



포팅메뉴얼

Docker 환경 구축

S3 bucket 생성 및 IAM 설정

S3 버킷 생성

S3 버킷 정책 편집

IAM 생성

Naver mail 설정

O:RE BE 서버 구축

- 1 Git Clone
- 2 `env.example.txt` 환경 변수 설정
- 3 `.env` 파일 생성
- 4 docker image 빌드 및 컨테이너 생성

ORE App 다운로드 및 가이드

- 1 O:RE App 다운로드
- 2 ORE.exe 실행
- 3 구축된 서버 도메인 입력
- 4 관리자 회원가입 또는 로그인

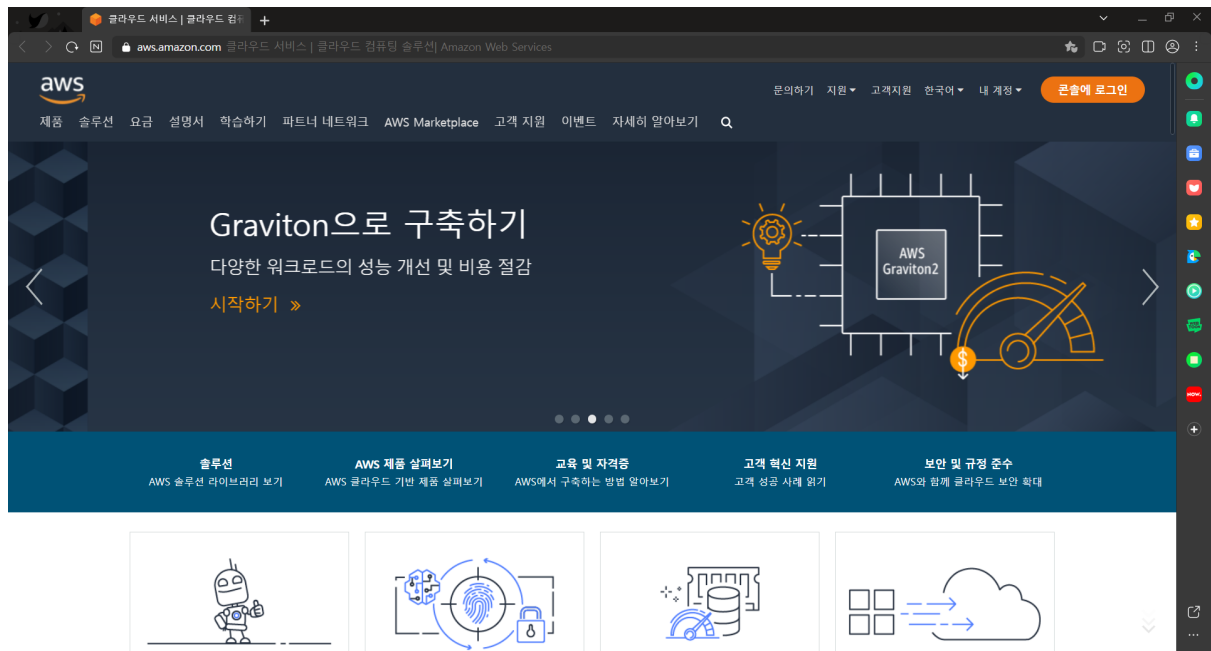
Docker 환경 구축

아래 사이트를 이용하여 docker 및 docker-compose 환경구축

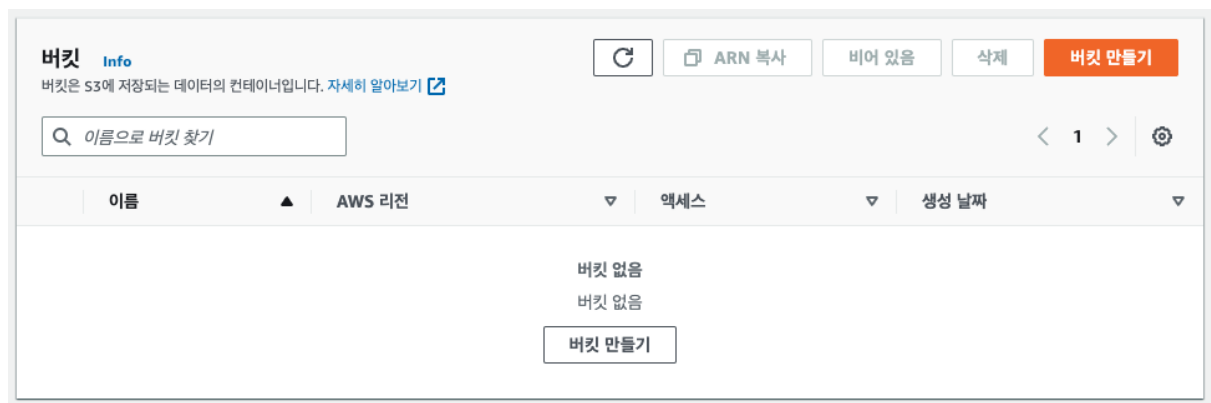
```
https://docs.docker.com/engine/install/  
https://docs.docker.com/compose/install/
```

S3 bucket 생성 및 IAM 설정

S3 버킷 생성



AWS 접속



S3 대시보드 접속 후 버킷 만들기 클릭

버킷 만들기 Info

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

일반 구성

버킷 이름

myawsbucket

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

AWS 리전

아시아 태평양(서울) ap-northeast-2

기존 버킷에서 설정 복사 - 선택 사항

다음 구성의 버킷 설정만 복사됩니다.

버킷 선택

버킷 이름 및 리전 설정

이 버킷의 퍼블릭 액세스 차단 설정

퍼블릭 액세스는 ACL(엑세스 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 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(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.



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.

퍼블릭 액세스 권한 설정

버킷 버전 관리

버전 관리는 객체의 여러 버전을 동일한 버킷에서 관리하기 위한 수단입니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 객체의 각 버전을 보존, 검색 및 복원할 수 있습니다. 버전 관리를 통해 의도치 않은 사용자 작업과 애플리케이션 장애를 모두 복구할 수 있습니다. [자세히 알아보기](#)

버킷 버전 관리

- ☒ 비활성화
☐ 활성화

태그 (0) - 선택 사항

버킷 태그를 사용하여 스토리지 비용을 추적하고 버킷을 구성할 수 있습니다. [자세히 알아보기](#)

이 버킷과 연결된 태그가 없습니다.

태그 추가


기본 암호화

이 버킷에 저장된 새 객체를 자동으로 암호화합니다. [자세히 알아보기](#)

서버 측 암호화

- ☒ 비활성화
☐ 활성화

▶ 고급 설정

 버킷을 생성한 후 파일과 폴더를 해당 버킷에 업로드할 수 있고, 추가 버킷 설정도 구성할 수 있습니다.

취소

버킷 만들기

버킷 생성

S3 버킷 정책 편집

정책생성기

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) arn:aws:s3::버킷이름/*

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

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

[Add Statement](#)

Actions : GetObject만 선택

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

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3::버킷이름/*	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](#)

Generate Policy 선택

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": "Policy1668688568072",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1668688529081",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::버킷이름/*",
      "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 technologies.

Close

내용 복사

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:::ore-s3

정책

1

문 편집

문 선택

정책에서 기존 문을 선택하거나 새 문을 추가합니다.

+ 새 문 추가

버킷 정책 편집

포팅메뉴얼

6

IAM 생성

IAM > 사용자

사용자 (0) 정보

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

새 사용자 추가

삭제

새 사용자 추가

사용자 이름 또는 액세스 키로 사용자 찾기

< 1 > ⓘ

사용자 이름	그룹	마지막 활동	MFA	암호 수명	활성 키 수명
표시할 리소스 없음					

IAM 대시보드 접속 및 사용자추가

사용자 추가

1 2 3 4 5

사용자 세부 정보 설정

동일한 액세스 유형 및 권한을 사용하여 한 번에 여러 사용자를 추가할 수 있습니다. [자세히 알아보기](#)

사용자 이름*

다른 사용자 추가

AWS 액세스 유형 선택

이러한 사용자가 주로 AWS에 액세스하는 방법을 선택합니다. 프로그래밍 방식의 액세스만 선택하면 사용자가 위임된 역할을 사용하여 콘솔에 액세스하는 것을 방지할 수 없습니다. 액세스 키와 자동 생성된 암호가 마지막 단계에서 제공됩니다. [자세히 알아보기](#)

- AWS 자격 증명 유형 선택*

☐ 액세스 키 – 프로그래밍 방식 액세스

AWS API, CLI, SDK 및 기타 개발 도구에 대해 액세스 키 ID 및 비밀 액세스 키 을(들) 활성화합니다.

☐ 암호 – AWS 관리 콘솔 액세스

사용자가 AWS Management Console에 로그인할 수 있도록 허용하는 비밀번호 을(들) 활성화합니다.

* 필수

취소


다음: 권한


사용자 이름 작성 및 AWS 자격 증명 유형 액세스키 선택


사용자 추가

1 2 3 4 5

▼ 권한 설정

 그룹에 사용자 추가

 기존 사용자에서 권한 복사

 기존 정책 직접 연결

정책 생성 정책 필터 1 결과 표시

▶ 권한 경계 설정

취소 이전 다음: 태그

S3FullAccess 정책 추가

사용자 추가

1 2 3 4 5



성공

아래에 표시된 사용자를 생성했습니다. 사용자 보안 자격 증명을 보고 다운로드할 수 있습니다. AWS Management Console 로그인을 위한 사용자 지침을 이메일로 보낼 수도 있습니다. 지금이 이 자격 증명을 다운로드할 수 있는 마지막 기회입니다. 하지만 언제든지 새 자격 증명을 생성할 수 있습니다.

AWS Management Console 액세스 권한이 있는 사용자가 <https://783226195545.signin.aws.amazon.com/console>에 로그인할 수 있습니다.

다운로드 .csv 다운로드

	사용자	액세스 키 ID	비밀 액세스 키
▶	oreAdmin		***** 표시

닫기

사용자추가 완료

Naver mail 설정

환경 설정

- 기본 설정
- 메일함관리
- 메일 자동분류
- 서명/빠른 답장
- 부재 중 설정
- 새 메일 알림
- 스팸 설정
- 외부메일 가져오기
- POP3/IMAP 설정
- 단축키

POP3/SMTP 설정

IMAP/SMTP 설정

POP3/SMTP 사용

- ☒ 사용함 ☐ 사용 안 함

스마트폰, 아웃룩 등에서 네이버 메일을 확인할 수 있도록 POP3/SMTP를 설정합니다.

적용 범위

- ☐ 지금부터 새로 받는 메일만 받음 ☒ 기존에 받은 메일을 포함하여 받음

읽음 표시

- ☒ POP3로 읽어간 메일을 읽음 표시 ☐ POP3로 읽어간 메일을 읽지 않음으로 표시

원본 저장

- ☒ 네이버 메일에 원본 저장 ☐ 메일 프로그램 설정에 따라 저장 또는 삭제

외부메일 처리

- ☒ POP3로 읽어갈 때 외부메일을 포함하지 않음 ☐ POP3로 읽어갈 때 외부메일을 포함

기본 설정으로 되돌리기

취소

저장

- POP3/SMTP 사용함 설정

O:RE BE 서버 구축

1 Git Clone

```
git clone https://lab.ssafy.com/s07-final/S07P31A504
cd S07B31A504
```

2 env.example.txt 환경 변수 설정

```
# Domain of service
DOMAIN=도메인주소

# Mysql
MYSQL_ROOT_PASSWORD=root계정 비밀번호
MYSQL_USER=생성할 유저명
MYSQL_PASSWORD=유저 비밀번호
MYSQL_DATABASE=생성할 DATABASE 이름

# S3
REGION=s3 지역
ACCESS_KEY=S3 IAM access key
```

```
SECRET_KEY=S3 IAM secret key  
BUCKET=S3 Bucket이름
```

```
# mail - naver 계정만 가능  
MAIL_USERNAME=naver아이디  
MAIL_PASSWORD=naver비밀번호
```

3 파일 생성

```
cp env.example.txt .env
```

4 docker image 빌드 및 컨테이너 생성

```
docker-compose up -d
```

ORE App 다운로드 및 가이드

1 O:RE App 다운로드

 [다운받기](#)

2 ORE.exe 실행

3 구축된 서버 도메인 입력

4 관리자 회원가입 또는 로그인