

NAVER Cloud Platform Lab Guide

핸즈온(Hands-on) 과정

NAVER Cloud Platform

2023.08

Lab 1 : 서버 생성 및 접속 (15 분)

1. 웹 서버를 위한 VPC 및 Subnet 만들기

"Product & Services > VPC > VPC Management 선택 > +VPC 생성" 선택

"VPC 이름" 에 lab1-vpc 라고 입력

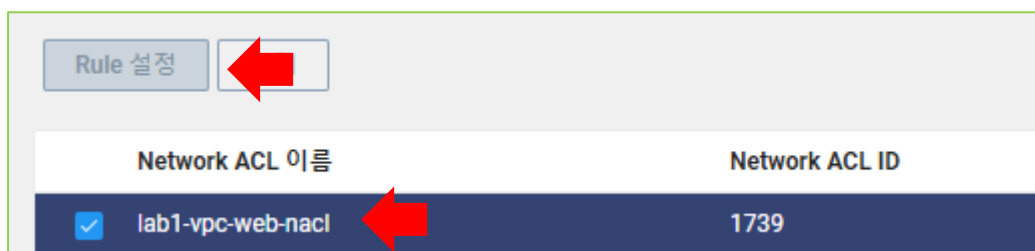
"IP 주소 범위" 에 10.0.0.0/16 라고 입력 후 생성 클릭

"Product & Services > VPC > Network ACL > +Network ACL 생성" 선택

"Network ACL 이름"에 lab1-vpc-web-nacl 라고 입력

"VPC"는 lab1-vpc 선택 후 생성 클릭

"lab1-vpc-web-nacl"을 선택 후, 상단 "Rule 설정" 클릭



*Inbound 규칙 설정

우선순위: 0, 프로토콜: ICMP, 접근 소스: 0.0.0.0/0, 허용여부: 허용 선택 후, "+추가" 클릭

우선순위: 1, 프로토콜: TCP, 접근 소스: 0.0.0.0/0, 포트: 80, 허용여부: 허용 선택 후, "+추가" 클릭

우선순위: 2, 프로토콜: TCP, 접근 소스: myIp, 포트: 22, 허용여부: 허용 선택 후, "+추가" 클릭

우선순위: 197, 프로토콜: TCP, 접근소스: 0.0.0.0/0, 포트: 22, 허용여부: 차단 선택 후, "+추가" 클릭

상세 정보	Inbound 규칙	Outbound 규칙			
우선순위	프로토콜	접근 소스	포트	허용여부	
0	ICMP	0.0.0.0/0 (전체)		허용	
1	TCP	0.0.0.0/0 (전체)	80	허용	
2	TCP	125.178.208.204/32	22	허용	
197	TCP	0.0.0.0/0 (전체)	22	차단	

***Outbound 규칙 설정**

우선순위: 0, 프로토콜: ICMP, 접근 소스: 0.0.0.0/0, 허용여부: 허용 선택 후, "+추가" 클릭

우선순위: 1, 프로토콜: TCP, 접근 소스: 0.0.0.0/0, 포트: 1-65535, 허용여부: 허용 선택 후, "+추가" 클릭

우선순위: 2, 프로토콜: UDP, 접근 소스: 0.0.0.0/0, 포트: 1-65535, 허용여부: 허용 선택 후, "+추가" 클릭

상세 정보	Inbound 규칙	Outbound 규칙			
우선순위	프로토콜	목적지	포트	허용여부	
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	

"Product & Services > VPC > Subnet Management 선택 > +Subnet 생성" 선택

다음과 같이 내용 설정 후 생성 클릭

*Subnet 이름 : lab1-vpc-web-sub1

*VPC : lab1-vpc 선택

*IP 주소 범위 : 10.0.1.0/24

*가용 Zone : KR-2

*Network ACL : lab1-vpc-web-nacl 선택

*Internet Gateway 전용 여부 : Y (Public) 선택

*용도 : 일반 선택

Subnet 이름

lab1-vpc-web-sub1

VPC

lab1-vpc (10.0.0.0/16)

IP 주소 범위

10.0.1.0/24

가용 Zone

KR-2

Network ACL

lab1-vpc-web-nacl

Internet Gateway 전용 여부

☒ Y (Public)
 ☐ N (Private)

용도

☒ 일반
 ☐ LoadBalancer

일반서버에서만 사용 가능한 서브넷입니다.

2. 웹서버 ACG 만들기

“Product & Services > Server > ACG 선택 > +ACG 생성” 선택

“ACG 이름” 에 lab1-acg 입력

“VPC”에 lab1-vpc 선택 후 하단 “생성” 클릭

‘lab1-acg’ ACG를 선택 후 상단의 “ACG 설정”을 선택합니다.

*Inbound 규칙 설정

프로토콜 : ICMP, 접근 소스 : 0.0.0.0/0 입력 후, “+추가” 클릭

프로토콜 : TCP, 접근 소스 : 0.0.0.0/0 허용 포트 (서비스) : 80 입력 후, “+추가” 클릭

프로토콜 : TCP, 접근 소스 : myip 허용 포트 : 22 선택 후, “+추가” 클릭

프로토콜 : TCP, 접근 소스 : mylp 허용 포트 : 3389 선택 후, "+추가" 클릭

*Outbound 규칙 설정

프로토콜 : ICMP, 목적지 : 0.0.0.0/0 입력 후, "+추가" 클릭

프로토콜 : TCP, 목적지 : 0.0.0.0/0 허용 포트 : 1-65535 입력 후, "+추가" 클릭

프로토콜 : UDP, 목적지 : 0.0.0.0/0 허용 포트 : 1-65535 입력 후, "+추가" 클릭

하단의 "적용" 버튼 클릭

상세 정보	Inbound 규칙	Outbound 규칙
프로토콜	접근 소스	허용 포트
ICMP	0.0.0.0/0	
TCP	125.178.208.204/32	22
TCP	0.0.0.0/0	80

상세 정보	Inbound 규칙	Outbound 규칙
프로토콜	목적지	허용 포트
TCP	0.0.0.0/0	1-65535
UDP	0.0.0.0/0	1-65535
ICMP	0.0.0.0/0	

3. 초기화 스크립트 만들기

"Product & Services > Server > Init Script > + Script 생성" 선택합니다.

스크립트 이름 : lab-script

OS 타입 : Linux

"Script" 항목 내용에 하기 교본 Box의 내용을 복사하여 붙여넣음

스크립트의 내용은 서버 부팅 후 아파치 웹서버와 PHP를 설치하고 테스트 페이지를 다운받은 후,

설정 내용을 수정 후 아파치 웹서버를 기동하는 스크립트입니다.

```
#!/bin/bash
yum -y remove mariadb-libs
yum -y install httpd php mysql php-mysql
systemctl enable httpd
cd /var/www/html
wget http://211.249.50.207/lab/lab.tgz
tar xvfz lab.tgz
cat phpadd >> /etc/httpd/conf/httpd.conf
systemctl start httpd
```

서버 생성 시 자동으로 실행되는 스크립트를 사용자가 직접 생성할 수 있습니다.
사용자 Script로 인해 발생한 인프라 장애는 서비스 고객센터에서 처리할 수 없습니다.

(● 필수 입력 사항입니다.)

Script 이름

OS 타입 ☒ Linux ☐ Window

설명

Script

```
#!/bin/bash
yum -y install httpd php
chkconfig httpd on
cd /var/www/html
wget http://211.249.50.207/lab/lab.tgz
tar xvfz lab.tgz
cat phpadd >> /etc/httpd/conf/httpd.conf
/etc/rc.d/init.d/httpd start
```

0 / 1000 Bytes

0.2 / 1024 Kbytes

* Linux 환경에서는 Python, Perl, Shell 등의 스크립트를 사용할 수 있습니다.
- 단 첫 줄에 #!/usr/bin/env python, #!/bin/perl, #!/bin/bash 등과 같은 형태로 실행하고자 하는 스크립트 경로를 지정해야 합니다.
* Windows 환경에서는 Visual Basic 스크립트만 작성할 수 있습니다.
- 단, 스크립트의 내용은 영문으로만 작성해야 합니다.

4. 웹서버 만들기

“Product & Services > Server > + 서버생성” 클릭

“서버 이미지 이름” 에서 **Centos-7.8-64** , 우측의 “다음 >”을 클릭

서버 이미지 이름	설명
 centos-7.3-64	CentOS 7.3 (64-bit) (커널 업데이트 시 서버의 정상적인 사용이 불가능할 수 있으며 이에 따른 복구는 지원하지 않습니다.)
 centos-7.8-64	CentOS 7.8 (64-bit) (커널 업데이트 시 서버의 정상적인 사용이 불가능할 수 있으며 이에 따른 복구는 지원하지 않습니다.)
 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.)

“VPC”와 “Subnet”은 앞에 만든 것으로 선택합니다.

“서버 타입”은 “Standard” , “vCPU 2개, 메모리 8GB, 디스크 50GB” 를 선택

“서버 개수”는 1, “서버 이름”은 lab1-org1 를 입력

“Network Interface”는 new interface 선택, IP는 10.0.1.101 을 입력 후, “+추가” 클릭

“Script 선택”에서 앞에서 저장한 lab-script 를 선택, “다음 >” 클릭

VPC lab1-vpc VPC 생성

Subnet lab1-vpc-web-sub1 | KR-2 | 10.0.1.0/24 | Public Subnet 생성

공인 IP 연결을 위해서는 반드시 Public Subnet을 선택해야 합니다.

스토리지 종류 ☒ SSD ☐ HDD

서버 타입 Standard

[Standard] vCPU 2개, 메모리 8GB, [SSD]디스크 50GB [g2s2-g2-

스토리지 암호화 적용 ☐

암호화 기본 스토리지(OS)가 적용된 서버에는 암호화된 추가 스토리지만 연결할 수 있습니다.
마찬가지로, 암호화 되지 않은 기본 스토리지가 적용된 서버는 암호화 적용되지 않은 추가 스토리지만 연결 가능합니다.

요금제 선택 ☒ 월요금제 ☐ 시간 요금제 월 88,000원 (OS 제외)

서버 개수 1

서버 이름 lab1-org1

☒ 입력하신 서버 이름으로 hostname을 설정합니다.

Network Interface

디바이스	Network Interface	Subnet	IP
eth1	new interface	- select -	미입력시 지 + 추가
eth0	new interface	lab1-vpc-web-sub1 KR-2 10.0.1.0/24 Public	10.0.1.101/32 ✕

블리 배치 그룹 ☐

반납 보호 ☐ 설정 ☒ 해제

반납 보호를 설정하면 실수로 반납하는 사고를 방지할 수 있습니다.

메모

0 / 1000 Bytes

Script 선택 lab-script

스토리지 정보 기본 설정으로 두고 “다음 >” 클릭

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

스토리지 설정

서버의 블록 스토리지 스택을 설정합니다.
블록 스토리지 요금은 생성 시점부터 요금이 과금되므로, 사용하지 않을 때는 반드시 반납하시기를 권장드립니다. (• 필수 입력 사항입니다.)

+ 스토리지 추가

순번	스토리지 이름	스토리지 유형	스냅샷 이름	크기(GB)	스토리지 타입	IOPS	스토리지 암호화 적용
0	lab1-org1의 기본 스토리지	기본 스토리지	-	50	SSD	4000	N

“새로운 인증키 생성”에서 인증키 이름에 NCP오늘날짜 (예, ncp20200325)을 입력하고 인증키 생성 및 저장을 클릭합니다.

네트워크 접근 설정에서 디바이스 “eth0” 에 lab1-acg 를 선택

- ACG는 네트워크 디바이스 마다 할당이 가능하며, 1개의 네트워크 디바이스 당 최대 3개의 ACG 매핑 가능
서버 생성을 클릭하면 서버가 만들어집니다.

✓ 서버 이미지 선택

✓ 서버 설정

✓ 인증키 설정

✓ 방화벽 설정

5 최종 확인

[서버 생성] 버튼을 클릭하면 서버가 생성됩니다.

서버 이미지

서버 이미지 이름	centos-6.6-64	서버 이미지 설명	CentOS 6.6 (64-bit)
-----------	---------------	-----------	---------------------

서버

스토리지 종류	SSD	서버 이름	lab1-org
서버 타입	[Standard] vCPU 2개, 메모리 4GB, [SSD]디스크 50GB	요금제	월요금제
Region	한국	메모	
Zone	KR-1	반납 보호	해제

인증키

인증키 이름	NCP-lab
--------	---------

Access Control Group

ACG 이름	lab1-acg(21563)
--------	-----------------

Script 선택

lab-script	상세내용
------------	------

< 이전

✓ 서버 생성

5. 공인 IP 설정

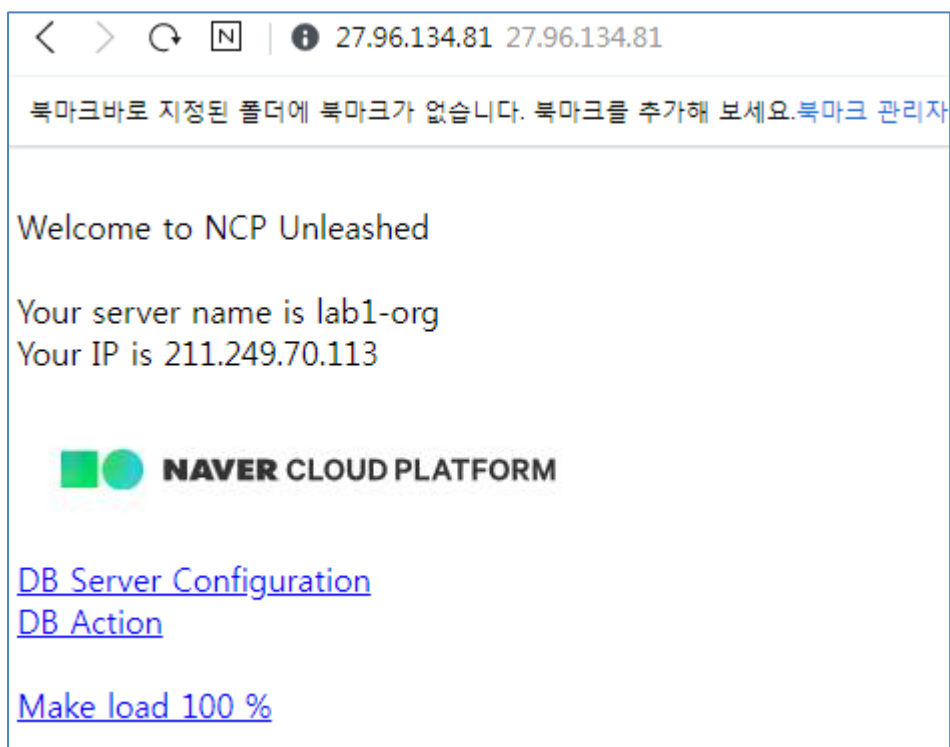
먼저 서버 탭에서 좌측 메뉴의 “Public IP”를 선택합니다.

상단의 “공인 IP 신청”을 선택합니다.



“적용 서버 선택”에 lab1-org1을 선택합니다.

웹 브라우저를 이용해 부여 받은 공인 IP로 접근해봅니다.



6. Lab1-org에 추가 스토리지 추가

Lab1-org 서버를 선택한 후 상단 메뉴의 서버 관리 및 설정 변경을 선택 후 스토리지 추가 선택

“스토리지 종류”: SSD

“스토리지 이름”: lab1-org-disk1

“크기” : 10GB

스토리지 추가

스토리지 이름과 크기를 입력해 주세요.

(필수 입력 사항입니다.)

서버 이름: lab1-org

스토리지 종류: ☐ HDD ☒ SSD

스토리지 이름: lab1-org-disk1

스냅샷 선택: (선택 없음)

크기: 10 GB

Max IOPS: 4000

메모: 0 / 1000 Bytes

서버를 클릭하면 스토리지가 생성된 것을 확인할 수 있습니다.

<input type="checkbox"/>	서버 이름	서버 이미지 이름	서버 구성	상태
<input type="checkbox"/>	lab1-clone	centos-6.6-64	[Standard] 2vCPU, 4GB Mem	● 운영중
<input checked="" type="checkbox"/>	lab1-org	centos-6.6-64	[Standard] 2vCPU, 4GB Mem	● 운영중

상세정보

서버 이름 (Instance ID)	lab1-org (498006)
상태	운영중
생성 일시	2017-10-11 오후 3:22
구동 일시	2017-10-11 오후 3:25
비공인 IP	10,33,45,42
담당자 <input type="button" value="EDIT"/>	Account
모니터링 <input type="button" value="📊"/>	기본
인증키 <input type="button" value="🔑"/>	NCP-KEY
스토리지 <input type="button" value="📁"/>	[SSD] lab1-org 의 기본 스토리지 50 GB /dev/xvda [SSD] lab1-org-disk1 10 GB /dev/xvdb

7. 이미지 생성

Lab1-org1 서버를 선택한 후, “상단의 서버 관리 및 설정 변경” 에서 “내 서버 이미지” 선택

서버 이미지 이름 : lab1-org-image

내 서버 이미지 생성

서버의 모든 스토리지를 서버 이미지로 생성합니다.

생성된 서버 이미지는 동일한 데이터를 가지는 새로운 서버를 생성하는데 활용됩니다.(단, 부팅 디스크 크기는 동일)

필수 입력 사항입니다.

서버 이름

lab1-org

서버 이미지 크기

60GB

서버 이미지 이름

lab1-org-image

메모

0 / 1000 Bytes

취소

생성

"Server > Server Image" 메뉴에서 lab1-org-image가 만들어진 것을 확인할 수 있습니다.

Server / [Server Image](#)

Server Image

특정 사점 서버의 전체 내용과 구조를 보관합니다.

+ 서버 생성

상품 더 알아보기

X 다운로드

↺ 새로고침

▼

개선안내

[Server] Image Builder 기능 추가 안내

더보기

서버 이미지 삭제

다른 리전으로 복제

필터

OS: [전체](#)

<input type="checkbox"/> 서버 이미지 이름	OS	상태	원본 서버 이름	생성 일시
<input checked="" type="checkbox"/> lab1-org-image	[영문] Windows Server 2012(64bit) R2	● 생성됨	lab1-org	2018-04-12 오전 10:50

상세정보

서버 이미지 이름 (Instance ID)

lab1-org-image (6566)

원본 서버 이미지 이름

win-2012-64-R2-en

원본 서버 이름

lab1-org

출 크기

60GB

설명 수정

8. 내 서버 이미지로 서버 만들기

Lab1-org-image 이미지를 이용하여 lab1-org1와 동일한 서버를 만들고자 합니다.

"Compute > Server > Server Image"에서 lab1-org-image를 선택하고 상단 메뉴의 "+서버생성"을 클릭합니다.

서버 이름 : lab1-org2

Network Interface IP : 10.0.1.102

Script 선택 : 선택 안함

나머지 설정/스펙은 lab1-org1 과 동일하게 설정합니다.

VPC

lab1-vpc

VPC 생성

Subnet

lab1-vpc-web-sub1 | KR-2 | 10.0.1.0/24 | Public

Subnet 생성

공인 IP 연결을 위해서는 반드시 Public Subnet을 선택해야 합니다.

스토리지 종류

☒ SSD
 ☐ HDD

서버 타입

Standard

[Standard] vCPU 2개, 메모리 8GB, [SSD]디스크 50GB [g2]s2-g2-

요금제 선택

☒ 월요금제
 ☐ 시간 요금제
 월 88,000원 (OS 제외)

서버 개수

1

서버 이름

lab1-org2

☒ 입력하신 서버 이름으로 hostname을 설정합니다.

Network Interface

디바이스	Network Interface	Subnet	IP
eth1	new interface	- select -	미입력시 지
eth0	new interface	lab1-vpc-web-sub1 KR-2 10.0.1.0/24 Public	10.0.1.102/32

블리 배치 그룹

☐

반납 보호

☐ 설정
 ☒ 해제

반납 보호를 설정하면 실수로 반납하는 사고를 방지할 수 있습니다.

메모

0 / 1000 Bytes

Script 선택

선택없음

인증키는 '보유하고 있는 인증키 이용'을 클릭한 후, lab1-org 서버 생성시에 다운받은 인증키를 선택합니다.

ACG는 lab1-acg를 선택합니다.

Lab 2 : DNS와 로드 밸런서 구성 (15분)

1. 로드 밸런서를 위한 Subnet 생성

“VPC > Subnet Management” 상단의 “+Subnet 생성” 선택

다음과 같이 내용 설정 후 생성 클릭

“Subnet 이름” : lab1-vpc-lb-sub1

“VPC” : lab1-vpc

“IP 주소 범위” : 10.0.2.0/24

“가용 Zone” : KR-2

“Network ACL” : lab1-vpc-web-nacl

“Internet Gateway 전용 여부” : N (private)

“용도” : LoadBalancer

2. 타겟 그룹 생성

“Target Group 이름” : lab-tg

“Target 유형” : VPC Server

“VPC” : lab1-vpc

“프로토콜” : HTTP

“포트” : 80

Target Group 생성

생성할 Target Group의 이름을 입력하고 Target 유형과 포함될 Target의 VPC를 선택해주세요.
프로토콜에 따라 연결 가능한 로드밸런서 유형이 다릅니다. (필수 입력 사항입니다.)

Target Group 이름	lab-tg
Target 유형	VPC Server
VPC	lab1-vpc (10.0.0.0/16)
프로토콜	HTTP
포트	80
메모	

0 / 1000 Bytes

[Health check 설정]

“프로토콜” : HTTP

“포트” : 80

“URL Path” : /

“HTTP Method” : HEAD

“HTTP Check 주기 (초)” : 30

“정상/실패 임계값” : 2

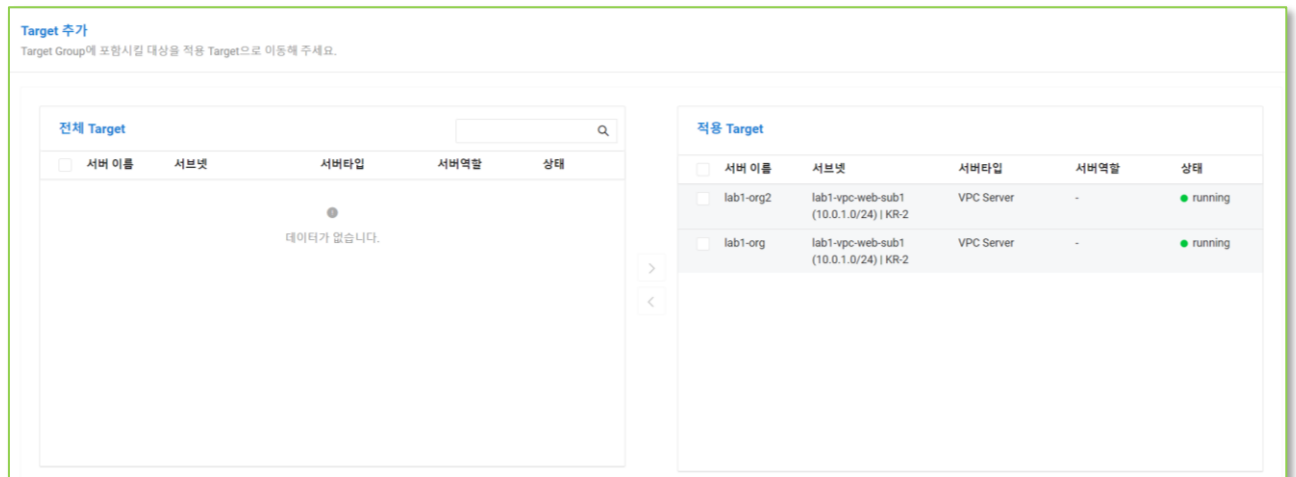
Health Check 설정

Target에 대한 Health Check를 위한 정보를 입력하세요.
Health Check에 실패한 서버는 로드밸런싱 대상에서 제외됩니다. (필수 입력 사항입니다.)

프로토콜	HTTP
포트	80
URL Path	/
HTTP Method	HEAD
Health Check 주기 (초)	30
정상 임계값	2
실패 임계값	2

[Target 추가]

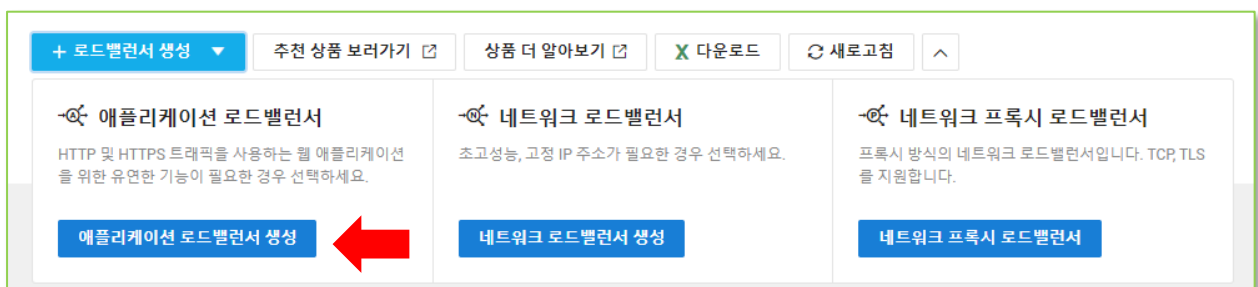
적용 Target에 서버 lab1-org, lab1-org2 이동



3. 로드 밸런서 생성

웹 서비스의 가용성을 확보하기 위한 로드 밸런서를 구성하고자 합니다.

“Product & Services > Networking > Load Balancer” 를 선택합니다. 그리고 상단의 “+ 로드 밸런서 생성” 선택 항목 중, “애플리케이션 로드밸런서 생성”을 클릭합니다.



다음과 같이 로드밸런서를 설정합니다

“로드 밸런서 이름”: lab-lb

“Network” : Public IP

“부하 처리 성능”: Small

“대상 VPC” : lab1-vpc

“서브넷 선택”: KR-2 / lab1-vpc-lb-sub1

유형 Application

로드밸런서 이름

Network ☐ Private IP ☒ Public IP

부하 처리 성능 ☒ Small ☐ Medium ☐ Large

대상 VPC

서브넷 선택 ☒ KR-2 ☐ KR-1

[서브넷 생성](#)

“리스너 설정”은 디폴트 값을 “+추가” 합니다.

프로토콜	로드밸런서 포트	서버프로토콜	서버포트	L7 Health Check	HTTP/2	Sticky Session	설정
HTTP	80	HTTP	80	/	<input type="checkbox"/>	<input type="checkbox"/>	+ 추가
HTTP	80	HTTP	80	/	<input type="checkbox"/>	<input type="checkbox"/>	× 삭제

“Target Group 선택”서 “전체서버” 리스트에서 “lab1-org1”과 “lab1-org2”를 ‘적용서버’ 항목으로 추가합니다.

Target Group 선택
적용할 Target Group을 선택해주세요.
로드밸런서 타입에 따라 선택할 수 있는 프로토콜이 제한됩니다.

Target Group [Target Group 생성](#)

Target Group 설정

Target Group 이름	lab2-tg	Target 유형	VPC Server
프로토콜	HTTP	포트	80

Health Check 설정

프로토콜	HTTP	포트	80
URL Path	/	검사 주기	30

적용 Target

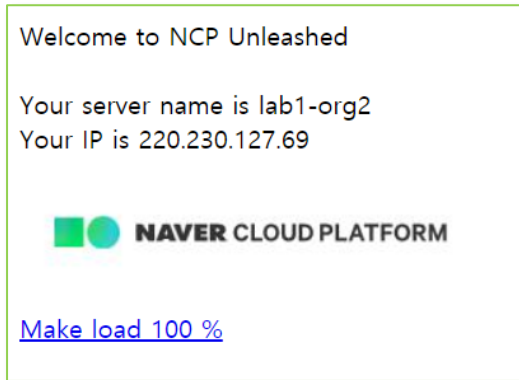
Target 타입	서버 이름	서브넷	서버역할	상태
VPC Server	lab2-org2	lab2-vpc-web-sub1 (10.0.1.0/24) KR-2	-	● running
VPC Server	lab2-org1	lab2-vpc-web-sub1 (10.0.1.0/24) KR-2	-	● running

정상적으로 적용이 되면 다음과 같이 상태는 운영 중으로 나오게 됩니다.

로드 밸런서에 접속하기 위해서는 ‘접속정보’ 항목(도메인 이름)을 복사하여 웹 브라우저 주소창에 입력합니다.

로드밸런서 설정 변경	서브넷 변경	리스너 설정 변경	인증서 변경	적용 서버 변경	로드밸런서 삭제	모니터링	로드밸런서 상태 확인
<input checked="" type="checkbox"/> 로드밸런서 이름	상태	네트워크	VPC	유형	접속 정보	서버 대수	메모
<input checked="" type="checkbox"/> lab-lb	● 운영중		lab1-vpc	APPLICATION	lab-lb-5192271-ed579ce4f c52.kr.lb.navercloud.com	2 대	^

웹 브라우저에서 접속하여 새로고침을 누르면, LB 기능으로 인해 lab1-org1 과 lab1-org2 서버에 분산되어 접속하게 되는 것을 확인할 수 있습니다.

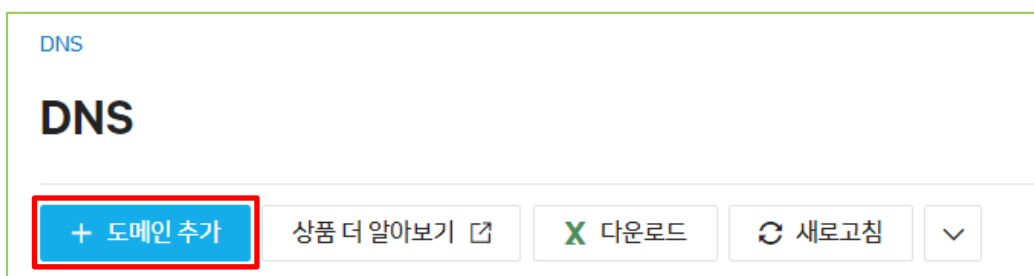


2. 도메인 등록 (demo)

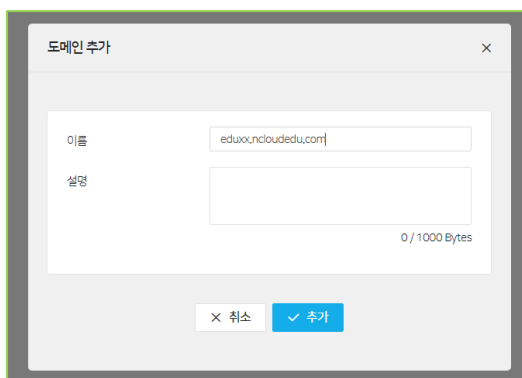
사전에 ncloudedu.com 도메인이 등록되어 있고 ncloudedu.com에서 교육 계정별도 도메인을 생성하여 위임하였습니다.

따라서, 도메인 등록기관에서 도메인을 등록하는 과정은 완료되었으며 LAB에서는 도메인을 등록하고 호스트를 등록하겠습니다.

"Products & Services > Networking > Global DNS" 에서 "+ 도메인 추가" 선택



도메인 "이름" 에 계정명.ncloudedu.com 입력 → (예시) edu01.ncloudedu.com



다음과 같이 네임서버 기본 정보가 채워진 것을 확인



3. 서버를 등록

“Global DNS > Record” 메뉴의 ‘DNS’ 에서 상단의 “레코드 추가”를 클릭

레코드명 : server1

레코드타입 : A

레코드값 : lab1-org1 서버 공인 IP (서버 정보에서 앞에서 부여한, 공인IP 값)



입력 후, 화면 하단 “추가”선택

웹브라우저에서 server1.eduxx.ncloudedu.com 으로 접속 확인

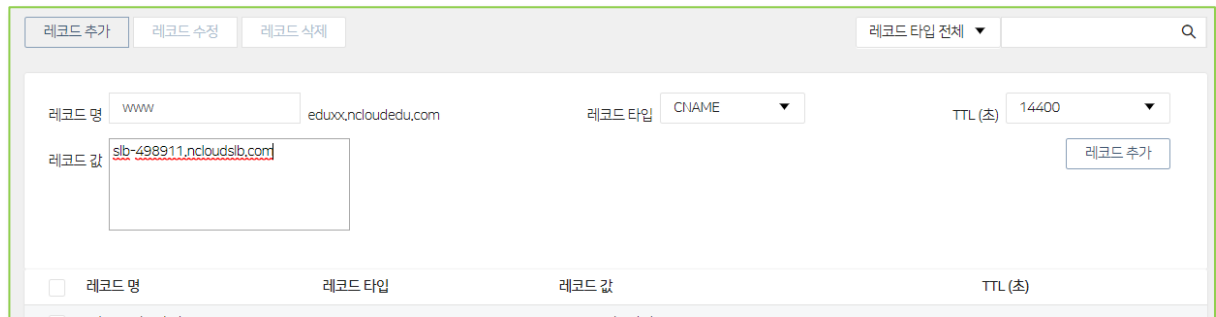
4. 로드밸런서를 등록

“Global DNS > Record” 메뉴의 ‘DNS’ 에서 상단의 “레코드 추가”를 선택하고

레코드명 : www

레코드타입 : CNAME

레코드값 : 로드밸런서 접속정보를 입력 (로드밸런서의 접속정보 항목)



The screenshot shows the '레코드 추가' (Add Record) form in the Naver Cloud Platform DNS console. The form is titled '레코드 추가' and has tabs for '레코드 추가', '레코드 수정', and '레코드 삭제'. The '레코드 타입 전체' (All Record Types) dropdown is set to 'CNAME'. The '레코드명' (Record Name) is 'www' and the '레코드값' (Record Value) is 'slb-498911.ncloudslb.com'. The 'TTL (초)' (TTL in seconds) is set to '14400'. A '레코드 추가' (Add Record) button is visible. Below the form, there is a table with columns: '레코드명' (Record Name), '레코드 타입' (Record Type), '레코드 값' (Record Value), and 'TTL (초)' (TTL in seconds). The table is currently empty.

레코드명	레코드 타입	레코드 값	TTL (초)
------	--------	-------	---------

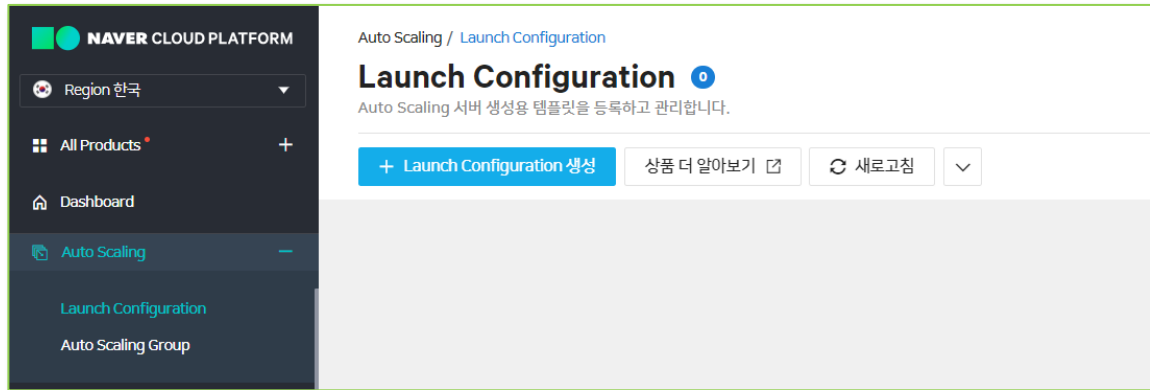
입력 후, 화면 하단 “추가” 선택

웹브라우저에서 www.eduxx.ncloudedu.com 으로 접속 확인 → (예시) www.edu01.ncloudedu.com

Lab 3 : 이벤트 대응과 비용 최적화를 위한 AutoScaling 구성 (30분)

1. Launch Configuration 구성

“Server > Auto Scaling > Launch Configuration”의 “+Launch Configuration 생성” 선택

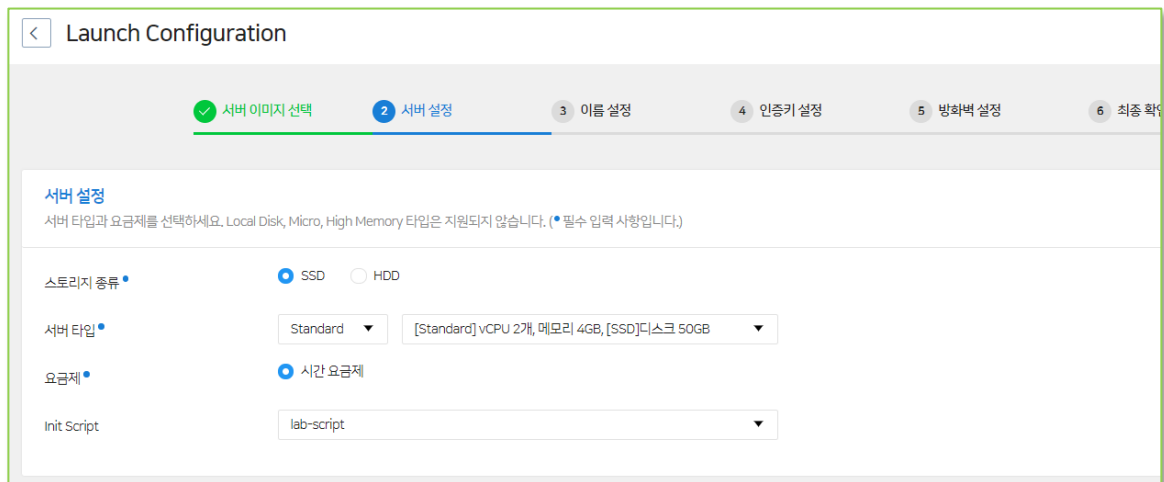


OS는 Centos-7.8-64 선택

“스토리지 종류”는 SSD

“서버타입” 선택

“Init Script”에 lab-script 선택 후, “다음” 클릭



“Launch Configuration 이름”에 lab6-1c 입력

< Launch Configuration

✓ 서버 이미지 선택 ✓ 서버 설정 3 이름 설정

서버 설정
Launch Configuration 설정을 입력합니다. (* 필수 입력 사항입니다.)

Launch Configuration 이름

2. Auto Scaling Group 생성

"Auto Scaling > Auto Scaling Group" 선택 후, "+ Auto Scaling Group 생성" 클릭

"Launch Configuration 선택" 에서 "lab6-ic" 선택, 하단의 다음을 선택

1 Launch Configuration 선택 2 그룹 설정 3 정책/일정 설정 4 정보 설정

Launch Configuration을 선택합니다.

Launch Configuration 이름	서버 이미지 이름	이미지 구분	서버 구성
<input checked="" type="radio"/> lab6-ic	centos-6.6-64	기본 이미지	[Standard] vCPU 2개, 메모리 4GB, [SSD]디스크 50GB

"Auto Scaling Group 설정"에서 오토 스케일링의 범위 및 서버가 속할 VPC/Subnet과 로드밸런서 선택

Auto Scaling 그룹 이름

VPC

Subnet

서버 이름 Prefix

최소 용량

최대 용량

기대 용량

클라우드 기본값(초)

헬스 체크 보류 기간

헬스 체크 유형

로드밸런서 ☒ 로드밸런서에 연결(최대 10개까지 선택 가능)

Auto Scaling Group 이름 : lab6-asg

VPC: lab1-vpc

Subnet: lab1-vpc-web-sub1

최소 용량 : 1 → 최소 생성 서버수

최대 용량 : 3 → auto scalling 그룹 내에서 생성될 수 있는 최대 서버 개수의 제한

기대 용량 : 2 → 2대씩 생성되는 것

쿨다운 기본값(초) : 10

헬스 체크 보류 기간 : 60초

헬스 체크 유형 : '로드밸런서' 선택 -> 'lab-lb' 선택 후, "다음 >" 을 클릭

"네트워크 접근 설정"에서는 "lab1-acg" 를 선택합니다.

The screenshot shows the 'Network Access Settings' (네트워크 접근 설정) step in the NCP console. At the top, there are three progress indicators: 'Launch Configuration Selection' (선택), 'Group Settings' (그룹 설정), and 'Network Access Settings' (3). Below the indicators, the title '네트워크 접근 설정' is followed by instructions: '보유하고 있는 ACG를 선택주세요. (*필수 입력 사항입니다.)' and 'ACG(Access Control Group)은 별도의 방화벽 구축없이, 서버 그룹에 대한 네트워크 접근 제어'. The 'Subnet' field is set to 'lab1-vpc-web-sub1'. The 'ACG' field is a dropdown menu with 'lab1-acg' selected, indicated by a green button with 'lab1-acg' and a close icon. Below the dropdown, it says '최대 3개까지 선택가능'.

일정 설정에서 "정책 설정"을 선택 후,

"서버 수 증가 정책"에서

"정책 이름" : add

"Scaling 설정" : "증감변경" → "1" (server) 입력, 추가

"서버 수 감소 정책"에서

"정책 이름" : sub

"Scaling 설정" : "증감변경" → "1" (server) 입력 , 반납

일정을 설정합니다.
 • 필수 입력 사항입니다.

☐ 나중에 설정
 ☒ 정책 설정
 ☐ 일정 설정

서버 수 증가 정책

정책 이름

Scaling 설정 server(s)

최소 조정 폭

클다운(초)

서버 수 감소 정책

정책 이름

Scaling 설정 server(s)

최소 조정 폭

클다운(초)

완료를 하게 되면 Server > Server 에서 처음엔 서버 2대가 생성되고,

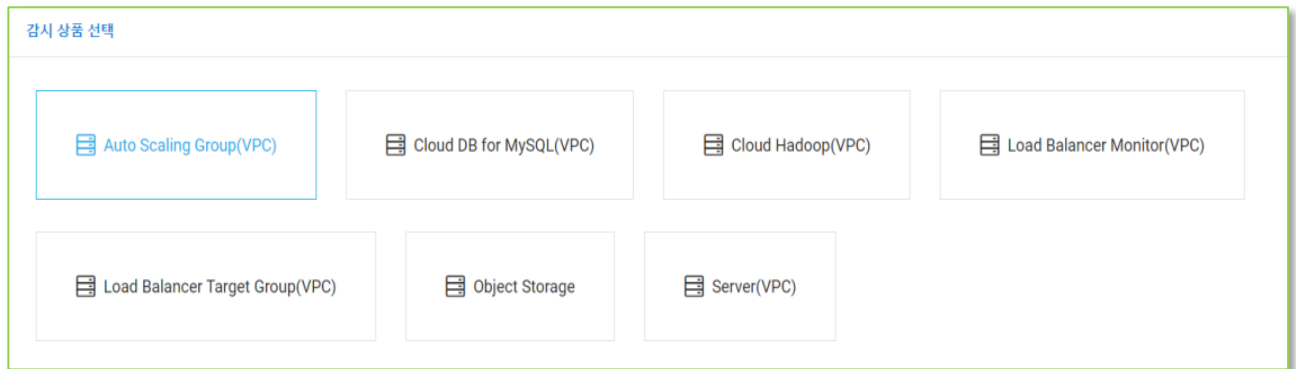
웹 페이지에서 부하가 생성되면, 서버가 3대로 생성되는 것을 확인할 수 있습니다.

Server 10				
커널 업데이트는 지원하지 않으며, 업데이트 진행시 VM 사용이 불가능하며, 복구를 지원하지 않습니다.				
<div> <div>+ 서버 생성</div> <div> 상품 더 알아보기 다운로드 새로고침 </div> </div>				
<div> <div>시작</div> <div>정지</div> <div>재시작</div> <div>반납</div> <div>강제 정지</div> <div>서버 접속 콘솔</div> <div>모니터링</div> <div>포트 포워딩 설정</div> </div>				
<div> <div>서버 관리 및 설정 변경</div> </div>				
<input type="checkbox"/> 서버 이름	서버 이미지 이름	서버 구성	상태	비공인 IP
<input type="checkbox"/> s-3dz1lcbmmn4n	centos-6.6-64	[Standard] 2vCPU, 4GB Mem ...	● 생성중	10.41.5.7
<input type="checkbox"/> s-4tl9f1cszl002	centos-6.6-64	[Standard] 2vCPU, 4GB Mem ...	● 운영중	10.41.82
<input type="checkbox"/> s-4tl9f1cszl001	centos-6.6-64	[Standard] 2vCPU, 4GB Mem ...	● 운영중	10.41.16
<input type="checkbox"/> lab3-win	win-2012-64-R2-en	[Standard] 2vCPU, 4GB Mem ...	● 정지	10.41.6.2
<input type="checkbox"/> lab1-org2	centos-6.6-64	[Standard] 4vCPU, 4GB Mem ...	● 운영중	10.41.16
<input type="checkbox"/> lab1-org	centos-6.6-64	[Standard] 2vCPU, 4GB Mem ...	● 운영중	10.41.85

3. Group Event 설정

“Management > Cloud Insight > Configuration > Event Rule” 상단 “+ Event Rule 생성”를 클릭

감시 상품 선택에서, “VPC Auto Scaling” 으로 선택합니다.



“+그룹 생성” 클릭하여 감시 대상 그룹을 생성

*그룹이름: lab-asg-group 입력

“선택 가능한 감시 대상 (1개)” 에서 ‘lab6-asg’ 선택

생성된 감시 그룹을 선택 후, “생성” 버튼을 누릅니다.

“감시항목설정” 에서 ‘+템플릿 생성’을 클릭하여 감시 항목 및 조건 설정을 위한 템플릿을 하나 만듭니다.

*템플릿 이름: CPU_template

*Metric: ‘avg_cpu_used_rto’ 선택 후, 다음을 클릭

‘Condition’ 항목(조건 설정)은 Warning, >= 10, AVG, 1min 으로 입력 후, 저장.

Metric	Description	Dimension ②	Level	Condition	Method	Duration
avg_cpu_us...	CPU Utilization		WARNING ▼	>= ▼ 10	AVG ▼	1 min

액션 설정에서는 Auto Scaling 정책을 선택 후, add 정책을 선택합니다.

최종 확인 후, 규칙 이름을 asg_add 로 하여 생성합니다.

Lab 4 : Cloud DB의 활용

1. DB를 위한 서브넷 및 NAT Gateway 생성

“VPC > Subnet Management 선택 > +Subnet 생성” 선택

다음과 같이 내용 설정 후 생성 클릭

*Subnet 이름 : lab1-vpc-db-sub1

*VPC : lab1-vpc

*IP 주소 범위 : 10.0.3.0/24

*가용 Zone : KR-2

*Network ACL : lab1-vpc-web-nacl

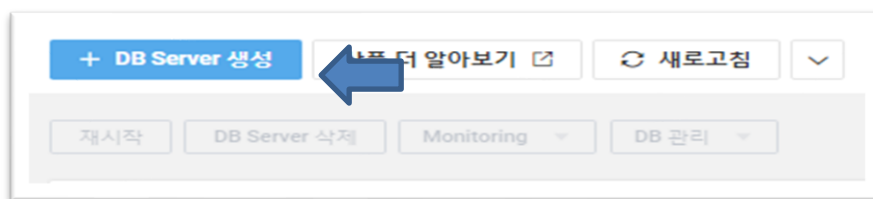
*Internet Gateway 전용 여부 : **N**

*용도 : **일반**

2. Cloud DB (CDB) 구성

기존에 DB 서버가 웹서버와 한 서버에 구성되어 있다면 가용성을 위해 DB서버를 웹서버로부터 분리하는 작업을 진행하여야 합니다. 이를 위해 실습에서는 Cloud DB for MySQL를 이용한 DB서버 구성을 진행합니다.

Cloud DB for MySQL을 선택하고 상단의 “DB Server 생성”을 선택합니다.



*VPC : lab1-vpc

*Subnet : lab1-vpc-db-sub1

*DB Server 타입 : Standard vCPU 2개, 메모리 8GB

*데이터 스토리지 타입 : SSD

*DB Server 이름 : edu

*DB 서비스 이름은 ncp-edu

DBMS 종류	MySQL		
DB 엔진 버전	mysql(5.7.29)		
DB 라이선스	General Public License		
고가용성 지원	<input checked="" type="checkbox"/> 고가용성을 선택하면 Standby DB Server를 포함하여 2대의 서버가 생성되며 추가 요금이 발생합니다.		
Multi Zone	<input type="checkbox"/> Master DB 2대를 서로 다른 Zone 에 생성하여 더욱 높은 가용성을 제공합니다.		
VPC	lab1-vpc		VPC 생성
Subnet	lab1-vpc-db-sub1 KR-2 Private		Subnet 생성
	Public 도메인은 Public subnet 에 생성된 DB 서버에서만 이용 신청이 가능합니다. DB 서버 생성 이후에 subnet 이전은 불가능합니다.		
DB Server 타입	Standard vCPU 2개, 메모리 8GB		
데이터 스토리지 암호화 적용	<input type="checkbox"/> 암호화 적용시 DB 데이터는 암호화 되어 스토리지에 저장됩니다. DB 서버 생성이후에는 스토리지 암호화 설정 변경이 불가능합니다.		
데이터 스토리지 타입	<input checked="" type="radio"/> SSD <input type="radio"/> HDD 설치 이후에 스토리지 타입은 변경되지 않습니다.		
데이터 스토리지 용량	기본 10GB 10GB 단위로 과금되며, 최대 6000GB 까지 자동 증가합니다.		
요금제	시간 요금제 요금 안내		
DB Server 이름	edu	-001-xxxx	최소 3글자, 최대 20자
	호스트명 중복 방지를 위해 임의의 text가 추가로 포함되어 만들어 집니다.(xxxx)		
DB 서비스 이름	ncp-edu		최소 3글자, 최대 30자
ACG 설정	Cloud DB 를 위한 ACG는 자동 생성됩니다.(예 : cloud-mysql-*) DB Server 접근을 위한 ACG 설정은 사용자 가이드를 참고하세요.		
<div>취소</div> <div>다음 ></div>			

*USER ID: student / *HOST(IP) : '%' / *USER 암호: abc123!@# / *기본 DB명: lab2db

USER ID는 DB 접속 시 사용하는 아이디이며 호스트는 MYSQL에서 접근 제어를 위한 부분입니다.

%는 모든 호스트에서 접근 가능하도록 하는 설정입니다.

CDB가 생성되면, DB에 접속하고자 하는 서버의 포트 오픈을 ACG에 추가하여야 합니다.

Server > ACG로 가서 자동으로 생성된 CDB의 ACG 설정을 누르고, Inbound 규칙을 다음과 같이 추가합니다.

*프로토콜 : TCP

*접근 소스 : lab1-acg

*허용포트 : 3306

ACG 규칙 설정 | cloud-db-bz30

ACG 에 적용된 상세 규칙을 표시합니다.

프로토콜	접근 소스	허용 포트 (서비스)	메모	설정
TCP	lab1-acg(17770)	3306	웹서버에서의 접근 허용	삭제
TCP	cloud-db-bz30(27674)	3306	for the DB service itself (automatically created, don't delete it)	삭제

• 변경사항이 아직 저장되지 않았습니다.

[× 닫기](#) [✓ 적용](#)

실제로 접속을 해보겠습니다.

접속을 위해서는 mysql client가 설치되어 있어야 하는데 init script를 통해 설치 완료되어 있습니다.

```
mysql -u student -h CDB도메인 -p
```

RDS 접속정보는 콘솔에서 RDS 정보를 통해 확인할 수 있습니다.

DB 서비스 이름	ncp-edu
DB Server 이름	edu-001
Private 도메인	db-3s450.cdb.ntruss.com
Public 도메인	미할당
상태	생성중
생성 일시	2020-04-24 오후 2:09 (UTC+09:00)
구동 일시	2020-04-24 오후 2:14 (UTC+09:00)
데이터 스토리지 타입	HDD
데이터 스토리지 용량	0GB / 10GB (사용량) / (가용량)
ACG	cloud-db-2f6hr (187260)

```
[root@lab1-org ~]# mysql -u student -p -h db-3s450.cdb.ntruss.com
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2000
Server version: 5.7.29-log MySQL Community Server (GPL)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

그리고 다음 명령어로 lab2db가 생성되어 있음을 확인할 수 있습니다.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| lab2db |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.00 sec)
```

Demo 1 : NAS 구성 (30분)

1. NFS 생성

"Storage > NAS > NAS Volume" 에서 "+ NAS 볼륨 생성" 선택

<

NAS 볼륨 생성

1 볼륨 생성

2 NFS 접근 제어 설정

3 최종 확인

볼륨 생성

NAS 볼륨 생성을 위한 기본 설정 사항을 입력해주세요. (● 필수 입력 사항입니다.)

NAS 요금은 생성시에 제공되는 최소 기본 볼륨 용량, 추가 볼륨 용량 요금을 합산하여 부과합니다.

Zone 선택 ●

KR-2

▼

NAS 볼륨 이름 ●

n002641_

lab3nfs

고객 식별을 위해 이미 입력된 NAS 볼륨 이름 뒤에 3~20자까지 NAS 볼륨 이름을 입력할 수 있습니다.

볼륨 용량 설정 ●

500

GB

볼륨 기본 용량은 500GB ~ 10,000GB이며, 100GB 단위로 추가하실 수 있습니다.

프로토콜 설정 ●

☒ NFS
 ☐ CIFS

CentOS, Ubuntu 등 리눅스 서버에서 마운트하실 수 있습니다.

볼륨 암호화

☐ 볼륨 암호화 적용

볼륨 별로 암호화가 적용되고 최초 생성 시에만 적용이 가능합니다.

다음 >

***폴룸명** : lab3nfs

***볼륨 용량 설정 : 500GB**

*프로토콜 설정 : NFS 후, "다음 >" 클릭

✓

블록 생성

2

NFS 접근 제어 설정

3

최종 확인

NFS 접근 제어 설정

NAS블록을 마운트하기 원하는 Server를 선택하시면, [ACL\(네트워크 접근 제어\)설정](#)이 완료됩니다.
(서버이름 [Double-click](#) 하시기나 사설IP를 직접 입력하시면 됩니다.)

전체서버

서버 이름

▼

🔍

서버 이름	IP	상태
lab1-org	10.33.45.54	● 운영중
lab1-org2	10.34.18.246	● 운영중

ACL 설정 서버

서버 이름	IP	상태
lab1-org	10.33.45.54	● 운영중 <div>✕</div>
lab1-org2	10.34.18.246	● 운영중 <div>✕</div>

2. 서버에서 마운트

먼저 lab1-org에서 마운트를 진행합니다.

CentOS 6.x 이상의 Linux에서 NFS를 사용하기 위해서는 기본적으로 nfs-utils 패키지를 설치하여야 합니다.

설치 명령어는 다음과 같습니다.

yum install nfs-utils -y

```
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : libgssglue-0.1-11.el6.x86_64      1/8
  Installing : libtirpc-0.2.1-15.el6.x86_64     2/8
  Installing : rpcbind-0.2.0-16.el6.x86_64      3/8
  Installing : python-argparse-1.2.1-2.1.el6.noarch 4/8
  Installing : libevent-1.4.13-4.el6.x86_64     5/8
  Installing : keyutils-1.4-5.el6.x86_64        6/8
  Installing : nfs-utils-lib-1.1.5-13.el6.x86_64 7/8
  Installing : 1:nfs-utils-1.2.3-78.el6_10.2.x86_64 8/8
  Verifying  : rpcbind-0.2.0-16.el6.x86_64      1/8
  Verifying  : keyutils-1.4-5.el6.x86_64        2/8
  Verifying  : libevent-1.4.13-4.el6.x86_64     3/8
  Verifying  : nfs-utils-lib-1.1.5-13.el6.x86_64 4/8
  Verifying  : libtirpc-0.2.1-15.el6.x86_64     5/8
  Verifying  : 1:nfs-utils-1.2.3-78.el6_10.2.x86_64 6/8
  Verifying  : python-argparse-1.2.1-2.1.el6.noarch 7/8
  Verifying  : libgssglue-0.1-11.el6.x86_64     8/8

Installed:
  nfs-utils.x86_64 1:1.2.3-78.el6_10.2

Dependency Installed:
  keyutils.x86_64 0:1.4-5.el6          libevent.x86_64 0:1.4.13-4.el6
  libgssglue.x86_64 0:0.1-11.el6       libtirpc.x86_64 0:0.2.1-15.el6
  nfs-utils-lib.x86_64 0:1.1.5-13.el6  python-argparse.noarch 0:1.2.1-2.1.el6
  rpcbind.x86_64 0:0.2.0-16.el6

Complete!
```

참고로 CentOS 5.x 버전에는 이미 설치되어 있습니다.

NFS를 사용하기 위해서는 RPC 데몬이 기동되어야 합니다.

기동시키는 명령어는 다음과 같습니다.

systemctl start rpcbind


```
[root@lab1-org ~]# systemctl status rpcbind
● rpcbind.service - RPC bind service
   Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; indirect; vendor preset: enabled)
   Active: inactive (dead)
[root@lab1-org ~]# systemctl start rpcbind
[root@lab1-org ~]# systemctl status rpcbind
● rpcbind.service - RPC bind service
   Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; indirect; vendor preset: enabled)
   Active: active (running) since Wed 2020-05-06 19:17:21 KST; 2s ago
     Process: 7900 ExecStart=/sbin/rpcbind -w $RPCBIND_ARGS (code=exited, status=0/SUCCESS)
    Main PID: 7901 (rpcbind)
   CGroup: /system.slice/rpcbind.service
           └─7901 /sbin/rpcbind -w
```

systemctl enable rpcbind

```
[root@lab1-org ~]# systemctl enable rpcbind && systemctl is-enabled rpcbind
Created symlink from /etc/systemd/system/multi-user.target.wants/rpcbind.service to /usr/lib/systemd/system/rpcbind.service.
enabled
```

NAS를 마운트하기 위해서는 먼저 마운트 포인트를 만들어 주어야 합니다.

mkdir 명령어로 먼저 마운트 포인트를 생성 합니다.

/mnt/nas 라는 디렉터리를 만듭니다.

mkdir /mnt/nas

관리 콘솔에서 NAS 신청을 통해 받은 볼륨명과 생성한 마운트 포인트를 이용하여 마운트를 합니다. 마운트는 다음과 같습니다.

mount -t nfs [마운트 정보] [마운트 포인트]

예를 들어, 10.10.10.10:/vol/nas 라는볼륨을 받았다면 다음과 같은 명령으로 마운트 할 수 있습니다.

mount -t nfs 10.10.10.10:/vol/nas /mnt/nas

마운트 정보	10.250.53.73:/n001636_lab3nfs
프로토콜	NFS
이벤트 설정	미설정

참고로 위 캡처 화면의 NAS 마운트 정보를 이용할 경우, 하기와 같이 마운트 명령어를 이용하면 됩니다.

```
[root@lab1-org /]#
[root@lab1-org /]#
[root@lab1-org /]# mount -t nfs 10.250.53.73:/n001636_lab3nfs /mnt/nas
[root@lab1-org /]#
```

그리고 lab1-org2도 위의 작업을 동일하게 진행합니다.

최종적으로 공유가 잘 되는지 확인하기 위해 lab1-org 에서 다음 명령어를 수행합니다.

```
cp /var/www/html/* /mnt/nas
```

그리고 lab1-org2 에서 다음과 같은 명령어를 수행합니다.

```
ls /mnt/nas
```

그러면 lab1-org에서 복사한 파일을 lab1-org2에서도 볼 수 있는 것을 확인할 수 있습니다.

3. CIFS 생성

Windows의 경우 CIFS를 생성하여야 합니다.

블록 생성
 NAS 블록 생성을 위한 기본 설정 사항을 입력해주세요. (●필수 입력 사항입니다.)
 NAS 요금은 생성시에 제공되는 최소 기본 블록 용량, 추가 블록 용량 요금을 합산하여 부과합니다.

Zone 선택 ●

KR-2

NAS 블록 이름 ●

n001636_ lab3cifs

고객 식별을 위해 이미 입력된 NAS 블록 이름 뒤에 3~20자까지 NAS 블록 이름을 입력할 수 있습니다.

블록 용량 설정 ●

500

 GB

블록 기본 용량은 500GB ~ 10,000GB이며, 100GB 단위로 추가하실 수 있습니다.

프로토콜 설정 ●

☐ NFS
 ☒ CIFS

Windows 서버에서 마운트하실 수 있습니다.

블록 암호화

☐ 블록 암호화 적용

블록 별로 암호화가 적용되고 최초 생성 시에만 적용이 가능합니다.

NAS 블록 생성을 눌러 블록을 생성합니다.

*블록명 : lab3cifs

*블록 용량 설정 : 500GB

*프로토콜 설정 : CIFS

다음 단계에서 CIFS 인증 정보 설정 화면에서, ID 와 비밀번호 를 입력합니다.

(ID : student 비밀번호 : ncp!@123)

<

NAS 볼륨 생성

✓ 볼륨 생성

2 CIFS 인증 정보 설정

CIFS 인증 정보 설정

Windows Server에서 NAS볼륨을 마운트하려면 최초 1회 ID와 비밀번호 확인이 필요합니다.
(서버 접속을 위한 ID와 비밀번호는 고객별로 1개만 설정할 수 있습니다.)

ID

edu02navercorpcom
마운트 접속 ID는 6자리 이상 20자리 미만의 영문, 숫자의 조합으로 입력할 수 있습니다.

비밀번호

spo
비밀번호는 영문,숫자,특수문자(!@%*&* 만 허용)를 조합하여 8~14자로 구성하셔야 하여 공백이 들어갈 수 없습니다.

< 이전

다음 >

4. 네트워크 드라이브 연결

CIFS는 Windows를 위한 공용 스토리지인만큼 Windows 서버를 만들어야 합니다.

Compute > Server > Server 탭에서 서버 생성

- 다음과 같이 Windows 서버 생성 (win-2016-64-en)
- VPC : lab1-vpc
- Subnet : lab1-vpc-web-sub1
- 서버타입 : standard
- 서버이름 : lab3-win
- 네트워크 인터페이스 : '+추가' 버튼 클릭(자동 기입)
- 공인IP : '새로운 공인IP 할당' 선택

하단의 다음 버튼 클릭

lab1-org1서버 생성 시 만들었던 인증키 선택 후 하단의 다음 버튼 클릭

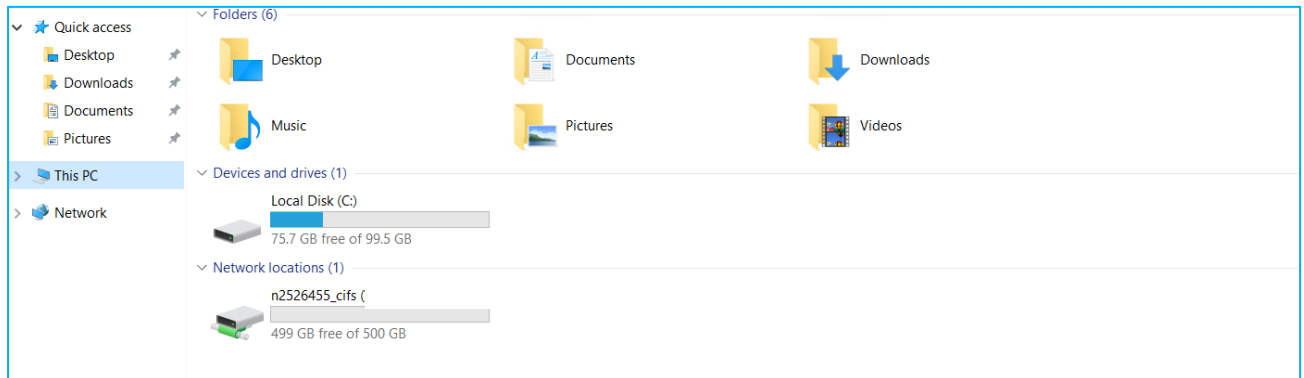
ACG 는 lab1-acg 선택 후 하단의 다음 버튼 클릭 후, 다음 페이지에서 '서버 생성' 클릭

원격데스크톱 연결 > 윈도우서버IP:3389로 접속

서버에 로그인 후 다음과 같이 Windows에서 네트워크 드라이브로 연결을 합니다.

- Windows 서버에서 i-nas_start을 클릭한 후 Windows System > This PC를 클릭
- This PC 창 왼쪽의 This PC 항목을 마우스 오른쪽 버튼으로 클릭한 후 Map network drive... 메뉴를 클릭
- Map Network Drive 팝업 창에서 다음 설정값을 선택하거나 입력하고 옵션을 설정한 후 [Finish] 버튼을 클릭
 - Drive: CIFS 볼륨을 연결(마운트)할 드라이브 이름(<예시> Z:)
 - Folder: CIFS 볼륨의 마운트 정보(<예시> \\W10.000.00.00\\n0000000_CIFS001, NAS 볼륨 상세 화면의 마운트 정보 항목 참고)
 - Reconnect at sign-in(옵션): 서버가 재부팅한 후에도 네트워크 드라이브 연결(마운트) 유지
 - Connect using different credentials(옵션): 네트워크 드라이브 연결 시 CIFS 볼륨의 인증 정보 입력을 요청

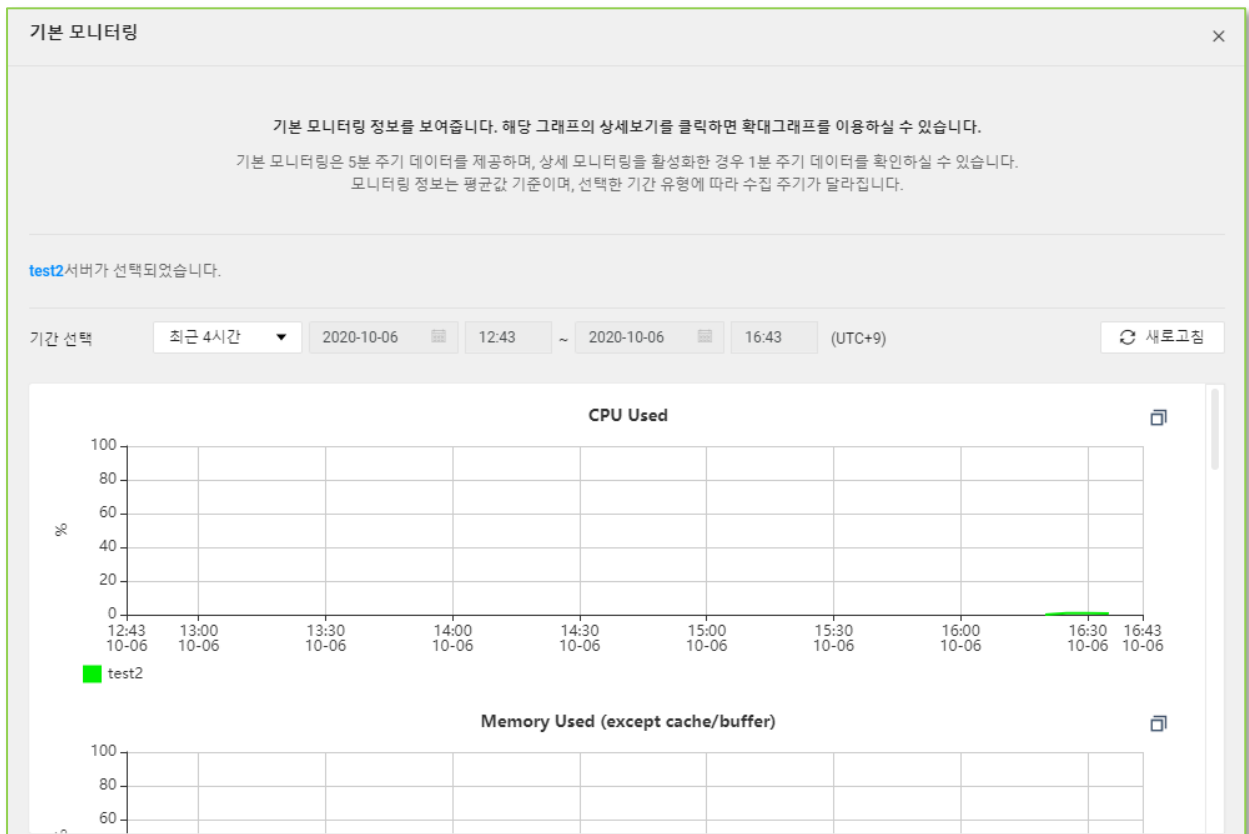
Enter Network Credentials 팝업 창에서 NAS 볼륨 생성 시 설정한 CIFS 인증 정보(User name, Password)를 입력한 후 [OK] 버튼을 클릭



Demo 2 : 서비스 안정성을 확보하는 모니터링 (30분)

1. 서버 기본 모니터링

Compute > Server 에서 서버 목록중 lab1-org나 lab1-org2를 선택하고 상단의 모니터링을 클릭



기간 선택에서 다양한 기간 혹은 기간을 직접 입력하여 원하는 시간대의 모니터링 값을 살펴볼 수 있습니다.

서버 기본 모니터링에서는 CPU 사용률, 네트워크 트래픽, 메모리 사용률, 스왑메모리 사용률, 디스크 사용률, 디스크 I/O를 확인할 수 있습니다.

2. 로드밸런서 기본 모니터링

Networking > Load Balancer에서 lab1-lb를 선택하고 상단의 모니터링을 클릭

Load Balancer

+ 로드밸런서 생성
추천 상품 보러가기
상품 더 알아보기
다운로드
새로 고침

로드밸런서 설정 변경
적용 서버 변경
로드밸런서 삭제
모니터링
SSL 인증서 관리
로드밸런서 상태 확인

<input type="checkbox"/>	로드밸런서 이름	상태	네트워크	접속 정보	서버 대수	메모
<input checked="" type="checkbox"/>	lab-lb	● 운영중	공인	slb-4061130.ncloudslb.com	2 대	

상세정보

로드밸런서 이름 (Instance ID)lab-lb (4061130)
생성일시2020-04-23 오후 6:00 (UTC+09:00)
AccessControlGroup소스ncload-load-balancer
네트워크공인
로드밸런싱 알고리즘Round Robin
적용 서버lab1-org2 연결상태 : ● 성공
lab1-org 연결상태 : ● 성공

접속 정보slb-4061130.ncloudslb.com 로드밸런서 설정가이드
상태운영중 로드밸런서 상태 확인
ZoneKR-2
HTTP Keep-alive 적용Off
Connection Idle Timeout60 초
설정 (default : 60초)



Traffic In

Traffic Out

확인

로드밸런서 모니터링에서는 현재 동접, 초당 접속자, 트래픽을 확인할 수 있습니다.

3. 통보 대상 설정

Management > Cloud Insight > Notification Recipient 에서 대상자 추가 버튼을 클릭합니다.

VPC / Cloud Insight(Monitoring) / Notification Recipient

Notification Recipient

통보대상자 정보를 등록해 두시면, 모니터링 등 이벤트 발생 시 통보 대상으로 설정하실 수 있습니다.

+ 대상자 추가
▼

대상자그룹	전체 대상자 0
전체 대상자	+

(•필수 입력 사항입니다.)

대상자 이름 •

설명

v [개인정보 수집, 이용에 대한 안내]

네이버 클라우드 플랫폼에서는 개인정보 수집, 이용 등 처리에 있어 아래의 사항을 정보주체에게 안내합니다.

- 1.수집/이용 목적: 주요 이벤트(장애 등) 발생 시 통보
- 2.항목: (필수항목)성명, 메일 주소, (선택항목)휴대폰번호
- 3.보유/이용기간: 알림 대상자 삭제시 또는 탈퇴시까지

위 개인정보 수집 및 이용에 대한 안내사항에 동의 합니다.

이메일 주소 • @

휴대폰 번호

인증번호 입력

인증번호를 아직 받지 못하셨다면 휴대폰 번호를 확인해 주세요

그룹선택

대상자 이름 : 수강자 이름

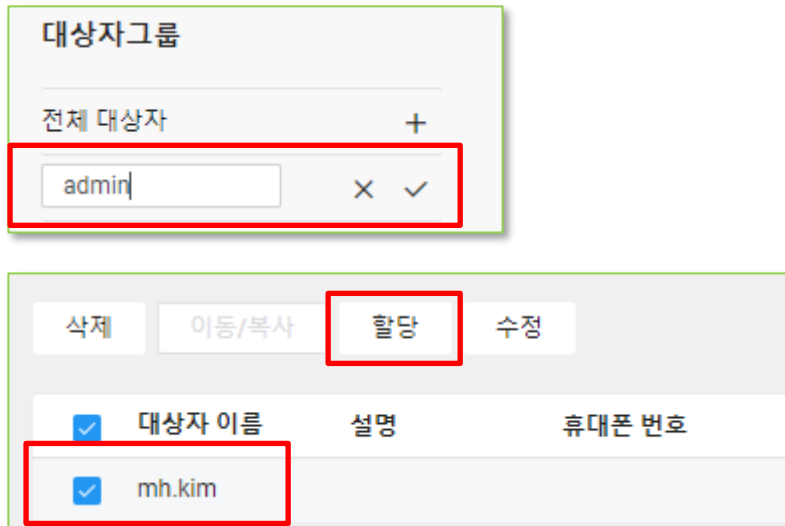
이메일 주소 : 수강자가 바로 확인 가능한 이메일 주소

휴대폰 번호 : 수강자 휴대폰 번호

인증번호 전송을 클릭하고 인증번호 수신 후 인증번호 입력란에 인증번호 입력 후 확인 클릭. 후 등록 선택하면 이벤트 발생 시 알람을 받을 대상자가 추가됩니다.

그 다음 전체 대상자 옆에 + 버튼을 클릭하여 admin 이라는 통보 그룹을 생성합니다.

앞서 만든 계정을 해당 통보 그룹에 할당합니다.



4. 이벤트 알람 설정

Management&Governance > Cloud Insight > Configuration > Event Rule > +Event Rules 생성 선택,

- 상단의 'Event rule 생성' 클릭
- 감시 상품 선택에서 'sever(VPC)' 선택
- 감시대상 설정 화면에서 상단의 '+그룹 생성' 클릭
 - 그룹 이름 : svr_mon
 - 선택 가능한 감시 대상 : lab1-org1, lab1-org2 선택 후 아래 방향 화살표 클릭
 - 하단의 '생성' 버튼 클릭

그룹 생성

그룹 이름과 설명을 입력하고, 그룹에 포함할 감시 대상을 선택해 그룹을 생성합니다.(• 필수 입력 사항입니다.)

Product Type Server(VPC)

그룹 이름 svr_mon

그룹 설명 0/300 bytes

선택 가능한 감시 대상 (7개) 검색어를 입력하세요

<input type="checkbox"/> Target	Detail	모니터링
<input type="checkbox"/> hands-on	nm:PUBLIC:VPCServer:KR:2526455:Server/12638395	기본
<input type="checkbox"/> script-test-svr	nm:PUBLIC:VPCServer:KR:2526455:Server/12088862	기본
<input type="checkbox"/> default-pool-w-1muw	nm:PUBLIC:VPCServer:KR:2526455:Server/12082631	기본

선택한 감시 대상 (2개)

<input type="checkbox"/> Target	Detail	모니터링
<input type="checkbox"/>	nm:PUBLIC:VPCServer:SGN:2526455:Server/10228613	기본
<input type="checkbox"/>	nm:PUBLIC:VPCServer:KR:2526455:Server/11376791	기본

× 취소 ✓ 생성

- 감시 대상 설정에서 방금 만든 'svr_mon'선택 후 하단의 '다음'버튼 클릭
- 감시 항목 설정에서 상단의 '+템플릿 생성'클릭
 - 템플릿 이름 : mon_svr
 - 메트릭 : sever 탭 > SERVER/avg_cpu_used_rto 선택
 - 하단의 '다음' 버튼 클릭
 - 레벨 : warning
 - 조건 : >=, 80
 - 집약방법 : AVG
 - 지속시간 : 1분
 - 하단의 '저장'버튼 클릭
- 'mon_svr' 템플릿 선택 후, 하단의 '다음'버튼 클릭
- 통보대상자 그룹에서 'admin'선택 후 하단의 '다음'버튼 클릭

- 규칙 이름 'mon_svr_rule' 입력 후 하단의 '생성' 버튼 클릭

기본정보

(필수 입력 사항입니다.)

규칙 이름

mon_svr_rule

설명

0/300 bytes

설정 내역

Rules 전체 보기

감시 대상

Target	Detail
lab1-svr	nrm.PUB.VPCServer.SGN.2526455.Server/10228613
k8s-tool	nrm.PUB.VPCServer.KR.2526455.Server/11376791

감시 항목 및 조건

메트릭	디멘션	레벨	조건	집약 방법	지속시간	상세보기
SERVER/avg_cpu_used_rto		WARNING	>= 80	AVG	1 minute	보기

액션

Type	Name	Detail	추가 알림 설정
알림 메시지 발송	admin	SMS, EMAIL	리마인드 미 설정 / 종료 알림 OFF

Demo 3 : CLA를 통한 로그 수집 및 분석 (15분)

1. 분석할 로그와 서버 설정

Analytics > Cloud Log Analytics > Management 선택한 후

서버 목록중 lab1-org 선택하고 상단의 수집설정을 클릭

Cloud Log Analytics / Management

Management

상종 더 알아보기 다운로드 새로고침

Server CDB-MySQL CDB-MSSQL Bare Metal Server

수집 설정 수집 해제 서버 이름

서버 이름	서버 이미지 이름	상태	비공인 IP	ZONE
lab3-win	win-2012-64-R2-en	정지	10.41.6.229	KR-2
lab1-org2	centos-6.6-64	운영중	10.41.165.155	KR-2
lab1-org	centos-6.6-64	운영중	10.41.85.108	KR-2

서버 이름: lab1-org
 상태: 운영중
 생성 일시: 2020-04-23 17:40 (UTC+0900)
 비공인 IP: 10.41.85.108
 Log 수집 Type 개수: 미수집상태

서버 이미지 이름: centos-6.6-64
 OS: CentOS 6
 구동 일시: 2020-04-24 15:45 (UTC+0900)
 Log 수집 설정 일시
 Install Key

Syslog, Apache, Custom Log를 순서대로 선택

Custom Log 항목에서

Log Type : Secure

Log 경로 : /var/log/secure 입력 후 추가 후, 적용을 클릭

Log 수집 설정

서버 이름	Log Template	Log Type	Log 경로
	Custom Log	input log type	input log path
lab4	APACHE	apache_error	/var/log/httpd/error_log
	APACHE	apache_access	/var/log/httpd/access_log
	SYSLOG	SYSLOG	/var/log/messages

취소 적용

2. Cloud Log Analytics 상품을 사용하기 위한 서버 내 agent 설치

하기 화면의 가이드 처럼 서버에 접속하여 실행

Cloud Log Analytics 상품을 사용하기 위한 서버 내 agent 설치 방법 가이드

설정하신 로그 수집 정보의 등록이 완료되었습니다.
로그 수집을 시작하기 위해서는 설정한 서버들에 다음과 같은 절차로 agent가 설치되어야 합니다.
콘솔 화면에서 수집 설정 등록을 완료 하였어도, 서버에 agent가 설치되지 않으면 로그가 수집되지 않으니 참고하시기 바랍니다.

- 로그 수집 서버에 접속해 로그인을 합니다.
자세한 서버 접속 방법은 사용자 가이드의 "[서버 접속 가이드](#)"를 참고하시기 바랍니다.
- 아래 표시된 "로그 수집 agent 설치 명령어"를 서버에서 실행합니다. 클립보드에 복사하기를 이용하시면 편리합니다.
로그 수집 agent 설치 명령어 :
Linux: [클립보드에 복사하기](#)
`curl -s http://cm.cla.ncloud.com/setupCla/@cc54715c0074feda0ddc499995b677b | sudo sh`
- "로그 수집 agent 설치 명령어"를 서버에서 실행하면 자동으로 agent 다운로드 및 설치, 설정까지 진행됩니다.
설정이 완료되면 아래와 같은 메시지가 출력됩니다.
로그 수집 agent 설치 명령어 실행 결과 **===== Finish Installation =====**
- Cloud Log Analytics 대시보드 화면에서 설정한 서버의 로그가 수집되고 있는지 확인합니다.
만약 수집이 안되는 경우 agent 설치 중 오류가 발생했는지 확인하고, 2번 단계를 다시 진행해 주시기 바랍니다.

[닫기](#)

서버 재시작이 완료되면 lab1-org 서버에 SSH로 접근하고, 웹페이지에 접근을 수차례 시도합니다. 그 후CLA 페이지에서 로그가 수집되는 것을 확인할 수 있습니다.

