달 규칙을 추가합니다.
> **D.** 이 새 도메인과 온프레미스 Active Directory 도메인 간의 양방향 신뢰를 통해 VPC에 새 Active Directory 도메인 컨트롤러를 프로비저닝합니다.
>
> 해설
> 정답: C
> Amazon Route 53 Resolver를 사용하여 DNS 엔드포인트를 생성하고 조건부 포워딩 규칙을 추가하여 온프레미스 데이터 센터와 VPC 간에 DNS 네임스페이스를 해결함.
> Amazon Route 53 Resolver를 사용하여 DNS 엔드포인트를 생성하고 조건부 전달 규칙을 설정하는 것이 가장 관리 오버헤드가 적은 해결책
> 이 솔루션은 최소한의 관리 오버헤드로 온프레미스 Active Directory 도메인에 대한 DNS 요청을 처리할 수 있음.
> Route 53 Resolver는 온프레미스 DNS 서버와의 통합을 쉽게 하고, 별도의 인프라를 관리할 필요 없이 DNS 쿼리를 원활하게 처리할 수 있음.

◆ | **Q#0323.** | **Ref#0323.**
회사는 환경 데이터를 처리합니다. 이 회사는 도시의 다양한 영역에서 연속적인 데이터 스트림을 제공하기 위해 센서를 설치했습니다. 데이터는 JSON 형식으로 제공됩니다.

회사는 AWS 솔루션을 사용하여 저장을 위해 고정된 스키마가 필요하지 않은 데이터베이스에 데이터를 전송하려고 합니다. 데이터는 실시간으로 전송되어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** Amazon Kinesis Data Firehose를 사용하여 Amazon Redshift로 데이터를 보냅니다.
> **B.** Amazon Kinesis Data Streams를 사용하여 Amazon DynamoDB로 데이터를 보냅니다.
> **C.** Amazon Managed Streaming for Apache Kafka(Amazon MSK)를 사용하여 데이터를 Amazon Aurora로 보냅니다.
> **D.** Amazon Kinesis Data Firehose를 사용하여 Amazon Keyspaces(Apache Cassandra용)로 데이터를 보냅니다.
>
> 해설
> 정답:B
> Amazon Kinesis Data Streams를 사용하여 데이터를 실시간으로 수집하고, 이를 스키마가 필요 없는 NoSQL DB인 Amazon DynamoDB로 전송하는 방법이 최적.
> DynamoDB는 JSON 형식의 데이터를 저장하는 데 적합하며, 스키마리스 저장소로 실시간 데이터를 처리할 수 있음.
> 다른 옵션들은 다음과 같은 이유로 적절하지 않음:
> A: Amazon Redshift는 관계형 데이터베이스로, 스키마가 필요함.
> C: Amazon Aurora는 관계형 데이터베이스로, 스키마가 필요함.
> D: Amazon Keyspaces (for Apache Cassandra)는 적절한 솔루션이지만 Kinesis Data Firehose는 키스페이스로 데이터를 보낼 수 없음.

◆ | **Q#0324.** | **Ref#0324.**
회사는 온프레미스 데이터 센터의 레거시 애플리케이션을 AWS로 마이그레이션하고 있습니다. 애플리케이션은 MongoDB를 키-값 데이터베이스로 사용합니다. 회사의 기술 지침에 따라 모든 Amazon EC2 인스턴스는 인터넷 연결 없이 프라이빗 서브넷에서 호스팅되어야 합니다. 또한 애플리케이션과 데이터베이스 간의 모든 연결은 암호화되어야 합니다. 데이터베이스는 수요에 따라 확장할 수 있어야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 프로비저닝된 IOPS 볼륨이 있는 애플리케이션을 위한 새로운 Amazon DocumentDB(MongoDB 호환) 테이블을 생성합니다. 인스턴스 엔드포인트를 사용하여 Amazon DocumentDB에 연결합니다.
> **B.** 온디맨드 용량을 갖춘 애플리케이션을 위한 새로운 Amazon DynamoDB 테이블을 생성합니다. DynamoDB용 게이트웨이 VPC 엔드포인트를 사용하여 DynamoDB 테이블에 연결합니다.
> **C.** 온디맨드 용량을 갖춘 애플리케이션을 위한 새로운 Amazon DynamoDB 테이블을 생성합니다. DynamoDB용 인터페이스 VPC 엔드포인트를 사용하여 DynamoDB 테이블에 연결합니다.
> **D.** 프로비저닝된 IOPS 볼륨이 있는 애플리케이션을 위한 새로운 Amazon DocumentDB(MongoDB 호환) 테이블을 생성합니다. 클러스터 엔드포인트를 사용하여 Amazon DocumentDB에 연결합니다.
>
> 해설
> 정답: B
> 새로운 Amazon DynamoDB 테이블을 생성하고 DynamoDB용 게이트웨이 VPC 엔드포인트를 사용하여 테이블에 연결하는 방법이 가장 적합함.
> Amazon DynamoDB는 완전 관리형 NoSQL 데이터베이스 서비스로, 온디맨드 용량을 갖춘 애플리케이션에 적합
> 프로비저닝된 IOPS 볼륨이 있는 데이터베이스는 수요에 따라 확장가능하지 않음.(A,D out)
> DynamoDB는 다음과 같은 특징을 제공:
> - 프라이빗 서브넷에서 호스팅: DynamoDB 테이블은 프라이빗 서브넷에서 실행될 수 있으며 인터넷 연결 없이 사용할 수 있음
> - 암호화: DynamoDB는 데이터베이스 간의 모든 연결을 SSL/TLS를 통해 암호화함.
> - 확장성: DynamoDB는 수요에 따라 자동으로 확장 가능하며, 리플리카 세트를 관리함.
> 따라서 온디맨드 용량을 갖춘 애플리케이션에는 DynamoDB를 사용하여 데이터베이스를 구축하고, VPC 엔드포인트를 통해 애플리케이션과 연결할 수 있음.

◆ | **Q#0325.** | **Ref#0325.**
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.

해설
정답: B
AWS Database Migration Service (DMS)를 사용한 마이그레이션
AWS DMS를 사용하면 MongoDB 데이터베이스를 Amazon DocumentDB로 쉽게 마이그레이션 가능
MongoDB에서 사용하는 애플리케이션 코드와 동일한 드라이버 및 도구를 사용하여 데이터를 Amazon DocumentDB로 이동
일회성 마이그레이션 또는 변경 사항 복제를 통해 원본과 대상을 동기화된 상태로 유지

◆ | **Q#0326.** | **Ref#0326.**
한 회사가 AWS에서 실행되도록 애플리케이션을 재설계하고 있습니다. 회사의 인프라에는 여러 Amazon EC2 인스턴스가 포함되어 있습니다. 회사의 개발팀에는 다양한 수준의 액세스가 필요합니다. 회사는 모든 Windows EC2 인스턴스를 AWS의 Active Directory 도메인에 조인하도록 요구하는 정책을 구현하려고 합니다. 또한 회사는 다중 요소 인증(MFA)과 같은 향상된 보안 프로세스를 구현하려고 합니다. 회사는 가능한 한 관리형 AWS 서비스를 사용하기를 원합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Microsoft Active Directory 구현을 위한 AWS 디렉터리 서비스를 생성합니다. Amazon Workspace를 시작하십시오. 도메인 보안 구성 작업을 위해 Workspace에 연결하고 사용합니다.
B. Microsoft Active Directory 구현을 위한 AWS 디렉터리 서비스를 생성합니다. EC2 인스턴스를 시작합니다. 도메인 보안 구성 작업을 위해 EC2 인스턴스에 연결하고 사용합니다.
C. AWS Directory Service Simple AD 구현을 생성합니다. EC2 인스턴스를 시작합니다. 도메인 보안 구성 작업을 위해 EC2 인스턴스에 연결하고 사용합니다.
D. AWS Directory Service Simple AD 구현을 생성합니다. Amazon Workspace를 시작하십시오. 도메인 보안 구성 작업을 위해 Workspace에 연결하고 사용합니다.

해설
정답: A
회사는 관리 오버헤드를 줄이기 위해 가능한 한 관리형 AWS 서비스를 원함. EC2 인스턴스는 AWS 관리형 서비스가 아니므로 추가적인 관리 작업이 필요함.
AWS Directory Service for Microsoft Active Directory 또는 Simple AD를 사용하여 AWS Directory Service에서 도메인을 호스팅
Amazon Workspaces: 이는 AWS 관리 서비스이며, 기본적으로 도메인에 가입할 수 있으며, MFA(Multi-Factor Authentication)를 포함한 보안 설정도 가능.

◆ | **Q#0327.** | **Ref#0327.**
회사에서 온프레미스 애플리케이션을 AWS로 마이그레이션하려고 합니다. 애플리케이션용 데이터베이스는 구조화된 제품 데이터와 임시 사용자 세션 데이터를 저장합니다. 회사는 사용자 세션 데이터에서 제품 데이터를 분리해야 합니다. 또한 회사는 재해 복구를 위해 다른 AWS 리전에 복제를 구현해야 합니다.

최고의 성능으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 제품 데이터와 사용자 세션 데이터를 호스팅하기 위해 별도의 스키마를 사용하여 Amazon RDS DB 인스턴스를 생성합니다. 다른 리전의 DB 인스턴스에 대한 읽기 전용 복제본을 구성합니다.
B. 제품 데이터를 호스팅할 Amazon RDS DB 인스턴스를 생성합니다. 다른 리전의 DB 인스턴스에 대한 읽기 전용 복제본을 구성합니다. 사용자 세션 데이터를 호스팅하기 위해 Amazon ElastiCache for Memcached에 글로벌 데이터 스토어를 생성합니다.
C. 두 개의 Amazon DynamoDB 글로벌 테이블을 생성합니다. 하나의 글로벌 테이블을 사용하여 제품 데이터를 호스팅합니다. 다른 전역 테이블을 사용하여 사용자 세션 데이터를 호스팅합니다. 캐싱

에는 DynamoDB Accelerator(DAX)를 사용합니다.
D. 제품 데이터를 호스팅할 Amazon RDS DB 인스턴스를 생성합니다. 다른 리전의 DB 인스턴스에 대한 읽기 전용 복제본을 구성합니다. 사용자 세션 데이터를 호스팅할 Amazon DynamoDB 전역 테이블을 생성합니다.

해설
정답: **D**
요구사항을 가장 잘 충족하고 최고 성능을 제공하는 솔루션은 제품 데이터를 Amazon RDS에 호스팅하고 사용자 세션 데이터를 Amazon DynamoDB 글로벌 테이블에 호스팅하는 것임.
제품 데이터와 사용자 세션 데이터를 분리하여 최적의 성능과 가용성을 제공함.
Amazon RDS는 제품 데이터에 대해 안정적이고 확장 가능한 관계형 데이터베이스 솔루션을 제공하며,
DynamoDB는 비구조화된 데이터에 대해 빠르고 확장 가능한 NoSQL 데이터베이스 솔루션을 제공함.
또한 다른 리전에 읽기 전용 복제본을 구성하여 재해 복구를 위한 고가용성을 보장

◆ | **Q#0328.** | **Ref#0328.**
회사는 AWS Control Tower를 사용하여 AWS에서 다중 계정 구조를 조정합니다. 회사는 AWS Organizations, AWS Config 및 AWS Trusted Advisor를 사용하고 있습니다. 회사에는 개발자가 AWS에서 실험하는 데 사용하는 개발 계정에 대한 특정 OU가 있습니다. 회사에는 수백 명의 개발자가 있으며 각 개발자는 개별 개발 계정을 가지고 있습니다.

회사는 이러한 개발 계정의 비용을 최적화하려고 합니다. 이러한 계정의 Amazon EC2 인스턴스와 Amazon RDS 인스턴스는 버스트 가능해야 합니다. 회사는 관련성이 없는 기타 서비스의 이용을 거부하고자 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 권장해야 합니까?

A. AWS Organizations에서 사용자 지정 SCP를 생성하여 버스트 가능한 인스턴스의 배포만 허용하고 관련 없는 서비스는 허용하지 않습니다. 개발 OU에 SCP를 적용합니다.
B. AWS Control Tower에서 사용자 지정 탐지 제어(가드레일)를 생성합니다. 버스트 가능한 인스턴스의 배포만 허용하고 관련 없는 서비스는 허용하지 않도록 제어(가드레일)를 구성합니다. 개발 OU에 제어(가드레일)를 적용합니다.
C. AWS Control Tower에서 사용자 지정 예방 제어(가드레일)를 생성합니다. 버스트 가능한 인스턴스의 배포만 허용하고 관련 없는 서비스는 허용하지 않도록 제어(가드레일)를 구성합니다. 개발 OU에 제어(가드레일)를 적용합니다.
D. AWS Control Tower 계정에서 AWS Config 규칙을 생성합니다. 버스트 가능한 인스턴스의 배포만 허용하고 관련 없는 서비스는 허용하지 않도록 AWS Config 규칙을 구성합니다. AWS CloudFormation StackSets를 사용하여 개발 OU에 AWS Config 규칙을 배포합니다.

해설
정답: **A**
AWS Organizations에서 사용자 지정 SCP(Service Control Policies)를 생성하여 버스터블 인스턴스의 배포만 허용하고 관련 없는 서비스를 금지함. 이 SCP를 개발용 OU에 적용.
이 문제에서는 AWS Control Tower를 사용하여 개발 계정을 관리하고 있으며, 이를 통해 사용자 지정 SCP를 적용하는 것이 가장 적절함.
SCP를 사용하여 특정 서비스와 인스턴스 유형의 제한을 중앙에서 강제할 수 있으며, SCP는 AWS Organizations에서 중앙 집중식으로 관리됩니다.
사용자 지정 SCP를 개발 OU에 적용하면 해당 OU 내의 모든 계정에 제한이 적용되어 개발자가 허용된 리소스 및 서비스만 사용하도록 효과적으로 제한됨.
AWS Control Tower 가드레일(B,C)은 세분화된 서비스 수준 제한보다는 주로 거버넌스 및 규정 준수 목적으로 사용됨.

◆ | **Q#0329.** | **Ref#0329.**
금융 서비스 회사는 Amazon EC2 인스턴스 및 AWS Lambda 함수에서 복잡한 다중 계층 애플리케이션을 실행합니다. 애플리케이션은 Amazon S3에 임시 데이터를 저장합니다. S3 객체는 45분 동안만 유효하며 24시간 후에 삭제됩니다.

회사는 AWS CloudFormation 스택을 시작하여 애플리케이션의 각 버전을 배포합니다. 스택은 애플리케이션을 실행하는 데 필요한 모든 리소스를 생성합니다. 회사가 새 애플리케이션 버전을 배포하고 검증할 때 회사는 이전 버전의 CloudFormation 스택을 삭제합니다.

회사는 최근 이전 애플리케이션 버전의 CloudFormation 스택을 삭제하려고 시도했지만 작업이 실패했습니다. 분석에 따르면 CloudFormation이 기존 S3 버킷을 삭제하지 못한 것으로 나타났습니다. 솔루션 설계자는 애플리케이션 아키텍처를 크게 변경하지 않고 이 문제를 해결해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 특정 S3 버킷에서 모든 파일을 삭제하는 Lambda 함수를 구현합니다. 이 Lambda 함수를 CloudFormation 스택에 사용자 지정 리소스로 통합합니다. 사용자 지정 리소스에 S3 버킷의 리소스를 가리키는 DependsOn 속성이 있는지 확인하세요.
> **B.** Amazon Elastic File System(Amazon EFS) 파일 시스템을 프로비저닝하여 Amazon S3 대신 임시 파일을 저장하도록 CloudFormation 템플릿을 수정합니다. 파일 시스템과 동일한 VPC에서 실행되도록 Lambda 함수를 구성합니다. 파일 시스템을 EC2 인스턴스 및 Lambda 함수에 탑재합니다.
> **C.** CloudF 구성 스택을 수정하여 생성 후 45분 후에 모든 객체가 만료되는 S3 수명 주기 규칙을 생성합니다. S3 버킷의 리소스를 가리키는 DependsOn 속성을 추가합니다.
> **D.** CloudFormation 스택을 수정하여 값이 삭제된 DeletionPolicy 속성을 S3 버킷에 연결합니다.
>
> 해설
> 정답: **A**
> 비어 있지 않은 S3 버킷은 삭제불가 하므로 S3 버킷을 삭제할 때는 먼저 버킷을 비워야 함.
> 이를 위해 CloudFormation 스택에 Lambda 함수를 구현하여 버킷을 삭제하기 전에 해당 버킷을 비우는 작업을 수행해야 함.
> Lambda 함수를 사용하여 CloudFormation 스택의 사용자 지정 리소스로 통합하고,
> 이 사용자 지정 리소스가 S3 버킷 리소스를 가리키는 DependsOn 속성을 갖도록 구성.

◆ | **Q#0330.** | **Ref#0330.**
한 회사에서 모바일 게임을 개발했습니다. 게임의 백엔드는 온프레미스 데이터 센터에 있는 여러 가상 머신에서 실행됩니다. 비즈니스 로직은 여러 기능이 포함된 REST API를 사용하여 노출됩니다. 플레이어 세션 데이터는 중앙 파일 저장소에 저장됩니다. 백엔드 서비스는 조절을 위해 그리고 라이브 트래픽과 테스트 트래픽을 구별하기 위해 다양한 API 키를 사용합니다.

게임 백엔드의 부하는 하루 종일 달라집니다. 피크 시간대에는 서버 용량이 충분하지 않습니다. 플레이어 세션 데이터를 가져올 때 지연 시간 문제도 있습니다. 경영진은 솔루션 설계자에게 게임의 다양한 로드를 처리하고 대기 시간이 짧은 데이터 액세스를 제공할 수 있는 클라우드 아키텍처를 제시하도록 요청했습니다. API 모델은 변경되어서는 안 됩니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** NLB(Network Load Balancer)를 사용하여 REST API를 구현합니다. NLB 뒤의 Amazon EC2 인스턴스에서 비즈니스 로직을 실행합니다. Amazon Aurora Serverless에 플레이어 세션 데이터를 저장합니다.
> **B.** ALB(Application Load Balancer)를 사용하여 REST API를 구현합니다. AWS Lambda에서 비즈니스 로직을 실행합니다. 온디맨드 용량으로 Amazon DynamoDB에 플레이어 세션 데이터를 저장합니다.
> **C.** Amazon API Gateway를 사용하여 REST API를 구현합니다. AWS Lambda에서 비즈니스 로직을 실행합니다. 온디맨드 용량으로 Amazon DynamoDB에 플레이어 세션 데이터를 저장합니다.

D. AWS AppSync를 사용하여 REST API를 구현합니다. AWS Lambda에서 비즈니스 로직을 실행합니다. Amazon Aurora Serverless에 플레이어 세션 데이터를 저장합니다.

해설
정답: C
REST API를 구현하는 가장 적합한 방법은 Amazon API Gateway를 사용하는 것임.
비즈니스 로직을 실행하는 데 AWS Lambda를 사용하고, 플레이어 세션 데이터를 Amazon DynamoDB에 저장.
이러한 조합은 변동하는 부하를 처리하고 저지연으로 데이터에 액세스할 수 있는 효율적인 클라우드 아키텍처를 제공함.

331 (김성원) 1회차 完

◆ | **Q#0331.** | **Ref#0331.**
한 회사가 애플리케이션을 AWS 클라우드로 마이그레이션하고 있습니다. 애플리케이션은 온프레미스 데이터 센터에서 실행되며 매일 밤 마운트된 NFS 파일 시스템에 수천 개의 이미지를 씁니다. 회사는 애플리케이션을 마이그레이션한 후 Amazon Elastic File System(Amazon EFS) 파일 시스템이 탑재된 Amazon EC2 인스턴스에서 애플리케이션을 호스팅합니다.

회사는 AWS에 대한 AWS Direct Connect 연결을 설정했습니다. 마이그레이션 중단 전에 솔루션 설계자는 새로 생성된 온프레미스 이미지를 EFS 파일 시스템에 복제하는 프로세스를 구축해야 합니다.

이미지를 복제하는 가장 운영상 효율적인 방법은 무엇입니까?

A. 온프레미스 파일 시스템에서 Amazon S3로 aws s3 sync 명령을 실행하도록 정기적인 프로세스를 구성합니다. Amazon S3의 이벤트 알림을 처리하고 Amazon S3의 이미지를 EFS 파일 시스템으로 복사하도록 AWS Lambda 함수를 구성합니다.
B. NFS 마운트 지점을 사용하여 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 온프레미스 서버에 파일 게이트웨이 파일 시스템을 탑재합니다. 이미지를 마운트 지점에 주기적으로 복사하는 프로세스를 구성합니다.
C. NFS 파일 시스템에 액세스할 수 있는 온프레미스 서버에 AWS DataSync 에이전트를 배포합니다. 퍼블릭 VIF를 사용하여 Direct Connect 연결을 통해 S3 버킷으로 데이터를 보냅니다. Amazon S3의 이벤트 알림을 처리하고 Amazon S3의 이미지를 EFS 파일 시스템으로 복사하도록 AWS Lambda 함수를 구성합니다.
D. NFS 파일 시스템에 액세스할 수 있는 온프레미스 서버에 AWS DataSync 에이전트를 배포합니다. 프라이빗 VIF를 사용하여 Direct Connect 연결을 통해 Amazon EFS용 AWS PrivateLink 인터페이스 VPC 엔드포인트로 데이터를 보냅니다. 24시간마다 EFS 파일 시스템에 이미지를 보내도록 DataSync 예약 작업을 구성합니다.

해설
정답: D

운영적으로 가장 효율적이며, 최소한의 관리 오버헤드로 요구 사항을 충족합니다.
AWS DataSync는 데이터를 효율적으로 전송하는 데 사용할 수 있으며, 프라이빗 VIF를 통해 Direct Connect 연결을 사용하면 보안 및 성능을 최적화할 수 있습니다.
프라이빗 VIF와 함께 AWS PrivateLink를 활용하면 온프레미스 환경과 Amazon EFS 파일 시스템 간의 비공개적이고 안전한 연결이 보장됩니다. 이렇게 하면 공용 인터넷 액세스가 필요하지 않습니다.

◆ | **Q#0332.** | **Ref#0332.**
한 회사는 최근 온프레미스 데이터 센터에서 AWS 클라우드로 웹 애플리케이션을 마이그레이션했습니다. 웹 애플리케이션 인프라는 요청을 처리하기 위해 Amazon Elastic Container Service(Amazon ECS)를 사용하여 ALB(Application Load Balancer)로 라우팅하는 Amazon CloudFront 배포로 구성됩니다. 최근 보안 감사에서는

CloudFront와 ALB 엔드포인트를 모두 사용하여 웹 애플리케이션에 액세스할 수 있는 것으로 나타났습니다. 그러나 회사에서는 CloudFront 엔드포인트를 통해서만 웹 애플리케이션에 액세스할 수 있도록 요구합니다.

최소한의 노력으로 이 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

> **A.** 새 보안 그룹을 생성하여 CloudFront 배포에 연결합니다. CloudFront 보안 그룹에서만 액세스를 허용하도록 ALB 보안 그룹 수신을 업데이트합니다.
> **B.** com.amazonaws.global.cloudfront.origin-facing CloudFront 관리형 접두사 목록에서만 액세스를 허용하도록 ALB 보안 그룹 수신을 업데이트합니다.
> **C.** Elastic Load Balancing을 위한 com.amazonaws.region.elasticloadbalancing VPC 인터페이스 엔드포인트를 생성합니다. ALB 체계를 인터넷 연결에서 내부로 업데이트합니다.
> **D.** AWS가 제공한 ip-ranges.json 문서에서 CloudFront IP를 추출합니다. CloudFront IP에서만 액세스를 허용하도록 ALB 보안 그룹 수신을 업데이트합니다.
>
> 해설
> 정답: B
>
> CloudFront 접두사 목록에서만 ALB SG에 대한 수신 액세스를 허용합니다
> ALB 보안 그룹의 수신 규칙을 업데이트하여 CloudFront 관리 프리픽스 목록만 허용하는 방법으로, 가장 간단하고 효과적인 솔루션입니다.
> 이를 통해 ALB에 대한 접근을 CloudFront에서 오는 트래픽으로 제한할 수 있습니다. 다른 옵션들보다 설정이 간편하며, CloudFront와 ALB 간의 통신을 보장합니다.

◆ | **Q#0333.** | **Ref#0333.**
회사는 ALB(Application Load Balancer)와 Amazon ECS 클러스터에서 호스팅되는 Docker 애플리케이션을 사용하여 커뮤니티 포럼 사이트를 호스팅합니다. 사이트 데이터는 MySQL용 Amazon RDS에 저장되고 컨테이너 이미지는 ECR에 저장됩니다. 회사는 RTO가 24시간 이하, RPO가 8시간 이하인 재해 복구 SLA를 고객에게 제공해야 합니다.

다음 솔루션 중 요구 사항을 충족하는 가장 비용 효율적인 방법은 무엇입니까?

> **A.** AWS CloudFormation을 사용하여 두 지역에 동일한 ALB, EC2, ECS 및 RDS 리소스를 배포하십시오. 8시간마다 RDS 스냅샷을 예약합니다. RDS 다중 지역 복제를 사용하여 보조 지역의 데이터베이스 복사본을 업데이트합니다. 오류가 발생하면 최신 스냅샷에서 복원하고 Amazon Route 53 DNS 장애 조치 정책을 사용하여 자동으로 고객을 보조 지역의 ALB로 리디렉션합니다.
> **B.** 두 지역의 ECR에 Docker 이미지를 저장합니다. 스냅샷을 보조 지역에 복사하여 8시간마다 RDS 스냅샷을 예약합니다. 오류가 발생하는 경우 AWS CloudFormation을 사용하여 보조 지역에 ALB, EC2, ECS 및 RDS 리소스를 배포하고, 최신 스냅샷에서 복원하고, 보조 지역의 ALB를 가리키도록 DNS 레코드를 업데이트합니다.
> **C.** AWS CloudFormation을 사용하여 보조 지역에 동일한 ALB, EC2, ECS 및 RDS 리소스를 배포합니다. Amazon S3에 대한 시간별 RDS MySQL 백업을 예약하고 지역 간 복제를 사용하여 보조 지역의 버킷에 데이터를 복제합니다. 오류가 발생하면 최신 Docker 이미지를 보조 지역의 Amazon ECR로 가져오고, EC2 인스턴스에 배포하고, 최신 MySQL 백업을 복원하고, 보조 지역의 ALB를 가리키도록 DNS 레코드를 업데이트하세요.
> **D.** 인스턴스 크기와 노드 수를 늘리기 위한 조정 정책을 사용하여 AWS Auto Scaling 그룹의 Docker용 ALB 및 최소 리소스 EC2 배포를 사용하여 보조 지역에 파일럿 라이트 환경을 배포합니다. RDS 데이터의 리전 간 읽기 복제본을 생성합니다. 오류가 발생하는 경우 복제본을 기본으로 승격하고 보조 지역의 ALB를 가리키도록 DNS 레코드를 업데이트합니다.
>
> 해설
> 정답: B
>
> 두 지역의 ECR 및 RDS 스냅샷: Docker 이미지를 두 지역의 ECR에 저장하고 RDS 스냅샷을 보조 지역

에 복사하는 것은 좋은 전략입니다.
오류가 발생하면 CloudFormation은 필요한 리소스를 보조 지역에 배포하고 DNS가 업데이트됩니다.
이 옵션은 전체 복제 환경이나 다중 지역 복제를 지속적으로 유지할 필요가 없으므로 A보다 비용 효율적입니다.

◆ | **Q#0334.** | **Ref#0334.**
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 OU를 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.

해설
정답: B

AWS Control Tower를 사용하여 조직을 관리하고 보호하는데 필요한 일관된 관리 및 보안 기준을 자동으로 설정해 주기 때문에 최소한의 운영 오버헤드로 요구 사항을 충족
Control Tower는 다양한 사전 구성된 가드레일을 제공하여 계정 관리 및 보안을 쉽게 설정할 수 있으며,
AWS IAM Identity Center (Single Sign-On)을 통해 온프레미스 AD FS 서버와의 통합도 쉽게 구현할 수 있음.
필요한 경우 추가적인 OU 및 AWS Config 구성을 통해 유연성을 제공할 수 있음.

◆ | **Q#0335.** | **Ref#0335.**
온라인 잡지가 이번 달 최신판을 출시할 예정입니다. 이 버전은 전 세계적으로 최초로 배포될 예정입니다. 이 잡지의 동적 웹 사이트는 현재 웹 계층 앞에 Application Load Balancer, 웹 및 애플리케이션 서버용 Amazon EC2 인스턴스 집합, Amazon Aurora MySQL을 사용하고 있습니다. 웹사이트의 일부에는 정적 콘텐츠가 포함되어 있으며 거의 모든 트래픽은 읽기 전용입니다.

이 잡지는 새 판이 출시되면 인터넷 트래픽이 크게 급증할 것으로 예상하고 있습니다. 출시 다음 주에는 최적의 성능이 최우선 과제입니다.

전 세계 사용자의 시스템 응답 시간을 줄이기 위해 솔루션 아키텍트가 수행해야 하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

> **A.** 논리적 교차 리전 복제를 사용하여 Aurora MySQL 데이터베이스를 보조 리전에 복제하십시오. 웹 서버를 Amazon S3로 교체합니다. 리전 간 복제 모드로 S3 버킷을 배포합니다.
> **B.** 웹 및 애플리케이션 계층이 각각 Auto Scaling 그룹에 있는지 확인합니다. AWS Direct Connect 연결을 도입합니다. 전 세계 지역에 웹 및 애플리케이션 계층을 배포합니다.
> **C.** Amazon Aurora에서 MySQL용 Amazon RDS로 데이터베이스를 마이그레이션합니다. 세 가지 애플리케이션 계층(웹, 애플리케이션, 데이터베이스)이 모두 프라이빗 서브넷에 있는지 확인하세요.
> **D.** 물리적 교차 리전 복제를 위해 Aurora 글로벌 데이터베이스를 사용하십시오. 정적 콘텐츠 및 리소스에 대해 리전 간 복제와 함께 Amazon S3를 사용하십시오. 전 세계 지역에 웹 및 애플리케이션 계층을 배포합니다.
> **E.** 지연 시간 기반 라우팅 및 Amazon CloudFront 배포 기능을 갖춘 Amazon Route 53을 소개합니다. 웹 및 애플리케이션 계층이 각각 Auto Scaling 그룹에 있는지 확인합니다.
>
> 해설
> 정답: D,E
>
> Aurora 글로벌 데이터베이스를 사용하여 물리적 교차 리전 복제를 설정하여 데이터베이스 성능을 최적화
> Amazon S3를 교차 리전 복제와 함께 사용하여 정적 콘텐츠의 전송 속도를 높임.
> Amazon Route 53과 지연 시간 기반 라우팅을 사용하여 사용자가 가장 가까운 서버로 라우팅되도록 함.
> Amazon CloudFront를 사용하여 콘텐츠 전송 네트워크(CDN)를 통해 빠르게 정적 콘텐츠를 제공

◆ | **Q#0336.** | **Ref#0336.**
온라인 게임 회사는 AWS에서 워크로드 비용을 최적화해야 합니다. 회사는 전용 계정을 사용하여 온라인 게임 애플리케이션과 분석 애플리케이션을 위한 프로덕션 환경을 호스팅합니다.

Amazon EC2 인스턴스는 게임 애플리케이션을 호스팅하며 항상 사용 가능해야 합니다. EC2 인스턴스는 일년 내내 실행됩니다. 분석 애플리케이션은 Amazon S3에 저장된 데이터를 사용합니다. 분석 애플리케이션은 문제 없이 중단되었다가 재개될 수 있습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

> **A.** 온라인 게임 애플리케이션 인스턴스에 대한 EC2 Instance Savings Plan을 구매하십시오. 분석 애플리케이션에 온디맨드 인스턴스를 사용합니다.
> **B.** 온라인 게임 애플리케이션 인스턴스에 대한 EC2 인스턴스 Savings Plan을 구매합니다. 분석 애플리케이션에 스팟 인스턴스를 사용합니다.
> **C.** 온라인 게임 애플리케이션 및 분석 애플리케이션에 스팟 인스턴스를 사용합니다. 할인된 가격으로 서비스를 프로비저닝하려면 AWS Service Catalog에 카탈로그를 설정하세요.
> **D.** 온라인 게임 애플리케이션에 온디맨드 인스턴스를 사용합니다. 분석 애플리케이션에 스팟 인스턴스를 사용합니다. 할인된 가격으로 서비스를 프로비저닝하려면 AWS Service Catalog에 카탈로그를 설정하세요.
>
> 해설
> 정답: B
>
> EC2 인스턴스 Savings Plan은 연중 내내 실행되는 게임 애플리케이션에 적합, 비용을 절감, 항상 사용 가능해야 하는 게임 애플리케이션에 안정성을 제공
> 스팟 인스턴스는 중단되어도 무방한 분석 애플리케이션에 적합

◆ | **Q#0337.** | **Ref#0337.**
회사는 수백 개의 프로덕션 AWS 계정에서 애플리케이션을 실행합니다. 회사는 모든 기능이 활성화된 AWS

Organizations를 사용하며 AWS Backup을 사용하는 중앙 집중식 백업 작업을 수행합니다.

회사는 랜섬웨어 공격을 우려하고 있습니다. 이러한 문제를 해결하기 위해 회사는 모든 백업이 어떤 프로덕션 계정에서든지 특권 사용자 자격 증명이 침해되더라도 견딜 수 있어야 한다는 새로운 정책을 만들었습니다.

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

> **A.** 지정된 비프로덕션 계정에서 AWS Backup 볼트를 사용하여 교차 계정 백업을 구현합니다.
> **B.** AWS Backup 볼트 수정을 제한하는 SCP를 추가합니다.
> **C.** 규정 준수 모드에서 AWS Backup Vault Lock을 구현합니다.
> **C.** AWS Backup에 할당된 IAM 서비스 역할에 대한 최소 권한 액세스를 구현합니다.
> **D.** 콜드 계층에 항상 하나 이상의 백업이 존재하도록 백업 빈도, 수명 주기 및 보존 기간을 구성합니다.
> **E.** 지정된 비프로덕션 계정의 Amazon S3 버킷에 모든 백업을 기록하도록 AWS Backup을 구성합니다. S3 버킷에 S3 객체 잠금이 활성화되어 있는지 확인하세요.
>
> 해설
> 정답: A,B,C
>
> 교차 계정 백업(A): 교차 계정 백업을 사용하여 프로덕션 계정이 침해되더라도 백업 데이터를 보호할 수 있음.
> SCP 추가(B): SCP(Service Control Policies)를 통해 백업 볼트 수정에 대한 제한을 추가함으로써 추가적인 보호 계층을 제공.
> AWS Backup Vault Lock(C): 컴플라이언스 모드에서 Vault Lock을 구현하여 백업 데이터를 삭제 또는 변경할 수 없도록 함.
> D->백업 빈도를 구성해도 위반을 방지하는 데 아무런 도움이 되지 않습니다. 수명주기는 백업 삭제를 방지하지 않음.
> E->AWS 백업은 현재 S3를 백업용 스토리지 위치로 지원하지 않습니다. AWS 백업을 사용하여 S3 버킷을 백업할 수 있지만 백업을 저장하는 데는 사용할 수 없습니다.

◆ | **Q#0338.** | **Ref#0338.**
회사는 AWS 계정의 Amazon CloudWatch 로그를 하나의 중앙 로깅 계정으로 집계해야 합니다. 수집된 로그는 생성된 AWS 리전에 남아 있어야 합니다. 그런 다음 중앙 로깅 계정은 로그를 처리하고, 로그를 표준 출력 형식으로 정규화하고, 추가 처리를 위해 출력 로그를 보안 도구로 스트리밍합니다.

솔루션 설계자는 수집해야 하는 대량의 로깅 데이터를 처리할 수 있는 솔루션을 설계해야 합니다. 정규 업무 시간 동안보다 정규 업무 시간 외에는 로깅이 덜 발생합니다. 로깅 솔루션은 예상 부하에 따라 확장되어야 합니다. 솔루션 아키텍트는 다중 계정 로깅 프로세스를 처리하기 위해 AWS Control Tower 설계를 사용하기로 결정했습니다.

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

> **A.** 중앙 로깅 계정에 대상 Amazon Kinesis 데이터 스트림을 생성합니다.
> **B.** 중앙 로깅 계정에 대상 Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다.
> **C.** Amazon CloudWatch Logs에 Amazon Kinesis 데이터 스트림에 데이터를 추가할 수 있는 권한을 부여하는 IAM 역할을 생성합니다. 신뢰 정책을 만듭니다. IAM 역할에 신뢰 정책을 지정합니다. 각 회원 계정에서 각 로그 그룹에 대한 구독 필터를 생성하여 Kinesis 데이터 스트림으로 데이터를 보냅니다.
> **D.** Amazon CloudWatch Logs에 Amazon Simple Queue Service(Amazon SQS) 대기열에 데이터를 추가할 수 있는 권한을 부여하는 IAM 역할을 생성합니다. 신뢰 정책을 만듭니다. IAM 역할에 신뢰 정책을 지정합니다. 각 회원 계정에서 모든 로그 그룹에 대한 단일 구독 필터를 생성하여 SQS 대기열로 데이터를 보냅니다.
> **E.** AWS Lambda 함수를 생성합니다. 중앙 로깅 계정의 로그를 정규화하고 보안 도구에 로그를 쓰도록 Lambda 함수를 프로그래밍합니다.

F. AWS Lambda 함수를 생성합니다. 회원 계정의 로그를 정규화하고 보안 도구에 로그를 쓰도록 Lambda 함수를 프로그래밍합니다.

해설
정답: A,C,E

Kinesis 데이터 스트림을 사용하여 대량의 로그 데이터를 실시간으로 처리할 수 있습니다.
IAM 역할을 통해 CloudWatch Logs가 Kinesis 데이터 스트림에 로그를 전송할 수 있습니다.
Lambda 함수를 사용하여 로그를 표준 형식으로 변환하고 보안 도구로 스트리밍

◆ | **Q#0339.** | **Ref#0339.**
회사는 온프레미스 데이터 센터의 레거시 애플리케이션을 AWS로 마이그레이션하고 있습니다. 애플리케이션은 단일 애플리케이션 서버와 Microsoft SQL Server 데이터베이스 서버로 구성됩니다. 각 서버는 연결된 여러 볼륨에서 500TB의 데이터를 소비하는 VMware VM에 배포됩니다.

이 회사는 가장 가까운 AWS 지역에서 온프레미스 데이터 센터까지 10Gbps AWS Direct Connect 연결을 설정했습니다. Direct Connect 연결은 현재 다른 서비스에서 사용되지 않습니다.

가동 중지 시간을 최소화하면서 애플리케이션을 마이그레이션하려면 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (2개를 선택하세요.)

A. AWS SMS(AWS Server Migration Service) 복제 작업을 사용하여 데이터베이스 서버 VM을 AWS로 마이그레이션합니다.
B. VM Import/Export를 사용하여 애플리케이션 서버 VM을 가져옵니다.
C. VM 이미지를 AWS Snowball Edge Storage Optimized 디바이스로 내보냅니다.
D. AWS SMS(AWS Server Migration Service) 복제 작업을 사용하여 애플리케이션 서버 VM을 AWS로 마이그레이션합니다.
E. AWS DMS(AWS Database Migration Service) 복제 인스턴스를 사용하여 데이터베이스를 Amazon RDS DB 인스턴스로 마이그레이션합니다.

해설
정답: D,E

AWS SMS를 사용하면 기존 온프레미스 VM을 AWS로 쉽게 마이그레이션할 수 있음. 이는 큰 데이터 볼륨을 포함한 전체 서버를 마이그레이션하는 데 적합
AWS DMS를 사용하면 데이터베이스를 최소한의 다운타임으로 AWS로 마이그레이션할 수 있음. 이는 특히 큰 데이터베이스를 마이그레이션하는 데 유용하며, 지속적인 데이터 동기화를 지원

◆ | **Q#0340.** | **Ref#0340.**
회사는 온프레미스로 서버 집합을 운영하고 AWS Organizations의 조직에서 Amazon EC2 인스턴스 집합을 운영합니다. 회사의 AWS 계정에는 수백 개의 VPC가 포함되어 있습니다. 회사는 AWS 계정을 온프레미스 네트워크에 연결하려고 합니다. AWS Site-to-Site VPN 연결은 이미 단일 AWS 계정에 설정되어 있습니다. 회사는 어떤 VPC가 다른 VPC와 통신할 수 있는지 제어하려고 합니다.

최소한의 운영 노력으로 이러한 수준의 제어를 달성할 수 있는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. AWS 계정에서 전송 게이트웨이를 생성하십시오. AWS Resource Access Manager(AWS RAM)를 사용하여 계정 간에 전송 게이트웨이를 공유합니다.
B. 모든 VPC 및 VPN에 대한 연결을 구성합니다.
C. Transit Gateway 라우팅 테이블을 설정합니다. VPC 및 VPN을 라우팅 테이블과 연결합니다.
D. VPC 간 VPC 피어링을 구성합니다.
E. VPC와 VPN 간의 연결을 구성합니다.
F. VPC 및 VPN에 라우팅 테이블을 설정합니다.

해설

정답: A,B,C

Transit Gateway는 여러 VPC와 온프레미스 네트워크 간의 중앙 허브 역할을 합니다. AWS RAM을 사용하면 여러 계정에서 Transit Gateway를 공유할 수 있습니다.
모든 VPC와 VPN을 Transit Gateway에 연결해야 합니다. 이를 통해 트래픽이 Transit Gateway를 통해 라우팅될 수 있습니다.
Transit Gateway 라우트 테이블을 설정하여 어떤 VPC가 서로 통신할 수 있는지 제어할 수 있습니다. 이를 통해 필요한 경우 특정 VPC 간의 트래픽을 제한할 수 있습니다.

341 (박지수) 2회차 完

◆ | **Q#0341.** | **Ref#0341.**
회사는 AWS에서의 애플리케이션 비용을 최적화해야 합니다. 애플리케이션은 AWS Fargate에서 실행되는 AWS Lambda 함수와 Amazon Elastic Container Service(Amazon ECS) 컨테이너를 사용합니다. 이 애플리케이션은 쓰기 집약적이며 Amazon Aurora MySQL 데이터베이스에 데이터를 저장합니다.

애플리케이션의 로드가 일정하지 않습니다. 애플리케이션이 장기간 사용되지 않은 후 갑자기 트래픽이 크게 증가하거나 감소합니다. 데이터베이스는 로드를 처리할 수 없는 메모리 최적화 DB 인스턴스에서 실행됩니다.

솔루션 설계자는 트래픽 변화를 처리할 수 있도록 확장할 수 있는 솔루션을 설계해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 데이터베이스에 추가 읽기 전용 복제본을 추가합니다. 인스턴스 Savings Plan과 RDS 예약 인스턴스를 구매하세요.
B. 여러 작성자 인스턴스가 있는 Aurora DB 클러스터로 데이터베이스를 마이그레이션합니다. 인스턴스 Savings Plan을 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.

해설
정답: D

Aurora Serverless v1: 사용량에 따라 자동으로 확장하고 축소하여 비용을 절감. 사용량이 없는 경우 비용이 발생하지 않으며, 갑작스러운 트래픽 증가에도 자동으로 확장하여 부하를 처리.
Compute Savings Plan: Aurora Serverless의 리소스 사용량에 대해 절약할 수 있는 계획을 제공. 사용량을 예측할 수 없으므로 특정 인스턴스 타입에 적용하는 인스턴스 Savings Plan 보다 리소스 사용에 대한 할인을 적용하는 Compute Savings Plan 구매하는 것이 적절함

◆ | **Q#0342.** | **Ref#0342.**
한 회사가 애플리케이션을 AWS 클라우드로 마이그레이션했습니다. 애플리케이션은 ALB(Application Load Balancer) 뒤에 있는 두 개의 Amazon EC2 인스턴스에서 실행됩니다.
애플리케이션 데이터는 추가 EC2 인스턴스에서 실행되는 MySQL 데이터베이스에 저장됩니다. 애플리케이션의 데이터베이스 사용은 읽기 중심입니다.

애플리케이션은 각 EC2 인스턴스에 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨에서 정적 콘텐츠를 로드합니다. 정적 콘텐츠는 자주 업데이트되므로 각 EBS 볼륨에 복사해야 합니다.

애플리케이션의 로드는 하루 종일 변경됩니다. 사용량이 많은 시간에는 애플리케이션이 들어오는 요청을 모두 처리할 수 없습니다. 추적 데이터에 따르면 데이터베이스는 피크 시간 동안 읽기 로드를 처리할 수 없습니다.

애플리케이션의 안정성을 향상시키는 솔루션은 무엇입니까?

A. 애플리케이션을 AWS Lambda 함수 세트로 마이그레이션합니다. Lambda 함수를 ALB의 대상으로 설정합니다. 정적 콘텐츠를 위한 새로운 단일 EBS 볼륨을 생성합니다. 새 EBS 볼륨에서 읽도록 Lambda 함수를 구성합니다. 데이터베이스를 MySQL 다중 AZ DB 클러스터용 Amazon RDS로 마이그레이션합니다.
B. 애플리케이션을 AWS Step Functions 상태 머신 세트로 마이그레이션합니다. 정적 콘텐츠에 대한 ALCreate an Amazon Elastic File System(Amazon EFS) 파일 시스템의 대상으로 상태 시스템을 설정합니다. EFS 파일 시스템에서 읽도록 상태 시스템을 구성합니다. 리더 DB 인스턴스를 사용하여 데이터베이스를 Amazon Aurora MySQL Serverless v2로 마이그레이션합니다.
C. 애플리케이션을 컨테이너화합니다. 애플리케이션을 Amazon Elastic Container Service(Amazon ECS) 클러스터로 마이그레이션합니다. 애플리케이션을 호스팅하는 작업에는 AWS Fargate 시작 유형을 사용합니다. 정적 콘텐츠를 위한 새로운 단일 EBS 볼륨을 생성합니다. ECS 클러스터에 새 EBS 볼륨을 마운트합니다. ECS 클러스터에서 AWS Application Auto Scaling을 구성합니다. ECS 서비스를 ALB의 대상으로 설정합니다. 데이터베이스를 MySQL 다중 AZ DB 클러스터용 Amazon RDS로 마이그레이션합니다.
D. 애플리케이션을 컨테이너화합니다. 애플리케이션을 Amazon Elastic Container Service(Amazon ECS) 클러스터로 마이그레이션합니다. 애플리케이션을 호스팅하는 작업에는 AWS Fargate 시작 유형을 사용합니다. 정적 콘텐츠를 위한 Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. EFS 파일 시스템을 각 컨테이너에 탑재합니다. ECS 클러스터에서 AWS Application Auto Scaling을 구성합니다. ECS 서비스를 ALB의 대상으로 설정합니다. 리더 DB 인스턴스를 사용하여 데이터베이스를 Amazon Aurora MySQL Serverless v2로 마이그레이션합니다.

해설
정답: D
자주 업데이트되는 정적 컨텐츠 관리에는 EFS가 용이
Reader DB 인스턴스를 사용한 Aurora MySQL Serverless는 트래픽 증가에 따른 확장성 제공, 읽기 부하 효과적으로 관리

◆ | **Q#0343.** | **Ref#0343.**
솔루션 아키텍트는 적절한 권한이 있는 AWS 사용자 또는 역할만 새로운 Amazon API Gateway 엔드포인트에 액세스할 수 있는지 확인하려고 합니다. 솔루션 설계자는 요청의 대기 시간을 분석하고 서비스 맵을 생성하기 위해 각 요청에 대한 엔드투엔드 보기를 원합니다.

솔루션 설계자는 어떻게 API 게이트웨이 액세스 제어를 설계하고 요청 검사를 수행할 수 있나요?

A. API Gateway 방식의 경우 인증을 AWS_IAM으로 설정하세요. 그런 다음 IAM 사용자 또는 역할에 REST API 리소스에 대한 execute-api:Invoke 권한을 부여합니다. 엔드포인트에 액세스할 때 API 호출자가 AWS 서명으로 요청에 서명하도록 활성화합니다. AWS X-Ray를 사용하여 API Gateway에 대한 사용자 요청을 추적하고 분석합니다.
B. API 게이트웨이 리소스의 경우 CORS를 활성화로 설정하고 Access-Control-Allow-Origin 헤더에 회사 도메인만 반환합니다. 그런 다음 IAM 사용자 또는 역할에 REST API 리소스에 대한 실행-api:Invoke 권한을 부여합니다. Amazon CloudWatch를 사용하여 API Gateway에 대한 사용자 요청을 추적하고 분석합니다.
C. AWS Lambda 함수를 사용자 지정 권한 부여자로 생성하고 API 클라이언트에 호출 시 키와 비밀을 전달하도록 요청한 다음 Lambda를 사용하여 IAM 시스템에 대해 키/비밀 쌍을 검증합니다. AWS X-Ray를 사용하여 API Gateway에 대한 사용자 요청을 추적하고 분석합니다.
D. API Gateway용 클라이언트 인증서를 생성합니다. 엔드포인트에 액세스해야 하는 AWS 사용자 및 역할에 인증서를 배포합니다. 엔드포인트에 액세스할 때 API 호출자가 클라이언트 인증서를 전달하도록 활성화합니다. Amazon CloudWatch를 사용하여 API Gateway에 대한 사용자 요청을 추적하고 분석합니다.

해설

정답: A

API Gateway 메소드에 대해 권한을 AWS_IAM으로 설정하고, IAM 사용자나 역할에게 execute-api:Invoke 권한을 부여
엔드포인트에 액세스할 때 AWS Signature로 요청에 서명하도록 API 호출자에게 설정 함.
AWS X-Ray를 사용하여 API Gateway에 대한 사용자 요청을 추적하고 분석.

◆ | **Q#0344.** | **Ref#0344.**
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 변경 사항을 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 변경 사항을 승인하기 전에 테스트 환경에 배포하고 수동 테스트 계획을 실행하세요.
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.

해설
정답: B

AWS CodeBuild를 사용한 자동 테스트, CloudFormation 변경 세트 사용, AWS CodeDeploy를 통한 블루/그린 배포 패턴 사용
자동화된 테스트: AWS CodeBuild를 사용하여 테스트 환경에서 자동 테스트를 실행
변경 집합 평가: CloudFormation 변경 집합을 사용하여 배포 전 변경 사항을 평가
블루/그린 배포: AWS CodeDeploy를 사용하여 블루/그린 배포 패턴을 활용. 이 패턴을 사용하면 변경 사항을 평가하고 필요한 경우 롤백할 수 있음.

◆ | **Q#0345.** | **Ref#0345.**
동부 해안에 본사를 둔 북미 회사는 us-east-1 지역의 Amazon EC2에서 실행되는 새로운 웹 애플리케이션을 배포하고 있습니다. 애플리케이션은 사용자 요구를 충족하고 탄력성을 유지하기 위해 동적으로 확장되어야 합니다. 또한 애플리케이션에는 us-west-1 리전의 active-passive 구성에서 재해 복구 기능이 있어야 합니다.

us-east-1 리전에서 VPC를 생성한 후 솔루션 아키텍트가 수행해야 하는 단계는 무엇입니까?

A. us-west-1 리전에 VPC를 생성합니다. 리전 간 VPC 피어링을 사용하여 두 VPC를 모두 연결합니다. 여러 가용 영역(AZ)에 걸쳐 있는 Application Load Balancer(ALB)를 us-east-1 지역의 VPC에 배포합니다. 두 VPC에 걸쳐 있고 ALB에서 제공하는 Auto Scaling 그룹의 일부로 각 지역의 여러 AZ에 EC2 인스턴스를 배포합니다.
B. 여러 가용 영역(AZ)에 걸쳐 있는 ALB(Application Load Balancer)를 us-east-1 지역의 VPC에 배포

합니다. ALB에서 제공하는 Auto Scaling 그룹의 일부로 여러 AZ에 EC2 인스턴스를 배포합니다. 동일한 솔루션을 us-west-1 리전에 배포합니다. 두 리전에 걸쳐 고가용성을 제공하기 위해 장애 조치 라우팅 정책과 상태 확인이 활성화된 Amazon Route 53 레코드 세트를 생성합니다.
C. us-west-1 리전에 VPC를 생성합니다. 리전 간 VPC 피어링을 사용하여 두 VPC를 모두 연결합니다. 두 VPC 모두에 걸쳐 있는 ALB(Application Load Balancer)를 배포합니다. ALB가 제공하는 각 VPC에서 Auto Scaling 그룹의 일부로 여러 가용 영역에 EC2 인스턴스를 배포합니다. ALB를 가리키는 Amazon Route 53 레코드를 생성합니다.
D. 여러 가용 영역(AZ)에 걸쳐 있는 ALB(Application Load Balancer)를 us-east-1 지역의 VPC에 배포합니다. ALB에서 제공하는 Auto Scaling 그룹의 일부로 여러 AZ에 EC2 인스턴스를 배포합니다. us-west-1 리전에 동일한 솔루션을 배포합니다. 해당 지역의 ALB를 가리키는 각 지역에 별도의 Amazon Route 53 레코드를 생성합니다. Route 53 상태 확인을 사용하여 두 리전에 걸쳐 고가용성을 제공합니다.

해설
정답: B

두 리전 모두에서 ALB와 EC2 인스턴스 자동 확장 구현한 후 장애 조치 라우팅 정책이 포함된 Route53 생성
A(x), C(x): ALB는 여러 리전 간 걸쳐있을 수 없음 : A,C 오답

◆ | **Q#0346.** | **Ref#0346.**
회사에는 여러 .NET Framework 구성 요소에서 실행되는 레거시 응용 프로그램이 있습니다. 구성 요소는 동일한 Microsoft SQL Server 데이터베이스를 공유하고 MSMQ(Microsoft Message Queuing)를 사용하여 비동기적으로 서로 통신합니다.

회사는 컨테이너화된 .NET Core 구성 요소로의 마이그레이션을 시작하고 있으며 AWS에서 실행되도록 애플리케이션을 리팩터링하려고 합니다. .NET Core 구성 요소에는 복잡한 오케스트레이션이 필요합니다. 회사는 네트워킹 및 호스트 구성을 완전히 제어할 수 있어야 합니다. 애플리케이션의 데이터베이스 모델은 강력한 관계형입니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS App Runner에서 INET Core 구성 요소를 호스팅합니다. SQL Server용 Amazon RDS에서 데이터베이스를 호스팅합니다. 비동기 메시징에는 Amazon EventBiridge를 사용하십시오.
B. AWS Fargate 시작 유형을 사용하여 Amazon Elastic Container Service(Amazon ECS)에서 .NET Core 구성 요소를 호스팅합니다. Amazon Dynamo에서 데이터베이스 호스팅비동기 메시징을 위해 Amazon Simple 알림 서비스(Amazon SNS)를 사용하세요.
C. AWS Elastic Beanstalk에서 .NET Core 구성 요소를 호스팅합니다. Amazon Aurora PostgreSQL Serverless v2에서 데이터베이스를 호스팅합니다. 비동기 메시징에는 Amazon Managed Streaming for Apache Kafka(Amazon MSK)를 사용합니다.
D. Amazon EC2 시작 유형을 사용하여 Amazon Elastic Container Service(Amazon ECS)에서 .NET Core 구성 요소를 호스팅합니다. Amazon Aurora MySQL Serverless v2에서 데이터베이스를 호스팅합니다. 비동기 메시징에는 Amazon Simple Queue Service(Amazon SQS)를 사용합니다.

해설
정답: D
EC2 시작 유형이 포함된 ECS는 필요한 제어 및 컨테이너 오케스트레이션 기능 제공
Aurora MySQL Serverless는 관계형 데이터베이스 모델 지원
SQS는 비동기 메시징 요구사항에 부합하며 MSMQ를 적절하게 대체할 수 있음

App Runner는 복잡한 오케스트레이션 미지원(Ax), DynamoDB는 비관계형 데이터베이스(Bx), Elastic Beanstalk는 복잡한 오케스트레이션 제어 미제공(Cx)

◆ | **Q#0347.** | **Ref#0347.**
솔루션 아키텍트가 단일 가용 영역 내의 배치 그룹에서 여러 Amazon EC2 인스턴스를 시작했습니다. 시스템에 대한 추가 로드로 인해 솔루션 설계자는 배치 그룹에 새 인스턴스를 추가하려고 시도합니다. 그러나 솔루션 설계자는 용량 부족 오류를 수신합니다.

이 문제를 해결하려면 솔루션 설계자가 무엇을 해야 합니까?

> **A.** 스프레드 배치 그룹을 사용하십시오. 각 가용 영역에 대해 최소 8개의 인스턴스를 설정합니다.
> **B.** 배치 그룹의 모든 인스턴스를 중지하고 시작합니다. 다시 실행해 보세요.
> **C.** 새 배치 그룹을 생성합니다. 새 배치 그룹을 원래 배치 그룹과 병합합니다.
> **D.** 배치 그룹에서 전용 호스트로 추가 인스턴스를 시작합니다.
>
> 해설
> 정답: B
> 배치 그룹에 이미 실행 중인 인스턴스가 있는 경우에는 그 인스턴스들을 중지하고 다시 시작하여 리소스가 충분한 곳에 인스턴스를 시작할 수 있도록 합니다.
> 이러한 작업을 통해 리소스 예약이 올바르게 조정되어 용량 부족 오류를 해결할 수 있습니다.

◆ | **Q#0348.** | **Ref#0348.**
한 회사는 IaC(Infrastructure as Code)를 사용하여 두 개의 Amazon EC2 인스턴스 세트를 프로비저닝했습니다. 이러한 사례는 몇 년 동안 동일하게 유지되었습니다.

회사의 사업은 지난 몇 달 동안 급속히 성장했습니다. 이에 대응하여 회사 운영팀에서는 갑작스러운 트래픽 증가를 관리하기 위해 Auto Scaling 그룹을 구현했습니다. 회사 정책에 따라 실행 중인 모든 운영 체제에 보안 업데이트를 매월 설치해야 합니다.

최신 보안 업데이트에는 재부팅이 필요했습니다. 결과적으로 Auto Scaling 그룹은 인스턴스를 종료하고 패치가 적용되지 않은 새 인스턴스로 교체했습니다.

이 문제의 재발을 피하기 위해 솔루션 설계자는 어떤 단계 조합을 권장해야 합니까? (2개를 선택하세요.)

> **A.** 교체를 위해 가장 오래된 시작 구성을 대상으로 하도록 업데이트 정책을 설정하여 Auto Scaling 그룹을 수정합니다.
> **B.** 다음 패치 점검 전에 새로운 Auto Scaling 그룹을 생성합니다. 유지 관리 기간 동안 두 그룹을 모두 패치하고 인스턴스를 재부팅합니다.
> **C.** Auto Scaling 그룹 앞에 Elastic Load Balancer를 생성합니다. Auto Scaling 그룹이 종료된 인스턴스를 교체한 후 대상 그룹 상태 확인이 정상으로 반환되도록 모니터링을 구성합니다.
> **D.** AMI를 패치하고, 시작 구성을 업데이트하고, Auto Scaling 인스턴스 새로 고침을 호출하는 자동화 스크립트를 생성합니다.
> **E.** Auto Scaling 그룹 앞에 Elastic Load Balancer를 생성합니다. 인스턴스에 종료 방지 기능을 구성합니다.
>
> 해설
> 정답: C,D
> Auto Scaling 그룹 앞에 ELB를 생성하면 인스턴스 종료 및 시작에 대한 영향을 최소화 할 수 있음.
> ELB가 트래픽을 사용 가능한 인스턴스로 유도할 수 있음
> AMI를 패치하고, 배포설정을 업데이트하며, Auto Scaling 그룹에서 인스턴스를 새로 고칠 수 있게 하면, 패치가 설치되고 인스턴스가 재부팅되어도 Auto Scaling 그룹이 자동으로 새로고침되어 새로운 (그리고 패치된) AMI를 기반으로 새 인스턴스를 시작합니다.

◆ | **Q#0349.** | **Ref#0349.**
데이터 과학자 팀은 Amazon SageMaker 인스턴스와 SageMaker API를 사용하여 기계 학습(ML) 모델을 교육하고 있습니다. SageMaker 인스턴스는 인터넷에 대한 액세스 권한이 없거나 인터넷에서 액세스할 수 없는 VPC에 배포

됩니다. ML 모델 훈련을 위한 데이터 세트는 Amazon S3 버킷에 저장됩니다. 인터페이스 VPC 엔드포인트는 Amazon S3 및 SageMaker API에 대한 액세스를 제공합니다.

경우에 따라 데이터 과학자는 워크플로의 일부로 사용하는 Python 패키지를 업데이트하기 위해 PyPI(Python Package Index) 리포지토리에 액세스해야 합니다. 솔루션 설계자는 SageMaker 인스턴스가 인터넷에서 격리된 상태를 유지하도록 하면서 PyPI 저장소에 대한 액세스를 제공해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** 데이터 과학자가 액세스해야 하는 각 패키지에 대해 AWS CodeCommit 리포지토리를 생성합니다. PyPI 리포지토리와 CodeCommit 리포지토리 간의 코드 동기화를 구성합니다. CodeCommit에 대한 VPC 엔드포인트를 생성합니다.
> **B.** VPC에 NAT 게이트웨이를 생성합니다. PyPI 저장소 엔드포인트에만 액세스를 허용하는 네트워크 ACL을 사용하여 인터넷에 액세스할 수 있도록 VPC 경로를 구성합니다.
> **C.** 인터넷 액세스를 허용하려면 VPC구성 VPC 경로에 NAT 인스턴스를 생성합니다. PyPI 리포지토리 엔드포인트에만 액세스를 허용하는 SageMaker 노트북 인스턴스 방화벽 규칙을 구성합니다.
> **D.** AWS CodeArtifact 도메인 및 리포지토리를 생성합니다. CodeArtifact 리포지토리에 public:pypi에 대한 외부 연결을 추가합니다. CodeArtifact 리포지토리를 사용하도록 Python 클라이언트를 구성합니다. CodeArtifact에 대한 VPC 엔드포인트를 생성합니다.
>
> 해설
> 정답: D
> CodeArtifact를 사용하면 SageMaker 인스턴스에 대한 격리, 보안 및 비용 효율성을 유지하면서 PyPI에 대한 액세스 제공 요구 사항을 효과적으로 충족할 수 있음
>
> CodeArtifact를 사용하면 인기 있는 패키지 관리자를 사용하여 아티팩트를 저장할 수 있으며 Maven, Gradle, npm, Yarn, Twine, pip, NuGet 및 SwiftPM과 같은 빌드 도구를 사용할 수 있습니다.

◆ | **Q#0350.** | **Ref#0350.**
솔루션 설계자는 재해 복구 요구 사항이 엄격한 정부 기관에서 근무합니다. 모든 Amazon Elastic Block Store(Amazon EBS) 스냅샷은 2개 이상의 추가 AWS 리전에 저장되어야 합니다. 기관은 또한 가능한 최저 운영 간접비를 유지해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** EBS 스냅샷을 추가 지역에 복사하기 위해 매일 한 번 실행되도록 Amazon Data Lifecycle Manager(Amazon DLM)에서 정책을 구성합니다.
> **B.** Amazon EventBridge를 사용하여 EBS 스냅샷을 추가 지역에 복사하도록 AWS Lambda 함수를 예약합니다.
> **C.** AWS 백업을 설정하여 EBS 스냅샷을 생성합니다. EBS 스냅샷을 추가 지역에 복사하도록 Amazon S3 교차 지역 복제를 구성합니다.
> **D.** Amazon EC2 Image Builder가 매일 한 번 실행되도록 예약하여 AMI를 생성하고 AMI를 추가 지역에 복사합니다.
>
> 해설
> 정답: A
> DLM 사용하여 스냅샷을 추가 리전으로 자동 복사하도록 구성
> 재해 복구를 위해 스냅샷이 여러 지역에 저장되도록 보장하면서 최소한의 운영 오버헤드 요구사항 충족
>
> Amazon Data Lifecycle Manager(DLM)은 EBS 스냅샷 관리를 자동화하는 데 사용될 수 있습니다. 하루에 한 번씩 EBS 스냅샷을 생성하고 이를 추가 리전으로 복사하는 정책을 구성할 수 있습니다. DLM을 사용하면 운영 오버헤드가 낮아지고, 재해 복구 요구사항을 충족할 수 있습니다.

351 (정창화) 3회차 完

◆ | **Q#0351.** | **Ref#0351.**
회사에 필요한 것보다 더 큰 Amazon EC2 인스턴스를 시작하는 프로젝트가 있습니다. 이 활동을 기업 IT 외부에 유지하라는 정책 제한으로 인해 프로젝트 계정은 AWS Organizations의 회사 조직에 속할 수 없습니다. 회사는 프로젝트 계정의 개발자가 t3.small EC2 인스턴스를 시작하는 것만 허용하려고 합니다. 이러한 EC2 인스턴스는 us-east-2 리전으로 제한되어야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** 새 개발자 계정을 만드세요. 모든 EC2 인스턴스, 사용자 및 자산을 us-east-2로 이동합니다. AWS Organizations에서 회사 조직에 계정을 추가합니다. 지역 선호도를 나타내는 태그 지정 정책을 시행합니다.
> **B.** us-east-2에서 t3.small EC2 인스턴스를 제외한 모든 EC2 인스턴스의 시작을 거부하는 SCP를 생성합니다. SCP를 프로젝트 계정에 연결합니다.
> **C.** us-east-2의 각 개발자에 대해 t3.small EC2 예약 인스턴스를 생성하고 구매합니다. 각 개발자에게 이름을 태그로 사용하여 특정 EC2 인스턴스를 할당합니다.
> **D.** us-east-2에서 t3.small EC2 인스턴스만 시작하도록 허용하는 IAM 정책을 생성합니다. 개발자가 프로젝트 계정에서 사용하는 역할 및 그룹에 정책을 연결합니다.
>
> 해설
> 정답: D
> IAM 정책을 생성하여 사용자 수행 작업을 정확하게 제어가능. 이 정책을 통해 t3.small 인스턴스만 시작할 수 있도록 하고, us-east-2 리전으로 제한할 수 있음.
> 이 방법은 계정 구조 변경이나 AWS Organizations와의 통합을 요구하지 않으므로 간단함.
> 서비스 제어 정책(SCP)은 AWS Organizations의 기능이므로 사용할 수 없음.

◆ | **Q#0352.** | **Ref#0352.**
어느 과학 회사가 Amazon S3 버킷에서 텍스트 및 이미지 데이터를 처리해야 합니다. 데이터는 심우주 임무의 시간이 중요한 실시간 단계 동안 여러 레이더 스테이션에서 수집됩니다. 레이더 스테이션은 데이터를 소스 S3 버킷에 업로드합니다. 데이터 앞에는 레이더 스테이션 식별 번호가 붙습니다.

회사는 두 번째 계정에 대상 S3 버킷을 생성했습니다. 규정 준수 목적을 충족하기 위해 소스 S3 버킷에서 대상 S3 버킷으로 복사해야 합니다. 이 복제는 소스 S3 버킷의 모든 객체를 포함하는 S3 복제 규칙을 통해 수행됩니다.

특정 레이더 기지가 가장 정확한 데이터를 가지고 있는 것으로 식별되었습니다. 이 레이더 기지에서 데이터 복제는 소스 S3 버킷에 객체를 업로드한 후 30분 이내에 완료되었는지 모니터링해야 합니다.

솔루션 아키텍트는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** AWS DataSync 에이전트를 설정하여 소스 S3 버킷에서 대상 S3 버킷으로 접두사가 붙은 데이터를 복제합니다. 작업에서 사용 가능한 모든 대역폭을 사용하도록 선택하고, 작업이 'TRANSFERRING' 상태인지 모니터링합니다. 이 상태가 변경되면 알림을 시작하는 Amazon EventBridge 규칙을 생성합니다.
> **B.** 두 번째 계정에서 가장 정확한 데이터를 가진 레이더 기지로부터 데이터를 수신하기 위한 또 다른 S3 버킷을 생성합니다. 다른 레이더 기지들과의 복제를 분리하기 위해 이 새로운 S3 버킷에 대해 새로운 복제 규칙을 설정합니다. 대상 버킷으로의 최대 복제 시간을 모니터링합니다. 시간이 원하는 임계값을 초과할 때 알림을 시작하는 Amazon EventBridge 규칙을 생성합니다.
> **C.** 소스 S3 버킷에서 Amazon S3 Transfer Acceleration을 활성화하고, 가장 정확한 데이터를 가진 레이더 기지를 새로운 엔드포인트를 사용하도록 구성합니다. S3 대상 버킷의 'TotalRequestLatency' 메트릭을 모니터링합니다. 이 상태가 변경되면 알림을 시작하는 Amazon EventBridge 규칙을 생성합니다.
> **D.** 가장 정확한 데이터를 가진 레이더 기지의 접두사를 사용하는 키를 필터링하는 새로운 S3 복제

규칙을 소스 S3 버킷에 생성합니다. S3 복제 시간 제어(S3 RTC)를 활성화합니다. 대상 버킷으로의 최대 복제 시간을 모니터링합니다. 시간이 원하는 임계값을 초과할 때 알림을 시작하는 Amazon EventBridge 규칙을 생성합니다.

해설
정답: D
D는 가장 정확한 데이터를 가진 레이더 기지의 데이터를 빠르고 신뢰성 있게 복제하기 위해 필요한 조치를 제공함.
S3 복제 시간 제어(S3 RTC)는 데이터가 15분 이내에 복제되도록 보장하므로 30분 이내에 복제가 완료되는지를 모니터링하는 요구 사항을 충족함.
또한, Amazon EventBridge 규칙을 사용하여 시간이 초과될 경우 알림을 설정할 수 있음.
이는 정확하고 시간에 민감한 데이터 전송을 보장하는 데 적합함.

◆ | **Q#0353.** | **Ref#0353.**
회사에서 온프레미스 데이터 센터를 AWS 클라우드로 마이그레이션하려고 합니다. 여기에는 수천 개의 가상화된 Linux 및 Microsoft Windows 서버, SAN 스토리지, MySQL이 포함된 Java 및 PHP 애플리케이션, Oracle 데이터베이스가 포함됩니다. 동일한 데이터 센터 또는 외부에서 호스팅되는 종속 서비스가 많이 있습니다. 기술 문서가 불완전하고 오래되었습니다. 솔루션 아키텍트는 현재 환경을 이해하고 마이그레이션 후 클라우드 리소스 비용을 추정해야 합니다.

솔루션 설계자는 클라우드 마이그레이션을 계획하기 위해 어떤 도구 또는 서비스를 사용해야 합니까? (3개를 선택하세요.)

A. AWS 애플리케이션 검색 서비스
B. AWS SMS
C. AWS 엑스레이
D. AWS 클라우드 채택 준비 도구(CART)
E. 아마존 인스펙터
F. AWS 마이그레이션 허브

해설
정답: A, D, F
AWS Application Discovery Service: 이 서비스는 온프레미스 데이터 센터의 서버, 애플리케이션 및 종속성을 자동으로 검색하고 수집해줌.
AWS Cloud Adoption Readiness Tool (CART): 이 도구는 회사의 클라우드 준비 상태를 평가하고 마이그레이션 계획을 지원함.
AWS Migration Hub: 이 서비스는 여러 AWS 및 파트너 마이그레이션 도구를 중앙에서 관리하고 마이그레이션 상태를 추적할 수 있게 해줌.

◆ | **Q#0354.** | **Ref#0354.**
솔루션 아키텍트가 애플리케이션의 출시 전에 복원력을 검토하고 있습니다. 애플리케이션은 VPC의 프라이빗 서브넷에 배포된 Amazon EC2 인스턴스에서 실행됩니다. EC2 인스턴스는 최소 용량이 1이고 최대 용량이 1인 Auto Scaling 그룹에 의해 프로비저닝됩니다. 애플리케이션은 데이터를 Amazon RDS for MySQL DB 인스턴스에 저장합니다. VPC는 세 개의 가용 영역에 서브넷이 구성되어 있으며 단일 NAT 게이트웨이로 구성되어 있습니다.

솔루션 아키텍트는 애플리케이션이 여러 가용 영역에서 작동할 수 있도록 보장하는 솔루션을 추천해야 합니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 다른 가용 영역에 추가 NAT 게이트웨이를 배포합니다. 적절한 경로로 라우팅 테이블을 업데이트합니다. MySQL용 RDS DB 인스턴스를 다중 AZ 구성으로 수정합니다. 가용 영역 전체에서 인스턴스를 시작하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹의 최소 용량과 최대 용량을 3으로 설정합니다.
B. NAT 게이트웨이를 가상 프라이빗 게이트웨이로 교체합니다. MySQL용 RDS DB 인스턴스를

Amazon Aurora MySQL DB 클러스터로 교체합니다. VPC의 모든 서브넷에서 인스턴스를 시작하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹의 최소 용량과 최대 용량을 3으로 설정합니다.
C. NAT 게이트웨이를 NAT 인스턴스로 교체합니다. MySQL용 RDS DB 인스턴스를 PostgreSQL용 RDS DB 인스턴스로 마이그레이션합니다. 다른 가용 영역에서 새 EC2 인스턴스를 시작합니다.
D. 다른 가용 영역에 추가 NAT 게이트웨이를 배포합니다. 적절한 경로로 라우팅 테이블을 업데이트합니다. RDS for MySQL DB 인스턴스의 자동 백업을 켜고 백업을 7일 동안 보관하도록 수정합니다. Auto Scaling 그룹이 VPC의 모든 서브넷에서 인스턴스를 시작하도록 구성합니다. Auto Scaling 그룹의 최소 용량과 최대 용량을 1로 유지합니다.

해설
정답: A
A는 애플리케이션의 고가용성과 복원력을 보장하기 위해 필요한 모든 조치를 포함하고 있음.
여러 가용 영역에 NAT 게이트웨이를 배포하고 라우팅 테이블을 업데이트함으로써 네트워크 경로의 단일 장애점을 제거할 수 있음.
RDS for MySQL DB 인스턴스를 Multi-AZ 구성으로 수정하여 데이터베이스의 고가용성을 보장
여러 가용 영역에 인스턴스를 배포하도록 Auto Scaling 그룹을 구성하고 최소 및 최대 용량을 3으로 설정하여 애플리케이션 인스턴스의 고가용성을 보장.
이러한 조치는 애플리케이션이 여러 가용 영역에서 안정적으로 작동할 수 있도록 함

◆ | **Q#0355.** | **Ref#0355.**
한 회사가 온프레미스 트랜잭션 처리 애플리케이션을 AWS로 마이그레이션할 계획입니다. 애플리케이션은 회사 데이터 센터의 VM에서 호스팅되는 Docker 컨테이너 내에서 실행됩니다. Docker 컨테이너에는 애플리케이션이 트랜잭션 데이터를 기록하는 공유 스토리지가 있습니다.

거래는 시간에 민감합니다. 애플리케이션 내부의 거래량은 예측할 수 없습니다. 회사는 증가하는 수요에 맞춰 처리량을 자동으로 확장하는 지연 시간이 짧은 스토리지 솔루션을 구현해야 합니다. 회사는 애플리케이션을 더 이상 개발할 수 없으며 Docker 호스팅 환경을 계속 관리할 수 없습니다.

이러한 요구 사항을 충족하려면 회사에서 애플리케이션을 AWS로 어떻게 마이그레이션해야 합니까?

A. 애플리케이션을 실행하는 컨테이너를 Amazon Elastic Kubernetes Service(Amazon EKS)로 마이그레이션합니다. Amazon S3를 사용하여 컨테이너가 공유하는 거래 데이터를 저장합니다.
B. 애플리케이션을 실행하는 컨테이너를 Amazon Elastic Container Service(Amazon ECS)용 AWS Fargate로 마이그레이션합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. Fargate 작업 정의를 생성합니다. EFS 파일 시스템을 가리키도록 작업 정의에 볼륨을 추가합니다.
C. 애플리케이션을 실행하는 컨테이너를 Amazon Elastic Container Service(Amazon ECS)용 AWS Fargate로 마이그레이션합니다. Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성합니다. Fargate 작업 정의를 생성합니다. 실행 중인 각 작업에 EBS 볼륨을 연결합니다.
D. Amazon EC2 인스턴스를 시작합니다. EC2 인스턴스에 Docker를 설치합니다. 컨테이너를 EC2 인스턴스로 마이그레이션합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. EFS 파일 시스템의 EC2 인스턴스에 탑재 지점을 추가합니다.

해설
정답: B
B는 회사가 Docker 호스팅 환경을 관리할 필요 없이 애플리케이션을 AWS로 마이그레이션할 수 있는 최상의 방법을 제공함.
AWS Fargate는 서버리스 방식으로 컨테이너를 관리할 수 있게 해주며, Amazon ECS를 통해 컨테이너 오케스트레이션을 처리함.
Amazon EFS는 낮은 대기 시간의 공유 파일 시스템으로, 컨테이너가 공유 스토리지를 필요로 하는 애플리케이션에 적합
EFS는 자동으로 처리량을 확장하여 증가하는 수요를 충족할 수 있음.

◆ | **Q#0356.** | **Ref#0356.**
한 회사가 AWS 클라우드로 마이그레이션할 계획을 갖고 있습니다. 이 회사는 Windows 서버와 Linux 서버에서 많은 애플리케이션을 호스팅합니다. 일부 서버는 물리적 서버이고 일부 서버는 가상 서버입니다. 회사는 온프레미스 환경에서 여러 유형의 데이터베이스를 사용합니다. 회사는 온프레미스 서버 및 애플리케이션에 대한 정확한 인벤토리를 보유하고 있지 않습니다.

회사는 마이그레이션 중에 리소스 크기를 조정하려고 합니다. 솔루션 설계자는 네트워크 연결 및 애플리케이션 관계에 대한 정보를 얻어야 합니다. 솔루션 설계자는 회사의 현재 환경을 평가하고 마이그레이션 계획을 개발해야 합니다.

솔루션 설계자에게 마이그레이션 계획을 개발하는 데 필요한 정보를 제공하는 솔루션은 무엇입니까?

> **A.** Migration Evaluator를 사용하여 AWS에 환경 평가를 요청하십시오. AWS Application Discovery Service Agentless Collector를 사용하여 Migration Evaluator Quick Insights 보고서로 세부 정보를 가져옵니다.
> **B.** AWS Migration Hub를 사용하고 서버에 AWS Application Discovery Agent를 설치하십시오. Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기를 배포합니다. Migration Hub Strategy Recommendations을 사용하여 보고서를 생성합니다.
> **C.** AWS Migration Hub를 사용하고 서버에서 AWS Application Discovery Service Agentless Collector를 실행합니다. AWS Application Migration Service를 사용하여 서버와 데이터베이스를 그룹화합니다. Migration Hub 전략 권장 사항을 사용하여 보고서를 생성합니다.
> **D.** AWS Migration Hub 가져오기 도구를 사용하여 회사의 온프레미스 환경에 대한 세부 정보를 로드합니다. Migration Hub 전략 권장 사항을 사용하여 보고서를 생성합니다.
>
> 해설
> 정답: B
> 회사의 온프레미스 서버와 애플리케이션에 대한 정확한 정보를 얻기 위해 AWS Migration Hub와 AWS Application Discovery Agent를 사용하여 데이터를 수집.
> Migration Hub Strategy Recommendations 애플리케이션 데이터 수집기를 배포하여 추가적인 전략적 권장 사항을 얻을 수 있음.
> 이 방법은 현재 환경을 평가하고 적절한 마이그레이션 계획을 개발하는 데 필요한 정보를 제공

◆ | **Q#0357.** | **Ref#0357.**
금융 서비스 회사는 대규모 글로벌 은행에 애플리케이션 규정 준수를 위한 SaaS(Software-as-a-Service) 플랫폼을 판매합니다. SaaS 플랫폼은 AWS에서 실행되며 AWS Organizations의 조직에서 관리되는 여러 AWS 계정을 사용합니다. SaaS 플랫폼은 전 세계적으로 많은 AWS 리소스를 사용합니다.

규정 준수를 위해 AWS 리소스에 대한 모든 API 호출을 감사하고, 변경 사항을 추적하고, 내구성 있고 안전한 데이터 저장소에 저장해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 새로운 AWS CloudTrail 추적을 생성합니다. 조직의 마스터 계정에 있는 기존 Amazon S3 버킷을 사용하여 로그를 저장합니다. 모든 AWS 리전에 추적을 배포합니다. S3 버킷에서 MFA 삭제 및 암호화를 활성화합니다.
> **B.** 조직의 각 구성원 계정에 새로운 AWS CloudTrail 추적을 생성합니다. 로그를 저장할 새 Amazon S3 버킷을 생성합니다. 모든 AWS 리전에 추적을 배포합니다. S3 버킷에서 MFA 삭제 및 암호화를 활성화합니다.
> **C.** 조직의 마스터 계정에 새로운 AWS CloudTrail 추적을 생성합니다. 로그를 저장하기 위해 버전 관리가 활성화된 새 Amazon S3 버킷을 생성합니다. 조직의 모든 계정에 대한 추적을 배포합니다. S3 버킷에서 MFA 삭제 및 암호화를 활성화합니다.
> **D.** 조직의 마스터 계정에 새로운 AWS CloudTrail 추적을 생성합니다. 로그를 저장할 새 Amazon S3 버킷을 생성합니다. 로그를 추적할 외부 관리 시스템에 로그 파일 전송 알림을 보내도록 Amazon Simple 알림 서비스(Amazon SNS)를 구성합니다. S3 버킷에서 MFA 삭제 및 암호화를 활성화합니다.

해설
정답: C
운영 오버헤드 최소화: 조직의 Master 계정에서 단일 CloudTrail 트레일을 생성하여 모든 계정을 관리하면 각 계정별로 별도의 트레일을 생성하는 것보다 관리가 훨씬 용이함.
중앙 집중식 로깅: 모든 로그를 한 곳에 중앙 집중식으로 저장하면 로그 관리 및 분석이 더 쉬워짐.
버전 관리 및 보안: S3 버킷에서 버전 관리를 활성화하고, MFA 삭제와 암호화를 설정하여 로그 데이터의 내구성과 보안을 강화할 수 있음.
A: 기존 S3 버킷을 사용하여 비용을 절감할 수 있지만, 버전 관리가 없으므로 데이터 무결성에 취약.
B: 각 계정마다 개별 트레일을 생성하여 운영 오버헤드가 증가.
D: 추가적인 SNS 구성과 외부 관리 시스템 통합이 필요하므로 운영 오버헤드가 더 큼.

◆ | **Q#0358.** | **Ref#0358.**
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 인스턴스를 시작합니다.
D. 분산 배치 그룹에서 컴퓨팅 최적화 EC2 인스턴스를 시작합니다.

해설
정답: C
클러스터 배치 그룹: 인스턴스를 물리적으로 가까운 위치에 배치하여 네트워크 지연 시간을 최소화하고 높은 네트워크 대역폭을 제공하는 데 최적화되어 있음.
분산 인메모리 데이터베이스와 같은 응용 프로그램은 낮은 네트워크 지연 시간과 높은 네트워크 처리량이 중요하므로 클러스터 배치 그룹이 적합.
메모리 최적화 EC2 인스턴스: 인메모리 데이터베이스의 경우, 대량의 데이터를 메모리에 저장하고 빠르게 액세스해야 하므로 메모리 최적화 인스턴스가 필요
이러한 인스턴스는 높은 메모리 용량과 메모리 대역폭을 제공하여 데이터베이스 성능을 극대화할 수 있음.

◆ | **Q#0359.** | **Ref#0359.**
회사는 VM에서 호스팅되는 약 100만 개의.csv 파일로 온프레미스에 정보를 유지 관리합니다. 데이터 크기는 처음에 10TB이며 매주 1TB씩 증가합니다. 회사는 AWS 클라우드에 대한 데이터 백업을 자동화해야 합니다.

데이터 백업은 매일 이루어져야 합니다. 회사에는 지정된 소스 디렉터리에 있는 데이터의 하위 집합만 백업하기 위해 사용자 지정 필터를 적용하는 솔루션이 필요합니다. 회사는 AWS Direct Connect 연결을 설정했습니다.

최소한의 운영 오버헤드로 백업 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 멀티파트 업로드와 함께 Amazon S3 CopyObject API 작업을 사용하여 기존 데이터를 Amazon S3에 복사합니다. CopyObject API 작업을 사용하여 매일 Amazon S3에 새 데이터를 복제합니다.
B. AWS Backup에서 백업 계획을 생성하여 Amazon S3에 데이터를 백업합니다. 매일 실행되도록 백업 계획을 예약합니다.
C. AWS DataSync 에이전트를 온프레미스 하이퍼바이저에서 실행되는 VM으로 설치합니다. 매일 Amazon S3에 데이터를 복제하도록 DataSync 작업을 구성합니다.
D. 초기 백업에는 AWS Snowball Edge 디바이스를 사용합니다. 매일 Amazon S3에 대한 증분 백업을 위해 AWS DataSync를 사용하십시오.

해설
정답: C
AWS DataSync는 데이터를 온프레미스에서 AWS로 효율적이고 안전하게 전송할 수 있는 최적의 솔루션임.
- DataSync는 매일 데이터 전송을 자동화할 수 있음.
- DataSync는 전송 시 데이터 필터링 옵션을 제공하여 지정된 소스 디렉터리의 데이터 하위 집합만 전송할 수 있음.
- DataSync 에이전트를 VM에 설치하고 작업을 구성하면 지속적으로 관리할 필요가 없어 운영 오버헤드가 최소화됨.
B: AWS Backup은 온프레미스 데이터 백업을 지원하지 않음.
확실히 당신은 잘못 먹었습니다. ㅋㅋ

◆ | **Q#0360.** | **Ref#0360.**
금융 서비스 회사는 전 세계 수천 명의 고객이 사용하는 자산 관리 제품을 보유하고 있습니다. 고객은 설문조사를 통해 제품에 대한 피드백을 제공합니다. 회사는 Amazon EMR에서 실행되는 새로운 분석 솔루션을 구축하여 이러한 설문조사의 데이터를 분석하고자 합니다. 다음과 같은 사용자 역할이 각각 다른 작업을 수행하기 위해 분석 솔루션에 접근해야 합니다:

• 관리자: 팀의 요구사항에 따라 분석 팀을 위해 EMR 클러스터를 프로비저닝
• 데이터 엔지니어: 데이터 세트를 처리, 변환 및 보강하기 위한 ETL 스크립트 실행
• 데이터 분석가 : SQL 및 Hive 쿼리를 실행하여 데이터 분석

솔루션 아키텍트는 모든 사용자 역할이 필요한 리소스에만 최소 권한으로 접근할 수 있도록 해야 합니다. 사용자 역할은 승인되고 인증된 애플리케이션만 시작할 수 있어야 합니다. 또한 모든 리소스에 태그를 지정해야 합니다.

다음 솔루션 중 어느 것이 최소한의 운영 오버헤드로 이 요구사항을 충족합니까?

A. 각 사용자 역할에 대해 IAM 역할을 생성합니다. 해당 역할을 사용하는 사용자가 수행할 수 있는 작업을 정의하는 ID 기반 정책을 첨부합니다. 비규격 리소스를 확인하는 AWS Config 규칙을 생성합니다. 관리자가 비규격 리소스를 수정하도록 알리도록 규칙을 구성합니다.
B. EMR 클러스터를 시작할 때 Kerberos 기반 인증을 설정합니다. 클러스터별 Kerberos 옵션과 함께 Kerberos 보안 구성을 지정합니다.
C. AWS Service Catalog를 사용하여 배포 가능한 Amazon EMR 버전, 클러스터 구성 및 각 사용자 역할에 대한 권한을 제어합니다.
D. AWS CloudFormation을 사용하여 EMR 클러스터를 시작합니다. 클러스터 생성 중에 EMR 클러스터에 리소스 기반 정책을 첨부합니다. 비규격 클러스터와 비규격 Amazon S3 버킷을 확인하는 AWS Config 규칙을 생성합니다. 관리자가 비규격 리소스를 수정하도록 알리도록 규칙을 구성합니다.

해설
정답: C
AWS Service Catalog는 조직이 승인된 AWS 리소스를 관리하고 배포하는 데 사용되는 서비스로 다음과 같은 요구사항을 충족할 수 있음:
- 권한 제어: 각 사용자 역할에 필요한 최소 권한을 부여할 수 있음.
- 승인된 애플리케이션 실행: EMR 버전 및 클러스터 구성을 제어하여 승인된 애플리케이션만 사용할 수 있게 함.
- 태그 지정: 모든 리소스에 태그를 지정하여 리소스를 관리할 수 있음.

361 (나권서) 1회차 完

◆ | **Q#0361.** | **Ref#0361.**
SaaS(Software as a Service) 회사는 AWS를 사용하여 AWS PrivateLink에서 제공하는 서비스를 호스팅합니다. 이 서비스는 Network Load Balancer(NLB) 뒤에 있는 3개의 Amazon EC2 인스턴스에서 실행되는 독점 소프트웨어로 구

성됩니다. 인스턴스는 eu-west-2 지역의 여러 가용 영역에 있는 프라이빗 서브넷에 있습니다. 회사의 모든 고객은 eu-west-2에 있습니다.

그러나 회사는 이제 us-east-1 지역에서 새로운 고객을 확보했습니다. 회사는 us-east-1에 새 VPC와 새 서브넷을 생성합니다. 회사는 두 리전의 VPC 간에 리전 간 VPC 피어링을 설정합니다.

회사는 신규 고객에게 SaaS 서비스에 대한 액세스 권한을 부여하려고 하지만 us-east-1에 새로운 EC2 리소스를 즉시 배포하는 것을 원하지 않습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** eu-west-2에 있는 기존 NLB를 사용하도록 us-east-1에서 PrivateLink 엔드포인트 서비스를 구성합니다. 특정 AWS 계정에 SaaS 서비스에 연결할 수 있는 액세스 권한을 부여합니다.
> **B.** us-east-1에 NLB를 생성합니다. SaaS 서비스를 호스팅하는 eu-west-2에서 회사 인스턴스의 IP 주소를 사용하는 IP 대상 그룹을 생성합니다. us-east-1에 있는 NLB를 사용하는 PrivateLink 엔드포인트 서비스를 구성합니다. 특정 AWS 계정에 SaaS 서비스에 연결할 수 있는 액세스 권한을 부여합니다.
> **C.** eu-west-2의 EC2 인스턴스 앞에 Application Load Balancer(ALB)를 생성합니다. us-east-1에서 NLB를 생성합니다. us-east-1에 있는 NLB를 eu-west-2에 있는 ALB를 사용하는 ALB 대상 그룹과 연결합니다. us-east-1에 있는 NLB를 사용하는 PrivateLink 엔드포인트 서비스를 구성합니다. 특정 AWS 계정에 SaaS 서비스에 연결할 수 있는 액세스 권한을 부여합니다.
> **D.** AWS Resource Access Manager(AWS RAM)를 사용하여 eu-west-2에 있는 EC2 인스턴스를 공유합니다. us-east-1에서 eu-west-2의 공유 EC2 인스턴스를 포함하는 NLB와 인스턴스 대상 그룹을 생성합니다. us-east-1에 있는 NLB를 사용하는 PrivateLink 엔드포인트 서비스를 구성합니다. 특정 AWS 계정에 SaaS 서비스에 연결할 수 있는 액세스 권한을 부여합니다.
>
> 해설
> 정답: B(x), **A**
>
> A: 이제 지역 내 및 지역 간 VPC 피어링 연결을 통해 AWS PrivateLink 엔드포인트에 액세스할 수 있습니다.
> 프라이빗 링크는 지역 간 vpc 피어링을 통한 액세스를 지원합니다.
> AWS PrivateLink, 이제 VPC 피어링을 통한 액세스 지원
>
> PrivateLink 엔드포인트 서비스를 통해 기존 NLB를 사용하여 다른 리전에서 서비스를 이용할 수 있습니다.
> 고객의 트래픽이 인터 리전 VPC 피어링을 통해 전달되며, 새로운 리전에 EC2 인스턴스를 배포할 필요가 없습니다.
> 특정 AWS 계정에 접근 권한을 부여하여 보안을 강화할 수 있습니다.

◆ | **Q#0362.** | **Ref#0362.**
회사는 두 AWS 리전에서 점점 늘어나는 Amazon S3 버킷 수를 모니터링해야 합니다. 또한 회사는 Amazon S3에서 암호화된 객체의 비율을 추적해야 합니다. 회사에는 내부 규정 준수 팀을 위해 이 정보를 표시하는 대시보드가 필요합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 각 지역에 새로운 3 Storage Lens 대시보드를 생성하여 버킷 및 암호화 지표를 추적합니다. 규정 준수 팀을 위해 두 지역 대시보드의 데이터를 Amazon QuickSight의 단일 대시보드로 집계합니다.
> **B.** 각 지역에 AWS Lambda 함수를 배포하여 버킷 수와 객체의 암호화 상태를 나열합니다. 이 데이터를 Amazon S3에 저장합니다. Amazon Athena 쿼리를 사용하여 규정 준수 팀을 위해 Amazon QuickSight의 사용자 지정 대시보드에 데이터를 표시합니다.
> **C.** S3 Storage Lens 기본 대시보드를 사용하여 버킷 및 암호화 지표를 추적합니다. S3 콘솔에서 직접 대시보드에 대한 액세스 권한을 규정 준수 팀에 부여하세요.

D. S3 객체 생성을 위한 AWS CloudTrail 이벤트를 감지하는 Amazon EventBridge 규칙을 생성합니다. Amazon DynamoDB에 암호화 지표를 기록하기 위해 AWS Lambda 함수를 호출하는 규칙을 구성합니다. Amazon QuickSight를 사용하여 규정 준수 팀을 위한 대시보드에 지표를 표시합니다.

해설
정답: C
S3 Storage Lens를 사용하여 버킷 및 암호화 메트릭을 추적하는 것이 가장 간단하고 추가 작업 부하가 적고 추가적인 대시보드나
사용자 정의 개발이 필요하지 않고, 기본 대시보드가 있어 운영을 간단하게 유지할 수 있음

◆ | **Q#0363.** | **Ref#0363.**
한 회사의 CISO는 솔루션 설계자에게 회사의 현재 CI/CD 관행을 재설계하여 취약점이 발견될 경우 가동 중지 시간을 최소화하면서 애플리케이션에 대한 패치 배포가 가능한 한 빨리 이루어질 수 있도록 요청했습니다. 또한 회사는 오류가 발생할 경우 변경 사항을 신속하게 롤백할 수 있어야 합니다.

웹 애플리케이션은 Application Load Balancer 뒤의 Amazon EC2 인스턴스 집합에 배포됩니다. 이 회사는 현재 GitHub를 사용하여 애플리케이션 소스 코드를 호스팅하고 있으며 애플리케이션을 구축하기 위해 AWS CodeBuild 프로젝트를 구성했습니다. 또한 회사는 AWS CodePipeline을 사용하여 기존 CodeBuild 프로젝트를 사용하여 GitHub 커밋에서 빌드를 트리거할 계획입니다.

모든 요구 사항을 충족하는 CI/CD 구성은 무엇입니까?

A. 내부 배포용으로 구성된 AWS CodeDeploy를 사용하여 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있는 경우 다른 코드 업데이트를 푸시하세요.
B. 블루/그린 배포용으로 구성된 AWS CodeDeploy를 사용하여 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있는 경우 CodeDeploy를 사용하여 수동 롤백을 트리거합니다.
C. AWS CloudFormation을 사용하여 테스트 및 프로덕션 스택을 위한 파이프라인을 생성하는 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있으면 다른 코드 업데이트를 푸시하세요.
D. AWS OpsWorks 및 내부 배포를 사용하여 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있으면 다른 코드 업데이트를 푸시하세요.

해설
정답: B
AWS CodeDeploy를 blue/green 배포용으로 설정된 deploy 단계를 포함하는 CodePipeline를 구성하여 새로 배포된 코드를 모니터링하고
문제가 발견되면 CodeDeploy를 사용하여 수동 롤백을 트리거하는 방식으로 요구 사항을 충족하고 이를 통해 빠르게 롤백하고
최소한의 다운타임으로 패치를 배포할 수 있음

◆ | **Q#0364.** | **Ref#0364.**
한 회사가 AWS Organizations의 조직을 이용하여 다수의 AWS 계정을 관리하고 있습니다. 회사의 다양한 사업부는 Amazon EC2 인스턴스에서 애플리케이션을 실행합니다. 회사가 각 사업 단위의 비용을 추적할 수 있도록 모든 EC2 인스턴스에는 BusinessUnit 태그가 있어야 합니다.

최근 감사 결과 일부 인스턴스에 이 태그가 누락된 것으로 나타났습니다. 회사에서는 누락된 태그를 인스턴스에 수동으로 추가했습니다.

향후 태그 요구 사항을 적용하려면 솔루션 설계자가 무엇을 해야 합니까?

A. 조직에서 태그 정책을 활성화합니다. BusinessUnit 태그에 대한 태그 정책을 생성합니다. 태그 키 대문자 사용 준수가 꺼져 있는지 확인하세요. ec2:instance 리소스 유형에 대한 태그 정책을 구현합니다. 태그 정책을 조직의 루트에 연결합니다.
B. 조직에서 태그 정책을 활성화합니다. BusinessUnit 태그에 대한 태그 정책을 생성합니다. 태그 키

대문자 사용 준수가 켜져 있는지 확인하세요. ec2:instance 리소스 유형에 대한 태그 정책을 구현합니다. 태그 정책을 조직의 마스터 계정에 연결합니다.
C. SCP를 생성하고 SCP를 조직의 루트에 연결합니다. SCP에 다음 설명을 포함합니다.

```
{
   "Sid": "DenyEC2Creation",
   "Effect": "Deny",
   "Action": [
       "ec2:RunInstances"
   ],
   "Resource": [
       "arn:aws:ec2:*:*:instance/*"
   ],
   "Condition": {
       "Null:" {
             "aws:RequestTag/BusinessUnit": "true"
         }
   }
}
```

D. SCP를 생성하고 SCP를 조직의 마스터 계정에 연결합니다. SCP에 다음 설명을 포함합니다.

```
{
   "Sid": "DenyEC2Creation",
   "Effect": "Deny",
   "Action": [
       "ec2:RunInstances"
   ],
   "Resource": [
       "arn:aws:ec2:*:*:instance/*"
   ],
   "Condition": {
       "Null:" {
             "aws:RequestTag/BusinessUnit": "false"
       }
   }
}
```

해설
정답: C
모든 AWS 리소스의 태그를 강제 적용하려면 SCP(Service Control Policy)를 사용해야함
마스터 계정은 계정을 만들고, 지불을 관리하고, 조직을 만드는 등의 장소. 조직의 루트는 정책을 적용하는 곳. 따라서 조직의 루트에 SCP 연결필요
SCP를 사용하면 조직의 태그 지정 제한 지침에 따라 태그가 지정되지 않은 새로운 AWS 리소스가 생성되는 것을 방지
태그 정책은 특정 태그의 key와 value를 제어하지만 태그 자체를 강제 적용할 수는 없음.

◆ | **Q#0365.** | **Ref#0365.**
한 회사가 수천 개의 Amazon EC2 인스턴스로 구성된 워크로드를 실행하고 있습니다. 워크로드는 여러 퍼블릭 서브넷과 프라이빗 서브넷이 포함된 VPC에서 실행 중입니다. 퍼블릭 서브넷에는 기존 인터넷 게이트웨이에 대한 0.0.0.0/0 경로가 있습니다. 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 추

가합니다.
C. 기존 VPC를 업데이트하고 Amazon 제공 IPv6 CIDR 블록을 VPC 및 모든 서브넷과 연결합니다. 외부 전용(egress-only) 인터넷 게이트웨이를 만듭니다. 모든 프라이빗 서브넷의 VPC 라우팅 테이블을 업데이트하고 외부 전용(egress-only) 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.

해설
정답: C
Amazon에서 제공하는 IPv6 CIDR 블록 사용: Amazon에서 제공하는 IPv6 CIDR 블록을 사용하는 것이 더 간편하고 AWS 서비스와의 통합이 원활
egress 전용 인터넷 게이트웨이는 프라이빗 서브넷의 인스턴스가 공용 인터넷에 접근할 수 있지만, 외부 공용 인터넷에서 프라이빗 서브넷 인스턴스로 접근은 차단.
egress-only 인터넷 게이트웨이는 IPv6를 사용하는 VPC 환경에서 프라이빗 서브넷의 인스턴스를 보호하면서도 인터넷에 접근할 수 있도록 함. 보안을 유지하면서도 필요한 인터넷 연결을 제공.
- NAT gateway는 IPv6를 지원하지 않음

◆ | **Q#0366.** | **Ref#0366.**
한 회사는 Amazon API Gateway를 사용하여 민감한 데이터에 대한 액세스를 제공하는 프라이빗 REST API를 배포하고 있습니다. API는 VPC에 배포된 애플리케이션에서만 액세스할 수 있어야 합니다. 회사는 API를 성공적으로 배포했습니다. 그러나 VPC에 배포된 Amazon EC2 인스턴스에서는 API에 액세스할 수 없습니다.

EC2 인스턴스와 API 간의 연결을 제공하는 솔루션은 무엇입니까?

A. API 게이트웨이용 인터페이스 VPC 엔드포인트를 생성합니다. apigateway:* 작업을 허용하는 엔드포인트 정책을 연결합니다. VPC 엔드포인트에 대한 프라이빗 DNS 이름 지정을 비활성화합니다. VPC에서의 액세스를 허용하는 API 리소스 정책을 구성합니다. API에 액세스하려면 VPC 엔드포인트의 DNS 이름을 사용하십시오.
B. API 게이트웨이용 인터페이스 VPC 엔드포인트를 생성합니다. Execute-api:Invoke 작업을 허용하는 엔드포인트 정책을 연결합니다. VPC 엔드포인트에 대한 프라이빗 DNS 이름 지정을 활성화합니다. VPC 엔드포인트에서의 액세스를 허용하는 API 리소스 정책을 구성합니다. API 엔드포인트의 DNS 이름을 사용하여 API에 액세스합니다.
C. NLB(Network Load Balancer)와 VPC 링크를 생성합니다. API 게이트웨이와 NLB 간의 프라이빗 통합을 구성합니다. API 엔드포인트의 DNS 이름을 사용하여 API에 액세스합니다.
D. ALB(Application Load Balancer)와 VPC 링크를 생성합니다. API Gateway와 ALB 간의 프라이빗 통합을 구성합니다. ALB 엔드포인트의 DNS 이름을 사용하여 API에 액세스합니다.

해설
정답: B
API Gateway에 대한 인터페이스 VPC 엔드포인트를 생성하고, 적절한 권한을 부여한 후, VPC 엔드포인트에 대한 Private DNS 네이밍을 활성화하고,
API 리소스에 대한 액세스를 허용하는 API 리소스정책을 구성한 후 API 엔드포인트의 DNS 이름을 사용하여 API에 접근할 수 있음
VPC 엔드포인트에 대한 Private DNS 네이밍 활성화

◆ | **Q#0367.** | **Ref#0367.**
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.

해설
정답: C
각 회원 계정에 OrganizationAccountAccessRole IAM 역할을 생성하고, 마스터 계정에 해당 IAM 역할을 맡을 수 있는 권한을 부여하면
이를 통해 중앙 마스터 계정이 각 회원 계정에 접근하여 청구 및 액세스 정책을 관리할 수 있음.

◆ | **Q#0368.** | **Ref#0368.**
회사에는 퍼블릭 IP를 사용하여 여러 Amazon EC2 인스턴스에 컨테이너화 및 배포된 애플리케이션 서비스가 있습니다. Apache Kafka 클러스터가 EC2 인스턴스에 배포되었습니다. PostgreSQL 데이터베이스가 PostgreSQL용 Amazon RDS로 마이그레이션되었습니다. 회사는 주력 제품의 새 버전이 출시되면 플랫폼 주문이 크게 증가할 것으로 예상하고 있습니다.

현재 아키텍처의 어떤 변경 사항이 운영 오버헤드를 줄이고 제품 릴리스를 지원합니까?

A. Application Load Balancer 뒤에 EC2 Auto Scaling 그룹을 생성합니다. DB 인스턴스에 대한 추가 읽기 전용 복제본을 생성합니다. Amazon Kinesis 데이터 스트림을 생성하고 데이터 스트림을 사용하도록 애플리케이션 서비스를 구성합니다. Amazon S3에서 직접 정적 콘텐츠를 저장하고 제공합니다.
B. Application Load Balancer 뒤에 EC2 Auto Scaling 그룹을 생성합니다. 다중 AZ 모드에서 DB 인스턴스를 배포하고 스토리지 Auto Scaling을 활성화합니다. Amazon Kinesis 데이터 스트림을 생성하고 데이터 스트림을 사용하도록 애플리케이션 서비스를 구성합니다. Amazon S3에서 직접 정적 콘텐츠를 저장하고 제공합니다.
C. Application Load Balancer 뒤의 EC2 인스턴스에 생성된 Kubernetes 클러스터에 애플리케이션을 배포합니다. 다중 AZ 모드에서 DB 인스턴스를 배포하고 스토리지 Auto Scaling을 활성화합니다. Apache Kafka용 Amazon Managed Streaming 클러스터를 생성하고 클러스터를 사용하도록 애플리케이션 서비스를 구성합니다. Amazon CloudFront 배포 뒤의 Amazon S3에 정적 콘텐츠를 저장합니다.
D. AWS Fargate를 사용하여 Amazon Elastic Kubernetes Service(Amazon EKS)에 애플리케이션을 배포하고 Application Load Balancer 뒤에서 자동 확장을 활성화합니다. DB 인스턴스에 대한 추가 읽기 전용 복제본을 생성합니다. Apache Kafka용 Amazon Managed Streaming 클러스터를 생성하고 클러스터를 사용하도록 애플리케이션 서비스를 구성합니다. Amazon CloudFront 배포 뒤의 Amazon S3에 정적 콘텐츠를 저장합니다.

해설
정답: D
AWS Fargate는 서버리스 컴퓨팅 서비스로 사용자가 서버 또는 인프라 관리에 신경 쓰지 않고 애플리케이션을 실행하면되고,
컨테이너 기반 애플리케이션을 실행할 때 컨테이너에 필요한 리소스를 관리하고 조정할 필요가 없음
Amazon EKS와 AWS Fargate 사용: EKS와 Fargate를 사용하면 EC2 인스턴스 관리를 줄일 수 있으며, 자동 확장을 통해 수요에 따라 리소스를 동적으로 관리할 수 있습니다.
Application Load Balancer: ALB를 사용하여 트래픽을 효율적으로 분산시켜 애플리케이션의 가용성

과 확장성을 보장합니다.
읽기 복제본 추가: DB 인스턴스에 추가 읽기 복제본을 생성하여 읽기 트래픽을 분산시키고 성능을 향상시킵니다.
Amazon Managed Streaming for Apache Kafka: 관리형 Kafka 클러스터를 사용하여 데이터 스트림 처리를 간소화하고 운영 오버헤드를 줄입니다.
Amazon S3 및 CloudFront: 정적 콘텐츠를 S3에 저장하고 CloudFront를 통해 제공하여 전 세계적으로 빠르고 안전하게 콘텐츠를 배포할 수 있습니다.

◆ | **Q#0369.** | **Ref#0369.**
회사는 온프레미스 데이터 센터에서 VPN을 호스팅합니다. 직원들은 현재 VPN에 연결하여 Windows 홈 디렉터리에 있는 파일에 액세스합니다. 최근 원격으로 근무하는 직원이 크게 늘었습니다. 그 결과, 데이터 센터 연결에 대한 대역폭 사용량이 업무 시간 동안 100%에 도달하기 시작했습니다.

회사는 회사의 원격 인력의 성장을 지원하고, 데이터 센터 연결을 위한 대역폭 사용량을 줄이고, 운영 오버헤드를 줄이는 솔루션을 AWS에서 설계해야 합니다.

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

A. AWS Storage Gateway 볼륨 게이트웨이를 생성합니다. 볼륨 게이트웨이에서 온프레미스 파일 서버로 볼륨을 탑재합니다.
B. 홈 디렉터리를 Windows 파일 서버용 Amazon FSx로 마이그레이션합니다.
C. 홈 디렉터리를 Amazon FSx for Lustre로 마이그레이션합니다.
D. 원격 사용자를 AWS Client VPN으로 마이그레이션합니다.
E. 온프레미스 데이터 센터에서 AWS로 AWS Direct Connect 연결을 생성합니다.

해설
정답: BD
기존 파일 스토리지를 Windows 파일 서버용 FSx로 마이그레이션
AWS Client VPN을 사용하면 원격 사용자가 온프레미스 데이터 센터에 대한 VPN 연결 없이도 Amazon FSx for Windows File Server를 포함한 AWS 리소스에 안전하게 연결가능.
원격 사용자를 AWS Client VPN으로 마이그레이션하면 사용자가 AWS에서 직접 리소스에 액세스하게 되므로 온프레미스 데이터 센터 연결 시 대역폭 사용량을 줄이는 데 도움이 될 수 있음.
이 접근 방식은 온프레미스 데이터 센터에서 VPN 인프라를 유지 관리하는 것에 비해 확장성이 뛰어나고 운영 오버헤드를 적게 관리할 수 있음.

◆ | **Q#0370.** | **Ref#0370.**
회사에는 여러 AWS 계정이 있습니다. 이 회사는 최근 보안 감사를 통해 Amazon EC2 인스턴스에 연결된 암호화되지 않은 Amazon Elastic Block Store(Amazon EBS) 볼륨이 많이 발견되었습니다.

솔루션 설계자는 암호화되지 않은 볼륨을 암호화하고 나중에 암호화되지 않은 볼륨이 자동으로 감지되도록 해야 합니다. 또한 회사는 규정 준수 및 보안에 중점을 두고 여러 AWS 계정을 중앙에서 관리할 수 있는 솔루션을 원합니다.

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

A. AWS Organizations에서 조직을 생성합니다. AWS Control Tower를 설정하고 강력히 권장되는 컨트롤(가드레일)을 켜십시오. 모든 계정을 조직에 가입하세요. AWS 계정을 OU로 분류합니다.
B. AWS CLI를 사용하여 모든 AWS 계정의 암호화되지 않은 모든 볼륨을 나열합니다. 암호화되지 않은 모든 볼륨을 제자리에 암호화하는 스크립트를 실행하십시오.
C. 암호화되지 않은 각 볼륨의 스냅샷을 생성합니다. 암호화되지 않은 스냅샷에서 새 암호화된 볼륨을 생성합니다. 기존 볼륨을 분리하고 암호화된 볼륨으로 교체합니다.
D. AWS Organizations에서 조직을 생성합니다. AWS Control Tower를 설정하고 필수 제어(가드레일)를 켭니다. 모든 계정을 조직에 가입하세요. AWS 계정을 OU로 분류합니다.

E. AWS CloudTrail을 활성화합니다. 암호화되지 않은 볼륨을 감지하고 자동으로 암호화하도록 Amazon EventBridge 규칙을 구성합니다.

해설
정답: AC
강력히 권장되는 가드레일: Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨에 대해 암호화가 활성화되었는지 여부를 감지.
볼륨이나 스냅샷을 제자리에서 암호화할 수 없음. 암호화되지 않은 스냅샷에서 새 암호화된 볼륨을 생성하고 이를 인스턴스에 연결해야 함.

371 (노종옥) 1회차 完

◆ | **Q#0371.** | **Ref#0371.**
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 ID 공급자(IdP)로 사용자 풀을 구성합니다. 앱 클라이언트를 만듭니다. 앱 클라이언트를 사용자 풀과 연결합니다. ALSpecify에 대한 리스너 규칙을 생성합니다. 리스너 규칙에 대한 authenticate-cognito 작업을 지정합니다. 사용자 풀과 앱 클라이언트를 사용하도록 리스너 규칙을 구성합니다.
C. 디렉터리를 새로운 IAM 자격 증명 공급자(IdP)로 추가합니다. SAML 2.0 연동 엔터티 유형을 가진 새 IAM 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 IAM ID 센터(AWS Single Sign-On)를 활성화합니다. SAML을 사용하는 외부 ID 공급자(IdP)로 디렉터리를 구성합니다. 자동 프로비저닝 방법을 사용합니다. SAML 2.0 연동 엔터티 유형을 가진 새 IAM 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.

해설
정답: B

Amazon Cognito 사용자 풀: Cognito는 다양한 ID 공급자와 통합할 수 있으며, Microsoft Active Directory를 지원하는 연합 ID 공급자를 설정할 수 있습니다.
연합(federated) ID 공급자 설정: 디렉토리의 메타데이터를 사용하여 Cognito 사용자 풀을 연합 ID 공급자로 설정합니다.
ALB와 통합: ALB의 리스너 규칙을 설정하여 Cognito를 사용한 인증을 처리합니다. 이는 사용자의 인증을 중앙 집중화하고 관리하기 쉽게 만듭니다.
이 접근 방식은 Microsoft Active Directory와의 통합을 지원하고, ALB를 통해 안전하게 인증을 처리할 수 있도록 합니다.

◆ | **Q#0372.** | **Ref#0372.**
한 회사에 많은 방문자에게 서비스를 제공하는 웹사이트가 있습니다. 회사는 기본 AWS 지역과 재해 복구(DR) 지역에 웹사이트용 백엔드 서비스를 배포합니다.

단일 Amazon CloudFront 배포가 웹 사이트에 배포됩니다. 회사는 기본 지역의 백엔드 서비스에 대한 상태 확인 및 장애 조치 라우팅 정책이 포함된 Amazon Route 53 레코드 세트를 생성합니다. 회사는 Route 53 레코드 세트를 CloudFront 배포의 오리진으로 구성합니다. 회사는 DR 지역의 백엔드 서비스 엔드포인트를 가리키는 다른 레코드 세트를 보조 장애 조치 레코드 유형으로 구성합니다. 두 레코드 세트 모두의 TTL은 60초입니다.

현재 장애 조치에는 1분 이상 소요됩니다. 솔루션 설계자는 가장 빠른 장애 조치 시간을 제공하는 솔루션을 설계해야 합니다.

이 목표를 달성할 솔루션은 무엇입니까?

> **A.** 추가 CloudFront 배포를 배포합니다. 두 CloudFront 배포 모두에 대한 상태 확인이 포함된 새로운 Route 53 장애 조치 레코드 세트를 생성합니다.
> **B.** 각 지역의 백엔드 서비스에 사용되는 기존 Route 53 레코드 세트에 대해 TTL을 4초로 설정합니다.
> **C.** 대기 시간 라우팅 정책을 사용하여 백엔드 서비스에 대한 새 레코드 세트를 생성합니다. CloudFront 배포에서 레코드 세트를 오리진으로 사용합니다.
> **D.** 각 백엔드 서비스 지역에 하나씩, 두 개의 오리진을 포함하는 CloudFront 오리진 그룹을 생성합니다. CloudFront 배포에 대한 캐시 동작으로 오리진 장애 조치를 구성합니다.
>
> 해설
> 정답:D
>
> D는 가장 빠른 장애 조치 시간을 제공할 수 있는 솔루션
> CloudFront 오리진 그룹: 오리진 그룹을 사용하면 두 오리진 중 하나가 실패할 경우 CloudFront가 자동으로 대체 오리진으로 전환합니다.
> 캐시 동작으로 오리진 장애 조치를 구성하면 CloudFront는 실패한 오리진에 대한 요청을 감지하고, 즉시 대체 오리진으로 라우팅을 전환. 이는 DNS 레코드의 TTL을 기다릴 필요가 없어 매우 빠른 전환을 보장.
> CloudFront 오리진 그룹을 사용하는 방법은 DNS에 의존하지 않으며 CloudFront의 자체 기능을 통해 즉각적인 장애 조치를 제공

◆ | **Q#0373.** | **Ref#0373.**
회사는 여러 AWS 계정을 사용하고 있으며 이러한 계정에서 프로덕션 및 비프로덕션 워크로드를 실행하는 여러 DevOps 팀을 보유하고 있습니다. 회사는 DevOps 팀이 사용하지 않는 일부 AWS 서비스에 대한 액세스를 중앙에서 제한하려고 합니다. 회사는 AWS Organizations를 사용하기로 결정하고 모든 AWS 계정을 조직에 성공적으로 초대했습니다. 그들은 현재 사용 중인 서비스에 대한 액세스를 허용하고 몇 가지 특정 서비스를 거부하려고 합니다. 또한 여러 계정을 하나의 단위로 함께 관리하려고 합니다.

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

> **A.** 거부 목록 전략을 사용하십시오.
> **B.** AWS IAM의 Access Advisor를 검토하여 최근에 사용된 서비스를 확인합니다.
> **C.** AWS Trusted Advisor 보고서를 검토하여 최근에 사용한 서비스를 확인합니다.
> **D.** 기본 FullAWSAccess SCP를 제거합니다.
> **E.** OU(조직 단위)를 정의하고 OU에 구성원 계정을 배치합니다.
> **F.** 기본 DenyAWSAccess SCP를 제거합니다.
>
> 해설
> 정답:ABE

중앙에서 특정 AWS 서비스에 대한 액세스를 제한하고, 여러 계정을 하나의 단위로 관리하고자 할 때는

A: Deny 리스트 전략 사용: 특정 서비스에 대한 접근을 제한하려면 명시적으로 Deny 정책을 사용하라.
B: AWS IAM의 Access Advisor를 검토하여 최근 사용된 서비스 확인: Access Advisor는 각 IAM 역할이나 사용자에 의해 어떤 서비스가 실제로 사용되고 있는지 파악가능.
E: 조직 단위(OUs)를 정의하고 구성원 계정을 OUs에 배치: AWS Organizations에서 조직 단위로 계정을 그룹화하여 비슷한 보안 요구 사항을 가진 계정을 함께 관리.
D(x): 기본 FullAWSAccess SCP를 제거하는 것은 전체 계정에 대한 접근을 차단할 수 있으므로 부적절함.
F(x): 기본 DenyAWSAccess SCP를 제거하는 것은 조직에서 Deny 정책을 효과적으로 사용할 수 없게 함.
C(x): Trusted Advisor 보고서는 비용 최적화, 보안 권장 사항 등을 제공하지만, 최근 사용된 서비스 정보는 제공하지 않음.

◆ | **Q#0374.** | **Ref#0374.**
한 라이브 이벤트 회사가 AWS에서 티켓 신청을 위한 확장 솔루션을 설계하고 있습니다. 이 애플리케이션은 세일 이벤트 기간 동안 활용도가 가장 높습니다. 각 판매 이벤트는 예정된 일회성 이벤트입니다. 애플리케이션은 Auto Scaling 그룹에 있는 Amazon EC2 인스턴스에서 실행됩니다. 애플리케이션은 데이터베이스 계층으로 PostgreSQL을 사용합니다.

회사는 세일 이벤트 중 가용성을 최대화하기 위해 확장 솔루션이 필요합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. EC2 인스턴스에 예측 확장 정책을 사용하십시오. 읽기 전용 복제본을 자동으로 확장하여 Amazon Aurora PostgreSQL Serverless v2 다중 AZ DB 인스턴스에서 데이터베이스를 호스팅합니다. AWS Step Functions 상태 시스템을 생성하여 병렬 AWS Lambda 함수를 실행하여 판매 이벤트 전에 데이터베이스를 미리 예열하세요. 상태 시스템을 호출하는 Amazon EventBridge 규칙을 생성합니다.
B. EC2 인스턴스에 대해 예약된 확장 정책을 사용합니다. 읽기 전용 복제본을 자동으로 확장하여 PostgreSQL Mulli-AZ DB 인스턴스용 Amazon RDS에서 데이터베이스를 호스팅합니다. 판매 이벤트 전에 더 큰 읽기 전용 복제본을 생성하기 위해 AWS Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. 더 큰 읽기 전용 복제본으로 장애 조치합니다. 판매 이벤트 후 읽기 전용 복제본을 축소하기 위해 다른 Lambda 함수를 호출하는 또 다른 EventBridge 규칙을 생성합니다.
C. EC2 인스턴스에 예측 확장 정책을 사용합니다. 읽기 전용 복제본을 자동으로 확장하여 PostgreSQL MultiAZ DB 인스턴스용 Amazon RDS에서 데이터베이스를 호스팅합니다. AWS Step Functions 상태 시스템을 생성하여 병렬 AWS Lambda 함수를 실행하여 판매 이벤트 전에 데이터베이스를 미리 예열하세요. 상태 시스템을 호출하는 Amazon EventBridge 규칙을 생성합니다.
D. EC2 인스턴스에 대해 예약된 확장 정책을 사용합니다. Amazon Aurora PostgreSQL 다중 AZ DB 클러스터에서 데이터베이스를 호스팅합니다. 판매 이벤트 전에 AWS Lambda 함수를 호출하여 더 큰 Aurora 복제본을 생성하는 Amazon EventBridge 규칙을 생성합니다. 더 큰 Aurora 복제본으로 장애 조치합니다. 판매 이벤트 후 Aurora 복제본을 축소하기 위해 다른 Lambda 함수를 호출하는 또 다른 EventBridge 규칙을 생성합니다.

해설
정답:D
1. 예약된 확장 정책: 높은 트래픽 이벤트가 예측 가능한 경우에 최적. 이를 통해 이벤트 전에 대량 트래픽을 감당할 수 있도록 EC2 인스턴스를 미리 확장하고 이벤트 후에 축소가능.
2. Amazon Aurora PostgreSQL: 이는 고성능 데이터베이스 솔루션이며, 이러한 중요한 작업에 필요한 신뢰성을 제공.

3. Aurora 복제본의 활용: 이벤트 동안 더 큰 Aurora 복제본을 사용하고 이후에 축소함으로써, 자원 이용의 효율성을 높일 수 있음.

◆ | **Q#0375.** | **Ref#0375.**
회사는 온프레미스에서 인트라넷 애플리케이션을 실행합니다. 회사는 애플리케이션의 클라우드 백업을 구성하려고 합니다. 회사는 이 솔루션을 위해 AWS Elastic Disaster Recovery를 선택했습니다.

회사에서는 복제 트래픽이 공용 인터넷을 통해 이동하지 않도록 요구합니다. 또한 인터넷에서 애플리케이션에 액세스할 수 없어야 합니다. 다른 응용 프로그램에는 대역폭이 필요하기 때문에 회사는 이 솔루션이 사용 가능한 모든 네트워크 대역폭을 소비하는 것을 원하지 않습니다.

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

A. 최소 2개의 프라이빗 서브넷, 2개의 NAT 게이트웨이 및 1개의 가상 프라이빗 게이트웨이가 있는 VPC를 생성합니다.
B. 2개 이상의 퍼블릭 서브넷, 가상 프라이빗 게이트웨이 및 인터넷 게이트웨이가 있는 VPC를 생성합니다.
C. 온프레미스 네트워크와 대상 AWS 네트워크 간에 AWS Site-to-Site VPN 연결을 생성합니다.
D. 온프레미스 네트워크와 대상 AWS 네트워크 사이에 AWS Direct Connect 연결과 Direct Connect 게이트웨이를 생성합니다.
E. 복제 서버 구성 시 데이터 복제를 위해 개인 IP 주소를 사용하는 옵션을 선택합니다.
F. 대상 서버의 시작 설정을 구성하는 동안 복구 인스턴스의 개인 IP 주소가 원본 서버의 개인 IP 주소와 일치하는지 확인하는 옵션을 선택합니다.

해설
정답:ADE

A: 프라이빗 서브넷을 사용하여 애플리케이션이 인터넷에 노출되지 않도록 보장. NAT 게이트웨이를 통해 프라이빗 서브넷의 리소스가 아웃바운드 인터넷 트래픽을 가질 수 있게 함.
가상 프라이빗 게이트웨이를 통해 온프레미스 네트워크와 안전하게 연결.
D: Direct Connect는 고속의 전용 연결을 제공, 공용 인터넷을 사용하지 않으므로 보안과 신뢰성을 높임. Direct Connect 게이트웨이를 통해 여러 VPC와 연결.
E: 개인 IP 주소를 사용하여 복제 트래픽이 공용 인터넷을 통하지 않고 프라이빗 네트워크를 통해 전송되도록 보장.

◆ | **Q#0376.** | **Ref#0376.**
이미지 스토리지 서비스를 제공하는 회사가 고객용 솔루션을 AWS에 배포하려고 합니다. 수백만 명의 개인 고객이 이 솔루션을 사용할 것입니다. 이 솔루션은 대용량 이미지 파일 배치를 수신하고, 파일 크기를 조정하고, 최대 6개월 동안 Amazon S3 버킷에 파일을 저장합니다.

솔루션은 수요의 상당한 변화를 처리해야 합니다. 또한 솔루션은 기업 규모에서 안정적이어야 하며 오류 발생 시 처리 작업을 다시 실행할 수 있는 기능도 갖추고 있어야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. AWS Step Functions를 사용하여 사용자가 이미지를 저장할 때 발생하는 S3 이벤트를 처리합니다. 이미지의 크기를 조정하고 S3 버킷의 원본 파일을 바꾸는 AWS Lambda 함수를 실행합니다. 6개월 후에 저장된 모든 이미지가 만료되도록 S3 수명 주기 만료 정책을 생성합니다.
B. Amazon EventBridge를 사용하여 사용자가 이미지를 업로드할 때 발생하는 S3 이벤트를 처리합니다. 이미지의 크기를 조정하고 S3 버킷의 원본 파일을 바꾸는 AWS Lambda 함수를 실행합니다. 6개월 후에 저장된 모든 이미지가 만료되도록 S3 수명 주기 만료 정책을 생성합니다.
C. 사용자가 이미지를 저장할 때 S3 이벤트 알림을 사용하여 AWS Lambda 함수를 호출합니다. Lambda 함수를 사용하여 이미지 크기를 조정하고 S3 버킷에 원본 파일을 저장합니다. 6개월 후에 저장된 모든 이미지를 S3 Standard-Infrequent Access(S3 Standard-IA)로 이동하는 S3 수명 주기 정

책을 생성합니다.
D. Amazon Simple Queue Service(Amazon SQS)를 사용하여 사용자가 이미지를 저장할 때 발생하는 S3 이벤트를 처리합니다. 이미지 크기를 조정하고 S3 Standard-Infrequent Access(S3 Standard-IA)를 사용하는 S3 버킷에 크기 조정된 파일을 저장하는 AWS Lambda 함수를 실행합니다. 6개월 후에 저장된 모든 이미지를 S3 Glacier Deep Archive로 이동하는 S3 수명 주기 정책을 생성합니다.

해설
정답: B

AWS Lambda 및 S3 수명 주기 만료 정책이 포함된 Amazon EventBridge (B): 가장 비용 효율적이고 적절한 솔루션.
이는 이미지 처리를 위한 AWS Lambda의 확장성과 유연성을 Amazon EventBridge의 간단한 이벤트 처리와 결합하고 S3 만료 정책을 통해 이미지 수명 주기를 적절하게 관리.
A(x): Step Function 사용은 복잡성과 비용이 증가함.
D(x): 불필요한 장기 보관 단계가 포함되어 있음.

◆ | **Q#0377.** | **Ref#0377.**
회사에는 회사의 각 부서에 대한 별도의 AWS 계정을 포함하는 AWS Organizations에 조직이 있습니다. 다양한 부서의 애플리케이션 팀이 독립적으로 솔루션을 개발하고 배포합니다.

회사는 컴퓨팅 비용을 줄이고 부서 전체에서 비용을 적절하게 관리하기를 원합니다. 또한 회사는 개별 부서의 청구에 대한 가시성을 향상하고자 합니다. 회사는 컴퓨팅 리소스를 선택할 때 운영 유연성을 잃고 싶지 않습니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 각 부서에 AWS 예산을 사용하십시오. 태그 편집기를 사용하여 적절한 리소스에 태그를 적용합니다. EC2 Instance Savings Plan을 구매하세요.
B. 통합 결제를 사용하도록 AWS Organizations를 구성합니다. 부서를 식별하는 태그 지정 전략을 구현합니다. SCP를 사용하여 적절한 리소스에 태그를 적용합니다. EC2 Instance Savings Plan을 구매하세요.
C. 통합 결제를 사용하도록 AWS Organizations를 구성합니다. 부서를 식별하는 태그 지정 전략을 구현합니다. 태그 편집기를 사용하여 적절한 리소스에 태그를 적용합니다. Compute Savings Plan을 구매하세요.
D. 각 부서에 AWS 예산을 사용합니다. SCP를 사용하여 적절한 리소스에 태그를 적용합니다. Compute Savings Plan을 구매하세요.

해설
정답:C
A: 통합 청구가 부족하여 비용 가시성과 할인 가능성이 제한됩니다
B: SCP는 주로 태그 적용이 아닌 규정 준수 시행을 위한 것입니다.
D: 비용 가시성 및 관리 측면에서 통합 청구의 이점을 놓칩니다.

◆ | **Q#0378.** | **Ref#0378.**
한 회사에 사진과 비디오를 Amazon S3 버킷에 안전하게 업로드하는 웹 애플리케이션이 있습니다. 회사는 인증된 사용자만이 콘텐츠를 게시할 수 있도록 요구하고 있습니다. 애플리케이션은 브라우저 인터페이스를 통해 객체를 업로드하는 데 사용되는 미리 서명된 URL을 생성합니다. 대부분의 사용자는 100MB보다 큰 개체의 업로드 시간이 느리다고 보고합니다.

인증된 사용자만 콘텐츠를 게시할 수 있도록 허용하면서 이러한 업로드 성능을 향상시키기 위해 솔루션 설계자는 무엇을 할 수 있습니까?

A. S3 서비스 프록시로 리소스가 있는 엣지 최적화 API 엔드포인트를 사용하여 Amazon API Gateway를 설정합니다. S3 PutObject 작업을 노출하려면 이 리소스에 대한 PUT 메서드를 구성하십시오. COGNITO_USER_POOLS 권한 부여자를 사용하여 API 게이트웨이를 보호합니다. 브라우저 인

터페이스에서 미리 서명된 URL 대신 API 게이트웨이를 사용하여 객체를 업로드하도록 합니다.
B. S3 서비스 프록시로 리소스가 있는 지역 API 엔드포인트를 사용하여 Amazon API Gateway를 설정합니다. S3 PutObject 작업을 노출하려면 이 리소스에 대한 PUT 메서드를 구성하십시오. AWS Lambda 권한 부여자를 사용하여 API 게이트웨이를 보호합니다. 브라우저 인터페이스에서 미리 서명된 URL 대신 API 게이트웨이를 사용하여 객체를 업로드하도록 합니다.
C. S3 버킷에서 S3 Transfer Acceleration 엔드포인트를 활성화합니다. 미리 서명된 URL을 생성할 때 엔드포인트를 사용하세요. 브라우저 인터페이스가 S3 멀티파트 업로드 API를 사용하여 객체를 이 URL에 업로드하도록 합니다.
D. 대상 S3 버킷에 대한 Amazon CloudFront 배포를 구성합니다. CloudFront 캐시 동작에 대해 PUT 및 POST 메서드를 활성화합니다. OAI(원본 액세스 ID)를 사용하도록 CloudFront 오리진을 업데이트합니다. 버킷 정책에서 OAI 사용자에게 3: PutObject 권한을 부여합니다. CloudFront 배포를 사용하여 브라우저 인터페이스에서 객체를 업로드하도록 합니다.

해설
정답:C
S3 Transfer Acceleration은 S3 버킷으로의 큰 파일 업로드 속도를 대폭 향상시키는 기능입니다. Transfer Acceleration을 사용하려면 미리 서명된 URL을 생성할 때 Transfer Acceleration 엔드포인트를 사용해야 합니다.

◆ | **Q#0379.** | **Ref#0379.**
한 대기업이 전체 IT 포트폴리오를 AWS로 마이그레이션하고 있습니다. 회사의 각 사업부에는 개발 및 테스트 환경을 모두 지원하는 독립형 AWS 계정이 있습니다. 프로덕션 워크로드를 지원하기 위한 새로운 계정이 곧 필요할 것입니다.

재무 부서에는 중앙 집중식 결제 방법이 필요하지만 비용을 할당하기 위해 각 그룹의 지출에 대한 가시성을 유지해야 합니다.

보안 팀에는 회사의 모든 계정에서 IAM 사용을 제어하기 위한 중앙 집중식 메커니즘이 필요합니다.

다음 옵션의 어떤 조합이 최소한의 노력으로 회사의 요구 사항을 충족합니까? (2개를 선택하세요.)

A. 각 계정으로 시작되는 공통 IAM 권한을 정의하는 매개변수화된 AWS CloudFormation 템플릿 모음을 사용하십시오. 최소 권한 모델을 시행하려면 모든 신규 및 기존 계정에서 적절한 스택을 시작해야 합니다.
B. AWS Organizations를 사용하여 선택한 지불자 계정에서 새 조직을 생성하고 조직 단위 계층 구조를 정의합니다. 기존 계정을 조직에 초대하고 조직을 사용하여 새 계정을 만듭니다.
C. 각 사업부가 자체 AWS 계정을 사용하도록 요구합니다. 각 AWS 계정에 적절하게 태그를 지정하고 비용 탐색기를 활성화하여 지불 거절을 관리합니다.
D. AWS Organizations의 모든 기능을 활성화하고 하위 계정에 대한 IAM 권한을 필터링하는 적절한 서비스 제어 정책을 설정합니다.
E. 회사의 모든 AWS 계정을 단일 AWS 계정으로 통합합니다. 청구 목적으로 태그를 사용하고 IAM의 액세스 관리자 기능을 사용하여 최소 권한 모델을 시행합니다.

해설
정답:BD
B와 D는 재무 부서와 보안 팀의 요구 사항을 모두 충족하는 효율적이고 확장 가능한 중앙 집중식 솔루션을 제공합니다.

◆ | **Q#0380.** | **Ref#0380.**
한 회사에는 수천 개의 기상 관측소에서 수집된 기상 데이터를 분석하는 솔루션이 있습니다. 기상 관측소는 AWS

Lambda 기능이 통합된 Amazon API Gateway REST API를 통해 데이터를 보냅니다. Lambda 함수는 데이터 사전 처리를 위해 타사 서비스를 호출합니다. 타사 서비스가 과부하되어 전처리에 실패하여 데이터가 손실됩니다.

솔루션 아키텍트는 솔루션의 탄력성을 향상해야 합니다. 솔루션 설계자는 데이터가 손실되지 않도록 하고 오류가 발생하면 나중에 데이터를 처리할 수 있는지 확인해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

> **A.** Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. API에 대한 배달 못한 편지 대기열로 대기열을 구성합니다.
> **B.** 두 개의 Amazon Simple Queue Service(Amazon SQS) 대기열(기본 대기열과 보조 대기열)을 생성합니다. 보조 대기열을 기본 대기열의 배달 못한 편지 대기열로 구성합니다. 기본 대기열에 대한 새로운 통합을 사용하도록 API를 업데이트하세요. Lambda 함수를 기본 대기열의 호출 대상으로 구성합니다.
> **C.** 두 개의 Amazon EventBridge 이벤트 버스(기본 이벤트 버스와 보조 이벤트 버스)를 생성합니다. 기본 이벤트 버스에 대한 새로운 통합을 사용하도록 API를 업데이트하세요. 기본 이벤트 버스의 모든 이벤트에 반응하도록 EventBridge 규칙을 구성합니다. Lambda 함수를 규칙의 대상으로 지정합니다. Lambda 함수의 실패 대상으로 보조 이벤트 버스를 구성합니다.
> **D.** 사용자 지정 Amazon EventBridge 이벤트 버스를 생성합니다. 이벤트 버스를 Lambda 함수의 실패 대상으로 구성합니다.
>
> 해설
> 정답:B
> 기본 대기열에서 메시지를 처리하지 못하는 경우에는 보조 대기열(배달 못한 편지 대기열)로 메시지를 전달할 수 있어 데이터 손실을 막을 수 있고, 분석을 나중에 처리할 수 있게 됩니다
> Eventbridge는 API 게이트웨이의 대상이 될 수 없습니다.

381 (백은희) 2회차 完

◆ | **Q#0381.** | **Ref#0381.**
한 회사는 3계층 웹 아키텍처를 사용하여 AWS에 전자상거래 웹사이트를 구축했습니다. 애플리케이션은 Java 기반이며 Amazon CloudFront 배포, Auto Scaling 그룹에 있는 Amazon EC2 인스턴스의 Apache 웹 서버 계층, 백엔드 Amazon Aurora MySQL 데이터베이스로 구성됩니다.

지난 달 프로모션 판매 이벤트 중에 사용자가 장바구니에 항목을 추가하는 동안 오류 및 시간 초과가 발생했다고 보고했습니다. 운영팀은 웹 서버에서 생성된 로그를 복구하고 Aurora DB 클러스터 성능 지표를 검토했습니다. 로그가 수집되기 전에 일부 웹 서버가 종료되었으며 Aurora 지표가 쿼리 성능 분석에 충분하지 않았습니다.

피크 트래픽 이벤트 중에 애플리케이션 성능 가시성을 개선하기 위해 솔루션 설계자가 수행해야 하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

> **A.** Amazon CloudWatch Logs에 느린 쿼리 및 오류 로그를 게시하도록 Aurora MySQL DB 클러스터를 구성하십시오.
> **B.** AWS X-Ray SDK를 구현하여 EC2 인스턴스에서 들어오는 HTTP 요청을 추적하고 Java용 X-Ray SDK를 사용하여 SQL 쿼리 추적을 구현합니다.
> **C.** 느린 쿼리 및 오류 로그를 Amazon Kinesis로 스트리밍하도록 Aurora MySQL DB 클러스터를 구성합니다.
> **D.** EC2 인스턴스에 Amazon CloudWatch Logs 에이전트를 설치하고 구성하여 Apache 로그를 CloudWatch Logs로 보냅니다.
> **E.** Amazon EC2 및 Aurora에서 애플리케이션 활동을 수집하고 분석하도록 AWS CloudTrail을 활성화하고 구성합니다.
> **F.** Aurora MySQL DB 클러스터 성능 벤치마킹을 활성화하고 스트림을 AWS X-Ray에 게시합니다.

해설
정답: A B D
A, 느린 쿼리와 오류 로그를 Amazon CloudWatch Logs에 게시하도록 설정하면, Aurora MySQL DB 클러스터의 성능 문제를 모니터링하고 분석할 수 있습니다. 이를 통해 실시간으로 문제를 식별하고 대응할 수 있습니다.
B, AWS X-Ray를 사용하여 EC2 인스턴스로 들어오는 HTTP 요청과 SQL 쿼리를 추적하면, 애플리케이션의 성능 병목 현상을 식별하고 문제를 해결하는 데 도움이 됩니다. X-Ray SDK를 사용하면 요청 경로를 시각화하고 문제를 신속하게 진단할 수 있습니다.
D, EC2 인스턴스에 Amazon CloudWatch Logs 에이전트를 설치하고 Apache 로그를 CloudWatch Logs로 전송하도록 구성하면, 웹 서버 로그를 중앙에서 모니터링하고 분석할 수 있습니다. 이를 통해 웹 서버가 종료되기 전에 로그를 수집하고 분석할 수 있습니다.

◆ | **Q#0382.** | **Ref#0382.**
계절별 인력을 위한 채용 게시판을 제공하는 회사에서는 트래픽과 사용량이 증가하고 있습니다. 백엔드 서비스는 Application Load Balancer 뒤의 두 Amazon EC2 인스턴스에서 실행되며, Amazon DynamoDB가 데이터 저장소로 사용됩니다. 성수기에는 애플리케이션 읽기 및 쓰기 트래픽이 느립니다.

최소한의 개발 노력으로 성수기를 처리할 수 있는 확장 가능한 애플리케이션 아키텍처를 제공하는 옵션은 무엇입니까?

A. 백엔드 서비스를 AWS Lambda로 마이그레이션합니다. DynamoDB의 읽기 및 쓰기 용량을 늘립니다.
B. 백엔드 서비스를 AWS Lambda로 마이그레이션합니다. 전역 테이블을 사용하도록 DynamoDB를 구성합니다.
C. 백엔드 서비스에 Auto Scaling 그룹을 사용합니다. DynamoDB Auto Scaling을 사용합니다.
D. 백엔드 서비스에 Auto Scaling 그룹을 사용합니다. Amazon Simple Queue Service(Amazon SQS) 및 AWS Lambda 함수를 사용하여 DynamoDB에 씁니다.

해설
정답: C
Auto Scaling groups for the backend services: EC2 인스턴스를 Auto Scaling 그룹으로 설정하면 트래픽 증가에 따라 자동으로 인스턴스 수를 조정하여 확장성을 확보할 수 있습니다. 이는 백엔드 서비스의 성능을 개선하는 데 도움이 됩니다.
DynamoDB auto scaling: DynamoDB 자동 스케일링을 사용하면 테이블의 읽기 및 쓰기 용량이 자동으로 조정되어 트래픽 증가에 대응할 수 있습니다. 이는 DynamoDB의 성능을 자동으로 관리하여 피크 시즌 동안의 느린 읽기 및 쓰기 문제를 해결합니다.
Lambda로 백엔드 서비스를 마이그레이션하는 것은 개발 노력이 많이 들 수 있으며, SQS를 신규구성하는 것은 추가적인 설정이 필요합니다.

◆ | **Q#0383.** | **Ref#0383.**
한 회사가 클라우드로 마이그레이션하고 있습니다. 기존 데이터 센터 환경의 가상 머신 구성을 평가하여 새로운 Amazon EC2 인스턴스의 크기를 정확하게 조정할 수 있는지 확인하려고 합니다. 회사는 CPU, 메모리, 디스크 사용률과 같은 지표를 수집하려고 하며 각 인스턴스에서 실행 중인 프로세스에 대한 인벤토리가 필요합니다. 또한 회사는 네트워크 연결을 모니터링하여 서버 간의 통신을 매핑하려고 합니다.

이 데이터를 가장 비용 효율적으로 수집할 수 있는 방법은 무엇입니까?

A. AWS Application Discovery Service를 사용하고 데이터 센터의 각 가상 머신에 데이터 수집 에이전트(Agent-based)를 배포합니다.
B. 로컬 환경 내의 모든 서버에서 Amazon CloudWatch 에이전트를 구성하고 Amazon CloudWatch Logs에 지표를 게시합니다.
C. AWS Application Discovery Service를 사용하고 기존 가상화 환경에서 에이전트 없는(Agentless) 검색을 활성화합니다.

D. AWS Management Console에서 AWS Application Discovery Service를 활성화하고 VPN을 통한 검색을 허용하도록 회사 방화벽을 구성합니다.

해설
정답: A
AWS Application Discovery Service와 에이전트 기반 디스커버리: AWS Application Discovery Service는 가상 머신의 메트릭과 프로세스 데이터를 수집하는 데 사용될 수 있으며, 네트워크 연결 세부 사항을 수집하기 위해 에이전트 기반 디스커버리를 배포해야 합니다.
비용 효율성: 에이전트 기반 디스커버리는 네트워크 통신을 포함한 다양한 메트릭을 효과적으로 수집할 수 있으며, 추가적인 소프트웨어 설치와 관리가 필요하지만 다른 방법보다 정확한 데이터를 수집할 수 있습니다.
Agentless 디스커버리는 실행 중인 프로세스 데이터와 네트워크 인바운드/아웃바운드 연결 정보를 수집하지 못합니다.

◆ | **Q#0384.** | **Ref#0384.**
회사는 AWS 클라우드에서 실행되는 SaaS(Software as a Service) 애플리케이션을 제공합니다. 애플리케이션은 NLB(Network Load Balancer) 뒤의 Amazon EC2 인스턴스에서 실행됩니다. 인스턴스는 Auto Scaling 그룹에 속하며 단일 AWS 리전의 3개 가용 영역(AZ)에 분산되어있습니다.

회사는 추가 리전에 애플리케이션을 배포하고자 하며, 회사는 고객이 IP 주소를 허용 목록에 추가할 수 있도록 애플리케이션에 대한 고정(Static) IP 주소를 고객에게 제공해야 합니다. 또한, 고객을 지리적으로 가장 가까운 리전으로 자동으로 라우팅해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. Amazon CloudFront 배포판을 생성합니다. CloudFront 오리진 그룹을 생성합니다. 각 추가 지역에 대한 NLB를 원본 그룹에 추가합니다. 고객에게 배포 엣지 위치의 IP 주소 범위를 제공합니다.
B. AWS Global Accelerator Standard Accelerator(표준가속기)를 생성합니다. 각 추가 지역에서 NLB에 대한 Standard Accelerator(표준가속기) 엔드포인트를 생성합니다. 고객에게 Global Accelerator IP 주소를 제공합니다.
C. Amazon CloudFront 배포판을 생성합니다. 각 추가 지역에서 NLB에 대한 사용자 지정 원본을 만듭니다. 고객에게 배포 엣지 위치의 IP 주소 범위를 제공합니다.
D. AWS Global Accelerator Custom Routing Accelerator(사용자 지정 라우팅 가속기)를 생성합니다. 사용자 정의 라우팅 가속기에 대한 수신기를 만듭니다. 각 추가 지역에 NLB에 대한 IP 주소와 포트를 추가합니다. 고객에게 Global Accelerator IP 주소를 제공합니다.

해설
정답: B
솔루션 요구사항 : 정적 IP 주소 제공, 지리적으로 가장 가까운 리전으로 자동 라우팅
AWS Global Accelerator는 정적 IP 주소를 제공하며, 트래픽을 여러 리전에 있는 애플리케이션 엔드포인트로 라우팅하는 글로벌 네트워크 서비스입니다. Global Accelerator를 사용하면 고객에게 제공할 단일 정적 IP 주소를 받을 수 있으며, 이 주소는 고객의 지리적 위치에 따라 가장 가까운 리전으로 트래픽을 라우팅할 수 있습니다.
Standard Accelerator는 여러 리전에 있는 NLB를 엔드포인트로 설정할 수 있습니다. 이렇게 하면 모든 리전의 NLB에 대한 단일 정적 IP 주소를 고객에게 제공할 수 있습니다.
CloudFront는 정적 IP 주소를 제공하지 않으며, Custom Routing Accelerator는 특정 포트와 IP 주소로 트래픽을 라우팅하는 데 사용됩니다.

◆ | **Q#0385.** | **Ref#0385.**
한 회사가 AWS 클라우드에서 여러 워크로드를 실행하고 있습니다. 회사에는 소프트웨어 개발을 위한 별도의 부서가 있습니다. 회사는 AWS Organizations 및 SAML과의 연동을 사용하여 개발자에게 AWS 계정의 리소스를 관리할 수 있는 권한을 부여합니다. 각 개발 부서는 프로덕션 워크로드를 공통 프로덕션 계정에 배포합니다.

최근 프로덕션 계정에서, 한 개발 부서 구성원이 다른 개발 부서에 속한 EC2 인스턴스를 종료하는 사건이 발생했습니다. 솔루션 설계자는 향후 유사한 사고가 발생하지 않도록 방지하는 솔루션을 만들어야 합니다. 또한 솔루션은 개발자 자신들의 워크로드에 사용되는 인스턴스를 관리할 수 있도록해야 합니다.

이러한 요구 사항을 충족하는 전략은 무엇입니까?

> **A.** 각 개발 단위에 대해 AWS Organizations에서 별도의 OU를 생성합니다. 생성된 OU를 회사 AWS 계정에 할당합니다. 개발 단위 이름과 일치하는 DevelopmentUnit 리소스 태그에 대한 거부 작업 및 StringNotEquals 조건을 사용하여 별도의 SCP를 생성합니다. 해당 OU에 SCP를 할당합니다.
> **B.** SAML 연동 중에 DevelopmentUnit의 속성을 AWS Security Token Service(AWS STS) 세션 태그로 전달합니다. DevelopmentUnit 리소스 태그 및 aws:PrincipalTag/DevelopmentUnit에 대한 거부 작업 및 StringNotEquals 조건을 사용하여 개발자가 맡은 IAM 역할에 대한 IAM 정책을 업데이트합니다.
> **C.** SAML 연동 중에 DevelopmentUnit의 속성을 AWS Security Token Service(AWS STS) 세션 태그로 전달합니다. DevelopmentUnit 리소스 태그 및 aws:PrincipalTag/DevelopmentUnit에 대한 허용 작업과 StringEquals 조건을 사용하여 SCP를 생성합니다. SCP를 루트 OU에 할당합니다.
> **D.** 각 개발 단위에 대해 별도의 IAM 정책을 만듭니다. 모든 IAM 정책에 대해 DevelopmentUnit 리소스 태그와 개발 단위 이름에 대한 허용 작업과 StringEquals 조건을 추가합니다. SAML 연동 중에 AWS Security Token Service(AWS STS)를 사용하여 IAM 정책을 할당하고 개발 단위 이름을 가정된 IAM 역할과 일치시킵니다.
>
> 해설
> 정답: B
> DevelopmentUnit 속성을 AWS STS 세션 태그로 전달: 개발자가 SAML 연동을 통해 자신의 IAM 역할을 맡을 때, DevelopmentUnit 속성을 세션 태그로 전달합니다. 이 세션 태그는 사용자가 속한 개발 부서(Unit)의 이름을 전달합니다.
> IAM 정책 업데이트: 개발자가 SAML 연동을 통해 자신의 IAM 역할을 맡을 때, DevelopmentUnit 속성을 세션 태그로 전달합니다. 이 세션 태그는 사용자가 속한 개발 부서(Unit)의 이름을 전달합니다.
> StringNotEquals 조건: StringNotEquals 조건을 사용하여 명시적으로 거부 동작을 설정합니다. 이는 리소스가 개발자의 부서(Unit)에 속하지 않은 경우 어떠한 작업도 거부하도록 합니다.
> B는 세션 태그를 활용하여 세밀한 제어를 IAM 정책 내에서 직접 수행할 수 있도록 하여, 개발자가 자신들의 리소스만 관리하고 다른 유닛의 리소스에는 접근할 수 없도록 합니다.

◆ | **Q#0386.** | **Ref#0386.**
한 엔터프라이즈 회사가 사용자를 위한 인프라 서비스 플랫폼을 구축하고 있습니다. 회사에는 다음과 같은 요구 사항이 있습니다.

• 사용자가 승인되지 않은 서비스를 프로비저닝할 수 없도록 AWS 인프라를 시작할 때 사용자에게 최소 권한 액세스를 제공합니다.
• 중앙 계정을 사용하여 인프라 서비스 생성을 관리합니다.
• AWS Organizations의 여러 계정에 인프라 서비스를 배포하는 기능을 제공합니다.
• 사용자가 시작한 모든 인프라에 태그를 적용하도록 강제하는 기능을 제공합니다.

AWS 서비스를 사용하는 어떤 작업 조합이 이러한 요구 사항을 충족합니까? (3개를 선택하세요.)

> **A.** AWS CloudFormation 템플릿을 사용하여 인프라 서비스를 개발합니다. 중앙 Amazon S3 버킷에 템플릿을 추가하고 S3 버킷 정책에 액세스해야 하는 IAM 역할 또는 사용자를 추가합니다.
> **B.** AWS CloudFormation 템플릿을 사용하여 인프라 서비스를 개발합니다. 중앙 AWS 계정에서 생성된 포트폴리오에 각 템플릿을 AWS Service Catalog 제품으로 업로드합니다. 이러한 포트폴리오를 회사를 위해 생성된 조직 구조와 공유합니다.
> **C.** 사용자 IAM 역할이 AWSCloudFormationFullAccess 및 AmazonS3ReadOnlyAccess 권한을 갖도록 허용합니다. AWS CloudFormation 및 Amazon S3를 제외한 모든 서비스를 거부하려면 AWS 계정 루트 사용자 수준에서 조직 SCP를 추가합니다.

D. 사용자 IAM 역할이 ServiceCatalogEndUserAccess 권한만 갖도록 허용합니다. 자동화 스크립트를 사용하여 중앙 포트폴리오를 로컬 AWS 계정으로 가져오고, TagOption을 복사하고, 사용자 액세스를 할당하고, 런치 제약 조건을 적용합니다.
E. AWS Service Catalog TagOption 라이브러리를 사용하여 회사에서 요구하는 태그 목록을 유지 관리합니다. AWS Service Catalog 제품 또는 포트폴리오에 TagOption을 적용합니다.
F. AWS CloudFormation 리소스 태그 속성을 사용하여 사용자를 위해 생성될 모든 CloudFormation 템플릿에 태그 적용을 적용합니다.

해설
정답: B D E
B : 이 방법은 중앙 관리 계정을 통해 CloudFormation 템플릿을 관리하고, Service Catalog 포트폴리오를 통해 여러 계정에 배포하는 기능을 제공합니다. 이를 통해 중앙 집중식 관리가 가능하고, 서비스 배포가 효율적으로 이루어집니다.
D : 이 방법은 사용자에게 필요한 최소 권한만을 부여하고, 자동화 스크립트를 통해 중앙에서 관리되는 포트폴리오를 각 로컬 계정에 배포하며, 태그 옵션 및 런치 제약 조건을 적용합니다. 이를 통해 권한 관리와 태그 적용을 효과적으로 수행할 수 있습니다.
E : 이 방법은 회사에서 필요한 태그를 중앙에서 관리하고, Service Catalog를 통해 모든 인프라 리소스에 태그를 적용할 수 있게 합니다. 이를 통해 태그 일관성을 유지하고, 정책을 강제할 수 있습니다.

◆ | **Q#0387.** | **Ref#0387.**
회사에서 새로운 웹 애플리케이션을 배포합니다. 설정의 일부로 회사는 Amazon Kinesis Data Firehose를 통해 Amazon S3에 로그인하도록 AWS WAF를 구성합니다. 회사는 Amazon Athena 쿼리를 개발하여 매일 한 번씩 지난 24시간의 AWS WAF 로그 데이터를 반환합니다. 일일 로그 양은 일정하지만, 시간이 지남에 따라 동일한 쿼리가 실행되는 시간이 점점 길어지고 있습니다.

솔루션 설계자는 쿼리 시간이 계속해서 증가하지 않도록 솔루션을 설계해야 합니다. 솔루션은 운영 오버헤드를 최소화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 매일의 AWS WAF 로그를 하나의 로그 파일로 통합하는 AWS Lambda 함수를 생성합니다.
B. 매일 다른 S3 버킷으로 로그를 보내도록 AWS WAF를 구성하여 스캔되는 데이터의 양을 줄입니다.
C. Amazon S3의 데이터를 날짜 및 시간별로 분할하도록 Kinesis Data Firehose 구성을 업데이트합니다. Amazon Redshift용 외부 테이블을 생성합니다. 데이터 소스를 쿼리하도록 Amazon Redshift Spectrum을 구성합니다.
D. 날짜 및 시간별로 데이터를 분할하도록 Kinesis Data Firehose 구성 및 Athena 테이블 정의를 수정합니다. Athena 쿼리를 변경하여 관련 파티션을 조회하도록 합니다.

해설
정답: D
AWS WAF 로그 데이터가 시간에 따라 축적되면서 Athena 쿼리가 처리해야 할 데이터 양이 증가하고, 그 결과 쿼리 시간이 점점 길어지게 됩니다. 데이터를 효과적으로 관리하고 쿼리 시간을 줄이기 위해서는 데이터를 파티셔닝하는 것이 좋습니다. 이는 Athena가 전체 데이터 세트를 스캔하는 대신 필요한 파티션만 스캔하도록 하기 때문에 쿼리 성능을 크게 향상시킬 수 있습니다.

◆ | **Q#0388.** | **Ref#0388.**
한 회사는 퍼블릭 ALB(Application Load Balancer) 뒤에 있는 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 실행되는 웹 애플리케이션을 개발하고 있습니다. 특정 국가의 사용자만 애플리케이션에 액세스할 수 있어야 합니다. 회사에는 차단된 액세스 요청을 기록하는 기능이 필요합니다. 솔루션에는 최소한의 유지 관리만 필요합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

> **A.** 지정된 국가에 속하는 IP 범위 목록을 포함하는 IPSet을 생성합니다. AWS WAF 웹 ACL을 생성합니다. IPSet의 IP 범위에서 발생하지 않는 요청을 차단하는 규칙을 구성합니다. 규칙을 웹 ACL과 연결합니다. 웹 ACL을 ALB와 연결합니다.
> **B.** AWS WAF 웹 ACL을 생성합니다. 지정된 국가에서 발생하지 않는 요청을 차단하는 규칙을 구성합니다. 규칙을 웹 ACL과 연결합니다. 웹 ACL을 ALB와 연결합니다.
> **C.** 지정된 국가에서 발생하지 않는 요청을 차단하도록 AWS Shield를 구성합니다. AWS Shield를 ALB와 연결합니다.
> **D.** 지정된 국가에 속한 IP 범위에서 포트 80 및 443을 허용하는 보안 그룹 규칙을 생성합니다. 보안 그룹을 ALB와 연결합니다.
>
> 해설
> 정답: B
> AWS WAF(웹 애플리케이션 방화벽)의 GeoMatch 조건 기능 : GeoMatch 조건은 IP 주소의 지리적 위치에 따라 요청을 차단하거나 허용하는 데 사용됩니다. Country: 특정 국가의 IP 주소에서 오는 요청을 식별합니다. GeoMatch: 특정 대륙, 국가 또는 지역에서 오는 요청을 식별합니다.
> 지정된 국가에 속하는 IP 범위 목록의 IPSet을 생성할 필요가 없습니다.
> AWS Shield는 DDoS 공격 등을 방어하기 위한 서비스입니다.

◆ | **Q#0389.** | **Ref#0389.**
한 회사가 온프레미스 인프라에서 AWS 클라우드로 애플리케이션을 마이그레이션하고 있습니다. 마이그레이션 설계 회의에서 회사는 레거시 Windows 파일 서버의 가용성 및 복구 옵션에 대한 우려를 표명했습니다. 파일 서버에는 데이터 손상이나 데이터 손실 시 다시 생성할 수 없는 중요한 비즈니스 크리티컬 데이터가 포함되어 있습니다. 규정 준수 요구 사항에 따라 데이터는 공용 인터넷을 통해 이동해서는 안 됩니다. 회사는 가능한 경우 AWS 관리형 서비스로 전환하려고 합니다.

회사는 Amazon FSx for Windows File Server 파일 시스템에 데이터를 저장하기로 결정했습니다. 솔루션 아키텍트는 재해 복구(DR) 목적으로 데이터를 다른 AWS 리전에 복사하는 솔루션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

> **A.** DR 지역에 대상 Amazon S3 버킷을 생성합니다. Amazon FSx 파일 게이트웨이를 사용하여 기본 지역의 FSx for Windows File Server 파일 시스템과 DR 지역의 S3 버킷 간에 연결을 설정합니다. FSx 파일 게이트웨이에서 S3 버킷을 연속 백업 소스로 구성합니다.
> **B.** DR 지역에 FSx for Windows File Server 파일 시스템을 생성합니다. AWS Site-to-Site VPN을 사용하여 기본 리전인 VPC와 DR 리전의 VPC 간에 연결을 설정합니다. VPN 엔드포인트를 사용하여 통신하도록 AWS DataSync를 구성합니다.
> **C.** DR 지역에 FSx for Windows File Server 파일 시스템을 생성합니다. VPC 피어링을 사용하여 기본 지역의 VPC와 DR 지역의 VPC 간의 연결을 설정합니다. AWS PrivateLink와 인터페이스 VPC 엔드포인트를 사용하여 통신하도록 AWS DataSync를 구성합니다.
> **D.** DR 지역에 FSx for Windows File Server 파일 시스템을 생성합니다. 각 리전의 AWS Transit Gateway를 사용하여 기본 리전의 VPC와 DR 리전의 VPC 간의 연결을 설정합니다. AWS Transfer Family를 사용하여 프라이빗 AWS 백본 네트워크를 통해 기본 지역의 FSx for Windows File Server 파일 시스템과 DR 지역의 FSx for Windows File Server 파일 시스템 간에 파일을 복사합니다.
>
> 해설
> 정답: C
> VPC 피어링과 AWS PrivateLink를 사용하여 AWS DataSync를 구성하는 것은 높은 보안과 효율적인 데이터 전송을 제공합니다. VPC 피어링은 간단하게 리전 간 VPC 연결을 설정할 수 있고, PrivateLink는 데이터가 공용 인터넷을 거치지 않도록 보장합니다.
> AWS DataSync는 데이터를 자동화된 방식으로 클라우드로 이동하거나 클라우드 간에 이동할 수 있는 데이터 전송 서비스입니다. DataSync는 대용량 데이터를 신속하게 전송할 수 있으며, 데이터 검

증과 암호화를 통해 전송 중 데이터 무결성과 보안을 보장합니다.

◆ | **Q#0390.** | **Ref#0390.**
한 회사는 현재 복구 목표 지점(RPO)이 5분 미만이고 복구 목표 시간(RTO)이 10분 미만인 애플리케이션의 설계 단계에 있습니다. 솔루션 아키텍처 팀은 데이터베이스가 약 10TB의 데이터를 저장할 것으로 예상하고 있습니다. 설계의 일환으로 그들은 회사에 보조 리전으로 장애 조치(Failover)할 수 있는 기능을 제공할 데이터베이스 솔루션을 찾고 있습니다.

가장 저렴한 비용으로 이러한 비즈니스 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A. Amazon Aurora DB 클러스터를 배포하고 5분마다 클러스터의 스냅샷을 찍습니다. 스냅샷이 완료되면 스냅샷을 보조 리전에 복사하여 장애 발생 시 백업으로 사용하세요.
B. 보조 리전에 교차 리전 읽기 전용 복제본이 있는 Amazon RDS 인스턴스를 배포합니다. 오류가 발생하면 읽기 전용 복제본을 기본(Primary) 복제본으로 승격하세요.
C. 기본 리전에 Amazon Aurora DB 클러스터를 배포하고 보조 리전에 또 다른 클러스터를 배포합니다. AWS DMS를 사용하여 보조 리전을 동기화 상태로 유지하세요.
D. 동일한 리전에 읽기 전용 복제본이 있는 Amazon RDS 인스턴스를 배포합니다. 오류가 발생하면 읽기 전용 복제본을 기본 복제본으로 승격하세요.

해설
정답: B
읽기 복제본을 주(primary)로 승격하면 신속한 장애 복구가 가능합니다. 읽기 복제본은 실시간으로 데이터를 복제하므로 RPO가 5분 미만입니다.
동일한 리전에 구성할 경우, RPO/RTO는 충족할 수 있으나 지리적 재해에 대비할 수 없습니다.

391 (김지형) 2회차 完

◆ | **Q#0391.** | **Ref#0391.**
금융 회사는 새로운 디지털 지갑 애플리케이션을 위해 별도의 AWS 계정을 생성해야 합니다. 회사는 AWS Organizations를 사용하여 계정을 관리합니다. 솔루션 아키텍트는 마스터 계정의 IAM 사용자 Support1을 사용하여 이메일 주소가 Finance1@example.com인 새 멤버 계정을 생성합니다.

새 멤버 계정에 IAM 사용자를 생성하려면 솔루션 아키텍트가 무엇을 해야 합니까?

A. Finance1@example.com으로 전송된 초기 AWS Organizations 이메일의 64자 암호를 사용하여 AWS 계정 루트 사용자 자격 증명으로 AWS Management Console에 로그인합니다. 필요에 따라 IAM 사용자를 설정합니다.
B. 마스터 계정에서 역할을 전환하여 새 회원 계정의 계정 ID로 OrganizationAccountAccessRole 역할을 맡습니다. 필요에 따라 IAM 사용자를 설정합니다.
C. AWS Management Console 로그인 페이지로 이동합니다. "루트 계정 자격 증명을 사용하여 로그인"을 선택하십시오. 이메일 주소 Finance 1@example.com과 마스터 계정의 루트 비밀번호를 사용하여 로그인하세요. 필요에 따라 IAM 사용자를 설정합니다.
D. AWS Management Console 로그인 페이지로 이동합니다. 새 회원 계정의 계정 ID와 Support1 IAM 자격 증명을 사용하여 로그인합니다. 필요에 따라 IAM 사용자를 설정합니다.

해설
정답: B
AWS에서 새 멤버 계정을 만들 때, AWS Organizations는 자동으로
'OrganizationAccountAccessRole'이라는 IAM 역할을 해당 계정에 생성합니다.
이 역할은 새 멤버 계정에 대한 전체 관리 권한을 갖습니다.
따라서 옵션에서와 같이 관리 계정에서 이 역할을 임의로 설정하여 새 멤버 계정의 IAM 사용자를

설정하는 것은 가능합니다.
이는 루트 계정의 자격 증명 공유 없이 멤버 계정에 대한 일시적이지만 제어 가능한 액세스를 제공하므로 보안을 강화하고 관리 오버헤드를 줄일 수 있습니다.

◆ | **Q#0392.** | **Ref#0392.**
자동차 렌탈 회사는 모바일 앱에 데이터를 제공하기 위해 서버리스 REST API를 구축했습니다. 이 앱은 지역 엔드포인트가 있는 Amazon API Gateway API, AWS Lambda 함수, Amazon Aurora MySQL 서버리스 DB 클러스터로 구성됩니다. 회사는 최근 파트너사의 모바일 앱에 API를 오픈했습니다. 요청 수가 크게 증가하여 산발적인 데이터베이스 메모리 오류가 발생했습니다.

API 트래픽 분석에 따르면 클라이언트는 짧은 시간 내에 동일한 쿼리에 대해 여러 HTTP GET 요청을 하고 있는 것으로 나타났습니다. 업무 시간 동안 트래픽이 집중되며 휴일 및 기타 행사 기간에는 트래픽이 급증합니다.

회사는 솔루션과 관련된 비용 증가를 최소화하면서 추가 사용량을 지원하는 능력을 향상해야 합니다.

이러한 요구 사항을 충족하는 전략은 무엇입니까?

A. API Gateway 지역 엔드포인트를 엣지 최적화 엔드포인트로 변환합니다. 프로덕션 단계에서 캐싱을 활성화합니다.
B. Redis 캐시용 Amazon ElastiCache를 구현하여 데이터베이스 호출 결과를 저장합니다. 캐시를 사용하도록 Lambda 함수를 수정합니다.
C. Aurora Serverless DB 클러스터 구성을 수정하여 사용 가능한 최대 메모리 양을 늘립니다.
D. API Gateway 프로덕션 단계에서 조절을 활성화합니다. 수신 통화를 제한하려면 속도와 버스트 값을 설정하세요.

해설
정답: A
과도한 요청으로 인해 데이터베이스 메모리에 문제가 발생하고, 주로 "동일한 쿼리에 대한 여러 HTTP GET 요청"이 문제를 일으키고 있다고 합니다.
캐싱 기능을 사용하면, 동일한 쿼리에 대한 결과를 메모리에 저장해두고 필요할 때마다 바로 제공함으로써 데이터베이스의 부담을 크게 줄일 수 있습니다.
A에서 제안하는 전략은 API Gateway에서 캐싱을 활성화하고, Regional endpoint를 edge-optimized endpoint로 변환하는 것입니다.
edge-optimized API는 API Gateway가 클라이언트에게 가장 가까운 CloudFront edge location에서 API 요청을 받고 응답하도록 허용하므로 사용자의 요청이 실제 API가 배포된 리전까지 도달하는 것을 막아줍니다.
아마존 API Gateway 캐싱 기능이 캐시 대상으로 설정된 항목을 요청할 때 Lambda 호출 수를 줄여 비용을 절약하는 효과도 있습니다.

◆ | **Q#0393.** | **Ref#0393.**
한 회사가 온프레미스 애플리케이션과 MySQL 데이터베이스를 AWS로 마이그레이션하고 있습니다. 애플리케이션은 매우 민감한 데이터를 처리하며 데이터베이스에 새로운 데이터가 지속적으로 업데이트됩니다. 데이터는 인터넷을 통해 전송되어서는 안 됩니다. 또한 회사는 전송 중인 데이터와 저장 중인 데이터를 암호화해야 합니다.

데이터베이스 크기는 5TB입니다. 회사는 이미 MySQL DB 인스턴스용 Amazon RDS에 데이터베이스 스키마를 생성했습니다. 회사는 AWS에 1Gbps AWS Direct Connect 연결을 설정했습니다. 회사는 또한 공개 VIF와 비공개 VIF를 설정했습니다. 솔루션 아키텍트는 가동 중지 시간을 최소화하면서 데이터를 AWS로 마이그레이션하는 솔루션을 설계해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 데이터베이스 백업을 수행하십시오. 백업 파일을 AWS Snowball Edge Storage Optimized 디바이스에 복사합니다. 백업을 Amazon S3로 가져옵니다. 유휴 암호화에는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화를 사용합니다. 전송 중 암호화에는 TLS를 사용합니다. Amazon S3에서 DB 인스턴스로 데이터를 가져옵니다.

B. AWS Database Migration Service(AWS DMS)를 사용하여 데이터를 AWS로 마이그레이션합니다. 프라이빗 서브넷에 DMS 복제 인스턴스를 생성합니다. AWS DMS용 VPC 엔드포인트를 생성합니다. 전체 로드와 변경 데이터 캡처(CDC)를 사용하여 온프레미스 데이터베이스에서 DB 인스턴스로 데이터를 복사하도록 DMS 작업을 구성합니다. 유휴 암호화에는 AWS Key Management Service(AWS KMS) 기본 키를 사용합니다. 전송 중 암호화에는 TLS를 사용합니다.
C. 데이터베이스 백업을 수행합니다. AWS DataSync를 사용하여 백업 파일을 Amazon S3로 전송합니다. 유휴 암호화에는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화를 사용합니다. 전송 중 암호화에는 TLS를 사용합니다. Amazon S3에서 DB 인스턴스로 데이터를 가져옵니다.
D. Amazon S3 파일 게이트웨이를 사용하십시오. AWS PrivateLink를 사용하여 Amazon S3에 대한 비공개 연결을 설정합니다. 데이터베이스 백업을 수행합니다. 백업 파일을 Amazon S3에 복사합니다. 유휴 암호화에는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화를 사용합니다. 전송 중 암호화에는 TLS를 사용합니다. Amazon S3에서 DB 인스턴스로 데이터를 가져옵니다.

해설
정답: B
AWS DMS는 완전한 로드와 CDC 방법을 사용하여 데이터를 마이그레이션하는 것을 지원하기 때문에 크고 끊임없이 변하는 데이터베이스를 마이그레이션하는 데 적합합니다.
이 솔루션은 소스 데이터베이스와 대상 데이터베이스 간에 지속적인 동기화를 유지합니다. AWS Key Management Service와 TLS는 요구되는 암호화를 안식시키고 전송합니다.
AWS DMS를 위한 VPC 엔드포인트는 데이터가 인터넷을 통해 전송되는 것을 방지하여 회사의 보안 요구 사항을 충족시킵니다.

◆ | **Q#0394.** | **Ref#0394.**
Accompany는 AWS에 빅 데이터 분석을 위한 새로운 클러스터를 배포하고 있습니다. 클러스터는 여러 가용 영역에 분산되어 있는 여러 Linux Amazon EC2 인스턴스에서 실행됩니다.

클러스터의 모든 노드에는 공통 기본 파일 스토리지에 대한 읽기 및 쓰기 액세스 권한이 있어야 합니다. 파일 스토리지는 가용성이 높고 복원력이 있어야 하며 POSIX(이동식 운영 체제 인터페이스)와 호환되어야 하며 높은 수준의 처리량을 수용해야 합니다.

이러한 요구 사항을 충족하는 스토리지 솔루션은 무엇입니까?

A. Amazon S3 버킷에 연결된 AWS Storage Gateway 파일 게이트웨이 NFS 파일 공유를 프로비저닝합니다. 클러스터의 각 EC2 인스턴스에 NFS 파일 공유를 탑재합니다.
B. 범용 성능 모드를 사용하는 새로운 Amazon Elastic File System(Amazon EFS) 파일 시스템을 프로비저닝합니다. 클러스터의 각 EC2 인스턴스에 EFS 파일 시스템을 탑재합니다.
C. io2 볼륨 유형을 사용하는 새로운 Amazon Elastic Block Store(Amazon EBS) 볼륨을 프로비저닝합니다. 클러스터의 모든 EC2 인스턴스에 EBS 볼륨을 연결합니다.
D. 최대 I/O 성능 모드를 사용하는 새로운 Amazon Elastic File System(Amazon EFS) 파일 시스템을 프로비저닝합니다. 클러스터의 각 EC2 인스턴스에 EFS 파일 시스템을 탑재합니다.

해설
정답: D
키워드는 높은 수준의 처리량, 최대 I/O 모드: 빅데이터 분석과 같은 병렬화된 워크로드에 가장 적합합니다.
General Purpose 성능 모드는 최소의 연산 지연을 제공하며 모든 파일 시스템의 기본 설정입니다. 이것은 고성능 워크로드, 예를 들어 대용량 데이터 분석을 위해 높은 처리량을 처리하는 데 이상적입니다.
Max I/O 성능 모드는 일반 사용자 모드보다 연산당 지연 시간이 많이 걸립니다. 이 모드는 고도로 병렬화된 워크로드 (즉, 수백 또는 수천 개의 컨테이너나 쓰레드로부터 동시에 파일 시스템에 대한 요청이 발생할 수 있는 워크로드)를 위해 설계되었지만, 여기서는 '클러스터를 실행하는 많은 Linux Amazon EC2 인스턴스'라고만 언급되었으며 특히 '수천 개'까지 제공하지는 않았습니다.
따라서, 데이터 분석에 대한 요구 사항을 고려할 때, 이러한 요구 사항을 가장 잘 충족하는 옵션은

'일반 목적 성능 모드'를 사용하는 새로운 EFS 파일 시스템을 프로비저닝하고 각 EC2 인스턴스에 EFS 파일 시스템을 마운트하는 옵션 B입니다.

◆ | **Q#0395.** | **Ref#0395.**
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 v1 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 RTO는 5분, RPO는 1분입니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. 대상 리전에 Aurora Serverless v1 데이터베이스의 읽기 전용 복제본을 생성하십시오. AWS SAM을 사용하여 Runbook을 생성하여 대상 리전에 솔루션을 배포합니다. 재해 발생 시 읽기 전용 복제본을 기본 복제본으로 승격합니다.
B. Aurora Serverless v1 데이터베이스를 원본 지역과 대상 지역에 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 v1 DB 클러스터를 생성합니다. 대상 지역에서 솔루션을 시작합니다. 활성-수동 구성에서 작동하도록 두 지역 솔루션을 구성합니다.
D. Aurora Serverless v1 데이터베이스를 원본 지역과 대상 지역에 걸쳐 확장되는 표준 Aurora MySQL 글로벌 데이터베이스로 변경합니다. 대상 지역에서 솔루션을 시작합니다. 활성-수동 구성에서 작동하도록 두 지역 솔루션을 구성합니다.

해설
정답: D
Aurora Serverless v1이 리드 레플리카, 크로스리전 레플리카 또는 글로벌 데이터베이스를 지원하지 않으므로 RTO 및 RPO 요구사항을 충족시키려면 표준 Aurora MySQL로 변경해야 합니다.
참고로 Aurora MySQL은 글로벌 데이터베이스를 지원하여 데이터를 두 리전 간에 복제할 수 있습니다.
또한 AWS 리전 전체에 솔루션을 배포하려면 타깃 리전에서 솔루션을 시작해야 하며, 복구 시에는 두 리전의 솔루션을 활성-비활성 설정으로 구성해 전환을 빠르게 할 수 있습니다.

◆ | **Q#0396.** | **Ref#0396.**
한 회사가 여행사 체인을 소유하고 있으며 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 회사 직원들은 여행지에 대한 정보를 검색하기 위해 애플리케이션을 사용합니다. 목적지 콘텐츠는 매년 4회 업데이트됩니다.

두 개의 고정 Amazon EC2 인스턴스가 애플리케이션을 제공합니다. 이 회사는 EC2 인스턴스에 대한 탄력적 IP 주소를 반환하는 travel.example.com의 다중 값 레코드가 있는 Amazon Route 53 공용 호스팅 영역을 사용합니다. 애플리케이션은 Amazon DynamoDB를 기본 데이터 스토어로 사용합니다. 회사는 캐싱 솔루션으로 자체 호스팅 Redis 인스턴스를 사용합니다.

콘텐츠를 업데이트하는 동안 EC2 인스턴스 및 캐싱 솔루션의 로드가 급격히 증가합니다. 이러한 부하 증가로 인해 여러 차례 가동 중지 시간이 발생했습니다. 솔루션 설계자는 애플리케이션의 가용성이 높고 콘텐츠 업데이트로 생성되는 로드를 처리할 수 있도록 애플리케이션을 업데이트해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. DynamoDB Accelerator(DAX)를 인 메모리 캐시로 설정합니다. DAX를 사용하도록 애플리케이션을 업데이트합니다. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. ALB(Application Load Balancer)를 생성합니다. Auto Scaling 그룹을 ALB의 대상으로 설정합니다. ALB의 DNS 별칭을 대상

으로 하는 단순 라우팅 정책을 사용하도록 Route 53 레코드를 업데이트합니다. 콘텐츠가 업데이트되기 전에 EC2 인스턴스에 대한 예약된 조정을 구성합니다.
B. Redis용 Amazon ElastiCache를 설정합니다. ElastiCache를 사용하도록 애플리케이션을 업데이트합니다. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. Amazon CloudFront 배포를 생성하고 Auto Scaling 그룹을 배포의 원본으로 설정합니다. CloudFront 배포의 DNS 별칭을 대상으로 하는 단순 라우팅 정책을 사용하도록 Route 53 레코드를 업데이트합니다. 콘텐츠가 업데이트되기 전에 EC2 인스턴스를 수동으로 확장합니다.
C. Memcached용 Amazon ElastiCache를 설정합니다. ElastiCache를 사용하도록 애플리케이션을 업데이트합니다. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. ALB(Application Load Balancer)를 생성합니다. Auto Scaling 그룹을 ALB의 대상으로 설정합니다. ALB의 DNS 별칭을 대상으로 하는 단순 라우팅 정책을 사용하도록 Route 53 레코드를 업데이트합니다. 콘텐츠가 업데이트되기 전에 애플리케이션에 대한 예약된 크기 조정을 구성합니다.
D. DynamoDB Accelerator(DAX)를 인 메모리 캐시로 설정합니다. DAX를 사용하도록 애플리케이션을 업데이트하세요. EC2 인스턴스에 대한 Auto Scaling 그룹을 생성합니다. Amazon CloudFront 배포를 생성하고 Auto Scaling 그룹을 배포의 원본으로 설정합니다. CloudFront 배포의 DNS 별칭을 대상으로 하는 단순 라우팅 정책을 사용하도록 Route 53 레코드를 업데이트합니다. 콘텐츠가 업데이트되기 전에 EC2 인스턴스를 수동으로 확장합니다.

해설
정답: A
DynamoDB Accelerator(DAX)는 다이나모DB의 초고속 캐싱 메커니즘으로, 애플리케이션의 반응성을 향상시키면서 데이터베이스의 읽기 부하를 줄입니다. 이는 애플리케이션을 더 높은 부하를 처리하는 데 도움이 됩니다.
EC2 오토 스케일링 그룹은 과부하나 실패에 대응하여 EC2 인스턴스의 수를 자동으로 조정합니다. 이는 애플리케이션의 가용성을 보장하고 부하가 급증할 때 처리 용량을 늘립니다.
ALB는 여러 대의 EC2 인스턴스에 트래픽을 자동으로 분산시킵니다. 이는 지연 시간과 오류 비율을 줄이는 데 도움이 됩니다.
Route 53의 단순 라우팅 정책은 사용자가 요청한 컨텐츠를 가장 빠르게 제공하는 데 가장 효율적인 리소스로 사용자의 트래픽을 라우팅합니다.

◆ | **Q#0397.** | **Ref#0397.**
회사는 맞춤형 모바일 앱을 사용하여 모바일 장치에서 업로드할 이미지 데이터를 저장하고 처리해야 합니다. 주중 오전 8시부터 오후 5시 사이에 사용량이 가장 많아 분당 수천 건의 업로드가 발생합니다. 그 외에는 앱을 거의 사용하지 않습니다. 이미지 처리가 완료되면 사용자에게 알림이 전송됩니다.

로드를 처리할 수 있도록 이미지 처리를 확장할 수 있도록 솔루션 설계자는 어떤 작업 조합을 취해야 합니까? (3개를 선택하세요.)

A. 모바일 소프트웨어의 파일을 Amazon S3에 직접 업로드합니다. S3 이벤트 알림을 사용하여 Amazon MQ 대기열에 메시지를 생성합니다.
B. 모바일 소프트웨어의 파일을 Amazon S3에 직접 업로드합니다. S3 이벤트 알림을 사용하여 Amazon Simple Queue Service(Amazon SQS) 표준 대기열에 메시지를 생성합니다.
C. 대기열에서 메시지를 사용할 수 있을 때 이미지 처리를 수행하도록 AWS Lambda 함수를 호출합니다.
D. S3 배치 작업 작업을 호출하여 대기열에서 메시지를 사용할 수 있을 때 이미지 처리를 수행합니다.
E. 처리가 완료되면 Amazon Simple 알림 서비스(Amazon SNS)를 사용하여 모바일 앱에 푸시 알림을 보냅니다.
F. 처리가 완료되면 Amazon Simple Email Service(Amazon SES)를 사용하여 모바일 앱에 푸시 알림을 보냅니다.

해설

정답: B, C, E
B : Amazon S3는 대규모 데이터 저장에 적합하며, 업로드된 이미지를 저장하기에 적당합니다. 또한, S3 이벤트 알림은 새로운 객체가 추가되거나 기존 객체가 삭제될 때 알림을 보낼 수 있으므로 이를 활용하여 SQS 표준 큐에 메시지를 생성하는 것이 효율적입니다.
C : AWS Lambda는 이벤트에 반응하여 코드를 자동으로 실행하는 서버리스 컴퓨트 서비스입니다. SQS에서 메시지를 받아 이를 처리하는 데 Lambda 함수를 사용하는 것이 효율적이며, 이에 필요한 코드만 실행하므로 비용 효율적이며 확장성이 뛰어납니다.
E : 이미지 처리가 완료된 후에 사용자에게 알려야 하는 경우, Amazon SNS를 사용하여 푸시 알림을 보내는 것이 바람직합니다. Amazon SNS는 푸시 알림, SMS, 이메일 등을 포함한 고도로 확장 가능한 메시지 및 알림 서비스입니다.

◆ | **Q#0398.** | **Ref#0398.**
한 회사가 AWS에서 애플리케이션을 구축하고 있습니다. 애플리케이션은 분석을 위해 Amazon OpenSearch Service 클러스터에 로그를 보냅니다. 모든 데이터는 VPC 내에 저장되어야 합니다.

회사의 개발자 중 일부는 집에서 일합니다. 다른 개발자들은 세 곳의 회사 사무실에서 근무합니다. 개발자는 OpenSearch 서비스에 액세스하여 로컬 개발 컴퓨터에서 직접 로그를 분석하고 시각화해야 합니다.

어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS 클라이언트 VPN 엔드포인트를 구성하고 설정합니다. 클라이언트 VPN 엔드포인트를 VPC의 서브넷과 연결합니다. 클라이언트 VPN 셀프 서비스 포털을 구성합니다. 개발자에게 클라이언트 VPN용 클라이언트를 사용하여 연결하도록 지시합니다.
B. 전송 게이트웨이를 생성하고 이를 VPC에 연결합니다. AWS 사이트 간 VPN을 생성합니다. Transit Gateway에 대한 연결을 생성합니다. 개발자에게 OpenVPN 클라이언트를 사용하여 연결하도록 지시합니다.
C. 전송 게이트웨이를 생성하고 이를 AWS Direct Connect 연결을 통해 VPOrder에 연결합니다. Direct Connect 연결에 퍼블릭 VIF를 설정합니다. 퍼블릭 VIF를 전송 게이트웨이와 연결합니다. 개발자에게 Direct Connect 연결에 연결하도록 지시합니다.
D. VPC의 퍼블릭 서브넷에 배스천 호스트를 생성하고 구성합니다. 회사 CIDR 범위에서 SSH 액세스를 허용하도록 배스천 호스트 보안 그룹을 구성합니다. 개발자에게 SSH를 사용하여 연결하도록 지시합니다.

해설
정답: A
AWS 클라이언트 VPN을 사용하면 사용자는 안전하게 VPC 리소스에 액세스할 수 있습니다. 또한, 로컬에서 AWS로의 연결은 트래픽을 인터넷을 통해 전송하는 것보다 더 안전합니다.
이 방법을 사용하면 회사의 개발자들이 자신의 로컬 개발 환경에서 직접 Amazon OpenSearch Service에 접속하여 로그를 분석하고 시각화할 수 있습니다.
그리고 클라이언트 VPN은 사용자의 환경에 관계없이 어디서나 안전하게 연결할 수 있습니다. 이는 회사 내부에서 일하는 개발자와 재택근무하는 개발자 모두에게 안전하고 안정적인 접근 경로를 제공합니다.

◆ | **Q#0399.** | **Ref#0399.**
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.

솔루션 아키텍트는 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 IAM 역할을 사용하여 다른 리소스에 액세스합니다.

해설
정답: B, E
B. awsvpc 네트워크 모드를 사용하여 작업을 생성하면 네트워크 퍼포먼스를 최적화하고 각 작업에 작업 레벨의 보안 그룹을 적용하는 것을 가능하게 합니다. 이 방식은 리소스 간 통신을 제어하는 데 더 세분화 된 방법을 제공하므로 "최소 권한"원칙에 잘 부합합니다.
E. 작업에 보안 그룹을 적용하고, 다른 리소스에 액세스하기 위해 작업용 IAM 역할을 사용하면 작업에 보안 그룹을 적용하면 웹 앱과 관련된 각 마이크로서비스에 대해 보안 레벨을 미세하게 조정할 수 있으므로 보다 세분화된 보안 제어가 가능해집니다.
또한 IAM 역할을 사용하면 시작 시 컨테이너에 IAM 자격 증명을 전달하는 위험을 피할 수 있습니다.

◆ | **Q#0400.** | **Ref#0400.**
한 회사가 여러 AWS Lambda 함수와 Amazon DynamoDB 테이블로 구성된 서버리스 애플리케이션을 실행하고 있습니다. 이 회사는 Amazon Neptune DB 클러스터에 액세스하기 위해 Lambda 함수가 필요한 새로운 기능을 만들었습니다. Neptune DB 클러스터는 VPC의 서브넷 3개에 위치합니다.

다음 중 Lambda 함수가 Neptune DB 클러스터 및 DynamoDB 테이블에 액세스하도록 허용하는 솔루션은 무엇입니까? (2개를 선택하세요.)

A. Neptune VPC에 3개의 퍼블릭 서브넷을 생성하고 인터넷 게이트웨이를 통해 트래픽을 라우팅합니다. 세 개의 새로운 퍼블릭 서브넷에서 Lambda 함수를 호스팅합니다.
B. Neptune VPC에 3개의 프라이빗 서브넷을 생성하고 NAT 게이트웨이를 통해 인터넷 트래픽을 라우팅합니다. 세 개의 새로운 프라이빗 서브넷에서 Lambda 함수를 호스팅합니다.
C. Neptune 보안 그룹을 VP업데이트 외부에서 Lambda 함수를 호스팅하여 Lambda 함수의 IP 범위에서의 액세스를 허용합니다.
D. VPC 외부에서 Lambda 함수를 호스팅합니다. Neptune 데이터베이스에 대한 VPC 엔드포인트를 생성하고 Lambda 함수가 VPC 엔드포인트를 통해 Neptune에 액세스하도록 합니다.
E. Neptune VPC에 3개의 프라이빗 서브넷을 생성합니다. 세 개의 새로운 격리된 서브넷에서 Lambda 함수를 호스팅합니다. DynamoDB용 VPC 엔드포인트를 생성하고 DynamoDB 트래픽을 VPC 엔드포인트로 라우팅합니다.

해설
정답: B, E
B. 프라이빗 서브넷 내에서 Lambda를 호스팅하면 VPC 내 Neptune 클러스터에 안전하게 액세스할 수 있습니다. NAT 게이트웨이를 통한 인터넷 트래픽 라우팅은 외부 리소스와의 통신을 가능하게 합니다.
E. 이 옵션도 Lambda 함수가 Neptune에 안전하게 액세스할 수 있도록 해줍니다. 또한 DynamoDB와의 통신을 위해 VPC 엔드포인트를 사용하면, 함수가 인터넷을 통해 DynamoDB에 액세스할 필요 없이 내부 네트워크를 통해 직접 DynamoDB에 액세스할 수 있습니다.