

# AWS Cloudfront 배포

## AWS

아마존에서 서비스하는 클라우드 컴퓨팅 사이트

- 데이터를 보관하고 서비스에 필요한 가상의 IT 기술들을 대여해주는 곳(웹 서버 등)

## 1. 회원가입

### 1. AWS 회원가입

- a. <https://aws.amazon.com/ko/> - 해외결제 가능한 카드 필요

### 2. 가비아 회원가입

- a. <https://www.gabia.com/>

## 2. 가비아 도메인 구입

- [주소](#)

### 1. 원하는 도메인 검색 후 구입 (1년이 최저가)

gabia.도메인호스팅홈페이지커머스클라우드IDC보안메일/그룹웨어

김요진 님로그아웃My가비아고객센터

www.openwebsevice여러개 검색Q 검색⚙

이미 등록된 도메인입니다. openwebsevice.com

도메인 소유자가 \$1,488로 판매를 희망합니다.  
꼭 필요한 도메인이라면 구매대행을 이용해 보세요.

추천 도메인이벤트 도메인KOR 도메인국가 도메인브랜드 도메인

☒ 등록 가능

openwebsevice.co.kr 대한민국	EVENT 15,000원 / 21,000원	선택
openwebsevice.kr 대한민국	EVENT 15,000원 / 21,000원	선택
openwebsevice.shop	EVENT 500원 / 49,000원	선택
openwebsevice.store	EVENT 500원 / 77,000원	선택
openwebsevice.net	24,000원	선택
openwebsevice.site	EVENT 1,900원 / 49,000원	선택
openwebsevice.org	22,000원	선택
openwebsevice.me 몬테네그로	EVENT 7,000원 / 29,000원	선택
openwebsevice.한국 대한민국	21,000원	선택
openwebsevice.io 영국령 인도양 지역	100,000원	선택
openwebsevice.biz	25,000원	선택

도메인 장바구니

1개 등록 선택 X

openwebsevice.store X

신청하기

견적서 출력

## 서비스 신청



결제가 성공적으로 완료되었습니다.

결제 정보		계좌번호 SMS 발송	
주문번호	REG20230921-5519470		
입금할 금액	950원 (VAT 포함)	해금주	㈜ 가비아
입금 은행	NH농협	입금 계좌	79004961105971
입금 기한	2023.10.06까지 입금하지 않으면 자동 취소됩니다.		
<div><ul style="list-style-type: none"><li>* 해당 계좌번호는 가상계좌번호로 입금자명에 상관없이 실시간으로 입금확인 되어 자동으로 등록 처리됩니다.</li><li>* 타인이 먼저 도메인을 등록/결제 할 경우 입금 기한에 상관없이 등록이 불가능할 수 있으나 빠른 입금 부탁드립니다.</li><li>* 입금 확인은 입금 후 10~15분 정도 소요될 수 있습니다.</li><li>* 입금하심 계좌의 예금주는 '서울반크', KCP(한국사이버결제) 또는 '에이비이' 등으로 표시될 수 있습니다. 정확한 금액을 입금해주시면, 모두 정상적으로 결제가 완료됩니다.</li></ul></div>			

신청 정보	
도메인 등록	openwebsservice.store/1년
* 일부 TLD의 경우 결제 완료 이후에도 등록 또는 만기일 연장이 실시간으로 진행되지 않을 수 있습니다.	

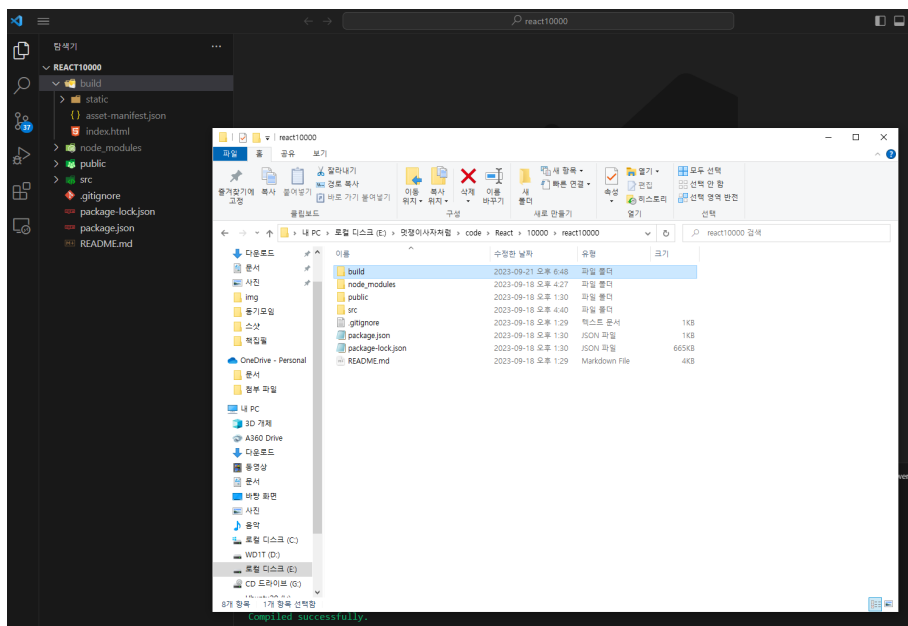
관리 정보			
소유자 정보			
소유자명(한글/영문)	김모건(MORGAN KIM)	이메일	jasinis102@gmail.com
전화번호	*82-1053165049	휴대전화	010-5316-9249
관리자 정보			
관리자명(한글/영문)	김모건(MORGAN KIM)	이메일	jasinis102@gmail.com
전화번호	*82-1053165049	휴대전화	010-5316-9249
내입 서버	ns.gabia.co.kr 43.201.170.100 ns1.gabia.co.kr 203.200.205.240 ns.gabia.net 121.78.117.39		

My 가비아 신청 내역 출력

## 3. S3 배포

- AWS에서 제공하는 데이터 저장소 [주소](#)

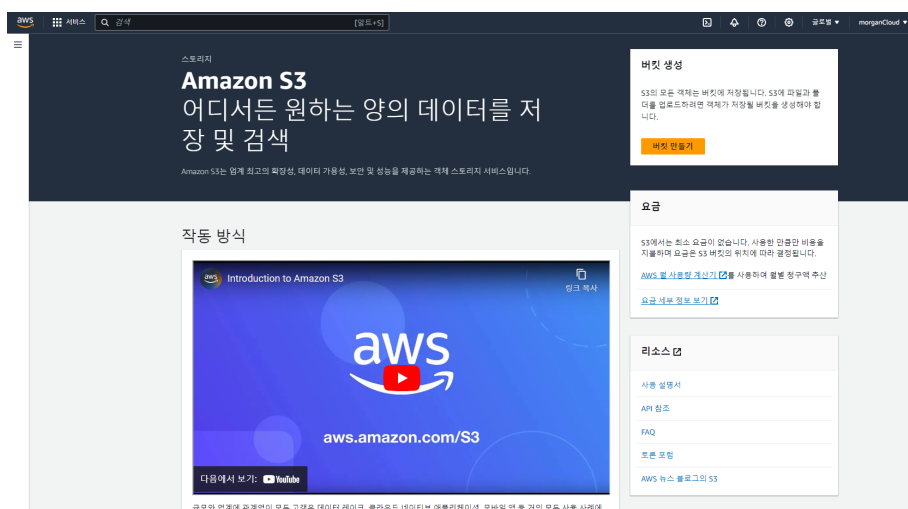
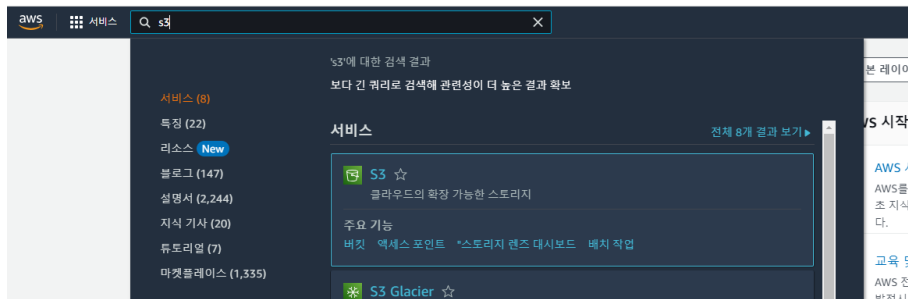
### 1. react project -> npm build



## 2. AWS S3 -> 버킷 만들기 -> 버킷 이름 마음대로 설정 ->

모든 퍼블릭 액세스 차단 해제 (S3 버킷에 접근을 허용) ->

[ 현재 설정으로 인해 이 버킷과 그 안에 포함된 객체가 퍼블릭 상태가 될 수 있음을 알고 있습니다.] 체크 [v]



### 이 버킷의 퍼블릭 액세스 차단 설정

퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지점 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 객체에 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 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지점 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 정책을 변경하지 않습니다.

##### ☐ 임의의 퍼블릭 버킷 또는 액세스 지점 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.



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.

## 3. build 폴더안에 있는 파일 업로드

aws

서비스

검색

[알트+S]

Amazon S3 > 버킷 > morganbuckettest > 업로드

업로드 정보

S3에 업로드할 파일 및 폴더를 추가합니다. 160GB보다 큰 파일을 업로드하려면 AWS CLI, AWS SDK 또는 Amazon S3 REST API를 사용합니다. [자세히 알아보기](#)

여기에 업로드할 파일과 폴더를 끌어서 놓거나, 파일 추가 또는 폴더 추가를 선택합니다.

파일 및 폴더 (9 합계, 580.1KB)

제거

파일 추가

폴더 추가

이 테이블의 모든 파일과 폴더가 업로드됩니다.

이름으로 찾기

< 1 >

<input type="checkbox"/>	이름	폴더	유형	크기
<input type="checkbox"/>	asset-manifest.json	-	application/json	531.0B
<input type="checkbox"/>	index.html	-	text/html	325.0B
<input type="checkbox"/>	main.64ce4ec7.css	static/css/	text/css	7.5KB
<input type="checkbox"/>	main.64ce4ec7.css....	static/css/	-	8.1KB
<input type="checkbox"/>	main.8cf5896b.js	static/js/	text/javascript	167.4KB
<input type="checkbox"/>	main.8cf5896b.js.LI...	static/js/	text/plain	971.0B
<input type="checkbox"/>	main.8cf5896b.js.map	static/js/	-	358.3KB
<input type="checkbox"/>	licat.b32a67e86adb...	static/media/	image/png	25.6KB
<input type="checkbox"/>	title_bg.aa3294909e...	static/media/	image/png	11.5KB

대상

대상

s3://morganbuckettest

▶ 대상 세부 정보

지정된 대상에 저장된 새 객체에 영향을 미치는 버킷 설정.

▶ 권한

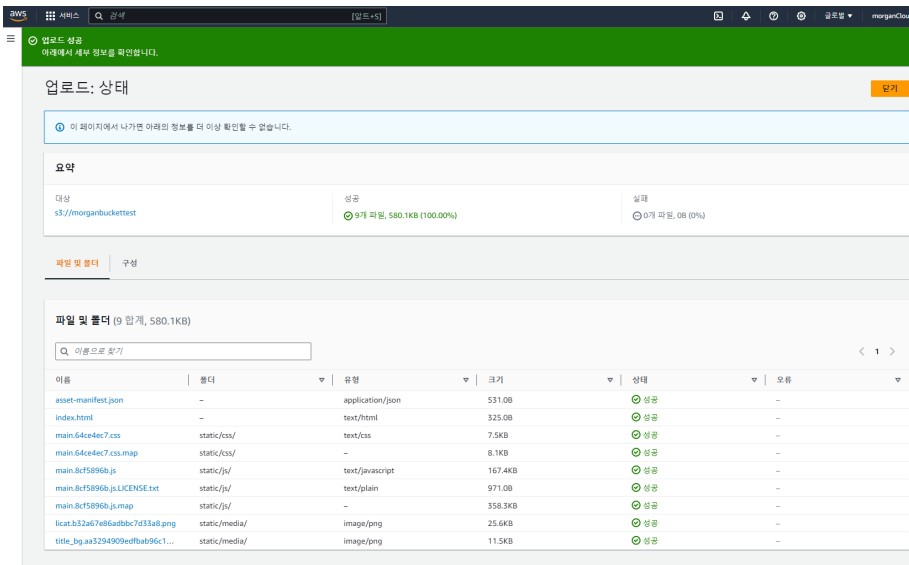
다른 AWS 계정에 퍼블릭 액세스 및 액세스 권한을 부여합니다.

▶ 속성

스토리지 클래스, 암호화 설정, 태그 등을 지정합니다.

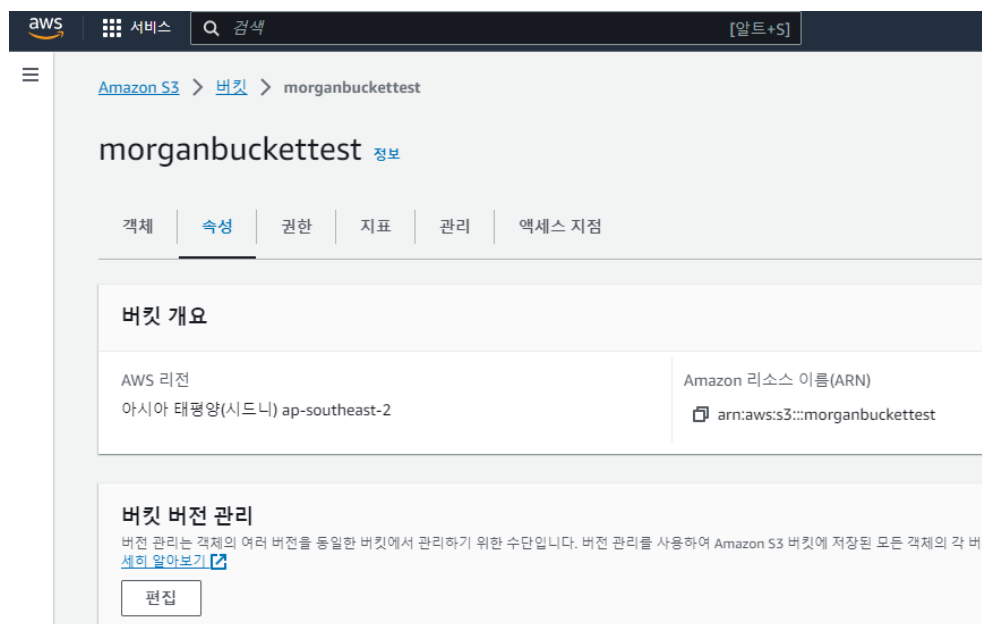
취소

업로드



#### 4. 속성 -> 정적 웹사이트 호스팅 -> 편집 -> 활성화 ->

웹사이트의 기본 페이지 index.html, 오류 시 나타날 페이지 index.html



#### 정적 웹 사이트 호스팅

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

편집

정적 웹 사이트 호스팅

비활성됨

aws

서비스

검색

[알트+S]

aws

Amazon S3 > 버킷 > morganbuckettest > 정적 웹 사이트 호스팅 편집

정적 웹 사이트 호스팅 편집

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 - 선택 사항

오류가 발생하면 반환됩니다.

index.html

리디렉션 규칙 - 선택 사항

JSON으로 작성된 리디렉션 규칙은 특정 콘텐츠에 대한 웹 페이지 요청을 자동으로 리디렉션합니다. 자세히 알아보기

aws

서비스

검색

[알트+S]

aws

정적 웹 사이트 호스팅을 편집했습니다.

Amazon S3 > 버킷 > morganbuckettest

morganbuckettest

객체 | **속성** | 권한 | 지표 | 관리 | 액세스 지점

버킷 개요

AWS 리전

아시아 태평양(시드니) ap-southeast-2

Amazon 리소스 이름(ARN)

am:aws:s3::morganbuckettest

생성 날짜

2023. 9. 21. pm 7:03:40 PM KST

정적 웹 사이트 호스팅

이 버킷을 사용하여 웹 사이트를 호스팅하거나 요청을 리디렉션합니다. 자세히 알아보기

정적 웹 사이트 호스팅

활성화된

호스팅 유형

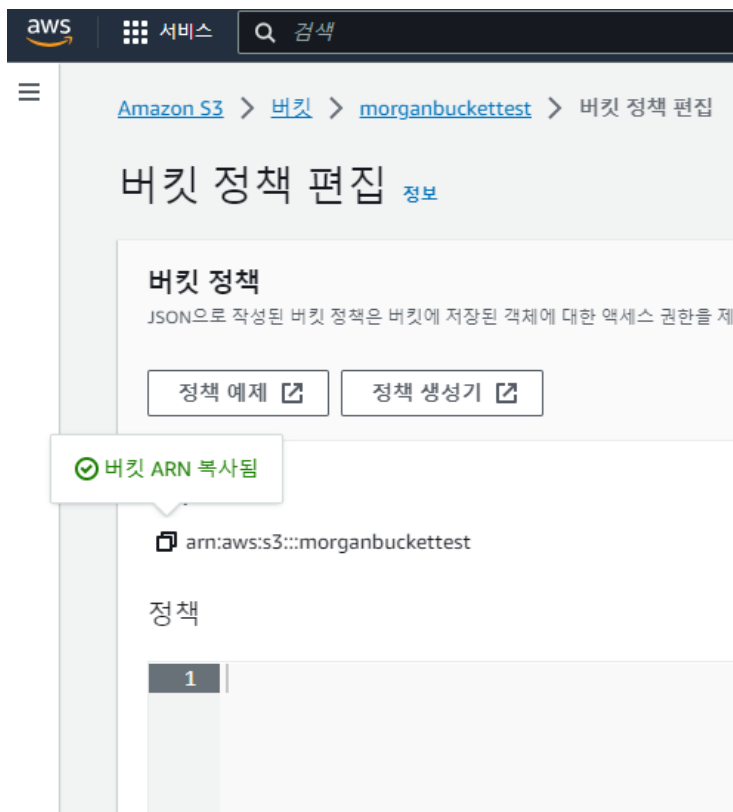
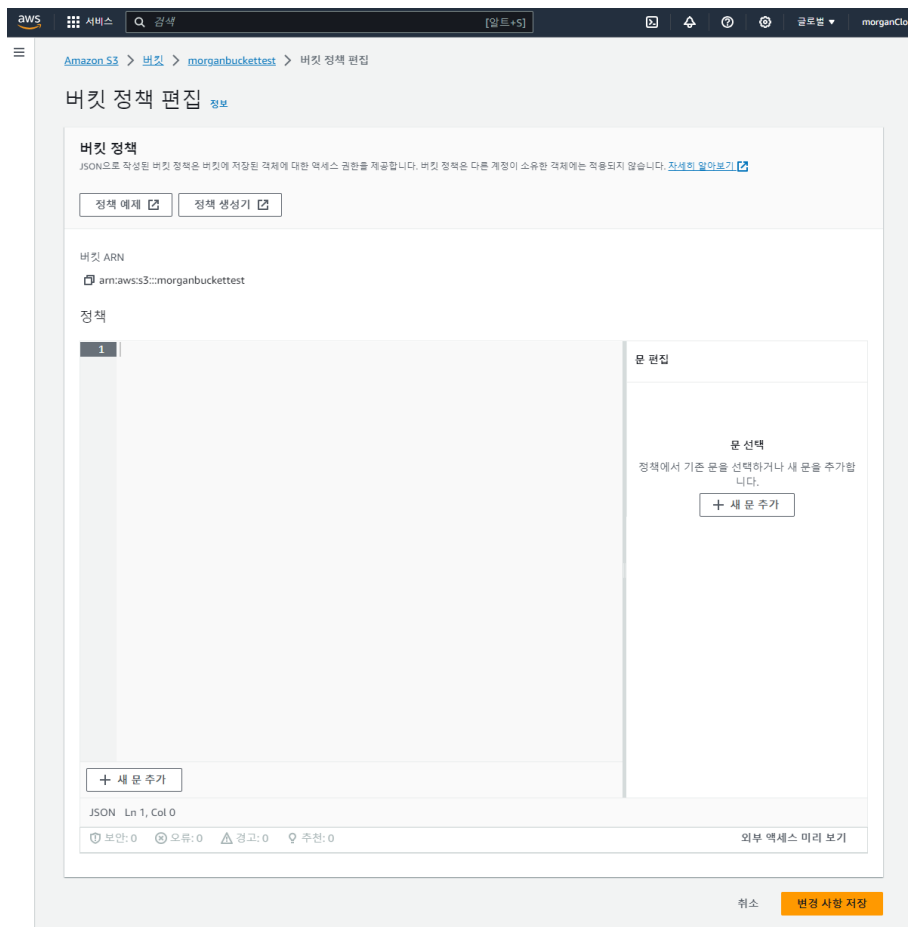
버킷 호스팅

버킷 웹 사이트 엔드포인트

버킷을 정적 웹 사이트로 구성하면, 해당 웹 사이트를 버킷의 AWS 리전별 웹 사이트 엔드포인트에서 사용할 수 있습니다. 자세히 알아보기

http://morganbuckettest.s3-website-ap-southeast-2.amazonaws.com

## 5. 권한 -> 버킷 정책 편집 -> 버킷 ARN 복사 -> 정책 생성기



- Step 1: Select Type of Policy = S3 Bucket Policy 선택  
( S3에 대한 접근 권한을 주기 위한 설정 )
- Effect -> Allow (허용) 클릭
- Principal -> \* 입력 ( 아무나 접근 가능 )
- Actions -> GetObject ( 버킷에 업로드된 파일을 읽을 수 있다. )



## AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating 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, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

### 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

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 ☐ All Actions ("\*")

Amazon Resource Name (ARN)

☐ GetMultiRegionAccessPointPolicyStatus  
☐ GetMultiRegionAccessPointRoutes  
☒ GetObject  
☐ GetObjectAcl  
☐ GetObjectAttributes  
☐ GetObjectLegalHold  
☐ GetObjectRetention  
☐ GetObjectTorrent

[BucketName]/\${KeyName}.

**Warning:** You must enter a valid ARN.

### 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.

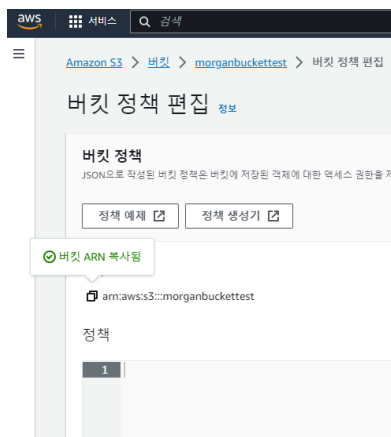
**Add one or more statements above to generate a policy.**

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 technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An **amazon.com** company

## 10. Amazon Resource Name (ARN) -> 버킷ARN/\* ( 모든 파일에 대해 읽기 가능 )



### 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

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 ☐ All Actions ("\*")

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.

Use a comma to separate multiple values.

Add Conditions (Optional)

**Add Statement**



## 11. Generate Policy 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) products and resources. For more information about creating 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, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

#### 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

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 -- Select Actions -- ☐ All Actions (\*\*)

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{Keyname}`.  
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

[Add Statement](#)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
<ul style="list-style-type: none"><li>*</li></ul>	Allow	<ul style="list-style-type: none"><li>s3:GetObject</li></ul>	<code>arn:aws:s3:::morganbuckettest/*</code>	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](#)

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 technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An [amazon.com](#) company

## 12. JSON 데이터 복사 -> 버킷 정책 편집에 내용 붙여넣기 -> 변경 사항 저장

The screenshot shows the AWS Policy Generator interface with a modal window titled "Policy JSON Document" open. The modal contains the following JSON policy document:

```
{
  "Id": "Policy169291036166",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt169291036166",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::morganbuckettest/*",
      "Principal": "*"
    }
  ]
}
```

The modal also includes instructions: "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." and a "Close" button.

서비스

검색

알림

5

AWS

로그인

로그아웃

Amazon S3

버킷

morganbuckettest

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

am:aws:s3::morganbuckettest

정책

1

{

2

"id": "Policy1695291852358",

3

"Version": "2012-10-17",

4

"Statement": [

5

{

6

"Sid": "Stmt1695291836166",

7

"Action": [

8

"s3:GetObject"

9

],

10

"Effect": "Allow",

11

"Resource": "arn:aws:s3::morganbuckettest/\*",

12

"Principal": "\*"

13

}

14

]

15

}

문 편집

문 선택

정책에서 기존 문을 선택하거나 새 문을 추가합니다.

+ 새 문 추가

+ 새 문 추가

JSON

Ln 15, Col 1

보안: 0

오류: 0

경고: 0

주해: 0

외부 액세스 미리 보기

취소

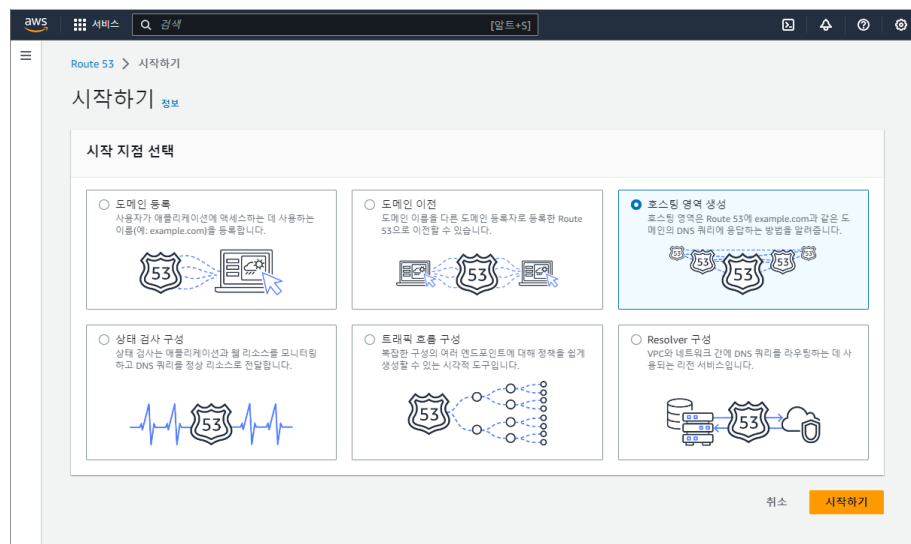
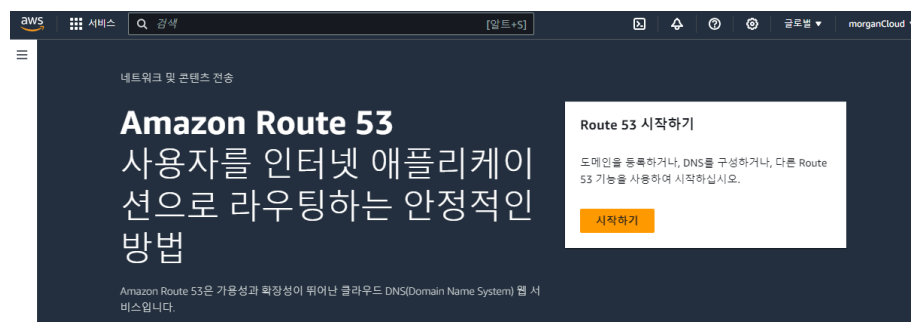
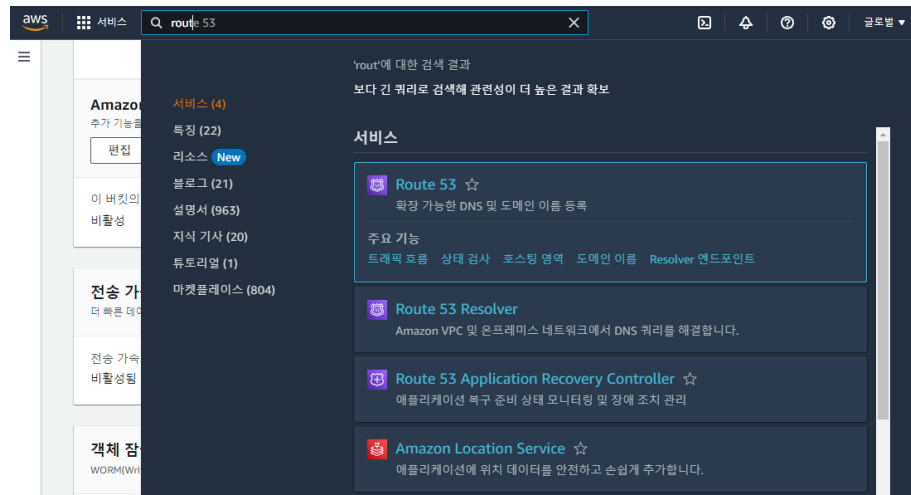
변경 사항 저장

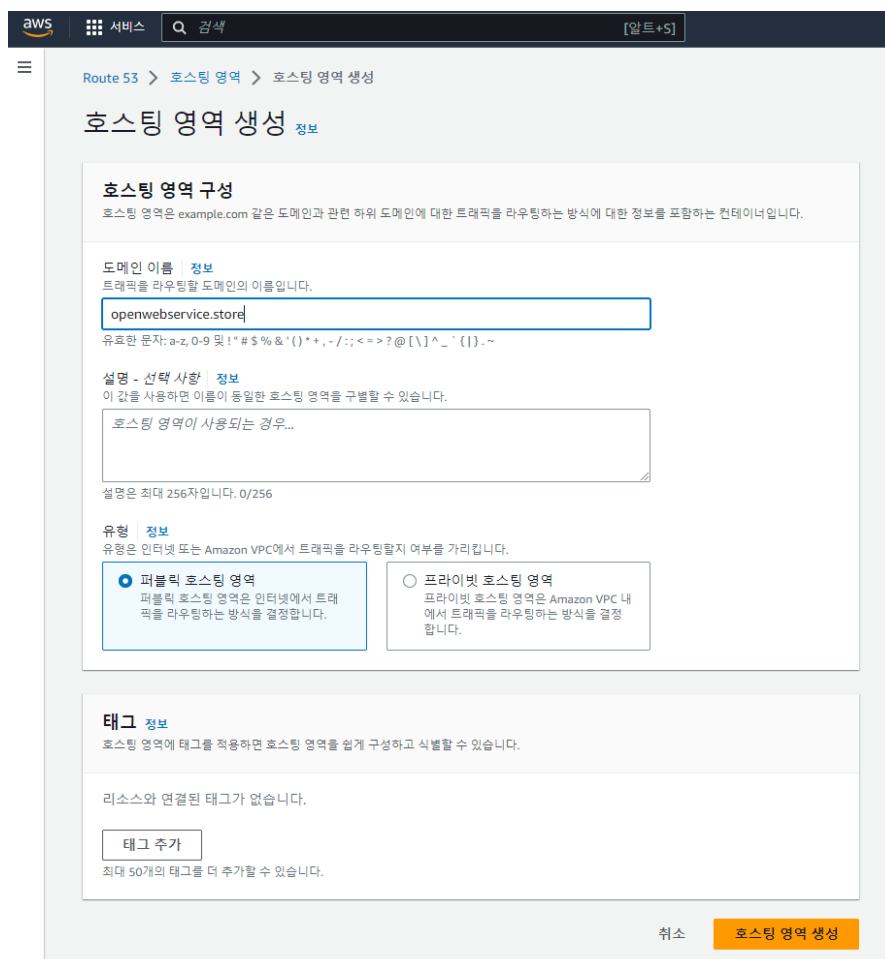
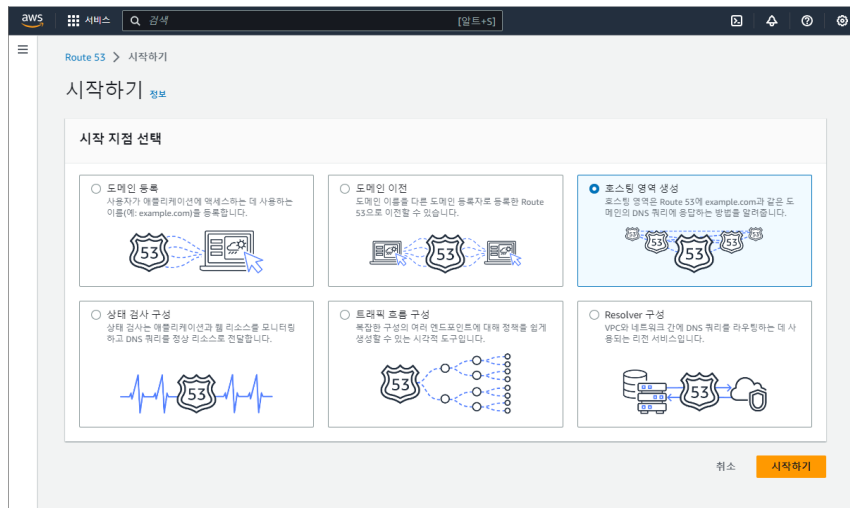
## 4. AWS Route 53 도메인 연결

- 도메인을 등록하고 리소스에 연결하여서 사용하기 위한 서비스
- [주소](#)

1. 시작하기 -> 대시보드 -> 호스팅 영역 생성 ->

도메인 이름 : 구입한 도메인 이름 -> 호스팅 영역 생성





2. 네임서버 4개를 가비아와 연결 (값/트래픽 라우팅 대상) ->
3. <https://www.gabia.com/> 가비아 이동 -> My가비아 -> 이용중인 서비스 -> 도메인 -> (구입한 도메인) 관리 -> 네임서버 설정 -> Route 53 호스팅 영역을 통해 생성한 네임서버 4개 입력 (끝에 점 한 개 빼고 넣기)

네임서버 = [www.naver.com](http://www.naver.com) 도메인 주소로 접속했을 시 실제 고유 IP주소로 변환해주는 역할

Route 53

대시보드

호스팅 영역

상태 검사

▼ IP 기반 라우팅

CIDR 모음

▼ 트래픽 흐름

트래픽 정책

정책 레코드

▼ 도메인

등록된 도메인

요청

▼ 확인자

VPC

인바운드 엔드포인트

아웃바운드 엔드포인트

규칙

쿼리 로깅

Outposts

DNS 방화벽

애플리케이션 복구 컨트롤러

이전 콘솔로 전환

openwebservice.store이(가) 생성되었습니다.

이제 호스팅 영역에 레코드를 생성하여 Route 53에서 도메인에 대한 트래픽을 라우팅하는 방법을 지정할 수 있습니다.

Route 53 > 호스팅 영역 > openwebservice.store

패널 openwebservice.store 정보

영역 삭제 레코드 테스트 쿼리 로깅 구성

호스팅 영역 세부 정보

호스팅 영역 편집

레코드(2) DNSSEC 서명 호스팅 영역 태그(0)

레코드 (2) 정보

Automatic 모드는 최상의 플리 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

레코드 삭제 영역 파악 가져오기 레코드 생성

속성 또는 값을 기준으로 레코드 필터링

유형 라우팅 정책 별칭

레코드 ... 유형 라우팅 ... 차별... 별칭 값/트래픽 라우팅 대상 TTL

openwebs... NS 단순 - 아니요 ns-672.awsdns-20.net. ns-233.awsdns-29.com. ns-2043.awsdns-63.co.uk. ns-1183.awsdns-19.org. 172

openwebs... SOA 단순 - 아니요 ns-672.awsdns-20.net. awsd... 900

김모건님

My 정보 관리

9월 결제 예상 금액

결제 수단 등록하기

010-5316-\*\*\*\*

jasini\*\*\*2@gmail.com

0원

1% 더 할인 받으려면? 정기결제 신청하기

결제 관련 바로가

이용 중인 서비스

다시보드 뷰토리얼보기

미결제 주문서

0개 발급

결제하지 않은 주문서 및 가상 계좌

세금 계산서

0개 발급 가능

이런 달 기준 발급 가능한 세금 계산서

카드

0개 생성

구매할 서비스 목록이 담긴 주문서

예지금

0원

현금처럼 사용 가능한 예지금

현재 이용 중인 서비스를 확인하세요.

진짜보기

이용 중인 서비스 관리 버튼입니다.

도메인 1건 >

IT환경의 최적화된 가비아 서비스를 이용해보세요.

호스팅 홈페이지 쇼핑물

클라우드 하이웍스 IDC

보안

DNS 관리툴

소유권 이전

담당자 설정

도메인 통합 관리툴

관리 정보 입력 필요 서비스 0건 >

9월 연장 필요 서비스 0건 >

이용 중인 서비스 전체 1건

소유권 이전 담당자 설정

DNS 관리툴

도메인 통합 관리툴

결제 수단 등록 >

결제 수단을 미리 등록하여 서비스 신청 및 연장을 편리하게 진행하세요

도메인

도메인 또는 일련번호(1) 입력

상세 검색

검색

초기화

전체 1건

10 20 50 100

도메인 openwebservice.store 2023-09-21 ~ 2024-09-21 (D-366) 연장 > 77,000원/년 관리

< 1 >



네임서버 설정

☐ 전체 가비아 네임서버 사용

openwebsevice.store

네임서버 목록

구분	호스트명	구분	호스트명
1차	ns-672.awsdns-20.net	2차	ns-233.awsdns-29.com
3차	ns-2043.awsdns-63.co.uk	4차	ns-1183.awsdns-19.org

- 네임서버는 IP(숫자)를 제외한 호스트명만 입력합니다. (예. ns.gabia.co.kr)
- 네임서버 값을 복사해서 입력하는 경우, 공란이 포함되지 않도록 주의하시기 바랍니다.
- 각 도메인마다 네임서버 최소/최대 값이 다릅니다.
- 따라서 여러 개의 네임 서버를 입력하여도 도메인의 허용된 개수에 따라 적용됩니다.
- 가비아 네임서버는 DNSSEC를 지원하지 않습니다. DNSSEC이 설정된 도메인을 가비아 네임서버로 변경하시는 경우, 웹사이트 접속(리플링)이 제한됩니다.

+ 추가

소유자 인증

소유자 인증

소유자 인증

인증 완료

- 반드시 소유자 인증을 완료해야 소유자 정보를 변경하실 수 있습니다.
- 소유자 인증에 실패했을 경우, 고객센터 1544-4370 또는 1:1로 문의하시기 바랍니다.

적용

목록으로

네임서버 설정

☐ 전체 가비아 네임서버 사용

openwebsevice.store

네임서버 목록

구분	호스트명	구분	호스트명
1차	ns-672.awsdns-20.net	2차	ns-233.awsdns-29.com
3차	ns-2043.awsdns-63.co.uk	4차	ns-1183.awsdns-19.org

- 네임서버는 IP(숫자)를 제외한 호스트명만 입력합니다. (예. ns.gabia.co.kr)
- 네임서버 값을 복사해서 입력하는 경우, 공란이 포함되지 않도록 주의하시기 바랍니다.
- 각 도메인마다 네임서버 최소/최대 값이 다릅니다.
- 따라서 여러 개의 네임 서버를 입력하여도 도메인의 허용된 개수에 따라 적용됩니다.
- 가비아 네임서버는 DNSSEC를 지원하지 않습니다. DNSSEC이 설정된 도메인을 가비아 네임서버로 변경하시는 경우, 웹사이트 접속(리플링)이 제한됩니다.

+ 추가

소유자 인증

소유자 인증

소유자 인증

인증 완료

- 반드시 소유자 인증을 완료해야 소유자 정보를 변경하실 수 있습니다.
- 소유자 인증에 실패했을 경우, 고객센터 1544-4370 또는 1:1로 문의하시기 바랍니다.

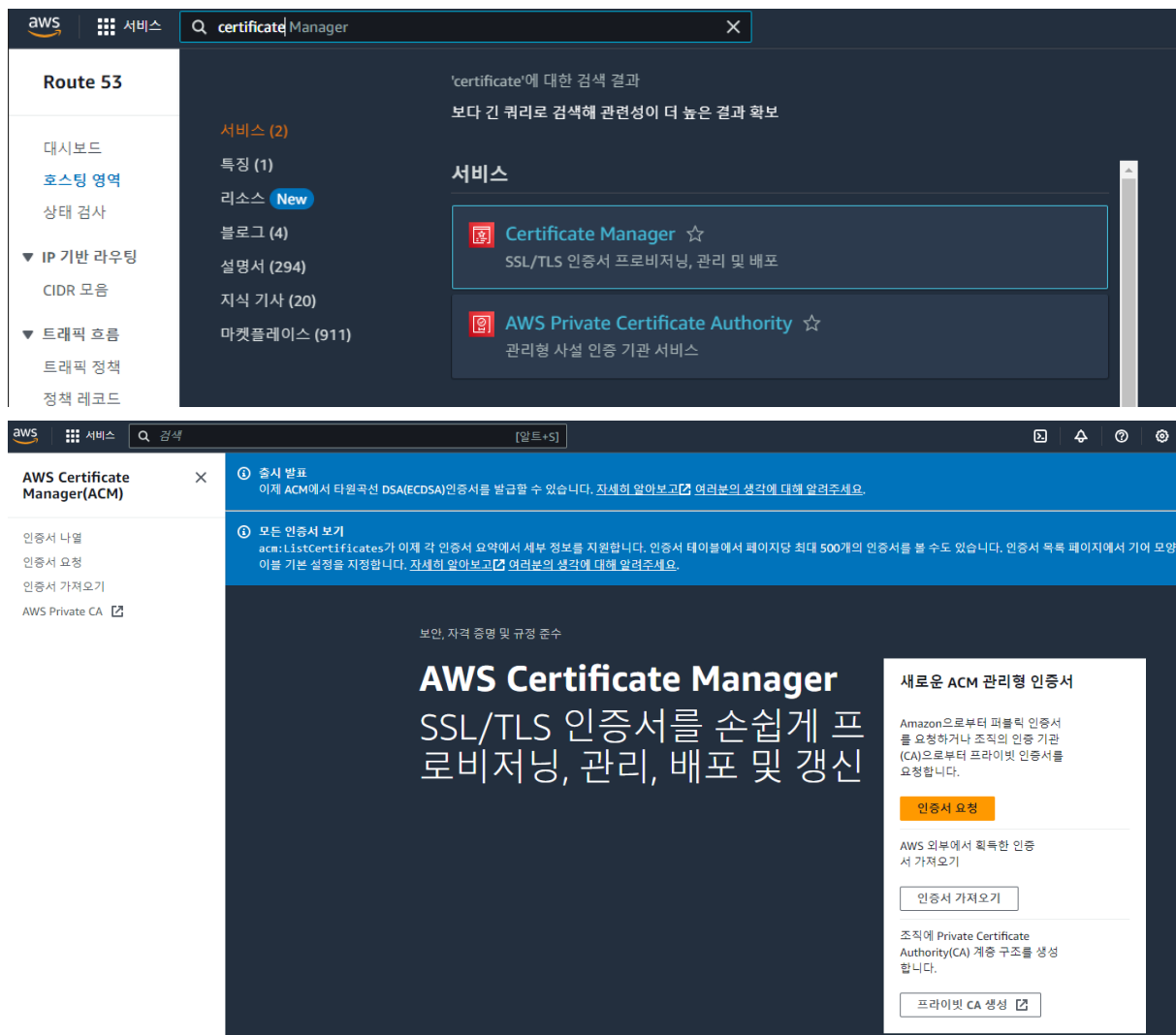
적용

목록으로

## 5. AWS Certificate Manager (ACM)

### 주소

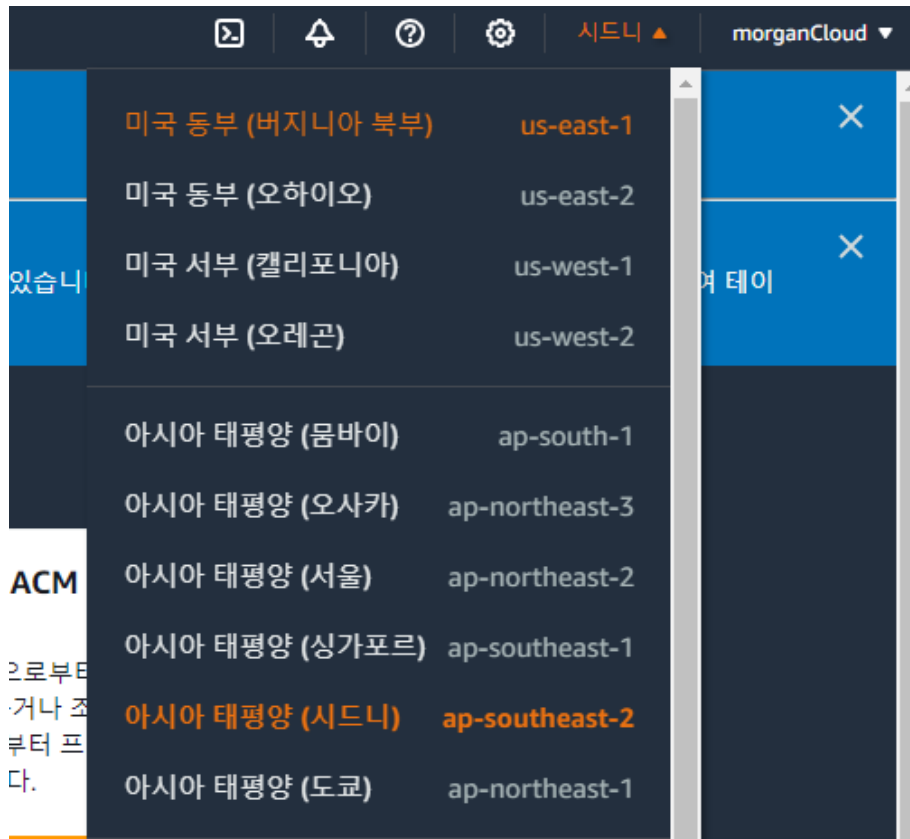
- SSL/TLS (Secure Sockets Layer/Transport Layer Security) 인증서를 관리하고 프로비저닝(제공) 하는 역할
- 장점 :
  1. SSL/TLS 인증서는 배포한 웹사이트의 데이터 통신을 암호화하고 안전하게 보호해주는 역할
  2. 브라우저의 검색 엔진에서 SSL/TLS를 사용하는 웹 사이트를 더 선호하며 SEO에 대해서 우선 순위를 차지하여 사용자 경험 향상



1. 국가를 미국 동부-버지니아 북부로 설정 (AWS에서 여기에서만 인증서를 관리)  
인증서 요청 -> 퍼블릭 인증서 요청 ->  
완전히 정규화된 도메인 이름 (보안을 적용하려는 도메인 이름 입력) ->  
-> 도메인 주소 입력  
-> \*.도메인 주소 입력



-> 요청



AWS Certificate Manager > 인증서 > 인증서 요청

## 인증서 요청

**인증서 유형 정보**  
ACM 인증서는 인터넷 또는 내부 네트워크 내에서 안전한 통신 역세스를 설정하는 데 사용할 수 있습니다. ACM이 제공할 인증서 유형을 선택합니다.

☒ 퍼블릭 인증서 요청  
Amazon으로부터 퍼블릭 SSL/TLS 인증서를 요청합니다. 기본적으로 브라우저 및 운영 체제는 퍼블릭 인증서를 신뢰합니다.

☐ 프라이빗 인증서 요청  
발급할 수 있는 프라이빗 CA가 없습니다.

프라이빗 인증서를 요청하려면 Private Certificate Authority(CA)를 생성해야 합니다. Private CA를 생성하려면 다음을 참조하십시오. [AWS Private Certificate Authority](#)

[취소](#) [다음](#)

AWS Certificate Manager > 인증서 > 인증서 요청 > 퍼블릭 인증서 요청

## 퍼블릭 인증서 요청

**도메인 이름**  
인증서에 대해 하나 이상의 도메인 이름을 제공합니다.

**완전히 정규화된 도메인 이름 정보**

[제거](#)

[제거](#)

[이 인증서에 다른 이름 추가](#)

이 인증서에 이름을 추가할 수 있습니다. 예를 들어, 'www.example.com'에 대한 인증서를 요청하는 경우 고객이 두 이름 중 하나로 사이트에 접속할 수 있도록 'example.com'이라는 이름을 추가할 수 있습니다.

AWS Certificate Manager > 인증서 > 인증서 요청 > 퍼블릭 인증서 요청

## 퍼블릭 인증서 요청

**도메인 이름**  
 인증서에 대해 하나 이상의 도메인 이름을 제공합니다.

완전히 정규화된 도메인 이름 **정보**  
 제거  
 제거  

이 인증서에서 이름을 추가할 수 있습니다. 예를 들어, 'www.example.com'에 대한 인증서를 요청하는 경우 고객이 두 이름 중 하나로 사이트에 접속할 수 있도록 'example.com'이라는 이름을 추가할 수 있습니다.

**검증 방법** **정보**  
 도메인 소유권을 검증하기 위한 방법 선택

☒ **DNS 검증 - 권장**  
 인증서 요청에서 도메인에 대한 DNS 구성을 수정할 권한이 있는 경우 이 옵션을 선택합니다.

☐ **이메일 검증**  
 인증서 요청에서 도메인에 대한 DNS 구성을 수정할 권한을 소유하지 않거나 획득할 수 없는 경우 이 옵션을 선택합니다.

**키 알고리즘** **정보**  
 암호화 알고리즘을 선택합니다. 일부 알고리즘은 일부 AWS 서비스에서 지원되지 않을 수 있습니다.

☒ **RSA 2048**  
 RSA는 가장 널리 사용되는 키 유형입니다.

☐ **ECDSA P256**  
 암호화 강도는 RSA 3072와 동일합니다.

☐ **ECDSA P384**  
 암호화 강도는 RSA 7680와 동일합니다.

**태그** **정보**  
 인증서를 쉽게 관리할 수 있도록 선택적으로 각 리소스에 고유한 메타데이터를 태그 형식으로 지정할 수 있습니다.

이 리소스와 연결된 태그가 없습니다.

태그를 50개 더 추가할 수 있습니다.

취소

이전

요청

## 2. DNS 검증을 위해 Route 53에서 레코드 생성 -> 레코드 생성

AWS Certificate Manager > 인증서

인증서 (1)

< 1 >

<input type="checkbox"/>	인증서 ID	도메인 이름	유형	상태	사용 중	경신 자격	키 알고리즘
<input type="checkbox"/>	4c084294-f6f6-43b7-bd66-bc3c7c0cd993	openwebservice.store	Amazon 발급	인증 대기 중	아니요	부적격	RSA 2048

AWS Certificate Manager > 인증서 > 4c084294-f6f6-43b7-bd66-bc3c7c0cd993

### 4c084294-f6f6-43b7-bd66-bc3c7c0cd993

**인증서 상태**

식별자  
 4c084294-f6f6-43b7-bd66-bc3c7c0cd993

상태  
 인증 대기 중 **정보**

ARN  
 arn:aws:acm:us-east-1:099007247692:certificate/4c084294-f6f6-43b7-bd66-bc3c7c0cd993

유형  
 Amazon 발급

도메인 (2)

< 1 >

도메인	상태	경신 상태	유형	CNAME 이름	CNAME 값
openwebservice.store	인증 대기 중	-	CNAME	_d4839f7316dd2eb2b82ce979a55fb09e.openwebservice.store.	_7f643e31ef46010762a0cd6182e6471c.wsbhgzrqq.acm-validations.aws.
*.openwebservice.store	인증 대기 중	-	CNAME	_d4839f7316dd2eb2b82ce979a55fb09e.openwebservice.store.	_7f643e31ef46010762a0cd6182e6471c.wsbhgzrqq.acm-validations.aws.

## Amazon Route 53에서 DNS 레코드 생성 (2/2)

도메인 검색

2 일치 항목

&lt; 1 &gt;

검증 상태: 검증 대기 중 ✕

검증 상태: 실패 ✕

도메인이 Route 53에 있습니까?: 예 ✕

필터 지우기

<input checked="" type="checkbox"/>	도메인	검증 상태	유형	CNAME 이름	CNAME 값	도메인이 Route 53에 있습니까?
<input checked="" type="checkbox"/>	openwebser vice.store	🕒 검증 대기 중	CNAME	_d4839f7316dd2eb 2b82ce979a55fb09 e.openwebservice.s tore.	_7f643e31ef460 10762a0cd6182 e6471c.wsbhgqr qqg.acm- validations.aws.	예
<input checked="" type="checkbox"/>	*.openwebs ervice.store	🕒 검증 대기 중	CNAME	_d4839f7316dd2eb 2b82ce979a55fb09 e.openwebservice.s tore.	_7f643e31ef460 10762a0cd6182 e6471c.wsbhgqr qqg.acm- validations.aws.	예

취소

레코드 생성

🕒 DNS 레코드를 성공적으로 생성했습니다.  
Amazon Route 53에서 ID가 4c084294-f6f6-43b7-bd66-bc3c7c0cd993인 인증서에 대한 DNS 레코드를 성공적으로 생성했습니다.

4c084294-f6f6-43b7-bd66-bc3c7c0cd993

삭제

## 인증서 상태

식별자

4c084294-f6f6-43b7-bd66-bc3c7c0cd993

상태

🕒 검증 대기 중 [정보](#)

ARN

 arn:aws:acm:us-east-1:099007247692:certificate/4c084294-f6f6-43b7-bd66-bc3c7c0cd993

유형

Amazon 발급

## 도메인 (2)

Route 53에서 레코드 생성

CSV로 내보내기 📄

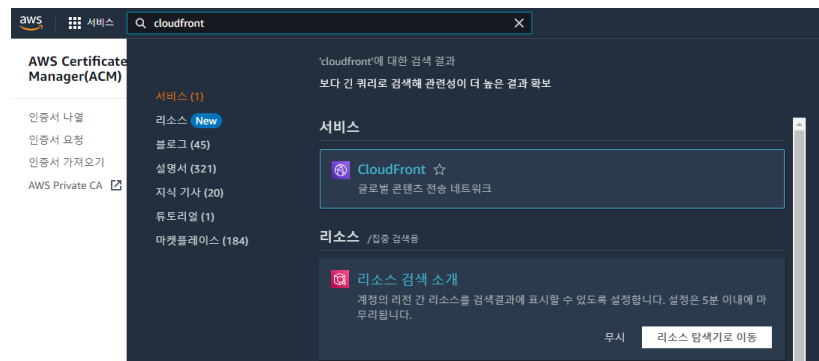
&lt; 1 &gt;

도메인	상태	갱신 상태	유형	CNAME 이름	CNAME 값
openwebservice.store	🕒 검증 대기 중	-	CNAME	 _d4839f7316dd2eb2b82ce979a55fb09e.openwebservice.store.	 _7f643e31ef46010762a0cd6182e6471c.wsbhgqrqqg.acm-validations.aws.
*.openwebservice.store	🕒 검증 대기 중	-	CNAME	 _d4839f7316dd2eb2b82ce979a55fb09e.openwebservice.store.	 _7f643e31ef46010762a0cd6182e6471c.wsbhgqrqqg.acm-validations.aws.

## 6. AWS CloudFront

### 주소

- 전세계에 분산된 AWS 네트워크를 통해 다른 배포 방법보다 보다 신속하게 브라우저에 접근 가능
- 브라우저에 대한 모니터링 및 로그 분석 가능
- DDoS 공격, 방화벽 등 보안 기능 제공 (요금 추가 부과)



### 네트워킹 및 콘텐츠 전송

## Amazon CloudFront

# 짧은 대기 시간과 빠른 전송 속도 로 콘텐츠를 안전하게 제공

Amazon CloudFront는 짧은 대기 시간과 빠른 전송 속도로 전 세계 고객에게 데이터, 비디오, 애플리케이션 및 API를 안전하게 전달하는 고속 콘텐츠 전송 네트워크(CDN) 서비스입니다.

#### CloudFront 시작하기

5분 이내에 Amazon S3 버킷, Application Load Balancer, Amazon API Gateway API 등에 대해 빠르고 안정적인 콘텐츠 전송을 지원합니다.

[CloudFront 배포 생성](#)

#### AWS 프리 티어

1TB의 데이터 송신

10,000,000건의 HTTP 또는 HTTPS 요청

2,000,000건의 CloudFront 함수 호출

매월 상시 무료

#### 요금(미국)

매월 첫 1TB 데이터 전송 무료

10TB/월	USD 0.085/GB
HTTP 요청	10,000건당 USD 0.0075
HTTPS 요청	10,000건당 USD 0.0100

월 10TB 이상을 역정하는 고객은 요금 할인을 받을 수 있습니다. [요금 보기](#)

#### 이점 및 기능

##### 대기 시간 감소

CloudFront 네트워크에는 원전 이동화 병렬 1000개 이상으로 연결된 225개 이상의 상륙 접속 위치(PoP)가 있어 최종 사용자에게 매우 낮은 대기 시간 성능과 고효율성을 제공합니다. CloudFront는 캐시된 콘텐츠 또는 동적 콘텐츠를 제공할 때 네트워크 상태를 자동으로 감지하고 사용자의 트래픽을 지능적으로 라우팅합니다.

##### 비용 절감

CloudFront를 사용하여 감지된 AWS는 요청을 통합하고 AWS 원본에서 데이터 전송 요금을 제거합니다. CloudFront는 선결제 없이 간단한 종량제 요금 및 최대 30%까지 추가 비용을 절감하는 데 도움이 되는 CloudFront 보안 결박 번들 등 사용자 정의가 가능한 요금 옵션을 제공합니다.

##### 보안 개선

경계 보호, 트래픽 암호화 및 액세스 제어를 위해 CloudFront를 사용합니다. AWS Shield Standard는 추가 비용 없이 DDoS 공격으로부터 CloudFront를 통해 전송되는 트래픽을 보호합니다. 애플리케이션 보안을 위해 AWS WAF, 관리형 규칙 및 관리형 서드 파티 방화벽 옵션을 CloudFront 워크로드에 통합할 수 있습니다.

##### 사용자 정의 전송

서비스를 컴퓨팅 기능을 사용하면 AWS CDN 엣지에서 자체 코드를 안전하게 실행할 수 있습니다. 비즈니스가 직면한 고유한 과제를 극복하고 비용, 성능 및 보안 간에 고유한 균형을 이루도록 전송을 사용자 정의하세요.

## 1. CloudFront 배포 생성 -> 원본 도메인 -> 정적 웹사이트 도메인 주소 ->

aws 서비스 검색 [알트+s]

CloudFront > 배포 > 생성

### 배포 생성

#### 원본

원본 도메인  
AWS 원본을 선택하거나 사용자 원본의 도메인 이름을 입력합니다.

원본 도메인 선택

Amazon S3
morganbuckettest.s3.amazonaws.com
Elastic Load Balancer
원본을 사용할 수 없습니다.
API Gateway
원본을 사용할 수 없습니다.
Mediastore container
원본을 사용할 수 없습니다.
Mediapackage container
원본을 사용할 수 없습니다.

Origin Shield는 원본의 부하를 줄이고 가용성을 보호하는 데 도움이 되는 추가 캐싱 계층입니다.

☒ 아니요  
☐ 예

▶ 추가 설정

#### 원본 도메인

AWS 원본을 선택하거나 사용자 원본의 도메인 이름을 입력합니다.

원본 도메인 선택

morganbuckettest.s3.ap-southeast-2.amazonaws.com

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

## 2. 뷰어 프로토콜 -> Redirect HTTP to HTTPS 선택

( http 도메인으로 접속하더라도 https로 이동 )

### 기본 캐시 동작

경로 패턴 정보

기본값(\*)

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.

### 3. 웹 애플리케이션 방화벽(WAF) -> 보안모드 활성화/비활성화 (선택사항)

웹사이트 접속 및 공격을 포함한 1천만 건당 \$14달러 발생

#### 웹 애플리케이션 방화벽(WAF)

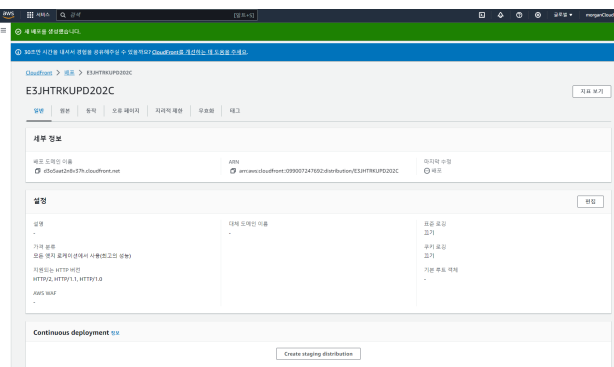
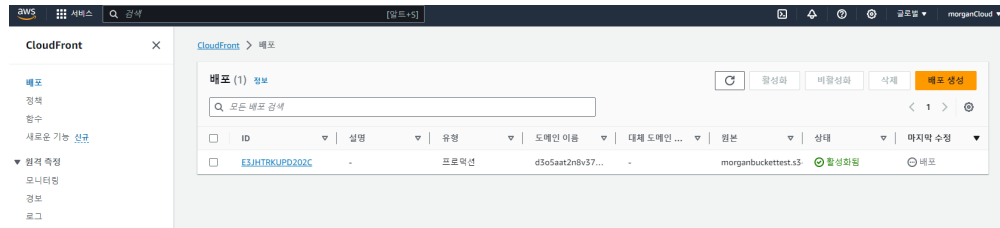
☐ 보안 보호 활성화

AWS WAF를 사용하여 가장 일반적인 웹 위험과 보안 취약성으로부터 애플리케이션을 안전하게 보호하세요. 차단된 요청은 웹 서버에 도달하기 전에 중지됩니다.

☒ 보안 보호 비활성화

애플리케이션에 AWS WAF의 보안 보호 기능이 필요하지 않은 경우 이 옵션을 선택하세요.

### 4. 대체 도메인 이름(CNAME) -> www.도메인 이름, 도메인 이름 총 2개 각각 생성 ->



### 5. 사용자 정의 SSL 인증서 -> 인증서 선택 ->

#### 웹 애플리케이션 방화벽(WAF)

☐ 보안 보호 활성화

AWS WAF를 사용하여 가장 일반적인 웹 위험과 보안 취약성으로부터 애플리케이션을 안전하게 보호하세요. 차단된 요청은 웹 서버에 도달하기 전에 중지됩니다.

☒ 보안 보호 비활성화

애플리케이션에 AWS WAF의 보안 보호 기능이 필요하지 않은 경우 이 옵션을 선택하세요.

#### 설정

**가격 분류** 정보

지불하려는 코그가와 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 레코드로 제공하는 파일에 대해 URL에서 사용하는 사용자 정의 도메인 이름을 추가합니다.

① 대체 도메인 이름 목록을 추가하려면 **대량 편집기(들)**를 사용하십시오.

**사용자 정의 SSL 인증서 - 선택 사항**

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

☒ openwebservice.store [인증서 요청](#)

레거시 플라이언트 지원 - 월 600달러에서 비해 배분된 요금이 적용됩니다. 대부분의 고객은 이를 필요로 하지 않습니다. CloudFront는 각 CloudFront 엣지 로케이션에 전용 IP 주소를 할당함으로써 HTTPS를 통해 콘텐츠를 서비스합니다.

☐ 활성화됨

**보안 정책**

보안 정책은 CloudFront가 하이퍼레이언트와 HTTPS 연결에 사용하는 SSL 또는 TLS 프로토콜 및 특정 암호를 결정합니다.

☒ TLSv1.2\_2021(권장)

☐ TLSv1.2\_2019

☐ TLSv1.2\_2018

☐ TLSv1.1\_2016

☐ TLSv1\_2016

☐ TLSv1

## 6. 기본값 루트 객체 -> index.html -> 변경 사항 저장

지원되는 HTTP 버전  
추가 HTTP 버전에 대한 지원을 추가합니다. HTTP/1.0 및 HTTP/1.1이 기본값으로 지원됩니다.

☒ HTTP/2  
☐ HTTP/3

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

표준 로깅  
Amazon S3 버킷으로 전송된 뷰어 요청의 로그를 가져옵니다.

☒ 끄기  
☐ 켜기

IPv6  
☐ 끄기  
☒ 켜기

설명 - 선택 사항

취소 변경 사항 저장

## 7. Route 53 이동 -> 호스팅 영역 -> 레코드 생성 -> 레코드 이름 www -> 별칭 클릭 -> 엔드 포인트 -> Cloudfront 배포에 대한 별칭 -> 배포 주소 선택 -> 레코드 생성

aws 서비스 검색 [알트+S]

Route 53

Route 53 > 호스팅 영역

호스팅 영역 (1)  
Automatic 모드는 최상의 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

호스팅 영역 이름	유형	생성자	레코드 수	설명	호스팅 영역 ID
openwebservice.store	파블릭	Route 53	3	-	Z0268339235719POD4PKU

aws 서비스 검색 [알트+S]

Route 53

Route 53 > 호스팅 영역 > openwebservice.store

**openwebservice.store** 정보

호스팅 영역 세부 정보

레코드(3) DNSSEC 서명 호스팅 영역 태그(0)

레코드(3) 정보  
Automatic 모드는 최상의 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

레코드 ...	유형	라우팅 ...	차별...	별칭	값/트래픽 라우팅 대상	TTL
openwebs...	NS	단순	-	아니요	ns-672.awsdns-20.net. ns-233.awsdns-29.com. ns-2043.awsdns-63.co.uk. ns-1183.awsdns-19.org.	172
openwebs...	SOA	단순	-	아니요	ns-672.awsdns-20.net. awsd...	900
_d4839f7...	CNAME	단순	-	아니요	_7f643e31ef46010762a0cd6...	300

Route 53 > 호스팅 영역 > openwebservice.store > 레코드 생성

### 레코드 생성 정보

**빠른 레코드 생성** [마법사로 전환](#)

▼ 레코드 1 삭제

레코드 이름 [정보](#)  .openwebservice.store 레코드 유형 [정보](#) A - IPv4 주소 및 일부 AWS 리소스로 트래픽 라우팅

루트 도메인에 대한 레코드를 생성하려면 비워 둡니다.

☒ **별칭**

트래픽 라우팅 대상 [정보](#) CloudFront 배포에 대한 별칭

미국 동부(버지니아 북부)

CloudFront 배포 및 동일한 호스팅 영역의 다른 레코드에 대한 별칭은 전역적 별칭이며 미국 동부(버지니아 북부)에서만 사용할 수 있습니다.

×

라우팅 정책 [정보](#) 단순 라우팅 대상 상태 평가 ☐ 아니요

다른 레코드 추가

[기존 레코드 보기](#)  
다음 표에는 openwebservice.store의 기존 레코드가 나열되어 있습니다.

[취소](#) [레코드 생성](#)

8. 레코드 생성 -> 레코드 이름 없음, www 있는 것 총 2개 -> 레코드 유형 CNAME -> 값 = Cloudfront 배포 도메인 입력 -> 레코드 생성

Route 53 > 호스팅 영역 > openwebservice.store > 레코드 생성

### 레코드 생성 정보

**빠른 레코드 생성** [마법사로 전환](#)

▼ 레코드 1 삭제

레코드 이름 [정보](#)  .openwebservice.store 레코드 유형 [정보](#) CNAME - 다른 도메인 이름과 일부 AWS 리소스로 트래픽 라우팅

루트 도메인에 대한 레코드를 생성하려면 비워 둡니다.

☐ **별칭**

**값** [정보](#)

별도의 줄에 여러 값을 입력합니다.

TTL(초) [정보](#)     라우팅 정책 [정보](#) 단순 라우팅

권장 값: 60~172,800(2일)

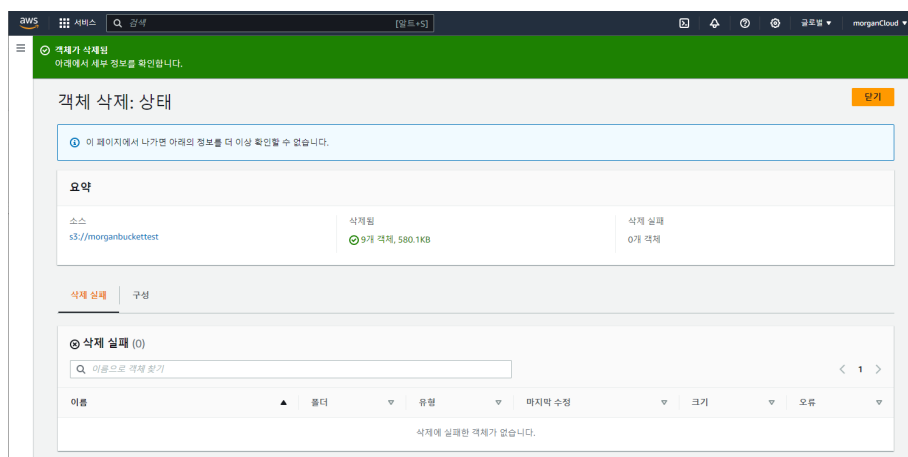
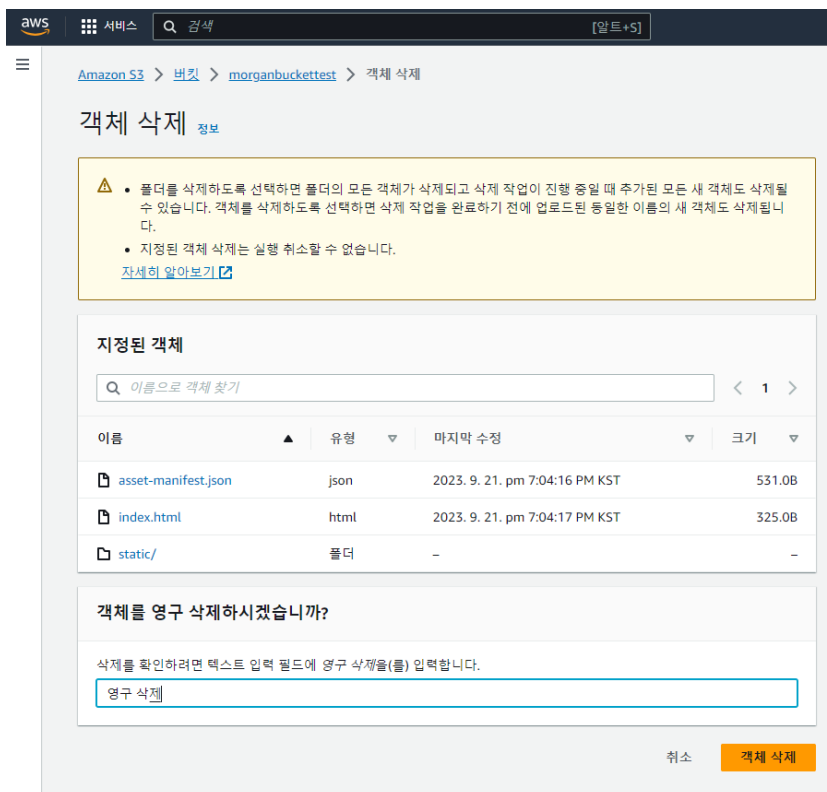
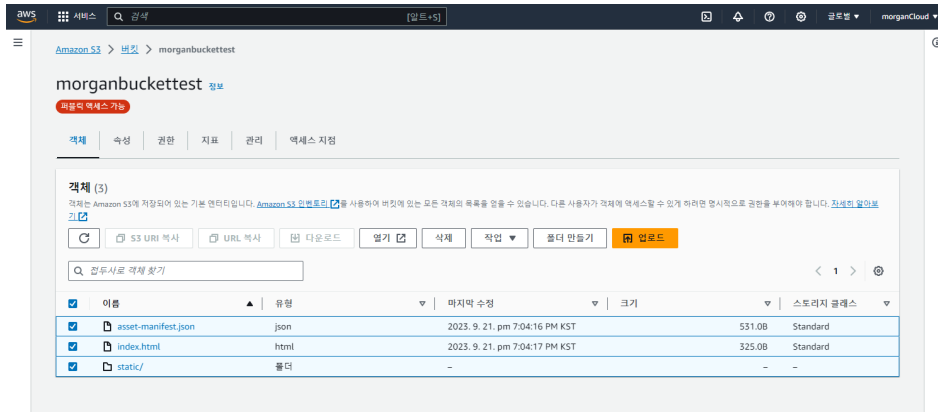
다른 레코드 추가

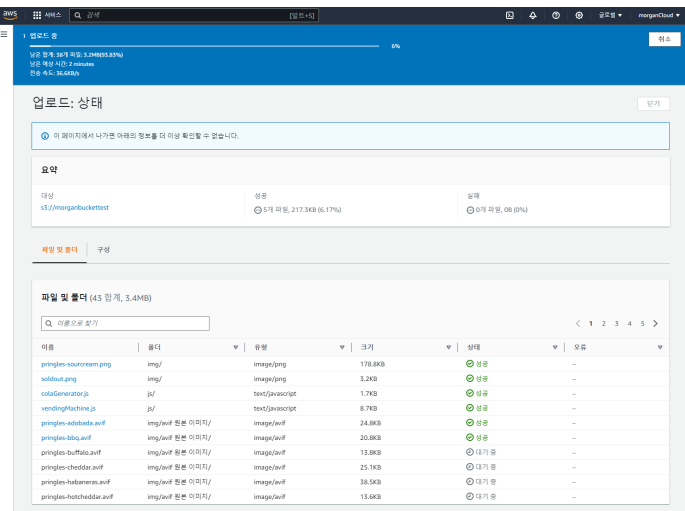
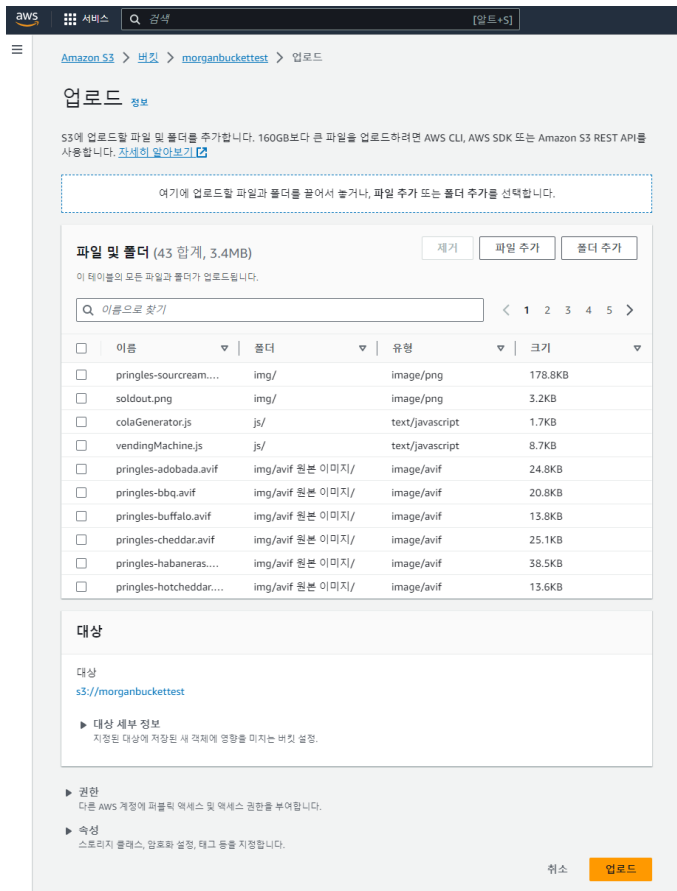
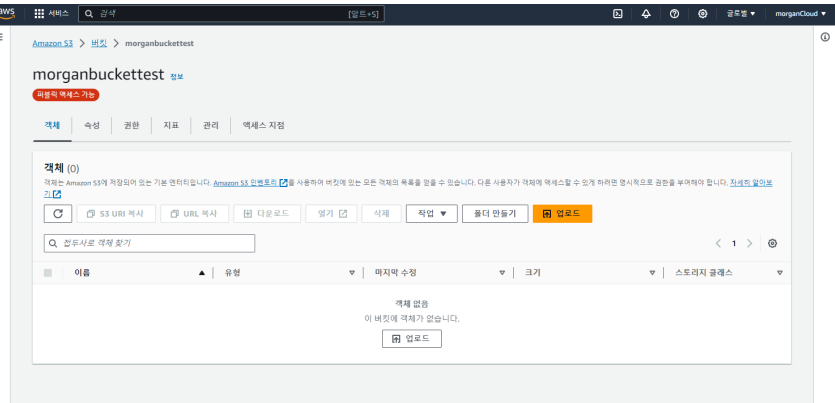
[취소](#) [레코드 생성](#)



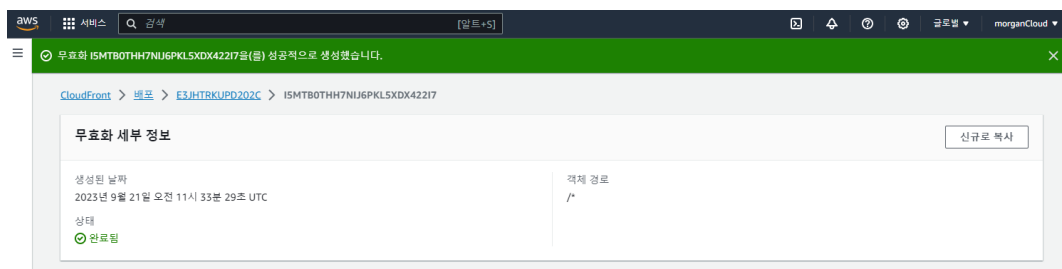
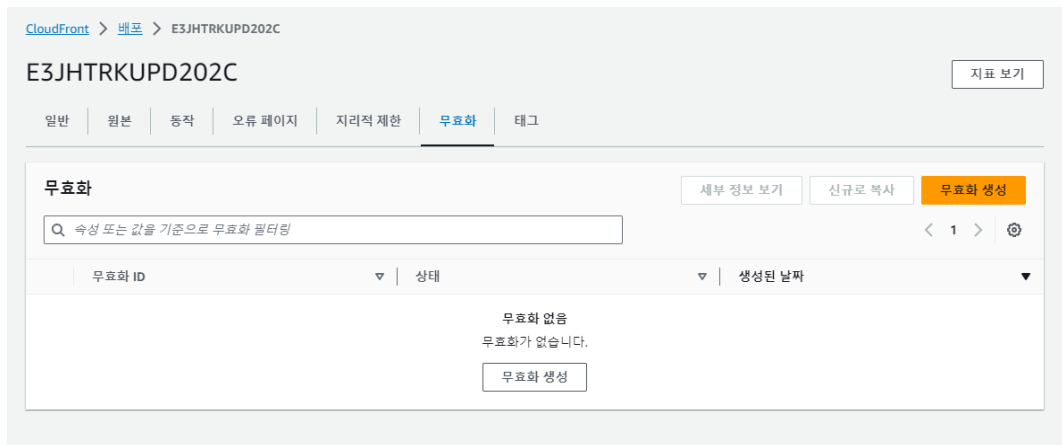
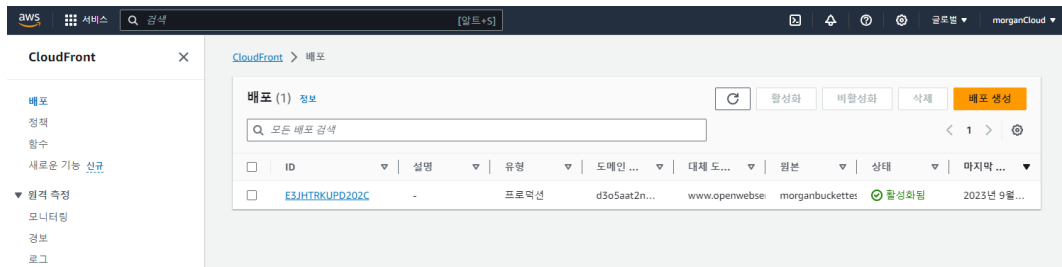
## 7. 페이지 내용을 바꾸고 싶으면

### 1. S3 -> 파일 모두 삭제 -> 바꿀 페이지 build 파일 모두 새로 업로드





## 2. Cloudfront -> 무효화 탭 -> 무효화 생성 -> /\* 입력 -> 무효화 생성 버튼 클릭



## 8. 비활성화 하기

### 1. Cloudfront - 배포 비활성화

CloudFront > 배포

배포 (1) 정보

모든 배포 검색

ID	설명	유형	도메인 이름	대체 도메인 ...	원본	상태	마지막 수정
E3JHTRKUPD202C	-	프로덕션	d3o5aat2n8v37...	www.openwebservice	morganbuckettest.s3	활성화됨	2023년 9월 21...

배포를 비활성화하시겠습니까?

이 1 배포를 비활성화하시겠습니까? 비활성화된 경우 배포가 오프라인 상태이며 요청에 응답할 수 없습니다. 나중에 배포를 활성화하여 복원할 수 있습니다.

E3JHTRKUPD202C

취소 비활성화

### 2. S3 -> 버킷 -> 퍼블릭 액세스 차단(버킷 설정) 편집 -> 모든 퍼블릭 액세스 차단

Amazon S3

계정 스냅샷

Storage Lens는 스토리지 사용량 및 활동 추세에 대한 가시성을 제공합니다. 자세히 알아보기

Storage Lens 대시보드 보기

버킷 (1) 정보

버킷은 S3에 저장되는 데이터의 컨테이너입니다. 자세히 알아보기

이름으로 버킷 찾기

이름	AWS 리전	액세스	생성 날짜
morganbuckettest	아시아 태평양(시드니) ap-southeast-2	퍼블릭	2023. 9. 21. pm 7:03:40 PM KST

aws 서비스 검색 [알트+S]

Amazon S3 > 버킷 > morganbuckettest

morganbuckettest 정보

퍼블릭 액세스 가능

객체 속성 권한 지표 관리 액세스 지점

권한 개요

액세스 퍼블릭

퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체가 적용됩니다. AWS에서는 [모든 퍼블릭 액세스 차단]을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션에 맞게 개별 설정을 사용자 지정할 수 있습니다. 자세히 알아보기

편집

모든 퍼블릭 액세스 차단

비활성

이 버킷의 개별 퍼블릭 액세스 차단 설정

aws

서비스

검색

[알트+S]

Amazon S3 > 버킷 > morganbuckettest > 퍼블릭 액세스 차단 편집(버킷 설정)

퍼블릭 액세스 차단 편집(버킷 설정) 정보

퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 ACL(엑세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대한 퍼블릭 액세스가 차단되었는지 확인하려면 [모든 퍼블릭 액세스 차단]을 활성화합니다. 이 설정은 이 버킷 및 해당 액세스 지점에만 적용됩니다. AWS에서는 [모든 퍼블릭 액세스 차단]을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 버킷 또는 내부 객체에 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 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 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지점 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 정책을 변경하지 않습니다.

☒ 임의의 퍼블릭 버킷 또는 액세스 지점 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.

취소

변경 사항 저장

퍼블릭 액세스 차단 편집(버킷 설정) X

이 설정은 이 버킷과 버킷 안의 모든 객체에 대한 퍼블릭 액세스를 차단합니다.

설정을 확인하려면 필드에 확인을(를) 입력합니다.

확인

취소

확인

Amazon S3 > 버킷 > morganbuckettest

morganbuckettest 정보

객체

속성

권한

지표

관리

액세스 지점

권한 개요

엑세스

이 계정의 권한 부여된 사용자만

퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 ACL(엑세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대한 퍼블릭 액세스가 차단되었는지 확인하려면 [모든 퍼블릭 액세스 차단]을 활성화합니다. 이 설정은 이 버킷 및 해당 액세스 지점에만 적용됩니다. AWS에서는 [모든 퍼블릭 액세스 차단]을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 버킷 또는 내부 객체에 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 개별 설정을 사용자 지정할 수 있습니다. 자세히 알아보기

편집

모든 퍼블릭 액세스 차단

☒ 활성화

▶ 이 버킷의 개별 퍼블릭 액세스 차단 설정