

와플스튜디오 23.5기

프론트엔드 세미나 6주차

강의자: 김연우

오늘의 목표

- ✓ 프론트엔드 인프라 (AWS CF/S3)
- ✓ CI/CD

프론트엔드 인프라

React 페이지는 모두에게 동일한 코드를 전달합니다.

React는 서버로부터 데이터만을 받아오고, 브라우저에서 직접 js를 사용하여 그려줘야 합니다. (CSR)

따라서 서버로부터 어떤 응답을 받더라도 브라우저에 존재하는 파일 자체는 동일합니다.

=> React 어플리케이션을 배포할 때에는 누가 들어오든지 상관없이 동일한 파일만을 제공하면 됩니다.

스토리지 (S3)

서버용 컴퓨터는 성능이 좋고 비싸기 때문에 서버 대신 **더 가벼운 곳**에 저장하는 게 비용상 이득입니다.

좋은 컴퓨터(EC2) 대신 그냥 저장소(S3)에 넣어두고 넣었다 빼도 상관이 없습니다.

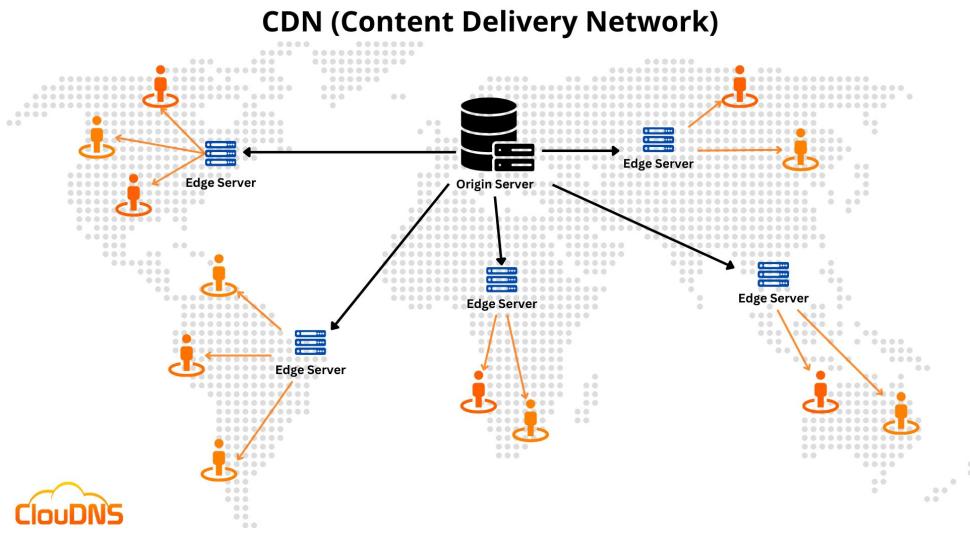
Type	CPU Units	CPU Cores	Memory
Micro (t1.micro)	Up to 2 ECUs	1 Core	613 MB
Large (m1.large)	4 ECUs	2 Cores	7.5 GB
Extra Large (m1.xlarge)	8 ECUs	4 Cores	15 GB
High-Memory Extra Large (m2.xlarge)	6.5 ECUs	2 Cores	17.1 GB
High-Memory Double Extra Large (m2.2xlarge)	13 ECUs	4 Cores	34.2 GB
High-Memory Quadruple Extra Large (m2.4xlarge)	26 ECUs	8 Cores	68.4 GB
High-CPU Extra Large (c1.xlarge)	20 ECUs	8 Cores	7 GB

ec2는 AWS에서 제공하는 컴퓨터와 같습니다.
리액트 어플리케이션에서는 이러한 성능을 고려하지
않아도 상관 없습니다.

CDN (CloudFront)

스토리지에서 리소스를 꺼내올 때 여러 나라에서도 효율적으로 접근할 수 있도록 합니다.

e.g. 한국에 스토리지를 두고 한국에서 접속 vs 한국에 스토리지를 두고 미국에서 접속
-> 여러 곳에 캐시 노드를 두고 스토리지와 연결해둔다.



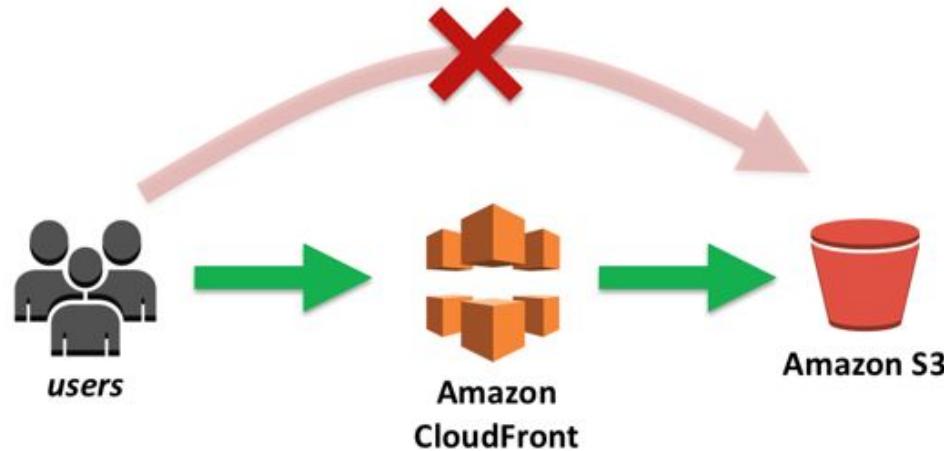
유저 → 가장 가까운 캐시노드 → 스토리지

- 1) 유저로부터 가장 가까운 캐시노드를 확인합니다.
- 2) 캐시노드에 캐시된 파일이 있다면 바로 유저에게 전달합니다.
- 3) 캐시노드에 캐시된 파일이 없다면 연결된 스토리지에 요청을 보냅니다.

S3 + CloudFront

CDN은 S3로부터 리소스를 받아 캐싱해놓습니다.

유저는 Cloudfront에 캐싱된 리소스를 받으며, S3에 직접 접근하지 않습니다.



CI/CD

CI (Continuous Integration)

코드 품질을 지속적으로 유지하는 것

코드가 변경될 때 테스트를 통해 코드 품질 및 버그를 조기에 잡습니다.

```
name: ci
```

```
on:  
  pull_request:  
    branches:  
      - main  
  push:  
    branches:  
      - main
```

코드가 변경될 때 시행된다.

```
jobs:  
  ci:  
    runs-on: ubuntu-latest
```

```
steps:  
  - uses: actions/checkout@v4  
  - uses: actions/setup-node@v4  
    with:  
      node-version: '20.11.1'  
  - name: Install dependencies  
    run: yarn install  
  - name: Check  
    run: yarn check-all
```

CI (Continuous Integration)

코드 품질을 지속적으로 유지하는 것

코드가 변경될 때 테스트를 통해 코드 품질 및 버그를
조기에 잡습니다.

```
name: ci

on:
  pull_request:
    branches:
      - main
  push:
    branches:
      - main

jobs:
  ci:
    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v4
      - uses: actions/setup-node@v4
        with:
          node-version: '20.11.1'
      - name: Install dependencies
        run: yarn install
      - name: Check
        run: yarn check-all
```

코드의 품질을 확인한다.

CD (Continuous Delivery/Deployment)

CI를 통과한 이후에 변경된 코드를 자동으로 운영 서버에 배포합니다.

곧 실습 때 만들어봅니다.

코드가 바뀌었는지 어떻게 아나요?

코드의 변경이 일어났다는 것은 어떻게 알 수 있을까요?

깃허브 등에서는 github action 등의 자체 서비스를 제공하여 코드의 변화를 감지할 수 있도록 합니다.

이외에도 jenkins 등의 독립적인 서버를 띄워 코드 변화를 감지할 수도 있습니다.

IAM (Identity and Access Management)

aws에서는 aws 리소스에 접근할 때 IAM을 사용하여 안전하게 사용할 수 있도록 합니다.

누가 (Identity) 어떤 작업(Access)을 할지 관리하는 서비스입니다.

IAM을 사용하면 내가 아니더라도 배포 자동화 도구가 aws 리소스에 접근하는 것을 허용할 수 있습니다.

실습: AWS S3 + CloudFront로 배포하기

AWS 회원가입

다들 계정 있으시죠?

만약 프리티어가 만료된 경우에는 메일 별칭을 사용하면 새로운 프리티어 계정을 하나 더 생성할 수 있습니다.

yeonuKim+2025@gmail.com 이런 식으로 별칭 이메일을 만들면 새로운 계정으로 인식하여 생성됩니다.

더 알아보고 싶다면: [프리티어 무한 생성하기](#)

IAM 생성하기

지금은 루트 계정으로 들어와 있지만, 앞으로는 허용된 권한만 수행하는 IAM 계정으로만 작업합니다.

우리가 사용할 것은 S3, Cloudfront, IAM 계정 권한이므로 해당 권한을 가진 IAM 계정을 생성합니다.

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리 신규

▼ 보고서 액세스

Access Analyzer

외부 액세스

미사용 액세스

분석기 설정

자격 증명 보고서

주진 활동

IAM 대시보드 정보

보안 권장 사항 0

✓ 루트 사용자에게 MFA 있음

루트 사용자에 대해 멀티 팩터 인증(MFA)을 적용하면 이 계정의 보안이 강화됩니다.

✓ 루트 사용자에게 활성 액세스 키가 없음

루트 사용자 대신 IAM 사용자에 연결된 액세스 키를 사용하면 보안이 향상됩니다.

IAM 리소스

이 AWS 계정의 리소스

사용자 그룹

1

사용자

4

역할

3

정책

2

ID 제공업체

0

새로운 기능 ⓘ

IAM의 기능 업데이트

모두 보기

- AWS IAM announces support for encrypted SAML assertions. 4주 전
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 1개월 전
- IAM Roles Anywhere credential helper now supports TPM 2.0. 3개월 전

AWS 계정

계정 ID

계정 별칭

생성

이 계정의 IAM 사용자를 위한 로그인 URL

Quick Links

내 보안 자격 증명

액세스 키, 멀티 팩터 인증(MFA) 및 기타 자격 증명을 관리합니다.

도구 ⓘ

정책 시뮬레이터

시뮬레이터는 선택한 정책을 평가하고 지정한 각 작업에 대해 유효한 권한을 결정합니다.

Identity and Access Management(IAM)

[] IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리 [신규](#)

▼ 보고서 액세스

Access Analyzer

외부 액세스

미사용 액세스

분석기 설정

자격 증명 보고서

[] []

사용자 (4) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.



삭제

사용자 생성

[] 검색

<

1

>



<input type="checkbox"/>	사용자 이름	▲ 경로	▼ 그룹	▼ 마지막 활동	▼ MFA	▼ 암호 수명	▼ 콘솔 마지막 로그인	▼ 액세스
<input type="checkbox"/>	[REDACTED]	/	1	⚠ 366일 전	-	⚠ 411일	⚠ March 03, 2024, 00:09 (U)	Act
<input type="checkbox"/>	[REDACTED]	/	0	⚠ 117일 전	-	-	-	Act
<input type="checkbox"/>	[REDACTED]	/	0	⚠ 117일 전	-	⚠ 117일	November 06, 2024, 1...	-
<input type="checkbox"/>	[REDACTED]	/	0	⚠ 117일 전	-	-	-	Act

- 2단계
권한 설정
- 3단계
검토 및 생성
- 4단계
암호 검색

사용자 세부 정보

사용자 이름

사용자 이름은 최대 64자까지 가능합니다. 유효한 문자: A~Z, a~z, 0~9 및 + = . @ _ -(하이픈)

AWS Management Console에 대한 사용자 액세스 권한 제공 – 선택 사항

사람에게 콘솔 액세스 권한을 제공하는 경우 IAM Identity Center에서 액세스를 관리하는 것은 모범 사례입니다.

① 사람에게 콘솔 액세스 권한을 제공하고 있습니까?

사용자 유형

Identity Center에서 사용자 지정 - 권장

Identity Center를 사용하여 사람에게 콘솔 액세스 권한을 제공하는 것이 좋습니다. Identity Center를 사용하면 AWS 계정 및 클라우드 애플리케이션에 대한 사용자 액세스를 중앙에서 관리할 수 있습니다.

IAM 사용자를 생성하고 싶음

액세스 키, AWS CodeCommit이나 Amazon Keypaces에 대한 서비스별 보안 인증 정보 또는 비상 계정 액세스를 위한 백업 보안 인증 정보를 통해 프로그래밍 방식 액세스를 활성화해야 하는 경우에만 IAM 사용자를 생성하는 것이 좋습니다.

콘솔 암호

자동 생성된 암호

사용자를 생성한 후 암호를 볼 수 있습니다.

사용자 지정 암호

사용자의 사용자 지정 암호를 입력합니다.

- 8자 이상이어야 합니다.
- 다음 문자 유형 중 세 가지 이상을 조합하여 포함해야 합니다. 대문자(A~Z), 소문자(a~z), 숫자(0~9), 기호 ! @ # \$ % ^ & * () _ + -(하이픈) = [] { } | `

암호 표시

사용자는 다음 로그인 시 새 암호를 생성해야 합니다 - 권장

사용자는 IAMUserChangePassword 정책을 자동으로 가져와 암호를 변경할 수 있도록 허용합니다.

해당 비밀번호로 aws 콘솔
로그인을 할 예정이니 꼭
기억해주세요.

② 이 IAM 사용자를 생성한 후 액세스 키 또는 AWS CodeCommit이나 Amazon Keypaces에 대한 서비스별 보안 인증 정보를 통해 프로그래밍 방식 액세스를 생성할 수 있습니다. [자세히 알아보기](#)

최소

다음

- 1단계
사용자 세부 정보 지정
- 2단계
권한 설정
- 3단계
검토 및 생성
- 4단계
암호 검색

권한 설정

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 직무별로 사용자의 권한을 관리하려면 그룹을 사용하는 것이 좋습니다. [자세히 알아보기](#)

권한 옵션

그룹에 사용자 추가

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자 권한을 관리하는 것이 좋습니다.

권한 복사

기존 사용자의 모든 그룹 멤버십, 연결된 관리형 정책 및 인라인 정책을 복사합니다.

직접 정책 연결

관리형 정책을 사용자에게 직접 연결합니다. 사용자에게 연결하는 대신, 정책을 그룹에 연결한 후 사용자를 적절한 그룹에 추가하는 것이 좋습니다.

권한 정책 (1335)

새 사용자에 연결할 정책을 하나 이상 선택합니다

AmazonS3FullAccess, CloudFrontFullAccess,
IAMUserChangePassword를 검색하여 넣기



정책 생성

필터링 기준 유형



검색

모든 유형

< 1 2 3 4 5 6 7 ... 67 >



정책 이름

▲ 유형

▼ 연결된 엔터티

[AccessAnalyzerServiceRolePolicy](#)

AWS 관리형

0

[AdministratorAccess](#)

AWS 관리형 - 직무

1

[AdministratorAccess-Amplify](#)

AWS 관리형

0

[AdministratorAccess-AWSElasticBeanstalk](#)

AWS 관리형

0

- 1단계 사용자 세부 정보 지정
- 2단계 권한 설정
- 3단계 검토 및 생성
- 4단계 임호 검색

검토 및 생성

선택 사항을 검토합니다. 사용자를 생성한 후 자동 생성된 임호를 보고 다운로드할 수 있습니다(활성화된 경우).

사용자 세부 정보

사용자 이름

콘솔 암호 유형

Custom password

암호 재설정 필요

아니요

권한 요약

이름

▲ | 유형

▼ | 다음과 같이 사용

< 1 >

[AmazonS3FullAccess](#)

AWS 관리형

권한 정책

[CloudFrontFullAccess](#)

AWS 관리형

권한 정책

[IAMUserChangePassword](#)

AWS 관리형

권한 정책

태그 - 선택 사항

태그는 리소스를 식별, 구성 또는 검색하는데 도움이 되도록 AWS 리소스에 추가할 수 있는 키 값 페어입니다. 이 사용자와 연결할 태그를 선택합니다.

리소스와 연결된 태그가 없습니다.

새 태그 추가

최대 50개의 태그를 더 추가할 수 있습니다.

취소

이전

사용자 생성

① 사용자가 성공적으로 생성됨

AWS Management Console에 로그인하기 위한 사용자의 암호와 이메일 지침을 보고 다운로드할 수 있습니다.

[사용자 보기](#)

- 1단계 사용자 세부 정보 지정
- 2단계 권한 설정
- 3단계 검토 및 생성
- 4단계 암호 검색

암호 검색

아래에서 사용자의 암호를 보고 다운로드하거나 AWS 관리 콘솔에 로그인하기 위한 사용자 지침을 이메일로 보낼 수 있습니다. 지금이 이 암호를 확인 및 다운로드할 수 있는 유일한 시간입니다.

콘솔 로그인 세부 정보

콘솔 로그인 URL



사용자 이름



콘솔 암호



이 URL로 접속하면 따로 계정 번호를 외울 필요가 없습니다.
대신 사용자 이름, 암호는 직접 입력해야하니 꼭 따로 저장하거나
외워두세요.

[취소](#)[.csv 파일 다운로드](#)[사용자 목록으로 돌아가기](#)

IAM 계정으로 접속하기

루트 계정은 모든 권한이 허용되어 있어 함부로 사용하면 안 됩니다.

앞으로는 우리에게 사용할 권한만을 가진 IAM 계정을 사용하여 세팅합니다.

콘솔 홈 정보

IAM 이름@IAM 번호

e.g. pironeer@1234-5678-9012

기본 레이아웃

:: 최근에 방문한 서비스 정보



최근에 방문한 서비스 없음

자주 방문하는 AWS 서비스 중 하나를 살펴봅니다.

EC2 S3 Aurora and RDS Lambda

모든 서비스 보기

:: AWS 시작

AWS 시작하기

:: AWS Health 정보

:: 비용 및 사용량 정보

이번 달 비용

비용 내역

:: 애플리케이션 (0) 정보

리전: Asia Pacific (Seoul)

ap-northeast-2(현재 리전) ▾

🔍 애플리케이션 찾기

< 1 >

이름 ▾ | 설명 ▾ | 리전 ▾ | 최초 계정 ▾ ★ ▲

☒ ► servicecatalog>ListApplications에 대한 액세스 거부됨

S3 생성하기

정적 파일을 저장할 S3 버킷을 생성합니다.

스토리지

Amazon S3

어디서든 원하는 양의 데이터를 저장 및 검색

Amazon S3는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 객체 스토리지 서비스입니다.

작동 방식



버킷 생성

S3의 모든 객체는 버킷에 저장됩니다. S3에 파일과 폴더를 업로드하려면 객체가 저장될 버킷을 생성해야 합니다.

[버킷 만들기](#)

요금

S3에서는 최소 요금이 없습니다. 사용한 만큼만 비용을 지불하며 요금은 S3 버킷의 위치에 따라 결정됩니다.

[AWS 월 사용량 계산기](#) 를 사용하여 월별 청구액 추산

[요금 세부 정보 보기](#)

리소스

[사용 설명서](#)

버킷 만들기

정보

버킷은 S3에 저장되는 데이터의 컨테이너입니다.

일반 구성

AWS 리전

아시아 태평양(서울) ap-northeast-2

버킷 이름

myawsbucket

버킷 이름은 글로벌 네임스페이스 내에서 고유해야 하며 버킷 이름 지정 규칙을 따라야 합니다. [버킷 이름 지정 규칙 보기](#)

기존 버킷에서 설정 복사 - 선택 사항

다음 구성의 버킷 설정만 복사됩니다.

버킷 선택

형식: s3://bucket/prefix

기본 설정으로 생성합니다.

이때 버킷 이름은 세팅 시 자주 사용되니 메모장에 적어두세요.

객체 소유권

정보

다른 AWS 계정에서 이 버킷에 작성한 객체의 소유권 및 액세스 제어 목록(ACL)의 사용을 제어합니다. 객체 소유권은 객체에 대한 액세스를 지정할 수 있는 사용자를 결정합니다.

ACL 비활성화됨(권장)

이 버킷의 모든 객체는 이 계정이 소유합니다. 이 버킷과 그 객체에 대한 액세스는 정책을 통해서만 지정됩니다.

객체 소유권

버킷 소유자 적용

ACL 활성화됨

이 버킷의 객체는 다른 AWS 계정에서 소유할 수 있습니다. 이 버킷 및 객체에 대한 액세스는 ACL을 사용하여 지정할 수 있습니다.

CloudFront 생성하기

정적 파일을 캐싱해 둘 CloudFront 배포를 생성합니다.

네트워킹 및 콘텐츠 전송

Amazon CloudFront

짧은 대기 시간과 빠른 전송 속도로 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.

이점 및 기능

대기 시간 감소

CloudFront 네트워크에는 원전 이중화 병렬 100GbE 광섬유로 연결된 225개 이상의 상호 접속 위치(POP)가 있어 최종 사용자에게 매우 낮은 대기 시간 성능과 고가용성을 제공합니다. CloudFront는 캐시링 콘텐츠 또는 동적 콘텐츠를 제공할 때 네트워크 상태를 자동으로 매핑하고 사용자의 트래픽을 지능적으로 라우팅합니다.

비용 절감

CloudFront를 사용하여 강화된 AWS는 요청을 통합하고 AWS 원본에서 데이터 전송 요금을 제거합니다. CloudFront는 선결제 없이 간단한 종량 제 요금 및 최대 30%까지 추가 비용을 절감하는 데 도움이 되는 CloudFront 보안 절약 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 보호를 위해 AWS WAF, 관리형 규칙 및 관리형 서드 파티 방화벽 옵션을 CloudFront 워크로드에 통합할 수 있습니다.

사용자 정의 전송

서비스 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.

CloudFront 시작하기

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

CloudFront 배포 생성

AWS 프리 티어

1TB의 데이터 송신

10,000,000건의 HTTP 또는 HTTPS 요청

2,000,000개의 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 약정하는 고객은 요금 할인
© 2024 Amazon.com, Inc. or its affiliates.

배포 생성

원본

Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

 오리진 선택

Amazon S3



Elastic Load Balancer

No origins available.

API Gateway

No origins available.

Mediastore container

원본을 사용할 수 없습니다.

Mediapackage container

원본을 사용할 수 없습니다.

Mediapackage V2 endpoints

No origins available.

VPC origins

No origins available.

기본적으로 파일을 가져올 원본을 설정합니다.

(추후에 다른 원본을 추가할 수 있습니다. 여기에서 설정한 원본은 리액트 파일들을 받아올 스토리지로 설정해주세요)

기본 캐시 동작

[경로 패턴](#) | [정보](#)

Enter the origin path

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.

Select an origin access control

Create new OAC

사용자 정의 헤더 추가 - 선택 사항

CloudFront는 원본으로 보내는 모든 요청에 이 헤더를 포함합니다.

헤더 추가

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

▶ 추가 설정

기본 캐시 동작

경로 패턴 | 정보

기본값(*)

Enter the origin path

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.

Select an origin access control

사용자 정의 헤더 추가 - 선택 사항

CloudFront는 원본으로 보내는 모든 요청에 이 헤더를 포함합니다.

헤더 추가

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce the load on your origin and

아니요

예

▶ 추가 설정

기본 캐시 동작

경로 패턴 | 정보

기본값(*)

Create new OAC

이름

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

설명 - 선택 사항

설명은 최대 256자까지 입력할 수 있습니다.

설명 입력

서명 동작

○ 요청 서명 안 함

○ 서명 요청(권장)

 승인 헤더 재정의 안 함

수신 요청에 승인 헤더가 있는 경우 서명하지 마세요.

취소

Create

서명된 요청에 대해서만 S3 요청을 허용합니다.

더 알아보고 싶다면: [presigned url](#)

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)을 사용하여 S3 버킷에 액세스합니다.

Origin access control

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

pironeer-2025-1-seminar-test.s3.ap-northeast-2.amazonaws.com

Create new OAC

⚠️ S3 버킷 정책을 업데이트해야 함

CloudFront는 배포를 생성한 후 정책 설명을 제공합니다.

사용자 정의 헤더 추가 - 선택 사항

CloudFront는 원본으로 보내는 모든 요청에 이 헤더를 포함합니다.

헤더 추가

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce the load on

- 아니요
- 예

▶ 추가 설정

기본적으로 CloudFront에서 원본으로 요청을 넘길 때
헤더에 달았던 커스텀 헤더는 무시됩니다.
만약 원본으로 전달하고 싶다면 “헤더 추가”에서 설정해줘야 합니다.

기본 캐시 동작

경로 패턴 | 정보

기본값(*)

자동으로 객체 압축 | 정보

- No



My-Header가 뛰임
그냥 무시해야지

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

모든 요청은 https로 들어가도록 설정합니다.

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 주소로만 요청할 수 있습니다.

- No
- Yes

현재는 S3로 부터 가져오는 요청만을 허용하므로 get, head만 설정해도 상관 없습니다.

하지만 추후 서버 origin이 추가되거나 S3 변경 요청이 허용된다면 세 번째 옵션을 켜줘야 합니다.

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

Policy with caching enabled. Supports Gzip and Brotli compression.

Recommended for S3 ▾



함수 연결 - 선택 사항 정보

이 캐시 동작과 연결할 잇지 함수와 함수를 호출하는 CloudFront 이벤트를 선택합니다.

함수 유형	함수 ARN/이름	바디 포함
뷰어 요청	연결 없음	
뷰어 응답	연결 없음	
원본 요청	연결 없음	
원본 응답	연결 없음	

웹 애플리케이션 방화벽(WAF) 정보

보안 보호 활성화

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

보안 보호 비활성화

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

▼ 보안 보호 기능 포함됨

- 웹 애플리케이션에서 발견되는 가장 일반적인 취약점으로부터 보호합니다.
- 애플리케이션의 취약점을 발견하는 의의적인 행위자로부터 보호합니다.
- Amazon 내부 위협 인텔리전스를 기반으로 잠재적 위협으로부터 IP 주소 차단

돈이 나갈 수 있다고 하니 꺼둡니다.

예상 가격

- ▶ 이 AWS WAF 구성은 월별 요청 1천만 건에 \$14 정도의 요금이 부과될 것으로 추정됩니다.

설정

Anycast static IP list - optional 정보
Failover traffic from a small set of IP addresses

설정

Anycast static IP list - optional | 정보
Deliver traffic from a small set of IP addresses

There are no Anycast static IP lists available

Create an Anycast static IP list

There are no Anycast static IP lists available

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

① 대체 도메인 이름 목록을 추가하려면 대량 편집기(들) 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 지원됩니다.

- HTTP/2
- HTTP/3

나중에 자체 도메인을 사용할 때 해당 내용을 설정합니다.
cname: 도메인 넣기
ssl certification: 해당 도메인에 대한 인증서 넣기

기본값 루트 객체 - 선택 사항

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

Introducing the CloudFront Security Dashboard

The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

**(?) 새 배포를 생성했습니다.**

To get in-depth monitoring information for your distribution's internet traffic, [create an Internet Monitor](#).

**⚠️ S3 버킷 정책을 업데이트해야 합니다.**

정책 설명에서 CloudFront 원본 액세스 제어에 대한 읽기 액세스를 허용하여 배포 구성을 완료하세요. 정책을 업데이트하려면 S3 버킷 권한으로 이동합니다.

정책 복사



일반 보안 원본 동작 오류 페이지 무효화 태그 Logging

Cloudfront에서 S3에 접근할 수 있어야 합니다.
따라서 S3에 해당 내용을 적용해줘야 합니다.

세부 정보

배포 도메인 이름

ARN

마지막 수정

배포

편집

설정

설명

-
가격 분류

모든 잇지 로케이션에서 사용(최고의 성능)

지원되는 HTTP 버전

HTTP/2, HTTP/1.1, HTTP/1.0

cloudfront arn을 메모장에 저장해두세요.
세팅할 때 자주 쓰입니다.

Cookie logging
[보기](#)

기본 루트 객체

Continuous deployment 정보

사용자 정의 오류 응답 생성

오류 응답 정보

HTTP 오류 코드

원본이 이 오류 코드를 전송할 때 사용자 정의 오류 응답을 사용자 정의합니다.

403: 금지됨

캐싱 최소 TTL 오류

오류 캐싱 최소 라이브 시간(TTL)을 초 단위로 입력합니다.

10

오류 응답 사용자 정의

원본에서 받은 오류 대신 사용자 정의 오류 응답을 보냅니다.

아니요

예

응답 페이지 경로

사용자 정의 오류 응답 페이지의 경로를 입력합니다.

/index.html

HTTP 응답 코드

뷰어로 돌아갈 HTTP 상태 코드를 선택합니다. CloudFront는 원본에서 받은 것과 다른 상태 코드를 뷰어에게 반환할 수 있습니다.

200: 확인

SPA이므로 정의되지 않은 URL로 요청이 들어온 경우에 403이 뜰 수 있습니다.

e.g. www.mypage.com/post

-> 등록된 리소스 중 www.mypage.com/post가 없으므로 403이 나타남.

403이 떠도 200 코드를 내려주면 불필요한 에러를 무시할 수 있습니다.

취소

사용자 정의 오류 응답 생성

S3 정책 변경하기

S3 정책을 변경해줍니다.

```
{  
    "Version": "2008-10-17",  
    "Id": "PolicyForCloudFrontPrivateContent",  
    "Statement": [  
        {  
            "Sid": "AllowCloudFrontServicePrincipal",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "cloudfront.amazonaws.com"  
            },  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::{s3 버킷}/*",  
            "Condition": {  
                "StringEquals": {  
                    "AWS:SourceArn": "{cloudfront arn}"  
                }  
            }  
        }  
    ]  
}
```



Amazon S3



법용 버킷

디렉터리 버킷

테이블 버킷

Access Grants

액세스 지점

객체 Lambda 액세스 지점

다중 리전 액세스 지점

배치 작업

S3용 IAM Access Analyzer

이 계정의 퍼블릭 액세스 차단 설정

▼ Storage Lens

대시보드

Storage Lens 그룹

AWS Organizations 설정

기능 스포트라이트

11

객체

속성

권한

지표

관리

액세스 지점

정보

권한 개요

액세스 찾기

액세스 조사 결과는 IAM 외부 액세스 분석기에서 제공합니다. [IAM 분석기 조사 결과가 작동하는 방식](#)에 대해 자세히 알아보세요.

[ap-northeast-2에 대한 분석기 보기](#)

편집

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 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 아래 개별 설정을 사용자 지정할 수 있습니다. [자세히 알아보기](#)

모든 퍼블릭 액세스 차단

 활성화

▶ 이 버킷의 개별 퍼블릭 액세스 차단 설정

편집

삭제

버킷 정책

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



Amazon S3



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

범용 버킷

디렉터리 버킷

테이블 버킷

Access Grants

액세스 지점

객체 Lambda 액세스 지점

다중 리전 액세스 지점

배치 작업

S3용 IAM Access Analyzer

이 계정의 퍼블릭 액세스 차단 설정

▼ Storage Lens

대시보드

Storage Lens 그룹

AWS Organizations 설정

기능 스포트라이트 11

▶ S3용 AWS Marketplace

버킷 ARN

정책

```
1 [ {  
2     "Version": "2008-10-17",  
3     "Id": "PolicyForCloudFrontPrivateContent",  
4     "Statement": [  
5         {  
6             "Sid": "AllowCloudFrontServicePrincipal",  
7             "Effect": "Allow",  
8             "Principal": {  
9                 "Service": "cloudfront.amazonaws.com"  
10            },  
11            "Action": "s3:GetObject",  
12            "Resource": [REDACTED]  
13        },  
14        {  
15            "Condition": {  
16                "StringEquals": {  
17                    "AWS:SourceArn": [REDACTED]  
18                }  
19            }  
20        }  
21    ]  
22 }]
```

정책을 복불해줍니다.

JSON Ln 20, Col 8 ⚙ 오류: 0 ⚙ 경고: 0

취소

변경 사항 저장

Amazon S3



버킷 정책을 편집했습니다.

그룹: <http://acs.amazonaws.com/groups/global/AllUsers>

범용 버킷

디렉터리 버킷

테이블 버킷

Access Grants

액세스 지점

객체 Lambda 액세스 지점

다중 리전 액세스 지점

배치 작업

S3용 IAM Access Analyzer

이 계정의 퍼블릭 액세스 차단 설정

▼ Storage Lens

대시보드

Storage Lens 그룹

AWS Organizations 설정

기능 스포트라이트 11

▶ S3용 AWS Marketplace

인증된 사용자 그룹(AWS 계정이 있는 모든 사용자)

그룹: <http://acs.amazonaws.com/groups/global/AuthenticatedUsers>

S3 로그 전달 그룹

그룹: <http://acs.amazonaws.com/groups/s3/LogDelivery>

CORS(Cross-origin 리소스 공유)

JSON으로 작성된 CORS 구성은 한 도메인에 로드되어 다른 도메인의 리소스와 상호 작용하는 클라이언트 웹 애플리케이션에 대한 방법을 정의합니다. [자세히](#)

추후에 이미지 또는 리소스 업로드/다운로드 시 해당 설정을 변경해줘야 합니다.

표시할 구성 없음

더 알아보고 싶다면: [presigned url & cors](#)

배포를 위한 IAM 설정하기

모든 프론트엔드 인프라 설정이 완료되었습니다.

앞으로는 우리에게 사용할 권한만을 가진 IAM 계정을 사용하여 세팅합니다.

Identity and Access Management(IAM)

IAM 검색

데시보드

액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리 [신규](#)

보고서 액세스

Access Analyzer

외부 액세스

미사용 액세스

분석기 설정

자격 증명 보고서

조직 활동

서비스 제어 정책

리소스 제어 정책 [신규](#)IAM 자격 증명 센터 [문서](#)AWS Organizations [문서](#)

사용자 (5) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.



삭제

사용자 생성

검색

< 1 > ⌂

사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인	액세스 키 ID	활성 키 수명	마지막
piro20_yeonuKim	/	1	⚠️ 367일 전	-	⚠️ 412일	⚠️ March 03, 2024, 00:09 (U)	Active - AKIAYS2NTZX...	⚠️ 412일	-
pironeer-2025-1-seminar-test	/	0	⌚ 1시간 전	-	⌚ 1시간	March 05, 2025, 09:47...	-	-	-
waffle-studio-2024-deploy	/	0	⚠️ 118일 전	-	-	-	Active - AKIAYS2NTZX...	⚠️ 118일	⚠️ 118일
waffle-studio-2024-fe-semina...	/	0	⚠️ 118일 전	-	⚠️ 118일	November 06, 2024, 1...	-	-	-
waffle-studio-2024-prod-deploy	/	0	⚠️ 118일 전	-	-	-	Active - AKIAYS2NTZX...	⚠️ 118일	⚠️ 118일

- 1단계
 사용자 세부 정보 지정
- 2단계
 권한 설정
- 3단계
 검토 및 생성

사용자 세부 정보 지정

사용자 세부 정보

사용자 이름

사용자 이름은 최대 64자까지 가능합니다. 유효한 문자: A~Z, a~z, 0~9 및 + = _ -(하이픈)

AWS Management Console에 대한 사용자 액세스 권한 제공 – 선택 사항

사람에게 콘솔 액세스 권한을 제공하는 경우 IAM Identity Center에서 액세스를 관리하는 것은 모범 사례입니다.

ⓘ 이 IAM 사용자를 생성한 후 액세스 키 또는 AWS CodeCommit이거나 Amazon S3에 대한 액세스 키를 사용하여 사용자에게 콘솔 액세스 권한을 제공하는 경우 IAM Identity Center에서 액세스를 관리하는 것은 모범 사례입니다.

배포를 위한 IAM 계정은 따로 콘솔 로그인을 할 필요가 없으므로 해당 설정을 진행하지 않아도 됩니다.
(github action으로만 IAM 권한을 사용할 예정입니다.)

취소

다음

권한 정책 (1335)

새 사용자에 연결할 정책을 하나 이상 선택합니다.



정책 생성

필터링 기준 유형			
검색		모든 유형	▼
□	정책 이름	▲ 유형	▼ 연결된 엔터티
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS 관리형	0
<input type="checkbox"/>	AdministratorAccess	AWS 관리형 - 직무	1
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS 관리형	0
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS 관리형	0
<input type="checkbox"/>	AIOpsAssistantPolicy	AWS 관리형	0
<input type="checkbox"/>	AIOpsConsoleAdminPolicy	AWS 관리형	0
<input type="checkbox"/>	AIOpsOperatorAccess	AWS 관리형	0
<input type="checkbox"/>	AIOpsReadOnlyAccess	AWS 관리형	0

사전에 정의된 권한과 다른 정책이 필요하므로
새롭게 생성해줍니다.

- 1단계
 권한 지정
2단계
 검토 및 생성

권한 지정 정보

서비스, 작업, 리소스 및 조건을 선택하여 권한을 추가합니다. JSON 편집기를 사용하여 권한 설명문을 작성합니다.

정책 편집기

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [],  
8       "Resource": []  
9     }  
10   ]  
11 }
```

다음 슬라이드의 json을 복불해주세요.

시작적 JSON 작업 ▾

문 편집

문 선택

정책에서 기존 문을 선택하거나 새 문을 추가합니다.

+ 새 문 추가

+ 새 문 추가

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:PutObject",  
                "s3:GetObject",  
                "s3:DeleteObject",  
                "s3>ListBucket"  
            ],  
            "Resource": [  
                "arn:aws:s3:::{s3Arn}/*",  
                "arn:aws:s3:::{s3Arn}"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "cloudfront>CreateInvalidation"  
            ],  
            "Resource": [  
                "{cloudfrontArn}"  
            ]  
        }  
    ]  
}
```

- 1단계
권한 지정
- 2단계
 검토 및 생성

검토 및 생성

권한을 검토하고 세부 정보 및 태그를 지정합니다.

정책 세부 정보

정책 이름

이 정책을 식별하는 의미 있는 이름을 입력합니다.

최대 128자입니다. 영숫자 및 '+=.,@_-' 문자를 사용하세요.

설명 - 선택 사항

이 정책에 대하여 간단한 설명을 추가합니다.

최대 1,000자입니다. 영숫자 및 '+=.,@_-' 문자를 사용하세요.

이 정책에 정의된 권한

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다. IAM 자격 증명(사용자, 사용자 그룹 또는 역할)에 대한 권한을 정의하려면 여기에 정책을 연결합니다.

편집

검색

허용(서비스 439개 중 2개)

나머지 서비스 437개 표시

서비스	▲ 액세스 수준	▼ 리소스	요청 조건
CloudFront	제한적: 쓰기		None
S3	제한적: 나열, 읽기, 쓰기	Multiple	None

동일한지 확인해주세요.

취소

이전

정책 생성

다시 IAM 사용자 생성으로 돌아와주세요.

- 1단계 사용자 세부 정보 지정
- 2단계 **권한 설정**
- 3단계 검토 및 생성

권한 설정

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 직무별로 사용자의 권한을 관리하려면 그룹을 사용하는 것이 좋습니다. 자세히 알아보기 

권한 옵션

 그룹에 사용자 추가

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자 권한을 관리하는 것이 좋습니다.

 권한 복사

기존 사용자의 모든 그룹 멤버십, 연결된 관리형 정책 및 인라인 정책을 복사합니다.

 직접 정책 연결

관리형 정책을 사용자에게 직접 연결합니다. 사용자에게 연결하는 대신, 정책을 그룹에 연결한 후 사용자를 적절한 그룹에 추가하는 것이 좋습니다.

권한 정책 (1336)

새 사용자에 연결할 정책을 하나 이상 선택합니다.

새로고침을 누른 뒤 내가 생성한 정책 이름을
검색해주세요.



정책 생성

 pir

모든 유형

▼

2 개 일치



1



정책 이름

▲ | 유형

▼ | 연결된 엔터티

▼

AmazonMQApiReadOnlyAccess AWS 관리형

0

pironeer-2025-1-seminar-deploy 고객 관리형

0

▶ 권한 경계 설정 - 선택 사항

취소

이전

다음

- 1단계 사용자 세부 정보 지정
- 2단계 권한 설정
- 3단계 검토 및 생성

검토 및 생성

선택 사항을 검토합니다. 사용자를 생성한 후 자동 생성된 임호를 보고 다운로드할 수 있습니다(활성화된 경우).

사용자 세부 정보

사용자 이름

콘솔 암호 유형

None

암호 재설정 필요

아니요

권한 요약

이름 []

▲ | 유형

▼ | 다음과 같이 사용

고객 관리형

권한 정책

< 1 >

태그 - 선택 사항

태그는 리소스를 식별, 구성 또는 검색하는 데 도움이 되도록 AWS 리소스에 추가할 수 있는 키 값 페어입니다. 이 사용자와 연결할 태그를 선택합니다.

리소스와 연결된 태그가 없습니다.

새 태그 추가

최대 50개의 태그를 더 추가할 수 있습니다.

취소

이전

사용자 생성

배포를 위한 IAM 엑세스 키 생성하기

배포를 위한 IAM 계정은 콘솔로 로그인하여 사용하지 않습니다.

따라서 외부에서도 접속하기 위해서는 엑세스 키를 발급받아 사용할 수 있습니다.



IAM



사용자



Identity and Access Management(IAM)

[IAM 검색](#)

대시보드

액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리 [신규](#)

보고서 액세스

Access Analyzer

외부 액세스

미사용 액세스

분석기 설정

자격 증명 보고서

조직 활동

서비스 제어 정책

리소스 제어 정책 [신규](#)IAM 자격 증명 센터 [\[?\]](#)AWS Organizations [\[?\]](#)

정보

요약

ARN

콘솔 액세스
비활성화됨액세스 키 1
액세스 키 만들기

생성됨

March 05, 2025, 11:16 (UTC+09:00)

마지막 콘솔 로그인

-

권한

그룹

태그

보안 자격 증명

마지막 액세스

콘솔 로그인

콘솔 로그인 링크

콘솔 액세스 활성화

콘솔 암호
활성화되지 않음

멀티 팩터 인증(MFA) (0)

MFA를 사용하여 AWS 환경의 보안을 강화합니다. MFA로 로그인하려면 MFA 디바이스의 인증 코드가 필요합니다. 각 사용자는 MFA 디바이스를 최대 8개까지 할당할 수 있습니다. 자세히 알아보기 [\[?\]](#)

삭제

재동기화

MFA 디바이스 할당

유형

식별자

인증

생성 날짜

MFA 디바이스가 없습니다. MFA 디바이스를 할당하여 AWS 환경 보안 개선하기

MFA 디바이스 할당

액세스 키 (0)

액세스 키를 사용하여 AWS CLI, AWS Tools for PowerShell, AWS SDK 또는 직접 AWS API 호출을 통해 AWS에 프로그래밍 방식 호출을 전송합니다. 한 번에 최대 두 개의 액세스 키(활성 또는 비활성)를 가질 수 있습니다. 자세히 알아보기 [\[?\]](#)

액세스 키 만들기

- 1단계
액세스 키 모범 사례 및 대안
- 2단계 - 선택 사항
설명 태그 설정
- 3단계
액세스 키 검색

액세스 키 모범 사례 및 대안 정보

보안 개선을 위해 액세스 키와 같은 장기 자격 증명을 사용하지 마세요. 다음과 같은 사용 사례와 대안을 고려하세요.

사용 사례

Command Line Interface(CLI)

AWS CLI를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

로컬 코드

로컬 개발 환경의 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

AWS 컴퓨팅 서비스에서 실행되는 애플리케이션

Amazon EC2, Amazon ECS 또는 AWS Lambda와 같은 AWS 컴퓨팅 서비스에서 실행되는 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

서드 파티 서비스

AWS 리소스를 모니터링 또는 관리하는 서드 파티 애플리케이션 또는 서비스에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

AWS 외부에서 실행되는 애플리케이션

이 액세스 키를 사용하여 AWS 리소스에 액세스해야 하는 AWS 외부의 데이터 센터 또는 기타 인프라에서 실행 중인 워크로드를 인증할 것입니다.

기타

귀하의 사용 사례가 여기에 나열되어 있지 않습니다.

⚠ 권장되는 대안

- 브라우저 기본 CLI인 [AWS CloudShell](#)을 사용하여 명령을 실행합니다. [자세히 알아보기](#)
- [AWS CLI V2](#) 사용하고 IAM 자격 증명 센터의 사용자를 통한 인증을 활성화합니다. [자세히 알아보기](#)

확인

위의 권장 사항을 이해했으며 액세스 키 생성을 계속하려고 합니다.

취소

다음

액세스 키 생성됨

지금이 아니면 비밀 액세스 키를 보거나 다운로드할 수 없습니다. 나중에 복구할 수 없습니다. 하지만 언제든지 새 액세스 키를 생성할 수 있습니다.

1단계
액세스 키 모범 사례 및 대안2단계 - 선택 사항
설명 태그 설정3단계
 액세스 키 검색

액세스 키 검색

정보

액세스 키

분실하거나 잊어버린 비밀 액세스 키는 검색할 수 없습니다. 대신 새 액세스 키를 생성하고 이전 키를 비활성화합니다.

액세스 키

비밀 액세스 키

 ***** 표시

액세스 키 모범 사례

- 액세스 키를 일반 텍스트, 코드 리포지토리 또는 코드로 저장해서는 안됩니다.
- 더 이상 필요 없는 경우 액세스 키를 비활성화하거나 삭제합니다.
- 최소 권한을 활성화합니다.
- 액세스 키를 정기적으로 교체합니다.

액세스 키 관리에 대한 자세한 내용은 [AWS 액세스 키 관리 모범 사례](#)를 참조하세요.

 .csv 파일 다운로드

완료

CD 구축하기

준비해놓은 프로젝트를 클론코딩을 AWS Cloudfront와 S3를 사용하여 배포합니다.

준비해놓은 프로젝트 레포지토리를 VSCode에서 열어주세요.

.github/workflow/{각자 넣을 파일 이름}.yml 파일을 생성하고 다음 슬라이드의 yaml을 복붙해주세요.

```
name: deploy-client

on:
  push:
    branches:
      - main
  workflow_dispatch:

jobs:
  deploy:
    name: Deploy
    runs-on: ubuntu-latest

    steps:
      - name: Checkout
        uses: actions/checkout@v4
      - name: Setup Node
        uses: actions/setup-node@v4
        with:
          node-version: '20.11.1'

      - name: Build & Export
        run:
          yarn install
          yarn build

      - name: Deploy to S3 and Invalidate Cloudfront in prod mode
        env:
          AWS_ACCESS_KEY_ID: ${{ secrets.AWS_ACCESS_KEY_ID }}
          AWS_SECRET_ACCESS_KEY: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
          AWS_REGION: ap-northeast-2
```

CD 구축하기

`{{secrets.something}}`은 깃허브에 저장된 비밀키를 의미합니다.

준비해놓은 프로젝트 레포지토리 settings에 들어가주세요.

Moderation options

Code and automation

Branches

Tags

Rules

Actions

Webhooks

Environments

Pages

Custom properties

Security

Code security

Deploy keys

Secrets and variables

Actions

Codespaces

Dependabot

Integrations

GitHub Apps

Email notifications

Anyone with collaborator access to this repository can use these secrets and variables for actions. They are not passed to workflows that are triggered by a pull request from a fork.

Secrets

Variables

Environment secrets

This environment has no secrets.

Manage environment secrets

Repository secrets

New repository secret

Name	Last updated	
AWS_ACCESS_KEY_ID	3 months ago	 
AWS_SECRET_ACCESS_KEY	3 months ago	 
VITE_GOOGLE_CLIENT_ID	2 months ago	 

Organization secrets

There are no organization secrets available to this repository.

CD 구축하기

AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY를 추가해주세요.

이후 .github의 변경사항을 포함한 PR을 올려 배포가 잘 되는지 확인해주세요.

Deploy에 실패했을 때

일일이 다시 PR을 올리지 않아도 workflow를 사용하여 다시 배포를 수행할 수 있습니다.

The screenshot shows the GitHub Actions interface for the repository '22-5-team1-web'. The left sidebar lists 'Actions' (ci, deploy-client), 'Management' (Caches, Attestations, Runners, Usage metrics, Performance metrics), and 'All workflows'. The main area displays 'All workflows' with a total of 662 workflow runs. A specific run for 'deploy-client' is highlighted with a red box, showing it was triggered by a commit ('deploy-client #119: Commit 8572a5d pushed by GlassyFoolze') and completed successfully ('Event: main', status: green, duration: 42s). Other runs for the same workflow are listed below, all showing similar details.

Workflow Run Details	Status	Duration	More Options
deploy-client #119: Commit 8572a5d pushed by GlassyFoolze	main	15 hours ago 42s	...
deploy-client #450: Commit 8572a5d pushed by GlassyFoolze	main	15 hours ago 46s	...
deploy-client #449: Pull request #357 synchronize by GlassyFoolze	feat/#356/GlassyFoolze	15 hours ago 1m 37s	...
deploy-client #448: Pull request #357 synchronize by GlassyFoolze	feat/#356/GlassyFoolze	2 days ago 52s	...
deploy-client #447: Pull request #357 synchronize by GlassyFoolze	feat/#356/GlassyFoolze	2 days ago 51s	...

Deploy에 실패했을 때

일일이 다시 PR을 올리지 않아도 workflow를 사용하여 다시 배포를 수행할 수 있습니다.

The screenshot shows the GitHub Actions details page for a workflow named 'deploy-client.yml' triggered by a push. The workflow has one job, 'Deploy', which is successful and completed in 33 seconds. A red box highlights the 'Re-run all jobs' button in the top right corner of the workflow card.

wafflestudio / 22-5-team1-web

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

You only have a single verified email address. We recommend verifying at least one more email address to ensure you can recover your account if you lose access to your primary email. Email settings

← deploy-client ✅ 아이디/비번 찾기 페이지 생성 #119 Re-run all jobs

Triggered via push 15 hours ago Status Success Total duration 42s Artifacts

GlassyFoolze pushed → 8572a5d main

Summary

Jobs Deploy

Run details

Usage

Workflow file

deploy-client.yml
on: push

Deploy 33s

Q&A

CORS

여러분은 앞으로 CORS를 꼭 한번은 겪게 될 것입니다

 Evan moon
<https://evan-moon.github.io> › 2020/05/21 › about-cors :

CORS는 왜 이렇게 우리를 힘들게 하는걸까?

2020. 5. 21. — 이번 포스팅에서는 웹 개발자라면 한번쯤은 얻어맞아 봤을 법한 **CORS(Cross-Origin Resource Sharing)** 정책에 대한 이야기를 해보려고 한다.

 Inpa Dev 🚧
<https://inpa.tistory.com> › entry › WEB-🎨-CORS-💯-정... :

악명 높은 CORS 개념 & 해결법 - 정리 끝판왕 - Inpa Dev

2022. 11. 28. — **CORS**를 해결하는 방법 총정리 · 1. Chrome 확장 프로그램 이용 · 2. 프록시 사이트 이용하기 · 3. 서버에서 Access-Control-Allow-Origin 헤더 세팅하기.

 티스토리
<https://teddy0.tistory.com> › ... :

CORS란 무엇인가? (그만 괴롭혀..) - 곰곰이 이해하는 프로그래밍

2024. 1. 9. — CORS(Cross Origin Resource Sharing). 이름 그대로 다른 출처의 자원의 공유에 대한 정책입니다. 다른 출처의 자원에 대해 SOP를 위반하지만 CORS 정책 ...

여러분은 앞으로 CORS를 꼭 한번은 겪게 될 것입니다

해결하는 방법은 정형화되어 있지만, 가끔 백엔드 문제인지 프론트 문제인지 헷갈릴 때가 있습니다.

스웨거에서는 되는데 사이트에서는 안 될 때에도 주로 CORS 문제일 가능성이 높습니다.

먼저 알아야 할 것: Origin

정보를 제공하는 주체를 Origin이라고 합니다.

보통 url에서 프로토콜과 호스트, 포트를 모두 합친 것을 Origin으로 규정합니다.

`https://github.com:443/pironeer-seminar/seminar-2025-1`

Same Origin Policy VS Cross Origin Policy

브라우저 - 서버 사이에 지켜야하는 내용 (== 정책 == Policy)

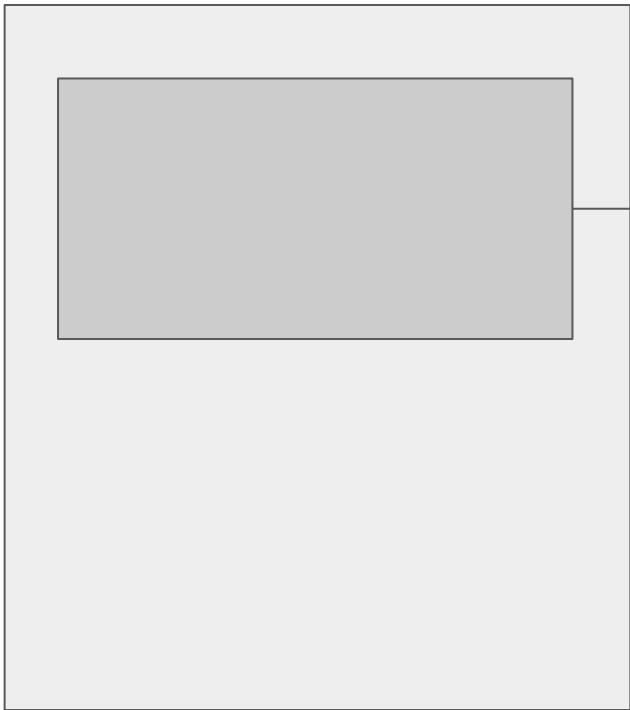
Same Origin Policy: 동일한 Origin에서의 데이터 전달에 대한 정책

Cross Origin Policy: 서로 다른 Origin에서의 데이터 전달에 대한 정책

★ 정책: 어떠한 서비스를 사용할 때 지켜야하는 내용

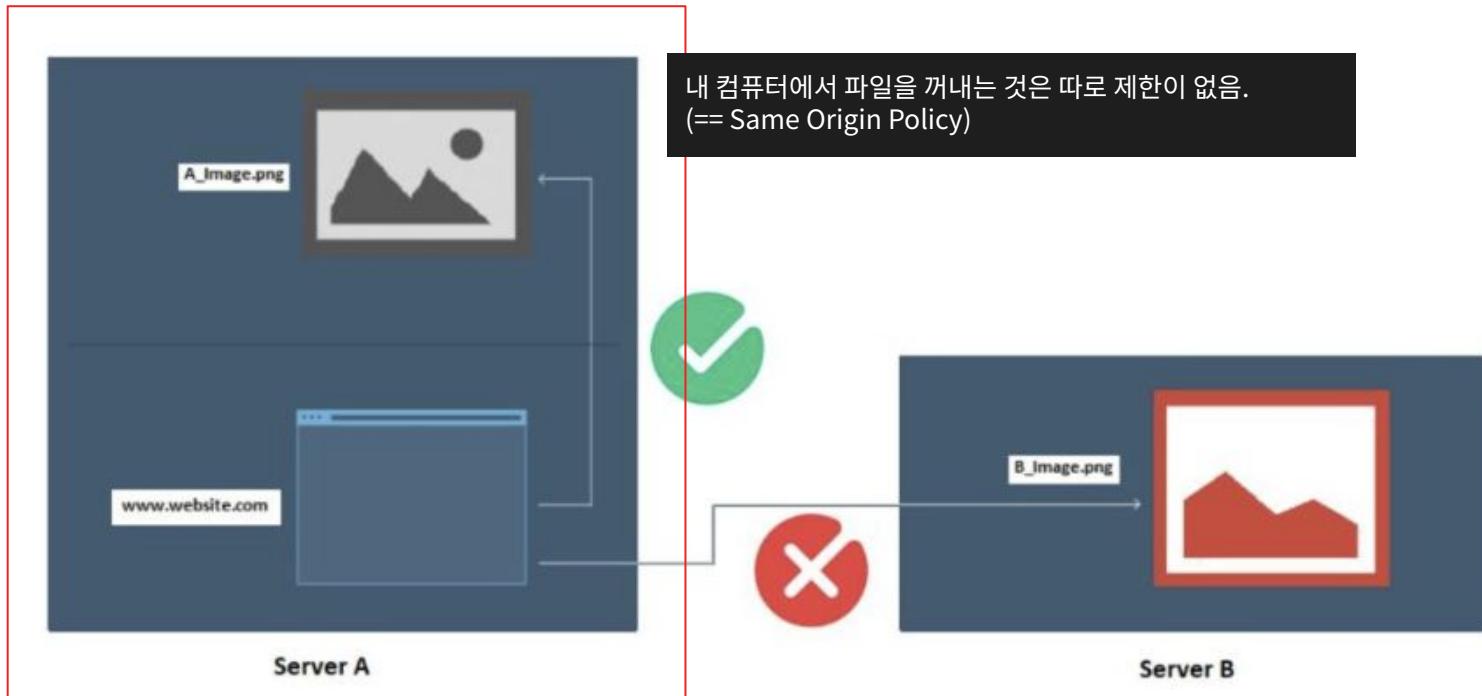
어떤 경우가 문제 될 수 있는가

<https://www.navar.com>
(피싱 사이트)

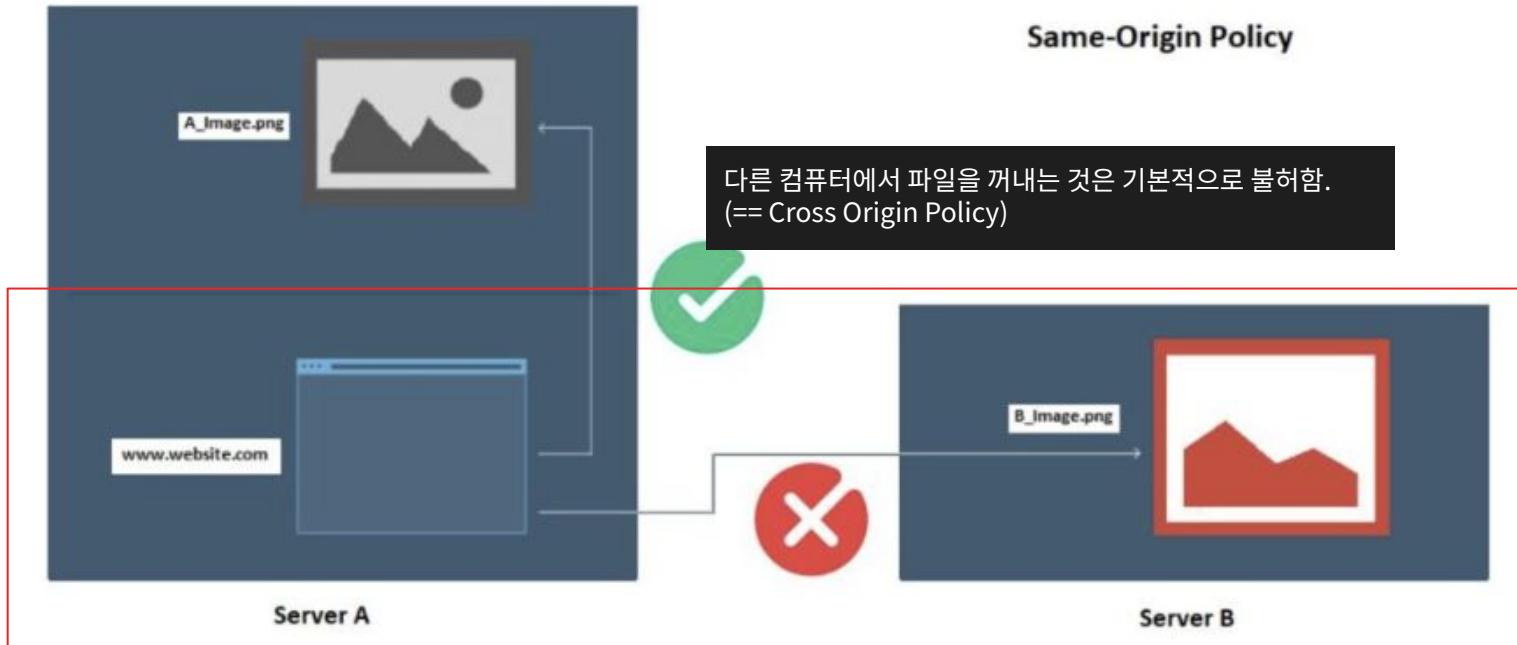


<https://www.naver.com>의 내용물을 iframe으로 보여준다.
-> 쉽게 사용자가 입력한 값을 탈취할 수 있음

Same Origin Policy VS Cross Origin Policy



Same Origin Policy VS Cross Origin Policy



피싱 사이트 문제 해결하기

<https://www.navar.com>
(피싱 사이트)

<https://www.naver.com>의 내용물을 iframe으로 보여준다.



하지만 현재 Origin은 www.naver.com이므로
“브라우저”에서 <https://www.naver.com> 서버가 허용한 Origin들
중에

navar가 있는지 확인해본다. (preflight)
만약 허용된 Origin이 아니라면 아예 본 요청 자체를 보내지 않는다.

-> 정보를 탈취하기 어려워진다.

브라우저 - 서버 요청 상황을 봅시다

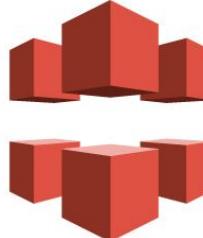
현재 url
<https://www.yeonu-blog.com>



index.html을 받아옴



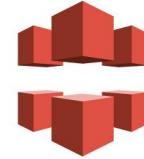
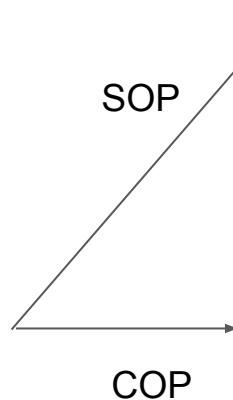
<https://www.yeonu-blog.com>
Cloudfront = 내 Origin로 인식



브라우저 - 서버 요청 상황을 봅시다

<https://www.yeonu-blog.com>
Cloudfront = 내 Origin으로 인식

요청하는 origin과 제공하는 origin이 서로 다릅니다.



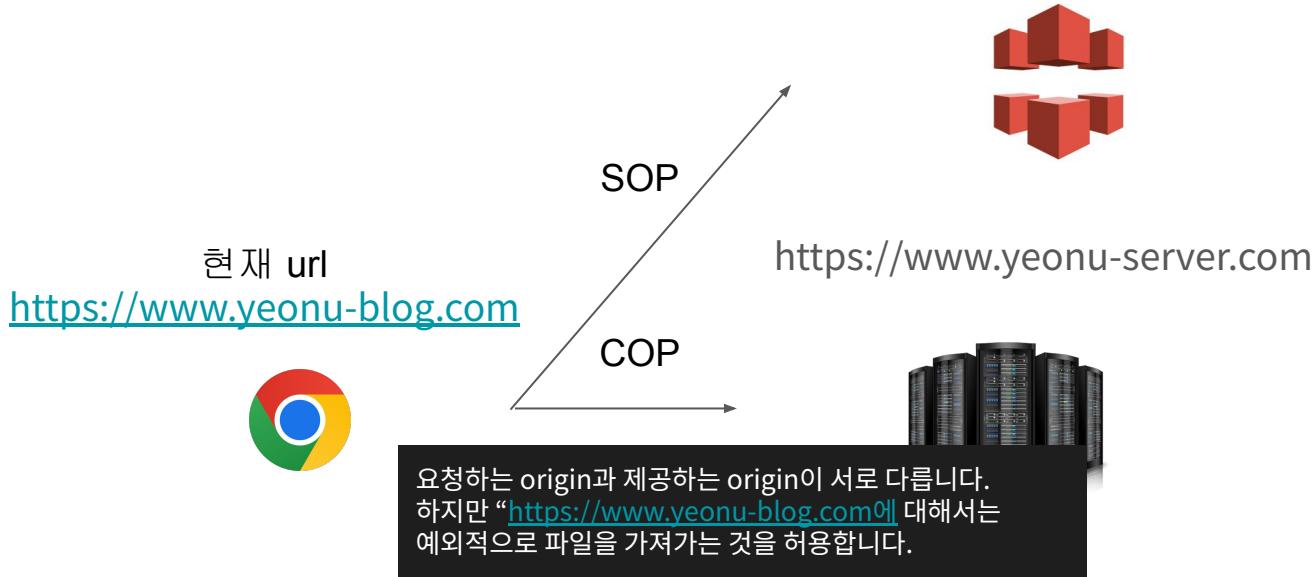
브라우저 - 서버 요청 상황을 봅시다

```
> fetch('https://google.com')
< ◀ Promise {<pending>}
✖ Failed to load https://google.com/: Redirect from flaviocopes.com/:1
  'https://google.com/' to 'https://www.google.it/?gfe_rd=cr&dcr=0&ei=TiDHWtehBcPCXprvpIgF'
  has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on
  the requested resource. Origin 'https://flaviocopes.com' is therefore not allowed access.
  If an opaque response serves your needs, set the request's mode to 'no-cors' to fetch the
  resource with CORS disabled.
✖ Uncaught (in promise) TypeError: Failed to fetch flaviocopes.com/:1
> |
```

그럼 어떻게 하죠..?

방법 1) 특정 origin에 대해서는 파일을 가져가도 된다고 “서버”에서 허용해주면 됩니다.

<https://www.yeonu-blog.com>



CORS에 대한 오해 - 서버에서 막하는 게 아니라, “브라우저”에서 막힌다

앞서 말했듯이 SOP, COP 등은 **브라우저와 서버** 사이에서 데이터를 교환하는 규칙입니다.

브라우저에서는 사전에 어떤 서버로부터 응답을 받는지 확인하여 본 요청의 실행을 제한합니다.

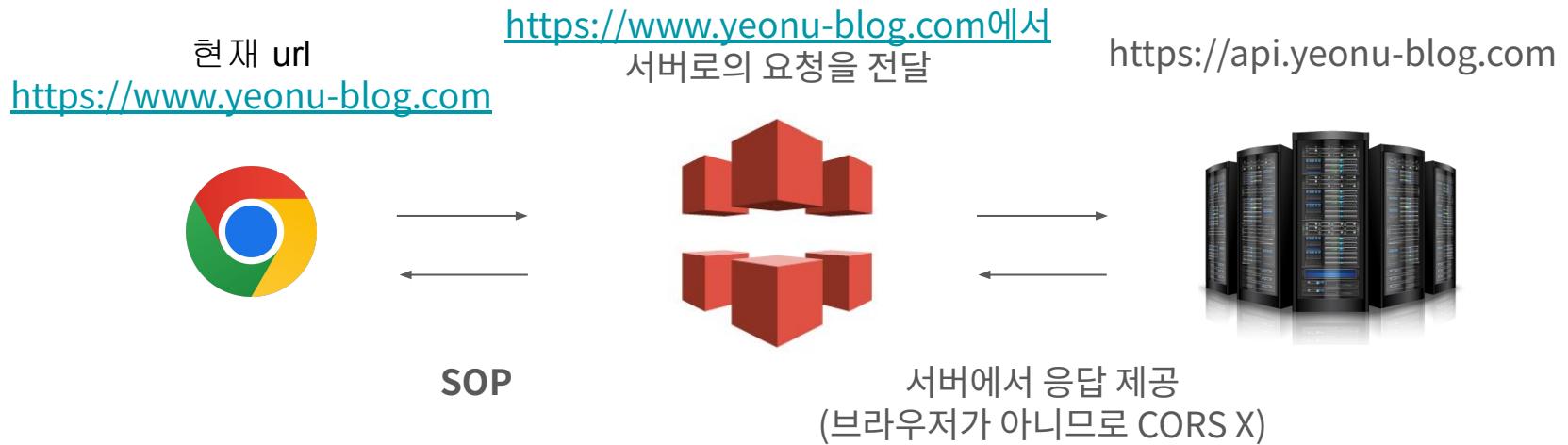
브라우저는 본 요청을 보내기 전 preflight 요청을 보내 유효한 Origin에 보내는지 확인하고, 유효하지 않다면 본 요청을 막아버립니다.

만약 브라우저에서 보내는 모든 응답의 Origin을 CDN 주소로 설정하고, CDN이 사이에서 서버로부터 응답을 받아온 뒤 브라우저로 전달한다면 CORS를 해결할 수 있습니다.

더 알아보고 싶다면: [요청의 종류](#)

그럼 어떻게 하죠..?

방법 2) 아니면 서버를 CDN(브라우저가 내 Origin라고 인식하는 곳) 뒤에 숨겨둡니다.
브라우저 사이에 CDN을 놓고 CDN을 거쳐 서버 응답을 받는다면 origin을 동일하게 맞춰줄 수도 있습니다.



CORS를 해결해봅시다! - 방법 1

서버 개발자 친구에게 카톡을 보냅니다.

CORS가 뜨는데, {프론트엔드 도메인명}과 {개발 환경에서의 URL, 아마도 `http://localhost:5173/`}에 대해 CORS를 풀어줘

라고 하면 서버 개발자 친구가 알아서 잘 허용해줄 것입니다.

CORS를 해결해봅시다! - 방법 2

CloudFront에서 /api로 끝나는 요청에 대해서는 모두 서버로 요청을 넘기도록 설정합니다.

지표 보기

일반 | 보안 | **원본** | 동작 | 오류 페이지 | 무효화 | 태그 | Logging**원본**

🔍 속성 또는 값을 기준으로 원본 필터링

| 원본 이름 ▾ | 원본 도메인 ▾ | 원본 경로 ▾ | 원본 유형 ▾ | Origin Shi... ▾ |

○ [Redacted] [Redacted] S3 -

편집

삭제

원본 생성

< 1 > ⚙

원본 그룹

🔍 속성이나 값을 기준으로 원본 그룹 필터링

| 원본 그룹 이름 ▾ | 원본 ▾ | 장애 조치 기준 ▾ |

원본 그룹 없음
원본 그룹이 없습니다.

원본 그룹 생성

편집

삭제

원본 그룹 생성

< 1 > ⚙

원본 생성

설정

Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#) ⓘ

 X

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

프로토콜 | 정보

- HTTP만 해당
- HTTPS만 해당
- 브이 일치

서버 도메인을 입력해줍니다.

만약 서버 도메인이 https로 배포되어 있다면 https 프로토콜,
http만 배포가 되어 있다면 http 프로토콜을 선택해주세요.

HTTPS port

Enter your origin's HTTPS port. The default is port 443.

443

Minimum Origin SSL protocol

The minimum SSL protocol that CloudFront uses with the origin.

- TLSv1.2
- TLSv1.1
- TLSv1
- SSLv3

- TLSv1
- SSLv3

Origin path - *optional*

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

Enter the origin path

이름

이 원본의 이름을 입력합니다.

api.yeonu-server.com

사용자 정의 헤더 추가 - 선택 사항

CloudFront는 원본으로 보내는 모든 요청에 이 헤더를 포함합니다.

헤더 추가

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

▶ 추가 설정

취소

원본 생성

지표 보기

일반 보안 원본

동작

오류 페이지

무효화

태그

Logging

동작

 속성 또는 값을 기준으로 동작 필터링

저장

위로 이동

아래로 이동

편집

삭제

동작 생성

우선 순위	경로 패턴	원본 또는 원본 그룹	뷰어 프로토콜 정책	캐시 정책 이름	원본 요청 정책 이름	응답 헤더 정책 이름
<input type="radio"/> 0	기본값(*)	[Redacted]	HTTP 및 HTTPS	Managed-CachingOptimized	-	-

동작 생성

설정

경로 패턴 | 정보

🔍 /api/* X

원본 및 원본 그룹

api.yeonu-server.com ▼

자동으로 객체 압축 | 정보

- No
 Yes

뷰어

https 배포가 되어 있다면 https only를 선택해도 됩니다.

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

▶ 미제작된 세션이나 모두 유저는 CloudFront에서 제공되는 모든 자원에 접근할 수 있습니다.

- 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.

CachingDisabled

Policy with caching disabled

Recommended for path pattern



[Create cache policy](#) [정책 보기](#)

원본 요청 정책 - 선택 사항

기존 원본 요청 정책을 선택하거나 새 정책을 생성합니다.

AllViewer

Policy to forward all parameters in viewer requests

Recommended for custom origins



[Create origin request policy](#) [정책 보기](#)

응답 헤더 정책 - 선택 사항

기존 응답 헤더 정책을 선택하거나 새 정책을 생성합니다.

응답 헤더 선택

[Create response headers policy](#)

▶ 추가 설정



CloudFront



배포

정책

함수

Static IPs

VPC 오리진

새로운 기능

▼ 원격 측정

모니터링

경보

로그

▼ 보고서 및 분석

캐시 통계

인기 객체

상위 레퍼러

사용량

뷰어

▼ 보안

원본 액세스

필드 수준 암호화

이름

origin request policy의 이름을 입력합니다.

set-cookies

설명 - 선택 사항

origin request policy에 대한 설명을 입력합니다.

Origin request settings 정보

기본적으로는 모든 헤더, 문자열, 쿠키가 무시됩니다.

헤더

원본 요청에 포함할 헤더를 선택합니다.

모든 뷰어 헤더

쿼리 문자열

원본 요청에 포함할 쿼리 문자열을 선택합니다.

모두

쿠키

원본 요청에 포함할 쿠키를 선택합니다.

모두

취소

생성

▶ 모든 리소스를 새 버전으로 업데이트 시킬 때마다 모든 리소스에 대한 요청은 구성을 사용하여 처리되며, 원본 서버는 리소스에 대한 요청을 처리합니다.

- 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.

CachingDisabled

Policy with caching disabled

Recommended for path pattern



[Create cache policy](#) [정책 보기](#)

커스텀한 request policy를 넣어줍니다.

원본 요청 정책 - 선택 사항

기존 원본 요청 정책을 선택하거나 새 정책을 생성합니다.

AllViewer

Policy to forward all parameters in viewer requests

Recommended for custom origins



[Create origin request policy](#) [정책 보기](#)

응답 헤더 정책 - 선택 사항

기존 응답 헤더 정책을 선택하거나 새 정책을 생성합니다.

응답 헤더 선택

[Create response headers policy](#)

커스텀 헤더가 있다면 해당 설정도 추가해줍니다.

▶ 추가 설정

응답 헤더 정책 생성

세부 정보

이름

response headers policy의 이름을 입력합니다.

설명 - 선택 사항

response headers policy에 대한 설명을 입력합니다.

교차 오리진 리소스 공유(CORS) - 선택 사항 [정보](#)

CORS 구성

보안 헤더 - 선택 사항 [정보](#)

Strict-Transport-Security [정보](#)

X-Content-Type-Options [정보](#)

X-Frame-Options [정보](#)

X-XSS-Protection 정보

Referrer-Policy 정보

Content-Security-Policy 정보

사용자 시정 헤더 - 선택 사항 정보

이름

값

오리진 재정의

제거

헤더 추가

헤더 제거 - 선택 사항 정보

헤더 추가

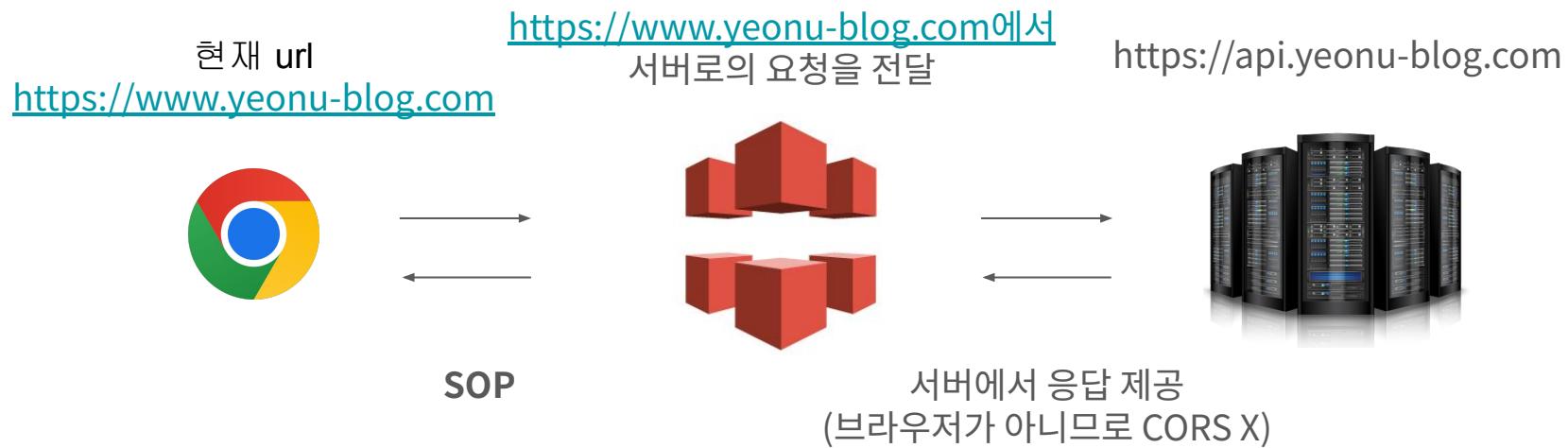
서버 타이밍 헤더 - 선택 사항 정보

활성화

CORS를 해결해봅시다! - 방법 2

이제 서버에서 별다른 설정을 하지 않아도 CORS 문제가 나타나지 않습니다.

하지만 개발 환경에서는 Cloudfront가 없는데 어떻게 설정하면 좋을까요?



CORS를 해결해봅시다! - 방법 2

Cloudfront 대신 vite가 생성한 개발 서버를 사용합니다.

참고) 개발 환경에서도 해당 url로 리소스를 받고 있으니 따로 vite가 서버를 띄워주고 있음을 알 수 있습니다.



```
// vite.config.ts

import react from '@vitejs/plugin-react-swc';
import path from 'path';
import { defineConfig } from 'vite';

// https://vitejs.dev/config/
export default defineConfig({
  plugins: [react()],
  server: {
    proxy: {
      '/api': {
        target: 'https://서버 도메인 or CloudFront 도메인/api',
        changeOrigin: true,
        secure: false,
      },
    },
  },
});
```

vite 개발 서버에서 api서버로부터 응답을 받아 브라우저로 제공해줍니다.

Q&A

과제 공지

과제 1: 스누인턴 2

공고를 확인할 수 있는 랜딩 페이지를 생성합니다.

이때 공고 필터링 및 찜하기 기능을 구현합니다. ([피그마 링크](#))

과제 1: 스누인턴 2

랜딩페이지: 공고를 3개씩 보여주고, 페이지네이션이 가능하도록 설계합니다.

페이지네이션 버튼은 5개씩만 보여줍니다.

회사 로고 이미지는 넣지 말고 그냥 블럭으로 처리해주세요

GET /api/post 요청을 사용합니다.

직군 필터

모집상태 ▾ 업종 ▾

최신순 ▾ ○ 초기화



레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...



레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

과제 1: 스누인턴 2

랜딩페이지: “직군필터” 클릭 시 원하는 직군만 선택할 수 있도록 합니다. (다중 선택 가능)

서버 요청 시에는 query parameter를 활용해주세요. (자세한 옵션은 뒤에 설명)

직군 필터



개발

- 전체
- 프론트엔드 개발
- 서버 · 백엔드 개발
- 앱 개발
- 기타 분야

기획

- 전체

디자인

- 전체

마케팅

- 전체

지역 ▾ 근무 형태 ▾ 기타 ▾

최신순 ▾ 초기화



레빗



과제 1: 스누인턴 2

랜딩페이지: “모집상태”, “업종”, “최신순”, “초기화” 버튼 클릭 시의 필터링도 구현해주세요.

서버 요청 시에는 query parameter를 활용해주세요. (자세한 옵션은 뒤에 설명)

직군 필터

모집상태 ▾ 업종 ▾

전체
 모집중

초기화 적용

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

 레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

< 1 2 3 4 5 >

과제 1: 스누인턴 2

쿼리 파라미터 사용시 유의사항

1. 반드시 URLSearchParams를 사용하여 인코딩해주세요
(한글, 특수기호 등이 깨질 수 있음.)
2. 여러개의 값을 합치실 때에도 URLSearchParams를 사용해주세요.

자세한 내용은 예시로 올려드린 [유틸함수](#)를 참고해주세요.

과제 1: 스누인턴 2

파라미터	타입	필수 여부	설명
positions	list(string)	필수 X	직무 카테고리 이름
isActive	boolean	필수 X	true: 모집 마감되지 않은 것만, false: 전체 (기본값: false)
order	int	필수 X (기본값: 0)	정렬 기준: 0 → 최신순 (updatedAt 기준), 1 → 마감순 (employmentEndDate 기준)
domains	list(string)	필수 X	도메인 이름 목록 (예: "EDUCATION", "FINTECH", 등)

e.g.

직무 프론트엔드 개발, 모집중인 것만, 도메인은 헬스테크

<https://www.example.com/?roles=FRONT&isActive=true&domains=HEALTHTECH>

직무 앱 개발 + 백엔드 개발

<https://www.example.com/?roles=BACKEND%2CAPP>
(%2는 인코딩 과정에서 들어가는 것이므로 임의로 넣지 말것)

과제 1: 스누인턴 2

직무 카테고리 이름

개발: FRONT, APP, BACKEND, DATA, OTHERS

(개발 전체 선택 시 5개 모두 query parameter로 전달)

디자인: DESIGN

기획: PLANNER

마케팅: MARKETING,

직군 필터

^

개발

- 전체
- 프론트엔드 개발
- 서버 · 백엔드 개발
- 앱 개발
- 기타 분야

기획

- 전체

디자인

- 전체

마케팅

- 전체

지역 ▾ 근무 형태 ▾ 기타 ▾

최신순 ▾ 초기화



레빗



과제 1: 스누인턴 2

도메인 이름 목록

'FINTECH', 'HEALTHTECH', 'EDUCATION', 'ECOMMERCE',
'FOODTECH', 'MOBILITY', 'CONTENTS', 'B2B', 'OTHERS',

과제 1: 스누인턴 2

전체적으로 쿼리 파라미터가 돌아가는 방식을 보다 쉽게 이해하고 싶다면
[위 링크](#)로 들어가서 체험해보세요.

과제 1: 스누인턴 2

추가 스펙 1. 페이지네이션을 클릭했을 때에도 필터가 고정되도록 구현해주세요.
만약 필터를 새로 누르셨다면 페이지네이션이 다시 1로 돌아오도록 구현해주세요.

과제 1: 스누인턴 2

랜딩페이지: 로그인 이후 “찜하기” 여부에 따라 북마크 표시가 다르게 보이도록 해주세요.
이때 북마크 버튼을 클릭했을 때 찜하기 또는 찜하기 해제가 수행되도록 해주세요.

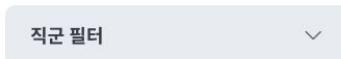
이미 찜한 북마크 클릭 -> 찜하기 해제

아직 찜하지 않은 북마크 클릭 -> 찜하기

찜하기는 [POST api/post/{post_id}/bookmark](#)

찜하기 해제는 [DELETE api/post/{post_id}/bookemark](#)

를 사용해주세요.



모집상태 ▾ 업종 ▾

최신순 ▾ C 초기화

 레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

 레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

과제 1: 스누인턴 2

랜딩페이지: 만약 로그인하지 않았다면 모든 북마크가 해제된 상태로 보이도록 해주세요.
이때 찜하기 버튼을 클릭하면 로그인 유도 모달이 나타나도록 해주세요.

직군 필터

모집종 ▾ 업종 ▾

최신순 ▾ C 초기화

레브잇

찜하기를 하려면 로그인이 필요해요

계정이 없으시다면
지금 바로 회원가입해보세요

로그인하기

뒤로 가기

레브잇

React Frontend Developer

교육

마감까지 D-12

최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

< 1 2 3 4 5 >

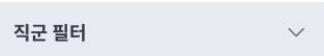
과제 1: 스누인턴 2

추가 스펙 2: 필터 포커싱

- 필터가 적용되면 진하게 표시
- 하나만 선택 가능하면 (모집중 OR 최신순) 어떤 것을 선택했는지 보이도록 하기
- 여러개 선택 가능하면 그냥 진하게만 표시하기

추가 스펙 3: 필터 저장

적용한 필터 및 페이지네이션이 새로고침해도 유지되도록 설정하기



레브잇
React Frontend Developer
교육
마감까지 D-12
최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

레브잇
React Frontend Developer
교육
마감까지 D-12
최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 혁신합니다. 최신 LLM 오픈 소스 모델과 자체개발 멀티모달 AI를 이용하여 초콜릿 쿠키 업계를 ...

과제 1: 스누인턴 2

API 상세
GET api/post

로그인한 경우에는 header에 JWT를 담고,
그렇지 않은 경우에는 빈 상태로 요청 보내기

적절한 Query parameter 사용

Request

```
{  
    "posts": [  
        {  
            "id": "string", // post id (찜하기 기능에서 사용)  
            ...  
            "companyName": "string", // 회사 이름  
            ...  
            "employmentEndDate": "2025-10-17T13:31:03.134Z", // 마감일  
            "positionTitle": "string", // e.g. React Frontend 개발자  
            "domain": "FINTECH",  
            "slogan": "string", // 카드 하단에 들어갈 한 줄 소개  
            ...  
            "headCount": 0, // 모집 인원수  
            "isBookmarked": true, // 북마크 여부 (로그인하지 않으면 모두 false)  
            ...  
        }  
    ],  
    "paginator": {  
        "lastPage": 0  
    }  
}
```

Response

과제 1: 스누인턴 2

API 상세

POST api/post/{post_id}/bookmark

header에 JWT 담아서 보내주기

post id를 path parameter로 넣어주기

없음 .

Request

Response

과제 1: 스누인턴 2

API 상세

DELETE api/post/{post_id}/bookmark

header에 JWT 담아서 보내주기

post id를 path parameter로 넣어주기

없음 .

Request

Response

과제 1: 스누인턴 2

11/7 (금) 오후 8시 전까지 깃허브 링크과 배포링크를 “Frontend-잡담”에 업로드해주세요.
조원이 세 명인 조에서는 추가 스펙 하나를 포함하여 구현해주세요.

이번 과제는 스펙이 상당합니다. 거의 3주 동안 구현하므로 미리미리 해두시는 것을 추천드립니다.

참고 깃허브: [스누인턴 웹 클라이언트](#)

과제 2: 조원들과 모각작하기

11/7 오후 8시 전까지 조원들과 함께 모각작 인증샷을 찍어 “Frontend-잡담”에 업로드해주세요.