

AWS S3 배포

잠깐!

Local

Build

Amazon S3

버킷 생성

파일 업로드

정적 호스팅 설정

정책 설정

Client-Server 연동

Server

Client

잠깐!

- 서버와 클라이언트의 통신은 **HTTP**로 이뤄진다고 가정합니다.
- 따라서 배포된 서버 또한 **HTTPS**를 사용하지 **않아야** 합니다.
- 만약 배포된 서버가 HTTPS라면 **S3**대신 **Netlify**에 배포하는 것을 추천합니다.

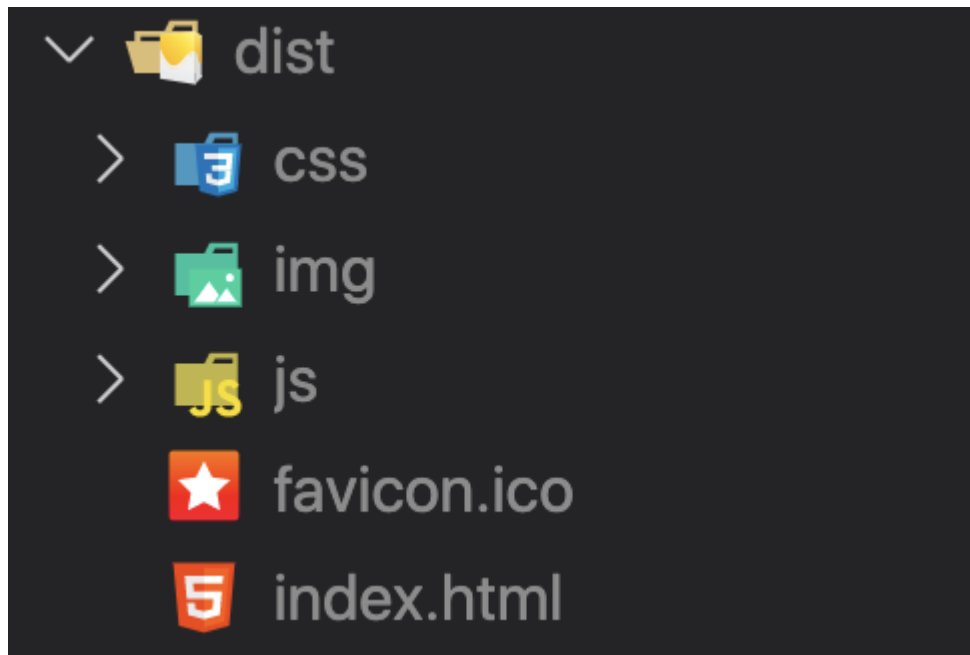
Local

Build

- Vue 프로젝트 경로에서 아래 명령어로 dist 폴더 생성

```
npm run build
```

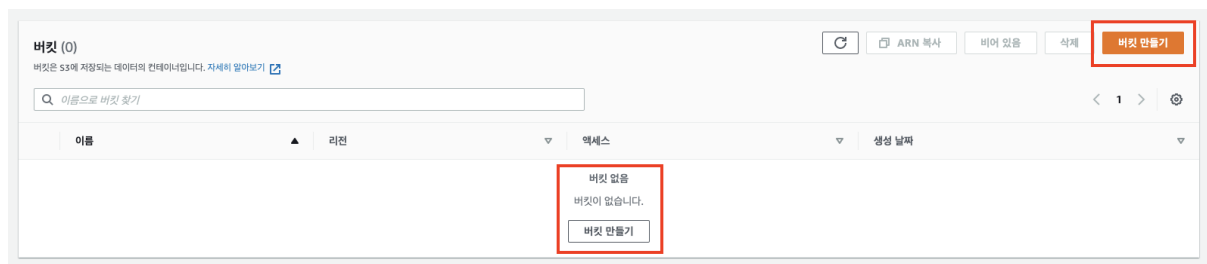
- dist 폴더 생성 확인



Amazon S3

버킷 생성

1. 버킷 만들기 버튼 클릭



2. 버킷 이름 작성 & 리전 선택 (아시아 태평양(서울))

버킷 만들기

버킷은 S3에 저장되는 데이터의 컨테이너입니다. [자세히 알아보기](#)

일반 구성

버킷 이름

ssafy4-final-pjt

버킷 이름은 고유해야 하며 공백 또는 대문자를 포함할 수 없습니다. [버킷 이름 지정 규칙 참조](#)

리전

아시아 태평양(서울) ap-northeast-2

기존 버킷에서 설정 복사 - 선택 사항
다음 구성의 버킷 설정만 복사됩니다.

버킷 선택

3. 퍼블릭 액세스 차단 해제 및 동의 버튼 체크

퍼블릭 액세스 차단을 위한 버킷 설정

퍼블릭 액세스는 ACL(엑세스 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 지정에만 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(엑세스 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(엑세스 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 지정에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.

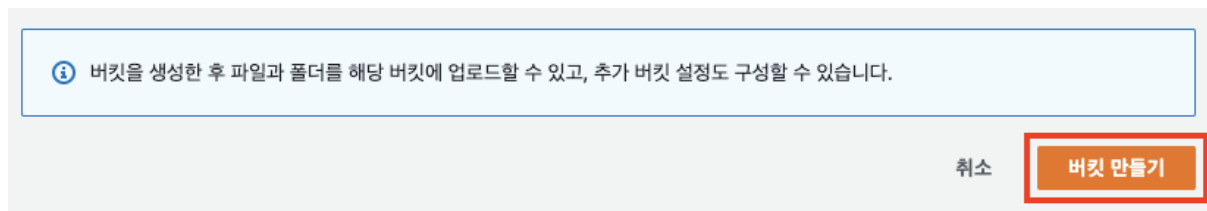


모든 퍼블릭 액세스 차단을 비활성화하면 이 버킷과 그 안에 포함된 객체가 퍼블릭 상태가 될 수 있습니다.

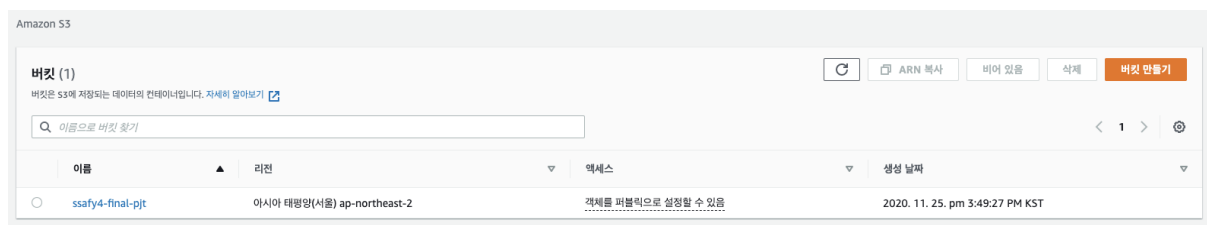
정적 웹 사이트 호스팅과 같은 구체적으로 확인된 사용 사례에서 퍼블릭 액세스가 필요한 경우가 아니면 모든 퍼블릭 액세스 차단을 활성화하는 것이 좋습니다.

☒ 현재 설정으로 인해 이 버킷과 그 안에 포함된 객체가 퍼블릭 상태가 될 수 있음을 알고 있습니다.

4. 밑으로 내려와서 버킷 만들기 클릭

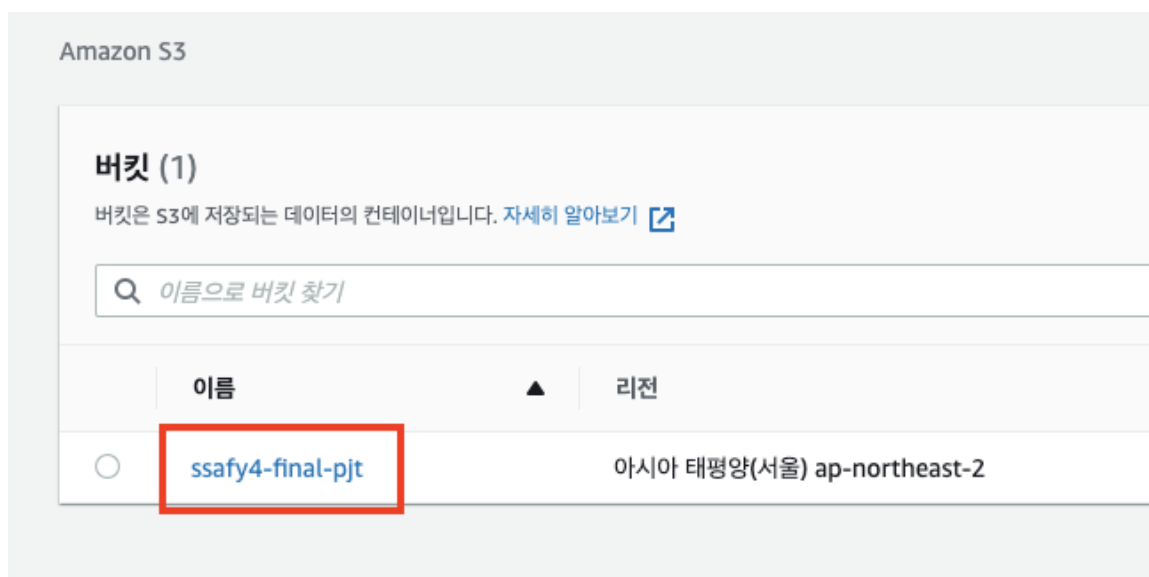


5. 버킷 생성 확인

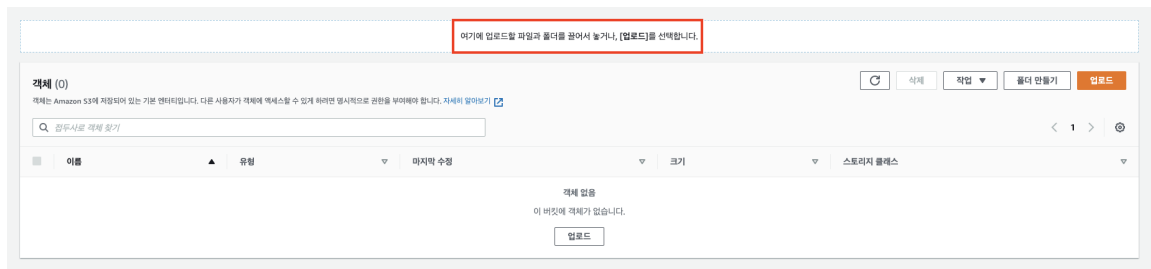


파일 업로드

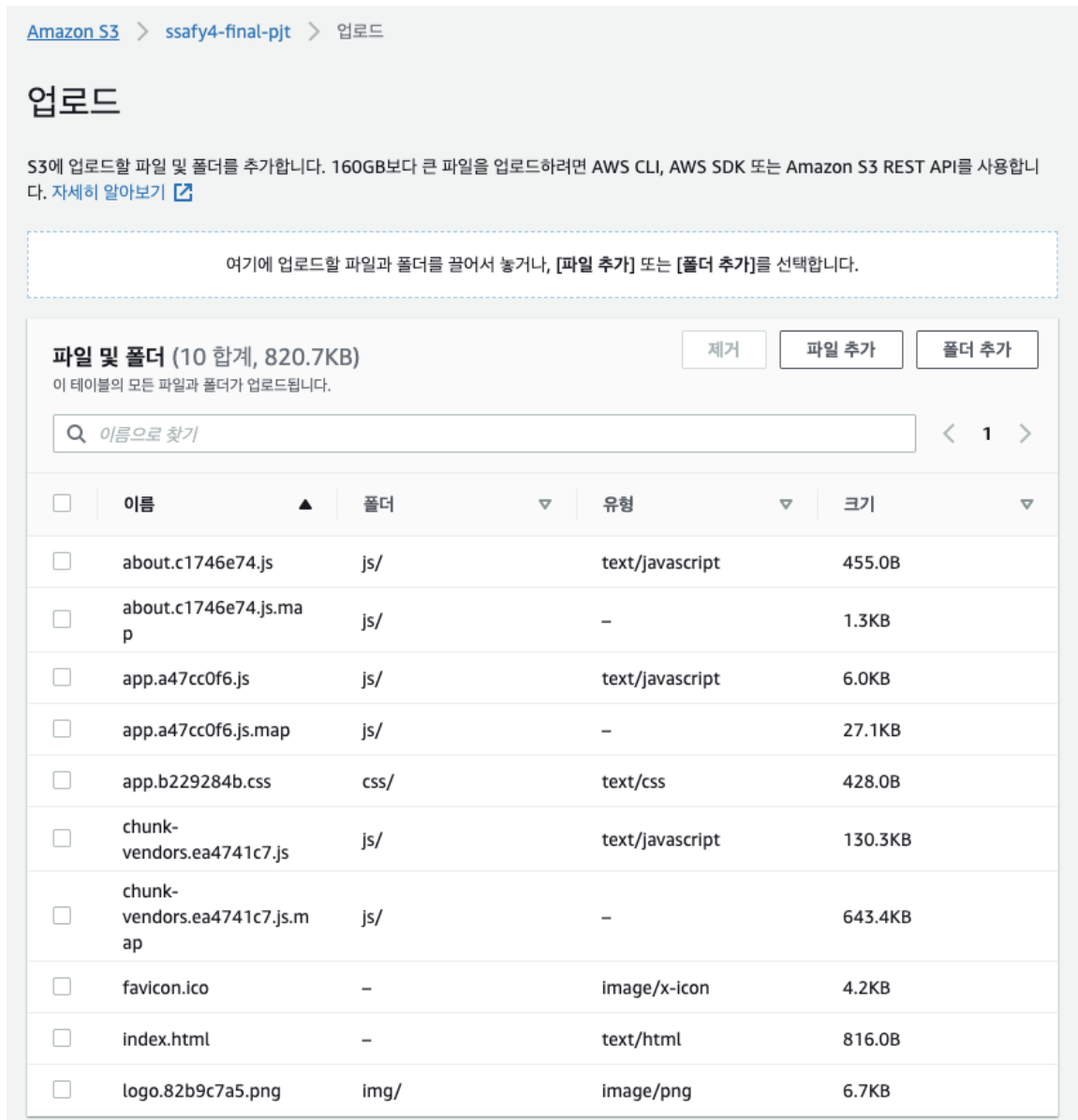
1. 버킷명 클릭



2. dist 폴더 안에 있는 파일 전체 drag & drop으로 업로드



3. 업로드 후 모습

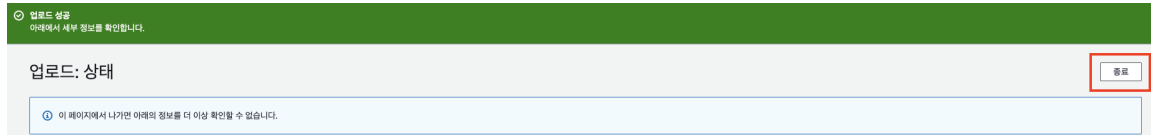


4. 하단 업로드 버튼 클릭

취소

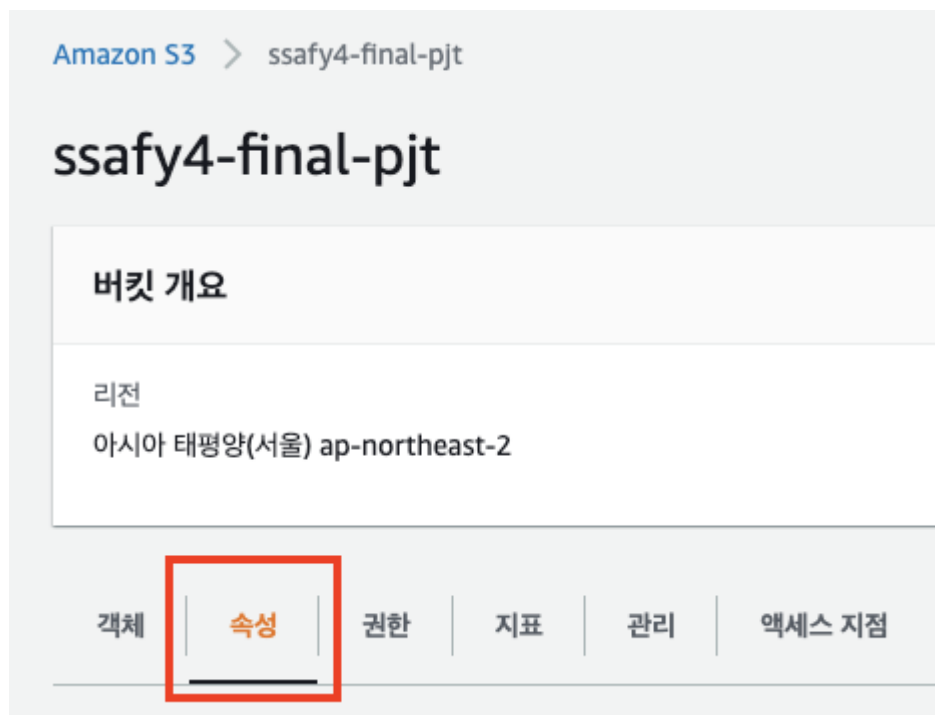
업로드

5. 업로드 성공 확인 후 우측 종료 버튼 클릭

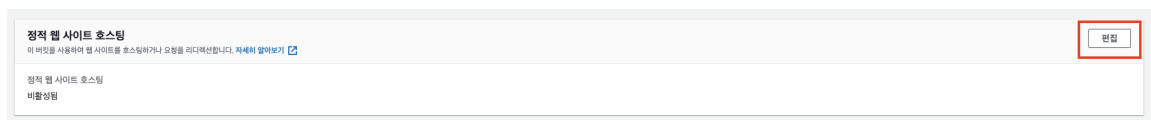


정적 호스팅 설정

1. 속성 탭 클릭



2. 최하단 정적 웹 사이트 호스팅 섹션에서 편집 클릭



3. 활성화 클릭 및 인덱스와 오류 문서에 아래와 같이 기입 (index.html)

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](#)

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.

index.html

오류 문서

오류가 발생하면 반환됩니다.

index.html

4. 변경 사항 저장 클릭

5. 정적 웹 사이트 호스팅 섹션 변경 확인

- 버킷 웹 사이트 엔드포인트 확인 (== Vue 접속 주소)

정적 웹 사이트 호스팅

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

정적 웹 사이트 호스팅

활성화됨

호스팅 유형

버킷 호스팅

버킷 웹 사이트 엔드포인트

버킷을 정적 웹 사이트로 구성하면, 해당 웹 사이트를 버킷의 AWS 리전별 웹 사이트 엔드포인트에서 사용할 수 있습니다. [자세히 알아보기](#)

<http://ssafy4-final-pjt.s3-website.ap-northeast-2.amazonaws.com>

6. 엔드포인트로 접속 후 403 에러 확인

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 4B6DEE72BE1D6C0E
- HostId: 69zYj+HEn2pbjHV43K96YJaojcIV9ytKR0hAZDx6EuCmJFTzVLsim80a2XbKBSmzVg70FTWSHls=


An Error Occurred While Attempting to Retrieve a Custom Error Document

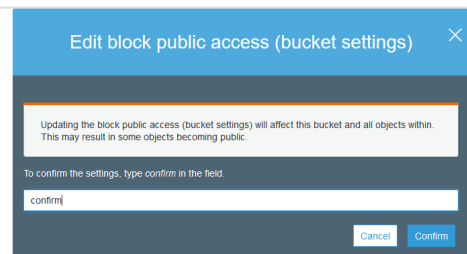
- Code: AccessDenied
- Message: Access Denied

정책 설정

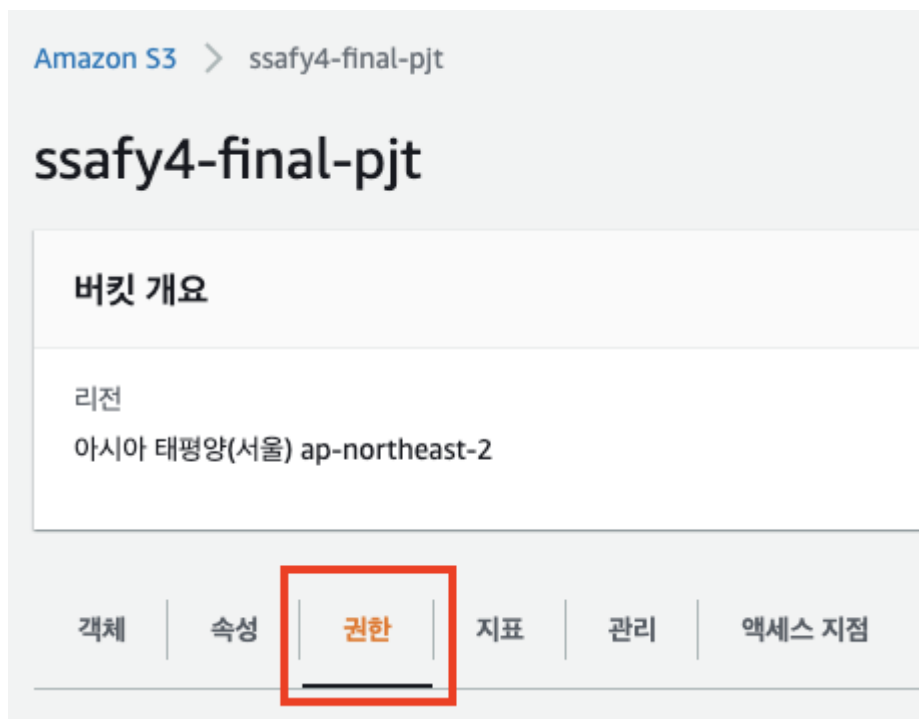
웹 사이트 액세스에 대한 권한 설정

버킷을 정적 웹 사이트로 구성할 때, 웹 사이트를 퍼블릭으로 설정하려면 퍼블릭 읽기 액세스 권한을 부여할 수 있습니다. 버킷을 공개적으로 읽기 가능하게 만들려면 버킷에 대해 퍼블릭 액세스 차단 설정을 비활

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



1. 권한 탭 클릭

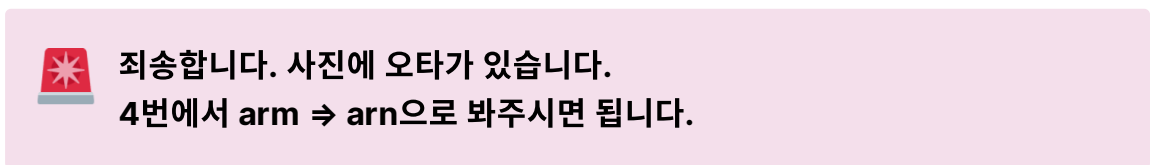


2. 권한 섹션 내 버킷 정책탭에서 편집 버튼 클릭

3. 정책 생성기 버튼 클릭



4. 아래 사진의 내용을 참고하여 편집 후 Add Statement 클릭



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) pr policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), [Queue Policy](#).

Select Type of Policy S3 Bucket Policy **1. S3 Bucket Policy 선택**

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal **2. Asterisk(*) 설정**
Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services (*)
Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected **3. GetObject 선택** Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::ssafy4-fin **4. arm:aws:s3:::버킷이름/***
ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>. Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

5. 내용 확인 후 Generate Policy 클릭

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:GetObject	arn:aws:s3:::ssafy4-final-pjt/*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

6. 모달 창 내부 JSON 내용 복사 후 창 닫기

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.

```
{
  "Id": "Policy1606288654187",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1606288619975",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::ssafy4-final-pjt/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services

Close

7. 버킷 정책 편집 창으로 돌아와서 복사한 내용 붙여넣기 후 변경사항 저장

버킷 정책 편집

버킷 정책

JSON으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다. [자세히 알아보기](#)

정책 예제

정책 생성기

버킷 ARN

arn:aws:s3:::ssafy4-final-pjt

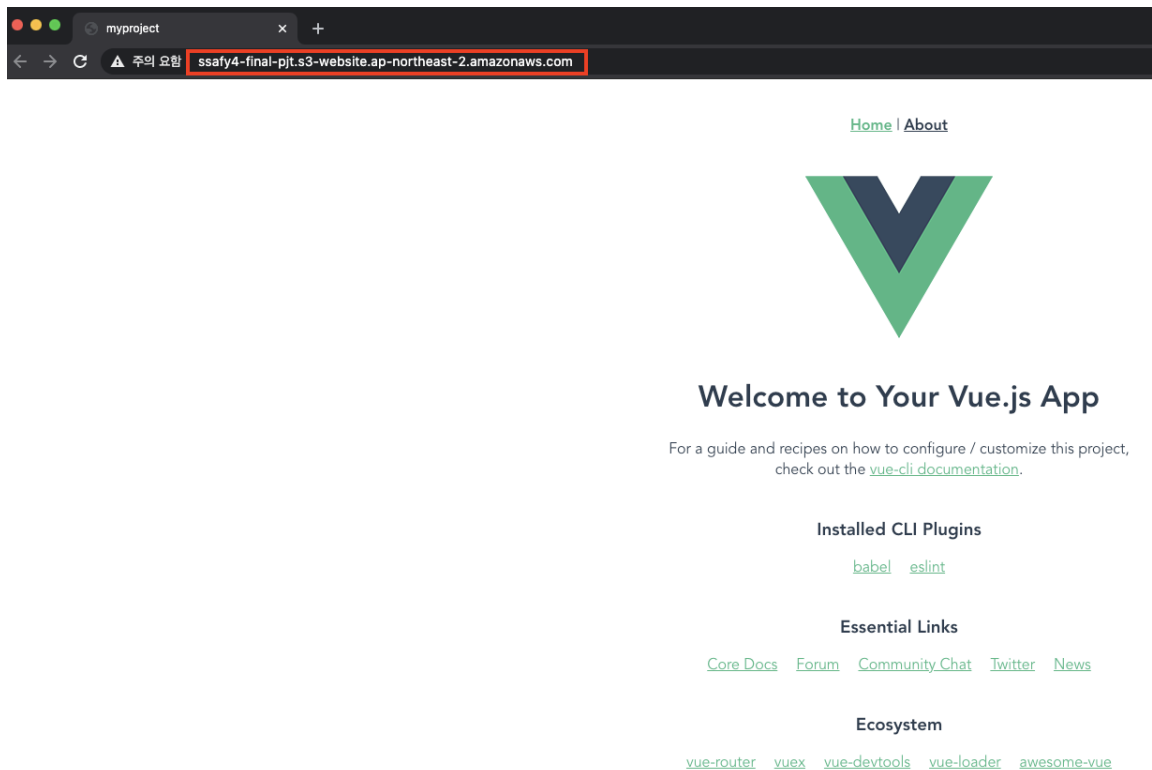
정책

```
1 {  
2   "Id": "Policy1606288654187",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmt1606288619975",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::ssafy4-final-pjt/*",  
12      "Principal": "*"   
13    }  
14  ]  
15 }
```

취소

변경 사항 저장

8. 브라우저에서 위의 **버킷 엔드포인트 주소**로 접속 후 정상 배포 확인



Client-Server 연동

Server

- CORS whitelist 추가

```
CORS_ALLOWED_ORIGINS = [  
    "S3 버킷 엔드포인트 주소",  
]
```

Client

- API 요청 주소 수정

(아래 코드는 예시입니다. 각 프로젝트의 상황에 맞게 바꿔주시면 됩니다.)

```
const BASE_URL = 'http://배포된_서버_도메인_또는_PUBLIC_IP'  
axios.get(`${BASE_URL}/api/movies/`)  
  .then(...)  
  .catch(...)
```

