

STT 서비스 구축을 위한 AWS 설정 과정

학과: 정보컴퓨터공학부

과목명: 클라우드컴퓨팅

7조 김태훈 박민재 김성문 박재열

1. 목적

STT 서비스 구축을 위해 AWS에서 제공하는 서비스를 생성 및 설정하며, 서비스들끼리 연결시킨다.

2. 전체 다이어그램

언어코드

영어(영국) : en-GB
영어(미국) : en-US
한국어 : ko-KR
일본어 : ja-JP
중국어(간체) : zh-CN
중국어(번체) : zh-TW
자동감지 : "auto"(IdentifyLanguage=True)
<https://docs.aws.amazon.com/transcribe/latest/dg/supported-languages.html>
https://docs.aws.amazon.com/transcribe/latest/APIReference/API_StartTranscriptionJob.html

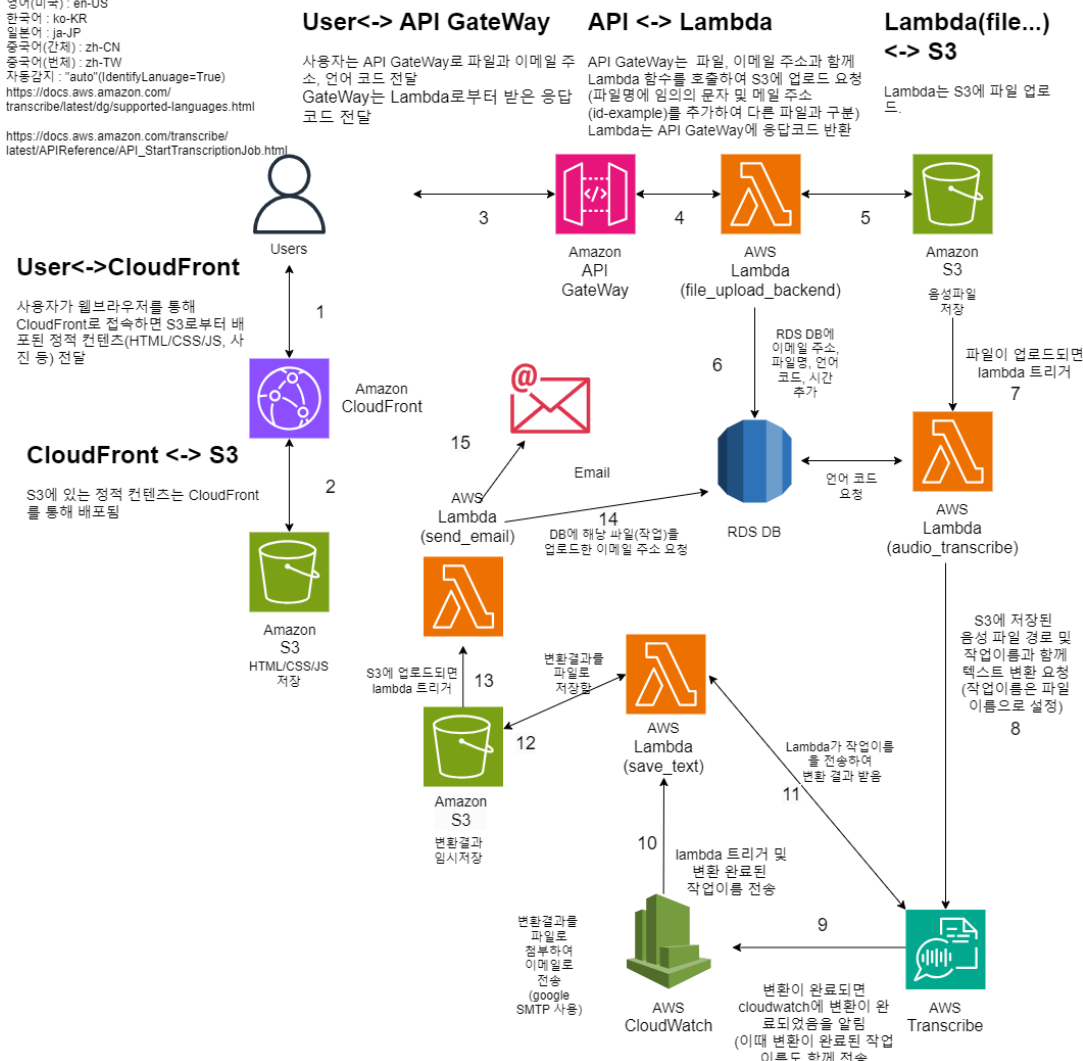


그림 1 전체 다이어그램

전체 다이어그램은 위와 같다.

3. 정적 웹사이트 구축

Amazon S3, Amazon CloudFront를 사용하여 정적인 파일(html/css/js)를 호스팅하는 웹페이지를 구축한다.

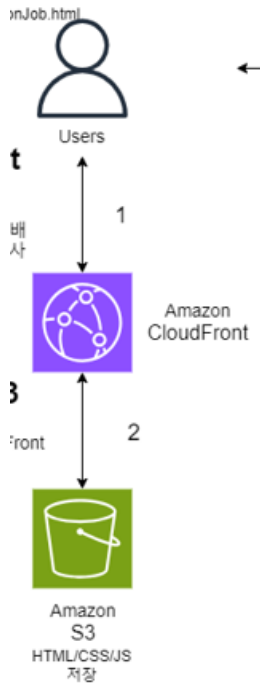
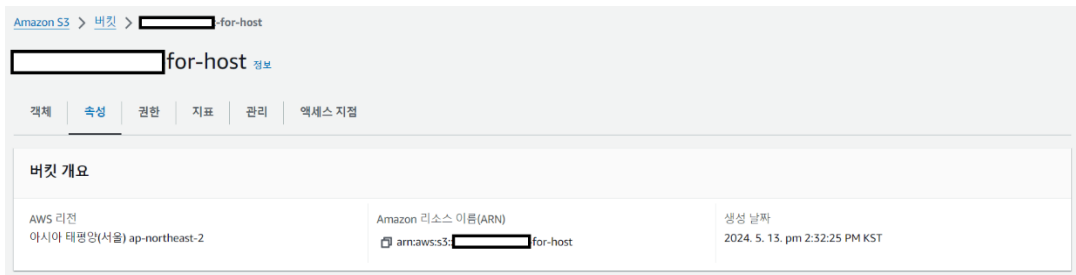


그림 2 정적 웹사이트 구축

즉 그림1에서 위 부분을 구성한다.

(1) s3 버킷 생성



버킷 이름을 지정하여 버킷을 만든다.

이 버킷의 퍼블릭 액세스 차단 설정

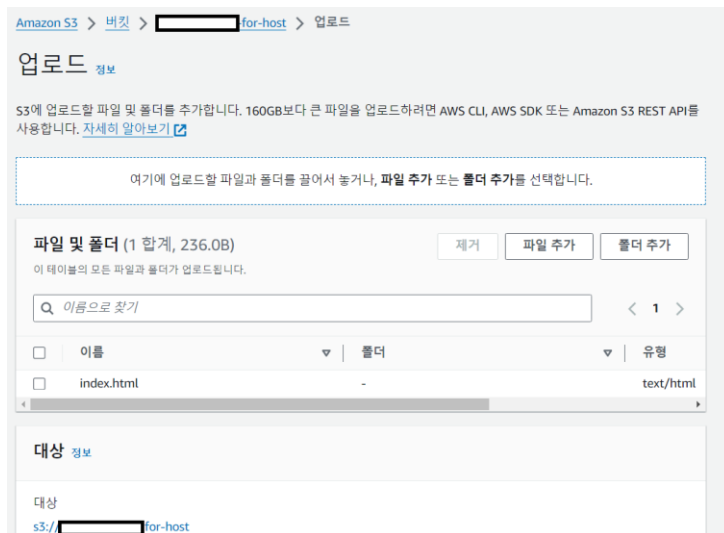
퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지정 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 이 버킷 및 해당 객체에 대한 퍼블릭 액세스가 차단되었는지 확인하려면 모든 퍼블릭 액세스 차단을 활성화합니다. 이 설정은 이 버킷 및 해당 액세스 지점에만 적용됩니다. AWS에서는 모든 퍼블릭 액세스 차단을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 이 버킷 또는 내부 객체에 대한 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 아래 개별 설정을 사용자 지정할 수 있습니다. [자세히 알아보기](#)

☒ **모든 퍼블릭 액세스 차단**

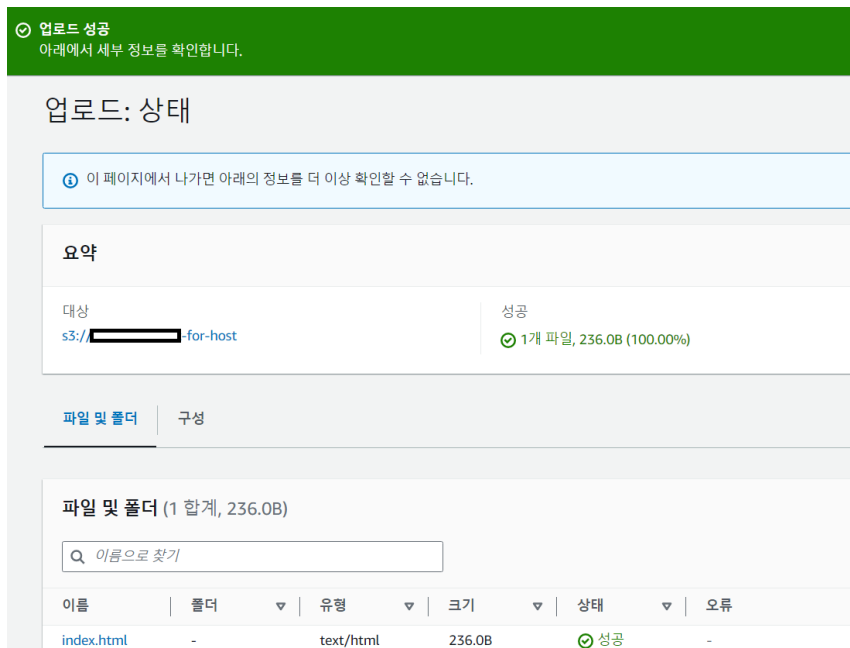
이 설정을 활성화하면 아래 4개의 설정을 모두 활성화한 것과 같습니다. 다음 설정 각각은 서로 독립적입니다.

- ☒ **새 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단**
S3은 새로 추가된 버킷 또는 객체에 적용되는 퍼블릭 액세스 권한을 차단하며, 기존 버킷 및 객체에 대한 새 퍼블릭 액세스 ACL 생성을 금지합니다. 이 설정은 ACL을 사용하여 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 권한을 변경하지 않습니다.
- ☒ **임의의 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단**
S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 ACL을 무시합니다.
- ☒ **새 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단**
S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지정 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 정책을 변경하지 않습니다.
- ☒ **임의의 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 및 교차 계정 액세스 차단**
S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 정책을 사용하는 버킷 또는 액세스 지점에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.

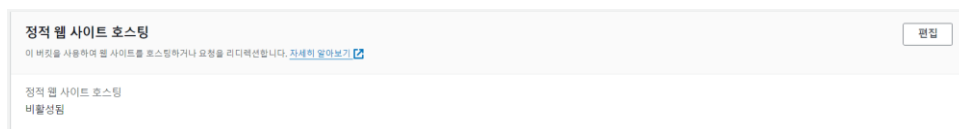
cloudfront를 이용하여 서비스할 예정이므로, 퍼블릭엑세스는 차단한다.



s3에 index.html 파일을 업로드한다(테스트용).



업로드 성공 메시지를 확인한다.



s3의 속성에서 정적 웹사이트 호스팅 설정을 편집한다.

정적 웹 사이트 호스팅 편집
정보
정보

정적 웹 사이트 호스팅

이 버킷을 사용하여 웹 사이트를 호스팅하거나 요청을 리디렉션합니다. [자세히 알아보기](#)

정적 웹 사이트 호스팅

☐ 비활성화

☒ 활성화

호스팅 유형

☒ 정적 웹 사이트 호스팅
버킷 엔드포인트를 웹 주소로 사용합니다. [자세히 알아보기](#)

☐ 객체에 대한 요청 리디렉션
요청을 다른 버킷 또는 도메인으로 리디렉션합니다. [자세히 알아보기](#)

i 고객이 웹 사이트 엔드포인트의 콘텐츠에 액세스할 수 있게 하려면 모든 콘텐츠를 공개적으로 읽기 가능하도록 설정해야 합니다. 이렇게 하려면, 버킷에 대한 S3 퍼블릭 액세스 차단 설정을 편집하면 됩니다. 자세한 내용은 [Amazon S3 퍼블릭 액세스 차단 사용](#) 참조하십시오.

인덱스 문서

웹 사이트의 홈 페이지 또는 기본 페이지를 지정합니다.

오류 문서 - 선택 사항

오류가 발생하면 반환됩니다.

위와 같이 정적 웹사이트 호스팅을 활성화하고, index.html을 기본 페이지로 설정한다.

(2) cloudfront 설정

Origin domain
Choose an AWS origin, or enter your origin's domain name.

! 이 S3 버킷은 S3 웹 사이트로 구성됩니다. 이 배포를 웹 사이트로 사용하려는 경우 버킷 엔드포인트 대신 S3 웹 사이트 엔드포인트를 사용하는 것이 좋습니다.

[웹 사이트 엔드포인트 사용](#)

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

이름
이 원본의 이름을 입력합니다.

원본 액세스 | 정보

☐ 공개
버킷은 공개 액세스를 허용해야 합니다.

☒ 원본 액세스 제어 설정(권장)
버킷은 CloudFront에 대한 액세스만 제한할 수 있습니다.

☐ Legacy access identities
CloudFront 원본 액세스 ID(OAI)를 사용하여 S3 버킷에 액세스합니다.

Origin access control
Select an existing origin access control (recommended) or create a new control.

Create new OAC

i 이 정책 설정을 사용하여 CloudFront에 대한 액세스를 허용해야 합니다. S3 버킷에 액세스할 수 있는 CloudFront 권한 부여에 대해 자세히 알아보세요.

[정책 복사](#)

i S3 버킷 권한으로 이동

사용자 정의 헤더 추가 - 선택 사항
CloudFront는 원본으로 보내는 모든 요청에 이 헤더를 포함합니다.

Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

☐ 아니요

☒ 예

그리고 cloudfront를 설정한다. origin domain은 정적 웹사이트 호스팅을 활성화한 s3로 설정하고, OAC를 설정한다(후술). 그리고 Origin Shield를 활성화한다.

동작 편집

설정

경로 패턴 | 정보

기본값(*)

원본 및 원본 그룹

s3-website.ap-northeast-2.amazonaws.com

자동으로 객체 압축 | 정보

☐ No
 ☒ Yes

뷰어

뷰어 프로토콜 정책

☐ HTTP and HTTPS
 ☒ Redirect HTTP to HTTPS
 ☐ HTTPS only

허용된 HTTP 방법

☒ GET, HEAD
 ☐ GET, HEAD, OPTIONS
 ☐ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

뷰어 액세스 제한

뷰어 액세스를 제한하는 경우 뷰어는 CloudFront 서명된 URL 또는 서명된 쿠키를 사용하여 사용자의 콘텐츠에 액세스해야 합니다.
 ☒ No
 ☐ Yes

캐시 키 및 원본 요청

캐시 정책 및 원본 요청 정책을 사용하여 캐시 키 및 원본 요청을 제어할 것을 권장합니다.
 ☒ Cache policy and origin request policy (recommended)
 ☐ Legacy cache settings

캐시 정책

기존 캐시 정책을 선택하거나 새 캐시 정책을 생성합니다.

CachingOptimized
 Recommended for S3

 Policy with caching enabled. Supports Gzip and Brotli compression.

Create cache policy
 Edit
 Delete

그리고 cloudfront의 동작을 편집한다. GET, HEAD를 허용하고, 캐시 정책을 CachingOptimized로 설정하여 cloudfront가 s3의 콘텐츠를 캐싱하도록 한다.

설정

가격 분류 | 정보

지불하려는 최고가와 연관된 가격 분류를 선택합니다.
 ☒ 모든 엣지 로케이션에서 사용(최고의 성능)
 ☐ 북미 및 유럽만 사용
 ☐ 북미, 유럽, 아시아, 중동 및 아프리카에서 사용

대체 도메인 이름(CNAME) - 선택 사항

이 배포에서 제공하는 파일에 대해 URL에서 사용하는 사용자 정의 도메인 이름을 추가합니다.

항목 추가

☒ 대체 도메인 이름 목록을 추가하려면 대량 편집기를(를) 사용하십시오.

Custom SSL certificate - optional

AWS Certificate Manager의 인증서를 연결합니다. 인증서는 반드시 미국 동부(버지니아 북부) 리전(us-east-1)에 있어야 합니다.

인증서 선택

인증서 요청

지원되는 HTTP 버전

추가 HTTP 버전에 대한 지원을 추가합니다. HTTP/1.0 및 HTTP/1.1이 기본값으로 지원합니다.
 ☒ HTTP/2
 ☐ HTTP/3

기본값 루트 객체 - 선택 사항

뷰어가 특정 객체 대신 루트 URL(/)을 요청할 때 반환할 객체(파일 이름)입니다.

/index.html

표준 로깅

Amazon S3 버킷으로 전송된 뷰어 요청의 로그를 가져옵니다.
 ☒ 끄기
 ☐ 켜기

IPv6

☐ 끄기
 ☒ 켜기

모든 엣지 로케이션에 콘텐츠를 배포하고, xxxx.cloudfront.net으로 접속 시 index.html을 반환하도록 한다. HTTP/2 를 지원하도록 설정하고, IPv6를 켜다.

일반	보안	원본	동작	오류 페이지	무효화	태그
----	----	----	----	--------	-----	----

오류 페이지				편집	삭제	사용자 정의 오류 응답 생성
HTTP 오류 코드	최소 TTL(초)	응답 페이지 경로	HTTP 응답 코드			
○ 403	10	/index.html	200			

사용자가 정의되지 않은 리소스를 호출했을 경우, s3에서 403 forbidden을 반환하게 되고, cloudfront에서는 이를 index.html(응답 코드 200)로 사용자에게 응답한다. 즉 정의되지 않은 리소스를 호출하면 사용자는 초기화면(index.html)로 돌아간다.

(3) OAC 생성 및 버킷 정책 편집

Create new OAC

×

이름

이름은 고유해야 합니다. 문자, 숫자 및 대부분의 특수 문자를 사용할 수 있습니다. 최대 64자까지 사용할 수 있습니다.

hostingOAC

설명 - 선택 사항

설명은 최대 256자까지 입력할 수 있습니다.

host to S3

서명 동작

☐ 요청 서명 안 함
 ☒ 서명 요청 (권장)

☐ 승인 헤더 재정의 안 함

수신 요청에 승인 헤더가 있는 경우 서명하지 마세요.

원본 유형

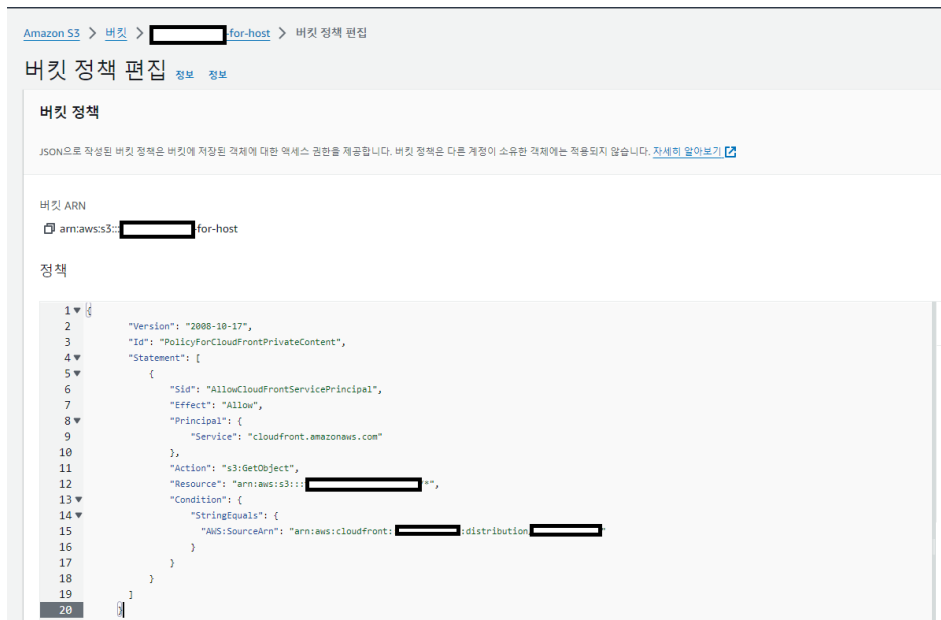
S3

원본 유형은 원본 도메인과 동일한 유형이어야 합니다.

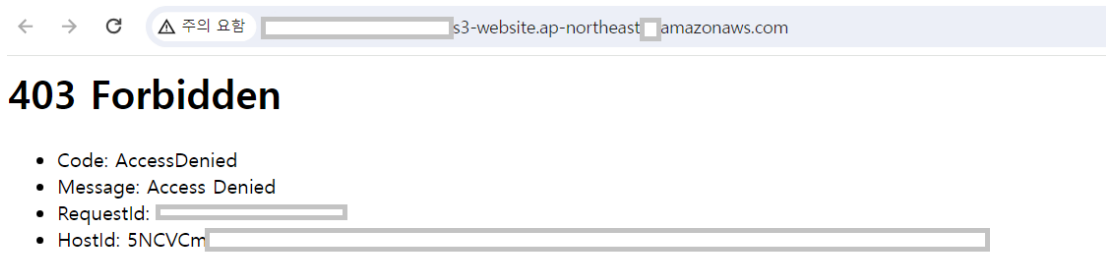
취소

Create

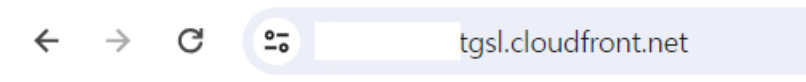
OAC를 생성한다 OAC를 생성하여 cloudfront가 s3에 접근할 수 있도록 한다.



OAC를 생성하면 s3 버킷 정책을 편집하라고 알려준다. s3 버킷 정책에 넣을 내용과 함께 안내되므로, 이를 s3 버킷 정책에 입력한다.



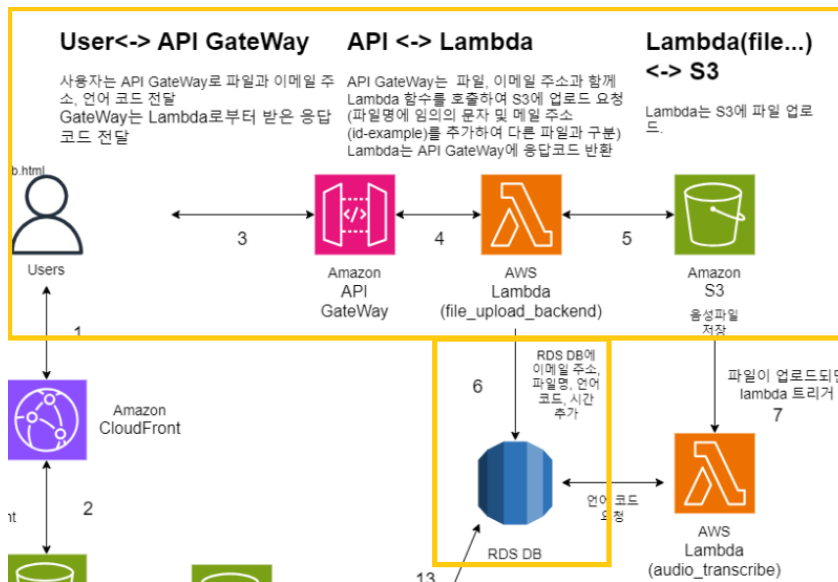
s3로 바로 접속하면 403 Forbidden 메시지와 함께 접속이 차단되며, https도 지원되지 않는다.



hello world!

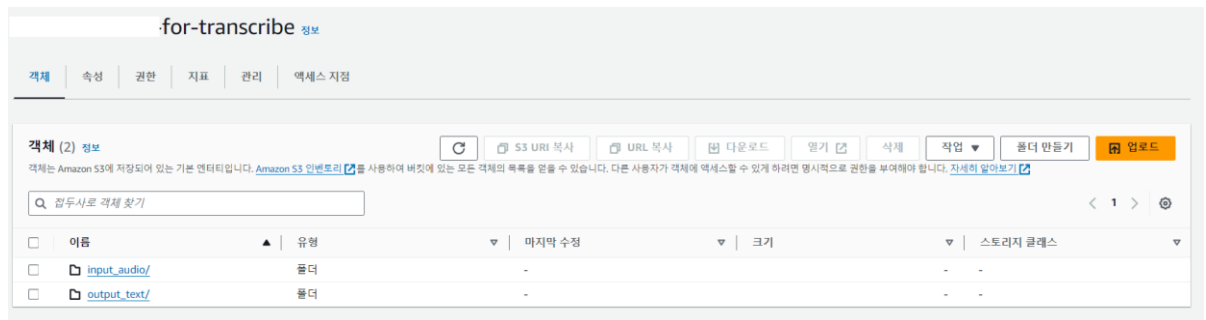
cloudfront로 접속하면 위와 같이 잘 접속되는 것을 확인할 수 있고, https도 지원되는 것을 확인할 수 있다.

4. 파일 업로드 구축



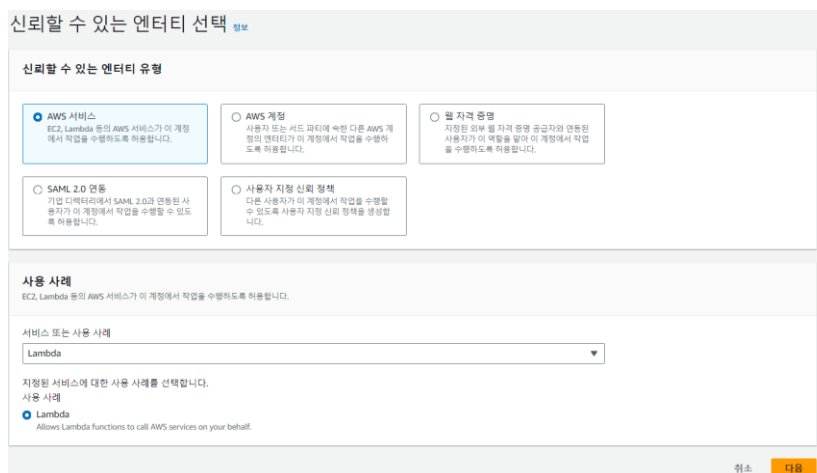
이제 위와 같이 다이어그램에서 API Gateway, file_backend_lambda 함수, 음성파일 저장하는 S3, 음성파일 관련정보(이메일, 파일명, 언어코드, 업로드 시간)를 저장하는 RDS DB(mysql)를 만든다.

(1) 버킷 생성



s3 버킷을 만들고, input_audio와 output_text 폴더를 만든다. input_audio는 업로드된 음성 파일이, output_text는 변환 결과가 임시 저장되는 곳이다. 속성 탭에서, 모든 퍼블릭 액세스를 차단해야한다.

(2) lambda 함수에 적용할 IAM 생성



file_upload_backend 람다 함수를 위한 IAM를 만든다.

IAM > 역할 > role-file-upload

role-file-upload 정보

Allows Lambda functions to call S3 and CloudWatch

요약

생성 날짜
May 13, 2024, 15:47 (UTC+09:00)

마지막 활동
-

ARN
arn:aws:iam:::role/role-file-upload

최대 세션 지속 시간
1시간

권한 | 신뢰 관계 | 태그 | 액세스 관리자 | 세션 취소

권한 정책 (4) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

필터링 기준 유형
모든 유형

<input type="checkbox"/>	정책 이름	유형	연결된 엔터티
<input type="checkbox"/>	AmazonRDSFullAccess	AWS 관리형	1.
<input type="checkbox"/>	AmazonS3FullAccess	AWS 관리형	2.
<input type="checkbox"/>	AWSLambdaVPCLocalAccessExecutionRole	AWS 관리형	1.
<input type="checkbox"/>	CloudWatchLogsFullAccess	AWS 관리형	1.

file_upload_backend 람다 함수를 위한 IAM은 RDS와 S3에 접근하여야 되고, RDS DB가 속한 VPC에 접속할 수 있어야 한다.

(3) lambda 함수 생성

Lambda > 함수 > 함수 생성

함수 생성 정보

다음 옵션 중 하나를 선택하여 함수를 생성합니다.

☒ **새로 작성**
간단한 Hello World 예제는 시작하십시오.

☐ **블루프린트 사용**
샘플 코드 및 구축 Lambda 애플리케이션을 위한 :

기본 정보

함수 이름
함수의 용도를 설명하는 이름을 입력합니다.

file-upload-backend

공백 없이 문자, 숫자, 하이픈 또는 밑줄만 사용합니다.

런타임 정보
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Node.js 20.x

아키텍처 정보
함수 코드에 대해 원하는 명령 세트 아키텍처를 선택합니다.

☒ x86_64

☐ arm64

권한 정보
기본적으로 Lambda는 Amazon CloudWatch Logs에 로그를 업로드하는 권한을 가진 실행 역할을 생성합니다. 이 기본 역할은 나중에 트리거를 추가할 때 사용자 지정할 수

▼ 기본 실행 역할 변경

실행 역할
함수에 대한 권한을 정의하는 역할을 선택합니다. 사용자 지정 역할을 생성하려면 IAM 콘솔로 이동하십시오.

☐ 기본 Lambda 권한을 가진 새 역할 생성

☒ 기존 역할 사용

☐ AWS 정책 템플릿에서 새 역할 생성

기존 역할
생성한 기본 역할 중에 이 Lambda 함수와 함께 사용할 역할을 선택합니다. 이 역할에는 Amazon CloudWatch Logs에 로그를 업로드할 수 있는 권한이 있어야 합니다.

role-file-upload

IAM 콘솔에서 role-file-upload 역할을 확인합니다.

이제 함수를 생성한다. 런타임은 node.js 20 x로 설정하고, 역할을 아까 만든 role-file-upload로 설정한다.

기본 설정 정보

설명 - 선택 사항

메모리 정보
구성된 메모리에 비례하는 CPU가 함수에 할당됩니다.

512

 MB
메모리를 128MB~10240MB 범위로 설정

임시 스토리지 정보
함수에 대해 최대 10GB의 임시 스토리지(/tmp)를 구성할 수 있습니다. [요금 보기](#)

512

 MB
임시 스토리지(/tmp)를 512MB~10240MB 사이로 설정합니다.

SnapStart 정보
함수가 초기화된 후 Lambda가 함수의 스냅샷을 캐싱하도록 설정해 시작 시간을 단축합니다. 함수 코드가 스냅샷 작업 여부를 평가하려면 [SnapStart 호환성 고려 사항](#)을 검토하세요.

None

지원되는 런타임: Java 11, Java 17, Java 21.

제한 시간

1

 분

30

 초

실행 역할
함수에 대한 권한을 정의하는 역할을 선택합니다. 사용자 지정 역할을 생성하려면 [IAM 콘솔](#)로 이동하십시오.
☒ 기존 역할 사용

lambda 함수를 만든 후. 설정에서 메모리와 제한시간을 변경한다. 메모리는 기존 128MB에서 512MB로, 제한 시간은 기존 3초에서 1분 30초로 변경한다. s3에 파일을 저장하고, RDS DB에 데이터를 써야하므로 , 제한 시간을 늘렸다.

(4) API 생성

REST API

API 관리 기능과 함께 요청 및 응답을 완벽하게 제어할 수 있는 REST API를 개발합니다.

다음과 호환됩니다.
Lambda, HTTP, AWS 서비스

가져오기

구축

이제 API GateWay 메뉴로 가서, REST API를 구축한다.

REST API 생성

API 세부 정보

☒ **새 API**
 새 REST API를 생성합니다.

☐ **기존 API 복제**
 이 AWS 계정에서 API 사본을 생성합니다.

☐ **API 가져오기**
 OpenAPI 정의에서 API를 가져옵니다.

☐ **예제 API**
 예제 API를 통해 API 게이트웨이에 대해 알아보세요.

API 이름

설명 - 선택 사항

API 엔드포인트 유형
 리전 API는 현재 AWS 리전에 배포되어 있습니다. 엣지 최적화 API는 요청을 가장 가까운 CloudFront 접속 지점으로 라우팅합니다. 프라이빗 API는 VPC에서만 액세스할 수 있습니다.

지역

취소

API 생성

API 세부 정보에서 이름은 file-upload-api로 설정하고, API 엔드포인트 유형은 지역으로 설정한다.

리소스 생성

리소스 세부 정보

☒ **프록시 리소스 정보**
 프록시 리소스는 모든 하위 리소스에 대한 요청을 처리합니다. 프록시 리소스를 생성하려면 더하기 기호로 끝나는 경로 파라미터(예: {proxy+})를 사용합니다.

리소스 경로

리소스 이름

☒ **오리진 간 리소스 공유(CORS) 정보**
 모든 오리진, 모든 메서드 및 몇 가지 공통 헤더를 허용하는 OPTIONS 메서드를 생성합니다.

취소

리소스 생성

만들어진 API에 리소스 생성을 클릭하여 하위 리소스를 생성한다. 즉 호출될 때

xxxxxx.execute-api.ap-xxxxxxxxx.amazonaws.com/(배포 스테이지)/file-upload로 호출된다. (배포 스테이지는 배포할 때 설정)

하위 리소스를 생성할 때 CORS를 체크한다.

메서드 생성

메서드 세부 정보

메서드 유형

메서드 유형 선택

통합 유형

☒ Lambda 함수

API를 Lambda 함수와 통합합니다.



☐ HTTP

기존 HTTP 엔드포인트와 통합합니다.



☐ Mock

API Gateway 매핑 및 변환을 기반으로 응답을 생성합니다.



☐ AWS 서비스

AWS 서비스와 통합합니다.



☐ VPC 링크

퍼블릭 인터넷을 통해 액세스할 수 없는 리소스와 통합합니다.

☒ Lambda 프록시 통합

요청을 구조화된 이벤트로

Lambda 함수

Lambda 함수 이름 또는 별칭

ap-northe...

arn:aws:lambda:ap-northeast-1:123456789012:function:file-upload-backend

arn:aws:lambda:ap-northeast-1:123456789012:function:file-upload-backend

arn:aws:lambda:ap-northeast-1:123456789012:function:send_email

arn:aws:lambda:ap-northeast-1:123456789012:function:audio_transcribe

arn:aws:lambda:ap-northeast-1:123456789012:function:audio_transcribe

API Gateway에 Lambda 함수를 간접적으로 호출할 권한을 부여합니다. 이 기능을 끄면 함수의 리소스 정책을 직접 업데이트하거나 API Gateway가 함수를 간접적으로 호출하는 데 사용하는 호출 역할을 제공하세요.

☒ 기본 제한 시간

기본 제한 시간은 29초입니다.



Lambda 프록시 통합

요청을 구조화된 이벤트로 Lambda 함수에 전송합니다.

그리고 API가 실행할 것을 선택한다. 여기서는 lambda 함수를 실행하고, lambda 함수 중 file-upload-backend 함수를 실행하는 것으로 설정한다. 그리고, multipart/form-data를 받기 위해 lambda 프록시 통합을 활성화한다.

Deploy API

API를 배포할 스테이지를 생성하거나 선택합니다. 배포 기록을 사용하여 스테이지의 활성 배포를 되돌리거나 변경할 수 있습니다. [Learn more](#)

스테이지

새 스테이지

스테이지 이름

prod

기본 설정으로 새 스테이지가 생성됩니다. 스테이지 페이지에서 스테이지 설정을 편집합니다.

배포 설명

file-upload-api

취소

배포

그리고 위와 같이 API를 배포한다. 스테이지 이름을 prod로 했으므로, 파일 업로드 요청시 API 주소는 xxxxxx.execute-api.ap-xxxxxxxxx.amazonaws.com/prod/file-upload 가 된다.

(5) RDS 생성

설정

DB 인스턴스 식별자 정보

DB 인스턴스 이름을 입력하세요. 이름은 현재 AWS 리전에서 AWS 계정이 소유하는 모든 DB 인스턴스에 대해 고유해야 합니다.

-info

DB 인스턴스 식별자는 대소문자를 구분하지 않지만 'mydbinstance'와 같이 모두 소문자로 저장됩니다. 제약: 1~60자의 영숫자 또는 하이픈으로 구성되어야 합니다. 첫 번째 문자는 글자여야 합니다. 하이픈 2개가 연속될 수 없습니다. 하이픈으로 끝날 수 없습니다.

▼ 자격 증명 설정

마스터 사용자 이름 정보

DB 인스턴스의 마스터 사용자에 로그인 ID를 입력하세요.

1~16자의 영숫자. 첫 번째 문자는 글자여야 합니다.

자격 증명 관리

AWS Secrets Manager를 사용하거나 마스터 사용자 자격 증명을 관리할 수 있습니다.

☐ AWS Secrets Manager에서 관리 - 가장 뛰어난 안정성

RDS는 자동으로 암호를 생성하고 AWS Secrets Manager를 사용하여 전체 수명 주기 동안 암호를 관리합니다.

☒ 자체 관리

사용자가 암호를 생성하거나 RDS에서 암호를 생성하고 사용자가 관리할 수 있습니다.

☒ 암호 자동 생성

Amazon RDS에서 자동으로 암호를 생성하거나 사용자가 직접 암호를 지정할 수 있습니다.

① 데이터베이스를 생성한 후 자격 증명을 볼 수 있습니다. 데이터베이스 생성 배너에서 '자격 증명 세부 정보 보기'를 클릭하면 암호를 볼 수 있습니다.

이제 DB를 생성한다. DB 인스턴스 식별자를 설정하고, 마스터 사용자 이름과 비밀번호를 설정한다. 암호 자동 생성을 체크하면 생성 후에, 비밀번호가 담겨진 파일을 다운받게 되고, 이 안에 비밀번호가 담겨있게 된다. 이 파일을 메모장으로 열면 무작위의 숫자와 문자로 이루어진 비밀번호가 들어있다.

▼ 추가 구성

데이터베이스 옵션, 암호화 커짐, 백업 커짐, 역추적 커짐, 유지 관리, CloudWatch Logs, 삭제 방지 커짐.

데이터베이스 옵션

초기 데이터베이스 이름 정보

-info

데이터베이스 이름을 지정하지 않으면 Amazon RDS에서 데이터베이스를 생성하지 않습니다.

DB 파라미터 그룹 정보

default.mysql8.0

옵션 그룹 정보

default:mysql-8-0

백업

☒ 자동 백업을 활성화합니다.

데이터베이스의 특정 시점 스냅샷을 생성합니다.

⚠ 자동 백업 기능은 현재 InnoDB 스토리지 엔진에 대해서만 지원됩니다. MyISAM을 사용하는 경우 [여기를](#)에서 자세한 정보를 참조하세요.

DB는 mysql로 설정하고, 자동 백업을 활성화한다.

연결 및 보안

엔드포인트 및 포트

엔드포인트

포트

3306

네트워킹

가용 영역

ap-

VPC

vpc-

서브넷 그룹

default

서브넷

subnet-

subnet-

subnet-

subnet-

네트워크 유형

IPv4

보안

VPC 보안 그룹

default

활성

퍼블릭 액세스 가능

예

인증 기관 정보

rds-

인증 기관 날짜

(UTC+09:00)

DB 인스턴스 인증서 만료 날짜

(UTC+09:00)

그리고 위와 같이 RDS가 속할 VPC와 VPC 보안 그룹을 설정한다. 이 설정을 통해 VPC에 속한 사용자/lambda 함수만 DB에 접속할 수 있게 한다.

Lambda

>

함수

>

file-upload-backend

>

VPC 편집

VPC 편집

VPC

계정의 VPC에 함수를 연결하면 VPC가 액세스를 제공하지 않는 한 인터넷에 액세스할 수 없습니다. 함수에 인터넷 액세스 권한을 부여하려면 퍼블릭 서브넷의 NAT 게이트웨이로 아웃바운드 트래픽을 라우팅합니다.

[자세히 알아보기](#)

VPC 정보

액세스할 함수에 대한 VPC를 선택합니다.

vpc

(17 / 16)

☐ 이중 스택 서브넷에 IPv6 트래픽 허용

IPv4 및 IPv6 CIDR 블록이 모두 있는 서브넷에 대한 아웃바운드 IPv6 트래픽을 허용할 수 있습니다.

서브넷

VPC 구성을 설정하는 데 사용할 Lambda의 VPC 서브넷을 선택합니다.

서브넷 선택

subnet-

/20

ap-northeast-2a

×

subnet

0/20

ap-northeast-2c

×

subnet

0/20

ap-northeast-2b

×

subnet

0/20

ap-northeast-2d

×

보안 그룹

Lambda가 VPC 구성을 설정하는 데 사용할 VPC 보안 그룹을 선택합니다. 아래 표에서는 선택한 보안 그룹의 인바운드 규칙과 아웃바운드 규칙을 보여줍니다.

보안 그룹 선택

sg-

default

default VPC security group

×

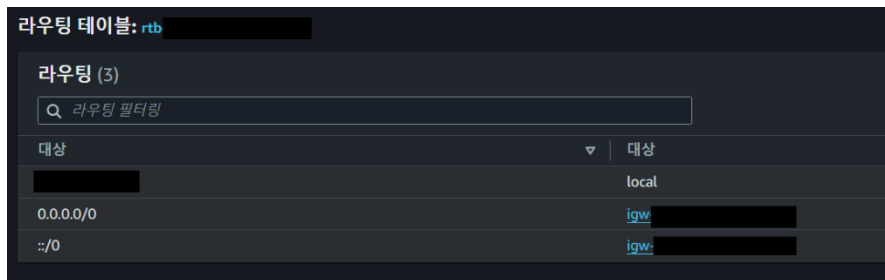
이전에 만들었던 lambda 함수에서 VPC 편집에 접속하여, RDS가 속한 VPC와 보안 그룹으로 설정한다.



VPC 보안 그룹의 인바운드 규칙은 위와 같다. 보안 그룹에 속한 모든 트래픽 및 mysql로 접속하는 나의 IP는 허용하도록 설정하였다.

<https://hossamelshahawi.com/2021/10/24/fix-errno97-address-family-not-supported-by-protocol/>

를 참고하여 vpc에 ipv6 주소를 추가한다.

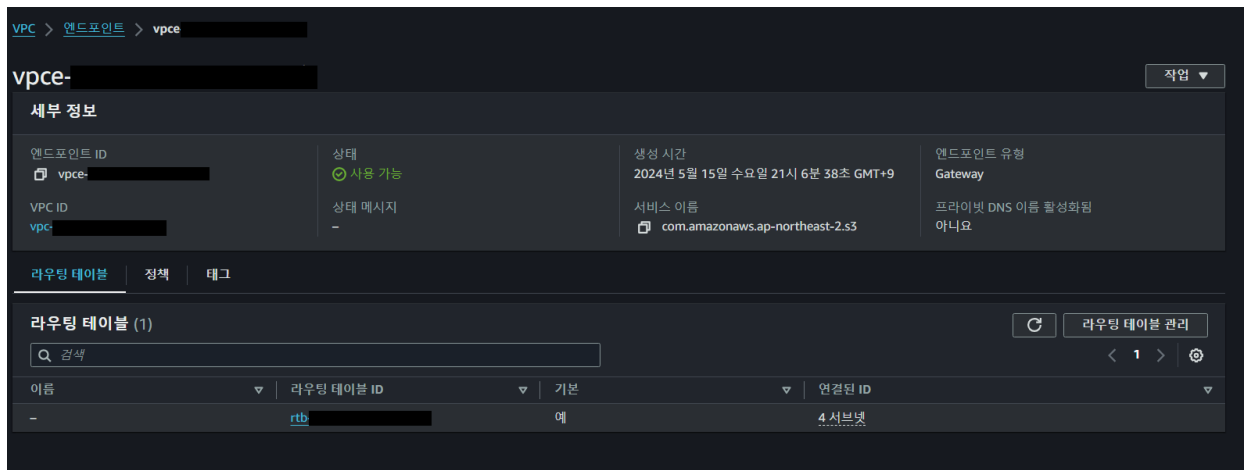


그리고 vpc 라우팅테이블에 ipv6를 인터넷 게이트웨이에 연결한다.

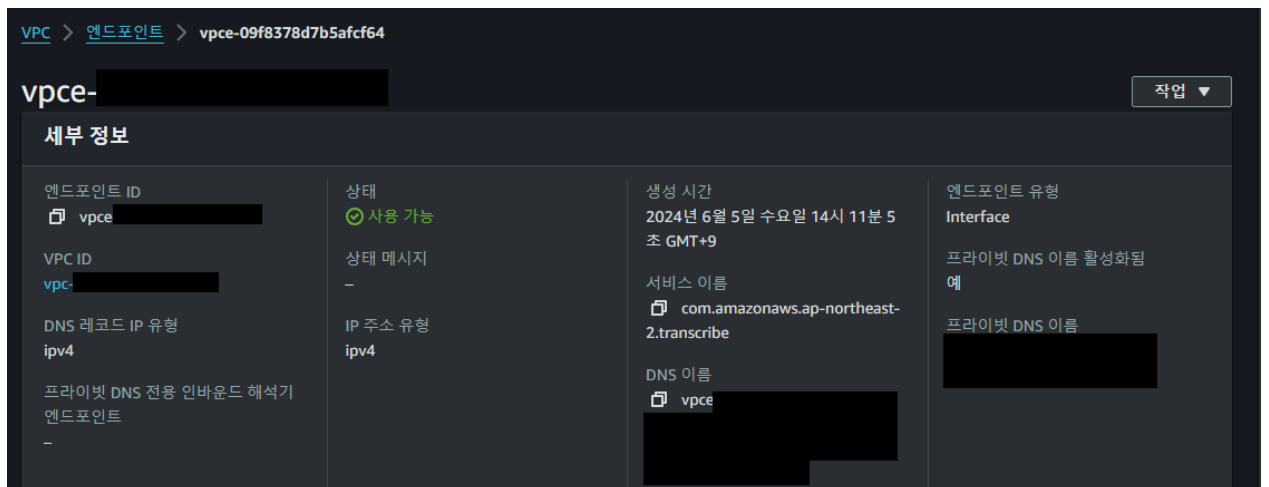
```
MySQL [info] ap-northeast-1 rds.amazonaws.com:3306 ssl [audi... SQL] > create table fileTable(email VARCHAR(320) NOT NULL, filename VARCHAR(600) NOT NULL, language VARCHAR(10) NOT NULL, time TIMESTAMP NOT NULL);
Query OK, 0 rows affected (0.0374 sec)
```

mysql shell을 이용하여 접속하여 database와 테이블을 생성한다. 테이블은 위와 같이 생성하며, 구체적으로는 아래와 같다,

fileTable(email VARCHAR(32) NOT NULL, filename VARCHAR(600) NOT NULL, language VARCHAR(10) NOT NULL, time TIMESTAMP NOT NULL)

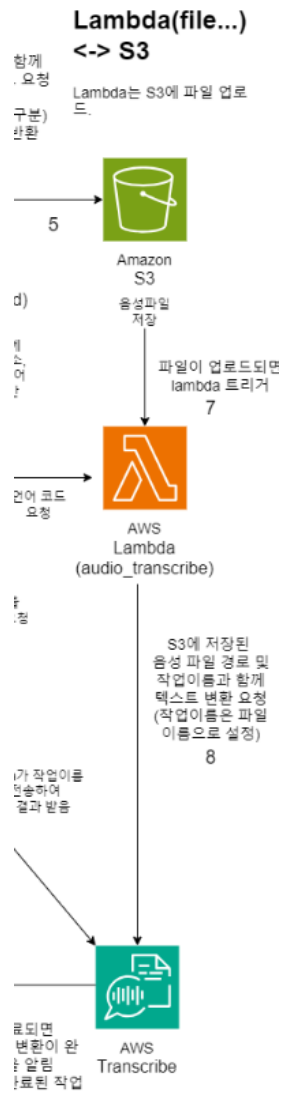


또한 vpc 엔드포인트를 생성하여, vpc에 속한 lambda 함수가 S3에 접속할 수 있도록 한다.



vpc 엔드포인트를 생성하여, vpc에 속한 lambda 함수가 transcribe에 접속할 수 있도록 한다.

5. transcribe 구축



이제 다이어그램에서 S3가 audio_transcribe 람다 함수를 트리거하는 것, 해당 lambda 함수가 AWS Transcribe에 변환 요청하는 것을 구축한다.

(1) IAM 생성

IAM > 역할 > audio_transcribe_role

audio_transcribe_role 정보

Allows Lambda functions to call AWS services on your behalf.

요약

생성 날짜
May 13, 2024, 18:58 (UTC+09:00)

마지막 활동
-

권한 | 신뢰 관계 | 태그 | 액세스 관리자 | 세션 취소

권한 정책 (4) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

검색

필터링 기...

<input type="checkbox"/>	정책 이름	유형
<input type="checkbox"/>	AmazonRDSFullAccess	AWS 관리형
<input type="checkbox"/>	AmazonS3FullAccess	AWS 관리형
<input type="checkbox"/>	AmazonTranscribeFullAccess	AWS 관리형
<input type="checkbox"/>	AWSLambdaVPCLambdaAccessExecutionRole	AWS 관리형

audio_transcribe에 적용할 IAM을 생성한다. 이 람다 함수는 RDS, S3, Transcribe에 FullAccess가 가능해야 하고, VPC에 접근할 수 있도록 한다.

(2) lambda 함수 생성

함수 이름
함수의 용도를 설명하는 이름을 입력합니다.

audio_transcribe

공백 없이 문자, 숫자, 하이픈 또는 밑줄만 사용합니다.

런타임 정보
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Python 3.12

아키텍처 정보
함수 코드에 대해 원하는 명령 세트 아키텍처를 선택합니다.

☒ x86_64

☐ arm64

권한 정보
기본적으로 Lambda는 Amazon CloudWatch Logs에 로그를 업로드하는 권한을 가진 실행 역할을 생성합니다. 이 기본 역할은 나중에...

▼ 기본 실행 역할 변경

실행 역할
함수에 대한 권한을 정의하는 역할을 선택합니다. 사용자 지정 역할을 생성하려면 IAM 콘솔로 이동하십시오.

☐ 기본 Lambda 권한을 가진 새 역할 생성

☒ 기존 역할 사용

☐ AWS 정책 템플릿에서 새 역할 생성

기존 역할
생성한 기존 역할 중에 이 Lambda 함수와 함께 사용할 역할을 선택합니다. 이 역할에는 Amazon CloudWatch Logs에 로그를 업로드할...

audio_transcribe_role

IAM 콘솔에서 audio_transcribe_role 역할을 확인합니다.

위와 같이 audio_transcribe 람다 함수를 python 3.12로 생성한다.

(3) 이벤트 알림 생성

이벤트 알림 생성

정보정보

알림을 활성화하려면 먼저 Amazon S3에서 게시할 이벤트와 Amazon S3에서 알림을 전송할 대상을 식별하는 알림 구성을 추가해야 합니다.

일반 구성

이벤트 이름

fileupload

이벤트 이름은 255자 이내여야 합니다.

접두사 - 선택 사항

지정된 문자로 시작하는 키가 있는 객체로 알림을 제한합니다.

input_audio/

접미사 - 선택 사항

지정된 문자로 끝나는 키가 있는 객체로 알림을 제한합니다.

.mp3

이벤트 유형

알림을 수신할 이벤트를 하나 이상 지정합니다. 각 그룹에 대해 모든 이벤트에 적용되는 이벤트 유형을 선택하거나 하나 이상의 개별 이벤트를 선택할 수 있습니다.

객체 생성

☐ 모든 객체 생성 이벤트

s3:ObjectCreated:*

☒ 전송

s3:ObjectCreated:Put

☐ 게시

s3의 속성에서 이벤트 알림을 생성한다. s3에 input_audio 폴더에 mp3 파일이 put되면 이벤트가 발생하도록 설정한다.

대상

Amazon S3가 대상에 메시지를 게시하려면, 먼저 관련 API를 호출하여 SNS 주제, SQS 대기열 또는 Lambda 함수에 메시지를 게시하는 데 필요한 권한을 Amazon S3 보안 주체에 부여해야 합니다. 자세히 알아보기

대상

이벤트를 게시할 대상을 선택합니다. 자세히 알아보기

☒ Lambda 함수

S3 이벤트를 기반으로 Lambda 함수 스크립트를 실행합니다.

☐ SNS 주제

병렬 처리를 위해 시스템으로 메시지를 팬아웃하거나 사람에게 직접 메시지를 팬아웃합니다.

☐ SQS 대기열

서버에서 읽을 수 있도록 SQS 대기열로 알림을 전송합니다.

Lambda 함수 지정

☒ Lambda 함수에서 선택

☐ Lambda 함수 ARN 입력

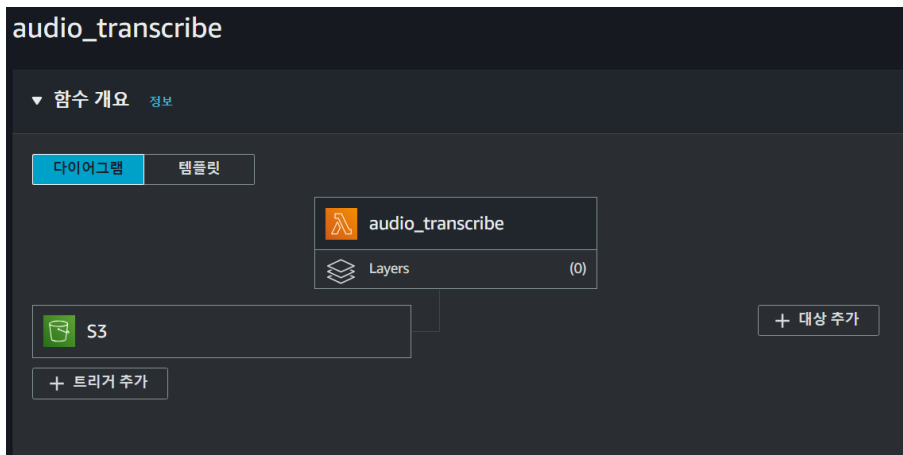
Lambda 함수

audio_transcribe

취소

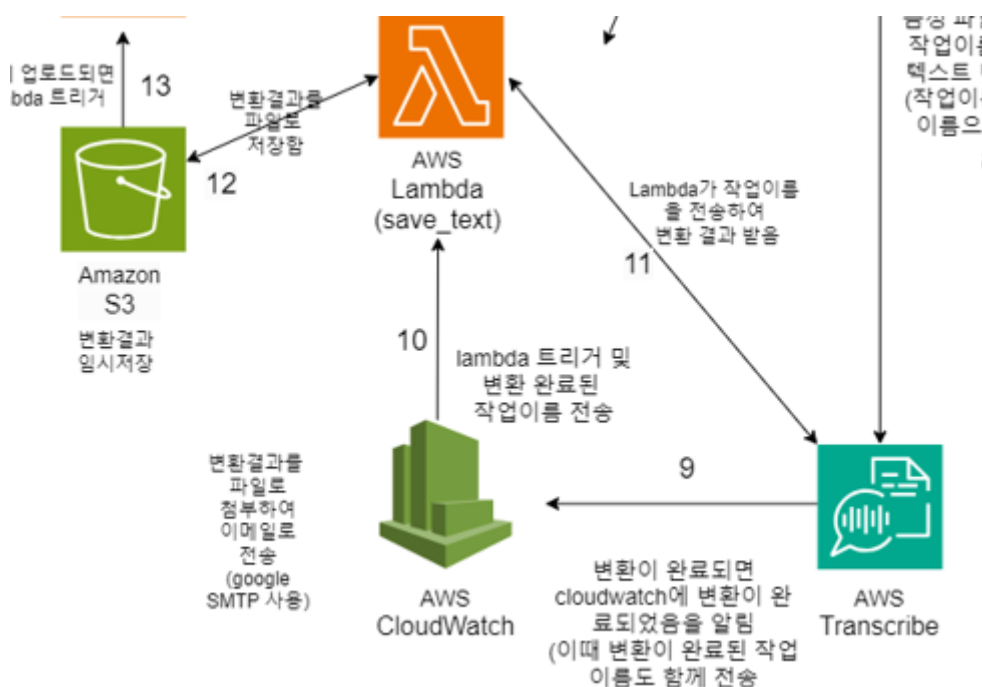
변경 사항 저장

그리고 해당 이벤트는 audio_transcribe를 호출하도록 설정한다.



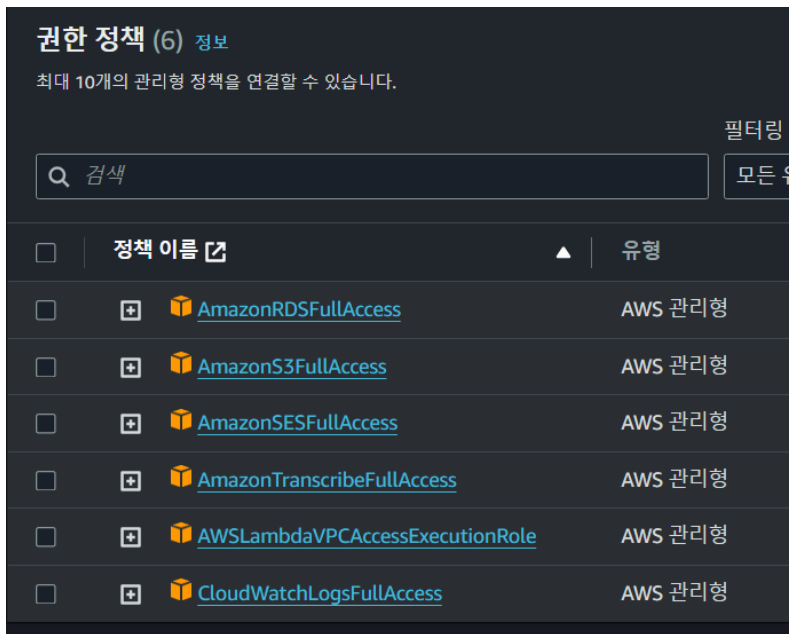
이제 람다 함수에서 위와 같이 S3가 트리거로 설정된 것을 확인할 수 있다.

6. save_text 구축

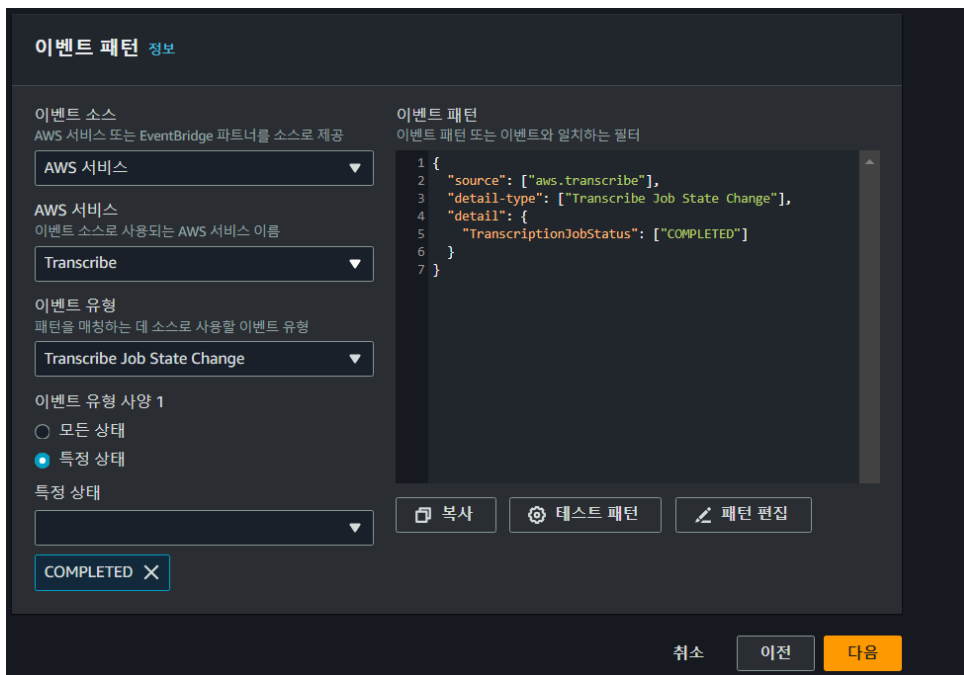


이제 cloudwatch가 AWS Transcribe의 변환 완료 이벤트를 감지해 (eventbridge가) save_text을 호출하는 것을 구축한다.

(1) IAM 생성



send_email 람다 함수에 적용할 IAM을 생성한다 이 IAM은 RDS, Transcribe, VPC, CloudWatchLog에 접근할 수 있어야 한다.



이제 eventbridge에서 어떤 이벤트를 감지할지 이벤트 패턴을 생성한다. 위와 같이 aws.transcribe 서비스의 작업 상태가 완료(COMPLETED)인 것으로 설정한다.

대상 선택



권한

참고: EventBridge 콘솔을 사용할 때, EventBridge는 선택된 대상에 대한 적절한 권한을 자동으로 구성합니다. AWS CLI, SDK 또는 CloudFormation을 사용하는 경우 적절한 권한을 구성해야 합니다.

대상 1개

대상 유형

EventBridge 이벤트 버스, EventBridge API 대상(SaaS 파트너) 또는 다른 AWS 서비스를 대상으로 선택합니다.

- ☐ EventBridge 이벤트 버스
- ☐ EventBridge API 대상
- ☒ AWS 서비스

대상 선택 | 정보

이벤트가 이벤트 패턴과 일치하거나 일정이 트리거될 때 호출할 대상을 선택합니다(규칙당 5개의 대상으로 제한).

Lambda 함수

함수

save_text

▶ 버전/별칭 구성

▶ 추가 설정

다른 대상 추가

취소

검토 및 업데이트단계로 건너뛰기

이전

다음

해당 이벤트 패턴이 발생하면 send_email 람다 함수를 호출하도록 설정한다.

save_text

함수 개요 정보

다이어그램

템플릿



save_text



Layers

(0)



EventBridge(CloudWatch Events)

+ 대상 추가

+ 트리거 추가

코드

테스트

모니터링

구성

별칭

버전

이제 send_email 람다 함수에 EventBridge가 트리거로 설정된 것을 확인할 수 있다.

코드	테스트	모니터링	구성	별칭	버전				
일반 구성			<h3>환경 변수 (1)</h3> <p>아래의 환경 변수는 기본 Lambda 서비스 키를 이용해 저장 중 암호화됩니다.</p> <div> <input type="text" value="환경 변수 찾기"/> </div> <table border="1"> <thead> <tr> <th>키</th> <th>값</th> </tr> </thead> <tbody> <tr> <td>BUCKET_NAME</td> <td></td> </tr> </tbody> </table>			키	값	BUCKET_NAME	
키	값								
BUCKET_NAME									
트리거									
권한									
대상									
함수 URL									
환경 변수									
태그									
VPC									
RDS 데이터베이스									

save_text 람다함수의 환경변수를 설정한다.

7. send_email 구성

(1) 이벤트 알림 생성

s3 버킷에 텍스트 파일이 업로드되면, 이메일을 보내는 send_email 람다 함수를 트리거하는 것을 구현한다.

[Amazon S3](#) > [버킷](#) > [transcribe](#) > 이벤트 알림 생성

이벤트 알림 생성

정보 정보

알림을 활성화하려면 먼저 Amazon S3에서 게시할 이벤트와 Amazon S3에서 알림을 전송할 대상을 식별하는 알림 구성을 추가해야 합니다.

일반 구성

이벤트 이름

이벤트 이름은 255자 이내여야 합니다.

접두사 - 선택 사항

지정된 문자로 시작하는 키가 있는 객체로 알림을 제한합니다.

접미사 - 선택 사항

지정된 문자로 끝나는 키가 있는 객체로 알림을 제한합니다.

이벤트 유형

알림을 수신할 이벤트를 하나 이상 지정합니다. 각 그룹에 대해 모든 이벤트에 적용되는 이벤트 유형을 선택하거나 하나 이상의 개별 이벤트를 선택할 수 있습니다.

객체 생성

☐ 모든 객체 생성 이벤트
s3:ObjectCreated:*

☒ 전송
s3:ObjectCreated:Put

☐ 게시
s3:ObjectCreated:Post

☐ 복사
s3:ObjectCreated:Copy

☐ 멀티파트 업로드 완료
s3:ObjectCreated:CompleteMultipartUpload

8. 결론

AWS 콘솔을 이용하여 다양한 AWS 서비스를 생성하고, 서비스들끼리 연결시켰다. AWS를 이용하여 서비스를 구축하면서, AWS에 생각보다 다양한 기능이 있음을 알게 되었다.

9. 참고 자료

- <https://duckgugong.tistory.com/336>
- <https://heytech.tistory.com/403>
- <https://medium.com/@manishdiddi03/automating-audio-transcription-how-to-use-aws-api-gateway-s3-sns-lambda-and-transcribe-to-20c220b1e77f>
- <https://medium.com/analytics-vidhya/transcribing-audio-files-with-amazon-transcribe-lambda-s3-474dc9a1ced7>
- <https://velog.io/@chaduri7913/AWS-RDS-Lambda-%EC%97%B0%EA%B2%B0%ED%95%98%EA%B8%B0>