

231208 (AWS 클라우드)

자바스프링

2023/12/08 18:19

<http://blog.naver.com/sophia2164/223286947500>

AWS

Virtual Box는 윈도우 OS 위에서 돌아간다

JVM Java Virtual Box는 자바가 개발한 Virtual machine

노드 넥스트 뷰 리액트

자바스크립트가 훌륭한 언어는 아니다

컴파일언어 c w자바

OSI 7계층

데이터 전송위한 통로: 인터페이스 넘버, 포트 번호(지정해야 통신가능)

포트번호 : 개발자는

ip addresses. TCP - 네트워크관리자가 보는 것. 물리적인

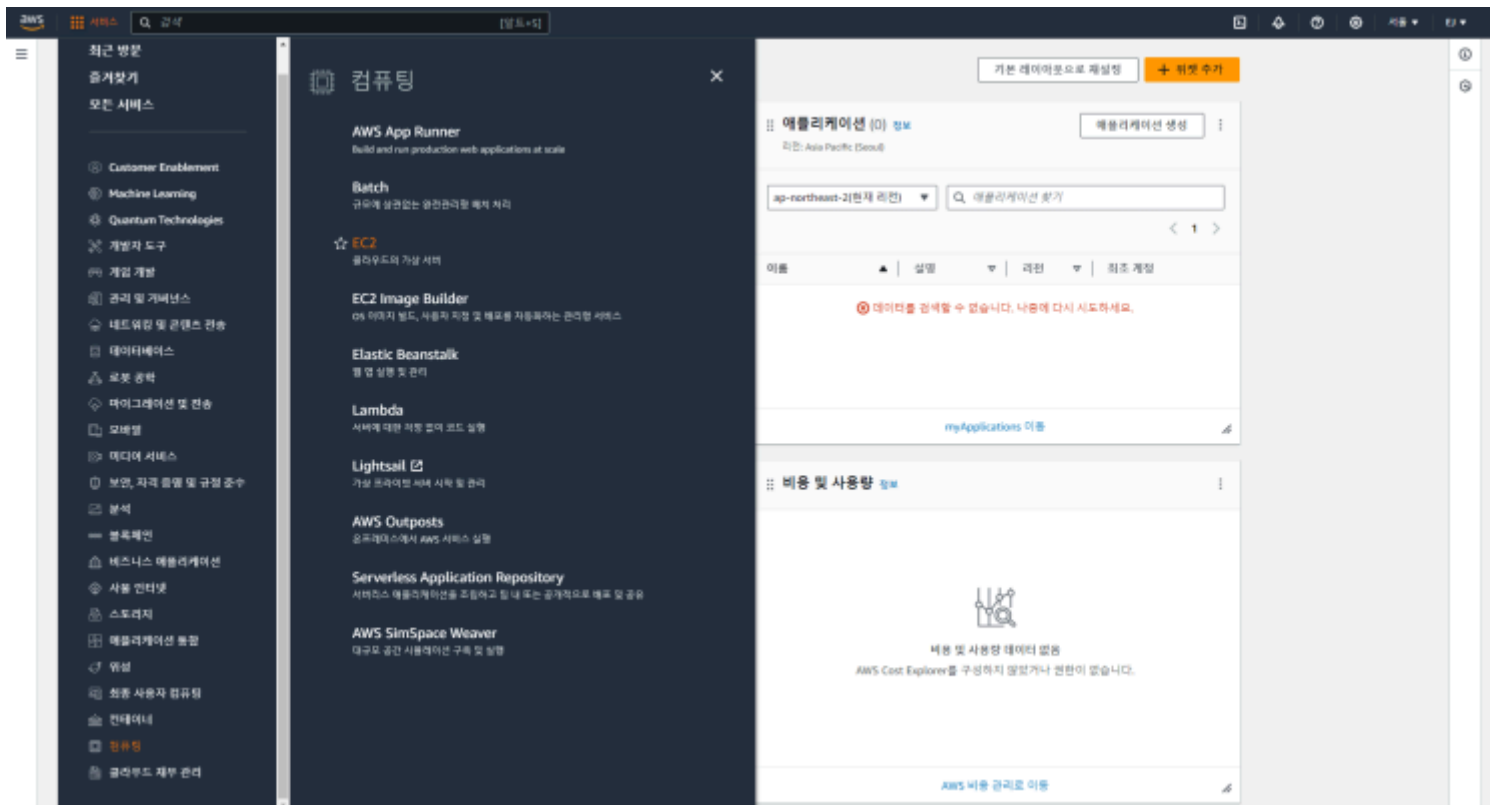
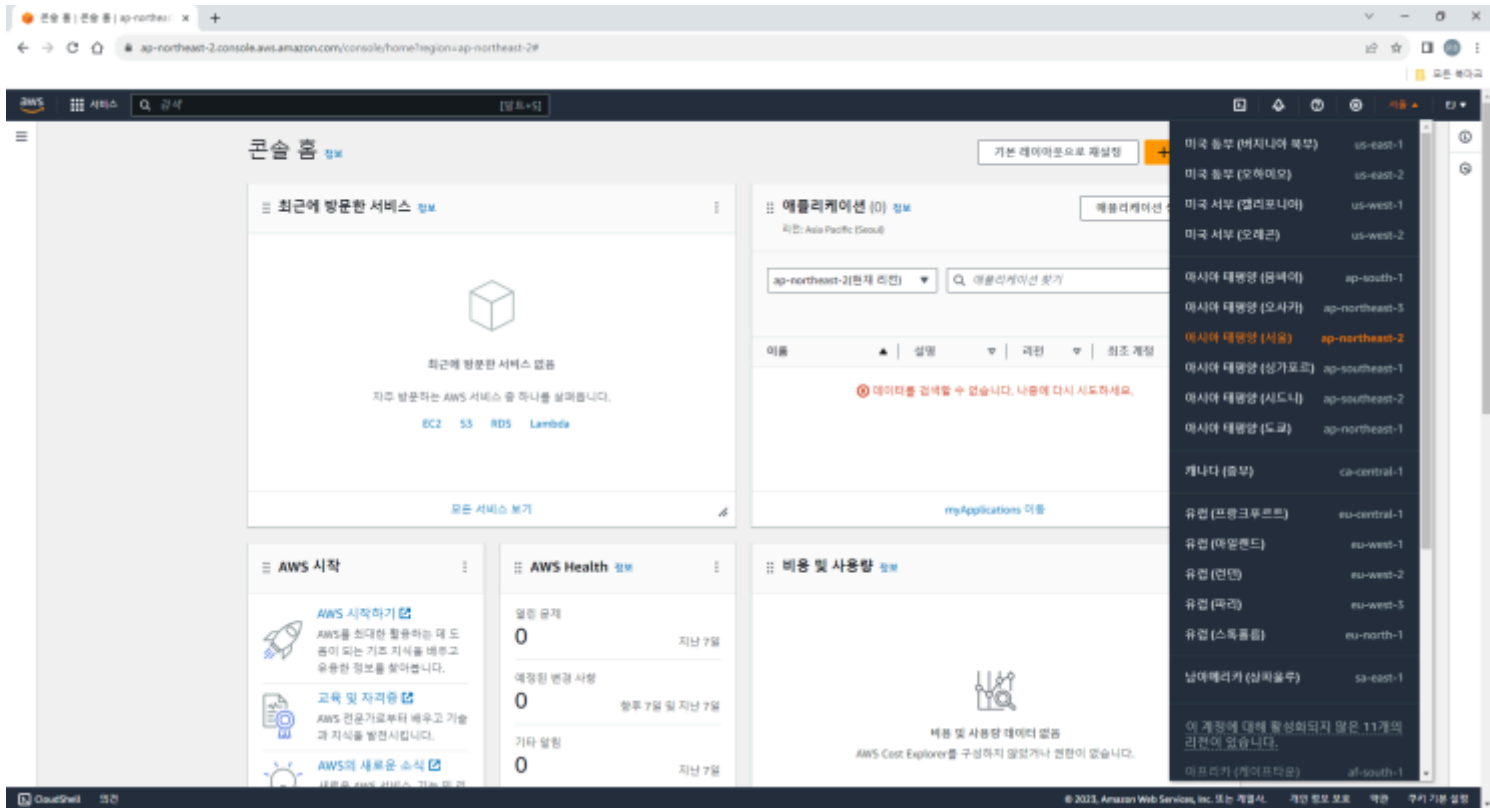
Nic 값: 인터페이스번호

리눅스가 파이썬사용하기 좋음

C언어의 기반의 "유닉스"가 어려워서 간결하게 만든 것이 "리눅스"

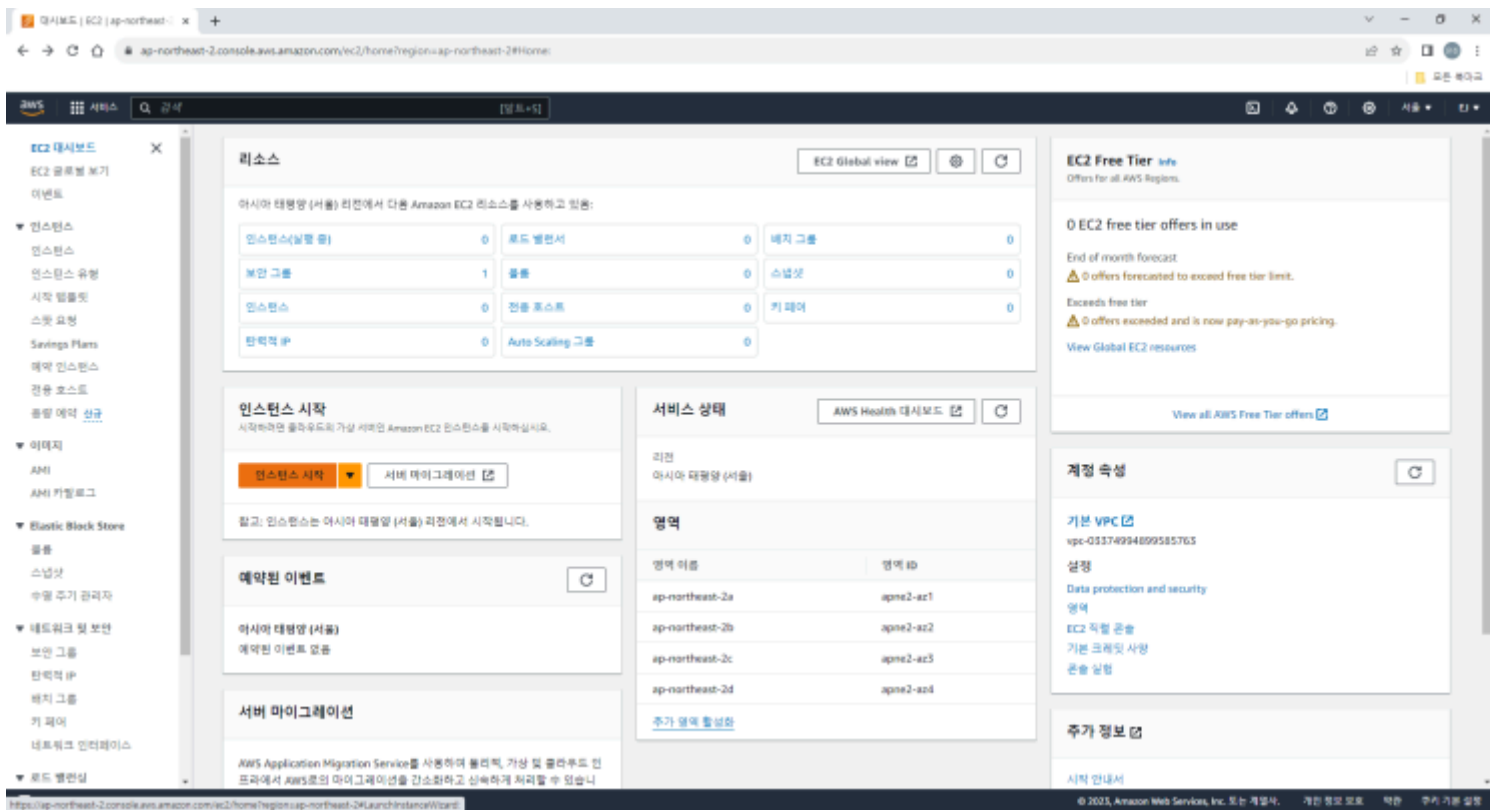
1. AWS 계정 생성
2. 인스턴스 (내가 만들고 싶은 가상서버) 생성 // 이외에 여러가지들이 있다
3. 외부에서 접속해야 할때는 탄력적 아이피를 줘야 한다.
4. (외부에서 오는 허가된 접속인지 확인하는 보안 키인 pem(리눅스용)를 키페어때 생성(인증서 비슷) -> 텔레프로그램 PuTTY에 쓰기 위해서는 ppk로 바꾼다.
(PuTTY에서 pem 로드해두고 private key save 눌러서 설정)
- 푸티는 ppk가 필요하기 때문에 putty gen에서 pem을 ppk로 변환해줘야 한다.
5. [보안그룹] - [인바운드 규칙]에서 포트번호 22번으로 SSH 개방해두는 것이 필수

AWS 가입



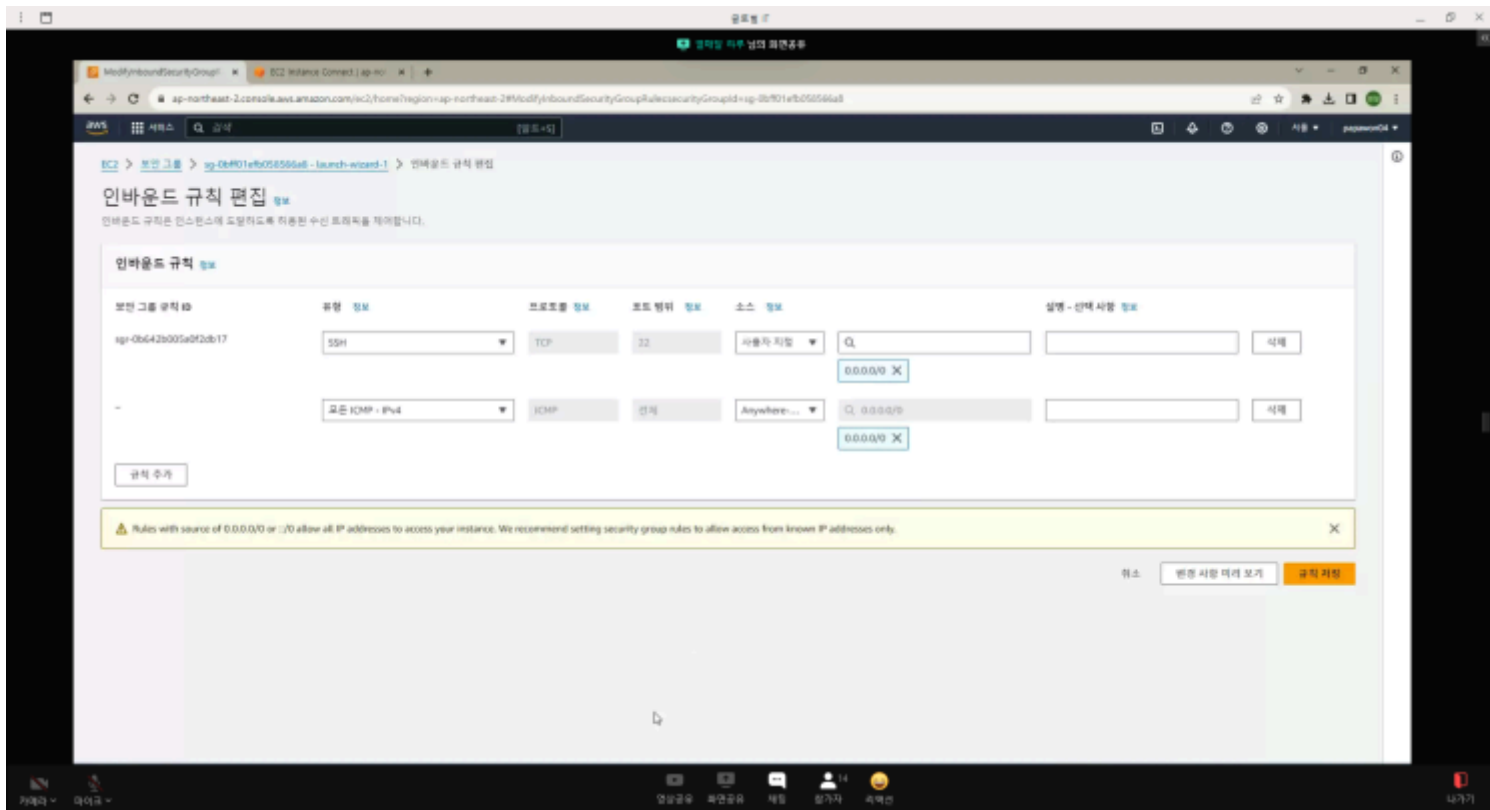
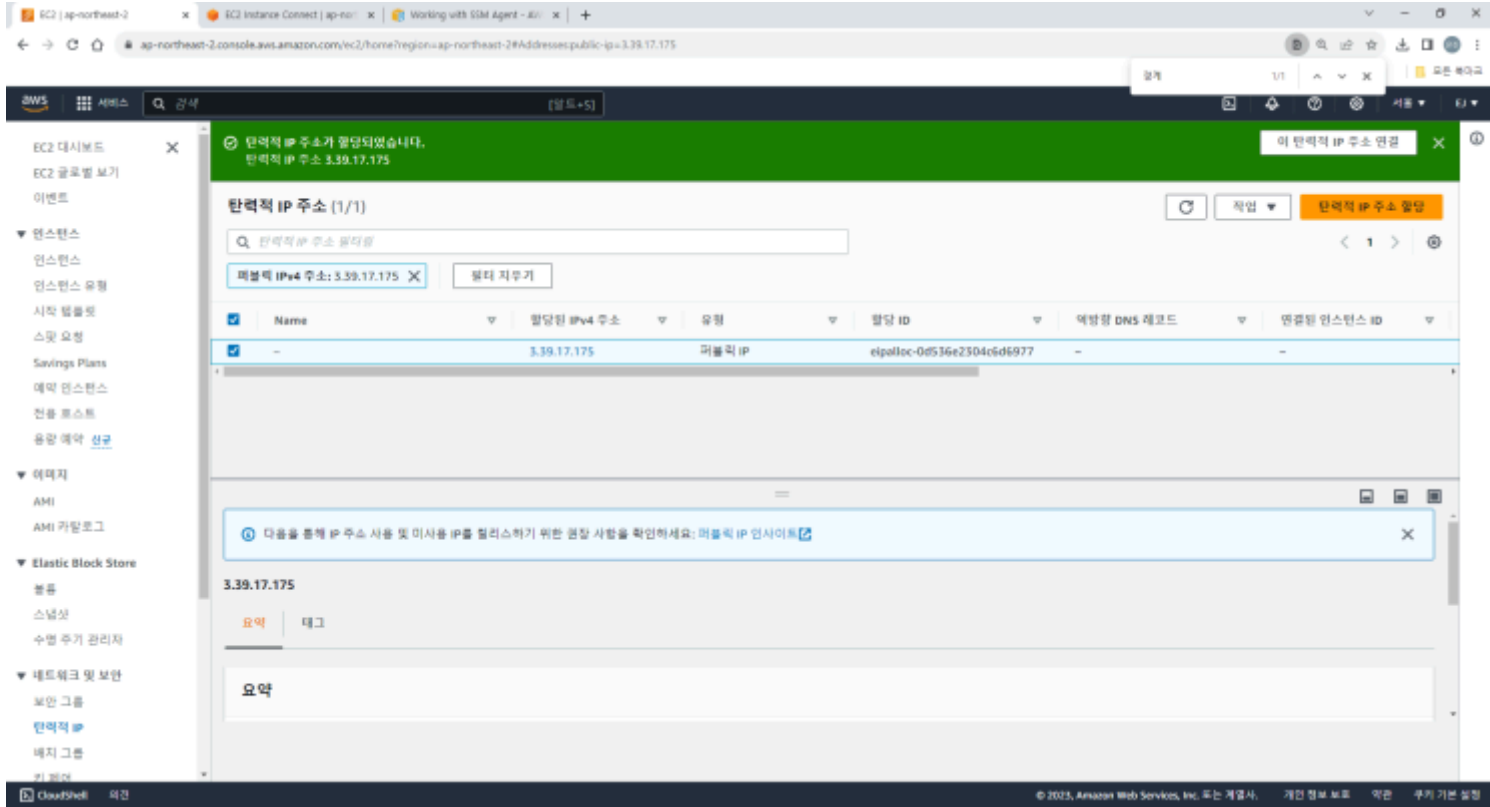
인스턴스 : 내가 작업할 공간

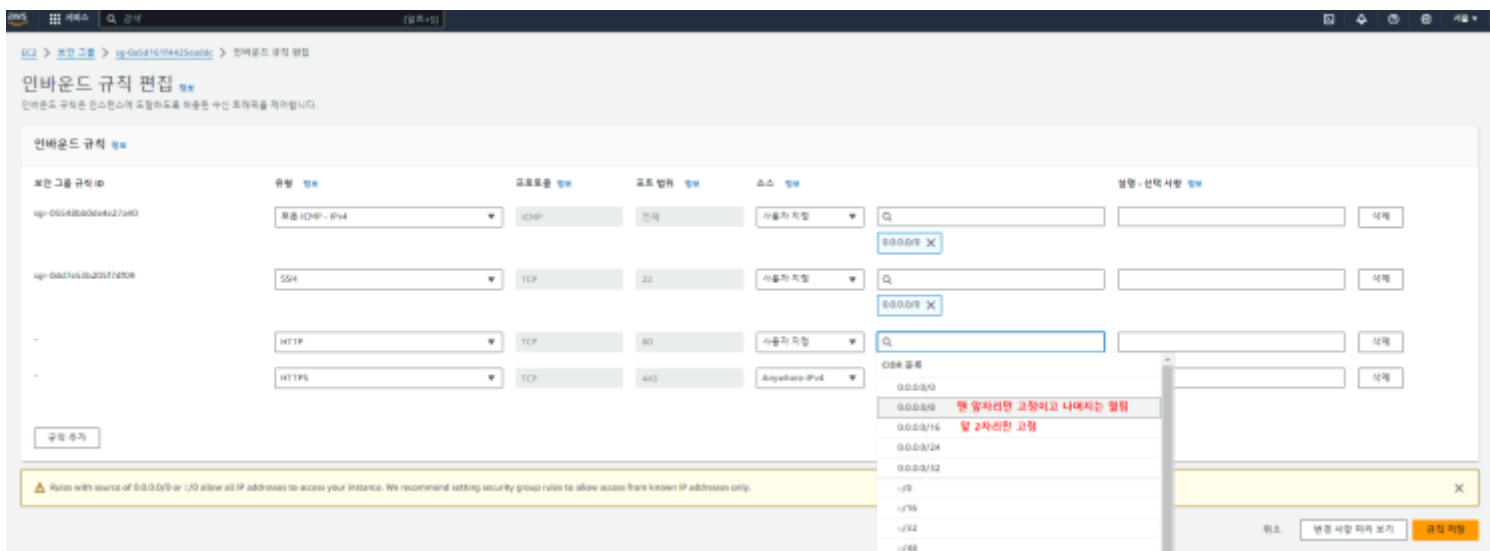
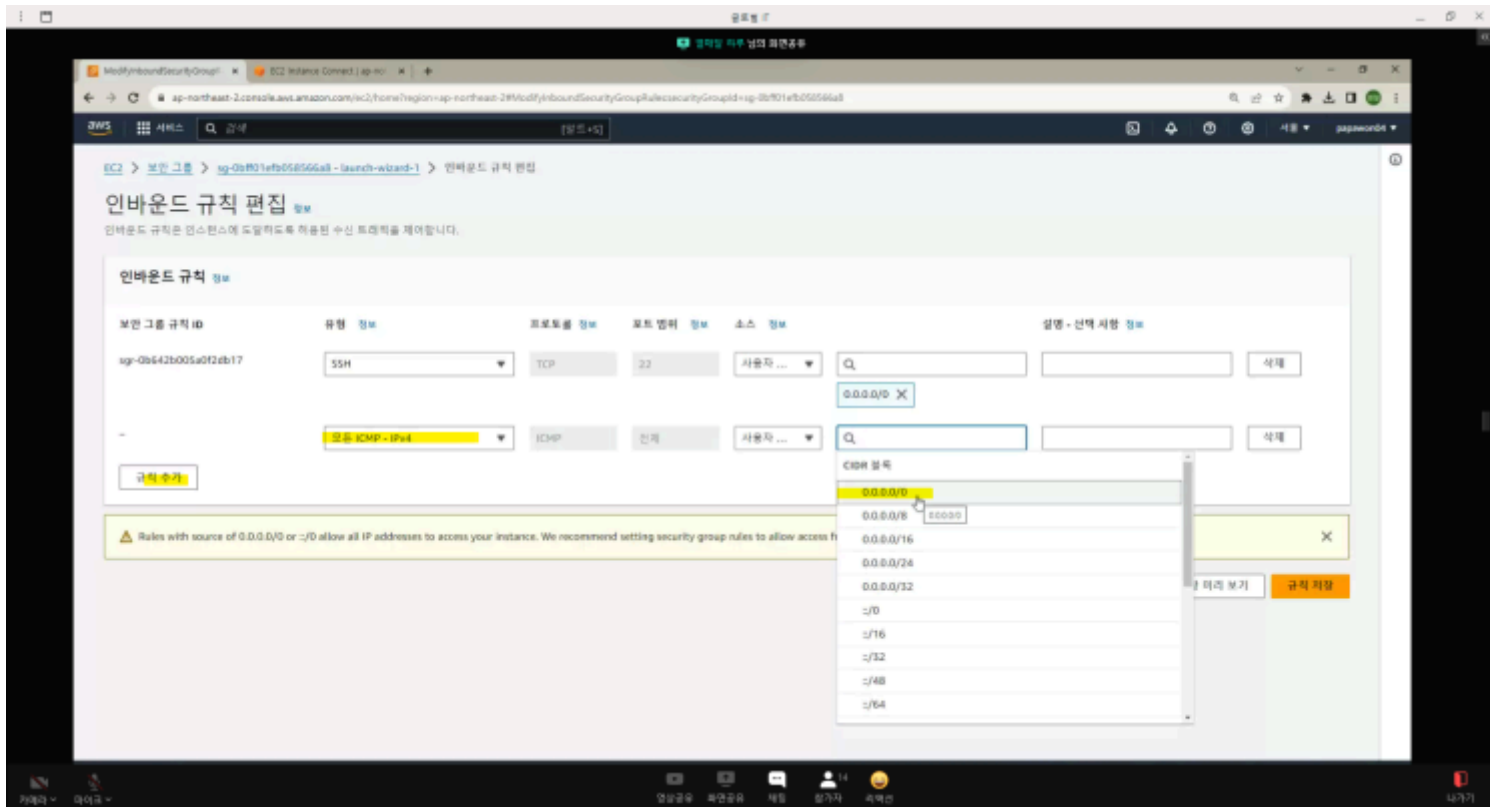
EC2 대시보드- 인스턴스 시작



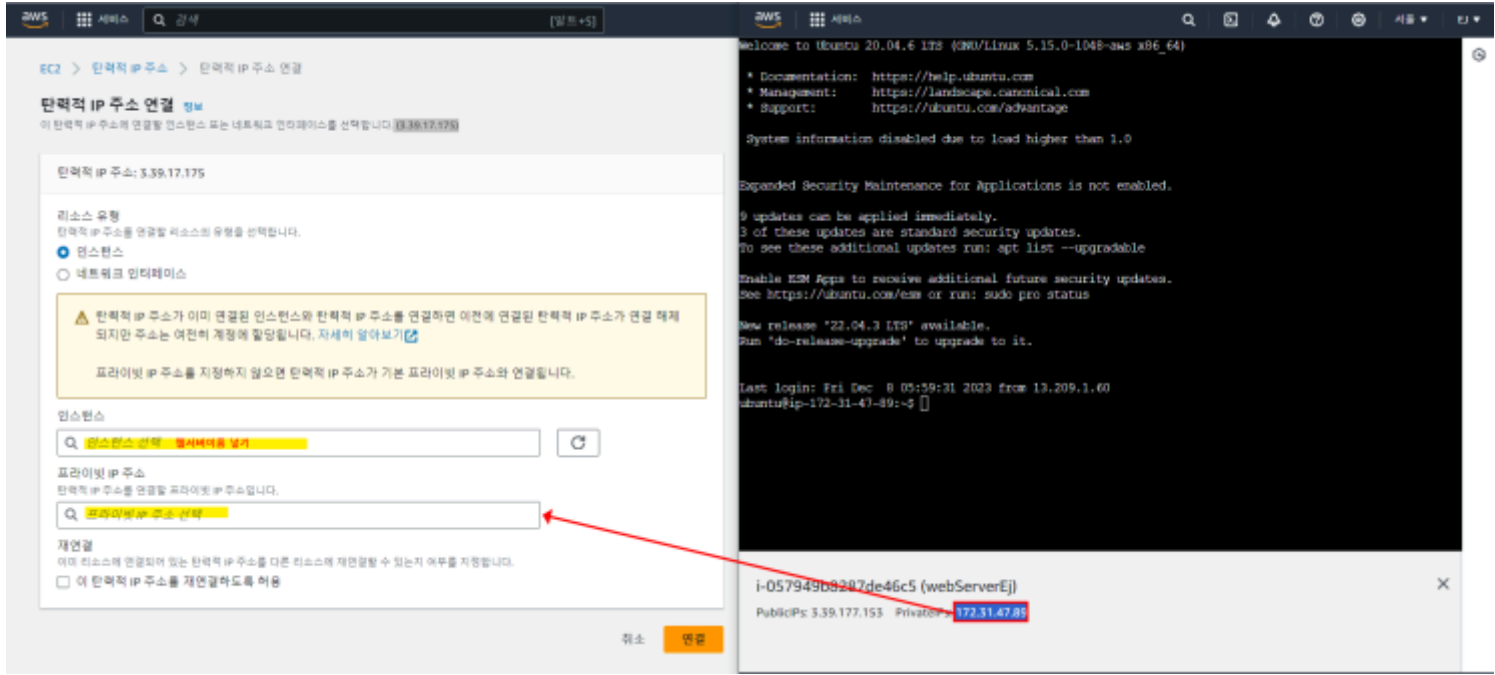
AWS(Amazon Web Services)에서 키페어(key pair)는 EC2 인스턴스에 대한 보안 액세스를 제어하는 데 사용되는 인증 정보입니다. 키페어는 EC2 인스턴스에 연결하고 인스턴스를 안전하게 관리하기 위해 사용됩니다. 키페어는 공개 키와 개인 키로 이루어져 있습니다.

탄력적ip 할당





1.



```
aws | 서비스 | Q 검색 [알트+S]
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1048-aws x86_64)

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

System information as of Fri Dec  8 06:50:02 UTC 2023

System load:  0.0              Processes:            97
Usage of /:   6.3% of 28.89GB   Users logged in:     0
Memory usage: 18%              IPv4 address for eth0: 172.31.47.89
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

9 updates can be applied immediately.
3 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec  8 06:17:51 2023 from 13.209.1.59
ubuntu@ip-172-31-47-89:~$
```

i-057949b8287de46c5 (webServerEj)
탄력적 IP주소 = 퍼블릭IP주소가 동일해졌다
PublicIPs: 3.39.17.175 PrivateIPs: 172.31.47.89

할당 완료

PuTTY, PuTTYgen 실행

PuTTY gen 실행

PutTY Key Generator ? X

File Key Conversions Help

Key
No key.

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:
☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:

PutTY Key Generator ? X

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDV5ALo3t+sObthb3CE9UDh
+RNxYOZx1KzFWlmmynu6Q/nmfgywskNRdj9pu8/c5HYIDJ
+M9H1lauVHbW3L2Wlls0T7oaeNQMtAm3wMynbF1LFokQ1pTi2l4GqxUx4XQRmZBry
+KAzlkJ5RMW/CjKHO73i7KCNKzPA8ahbSrlmnZJhlAa6vHXTB4tgE4JArYx6qI6DWX95aM5Vfo3/Tji7qGt7LRpH
pcTguvJg2ln
```

Key fingerprint:

Key comment:

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

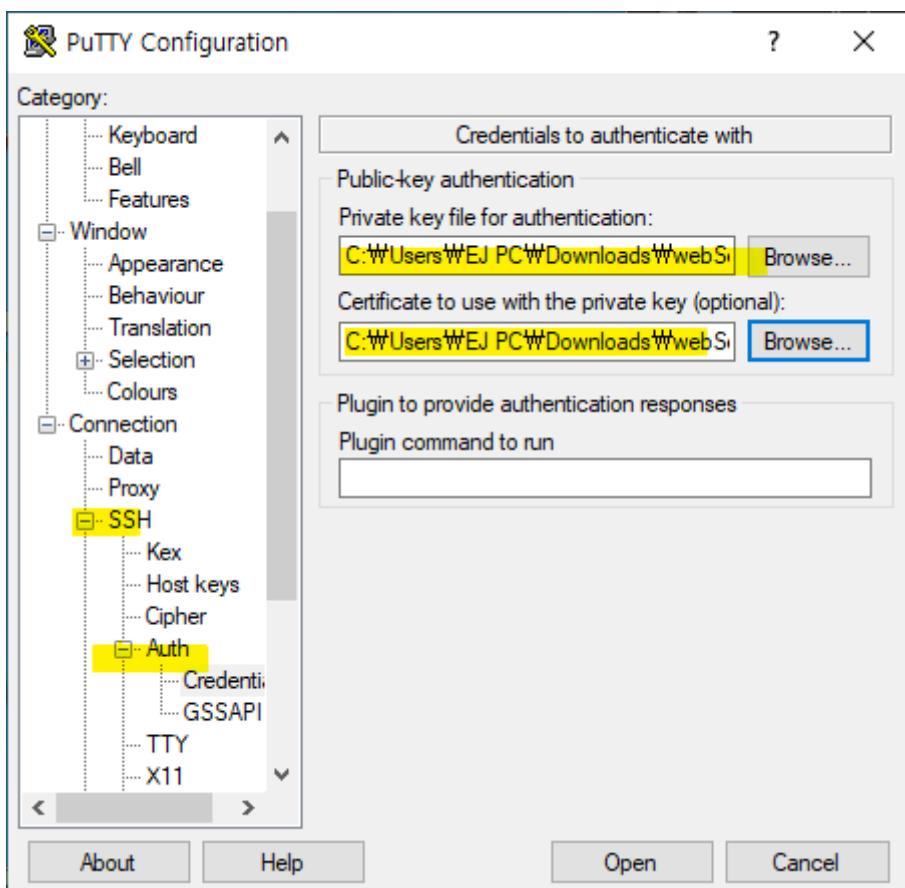
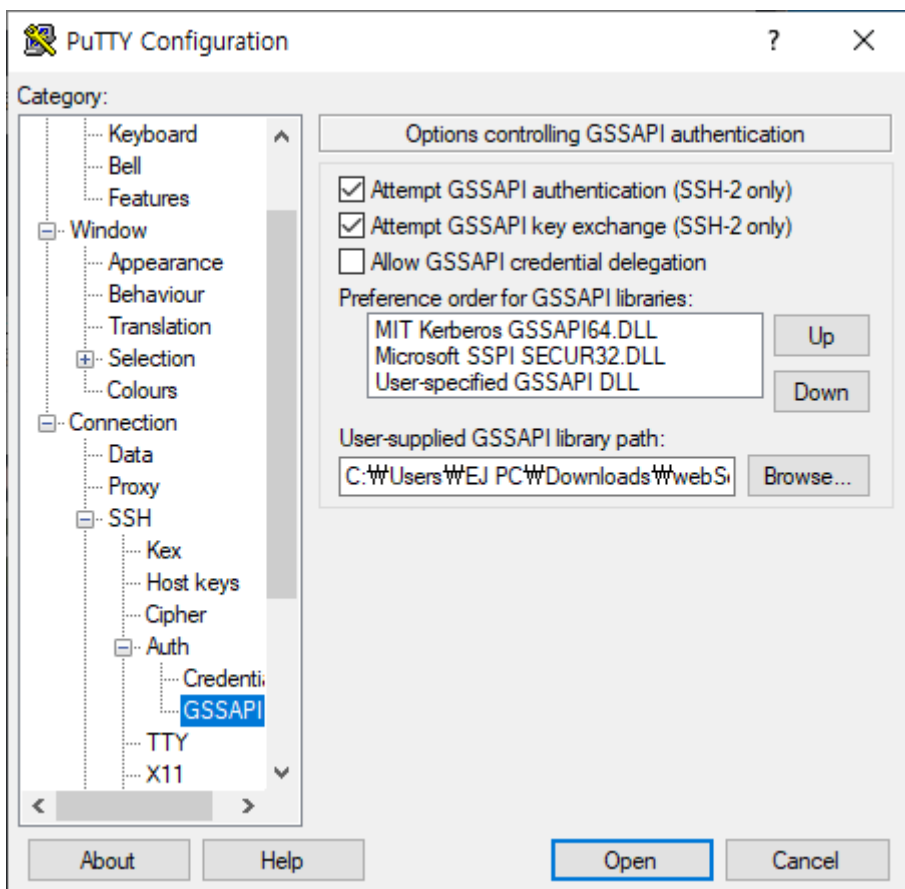
Save the generated key Save public key Save private key

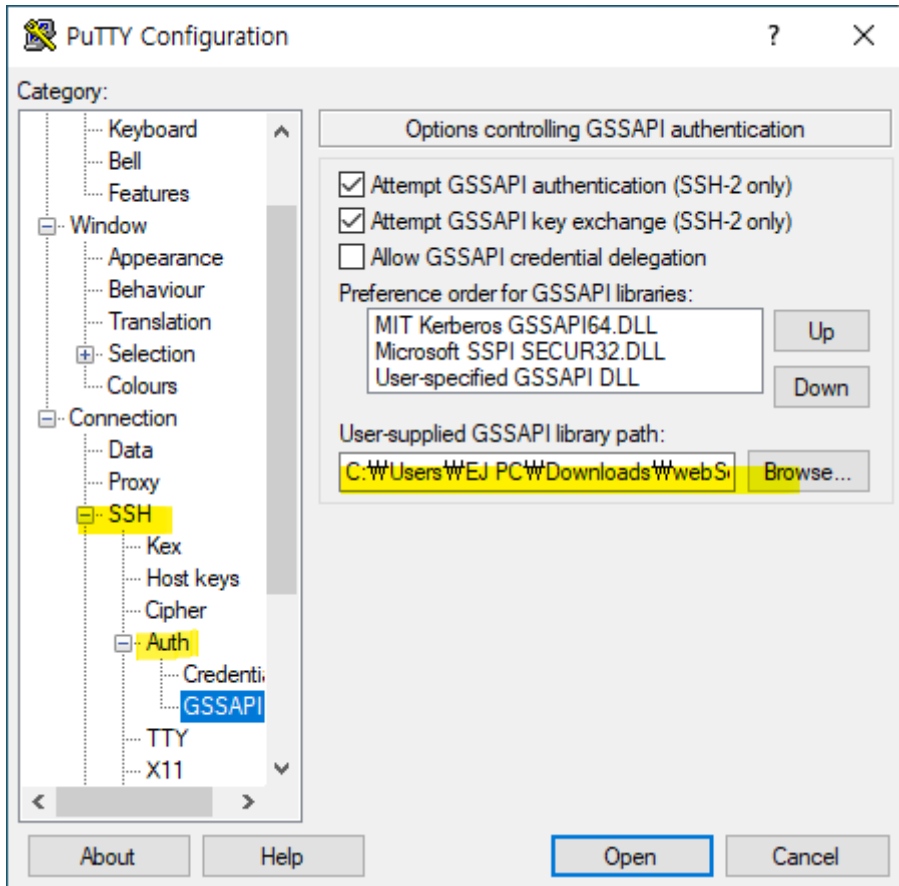
Parameters

Type of key to generate:
☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:

]

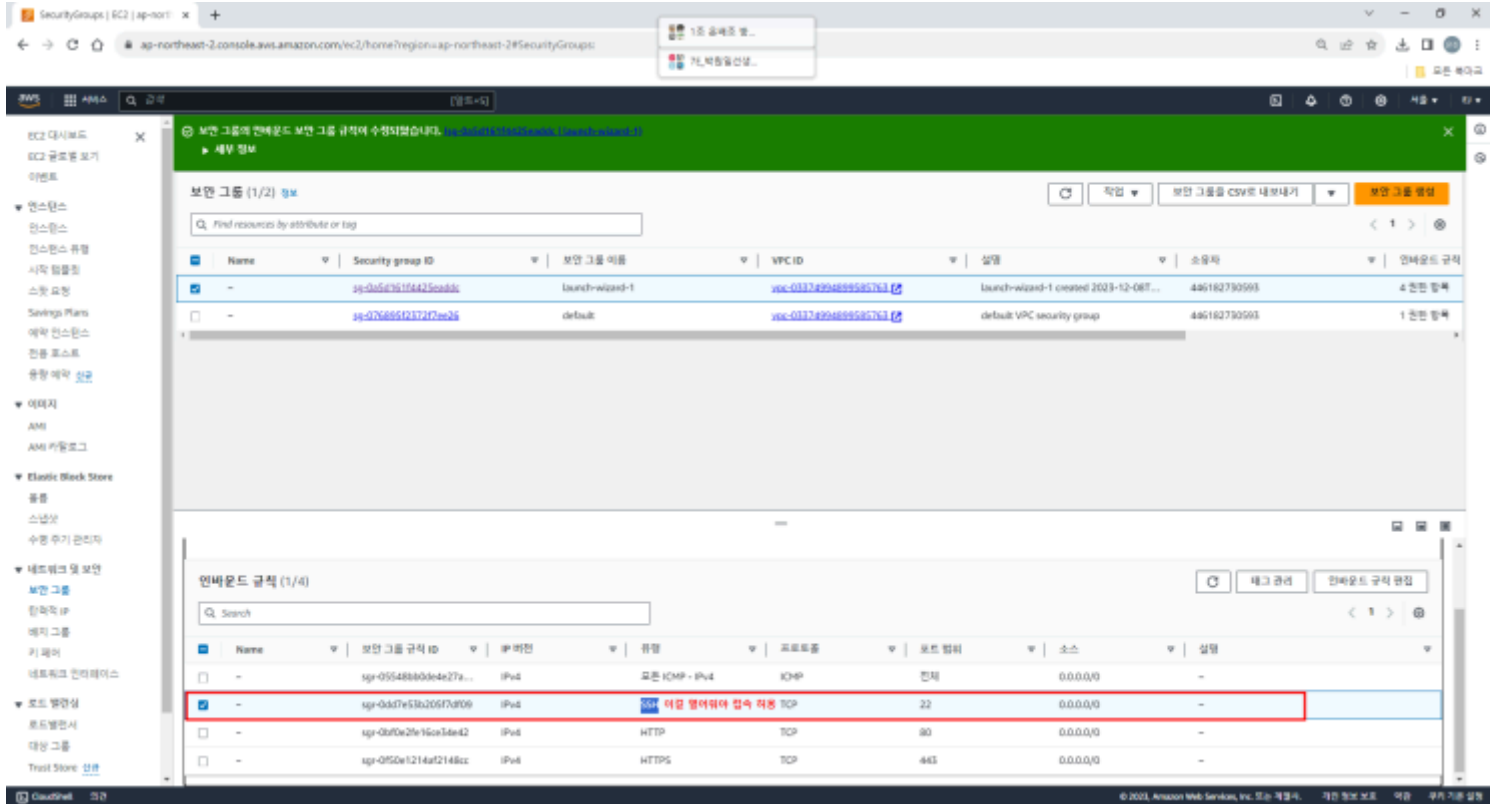




pem은 mac 리눅스에서

window에서는 ppk

윈도우는 푸티 사용하고 푸티는 PPK확장자 사용한다. .pem 을 .ppk로 변환하는 과정 필요
load할 때 설정값 저장해야 '접속 허용'된다.



AWS 에서

1. 인스턴스 생성
2. 보안그룹- 인바운드 규칙 편집(Launch-wizard)
3. 탄력적IP연결
4. PuTTY generater로 .pem을 ppk로 변환하고
PuTTY로 IP주소 넣고 새로 Save

1. 대칭 키 (비밀키) : 64비트까지만 사용 안한다.
암호=복호

2. 비대칭 키

(개인) 암호 key \neq 복호 key (공개 key)

1쌍의 Key pair 키페어

내가 (복호 key)공개 key를 여러명에게 보내서 그들이 열어 볼 수 있게 한다.

니가 암호화를 잘 해서 보내줘야 한다 그러려면

비대칭 키(Asymmetric Key)는 공개 키(Public Key)와 개인 키(Private Key)라는 두 종류의 키를 사용하는 암호화 체계를 말합니다. 이러한 암호화 방식은 한 키로는 암호화만 하고, 다른 키로는 복호화만 할 수 있어서 "비대칭"이라는 용어가 사용됩니다.

여기서는 주로 사용되는 비대칭 키 알고리즘 중 하나인 RSA(Rivest-Shamir-Adleman) 알고리즘을 기준으로 설명하겠습니다.

1. 공개 키 (Public Key):

- 공개 키는 누구나 알 수 있고, 메시지를 암호화하는 데 사용
- 일반적으로 사용자의 식별 정보와 함께 공개되며, 다른 이들이 해당 사용자에게 안전하게 메시지를 전송할 수 있도록 하는 열쇠

2. 개인 키 (Private Key):

- 개인 키는 사용자만이 알고 있고, 암호화된 메시지를 해독하는 데 사용
- 공개 키로 암호화된 메시지는 해당 개인 키로만 해독할 수 있음