

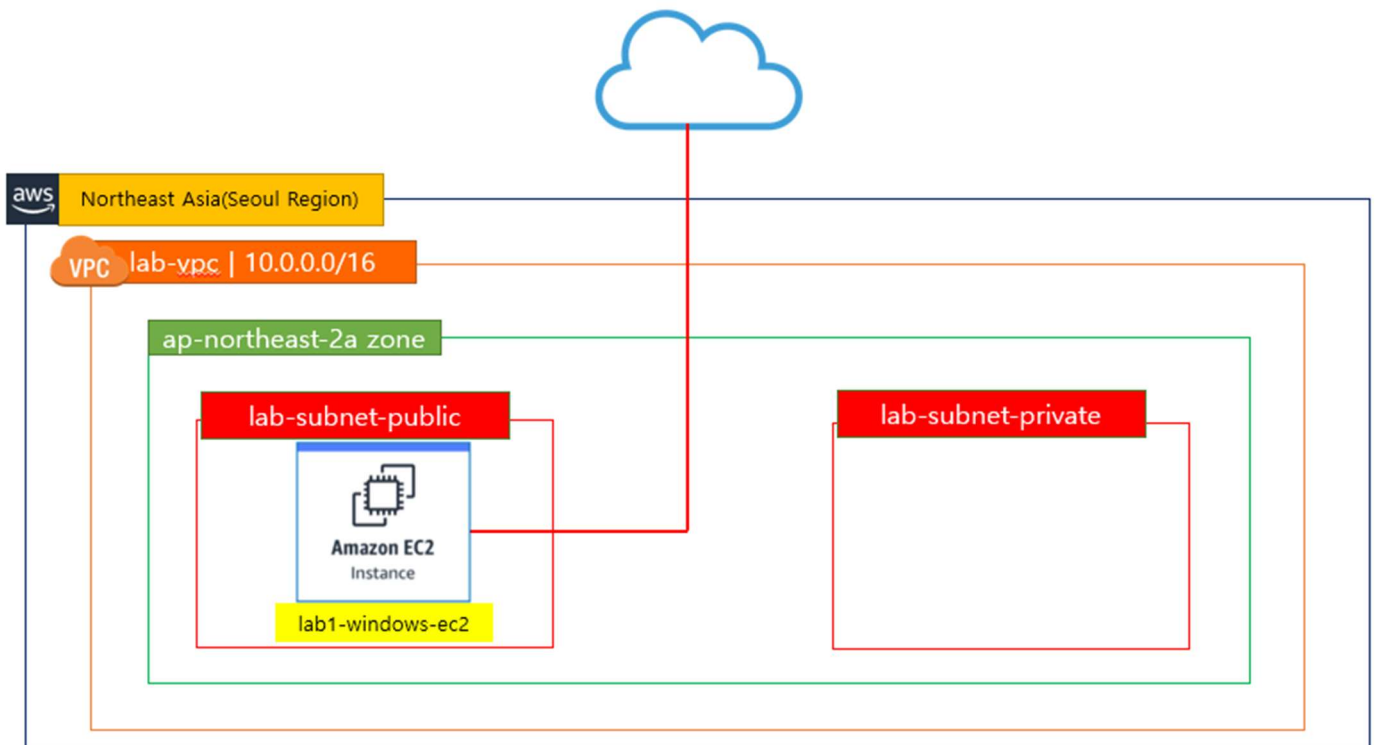
Lab1. EC2를 이용해서 Windows Instance 서버 만들기

목적

Amazon EC2(Elastic Compute Cloud)를 사용하여 Windows 인스턴스를 생성하고 접속하는 방법을 학습한다. 또한 생성된 Windows 서버의 시작, 중지 및 EC2 인스턴스에 대한 삭제 방법을 다뤄본다. 이 학습은 AWS Free-Tier를 활용하여 진행한다.

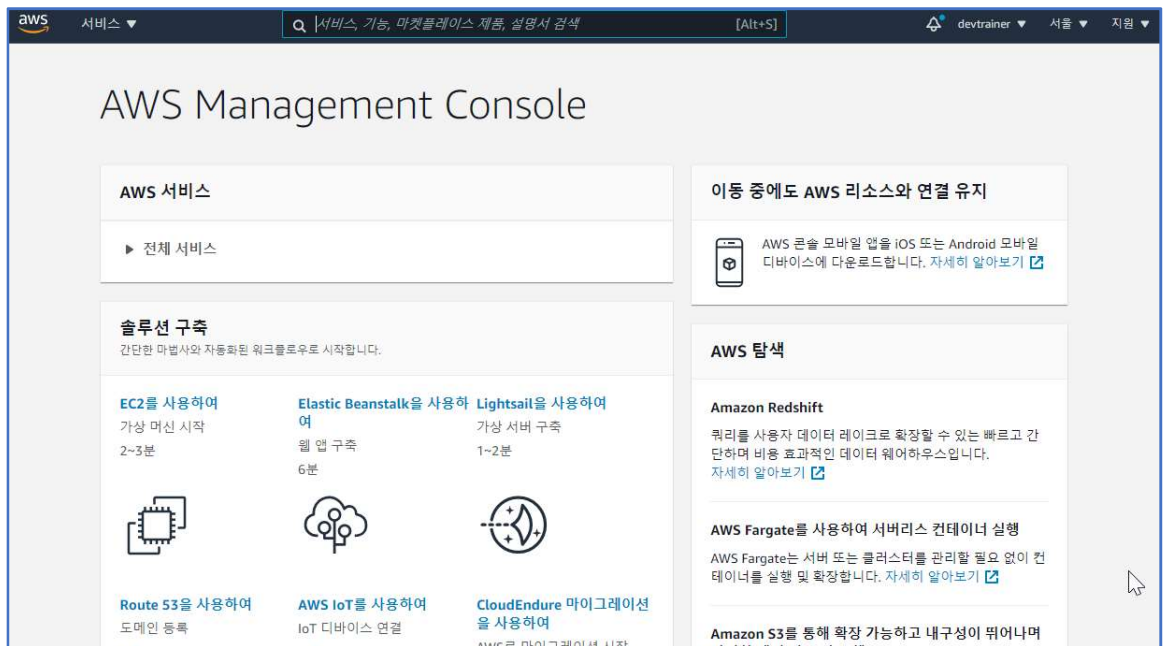
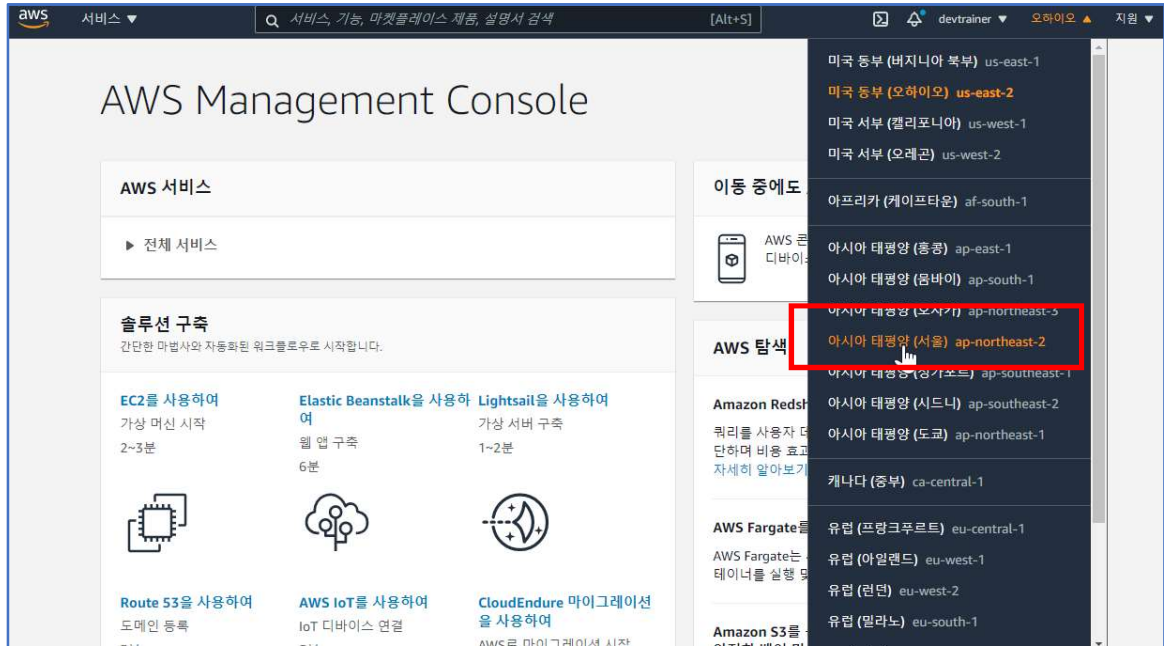
사전 준비물

AWS Free-Tier 계정

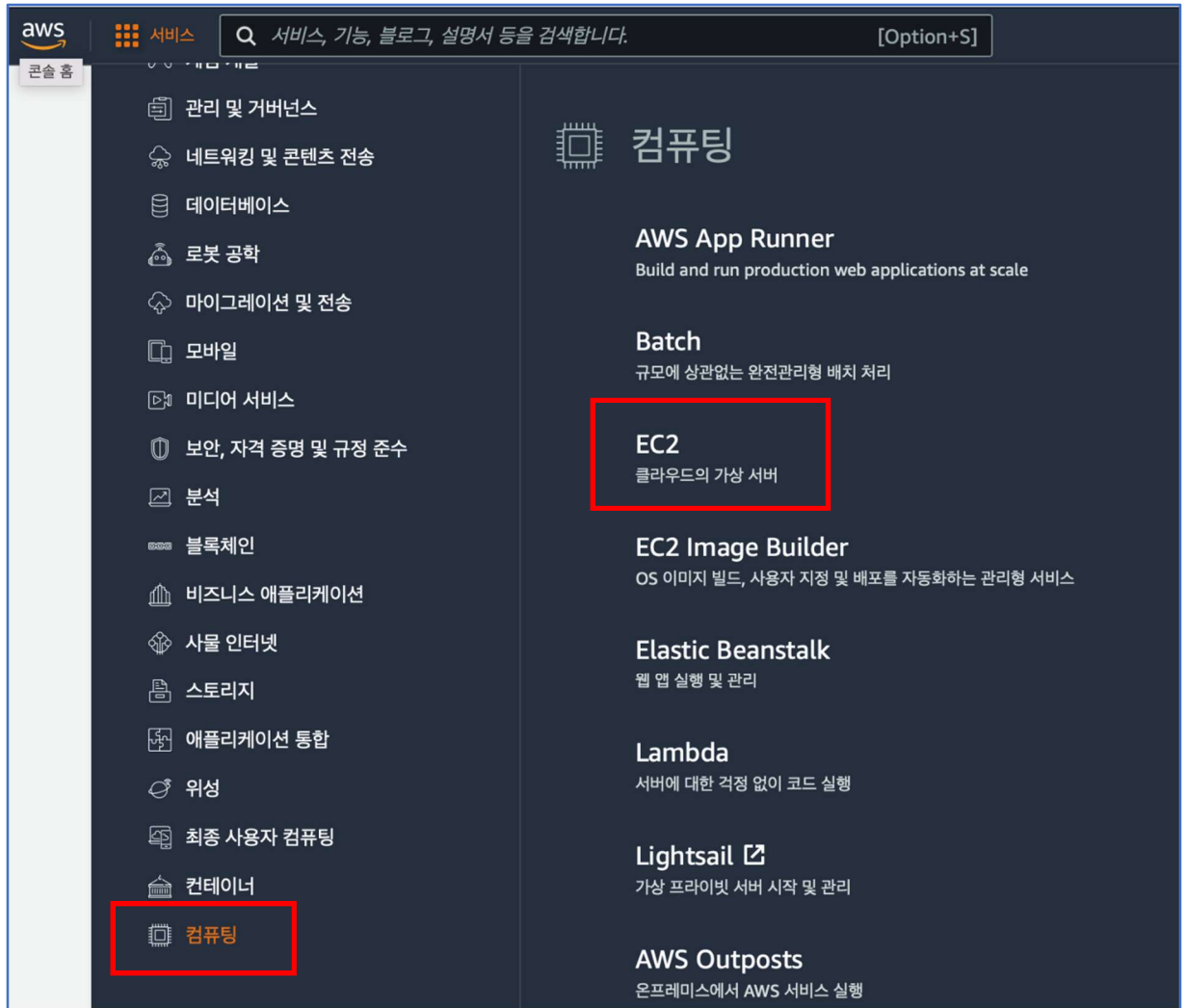


Windows 서버 EC2 인스턴스 생성하기

- A. 로그인 후 우측 상단에 AWS 리전 선택 항목에서 [아시아 태평양(서울)]을 선택하여 [서울] 페이지로 접속한다.



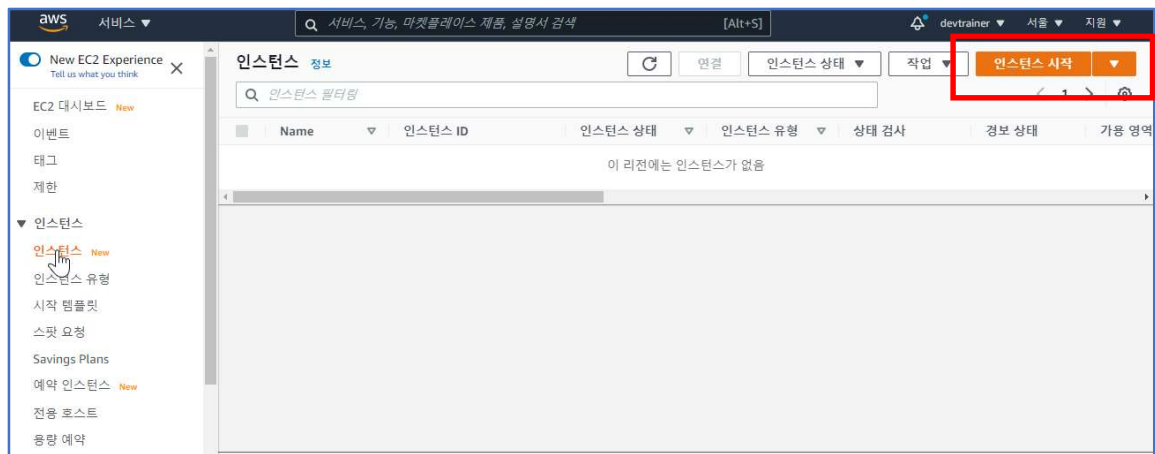
B. 이번에는 좌측 상단의 [서비스] > [컴퓨팅] > [EC2]를 클릭하여 해당 페이지로 이동한다.



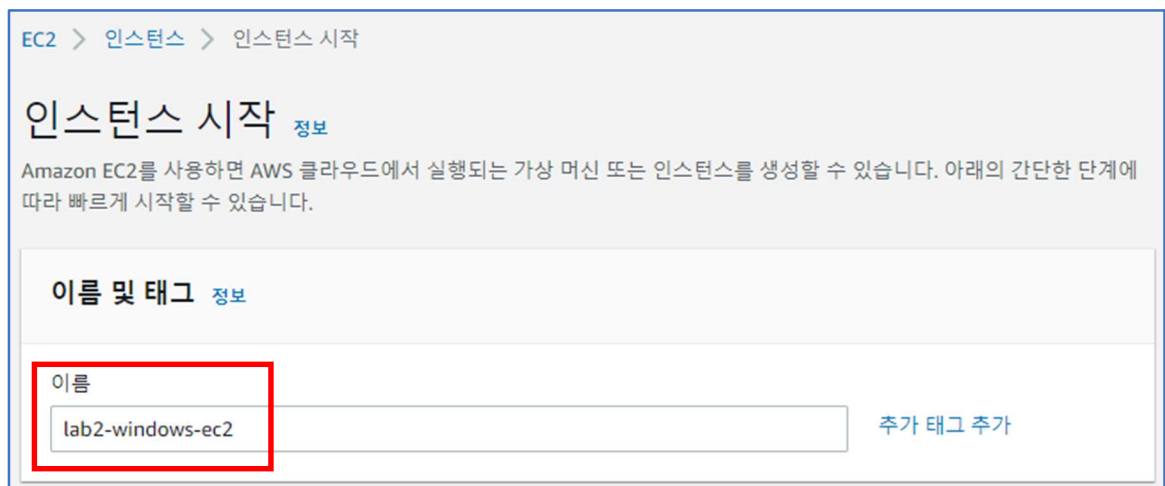
C. 왼쪽 항목에서 [인스턴스]를 선택하여 해당 페이지로 이동한다.



D. 우측 상단의 [인스턴스 시작] 오렌지 색 버튼을 클릭한다.



E. [인스턴스 시작]에서 [이름 및 태그]의 값을 "lab2-windows-ec2"로 입력한다.



- F. [애플리케이션 및 OS 이미지] 페이지에서, [Quick Start]목록 중 [Microsoft Windows]를 마우스로 선택 후, 그 아래 세부사항 목록을 클릭하여 [Microsoft Windows Server 2022 Base]를 선택한다.

▼ 애플리케이션 및 OS 이미지(Amazon Machine Image) 정보

AMI는 인스턴스를 시작하는 데 필요한 소프트웨어 구성(운영 체제, 애플리케이션 서버 및 애플리케이션)이 포함된 템플릿입니다. 아래에서 찾고 있는 항목이 보이지 않으면 AMI를 검색하거나 찾아보십시오.

수천 개의 애플리케이션 및 OS 이미지를 포함하는 전체 카탈로그 검색

Quick Start

Amazon Linux macOS Ubuntu **Windows** Red Hat S

aws Mac ubuntu Microsoft Red Hat

더 많은 AMI 찾아보기
AWS, Marketplace 및 커뮤니티의 AMI 포함

Amazon Machine Image(AMI)

Microsoft Windows Server 2022 Base 프리 티어 사용 가능 ▼
ami-0fb5bafc1450ca205 (64비트(x86))
가상화: hvm ENA 활성화됨: true 루트 디바이스 유형: ebs

설명
Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

아키텍처	AMI ID
64비트(x86)	ami-0fb5bafc1450ca205

확인된 공급 업체

- G. [인스턴스 유형] 섹션에서 [인스턴스 유형]을 "t2.micro"를 선택한다.

▼ 인스턴스 유형 정보

인스턴스 유형

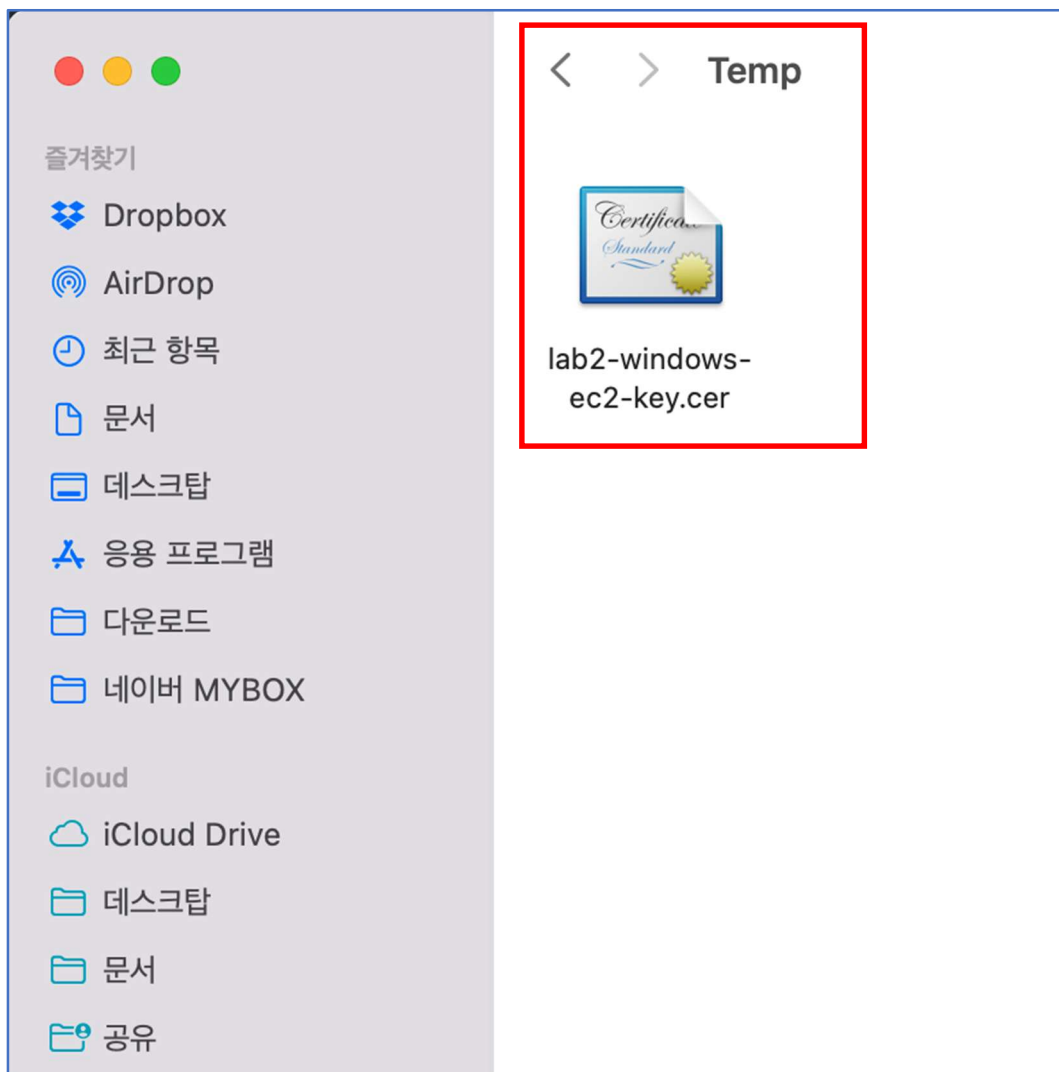
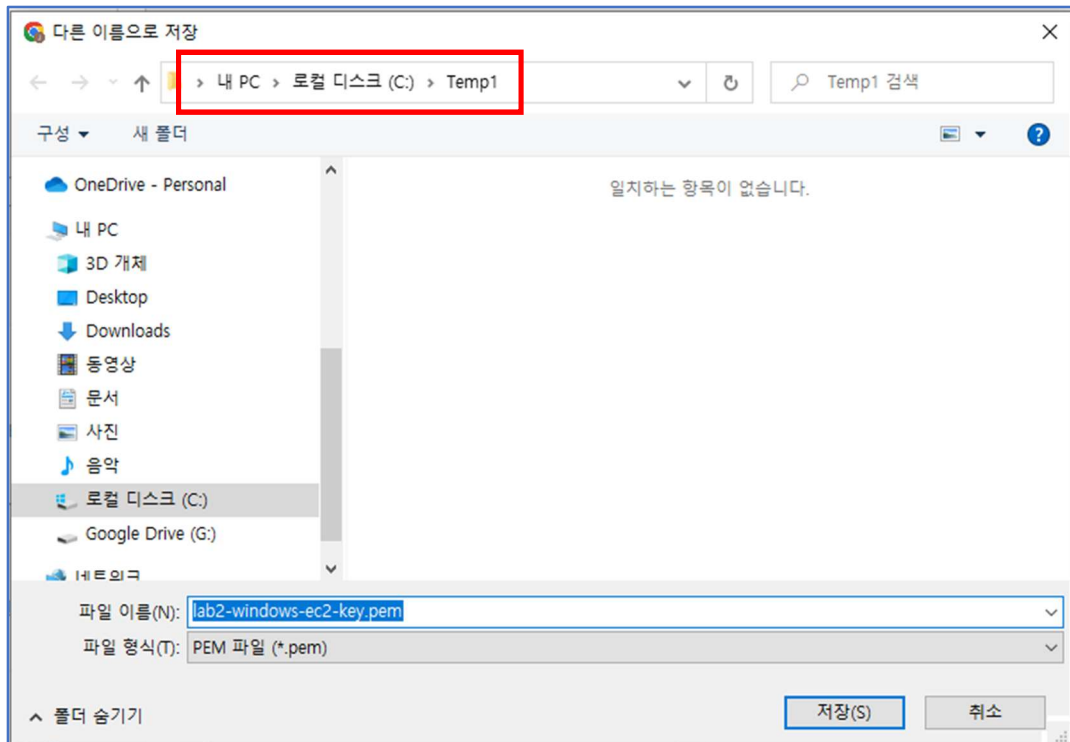
t2.micro 프리 티어 사용 가능 ▼
패밀리: t2 1 vCPU 1 GiB 메모리 온디맨드 Linux 요금: 0.0116 USD 시간당
온디맨드 Windows 요금: 0.0162 USD 시간당

인스턴스 유형 비교

H. [키 페어(로그인)] 섹션에서 [새 키 페어 생성]을 클릭한다.

I. [키 페어 생성]창에서 [키 페어 이름]을 “lab2-windows-ec2-key”로 입력하고, [프라이빗 키 파일 형식]에서 [.pem]을 선택한 후, [키 페어 생성] 오렌지 색 버튼을 클릭한다.

J. [다른 이름으로 저장] 창에서 찾기 쉬운 위치에 **pem** 파일을 저장한다.



- K. [네트워크 설정] 섹션에서 Lab1에서 생성한 VPC와 서브넷 정보를 확인할 수 있다. [편집] 버튼을 클릭한다.

▼ 네트워크 설정 정보

편집

네트워크 정보
vpc-01d721e15c781dacd | lab1-vpc-vpc

서브넷 정보
subnet-0e8ee4da6f5a97f63 | lab1-vpc-subnet-public1-ap-northeast-2a

퍼블릭 IP 자동 할당 정보
비활성화

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

다음 규칙을 사용하여 'launch-wizard-1'(이)라는 새 보안 그룹을 생성합니다.

☒ 에서 RDP 트래픽 허용
인스턴스 연결에 도움 위치 무관
0.0.0.0/0

☐ 인터넷에서 HTTPS 트래픽 허용
예를 들어 웹 서버를 생성할 때 엔드포인트를 설정하려면

☐ 인터넷에서 HTTP 트래픽 허용
예를 들어 웹 서버를 생성할 때 엔드포인트를 설정하려면

⚠ 소스가 0.0.0.0/0인 규칙은 모든 IP 주소에서 인스턴스에 액세스하도록 허용합니다. 알려진 IP 주소의 액세스만 허용하도록 보안 그룹을 설정하는 것이 좋습니다.

- L. 아래와 같이 [퍼블릭 IP 자동 할당]의 값을 [활성화]로 수정한다.

▼ 네트워크 설정 정보

VPC - 필수 정보
vpc-01d721e15c781dacd (lab1-vpc-vpc)
172.16.0.0/16

서브넷 정보
subnet-0e8ee4da6f5a97f63 lab1-vpc-subnet-public1-ap-northeast-2a
VPC: vpc-01d721e15c781dacd 소유자: 789534828835
가용 영역: ap-northeast-2a IP 주소 사용 가능: 4090 CIDR: 172.16.0.0/20

퍼블릭 IP 자동 할당 정보
활성화

M. [방화벽(보안 그룹)] 섹션에서 다음과 같이 설정한다.

A. [보안 그룹 생성]

B. [보안 그룹 이름] : lab2-windows-sg

C. [설명] : Security Group for Windows Instance

D. [인바운드 보안 그룹 규칙] : 기본값

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
lab2-windows-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 Windows Instance

인바운드 보안 그룹 규칙
▼ 보안 그룹 규칙 1 (TCP, 3389, 0.0.0.0/0) 제거

유형 정보	프로토콜 정보	포트 범위 정보
rdp	TCP	3389

소스 유형 정보	원본 정보	설명 - optional 정보
위치 무관	Q CIDR, 접두사 목록 또는 보안 그룹 0.0.0.0/0 X	예: 관리자 데스크톱용 SSH

⚠ 소스가 0.0.0.0/0인 규칙은 모든 IP 주소에서 인스턴스에 액세스하도록 허용합니다. 알려진 IP 주소의 액세스만 허용하도록 보안 그룹을 설정하는 것이 좋습니다.

N. [스토리지 구성] 섹션에서 스토리지는 기본값 그대로 사용하기로 한다. 오른쪽의 [인스턴스 시작] 버튼을 클릭한다.

▼ 스토리지 구성 정보 어드밴스드

1x 30 GiB gp2 루트 볼륨

① 프리 티어를 사용할 수 있는 고객은 최대 30GB의 EBS 범용(SSD) 또는 마그네틱 스토리지를 사용할 수 있습니다.

새 볼륨 추가

선택한 AMI에 인스턴스가 허용하는 것보다 많은 인스턴스 스토어 볼륨이 포함되어 있습니다. AMI에서 처음 0개의 인스턴스 스토어 볼륨에만 액세스할 수 있습니다.

0 x 파일 시스템 편집

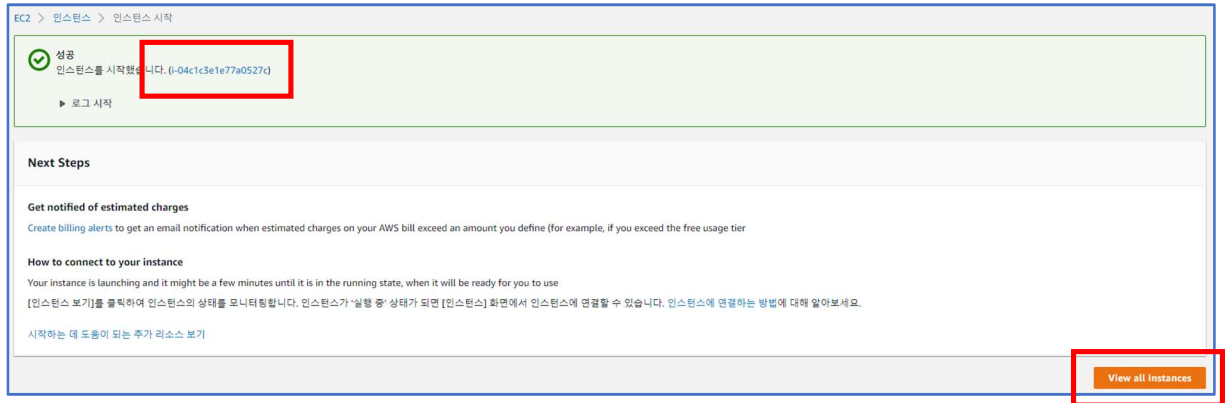
▶ 고급 세부 정보 정보

스토리지(볼륨)
1개의 볼륨 - 30GiB

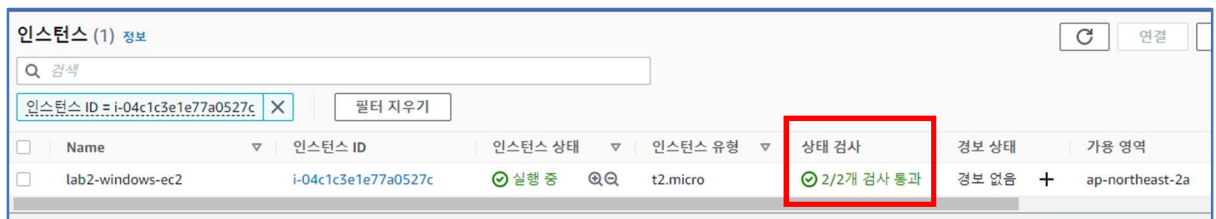
① 프리 티어: 첫 해에는 랙별 프리 티어 AMI에 대한 t2.micro(또는 t2.micro를 사용할 수 없는 리전의 t3.micro) 인스턴스 사용량 750시간, EBS 스토리지 30GiB, IO 2백만 개, 스냅샷 1GB, 인터넷 대역폭 100GB가 포함됩니다.

취소 **인스턴스 시작**

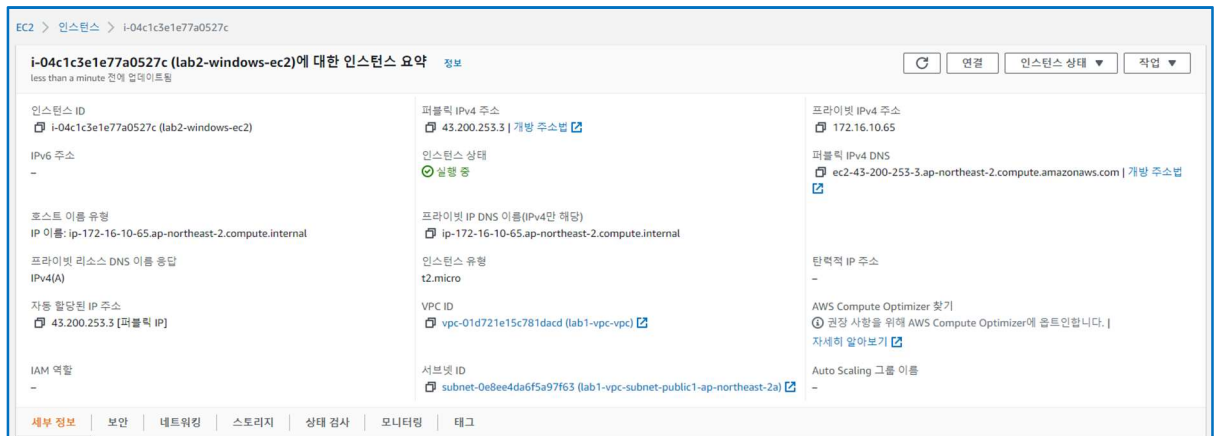
- O. 성공적으로 인스턴스가 생성되면 페이지 우측 하단의 **[View all instances]** 버튼을 클릭하거나, 인스턴스 링크를 클릭해서 인스턴스 목록 페이지로 이동한다.



- P. **[상태 검사]**의 값이 **"2/2개 검사 통과"**임을 확인한다.

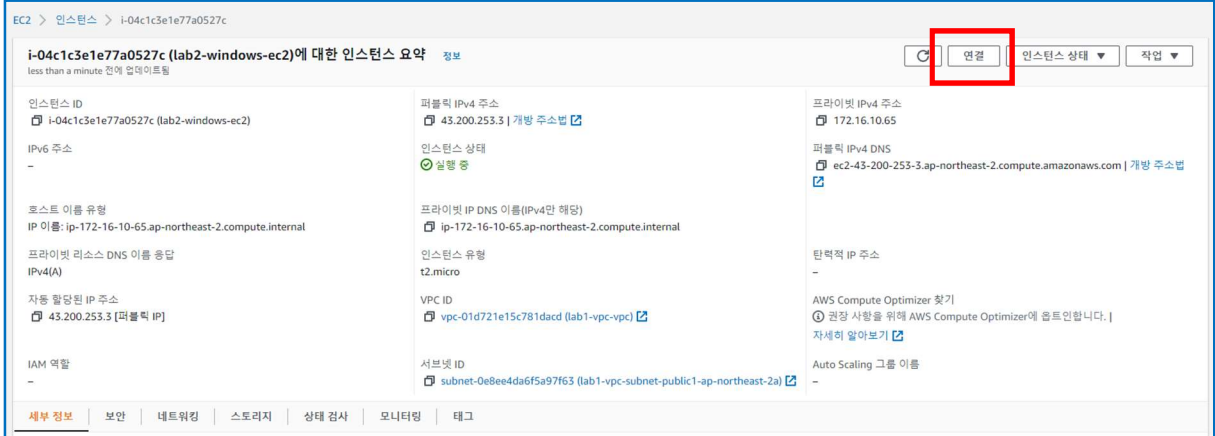


- Q. 인스턴스 생성이 모두 마친 후, 방금 생성한 인스턴스 ID를 클릭해서 세부 내용을 살펴본다.



Windows 인스턴스 접속하기

- A. 해당 [인스턴스 ID]를 클릭해 보자. 그리고 해당 [인스턴스 요약] 페이지가 나타나면 우측 상단의 [연결] 버튼을 클릭한다.



EC2 > 인스턴스 > i-04c1c3e1e77a0527c

i-04c1c3e1e77a0527c (lab2-windows-ec2)에 대한 인스턴스 요약 정보

less than a minute 전에 업데이트됨

인스턴스 ID
i-04c1c3e1e77a0527c (lab2-windows-ec2)

퍼블릭 IPv4 주소
43.200.253.3 | [개방 주소법](#)

인스턴스 상태
실행 중

퍼블릭 IPv4 DNS
ec2-43-200-253-3.ap-northeast-2.compute.amazonaws.com | [개방 주소법](#)

호스트 이름 유형
IP 이름: ip-172-16-10-65.ap-northeast-2.compute.internal

프라이빗 리소스 DNS 이름 응답
IPv4(A)

자동 할당된 IP 주소
43.200.253.3 [퍼블릭 IP]

IAM 역할
-

프라이빗 IP 주소
172.16.10.65

퍼블릭 IPv4 DNS
ec2-43-200-253-3.ap-northeast-2.compute.amazonaws.com | [개방 주소법](#)

탄력적 IP 주소
-

AWS Compute Optimizer 찾기
권장 사항을 위해 AWS Compute Optimizer에 출력합니다. | [자세히 알아보기](#)

Auto Scaling 그룹 이름
-

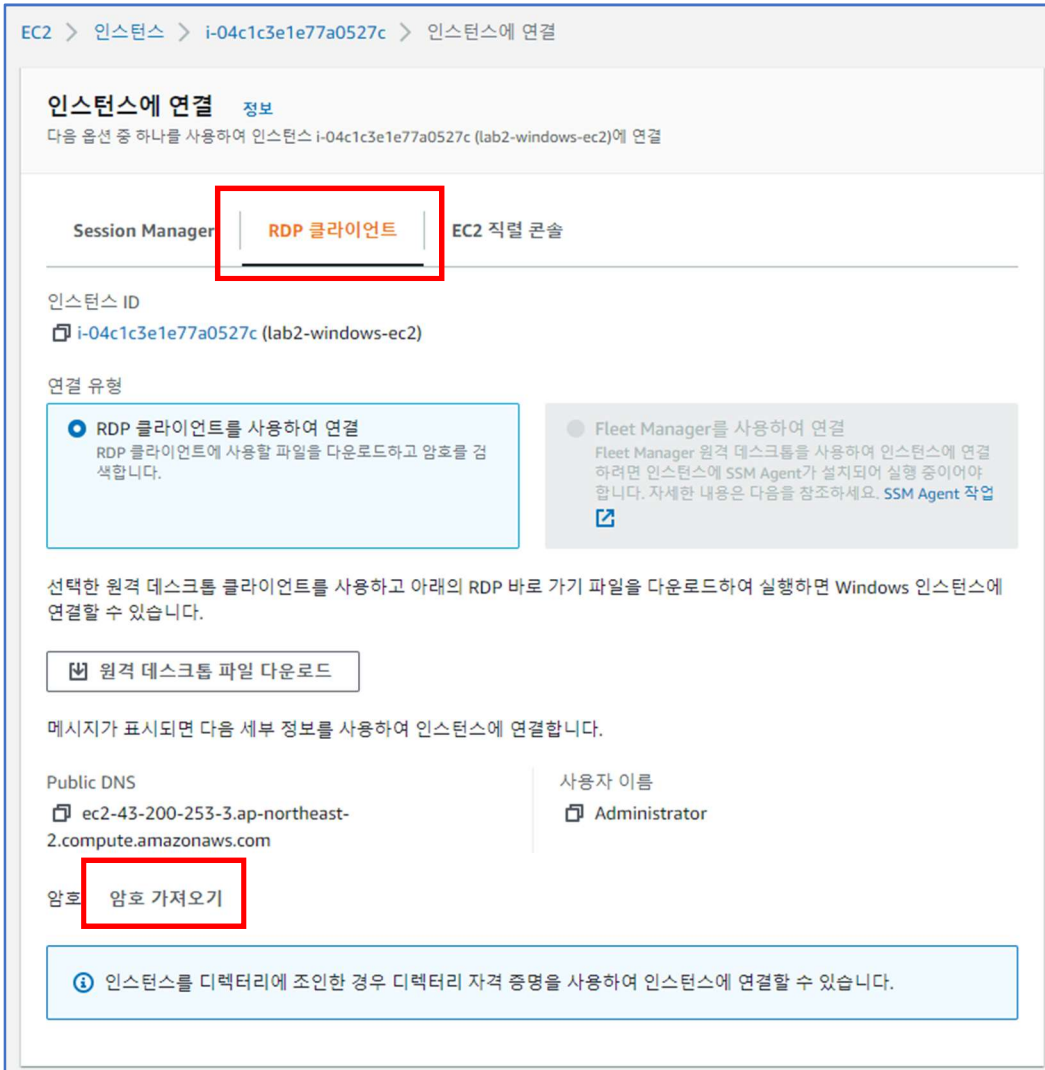
인스턴스 유형
t2.micro

VPC ID
vpc-01d721e15c781dacc (lab1-vpc-vpc)

서브넷 ID
subnet-0e8ee4da6f5a97f63 (lab1-vpc-subnet-public1-ap-northeast-2a)

세부 정보 | 보안 | 네트워킹 | 스토리지 | 상태 검사 | 모니터링 | 태그

- B. [RDP 클라이언트] 탭을 선택한다. 그리고 접속 암호 확인을 위해 [암호 가져오기] 링크를 클릭한다.



EC2 > 인스턴스 > i-04c1c3e1e77a0527c > 인스턴스에 연결

인스턴스에 연결 정보

다음 옵션 중 하나를 사용하여 인스턴스 i-04c1c3e1e77a0527c (lab2-windows-ec2)에 연결

Session Manager | **RDP 클라이언트** | EC2 직렬 콘솔

인스턴스 ID
i-04c1c3e1e77a0527c (lab2-windows-ec2)

연결 유형

- RDP 클라이언트를 사용하여 연결**
RDP 클라이언트에 사용할 파일을 다운로드하고 암호를 검색합니다.
- Fleet Manager를 사용하여 연결
Fleet Manager 원격 데스크톱을 사용하여 인스턴스에 연결하려면 인스턴스에 SSM Agent가 설치되어 실행 중이어야 합니다. 자세한 내용은 다음을 참조하세요. [SSM Agent 작업](#)

선택한 원격 데스크톱 클라이언트를 사용하고 아래의 RDP 바로 가기 파일을 다운로드하여 실행하면 Windows 인스턴스에 연결할 수 있습니다.

[원격 데스크톱 파일 다운로드](#)

메시지가 표시되면 다음 세부 정보를 사용하여 인스턴스에 연결합니다.

Public DNS
ec2-43-200-253-3.ap-northeast-2.compute.amazonaws.com

사용자 이름
Administrator

암호
[암호 가져오기](#)


인스턴스를 디렉터리에 조인한 경우 디렉터리 자격 증명을 사용하여 인스턴스에 연결할 수 있습니다.

C. [Windows 암호 가져오기] 페이지에서, [Browse] 버튼을 클릭한다.


Windows 암호 가져오기 정보

이 인스턴스에 대한 초기 Windows 관리자 암호를 검색하고 해독합니다.

암호를 해독하려면 이 인스턴스에 대한 키 페어가 필요합니다.

 이 인스턴스와 연결된 키 페어
lab2-windows-ec2-key

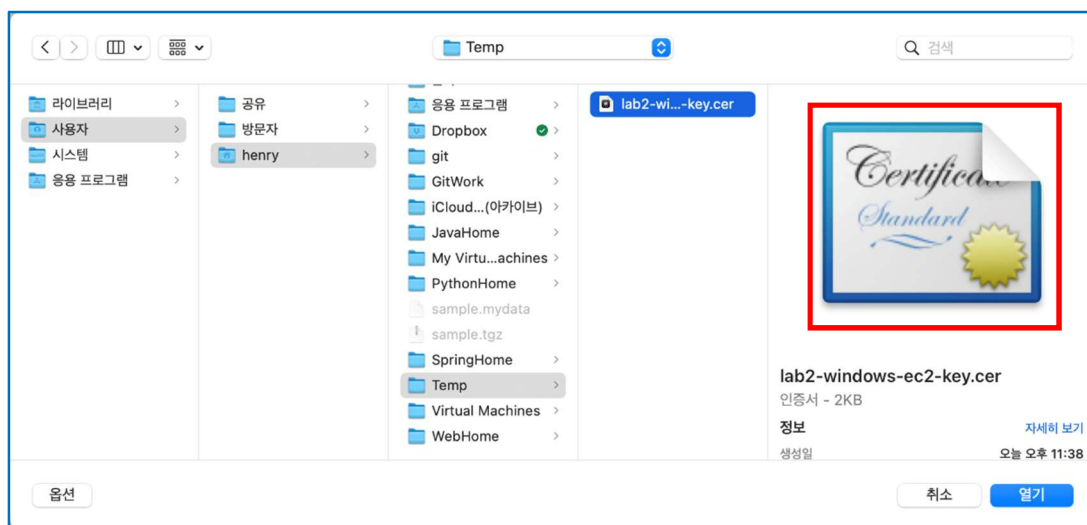
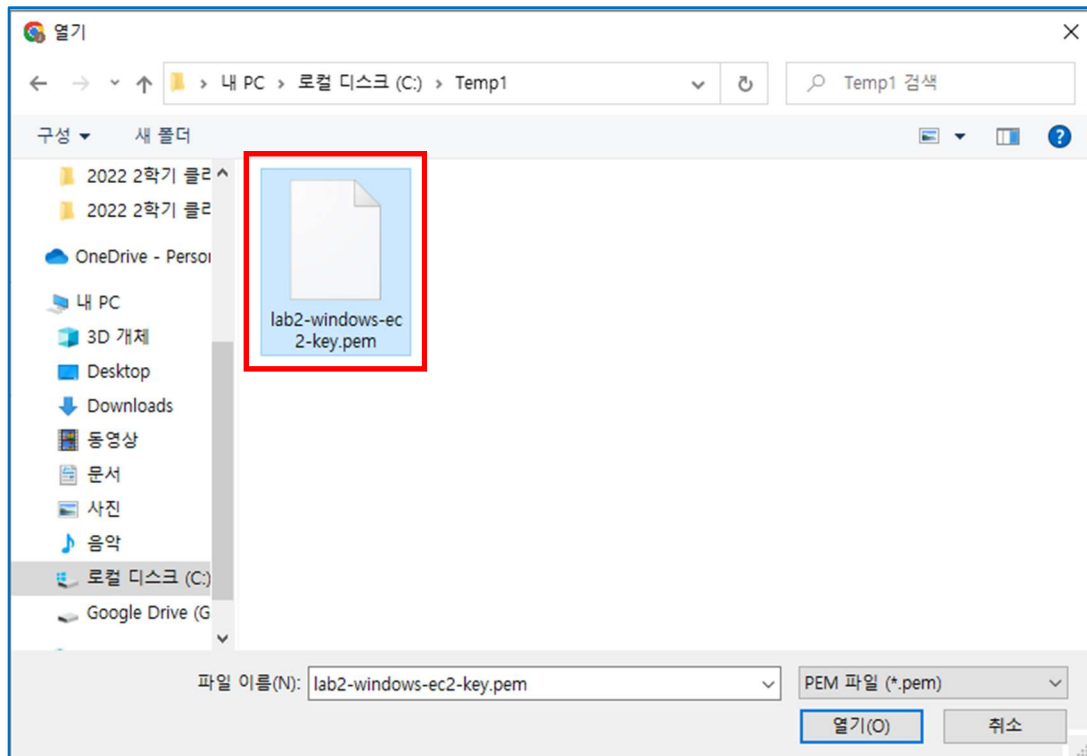
키 페어로 이동:

 Browse

또는 아래 키 페어 내용을 복사하여 붙여 넣습니다.

[취소](#) [암호 해독](#)

- D. 로컬 PC에 저장된 "키 페이 파일(PEM)"(lab2-windows-ec2-key.pem)을 선택 후 [열기] 버튼 (Windows) 또는 [열기](macOS)을 클릭한다.



- E. 자동으로 해당 키 페어가 복사되어 들어온다. [암호 해독] 오렌지색 버튼을 클릭한다.

Windows 암호 가져오기 정보

이 인스턴스에 대한 초기 Windows 관리자 암호를 검색하고 해독합니다.

암호를 해독하려면 이 인스턴스에 대한 키 페어가 필요합니다.

 이 인스턴스와 연결된 키 페어
lab2-windows-ec2-key

키 페어로 이동:

 Browse

 lab2-windows-ec2-key.pem
1.678KB

또는 아래 키 페어 내용을 복사하여 붙여 넣습니다.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAA1OyeY6hipVzmhmQme19w2WM0YtcvRV9l3k9K5pNzofw5BzIN
Z2rV1TSXidJE2kzPGcqrK6LurwiPdUZNFFWZpOuVju8mlR9zDvwMLU/q/nlh7+v/
G8CTWP/0Fv6slv3T2xB7FyffWlVl2T4skXZ+eIPYayD5QtGnOWu9kkgIfmCw2w5
+y8C+ViG6LdOZhajdk83+B/RzwGcfRYuQnApOn3jUr5B+gWv7JVrgCfudCguBcE2
kHSybSWyto/Y+2SHeGsfLd9RGiG9+WWtKNwWaU+SmuGV/LyvUBW1GrF8zHVY13od
zvkdIRO/r75BifVJgsmEhHo1mDfiaearCCjS0wIDAQABAolBAQCeh+pJ8wY3btro
dsq8Esx33sgTS3oTobq78benw2NV2PAw7lBSjpXVH0owwFCpZITSBDa7z5z8z1fY
```

취소

암호 해독

- F. 암호 해독에 성공했다. 암호 해독의 결과는 아래 그림과 같이 해독한 암호가 보인다.

인스턴스에 연결 정보

다음 옵션 중 하나를 사용하여 인스턴스 i-04c1c3e1e77a0527c (lab2-windows-ec2)에 연결

Session Manager


RDP 클라이언트

EC2 직렬 콘솔

인스턴스 ID
 i-04c1c3e1e77a0527c (lab2-windows-ec2)

연결 유형

 RDP 클라이언트를 사용하여 연결
RDP 클라이언트에 사용할 파일을 다운로드하고 암호를 검색합니다.


 Fleet Manager를 사용하여 연결
Fleet Manager 원격 데스크톱을 사용하여 인스턴스에 연결하려면 인스턴스에 SSM Agent가 설치되어 실행 중이어야 합니다. 자세한 내용은 다음을 참조하세요. [SSM Agent 작업](#)

선택한 원격 데스크톱 클라이언트를 사용하고 아래의 RDP 바로 가기 파일을 다운로드하여 실행하면 Windows 인스턴스에 연결할 수 있습니다.

 원격 데스크톱 파일 다운로드

메시지가 표시되면 다음 세부 정보를 사용하여 인스턴스에 연결합니다.

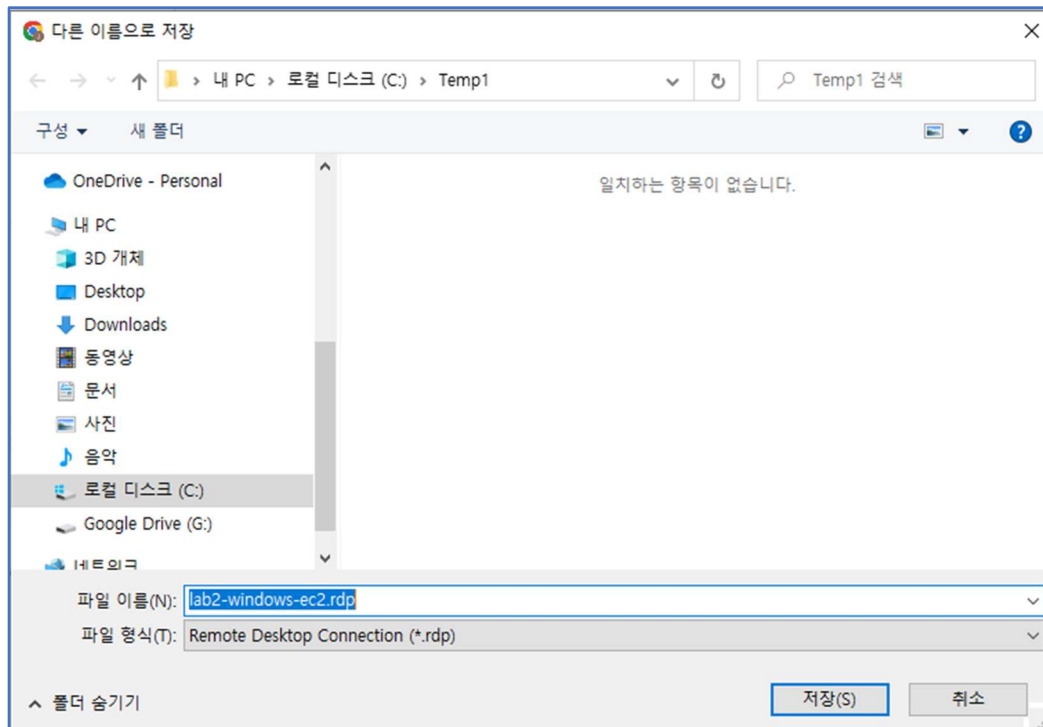
Public DNS
 ec2-43-200-253-3.ap-northeast-2.compute.amazonaws.com

사용자 이름
 Administrator

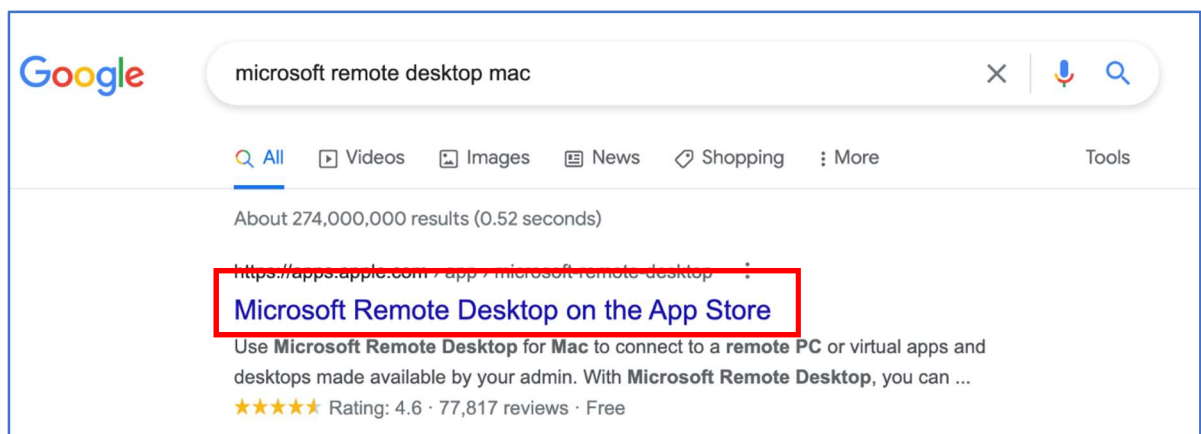
암호
 Mji.5=BJFF)lH\$(PtE3wSvWU.BOGrr)

 인스턴스를 디렉터리에 조인한 경우 디렉터리 자격 증명을 사용하여 인스턴스에 연결할 수 있습니다.

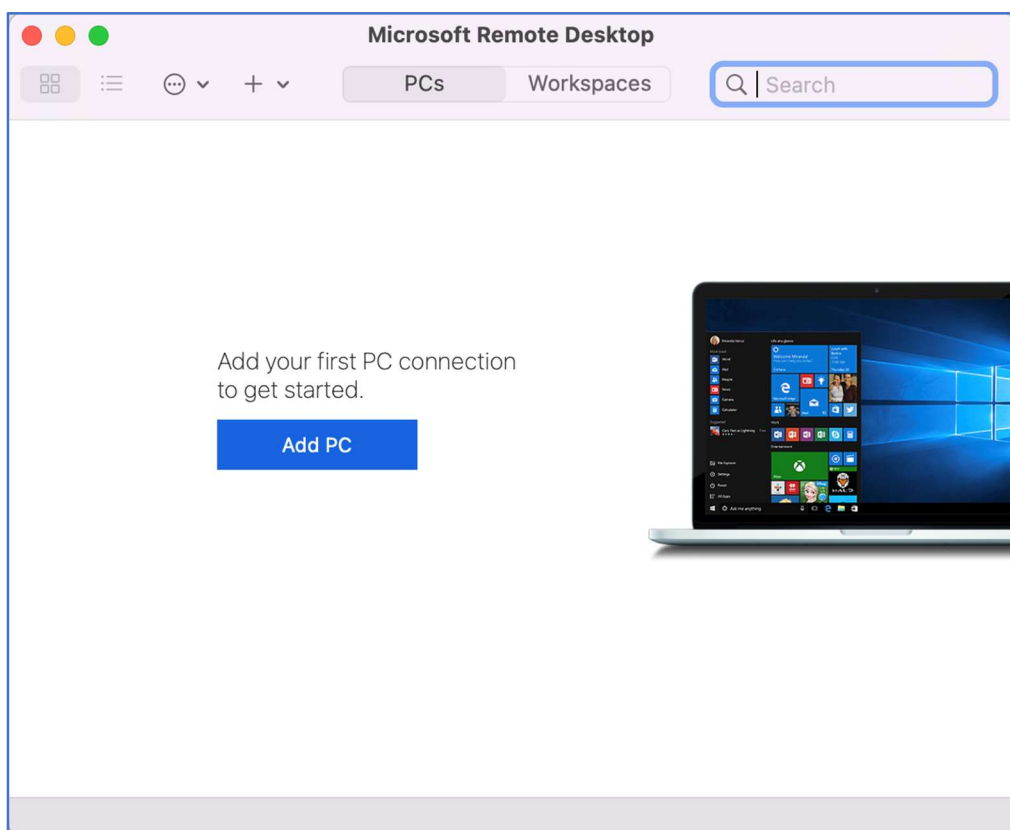
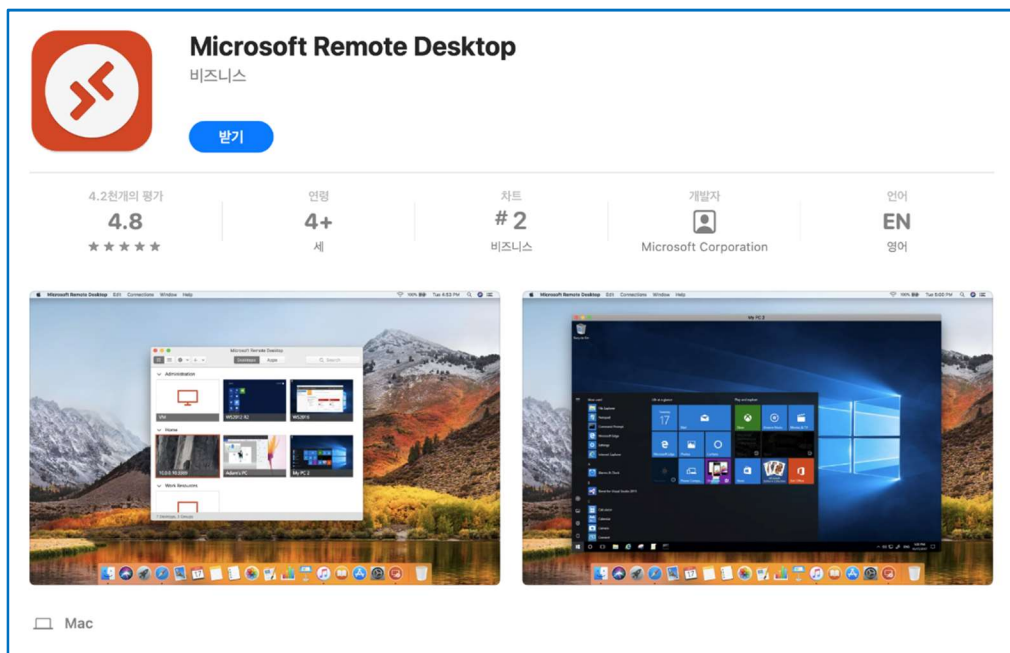
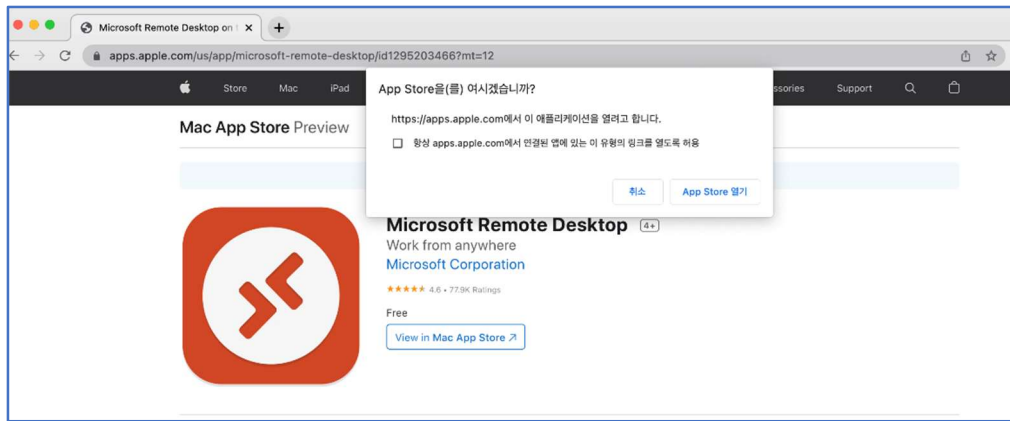
- G. 이제 해독된 암호를 사용해서 [원격 데스크톱 파일 다운로드] 버튼을 클릭하여 접속 프로그램을 다운로드 받는다.



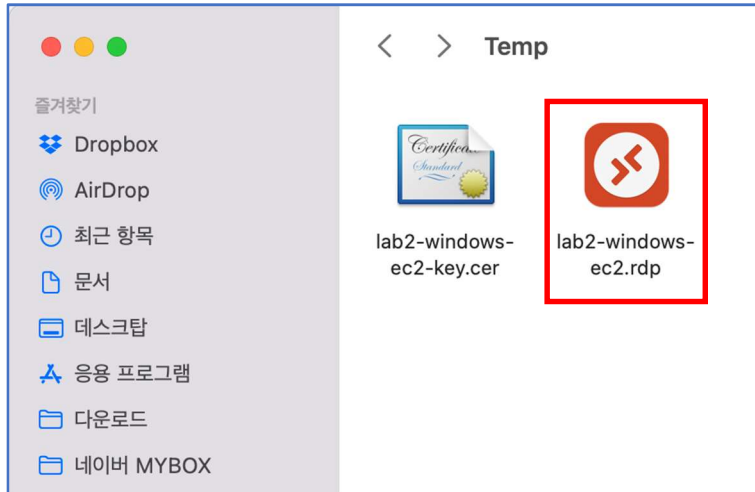
- H. 만일 AWS의 EC2를 접근하려는 노트북 또는 데스크탑의 OS가 macOS라면 “Microsoft Remote Desktop”을 설치하기 위해 검색엔진에서 다음과 같이 “microsoft remote desktop mac”으로 검색한다. 만일 Windows를 OS로 사용하면 아래 페이지의 M번으로 이동한다.



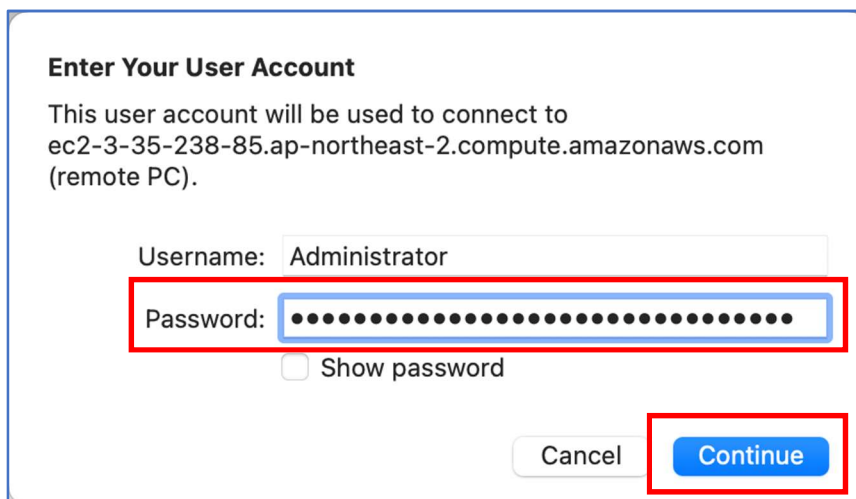
- I. 앱 스토어에서 제공하는 앱을 선택해서 설치한다.



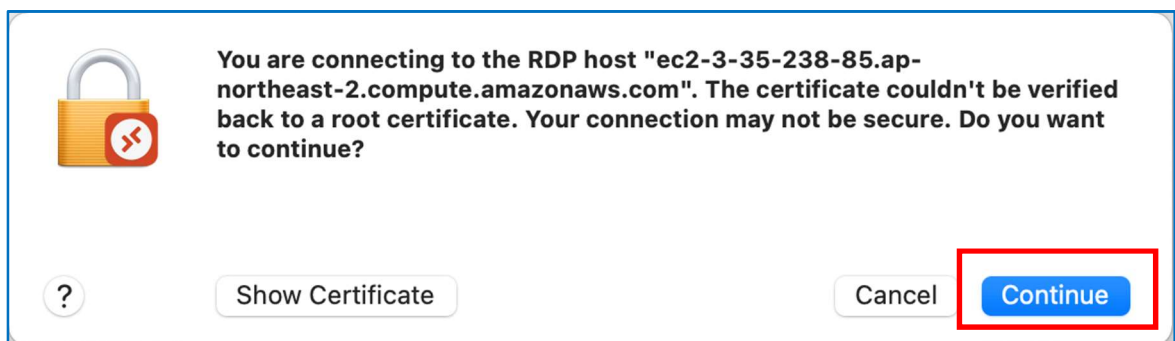
- J. 다운로드 받은 **lab2-windows-ec2.rdp** 파일을 더블 클릭하여 **Microsoft Remote Desktop** 프로그램을 실행한다.



- K. **[Enter Your User Account]** 창에서, **[Username]**은 "Administrator"로 자동으로 입력되어 있고, **[Password]**는 암호해독된 패스워드를 복사하여 붙여 넣는다. 그리고 **[Continue]**를 클릭한다.



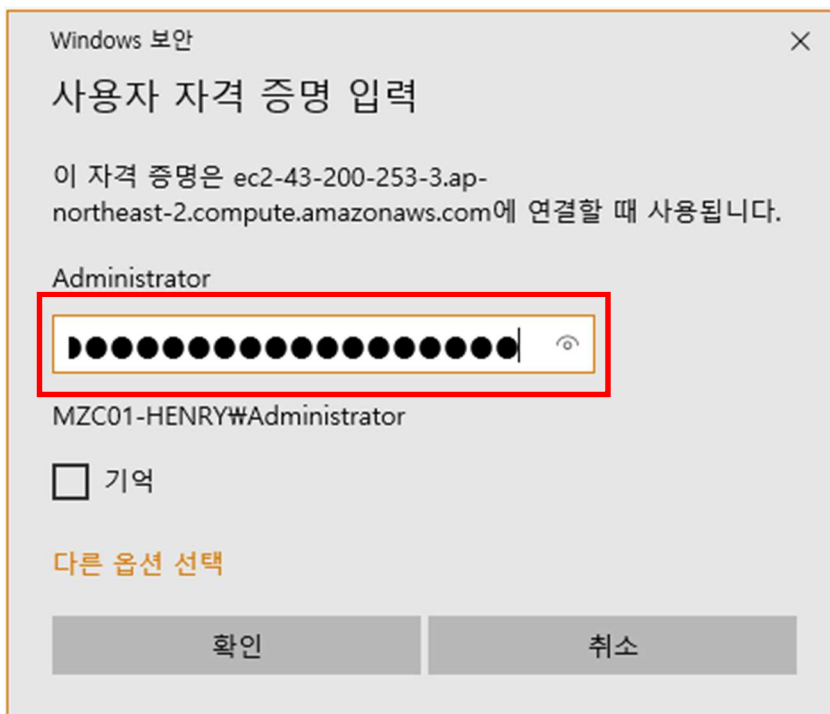
- L. 그 다음에 나오는 확인 창에서도 **[Continue]**를 클릭한다.



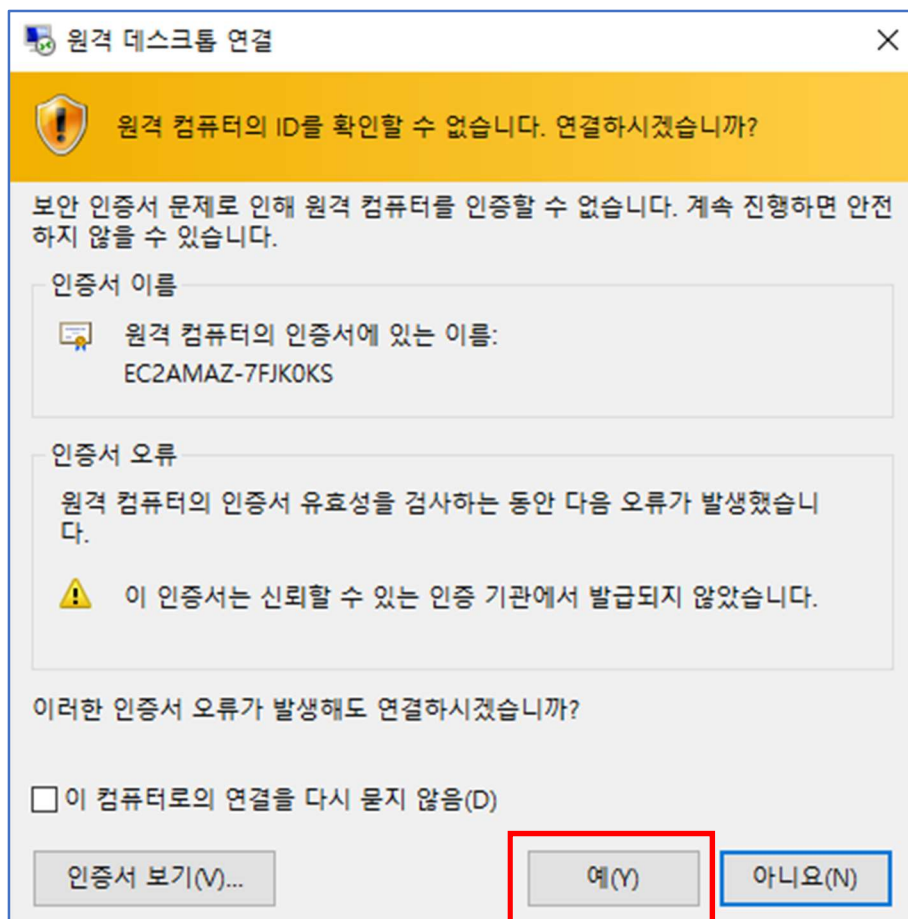
- M. Windows 운영체제는 별다른 프로그램 설치없이 바로 **[원격 데스크톱 연결]**창이 나타난다. **[연결]** 버튼을 클릭한다.



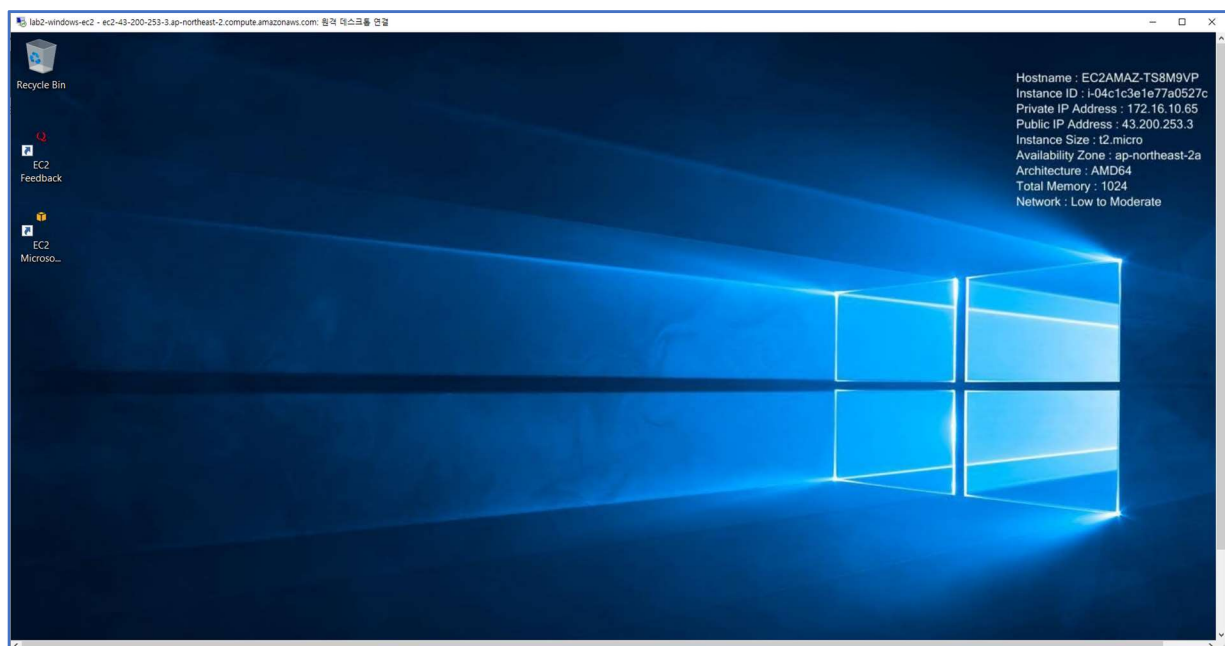
- N. 아이디는 **[Administrator]**이고 암호는 위의 F번의 그림에 있는 해독된 암호를 복사하여 붙여넣기 후 **[확인]** 버튼을 클릭하여 로그인한다.



- O. "이러한 인증서 오류가 발생해도 연결하시겠습니까?" 에서 [예]를 클릭한다.

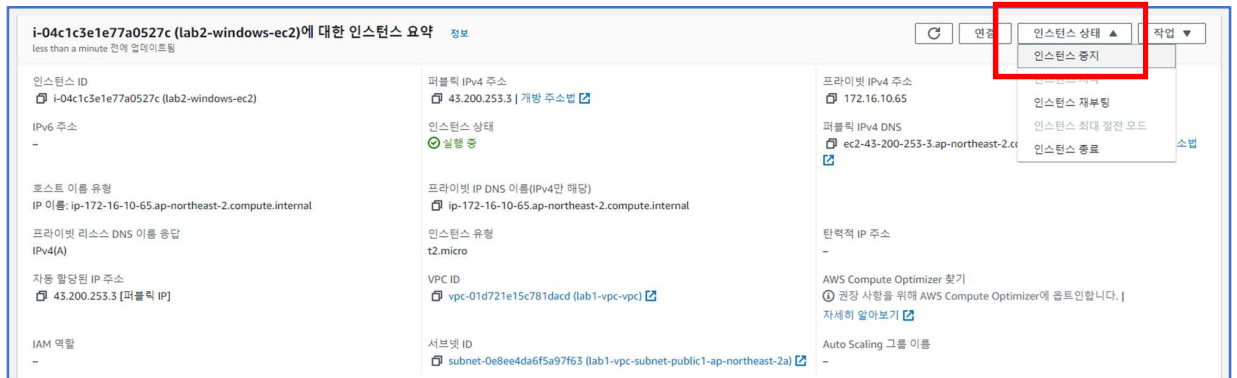


- P. 드디어 AWS EC2 가상머신에 로그인 성공했다.

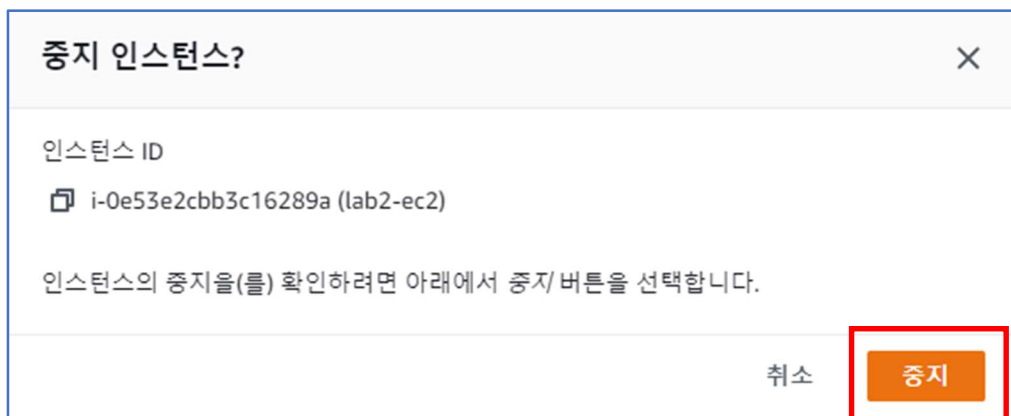


Windows 서버 시작, 중지하기

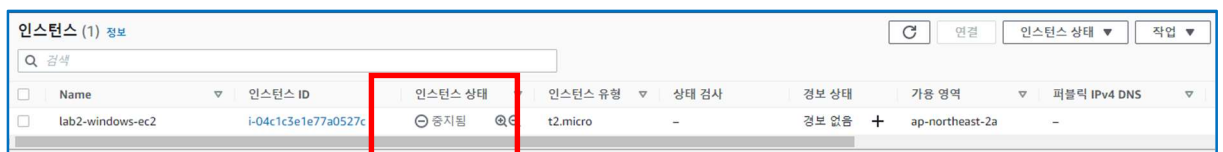
- A. 방금 생성한 Windows Server 인스턴스를 중지시키기 위해서는 서버에 원격으로 접속한 다음, 서버에서 **[Shut down]**를 수행하거나, **[인스턴스 요약]** 페이지에서 해당 인스턴스를 선택 후 **[인스턴스 중지]**를 선택하여 인스턴스를 중지할 수 있다.



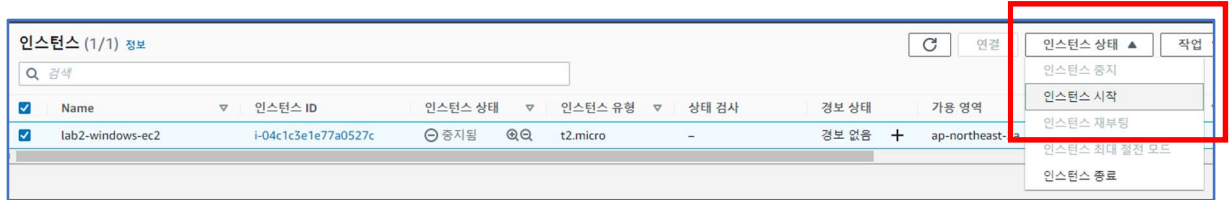
- B. **[중지]** 버튼을 클릭한다.



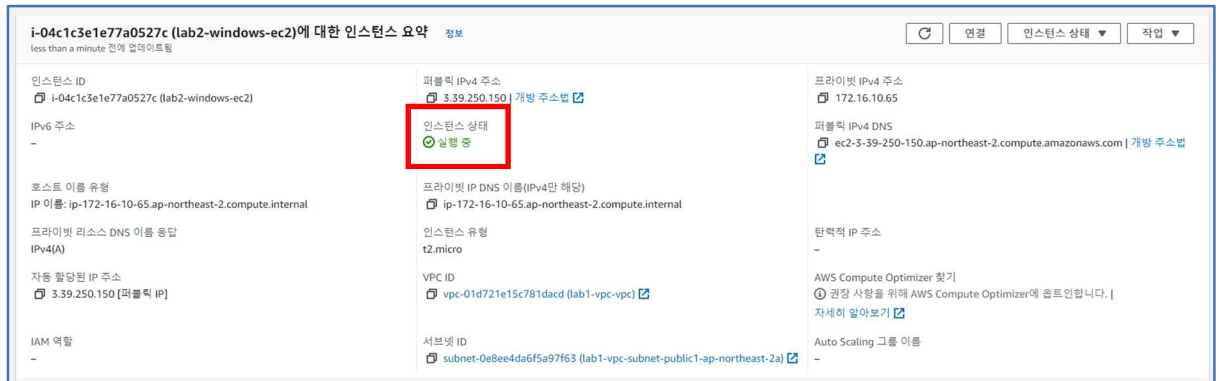
- C. 잠시 후 **[인스턴스]** 페이지에서 해당 Windows Server 인스턴스가 "중지됨"을 확인할 수 있다.



D. 다시 해당 인스턴스를 시작하려면 [인스턴스 요약]페이지에서 [인스턴스 시작]을 선택하면 된다.

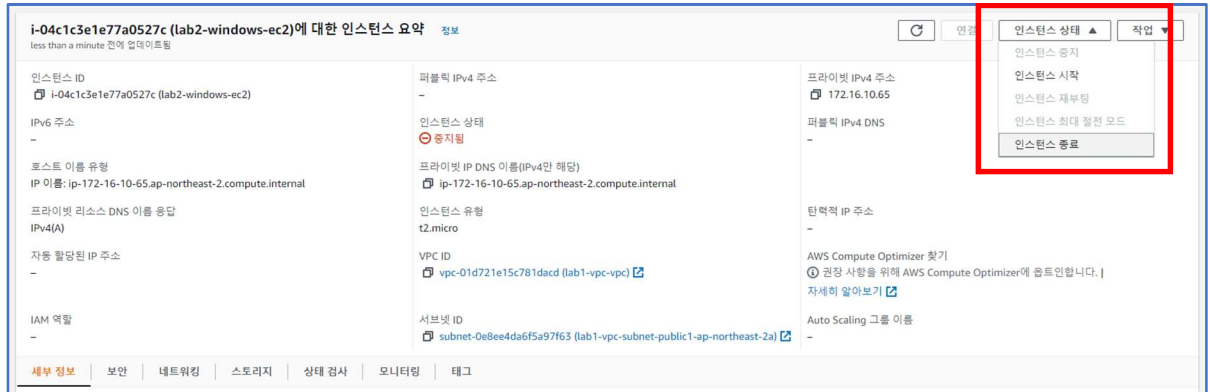


E. 다시 연결하려면 해당 인스턴스의 [인스턴스 요약] 페이지에서 [인스턴스 유형]이 "실행 중"임을 확인한 후, 위의 연결 과정을 다시 실행하면 된다.

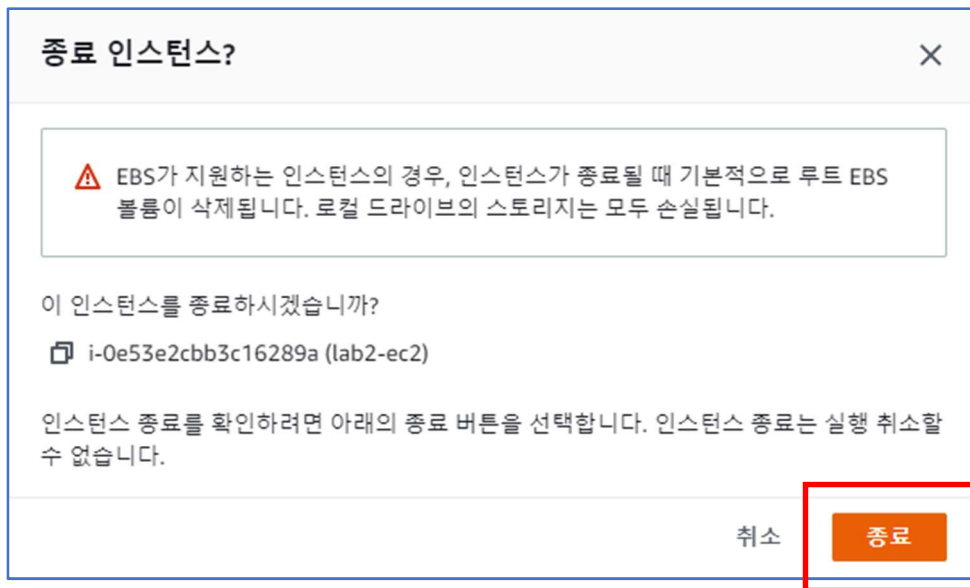


Windows Server 인스턴스 영구 삭제하기

- A. 해당 인스턴스의 [인스턴스 요약] 페이지에서 [인스턴스 유형]이 “중지됨”을 확인 한 다음, [인스턴스 상태]에서 [인스턴스 종료]를 선택한다.



- B. [인스턴스 종료]를 선택하면 아래의 그림과 같이 [종료 인스턴스]창이 나타나고 여기서 [종료]를 클릭한다.



- C. 잠시 뒤, [인스턴스] 페이지에서 확인해 보면 해당 인스턴스가 “종료됨” 상태임을 알 수 있다.

