

## Lab2. IAM User, Group 생성 및 역할 다루기

### 목적

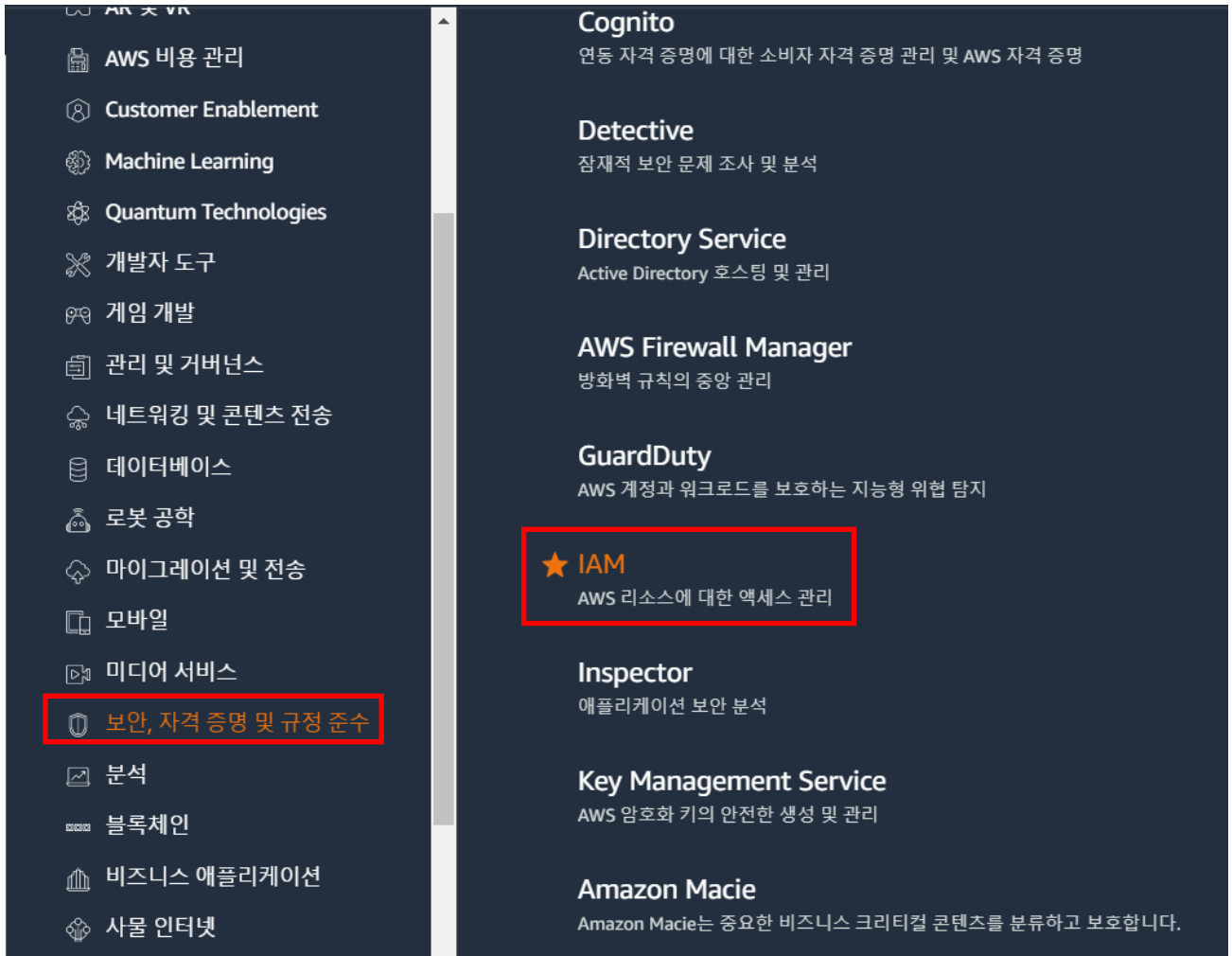
이번 실습에서는 Amazon IAM의 사용 방법을 배우기 위해 IAM User와 Group을 생성하고, 생성된 계정에 대해 역할 정책을 할당하는 방법을 다룬다. 또한 별도의 계정을 생성해서 접속 정보를 할당하여, 다른 사용자에게 전달하고, 전달된 계정으로 로그인하는 방법과 권한에 대해 확인과 교차 설계 방법에 대해 실습한다. 두번째 실습에서는 IAM의 역할 정책에 대한 활용 방법을 다룬다. EC2 인스턴스에 IAM 역할을 활용하여 S3에 접근 권한을 부여하고, 이를 통해 S3에 대한 접근 권한을 획득하는 방법을 다룬다.

### 사전 준비물

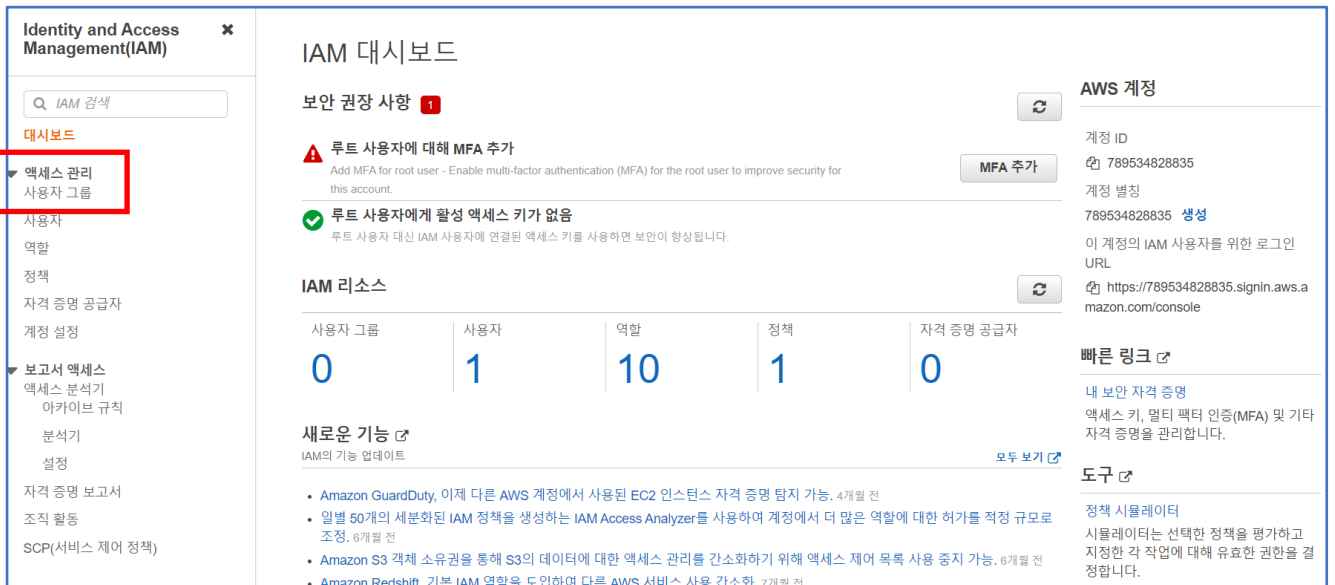
AWS Free-Tier 계정

# IAM User 및 Group 생성

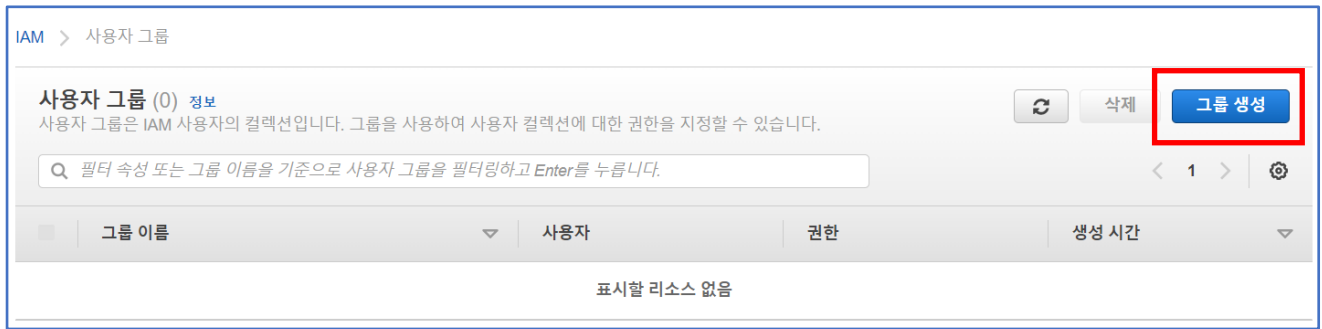
1. [서비스] > [보안, 자격 증명 및 규정 준수] > [IAM] 메뉴를 클릭한다.



2. [IAM 대시보드] 페이지이다. [액세스 관리] > [사용자 그룹] 메뉴를 클릭한다.



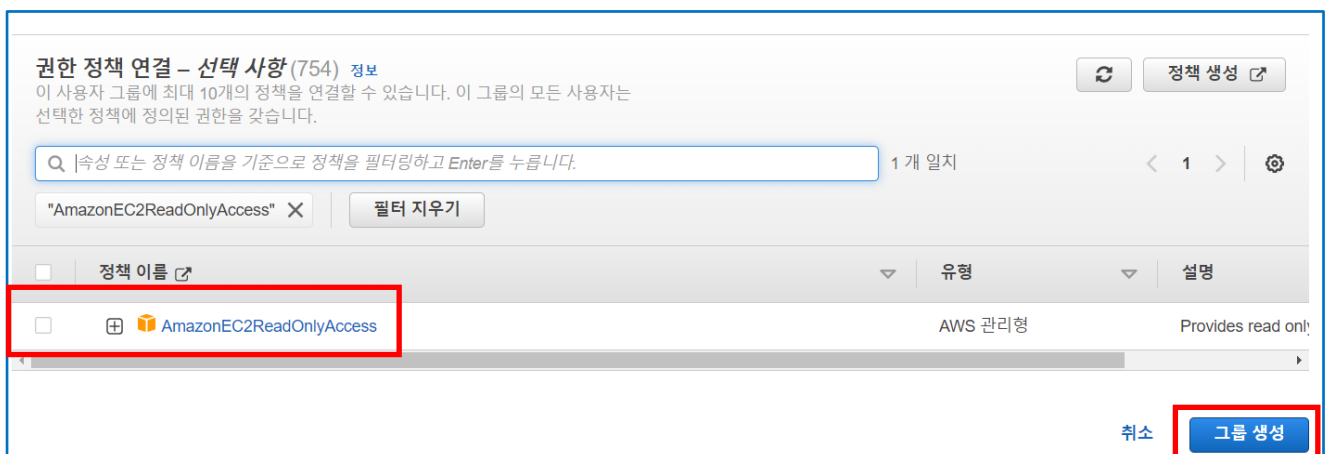
3. [사용자 그룹] 페이지에서 [그룹 생성] 버튼을 클릭한다.



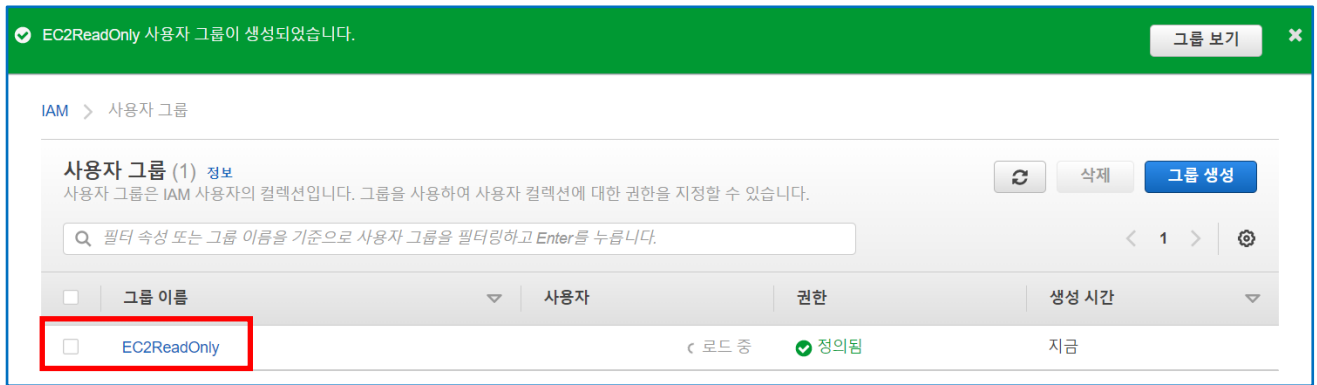
4. [사용자 그룹 생성] 페이지에서, [사용자 그룹 이름]을 EC2ReadOnly로 입력한다.



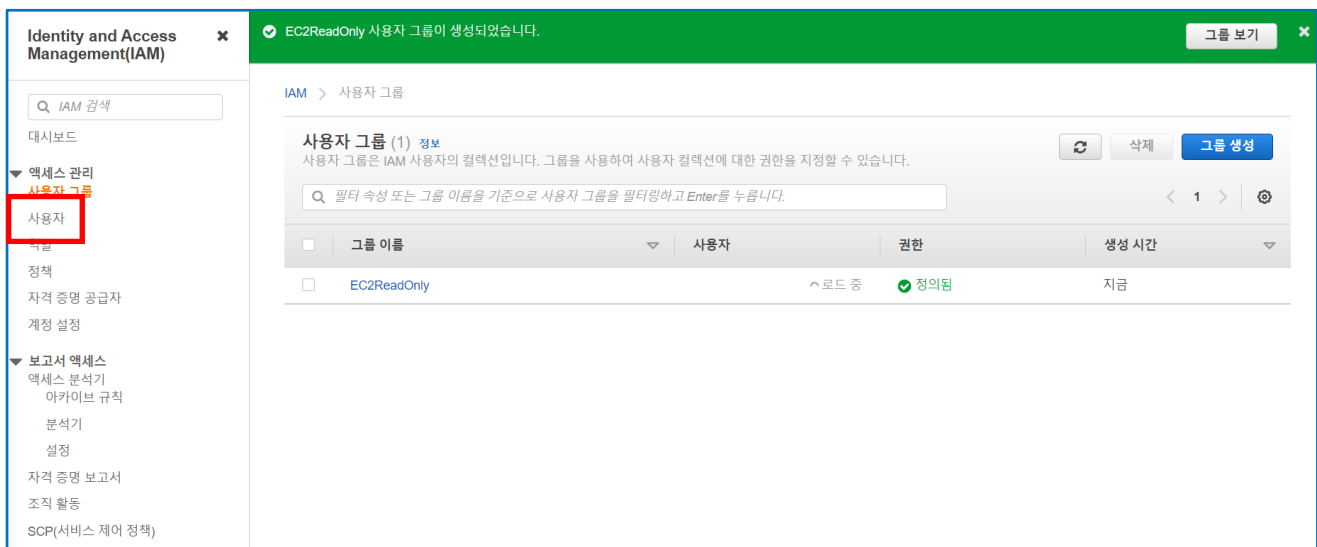
5. 페이지를 아래로 스크롤다운하여 [권한 정책 연결] 섹션에서 필터 검색에서 AmazonEC2ReadOnlyAccess를 입력해서 검색 결과로 나온 [정책 이름]에서 AmazonEC2ReadOnlyAccess 체크한 후, [그룹 생성]을 클릭한다.



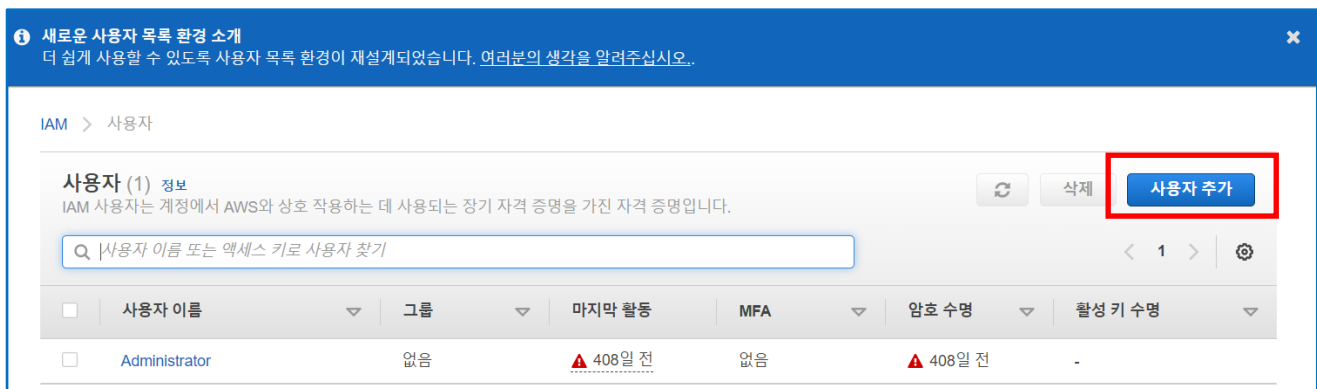
6. [사용자 그룹] EC2ReadOnly가 생성되었다.



7. [IAM] 페이지 좌측 메뉴 중 [사용자]를 클릭한다.



8. [사용자] 페이지에서 [사용자 추가] 파란색 버튼을 클릭한다.



9. [사용자 추가] 페이지에서 [사용자 이름]에 AWS\_User를 입력한다.

10. 페이지를 아래로 스크롤다운하여 [AWS 액세스 유형 선택] 섹션에서 다음의 각 값을 설정한 후, [다음: 권한]을 클릭한다.


A. [AWS 자격 증명 유형 선택] : 암호 – AWS 관리 콘솔 액세스


B. [콘솔 비밀번호] : 사용자 지정 비밀번호 / Suwon#AWS0307


C. [비밀번호 재설정 필요] : 체크 해제

11. [권한 설정] 섹션에서 [그룹에 사용자 추가]를 선택하고, [그룹에 사용자 추가] 섹션에 EC2ReadOnly 체크하고 [다음: 태그]를 클릭한다.

▼ 권한 설정

 그룹에 사용자 추가

 기존 사용자에서 권한 복사

 기존 정책 직접 연결

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

### 그룹에 사용자 추가

그룹 생성

↺ 새로 고침

Q 검색

1 결과 표시

그룹	연결된 정책
<input checked="" type="checkbox"/> EC2ReadOnly	AmazonEC2ReadOnlyAccess

▶ 권한 경계 설정

취소

이전

다음: 태그

12. [태그 추가(선택 사항)] 섹션에서 [키]를 Name으로, [값]을 lab-iam-user로 입력하고 [다음: 검토]를 클릭한다.

### 태그 추가(선택 사항)

IAM 태그는 사용자 사용자에게 추가할 수 있는 키-값 페어입니다. 태그는 이메일 주소와 같은 사용자 정보를 포함하거나 정책과 같은 내용일 수 있습니다. 태그를 사용하여 이 사용자에게 대한 액세스를 구성, 추적 또는 제어할 수 있습니다. [자세히 알아보기](#)

키	값(선택 사항)	제거
Name	lab-iam-user	✕

새 키 추가

49 태그를 더 추가할 수 있습니다.

취소

이전

다음: 검토

13. [검토] 페이지에서 [사용자 만들기]를 클릭한다.

### 검토

선택 항목을 검토합니다. 사용자를 생성한 후 자동으로 생성된 비밀번호와 액세스 키를 보고 다운로드할 수 있습니다.

#### 사용자 세부 정보

사용자 이름	AWS_User
AWS 액세스 유형	AWS Management Console 액세스 - 비밀번호 사용
콘솔 비밀번호 유형	사용자 지정
비밀번호 재설정 필요	아니요
권한 경계	권한 경계가 설정되지 않았습니다

#### 권한 요약

위에 표시된 사용자를 다음 그룹에 추가합니다.

유형	이름
그룹	EC2ReadOnly

#### 태그

새로운 사용자에게 다음 태그가 제공됩니다

키	값
Name	lab-iam-user

[취소](#) [이전](#) [사용자 만들기](#)

14. 사용자가 성공적으로 생성되었다. [닫기]를 클릭한다.

✓ **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.

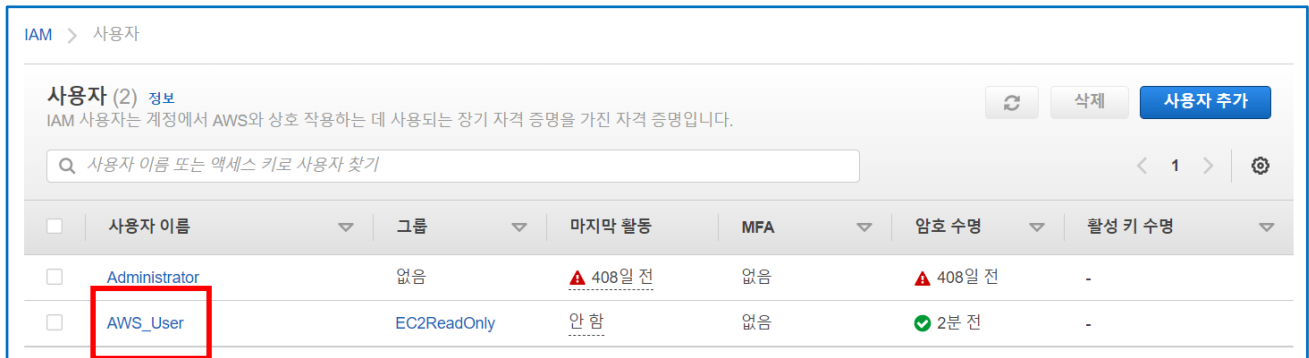
AWS Management Console 액세스 권한이 있는 사용자가 <https://789534828835.signin.aws.amazon.com/console>에 로그인할 수 있습니다.

[.csv 다운로드](#)

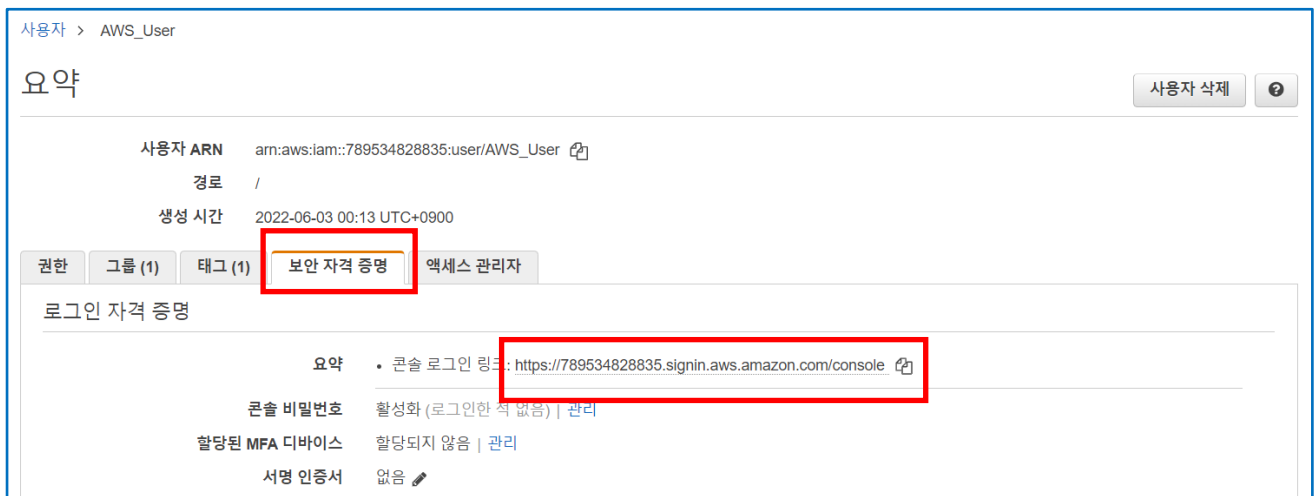
	사용자	이메일 로그인 지침
▶ ✓	AWS_User	<a href="#">이메일 전송</a>

[닫기](#)

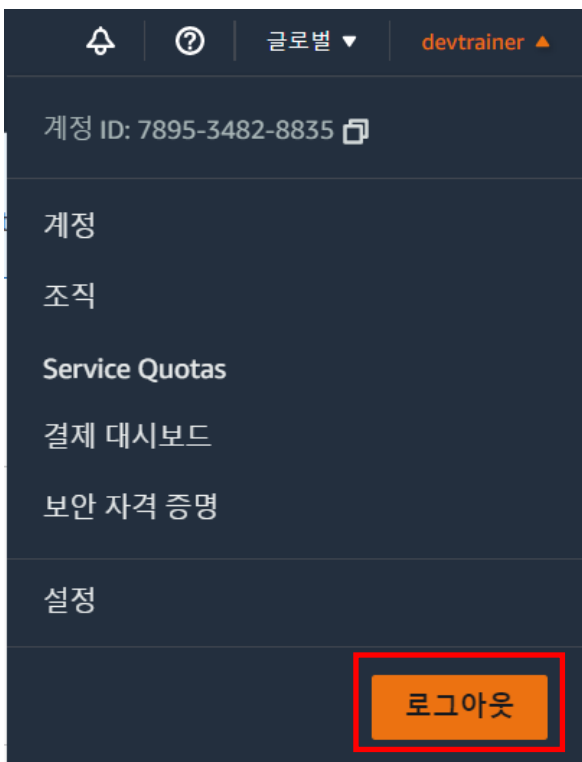
15. [사용자] 페이지에서 방금 생성한 사용자 **AWS\_User**를 클릭한다.



16. **AWS\_User**의 요약페이지에서 [보안 자격 증명] 탭을 클릭한 후, [요약]의 [콘솔 로그인 링크]를 복사한다.

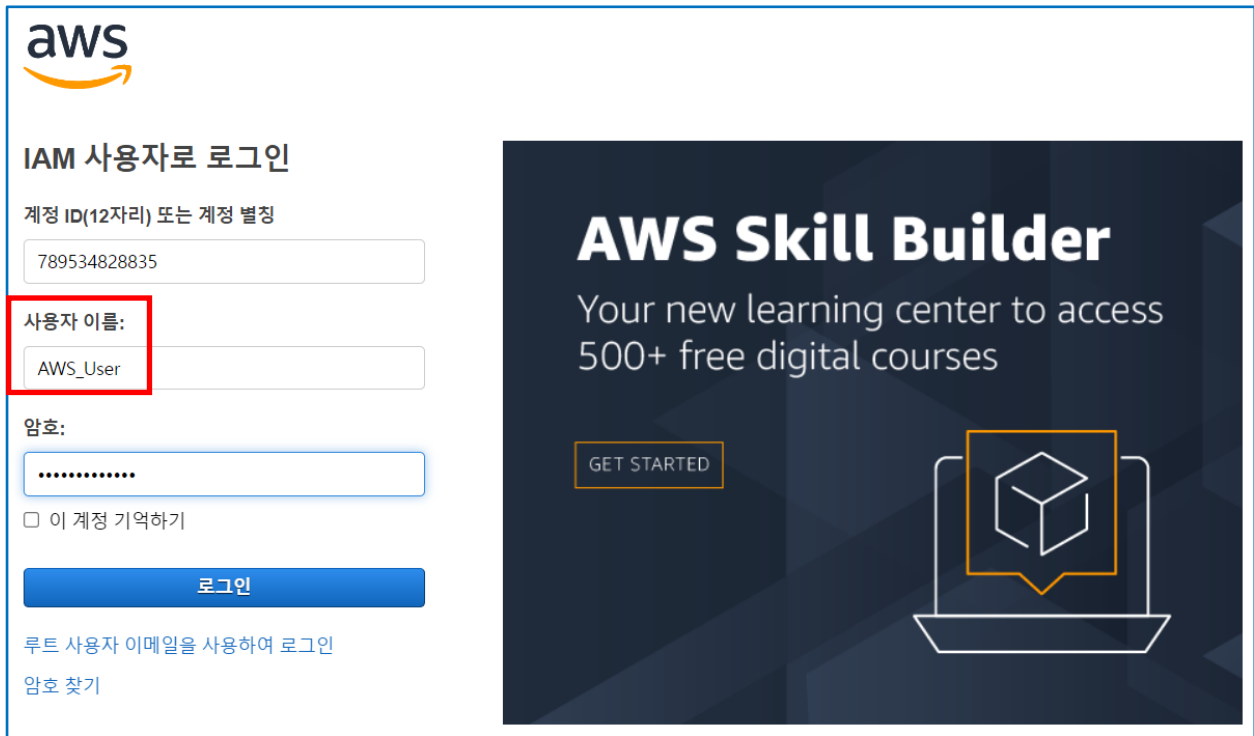


17. 지금 로그인한 사용자 **로그아웃**한다.



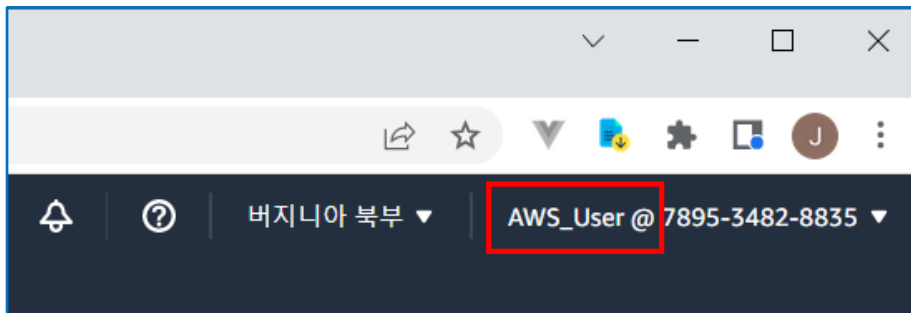


18. 복사한 주소를 웹브라우저에 입력하여 **AWS\_User** 계정으로 로그인한다.



The image shows the AWS IAM login page. On the left, there is a login form with the AWS logo at the top. The form is titled "IAM 사용자로 로그인" (Log in with IAM user). It contains three input fields: "계정 ID(12자리) 또는 계정 별칭" (Account ID (12 digits) or account alias) with the value "789534828835", "사용자 이름:" (User name:) with the value "AWS\_User", and "암호:" (Password:). Below the password field is a checkbox labeled "이 계정 기억하기" (Remember this account). A blue "로그인" (Log in) button is at the bottom of the form. Below the button are links for "루트 사용자 이메일을 사용하여 로그인" (Log in with root user email) and "암호 찾기" (Reset password). On the right, there is a dark blue banner for "AWS Skill Builder" with the text "Your new learning center to access 500+ free digital courses" and a "GET STARTED" button. An illustration of a laptop with a cube on its screen is also present.

19. 방금 생성한 계정 **AWS\_User**로 로그인했다.



20. 방금 로그인한 계정으로 새 VPC 를 생성하려고 [VPC] 페이지로 이동하여 VPC 마법사를 통해 VPC를 생성 하려고 [VPC 생성]을 클릭한다.

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. The left sidebar contains configuration options for the VPC, including private IP address range, CIDR block, NAT gateway, and VPC endpoints. The main area shows a preview of the VPC configuration, including the VPC name, subnets, and DNS settings. The 'VPC 생성' button is highlighted with a red box.

21. 해당 IAM 계정은 **EC2 Read Only Access** 권한만을 가지고 있으므로 다음과 같이 오류가 표시되며, VPC 생성 이 되지 않는다.

The screenshot shows the 'Create VPC workflow' page in the AWS Management Console. The page displays a message about the VPC creation experience. Below the message, there is an error section titled '오류' (Error) with a red box around it. The error message states: 'You are not authorized to perform this operation. Encoded authorization failure message: X-ABanl1lVgvfTJwk7mT9dUM3yz8bxEdlbWBz8REzf94wrDKYW6cHvJZgT9p3BO0kRBv\_NZge1d3VKiBiG i46yEUKjw8LU7QzM9mgbA7NnSIO9DXl6l1DErY5GwYqIq54wAPd50CO2NEqSKnMgnxMjYdQaabC-EOLoYO6A9qkG9-yZEACmUXZuZ9XHG1MGSayYI-3X4tFfo7gllkGK-z8lQ5F46sHXfbEsyUQ3dskHtQgTvvlNzAGAnNzA4EmUYedu61ylyyLMD07I2xJ7MDEu5udb7KdubZvP BaCIL2ty00lwjCYyFc6qVyG5N765MNC\_cce7X565E2r1\_bV6OGyryCnWYkmYDnPKc1qqfNy6A-OHlAgiaaZ7CRtAelzXFrZY7u2UWSt18Hw97uBkrGeZu5X-j\_IzPj8tV9XB5chtd0z-ISVx2JhdUBSsZHLRR1bu3jZW8jnna-5wlOBnfpuzHjDikHXmNZcKES6NTZaFShlbz-WLBfPwfMST5hRQblKw'. At the bottom of the page, there are buttons for '취소' (Cancel), '뒤로' (Back), and '재시도' (Retry).

# IAM Role 생성 및 IAM Role 정책을 통한 EC2 권한 할당

1. [서비스] > [보안, 자격증명 및 규정준수] > [IAM]으로 이동한다. 다음 그림과 같이 앞의 실습에서 생성한 [사용자 그룹]과 [사용자]의 수를 확인할 수 있다. [사용자 그룹]은 EC2ReadOnly이고, 현재 [사용자]는 관리자인 Administrator와 AWS\_User 2명이다. 좌측 메뉴 중 [액세스 관리] > [역할]을 클릭한다.

Identity and Access Management(IAM)

IAM 대시보드

보안 권장 사항 1

루트 사용자에게 MFA 추가  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [MFA 추가](#)

루트 사용자에게 활성 액세스 키가 없음  
루트 사용자 대신 IAM 사용자에게 연결된 액세스 키를 사용하면 보안이 향상됩니다.

**IAM 리소스**

사용자 그룹	사용자	역할	정책	자격 증명 공급자
1	2	10	1	0

새로운 기능

IAM의 기능 업데이트

- Amazon GuardDuty, 이제 다른 AWS 계정에서 사용된 EC2 인스턴스 자격 증명 탐지 가능. 5개월 전
- 일별 50개의 세분화된 IAM 정책을 생성하는 IAM Access Analyzer를 사용하여 계정에서 더 많은 역할에 대한 허가를 적정 규모로 조정. 6개월 전
- Amazon S3 객체 소유권을 통해 S3의 데이터에 대한 액세스 관리를 간소화하기 위해 액세스 제어 목록 사용 중지 가능. 6개월 전
- Amazon Redshift 기본 IAM 역할을 도입하여 다른 AWS 서비스 사용 간소화. 6개월 전

AWS 계정

계정 ID  
ID 789534828835

계정 별칭  
789534828835 [생성](#)

이 계정의 IAM 사용자를 위한 로그인 URL  
<https://789534828835.signin.aws.amazon.com/console>

빠른 링크

내 보안 자격 증명  
액세스 키, 멀티 팩트 인증(MFA) 및 기타 자격 증명을 관리합니다.

도구

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

2. 페이지 우측의 [역할 만들기]를 클릭한다.

IAM > 역할

역할 (10) 정보

IAM 역할은 단기간 동안 유효한 자격 증명을 가진 특정 권한이 있는 자격 증명입니다. 신뢰할 수 있는 개체가 역할을 맡을 수 있습니다.

[검색](#)

[새 역할 만들기](#)

역할 이름	신뢰할 수 있는 개체	마지막 ...
<input type="checkbox"/> AWSServiceRoleForAmazonElasticFileSystem	AWS 서비스: elasticfilesystem (서비스 연결 역할)	22일 전
<input type="checkbox"/> AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS 서비스: dynamodb.application-autoscaling (서비스 연결 역할)	13일 전
<input type="checkbox"/> AWSServiceRoleForAutoScaling	AWS 서비스: autoscaling (서비스 연결 역할)	49일 전
<input type="checkbox"/> AWSServiceRoleForBackup	AWS 서비스: backup (서비스 연결 역할)	22시간 전
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	AWS 서비스: elasticloadbalancing (서비스 연결 역할)	49일 전
<input type="checkbox"/> AWSServiceRoleForGlobalAccelerator	AWS 서비스: globalaccelerator (서비스 연결 역할)	-
<input type="checkbox"/> AWSServiceRoleForRDS	AWS 서비스: rds (서비스 연결 역할)	1시간 전
<input type="checkbox"/> AWSServiceRoleForSupport	AWS 서비스: support (서비스 연결 역할)	-

3. [1단계 신뢰할 수 있는 엔터티 선택]에서는 [신뢰할 수 있는 엔터티 유형] 섹션에서 [AWS 서비스]를 선택하고, [사용 사례] 섹션에서는 [EC2]를 선택하고 [다음] 버튼을 클릭한다.

IAM > 역할 > 역할 생성

1단계  
신뢰할 수 있는 엔터티 선택

2단계  
권한 추가

3단계  
이름 지정, 검토 및 생성

### 신뢰할 수 있는 엔터티 선택

신뢰할 수 있는 엔터티 유형

- ☒ AWS 서비스  
EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.
- ☐ AWS 계정  
사용자 또는 서드 파티에 속한 다른 AWS 계정의 엔터티가 이 계정에서 작업을 수행하도록 허용합니다.
- ☐ 웹 자격 증명  
지정된 외부 웹 자격 증명 공급자와 연동된 사용자가 이 역할을 맡아 이 계정에서 작업을 수행하도록 허용합니다.
- ☐ SAML 2.0 연동  
기업 디렉터리에서 SAML 2.0과 연동된 사용자가 이 계정에서 작업을 수행할 수 있도록 허용합니다.
- ☐ 사용자 지정 신뢰 정책  
다른 사용자가 이 계정에서 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

사용 사례  
EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

일반 사용 사례

- ☒ EC2  
Allows EC2 instances to call AWS services on your behalf.
- ☐ Lambda  
Allows Lambda functions to call AWS services on your behalf.

다른 AWS 서비스의 사용 사례:  
사용 사례를 조회할 서비스 선택

취소 **다음**

4. [2단계 권한 추가]에서는 [권한 정책] 섹션에서 필터에 RDS라고 입력한 후 결과에서 AmazonRDSFullAccess를 선택하고 [다음] 버튼을 클릭한다.

IAM > 역할 > 역할 생성

1단계  
신뢰할 수 있는 엔터티 선택

2단계  
권한 추가

3단계  
이름 지정, 검토 및 생성

### 권한 추가

권한 정책 (선택됨 1/754)  
새 역할에 연결할 정책을 하나 이상 선택합니다.

검색 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다. 10 개 일치

**"RDS"** X 필터 지우기

<input checked="" type="checkbox"/>	정책 이름	유형	설명
<input checked="" type="checkbox"/>	AmazonRDSFullAccess	AWS 관...	Provides full access to Amazon RDS via the AWS Management C...
<input type="checkbox"/>	AmazonRDSDirectoryServiceAccess	AWS 관...	Allow RDS to access Directory Service Managed AD on behalf of t...
<input type="checkbox"/>	RDSCloudHsmAuthorizationRole	AWS 관...	Default policy for the Amazon RDS service role.
<input type="checkbox"/>	AmazonRDSDataFullAccess	AWS 관...	Allows full access to use the RDS data APIs, secret store APIs for ...
<input type="checkbox"/>	AmazonRDSReadOnlyAccess	AWS 관...	Provides read only access to Amazon RDS via the AWS Manage...
<input type="checkbox"/>	AWSQuickSightDescribeRDS	AWS 관...	Allow QuickSight to describe the RDS resources
<input type="checkbox"/>	AmazonRDSEnhancedMonitoringRole	AWS 관...	Provides access to Cloudwatch for RDS Enhanced Monitoring

5. [3단계 이름 지정, 검토 및 생성] 페이지에서는 먼저 [역할 이름]에 lab-IAMRole-DEV라고 입력하고, 페이지 스크롤다운한다.

IAM > 역할 > 역할 생성

1단계  
신뢰할 수 있는 엔터티 선택

2단계  
권한 추가

3단계  
이름 지정, 검토 및 생성

## 이름 지정, 검토 및 생성

### 역할 세부 정보

역할 이름  
이 역할을 식별하는 의미 있는 이름을 입력합니다.

lab-IAMRole-DEV

Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters.

설명  
이 정책에 대하여 간단한 설명을 추가합니다.

Allows EC2 instances to call AWS services on your behalf.

6. [태그] 섹션에서 [태그 추가] 버튼을 클릭하여, [키]는 Name으로, [값]은 lab-IAMRole-DEV라고 입력하고 [역할 생성] 파란색 버튼을 클릭한다.

2단계: 권한 추가

권한 정책 요약

정책 이름	유형	다음으로서 연결됨
AmazonRDSFullAccess	AWS 관리형	권한 정책

### 태그

#### 태그 추가 (선택 사항)

태그는 리소스를 식별, 구성 또는 검색하는 데 도움이 되도록 AWS 리소스에 추가할 수 있는 키-값 페어입니다.

키	값 - 선택 사항
Name	lab-IAMRole-DEV

태그 제거

태그 추가

최대 49개의 태그를 더 추가할 수 있음

취소 이전 **역할 생성**

7. 새 역할이 성공적으로 생성됐음을 확인한다.

역할 (11) 정보

IAM 역할은 단기간 동안 유효한 자격 증명을 가진 특정 권한이 있는 자격 증명입니다. 신뢰할 수 있는 개체가 역할을 맡을 수 있습니다.

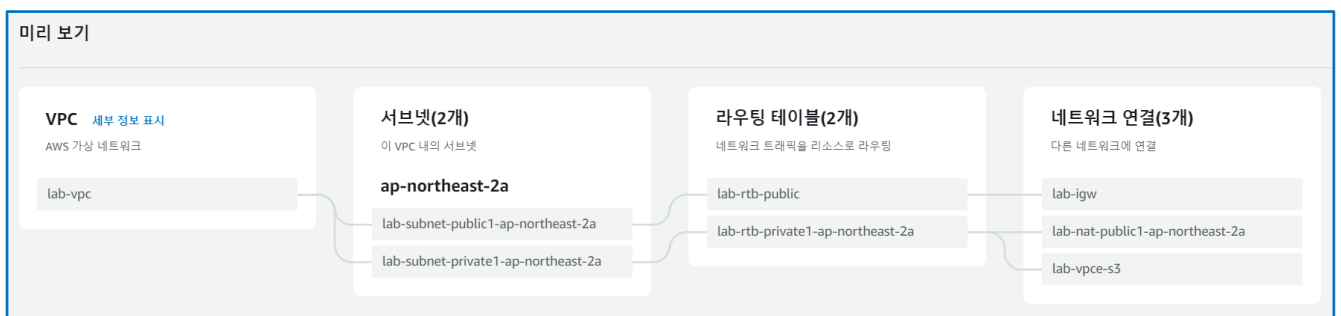
검색

1

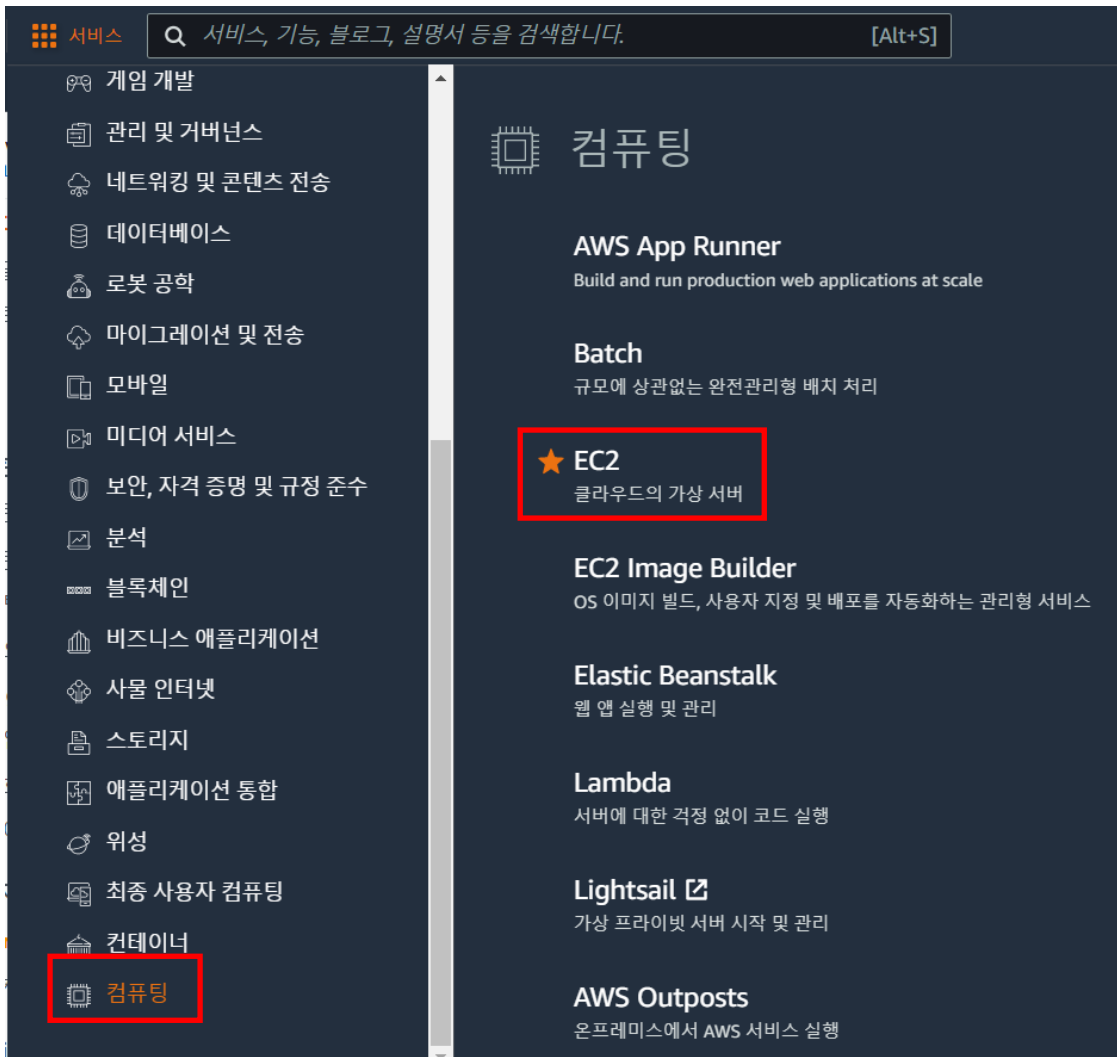
역할 이름	신뢰할 수 있는 개체	마지막 ...
<input type="checkbox"/> AWSServiceRoleForAmazonElasticFileSystem	AWS 서비스: elasticfilesystem (서비스 연결 역할)	22일 전
<input type="checkbox"/> AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS 서비스: dynamodb.application-autoscaling (서비스 연결 역할)	13일 전
<input type="checkbox"/> AWSServiceRoleForAutoScaling	AWS 서비스: autoscaling (서비스 연결 역할)	49일 전
<input type="checkbox"/> AWSServiceRoleForBackup	AWS 서비스: backup (서비스 연결 역할)	22시간 전
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	AWS 서비스: elasticloadbalancing (서비스 연결 역할)	49일 전
<input type="checkbox"/> AWSServiceRoleForGlobalAccelerator	AWS 서비스: globalaccelerator (서비스 연결 역할)	-
<input type="checkbox"/> AWSServiceRoleForRDS	AWS 서비스: rds (서비스 연결 역할)	1시간 전
<input type="checkbox"/> AWSServiceRoleForSupport	AWS 서비스: support (서비스 연결 역할)	-
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS 서비스: trustedadvisor (서비스 연결 역할)	-
<input type="checkbox"/> helloworld0530-role-jg99ztoi	AWS 서비스: lambda	6일 전
<input type="checkbox"/> lab-IAMRole-DEV	AWS 서비스: ec2	-

8. 다음과 같이 **VPC**를 생성한다.

- A. [VPC 설정] : VPC, 서브넷 등
- B. [이름 태그 자동 생성] : 자동생성 체크 / lab
- C. [IPv4 CIDDR 블록] : 10.0.0.0/16
- D. [태넌시] : 기본값
- E. [가용 영역(AZ)] : 1 / ap-northeast-2a
- F. [퍼블릭 서브넷 수] / [프라이빗 서브넷 수] : 각 1개씩
- G. [NAT 게이트웨이] : AZ당 1개
- H. [VPC 엔드포인트] : S3 게이트웨이
- I. [DNS 옵션] : DNS 호스트 이름 활성화 / DNS 확인 활성화



9. 역할 할당 및 테스트를 위해 [서비스] > [컴퓨팅] > [EC2]를 클릭한다.



10. 다음과 같이 각각의 값을 설정하여 EC2 인스턴스를 생성한다. 나머지 단계의 값은 기본값을 사용한다.

- A. [단계 1 : Amazon Machine Image(AMI) 선택] : Amazon Linux 2 AMI(HVM) – Kernel 5.10, SSD Volume Type, 64 비트(x86)
- B. [단계 2 : 인스턴스 유형 선택] : t2.micro
- C. [단계 3 : 인스턴스 세부 정보 구성] : lab-vpc, lab-subnet-public1-ap-northeast-2a, 퍼블릭 IP 자동 할당 / 활성화
- D. [IAM 역할] : lab-IAMRole-DEV

배치 그룹 ⓘ	<input type="checkbox"/> 배치 그룹에 인스턴스 추가
용량 예약 ⓘ	열기
도메인 조인 디렉터리 ⓘ	디렉터리 없음 <span>↕</span> 새 디렉터리 생성
IAM 역할 ⓘ	lab-IAMRole-DEV <span>↕</span> 새 IAM 역할 생성

- E. [단계 6 : 보안 그룹 생성] : lab-sg

11. [서비스] > [스토리지] > [S3]로 이동하여 다음과 같이 새로운 **Bucket**을 생성한다.

A. [버킷 이름] : lab-xxx

B. [AWS 리전] : 아시아 태평양(서울) ap-northeast-2

Amazon S3 > 버킷 > 버킷 만들기

## 버킷 만들기 정보

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

### 일반 구성

버킷 이름

lab-henry0604-bucket

버킷 이름은 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

C. [모든 퍼블릭 액세스 차단] : 해제

D. [현재 설정으로 인해...알고 있습니다.] 체크


### 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 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.

E. [태그] : Name / lab-xxx



태그 (1) - 선택 사항

버킷에 태그를 지정하여 스토리지 비용 또는 기타 기준을 추적합니다. 자세히 알아보기

키

Name

lab-henry0604-bucket

제거

값 - 선택 사항

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

12. 방금 생성한 **bucket**에 **Syllabus.pdf** 파일을 업로드했다.

Amazon S3 > 버킷 > lab-henry0604-bucket

lab-henry0604-bucket 정보

객체

속성

권한

지표

관리

액세스 지정

객체 (1)

객체는 Amazon S3에 저장되어 있는 기본 엔티티입니다. Amazon S3 인벤토리를 사용하여 버킷에 있는 모든 객체의 목록을 얻을 수 있습니다. 다른 사용자가 객체에 액세스할 수 있게 하려면 명시적으로 권한을 부여해야 합니다. 자세히 알아보기

새 객체 업로드

S3 URI 복사

URL 복사

다운로드

열기

삭제

작업

폴더 만들기

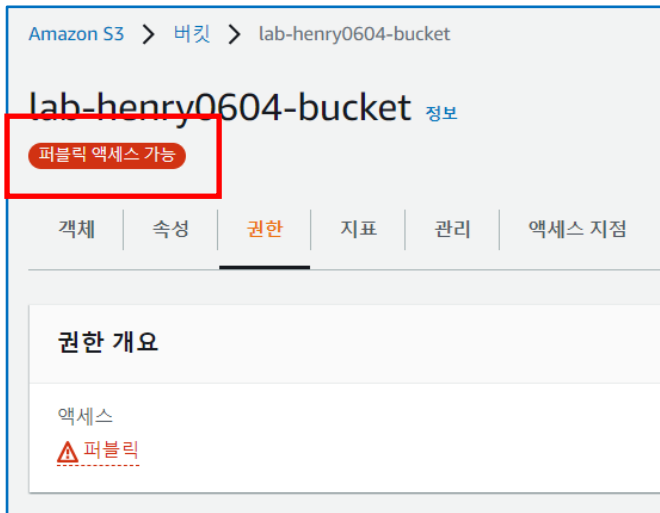
업로드

검색

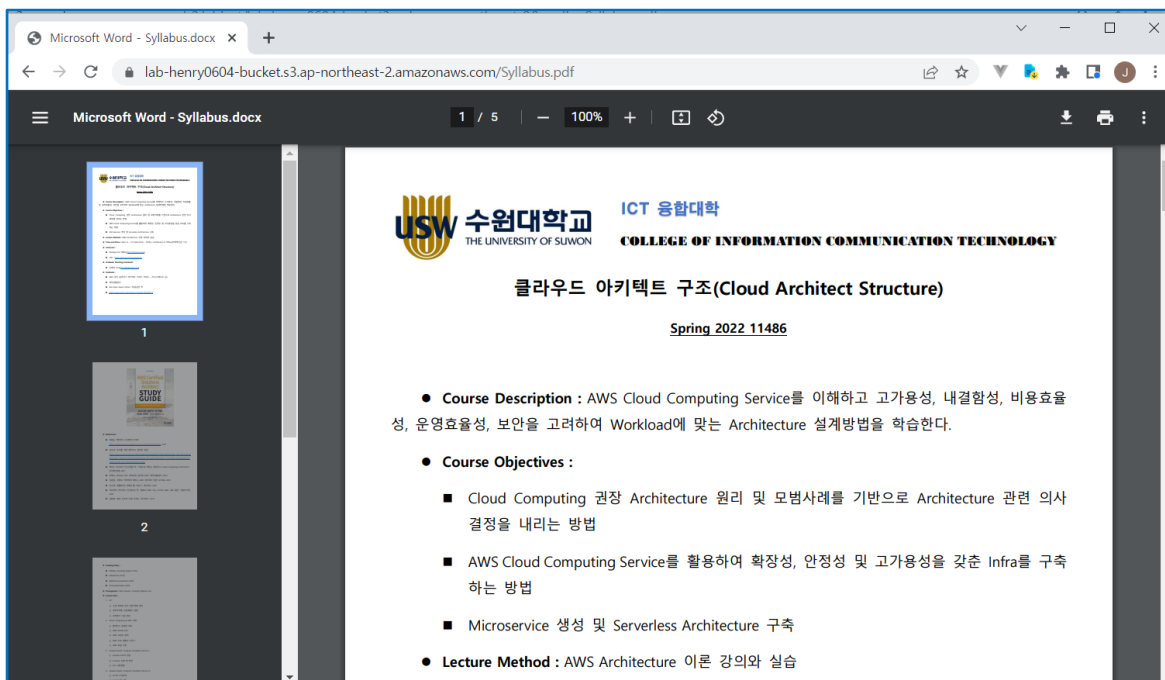
업로드

이름	유형	마지막 수정	크기	스토리지 클래스
Syllabus.pdf	pdf	2022. 6. 4. pm 3:30:00 PM KST	292.5KB	Standard

13. 그리고 방금 생성한 **bucket**을 누구나 접근할 수 있게끔 **[퍼블릭 액세스 가능]**하게 수정했다.



14. 퍼블릭 액세스가 가능한지 업로드한 객체의 **[객체 URL]**을 복사해서 웹 브라우저에서 테스트했다. 다음과 같이 액세스가 잘 됨을 확인할 수 있다.



15. 이제 위 실습에서 생성한 **EC2 인스턴스**에 **SSH**로 접근해 본다. 접속 후 다음 명령으로 시스템 업데이트 한다.

**\$ sudo yum update**

```
Installing : kernel-5.10.112-108.499.amzn2.x86_64
Cleanup    : curl-7.79.1-1.amzn2.0.1.x86_64
Cleanup    : libcurl-7.79.1-1.amzn2.0.1.x86_64
Cleanup    : openldap-2.4.44-23.amzn2.0.3.x86_64
Cleanup    : iproute-5.10.0-2.amzn2.0.1.x86_64
Cleanup    : kernel-tools-5.10.109-104.500.amzn2.x86_64
Verifying  : kernel-5.10.112-108.499.amzn2.x86_64
Verifying  : curl-7.79.1-2.amzn2.0.1.x86_64
Verifying  : libcurl-7.79.1-2.amzn2.0.1.x86_64
Verifying  : kernel-tools-5.10.112-108.499.amzn2.x86_64
Verifying  : iproute-5.10.0-2.amzn2.0.2.x86_64
Verifying  : openldap-2.4.44-23.amzn2.0.4.x86_64
Verifying  : iproute-5.10.0-2.amzn2.0.1.x86_64
Verifying  : curl-7.79.1-1.amzn2.0.1.x86_64
Verifying  : openldap-2.4.44-23.amzn2.0.3.x86_64
Verifying  : libcurl-7.79.1-1.amzn2.0.1.x86_64
Verifying  : kernel-tools-5.10.109-104.500.amzn2.x86_64

Installed:
kernel.x86_64 0:5.10.112-108.499.amzn2

Updated:
curl.x86_64 0:7.79.1-2.amzn2.0.1 iproute.x86_64 0:5.10.0-2.amzn2.0.2 kernel-tools.x86_64 0:5.10.112-108.499.amzn2 libcurl.x86_64 0:7.79.1-2.amzn2.0.1
openldap.x86_64 0:2.4.44-23.amzn2.0.4

Complete!
[ec2-user@ip-10-0-13-253 ~]$
```

16. 다음과 같이 **AWS S3**에 연결하려고 **S3**에 업로드한 **Syllabus.pdf** 파일의 **[S3 URI]**로 접속했다. 하지만 **Access Denied** 메시지를 받았다. 즉, **EC2**가 **S3**에 접근 권한이 없으므로 발생하는 문제이다.

Amazon S3 > 버킷 > lab-henry0604-bucket > Syllabus.pdf

Syllabus.pdf 정보

S3 URI 복사 다운로드 열기 객체 작업

속성 권한 버전

객체 개요

소유자	c75673606213e161e2f8b508b74d968c693f3b1b316fafbb11a2a8cbc0cb9762
AWS 리전	아시아 태평양(서울) ap-northeast-2
마지막 수정	2022. 6. 4. pm 3:30:00 PM KST
크기	292.5KB
유형	pdf
키	Syllabus.pdf

S3 URI

s3://lab-henry0604-bucket/Syllabus.pdf

Amazon 리소스 이름(ARN)

arn:aws:s3:::lab-henry0604-bucket/Syllabus.pdf

엔터티 태그(Etag)

d75c1db7b27706dacf2ab13ddd185239

객체 URL

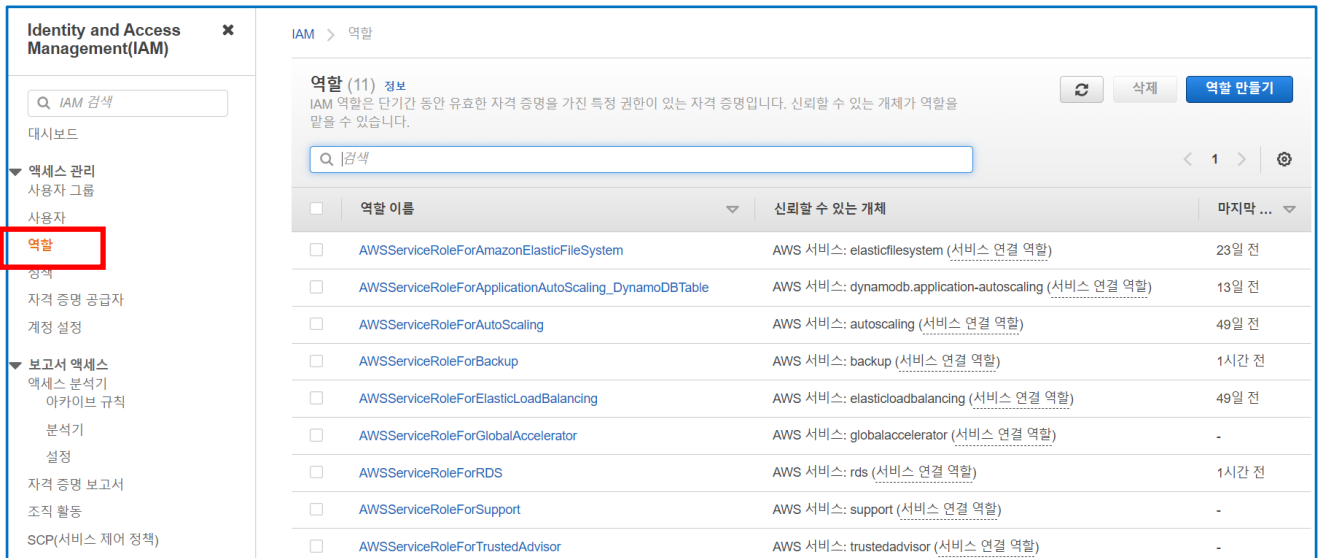
https://lab-henry0604-bucket.s3.ap-northeast-2.amazonaws.com/Syllabus.pdf

**\$ aws s3 ls s3://버킷명**

```
1 AWS EC2 Instance x +
[ec2-user@ip-10-0-13-253 ~]$
[ec2-user@ip-10-0-13-253 ~]$
[ec2-user@ip-10-0-13-253 ~]$ aws s3 ls s3://lab-henry0604-bucket/

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-10-0-13-253 ~]$
```

17. IAM Role에 S3 권한을 추가하기 위해 [IAM 역할] 페이지로 이동한다.



Identity and Access Management(IAM)

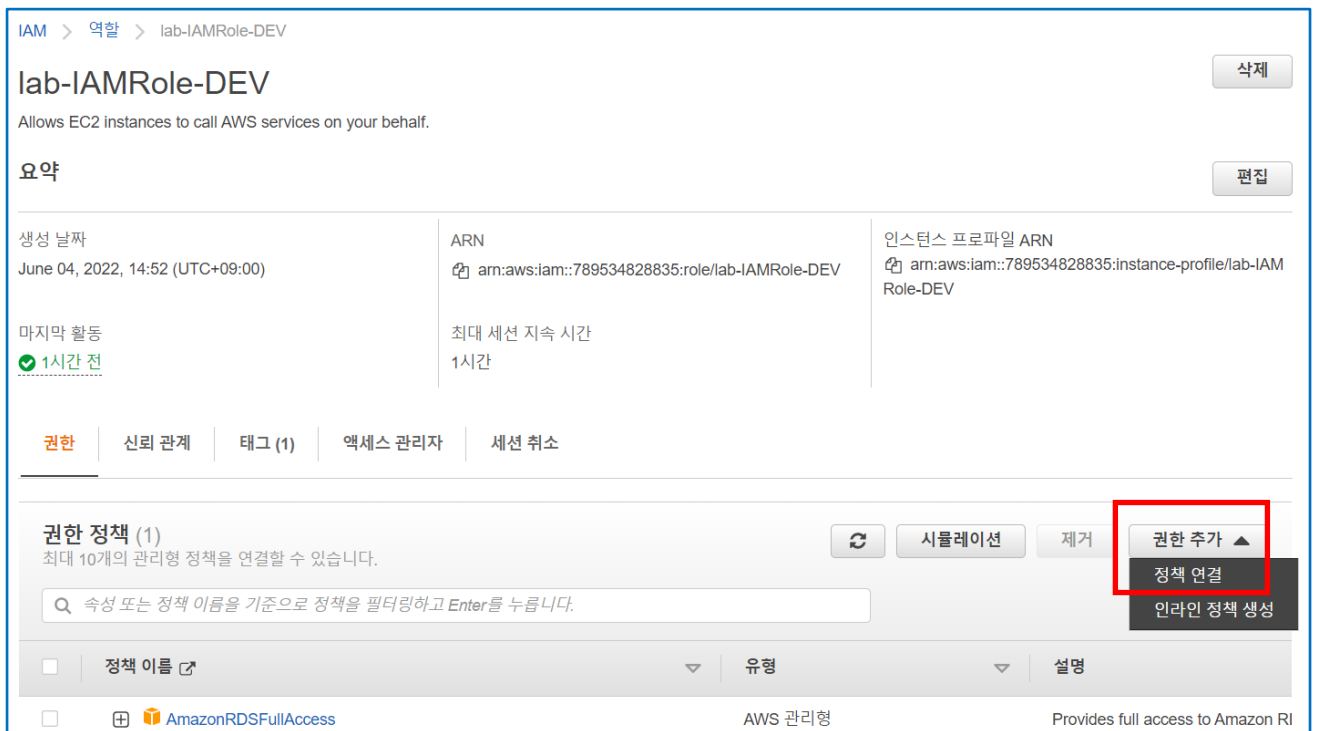
역할 (11) 정보

IAM 역할은 단기간 동안 유효한 자격 증명을 가진 특정 권한이 있는 자격 증명입니다. 신뢰할 수 있는 개체가 역할을 맡을 수 있습니다.

역할 이름

역할 이름	신뢰할 수 있는 개체	마지막 ...
AWSServiceRoleForAmazonElasticFileSystem	AWS 서비스: elasticfilesystem (서비스 연결 역할)	23일 전
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS 서비스: dynamodb.application-autoscaling (서비스 연결 역할)	13일 전
AWSServiceRoleForAutoScaling	AWS 서비스: autoscaling (서비스 연결 역할)	49일 전
AWSServiceRoleForBackup	AWS 서비스: backup (서비스 연결 역할)	1시간 전
AWSServiceRoleForElasticLoadBalancing	AWS 서비스: elasticloadbalancing (서비스 연결 역할)	49일 전
AWSServiceRoleForGlobalAccelerator	AWS 서비스: globalaccelerator (서비스 연결 역할)	-
AWSServiceRoleForRDS	AWS 서비스: rds (서비스 연결 역할)	1시간 전
AWSServiceRoleForSupport	AWS 서비스: support (서비스 연결 역할)	-
AWSServiceRoleForTrustedAdvisor	AWS 서비스: trustedadvisor (서비스 연결 역할)	-

18. [역할 이름] 목록에서 위에서 생성한 lab-IAMRole-DEV를 클릭하여 상세 페이지로 이동한다. [권한 추가] > [정책 연결]을 클릭한다.



IAM > 역할 > lab-IAMRole-DEV

## lab-IAMRole-DEV

Allows EC2 instances to call AWS services on your behalf.

요약

생성 날짜  
June 04, 2022, 14:52 (UTC+09:00)

ARN  
arn:aws:iam::789534828835:role/lab-IAMRole-DEV

인스턴스 프로파일 ARN  
arn:aws:iam::789534828835:instance-profile/lab-IAM Role-DEV

마지막 활동  
1시간 전

최대 세션 지속 시간  
1시간

권한 | 신뢰 관계 | 태그 (1) | 액세스 관리자 | 세션 취소

권한 정책 (1)  
최대 10개의 관리형 정책을 연결할 수 있습니다.

속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

정책 이름	유형	설명
AmazonRDSFullAccess	AWS 관리형	Provides full access to Amazon RI

19. 필터에 **S3**를 입력해서 검색하고, **[정책 이름]** 검색 결과에서 **AmazonS3FullAccess**를 클릭하여 선택한 다음, **[정책 연결]** 파란색 버튼을 클릭한다.

The screenshot shows the AWS IAM console interface for the role 'lab-IAMRole-DEV'. The '현재 권한 정책 (1)' section shows one attached policy. The '기타 권한 정책 (선택됨 1/753)' section has a search filter 'S3' applied. The 'AmazonS3FullAccess' policy is selected, highlighted with a red box. The '정책 연결' button is also highlighted with a red box.

선택	정책 이름	유형	설명
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS 관리형	Provides full access to all buckets via th...
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS 관리형	Provides access to manage S3 settings...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS 관리형	Policy used by QuickSight team to acce...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS 관리형	Provides read only access to all bucket...
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS 관리형	Provides full access to Amazon S3 on ...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Backup	AWS 관리형	Policy containing permissions necessar...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Restore	AWS 관리형	Policy containing permissions necessar...
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS 관리형	Provides AWS Lambda functions permi...
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS 관리형	Provides read only access to Amazon S...

20. 생성한 **역할**의 상세 페이지에 아래 그림과 같이 **AmazonS3FullAccess** 권한이 추가됐음을 확인한다.

The screenshot shows the AWS IAM console interface for the role 'lab-IAMRole-DEV'. The '권한' tab is selected, and the '권한 정책 (2)' section shows two attached policies: 'AmazonRDSFullAccess' and 'AmazonS3FullAccess'. The 'AmazonS3FullAccess' policy is highlighted with a red box.

선택	정책 이름	유형	설명
<input type="checkbox"/>	AmazonRDSFullAccess	AWS 관리형	Provides full access to Amazon RDS via the...
<input type="checkbox"/>	AmazonS3FullAccess	AWS 관리형	Provides full access to all buckets via the A...

21. [IAM 역할]에 권한 추가 후 다음과 같이 S3에 접근이 가능함을 확인할 수 있다.

```
1 AWS EC2 Instance x +
[ec2-user@ip-10-0-13-253 ~]$
[ec2-user@ip-10-0-13-253 ~]$
[ec2-user@ip-10-0-13-253 ~]$ aws s3 ls s3://lab-henry0604-bucket/

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-10-0-13-253 ~]$
[ec2-user@ip-10-0-13-253 ~]$ aws s3 ls s3://lab-henry0604-bucket/
2022-06-04 06:30:00      299526 Syllabus.pdf
[ec2-user@ip-10-0-13-253 ~]$
```