

# AWS 클라우드 인프라 연구 및 구현

정지훈

# 목차

## 1.개요

1-1).클라우드란?

1-2)특징

1-3)유형

1-4)장/단점

1-4-1) 정량적 장점/정서적 장점

## 2.실습구현

2-1)인스턴스 생성

2-2)Linux 서버

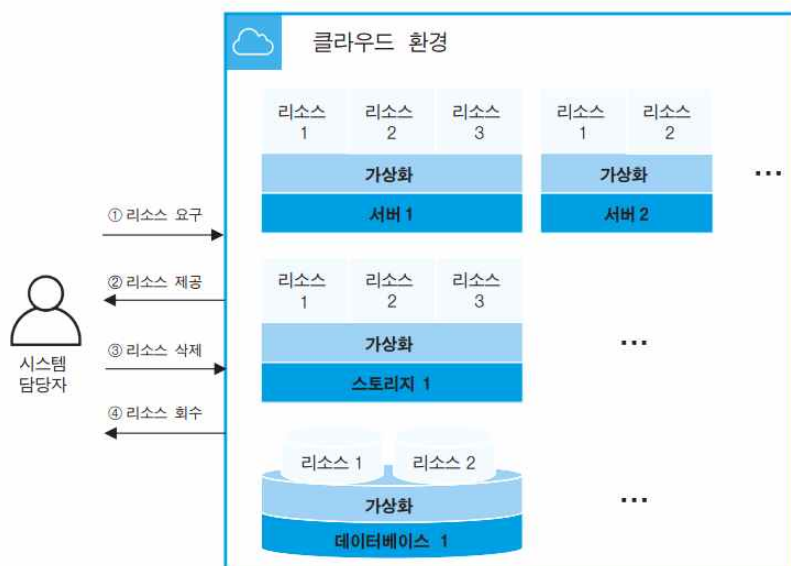
2-3)FTP 서버

## 1. 개요

AWS 클라우드 서비스를 이용하여 인프라 연구하면서 구축한다.

### 1-1)클라우드란?

: 하드웨어나 소프트웨어 등을 직접 구축하지 않고, 제2의 전문업체로부터 인터넷을 통해 필요한 IT 자원을 원하는 만큼 받아 즉시 사용할 수 있으며, 사용한 시간만큼 비용을 지불하면 되는 서비스



### 1-2)클라우드 특징

-접속 용이성

시간과 장소에 상관없이 인터넷을 통해 클라우드 서비스 이용

-유연성

갑작스러운 이용량 증가나 이용자 수 변화에 신속하고 유연하게 대응 할 수 있기 때문에 중단없이 서비스를 제공

-주문형 셀프서비스

사용자는 클라우드 서비스 제공자와 직접적인 요청이나 상호작용

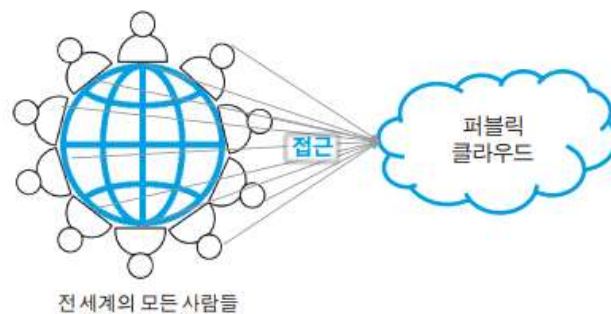
을 거치지 않고, 자율적으로 자신이 원하는 클라우드 서비스 이용

-사용량 기반 과금제

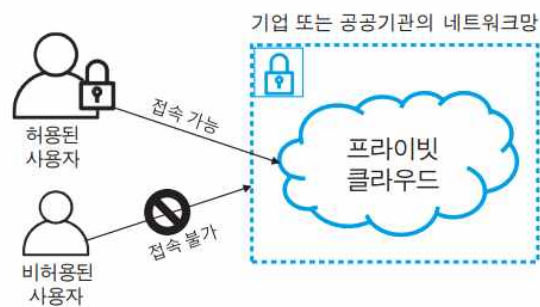
클라우드 사용자는 서비스 사용량에 대해서만 비용 지불

### 1-3)클라우드 유형

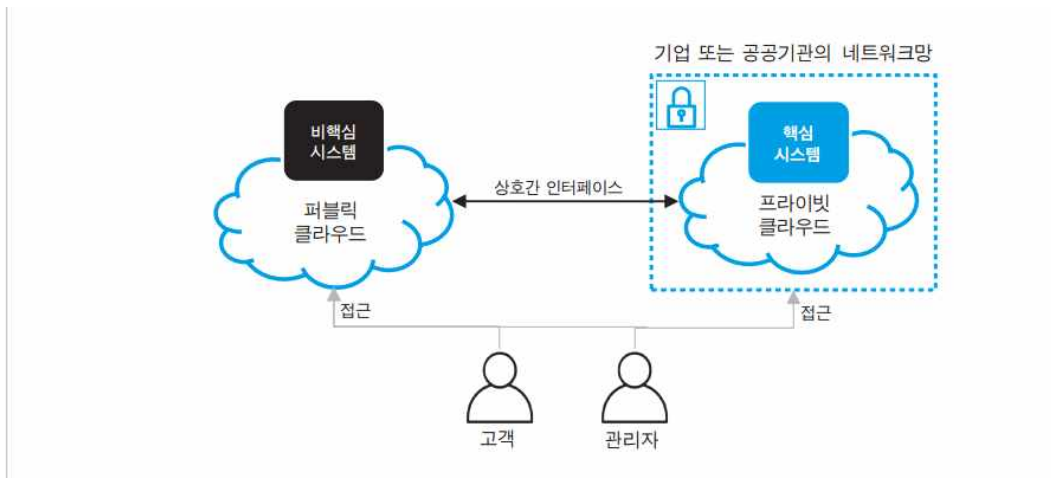
퍼블릭 클라우드 유형: 전 세계에 있는 누구나 인터넷을 통해 접근해서 클라우드 서비스를 활용하는 것



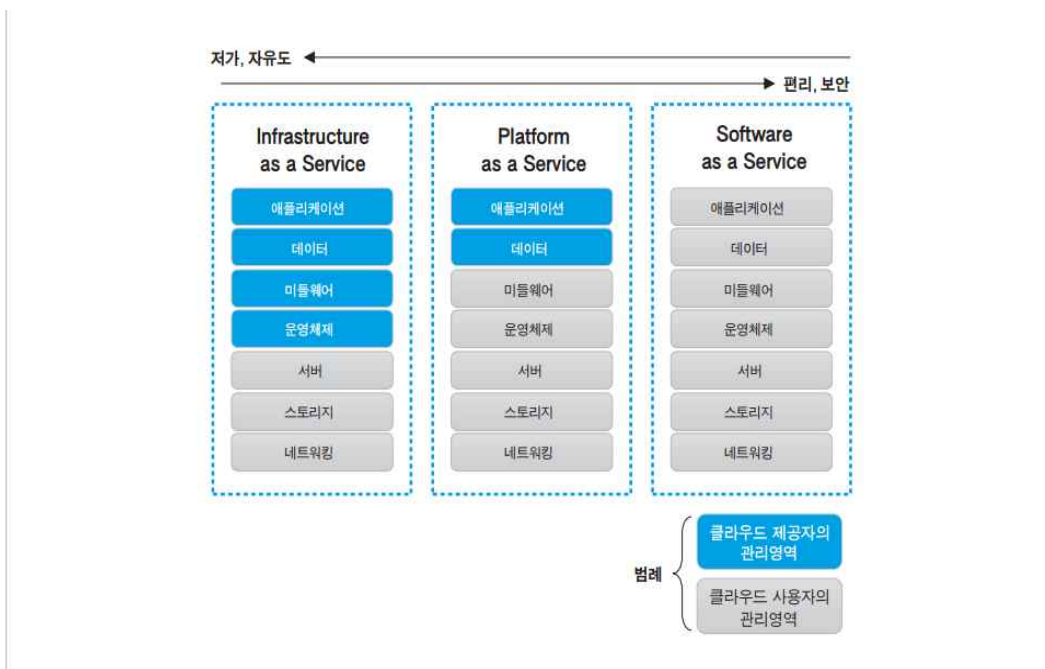
프라이빗 클라우드 : 허가된 그룹내에서만 활용



하이브리드 클라우드: 퍼블릭 클라우드와 프라이빗 클라우드를 결합한 형태



## 서비스 모델에 따른 클라우드 유형



-IaaS(Infrastructure as a Service)

: 인프라(서버, 네트워크, 스토리지 등)에 한해서만 지원받는 서비스 모델

-PaaS(Platform as a Service)

: IaaS 영역을 포함하고 그 위에 플랫폼(애플리케이션 또는 소프트웨어를 실행하기 위한 환경) 영역까지 제공되는 서비스, 개발환경에 대한 구축을 고민할 필요 없이 빠르게 사용하고 쉽게 개발

한다

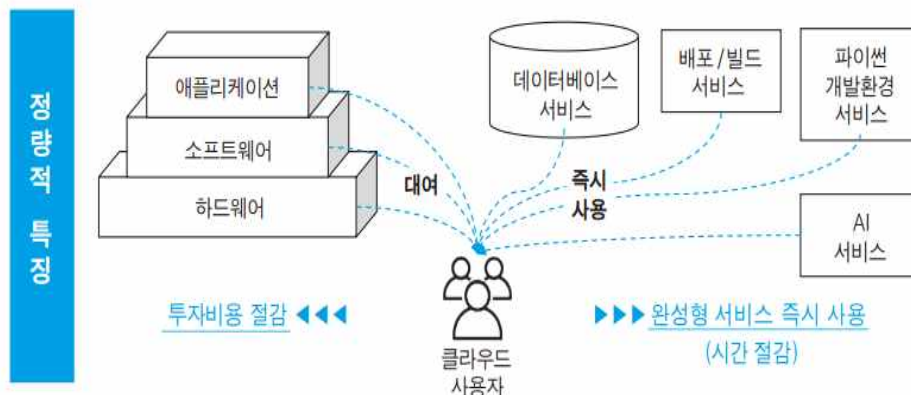
(ex) AWS의 RDS Relational Database Service

-Saas(Software as a Service)

:최종 소프트웨어로 일반 사용자 수준의 서비스를 바로 활용하는 것, (ex)마이크로소프트 365

## 1-4) 클라우드 장/단점

장점: 비용과 시간 투자 측면, 자원의 효율적 활용과 생산성 측면에 강점



## 정량적/정성적 장점

### 정량적 장점

\*비용 절감: IT 자원(하드웨어, 소프트웨어, 애플리케이션)을 다른 사용자와 공유하고, 소유가 아니라 대여하여 사용하기 때문에 구매/유지 및 인건비, 유지보스 등의 비용이 절감

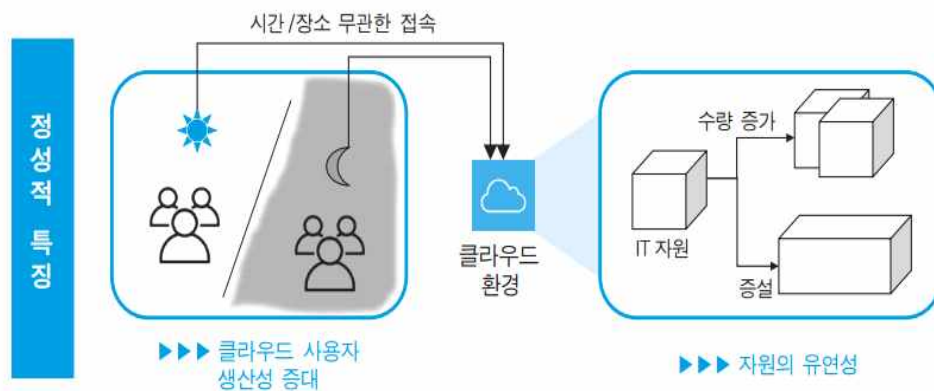
\*완성형 서비스 활용으로 시간 절감: 플랫폼과 애플리케이션 자

체를 즉시 사용 가능하므로, 자유롭고 빠른 개발환경과 비즈니스 트렌드의 변화 속도에 맞춰 신속하게 대응 가능

## 정성적 특징

\*생산성 향상: 인터넷만 되면 언제, 어디서나 스마트폰 등의 다양한 단말기를 통해 업무가 가능하므로, 스마트 워크 실현 가능

\*자원의 유연성: IT 자원의 수요 변화에 신속하고 탄력적으로 대응할 수 있어 필요한 만큼 IT 자원을 활용하는 것이 가능



## 단점

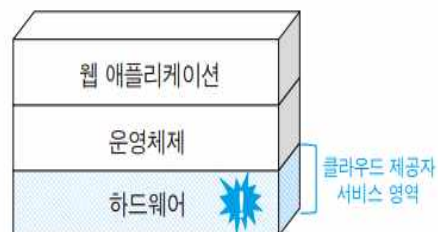
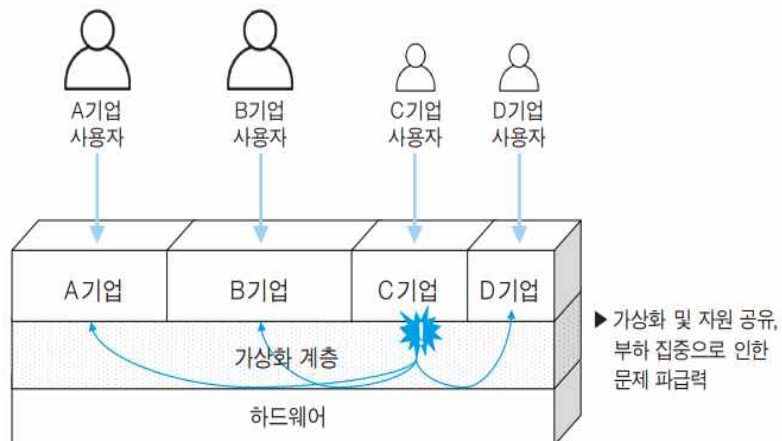
\*가상화 인프라 취약성: 가상화 기술을 통해 클라우드 사용자들의 개별 가상서버들이 상호 연결되어 다양한 공격 경로가 발생할 수 있으며, 가상서버와 하이퍼바이저로의 해킹 시도, DDoS 공격, 악성코드 전파 등이 상대적으로 쉬움

\*자원 공유로 인한 취약성: 동일 호스트상에 타인의 정보가 혼재되어 비인가자의 정보 접근 가능성이 큼

\*자원 집중화로 인한 취약성: 예기치 않게 클라우드의 특정 지역 (Region)에서 장애가 발생하면, 이용자 서비스 연쇄 중단과 대규

모 피해 발생 가능

\*장애 발생에 대한 블랙박스 문제: 클라우드 환경 자체에 장애나 이슈가 발생한 경우에는 클라우드



(IaaS 서비스를 활용하는 것으로 가정)

클라우드 제공자가 하드웨어 이슈를 조치하기 전까지,  
사용자는 원인과 진척 상황을 알기 어려움

▶▶▶ Blackbox 문제



## 2. 실습구현

### 2-1)인스턴스생성 (AWS 윈도우 서버 실행하기)

#### (1) 이름 : Example9 작성

이름 및 태그 정보

이름  
Example9

추가 태그 추가

▼ 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.

Q 수천 개의 애플리케이션 및 OS 이미지를 포함하는 검색 키를 입력하십시오

최근 사용 Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S

더 많은 AMI 찾아보기

AWS, Marketplace 및 커뮤니티의 AMI 포함

▼ 요약

인스턴스 개수 정보  
1

소프트웨어 이미지(AMI)  
Microsoft Windows Server 2019... 더 보기  
ami-05381ede339c68f49

가상 서버 유형(인스턴스 유형)  
t2.micro

방화벽(보안 그룹)  
새 보안 그룹

스토리지(볼륨)  
1개의 볼륨 - 30GiB

프리 티어 첫 해에는 월별 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**

#### (2) 네트워크 편집 > 보안 그룹 규칙 > RDP 소스유형 내 IP로 설정

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  
launch-wizard-6 created 2022-08-31T03:30:15.953Z

연바운드 보안 그룹 규칙

▼ 보안 그룹 규칙 1 (TCP, 3389, 221.157.163.135/32)

제거

유형 정보	프로토콜 정보	포트 범위 정보
rdp	TCP	3389

소스 유형 정보  
내 IP

원본 정보  
CIDR, 협동사 목록 또는 보안 그룹  
221.157.163.135/32

설명 - optional 정보  
예: 관리자 데스크톱용 SSH

보안 그룹 규칙 추가

▼ 스토리지 구성 정보

1x 30 GiB gp2 루트 볼륨

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

▼ 요약

인스턴스 개수 정보  
1

소프트웨어 이미지(AMI)  
Microsoft Windows Server 2019... 더 보기  
ami-05381ede339c68f49

가상 서버 유형(인스턴스 유형)  
t2.micro

방화벽(보안 그룹)  
새 보안 그룹

스토리지(볼륨)  
1개의 볼륨 - 30GiB

프리 티어 첫 해에는 월별 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**

### (3) 키 페어 생성(SSH 연결)

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

hoonie

새 키 페어 생성

### (4) 인스턴스 연결

New EC2 Experience

EC2 대시보드

EC2 글로벌 보기

이벤트

태그

제한

인스턴스

인스턴스 유형

시작 템플릿

스팟 요청

Savings Plans

예약 인스턴스

전용 호스트

용량 예약

이미지

AMI

AMI 카탈로그

Elastic Block Store

볼륨

스냅샷

인스턴스 (1/7) 정보

연결

인스턴스 상태

작업

인스턴스 시작

검색

Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS	퍼블릭 IP
Example6	i-03443f6fb89c6a0ac	종료됨	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	-	43.200.1...
Example5	i-04b835f29006295c3	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	ec2-13-124-177-85.ap-...	13.124.1...
Example 4	i-0ec7ffdb14b28e258	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	ec2-15-164-94-208.ap-...	15.164.9...
Example1	i-0ed19a2b672a68f54	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	ec2-13-124-6-73.ap-no...	13.124.6...
Example8	i-0bed22cb33e788271	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	ec2-54-180-119-187.ap...	54.180.1...
Example9	i-0660df1d8e14d237c	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	ec2-43-200-171-223.ap...	43.200.1...

인스턴스: i-0660df1d8e14d237c(Example9)

플랫폼

AMI ID

모니터링

플랫폼 세부 정보

AMI 이름

중요 방지

중지 방지

시작 시간

AMI 위치

비활성

Wed Aug 31 2022 12:31:56 GMT+0900 (한국 표준시) (44 minutes)

amazon/Windows\_Server-2012-R2\_RTM-English-64Bit-Base-2022.08.10

인스턴스 자동 복구

수명 주기

중지-최대 절전 모드 동작

기본값

정상

비활성

AMI 시작 인덱스

키 페어 이름

상태 전환 이유

0

none

-

연결

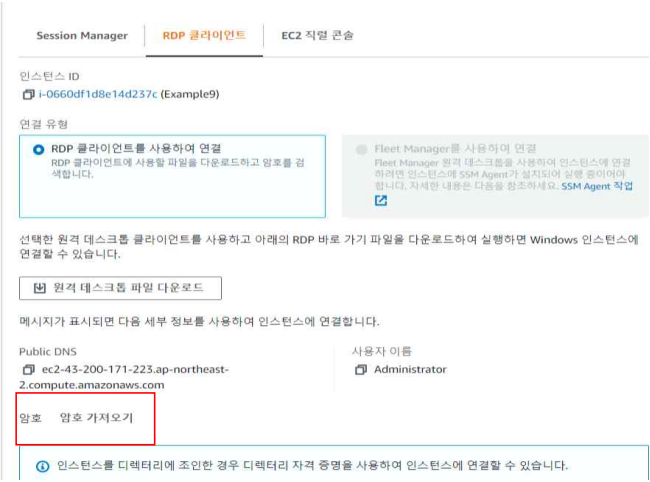
인스턴스를 선택하고 싶으신가요? 새로 추가된 다음 기기를 Unified Settings에서 선택할 수 있습니다.

© 2022, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호

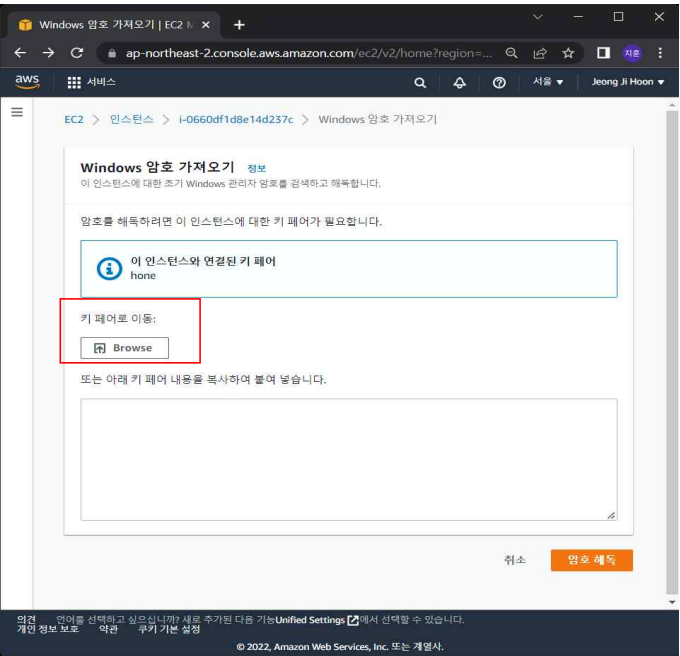
약관

루키 기본 설정

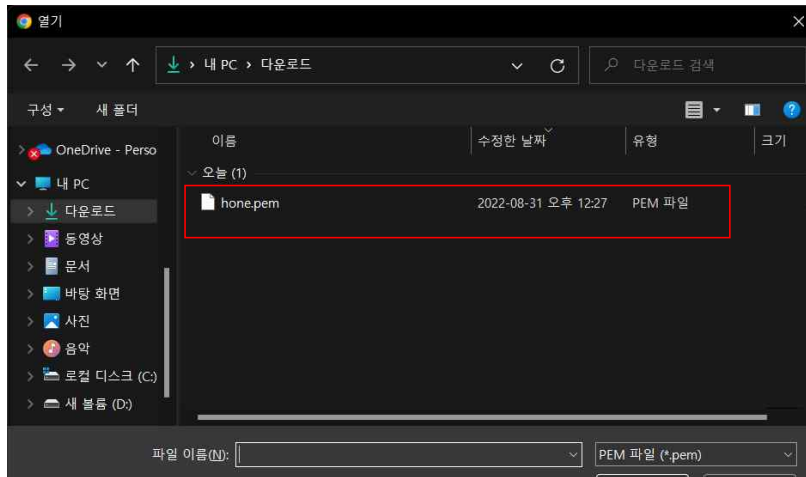
RDP 클라이언트 > 암호 가져오기클릭



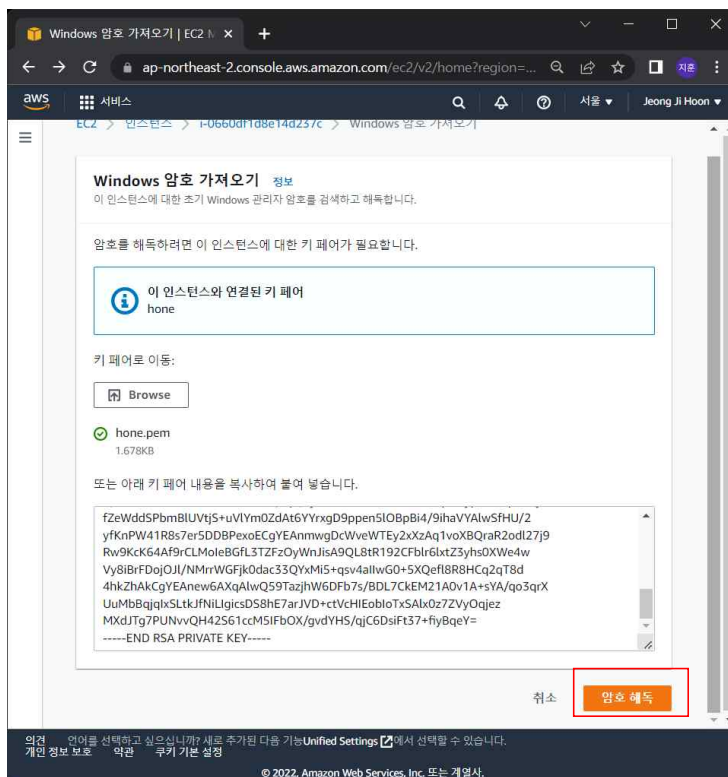
-Browse버튼 클릭



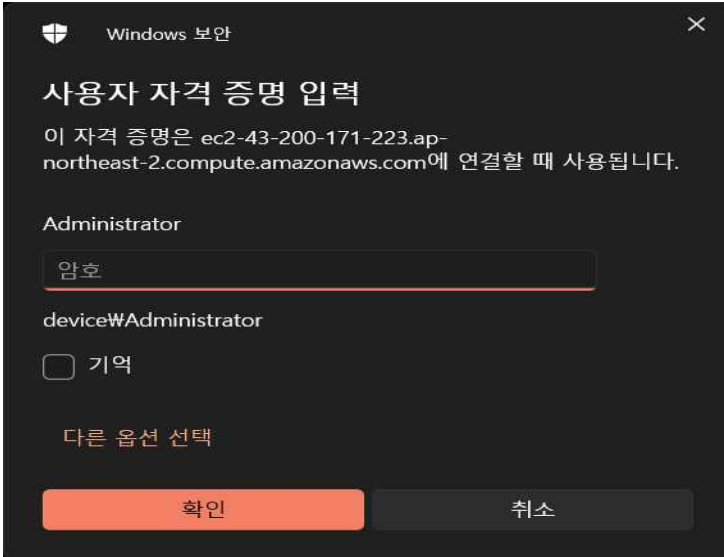
-해당 \*.pem 선택



-암호 해독 버튼 클릭



-암호 해독 후 생긴 비밀번호 입력 > 확인



Windows 보안

### 사용자 자격 증명 입력

이 자격 증명은 ec2-43-200-171-223.ap-northeast-2.compute.amazonaws.com에 연결할 때 사용됩니다.

Administrator

암호

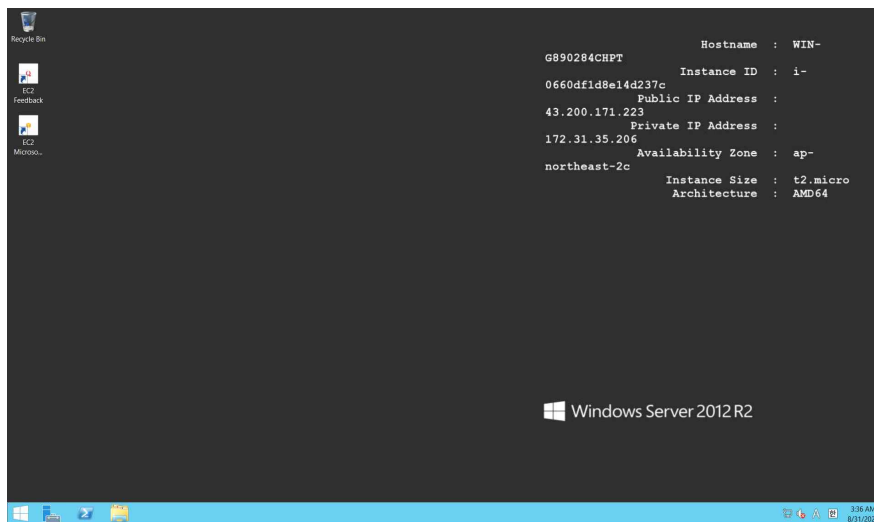
deviceWAdministrator

☐ 기억

다른 옵션 선택

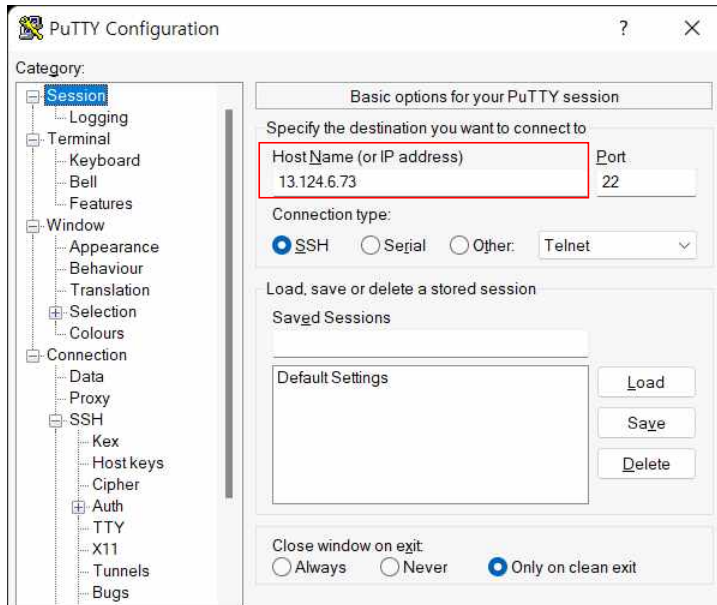
확인 취소

-정상적으로 동작

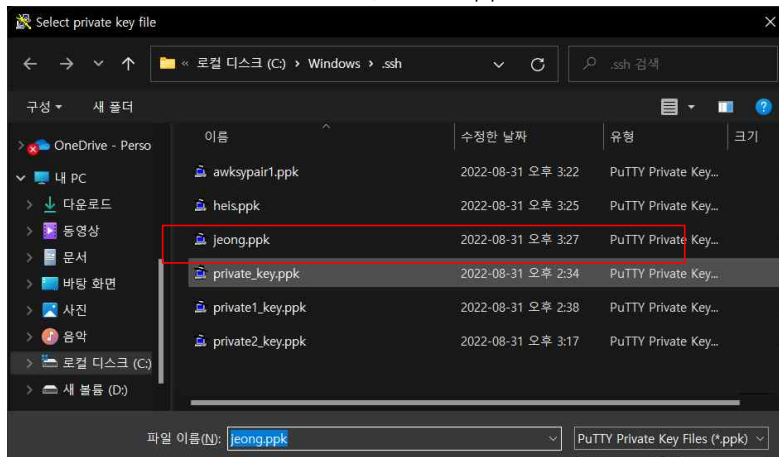


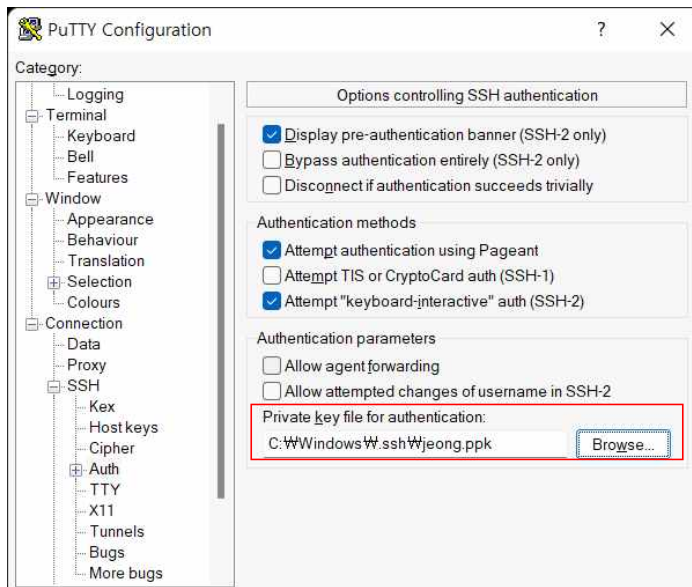
## 2-2) Linux서버

HostName(or IP address) 해당하는 IP 입력



-SSH > Auth > Browse > 해당하는 ppk





login as: ec2-user 입력하면 연결이 정상적으로 된 것을 확인할 수 있다

```
ec2-user@ip-172-31-8-77:~
login as: ec2-user
Authenticating with public key "Jeong" from agent
Last login: Wed Aug 31 10:49:13 2022 from 221.157.163.135

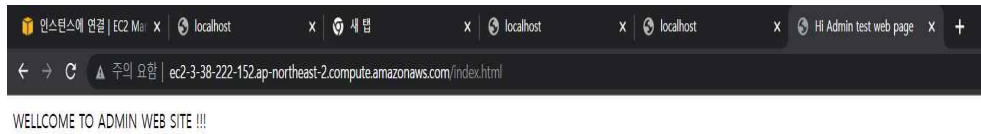
  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-8-77 ~]$
```

패키지 설치

```
#yum install -y firewall httpd mod_ssl
#systemctl enable --now httpd
#systemctl restart httpd
#firewall-cmd --permanent --add-service=httpd
#firewall-cmd --reload
```

-설정 한 웹페이지 화면이 나오는 것을 확인



## 2-3) FTP 서버

-vsftpd 설치 (# yum install -y vsftpd)

```
root@ip-172-31-8-77:/var/www/html
└─3479 /usr/sbin/httpd -DFOREGROUND
└─3523 /usr/sbin/httpd -DFOREGROUND

Aug 31 10:52:06 ip-172-31-8-77.ap-northeast-2.compute.internal systemd[1]: St...
Aug 31 10:52:06 ip-172-31-8-77.ap-northeast-2.compute.internal systemd[1]: St...
Hint: Some lines were ellipsized, use -l to show in full.
[root@ip-172-31-8-77 html]# clear
[root@ip-172-31-8-77 html]# yum -y install vsftpd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 00:00:00
Resolving Dependencies
--> Running transaction check
--> Package vsftpd.x86_64 0:3.0.2-25.amzn2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
vsftpd x86_64 3.0.2-25.amzn2 amzn2-core 170 k
Transaction Summary
-----
Install 1 Package
```

- vsftpd 재기동 및 status로 상태(active)확인

```
[root@ip-172-31-8-77 etc]# systemctl restart vsftpd
[root@ip-172-31-8-77 etc]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-08-31 12:05:20 UTC; 6s ago
     Process: 2068 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 2069 (vsftpd)
      CGroup: /system.slice/vsftpd.service
              └─2069 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Aug 31 12:05:20 ip-172-31-8-77.ap-northeast-2.compute.internal systemd[1]: Starting Vsftpd ftp daemon...
```



- vi /etc/vsftpd/vsftpd.conf > annonymous\_enable=NO로 변경 (보안설정)

```
root@ip-172-31-8-77:/etc/httpd/conf.d
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Steware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that 022 is used by most other ftp'd's
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
```

#방화벽등록 및 확인

```
-#firewall-cmd --permanent --add-service=ftp
-#firewall-cmd --reload
-#fierwall-cmd --list-all (ftp가 들어가있는지 확인!)
```

-banner\_file=/etc/vsftpd/banner.txt 문장을 추가.

```
root@ip-172-31-8-77:/etc
# Since, however, some broken FTP clients such as "mlftp" and "Mlurk" assume
# the presence of the "-s" option, so there is a timing case for enabling it,
# we require enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on "both" IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must use two copies of vsftpd with the configuration
# files.
# Make sure that one of the listen options is commented !!
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
#
# banner_file=/etc/vsftpd/banner.txt
chroot_local_user=YES
allow_writeable_chroot=YES
chroot_list_enable=YES
```

-인바이드 보안 그룹 > 규칙추가 > 20-21 추가 > 허용범위 0.0.0.0 선택 후 저장

EC2 > 보안 그룹 > sg-0598a6d2d7ef91b30 - launch-wizard-9 > 인바운드 규칙 편집

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보

보안 그룹 규칙 ID	유형	정보	프로토콜	포트 범위	소스	설명 - 선택 사항	작업
sg-07d661f978446aff3	SSH	TCP	22	사용자 ...	Q	221.157.163.135/32	삭제
sg-09eba106d0bcb2235	HTTP	TCP	80	사용자 ...	Q	221.157.163.135/32	삭제
sg-016c5e682d47bd2fc	사용자 지정 TCP	TCP	20 - 21	Anywh...	Q	0.0.0.0/0	삭제

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

-ftp 주소 입력하면 정상적으로 출력되면서 Name:user01, passowrd; user01 입력하면 정상적으로 되는 것을 확인

```
ftp> quit
[root@main /vscode/shellproject]# ftp 3.38.222.152
Connected to 3.38.222.152 (3.38.222.152).
220-+=====+
220-|
220-| Welcome to linux100.example.com |
220-|
220-| This is the linux100.example.com test server. |
220-|
220-| If you have not already done so, make sure |
220-| you have read the Downloading/Installation, |
220-| FAQ, and Disclaimer links on |
220-| http://www.solaris254.example.com. |
220-|
220-| This is a restricted access system. All |
220-| tranfers are logged. If you disagree |
220-| with this practice, log off now. |
220-|
220-| Questions go to SeoungChan Baik at |
220-| the address given on linux100.example.com |
220-|
220-+=====+
220
Name (3.38.222.152:root): user01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```