

## Lab3. NCP에서 Linux Server 가상 서버 만들기

### 1. 목적

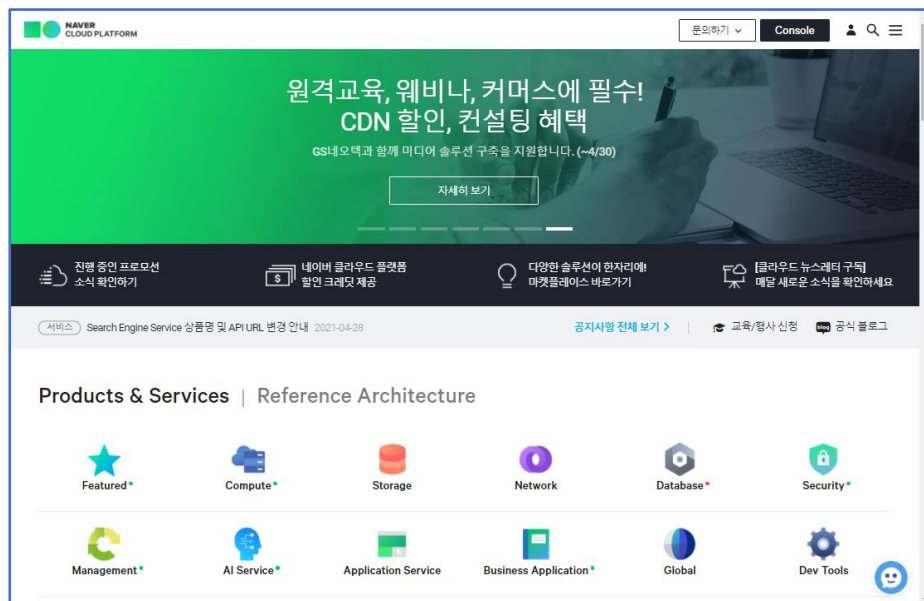
이 실습에서는 Naver Cloud Platform에서 Windows Server 가상 머신을 만들고 중지 및 삭제한다. 또한 대표적인 웹 서버인 Apache Web Server를 설치한다.

### 2. 사전 준비물

- Naver Cloud Platform 계정

### 3. NCP연결 후 Network 관련 서비스 생성하기

- A. 웹 브라우저를 열고 Naver Cloud Platform에 접속한다. <https://www.ncloud.com/>



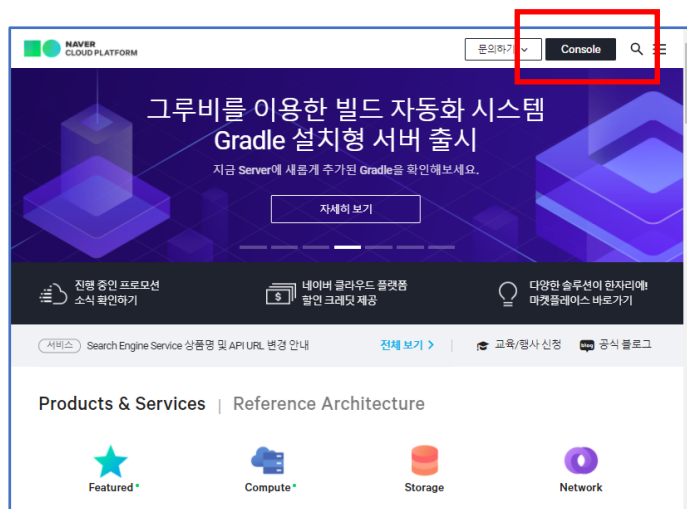
- B. 화면 우측 상단의 **[로그인]** 링크 또는 사람 모양의 아이콘을 클릭하여 로그인한다.

## 로그인

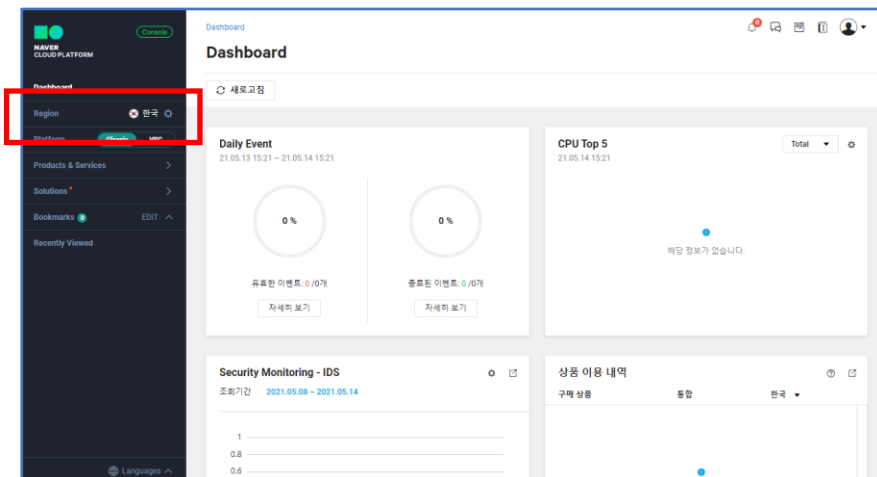
☐ 아이디 저장

[회원가입](#) | [아이디 찾기](#) | [비밀번호 찾기](#)

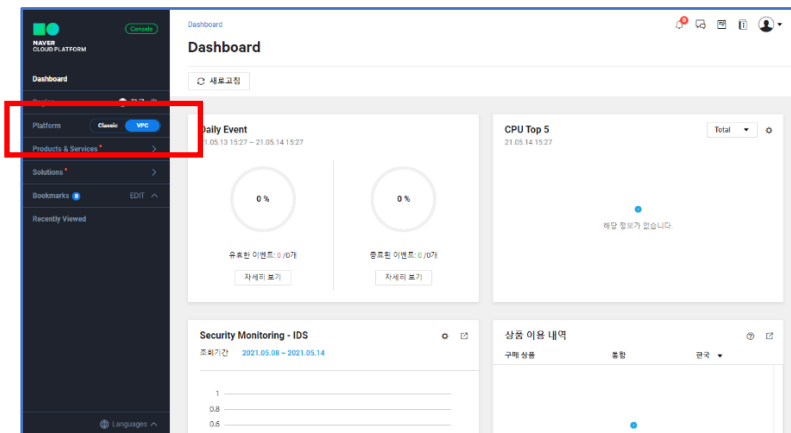
- C. Login이 된 후 이제 **[Console]**로 들어가도록 한다. 페이지 우측 상단의 **[Console]** 검은색 버튼을 클릭한다.



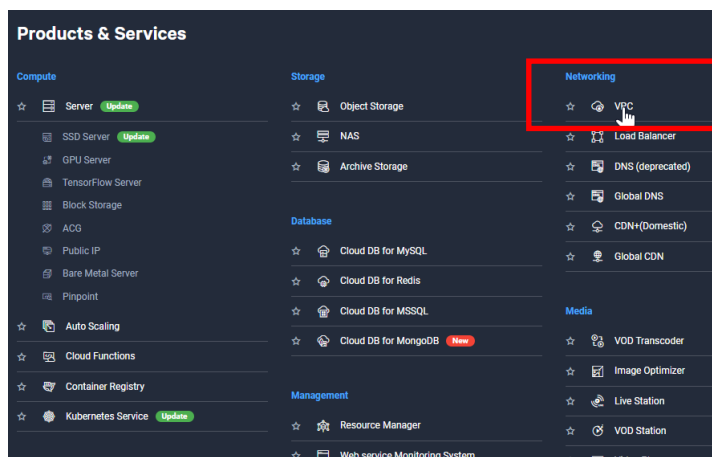
- D. **[Dashboard]** 페이지이다. 먼저 좌측 메뉴에서 **[Region]**이 **[한국]**에 맞춰져 있는지 확인한다.



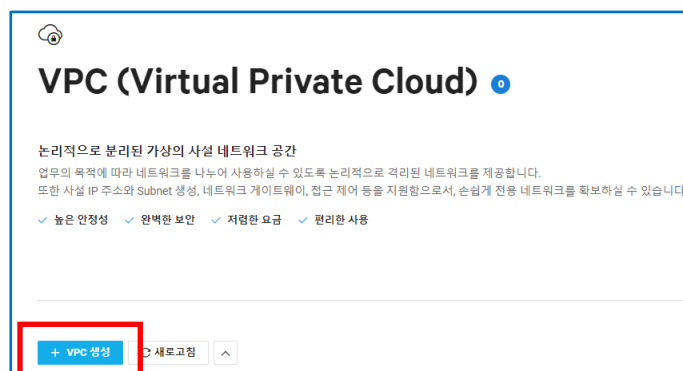
- E. 그리고 **[Platform]**이 **[VPC]**에 맞춰져 있는지 확인한다. 혹시 **[Classic]**에 맞춰져 있다면 **[VPC]**로 마우스를 드래그하여 맞춘다.



- F. 서버를 생성하기 전에 먼저 VPC 즉 Virtual Private Cloud부터 생성한다. **[Products & Services] > [Networking] > [VPC]**를 클릭한다.



- G. **[VPC (Virtual Private Cloud)]** 페이지이다. 아직 실습에서 VPC를 생성한 적이 없기 때문에 새 VPC를 생성하기 위해 **[+VPC 생성]** 파란색 버튼을 클릭한다.



- H. 다음과 같이 값을 입력한다. [VPC 이름]은 lab3-vpc, [IP 주소 범위]는 172.16.0.0/16 으로 입력하고 [생성] 파란색 버튼을 클릭한다.

VPC 생성

VPC를 생성합니다.

VPC는 논리적으로 격리된 네트워크 공간을 제공합니다.

VPC의 IP 주소 범위는, private 대역(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) 내에서 /16~/28 범위여야 합니다.

(필수 입력 사항입니다.)

VPC 이름: lab3-vpc

IP 주소 범위: 172.16.0.0/16

× 취소    ✓ 생성

- I. 여기서 주의할 점은 VPC목록에는 있지만, [상태]는 반드시 [운영중]이어야 한다는 점이다.

VPC (Virtual Private Cloud)

+ VPC 생성    새로고침    ▼

삭제

VPC 이름	VPC ID	상태	CIDR 블록
<input type="checkbox"/> lab3-vpc	7861	● 운영중	172.16.0.0/16

- J. 이번에는 Network ACL을 설정한다. Network ACL을 설정하려면 좌측 **Dashboard**에서 [VPC] > [Network ACL] > [ACL Rule] 메뉴를 클릭한다. 기본적으로 **Default ACL**이 있고, 이 **Default ACL**은 삭제가 되지 않는다. 새 Network ACL을 생성하기 위해 [+Network ACL 생성] 파란색 버튼을 클릭한다.

Network ACL

+ Network ACL 생성    새로고침    ▼

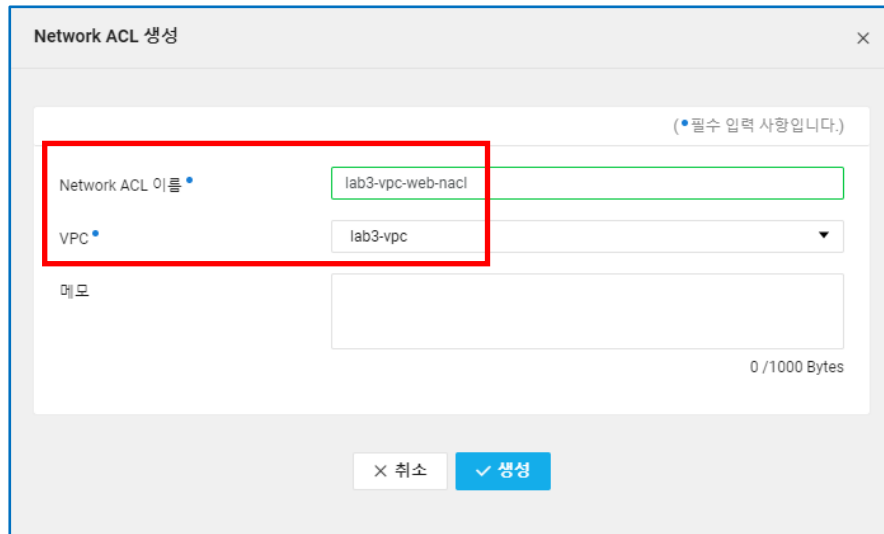
Rule 설정    삭제    Network ACL 이름    🔍    Filter    Subnet 적용 여부: ✓ 전체    ▼

Network ACL 이름	Network ACL ID	VPC 이름	적용 Subnet 수	메모
<input type="checkbox"/> lab3-vpc-default-network-acl	11161	lab3-vpc	0	VPC [lab3-vpc] default Network ACL

- K. 다음과 같이 값을 입력한 다음, [생성] 파란색 버튼을 클릭한다.

① [Network ACL 이름] : lab3-vpc-web-nacl

② [VPC] : lab3-vpc



Network ACL 생성

(필수 입력 사항입니다.)

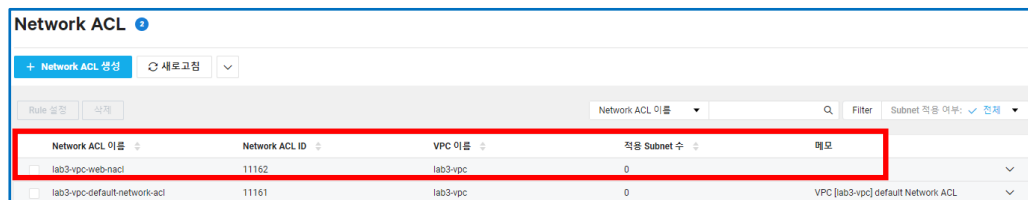
Network ACL 이름: lab3-vpc-web-nacl

VPC: lab3-vpc

메모: 0 / 1000 Bytes

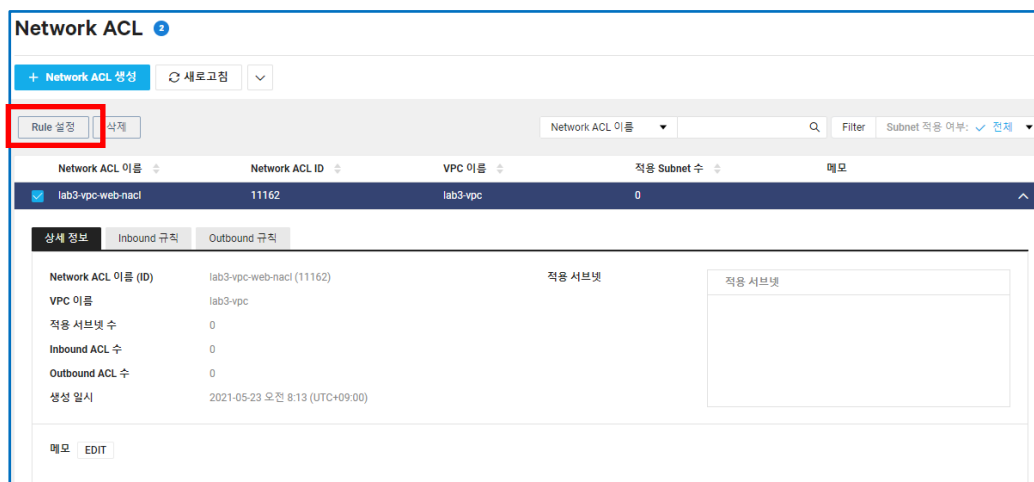
× 취소    ✓ 생성

L. 방금 생성한 Network ACL을 확인할 수 있다.



Network ACL 이름	Network ACL ID	VPC 이름	적용 Subnet 수	메모
lab3-vpc-web-nacl	11162	lab3-vpc	0	
lab3-vpc-default-network-acl	11161	lab3-vpc	0	VPC [lab3-vpc] default Network ACL

M. 방금 생성한 [lab3-vpc-web-nacl] 체크박스에 체크해보자. [상세 정보] 탭이 보인다.  
이 ACL에 Rule을 설정하기 위해 [Rule 설정] 버튼을 클릭한다.



Network ACL

+ Network ACL 생성    새로고침

Rule 설정    삭제

Network ACL 이름	Network ACL ID	VPC 이름	적용 Subnet 수	메모
lab3-vpc-web-nacl	11162	lab3-vpc	0	

상세 정보    Inbound 규칙    Outbound 규칙

Network ACL 이름 (ID): lab3-vpc-web-nacl (11162)    적용 서브넷

VPC 이름: lab3-vpc    적용 서브넷

적용 서브넷 수: 0

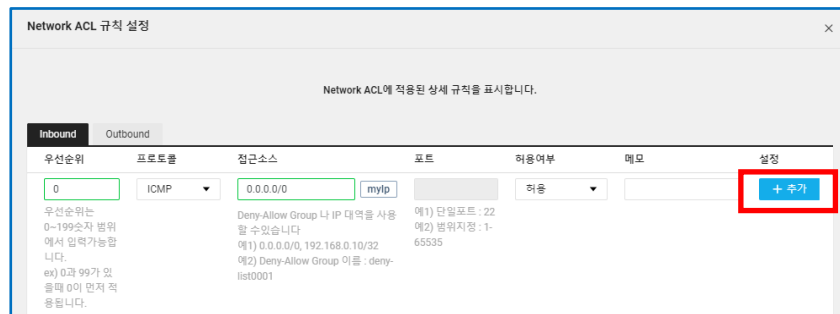
Inbound ACL 수: 0

Outbound ACL 수: 0

생성 일시: 2021-05-23 오전 9:13 (UTC+09:00)

메모    EDIT

- N. 다음과 같이 **[Network ACL 규칙 설정]** 페이지에서 **[Inbound]** Rule을 추가하기로 한다. 각 항목을 입력을 마치면 **[+추가]** 파란색 버튼을 클릭한다.




The screenshot shows the 'Network ACL 규칙 설정' window with the 'Inbound' tab selected. The configuration fields are as follows:

우선순위	프로토콜	접근소스	포트	허용여부	메모	설정
0	ICMP	0.0.0.0/0	mylp	허용		+ 추가

Below the form, there is explanatory text for the priority and source address fields.

- ① **[우선순위] : 0, [프로토콜] : ICMP, [접근소스] : 0.0.0.0/0, [허용여부] : 허용**
- ② **[우선순위] : 1, [프로토콜] : TCP, [접근소스] : 0.0.0.0/0, [포트] : 80, [허용여부] : 허용**
- ③ **[우선순위] : 2, [프로토콜] : TCP, [접근소스] : mylp, [포트] : 22, [허용여부] : 허용**



The screenshot shows the 'Network ACL 규칙 설정' window with the 'Inbound' tab selected. The configuration fields are as follows:

우선순위	프로토콜	접근소스	포트	허용여부	메모	설정
	TCP		mylp	허용		+ 추가

Below the form, there is a table showing the configured rules:

우선순위	프로토콜	접근소스	포트	허용여부	메모	설정
0	ICMP	0.0.0.0/0 (전체)		허용		✖
1	TCP	0.0.0.0/0 (전체)	80	허용		✖
2	TCP	121.136.18.98/32	22	허용		✖

- O. 이번에는 **[Outbound]** 탭을 맞추고 **[Inbound]** 설정했던 방식으로 다음의 Rule을 추가한다.

- ① **[우선순위] : 0, [프로토콜] : ICMP, [목적지] : 0.0.0.0/0, [허용여부] : 허용**
- ② **[우선순위] : 1, [프로토콜] : TCP, [목적지] : 0.0.0.0/0, [포트] : 1-65535, [허용여부] : 허용**
- ③ **[우선순위] : 2, [프로토콜] : UDP, [목적지] : 0.0.0.0/0, [포트] : 1-65535, [허용여부] : 허용**

Network ACL 규칙 설정

Network ACL에 적용된 상세 규칙을 표시합니다.

Inbound Outbound

우선순위	프로토콜	목적지	포트	허용여부	메모	설정
<input type="text"/> 우선순위는 0~199숫자 범위에서 입력가능합니다. ex) 0과 99가 있을때 0이 먼저 적용됩니다.	TCP	<input type="text"/> myip Deny-Allow Group 나 IP 대역을 사용할 수 있습니다. 예1) 0.0.0.0/0, 192.168.0.10/32 예2) Deny-Allow Group 이름 : deny-list0001	<input type="text"/> 1-65535 예1) 단일포트 : 22 예2) 범위지정 : 1-65535	허용	<input type="text"/>	+ 추가
0	ICMP	0.0.0.0/0 (전체)		허용		✕
1	TCP	0.0.0.0/0 (전체)	1-65535	허용		✕
2	UDP	0.0.0.0/0 (전체)	1-65535	허용		✕

- P. [Inbound]와 [Outbound] 모두 추가했으면 마지막으로 화면 아래쪽의 [적용] 파란색 버튼을 클릭한다.

Network ACL 규칙 설정

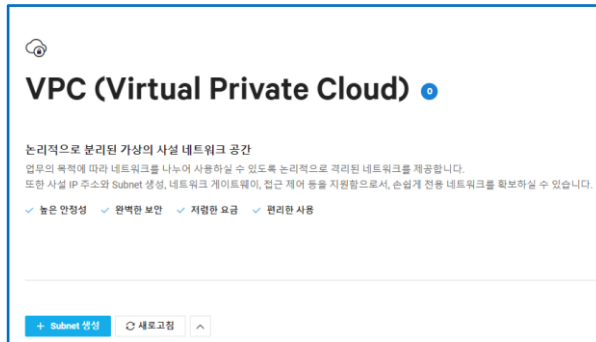
Network ACL에 적용된 상세 규칙을 표시합니다.

Inbound Outbound

우선순위	프로토콜	목적지	포트	허용여부	메모	설정
<input type="text"/> 우선순위는 0~199숫자 범위에서 입력가능합니다. ex) 0과 99가 있을때 0이 먼저 적용됩니다.	TCP	<input type="text"/> myip Deny-Allow Group 나 IP 대역을 사용할 수 있습니다. 예1) 0.0.0.0/0, 192.168.0.10/32 예2) Deny-Allow Group 이름 : deny-list0001	<input type="text"/> 1-65535 예1) 단일포트 : 22 예2) 범위지정 : 1-65535	허용	<input type="text"/>	+ 추가
0	ICMP	0.0.0.0/0 (전체)		허용		✕
1	TCP	0.0.0.0/0 (전체)	1-65535	허용		✕
2	UDP	0.0.0.0/0 (전체)	1-65535	허용		✕

✕ 취소 ✓ 적용

- Q. 이번에는 Subnet을 생성한다. Subnet을 생성하려면 좌측 **Dashboard**에서 [VPC] > [Subnet Management] 메뉴를 클릭한다.



R. 새 Subnet을 생성하기 위해 **[+Subnet 생성]** 파란색 버튼을 클릭한다.

S. 다음과 같이 각 항목의 값을 입력한 다음, **[생성]** 파란색 버튼을 클릭한다.

- ① **[Subnet 이름]** : lab3-vpc-web-subnet
- ② **[VPC]** : lab3-vpc(172.16.0.0/16)
- ③ **[IP 주소 범위]** : 172.16.1.0/24
- ④ **[가용 Zone]** : KR-2
- ⑤ **[Network ACL]** : lab3-vpc-web-nacl
- ⑥ **[Internet Gateway 전용 여부]** : Y (Public)
- ⑦ **[용도]** : 일반

Subnet 생성

Subnet을 생성합니다.  
VPC 내에 세분화된 격리 공간을 제공합니다.  
IP 주소 범위는 VPC 주소 범위 이하로만 지정이 가능하며,  
private 대역(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) 내에서 /16~/28 범위여야 합니다.  
생성 이후 Network ACL 만 변경이 가능하므로 생성시 주의해주시기 바랍니다.

(\* 필수 입력 사항입니다.)

Subnet 이름
lab3-vpc-web-subnet

VPC
lab3-vpc (172.16.0.0/16)

IP 주소 범위
172.16.1.0/24

가용 Zone
KR-2

Network ACL
lab3-vpc-web-nacl

Internet Gateway 전용 여부
☒ Y (Public) ☐ N (Private)

용도
☒ 일반 ☐ LoadBalancer ☐ BareMetal  
일반서버에서만 사용 가능한 서버넷입니다.

× 취소

✓ 생성

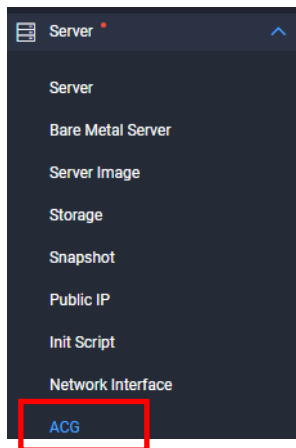


T. 생성 후 [Subnet] 페이지에서 현재 [상태]가 [운영중]임을 확인해야 한다.

Subnet 이름	Subnet ID	상태	VPC 이름	IP 주소 범위	Zone	Internet Gateway 적용 여부	용도
lab3-vpc-web-subnet	15461	● 운영중	lab3-vpc	172.16.1.0/24	KR-2	Y (Public)	일반

#### 4. Web Server ACG 생성 후, Web Server 생성하기

A. ACG를 생성하기 위해 좌측 [Dashboard]의 [Products & Services] > [Compute] > [ACG] 메뉴를 클릭한다.



B. **ACG** 역시 **Default ACG**가 있다. 이번 실습에서는 새 ACG를 생성하기로 한다. [+ACG 생성] 파란색 버튼을 클릭한다.

ACG 이름	ACG ID	VPC 이름	적용 Network Interface 수	메모
lab3-vpc-default-acg	16241	lab3-vpc	0	VPC [lab3-vpc] default ACG

C. [ACG 생성] 창이다. 다음과 같이 값을 입력하고 [생성] 파란색 버튼을 클릭한다.

① [ACG 이름] : lab3-acg

② [VPC] : lab3-vpc

ACG 생성

( \*필수 입력 사항입니다.)

ACG 이름

VPC

메모

0/1000 bytes

× 취소 ✓ 생성

- D. 방금 생성한 **lab3-acg** 목록에서 확인하고, 체크박스 체크한 다음, **[ACG 설정]** 버튼을 클릭한다.

ACG 2

+ ACG 생성 상품 더 알아보기 다운로드 새로고침

ACG 설정 ACG 삭제 ACG 이름

ACG 이름	ACG ID	VPC 이름	적용 Network Interface 수	메모
<input checked="" type="checkbox"/> lab3-acg	16242	lab3-vpc	0	
<input type="checkbox"/> lab3-vpc-default-acg	16241	lab3-vpc	0	VPC [lab3-vpc] default ACG

<< < 1 > >>

- E. **[ACG 규칙 설정]** 창이다. 위에서 ACL 목록 추가처럼 **[Inbound]**와 **[Outbound]** 모두 다음과 같이 값을 입력할 때, 각 값을 입력한 후에는 반드시 **[+추가]** 버튼을 클릭한다.

ACG 규칙 설정 | lab2-acg

ACG 에 적용된 상세 규칙을 표시합니다.

Inbound Outbound

프로토콜  접근 소스  myip 허용 포트

메모

예1) 단일포트: 22  
예2) 범위지정: 1-65535

예2) ACG 이름: my-acg-1

Detail

설정 + 추가

① [Inbound] 규칙

- I. [프로토콜] : ICMP, [접근 소스] : 0.0.0.0/0
- II. [프로토콜] : TCP, [접근 소스] : 0.0.0.0/0, [허용 포트] : 80
- III. [프로토콜] : TCP, [접근 소스] : mylp, [허용 포트] : 22

ACG 규칙 설정 | lab3-acg

ACG 에 적용된 상세 규칙을 표시합니다.

Inbound Outbound

프로토콜 \* 접근 소스 \* 허용 포트 \* 메모 설정

TCP [ ] mylp [ ] + 추가

예1) IP: 0.0.0.0/0, 192.168.1.0/24, 192.168.1.7  
예2) ACG 이름 : my-acg-1  
Detail

TCP 121.136.18.98/32 22 [X]

TCP 0.0.0.0/0(전체) 80 [X]

ICMP 0.0.0.0/0(전체) [X]

② [Outbound] 규칙

- I. [프로토콜] : ICMP, [목적지] : 0.0.0.0/0
- II. [프로토콜] : TCP, [목적지] : 0.0.0.0/0, [허용 포트] : 1-65535
- III. [프로토콜] : UDP, [목적지] : 0.0.0.0/0, [허용 포트] : 1-65535

ACG 규칙 설정 | lab3-acg

ACG 에 적용된 상세 규칙을 표시합니다.

Inbound Outbound

프로토콜 \* 목적지 \* 허용 포트 \* 메모 설정

TCP [ ] mylp [ ] + 추가

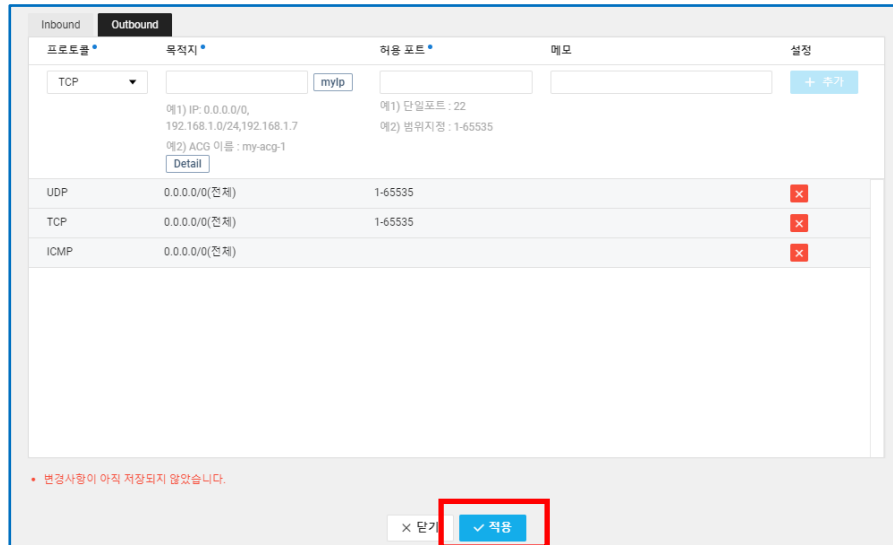
예1) IP: 0.0.0.0/0, 192.168.1.0/24, 192.168.1.7  
예2) ACG 이름 : my-acg-1  
Detail

UDP 0.0.0.0/0(전체) 1-65535 [X]

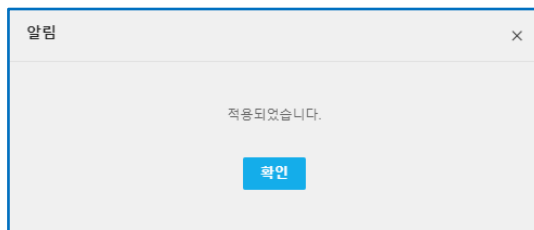
TCP 0.0.0.0/0(전체) 1-65535 [X]

ICMP 0.0.0.0/0(전체) [X]

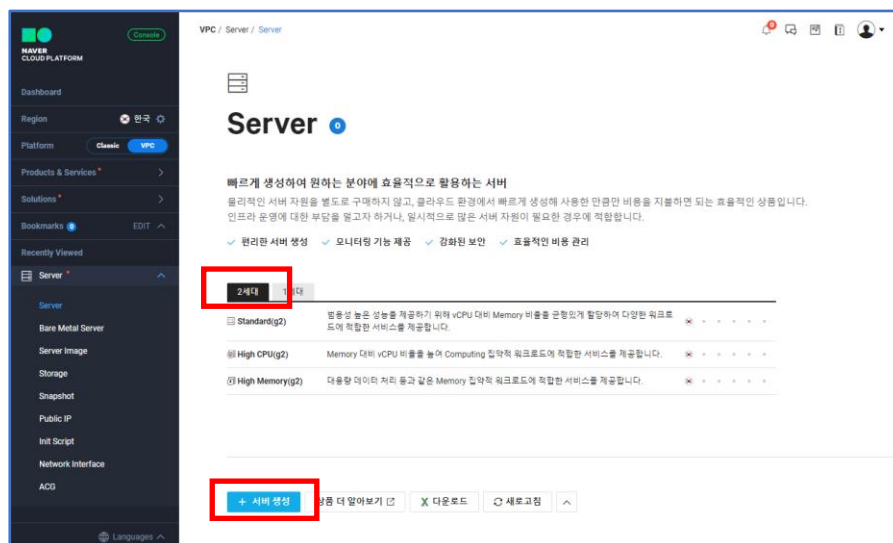
③ 반드시 페이지 하단의 [적용] 파란색 버튼을 클릭한다.



F. ACG 적용 되었다.



G. 이제 Web Server 역할을 할 서버를 생성하자. [Dashboard]의 [Server] 메뉴를 클릭한다. [Server] 페이지에 들어왔다. [2세대]에 맞추고 페이지 아래의 [+서버 생성]을 클릭한다.



- H. 모두 5단계를 거쳐서 서버를 생성한다. 첫번째 단계로 [서버 이미지 선택]이다. 이번 실습에서는 Linux Server를 생성하기 때문에 [부팅 디스크 크기]는 50GB에 맞춘다. [이미지타입]은 [OS]에, [OS 이미지타입]은 [Ubuntu]에 [서버 타입]은 [Standard]에 맞추고 [서버 이미지 이름]에서 ubuntu-18.04의 [다음] 파란색 버튼을 클릭하여 다음 단계로 넘어간다.

1 서버 이미지 선택 2 서버 설정 3 인스턴스 설정 4 네트워크 접근 설정 5 최종 확인

CentOS, Ubuntu, Windows 및 DBMS 서버 이미지를 제공합니다. 이미지 및 부팅 디스크 크기를 선택하세요.

- 현재 Windows 에 대해서만 부팅 디스크로 100GB 선택이 가능합니다.
- 각각의 서버 타입별로 제공하는 서버 이미지가 상이하므로 이를 확인하시어 서버를 생성해주세요.

부팅 디스크 크기 ☒ 50GB ☐ 100GB

이미지타입 ☒ OS ☐ Application

OS 이미지타입 ☐ All ☐ CentOS ☒ Ubuntu ☐ Windows

서버 타입 ☐ High CPU ☒ Standard ☐ High-Memory ☐ GPU ☐ CPU Intensive

서버 이미지 이름	설명	
ubuntu-16.04-64-server	Ubuntu Server 16.04 (64-bit) (커널 업데이트 시 서버의 정상적인 사용이 불가능할 수 있으며 이에 따른 복구는 지원하지 않습니다.)	다음 >
ubuntu-18.04	Ubuntu Server 18.04 (64-bit) (커널 업데이트 시 서버의 정상적인 사용이 불가능할 수 있으며 이에 따른 복구는 지원하지 않습니다.)	다음 >

- I. 2단계 [서버 설정] 단계이다. 다음의 각 값을 입력하자.

- ① [VPC] : lab3-vpc
- ② [Subnet] : lab3-vpc-web-subnet | KR-2 | 172.16.1.0/24 | Public
- ③ [스토리지 종류] : SSD
- ④ [서버 세대] : g2
- ⑤ [서버 타입] : Standard, [Standard] vCPU 2개, 메모리 8GB, [SSD]디스크 50GB [g2] s2-g2-s50
- ⑥ [요금제 선택] : 시간 요금제
- ⑦ [서버 개수] : 1
- ⑧ [서버 이름] : lab3-webserver

1 서버 이미지 선택 2 서버 설정 3 인증키 설정 4 네트워크 접근 설정 5 최종 확인

### 서버 설정

서버 타입과 요금제를 선택하세요. (\*필수 입력 사항입니다.)

VPC  [VPC 생성](#)

Subnet  [Subnet 생성](#)

공인 IP 연결을 위해서는 반드시 Public Subnet을 선택해야 합니다.

스토리지 종류 ☒ SSD ☐ HDD

서버 타입

요금제 선택 ☐ 월요금제 ☒ 시간 요금제 시간 당 123원 (OS 제외)

서버 개수

서버 이름

☒ 입력하신 서버 이름으로 hostname을 설정합니다.

- J. 페이지를 계속 아래로 내려서 **[Network Interface]** 와 **[공인 IP]**를 설정한다. **[IP]**의 값을 놓지 않고 **[+추가]** 버튼을 클릭하면 자동 IP로 설정되고 다음과 같이 Subnet의 범위 안에서 **172.16.1.101**을 입력하고 **[+추가]** 버튼을 누르면 값이 **172.16.1.101/32**로 설정된다. **[공인 IP]**로 외부에서 직접 접근하려면 **[새로운 공인 IP 할당]** 옵션 버튼을 클릭한다. 이제 **[다음]** 파란색 버튼을 클릭하여 다음 단계로 넘어간다.

Network Interface

디바이스	Network Interface	Subnet	IP
eth1	<input type="text" value="new interface"/>	<input type="text" value="- select -"/>	<input type="text" value="미입력시 자동할당"/>
eth0	<input type="text" value="new interface"/>	<input type="text" value="lab3-vpc-web-subnet   KR-2   172.16.1.0/24   Public"/>	<input type="text" value="172.16.1.101/32"/> <input type="button" value="X"/>

공인 IP ☐ 미설정 ☒ 새로운 공인 IP 할당 신정된 공인 IP는 보유하신 동안 요금이 과금되므로, 사용하지 않을 때는 반납하시기를 권장드립니다. (월 이용료: 4,032원)  
서버 생성시 공인 IP를 함께 생성하시려면 Subnet 타입은 Public Subnet, 서버 개수는 1개여야 합니다.

불리 배지 그룹 ☐

반납 보호 ☐ 설정 ☒ 해제 반납 보호를 설정하면 실수로 반납하는 사고를 방지할 수 있습니다.

메모

Script 선택

< 이전 **다음 >**

- K. 다음 단계는 **[인증키 설정]** 단계이다. 로그인을 위한 아이디와 비밀번호를 대체하는 키다. **[새로운 인증키 생성]** 옵션 버튼을 선택하고 **[인증키 이름]**을 **lab3-key**라고 입력하고 **[인증키 생성 및 저장]** 파란색 버튼을 클릭한다.

✓ 서버 이미지 선택
✓ 서버 설정
3 인증키 설정
4 네트워크 접근 설정
5 최종 확인

### 인증키 설정

보유하고 있는 인증키를 선택하거나 새로운 인증키를 생성하세요. 인증키는 관리자 비밀번호를 얻는데 사용합니다. (● 필수 입력 사항입니다.)

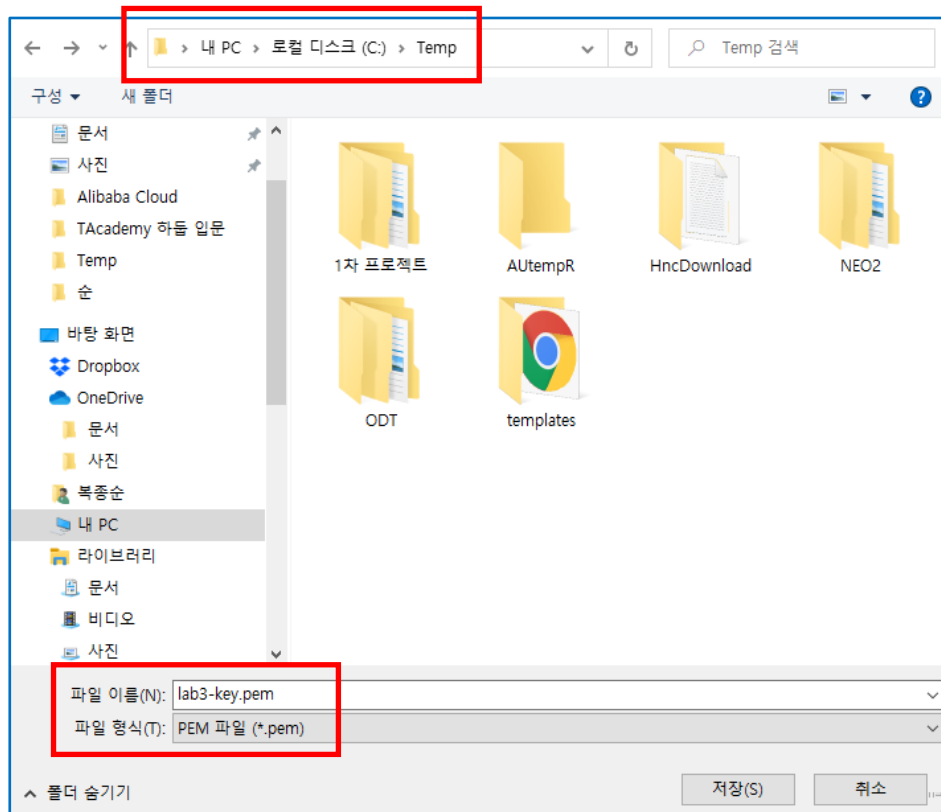
☐ 보유하고 있는 인증키 이용
   
☒ 새로운 인증키 생성

인증키 이름  인증키 생성 및 저장

인증키 이름을 입력 후 [인증키 생성 및 저장]을 클릭하여 인증키를 생성해 컴퓨터에 저장하세요.  
인증키는 해당 서버의 관리자 비밀번호 확인에 이용되니 안전한 곳에 저장하시기 바랍니다

< 이전
다음 >

L. 인증키를 찾기 쉬운 위치에 저장한다.



M. [다음] 파란색 버튼을 클릭하여 다음 단계로 이동한다.

☒ 서버 이미지 선택
 ☒ 서버 설정
 ☒ 인증키 설정
 ☐ 네트워크 접근 설정
 ☐ 최종 확인

### 인증키 설정

보유하고 있는 인증키를 선택하거나 새로운 인증키를 생성하세요. 인증키는 관리자 비밀번호를 얻는데 사용됩니다. (\* 필수 입력 사항입니다.)

☐ 보유하고 있는 인증키 이동  
☒ 새로운 인증키 생성

인증키 이름:  인증키 생성 및 저장

인증키 이름을 입력 후 [인증키 생성 및 저장]를 클릭하여 인증키를 사용자 컴퓨터에 저장하세요.  
인증키는 해당 서버의 관리자 비밀번호 확인에 이용되니 안전한 곳에 저장하시기 바랍니다

< 이전
다음 >

- N. [네트워크 접근 설정] 단계이다. 이미 앞에서 생성한 ACG 즉 **lab3-acg**를 선택하고 **[다음]** 파란색 버튼을 클릭하여 마지막 단계로 넘어간다.

☒ 서버 이미지 선택
 ☒ 서버 설정
 ☒ 인증키 설정
 ☒ 네트워크 접근 설정
 ☐ 최종 확인

### 네트워크 접근 설정

보유하고 있는 ACG를 선택하거나 새로운 ACG를 생성해주세요. (\* 필수 입력 사항입니다.)  
ACG(Access Control Group)은 별도의 방화벽 구축없이, 서버 그룹에 대한 네트워크 접근 제어 및 관리를 돕는 상품입니다.

디바이스	ACG
eth0 *	lab3-acg x

최대 3개까지 선택가능

설정 시 주의사항

- '신규 Network Interface'로 지정해서 생성된 ACG만 설정 가능합니다.
- 기존에 생성된 'Network Interface'를 사용하는 경우 해당 Network Interface의 ACG를 사용하게 됩니다.

< 이전
다음 >

- O. 이제 마지막 단계인 **[최종 확인]** 단계이다. 각 항목을 살펴보고 이상이 없으면 페이지 제일 하단의 **[서버 생성]** 초록색 버튼을 클릭한다.

☒ 서버 이미지 선택
 ☒ 서버 설정
 ☒ 인증키 설정
 ☒ 네트워크 접근 설정
 ☒ 최종 확인

### 최종 확인

[서버 생성] 버튼을 클릭하면 서버가 생성됩니다.

#### 서버 이미지

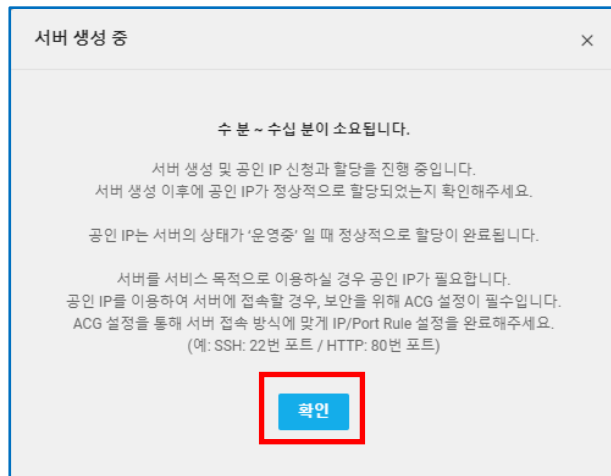
서버 이미지 이름	서버 이미지 설명
ubuntu-18.04	Ubuntu Server 18.04 (64-bit)

#### Script 선택

< 이전
✓ 서버 생성



- P. [서버 생성 중] 창이 나타난다. [확인] 버튼을 클릭한다.



- Q. 잠시 기다리면 실습에서 생성한 Web Server 역할을 할 서버의 [상태]가 [생성중] → [부팅중] → [설정중] → [운영중]까지 변경된다. 최종적으로 [운영중]으로 되어야 한다.

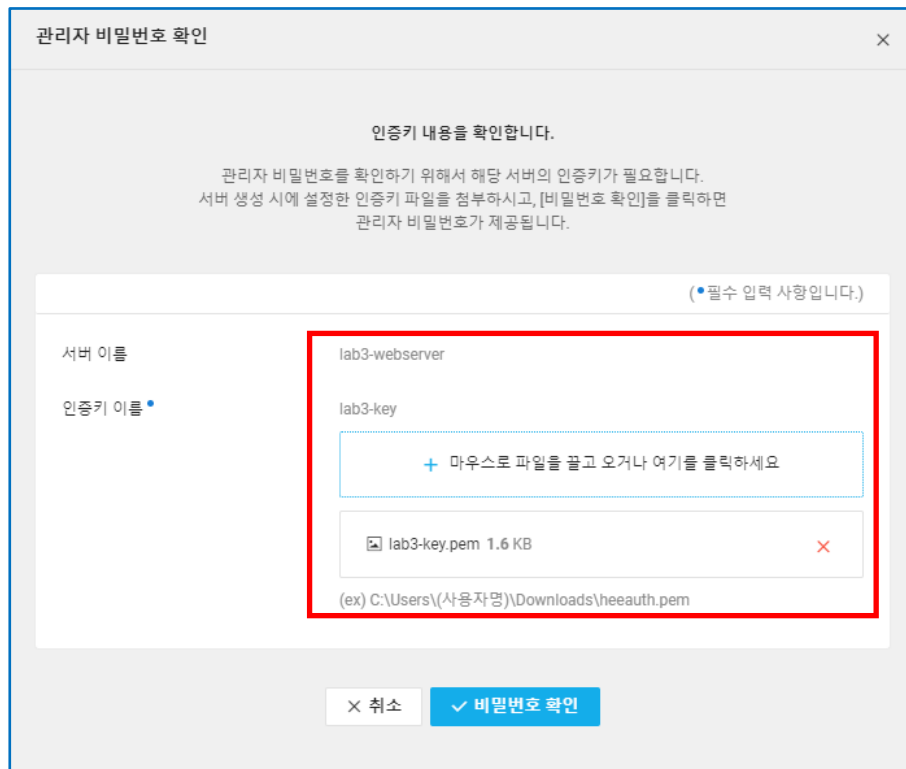


## 5. Linux Server 서버에 연결하기

- A. 접속하려는 [서버 이름]에 체크하고 [서버 관리 및 설정 변경] 드롭다운 버튼을 클릭하여 [관리자 비밀번호 확인] 메뉴를 클릭한다 .



- B. **[관리자 비밀번호 확인]** 창이 나타난다. 위에서 저장했던 인증키를 드래그하여 네모 박스 안에 넣는다. 그리고 **[비밀번호 확인]** 파란색 버튼을 클릭한다.



관리자 비밀번호 확인

인증키 내용을 확인합니다.

관리자 비밀번호를 확인하기 위해서 해당 서버의 인증키가 필요합니다.  
서버 생성 시에 설정한 인증키 파일을 첨부하시고, [비밀번호 확인]을 클릭하면  
관리자 비밀번호가 제공됩니다.

(● 필수 입력 사항입니다.)

서버 이름 lab3-webserver

인증키 이름 lab3-key

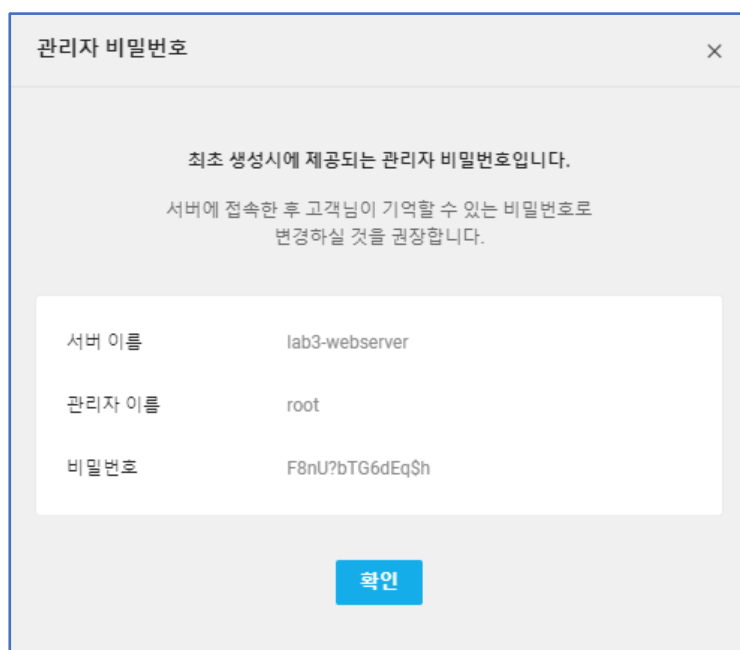
+ 마우스로 파일을 끌고 오거나 여기를 클릭하세요

lab3-key.pem 1.6 KB

(ex) C:\Users\<사용자명>\Downloads\heeauth.pem

× 취소 ✓ 비밀번호 확인

- C. **[최초 생성시에 제공되는 관리자 비밀번호입니다.]**라고 메시지가 나오면서 서버에 접속한 후 보다 쉽게 관리할 수 있는 비밀번호로 변경하라고 한다. **[확인]** 버튼을 클릭한다. 현재의 비밀번호를 복사하여 메모장에 붙여넣는다.



관리자 비밀번호

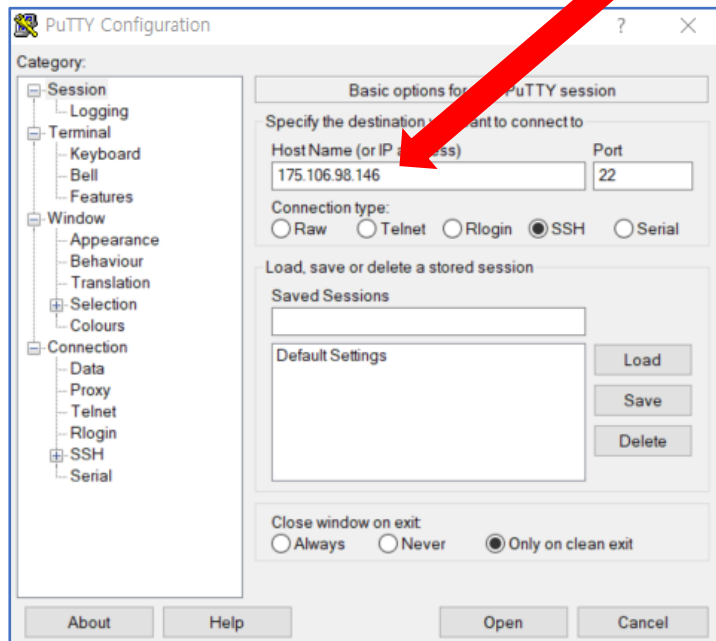
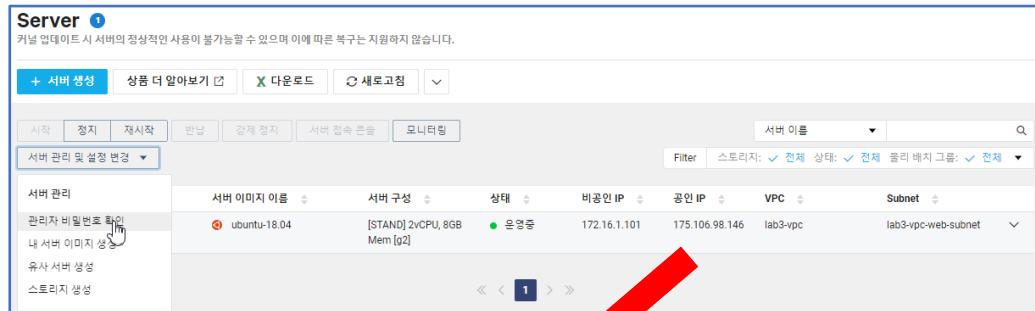
최초 생성시에 제공되는 관리자 비밀번호입니다.

서버에 접속한 후 고객님의 기억할 수 있는 비밀번호로  
변경하실 것을 권장합니다.

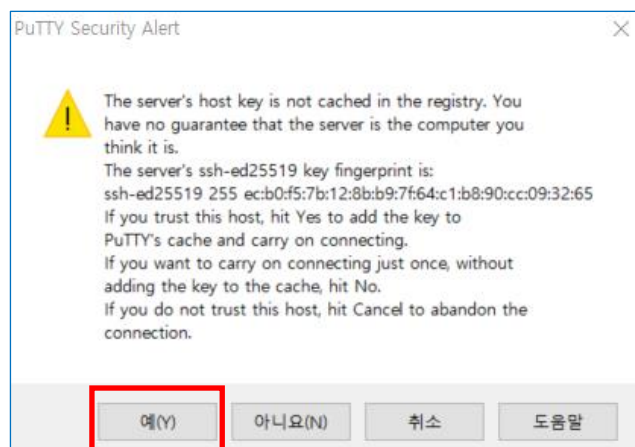
서버 이름	lab3-webserver
관리자 이름	root
비밀번호	F8nU?bTG6dEq\$H

확인

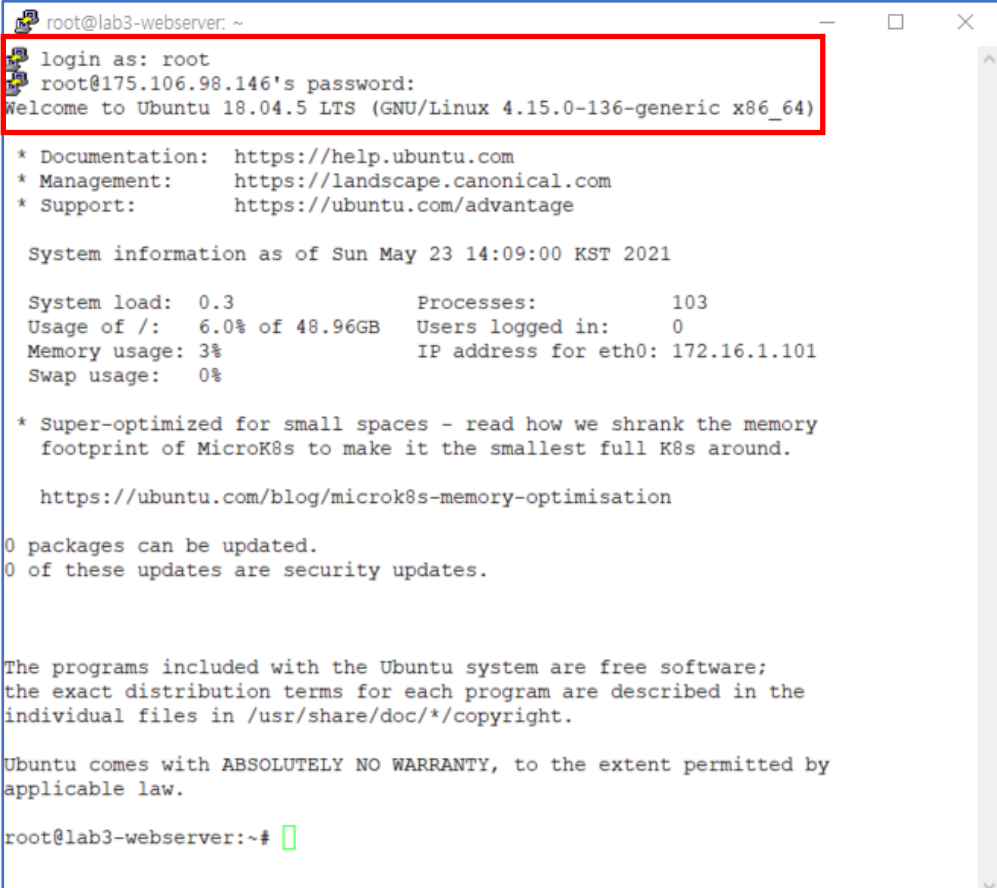
- D. 여러분의 데스크톱 혹은 Notebook에서 **[PuTTY]** 프로그램을 찾아서 해당 프로그램을 실행시킨다. 그리고 방금 생성한 서버의 **[공인 IP]** 주소를 복사하여 **[Host Name (or IP address)]**에 해당 IP를 넣는다. 그리고 **[Open]** 버튼을 클릭하여 서버에 연결하자.



- E. **[PuTTY Security Alert]**창이 나타난다. **[예(Y)]**를 클릭한다.



- F. [PuTTY] 터미널에서 아이디는 **root**로, 비밀번호는 방금 메모장에 복사한 관리자 비밀번호를 복사한 후 붙여 넣기를 위해 마우스 오른쪽 클릭을 한다. 그리고 엔터키를 누르면 서버에 연결이 된다.



```
root@lab3-webserver: ~  
login as: root  
root@175.106.98.146's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-136-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sun May 23 14:09:00 KST 2021  
  
System load:  0.3               Processes:            103  
Usage of /:   6.0% of 48.96GB   Users logged in:     0  
Memory usage: 3%               IP address for eth0: 172.16.1.101  
Swap usage:   0%  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  
  https://ubuntu.com/blog/microk8s-memory-optimisation  
  
0 packages can be updated.  
0 of these updates are security updates.  
  
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.  
  
root@lab3-webserver:~#
```

- G. 이렇게 해서 **NCP**에서 **Linux Server**를 배포하고 연결하는데 성공했다.

## 6. Web Server 프로그램 설치하기

- A. 연결된 Linux Server에서 다음의 명령을 수행해서 apt list를 업데이트 하자.

**# apt update**

```
root@lab3-webserver:~# apt update
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [2,070
kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [413 k
B]
Get:7 http://archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages
[344 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en
[46.8 kB]
Get:9 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1
,735 kB]
Get:10 http://archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [
369 kB]
Get:11 http://archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages
[25.0 kB]
Get:12 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [1,7
26 kB]
Get:13 http://archive.ubuntu.com/ubuntu bionic-security/main Translation-en [322
kB]
Get:14 http://archive.ubuntu.com/ubuntu bionic-security/restricted amd64 Package
s [323 kB]
Get:15 http://archive.ubuntu.com/ubuntu bionic-security/restricted Translation-e
n [43.2 kB]
Get:16 http://archive.ubuntu.com/ubuntu bionic-security/universe amd64 Packages
[1,126 kB]
Get:17 http://archive.ubuntu.com/ubuntu bionic-security/universe Translation-en
[254 kB]
Get:18 http://archive.ubuntu.com/ubuntu bionic-security/multiverse amd64 Package
s [19.2 kB]
Fetched 9,068 kB in 6s (1,620 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
56 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@lab3-webserver:~#
```

- B. 터미널에서 다음의 명령어를 사용해서 **Apache Web Server**를 설치한다. 계속 설치를 진행할 것인가 묻는 곳에서 'y'를 넣고 Enter key를 누르거나 기본값으로 'Y'에 맞춰져 있기 때문에 그냥 Enter key를 넣어도 된다.

**# apt install apache2**

```
root@lab3-webserver:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom
  openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 56 not upgraded.
Need to get 1,729 kB of archives.
After this operation, 6,985 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- C. 설치가 완료되었다.

```
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...
Processing triggers for systemd (237-3ubuntu10.44) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
root@lab3-webserver:~#
```

- D. 이제 **Apache Web Server**가 제대로 설치됐는지 확인해 보자. 다음의 명령어를 입력한다.

# **apache2 -v**

```
root@lab3-webserver: ~
root@lab3-webserver:~# apache2 -v
Server version: Apache/2.4.29 (Ubuntu)
Server built: 2020-08-12T21:33:25
root@lab3-webserver:~#
```

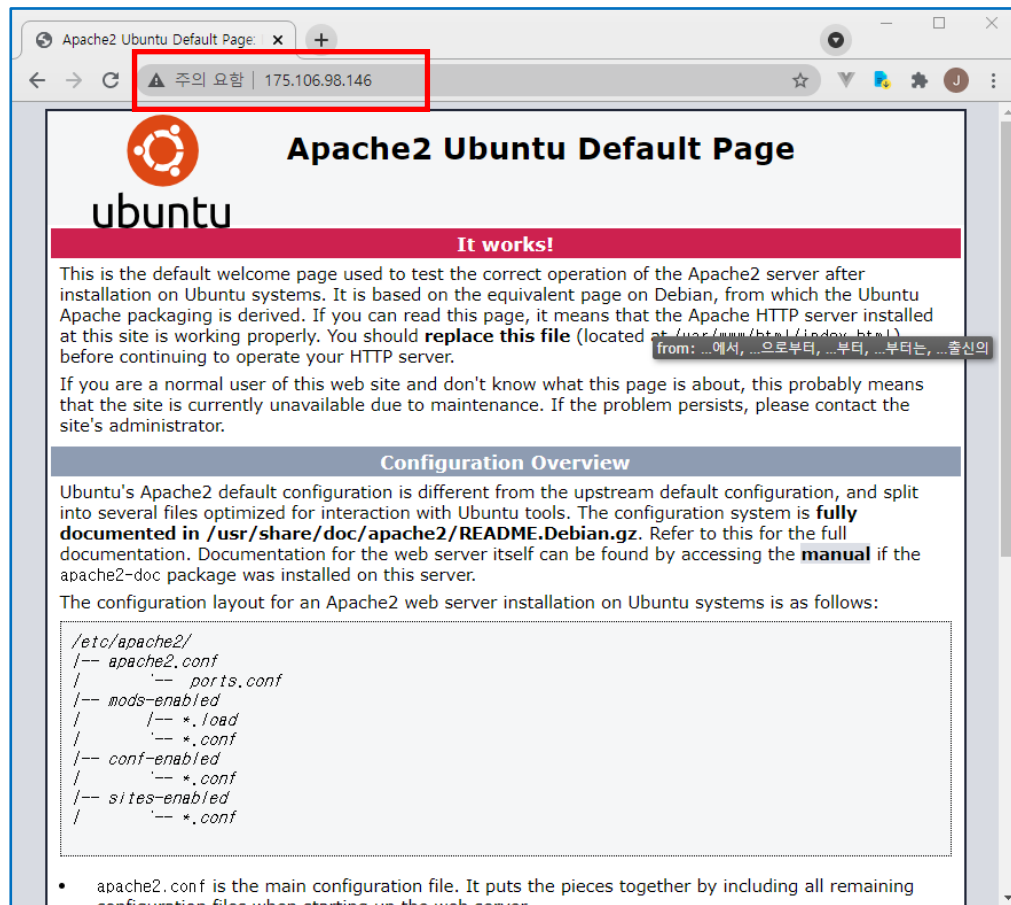
- E. 설치된 **Apache Web Server**가 제대로 구동되는지 확인해보자. 다음의 명령어로 확인할 수 있다.

# **netstat -ntlp**

```
root@lab3-webserver: ~
root@lab3-webserver:~# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
503/rpcbind
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
16437/apache2
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
709/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1014/sshd
root@lab3-webserver:~#
```

- F. **Linux Server**의 공인 IP 주소를 이용해서 웹브라우저로 접속해 보자. Linux Server의 [공용 IP 주소]를 복사하여 여러분의 웹브라우저를 열고 주소창에 복사한 주소를

붙여 넣는다. 그러면 아래 그림과 같이 **Apache Web Server**의 **Welcome** 화면을 확인하게 될 것이다.



- G. 해당 공인 IP 주소로 여러분의 노트북이나 데스크톱에서 명령 프롬프트창을 이용해서 PING test를 해도 잘 연결되는 것을 확인할 수 있다.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devex>ping 175.106.98.146

Ping 175.106.98.146 32바이트 데이터 사용:
175.106.98.146의 응답: 바이트=32 시간=5ms TTL=53
175.106.98.146의 응답: 바이트=32 시간=4ms TTL=53
175.106.98.146의 응답: 바이트=32 시간=4ms TTL=53
175.106.98.146의 응답: 바이트=32 시간=5ms TTL=53

175.106.98.146에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 4ms, 최대 = 5ms, 평균 = 4ms

C:\Users\devex>
```

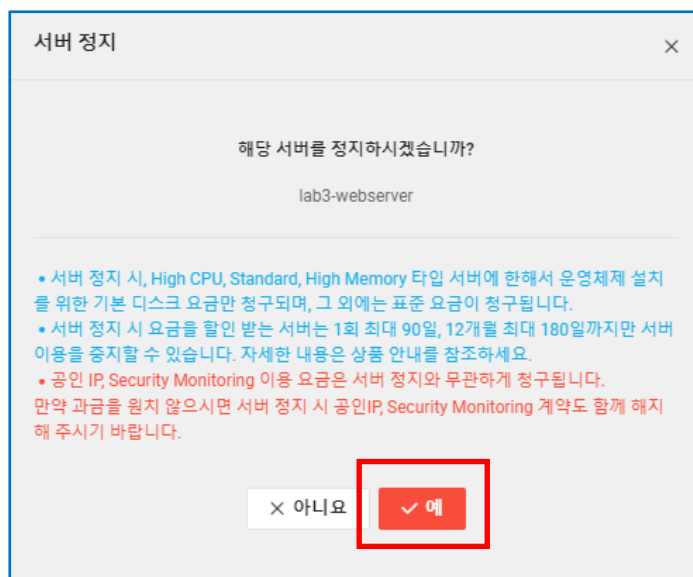


## 7. Linux 서버 시작, 중지 및 삭제하기

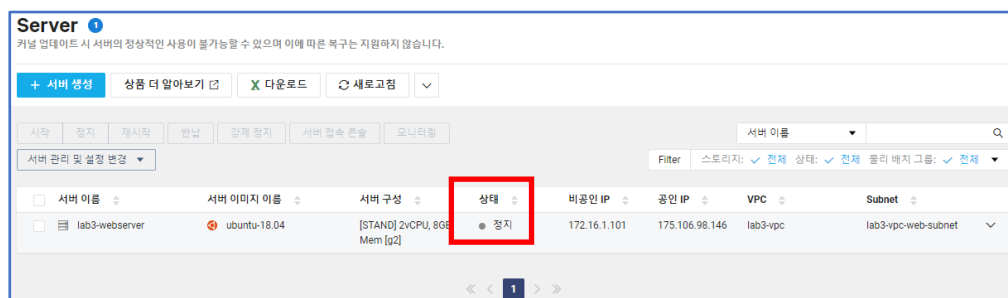
- A. 방금 생성한 Linux Server 서버를 중지시키기 위해서는 서버에 원격으로 접속한 다음 중지[Shut down]를 수행하거나, [Server] 페이지에서 해당 서버를 선택 후 [정지]를 선택하여 서버를 정지할 수 있다.



- B. [서버정지] 창에서, [예] 클릭하여 서버를 정지한다.



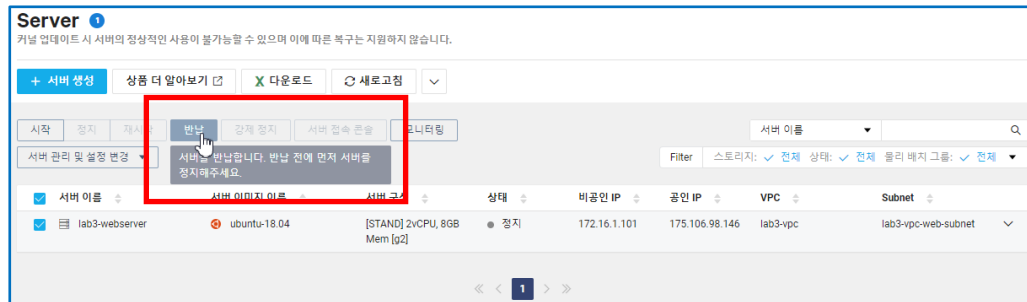
- C. 잠시 후 [Server] 페이지에서 해당 서버가 정지임을 확인할 수 있다. [PuTTY]에서 서버와의 연결은 자동으로 끊어진다.



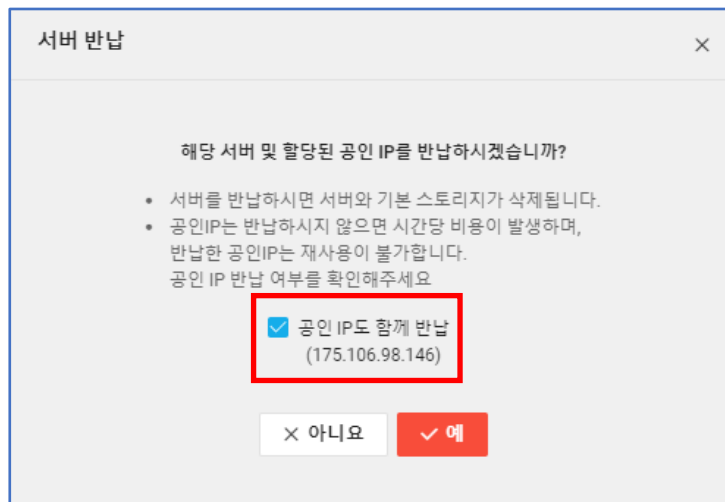


## 8. Linux Server 서버 반납하기

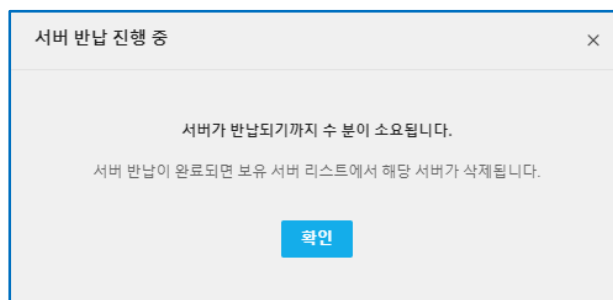
A. 이번에는 해당 서버를 반납해 보자. 서버를 선택하고 **[반납]** 버튼을 클릭한다.



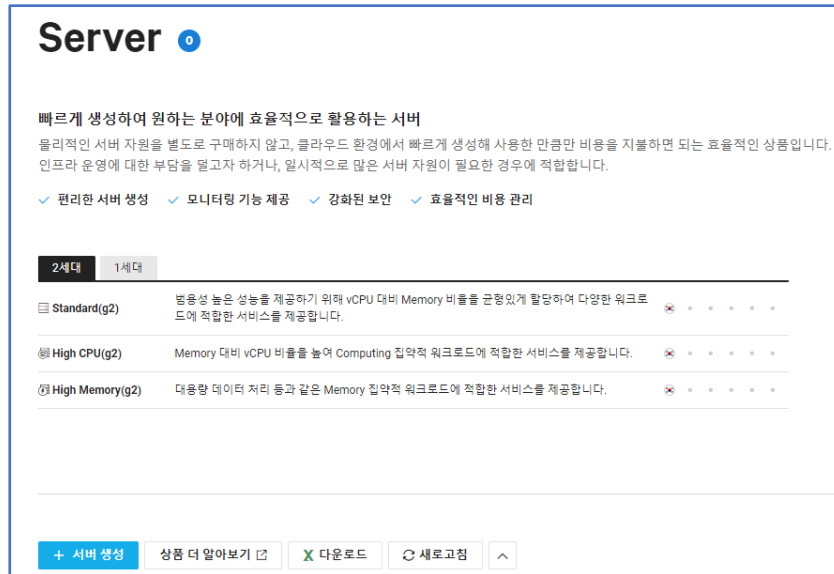
B. **[서버 반납]**창이 나타나면 아래의 그림과 같이 **[공인 IP도 함께 반납]** 체크박스 체크하고 **[예]**를 클릭하여 서버를 반납한다.



C. 서버 생성때와 마찬가지로 **[서버 반납 진행 중]**이라는 창이 나오며, 수분이 소요된다고 알림의 창이 나타난다.

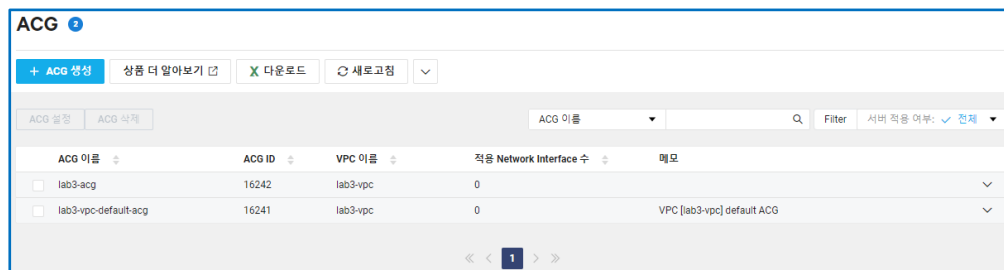


D. 잠시 뒤, 서버 반납이 이뤄지면 **[Server]** 처음 페이지로 돌아간다.

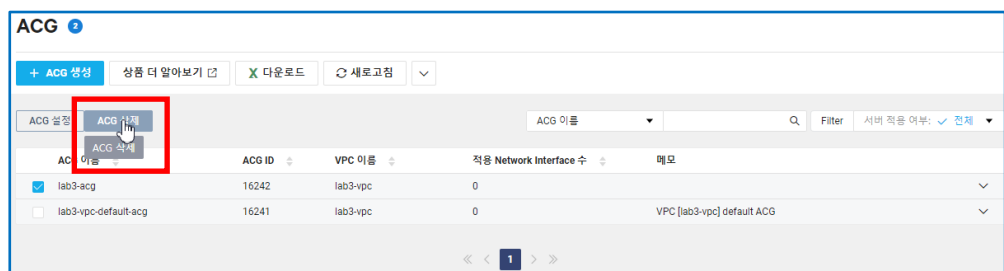


## 9. 나머지 Resource 자원 반납하기

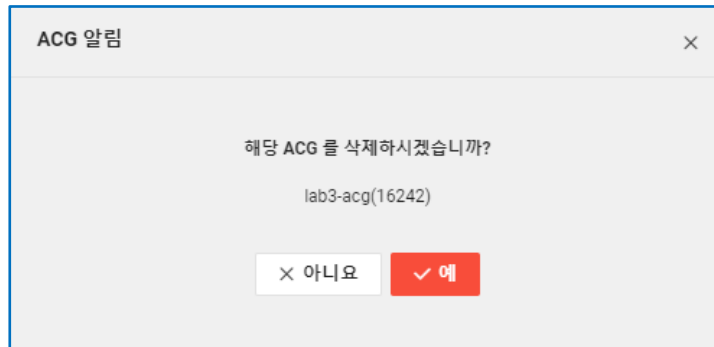
A. 이번 실습에서는 Linux Server만 생성한 것이 아니다. **[Compute]**에서는 아직 **ACG**도 남아있고, **[Networking]**에서는 **VPC, Subnet, Network ACL**도 있다. 먼저 **[Compute]**의 **ACG**를 삭제하자. 좌측 메뉴의 **[Server] > ACG** 메뉴를 클릭한다.



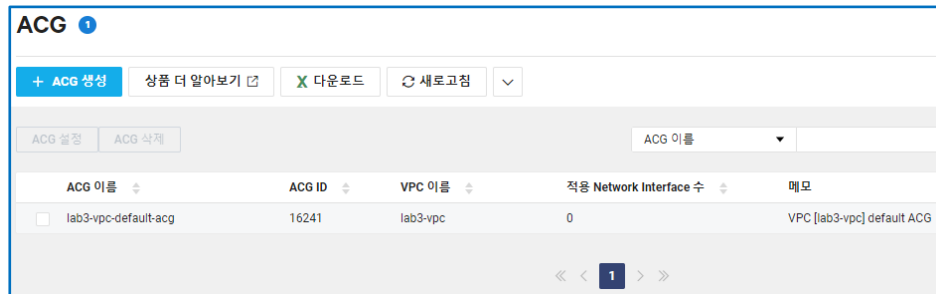
B. **Default-acg**는 삭제되지 않는다. 우리가 실습을 하면서 생성한 **lab3-acg**를 체크해서 선택한다. 그리고 **[ACG 삭제]** 버튼을 클릭한다.



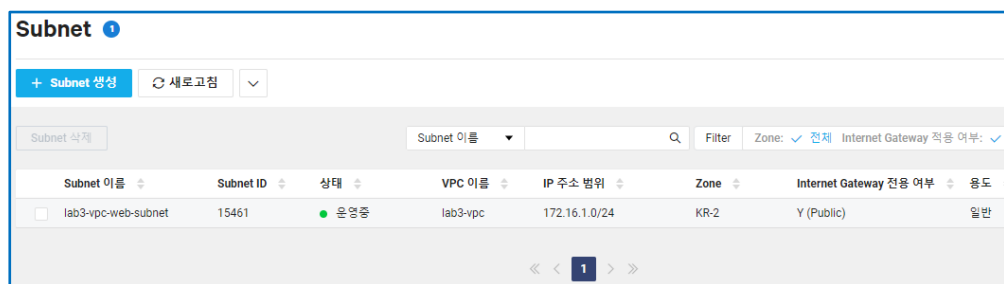
- C. **[ACG 알림]** 창에서 **[예]** 빨간색 버튼을 클릭하여 우리가 실습을 통해 생성한 ACG를 삭제한다.



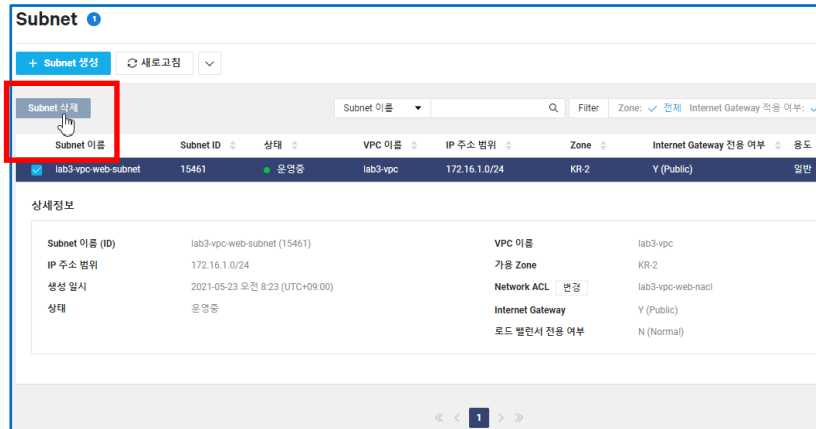
- D. 삭제에 성공하면 default-acg만 목록에 남는다.



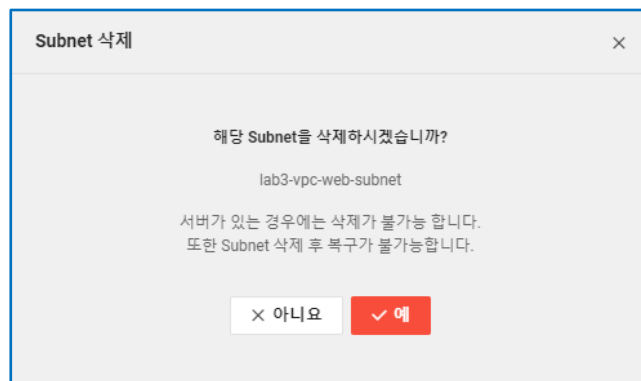
- E. 이제 **[Networking]** 쪽 자원도 삭제한다. 좌측메뉴에서 **[VPC]**의 **[Subnet Management]**를 클릭한다 .



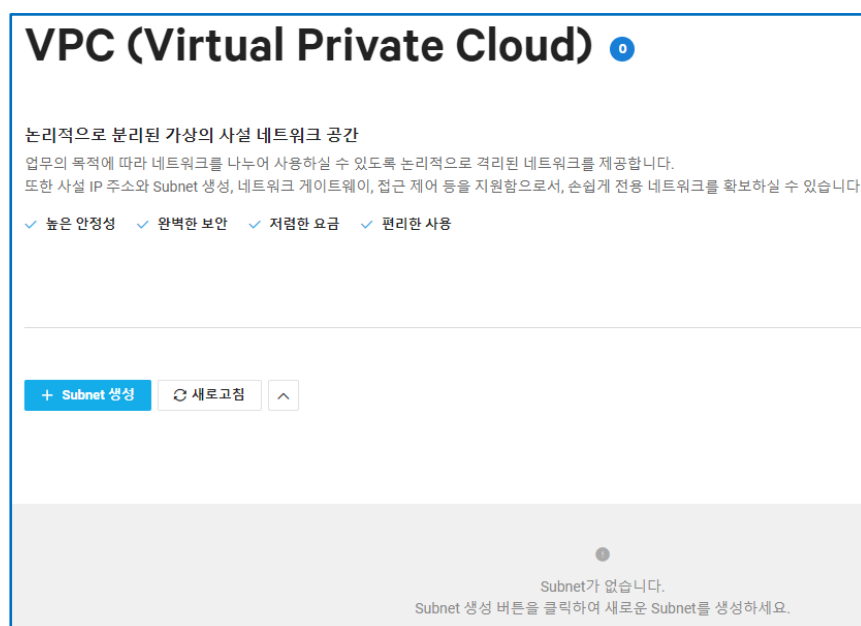
- F. 이번 실습에서 생성한 **lab3-vpc-web-subnet**을 체크해서 선택한 다음, **[Subnet 삭제]** 버튼을 클릭한다.



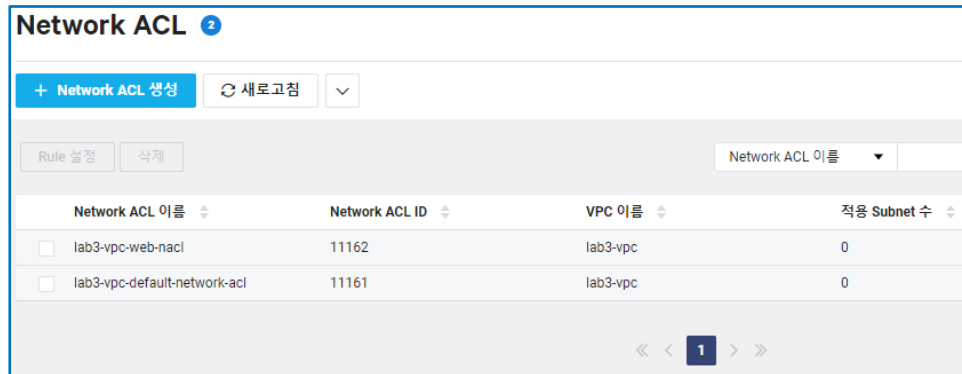
G. [Subnet 삭제] 창이 나타난다. 삭제를 위해 [예] 빨간색 버튼을 클릭한다.



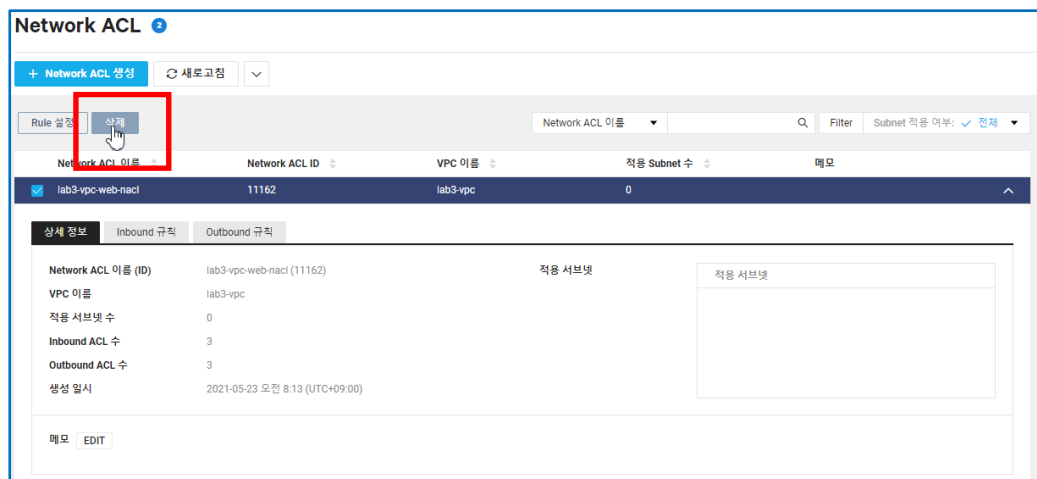
H. Subnet이 삭제 성공하면 초기 화면으로 돌아간다.



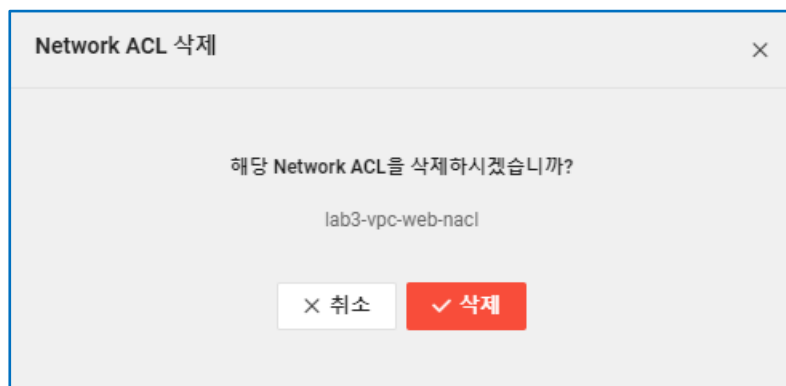
- I. [Network ACL]을 삭제하기 위해 좌측메뉴에서 [VPC] > [Network ACL] > [ACL Rule]를 클릭한다.



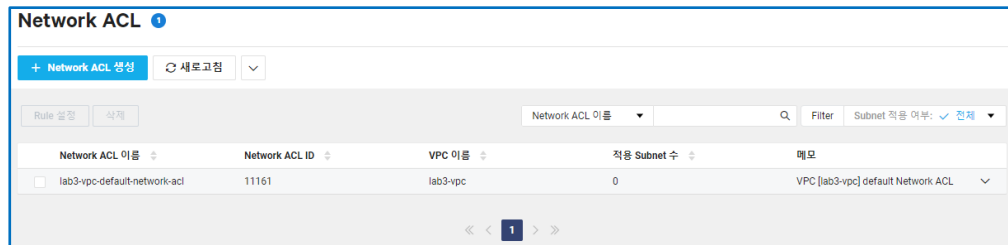
- J. 역시 **default-acl**은 삭제되지 않는다. 우리가 실습을 통해 생성한 **lab3-vpc-web-nacl**을 체크해서 선택한 다음 [삭제] 버튼을 클릭한다.



- K. [Network ACL 삭제]창이다. [삭제] 빨간색 버튼을 클릭하여 삭제한다 .



- L. 삭제 성공하면 **default-acl**만 목록에 남는다.



Network ACL 1

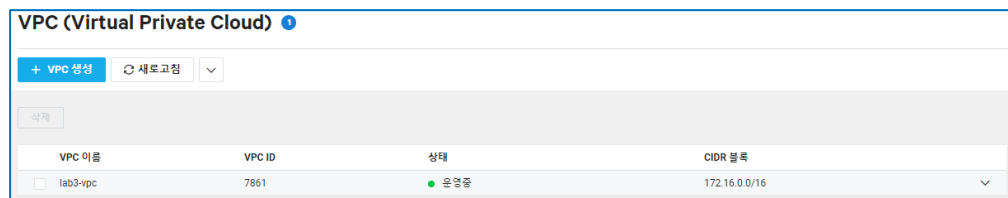
+ Network ACL 생성 새로고침

Rule 설정 삭제 Network ACL 이름 Filter Subnet 적용 여부: 전체

Network ACL 이름	Network ACL ID	VPC 이름	적용 Subnet 수	메모
lab3-vpc-default-network-acl	11161	lab3-vpc	0	VPC [lab3-vpc] default Network ACL

<< 1 >>

- M. 이번에는 **VPC**를 삭제해 본다. 좌측메뉴에서 **[VPC] > [VPC Management]** 메뉴를 클릭한다.



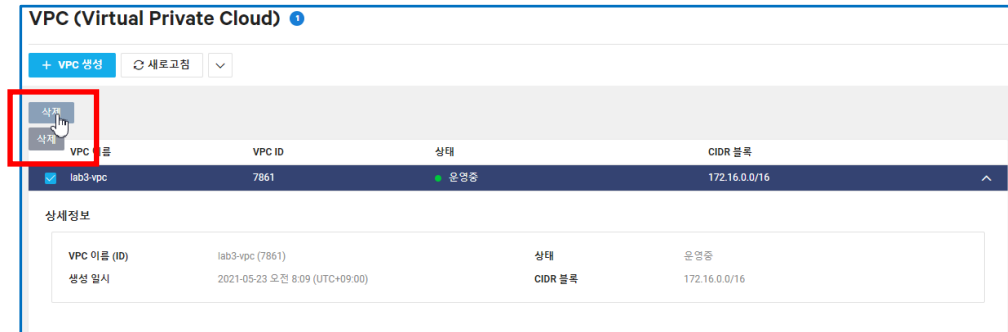
VPC (Virtual Private Cloud) 1

+ VPC 생성 새로고침

삭제

VPC 이름	VPC ID	상태	CIDR 블록
lab3-vpc	7861	● 운영중	172.16.0.0/16

- N. 실습에서 생성했던 **lab3-vpc**를 체크해서 선택한 다음, **[삭제]** 버튼을 클릭하자.



VPC (Virtual Private Cloud) 1

+ VPC 생성 새로고침

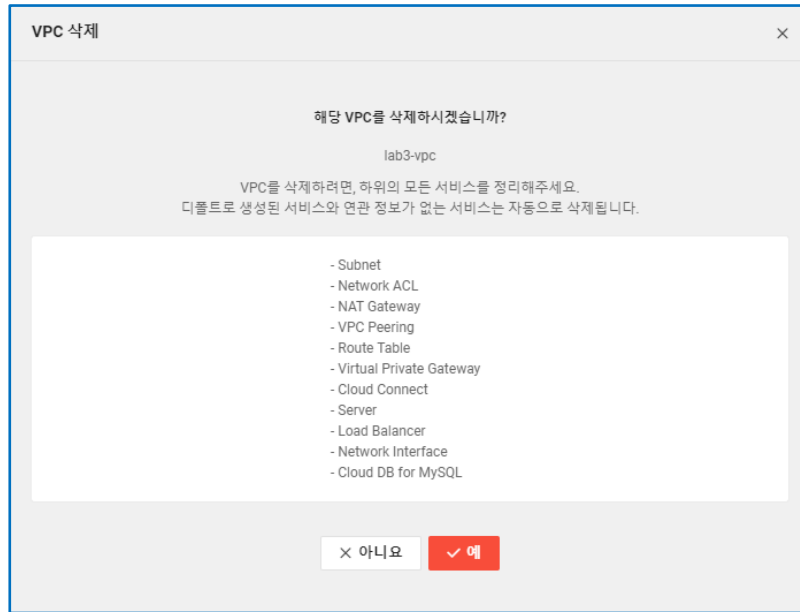
삭제 삭제

VPC 이름	VPC ID	상태	CIDR 블록
lab3-vpc	7861	● 운영중	172.16.0.0/16

상세정보

VPC 이름 (ID)	lab3-vpc (7861)	상태	운영중
생성 일시	2021-05-23 오전 8:09 (UTC+09:00)	CIDR 블록	172.16.0.0/16

- O. **[VPC 삭제]** 창이 나타난다. 여기서 목록에 있는 내용을 보고 혹시 미처 삭제하지 못한 자원이 있는지 확인하고 없으면 **VPC**를 삭제하기 위해 **[예]** 빨간색 버튼을 클릭한다.



P. 삭제에 성공하면 [보유중인 VPC가 없습니다.] 화면을 보게 된다.

