

기업은 인공지능 및 기계 학습(AI/ML) 연구를 수행하는 고객에게 데이터 세트를 제공합니다. 데이터 세트는 us-east-1 리전의 Amazon S3 버킷에서 호스팅되는 형식이 지정된 거대한 파일입니다. 기업은 소비자가 특정 데이터 세트에 대한 액세스 권한을 구매할 수 있는 웹 애플리케이션을 실행합니다. 여러 Amazon EC2 인스턴스를 사용하여 웹 애플리케이션을 호스팅한 다음 Application Load Balancer를 통해 라우팅합니다. 구매 후 구매자는 파일에 대한 액세스 권한을 부여하는 S3 서명 URL을 받습니다.

고객은 북미와 유럽 전역에 있습니다. 조직은 성능을 유지하거나 개선하면서 데이터 전송 비용을 낮추기를 원합니다.

이러한 기준이 충족되도록 솔루션 설계자는 어떤 조치를 취해야 합니까?

주요 키워드 S3, 데이터 배포

문제 상황 분석 S3 버킷에 있는 거대한 파일, ALB 통해서 라우팅, 파일 액세스권한

틀린이유 거대한 파일이 정적데이터일줄 몰랐음.. 뭔가 빠른거하면 A랑 C겠지 고민하다가 A골랐네요

풀이 과정

A. [Transfer Acceleration](#)은 Client와 S3 버킷간 장거리 전송을 빠르게 지원하는 서비스. 추가 데이터 전송요금이 부과되므로 탈락

B. 제일 무난한 속도 가속화 서비스는 CloudFront

C. [S3 교차리전복제](#)를 사용할 경우 성능개선은 되겠지만 S3버킷이 두개로 늘어나니까 비용상승될 것같아서 탈락

D. 데이터를 스트리밍한다고해서 특별히 성능이 개선되거나 할건 같지 않을것같아서 탈락

+ [미리서명된 URL 사용](#) 기본적으로 S3 의 모든 객체 및 버킷은 프라이빗.

미리 서명된 URL 을 사용하여 선택적으로 객체공유 및 고객/사용자가 AWS 보안 자격 증명이나 권한 없이 버킷에 객체를 업로드하는 것을 허용

URL 이 만료되어 만료 시간에 도달하면 더 이상 작동하지 않습니다

04/18-2

한 비즈니스에서 단일 AWS 리전에 배포할 새로운 웹 애플리케이션을 개발 중입니다. Amazon EC2 인스턴스와 Amazon RDS 데이터베이스 인스턴스를 사용할 애플리케이션에는 2계층 설계가 필요합니다. 솔루션 설계자는 모든 구성 요소에 쉽게 액세스할 수 있는 방식으로 응용 프로그램의 아키텍처를 계획해야 합니다.

이러한 요구 사항을 충족하는 데 가장 비용 효율적인 접근 방식은 무엇입니까?

- A. 추가 리전에 EC2 인스턴스를 배포합니다. 다중 AZ 옵션이 활성화된 DB 인스턴스를 생성합니다.
- B. 동일한 리전 및 동일한 가용 영역에 모든 EC2 인스턴스를 배포합니다. 다중 AZ 옵션이 활성화된 DB 인스턴스를 생성합니다.
- C. 동일한 리전 내의 2개 이상의 가용 영역에 EC2 인스턴스를 배포합니다. 단일 가용 영역에 DB 인스턴스를 생성합니다.
- D. 동일한 리전 내의 2개 이상의 가용 영역에 EC2 인스턴스를 배포합니다. 다중 AZ 옵션이 활성화된 DB 인스턴스를 생성합니다.

풀이 과정

- A. 단일리전에 배포할건데 굳이 추가리전에 배포할필요가? 탈락
- B. 동일한 리전 및 동일가용영역, 다중AZ옵션DB까지 틀린건 아니지만 D가 가용영역2개이상이라 더 좋음
- C. 단일 가용영역> 쉽게액세스 아쉬움
- D. EC2인스턴스도 다중AZ, DB인스턴스도 다중AZ.

주요 키워드 EC2, RDS 인스턴스 배포 방식

문제 상황 분석

단일 리전내에서, EC2인스턴스와 RDS를 배포, 쉽게 액세스할 수 있을것, 비용효율적

틀린 이유

다중AZ옵션은 비용이 발생한다고 알고있어서 뺐는데,

모든 구성요소에 쉽게 액세스할 수 있을것이 요구사항이고, 이를 충족하면서 비용효율적인거라 빼면 안될것같습니다.

04/18-3

기업은 직원에게 기밀 및 민감한 데이터에 대한 보안 액세스를 제공해야 합니다. 회사는 승인된 개인만 데이터에 액세스할 수 있도록 보장하기를 원합니다. 데이터는 작업자의 장치에 안전하게 다운로드되어야 합니다.

파일은 온프레미스 Windows 파일 서버에 보관됩니다. 그러나 원격 트래픽이 증가함에 따라 파일 서버의 용량이 고갈되고 있습니다.

어떤 솔루션이 이러한 기준을 충족할까요?

- A. 파일 서버를 퍼블릭 서브넷의 Amazon EC2 인스턴스로 마이그레이션합니다. 직원의 IP 주소에 대한 인바운드 트래픽을 제한하도록 보안 그룹을 구성합니다.
- B. 파일을 Windows 파일 서버용 Amazon FSx 파일 시스템으로 마이그레이션합니다. Amazon FSx 파일 시스템을 온프레미스 Active Directory와 통합합니다. AWS 클라이언트 VPN을 구성합니다.
- C. 파일을 Amazon S3로 마이그레이션하고 프라이빗 VPC 엔드포인트를 생성합니다. 다운로드를 허용하려면 서명된 URL을 만듭니다.
- D. 파일을 Amazon S3로 마이그레이션하고 퍼블릭 VPC 엔드포인트를 생성합니다. 직원이 AWS Single Sign-On으로 로그인하도록 허용합니다.

풀이 과정

B. 윈도우 파일서버+보안엑세스> FSx선택

디렉터리 서비스: 이름을 기준으로 대상을 찾아 조회하거나 편집할 수 있는 서비스/DNS도 디렉터리 서비스의 일종(도메인 이름으로 IP 주소를 조회)

DAP(Directory Access Protocol): 네트워크 상에서 조직이나 개인정보 혹은 파일이나 디바이스 정보 등을 찾아보는 것을 가능하게 만든 소프트웨어 프로토콜. OSI 전체 프로토콜 스택을 지원하며 운영에 매우 많은 컴퓨팅 자원을 필요로 하는 아주 무거운 프로토콜

LDAP(Lightweight Directory Access Protocol): Lightweight-경량의, 가벼운, DAP의 복잡성을 줄이고 TCP/IP 레이어에서 더 적은 비용으로 DAP의 많은 기능적인 부분을 조작

Active Directory: 마이크로 소프트에서 만든 LDAP 디렉토리 서비스. 중앙에 DB를 생성하여 사용자 인증 및 권한부여, 서버와 클라이언트는 DB를 통해 Resource 검색

주요 키워드 스토리지 서비스> S3, FSx

문제 상황 분석

보안엑세스, 승인된사람에게만 접근허용, Windows파일서버, 트래픽 증가로 인한 용량부족

FSx

완전한 네이티브 Windows 파일 시스템을 바탕으로 하는 완전 관리형 Microsoft Windows 파일 서버를 제공

리눅스의NFS>EFS라면 윈도우는 FSx라고 이해중

Active Directory

중앙 DB를 통해 윈도우 기반 서버에 대한 인증서비스 및 LDAP 디렉터리 서비스 제공

04/19-1

비즈니스는 AWS를 사용하여 웹 사이트를 호스팅합니다. 조직은 극도로 변동하는 수요를 수용하기 위해 Amazon EC2 Auto Scaling을 활용했습니다. 경영진은 회사가 특히 3계층 애플리케이션의 프론트 엔드에서 인프라를 과도하게 프로비저닝하고 있다고 우려하고 있습니다. 솔루션 아키텍트의 주요 책임은 성능 저하 없이 비용이 최소화되도록 보장하는 것입니다.

이를 달성하기 위한 솔루션 설계자의 역할은 무엇입니까?

- A. 예약 인스턴스에서 Auto Scaling을 사용합니다.
- B. 예약된 조정 정책으로 Auto Scaling을 사용합니다.
- C. 일시 중단-재개 기능과 함께 Auto Scaling을 사용합니다.
- D. 대상 추적 조정 정책과 함께 Auto Scaling을 사용합니다.

풀이 과정

- A. 예약인스턴스는 1/3년 기간의 인스턴스 사용량을 사전 계약해서 온디맨드 대비 저렴하게 이용가능한 서비스. 오토스케일링과 크게 상관없음.
- B. 예약된 조정 정책은 예측가능한 부하량일 때 사용. 극도로 변동하는 상황에 맞지 않음.
- C. 조정 일시 중단-재개는 일시적으로 오토스케일링 기능을 끄거나 키는 것.
- D. 대상 추적 조정 정책은 조정에 필요한 지표를 선정하고(CPU사용량 등), 목표값(40%이상 또는 80%이상등)을 설정해 오토스케일링 조정.

주요 키워드 EC2 Auto Scaling, 3계층 아키텍처

문제 상황 분석

극도로 변동하는 수요.

프론트엔드에서 인프라가 과도하게 배포중.

성능저하 없이 비용최적화 할 것

04/19-2

Amazon EC2 인스턴스에서 기업은 애플리케이션을 실행합니다. 애플리케이션은 us-east-1 리전의 3개 가용 영역 내 프라이빗 서브넷에 배포됩니다. 파일을 다운로드하려면 인스턴스가 인터넷에 액세스할 수 있어야 합니다. 조직은 지역 전체에서 쉽게 액세스할 수 있는 디자인을 찾고 있습니다.

인터넷 액세스가 중단되지 않도록 하려면 어떤 솔루션을 수행해야 하나요?

- A. 각 가용 영역의 프라이빗 서브넷에 NAT 인스턴스를 배포합니다.
- B. 각 가용 영역의 퍼블릭 서브넷에 NAT 게이트웨이를 배포합니다.
- C. 각 가용 영역의 프라이빗 서브넷에 전송 게이트웨이를 배포합니다.
- D. 각 가용 영역의 퍼블릭 서브넷에 인터넷 게이트웨이를 배포합니다.

풀이 과정

- A. NAT기기(게이트웨이/인스턴스/로드밸런서)는 퍼블릭서브넷에 배치필요. 권장사항은 NAT 게이트웨이를 사용하는 것
- B. 권장사항. 퍼블릭에 NAT G/W배포**
- C. 프라이빗서브넷도 탈락, 전송게이트웨이는 Site to Site VPN에서 사용되는 개념으로 VPC와 온프레미스간 통신 용도
- D. 일반 인터넷 게이트웨이는 퍼블릭영역의 인스턴스만 가능.

주요 키워드

VPC-EC2 배포

문제 상황 분석

다중 AZ의 프라이빗 서브넷에 EC2 인스턴스 배포

사용자 접근 허용

04/19-3

회사 시설의 각 입구에는 배지 판독기가 장착되어 있습니다. 배지가 스캔되면 판독기는 해당 특정 항목을 입력하려고 시도한 사람을 나타내는 HTTPS 메시지를 전송합니다.

솔루션 설계자는 이러한 센서 신호를 처리할 시스템을 개발해야 합니다. 솔루션은 회사의 보안 직원이 분석할 수 있도록 결과를 제공하여 액세스 가능성이 높아야 합니다.

솔루션 아키텍트가 권장해야 하는 시스템 설계는 무엇입니까?

A. Amazon EC2 인스턴스를 시작하여 HTTPS 엔드포인트 역할을 하고 메시지를 처리합니다. 결과를 Amazon S3 버킷에 저장하도록 EC2 인스턴스를 구성합니다.

B. Amazon API Gateway에서 HTTPS 엔드포인트를 생성합니다. AWS Lambda 함수를 호출하여 메시지를 처리하고 결과를 Amazon DynamoDB 테이블에 저장하도록 API Gateway 엔드포인트를 구성합니다.

C. Amazon Route 53을 사용하여 수신 센서 메시지를 AWS Lambda 함수로 보냅니다. 메시지를 처리하고 결과를 Amazon DynamoDB 테이블에 저장하도록 Lambda 함수를 구성합니다.

D. Amazon S3용 게이트웨이 VPC 엔드포인트를 생성합니다. 센서 데이터가 VPC 엔드포인트를 통해 S3 버킷에 직접 기록될 수 있도록 시설 네트워크에서 VPC로의 Site-to-Site VPN 연결을 구성합니다.

주요 키워드

음.. 네트워크 통신 과정에 대한 일반적인 이해..?

문제 상황 분석

특정 데이터를 HTTPS를 통해 받음

받은 데이터를 분석하여 액세스 가능해야함

풀이 과정

A. S3는 DB가 아니라 단순 저장(스토리지)서비스라서 분석이 안되지 않을까요? 그렇게 생각했는데 확신은 없네요

B. Lambda-API G/W를 활용한 서버리스 구조. 결과 DynamoDB 연계. 타당타당

C. Route 53은 DNS 서비스.

D. A랑 비슷하게 S3를 활용했기 때문에 탈락.

04/20-1

새 워크로드를 구현하기 전에 솔루션 설계자는 회사의 현재 IAM 규칙을 검사하고 업데이트해야 합니다. 다음 정책은 솔루션 설계자가 작성했습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "NotAction": "s3:PutObject",
    "Resource": "*",
    "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}
  }]
}
```

정책의 순 효과는 무엇입니까?

- A. 다중 요소 인증(MFA)이 활성화된 경우 사용자는 s3:PutObject를 제외한 모든 작업이 허용됩니다.
- B. 다중 요소 인증(MFA)이 활성화되지 않은 경우 사용자는 s3:PutObject를 제외한 모든 작업이 허용됩니다.
- C. 다중 요소 인증(MFA)이 활성화된 경우 사용자는 s3:PutObject를 제외한 모든 작업이 거부됩니다.
- D. 다중 요소 인증(MFA)이 활성화되지 않은 경우 사용자는 s3:PutObject를 제외한 모든 작업이 거부됩니다.

풀이 과정

"Effect": "Deny" > "효과": "거부"

"NotAction": "s3:PutObject" > "활동 안함": "s3:PutObject"

"Resource": "*" > "리소스": "모든 것"

"Condition": "MFA": "false" > "조건": "MFA": "비활성화"

거부하십쇼, s3:PutObject 활동 안함, 모든 대상에 대해, MFA가 비활성화라면 > 정리하면 **D**

주요 키워드

IAM Policy

문제 상황 분석

다음.. json 파일을.. 읽으십시오..?

04/20-2

실시간 처리를 허용하려면 웹 애플리케이션이 Amazon S3에 주문 데이터를 유지해야 합니다. 솔루션 설계자는 확장 가능하고 내결함성이 있는 아키텍처를 설계해야 합니다.

어떤 솔루션이 이러한 기준을 충족합니까? (2개를 선택하세요.)

- A. Amazon DynamoDB 테이블에 주문 이벤트를 씁니다. DynamoDB 스트림을 사용하여 페이로드를 구문 분석하고 Amazon S3에 데이터를 쓰는 AWS Lambda 함수를 트리거합니다.
- B. Amazon Simple Queue Service(Amazon SQS) 대기열에 주문 이벤트를 씁니다. 대기열을 사용하여 페이로드를 구문 분석하고 Amazon S3에 데이터를 쓰는 AWS Lambda 함수를 트리거합니다.
- C. Amazon Simple Notification Service(Amazon SNS) 주제에 주문 이벤트를 씁니다. SNS 주제를 사용하여 페이로드를 구문 분석하고 Amazon S3에 데이터를 쓰는 AWS Lambda 함수를 트리거합니다.
- D. Amazon Simple Queue Service(Amazon SQS) 대기열에 주문 이벤트를 씁니다. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 사용하여 페이로드를 구문 분석하고 Amazon S3에 데이터를 쓰는 AWS Lambda 함수를 트리거합니다.
- E. Amazon Simple Notification Service(Amazon SNS) 주제에 주문 이벤트를 씁니다. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 사용하여 페이로드를 구문 분석하고 Amazon S3에 데이터를 쓰는 AWS Lambda 함수를 트리거합니다.

틀린 이유

SNS&SQS를 묶어서 쓰는거를 기준으로 생각하고 뭔가 확장가능/내결함성이라길래 뭔지는 모르지만 EventBridge까지 섞어서 DE 골랐었네요.

풀이 과정

A. 실시간 처리가 필요하므로 데이터 캡처 스트리밍을 거의 실시간으로 지원하는 DynamoDB 스트림을 써야하나보구나라고 이해했습니다.

B. 내결함성과 가용성이라면 좀더 SQS가 어울리지 않을까요? 흑흑 왜 SNS가 답이지

C. SNS는 게시자에서 구독자에게로 메시지를 전송하는 관리형 서비스. 여기서는 웹어플(게시자)가 S3에게(구독자)에게로 데이터를 보내는 상황같은데 SNS는 메시지 발송 실패시 별도의 배달못한 메시지 대기열이 없으면 그대로 데이터를 삭제하지않나요? 근데 그건 또 내결함성은 아닌가 으으

DE BC와 차이점은 이벤트 브릿지를 쓰냐 안쓰냐 차이점인거같아요. 이벤트 브릿지는 데이터 전달용 서비스지 구문분석용 서비스가 아니라서 오답일까요? 그렇다해도 대기열이나 SNS주제가 뭔가 데이터 분석에 사용하는 서비스는 아닌거같은데..

EventBridge 다양한 소스에서 들어오는 데이터와 어플리케이션을 연결시켜주는 서버리스 이벤트 버스 서비스. CloudWatch Events에서 여러 추가기능을 덧붙임

주요 키워드

S3, SNS&SQS, EventBridge

문제 상황 분석

실시간 처리 위해 S3 주문데이터가 유지되는 솔루션 생성

04/20-3

us-east-1 지역의 비즈니스에서 사진 호스팅 서비스를 제공합니다. 많은 국가의 사용자가 프로그램을 사용하여 이미지를 업로드하고 탐색할 수 있습니다. 일부 사진은 몇 달 동안 조회수가 높은 반면 다른 사진은 일주일 미만 동안 조회수가 적습니다. 이 프로그램은 최대 20MB 크기의 사진 업로드를 지원합니다. 서비스는 사진 정보를 기반으로 각 사용자에게 어떤 사진을 보여줄지 결정합니다.

적합한 사용자에게 가장 비용 효율적인 액세스를 제공하는 옵션은 무엇입니까?

- A. Amazon DynamoDB에 사진을 저장합니다. 자주 보는 항목을 캐시하려면 DynamoDB Accelerator(DAX)를 커십시오.
- B. Amazon S3 Intelligent-Tiering 스토리지 클래스에 사진을 저장합니다. 사진 메타데이터와 해당 S3 위치를 DynamoDB에 저장합니다.
- C. Amazon S3 Standard 스토리지 클래스에 사진을 저장합니다. S3 수명 주기 정책을 설정하여 30일이 지난 사진을 S3 Standard-Infrequent Access(S3 Standard-IA) 스토리지 클래스로 이동합니다. 객체 태그를 사용하여 메타데이터를 추적합니다.
- D. Amazon S3 Glacier 스토리지 클래스에 사진을 저장합니다. S3 수명 주기 정책을 설정하여 30일이 지난 사진을 S3 Glacier Deep Archive 스토리지 클래스로 이동합니다. 사진 메타데이터와 해당 S3 위치를 Amazon Elasticsearch Service(Amazon ES)에 저장합니다.

틀린이유

단순히 일부 빈번/일부아닌 사진 저장에 대한 솔루션이라고 생각해서 C를 선택

풀이 과정

A. DynamoDB의 최대 항목크기는 400KB, 사진은 최대 20MB 탈락

B. S3 Intelligent-Tiering은 데이터 액세스 패턴에 따라 유동적으로 저장계층을 변경함.

C. 30일이 지난 데이터를 S3standard-IA로 옮기면 몇 달동안 조회수가 높기 때문에 아직 빈번한 액세스여도 IA로 옮겨지므로 탈락

D. Glacier의 데이터를 받아오는데는 별도의 절차가 필요하기 때문에 호스팅 서비스에 비적합 30일 변경도 비적합

주요 키워드

S3 스토리지

문제 상황 분석

사진 저장, 일부 데이터는 빈번하게 사용/일부는 아님.

비용 효율적인 서비스는?