

kt cloud

Basic Course Hands on Lab

(7) H/A Architecture

Copyright© 2023 kt cloud corp. All rights reserved.

실습. LB를 통한 HA 구성하기

01

서버 생성과
설정

02

Load Balancer
구성

03

테스트 및
마무리

실제 운영환경에서는 고가용성을 위해 여러대의 서버가 동일한 서비스를 하면서 한 서버에서 문제가 발생하더라도 서비스를 지속적으로 할 수 있도록 서버들을 묶고, 그 앞에 Load Balancer를 두는 H/A 구성을 합니다.

kt cloud에서 이러한 구성을 위해 서버를 생성하고, 그 앞단에 Load Balancer를 배치시키기 위해서는 어떠한 단계를 거치게 되는지 실습을 통해 알아보니다.

실습 과정은 크게 세 개로 나누어 집니다.

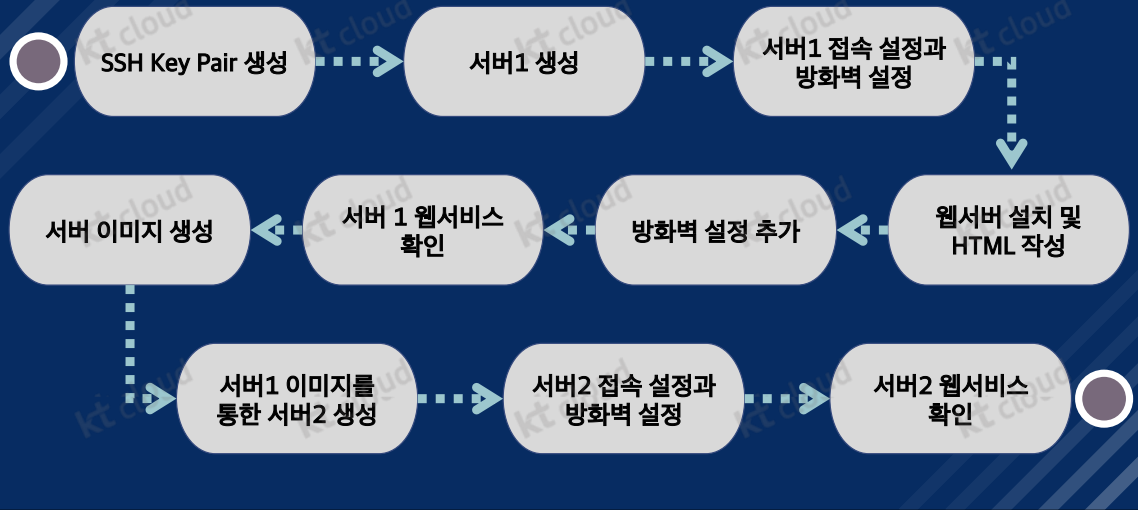
첫번째, 기존의 컴퓨팅 실습과 유사하게 서버를 2개를 생성하고, 각각 서비스를 띄워서 확인을 합니다.

두번째, Load Balancer를 생성하고 앞서 생성한 두 서버의 앞에 배치시킵니다.

이 때, StaticNAT를 사용하여 공인IP와 사설IP를 매핑합니다.

마지막으로 이 HA 구성이 어떻게 동작하는지 살펴보고, 일련의 과정에서 생성한 서비스와 설정을 삭제하는 것으로 실습을 마무리 합니다.

실습 1. 서버 생성과 설정



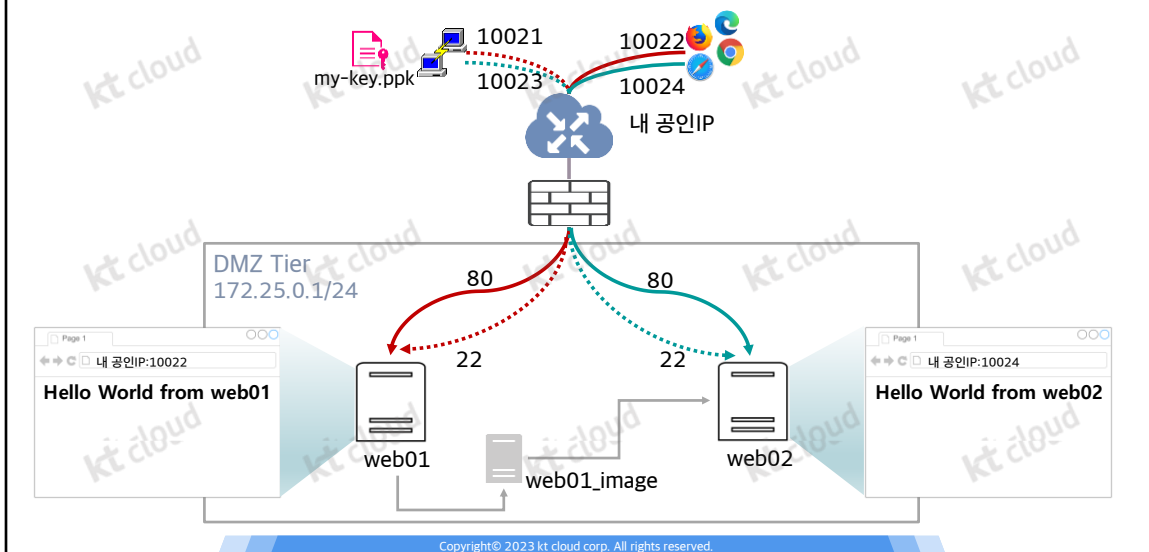
실습 1은 서버 생성과 관련된 실습입니다.

이미 Computing 실습에서 접해보았던 내용으로 마지막 복습으로 각자 생성해 보도록 하겠습니다.

실습의 과정은 기존의 내용을 참조하시되, 제시된 정보를 확인하여 만들어 보도록 합니다.

실습 교재에 제시된 이름이나 포트 정보 등은 임의로 바꾸셔도 무방하나, 잘 메모하셔서 진행에 어려움이 없도록 주의합니다.

실습 1. 개요



구성하고자 하는 서비스는 위와 같습니다.

- 2개의 웹 서비스를 하는 서버를 구성합니다.
- 각각의 서버는 Web 포트(80)와 SSH포트(22)를 열어 두고, 외부에서 이에 대한 접근을 할 것입니다.
- 하나의 공인 IP를 통해 접근하기 때문에 각각의 포트는 80,22와는 다른 공인 포트 정보를 가집니다.
- SSH 접속시에 필요한 Private Key를 생성하며, 이름은 my-key 입니다.
- 두 서버에는 웹 서버를 설치하고, index.html에는 두 서버를 구분하기 위해 내용을 각기 달리합니다.

지정하는 값과 이름에 대한 상세 사항은 다음 페이지를 참조합니다.

실습 1. 접근제어, 방화벽 정보

구분		Public Port	Private Port
web01	SSH	10021	22
	Web	10022	80
web02	SSH	10023	22
	Web	10024	80

Action	Source	Source CIDR	Destination
Allow	external	all	PF_공인IP_10021_TCP
Allow	external	all	PF_공인IP_10022_TCP
Allow	external	all	PF_공인IP_10023_TCP
Allow	external	all	PF_공인IP_10024_TCP

Copyright© 2023 kt cloud corp. All rights reserved.

두 서버에 각 2개의 포트를 사용하여 접근하게 되므로, 총 4개의 공인포트와의 매핑이 있습니다. 이 부분은 [접속 설정]에서 관리합니다.

이들 포트에 대한 접근을 허용하려면, 방화벽 설정에서 각 Port Forwarding에 대한 허용 정책을 추가합니다.

참고로, 웹서버의 설치파일 다운로드 작업을 위해 80,53 포트 허용 정책도 추가합니다.

1-1. SSH Key Pair 생성

SSH Key Pair
가상 서버 접속에 사용할 SSH Key Pair를 관리합니다.

SSH Key Pair 생성 삭제 모든 위치 >

이름	위치	Fingerprint
SSH Key Pair 목록 (가상 서버에 연결 가능)		

SSH Key Pair 생성합니다.

위치 DX-M1

이름 my-key 6/100

Key 이름 : my-key

취소 생성하기

[Server]-[SSH Key Pair] 메뉴를 선택하고,
[SSH Key Pair 생성]버튼 클릭

Copyright© 2023 kt cloud corp. All rights reserved.

먼저 SSH Key Pair를 생성합니다.

[Server]-[SSH Key Pair]메뉴를 클릭하여 새로운 키를 생성합니다.

여기서의 이름은 **my-key** 라고 하겠습니다.

1-2. SSH Key Pair 저장

The screenshot displays the 'SSH Key Pair' management page. At the top, a message states 'SSH Key Pair 생성이 완료되었습니다.' (SSH Key Pair creation is complete). Below this, a table lists the generated key pair with columns for '이름' (Name), '위치' (Location), and 'Fingerprint'. The entry 'my-key' is highlighted with a red box. To the right, a '다운로드' (Download) button is also highlighted with a red box. A red arrow points from this button to a file explorer window showing the downloaded file 'my-key.pem'. A '주의' (Warning) box on the right contains instructions: 'SSH Key Pair 생성 완료 창에서 [다운로드]를 반드시 클릭하여 내 컴퓨터에 저장' (Must click [Download] in the completion window to save to the computer) and '이후에는 다운로드가 불가능하므로, 키를 분실하거나 문제가 발생하면 새로운 키로 다시 생성해야 함' (Afterwards, download is not possible, so if the key is lost or a problem occurs, a new key must be generated). Below the table, a red box highlights the 'my-key' entry and its fingerprint 'fe:04:39:b5:19:bcc7:54:cd:88:fc:de:04:ec:37:42'.

SSH Key Pair 생성이 완료되었습니다.

이름 my-key

! Key Pair는 이 페이지와 Email로 1회만 제공됩니다.

닫기 다운로드

주의

SSH Key Pair 생성 완료 창에서 [다운로드]를 반드시 클릭하여 내 컴퓨터에 저장

이후에는 다운로드가 불가능하므로, 키를 분실하거나 문제가 발생하면 새로운 키로 다시 생성해야 함

Key 이름.pem 파일 다운로드

SSH Key Pair

가상 서버 접속에 사용할 SSH Key Pair를 관리합니다.

SSH Key Pair 생성 삭제 모든 위치 >

이름	위치	Fingerprint
my-key	DX-M1	fe:04:39:b5:19:bcc7:54:cd:88:fc:de:04:ec:37:42

Copyright© 2023 kt cloud corp. All rights reserved.

생성이 되고 나면 생성 완료창이 뜹니다. 이 창에서 **[다운로드]**를 반드시 클릭하여서 내 컴퓨터에 이 키를 저장해야 이후 접속에서 사용할 수 있습니다.

키의 다운로드는 이 완료창에서만 가능하므로, 꼭 다운로드하도록 합니다.

* 주의하실 점은, 이 창이 뜨기 전에 다른 페이지로 이동하면 이 창을 확인할 수 없습니다. 시간이 조금 소요되더라도 완료창을 기다립니다.

1-3. web01 서버 생성(1)

The screenshot shows the kt cloud console interface. On the left, a sidebar menu lists various services: User, IAM, Server, Networking, Tier, Server Image, Volume, Volume Snapshot, Traffic, SSH Key Pair, Log History, and Virtual IP. The 'Server' menu item is highlighted with a red box. A red arrow points from this box to the '서버 생성' (Create Server) button in the top navigation bar. The main content area is titled 'Server' and contains a sub-header '가상 서버를 관리합니다.' (Manage virtual servers). Below this, there are buttons for '서버 생성' (Create Server), '시작' (Start), '정지' (Stop), '재시작' (Restart), '강제재시작' (Force Restart), '삭제' (Delete), '접속설정' (Connect Settings), and a dropdown menu. To the right of these buttons is a search icon, a '모든 위치 · 모든 상태 >' link, and a refresh icon. Below the buttons is a table with columns: 이름 (Name), 상태 (Status), 위치 (Location), 운영체제 (OS), 사양 (Spec), 상품 (Product), 볼륨 타입 (Volume Type), 사설IP (Private IP), 추가사설IP (Additional Private IP), and 생성일시 (Creation Time). A text box at the bottom of the screenshot contains the instruction: '[Server]-[Server] 메뉴를 선택하고, [서버 생성]버튼 클릭' (Select [Server]-[Server] menu and click [Create Server] button).

Copyright© 2023 kt cloud corp. All rights reserved.

이제 첫번째 서버를 생성합니다.

[Server]-[Server] 메뉴에서 제일 왼쪽의 [서버 생성]을 클릭합니다.

1-3. web01 서버 생성(2)

서버 생성

위치

Tier ①

서버 이름 ②

서버 용도

서버 타입

루트 볼륨 크기

Key Pair ③

실습1 개요 페이지를 참조하여 입력 값을 확인

- ① Tier : 서버가 존재할 Tier. 여기서는 반드시 **DMZ**로 설정
- ② 서버 이름 : 서버 이름은 고유해야 하며, **web01**로 지정
- ③ Key Pair : 이후 SSH로 접속할 때 필요하므로,
이전 단계에서 생성한 **my-key**를 선택

서버 생성시 입력하는 값들을 살펴봅시다.

먼저 처음 개요 그림과 같이, 이 서버는 DMZ에 위치할 것이며, 이전 단계에서 생성한 my-key를 이용할 것입니다.

상세 입력 사항은 다음과 같습니다.

- Tier : **DMZ**
- 서버 이름 : **web01**
- 서버 용도 : ETC
- 서버 타입 : HDD
- 루트 볼륨 크기 : 50GB
- Key Pair : **my-key**

1-3. web01 서버 생성(3)

CPU-AMD Server	CentOS	CentOS 7.2 64bit	1vcore 1GB
CPU-Intel Server	Ubuntu	CentOS 7.6 64bit	1vcore 2GB
Application	Redhat Linux	CentOS 7.8 64bit	2vcore 2GB
GPU Server	Windows	CentOS 7.9 64bit	2vcore 4GB
Hyperscale AI Computing	DEBIAN		2vcore 8GB
DB	Rocky(BETA)		2vcore 16GB
			4vcore 4GB
			4vcore 8GB

서버 기본 정보 하단의 서버 사양은 서버의 용도에 맞추어 선택함.

여기서는 간단한 실습을 위한 용도이므로 다음과 같이 선택

- CPU-Intel Server
- CentOS
- CentOS 7.9
- 1vcore 1GB

서버 생성 화면 하단의 서버 스펙 부분에서 각각을 선택합니다.
여기서는 단순 테스트 용이므로 가장 적은 사양으로 선택하겠습니다.

- CPU-Intel Server
- CentOS
- CentOS 7.9
- 1vcore 1GB

1-4. web01 서버 확인

Server

가상 서버를 관리합니다.

서버 생성

삭제

정지

재시작

상태 재시작

복제

입력값...

모든 위치 · 모든 상태 >

<input type="checkbox"/>	이름	상태	위치	운영체제
<input type="checkbox"/>	web01	● 사용	DX-M1	centos-7.9-64bit

생성한 web01 서버를 선택하고 [...]를 클릭하여 상세정보를 확인
이전의 입력 값들로 구성이 되어 있는지 확인

서버명

web01

요금제

월요금제

hostname

web01

SSH Key Pair

my-key

서버 ID

4378b82b-31fc-4e19-8d82-d985919a03f0

종류

표준

운영체제

centos-7.2-64bit

사양

1 vCore 1 GB

Volume

총50GB

상태

● 사용

위치

DX-M1

Copyright© 2023 kt cloud corp. All rights reserved.

서버가 생성되는데 시간이 약간 소요됩니다.

서버가 다 생성되고 나면, 사설 IP가 할당되고, 서버의 상태가 사용으로 되어 구동 중임을 알 수 있습니다.

생성이 완료되면 [...] 버튼을 눌러서 서버의 입력 내용을 다시 한번 확인합니다.

1-5. web01 서버 접속설정(22 포트)

web01

22(SSH) 내 공인 IP 10021 TCP

외부에서 접속할 공인 IP 선택 및 공인 Port 지정
(22번 포트에 대해 10021로 지정, 실습1 개요 참조)

+ 추가

web01 서버 접속을 설정합니다.

서버	사설Port	공인IP	공인Port	프로토콜
<input type="checkbox"/> web01	22	내 공인 IP	10021	TCP

Copyright© 2023 kt cloud corp. All rights reserved.

이제 외부에서 접근이 가능하도록 접속 설정을 해보겠습니다.

접속 설정은 클라우드 내부의 자원들은 각각 고유한 사설 IP를 가지고 있으나, 외부에서의 접근은 계정생성시 할당된 공인 IP 하나만을 이용하여 접근하게 됩니다.

따라서, 공인 IP의 여러 포트를 분할하여 각각 서버/서비스와 매핑하는 과정이 이 접속 설정입니다.

우리는 제일 먼저 지금 생성한 **web01**을 SSH로 접근해야 하므로, 이 서버의 **22번** 포트를 공인 IP의 **10021**포트로 매핑하겠습니다.

1-6. 아웃바운드 방화벽 규칙 추가

방화벽을 설정합니다. (IP or URL)

※방화벽 설정 가이드

삭제 이동

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	-	-	-

All Allow 아웃바운드 규칙 추가(이후 이 규칙은 삭제하지 않습니다)

Allow

DMZ_Sub

0.0.0.0/0

ALL

external

0.0.0.0/0

Start

End

Copyright© 2023 kt cloud corp. All rights reserved.

이후 생성된 가상서버에 필요한 패키지 설치 등을 진행하기 위해 필요한 추가 아웃바운드 규칙을 추가합니다.

예제에서는 yum 사용 및 DNS 사용 등을 모든 아웃바운드를 허용하는 규칙을 추가합니다.

이 설정은 과정 종료 시까지 삭제하지 않습니다.

1-7. web01 방화벽 설정

외부에서 접속을 하기 위해서 방화벽에서 허용(Allow) 정책을 추가해야 함
[Server]-[Networking] 메뉴를 선택하고, 해당 공인 IP 선택 후 [방화벽]버튼 클릭

Allow external 0.0.0.0/0 TCP DMZ_Sub PF_210.104.79.24_100... Start End

클라우드 외부에서 접근하는 것에 대한 허용

이전 단계에서 설정한 접속설정(PF_공인IP_10021_TCP) 선택

방화벽을 설정합니다. (IP or URL)
※방화벽 설정 가이드 보기

삭제 이동

설정 내용 확인

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명
<input type="checkbox"/>	1	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	.10021.T...		

예시는 외부에서 DMZ Tier로의 10021 포트에 대한 접근 허용 방화벽 규칙을 추가하고 있습니다.

1-7. web01 방화벽 설정

방화벽을 설정합니다. (IP or URL)

※방화벽 설정 가이드 >

삭제 이동

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	- -	●	-
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10021_...	●	-

방화벽 설정은 총 2개를 추가

(Putty 접속용)

- 외부에서 **web01**의 22번 포트에 대한 허용 : 외부에서의 접근이므로 **external → DMZ/PF_내 공인IP_10021_TCP**
(**web01**에서 Apache 설치를 위한 사이트 접속/파일전송용)
- 외부로 나가는 허용 : **DMZ → external All 포트**

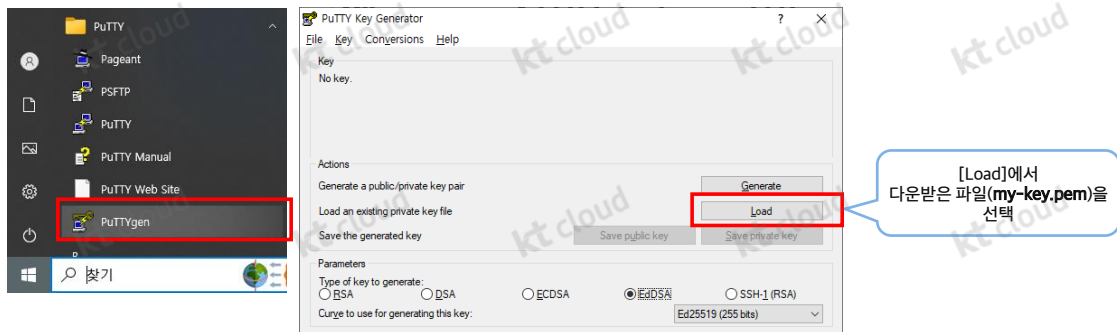
Copyright© 2023 kt cloud corp. All rights reserved.

15

web01에 접속 후에 웹 서버를 설치하게 됩니다. 웹 서버 설치 프로그램을 다운로드 받고 미러링 사이트를 찾기 위해서 **web01**에서 외부로 나가는 방화벽 정책도 추가로 설정합니다.

실제로는 명확히 사용하는 포트를 지정하는 것이 맞습니다만, 이번 실습에서는 편의상 All 포트로 설정하도록 하겠습니다.

1-8. .pem 파일을 이용한 Key 생성(1)

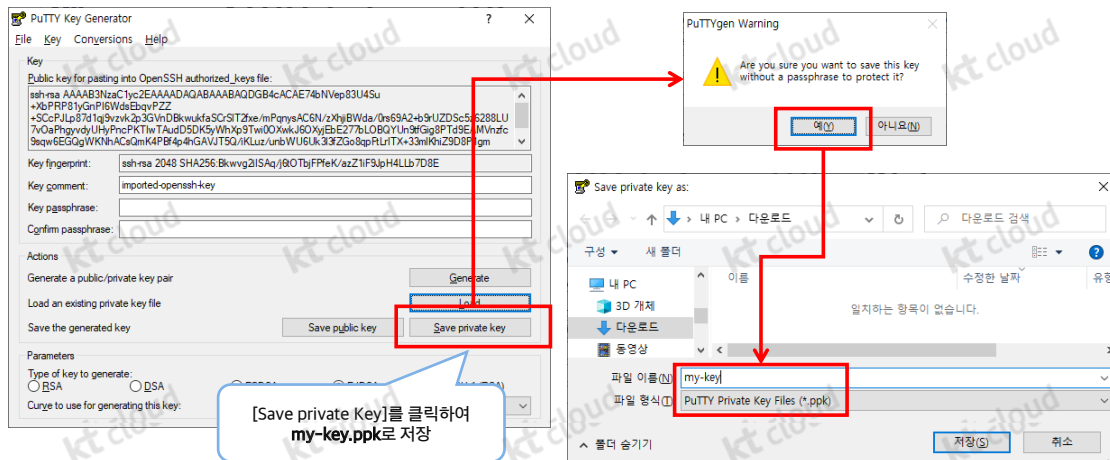


SSH 접속에 앞서

첫번째 단계에서 다운로드했던 Key Pair 파일은 확장자가 **.pem** 파일로, 이 파일을 이용하여 Private Key를 생성해야 함

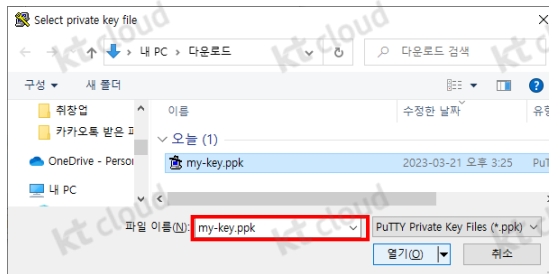
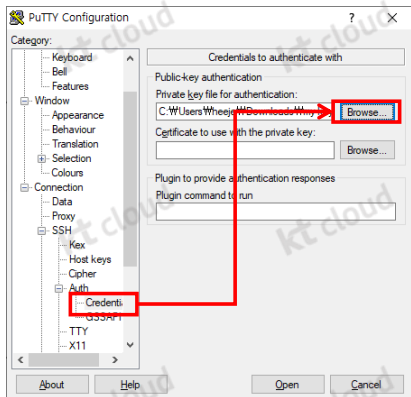
이제 내 컴퓨터로 돌아와 PuTTY를 이용한 접속을 해보겠습니다.
접속을 위해서 IP/PW가 아닌 1-2에서 저장한 Key를 이용합니다. 이 저장한 파일을 바로 사용하지는 못하고, private key로 변환이 필요합니다.
그래서 PuTTY Key Generator를 실행하여, 저장한 **my-key.pem** 파일을 Load 합니다.

1-8. .pem 파일을 이용한 Key 생성(2)



my-key.pem 파일을 Load 한 후, [Save private key]버튼을 누르면 .ppk 형태로 저장이 가능합니다.
이름을 **my-key.ppk**로 하여 파일을 저장합니다.

1-9. Putty 세션 설정(1)



PuTTY를 실행하고, Configuration 정보에서

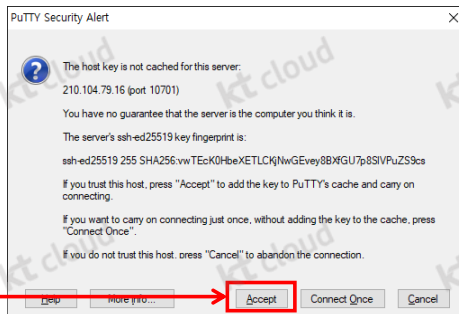
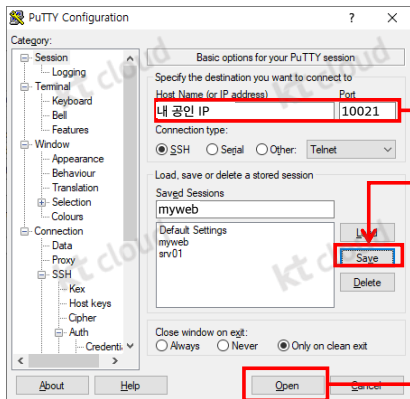
[Connection]-[SSH]-[Auth]-[Credentials] 선택

Private key file for authentication 의 [Browse] 클릭하여

생성한 **my-key.ppk** 선택

다시 PuTTY를 실행하여 환경 설정 정보에서 저장한 **my-key.ppk** 파일을 설정합니다.

1-9. Putty 세션 설정(2)



Key 설정이 되었으면, [Session]을 클릭하고 다음의 정보 입력

- Host Name : 내 공인IP
- Port : 10021

이후에 다시 접속할 수 있으므로, [Save]버튼을 눌러서 Session 정보 저장 후, [Open]클릭

이제 접속할 kt cloud 공인 IP 주소와 공인 Port 를 입력합니다.
이후에 다시 접속할 수 있으므로 이 세션 정보는 [Save]를 눌러 저장합니다.
그런 다음, 이제 서버로 접속하기 위해 [Open]을 클릭합니다.

1-10. web01에 SSH 접속

```
centos@web01~$ login as: centos
Authenticating with public key "imported-openssh-key"
[centos@web01. ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.25.0.174 netmask 255.255.255.0 broadcast 172.25.0.255
    inet6 fe80::f816:3eff:fe74:bd5b prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:74:bd:5b txqueuelen 1000 (Ethernet)
    RX packets 689 bytes 58263 (56.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 612 bytes 58761 (57.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[centos@web01. ~]$ sudo -i
[root@web01. ~]#
```

login as에 centos 입력

ifconfig 명령어를 입력하여

현재 접속한 web01의 사설 IP 주소를 확인

web01을 생성시에 OS를 **CentOS**로 선택했으므로, login as: 에 계정명을 **centos**로 입력합니다.

(참고로, D1의 경우 root로의 로그인도 불가능합니다. 접속 후 sudo 명령어로 root 권한을 받아야 합니다.)

접속을 한 후, 창의 타이틀에 web01 이라고 나오지만, 명령어로도 접속한 서버를 확인 할 수 있습니다.

ifconfig 명령어를 입력하고, eth0의 사설 IP 주소와 콘솔의 web01 정보에서의 사설 IP 주소가 일치함을 확인합니다.

그런 다음 웹서버의 설치는 root 권한이 필요하므로, **sudo -i** 명령어를 입력합니다.

1-11. web01의 웹서버 구성

웹서버 설치 과정

root 권한 획득	sudo -i
httpd 설치	yum install -y httpd
httpd 서비스 시작	systemctl start httpd
httpd 서비스 자동 시작 설정	systemctl enable httpd

```
root@web01~  
Redirecting to /bin/systemctl start httpd.service  
[root@web01 ~]# systemctl start httpd  
[root@web01 ~]# systemctl enable httpd  
[root@web01 ~]#
```

Index.html 작성

```
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

Copyright© 2023 kt cloud corp. All rights reserved.

21

이제 다음의 단계로 웹 서버를 설치합니다.

1. httpd 설치

- 명령어 : **yum install httpd -y**

2. httpd 서비스 시작

- 명령어 : **systemctl start httpd**

3. httpd 서비스 자동 시작 설정하기

- 명령어 : **systemctl enable httpd**

(서버를 다시 시작할 때마다 httpd 서비스를 수동으로 시작할 필요 없이 자동으로 시작하도록 설정합니다.)

설치가 끝나면 index.html 을 작성합니다.

- 명령어 : **echo "<h1>Hello World from \$(hostname -f)</h1>" > /var/www/html/index.html**

1-12. web01 서버 접속설정(80 포트)

web01 서버 접속을 설정합니다.

서버	사실Port	공인IP	공인Port	프로토콜
<input type="checkbox"/> \ web01	22	내 공인 IP	10021	TCP
<input type="checkbox"/> \ web01	80	내 공인 IP	10022	TCP

웹 페이지를 보기 위해
외부에서 접속할 공인 IP 선택 및 공인 Port 지정
(80번 포트에 대해 10022로 지정. 실습1 개요 참조)

web01

80

내 공인 IP

10022

TCP

☐ 포트범위로 설정

+ 추가

Copyright© 2023 kt cloud corp. All rights reserved.

22

이제 설치한 웹 서비스를 외부에서 접근하도록 설정합니다.
먼저 [접속 설정]에서 **web01** 서버의 **80** 사실포트에 대해 **10022** 공인포트로
연결을 [추가]합니다.

1-13. Web 접속을 위한 방화벽 정책 추가

삭제 이동

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명	
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	- -	●	-	☑
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_ 내 공인 IP _10021...	- -	●	-	☑
<input type="checkbox"/>	3	allow	external	all	TCP	DMZ_Sub	PF_ 내 공인 IP _10022...	- -	●	-	☑

웹 페이지 접속을 위해 방화벽 설정을 1개를 추가
외부에서 web01의 80번 포트에 대한 허용 : 외부에서의 접근이므로
external → DMZ/PF_공인IP_10022_TCP

+ 추가

Allow external 0.0.0.0 TCP DMZ_Sub PF_ 내 공인 IP _10.. Start End

Copyright© 2023 kt cloud corp. All rights reserved. 23

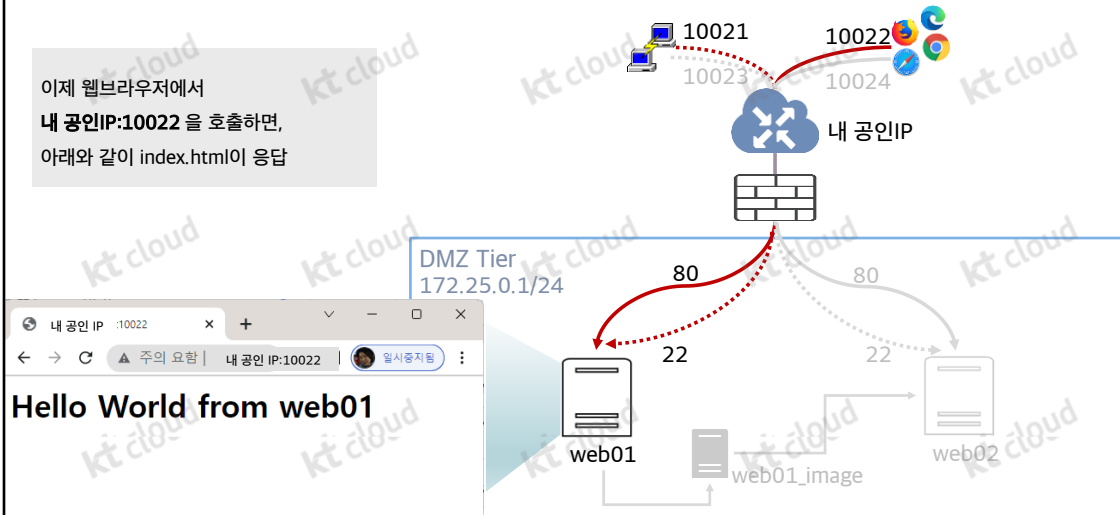
외부에서 접속하기 위해 방화벽 정책도 추가합니다.

외부에서 **10022**포트(사설 포트 **80**)로의 접근을 허용하는 정책을 추가합니다.

- Source : **external, All CIDR**
- Destination : **DMZ tier/PF_공인IP_10022_TCP**

1-14. web01 호출하기

이제 웹브라우저에서
내 공인IP:10022 을 호출하면,
아래와 같이 index.html이 응답



이제 공인 IP:10022을 웹 브라우저에서 호출하면 **index.html**의 내용이 뜨는 것을 확인할 수 있습니다.
오른쪽 그림과 같이 우리는 **web01**의 설정을 완료했습니다.

1-15. 서버 이미지 생성하기(1)

Server

가상 서버를 관리합니다.

서버 생성

정지

재시작

강제재시작

삭제

접속설정

...

모든 위치 · 모든 상태 >

이름	상태	위치	운영체제	사양
<input checked="" type="checkbox"/> web01	●...	DX-M1	centos-7.9-64bit	1vcore 1GB

web01 서버를 정지합니다.

서버를 정지한 후에도 정지요금이 별도로 부과됩니다.
요금부과를 원하지 않으실 경우, 서버정지 후 삭제해 주시기 바랍니다.
(단, GPU Server의 경우, 정지 시에도 사용 요금이 부과됩니다.)

* 정지요금: 표준Memory - 12,000원/월 (400원/일(월요금제), 17원/시간(시간요금제))
High Memory - 36,000원/월 (1,200원/일(월요금제), 50원/시간(시간요금제))

- 정지요금은 Server(VM)에만 한정되어 제공되며, 자세한 내용은 server 요금페이지를 참고해 주시기 바랍니다.
- 서버 정지 시에는 VM별로 제공되는 네트워크 무료 트래픽이 정지 기간 만큼 조정되어 제공됩니다.
- 상품변경을 위해 서버를 정지하는 경우, 서버 정지 전 반드시 변경 가능 사양 정보 확인 후 진행해 주시기 바랍니다.

취소 **정지하기**

서버 이미지를 생성하기 위해서는
구동중인 web01 서버를 일단 정지해야 함
web01 서버 선택-[정지]클릭

Copyright© 2023 kt cloud corp. All rights reserved.

web02 서버는 서버의 이미지를 이용해서 생성할 것입니다.
그러기 위해 지금 생성한 **web01**의 서버에서 이미지를 만들어야 하는데, 서버 이미지는 서버가 구동 중에는 생성이 불가능합니다.
일단 **web01** 서버를 정지시킵니다.

1-15. 서버 이미지 생성하기(2)

The screenshot shows the '서버 생성' (Server Creation) page. A red arrow points to the '서버 생성' button. Another red arrow points to the 'web01' server in the list, which has a red dot indicating it is stopped. A third red arrow points to the '이미지 생성' (Create Image) option in the dropdown menu. A fourth red arrow points to the '이미지 생성' button in the 'srv01' image creation window. The image name 'web01-image' is entered in the '이미지 이름' field.

서버 상태가 중지(●로 바뀐 것을 확인하고 [...]-[이미지 생성] 클릭

서버 이미지 생성 창에서 이미지 이름을 **web01-image**로 지정, [이미지 생성]클릭

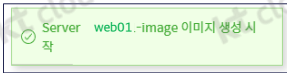
서버가 중단되어 상태가 변경되면 [이미지 생성] 메뉴가 활성화됩니다.
web01 서버를 선택하고, [...]를 클릭하여 [이미지 생성]을 클릭합니다.

이미지 생성창에서 이미지 이름을 지정합니다.

- 이미지 이름 : **web01-image**

이름을 입력하고, [이미지 생성]을 클릭합니다.

1-15. 서버 이미지 생성하기(3)



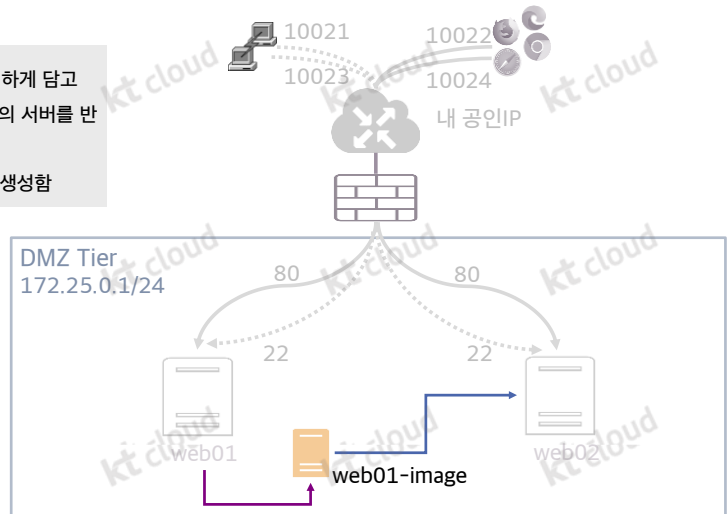
[이미지 생성]클릭 후 우측 상단에 이미지 생성 시작 알림이 뜨고 조금 기다리면 아래와 같이 생성된 이미지 확인 가능

Server Image						
가상 서버의 이미지를 관리합니다.						
서버 생성	삭제	공유 수락	...	모든 위치 · 모두 >	🔍	🔄
이름 ↓	운영체제	위치	상태	공유설정	볼륨 크기	생성일시
<input type="checkbox"/> web01-image	centos-7.9-64bit	DX-M1	● 사용	공유가능	1.30GB	03/21/2023 16:39:23

서버 이미지 생성이 완료되면 위와 같이 목록에 보여지고 상태도 **사용**으로 바뀝니다.

1-16. web01-image 생성과 활용

web01-image는 **web01**의 구성과 파일을 동일하게 담고 있는 형상으로, 이 이미지를 활용해서 같은 모양의 서버를 반복해서 생성할 수 있음
이 이미지를 활용하여 이후 단계에서 **web02**를 생성함



Copyright© 2023 kt cloud corp. All rights reserved.

28

지금의 과정은 그림과 같이 **web01**의 형상을 **web01-image** 라는 이미지 파일로 만든 것입니다.
이제 이 이미지 파일을 이용해서 **web02**를 만들어 보겠습니다.

1-17. 이미지를 이용한 web02 서버 생성하기(1)

Server Image

가상 서버의 이미지를 관리합니다.

서버 생성 삭제 공유 수락 ... 모든 위치 - 모두 >

이름 ↓	운영체제	위치	상태	공유설정	볼륨 크기	생성일시
<input checked="" type="checkbox"/> web01-image	centos-7.9-64bit	DX-M1	● 사용	공유가능	1.30GB	03/21/2023 16:39:23

web01과는 다르게 이미지로 생성하므로
[Server]-[Server Image] 메뉴를 선택하고,
web01-image 체크하여 [Server 생성]버튼 클릭

만들어진 image는 [Server]-[Server image]에서도 확인이 가능합니다.
여기서 **web01-image**를 선택하고 [서버 생성]을 클릭합니다.

1-17. 이미지를 이용한 web02 서버 생성하기(2)

서버 생성

위치: DX-M1

Tier: ① DMZ_Sub

서버 이름: ② web02

서버 용도: WEB AP DB ETC

서버 타입: HDD SSD

루트 볼륨 크기: 50GB 100GB

Key Pair: ③ my-key

Server Image: CPU: GPU: AMD

srv01-image(centos-7.9-64bit)

1vCore 1GB
1 vCore 2GB
2 vCore 2GB

이미지로 생성하기 때문에 OS는 이미지의 대상 서버에서 지정한 대로 centos7.9로 고정됨

실습1 개요 페이지를 참조하여 입력 값을 확인

① Tier : web01과 동일한 Tier인 **DMZ** 로 설정

② 서버 이름 : 서버 이름은 고유해야 하며, **web02**로 지정

③ Key Pair : web01과 동일한 키인 **my-key** 를 선택

Copyright© 2023 kt cloud corp. All rights reserved.

30

web02 서버를 만듭니다.
서버 정보는 다음과 같습니다.

- Tier : **DMZ**
- 서버 이름 : **web02**
- Key Pair : **my-key**

대부분의 항목이 일반 서버 생성 항목과 흡사합니다만, OS 부분은 이미 이미지에 만들어져 있는 부분이므로 **web01**과 같은 **centos 7.9**가 됩니다.

1-17. 이미지를 이용한 web02 서버 생성하기(3)

Server

가상 서버를 관리합니다.

서버 생성

시작

정지

재시작

강제재시작

삭제

접속설정

...

모든 위치 · 모든 상태 >

🔍 📄 ↺

<input type="checkbox"/>	이름 ↓	상태	위치	운영체제	사양	상품	볼륨타입	사설IP	추가사설IP	생성일시
<input type="checkbox"/>	web01	● 사용	DX-M1	centos-7.9-64bit	1vcore 1GB	표준	HDD	172.25.0.174	-	03/21/2023 15:0...
<input type="checkbox"/>	web02	● 사용	DX-M1	srv01-image	1vcore 1GB	표준	HDD	172.25.0.68	-	03/21/2023 16:5...

- [Server]-[Server] 메뉴를 선택하여 이제 생성된 서버가 2개 임을 알 수 있음.
- 같은 서버이지만, **web02**는 이미지를 통해 생성한 것이므로 운영체제가 다르게 표시됨

Copyright© 2023 kt cloud corp. All rights reserved.

31

이제 두 개의 서버가 생겼습니다. 목록에서 보여지는 두 서버는 차이가 없지만 운영체제 부분이 다를 수 있습니다.

1-18. web02 접속 설정

서버 생성 시작 중지 삭제 강제재시작 접속설정 ... 모든 위치 · 모든 상태

이름 ↓	상태	위치	운영체제	사양	상품	볼륨타입	사설IP	추가사설IP	생성일시
<input type="checkbox"/> web01	● 사용	DX-M1	centos-7.9-64bit	1vcore 1GB	표준	HDD	172.25.0.174	-	03/21/2023 15:0...
<input checked="" type="checkbox"/> web02	● 사용	DX-M1	srv01-image	1vcore 1GB	표준	HDD	172.25.0.68	-	03/21/2023 16:5...

srv02 서버 접속을 설정합니다.

서버	사설Port	공인IP	공인Port	프로토콜
<input type="checkbox"/> web02	80	내 공인 IP	10704	TCP
<input type="checkbox"/> web02	22	내 공인 IP	10703	TCP

web02

80 210.104.79.16 10704 TCP

web01과 동일한 서비스 및 접속을 할 것이므로, 두 개의 접속 설정을 추가 (실습1 개요 참조)

- 사설 IP 22 포트 - 공인IP 10023포트
- 사설 IP 80 포트 - 공인IP 10024포트

+ 추가

Copyright© 2023 kt cloud corp. All rights reserved.

이제 **web02** 서버도 **web01**과 동일하게 접근이 가능하도록 설정합니다.
마찬가지로 SSH 접근과 web 접근을 할 것이므로, 두 개의 접속 설정을 합니다.

- 사설 IP 22 포트 - 공인IP 10023포트
- 사설 IP 80 포트 - 공인IP 10024포트

1-19. web02 방화벽 설정

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명	
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	- - -	●	-	☑
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10021_...	- - -	●	☑
<input type="checkbox"/>	3	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10022_...	- - -	●	☑
<input type="checkbox"/>	4	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10023_...	- - -	●	☑

+ 추가

Allow ▾ external ▾ 0.0.0.0/0 TCP ▾ DMZ_Sub ▾ PF_210.104.79.16_107_ ▾ Start ▾ End

방화벽 설정은 외부에서 web02의 22번 포트에 대한 허용 정책을 추가

: 외부에서의 접근이므로 **external → DMZ/PF_공인IP_10023_TCP**

* web01에서 이미 설정한 Apache 설치를 위한 사이트 접속/파일전송용 방화벽 정책은 web02에서 공통적으로 적용됨

방화벽 설정도 추가합니다.

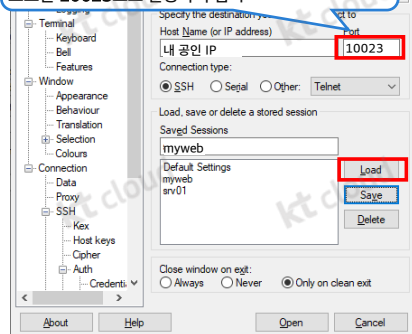
같은 DMZ tier 내에 있으므로 방화벽을 같이 쓰게 됩니다. 따라서 **web02**도 기존에 설정해 둔 방화벽 설정의 적용을 받게 됩니다.

여기에 **web02**의 SSH 접근이 가능하도록 다음의 설정을 추가합니다.

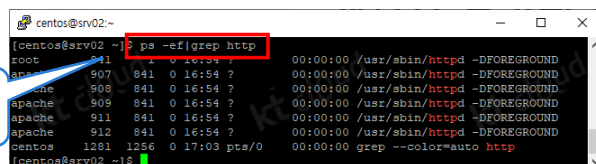
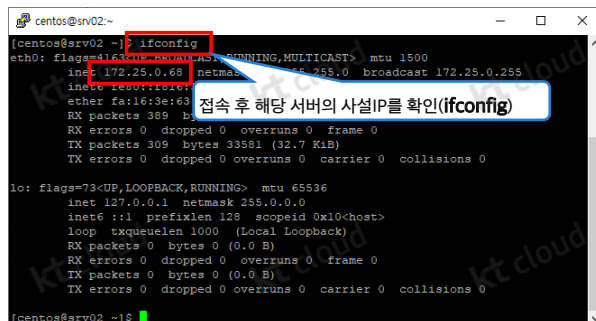
- **Allow, external/all → DMZ/PF_공인IP_10023_TCP**

1-20. web02에 SSH 접속

Putty에 저장된 web01의 Session 설정을 [Load]하여
포트만 10023으로 변경하여 접속



서버 이미지에서 이미 설치되어 web02에서
구동되는 웹서버 확인 (ps -ef|grep http)



다시 내 컴퓨터의 PuTTY를 실행시켜 접속합니다.
설정은 동일하지만 Port가 10023임을 유의합니다.
같은 방법으로 centos로 로그인하고, web02 임을 확인합니다.
주의할 점은 이 서버는 이미지를 통해서 만들어졌으므로, 기존에 web01에 설
치되고 실행설정 되어 있는 webserver가 구동되고 있음을 알 수 있습니다.
확인을 위해 다음의 명령어를 실행합니다.

ps -ef|grep http

1-21. web02의 웹 페이지 수정하기

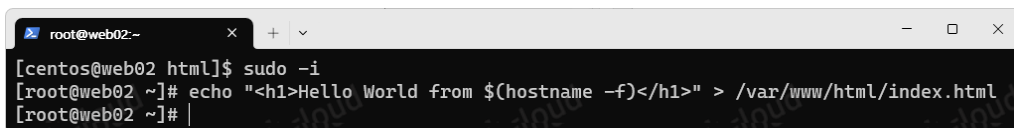
웹서버 설치 과정

root 권한 획득

sudo -i

Index.html 작성

```
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```



```
root@web02:~  
[centos@web02 html]$ sudo -i  
[root@web02 ~]# echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html  
[root@web02 ~]#
```

Copyright© 2023 kt cloud corp. All rights reserved.

35

index.html도 마찬가지로 존재하지만, 이후 실습에서 두 서버 간의 구분을 위해 텍스트를 약간 수정하겠습니다.

echo "<h1>Hello World from \$(hostname -f)</h1>" > /var/www/html/index.html

1-22. Web 접속을 위한 방화벽 정책 추가하기

방화벽을 설정합니다. (IP or URL)

※방화벽 설정 가이드 더보기

삭제

이동

X

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Dest내 공인 IP	Destination Port	위험도	설명	
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	- - -	●	-	☑
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10021....	●	-	☑
<input type="checkbox"/>	3	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10022....	●	-	☑
<input type="checkbox"/>	4	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10023....	●	-	☑
<input type="checkbox"/>	5	allow	external	all	TCP	DMZ_Sub	PF_내 공인 IP	_10024....	●	-	☑

web02 웹 페이지 접속을 위해 방화벽 설정을 1개를 추가
외부에서 web02의 80번 포트에 대한 허용 : 외부에서의 접근이므로
external → DMZ/PF_공인IP_10024_TCP

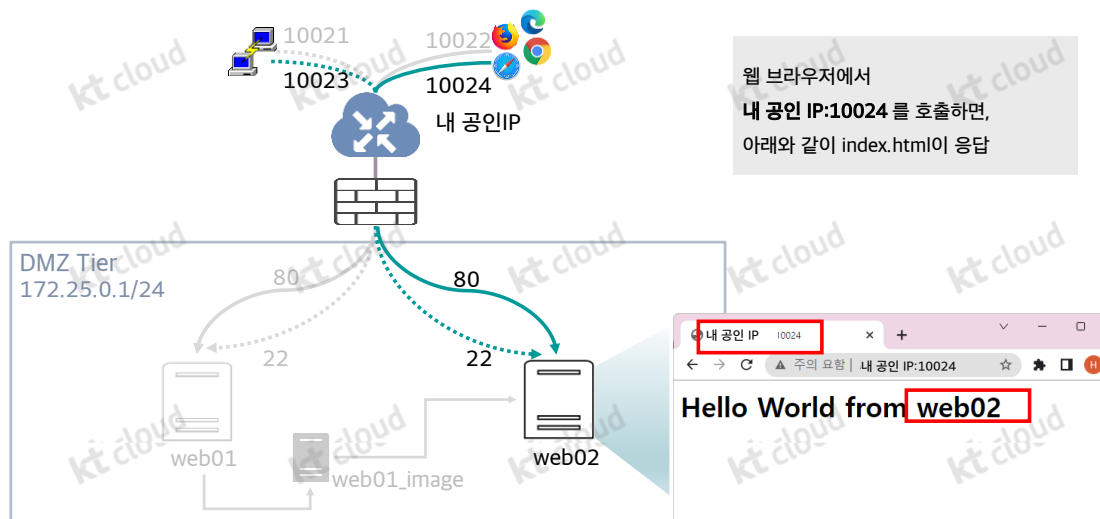
Copyright© 2023 kt cloud corp. All rights reserved.

36

이제 다시 콘솔의 방화벽 설정에서 web02의 웹 포트도 허용 정책을 추가합니다.

Allow, external/all → DMZ/PF_공인IP_10024_TCP

1-23. web02 호출하기



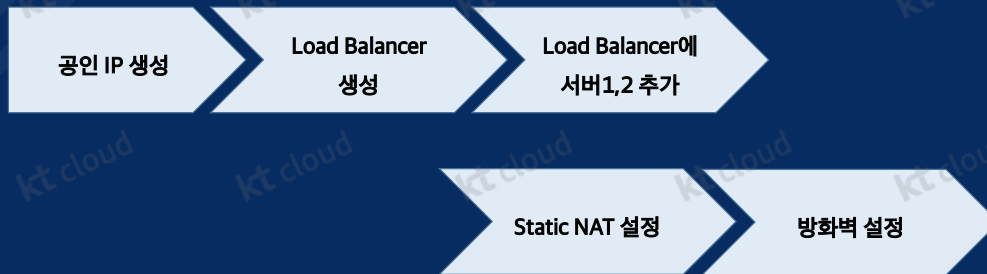
Copyright© 2023 kt cloud corp. All rights reserved.

37

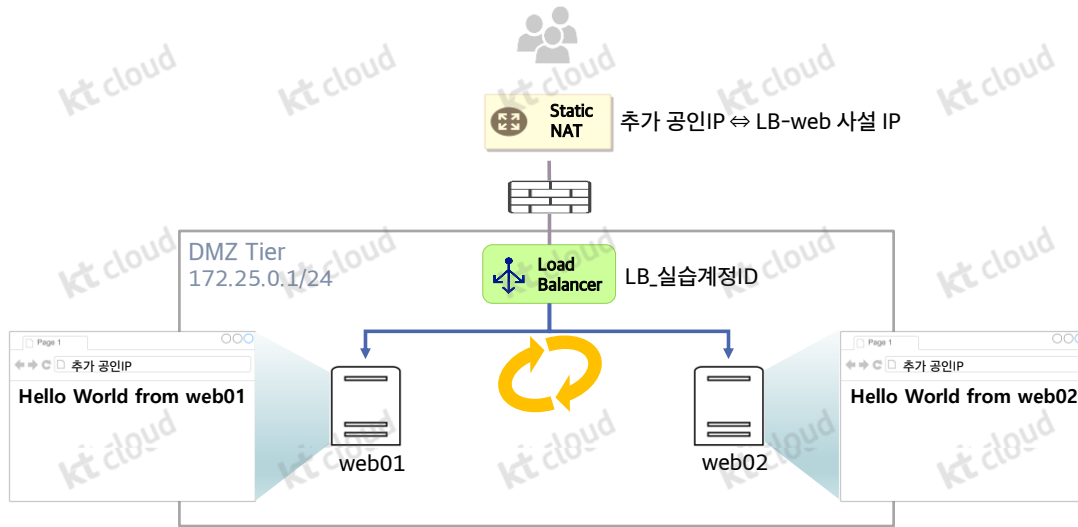
이제는 웹 브라우저에서 web02를 호출해 보겠습니다.
웹 브라우저에서 **공인 IP:10024** 를 호출하여
화면과 같은 문구(02)가 나오는지 확인합니다.

지금까지 각각의 웹 서비스를 하는 두 개의 서버 생성을 완료했습니다.

실습 2. Load Balancer 구성



실습 2. 개요



이제는 각각의 두 서버를 하나의 서비스처럼 관리하면서 요청에 대한 부하를 분산시키고, 하나의 서버에 문제가 발생하더라도 서비스가 지속될 수 있도록 서버의 앞에 로드밸런서를 위치 시킵니다.
그리고 이 로드밸런서를 위한 별도의 공인 IP를 생성한 다음, 그 IP와 생성한 로드밸런서를 1:1로 매핑하는 StaticNAT 설정을 해보겠습니다.

2-1. 추가 공인 IP 생성(1)

Networking
가상 서버의 접속 설정과 공인IP를 관리합니다.

IP 생성 | 접속설정 | 방화벽 | Static NAT | Static Route | 삭제 | ... | 모든 위치 · 모두 > | 🔍 | 📄 | ↻

<input type="checkbox"/> 공인IP ↓	위치	타입	Static NAT	TYPE
<input checked="" type="checkbox"/> 내 공인 IP	DX-M1	기본	-	SRCNAT

처음 계정이 생성되면 1개의 공인 IP를 가지고 있음

필요시 공인 IP를 추가로 사용가능
[Server]-[Networking] 메뉴 선택,
[IP 생성] 클릭

공인IP를 생성합니다.

위치: DX-M1

월 요금제 | 시간 요금제
7원/시간

취소 | **생성하기**

공인 IP는 내가 지정할 수 없고 임의의 IP를 할당받으므로, 추가 설정없이 [생성하기]를 클릭

Copyright© 2023 kt cloud corp. All rights reserved.

제일 먼저 추가 공인 IP를 생성합니다.

계정에는 기본적으로 한 개의 공인 IP가 있는데, 필요시 추가적으로 공인 IP를 여러 개 생성할 수 있습니다.

[Server]-[Networking] 에서 [IP 생성]을 클릭하여, [생성하기]를 클릭합니다.

참고로 공인 IP는 가용한 IP 중에서 하나를 할당 받으므로 사용자가 IP를 지정할 수 없습니다.

2-1. 추가 공인 IP 생성(2)

IP 생성	접속설정	방화벽	Static NAT	Static Route	삭제	...	모든 위치 · 모두 >	Q	XII	↺
<input type="checkbox"/>	공인IP ↓	위치	타입	Static NAT	TYPE					
<input type="checkbox"/>	내 공인 IP	DX-M1	기본	-	SRCNAT					
<input type="checkbox"/>	추가 공인 IP	DX-M1	추가	-	ASSOCIATE					

추가된 공인 IP는 타입이 **추가** 라고 표시되며, Type 부분도 **ASSOCIATE** 라고 되어 있음

기본 공인 IP는 TYPE이 **SRCNAT** 라고 나오지만, 추가로 생성한 공인 IP는 **ASSOCIATE**라고 나옵니다.
타입도 **기본**과 **추가**로 구분됩니다.

2-2. 로드밸런서 생성(1)

Load Balancer
로드밸런서를 관리합니다.

로드밸런서 생성 변경 삭제 인증서 관리 인증서 등록 ... 모든 위치 >

이름	위치	옵션	타입	IP	Port	상태
----	----	----	----	----	------	----

[Load Balancer]-[Load Balancer]를 선택하면 로드밸런서 관리 화면으로 바뀌고, 상단 버튼 중 [로드밸런서 생성]을 클릭

Copyright© 2023 kt cloud corp. All rights reserved. 42

이제 로드밸런서를 만들어 봅니다.

[Load Balancer]-[Load Balancer] 메뉴를 선택하고, [로드밸런서 생성]을 클릭합니다.

2-2. 로드밸런서 생성(2)

로드밸런서 생성

로드밸런서 생성 폼의 설정값:

- 위치: DX-M1
- Tier: ① DMZ_Sub
- 로드밸런서 이름: ② LB_실습계정ID
- 서비스 IP / PORT: ③ 신규할당 IP, 80
- 타입: HTTP, TCP, HTTPS(bridge), HTTPS, FTP
- 옵션: ④ Round Robin, Src IP Hash, Least Response, Least Connection, Src IP Hash+Port
- Health Check Protocol: TCP, HTTP, HTTPS

로드밸런서 설정값

- Tier : 로드밸런서는 [실습 2 개요]의 그림과 같이 특정 Tier 내부에 존재하므로, 로드밸런서가 위치할 Tier를 지정. 여기서는 **DMZ**
- 로드밸런서 이름 : **LB_실습계정ID**로 설정
- 서비스 IP/Port : 사실IP를 **신규로 할당** 받음. LB의 IP는 4번째 옥텟이 181~199중 하나로 지정. 웹 서비스에 대한 로드 밸런싱으로 **80포트** 지정
- 옵션 : 로드 밸런싱 알고리즘에 대한 선택으로, **Round Robin**(무조건 한번씩 순환)으로 설정

여기서의 Health Check란 로드밸런서에 연결된 서버들의 상태를 주기적으로 확인하는 것을 의미하며, 이 확인 작업시에 사용할 방법을 지정하는 것

Copyright© 2023 kt cloud corp. All rights reserved.

43

생성할 로드밸런서의 상세 사항을 입력합니다.
이 실습에서의 로드밸런서 설정값은 다음과 같습니다.

- Tier : **DMZ**
- 로드밸런서 이름 : **LB_실습계정ID**
- 서비스 IP/Port : **신규 할당 IP, 80**
- 옵션 : **Round Robin**

2-2. 로드밸런서 생성(3)

적용 서버

서버	사실 Port	타입2
<input type="checkbox"/> web02 (web02...)	80	HTTP
<input type="checkbox"/> web01 (web01...)	80	HTTP

web01 (web01...)

로드밸런서 적용 서버

- 로드밸런서는 여러 서버들의 앞 단에서 요청을 받아 속한 서버들에게 전달하는 것으로 이렇게 요청을 전달할 서버 지정
- 어떤 서비스(HTTP/HTTPS)를 하는지, 어떤 포트로 요청을 받을지 등을 선택
- 여기서는 실습 1에서 생성한 두 서버를 추가
 - web01/80 port/HTTP
 - web02/80 port/HTTP

Copyright© 2023 kt cloud corp. All rights reserved.

44

그 아래 로드밸런서가 요청을 전달할 서버를 추가합니다.
실습 1에서 만든 두개의 서버를 추가해 보겠습니다.

- **web01/80 port/HTTP**
- **web02/80 port/HTTP**

2-2. 로드밸런서 생성(4)

Load Balancer						
로드밸런서를 관리합니다.						
<div>로드밸런서 생성 변경 삭제 인증서 관리 인증서 등록 ... 모든 위치 ></div>						
이름	위치	알고리즘	타입	IP	Port	상태
<input type="checkbox"/> LB_실습계정ID	DX-M1	Round robin	HTTP	172.25.0.181	80	● UP

로드밸런서 생성을 하게 되면 우측 상단에 로드밸런서 생성에 관한 알림이 뜨고,
잠시 뒤 우리가 생성한 **LB_실습계정ID**가 ●UP 상태로 바뀜
LB_실습계정ID는 임의로 할당받은 **172.25.0.181**의 사설 IP를 가짐

Copyright© 2023 kt cloud corp. All rights reserved.

45

로드밸런서 **LB_실습계정ID** 생성이 완료되면 UP 상태로 목록에 만들어집니다.
여기서의 IP는 사설 IP 이며 아직 외부에서 접근이 불가능합니다.

2-3. 로드밸런서 확인

로드밸런서 생성						
변경		삭제	인증서 관리	인증서 등록	모든 위치 >	
이름	위치	알고리즘	상세 정보	Port	상태	
<input checked="" type="checkbox"/> LB_실습계정ID	DX-M1	Round robin	적용 서버	172.25.0.181	80	UP
정책제 신청						

변경							
서버	사실 IP	사실 Port	Throughput	Server Connections	TTFB	Request	상태
web02 (1509101...)	172.25.0.68	80	0 (Mbps)	9	0	0	UP
web01 (b3a0d1c...)	172.25.0.174	80	0 (Mbps)	9	0	0	UP

LB_실습계정ID를 선택 후, [...]클릭하여 [적용 서버]를 선택하면 등록된 서버 목록을 확인 가능
여기서는 실습 1에서 생성한 두 서버 **web01**, **web02**가 있어야 함

만들어진 이후에도 로드밸런서에서 어느 서버에 요청을 전달하는지 확인이 가능합니다.

로드밸런서를 선택한 후 [...]에서 [적용 서버]를 클릭하면 추가된 서버가 두 개임을 알 수 있습니다.

2-4. 로드밸런서의 위치와 연결 서버



이제까지의 설정은 두 서버의 앞에 로드밸런서 **LB_실습계정ID**를 두고, 서버를 **LB_실습계정ID**와 연결시켰습니다. 이 **LB_실습계정ID**는 두 서버를 Round Robin 형태로 번갈아가며 요청을 전달할 것입니다.

그림에서 보다시피 이 **LB_실습계정ID**는 DMZ 내부에 존재하며 아직 외부에서 접근이 불가능한 상태입니다.

2-5. Static NAT 설정(1)

Networking
가상 서버의 접속 설정과 공인IP를 관리합니다.

외부에서의 접근을 위해 2-1에서 생성한 추가 공인 IP를 로드밸런서 LB_실습계정ID와 연결하기 위해 [Static NAT]를 클릭하여 설정

공인IP 관리

공인IP	위치	타입	Static NAT	TYPE
내 공인 IP	DX-M1	기본	-	SRCNAT
<input checked="" type="checkbox"/> 추가 공인 IP	DX-M1	추가		ASSOCIATE

추가 공인 IP 공인IP를 Static NAT으로 설정합니다.

이 공인 IP는 다른 사설 IP를 가지는 서비스와 공유하지 않고, LB_실습계정ID 전용으로 사용하도록 매핑하고 [추가] 클릭

로드밸런서 LB_실습계정ID

StaticNat설정을 하시겠습니까.

취소 **설정하기**

Copyright© 2023 kt cloud corp. All rights reserved.

이제 외부에서 접근할 수 있도록 공인 IP와 매핑을 합니다.

이따 실습 1과는 다르게 새롭게 추가한 공인 IP와 이 **LB_실습계정ID**를 연결 할 것입니다.

그리고 **LB_실습계정ID**가 추가IP는 전용으로 사용하게 되므로 별도의 포트 포워딩과 같은 설정은 없습니다.

이를 위해 추가 IP를 선택하고 [Static NAT]를 설정합니다.

주의할 것은 설정할 때 서버가 아닌 로드밸런서 **LB_실습계정ID**를 추가한다는 점을 유의합니다.

2-5. Static NAT 설정(2)

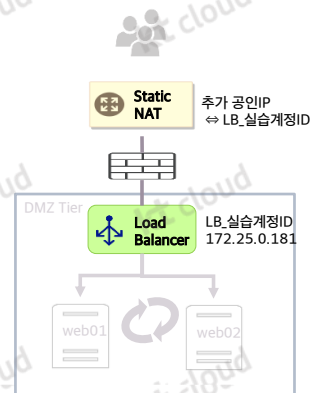
Networking

가상 서버의 접속 설정과 공인IP를 관리합니다.

IP 생성 접속설정 방화벽 Static NAT Static Route 삭제 ... 모든 위치 · 모두 >

<input type="checkbox"/> 공인IP ↓	위치	타입	Static NAT	TYPE
<input type="checkbox"/> 내 공인 IP	DX-M1	기본	-	SRCNAT
<input checked="" type="checkbox"/> 추가 공인 IP	DX-M1	추가	LB_실습계정ID	STATICNAT

연결이 완료되면, 추가 공인 IP의 Static NAT 탭에 매핑된 **LB_실습계정ID**가 표시되고, TYPE 부분도 ASSOCIATE에서 STATICNAT 라고 바뀜



설정이 완료되면 공인 IP 목록에 Static NAT 부분에 로드밸런서 **LB_실습계정 ID**가 보이고, TYPE이 **STATICNAT**로 바뀐 것을 알 수 있습니다. 이제 오른쪽 그림과 같이 외부에서 접근할 수 있도록 공인 IP가 매핑되었습니다.

Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명	
<input type="checkbox"/> 1	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10701_T	--	●	-	
<input type="checkbox"/> 2	allow	DMZ_Sub	all	TCP	external	all	80-80	●	-	
<input type="checkbox"/> 3	allow	DMZ_Sub	all	UDP	external	all	53-53	●	-	
<input type="checkbox"/> 4	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10702_T...	--	●	-	
<input type="checkbox"/> 5	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10703_T...	--	●	-	
<input type="checkbox"/> 6	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10704_T...	--	●	-	

Static NAT는 접속설정(PF)과는 달리 사설 IP와 공인 IP가 1:1로 연결되기 때문에 명명에서 별도의 포트를 명시하거나 프로토콜을 지정하는 것 없이 **SN_공인 IP**로 설정됩니다.

Static NAT에서 추가 공인 IP는 **LB_실습계정ID**와 연결되도록 설정하였으므로, 이 **SN_공인 IP**는 로드밸런서 **LB_실습계정ID**를 지칭하게 됩니다.

2-6. Load Balancer 접속을 위한 방화벽 정책 추가(2)

Firewall 210.104.79.17Firewall
생성 성공

방화벽을 설정합니다. (IP or URL)
※방화벽 설정 가이드 >

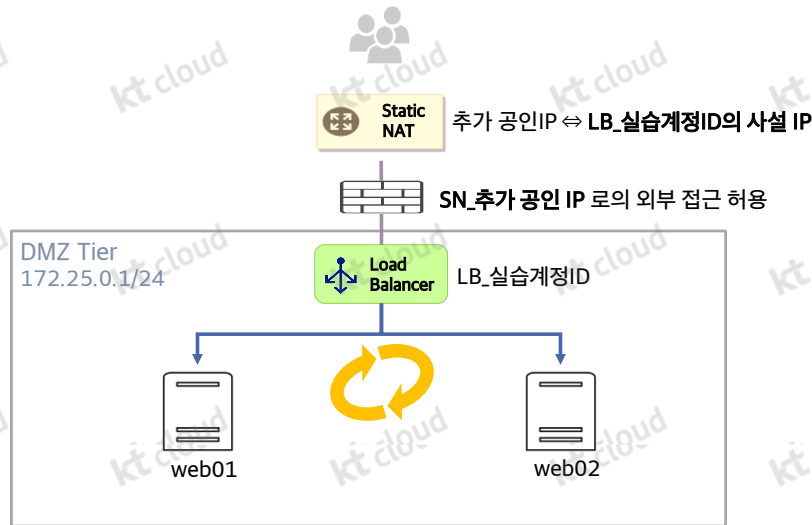
삭제	이동											추가
<input type="checkbox"/>	1	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10701	☑
<input type="checkbox"/>	2	allow	DMZ_Sub	all	TCP	external	all	80-80	☑
<input type="checkbox"/>	3	allow	DMZ_Sub	all	UDP	external	all	53-53	☑
<input type="checkbox"/>	4	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10702	☑
<input type="checkbox"/>	5	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10703	☑
<input type="checkbox"/>	6	allow	external	all	TCP	DMZ_Sub	PF_210.104.79.16_10704	☑
<input type="checkbox"/>	7	allow	external	all	TCP	DMZ_Sub	SN_추가 공인 IP	☑

Copyright© 2023 kt cloud corp. All rights reserved.

51

다음과 같이 Static NAT에 대한 추가적인 방화벽 정책이 추가되었습니다.

실습 2. 요약



Copyright© 2023 kt cloud corp. All rights reserved.

이제 두 서버 앞에 로드밸런서와 Static NAT 설정, 방화벽 설정이 모두 완료되었습니다. 다음 단계에서 이제 호출해보겠습니다.

실습 3. 테스트 및 마무리

Round Robin 확인

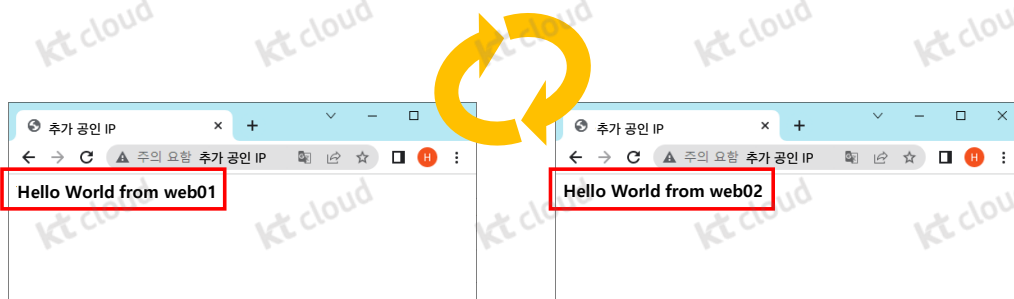
기존 공인IP를
통한 접근 확인

방화벽 정책 삭제

기존 공인IP를
통한 접근 재확인

실습 서비스 삭제

3-1. 로드밸런서의 Round Robin 확인



LB_실습계정ID를 생성할 때 Round Robin 알고리즘으로 두 서버를 호출하도록 설정
→ 브라우저에서 추가 공인 IP를 입력하여 두 페이지가 번갈아 나오는지 확인

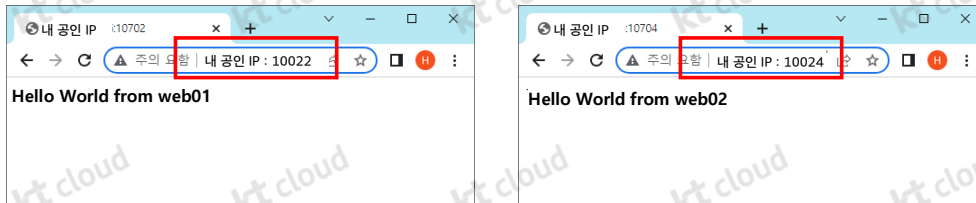
Copyright© 2023 kt cloud corp. All rights reserved.

54

추가 사설 IP를 이용해서 웹 브라우저에서 호출합니다.
reload 할 때마다 페이지가 바뀌는 것을 확인합니다.

이 것은 서버 앞 단의 로드밸런서 **LB_실습계정ID**가 Round Robin 방식으로 **web01**과 **web02**에게 번갈아서 요청을 전달하고 있기 때문입니다.

3-2. 기존 IP를 통한 접속 확인



실습 2에서 **LB_실습계정ID**를 거쳐서 서버를 호출하게 만들었지만,
실습 1에서 했던 것처럼 기존의 공인 IP와 포트로도 접근이 가능함
→ 실제 로드밸런서를 통해서 부하분산과 HA 구성을 위해서는 개별 서버로의 직접적인 접근은 제한해야 함

Copyright© 2023 kt cloud corp. All rights reserved.

55

문제는 로드밸런서로의 접근 뿐 아니라, 기존의 접근(기본 공인아이피를 통한 **10022,10024** 포트 접근)도 가능하다는 것입니다.
로드밸런서를 통해서 서버의 접근을 단일화하여 개별 서버로의 접근은 막도록 하는 것이 보안상으로나 서버의 부하분산에 있어서 고른 분산이 가능하므로, 이 부분에 대해 처리해보겠습니다.

3-3. 방화벽 정책 삭제(1)

Networking
가상 서버의 접속 설정과 공인IP를 관리합니다.

IP 생성 접속 방화벽 Static NAT Static Route 삭제 ... 모든 위치 · 모두 > 🔍 📄 ↺

<input type="checkbox"/>	공인IP ↓	위치	타입	Static NAT	TYPE
<input checked="" type="checkbox"/>	내 공인 IP	DX-M1	기본		SRCNAT
<input type="checkbox"/>	추가 공인 IP	DX-M1	추가	LB, 실습계정ID	STATICNAT

외부에서 내부 서버의 Web 포트(10022, 10024)에 접근하지 못하도록 실습 1에서 사용한 내 공인 IP에서의 Web 포트 허용 정책을 삭제해야 함

→ 다시 [Server]-[Networking]에서 기존 공인 IP를 선택하고 [방화벽] 클릭

Copyright© 2023 kt cloud corp. All rights reserved.

56

방법은 간단합니다. 방화벽에서 해당 부분에 대한 허용 정책을 삭제하기만 하면 더 이상 접근은 불가능합니다.
방화벽은 기본적으로 설정하지 않으면 All Deny 정책이 적용됩니다.

3-3. 방화벽 정책 삭제(2)

삭제		이동											
	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR		Destination Port	위험도	설명		
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all		--	●	-	<input type="checkbox"/>	
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.2/2_10021_...		--	●	-	<input type="checkbox"/>	
<input type="checkbox"/>	3	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.2/2_10022_...		--	●	-	<input type="checkbox"/>	
<input type="checkbox"/>	4	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.2/2_10023_...		--	●	-	<input type="checkbox"/>	
<input type="checkbox"/>	5	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.2/2_10024_...		--	●	-	<input type="checkbox"/>	

10022, 10024에 대한 external 접근을 allow 하는 두 정책을 찾아서 각각 [삭제]클릭

다음과 같이 해당 포트에 대한 접근 정책을 선택하여 [삭제]를 합니다.

3-3. 방화벽 정책 삭제(3)

방화벽정책 삭제 210.104.79.16방화벽 룰 삭제성공

	Priority	Action	Source Network	Source CIDR	Protocol	Destination Network	Destination CIDR	Destination Port	위험도	설명
<input type="checkbox"/>	1	allow	DMZ_Sub	all	ALL	external	all	- - -	●	-
<input type="checkbox"/>	2	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.231_10021_...	- - -	●	-
<input type="checkbox"/>	3	allow	external	all	TCP	DMZ_Sub	PF_210.90.172.231_10023_...	- - -	●	-
<input type="checkbox"/>	5	allow	external	all	TCP	DMZ_Sub	SN_210.104.79.17	- - -	●	-

두 정책이 삭제되고 나머지 방화벽 정책은 유효하게 남겨둬
더 이상 서버에 SSH로 접근할 일이 없으면 10021, 10023 포트와 관련된 정책도 삭제할 수 있으며,
추가 다운로드 설치 작업이 없다면 1번의 정책도 삭제는 가능함

두 정책이 삭제 되었습니다. 이제 다시 확인해보겠습니다.

3-4. 기존 IP를 통한 접속 재확인

The screenshot shows two browser windows. The left window, titled '내 공인 IP', shows a connection error to '210.104.79.16' with the message '사이트에 연결할 수 없음' (Cannot connect to the site) and 'ERR_CONNECTION_TIMED_OUT'. The right window, titled '추가 공인 IP', shows a successful connection to '210.104.79.16' with the message 'Hello World from web01'.

1. 기존 IP를 통해 직접 서버에 연결

사이트에 연결할 수 없음

210.104.79.16에서 응답하는 데 시간이 너무 오래 걸립니다.

다음 방법을 시도해 보세요.

- 연결 확인
- 프록시 및 방화벽 확인
- Windows 네트워크 진단 프로그램 실행

ERR_CONNECTION_TIMED_OUT

2. 추가 공인 IP를 통해 LB-web에 연결

Hello World from web01

방화벽 정책을 수정 후
1. 각각의 서버에 직접 연결과 2. LB_실습계정ID를 통한 연결을 비교

이제는 기본 공인IP로의 접근은 더 이상 불가능하며, 로드밸런서 **LB_실습계정ID**를 통한 접근(추가 공인 IP 접근)만 가능합니다.

3-5. 실습 서비스 삭제

주의

서비스의 삭제는 생성 순서의 역순으로 진행합니다.

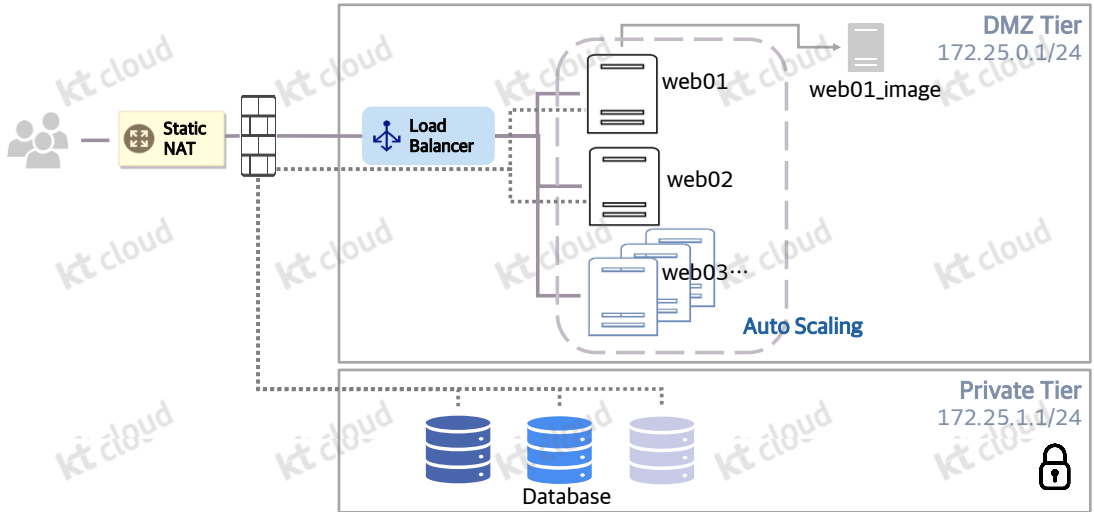
LB 서비스	방화벽 설정 삭제	[Server]-[Networking]-[방화벽]-추가한 정책-각각[삭제]
	Static NAT 해제	[Server]-[Networking]-추가 공인 IP 선택-[Static NAT]클릭
	Load Balancer 삭제	[Load Balancer] - [Load Balancer]- LB_실습계정ID 선택-[삭제]
	추가 공인 IP 삭제	[Server]-[Networking]- 추가 공인 IP 선택-[삭제]
서버	접속 설정 삭제	[Server]-[Networking]- 공인 IP -[접속 설정]- 10021~10024 각각 선택-[삭제]
	서버 이미지 삭제	[Server]-[Server Image]- web01-image 선택-[삭제]
	web02 서버 삭제	[Server]-[Server]- web02 중지- web02 삭제
	web01 서버 삭제	[Server]-[Server]- web01 중지- web01 삭제
SSH Key Pair	my-key 삭제	[Server]-[SSH Key Pair]- my-key 선택-[삭제]

Copyright© 2023 kt cloud corp. All rights reserved.

60

실습이 끝났습니다. 서비스의 삭제를 할 때는 생성한 역순으로 삭제하는 것을 권장 드립니다.
위 표의 위에서 아래 순으로 하나씩 삭제하시면 되겠습니다.
수고하셨습니다.

운영 환경에서의 구성 - 2 Tier 구성



Copyright© 2023 kt cloud corp. All rights reserved.

Appendix

A. PowerShell로 SSH 접속하기

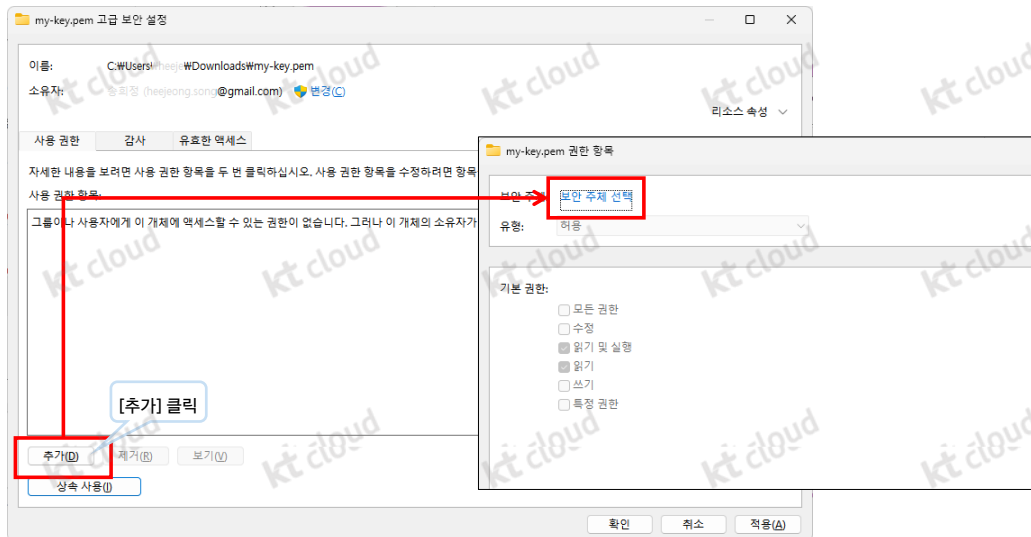
B. Mac 에서 SSH 접속하기

다운로드한 .pem 파일의 [속성] 선택

A-2. pem 고급 보안 설정



A-2. pem 고급 보안 설정



Copyright© 2023 kt cloud corp. All rights reserved.

65

A-3. 사용하는 윈도우 계정의 권한 추가

사용자 또는 그룹 선택

개체 유형을 선택하십시오(S).

사용자, 그룹, 또는 기본 제공 보안 주제

개체 유형(O)...

찾을 위치를 선택하십시오(E).

BOOK-0Q0RQCQS2I

위치(L)...

선택할 개체 이름 입력하십시오(예제)(E).

이름 확인(O)

그룹(S)...

확인

my-key.pem 권한 항목

보안 주제: my-key.pem (ktcloudong.song@gmail.com)

보안 주제 선택

유형: 허용

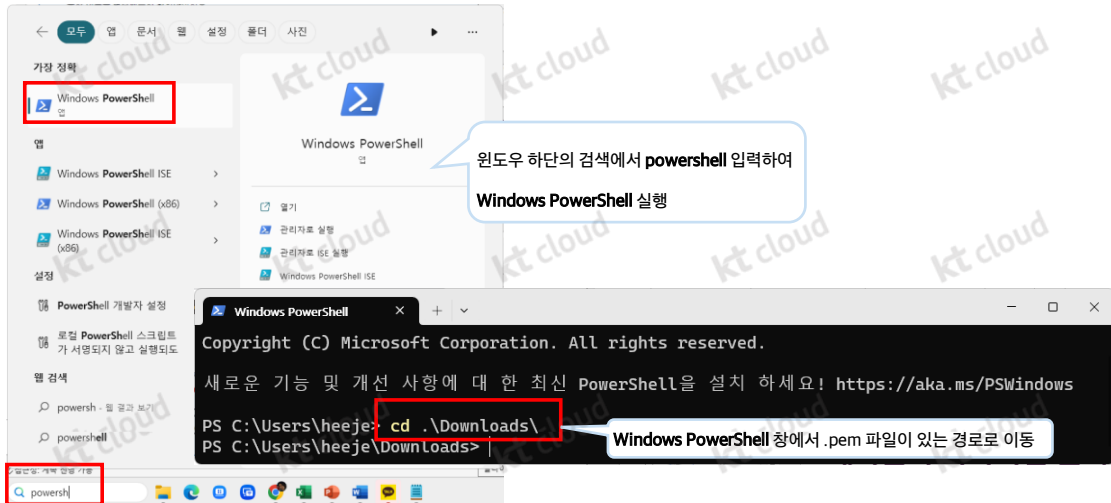
기본 권한:

- ☐ 모든 권한
- ☐ 수정
- ☒ 읽기 및 실행
- ☒ 읽기
- ☐ 쓰기
- ☐ 특정 권한

읽기 및 실행과 읽기에 체크 후 [확인] 클릭

현재 사용하는 윈도우 계정 입력 후
[이름확인] 클릭 후
[확인] 클릭

A-4. Windows PowerShell 실행



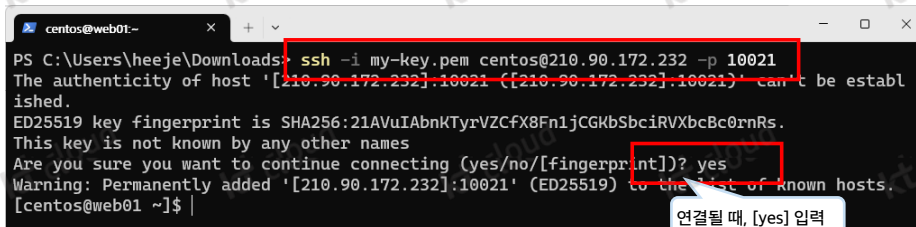
A-5. SSH 접속

Pem 파일이 현재 경로에 존재하는 경우 접속 문자열 :

- (형식) `ssh -i pemfile_name centos@server_ip_address -p port_number`
- (예시) `ssh -i my-key.pem centos@210.90.172.232 -p 10021`

Pem 파일이 현재 경로에 없거나 경로 생략시 접속 에러가 발생하는 경우 :

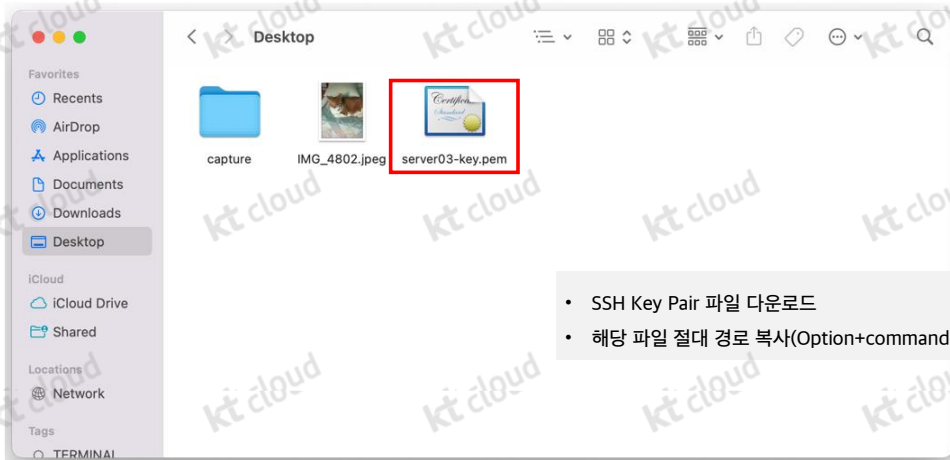
- (형식) `ssh -i "path/pemfile_name" centos@server_ip_address -p port_number`
- (예시) `ssh -i "C:\Users\Wheeje\Downloads\my-key.pem" centos@210.90.172.232 -p 10021`



A terminal window titled 'centos@web01:~' shows the execution of the command `ssh -i my-key.pem centos@210.90.172.232 -p 10021`. The output displays the host's authenticity warning, the key fingerprint (SHA256:21AVuIAbnKTyrVZCfX8Fn1jCGKbSbcirVXbcBc0rnRs), and a prompt asking to continue connecting. A red box highlights the command line, and another red box highlights the response 'yes' to the prompt. A callout bubble points to the 'yes' response with the text '연결될 때, [yes] 입력'.

```
PS C:\Users\heeje\Downloads> ssh -i my-key.pem centos@210.90.172.232 -p 10021
The authenticity of host '[210.90.172.232]:10021 ([210.90.172.232]:10021)' can't be established.
ED25519 key fingerprint is SHA256:21AVuIAbnKTyrVZCfX8Fn1jCGKbSbcirVXbcBc0rnRs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[210.90.172.232]:10021' (ED25519) to the list of known hosts.
[centos@web01 ~]$
```

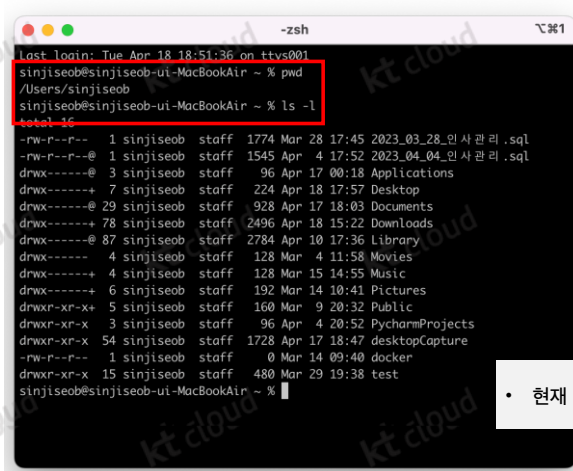
B-1. SSH Key Pair 경로 복사



- SSH Key Pair 파일 다운로드
- 해당 파일 절대 경로 복사(option+command+c)

Copyright© 2023 kt cloud corp. All rights reserved.

B-2. 기본 터미널 실행



```
sinjiseob@sinjiseob-ui-MacBookAir ~ % pwd
/Users/sinjiseob
sinjiseob@sinjiseob-ui-MacBookAir ~ % ls -l
total 16
-rw-r--r--  1 sinjiseob  staff   1774 Mar 28 17:45 2023_03_28_인사관리.sql
-rw-r--r--  1 sinjiseob  staff   1545 Apr  4 17:52 2023_04_04_인사관리.sql
drwx-----  3 sinjiseob  staff    96 Apr 17 00:18 Applications
drwx-----  7 sinjiseob  staff   224 Apr 18 17:57 Desktop
drwx----- 29 sinjiseob  staff   928 Apr 17 18:03 Documents
drwx----- 78 sinjiseob  staff  2496 Apr 18 15:22 Downloads
drwx----- 87 sinjiseob  staff  2784 Apr 10 17:36 Library
drwx-----  4 sinjiseob  staff   128 Mar  4 11:58 Movies
drwx-----  4 sinjiseob  staff   128 Mar 15 14:55 Music
drwx-----  6 sinjiseob  staff   192 Mar 14 10:41 Pictures
drwxr-xr-x+  5 sinjiseob  staff   160 Mar  9 20:32 Public
drwxr-xr-x  3 sinjiseob  staff    96 Apr  4 20:52 PycharmProjects
drwxr-xr-x 54 sinjiseob  staff  1728 Apr 17 18:47 desktopCapture
-rw-r--r--  1 sinjiseob  staff     0 Mar 14 09:40 docker
drwxr-xr-x 15 sinjiseob  staff   480 Mar 29 19:38 test
sinjiseob@sinjiseob-ui-MacBookAir ~ %
```

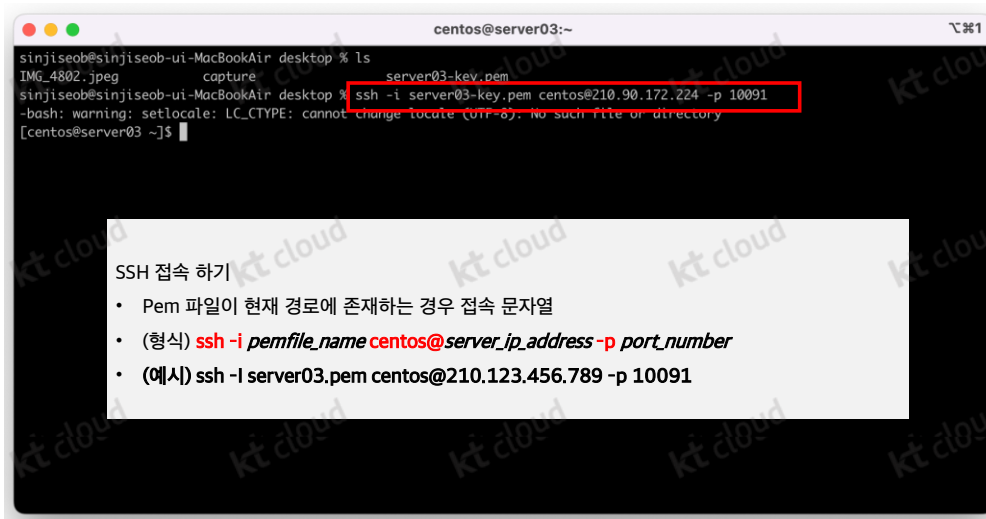
- 현재 경로 및 파일 목록 확인

B-3. 경로 이동

```
-zsh
/Users/sinjiseob
sinjiseob@sinjiseob-ui-MacBookAir ~ % ls -l
total 16
-rw-r--r--  1 sinjiseob  staff   1774 Mar 28 17:45 2023_03_28_인사관리.sql
-rw-r--r--  1 sinjiseob  staff   1545 Apr  4 17:52 2023_04_04_인사관리.sql
drwx-----@ 3 sinjiseob  staff    96 Apr 17 00:18 Applications
drwx-----+ 7 sinjiseob  staff   224 Apr 18 17:57 Desktop
drwx-----@ 29 sinjiseob  staff   928 Apr 17 18:03 Documents
drwx-----+ 78 sinjiseob  staff  2496 Apr 18 15:22 Downloads
drwx-----@ 87 sinjiseob  staff  2784 Apr 10 17:36 Library
drwx-----+ 4 sinjiseob  staff   128 Mar  4 11:58 Movies
drwx-----+ 4 sinjiseob  staff   128 Mar 15 14:55 Music
drwx-----+ 6 sinjiseob  staff   192 Mar 14 10:41 Pictures
drwxr-xr-x+ 5 sinjiseob  staff   160 Mar  9 20:32 Public
drwxr-xr-x  3 sinjiseob  staff    96 Apr  4 20:52 PycharmProjects
drwxr-xr-x 54 sinjiseob  staff  1728 Apr 17 18:47 desktopCapture
-rw-r--r--  1 sinjiseob  staff    80 Mar 14 09:40 docker
drwxr-xr-x 15 sinjiseob  staff   480 Mar 20 10:28 test
sinjiseob@sinjiseob-ui-MacBookAir ~ % cd Desktop
sinjiseob@sinjiseob-ui-MacBookAir Desktop % ls -l
total 3968
-rw-r--r--@ 1 sinjiseob  staff  2024114 Mar 14 10:42 IMG_4802.jpeg
drwxr-xr-x@ 7 sinjiseob  staff    224 Apr 18 10:06 capture
-rw-----@ 1 sinjiseob  staff   1702 Apr 18 13:20 server03-key.pem
sinjiseob@sinjiseob-ui-MacBookAir Desktop %
```

- pem 파일 저장된 경로로 이동
- pem파일 확인(예 : server03-key.pem)

B-4. SSH 접속(1)



Copyright© 2023 kt cloud corp. All rights reserved.

B-4. SSH 접속(2)



Copyright© 2023 kt cloud corp. All rights reserved.

