Q1

금융 회사는 사용자를 위해 매월 불변의 은행 계좌 명세서를 생성하는 시스템을 구축하고 있습니다. 명령문은 Amazon S3에 저장됩니다. 사용자는 월별 명세서에 즉시 액세스하거나 최대 2년까지 액세스할 수 있어야 합니다. 일부 사용자는 자신의 명령문에 자주 액세스하지만 다른 사용자는 자신의 명령문에 거의 액세스하지 않습니다. 회사의 보안 및 규정 준수 정책에 따라 명세서는 최소 7년 동안 보관해야 합니다.

회사의 요구 사항을 충족하는 가장 비용 효율적인 솔루션은 무엇입니까?

A. 객체 잠금이 비활성화된 S3 버킷을 생성합니다. 명령문을 S3 스탠다드에 저장합니다. 30일 후에 데이터를 S3 Standard-Infrequent Access (S3 Standard-IA) 로 이전하도록 S3 수명 주기 정책을 정의합니다. 2년 후 데이터를 S3 Glacier Deep 아카이브로 이동하도록 또 다른 S3 수명 주기 정책을 정의합니다. 7년 미만의 아카이브에 대한 삭제 거부 권한이 있는 S3 Glacier 저장소 잠금 정책을 연결합니다.

B. 버전 관리가 활성화된 S3 버킷을 생성합니다. S3 인텔리전트 티어링에 명령문을 저장합니다. 동일 리전 복제를 사용하여 백업 S3 버킷에 객체를 복제합니다. 백업 S3 버킷에 대한 S3 수명 주기 정책을 정의하여 데이터를 S3 Glacier로 이동합니다. 7년 미만의 아카이브에 대한 삭제 거부 권한이 있는 S3 Glacier 저장소 잠금 정책을 연결합니다.

C. 객체 잠금이 활성화된 S3 버킷을 생성합니다. S3 인텔리전트 티어링에 명령문을 저장합니다. 기본 보존 기간이 2년인 규정 준수 모드를 사용하도록 설정합니다. 2년 후 데이터를 S3 Glacier로 이동하도록 S3 수명 주기 정책을 정의합니다. 7년 미만의 아카이브에 대한 삭제 거부 권한이 있는 S3 Glacier 저장소 잠금 정책을 연결합니다.

D. 버전 관리가 비활성화된 S3 버킷을 생성합니다. S3 One Zone-Infrequent Access (S3 One Zone-IA) 에 명령문을 저장합니다. 2년 후 데이터를 S3 Glacier Deep 아카이브로 이동하도록 S3 수명 주기 정책을 정의합니다. 7년 미만의 아카이브에 대한 삭제 거부 권한이 있는 S3 Glader 저장소 잠금 정책을 연결합니다.

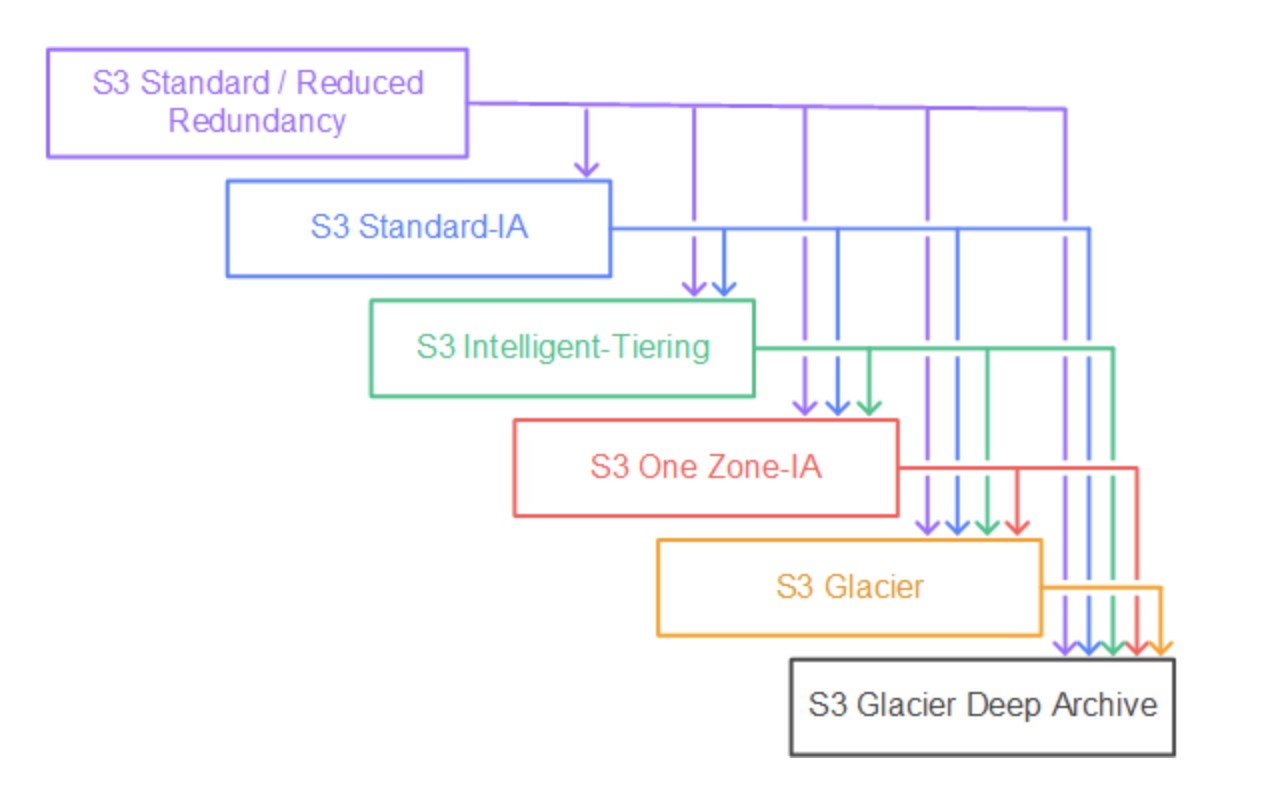
Answer: C

설명

S3 수명 주기 구성은 Amazon S3가 객체 그룹에 적용하는 작업을 정의하는 규칙 집합입니다. 조치는 객체를 다른 스토리지 클래스로 전환하거나 객체를 만료(삭제)하는 것입니다.

이 경우 더 이상 자주 액세스하지 않을 때 객체를 S3 Glacier(저비용 아카이브)로 이동하고 더 이상 보관할 필요가 없을 때 객체를 만료시키는 수명 주기 정책을 생성할 수 있습니다.

다음 이미지는 스토리지 클래스 간 지원 전환을 위한 폭포수 모델을 보여줍니다.



Q2

한 솔루션 설계자가 AWS 환경에 대한 사용자의 액세스를 인증하기 위해 회사의 온프레미스 IdP (자격 증명 공급자) 와 함께 SAML 2.0 연동 자격 증명 솔루션을 구현했습니다. 솔루션스 아키텍트가 페더레이션 자격 증명 웹 포털을 통해 인증을 테스트하면 AWS 환경에 대한 액세스 권한이 부여됩니다. 그러나 테스트 사용자가 페더레이션 자격 증명 웹 포털을 통해 인증을 시도하면 AWS 환경에 액세스할 수 없습니다.

ID 페더레이션이 속성이 구성되어 있는지 확인하기 위해 솔루션스 아키텍트가 확인해야 하는 항목은 무엇입니까?(세 개 선택)

A. IAM 사용자의 권한 pokey가 해당 사용자에 대해 SAML 연동을 사용할 수 있도록 허용했습니다.

B. 페더레이션 사용자 또는 페더레이션 그룹의 신뢰 정책에 대해 생성된 IAM 역할은 SAML 공급자를 원칙으로 설정했습니다.

C. 테스트 사용자는 회사 IdP의 AWS 페더레이션 사용자 그룹에 속해 있지 않습니다.

D. 웹 포털은 SAML 공급자의 ARN, IAM 역할의 ARN 및 IdP의 SAML 어설션을 사용하여 AWS STS 가정 역할을 호출합니다.

E. 온프레미스 IdP의 DNS 호스트 이름은 AWS 환경 VPC에서 연결할 수 있습니다.

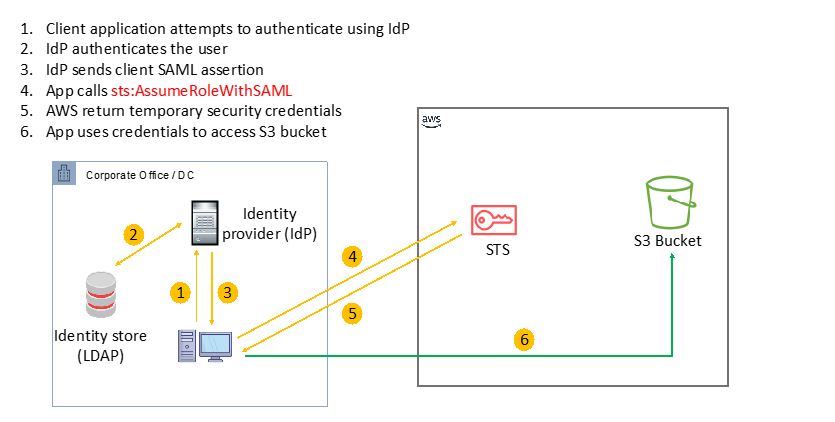
F. 회사의 IdP는 사용자 또는 그룹이 회사를 적절한 권한이 있는 IAM 역할에 속성 매핑하는 SAML 어설션을 정의합니다.

Answer: B, D, F

설명

AWS는 많은 자격 증명 공급자(IdP)가 사용하는 공개 표준인 SAML 2.0(Security Assertion Markup Language 2.0)으로 자격 증명 연동을 지원합니다. 이 기능은 연합 SSO(Single Sign-On)를 활성화하므로 조직의 모든 사람에 대해 IAM 사용자를 생성하지 않고도 사용자가 AWS Management Console에 로그인하거나 AWS API 작업을 호출할 수 있습니다.

아래 다이어그램에서는 클라이언트가 Amazon S3 버킷에 대한 임시 액세스 권한을 부여받은 상황에서 인증 프로세스를 보여줍니다.



정답은 다음 사실을 기반으로 검증됩니다.

· 4단계에서 클라이언트 앱은 AWS STS AssumeRoleWithSAML API를 호출하여 SAML 공급자의 ARN, 수임할 역할의 ARN, IdP의 SAML 어설션을 전달합니다.

· IdP와 AWS가 서로를 신뢰하도록 구성할 때 IAM에서 하나 이상의 IAM 역할을 생성합니다. 역할의 신뢰 정책에서 SAML 공급자를 보안 주체로 설정하여 조직과 AWS 간의 신뢰 관계를 설정합니다. 그리고…

· 조직의 IdP에서 조직의 사용자 또는 그룹을 IAM 역할에 매핑하는 어설션을 정의합니다.

참조:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_providers\_saml.html

Q3

솔루션 설계자는 회사에 온프레미스 데이터 처리 애플리케이션을 AWS 클라우드로 마이그레이션하는 방법에 대해 조언해야 합니다. 현재 사용자는 웹 포털을 통해 입력 파일을 업로드합니다. 그런 다음 웹 서버는 업로드된 파일을 NAS에 저장하고 메시지 큐를 통해 처리 서버에 메시지를 보냅니다. 각 미디어 파일을 처리하는 데 최대 1시간이 걸릴 수 있습니다. 이 회사는 업무 시간 중에 처리 대기 중인 미디어 파일의 수가 상당히 늘어나고 업무 시간이 지나면 파일 수가 급격히 감소한다고 판단했습니다.

가장 비용 효율적인 마이그레이션 권장 사항은 무엇입니까?

A. Amazon SQS를 사용하여 대기열을 생성합니다. 새 대기열에 게시하도록 기존 웹 서버를 구성합니다. 대기열에 메시지가 있으면 AWS Lambda 함수를 호출하여 대기열에서 요청을 가져오고 파일을 처리합니다. 처리된 파일을 Amazon S3 버킷에 저장합니다.

B. Amazon MQ를 사용하여 대기열을 생성합니다. 새 대기열에 게시하도록 기존 웹 서버를 구성합니다. 대기열에 메시지가 있으면 새 Amazon EC2 인스턴스를 생성하여 대기열에서 요청을 가져오고 파일을 처리합니다. 처리된 파일을 Amazon EFS에 저장합니다. 작업이 완료된 후 EC2 인스턴스를 종료합니다.

C. Amazon MQ를 사용하여 대기열을 생성합니다. 새 대기열에 게시하도록 기존 웹 서버를 구성합니다.대기열에 메시지가 있으면 AWS Lambda 함수를 호출하여 대기열에서 요청을 가져오고 파일을 처리합니다. 처리된 파일을 Amazon EFS에 저장합니다.

D. Amazon SQS를 사용하여 대기열을 생성합니다. 새 대기열에 게시하도록 기존 웹 서버를 구성합니다. EC2 Auto Scaling 그룹의 Amazon EC2 인스턴스를 사용하여 대기열에서 요청을 가져오고 파일을 처리합니다. SQS 대기열 길이에 따라 EC2 인스턴스를 조정합니다. 처리된 파일을 Amazon S3 버킷에 저장합니다.

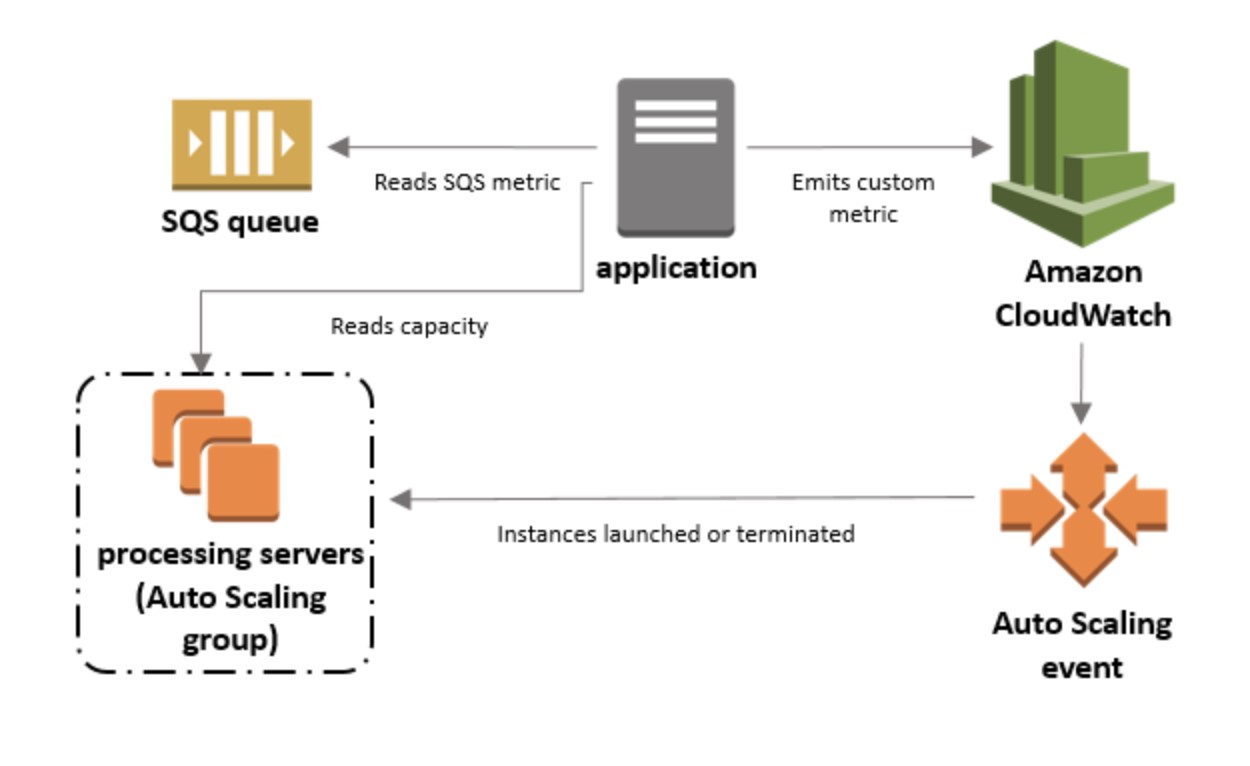
Answer: D

설명

가장 좋은 솔루션은 메시지 대기열에 Amazon SQS, 처리 계층에 Amazon EC2 Auto Scaling, 스토리지 계층에 Amazon S3를 사용하는 것입니다. 이 솔루션은 모든 요구 사항을 충족하며 사용 가능한 가장 저렴한 옵션입니다.

ASG는 ApproximateNumberOfMessages 대기열 속성을 기반으로 확장되도록 구성해야 합니다. 이는 조정 기준으로 사용할 대기열의 메시지 수를 정의하는 인스턴스당 허용 가능한 백로그 메트릭과 함께 사용됩니다.

다음 다이어그램은 이 구성의 아키텍처를 보여줍니다.



잘못됨: A. Lambda는 1시간 동안 파일을 처리할 수 없습니다. 최대 실행 시간은 15분입니다.

잘못됨: B. 인스턴스가 매번 종료되면 대기열을 어떻게 폴링할 수 있습니까? 이것은 실행 가능한 솔루션이 아닙니다.

잘못됨: C. 앞서 언급한 대로 Lambda를 사용할 수 없습니다(최대 실행 제한).

Q4

한 회사에서 로컬 드라이브에 야간 200GB 내보내기를 기록하는 온-프레미스 Microsoft SQL Server 데이터베이스를 보유하고 있습니다. 이 회사는 백업을 Amazon S3의 보다 강력한 클라우드 스토리지로 이전하려고 합니다. 이 회사는 온프레미스 데이터 센터와 AWS 간에 10Gbps의 AWS 직접 연결 연결을 설정했습니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 새 S3 버킷을 생성합니다. 직접 연결 연결에 연결된 VPC 내에 AWS 스토리지 게이트웨이 파일 게이트웨이를 배포합니다. 새 SMB 파일 공유를 만듭니다.야간 데이터베이스 내보내기를 새 SMB 파일 공유에 기록합니다.

B. 직접 연결 연결에 연결된 VPC 내에 Windows용 Amazon FSx 파일 서버 단일 AZ 파일 시스템을 생성합니다. 새 SMB 파일 공유를 만듭니다.Amazon FSx 파일 시스템의 SMB 파일 공유에 야간 데이터베이스 내보내기를 작성합니다. 백업을 활성화합니다.

C. 직접 연결 연결에 연결된 VPC 내에 Windows용 Amazon FSx 파일 서버 다중 AZ 시스템을 생성합니다. 새 SMB 파일 공유를 만듭니다.Amazon FSx 파일 시스템의 SMB 파일 공유에 야간 데이터베이스 내보내기를 작성합니다. 야간 백업을 활성화합니다.

D. 새 S3 버킷을 생성합니다. 직접 연결 연결에 연결된 VPC 내에 AWS 스토리지 게이트웨이 볼륨 게이트웨이를 배포합니다. 새 SMB 파일 공유를 만듭니다.볼륨 게이트웨이의 새 SMB 파일 공유에 야간 데이터베이스 내보내기를 작성하고 이 데이터를 S3 버킷으로 자동 복사합니다.

Answer: A

Q5

한 기업이 온프레미스 데이터 센터의 가상 머신에서 103개의 LOB (기간 업무) 애플리케이션을 실행합니다. 많은 응용 프로그램이 간단한 PHP입니다. Java 또는 Ruby 웹 애플리케이션은 더 이상 활발하게 개발되지 않으며 트래픽을 거의 제공하지 않습니다.

가장 낮은 인프라 비용으로 이러한 애플리케이션을 AWS로 마이그레이션하려면 어떤 접근 방식을 사용해야 합니까?

A. 로드 밸런서 없이 애플리케이션을 단일 인스턴스 AWS Elastic Beanstalk 환경으로 배포합니다.

B. AWS SMS를 사용하여 각 가상 머신에 대한 AML을 생성하고 이를 Amazon EC2에서 실행합니다.

C. 각 애플리케이션을 Docker 이미지로 변환하고 애플리케이션 로드 밸런서 뒤에 있는 작은 Amazon ECS 클러스터에 배포합니다.

D. VM Import/Export를 사용하여 각 가상 머신에 대한 AML을 생성하고 사용자 지정 이미지를 구성하여 단일 인스턴스 AWS Elastic Beanstalk 환경에서 실행할 수 있습니다.

Answer: A

설명

가장 간단한 옵션은 애플리케이션 코드를 Elastic Beanstalk에 업로드하는 것입니다. 그러면 Amazon EC2 인스턴스에서 실행되는 관리형 환경이 생성됩니다. Elastic Beanstalk는 Java, .NET, PHP, Node.js, Python, Ruby, Go 및 Docker로 개발된 웹 애플리케이션을 실행하는 데 가장 적합합니다.

로드 밸런서는 각 애플리케이션의 인스턴스가 하나만 있고 로드 밸런서는 많은 이점을 제공하지 않으며 비용이 증가하므로 사용해서는 안 됩니다.

잘못됨: B. 이것은 작동하지만 운영상 더 간단한 접근 방식은 애플리케이션 코드를 가져와 Elastic Beanstalk에 배포하는 것입니다.

잘못됨: C. 이를 위해서는 운영 오버헤드를 수반하는 애플리케이션 리팩토링이 필요합니다. 또한 단일 ALB 뒤에 100개 이상의 단일 컨테이너 애플리케이션이 있는 경우 요청이 무작위로 분산되어 올바른 애플리케이션으로 전달되지 않습니다. 복잡한 경로 기반 라우팅 및 대상 그룹 구성으로 이 문제를 해결할 수 있지만 이점이 거의 없이 매우 복잡해집니다. Route 53을 사용하여 트래픽을 올바른 컨테이너로 보내는 것이 좋습니다.

참조:

https://aws.amazon.com/elasticbeanstalk/details/

Q6

한 회사가 수많은 loT 디바이스로부터 많은 양의 데이터를 수집하고 있습니다. 데이터는 영구 Amazon EMR 클러스터의 하둡 분산 파일 시스템 (HDFS) 에 최적화된 행 열 형식 (ORC) 파일로 저장됩니다. 이 회사의 데이터 분석 팀은 동일한 EMR 클러스터에 배포된 Apache Presto의 SQL을 사용하여 데이터를 쿼리합니다. 쿼리는 대용량 데이터를 스캔하며 항상 15분 미만 동안 실행되며 오후 5시에서 오후 10시 사이에만 실행됩니다. 회사는 현재 솔루션과 관련된 높은 비용에 대해 우려하고 있습니다. 솔루션 설계자는 SQL 데이터 쿼리가 가능한 가장 비용 효율적인 솔루션을 제안해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon S3에 데이터를 저장합니다. Amazon Redshift 스펙트럼을 사용하여 데이터를 쿼리합니다.

B. Amazon S3에 데이터를 저장합니다. AWS Glue 데이터 카탈로그와 Amazon Athena를 사용하여 데이터를 쿼리합니다.

C. EMR File System (EMRFS) 에 데이터를 저장합니다. Amazon EMR에서 프레스토(Presto)를 사용하여 데이터를 쿼리합니다.

D. Amazon Redshift에 데이터를 저장합니다. Amazon Redshift를 사용하여 데이터를 쿼리합니다.

Answer: B

설명

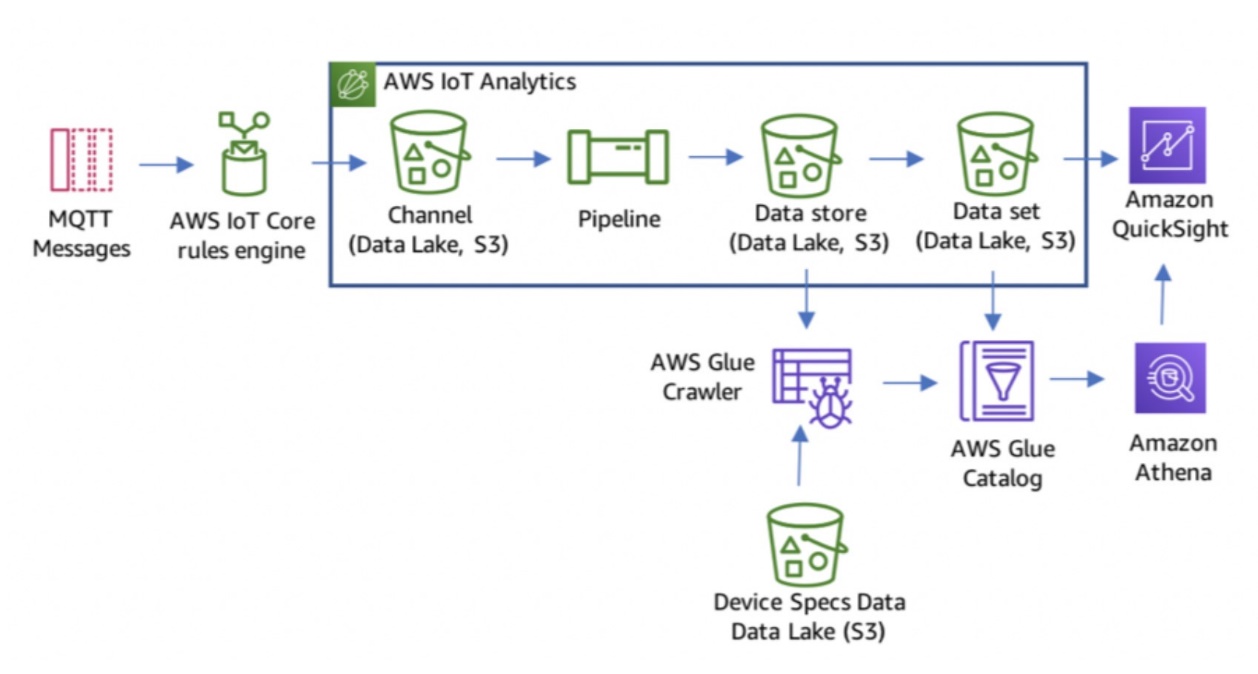
가장 저렴한 옵션은 Glue ETL 작업을 사용하여 Amazon S3로 데이터를 추출하는 것입니다. Glue 데이터 카탈로그에서 테이블을 생성할 수 있으며 Amazon Athena를 사용하여 쿼리를 실행할 수 있습니다. 이것은 모든 요구 사항을 충족하는 완전한 서버리스 솔루션입니다.

여기에서 작동하는 여러 옵션이 있지만 성능 제약도 해결하는 가장 비용 효율적이고 탄력적인 솔루션을 선택해야 합니다. 완전한 서버리스 아키텍처를 사용하면 이러한 모든 목표를 달성할 수 있습니다.

데이터는 처음에 Amazon S3에 저장될 수 있으며, 그런 다음 AWS Glue가 소스 버킷으로 전달되어 데이터에 대한 변환을 실행하고 결과를 다른 S3 버킷에 저장할 수 있습니다. Glue 데이터 카탈로그는 S3 데이터 레이크의 데이터에 대한 메타데이터를 저장하는 데 사용됩니다.

Athena를 사용하여 S3 버킷에서 변환된 데이터를 쿼리할 수 있습니다. Amazon Athena ODBC 드라이버를 사용하여 기존 분석 도구에서 Athena에 연결할 수 있습니다.

아래 다이어그램의 아키텍처는 AWS IoT Analytics 채널을 사용하는 유사한 솔루션을 보여줍니다. 여기에는 AWS Glue 및 Athena도 포함됩니다. QuickSight를 사용하여 데이터를 시각화하는 대신 질문 시나리오의 솔루션은 ODBC를 통해 연결하는 타사 분석 도구를 사용합니다.



잘못됨: C. 이 솔루션을 사용하려면 RedShift 클러스터에서 인스턴스를 실행해야 하므로 비용이 더 많이 듭니다.

잘못됨: D. 이 솔루션을 사용하려면 RedShift 클러스터에서 인스턴스를 실행해야 하므로 비용이 더 많이 듭니다.

Q7

한 소프트웨어 회사에서 Amazon API Gateway를 사용하여 REST API를 사용하는 애플리케이션을 배포했습니다. AWS 람다 함수 및 Amazon DynamoDB 테이블이 있습니다. 애플리케이션에서 PUT 요청 중 오류 수가 증가하고 있습니다. 대부분의 PUT 호출은 특정 API 키로 인증된 소수의 클라이언트에서 발생합니다. 한 솔루션 설계자가 많은 수의 PUT 요청이 한 클라이언트에서 발생했음을 확인했습니다. API는 중요하지 않으며 클라이언트는 실패한 호출의 재시도를 허용할 수 있습니다. 그러나 이러한 오류는 고객에게 표시되며 API의 평판에 피해를 주고 있습니다.

솔루션 설계자는 고객 경험을 개선하기 위해 무엇을 권장해야 합니까?

A. 클라이언트 애플리케이션에서 지수 백오프와 불규칙한 변동이 있는 재시도 로직을 구현합니다. 오류가 발견되고 설명적인 오류 메시지로 처리되었는지 확인합니다.

B. API 게이트웨이 수준에서 사용량 계획을 통해 API 제한을 구현합니다. 클라이언트 애플리케이션이 코드 429 응답을 오류 없이 처리하는지 확인합니다.

C. API 캐싱을 켜서 프로덕션 단계의 응답성을 향상시킵니다. 10분 부하 테스트를 실행합니다. 캐시 용량이 워크로드에 적합한지 확인합니다.

D. Lambda 함수 수준에서 예약 동시성을 구현하여 갑작스러운 트래픽 증가 시 필요한 리소스를 제공합니다.

Answer: A

Q8

모바일 게임을 개발 중인 회사는 두 AWS 리전에서 게임 자산을 제공하고 있습니다.게임 자산은 각 리전의 Application Load Balancer (ALB) 뒤에 있는 Amazon EC2 인스턴스 세트에서 제공됩니다. 회사는 가장 가까운 지역에서 게임 자산을 가져와야 합니다. 가장 가까운 리전에서 게임 애셋을 사용할 수 없게 되면 다른 리전에서 가져와야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. Amazon CloudFront 배포를 생성합니다. 각 ALB에 대해 하나의 오리진이 있는 오리진 그룹을 생성합니다. 원점 중 하나를 기본으로 설정합니다.

B. 각 ALB에 대해 Amazon Route 53 상태 확인을 생성합니다. 두 ALB를 가리키는 Route 53 장애 조치 라우팅 레코드를 생성합니다. Evaluate Target Health 값을 YES로 설정합니다.

C. 각각 하나의 ALB를 오리진으로 사용하는 두 개의 Amazon CloudFront 배포를 생성합니다. 두 개의 CloudFront 배포를 가리키는 Amazon Route 53 장애 조치 라우팅 레코드를 생성합니다. Evaluate Target Health 값을 YES로 설정합니다.

D. 각 ALB에 대해 Amazon Route 53 상태 확인을 생성합니다. 두 ALB를 가리키는 Route 53 지연 시간 별칭 레코드를 생성합니다. Evaluate Target Health 값을 YES로 설정합니다.

Answer: D

https://www.examtopics.com/discussions/amazon/view/51242-exam-aws-certified-solutions-architect-professional-topic-1/

Q9

한 회사에서 인터넷을 통해 액세스할 수 있는 SFTP 서버를 통해 고객에게 파일을 제공하고 있습니다. SFTP 서버는 탄력적 IP 주소가 연결된 단일 Amazon EC2 인스턴스에서 실행됩니다. 고객은 탄력적 IP 주소를 통해 SFTP 서버에 연결하고 인증에 SSH를 사용합니다. 또한 EC2 인스턴스에는 모든 고객 IP 주소에서 액세스할 수 있는 연결된 보안 그룹이 있습니다. 솔루션 설계자는 가용성을 높이고 인프라 관리의 복잡성을 최소화하며 파일에 액세스하는 고객의 업무 중단을 최소화하는 솔루션을 구현해야 합니다. 솔루션이 고객 연결 방식을 바꿔서는 안 됩니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS Transfer 패밀리 서버 생성 공개적으로 액세스 가능한 엔드포인트로 트랜스퍼 패밀리 서버 구성 SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. 트랜스퍼 패밀리 서버를 S3 버킷으로 지정합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

B. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS 트랜스퍼 패밀리 서버를 생성합니다. VPC에서 호스팅하는 인터넷 연결 엔드포인트를 사용하여 트랜스퍼 패밀리 서버를 구성합니다. SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. 고객 IP 주소가 있는 보안 그룹을 새 엔드포인트에 연결합니다. 패밀리 전송 서버가 S3 버킷을 가리키도록 합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

C. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 새 Amazon Elastic File System (Amazon EFS) 파일 시스템을 생성합니다. AWS Fargate 작업 정의를 생성하여 SFTP 서버를 실행합니다. 작업 정의에서 EFS 파일 시스템을 마운트로 지정합니다. 작업 정의를 사용하여 Fargate 서비스를 만들고 서비스 앞에 NLB (네트워크 부하 분산 장치) 를 배치합니다. 서비스를 구성할 때 고객 IP 주소가 있는 보안 그룹을 SFTP 서버를 실행하는 작업에 연결합니다. 탄력적 IP 주소를 NLB와 연결합니다.SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

D. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 다중 연결 Amazon Elastic Block Store (Amazon EBS) 볼륨을 생성합니다. 탄력적 IP 주소가 연결된 NLB (네트워크 로드 밸런서) 를 만듭니다. SFTP 서버를 실행하는 EC2 인스턴스로 Auto Scaling 그룹 생성 Auto Scaling 그룹에서 시작되는 인스턴스가 새로운 다중 연결 EBS 볼륨을 연결하도록 정의 NLB 뒤에 인스턴스를 자동으로 추가하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹이 시작하는 EC2 인스턴스에 대한 고객 IP 주소를 허용하는 보안 그룹입니다. SFTP 서버의 모든 파일을 새 다중 연결 EBS 볼륨으로 동기화합니다.

Answer: B

Q10

한 게임 회사에서 Amazon RDS 데이터베이스의 다중 AZ 배포를 사용하여 게임 리더보드를 만들었습니다. 사용자 수가 증가하고 있으며 개별 플레이어 순위를 얻기 위한 쿼리는 시간이 지남에 따라 점점 느려지고 있습니다. 이 회사는 향후 버전에 대한 사용자 급증을 예상하고 확장성과 성능을 위해 설계를 최적화하려고 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 데이터베이스를 Amazon DynamoDB로 마이그레이션합니다. 지시선을 다른 테이블에 저장합니다.Apache HiveQL JOIN 문을 사용하여 리더보드를 빌드합니다.

B. 리더보드 데이터를 RDS DB 인스턴스에 보관합니다. Redis용 Amazon ElastiCache 클러스터의 다중 AZ 배포를 프로비저닝합니다.

C. Amazon S3 버킷을 대상으로 하는 Amazon Kinesis 데이터 파이어호스를 사용하여 순위표 데이터를 스트리밍합니다. 순위표에 대해 Amazon Athena를 사용하여 S3 버킷을 쿼리합니다.

D. RDS DB 인스턴스에 읽기 전용 복제본을 추가합니다. RDS 프록시 데이터베이스 프록시를 추가합니다.

Answer: B

Q11

솔루션스 아키텍트가 AWS Import/Export의 Amazon EC2 VM 가져오기 기능을 사용하여 온프레미스 환경에서 VM을 가져오고 있습니다. 솔루션스 아키텍트가 AMI를 생성하고 해당 AMI를 기반으로 하는 Amazon EC2 인스턴스를 프로비저닝했습니다. EC2 인스턴스는 VPC의 퍼블릭 서브넷 내에서 실행되며 퍼블릭 IP 주소가 할당됩니다. EC2 인스턴스는 AWS 시스템 관리자 콘솔에서 관리형 인스턴스로 표시되지 않습니다. 이 문제를 해결하기 위해 솔루션 설계자가 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. Systems Manager 에이전트가 인스턴스에 설치되어 있고 실행 중인지 확인합니다.

B. 인스턴스에 Systems Manager를 위한 적절한 IAM 역할이 할당되었는지 확인합니다.

C. VPC에 VPC 엔드포인트가 있는지 확인합니다.

D. AWS Application Discovery Agent가 구성되었는지 확인합니다.

E. Systems Manager에 대한 서비스 연결 역할이 올바르게 구성되었는지 확인합니다.

Answer: A, B

관리형 인스턴스는 Systems Manager와 함께 사용하도록 구성된 Amazon EC2 인스턴스입니다. 관리형 인스턴스는 Run Command, Patch Manager 및 Session Manager와 같은 Systems Manager 서비스를 사용할 수 있습니다.

관리형 인스턴스가 되려면 인스턴스가 다음 사전 조건을 충족해야 합니다.

・AWS Systems Manager 에이전트(SSM 에이전트)가 설치되어 실행 중입니다.

・SSM 에이전트를 사용하여 Systems Manager 엔드포인트에 연결되어 있습니다.

・올바른 AWS Identity and Access Management(IAM) 역할이 연결되어 있습니다.

・인스턴스 메타데이터 서비스에 연결되어 있습니다.

https://aws.amazon.com/ko/premiumsupport/knowledge-center/systems-manager-ec2-instance-not-appear/

Q12

한 회사에서 AWS 조직을 사용하여 여러 AWS 계정을 관리하고 있습니다. 보안을 위해 회사는 모든 조직의 멤버 계정에서 타사 알림 시스템과 통합할 수 있는 Amazon Simple Notification Service (Amazon SNS) 주제를 생성해야 합니다. 한 솔루션스 아키텍트는 AWS CloudFormation 템플릿을 사용하여 SNS 주제와 스택 세트를 생성하여 CloudFormation 스택의 배포를 자동화했습니다. 조직에서 신뢰할 수 있는 액세스가 활성화되었습니다.

솔루션스 아키텍트는 모든 AWS 계정에 CloudFormation 스택세트를 배포하기 위해 무엇을 해야 합니까?

A. 조직 멤버 계정에 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택세트 드리프트 감지를 사용합니다.

B. 조직 구성원 계정에서 스택을 만듭니다. 셀프 서비스 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택세트 자동 배포를 활성화합니다.

C. 조직 관리 계정에서 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다.CloudFormation 스택세트 자동 배포를 활성화합니다.

D. 조직 관리 계정에서 스택을 만듭니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택 세트 드리프트 감지를 활성화합니다.

Answer: C

Q13

한 회사가 게놈 정보를 수집하는 유전자 보고 장치를 개발하여 연구자들이 다양한 집단에서 대량의 데이터 샘플을 수집할 수 있도록 지원하고 있습니다. 이 장치는 매초 8KB의 게놈 데이터를 데이터를 처리 및 분석하고 연구자에게 정보를 제공해야 하는 데이터 플랫폼으로 푸시합니다. 데이터 플랫폼은 다음 사항을 충족해야 합니다.

요구 사항:

\* 인바운드 게놈 데이터에 대한 거의 실시간 분석을 제공합니다.

\* 데이터가 유연하고 평행하며 내구성이 있는지 확인하십시오.

\* 처리 결과를 데이터 웨어하우스로 전달합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 전략을 사용해야 합니까?

A. Amazon Kinesis Data Firehose를 사용하여 인바운드 센서 데이터를 수집하고 Kinesis 클라이언트로 데이터를 분석한 다음 그 결과를 Amazon RDS 인스턴스에 저장합니다.

B. Amazon Kinesis 데이터 스트림을 사용하여 인바운드 센서 데이터를 수집하고 Kinesis 클라이언트로 데이터를 분석한 다음 Amazon EMR을 사용하여 결과를 Amazon Redshift 클러스터에 저장합니다.

C. Amazon S3를 사용하여 인바운드 디바이스 데이터를 수집하고 Kinesis를 사용하여 Amazon SQS에서 데이터를 분석한 다음 그 결과를 Amazon Redshift 클러스터에 저장합니다.

D. Amazon API Gateway를 사용하여 요청을 Amazon SQS 대기열에 넣고, AWS Lambda 함수로 데이터를 분석하고, 그 결과를 Amazon EMR을 사용하는 Amazon Redshift 클러스터에 저장합니다.

Answer: B

설명

솔루션은 거의 실시간 분석을 지원해야 합니다. 이를 위해 Amazon Kinesis 데이터 스트림은 Amazon EMR을 사용하여 데이터를 처리 및 분석하는 클라이언트와 함께 사용할 수 있습니다. 솔루션은 또한 데이터 웨어하우스에 결과를 제공해야 하며 Amazon RedShift는 이러한 목적에 이상적입니다.

잘못됨: A. Firehose는 Kinesis 클라이언트를 사용하지 않습니다. 대상에 직접 데이터를 로드합니다.

잘못됨: C. Amazon S3는 이 규모의 스트리밍 데이터를 거의 실시간으로 수집하는 데 사용해서는 안 됩니다. Amazon Kinesis는 이 사용 사례에 더 적합합니다. SQS에서 Kinesis로 분석하는 것도 의미가 없습니다.

잘못됨: D. API Gateway는 스트리밍 데이터에 사용되어서는 안 되며 데이터를 SQS 대기열에 직접 넣을 수 없습니다.

참조:

https://aws.amazon.com/kinesis/data-streams/getting-started/

https://docs.aws.amazon.com/streams/latest/dev/shared-throughput-kcl-consumers.html

https://aws.amazon.com/emr/

https://aws.amazon.com/redshift/

Q14

한 회사에서 AWS CloudFormation을 사용하여 인프라를 배포하고 있습니다. 이 회사는 프로덕션 CloudFormation 스택이 삭제되면 Amazon RD5 데이터베이스 또는 Amazon EBS 볼륨에 저장된 중요한 데이터도 삭제될 수 있다고 우려하고 있습니다.

이제 회사는 사용자가 실수로 이런 식으로 데이터를 삭제하는 것을 막을 수 있습니까?

A. CloudFormation 템플릿을 수정하여 RDS 및 EBS 리소스에 삭제 정책 속성을 추가합니다.

B. RDS 및 EBS 리소스의 삭제를 허용하지 않는 스택 정책을 구성합니다.

C. "aws:cloudformation:stack-name'' 태그로 지연된 RDS 및 EBS 리소스의 삭제를 거부하도록 IAM 정책을 수정합니다.

D. AWS 구성 규칙을 사용하여 RDS 및 EBS 리소스가 삭제되지 않도록 합니다.

Answer: A

Q15

회사에 새로운 보안 정책이 있습니다. 이 정책은 회사가 Amazon S3 버킷에서 데이터를 검색하는 모든 이벤트를 기록하도록 요구합니다. 회사는 이러한 감사 로그를 전용 S3 버킷에 저장해야 합니다. 이 회사는 중앙 집중식 로깅을 위해 지정된 AWS 계정에 감사 로그 S3 버킷을 만들었습니다. S3 버킷에는 쓰기 전용 교차 계정 액세스를 허용하는 버킷 정책이 있습니다. 솔루션 설계자는 모든 S3 객체 수준 액세스가 현재 S3 버킷 및 향후 S3 버킷에 대해 기록되도록 해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 모든 현재 S3 버킷에 대해 서버 액세스 로깅을 활성화합니다. 감사 로그 S3 버킷을 감사 로그의 대상으로 사용

B. 모든 현재 S3 버킷과 감사 로그 S3 버킷 간의 복제 활성화 감사 로그 S3 버킷에서 S3 버전 관리 활성화합니다.

C. 객체에 액세스할 때마다 AWS Lambda 함수를 호출하도록 현재 모든 S3 버킷에 대한 S3 이벤트 알림을 구성합니다. Lambda 로그를 감사 로그 S3 버킷에 저장합니다.

D. AWS CloudTrail을 활성화하고 감사 로그 S3 버킷을 사용하여 로그 저장 S3 이벤트 소스, 현재 S3 버킷 및 향후 S3 버킷에 대한 데이터 이벤트 로깅을 활성화합니다.

Answer: D

Q16

북미의 한 금융 서비스 회사는 AWS에서 고객에게 새로운 온라인 웹 애플리케이션을 출시할 계획입니다. 이 회사는 Amazon EC2 인스턴스의 us-east-1 리전에서 애플리케이션을 시작할 예정입니다. 애플리케이션은 가용성이 높아야 하며 사용자 트래픽에 맞게 동적으로 확장되어야 합니다. 이 회사는 또한 액티브-패시브 장애 조치를 사용하여 us-west-1 리전에서 애플리케이션에 대한 재해 복구 환경을 구현하려고 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. us-east-1에 VPC를 생성하고 미국-서부-1에 VPC를 생성합니다. VPC 피어링 구성 us-east-1 VPC에서 두 VPC의 여러 가용 영역으로 확장되는 Application Load Balancer (ALB) 를 생성합니다. 두 VPC의 여러 가용 영역에 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 ALB 뒤에 배치합니다.

B. us-east-1에 VPC를 생성하고 미국-서부-1에 VPC를 생성합니다. us-east-1 VPC에서. 해당 VPC의 여러 가용 영역으로 확장되는 Application Load Balancer (ALB) 를 생성합니다. us-east-1 VPC의 여러 가용 영역에 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 ALB 뒤에 배치합니다. us-west-1 VPC에서 동일한 구성을 설정합니다. Amazon Route 53 호스팅 영역 생성 각 ALB에 대해 별도의 레코드 생성 상태 확인을 활성화하여 리전 간 고가용성을 보장합니다.

C. us-east-1에 VPC를 만들고 us-west-1에 VPC를 생성합니다. us-east-1 VPC에서는 해당 VPC의 여러 가용 영역에 걸쳐 확장되는 Application Load Balancer (ALB) 를 생성합니다. us-east-1 VPC의 여러 가용 영역에 EC2 인스턴스를 배포하는 Auto Scaling 그룹을 생성합니다. Auto Scaling 그룹을 ALB 뒤에 배치합니다. 미국-서부-1 VPC에서 동일한 구성을 설정합니다. Amazon Route 53 호스팅 영역을 생성합니다. 각 ALB에 대해 별도의 레코드 생성 상태 확인을 활성화하고 각 레코드에 대한 장애 조치 라우팅 정책을 구성합니다.

D. us-east-1에 VPC를 생성하고 미국-서부-1에 VPC를 생성합니다. VPC 피어링 구성 us-east-1 VPC에서 두 VPC의 여러 가용 영역에 EC2 인스턴스를 배포하는 Auto Scaling 그룹 생성에서 여러 가용 영역으로 확장되는 ALB (애플리케이션 로드 밸런서) 를 생성합니다.오토 스케일링 그룹을 ALB 뒤에 배치합니다. Amazon Route 53 호스트를 생성합니다. ALB에 대한 레코드를 생성합니다.

Answer: D

Q17

한 회사에서 Windows 파일 서버의 온프레미스에 데이터를 저장하고 있습니다. 이 회사는 매일 5GB의 새로운 데이터를 생산합니다. 이 회사는 Windows 기반 워크로드의 일부를 AWS로 마이그레이션했으며 클라우드의 파일 시스템에서 데이터를 사용할 수 있어야 했습니다. 이 회사는 이미 온프레미스 네트워크와 AWS 간에 AWS Direct Connect 연결을 구축했습니다.

회사에서 사용해야 하는 데이터 마이그레이션 전략은 무엇입니까?

A. AWS Storage Gateway의 파일 게이트웨이 옵션을 사용하여 기존 Windows 파일 서버를 교체하고 기존 파일 공유를 새 파일 게이트웨이로 지정합니다.

B. AWS DataSync를 사용하여 온프레미스 윈도우 파일 서버와 Amazon FSx 간에 데이터를 복제하는 일일 작업을 예약합니다.

C. AWS 데이터 파이프라인을 사용하여 온프레미스 Windows 파일 서버와 Amazon Elastic File System (Amazon EFS) 간에 데이터를 복제하는 일일 작업을 예약합니다.

D. AWS DataSync를 사용하여 온프레미스 Windows 파일 서버와 Amazon Elastic File System (Amazon EFS) 간에 데이터를 복제하는 일일 작업을 예약합니다.

Answer: B

Q18

한 대규모 교육 회사는 최근 여러 대학의 내부 애플리케이션에 대한 액세스를 제공하기 위해 Amazon Workspaces를 도입했습니다.　이 회사는 Windows용 Amazon FSx 파일 서버 타일 시스템에 사용자 프록시를 저장하고 있습니다.　Me 시스템은 DNS 별칭으로 구성되며 자체 관리형 Active Directory에 연결됩니다.　더 많은 사용자가 Workspaces를 사용하기 시작하면 로그인 시간이 허용되지 않는 수준으로 늘어납니다.　조사 결과 파일 시스템의 성능이 저하된 것으로 나타났습니다.　이 회사는 처리량이 16MBps인 HDD 스토리지에 파일 시스템을 만들었습니다.　솔루션 설계자는 정의된 유지 관리 기간 동안 파일 시스템의 성능을 향상시켜야 합니다.

최소한의 관리 노력으로 이러한 요구 사항을 충족하기 위해 솔루션 설계자가 수행해야 하는 작업은 무엇입니까?

A. AWS Backup을 사용하여 파일 시스템의 지정 시간 백업을 생성합니다. Windows 파일 서버 파일 시스템용 새 FSx로 백업을 복원합니다. 스토리지 유형으로 SSD 선택 처리 용량으로 32MBps를 선택합니다. 백업 및 복원 프로세스가 완료되면 DNS 별칭을 적절히 조정합니다.　원본 파일 시스템을 삭제합니다.

B. 파일 시스템에서 사용자 연결 해제 Amazon FSx 콘솔에서 처리 용량을 32MBps로 업데이트합니다. 스토리지 유형을 SSD로 업데이트 사용자를 파일 시스템에 다시 연결합니다.

C. AWS 데이터싱크 에이전트를 새 Amazon EC2 인스턴스에 배포합니다.　작업 만들기 기존 파일 시스템을 원본 위치로 구성 SSD 스토리지와 32MBps의 처리량을 대상 위치로 사용하여 Windows 파일 서버용 새 FSx 파일 시스템을 구성합니다.　작업 예약 작업이 완료되면 그에 따라 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

D. Windows PowerShell 명령을 사용하여 기존 파일 시스템에서 섀도 복사본을 사용하도록 설정합니다.　섀도 복제본 작업을 예약하여 파일 시스템의 시점 백업을 만듭니다.　이전 버전을 복원하도록 선택합니다.　SSD 스토리지 및 32MBps의 처리량을 사용하여 Windows 파일 서버용 새 FSx 파일 시스템 만들기 복사 작업이 완료되면 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

Answer: D

Q19

한 회사가 기존 온프레미스 시스템과 AWS의 새로운 백엔드 간에 하이브리드 솔루션을 구축하고 있습니다. 이 회사는 현재 IT 인프라의 상태를 모니터링하고 문제에 대한 대응을 자동화하는 관리 애플리케이션을 보유하고 있습니다. 이 회사는 소비된 AWS 서비스의 상태를 애플리케이션에 통합하려고 합니다. 애플리케이션은 HTTPS 엔드포인트를 사용하여 업데이트를 수신합니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 접근 방식은 무엇입니까?

A. 온프레미스 시스템에서 운영 이벤트를 수집하도록 AWS Systems Manager OpsCenter를 구성합니다. 온프레미스 관리 애플리케이션을 폐기하고 OpsCenter를 허브로 채택하십시오.

B. AWS Personal Health Dashboard에서 AWS Health이벤트의 변경 사항을 감지하고 이에 대응하도록 Amazon EventBridge (Amazon CloudWatch Events) 를 구성합니다. Amazon Simple Notification Service (Amazon SNS) 주제에 메시지를 게시하고 관리 애플리케이션의 HTTPS 엔드포인트에 주제를 구독하도록 EventBridge (CloudWatch 이벤트) 이벤트를 구성합니다.

C. AWS Health API를 호출하여 AWS 서비스의 상태 이벤트를 폴링하도록 온프레미스 관리 애플리케이션을 수정합니다.

D. AWS Service Health Dashboard에서 AWS 상태 이벤트의 변경 사항을 감지하고 이에 대응하도록 Amazon EventBridge (Amazon CloudWatch Events) 를 구성합니다. Amazon Simple Notification Service (Amazon SNS) 주제에 메시지를 게시하도록 EventBridge (CloudWatch Events) 이벤트를 구성하고, 사용 중인 서비스에 해당하는 주제 필터를 사용하여 관리 애플리케이션의 HTTPS 엔드포인트에 주제를 구독합니다.

Answer: B

Q20

한 회사가 온프레미스 환경에서 3계층 웹 애플리케이션을 호스팅하고 있습니다. 최근 트래픽이 급증하여 가동 중지 시간이 발생하고 상당한 재정적 영향이 발생했기 때문에 회사 경영진은 애플리케이션을 AWS로 이전하도록 명령했습니다. 응용 프로그램은 .NET으로 작성되었으며 MySQL 데이터베이스에 종속되어 있습니다. 솔루션 설계자는 20만 명의 일일 사용자 요구를 충족하기 위해 확장 가능하고 가용성이 높은 솔루션을 설계해야 합니다.

솔루션 설계자는 적절한 솔루션을 설계하기 위해 어떤 단계를 수행해야 합니까?

A. AWS Elastic Beanstalk를 사용하여 웹 서버 환경과 Amazon RDS MySQL 다중 AZ DB 인스턴스가 포함된 새 애플리케이션을 생성합니다. 환경에서는 여러 가용 영역에 있는 Amazon EC2 Auto Scaling 그룹 앞에서 Network Load Balancer (NLB)를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 NLB로 트래픽을 라우팅합니다.

B. AWS CloudFormation을 사용하여 3개의 가용 영역에 걸쳐 있는 Amazon EC2 오토 스케일링 그룹 앞에 Application Load Balancer (ALB)가 포함된 스택을 시작합니다. 스택은 삭제 유지 정책을 사용하여 Amazon Aurora MySQL DB 클러스터의 다중 AZ 배포를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 ALB로 트래픽을 라우팅합니다.

C. AWS Elastic Beanstalk를 사용하여 각 리전에 Application Load Balancer (ALB)가 있는 두 개의 개별 리전에 걸쳐 있는 자동으로 확장되는 웹 서버 환경을 생성합니다. 리전 간 읽기 전용 복제본이 있는 Amazon Aurora MySQL DB 클러스터의 다중 AZ 배포를 생성합니다. Amazon Route 53을 지리적 근접성 라우팅 정책과 함께 사용하여 두 리전 간에 트래픽을 라우팅합니다.

D. AWS CloudFormation을 사용하여 3개의 가용 영역에 걸쳐 있는 스팟 인스턴스의 Amazon ECS 클러스터 앞에 Application Load Balancer (ALB)가 포함된 스택을 시작합니다. 스택은 스냅샷 삭제 정책을 사용하여 Amazon RDS MySQL DB 인스턴스를 시작해야 합니다. Amazon Route 53 별칭 레코드를 사용하여 회사 도메인에서 ALB로 트래픽을 라우팅합니다.

Answer: B

Q21

한 회사의 보안 규정 준수 요구 사항에 따르면 모든 Amazon EC2 이미지의 취약성을 스캔하고 CVE 평가를 통과해야 합니다. 솔루션 설계자가 개발자가 사용할 수 있는 보안 승인 AMI를 생성하는 메커니즘을 개발하고 있습니다. 새로운 AMI는 자동화된 평가 프로세스를 거쳐 승인됨으로 표시되어야 개발자가 사용할 수 있습니다. 승인된 이미지는 규정 준수를 위해 30일마다 스캔해야 합니다.

솔루션 설계자가 모범 사례를 따르면서 이러한 요구 사항을 충족하기 위해 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. AWS 시스템 관리자 EC2 에이전트를 사용하여 스캔해야 하는 AMI에서 시작된 EC2 인스턴스에 대해 CVE 평가를 실행합니다.

B. AWS Lambda를 사용하여 자동 승인 규칙 작성 승인된 AMI 목록을 AWS 시스템 관리자 파라미터 스토어에 저장 Amazon EventBridge를 사용하여 30일마다 모든 EC2 인스턴스에서 AWS 시스템 관리자 자동화 문서를 트리거합니다.

C. Amazon 인스펙터를 사용하여 스캔해야 하는 AMI에서 시작된 EC2 인스턴스에 대해 CVE 평가를 실행합니다.

D. AWS Lambda를 사용하여 자동 승인 규칙 작성 승인된 AMI 목록을 AWS Systems Manager 파라미터 스토어에 저장 관리형 AWS Config 규칙을 사용하여 모든 EC2 인스턴스를 지속적으로 검색하고, 수정을 위해 AWS Systems Manager 자동화 문서를 사용합니다.

E. AWS CloudTrail을 사용하여 스캔해야 하는 AMI에서 시작된 EC2 인스턴스에 대해 CVE 평가를 실행합니다.

Answer: B, C

설명

AWS Lambda를 사용하여 AMI에 대한 승인 프로세스를 실행한 다음 결과를 AWS Systems Manager Parameter Store에 자동으로 저장할 수 있습니다.

CVE 평가의 경우 Amazon Inspector를 사용하여 CVE(Common Vulnerabilities and Exposures) 패키지와 같은 AWS 관리형 규칙 패키지를 사용하여 Amazon EC2 인스턴스의 보안 평가를 수행할 수 있습니다.

그런 다음 Amazon EventBridge(CloudWatch Events)를 사용하여 반복 일정(30일)에 따라 AWS Systems Manager Automation 문서를 실행하는 예약된 트리거를 생성할 수 있습니다. AWS Systems Manager는 실행 중인 인스턴스를 업데이트하여 적용해야 하는 보안 업데이트를 최신 상태로 유지합니다.

잘못됨: A. Systems Manager에는 CVE 평가가 없습니다. 이 목적을 위해 설계되고 패키지가 미리 구성된 Amazon Inspector를 사용하십시오.

잘못됨: D. Amazon Inspector는 CVE 평가에 더 적합합니다.

잘못됨: E. AWS CloudTrail는CVE 평가에는 적합하지 않습니다.

참조:

https://aws.amazon.com/blogs/security/how-to-set-up-continuous-golden-ami-vulnerability-assessments-with-amazon-inspector/

Q22

모바일 게임 회사가 글로벌 시장으로 확장하고 있습니다. 이 회사의 게임 서버는 us-east-1 지역에서 실행됩니다. 게임의 클라이언트 애플리케이션은 UDP를 사용하여 게임 서버와 통신하며 고정 IP 주소 집합에 연결할 수 있어야 합니다. 이 회사는 여러 대륙에서 게임에 액세스 할 수 있기를 원합니다. 이 회사는 또한 게임이 네트워크 성능과 글로벌 가용성을 유지하기를 원합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 게임 서버 앞에 Application Load Balancer (ALB) 를 프로비저닝합니다. 지리적 제한이 없는 Amazon CloudFront 배포를 생성합니다. ALB를 오리진으로 설정 CloudFront 넷 도메인 이름에 대해 DNS 조회를 수행합니다. 게임의 클라이언트 애플리케이션에서 결과 IP 주소를 사용합니다.

B. 각 AWS 리전에서 게임 서버를 프로비저닝합니다. 게임 서버 앞에 애플리케이션 로드 밸런서를 프로비저닝합니다. 게임의 클라이언트 애플리케이션이 DNS 조회에 사용할 Amazon Route 53 지연 시간 기반 라우팅 정책을 생성합니다.

C. 각 AWS 리전에 게임 서버 프로비저닝 게임 서버 앞에 Network Load Balancer (NLB) 를 프로비저닝합니다. AWS 글로벌 액셀러레이터에서 액셀러레이터를 생성하고 각 리전에 엔드포인트 그룹을 구성합니다. NLB와 해당 리전 엔드포인트 그룹을 연결합니다. 게임 클라이언트의 애플리케이션이 글로벌 액셀러레이터 엔드포인트를 가리키도록 합니다.

D. 각 AWS 리전에 게임 서버 프로비저닝 게임 서버 앞에 Network Load Balancer (NLB)를 프로비저닝합니다. 지리적 제한이 없는 Amazon CloudFront 배포를 생성합니다. NLB를 오리진으로 설정합니다. CloudFront 넷 도메인 이름에 대해 DNS 조회를 수행합니다. 게임의 클라이언트 애플리케이션에서 결과 IP 주소를 사용합니다.

Answer: C

Elastic Load Balancing은 이미 지원되는 TCP 프로토콜 외에도 Network Load Balancer에서 UDP 프로토콜을 지원합니다. 이번 출시로 Network Load Balancer 뒤에 인증 및 권한 부여, 로깅, DNS 및 IoT와 같은 UDP 프로토콜을 사용하는 서비스를 배포할 수 있으므로 짧은 지연 시간, 규모 및 안정성의 이점이 있습니다.

NLB(Network Load Balancer)는 UDP 프로토콜을 지원하며 애플리케이션 인스턴스 앞에 배치할 수 있습니다. 이 구성은 인스턴스가 프라이빗 서브넷에서 실행 중인 경우 보안을 추가할 수 있습니다.

Network Load Balancer는 다중 프로토콜 수신기도 제공하므로 Network Load Balancer 뒤의 동일한 포트에서 TCP 및 UDP 프로토콜을 사용하는 DNS와 같은 애플리케이션을 실행할 수 있습니다. 또한 Network Load Balancer는 클라이언트의 소스 IP를 백엔드 애플리케이션에 보존합니다.

Global Accelerator는 하나 이상의 AWS 리전에서 실행되는 애플리케이션에 에지에서 패킷을 프록시하여 TCP 또는 UDP를 통한 광범위한 애플리케이션의 성능을 향상시킵니다.

CloudFront는 캐시 가능한 콘텐츠와 동적 콘텐츠 모두의 성능을 향상시킵니다.

https://docs.aws.amazon.com/ko\_kr/elasticloadbalancing/latest/network/introduction.html

Q23

한 비디오 스트리밍 회사에서 최근 비디오 공유를 위한 모바일 앱을 출시했습니다. 이 앱은 us-east-1 리전의 Amazon S3 버킷에 다양한 파일을 업로드합니다. 파일 크기는 1GB에서 10GB까지 다양합니다. 호주에서 앱에 액세스하는 사용자는 시간이 오래 걸리는 업로드를 경험했습니다. 솔루션스 아키텍트는 이러한 업로드에 대해 앱의 성능을 개선해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?(두 개 선택)

A. S3 버킷에서 S3 Transfer Acceleration을 활성화합니다. 업로드에 Transfer Acceleration 엔드포인트를 사용하도록 앱을 구성합니다.

B. 업로드를 수신할 각 리전에서 S3 버킷을 구성합니다. S3 교차 리전 복제를 사용하여 파일을 배포 S3 버킷으로 복사합니다.

C. 지연 시간 기반 라우팅으로 Amazon Route 53을 설정하여 업로드를 가장 가까운 S3 버킷 리전으로 라우팅합니다.

D. 비디오 파일을 청크로 나누도록 앱을 구성합니다. 멀티파트 업로드를 사용하여 Amazon S3로 파일을 전송합니다.

E. 업로드하기 전에 파일에 임의의 접두사를 추가하도록 앱을 수정합니다.

Answer: A, D

설명

Amazon S3 Transfer Acceleration을 사용하면 클라이언트와 S3 버킷 간의 장거리 파일 전송을 빠르고 쉽고 안전하게 수행할 수 있습니다. Transfer Acceleration은 Amazon CloudFront의 전 세계에 분산된 엣지 로케이션을 활용합니다. 데이터가 엣지 로케이션에 도착하면 데이터는 최적화된 네트워크 경로를 통해 Amazon S3로 라우팅됩니다.

Transfer Acceleration은 다음 사용 사례에 적합한 솔루션입니다.

- 전 세계에서 중앙 집중식 버킷에 업로드하는 고객이 있습니다.

- 대륙에 걸쳐 정기적으로 기가바이트에서 테라바이트로 데이터를 전송합니다.

- Amazon S3에 업로드할 때 인터넷을 통해 사용 가능한 대역폭을 모두 활용할 수 없습니다.

멀티파트 업로드는 파일의 일부를 병렬로 전송하고 성능 속도를 높일 수 있습니다. 이것은 확실히 애플리케이션 코드에 내장되어야 합니다. 또한 멀티파트 업로드는 모든 부분의 오류를 정상적으로 처리하여 해당 부분이 재전송될 수 있도록 합니다.

멀티파트 업로드와 함께 Transfer Acceleration을 사용하면 데이터를 업로드할 때 속도가 크게 향상됩니다.

참조:

https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html

Q24

기업은 애플리케이션 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 여러 Amazon EC2 인스턴스에 분산되어 있는 애플리케이션을 운영합니다. 보안 팀에서 검사할 수 있도록 모든 애플리케이션 액세스 시도에 액세스할 수 있어야 합니다. 클라이언트의 IP 주소, 연결 종류 및 사용자 에이전트를 모두 제공해야 합니다.

이러한 기준을 충족하는 솔루션은 무엇입니까?

A. EC2 세부 모니터링을 활성화하고 네트워크 로그를 포함합니다. Amazon Kinesis 데이터 Firehose를 통해 보안 팀이 분석에 사용하는 Amazon Elasticsearch Service (Amazon ES) 클러스터로 모든 로그를 전송합니다.

B. 모든 EC2 인스턴스 네트워크 인터페이스에 대해 VPC 흐름 로그를 활성화합니다. VPC 흐름 로그를 Amazon S3 버킷에 게시합니다. 보안 팀에서 Amazon Athena를 사용하여 로그를 쿼리하고 분석하도록 합니다.

C. 애플리케이션 로드 밸런서에 대한 액세스 로그를 활성화하고 로그를 Amazon S3 버킷에 게시합니다. 보안 팀에서 Amazon Athena를 사용하여 로그를 쿼리하고 분석하도록 합니다.

D. 트래픽 미러링을 활성화하고 모든 EC2 인스턴스 네트워크 인터페이스를 소스로 지정합니다. Amazon Kinesis Data Firehose를 통해 모든 트래픽 정보를 보안 팀이 분석에 사용하는 Amazon Elasticsearch Service (Amazon ES) 클러스터로 전송합니다.

Answer: C

Q25

퍼블릭 리테일 웹 애플리케이션은 Amazon RDS MySQL 다중 AZ 배포가 지원되는 리전의 여러 가용 영역 (AZ) 에서 실행되는 Amazon EC2 인스턴스 앞에 애플리케이션 로드 밸런서 (ALB) 를 사용합니다. 대상 그룹 상태 확인은 HTTP를 사용하도록 구성되며 제품 카탈로그 페이지를 가리킵니다. Auto Scaling은 ALB 상태 확인을 기반으로 웹 집합 크기를 유지하도록 구성됩니다. 최근에 응용 프로그램이 중단되었습니다. 가동 중단 중에 Auto Scaling이 인스턴스를 지속적으로 교체했습니다. 후속 조사에서 웹 서버 메트릭이 정상 범위 내에 있지만 데이터베이스 계층에 높은 로드가 발생하여 쿼리 응답 시간이 크게 증가한 것으로 확인되었습니다.

다음 중 향후 성장을 위해 전체 애플리케이션 스택의 가용성 및 기능에 대한 모니터링 기능을 향상시키면서 이러한 문제를 해결할 수 있는 변경 사항은 무엇입니까?(두 개 선택)

A. Amazon RDS MySQL에 대한 읽기 전용 복제본을 구성하고 웹 애플리케이션에서 단일 리더 엔드포인트를 사용하여 백엔드 데이터베이스 티어의 로드를 줄입니다.

B. 대상 그룹 상태 확인이 제품 카탈로그 페이지 대신 간단한 HTML 페이지를 가리키도록 구성하고 Amazon Route 53 상태 확인을 제품 페이지에 대해 구성하여 전체 애플리케이션 기능을 평가합니다. 사이트에 장애가 발생할 경우 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.

C. 전체 애플리케이션 기능을 평가하기 위해 Amazon EC2 웹 서버의 TCP 검사와 제품 페이지에 대한 Amazon Route 53 상태 확인을 사용하도록 대상 그룹 상태 확인을 구성합니다. 사이트에 장애가 발생할 경우 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.

D. 데이터베이스 계층에서 부하가 높고 장애가 있는 RDS 인스턴스를 복구하는 작업을 사용하여 Amazon RDS에 대한 Amazon CloudWatch 경보를 구성합니다.

E. Amazon ElastiCache 클러스터를 구성하고 웹 애플리케이션과 RDS MySQL 인스턴스 사이에 배치하여 백엔드 데이터베이스 티어의 부하를 줄입니다.

Answer: B, E

Q26

한 회사가 AWS 클라우드에서 단일 페이지 웹 애플리케이션을 호스팅하고 있습니다. 이 회사는 Amazon CloudFront를 사용하여 목표 고객에게 도달하고 있습니다. CloudFront 배포에는 오리진으로 구성된 Amazon S3 버킷이 있습니다. 웹 애플리케이션의 정적 파일은 이 S3 버킷에 저장됩니다. 이 회사는 간단한 라우팅 정책을 사용하여 Amazon Route 53 A 레코드를 구성했습니다. 레코드는 CloudFront 배포를 가리킵니다. 이 회사는 새 버전의 응용 프로그램에 대해 canary 배포 릴리스 전략을 사용하려고 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 권장해야 합니까?

A. 애플리케이션의 새 버전에 대한 두 번째 CloudFront 배포를 생성합니다. 가중치 기반 라우팅 정책을 사용하도록 Route 53 레코드를 업데이트합니다.

B. 람다 @Edge 함수를 생성합니다. 가중치 알고리즘을 구현하도록 함수를 구성하고 URL을 다시 작성하여 사용자를 새 버전의 애플리케이션으로 안내합니다.

C. 새 S3 버킷에 대한 두 번째 S3 버킷과 두 번째 CloudFront 오리진을 생성합니다. 두 오리진을 모두 포함하는 CloudFront 오리진 그룹을 생성합니다. 오리진 그룹에 대한 오리진 웨이트를 구성합니다.

D. 두 개의 람다 @Edge 함수를 생성합니다. 각 함수를 사용하여 애플리케이션 버전 중 하나를 제공합니다. CloudFront 가중치 Lambda @Edge 호출 정책을 설정합니다.

Answer: A

Q27

한 회사에서 Amazon Athena 사용 비용을 관리하려고 합니다. 이 회사는 Athena 사용을 위해 특정 월 예산을 할당했습니다. 솔루션 설계자는 회사가 예산 금액을 초과하지 않도록 하는 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 예산을 사용합니다. Athena 사용 비용이 해당 월의 예산 금액에 도달하는 경우에 대한 경보를 생성합니다. 월말까지 Athena를 비활성화하도록 AWS 예산 작업을 구성합니다.

B. 비용 탐색기를 사용하여 Athena 사용 비용이 해당 월의 예산 금액에 도달하는 경우에 대한 경고를 생성합니다. Amazon Simple Notification Service (Amazon SNS) 주제에 알림을 게시하도록 비용 탐색기를 구성합니다.

C. AWS 트러스티드 어드바이저를 사용하여 Athena 사용 비용을 추적합니다. 비용이 해당 월의 예산 금액에 도달할 때마다 월말까지 Athena를 비활성화하도록 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 구성합니다.

D. Athena 작업 그룹을 사용하여 스캔할 수 있는 데이터 양에 대한 제한을 설정합니다. Athena의 월 예산 및 현재 가격에 적합한 한도를 설정하십시오.

Answer: D

Q28

한 개발자가 Amazon S3 버킷에서 객체를 다운로드하려고 할 때 오류 403: 액세스 거부 메시지가 표시된다고 보고합니다. S3 버킷은 VPC 내부의 S3 엔드포인트를 사용하여 액세스되며 AWS KMS 키로 암호화됩니다. 솔루션 설계자가 개발자가 계정에서 객체 다운로드를 허용하는 올바른 IAM 역할을 맡고 있음을 확인했습니다. S3 버킷 정책과 NACL도 유효합니다.

이 문제를 해결하기 위해 솔루션 설계자가 수행해야 하는 추가 단계는 무엇입니까?

A. S3 버킷에서 모든 퍼블릭 액세스 차단이 활성화되지 않았는지 확인합니다.

B. IAM 경로가 참조된 KMS 키를 해독할 수 있는 권한이 있는지 확인합니다.

C. IAM 역할에 올바른 신뢰 관계가 구성되어 있는지 확인합니다.

D. 로컬 방화벽 규칙으로 인해 S3 엔드포인트에 대한 액세스가 차단되지 않는지 확인합니다.

Answer: B

설명

IAM 사용자가 사용자에게 전체 권한이 있는 객체에 액세스할 수 없는 경우 객체가 AWS KMS로 암호화되었는지 확인하십시오. Amazon S3 콘솔을 사용하여 객체의 암호화 정보가 포함된 객체의 속성을 볼 수 있습니다.

객체가 KMS로 암호화된 경우 KMS 키 정책이 IAM 사용자에게 다음 작업에 대한 권한을 부여하는지 확인하십시오.

- "km:암호화"

- "km:복호화"

- "kms:ReEncrypt\*"

- "km:DataKey 생성\*"

- "km:DescribeKey"

잘못됨: A. 이는 공개 액세스의 경우가 아니며, 권한이 올바르게 설정된 IAM 역할을 사용하여 S3 버킷에 액세스하고 있습니다.

잘못됨: C. IAM 역할 신뢰 관계가 올바르게 구성되지 않은 경우 사용자는 역할을 수임할 수 없으며 질문에는 사용자가 역할을 수임했다고 나와 있습니다.

잘못됨: D. NACL이 유효하고 S3에서 액세스 거부 오류가 생성되고 있으며 방화벽에서 생성되지 않습니다.

참조:

https://aws.amazon.com/premiumsupport/knowledge-center/s3-troubleshoot-403/

Q29

한 회사가 JavaScript로 단일 페이지 웹 애플리케이션을 개발했습니다.소스 코드는 us-east-1 리전의 단일 Amazon S3 버킷에 저장됩니다. 이 회사는 Amazon CloudFront를 통해 글로벌 사용자 기반에 웹 애플리케이션을 제공합니다. 회사는 애플리케이션 사용자에게 알리지 않고 두 가지 버전의 웹 사이트를 실험하려고합니다. 웹 사이트의 각 버전은 자체 S3 버킷에 상주합니다. 이 회사는 신제품 마케팅에서 가장 성공적인 버전을 확인하려고 합니다. 솔루션은 유럽에 기반을 둔 애플리케이션 사용자를 새 웹 사이트 디자인으로 보내야 합니다. 솔루션은 미국에 기반을 둔 응용 프로그램 사용자를 현재 웹 사이트 디자인으로 보내야 합니다. 그러나 몇 가지 예외가 있습니다. 회사는 사용자의 위치에 관계없이 특정 사용자를 새 웹 사이트 디자인으로 리디렉션할 수 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 2개의 CloudFront 배포를 구성합니다. Amazon Route 53에서 지리적 위치 라우팅 정책을 구성하여 클라이언트의 위치를 기반으로 트래픽을 적절한 CloudFront 엔드포인트로 라우팅합니다.

B. 단일 CloudFront 배포를 구성합니다. 사이트의 각 버전에 대해 서로 다른 경로를 사용하여 비헤이비어를 만듭니다. 기본 경로에서 Lambda @Edge 를 구성하여 리디렉션을 생성하고 클라이언트를 올바른 버전의 웹 사이트로 보냅니다.

C. 단일 CloudFront 배포를 구성합니다. 배포에서 대체 도메인 이름을 구성합니다. 클라이언트가 HTTP 요청에서 사용하는 도메인 이름을 기반으로 사용자를 서로 다른 S3 오리진으로 라우팅하도록 두 가지 동작을 구성합니다.

D. Lambda @Edge 로 단일 CloudFront 배포를 구성합니다. Lambda @Edge 를 사용하여 요청 속성을 기반으로 여러 오리진에 사용자 요청을 보냅니다.

Answer: C

Q30

한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 애플리케이션 로드 밸런서 뒤의 여러 가용 영역에 있는 Amazon EC2 인스턴스 플릿에서 실행되는 마이크로서비스로 구성됩니다. 이 회사는 최근 Amazon API 게이트웨이에서 구현된 새로운 REST API를 추가했습니다. EC2 인스턴스에서 실행되는 일부 이전 마이크로서비스는 이 새 API를 호출해야 합니다. 이 회사는 퍼블릭 인터넷에서 API에 액세스하는 것을 원하지 않으며 독점 데이터가 퍼블릭 인터넷을 통과하는 것을 원하지 않습니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. VPC와 API 게이트웨이 간에 AWS 사이트 간 VPN 연결을 생성합니다. API Gateway를 사용하여 각 마이크로서비스에 대해 고유한 API 키를 생성합니다. 키를 요구하도록 API 메서드를 구성합니다.

B. API Gateway용 인터페이스 VPC 엔드포인트를 생성하고 특정 API에 대한 액세스만 허용하도록 엔드포인트 정책을 설정합니다. VPC 엔드포인트에서의 액세스만 허용하도록 API Gateway에 리소스 정책을 추가합니다.

C. IAM 인증을 사용하도록 API 게이트웨이 수정 API 게이트웨이에 대한 액세스를 허용하도록 EC2 인스턴스에 할당된 IAM 역할에 대한 IAM 정책을 업데이트합니다. API 게이트웨이를 새 VPC로 이동 전송 게이트웨이를 배포하고 VPC를 연결합니다.

D. AWS Global Accelerator에서 Accelerator를 생성하고 Accelerator를 API 게이트웨이에 연결합니다. 생성된 Global Accelerator 엔드포인트 IP 주소에 대한 경로를 사용하여 모든 VPC 서브넷의 라우팅 테이블을 업데이트합니다. 인증에 사용할 각 서비스에 대한 API 키를 추가합니다.

Answer: B

https://docs.aws.amazon.com/ko\_kr/apigateway/latest/developerguide/apigateway-private-apis.html

Q31

교육 회사는 전 세계 대학생들이 사용하는 웹 애플리케이션을 실행하고 있습니다. 애플리케이션은 애플리케이션 로드 밸런서 (ALB) 뒤에 있는 Auto Scaling 그룹의 Amazon Elastic Container Service (Amazon ECS) 클러스터에서 실행됩니다. 시스템 관리자는 실패한 로그인 시도 횟수가 매주 급증하는 것을 감지하여 응용 프로그램의 인증 서비스를 압도합니다. 실패한 모든 로그인 시도는 매주 변경되는 약 500개의 서로 다른 IP 주소에서 발생합니다. 솔루션 설계자는 실패한 로그인 시도가 인증 서비스를 압도하는 것을 방지해야 합니다.

운영 효율성이 가장 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 방화벽 관리자를 사용하여 IP 주소로부터의 액세스를 거부하는 보안 그룹 및 보안 그룹 정책을 생성합니다.

B. 속도 기반 규칙을 사용하여 AWS WAF 웹 ACL을 생성하고 규칙 작업을 차단으로 설정합니다. 웹 ACL을 ALB에 연결합니다.

C. AWS 방화벽 관리자를 사용하여 특정 CIOR 범위에 대한 액세스만 허용하는 보안 그룹 및 보안 그룹 정책을 생성합니다.

D. IP 집합 일치 규칙이 있는 AWS WAF 웹 ACL을 생성하고 규칙 작업을 차단으로 설정합니다. 웹 ACL을 ALB에 연결합니다.

Answer: B

Q32

회사에서 레스토랑 리뷰 웹 사이트를 유지 관리합니다. 이 웹 사이트는 파일이 Amazon S3에 저장되고 Amazon CloudFront를 사용하여 전송되는 단일 페이지 애플리케이션입니다. 회사는 매일 수동으로 제거되는 여러 개의 가짜 게시물을 수신합니다. 보안 팀은 대부분의 가짜 게시물이 동일한 글로벌 지역 내에서 평판이 좋지 않은 IP 주소를 가진 봇의 게시물임을 확인했습니다. 팀은 봇이 웹 사이트에 액세스하지 못하도록 제한하는 솔루션을 만들어야 합니다.

솔루션 설계자는 어떤 전략을 사용해야 합니까?

A. AWS 방화벽 관리자를 사용하여 CloudFront 배포 보안 설정을 제어합니다. 지리적 차단 규칙을 만들어 방화벽 관리자와 연결합니다.

B. AWS WAF 웹 ACL을 CloudFront 배포와 연결합니다. 거부 작업이 있는 웹 ACL에 대한 관리형 Amazon IP 평판 규칙 그룹을 선택합니다.

C. AWS 방화벽 관리자를 사용하여 CloudFront 배포 보안 설정을 제어합니다. 관리형 Amazon IP 평판 규칙 그룹을 선택하고 거부 작업을 통해 방화벽 관리자와 연결합니다.

D. AWS WAF 웹 ACL을 CloudFront 배포와 연결합니다. 거부 작업이 있는 지리적 일치 문을 사용하여 웹 ACL에 대한 규칙 그룹을 만듭니다.

Answer: B

Q33

한 금융 회사가 현재 세대의 Linux EC2 인스턴스에서 비즈니스 크리티컬 애플리케이션을 실행하고 있습니다. 이 애플리케이션에는 대량의 I/O 작업을 수행하는 자체 관리형 MySQL 데이터베이스가 포함되어 있습니다. 한 달 동안 적당한 양의 트래픽을 처리하기 위해 응용 프로그램이 제대로 작동합니다. 그러나 증가하는 수요를 충족하기 위해 인프라 내에서 Elastic Load Balancer와 Auto Scaling을 사용하고 있더라도 월말 보고로 인해 매월 마지막 3일 동안에는 속도가 느려집니다.

다음 중 데이터베이스가 성능에 미치는 영향을 최소화하면서 월말 로드를 처리할 수 있는 작업은 무엇입니까?

A. 탄력적 로드 밸런서를 사전 워밍하고 더 큰 인스턴스 유형을 사용하여 모든 Amazon EBS 볼륨을 GP2 볼륨으로 변경합니다.

B. 데이터베이스 클러스터를 Amazon RDS로 일회성 마이그레이션하고 월말에 로드를 처리하기 위해 여러 개의 추가 읽기 전용 복제본을 생성합니다.

C. AWS Lambda와 함께 Amazon CioudWatch를 사용하여 특정 CloudWatch 지표를 기반으로 클러스터에 있는 Amazon EBS 볼륨의 유형, 크기 또는 IOPS를 변경합니다.

D. 월말 전에 스냅샷을 생성한 후 나중에 되돌려 기존 Amazon EBS 볼륨을 사용 가능한 최대 스토리지 크기와 초당 I/O를 가진 새 PIOPS 볼륨으로 교체합니다.

Answer: B

Q34

한 회사에서 AWS 조직을 사용하여 1,000개 이상의 AWS 계정을 관리합니다. 이 회사는 새로운 개발자 조직을 만들었습니다. 새 개발자 조직으로 이동해야 하는 540개의 개발자 멤버 계정이 있습니다. 모든 계정은 필요한 모든 정보로 설정되므로 각 계정을 독립 실행형 계정으로 운영할 수 있습니다.

솔루션 설계자가 모든 개발자 계정을 새 개발자 조직으로 이전하기 위해 수행해야 하는 단계는 무엇입니까?(세 개 선택)

A. 이전 조직의 관리 계정에서 조직 API에서 MoveAccount 작업을 호출하여 개발자 계정을 새 개발자 조직으로 마이그레이션합니다.

B. 관리 계정에서 조직 API의 조직에서 계정 제거 작업을 사용하여 이전 조직의 각 개발자 계정을 제거합니다.

C. 각 개발자 계정에서 조직 API의 조직에서 계정 제거 작업을 사용하여 이전 조직의 계정을 제거합니다.

D. 새 개발자 기관의 관리 계정에 로그인하고 개발자 계정 마이그레이션의 대상 역할을 하는 자리 표시자 구성원 계정을 만듭니다.

E. 새 개발자 조직의 관리 계정에서 조직 API의 조직 간 초대 작업을 호출하여 개발자 계정에 초대를 보냅니다.

F. 각 개발자가 자신의 계정에 로그인하고 새 개발자 조직에 가입하도록 확인합니다.

Answer: B, D, E

Q35

한 회사의 사이트 안정성 엔지니어가 회사가 인수한 계정 내에서 Windows 파일 서버용 Amazon FSx 배포를 검토하고 있습니다. 회사 정책에 따르면 모든 Amazon FSx 파일 시스템은 가용 영역 전체에서 고가용성을 유지하도록 구성해야 합니다. 검토 중에 사이트 안정성 엔지니어는 Amazon FSx 파일 시스템 중 하나가 단일 AZ 2의 배포 유형을 사용했음을 발견했습니다. 솔루션 설계자는 이 Amazon FSx 파일 시스템을 회사 정책에 맞게 조정하면서 가동 중지 시간을 최소화해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 이 Amazon FSx 타일 시스템에 대해 배포 유형을 다중 AZ로 재구성합니다.

B. 배포 유형이 다중 AZ인 새 Amazon FSx 파일 시스템을 생성합니다. AWS DataSync를 사용하여 데이터를 새로운 Amazon FSx 파일 시스템으로 전송합니다. 사용자에게 새 위치를 안내합니다.

C. 배포 유형이 단일 AZ 2인 두 번째 Amazon FSx 파일 시스템을 생성합니다. AWS DataSync를 사용하여 데이터를 동기화된 상태로 유지합니다. 장애 발생 시 사용자를 두 번째 Amazon FSx 파일 시스템으로 전환합니다.

D. AWS 관리 콘솔을 사용하여 Amazon FSx 파일 시스템을 백업합니다. 배포 유형이 다중 AZ인 새 Amazon FSx 파일 시스템을 생성합니다. 백업을 새 Amazon FSx 파일 시스템으로 복원합니다. 사용자에게 새 위치를 안내합니다.

Answer: B

Q36

한 회사가 여러 AWS 계정에서 AWS WAF 규칙을 관리하기 위해 AWS WAF 솔루션을 배포하려고 합니다. 계정은 AWS 조직의 서로 다른 OU에서 관리됩니다. 관리자는 필요에 따라 관리형 AWS WAF 규칙 세트에서 계정 또는 OU를 추가하거나 제거할 수 있어야 합니다. 또한 관리자는 모든 계정에서 규정을 준수하지 않는 AWS WAF 규칙을 자동으로 업데이트하고 수정할 수 있어야 합니다.

운영 오버헤드가 가장 적은 상태에서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 방화벽 관리자를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리합니다. AWS Systems Manager 파라미터 스토어 파라미터를 사용하여 관리할 계정 번호와 OU를 저장합니다. 필요에 따라 파라미터를 업데이트하여 계정 또는 OU를 추가하거나 제거합니다. Amazon EventBridge (Amazon CloudWatch Events) 규칙을 사용하여 파라미터에 대한 변경 사항을 식별하고 AWS Lambda 함수를 호출하여 방화벽 관리자 관리 계정의 보안 정책을 업데이트합니다.

B. 선택한 OU의 모든 리소스가 AWS WAF 규칙을 연결하도록 요구하는 조직 전체의 AWS Config규칙을 배포합니다. AWS Lambda를 사용하여 규정 미준수 리소스를 수정하여 자동화된 수정 작업을 배포합니다. AWS 구성 규칙이 적용되는 동일한 OU를 대상으로 하는 AWS CloudFormation 스택 세트를 사용하여 AWS WAF 규칙을 배포합니다.

C. 조직의 관리 계정에 AWS WAF 규칙을 생성합니다. AWS Lambda 환경 변수를 사용하여 계정 번호와 OU를 저장하여 관리 계정 또는 OU를 추가하거나 제거하는 데 필요한 경우 환경 변수 업데이트 멤버 계정에 교차 계정 IAM 역할을 생성합니다. 멤버 계정에서 AWS WAF 규칙을 생성하고 업데이트하기 위해 Lambda 함수에서 AWS 보안 토큰 서비스 (AWS STS) 를 사용하여 역할을 가정하십시오.

D. AWS 컨트롤 타워를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리합니다. AWS 키 관리 서비스 (AWS KMS) 를 사용하여 계정 번호와 OU를 저장하여 계정 또는 OU를 추가하거나 제거하는 데 필요한 경우 AWS KMS 업데이트를 관리합니다. 멤버 계정에서 IAM 사용자 생성 관리 계정의 AWS Control Tower가 액세스 키와 보안 액세스 키를 사용하여 멤버 계정에서 AWS WAF 규칙을 생성하고 업데이트할 수 있도록 허용합니다.

Answer: B

Q37

멀티 플레이어 온라인 게임을 설계하는 회사는 유럽 이외의 지역으로 사용자 기반을 확장하려고합니다. 회사는 상당한 양의 UDP 트래픽을 게임의 모든 실시간 및 대화 형 세션을 유지하기 위해 전송합니다. 이 회사는 빠른 확장을 계획하고 있으며 사용자에게 최적화 된 온라인 경험을 제공하기 위해 아키텍처를 구축하고자합니다.

사용자의 지연 시간이 가장 낮은 이러한 요구 사항을 충족하는 아키텍처는 무엇입니까?

A. 단일 AWS 리전에 다중 AZ 환경을 설정합니다. Amazon CloudFront를 사용하여 사용자 세션을 캐싱합니다.

B. 여러 AWS 리전에 환경 설정 AWS 글로벌 액셀러레이터에서 액셀러레이터를 생성하고 다른 리전의 엔드포인트를 여기에 추가합니다.

C. 여러 AWS 리전에 환경을 설정합니다. Amazon Route 5.3를 사용하고 지연 시간 기반 라우팅을 선택합니다.

D. 단일 AWS 리전에 다중 AZ 환경을 설정합니다. AWS Lambda @Edge 를 사용하여 사용자에게 더 가까운 곳에서 세션을 업데이트합니다.

Answer: B

Q38

한 의료 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 이 응용 프로그램은 개발중인 의약품의 효과를 시뮬레이션합니다. 응용 프로그램은 구성과 시뮬레이션의 두 부분으로 구성됩니다. 구성 부분은 Amazon Elastic Container Service (Amazon ECS) 클러스터의 AWS Fargate 컨테이너에서 실행됩니다. 시뮬레이션 부분은 대규모 컴퓨팅 최적화 Amazon EC2 인스턴스에서 실행됩니다. 시뮬레이션이 중단되면 다시 시작할 수 있습니다. 구성 부품은 일정한 부하로 하루 24시간 실행됩니다. 시뮬레이션 부품은 가변 부하로 매일 밤 몇 시간 동안만 실행됩니다. 이 회사는 시뮬레이션 결과를 Amazon S3에 저장하고 연구원들은 30일 동안 결과를 사용합니다. 회사는 시뮬레이션을 10년 동안 보관해야 하며 5시간 이내에 시뮬레이션을 검색할 수 있어야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. EC2 인스턴스 절약 플랜을 구매하여 구성 부분의 사용량을 충당합니다. EC2 스팟 인스턴스를 사용하여 시뮬레이션 부분 실행 S3 수명 주기 정책을 생성하여 30일이 넘은 객체를 S3 인텔리전트 계층화로 전환합니다.

B. EC2 인스턴스 절감 플랜을 구매하여 구성 부분과 시뮬레이션 부분의 사용량을 충당합니다. 30일 이상 오래된 객체를 S3 Glacier로 이전하는 S3 수명 주기 정책을 생성합니다.

C. Compute Savings 플랜을 구매하여 구성 부분의 사용량을 충당합니다. EC2 스팟 인스턴스를 사용하여 시뮬레이션 부분을 실행합니다. 30일 이상 오래된 객체를 S3 Glacier로 이전하는 S3 수명 주기 정책을 생성합니다.

D. Compute Savings Plans를 구매하여 구성 부분의 사용량을 충당합니다. 시뮬레이션 부분에 대해 EC2 예약 인스턴스를 구매합니다. 30일 이상 오래된 객체를 S3 Glacier Deep Archive로 전환하는 S3 수명 주기 정책을 생성합니다.

Answer: C

Q39

한 회사가 글로벌 확장성 및 성능을 위해 Amazon CloudFront를 활용하는 복잡한 웹 애플리케이션을 보유하고 있습니다. 시간이 지남에 따라 사용자는 웹 애플리케이션의 속도가 느려지고 있다고 보고합니다. 이 회사의 운영 팀은 CloudFront 캐시 적중률이 꾸준히 떨어지고 있다고 보고했습니다. 캐시 메트릭 보고서는 일부 URL의 쿼리 문자열이 일관되지 않은 순서로 정렬되어 있으며 경우에 따라 대소문자로, 경우에 따라 소문자로 지정되기도 합니다.

캐시 적중률을 최대한 빨리 높이기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?

A. Lambda @Edge 함수를 배포하여 파라미터를 이름별로 정렬하고 강제로 소문자로 지정합니다. CloudFront 뷰어 요청 트리거를 선택하여 함수를 호출합니다.

B. CloudFront 배포를 업데이트하여 쿼리 문자열 파라미터에 따라 캐싱을 비활성화합니다.

C. 로드 밸런서 다음에 역방향 프록시를 배포하여 URL 문자열을 소문자로 강제하도록 애플리케이션에서 전송된 URL을 사후 처리합니다.

D. CloudFront 배포를 업데이트하여 대/소문자를 구분하지 않는 쿼리 문자열 처리를 지정합니다.

Answer: A

Q40

한 회사가 AWS에서 서비스형 소프트웨어 (SaaS) 애플리케이션을 실행합니다. 애플리케이션은 AWS Lambda 함수와 MySQL용 Amazon RDS 다중 AZ 데이터베이스를 기반으로 합니다. 시장 이벤트가 진행되는 동안 애플리케이션의 워크로드는 평소보다 훨씬 높습니다. 사용자는 많은 데이터베이스 연결로 인해 피크 기간 동안 응답 시간이 느리다는 것을 알 수 있습니다. 회사는 데이터베이스의 확장 가능한 성능과 가용성을 개선해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 리소스 사용률이 임계값에 도달하면 Lambda 함수를 트리거하여 MySQL용 Amazon RDS 읽기 전용 복제본을 추가하는 Amazon CloudWatch 경보 작업을 생성합니다.

B. 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Lambda hardier 함수 외부에 데이터베이스 연결 풀을 추가합니다.

C. 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Amazon Route 53 가중치 기반 레코드를 사용합니다.

D. 데이터베이스를 Amazon Aurora로 마이그레이션하고 Aurora 복제본을 추가합니다. 데이터베이스 연결 풀을 관리하도록 Amazon RDS 프록시를 구성합니다.

Answer: D

Q41

회사에는 여러 사업부가 있습니다. 각 사업부에는 자체 AWS 계정이 있으며 해당 계정 내에서 단일 웹 사이트를 실행합니다. 이 회사에는 단일 로깅 계정도 있습니다. 각 사업부 웹 사이트의 로그는 로깅 계정의 단일 Amazon S3 버킷으로 집계됩니다. S3 버킷 정책은 각 사업부에 버킷에 데이터를 쓸 수 있는 액세스 권한을 제공하며 데이터를 암호화해야 합니다. 회사는 단일 AWS Key Management Service(AWS KMS) CMK를 사용하여 버킷에 업로드된 로그를 암호화해야 합니다. 데이터를 보호하는 CMK는 365일에 한 번씩 교체해야 합니다.

회사가 이러한 요구 사항을 충족하기 위해 사용하는 데 가장 효율적인 전략은 무엇입니까?

A. 로깅 계정에서 고객 관리형 CMK 만들기 로깅 계정에만 액세스할 수 있도록 CMK 키 정책을 업데이트합니다. 365일마다 CMK를 수동으로 교체합니다.

B. 로깅 계정에서 고객 관리 CMK를 생성합니다. CMK 키 정책을 업데이트하여 로깅 계정 및 사업부 계정에 대한 액세스를 제공합니다. CMK의 자동 회전을 활성화합니다.

C. 전환 계정에서 AWS 관리형 CMK를 사용합니다. 로깅 계정 및 사업부 계정에 대한 액세스 권한을 제공하도록 CMK 키 정책을 업데이트합니다. 365일마다 CMK를 수동으로 교체합니다.

D. 전환 계정에서 AWS 관리형 CMK를 사용합니다. 전환 계정에만 액세스할 수 있도록 CMK 키 정책을 업데이트합니다. CMK의 자동 회전을 활성화합니다.

Answer: B

Q42

한 회사에서 애플리케이션을 AWS 클라우드로 마이그레이션하고 있습니다.이 애플리케이션은 온프레미스 데이터 센터에서 실행되며 매일 밤 마운트된 NFS 파일 시스템에 수천 개의 이미지를 기록합니다. 이 회사는 애플리케이션을 마이그레이션한 후 Amazon Elastic File System (Amazon EFS) 파일 시스템이 탑재된 Amazon EC2 인스턴스에서 애플리케이션을 호스팅합니다. 이 회사는 마이그레이션 전환 전에 AWS에 대한 AWS Direct Connect 연결을 설정했습니다. 솔루션 설계자는 새로 생성된 온프레미스 이미지를 EFS 파일 시스템에 복제하는 프로세스를 구축해야 합니다.

이미지를 복제하는 가장 효율적인 운영 방법은 무엇입니까?

A. 온프레미스 파일 시스템에서 Amazon S3로 AWS S3 sync 명령을 실행하도록 주기적인 프로세스를 구성합니다. Amazon S3의 이벤트 알림을 처리하고 Amazon S3에서 EFS 파일 시스템으로 이미지를 복사하도록 AWS Lambda 함수를 구성합니다.

B. NFS 마운트 포인트와 함께 AWS 스토리지 게이트웨이 파일 게이트웨이를 배포합니다. 온프레미스 서버에 파일 게이트웨이 파일 시스템을 마운트합니다. 이미지를 마운트 지점에 주기적으로 복사하는 프로세스를 구성합니다.

C. NFS 파일 시스템에 액세스할 수 있는 온프레미스 서버에 AWS DataSync 에이전트를 배포합니다. 퍼블릭 VIF를 사용하여 직접 연결 연결을 통해 S3 버킷으로 데이터를 전송합니다. Amazon S3의 이벤트 알림을 처리하고 Amazon S3에서 EFS 파일 시스템으로 이미지를 복사하도록 AWS Lambda 함수를 구성합니다.

D. NFS 파일 시스템에 액세스할 수 있는 온프레미스 서버에 AWS DataSync 에이전트를 배포합니다. 프라이빗 VIF를 사용하여 직접 연결 연결을 통해 Amazon EFS의 AWS 프라이빗 링크 인터페이스 VPC 엔드포인트로 데이터를 전송합니다. 24시간마다 이미지를 EFS 파일 시스템으로 전송하도록 DataSync 예약 작업을 구성합니다.

Answer: A

Q43

한 회사에서 온프레미스 데이터 센터에서 AWS로 레거시 애플리케이션을 마이그레이션하고 있습니다. 응용 프로그램은 MongoDB를 키-값 데이터베이스로 사용합니다. 이 회사의 기술 지침에 따르면 모든 Amazon EC2 인스턴스는 인터넷 연결 없이 프라이빗 서브넷에서 호스팅되어야 하며, 애플리케이션과 데이터베이스 간의 모든 연결은 암호화되어야 합니다. 데이터베이스는 수요에 따라 확장할 수 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 프로비저닝된 IOPS 볼륨이 있는 애플리케이션에 대해 새 Amazon DocumentDB (MongoDB 호환성 포함) 테이블을 생성합니다. 인스턴스 엔드포인트를 사용하여 Amazon DocumentDB에 연결합니다.

B. 온디맨드 용량이 있는 애플리케이션에 대한 새 Amazon DynamoDB 테이블을 생성합니다. DynamoDB용 게이트웨이 VPC 엔드포인트를 사용하여 DynamoDB 테이블로 연결합니다.

C. 온디맨드 용량이 있는 애플리케이션에 대한 새 Amazon DynamoDB 테이블을 생성합니다. DynamoDB에 대한 인터페이스 VPC 엔드포인트를 사용하여 DynamoDB 테이블에 연결합니다.

D. 프로비저닝된 IOPS 볼륨이 있는 애플리케이션에 대해 새 Amazon DocumentDB (MongoDB 호환성 포함) 테이블을 생성합니다. 클러스터 엔드포인트를 사용하여 Amazon DocumentDB에 연결합니다.

Answer: C

Q44

전자 상거래 비즈니스는 IT 인프라를 현대화하고 있으며 AWS 서비스를 사용할 계획입니다. 이 회사의 최고 정보 책임자 (CIO) 는 솔루션 설계자에게 단순하고 가용성이 높으며 느슨하게 연결된 주문 처리 애플리케이션을 설계하는 임무를 맡았습니다. 주문은 Amazon DynamoDB 데이터베이스에 저장되기 전에 애플리케이션에서 수신 및 처리됩니다. 애플리케이션은 간헐적으로 트래픽을 수신하며 주문을 신속하게 처리하기 위해 마케팅 캠페인 중에 증가할 수 있어야 합니다.

다음 중 요구 사항을 충족하는 데 가장 책임감 있는 방법은 무엇입니까?

A. Amazon EC2 호스팅 데이터베이스에서 주문을 받고 EC2 인스턴스를 사용하여 처리합니다.

B. Amazon SQS 대기열에서 주문을 수신하고 AWS Lambda 함수를 트리거하여 주문을 처리합니다.

C. AWS 스텝 함수 프로그램을 사용하여 주문을 수신하고 Amazon ECS 컨테이너를 트리거하여 주문을 처리합니다.

D. Amazon Kinesis 데이터 스트림에서 주문을 수신하고 Amazon EC2 인스턴스를 사용하여 주문을 처리합니다.

Answer: B

Q45

팀은 회사 전체의 행동 데이터를 수집하고 라우팅합니다. 이 회사는 퍼블릭 서브넷, 프라이빗 서브넷 및 인터넷 게이트웨이가 있는 다중 AZ VPC 환경을 실행합니다. 각 퍼블릭 서브넷에는 NAT 게이트웨이도 포함되어 있습니다. 대부분의 워크로드는 프라이빗 서브넷에서 실행됩니다. 솔루션 설계자는 인프라를 검토해야 합니다. 솔루션 설계자는 비용을 줄이고 애플리케이션의 기능을 유지해야 합니다. 솔루션 설계자는 비용 탐색기를 사용하여 EC2 기타 범주의 비용이 지속적으로 높다는 것을 알고 있습니다. 추가 검토에 따르면 NATgateway-bytes 요금은 EC2 기타 범주의 비용을 증가시키고 있습니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. VPC 흐름 로그를 활성화합니다. Amazon Athena를 사용하여 제거할 수 있는 트래픽의 로그를 분석합니다. 보안 그룹이 높은 비용을 초래하는 트래픽을 차단하고 있는지 확인합니다.

B. Kinesis 데이터 스트림용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. 애플리케이션에 인터페이스 VPC 엔드포인트를 사용할 수 있는 올바른 IAM 권한이 있는지 확인합니다.

C. VPC 흐름 로그와 Amazon Detective을 활성화합니다. Kinesis Data Streams와 관련이 없는 트래픽에 대한 탐지 결과 검토 해당 트래픽을 차단하도록 보안 그룹을 구성합니다.

D. Kinesis 데이터 스트림용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. VPC 엔드포인트 정책이 애플리케이션의 트래픽을 허용하는지 확인합니다.

Answer: D

Q46

한 솔루션 설계자가 Amazon S3 웹 사이트 엔드포인트를 오리진으로 사용하여 Amazon CloudFront 배포에 있는 공개적으로 액세스 가능한 웹 애플리케이션을 설계하고 있습니다. 솔루션이 배포되면 웹 사이트에서 오류 403: 액세스 거부 메시지를 반환합니다.

솔루션 설계자가 문제를 해결하기 위해 취해야 하는 단계는 무엇입니까?(두 개 선택)

A. S3 버킷에서 S3 블록 퍼블릭 액세스 옵션을 제거합니다.

B. S3 버킷에서 요청자 지불 옵션을 제거합니다.

C. CloudFront 배포에서 원본 액세스 ID (OAI) 를 제거합니다.

D. 스토리지 클래스를 S3 Standard에서 S3 One Zone-Infrequent Access (S3 One Zone-IA) 로 변경합니다.

E. S3 객체 버전 관리를 비활성화합니다.

Answer: A, B

설명

CloudFront 배포에서 웹 사이트 엔드포인트를 사용하는 경우 액세스 거부 오류를 방지하려면 다음 요구 사항을 확인하십시오.

• 버킷의 객체는 공개적으로 액세스할 수 있어야 합니다.

• 버킷의 객체는 AWS Key Management Service(AWS KMS)로 암호화할 수 없습니다.

• 버킷 정책은 s3:GetObject에 대한 액세스를 허용해야 합니다.

• 버킷 정책이 퍼블릭 읽기 액세스 권한을 부여하는 경우 버킷을 소유한 AWS 계정도 객체를 소유해야 합니다.

• 요청된 객체는 버킷에 있어야 합니다.

• 버킷에서 Amazon S3 퍼블릭 액세스 차단을 비활성화해야 합니다.

• 요청자 지불이 활성화된 경우 요청에 request-payer 매개변수가 포함되어야 합니다.

• Referer 헤더를 사용하여 CloudFront에서 S3 오리진으로의 액세스를 제한하는 경우 사용자 지정 헤더를 검토하십시오.

https://aws.amazon.com/ko/premiumsupport/knowledge-center/s3-website-cloudfront-error-403/

Q47

기업은 하이브리드 DNS 솔루션을 설계해야 합니다. 이 솔루션은 도메인 cloud.example.com에 대해 Amazon Route 53 프라이빗 호스팅 영역을 사용하여 VPC 내부에 포함된 리소스에 액세스합니다. 회사의 DNS 확인 기준은 다음과 같습니다.

\* 온프레미스 시스템은 cloud.example.com을 확인하고 연결할 수 있어야 합니다.

\* 모든 VPC는 cloud.example.com을 해결할 수 있어야 합니다.

온프레미스 기업 네트워크와 AWS 트랜짓 게이트웨이 사이에는 AWS Direct Connect 링크가 이미 존재합니다.

이러한 기준이 가능한 최고의 성능으로 충족되도록 하려면 어떤 아키텍처를 채택해야 합니까?

A. 프라이빗 호스팅 영역을 모든 VPC에 연결합니다. 공유 서비스 VPC에서 Route 53 인바운드 확인자를 생성합니다. 모든 VPC를 전송 게이트웨이에 연결하고 cloud.example.com용 온프레미스 DNS 서버에서 인바운드 확인자를 가리키는 전달 규칙을 만듭니다.

B. 프라이빗 호스팅 영역을 모든 VPC에 연결합니다. 공유 서비스 VPC에 Amazon EC2 조건부 전달자를 배포합니다. 모든 VPC를 전송 게이트웨이에 연결하고 cloud.example.com용 온프레미스 DNS 서버에서 조건부 전달자를 가리키는 전달 규칙을 만듭니다.

C. 프라이빗 호스팅 영역을 공유 서비스 VPC에 연결합니다. 공유 서비스 VPC에서 Route 53 아웃바운드 확인자를 생성합니다. 모든 VPC를 전송 게이트웨이에 연결하고 cloud.example.com의 온-프레미스 DNS 서버에서 아웃바운드 확인 프로그램을 가리키는 전달 규칙을 만듭니다.

D. 프라이빗 호스팅 영역을 공유 서비스 VPC에 연결합니다. 공유 서비스 VPC에서 Route 53 인바운드 확인자를 생성합니다. 공유 서비스 VPC를 전송 게이트웨이에 연결하고 cloud.example.com용 온프레미스 DNS 서버에서 인바운드 해석기를 가리키는 전달 규칙을 생성합니다.

Answer: A

Q48

한 회사가 API를 AWS에 배포하려고 합니다. 이 회사는 로드 밸런서 뒤에서 AWS Fargate에서 API를 실행할 계획입니다. API를 사용하려면 헤더 기반 라우팅을 사용해야 하며 AWS Direct Connect 연결 및 프라이빗 VIF를 통해 온프레미스 네트워크에서 액세스할 수 있어야 합니다. 회사는 API에 연결하는 클라이언트 IP 주소를 AWS의 허용 목록에 추가해야 합니다. 또한 회사는 API의 IP 주소를 허용 목록에 추가해야 합니다. 회사의 보안 팀은 /27 CIDR 범위를 허용 목록에 추가할 수 있도록 허용할 것입니다. 솔루션은 복잡성과 운영 오버헤드를 최소화해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Fargate 작업 배포와 동일한 서브넷에 새 NLB (네트워크 부하 분산 장치) 를 만듭니다. API에 액세스해야 하는 클라이언트 IP 주소만 포함하는 보안 그룹을 만듭니다. 새 보안 그룹을 Fargate 작업에 연결합니다. 보안 팀에 허용 목록에 대한 NLB의 IP 주소를 제공합니다.

B. /27 서브넷을 새로 두 개 만듭니다. 새 서브넷으로 확장되는 새 애플리케이션 로드 밸런서 (ALB) 를 만듭니다. API에 액세스해야 하는 클라이언트 IP 주소만 포함하는 보안 그룹을 만듭니다. 보안 그룹을 ALB에 연결합니다.보안 팀에 허용 목록에 대한 새 서브넷 IP 범위를 제공합니다.

C. /27 서브넷을 새로 두 개 만듭니다. 새 서브넷으로 확장되는 새 NLB (네트워크 부하 분산 장치) 를 만듭니다.새 서브넷 내에 새 애플리케이션 로드 밸런서 (ALB) 를 생성합니다. API에 액세스해야 하는 클라이언트 IP 주소만 포함하는 보안 그룹을 만듭니다. 보안 그룹을 ALB에 연결합니다. ALB의 IP 주소를 NLB 뒤의 대상으로 추가합니다. 보안 팀에 허용 목록에 대한 NLB의 IP 주소를 제공합니다.

D. Fargate 작업 배포와 동일한 서브넷에 새 애플리케이션 로드 밸런서 (ALB) 를 생성합니다. API에 액세스해야 하는 클라이언트 IP 주소만 포함하는 보안 그룹을 만듭니다. 보안 그룹을 ALB에 연결합니다. 보안 팀에 허용 목록에 대한 ALB의 IP 주소를 제공합니다.

Answer: D

Q49

소매업체는 Amazon EC2 인스턴스에서 실행되는 Amazon Elastic Container Service (Amazon ECS) 클러스터에서 비즈니스 크리티컬 웹 서비스를 실행합니다. 웹 서비스는 최종 사용자로부터 POST 요청을 수신하고 별도의 EC2 인스턴스에서 실행되는 MySQL 데이터베이스에 데이터를 씁니다. 회사는 데이터 손실이 발생하지 않도록 해야 합니다.현재 코드 배포 프로세스에는 ECS 서비스의 수동 업데이트가 포함됩니다. 최근 배포 중에 최종 사용자는 유효한 웹 요청에 대한 응답으로 502 Bad Gateway 오류가 간헐적으로 발생했습니다. 이 회사는 이 문제가 반복되는 것을 방지하기 위해 신뢰할 수 있는 솔루션을 구현하고자 합니다. 이 회사는 또한 코드 배포를 자동화하려고 합니다. 솔루션은 가용성이 높아야 하며 비용 효율성을 최적화해야 합니다.

이러한 요구 사항을 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. Fargate 시작 유형이 있는 ECS 클러스터에서 웹 서비스를 실행합니다. AWS CodePipeline 및 AWS CodeDeploy를 사용하여 유효성 검사 테스트와 함께 bule/green 배포를 수행하여 ECS 서비스를 업데이트합니다.

B. 프로비저닝된 IOPS SSD (io2) 스토리지를 사용하는 MySQL용 Amazon RDS 다중 AZ DB 인스턴스에서 실행되도록 MySQL 데이터베이스를 마이그레이션합니다.

C. Amazon Simple Queue Service (Amazon SQS) 대기열을 이벤트 소스로 구성하여 웹 서비스로부터 POST 요청을 수신합니다. 대기열을 폴링하도록 AWS Lambda 함수를 구성합니다.데이터베이스에 날짜를 기록합니다.

D. Fargate 시작 유형이 있는 ECS 클러스터에서 웹 서비스를 실행합니다. AWS CodePipeline 및 AWS CodeDeploy를 사용하여 카나리아 배포를 수행하여 ECS 서비스를 업데이트합니다.

Answer: C, D

Q50

온라인 소매 회사는 단일 서버의 온프레미스 데이터 센터에서 상태 저장 웹 기반 애플리케이션과 MySQL 데이터베이스를 호스팅합니다. 이 회사는 더 많은 마케팅 캠페인과 프로모션을 수행하여 고객 기반을 늘리려고합니다. 준비 과정에서 이 회사는 아키텍처의 안정성을 높이기 위해 애플리케이션과 데이터베이스를 AWS로 마이그레이션하려고 합니다.

최고 수준의 신뢰성을 제공해야 하는 솔루션은 무엇입니까?

A. 데이터베이스를 Amazon RDS MySQL 다중 AZ DB 인스턴스로 마이그레이션합니다. 애플리케이션 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Amazon Neptune에 세션을 저장합니다.

B. 데이터베이스를 Amazon Aurora MySQL로 마이그레이션합니다. 애플리케이션 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Redis용 Amazon ElastiCache 복제 그룹에 세션을 저장합니다.

C. 데이터베이스를 Amazon DocumentDB로 마이그레이션합니다 (MongoDB 호환성 사용). 네트워크 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 그룹에 애플리케이션을 배포합니다. Amazon Kinesis Data Firehose에 세션을 저장합니다.

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

Answer: B

Q51

한 회사가 AWS 클라우드에서 여러 프로젝트를 개발 및 호스팅하고 있습니다. 이 프로젝트는 AWS Organizations의 동일한 조직에 속한 여러 AWS 계정에서 개발됩니다. 회사는 소유 프로젝트에 비용 또는 클라우드 인프라를 할당해야 합니다. 모든 AWS 계정을 담당하는 팀은 여러 Amazon EC2 인스턴스에 비용 할당에 사용되는 프로젝트 태그가 부족하다는 사실을 발견했습니다.

솔루션 설계자가 문제를 해결하고 향후 발생하지 않도록 하기 위해 취해야 할 조치는 무엇입니까?(세 개 선택)

A. 각 계정에서 AWS Config 규칙을 생성하여 누락된 태그가 있는 리소스를 찾습니다.

B. 프로젝트 태그가 누락된 경우 ec2:RunLnStances에 대한 거부 작업을 사용하여 조직에서 SCP를 만듭니다.

C. 조직에서 Amazon Inspector를 사용하여 누락된 태그가 있는 리소스를 찾습니다.

D. 프로젝트 태그가 누락된 경우 ec2:RunInstances에 대한 거부 작업을 사용하여 각 계정에서 오전 1시 정책을 생성합니다.

E. 조직에서 누락된 프로젝트 태그가 있는 EC2 인스턴스 목록을 수집할 AWS Config 애그리게이터를 생성합니다.

F. AWS 보안 허브를 사용하여 누락된 프로젝트 태그가 있는 EC2 인스턴스 목록을 집계합니다.

Answer: A, C, D

Q52

한 회사가 eu-west-1 리전에서 애플리케이션을 실행하고 각 환경 개발, 테스트 및 프로덕션에 대해 하나의 계정을 보유하고 있습니다. 모든 환경은 상태 저장 Amazon EC2 인스턴스와 MySQL 데이터베이스용 Amazon RDS를 사용하여 주 7일 하루 24시간 실행됩니다. 데이터베이스의 크기는 500GB에서 800GB 사이입니다. 개발 팀과 테스트 팀은 업무 시간 중 영업일에 작업하지만 프로덕션 환경은 주 7일 하루 24시간 운영됩니다. 이 회사는 비용을 절감하고자 합니다. AH 리소스에는 개발, 테스트 또는 프로덕션이 핵심인 환경 태그가 지정됩니다.

최소한의 운영 노력으로 비용을 절감하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 매일 한 번 실행되는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다. 태그 날짜 및 시간을 기준으로 인스턴스를 시작하거나 중지하는 AWS Lambda 함수 하나를 호출하도록 규칙을 구성합니다.

B. 저녁에 매일 영업일에 실행되는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다. 태그를 기반으로 인스턴스를 중지하는 AWS Lambda 함수를 호출하도록 규칙을 구성합니다. 아침에 매일 영업일에 실행되는 두 번째 EventBridge (CloudWatch Events) 규칙을 생성합니다. 태그를 기반으로 인스턴스를 시작하는 다른 Lambda 함수를 호출하도록 두 번째 규칙을 구성합니다.

C. 저녁에 매일 영업일에 실행되는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다. 태그를 기반으로 인스턴스를 종료하는 AWS Lambda 함수를 호출하도록 규칙을 구성합니다.아침에 매일 영업일에 실행되는 두 번째 EventBridge (CloudWatch Events) 규칙을 생성합니다. 태그를 기반으로 마지막 백업에서 인스턴스를 복원하는 다른 Lambda 함수를 호출하도록 두 번째 규칙을 구성합니다.

D. 매시간 실행되는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.태그. 일 및 시간을 기준으로 인스턴스를 종료하거나 복원하는 하나의 AWS Lambda 함수를 호출하도록 규칙을 구성합니다.

Answer: C

Q53

한 회사가 AWS의 여러 환경에 애플리케이션을 배포했습니다. 프로덕션 및 테스트를 포함하여 이 회사는 프로덕션 및 테스트를 위한 별도의 계정을 보유하고 있으며, 사용자는 필요에 따라 팀 구성원 또는 서비스에 대한 추가 애플리케이션 사용자를 생성할 수 있습니다. 보안 팀은 운영 팀에 보안 자격 증명에 대한 중앙 집중식 제어와 환경 간 권한 관리를 개선하여 프로덕션과 테스트 간의 격리를 개선하도록 요청했습니다.

다음 중 이 목표를 가장 안전하게 달성할 수 있는 옵션은 무엇입니까?

A. 자격 증명 계정과 같은 사용자 및 서비스 계정을 보유할 새 AWS 계정을 생성합니다. ID 계정에서 사용자 및 그룹을 생성합니다. 프로덕션 및 테스트 계정에서 적절한 권한이 있는 역할을 생성합니다. 역할에 대한 신뢰 정책에 ID 계정을 추가합니다.

B. 프로덕션 및 테스트 계정의 권한을 수정하여 새 IAM 사용자 생성을 운영 팀의 구성원으로 제한합니다. 각 계정에 강력한 IAM 암호 정책을 설정합니다. 각 계정에 새 IAM 사용자 및 그룹을 생성하여 직무를 완료하는 데 필요한 서비스로만 개발자 액세스를 제한합니다.

C. 사용자 계정이 보안 정책을 준수하는지 확인하는 각 계정에서 실행되는 스크립트를 만듭니다. 준수하지 않는 사용자 또는 서비스 계정을 비활성화합니다.

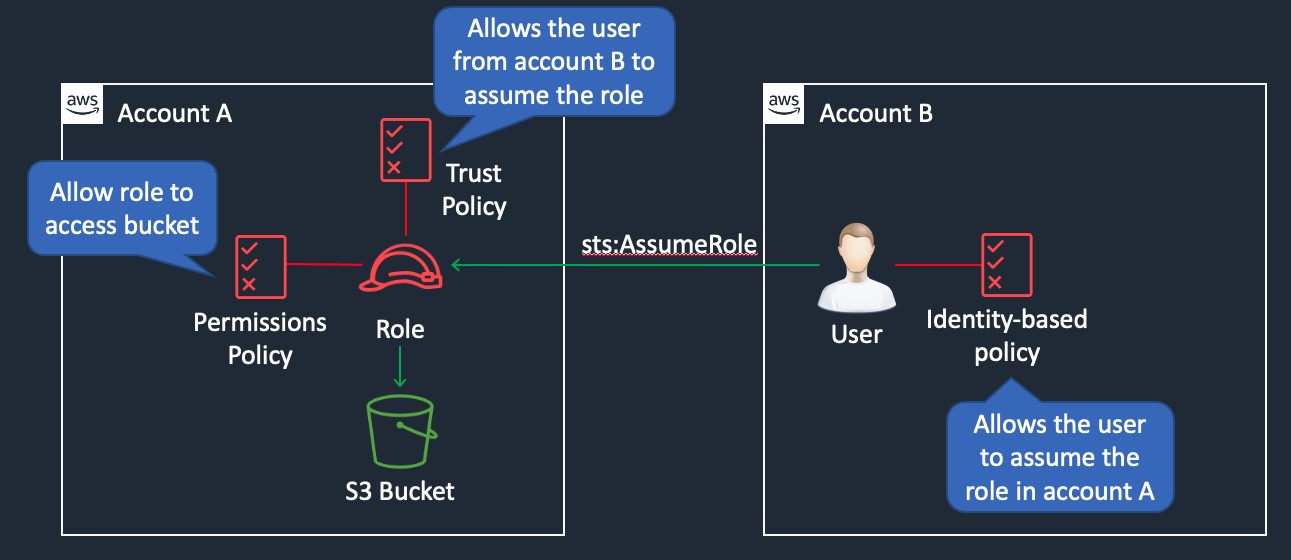
D. 프로덕션 계정에서 모든 사용자 계정을 생성합니다. 프로덕션 계정 및 테스트 계정에서 액세스할 역할을 생성합니다. 프로덕션 계정에서 테스트 계정으로 교차 계정 액세스 권한을 부여합니다.

Answer: A

설명

이 상황에 대한 AWS 모범 사례는 자격 증명 계정을 사용하여 모든 사용자 및 서비스 계정을 저장하는 것입니다. 그런 다음 액세스할 계정에서 역할을 만들고 ID 계정 사용자(또는 전체 계정)가 역할을 맡을 수 있도록 권한을 위임합니다. 이를 통해 보안 ID를 중앙에서 제어할 수 있습니다.

두 계정 간의 교차 계정 액세스에 대한 구성은 아래에 설명되어 있습니다. 이 다이어그램에서 계정 B(ID 계정)의 사용자는 계정 A(리소스 계정)의 역할을 수임하고 S3 버킷에 액세스할 수 있습니다.



잘못됨: D. 올바르지 않습니다. ID에 대해 별도의 계정을 만들어야 합니다.

참조:

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\_cross-account-with-roles.html

Q54

온프레미스 Oracle 데이터 웨어하우스에서 30TB Oracle 데이터 웨어하우스인 Amazon Redshift로 이전하려는 기업이 있습니다. 이 조직은 AWS 스키마 변환 도구 (AWS SCT) 를 사용하여 이전 데이터 웨어하우스의 스키마를 Amazon Redshift 스키마로 변환했습니다. 또한 조직은 마이그레이션 평가 보고서를 사용하여 완료해야 하는 수동 작업을 강조했습니다.

조직은 2주간의 데이터 동결에 맞춰 데이터를 새로운 Amazon Redshift 클러스터로 이동해야 합니다. 온프레미스 데이터 웨어하우스와 AWS 간의 유일한 네트워크 링크는 50Mbps 인터넷 연결입니다.

이러한 기준을 충족하는 마이그레이션 접근 방식은 무엇입니까?

A. AWS DATABASE MIGRATION SERVICE (AWS DMS) 복제 인스턴스를 생성합니다. 기업 방화벽을 통해 데이터 웨어하우스에 도달하도록 복제 인스턴스의 퍼블릭 IP 주소를 승인합니다.데이터 고정 기간이 시작될 때 실행할 마이그레이션 작업을 만듭니다.

B. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 데이터를 Amazon S3 버킷으로 전송할 추출, 업로드 및 복사 작업을 정의합니다. 데이터를 Amazon Redshift 클러스터로 복사합니다. 데이터 고정 기간이 시작될 때 작업을 실행합니다.

C. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 사이트 간 VPN 연결을 만듭니다. 적절한 크기의 AWS DATABASE MIGRATION SERVICE (AWS DMS) 복제 인스턴스를 생성합니다. VPN 연결을 통해 온프레미스 데이터 웨어하우스에 액세스할 수 있도록 복제 인스턴스의 IP 주소를 승인합니다.

D. AWS Snowball Edge에서 작업을 생성하여 Amazon S3로 데이터를 가져옵니다. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 데이터를 Snowball Edge 디바이스로 전송할 로컬 및 AWS DATABASE MIGRATION SERVICE (AWS DMS) 작업을 정의합니다.Snowball Edge 디바이스가 AWS로 반환되고 Amazon S3에서 데이터를 사용할 수 있는 경우 AWS DMS 하위 작업을 실행하여 데이터를 Amazon Redshift에 복사합니다.

Answer: D

Q55

한 회사가 최근에 피어링된 VPC의 Amazon EC2 Linux 인스턴스 그룹에서 실행되는 새로운 애플리케이션을 배포했습니다. VPC 이 회사는 배스천 호스트 역할을 하는 EC2 Linux 인스턴스를 시작했습니다. 애플리케이션 인스턴스의 보안 그룹은 배스천 호스트의 프라이빗 IP에서 TCP 포트 22에 대한 액세스만 허용합니다.배스천 호스트의 보안 그룹에서는 0.0.0.0/0에서 TCP 포트 22에 액세스할 수 있으므로 시스템 관리자는 SSH를 사용하여 여러 지점의 애플리케이션 인스턴스에 원격으로 로그인할 수 있습니다. 한 클라우드 엔지니어는 배스천 호스트의 운영 체제 로그를 살펴보면서 전 세계 여러 위치에서 배스천 호스트에 대한 수천 건의 SSH 로그인에 실패한 것을 발견했습니다. 클라우드 엔지니어는 애플리케이션 인스턴스에 원격 액세스가 부여되는 방식을 변경하려고 하며 다음 요구 사항을 충족하려고 합니다.

\* 무차별 대입 SSH 로그인 시도 제거

\* SSH 세션 중에 실행되는 명령 로그 유지

\* 포트 전달 기능 유지

애플리케이션 인스턴스에 대한 원격 액세스에 대한 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 시스템 관리자와 통신하도록 애플리케이션 인스턴스를 구성합니다. 세션 관리자를 사용하여 애플리케이션 인스턴스와 세션을 설정할 수 있는 액세스 권한을 시스템 관리자에게 부여합니다. 배스천 호스트를 종료합니다.

B. 지점의 공용 IP 주소에서 오는 트래픽만 허용하도록 배스천 호스트의 보안 그룹을 업데이트합니다.

C. AWS 클라이언트 VPN 엔드포인트를 구성하고 각 시스템 관리자에게 인증서를 프로비저닝하여 애플리케이션 VPC에 대한 VPN 연결을 설정합니다. 클라이언트 VPN IPv4 CIDR의 트래픽만 허용하도록 애플리케이션 인스턴스의 보안 그룹을 업데이트합니다. 배스천 호스트를 종료합니다.

D. AWS 시스템 관리자와 통신하도록 애플리케이션 인스턴스를 구성합니다. Systems Manager Run Command를 사용하여 응용 프로그램 인스턴스에 명령을 실행할 수 있는 시스템 관리자에게 액세스 권한을 부여합니다. 배스천 호스트를 종료합니다.

Answer: A

Q56

한 금융 회사가 Amazon S3 버킷에 재무 기록을 저장하고 있습니다. 회사는 모든 금융 거래에 대한 기록을 유지합니다. 규제 요건에 따라 기록 후 최소 1년 동안은 기록을 수정할 수 없습니다. 레코드는 정기적으로 읽으며 즉시 액세스할 수 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 새 S3 버킷을 생성합니다. S3 객체 잠금을 켜고 기본 보존 기간을 1년으로 설정한 다음 보존 모드를 규정 준수 모드로 설정합니다. 모든 레코드를 새 S3 버킷에 저장합니다.

B. S3 수명 주기 규칙을 생성하여 새 객체를 S3 Glacier 스토리지 티어로 즉시 전송합니다. 보존 기간이 1년인 S3 Glacier 저장소 잠금 정책을 생성합니다.

C. S3 수명 주기 규칙을 생성하여 새 객체를 S3 인텔리전트 계층화 스토리지 계층으로 즉시 전송합니다. 보존 기간을 1년으로 설정합니다.

D. s3:x-amz-객체 보존 헤더가 1년이 아닌 조건으로 PutObject 작업에 대한 거부 작업이 포함된 S3 버킷 정책을 생성합니다.

Answer: A

Q57

소매 회사는 일련의 데이터 파일을 다른 회사에 제공해야합니다. 이것이 비즈니스 파트너입니다. 이러한 파일은 소매 회사에 속한 계정 A의 Amazon S3 버킷에 저장됩니다. 이 비즈니스 파트너 회사는 IAM 사용자 USER\_DataProcessor 중 한 명이 자체 AWS 계정 (계정 B) 에서 파일에 액세스하기를 원합니다.

USER\_DataProcessor가 S3 버킷에 성공적으로 액세스할 수 있도록 회사에서 수행해야 하는 단계 조합은 무엇입니까?

A. 계정 A의 S3 버킷에 대한 교차 출처 리소스 공유 (CORS) 기능을 켭니다.

B. 계정 A에서 S3 버킷 정책을 다음과 같이 설정합니다.

C. 계정 A에서 S3 버킷 정책을 다음과 같이 설정합니다.

Answer: C

**문제이상함**

Q58

한 회사가 온프레미스에서 AWS 클라우드로 애플리케이션을 마이그레이션하고 있습니다. 이러한 애플리케이션은 회사의 내부 웹 양식을 강화합니다. 이러한 웹 양식은 분기마다 여러 번 특정 이벤트에 대한 데이터를 수집합니다. 웹 양식은 간단한 SQL 문을 사용하여 데이터를 로컬 관계형 데이터베이스에 저장합니다. 데이터 수집은 각 이벤트에 대해 발생하며 온-프레미스 서버는 대부분 유휴 상태입니다. 회사는 웹 양식을 지원하는 유휴 인프라의 양을 최소화해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon EC2 이미지 빌더를 사용하여 레거시 서버용 AMI를 생성합니다. AMI를 사용하여 EC2 인스턴스를 프로비저닝하여 AWS에서 애플리케이션을 다시 생성합니다. 클라우드.EC2 인스턴스 앞에 애플리케이션 로드 밸런서 (ALB) 를 배치합니다. Amazon Route 53을 사용하여 웹 양식의 DNS 이름이 ALB를 가리키도록 합니다.

B. Amazon DynamoDB 테이블 하나를 생성하여 모든 데이터 입력에 대한 데이터를 저장합니다. 애플리케이션 양식 이름을 테이블 키로 사용하여 데이터 항목을 구분합니다. Amazon Kinesis 데이터 스트림을 생성하여 데이터 입력을 수신하고 그 입력을 DynamoDB에 저장합니다. Amazon Route 53을 사용하여 웹 양식의 DNS 이름이 Kinesis 데이터 스트림의 엔드포인트를 가리키도록 합니다.

C. 레거시 웹 양식 응용 프로그램의 각 서버에 대해 Docker 이미지를 만듭니다. AWS Fargate에서 Amazon Elastic Container Service (Amazon ECS) 클러스터를 생성합니다. 애플리케이션 로드 밸런서를 ECS 클러스터 앞에 배치합니다. Fargate 작업 저장소를 사용하여 웹 양식 데이터를 저장합니다.

D. Amazon Aurora 서버리스 클러스터를 프로비저닝합니다. 각 웹 양식의 데이터 저장소에 대해 여러 스키마를 빌드합니다. Amazon API Gateway와 AWS Lambda 함수를 사용하여 데이터 입력 양식을 다시 생성합니다. Amazon Route 53을 사용하여 웹 양식의 DNS 이름이 해당 API 게이트웨이 엔드포인트를 가리키도록 합니다.

Answer: D

Q59

한 회사에서 퍼블릭 IP를 사용하여 여러 Amazon EC2 인스턴스에 컨테이너화 및 배포된 애플리케이션 서비스를 보유하고 있습니다. Apache Kafka 클러스터가 EC2 인스턴스에 배포되었습니다. PostgreSQL 데이터베이스가 Amazon RDS 또는 포스트그레SQL로 마이그레이션되었습니다. 이 회사는 주력 제품의 새 버전이 출시되면 플랫폼에서 주문이 크게 증가 할 것으로 예상합니다.

현재 아키텍처에 어떤 변화가 운영 오버헤드를 줄이고 제품 출시를 지원할 수 있을까요?

A. 애플리케이션 로드 밸런서 뒤에 EC2 Auto Scaling 그룹을 생성합니다. DB 인스턴스에 대한 추가 읽기 전용 복제본을 생성합니다. Amazon Kinesis 데이터 스트림을 생성하고 애플리케이션 서비스를 구성합니다. 데이터 스트림을 사용합니다. Amazon S3에서 직접 정적 콘텐츠를 저장하고 제공합니다.

B. 애플리케이션 로드 밸런서 뒤에 EC2 Auto Scaling 그룹을 생성합니다. 다중 AZ 모드로 DB 인스턴스를 배포하고 스토리지 자동 확장을 활성화합니다. Amazon Kinesis 데이터 스트림을 생성하고 데이터 스트림을 사용하도록 애플리케이션 서비스를 구성합니다. Amazon S3에서 직접 정적 콘텐츠를 저장하고 제공합니다.

C. 애플리케이션 로드 밸런서 뒤에 있는 EC2 인스턴스에 생성된 Kubernetes 클러스터에 애플리케이션을 배포합니다. 다중 AZ 모드로 DB 인스턴스를 배포하고 스토리지 자동 확장을 활성화합니다. Apache Kafka용 Amazon 관리형 스트리밍 클러스터를 생성하고 클러스터를 사용하도록 애플리케이션 서비스를 구성합니다. Amazon CloudFront 배포 뒤에 있는 Amazon S3에 정적 콘텐츠를 저장합니다.

D. AWS Fargate를 사용하여 Amazon Elastic Kubernetes Service (Amazon EKS) 에 애플리케이션을 배포하고 애플리케이션 로드 밸런서 뒤에서 자동 확장을 활성화합니다. DB 인스턴스에 대한 추가 읽기 전용 복제본을 생성합니다. Apache Kafka용 Amazon 관리형 스트리밍 클러스터를 생성하고 클러스터를 사용하도록 애플리케이션 서비스를 구성합니다. Amazon CloudFront 배포 뒤에 있는 Amazon S3에 정적 콘텐츠를 저장합니다.

Answer: D

Q60

웹 애플리케이션은 사이트 간 VPN을 통해 회사의 온프레미스 데이터 센터에 연결된 전용 VPC에서 호스팅됩니다. 이 응용 프로그램은 회사 네트워크를 통해서만 사용할 수 있습니다. 이 애플리케이션은 업무 시간 중에만 활용되는 비프로덕션 임시 애플리케이션입니다. 워크로드는 일반적으로 가벼우며 급증은 짧습니다. 백엔드에서 애플리케이션은 Amazon Aurora MySQL이 제공하는 데이터베이스 클러스터를 사용합니다. VPC에는 인터넷 게이트웨이와 NAT 게이트웨이가 장착되어 있습니다. 웹 서버는 Auto Scaling 그룹의 탄력적 로드 밸런서 뒤에 있는 프라이빗 서브넷에 있습니다. 또한 웹 서버는 인터넷을 통해 Amazon S3 버킷으로 데이터를 전송합니다. 솔루션 설계자의 주요 목표는 운영 비용을 최소화하고 설계를 단순화하는 것입니다.

솔루션 설계자는 어떤 접근 방식을 사용해야 합니까?

A. Auto Scaling 그룹 설정을 검토하고 업무 시간에만 Amazon EC2 인스턴스를 작동하도록 예약된 작업이 지정되어 있는지 확인합니다. 웹 서버 EC2 인스턴스에 대해 3년 정기 예약 인스턴스를 사용합니다. 인터넷 게이트웨이를 분리하고 VPC에서 NAT 게이트웨이를 제거합니다. Aurora 서버리스 데이터베이스를 사용하고 S3 버킷에 대한 VPC 엔드포인트를 설정합니다.

B. Auto Scaling 그룹 설정을 검토하고 업무 시간에만 Amazon EC2 인스턴스를 작동하도록 예약된 작업이 지정되어 있는지 확인합니다. 인터넷 게이트웨이를 분리하고 VPC에서 NAT 게이트웨이를 제거합니다. Aurora 서버리스 데이터베이스를 사용하고 S3 버킷에 대한 VPC 엔드포인트를 설정한 다음, 변경 사항과 관련된 네트워크 라우팅 및 보안 규칙 및 정책을 업데이트합니다.

C. Auto Scaling 그룹 설정을 검토하고 업무 시간에만 Amazon EC2 인스턴스를 작동하도록 예약된 작업이 지정되어 있는지 확인합니다. VPC에서 인터넷 게이트웨이를 분리하고 Aurora 서버리스 데이터베이스를 사용합니다. S3 버킷에 대한 VPC 엔드포인트를 설정한 다음 변경 사항과 관련된 네트워크 라우팅 및 보안 규칙 및 정책을 업데이트합니다.

D. 웹 서버 Amazon EC2 인스턴스에 대해 3년 예약된 예약 인스턴스를 사용합니다. VPC에서 NAT 게이트웨이를 제거하고 S3 버킷에 대한 VPC 엔드포인트를 설정합니다. Amazon CloudWatch와 AWS Lambda를 사용하여 Aurora DB 클러스터를 중지하고 시작하여 업무 시간에만 작동하도록 합니다. 변경 사항과 관련된 네트워크 라우팅 및 보안 규칙 및 정책을 업데이트합니다.

Answer: B

Q61

비즈니스는 잘 알려진 공개 전자 상거래 웹 사이트를 운영합니다. 사용자 기반은 지역 차원에서 국가 수준으로 빠르게 확장되고 있습니다. 웹 사이트는 웹 서버와 MySQL 데이터베이스를 사용하여 사내에서 호스팅됩니다. 기업은 AWS로 부담을 이전하고자 합니다. 솔루션 설계자는 다음을 위한 솔루션을 개발해야 합니다.

\* 보안 향상

\* 신뢰성 향상

\* 가용성 향상

\* 지연 시간 감소

\* 유지 보수 감소

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 조치를 함께 수행해야 합니까?(세 개 선택)

A. 애플리케이션 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 웹 서버에 대해 2개의 가용 영역에서 Amazon EC2 인스턴스를 사용합니다.

B. 데이터베이스를 다중 AZ Amazon Aurora MySQL DB 클러스터로 마이그레이션합니다.

C. 두 가용 영역에서 Amazon EC2 인스턴스를 사용하여 고가용성 MySQL 데이터베이스 클러스터를 호스팅합니다.

D. Amazon S3에서 정적 웹 사이트 콘텐츠를 호스팅합니다. S3 Transfer Acceleration을 사용하여 웹 페이지를 제공하는 동안 지연 시간을 줄일 수 있습니다. AWS WAF를 사용하여 웹 사이트 보안을 개선합니다.

E. Amazon S3에서 정적 웹 사이트 콘텐츠를 호스팅합니다. Amazon CloudFront를 사용하여 웹 페이지를 제공하는 동안 지연 시간을 줄일 수 있습니다. AWS WAF를 사용하여 웹 사이트 보안을 개선합니다.

F. 데이터베이스를 MySQL용 단일 AZ Amazon RDS DB 인스턴스로 마이그레이션합니다.

Answer: A, B, E

설명

이는 표준 보안, 성능 및 안정성 요구 사항이 필요한 클라우드로의 간단한 마이그레이션입니다. 이러한 요구 사항을 충족하려면 웹 계층에 대해 여러 AZ에 걸쳐 ASG를 생성해야 합니다. 이것은 들어오는 연결을 배포하기 위해 ALB 뒤에 있어야 합니다.

데이터베이스 계층의 경우 다른 AZ에 Aurora 복제본이 있는 Aurora MySQL DB 클러스터가 다중 AZ 장애 조치를 제공합니다. 이렇게 하면 DB 계층의 가용성이 높아지고 유지 관리가 줄어듭니다.

글로벌 사용자의 성능을 향상시키는 또 다른 방법은 Amazon S3에서 정적 콘텐츠를 호스팅하고 Amazon CloudFront CDN을 사용하여 전 세계 엣지 로케이션에 콘텐츠를 캐시하는 것입니다. AWS WAF를 추가하면 보안이 추가됩니다.

잘못됨: C. 유지 관리를 위해 더 많은 유지 관리가 필요하므로 최상의 솔루션이 아닙니다.

잘못됨: D. Transfer Acceleration은 CloudFront Edge 네트워크를 사용하여 데이터를 업로드하기 위한 것입니다. 정적 자산을 제공하려면 CloudFront 배포를 사용하십시오.

잘못됨: F. 이것은 필요한 가용성을 제공하지 않으며, 다른 AZ에 Aurora 복제본을 배포하면 고가용성이 제공됩니다.

참조:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-awswaf.html

Q62

한 회사가 단일 AWS 리전에서 여러 AWS 계정을 사용합니다. 한 솔루션 설계자가 AppDev, AppTest 및 AppProd 계정에서 ELB (Elastic Load Balancers) 에서 생성된 로그를 통합하는 솔루션을 설계하고 있습니다. 로그는 중앙 AWS 계정의 s3-eib-logs라는 기존 Amazon S3 버킷에 저장해야 합니다. 중앙 계정은 로그 통합에만 사용되며 ELB가 배포되지 않은 ELB 로그는 저장 시 암호화되어야 합니다.

솔루션 설계자가 솔루션을 구축하기 위해 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. 중앙 AWS 계정 ID에 대해 s3 풋버킷 로깅 작업을 허용하도록 s3-elb-logs 버킷에 대한 S3 버킷 정책을 업데이트합니다.

B. s3-eib-logs 버킷에 대한 S3 버킷 정책을 업데이트하여 앱데브 앱테스트 및 앱프로덕션 계정 ID에 대해 s3 PutObject 및 s3 객체 삭제 작업을 허용합니다.

C. s3-elb-logs 버킷에 대한 S3 버킷 정책을 업데이트하여 앱데브 앱테스트 및 앱프로덕션 계정 ID에 대해 s3 PutObject 작업을 허용합니다.

D. ELB에 대한 액세스 로깅을 활성화합니다. S3 위치를 s3-elb-로그 버킷으로 설정합니다.

E. s3-elb-logs S3 버킷에 대해 S3 관리형 암호화 키 (SSE-S3) 로 서버 측 암호화를 사용하여 Amazon S3 기본 암호화를 활성화합니다.

Answer: A, E

Q63

대기업에는 여러 사업부가 있습니다. 각 사업부에는 용도가 다른 여러 AWS 계정이 있습니다. 회사의 CIO는 각 사업부에 회사의 다른 부서와 공유하는 데 유용한 데이터가 있다는 것을 알고 있습니다. 총 10PB의 데이터는 1.000개의 AWS 계정 사용자와 공유해야 합니다. 데이터는 독점적이므로 일부 데이터는 특정 직무 유형의 사용자만 사용할 수 있어야 합니다. 일부 데이터는 시뮬레이션과 같은 집약적 워크로드의 처리량에 사용됩니다. 새로운 이니셔티브 인수 및 매각으로 인해 계정 수가 자주 변경됩니다. 솔루션 설계자는 AWS에서 사용할 데이터를 회사 내 모든 직원과 공유할 수 있는 시스템을 설계하도록 요청받았습니다.

확장 가능한 방식으로 데이터를 안전하게 공유할 수 있는 접근 방식은 무엇입니까?

A. 데이터를 단일 Amazon S3 버킷에 저장합니다. S3 버킷의 객체 접두사를 기반으로 적절한 읽기/쓰기 액세스를 허용하는 작업 유형 및 사업부의 모든 조합에 대해 IAM 역할을 생성합니다. 역할에는 사업부의 AWS 계정이 역할을 맡을 수 있도록 허용하는 신뢰 정책이 있어야 합니다. 각 사업부의 AWS 계정에서 IAM을 사용하여 다른 직무 유형에 대한 역할을 수임하지 못하도록 합니다. 사용자는 사업부의 AWS 계정에서 AssumeRole을 사용하여 데이터에 액세스할 수 있는 자격 증명을 얻습니다. 그러면 사용자는 S3 클라이언트에서 이러한 자격 증명을 사용할 수 있습니다.

B. 데이터를 단일 Amazon S3 버킷에 저장합니다. 조건을 사용하여 각 사용자의 사업부 및 작업 유형에 따라 읽기 및 쓰기 액세스 권한을 부여하는 버킷 정책을 작성합니다. 버킷에 액세스하는 AWS 계정이 있는 사업부와 IAM 사용자 이름에 접두사가 있는 작업 유형을 결정합니다. 사용자는 S3 클라이언트가 있는 사업부의 AWS 계정에서 IAM 자격 증명을 사용하여 데이터에 액세스할 수 있습니다.

C. 일련의 Amazon S3 버킷에 데이터를 저장합니다. 사용자를 인증하고 사용자가 애플리케이션을 통해 데이터를 다운로드하거나 업로드할 수 있도록 하는 회사의 자격 증명 공급자 (IdP) 와 통합된 Amazon EC2에서 실행되는 애플리케이션을 생성합니다. 응용 프로그램은 IdP의 사업부 및 작업 유형 정보를 사용하여 사용자가 응용 프로그램을 통해 업로드하고 다운로드할 수 있는 항목을 제어합니다. 사용자는 애플리케이션의 API를 통해 데이터에 액세스할 수 있습니다.

D. 일련의 Amazon S3 버킷에 데이터를 저장합니다. 회사의 자격 증명 공급자 (IdP) 와 통합된 AWS STS 토큰 자동 판매기를 생성합니다. 사용자가 로그인할 때 토큰 자동 판매기에 사용자의 액세스를 제한하는 역할을 가정하는 IAM 정책을 연결하거나 사용자에게 액세스 권한이 있는 데이터만 업로드하도록 합니다. 사용자는 토큰 자동 판매기의 웹 사이트 또는 API에 인증하여 자격 증명을 얻은 다음 S3 클라이언트에서 해당 자격 증명을 사용할 수 있습니다.

Answer: D

Q64

한 회사가 사용자를 지원하기 위해 AWS에서 LOB (비즈니스 톤 오브 비즈니스: running a tone-of-business) 애플리케이션을 실행하고 있습니다. 애플리케이션은 하나의 VPC에서 실행됩니다. 재해 복구를 위해 다른 AWS 리전의 두 번째 VPC에 백업 사본이 있습니다. 이 회사는 온프레미스 네트워크와 AWS 간에 단일 AWS Direct Connect 연결을 보유하고 있습니다. 연결은 Direct Connect 게이트웨이에서 종료됩니다. 애플리케이션에 대한 모든 액세스는 회사의 온프레미스 네트워크에서 시작되어야 하며, 전송 중에 IPsec을 사용하여 트래픽을 암호화해야 합니다. 이 회사는 필요한 암호화를 제공하기 위해 Direct Connect 연결을 통해 VPN 터널을 통해 트래픽을 라우팅하고 있습니다. 무중단 업무 운영 감사는 Direct Connect 연결이 애플리케이션 액세스에 대한 잠재적 단일 실패 지점을 나타낸다고 판단합니다. 회사는 이 문제를 최대한 빨리 해결해야 합니다.

이러한 요구 사항을 충족하는 접근 방식은 무엇입니까?

A. 다른 직접 연결 위치에 대한 두 번째 직접 연결 연결을 주문합니다. 동일한 직접 연결 게이트웨이에서 두 번째 직접 연결 연결을 종료합니다.

B. 인터넷을 통한 AWS 사이트 간 VPN 연결을 구성합니다. 보조 리전의 가상 프라이빗 게이트웨이에서 VPN 연결을 종료합니다.

C. 대중 교통 게이트웨이를 생성합니다. VPC를 전송 게이트웨이에 연결하고 전송 게이트웨이를 Direct Connect 게이트웨이에 연결합니다. AWS 사이트 간 VPN 연결을 구성하고 전송 게이트웨이에서 종료합니다.

D. 대중 교통 게이트웨이를 생성합니다. VPC를 전송 게이트웨이에 연결하고 전송 게이트웨이를 Direct Connect 게이트웨이에 연결합니다.두 번째 Direct Connect 연결을 주문하고 전송 게이트웨이에서 종료합니다.

Answer: C

Q65

솔루션스 아키텍트는 엄격한 재해 복구 요구 사항이 있는 정부 기관에서 근무합니다. 모든 Amazon Elastic Block Store (Amazon EBS) 스냅샷은 최소 2개의 추가 AWS 리전에 저장해야 합니다. 또한 기관은 가능한 가장 낮은 운영 간접비를 유지해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon Data Lifecycle Manager (Amazon DLM) 에서 매일 한 번 실행되도록 정책을 구성하여 EBS 스냅샷을 추가 리전으로 복사합니다.

B. Amazon EventBridge (Amazon CloudWatch Events) 를 사용하여 EBS 스냅샷을 추가 리전으로 복사하도록 AWS Lambda 함수를 예약합니다.

C. AWS 백업을 설정하여 EBS 스냅샷을 생성합니다. EBS 스냅샷을 추가 리전으로 복사하도록 Amazon S3 교차 리전 복제를 구성합니다.

D. Amazon EC2 이미지 빌더가 하루에 한 번 실행되도록 예약하여 AMI를 생성하고 AMI를 추가 리전으로 복사합니다.

Answer: A

Q66

한 회사에서 이벤트 지속성을 위해 PostgreSQL 데이터베이스를 사용하는 온프레미스 모니터링 솔루션을 보유하고 있습니다. 과도한 수집으로 인해 데이터베이스를 확장할 수 없으며 스토리지가 부족해지는 경우가 많습니다. 이 회사는 하이브리드 솔루션을 만들려고 하며 이미 네트워크와 AWS 간에 VPN 연결을 설정했습니다. 솔루션에는 다음 특성이 포함되어야 합니다.

\* 운영 복잡성을 최소화하는 관리형 AWS 서비스.

\* 데이터 처리량에 맞게 자동으로 확장되며 지속적인 관리가 필요하지 않은 버퍼입니다.

\* 거의 실시간으로 이벤트를 관찰할 수 있는 대시보드를 만드는 시각화 도구

\* 반 구조화 JSON 데이터 및 동적 스키마를 지원합니다.

어떤 구성 요소 조합을 통해 이러한 요구 사항을 충족하는 모니터링 솔루션을 만들 수 있을까요?(두 개 선택)

A. Amazon Kinesis Data Firehose를 사용하여 이벤트를 버퍼링합니다. AWS Lambda 함수를 생성하여 이벤트를 처리하고 변환합니다.

B. Amazon Kinesis 데이터 스트림을 생성하여 이벤트를 버퍼링합니다. AWS Lambda 함수를 생성하여 이벤트를 처리하고 변환합니다.

C. 이벤트를 수신하도록 Amazon Aurora PostgreSQL DB 클러스터를 구성합니다. Amazon QuickSight를 사용하여 데이터베이스에서 읽고 실시간에 가까운 시각화 및 대시보드를 생성할 수 있습니다.

D. 이벤트를 수신하도록 Amazon Elasticsearch Service (Amazon ES) 를 구성합니다. Amazon ES와 함께 배포된 Kibana 엔드포인트를 사용하여 실시간에 가까운 시각화 및 대시보드를 생성합니다.

E. 이벤트를 수신하도록 Amazon Neptune DB 인스턴스를 구성합니다. Amazon QuickSight를 사용하여 데이터베이스에서 읽고 실시간에 가까운 시각화 및 대시보드를 생성할 수 있습니다.

Answer: A, D

Q67

회사에는 AWS 조직에 많은 AWS 계정이 있는 조직이 있습니다. 솔루션스 아키텍트는 회사가 조직의 AWS 계정에 대한 일반적인 보안 그룹 규칙을 관리하는 방식을 개선해야 합니다. 이 회사는 각 AWS 계정의 허용 목록에 IP CIDR 범위의 공통 집합을 가지고 있으며, 회사의 온프레미스 네트워크에 대한 액세스를 허용합니다. 각 계정 내의 개발자는 보안 그룹에 새 IP CIDR 범위를 추가할 책임이 있습니다. 보안 팀에는 자체 AWS 계정이 있습니다. 현재 보안 팀은 허용 목록이 변경되면 다른 AWS 계정의 소유자에게 알립니다. 솔루션 설계자는 모든 계정에 공통 CIDR 범위 집합을 배포하는 솔루션을 설계해야 합니다.

최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 보안 팀의 AWS 계정에서 Amazon Simple Notification Service (Amazon SNS) 주제를 설정합니다. 각 AWS 계정에 AWS Lambda 함수를 배포합니다.SNS 주제가 메시지를 수신할 때마다 실행되도록 Lambda 함수를 구성합니다. IP 주소를 입력으로 받아 계정의 보안 그룹 목록에 추가하도록 Lambda 함수를 구성합니다. SNS 주제에 메시지를 게시하여 변경 사항을 배포하도록 보안 팀에 지시합니다.

B. 조직 내 각 AWS 계정에 새 고객 관리형 접두사 목록 생성 각 계정의 접두사 목록을 모든 내부 CIDR 범위로 채우기 보안 그룹의 계정에서 새 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알림 보안에 지시팀에서 각 AWS 계정 소유자와 업데이트를 공유할 수 있습니다.

C. 보안 팀의 AWS 계정에 새 고객 관리형 접두사 목록을 생성합니다. 고객 관리형 접두사 목록을 모든 내부 CIDR 범위로 채웁니다.AWS 리소스 액세스 관리자를 사용하여 고객 관리형 접두사 목록... 조직 공유 각 AWS 계정의 소유자에게 보안 그룹에서 새 고객 관리형 접두사 목록 ID를 허용하도록 알립니다.

D. ….

Answer: A

**보기이상함**

Q68

한 회사에서 Oracle Solaris NFS 스토리지 어레이를 폐기하려고 합니다. 이 회사는 인터넷 네트워크 연결을 통해 Amazon S3의 여러 목적지로 데이터를 신속하게 마이그레이션해야 합니다. Amazon Elastic File System (Amazon EFS), 및 윈도우용 Amazon FSx 파일 서버입니다. 또한 전체 초기 복제본과 스토리지 시스템이 폐기될 때까지 변경 사항을 점진적으로 전송해야 합니다. 모든 데이터를 암호화하고 무결성을 검사해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 권장해야 합니까?

A. CloudEndure를 구성합니다. 프로젝트를 만들고 CloudEndure 에이전트와 토큰을 스토리지 배열에 배포합니다. 마이그레이션 계획을 실행하여 전송을 시작합니다.

B. AWS DataSync를 구성합니다. DataSync 에이전트를 구성하고 로컬 네트워크에 배포합니다. 전송 작업을 생성하고 전송을 시작합니다.

C. aws S3 sync 명령을 구성합니다. 자격 증명을 사용하여 클라이언트 측에서 AWS 클라이언트를 구성합니다. sync 명령을 실행하여 전송을 시작합니다.

D. FTP용 AWS 전송을 구성합니다. 자격 증명을 사용하여 FTP 클라이언트를 구성합니다. 클라이언트를 연결하고 동기화하도록 스크립트하여 전송을 시작합니다.

Answer: B

Q69

한 회사에서 Auto Scaling 그룹의 Amazon EC2 인스턴스를 사용하여 AWS 클라우드에서 비디오를 처리하고 있습니다. 비디오를 처리하는 데 30분이 걸립니다.Amazon 단순 대기열 서비스 (Amazon SQS) 대기열의 동영상 수에 따라 여러 EC2 인스턴스가 확장 및 축소됩니다.이 회사는 대상 배달 못한 편지 대기열과 MaxReceiveCount를 1로 지정하는 재구동 정책을 사용하여 SQS 대기열을 구성했습니다. 이 회사는 SQS 대기열의 가시성 제한 시간을 1시간으로 설정했습니다. 이 회사는 배달 못한 편지 대기열에 메시지가 있을 때 개발 팀에 알리기 위해 Amazon CloudWatch 경보를 설정했습니다. 하루 동안 여러 번 개발 팀은 메시지가 데드 레터 대기열에 있고 비디오가 제대로 처리되지 않았다는 알림을 받습니다. 조사 결과 애플리케이션 로그에서 오류가 발견되지 않았습니다.

이 문제를 어떻게 해결할 수 있을까요?

A. EC2 인스턴스에 대한 종료 보호를 켭니다.

B. SQS 대기열의 가시성 제한 시간을 3시간으로 업데이트합니다.

C. 처리 중에 인스턴스에 대한 축소 보호를 구성합니다.

D. 리드라이브 정책을 업데이트하고 MaxReceiveCount를 0으로 설정합니다.

Answer: C

Q70

한 회사에서 온프레미스 데이터 센터에서 여러 애플리케이션을 실행하고 있습니다. 데이터 센터는 VMware vCenter에서 관리하는 윈도우와 리눅스 VM을 혼합하여 실행합니다. 솔루션스 아키텍트는 애플리케이션을 AWS로 마이그레이션하기 위한 계획을 세워야 합니다. 그러나 솔루션스 아키텍트는 애플리케이션에 대한 설명서가 최신 상태가 아니며 완전한 인프라 다이어그램이 아님을 알게 됩니다. 이 회사의 개발자는 솔루션 설계자와 애플리케이션 및 현재 사용에 대해 논의할 시간이 부족합니다.

솔루션 설계자는 필요한 정보를 수집하기 위해 무엇을 해야 합니까?

A. VMware 클러스터의 OVA 이미지를 사용하여 AWS Server Migration Service (AWS SMS) 커넥터를 배포하여 VM에서 구성 및 사용률 데이터를 수집합니다.

B. AWS Migration Portfolio Assessment (MPA) 도구를 사용하여 각 VM에 연결하여 구성 및 사용률 데이터를 수집합니다.

C. 각 VM에 AWS Application Discovery Service를 설치하여 구성 및 사용률 데이터를 수집합니다.

D. 온프레미스 VM을 AWS 마이그레이션 허브에 등록하여 구성 및 사용률 데이터를 수집합니다.

Answer: C

설명

AWS Discovery Agent는 검색 및 마이그레이션을 대상으로 하는 온프레미스 서버 및 VM에 설치하는 AWS 소프트웨어입니다. 에이전트는 시스템 구성, 시스템 성능, 실행 중인 프로세스 및 시스템 간의 네트워크 연결 세부 정보를 캡처합니다. 에이전트는 대부분의 Linux 및 Windows 운영 체제를 지원하며 물리적 온프레미스 서버, Amazon EC2 인스턴스 및 가상 머신에 배포할 수 있습니다.

위에서 설명한 대로 가상 머신에서 에이전트를 사용할 수 있지만 VMware 가상 머신용 Agentless Discovery 커넥터를 사용하는 것이 더 효율적입니다. 이 커넥터는 VMware vCenter에 설치할 수 있습니다.

AWS Discovery Connector는 VMware VM(가상 머신)에 대한 정보만 수집할 수 있는 VMware 어플라이언스입니다. OVA(Open Virtualization Archive) 파일을 사용하여 VMware vCenter Server 환경에서 Discovery Connector를 VM으로 설치합니다. Discovery Connector는 운영 체제에 관계없이 VMware 메타데이터를 사용하여 서버 정보를 수집하기 때문에 초기 온프레미스 인프라 평가에 필요한 시간을 최소화합니다.

참조:

https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html

https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-connector.html

Q71

금융 서비스 회사는 수백만 건의 과거 주식 거래를 Amazon DynamoDB 테이블에 로드했습니다. 이 테이블은 온디맨드 용량 모드를 사용합니다. 매일 자정에 몇 백만 개의 새 레코드가 테이블에 로드됩니다. 테이블에 대한 애플리케이션 읽기 작업은 하루 종일 버스트에서 발생하며 제한된 키 세트가 반복적으로 조회됩니다. 이 회사는 DynamoDB와 관련된 비용을 줄여야 합니다.

이 요구 사항을 충족하기 위해 솔루션 설계자가 권장해야 하는 전략은 무엇입니까?

A. DynamoDB 테이블 앞에 Amazon ElastiCache 클러스터를 배포합니다.

B. DynamoDB Accelerator (DAX) 를 배포합니다. 비용 탐색기에서 DynamoDB 자동 조정 구매 절감 플랜을 구성합니다.

C. 프로비전된 용량 모드 사용 비용 탐색기에서 저축 계획 구매.

D. DynamoDB Accelerator (DAX) 를 배포합니다. 프로비저닝된 용량 모드 사용 DynamoDB 자동 확장을 구성합니다.

Answer: A

Q72

한 회사가 AWS에서 웹 애플리케이션을 호스팅할 계획이며 Amazon EC2 인스턴스 그룹 전체에서 트래픽을 로드 밸런싱하기 위해 노력하고 있습니다. 보안 요구 사항 중 하나는 클라이언트와 웹 서버 간에 전송되는 종단 간 암호화를 활성화하는 것입니다.

이 요구 사항을 충족하는 솔루션은 무엇입니까?

A. EC2 인스턴스를 애플리케이션 로드 밸런서 (ALB) 뒤에 배치하고 AWS 인증서 관리자 (ACM) 를 사용하여 SSL 인증서를 프로비저닝하고 SSL 인증서를 ALB에 연결합니다. SSL 인증서를 내보내고 각 EC2 인스턴스에 설치합니다. ㄴ포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 ALB를 구성합니다.

B. EC2 인스턴스를 대상 그룹과 연결합니다. AWS 인증서 관리자 (ACM) 를 사용하여 SSL 인증서를 프로비저닝합니다. Amazon CloudFront 배포를 생성하고 SSL 인증서를 사용하도록 구성합니다. 대상 그룹을 오리진 서버로 사용하도록 CloudFront를 설정합니다.

C. EC2 인스턴스를 애플리케이션 로드 밸런서 (ALB) 뒤에 배치합니다. AWS 인증서 관리자 (ACM) 를 사용하여 SSL 인증서를 프로비저닝하고 SSL 인증서를 ALB에 연결합니다. 타사 SSL 인증서를 프로비저닝하고 각 EC2 인스턴스에 설치합니다. 포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 ALB를 구성합니다.

D. EC2 인스턴스를 NLB (네트워크 로드 밸런서) 뒤에 배치합니다. 타사 SSL 인증서를 프로비저닝하고 NLB 및 각 EC2 인스턴스에 설치합니다. 포트 443에서 수신 대기하고 인스턴스의 포트 443으로 트래픽을 전달하도록 NLB를 구성합니다.

Answer: C

Q73

한 회사에서 Production이라는 단일 OU가 있는 AWS 조직을 사용하여 여러 계정을 관리합니다. 모든 계정은 프로덕션 OU의 구성원입니다. 관리자는 조직의 루트에 있는 거부 목록 SCP를 사용하여 제한된 서비스에 대한 액세스를 관리합니다. 이 회사는 최근에 새 사업부를 인수하고 새 부서의 기존 AWS 계정을 조직에 초대했습니다. 새로운 사업부의 관리자는 온보딩한 후 회사의 정책을 충족하기 위해 기존 AWS Config 규칙을 업데이트할 수 없음을 알게 되었습니다.

관리자가 추가 장기 유지 관리를 도입하지 않고 현재 정책을 변경하고 계속 적용할 수 있는 옵션은 무엇입니까?

A. AWS Config에 대한 액세스를 제한하는 조직의 루트 SCP를 제거합니다. 회사의 표준 AWS Config 규칙에 따라 AWS 서비스 카탈로그 제품을 생성하고 새 계정을 포함하여 조직 전체에 배포합니다.

B. 새 계정에 대한 온보딩이라는 임시 OU를 생성합니다. AWS Config 작업을 허용하려면 온보딩 OU에 SCP를 적용합니다. AWS Config 조정이 완료되면 새 계정을 프로덕션 OU로 이동합니다.

C. 거부 목록 SCP에서 조직의 루트 SCP를 변환하여 목록 SCP가 필요한 서비스만 허용하도록 허용합니다. 조직의 루트에 SCP를 임시로 적용하여 새 계정의 보안 주체에 대해서만 AWS Config 작업을 허용합니다.

D. 새 계정에 대해 온보딩이라는 임시 OU를 생성합니다. 온보딩 OU에 SCP를 적용하여 AWS Config 작업을 허용합니다. 조직의 루트 SCP를 프로덕션 OU로 이동합니다. AWS Config에 대한 조정이 완료되면 새 계정을 프로덕션 OU로 이동합니다.

Answer: B

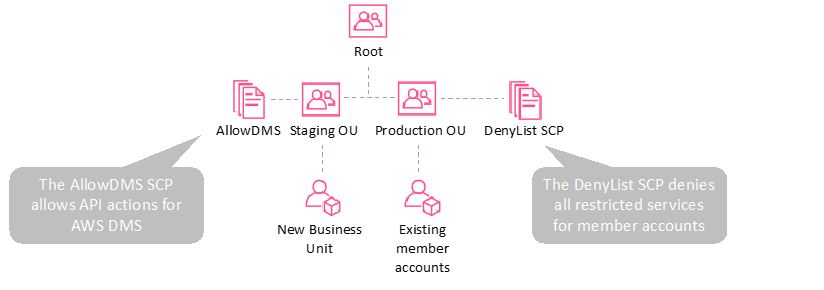
설명

거부 목록 전략은 암시적 거부를 사용하며 모든 작업을 허용하는 루트 수준(기본적으로)에 AWSFullAccess라는 SCP가 적용됩니다. 이 경우 회사는 특정 서비스에 대한 액세스를 거부하는 루트 수준의 거부 목록 SCP를 적용했습니다.

AWS 조직에서는 모든 계정에 위의 모든 부모에 의해 허용된 권한만 있습니다. 허용 정책 문에 포함되지 않음으로써 또는 명시적으로(거부 정책 문에 포함됨으로써) 계정 위의 모든 수준에서 권한이 차단되면 영향을 받는 계정의 사용자 또는 역할이 해당 권한을 사용할 수 없습니다.

따라서 루트 수준에서 거부된 OU의 서비스를 허용할 수 없습니다. 유일한 해결책은 거부 목록을 루트 수준에서 프로덕션 OU로 이동한 다음(다른 모든 계정에 대해 여전히 유효함을 의미함) AWS DMS를 허용하는 SCP로 임시 OU를 생성하는 것입니다(AWSFullAccess는 제거되지 않았습니다).

아래 다이어그램은 DenyList SCP가 프로덕션 OU로 이동된 후의 임시 구성을 보여줍니다.



잘못됨: A. 이렇게 하면 필요한 것보다 더 많은 권한이 있는 모든 구성원 계정에 대해 AWS Config가 활성화되므로 이것이 최선의 옵션은 아닙니다.

잘못됨: C. SCP 변환과 관련된 작업이 훨씬 더 많으며 거부 목록 SCP를 루트에서 프로덕션 OU로 이동하여 계층 구조의 상위에서 제한을 제거하는 것이 훨씬 더 간단합니다.

잘못됨: D. 루트 수준의 거부 목록 SCP는 그 아래의 모든 수준에서 제한된 작업을 허용하지 않으므로 작동하지 않습니다.

참조:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_policies\_scps.html

Q74

회사는 데이터베이스와 웹 사이트로 구성된 클라우드에서 애플리케이션을 실행합니다. 사용자는 웹 사이트에 데이터를 게시하고, 데이터를 처리하고, 이메일로 데이터를 다시 보낼 수 있습니다. 데이터는 Amazon EC2 인스턴스에서 실행되는 MySQL 데이터베이스에 저장됩니다. 데이터베이스는 두 개의 프라이빗 서브넷이 있는 VPC에서 실행 중입니다.웹 사이트가 하나의 퍼블릭 서브넷이 있는 다른 VPC의 단일 EC2 인스턴스에서 Apache Tomcat에서 실행 중입니다. 데이터베이스와 웹 사이트 VPC 간에는 단일 VPC 피어링 연결이 있습니다. 트래픽이 많아 지난 한 달 동안 웹 사이트가 여러 차례 중단되었습니다. 솔루션 설계자가 애플리케이션의 안정성을 높이기 위해 취해야 할 조치는 무엇입니까?(세 개 선택)

A. 애플리케이션 로드 밸런서 뒤에 여러 EC2 인스턴스가 있는 Auto Scaling 그룹에 Tomcat 서버를 배치합니다.

B. 추가 VPC 피어링 연결을 프로비저닝합니다.

C. 하나의 Aurora 복제본을 사용하여 MySQL 데이터베이스를 AmazonAurora로 마이그레이션합니다.

D. 데이터베이스 VPC에 두 개의 NAT 게이트웨이를 프로비저닝합니다.

E. Tomcat 서버를 데이터베이스 VPC로 이동합니다.

F. 웹 사이트 VPC의 다른 가용 영역에 추가 퍼블릭 서브넷을 생성합니다.

Answer: A, C, F

Q75

인사말 카드 회사는 최근 고객이 회사 플랫폼을 통해 좋아하는 유명인에게 카드를 보낼 수 있다고 광고했습니다. 광고가 게시 된 이후 플랫폼은 매초 10.000 명의 순 사용자로부터 지속적인 트래픽을 받았습니다. 이 플랫폼은 애플리케이션 로드 밸런서 (ALB) 뒤에 있는 m5.xlarge Amazon EC2 인스턴스에서 실행됩니다. 인스턴스는 Auto Scaling 그룹에서 실행되며 Amazon Linux를 기반으로 하는 사용자 지정 AMI를 사용합니다. 이 플랫폼은 기본 엔드포인트와 리더 엔드포인트를 사용하는 고가용성 Amazon Aurora MySQL DB 클러스터를 사용합니다. 또한 이 플랫폼은 클러스터 엔드포인트를 사용하는 Redis용 Amazon ElastiCache 클러스터를 사용합니다. 플랫폼은 각 고객에 대해 새로운 프로세스를 생성하고 각 고객의 세션 동안 MySQL에 대한 열린 데이터베이스 연결을 유지합니다. 그러나 플랫폼의 리소스 사용량은 적습니다.많은 고객이 플랫폼에 연결할 때 오류를 보고합니다. 로그에 Aurora 데이터베이스에 대한 연결이 실패하고 있음을 알 수 있습니다. Amazon CloudWatch 측정치는 CPU 로드가 플랫폼 전체에서 견인되고 ALB를 통해 플랫폼에 성공적으로 연결되었음을 보여줍니다.

오류를 가장 비용 효율적으로 해결할 수 있는 솔루션은 무엇입니까?

A. Amazon CloudFront 배포를 설정합니다. ALB를 오리진으로 설정 모든 고객 트래픽을 CloudFront 배포 엔드포인트로 이동합니다.

B. Amazon RDS 프록시 사용 프록시를 사용하도록 데이터베이스 연결을 재구성합니다.

C. Aurora MySQL 클러스터의 리더 노드 수를 늘립니다.

D. Redis용 ElastiCache 클러스터의 노드 수를 늘립니다.

Answer: C

Q76

온라인 잡지가 이번 달에 최신판을 출시합니다. 이 에디션은 전 세계에 가장 먼저 배포됩니다. 이 매거진의 동적 웹 사이트는 현재 웹 티어 앞의 애플리케이션 로드 밸런서, 웹 및 애플리케이션 서버용 Amazon EC2 인스턴스 집합, Amazon Aurora MySQL을 사용합니다. 웹 사이트의 일부에는 정적 콘텐츠가 포함되어 있으며 거의 모든 트래픽은 읽기 전용입니다. 이 잡지는 새 버전이 출시 될 때 인터넷 트래픽이 크게 증가 할 것으로 예상하고 있습니다. 최적의 성능은 출시 다음 주 동안 최우선 과제입니다.

솔루션 설계자가 전 세계 사용자의 시스템 응답 시간을 줄이기 위해 취해야 할 단계는 무엇입니까?(두 개 선택)

A. 논리적 교차 리전 복제를 사용하여 Aurora MySQL 데이터베이스를 보조 리전으로 복제합니다. 교차 리전 복제 모드에서 웹 서버를 Amazon S3 Deploy S3 버킷으로 바꿉니다.

B. 웹 및 애플리케이션 계층이 각각 m Auto Scaling 그룹인지 확인합니다. AWS Direct Connect 연결 소개 전 세계 리전에 웹 및 애플리케이션 계층을 배포합니다.

C. 데이터베이스를 Amazon Aurora에서 MySQL용 Amazon RDS로 마이그레이션합니다. 세 가지 애플리케이션 계층 (웹, 애플리케이션 및 데이터베이스) 이 모두 프라이빗 서브넷에 있는지 확인합니다.

D. 물리적 교차 리전 복제에 Aurora 글로벌 데이터베이스를 사용합니다. 정적 콘텐츠 및 리소스에 대해 교차 리전 복제와 함께 Amazon S3를 사용합니다. 전 세계 리전에 웹 및 애플리케이션 계층을 배포합니다.

E. 지연 시간 기반 라우팅과 Amazon CloudFront배포를 갖춘 Amazon루트 53을 소개합니다. 웹 및 애플리케이션 계층이 각각 Auto Scaling 그룹에 속하는지 확인합니다.

Answer: D, E

설명

Amazon CloudFront를 사용하여 Auto Scaling 그룹의 여러 리전에서 시작된 EC2 인스턴스와 정적 자산을 함께 제공함으로써 글로벌 사용자에 맞게 웹 사이트 성능을 최적화할 수 있습니다. 트래픽을 올바른 인스턴스로 보내기 위해 가장 가까운(지연 시간이 가장 짧은) AWS 리전으로 트래픽을 보내는 Route 53에서 지연 시간 기반 라우팅 정책을 생성할 수 있습니다.

데이터베이스 계층은 Aurora 글로벌 데이터베이스로 구성할 수 있습니다. 이 구성은 데이터베이스 성능에 영향을 주지 않고 데이터를 복제하고, 각 지역에서 짧은 대기 시간으로 빠른 로컬 읽기를 가능하게 하고, 지역 전체의 중단으로부터 재해 복구를 제공합니다.

이 솔루션은 읽기에 대한 고성능을 제공하도록 최적화되어 있습니다. 기본 Aurora 데이터베이스에 쓰고 로컬 엔드포인트에 읽기를 보내려면 애플리케이션을 업데이트해야 합니다.

잘못됨: A. S3는 동적 웹 사이트이므로 웹 서버의 대체품으로 사용할 수 없으며 S3는 정적 웹 사이트를 호스팅하는 데만 사용할 수 있습니다.

잘못됨: B. AWS Direct Connect(DX) 연결은 여기에서 의미가 없습니다. DX 연결은 데이터 센터와 AWS 간의 네트워크 성능을 최적화하는 데 사용됩니다.

잘못됨: C. 데이터베이스 유형을 마이그레이션하거나 EC2 인스턴스 대신 Lambda 함수를 사용할 필요가 없습니다. Auto Scaling EC2 인스턴스를 사용하면 적절한 성능을 제공할 수 있으며 프로세스가 얼마나 오래 실행될 수 있으며 서버리스 기능으로 마이그레이션할 수 있는지 여부도 알 수 없습니다. 여기에 비용 절감에 대한 언급도 없으며 계층 분리에 대한 요구 사항도 없습니다.

참조:

https://aws.amazon.com/rds/aurora/global-database/

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Q77

회사는 프런트 엔드 및 전자 상거래 계층으로 전자 상거래 플랫폼을 운영합니다.두 계층 모두 LAMP 스택에서 실행되며 AWS에 가상 제품이 있는 로드 밸런싱 어플라이언스 뒤에서 프런트 엔드 인스턴스가 실행됩니다. 현재 운영 팀은 SSH를 사용하여 인스턴스에 로그인하여 패치를 유지 관리하고 다른 문제를 해결합니다. 이 플랫폼은 최근 다음과 같은 여러 공격의 대상이었습니다.

\* 디도스 공격

\* SOL 주입 공격

\* 웹 서버의 SSH 계정에 대한 몇 가지 성공적인 사전 공격.

이 회사는 AWS로 마이그레이션하여 전자 상거래 플랫폼의 보안을 개선하고자 합니다.이 회사의 솔루션 설계자는 다음 접근 방식을 사용하기로 결정했습니다.

\* 기존 애플리케이션 코드 검토 및 SQL 삽입 문제 해결

\* 웹 애플리케이션을 AWS로 마이그레이션하고 최신 AWS Linux AMI를 활용하여 초기 보안 패치를 해결

\* 시스템 관리자가 필요에 따라 모든 인스턴스에서 명령을 실행할 수 있도록AWS Systems Manager를 설치하여 패치를 관리

높은 가용성을 제공하고 위험을 최소화하면서 식별된 공격 유형 중 처리할 추가 단계는 무엇입니까?

A. 특정 IP에 대한 액세스를 제한하는 보안 그룹을 사용하여 Amazon EC2 인스턴스에 대한 SSH 액세스를 활성화합니다. 온프레미스 MySQL을 Amazon RDS 다중 AZ로 마이그레이션합니다. AWS Marketplace에서 타사 로드 밸런서를 설치하고 기존 규칙을 로드 밸런서의 AWS 인스턴스로 마이그레이션합니다. DDoS 보호를 위해 AWS Shield표준을 활성화합니다.

B. Amazon EC2 인스턴스에 대한 SSH 액세스를 비활성화합니다. 온프레미스 MySQL을 Amazon RDS 다중 AZ로 마이그레이션 Elastic로드 밸런서를 활용하여 로드를 분산하고 보호를 위해 AWS Shield 어드밴스드를 활성화합니다. 웹 사이트 앞에 Amazon CloudFront 배포를 추가합니다. 배포에서 AWS WAF를 활성화하여 규칙을 관리합니다.

C. 특정 IP 주소에 대한 액세스를 제한하여 보안이 설정된 배스천 호스트를 통해 Amazon EC2 인스턴스에 대한 SSH 액세스 활성화 온프레미스 MySQL을 자체 관리형 EC2 인스턴스로 마이그레이션 AWS Elastic로드 밸런서를 활용하여 로드를 분산하고 DDoS 보호를 위한 AWS Shield 표준을 활성화합니다. 웹 사이트 앞에 Amazon CloudFront 배포를 추가합니다.

D. EC2 인스턴스에 대한 SSH 액세스를 비활성화합니다. 온프레미스 MySQL을 Amazon RDS 단일 AZ로 마이그레이션합니다. AWS Elastic 로드 밸런서를 활용하여 로드 분산 웹 사이트 앞에 Amazon CloudFront 배포를 추가합니다. 배포에서 AWS WAF를 활성화하여 규칙을 관리합니다.

Answer: B

Q78

한 회사가 온프레미스 데이터 센터를 AWS 클라우드로 마이그레이션하려고 합니다. 여기에는 수천 개의 가상화된 Linux 및 Microsoft Windows 서버, SAN 스토리지, MySQL을 사용하는 Java 및 PHP 애플리케이션, Oracle 데이터베이스가 포함됩니다. 동일한 데이터 센터 또는 외부에서 호스팅되는 많은 종속 서비스가 있습니다. 기술 문서가 불완전하고 오래되었습니다. 솔루션 설계자는 현재 환경을 이해하고 마이그레이션 후 클라우드 리소스 비용을 추정해야 합니다.

솔루션 설계자가 클라우드 마이그레이션을 계획하기 위해 사용해야 하는 도구 또는 서비스는 무엇입니까?(세 개 선택)

A. AWS Application Discovery Service

B. AWS SMS

C. AWS X-Ray

D. AWS Cloud Adoption Readiness Tool (CART)

E. Amazon Inspector

F. AWS Migration Hub

Answer: A, D, F

설명

도구와 서비스의 조합은 이 조직이 클라우드 마이그레이션을 계획하는 데 도움이 됩니다. AWS Application Discovery Service는 기업 고객이 온프레미스 데이터 센터에 대한 정보를 수집하여 마이그레이션 프로젝트를 계획하는 데 도움이 됩니다.

AWS Application Discovery Service는 서버 사용 데이터 및 종속성 매핑을 수행하고 서버에서 구성, 사용량 및 동작 데이터를 수집 및 표시하여 워크로드를 더 잘 이해할 수 있도록 도와줍니다.

이 데이터를 CSV 파일로 내보내고 이를 사용하여 AWS에서 실행하는 총 소유 비용(TCO)을 추정하고 AWS로의 마이그레이션을 계획할 수 있습니다. 또한 이 데이터는 검색된 서버를 마이그레이션하고 AWS로 마이그레이션되는 진행 상황을 추적할 수 있는 AWS Migration Hub에서도 사용할 수 있습니다.

AWS Cloud Adoption Readiness Tool (CART)는 모든 규모의 조직이 클라우드 채택 및 엔터프라이즈 클라우드 마이그레이션을 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 됩니다. 이 16개 질문으로 구성된 온라인 설문 조사 및 평가 보고서는 비즈니스, 사람, 프로세스, 플랫폼, 운영 및 보안을 포함한 6가지 관점에서 클라우드 마이그레이션 준비 상태를 자세히 설명합니다.

참조:

https://aws.amazon.com/application-discovery/

https://cloudreadiness.amazonaws.com/#/cart

https://aws.amazon.com/migration-hub/

Q79

한 회사에서 사용자 지정 지표에 따라 동적으로 확장되는 Auto Scaling 그룹에서 온디맨드 Amazon EC2 인스턴스를 사용하여 웹 애플리케이션을 실행하고 있습니다. 광범위한 테스트를 거친 후 회사는 m5.2xlarge 인스턴스 크기가 워크로드에 가장 적합하다고 판단했습니다. 애플리케이션 데이터는 최적의 것으로 확인된 db.r4.4xlarge Amazon RDS 인스턴스에 저장됩니다. 웹 애플리케이션에 대한 트래픽은 하루 동안 무작위로 급증합니다. 응용 프로그램의 안정성에 영향을 주지 않으면서 비용을 추가로 절감하기 위해 회사에서 구현해야 하는 다른 비용 최적화 방법은 무엇입니까?

A. Auto Scaling 그룹에서 인스턴스 수를 두 배로 늘리고 인스턴스 크기를 m5.large로 줄입니다.

B. RDS 데이터베이스의 용량과 지속적으로 실행되는 최소 EC2 인스턴스 수를 예약합니다.

C. RDS 인스턴스 크기를 db.r4.xlarge로 줄이고 동일한 크기의 읽기 전용 복제본 5개를 추가하여 안정성을 제공합니다.

D. 모든 EC2 인스턴스에 대한 용량을 예약하고 RDS 데이터베이스에 스팟 인스턴스 요금을 활용합니다.

Answer: B

Q80

한 솔루션스 아키텍트가 AWS에서 실행되는 최근 마이그레이션된 애플리케이션의 안정성을 평가하고 있습니다. 프런트 엔드는 Amazon S3에서 호스팅되며 Amazon CloudFront에 의해 가속화됩니다. 애플리케이션 계층은 탄력적 IP 주소를 사용하는 Amazon EC2 온디맨드 인스턴스의 상태 비저장 Docker 컨테이너에서 실행됩니다. 스토리지 계층은 애플리케이션 계층과 동일한 가용 영역의 EC2 예약 인스턴스에서 실행되는 MongoDB 데이터베이스입니다.

애플리케이션 코드 변경을 최소화하면서 단일 장애 지점을 제거하기 위해 솔루션 설계자가 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. Amazon API Gateway에서 REST API를 생성하고 AWS Lambda 함수를 애플리케이션 계층으로 사용합니다.

B. 애플리케이션 로드 밸런서를 생성하고 Docker 컨테이너를 AWS Fargate로 마이그레이션합니다.

C. 스토리지 계층을 Amazon DynamoDB로 마이그레이션합니다.

D. 스토리지 계층을 Amazon DocumentDB로 마이그레이션합니다 (MongoDB 호환성 사용).

E. 애플리케이션 로드 밸런서를 생성하고 스토리지 계층을 EC2 Auto Scaling 그룹으로 이동합니다.

Answer: B, D

Q81

한 회사가 인프라를 AWS 클라우드로 마이그레이션하고 있습니다. 회사는 다양한 프로젝트에 대한 다양한 규제 표준을 준수해야 합니다. 회사에는 다중 계정 환경이 필요합니다. 솔루션 설계자는 기본 인프라를 준비해야 합니다. 솔루션은 일관된 관리 및 보안 기준을 제공해야 하지만 다양한 AWS 계정 내에서 다양한 규정 준수 요구 사항에 대한 유연성을 제공해야 합니다. 또한 이 솔루션은 기존 온-프레미스 AD FS (Active Directory Federation Services) 서버와 통합해야 합니다.

운영 오버헤드가 가장 적은 상태에서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 조직에서 조직을 생성합니다. 모든 계정에서 최소 권한 액세스를 위해 단일 SCP를 만듭니다.모든 계정에 대해 단일 OU를 만듭니다. 온프레미스 AD FS 서버와 페더레이션할 IAM 자격 증명 공급자를 구성합니다. 로그 생성 서비스가 로그 이벤트를 중앙 계정으로 보내도록 정의된 프로세스를 사용하여 중앙 토글 계정을 구성합니다. 모든 계정에 대한 적합성 팩이 있는 중앙 계정에서 AWS Config를 활성화합니다.

B. AWS 조직에서 조직을 생성합니다. 조직에서 AWS 컨트롤 타워를 활성화합니다.SCP에 포함된 가드레일을 검토하십시오. AWS Config에서 추가가 필요한 영역을 확인합니다. 필요에 따라 OU를 추가합니다. 온프레미스 AD FS 서버에 AWS 싱글 사인온을 연결합니다.

C. AWS 조직에 조직을 생성합니다. 최소 권한 액세스를 위한 SCP 생성 OU 구조를 생성하고 이를 사용하여 AWS 계정을 그룹화합니다. AWS Single Sign-On을 온프레미스 AD FS 서버에 연결합니다. 로그 생성 서비스를 위해 정의된 프로세스를 사용하여 중앙 로깅 계정을 구성하여 중앙 계정 Enable AWS에 로그 이벤트를 전송합니다. 애그리게이터 및 적합성 팩을 사용하여 중앙 계정에서 구성합니다.

D. AWS 조직에 조직을 생성합니다. 조직에서 AWS 관제탑을 활성화합니다. SCP에 대한 가드레일을 검토하십시오. AWS Config에서 추가가 필요한 영역을 확인하십시오. 온프레미스 ADFS 서버와의 페더레이션을 위해 IAM 자격 증명 공급자를 구성합니다.

Answer: A

Q82

한 회사에서 AWS로 마이그레이션할 계획입니다. 솔루션 설계자는 플릿에서 AWS 애플리케이션 검색 서비스를 사용하여 Oracle 데이터 웨어하우스와 여러 PostgreSQL 데이터베이스가 있음을 발견합니다.

라이선스 비용과 운영 오버헤드를 줄일 수 있는 마이그레이션 패턴의 조합은 무엇입니까?(두 개 선택)

A. AWS DMS를 사용하여 Oracle 데이터 웨어하우스를 Amazon EC2로 옮깁니다.

B. AWS SCT 및 AWS DMS를 사용하여 Oracle 데이터 웨어하우스를 Amazon Redshift로 마이그레이션합니다.

C. AWS DMS를 사용하여 PostgreSQL 데이터베이스를 들어 올리고 Amazon EC2로 이동합니다.

D. AWS DMS를 사용하여 PostgreSQL 데이터베이스를 포스트그레SQL용 Amazon RDS로 마이그레이션합니다.

E. AWS DMS를 사용하여 Oracle 데이터 웨어하우스를 Amazon EMR 관리형 클러스터로 마이그레이션합니다.

Answer: B, D

설명

이 시나리오에서 우리는 각 데이터베이스를 실행할 최적의 플랫폼과 거기에 도달하기 위한 최적의 마이그레이션 경로를 결정해야 합니다. 비용 및 운영 오버헤드를 최소화해야 합니다.

Oracle 데이터 웨어하우스를 위한 최상의 솔루션은 데이터 웨어하우스(OLAP용 관계형 DB 사용 사례)를 실행하도록 설계된 관리형 서비스인 Amazon RedShift로 마이그레이션하는 것입니다. 이렇게 하려면 스키마를 수정해야 하므로 AWS SCT를 사용해야 하며 AWS DMS가 실제 데이터를 마이그레이션할 수 있습니다.

MySQL 데이터베이스의 경우 MySQL용 Amazon RDS에서 실행할 수 있습니다. 이렇게 하면 관리 서비스가 제공되며 스키마를 수정할 필요가 없습니다. 따라서 AWS SCT 없이 AWS DMS를 사용할 수 있습니다.

참조:

https://aws.amazon.com/getting-started/hands-on/migrate-oracle-to-amazon-redshift/

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-mysql-database-to-amazon-rds-for-mysql.html

Q83

한 솔루션 설계자가 10개의 기존 계정이 있는 다중 계정 구조를 설계하고 있습니다. 설계는 다음 요구 사항을 충족해야 합니다.

\* 모든 계정을 하나의 조직으로 통합합니다.

\* 관리 계정 및 보조 계정에서 Amazon EC2 서비스에 대한 전체 액세스 권한을 허용합니다.

\* 보조 계정을 추가하는 데 필요한 노력을 최소화하십시오.

솔루션에 어떤 단계 조합을 포함해야 합니까?(두 개 선택)

A. 관리 계정에서 조직 만들기 관리 계정에서 보조 계정으로 초대 보내기 초대를 수락하고 OU를 만듭니다.

B. 관리 계정에서 조직을 만듭니다. 각 보조 계정에서 관리 계정으로 조인 요청을 보냅니다. 요청을 수락하고 OU를 만듭니다.

C. 관리 계정과 보조 계정 간에 VPC 피어링 연결을 생성합니다. VPC 피어링 연결 요청을 수락합니다.

D. 전체 EC2 액세스를 가능하게 하는 SCP (서비스 제어 정책) 를 생성하고 정책을 OU에 연결합니다.

E. 전체 EC2 액세스 정책을 생성하고 정책을 각 계정의 역할에 매핑합니다. 다른 모든 계정을 신뢰하여 역할을 맡습니다.

Answer: A, E

Q84

소매업체에서는 Amazon S3 버킷에 인보이스 파일을 저장하고 파일에 대한 메타데이터를 Amazon DynamoDB 테이블에 저장하는 애플리케이션을 실행 중입니다. 애플리케이션 소프트웨어는 us-east-1과 eu-west-1에서 모두 실행됩니다. S3 버킷과 DynamoDB 테이블은 us-east-1에 있습니다. 이 회사는 데이터 손상 및 두 지역에 대한 연결 손실로부터 스스로를 보호하고자 합니다.

이러한 요구 사항을 충족하는 옵션은 무엇입니까?

A. DynamoDB 글로벌 테이블을 생성하여 us-east-1과 eu-west-1 간에 데이터를 복제합니다. us-east-1의 DynamoDB 테이블에서 연속 백업을 활성화합니다. S3 버킷에서 버전 관리를 활성화합니다.

B. Amazon CloudWatch Events에 의해 트리거되는 AWS Lambda 함수를 생성하여 DynamoDB 테이블을 정기적으로 백업합니다. us-east-1에서 eu-west-1으로의 S3 교차 리전 복제를 설정합니다. us-east-1의 S3 버킷에서 MFA 삭제를 설정합니다.

C. DynamoDB 글로벌 테이블을 생성하여 us-east-1과 eu-west-1 간에 데이터를 복제합니다. S3 버킷에서 버전 관리를 활성화합니다. S3 버킷에 엄격한 ACL을 구현합니다.

D. DynamoDB 글로벌 테이블을 생성하여 us-east-1과 eu-west-1 간에 데이터를 복제합니다. us-east-1의 DynamoDB 테이블에서 연속 백업을 활성화합니다. us-east-1에서 eu-west-1으로의 S3 교차 리전 복제를 설정합니다.

Answer: D

설명

DynamoDB 글로벌 테이블은 다중 지역, 다중 활성 데이터베이스입니다. 즉, 여러 리전에서 테이블을 생성하고 해당 테이블에 쓸 수 있으며 AWS가 항목을 동기화합니다. 이것은 데이터베이스 테이블에 필요한 중복성을 제공합니다. DynamoDB 연속 백업을 활성화할 수 있습니다. 이는 초당 세분성을 제공하고 PITR이 활성화된 시간부터 이전 35일까지의 1초 단위로 복원합니다. 이것은 데이터 손상으로부터 보호합니다.

Amazon S3의 경우 버전 관리가 활성화되어야 하는 교차 리전 복제를 활성화할 수 있습니다. 이것은 변경 사항의 동기화와 데이터 손상의 경우 버전 관리 기록을 제공합니다.

잘못됨: A는 올바르지 않습니다. ACL은 데이터 손상으로부터 보호할 수 없으며 여기에 DynamoDB 테이블의 데이터를 손상으로부터 보호하기 위한 솔루션이 없습니다.

잘못됨: B는 올바르지 않습니다. 연속 백업만 활성화하면 Lambda를 사용할 필요가 없습니다. MFA 삭제는 데이터 손상으로부터 보호하지 않습니다.

잘못됨: C는 올바르지 않습니다. 버전 관리는 데이터 손상에 도움이 되지만 데이터를 다른 리전에 복제하는 솔루션은 없습니다.

참조:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html

https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-continuous-backups-and-point-in-time-recovery-pitr/

Q85

한 회사에서 호스팅하거나 온프레미스하는 VMware vSphere VM에서 Windows 서버를 실행하는 애플리케이션을 개발했습니다. 응용 프로그램 데이터는 응용 프로그램을 통해 읽어야 하는 독점 형식으로 저장됩니다. 회사는 서버와 애플리케이션을 수동으로 프로비저닝했습니다. Pan of us 재해 복구 계획으로서 이 회사는 AWS에서 애플리케이션을 호스팅할 수 있는 기능이 일시적으로 회사의 온프레미스 환경을 사용할 수 없게 되었다고 경고합니다. 이 회사는 재해 복구 이벤트가 RPO 15 5분에 완료된 후 애플리케이션이 온프레미스 호스팅으로 돌아가기를 원합니다.

운영 오버헤드가 가장 적은 상태에서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 데이터 동기화를 구성합니다. 데이터를 Amazon Elastic Block Store (Amazon EBS) 볼륨으로 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 AWS CloudFormation 템플릿을 사용하여 Amazon EC2 인스턴스를 프로비저닝하고 EBS 볼륨을 연결합니다.

B. CloudEndure 재해 복구 구성 Amazon Elastic Block Store (Amazon EBS) 볼륨에 연결된 복제 Amazon EC2 인스턴스에 데이터를 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 CloudEndure를 사용하여 복제된 볼륨을 사용하는 EC2 인스턴스를 시작합니다.

C. AWS 스토리지 게이트웨이 웹 게이트웨이를 프로비저닝합니다. 데이터 로그를 Amazon S3 버킷으로 다시 생성합니다.온프레미스 환경을 사용할 수 없는 경우 AWS Backup을 사용하여 데이터를 Amazon Elastic Block Store (Amazon EBS) 볼륨으로 복원하고 이러한 EBS 볼륨에서 Amazon EC2 인스턴스를 시작합니다.

D. AWS에서 Windows용 Amazon FS\* 파일 서버 파일 시스템을 프로비저닝합니다. 시스템에 데이터를 복제합니다. 온프레미스 환경을 사용할 수 없는 경우 AWS CloudFormation 템플릿을 사용하여 Amazon EC2 인스턴스를 프로비저닝하고 AWS:CloudFormation: :lnit 명령을 사용하여 Amazon FSx 파일 공유를 마운트합니다.

Answer: D

Q86

한 회사에서 오라클용 Amazon RDS 데이터베이스를 다른 AWS 계정의 PostgreSQL용 RDS DB 인스턴스로 마이그레이션할 계획입니다. 솔루션 설계자는 다운타임이 필요 없고 마이그레이션을 완료하는 데 필요한 시간을 최소화할 수 있는 마이그레이션 전략을 설계해야 합니다. 마이그레이션 전략은 모든 기존 데이터와 마이그레이션 중에 만들어진 새 데이터를 복제해야 합니다. 마이그레이션 프로세스 완료 시 대상 데이터베이스는 원본 데이터베이스와 동일해야 합니다. 현재 모든 애플리케이션은 Oracle DB 인스턴스용 RDS와 통신하기 위한 엔드포인트로 Amazon Route 53 CNAME 레코드를 사용합니다. Oracle DB용 RDS는 프라이빗 서브넷에 있습니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. 대상 계정에 PostgreSQL DB 인스턴스용 새 RDS를 생성합니다. AWS 스키마를 사용합니다. 변환 도구 (AWS SCT) 를 사용하여 원본 데이터베이스에서 대상 데이터베이스로 데이터베이스 스키마를 마이그레이션합니다.

B. AWS 스키마 변환 도구 (AWS SCT) 를 사용하여 원본 데이터베이스의 스키마 및 초기 데이터가 있는 대상 계정에 PostgreSQL DB 인스턴스용 새 RDS를 생성합니다.

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

D. 일시적으로 원본 DB 인스턴스에 공개적으로 액세스할 수 있도록 허용하여 대상 계정의 VPC에서 연결을 제공합니다. 대상 계정의 VPC에서 데이터베이스 포트의 트래픽을 허용하도록 각 DB 인스턴스에 연결된 보안 그룹을 구성합니다.

E. 대상 계정에서 AWS DMS (데이터베이스 마이그레이션 서비스) 를 사용하여 원본 데이터베이스에서 대상 데이터베이스로 전체 로드+변경 데이터 캡처 (CDC) 마이그레이션을 수행합니다. 마이그레이션이 완료되면 대상 DB 인스턴스 엔드포인트를 가리키도록 CNAME 레코드를 변경합니다.

F. 대상 계정에서 AWS DMS (데이터베이스 마이그레이션 서비스) 를 사용하여 원본 데이터베이스에서 대상 데이터베이스로 변경 데이터 캡처 (CDC) 마이그레이션을 수행합니다. 마이그레이션이 완료되면 대상 DB 인스턴스 엔드포인트를 가리키도록 CNAME 레코드를 변경합니다.

Answer: B, C, E

Q87

한 회사의 CISO는 솔루션 설계자에게 회사의 현재 CI/CD 관행을 다시 엔지니어링하여 취약점이 발견될 경우 가동 중지 시간을 최소화하면서 애플리케이션에 패치를 최대한 빨리 배포할 수 있도록 해달라고 요청했습니다. 또한 오류 발생 시 변경 사항을 신속하게 롤백할 수 있어야 합니다. 웹 애플리케이션은 애플리케이션 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스 플릿에 배포됩니다. 이 회사는 현재 GitHub를 사용하여 애플리케이션 소스 코드를 호스팅하고 있으며 애플리케이션을 빌드하도록 AWS CodeBuild 프로젝트를 구성했습니다. 이 회사는 또한 AWS CodePipeline을 사용하여 기존 코드빌드 프로젝트를 사용하여 GitHub 커밋에서 빌드를 트리거할 계획입니다.

모든 요구 사항을 충족하는 CI/CD 구성은 무엇입니까?

A. 인플레이스(in-place) 배포용으로 구성된 AWS CodeDeploy를 사용하여 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있으면 다른 코드 업데이트를 푸시합니다.

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 배포 단계로 CodePipeline을 구성하여 테스트 및 프로덕션 스택용 파이프라인을 생성합니다. 새로 배포된 코드를 모니터링하고 문제가 있는 경우 다른 코드 업데이트를 푸시합니다.

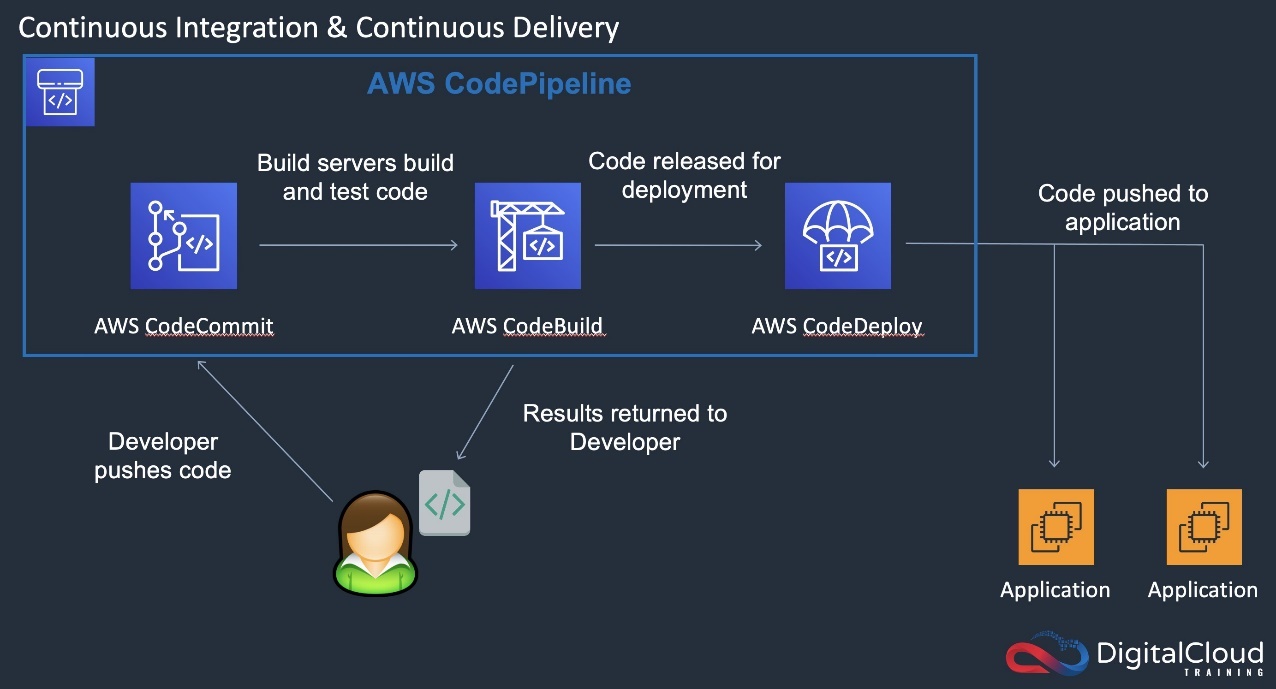
D. AWS OpsWorks 및 현재 위치 배포를 사용하여 배포 단계로 CodePipeline을 구성합니다. 새로 배포된 코드를 모니터링하고 문제가 있으면 다른 코드 업데이트를 푸시합니다.

Answer: B

설명

업데이트를 빠르게 배포하는 가장 좋은 방법은 소스를 CodeCommit으로 설정하고 빌드를 CodeBuild 프로젝트로 설정하고 배포 단계를 CodeDeploy를 사용하여 업데이트를 애플리케이션에 푸시하도록 구성된 CodePipeline에서 파이프라인을 생성하는 것입니다. 블루/그린 배포 전략은 코드에 문제가 있는 경우 롤백을 쉽고 빠르게 수행할 수 있도록 합니다.

이 솔루션에 설명된 아키텍처는 다음 다이어그램과 같습니다.



잘못됨: A. 인플레이스(in-place) 배포 전략을 사용하면 모든 애플리케이션 인스턴스가 동시에 업데이트되므로 코드에 문제가 있는 경우 더 많은 사용성 문제가 발생할 수 있으며 롤백에 더 많은 시간이 소요되고 중단됩니다.

잘못됨: C. CodeDeploy는 블루/그린 배포 전략과 함께 사용해야 합니다. 이것은 더 간단하고 단계적 방식으로 새 코드로 전환하고 문제가 발생할 경우 축소할 수 있는 원활한 기능을 제공합니다.

잘못됨: D. OpsWorks가 아닌 CodeDeploy를 사용하고 인플레이스 대신 블루/그린 배포 전략을 사용해야 합니다.

참조:

https://aws.amazon.com/blogs/devops/use-aws-codedeploy-to-implement-blue-green-deployments-for-aws-fargate-and-amazon-ecs/

Q88

한 회사가 데이터 분석 환경을 온프레미스에서 AWS로 마이그레이션하려고 합니다.　환경은 두 개의 간단한 Node js 애플리케이션으로 구성됩니다.　애플리케이션 중 하나가 센서 데이터를 수집하여 MySQL 데이터베이스에 로드합니다.　다른 애플리케이션은 데이터를 보고서로 집계합니다.　집계 작업이 실행될 때. 일부 로드 작업이 올바르게 실행되지 않습니다.　회사는 데이터 로드 문제를 해결해야 합니다.　또한 회사 고객의 중단이나 변경 없이 마이그레이션을 수행해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. Amazon Aurora MySQL 데이터베이스를 온프레미스 데이터베이스의 복제 대상으로 설정합니다.　Aurora MySQL 데이터베이스에 대한 Aurora 복제본을 생성하고 Aurora 복제본에 대해 실행할 집계 작업을 이동합니다.　수집 엔드포인트를 NLB (네트워크 로드 밸런서) 뒤에서 AWS Lambda 함수로 설정하고 Amazon RDS 프록시를 사용하여 Aurora MySQL 데이터베이스에 씁니다. 데이터베이스가 동기화되면 복제 작업을 비활성화하고 Aurora 복제본을 기본 인스턴스로 다시 시작합니다.　수집기 DNS 레코드가 NLB를 가리키도록 합니다.

B. Amazon Aurora MySQL 데이터베이스 설정 AWS DMS (데이터베이스 마이그레이션 서비스) 를 사용하여 온프레미스 데이터베이스에서 Aurora로 연속 데이터 복제 수행 Aurora MySQL 데이터베이스에 대해 실행할 집계 작업 이동 ALB (애플리케이션 로드 밸런서) 뒤에 수집 엔드포인트를 Amazon으로 설정Auto Scaling 그룹의 EC2 인스턴스 데이터베이스가 동기화되면 수집기 DNS 레코드가 ALB를 가리키도록 합니다. 　온프레미스에서 AWS로 전환한 후 AWS DMS 동기화 작업을 비활성화합니다.

C. Amazon Aurora MySQL 데이터베이스 설정 AWS DMS (데이터베이스 마이그레이션 서비스) 를 사용하여 온프레미스 데이터베이스에서 Aurora로 연속 데이터 복제 수행 Aurora MySQL 데이터베이스용 Aurora 복제본을 생성하고 Aurora에 대해 실행할 집계 작업을 이동합니다.　복제본 애플리케이션 로드 밸런서 (ALB) 뒤에서 AWS Lambda가 작동하도록 수집 엔드포인트를 설정하고 Amazon RDS 프록시를 사용하여 Aurora MySQL 데이터베이스에 씁니다.　데이터베이스가 동기화되면 수집기 DNS 레코드가 ALB를 가리키도록 합니다. 온프레미스에서 AWS로 전환한 후 AWS DMS 동기화 작업을 비활성화합니다.

D. Amazon Aurora MySQL 데이터베이스 설정 Aurora MySQL 데이터베이스에 대한 Aurora 복제본을 생성하고 Aurora 복제본에 대해 실행할 집계 작업을 이동합니다. 수집 엔드포인트를 Amazon Kinesis 데이터 스트림으로 설정합니다.　 Amazon Kinesis Data Firehose를 사용하여 데이터를 Aurora MySQL 데이터베이스로 복제합니다.　 데이터베이스가 동기화되면 복제 작업을 비활성화하고 기본 인스턴스로 Aurora 복제본을 다시 시작합니다. 수집기 DNS 레코드가 Kinesis 데이터 스트림을 가리키도록 합니다.

Answer: C

Q89

대기업은 단일 AWS 리전에서 실행되는 비즈니스 크리티컬 애플리케이션을 보유하고 있습니다. 애플리케이션은 여러 Amazon EC2 인스턴스와 하나의 Amazon RDS 다중 AZ DB 인스턴스로 구성됩니다. EC2 인스턴스는 여러 가용 영역에 걸쳐 하나의 Amazon EC2 오토 스케일링 그룹에서 실행됩니다. 솔루션 설계자가 애플리케이션에 대한 재해 복구 (DR) 계획을 구현하고 있습니다. 솔루션 설계자는 DR 리전이라고 하는 새 리전에 파일럿 라이트 애플리케이션 배포를 만들었습니다. DR 환경에는 단일 EC2 인스턴스와 RDS DB 인스턴스의 읽기 전용 복제본이 있는 Auto Scaling 그룹이 있습니다. 솔루션 설계자는 기본 애플리케이션 환경에서 DR 지역의 파일럿 라이트 환경으로 페일오버를 자동화해야 합니다.

운영 효율성이 가장 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 기본 리전의 애플리케이션 환경에서 재해 복구 리전의 Amazon CloudWatch에 애플리케이션 가용성 지표를 게시합니다. 애플리케이션 가용성 지표 전송이 중지될 때 호출되는 CloudWatch 경보를 DR 리전에 생성합니다. 재해 복구 리전의 Amazon Simple Notification Service (Amazon SNS) 주제에 알림을 보내도록 CloudWatch 경보를 구성합니다. 애플리케이션 소유자에게 메시지를 전송하는 SNS 주제에 이메일 구독을 추가합니다. 알림이 표시되면 시스템 운영자에게 AWS Management Console에 로그인하고 애플리케이션에 대한 장애 조치 작업을 시작하도록 지시합니다.

B. 기본 리전에서 애플리케이션의 EC2 인스턴스 중 하나를 사용하여 5분마다 실행되는 cron 작업 생성 애플리케이션이 사용 가능한지 여부를 확인하도록 cron 작업을 구성합니다. 오류가 발생하면 cron 작업이 시스템 운영자에게 알리고 애플리케이션 서비스를 다시 시작하려고 합니다.

C. 기본 리전에서 애플리케이션의 EC2 인스턴스 중 하나를 사용하여 5분마다 실행되는 cron 작업 생성 cron 작업을 구성하여 애플리케이션이 사용 가능한지 확인합니다. 실패 시 크론 작업은 읽기 전용 복제본을 승격하고 Auto Scaling 그룹에 EC2 인스턴스를 추가하여 DR 환경을 수정합니다.

D. 기본 리전의 애플리케이션 환경에서 재해 복구 리전의 Amazon CloudWatch에 애플리케이션 가용성 메트릭을 게시합니다. 애플리케이션 가용성 메트릭의 전송이 중지될 때 호출되는 CloudWatch 경보를 DR 리전에 생성합니다. 알림을 보내도록 CloudWatch 경보를 구성합니다. DR 리전의 Amazon Simple Notification Service (Amazon SNS) 주제로 읽기 전용 복제본을 승격하고 EC2 인스턴스를 Auto Scaling 그룹에 추가하려면 재해 복구 리전의 Amazon SNS에서 호출하는 AWS Lambda 함수를 사용합니다.

Answer: D

Q90

소프트웨어 개발 회사에는 원격으로 작업하는 여러 엔지니어가 있습니다.이 회사는 Amazon EC2 인스턴스에서 AD DS (액티브 디렉토리 도메인 서비스) 를 실행하고 있습니다.이 회사의 보안 정책에 따르면 VPC에 배포된 모든 내부 비공개 서비스는 VPN MFA (다단계 인증) 를 통해 액세스할 수 있어야 하며 VPN에 액세스하는 데 사용해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. AWS 사이트 간 VPN 연결 생성 VPN과 AD DS 간의 통합을 구성합니다. MFA 지원이 활성화된 Amazon 워크스페이스 클라이언트를 사용하여 VPN 연결을 설정합니다.

B. AWS 클라이언트 VPN 엔드포인트를 생성합니다. AD DS와의 통합을 위한 AD 커넥터 디렉터리를 만듭니다. AD 커넥터용 MFA를 활성화합니다. AWS 클라이언트 VPN을 사용하여 VPN 연결을 설정합니다.

C. AWS VPN 클라우드허브를 사용하여 여러 AWS 사이트 간 VPN 연결을 생성합니다. AWS VPN 클라우드허브와 AD DS 간의 통합을 구성합니다. AWS Cop4ot을 사용하여 VPN 연결을 설정합니다.

D. Amazon워크링크 엔드포인트를 생성합니다. Amazon워크링크와 AD DS 간의 통합을 구성합니다. Amazon워크링크에서 MFA를 활성화합니다. AWS 클라이언트 VPN을 사용하여 VPN 연결을 설정합니다.

Answer: B

Q91

솔루션스 아키텍트는 Auto Scaling 그룹의 Amazon EC2 인스턴스에 운영 워크로드를 배포했습니다. VPC 아키텍처는 Auto Scaling 그룹이 대상으로 하는 각 서브넷이 있는 2개의 가용 영역 (AZ) 에 걸쳐 있습니다. VPC가 온프레미스 환경에 연결되어 있어 연결을 중단할 수 없습니다. Auto Scaling 그룹의 최대 크기는 서비스 중인 인스턴스 20개입니다. VPC IPv4 주소 지정은 다음과 같습니다.

PVC 사이다: 10.0.0.0/23

AZ1 서브넷 CIDR: 10.0.0.0/24

AZ2 서브넷 CIDR: 10.0.1.0/24

배포 이후 리전에서 세 번째 AZ를 사용할 수 있게 되었습니다. 솔루션 설계자는 IPv4 주소 공간을 추가하지 않고 서비스 중단 없이 새로운 AZ를 채택하려고 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AZ2 서브넷만 사용하도록 Auto Scaling 그룹을 업데이트합니다. 이전 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 만듭니다. 새 AZ1 서브넷도 사용하도록 Auto Scaling 그룹을 조정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 Auto Scaling 그룹을 조정합니다. 현재 AZ2 서브넷을 제거합니다.원래 AZ1 서브넷에서 주소 공간의 두 번째 절반을 사용하여 새 AZ2 서브넷을 만듭니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 만든 다음 세 개의 새 서브넷을 모두 대상으로 하도록 Auto Scaling 그룹을 업데이트합니다.

B. AZ1 서브넷에서 EC2 인스턴스를 종료합니다. 주소 공간의 절반을 사용하여 AZ1 서브넷을 삭제하고 다시 만듭니다. 이 새 서브넷을 사용하도록 Auto Scaling 그룹을 업데이트합니다.두 번째 AZ에 대해 이 단계를 반복합니다. AZ3에서 새 서브넷을 정의한 다음 세 개의 새 서브넷을 모두 대상으로 하도록 Auto Scaling 그룹을 업데이트합니다.

C. 동일한 IPv4 주소 공간을 가진 새 VPC를 생성하고 각 AZ에 하나씩 3개의 서브넷을 정의합니다. 기존 Auto Scaling 그룹을 업데이트하여 새 VPC의 새 서브넷을 대상으로 지정합니다.

D. AZ2 서브넷만 사용하도록 Auto Scaling 그룹을 업데이트합니다. 이전 주소 공간을 갖도록 AZ1 서브넷을 업데이트합니다. AZ1 서브넷도 다시 사용하도록 Auto Scaling 그룹을 조정합니다. 인스턴스가 정상이면 AZ1 서브넷만 사용하도록 Auto Scaling 그룹을 조정합니다. 현재 AZ2 서브넷을 업데이트하고 원래 AZ1 서브넷에서 주소 공간의 두 번째 절반을 할당합니다. 원래 AZ2 서브넷 주소 공간의 절반을 사용하여 새 AZ3 서브넷을 만든 다음 세 개의 새 서브넷을 모두 대상으로 하도록 Auto Scaling 그룹을 업데이트합니다.

Answer: A

Q92

회사에는 퍼블릭 서브넷과 프라이빗 서브넷으로 구분되는 Amazon VPC가 있습니다. 웹 애플리케이션은 Amazon VPC에서 실행되며 각 서브넷에는 자체 NACL이 있습니다. 퍼블릭 서브넷의 CIDR은 10.0.0.0/24입니다. 애플리케이션 로드 밸런서가 퍼블릭 서브넷에 배포됩니다. 프라이빗 서브넷의 CIDR은 10.0.1.0/24입니다. 포트 80에서 웹 서버를 실행하는 Amazon EC2 인스턴스는 프라이빗 서브넷에서 시작됩니다. Application Load Balancer가 웹 애플리케이션에 액세스하는 데 필요한 네트워크 트래픽만 퍼블릭 서브넷과 프라이빗 서브넷 간에 이동할 수 있습니다.

프라이빗 서브넷의 NACL이 요구 사항을 충족하도록 하기 위해 어떤 규칙 모음을 작성해야 합니까?(두 개 선택)

A. 소스 0.0 0.0/0의 포트 80에 대한 인바운드 규칙입니다.

B. 소스 10.0.0.0/24의 포트 80에 대한 인바운드 규칙입니다.

C. 대상 0.0.0.0/0으로 향하는 포트 80에 대한 아웃바운드 규칙입니다.

D. 대상 10.0.0.0/24로 향하는 포트 80에 대한 아웃바운드 규칙입니다.

E. 1024에서 65535까지 대상 10.0.0.0/24로 향하는 포트에 대한 아웃바운드 규칙입니다.

Answer: B, E

Q93

한 회사가 프로덕션 AWS 계정의 Amazon EC2 인스턴스에서 웹 애플리케이션을 실행하고 있습니다. 이 회사는 분석 및 보관을 위해 웹 애플리케이션에서 생성된 모든 로그를 중앙 AWS 계정으로 복사해야 합니다. 회사의 AWS 계정은 현재 독립적으로 관리됩니다. 로깅 에이전트는 중앙 AWS 계정의 Amazon S3 버킷에 tog 파일을 업로드하도록 EC2 인스턴스에 구성됩니다.

솔루션 설계자는 프로덕션 계정이 중앙 계정에 로그 파일을 저장할 수 있는 솔루션에 대한 액세스 권한을 제공해야 합니다. 중앙 계정에는 tog 파일에 대한 읽기 권한도 있어야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 중앙 계정에서 교차 계정 역할을 생성합니다. 로그를 복사할 때 프로덕션 계정의 역할을 가정합니다.

B. 프로덕션 계정 ID를 보안 주체로 사용하여 S3 버킷에 정책을 생성합니다. 위임된 사용자의 S3 액세스를 허용합니다.

C. 프로덕션 계정에 있는 EC2 인스턴스의 CIDR 범위에서만 액세스할 수 있는 S3 버킷에 정책을 생성합니다. 프로덕션 계정 ID를 보안 주체로 사용합니다.

D. 프로덕션 계정에서 교차 계정 역할을 생성합니다. 로그를 복사할 때 프로덕션 계정의 역할을 가정합니다.

Answer: A

Q94

한 회사에서 여러 AWS Lambda 함수와 Amazon DynamoDB 테이블로 구성된 서버리스 애플리케이션을 실행하고 있습니다. 이 회사는 Lambda 함수가 Amazon Neptune DB 클러스터에 액세스해야 하는 새로운 기능을 만들었습니다. Neptune DB 클러스터는 VPC의 세 서브넷에 있습니다.

Lambda 함수가 Neptune DB 클러스터와 DynamoDB 테이블에 액세스할 수 있도록 허용하는 솔루션은 무엇입니까?(두 개 선택)

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. VPC 외부에서 Lambda 함수를 호스팅합니다. Lambda 함수의 IP 범위에서의 액세스를 허용하도록 Neptune 보안 그룹을 업데이트합니다.

D. VPC 외부에서 Lambda 함수를 호스팅합니다. Neptune 데이터베이스에 대한 VPC 엔드포인트를 생성하고 Lambda 함수가 VPC 엔드포인트를 통해 Neptune에 액세스하도록 합니다.

E. Neptune VPC에 프라이빗 서브넷을 세 개 생성합니다. Lambda 함수를 세 개의 새로운 격리된 서브넷으로 호스팅합니다. DynamoDB에 대한 VPC 엔드포인트를 생성하고 DynamoDB 트래픽을 VPC 엔드포인트로 라우팅합니다.

Answer: B, E

Q95

한 회사에서 온프레미스 데이터 분석 애플리케이션을 AWS로 마이그레이션할 계획입니다. 애플리케이션은 여러 서버에서 호스팅되며 일관된 시스템 시간이 필요합니다. 이 회사는 온프레미스 데이터 센터에서 AWS로 AWS Direct Connect 연결을 구축했습니다. 이 회사는 모든 온프레미스 서버의 NTP 소스 역할을 하는 고정밀 stratum-0 아토믹 도크 네트워크 어플라이언스를 보유하고 있습니다. AWS로의 마이그레이션이 완료되면 애플리케이션을 호스팅하는 모든 Amazon EC2 인스턴스의 클럭이 온프레미스 원자시계 네트워크 어플라이언스와 동기화되어야 합니다.

관리 부담을 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 온프레미스 NTP 서버 주소로 DHCP 옵션 세트를 구성합니다. 옵션 세트를 VPC에 할당합니다. AWS와 온프레미스 네트워크 간에 NTP 트래픽이 허용되는지 확인합니다.

B. 169.254.169.123에서 Amazon시간 동기화 서비스를 사용할 사용자 지정 AMI를 생성합니다. 애플리케이션에 이 AMI를 사용합니다. AWS 구성을 사용하여 NTP 구성을 감사합니다.

C. AWS 마켓플레이스에서 타사 시간 서버를 배포합니다. 온-프레미스 원자시계 네트워크 어플라이언스와 동기화하도록 시간 서버를 구성합니다. 타사 서버가 포함된 VPC의 네트워크 ACL에서 NTP 트래픽의 인바운드가 허용되는지 확인합니다.

D. 온프레미스 원자시계 네트워크 어플라이언스에서 VPC로의 IPsec VPN 터널을 생성하여 직접 연결 연결을 통해 트래픽을 암호화합니다. 터널을 통해 NTP 트래픽을 전달하도록 VPC 라우팅 테이블을 구성합니다.

Answer: B

Q96

AWS 고객은 온프레미스에서 실행되는 웹 애플리케이션을 보유하고 있습니다. 웹 애플리케이션은 방화벽 뒤에 있는 타사 API에서 데이터를 가져옵니다. 타사는 각 클라이언트의 허용 목록에서 하나의 공개 CIDR 블록만 허용합니다. 고객이 웹 애플리케이션을 AWS 클라우드로 마이그레이션하려고 합니다. 애플리케이션은 VPC의 애플리케이션 로드 밸런서 (ALB) 뒤에 있는 Amazon EC2 인스턴스 세트에서 호스팅됩니다. ALB는 퍼블릭 서브넷에 있습니다. EC2 인스턴스는 프라이빗 서브넷에 있습니다. NAT 게이트웨이는 프라이빗 서브넷에 대한 인터넷 액세스를 제공합니다.

솔루션 설계자는 마이그레이션 후에도 웹 애플리케이션이 타사 API를 계속 호출할 수 있도록 어떻게 해야 합니까?

A. 고객 소유의 퍼블릭 IP 주소 블록을 VPC에 연결합니다. VPC에서 퍼블릭 서브넷에 퍼블릭 IP 주소 지정을 활성화합니다.

B. AWS 계정에서 고객 소유의 퍼블릭 IP 주소 블록을 등록합니다. 주소 블록에서 Elastic IP 주소를 생성하고 VPC의 NAT 게이트웨이에 할당합니다.

C. 고객 소유 IP 주소 블록에서 Elastic IP 주소를 생성합니다. 정적 탄력적 IP 주소를 ALB에 할당합니다.

D. AWS 계정에서 고객 소유의 퍼블릭 IP 주소 블록을 등록합니다. 주소 블록의 탄력적 IP 주소를 사용하도록 AWS Global Accelerator를 설정합니다. ALB를 액셀러레이터 끝점(endpoint)으로 설정합니다.

Answer: B

Q97

새로운 스타트업이 AWS Lambda를 컴퓨팅의 기본 소스로 사용하여 서버리스 애플리케이션을 실행하고 있습니다. 모든 사용자에게 변경 사항을 배포하기 전에 하위 집합의 사용자가 새 버전의 응용 프로그램을 사용할 수 있도록 해야 합니다. 개발자는 배포를 중지하고 간편한 롤백 메커니즘에 액세스할 수 있어야 합니다. 솔루션스 아키텍트는 새 버전이 출시되면 AWS CodeDeploy를 사용하여 변경 사항을 배포하기로 결정합니다.

솔루션 설계자는 어떤 CodeDeploy 구성을 사용해야 합니까?

A. 블루/그린 배포

B. 선형 배포

C. 카나리아 배포

D. 모든 기능을 한 번에 배포

Answer: C

Q98

AWS 조직 내에 AWS 계정이 많은 조직이 있는 회사가 있습니다. AWS 계정 중 하나가 전송 계정으로 지정되고 다른 모든 AWS 계정과 공유되는 전송 게이트웨이가 있습니다. AWS 사이트 간 VPN 연결은 회사의 글로벌 지사와 전송 계정 간에 구성됩니다. 이 회사는 모든 계정에서 AWS Config를 활성화했습니다. 이 회사의 네트워킹 팀은 글로벌 지사에 속한 내부 IP 주소 범위 목록을 중앙에서 관리해야 합니다. 개발자 이 목록을 참조하여 애플리케이션에 안전하게 액세스할 수 있습니다.

운영 오버헤드가 가장 적은 상태에서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon S3에서 호스팅되고 모든 내부 IP 주소 범위를 나열하는 JSON 파일을 생성합니다. JSON 파일이 업데이트될 때 관련될 수 있는 각 계정에서 Amazon Simple Notification Service (Amazon SNS) 주제를 구성합니다. AWS Lambda 함수를 SNS 주제에 구독하여 업데이트된 IP 주소 범위 보기로 모든 관련 보안 그룹 규칙을 업데이트합니다.

B. 모든 내부 IP 주소 범위를 포함하는 새 AWS Config 관리형 규칙을 생성합니다. 규칙을 사용하여 각 계정의 보안 그룹이 IP 주소 범위 목록을 준수하는지 확인합니다. 탐지된 모든 비준수 보안 그룹을 자동으로 수정하도록 규칙을 구성합니다.

C. 전송 계정에서 모든 내부 IP 주소 범위를 포함하는 VPC 접두사 목록을 생성합니다. AWS 리소스 액세스 관리자를 사용하여 접두사 목록을 다른 모든 계정과 공유합니다. 공유 접두사 목록을 사용하여 보안 그룹 규칙을 다른 계정으로 구성합니다.

D. 전송 계정에서 모든 내부 IP 주소 범위로 보안 그룹을 만듭니다. 전송 계정의 보안을 참조하도록 다른 계정의 보안 그룹을 구성합니다.

Answer: A

Q99

기업에서는 모든 내부 애플리케이션이 연결을 위해 프라이빗 IP 주소를 사용해야 합니다. 한 솔루션스 아키텍트가 이 정책을 수용하기 위해 AWS 퍼블릭 서비스에 연결할 인터페이스 엔드포인트를 설정했습니다. 솔루션 설계자는 서비스 이름이 공용 IP 주소로 확인되고 내부 서비스가 인터페이스 엔드포인트에 연결할 수 없음을 관찰합니다.

이 문제를 해결하기 위해 솔루션 설계자는 어떤 절차를 사용해야 합니까?

A. 인터페이스 엔드포인트에 대한 경로로 서브넷 라우팅 테이블을 업데이트합니다.

B. VPC 속성에서 프라이빗 DNS 옵션을 활성화합니다.

C. AWS 서비스에 연결할 수 있도록 인터페이스 엔드포인트에서 보안 그룹을 구성합니다.

D. 내부 애플리케이션에 대한 조건부 전달자를 사용하여 Amazon Route 53 프라이빗 호스팅 영역을 구성합니다.

Answer: C

설명

엔드포인트 네트워크 인터페이스와 연결된 보안 그룹이 엔드포인트 네트워크 인터페이스와 서비스와 통신하는 VPC의 리소스 간의 통신을 허용하는지 확인해야 합니다.

인터페이스 엔드포인트를 생성하면 엔드포인트별 DNS 호스트 이름이 생성됩니다. AWS 서비스 및 AWS Marketplace 파트너 서비스의 경우 프라이빗 DNS 옵션(기본적으로 활성화됨)은 프라이빗 호스팅 영역을 VPC와 연결합니다.

호스팅 영역에는 VPC에 있는 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인되는 서비스의 기본 DNS 이름(예: ec2.us-east-1.amazonaws.com)에 대한 레코드 세트가 포함되어 있습니다. 이렇게 하면 엔드포인트별 DNS 호스트 이름 대신 기본 DNS 호스트 이름을 사용하여 서비스에 요청할 수 있습니다.

엔드포인트에서 프라이빗 DNS를 활성화하면 인스턴스는 기본 DNS 호스트 이름 또는 엔드포인트별 DNS 호스트 이름을 사용하여 인터페이스 엔드포인트를 통해 AWS 서비스 요청을 보낼 수 있습니다.

잘못됨: A는 올바르지 않습니다. 인터페이스 엔드포인트에 대한 라우팅 테이블을 업데이트할 필요가 없습니다(게이트웨이 엔드포인트에 대해 수행).

잘못됨: B는 올바르지 않습니다. 프라이빗 DNS는 AWS 서비스 및 AWS Marketplace 파트너 서비스용으로 생성된 엔드포인트에 대해 기본적으로 활성화되어 있습니다.

잘못됨: D는 올바르지 않습니다. 이것은 불필요합니다. 프라이빗 호스팅 영역은 프라이빗 DNS 옵션이 활성화된 경우(기본값) VPC와 기본적으로 연결되는 프라이빗 호스팅 영역입니다.

참조:

https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html

https://docs.aws.amazon.com/vpc/latest/userguide/verify-domains.html

Q100

한 회사에서 비즈니스 크리티컬 멀티 티어 애플리케이션을 AWS로 이전하고 있습니다. 아키텍처는 데스크톱 클라이언트 애플리케이션과 서버 인프라로 구성됩니다. 서버 인프라는 애플리케이션 가동 시간 SLA를 99.95% 로 유지하지 못하는 경우가 많은 온프레미스 데이터 센터에 있습니다. 솔루션 설계자는 SLA를 충족하거나 초과할 수 있도록 애플리케이션을 다시 설계해야 합니다. 응용 프로그램에는 단일 가상 시스템에서 실행되는 PostgreSQL 데이터베이스가 포함되어 있습니다. 비즈니스 로직 및 프레젠테이션 계층은 여러 가상 시스템 간에 로드 밸런싱됩니다. 원격 사용자는 이 지연 시간에 민감한 애플리케이션을 사용하는 동안 로드 시간이 느리다고 불평합니다.

다음 중 사용자 환경을 개선하고 비용을 최소화하면서 애플리케이션을 거의 변경하지 않고 가용성 요구 사항을 충족하는 것은 무엇입니까?

A. 데이터베이스를 Amazon EC2의 PostgreSQL 데이터베이스로 마이그레이션합니다. 애플리케이션 로드 밸런서 뒤에 자동으로 확장되는 Amazon ECS 컨테이너에서 애플리케이션 및 프레젠테이션 레이어를 호스팅합니다. 각 최종 사용자에게 Amazon Workspaces 작업 공간을 할당하여 사용자 환경을 개선합니다.

B. 데이터베이스를 Amazon RDS Aurora 포스트그레SQL 구성으로 마이그레이션합니다. 애플리케이션 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스의 Auto Scaling 구성에서 애플리케이션 및 프레젠테이션 계층을 호스팅합니다. Amazon AppStream 2.0을 사용하여 사용자 경험을 개선할 수 있습니다.

C. 데이터베이스를 Amazon RDS PostgreSQL 다중 AZ 구성으로 마이그레이션합니다. 네트워크 로드 밸런서 뒤에 자동으로 확장되는 AWS Fargate 컨테이너에서 애플리케이션 및 프레젠테이션 계층을 호스팅합니다. Amazon ElastiCache를 사용하여 사용자 경험을 개선할 수 있습니다.

D. 두 개 이상의 노드가 있는 Amazon Redshift 클러스터로 데이터베이스를 마이그레이션합니다. 애플리케이션 로드 밸런서 뒤에 자동으로 확장되는 Amazon ECS 컨테이너에서 애플리케이션 및 프레젠테이션 레이어를 결합하고 호스팅합니다. Amazon CloudFront를 사용하여 사용자 환경을 개선할 수 있습니다.

Answer: B

설명

Amazon RDS의 가동 시간 SLA는 99.95%입니다. 따라서 솔루션 비용을 증가시키는 다중 AZ 구성을 추가할 필요가 없습니다. 컴퓨팅 계층의 경우 컨테이너 또는 EC2 인스턴스가 될 수 있습니다. EC2 인스턴스를 사용하여 애플리케이션에 대한 변경을 최소화하는 것이 약간 더 쉬울 수 있지만 작동할 수 있습니다. 사용자 경험 문제를 해결하려면 Amazon AppStream 2.0을 사용해야 합니다.

Amazon AppStream 2.0은 완전 관리형 비영구 애플리케이션 및 데스크톱 스트리밍 서비스입니다. AppStream 2.0에서 데스크톱 애플리케이션을 중앙에서 관리하고 모든 컴퓨터에 안전하게 제공합니다. 애플리케이션이 특정 사용 사례에 최적화된 가상 머신에서 실행되고 각 스트리밍 세션이 네트워크 조건에 자동으로 조정되기 때문에 각 최종 사용자는 유연하고 반응이 빠른 환경을 갖습니다.

잘못됨: A. RDS 관리형 서비스는 데이터베이스에 더 적합하고 AppStream 2.0은 최적화된 데스크톱 애플리케이션에 더 적합합니다.

잘못됨: C. AppStream 2.0은 데스크톱 애플리케이션에 더 적합합니다. ElastiCache는 데이터베이스 쿼리 성능을 향상시킵니다.

잘못됨: D. CloudFront는 데스크톱 애플리케이션의 성능 최적화에 적합하지 않습니다.

참조:

https://aws.amazon.com/rds/sla/

https://aws.amazon.com/appstream2/

Q101

한 기업이 주문 시스템에 이벤트 중심 아키텍처를 채택했습니다. 시스템은 첫 번째 테스트 중에 주문 처리를 중단했습니다. 추가 로그를 조사한 결과 Amazon SQS (Amazon Simple Queue Service) 표준 대기열의 단일 주문 메시지로 인해 백엔드 문제가 발생하여 추가 주문 메시지가 처리되지 않는 것으로 나타났습니다. 대기열의 가시성 제한 시간은 30초이고 백엔드 처리 시간 초과는 10초입니다. 솔루션 설계자는 잘못된 주문 메시지를 평가하고 후속 메시지가 시스템에서 처리되도록 보장해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 접근 방식을 사용해야 합니까?

A. 가시성 제한 시간에 맞게 백엔드 처리 시간 제한을 30초로 늘립니다.

B. 대기열의 가시성 제한 시간을 줄여 잘못된 메시지를 자동으로 제거합니다.

C. 잘못된 메시지를 격리하기 위해 새 SQS FIFO 대기열을 배달 못한 편지 대기열로 구성합니다.

D. 새 SQS 표준 대기열을 배달 못한 편지 대기열로 구성하여 잘못된 메시지를 격리합니다.

Answer: D

Q102

한 회사가 개발, 테스트 및 프로덕션의 세 가지 환경에서 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 이 회사는 AMI를 사용하여 EC2 인스턴스를 배포합니다. 이 회사는 각 환경의 각 릴리스에 대해 사용자 지정 배포 스크립트 및 인프라 오케스트레이션 도구를 사용하여 AMI를 구축합니다. 이 회사는 배포 프로세스에서 오류를 받고 있습니다.운영 체제 패키지를 다운로드하는 동안이나 타사 Git 호스팅 서비스에서 응용 프로그램 코드를 설치하는 동안 오류가 나타납니다. 이 회사는 모든 환경에서 보다 안정적으로 구축해야 합니다.

이러한 요구 사항을 충족하는 단계 조합은 무엇입니까?(세 개 선택)

A. 애플리케이션 코드를 AWS 코드커밋 Git 리포지토리에 미러링합니다. 리포지토리를 사용하여 EC2 AMI를 구축합니다.

B. 릴리스마다 환경마다 하나씩 여러 EC2 AMI를 생성합니다.

C. 모든 환경에서 사용할 각 릴리스마다 EC2 AMI를 하나씩 생성합니다.

D. 애플리케이션 코드를 Amazon S3 스토리지를 사용하는 타사 Git 리포지토리에 미러링합니다. 리포지토리를 배포에 사용합니다.

E. 사용자 지정 스크립트 및 도구를 AWS CodeBuild로 대체합니다. EC2 이미지 빌더를 사용하도록 인프라 배포 프로세스를 업데이트합니다.

Answer: A, C, E

Q103

Amazon ECS 인스턴스 집합은 Amazon SQS 대기열을 폴링하고 Amazon DynamoDB 데이터베이스의 항목을 업데이트하는 데 사용됩니다. 테이블의 항목이 업데이트되지 않고 SQS 대기열이 가득 찼습니다. Amazon CloudWatch 로그에 테이블 업데이트 시도 시 400개의 오류가 일관되게 표시됩니다. 프로비저닝된 쓰기 용량 단위가 적절하게 구성되어 있고 스로틀링이 발생하지 않습니다.

실패의 가능한 원인은 무엇입니까?

A. ECS 서비스가 삭제되었습니다.

B. ECS 구성에 Auto Scaling 그룹이 포함되어 있지 않음

C. ECS 인스턴스 작업 실행 IAM 역할이 수정되었습니다.

D. ECS 임무 역할이 수정되었습니다.

Answer: D

Q104

한 기업이 AWS를 사용하여 웹 서버, 애플리케이션 서버 및 Amazon RDS MySQL 데이터베이스 인스턴스를 포함하는 3계층 애플리케이션을 호스팅합니다. 한 솔루션 설계자가 5분 RPO (복구 지점 목표) 로 재해 복구 (DR) 솔루션을 개발하고 있습니다.

비즈니스 요구 사항을 가장 잘 충족하는 옵션은 무엇입니까?

A. 5분마다 모든 서버의 교차 리전 백업을 수행하도록 AWS Backup을 구성합니다. 재해 발생 시 AWS CloudFormation을 사용하여 백업에서 재해 복구 리전의 3개 계층을 다시 프로비저닝합니다.

B. AWS CloudFormation 드리프트 감지를 사용하여 DR 리전에서 실행 중인 웹 및 애플리케이션 서버 스택의 또 다른 사본을 유지 관리합니다. DB 인스턴스의 교차 리전 스냅샷을 5분마다 DR 리전으로 구성합니다. 재해가 발생할 경우 DR 리전의 스냅샷을 사용하여 DB 인스턴스를 복원합니다.

C. Amazon EC2 이미지 빌더를 사용하여 웹 및 애플리케이션 서버의 AMI를 생성하고 기본 리전과 DR 리전 모두에 복사합니다. DR 리전에 DB 인스턴스의 리전 간 읽기 전용 복제본을 생성합니다.재해가 발생할 경우 읽기 전용 복제본을 마스터로 승격하고 AMI를 사용하여 AWS CloudFormation으로 서버를 다시 프로비저닝합니다.

D. DR 영역에서 웹 및 애플리케이션 서버의 AMI를 생성합니다. 예약된 AWS Glue 작업을 사용하여 DB 인스턴스를 DR 리전의 다른 DB 인스턴스와 동기화합니다. 재해가 발생할 경우 DR 리전의 DB 인스턴스로 전환하고 AMI를 사용하여 AWS CloudFormation으로 서버를 다시 프로비저닝합니다.

Answer: C

Q105

한 회사가 Amazon EC2 인스턴스에서 새로운 웹 애플리케이션을 출시하고 있습니다. 개발 및 프로덕션 워크로드는 별도의 AWS 계정에 존재합니다. 회사의 보안 요구 사항에 따라 자동화된 구성 도구만 프로덕션 계정에 액세스할 수 있습니다. 이 회사의 보안 팀은 프로덕션 AWS 계정 또는 EC2 인스턴스에 대한 수동 액세스가 발생할 경우 즉시 알림을 받고자 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자가 프로덕션 계정에서 수행해야 하는 작업 조합은 무엇입니까?(세 개 선택)

A. 애플리케이션의 기본 AWS 리전에서 AWS CloudTrail 로그를 켭니다. Amazon Athena를 사용하여 AWS 콘솔 로그인 이벤트에 대한 로그를 쿼리합니다.

B. 경보가 활성화될 때 보안 팀에 이메일을 보내도록 Amazon Simple Email Service (Amazon SES) 를 구성합니다.

C. Auto Scaling 그룹에 EC2 인스턴스를 배포합니다. 키 페어 없이 인스턴스를 배포하도록 시작 템플릿을 구성합니다. 시스템 액세스 로그를 캡처하도록 Amazon CloudWatch 로그를 구성합니다. 사용자가 EC2 인스턴스에 로그인할 때 감지할 로그를 기반으로 하는 Amazon CloudWatch 경보를 생성합니다.

D. 경보가 활성화될 때 보안 팀에 메시지를 보내도록 Amazon Simple Notification Service (Amazon SNS) 주제를 구성합니다.

E. 모든 AWS 리전에 대해 AWS CloudTrail로그를 켭니다. AWS 콘솔 로그인 이벤트가 감지될 때 알림을 제공하도록 Amazon CloudWatch 경보를 구성합니다.

F. EC2 인스턴스를 Auto Scaling 그룹에 배포합니다. 시작 후 키 페어를 삭제하도록 시작 템플릿을 구성합니다. 시스템 액세스 로그에 대한 Amazon CloudWatch 로그를 구성합니다. Amazon CloudWatch 대시보드를 생성하여 시간 경과에 따른 사용자 로그인을 표시합니다.

Answer: C, D, E

https://www.examtopics.com/discussions/amazon/view/59937-exam-aws-certified-solutions-architect-professional-topic-1/

Q106

한 회사에서 인기있는 비디오 게임의 새 릴리스를 개발하여 공개적으로 다운로드 할 수 있도록하려고합니다. 새 릴리스 패키지의 크기는 약 5GB입니다. 이 회사는 온프레미스 데이터 센터에서 호스팅되는 Linux 기반의 공개 FTP 사이트에서 기존 릴리스에 대한 다운로드를 제공합니다. 이 회사는 전 세계 사용자가 새 릴리스를 다운로드 할 것으로 예상합니다. 이 회사는 사용자의 위치에 관계없이 향상된 다운로드 성능과 낮은 전송 비용을 제공하는 솔루션을 원합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 마운트된 Amazon EBS 볼륨에 게임 파일을 저장합니다.EC2 인스턴스에서 FTP 서비스를 구성합니다. Auto Scaling 그룹 앞에 애플리케이션 로드 밸런서를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.

B. Auto Scaling 그룹 내의 Amazon EC2 인스턴스에 연결된 Amazon EFS 볼륨에 게임 파일을 저장합니다. 각 EC2 인스턴스에서 FTP 서비스를 구성합니다.Auto Scaling 그룹 앞에 애플리케이션 로드 밸런서를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.

C. 웹 사이트 호스팅용 Amazon Route 53과 Amazon S3 버킷을 구성합니다. 게임 파일을 S3 버킷에 업로드합니다.웹 사이트에 Amazon CloudFront를 사용합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.

D. 웹 사이트 호스팅용 Amazon Route 53과 Amazon S3 버킷을 구성합니다. 게임 파일을 S3 버킷에 업로드합니다.S3 버킷에 대해 요청자 지불을 설정합니다. 사용자가 패키지를 다운로드할 수 있도록 게임 다운로드 URL을 게시합니다.

Answer: C

Q107

동부 해안에 본사가 있는 북미 회사는 us-east-1 리전의 Amazon EC2에서 실행되는 새로운 웹 애플리케이션을 배포하고 있습니다. 애플리케이션은 사용자 요구를 충족하고 복원력을 유지하기 위해 동적으로 확장되어야 합니다. 또한 응용 프로그램에는 us-west-1 지역의 액티브-패시브 구성에서 재해 복구 기능이 있어야 합니다.

us-east-1 리전에서 VPC를 생성한 후 솔루션스 아키텍트는 어떤 단계를 수행해야 합니까?

A. 미국 서부-1 리전에 VPC를 생성합니다. 리전 간 VPC 피어링을 사용하여 두 VPC를 모두 연결합니다. 여러 가용 영역 (AZ) 에 걸쳐 있는 애플리케이션 로드 밸런서 (ALB) 를 useast-1 리전의 VPC에 배포합니다. 두 VPC에 걸쳐 있고 ALB에서 서비스를 제공하는 Auto Scaling 그룹의 일부로 각 리전의 여러 AZ에 EC2 인스턴스를 배포합니다.

B. 여러 가용 영역 (AZ) 에 걸쳐 있는 애플리케이션 로드 밸런서 (ALB) 를 us-east-1 리전의 VPC에 배포합니다. ALB가 제공하는 Auto Scaling 그룹의 일부로 여러 AZ에 EC2 인스턴스를 배포합니다. us-west-1 리전에 동일한 솔루션 배포 장애 조치 라우팅 정책 및 상태 확인이 활성화된 Amazon Route 53 레코드 세트를 생성하여 두 리전 모두에서 고가용성을 제공합니다.

C. 미국 서부-1 리전에 VPC를 생성합니다. 리전 간 VPC 피어링을 사용하여 두 VPC 모두 연결 두 VPC에 걸쳐 있는 애플리케이션 로드 밸런서 (ALB) 배포 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 애플리케이션 로드 밸런서 (ALB) 를 us-east-1 리전의 VPC에 배포합니다. ALB가 제공하는 Auto Scaling 그룹의 일부로 여러 AZ에 EC2 인스턴스를 배포합니다. 동일한 솔루션을 us-west-1 리전에 배포합니다.각 리전에서 해당 리전의 ALB를 가리키는 별도의 Amazon Route 53 레코드를 생성합니다. Route 53 상태 확인을 사용하여 두 리전 모두에서 고가용성을 제공합니다.

Answer: B

https://www.examtopics.com/discussions/amazon/view/35775-exam-aws-certified-solutions-architect-professional-topic-1/

Q108

한 회사는 많은 AWS 계정을 보유하고 있으며 AWS Organizations를 사용하여 모든 계정을 관리합니다. 솔루션 설계자는 회사에서 여러 계정에서 공통 네트워크를 공유하는 데 사용할 수 있는 솔루션을 구현해야 합니다. 이 회사의 인프라 팀에는 VPC가 있는 전용 인프라 계정이 있습니다. 인프라 팀은 이 계정을 사용하여 네트워크를 관리해야 합니다. 개별 계정은 자체 네트워크를 관리할 수 없습니다. 하지만 개별 계정은 서브넷 내에서 AWS 리소스를 생성할 수 있어야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자가 수행해야 하는 작업 조합은 무엇입니까?(두 개 선택)

A. 인프라 계정에 전송 게이트웨이를 생성합니다.

B. AWS 조직 관리 계정에서 리소스 공유를 활성화합니다.

C. AWS 조직의 조직 내 각 AWS 계정에 VPC를 생성합니다. 인프라 계정의 VPC와 동일한 CIDR 범위 및 서브넷을 공유하도록 VPC를 구성합니다. 인프라 계정의 VPC와 각 개별 계정의 VPC를 피어링합니다.

D. 인프라 계정의 AWS 리소스 액세스 관리자에서 리소스 공유를 생성합니다. 공유 네트워크를 사용할 특정 AWS 조직 OU를 선택합니다. 리소스 공유와 연결할 각 서브넷을 선택합니다.

E. 인프라 계정의 AWS 리소스 액세스 관리자에서 리소스 공유를 생성합니다. 공유 네트워크를 사용할 특정 AWS 조직 OU를 선택합니다. 리소스 공유와 연결할 각 접두사 목록을 선택합니다.

Answer: B, D

Q109

한 회사에서 Amazon EFS에 저장된 많은 수의 공유 파일을 생성하는 긴밀하게 결합된 워크로드를 위해 AWS에 HPC (고성능 컴퓨팅) 클러스터를 구축했습니다. 클러스터의 Amazon EC2 인스턴스 수가 100개일 때 클러스터의 성능이 양호했습니다. 하지만 클러스터 크기를 1,000개의 EC2 인스턴스로 늘렸을 때 전반적인 성능은 예상보다 훨씬 낮았습니다.

솔루션 설계자가 HPC 클러스터에서 최대 성능을 달성하기 위해 선택해야 하는 설계 선택 모음은 무엇입니까?(세 개 선택)

A. HPC 클러스터가 단일 가용 영역 내에서 시작되었는지 확인합니다.

B. EC2 인스턴스를 시작하고 네 배수의 탄력적 네트워크 인터페이스(ENI)를 연결합니다.

C. Elastic Fabric Adapter (EFA) 가 활성화된 EC2 인스턴스 유형을 선택합니다.

D. 클러스터가 여러 가용 영역에서 시작되었는지 확인합니다.

E. Amazon EFS를 교체하면 RAID 어레이에서 여러 Amazon EBS 볼륨을 획득합니다.

F. Amazon EFS를 Lustre용 Amazon FSx로 교체합니다.

Answer: A, C, F

설명

긴밀하게 연결된 워크로드가 있는 HPC 클러스터를 사용하려면 고성능 및 짧은 대기 시간의 노드 간 통신이 필요합니다. EFA(Elastic Fabric Adapter)는 고객이 AWS에서 대규모 노드 간 통신이 필요한 애플리케이션을 실행할 수 있게 해주는 Amazon EC2 인스턴스용 네트워크 인터페이스입니다.

지원되는 EC2 인스턴스와 함께 EFA를 사용하는 것 외에도 AWS는 인스턴스를 단일 가용 영역으로 시작하여 노드 간 지연 시간을 줄이는 것이 좋습니다.

설계에서 대기 시간의 또 다른 원인은 EFS 파일 시스템일 수 있습니다. Amazon FSx for Lustre는 컴퓨팅 워크로드를 위한 비용 효율적이고 확장 가능한 고성능 스토리지를 제공하는 완전 관리형 서비스입니다. FSx for Lustre는 밀리초 미만의 대기 시간, 초당 최대 수백 기가바이트의 처리량, 수백만 IOPS를 제공합니다.

EFS를 Lustre로 교체하면 스토리지 작업의 대기 시간이 줄어듭니다.

잘못됨: B. HPC 워크로드에서는 대기 시간이 가장 큰 문제이며 대기 시간을 줄이기 위해 ENI(탄력적 네트워크 인터페이스)보다 EFS 어댑터를 사용하는 것이 좋습니다.

잘못됨: D. 클러스터는 성능을 위해 단일 AZ에서 시작되어야 합니다.

참조:

https://aws.amazon.com/fsx/lustre/

https://aws.amazon.com/hpc/efa/

Q110

한 미디어 회사에서 Amazon DynamoDB를 사용하여 스트리밍할 수 있는 영화 카탈로그에 대한 메타데이터를 저장합니다. 각 미디어 항목에는 미디어에 대한 설명, 검색 태그 목록 및 유사한 데이터를 마무리하는 사용자 대면 콘텐츠가 포함됩니다. 또한 미디어 항목에는 동영상 파일과 관련된 Amazon S3 키 이름 목록이 포함됩니다. 이 회사는 버전 관리가 활성화된 단일 S3 버킷에 이러한 동영상 파일을 저장합니다. 이 회사는 Amazon CloudFront를 사용하여 이러한 영화 파일을 제공합니다. 이 회사는 100.000개의 미디어 항목을 보유하고 있으며, 각 미디어 항목은 동일한 미디어의 서로 다른 인코딩을 나타내는 다양한 S3 객체를 가질 수 있습니다. 동일한 미디어 항목에 속하는 S3 객체는 동일한 키 접두사 (임의의 고유 ID) 로 그룹화됩니다. 미디어 제공업체와의 계약이 만료되기 때문에 회사는 2.000개의 미디어 항목을 제거해야 합니다. 회사는 이러한 미디어 항목과 관련된 Amazon S3의 모든 DynamoDB 키와 동영상 파일을 36시간 이내에 완전히 삭제해야 합니다. 회사는 콘텐츠를 복구할 수 없도록 해야 합니다.

이러한 요구 사항을 충족하는 작업 조합은 무엇입니까?(두 개 선택)

A. TTL 필드를 사용하여 DynamoDB 테이블을 구성합니다. AWS Lambda 함수를 생성하고 호출하여 조건부 업데이트를 수행합니다. 영향을 받는 모든 미디어 항목에 대한 계약 만료 시간으로 TTL 필드를 설정합니다.

B. 계약의 만료 날짜를 기준으로 S3 수명 주기 객체 만료 규칙을 구성합니다.

C. 영향을 받는 모든 DynamoDB 레코드에 대해 조건부 삭제를 수행하는 스크립트를 작성합니다.

D. S3 버킷의 버전 관리를 일시적으로 중단합니다. 영향을 받는 객체를 삭제하는 AWS Lambda 함수를 생성하고 호출합니다. 작업이 완료되면 버전 관리를 다시 활성화합니다.

E. Amazon S3에서 객체를 삭제하는 스크립트 작성 각 요청에서 NoncurrentDays 속성이 0으로 설정된 NoncurrentVersionExpiration 속성을 지정합니다.

Answer: C, E

Q111

회사는 데이터베이스를 실행하는 모든 Amazon EC2 인스턴스가 공유 VPC의 동일한 서브넷 내에 있어야 한다는 정책을 가지고 있습니다. 관리자는 보안 규정 준수 요구 사항을 준수해야 하며 공유 계정에 직접 로그인할 수 없습니다. 모든 회사 계정은 AWS Organizations에서 동일한 조직의 구성원입니다. 회사가 성장함에 따라 계정 수가 급격히 증가 할 것입니다. 솔루션스 아키텍트는 AWS 리소스 액세스 관리자를 사용하여 공유 계정에 리소스 공유를 생성합니다.

이러한 요구 사항을 충족하는 가장 운영 효율적인 구성은 무엇입니까?

A. 리소스 공유에 VPC를 추가합니다. 계정 ID를 보안 주체로 추가합니다.

B. VPC 내의 모든 서브넷을 리소스 공유에 추가합니다. 계정 ID를 보안 주체로 추가합니다.

C. VPC 내의 모든 서브넷을 리소스 공유에 추가합니다. 조직을 주도자로 추가합니다.

D. 리소스 공유에 VPC를 추가합니다. 조직을 주도자로 추가합니다.

Answer: C

Q112

솔루션 설계자가 새로운 클라우드 배포를 위한 네트워크를 설계하고 있습니다. 라우팅 테이블을 수정하고 변경하려면 각 계정에 자율성이 필요합니다. 중앙 집중식으로 제어되는 송신 인터넷 연결도 필요합니다. 클라우드 공간은 수천 개의 AWS 계정으로 증가할 것으로 예상됩니다.

이러한 요구 사항을 충족하는 아키텍처는 무엇입니까?

A. 각 계정의 독립 실행형 VPC에 대한 VPN 연결이 있는 중앙 집중식 전송 VPC입니다. 아웃바운드 인터넷 트래픽은 방화벽 어플라이언스에 의해 제어됩니다.

B. 각 계정의 서브넷이 있는 중앙 집중식 공유 VPC.아웃바운드 인터넷 트래픽은 프록시 서버 집합을 통해 제어됩니다.

C. 인터넷에 대한 경로가 있는 방화벽 집합을 포함하기 위해 중앙 자산을 호스팅하는 공유 서비스 VPC입니다. 각 스포크 VPC는 중앙 VPC를 피어링합니다.

D. 각 VPC가 연결될 공유 전송 게이트웨이입니다. 아웃바운드 인터넷 액세스는 VPN에 연결된 방화벽을 통해 라우팅됩니다.

Answer: D

Q113

회사는 중앙 위치에서 여러 부서의 여러 AWS 계정을 생성하고 관리해야 합니다. 보안 팀에는 자체 AWS 계정에서 모든 계정에 대한 읽기 전용 액세스 권한이 필요합니다. 이 회사는 AWS Organizations를 사용하고 있으며 보안 팀의 계정을 생성했습니다.

솔루션 설계자는 이러한 요구 사항을 어떻게 충족해야 합니까?

A. 조직계정 액세스 역할 IAM 역할을 사용하여 각 구성원 계정에서 읽기 전용 액세스 권한이 있는 새 IAM 정책을 생성합니다. 각 멤버 계정의 IAM 정책과 보안 계정 간에 신뢰 관계를 설정합니다. 보안 팀에 IAM 정책을 사용하여 액세스 권한을 얻도록 요청합니다.

B. 조직계정 액세스 역할 IAM 역할을 사용하여 각 구성원 계정에서 읽기 전용 액세스 권한이 있는 새 IAM 역할을 생성합니다. 각 멤버 계정의 IAM 역할과 보안 계정 간에 신뢰 관계를 설정합니다.보안 팀에 IAM 역할을 사용하여 액세스 권한을 얻도록 요청합니다.

C. 보안 팀에 AWS 보안 토큰 서비스 (AWS STS) 를 사용하여 보안 계정에서 마스터 계정의 조직 계정 액세스 역할 IAM 역할에 대한 AssumeRole API를 호출하도록 요청합니다. 생성된 임시 자격 증명을 사용하여 액세스 권한을 얻습니다.

D. 보안 팀에 AWS 보안 토큰 서비스 (AWS STS) 를 사용하여 보안 계정에서 멤버 계정의 조직 계정 액세스 역할 IAM 역할에 대한 AssumeRole API를 호출하도록 요청합니다. 생성된 임시 자격 증명을 사용하여 액세스 권한을 얻습니다.

Answer: D

Q114

솔루션스 아키텍트는 IT 비용에 매우 민감하고 매월 예측 가능한 AWS 지출로 이어질 수 있는 제어 기능을 구현하고자 하는 회사와 협력하고 있습니다.

회사에서 월별 AWS 사용량을 제어 및 모니터링하여 목표 금액에 최대한 근접한 비용을 달성하는 데 도움이 될 수 있는 단계 조합은 무엇입니까?(세 가지를 선택)

A. Amazon EC2 인스턴스를 시작할 때 사용자가 비용 할당을 위해 '워크로드' 태그를 지정해야 하는 IAM 정책을 구현합니다.

B. AWS Support에 연락하여 사용자가 특정 개수보다 많은 인스턴스 유형을 시작할 수 없도록 계정에 제한을 적용하도록 요청합니다.

C. 계정의 예상 Amazon EC2 사용량의 100% 를 충당하는 모든 선결제 예약 인스턴스를 구매합니다.

D. 시작할 수 있는 인스턴스 수를 제한하는 조건을 사용자의 IAM 정책에 배치합니다.

E. AWS 결제 및 비용 관리 콘솔에서 '워크로드'를 비용 할당 태그로 정의합니다.

F. 지정된 워크로드가 정의된 비용을 초과할 것으로 예상되는 경우 이를 알리고 알리도록 AWS Budgets를 설정합니다.

Answer: A, E, F

Q115

한 회사에서 AWS Organizations를 사용하여 여러 계정을 관리하고 있습니다. 규제 요구 사항으로 인해 회사는 특정 멤버 계정을 리소스 배포가 허용되는 특정 AWS 리전으로 제한하려고 합니다. 계정의 리소스는 태그를 지정하고 그룹 표준에 따라 적용하며 최소한의 구성으로 중앙에서 관리해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 특정 멤버 계정에 AWS Config 규칙을 생성하여 리전을 제한하고 태그 정책을 적용합니다.

B. AWS 결제 및 비용 관리 콘솔의 마스터 계정에서 특정 멤버 계정의 리전을 비활성화하고 루트에 태그 정책을 적용합니다.

C. 특정 멤버 계정을 루트와 연결합니다. 조건을 사용하여 태그 정책 및 SCP를 적용하여 지역을 제한합니다.

D. 특정 구성원 계정을 새 OU와 연결합니다. 조건을 사용하여 태그 정책 및 SCP를 적용하여 지역을 제한합니다.

Answer: D

Q116

한 회사가 AWS에 클라우드 인프라를 보유하고 있으므로 솔루션 설계자는 인프라를 코드로 정의해야 합니다. 인프라는 현재 하나의 AWS 리전에 배포되어 있습니다. 이 회사의 비즈니스 확장 계획에는 여러 AWS 계정의 여러 리전에 배포하는 것이 포함됩니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. AWS CloudFormation템플릿을 사용하여 IAM 정책을 추가하여 다양한 계정을 제어합니다. 템플릿을 여러 리전에 배포합니다.

B. AWS Organizations을 사용합니다. 관리 계정에서 AWS CloudFormation 템플릿을 배포합니다. AWS Control Tower를 사용하여 계정 간 배포를 관리합니다.

C. AWS 조직 및 AWS CloudFormation스택 세트를 사용합니다. 필요한 IAM 권한이 있는 계정에서 CloudFormation템플릿을 배포합니다.

D. 중첩 스택을 AWS CloudFormation템플릿과 함께중첩된 스택을 사용하여 리전을 변경합니다.

Answer: B

Q117

대기업에서 널리 사용되는 웹 애플리케이션을 운영하고 있습니다. 애플리케이션은 프라이빗 서브넷의 Auto Scaling 그룹에 있는 여러 Amazon EC2 Linux 인스턴스에서 실행됩니다. 애플리케이션 로드 밸런서가 프라이빗 서브넷의 Auto Scaling 그룹에 있는 인스턴스를 대상으로 합니다. AWS 시스템 관리자 세션 관리자가 구성되어 있으며 AWS 시스템 관리자 에이전트가 모든 EC2 인스턴스에서 실행 중입니다. 이 회사는 최근 애플리케이션의 새 버전을 출시했습니다. 일부 EC2 인스턴스는 이제 비정상으로 표시되어 종료되고 있으며, 그 결과 애플리케이션이 감소된 용량으로 실행되고 있습니다. 솔루션 설계자는 수집된 Amazon CloudWatch 로그를 분석하여 근본 원인을 파악하려고 합니다. 하지만 로그가 결정적이지 않습니다.

솔루션 설계자가 문제를 해결하기 위해 EC2 인스턴스에 액세스하려면 어떻게 해야 합니까?

A. Auto Scaling 그룹의 상태 점검 조정 프로세스를 일시 중단합니다. 세션 관리자를 사용하여 비정상으로 표시된 인스턴스에 로그인합니다.

B. EC2 인스턴스 종료 보호를 활성화합니다. 세션 관리자를 사용하여 비정상으로 표시된 인스턴스에 로그인합니다.

C. Auto Scaling 그룹에서 종료 정책을 가장 오래된 인스턴스로 설정합니다. 세션 관리자를 사용하여 비정상으로 표시된 인스턴스에 로그인합니다.

D. Auto Scaling 그룹의 종료 프로세스를 일시 중지합니다. 세션 관리자를 사용하여 비정상으로 표시된 인스턴스에 로그인합니다.

Answer: D

Q118

솔루션 설계자는 가용성, 데이터 내구성 및 확장성을 개선하기 위해 레거시 Java 애플리케이션을 재설계할 책임이 있습니다. 현재 애플리케이션은 고용량 메모리 Amazon EC2 인스턴스 하나에서 실행됩니다. 업스트림 클라이언트의 HTTP 요청을 수락하고 이를 인 메모리 대기열에 추가하고 200 상태로 응답합니다. 별도의 애플리케이션 스레드는 대기열에서 항목을 읽고 처리한 다음 결과를 Amazon RDS MySQL 인스턴스에 유지합니다. 각 항목의 처리 시간은 평균 90초가 걸리며, 대부분은 외부 서비스 호출을 기다리는 데 소요되지만 응용 프로그램은 여러 항목을 병렬로 처리하도록 작성됩니다. 이 서비스에 대한 트래픽은 예측할 수 없습니다. 로드가 많은 기간에는 애플리케이션이 백로그를 처리하는 동안 항목이 한 시간 이상 내부 대기열에 있을 수 있습니다. 또한 단일 애플리케이션 노드에 장애가 발생할 경우 현재 시스템의 가용성 및 데이터 손실 문제가 발생합니다. 이 서비스에 액세스하는 클라이언트는 수정할 수 없습니다. 시간이 초과되어 요청을 재시도하기 전에 10초 이내에 전송하는 각 HTTP 요청에 대한 응답을 수신할 것으로 예상합니다.

처리 대기 시간을 줄이고 비용을 최소화하면서 시스템의 가용성과 내구성을 개선하는 접근 방식은 무엇입니까?

A. Lambda 프록시 통합을 사용하여 요청을 AWS Lambda 함수로 전달하는 Amazon API Gateway REST API를 생성합니다. 핵심 처리 코드를 Lambda 함수로 마이그레이션하고 프록시 이벤트를 내부 애플리케이션 데이터 모델로 변환하고 처리 모듈을 호출하는 핸들러 메서드를 제공하는 래퍼 클래스를 작성합니다.

B. 서비스 프록시를 사용하여 Amazon SQS 대기열에 항목을 넣는 Amazon API Gateway REST API를 생성합니다. 기존 애플리케이션에서 코어 처리 코드를 추출하고 이를 업데이트하여 인 메모리 대기열 대신 Amazon SQS에서 항목을 가져옵니다. Amazon SQS 대기열의 대략적인 메시지 수에 따라 동적으로 확장되는 Auto Scaling 그룹 내의 소규모 EC2 인스턴스에 새 처리 애플리케이션을 배포합니다.

C. Amazon RDS 대신 Amazon DynamoDB를 사용하도록 애플리케이션을 수정합니다. DynamoDB 테이블에 대한 오토 스케일링을 구성합니다. CPU 사용률을 기반으로 하는 조정 정책을 사용하여 Auto Scaling 그룹 내에 애플리케이션을 배포합니다. 메모리 매핑된 파일이 있는 인 메모리 대기열을 인스턴스 스토어 볼륨으로 되돌리고 해당 파일을 Amazon S3에 주기적으로 씁니다.

D. 인 메모리 대기열 대신 Redis 작업 대기열을 사용하도록 애플리케이션을 업데이트합니다. 애플리케이션에 대한 Docker 컨테이너 이미지를 빌드합니다. 애플리케이션 컨테이너와 Redis를 호스팅할 별도의 컨테이너를 포함하는 Amazon ECS 작업 정의를 생성합니다. AWS Fargate를 사용하여 새 작업 정의를 ECS 서비스로 배포하고 자동 확장을 활성화합니다.

Answer: B

Q119

한 회사가 3계층 웹 아키텍처를 사용하여 AWS에서 전자 상거래 웹 사이트를 구축했습니다. 이 애플리케이션은 자바 기반이며 Amazon CloudFront 배포, 오토 스케일링 그룹의 Amazon EC2 인스턴스로 구성된 Apache 웹 서버 레이어 및 백엔드 Amazon Aurora MySQL 데이터베이스로 구성됩니다. 지난달 프로모션 판매 이벤트 기간 동안 사용자는 장바구니에 품목을 추가하는 동안 오류와 시간 초과를 보고했습니다. 운영 팀은 웹 서버에서 생성된 로그를 복구하고 Aurora DB 클러스터 성능 지표를 검토했습니다. 로그를 수집하기 전에 일부 웹 서버가 종료되었으며 Aurora 메트릭이 쿼리 성능 분석에 충분하지 않았습니다.

트래픽이 폭주하는 상황에서 애플리케이션 성능 가시성을 개선하기 위해 솔루션 설계자가 수행해야 하는 단계는 무엇입니까?(세 개 선택)

A. 느린 쿼리 및 오류 로그를 Amazon CloudWatch 로그에 게시하도록 Aurora MySQL DB 클러스터를 구성합니다.

B. AWS X-Ray SDK를 구현하여 EC2 인스턴스에서 수신되는 HTTP 요청을 추적하고 자바용 X-Ray SDK를 사용하여 SQL 쿼리의 추적을 구현합니다.

C. 느린 쿼리 및 오류 로그를 Amazon Kinesis로 스트리밍하도록 Aurora MySQL DB 클러스터를 구성합니다.

D. EC2 인스턴스에 Amazon CloudWatch 로그 에이전트를 설치하고 구성하여 Apache 로그를 CloudWatch 로그로 전송합니다.

E. AWS CloudTrail을 활성화하고 구성하여 Amazon EC2 및 Aurora에서 애플리케이션 활동을 수집하고 분석합니다.

F. Aurora MySQL DB 클러스터 성능 벤치마킹을 활성화하고 스트림을 AWS XRay에 게시합니다.

Answer: A, B, D

설명

Amazon Aurora의 경우 MySQL 오류 로그, 느린 쿼리 로그 및 일반 로그를 모니터링할 수 있습니다. MySQL 오류 로그는 기본적으로 생성됩니다. DB 파라미터 그룹에서 파라미터를 설정하여 느린 쿼리 및 일반 로그를 생성할 수 있습니다. 이 데이터는 Aurora 데이터베이스 계층의 모든 문제를 해결하는 데 도움이 됩니다.

AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고 해당 데이터를 보고, 필터링하고, 통찰력을 확보하여 문제와 최적화 기회를 식별하는 데 사용할 수 있는 도구를 제공하는 서비스입니다. AWS SDK를 사용하여 X-Ray API를 사용하는 프로그램을 개발할 수 있습니다. 이 경우 애플리케이션은 자바에서 실행되므로 자바용 X-Ray SDK를 사용해야 합니다.

일부 인스턴스는 로그를 수집하기 전에 ASG에 의해 종료되었습니다. 이 문제가 다시 발생하지 않도록 CloudWatch Logs 에이전트를 인스턴스에 설치할 수 있습니다. 에이전트는 로그를 정기적으로 CloudWatch 로그로 스트리밍하므로(구성 가능) 다음에 로그가 손실되지 않습니다.

Q120

회사에는 보고서를 생성하여 Amazon S3 버킷에 저장하는 애플리케이션이 있습니다. 사용자가 보고서에 액세스하면 애플리케이션은 사용자가 보고서를 다운로드할 수 있도록 서명된 URL을 생성합니다. 이 회사의 보안 팀은 파일이 공개되어 있으며 누구나 인증없이 파일을 다운로드 할 수 있음을 발견했습니다. 회사는 문제가 해결될 때까지 새 보고서 생성을 중단했습니다.

애플리케이션의 정상적인 워크플로에 영향을 주지 않으면서 보안 문제를 즉시 해결할 수 있는 조치는 무엇입니까?

A. 인증되지 않은 사용자에 대해 모든 정책을 적용하는 AWS Lambda 함수를 생성합니다. 예약된 이벤트를 생성하여 Lambda 함수를 호출합니다.

B. AWS Trusted Advisor 버킷 권한을 검토하고 권장 작업을 구현합니다.

C. 버킷의 모든 객체에 프라이빗 ACL을 배치하는 스크립트를 실행합니다.

D. Amazon S3의 퍼블릭 액세스 차단 기능을 사용하여 버킷에서 IgnorePublicAcis 옵션을 TRUE로 설정합니다.

Answer: D

Q121

한 회사가 us-east-1 리전의 AWS에서 웹 애플리케이션을 호스팅합니다. 애플리케이션 서버는 애플리케이션 로드 밸런서 뒤에 있는 3개의 가용 영역에 분산되어 있습니다. 데이터베이스는 Amazon EC2 인스턴스의 MySQL 데이터베이스에서 호스팅됩니다. 솔루션 설계자는 RTO가 5분 미만이고 RPO가 1분 미만인 AWS 서비스를 사용하여 리전 간 데이터 복구 솔루션을 설계해야 합니다. 이 솔루션스 아키텍트는 us-west-2에 애플리케이션 서버를 배포하고 있으며 Amazon Route 53 상태 확인 및 DNS 장애 조치를 us-west-2로 구성했습니다.

솔루션 설계자는 어떤 추가 단계를 수행해야 합니까?

A. us-west-2에 리전 간 읽기 전용 복제본이 있는 MySQL용 Amazon RDS 인스턴스로 데이터베이스를 마이그레이션합니다.

B. 기본 데이터베이스가 us-east-1에 있고 보조 데이터베이스가 us-west-2에 있는 Amazon Aurora 글로벌 데이터베이스로 데이터베이스를 마이그레이션합니다.

C. 다중 AZ 배포를 사용하여 데이터베이스를 MySQL용 Amazon RDS 인스턴스로 마이그레이션합니다.

D. 미국 서부-2의 Amazon EC2 인스턴스에 MySQL 대기 데이터베이스를 생성합니다.

Answer: B

Q122

AWS에서 애플리케이션을 실행하는 회사는 최근 새로운 SaaS (software-as-a-service) 데이터 공급업체에 가입했습니다. 공급업체는 공급업체가 AWS 환경에서 호스팅하는 REST API를 통해 데이터를 제공합니다. 공급업체는 API에 연결하기 위한 여러 옵션을 제공하며 가장 좋은 연결 방법을 찾기 위해 회사와 협력하고 있습니다. 회사의 AWS 계정은 AWS 환경에서 아웃바운드 인터넷 액세스를 허용하지 않습니다. 공급업체의 서비스는 회사 애플리케이션과 동일한 AWS 리전의 AWS에서 실행됩니다. 솔루션 설계자는 회사의 VPC에서 API의 가용성을 높이기 위해 공급업체의 API에 대한 연결을 구현해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 데이터 서비스에 대한 공급업체의 공개 API 주소에 연결합니다.

B. 공급업체의 VPC와 회사의 VPC 간의 VPC 피어링 연결을 통해 공급업체에 연결합니다.

C. AWS PrivateLink를 사용하는 VPC 엔드포인트 서비스를 통해 벤더에 연결합니다.

D. 공급업체가 제공하는 공용 배스천 호스트에 연결하여 API 트래픽을 터널링합니다.

Answer: C

Q123

한 회사가 AWS에서 애플리케이션을 실행합니다. AWS Lambda 함수는 자격 증명을 사용하여 MySQL DB 인스턴스용 Amazon RDS에 인증합니다. 보안 위험 평가에서 이러한 자격 증명이 자주 교체되지 않는 것으로 확인되었습니다. 또한 DB 인스턴스에 대해 저장 시 암호화가 활성화되지 않습니다. 보안 팀에서는 이 두 가지 문제를 모두 해결하도록 요구합니다.

솔루션 설계자는 이러한 보안 위험을 해결하기 위해 어떤 전략을 권장해야 합니까?

A. AWS Secrets Manager에서 데이터베이스 자격 증명을 저장 및 검색하고 자격 증명 교체를 활성화하도록 Lambda 함수를 구성합니다. DB 인스턴스의 스냅샷을 생성하고 해당 스냅샷의 사본을 암호화합니다. DB 인스턴스를 암호화된 스냅샷을 기반으로 하는 새 DB 인스턴스로 교체합니다.

B. DB 인스턴스에서 IAM DB 인증을 활성화합니다. Lambda 실행 역할에 DB 인스턴스에 대한 액세스 권한을 부여합니다. DB 인스턴스를 수정하고 암호화를 활성화합니다.

C. DB 인스턴스에서 IAM DB 인증을 활성화합니다. Lambda 실행 역할에 DB 인스턴스에 대한 액세스 권한을 부여합니다.DB 인스턴스의 암호화된 읽기 전용 복제본을 생성합니다. 암호화된 읽기 전용 복제본을 새 기본 노드로 승격합니다.

D. 데이터베이스 자격 증명을 암호화된 AWS Systems Manager 파라미터 스토어 파라미터로 저장하고 검색하도록 Lambda 함수를 구성합니다. 자격 증명을 자동으로 교체하려면 다른 Lambda 함수를 생성합니다. DB 인스턴스의 암호화된 읽기 전용 복제본을 생성합니다. 암호화된 읽기 전용 복제본을 새 기본 노드로 승격합니다.

Answer: A

AWS Secrets Manager를 사용하여 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 암호를 교체, 관리 및 검색할 수 있습니다. 보안 및 규정 준수 요구 사항을 충족하는 데 도움이 될 수 있는 보안 비밀을 자동으로 교체하도록 Secrets Manager를 구성할 수 있습니다. Secrets Manager는 Amazon RDS에서 MySQL, PostgreSQL 및 Amazon Aurora에 대한 내장 통합을 제공하며 이러한 데이터베이스에 대한 자격 증명을 기본적으로 교체할 수 있습니다.

Q124

한 회사의 솔루션 설계자가 AWS에서 실행되는 애플리케이션을 위한 재해 복구 (DR) 솔루션을 설계하고 있습니다. 이 애플리케이션은 PostgreSQL 11.7을 데이터베이스로 사용합니다. 회사의 PRO(복구 지점 목표)는 30 초입니다. 솔루션 설계자는 us-east-1 리전의 기본 데이터베이스와 us-west-2 리전의 데이터베이스를 사용하여 DR 솔루션을 설계해야 합니다.

애플리케이션 변경을 최소화하면서 이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. us-east-1의 PostgreSQL용 Amazon RDS로 데이터베이스를 마이그레이션합니다. us-west-2에서 읽기 전용 복제본을 설정하여 읽기 전용 복제본을 설정합니다. RDS 데이터베이스의 관리형 PRO를 30초로 설정합니다.

B. us-east-1의 PostgreSQL을 위해 데이터베이스를 Amazon으로 마이그레이션합니다. us-west-2의 가용 영역에 예비 복제본을 설정하고 RDS 데이터베이스의 관리형 PRO를 30초로 설정합니다.

C. 기본 리전은 us-east-1이고 보조 리전은 us-west-2인 Amazon Aurora PostgreSQL 글로벌 데이터베이스로 데이터베이스를 마이그레이션합니다. Aurora 데이터베이스의 관리형 PRO를 30초로 설정합니다.

D. 데이터베이스를 us-east-1의 Amazon DynamoDB로 마이그레이션합니다. us-west-2에서 생성된 복제본 테이블로 전역 테이블을 설정합니다.

Answer: C

https://aws.amazon.com/ko/about-aws/whats-new/2020/06/amazon-aurora-postgresql-global-database-supports-managed-recovery-point-objective-RPO/?nc1=h\_ls

Q125

AWS에서 호스팅하는 전자 상거래 웹 사이트는 범용 SSD 스토리지와 함께 MySQL용 Amazon RDS 데이터베이스 인스턴스를 사용합니다. 수요에 따라 개발자는 적절한 인스턴스 유형을 선택하고 적절한 여유 공간으로 100GB의 스토리지를 설정했습니다.

몇 주 동안 웹 사이트는 마케팅 노력이 시작될 때까지 정상적으로 운영되었습니다. 사용자는 프로모션 둘째 날에 긴 대기 시간과 시간 초과에 대해 불평했습니다. Amazon CloudWatch 측정에 따르면 데이터베이스 인스턴스에 대한 읽기 및 쓰기 모두 응답 시간이 길었습니다. CloudWatch 데이터에 따르면 CPU와 RAM의 40% ~ 50% 가 사용되고 있지만 충분한 여유 스토리지 공간은 여전히 사용할 수 있습니다. 응용 프로그램 서버 로그에 데이터베이스 연결 문제가 있다는 징후는 없습니다.

마케팅 캠페인 실패의 근본 원인은 무엇일까요?

A. 설정 단계에서 디스크 스토리지 부족 프로비저닝으로 인해 I/O 크레딧 밸런스가 소진되었습니다.

B. 이로 인해 테이블의 데이터가 자주 변경되어 쿼리를 최적화하기 위해 인덱스를 다시 작성해야 했습니다.

C. 데이터베이스 인스턴스에 허용되는 최대 연결 수를 모두 소모했습니다.

D. MySQL DB 인스턴스용 RDS에 사용할 수 있는 네트워크 대역폭이 모두 소모되었습니다

Answer: A

설명

범용 SSD 스토리지의 기준 I/O 성능은 GiB당 3IOPS이며 최소 100IOPS입니다. 이 관계는 볼륨이 클수록 성능이 더 좋다는 것을 의미합니다. 이 경우 볼륨은 100GB에 불과하므로 300IOPS 성능만 갖습니다.

범용 SSD 스토리지를 사용할 때 DB 인스턴스는 540만 I/O 크레딧의 초기 I/O 크레딧 잔고를 받습니다. 이 초기 크레딧 잔고는 30분 동안 3,000IOPS의 버스트 성능을 유지하기에 충분합니다. 이 균형은 부팅 볼륨에 대한 빠른 초기 부팅 주기를 제공하고 다른 응용 프로그램에 대한 우수한 부트스트랩 경험을 제공하도록 설계되었습니다.

볼륨은 볼륨 크기의 각 GiB에 대해 3IOPS의 기준 성능 속도로 I/O 크레딧을 얻습니다. 예를 들어 100GiB SSD 볼륨의 기준 성능은 300IOPS입니다.

이 시나리오에서 증가된 로드로 인해 마케팅 기간이 끝나기 전에 I/O 크레딧 잔액이 소진되었음을 알 수 있습니다. 즉, I/O 크레딧이 충분할 때까지 성능이 제한됩니다.

참조:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\_Storage.html

Q126

한 회사에서 마케팅 팀이 고객 레코드에 대한 SQL 쿼리를 수행하여 시장 세그먼트를 식별할 수 있도록 허용하려고 합니다. 데이터는 수백 개의 파일에 분산되어 있습니다.기록은 전송 중 및 저장 중에 암호화되어야 합니다. 팀 관리자는 사용자 및 그룹을 관리할 수 있어야 하지만 SQL 쿼리에 필요하지 않은 서비스 또는 리소스에 대한 액세스 권한은 팀 구성원이 없어야 합니다. 또한 관리자는 쿼리를 감사하고 쿼리가 보안 팀에서 정의한 규칙을 위반할 경우 알림을 받아야 합니다. AWS 조직은 관리자가 있는 새 계정 및 AWS IAM 사용자를 생성하는 데 사용되었습니다.

팀 관리자의 권한입니다.

이러한 요구 사항을 충족하는 설계는 무엇입니까?

A. IAM, Amazon RDS 및 AWS CloudTrail에 대한 액세스를 허용하는 SCP (서비스 제어 정책) 를 적용합니다. Amazon RDS MySQL에서 고객 레코드를 로드하고 AWS CLI를 사용하여 쿼리를 실행하도록 사용자를 교육합니다. RDS 데이터베이스 인스턴스에서 쿼리 로그를 Amazon CloudWatch 로그로 스트리밍합니다. AWS Lambda 함수와 함께 구독 필터를 사용하여 개인 데이터에 대한 쿼리를 감사하고 경보를 울립니다.

B. IAM, Amazon Athena, Amazon S3 및 AWS CloudTrail을 제외한 모든 서비스에 대한 액세스를 거부하는 SCP (서비스 제어 정책) 를 적용합니다. Amazon S3에 고객 레코드 파일을 저장하고 Athena를 통해 CLI를 사용하여 쿼리를 실행하도록 사용자를 교육합니다. CloudTrail 이벤트를 분석하여 개인 데이터에 대한 쿼리를 감사하고 경보를 보냅니다.

C. IAM, Amazon DynamoDB 및 AWS CloudTrail을 제외한 모든 서비스에 대한 액세스를 거부하는 SCP (서비스 제어 정책) 를 적용합니다. DynamoDB에 고객 레코드를 저장하고 AWS CLI를 사용하여 쿼리를 실행하도록 사용자를 교육합니다. DynamoDB 스트림이 실행된 쿼리를 추적하고 실시간 모니터링 및 알림을 위해 AWS Lambda 함수를 사용하도록 설정합니다.

D. IAM, Amazon Athena, Amazon S3 및 AWS CloudTrail에 대한 액세스를 허용하는 SCP (서비스 제어 정책) 를 적용합니다. 고객 레코드를 Amazon S3에 파일로 저장하고 사용자에게 Amazon S3 선택 기능을 활용하고 AWS CLI를 사용하여 쿼리를 실행하도록 교육합니다. S3 객체 수준 로깅을 활성화하고 CloudTrail 이벤트를 분석하여 개인 데이터에 대한 쿼리를 감사하고 경보를 보냅니다.

Answer: B

Q127

한 회사에서 현재 소스 제어를 위해 AWS CodeCommit을 사용하고 지속적인 통합을 위해 AWS CodePipeline을 사용하고 있습니다. 파이프라인에는 아티팩트를 빌드하기 위한 빌드 단계가 있으며, 이 빌드 단계는 Amazon S3 버킷에 스테이징됩니다.

이 회사는 기존 프로세스에서 다양한 개선 기회를 확인했으며 솔루션 설계자에게 다음과 같은 요구 사항이 부여되었습니다.

\* 기능 개발을 지원하는 새 파이프라인을 생성합니다.

\* 프로덕션 애플리케이션에 영향을 주지 않고 기능 개발을 지원합니다.

\* 단위 테스트와 함께 지속적인 테스트를 통합합니다.

\* 개발 및 프로덕션 아티팩트를 분리합니다.

\* 테스트 코드를 프로덕션 코드로 병합하는 기능 지원

솔루션 설계자는 이러한 요구 사항을 어떻게 충족해야 합니까?

A. CodeCommit 기능 브랜치에서 별도의 파이프라인을 트리거합니다. 단위 테스트를 실행하는 데 AWS 코드빌드를 사용합니다. CodeBuild를 사용하여 별도의 테스트 계정에서 S3 버킷 내에 아티팩트를 스테이징합니다.

B. CodeCommit 기능 브랜치에서 별도의 파이프라인을 트리거합니다. 단위 테스트를 실행하는 데 AWS Lambda를 사용합니다. AWS CodeDeploy를 사용하여 별도의 테스트 계정에서 S3 버킷 내에 아티팩트를 스테이징합니다.

C. CodeCommit 태그에서 별도의 파이프라인을 트리거합니다. 단위 테스트 실행에 Jenkins를 사용합니다. 별도의 테스트 계정에서 S3 버킷으로 아티팩트를 스테이징하기 위한 대상으로 S3를 사용하여 파이프라인에 스테이지를 생성합니다.

D. 기능 개발을 위한 별도의 CodeCommit 리포지토리를 만들고 이를 사용하여 파이프라인을 트리거합니다. 단위 테스트를 실행하는 데 AWS Lambda를 사용합니다. AWS CodeBuild를 사용하여 동일한 프로덕션 계정의 서로 다른 S3 버킷 내에 아티팩트를 스테이징합니다.

Answer: A

설명

분기는 커밋에 대한 포인터 또는 참조입니다. 개발 시 작업을 정리하는 편리한 방법입니다. 분기를 사용하여 다른 분기의 작업에 영향을 주지 않고 새 버전이나 다른 버전의 파일에 대한 작업을 분리할 수 있습니다. 이 경우 분기는 별도의 파이프라인을 트리거할 수 있으며 해당 파이프라인에서 단위 테스트를 실행하는 데 CodeBuild를 사용할 수 있습니다. 아티팩트는 프로덕션 환경과의 격리를 위해 별도의 계정에 저장할 수 있습니다.

잘못됨: B는 올바르지 않습니다. CodeBuild는 Lambda 대신 단위 테스트를 실행하는 데 사용해야 합니다.

잘못됨: D는 올바르지 않습니다. 별도의 CodeCommit 리포지토리 대신 분기를 사용할 수 있으며, CodeBuild는 단위 테스트를 실행해야 하며 별도의 계정은 아티팩트를 저장하는 데 사용해야 합니다.

참조:

https://docs.aws.amazon.com/codecommit/latest/userguide/branches.html

Q128

회사에는 사진과 비디오를 Amazon S3 버킷에 안전하게 업로드하는 웹 애플리케이션이 있습니다. 회사는 인증된 사용자만 콘텐츠를 게시할 수 있도록 요구합니다. 애플리케이션은 브라우저 인터페이스를 통해 객체를 업로드하는 데 사용되는 미리 서명된 URL을 생성합니다. 대부분의 사용자는 100MB를 초과하는 객체에 대해 업로드 시간이 느리다고 보고하고 있습니다. 인증된 사용자만 콘텐츠를 게시할 수 있도록 하면서 이러한 업로드의 성능을 개선하기 위해 솔루션스 아키텍트가 할 수 있는 일은 무엇일까요?

A. 리소스를 S3 서비스 프록시로 사용하는 엣지 최적화 API 엔드포인트를 사용하여 Amazon API Gateway를 설정합니다. S3 PutObject 작업을 노출하도록 이 리소스에 대한 PUT 메서드를 구성합니다. COGNITO\_USER\_POOLS 권한 부여자를 사용하여 API 게이트웨이를 보호합니다. 브라우저 인터페이스에서 미리 서명된 URL 대신 API Gateway를 사용하여 객체를 업로드하도록 합니다.

B. 리소스를 S3 서비스 프록시로 사용하는 리전 API 엔드포인트로 Amazon API Gateway를 설정합니다. S3 PutObject 작업을 노출하도록 이 리소스에 대한 PUT 메서드를 구성합니다. AWS Lambda 권한 부여자를 사용하여 API 게이트웨이를 보호합니다. 브라우저 인터페이스에서 미리 서명된 URL 대신 API Gateway를 사용하여 API 객체를 업로드하도록 합니다.

C. S3 버킷에서 S3 전송 가속 엔드포인트를 활성화합니다. 미리 서명된 URL을 생성할 때 엔드포인트를 사용합니다. 브라우저 인터페이스에서 S3 멀티파트 업로드 API를 사용하여 이 URL에 객체를 업로드하도록 합니다.

D. 대상 S3 버킷에 대한 Amazon CloudFront 배포를 구성합니다. CloudFront 캐시 동작에 대해 PUT 및 POST 메서드를 활성화합니다.OAI (오리진 액세스 ID) 를 사용하도록 CloudFront 오리진을 업데이트합니다. 버킷 정책에서 OAI 사용자에게 s3:PutObject 권한을 부여합니다. 브라우저 인터페이스가 CloudFront 배포를 사용하여 객체를 업로드하도록 합니다.

Answer: C

Q129

한 회사에서 퀵 서비스 레스토랑을 운영합니다. 레스토랑은 매일-4 시간 동안 판매 트래픽이 높은 예측 가능한 모델을 따릅니다. Sates 트래픽은 피크 시간 외에는 더 낮습니다. POS 및 관리 플랫폼은 AWS 클라우드에 배포되며 Amazon DynamoDB를 기반으로 하는 백엔드가 있습니다. 데이터베이스 테이블은 100.000개의 RCU와 80.000 WCU의 프로비저닝된 처리량 모드를 사용하여 알려진 최대 리소스 소비량과 일치합니다. 이 회사는 DynamoDB 비용을 줄이고 IT 직원의 운영 오버헤드를 최소화하고자 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. 프로비저닝된 RCU와 WCU를 줄입니다.

B. 온디맨드 용량을 사용하도록 DynamoDB 테이블을 변경합니다.

C. 테이블에 Dynamo DB 자동 좌석을 활성화합니다.

D. 매일 4시간 동안 최대 부하를 감당할 수 있는 1년 예약 용량을 구매합니다.

Answer: C

Q130

한 전자 상거래 회사가 AWS에서 인프라를 실행합니다. 이 회사는 Amazon 탄력적 쿠버네티스 서비스 (Amazon EKS) 클러스터 앞에 있는 애플리케이션 로드 밸런서 (ALB) 를 통해 웹 및 모바일 클라이언트에 API를 노출합니다. EKS 클러스터는 API를 제공하는 수천 개의 포드를 실행합니다. 새로운 대륙으로 전송을 확장한 후 회사는 Amazon CloudFront 배포를 추가하고 ALB를 오리진으로 설정합니다. 이 회사는 또한 아키텍처에 AWS WAF를 추가했습니다. 새 아키텍처를 구현한 후에는 API 호출이 크게 발생합니다.그러나 HTTP 상태 코드 504 (게이트웨이 시간 초과) 오류와 HTTP 상태 코드 502 (잘못된 게이트웨이) 오류가 갑자기 증가합니다. 이러한 오류 증가는 특정 도메인에 대한 것으로 보입니다.

이러한 오류의 원인이 될 수 있는 요인은 무엇입니까?(두 개 선택)

A. AWS WAF가 의심스러운 요청을 차단하고 있습니다.

B. 오리진이 CloudFront에서 제대로 구성되지 않았습니다.

C. 클라우드프론트와 오리진 간에 SSL/TLS 핸드셰이크 문제가 있습니다.

D. EKS 쿠버네티스 파드가 순환되고 있다.

E. 일부 파드는 API 호출에 응답하는 데 30초 이상 걸린다.

Answer: B, C

Q131

한 회사에서 Amazon EC2 인스턴스 플릿에 분산된 인 메모리 데이터베이스를 배포하고 있습니다. 플릿은 기본 노드와 8개의 작업자 노드로 구성됩니다. 기본 노드는 클러스터 상태를 모니터링하고, 사용자 요청을 수락하고, 사용자 요청을 작업자 노드에 배포하고, 집계 응답을 클라이언트로 다시 보내는 작업을 담당합니다. 작업자 노드는 서로 통신하여 데이터 파티션을 복제합니다. 이 회사는 최대 성능을 달성하기 위해 가능한 가장 낮은 네트워킹 대기 시간을 요구합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

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.

Answer: A

Q132

한 엔터프라이즈 회사에서 개발자가 AWS Marketplace를 통해 타사 소프트웨어를 구매할 수 있도록 허용하려고 합니다. 이 회사는 전체 기능이 활성화된 AWS Organizations의 계정 구조를 사용하며, 조달 관리자가 사용할 각 조직 단위 (OU) 에 공유 서비스 계정을 보유하고 있습니다. 조달 팀의 정책에 따르면 개발자는 승인된 목록에서만 타사 소프트웨어를 얻고 AWS Marketplace에서 프라이빗 마켓플레이스를 사용하여 이 요구 사항을 충족할 수 있어야 합니다. 조달 팀은 프라이빗 마켓플레이스 관리를 procurement-manager-role이라는 역할로 제한하려고 합니다. 이 역할은 조달 관리자가 맡을 수 있습니다. 회사의 다른 IAM 사용자, 그룹, 역할 및 계정 관리자는 프라이빗 마켓플레이스 관리 액세스를 거부해야 합니다.

이러한 요구 사항을 충족하는 아키텍처를 설계하는 가장 효율적인 방법은 무엇입니까?

A. 조직의 모든 AWS 계정에서 조달 관리자 역할이라는 IAM 역할을 생성합니다. PowerUserAccess 관리형 정책을 역할에 추가합니다. 모든 AWS 계정의 모든 IAM 사용자 및 역할에 인라인 정책을 적용하여 AWS 프라이빗 마켓플레이스관리자전체 액세스 관리형 정책에 대한 권한을 거부합니다.

B. 조직의 모든 AWS 계정에서 조달 관리자 역할이라는 IAM 역할을 생성합니다. 관리자 액세스 관리형 정책을 역할에 추가합니다. AWS 프라이빗 마켓플레이스관리자전체 액세스 관리형 정책으로 권한 경계를 정의하고 이를 모든 개발자 역할에 연결합니다.

C. 조직의 모든 공유 서비스 계정에서 조달 관리자-역할이라는 IAM 역할을 생성합니다. AWS 프라이빗 마켓플레이스 관리자전체 액세스 관리형 정책을 역할에 추가합니다. 조직의 루트 수준 SCP를 생성하여 procurement-manager-role이라는 역할을 제외한 모든 사람에게 비공개 마켓플레이스 관리 권한을 거부합니다. 조직의 모든 사용자에게 procurement-manager-role이라는 IAM 역할을 만들 수 있는 권한을 거부하려면 다른 조직의 루트 수준 SCP를 생성합니다.

D. 개발자가 사용할 모든 AWS 계정에서 조달 관리자 역할이라는 IAM 역할을 생성합니다. AWS 프라이빗 마켓플레이스 관리자전체 액세스 관리형 정책을 역할에 추가합니다. 조직에서 SCP를 생성하여 조달 관리자 역할이라는 역할을 제외한 모든 사람에게 비공개 마켓플레이스를 관리할 수 있는 권한을 거부합니다. 조직의 모든 공유 서비스 계정에 SCP를 적용합니다.

Answer: C

Q133

한 솔루션 설계자가 회사의 온프레미스 네트워크를 AWS에서 회사의 현재 및 미래의 모든 VPC와 연결하는 솔루션을 설계하고 있습니다. 이 회사는 5개의 다른 AWS 리전에서 VPC를 실행하고 있으며 각 리전에 최소 15개의 VPC를 보유하고 있습니다.

이 회사의 AWS 사용량은 지속적으로 증가하고 있으며 계속 증가할 것입니다. 또한 5개 리전 전체의 모든 VPC는 서로 통신할 수 있어야 합니다. 이 솔루션은 확장성과 관리 용이성을 극대화해야 합니다. 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 각 리전에 전송 게이트웨이를 설정합니다. 온프레미스 방화벽과 온프레미스 네트워크에 가장 가까운 리전의 전송 게이트웨이 간에 중복 AWS 사이트 간 VPN 연결을 설정합니다. 모든 전송 게이트웨이를 서로 피어링합니다. 모든 VPC를 해당 리전의 전송 게이트웨이에 연결합니다.

B. 온프레미스 네트워크로 연결되는 중복 AWS 사이트 간 VPN 터널을 위한 AWS CloudFormation 템플릿을 생성합니다. 각 VPC에 대해 CloudFormation 템플릿을 배포합니다. VPC와 VPC 간 통신을 위해 모든 VPC 간에 VPC 피어링을 설정합니다.

C. 각 리전에 전송 게이트웨이 설정 온프레미스 방화벽과 각 전송 게이트웨이 간에 중복 AWS 사이트 간 VPN 연결을 설정합니다. 회사의 온프레미스 방화벽을 통해 서로 다른 리전 간에 트래픽을 라우팅합니다.모든 VPC를 해당 리전의 전송 게이트웨이에 연결

D. 온프레미스 네트워크에 대한 중복 AWS 사이트 간 VPN 터널을 위한 AWS CloudFormation 템플릿을 생성합니다. 각 VPC에 대해 CloudFormation 템플릿을 배포합니다. 회사의 온프레미스 방화벽을 통해 서로 다른 리전 간에 트래픽을 라우팅합니다.

Answer: A

Q134

한 회사가 AWS에 서버리스 멀티 테넌트 콘텐츠 관리 시스템을 갖추고 있습니다. 아키텍처에는 AWS Lambda가 인증한 사용자 지정 AWS Gateway API를 사용하는 Amazon API Gateway API와 상호 작용하는 웹 기반 프런트 엔드가 포함되어 있습니다. 권한 부여자는 테넌트 ID로 사용자를 인증하고 JSON 웹 토큰 (JWT) 토큰으로 정보를 인코딩합니다. 인증 후 API 게이트웨이를 통한 각 API 호출은 요청을 이행하기 위해 단일 Amazon DynamoDB 테이블과 상호 작용하는 Lambda 함수를 대상으로 합니다. 보안 표준을 준수하기 위해 회사는 임차인 간의 더 강력한 격리가 필요합니다. 이 회사는 첫해 내에 수백 명의 고객을 확보 할 것입니다.

최소한의 운영으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 테이블 이름에 테넌트 ID를 사용하여 각 테넌트에 대한 DynamoDB 테이블을 생성합니다. JWT 토큰을 사용하여 테넌트별 적절한 Lambda 실행 역할을 검색하는 서비스를 생성합니다. IAM 정책을 실행 역할에 연결하여 테넌트의 DynamoDB 테이블에만 액세스하도록 허용합니다.

B. DynamoDB 테이블의 파티션 키에 테넌트 ID 정보를 추가합니다. JWT 토큰을 사용하여 테넌트별 적절한 Lambda 실행 역할을 검색하는 서비스를 생성합니다. IAM 정책을 실행 역할에 연결하여 키가 테넌트 ID와 일치하는 경우에만 테이블의 항목에 대한 액세스를 허용합니다.

C. 애플리케이션의 각 테넌트에 대해 별도의 AWS 계정을 생성합니다. 각 테넌트에 전용 인프라를 사용합니다. 교차 계정 네트워크 연결이 없는지 확인합니다.

D. 모든 DynamoDB 테이블에 테넌트 ID를 정렬 키로 추가합니다. 각 Lambda 함수에 로직을 추가하여 JWT 토큰에서 가져온 테넌트 ID를 DynamoDB 테이블의 모든 작업에서 정렬 키로 사용합니다.

Answer: B

Q135

한 회사에서 프로모션 오퍼를 소개하는 대규모 이벤트를 계획하고 있습니다. 이 회사의 웹 사이트는 AWS에서 호스팅되며 PostgreSQL DB 인스턴스용 Amazon RDS의 지원을 받습니다. 이 웹 사이트에는 프로모션에 대해 설명하고 사용자 정보 및 기본 설정을 수집하는 등록 페이지가 포함되어 있습니다. Management는 예측할 수 없는 대량의 트래픽을 주기적으로 예상하므로 많은 데이터베이스 쓰기가 발생합니다. 솔루션 설계자는 기본 데이터 모델을 변경하지 않고 제출물이 데이터베이스에 커밋되기 전에 삭제되지 않도록 하는 솔루션을 구축해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 이벤트 직전에 예상 수요에 맞게 기존 DB 인스턴스를 확장합니다. 그런 다음 이벤트가 끝난 후 축소합니다.

B. Amazon SQS를 사용하여 애플리케이션 계층과 데이터베이스 계층을 분리합니다. 대기열에서 데이터베이스로 항목을 쓰도록 AWS Lambda 함수를 구성합니다.

C. Amazon DynamoDB로 마이그레이션하고 자동 조정을 통해 처리 용량을 관리합니다.

D. Memcached용 Amazon ElastiCache를 사용하여 DB 인스턴스에 대한 쓰기 용량을 늘립니다.

Answer: B

설명

레코드 삭제를 방지하려면 애플리케이션과 데이터베이스 계층을 분리하는 것이 이 특정 시나리오에 가장 적합한 솔루션입니다. 이것은 애플리케이션이 동기 응답을 요구하지 않기 때문에 작동합니다(단지 사용자 정보를 DB에 쓰기만 하면 됨). 대안은 데이터베이스 인스턴스의 쓰기 용량을 늘리는 것이지만 트래픽을 예측할 수 없기 때문에 프로비저닝할 용량이 어느 정도인지 알기 어렵기 때문에 성능이 저하되거나 필요한 비용보다 높을 수 있습니다.

잘못됨: A. RDS 데이터베이스 인스턴스를 확장 또는 축소하도록 예약할 수 없습니다.

잘못됨: C. DynamoDB는 NoSQL(비관계형) 데이터베이스이고 RDS는 관계형 데이터베이스입니다. 이 솔루션은 기본 데이터 모델을 변경하므로 옵션이 아닙니다.

잘못됨: D. ElastiCache는 쓰기 성능이 아니라 읽기 성능을 향상시키는 데 사용됩니다.

참조:

https://docs.aws.amazon.com/AWSSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html

Q136

개발팀은 사용자에게 실시간에 가까운 데이터를 제공하는 새로운 항공편 추적기 애플리케이션을 만들었습니다. 애플리케이션에는 단일 가용 영역에 있는 2개의 대형 Amazon EC2 인스턴스 앞에 ALB (애플리케이션 로드 밸런서) 로 구성된 프런트 엔드가 있습니다. 데이터는 단일 Amazon RDS MySQL DB 인스턴스에 저장됩니다. Amazon Route 53 DNS 레코드는 ALB를 가리킵니다. 경영진은 개발 팀이 최소한의 운영 오버헤드로 최대의 신뢰성을 달성하기 위해 솔루션을 개선하기를 원합니다.

팀은 어떤 조치를 취해야 하나요?

A. RDS MySQL 읽기 전용 복제본을 생성합니다애플리케이션을 여러 AWS 리전에 배포합니다. Route 53 지연 시간 기반 라우팅 정책을 사용하여 애플리케이션으로 라우팅합니다.

B. DB 인스턴스를 다중 AZ로 구성합니다. 애플리케이션을 ALB 뒤의 서로 다른 가용 영역에 있는 2개의 추가 EC2 인스턴스에 배포합니다.

C. DB 인스턴스를 Amazon DynamoDB 글로벌 테이블로 교체합니다. 여러 AWS 리전에 애플리케이션을 배포합니다. Route 53 지연 시간 기반 라우팅 정책을 사용하여 애플리케이션으로 라우팅합니다.

D. DB 인스턴스를 Amazon Aurora와 Aurora 복제본으로 교체합니다. ALB 뒤에 있는 Auto Scaling 그룹의 여러 가용 영역에 걸쳐 소규모 EC2 인스턴스 여러 개에 애플리케이션을 배포합니다.

Answer: D

Q137

금융 서비스 조직은 개인 식별 정보를 애플리케이션 로그에 기록하며, 이 로그는 Amazon S3에 저장됩니다. 로그 파일은 규정 준수 표준을 준수하기 위해 저장 시 암호화되어야 합니다. 보안 팀은 회사의 온-프레미스 HSM (하드웨어 보안 모듈) 을 사용하여 CMK 콘텐츠를 생성하도록 지정했습니다.

솔루션 설계자는 이러한 요구 사항을 준수하기 위해 어떤 절차를 수행해야 합니까?

A. AWS CloudHSM 클러스터를 생성합니다. AWS CloudHSM을 키 구성 요소의 소스 및 AWS CloudHSM의 오리진으로 사용하여 AWS KMS에서 새 CMK를 생성합니다. CMK에서 1년 동안 자동 키 교체를 활성화합니다. 로깅 버킷에 암호화되지 않은 데이터의 업로드를 허용하지 않고 암호화 소스가 AWS KMS여야 하는 버킷 정책을 구성합니다.

B. AWS Direct Connect 연결을 프로비저닝하여 온프레미스 하드웨어와 VPC 간에 RFC 1918 주소 공간이 중복되지 않도록 합니다. 로깅 버킷에 모든 객체를 암호화해야 하는 AWS 버킷 정책을 구성합니다. AWS 환경의 온프레미스 HSM에 암호화 키 구성 요소를 쿼리하도록 로깅 애플리케이션을 구성하고 각 로깅 이벤트에 대해 고유한 CMK를 생성합니다.

C. AWS KMS에서 키 구성 요소가 없고 원본이 외부인 CMK를 생성합니다. AWS에서 제공하는 퍼블릭 키 및 가져오기 토큰을 사용하여 온프레미스 HSM에서 생성된 키 구성 요소를 CMK로 가져옵니다. 로깅 버킷에 암호화되지 않은 데이터의 업로드를 허용하지 않고 암호화 소스가 AWS KMS여야 하는 버킷 정책을 구성합니다.

D. AWS에서 제공하는 키 구성 요소 및 AWS\_KMS의 오리진을 사용하여 AWS KMS에서 새 CMK를 생성합니다. 이 CMK를 비활성화하고 AWS에서 제공하는 퍼블릭 키 및 가져오기 토큰을 사용하여 온프레미스 HSM의 키 구성 요소로 키 구성 요소를 덮어씁니다. CMK를 다시 활성화합니다.CMK에서 1년 동안 자동 키 교체를 활성화합니다. 로깅 버킷에 암호화되지 않은 데이터의 업로드를 허용하지 않고 암호화 소스가 AWS KMS여야 하는 버킷 정책을 구성합니다.

Answer: C

Q138

한 회사에서 정적 포트에서 TCP를 사용하여 액세스할 수 있는 새 서비스를 개발 중입니다. 솔루션 설계자는 서비스의 가용성이 높고, 가용 영역 전체에 중복성이 있으며, 공개적으로 액세스할 수 있는 DNS 이름 myservice.com을 사용하여 액세스할 수 있는지 확인해야 합니다. 서비스는 다른 회사가 허용 목록에 주소를 추가할 수 있도록 고정 주소 할당을 사용해야 합니다. 리소스가 단일 리전의 여러 가용 영역에 배포되었다고 가정합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 각 인스턴스에 대해 탄력적 IP 주소를 사용하여 Amazon EC2 인스턴스를 생성합니다. NLB (네트워크 부하 분산 장치) 를 만들고 정적 TCP 포트를 노출합니다. EC2 인스턴스를 NLB에 등록합니다. my.service.com이라는 새 이름 서버 레코드 세트를 생성하고 EC2 인스턴스의 탄력적 IP 주소를 레코드 세트에 할당합니다. EC2 인스턴스의 탄력적 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

B. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다. ECS 클러스터의 퍼블릭 IP 주소를 생성하고 할당합니다. NLB (네트워크 부하 분산 장치) 를 만들고 TCP 포트를 노출합니다. 대상 그룹을 생성하고 ECS 클러스터 이름을 NLB에 할당합니다. my.service.com이라는 새 A 레코드 세트를 생성하고 ECS 클러스터의 퍼블릭 IP 주소를 레코드 세트에 할당합니다. ECS 클러스터의 퍼블릭 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

C. 서비스에 대한 Amazon EC2 인스턴스를 생성합니다. 각 가용 영역에 대해 하나의 탄력적 IP 주소를 생성합니다.NLB (네트워크 부하 분산 장치) 를 만들고 할당된 TCP 포트를 노출합니다. 탄력적 IP 주소를 각 가용 영역의 NLB에 할당합니다. 대상 그룹을 생성하고 NLB에 EC2 인스턴스를 등록합니다. my.service.com이라는 새 A (별칭) 레코드 세트를 만들고 NLB DNS 이름을 레코드 세트에 할당합니다.

D. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다. 클러스터의 각 호스트에 대한 퍼블릭 IP 주소를 생성하고 할당합니다. ALB (애플리케이션 로드 밸런서) 를 생성하고 정적 TCP 포트를 노출합니다. 대상 그룹을 생성하고 ECS 서비스 정의 이름을 ALB에 할당합니다. 새 CNAME 레코드 세트를 만들고 퍼블릭 IP 주소를 레코드 세트에 연결합니다. Amazon EC2 인스턴스의 탄력적 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

Answer: C

Q139

AWS 클라우드에서 비즈니스는 컨테이너화된 대규모 워크로드를 운영하고 있습니다. 약 100개의 개별 서비스가 이 과제로 구성됩니다. 워크로드는 Amazon Elastic Container Service (Amazon ECS) 를 사용하여 회사에서 오케스트레이션합니다. 최근 이 회사의 개발 팀은 ECS 클러스터의 Amazon EC2 인스턴스에서 AWS Fargate로 전환했습니다. 이전에는 워크로드가 계정의 최대 EC2 인스턴스 수를 모두 소모하는 데 위험할 정도로 가까워졌습니다. 조직은 워크로드가 ECS 작업의 허용 수를 초과할 것이라고 우려하고 있습니다. 솔루션 설계자는 Fargate가 최대 작업 용량의 80% 를 초과할 때 개발 팀에 알리는 솔루션을 구축해야 합니다.

이 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?

A. Amazon CloudWatch를 사용하여 ECS 클러스터의 각 서비스에 대한 샘플 카운트 통계를 모니터링합니다. 수학 표현식 샘플 개수/SERVICE\_QUOTA (서비스) \*100이 80보다 큰 경우에 대한 경보를 설정합니다. Amazon Simple Notification Service (Amazon SNS) 를 사용하여 개발 팀에 알립니다.

B. Amazon CloudWatch를 사용하여 AWS/사용량 지표 네임스페이스 아래에 게시된 서비스 할당량을 모니터링합니다. 수학 표현식 메트릭/서비스\_할당량 (메트릭) \*100이 80보다 큰 경우에 대한 경보를 설정합니다. Amazon Simple Notification Service (Amazon SNS) 를 사용하여 개발 팀에 알립니다.

C. AWS Lambda 함수를 생성하여 ECS 클러스터에서 세부 지표를 폴링합니다. 실행 중인 Fargate 작업 수가 80개를 초과하는 경우 Amazon Simple Email Service (Amazon SES) 를 호출하여 개발 팀에 알립니다.

D. AWS 구성 규칙을 생성하여 파게이트 서비스\_쿼터가 80보다 큰지 여부를 평가합니다. AWS Config 규칙이 규정을 준수하지 않을 경우 Amazon Simple Email Service (Amazon SES) 를 사용하여 개발 팀에 알립니다.

Answer: B

Q140

한 회사가 웹 애플리케이션을 AWS로 이전하려고 합니다. 응용 프로그램은 세션 정보를 각 웹 서버에 로컬로 저장하므로 Auto Scaling이 어려워집니다. 마이그레이션 중에 응용 프로그램이 다시 작성되어 세션 데이터를 웹 서버에서 분리합니다. 이 회사는 낮은 지연 시간, 확장성 및 가용성을 필요로 합니다.

세션 정보를 가장 비용 효율적인 방식으로 저장하기 위한 요구 사항을 충족하는 서비스는 무엇입니까?

A. 멤캐시드 엔진을 사용하는 Amazon ElastiCache

B. Amazon S3

C. Amazon RDS MySQL

D. Redis 엔진을 사용하는 Amazon ElastiCache

Answer: D

Q141

한 의료 회사가 일련의 Amazon EC2 인스턴스에서 REST API를 튜닝하고 있습니다. EC2 인스턴스는 애플리케이션 로드 밸런서 (ALB) 뒤에 있는 Auto Scaling 그룹을 시작합니다. ALB는 3개의 퍼블릭 서브넷에서 실행되며 EC2 인스턴스는 3개의 프라이빗 서브넷에서 실행됩니다. 이 회사는 ALB을 유일한 오리진으로 사용하는 Amazon CloudFront 배포를 배포했습니다.

원본 보안을 강화하기 위해 솔루션 설계자가 추천해야 하는 솔루션은 무엇입니까?

A. AWS 보안 관리자에 임의의 문자열을 저장합니다. 자동 시크릿 로테이션을 위한 AWS Lambda 함수를 생성합니다. 임의 문자열을 오리진 요청에 대한 사용자 지정 HTTP 헤더로 삽입하도록 CloudFront를 구성합니다. 사용자 지정 헤더에 대한 문자열 일치 규칙이 있는 AWS WAF 웹 ACL 규칙을 생성합니다. 웹 ACL을 AL8과 연결합니다.

B. CloudFront 서비스 IP 주소 범위의 IP 일치 조건을 사용하여 AWS WAF 웹 ACL 규칙을 생성합니다. 웹 ACL을 ALB와 연결합니다.ALB를 세 개의 프라이빗 서브넷으로 이동합니다.

C. AWS Systems Manager 파라미터 스토어에 임의의 문자열을 저장합니다. 문자열에 대한 매개 변수 저장소 자동 회전을 구성합니다. 임의 시어링을 오리진 요청에 대한 사용자 지정 HTTP 헤더로 삽입하도록 CloudFront를 구성합니다. 사용자 지정 HTTP 헤더의 값을 검사하고 ALB에서 액세스를 차단합니다.

D. AWS 쉴드 어드밴스를 구성합니다. CloudFront 서비스 IP 주소 범위에서의 연결을 허용하는 보안 그룹 정책을 생성합니다. 정책을 AWS Shield 어드밴스드에 추가하고 정책을 ALB에 연결합니다.

Answer: A

Q142

솔루션스 아키텍트는 AWS Organizations를 사용하여 회사의 여러 AWS 계정을 관리합니다. 조직에 대해 전체 조직 기능 세트가 활성화됩니다. 모든 프로덕션 AWS 계정은 “프로덕션”이라는 OU 아래에 존재합니다. 시스템 운영자는 IAM 역할을 사용하여 이러한 계정 내에서 전체 관리 권한을 갖습니다. 이 회사는 모든 프로덕션 계정의 보안 그룹이 TCP 포트 22에 대한 인바운드 트래픽을 허용하지 않도록 하려고 합니다. 모든 비준수 보안 그룹은 즉시 수정해야 하며 포트 22를 허용하는 새 규칙을 만들 수 없습니다.

윈치 솔루션은 이러한 요구 사항을 충족합니까?

A. 값이 22인 ec2:tngress 규칙 조건으로 보안 그룹 만들기 작업을 거부하는 SCP를 작성합니다. SCP를 '프로덕션' OU에 적용합니다.

B. 모든 계정에 대해 AWS CloudTrail 추적 구성 조직 관리 계정의 Amazon S3 버킷으로 CloudTrail 로그를 전송합니다. 보안 그룹을 설명하고 수정하기 위해 모든 프로덕션 계정에서 역할을 수임할 수 있는 권한을 가진 관리 계정에 AWS Lambda 함수를 구성합니다. S3 버킷의 모든 PutObject 이벤트에서 Lambda 함수를 호출하도록 Amazon S3 구성 비준수 보안 그룹 작업에 대해 각 CloudTrail 이벤트를 분석하고 문제를 자동으로 해결하도록 Lambda 함수를 구성합니다.

C. 조직 관리 계정에서 Amazon EvertBridge (Amazon CloudWatch Events) 이벤트 버스를 생성합니다. AWS Cloud Formation 템플릿을 생성하여 CreateSecurityGroup 이벤트를 프로덕션 계정에서 이벤트 버스로 전송하는 구성을 배포합니다. 모든 프로덕션 계정에서 역할을 수임할 수 있는 권한을 가진 관리 계정에서 AWS Lambda 함수를 구성하여 보안 그룹을 설명하고 수정합니다. Lambda 함수를 호출하도록 이벤트 버스를 구성합니다. 규정을 준수하지 않는 보안 그룹 작업에 대한 각 이벤트를 분석하고 문제를 자동으로 해결하도록 Lambda 함수를 구성합니다.

D. AWS CloudFormation 템플릿을 생성하여 AWS 구성을 켭니다. INCOMING\_SSH\_DISABLED AWS Config 관리형 규칙을 활성화합니다. AWS Config 검색 결과에 따라 실행되고 규정 미준수 리소스를 수정하는 AWS Lambda 함수를 배포합니다. “프로덕션” OU에 할당된 스택셋을 사용하여 CloudFormation템플릿을 배포합니다. OU에 SCP를 적용하여 CloudFormation 템플릿이 프로비저닝하는 리소스의 수정을 거부합니다.

Answer: D

Q143

솔루션 설계자는 Amazon EC2 인스턴스 집합에 애플리케이션을 배포해야 합니다. EC2 인스턴스는 Auto Scaling 그룹의 프라이빗 서브넷에서 실행됩니다. 애플리케이션은 각 EC2 인스턴스에서 초당 100MB의 속도로 로그를 생성할 것으로 예상됩니다. Amazon EMR 클러스터가 추가 처리를 위해 사용할 수 있도록 로그를 Amazon S3 버킷에 저장해야 합니다. 로그는 처음 90일 동안 빠르게 액세스할 수 있어야 하며 그 후 48시간 이내에 검색할 수 있어야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 솔루션은 무엇입니까?

A. S3 Standard스토리지가 있는 S3 버킷에 각 EC2 인스턴스에서 로그를 기록하도록 S3 복사 작업을 설정합니다. 프라이빗 서브넷 내에서 NAT 인스턴스를 사용하여 Amazon S3에 연결합니다. S3 수명 주기 정책을 생성하여 90일이 넘은 로그를 S3 Glacier로 이동합니다.

B. S3 Standard 스토리지가 있는 S3 버킷으로 각 EC2 인스턴스에서 로그를 복사하도록 S3 동기화 작업을 설정합니다. Amazon S3에 대한 게이트웨이 VPC 엔드포인트를 사용하여 Amazon S3에 연결합니다. S3 수명 주기 정책을 생성하여 90일이 넘은 로그를 3 Glacier Deep Archive로 이동합니다.

C. 각 EC2 인스턴스에서 S3 Standard 스토리지가 있는 S3 버킷으로 로그를 복사하도록 S3 배치 작업을 설정합니다. 프라이빗 서브넷이 있는 NAT 게이트웨이를 사용하여 Amazon S3 Create S3 수명 주기 정책에 연결하여 90일보다 오래된 로그를 S3 Glacier Deep Archive로 이동합니다.

D. 각 EC2 인스턴스의 로그를 S3 Standard 스토리지가 있는 S3 버킷으로 복사하도록 S3 동기화 작업을 설정합니다. Amazon S3용 게이트웨이 VPC 엔드포인트를 사용하여 Amazon S3에 연결합니다. S3 수명 주기 정책을 생성하여 90일보다 오래된 로그를 S3 Glacier로 이동합니다.

Answer: D

Q144

한 회사가 단일 AWS 리전에서 서버리스 애플리케이션을 실행합니다.응용 프로그램은 외부 URL에 액세스하고 해당 사이트에서 메타데이터를 추출합니다. 이 회사는 Amazon Simple Notification Service (Amazon SNS) 주제를 사용하여 URL을 Amazon Simple Queue Service (Amazon SQS) 대기열에 게시합니다. AWS Lambda 함수는 대기열을 이벤트 소스로 사용하고 대기열의 URL을 처리합니다. 결과는 Amazon S3 버킷에 저장됩니다. 회사는 사이트 현지화의 가능한 차이점을 비교하기 위해 다른 지역의 각 URL을 처리하려고 합니다. URL은 기존 지역에서 게시되어야 합니다. 결과는 현재 리전의 기존 S3 버킷에 기록되어야 합니다.

이러한 요구 사항을 충족하는 다중 리전 배포를 생성하는 변경 사항의 조합은 무엇입니까?(두 개 선택)

A. Lambda 함수가 포함된 SQS 대기열을 다른 리전에 배포합니다.

B. 각 리전의 SNS 주제를 SQS 대기열에 구독합니다.

C. 각 리전의 SQS 대기열을 각 리전의 SNS 주제에 구독합니다.

D. 각 리전의 SNS 주제에 URL을 게시하도록 SQS 대기열을 구성합니다.

E. SNS 주제와 Lambda 함수를 다른 리전에 배포합니다.

Answer: C, D

Q145

솔루션 설계자는 새 Amazon S3 버킷에 저장될 객체에 대해 클라이언트 측 암호화 메커니즘을 구현해야 합니다.솔루션스 아키텍트는 이를 위해 AWS 키 관리 서비스 (AWS KMS) 에 저장되는 CMK를 생성했습니다.

솔루션스 아키텍트는 다음과 같은 IAM 정책을 생성하여 IAM 역할에 연결했습니다.



테스트 중에 솔루션 아키텍트는 S3 버킷의 기존 테스트 객체를 성공적으로 가져올 수 있었습니다. 하지만 새 객체를 업로드하려고 하면 오류 메시지가 표시되었습니다.오류 메시지는 나에게 행동이 금지되었다고 말했습니다.

모든 요구 사항을 충족하기 위해 솔루션스 아키텍트가 IAM 정책에 추가해야 하는 작업은 무엇입니까?

A. Kms:GenerateDataKey

B. KmsGetKeyPolpcy

C. kmsGetPubKKey

D. kms:SKjn

Answer: A

Q146

한 회사가 인기있는 온라인 게임의 속편을 만들고 있습니다.전 세계의 많은 사용자가 출시 후 첫 주 이내에 게임을 플레이합니다.현재 이 게임은 단일 AWS 리전에 배포된 다음 구성 요소로 구성되어 있습니다.

\* 게임 자산을 저장하는 Amazon S3 버킷

\* 플레이어 점수를 저장하는 Amazon DynamoDB 테이블

솔루션 설계자는 wifi가 지연 시간을 줄이고 안정성을 개선하며 구현하는 데 최소한의 노력으로 지역 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. Amazon CloudFront 배포를 생성하여 S3 버킷의 자산을 처리합니다. S3 교차 리전 복제 구성 새 리전에 새 DynamoDB 테이블 생성 DynamoDB 글로벌 테이블의 복제본 대상으로 새 테이블을 사용합니다.

B. Amazon CloudFront 배포를 생성하여 S3 버킷의 자산을 제공합니다. S3 동일 리전 복제를 구성합니다.새 리전에 새 DynamoDB 테이블을 생성합니다. 변경 데이터 캡처 (CDC: change data capture) 와 함께 AWS Database Migration Service (AWS DMS) 를 사용하여 DynamoDB 테이블 간에 비동기 복제를 구성합니다.

C. 새 리전에 다른 S3 버킷을 생성하고 버킷 간에 S3 교차 리전 복제를 구성합니다. Amazon CloudFront 배포를 생성하고 각 리전의 S3 버킷에 액세스하는 두 오리진으로 오리진 장애 조치를 구성합니다. Amazon DynamoDB 스트림을 활성화하여 DynamoDB 글로벌 테이블을 구성하고 새 리전에 복제본 테이블을 추가합니다.

D. 동일한 리전에 다른 S3 버킷을 생성하고 버킷 간에 S3 동일 리전 복제 구성- Amazon CloudFront 배포를 생성하고 두 오리진이 S3 버킷에 액세스하도록 오리진 장애 조치를 구성합니다. 새 리전에 새 DynamoDB 테이블 생성 새 테이블을 다음에 대한 복제본 대상으로 사용DynamoDB 글로벌 테이블입니다.

Answer: C

Q147

한 회사가 AWS CodePipeline 및 AWS CloudFormation을 사용하여 AWS에 애플리케이션을 배포하는 방법을 표준화했습니다. 응용 프로그램은 타이프 라이터와 파이썬에 있습니다. 이 회사는 최근 Python 스크립트를 사용하여 AWS에 애플리케이션을 배포하는 또 다른 비즈니스를 인수했습니다. 새로 인수한 회사의 개발자는 CloudFormation으로 애플리케이션을 이전하는 것을 주저합니다. 새로운 도메인별 언어를 배우고 루핑과 같은 언어 기능에 대한 액세스를 제거해야 하기 때문입니다. 개발자들의 우려 사항을 해결하면서 확보한 애플리케이션을 배포 표준에 신속하게 적용할 수 있는 방법은 무엇입니까?

A. CloudFormation 템플릿을 생성하고 Python 스크립트의 일부를 인스턴스 사용자 데이터로 재사용합니다. AWS Cloud Development Kit (AWS CDK) 를 사용하여 이러한 템플릿을 사용하여 애플리케이션을 배포합니다. AWS CDK를 CodePipeline에 통합하고 이러한 템플릿을 사용하여 애플리케이션을 AWS에 배포합니다.

B. AWS CodeBuild 내에서 타사 리소스 프로비저닝 엔진을 사용하여 기존 및 인수된 회사의 배포 프로세스를 표준화합니다. CodePipeline을 사용하여 코드빌드 작업을 오케스트레이션합니다.

C. AWS OpsWorks에서 표준화합니다. OpsWorks를 CodePipeline과 통합합니다. 개발자가 Chef 레시피를 생성하여 AWS에 애플리케이션을 배포하도록 합니다.

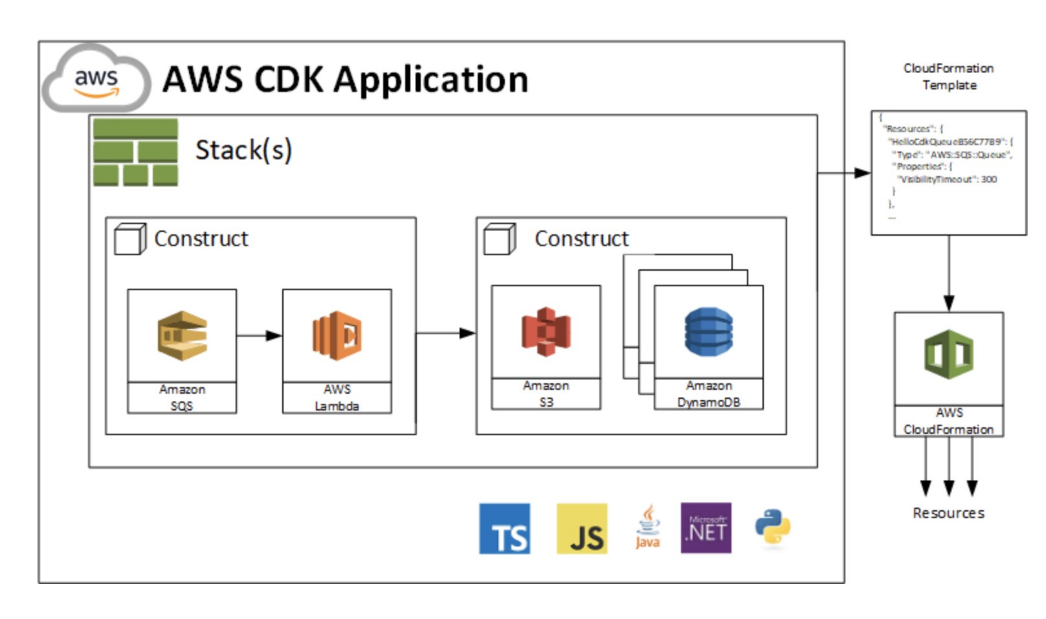
D. Typescript 또는 Python을 사용하여 AWS 리소스를 정의합니다. AWS Cloud Development Kit (AWS CDK) 를 사용하여 개발자 코드에서 CloudFormation 템플릿을 생성하고 AWS CDK를 사용하여 CloudFormation스택을 생성합니다. AWS CDK를 CodePipeline에서 코드빌드 작업으로 통합합니다.

Answer: D

설명

AWS CDK는 클라우드 인프라를 코드로 정의하고 AWS CloudFormation을 통해 프로비저닝하기 위한 소프트웨어 개발 프레임워크입니다. AWS CDK를 사용하여 친숙한 프로그래밍 언어로 클라우드 리소스를 정의할 수 있습니다. AWS CDK는 TypeScript, JavaScript, Python, Java 및 C#/.Net을 지원합니다.

개발자는 지원되는 프로그래밍 언어 중 하나를 사용하여 구성이라고 하는 재사용 가능한 클라우드 구성요소를 정의할 수 있습니다. 이를 스택과 앱으로 함께 구성합니다. 아래 다이어그램은 AWS CDK 애플리케이션이 구성되는 방식을 보여줍니다.



잘못됨: A. 인스턴스 사용자 데이터를 사용하여 JavaScript 또는 TypeScript 코드를 실행할 수 없습니다. 이것은 이러한 응용 프로그램 중 하나를 배포하는 방법이 아닙니다.

잘못됨: B. CodeBuild는 리소스 프로비저닝을 수행하지 않습니다. CodeDeploy 또는 CloudFormation은 수행합니다.

참조:

https://docs.aws.amazon.com/cdk/latest/guide/home.html

Q148

회사는 월별 AWS 청구서에서 각 애플리케이션 또는 팀에 귀속되는 비용을 결정해야 합니다. 또한 회사는 지난 12개월의 비용을 비교하고 향후 12개월 동안의 비용을 예측하는 데 도움이 되는 보고서를 생성할 수 있어야 합니다. 솔루션스 아키텍트는 이러한 비용 보고서를 제공하는 AWS 결제 및 비용 관리 솔루션을 추천해야 합니다.

이러한 요구 사항을 충족하는 작업 조합은 무엇입니까?(세 개 선택)

A. 애플리케이션과 팀을 나타내는 사용자 정의 비용 할당 태그를 활성화합니다.

B. 애플리케이션과 팀을 나타내는 AWS에서 생성한 비용 할당 태그를 활성화합니다.

C. 청구 및 비용 관리에서 각 애플리케이션에 대한 비용 범주를 생성합니다.

D. 결제 및 비용 관리에 대한 IAM 액세스를 활성화합니다.

E. 비용 예산을 생성합니다.

F. 비용 탐색기를 활성화합니다.

Answer: A, C, F

Q149

과학 조직에서는 Amazon S3 버킷에 저장된 텍스트 및 그림 데이터를 처리해야 합니다. 데이터는 임무의 실시간 시간이 중요한 단계에서 수많은 레이더 스테이션에서 수집됩니다. 데이터는 레이더 스테이션에 의해 소스 S3 버킷으로 업로드됩니다. 데이터 앞에는 레이더 스테이션의 식별 번호가 붙습니다. 두 번째 계정에서 비즈니스는 대상 S3 버킷을 구축했습니다. 규정 준수 목표를 충족하려면 원본 S3 버킷에서 대상 S3 버킷으로 데이터를 전송해야 합니다. 복제는 원본 S3 버킷의 모든 항목을 포함하는 S3 복제 규칙을 사용하여 수행됩니다. 단일 레이더 스테이션이 가장 정확한 데이터를 보유한 것으로 인식되었습니다. 이 레이더 스테이션에서는 레이더 스테이션이 소스 S3 버킷에 항목을 업로드한 후 30분 이내에 데이터 복제를 완료해야 합니다.

이러한 기준을 충족하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?

A. AWS DataSync 에이전트를 설정하여 접두사가 붙은 데이터를 원본 S3 버킷에서 대상 S3 버킷으로 복제합니다. 작업에서 사용 가능한 모든 대역폭을 사용하려면 선택하고 작업을 모니터링하여 TRANSERING 상태인지 확인합니다. 이 상태가 변경될 경우 알림을 트리거하는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

B. 두 번째 계정에서 레이더 스테이션에서 가장 정확한 데이터로 데이터를 수신할 또 다른 S3 버킷을 생성합니다. 이 새 S3 버킷에 대한 새 복제 규칙을 설정하여 복제를 다른 레이더 스테이션과 분리합니다. 대상에 대한 최대 복제 시간을 모니터링합니다.시간이 원하는 임계값을 초과할 때 알림을 트리거하는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

C. 원본 S3 버킷에서 Amazon S3 전송 가속을 활성화하고 새 엔드포인트를 사용하도록 가장 정확한 데이터로 레이더 스테이션을 구성합니다. S3 대상 버킷의 총 요청 지연 지표를 모니터링합니다. 이 상태가 변경될 경우 알림을 트리거하는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

D. 가장 정확한 데이터로 레이더 스테이션의 접두사를 사용하는 키를 필터링하는 새 S3 복제 규칙을 원본 S3 버킷에 생성합니다.S3 복제 시간 제어 (S3 RTC) 를 활성화합니다. 대상에 대한 최대 복제 시간을 모니터링합니다.시간이 원하는 임계값을 초과할 때 알림을 트리거하는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

Answer: D

Q150

한 회사가 온프레미스에서 AWS 클라우드로 3계층 웹 애플리케이션을 마이그레이션하고 있습니다. 이 회사는 마이그레이션 프로세스에 대해 다음과 같은 요구 사항을 가지고 있습니다.

\* 온프레미스 환경에서 머신 이미지를 수집합니다.

\* 프로덕션 컷오버까지 온프레미스 환경에서 AWS 환경으로 변경 사항을 동기화합니다.

\* 생산 컷오버를 실행할 때 가동 중지 시간을 최소화합니다.

\* 가상 머신의 루트 볼륨과 데이터 볼륨을 마이그레이션합니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS Server Migration Service (SMS) 를 사용하여 애플리케이션의 각 계층에 대한 복제 작업을 생성하고 시작합니다. AWS SMS에서 생성한 AMI에서 인스턴스를 시작합니다. 초기 테스트 후 최종 복제를 수행하고 업데이트된 AMI에서 새 인스턴스를 생성합니다.

B. AWS CLIVM 가져오기/내보내기 스크립트를 생성하여 각 가상 머신을 마이그레이션합니다. 스크립트가 점증적으로 실행되도록 예약하여 응용 프로그램의 변경 사항을 유지합니다. VM 가져오기/내보내기를 통해 생성된 AMI에서 인스턴스를 시작합니다. 테스트가 완료되면 스크립트를 다시 실행하여 최종 가져오기를 수행하고 AMI에서 인스턴스를 시작합니다.

C. AWS Server Migration Service (SMS) 를 사용하여 운영 체제 볼륨을 업로드합니다. AWS CLI 임포트-스냅 핫 명령 '또는 데이터 볼륨을 사용합니다. AWS SMS에서 생성한 AMI에서 인스턴스를 시작하고 데이터 볼륨을 인스턴스에 연결합니다. 초기 테스트 후 최종 복제를 수행하고 복제된 AMI에서 새 인스턴스를 시작합니다. 그런 다음 데이터 볼륨을 인스턴스에 연결합니다.

D. AWS 애플리케이션 검색 서비스 및 AWS 마이그레이션 허브를 사용하여 가상 머신을 애플리케이션으로 그룹화합니다. AWS CLI VM 가져오기/내보내기 스크립트를 사용하여 가상 시스템을 AMI로 가져옵니다. 스크립트가 점증적으로 실행되도록 예약하여 응용 프로그램의 변경 사항을 유지합니다. AMI에서 인스턴스를 시작합니다. 초기 테스트 후 최종 가상 머신 가져오기를 수행하고 AMI에서 새 인스턴스를 시작합니다.

Answer: A

Q151

한 회사가 AWS에서 전 세계 방문자가 있는 사진 웹 사이트를 호스팅합니다. 웹 사이트는 지난 12개월 동안 트래픽이 꾸준히 증가했으며 사용자는 이미지 표시가 지연되었다고 보고했습니다. 이 회사는 Amazon CloudFront가 최소한의 지연 시간으로 방문자에게 사진을 전송하도록 구성하려고 합니다.

이 목표를 달성할 수 있는 조치는 무엇입니까?(두 개 선택)

A. CloudFront 배포에서 최소 TTL 및 최대 TTL을 0으로 설정합니다.

B. CloudFront 배포에서 최소 TTL 및 최대 TTL을 높은 값으로 설정합니다.

C. CloudFront 배포를 설정하여 모든 헤더, 모든 쿠키 및 모든 쿼리 문자열을 오리진에 전달합니다.

D. 요청자와 지리적으로 더 가까운 추가 원천 서버를 설정합니다. Amazon Route 53에서 지연 시간 기반 라우팅을 구성합니다.

E. CloudFront 배포에서 가격 등급 100을 선택합니다.

Answer: B, D

Q152

한 회사에서 개발자가 Amazon EC2, Amazon S3 및 Amazon DynamoDB만 사용하도록 제한하기 위해 AWS Organizations을 구현하는 중입니다. 개발자 계정은 전용 OU (조직 구성 단위) 에 있습니다. 솔루션 설계자는 개발자 계정에 다음 SCP를 구현했습니다.



이 정책이 배포되면 개발자 계정의 IAM 사용자는 정책에 나열되지 않은 AWS 서비스를 계속 사용할 수 있습니다. 이 정책의 범위를 벗어난 서비스를 사용하는 개발자의 능력을 없애기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 제한해야 하는 각 AWS 서비스에 대해 명시적인 거부 문을 생성합니다.

B. 개발자 계정의 OU에서 전체 AWS 액세스 SCP를 제거합니다.

C. 모든 서비스를 명시적으로 거부하도록 전체 AWS 액세스 SCP를 수정합니다.

D. SCP의 끝에 와일드카드를 사용하여 명시적 거부 문을 추가합니다.

Answer: B

Q153

한 회사에서 허브 앤 스포크 모델에 AWS Transit Gateway를 사용하여 여러 VPC 간의 네트워크 트래픽을 관리합니다. 이 회사는 100Gbps의 속도로 데이터를 전송할 수 있어야 하는 새로운 서비스를 개발 중입니다. 이 회사는 동일한 AWS 리전에 있는 다른 VPC에 더 빠르게 연결해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 필요한 VPC 간에 VPC 피어링을 설정합니다. 모든 라우팅 테이블이 필요에 따라 업데이트되었는지 확인합니다.

B. VPC에 추가 전송 게이트웨이를 연결합니다. 그에 따라 라우팅 테이블을 업데이트합니다.

C. 필요한 VPC 간에 동일 비용 다중 경로 (ECMP) 라우팅을 사용하는 AWS 사이트 간 VPN 연결을 생성합니다.

D. 필요한 VPC에서 기존 전송 게이트웨이로 추가 연결을 생성합니다.

Answer: D

Q154

한 회사에서 온프레미스에서 AWS로 애플리케이션을 마이그레이션할 계획입니다. 이 애플리케이션은 현재 Oracle 데이터베이스를 사용하고 있으며 마이그레이션의 일부로 새 인프라로 전환할 때 1시간의 짧은 다운타임을 허용할 수 있습니다. 데이터베이스 엔진은 MySQL로 변경됩니다. 솔루션 설계자는 필요한 작업과 시간을 최소화하면서 마이그레이션을 수행하는 데 사용할 수 있는 AWS 서비스를 결정해야 합니다.

다음 중 요구 사항을 충족하는 것은 무엇입니까?

A. AWS SCT를 사용하여 스키마 스크립트를 생성하고 마이그레이션 전에 대상에 적용합니다. AWS DMS를 사용하여 현재 스키마를 분석하고 최적의 데이터베이스 엔진에 대한 권장 사항을 제공합니다. 그런 다음 AWS DMS를 사용하여 권장 엔진으로 마이그레이션합니다. AWS SCT를 사용하여 애플리케이션에 포함된 SQL 코드를 변환할 수 있는 항목과 수동으로 수행해야 하는 작업을 식별합니다.

B. AWS SCT를 사용하여 스키마 스크립트를 생성하고 마이그레이션 전에 대상에 적용합니다. AWS DMS를 사용하여 온프레미스 데이터베이스에서 AWS로 데이터를 이동하기 시작합니다. 최초 복사 후 AWS DMS를 사용하여 새 데이터베이스로 전환할 때까지 데이터베이스 동기화를 유지합니다. AWS SCT를 사용하여 애플리케이션에 포함된 SOL 코드를 변환할 수 있는 항목과 수동으로 수행해야 하는 작업을 식별합니다.

C. AWS DMS를 사용하면 데이터베이스 엔진을 Amazon EC2에 직접 설치하거나 Amazon RDS로 이동하는 것 중에서 최적의 대상 배포를 식별할 수 있습니다. 그런 다음 AWS DMS를 사용하여 플랫폼으로 마이그레이션합니다. AWS 애플리케이션 검색 서비스를 사용하여 애플리케이션에 포함된 SQL 코드를 변환할 수 있는 항목과 수동으로 수행해야 하는 작업을 식별합니다.

D. AWS DMS를 사용하여 온프레미스 데이터베이스에서 AWS로 데이터 이동 시작 초기 복사 후 AWS DMS를 사용하여 새 데이터베이스로 전환할 때까지 계속해서 데이터베이스를 동기화 상태로 유지합니다. AWS Application Discovery Service를 사용하여 애플리케이션에 포함된 SQL 코드를 사용할 수 있는 항목과 사용해야 하는 요소를 파악합니다. 수동으로 할 수 있습니다.

Answer: B

Q155

한 회사가 전 세계 여러 지역에서 웹 기반 애플리케이션을 출시하고 있습니다. 애플리케이션은 프라이빗 Amazon S3 버킷에 저장된 정적 콘텐츠와 ALB (애플리케이션 로드 밸런서) 뒤에 있는 dyna ECS 컨테이너로 구성됩니다. 이 회사는 정적 및 동적 애플리케이션 콘텐츠에 Amazon CloudFront를 통해서만 액세스할 수 있어야 합니다.

CloudFront에 대한 직접 콘텐츠 액세스를 제한하기 위해 솔루션스 아키텍트가 권장하는 단계는 무엇입니까?(세 개 선택)

A. 사용자 지정 헤더가 있는지 확인하고 웹 ACL을 ALB와 연결하는 규칙을 사용하여 AWS WAF에서 웹 ACL을 생성합니다.

B. 사용자 지정 헤더가 있는지 확인하고 웹 ACL을 CloudFront 배포와 연결하는 규칙을 사용하여 AWS WAF에서 웹 ACL을 생성합니다.

C. 오리진 요청에 사용자 지정 헤더를 추가하도록 CloudFront를 구성합니다.

D. HTTP 요청에 사용자 지정 헤더를 추가하도록 ALB를 구성합니다.

E. CloudFront 배포에서만 액세스할 수 있도록 S3 버킷 ACL을 업데이트합니다.

F. CloudFront 오리진 액세스 ID (OAI) 를 생성하여 CloudFront 배포에 추가합니다. OAI에 대한 액세스만 허용하도록 S3 버킷 정책을 업데이트합니다.

Answer: B, C, F

설명

사용자 지정 출처를 사용하는 경우 선택적으로 사용자 지정 헤더를 설정하여 액세스를 제한할 수 있습니다. CloudFront가 사용자 지정 오리진에서 파일을 가져오려면 CloudFront에서 표준 HTTP(또는 HTTPS) 요청을 사용하여 파일에 액세스할 수 있어야 합니다.

사용자 지정 헤더를 사용하면 콘텐츠에 대한 액세스를 추가로 제한하여 사용자가 직접 액세스할 수 없고 CloudFront를 통해서만 액세스할 수 있도록 할 수 있습니다. 이 경우 AWS WAF 웹 ACL을 사용하여 요청을 필터링하고 사용자 지정 헤더가 있는지 확인할 수 있습니다.

Amazon S3의 경우 원본 액세스 ID(OAI)를 사용할 수 있습니다. OAI는 배포와 연결된 특별한 CloudFront 사용자입니다. OAI를 생성한 후 CloudFront에서 OAI를 사용하여 버킷의 파일에 액세스하고 이를 사용자에게 제공하고 다른 액세스를 제한할 수 있도록 S3 버킷 권한을 수정할 수 있습니다.

잘못됨: A. 웹 ACL은 CloudFront 배포가 아니라 ALB와 연결되어야 합니다.

잘못됨: D. ALB는 요청에 사용자 지정 헤더를 추가할 수 없습니다. 이 작업은 CloudFront에서 수행한 다음 ALB에 적용된 웹 ACL을 사용하여 유효성을 검사해야 합니다.

잘못됨: E. 이것은 최선의 해결책이 아닙니다(가능하지만). 시간이 지남에 따라 변경되는 CloudFront IP 주소보다 OAI를 사용하는 것이 관리상 더 쉽습니다.

참조:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-overview.html#forward-custom-headers-restrict-access

Q156

스타트업은 AWS 앱용 백업 솔루션의 아키텍처가 거의 완성되고 있습니다. 모든 앱은 AWS에서 호스팅되며 각 티어는 최소 2개의 가용 영역을 사용합니다.

IT는 회사 정책에 따라 운영 및 재해 복구라는 두 곳 이상의 위치에서 모든 데이터의 야간 백업을 유지 관리해야 합니다. 장소는 지리적으로 구분되어야 합니다. 또한 이 회사는 백업에 즉시 액세스하여 운영 데이터 센터에서, 재해 복구 사이트에서 24시간 이내에 복원할 수 있어야 합니다. 이상적으로는 모든 백업 작업을 완전히 자동화해야 합니다.

가장 비용 효율적이고 모든 요구 사항을 충족하는 백업 시스템은 무엇입니까?

A. 프로덕션 리전의 백업 미디어 서버에 연결된 대용량 Amazon EBS 볼륨에 모든 데이터를 백업합니다. 자동화된 스크립트를 실행하여 야간에 이러한 볼륨의 스냅샷을 생성하고 이러한 스냅샷을 재해 복구 리전에 복사합니다.

B. 재해 복구 리전의 Amazon S3에 모든 데이터를 백업합니다. 수명 주기 정책을 사용하여 이 데이터를 프로덕션 리전의 Amazon Glacier로 즉시 이동합니다. 데이터만 복제되므로 재해 복구 리전의 S3 버킷에서 데이터를 제거합니다.

C. 프로덕션 리전의 Amazon Glacier에 모든 데이터를 백업합니다. 재해 복구 리전의 Amazon Glacier로 이 데이터의 리전 간 복제를 설정합니다. 60일보다 오래된 데이터를 모두 삭제하도록 수명 주기 정책을 설정합니다.

D. 프로덕션 리전의 Amazon S3에 모든 데이터를 백업합니다. 이 S3 버킷의 리전 간 복제를 다른 리전으로 설정하고 두 번째 리전에 수명 주기 정책을 설정하여 이 데이터를 즉시 Amazon Glacier로 이동합니다.

Answer: D

Q157

한 기업이 기존 오케스트레이션 기술을 사용하여 수천 개의 Amazon EC2 인스턴스를 관리하고 있습니다. 최근 침투 테스트에서 조직의 소프트웨어 스택에서 약점이 발견되었습니다. 이러한 위험으로 인해 조직은 현재 제조 환경에 대한 종합적인 평가를 수행했습니다. 조사에 따르면 환경에 다음과 같은 취약점이 존재합니다.

\* 오래된 라이브러리와 알려진 취약점이 있는 운영 체제가 프로덕션에서 사용되고 있습니다.

\* 회사에서 호스팅하고 관리하는 관계형 데이터베이스는 알려진 취약점이 있는 지원되지 않는 버전을 실행하고 있습니다.

\* 데이터베이스에 저장된 데이터는 암호화되지 않습니다.

솔루션스 아키텍트는 AWS Config를 활용하여 AWS 리소스 설정에 대한 회사의 규칙 및 표준 준수 여부를 정기적으로 감사 및 분석하는 것을 목표로 합니다.

기업이 모범 사례를 준수하면서 주변 환경을 보호하고 리소스를 관리할 수 있는 추가 조치는 무엇입니까?

A. AWS 애플리케이션 검색 서비스를 사용하여 실행 중인 모든 EC2 인스턴스 평가 AWS CLI를 사용하여 각 인스턴스를 수정하고, EC2 사용자 데이터를 사용하여 부팅 중에 AWS Systems Manager 에이전트를 설치합니다. 패치가 시스템 관리자 유지 관리 Windows 작업으로 실행되도록 예약합니다. 모든 관계형 데이터베이스를 Amazon RDS로 마이그레이션하고 AWS KMS 암호화를 활성화합니다.

B. EC2 인스턴스용 AWS CloudFormation 템플릿을 생성합니다. CloudFormation 템플릿의 EC2 사용자 데이터를 사용하여 AWS 시스템 관리자 에이전트를 설치하고 모든 Amazon EBS 볼륨에서 AWS KMS 암호화를 활성화합니다. CloudFormation이 실행 중인 모든 인스턴스를 대체하게Systems Manager 패치 관리자를 사용하여 패치 기준을 설정하고 시스템 관리자 유지 관리 기간 작업을 배포하여 패치 기준선을 사용하여 AWS-RunPatchBaseline을 실행합니다.

C. 회사의 현재 오케스트레이션 도구를 사용하여 모든 기존 인스턴스에 AWS Systems Manager 에이전트를 설치합니다. Systems Manager Run Command를 사용하여 운영 체제별 도구를 사용하여 각 인스턴스에서 소프트웨어를 업그레이드하는 명령 목록을 실행합니다. 모든 Amazon EBS 볼륨에서 AWS KMS 암호화를 활성화합니다.

D. 회사의 현재 오케스트레이션 도구를 사용하여 모든 기존 인스턴스에 AWS Systems Manager 에이전트를 설치합니다. 모든 관계형 데이터베이스를 Amazon RDS로 마이그레이션하고 AWS KMS 암호화를 활성화합니다. Systems Manager 패치 관리자를 사용하여 패치 기준을 설정하고 시스템 관리자 유지 관리 기간 작업을 배포하여 패치 기준선을 사용하여 AWS-RunPatchBaseline을 실행합니다.

Answer: D

Q158

대규모 다국적 기업이 AWS에서 전 세계 직원이 사용하는 작업표 애플리케이션을 실행합니다. 애플리케이션은 Elastic Load Balancing (ELB) 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 실행되며 Amazon RDS MySQL 다중 AZ 데이터베이스 인스턴스에 데이터를 저장합니다. CFO는 애플리케이션을 사용할 수 없는 경우 비즈니스에 미치는 영향에 대해 우려하고 있습니다. 애플리케이션을 2시간 이상 중단해서는 안 되지만 솔루션은 가능한 한 비용 효율적이어야 합니다.

솔루션 설계자는 데이터 손실을 최소화하면서 CFO의 요구 사항을 어떻게 충족해야 합니까?

A. 다른 리전에서는 읽기 전용 복제본을 구성하고 인프라의 복사본을 생성합니다. 문제가 발생하면 읽기 전용 복제본을 승격하고 Amazon RDS 다중 AZ 데이터베이스 인스턴스로 구성합니다. 다른 리전의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

B. Amazon RDS 다중 AZ 데이터베이스 인스턴스의 60분 스냅샷으로 구성된 1일 창을 구성합니다. 최신 스냅샷을 사용하는 애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다. 문제가 발생하면 AWS CloudFormation 템플릿을 사용하여 다른 리전에 환경을 생성합니다. 다른 리전의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

C. 다른 리전으로 복사되는 Amazon RDS 다중 AZ 데이터베이스 인스턴스의 60분 스냅샷으로 구성된 1일 창을 구성합니다. 복사된 최신 스냅샷을 사용하는 애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다. 문제가 발생하면 AWS CloudFormation 템플릿을 사용하여 다른 리전에 환경을 생성합니다. 다른 리전의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

D. 다른 리전에서 읽기 전용 복제본을 구성합니다. 애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다.문제가 발생하면 읽기 전용 복제본을 승격하고 Amazon RDS 다중 AZ 데이터베이스 인스턴스로 구성한 다음 AWS CloudFormation 템플릿을 사용하여 승격된 Amazon RDS 인스턴스를 사용하여 다른 리전에 환경을 만듭니다. 다른 리전의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

Answer: D

Q159

한 회사에 Amazon EC2 오토 스케일링 그룹의 Amazon EC2 인스턴스에서 실행되는 애플리케이션이 있습니다. 이 회사는 AWS CodePipeline을 사용하여 애플리케이션을 배포합니다. Auto Scaling 그룹에서 실행되는 인스턴스는 조정 이벤트로 인해 지속적으로 변경됩니다. 회사에서 새 애플리케이션 코드 버전을 배포할 때 회사는 새로운 대상 EC2 인스턴스에 AWS CodeDeploy 에이전트를 설치하고 해당 인스턴스를 CodeDeploy 배포 그룹에 연결합니다. 애플리케이션은 다음 24시간 내에 실행되도록 설정되어 있습니다.

솔루션 설계자는 최소한의 운영 오버헤드로 애플리케이션 배포 프로세스를 자동화하기 위해 무엇을 권장해야 합니까?

A. 새 EC2 인스턴스가 오토 스케일링 그룹으로 시작될 때 AWS Lambda 함수를 호출하도록 Amazon EventBridge (Amazon CloudWatch Events) 를 구성합니다. Lambda 함수를 코딩하여 EC2 인스턴스를 CodeDeploy 배포 그룹과 연결합니다.

B. 새 코드를 배포하기 전에 Amazon EC2 Auto Scaling 작업을 일시 중단하는 스크립트를 작성합니다. 배포가 완료되면 새 AMI를 생성하고 새로운 시작에 새 AMI를 사용하도록 Auto Scaling 그룹의 시작 템플릿을 구성합니다.Amazon EC2 오토 스케일링 작업 재개

C. 새 코드가 포함된 새 AMI를 생성하는 새 AWS CodeBuild 프로젝트를 생성합니다. Auto Scaling 그룹의 시작 템플릿을 새 AMI로 업데이트하도록 CodeBuild를 구성합니다. Amazon EC2 자동 조정 인스턴스 새로 고침 작업을 실행합니다.

D. CodeDeploy 에이전트가 설치된 새 AMI를 생성합니다. 새 AMI를 사용하도록 Auto Scaling 그룹의 시작 템플릿을 구성합니다. CodeDeploy 배포 그룹을 EC2 인스턴스 대신 오토 스케일링 그룹과 연결합니다.

Answer: C

Q160

한 회사가 각 엔지니어링 팀을 위해 AWS Organizations에서 OU를 생성했습니다. 각 OU는 여러 AWS 계정을 소유합니다. 이 조직에는 수백 개의 AWS 계정이 있습니다. 솔루션 설계자는 각 OU가 AWS 계정 전체의 사용 비용 내역을 볼 수 있도록 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 리소스 액세스 관리자를 사용하여 각 OU에 대한 AWS 비용 및 사용 보고서 (CUR) 를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.

B. AWS 조직 관리 계정에서 AWS 비용 및 사용 보고서 (CUR) 를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.

C. 각 AWS 조직 멤버 계정에서 AWS 비용 및 사용 보고서 (CUR) 를 생성합니다. 각 팀이 Amazon QuickSight 대시보드를 통해 CUR을 시각화할 수 있도록 허용합니다.

D. AWS 시스템 관리자를 사용하여 AWS 비용 및 사용 보고서 (CUR) 를 생성합니다. 각 팀이 시스템 관리자 OpsCenter 대시보드를 통해 CUR을 시각화할 수 있습니다.

Answer: B

Q161

한 회사가 온프레미스 시스템에서 Amazon S3 버킷으로 데이터를 전송하려고 합니다. 이 회사는 세 개의 서로 다른 계정에 S3 버킷을 만들었습니다. 회사는 인터넷을 통해 데이터를 이동하지 않고 데이터를 비공개로 전송해야 합니다. 이 회사에는 AWS에 대한 기존 전용 연결이 없습니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(두 개 선택)

A. AWS 클라우드에서 네트워킹 계정 설정 네트워킹 계정에 프라이빗 VPC를 생성합니다. 온프레미스 환경과 프라이빗 VPC 간에 프라이빗 VIF로 AWS Direct Connect 연결을 설정합니다.

B. AWS 클라우드에서 네트워킹 계정 설정 네트워킹 계정에 프라이빗 VPC를 생성합니다. 온프레미스 환경과 프라이빗 VPC 간에 퍼블릭 VIF로 AWS Direct Connect 연결을 설정합니다.

C. 네트워킹 계정에 Amazon S3 인터페이스 엔드포인트를 생성합니다.

D. 네트워킹 계정에 Amazon S3 게이트웨이 엔드포인트를 생성합니다.

E. AWS 클라우드에서 네트워킹 계정을 설정합니다. 네트워킹 계정에 프라이빗 VPC를 생성합니다. 네트워크 계정의 VPC로 S3 버킷을 호스팅하는 계정의 VPC를 피어링합니다..

Answer: A, D

Q162

한 회사가 온프레미스 데이터 센터에서 2계층 웹 기반 애플리케이션을 실행하고 있습니다. 애플리케이션 계층은 상태 저장 애플리케이션을 실행하는 단일 서버로 구성됩니다.응용 프로그램은 별도의 서버에서 실행되는 PostgreSQL 데이터베이스에 연결됩니다. 애플리케이션의 사용자 기반이 크게 증가할 것으로 예상되므로 이 회사는 애플리케이션과 데이터베이스를 AWS로 마이그레이션하고 있습니다. 이 솔루션은 AmazonAurora 포스트그레SQL, Amazon EC2 오토 스케일링, 탄력적 로드 밸런싱을 사용합니다.

애플리케이션 및 데이터베이스 계층을 확장할 수 있는 일관된 사용자 환경을 제공하는 솔루션은 무엇입니까?

A. Aurora 복제본에 대해 Aurora자동 스케일링을 활성화합니다. 최소 미결 요청 라우팅 알고리즘과 고정 세션을 사용하도록 설정한 네트워크 로드 밸런서를 사용합니다.

B. Aurora 쓰기에 대해 Aurora자동 스케일링을 활성화합니다. 라운드 로빈 라우팅 알고리즘과 고정 세션을 사용하도록 설정한 애플리케이션 로드 밸런서를 사용합니다.

C. Aurora 복제본에 대해 Aurora자동 스케일링을 활성화합니다. 로빈 라우팅 및 상태별 세션을 사용하도록 설정한 상태에서 애플리케이션 로드 밸런서를 사용합니다.

D. Aurora 작성자에 위해 Aurora스케일링을 활성화합니다. 최소 미결 요청 라우팅 알고리즘과 고정 세션을 사용하도록 설정한 네트워크 로드 밸런서를 사용합니다.

Answer: C

설명

Aurora Auto Scaling은 단일 마스터 복제를 사용하여 Aurora DB 클러스터에 프로비저닝된 Aurora 복제본 수를 동적으로 조정합니다. 조정 정책을 정의하고 Aurora DB 클러스터에 적용합니다.

조정 정책은 Aurora Auto Scaling에서 관리할 수 있는 Aurora 복제본의 최소 및 최대 수를 정의합니다. 정책에 따라 Aurora Auto Scaling은 Amazon CloudWatch 지표 및 대상 값을 사용하여 결정된 실제 워크로드에 따라 Aurora 복제본 수를 늘리거나 줄입니다.

기본적으로 라운드 로빈 라우팅 알고리즘은 대상 그룹 수준에서 요청을 라우팅하는 데 사용됩니다. 대신 최소 미해결 요청 라우팅 알고리즘을 지정할 수 있습니다.

애플리케이션에 대한 요청의 복잡성이 다양하거나 대상의 처리 능력이 다를 때 미해결 요청을 가장 적게 사용하는 것을 고려하십시오. 라운드 로빈은 요청과 대상이 유사하거나 요청을 대상 간에 균등하게 분배해야 하는 경우에 좋은 선택입니다.

이 경우 인스턴스가 동일한 처리 기능을 가지며 요청이 인스턴스 간에 고르게 라우팅되어야 하므로 라운드 로빈 알고리즘이 최선의 선택이 될 것입니다.

Aurora Auto Scaling을 사용하면 Aurora DB 클러스터가 연결 또는 워크로드의 급격한 증가를 처리할 수 있습니다. 연결 또는 워크로드가 감소하면 Aurora Auto Scaling에서 불필요한 Aurora 복제본을 제거하여 사용하지 않은 프로비저닝된 DB 인스턴스에 대해 비용을 지불하지 않습니다.

잘못됨: A. 최소 미해결 요청 알고리즘은 위에서 설명한 것처럼 여기에서 최선의 선택이 아닙니다.

잘못됨: D. NLB는 이 알고리즘을 사용하지 않고 흐름 해시 알고리즘을 사용합니다.

참조:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScaling.html

Q163

회사에는 사용자가 짧은 비디오를 업로드 할 수있는 웹 애플리케이션이 있습니다. 비디오는 Amazon EBS 볼륨에 저장되고 분류를 위해 사용자 지정 인식 소프트웨어로 분석됩니다. 웹 사이트에는 특정 달에 트래픽이 가장 많은 정적 콘텐츠가 포함되어 있습니다. 아키텍처는 웹 애플리케이션용 Auto Scaling 그룹에서 실행되는 Amazon EC2 인스턴스와 Amazon SQS 대기열을 처리하기 위해 Auto Scaling 그룹에서 실행되는 EC2 인스턴스로 구성됩니다. 이 회사는 가능한 경우 AWS 관리형 서비스를 사용하여 운영 오버헤드를 줄이고 타사 소프트웨어에 대한 종속성을 제거하도록 애플리케이션을 재설계하려고 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 웹 애플리케이션에는 Amazon ECS 컨테이너를 사용하고 SQS 대기열을 처리하는 Auto Scaling 그룹에는 스팟 인스턴스를 사용합니다. 사용자 지정 소프트웨어를 Amazon 인식(Amazon Rekognition)으로 교체하여 비디오를 분류합니다.

B. 업로드된 비디오를 Amazon EFS에 저장하고 파일 시스템을 웹 애플리케이션용 EC2 인스턴스에 마운트합니다. 동영상을 분류하기 위해 Amazon Rekognition API를 호출하는 AWS Lambda 함수로 SQS 대기열을 처리합니다.

C. Amazon S3에서 웹 애플리케이션을 호스팅합니다. 업로드한 비디오를 Amazon S3에 저장합니다.S3 이벤트 알림을 사용하여 SQS 대기열에 이벤트 게시 비디오를 분류하기 위해 Amazon Rekognition API를 호출하는 AWS Lambda 함수로 SQS 대기열을 처리합니다.

D. AWS Elastic Beanstalk를 사용하여 웹 애플리케이션용 Auto Scaling 그룹에서 EC2 인스턴스를 시작하고 작업자 환경을 시작하여 SQS 대기열을 처리합니다. 사용자 지정 소프트웨어를 Amazon Rekognition으로 교체하여 비디오를 분류합니다.

Answer: C

설명

정적 웹 사이트의 경우 Amazon S3 버킷을 사용할 수 있습니다. 그러면 S3 이벤트 알림은 동영상이 버킷에 업로드될 때마다 Lambda 함수 호출을 트리거할 수 있습니다. 그러면 Lambda 함수가 이미지를 처리하고 Rekognition API를 호출하여 얼굴 분석을 수행할 수 있습니다. 이 솔루션은 관리형 AWS 서비스를 사용하며 운영 오버헤드를 줄입니다.

잘못됨: A. Lambda는 임시 작업에 ECS보다 더 적합합니다. 또한 맞춤형 인식 소프트웨어는 aws 관리형 서비스인 Rekognition으로 교체할 수 있습니다.

잘못됨: B. EC2 및 EFS보다 Lambda 및 S3를 사용하는 것이 운영상 더 효율적입니다.

참조:

https://aws.amazon.com/rekognition/

https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

Q164

한 회사에서 Amazon EC2 인스턴스에서 Apache 하둡 클러스터를 실행하고 있습니다. 하둡 클러스터는 주간 운영 보고서를 위해 약 100TB의 데이터를 저장하고 데이터 과학자가 데이터를 검색하기 위해 가끔 액세스할 수 있도록 합니다. 회사는 이 데이터를 저장하고 제공하는 데 드는 비용과 운영 복잡성을 줄여야 합니다.

가장 비용 효율적인 방식으로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 하둡 클러스터를 EC2 인스턴스에서 Amazon EMR로 이동합니다. 데이터 액세스 패턴을 동일하게 유지할 수 있습니다.

B. 가동 중지 시간 동안 EC2 인스턴스의 크기를 더 작은 인스턴스 유형으로 조정하고 보고서를 생성하기 전에 인스턴스의 크기를 더 큰 인스턴스 유형으로 조정하는 스크립트를 작성합니다.

C. 데이터를 Amazon S3로 이동하고 Amazon Athena를 사용하여 보고서에 대한 데이터를 쿼리합니다. 데이터 과학자가 Amazon S3에서 직접 데이터에 액세스할 수 있도록 허용합니다.

D. 데이터를 Amazon DynamoDB로 마이그레이션하고 보고서를 수정하여 DynamoDB에서 데이터를 가져옵니다. 데이터 과학자가 DynamoDB에서 직접 데이터에 액세스할 수 있도록 허용합니다.

Answer: C

Q165

한 회사에는 메시지 큐 원격 분석 전송 (MQTT: Message Queuing Telemetry Transport) 프로토콜을 사용하여 온-프레미스 Apache Kafka 서버로 데이터를 전송하는 센서가 10.000개 이상 있습니다. 온프레미스 Kafka 서버는 데이터를 변환한 다음 그 결과를 Amazon S3 버킷에 객체로 저장합니다. 최근 Kafka 서버가 충돌했습니다. 서버가 복원되는 동안 회사는 센서 데이터를 잃었습니다. 솔루션스 아키텍트는 유사한 발생을 방지하기 위해 가용성과 확장성이 뛰어난 새로운 디자인을 AWS에서 생성해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 두 개의 Amazon EC2 인스턴스를 시작하여 두 가용 영역에 걸쳐 활성/대기 구성으로 Kafka 서버를 호스팅합니다. Amazon Route 53에서 도메인 이름을 생성합니다. Route 53 장애 조치 정책 생성 데이터를 도메인 이름으로 전송하도록 센서를 라우팅합니다.

B. 온프레미스 Kafka 서버를 Amazon Managed Streaming for Apache Kafka(Amazon MSK)로 마이그레이션합니다. Amazon MSK 브로커를 가리키는 NLB(Network Load Balancer)를 생성합니다. NLB 상태 확인 사용 데이터를 NLB로 보내도록 센서를 라우팅합니다.

C. AWS loT Core를 배포하고 이를 Amazon 키네시스 데이터 파이어호스 전송 스트림에 연결합니다. AWS Lambda 함수를 사용하여 데이터 변환 처리 센서를 라우팅하여 데이터를 AWS loT Core로 전송합니다.

D. AWS 로트 코어를 배포하고 카프카 서버를 호스팅할 Amazon EC2 인스턴스를 시작합니다. 데이터를 EC2 인스턴스로 전송하도록 AWS LoT Core 구성 데이터를 AWS IoT Core로 전송하도록 센서를 라우팅합니다.

Answer: A

Q166

AWS에서 기업은 IoT 플랫폼을 호스팅합니다.기업 주변에 위치한 IoT 센서는 애플리케이션 로드 밸런서 뒤의 Amazon EC2 인스턴스에서 호스팅되는 회사의 Node.js API 서버로 데이터를 전송합니다. 데이터는 Amazon RDS MySQL DB 인스턴스의 4TB 범용 SSD 디스크에 저장됩니다.

회사가 현장에 배치 한 센서의 수는 시간이 지남에 따라 증가했으며 계속해서 급격히 확장 될 것으로 보입니다. API 서버는 항상 과밀하며 RDS 측정 결과는 쓰기 지연 시간이 길다는 것을 나타냅니다.

다음 중 플랫폼의 비용 효율성을 유지하면서 추가 센서가 제공됨에 따라 어려움을 영구적으로 치료하고 향후 확장을 허용하는 변경 사항은 무엇입니까?(두 개 선택)

A. MySQL 범용 SSD 스토리지의 크기를 6TB로 조정하여 볼륨의 IOPS를 개선합니다.

B. RDS MySQL DB 인스턴스 대신 Amazon Aurora를 사용하도록 데이터베이스 계층을 재설계하고 읽기 전용 복제본을 추가합니다.

C. Amazon Kinesis 데이터 스트림과 AWS Lambda를 활용하여 원시 데이터를 수집하고 처리합니다.

D. AWS-X-ray를 사용하여 애플리케이션 문제를 분석 및 디버깅하고 부하에 맞게 API 서버를 더 추가합니다.

E. RDS MySQL DB 인스턴스 대신 Amazon DynamoDB를 사용하도록 데이터베이스 계층을 다시 설계합니다.

Answer: C, E

Q167

한 회사에서 단일 공유 VPC에서 호스팅되는 중앙 집중식 Amazon EC2 애플리케이션을 제공합니다. 중앙 집중식 애플리케이션은 다른 사업부의 VPC에서 실행되는 클라이언트 애플리케이션에서 액세스할 수 있어야 합니다. 중앙 집중식 응용 프로그램 프런트 엔드는 확장성을 위해 NLB (네트워크 부하 분산 장치) 로 구성됩니다.최대 10개의 사업부 VPC를 공유 VPC에 연결해야 합니다. 비즈니스 단위 VPC CIDR 블록 중 일부는 공유 VPC와 겹치고 일부는 서로 겹칩니다. 공유 VPC의 중앙 집중식 애플리케이션에 대한 네트워크 연결은 승인된 사업부 VPC에서만 허용되어야 합니다.

솔루션 설계자가 사업부 VPC의 클라이언트 애플리케이션에서 공유 VPC의 중앙 집중식 애플리케이션으로 연결을 제공하기 위해 사용해야 하는 네트워크 구성은 무엇입니까?

A. AWS 전송 게이트웨이를 생성합니다. 공유 VPC와 승인된 사업부 VPC를 전송 게이트웨이에 연결합니다. 단일 전송 게이트웨이 라우팅 테이블을 생성하여 연결된 모든 VPC와 연결합니다. 첨부 파일에서 라우팅 테이블로 경로를 자동으로 전파할 수 있습니다. 전송 게이트웨이로 트래픽을 전송하도록 VPC 라우팅 테이블 구성

B. 중앙 집중식 애플리케이션 NLB를 사용하여 VPC 엔드포인트 서비스를 생성하고 엔드포인트 수락을 요구하는 옵션을 활성화합니다. 엔드포인트 서비스의 서비스 이름을 사용하여 각 사업부 VPC에 VPC 엔드포인트를 생성합니다. 엔드포인트 서비스 콘솔에서 승인된 엔드포인트 요청을 수락합니다.

C. 각 사업부 VPC에서 공유 VPC로의 VPC 피어링 연결을 생성합니다. 공유 VPC 콘솔에서 VPC 피어링 연결을 수락합니다. VPC 피어링 연결로 트래픽을 전송하도록 VPC 라우팅 테이블을 구성합니다.

D. 공유 VPC에 대한 가상 프라이빗 게이트웨이를 구성하고 승인된 각 사업부 VPC에 대한 고객 게이트웨이를 생성합니다. 사업부 VPC에서 공유 VPC로 사이트 간 VPN 연결을 설정합니다. VPN 연결로 트래픽을 전송하도록 VPC 라우팅 테이블을 구성합니다.

Answer: B

Q168

기업이 온프레미스 데이터 센터에서 실행되는 VMware 인프라에서 Amazon EC2로 애플리케이션을 이전하고자 합니다. 마이그레이션하는 동안 솔루션 설계자는 소프트웨어 및 구성 설정을 유지해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. Windows 파일 서버용 Amazon FSx에 데이터 스토어를 복제하기 시작하도록 AWS DataSync 에이전트를 구성합니다. SMB 공유를 사용하여 VMware 데이터 저장소를 호스팅합니다. VM 가져오기/내보내기를 사용하여 VM을 Amazon EC2로 이동합니다.

B. VMware vSphere 클라이언트를 사용하여 애플리케이션을 OVF (개방형 가상화 형식) 형식의 이미지로 내보냅니다. Amazon S3 버킷을 생성하여 대상 AWS 리전에 이미지를 저장합니다. VM 가져오기를 위한 IAM 역할을 생성하고 적용합니다.AWS CLI를 사용하여 EC2 가져오기 명령을 실행합니다.

C. 공통 인터넷 파일 시스템 (CIFS) 공유를 내보내도록 파일 서비스용 AWS 스토리지 게이트웨이를 구성합니다. 공유 폴더에 백업 복사본을 만듭니다. AWS 관리 콘솔에 로그인하고 백업 사본에서 AMI를 생성합니다. AMI를 기반으로 하는 EC2 인스턴스를 시작합니다.

D. AWS Systems Manager에서 하이브리드 환경에 대한 관리형 인스턴스 활성화를 생성합니다. 온프레미스 VM에 시스템 관리자 에이전트를 다운로드하여 설치합니다. 시스템 관리자에 VM을 등록하여 관리형 인스턴스로 만듭니다. AWS 백업을 사용하여 VM의 스냅샷을 생성하고 AMI를 생성합니다. AMI를 기반으로 하는 EC2 인스턴스를 시작합니다.

Answer: B

Q169

한 회사에서 여러 AWS 계정을 사용하고 있습니다. DNS 레코드는 계정 A의 Amazon Route 53에 대한 프라이빗 호스팅 영역에 저장됩니다. 이 회사의 애플리케이션과 데이터베이스는 계정 B에서 실행되고 있습니다. 솔루션 설계자는 2계층 애플리케이션을 배포합니다. 구성을 간소화하기 위해 새 VPC에서 Amazon RDS용 db.example com CNAME 레코드 세트엔드포인트가 Amazon Route 53용 프라이빗 호스팅 영역에 생성되었습니다. 배포 중에 응용 프로그램을 시작하지 못했습니다. 문제 해결 결과 Amazon EC2 인스턴스에서 db.example com을 확인할 수 없는 것으로 나타났습니다. 솔루션 설계자는 Route 53에서 레코드 세트가 올바르게 생성되었음을 확인했습니다.

이 문제를 해결하기 위해 솔루션 설계자가 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. 새 VPC의 별도 EC2 인스턴스에 데이터베이스 배포 프라이빗 호스팅 영역에서 인스턴스의 프라이빗 IP에 대한 레코드 세트를 생성합니다.

B. SSH를 사용하여 애플리케이션 티어 EC2 인스턴스에 연결합니다. /eto/resolv 구성 파일에 RDS 엔드포인트 IP 주소를 추가합니다.

C. 권한 부여를 생성하여 계정 A의 프라이빗 호스팅 영역을 계정 B의 새 VPC와 연결합니다.

D. example.com 도메인 m 계정 B에 대한 프라이빗 호스팅 영역을 생성합니다. AWS 계정 간에 Route 53 복제를 구성합니다.

E. 계정 B의 새 VPC를 계정 A의 호스팅 영역과 연결합니다. 계정 A에서 연결 권한 삭제

Answer: C, E

설명

애플리케이션은 다른 AWS 계정의 프라이빗 호스팅 영역에서 생성된 레코드 세트를 확인할 수 없습니다. 이 문제에 대한 해결책은 관리 계정의 Route 53 프라이빗 호스팅 영역을 프로덕션 계정의 VPC와 연결하는 것입니다.

한 AWS 계정(계정 A)의 Route 53 프라이빗 호스팅 영역을 다른 AWS 계정(계정 B)에 속한 가상 프라이빗 클라우드와 연결하려면 AWS CLI를 사용하여 다음 단계를 따르십시오.

1. 계정 A의 인스턴스에서 계정 A의 프라이빗 호스팅 영역과 계정 B의 가상 프라이빗 클라우드 간의 연결을 승인합니다.

2. 계정 B의 인스턴스에서 계정 A의 프라이빗 호스팅 영역과 계정 B의 가상 프라이빗 클라우드 간의 연결을 생성합니다.

3. 연결이 생성된 후 연결 권한을 삭제합니다.

잘못됨: A. 레코드는 개인 IP 주소가 아니라 RDS 데이터베이스의 DNS 엔드포인트를 가리키는 CNAME 레코드여야 합니다.

잘못됨: B. 이것은 RDS 인스턴스의 IP 주소를 사용해서는 안 되며 DNS 엔드포인트를 가리키는 CNAME이 선호되기 때문에 모범 사례가 아닙니다.

잘못됨: D. Route 53에서는 호스팅 영역에 대한 복제를 구성할 수 없습니다.

참조:

https://aws.amazon.com/premiumsupport/knowledge-center/private-hosted-zone-different-account/

Q170

한 회사가 글로벌 멀티 플레이어 게임 플랫폼을 구현했습니다. 이 플랫폼을 사용하려면 게임 클라이언트가 단일 AWS 리전의 Amazon EC2 인스턴스 플릿에서 호스팅되는 서버 인프라에 안정적이고 지연 시간이 짧은 액세스가 필요합니다. 게임 클라이언트는 사용자 지정 TCP 프로토콜을 사용하여 서버 인프라에 연결합니다. 애플리케이션 아키텍처에서는 서버 소프트웨어에서 클라이언트 IP 주소를 사용할 수 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Network Load Balancer (NLB) 를 생성하고 EC2 인스턴스를 대상 그룹에 추가합니다. Amazon CloudFront Real Time Messaging Protocol (RTMP: 실시간 메시징 프로토콜) 배포를 생성하고 NLB의 DNS 엔드포인트를 가리키도록 오리진을 구성합니다. 프록시 프로토콜 버전 2 헤더를 사용하여 클라이언트 IP 주소를 보존합니다.

B. AWS Direct Connect 게이트웨이를 사용하여 전 세계 여러 리전에 있는 여러 Direct Connect 위치를 연결합니다. 지리적 위치 라우팅으로 Amazon Route 53을 구성하여 가장 가까운 직접 연결 위치로 트래픽을 전송합니다. EC2 인스턴스가 포함된 VPC를 직접 연결 게이트웨이와 연결합니다.

C. AWS Global Accelerator에서 액셀러레이터를 생성하고 단일 엔드포인트 그룹을 가리키도록 리스너를 구성합니다. 각 EC2 인스턴스를 엔드포인트 그룹에 엔드포인트로 추가 모든 EC2 엔드포인트에서 엔드포인트 그룹 가중치를 동일하게 구성합니다.

D. Application Load Balancer (ALB) 를 생성하고 EC2 인스턴스를 대상 그룹에 추가합니다. ALB의 DNS 엔드포인트를 가리키는 Amazon Route 53 지연 시간 기반 별칭 레코드 세트를 생성합니다.

Answer: B

Q171

한 회사가 인기있는 온라인 게임의 속편을 만들고 있습니다.전 세계의 많은 사용자가 출시 후 첫 주 이내에 게임을 플레이합니다.현재 이 게임은 단일 AWS 리전에 배포된 다음 구성 요소로 구성되어 있습니다.

\* 게임 자산을 저장하는 Amazon S3 버킷

\* 플레이어 점수를 저장하는 Amazon DynamoDB 테이블

솔루션 설계자는 wifi가 지연 시간을 줄이고 안정성을 개선하며 구현하는 데 최소한의 노력으로 지역 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. Amazon CloudFront 배포를 생성하여 S3 버킷의 자산을 처리합니다. S3 교차 리전 복제 구성 새 리전에 새 DynamoDB 테이블 생성 DynamoDB 글로벌 테이블의 복제본 대상으로 새 테이블을 사용합니다.

B. Amazon CloudFront 배포를 생성하여 S3 버킷의 자산을 제공합니다. S3 동일 리전 복제를 구성합니다.새 리전에 새 DynamoDB 테이블을 생성합니다. 변경 데이터 캡처 (CDC: change data capture) 와 함께 AWS Database Migration Service (AWS DMS) 를 사용하여 DynamoDB 테이블 간에 비동기 복제를 구성합니다.

C. 새 리전에 다른 S3 버킷을 생성하고 버킷 간에 S3 교차 리전 복제를 구성합니다. Amazon CloudFront 배포를 생성하고 각 리전의 S3 버킷에 액세스하는 두 오리진으로 오리진 장애 조치를 구성합니다. Amazon DynamoDB 스트림을 활성화하여 DynamoDB 글로벌 테이블을 구성하고 새 리전에 복제본 테이블을 추가합니다.

D. 동일한 리전에 다른 S3 버킷을 생성하고 버킷 간에 S3 동일 리전 복제 구성- Amazon CloudFront 배포를 생성하고 두 오리진이 S3 버킷에 액세스하도록 오리진 장애 조치를 구성합니다. 새 리전에 새 DynamoDB 테이블 생성 새 테이블을 다음에 대한 복제본 대상으로 사용DynamoDB 글로벌 테이블입니다.

Answer: C

Q172

한 회사가 단일 지리적 리전의 사용자에게 피아트 서비스를 제공하는 애플리케이션 워크로드를 지원하기 위해 다중 계정 AWS 환경에 대한 연결을 구성하고 있습니다. 워크로드는 두 위치에 배포된 고가용성 온프레미스 레거시 시스템에 의존합니다. AWS 워크로드가 레거시 시스템에 대한 연결을 마니아하는 것이 중요하며 최소 5Gbps의 대역폭이 필요합니다. AWS 내의 모든 애플리케이션 워크로드는 서로 연결되어 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 온프레미스 위치별로 DX 파트너로부터 여러 개의 AWS Direct Connect (DX) 10Gbps 전용 연결을 구성합니다. 각 AWS 계정의 각 연결에 프라이빗 가상 인터페이스를 생성합니다. VPC 각 VPC에 연결된 가상 프라이빗 게이트웨이와 프라이빗 가상 인터페이스를 연결합니다.

B. 온프레미스 위치별로 두 개의 DX 파트너로부터 여러 개의 AWS Direct Connect (DX) 10Gbps 전용 연결을 구성합니다. 각 AWS 계정 VPC에 대해 가상 프라이빗 게이트웨이를 생성하고 연결합니다. 중앙 네트워크 계정인 DX 게이트웨이를 생성하여 가상 프라이빗 게이트웨이와 연결합니다. 각 DX 연결에 공용 가상 인터페이스를 만들고 인터페이스를 DX 게이트웨이와 연결합니다.

C. 온프레미스 위치별로 2개의 DX 파트너로부터 여러 개의 AWS Direct Connect (DX) 10Gbps 전용 연결을 구성합니다. 중앙 네트워크 계정에 전송 게이트웨이와 DX 게이트웨이를 생성합니다. 각 DX 인터레이스에 대한 전송 가상 인터페이스를 생성하여 DX 게이트웨이와 연결합니다. DX 게이트웨이와 전송 게이트웨이 간에 게이트웨이 연결을 생성합니다.

D. 온프레미스 위치별로 DX 파트너로부터 여러 개의 AWS Direct Connect (DX) 10Gbps 전용 연결을 구성합니다. 각 AWS 계정 VPC에 대해 가상 프라이빗 게이트웨이를 생성하고 연결합니다. 중앙 네트워크 계정에 전송 게이트웨이를 만들고 이를 가상 프라이빗 게이트웨이와 연결합니다. 각 DX 연결에 전송 가상 인터페이스를 만들고 인터페이스를 전송 게이트웨이에 연결합니다.

Answer: C

Q173

회사의 AWS 아키텍처는 현재 각 인스턴스에 저장된 액세스 키와 보안 액세스 키를 사용하여 AWS 서비스에 액세스합니다. 데이터베이스 자격 증명은 각 인스턴스에서 하드 코딩됩니다. 명령줄 원격 액세스를 위한 SSH 키는 보안 Amazon S3 버킷에 저장됩니다. 이 회사는 솔루션 설계자에게 운영을 복잡하게 추가하지 않고 아키텍처의 보안 상태를 개선하도록 요청했습니다.

솔루션 설계자는 이 작업을 수행하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. IAM 역할과 함께 Amazon EC2 인스턴스 프로필을 사용합니다.

B. AWS 보안 관리자를 사용하여 액세스 키와 보안 액세스 키를 저장합니다.

C. AWS Systems Manager 파라미터 스토어를 사용하여 데이터베이스 자격 증명을 저장합니다.

D. 원격 액세스를 위해 안전한 Amazon EC2 배스천 호스트 플릿을 사용합니다.

E. AWS KMS를 사용하여 데이터베이스 자격 증명을 저장합니다.

F. 원격 액세스를 위해 AWS 시스템 관리자 세션 관리자를 사용합니다.

Answer: A, C, F

Q174

온라인 전자 상거래 비즈니스가 AWS에서 워크로드를 실행하고 있습니다. 애플리케이션 아키텍처는 웹 티어, 비즈니스 로직을 위한 애플리케이션 티어, 사용자 및 트랜잭션 데이터 관리를 위한 데이터베이스 티어를 포함한다. 데이터베이스 서버의 메모리 요구 사항은 100GB입니다. 비즈니스에는 RTO가 5분이고 RPO가 1시간인 애플리케이션에 대해 비용 효율적인 재해 복구가 필요합니다. 또한 이 비즈니스는 기본 사이트와 대체 사이트 간의 최소 거리가 250마일인 지역 외 재해 복구에 대한 규제 요구 사항을 가지고 있습니다.

다음 중 이 고객을 위해 재해 복구 요구 사항을 충족하는 포괄적인 솔루션을 만들기 위해 솔루션 설계자가 설계할 수 있는 옵션은 무엇입니까?

A. 애플리케이션 및 데이터베이스 데이터를 자주 백업하고 Amazon S3에 복사합니다. S3 교차 리전 복제를 사용하여 백업을 복제하고, AWS Cloud Formation을 사용하여 재해 복구를 위한 인프라를 인스턴스화하고 Amazon S3에서 데이터를 복원합니다.

B. 기본 데이터베이스가 미러링으로 구성된 파일럿 라이트 환경을 사용하여 대체 리전의 m4.large에 대기 데이터베이스를 구축합니다. 재해 발생 시 AWS Cloud Formation을 사용하여 웹 서버, 애플리케이션 서버 및 로드 밸런서를 인스턴스화하여 대체 리전에 애플리케이션을 가동할 수 있습니다. 전체 프로덕션 수요를 충족하도록 데이터베이스의 크기를 세로로 조정하고 Amazon Route 53을 사용하여 트래픽을 대체 리전으로 전환합니다.

C. 웹 서버 인스턴스 1개, 애플리케이션 서버 인스턴스 1개 및 대기 모드의 데이터베이스 서버 복제된 인스턴스를 포함하는 대체 리전에서 전체 기능을 갖춘 운용 환경의 축소 버전을 사용합니다. 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 웹 및 애플리케이션 계층을 배치합니다. 그러면 로드가 애플리케이션에 도달하면 자동으로 조정됩니다. Amazon Route 53을 사용하여 트래픽을 대체 리전으로 전환합니다.

D. 용량이 동일한 두 리전 모두에서 완전한 기능을 갖춘 웹 애플리케이션 및 데이터베이스 계층을 갖춘 다중 리전 솔루션을 사용합니다. 한 리전에서만 기본 데이터베이스를 활성화하고 다른 리전에서는 대기 데이터베이스를 활성화합니다. Amazon Route 53을 사용하면 상태 확인 라우팅 정책을 사용하여 한 리전에서 다른 리전으로 트래픽을 자동으로 전환할 수 있습니다.

Answer: C

설명

5분의 RTO(복구 시간 목표)는 애플리케이션이 장애 조치를 취하고 5분 이내에 재해 복구 지역에서 완전히 작동해야 함을 의미합니다. 1시간의 RPO(복구 지점 목표)는 1시간 이상의 데이터가 손실될 수 없음을 의미합니다.

5분의 RTO는 짧기 때문에 데이터베이스를 사용할 수 있고 완전히 복제하고 로드를 처리하기 위해 추가 인스턴스를 빠르게 시작할 수 있는 능력이 중요합니다. 앱 및 웹 계층의 인스턴스를 하나 이상 사용할 수 있도록 하면 Route 53(장애 조치 라우팅)으로 라우팅되는 수신 연결이 거의 즉시 서비스됩니다.

데이터베이스 계층을 사용 가능하고 복제하려면 가장 빠른 옵션은 MySQL용 데이터베이스 미러링을 사용하고 자동으로 장애 조치 프로세스를 구성하는 것입니다(스크립팅을 통해 수행할 수 있음).

참조:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\_MySQL.Replication.html

Q175

한 솔루션 설계자가 PostgreSQL DB 인스턴스용 Amazon RDS를 사용하는 웹 애플리케이션을 구축하고 있습니다. DB 인스턴스는 쓰기보다 더 많은 읽기를 수신할 것으로 예상됩니다. 솔루션스 아키텍트는 대량의 읽기 트래픽을 수용할 수 있고 DB 인스턴스의 가용성이 높은지 확인해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 단계를 수행해야 합니까?(세 개 선택)

A. 읽기 전용 복제본을 여러 개 생성하여 Auto Scaling 그룹에 넣습니다.

B. 서로 다른 가용 영역에 여러 읽기 전용 복제본을 생성합니다.

C. TTL 및 가중치 기반 라우팅 정책을 사용하여 Amazon Route 53 호스팅 영역과 각 읽기 전용 복제본에 대한 레코드 세트를 생성합니다.

D. 애플리케이션 로드 밸런서 (ALB) 를 생성하고 읽기 전용 복제본을 ALB 뒤에 배치합니다.

E. 실패한 읽기 전용 복제본을 감지하도록 Amazon CloudWatch 경보를 구성합니다. AWS Lambda 함수를 직접 호출하여 Route 53 레코드 세트를 삭제하도록 경보를 설정합니다.

F. 엔드포인트를 사용하여 각 읽기 전용 복제본에 대해 Amazon Route 53 상태 확인을 구성합니다.

Answer: B, C, F

Q176

온프레미스 Oracle 데이터 웨어하우스에서 30TB Oracle 데이터 웨어하우스인 Amazon Redshift로 이전하려는 기업이 있습니다. 이 조직은 AWS 스키마 변환 도구 (AWS SCT) 를 사용하여 이전 데이터 웨어하우스의 스키마를 Amazon Redshift 스키마로 변환했습니다. 또한 조직은 마이그레이션 평가 보고서를 사용하여 완료해야 하는 수동 작업을 강조했습니다.

조직은 2주간의 데이터 동결에 맞춰 데이터를 새로운 Amazon Redshift 클러스터로 이동해야 합니다. 온프레미스 데이터 웨어하우스와 AWS 간의 유일한 네트워크 링크는 50Mbps 인터넷 연결입니다.

이러한 기준을 충족하는 마이그레이션 접근 방식은 무엇입니까?

A. AWS DATABASE MIGRATION SERVICE (AWS DMS) 복제 인스턴스를 생성합니다. 기업 방화벽을 통해 데이터 웨어하우스에 도달하도록 복제 인스턴스의 퍼블릭 IP 주소를 승인합니다.데이터 고정 기간이 시작될 때 실행할 마이그레이션 작업을 만듭니다.

B. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 데이터를 Amazon S3 버킷으로 전송할 추출, 업로드 및 복사 작업을 정의합니다. 데이터를 Amazon Redshift 클러스터로 복사합니다. 데이터 고정 기간이 시작될 때 작업을 실행합니다.

C. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 사이트 간 VPN 연결을 만듭니다. 적절한 크기의 AWS DATABASE MIGRATION SERVICE (AWS DMS) 복제 인스턴스를 생성합니다. VPN 연결을 통해 온프레미스 데이터 웨어하우스에 액세스할 수 있도록 복제 인스턴스의 IP 주소를 승인합니다.

D. AWS Snowball Edge에서 작업을 생성하여 Amazon S3로 데이터를 가져옵니다. 온프레미스 서버에 AWS SCT 추출 에이전트를 설치합니다. 데이터를 Snowball Edge 디바이스로 전송할 로컬 및 AWS DATABASE MIGRATION SERVICE (AWS DMS) 작업을 정의합니다.Snowball Edge 디바이스가 AWS로 반환되고 Amazon S3에서 데이터를 사용할 수 있는 경우 AWS DMS 하위 작업을 실행하여 데이터를 Amazon Redshift에 복사합니다.

Answer: D

Q177

새로운 애플리케이션이 AWS Fargate를 통해 Amazon Elastic Container Service (Amazon ECS) 에서 실행 중입니다. 애플리케이션은 Amazon Aurora MySQL 데이터베이스를 사용합니다.애플리케이션과 데이터베이스는 서로 다른 보안 그룹이 구성된 VPC의 동일한 서브넷에서 실행됩니다. 데이터베이스의 암호는 AWS 비밀 관리자에 저장되며 DB\_PASSWORD 환경 변수를 통해 애플리케이션으로 전달됩니다. 데이터베이스의 호스트 이름은 DB\_HOST 환경 변수를 통해 응용 프로그램에 전달됩니다.응용 프로그램이 데이터베이스에 액세스하지 못했습니다.

이 오류를 해결하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?(세 개 선택)

A. 컨테이너에 이름이 “DB\_PASSWORD”인 환경 변수가 “valueFrom”으로 지정되어 있고 시크릿의 ARN이 있는지 확인합니다.

B. 컨테이너에 이름이 “DB\_PASSWORD”인 환경 변수가 “valueFrom”으로 지정되어 있고 시크릿의 시크릿 이름이 지정되어 있는지 확인한다.

C. Fargate 서비스 보안 그룹이 MySQL TCP 포트 3306에 있는 Aurora MySQL 데이터베이스의 인바운드 네트워크 트래픽을 허용하는지 확인합니다.

D. Aurora MySQL 데이터베이스 보안 그룹이 MySQL TCP 포트 3306의 파게이트 서비스로부터의 인바운드 네트워크 트래픽을 허용하는지 확인합니다.

E. 컨테이너에 DB 인스턴스 엔드포인트의 호스트 이름과 함께 이름이 “DB\_HOST”인 환경 변수가 지정되어 있는지 확인합니다.

F. 컨테이너에 DB 클러스터 엔드포인트의 호스트 이름과 함께 이름이 “DB\_HOST”인 환경 변수가 지정되어 있는지 확인합니다.

Answer: A, D, F

Q178

한 회사에서 Amazon EC2 인스턴스에서 애플리케이션을 실행합니다. 이 회사는 인스턴스에 Auto Scaling 그룹을 사용할 계획입니다. 이 전환의 일환으로 솔루션 설계자는 Amazon CloudWatch Logs가 모든 새 인스턴스에서 로그를 자동으로 수집하도록 해야 합니다. 새로운 Auto Scaling 그룹은 Amazon Linux 2 AMI를 포함하고 키 페어는 포함하지 않는 시작 템플릿을 사용합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다. CloudWatch 에이전트 구성을 Amazon S3 버킷에 저장합니다. EC2 사용자 데이터 스크립트를 작성하여 Amazon S3에서 구성 파일을 가져옵니다. 초기 부팅 중에 인스턴스에서 CloudWatch 에이전트를 구성합니다.

B. AWS 시스템 관리자 파라미터 스토어에서 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다. 구성을 사용하여 CloudWatch 에이전트를 설치 및 구성하는 시스템 관리자 문서를 생성합니다. 인스턴스가 실행 상태가 될 때마다 문서를 실행하는 시스템 관리자 실행 명령 대상을 사용하여 기본 이벤트 버스에 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

C. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다. AWS 시스템 관리자 세션 관리자를 사용하여 CloudWatch 에이전트를 설치하고 구성하는 AWS Lambda 함수를 생성합니다. Lambda 패키지 내에 에이전트 구성을 포함합니다. AWS Config 사용자 지정 규칙을 생성하여 EC2 인스턴스에 대한 변경 사항을 식별하고 Lambda 함수를 호출합니다.

D. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다. CloudWatch 에이전트 구성을 AWS Lambda 배포 패키지의 일부로 저장합니다. AWS CloudTrail을 사용하여 EC2 태깅 이벤트를 캡처하고 에이전트 설치를 시작합니다. AWS CodeBuild를 사용하여 워크로드를 실행하는 인스턴스에서 CloudWatch 에이전트를 구성합니다.

Answer: B

Q179

금융 서비스 비즈니스는 정기적으로 신용 카드 서비스 파트너로부터 자동화된 데이터 피드를 받습니다. 15분마다 약 5,000개의 레코드가 일반 텍스트로 HTTPS를 통해 서버 측 암호화를 사용하는 Amazon S3 버킷으로 바로 전송됩니다. 이 피드는 신용 카드 기본 계정 번호 (PAN) 와 관련된 개인 식별 정보 (PII) 를 제공합니다. 추가 내부 처리를 위해 데이터를 다른 S3 버킷으로 전송하기 전에 조직은 PAN을 자동으로 마스킹해야 합니다. 또한 비즈니스는 데이터를 JSON 형식으로 변환하기 전에 특정 정보를 삭제하고 결합해야 합니다. 또한 향후 추가 스트림이 가능하므로 모든 설계를 쉽게 확장 할 수 있어야합니다.

이러한 기준을 충족하는 솔루션은 무엇입니까?

A. 파일 전송 시 각 레코드를 추출하여 Amazon SQS 대기열에 쓰는 AWS Lambda 함수를 트리거합니다. 새 메시지가 SQS 대기열에 도착하면 다른 Lambda 함수를 트리거하여 레코드를 처리하고 결과를 Amazon S3의 임시 위치에 기록합니다. SQS 대기열이 비어 있으면 최종 Lambda 함수를 트리거하여 레코드를 JSON 형식으로 변환하고 결과를 내부 처리를 위해 다른 S3 버킷으로 보냅니다.

B. 파일 전송 시 각 레코드를 추출하여 Amazon SQS 대기열에 쓰는 AWS Lambda 함수를 트리거합니다. SQS 대기열에 메시지가 포함된 경우 자동으로 단일 인스턴스로 확장되도록 AWS Fargate 컨테이너 애플리케이션을 구성합니다. 애플리케이션에서 각 레코드를 처리하고 레코드를 JSON 형식으로 변환하도록 합니다. 대기열이 비어 있으면 내부 처리를 위해 결과를 다른 S3 버킷으로 전송하고 AWS Fargate 인스턴스를 축소합니다.

C. 데이터 피드 형식을 기반으로 AWS Glue 크롤러 및 사용자 지정 분류기를 생성하고 일치하는 테이블 정의를 구축합니다. 파일 전송 시 AWS Lambda 함수를 트리거하여 AWS Glue ETL 작업을 시작하여 처리 및 변환 요구 사항에 따라 전체 레코드를 변환합니다. 출력 형식을 JSON으로 정의합니다. 완료되면 ETL 작업이 내부 처리를 위해 다른 S3 버킷으로 결과를 보내도록 합니다.

D. 데이터 피드 형식을 기반으로 AWS Glue 크롤러 및 사용자 지정 분류기를 생성하고 일치하는 테이블 정의를 구축합니다. 파일 전송에 대해 Amazon Athena 쿼리를 수행하여 Amazon EMR ETL 작업을 시작하여 처리 및 변환 요구 사항에 따라 전체 레코드를 변환합니다.출력 형식을 JSON으로 정의합니다. 완료되면 내부 처리를 위해 결과를 다른 S3 버킷으로 전송하고 EMR 클러스터를 축소합니다.

Answer: C

설명

Glue 크롤러를 사용하여 AWS Glue 데이터 카탈로그를 테이블로 채울 수 있습니다. 객체 생성 이벤트가 발생할 때 S3 이벤트 알림을 사용하여 Lambda 함수를 트리거할 수 있습니다. 그러면 Lambda 함수가 Glue ETL 작업을 트리거하여 민감한 데이터를 마스킹하고 출력 형식을 JSON으로 수정하는 레코드를 변환합니다. 이 솔루션은 모든 요구 사항을 충족합니다.

잘못됨: A. AWS Glue는 ETL 서비스이므로 Lambda를 사용하는 것보다 ETL 작업의 일부로 레코드를 처리하는 데 더 적합합니다.

잘못됨: B. AWS Glue는 ETL 작업에 선호됩니다. 또한 Lambda는 단일 Fargate 작업을 사용하는 것보다 확장성이 뛰어나고 응답 속도가 더 빠릅니다.

잘못됨: D. Amazon EMR은 ETL 작업에 사용되는 서비스가 아니므로 AWS Glue를 대신 사용해야 합니다.

참조:

https://docs.aws.amazon.com/glue/latest/dg/add-crawler.html

https://docs.aws.amazon.com/glue/

Q180

한 회사에서 애플리케이션을 AWS로 마이그레이션하고 있습니다. 마이그레이션 중에 완전 관리형 서비스를 최대한 많이 사용하려고 합니다. 회사는 다음 요구 사항에 따라 응용 프로그램 내에 크고 중요한 문서를 저장해야 합니다.

1.데이터는 내구성이 높고 가용성이 높아야 합니다.

2.데이터는 저장 및 전송 중에 항상 암호화되어야 합니다.

3.암호화 키는 회사에서 관리하고 주기적으로 교체해야 합니다.

다음 중 솔루션 설계자가 권장해야 하는 솔루션은 무엇입니까?

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

B. 버킷 정책과 함께 Amazon S3를 사용하여 버킷에 대한 연결에 HTTPS를 적용하고 객체 암호화를 위해 서버 측 암호화 및 AWS KMS를 적용합니다.

C. SSL과 함께 Amazon DynamoDB를 사용하여 DynamoDB에 연결합니다. AWS KMS 키를 사용하여 저장된 DynamoDB 객체를 암호화합니다.

D. Amazon EBS 볼륨이 연결된 인스턴스를 배포하여 이 데이터를 저장합니다. AWS KMS 키를 사용하는 E8S 볼륨 암호화를 사용하여 데이터를 암호화합니다.

Answer: B

Q181

회사는 모든 AWS 계정에 대해 중앙 집중식 로깅 아키텍처를 생성해야 합니다. 아키텍처는 AWS 계정의 모든 AWS CloudTrail 로그 및 VPC 흐름 로그에 대해 거의 실시간으로 데이터 분석을 제공해야 합니다. 이 회사는 Amazon Elasticsearch Service (Amazon ES) 를 사용하여 내 로깅 계정에서 로그 분석을 수행할 계획입니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 전략을 사용해야 합니까?

A. 각 AWS 계정에 CloudTrail 및 VPC 흐름 로그를 구성하여 포깅 계정의 중앙 집중식 Amazon S3 덕켓으로 데이터를 전송합니다. AWS Lambda 함수를 생성하여 S3 버킷에서 토글 계정인 Amazon ESM으로 데이터를 로드합니다.

B. 각 AWS 계정의 Amazon CloudWatch 로그에 있는 안개 그룹으로 데이터를 전송하도록 CloudTrail 및 VPC 흐름 로그를 구성합니다. 각 AWS 계정에 CloudWatch 구독 필터를 구성하여 Amazon Kinesis Data Firehose로 데이터를 전송합니다. 포깅 계정의 Kinesis Data Firehose에서 로깅 계정의 Amazon ES로 데이터를 로드합니다.

C. 각 AWS 계정의 개별 Amazon S3 버킷으로 데이터를 전송하도록 CloudTrail 및 VPC 흐름 로그를 구성합니다. S3 이벤트에 의해 트리거된 AWS Lambda 함수를 생성하여 중앙 집중식 로깅 버킷에 데이터를 복사합니다.또 다른 Lambda 함수를 생성하여 S3 버킷에서 로깅 계정의 Amazon ES로 데이터를 로드합니다.

D. 각 AWS 계정의 Amazon CloudWatch 로그에 있는 안개 그룹으로 데이터를 보내도록 CloudTrail 및 VPC 흐름 로그를 구성합니다. 각 AWS 계정에 AWS Lambda 함수를 생성하여 로그 그룹을 구독하고 토글 계정의 Amazon S3 버킷으로 데이터를 스트리밍합니다. 또 다른 Lambda 함수를 생성하여 S3 버킷의 데이터를 로깅 계정의 Amazon ES로 이동합니다.

Answer: B

Q182

한 회사에 애플리케이션이 있습니다. 한 달에 한 번 애플리케이션은 Amazon S3 버킷 내의 모든 객체를 포함하는 압축 파일을 생성합니다. 압축 전 개체의 총 크기는 1TB입니다. 애플리케이션은 5TB의 Amazon Elastic Block Store (Amazon EBS) 볼륨이 연결된 Amazon EC2 인스턴스에서 예약된 크론 작업을 사용하여 실행됩니다. 애플리케이션은 원본 S3 버킷의 모든 파일을 EBS 볼륨으로 다운로드하고, 파일을 압축한 후 대상 S3 버킷에 업로드합니다. 애플리케이션을 호출할 때마다 처음부터 끝까지 2시간이 걸립니다.

솔루션 설계자가 이 애플리케이션의 비용을 최적화하기 위해 취해야 할 조치의 조합은 무엇입니까?(두 개 선택)

A. 애플리케이션을 마이그레이션하여 AWS Lambda 함수를 실행합니다. Amazon EventBridge (Amazon CloudWatch Events) 를 사용하여 매달 한 번 실행되도록 Lambda 함수를 예약합니다.

B. 스트림을 사용하여 소스 파일을 다운로드하도록 응용 프로그램을 구성합니다. 스트림을 압축 라이브러리로 보냅니다. 압축 라이브러리의 출력을 Amazon S3의 대상 객체로 보냅니다.

C. Amazon S3에서 소스 파일을 다운로드하고 파일을 로컬 스토리지에 저장하도록 애플리케이션을 구성합니다. 파일을 압축하여 Amazon S3에 업로드합니다.

D. AWS Fargate에서 컨테이너로 실행되도록 애플리케이션을 구성합니다. Amazon EventBridge (Amazon CloudWatch Events) 를 사용하여 매월 한 번씩 작업이 실행되도록 예약합니다.

E. Amazon Elastic File System (Amazon EFS) 파일 시스템 프로비저닝 파일 시스템을 AWS Lambda 함수에 연결합니다.

Answer: C, D

Q183

한 생명 과학 회사는 오픈 소스 도구를 조합하여 데이터 분석 워크플로우를 관리하고 온프레미스 데이터 센터의 서버에서 실행되는 Docker 컨테이너를 사용하여 유전체학 데이터를 처리하고 있습니다. 시퀀싱 데이터가 생성되어 로컬 저장 영역 네트워크 (SAN) 에 저장되고, 그 후 데이터가 처리됩니다. 연구 개발 팀은 용량 문제를 겪고 있으며 워크로드 수요에 따라 확장하고 처리 시간을 몇 주에서 며칠로 단축하도록 AWS에서 유전체학 분석 플랫폼을 재설계하기로 결정했습니다. 이 회사는 고속 AWS 다이렉트 커넥트 연결을 보유하고 있습니다. 시퀀서는 각 게놈에 대해 약 200GB의 데이터를 생성하며 개별 작업은 이상적인 컴퓨팅 용량으로 데이터를 처리하는 데 몇 시간이 걸릴 수 있습니다. 최종 결과는 Amazon S3에 저장됩니다. 회사는 매일 10~15건의 작업 요청을 예상하고 있습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 정기적으로 예약된 AWS Snowball Edge 디바이스를 사용하여 시퀀싱 데이터를 AWS로 전송합니다. AWS가 Snowball 엣지 디바이스를 수신하고 데이터가 Amazon S3로 로드되면 S3 이벤트를 사용하여 AWS Lambda 함수를 트리거하여 데이터를 처리합니다.

B. AWS Data Pipeline을 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 Amazon EC2 Auto Scaling 그룹이 Docker 컨테이너를 실행하는 사용자 지정 AMI EC2 인스턴스를 시작하여 데이터를 처리하도록 트리거합니다.

C. AWS 데이터동기화를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 AWS 단계 함수 워크플로를 시작하는 AWS Lambda 함수를 트리거합니다. Docker 이미지를 Amazon Elastic Container Registry (Amazon ECR) 에 저장하고 AWS Batch가 컨테이너를 실행하고 시퀀싱 데이터를 처리하도록 트리거합니다.

D. AWS 스토리지 게이트웨이 파일 게이트웨이를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 Docker 컨테이너를 실행하는 Amazon EC2 인스턴스에서 실행되는 AWS 배치 작업을 트리거하여 데이터를 처리합니다.

Answer: C

Q184

한 회사가 각 사업부의 내부 클라우드 청구 전략을 변경하려고 합니다. 현재 클라우드 거버넌스 팀은 전체 클라우드 지출에 대한 보고서를 각 사업부의 책임자와 공유합니다. 이 회사는 AWS Organizations를 사용하여 각 사업부에 대해 별도의 AWS 계정을 관리합니다. Organizations의 기존 태그 지정 표준에는 응용 프로그램, 환경 및 소유자가 포함됩니다. 클라우드 거버넌스 팀은 각 사업부에서 클라우드 지출에 대한 월별 보고서를 받을 수 있도록 중앙 집중식 솔루션을 원합니다. 또한 솔루션은 설정된 임계값을 초과하는 모든 클라우드 지출에 대한 알림을 보내야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 방법은 무엇입니까?

A. 각 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 경고에 대해 각 사업부를 Amazon SNS 주제에 추가합니다.각 계정에서 비용 탐색기를 사용하여 각 사업부에 대한 월별 보고서를 만들 수 있습니다.

B. 조직의 마스터 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 경고에 대해 각 사업부를 Amazon SNS 주제에 추가합니다.조직의 마스터 계정에서 비용 탐색기를 사용하여 각 사업부에 대한 월별 보고서를 만듭니다.

C. 각 계정에서 AWS 예산을 구성하고 애플리케이션, 환경 및 소유자별로 그룹화된 예산 알림을 구성합니다. 각 경고에 대해 각 사업부를 Amazon SNS 주제에 추가합니다.각 계정의 AWS 결제 및 비용 관리 대시보드를 사용하여 각 사업부에 대한 월별 보고서를 생성합니다.

D. 조직의 마스터 계정에서 AWS 비용 및 사용 보고서를 활성화하고 애플리케이션, 환경 및 소유자별로 그룹화된 보고서를 구성합니다. AWS 비용 및 사용 보고서를 처리하고 예산 알림을 전송하며 각 사업부의 이메일 목록에 월별 보고서를 보내는 AWS Lambda 함수를 생성합니다.

Answer: B

Q185

한 회사가 AWS에서 데이터 집약적 애플리케이션을 실행하고 있습니다. 이 애플리케이션은 수백 개의 Amazon EC2 인스턴스로 구성된 클러스터에서 실행됩니다. 공유 파일 시스템은 200TB의 데이터를 저장하는 여러 EC2 인스턴스에서도 실행됩니다. 애플리케이션은 공유 파일 시스템의 데이터를 읽고 수정하고 보고서를 생성합니다. 작업은 매월 한 번 실행되고 공유 파일 시스템에서 파일의 하위 집합을 읽으며 완료하는 데 약 72시간이 걸립니다. 컴퓨팅 인스턴스는 Auto Scaling 그룹에서 확장되지만 공유 파일 시스템을 호스팅하는 인스턴스는 계속 실행됩니다. 컴퓨팅 인스턴스와 스토리지 인스턴스는 모두 동일한 AWS 리전에 있습니다. 솔루션 설계자는 공유 파일 시스템 인스턴스를 교체하여 비용을 줄여야 합니다. 파일 시스템은 72시간 실행 기간 동안 필요한 데이터에 대한 고성능 액세스를 제공해야 합니다.

이러한 요구 사항을 충족하면서 전체 비용 절감을 극대화할 수 있는 솔루션은 무엇입니까?

A. 기존 공유 파일 시스템의 데이터를 S3 인텔리전트 계층화 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업이 실행되기 전에 Amazon FSx for Lustre를 사용하여 지연 로드를 사용하여 Amazon S3의 데이터로 새 파일 시스템을 생성합니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.

B. 기존 공유 파일 시스템에서 다중 연결이 활성화된 대규모 Amazon Elastic Block Store (Amazon EBS) 볼륨으로 데이터를 마이그레이션합니다. Auto Scaling 그룹 시작 템플릿의 사용자 데이터 스크립트를 사용하여 EBS 볼륨을 각 인스턴스에 연결합니다. 작업 기간 동안 EBS 볼륨을 공유 스토리지로 사용합니다. 작업이 완료되면 EBS 볼륨을 분리합니다.

C. 기존 공유 파일 시스템의 데이터를 S3 Standard 스토리지 클래스를 사용하는 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업이 실행되기 전에 Amazon FSx for Lustre를 사용하여 배치 로드를 사용하여 Amazon S3의 데이터로 새 파일 시스템을 생성합니다. 작업 기간 동안 새 파일 시스템을 공유 스토리지로 사용합니다. 작업이 완료되면 파일 시스템을 삭제합니다.

D. 기존 공유 파일 시스템의 데이터를 Amazon S3 버킷으로 마이그레이션합니다. 매월 작업을 실행하기 전에 AWS 스토리지 게이트웨이를 사용하여 Amazon S3의 데이터로 파일 게이트웨이를 생성합니다. 파일 게이트웨이를 작업의 공유 스토리지로 사용합니다. 작업이 완료되면 파일 게이트웨이를 삭제합니다.

Answer: C

Q186

한 회사에서 MySQL용 Amazon RDS 데이터베이스를 사용하여 데이터를 저장하는 중요한 애플리케이션을 실행하고 있습니다. RDS DB 인스턴스는 다중 AZ 모드로 배포됩니다. 최근 RDS 데이터베이스 장애 조치 테스트로 인해 애플리케이션이 40초 동안 중단되었습니다. 솔루션 설계자는 가동 중단 시간을 20초 미만으로 줄일 수 있는 솔루션을 설계해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. 데이터베이스 앞에 Memcached용 Amazon ElastiCache를 사용합니다.

B. 데이터베이스 앞에서 Redis용 Amazon ElastiCache를 사용합니다.

C. 데이터베이스 앞에 RDS 프록시를 사용합니다.

D. 데이터베이스를 AmazonAurora MySQL로 마이그레이션합니다.

E. AmazonAurora 복제본을 생성합니다.

F. MySQL용 RDS 읽기 전용 복제본을 생성합니다.

Answer: A, B, F

Q187

개발 팀은 회사 내에서 새 API를 서버리스 애플리케이션으로 배포합니다. 이 팀은 현재 AWS 관리 콘솔을 사용하여 Amazon API Gateway를 프로비저닝하고 있습니다. AWS Lambda 및 Amazon DynamoDB 리소스 솔루션 아키텍트는 이러한 서버리스 API의 향후 배포를 자동화하는 임무를 맡았습니다. 이를 어떻게 수행할 수 있습니까?

A. Lambda 지원 사용자 지정 리소스와 함께 AWS CloudFormation을 사용하여 API 게이트웨이를 프로비저닝합니다. AWS::DynamoDB::Table 및 AWS::Lambda::Function 리소스를 사용하여 Amazon DynamoDB 테이블 및 Lambda 함수를 생성합니다. 스크립트를 작성하여 CloudFormation 템플릿의 배포를 자동화합니다.

B. AWS 서버리스 애플리케이션 모델을 사용하여 리소스를 정의합니다. YAML 템플릿 및 애플리케이션 파일을 코드 리포지토리에 업로드합니다. AWS CodePipeline을 사용하여 코드 리포지토리에 연결하고 AWS CodeBuild를 사용하여 빌드할 작업을 생성합니다. CodePipeline의 AWS CloudFormation 배포 공급자를 사용하여 솔루션을 배포합니다.

C. AWS CloudFormation을 사용하여 서버리스 애플리케이션을 정의합니다. Lambda 함수에 버전 관리를 구현하고 버전을 가리키는 별칭을 생성합니다. 배포 시 가중치를 구성하여 트래픽을 최신 버전으로 전환하고 트래픽이 이동함에 따라 가중치를 점진적으로 업데이트합니다.

D. 애플리케이션 코드를 AWS CodeCommit 코드 리포지토리에 커밋합니다. AWS CodePipeline을 사용하여 코드커밋 코드 리포지토리에 연결합니다. AWS 코드빌드를 사용하여 AWS CodeDeploy를 사용하여 Lambda 함수를 빌드하고 배포합니다. CodeDeploy에서 배포 기본 설정 유형을 지정하여 트래픽을 새 버전으로 점진적으로 이동합니다.

Answer: B

Q188

한 회사가 EU 북부1 리전의 Amazon EC2에서 가용성이 높은 데이터 수집 애플리케이션을 실행하고 있습니다. 애플리케이션은 최종 사용자 디바이스에서 데이터를 수집하고 Amazon Kinesis 데이터 스트림과 레코드를 처리하는 AWS Lambda 함수 세트에 레코드를 씁니다. 회사는 레코드 처리 출력을 eu-north-1의 Amazon S3 버킷으로 유지합니다. 이 회사는 S3 버킷의 데이터를 Amazon Athena의 데이터 소스로 사용합니다.

A. 각 Iwo의 새 리전에서 VPC에서 실행되도록 Lambda 함수를 설정합니다. 해당 VPC에 S3 게이트웨이 엔드포인트를 설정합니다.

B. eu-north-1의 S3 버킷에서 S3 전송 가속화 켜기 애플리케이션이 S3 버킷에 데이터를 업로드할 때 새로운 S3 가속 엔드포인트를 사용하도록 애플리케이션을 변경합니다.

C. 새로운 두 리전 각각에 S3 버킷을 생성합니다. 새로운 리전 각각에 애플리케이션을 설정하여 해당 S3 버킷에 업로드하도록 S3 교차 리전 복제를 설정하여 데이터를 eu-north-1의 S3 버킷에 복제합니다.

D. Lambda 함수의 메모리 요구 사항을 늘려 사용 가능한 코어가 여러 개인지 확인합니다. 애플리케이션에서 Amazon S3 Lambda에 데이터를 업로드할 때 멀티파트 업로드 기능을 사용합니다.

Answer: A

**문제이상함**

함수 실행 시간을 최적화하기 위해 Lambda 함수에 할당된 메모리를 늘릴 수 있습니다. 이렇게 하면 각 기능 실행에 할당된 CPU 양이 비례적으로 증가합니다.

Lambda함수의 성능을 높이는 문제라면 D가 답일듯.

Q189

한 회사에서 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 0.0.0.0/0의 경로가 있습니다. 프라이빗 서브넷에는 기존 NAT 게이트웨이에 대한 0.0.0.0/0의 경로가 있습니다. 솔루션 설계자는 IPv6을 사용하려면 전체 EC2 인스턴스 플릿을 마이그레이션해야 합니다. 프라이빗 서브넷에 있는 EC2 인스턴스는 퍼블릭 인터넷에서 액세스할 수 없어야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

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

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

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

D. 기존 VPC를 업데이트하고 사용자 지정 IPv6 CIDR 블록을 VPC 및 모든 서브넷에 연결합니다. 새 NAT 게이트웨이를 만들고 IPv6 지원을 사용하도록 설정합니다. 모든 프라이빗 서브넷에 대한 VPC 라우팅 테이블을 업데이트하고: :/0에 대한 경로를 IPv6 지원 NAT 게이트웨이에 추가합니다.

Answer: C

Q190

한 회사가 여러 AWS 계정에서 AWS WAF 규칙을 관리하기 위해 AWS WAF 솔루션을 배포하려고 합니다. 계정은 AWS 조직의 서로 다른 OU에서 관리됩니다. 관리자는 필요에 따라 관리형 AWS WAF 규칙 세트에서 계정 또는 OU를 추가하거나 제거할 수 있어야 합니다. 또한 관리자는 모든 계정에서 규정을 준수하지 않는 AWS WAF 규칙을 자동으로 업데이트하고 수정할 수 있어야 합니다.

운영 오버헤드가 가장 적은 상태에서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. AWS 방화벽 관리자를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리합니다. AWS Systems Manager 파라미터 스토어 파라미터를 사용하여 관리할 계정 번호와 OU를 저장합니다. 필요에 따라 파라미터를 업데이트하여 계정 또는 OU를 추가하거나 제거합니다. Amazon EventBridge (Amazon CloudWatch Events) 규칙을 사용하여 파라미터에 대한 변경 사항을 식별하고 AWS Lambda 함수를 호출하여 방화벽 관리자 관리 계정의 보안 정책을 업데이트합니다.

B. 선택한 OU의 모든 리소스가 AWS WAF 규칙을 연결하도록 요구하는 조직 전체의 AWS Config규칙을 배포합니다. AWS Lambda를 사용하여 규정 미준수 리소스를 수정하여 자동화된 수정 작업을 배포합니다. AWS 구성 규칙이 적용되는 동일한 OU를 대상으로 하는 AWS CloudFormation 스택 세트를 사용하여 AWS WAF 규칙을 배포합니다.

C. 조직의 관리 계정에 AWS WAF 규칙을 생성합니다. AWS Lambda 환경 변수를 사용하여 계정 번호와 OU를 저장하여 관리 계정 또는 OU를 추가하거나 제거하는 데 필요한 경우 환경 변수 업데이트 멤버 계정에 교차 계정 IAM 역할을 생성합니다. 멤버 계정에서 AWS WAF 규칙을 생성하고 업데이트하기 위해 Lambda 함수에서 AWS 보안 토큰 서비스 (AWS STS) 를 사용하여 역할을 가정하십시오.

D. AWS 컨트롤 타워를 사용하여 조직 내 계정 전체에서 AWS WAF 규칙을 관리합니다. AWS 키 관리 서비스 (AWS KMS) 를 사용하여 계정 번호와 OU를 저장하여 계정 또는 OU를 추가하거나 제거하는 데 필요한 경우 AWS KMS 업데이트를 관리합니다. 멤버 계정에서 IAM 사용자 생성 관리 계정의 AWS Control Tower가 액세스 키와 보안 액세스 키를 사용하여 멤버 계정에서 AWS WAF 규칙을 생성하고 업데이트할 수 있도록 허용합니다.

Answer: B

Q191

한 회사가 AWS 클라우드에서 컨테이너식 애플리케이션을 실행하고 있습니다. 애플리케이션은 설정된 Amazon EC2 인스턴스에서 Amazon Elastic Container Service (Amazon ECS) 를 사용하여 실행됩니다. EC2 인스턴스는 Auto Scaling 그룹에서 실행됩니다. 이 회사는 Amazon Elastic Container Registry (Amazon ECR) 를 사용하여 컨테이너 이미지를 저장합니다. 새 이미지 버전이 업로드되면 새 이미지 버전에 고유한 태그가 지정됩니다. 이 회사는 새로운 이미지 버전에서 일반적인 취약성과 노출을 검사하는 솔루션이 필요합니다. 솔루션은 심각도 또는 심각도 높음 결과가 있는 새 이미지 태그를 자동으로 삭제해야 합니다. 또한 이러한 삭제가 발생할 경우 솔루션은 개발 팀에 알려야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 저장소에서 푸시 시 검사를 구성합니다. 중요 또는 심각도 높음 검색 결과가 있는 이미지에 대한 스캔이 완료되면 Amazon EventBndge (Amazon CloudWatch Events) 를 사용하여 AWS Step Functions 상태 머신을 호출합니다. Step Functions 상태 시스템을 사용하여 해당 이미지의 이미지 태그를 삭제하고 Amazon Simple Notification Service (Amazon SNS) 를 통해 개발 팀에 알립니다.

B. 리포지토리에서 푸시 시 스캔 구성 Amazon Simple Queue Service (Amazon SQS) 대기열로 푸시될 스캔 결과 구성 SQS 대기열에 새 메시지가 추가될 때 AWS Lambda 함수 호출 Lambda 함수를 사용하여 중요 또는 높음 검색 결과가 있는 이미지에 대한 이미지 태그를 삭제합니다. Amazon Simple Email Service (Amazon SES) 를 사용하여 개발 팀에 알립니다.

C. 매시간 수동 이미지 스캔을 시작하도록 AWS Lambda 함수를 예약합니다. 스캔이 완료되면 다른 Lambda 함수를 호출하도록 Amazon EventBridge (Amazon CloudWatch Events) 를 구성합니다. 두 번째 Lambda 함수를 사용하여 [위험] 또는 [심각도 높음] 검색 결과가 있는 이미지의 이미지 태그를 삭제합니다. Amazon Simple Notification Service (Amazon SNS) 를 사용하여 개발 팀에 알립니다.

D. 리포지토리에서 주기적 이미지 스캔 구성 Amazon Simple Queue Service (Amazon SQS) 대기열에 추가할 스캔 결과 구성 SQS 대기열에 새 메시지가 추가되면 AWS Step Functions 상태 머신을 호출합니다. Step Functions 상태 시스템을 사용하여 심각도 또는 심각도 높음 검색 결과가 있는 이미지의 이미지 태그를 삭제합니다. Amazon Simple Email Service (Amazon SES) 를 사용하여 개발 팀에 알립니다.

Answer: C

Q192

한 회사가 온프레미스 데이터 센터에서 인기 있는 웹 애플리케이션을 실행합니다. 이 애플리케이션은 매주 4백만 회의 조회수를 받습니다. 이 회사는 곧 게시 될 광고로 인해 트래픽이 200% 증가 할 것으로 예상합니다. 회사는 트래픽이 증가하기 전에 오리진의 부하를 줄여야 합니다. 이 회사는 전체 애플리케이션을 AWS 클라우드로 이전할 시간이 충분하지 않습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Amazon CloudFront 콘텐츠 전송 네트워크 (CDN) 를 생성합니다. 원본으로의 쿼리 전달을 활성화합니다. 쿼리 문자열을 포함하는 관리형 캐시 정책을 만듭니다. 온프레미스 로드 밸런서를 오리진으로 사용합니다. DNS 쿼리를 AWS로 오프로드하여 CloudFront CDN 트래픽을 처리합니다.

B. RTMP (실시간 메시징 프로토콜) 배포를 사용하는 Amazon CloudFront 콘텐츠 전송 네트워크 (CDN) 를 생성합니다. 원본으로의 쿼리 전달을 활성화합니다. 온프레미스 로드 밸런서를 오리진으로 사용합니다. DNS 쿼리를 AWS로 오프로드하여 CloudFront CDN 트래픽을 처리합니다.

C. AWS Global Accelerator에서 액셀러레이터를 생성합니다. HTTP 및 HTTPS TCP 포트에 대한 리스너를 추가합니다. 엔드포인트 그룹을 생성합니다. NLB (네트워크 부하 분산 장치) 를 만들어 엔드포인트 그룹에 연결합니다. NLB가 온-프레미스 서버를 가리키도록 합니다. DNS 쿼리를 AWS로 오프로드하여 AWS Global Accelerator 트래픽을 처리합니다.

D. AWS Global Accelerator에서 액셀러레이터를 생성합니다. HTTP 및 HTTPS TCP 포트에 대한 리스너를 추가합니다. 엔드포인트 그룹을 생성합니다. 애플리케이션 로드 밸런서 (ALB) 를 생성하여 엔드포인트 그룹에 연결합니다. ALB가 온프레미스 서버를 가리키도록 합니다. DNS 쿼리를 AWS로 오프로드하여 AWS Global Accelerator 트래픽을 처리합니다.

Answer: A

Q193

팀은 회사 전체의 행동 데이터를 수집하고 라우팅합니다. 이 회사는 퍼블릭 서브넷, 프라이빗 서브넷 및 인터넷 게이트웨이가 있는 다중 AZ VPC 환경을 실행합니다. 각 퍼블릭 서브넷에는 NAT 게이트웨이도 포함되어 있습니다. 대부분의 워크로드는 프라이빗 서브넷에서 실행됩니다. 솔루션 설계자는 인프라를 검토해야 합니다. 솔루션 설계자는 비용을 줄이고 애플리케이션의 기능을 유지해야 합니다. 솔루션 설계자는 비용 탐색기를 사용하여 EC2 기타 범주의 비용이 지속적으로 높다는 것을 알고 있습니다. 추가 검토에 따르면 NATgateway-bytes 요금은 EC2 기타 범주의 비용을 증가시키고 있습니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. VPC 흐름 로그를 활성화합니다. Amazon Athena를 사용하여 제거할 수 있는 트래픽의 로그를 분석합니다. 보안 그룹이 높은 비용을 초래하는 트래픽을 차단하고 있는지 확인합니다.

B. Kinesis 데이터 스트림용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. 애플리케이션에 인터페이스 VPC 엔드포인트를 사용할 수 있는 올바른 IAM 권한이 있는지 확인합니다.

C. VPC 흐름 로그와 Amazon Detective을 활성화합니다. Kinesis Data Streams와 관련이 없는 트래픽에 대한 탐지 결과 검토 해당 트래픽을 차단하도록 보안 그룹을 구성합니다.

D. Kinesis 데이터 스트림용 인터페이스 VPC 엔드포인트를 VPC에 추가합니다. VPC 엔드포인트 정책이 애플리케이션의 트래픽을 허용하는지 확인합니다.

Answer: D

Q194

한 회사에서 판매 거래 데이터를 Amazon DynamoDB 테이블에 저장합니다. 비정상적인 동작을 감지하고 신속하게 대응하려면 DynamoDB 테이블에 저장된 모든 변경 사항을 30분 이내에 기록해야 합니다.

요구 사항을 충족하는 솔루션은 무엇입니까?

A. DynamoDB 테이블을 Amazon EMR의 Apache 하이브 테이블에 매시간 복사하고 비정상적인 동작이 있는지 분석합니다. 비정상적인 동작이 감지되면 Amazon SNS 알림을 보냅니다.

B. AWS CloudTrail을 사용하여 DynamoDB 테이블을 변경하는 모든 API를 캡처합니다. CloudTrail 이벤트 필터링을 사용하여 비정상적인 동작이 감지되면 SNS 알림을 보냅니다.

C. Amazon DynamoDB 스트림을 사용하여 업데이트를 캡처하고 AWS Lambda로 전송합니다. Lambda 함수를 생성하여 Amazon Kinesis 데이터 스트림으로 레코드를 출력합니다. Amazon Kinesis 데이터 애널리틱스로 이상 징후를 분석할 수 있습니다. 비정상적인 행동이 감지되면 SNS 알림을 보냅니다.

D. Amazon CloudWatch Events의 이벤트 패턴을 사용하여 동작을 분석하기 위한 대상으로 AWS Lambda 함수를 사용하여 DynamoDB API 호출 이벤트를 캡처합니다. 비정상적인 행동이 감지되면 SNS 알림을 보냅니다.

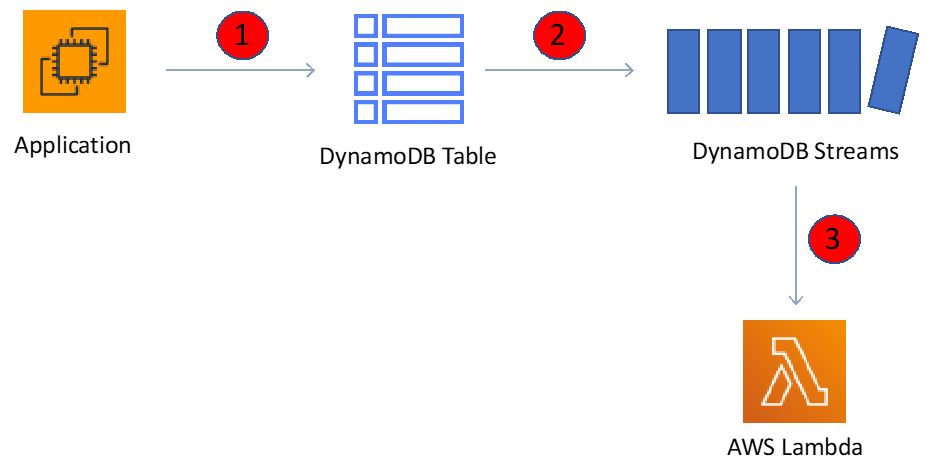
Answer: C

설명

DynamoDB 스트림은 DynamoDB 테이블에서 항목 수준 수정의 시간 순서 시퀀스를 캡처합니다. DynamoDB는 AWS Lambda와 통합되어 DynamoDB 스트림의 이벤트에 자동으로 응답하는 코드 조각인 트리거를 생성할 수 있습니다.

트리거를 사용하면 DynamoDB 테이블의 데이터 수정에 반응하는 애플리케이션을 구축할 수 있습니다. 이 경우 Lambda 함수는 데이터를 처리하고 사기 행위가 감지될 경우 Data Analytics가 데이터를 분석하고 SNS 알림을 보낼 수 있는 Kinesis Data Stream에 배치할 수 있습니다.

아래 다이어그램은 테이블(1)에서 데이터가 업데이트되고, 스트림에 수정 사항이 추가된(2), AWS Lambda가 레코드를 처리하는 방법(3)을 보여줍니다. 그런 다음 업데이트 기록은 Kinesis(표시되지 않음)를 사용하여 분석할 수 있습니다.



잘못됨: A. 이 솔루션은 작업에 잘못된 기능과 도구를 사용하며 정답만큼 자동화되어 있지 않습니다.

잘못됨: B. API 호출 캡처는 항목 수준에서 필요한 정보를 제공하지 않습니다. 항목에 대한 변경 사항을 캡처하려면 DynamoDB 스트림을 사용해야 합니다.

잘못됨: D. 항목 수준 수정을 캡처하려면 DynamoDB 스트림을 사용해야 하며 API 호출을 캡처하는 것은 도움이 되지 않습니다.

참조:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html

Q195

한 생명 과학 회사는 오픈 소스 도구를 조합하여 데이터 분석 워크플로우를 관리하고 온프레미스 데이터 센터의 서버에서 실행되는 Docker 컨테이너를 사용하여 유전체학 데이터를 처리하고 있습니다. 시퀀싱 데이터가 생성되어 로컬 저장 영역 네트워크 (SAN) 에 저장되고, 그 후 데이터가 처리됩니다. 연구 개발 팀은 용량 문제를 겪고 있으며 워크로드 수요에 따라 확장하고 처리 시간을 몇 주에서 며칠로 단축하도록 AWS에서 유전체학 분석 플랫폼을 재설계하기로 결정했습니다. 이 회사는 고속 AWS 다이렉트 커넥트 연결을 보유하고 있습니다. 시퀀서는 각 게놈에 대해 약 200GB의 데이터를 생성하며 개별 작업은 이상적인 컴퓨팅 용량으로 데이터를 처리하는 데 몇 시간이 걸릴 수 있습니다. 최종 결과는 Amazon S3에 저장됩니다. 회사는 매일 10~15건의 작업 요청을 예상하고 있습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 정기적으로 예약된 AWS Snowball Edge 디바이스를 사용하여 시퀀싱 데이터를 AWS로 전송합니다. AWS가 Snowball 엣지 디바이스를 수신하고 데이터가 Amazon S3로 로드되면 S3 이벤트를 사용하여 AWS Lambda 함수를 트리거하여 데이터를 처리합니다.

B. AWS Data Pipeline을 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 Amazon EC2 Auto Scaling 그룹이 Docker 컨테이너를 실행하는 사용자 지정 AMI EC2 인스턴스를 시작하여 데이터를 처리하도록 트리거합니다.

C. AWS 데이터동기화를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 AWS 단계 함수 워크플로를 시작하는 AWS Lambda 함수를 트리거합니다. Docker 이미지를 Amazon Elastic Container Registry (Amazon ECR) 에 저장하고 AWS Batch가 컨테이너를 실행하고 시퀀싱 데이터를 처리하도록 트리거합니다.

D. AWS 스토리지 게이트웨이 파일 게이트웨이를 사용하여 시퀀싱 데이터를 Amazon S3로 전송합니다. S3 이벤트를 사용하여 Docker 컨테이너를 실행하는 Amazon EC2 인스턴스에서 실행되는 AWS 배치 작업을 트리거하여 데이터를 처리합니다.

Answer: C

Q196

한 회사에 Auto Scaling 그룹에서 Amazon EC2 인스턴스를 사용하는 애플리케이션이 있습니다. 품질 보증 (QA) 부서는 애플리케이션을 테스트하기 위해 수명이 짧은 많은 환경을 시작해야 합니다. 애플리케이션 환경은 현재 부서의 관리자가 AWS CloudFormation 템플릿을 사용하여 시작하고 있습니다. 스택을 시작하기 위해 관리자는 CloudFormation EC2 및 오토 스케일링 API를 사용할 수 있는 권한이 있는 역할을 사용합니다. 관리자는 테스터가 자신의 환경을 시작할 수 있도록 허용하려고 하지만 각 사용자에게 광범위한 권한을 부여하고 싶지는 않습니다.

이러한 목표를 달성할 수 있는 셋업은 무엇입니까?

A. AWS CloudFormation 템플릿을 Amazon S3에 업로드합니다. QA 부서의 사용자에게 관리자의 역할을 수임하고 템플릿과 템플릿이 만드는 리소스에 대한 권한을 제한하는 정책을 추가할 수 있는 권한을 부여합니다. 사용자에게 CloudFormation 콘솔에서 템플릿을 실행하도록 교육합니다.

B. 환경 템플릿에서 AWS 서비스 카탈로그 제품을 생성합니다. 기존 역할이 있는 제품에 시작 제약 조건을 추가합니다.QA 부서의 사용자에게 AWS 서비스 카탈로그 API만 사용할 수 있는 권한을 부여합니다.사용자에게 AWS 서비스 카탈로그 콘솔에서 템플릿을 시작하도록 교육합니다.

C. AWS CloudFormation 템플릿을 Amazon S3에 업로드합니다. QA 부서의 사용자에게 CloudFormation 및 S3 API를 사용할 수 있는 권한을 부여합니다. 이 경우 템플릿과 템플릿이 생성하는 리소스에 대한 권한을 제한하는 조건이 적용됩니다. 사용자에게 CloudFormation 콘솔에서 템플릿을 실행하도록 교육합니다.

D. 환경 템플릿에서 AWS 엘라스틱 빈스토크 애플리케이션을 생성합니다. QA 부서의 사용자에게 Elastic Beanstalk 권한만 사용할 수 있는 권한을 부여합니다. Elastic Beanstalk CLI를 사용하여 Elastic Beanstalk 환경을 시작하도록 사용자를 교육하고 기존 역할을 서비스 역할로 환경에 전달합니다.

Answer: B

설명

시작 제약 조건은 최종 사용자가 제품을 시작할 때 AWS Service Catalog가 맡는 AWS Identity and Access Management(IAM) 역할을 지정합니다. IAM 역할은 IAM 사용자 또는 AWS 서비스가 AWS 서비스를 사용하기 위해 임시로 수임할 수 있는 권한 모음입니다.

시작 제약 조건이 없으면 최종 사용자는 자신의 IAM 자격 증명을 사용하여 제품을 시작하고 관리해야 합니다. 그렇게 하려면 AWS CloudFormation, 제품에서 사용하는 AWS 서비스 및 AWS Service Catalog에 대한 권한이 있어야 합니다. 시작 역할을 사용하면 대신 최종 사용자의 권한을 해당 제품에 필요한 최소 권한으로 제한할 수 있습니다.

이 솔루션을 사용하면 테스트 팀에게 테스트를 위해 AWS Service Catalog에서 제품을 시작할 수 있는 액세스 권한이 제공될 수 있으며 그들이 갖게 되는 유일한 권한은 서비스 카탈로그에서 제품을 실제로 배포할 수 있는 권한뿐입니다.

잘못됨: A. 이것은 피해야 하는 정의된 사용 사례 외부에서 서비스 API에 대한 권한을 사용할 수 있는 광범위한 액세스 권한을 테스트 팀에 제공하는 또 다른 솔루션입니다.

잘못됨: C. 이렇게 하면 제품을 시작하는 데 필요한 API에 대한 권한이 제한되지만 솔루션이 피하려는 서비스 카탈로그 제품 외부에서 해당 API를 사용할 수 있는 권한도 테스트 팀에 부여됩니다.

참조:

https://docs.aws.amazon.com/servicecatalog/latest/adminguide/constraints-launch.html

Q197

솔루션스 아키텍트는 친환경 배포 방법론을 사용하여 AWS Elastic Beanstalk 내에서 애플리케이션 환경을 업데이트해야 합니다. 솔루션 설계자는 기존 애플리케이션 환경과 동일한 환경을 만들고 새 환경에 애플리케이션을 배포합니다.

업데이트를 완료하려면 다음 작업을 수행해야 합니까?

A. Amazon Route 53을 사용하여 새 환경으로 리디렉션합니다.

B. 스왑 환경(Swap Environment) URL 옵션을 선택합니다.

C. Auto Scaling 시작 구성을 바꿉니다.

D. 그린 환경(green environment)을 가리키도록 DNS 레코드를 업데이트합니다.

Answer: B

Q198

Amazon S3에 데이터 레이크가 있는 회사는 여러 AWS 계정에 있는 수백 개의 애플리케이션에서 액세스해야 합니다. 이 회사의 정보 보안 정책에 따르면 S3 버킷은 퍼블릭 인터넷을 통해 액세스해서는 안되며 각 애플리케이션이 작동하는 데 필요한 최소한의 권한이 있어야 합니다. 이러한 요구 사항을 충족하기 위해 솔루션 설계자는 각 애플리케이션에 대해 특정 VPC로 제한된 S3 액세스 포인트를 사용할 계획입니다.

솔루션 설계자가 이 솔루션을 구현하기 위해 수행해야 하는 단계는 무엇입니까?(두 개 선택)

A. S3 버킷을 소유한 AWS 계정에서 각 애플리케이션에 대해 S3 액세스 포인트를 생성합니다. 애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다.액세스 포인트에서 액세스하도록 버킷 정책을 업데이트합니다.

B. 각 애플리케이션의 VPC에 Amazon S3에 대한 인터페이스 엔드포인트를 생성합니다. S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다. S3 엔드포인트에 대한 VPC 게이트웨이 연결을 생성합니다.

C. 각 애플리케이션의 VPC에 게이트웨이 엔드포인트 또는 Amazon S3를 생성합니다. S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다. 액세스 포인트에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.

D. 각 AWS 계정의 각 애플리케이션에 대한 S3 액세스 포인트를 생성하고 액세스 포인트를 S3 버킷에 연결합니다. 애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다. 액세스 포인트에서 액세스하도록 버킷 정책을 업데이트합니다.

E. 데이터 레이크의 VPC에 Amazon S3에 대한 게이트웨이 엔드포인트를 생성합니다. 엔드포인트 정책을 연결하여 S3 버킷에 대한 액세스를 허용합니다. 버킷에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.

Answer: A, C

Q199

미디어 회사에는 30TB의 디지털 뉴스 비디오 저장소가 있습니다. 이러한 비디오는 온프레미스 테이프 라이브러리의 테이프에 저장되며 MAM (Media Asset Management : 미디어 자산 관리) 시스템에서 참조됩니다. 이 회사는 이러한 비디오의 메타데이터를 자동화된 방식으로 강화하고 MAM 기능을 사용하여 검색 가능한 카탈로그에 넣고자 합니다. 회사는 사물, 풍경, 항목 또는 사람의 얼굴과 같은 비디오 정보를 기반으로 검색할 수 있어야 합니다. 각 사람의 이미지가 포함 된 동영상에 등장한 사람들의 얼굴이 포함 된 카탈로그를 사용할 수 있습니다. 이 회사는 이러한 비디오를 AWS로 마이그레이션하려고 합니다. 이 회사는 AWS와 고속 AWS Direct Connect로 연결되어 있으며 현재 파일 시스템에서 직접 MAM 솔루션 비디오 콘텐츠를 이동하려고 합니다. 지속적인 관리 오버헤드를 최소화하고 기존 시스템의 중단을 최소화하여 이러한 요구 사항을 어떻게 충족할 수 있습니까?

A. 온프레미스에서 AWS 스토리지 게이트웨이 파일 게이트웨이 어플라이언스를 설정합니다. MAM 솔루션을 사용하여 현재 아카이브에서 비디오를 추출하여 파일 게이트웨이로 푸시합니다. 얼굴 카탈로그를 사용하여 Amazon Rekognition에서 컬렉션을 구축합니다. Rekognition 자바스크립트 SDK를 호출하는 AWS Lambda 함수를 빌드하여 Rekognition이 파일 게이트웨이를 지원하는 Amazon S3 파일에서 비디오를 가져오고, 필요한 메타데이터를 검색하고, 메타데이터를 MAM 솔루션으로 푸시하도록 합니다.

B. 온프레미스에서 AWS 스토리지 게이트웨이 테이프 게이트웨이 어플라이언스를 설정합니다. MAM 솔루션을 사용하여 현재 아카이브에서 비디오를 추출하여 테이프 게이트웨이로 푸시합니다. 얼굴 카탈로그를 사용하여 Amazon Rekognition에서 컬렉션 구축 Rekognition 자바스크립트 SDK를 호출하는 AWS Lambda 함수를 빌드하여 Amazon Rekognition이 테이프 게이트웨이의 비디오를 처리하고 필요한 메타데이터를 MAM 솔루션으로 푸시하도록 합니다.

C. Amazon Kinesis 비디오 스트림을 사용하여 비디오 수집 스트림을 구성합니다. 얼굴 카탈로그를 사용하여 Amazon Rekognition에서 컬렉션을 구축합니다. MAM 솔루션의 비디오를 Kinesis 비디오 스트림으로 스트리밍합니다. 스트리밍된 비디오를 처리하도록 Amazon Rekognition을 구성합니다. 그런 다음 스트림 소비자를 사용하여 필요한 메타데이터를 검색하고 메타데이터를 MAM 솔루션으로 푸시합니다.Amazon S3에 비디오를 저장하도록 스트림을 구성합니다.

D. OpenCV 라이브러리를 실행하는 Amazon EC2 인스턴스를 설정합니다. 온프레미스 라이브러리에서 Amazon EBS 볼륨으로 동영상, 이미지 및 얼굴 카탈로그를 복사합니다.

Answer: A

Q200

금융 회사가 Amazon S3에서 데이터 레이크를 호스팅합니다. 이 회사는 매일 밤 여러 타사로부터 SFTP를 통해 재무 데이터 기록을 받습니다. 이 회사는 VPC의 퍼블릭 서브넷에 있는 Amazon EC2 인스턴스에서 자체 SFTP 서버를 실행합니다. 파일이 업로드된 후 동일한 인스턴스에서 실행되는 크론 작업에 의해 데이터 레이크로 이동됩니다. SFTP 서버는 Amazon Route 53을 사용하여 DNS SFTP.Examwe.com에서 연결할 수 있습니다.

SFTP 솔루션의 안정성과 확장성을 개선하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. EC2 인스턴스를 Auto Scaling 그룹으로 이동합니다. EC2 인스턴스를 애플리케이션 로드 밸런서 (ALB) 뒤에 배치합니다. SFTP 서버는 Amazon Route 53을 사용하여 DNS sftp.examWe.com에서 연결할 수 있습니다.

B. SFTP 서버를 SFTP용 AWS 전송으로 마이그레이션합니다. 서버 엔드포인트 호스트 이름을 가리키도록 Route 53에서 DNS 레코드 sftp.example.com을 업데이트합니다.

C. SFTP 서버를 AWS 스토리지 게이트웨이의 파일 게이트웨이로 마이그레이션합니다. 파일 게이트웨이 엔드포인트를 가리키도록 Route 53에서 DNS 레코드 sflp.example.com을 업데이트합니다.

D. EC2 인스턴스를 NLB (네트워크 로드 밸런서) 뒤에 배치합니다. NLB를 가리키도록 Route 53에서 DNS 레코드 sftp.example.com을 업데이트합니다.

Answer: B

Q201

한 회사에서 모놀리식 애플리케이션을 배포된 최신 애플리케이션 또는 AWS로 리팩토링할 계획입니다. 다음 요구 사항이 있는 응용 프로그램의 모뎀 설계를 지원하려면 CLCD 파이프라인을 업그레이드해야 합니다.

\* 매시간 여러 번 변경 사항을 릴리스할 수 있어야 합니다.

\* 가능한 한 빨리 변경 사항을 롤백할 수 있어야 합니다.

이러한 요구 사항을 충족하는 설계는 무엇입니까?

A. 애플리케이션 및 해당 구성을 포함하도록 AMI를 통합하는 CL-CD 파이프라인을 배포합니다. Amazon EC2 인스턴스를 교체하여 애플리케이션을 배포합니다.

B. 애플리케이션의 CI/CD 파이프라인에 대한 배포 대상으로 보조 환경에서 저장할 AWS Elastic Beanstak을 지정합니다. 배포하려면 스테이징 및 프로덕션 환경 URL을 교체합니다.

C. AWS Systems Manager를 사용하여 각 배포에 대해 인프라를 다시 프로비저닝합니다. Amazon EC2 사용자 데이터를 업데이트하여 Amazon S3에서 최신 코드 아트 팩트를 가져오고 Amazon Route 53 가중치 기반 라우팅을 사용하여 새 환경을 가리킵니다.

D. 사전 빌드된 AMI를 사용하여 Auto Scaling 이벤트의 팬으로 애플리케이션 업데이트를 롤아웃합니다. 새 버전의 AMI를 사용하여 인스턴스를 추가하고, 배포 이벤트 중에 구성된 종료 정책과 함께 이전 AMI 버전을 사용하는 모든 인스턴스를 단계적으로 폐지합니다.

Answer: B

Q202

기업이 웹 사이트를 온프레미스 데이터 센터에서 Amazon Web Services (AWS) 로 이전하고자 합니다. 동시에 가용성과 비용 효율성을 높이기 위해 웹 사이트를 컨테이너화된 마이크로서비스 아키텍처로 전환하고자 합니다. 회사의 보안 정책에 따라 권한 및 네트워크 권한은 가능한 최소한의 권한으로 모범 사례에 따라 설정되어야 합니다.

솔루션스 아키텍트는 애플리케이션의 보안 기준을 준수하고 이를 Amazon ECS 클러스터에 배포한 컨테이너식 아키텍처를 설계해야 합니다.

요구 사항을 준수하기 위해 배포 시 필요한 절차는 무엇입니까?(두 개 선택)

A. 브리지 네트워크 모드를 사용하여 작업을 생성합니다.

B. awsvpc 네트워크 모드를 사용하여 작업을 생성합니다.

C. Amazon EC2 인스턴스에 보안 그룹을 적용하고 EC2 인스턴스용 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.

Answer: B, E

Q203

한 솔루션스 아키텍트가 사용자 지정 도메인으로 두 AWS 리전의 사용자에게 서비스를 제공하는 웹 애플리케이션을 배포했습니다. 애플리케이션은 Amazon Route 53 지연 시간 기반 라우팅을 사용합니다. 솔루션스 아키텍트는 각 리전의 별도 가용 영역에 있는 한 쌍의 웹 서버와 가중치 기반 레코드 세트를 연결했습니다. 솔루션 설계자는 재해 복구 시나리오를 실행합니다. 한 리전의 모든 웹 서버가 중지되면 Route 53은 자동으로 사용자를 다른 리전으로 리디렉션하지 않습니다.

다음 중 이 문제의 근본 원인은 무엇입니까?(두 개 선택)

A. 웹 서버가 중지된 리전의 가중치가 다른 리전의 가중치보다 큽니다.

B. 보조 리전의 웹 서버 중 하나가 HTTP 상태 확인을 통과하지 못했습니다.

C. 지연 시간 리소스 레코드 세트는 가중치 기반 리소스 레코드 세트와 함께 사용할 수 없습니다.

D. 웹 서버가 중지된 지역의 도메인과 연결된 지연 시간 별칭 리소스 레코드 세트에 대해 대상 상태를 평가하는 설정이 설정되지 않았습니다.

E. 중지된 웹 서버와 연결된 하나 이상의 가중치 기반 리소스 레코드 세트에 대해 HTTP 상태 확인이 설정되지 않았습니다.

Answer: A, E

Q204

한 회사에서 미국에 있는 6곳의 파트너와 정보를 공유하기 위해 REST API를 만들고 있습니다. 이 회사는 Amazon API Gateway 리전 엔드포인트를 생성했습니다. 6개 파트너는 각각 하루에 한 번 API에 액세스하여 일일 판매량을 게시합니다. 초기 배포 후 회사는 전 세계 500개의 서로 다른 IP 주소에서 발생하는 초당 1,000개의 요청을 관찰합니다. 이 회사는 이러한 트래픽이 봇넷에서 발생한다고 생각하며 비용을 최소화하면서 API를 보호하기를 원합니다.

API를 보호하기 위해 회사는 어떤 접근 방식을 취해야 합니까?

A. API를 오리진으로 사용하여 Amazon CloudFront 배포를 생성합니다. 하루에 5개가 넘는 요청을 제출하는 클라이언트를 차단하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 CloudFront 배포와 연결합니다. OAI (origin access identity) 로 CloudFront를 구성하고 이를 배포와 연결합니다. OAI만 POST 메서드를 실행할 수 있도록 API 게이트웨이를 구성합니다.

B. API를 오리진으로 사용하여 Amazon CloudFront 배포를 생성합니다. 하루에 5개가 넘는 요청을 제출하는 클라이언트를 차단하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 CloudFront배포와 연결합니다. API 키로 채워진 CloudFront 배포에 사용자 지정 헤더를 추가합니다. POST 메서드에서 API 키를 요구하도록 API를 구성합니다.

C. 6개 파트너가 사용하는 IP 주소에 대한 액세스를 허용하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 API와 연결합니다. 요청 제한이 있는 리소스 정책을 생성하여 API와 연결합니다. POST 메서드에서 API 키를 요구하도록 API를 구성합니다.

D. 6개 파트너가 사용하는 IP 주소에 대한 액세스를 허용하는 규칙을 사용하여 AWS WAF 웹 ACL을 생성합니다. 웹 ACL을 API와 연결합니다. 요청 한도가 있는 사용량 계획을 생성하고 API와 연결합니다. API 키를 생성하여 사용량 계획에 추가합니다.

Answer: D

설명

사용량 계획과 관련된 요금 기반 규칙은 지속적으로 업데이트되는 후행 5분 기간 동안 각 클라이언트 IP에서 허용하는 웹 요청 수를 지정합니다. 사용 계획과 연결된 API 키는 요청에서 API 키를 사용하는 클라이언트에게만 액세스 권한이 부여되도록 합니다. 이 솔루션을 사용하려면 클라이언트의 IP 주소가 화이트리스트에 포함되어야 하고 API에 대한 요청에 사용할 API 키가 클라이언트에 배포되어야 합니다.

잘못됨: B는 오답입니다.

비율 기반 규칙은 각 발신 IP 주소에 대한 요청 비율을 추적하고 한도를 초과하는 비율로 IP에 대해 규칙 작업을 트리거합니다. 5분 시간 범위당 요청 수로 제한을 설정합니다. 요청을 하루에 10개로 제한하도록 AWS WAF 요금 기반 규칙을 구성할 수 없습니다. 또한 비용을 최소화하기 위해 이 솔루션에는 CloudFront가 필요하지 않습니다.

잘못됨: A. 위의 비율 기반 규칙과 같습니다. OAI는 S3 URL을 사용한 직접 액세스를 방지하기 위해 Amazon S3 버킷과 함께 사용되는 특수 CloudFront 사용자입니다. 일반적으로 서명된 URL 및 서명된 쿠키와 같은 다른 보호 기능과 함께 사용됩니다. API Gateway API에서는 OAI를 사용할 수 없습니다.

잘못됨: C. AWS WAF 리소스 정책은 보안 주체 또는 소스 IP 주소/CIDR 블록이 API를 호출할 수 있는지 여부를 제어합니다. 리소스 정책에는 연결된 요청 제한이 없습니다. 이에 대해 웹 ACL 속도 기반 규칙을 사용하십시오. 이 API는 데이터를 가져오고 게시하지 않는 데 사용되므로 API 키를 GET 메서드에 구성해야 합니다.

참조:

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies.html

https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gatew

Q205

한 회사는 온프레미스 데이터 센터에서 많은 서비스를 실행하고 있습니다. 데이터 센터는 AWS 다이렉트 커넥트 (DX) 및 IPsec VPN을 사용하여 AWS에 연결됩니다. 서비스 데이터는 민감하며 연결이 인터넷을 통과할 수 없습니다. 이 회사는 새로운 시장 부문으로 확장하고 AWS를 사용하는 다른 회사에 서비스를 제공하기 시작하기를 원합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. TCP 트래픽을 허용하는 VPC 엔드포인트 서비스를 생성하고, 이를 네트워크 로드 밸런서 뒤에서 호스팅하고, DX에서 서비스를 사용할 수 있도록 합니다.

B. HTTP 또는 HTTPS 트래픽을 허용하는 VPC 엔드포인트 서비스를 생성하고, 애플리케이션 로드 밸런서 뒤에서 호스팅하고, DX에서 서비스를 사용할 수 있도록 합니다.

C. 인터넷 게이트웨이를 VPC에 연결하고 네트워크 액세스 제어 및 보안 그룹 규칙이 관련 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다.

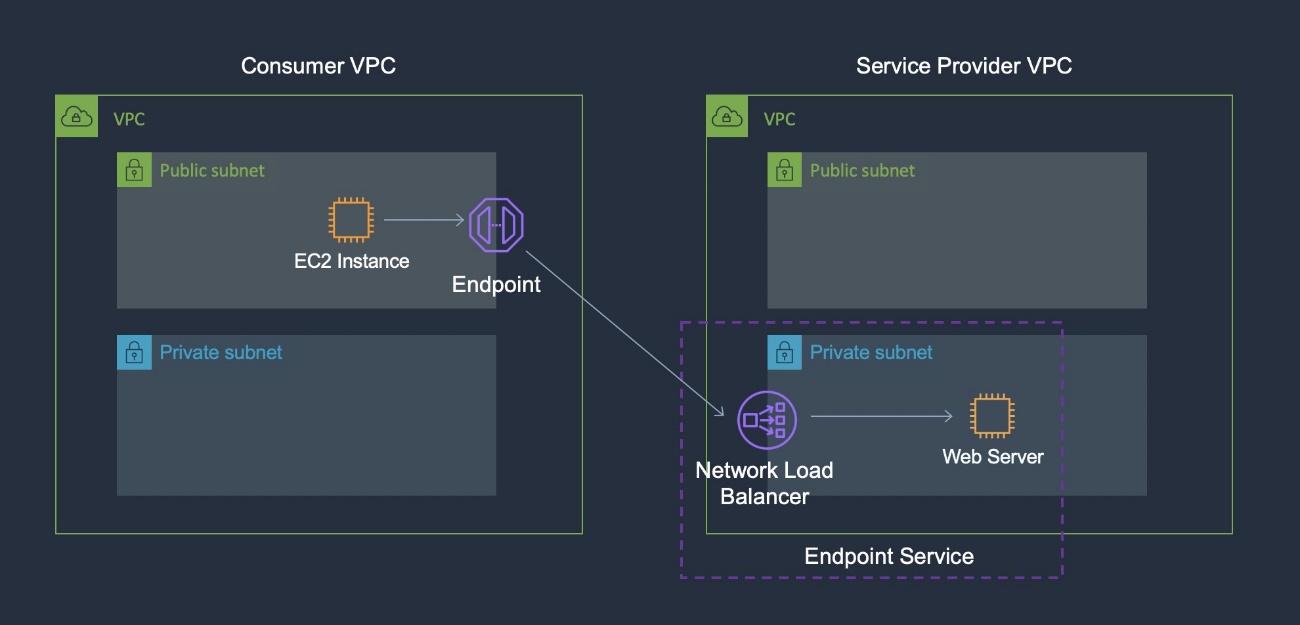
D. VPC에 NAT 게이트웨이를 연결하고 네트워크 액세스 제어 및 보안 그룹 규칙이 관련 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다.

Answer: A

설명

솔루션은 서비스 제공자 모델에서 VPC 엔드포인트 서비스를 사용하는 것입니다. 이 모델에서 네트워크 로드 밸런서는 애플리케이션 서비스 앞의 서비스 제공자 VPC에 생성되어야 합니다. NLB는 온프레미스 대상을 사용할 수 있습니다. 그런 다음 NLB를 사용하는 VPC 엔드포인트가 생성됩니다.

그런 다음 권한이 부여된 서비스 소비자는 선택적으로 서비스를 구성한 각 가용 영역에서 서비스에 대한 인터페이스 엔드포인트를 생성합니다. 이것은 아래 이미지에 설명되어 있습니다.



잘못됨: B. NLB는 VPC 엔드포인트 서비스에 사용해야 합니다.

잘못됨: D. 인터넷 게이트웨이는 피해야 하는 인터넷 기반 연결에 사용됩니다. VPC 엔드포인트 서비스에는 필요하지 않습니다.

참조:

https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service-overview.html

Q206

대규모 기업의 솔루션 설계자는 AWS Organizations의 조직 내 모든 AWS 계정에서 인터넷으로 보내는 아웃바운드 트래픽에 대한 네트워크 보안을 설정해야 합니다. 이 조직은 100개 이상의 AWS 계정을 보유하고 있으며, 이 계정은 중앙 집중식 AWS Transit Gateway를 사용하여 서로 라우팅됩니다. 각 계정에는 인터넷으로의 아웃바운드 트래픽을 위한 인터넷 게이트웨이와 NAT 게이트웨이가 모두 있습니다. 이 회사는 단일 AWS 리전에만 리소스를 배포합니다. 이 회사는 조직의 모든 AWS 계정에 대해 인터넷으로 전송되는 모든 아웃바운드 트래픽에 대해 중앙에서 관리되는 규칙 기반 필터링을 추가할 수 있어야 합니다. 아웃바운드 트래픽의 최대 로드는 각 가용 영역에서 25Gbps를 초과하지 않습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 인터넷으로의 아웃바운드 트래픽을 위한 새 VPC를 생성합니다. 기존 전송 게이트웨이를 새 VPC에 연결합니다. 새 NAT 게이트웨이를 구성합니다. 리전의 모든 가용 영역에서 규칙 기반 필터링을 위해 오픈 소스 인터넷 프록시를 실행하는 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 프록시의 Auto Scaling 그룹을 가리키도록 모든 기본 경로를 수정합니다.

B. 인터넷으로의 아웃바운드 트래픽을 위한 새 VPC를 생성합니다. 기존 전송 게이트웨이를 새 VPC에 연결합니다. 새 NAT 게이트웨이를 구성합니다.규칙 기반 필터링을 위해 AWS 네트워크 방화벽 방화벽을 사용합니다. 각 가용 영역에 네트워크 방화벽 엔드포인트를 생성합니다. 네트워크 방화벽 끝점을 가리키도록 모든 기본 경로를 수정합니다.

C. 각 AWS 계정에서 규칙 기반 필터링을 위한 AWS 네트워크 방화벽 방화벽을 생성합니다. 각 계정의 네트워크 방화벽 방화벽을 가리키도록 모든 기본 경로를 수정합니다.

D. 각 AWS 계정에서 규칙 기반 필터링을 위해 오픈 소스 인터넷 프록시를 실행하는 네트워크에 최적화된 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성합니다. 프록시의 Auto Scaling 그룹을 가리키도록 모든 기본 경로를 수정합니다.

Answer: B

Q207

한 소프트웨어 회사에서 각각 10개의 개발 팀에 3개의 AWS 계정을 사용하고 있습니다. 이 회사는 세 개의 NAT 게이트웨이가 포함된 AWS CloudFormation 표준 VPC 템플릿을 개발했습니다. 템플릿이 각 팀의 각 계정에 추가됩니다. 회사는 새로운 개발 팀이 추가 될 때마다 네트워크 비용이 증가 할 것이라고 우려하고 있습니다. 솔루션 설계자는 회사 솔루션의 신뢰성을 유지하고 운영 복잡성을 최소화해야 합니다.

이러한 요구 사항을 충족하면서 네트워크 비용을 줄이기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 공유 서비스 계정에 3개의 NAT 게이트웨이가 있는 단일 VPC를 생성합니다. 전송 게이트웨이를 통해 공유 서비스 계정 VPC의 NAT 게이트웨이로의 기본 경로를 사용하여 각 계정 VPC를 구성합니다. 표준 VPC 템플릿에서 모든 NAT 게이트웨이를 제거합니다.

B. 공유 서비스 계정에 3개의 NAT 게이트웨이가 있는 단일 VPC를 생성합니다. 공유 서비스 계정 VPC의 NAT 게이트웨이에 대한 VPC 피어링 연결을 통해 기본 경로로 각 계정 VPC를 구성합니다. 표준 VPC 템플릿에서 모든 NAT 게이트웨이를 제거합니다.

C. 표준 VPC 템플릿에서 두 개의 NAT 게이트웨이 제거 나머지 NAT 게이트웨이의 안정성을 보장하려면 NAT 게이트웨이 SLA를 사용합니다.

D. 공유 서비스 계정에 3개의 NAT 게이트웨이가 있는 단일 VPC를 생성합니다. 각 계정에서 공유 서비스 계정으로의 사이트 간 VPN 연결을 구성합니다.표준 VPC 템플릿에서 모든 NAT 게이트웨이를 제거합니다.

Answer: A

Q208

한 회사가 AWS 클라우드에서 애플리케이션을 실행하고 있습니다. 애플리케이션은 Amazon Elastic Container Service (Amazon ECS) 클러스터의 컨테이너에서 실행됩니다. ECS 작업에서는 Fargate 시작 유형을 사용합니다. 애플리케이션의 데이터는 관계형이며 Amazon Aurora MySQL에 저장됩니다. 규제 요구 사항을 충족하려면 애플리케이션 장애 발생 시 애플리케이션이 별도의 AWS 리전으로 복구할 수 있어야 합니다. 장애가 발생할 경우 데이터가 손실될 수 없습니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 다른 리전에 Aurora 복제본을 프로비저닝합니다.

B. 데이터를 다른 리전으로 지속적으로 복제할 수 있도록 AWS DataSync를 설정합니다.

C. 데이터를 다른 리전으로 지속적으로 복제하도록 AWS 데이터베이스 마이그레이션 서비스 (AWS DMS) 를 설정합니다.

D. AWS Database Migration Service (AWS DMS) 를 사용하여 5분마다 스냅샷을 예약합니다.

Answer: A

Q209

한 회사가 정적 콘텐츠로 구성된 새로운 글로벌 웹 사이트를 호스팅하려고 합니다.솔루션 설계자는 Amazon CloudFront를 OAI(origin access identity) 과 함께 사용하여 프라이빗 Amazon S3 버킷에 저장된 웹 사이트 콘텐츠에 액세스하는 솔루션을 개발하고 있습니다. 테스트 중에 솔루션스 아키텍트는 S3 버킷에서 404 오류를 수신합니다. 오류 메시지는 example.com/path/와 같이 슬래시로 끝나는 경로에 액세스하려는 시도에만 나타납니다. 이러한 요청은 기존 S3 객체 path/index.html 를 반환해야 합니다. 잠재적 솔루션이 CloudFront가 콘텐츠를 캐시하는 것을 막아서는 안 됩니다.

이 문제를 해결하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. CloudFront 오리진을 Amazon API Gateway 프록시 엔드포인트로 변경합니다. AWS Lambda 함수를 사용하여 S3 요청 URL을 다시 작성합니다.

B. CloudFront 오리진을 Amazon API Gateway 엔드포인트로 변경합니다. AWS 서비스 통합에서 S3 요청 URL을 다시 작성합니다.

C. 최종 사용자 요청 이벤트에 의해 호출되는 AWS Lambda @Edge 함수를 사용하여 S3 요청 URL을 다시 작성하도록 CloudFront 구성을 변경합니다.

D. S3 요청 URL을 다시 작성하기 위해 오리진 요청 이벤트에 의해 호출되는 AWS Lambda @Edge 함수를 사용하도록 CloudFront 구성을 변경합니다.

Answer: C

Q210

한 회사가 웹에 사용자가 임의의 사진을 업로드하고 검색 할 수있는 이미지 서비스를 구축하고 있습니다. 사용량이 가장 많을 때 전 세계 최대 10.000 명의 사용자가 이미지를 업로드합니다. 그러면 서비스가 업로드된 이미지에 텍스트를 오버레이하고 회사 웹 사이트에 게시됩니다.

솔루션 설계자는 어떤 설계를 구현해야 합니까?

A. 업로드된 이미지를 Amazon Elastic File System (Amazon EFS) 에 저장합니다. 각 이미지에 대한 애플리케이션 로그 정보를 Amazon CloudWatch 로그로 전송합니다. CloudWatch 로그를 사용하는 Amazon EC2 인스턴스 집합을 생성하여 어떤 이미지를 처리해야 하는지 결정합니다. 처리된 이미지를 Amazon EFS의 다른 디렉터리에 배치합니다.Amazon CloudFront를 활성화하고 오리진을 플릿의 EC2 인스턴스 중 하나가 되도록 구성합니다.

B. 업로드된 이미지를 Amazon S3 버킷에 저장하고 Amazon Simple Notification Service (Amazon SNS) 로 메시지를 전송하도록 S3 버킷 이벤트 알림을 구성합니다. 애플리케이션 로드 밸런서 (ALB) 뒤에 Amazon EC2 인스턴스 플릿을 생성하여 Amazon SNS에서 메시지를 가져와 이미지를 처리하고 Amazon Elastic File System (Amazon EFS) 에 배치합니다.SNS 메시지 볼륨에 대한 Amazon CloudWatch 지표를 사용하여 EC2 인스턴스를 확장할 수 있습니다. Amazon CloudFront를 활성화하고 오리진 로그를 EC2 인스턴스 앞에 있는 ALB로 구성합니다.

C. 업로드된 이미지를 Amazon S3 버킷에 저장하고 Amazon Simple Queue Service (Amazon SQS) 대기열로 메시지를 전송하도록 S3 버킷 이벤트 알림을 구성합니다. Amazon EC2 인스턴스 플릿을 생성하여 SQS 대기열에서 메시지를 가져와 이미지를 처리하고 다른 S3 버킷에 배치합니다. 대기열 깊이에 Amazon CloudWatch 지표를 사용하여 EC2 인스턴스를 확장할 수 있습니다. Amazon CloudFront를 활성화하고 오리진을 처리된 이미지가 포함된 S3 버킷이 되도록 구성합니다.

D. 업로드된 이미지를 Amazon EC2 스팟 인스턴스 플릿에 마운트된 공유 Amazon Elastic Block Store (Amazon EBS) 볼륨에 저장합니다. 업로드된 각 이미지에 대한 정보와 이미지가 처리되었는지 여부를 포함하는 Amazon DynamoDB 테이블을 생성합니다. Amazon EventBridge (Amazon CloudWatch Events) 규칙을 사용하여 EC2 인스턴스를 스케일아웃합니다. Amazon CloudFront를 활성화하고 오리진이 EC2 인스턴스 플릿 앞에 있는 탄력적 로드 밸런서를 참조하도록 구성합니다.

Answer: C

Q211

한 회사에서 AWS 조직을 사용하여 여러 AWS 계정을 관리하고 있습니다. 보안을 위해 회사는 모든 조직의 멤버 계정에서 타사 알림 시스템과 통합할 수 있는 Amazon Simple Notification Service (Amazon SNS) 주제를 생성해야 합니다. 한 솔루션스 아키텍트는 AWS CloudFormation 템플릿을 사용하여 SNS 주제와 스택 세트를 생성하여 CloudFormation 스택의 배포를 자동화했습니다. 조직에서 신뢰할 수 있는 액세스가 활성화되었습니다.

솔루션스 아키텍트는 모든 AWS 계정에 CloudFormation 스택세트를 배포하기 위해 무엇을 해야 합니까?

A. 조직 멤버 계정에 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택세트 드리프트 감지를 사용합니다.

B. 조직 구성원 계정에서 스택을 만듭니다. 셀프 서비스 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택세트 자동 배포를 활성화합니다.

C. 조직 관리 계정에서 스택 세트를 생성합니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다.CloudFormation 스택세트 자동 배포를 활성화합니다.

D. 조직 관리 계정에서 스택을 만듭니다. 서비스 관리 권한을 사용합니다.조직에 배포할 배포 옵션을 설정합니다. CloudFormation 스택 세트 드리프트 감지를 활성화합니다.

Answer: C

Q212

한 회사의 본사에서는 전 세계 작업자가 사용하는 문제 추적 시스템을 지원하는 대규모 온프레미스 MySQL 데이터베이스를 호스팅합니다. 이 조직은 이미 일부 워크로드에 AWS를 사용하고 있으며 데이터베이스 엔드포인트가 온프레미스 데이터베이스를 참조하도록 Amazon Route 53 항목을 구성했습니다. 경영진은 데이터베이스가 단일 장애 지점 역할을 하는 것에 대해 걱정하고 있으며, 솔루션 설계자가 데이터 손실이나 가동 중지 시간을 초래하지 않고 데이터베이스를 AWS로 재배치하도록 요청합니다.

솔루션 설계자는 어떤 활동을 구현해야 합니까?

A. Amazon Aurora DB 클러스터를 생성합니다. AWS DATABASE MIGRATION SERVICE (AWS DMS) 를 사용하여 온프레미스 데이터베이스에서 Aurora로 전체 로드를 수행합니다. Aurora 클러스터 엔드포인트를 가리키도록 데이터베이스의 Route 53 항목을 업데이트하고 온프레미스 데이터베이스를 종료합니다.

B. 업무 시간 외 시간에는 온-프레미스 데이터베이스를 종료하고 백업을 만듭니다. 이 백업을 Amazon Aurora DB 클러스터로 복원합니다. 복원이 완료되면 Aurora 클러스터 엔드포인트를 가리키도록 데이터베이스의 Route 53 항목을 업데이트하고 온프레미스 데이터베이스를 종료합니다.

C. Amazon Aurora DB 클러스터를 생성합니다. AWS DATABASE MIGRATION SERVICE (AWS DMS) 를 사용하여 온프레미스 데이터베이스에서 Aurora로의 연속 복제를 통해 전체 로드를 수행합니다. 마이그레이션이 완료되면 Aurora 클러스터 엔드포인트를 가리키도록 데이터베이스의 Route 53 항목을 업데이트하고 온프레미스 데이터베이스를 종료합니다.

D. 데이터베이스의 백업을 생성하고 이를 Amazon Aurora 멀티 마스터 클러스터로 복원합니다. 이 Aurora 클러스터는 온프레미스 데이터베이스와 함께 마스터-마스터 복제 구성에 있게 됩니다.Aurora 클러스터 엔드포인트를 가리키도록 데이터베이스의 Route 53 항목을 업데이트하고 온프레미스 데이터베이스를 종료합니다.

Answer: C

Q213

회사의 AWS 아키텍처는 현재 각 인스턴스에 저장된 액세스 키와 보안 액세스 키를 사용하여 AWS 서비스에 액세스합니다. 데이터베이스 자격 증명은 각 인스턴스에서 하드 코딩됩니다. 명령줄 원격 액세스를 위한 SSH 키는 보안 Amazon S3 버킷에 저장됩니다. 이 회사는 솔루션 설계자에게 운영을 복잡하게 추가하지 않고 아키텍처의 보안 상태를 개선하도록 요청했습니다.

솔루션 설계자는 이 작업을 수행하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. IAM 역할과 함께 Amazon EC2 인스턴스 프로필을 사용합니다.

B. AWS 보안 관리자를 사용하여 액세스 키와 보안 액세스 키를 저장합니다.

C. AWS Systems Manager 파라미터 스토어를 사용하여 데이터베이스 자격 증명을 저장합니다.

D. 원격 액세스를 위해 안전한 Amazon EC2 배스천 호스트 플릿을 사용합니다.

E. AWS KMS를 사용하여 데이터베이스 자격 증명을 저장합니다.

F. 원격 액세스를 위해 AWS 시스템 관리자 세션 관리자를 사용합니다.

Answer: A, C, F

Q214

글로벌 지사를 보유한 회사는 단일 AWS 리전에 대한 단일 1Gbps AWS Direct Connect 연결을 사용합니다. 회사의 온프레미스 네트워크는 연결을 사용하여 AWS 클라우드에 있는 회사 리소스와 통신합니다. 연결에는 단일 VPC에 연결되는 단일 프라이빗 가상 인터페이스가 있습니다. 솔루션 설계자는 동일한 리전에 중복 Direct Connect 연결을 추가하는 솔루션을 구현해야 합니다. 또한 이 솔루션은 회사가 다른 지역으로 확장됨에 따라 동일한 Direct Connect 연결 쌍을 통해 다른 지역에 대한 연결을 제공해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 직접 연결 게이트웨이를 프로비저닝합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다. 두 번째 직접 연결 연결을 만듭니다. 각 연결에 새 프라이빗 가상 인터레이스를 생성하고 두 프라이빗 가상 인터페이스를 모두 Direct Connect 게이트웨이에 연결합니다. 직접 연결 게이트웨이를 단일 VPC에 연결합니다.

B. 기존 프라이빗 가상 인터페이스를 유지합니다. 두 번째 직접 연결 연결을 만듭니다.새 연결에 새 프라이빗 가상 인터페이스를 생성하고 새 프라이빗 가상 인터페이스를 단일 VPC에 연결합니다.

C. 기존 프라이빗 가상 인터페이스를 유지합니다. 두 번째 직접 연결 연결을 만듭니다. 새 연결에 새 퍼블릭 가상 인터페이스를 생성하고 새 퍼블릭 가상 인터페이스를 단일 VPC에 연결합니다.

D. 전송 게이트웨이를 프로비저닝합니다. 기존 연결에서 기존 프라이빗 가상 인터페이스를 삭제합니다.두 번째 직접 연결 연결을 만듭니다. 각 연결에 새 프라이빗 가상 인터페이스를 생성하고 두 프라이빗 가상 인터페이스를 모두 전송 게이트웨이에 연결합니다. 전송 게이트웨이를 단일 VPC와 연결합니다.

Answer: A

Q215

한 회사의 솔루션 설계자가 AWS에서 실행되는 애플리케이션을 위한 재해 복구 (DR) 솔루션을 설계하고 있습니다. 이 애플리케이션은 PostgreSQL 11.7을 데이터베이스로 사용합니다. 회사의 PRO(복구 지점 목표)는 30 초입니다. 솔루션 설계자는 us-east-1 리전의 기본 데이터베이스와 us-west-2 리전의 데이터베이스를 사용하여 DR 솔루션을 설계해야 합니다.

애플리케이션 변경을 최소화하면서 이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. us-east-1의 PostgreSQL용 Amazon RDS로 데이터베이스를 마이그레이션합니다. us-west-2에서 읽기 전용 복제본을 설정하여 읽기 전용 복제본을 설정합니다. RDS 데이터베이스의 관리형 PRO를 30초로 설정합니다.

B. us-east-1의 PostgreSQL을 위해 데이터베이스를 Amazon으로 마이그레이션합니다. us-west-2의 가용 영역에 예비 복제본을 설정하고 RDS 데이터베이스의 관리형 PRO를 30초로 설정합니다.

C. 기본 리전은 us-east-1이고 보조 리전은 us-west-2인 Amazon Aurora PostgreSQL 글로벌 데이터베이스로 데이터베이스를 마이그레이션합니다. Aurora 데이터베이스의 관리형 PRO를 30초로 설정합니다.

D. 데이터베이스를 us-east-1의 Amazon DynamoDB로 마이그레이션합니다. us-west-2에서 생성된 복제본 테이블로 전역 테이블을 설정합니다.

Answer: C

https://aws.amazon.com/ko/about-aws/whats-new/2020/06/amazon-aurora-postgresql-global-database-supports-managed-recovery-point-objective-RPO/?nc1=h\_ls

Q216

회사는 사진 공유를 위한 소셜 네트워킹 애플리케이션을 보유하고 있습니다. 균일한 사용자 경험을 제공하기 위해 비즈니스는 사용자가 업로드한 사진을 프로그램에 게시하기 전에 일부 이미지 처리를 수행합니다. 이미지 처리는 Python 라이브러리 모음을 사용하여 수행됩니다.

현재 아키텍처는 다음과 같습니다.

\* 이미지 처리 파이썬 코드는 단일 Amazon EC2 인스턴스에서 실행되며 처리된 이미지를 ImageBucket이라는 Amazon S3 버킷에 저장합니다.

\* 다른 버킷에서 호스팅되는 프런트 엔드 애플리케이션은 ImageBucket에서 이미지를 로드하여 사용자에게 표시합니다.

전 세계적인 개발 목표를 가지고 있는 이 회사는 더 높은 수요에 맞게 애플리케이션을 확장하는 동시에 프로그램이 성장함에 따라 관리 복잡성을 줄이기 위해 현재 아키텍처를 수정하고자 합니다.

솔루션 설계자는 어떤 조정을 함께 수행해야 합니까?(두 개 선택)

A. 이미지 처리 EC2 인스턴스를 Auto Scaling 그룹에 배치합니다.

B. Amazon ECS 클러스터에 애플리케이션을 배포하고 서비스 오토 스케일링을 적용합니다.

C. AWS Lambda를 사용하여 이미지 처리 작업을 실행합니다.

D. 이미지버킷(ImageBucket) 앞에서 Amazon CloudFront를 사용합니다.

E. 이미지 처리에 Amazon 인식(Amazon Rekognition)을 사용합니다.

Answer: C, D

설명

명확하게 문서화되지는 않았지만 이미지 처리 작업은 Lambda 함수의 최대 실행 시간(15분)보다 짧을 수 있습니다. 따라서 Lambda는 더 비용 효율적일 수 있고 확장성이 뛰어납니다.

Amazon CloudFront는 처리된 이미지가 있는 S3 버킷으로 구성된 오리진과 함께 사용할 수 있습니다. 이렇게 하면 여러 지역의 앱 사용자가 엣지 로케이션에 캐시된 이미지를 뛰어난 성능으로 검색할 수 있으므로 더 나은 사용자 경험을 제공할 수 있습니다.

잘못됨: A. 이것은 약간의 개선을 제공하지만 Lambda만큼 개선을 나타내지는 않습니다. Lambda는 이 애플리케이션에 대해 매우 잘 확장될 것입니다.

잘못됨: B. 이것은 또한 이미지 처리에 유효한 솔루션이지만 Lambda보다 비용 효율적입니다.

잘못됨: E. 질문은 이미지가 "일관성"을 위해 처리되고 있음을 나타냅니다. 이것은 모호하지만 개체를 ​​식별하거나 Rekognition이 수행하는 분석 유형을 수행한다는 의미는 아닙니다.

참조:

https://aws.amazon.com/lambda/features/

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html

Q217

한 회사에서 온프레미스에서 AWS 클라우드로 애플리케이션을 마이그레이션할 계획입니다. 이 회사는 애플리케이션의 기본 데이터 스토리지를 AWS로 이전하여 마이그레이션을 시작합니다. 애플리케이션 데이터는 온프레미스의 공유 시스템에 저장되고 애플리케이션 서버는 SMB를 통해 공유 웹 시스템에 연결됩니다. 솔루션 설계자는 공유 스토리지에 Amazon S3 버킷을 사용하는 솔루션을 구현해야 합니다.

애플리케이션이 완전히 마이그레이션되고 네이티브 Amazon S3 API를 사용하도록 코드를 다시 작성할 때까지 애플리케이션은 SMB를 통해 데이터에 계속 액세스할 수 있어야 합니다. 솔루션 설계자는 애플리케이션 데이터를 AWS로 새 위치로 마이그레이션하는 동시에 온프레미스 애플리케이션이 데이터에 액세스할 수 있도록 허용해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. Windows용 Amazon FSx 파일 서버 파일 시스템을 새로 생성합니다. 온프레미스 파일 공유를 위한 위치 하나와 새 Amazon FSx 파일 시스템을 위한 하나의 위치로 AWS DataSync를 구성합니다. 온프레미스 파일 공유 위치에서 Amazon FSx 파일 시스템으로 데이터를 복사하는 새 DataSync 작업을 생성합니다.

B. 애플리케이션용 S3 버킷을 생성합니다. 온프레미스 스토리지에서 S3 버킷으로 데이터를 복사합니다.

C. AWS Server Migration Service (AWS SMS) VM을 온프레미스 환경에 배포합니다. AWS SMS를 사용하여 온프레미스에서 Amazon EC2 인스턴스로 파일 스토리지 서버를 마이그레이션합니다.

D. 애플리케이션용 S3 버킷을 생성합니다. 온프레미스 VM에 새 AWS Storage Gateway 파일 게이트웨이를 배포합니다. S3 버킷에 데이터를 저장하고 파일 게이트웨이와 연결된 새 파일 공유를 생성합니다. 온프레미스 스토리지의 데이터를 새 파일 게이트웨이 엔드포인트로 복사합니다.

Answer: D

Q218

한 회사가 설정의 일부로 새 웹 애플리케이션을 배포하고, Amazon Kinesis 데이터 파이어호스를 통해 Amazon S3에 로그인하도록 AWS WAF를 구성합니다. 이 회사는 지난 24시간의 AWS WAF 로그 데이터를 반환하기 위해 매일 한 번 실행되는 Amazon Athena 쿼리를 개발합니다. 일별 로그의 양은 일정하지만 시간이 지남에 따라 동일한 쿼리를 실행하는 데 더 많은 시간이 걸립니다. 솔루션 설계자는 쿼리 시간이 계속 늘어나지 않도록 솔루션을 설계해야 합니다. 솔루션은 운영 오버헤드를 최소화해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 매일의 AWS WAF 로그를 하나의 로그 파일로 통합하는 AWS Lambda 함수를 생성합니다.

B. 매일 다른 S3 버킷으로 로그를 전송하도록 AWS WAF를 구성하여 스캔되는 데이터의 양을 줄입니다.

C. Kinesis Data Firehose 구성을 업데이트하여 Amazon S3의 데이터를 날짜 및 시간별로 분할합니다. Amazon Redshift용 외부 테이블을 생성합니다. 데이터 소스를 쿼리하도록 Amazon Redshift 스펙트럼을 구성합니다.

D. Kinesis Data Firehose 구성 및 Athena 테이블 정의를 수정하여 날짜 및 시간별로 데이터를 분할합니다. Athena 쿼리를 변경하여 관련 파티션을 봅니다.

Answer: D

Q219

한 회사에서 직원이 VPN을 사용하여 연결하는 경우 집에서 원격으로 작업할 수 있도록 허용하는 새로운 정책을 도입했습니다. 이 회사는 여러 AWS 계정에서 VPC가 있는 내부 애플리케이션을 호스팅하고 있습니다.현재 AWS 사이트 간 VPN 연결을 통해 회사의 온프레미스 사무실 네트워크에서 애플리케이션에 액세스할 수 있습니다. 회사의 기본 AWS 계정에 있는 VPC에는 다른 AWS 계정의 VPC와 피어링 연결이 설정되어 있습니다. 솔루션 설계자는 직원들이 집에서 일하는 동안 사용할 수 있도록 확장 가능한 AWS Client VPN 솔루션을 설계해야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 솔루션은 무엇입니까?

A. 각 AWS 계정에 클라이언트 VPN 엔드포인트 생성 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.

B. mam AWS 계정에서 클라이언트 VPN 엔드포인트 생성 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.

C. 기본 AWS 계정에 클라이언트 VPN 엔드포인트 생성 각 AWS 계정에 연결된 전송 게이트웨이를 프로비저닝합니다. 내부 애플리케이션에 대한 액세스를 허용하는 필수 라우팅을 구성합니다.

D. 기본 AWS 계정에서 클라이언트 VPN 엔드포인트 생성 클라이언트 VPN 엔드포인트와 AWS 사이트 간 VPN 간의 연결을 설정합니다.

Answer: C

Q220

유럽의 한 대기업은 애플리케이션을 AWS 클라우드로 마이그레이션할 계획입니다. 이 회사는 다양한 비즈니스 그룹에 여러 AWS 계정을 사용합니다. 데이터 개인 정보 보호법에 따라 회사는 AWS 유럽 리전에만 개발자의 액세스를 제한해야 합니다.

최소한의 관리 오버헤드로 이 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 각 계정에서 IAM 사용자와 IAM 그룹을 생성합니다. 비유럽 리전에 대한 액세스를 제한하는 IAM 정책을 생성합니다. IAM 정책을 IAM 그룹에 연결합니다.

B. AWS 조직을 활성화하고, AWS 계정을 연결하고, 유럽 리전 및 비유럽 리전에 대한 OU를 생성합니다. SCP를 생성하여 비유럽 지역에 대한 액세스를 제한하고 정책을 OU에 연결합니다.

C. AWS 싱글 사인온을 설정하고 AWS 계정을 연결합니다. 비유럽 리전에 대한 액세스를 제한하는 정책을 사용하여 권한 집합을 생성합니다. 각 계정에 IAM 사용자 및 IAM 그룹을 생성합니다.

D. AWS 조직을 활성화하고, AWS 계정을 연결하고, 유럽 리전 및 비유럽 리전에 대한 OU를 생성합니다. 비유럽 지역에 대한 액세스를 제한하는 정책을 사용하여 권한 집합을 만듭니다. 기본 계정에서 IAM 사용자 및 IAM 그룹을 생성합니다.

Answer: B

Q221

한 회사에는 AWS 조직 내 조직의 멤버인 50개의 AWS 계정이 있습니다. 각 계정에는 여러 개의 VPC가 포함됩니다. 이 회사는 AWS Transit Gateway를 사용하여 각 멤버 계정의 VPC 간에 연결을 설정하려고 합니다. 새 멤버 계정이 생성될 때마다 새 VPC 및 전송 게이트웨이 연결을 생성하는 프로세스를 자동화하려고 합니다.

이러한 요구 사항을 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. 관리 계정에서 AWS 리소스 액세스 관리자를 사용하여 전송 게이트웨이를 멤버 계정과 공유합니다.

B. 관리 계정에서 AWS Organizations의 SCP를 사용하여 전송 게이트웨이를 멤버 계정과 공유합니다.

C. 멤버 계정에 새 VPC와 VPC 전송 게이트웨이 연결을 자동으로 생성하는 관리 계정에서 AWS CloudFormation 스택 세트를 시작합니다. 전송 게이트웨이 ID를 사용하여 첨부 파일을 관리 계정의 전송 게이트웨이와 연결합니다.

D. 멤버 계정에 새 VPC와 피어링 전송 게이트웨이 연결을 자동으로 생성하는 관리 계정에서 AWS CloudFormation 스택 세트를 시작합니다. 전송 게이트웨이 서비스 연결 역할을 사용하여 관리 계정의 전송 게이트웨이와 첨부 파일을 공유합니다.

E. 관리 계정에서 AWS Service Catalog를 사용하여 전송 게이트웨이를 멤버 계정과 공유합니다.

Answer: A, C

https://www.examtopics.com/discussions/amazon/view/60090-exam-aws-certified-solutions-architect-professional-topic-1/

Q222

데이터 분석 회사에는 여러 개의 예약 노드로 구성된 Amazon Redshift 클러스터가 있습니다. 직원 팀이 심층 감사 분석 보고서를 작성하고 있기 때문에 살포기가 예상치 못한 사용량이 급증하고 있습니다. 보고서를 생성하는 쿼리는 복잡한 읽기 쿼리이며 CPU를 많이 사용합니다.비즈니스 요구 사항에 따라 클러스터는 시간에 읽기 및 쓰기 쿼리를 처리할 수 있어야 합니다.

솔루션 설계자는 폭증하는 사용량을 수용할 수 있는 솔루션을 고안해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. Amazon EMR 클러스터를 프로비저닝합니다. 복잡한 데이터 처리 작업을 오프로드합니다.

B. Amazon CloudWatch에서 클러스터의 CPU 지표가 80% 에 도달할 때 클래식 크기 조정 작업을 사용하여 Amazon Redshift 클러스터에 용량을 추가할 수 있도록 AWS Lambda 함수를 배포합니다.

C. Amazon CloudWatch에서 클러스터의 CPU 지표가 80% 를 초과하는 경우 탄력적 크기 조정 작업을 사용하여 Amazon Redshift 클러스터에 용량을 추가하는 AWS Lambda 함수를 배포합니다.

D. Amazon Redshift 클러스터에 대한 동시성 확장 기능을 켭니다.

Answer: D

Q223

한 회사가 AWS 클라우드에서 온프레미스 주문 처리 플랫폼을 리팩토링하고 있습니다. 이 플랫폼에는 프런트 엔드를 백엔드에 연결하기 위해 VM RabbitMQ 플릿에서 호스팅되는 웹 프런트 엔드와 컨테이너식 백엔드 시스템을 실행하여 주문을 처리하는 Kubernetes 클러스터가 포함되어 있습니다. 회사는 응용 프로그램을 크게 변경하고 싶지 않습니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 웹 서버 VM의 AMI를 생성합니다. AMI와 애플리케이션 로드 밸런서를 사용하는 Amazon EC2 오토 스케일링 그룹을 생성합니다. 온프레미스 메시징 대기열을 대체하도록 Amazon MQ를 설정합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service (Amazon EKS) 를 구성합니다.

B. 사용자 지정 AWS Lambda 런타임을 생성하여 웹 서버 환경을 모방합니다. Amazon API 게이트웨이 API를 생성하여 프런트 엔드 웹 서버를 대체합니다. 온프레미스 메시징 대기열을 대체하도록 Amazon MQ를 설정합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service (Amazon EKS) 를 구성합니다.

C. 웹 서버 VM의 AMI를 생성합니다. AMI와 애플리케이션 로드 밸런서를 사용하는 Amazon EC2 오토 스케일링 그룹을 생성합니다. 온프레미스 메시징 대기열을 교체하도록 Amazon MQ 설정 주문 처리 백엔드를 호스팅할 다양한 EC2 인스턴스 플릿에 Kubernetes를 설치합니다.

D. 웹 서버 VM의 AMI를 생성합니다. AMI와 애플리케이션 로드 밸런서를 사용하는 Amazon EC2 오토 스케일링 그룹을 생성합니다. Amazon Simple Queue Service (Amazon SQS) 대기열을 설정하여 온프레미스 메시징 대기열을 대체합니다. 주문 처리 백엔드를 호스팅하도록 Amazon Elastic Kubernetes Service (Amazon EKS) 를 구성합니다.

Answer: A

Q224

소매업체는 PostgreSQL DB 인스턴스용 Amazon RDS를 사용하는 소규모 전자 상거래 웹 애플리케이션을 보유하고 있습니다. DB 인스턴스는 다중 AZ 옵션이 켜진 상태로 배포됩니다. 최근 애플리케이션 사용량이 기하급수적으로 증가했으며 사용자는 HTTP 503 오류를 자주 경험했습니다. 사용자가 오류를 보고했으며 회사의 명성은 떨어졌습니다. 회사는 확실한 근본 원인을 파악할 수 없었습니다. 이 회사는 운영 준비 상태를 개선하고 사용자가 사고를 발견하기 전에 경고를 받기를 원합니다. 또한 향후 사고의 근본 원인을 파악하기 위해 충분한 정보를 수집하려고 합니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. DB 인스턴스에 대해 향상된 모니터링 설정 해당 파라미터 그룹을 수정하여 모든 느린 쿼리에 대해 쿼리 로깅을 켭니다. Amazon CloudWatch 경보를 생성합니다. CloudWatch의 성능 지표를 기반으로 하는 적절한 임계값으로 경보를 설정합니다.

B. DB 인스턴스에 대해 향상된 모니터링 및 성능 통찰력을 켭니다. Amazon CloudWatch 경보 생성. CloudWatch의 성능 지표를 기반으로 하는 적절한 임계값으로 경보를 설정합니다.

C. DB 인스턴스의 PostgreSQL 로그에 대해 Amazon CloudWatch로 로그 내보내기를 켭니다. Amazon Elasticsearch Service (Amazon ES) 및 키바나(Kibana)를 사용하여 로그를 분석합니다. Kibana에서 대시보드를 만듭니다. 수집된 지표를 기반으로 하는 경고를 구성합니다.

D. DB 인스턴스에 대해 성능 인사이트 설정 해당 파라미터 그룹을 수정하여 모든 느린 쿼리에 대해 쿼리 로깅을 켭니다. Amazon CloudWatch 경보를 생성합니다. CloudWatch의 성능 지표를 기반으로 하는 적절한 임계값으로 경보를 설정합니다.

Answer: A

Q225

회사는 사용 기간 동안 동일한 물리적 호스트에서 실행해야 하는 라이센스가 있는 소프트웨어 패키지를 실행해야 합니다. 소프트웨어 패키지는 90일 동안만 사용됩니다. 이 회사는 30일마다 모든 인스턴스에 패치를 적용하고 다시 시작해야 합니다.

AWS를 사용하여 이러한 요구 사항을 충족하려면 어떻게 해야 합니까?

A. 자동 배치가 비활성화된 전용 인스턴스를 실행합니다.

B. 호스트 선호도가 호스트로 설정된 전용 호스트에서 인스턴스를 실행합니다.

C. 예약 인스턴스와 함께 온디맨드 인스턴스를 실행하여 일관된 배치를 보장합니다.

D. 종료가 90일 동안 설정된 라이선스가 부여된 호스트에서 인스턴스를 실행합니다.

Answer: B

Q226

연구 기관과 병원 그룹이 2PB의 게놈 데이터를 연구하기 위해 파트너십을 맺고 있습니다. 데이터를 소유한 기관은 데이터를 Amazon S3 버킷에 저장하고 정기적으로 업데이트합니다. 연구소는 파트너십의 모든 조직에 데이터에 대한 읽기 액세스 권한을 부여하고자 합니다. 파트너십의 모든 구성원은 비용에 매우 민감하며 S3 버킷으로 계정을 소유한 기관은 Amazon S3의 요청 및 데이터 전송 비용을 부담하는 것에 대해 우려하고 있습니다.

버킷을 소유한 기관이 S3 요청 및 데이터 전송에 대한 모든 비용을 부담하지 않으면서 데이터를 안전하게 공유할 수 있는 솔루션은 무엇입니까?

A. 파트너십의 모든 조직에 AWS 계정이 있는지 확인합니다. S3 버킷이 있는 계정에서 파트너쉽의 각 계정에 대해 데이터에 대한 읽기 액세스를 허용하는 교차 계정 역할을 생성합니다. 조직이 데이터에 액세스할 때 해당 읽기 역할을 가정하고 사용하도록 합니다.

B. 파트너십의 모든 조직에 AWS 계정이 있는지 확인합니다. 데이터를 소유하는 버킷에 버킷 정책을 생성합니다. 이 정책은 파트너쉽의 계정이 버킷에 대한 읽기 액세스 권한을 허용해야 합니다. 버킷에서 요청자 지불을 활성화합니다.조직이 데이터에 액세스할 때 AWS 자격 증명을 사용하도록 합니다.

C. 파트너십의 모든 조직에 AWS 계정이 있는지 확인합니다. 데이터를 소유한 기관이 버킷에 쓸 수 있도록 허용하는 버킷 정책을 사용하여 각 계정의 버킷을 구성합니다. 연구소 계정의 데이터를 다른 조직과 주기적으로 동기화합니다. 조직이 계정을 사용하여 데이터에 액세스할 때 AWS 자격 증명을 사용하도록 합니다.

D. 파트너십의 모든 조직에 AWS 계정이 있는지 확인합니다. S3 버킷이 있는 계정에서 파트너쉽의 각 계정에 대해 데이터에 대한 읽기 액세스를 허용하는 교차 계정 역할을 생성합니다. 버킷에서 요청자 지불을 활성화합니다.조직이 데이터에 액세스할 때 해당 읽기 역할을 가정하고 사용하도록 합니다.

Answer: B

Q227

경매 웹 사이트를 통해 사용자는 수집품에 입찰할 수 있습니다. 경매 규칙에 따라 각 입찰은 접수된 순서대로 한 번만 처리되어야 합니다. 현재 구현은 Amazon Kinesis 데이터 스트림에 입찰 레코드를 쓰는 Amazon EC2 웹 서버 플릿을 기반으로 합니다. 단일 12개의 대형 인스턴스에는 Kinesis 데이터 스트림에서 수신되는 입찰을 읽고 각 입찰을 처리하는 입찰 프로세서를 실행하는 cron 작업이 있습니다. 경매 사이트의 인기가 높아지고 있지만 사용자가 일부 입찰이 등록되지 않는다고 불평하고 있습니다. 문제 해결은 피크 수요 시간 동안 입찰 프로세서가 너무 느리다는 것을 나타냅니다.

입찰 처리의 신뢰성을 높일 수 있는 변경 사항은 무엇입니까?

A. Kinesis 데이터 스트림에 입찰을 게시할 때 Amazon Kinesis 생산자 라이브러리 (KPL) 를 사용하도록 웹 애플리케이션을 리팩토링합니다. 입찰 프로세서를 리팩토링하여 Kinesis Data Streams의 각 레코드가 읽지 않음, 처리 및 처리된 것으로 플래그를 지정합니다. 각 입찰 처리 실행을 시작할 때 Kinesis 데이터 스트림에서 처리되지 않은 레코드를 스캔합니다.

B. 웹 애플리케이션을 리팩토링하여 각 수신 입찰을 Kinesis 데이터 스트림 대신 Amazon SNS 주제에 게시합니다. 사용자가 입찰을 제출하는 즉시 각 입찰을 처리하는 AWS Lambda 함수를 트리거하도록 SNS 주제를 구성합니다.

C. 웹 애플리케이션을 리팩토링하여 각 수신 입찰을 Kinesis 데이터 스트림 대신 Amazon SQS FIFO 대기열에 게시합니다. 입찰 프로세서를 계속해서 SQS 대기열로 리팩토링합니다. 입찰 처리 EC2 인스턴스를 최소 및 최대 크기가 1인 Auto Scaling 그룹에 배치합니다.

D. EC2 인스턴스 유형을 t2.large에서 더 큰 일반 컴퓨팅 인스턴스 유형으로 전환합니다. Kinesis 데이터 스트림의 IncomingRecords 지표를 기반으로 입찰 프로세서를 실행하는 EC2 인스턴스 수를 확장하는 Auto Scaling 그룹에 입찰 프로세서 EC2 인스턴스를 배치합니다.

Answer: C

Q228

한 회사에서 Amazon EC2 Linux 인스턴스에서 상태 비저장 전용 ETL 애플리케이션을 실행합니다. 응용 프로그램이 Linux 바이너리이므로 소스 코드를 수정할 수 없습니다. 이 응용 프로그램은 단일 스레드이며 2GB RAM을 사용합니다. CPU를 많이 사용합니다. 응용 프로그램은 4시간마다 실행되도록 예약되고 최대 20분 동안 실행됩니다. 한 솔루션 설계자가 솔루션의 아키텍처를 수정하려고 합니다.

솔루션 설계자는 어떤 전략을 사용해야 합니까?

A. AWS Lambda를 사용하여 애플리케이션을 실행합니다. Amazon CloudWatch 로그를 사용하여 4시간마다 Lambda 함수를 호출합니다.

B. AWS Batch를 사용하여 애플리케이션 실행 AWS 단계 함수 상태 머신을 사용하여 4시간마다 AWS Batch 작업을 호출합니다.

C. AWS Fargate를 사용하여 애플리케이션 실행 Amazon EventBridge (Amazon CloudWatch Events) 를 사용하여 4시간마다 Fargate 작업을 호출합니다.

D. Amazon EC2 스팟 인스턴스를 사용하여 애플리케이션 실행 AWS CodeDepToy를 사용하여 4시간마다 애플리케이션을 배포하고 실행합니다.

Answer: B

Q229

회사는 AWS에서 실행 중인 내부 애플리케이션을 보유하고 있으며, 이 애플리케이션은 회사 웨어하우스에서 배송을 추적하고 처리하는 데 사용됩니다. 현재 시스템은 주문을 받은 후 직원에게 패키지 배송에 필요한 정보를 이메일로 보냅니다. 패키지가 배송되면 직원이 이메일에 회신하고 주문이 배송됨으로 표시됩니다. 이 회사는 애플리케이션에서 이메일 사용을 중단하고 서버리스 애플리케이션 모델로 전환하려고 합니다.

이러한 요구 사항을 충족하는 아키텍처 솔루션은 무엇입니까?

A. AWS Batch를 사용하여 패키지를 배송하는 데 필요한 다양한 작업을 구성합니다. AWS Batch에서 배송 레이블을 생성하고 인쇄하는 AWS Lambda 함수를 트리거하도록 합니다. 레이블이 스캔되면 웨어하우스를 떠날 때 다른 Lambda 함수가 프로세스를 AWS Batch 작업의 다음 단계로 이동하게 합니다.

B. 새 주문이 생성되면 Amazon SQS에 주문 정보를 저장합니다. AWS Lambda가 5분마다 대기열을 확인하고 필요한 작업을 처리하도록 합니다. 주문을 배송해야 하는 경우 Lambda가 웨어하우스에 라벨을 인쇄하도록 합니다. 라벨을 스캔한 후 웨어하우스를 떠날 때 Amazon EC2 인스턴스가 Amazon SQS를 업데이트하도록 합니다.

C. 애플리케이션을 업데이트하여 Amazon DynamoDB에 새 주문 정보를 저장합니다. 새 주문이 생성되면 AWS Step Functions 워크플로를 트리거하고 주문을 “진행 중”으로 표시한 다음 웨어하우스에 패키지 레이블을 인쇄합니다. 라벨이 스캔되고 이행되면 애플리케이션은 주문을 배송됨으로 표시하고 워크플로를 완료하는 AWS Lambda 함수를 트리거합니다.

D. Amazon EFS에 새 주문 정보를 저장합니다. 인스턴스가 NFS에서 새 정보를 가져와 해당 정보를 웨어하우스의 프린터로 보내도록 합니다. 라벨이 스캔되면 웨어하우스를 떠날 때 Amazon API Gateway가 인스턴스를 호출하여 Amazon EFS에서 주문 정보를 제거하도록 합니다.

Answer: C

Q230

한 회사에서 Amazon EC2 인스턴스를 사용하여 블로그 사이트를 호스팅할 웹 플릿을 배포했습니다. EC2 인스턴스는 애플리케이션 로드 밸런서 (ALB) 뒤에 있으며 Auto Scaling 그룹에서 구성됩니다. 웹 애플리케이션은 모든 블로그 콘텐츠를 Amazon EFS 볼륨에 저장합니다. 이 회사는 최근 블로거가 게시물에 비디오를 추가하는 기능을 추가하여 이전 사용자 트래픽의 10 배를 끌어 들였습니다. 사용자는 사이트에 도달하거나 비디오를 보는 동안 버퍼링 및 시간 초과 문제를보고합니다.

사용자의 문제를 해결하는 데 가장 비용 효율적이고 확장 가능한 배포는 무엇입니까?

A. 최대 I/O를 활성화하도록 Amazon EFS를 재구성합니다.

B. 스토리지로 인스턴스 스토어 볼륨을 사용하도록 블로그 사이트를 업데이트합니다. 시작 시 볼륨에 사이트 콘텐츠를 복사하고 종료 시 Amazon S3에 복사합니다.

C. Amazon CloudFront 배포를 구성합니다. 배포를 S3 버킷으로 지정하고 비디오를 EFS에서 Amazon S3로 마이그레이션합니다.

D. 모든 사이트 콘텐츠에 대해 Amazon CloudFront 배포를 설정하고 배포를 ALB로 지정합니다.

Answer: C

Q231

한 회사는 AWS 조직을 통해 생성된 조직의 일원으로 여러 AWS 계정을 보유하고 있습니다. 각 계정에는 us-east-2 리전에 VPC가 있으며 프로덕션 또는 개발 워크로드에 사용됩니다. 프로덕션 계정 전체의 Amazon EC2 인스턴스는 서로 통신해야 하며 개발 계정 전체의 EC2 인스턴스는 서로 통신해야 하지만 프로덕션 인스턴스와 개발 인스턴스는 서로 통신할 수 없습니다. 연결을 용이하게 하기 위해 회사는 공통 네트워크 계정을 만들었습니다. 이 회사는 AWS Transit Gateway를 사용하여 네트워크 계정의 us-east-2 리전에 전송 게이트웨이를 생성하고 AWS 리소스 액세스 관리자를 사용하여 전체 조직과 전송 게이트웨이를 공유했습니다. 그런 다음 네트워크 관리자는 각 계정의 VPC를 전송 게이트웨이에 연결한 후 EC2 인스턴스가 계정 간에 통신할 수 있게 되었습니다. 그러나 생산 및 개발 계정도 서로 통신할 수 있었습니다.

프로덕션 트래픽과 개발 트래픽이 완전히 격리되도록 솔루션 설계자는 어떤 단계를 수행해야 합니까?

A. 개발 EC2 인스턴스에 할당된 보안 그룹을 수정하여 프로덕션 EC2 인스턴스의 트래픽을 차단합니다. 프로덕션 EC2 인스턴스에 할당된 보안 그룹을 수정하여 개발 EC2 인스턴스의 트래픽을 차단합니다.

B. 연결할 계정 유형에 따라 각 VPC 연결에서 프로덕션 또는 개발 중 하나의 값으로 태그를 생성합니다. AWS Transit Gateway의 네트워크 관리자 기능을 사용하여 이 태그의 값에 따라 VPC 간 트래픽을 제한하는 정책을 생성합니다.

C. 프로덕션 및 개발 트래픽에 대해 별도의 라우팅 테이블을 생성합니다. 각 계정의 연결 및 기본 AWS Transit Gateway 라우팅 테이블에 대한 경로 전파를 삭제합니다. 개발 VPC를 개발 AWS Transit Gateway 라우팅 테이블에 연결하고 프로덕션 VPC를 프로덕션 라우팅 테이블에 연결하고 각 연결에서 자동 경로 전파를 활성화합니다.

D. 연결할 계정 유형에 따라 각 VPC 연결에서 프로덕션 또는 개발 중 하나의 값으로 태그를 생성합니다. 프로덕션 태그가 지정된 첨부 파일을 서로 라우팅하고 개발 태그가 지정된 첨부 파일을 서로 라우팅하도록 AWS Transit Gateway 라우팅 테이블을 수정합니다.

Answer: C

Q232

수백 개의 AWS 계정을 보유한 대규모 조직은 최근 새 예약 인스턴스를 구입하거나 이전 인스턴스를 업데이트하기 위한 표준화된 내부 절차를 개발했습니다. 이 접근 방식을 사용하려면 예약 인스턴스를 구매하거나 수정하는 데 관심이 있는 모든 사업부에서 구매 또는 실행 요청을 전담팀에 제출해야 합니다. 이전에는 비즈니스 부서가 자체 AWS 계정에서 독립적으로 예약 인스턴스를 구매하거나 수정했습니다.

가능한 가장 안전한 방식으로 새로운 절차를 사전에 시행하기 위해 어떤 활동을 조합해야 합니까?(두 개 선택)

A. 모든 AWS 계정이 모든 기능 모드에서 작동하는 AWS Organizations 구조의 일부인지 확인하십시오.

B. AWS Config를 사용하여 ec2:PurchaseReservedInstancesOffering 및 ec2:ModifyReservedInstances 작업에 대한 액세스를 거부하는 IAM 정책 연결에 대해 보고합니다.

C. 각 AWS 계정에서 ec2:PurchaseReservedInstancesOffering 및 ec2:ModifyReservedInstances 작업에 대한 DENY 규칙이 있는 IAM 정책을 생성합니다.

D. ec2:PurchaseReservedInstancesOffering 및 ec2:ModifyReservedInstances 작업에 대한 거부 규칙이 포함된 SCP를 만듭니다. SCP를 AWS Organizations 구조의 각 OU(조직 구성 단위)에 연결합니다.

E. 모든 AWS 계정이 통합 결제 기능 모드에서 작동하는 AWS Organizations 구조의 일부인지 확인합니다.

Answer: A, D

설명

기존 및 향후 구성원 계정 모두에 대해 작동하는 유일한 솔루션은 조직의 루트에 거부 정책을 적용하는 것입니다. 정책을 조직 루트에 연결하면 조직의 모든 OU 및 계정이 해당 정책을 상속하므로 추가되는 모든 새 계정이 자동으로 정책을 상속합니다.

SCP는 조직의 구성원 계정에만 영향을 줍니다. 관리 계정(마스터 계정이라고도 함)의 사용자 또는 역할에는 영향을 주지 않습니다. 따라서 관리 계정의 사용자는 예약 인스턴스를 구매할 수 있습니다.

정책 상속과 관련하여 다음 동작에 유의하십시오.

조직의 조직 엔터티(조직 루트, 조직 단위(OU) 또는 계정)에 정책을 연결할 수 있습니다.

조직 루트에 정책을 연결하면 조직의 모든 OU 및 계정이 해당 정책을 상속합니다.

특정 OU에 정책을 연결하면 해당 OU 또는 모든 하위 OU 바로 아래에 있는 계정이 정책을 상속합니다.

특정 계정에 정책을 연결하면 해당 계정에만 영향을 미칩니다.

Q233

솔루션 설계자가 모바일 장치에서 직원의 작업표 항목을 수락하는 응용 프로그램을 설계하고 있습니다. 작업표는 매주 제출되며 대부분의 제출은 금요일에 진행됩니다. 급여 관리자가 월별 보고서를 실행할 수 있는 형식으로 데이터를 저장해야 합니다. 인프라는 수신되는 데이터 및 보고 요청의 비율에 맞게 가용성과 확장성이 높아야 합니다.

운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. 여러 가용 영역에 걸쳐 로드 밸런싱을 사용하여 Amazon EC2 온디맨드 인스턴스에 애플리케이션을 배포합니다. 예약된 Amazon EC2 Auto Scaling을 사용하여 금요일에 많은 양의 제출이 이루어지기 전에 용량을 추가할 수 있습니다.

B. 여러 가용 영역에 걸쳐 로드 밸런싱과 함께 Amazon Elastic Container Service (Amazon ECS) 를 사용하여 컨테이너에 애플리케이션을 배포합니다. 예약된 Service Auto Scaling을 사용하여 금요일에 많은 양의 제출이 이루어지기 전에 용량을 추가할 수 있습니다.

C. 애플리케이션 프런트 엔드를 Amazon CloudFront에서 제공하는 Amazon S3 버킷에 배포합니다. AWS Lambda 프록시 통합으로 Amazon API Gateway를 사용하여 애플리케이션 백엔드를 배포합니다.

D. 작업표 제출 데이터를 Amazon Redshift에 저장합니다. Amazon Redshift를 데이터 소스로 사용하여 보고서를 생성하려면 Amazon OUickSight를 사용합니다.

E. 작업표 제출 데이터를 Amazon S3에 저장합니다. Amazon Athena와 Amazon OUickSight를 사용하여 Amazon S3를 데이터 소스로 사용하여 보고서를 생성합니다.

Answer: C, E

Q234

한 회사가 AWS에서 빅 데이터 분석을 위한 새 클러스터를 배포하고 있습니다. 클러스터는 여러 가용 영역에 분산되어 있는 여러 Linux Amazon EC2 인스턴스에서 실행됩니다.

클러스터의 모든 노드에는 공통 기본 파일 저장소에 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 스토리지 게이트웨이 파일 게이트웨이 NFS 파일 공유를 프로비저닝합니다. 클러스터의 각 EC2 인스턴스에 NFS 파일 공유를 마운트합니다.

B. 범용 성능 모드를 사용하는 새로운 Amazon Elastic File System (Amazon EFS) 파일 시스템을 프로비저닝합니다. 클러스터의 각 EC2 인스턴스에 EFS 파일 시스템을 마운트합니다.

C. lo2 볼륨 유형을 사용하는 새로운 Amazon Elastic Block Store (Amazon EBS) 볼륨을 프로비저닝합니다. EBS 볼륨을 클러스터의 모든 EC2 인스턴스에 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 마운트합니다.

Answer: D

Q235

한 솔루션스 아키텍트가 AWS Fargate로 워크로드 마이그레이션을 수행하고 있습니다. 작업은 외부에서 애플리케이션에 직접 연결되지 않은 VPC 내부의 프라이빗 서브넷에서만 실행할 수 있습니다.

Fargate 작업이 시작되면 다음 오류가 발생합니다.

CannotPullContainerError: API failure (500): Obtain https://111122223333.dkr.ecr.us-east-IAMazonaws.com/v2/: net/http: net/http: 연결이 설정되기 전에 요청이 중단됨.

이 상황을 바로 잡기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 작업을 시작할 때 공용 IP 자동 할당 설정에 대해 작업이 사용으로 설정되어 있는지 확인합니다.

B. 작업을 시작할 때 공용 IP 자동 할당 설정에 대해 작업이 사용 안 함으로 설정되어 있는지 확인합니다. 요청을 인터넷으로 라우팅하도록 VPC의 퍼블릭 서브넷에 NAT 게이트웨이를 구성합니다.

C. 작업을 시작할 때 공용 IP 자동 할당 설정에 대해 작업이 사용 안 함으로 설정되어 있는지 확인합니다. 요청을 인터넷으로 라우팅하도록 VPC의 프라이빗 서브넷에 NAT 게이트웨이를 구성합니다.

D. Fargate 작업 정의에서 네트워크 모드가 브리지로 설정되어 있는지 확인합니다.

Answer: B

설명

Fargate 작업이 시작되면 탄력적 네트워크 인터페이스에 컨테이너 이미지를 가져오기 위한 인터넷 경로가 필요합니다. 작업을 시작할 때 다음과 유사한 오류가 표시되는 경우 인터넷에 대한 경로가 존재하지 않기 때문입니다.

CannotPullContainerError: API failure (500): Obtain https://111122223333.dkr.ecr.us-east-IAMazonaws.com/v2/: net/http: 연결이 설정되기 전에 요청이 중단됨"

이 문제를 해결하려면 다음을 수행할 수 있습니다.

- 공개 서브넷에 있는 작업의 경우 작업을 시작할 때 공개 IP 자동 할당에 대해 ENABLED를 지정합니다.

- 비공개 서브넷에 있는 작업의 경우 작업을 시작할 때 공개 IP 자동 할당에 대해 비활성화를 지정하고 요청을 인터넷으로 라우팅하도록 VPC에서 NAT 게이트웨이를 구성합니다.

잘못됨: A. 작업이 프라이빗 서브넷에서 실행 중이고 퍼블릭 IP를 선택하지 않기 때문에 이것은 작동하지 않습니다.

잘못됨: C. NAT 게이트웨이는 퍼블릭 서브넷에 있어야 합니다.

참조:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task\_cannot\_pull\_image.html

Q236

한 회사에서 Amazon EC2 오토 스케일링 그룹에 대한 애플리케이션의 CI/CO에 AWS CodePipeline을 사용하고 있습니다. 모든 AWS 리소스는 AWS CloudFormation 템플릿에 정의되어 있습니다. 애플리케이션 아티팩트는 Amazon S3 버킷에 저장되고 인스턴스 사용자 데이터 스크립트를 사용하여 Auto Scaling 그룹에 배포됩니다. 애플리케이션이 더욱 복잡해짐에 따라 Cloud Formation 템플릿의 최근 리소스 변경으로 인해 계획되지 않은 다운타임이 발생했습니다.

솔루션 설계자는 템플릿 변경으로 인해 다운타임이 발생할 가능성을 줄이기 위해 CI'CD 파이프라인을 어떻게 개선해야 합니까?

A. 배포 스크립트를 조정하여 배포를 수행할 때 CloudFormation 오류 상태를 감지하고 보고합니다. 프로덕션 변경을 승인하기 전에 테스트 팀이 비프로덕션 환경에서 실행할 테스트 계획을 작성합니다.

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

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

D. AWS CodeDeploy 및 블루/그린 배포 패턴을 CloudFormation과 함께 사용하여 사용자 데이터 배포 스크립트를 대체합니다. 운영자가 실행 중인 인스턴스에 로그인하고 수동 테스트 계획을 통해 애플리케이션이 예상대로 실행되고 있는지 확인하도록 합니다.

Answer: B

Q237

디지털 마케팅 회사에는 다양한 팀에 속한 여러 AWS 계정이 있습니다. 크리에이티브 팀은 AWS 계정의 Amazon S3 버킷을 사용하여 회사 마케팅 캠페인의 콘텐츠로 사용되는 이미지와 미디어 파일을 안전하게 저장합니다. 크리에이티브 팀은 전략 팀이 객체를 볼 수 있도록 S3 버킷을 전략 팀과 공유하려고 합니다. 솔루션 설계자가 전략 계정에서 strategy\_reviewer라는 이름의 IAM 역할을 생성했습니다. 또한 솔루션스 아키텍트는 크리에이티브 계정에 사용자 지정 AWS 키 관리 서비스 (AWS KMS) 키를 설정하고 이 키를 S3 버킷과 연결했습니다. 하지만 Strategy 계정의 사용자가 IAM 역할을 수임하고 S3 버킷의 객체에 액세스하려고 하면 계정을 받게 됩니다. 솔루션스 아키텍트는 Strategy 계정의 사용자가 S3 버킷에 액세스할 수 있도록 해야 합니다. 솔루션은 이러한 사용자에게 필요한 최소 권한만 제공해야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. S3 버킷에 대한 읽기 권한이 포함된 버킷 정책을 생성합니다. 버킷 정책의 보안 주체를 Strategy 계정의 계정 ID로 설정합니다.

B. strategy\_reviewer IAM 역할을 업데이트하여 S3 버킷에 대한 모든 권한을 부여하고 사용자 지정 KMS 키에 대한 암호 해독 권한을 부여합니다.

C. 크리에이티브 계정에서 사용자 지정 KMS 키 정책을 업데이트하여 strategy\_reviewer IAM 역할에 암호 해독 권한을 부여합니다.

D. S3 버킷에 대한 읽기 권한이 포함된 버킷 정책을 생성합니다. 버킷 정책의 보안 주체를 익명 사용자로 설정합니다.

E. 크리에이티브 계정에서 사용자 지정 KMS 키 정책을 업데이트하여 strategy\_reviewer IAM 역할에 암호화 권한을 부여합니다.

F. strategy\_reviewer IAM 역할을 업데이트하여 S3 버킷에 대한 읽기 권한을 부여하고 사용자 지정 KMS 키에 대한 암호 해독 권한을 부여합니다.

Answer: A, C, F

Q238

한 회사가 온라인으로 티켓을 판매하고 7일마다 수요가 급증하는 애플리케이션을 보유하고 있습니다. 이 애플리케이션에는 Amazon EC2에서 실행되는 상태 비저장 프레젠테이션 계층, 비정형 데이터 카탈로그 정보를 저장하는 Oracle 데이터베이스 및 백엔드 API 계층이 있습니다.프런트 엔드 계층은 탄력적 로드 밸런서를 사용하여 3개의 가용 영역 (AZ) 에 걸쳐 9개의 온디맨드 인스턴스에 부하를 분산합니다. Oracle 데이터베이스는 단일 EC2 인스턴스에서 실행됩니다. 이 회사는 두 개 이상의 동시 캠페인을 실행할 때 성능 문제를 겪고 있습니다. 솔루션 설계자는 다음 요구 사항을 충족하는 솔루션을 설계해야 합니다.

\* 확장성 문제를 해결합니다.

\* 동시성 수준을 높입니다.

\* 라이선스 비용을 제거합니다.

\* 신뢰성을 향상시킵니다.

솔루션 설계자는 어떤 단계를 수행해야 합니까?

A. 온디맨드 인스턴스와 스팟 인스턴스를 조합하여 프런트 엔드에 대한 Auto Scaling 그룹을 생성하여 비용을 절감합니다. Oracle 데이터베이스를 단일 Amazon RDS 예약 DB 인스턴스로 변환합니다.

B. 온디맨드 인스턴스와 스팟 인스턴스를 조합하여 프런트 엔드에 대한 Auto Scaling 그룹을 생성하여 비용을 절감합니다. 데이터베이스 인스턴스의 복사본 2개를 추가로 생성한 다음 별도의 AZ에 데이터베이스를 배포합니다.

C. 온디맨드 인스턴스와 스팟 인스턴스를 조합하여 프런트 엔드에 대한 Auto Scaling 그룹을 생성하여 비용을 절감합니다. Oracle 데이터베이스의 테이블을 Amazon DynamoDB 테이블로 변환합니다.

D. 온디맨드 인스턴스를 스팟 인스턴스로 전환하여 프런트 엔드 비용을 절감합니다. Oracle 데이터베이스의 테이블을 Amazon DynamoDB 테이블로 변환합니다.

Answer: C

Q239

한 솔루션 설계자가 곧 출시될 새로운 애플리케이션을 위한 데이터 스토리지 및 검색 아키텍처를 설계하고 있습니다. 이 응용 프로그램은 전 세계 모든 장치에서 분당 수백만 개의 작은 레코드를 수집하도록 설계되었습니다. 각 레코드의 크기는 4KB 미만이며 짧은 지연 시간으로 검색할 수 있는 안정적인 위치에 저장해야 합니다. 데이터는 일시적이며 회사는 120일 동안만 데이터를 저장해야 하며, 그 이후에는 데이터를 삭제할 수 있습니다. 솔루션 설계자는 1년 동안 스토리지 요구 사항이 약 10-15TB라고 계산합니다.

가장 비용 효율적이고 설계 요구 사항을 충족하는 스토리지 전략은 무엇입니까?

A. 인덱싱된 검색이 가능하도록 각 수신 레코드를 Amazon S3 버킷에 단일.csv 파일로 저장하도록 애플리케이션을 설계합니다. 120일이 지난 데이터를 삭제하도록 수명 주기 정책을 구성합니다.

B. 각 수신 레코드를 규모에 맞게 구성된 Amazon DynamoDB 테이블에 저장하도록 애플리케이션을 설계합니다. 120일이 지난 레코드를 삭제하도록 DynamoDB TTL(Time to Live) 기능을 구성합니다.

C. Amazon RDS MySQL 데이터베이스의 단일 테이블에 각 수신 레코드를 저장하도록 애플리케이션을 설계합니다. 쿼리를 실행하는 야간 크론 작업을 실행하여 120일이 넘은 모든 레코드를 삭제합니다.

D. Amazon S3 버킷에 레코드를 쓰기 전에 수신 레코드를 일괄 처리하도록 애플리케이션을 설계합니다. 배치의 레코드 목록을 포함하도록 객체의 메타데이터를 업데이트하고 Amazon S3 메타데이터 검색 기능을 사용하여 데이터를 검색합니다. 120일 후에 데이터를 삭제하도록 수명 주기 정책을 구성합니다.

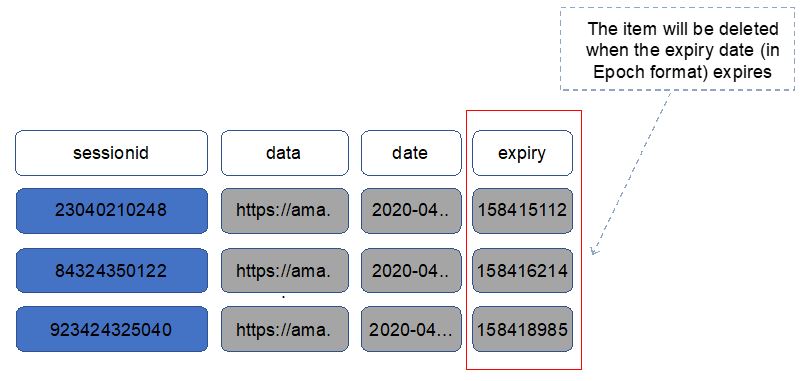
Answer: B

설명

Amazon DynamoDB는 필요한 처리량으로 확장할 수 있고 짧은 지연 시간을 제공하므로 적합한 데이터 저장소입니다. TTL 기능을 사용하여 데이터를 만료할 수 있습니다.

Amazon DynamoDB TTL(Time to Live)을 사용하면 항목별 타임스탬프를 정의하여 항목이 더 이상 필요하지 않은 시기를 결정할 수 있습니다. 지정된 타임스탬프의 날짜 및 시간 직후 DynamoDB는 쓰기 처리량을 소모하지 않고 테이블에서 항목을 삭제합니다. TTL은 워크로드 요구 사항에 맞게 최신 상태로 유지되는 항목만 유지하여 저장된 데이터 볼륨을 줄이는 수단으로 추가 비용 없이 제공됩니다.

아래 이미지는 만료 날짜를 Epoch 형식으로 지정하는 "만료" 열이 있는 테이블을 보여줍니다.



정답: "수신되는 각 레코드를 Amazon DynamoDB 테이블에 저장하십시오. 90일이 지난 레코드를 삭제하도록 DynamoDB TTL(Time to Live) 기능을 구성하십시오"가 정답입니다.

잘못됨: A. S3의 최대 객체 크기는 5TB입니다. 또한 파일 내의 항목은 만료될 수 없으며 전체 파일(객체)만 만료됩니다.

잘못됨: C. DynamoDB는 데이터 만료를 위한 기본 기능이 있고 SQL 데이터베이스보다 이러한 종류의 워크로드에 더 적합하기 때문에 더 적합합니다.

참조:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

Q240

신생 기업이 최신 Amazon Linux 2 AMI를 사용하여 프라이빗 서브넷에서 Amazon EC2 인스턴스 플릿을 호스팅합니다. 이 회사의 엔지니어는 문제 해결을 위해 인스턴스에 대한 SSH 액세스에 크게 의존합니다.

이 회사의 기존 아키텍처에는 다음이 포함됩니다.

\* 프라이빗 및 퍼블릭 서브넷이 있는 VPC와 NAT 게이트웨이.

\* 온프레미스 환경과의 연결을 위한 사이트 간 VPN

\* 온프레미스 환경에서 직접 SSH 액세스를 제공하는 EC2 보안 그룹.

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

솔루션 설계자는 어떤 전략을 사용해야 합니까?

A. EC2 인스턴스 플릿에 EC2 인스턴스 연결을 설치하고 구성합니다. 포트 22에서 인바운드 TCP를 허용하는 EC2 인스턴스에 연결된 모든 보안 그룹 규칙을 제거합니다. 엔지니어에게 EC2 인스턴스 연결 CLI를 사용하여 인스턴스에 원격으로 액세스하도록 안내합니다.

B. 엔지니어 디바이스의 IP 주소에 대해 포트 22의 인바운드 TCP만 허용하도록 EC2 보안 그룹을 업데이트합니다. 모든 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치하고 운영 체제 감사 로그를 CloudWatch 로그로 전송합니다.

C. 엔지니어 디바이스의 IP 주소에 대해 포트 22의 인바운드 TCP만 허용하도록 EC2 보안 그룹을 업데이트합니다.EC2 보안 그룹 리소스 변경에 대해 AWS Config를 활성화합니다. AWS Firewall Manager를 활성화하고 규칙 변경 사항을 자동으로 수정하는 보안 그룹 정책을 적용합니다.

D. AM2ONSSM 관리형 LN인스턴스 코어 관리형 정책이 연결된 IAM 역할을 생성합니다. IAM 역할을 모든 EC2 인스턴스에 연결합니다.EC2에 연결된 모든 보안 그룹 규칙을 제거합니다.

E. 포트 22에서 인바운드 TCP를 허용하는 인스턴스입니다. 엔지니어에게 디바이스용 AWS Systems Manager 세션 관리자 플러그인을 설치하고 시스템 관리자의 시작 세션 API 호출을 사용하여 인스턴스에 원격으로 액세스하도록 합니다.

Answer: B

Q241

대규모 급여 회사가 최근 소규모 직원 배치 회사와 합병되었습니다. 이 통합 회사는 이제 여러 사업부를 보유하고 있으며 각 사업부에는 자체 기존 AWS 계정이 있습니다. 솔루션스 아키텍트는 회사가 모든 AWS 계정에 대한 결제 및 액세스 정책을 중앙에서 관리할 수 있도록 해야 합니다. 솔루션스 아키텍트는 중앙 집중식 관리 계정에서 회사의 모든 멤버 계정으로 초대를 보내 AWS Organizations를 구성합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 다음 작업을 수행해야 합니까?

A. 각 구성원 계정에 OrganizationAccountAccess IAM 그룹을 생성합니다. 각 관리자에게 필요한 IAM 역할을 포함합니다.

B. 각 구성원 계정에서 OrganizationAccountAccessPolicy IAM 정책을 생성합니다. 교차 계정 액세스를 사용하여 구성원 계정을 관리 계정에 연결합니다.

C. 각 구성원 계정에서 OrganizationAccountAccessRole IAM 역할을 생성합니다. IAM 역할을 맡을 수 있는 권한을 관리 계정에 부여합니다.

D. 관리 계정에서 OrganizationAccountAccessRole IAM 역할을 생성합니다. 관리자 액세스 AWS 관리형 정책을 IAM 역할에 연결합니다. 각 구성원 계정의 관리자에게 IAM 역할을 할당합니다.

Answer: C

Q242

솔루션 설계자는 적절한 권한이 있는 AWS 사용자 또는 역할만 새로운 Amazon API Gateway 엔드포인트에 액세스할 수 있도록 하려고 합니다. 솔루션 설계자는 요청의 지연 시간을 분석하고 서비스 맵을 생성하기 위해 각 요청에 대한 엔드 투 엔드 뷰를 원합니다.

솔루션 설계자는 어떻게 API Gateway 액세스 제어를 설계하고 요청 검사를 수행할 수 있습니까?

A. API 게이트웨이 메서드의 경우 권한 부여를 AWS\_IAM으로 설정합니다. 그런 다음 REST API 리소스에 대한 IAM 사용자 또는 역할 실행-API 호출 권한을 부여합니다. 엔드포인트에 액세스할 때 API 호출자가 AWS 서명을 사용하여 요청에 서명할 수 있도록 합니다. AWS X-Ray를 사용하여 API 게이트웨이에 대한 사용자 요청을 추적하고 분석합니다.

B. API Gateway 리소스의 경우 CORS를 활성화로 설정하고 액세스 제어-허용-오리진 헤더에 회사 도메인만 반환합니다. 그런 다음 REST API 리소스에 대한 IAM 사용자 또는 역할 실행-API 호출 권한을 부여합니다. Amazon CloudWatch를 사용하여 API 게이트웨이에 대한 사용자 요청을 추적하고 분석할 수 있습니다.

C. 사용자 지정 권한 부여자로 AWS Lambda 함수를 생성하고 API 클라이언트에 호출할 때 키와 암호를 전달하도록 요청한 다음 Lambda를 사용하여 IAM 시스템에 대해 키/보안 페어를 확인합니다. AWS X-Ray를 사용하여 API 게이트웨이에 대한 사용자 요청을 추적하고 분석합니다.

D. API 게이트웨이에 대한 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 게이트웨이에 대한 사용자 요청을 추적하고 분석할 수 있습니다.

Answer: A

Q243

피트니스 모니터링 회사는 전 세계 소비자에게 서비스를 제공하며 수익의 대부분은 북미와 아시아에서 발생합니다. 회사는 읽기 집약적 사용자 권한 부여 응용 프로그램에 대해 다음 기준을 충족하는 인프라를 만들어야 합니다.

\* 모든 지역의 애플리케이션 문제에 대한 복원력을 갖추십시오.

\* 단일 리전의 데이터베이스에 기록합니다.

\* 여러 지역에서 읽습니다.

\* 각 리전의 애플리케이션 계층 전반에서 복원력을 지원합니다.

\* 애플리케이션에 반영된 관계형 데이터베이스 시맨틱을 지원합니다.

솔루션 설계자는 어떤 작업을 함께 수행해야 합니까?(두 개 선택)

A. 다중 응답 라우팅 정책과 결합된 Amazon Route 53 지리 근접성 라우팅 정책을 사용합니다.

B. 각 리전의 Amazon EC2 인스턴스에 웹, 애플리케이션 및 MySQL 데이터베이스 서버를 배포합니다. 읽기 및 쓰기가 리전에 로컬이 되도록 애플리케이션을 설정합니다.웹, 애플리케이션 및 데이터베이스 서버의 스냅샷을 생성하고 두 리전의 Amazon S3 버킷에 스냅샷을 저장합니다. 데이터베이스 계층에 대한 교차 리전 복제를 설정합니다.

C. 장애 조치 라우팅 정책과 결합된 Amazon Route 53 지리적 위치 라우팅 정책을 사용합니다.

D. 각 리전에서 MySQL 인스턴스용 웹, 애플리케이션 및 Amazon RDS를 설정합니다. 읽기가 로컬에서 이루어지고 쓰기가 사용자에 따라 분할되도록 애플리케이션을 설정합니다.웹, 애플리케이션 및 데이터베이스 서버에 대한 다중 AZ 장애 조치를 설정합니다. 데이터베이스 계층에 대한 교차 리전 복제를 설정합니다.

E. 각 리전에 액티브-액티브 웹 및 애플리케이션 서버를 설정합니다. 각 리전에 클러스터가 있는 Amazon Aurora 글로벌 데이터베이스를 배포합니다. 리전 내 Aurora 데이터베이스 엔드포인트를 사용하도록 애플리케이션을 설정합니다. 웹 애플리케이션 서버의 스냅샷을 생성하여 두 리전의 Amazon S3 버킷에 저장합니다.

Answer: A, E

Q244

한 회사가 마케팅 웹 사이트 및 콘텐츠 관리 시스템을 온프레미스 데이터 센터에서 AWS로 마이그레이션하고 있습니다. 이 회사는 웹 서버에 사용되는 Amazon EC2 인스턴스와 데이터베이스에 Amazon RDS 인스턴스를 사용하는 VPC에 AWS 애플리케이션을 배포하기를 원합니다. 이 회사에는 온-프레미스 시스템의 설치 프로세스를 설명하는 Runbook 문서가 있습니다. 회사는 Runbook 문서에 참조된 프로세스를 기반으로 AWS 시스템을 구축하려고 합니다. Runbook 문서에서는 서버의 운영 체제, 네트워크 설정, 웹 사이트 및 콘텐츠 관리 시스템 소프트웨어의 설치 및 구성에 대해 설명합니다. 마이그레이션이 완료된 후 회사는 다른 AWS 기능을 활용하기 위해 신속하게 변경할 수 있기를 원합니다.

향후 변경을 허용하면서 AWS에서 애플리케이션과 환경을 배포하고 자동화하려면 어떻게 해야 합니까?

A. Runbook을 업데이트하여 AWS 콘솔을 사용하여 애플리케이션의 VPC, EC2 인스턴스 및 RDS 인스턴스를 만드는 방법을 설명합니다. Runbook의 나머지 단계는 AWS 마이그레이션에서 발생할 수 있는 변경 사항을 반영하도록 업데이트해야 합니다.

B. AWS API를 사용하여 VPC를 생성하는 Python 스크립트를 작성합니다. EC2 인스턴스 및 애플리케이션용 RDS 인스턴스 런북의 나머지 단계를 구현하는 셸 스크립트를 작성합니다. Python 스크립트가 새로 생성된 인스턴스에서 셸 스크립트를 복사하고 실행하여 설치를 완료하도록 합니다.

C. 애플리케이션용 VPC, EC2 인스턴스 및 RDS 인스턴스를 생성하는 AWS Cloud Formation 템플릿을 작성합니다. Runbook의 나머지 단계가 AWS 마이그레이션에서 발생할 수 있는 변경 사항을 반영하도록 업데이트해야 합니다.

D. VPC, EC2 인스턴스 및 애플리케이션용 RDS 인스턴스를 생성하는 AWS CloudFormation 템플릿을 작성합니다. AWS CloudFormation 템플릿에 EC2 사용자 데이터를 포함하여 소프트웨어를 설치하고 구성합니다.

Answer: D

Q245

한 회사가 기업 데이터 센터를 온프레미스에서 AWS 클라우드로 마이그레이션하려고 합니다. 데이터 센터에는 VMware 및 Hyper-V를 사용하는 물리적 서버와 VM이 포함됩니다. 관리자는 데이터를 수집할 올바른 서비스 (또는 초기 마이그레이션 검색 프로세스) 를 선택해야 합니다. 데이터 형식은 AWS 마이그레이션 허브에서 지원해야 합니다. 또한 이 회사는 데이터에서 보고서를 생성할 수 있어야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 물리적 서버 및 모든 VM에서 데이터를 수집하려면 AWS 에이전트 없는 검색 커넥터를 사용합니다. 수집된 데이터를 Amazon S3에 저장합니다. S3 선택을 사용하여 데이터를 쿼리합니다. Amazon EC2에서 호스팅되는 Kibana를 사용하여 보고서를 생성합니다.

B. AWS 애플리케이션 검색 서비스 에이전트를 사용하여 물리적 서버 및 모든 VM에서 데이터를 수집합니다. 수집된 데이터를 Amazon Elastic File System (Amazon EFS) 에 저장합니다. Amazon Athena를 사용하여 데이터를 쿼리하고 보고서를 생성합니다.

C. 물리적 서버 및 Hyper-V에서의 데이터 수집을 위해 AWS 애플리케이션 검색 서비스 에이전트를 사용합니다. VMware에서 데이터를 수집하려면 AWS 에이전트리스 검색 커넥터를 사용하십시오. 수집된 데이터를 Amazon S3에 저장합니다. Amazon Athena를 사용하여 데이터를 쿼리합니다. Amazon QuickSight를 사용하여 보고서를 생성합니다.

D. 물리적 서버에서의 데이터 수집을 위해 AWS 시스템 관리자 에이전트를 사용합니다. 모든 VM에서 데이터를 수집하려면 AWS 에이전트 없는 검색 커넥터를 사용합니다. Amazon Redshift를 사용하여 수집된 데이터에서 보고서를 저장, 쿼리 및 생성합니다.

Answer: C

설명

AWS Application Discovery Service는 온프레미스 서버에 대한 사용 및 구성 데이터를 수집하여 AWS 클라우드로의 마이그레이션을 계획하는 데 도움이 됩니다. Application Discovery Service는 AWS Migration Hub와 통합되어 마이그레이션 상태 정보를 단일 콘솔로 집계하여 마이그레이션 추적을 간소화합니다.

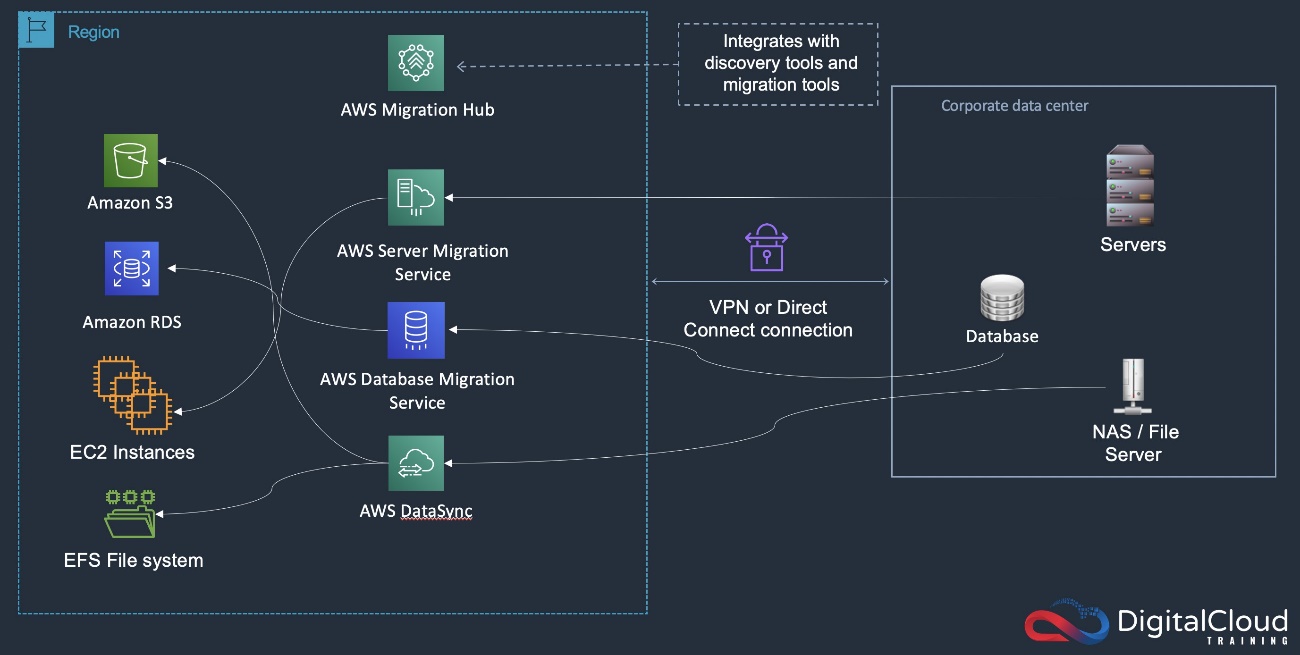
Application Discovery Service는 검색을 수행하고 온프레미스 서버에 대한 데이터를 수집하는 두 가지 방법을 제공합니다.

• 에이전트 없는 검색 – VMware에서 실행되는 VM을 식별합니다.

• 에이전트 기반 검색 – Hyper-V에서 실행되는 물리적 서버 및 VM에 사용됩니다.

보고를 위해 데이터를 Amazon S3에 저장하고 Amazon Athena 및 Amazon QuickSight를 사용하여 쿼리할 수 있습니다.

그런 다음 Migration Hub를 사용하여 AWS DMS를 사용하여 마이그레이션 프로세스를 관리할 수 있습니다.



잘못됨: A. 물리적 서버 또는 Hyper-V VM에서는 에이전트 없는 커넥터를 사용할 수 없습니다.

잘못됨: B. VMware VM에서 에이전트 없는 커넥터를 사용하는 것이 더 효율적입니다. Athena는 EFS에서 데이터를 쿼리할 수 없습니다.

잘못됨: D. Hyper-V VM에서는 에이전트 없는 검색 커넥터를 사용할 수 없습니다. RedShift는 값비싼 솔루션이 될 것이며 데이터를 읽고 쓰려면 애플리케이션 구성 요소가 필요합니다.

참조:

https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html

https://aws.amazon.com/quicksight/

Q246

솔루션 설계자는 회사의 Amazon EC2 인스턴스와 Amazon Elastic Block Store (Amazon EBS) 볼륨을 분석하여 회사에서 리소스를 효율적으로 사용하고 있는지 확인해야 합니다. 이 회사는 액티브/패시브 구성으로 배포된 여러 개의 대용량, 고용량 메모리 EC2 인스턴스 또는 호스트 데이터베이스 클러스터를 실행하고 있습니다. 이러한 EC2 인스턴스의 사용률은 데이터베이스를 사용하는 애플리케이션에 따라 다르며 회사에서는 패턴을 식별하지 못했습니다. 솔루션 설계자는 환경을 분석하고 결과를 바탕으로 조치를 취해야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 솔루션은 무엇입니까?

A. AWS 시스템 관리자 OpsCenter를 사용하여 대시보드를 생성합니다. EC2 인스턴스 및 해당 EBS 볼륨과 연결된 Amazon CloudWatch 지표에 대한 시각화를 구성합니다. 대시보드를 주기적으로 검토하고 사용 패턴을 식별합니다. 지표의 피크를 기준으로 EC2 인스턴스의 크기를 적절하게 조정합니다.

B. EC2 인스턴스와 해당 EBS 볼륨에 대한 Amazon CloudWatch 세부 모니터링을 켭니다. 지표를 기반으로 하는 대시보드를 만들고 검토합니다. 사용 패턴을 식별합니다. 지표의 피크를 기준으로 EC2 인스턴스의 크기를 적절하게 조정합니다.

C. 각 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다. AWS 컴퓨트 옵티마이저를 켜고 12시간 이상 실행되도록 합니다. 컴퓨팅 옵티마이저의 권장 사항을 검토하고 지침에 따라 EC2 인스턴스의 크기를 적절하게 조정합니다.

D. AWS 엔터프라이즈 지원 플랜에 가입합니다. AWS 신뢰할 수 있는 조언자를 켭니다. 12시간 기다립니다. Trusted Advisor의 권장 사항을 검토하고 지침에 따라 EC2 인스턴스의 크기를 적절하게 조정합니다.

Answer: C

https://www.examtopics.com/discussions/amazon/view/68919-exam-aws-certified-solutions-architect-professional-topic-1/

Q247

한 회사가 AWS에서 미디어 메타데이터 추출 파이프라인을 실행하고 있습니다. 파일 Amazon S3에 대한 참조가 포함된 알림은 Amazon Simple Notification Service (Amazon SNS) 주제로 전송됩니다. 파이프라인은 SNS 주제를 구독하는 여러 AWS Lambda 함수로 구성됩니다. Lambda 함수는 S3 파일을 추출하고 Amazon RDS PostgreSQL DB 인스턴스에 메타데이터를 씁니다. 사용자는 메타데이터에 대한 업데이트가 표시 속도가 느리거나 손실되는 경우가 있다고 보고합니다. 이 시간 동안 데이터베이스의 CPU 사용률이 높고 실패한 Lambda 호출 수가 증가합니다.

이 문제를 해결하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?(두 개 선택)

A. SNS 주제에서 마사지 전송 상태 활성화 지수 백오프가 있는 재시도를 활성화하도록 SNS 주제 전송 정책을 구성합니다.

B. Amazon Simple Queue Service (Amazon SQS) FIFO 대기열을 생성하고 대기열을 SNS 주제 SQS 대기열의 메시지를 소비하도록 Lambda 함수 구성에 가입합니다.

C. RDS 인스턴스에 대한 RDS 프록시 생성 프록시를 사용하여 RDS 인스턴스에 연결하도록 Lambda 함수를 업데이트합니다.

D. RDS 인스턴스에 대해 RDS 데이터 API를 활성화합니다. 데이터 API를 사용하여 RDS 인스턴스에 연결하도록 Lambda 함수를 업데이트합니다.

E. 각 Lambda 함수에 대한 Amazon Simple Queue Service (Amazon SQS) 표준 대기열을 생성하고 SNS 주제에 대한 대기열을 구독합니다. 해당 SQS 대기열의 메시지를 소비하도록 Lambda 함수를 구성합니다.

Answer: C, E

Q248

최근 한 대기업에서 Amazon RDS 및 Amazon DynamoDB 비용이 예상치 못한 증가를 경험했습니다. 이 회사는 AWS 결제 및 비용 관리의 세부 정보에 대한 가시성을 높여야 합니다. 많은 개발 및 프로덕션 계정을 포함하여 AWS Organizations와 관련된 다양한 계정이 있습니다. 조직 전체에 일관된 태그 지정 전략은 없지만 일관된 태그 지정과 함께 AWS Cloud Formation을 사용하여 모든 인프라를 배포해야 하는 지침이 마련되어 있습니다. 관리에는 모든 기존 및 향후 DynamoDB 테이블 및 RDS 인스턴스에 대한 비용 센터 번호와 프로젝트 ID 번호가 필요합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자가 제공해야 하는 전략은 무엇입니까?

A. 태그 편집기를 사용하여 기존 리소스에 태그를 지정합니다. 비용 할당 태그를 생성하여 비용 센터 및 프로젝트 ID를 정의하고 태그가 기존 리소스로 전파될 때까지 24시간을 허용합니다.

B. AWS Config 규칙을 사용하여 태그가 지정되지 않은 리소스에 대해 재무 팀에 알립니다. 중앙 집중식 AWS Lambda 기반 솔루션을 생성하여 교차 계정 역할을 사용하여 태그가 지정되지 않은 RDS 데이터베이스와 DynamoDB 리소스에 매시간 태그를 지정합니다.

C. 태그 편집기를 사용하여 기존 리소스에 태그를 지정합니다. 비용 할당 태그를 생성하여 비용 센터 및 프로젝트 ID를 정의합니다. SCP를 사용하여 리소스에 비용 센터 및 프로젝트 ID가 없는 리소스 생성을 제한합니다.

D. 비용 할당 태그를 생성하여 비용 센터 및 프로젝트 ID를 정의하고 태그가 기존 리소스로 전파될 때까지 24시간을 허용합니다. 기존 페더레이션 역할을 업데이트하여 리소스에 비용 센터 및 프로젝트 ID가 포함되지 않은 리소스를 프로비저닝할 권한을 제한합니다.

Answer: C

설명

태그를 사용하여 리소스를 구성하고 비용 할당 태그를 사용하여 세부 수준에서 AWS 비용을 추적할 수 있습니다. 비용 할당 태그를 활성화하면 AWS는 비용 할당 태그를 사용하여 비용 할당 보고서에서 리소스 비용을 구성하므로 AWS 비용을 더 쉽게 분류하고 추적할 수 있습니다.

모든 새 리소스에 태그를 추가하면 관리 팀이 비용을 더 잘 추적하고 특정 비용 센터 및 프로젝트에 비용을 할당할 수 있습니다.

서비스 제어 정책(SCP)을 사용하여 AWS Organizations의 계정에서 사용 가능한 최대 권한을 제한할 수 있습니다. SCP는 정책이며 조건문을 추가할 수 있습니다. 이 경우 태그가 지정된 경우에만 리소스 생성을 허용하는 조건문을 사용하여 SCP를 생성할 수 있습니다.

잘못됨: A. 여기에는 태그 적용을 시행하는 메커니즘이 없습니다.

잘못됨: B. 규정 준수를 위해 AWS Config를 사용할 수 있지만 더 나은 솔루션은 생성 시 태그를 적용하는 것입니다. Lambda를 사용하여 리소스에 태그를 지정하는 것은 어떤 태그를 어떤 리소스에 추가할지 식별하는 측면에서 복잡합니다.

잘못됨: D. 권한 경계는 사용자 계정에 적용되지만 SCP는 전체 AWS 계정에 적용되며 모든 사용자에게 더 쉽게 적용됩니다.

참조:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_policies\_scps.html

Q249

한 회사에서 NoSQL 데이터베이스용으로 설계된 다중 계층 웹 애플리케이션을 사용하여 AWS에서 전자 상거래 플랫폼을 호스팅할 계획입니다. 이 회사는 us-west-2 리전을 기본 리전으로 사용할 계획입니다.이 회사는 재해 복구를 위해 애플리케이션 및 데이터의 사본을 두 번째 리전인 us-west-1에서 사용할 수 있도록 보장하려고 합니다. 이 회사는 페일오버 시간을 가능한 한 낮게 유지하려고 합니다. 기본 서비스가 복원된 후 관리 상호 작용 없이 기본 리전으로 페일백할 수 있어야 합니다.

솔루션 설계자는 어떤 설계를 사용해야 합니까?

A. AWS CloudFormation 스택세트를 사용하여 웹 및 애플리케이션 티어에 대한 Auto Scaling 그룹이 있는 두 리전 모두에서 스택을 생성합니다. Amazon S3 교차 리전 복제를 사용하여 리전 간에 정적 콘텐츠를 비동기적으로 복제합니다. 중단 발생 시 Amazon Route 53 DNS 장애 조치 라우팅 정책을 사용하여 사용자를 us-west-1의 보조 사이트로 안내합니다. 데이터베이스 계층에는 Amazon DynamoDB 글로벌 테이블을 사용합니다.

B. AWS CloudFormation 스택세트를 사용하여 웹 및 애플리케이션 티어에 대한 Auto Scaling 그룹이 있는 두 리전 모두에서 스택을 생성합니다. Amazon S3 교차 리전 복제를 사용하여 리전 간에 정적 콘텐츠를 비동기적으로 복제합니다.중단 발생 시 Amazon Route 53 DNS 장애 조치 라우팅 정책을 사용하여 사용자를 us-west-1의 보조 사이트로 안내합니다. 데이터베이스 계층에 대해 Amazon Aurora 글로벌 데이터베이스를 배포합니다.

C. AWS Service Catalog를 사용하여 두 리전에 웹 및 애플리케이션 서버를 배포합니다. Amazon S3 교차 리전 복제를 사용하여 두 리전 간에 정적 콘텐츠를 비동기적으로 복제합니다. Amazon Route 53 상태 확인을 사용하여 기본 리전 장애를 식별하고 중단 시 퍼블릭 DNS 항목 목록을 보조 리전으로 업데이트합니다. 데이터베이스 티어에 대한 교차 리전 복제와 함께 MySQL용 Amazon RDS를

D. AWS CloudFormation 스택세트를 사용하여 웹 및 애플리케이션 티어에 대한 Auto Scaling 그룹을 사용하여 두 리전 모두에서 스택을 생성할 수 있습니다. Amazon S3 교차 리전 복제를 사용하여 리전 간에 정적 콘텐츠를 비동기적으로 복제합니다. Amazon S3의 정적 파일과 함께 Amazon CloudFront를 사용하고 프런트 엔드 웹 티어에는 다중 리전 오리진을 사용합니다. 각 리전에서 Amazon S3로의 예약 백업과 함께 Amazon DynamoDB 테이블을 사용합니다.

Answer: A

Q250

기업은 애플리케이션 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 여러 Amazon EC2 인스턴스에 분산되어 있는 애플리케이션을 운영합니다. 보안 팀에서 검사할 수 있도록 모든 애플리케이션 액세스 시도에 액세스할 수 있어야 합니다. 클라이언트의 IP 주소, 연결 종류 및 사용자 에이전트를 모두 제공해야 합니다.

이러한 기준을 충족하는 솔루션은 무엇입니까?

A. EC2 세부 모니터링을 활성화하고 네트워크 로그를 포함합니다. Amazon Kinesis 데이터 Firehose를 통해 보안 팀이 분석에 사용하는 Amazon Elasticsearch Service (Amazon ES) 클러스터로 모든 로그를 전송합니다.

B. 모든 EC2 인스턴스 네트워크 인터페이스에 대해 VPC 흐름 로그를 활성화합니다. VPC 흐름 로그를 Amazon S3 버킷에 게시합니다. 보안 팀에서 Amazon Athena를 사용하여 로그를 쿼리하고 분석하도록 합니다.

C. 애플리케이션 로드 밸런서에 대한 액세스 로그를 활성화하고 로그를 Amazon S3 버킷에 게시합니다. 보안 팀에서 Amazon Athena를 사용하여 로그를 쿼리하고 분석하도록 합니다.

D. 트래픽 미러링을 활성화하고 모든 EC2 인스턴스 네트워크 인터페이스를 소스로 지정합니다. Amazon Kinesis Data Firehose를 통해 모든 트래픽 정보를 보안 팀이 분석에 사용하는 Amazon Elasticsearch Service (Amazon ES) 클러스터로 전송합니다.

Answer: C

Q251

한 회사에서 AWS 조직을 사용하여 여러 AWS 계정을 관리합니다. 루트 OU 아래에 이 회사는 연구 및 DataOps라는 두 개의 OU를 보유하고 있습니다. 규제 요구 사항으로 인해 회사에서 조직에 배포하는 모든 리소스는 ap-Northeast-1 리전에 상주해야 합니다. 추가적으로.회사에서 DataOps OU에 배포하는 EC2 인스턴스는 사전 정의된 인스턴스 유형 목록을 사용해야 합니다. 솔루션 설계자는 이러한 제한을 적용하는 솔루션을 구현해야 합니다. 솔루션은 운영 효율성을 극대화하고 지속적인 유지 관리를 최소화해야 합니다. 이러한 요구 사항을 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. DataOps OU 아래의 한 계정에 IAM 역할을 생성합니다. 역할의 인라인 정책에서 ec2 인스턴스 유형 조건 키를 사용하여 특정 인스턴스 유형에 대한 액세스를 제한합니다.

B. 루트 OU 아래의 모든 계정에 IAM 사용자를 생성합니다. ap-northeast-1을 제외한 모든 AWS 리전에 대한 액세스를 제한하려면 각 사용자에 대한 인라인 정책에서 aws RequestedRegion 조건 키를 사용합니다.

C. SCP를 생성합니다. AWS:요청된 리전 조건 키를 사용하여 ap-북동-1을 제외한 모든 AWS 리전에 대한 액세스를 제한합니다. 루트 OU에 SCP를 적용합니다.

D. SCP를 생성합니다. EC2 리전 조건 키를 사용하여 apnortheast-1을 제외한 모든 AWS 리전에 대한 액세스를 제한합니다. SCP를 루트 OU, 데이터 운영 OU 및 연구 OU에 적용합니다.

E. SCP 생성: ec2:LNStanceType 조건 키를 사용하여 특정 인스턴스 유형에 대한 액세스를 제한합니다. SCP를 데이터 운영 OU에 적용합니다.

Answer: C, E

Q252

한 회사에서 Amazon S3를 사용하여 온프레미스 파일 스토리지 솔루션을 백업하려고 합니다. 이 회사의 온프레미스 파일 스토리지 솔루션은 NFS를 지원하며 NFS를 지원하는 새로운 솔루션을 원합니다. 5 일 후에 백업 파일을 아카이빙하려고 합니다. 회사에서 재해 복구를 위해 아카이브된 파일이 필요한 경우 해당 파일을 검색하기 위해 며칠을 기다릴 수 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 게이트웨이 배포 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 게이트웨이 배포 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.

Answer: D

Q253

한 솔루션스 아키텍트가 AWS Fargate에서 실행될 컨테이너화된 NET Core 애플리케이션을 구축하고 있습니다. 응용 프로그램의 백엔드를 사용하려면 가용성이 높은 Microsoft SQL Server가 필요합니다. 응용 프로그램의 모든 계층은 고가용성이어야 합니다. SQL Server에 대한 연결 문자열에 사용되는 자격 증명은.NET Core 프런트 엔드 컨테이너 내의 디스크에 저장하면 안 됩니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 전략을 사용해야 합니까?

A. 서비스 오토 스케일링을 사용하여 파게이트에서 실행되도록 SQL Server를 설정합니다. Fargate 작업 정의가 Fargate에서 실행 중인 SQL Server에 대한 자격 증명의 보안 값을 가져올 수 있도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다. AWS Secrets Manager에서 Fargate 작업 정의의 secrets 섹션에 있는 시크릿의 ARN을 지정합니다. 그러면 민감한 데이터가 시작 시 환경 변수로 컨테이너에 삽입되어 애플리케이션에서 읽어 연결 문자열을 구성할 수 있습니다. 여러 가용 영역에서 애플리케이션 로드 밸런서 뒤에 있는 서비스 Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

B. Amazon RDS에서 SQL 서버의 다중 AZ 배포를 생성합니다. RDS 데이터베이스에 대한 자격 증명에 대한 보안 정보를 AWS 비밀 관리자에서 생성합니다. Fargate 작업 정의가 Secrets Manager의 RDS 데이터베이스에 대한 자격 증명의 보안 값을 가져올 수 있도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다. Secrets Manager에서 Fargate 작업 정의의 secrets 섹션에 있는 시크릿의 ARN을 지정하면 민감한 데이터가 시작 시 환경 변수로 컨테이너에 삽입되어 애플리케이션에 읽어 연결 문자열을 구성할 수 있습니다. 여러 가용 영역에서 애플리케이션 로드 밸런서 뒤에 있는 서비스 Auto Scaling을 사용하여 Fargate에서 .NET Core 서비스를 설정합니다.

C. 오토 스케일링 그룹을 생성하여 Amazon EC2에서 SQL Server를 실행합니다. AWS 시크릿 매니저에서 EC2에서 실행되는 SQL Server에 대한 자격 증명을 위한 시크릿을 생성합니다. Fargate 작업 정의가 자격 증명의 보안 값을 EC2에서 SQL Server로 가져올 수 있도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다. Secrets Manager에서 Fargate 작업 정의의 secrets 섹션에 있는 시크릿의 ARN을 지정하면 민감한 데이터가 시작 시 환경 변수로 컨테이너에 삽입되어 애플리케이션에 읽어 연결 문자열을 구성할 수 있습니다. 여러 가용 영역에서 애플리케이션 로드 밸런서 뒤에 있는 서비스 Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

D. Amazon RDS에서 SQL 서버의 다중 AZ 배포를 생성합니다. RDS 데이터베이스에 대한 자격 증명에 대한 보안 정보를 AWS 비밀 관리자에서 생성합니다. Fargate 작업 정의에서.NET Core 컨테이너에 대한 비영구 빈 저장소를 만들어 중요한 정보를 저장합니다. Fargate 작업 정의가 Secrets Manager의 RDS 데이터베이스에 대한 자격 증명의 보안 값을 가져올 수 있도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다. Fargate 작업 정의의 secrets 섹션에 있는 Secrets Manager에서 시크릿의 ARN을 지정합니다. 그러면 시작 시 애플리케이션에서 읽어들여 연결 문자열을 구성하기 위해 중요한 데이터를 비영구 저장소에 쓸 수 있습니다. 여러 가용 영역에서 애플리케이션 로드 밸런서 뒤에 있는 서비스 Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

Answer: B

Q254

감사 중에 보안 팀은 개발 팀이 IAM 사용자 보안 액세스 키를 코드에 넣은 다음 AWS CodeCommit 리포지토리에 커밋하고 있음을 발견했습니다. 보안 팀은 이 보안 취약성의 인스턴스를 자동으로 찾아 수정하려고 합니다.

자격 증명이 자동으로 적절하게 보호되도록 보장하는 솔루션은 무엇입니까?

A. AWS Systems Manager Run Command를 사용하여 야간에 스크립트를 실행하여 개발 인스턴스에서 자격 증명을 검색합니다. 자격 증명이 발견되면 AWS 보안 관리자를 사용하여 자격 증명을 교체합니다.

B. 예약된 AWS Lambda 함수를 사용하여 CodeCommit에서 애플리케이션 코드를 다운로드하고 스캔합니다. 자격 증명이 발견되면 새 자격 증명을 생성하여 AWS KMS에 저장합니다.

C. CodeCommit 리포지토리에서 자격 증명을 검색하도록 Amazon Macie를 구성합니다. 자격 증명이 발견되면 AWS Lambda 함수를 트리거하여 자격 증명을 비활성화하고 사용자에게 알립니다.

D. CodeCommit 트리거를 구성하여 AWS Lambda 함수를 호출하여 자격 증명을 위한 새 코드 제출을 스캔합니다. 자격 증명이 발견되면 AWS IAM에서 자격 증명을 비활성화하고 사용자에게 알립니다.

Answer: D

설명

코드 푸시 또는 기타 이벤트가 Amazon Simple Notification Service(Amazon SNS)에서 알림 보내기 또는 AWS Lambda에서 함수 호출과 같은 작업을 트리거하도록 CodeCommit 리포지토리를 구성할 수 있습니다. 각 CodeCommit 리포지토리에 대해 최대 10개의 트리거를 생성할 수 있습니다. 이 경우 액세스 키에 대한 코드를 스캔하도록 AWS Lambda를 트리거할 수 있습니다.

잘못됨: C. Macie는 Amazon S3 버킷을 스캔하지만 AWS 관리형 서비스 버킷이므로 CodeCommit에 할당된 S3 버킷을 볼 수 없습니다.

잘못됨: B. KMS는 보안 액세스 키가 아닌 암호화 키를 저장하는 데 사용됩니다.

참조:

https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-notify.html

Q255

회사는 사용자가 콘텐츠 제공자가 선별한 키워드를 사용하여 비디오 및 관련 정보를 검색할 수 있는 기능을 제공하는 애플리케이션을 실행합니다. 애플리케이션 데이터는 800GB 크기의 온프레미스 Oracle 데이터베이스에 저장됩니다. 이 회사는 데이터를 Amazon Aurora MySQL DB 인스턴스로 마이그레이션하려고 합니다. 솔루션 설계자는 마이그레이션에 AWS 스키마 변환 도구 및 AWS Database Migration Service (AWS DMS) 를 사용할 계획입니다. 마이그레이션하는 동안 기존 데이터베이스는 진행 중인 요청을 처리해야 합니다. 마이그레이션은 다운타임을 최소화하면서 완료해야 합니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 마이그레이션 프로세스를 시작하기 전에 대상 데이터베이스에서 기본 키 인덱스, 보조 인덱스 및 참조 무결성 제약 조건을 만듭니다.

B. AWS DMS를 사용하여 Oracle에서 Aurora MySQL로의 변환 보고서를 실행합니다. 모든 문제를 해결합니다. 그런 다음 AWS DMS를 사용하여 데이터를 마이그레이션합니다.

C. 진행 중인 복제에 M5 또는 CS DMS 복제 인스턴스 유형을 사용합니다.

D. 마이그레이션 및 컷오버 프로세스가 완료될 때까지 대상 데이터베이스의 자동 백업 및 로깅을 해제합니다.

Answer: B

Q256

회사에 필요한 것보다 더 큰 Amazon EC2 인스턴스를 시작하는 프로젝트가 있습니다. 이 활동을 기업 IT 외부로 유지하기 위한 정책 제한으로 인해 프로젝트 계정은 AWS Organizations의 회사 조직에 속할 수 없습니다. 이 회사는 프로젝트 계정에서 개발자가 t3.small EC2 인스턴스를 시작할 수만 있도록 허용하려고 합니다. 이러한 EC2 인스턴스는 us-east-2 리전으로 제한되어야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 무엇을 해야 합니까?

A. 새 개발자 계정을 만듭니다. 모든 EC2 인스턴스, 사용자 및 자산을 us-east-2로 이동합니다. AWS 조직의 회사 조직에 계정을 추가합니다. 리전 선호도를 나타내는 태그 지정 정책을 적용합니다.

B. 미국-동부-2에 있는 i3.small EC2 인스턴스를 제외한 모든 EC2 인스턴스의 시작을 거부하는 SCP를 생성합니다. S CP를 프로젝트 계정에 연결합니다.

C. 미국-동부-2의 각 개발자를 위해 t3.small EC2 예약 인스턴스를 생성하고 구매합니다. 각 개발자에게 이름이 태그인 특정 EC2 인스턴스를 할당합니다.

D. us-east-2에서 t3.small EC2 인스턴스만 시작할 수 있도록 허용하는 IAM 정책을 생성합니다. 개발자가 프로젝트 계정에서 사용하는 역할 및 그룹에 정책을 연결합니다.

Answer: D

Q257

한 솔루션 설계자가 PostgreSQL DB 인스턴스용 Amazon RDS를 사용하는 웹 애플리케이션을 구축하고 있습니다. DB 인스턴스는 쓰기보다 더 많은 읽기를 수신할 것으로 예상됩니다. 솔루션스 아키텍트는 대량의 읽기 트래픽을 수용할 수 있고 DB 인스턴스의 가용성이 높은지 확인해야 합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 단계를 수행해야 합니까?(세 개 선택)

A. 읽기 전용 복제본을 여러 개 생성하여 Auto Scaling 그룹에 넣습니다.

B. 서로 다른 가용 영역에 여러 읽기 전용 복제본을 생성합니다.

C. TTL 및 가중치 기반 라우팅 정책을 사용하여 Amazon Route 53 호스팅 영역과 각 읽기 전용 복제본에 대한 레코드 세트를 생성합니다.

D. 애플리케이션 로드 밸런서 (ALB) 를 생성하고 읽기 전용 복제본을 ALB 뒤에 배치합니다.

E. 실패한 읽기 전용 복제본을 감지하도록 Amazon CloudWatch 경보를 구성합니다. AWS Lambda 함수를 직접 호출하여 Route 53 레코드 세트를 삭제하도록 경보를 설정합니다.

F. 엔드포인트를 사용하여 각 읽기 전용 복제본에 대해 Amazon Route 53 상태 확인을 구성합니다.

Answer: B, C, F

Q258

한 대기업은 수백 개의 AWS 계정에 배포된 VPC에서 워크로드를 실행합니다. 각 VPC는 여러 가용 영역에 걸쳐 있는 퍼블릭 서브넷과 프라이빗 서브넷으로 구성됩니다. NAT 게이트웨이는 퍼블릭 서브넷에 배포되며 프라이빗 서브넷에서 인터넷으로의 아웃바운드 연결을 허용합니다. 솔루션 설계자가 허브 앤 스포크 설계를 진행하고 있습니다. 스포크 VPC의 모든 프라이빗 서브넷은 송신 VPC를 통해 인터넷으로 트래픽을 라우팅해야 합니다. 솔루션스 아키텍트는 이미 중앙 AWS 계정의 송신 VPC에 NAT 게이트웨이를 배포했습니다.

솔루션 설계자가 이러한 요구 사항을 충족하기 위해 취해야 할 추가 단계는 무엇입니까?

A. 송신 VPC와 스포크 VPC 간에 피어링 연결을 생성합니다. 인터넷에 액세스할 수 있도록 필요한 라우팅을 구성합니다.

B. 전송 게이트웨이를 생성하여 기존 AWS 계정과 공유 기존 VPC를 전송 게이트웨이에 연결 인터넷에 액세스할 수 있도록 필요한 라우팅을 구성합니다.

C. 모든 계정에 전송 게이트웨이를 생성합니다. NAT 게이트웨이를 전송 게이트웨이에 연결합니다.인터넷에 액세스할 수 있도록 필요한 라우팅을 구성합니다.

D. 송신 VPC와 스포크 VPC 간에 AWS 프라이빗 링크 연결을 생성합니다. 인터넷에 액세스할 수 있도록 필요한 라우팅을 구성합니다.

Answer: B

Q259

한 회사가 AWS 클라우드에서 여러 워크로드를 실행하고 있습니다. 이 회사에는 소프트웨어 개발을 위한 별도의 부서가 있습니다. 이 회사는 AWS 조직 및 SAML과의 연동을 사용하여 개발자에게 AWS 계정의 리소스를 관리할 수 있는 권한을 부여합니다. 개발 단위는 각각 프로덕션 워크로드를 공통 프로덕션 계정에 배포합니다. 최근에 개발 단위의 구성원이 다른 개발 단위에 속한 EC2 인스턴스를 종료하는 프로덕션 계정에서 인시던트가 발생했습니다. 솔루션 설계자는 향후 유사한 사고가 발생하지 않도록 하는 솔루션을 만들어야 합니다. 또한 이 솔루션은 개발자가 워크로드에 사용되는 인스턴스를 관리할 수 있는 가능성이 낮아야 합니다.

이러한 요구 사항을 충족하는 전략은 무엇입니까?

A. 각 개발 단위에 대해 AWS 조직에 별도의 OU를 생성합니다. 생성된 OU를 회사 AWS 계정에 할당합니다. 개발 단위 이름과 일치하는 DevelopmentUnit 리소스 태그에 대해 거부 작업 및 문자열NoteEquals 조건을 사용하여 별도의 SCP를 만듭니다. SCP를 해당 OU에 할당합니다.

B. SAML 연동 중에 개발 유닛에 대한 속성을 AWS 보안 토큰 서비스 (AWS STS) 세션 태그로 전달합니다. 개발자가 가정한 IAM 역할에 대한 IAM 정책을 거부 작업 및 DevelopmentUnit 리소스 태그 및 AWS:PrincipalTag/ 개발 단위에 대한 문자열NotEquals 조건으로 업데이트합니다.

C. SAML 연동 중에 개발 유닛에 대한 속성을 AWS 보안 토큰 서비스 (AWS STS) 세션 태그로 전달합니다. 개발 단위 리소스 태그 및 AWS: 보안 주체 태그/개발 단위에 대해 allow 작업과 문자열 같음 조건을 사용하여 SCP를 만듭니다. SCP를 루트 OU에 할당합니다.

D. 각 개발 단위에 대해 별도의 IAM 정책을 생성합니다. 모든 IAM 정책에 대해 DevelopmentUnit 리소스 태그와 개발 단위 이름에 대해 허용 작업 및 문자열Equals 조건을 추가합니다. SAML 연동 중에 AWS 보안 토큰 서비스 (AWS STS) 를 사용하여 IAM 정책을 할당하고 개발 단위 이름을 가정된 IAM 역할에 일치시킵니다.

Answer: B

Q260

한 회사에서 Amazon API Gateway, Amazon DynamoDB 및 AWS Lambda를 사용하여 AWS에서 블로그 게시물 애플리케이션을 호스팅합니다. 애플리케이션은 현재 API 키를 사용하여 요청을 승인하지 않습니다. API 모델은 다음과 같습니다.

GET /posts/{postld} 를 사용하여 게시물 세부 정보를 가져옵니다

GET /users/{userld}. 사용자 세부 정보를 가져올 수 있습니다.

GET /comments/{commentld}: 주석 세부 정보를 얻으려면

회사는 사용자가 댓글 섹션에서 주제를 적극적으로 논의하고 있음을 알았으며 회사는 댓글을 실시간으로 표시하여 사용자 참여를 높이고 자합니다.

댓글 지연 시간을 줄이고 사용자 경험을 개선하기 위해 어떤 디자인을 사용해야 합니까?

A. Amazon CloudFront와 함께 엣지 최적화 API를 사용하여 API 응답을 캐시합니다.

B. 10초마다 GET comment[commented]을 요청하도록 블로그 애플리케이션 코드를 수정합니다.

C. AWS AppSync를 사용하고 웹 소켓을 활용하여 의견을 전달합니다.

D. Lambda 함수의 동시성 제한을 변경하여 API 응답 시간을 줄입니다.

Answer: C

Q261

솔루션 설계자가 여러 팀으로 구성된 회사의 AWS 계정 구조를 설계하고 있습니다. 모든 팀이 동일한 AWS 리전에서 작업하게 됩니다. 회사에는 온프레미스 네트워크에 연결된 VPC가 필요합니다. 이 회사는 온프레미스 네트워크를 오가는 총 50Mbps 미만을 기대합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. VPC와 필요한 서브넷을 프로비저닝하는 AWS CloudFormation 템플릿을 생성합니다. 템플릿을 각 AWS 계정에 배포합니다.

B. VPC와 필요한 서브넷을 프로비저닝하는 AWS CloudFormation 템플릿을 생성합니다. 템플릿을 공유 서비스 계정에 배포합니다. AWS 리소스 액세스 관리자를 사용하여 서브넷을 공유합니다.

C. 온프레미스 네트워크에 연결하려면 AWS 사이트 간 VPN과 함께 AWS Transit Gateway를 사용합니다. AWS 리소스 액세스 관리자를 사용하여 전송 게이트웨이를 공유합니다.

D. 온프레미스 네트워크에 연결하기 위해 AWS 사이트 간 VPN을 사용합니다.

E. 온프레미스 네트워크에 연결하기 위해 AWS Direct Connect를 사용합니다.

Answer: B, D

Q262

한 여행사가 Amazon Simple Email Service (Amazon SES) 를 통해 소비자에게 이메일 알림을 보내는 웹 애플리케이션을 개발했습니다. 조직은 이메일 전송 문제를 해결하기 위해 로깅을 허용해야 합니다. 또한 조직에는 수신자, 주제 및 전송 시간별로 검색을 수행할 수 있는 역량이 필요합니다.

이러한 요구 사항을 달성하기 위해 솔루션 설계자가 함께 수행해야 하는 작업은 무엇입니까?(두 개 선택)

A. Amazon Kinesis 데이터 파이어호스를 대상으로 사용하여 Amazon SES 구성 세트를 생성합니다. Amazon S3 버킷으로 로그를 전송하도록 선택합니다.

B. AWS CloudTrail 로깅을 활성화합니다. Amazon S3 버킷을 로그의 대상으로 지정합니다.

C. Amazon Athena를 사용하여 Amazon S3 버킷의 로그에서 수신자, 제목 및 전송 시간을 쿼리합니다.

D. AWS CloudTrail 로그 그룹을 생성합니다. 로그 그룹에 로그를 전송하도록 Amazon SES를 구성합니다.

E. Amazon Athena를 사용하여 수신자, 제목 및 전송 시간에 대해 Amazon CloudWatch의 로그를 쿼리합니다.

Answer: A, C

Q263

솔루션스 아키텍트는 회사의 AWS 조직 관리 계정에서 AWS 비용 및 사용 보고서 데이터를 제공해야 합니다. 이 회사에는 보고서를 저장할 Amazon S3 버킷이 이미 있습니다. 보고서는 다른 툴로 시각화할 수 있는 데이터베이스에 자동으로 수집되어야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(세 개 선택)

A. S3 버킷에 새 객체 생성이 트리거되는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.

B. AWS 비용 및 사용 보고서 구성을 생성하여 데이터를 S3 버킷으로 전송합니다.

C. S3 버킷에 새 객체 생성이 트리거될 AWS Glue 크롤러를 구성합니다.

D. S3 버킷에 새 객체 생성이 트리거될 AWS Lambda 함수를 생성합니다.

E. AWS Lambda 함수가 내 S3 버킷의 객체를 크롤링하도록 트리거할 AWS Glue 크롤러를 생성합니다.

F. Amazon EventBridge (Amazon CloudWatch Events) 규칙이 S3 버킷에서 객체를 크롤링하도록 트리거할 AWS Glue 크롤러를 생성합니다.

Answer: B, D, E

Q264

회사는 서버에 대한 패치 프로세스를 구현해야 합니다. 온프레미스 서버와 Amazon EC2 인스턴스는 다양한 도구를 사용하여 패치를 수행합니다. 관리에는 모든 서버와 인스턴스의 패치 상태를 보여주는 단일 보고서가 필요합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 조치를 취해야 합니까?

A. AWS 시스템 관리자를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리합니다. 시스템 관리자를 사용하여 패치 규정 준수 보고서를 생성합니다.

B. AWS OpsWorks를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리합니다. OpsWorks와 Amazon OuickSight 통합을 사용하여 패치 규정 준수 보고서를 생성합니다.

C. Amazon EventBridge (Amazon CloudWatch Events) 규칙을 사용하여 AWS 시스템 관리자 패치 수정 작업을 예약하여 패치를 적용합니다. Amazon 인스펙터를 사용하여 패치 규정 준수 보고서를 생성합니다.

D. AWS OpsWorks를 사용하여 온프레미스 서버 및 EC2 인스턴스의 패치를 관리합니다. AWS X-Ray를 사용하여 패치 상태를 AWS 시스템 관리자 OpsCenter에 게시하여 패치 규정 준수 보고서를 생성합니다.

Answer: A

Q265

한 스타트업 회사가 최근 대규모 전자 상거래 웹 사이트를 AWS로 마이그레이션했습니다.웹 사이트의 매출이 70% 증가했습니다. 소프트웨어 엔지니어는 비공개 GitHub 리포지토리를 사용하여 코드를 관리합니다. DevOps 학습은 빌드 및 단위 테스트에 Jenkins를 사용하는 것입니다. 엔지니어는 잘못된 빌드에 대한 알림을 받고 배포 중에 다운타임이 발생하지 않도록 해야 합니다. 또한 엔지니어는 프로덕션 변경 사항이 사용자에게 원활하고 중대한 문제가 발생할 경우 롤백할 수 있는지 확인해야 합니다.

소프트웨어 엔지니어는 AWS CodePipeline을 사용하여 빌드 및 배포 프로세스를 관리하기로 결정했습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. GitHub 웹 소켓을 사용하여 CodePipeline 파이프라인을 트리거합니다. AWS 코드빌드용 Jenkins 플러그인을 사용하여 단위 테스트를 수행합니다. 잘못된 빌드가 있으면 Amazon SNS 주제에 알림을 보냅니다. AWS CodeDeploy를 사용하여 현재 위치에서 한꺼번에 배포 구성으로 배포합니다.

B. GitHub 웹후크를 사용하여 CodePipeline 파이프라인을 트리거합니다. AWS 코드빌드용 Jenkins 플러그인을 사용하여 단위 테스트를 수행합니다. 잘못된 빌드가 있으면 Amazon SNS 주제에 알림을 보냅니다. AWS CodeDeploy를 사용하여 블루/그린 배포로 배포합니다.

C. GitHub 웹 소켓을 사용하여 CodePipeline 파이프라인을 트리거합니다. 유닛 테스트 및 정적 코드 분석에 AWS X-Ray를 사용합니다. 잘못된 빌드가 있으면 Amazon SNS 주제에 알림을 보냅니다. AWS CodeDeploy를 사용하여 블루/그린 배포로 배포합니다.

D. GitHub 웹후크를 사용하여 CodePipeline 파이프라인을 트리거합니다. 유닛 테스트 및 정적 코드 분석에 AWS X-Ray를 사용합니다. 잘못된 빌드가 있으면 Amazon SNS 주제에 알림을 보냅니다. AWS CodeDeploy를 사용하여 현재 위치에서 한 번에 모두 배포 구성으로 배포합니다.

Answer: B

설명

AWS CodePipeline은 GitHub 리포지토리가 변경될 때 GitHub에서 웹훅을 수신할 수 있습니다. Webhook은 CodePipeline에 파이프라인 실행을 시작하도록 지시할 수 있습니다.

AWS CodeBuild용 Jenkins 플러그인을 사용하여 CodeBuild를 Jenkins 빌드 작업과 통합할 수 있습니다. 빌드 작업을 Jenkins 빌드 노드로 보내는 대신 플러그인을 사용하여 빌드 작업을 CodeBuild로 보냅니다. 이렇게 하면 Jenkins 빌드 노드를 프로비저닝, 구성 및 관리할 필요가 없습니다.

SNS는 알림을 보내는 데 사용하는 명백한 도구이며 CodeDeploy는 블루/그린 배포 전략을 사용해야 합니다. 이 전략은 업데이트가 원활하고 필요한 경우 쉽게 롤백될 수 있도록 합니다.

잘못됨: A. 웹 소켓을 사용하여 CodePipeline을 트리거할 수 없으며 웹후크을 사용해야 합니다.

잘못됨: C. X-Ray는 단위 테스트에 사용할 수 없으며 추적에 사용됩니다. 또한 인플레이스(in-place) 일괄 배포 전략으로 인해 롤백이 어렵습니다.

잘못됨: D. . 웹 소켓을 사용하여 CodePipeline을 트리거할 수 없으며 웹후크을 사용해야 합니다.

참조:

https://aws.amazon.com/about-aws/whats-new/2018/05/aws-codepipeline-supports-push-events-from-github-via-webhooks/

https://docs.aws.amazon.com/codebuild/latest/userguide/jenkins-plugin.html

Q266

한 회사가 온프레미스에서 AWS 클라우드로 데이터 센터를 마이그레이션하고 있습니다. 마이그레이션을 완료하는 데 몇 개월이 걸립니다. 이 회사는 프라이빗 DNS 영역에 Amazon Route 53을 사용할 예정입니다. 마이그레이션 중에 회사는 AWS 서비스가 VPC의 DNS용 Route 53 확인자를 가리키도록 유지해야 합니다. 또한 온프레미스 DNS 서버에서 주소를 확인하는 기능도 유지해야 합니다. 솔루션스 아키텍트는 Amazon EC2 인스턴스가 네이티브 Route 53 엔드포인트를 사용하여 온프레미스 DNS 쿼리를 해결할 수 있도록 DNS를 설정해야 합니다.

이러한 요구 사항을 충족하는 구성 작성은 무엇입니까?

A. 온프레미스 DNS 서버 IP 주소를 가리키도록 설정된 Vie VPC DHCP 옵션 구성 EC2 인스턴스의 보안 그룹이 해당 DNS 서버 IP 주소의 포트 53에 대한 아웃바운드 액세스를 허용하는지 확인합니다.

B. DNS BIND를 설치하고 구성한 EC2 인스턴스를 시작합니다.EC2 인스턴스에 연결된 보안 그룹이 포트 53에 있는 온프레미스 DNS 서버 IP 주소에 액세스할 수 있는지 확인합니다. DNS 쿼리를 온-프레미스 DNS 서버 IP 주소로 전달하도록 BIND를 구성합니다. 마이그레이션된 각 EC2 인스턴스 DNS 설정이 BIND 서버 IP 주소를 가리키도록 구성합니다.

C. Route 53에서 새 아웃바운드 엔드포인트를 생성하고 VPC에 엔드포인트를 연결합니다. 엔드포인트에 연결된 보안 그룹이 포트 53에서 온-프레미스 DNS 서버 IP 주소에 액세스할 수 있는지 확인합니다. 온-프레미스에서 지정된 트래픽을 온프레미스 DNS 서버로 라우팅하는 새 Route 53 확인자 규칙을 생성합니다.

D. Route 53에서 온프레미스 도메인과 동일한 도메인 이름으로 새 프라이빗 DNS 영역을 생성합니다. 온-프레미스 DNS 서버 IP 주소를 레코드 주소로 사용하여 단일 와일드카드 레코드를 만듭니다.

Answer: C

Q267

한 회사가 AWS에서 REST API 애플리케이션을 설정할 계획입니다. 애플리케이션 팀이 AWS에 새로운 자격 증명 저장소를 설정하려고 합니다. IT 팀은 이 배포를 위해 인프라나 서버를 유지 관리하고 싶지 않습니다.

이러한 요구 사항을 충족하는 가장 운영 효율적인 솔루션은 무엇입니까?

A. 애플리케이션을 AWS Lambda 함수로 배포합니다. 애플리케이션에 대한 Amazon API Gateway REST API 엔드포인트를 설정합니다. Lambda 함수를 생성하고 Lambda 권한 부여자를 구성합니다.

B. AWS AppSync에 애플리케이션을 배포하고 AWS Lambda 해석기를 구성합니다. Amazon Cognito 사용자 풀을 설정하고 권한 부여를 위해 사용자 풀을 사용하도록 AWS AppSync를 구성합니다.

C. 애플리케이션을 AWS Lambda 함수로 배포합니다. 애플리케이션에 대한 Amazon API Gateway REST API 엔드포인트를 설정합니다. Amazon Cognito 사용자 풀을 설정하고 Amazon Cognito 권한 부여자를 구성합니다.

D. Amazon Elastic Kubemetes Service (Amazon EKS) 클러스터에 애플리케이션을 배포합니다. EKS 포드용 애플리케이션 로드 밸런서를 설정합니다. 인증을 위해 Amazon Cognito 사용자 풀 및 서비스 포드를 설정합니다.

Answer: C

Q268

한 회사에서 인터넷을 통해 액세스할 수 있는 SFTP 서버를 통해 고객에게 파일을 제공하고 있습니다. SFTP 서버는 탄력적 IP 주소가 연결된 단일 Amazon EC2 인스턴스에서 실행됩니다. 고객은 탄력적 IP 주소를 통해 SFTP 서버에 연결하고 인증에 SSH를 사용합니다. 또한 EC2 인스턴스에는 모든 고객 IP 주소에서 액세스할 수 있는 연결된 보안 그룹이 있습니다. 솔루션 설계자는 가용성을 높이고 인프라 관리의 복잡성을 최소화하며 파일에 액세스하는 고객의 업무 중단을 최소화하는 솔루션을 구현해야 합니다. 솔루션이 고객 연결 방식을 바꿔서는 안 됩니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS Transfer 패밀리 서버 생성 공개적으로 액세스 가능한 엔드포인트로 트랜스퍼 패밀리 서버 구성 SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. 트랜스퍼 패밀리 서버를 S3 버킷으로 지정합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

B. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다. AWS 트랜스퍼 패밀리 서버를 생성합니다. VPC에서 호스팅하는 인터넷 연결 엔드포인트를 사용하여 트랜스퍼 패밀리 서버를 구성합니다. SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다. 고객 IP 주소가 있는 보안 그룹을 새 엔드포인트에 연결합니다. 패밀리 전송 서버가 S3 버킷을 가리키도록 합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

C. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 새 Amazon Elastic File System (Amazon EFS) 파일 시스템을 생성합니다. AWS Fargate 작업 정의를 생성하여 SFTP 서버를 실행합니다. 작업 정의에서 EFS 파일 시스템을 마운트로 지정합니다. 작업 정의를 사용하여 Fargate 서비스를 만들고 서비스 앞에 NLB (네트워크 부하 분산 장치) 를 배치합니다. 서비스를 구성할 때 고객 IP 주소가 있는 보안 그룹을 SFTP 서버를 실행하는 작업에 연결합니다. 탄력적 IP 주소를 NLB와 연결합니다.SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

D. EC2 인스턴스에서 탄력적 IP 주소의 연결을 해제합니다. SFTP 파일 호스팅에 사용할 다중 연결 Amazon Elastic Block Store (Amazon EBS) 볼륨을 생성합니다. 탄력적 IP 주소가 연결된 NLB (네트워크 로드 밸런서) 를 만듭니다. SFTP 서버를 실행하는 EC2 인스턴스로 Auto Scaling 그룹 생성 Auto Scaling 그룹에서 시작되는 인스턴스가 새로운 다중 연결 EBS 볼륨을 연결하도록 정의 NLB 뒤에 인스턴스를 자동으로 추가하도록 Auto Scaling 그룹을 구성합니다. Auto Scaling 그룹이 시작하는 EC2 인스턴스에 대한 고객 IP 주소를 허용하는 보안 그룹입니다. SFTP 서버의 모든 파일을 새 다중 연결 EBS 볼륨으로 동기화합니다.

Answer: B

Q269

업계 규정을 준수하기 위해 솔루션 설계자는 회사의 본사가 위치한 미국을 비롯한 여러 퍼블릭 AWS 리전에 회사의 중요 데이터를 저장할 솔루션을 설계해야 합니다. 솔루션 설계자는 AWS에 저장된 데이터에 대한 액세스를 회사의 글로벌 WAN 네트워크에 제공해야 합니다. 보안 팀은 이 데이터에 액세스하는 트래픽이 공용 인터넷을 통과하지 않도록 의무화하고 있습니다.

솔루션 설계자는 요구 사항을 충족하고 비용 효율적인 고가용성 솔루션을 어떻게 설계해야 합니까?

A. 본사에서 사용 중인 모든 AWS 리전으로 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 본사로 트래픽을 전송 한 다음 해당 DX 연결로 트래픽을 전송하여 데이터에 액세스합니다.

B. 본사에서 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다.리전 간 VPC 피어링을 사용하여 다른 AWS 리전의 데이터에 액세스합니다.

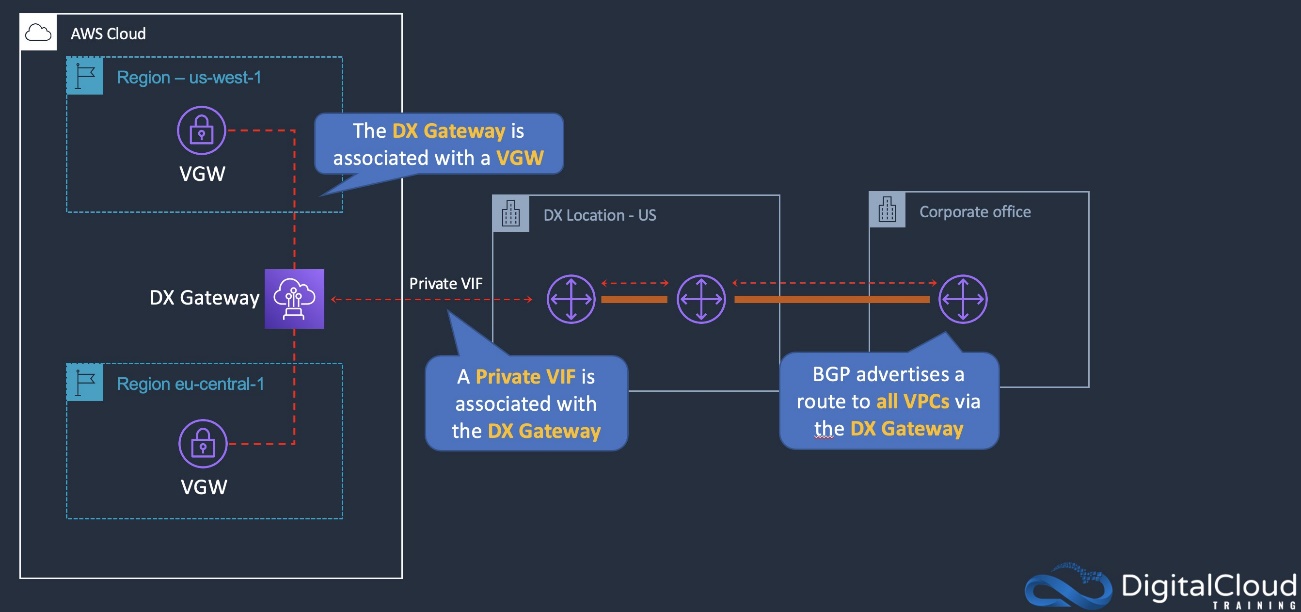
C. 본사에서 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다.AWS 전송 VPC 솔루션을 사용하여 다른 AWS 리전의 데이터에 액세스합니다.

D. 본사에서 AWS 리전으로 두 개의 AWS Direct Connect 연결을 설정합니다. 회사 WAN을 사용하여 DX 연결을 통해 트래픽을 전송합니다. 직접 연결 게이트웨이를 사용하여 다른 AWS 리전의 데이터에 액세스합니다.

Answer: D

설명

이것은 전송 게이트웨이 또는 가상 프라이빗 게이트웨이를 연결할 수 있는 DX 게이트웨이의 훌륭한 사용 사례입니다. 그런 다음 DX 게이트웨이를 사용하여 여러 AWS 리전에 대한 연결을 설정할 수 있습니다. 고가용성을 위해 이 솔루션에는 뉴욕 데이터 센터에서 2개의 DX 연결이 있어야 하며 WAN은 DX 연결을 통해 AWS로 연결을 전달하도록 BGP를 통해 구성해야 합니다.



잘못됨: A. DX 연결을 사용하여 여러 AWS 리전을 단일 데이터 센터에 연결하는 것은 비용이 많이 들고 필요하지 않기 때문에 원하지 않을 것입니다. 로컬 지역에 연결한 다음 거기에서 연결을 위해 DX 게이트웨이/Transit Gateway를 사용하는 것이 좋습니다.

잘못됨: B. 리전 간 VPC 피어링은 전이적 관계(전이적 피어링 없음)로 연결할 리전이 많은 경우 설정하기가 매우 복잡해집니다.

잘못됨: C. 전송 VPC는 ​​허브 및 스포크 모델에서 다른 VPC로 라우팅을 수행하도록 구성된 VPC입니다. 이것은 주로 대중 교통 게이트웨이로 대체되었습니다. 이 경우 여러 지역을 사용하고 있으므로 지역 간에 연결하려면 DX 게이트웨이를 사용해야 합니다.

Q270

한 회사에서 온프레미스 JavaScript 프런트 엔드 웹 애플리케이션을 관리합니다. 응용 프로그램은 회사 Active Directory로 보호되는 두 대의 서버에서 호스팅됩니다. 응용 프로그램은 응용 프로그램 서버에서 Java 기반 마이크로서비스 집합을 호출하고 클러스터된 MySQL 데이터베이스에 데이터를 저장합니다. 이 응용 프로그램은 평일 낮에 많이 사용됩니다.저녁과 주말에 가볍게 사용합니다. 애플리케이션에 대한 주간 트래픽이 급격히 증가했으며 그 결과 안정성이 떨어졌습니다. 이 회사는 마이크로서비스에 안전하게 연결하기 위한 API를 사용하여 서버 유지 관리가 필요 없는 솔루션을 사용하여 애플리케이션을 AWS로 마이그레이션하려고 합니다.

이러한 요구 사항을 충족하는 작업 조합은 무엇입니까?(세 개 선택)

A. Amazon S3에서 웹 애플리케이션을 호스팅합니다. 인증 및 권한 부여를 위해 SAML과 함께 Amazon Cognito 자격 증명 풀 (연동 자격 증명) 을 사용합니다.

B. 오토 스케일링을 사용하여 Amazon EC2에서 웹 애플리케이션을 호스팅합니다. 인증 및 권한 부여를 위해 Amazon Cognito 연동 및 Amazon에 로그인을 사용합니다.

C. Amazon API Gateway를 사용하여 API 계층을 생성합니다. AWS Fargate 컨테이너에서 마이크로서비스를 다시 호스팅합니다.

D. Amazon API Gateway를 사용하여 API 계층을 생성합니다. Amazon Elastic Container Service (Amazon ECS) 컨테이너에서 마이크로서비스를 다시 호스팅합니다.

E. 데이터베이스를 MySQL용 Amazon RDS로 다시 플랫폼합니다.

F. 데이터베이스를 Amazon Aurora MySQL 서버리스로 다시 플랫폼합니다.

Answer: A, C, F

Q271

회사에는 AWS 조직에 조직이 있습니다.이 조직은 별도의 사업부에 속하는 다수의 AWS 계정으로 구성됩니다.이 회사는 모든 Amazon EC2 인스턴스를 강화된 사용자 지정 AMI로 프로비저닝해야 합니다. 이 회사는 각 AWS 계정에 AMI에 대한 액세스 권한을 제공하는 솔루션을 원합니다.

운영 효율성이 가장 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. EC2 이미지 빌더로 AMI를 생성합니다. AWS CodePipeline 파이프라인을 생성하여 모든 AWS 계정에서 AMI를 공유합니다.

B. EC2 인스턴스에 Jenkins 배포 작업을 생성하여 모든 AWS 계정에서 AMI를 생성하고 공유합니다.

C. EC2 이미지 빌더와 AMI 생성 및 공유 AWS 서비스 카탈로그를 사용하여 모든 AWS 계정에서 AMI에 대한 액세스를 제공하는 제품을 구성합니다.

D. EC2 이미지 빌더로 AMI를 생성합니다. AWS Lambda 함수를 생성하여 모든 AWS 계정에서 AMI를 공유합니다.

Answer: C

Q271

회사에는 AWS 조직에 조직이 있습니다.이 조직은 별도의 사업부에 속하는 다수의 AWS 계정으로 구성됩니다.이 회사는 모든 Amazon EC2 인스턴스를 강화된 사용자 지정 AMI로 프로비저닝해야 합니다. 이 회사는 각 AWS 계정에 AMI에 대한 액세스 권한을 제공하는 솔루션을 원합니다.

운영 효율성이 가장 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. EC2 이미지 빌더로 AMI를 생성합니다. AWS CodePipeline 파이프라인을 생성하여 모든 AWS 계정에서 AMI를 공유합니다.

B. EC2 인스턴스에 Jenkins 배포 작업을 생성하여 모든 AWS 계정에서 AMI를 생성하고 공유합니다.

C. EC2 이미지 빌더와 AMI 생성 및 공유 AWS 서비스 카탈로그를 사용하여 모든 AWS 계정에서 AMI에 대한 액세스를 제공하는 제품을 구성합니다.

D. EC2 이미지 빌더로 AMI를 생성합니다. AWS Lambda 함수를 생성하여 모든 AWS 계정에서 AMI를 공유합니다.

Answer: C

Q272

한 회사가 Amazon EMR 플랫폼에 대한 비용 인식을 개선하고자 합니다. 이 회사는 각 팀의 Amazon EMR 사용량에 대한 예산을 보유하고 있습니다. 예산 임계값에 도달하면 예산 사무소의 배포 목록에 전자 메일로 알림을 보내야 합니다. 팀은 현재까지의 EMR 클러스터 비용을 볼 수 있어야 합니다. 솔루션 설계자는 다중 계정 환경에서 이 정책을 사전 예방적으로 중앙 집중식으로 적용할 수 있는 솔루션을 만들어야 합니다.

솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 조합해야 합니까?(두 개 선택)

A. NotificationsWithSubscnbers 속성이 있는 AWS 예산 예산 리소스를 포함하도록 AWS CloudFormation 템플릿을 업데이트합니다.

B. Amazon EMR 사용을 위한 Amazon CloudWatch 대시보드를 구현합니다.

C. 시작 시 실행되는 EMR 부트스트랩 작업을 생성하여 비용 탐색기 API를 호출하여 GetCostForecast 및 구독자 포함 알림 작업을 사용하여 클러스터에 예산을 설정합니다.

D. 각 팀에 대해 AWS Service Catalog 포트폴리오를 생성합니다. 각 팀의 Amazon EMR 클러스터를 제품으로서의 서비스 카탈로그 포트폴리오에 AWS CloudFormation 템플릿으로 추가합니다.

E. 청구를 위한 Amazon CloudWatch 지표 생성 비용이 예산 임계값을 초과할 경우 사용자 지정 알림을 생성합니다.

Answer: A, D

설명

AWS 예산을 사용하여 AWS Service Catalog 내에서 서비스 비용과 사용량을 추적할 수 있습니다. 예산을 AWS Service Catalog 제품 및 포트폴리오와 연결할 수 있습니다.

AWS 예산은 비용 또는 사용량이 예산 금액을 초과(또는 초과할 것으로 예측)될 때 알려주는 사용자 지정 예산을 설정할 수 있는 기능을 제공합니다.

예산이 제품과 연결된 경우 제품 및 제품 세부정보 페이지에서 예산에 대한 정보를 볼 수 있습니다. 예산이 포트폴리오와 연결된 경우 포트폴리오 및 포트폴리오 세부정보 페이지에서 예산에 대한 정보를 볼 수 있습니다.

제품 또는 포트폴리오를 클릭하면 상세 페이지로 이동합니다. 이러한 포트폴리오 세부정보 및 제품 세부정보 페이지에는 관련 예산에 대한 자세한 정보가 포함된 섹션이 있습니다. 예산 금액, 현재 지출 및 예상 지출을 볼 수 있습니다. 예산 세부 정보를 보고 예산을 편집할 수도 있습니다.

참조:

https://docs.aws.amazon.com/servicecatalog/latest/adminguide/catalogs\_budgets.html

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-budgets-budget.html

Q273

한 회사가 AWS Marketplace에서 타사 방화벽 어플라이언스 솔루션을 배포하여 회사의 AWS 환경을 떠나는 트래픽을 모니터링하고 보호하고 있습니다. 이 회사는 이 어플라이언스를 공유 서비스 VPC에 배포하고 어플라이언스를 통해 모든 아웃바운드 인터넷 바운드 트래픽을 라우팅하려고 합니다. 솔루션스 아키텍트는 안정성을 우선시하고 단일 AWS 리전 내의 방화벽 어플라이언스 간 장애 조치 시간을 최소화하는 배포 방법을 추천해야 합니다. 이 회사는 공유 서비스 VPC에서 다른 VPC로 라우팅을 설정했습니다. 솔루션 설계자는 이러한 요구 사항을 충족하기 위해 어떤 단계를 권장해야 합니까?(두 개 선택)

A. 두 방화벽 어플라이언스를 공유 서비스 VPC에 배포합니다. 각각 별도의 가용 영역에 있습니다.

B. 공유 서비스 VPC에 새 네트워크 로드 밸런서를 생성합니다. 새 대상 그룹을 생성하여 새 네트워크 로드 밸런서에 연결합니다. 각 방화벽 어플라이언스 인스턴스를 대상 그룹에 추가합니다.

C. 공유 서비스 VPC에 새 게이트웨이 로드 밸런서를 생성합니다. 새 대상 그룹을 생성하여 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. 두 방화벽 어플라이언스를 공유 서비스 VPC에 배포합니다. 각각 동일한 가용 영역에 있습니다.

Answer: A, C

Q274

한 회사가 애플리케이션 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 여러 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 애플리케이션에 대한 로드는 하루 종일 달라지며 EC2 인스턴스는 정기적으로 확장 및 축소됩니다. EC2 인스턴스의 로그 파일은 15분마다 중앙 Amazon S3 버킷으로 복사됩니다. 보안 팀은 종료된 EC2 인스턴스 중 일부에서 로그 파일이 누락되었음을 발견합니다.

로그 파일이 종료된 EC2 인스턴스에서 중앙 S3 버킷으로 복사되도록 보장하는 작업 세트는 무엇입니까?

A. 스크립트를 생성하여 로그 파일을 Amazon S3에 복사하고 EC2 인스턴스의 파일에 스크립트를 저장합니다. 오토 스케일링 수명 주기 후크 및 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성하여 오토 스케일링 그룹에서 수명 주기 이벤트를 감지합니다. 자동 확장:EC2\_Instance\_terminating 전환에서 AWS Lambda 함수를 호출하여 종료를 방지하기 위해 ABANDON을 Auto Scaling 그룹에 보내고, 스크립트를 실행하여 로그 파일을 복사하고, AWS SDK를 사용하여 인스턴스를 종료합니다.

B. 로그 파일을 Amazon S3로 복사하는 스크립트가 포함된 AWS 시스템 관리자 문서를 생성합니다. 오토 스케일링 수명 주기 후크 및 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성하여 오토 스케일링 그룹에서 수명 주기 이벤트를 감지합니다. 자동 확장:EC2\_Instance\_terminating 전환에서 AWS Lambda 함수를 호출하여 AWS 시스템 관리자 API sendCommand 작업을 호출하여 문서를 실행하여 로그 파일을 복사하고 자동 조정 그룹에 CONTINUE를 전송하여 인스턴스를 종료합니다.

C. 로그 전송 속도를 5분마다 변경합니다. 로그 파일을 Amazon S3에 복사하는 스크립트를 생성하고 EC2 인스턴스 사용자 데이터에 스크립트를 추가합니다. EC2 인스턴스 종료를 감지하는 Amazon EventBridge (Amazon CloudWatch Events) 규칙을 생성합니다.AWS CLI를 사용하여 사용자 데이터 스크립트를 실행하여 로그 파일을 복사하고 인스턴스를 종료하는 EventBridge (CloudWatch 이벤트) 규칙에서 AWS Lambda 함수를 호출합니다.

D. 로그 파일을 Amazon S3로 복사하는 스크립트가 포함된 AWS 시스템 관리자 문서를 생성합니다. Amazon Simple Notification Service (Amazon SNS) 주제에 메시지를 게시하는 Auto Scaling 수명 주기 후크를 생성합니다. SNS 알림에서 AWS 시스템 관리자 API sendCommand 작업을 호출하여 문서를 실행하여 로그 파일을 복사하고 ABANDON을 오토 스케일링 그룹에 전송하여 인스턴스를 종료합니다.

Answer: B

Q275

한 회사에서 Amazon CloudFront 배포를 사용하여 애플리케이션 로드 밸런서 뒤에서 실행되는 웹 애플리케이션의 정적 콘텐츠와 동적 콘텐츠를 모두 배포하고 있습니다. 웹 애플리케이션에는 동적 콘텐츠에 대한 사용자 인증 및 세션 추적이 필요합니다. CloudFront 배포에는 권한 부여, 호스트 및 에이전트 HTTP 허용 목록 헤더와 세션 쿠키를 오리진에 전달하도록 구성된 단일 캐시 동작이 있습니다. 다른 모든 캐시 동작 설정은 기본값으로 설정됩니다.배포 설정에서 일치하는 CNAME이 있는 CloudFront 배포에 유효한 ACM 인증서가 적용됩니다. ACM 인증서는 애플리케이션 로드 밸런서의 HTTPS 리스너에도 적용됩니다. CloudFront 오리진 프로토콜 정책이 HTTPS 전용으로 설정됨 캐시 통계 분석 보고서에 따르면 이 배포에 대한 실패율이 매우 높은 것으로 나타났습니다.

CloudFront와 애플리케이션 로드 밸런서 간의 SSL/TLS 핸드셰이크가 실패하지 않으면서 이 배포에 대한 캐시 적중률을 개선하기 위해 솔루션스 아키텍트는 무엇을 할 수 있을까요?

A. 정적 및 동적 콘텐츠에 대해 두 가지 캐시 동작을 만듭니다. 두 캐시 동작의 화이트리스트 헤더 섹션에서 User-Agent 및 Host HTTP 헤더를 제거합니다. 정적 콘텐츠에 대해 구성된 캐시 동작에 대해서는 화이트리스트 쿠키 섹션에서 세션 쿠키를 제거하고 화이트리스트 헤더 섹션에서 권한 부여 HTTP 헤더를 제거합니다.

B. 캐시 동작의 화이트리스트 헤더 섹션에서 사용자-에이전트 및 권한 부여 HTTP 헤더를 제거합니다. 그런 다음 승인을 위해 미리 서명된 쿠키를 사용하도록 캐시 동작을 업데이트합니다.

C. 허용 목록 헤더 섹션에서 Host HTTP 헤더를 제거하고 기본 캐시 동작에 대한 허용 목록 쿠키 섹션에서 세션 쿠키를 제거합니다. 자동 객체 압축을 활성화하고 사용자 권한 부여를 위해 Lambda @Edge 최종 사용자 요청 이벤트를 사용합니다.

D. 정적 및 동적 내용에 대해 두 가지 캐시 동작을 만듭니다. 두 캐시 동작의 화이트리스트 헤더 섹션에서 User-Agent HTTP 헤더를 제거합니다. 정적 콘텐츠에 대해 구성된 캐시 동작에 대해서는 화이트리스트 쿠키 섹션에서 세션 쿠키를 제거하고 화이트리스트 헤더 섹션에서 권한 부여 HTTP 헤더를 제거합니다.

Answer: D

Q276

회사에는 사용자 콘텐츠용 Amazon S3 버킷이 포함된 플랫폼이 있습니다. S3 버킷에는 수천 테라바이트의 객체가 있으며 모두 S3 표준 스토리지 클래스에 있습니다. 회사의 RTO는 6시간입니다. 회사는 기본 AWS 리전의 데이터를 다른 리전의 복제 S3 버킷으로 복제해야 합니다. 사용자 콘텐츠 S3 버킷에는 동영상 및 사진과 같은 사용자가 업로드한 파일이 포함되어 있습니다. 사용자 콘텐츠 S3 버킷에 예측할 수 없는 액세스 패턴이 있습니다. 사용자 수가 빠르게 증가하고 있으며, 이 회사는 스토리지 비용을 줄이기 위해 S3 수명 주기 정책을 만들고자 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. 사용자 콘텐츠 S3 버킷의 객체를 즉시 S3 Intelligent-Tiering으로 이동합니다.

B. 30일 후에 사용자 콘텐츠 S3 버킷의 객체를 S3 Intelligent-Tiering으로 이동합니다.

C. 복제 S3 버킷의 객체를 30일 후에는 S3 Standard-Infrequent Access (S3 Standard-IA) 로 이동하고 90일 후에는 S3 Glacier로 이동합니다.

D. 복제 S3 버킷의 객체를 30일 후에는 S3 One Zone-Infrequent Access (S3 One Zone-IA) 로 이동하고 90일 후에는 S3 Glacier Deep Archive로 이동합니다.

E. 복제 S3 버킷의 객체를 30일 후에는 S3 Standard-infrequent Access (S3 Standard-IA) 로 이동하고 180일 후에는 S3 Glacier Deep Archive로 이동합니다.

Answer: A, D

Q277

멀티미디어 회사는 비용 효율적인 방식으로 VOD (주문형 비디오) 콘텐츠를 가입자에게 제공해야 합니다. 비디오 파일의 크기는 1 ~ 15GB이며 일반적으로 처음 6 개월 동안 자주 볼 수 있으므로 액세스가 크게 줄어 듭니다. 회사는 구독자가 모든 비디오 파일을 즉시 사용할 수 있도록 요구합니다. 현재 약 30.000 개의 파일이 있으며 회사는 시간이 지남에 따라 그 수가 두 배로 늘어날 것으로 예상합니다.

회사의 VOD 콘텐츠를 제공하는 데 가장 비용 효율적인 솔루션은 무엇입니까?

A. S3 인텔리전트 티어링을 사용하여 비디오 파일을 Amazon S3 버킷에 저장합니다. Amazon CloudFront를 사용하여 S3 버킷을 오리진으로 사용하여 콘텐츠를 전송합니다.

B. AWS Elemental MediaConvert를 사용하고 적응형 비트레이트 비디오 파일을 Amazon S3에 저장합니다. Amazon S3에서 콘텐츠를 전송하도록 AWS Elemental MediaPackage 엔드포인트를 구성합니다.

C. 비디오 파일을 Amazon Elastic File System (Amazon EFS) Standard에 저장합니다. EFS 수명 주기 관리를 통해 6개월 후에 비디오 파일을 EFS 가끔 액세스로 이동할 수 있습니다. 탄력적 로드 밸런서 뒤에 Amazon EC2 오토 스케일링 그룹을 생성하여 Amazon EFS의 콘텐츠를 전송합니다.

D. 비디오 파일을 Amazon S3 스탠다드에 저장합니다. 비디오 파일을 6개월 후에는 S3 Standard-Infrequent Access (S3 Standard-IA) 로 이동하고 1년 후에는 S3 Glacier Deep 아카이브로 이동하는 S3 수명 주기 규칙을 생성합니다. Amazon CloudFront를 사용하여 S3 버킷을 오리진으로 사용하여 콘텐츠를 전송합니다.

Answer: A

Q278

회사에는 사용자가 비디오를 업로드할 수 있는 웹 사이트가 있습니다. 회사 정책에 따르면 업로드된 동영상은 제한된 콘텐츠에 대해 분석해야 합니다. 업로드된 동영상이 Amazon S3에 배치되고 메시지가 동영상의 위치와 함께 Amazon SQS 대기열로 푸시됩니다. 백엔드 애플리케이션은 Amazon SQS에서 이 위치를 가져와 비디오를 분석합니다. 비디오 분석은 컴퓨팅 집약적이며 낮에는 산발적으로 발생합니다. 웹 사이트는 수요에 따라 확장됩니다.비디오 분석 애플리케이션은 고정된 수의 인스턴스에서 실행됩니다. 피크 수요는 휴일 동안 발생하므로 회사는 이 기간 동안 애플리케이션에 인스턴스를 추가해야 합니다. 사용되는 모든 인스턴스는 현재 온디맨드 Amazon EC2 T2 인스턴스입니다.이 회사는 현재 솔루션의 비용을 줄이려고 합니다.

다음 중 가장 비용 효율적인 솔루션은 무엇입니까?

A. 웹 사이트를 T2 인스턴스에 유지합니다. 피크 수요를 처리하기 위해 예약 인스턴스를 사용하는 동안 사용량이 적은 시간에 필요한 최소 웹 사이트 인스턴스 수를 결정하고 스팟 인스턴스를 사용하여 인스턴스를 처리합니다. 비디오 분석 애플리케이션을 위해 Auto Scaling 그룹에서 Amazon EC2 R4 및 Amazon EC2 R5 예약 인스턴스를 사용합니다.

B. 웹 사이트를 T2 인스턴스에 유지합니다. 사용량이 적은 시간에 필요한 최소 웹 사이트 인스턴스 수를 결정하고 예약 인스턴스를 사용하여 최대 수요를 처리하는 동안 온디맨드 인스턴스를 사용합니다.Amazon EC2 C4 및 Amazon EC2 C5 스팟 인스턴스로 구성된 비디오 분석 애플리케이션에 스팟 집합을 사용합니다.

C. 웹 사이트를 AWS 엘라스틱 빈스토크 및 Amazon EC2 C4 인스턴스로 마이그레이션합니다. 사용량이 적은 시간에 필요한 최소 웹 사이트 인스턴스 수를 결정하고 온디맨드 인스턴스를 사용하여 스팟 용량을 사용하여 피크 수요를 처리합니다. C4 및 Amazon EC2 C5 인스턴스로 구성된 비디오 분석 애플리케이션에는 스팟 집합을 사용합니다.

D. 웹 사이트를 AWS 엘라스틱 빈스토크 및 Amazon EC2 R4 인스턴스로 마이그레이션합니다. 사용량이 적은 시간에 필요한 최소 웹 사이트 인스턴스 수를 결정하고 예약 인스턴스를 사용하여 최대 수요를 처리하는 동안 예약 인스턴스를 사용하여 최대 수요를 처리합니다. R4 및 Amazon EC2 R5 인스턴스로 구성된 비디오 분석 애플리케이션에는 스팟 집합을 사용합니다.

Answer: B

Q279

AWS 파트너 회사가 조직이라는 조직을 사용하여 AWS 조직에 서비스를 구축하고 있습니다. 이 서비스를 사용하려면 파트너 회사가 org2라는 별도의 조직에 있는 고객 계정의 AWS 리소스에 액세스할 수 있어야 합니다. 회사는 고객 계정에 대한 API 또는 명령줄 도구를 사용하여 최소 권한 보안 액세스를 설정해야 합니다.

org1이 org2의 리소스에 액세스하도록 허용하는 가장 안전한 방법은 무엇입니까?

A. 고객은 로그인하고 필요한 작업을 수행할 수 있도록 파트너 회사에 AWS 계정 액세스 키를 제공해야 합니다.

B. 고객은 IAM 사용자를 생성하고 IAM 사용자에게 필요한 권한을 할당해야 합니다. 그런 다음 고객은 파트너 회사에 자격 증명을 제공하여 로그인하고 필요한 작업을 수행해야 합니다.

C. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위해 액세스를 요청할 때 IAM 역할의 Amazon Resource Name (ARN) 을 사용해야 합니다.

D. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위한 액세스를 요청할 때 IAM 역할의 신뢰 정책에 있는 외부 ID를 포함하여 IAM 역할의 Amazon Resource Name (ARN) 을 사용해야 합니다.

Answer: D

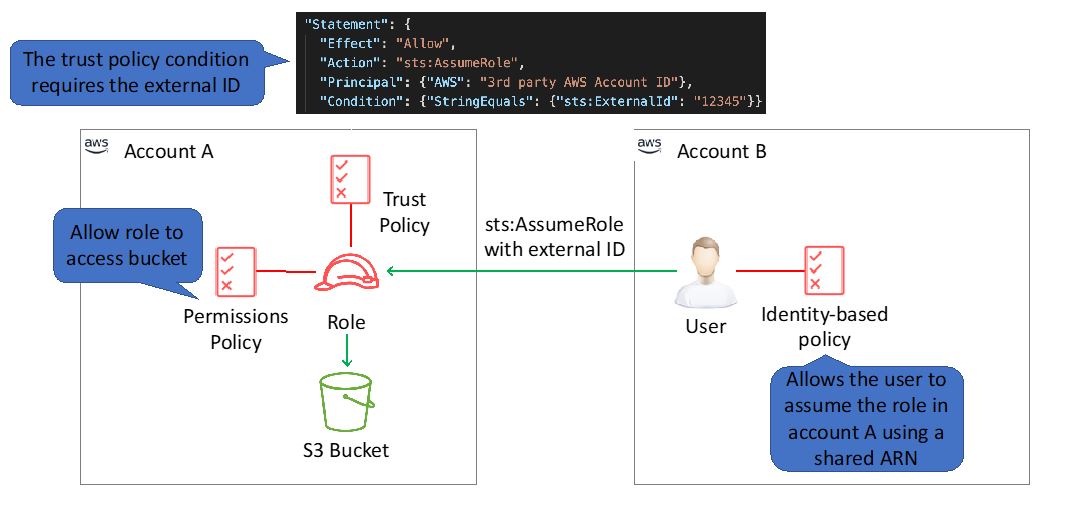
설명

때때로 제3자에게 AWS 리소스에 대한 액세스 권한을 부여해야 합니다(위임자 액세스). 이 시나리오의 한 가지 중요한 측면은 역할을 맡을 수 있는 사람을 지정하기 위해 IAM 역할 신뢰 정책에서 사용할 수 있는 선택적 정보인 외부 ID입니다.

역할을 수임할 때 제3자가 외부 ID를 제공하도록 요구하려면 선택한 외부 ID로 역할의 신뢰 정책을 업데이트하십시오.

역할을 수임할 때 외부 ID를 제공하려면 AWS CLI 또는 AWS API를 사용하여 해당 역할을 수임합니다.

다음 다이어그램은 이 구성을 보여줍니다.



잘못됨: A. 액세스 키는 절대 공유해서는 안 됩니다!

잘못됨: B. 사용자가 아닌 역할을 사용해야 합니다.

잘못됨: C. 이 답변에는 보안에 필요한 외부 ID가 없습니다.

참조:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-user\_externalid.html

Q280

한 회사에서 웹 애플리케이션을 개발했습니다. 이 회사는 애플리케이션 로드 밸런서 뒤에 있는 Amazon EC2 인스턴스 그룹에서 애플리케이션을 호스팅하고 있습니다. 이 회사는 애플리케이션의 보안 태세를 개선하고자 하며 AWS WAF 웹 ACL을 사용할 계획입니다. 이 솔루션은 애플리케이션에 대한 합법적인 트래픽에 부정적인 영향을 주어서는 안 됩니다.

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

A. 웹 ACL 규칙의 작업을 카운트로 설정합니다. AWS WAF 로깅 활성화 오탐에 대한 요청 분석 오탐을 방지하기 위해 규칙을 수정합니다. 시간이 지남에 따라 웹 ACL 규칙의 작업을 카운트에서 차단으로 변경합니다.

B. 웹 ACL에는 속도 기반 규칙만 사용하고 스로틀 제한을 가능한 높게 설정합니다. 제한을 초과하는 모든 요청을 일시적으로 차단합니다.중첩 규칙을 정의하여 속도 추적의 범위를 좁힙니다.

C. 웹 ACL 규칙의 작업을 차단으로 설정합니다. 웹 ACL에는 AWS 관리형 규칙 그룹만 사용 AWS WAF 샘플링된 요청 또는 AWS WAF 로그와 함께 Amazon CloudWatch 지표를 사용하여 규칙 그룹을 평가합니다.

D. 웹 ACL에는 사용자 지정 규칙 그룹만 사용하고 작업을 AWS WAF 로깅 활성화 허용으로 설정합니다. 오탐에 대한 요청 분석 오탐을 방지하기 위해 규칙을 수정합니다. 시간이 지남에 따라 웹 ACL 규칙의 작업을 허용에서 차단으로 변경합니다.

Answer: B

Q281

한 렌터카 회사에서 모바일 앱에 데이터를 제공하기 위해 서버리스 REST API를 구축했습니다. 이 앱은 리전 엔드포인트가 있는 Amazon API Gateway API, AWS Lambda 함수 및 Amazon Aurora MySQL 서버리스 DB 클러스터로 구성됩니다. 이 회사는 최근 파트너의 모바일 앱에 API를 공개했습니다. 요청 수가 크게 증가하여 산발적인 데이터베이스 메모리 오류가 발생했습니다. API 트래픽을 분석한 결과 클라이언트가 단기간에 동일한 쿼리에 대해 여러 HTTP GET 요청을 수행하고 있음을 알 수 있습니다. 업무 시간 중에 트래픽이 집중되어 급증합니다. 이 회사는 솔루션과 관련된 비용 증가를 최소화하면서 추가 사용을 지원할 수 있는 능력을 향상시켜야 합니다.

이러한 요구 사항을 충족하는 전략은 무엇입니까?

A. API Gateway 리전 엔드포인트를 엣지 최적화 엔드포인트로 변환 프로덕션 단계에서 캐싱을 활성화합니다.

B. Redis용 Amazon ElastiCache 캐시를 구현하여 데이터베이스 호출 결과를 저장합니다. 캐시를 사용하도록 Lambda 함수를 수정합니다.

C. 사용 가능한 최대 메모리 양을 늘리도록 Aurora 서버리스 DB 클러스터 구성을 수정합니다.

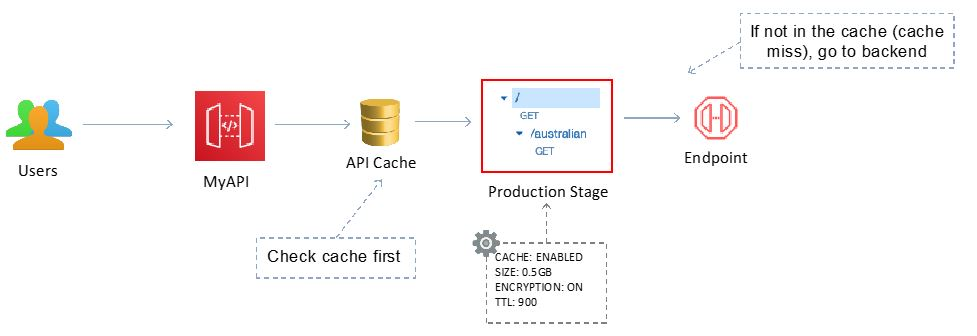
D. API Gateway 프로덕션 단계에서 스로틀 활성화 수신 통화를 제한하도록 속도 및 버스트 값을 설정합니다.

Answer: A

설명

에지 최적화 API 엔드포인트는 지리적으로 분산된 클라이언트에 가장 적합합니다. API 요청은 가장 가까운 CloudFront POP(Point of Presence)로 라우팅됩니다. 모바일 클라이언트의 경우 이 유형의 끝점에 대한 좋은 사용 사례입니다. 리전 엔드포인트는 리전 내에서만 들어오는 트래픽에 가장 적합합니다.

Amazon API Gateway에서 API 캐싱을 활성화하여 엔드포인트의 응답을 캐싱할 수 있습니다. 캐싱을 사용하면 엔드포인트에 대한 호출 수를 줄이고 API에 대한 요청 지연 시간도 개선할 수 있습니다.



잘못됨: B. 이렇게 하면 ElastiCache 클러스터가 비쌀 수 있으므로 솔루션과 관련된 비용이 증가합니다.

잘못됨: C. 이는 트래픽이 증가할 때뿐만 아니라 항상 데이터베이스 클러스터 비용이 더 많이 든다는 것을 의미합니다.

참조:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html

Q282

회사는 맞춤형 모바일 앱을 사용하여 모바일 장치에서 업로드할 이미지 데이터를 저장하고 처리해야 합니다. 사용량은 평일 오전 8시에서 오후 5시 사이에 최고치를 기록하며 분당 수천 건의 업로드가 발생합니다. 이 앱은 다른 시간에 거의 사용되지 않습니다. 이미지 처리가 완료되면 사용자에게 알림이 전송됩니다.

부하를 처리하기 위해 이미지 처리를 확장할 수 있도록 솔루션 설계자가 수행해야 하는 작업 조합은 무엇입니까?(세 개 선택)

A. 모바일 소프트웨어에서 Amazon S3로 직접 파일을 업로드합니다. S3 이벤트 알림을 사용하여 Amazon MQ 대기열에 메시지를 생성합니다.

B. 모바일 소프트웨어에서 Amazon S3로 직접 파일을 업로드합니다. S3 이벤트 알림을 사용하여 Amazon Simple Queue Service (Amazon SQS) 표준 대기열에 메시지를 생성합니다.

C. 대기열에서 메시지를 사용할 수 있을 때 AWS Lambda 함수를 호출하여 이미지 처리를 수행합니다.

D. 대기열에서 메시지를 사용할 수 있을 때 S3 배치 작업 작업을 호출하여 이미지 처리를 수행합니다.

E. 처리가 완료되면 Amazon Simple Notification Service (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.

Answer: B, C, E

Q283

한 회사가 단일 AWS 리전에 있는 5개의 Amazon EC2 인스턴스에서 실행해야 하는 새로운 애플리케이션을 보유하고 있습니다. 애플리케이션을 실행하려면 애플리케이션이 실행될 모든 EC2 인스턴스 간에 처리량이 높고 지연 시간이 짧은 네트워크 연결이 필요합니다. 응용 프로그램에 내결함성이 있어야 할 필요는 없습니다.

이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 5개의 새 EC2 인스턴스를 클러스터 배치 그룹으로 시작합니다.EC2 인스턴스 유형이 향상된 네트워킹을 지원하는지 확인합니다.

B. 동일한 가용 영역에 있는 Auto Scaling 그룹으로 5개의 새 EC2 인스턴스를 시작합니다. 각 EC2 인스턴스에 추가 탄력적 네트워크 인터페이스를 연결합니다.

C. 5개의 새 EC2 인스턴스를 파티션 배치 그룹으로 시작합니다.EC2 인스턴스 유형이 향상된 네트워킹을 지원하는지 확인합니다.

D. 5개의 새 EC2 인스턴스를 분산 배치 그룹으로 시작합니다. 각 EC2 인스턴스에 추가 탄력적 네트워크 인터페이스를 연결합니다.

Answer: A

Q284

한 회사에서 Amazon EMR 클러스터를 사용하여 빅 데이터 작업을 실행하고 있습니다.클러스터의 작업은 AWS 스텝 함수 익스프레스에 의해 호출됩니다. 다양한 Amazon Simple Queue Service (Amazon SQS) 대기열을 사용하는 워크플로입니다. 이 솔루션의 워크로드는 가변적이며 예측할 수 없는 Amazon CloudWatch 지표에 따르면 클러스터의 최대 사용률은 때때로 25% 에 불과하고 나머지 시간 동안은 클러스터가 유휴 상태임을 알 수 있습니다. 솔루션 설계자는 다양한 작업을 실행하는 데 걸리는 시간에 부정적인 영향을 주지 않으면서 클러스터 비용을 최적화해야 합니다.

이러한 요구 사항을 충족하는 가장 비용 효율적인 솔루션은 무엇입니까?

A. 클러스터 사용률을 기반으로 하는 사용자 지정 정책으로 코어 노드 및 작업 노드의 자동 크기 조정을 설정하여 EMR 클러스터를 수정합니다. 마스터 노드에 사용할 예약 인스턴스 용량을 구매합니다.

B. 마스터 노드 및 코어 노드에 전용 온디맨드 인스턴스의 인스턴스 집합을 사용하고 작업 노드에 스팟 인스턴스를 사용하도록 EMR 클러스터를 수정합니다. 부하를 처리할 각 노드 유형의 목표 용량을 정의합니다.

C. 마스터 노드와 코어 노드에 대한 예약 인스턴스를 구매합니다. EMR 클러스터의 모든 기존 작업 노드를 종료합니다.

D. 용량이 최적화된 스팟 인스턴스와 다양한 작업 집합을 사용하도록 EMR 클러스터를 수정합니다. 온디맨드 인스턴스와 스팟 인스턴스를 혼합하여 각 노드 유형의 목표 용량을 정의합니다.

Answer: B

Q285

AWS 파트너 회사가 조직이라는 조직을 사용하여 AWS 조직에 서비스를 구축하고 있습니다. 이 서비스를 사용하려면 파트너 회사가 org2라는 별도의 조직에 있는 고객 계정의 AWS 리소스에 액세스할 수 있어야 합니다. 회사는 고객 계정에 대한 API 또는 명령줄 도구를 사용하여 최소 권한 보안 액세스를 설정해야 합니다.

org1이 org2의 리소스에 액S세스하도록 허용하는 가장 안전한 방법은 무엇입니까?

A. 고객은 로그인하고 필요한 작업을 수행할 수 있도록 파트너 회사에 AWS 계정 액세스 키를 제공해야 합니다.

B. 고객은 IAM 사용자를 생성하고 IAM 사용자에게 필요한 권한을 할당해야 합니다. 그런 다음 고객은 파트너 회사에 자격 증명을 제공하여 로그인하고 필요한 작업을 수행해야 합니다.

C. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위해 액세스를 요청할 때 IAM 역할의 Amazon Resource Name (ARN) 을 사용해야 합니다.

D. 고객은 IAM 역할을 생성하고 IAM 역할에 필요한 권한을 할당해야 합니다. 그런 다음 파트너 회사는 필요한 작업을 수행하기 위한 액세스를 요청할 때 IAM 역할의 신뢰 정책에 있는 외부 ID를 포함하여 IAM 역할의 Amazon Resource Name (ARN) 을 사용해야 합니다.

Answer: D

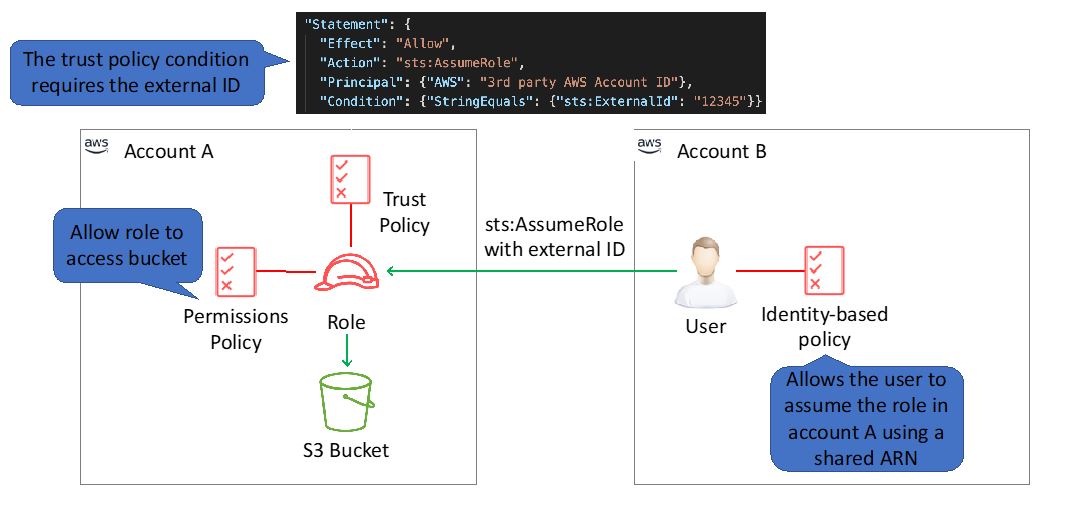
설명

때때로 제3자에게 AWS 리소스에 대한 액세스 권한을 부여해야 합니다(위임자 액세스). 이 시나리오의 한 가지 중요한 측면은 역할을 맡을 수 있는 사람을 지정하기 위해 IAM 역할 신뢰 정책에서 사용할 수 있는 선택적 정보인 외부 ID입니다.

역할을 수임할 때 제3자가 외부 ID를 제공하도록 요구하려면 선택한 외부 ID로 역할의 신뢰 정책을 업데이트하십시오.

역할을 수임할 때 외부 ID를 제공하려면 AWS CLI 또는 AWS API를 사용하여 해당 역할을 수임합니다.

다음 다이어그램은 이 구성을 보여줍니다.



잘못됨: A. 액세스 키는 절대 공유해서는 안 됩니다!

잘못됨: B. 사용자가 아닌 역할을 사용해야 합니다.

잘못됨: C. 이 답변에는 보안에 필요한 외부 ID가 없습니다.

참조:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-user\_externalid.html

Q286

한 솔루션 설계자가 온프레미스에서 Amazon Redshift로 영업 데이터가 포함된 50TB Oracle 데이터 웨어하우스를 마이그레이션하도록 지정되었습니다. 판매 데이터에 대한 주요 업데이트는 해당 월의 마지막 날에 발생합니다. 해당 월의 나머지 기간 동안 데이터 웨어하우스는 사소한 일일 업데이트만 받으며 주로 읽기 및 보고에 사용됩니다. 따라서 마이그레이션 프로세스는 해당 월의 첫 번째 날에 시작되어야 하며 다음 업데이트 집합이 발생하기 전에 완료되어야 합니다. 이렇게 하면 마이그레이션을 완료하는 데 약 30일이 소요되며 사소한 일일 변경 사항이 Amazon Redshift 데이터 웨어하우스와 동기화되었는지 확인할 수 있습니다. 마이그레이션은 일반적인 비즈니스 네트워크 작업에 영향을 줄 수 없으므로 인터넷을 통한 데이터 이동을 위해 마이그레이션에 할당되는 대역폭은 50Mbps입니다. 이 회사는 데이터 마이그레이션 비용을 낮게 유지하려고 합니다.

솔루션 설계자가 지정된 일정 내에 마이그레이션을 수행할 수 있는 단계는 무엇입니까?

A. Amazon EC2 인스턴스에 Oracle 데이터베이스 소프트웨어를 설치합니다. AWS와 회사의 데이터 센터 간에 VPN 연결을 구성합니다.Oracle RAC (실제 애플리케이션 클러스터) 에 가입하도록 Amazon EC2에서 실행 중인 Oracle 데이터베이스를 구성합니다. Amazon EC2의 Oracle 데이터베이스가 동기화를 마치면 AWS DMS 지속적 복제 작업을 생성하여 Amazon EC2의 Oracle 데이터베이스에서 Amazon Redshift로 데이터를 마이그레이션합니다. 데이터 마이그레이션이 완료되었는지 확인하고 Amazon Redshift로 전환을 수행합니다.

B. AWS Snowball 가져오기 작업을 생성합니다. Oracle 데이터 웨어하우스의 백업을 익스포트합니다. 내보낸 데이터를 Snowball 디바이스에 복사합니다.Snowball 디바이스를 AWS로 반환합니다. Oracle용 Amazon RDS 데이터베이스를 생성하고 백업 파일을 해당 RDS 인스턴스로 복원합니다. AWS DMS 작업을 생성하여 Oracle용 RDS 데이터베이스에서 Amazon Redshift로 데이터를 마이그레이션합니다. 인터넷을 통해 데이터 센터의 Oracle에서 Oracle용 RDS 데이터베이스로 일일 증분 백업을 복사합니다. 데이터 마이그레이션이 완료되었는지 확인하고 Amazon Redshift로 전환을 수행합니다.

C. Amazon EC2 인스턴스에 Oracle 데이터베이스 소프트웨어를 설치합니다. 마이그레이션 시간을 최소화하려면 1Gbps AWS Direct Connect 연결을 프로비저닝하여 AWS와 회사의 데이터 센터 간에 VPN 연결을 구성합니다. Amazon EC2에서 실행되는 Oracle 데이터베이스를 데이터 센터 Oracle 데이터베이스의 읽기 전용 복제본이 되도록 구성합니다. 회사의 온프레미스 데이터 센터와 Amazon EC2의 Oracle 데이터베이스 간의 동기화 프로세스를 시작합니다. Amazon EC2의 Oracle 데이터베이스가 온프레미스 데이터베이스와 동기화되면 AWS DMS 지속적 복제 작업을 생성하여 Amazon EC2에서 실행 중인 Oracle 데이터베이스 읽기 전용 복제본에서 Amazon Redshift로 데이터를 마이그레이션합니다.데이터 마이그레이션이 완료되었는지 확인하고 Amazon Redshift로 전환을 수행합니다.

D. AWS Snowball 가져오기 작업을 생성합니다. 추출 에이전트를 사용하여 회사 데이터 센터에 서버를 구성합니다. AWS SCT를 사용하여 추출 에이전트를 관리하고 Oracle 스키마를 Amazon Redshift 스키마로 변환합니다. 등록된 데이터 추출 에이전트를 사용하여 AWS SCT에서 새 프로젝트를 생성합니다 .진행 중인 변경 사항을 복제하여 AWS SCT에서 로컬 작업과 AWS DMS 작업을 생성합니다.데이터를 Snowball 디바이스로 복사하고 Snowball 디바이스를 AWS로 반환합니다. AWS DMS가 Amazon S3에서 Amazon Redshift로 데이터를 복사할 수 있도록 허용합니다. 데이터 마이그레이션이 완료되었는지 확인하고 Amazon Redshift로 전환을 수행합니다.

Answer: D

Q287

한 회사에서 Amazon WorkSpaces를 클라이언트 디바이스와 함께 사용하여 노후된 데스크톱을 교체하려고 합니다. 직원들은 데스크톱을 사용하여 임상 시험 데이터와 함께 작동하는 애플리케이션에 액세스합니다. 회사 보안 정책에 따르면 응용 프로그램에 대한 액세스는 회사 지점 위치로만 제한되어야 합니다. 이 회사는 향후 6개월 내에 지점을 추가하는 것을 고려하고 있습니다.

운영 효율성이 가장 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 지점의 공용 주소 목록을 사용하여 IP 액세스 제어 그룹 규칙을 만듭니다 .IP 액세스 제어 그룹을 작업공간 디렉터리와 연결합니다.

B. AWS 방화벽 관리자를 사용하여 지점 위치의 퍼블릭 주소 목록과 함께 IPset이 포함된 웹 ACL 규칙을 생성합니다. 웹 ACL을 Workspaces 디렉터리에 연결합니다.

C. AWS Certificate Manager (ACM) 를 사용하여 지점에 배포된 머신에 신뢰할 수 있는 디바이스 인증서를 발급합니다. Workspaces 디렉터리에서 제한된 액세스를 활성화합니다.

D. 지사의 공용 주소에 대한 액세스를 제한하도록 Windows 방화벽이 구성된 사용자 지정 작업 영역 이미지를 만듭니다. 이미지를 사용하여 작업 영역을 배포합니다.

Answer: C

Q288

한 회사에서 코드로서의 인프라 (laC: infrastructure as code) 를 사용하여 두 개의 Amazon EC2 인스턴스 세트를 프로비저닝했습니다. 인스턴스는 몇 년 동안 동일하게 유지되었습니다. 이 회사의 사업은 지난 몇 개월 동안 빠르게 성장했습니다. 이에 대응하여 회사의 운영 팀은 갑작스러운 트래픽 증가를 관리하기 위해 Auto Scaling 그룹을 구현했습니다. 회사 정책에 따라 실행 중인 모든 운영 체제에 매월 보안 업데이트를 설치해야 합니다. 최신 보안 업데이트를 수행하려면 재부팅해야 했습니다. 그 결과 Auto Scaling 그룹이 인스턴스를 종료하고 패치가 적용되지 않은 새 인스턴스로 교체했습니다.

솔톤 건축가가 이 문제의 재발을 피하기 위해 권장하는 단계 조합은 무엇입니까?(두 개 선택)

A. 교체를 위해 가장 오래된 시작 구성을 대상으로 업데이트 정책을 설정하여 Auto Scaling 그룹을 수정합니다.

B. 다음 패치 유지 관리 전에 새 Auto Scaling 그룹을 생성합니다. 유지 관리 기간 동안 두 그룹을 모두 패치하고 인스턴스를 재부팅합니다.

C. Auto Scaling 그룹 앞에 탄력적 로드 밸런서 생성 Auto Scaling 그룹이 종료된 인스턴스를 교체한 후 대상 그룹 상태 확인이 정상으로 돌아가도록 모니터링을 구성합니다.

자동화 스크립트를 생성하여 AMI를 패치합니다. 시작 구성을 업데이트하고 Auto Scaling 인스턴스 새로 고침을 호출합니다.

E. Auto Scaling 그룹 앞에 탄력적 로드 밸런서를 생성합니다. 인스턴스에서 종료 보호를 구성합니다.

Answer: A, C

Q289

한 회사에서 온프레미스 콘텐츠 관리 시스템 (CMS) 을 AWS Fargate로 마이그레이션하고 있습니다. 이 회사는 텍스트, 이미지 및 비디오가 포함 된 블로그 게시물에 CMS를 사용합니다. 이 회사는 게시물이 30 일 이상 지난 후 블로그 게시물에 대한 트래픽이 80% 이상 감소하는 것을 관찰했습니다. CMS는 여러 VM에서 실행되며 디스크에 애플리케이션 상태를 저장합니다. 이 애플리케이션 상태는 여러 가용 영역의 모든 인스턴스에서 공유됩니다. 이미지 및 기타 미디어는 별도의 NFS 파일 공유에 저장됩니다. 이 회사는 성능에 미치는 영향을 최소화하면서 기존 솔루션의 비용을 줄여야 합니다.

이러한 요구 사항을 가장 비용 효율적으로 충족하는 단계 조합은 무엇입니까?(두 개 선택)

A. Amazon S3 Standard 버킷에 미디어 저장 30일이 넘은 객체를 S3 Standard-Infrequent Access (S3 Standard-IA) 스토리지 클래스로 전환하는 S3 수명 주기 구성을 생성합니다.

B. Amazon Elastic File System (Amazon EFS) 볼륨에 미디어 저장 EFS 볼륨을 모든 Fargate 인스턴스에 연결합니다.

C. Amazon Elastic File System (Amazon EFS) 볼륨에 애플리케이션 상태 저장 EFS 볼륨을 모든 Fargate 인스턴스에 연결합니다.

D. Amazon Elastic Block Store (Amazon EBS) 볼륨에 애플리케이션 상태 저장 EBS 볼륨을 모든 Fargate 인스턴스에 연결합니다.

E. Amazon S3 Standard 버킷에 미디어 저장 30일이 넘은 객체를 S3 Glacier 스토리지 클래스로 전환하는 S3 수명 주기 구성을 생성합니다.

Answer: A, D

Q290

한 회사에서 VPC의 애플리케이션 로드 밸런서 (ALB) 뒤에 있는 Amazon EC2 인스턴스 그룹에서 실행되는 웹 애플리케이션을 호스팅합니다. 이 회사는 네트워크 페이로드를 분석하여 애플리케이션의 정교한 공격을 리버스 엔지니어링하려고합니다.

이 목표를 달성하기 위해 회사는 어떤 접근 방식을 취해야 합니까?

A. VPC 흐름 로그를 활성화합니다. 분석을 위해 흐름 로그를 Amazon S3 버킷에 저장합니다.

B. EC2 인스턴스의 네트워크 인터페이스에서 트래픽 미러링을 활성화합니다. 미러링된 트래픽을 저장 및 분석을 위해 타겟으로 전송합니다.

C. AWS WAF 웹 ACL을 생성하고 이를 ALB와 연결합니다. AWS WAF 로깅을 구성합니다.

D. ALB에 대한 로깅을 활성화합니다. 분석을 위해 Amazon S3 버킷에 로그를 저장합니다.

Answer: B