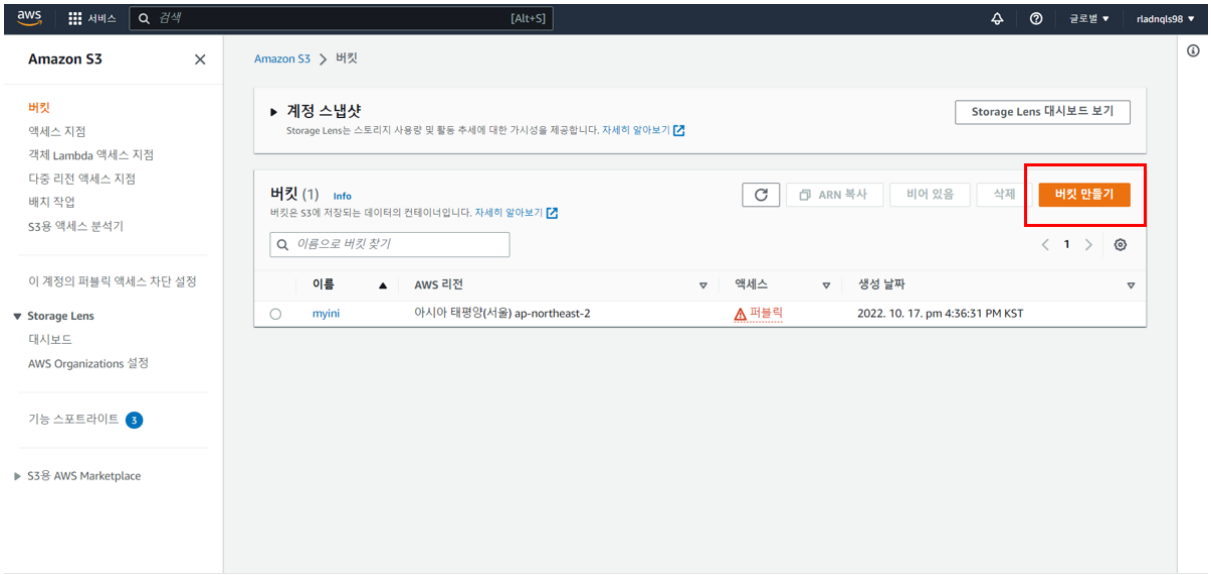
S3 가이드

목차

1. S3 버킷 등록

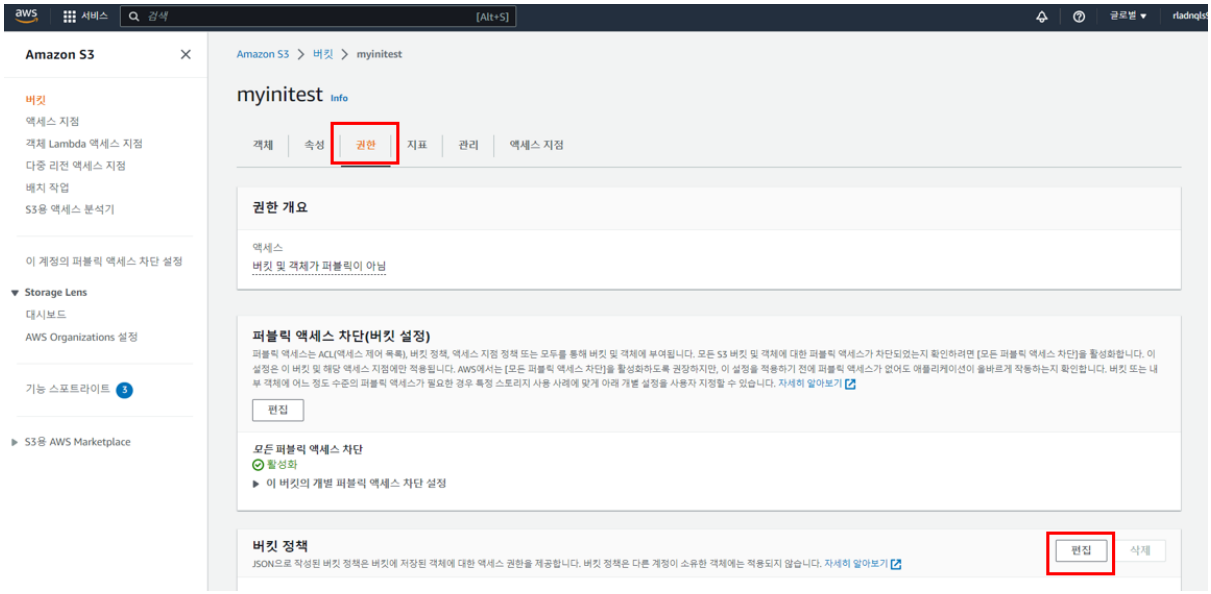
1.1. 버킷 생성

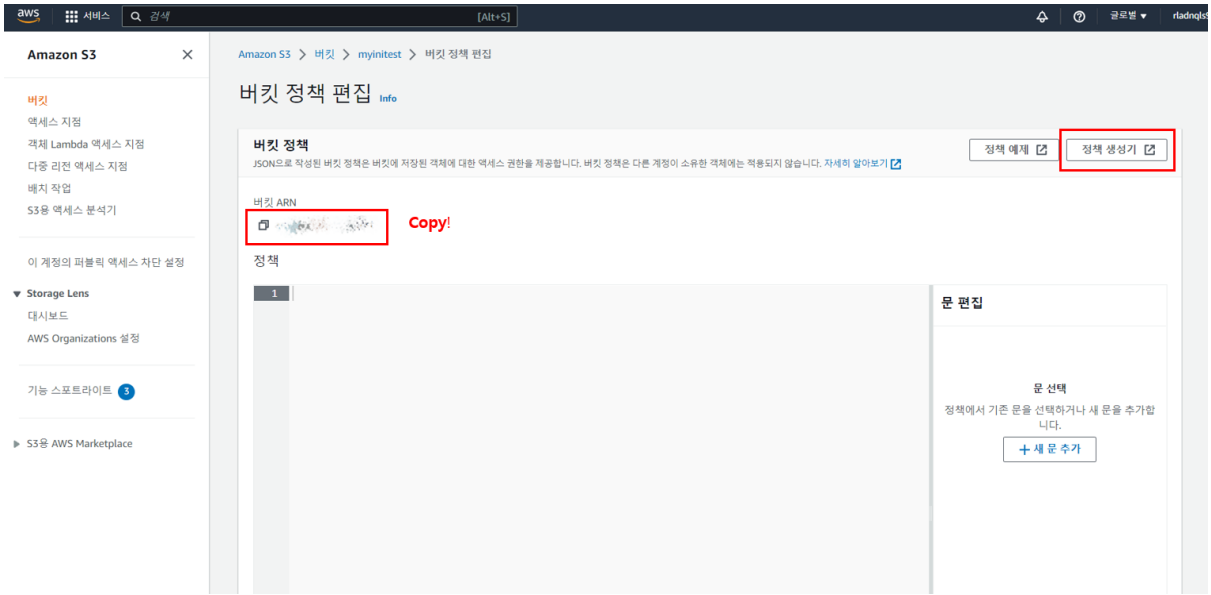
AWS S3에 접속해 버킷을 생성합니다.

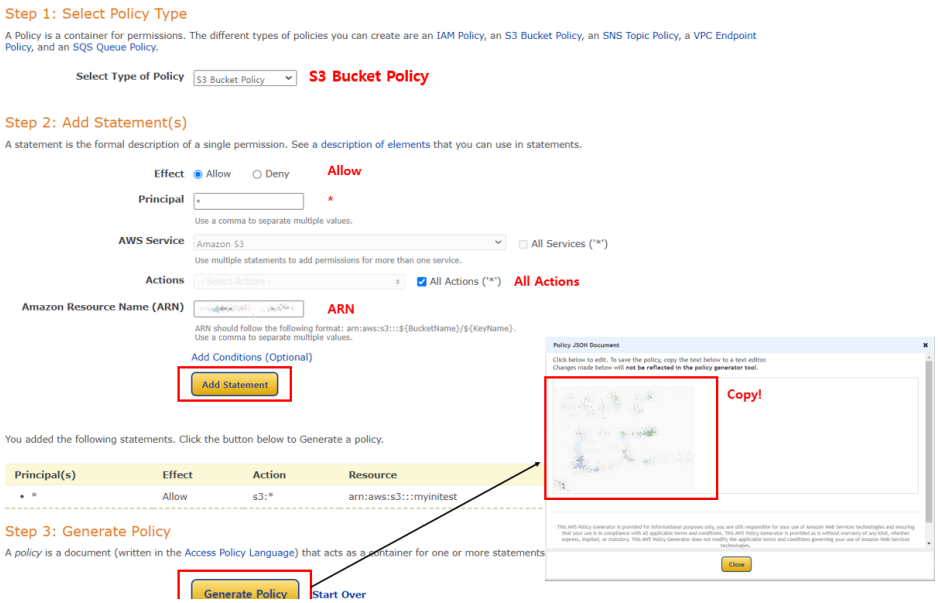


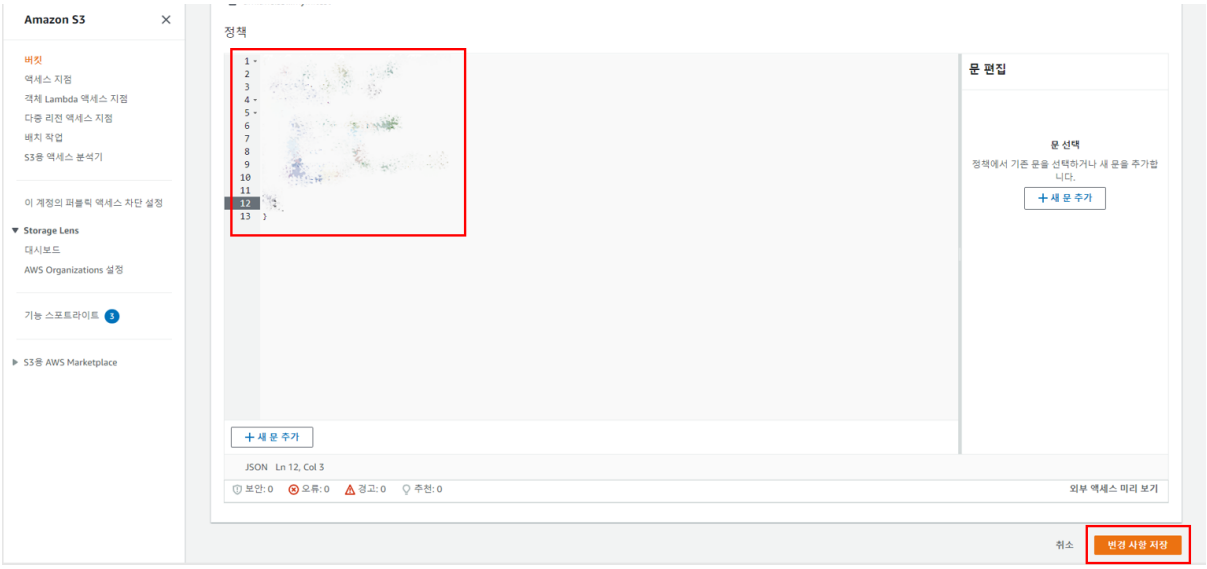
1.2. 정책등록

S3 버킷정책을 등록합니다.


Amazon S3
버킷
액세스 지점
객체 Lambda 액세스 지점
다중 리전 액세스 지점
배치 작업
S3용 액세스 분석기
이 계정의 퍼블릭 액세스 차단 설정
Storage Lens
대시보드
AWS Organizations 설정
기능 스포트라이트
S3용 AWS Marketplace
Amazon S3 > 버킷 > myinitest
myinitest Info
객체
속성
권한
지표
관리
액세스 지정
권한 개요
액세스
버킷 및 객체가 퍼블릭이 아님
퍼블릭 액세스 차단(버킷 설정)
편집
모든 퍼블릭 액세스 차단
활성화
이 버킷의 개별 퍼블릭 액세스 차단 설정
버킷 정책
편집
삭제


Amazon S3
버킷
액세스 지정
객체 Lambda 액세스 지정
다중 리전 액세스 지정
배치 작업
S3용 액세스 분석기
이 계정의 퍼블릭 액세스 차단 설정
Storage Lens
대시보드
AWS Organizations 설정
기능 스포트라이트
S3용 AWS Marketplace
Amazon S3 > 버킷 > myinitest > 버킷 정책 편집
버킷 정책 편집 Info
버킷 정책
정책 예제
정책 생성기
버킷 ARN
Copy!
정책
문 편집
문 선택
정책에서 기존 문을 선택하거나 새 문을 추가합니다.
+ 새 문 추가

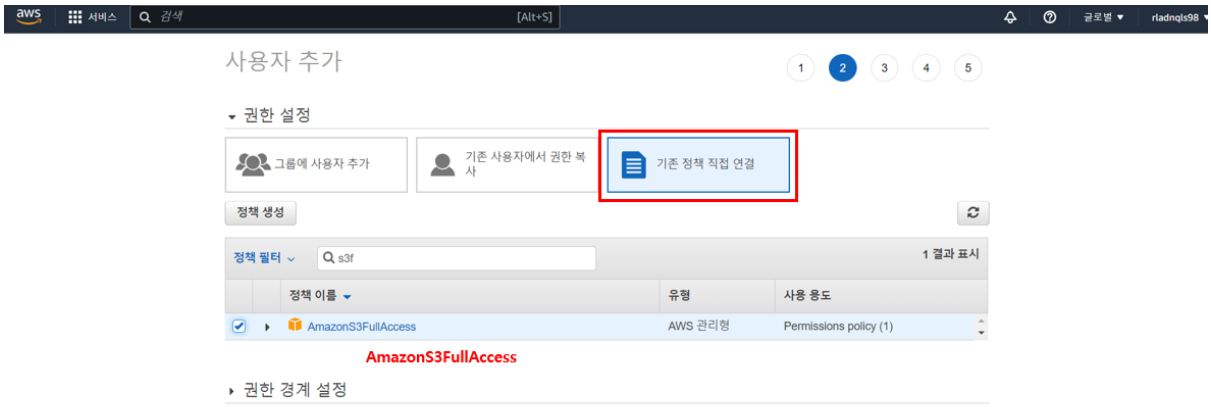

Step 1: Select Policy Type
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.
Select Type of Policy
S3 Bucket Policy
S3 Bucket Policy
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Allow
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
All Actions ('*')
All Actions
Amazon Resource Name (ARN)
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
*
Allow
s3:*
arn:aws:s3:::myinitest
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
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.
Copy!
Close



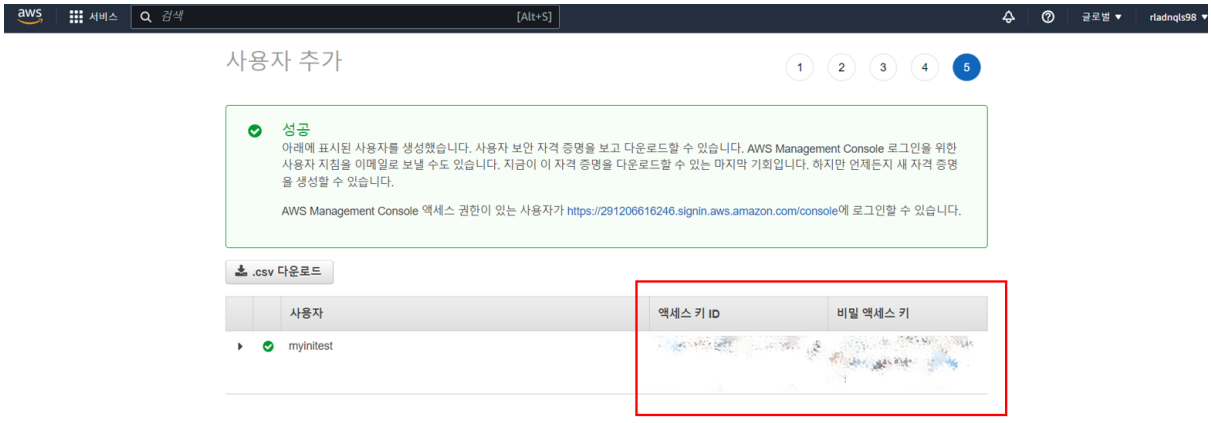
2. S3 IAM 등록

2.1. 사용자 등록


서비스
검색
[Alt+S]
글로벌
rladnqls98
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*
myinitest
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(를) 활성화합니다.
암호 – AWS 관리 콘솔 액세스
사용자가 AWS Management Console에 로그인할 수 있도록 허용하는 비밀번호 을(를) 활성화합니다.


서비스
검색
[Alt+S]
글로벌
rladnqls98
사용자 추가
1 2 3 4 5
권한 설정
그룹에 사용자 추가
기존 사용자에서 권한 복사
기존 정책 직접 연결
정책 생성
정책 필터
s3f
1 결과 표시
정책 이름
유형
사용 용도
AmazonS3FullAccess
AWS 관리형
Permissions policy (1)
AmazonS3FullAccess
권한 경계 설정

2.2. 액세스 키 복사


서비스
검색
[Alt+S]
글로벌
rladnqls98
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://291206616246.signin.aws.amazon.com/console에 로그인할 수 있습니다.
.csv 다운로드
사용자
액세스 키 ID
비밀 액세스 키
myinitest

3. build.gradle 설정

```
implementation 'org.springframework.cloud:spring-cloud-starter-aws:2.2.6.RELEASE'
```

4. application.yml 설정

```
cloud:
  aws:
    credentials:
      accessKey: #액세스 키
      secretKey: #비밀 액세스 키
    s3:
      bucket: #버킷이름
      path: #버킷주소
    region:
      static: ap-northeast-2
      auto: false
    stack:
      auto: false
```