

Lab2. Installing and Configuring AWS CLI

목적

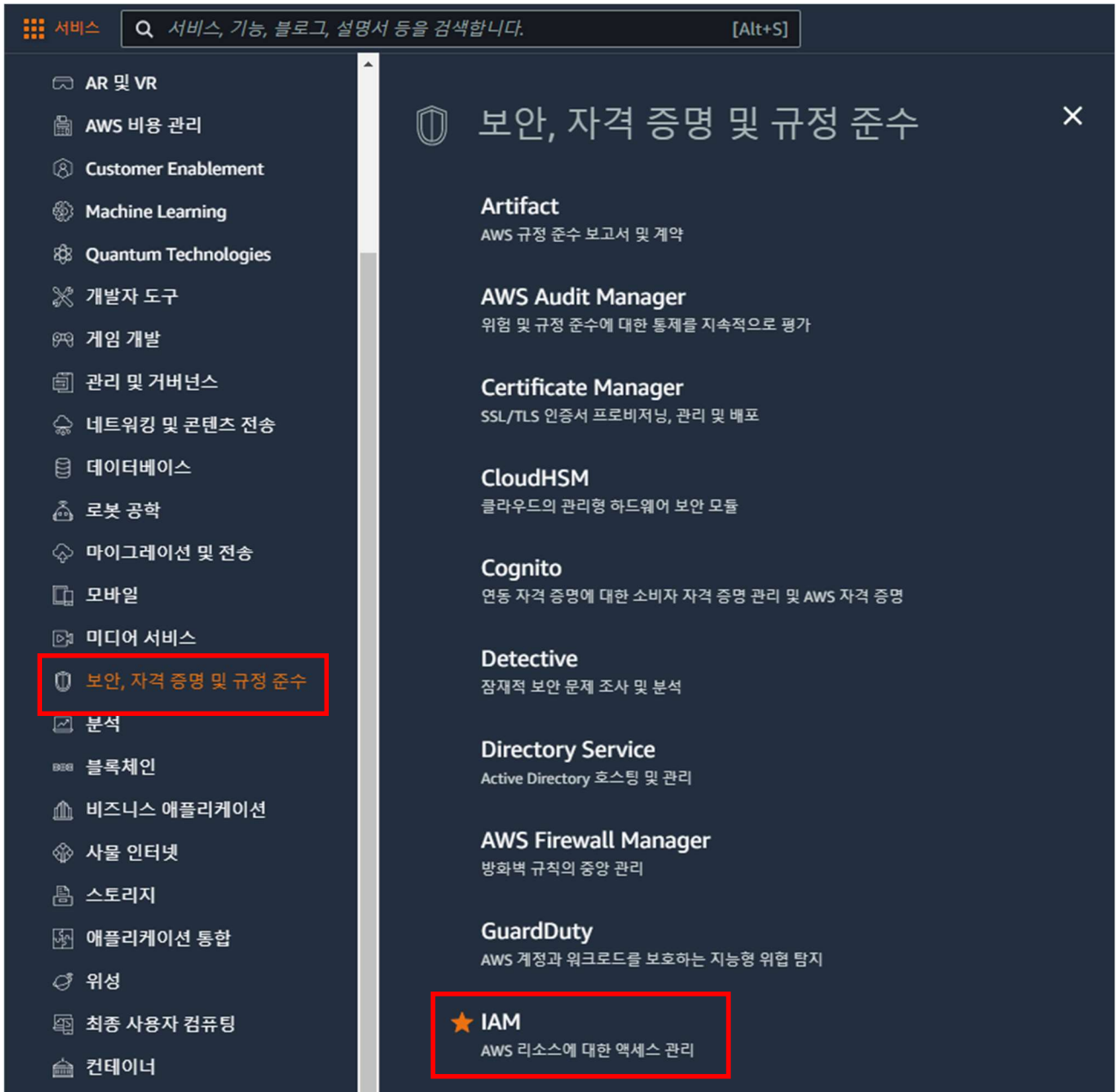
AWS CLI를 이용하기 위한 준비

사전 준비물

AWS Free-Tier 계정

Create an IAM User Account

1. **root** 계정으로 로그인 후, [서비스] > [보안, 자격 증명 및 규정 준수] > [IAM]을 클릭하여 IAM 페이지로 이동한다.



2. [IAM 대시보드] 페이지에서 왼쪽 메뉴 중 [액세스 관리] > [사용자]를 선택한다.

Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

설정

자격 증명 보고서

조직 활동

SCP(서비스 제어 정책)

IAM 대시보드

보안 권장 사항 1

⚠ 루트 사용자에게 대해 MFA 추가
루트 사용자에게 대해 MFA 추가 - 루트 사용자에게 대해 다중 인증(MFA)을 활성화하여 이 계정의 보안을 강화합니다.

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
0	1	14	10	0

새로운 기능

IAM의 기능 업데이트

- Amazon GuardDuty, 이제 다른 AWS 계정에서 사용된 EC2 인스턴스 자격 증명 탐지 가능. 8개월 전
- 일련 50개의 세분화된 IAM 정책을 생성하는 IAM Access Analyzer를 사용하여 계정에서 더 많은 역할에 대한 허가를 적정 규모로 조정. 9개월 전
- Amazon S3 객체 소유권을 통해 S3의 데이터에 대한 액세스 관리를 간소화하기 위해 액세스 제어 목록 사용 중지 가능. 10개월 전
- Amazon Redshift, 기본 IAM 역할을 도입하여 다른 AWS 서비스 사용 간소화. 10개월 전

모두 보기

3. [사용자] 페이지에서 새 사용자를 추가하기 위해 페이지 우측 상단의 [사용자 추가]를 클릭한다.

Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

설정

자격 증명 보고서

조직 활동

SCP(서비스 제어 정책)

IAM > 사용자

사용자 (0) 정보

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

Q 사용자 이름 또는 액세스 키로 사용자 찾기

사용자 이름 그룹 마지막 활동 MFA 암호 수명 활성 키 수명

표시할 리소스 없음

사용자 추가

4. [사용자 추가] 페이지에서, 다음 각 각의 값을 설정한다. 그리고 [다음:권한] 버튼을 클릭한다.

A. [사용자 이름] : Administrator

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

C. [콘솔 비밀번호] : [사용자 지정 비밀번호] 선택 후 입력

D. [비밀번호 재설정 필요] : 체크해제

사용자 추가

12345

사용자 세부 정보 설정

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

사용자 이름*

Administrator

[+ 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.

콘솔 비밀번호*

☐ 자동 생성된 비밀번호

☒ 사용자 지정 비밀번호

☐ 비밀번호 표시

비밀번호 재설정 필요

☐ 사용자가 다음에 로그인할 때 새 비밀번호 생성 요청
사용자가 비밀번호를 변경할 수 있도록 허용하는 [IAMUserChangePassword](#) 정책을 자동으로 가져옵니다.

* 필수

취소


다음: 권한


5. [권한 설정] 섹션에서 [그룹에 사용자 추가]를 선택하고 [그룹 생성] 버튼을 클릭한다.


사용자 추가


12345

▼ 권한 설정

 그룹에 사용자 추가

 기존 사용자에서 권한 복사

 기존 정책 직접 연결

 그룹 시작하기

아직 그룹을 생성하지 않았습니다. 그룹을 사용하여 직무, AWS 서비스 액세스 또는 사용자 지정 권한별로 사용자의 권한을 관리하는 것이 좋습니다. 그룹을 생성하여 시작하십시오. 자세히 알아보기

그룹 생성

▶ 권한 경계 설정

6. [그룹 생성]창에서, [그룹 이름]에는 **Administrators**를 입력하고, [정책 필터]를 클릭하여 [정책 유형] > [AWS 관리-직무]를 체크한다.

그룹 생성

그룹을 만들고 그룹에 연결할 정책을 선택하십시오. 그룹을 사용하여 직무, AWS 서비스 액세스 또는 사용자 지정 권한별로 사용자의 권한을 관리하는 것이 좋습니다.

그룹 이름

Administrators

정책 생성

↺ 새로 고침

정책 필터 ▼

Q 검색

필터 재설정

정책 유형

☐ 고객 관리형 (10)

☐ AWS 관리형 (760)



☒ AWS 관리 - 직무 (10)

정책 사용

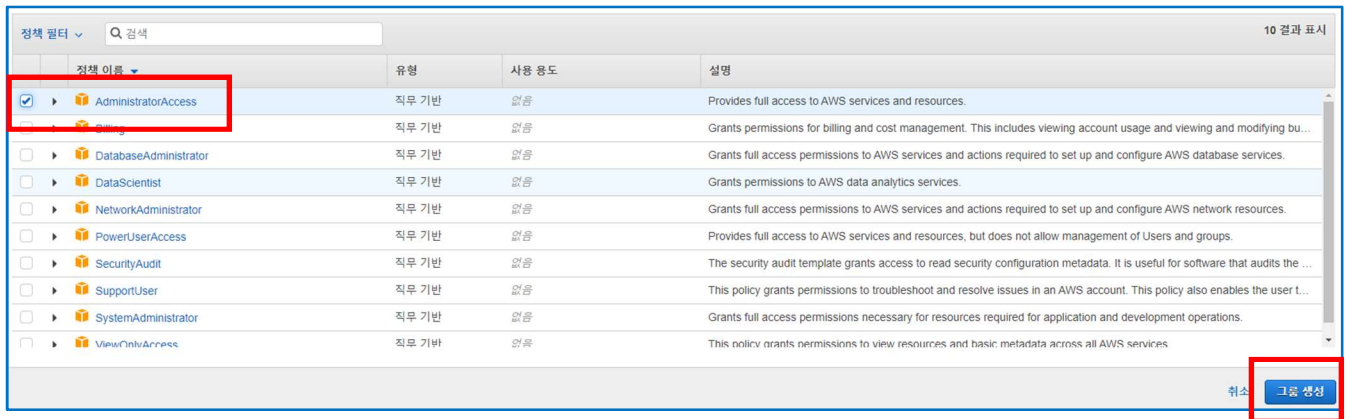
☐ 권한에 사용됨 (11)

☐ 경계에 사용됨 (0)

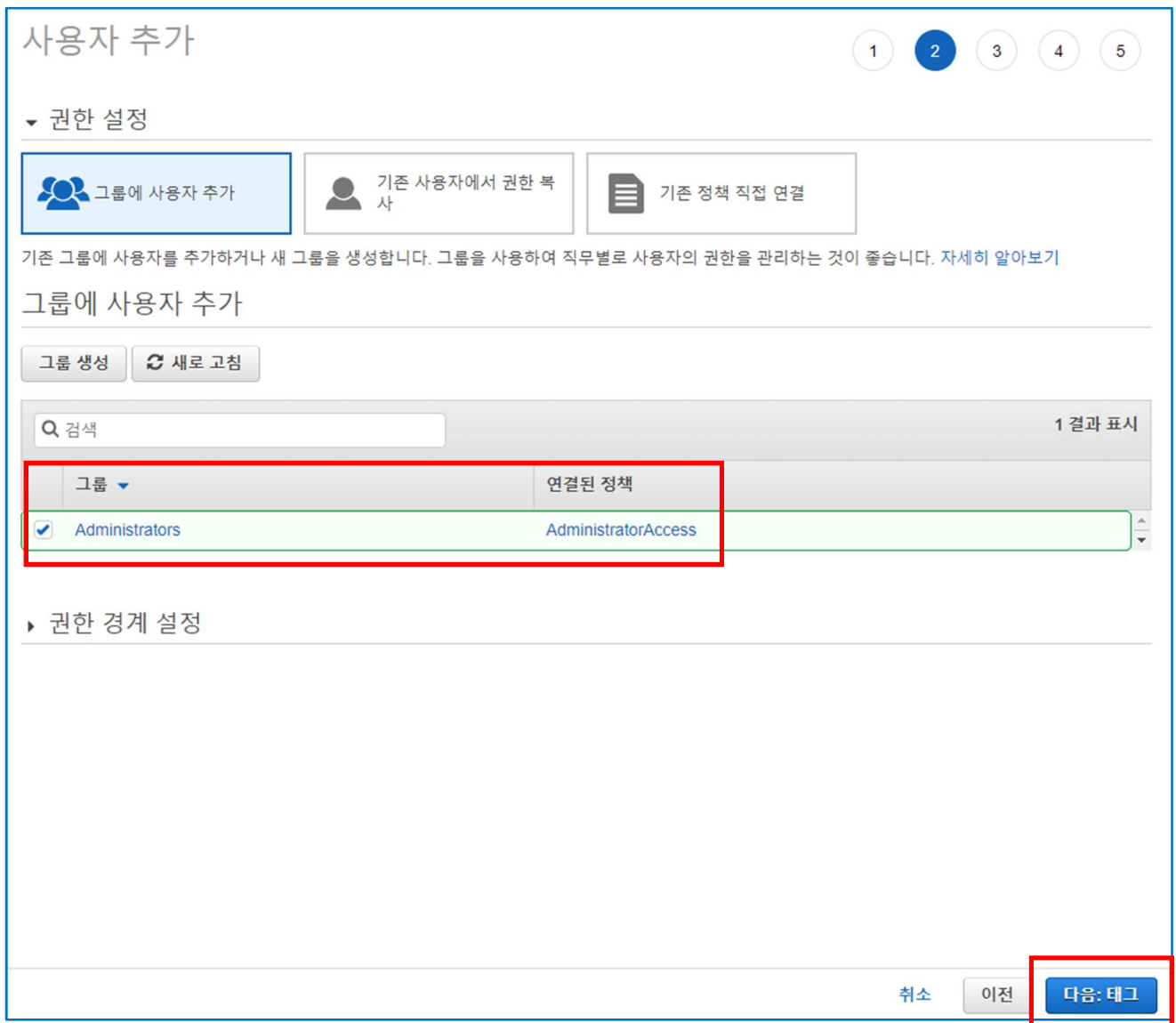
☐ 사용되지 않음 (769)

	유형	사용 용도
	직무 기반	없음
	직무 기반	없음
	직무 기반	없음
	직무 기반	없음
	직무 기반	없음
	직무 기반	없음
	직무 기반	없음
<input type="checkbox"/> ▶  SystemAdministrator	직무 기반	없음
<input type="checkbox"/> ▶  ViewOnlyAccess	직무 기반	없음

7. [정책 목록]에서 **AdministratorAccess**를 체크하고 [그룹생성] 버튼을 클릭하여 그룹을 생성한다.



8. [사용자 추가]페이지로 돌아왔다. 방금 생성한 그룹이 **Administrators**임을 확인하고 [다음:태그] 버튼을 클릭한다.



9. [태그 추가(선택 사항)] 페이지에서, [키]는 **Name**, [값]은 **lab-administrator-user**로 입력하고 [다음:검토]를 클릭한다.

사용자 추가

12345

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
<input type="text" value="Name"/>	<input type="text" value="lab-administrator-user"/>	✕
<input type="text" value="새 키 추가"/>	<input type="text"/>	

49 태그를 더 추가할 수 있습니다.

취소

이전

다음: 검토

10. [검토] 페이지에서 내용을 검토 후, 수정 사항이 없으면 [사용자 만들기]를 클릭한다.

사용자 추가

12345

검토

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

사용자 세부 정보

사용자 이름	Administrator
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	Administrators

태그

새로운 사용자에게 다음 태그가 제공됩니다

키	값
Name	lab-administrator-user

취소

이전

사용자 만들기

11. 사용자 추가가 성공적으로 수행되었다. [닫기]를 클릭하여 창을 닫는다.

사용자 추가

12345

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

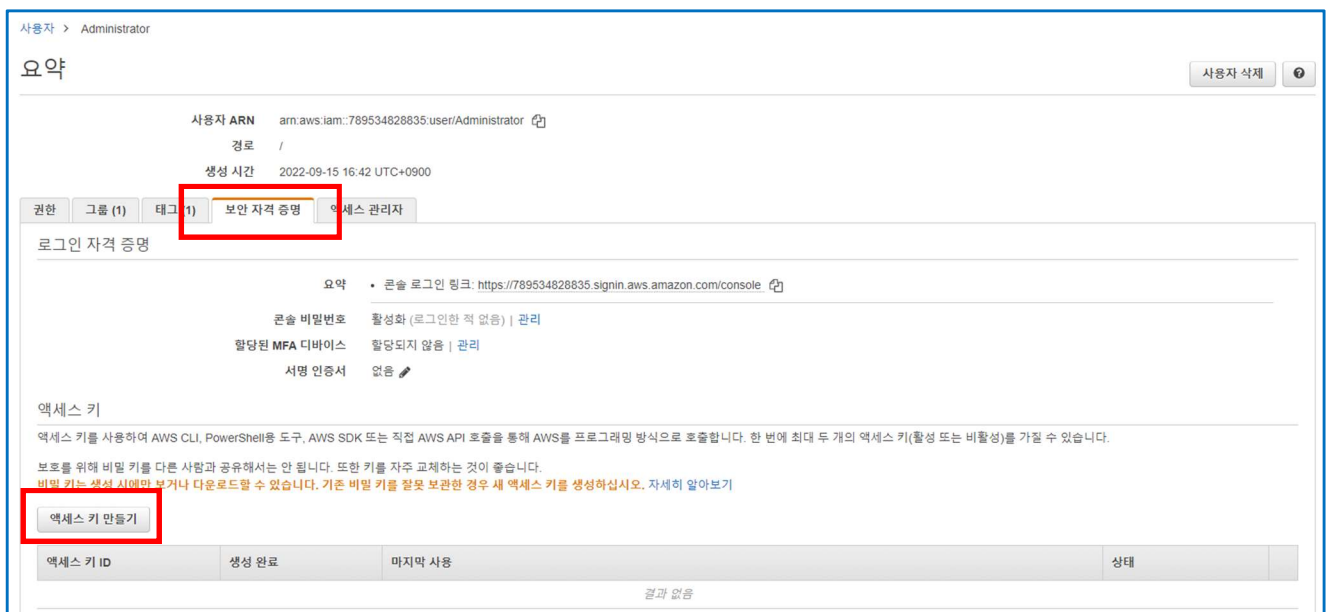
사용자	이메일 로그인 지침
▶ Administrator	이메일 전송

Create an Access Key ID and Secret Access Key

1. 방금 생성한 Administrator 계정을 확인할 수 있다. Administrator 계정에게 Access Key를 발급하기 위해 Administrator 계정을 클릭한다.



2. [요약] 페이지에서 [보안자격증명] 탭을 클릭한 후, [액세스 키] 섹션에서, [액세스 만들기] 버튼을 클릭한다.



3. [액세스 키 만들기] 창이 열리고, [액세스 키 ID]와 [비밀 액세스 키]가 생성되었다. [표시]를 클릭하여 [비밀 액세스 키]를 확인할 수 있다. 창을 닫은 후에는 내용을 확인할 수 없기 때문에 [.csv 파일 다운로드]를 클릭하여 반드시 액세스 키 페어를 별도의 위치에 잘 저장해야 한다. [닫기]를 클릭하여 창을 닫는다.

액세스 키 만들기

경고

GitHub과 같은 퍼블릭 플랫폼에 보안 액세스 키를 게시하지 마세요. 그럴 경우 계정 보안이 침해될 수 있습니다.

성공

이번 한 번만 비밀 액세스 키를 보거나 다운로드할 수 있습니다. 나중에 복구할 수 없습니다. 하지만 언제든지 새 액세스 키를 생성할 수 있습니다.

📄 .csv 파일 다운로드

액세스 키 ID	비밀 액세스 키
AKIA3PU7RNERWSOJGYVQ	***** 표시

닫기

4. 액세스 키가 성공적으로 생성되었다.

액세스 키

액세스 키를 사용하여 AWS CLI, PowerShell용 도구, AWS SDK 또는 직접 AWS API 호출을 통해 AWS를 프로그래밍 방식으로 호출합니다. 한 번에 최대 두 개의 액세스 키(활성 또는 비활성)를 가질 수 있습니다.

보안을 위해 비밀 키를 다른 사람과 공유해서는 안 됩니다. 또한 키를 자주 교체하는 것이 좋습니다.

비밀 키는 생성 시에만 보거나 다운로드할 수 있습니다. 기존 비밀 키를 잘못 보관한 경우 새 액세스 키를 생성하십시오. 자세히 알아보기

액세스 키 만들기

액세스 키 ID	생성 원료	마지막 사용	상태
AKIA3PU7RNERWSOJGYVQ	2022-09-15 16:51 UTC+0900	해당 사항 없음	(활성) 비활성화

Installing the Latest Version of the AWS CLI

- 이번 실습에서는 Windows OS에서 설치할 것이다. Linux 혹은 macOS를 사용하여 설치할 경우에는 <https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html> 여기를 참고하길 바란다.

AWS CLI installation instructions

Important

AWS CLI versions 1 and 2 use the same `aws` command name. If you previously installed AWS CLI version 1, see [Migrating from AWS CLI version 1 to version 2](#).

For installation instructions, expand the section for your operating system.

▶ Linux

▶ macOS

▶ Windows

- 아래 링크를 클릭하여 **Windows 64-bit용 AWS CLI MSI Installer**를 다운로드한다. 다운로드 받은 후 파일을 실행한다.

<https://awscli.amazonaws.com/AWSCLIV2.msi>

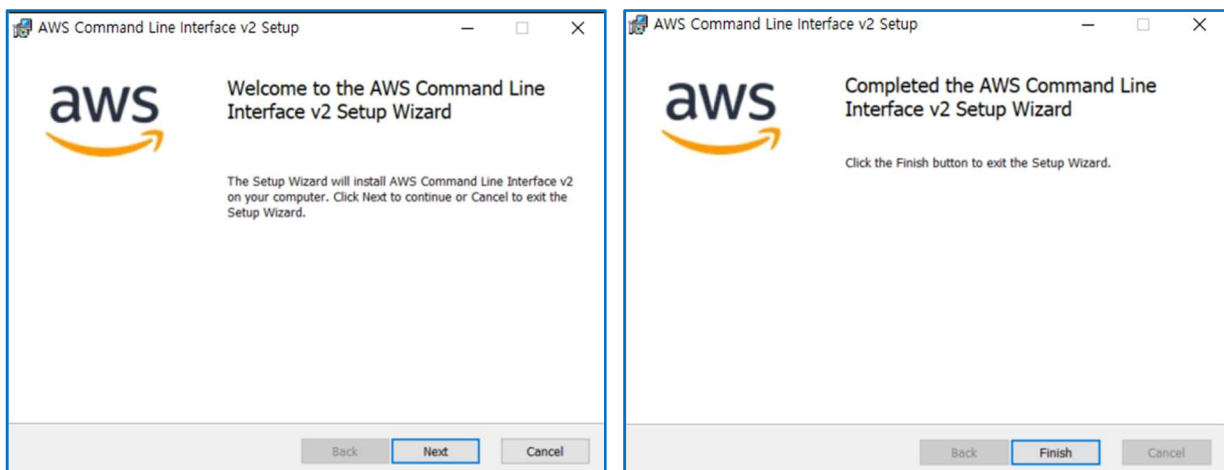
- 또는 **Windows Command** 창에서 다음과 같은 명령으로 실행할 수도 있다. 반드시 관리자 권한으로 실행해야 한다.

`msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi`

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

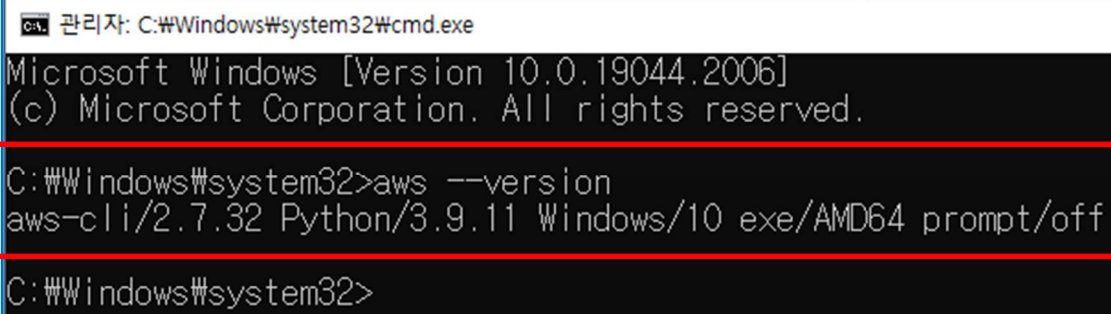
C:\Windows\system32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi
```

- 설치를 진행한다.



5. 반드시 **Command** 창을 닫았다가 다시 오픈한 후, 아래의 명령으로 설치 성공을 확인할 수 있다.

aws --version



```
관리자: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>aws --version
aws-cli/2.7.32 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\Windows\system32>
```

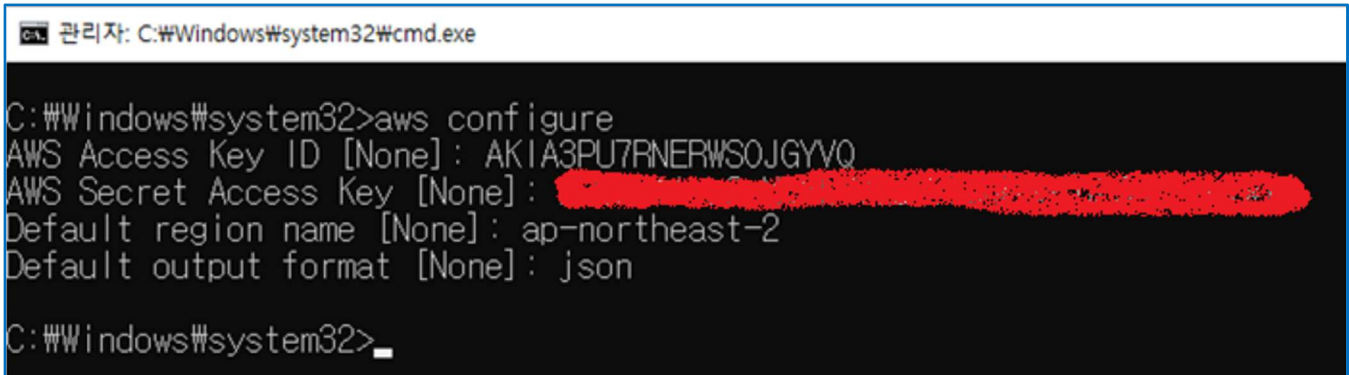
6. 위의 그림과 같은 결과가 나오면 성공적으로 설치된 것이다.

Configuring AWS CLI

1. **Windows Command** 창에서 **aws configure** 명령을 사용하여 환경 설정한다.

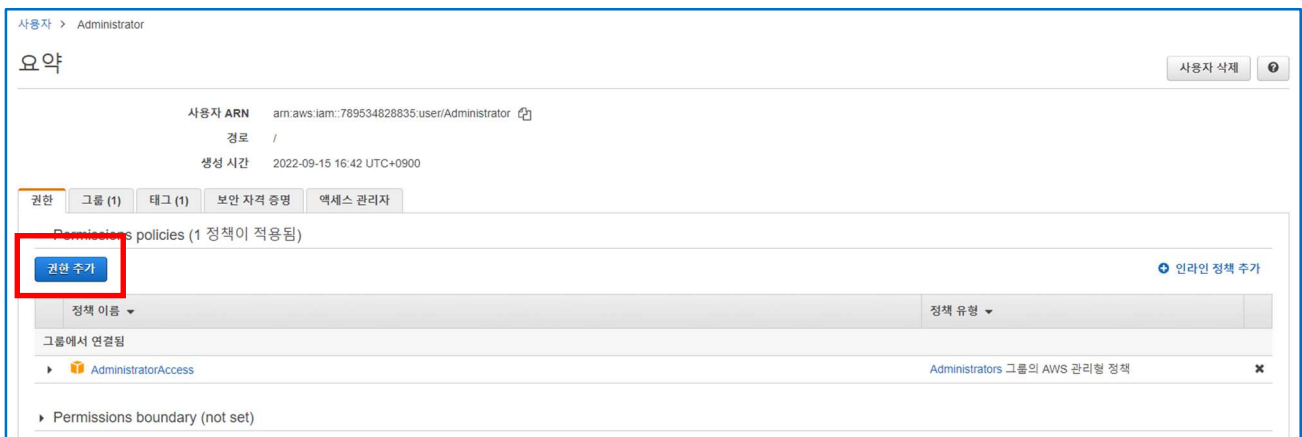
> **aws configure**

```
AWS Access Key ID [None]:  
AWS Secret Access Key [None]:  
Default region name [None]: ap-northeast-2  
Default output format [None]: json
```



```
C:\Windows\system32>aws configure  
AWS Access Key ID [None]: AKIA3PU7RNERWSOJGYVQ  
AWS Secret Access Key [None]: [REDACTED]  
Default region name [None]: ap-northeast-2  
Default output format [None]: json  
C:\Windows\system32>
```

2. 위에서 생성한 **Administrator** 사용자에게 권한을 추가하기 위해 **[권한 추가]**를 클릭한다.






3. [권한 부여] 페이지에서 [기존 정책 직접 연결]을 선택한다.

Administrator에 권한 추가

권한 부여

IAM 정책을 사용하여 권한을 부여합니다. 기존 정책을 할당하거나 새 정책을 생성할 수 있습니다.

 그룹에 사용자 추가  기존 사용자에서 권한 복사  기존 정책 직접 연결

정책 생성

정책 필터 777 결과 표시

<input type="checkbox"/>	정책 이름	유형	사용 용도
<input type="checkbox"/>	AdministratorAccess	직무 기반	Permissions policy (1)
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS 관리형	없음
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessLifeSizeDelegatedAccessPolicy	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS 관리형	없음
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS 관리형	없음
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS 관리형	없음
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS 관리형	없음
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS 관리형	없음




4. 다음의 정책을 검색하여 체크한 후, [다음:검토]를 클릭한다.

AWSLambda_FullAccess, AmazonAPIGatewayAdministrator, AmazonCognitoPowerUser

Administrator에 권한 추가

권한 부여

IAM 정책을 사용하여 권한을 부여합니다. 기존 정책을 할당하거나 새 정책을 생성할 수 있습니다.

 그룹에 사용자 추가  기존 사용자에서 권한 복사  기존 정책 직접 연결

정책 생성

정책 필터 3 결과 표시

<input type="checkbox"/>	정책 이름	유형	사용 용도
<input type="checkbox"/>	AmazonCognitoDeveloperAuthenticatedIdentities	AWS 관리형	없음
<input checked="" type="checkbox"/>	AmazonCognitoPowerUser	AWS 관리형	없음
<input type="checkbox"/>	AmazonCognitoReadOnly	AWS 관리형	없음

취소 **다음: 검토**

5. [권한 요약] 페이지에서 한 번 더 추가하려는 권한을 확인한 후, [권한 추가]를 클릭한다.

Administrator에 권한 추가

12

권한 요약

다음 정책이 위에 표시된 사용자에게 연결됩니다.

유형	이름
관리형 정책	AWSLambda_FullAccess
관리형 정책	AmazonAPIGatewayAdministrator
관리형 정책	AmazonCognitoPowerUser

[취소](#) [이전](#) [권한 추가](#)

6. 최종적으로 **Administrator** 사용자에게 4개의 정책이 설정된 것을 확인할 수 있다.

사용자 > Administrator

요약

사용자 삭제 ⓘ

사용자 ARN

am:aws:iam::789534828835:user/Administrator ⓘ

경로

/

생성 시간

2022-09-15 16:42 UTC+0900

권한

그룹 (1)

태그 (1)

보안 자격 증명

엑세스 관리자

▼ Permissions policies (4 정책이 적용됨)

[권한 추가](#) [인라인 정책 추가](#)

정책 이름 ▼	정책 유형 ▼	
직접 연결		
▶ AmazonAPIGatewayAdministrator	AWS 관리형 정책	✕
▶ AmazonCognitoPowerUser	AWS 관리형 정책	✕
▶ AWSLambda_FullAccess	AWS 관리형 정책	✕
그룹에서 연결됨		
▶ AdministratorAccess	Administrators 그룹의 AWS 관리형 정책	✕