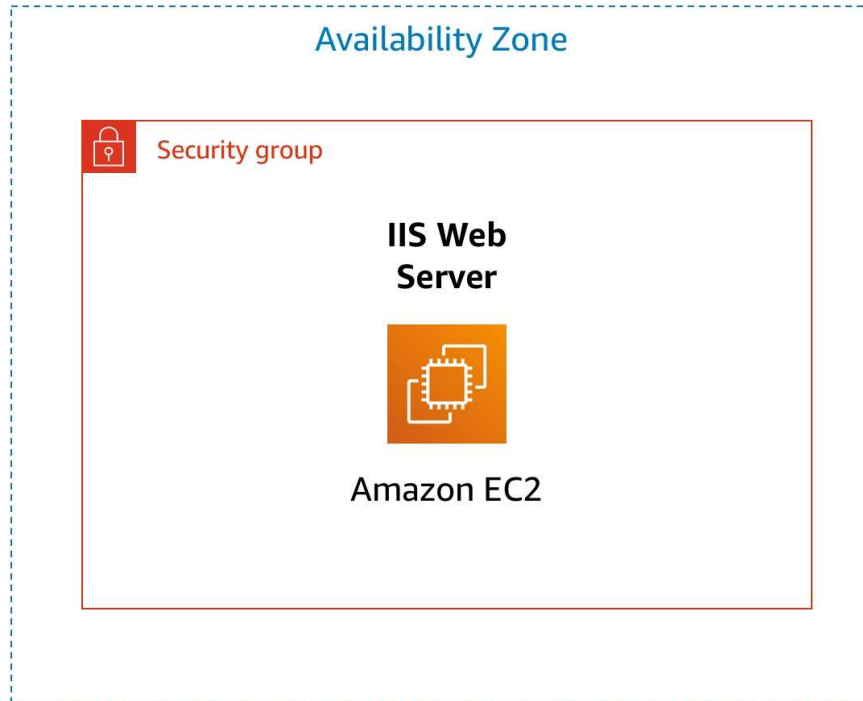


실습 – Ubuntu Server 설치 및 연결하기

개요



이 실습에서는 Amazon EC2 인스턴스의 시작, 크기 조정, 관리 및 모니터링에 대한 기본 개요를 제공한다.

Amazon Elastic Compute Cloud(Amazon EC2)는 클라우드에서 크기 조정 가능한 컴퓨팅 용량을 제공하는 웹 서비스이다. 개발자가 더 쉽게 웹 규모의 클라우드 컴퓨팅 작업을 할 수 있도록 설계되었다.

Amazon EC2의 간단한 웹 서비스 인터페이스를 통해 간편하게 필요한 용량을 얻고 구성할 수 있다. 사용자는 컴퓨팅 리소스를 완전히 제어하고 Amazon의 검증된 컴퓨팅 환경에서 리소스를 실행할 수 있다. Amazon EC2에서는 몇 분이면 새로운 서버 인스턴스를 확보하고 시작할 수 있으므로, 컴퓨팅 요구 사항의 변경에 따라 용량을 신속하게 Scale Up 및 Scale Down 할 수 있다.

또한 실제 사용한 만큼만 요금을 지불하면 되므로, 컴퓨팅 비용이 절약된다. Amazon EC2는 개발자에게 장애 발생 시 복원력이 뛰어난 애플리케이션을 구축하고 일반적인 장애 시나리오에서 애플리케이션을 격리할 수 있는 도구를 제공한다.

이 실습에서 다루는 주제

이 실습을 마치면 다음을 수행할 수 있다.

- 영구 종료 방지 기능이 활성화된 웹 서버 시작
- 웹 서버가 HTTP 액세스를 허용할 때 사용하는 보안 그룹의 수정

소요 시간

이 실습을 완료하는 데는 약 **45 분**이 소요된다.

과제 1: EC2 인스턴스 시작

이 과제에서는 *영구 종료 방지* 기능을 갖춘 Amazon EC2 인스턴스를 시작한다. 영구 종료 방지 기능은 EC2 인스턴스를 실수로 종료하는 것을 방지한다. 이 과제에서는 간단한 웹 서버를 배포하도록 하는 사용자 데이터 스크립트를 사용하여 인스턴스를 배포한다.

1. AWS 관리 콘솔의 [Services] 메뉴에서 [EC2]를 선택한다.
2. 대시보드 페이지에서 수행할 수 있도록 왼쪽 탐색 창에서 [EC2 Dashboard]를 선택한다.
3. [인스턴스 시작]을 선택한 다음 [인스턴스 시작]를 한 번 더 선택한다.

1 단계: EC2 인스턴스 이름 지정

사용자가 인스턴스의 이름을 지정할 때 AWS 는 키 값 페어를 생성한다. 이 페어의 키는 **Name** 이고, 값은 EC2 인스턴스에 입력하는 이름이다.

4. [이름 및 태그] 섹션의 [이름] 텍스트 상자에 **Web Server** 를 입력한다.

2 단계: Amazon Machine Image(AMI) 선택

AMI 는 클라우드의 가상 서버인 인스턴스를 시작하는 데 필요한 정보를 제공한다. AMI 는 다음을 포함한다.

- 인스턴스 루트 볼륨에 대한 템플릿(예: 애플리케이션을 포함한 운영 체제 또는 애플리케이션 서버)
- AMI 를 사용하여 인스턴스를 시작할 수 있는 AWS 계정을 제어하는 시작 권한
- 인스턴스 시작 시 인스턴스에 연결할 볼륨을 지정하는 블록 디바이스 매핑

Quick Start 목록에는 가장 자주 사용되는 AMI 가 포함된다. 자체 AMI 를 생성하거나, AWS 에서 실행되는 소프트웨어를 판매 또는 구매할 수 있는 온라인 상점인 AWS Marketplace 에서 AMI 를 선택할 수도 있다.

5. [Application and OS Images (Amazon Machine Image)] 섹션에서
6. **AMI Machine Image (AMI)**에서 **Amazon Linux 2023 AMI** 이미지가 기본적으로 선택되어 있을 것이다. 먼저 [Quick Start] 목록에서 Ubuntu 를 선택하고 목록에서 Ubuntu Server 22.04 LTS (HVM), SSD Volume Type 을 선택한다.

▼ **Application and OS Images (Amazon Machine Image)** [정보](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows


Microsoft

Red Hat

Red Hat

SUSE Li

SUSE


더 많은 AMI 찾아보기
AWS, Marketplace 및 커뮤니티의 AMI 포함

Amazon Machine Image(AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-086cae3329a3f7d75 (64비트(x86)) / ami-0f8536fc6ad2ba267 (64비트(Arm))
가상화: hvm ENA enabled: true 루트 디바이스 유형: ebs

프리 티어 사용 가능 ▼

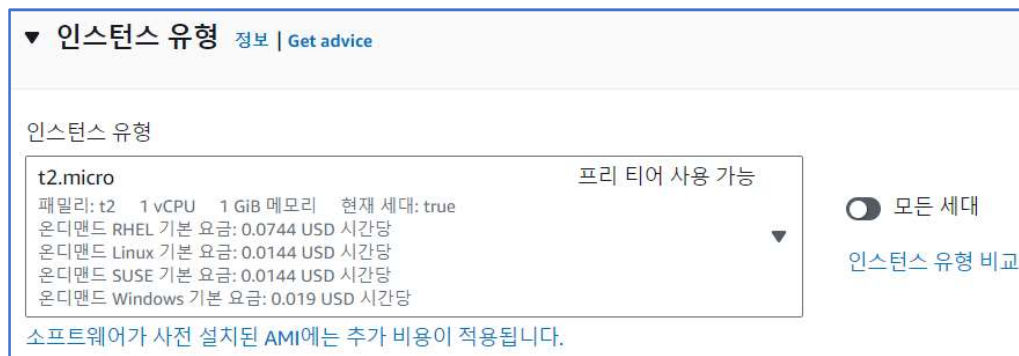
3 단계: 인스턴스 유형 선택

Amazon EC2 는 각 사용 사례에 맞게 최적화된 다양한 *인스턴스 유형*을 제공한다. 인스턴스 유형은 CPU, 메모리, 스토리지, 네트워킹 용량의 다양한 조합으로 구성되며, 애플리케이션에 따라 적합한 리소스 조합을 선택할 수 있는 유연성을 제공한다. 각 인스턴스 유형은 하나 이상의 *인스턴스 크기*를 포함하고 있어 대상 워크로드의 요구 사항에 따라 리소스의 크기를 조정할 수 있다.

t2.micro 인스턴스를 선택한다. 이 인스턴스 유형에는 가상 CPU 1 개와 1GiB 메모리가 있다.

7. 드롭다운에서 **t2.micro** 를 선택한다.

참고: 이 실습에서는 다른 인스턴스 유형을 사용하는 것이 제한될 수 있다.



4 단계: 키 페어 구성

Amazon EC2 는 Public 키 암호화 기법을 사용하여 로그인 정보를 암호화하고 복호화한다. 인스턴스에 로그인하려면 키 페어를 만들고, 인스턴스를 실행할 때 키 페어의 이름을 지정하고, 인스턴스에 연결할 때 Private 키를 제공해야 한다.

8. [키 페어(로그인)] 섹션에서 새로운 키를 생성하기 위해 [새 키 페어 생성] 링크를 클릭한다.
9. [키 페어 생성] 창에서 [키 페어 이름] 텍스트 상자에 **lab-ec2-key** 라고 입력한다.
10. 나머지 값은 기본값 그대로 사용한다. [키 페어 생성] 버튼을 클릭한다.

키 페어 생성

키 페어 이름

키 페어를 사용하면 인스턴스에 안전하게 연결할 수 있습니다.

lab-ec2-key

이름에는 최대 255개의 ASCII 문자를 포함할 수 있습니다. 앞 또는 뒤에 공백을 포함할 수 없습니다.

키 페어 유형

☒ RSA
RSA 암호화된 프라이빗 및 퍼블릭 키 페어

☐ ED25519
ED25519 암호화된 프라이빗 및 퍼블릭 키 페어

프라이빗 키 파일 형식

☒ .pem
OpenSSH와 함께 사용

☐ .ppk
PuTTY와 함께 사용

⚠

메시지가 표시되면 프라이빗 키를 사용자 컴퓨터의 안전하고 액세스 가능한 위치에 저장합니다. 나중에 인스턴스에 연결할 때 필요합니다.

자세히 알아보기

취소

키 페어 생성

11. 방금 생성한 Private Key 를 로컬 컴퓨터에 저장해야 한다. 실습을 위해 찾기 쉬운 곳에 저장한다.
(예:Windows 의 경우 C:\temp 폴더, macOS 의 경우 홈 디렉토리)

▼ 키 페어(로그인) 정보

키 페어를 사용하여 인스턴스에 안전하게 연결할 수 있습니다. 인스턴스를 시작하기 전에 선택한 키 페어에 대한 액세스 권한이 있는지 확인하세요.

키 페어 이름 - 필수

lab-ec2-key

새 키 페어 생성

5 단계: 네트워크 설정 구성

이 창을 사용하여 네트워킹 설정을 구성한다.

VPC 는 인스턴스를 시작할 Virtual Private Cloud(VPC)를 나타낸다. 개발, 테스트 및 프로덕션을 위한 서로 다른 VPC 를 포함하여 여러 개의 VPC 를 사용할 수 있다.

12. [네트워크 설정] 섹션에서 [편집]을 선택하여 다음과 같이 각각의 값을 설정한다.
선택합니다.

13. [VPC -required] : default-vpc(기본 VPC)

14. [서브넷] : ap-northeast-2a

15. [퍼블릭 IP 자동 할당] : 활성화

▼ 네트워크 설정 정보

VPC - required 정보

vpc-06cc1e03aaa8fd14e (Default-VPC) (기본값) ↕

172.31.0.0/16

서브넷 정보

subnet-0539a07bde3b1c1af public-subnet ↕

VPC: vpc-06cc1e03aaa8fd14e 소유자: 789534828835 가용 영역: ap-northeast-2a

사용 가능한 IP 주소: 4091 CIDR: 172.31.0.0/20

퍼블릭 IP 자동 할당 정보

활성화 ↕

보안 그룹은 하나 이상의 인스턴스에 대한 트래픽을 제어하는 가상 방화벽 역할을 한다. 인스턴스를 시작할 때 하나 이상의 보안 그룹을 인스턴스와 연결한다. 연결된 인스턴스와 트래픽을 주고받을 수 있게 하는 **규칙**을 각 보안 그룹에 추가한다. 언제든지 보안 그룹에 대한 규칙을 수정할 수 있다. 새 규칙은 보안 그룹과 연결된 모든 인스턴스에 자동으로 적용된다.

16. [방화벽(보안 그룹)] > [보안 그룹 생성] 선택

17. [보안 그룹 이름 - 필수] : lab-sg

18. [설명 - 필수] : Security group for Ubuntu Server

19. [인바운드 보안 그룹 규칙] : 기본값 그대로 사용

방화벽(보안 그룹) 정보

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 특정 트래픽이 인스턴스에 도달하도록 허용하는 규칙을 추가합니다.

☒ 보안 그룹 생성 ☐ 기존 보안 그룹 선택

보안 그룹 이름 - 필수

lab-sg

이 보안 그룹은 모든 네트워크 인터페이스에 추가됩니다. 보안 그룹을 만든 후에는 이름을 편집할 수 없습니다. 최대 길이는 255자입니다. 유효한 문자는 a~z, A~Z, 0~9, 공백 및 . _ : / () # . @ [] + = & ; ! \$ * 입니다.

설명 - 필수 정보

Security group for Ubuntu Server

인바운드 보안 그룹 규칙

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) 제거

유형	정보	프로토콜	정보	포트 범위	정보
ssh		TCP		22	

소스 유형	정보	원본	정보	설명 - optional	정보
위치 무관		Q CIDR, 접두사 목록 또는 보안 그룹		e.g. SSH for admin desktop	

0.0.0.0/0 X

6 단계: 스토리지 추가

Amazon EC2 는 Amazon Elastic Block Store(Amazon EBS)라고 하는 네트워크 연결 가상 디스크에 데이터를 저장한다.

이 실습에서는 기본 8 GiB 디스크 볼륨을 사용하여 EC2 인스턴스를 시작한다. 이 볼륨이 루트 볼륨('부트' 볼륨이라고도 함)이다.

20.[스토리지 구성] 섹션에서 기본 스토리지 구성을 유지한다.

▼ 스토리지 구성 정보 어드밴스드

1x 8 GiB gp2 루트 볼륨 (암호화되지 않음)

❗ 프리 티어를 사용할 수 있는 고객은 최대 30GB의 EBS 범용(SSD)또는 마그네틱 스토리지를 사용할 수 있습니다. X

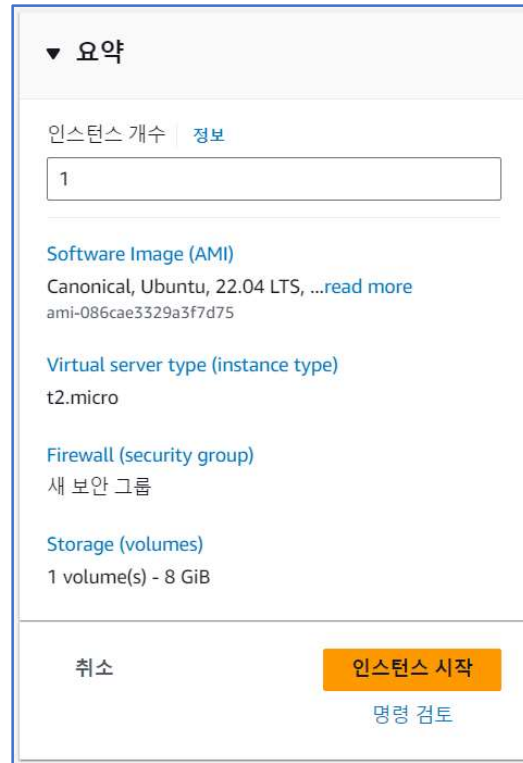
새 볼륨 추가

0 x 파일 시스템 편집

7 단계: EC2 인스턴스 시작하기

이제 EC2 인스턴스 설정을 구성했으므로 인스턴스를 시작할 차례이다.

21. 오른쪽 창에서 **Launch instance(인스턴스 시작)**를 선택한다.



▼ 요약

인스턴스 개수 | 정보

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-086cae3329a3f7d75

Virtual server type (instance type)
t2.micro

Firewall (security group)
새 보안 그룹

Storage (volumes)
1 volume(s) - 8 GiB

취소 인스턴스 시작 명령 검토

22. **View all instances(모든 인스턴스 보기)**를 선택한다.

인스턴스가 **Pending** 상태로 표시되며, 이는 시작 중임을 의미한다. 이후 **Running** 으로 변하는데, 이는 인스턴스 부팅이 시작되었다는 의미이다. 인스턴스에 액세스할 수 있을 때까지 잠시 시간이 걸릴 수 있다.

인스턴스에서 수신하는 퍼블릭 DNS 이름은 사용자가 인터넷상에서 해당 인스턴스에 접속할 때 사용된다.

23. **Web Server** 옆에 있는 확인란을 선택한다. **Details** 탭에 인스턴스의 세부 정보가 표시된다.

Details 탭에서 추가 정보를 보려면 창 구분선을 위로 끌어 올린다.

Details, Security 및 **Networking** 탭에 표시되는 정보를 검토한다.

24. 인스턴스에 다음이 표시될 때까지 기다린다.

참고: 새로 고침이 필요할 수 있다.

- Instance State: ● Running
- Status Checks: ✔ 2/2 checks passed

과제 2: 원격 서버 연결하기

25. 방금 설치한 Web Server 의 [세부 정보] 탭에서 [퍼블릭 IPv4 주소]를 확인한다.
26. 원격 서버와 연결하기 위해 Tabby 프로그램을 각 OS 별로 설치한 후, 다음과 같이 연결하기 위한 설정을 한다.

Web Server

Name: Web Server

Group: Ungrouped

Icon: fas fa-desktop

Color: #000000

Disable dynamic tab title: ☒ Connection name will be used instead

GENERAL | PORTS | ADVANCED | CIPHERS | COLORS | LOGIN SCRIPTS

Connection: Direct | Host: 13.124.10.57 | Port: 22

Username: ubuntu

Authentication method: Auto | Password | **Key** | Agent | Interactive

Private keys: file:///C:/Temp/lab-ec2-key.pem

Add a private key

Save Cancel

27. [Save] 버튼을 클릭하여 저장 후 원격 서버와 연결한다.

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1012-aws x86_64)

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

System information as of Tue Dec 19 03:02:05 UTC 2023

System load: 0.0166015625	Processes: 97
Usage of /: 20.5% of 7.57GB	Users logged in: 0
Memory usage: 21%	IPv4 address for eth0: 172.31.3.46
Swap usage: 0%	

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.


Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: `sudo pro status`

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in `/usr/share/doc/*/copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "`sudo <command>`".
See "`man sudo_root`" for details.

ubuntu@ip-172-31-3-46:~\$ 

과제 3: 웹 서버 설치, 보안 그룹 업데이터 그리고 액세스하기

28. Ubuntu Server 를 원격으로 연결한 다음, 다음과 같은 명령어를 사용하여 Apache Web Server 를 설치한다.

```
$ sudo apt update
$ sudo apt install -y apache2
$ sudo systemctl status apache2
```

```
ubuntu@ip-172-31-3-46:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-12-19 03:08:27 UTC; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2410 (apache2)
    Tasks: 55 (limit: 1121)
   Memory: 4.9M
      CPU: 54ms
   CGroup: /system.slice/apache2.service
           └─2410 /usr/sbin/apache2 -k start
             └─2412 /usr/sbin/apache2 -k start
               └─2413 /usr/sbin/apache2 -k start

Dec 19 03:08:27 ip-172-31-3-46 systemd[1]: Starting The Apache HTTP Server...
Dec 19 03:08:27 ip-172-31-3-46 systemd[1]: Started The Apache HTTP Server.
ubuntu@ip-172-31-3-46:~$
```

인스턴스 (1/1) 정보

🔄

연결

인스턴스 상태 ▼

작업 ▼

인스턴스 시작 ▼

🔍 Instance을 속성 또는(case-sensitive) 태그로 찾기

< 1 > ⚙️

☑	Name ↗	인스턴스 ID	인스턴스 상태 ▼	인스턴스 유형 ▼	상태 검사	경보 상태	가용 영역 ▼
☑	Web Server	i-09c6567c3d9bf7478	🟢 실행 중 🔍	t2.micro	🟢 2/2개 검사 통과	경보 없음 +	ap-northeast-2a

인스턴스: i-09c6567c3d9bf7478(Web Server) ⚙️ ✕

세부 정보

보안

네트워킹

스토리지

상태 검사

모니터링

태그

▼ 인스턴스 요약 정보

인스턴스 ID

📄 i-09c6567c3d9bf7478 (Web Server)

퍼블릭 IPv4 주소

📄 13.124.10.57 | [개방 주소법](#) 🔗

인스턴스 상태

🟢 실행 중

IPv6 주소

-

프라이빗 IPv4 주소

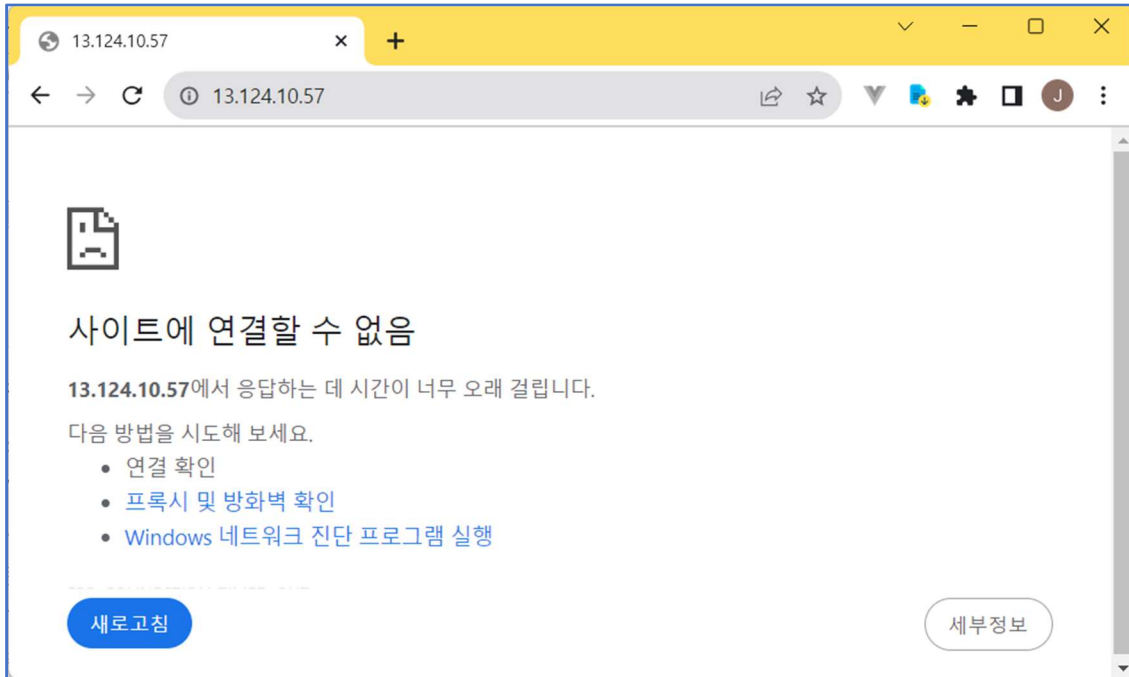
📄 172.31.3.46

퍼블릭 IPv4 DNS

📄 ec2-13-124-10-57.ap-northeast-2.compute.amazonaws.com | [개방 주소법](#) 🔗

29. 웹 브라우저에서 새 탭을 열고 [퍼블릭 IPv4 주소]를 복사해서 붙여 넣은 다음 **Enter** 키를 누른다.

질문: 웹 서버에 액세스할 수 있습니까? 안 될 이유는 없죠.

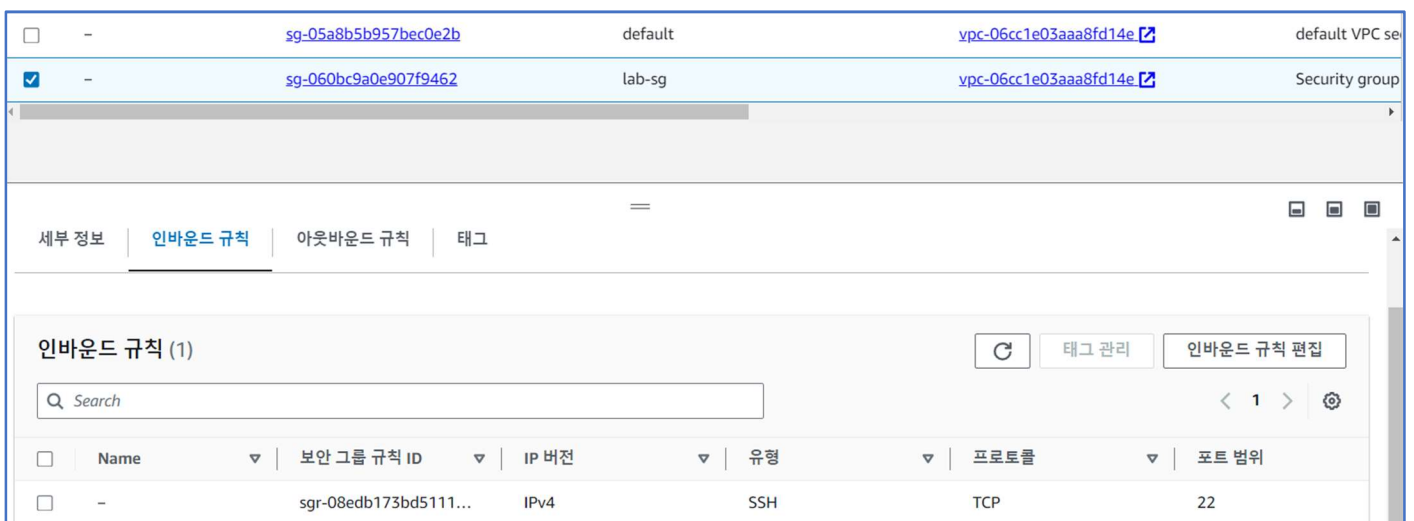


보안 그룹 이 HTTP 웹 요청에 사용되는 포트 80 에서 인바운드 트래픽을 허용하지 않기 때문에 현재 웹 서버에 액세스할 수 없다. 이 데모에서는 인스턴스 출입이 허용되는 네트워크 트래픽을 제한하기 위해 보안 그룹을 방화벽으로 사용하는 방법을 보여준다.

이 문제를 해결하기 위해 이제 포트 80 에서 웹 트래픽을 허용하도록 보안 그룹을 업데이트할 것이다.

30. 브라우저 탭이 열려 있는 상태에서 **EC2 Management Console** 탭으로 돌아간다.
31. 왼쪽 탐색 창의 **Network & Security(네트워크 및 보안)** 메뉴에서 **Security Groups(보안 그룹)**를 선택한다.
32. [보안 그룹 이름] 중 **lab-sg** 를 선택한다.
33. **Inbound rules(인바운드 규칙)** 탭을 선택한다.

현재 보안 그룹에는 규칙이 22 번 SSH 한 개 밖에 없다.



34. **Edit inbound rules(인바운드 규칙 편집)**을 선택한 후 **Add rule(규칙 추가)**을 선택하고 다음 설정으로 규칙을 구성합니다.

- **Type: HTTP**
- **Source: Anywhere-IPv4**
- **Save rules(규칙 저장)**를 선택한다.

인바운드 규칙 편집 정보
인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보

보안 그룹 규칙 ID	유형 <small>정보</small>	프로토콜 <small>정보</small>	포트 범위 <small>정보</small>	소스 <small>정보</small>	설명 - 선택 사항 <small>정보</small>	
sgr-08edb173bd51112d6	SSH	TCP	22	사용... 0.0.0.0/0 X		삭제
-	HTTP	TCP	80	Anyw... 0.0.0.0/0 X		삭제

규칙 추가

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

취소 변경 사항 미리 보기 **규칙 저장**

35. 이전에 열었던 웹 서버 탭으로 돌아가서 페이지를 새로 고친다.

Ubuntu Server 용 Apache 홈페이지가 나타난다.

