

여러 Amazon EC2 인스턴스는 애플리케이션을 호스팅하는 데 사용됩니다. 이 프로그램은 Amazon SQS 대기열에서 메시지를 읽고 Amazon RDS 데이터베이스에 쓴 다음 대기열에서 제거합니다. RDS 테이블에 중복 항목이 포함되는 경우가 있습니다. SQS 대기열에 중복 메시지가 없습니다.

솔루션 설계자는 메시지가 한 번만 처리되도록 어떻게 보장할 수 있습니까?

- A. CreateQueue API 호출을 사용하여 새 대기열을 만듭니다.
- B. AddPermission API 호출을 사용하여 적절한 권한을 추가합니다.
- C. ReceiveMessage API 호출을 사용하여 적절한 대기 시간을 설정합니다.
- D. ChangeMessageVisibility API 호출을 사용하여 가시성 시간 초과를 늘립니다.

주요 키워드 : **CreateQueue AddPermission, ReceiveMessage, ChangeMessageVisibility**

문제 요구사항 :

SQS에서 데이터를 가져와서 RDS에 입력하는 상황

RDS 값이 중복되는 경우가 생길 때 중복 없이 데이터를 처리할 수 있는 방법은?

SQS를 사용할 때 중복 없이 데이터를 받아올 수 있는 방법?

Amazon SQS(Simple Queue Service) API 서비스

SQS의 API가 종류가 너무 많고 어려워 간단하게 메모를 하였다

1. AddPermission

대기열에 특정한 권한을 부여할 수 있다.

(개발자로 하여 공유 대기열에 메시지를 작성하게 한다거나 대기열 크기를 조회할 수 있게 하는 등)

2. CreateQueue

새로운 표준 FIFO 대기열을 생성한다.

- 기존 대기열의 타입을 standard 에서 FIFO로 바꿀 수 없다(새로 만들어야함)
- 각 메시지를 숨기기 위한 Delayed 대기열을 새로 만들 수도 있다.

3. ReceiveMessage

특정 대기열에서 최대 10개까지 메시지를 가져온다

4. ChangeMessageVisibility

메시지의 가시성 시간 초과를 바꾼다

- 메시지 기본 시간 제한은 30초 최대 12시간

AddPermission

ChangeMessageVisibility

ChangeMessageVisibilityBatch

CreateQueue

DeleteMessage

DeleteMessageBatch

DeleteQueue

GetQueueAttributes

GetQueueUrl

ListDeadLetterSourceQueues

ListQueues

ListQueueTags

PurgeQueue

ReceiveMessage

RemovePermission

SendMessage

SendMessageBatch

SetQueueAttributes

TagQueue

UntagQueue

즐겁다



여러 Amazon EC2 인스턴스는 애플리케이션을 호스팅하는 데 사용됩니다. 이 프로그램은 Amazon SQS 대기열에서 메시지를 읽고 Amazon RDS 데이터베이스에 쓴 다음 대기열에서 제거합니다. RDS 테이블에 중복 항목이 포함되는 경우가 있습니다. SQS 대기열에 중복 메시지가 없습니다.

솔루션 설계자는 메시지가 한 번만 처리되도록 어떻게 보장할 수 있습니까?

A. CreateQueue API 호출을 사용하여 새 대기열을 만듭니다.

-> 새로운 대기열을 만드는 것으로 중복을 해결할 수 없을 것이라고 생각하여 선택 제외

B. AddPermission API 호출을 사용하여 적절한 권한을 추가합니다.

-> 대기열에 특정 소유자에게 해당되는 특정 권한을 부여하는 것이 중복 제거와는 무관하다 생각하여 제외

C. ReceiveMessage API 호출을 사용하여 적절한 대기 시간을 설정합니다.

-> 대기 시간을 가시성 시간으로 이해하여 가시성 시간을 연장하여 중복을 방지할 수 있을 줄 알았음(오답 이유)

** ReceiveMessage API는 가시성 시간이 만료되었을 때 호출자가 계속 처리하는 경우 중복 처리 될 수 있음 (중요)

D. ChangeMessageVisibility API 호출을 사용하여 가시성 시간 초과를 늘립니다.

-> 대기열의 데이터가 만료되기 전에 다시 가시성 시간을 살려놔서 깔끔하게 처리될 수 있도록 함(정답)

-> 만료된 데이터가 꼬일 경우 중복 처리 될 수 있을 듯(정답인 이유로 추측)



한 기업이 소매 웹사이트의 전 세계 출시를 발표했습니다. 웹사이트는 Elastic Load Balancer를 통해 라우팅되는 수많은 Amazon EC2 인스턴스에서 호스팅됩니다. 인스턴스는 Auto Scaling 그룹의 여러 가용 영역에 분산됩니다.

회사는 고객이 웹사이트를 보는 장치에 따라 맞춤형 자료를 제공하기를 원합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 단계를 함께 수행해야 할까요? (2개를 선택하세요.)

- A. 여러 버전의 콘텐츠를 캐시하도록 Amazon CloudFront를 구성합니다.
- B. 네트워크 로드 밸런서에서 호스트 헤더를 구성하여 트래픽을 다른 인스턴스로 전달합니다.
- C. User-Agent 헤더를 기반으로 특정 객체를 사용자에게 보내도록 Lambda@Edge 함수를 구성합니다.
- D. AWS Global Accelerator를 구성합니다. NLB(Network Load Balancer)로 요청을 전달합니다. 다른 EC2 인스턴스에 대한 호스트 기반 라우팅을 설정하도록 NLB를 구성합니다.
- E. AWS Global Accelerator를 구성합니다. NLB(Network Load Balancer)로 요청을 전달합니다. 다른 EC2 인스턴스에 대한 경로 기반 라우팅을 설정하도록 NLB를 구성합니다.

주요 키워드 : **User-Agent, NLB, Global Accelerator**

문제 요구사항 :

여러 인스턴스를 ELB를 통해 분산 운용하고 Auto Scaling까지 설정. 고객 웹사이트는 고객 맞춤 서비스로

중앙에서 보내주는 데이터가 아니라 엣지프론트 맞춤형 자료를 구성하려면 어떻게해야할까?



Amazon CloudFront

호스트에서 전세계로 직접 통신하지 않고 세계 각지의 Edge Location를 두어 최종 사용자와 근접하여 통신
중앙 집중이 아닌 지역 분산으로 좀 더 로컬 환경에 맞는 서비스 제공 가능

User-Agent 헤더

HTTP 요청을 보내는 디바이스와 브라우저 등 사용자의 식별 정보를 담고 있는 request header의 한 종류
이 헤더를 통해 요청을 보낸 사용자 환경을 알 수 있다!

AWS Global Accelerator

엣지 로케이션을 이용하여 트래픽 성능을 개선하고 이를 통해 인터넷 짱 빨라지는 서비스

호스트 기반 라우팅

www.naver.com에서 온 녀석들은 요쪽으로! www.google.co.kr에서 온 녀석들은 이쪽으로!

경로 기반 라우팅

주소 경로가 /yongheegenius/로 끝나는 녀석들은 이리로! 나머진 저기로!

한 기업이 소매 웹사이트의 전 세계 출시를 발표했습니다. 웹사이트는 Elastic Load Balancer를 통해 라우팅되는 수많은 Amazon EC2 인스턴스에서 호스팅됩니다. 인스턴스는 Auto Scaling 그룹의 여러 가용 영역에 분산됩니다.

회사는 고객이 웹사이트를 보는 장치에 따라 맞춤형 자료를 제공하기를 원합니다.

이러한 요구 사항을 충족하기 위해 솔루션 설계자는 어떤 단계를 함께 수행해야 할까요? (2개를 선택하세요.)

A. 여러 버전의 콘텐츠를 캐시하도록 Amazon CloudFront를 구성합니다.

-> 호스트 서버가 아닌 엣지 로케이션 캐시를 통해 로컬화 된 자료를 제공할 수 있다 생각해서 선택(정답)

B. 네트워크 로드 밸런서에서 호스트 헤더를 구성하여 트래픽을 다른 인스턴스로 전달합니다.

-> 호스트 헤더는 그냥 다 있는게 아닌가.. 회사의 주된 요구 사항이 맞춤형 자료라고 하면 애는 패스해도 될 것 같다

C. User-Agent 헤더를 기반으로 특정 객체를 사용자에게 보내도록 Lambda@Edge 함수를 구성합니다.

-> 호스트 서버가 아닌 엣지 로케이션 캐시를 통해 로컬화 된 자료를 제공할 수 있다 생각해서 선택(정답)

D. AWS Global Accelerator를 구성합니다. NLB(Network Load Balancer)로 요청을 전달합니다. 다른 EC2 인스턴스에 대한 호스트 기반 라우팅을 설정하도록 NLB를 구성합니다.

-> 호스트/경로 기반으로 특정 라우팅을 하고 싶다는 회사의 요구사항이 없었으므로 D,E는 모두 패스

E. AWS Global Accelerator를 구성합니다. NLB(Network Load Balancer)로 요청을 전달합니다. 다른 EC2 인스턴스에 대한 경로 기반 라우팅을 설정하도록 NLB를 구성합니다.



AWS CloudFront 소개 페이지

<https://aws.amazon.com/ko/cloudfront/>

AWS Network Load Balancer 공식 문서

https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/network/introduction.html

User-agent 헤더 설명 블로그

<https://velog.io/@ggong/User-agent-%EC%A0%95%ED%99%95%ED%95%98%EA%B2%8C-%ED%95%B4%EC%84%9D%ED%95%98%EA%B8%B0>

AWS Global Accelerator 공식 문서

<https://aws.amazon.com/ko/global-accelerator/?blogs-global-accelerator.sort-by=item.additionalFields.createdDate&blogs-global-accelerator.sort-order=desc&aws-global-accelerator-wn.sort-by=item.additionalFields.postDateTime&aws-global-accelerator-wn.sort-order=desc>

AWS는 비즈니스에서 OLTP(온라인 트랜잭션 처리) 부담을 수행하는 데 사용됩니다. 이 워크로드에는 암호화되지 않은 Amazon RDS 데이터베이스 인스턴스를 사용하여 다중 AZ 환경에 배포됩니다. 이 인스턴스의 데이터베이스는 매일 백업됩니다.

데이터베이스와 스냅샷이 지속적으로 암호화되도록 솔루션 설계자는 앞으로 무엇을 해야 할까요?

- A. 최신 DB 스냅샷 사본을 암호화합니다. 암호화된 스냅샷을 복원하여 기존 DB 인스턴스를 교체합니다.
- B. 암호화된 새 Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성하고 여기에 스냅샷을 복사합니다. DB 인스턴스에서 암호화를 활성화합니다.
- C. AWS Key Management Service(AWS KMS)를 사용하여 스냅샷을 복사하고 암호화를 활성화합니다. 암호화된 스냅샷을 기존 DB 인스턴스로 복원합니다.
- D. AWS Key Management Service(AWS KMS) 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 암호화된 Amazon S3 버킷에 스냅샷을 복사합니다.

주요 키워드 : **OLTP, RDS, KMS, EBS**

문제 요구사항 :

데이터베이스와 스냅샷을 지속적으로 암호화하면서 백업해야함

AWS는 비즈니스에서 OLTP(온라인 트랜잭션 처리) 부담을 수행하는 데 사용됩니다. 이 워크로드에는 암호화되지 않은 Amazon RDS 데이터베이스 인스턴스를 사용하여 다중 AZ 환경에 배포됩니다. 이 인스턴스의 데이터베이스는 매일 백업됩니다.

데이터베이스와 스냅샷이 지속적으로 암호화되도록 솔루션 설계자는 앞으로 무엇을 해야 할까요?

A. 최신 DB 스냅샷 사본을 암호화합니다. 암호화된 스냅샷을 복원하여 기존 DB 인스턴스를 교체합니다.

-> 스냅샷 사본을 암호화하고.. 스냅샷으로 다시 DB를 교체하고.. 이 문제는 나머지가 뭔 차이인지 모르겠습니다..(정답)

B. 암호화된 새 Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성하고 여기에 스냅샷을 복사합니다. DB 인스턴스에서 암호화를 활성화합니다.

C. AWS Key Management Service(AWS KMS)를 사용하여 스냅샷을 복사하고 암호화를 활성화합니다. 암호화된 스냅샷을 기존 DB 인스턴스로 복원합니다.

D. AWS Key Management Service(AWS KMS) 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 암호화된 Amazon S3 버킷에 스냅샷을 복사합니다.

거대한 Amazon EC2 인스턴스 집합에서 기업은 애플리케이션을 실행합니다. 이 프로그램은 Amazon에서 호스팅하는 DynamoDB 데이터베이스에 항목을 읽고 씁니다. DynamoDB 데이터베이스의 크기는 정기적으로 증가하지만 애플리케이션에는 이전 30일 동안의 데이터만 필요합니다. 조직은 구현하기에 비용 효율적이고 시간 효율적인 솔루션이 필요합니다.

어떤 솔루션이 이러한 기준을 충족합니까?

- A. AWS CloudFormation 템플릿을 사용하여 전체 솔루션을 배포합니다. 30일마다 CloudFormation 스택을 재배포하고 원래 스택을 삭제합니다.
- B. AWS Marketplace에서 모니터링 애플리케이션을 실행하는 EC2 인스턴스를 사용합니다. Amazon DynamoDB 스트림을 사용하여 테이블에 새 항목이 생성될 때 타임스탬프를 저장하도록 모니터링 애플리케이션을 구성합니다. EC2 인스턴스에서 실행되는 스크립트를 사용하여 30일보다 오래된 타임스탬프가 있는 항목을 삭제합니다.
- C. 테이블에 새 항목이 생성될 때 AWS Lambda 함수를 호출하도록 Amazon DynamoDB Streams를 구성합니다. 테이블에서 30일이 지난 항목을 삭제하도록 Lambda 함수를 구성합니다.
- D. 애플리케이션을 확장하여 현재 타임스탬프 값에 30일을 더한 값을 테이블에 생성되는 각각의 새 항목에 추가합니다. 속성을 TTL 속성으로 사용하도록 DynamoDB를 구성합니다.

주요 키워드 : **DynamoDB, DynamoDB Streams,** **내 답 C / 답 D**

문제 요구사항 :

30일 동안의 데이터를 관리해야하며 DynamoDB의 크기는 정기적으로 증가하는 상황

정기적으로 늘어나는 데이터를 계속 관리하되 30일만 관리하는 경우

거대한 Amazon EC2 인스턴스 집합에서 기업은 애플리케이션을 실행합니다. 이 프로그램은 Amazon에서 호스팅하는 DynamoDB 데이터베이스에 항목을 읽고 씁니다. DynamoDB 데이터베이스의 크기는 정기적으로 증가하지만 애플리케이션에는 이전 30일 동안의 데이터만 필요합니다. 조직은 구현하기에 비용 효율적이고 시간 효율적인 솔루션이 필요합니다.

어떤 솔루션이 이러한 기준을 충족합니까?

A. AWS CloudFormation 템플릿을 사용하여 전체 솔루션을 배포합니다. 30일마다 CloudFormation 스택을 재배포하고 원래 스택을 삭제합니다.

-> 30일 동안의 데이터만 필요하다고 해서 삭제하고 다시 배포하고 하는 것은 좀 아닌 것 같아서 선택 제외

B. AWS Marketplace에서 모니터링 애플리케이션을 실행하는 EC2 인스턴스를 사용합니다. Amazon DynamoDB 스트림을 사용하여 테이블에 새 항목이 생성될 때 타임스탬프를 저장하도록 모니터링 애플리케이션을 구성합니다. EC2 인스턴스에서 실행되는 스크립트를 사용하여 30일보다 오래된 타임스탬프가 있는 항목을 삭제합니다.

-> 거대한 EC2 집합에서 스크립트 전부 다 돌리고 뭐하고 비용과 시간 효율적이지 못한 것 같아서 선택 제외

C. 테이블에 새 항목이 생성될 때 AWS Lambda 함수를 호출하도록 Amazon DynamoDB Streams를 구성합니다. 테이블에서 30일이 지난 항목을 삭제하도록 Lambda 함수를 구성합니다.

-> DynamoDB Stream의 경우 최대 24시간까지 로그를 저장한다. 30일까지 못버팀 / 30일 저장할 수 있을줄(선택 이유)

D. 애플리케이션을 확장하여 현재 타임스탬프 값에 30일을 더한 값을 테이블에 생성되는 각각의 새 항목에 추가합니다. 속성을 TTL 속성으로 사용하도록 DynamoDB를 구성합니다.

-> 스냅샷 사본을 암호화하고.. 스냅샷으로 다시 DB를 교체하고.. 이 문제는 나머지가 뭘 차이인지 모르겠습니다..(정답)



솔루션 설계자는 Amazon Web Services(AWS) 클라우드에서 하이브리드 애플리케이션을 개발하고 있습니다. AWS Direct Link(DX)는 온프레미스 데이터 센터를 AWS에 연결하는 데 사용됩니다. AWS와 온프레미스 데이터 센터 간의 애플리케이션 연결은 매우 내구성이 있어야 합니다.

이러한 기준을 충족하려면 어떤 DX 설정을 사용해야 할까요?

- A. 그 위에 VPN을 사용하여 DX 연결을 구성합니다.
- B. 여러 DX 위치에서 DX 연결을 구성합니다.
- C. 가장 신뢰할 수 있는 DX 파트너를 사용하여 DX 연결을 구성합니다.
- D. DX 연결 위에 여러 가상 인터페이스를 구성합니다.

주요 키워드 : **AWS Direct link**

문제 요구사항 :
클라우드와 온프레미스 데이터센터를 더 안정적으로 연결할 수 있는 방법?

솔루션 설계자는 Amazon Web Services(AWS) 클라우드에서 하이브리드 애플리케이션을 개발하고 있습니다. AWS Direct Link(DX)는 온프레미스 데이터 센터를 AWS에 연결하는 데 사용됩니다. AWS와 온프레미스 데이터 센터 간의 애플리케이션 연결은 매우 내구성이 있어야 합니다.

이러한 기준을 충족하려면 어떤 DX 설정을 사용해야 할까요?

A. 그 위에 VPN을 사용하여 DX 연결을 구성합니다.

-> 내구성이랑 크게 상관 없는 것 같아서 패스

B. 여러 DX 위치에서 DX 연결을 구성합니다.

-> 연결 통로를 다변화하여 가용성과 내구성을 확보할 수 있음(정답)

C. 가장 신뢰할 수 있는 DX 파트너를 사용하여 DX 연결을 구성합니다.

-> Direct Link(DX) 파트너란 지역별 DX 서비스를 제공하는 로컬 파트너 업체(SKT 등). 신뢰할 수 있는지랑은 상관X

D. DX 연결 위에 여러 가상 인터페이스를 구성합니다.

-> 내구성이랑 크게 상관 없는 것 같아서 패스



Amazon EC2에서 기업은 Amazon RDS 데이터베이스에 의해 백업되는 매우 안전한 애플리케이션을 운영하고 있습니다. 모든 개인 식별 정보(PII)는 규정 준수 표준을 준수하기 위해 저장 시 암호화되어야 합니다.

최소한의 인프라 변경으로 이러한 요구 사항을 달성하기 위해 솔루션 설계자는 어떤 솔루션을 제안해야 할까요?

- A. AWS Certificate Manager를 배포하여 인증서를 생성합니다. 인증서를 사용하여 데이터베이스 볼륨을 암호화합니다.
- B. AWS CloudHSM을 배포하고 암호화 키를 생성하고 고객 마스터 키(CMK)를 사용하여 데이터베이스 볼륨을 암호화합니다.
- C. AWS Key Management Service 고객 마스터 키(AWS KMS CMK)를 사용하여 SSL 암호화를 구성하여 데이터베이스 볼륨을 암호화합니다.
- D. 인스턴스 및 데이터베이스 볼륨을 암호화하도록 AWS Key Management Service(AWS KMS) 키로 Amazon Elastic Block Store(Amazon EBS) 암호화 및 Amazon RDS 암호화를 구성합니다.

주요 키워드 : **OLTP, RDS, KMS, EBS**

문제 요구사항 :

데이터베이스와 스냅샷을 지속적으로 암호화하면서 백업해야함

AWS Key Management Service

데이터 보호에 사용되는 암호 키를 중앙 집중식으로 제어
AWS 서비스와 통합되어 운영이 가능함

AWS Certificate Manager

공인 및 사설 SSL/TLS 인증서를 관리 및 배포할 수 있도록 지원하는 서비스
외부 인증기관이 발급한 인증서를 가져와 ELB, CloudFront, API 등으로 배포 가능

AWS CloudHSM

AWS 클라우드상의 관리형 하드웨어 보안 모듈(HSM)

Amazon EC2에서 기업은 Amazon RDS 데이터베이스에 의해 백업되는 매우 안전한 애플리케이션을 운영하고 있습니다. 모든 개인 식별 정보(PII)는 규정 준수 표준을 준수하기 위해 저장 시 암호화되어야 합니다.

최소한의 인프라 변경으로 이러한 요구 사항을 달성하기 위해 솔루션 설계자는 어떤 솔루션을 제안해야 하나요?

A. AWS Certificate Manager를 배포하여 인증서를 생성합니다. 인증서를 사용하여 데이터베이스 볼륨을 암호화합니다.

-> Certificate Manager는 개인 식별 정보를 취급하지 않고 인터넷 SSL 인증서 등을 취급하므로 선택 제외

B. AWS CloudHSM을 배포하고 암호화 키를 생성하고 고객 마스터 키(CMK)를 사용하여 데이터베이스 볼륨을 암호화합니다.

C. AWS Key Management Service 고객 마스터 키(AWS KMS CMK)를 사용하여 SSL 암호화를 구성하여 데이터베이스 볼륨을 암호화합니다.

-> SSL 암호화와 PII 암호화는 다른 문제라고 생각됨

D. 인스턴스 및 데이터베이스 볼륨을 암호화하도록 AWS Key Management Service(AWS KMS) 키로 Amazon Elastic Block Store(Amazon EBS) 암호화 및 Amazon RDS 암호화를 구성합니다.

-> KMS와 RDS가 같이 나온 것이 이것뿐이라 이게 답으로 추측됨(정답)



기업은 SMB 프로토콜을 사용하여 온프레미스 데이터베이스를 로컬 파일 서버 공유에 백업합니다. 복구 목표를 달성하려면 일주일 분량의 백업 데이터에 즉시 액세스할 수 있어야 합니다. 일주일만 지나면 복구 가능성이 줄어들고 비즈니스는 이전 백업 데이터를 검색하는 데 지연이 발생할 수 있습니다.

이러한 기준이 가능한 최소한의 운영 작업으로 충족되도록 하기 위해 솔루션 설계자는 어떤 조치를 취해야 할까요?

- A. Windows 파일 서버용 Amazon FSx를 배포하여 원하는 모든 백업을 보관하기에 충분한 스토리지가 있는 노출된 파일 공유가 있는 파일 시스템을 생성합니다.
- B. 1주일의 백업을 저장할 수 있는 충분한 스토리지가 있는 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 파일 게이트웨이에서 백업이 SMB 공유를 가리키도록 합니다.
- C. Amazon Elastic File System(Amazon EFS)을 배포하여 원하는 모든 백업을 보관하기에 충분한 스토리지가 있는 노출된 NFS 공유가 있는 파일 시스템을 생성합니다.
- D. 계속해서 기존 파일 공유에 백업합니다. AWS Database Migration Service(AWS DMS)를 배포하고 복사 작업을 정의하여 1주일 이 지난 백업 파일을 Amazon S3에 복사하고 로컬 파일 저장소에서 백업 파일을 삭제합니다.

주요 키워드 : **Amazon FSx, AWS Storage Gateway, AWS EFS, AWS DMS**

요구사항 : 온프레미스->로컬 파일 서버 공유에 백업 + 일주일 분량 백업 데이터 **즉시** 접속 가능
-> 최소한의 작업으로 가능하게 해라

Amazon FSx

Windows Server에 구축되는 완전관리형 파일 스토리지

-> NetApp ONTAP, OpenZFS, Windows File Server, Lustre 중 사용 가능

AWS Storage Gateway

온프레미스 애플리케이션에 무제한의 클라우드 스토리지 액세스 제공
하이브리드 클라우드 스토리지 서비스

AWS EFS

Linux 워크로드에 대한 NFS 공유 파일 시스템 스토리지
따로 프로비저닝이 불필요한 서버리스 서비스

AWS DMS

SQL, NoSQL 등 데이터베이스를 마이그레이션 할 수 있게해주는 서비스

기업은 SMB 프로토콜을 사용하여 온프레미스 데이터베이스를 로컬 파일 서버 공유에 백업합니다. 복구 목표를 달성하려면 일주일 분량의 백업 데이터에 즉시 액세스할 수 있어야 합니다. 일주일의 시간이 지나면 복구 가능성이 줄어들고 비즈니스는 이전 백업 데이터를 검색하는 데 지연이 발생할 수 있습니다.

이러한 기준이 가능한 최소한의 운영 작업으로 충족되도록 하기 위해 솔루션 설계자는 어떤 조치를 취해야 할까요?

A. Windows 파일 서버용 Amazon FSx를 배포하여 원하는 모든 백업을 보관하기에 충분한 스토리지가 있는 노출된 파일 공유가 있는 파일 시스템을 생성합니다.

B. 1주일의 백업을 저장할 수 있는 충분한 스토리지가 있는 AWS Storage Gateway 파일 게이트웨이를 배포합니다. 파일 게이트웨이에서 백업이 SMB 공유를 가리키도록 합니다. -> 온프레미스와 연동한 하이브리드 클라우드 게이트웨이를 통해 SMB 파일 통신(정답)

C. Amazon Elastic File System(Amazon EFS)을 배포하여 원하는 모든 백업을 보관하기에 충분한 스토리지가 있는 노출된 NFS 공유가 있는 파일 시스템을 생성합니다.

D. 계속해서 기존 파일 공유에 백업합니다. AWS Database Migration Service(AWS DMS)를 배포하고 복사 작업을 정의하여 일주일의 백업 파일을 Amazon S3에 복사하고 로컬 파일 저장소에서 백업 파일을 삭제합니다.

-> DMS가 데이터베이스 전용 서비스고 일주일까지의 자료를 로컬 파일 저장소에서 즉시 접근할 수 있을거라 생각함(착각)



기업은 품목 가격을 기반으로 세금 계산을 자동화하는 API를 고객에게 제공합니다. 크리스마스 시즌에는 회사에 문의가 증가하여 응답 시간이 지연됩니다. 솔루션 설계자는 확장 가능하고 탄력적인 시스템을 만들어야 합니다.

이를 달성하기 위한 솔루션 설계자의 역할은 무엇입니까?

- A. Amazon EC2 인스턴스에서 호스팅되는 API를 제공합니다. EC2 인스턴스는 API 요청이 있을 때 필요한 계산을 수행합니다.
- B. 항목 이름을 허용하는 Amazon API Gateway를 사용하여 REST API를 설계합니다. API Gateway는 세금 계산을 위해 항목 이름을 AWS Lambda에 전달합니다.
- C. 뒤에 두 개의 Amazon EC2 인스턴스가 있는 Application Load Balancer를 생성합니다. EC2 인스턴스는 수신된 항목 이름에 대한 세금을 계산합니다.
- D. Amazon EC2 인스턴스에서 호스팅되는 API와 연결하는 Amazon API Gateway를 사용하여 REST API를 설계합니다. API Gateway는 세금 계산을 위해 항목 이름을 수락하고 EC2 인스턴스에 전달합니다.

주요 키워드 : **Amazon API Gateway**

요구사항 : 트래픽 증가 대응 가능한 확장 가능 탄력적 시스템

기업은 품목 가격을 기반으로 세금 계산을 자동화하는 API를 고객에게 제공합니다. 크리스마스 시즌에는 회사에 문의가 증가하여 응답 시간이 지연됩니다. 솔루션 설계자는 확장 가능하고 탄력적인 시스템을 만들어야 합니다.

이를 달성하기 위한 솔루션 설계자의 역할은 무엇입니까?

A. Amazon EC2 인스턴스에서 호스팅되는 API를 제공합니다. EC2 인스턴스는 API 요청이 있을 때 필요한 계산을 수행합니다.

B. 항목 이름을 허용하는 Amazon API Gateway를 사용하여 REST API를 설계합니다. API Gateway는 세금 계산을 위해 항목 이름을 AWS Lambda에 전달합니다. -> API Gateway로 API를 사용한다. 또한 람다의 경우 프로비저닝 불필요한 서버리스 서비스로 대용량의 데이터 처리도 자동으로 처리 가능하므로 탄력적으로 온디맨드 요금으로 사용 가능함

C. 뒤에 두 개의 Amazon EC2 인스턴스가 있는 Application Load Balancer를 생성합니다. EC2 인스턴스는 수신된 항목 이름에 대한 세금을 계산합니다. -> 확장 가능한 것은 Auto-Scaling 이라고 생각해서 선택 제외

D. Amazon EC2 인스턴스에서 호스팅되는 API와 연결하는 Amazon API Gateway를 사용하여 REST API를 설계합니다. API Gateway는 세금 계산을 위해 항목 이름을 수락하고 EC2 인스턴스에 전달합니다. ->인스턴스로 계산하는 것보단 람다가 나은 것 같아 제외



매일 회사의 수백 대의 에지 장치에서 1TB의 상태 알림이 생성됩니다. 각 경고의 파일 크기는 약 2KB입니다. 솔루션 설계자는 추가 조사를 위해 경고를 수집하고 저장하는 시스템을 제공해야 합니다.

비즈니스에는 액세스 가능성이 매우 높은 솔루션이 필요합니다. 그러나 비즈니스는 저비용 구조를 가져야 하며 추가 인프라를 처리하기를 원하지 않습니다.

또한 회사는 즉각적인 검사를 위해 14일 동안 데이터를 보유하고 오래된 데이터를 보관할 계획입니다.

이러한 요구 사항을 충족하는 가장 최적의 옵션은 무엇입니까?

A. Amazon Kinesis Data Firehose 전송 스트림을 생성하여 알림을 수집합니다. Amazon S3 버킷에 알림을 전달하도록 Kinesis Data Firehose 스트림을 구성합니다. 14일 후에 데이터를 Amazon S3 Glacier로 전환하도록 S3 수명 주기 구성을 설정합니다.

B. 두 가용 영역에서 Amazon EC2 인스턴스를 시작하고 Elastic Load Balancer 뒤에 배치하여 알림을 수집합니다. Amazon S3 버킷에 경고를 저장할 EC2 인스턴스에 대한 스크립트를 생성합니다. 14일 후에 데이터를 Amazon S3 Glacier로 전환하도록 S3 수명 주기 구성을 설정합니다.

C. Amazon Kinesis Data Firehose 전송 스트림을 생성하여 알림을 수집합니다. Amazon Elasticsearch Service(Amazon ES) 클러스터에 알림을 전달하도록 Kinesis Data Firehose 스트림을 구성합니다. Amazon ES 클러스터를 설정하여 매일 수동 스냅샷을 만들고 클러스터에서 14일이 지난 데이터를 삭제합니다.

D. Amazon Simple Queue Service(Amazon SQS) 표준 대기열을 생성하여 알림을 수집하고 메시지 보존 기간을 14일로 설정합니다. SQS 대기열을 폴링하고, 메시지의 수명을 확인하고, 필요에 따라 메시지 데이터를 분석하도록 소비자를 구성합니다. 메시지가 14일이 지난 경우 소비자는 메시지를 Amazon S3 버킷에 복사하고 SQS 대기열에서 메시지를 삭제해야 합니다.

주요 키워드 : **Amazon Kinesis Data Firehose, Amazon ES**

요구사항 : 상태 알림을 수집, 저비용, 추가 인프라 X, 14일 동안 데이터 보관 후 장기 보관 전환

	Amazon Kinesis Data Firehose	Amazon Kinesis Data Streams
공통점	완전관리형 실시간 스트리밍 데이터 처리 서비스 클라우드 내 실시간 데이터 처리	
차이점	처리 및 전송 실시간 데이터 스트림을 준비 및 로드	수집 및 저장 실시간으로 처리 및 분석

Amazon ES

대화형 로그 분석, 실시간 애플리케이션 모니터링 및 웹사이트 검색

현재 **Amazon OpenSearch Service**로 변경됨

-> JSON 데이터를 Logstash 및 Amazon Kinesis Firehose, API를 통해 Elasticsearch로 전송

매일 회사의 수백 대의 에지 장치에서 1TB의 상태 알림이 생성됩니다. 각 경고의 파일 크기는 약 2KB입니다. 솔루션 설계자는 추가 조사를 위해 경고를 수집하고 저장하는 시스템을 제공해야 합니다.

비즈니스에는 액세스 가능성이 매우 높은 솔루션이 필요합니다. 그러나 비즈니스는 저비용 구조를 가져야 하며 추가 인프라를 처리하기를 원하지 않습니다.

또한 회사는 즉각적인 검사를 위해 14일 동안 데이터를 보유하고 오래된 데이터를 보관할 계획입니다.

이러한 요구 사항을 충족하는 가장 최적의 옵션은 무엇입니까?

-> Firehose는 수집 및 저장에 특화되어 있다. 그리고 S3 수명주기 구성으로 장기 보관을 할 수 있다.

A. Amazon Kinesis Data Firehose 전송 스트림을 생성하여 알림을 수집합니다. Amazon S3 버킷에 알림을 전달하도록 Kinesis Data Firehose 스트림을 구성합니다. 14일 후에 데이터를 Amazon S3 Glacier로 전환하도록 S3 수명 주기 구성을 설정합니다.

B. 두 가용 영역에서 Amazon EC2 인스턴스를 시작하고 Elastic Load Balancer 뒤에 배치하여 알림을 수집합니다. Amazon S3 버킷에 경고를 저장할 EC2 인스턴스에 대한 스크립트를 생성합니다. 14일 후에 데이터를 Amazon S3 Glacier로 전환하도록 S3 수명 주기 구성을 설정합니다. -> 인스턴스를 시작하면 추가 인프라를 처리하는건데 인스턴스가 너무 익숙해서 당연히 있을거라고 생각함

C. Amazon Kinesis Data Firehose 전송 스트림을 생성하여 알림을 수집합니다. Amazon Elasticsearch Service(Amazon ES) 클러스터에 알림을 전달하도록 Kinesis Data Firehose 스트림을 구성합니다. Amazon ES 클러스터를 설정하여 매일 수동 스냅샷을 만들고 클러스터에서 14일이 지난 데이터를 삭제합니다. ->수동 스냅샷을 매일매일 만들면 너무 귀찮고 너무 공수가 많이 들어서 선택 제외

D. Amazon Simple Queue Service(Amazon SQS) 표준 대기열을 생성하여 알림을 수집하고 메시지 보존 기간을 14일로 설정합니다. SQS 대기열을 폴링하고, 메시지의 수명을 확인하고, 필요에 따라 메시지 데이터를 분석하도록 소비자를 구성합니다. 메시지가 14일이 지난 경우 소비자는 메시지를 Amazon S3 버킷에 복사하고 SQS 대기열에서 메시지를 삭제해야 합니다. 소비자 삭제해야하므로 자동화 x