네이버 클라우드 플랫폼
Professional 과정

Cloud Tech Frontier | 2023.06

문서정보

본 문서는 네이버클라우드플랫폼 공인 교육 – Professional 진행을 위한 실습 가이드입니다. 본 실습 가이드는 이론 교육과 더불어 실습 교육 시 활용됩니다.

Copyright © 2022 NAVER Cloud, Inc. All rights reserved

NAVER
CLOUD PLATFORM
NAVER CLOUD PLATFORM
Professional 과정

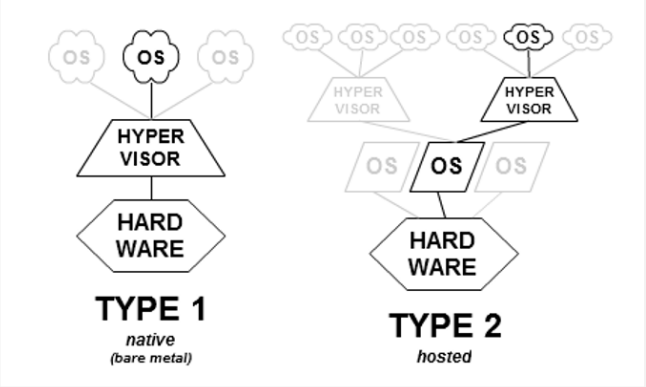
NAVER
CLOUD PLATFORM

201 Compute/Storage

Chapter 1. Compute / Containers 상품

Hypervisor

- 하드웨어와 VM 사이에 VM과 하드웨어를 관리하기 위한 가상화 관리 소프트웨어



NAVER CLOUD PLATFORM

하이퍼바이저

하이퍼바이저는 타입1과 같이 하드웨어와 VM 사이에서 하드웨어의 모든 리소스를 관장하는 방식이 있는 반면 타입2와 같이 하드웨어 OS가 설치되고 어플리케이션 형태로 하이퍼바이저가 동작하여 해당 하이퍼바이저 위에 VM이 설치되는 형태가 있습니다. 타입2의 경우 하드웨어에 설치된 OS를 호스트OS, 하이퍼바이저 위에 설치된 OS를 게스트OS라고 합니다.

하이퍼바이저에는 대표적으로 Xenserver, KVM, Hyper-V, VMWare 등이 있으며 IBM의 LP(Logical Partition)과 같은 방식도 존재합니다.

하이퍼바이저에 따라 설치 가능한 OS는 상이합니다.

전가상화와 반가상화

- 전가상화
  - 하드웨어 전체를 가상화하는 방식.
  - 하드웨어를 관리하는 하이퍼바이저(DOM0)가 VM들에게 하드웨어 리소스를 할당하는 방식.
  - 하이퍼바이저가 모든 리소스를 관리하는 만큼 성능적으로 오버헤드가 발생
  - VM은 일반적인 OS를 그대로 사용 가능

- 반가상화
  - 전가상화의 성능 저하를 해결하고자 모든 명령에 대해 DOM0를 통해 요청하는 방식이 아닌 하이퍼콜을 통해 직접 요청
  - 하이퍼콜을 사용하기 위해서는 VM의 OS가 이를 지원해야 함. (*OS 제약 발생)

NAVER CLOUD PLATFORM

전가상화

일반적으로 전가상화는 하드웨어의 리소스를 하이퍼바이저가 관리하는 방식으로 VM들은 하이퍼바이저가 제공하는 리소스를 할당 받아 사용됨. VM은 하이퍼바이저가 제공하는 가상의 하드웨어 드라이버를 이용하여 하드웨어 리소스에 접근합니다. 따라서 드라이버가 제공되지 않는 OS의 경우 전가상화에서 VM으로 구성할 수 없습니다

전가상화의 대표적인 케이스는 PC용 가상화솔루션이며 이는 전가상화 방식을 이용합니다.

모든 하드웨어 리소스를 하이퍼바이저가 관리할 수 있기 때문에 관리가 용이하지만 하이퍼바이저가 모든 리소스, 특히 네트 트래픽까지 처리해야 하기 때문에 성능에 있어 오버헤드가 발생합니다.

반가상화

전가상화의 성능 저하를 해결하고자 특정 명령에 대해서는 하이퍼바이저를 통해 하드웨어에 요청하지 않고 하이퍼콜을 통해 직접 요청하게 된다. 다만 하이퍼콜을 사용하기 위해서는 VM의 OS가 이를 지원해야 합니다.

서버 특징

- G1과 G2로 구분
  - CPU 성능이 비약적으로 발전하면서 신규 CPU 라인업은 G2로 명명
  - G2의 경우 vCPU와 RAM의 비율에 따라 3가지 서버 타입 제공
  - VPC 환경에서 일반 서버는 G2만 제공하며, GPU 서버는 G1 으로 제공됨

- CPU
  - vCPU 단위로 할당
  - CPU의 Core가 vCPU에 맵핑되는 구조
  - Over Commit 허용
  - 스펙 변경 가능

- Memory
  - GB 단위로 할당
  - Over Commit 허용 안함
  - 스펙 변경 가능

NAVER CLOUD PLATFORM

Over Commit

하이퍼바이저를 통해 VM에 제공되는 리소스는 물리적인 리소스가 아닌 가상의 리소스로서 물리적인 리소스와 별개로 물리적인 리소스보다 많은 리소스를 VM에 제공할 수 있습니다. 하지만 가상의 리소스는 물리적으로 하드웨어 리소스를 사용하는 만큼 물리적인 리소스보다 많은 가상 리소스를 제공하게 되면 성능저하가 발생하게 됩니다.

네이버 클라우드 플랫폼의 경우 CPU에 대해서만 Over Commit을 허용하고 있으며 Over Commit을 허용하지않는 물리적인 RAM 사용량을 기준으로 VM을 배치하게 됩니다.

vCPU

CPU는 다수의 Core로 구성되어 있으며 Hyper-Threading [1]기술을 적용하여 물리적으로 20Core의 경우 40Core로 표시됩니다. 예를 들어 물리 서버 CPU가 16Core라면 Hyper-Threading을 통해 32Core를 사용할 수 있고, 클라우드 플랫폼 설정인 CPU Over Commit을 8로 설정한다면 32*8 즉, 256개의 vCPU만큼의 VM을 PM에서 수용할 수 있습니다.
1vCPU는 1Core와 대응되나 Over Commit이 발생할 경우 다른 VM과 경쟁을 하게 됩니다.

[1] https://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html

서버 특징

- HDD
  - OS 영역이 기본 할당 (50GB or 100GB)
  - OS 영역은 용량 확장이나 축소 불가
  - SSD 타입과 HDD 타입으로 구분

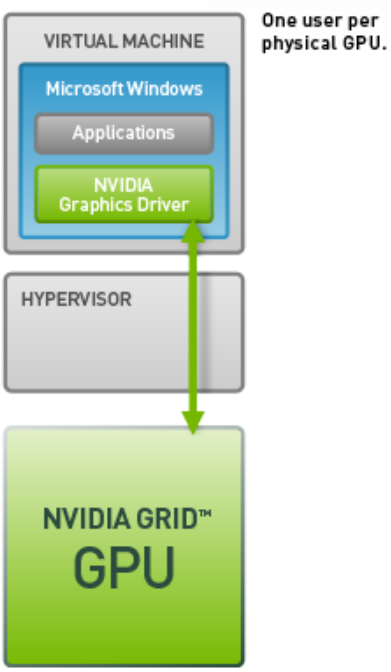
- GPU
  - GPU 단위로 할당 (GPU Core 단위로 할당하지 않음)
  - Pass Through 방식으로 제공
  - 그래픽카드 별 서버 한대 당 맵핑가능한 개수가 상이함 (V100은 최대 4개, T4 및 P40는 최대 2개)

- Network
  - Physical 10Gbps
  - Logical 1Gbps
  - 실제로 500Mbps~ 1Gbps 제공 (RX+TX)

NAVER CLOUD PLATFORM

GPU 할당 방식

하이퍼바이저에서 GPU 자원을 VM에 제공하기 위해 구성할 수 있는 방식은 크게 2가지가 있습니다.



1. PCI Pass-Through

VM 수용 노드의 PCI 슬롯에 장착된 GPU 디바이스에 직접 접근 가능하게 하는 방식이며, GPU 카드 단위로 제공되어 타 VM과 공유될 수 없어 GPU를 점유한 VM이 GPU를 사용하지 않고 있을 경우 활용도 면에서 효율성이 떨어지는 단점이 있습니다.

2. GRID GPU를 통한 vGPU 할당

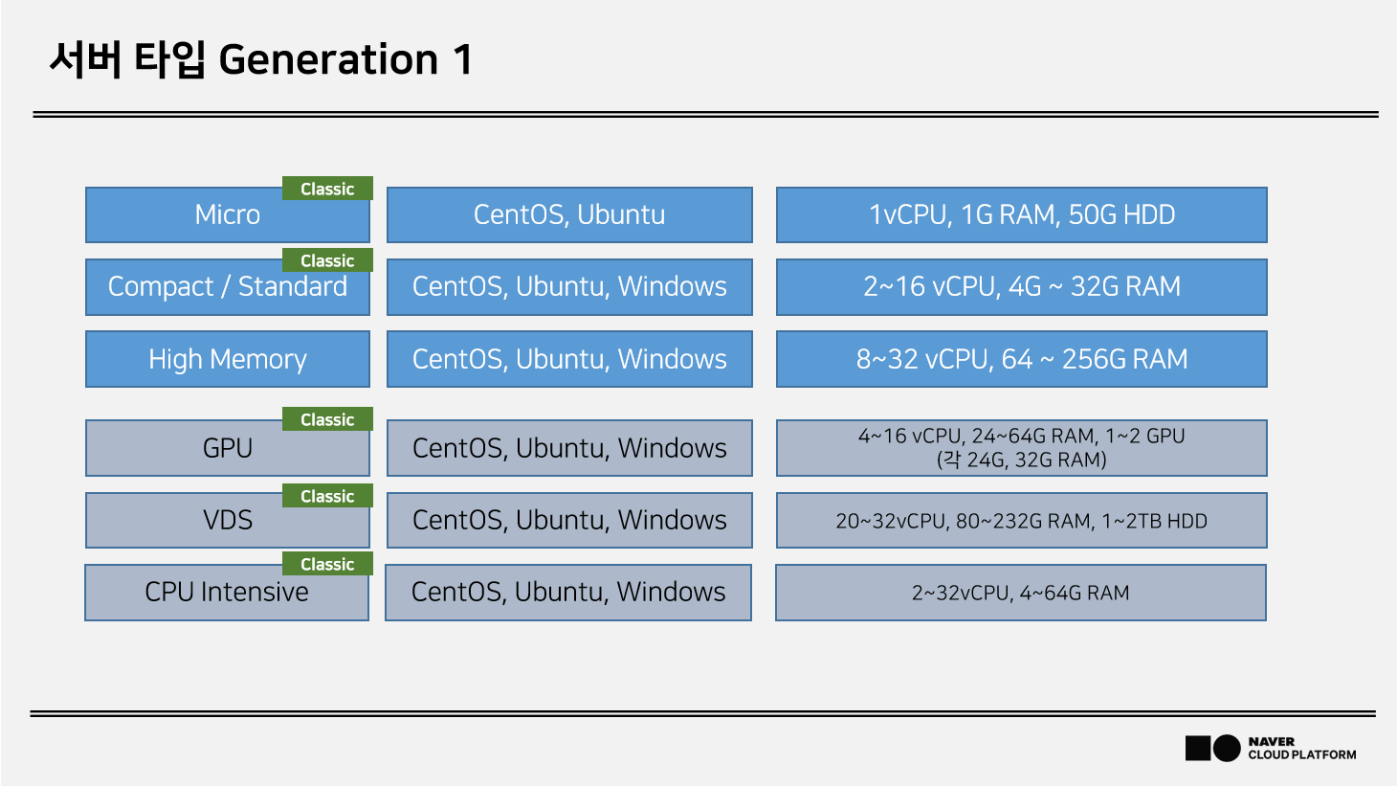
하이퍼바이저 레벨에서 GPU를 가상화하여 GPU의 Core를 VM에 할당할 수 있게 되어 다수의 VM들이 GPU를 공유할 수 있도록 지원하는 방식입니다.

네이버 클라우드 플랫폼에서는 카드 단위로 VM에 제공하는 Pass-Through 방식을 사용하고 있습니다.

네트워크 링크 할당 방식

네이버 클라우드 플랫폼의 물리적인 서버들은 10Gbps로 연결되어 있습니다. 하이퍼바이저에서는 VM에 1Gbps의 가상 네트워크를 제공하고 있으며 서버 스펙에 따라 실제로 제공되는 대역폭은 상이합니다.

또한 물리적인 링크가 Tx와 Rx가 분리되어 각각의 대역폭이 보장되는 반면 네이버 클라우드 플랫폼에서의 대역폭은 Tx와 Rx가 합쳐진 값입니다. 물리적으로는 일반적인 데이터 통신을 위한 링크와 서버 이미지가 저장된 네트워크 스토리지와 PM간 링크가 구분되어 있습니다.



서버 타입

네이버 클라우드 플랫폼의 서버들은 클러스터라는 하나의 집합으로 구분되어 있으며 네트워크와 같은 서버와 연결된 정보는 클러스터 단위로 할당이 되어 있습니다. 따라서 클러스터 내에서 서버의 이동 및 스펙 변경이 가능합니다.

Live Migration

라이브 마이그레이션은 VM이 On된 상태에서 기존 PM에서 다른 PM으로 이전하는 것을 의미합니다. 단순히 디스크의 내용만 마이그레이션되는 것이 아닌 메모리, 레지스트리까지 다른 PM으로 이전하는 것을 말하는데 메모리 마이그레이션에는 Pre-Copy Memory Migration 방식과 Post-Copy Memory Migration 방식이 있습니다.

두 방식의 가장 큰 차이는 메모리 복제 시점으로 Pre-Copy Memory Migration 방식은 이전하기 전에 메모리를 복사하고 VM을 정지시킨 후 새로운 PM에서 시작하는 방식이며 Post-Copy Memory Migration 방식은 VM을 정지시킨 후 메모리를 복사하여 새로운 PM에서 시작합니다.

네이버 클라우드 플랫폼의 경우 Post-Copy Memory Migration 방식을 사용하고 있습니다.

서버 타입 Generation 2

Standard	1:4	2C8G / 4C16G / ... / 32C128G
High Memory	1:8	2C16G / 4C32G / ... / 32C256G
High CPU	1:2	2C4G / 4C8G / ... / 32C64G

서버 타입 (vCPU와 Memory의 비)	상품코드	특징	추천 용도
Standard-g2 (4배수)	S-g2	범용성 높은 성능을 제공하기 위해 vCPU 대비 Memory 비율을 균형있게 할당하여 다양한 워크로드에 적합한 서비스를 제공합니다.	일반 데이터베이스 서버 개인 홈페이지 운영
High CPU-g2 (2배수)	C-g2	Memory 대비 vCPU 비율을 높여 Computing 집약적 워크로드에 적합한 서비스를 제공합니다.	과학적 모델링 게임 서버
High Memory-g2 (8배수)	M-g2	대용량 데이터 처리 등과 같은 Memory 집약적 워크로드에 적합한 서비스를 제공합니다.	고성능 데이터베이스 서버 대규모 게임 서비스

NAVER CLOUD PLATFORM

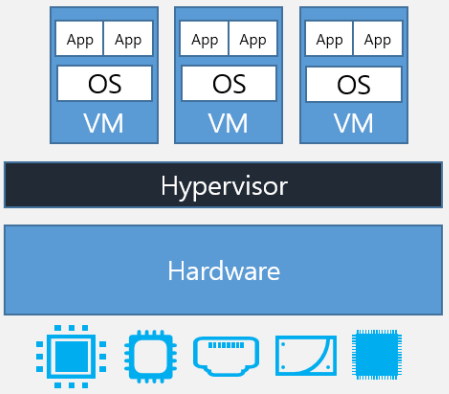
G2는 서버 타입을 보다 간결하고 쉽게 스펙을 구성함으로써 사용자가 원하는 사양을 손쉽게 구성할 수 있도록 구성하였습니다.

Standard 타입

- 일반적으로 사용하는 서버 타입
- CPU 와 Memory 비율 = 1 : 4

- 서버 사양 및 지원 OS

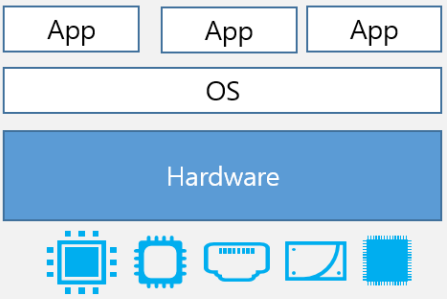
CPU (vCPU)	Memory(GB)	OS (50GB)	OS (100GB)
2	8	CentOS Ubuntu	Windows
4	16		
8	32		
16	64		
32	128		



NAVER CLOUD PLATFORM

Bare Metal Server

- 하이퍼바이저 없이 하드웨어의 자원을 그대로 사용
  - 기본적인 관리는 IPMI를 통해 관리
- 오라클과 같이 라이센스상 클라우드에 대한 제약이 있는 경우 사용
- 서버 사양 및 지원 OS
  - RAID 5, 1+0 지원
  - Classic 플랫폼 : CentOS, ORACLE Linux, Windows OS 제공
  - VPC 플랫폼 : CentOS, ORACLE Linux, RHEL, Windows OS 제공



※ VPC 플랫폼에서 제공하는 Bare Metal Server 스펙

CPU	Core 수	Memory	디스크
Single Intel Xeon Silver 4215 (2.6 GHz)	8	128	4*1.9TB SSD
Dual Intel Xeon Silver 4214 (2.2 GHz)	24	256	4*1.9TB SSD
Dual Intel Xeon Gold 5220 (2.2 GHz)	36	384	8*1.9TB SSD
Dual Intel Xeon Silver 4112(2.6GHz)	48	512	8*1.9TB SSD

NAVER CLOUD PLATFORM

스펙 선정 사유

Oracle DBMS의 경우 Standard Edition은 최대 8Core까지 지원하며, 8Core 이상의 서버에는 Enterprise Edition을 사용하여야 하는 제약사항이 있습니다.

GPU Server

- 병렬 처리에 최적화된 GPU 서버의 고성능 컴퓨팅 파워를 제공
  - 딥 러닝을 위한 GPU 서버 팜
    - NVIDIA **T4, V100 장착**
    - NVIDIA GRID 기술이 아닌 Pass Through 를 적용하여 제공
    - **V100은 서버 당 최대 4장의 GPU를, T4는 서버 당 최대 2장의 GPU를 제공**
  - GPU 제공 사양
    - T4: 8vCPU, 40GB Memory 당 GPU 1개, 16GB GPU 메모리 제공
    - V100: 8vCPU, 90GB Memory 당 GPU 1개, 32GB GPU 메모리 제공
  - 제공 OS
    - CentOS 7.3(T4 미지원) & 7.8 , Ubuntu 16.04 & 18.04, Windows 2016

NAVER CLOUD PLATFORM

GPU Server

- 제공 사양

타입	GPU	GPU 메모리	vCPU	메모리	디스크
V100	1개	32GB	8개	90GB	50GB / 100GB
	2개	64GB	16개	180GB	
	4개	128GB	32개	360GB	
T4	1개	16GB	4개	20GB	
			8개	40GB	
			16개	80GB	
	2개	32GB	8개	40GB	
			16개	80GB	
			32개	160GB	

- NVIDIA TESLA T4 모델과 최신 NVIDIA TESLA V100 모델을 이용한 GPU 서버 제공
- 운영체제 설치를 위한 기본 디스크가 제공되며, 추가 디스크는 디스크 당 최대 2,000GB 크기로 OS가 지원하는 개수만큼 직접 생성 가능

NAVER CLOUD PLATFORM

서비스		KR	SG	JP	USW	DE	HK
Compute	Server(Compact/STD)	O	O	O	O	O	O
	Server(High-mem)	O	O	O	O	O	X
	SSD Server	O	O	O	O	O	X
	GPU	O	X	X	X	X	X
	VDS	O	O	O	O	O	X
	Baremetal	O	O	O	O	O	X
	AutoScaling	O	O	O	O	O	X

	Cloud Functions	O	X	X	X	X	X
	HPC	O	X	X	X	X	X
	Container Registry	O	X	X	X	X	X

https://www.ncloud.com/product/global/globalRegion

(2021년 10월 기준)

구분	T4	V100	P40
Appearance			
CUDA Cores	2,560	5,120	3,840
Tensor Cores	320	640	N/A
GPU Memory	16GB	32GB	24GB
Memory Bandwidth	346GB/s	900GB/s	346GB/s
GPU boost Clock Speed	1,590 MHz	1,530 MHz	1,530 MHz
Single-Precision	8.1 TFLOPS	14 TFLOPS	12 TFLOPS
INT8	130 TOPS	224 TOPS	47 TOPS
Power	70W	250W	250W
Use Case	머신러닝 추론, 동영상 트랜스코딩, 대화형 그래픽 등	딥 러닝, 유체 역학, DNA 배열, 내진 해석, 자율주행 차량, 신약 개발 등	교육, 유추, 신경망 모델 등

FLOPS : 컴퓨터의 성능 향상, 성능 비교, 연산속도 측정, 성능 예측, 기대하는 바에 대한 성능 달성 여부의 검증, 시스템의 조율(tune up) 등에 대한 평가에 사용되는 평가항목에는 정량적 평가항목과 정성적 평가항목이 있다. 단위 시간당 처리량(through-put)·응답시간·명령 믹스(mix)·벤치마크(benchmark) 등은 정량적 평가항목이고, 시스템의 신뢰성·보수성·확장성·편리성 등은 추상적이고 감각적인 정성적 평가항목이다.

이들 평가 방법 중에서 프로그램을 실행할 때의 명령어 실행 빈도를 명령 믹스라고 하는데, 그 실행 빈도를 성능의 척도로 하였을 때 평가기준 단위에는 FLOPS와 MIPS(million instructions per second)가 있다.

MIPS는 1백만 회를 단위로 한 1초당 명령실행 횟수를 나타내며, FLOPS는 1초당 부동 소수점 연산(곱셈)의 명령 실행 횟수를 나타내는 단위이다. 그러나 MIPS값은 명령의 기능별 수준을 반영하지 않기 때문에 그 평가치를 신뢰하지 않는 경향도 있다. 범용 슈퍼컴퓨터에서는 성능향상을 위해 명령 실행상의 여러 단계들을 병렬로 다중처리함으로써 처리속도를 초고속화하기 때문에, MIPS 대신 매초당 부동 소수점 연산의 명령 실행 횟수인 FLOPS를 연산속도의 단위로 사용한다.

Preinstall Image

- DBMS
  - Tibero
- Application
  - Pipoint
  - JEUS
  - WebtoB
  - RabbitMQ
  - Superset
  - META Commerce
  - Tensorflow
  - Tomcat

※ Classic 에서 지원되는 추가 Preinstall Image
- Jenkins
- LAMP
- WordPress
- Joomla!
- Shadowsocks
- LEMP
- Hugo
- Gitlab CE
- Node.js
- Gradle
- MySQL
- Cubrid
- Redis
- MariaDB
- PostgreSQL

NAVER CLOUD PLATFORM

Pre-Install Image

일반적으로 많이 사용하는 DBMS 및 Application을 서버 이미지에 추가로 설치하여 제공하는 이미지 방식입니다.

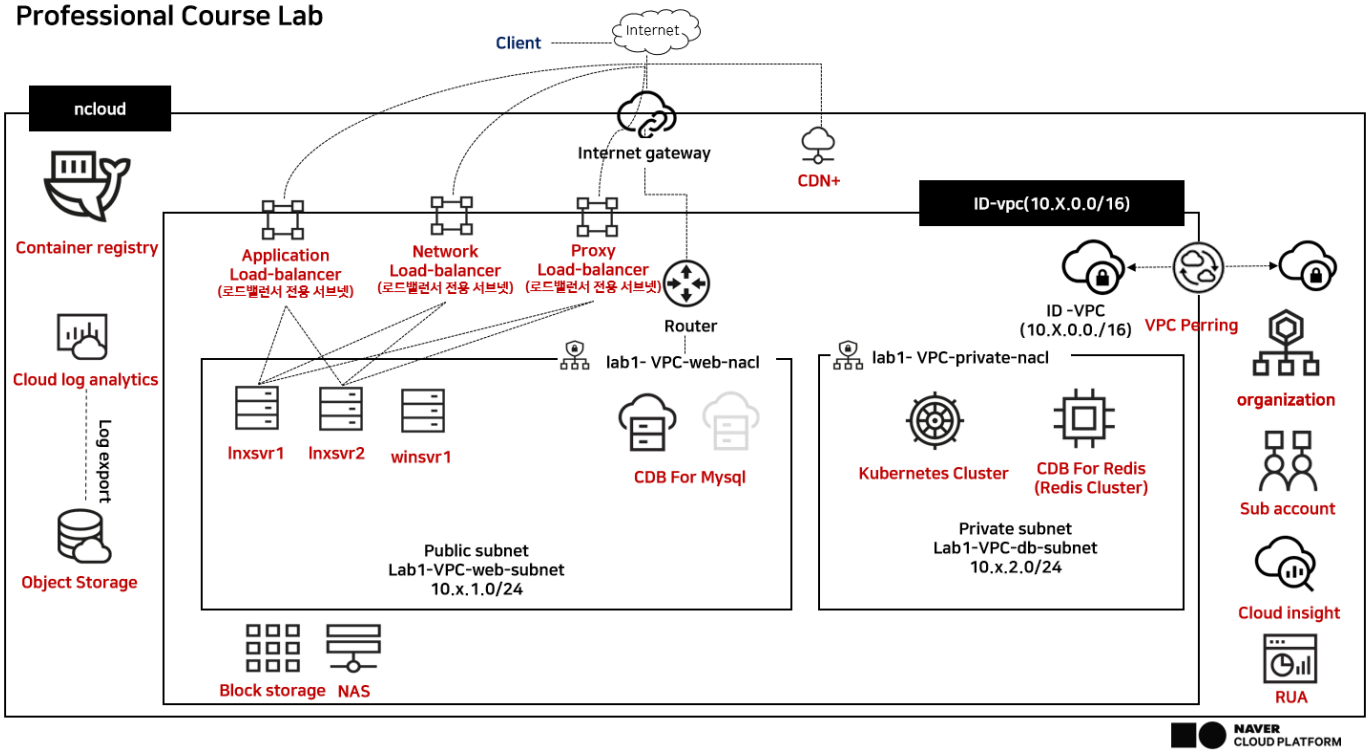
현재 일부 설치형 이미지는 Classic 플랫폼에서만 이용이 가능합니다.

서버 Operation – 서버 생성 1

- 리전 선택 혹은 VPC 및 Subnet 선택
  - 서버를 생성할 리전 선택
  - 서버를 생성할 VPC와 Subnet 선택
- 부팅 디스크 이미지 선택
  - 디스크, 이미지 타입 선택
- OS 선택
  - OS 이미지 선택
- 서버 설정
  - 존, 스토리지 종류, 서버 세대, 서버 타입, 요금제 선택

NAVER CLOUD PLATFORM

Professional Course Lab



Lab 1

- Cloud Log Analytics 서비스로 리눅스 서버 보안 로그 수집

Snapshot Operation

- 스토리지 단위로 스냅샷 생성

- 내서버 이미지와 다른 점
  - 내서버 이미지는 서버 단위로 스냅샷을 생성하는데 반해 스냅샷은 스토리지 단위로 스냅샷을 생성
  - 스냅샷은 추가 스토리지로만 변환 가능

- 용도
  - OS 영역의 문제로 부팅이 안되는 상황에서 OS 영역의 데이터를 복구해야 할 경우
    - OS영역의 스토리지를 스냅샷으로 생성하고
    - 해당 스냅샷을 다른 서버의 추가 스토리지로 변환 후
    - 해당 서버에서 원하는 데이터를 추출

NAVER CLOUD PLATFORM

- 라이브 스냅샷을 지원합니다.

스냅샷 대상은 볼륨에 한정됩니다. (참고. 스냅샷을 이용해서 서버를 생성할 수 없습니다)

Container Registry

- 컨테이너 이미지를 쉽게 저장하고 관리할 수 있는 컨테이너 레지스트리 관리 서비스
  - Public/Private Endpoint 제공을 통해 나만의 컨테이너 레지스트리를 구성
  - 도커 레지스트리 HTTP API V2 지원
- 저장소로 Object Storage를 이용
  - 컨테이너 관리가 용이
  - 컨테이너 취약점 분석 가능

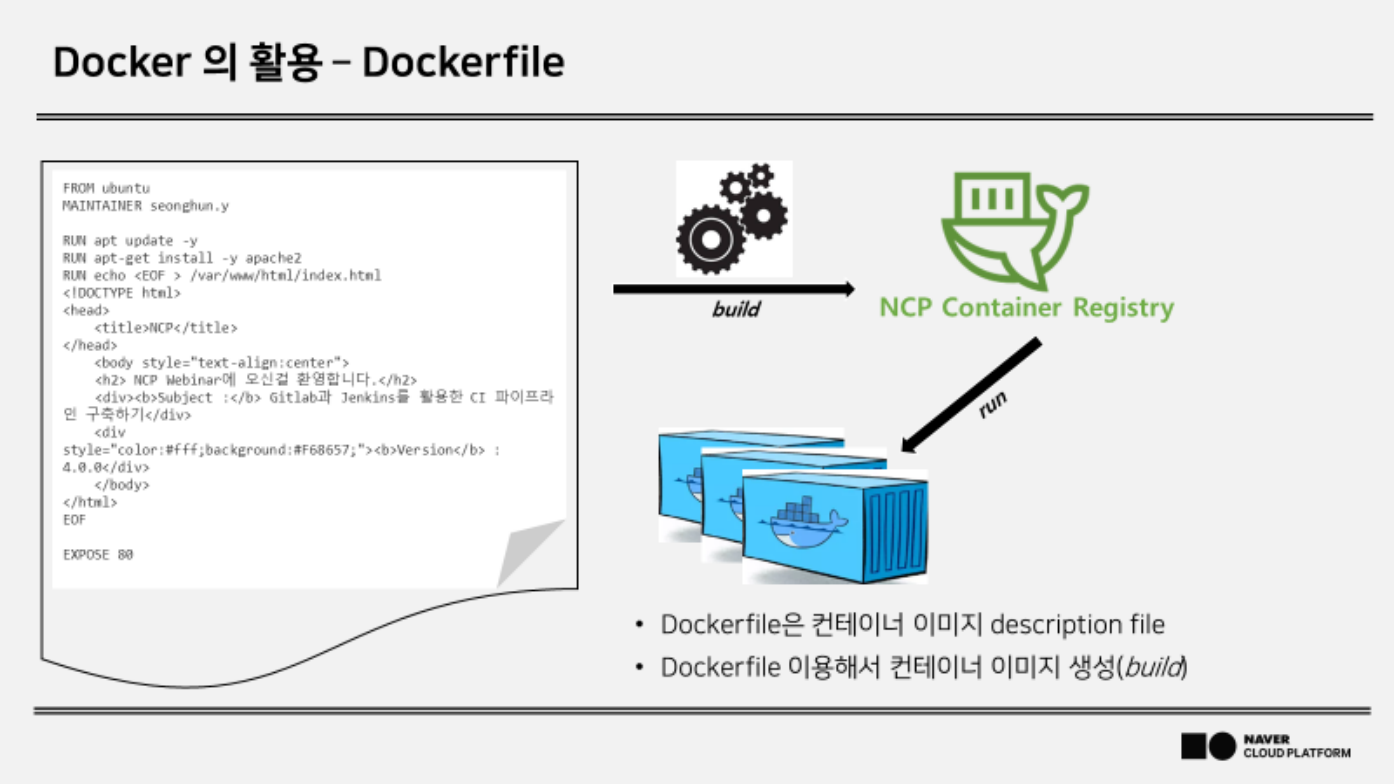
NAVER CLOUD PLATFORM

특성

네이버 클라우드 플랫폼의 서버 상품 및 도커 CLI와 쉽게 통합한 이용이 가능합니다.

또한 계정별 Push/Pull 권한 등의 권한제어가 가능하며, 도커 컨테이너 이미지에 대한 권한 관리 및 액세스 제어 정책을 구성할 수 있습니다.

Container Registry를 이용하기 위해서는 반드시 사전에 이미지 저장용도의 Object Storage 버킷을 만들어주셔야 합니다.



Dockerfile의 구조 및 Docker 기본 명령어

도커는 일반적으로 아래와 같은 구조로 작성됩니다.

FROM ubuntu:16.04	# 내가 만들 컨테이너 이미지의 베이스 이미지를 선택
MAINTAINER NAVERCLOUD	# 이미지를 만든 사람의 정보
RUN apt-get update	# 이미지로 뜰 컨테이너 내부에서 실행되야하는 명령어
RUN apt-get install apache2 -y	# 위와 동일
ADD welcome.html /var/www/html	# 특정 파일을 컨테이너 이미지에 추가 (파일이름/파일이 들어갈 위치)
EXPOSE 80	# 컨테이너 이미지에서 사용할 포트 설정
CMD apachectl -DFORGROUND	# 컨테이너가 실행될 때 마다 동작할 명령어 설정

위에서 언급된 명령어 말고도 도커에서 자주 쓰이는 기본 명령어들은 다음과 같습니다.

- LABEL: 라벨 설정
- ENV: 환경 변수 설정
- COPY: 파일 복사
- VOLUME: 볼륨 마운트
- WORKDIR: 작업 디렉토리 설정

도커란?

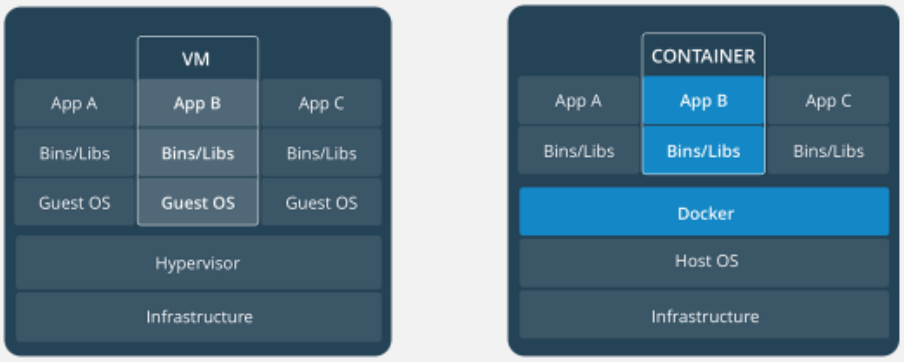
- Container 기반 오픈소스 플랫폼
- 2013년 3월 Python 컨퍼런스에서 Solomon Hykes가 "The Future of Linux Container" 세션에서 처음 소개

docker = Namespace
Cgroup
Union Filesystem
Overlay network
Docker Hub
API, etc..

기존에 있던 다양한 resource isolation 기술과 network, filesystem 기술들을 잘 조합하고
편의성을 올려 많은 개발자 / 엔지니어들에게 각광 받기 시작

NAVER CLOUD PLATFORM

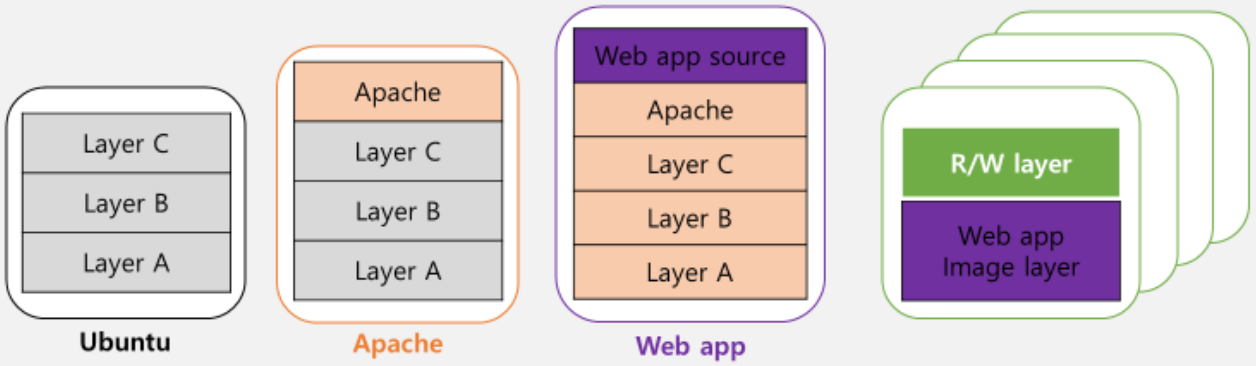
일반 VM과 컨테이너의 차이



- Virtualization은 단일 시스템에서 **여러 OS**가 동시에 실행
- Container는 **동일한 OS** 커널을 공유하며 시스템의 나머지 부분으로 **프로세스를 격리**
- 기존 가상화 기반으로 많이 사용되는 OS 전체 가상화 방식이 아닌, **하나의 OS 커널 위에** 각각의 개별 프로세스와 그에 따른 **환경을 격리화 시키는 방식**이다. OS 가상화 보다 오버헤드가 적고, 성능 손실이 적음.

NAVER CLOUD PLATFORM

Docker 특징 – Layered Image



- Docker는 Union Filesystem 이라는 기술을 이용해 여러 Layer를 하나의 파일 시스템으로 인식될 수 있도록 한다.
- 만약, 이미지에 수정 사항이 생기면, Layer를 추가하여 변경 분만 기록하고 최상단에는 항상 R/W layer가 존재
- 공통 부분은 Container들이 공유해 사용함으로써 효율적인 이미지 관리가 가능하다.

Docker 특징 – Docker Hub / Docker Registry

docker REGISTRY

docker hub

NCP Container Registry

AWS ECR

GCP Container Registry

- 사용자에 의해 생성된 이미지는 Docker Registry라는 이미지 저장 공간에 업로드할 수 있고, 다른 사용자의 이미지를 공유하여 사용 가능하다.
- Docker Hub, Private Registry (NCP Container Registry, ACR, ECR …)

NAVER CLOUD PLATFORM

Docker hub: https://hub.docker.com/

Lab 3

- Container Registry 서비스 생성
- Custom image 생성 후, Container Registry에 Push

Chapter 5. Storage 상품

NAS

- 다수의 VM이 **공유 가능한** 네트워크 볼륨 디바이스
- 용량은 500 ~10,000G으로 생성 가능, 100G 단위로 용량 증설 가능

- **NAS 특징**
  - NFS / CIFS 프로토콜 제공, 이기종 OS 간 공유 사용 위해 Samba 등의 추가 지원 필요
  - Live resizing 가능
  - 스냅샷 기능 제공 : 즉시 / 스케쥴 (-> 시점 복원 기능 제공)
  - 모니터링 기능 제공 (볼륨 사용량(%))
  - Custom IP에 NAVER Cloud Platform 내 VM 사설IP 등록을 통해 타 계정 VM 간 공유 사용 가능

NAVER CLOUD PLATFORM

- NAS 스냅샷
  - NAS 볼륨 가용량 안에서 스냅샷 저장 용량 비율(%) 설정 후 사용하게 되며, 설정 용량 초과 시 오래된(oldest) 스냅샷 이미지부터 삭제를 진행합니다.
  - 스냅샷 이미지를 이용 NAS 볼륨 복원 시 사용한 이미지 이후의 모든 스냅샷 이미지는 삭제 처리됩니다.

NAS

- 접근 제어
  - NFS의 경우 IP로 접근 제어
  - CIFS의 경우 ID와 패스워드로 접근 제어

- NAS Snapshot
  - NAS에 할당된 용량중 일정 부분을 스냅샷 공간으로 할당
  - Default는 스냅샷 미생성
  - 스냅샷은 스냅샷을 생성하는 시점에 NAS 스토리지에 있는 데이터에 대해 스냅샷 생성
  - 스냅샷은 최대 7일간 보관
  - 자동 생성 및 즉시 생성 가능

NAVER CLOUD PLATFORM

특성

네이버 클라우드 플랫폼 NAS 상품은 네이버 클라우드 플랫폼 인프라에 내부의 서버만 접근 가능합니다.

암호화 여부는 생성 시 설정이 가능하며, 한번 생성된 이후에는 설정을 변경할 수 없습니다.

Lab 5

- NAS 500GB 생성 (NFS)
- NAS Mount
- Snapshot 설정 및 테스트

NAVER
CLOUD PLATFORM

202 Network / Media

Chapter 1. Network & Content Delivery 상품

Lab 6

- (Demo)Peering 설정
  - VPN ID, 계정명, VPC 명 교환
  - Peering 구성
  - Route table 추가

Lab 7

- N-LB 로드밸런서 생성하기
  - Ncp-N-lb 로드밸런서 생성
  - Public IP 네트워크
  - TCP 프로토콜
  - Lnxsvr1, lnxsvr2 서버 추가

- A-LB 로드밸런서 생성하기
  - Ncp-A-lb 로드밸런서 생성
  - Public IP 네트워크
  - HTTP 프로토콜
  - Lnxsvr1, lnxsvr2 서버에 대해 URL로 분기

- Proxy LB 생성 및 클라이언트 IP 확인
  - Proxy LB 생성하기
  - 클라이언트 IP 확인을 위한 x-forwarded-for 설정

NAVER CLOUD PLATFORM

CDN+

- 사용자에게 컨텐츠를 보다 빠르고 안정적으로 전송하는 서비스
  - 원본 위치는 파일 스토리지 혹은 오리진 서버를 둘 수 있음
  - CDN을 사용하기 위해서는 CDN 도메인 혹은 보유 도메인을 이용하여야 함

- CDN이 언제 필요할까?
  - 대규모 파일 배포나 이미지 서비스, 동영상 서비스 등 대규모로 트래픽이 발생하는 경우
  - 웹서버를 통해 배포하게 되면 웹서버의 용량이 기하 급수적으로 커져야 함.
  - 이러한 대규모 트래픽에 효과적으로 대응하기 위한 서비스

- CDN에서 제공되는 형태
  - 원본 서버 캐싱 (파일 다운로드도 서버 캐싱의 형태)
  - 스트리밍 : 동영상이나 음악 파일을 스트리밍으로 제공 하는 경우

NAVER CLOUD PLATFORM

다양한 원본 서버 지원

원본으로 서버 뿐만 아니라 Object Storage도 지원, HTTP/HTTPS 도 지원하며 CDN은 HTTPS로 구성하면 원본 서버도 HTTPS로 구성하여야 함. 단, HTTPS 원본은 원본서버 혹은 Object Storage만 가능 (File Storage 불가)

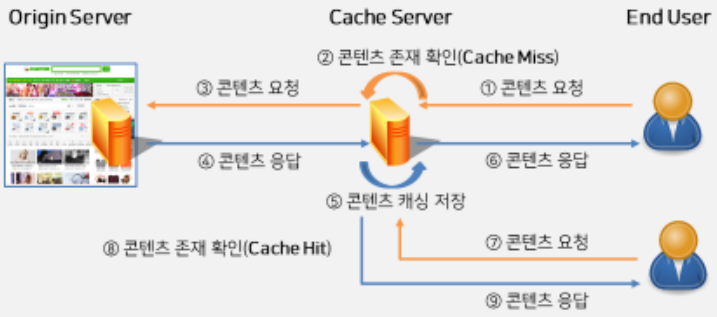
CDN 옵션

용어	설명
Purge	CDN 캐시서버에 저장 되어 있는 콘텐츠를 삭제하는 기능
Cache expiry	CDN에서 캐싱된 콘텐츠가 원본서버에서 변경되었는지 여부를 확인하는 주기를 지정
Streaming	네트워크(인터넷)를 기반으로 사용자들에게 멀티미디어 정보를 실-시간(Real-time)으로 제공하는 기술. 네이버 클라우드 플랫폼 CDN의 스트리밍 서비스는 HTTP Live Streaming, HTTP Pseudo Streaming, MPEG-DASH 프로토콜 지원.
Secure token	토큰 기반의 인증으로 허용된 접근에만 콘텐츠를 전달
Ignore query string	CDN 서비스가 원본 서버에 요청할 때 ?id=1234 와 같이 URL에 포함된 GET 파라미터를 제거한 후에 요청
Referrer domain	콘텐츠가 지정된 도메인에만 제공되므로 다른 사이트에서 참조되는 것을 방지함. 도메인은 www.domain.com 또는 *.domain.com 형식을 지원하며, 숫자, 영문자, "*", "-", "."만 사용 가능.
Access log	CDN 사용 로그를 확인할 수 있는 기능. CDN 사용 로그를 자신의 파일 스토리지 컨테이너에 약 10분 주기로 저장함. 서비스는 무료이나 파일이 저장되는 파일 스토리지 이용 요금은 따로 청구됨.

HIT	접속자가 요청한 콘텐츠가 유효한 형태로, CDN 캐시 서버에 있어 접속자의 요청에 대해서 바로 응답할 때 'HIT' 이라고 함.
MISS	요청한 콘텐츠가 CDN 캐시서버에 없을 경우 원본서버로부터 콘텐츠를 전송 받은 후 서버에 저장하게 되는 경우를 'MISS'라고 함. 이전에 요청된 이력이 없거나 유효 시간이 만료된 경우, 요청되었지만 응답한 적이 없거나 캐시를 하지 않도록 설정했을 경우에만 발생함.
BYPASS	원본서버 응답 헤더에 Set-Cookie 헤더가 있거나, Cache-Control 헤더에 private, no-cache, max-age=0 등의 내용이 있는 경우 CDN 서버에서 캐싱하지 않고 접속자에게 전달하는 것을 의미함.
동적 콘텐츠	PHP/ASP/JSP 등을 이용하여 접속자 별 요청에 대해서 서로 다른 콘텐츠를 응답하는 경우
정적 콘텐츠	일반적으로 JPG, PNG, GIF, MP4, ZIP, HWP, PDF 와 같이 모든 접속자에게 동일한 콘텐츠를 전달하는 경우

CDN+ 주요 옵션

- **캐싱(Caching) :** 사용자 요청에 의해 요구되는 콘텐츠를 빠르게 제공하기 위해 캐시 서버에 저장.
- **캐싱 Status :**
  1. **Cache Miss :** 콘텐츠 초기 요청 등 콘텐츠가 캐시 서버에 없는 경우 (원본 서버로부터 콘텐츠 전송 응답 및 캐싱)
  2. **Cache Hit :** 캐시 서버에 저장된 콘텐츠를 전송 응답



NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 CND+ 상품은 GS 네오텍을 통해 서비스합니다.

CDN+ 주요 옵션

- **Cashing expiry**
  - CDN+ 캐시 서버에서 캐싱된 콘텐츠가 원본 서버에서 변경되었는지 여부를 확인하는 주기를 지정합니다. 단, 원본 서버의 응답 헤더에 Cache-Control: max-age가 존재하면 해당 설정이 우선됩니다. 콘텐츠를 자주 업데이트하는 경우에는 짧게 지정하여 설정합니다. 단, 짧게 지정하면 원본의 부하가 늘어나니 주의해서 사용합니다.
- **Purge**
  - Purge는 캐시 서버에 저장된 콘텐츠를 삭제하는 기능
  - 대규모 수행 시 원본 부하 고려 필요
- **압축 설정**
  - 사용자의 User-Agent(브라우저 혹은 Device)가 Gzip/Unzip을 지원할 경우 콘텐츠를 압축하여 사용자에게 전달함으로써, 네트워크 품질이 낮은 사용자에게 압축 전송을 하면 응답 속도를 개선할 수 있습니다.
  - 원본 서버에서 콘텐츠 확장자 혹은 요청 헤더에 따라 압축/미압축 응답을 유연하게 적용하기 위해서는 '원본의 압축 설정과 동일하게 적용'을 선택하시면 됩니다.

NAVER CLOUD PLATFORM

CDN+ 주요 옵션

- 컨텐츠를 배포할 경우 사용자 별 컨텐츠 엑세스 권한을 제한할 필요가 있으며, CDN 상품을 이용해서 프라이빗 컨텐츠에 대한 엑세스를 제한하는 방법은 아래와 같이 2가지 방법이 있음

- Secure Token을 이용해서 다운로드 허용 시간 설정
  - Secure Token은 일회성으로 Access Token을 생성하여 콘텐츠 요청 시 인증을 통과한 요청에만 콘텐츠를 응답
  - Secure Token을 생성하는 SDK를 Programming 언어 별 제공(Python, JAVA, Ruby, NodeJS)
  -
- Referrer 설정을 통한 인가된 요청만 컨텐츠 딜리버리
  - 컨텐츠를 요청하는 Referrer 에 따른 컨텐츠에 대한 접근 제어를 설정할 수 있습니다.
  - 기본 설정으로 Referrer 가 없는 경우에 대해서도 컨텐츠 접근을 허용하므로 특정 Referrer 에 대해서만 허용하려면 CDN 상품 생성 시 엑세스를 허용할 도메인 설정과 "레퍼러 없는 경우 허용 여부" '설정을 "허용 안함'을 선택해야 합니다.

NAVER CLOUD PLATFORM

Global CDN

- CDN+ 가 국내용 CDN 서비스인데 반해 글로벌 CDN 서비스를 이용하고자 할 때
  - 아카마이(Akamai)를 통해 CDN 서비스
- CDN+와 GCDN을 동시에 이용하고자 하는 경우
  - GRM을 이용하여 해외 트래픽 분산

NAVER CLOUD PLATFORM

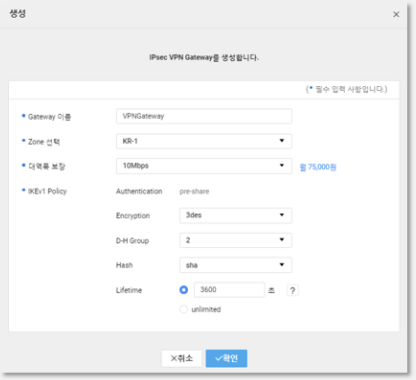
GCDN 용어 정리

용어	설명
서비스 도메인	서비스에서 콘텐츠 전송 시 사용자에게 노출되는 도메인을 의미. Global CDN 구성 후 이 도메인을 서비스 내에 링크해야 Global CDN 을 통해 콘텐츠를 캐싱하여 전송
원본	Global CDN 은 사용자 요청에 의하여 콘텐츠를 캐싱/전송하며, 캐싱의 콘텐츠를 가져오기 위한 서버
Caching	사용자 요청에 의해 요구되는 콘텐츠를 빠르게 제공하기 위해 캐시 서버에 저장
Cache Expiry	CDN 에서 캐싱된 콘텐츠가 원본 서버에서 변경되었는지 여부를 확인하는 주기를 지정
HIT	접속자가 요청한 콘텐츠가 유효한 형태로, CDN 캐시 서버에 있어 접속자의 요청에 대해서 바로 응답할 때 “Cache Hit”이라고 함
MISS	요청한 콘텐츠가 CDN 캐시서버에 없을 경우 원본 서버로부터 콘텐츠를 전송 받은 후 서버에 저장하게 되는 경우를 ‘MISS’라고 함. 이전에 요청된 이력이 없거나 유효 시간이 만료된 경우, 요청되었지만 응답한 적이 없거나 캐시를 하지 않도록 설정했을 경우에만 발생함.
BYPASS	원본 서버 응답 헤더에 Set-Cookie 헤더가 있거나, Cache-Control 헤더에 private, no-cache, max-age=0 등의 내용이 있는 경우 CDN 서버에서 캐싱하지 않고 접속자에게 전달하는 것을 의미함.
Ignore Query String	CDN 서비스가 원본 서버에 요청할 때 ?id=1234 와 같이 URL 에 포함된 GET 파라미터를 제거한 후에 요청
Referrer Domain	콘텐츠가 지정된 도메인에만 제공되므로 다른 사이트에서 참조되는 것을 방지함. 도메인은 www.domain.com 또는 *.domain.com 형식을 지원하며, 숫자, 영문자, "*", "-", "."만 사용 가능.
Secure Token	QueryString 기반의 Secure Token 을 활용하여 허용된 접근에만 콘텐츠를 전달

IPSEC VPN

- 고객의 사내망과 네이버 클라우드 플랫폼 간 사설 통신을 위한 IPSEC VPN
- 임대형 Managed IPsec VPN 형태로 서비스 제공 (VPN 장비 임대)
  - 안랩, 시큐아이, 주니퍼, 포티넷, 팔로알토, 퓨처시스템, 두루안, 소닉월, AXGATE, XN시스템즈 등
- ① 영업 담당자와의 컨설팅 > ② [상품 이용 신청서] 작성 및 제출 이후 상품 이용 가능

- ※ 참고) Classic 플랫폼 IPSEC VPN의 특징
  - Classic 플랫폼에서는 IPsec VPN을 콘솔을 통해 이용이 가능
  - Private Subnet 대역(192.168.x.x) 으로 Tunnel 생성 가능
  - BW 최대 30Mbps 제공



NAVER CLOUD PLATFORM

Lab 8

- CDN - 프라이빗 컨텐츠에 대한 엑세스 제한
  - Referrer 설정을 통한 인가된 요청만 컨텐츠 딜리버리 설정

과목소개

네이버클라우드플랫폼 공인교육과정 203 과목에서는 Database/Management/Analytics 상품에 대해 살펴봅니다.

Agenda

- 네이버클라우드플랫폼의 Database – Cloud DB
  - 네이버클라우드플랫폼 Cloud DB Overview 및 개요
  - 네이버클라우드플랫폼 Cloud DB 상품구성
  - Cloud DB Operation 기능 확인

- 네이버클라우드플랫폼 Management
  - 네이버클라우드플랫폼 Management 상품군의 개요 및 특징
  - Monitoring, Sub Account, WMS, Network Traffic Monitoring, Cloud Activity Tracer 등 상품 기능 소개

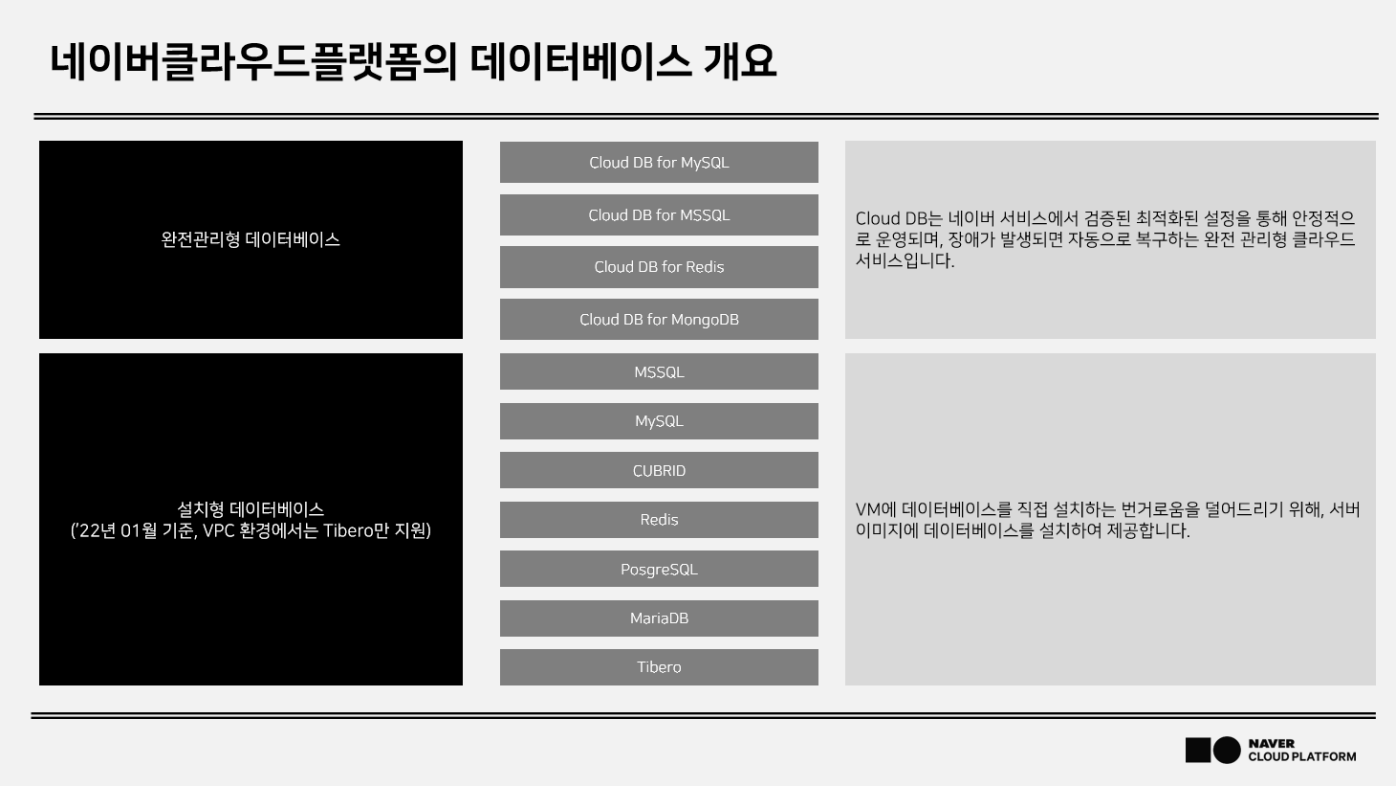
- 네이버클라우드플랫폼 Analytics
  - 네이버클라우드플랫폼 Analytics 상품군의 개요 및 특징
  - CLA, RUA, ELSA, Cloud Hadoop, Cloud Search 등의 상품 기능 소개

NAVER CLOUD PLATFORM

203 과목 아젠다

네이버클라우드플랫폼 Database 상품에서는 Database 설치형과 완전관리형에 대해 살펴봅니다. 네이버클라우드플랫폼의 Database 완전 관리형의 경우, Cloud DB로 상품명이 시작되며 각 Cloud DB 서비스에 대한 핵심 기능 및 타사 상품과의 스펙을 비교해볼 예정입니다. Management 상품군에서는 Monitoring, Sub Account, WMS, Network Traffic Monitoring, Cloud Activity Tracer에 대해서 자세히 살펴볼 예정입니다. 마지막으로 Analytics 상품에서는 CLA, RUA, ELSA, Cloud Hadoop, Cloud Search에 대해서 살펴보도록 하겠습니다.

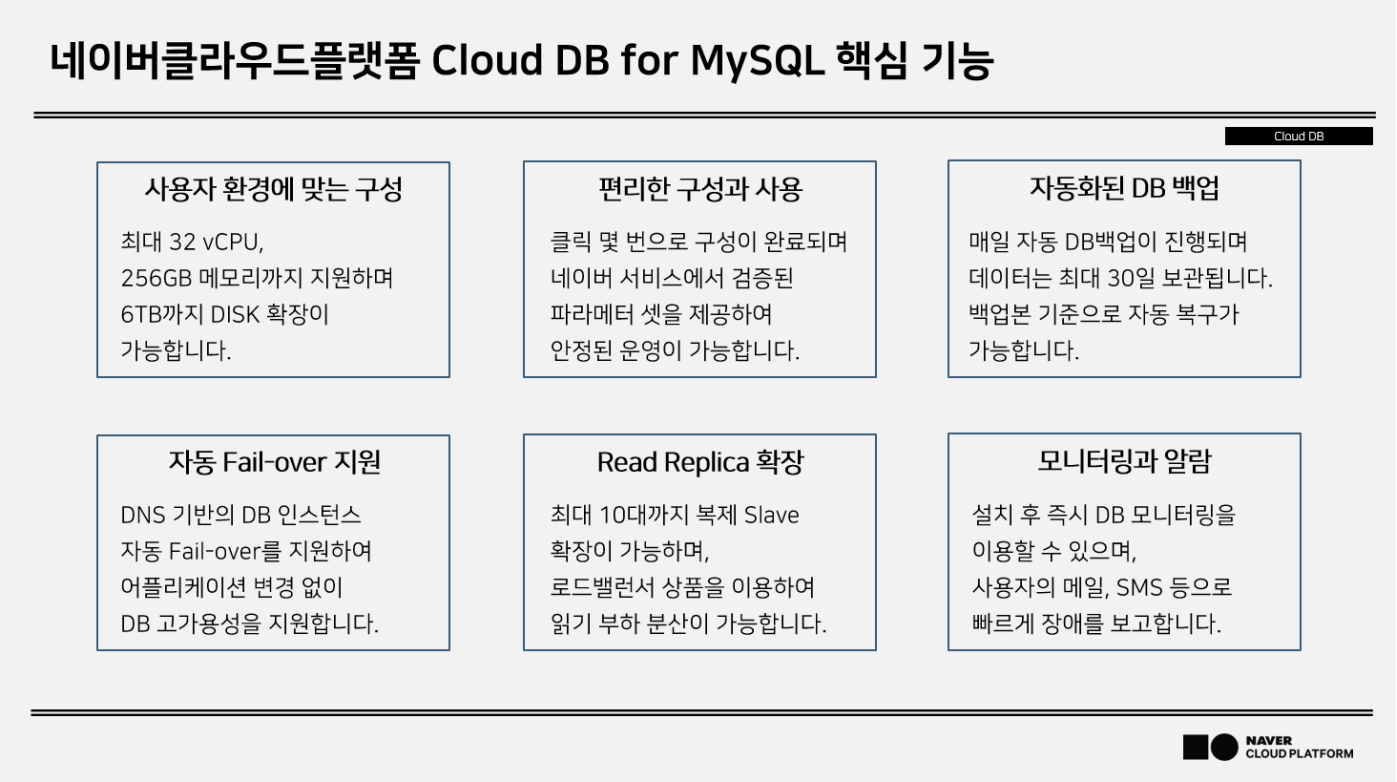
Chapter 1. 네이버클라우드플랫폼 데이터베이스



완전관리형 데이터베이스와 설치형 데이터베이스

네이버클라우드플랫폼의 Database 상품은 완전관리형 데이터베이스와 설치형 데이터베이스로 나뉩니다. 완전관리형 데이터베이스의 경우 Cloud DB라는 서비스명으로 시작되며 현재 MySQL, MS-SQL, Redis, Mongo(VPC only) 이렇게 4가지 DBMS를 제공하고 있습니다. (Cloud DB로 제공되는 DBMS는 지속적으로 추가되고 있습니다.) 설치형 데이터베이스의 경우, VM에 데이터베이스를 설치하는 번거로움을 없앤 서비스로서 서버 이미지 형태로 제공하고 있습니다. 그렇다면 완전관리형 데이터베이스와 설치형 데이터베이스는 어떤 차이점이 있는지 좀 더 자세히 살펴보도록 하겠습니다.

완전관리형 데이터베이스는 자동 Fail-over, 자동 back-up 등 데이터베이스 설정 시 어려운 작업들은 쉽게 위자드 형태로 구성하실 수 있습니다. 반면 데이터베이스 설정에 있어 일부 제한이 있을 수 있습니다. 설치형 데이터베이스의 경우 사용자가 직접 데이터베이스 설정 작업을 진행해야 하는 번거로움이 있지만 사용자가 원하는 대로 데이터베이스를 설정하실 수 있습니다.



Cloud DB for MySQL 핵심 기능

Cloud DB for MySQL의 핵심기능은 다음과 같습니다.

1) 사용자 환경에 맞는 구성이 가능합니다: 최대 32개 vCPU 256GB까지 제공되어 사용자가 원하는 스펙을 선택하여 데이터베이스를 생성하실 수 있으며 데이터스토리지가 최대 6TB까지 제공됩니다.

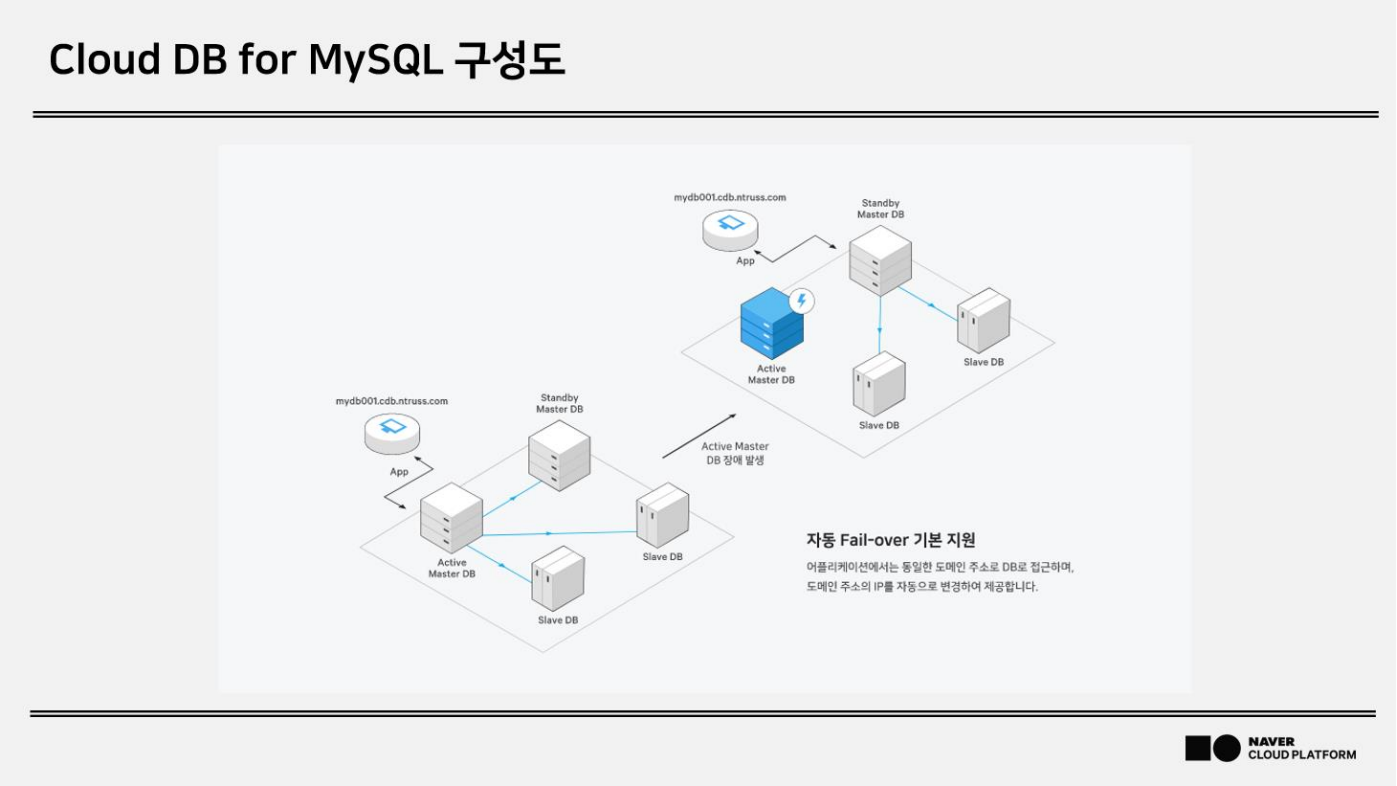
2) 편리한 구성과 사용이 가능합니다: 클릭 몇 번이면 쉽게 데이터베이스 생성 및 구성이 가능하며, 네이버 서비스를 제공하며 쌓은 경험이 반영된 파라미터 셋을 제공하여 안정적인 서비스 운영이 가능합니다.

3) 자동화된 DB 백업을 지원합니다: Cloud DB for MySQL 생성 시 설정한 백업 시간에 맞춰 자동 백업이 진행됩니다.

4) 자동 Fail-over 기능을 제공합니다: Master DB 상태를 체크하는 별도의 모니터 서버에서 DB 서버에 연결하여 쿼리 수행을 주기적으로 진행하고 약 1분간 연속해서 쿼리 응답이 없을 때(서버 장애나 DB 프로세스 다운 등) Master DB를 fail 상태로 인지하고 Standby Master로 Fail-over를 진행합니다.

5) Read Replica 확장이 가능합니다: 최대 10대까지 Slave DB를 추가할 수 있으며 추가된 Slave DB로 읽기 부하분산이 가능합니다.

6) 모니터링과 알람 기능을 제공합니다: 모니터링과 알람 기능을 제공하며 데이터베이스에 문제시 관리자가 빠르게 파악하고 작업할 수 있도록 지원합니다.



Cloud DB for MySQL 상품은 기본적으로 액티브 마스터 DB와 스탠바이 마스터 DB를 생성하여 액티브 마스터 DB 장애 시, 스탠바이 마스터DB로 자동 Fail-over 합니다. DNS 방식으로 이중화를 제공함으로써 어플리케이션의 변경이 필요 없습니다.

Cloud DB for MySQL 은 Slave DB 를 최대 5 대 추가할 수 있습니다. Slave DB 추가는 Master DB 생성 후, DB 관리 메뉴의 Slave 추가 메뉴를 통해 가능합니다. Slave DB 는 최신 백업파일을 바탕으로 생성된 후, 최신 트랜잭션 로그까지 반영하여 생성됩니다.

Cloud DB for MySQL

- DB 엔진 버전
  - MySQL5.7.19, MySQL5.7.25, MySQL5.7.29, MySQL5.7.32
  - MySQL8.0.18, MySQL8.0.21, MySQL8.0.25
- VPC 환경에서는 High CPU, Standard, High-memory 타입 제공
- 최대 10대의 Slave DB 추가 가능
- 데이터 스토리지는 HDD,SSD 중 선택 가능
  - 데이트 스토리지는 데이터베이스 데이터(테이블, 인덱스, 로그 등)의 데이터를 저장하는 스토리지
  - 기본 100GB부터 10GB 단위로 최대 6000GB까지 자동 증가
- 고가용성이 지원되는 스펙과 Stand alone 형태로 생성 가능
- Public Subnet에 생성된 Cloud DB for MySQL 서버에는 Public domain 부여를 통해 외부에서 접근 가능

NAVER CLOUD PLATFORM

Cloud DB for MySQL

- 멀티존 지원
  - Master DB 서버 2대를 서로 다른 Zone에 생성하여 높은 가용성 제공
  - Master DB 서버는 같은 속성의 Subnet에 위치

- Public Subnet과 Private Subnet에 구성하는 것의 차이
  - Public Subnet에 구성하는 경우 Public 도메인을 구성할 수 있으나 Private Subnet은 구성 불가

CDB Operation 1. DB Process list 확인

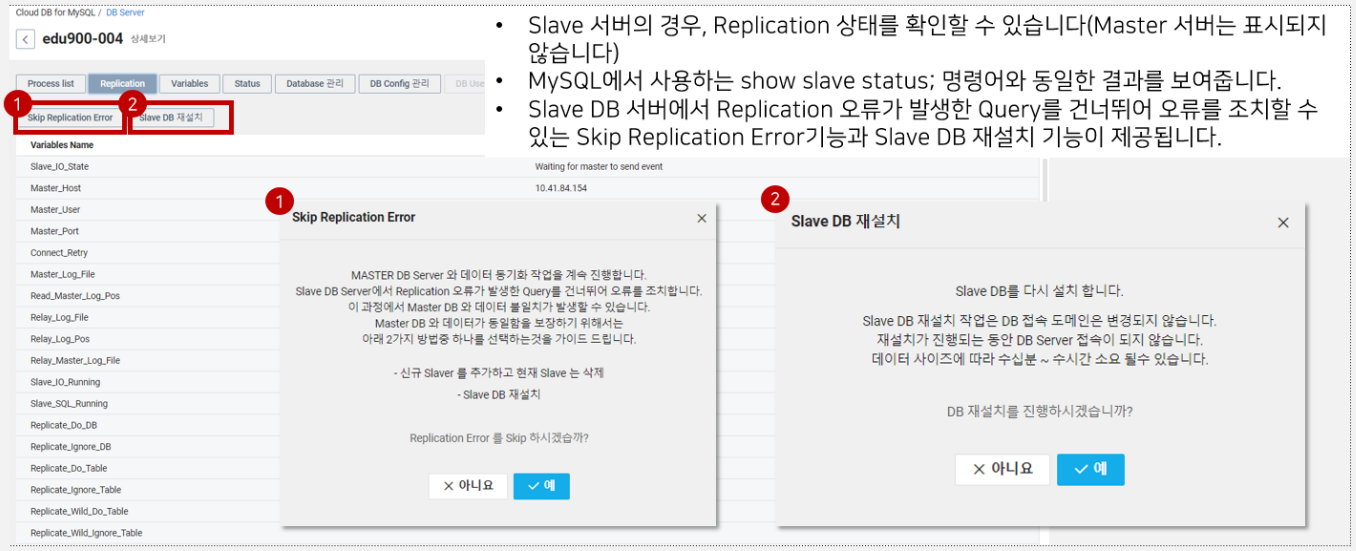
- 데이터베이스 서버에 현재 접속한 세션 리스트를 확인해볼 수 있습니다.
- MySQL에서 사용하는 show process list;와 동일합니다.
- 제공 항목

항목	설명
Session ID	접속한 세션의 고유번호
USER	접속한 세션이 사용한 유저명
HOST(IP)	접속한 세션의 호스트 IP 주소
DB	접속한 세션이 사용한 DB명
Command	접속한 세션이 수행한 명령어
Time	수행한 명령어의 수행 시간
State	접속한 세션의 상태를 나타내는 값

- Kill session
  - 선택된 Session ID를 강제로 종료
  - 강제로 종료한 세션은 복구 불가능
  - 하나의 세션만 선택 가능

NAVER CLOUD PLATFORM

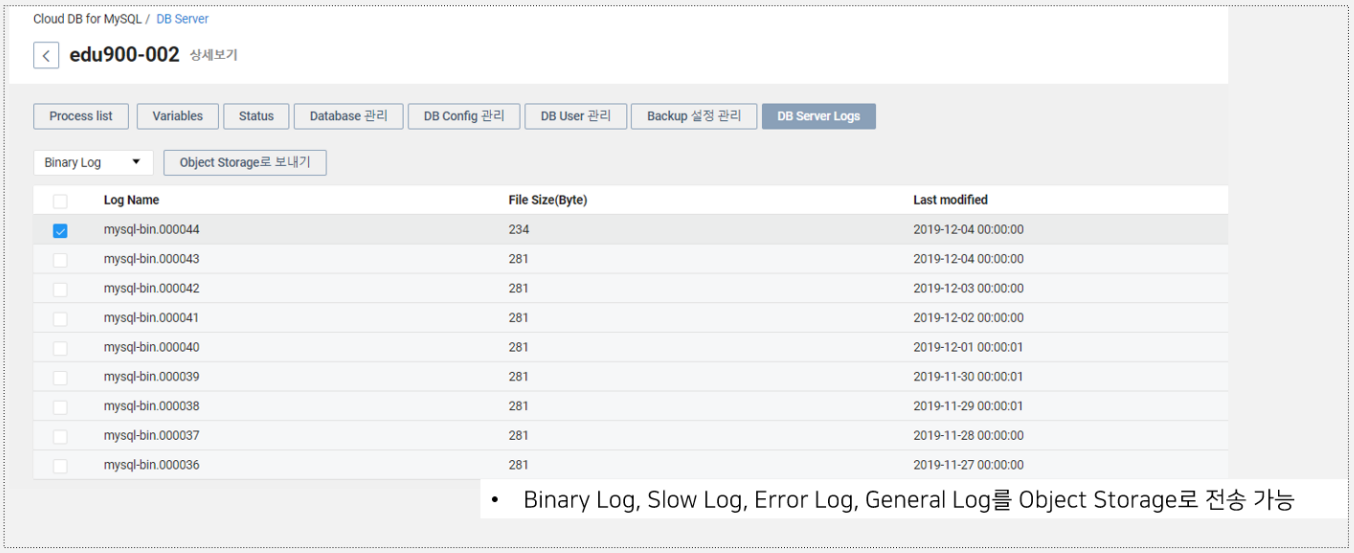
CDB Operation 2. Slave DB Replication 확인



- Slave 서버의 경우, Replication 상태를 확인할 수 있습니다(Master 서버는 표시되지 않습니다)
- MySQL에서 사용하는 show slave status; 명령어와 동일한 결과를 보여줍니다.
- Slave DB 서버에서 Replication 오류가 발생한 Query를 건너뛰어 오류를 조치할 수 있는 Skip Replication Error기능과 Slave DB 재설치 기능이 제공됩니다.

NAVER CLOUD PLATFORM

CDB Operation 3. DB 서버 로그 확인



Log Name	File Size(Byte)	Last modified
mysql-bin.000044	234	2019-12-04 00:00:00
mysql-bin.000043	281	2019-12-04 00:00:00
mysql-bin.000042	281	2019-12-03 00:00:00
mysql-bin.000041	281	2019-12-02 00:00:00
mysql-bin.000040	281	2019-12-01 00:00:01
mysql-bin.000039	281	2019-11-30 00:00:01
mysql-bin.000038	281	2019-11-29 00:00:01
mysql-bin.000037	281	2019-11-28 00:00:00
mysql-bin.000036	281	2019-11-27 00:00:00

- Binary Log, Slow Log, Error Log, General Log를 Object Storage로 전송 가능

CDB Operation 4. DB 백업 설정 및 복원

- 백업은 하루에 한번 매일 수행되며, 사용자 설정에 따라 최대 30일까지 보관이 가능합니다.
- 백업 관련 정보

항목	설명
DB서비스 이름	사용자가 지정한 서비스 이름
Backup 보관일	백업 파일의 보관일
Backup 시작 시간	백업이 시작되는 시간
Backup 데이터 크기	완료된 백업 파일의 크기
마지막 Backup 일자	백업이 가장 마지막으로 수행된 일자
상세정보보기	선택된 DB서버에 대한 백업 내용을 상세히 볼 수 있는 페이지로 이동

- 백업 파일을 바탕으로 데이터 베이스 복원 기능을 제공합니다.
- 백업 파일로 복원 시, 신규 VM이 생성되며 이 때 데이터베이스 서버는 Recovery 모드로 복원되며 데이터 조회만 가능합니다.
- 시점 복원 기능을 제공하여 복원 가능한 시간 범위 내에서 사용자가 원하는 시간대로 데이터 복원이 가능합니다(분 단위까지 지원)

NAVER CLOUD PLATFORM

CDB Operation 5. 이벤트 설정

- OS 영역 이벤트 항목

알람 항목	알람 세부 항목	설명
CPU	Used(%)	CPU 사용량
CPU	Iowait(%)	CPU Iowait 사용량
Memory	used(%)	메모리 사용량
Swap	swap_pct	Swap 메모리 발생량
Disk I/O	Read bytes / Write bytes	Disk의 읽기/쓰기 발생량
Network	bps in	NIC의 초당 outbound byte
Load Average	1min/5min/15min	서버 부하량
Filesystem	used(%)	디스크 사용량

- DB 영역 이벤트 항목

알람 항목	알람 세부 항목	설명
Connections	Running	DB 접속 세션 수
SlowQuery	SlowQueryCount	1초 이상 실행되는 쿼리 개수
Replication	Stop	복제 중단 정보
Replication	Delay	마스터 대비 복제 지연 시간
DB	Down	DB 다운 정보

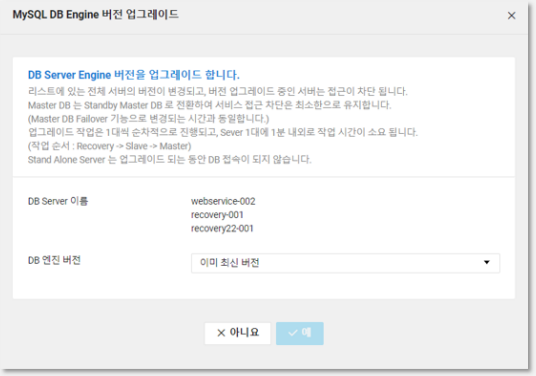
NAVER CLOUD PLATFORM

Cloud DB for MySQL 상세 기능 – 이벤트 History

Cloud DB for MySQL은 별도의 설정없이 Event History를 확인할 수 있으며, 생성된 Event History데이터는 영구 보관되며 기본적으로 1일 내에 발생한 데이터를 보여줍니다(그 이외의 기간에 대한 데이터를 보고 싶을 경우, 조회 하고 싶은 기간을 선택하시면 됩니다).

CDB Operation 6. DB 엔진 업그레이드

- MySQL의 Minor 버전 Rolling 업그레이드 지원
- 버전 업그레이드는 동일한 서비스 내 모든 DB서버 버전이 변경
- Master DB는 Standby Master DB로 전환하여 서비스 접근 차단을 최소화
- 업그레이드 작업은 1대씩 순차적으로 진행

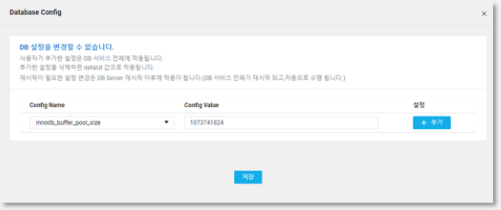


NAVER CLOUD PLATFORM

CDB Operation 7. DB Config관리

- 네이버클라우드플랫폼의 Cloud DB for MySQL에서는 DB 서버 상세보기 화면 > **DB Config 관리를 통해** 선택한 DB 서버의 설정을 변경할 수 있습니다.
- 기본적으로 자주 변경하는 대표적인 configuration은 아래와 같습니다.

1. innodb_buffer_pool_size
   - ✓ innodb_buffer_pool은 데이터 파일과 로그 파일이 기록되는 순서를 조정하는 역할과 디스크 액세스를 줄이기 위한 캐시의 역할을 합니다.
   - ✓ 보통 메모리의 50~80% 로 설정합니다.
   - ✓ 네이버클라우드플랫폼 innodb_buffer_pool_size는 default로 1073741824로 설정되어 있습니다.
   - ✓ 이 부분을 수정한 후에는 반드시 db를 재시작해야 합니다.



CDB Operation 7. DB Config관리

2. max connections
   - ✓ max connections 설정값 초과분에 대해서는 Too many connections 오류 발생합니다.
   - ✓ Default값은 3000입니다. (MySQL 5.7기준)
   - ✓ online중에 설정 및 적용 가능하나 db를 재시작해서 설정값을 확인하는 것이 좋습니다.
3. general log
   - ✓ mysql에서 실행되는 전체 쿼리에 대한 로그입니다.
   - ✓ 로그 출력형태는 general_log table에 쌓이는 방식으로 진행하고
   - ✓ 언제(Time), 누가(User), 어디서(Host) 쿼리를 수행했는지 여부 확인이 가능합니다.

그 밖에도 현재 CDB에서 제공되는 config 변경 건들 모두 자주 사용되는 변수를 모아두었음을 참고하시면 됩니다.

NAVER CLOUD PLATFORM

Lab 9

- Workbench로 Cloud DB for MySQL 사용하기
  - 샘플데이터 다운로드
  - 샘플데이터 Cloud DB for MySQL에 Import 하기
  - 유저 추가 후 콘솔에서 해당 추가 유저 불러오기
  - 데이터베이스 추가 하기
- Cloud DB for MySQL 주요 Config 값 설정 조정
- Cloud DB for MySQL 이벤트 설정하기
- Cloud DB for MySQL Fail-over 테스트

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 Cloud DB for MSSQL 핵심 기능

Cloud DB

"데이터베이스를 직접 구성했을 때의 번거로움을 덜어줄 수 있는
자동화된 기능을 제공하며, 콘솔상에서 쉽게 생성이 가능합니다."

사용자 환경에 맞는 구성

최대 24 vCPU,
128GB 메모리까지 지원하며
2TB까지 DISK 확장이
가능합니다.

편리한 구성과 사용

클릭 몇 번으로 구성이 완료되며
네이버 서비스에서 검증된
파라메터 셋을 제공하여
안정된 운영이 가능합니다.

자동화된 DB 백업

매일 자동 DB백업이 진행되며
데이터는 최대 30일 보관됩니다.
보관 기간 내의 특정 시점으로의
복원을 지원 합니다.

자동 Fail-over 지원

비용이 저렴한 Standard edition
을 사용하고도 자동 Failover 를
지원하여
어플리케이션 변경 없이
DB고가용성을 지원합니다.

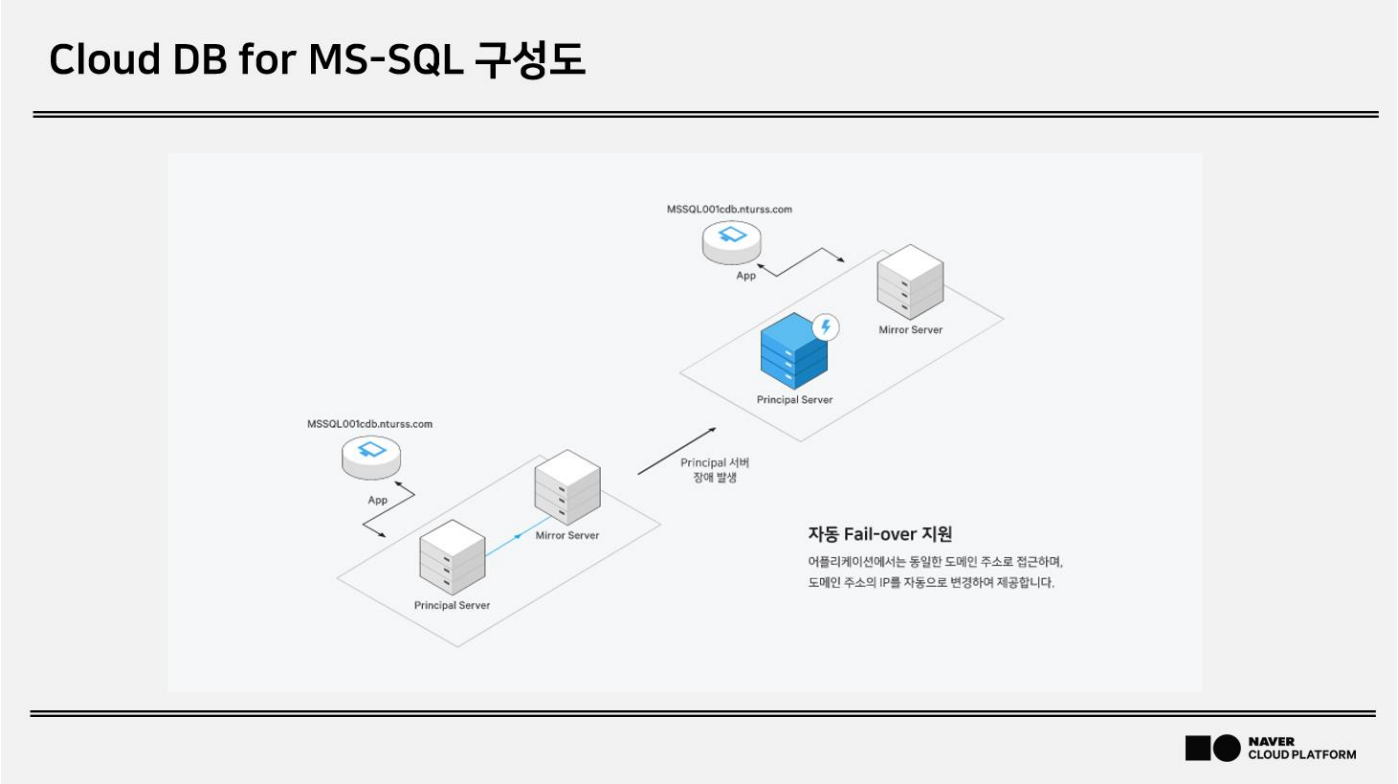
모니터링과 알람

설치 후 즉시 DB 모니터링을
이용할 수 있으며,
사용자의 메일, SMS 등으로
빠르게 장애를 보고합니다.

쿼리 분석

1분 단위의 쿼리 레벨
성능 분석을 지원하여
서비스 성능 과 안정성을 향상
시킬 수 있습니다.

NAVER CLOUD PLATFORM



Cloud DB for MS-SQL 구성

Cloud DB for MS-SQL은 Standard 타입과 High-memory 타입이 있으며 Standard 타입은 최대 vCPU 16개 32GB 메모리를 제공하며 High-memory 타입은 vCPU 24개 128GB까지 제공합니다. Cloud DB for MS-SQL 생성 시 고가용성 지원을 클릭하면 Principal DB와 Mirror DB가 생성이 되며 2개의 DB에 대한 시간당 요금이 발생하게 됩니다. (만약 고가용성 지원을 체크하지 않으면 Principal DB만 생성 됩니다.)

Cloud DB for MS-SQL

- Standard 타입과 High-memory 타입을 제공
- 데이터스토리지는 HDD,SSD 에서 선택
  - 데이터스토리지는 Cloud DB 생성 이후, 변경 불가능
  - 데이터스토리지는 100GB부터 2TB까지 10GB씩 자동 확장
- 고가용성이 지원되는 타입과 Stand-alone 타입 선택 가능
  - Stand-alone 타입으로 생성하였다가 고가용성 지원 타입으로 변경 가능
- 1분 단위의 쿼리 레벨 성능 분석 제공
- 자동 Fail-over 지원
  - 기본적으로 Principal DB와 Mirror DB를 생성하여 Principal DB 서버 장애 시 Mirror DB로 자동 Fail-over
- Slave DB는 5대까지 추가 가능

NAVER CLOUD PLATFORM

CDB Operation 1. DB Config 및 Config Group 관리

- DB Config 관리를 클릭하면, 선택한 DB서버에 적용할 Config Group을 변경할 수 있습니다.
  - Cloud DB 상품의 서비스 특성에 맞게 sp_config와 trace flag를 변경해 config group을 생성할 수 있음
  - Config group 생성 뿐만 아니라 변경, 삭제 가능
  - Config group이 적용된 서버가 있을 경우, config group 삭제 불가능
  - Config group을 이미 적용한 Cloud DB 서비스가 있다면, 해당 DB서버들도 변경 적용(재시작이 필요할 경우, 서버 재시작후 적용)

NAVER CLOUD PLATFORM

Cloud DB for MS-SQL Config Group

Cloud DB 상품의 서비스 특성에 맞게 sp_configure와 trace flag를 변경해 Config Group을 생성할 수 있습니다. 생성된 Config Group은 여러 Cloud DB 서비스에 적용이 가능합니다. Config Group을 이미 적용한 Cloud DB 서비스가 있다면 해당 DB 서버들도 변경 적용되며, 재시작이 필요한 변경은 Cloud DB 서버 재시작 후에 적용됩니다.

CDB for MS-SQL Operation 1. Config Group

생성 변경 삭제

DB Config Group 생성

Sp_configure 와 trace flag 를 변경하여 새로운 Config Group 을 생성 할 수 있습니다.
Config Group을 서버 별로 적용할 경우, 일부 재시작이 필요한 변경은 재시작 이후에 적용 됩니다.

Config Group 이름 : 생성 취소

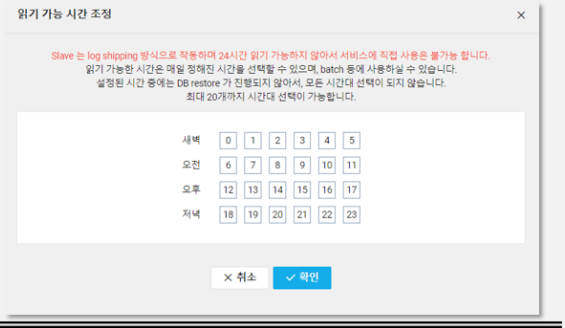
① ②

ID	NAME	VALUE	MIN	MAX	IS_DYNAMIC	DESC
103	user connections	0	0	32767	0	sp_configure
117	remote access	1	0	1	0	sp_configure
503	max worker threads	0	128	65535	1	sp_configure
505	network packet size (B)	4096	512	32767	1	sp_configure
518	show advanced options	1	0	1	1	sp_configure
1520	remote query timeout (s)	600	0	2147483647	1	sp_configure
1538	cost threshold for parallelism	5	0	32767	1	sp_configure
1539	max degree of parallelism	1	0	32767	1	sp_configure

NAVER CLOUD PLATFORM

CDB for MS-SQL Operation 2. Slave DB 추가

- Slave DB는 log shipping 방식으로 생성되며, transaction log 백업을 restore하는 동안에는 읽기가 불가능하여 일반 서비스 용도로는 사용이 불가능함
- 매일 주기적인 BI 및 Batch 작업에 적합함
- 시간 단위로 읽기 가능한 시간을 최대 20시간까지 설정 가능
- 읽기 가능 Slave는 최대 5대까지 생성 가능
- 읽기 가능 Slave의 spec을 변경하면, principal 과 mirror 서버도 함께 변경

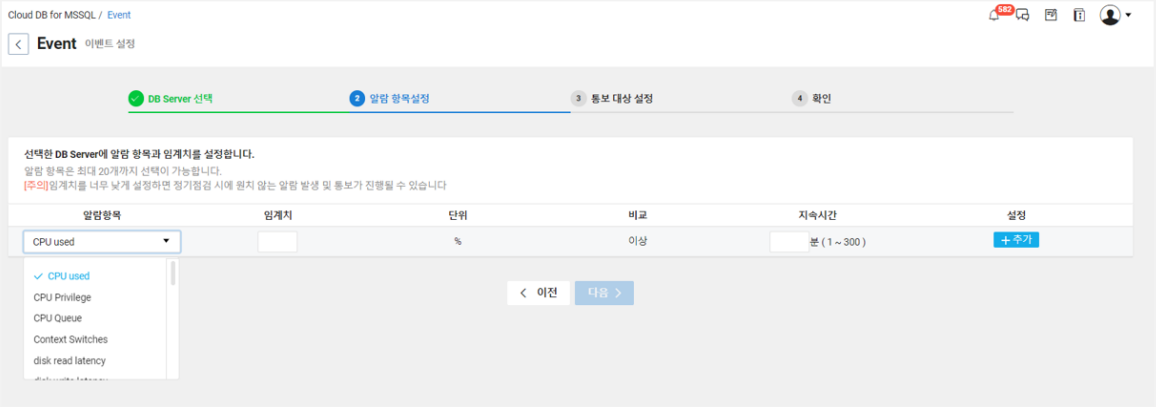


NAVER CLOUD PLATFORM

읽기가능 Slave는 Log-Shipping 방식으로 진행하여, transaction log 백업을 restore 하는 시간 동안에는 읽기가 불가능하여 일반 서비스 용도로는 사용할 수 없습니다. Slave DB는 매일 주기적인 Batch 및 BI 등의 목적으로 활용하기에 적합합니다.

CDB for MS-SQL Operation 3. 이벤트 설정

- Cloud DB for MSSQL 서버에서 발생한 이벤트 이력 확인 가능
- 서비스별로 알람 항목과 임계치를 설정하여, 임계치를 넘은 이벤트에 대해서 메일과 SMS로 실시간 통보 설정 가능



NAVER CLOUD PLATFORM

Cloud DB for MS-SQL 메뉴에서 서버에서 발생한 이벤트 및 서버 별로 알람 항목과 임계치를 설정하여, 임계치가 넘은 이벤트에 대해서 메일과 SMS로 실시간 통보 알람을 받을 수 있습니다. 알람 항목은 최대 20개까지 선택이 가능합니다.

통보에 대한 일시정지 기능을 통해, 배치 작업 등으로 이벤트가 발생한 상황에서 통보를 일시적으로 정지가 가능합니다. 이벤트 항목으로 설정가능한 항목은 아래와 같습니다.

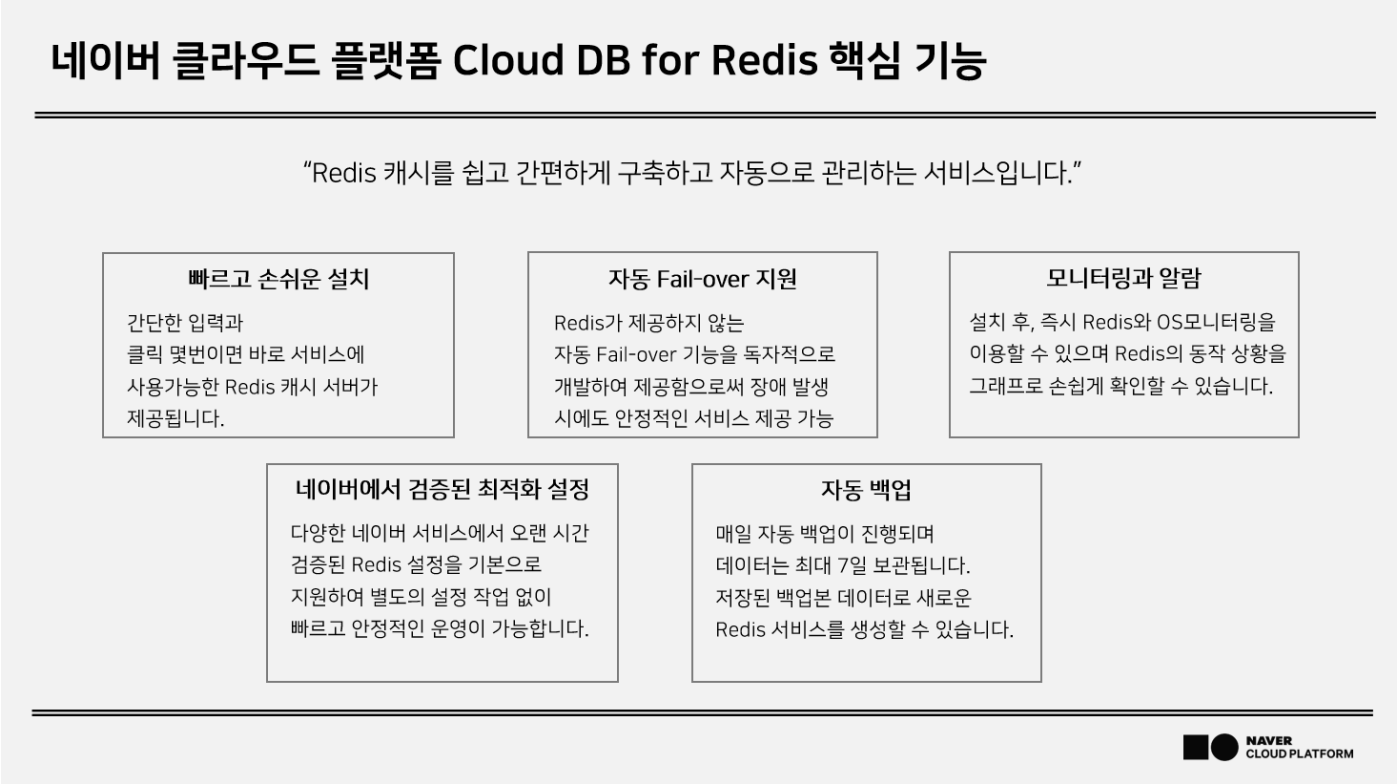
이벤트 명	performance counter 명	설명
CPU used	% Processor Time	CPU 사용량 (%)
CPU Privilege	% Privilege Time	커널 CPU 사용량 (%)
CPU Queue	Processor Queue Length	CPU 대기하는 스레드 수
Context Switches	Context Switches/sec	프로세서가 한 스레드에서 다른 스레드로 전환된 횟수
disk read latency	Avg. Disk Sec/Read	디스크 읽기 평균 소요시간
disk write latency	Avg. Disk Sec/Write	디스크 쓰기 평균 소요시간
disk queue length	disk Queue Length	디스크를 기다리는 스레드 수
disk read mbyte	Disk read Mbyte/sec	디스크 초당 읽기 양 (MB)
disk write mbyte	Disk write Mbyte/sec	디스크 초당 쓰기 양 (MB)
memory free megabyte	FREE MegaByte	사용하지 않는 여유 메모리 용량 (MB)
network in	Byte Received/sec	네트워크로 전송한 바이트 수 (byte)
network out	Byte Send/sec	네트워크로 전송받은 바이트 수 (byte)
network packet	Packets/sec	네트워크로 초당 보낸 패킷 수 (byte)
DB lazy write	Lazy writes/sec	버퍼 관리자의 지연 기록기가 기록한 버퍼 수
Free Pages	Free Pages	사용 가능한 페이지 수
Free Memory	Free Memory	사용 가능한 메모리 양 (KB)
Page Life Expectancy	Page Life Expectancy	DB 데이타 페이지가 참조 없이 버퍼 풀에 남아 있는 시간 (sec)
memorygrantpending	Memory Grants Pending	작업 공간 메모리 부여를 대기 중인 총 프로세스 수
query per second	Batch Requests/sec	초당 처리되는 쿼리 수
DB buffer lookup	Page lookups/sec	버퍼 풀에서 페이지를 찾기 위한 초당 요청 수
DB buffer reads	Page reads/sec	실행한 물리적 데이터베이스 페이지 초당 읽기 수
DB buffer writes	Page writes/sec	실행한 물리적 데이터베이스 페이지 초당 쓰기 수
latch wait	Total Latch Wait Time	마지막 1 초 동안의 래치 요청에 대한 총 래치 대기 시간 (ms)
lock wait	Lock Wait Time	마지막 1 초 동안의 잠금에 대한 총 대기 시간 (ms)

compile	SQL Compilations/sec	초당 컴파일 수
re-compile	SQL Re-Compilations/sec	초당 리컴파일 수
connections	User Connections	현재 연결된 커넥션 수
failover (master server down)		Principal 서버 장애로 Mirror 서버로 절체
recreation (slave server down)		Mirror 서버 장애로 Mirror 서버를 다시 생성
restart with failover		Principal 서버 재시작으로 Mirror 서버로 절체
restart without failover		Mirror 서버 재시작

CDB for MS-SQL Operation 4. 쿼리 분석

- 쿼리 수행 횟수 대비 CPU 소모량과 메모리 읽기 수는 상관관계 및 분포를 버블 차트로 표현
- X축은 해당 쿼리의 일별 수행 횟수 합계
- Y축은 해당 쿼리의 일별 CPU 소모량의 합계
- 버블의 크기로 해당 쿼리의 메모리 읽기 수 확인
- 버블을 클릭하면 어떤 쿼리인지 하단에 확인 가능

NAVER CLOUD PLATFORM



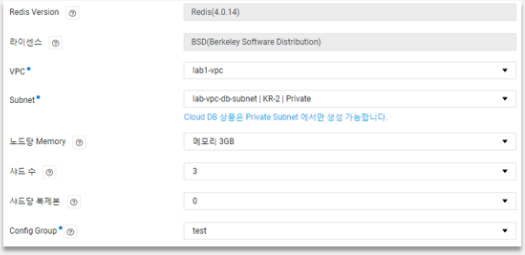
Cloud DB for Redis 핵심 기능

지금까지 Cloud DB for MSSQL과 MYSQL을 살펴보았습니다. 그 다음 소개드릴 Cloud DB는 Cloud DB for Redis입니다. 다른 Cloud DB 서비스와 마찬가지로 Cloud DB for Redis 서비스도 빠르고 손쉬운 설치 및 자동 Fail-over 기능을 제공합니다. 또한 그동안 네이버 서비스를 제공하며 검증된 설정을 기본으로 제공하여 빠르고 안정적인 운영이 가능하다는 특징을 가지고 있습니다. 현재 Cloud DB for Redis는 최대 7일 동안 데이터 백업 파일을 보관하고 있으며 매일 자동 백업 기능을 지원하고 있습니다.

VPC 환경에서는 Redis Cluster 지원을 통해 대용량 데이터도 인메모리 캐시에 저장할 수 있으며 Replica를 통한 읽기 분산이 가능합니다.

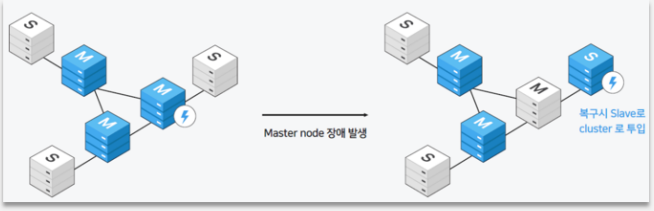
Cloud DB for Redis

- VPC 내 Private Subnet에만 생성 가능
- Simple 형태 혹은 Cluster 형태로 생성 가능
- Config Group 으로 여러 노드에 동일한 설정 적용 가능
- CPU 4core 고정, Memory 스펙만 변경 가능



- Redis Simple
  - Standby Master 노드를 통한 고가용성 지원 (*선택사항)

- Redis Cluster
  - Shard를 통해 데이터 분산 저장 (Auto-Sharding)
  - Shard는 최소 3개부터 최대 10개까지 구성 가능
  - Slave 노드(Shard의 Replica)를 통한 고가용성 지원
  - Config Group 으로 여러 노드에 동일한 설정 적용 가능



NAVER CLOUD PLATFORM

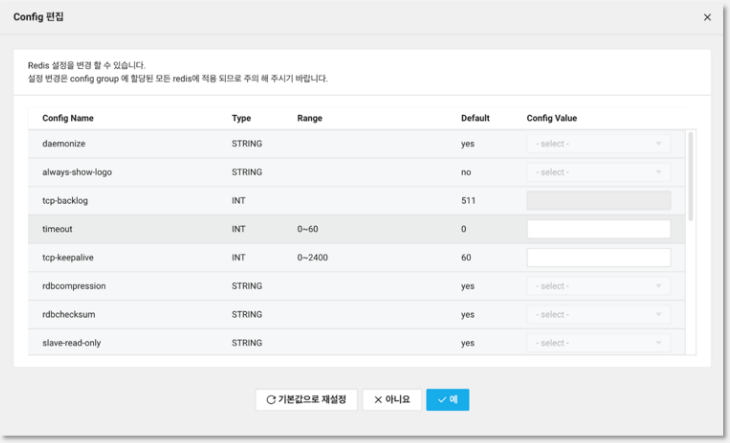
Redis 서버는 4Core 에 최적화 되어있어, 메모리 스펙만 변경 가능합니다

변경 가능한 메모리 스펙은 아래와 같습니다.

- Memory 1.5 GB
- Memory 3 GB
- Memory 6.4 GB
- Memory 12.8 GB
- Memory 25.6 GB

Cloud DB for Redis Operation 1. Config 관리

- Cloud DB for Redis에서 지원하는 Redis와 관련된 설정들을 변경할 수 있습니다.



설정 가능한 변수 목록
daemonize
always-show-logo
tcp-backlog
timeout
tcp-keepalive
rdbcompression
rdbchecksum
slave-read-only
maxclients
maxmemory-policy
cluster-require-full-coverage
slowlog-log-slower-than
slowlog-max-len
hash-max-ziplist-entries
hash-max-ziplist-value
list-compress-depth
set-max-intset-entries
zset-max-ziplist-entries
zset-max-ziplist-value

NAVER CLOUD PLATFORM

Cloud DB for Redis Operation 2. Monitoring 설정

- Redis서버에 대한 Redis Dashboard와 OS Dashboard를 제공합니다.
- 최근 4주 이내의 모니터링 지표를 확인할 수 있습니다.
- Redis Dashboard

그래프명	단위	설명
Memory Fragmentation Ratio	ratio(%)	운영체제에서 사용된 메모리와 Redis가 할당한 메모리의 비율
Instantaneous OPS Per Sec	avg activity / min	Redis Server에서 처리한 총 명령 횟수
Evicted keys	avg activity / min	maxmemory-policy에 의해 발생한 evicted key 수
Redis Used Memory	kb / min	사용하고 있는 메모리의 양
Keyspace Hits	avg activity / min	지정한 보고 간격 동안 성공한 키 조회 수
Key Space Misses	avg activity / min	지정한 보고 간격 동안 실패한 키 조회 수
Expired Keys	avg activity / min	expire 된 key

- OS Dashboard

그래프명	단위	설명
CPU Usage	used(%)	CPU 사용량
Swap	kb/min	Swap 메모리 발생량
Network	kb/min	NIC의 초당 in/outbound byte
Load Average		Load Average 상태값

NAVER CLOUD PLATFORM

Cloud DB for Redis Operation 3. Back-up 설정

- 백업 파일은 별도의 데이터 스토리지에 저장
- 원하는 시간에 백업이 진행되도록 설정이 가능하며,자동으로 선택할 경우 임의의 시간에 백업 진행
- 백업 파일은 백업 완료 시점의 데이터를 보관하므로, 복구 데이터베이스는 백업 완료 시점 기준의 데이터로 복구됩니다.

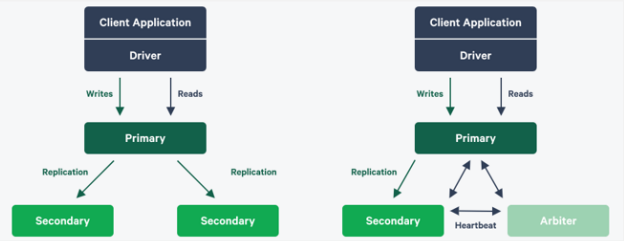
NAVER CLOUD PLATFORM

Cloud DB for Redis 백업 주기/기간

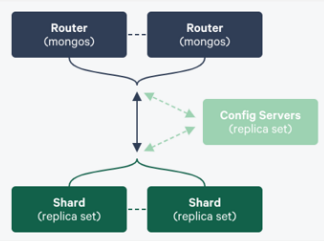
백업은 매일 1번씩 진행되며, 최대 7일까지 보관 가능합니다.

Cloud DB for MongoDB

- NoSQL의 대표적인 MongoDB를 쉽고 간편하게 사용할 수 있는 완전관리형 서비스
  - MongoDB 데이터베이스를 Sharding 과 Replica Set 방식으로 선택하여 손쉽게 구축하고 운영할 수 있는 상품
  - Community, Enterprise Edition 제공
  - 2TB 자동 디스크 확장 (기본 50GB 부터 시작, 10GB 단위로 확장)
  - 자동 Fail-Over 기능을 통한 고가용성 제공
  - 매일 자동으로 DB 백업이 진행되며 데이터는 최대 30일까지 보관
  - 로그 수집, 모니터링 및 이벤트 발생 시 알람 발송 기능 제공
  - Standalone, ReplicaSet 형태 혹은 Sharded Cluster 형태로 생성 가능



[ReplicaSet 구성]



[Sharded Cluster (Sharding) 구성]

NAVER CLOUD PLATFORM

Cloud DB for MongoDB

- Replica Set 구성
  - Mongod 프로세스가 올라간 노드의 집합으로, 실제 배포되는 MongoDB의 가장 기본적인 구성
  - Primary / Secondary / Arbiter 노드로 구성
  - Replica Set 생성 시에는 P-S-S 혹은 P-S-A 구조로 구성이 가능하며
  - 전체 구성 노드의 대수는 최소 3대 ~ 7개까지 생성이 가능
  - Arbiter 노드 생성은 선택 사항으로, 만들지 않거나 1대만 구성 가능

- Replica Set 동작 방식
  - 모든 Write 작업은 Primary노드 oplog에 기록되며
  - Secondary 노드는 Primary노드의 oplog를 복제하여, 해당 기록을 바탕으로 자신의 데이터셋에 반영
  - Primary 노드에 장애가 발생 시, Secondary 노드 중 1대가 자동으로 Primary로 승격
  - Arbiter 노드는 데이터셋을 저장하지 않으며, 장애 시 Primary 선출에만 참여

NAVER CLOUD PLATFORM

Cloud DB for MongoDB

- Sharded Cluster 구성
  - ReplicaSet, Mongos, Config 서버들의 집합
  - 데이터셋을 대용량으로 저장해야 하거나, 처리량이 많을 시 분산 저장할 수 있어 용이한 구성
  - Mongos 서버 수는 최소 2대 ~ 최대 5대 생성 가능
  - Config 서버 수는 3대로 고정

- Sharded Cluster 동작 방식
  - Mongos는 클라이언트와 Sharded Cluster 사이의 유일한 인터페이스
  - 클라이언트가 Mongos로 쿼리 요청을 전달하면
  - Mongos는 자신이 갖고있는 캐시데이터를 활용, 어떤 데이터가 어느 샤드(ReplicSet)에 있는지 추적
  - 해당 쿼리를 처리해야하는 shard 리스트를 뽑고 요청을 해당 shard로 전달 및 클라이언트에게 결과 반환
  - 이 때 전체 클러스터에 대한 메타데이터는 Config Server에 저장되어 있으며,
  - Mongos는 캐시데이터를 Config Server 로부터 가져옴

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 Cloud DB for PostgreSQL 핵심 기능

Cloud DB

"데이터베이스를 직접 구성했을 때의 번거로움을 덜어줄 수 있는
자동화된 기능을 제공하며, 콘솔상에서 쉽게 생성이 가능합니다."

사용자 환경에 맞는 구성

최대 32 vCPU,
256GB 메모리까지 지원하며
6TB (6000GB)까지 DISK 확장이
가능합니다.

편리한 구성과 사용

클릭 몇 번으로 구성이 완료되며
네이버 서비스에서 검증된
파라메터 셋을 제공하여
안정된 운영이 가능합니다.

자동화된 DB 백업

매일 자동 DB백업이 진행되며
데이터는 최대 30일 보관됩니다.
보관 기간 내의 특정 시점으로의
복원을 지원 합니다.

자동 Fail-over 지원

자동 Failover 를 지원하여
어플리케이션 변경 없이
DB고가용성을 지원합니다.

모니터링과 알람

설치 후 즉시 DB 모니터링을
이용할 수 있으며,
사용자의 메일, SMS 등으로
빠르게 장애를 보고합니다.

읽기 부하분산 가능

최대 5대까지 Read Replica DB
확장이 가능하며, Load Balancer
상품을 이용하여 데이터베이스 읽기
부하 분산이 가능합니다.

NAVER CLOUD PLATFORM

Cloud DB for PostgreSQL

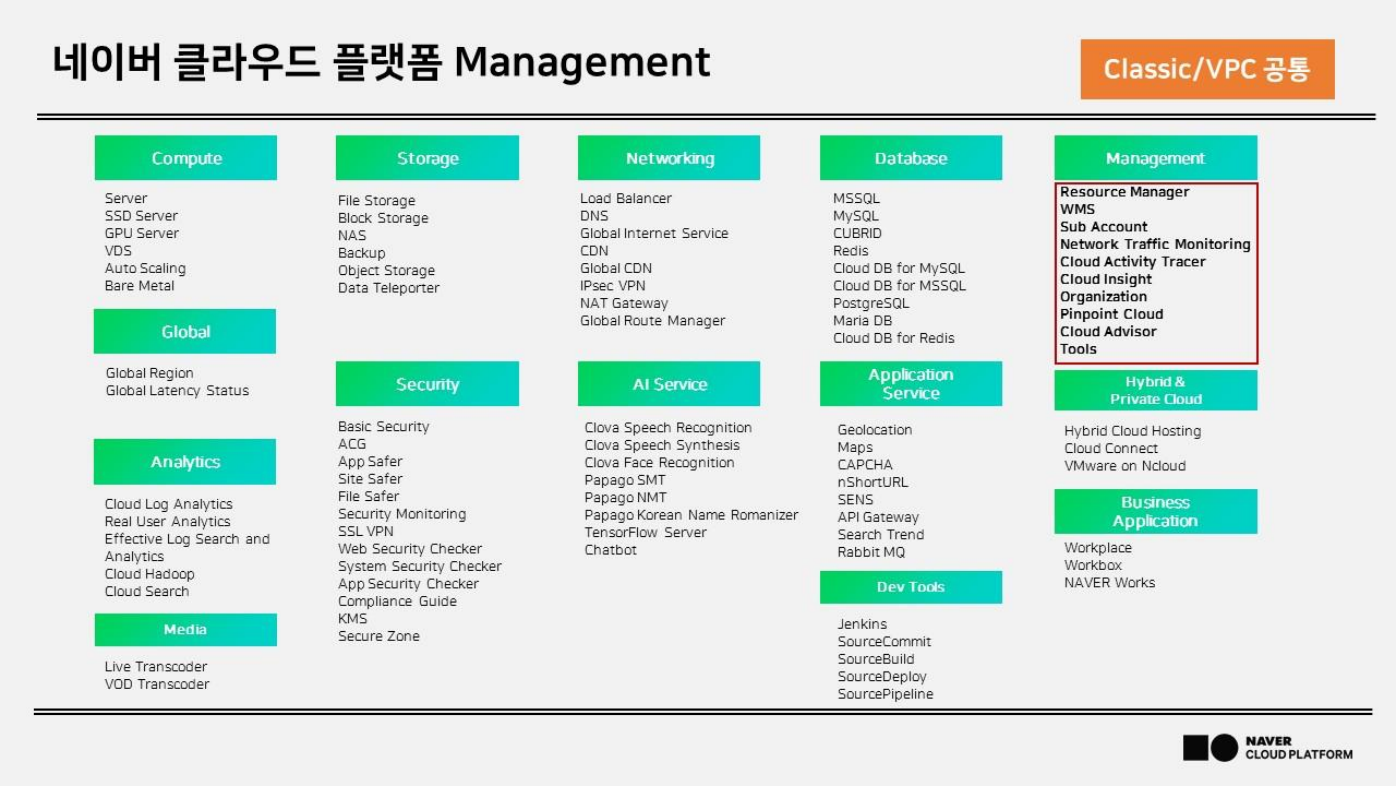
- 기능과 성능면에서 강점을 보이는 RDBMS PostgreSQL 을 완전관리형으로 제공하는 서비스
  - 관계형 DBMS의 기본적인 기능인 트랜잭션과 ACID(Atomicity, Consistency, Isolation, Durability)를 지원
  - 멀티존(Multi-Zone) 기능이 제공되어, Primary 와 Secondary를 분산 생성 및 운영이 가능
  - 기본 10GB 스토리지 제공, 10GB 단위로 6000GB 까지 자동 증가
  - 최대 5대까지 Read Replica 제공 (Load balancer 를 이용한 부하 분산)
  - 데이터베이스의 에러 로그와 슬로우쿼리 로그 등을 웹 콘솔을 통해 확인 가능

[자동 Fail-over 구성]

NAVER CLOUD PLATFORM

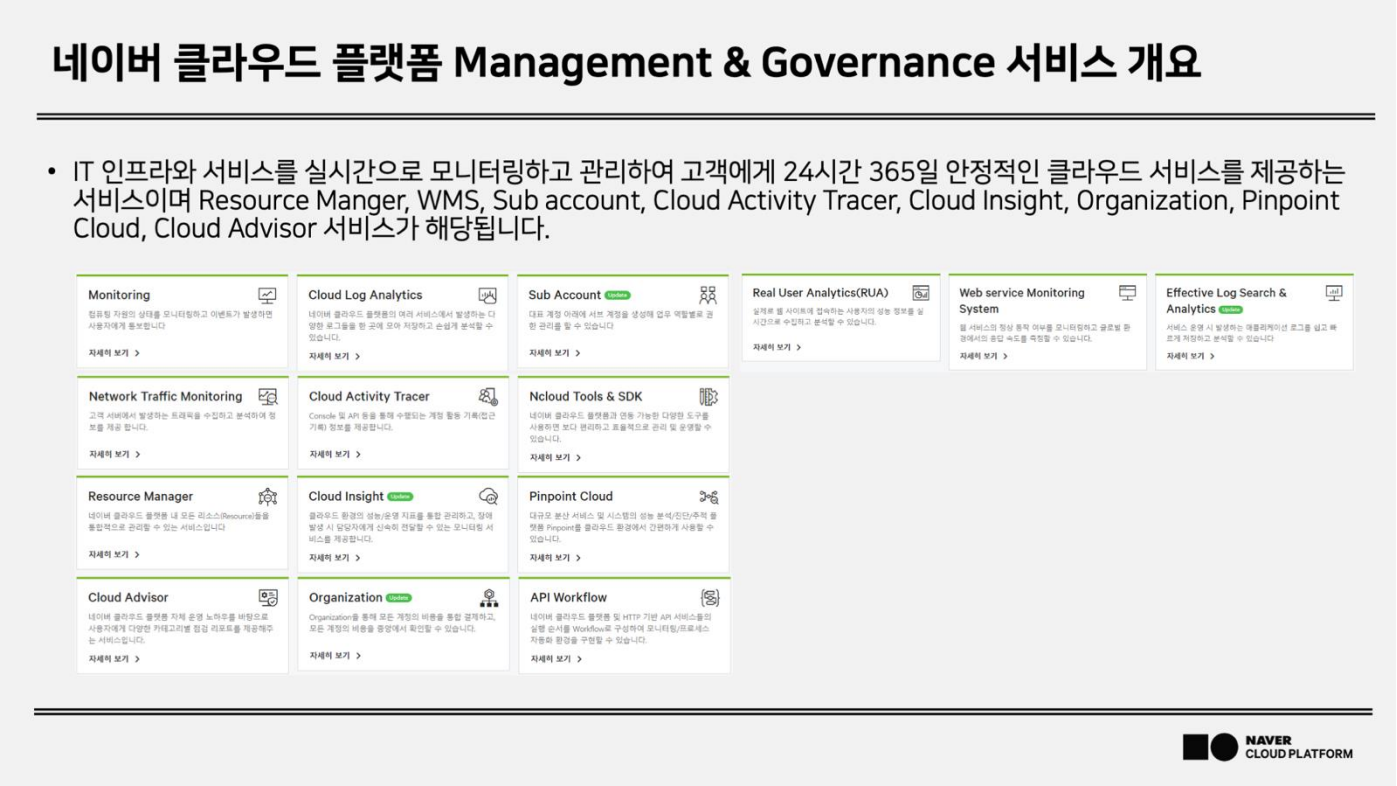
Chapter 2. 네이버클라우드플랫폼 Management

203 과정의 두번째 챕터는 네이버클라우드플랫폼의 Management 상품군에 대해서 살펴봅니다.



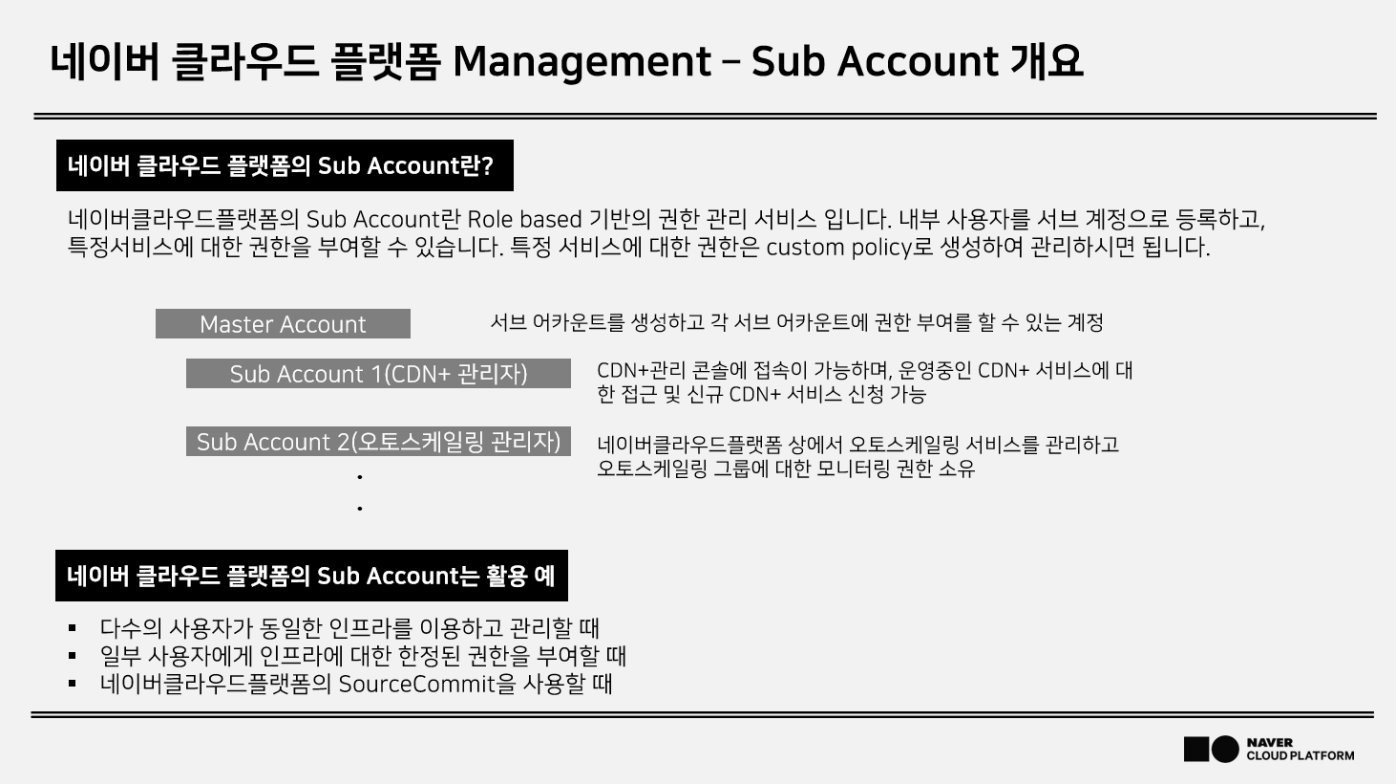
네이버클라우드플랫폼의 Management

네이버클라우드플랫폼의 Management 상품군에는 Monitoring, Sub account, WMS, Network Traffic Monitoring, Cloud Activity Tracer, Tools, Resource Manager, Cloud Insight 서비스가 제공됩니다.



네이버클라우드플랫폼 Management 서비스 개요

네이버클라우드플랫폼의 Management 상품은 네이버클라우드플랫폼에서 사용하고 계시는 인프라에 대한 실시간 모니터링 및 안정적인 서비스 클라우드 운영이 가능하도록 지원하는 서비스들이 모여 있습니다.



네이버클라우드플랫폼 Management – Sub Account 개요

네이버클라우드플랫폼에서는 내부 사용자들을 서브계정으로 등록하고 특정 서비스에 대한 권한을 부여할 수 있습니다. 서브 계정에 대한 권한 부여는 Role based로 진행하며 이미 정해져 있는 Pre-defined된 Role에 따른 권한 외에도 사용자들이 원하는 Custom policy를 등록하여 사용할 수 있습니다. (네이버클라우드플랫폼에서는 지속적으로 Sub Account에서 사용할 수 있는 Role을 추가하고 있습니다.)

네이버클라우드플랫폼 Sub Account는 다음과 같이 사용되어 인프라를 안전하게 운영하실 수 있도록 지원합니다.

1) 다수의 사용자가 동일한 인프라를 이용하고 관리할 시

2) 일부 사용자에게 인프라에 대한 한정된 권한을 부여하고 싶을 때

3) 네이버클라우드플랫폼의 Source Commit을 사용할 때

네이버 클라우드 플랫폼 Sub Account 세부 기능

네이버클라우드플랫폼에서 제공하는 Sub Account는 다음과 같은 세부 기능들로 구성되어 있습니다.

- **Dashboard**

서브 계정이 접속할 수 있는 페이지 설정 및 서브 계정 수 / 그룹 수 / 정책 수 / 접속 페이지 설정 /
최근 이벤트 로그(서브 계정이 작업한 로그)를 확인할 수 있습니다.

NAVER CLOUD PLATFORM

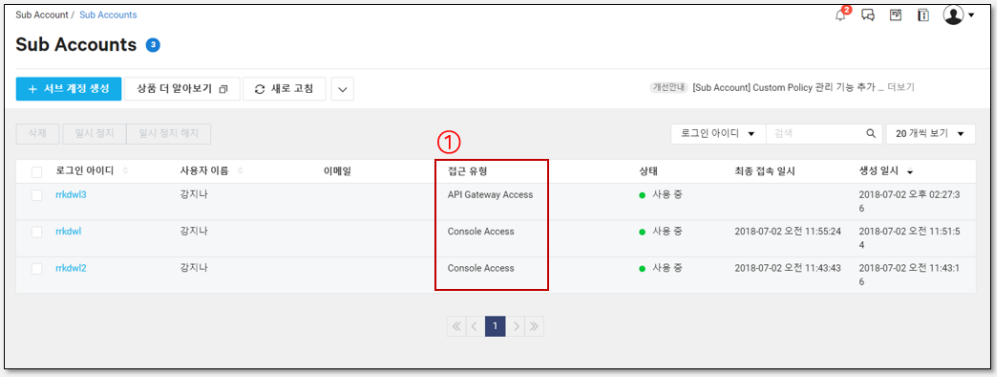
Dashboard

지금부터는 네이버클라우드플랫폼에서는 제공하는 Sub Account가 제공하는 세부 기능들에 대해서 살펴보도록 하겠습니다. 먼저 Sub Account 에서는 Dashboard 메뉴를 통해 서브 계정이 접속할 수 있는 별도의 URL을 만들 수 있을 뿐만 아니라 서브 계정 수, 그룹 수, 정책 수 등을 통합적으로 살펴볼 수 있도록 제공합니다. 특히 이벤트 로그 메뉴를 통해서 각 서브계정이 한 액션들에 대한 로그를 확인할 수 있습니다. (어떤 액션들이 기록되는 지, 그 로그는 언제를 기준으로 하는지)

네이버 클라우드 플랫폼 Sub Account 세부 기능

Sub Accounts

- 새로운 서브 계정을 생성하거나 기존에 있는 서브 계정의 정보를 수정/삭제, 일시정지/해지 가능
- 각 서브 계정 상세 페이지에는 그룹, 정책을 추가/삭제하거나 API Gateway사용에 필요한 API Key를 관리할 수 있습니다.



NAVER CLOUD PLATFORM

Sub Accounts

새로운 서브 계정을 생성하거나 기존에 있는 서브 계정의 정보를 수정/삭제, 일시 정지/해지할 수 있습니다. 각 서브 계정 상세 페이지에서는 그룹, 정책을 추가/삭제하거나 API Gateway 사용에 필요한 API Key를 관리하고 이벤트 로그를 확인할 수 있습니다.

네이버 클라우드 플랫폼 Sub Account 세부 기능

- **접근 유형**
  - Console Access: 서브 계정의 콘솔 접근을 허용하며,서브 계정의 관리 콘솔 접근 IP를 대역으로써 제한할 수 있습니다.
  - API Gateway Access: API Gateway 접근을 허용하며, 해당 항목을 선택하면 서브 계정 생성 후 상세 페이지에서 Access Key를 관리하고 해당 키를 이용하여 API Gateway를 사용할 수 있습니다. 또한 서브계정은 로그인 후 **포털 > 마이페이지 > 인증키 관리** 메뉴를 통해 본인의 Access Key를 관리할 수 있습니다.
- **2차인증설정**
  - 서브계정이 2차인증을 필수로 설정하여 사용하도록 할 수 있습니다.
  - 2차인증을 위한 정보는 서브계정이 최초 로그인할 때 처음 설정하게되며 포털의 **마이페이지 > 계정 관리 > 2차인증 관리**에서 수정할 수 있습니다.
- **비밀번호 재설정 필요**
  - 비밀번호 재설정 필요 항목에 체크한 경우 서브계정이 로그인 시 비밀번호 설정 페이지로 이동하여 비밀번호를 변경할 수 있도록 합니다.
  - 비밀번호 설정 페이지에서 비밀번호를 변경하지 않으면 이후 로그인 시마다 비밀번호 설정 페이지로 이동합니다.
  - 비밀번호 만료일을 설정하여 관리할 수 있습니다.

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 Sub Account 세부 기능

Groups

- 서브 계정 그룹을 생성/삭제하거나 이름을 변경할 수 있습니다.
- 그룹에 서브 계정이나 정책을 추가/삭제하여 다수의 서브 계정들에 동일한 정책이 반영되도록 할 수 있습니다.

* 기존 Sub Account의 권한과 Groups가 가지고 있는 권한은 'AND' 조건으로 제공됩니다.

NAVER CLOUD PLATFORM

Groups

Sub Accounts의 Groups메뉴에서 서브계정그룹을 생성하거나 삭제할 수 있습니다. 서브 계정의 그룹이 가질 수 있는 정책을 설정하고 해당 그룹에 속할 서브 계정을 지정하면 동일한 정책을 가지는 복수의 서브계정들을 손쉽게 관리할 수 있습니다.

NAVER CLOUD Platform

System Managed 정책 별 설명

https://docs.ncloud.com/ko/management/management-4-2.html

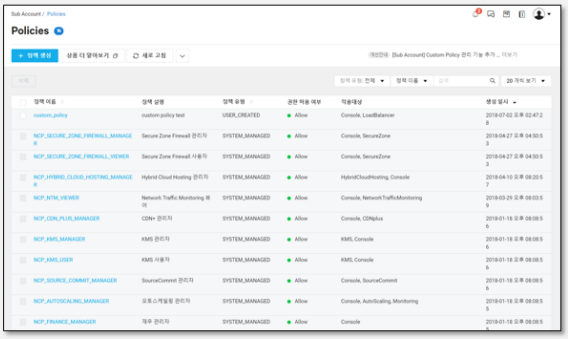
정책명	설명
NCP_FINANCE_MANAGER	포털 마이페이지의 이용 관리 메뉴, 결제수단 관리 메뉴를 확인할 수 있는 권한
NCP_INFRA_MANAGER	네이버 클라우드 플랫폼 내 모든 상품을 이용 가능하며, 포털 마이페이지 내 알림 관리를 접근할 수 있는 권한
NCP_SERVER_MANAGER	Server, Auto Scaling, Load Balancer 상품 내 모든 기능을 이용할 수 있는 권한
NCP_SERVER_OBSERVER	Server 상품 내 목록 보기, 조회 기능만 이용할 수 있는 권한
NCP_MONITORING_MANAGER	Monitoring 서비스 전체 이용 권한
NCP_MONITORING_VIEWER	Monitoring 서비스 내 목록 보기, 조회 기능만 이용할 수 있는 권한
NCP_AUTOSCALING_MANAGER	Auto Scaling, Monitoring 상품 내 모든 기능을 이용할 수 있는 권한 * 서버 조회 권한이 필요하면 NCP_SERVER_MANAGER 또는 NCP_SERVER_OBSERVER 권한 필요
NCP_SOURCE_COMMIT_MANAGER	SourceCommit 서비스에서 리파지토리를 생성할 수 있는 권한 * 생성한 리파지토리에 대하여 Admin 권한이 자동으로 부여되며 다른 서브 계정과 리파지토리를 공유할 수 있고 공유한 서브 계정에게 리파지토리 접근 권한을 부여할 수 있음
NCP_SOURCE_BUILD_MANAGER	SourceBuild 서비스에서 빌드 프로젝트를 생성할 수 있는 권한
NCP_SOURCE_DEPLOY_MANAGER	SourceDeploy 상품에서 배포 프로젝트를 생성할 수 있는 권한
NCP_SOURCE_PIPELINE_MANAGER	SourcePipeline 상품에서 파이프라인을 생성할 수 있는 권한
NCP_KMS_MANAGER	Key Management Service 내 모든 기능을 이용할 수 있는 권한 * 콘솔을 이용하여 모든 키에 대한 관리 기능을 수행할 수 있음
NCP_KMS_USER	Key Management Service 콘솔 접근 가능하며, 역할이 부여된 키에 대해서 허가된 기능만 사용 가능한 권한
NCP_CDN_PLUS_MANAGER	CDN+ 상품 내 모든 기능을 이용할 수 있는 권한
NCP_NTM_MANAGER	Network Traffic Monitoring 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_NTM_VIEWER	Network Traffic Monitoring 서비스를 이용할 수 있는 권한 (상품 신청 불가)
NCP_HYBRID_CLOUD_HOSTING_MANAGER	Hybrid Cloud Hosting 상품 내 모든 기능을 이용할 수 있는 권한
NCP_SECURE_ZONE_FIREWALL_MANAGER	Secure Zone 상품 내 모든 기능을 이용할 수 있는 권한
NCP_SECURE_ZONE_FIREWALL_VIEWER	Secure Zone 상품 내 목록 보기, 조회 기능만 이용할 수 있는 권한
NCP_MAILER_MANAGER	Cloud Outbound Mailer 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_OBJECT_STORAGE_MANAGER	Object Storage 상품 내 모든 기능을 이용할 수 있는 권한
NCP_API_GATEWAY_MANAGER	API Gateway 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_API_GATEWAY_VIEWER	API Gateway 서비스 내 조회 기능만 이용할 수 있는 권한
NCP_CLOUD_ACTIVITY_TRACER_MANAGER	Cloud Activity Tracer 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_WORKPLACE_K_MANAGER	Workplace k 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_WORKPLACE_G_MANAGER	Workplace g 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_ARCHIVE_STORAGE_MANAGER	Archive Storage 상품 내 모든 기능을 이용할 수 있는 권한
NCP_CONTAINER_REGISTRY_MANAGER	Container Registry 상품 내 모든 기능을 이용할 수 있는 권한
NCP_CONTAINER_REGISTRY_VIEWER	Container Registry 상품 내 대시보드 조회 및 Docker 컨테이너 이미지

	Pull 기능만 이용할 수 있는 권한
NCP_IMAGE_OPTIMIZER_MANAGER	Image Optimizer 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_IMAGE_OPTIMIZERY_VIEWER	Image Optimizer 서비스 내 조회 기능만 이용할 수 있는 권한
NCP_SENS_MANAGER	Simple & Easy Notification Service 내 SMS 발신번호 등록 기능을 제외한 모든 기능을 이용할 수 있는 권한
NCP_WMS_MANAGER	Web service Monitoring System 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_WMS_VIEWER	Web service Monitoring System 서비스 내 등록 되어있는 URL의 목록 및 결과 조회 기능만 이용할 수 있는 권한
NCP_GAMEPOT_MANAGER	GAMEPOT 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_GAMEPOT_VIEWER	GAMEPOT 서비스 내 조회 기능만 이용할 수 있는 권한
NCP_ELSA_MANAGER	Effective Log Search & Analytics 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_WORKBOX_MANAGER	WORKBOX 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_ELASTIC_SEARCH_MANAGER	Elasticsearch Service 내 모든 기능을 이용할 수 있는 권한
NCP_CLOUD_SEARCH_MANAGER	Cloud Search 서비스 내 모든 기능을 이용할 수 있는 권한
NCP_CLOUD_SEARCH_VIEWER	Cloud Search 서비스 내 상품 조회 및 문서 검색 기능만 이용할 수 있는 권한
NCP_RESOURCE_MANAGER_MANAGER	Resource Manager 서비스 내 모든 기능을 이용할 수 있는 권한

네이버 클라우드 플랫폼 Sub Account 세부 기능

Policies

- 서브 계정이 이용할 수 있는 권한들을 묶어 정책으로 제공합니다. 정책 목록 및 정책의 유형,권한, 적용대상을 확인할 수 있습니다.
- 서브 계정의 권한은 2가지 형태로 관리가 가능합니다.
  - System managed: 사용자 편의를 위해 몇 가지 상품에 대해 Change/View 권한을 미리 정의해두고 제공하는 정책
  - User created: 계정 사용자가 임의로 생성한 정책



NAVER CLOUD PLATFORM

Policies

네이버클라우드플랫폼 Sub Account의 Policies는 각 서브 계정들에게 부여할 수 있는 정책을 의미합니다. 정책 유형은 콘솔 접근형과 API 접근형이 있으며 둘 중에 하나의 접근 유형을 선택하거나 둘 다 선택이 가능합니다. 현재 네이버클라우드플랫폼에서 제공하는 Policies는 아래와 같습니다.

네이버 클라우드 플랫폼 Management – WMS 개요

"간단히 URL 등록만으로 시작되는 웹사이트 모니터링"

- **실시간 모니터링을 통한 서비스 안정성 향상**

URL만 등록하면 웹 페이지의 응답 속도 및 정상 동작 여부를 실시간으로 확인 가능
모니터링은 분 단위로 가능하고, 오류가 발생하면 SMS와 메일로 알람 수신

- **시나리오 기반 모니터링 수행**

사용자가 웹서비스를 이용하는 행동 패턴을 고려하여 시나리오를 작성하면 WMS가 시나리오에 해당하는 기능들이 잘 동작하는 지 확인 수행

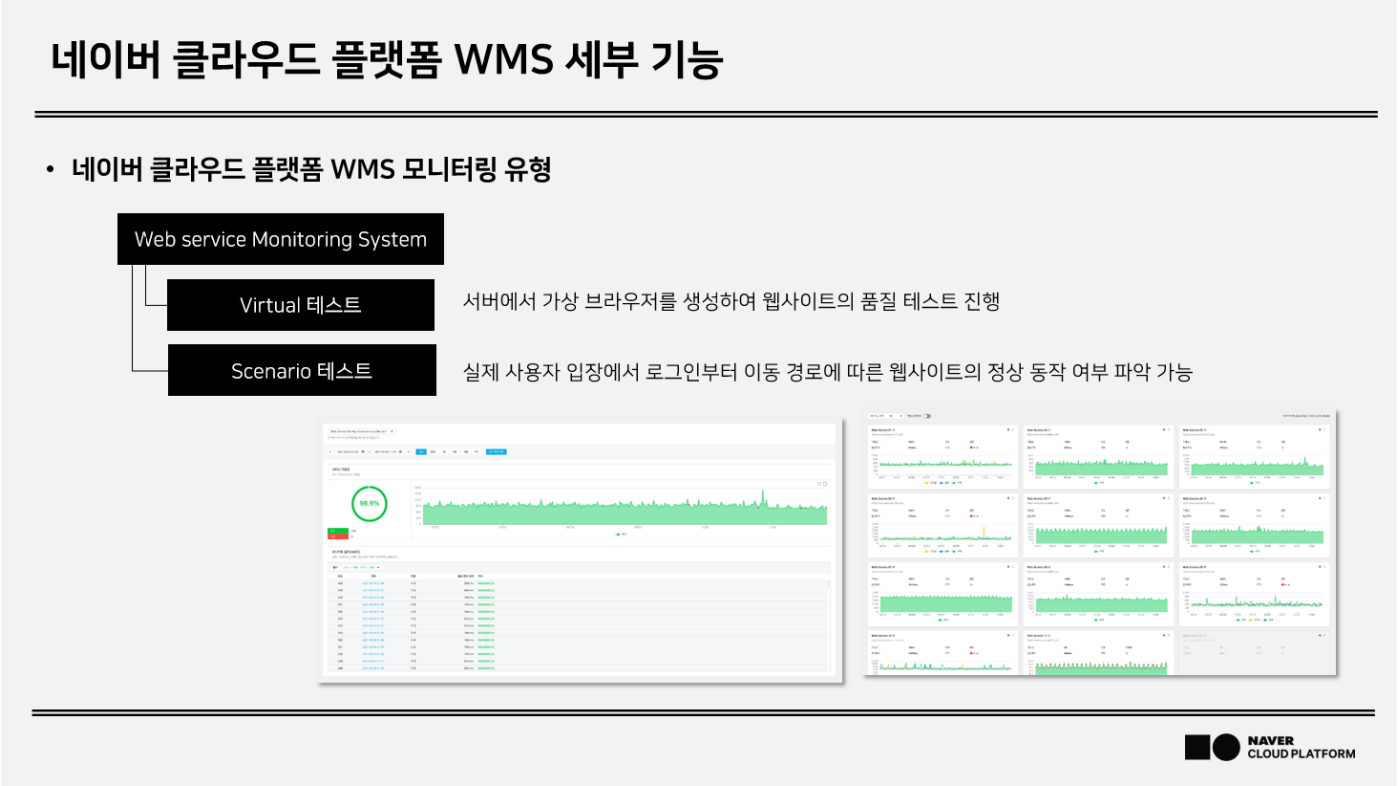
- **웹 서비스 글로벌 응답 속도 측정**

미국, 싱가폴, 일본, 홍콩,독일에서도 측정이 가능

NAVER CLOUD PLATFORM

네이버클라우드플랫폼 WMS

네이버클라우드플랫폼에서 제공하는 Management 상품군의 2번째 서비스는 WMS입니다. WMS는 간단히 URL만 등록하면 해당 웹사이트에 대한 모니터링을 진행하게 되며 웹사이트에 문제가 발생했을 시에는 SMS와 메일을 발송하여 담당자가 빠르게 문제를 파악할 수 있도록 지원합니다. 또한 실제 End-user의 사용패턴을 시나리오화 하여 웹사이트를 모니터링할 수 있는 시나리오 기반의 모니터링을 수행하실 수 있습니다. 현재 WMS 서비스는 국내뿐만 아니라 홍콩, 미국, 싱가폴, 일본,독일에서도 측정이 가능합니다.

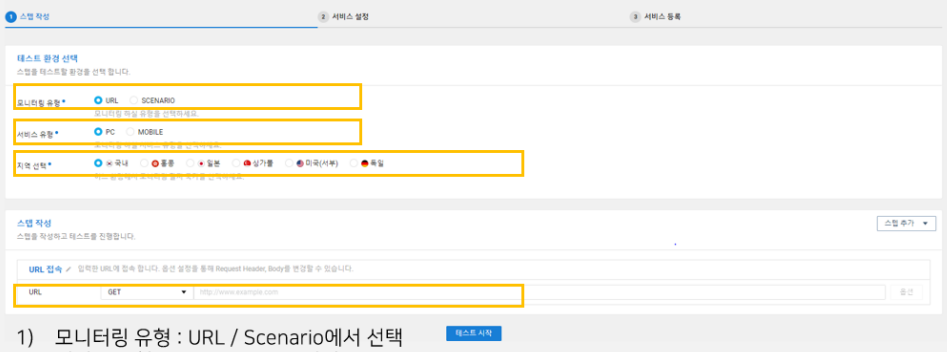


네이버클라우드플랫폼 WMS 세부기능

네이버클라우드플랫폼 WMS는 2가지 테스트 유형을 제공합니다. Virtual test는 서버에서 가상 브라우저를 생성하여 웹사이트 품질 테스트를 진행하며 Scenario 테스트는 실제 이용자 입장에서 로그인부터 이동 경로에 따른 웹사이트의 정상 동작여부를 파악합니다.

네이버 클라우드 플랫폼 WMS 세부 기능

- WMS의 모니터링 설정

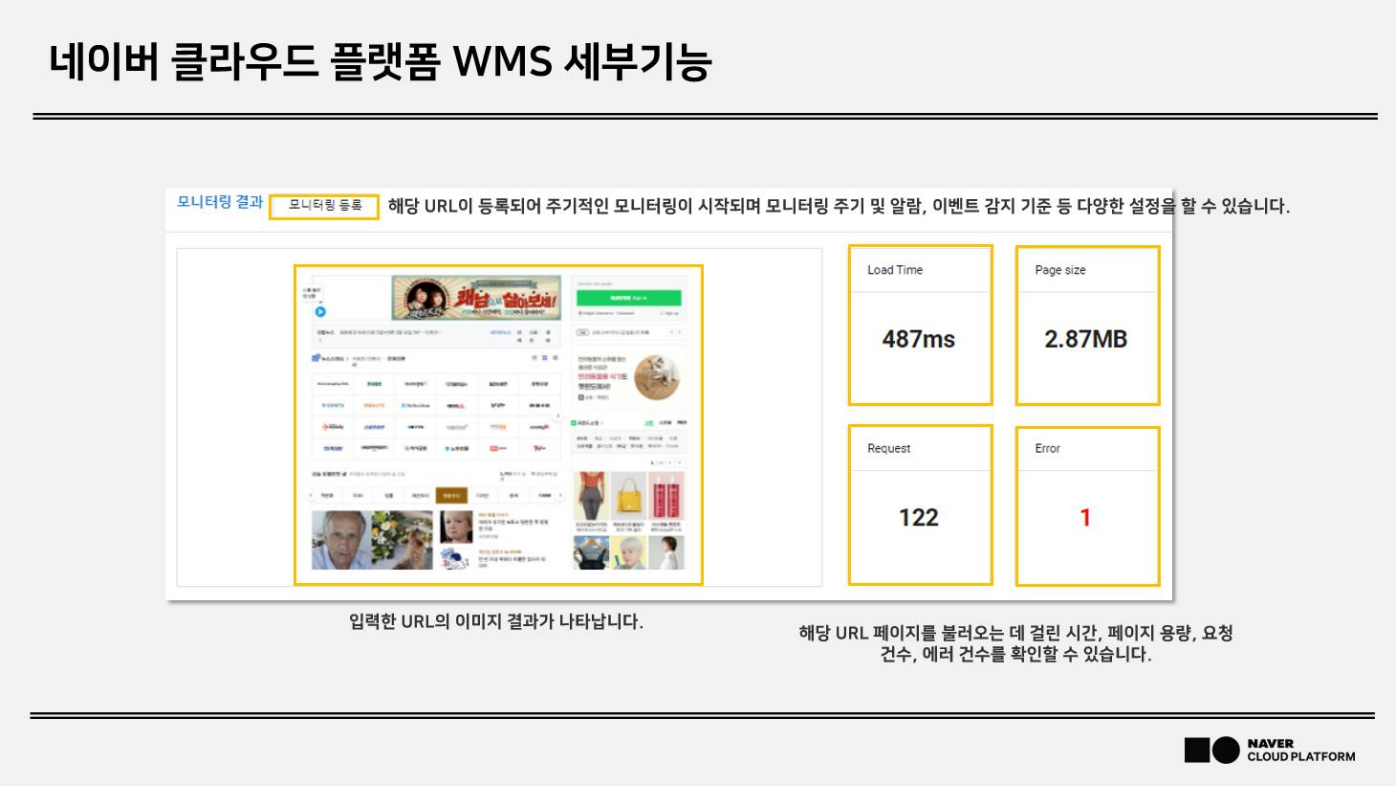


1) 모니터링 유형 : URL / Scenario에서 선택
2) 서비스 유형 : PC / Mobile 중 선택
3) 지역 선택 : 국내 /미국(서부) / 일본 / 홍콩 / 싱가폴 / 독일
4) 모니터링 URL : METHOD (GET, POST, PUT, DELETE, HEAD) 선택 및 WMS가 모니터링을 수행해야 할 URL 입력

NAVER CLOUD PLATFORM

WMS 세부기능

WMS에서 제공하는 모니터링 유형은 콘솔에서 선택할 수 있으며 URL/Scenario 중 1개를 선택하시면 됩니다. 서비스 유형은 PC와 Mobile 중 선택해 주시면 됩니다. 다음으로 선택해야 할 항목은 지역입니다. 현재 WMS에서 제공하고 있는 지역은 국내 외에도 미국/일본/홍콩/싱가폴/독일이 있습니다. 마지막으로 모니터링을 진행할 URL을 기입하면 됩니다.



WMS Monitoring 결과

다음 화면은 WMS에서 진행한 모니터링 결과 화면입니다. 각 지표에 대한 자세한 설명은 다음과 같습니다.

1) Load time

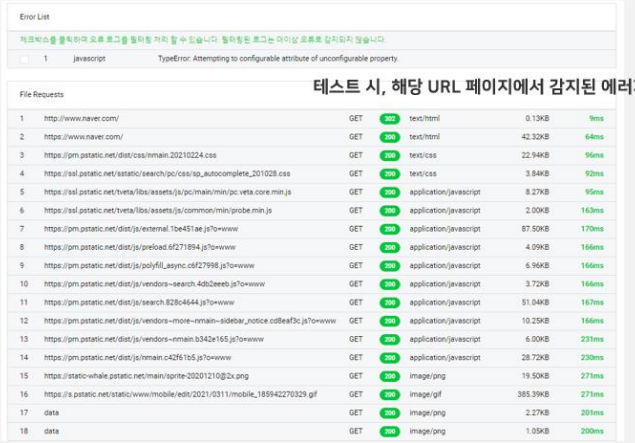
2) Service Health: 최근 측정한 데이터를 기반으로 서비스 종합 상태를 등급으로 나타냅니다.

3) Today Event: 현재 테스트 중인 URL에서 금일 발생한 이벤트 수를 보여줍니다.

4) Scenario: 테스트시나리오 내용을 보여줍니다.

5) File Requests: 다운로드 한 구성 요소들의 목록을 보여줍니다.

네이버 클라우드 플랫폼 WMS 세부 기능



Error List

체크박스를 클릭하여 오류 로그를 필터링 처리 할 수 있습니다. 필터링된 로그는 다이상 오류로 감지되지 않습니다.

1	javascript	TypeError: Attempting to configurable attribute of unconfigurable property.

File Requests

1	http://www.naver.com/	GET	302	text/html	0.13KB	9ms
2	https://www.naver.com/	GET	200	text/html	42.32KB	64ms
3	https://pm.pstatic.net/dist/css/nmain.20210224.css	GET	200	text/css	22.94KB	96ms
4	https://ssl.pstatic.net/sstatic/search/pc/css/sp_autocomplete_201028.css	GET	200	text/css	3.84KB	92ms
5	https://ssl.pstatic.net/tveta/libs/assets/js/pc/main/min/pc.veta.core.min.js	GET	200	application/javascript	8.27KB	95ms
6	https://ssl.pstatic.net/tveta/libs/assets/js/common/min/probe.min.js	GET	200	application/javascript	2.00KB	163ms
7	https://pm.pstatic.net/dist/js/external.1be451ae.js?o=www	GET	200	application/javascript	87.50KB	170ms
8	https://pm.pstatic.net/dist/js/preload.6f271894.js?o=www	GET	200	application/javascript	4.09KB	166ms
9	https://pm.pstatic.net/dist/js/polyfill_async.c6f27998.js?o=www	GET	200	application/javascript	6.96KB	166ms
10	https://pm.pstatic.net/dist/js/vendors~search.4db2eeeb.js?o=www	GET	200	application/javascript	3.72KB	166ms
11	https://pm.pstatic.net/dist/js/search.828c4644.js?o=www	GET	200	application/javascript	51.04KB	167ms
12	https://pm.pstatic.net/dist/js/vendors~more~nmain~sidebar_notice.cd8eaf3c.js?o=www	GET	200	application/javascript	10.25KB	166ms
13	https://pm.pstatic.net/dist/js/vendors~nmain.b342e165.js?o=www	GET	200	application/javascript	6.00KB	231ms
14	https://pm.pstatic.net/dist/js/nmain.c42f61b5.js?o=www	GET	200	application/javascript	28.72KB	230ms
15	https://static-whale.pstatic.net/main/sprite-20201210@2x.png	GET	200	image/png	19.50KB	271ms
16	https://s.pstatic.net/static/www/mobile/edit/2021/0311/mobile_185942270329.gif	GET	200	image/gif	385.39KB	271ms
17	data	GET	200	image/png	2.27KB	201ms
18	data	GET	200	image/png	1.05KB	200ms

테스트 시, 해당 URL 페이지에서 감지된 에러가 있을 경우 Error List에 표시됩니다.

해당 URL 페이지를 구성하는 요소들의 목록 및 상태 코드, Load Time을 확인할 수 있습니다.

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 WMS 세부 기능

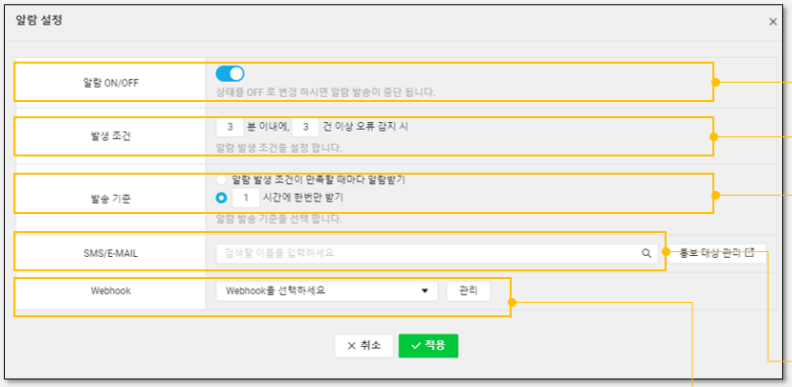
- WMS Notification 기능

모니터링 설정 및 관리

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 WMS 세부 기능

- 알람 설정



모니터링 알람은 'ON', 'OFF' 중 선택 가능

알람 발생 조건 설정

알람 발생 기준 설정
알람의 발생 빈도를 설정합니다. '1시간에 한 번만 받기'로 설정하게 되면 알람 발생 조건이 발생한 후 연속적으로 이벤트가 발생해서 계속해서 이벤트가 감지 되어도 같은 내용의 알람이 1시간 내에 1회 이상 가지 않게 됩니다.

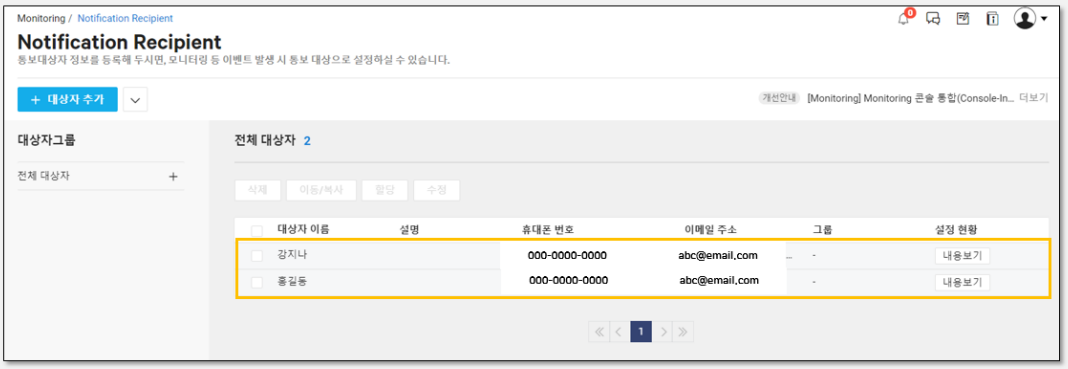
메일 수신자 설정

Webhook 수신 설정

네이버 클라우드 플랫폼 WMS 세부기능

- WMS Notification 기능

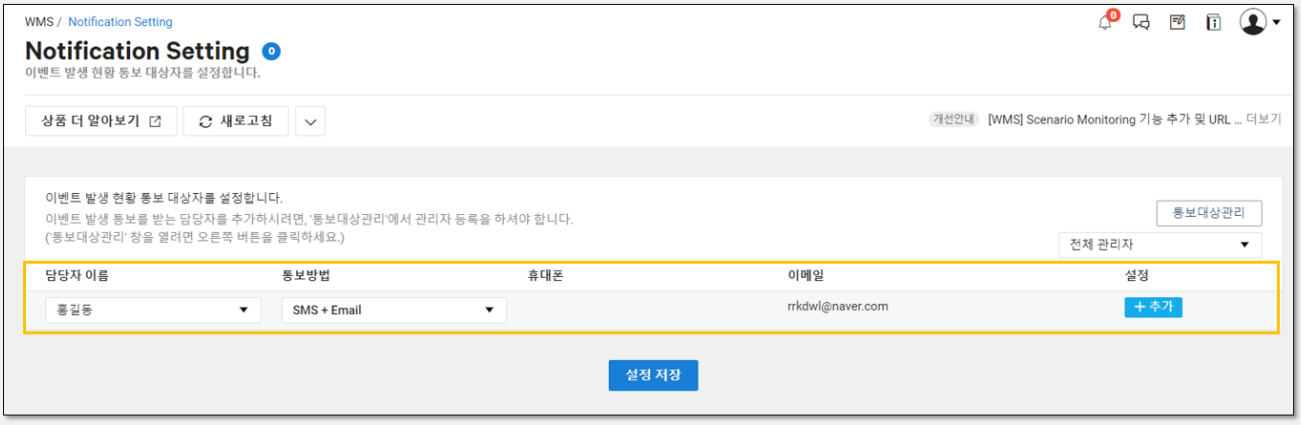
(1) 통보 대상자 관리



NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 WMS 세부기능

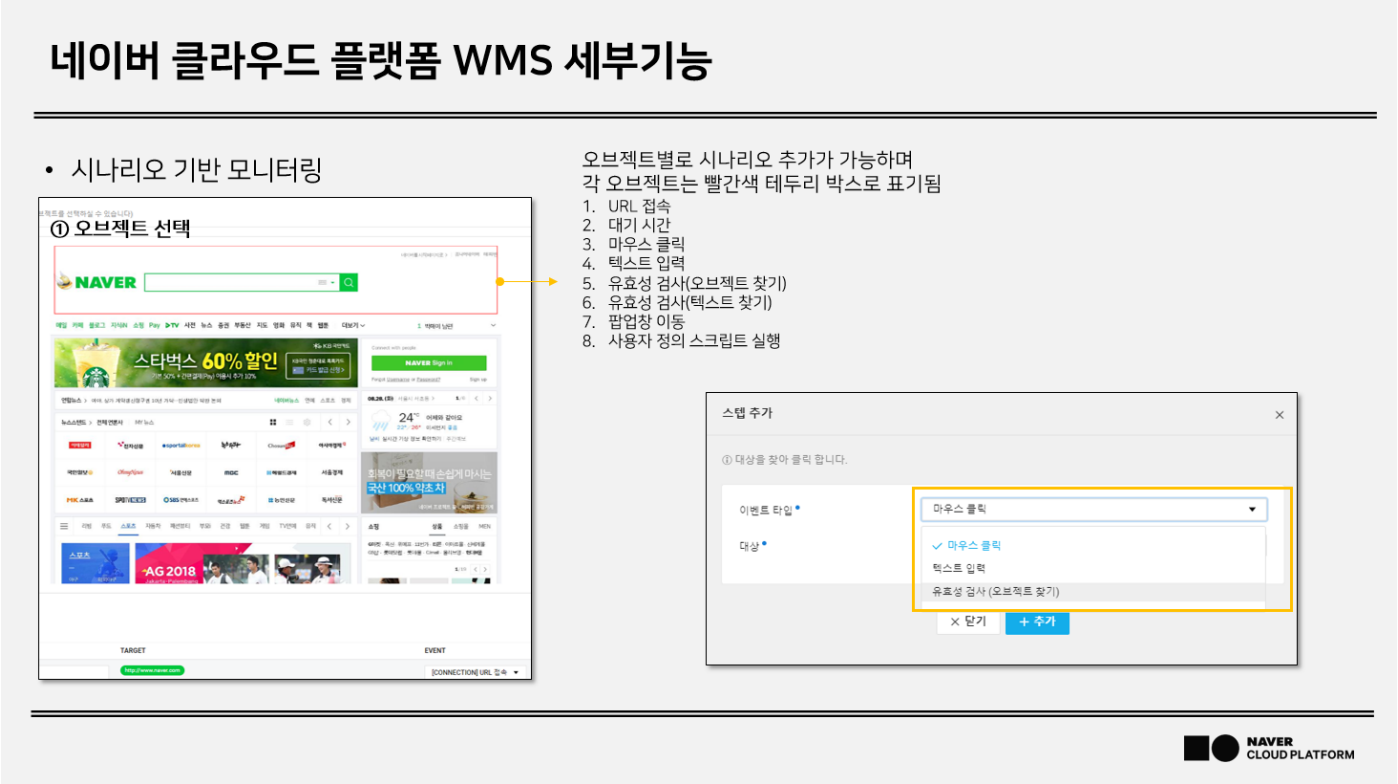
- Notification 세팅



NAVER CLOUD PLATFORM

Notification 셋팅

등록된 담당자를 선택하면 해당 담당자에 대한 통보 방법을 선택할 수 있으며 통보 설정을 하면 이벤트 발생 시 담당자에게 알람이 발송됩니다.



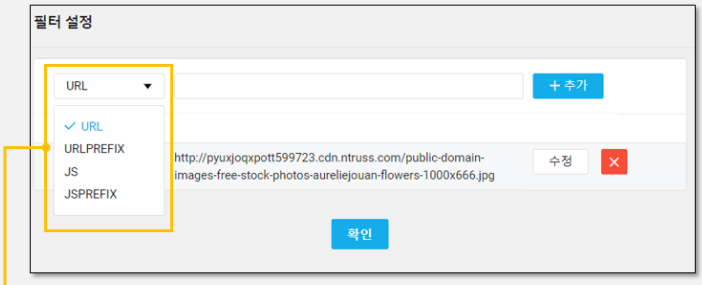
시나리오 기반 모니터링

WMS의 시나리오 기반의 모니터링은 실제 웹사이트 사용자들의 이용 패턴에 따라 해당 웹사이트가 정상적으로 동작하는 지 파악할 수 있도록 지원합니다.

- URL 접속 : 입력한 URL에 접속 합니다
- 대기 시간 : 입력한 시간 만큼 대기 합니다
- 마우스 클릭 : 대상을 찾아 클릭 합니다
- 텍스트 입력 : 대상을 찾아 텍스트를 입력 합니다
- 유효성 검사 (오브젝트 찾기) : 페이지에서 오브젝트를 찾습니다.
- 유효성 검사 (텍스트 찾기) : 페이지에서 텍스트를 찾습니다.
- 팝업 창 이동 : 팝업이 생성된 경우 해당 팝업으로 대상을 전환하여 모니터링 할 수 있습니다.
- 사용자 정의 스크립트 실행 : 사용자가 설정한 Javascript를 실행합니다.

네이버 클라우드 플랫폼 WMS 세부기능

- 필터링 기능



url	입력한 로그와 완벽히 일치하는 로그를 필터링하고 싶을 때
urlprefix	입력한 로그를 포함하고 있는 모든 로그를 필터링하고 싶을 때
js	입력한 스크립트와 완벽히 일치하는 스크립트를 필터링하고 싶을 때
Jsprefix	입력한 스크립트를 포함하고 있는 모든 스크립트를 필터링하고 싶을 때

NAVER CLOUD PLATFORM

필터링 기능

네이버 클라우드 플랫폼 WMS에서는 필터링 기능을 제공하고 있습니다. 필터링 기능을 통해 알람을 받고 싶지 않은 이벤트가 있다면 해당 이벤트 유형을 알람 대상에서 제외할 수 있습니다.

네이버 클라우드 플랫폼 Management - Network Traffic Monitoring

"패킷 정보를 분석하여 다양한 트래픽 정보 모니터링"

- **Network의 안정적인 운용**

고객의 서버에서 사용되는 네트워크 트래픽을 쉽게 확인하여 효과적인 장애 분석과 빠른 대응이 가능합니다.

- **고객 맞춤형 모니터링**

고객이 원하는 형태로 차트와 대시보드를 직접 생성하여 운영할 수 있습니다. 서버 별로 분류 할 뿐만 아니라 서버를 그룹별로 분류하여 관심 서버의 상태를 빠르게 확인하고 신속하게 대응할 수 있습니다.

- **고객 서비스의 사용자 국가 정보 분석**

사용자의 국가 정보를 기준으로 네트워크 모니터링을 할 수 있어, 고객의 서비스가 어떤 국가에서 많이 사용되는지 확인할 수 있습니다.

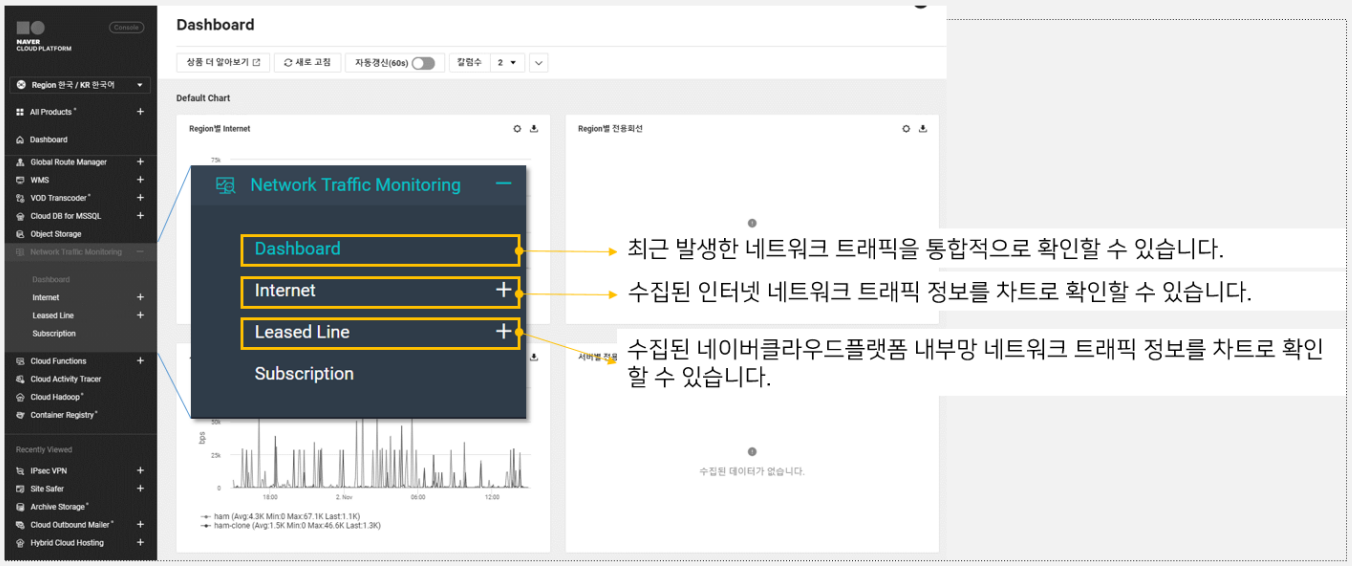
- **현재는 Outbound Traffic에 대해서만 모니터링이 가능하며 무료로 사용할 수 있습니다.**
- **2021년 9월 16일부터 Classic 환경에서는 Network Traffic Monitoring 상품을 신규로 신청하실 수 없습니다.**

NAVER CLOUD PLATFORM

Network Traffic Monitoring

네이버클라우드플랫폼 Management 상품 중 Network Traffic Monitoring에 대해 소개해 드립니다. Network Traffic Monitoring 서비스는 고객의 서버에서 사용되는 네트워크 트래픽을 쉽게 확인할 수 있는 서비스입니다. 특히 고객이 원하는 차트와 대시보드를 직접 생성하여 운영할 수 있으며 서버 별 분류 및 서버 그룹별 분류를 통해 서버 상태를 빠르게 확인하고 신속하게 대응할 수 있습니다. 네트워크 트래픽 모니터링 서비스에서는 사용자의 국가 정보를 기준으로도 네트워크 모니터링이 가능하기에 어느 국가에서 고객의 서비스가 많이 사용되는지도 유추가 가능합니다.

Network Traffic Monitoring 개요

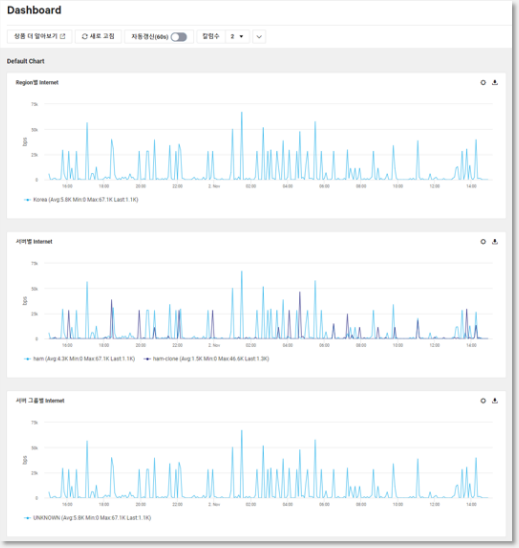


Network Traffic Monitoring 세부 기능 – Dashboard

- 기본으로 제공되는 7개 Default Chart

Default Chart
Region별 Internet Outbound
Region별 전용회선 Outbound
서버별 Internet
서버별 전용회선
서버 그룹별 Internet
서버 그룹별 전용회선
국가별 Internet

- 사용자가 원하는대로 구성할 수 있는 Custom Chart
- Export 기능 제공 : Data(Excel파일), Image 형태로 export 가능



NAVER CLOUD PLATFORM

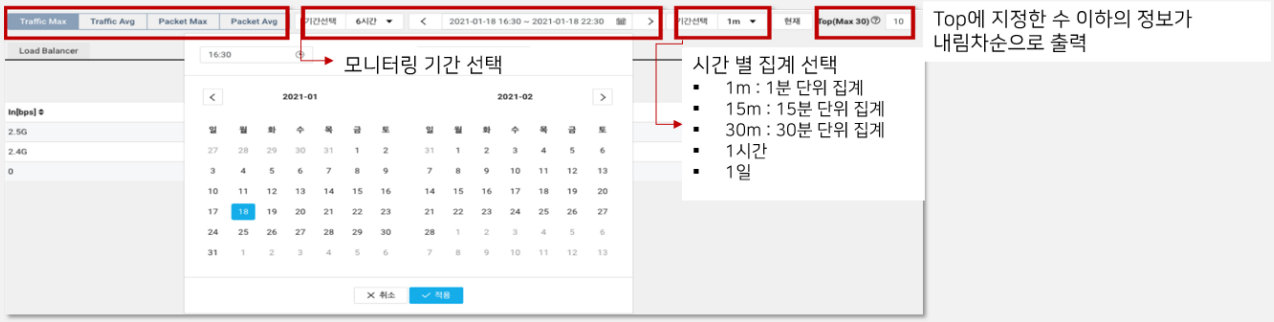
Network Monitoring Traffic Dashboard

Network Traffic Monitoring에서 기본적으로 제공되는 Default Dashboard는 7개가 있습니다. Region별 internet Outbound, Region별 전용회선 outbound, 서버별 Internet, 서버별 전용회선, 서버 그룹별 internet, 서버 그룹별 전용회선, 국가별 Internet에 대한 정보를 제공합니다.

위에 기본적으로 제공되는 대시보드 외에도 Custom chart를 구성할 수 있으며 export 기능을 통해 엑셀 파일이나 이미지 형태로 저장이 가능합니다.

Network Traffic Monitoring 세부 기능 – 차트 공통 기능

- 네이버 클라우드 플랫폼 Network Traffic Monitoring 에서 제공하는 차트 공통 기능은 다음과 같습니다.



- 다른 상품인 NAT Gateway, SSL VPN, IPsec VPN의 네트워크 트래픽은 수집되지 않습니다.
- 데이터의 최대 저장 기간은 30일입니다.
- 측정이 불가능한 네트워크 트래픽들은 __unclassified__으로 표기됩니다.

NAVER CLOUD PLATFORM

Network Traffic Monitoring Chart 공통 기능

Traffic/Flow/Packet 중 측정 단위를 선택이 가능하며 원하는 기간을 설정하여 선택된 기간 내에서의 모니터링을 필터링하여 확인할 수 있습니다. 또한 그래프의 형태를 line, area, stack 중에서 선택하여 사용하실 수 있습니다.

네이버 클라우드 플랫폼 Cloud Activity Tracer

"네이버 클라우드 플랫폼 계정 활동 로그의 자동 수집 & 간편한 View"

다양한 계정 활동 이력과 상세 정보의 자동 수집 및 기록

- Cloud Activity Tracer 서비스는 Console 및 API를 활용한 계정 활동과 Auto Scaling 등의 자동 스케줄러를 이용한 작업 활동을 포함하여 네이버 클라우드 플랫폼 계정 활동 로그를 자동으로 수집하고 기록합니다.

기록된 정보의 간편한 검색 및 필터링

- 수집된 계정 활동 이력 정보에 대한 간단한 검색 및 필터링이 필요할 경우, 네이버 클라우드 플랫폼 Console의 Cloud Activity Tracer 페이지 자체에서 제공하는 검색 및 필터링 도구를 통해 손쉽게 해결할 수 있습니다.

Cloud Log Analytics(필수 연동)가 제공하는 모든 기능 활용

- Cloud Activity Tracer가 수집하는 계정 활동 로그는 기본적으로 네이버 클라우드 플랫폼의 로그 관리/분석 시스템인 Cloud Log Analytics에 저장됩니다. 따라서 Cloud Log Analytics를 통해 계정 활동 로그 파일의 보관이 자동으로 이루어지며, Cloud Log Analytics에서 제공하는 로그 데이터 분석 대시보드 및 검색 기능들을 활용하여 로그 파일에 대한 간단한 분석도 가능합니다.

NAVER CLOUD PLATFORM

네이버클라우드플랫폼 Cloud Activity Tracer

네이버클라우드플랫폼의 Cloud Activity Tracer는 서브 활동들의 로그를 자동 수집하여 간편하게 살펴볼 수 있도록 제공합니다. 간단한 검색 및 필터링 기능을 제공하고 있습니다. 이렇게 생성된 계정 활동 로그는 CLA와 연동되어 저장됩니다(기본적으로 콘솔 및 API를 통한 계정 활동 로그가 수집되며 오토 스케일링 등 자동화된 스케줄러를 통한 작업 활동도 기록됩니다).

Cloud Activity Tracer 상세 기능

수집된 로그가 위와 같이 리스트 형태로 나타나며, 리스트에서는 해당 로그의 작업내역에 따라 [리전], [작업일시], [작업내역], [작업 상태(성공 여부)], [계정 유형], [계정명], [관련 서비스], [요청 Source] 정보를 확인할 수 있습니다.

Cloud Activity Tracer에서 수집하는 목록 : https://guide.ncloud-docs.com/docs/cat-cloudactivitytraceractivity

네이버 클라우드 플랫폼 Cloud Activity Tracer 상세 기능

Tracer를 생성하여 계정의 활동 기록을 주기적으로 Object Storage로 내보낼 수 있습니다.

- Default 타입 : Tracer 이름 및 상세 조건을 임의로 설정할 수 없는 타입으로 계정당 1개만 생성 가능하며 무료로 이용 가능합니다.
- Custom 타입 : Tracer 상세 조건을 임의로 설정할 수 있으며 계정당 여러 개의 Tracer를 생성할 수 있습니다. 단 내보내는 이벤트 데이터 건 수를 합산해 요금이 별도로 발생합니다.
- 리전, 상품, 계정 각각은 And 조건으로 필터되고, 리전, 상품, 계정 내에서의 다중 선택은 or 조건으로 필터되어 내보내기가 수행됩니다.
- JSON / CSV 두 가지 형식으로 내보내기를 수행할 수 있습니다.
  - CSV로 내보내기를 수행하는 경우, cell 표현 가능 범위(32767)가 넘는 데이터가 포함되는 경우 해당 데이터의 필드는 내보내기가 수행되지 않습니다. 이런경우 JSON으로 내보내기를 수행하세요.
- Tracer 조건에 해당하는 사용자의 활동 이력은 15일 이후 하루 단위로 Bucket으로 전송됩니다. 단, Tracer 신규 생성시에는 90일 이전 활동 이력부터 15일 전까지의 활동 이력을 Object Storage로 일괄로 내보냅니다.

NAVER CLOUD PLATFORM

Tools 개요

"네이버 클라우드 플랫폼과의 연동을 통한 편하고 효율적인 운영"

- **PC 및 모바일을 통한 편리한 관리**
  Console에 접속하여 Dashboard에서 이벤트, 리소스 Top 5, 결제정보, 상품이용내역, 공지사항 등을 확인
  Android 및 iOS 콘솔 앱을 지원, 모바일에서도 콘솔 이용 가능

- **CLI / SDK / API 를 통한 리소스 제어**
  Console 접속 없이 Windows/Linux 환경에서 CLI, SDK, API 를 통한 서비스 운영 가능

- **그 외 다양한 도구**
  Packer, Terraform 등의 오픈 소스 도구를 통한 클라우드 관리 기능 제공
  Data Migration Tool을 통해 On-Prem -> 클라우드로 DB를 이관하거나, 클라우드 상 DB를 내려받는 기능 제공
  SQL Server DBA Tool 을 통해 관리자 권한이 있는 HA 구성의 SQL 서비스 제공
  Active Directory Tool 을 통해 서버에 접속하지 않고도 HA 구성의 AD 구축이 가능

NAVER CLOUD PLATFORM

Resource Manager 개요

"네이버 클라우드 플랫폼 내 모든 리소스를 통합적으로 관리"

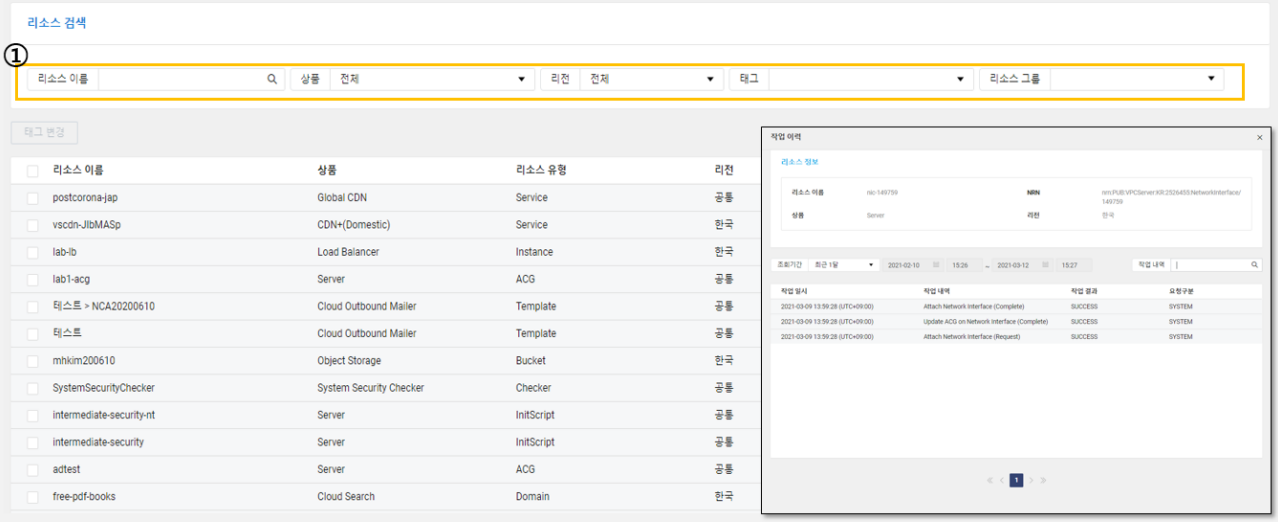
- **전체 리소스 관리 및 검색**
  네이버 클라우드 플랫폼 내 생성한 모든 리소스를 한 눈에 확인
  리소스명, 상품, 리전, 태그 및 그룹 조건에 의하여 원하는 리소스를 빠르게 검색 가능

- **리소스 별 작업 이력 제공**
  네이버 클라우드 플랫폼 내 생성된 모든 리소스 별 생성 및 변경 이력 확인

- **그룹 및 태그 지정**
  여러 리소스들을 서비스, 부서 및 담당자 등 다양한 목적에 따라 그룹 및 태그 지정 가능

NAVER CLOUD PLATFORM

Resource Manager 실제 화면



① 리소스 이름, 상품군, 리전, 태그 및 리소스 그룹에 따른 분류 별 리소스 검색이 가능합니다

NAVER CLOUD PLATFORM

Cloud Insight 개요

"클라우드 환경의 가시성/통찰력을 확보, 서비스의 연속성을 향상"

- **지표 조회 및 시각화**
  네이버 클라우드 플랫폼 상품의 성능/운영 지표를 다양한 형태(Line Chart, Area Chart)로 시각화 가능
  사용자 설정에 따른 Custom Metric 도 추가 지원
  현재 Compute, Networking, Analytics 상품 지원 (지속적으로 업데이트 할 예정)

- **사용자 대시보드 구성**
  성능/운영 지표를 위젯 형식으로 만들어 나만의 대시보드 생성 가능

- **Event Rule 및 Event 관리**
  장애 조짐이 의심되는 상황 및 실제 장애 상황을 식별할 수 있도록 Event Rule 을 생성 가능
  각 Event 마다 담당자를 지정할 수 있으며, SMS 및 Email을 통한 장애 전파 알람 가능

- **유지보수 일정 관리**
  유지보수 일정을 등록하여 해당 시간 동안 SMS 및 이메일 발송을 중지

NAVER CLOUD PLATFORM

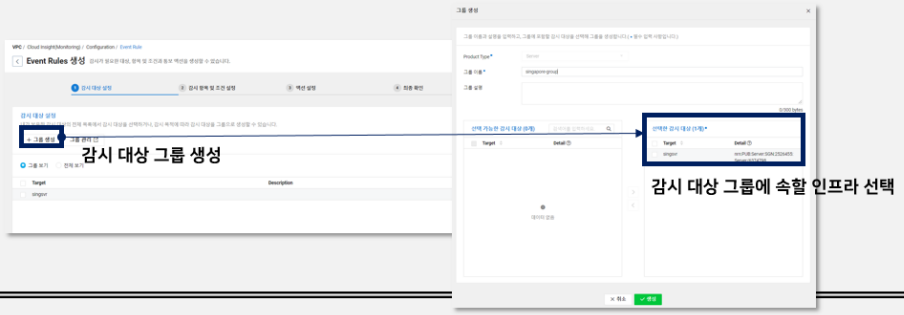
Cloud Insight

- Cloud Insight 내 Event Rules 생성을 통해 감시가 필요한 대상, 항목 및 조건과 Event 발생시 SMS나 이메일로 담당자에게 통보 알람을 발송하도록 설정할 수 있습니다.
- Event rule 설정은 1) 감시 상품 선택 → 2) 감시 대상 선택 → 3) 감시 항목(메트릭 항목) 선택 → 4) 메트릭 조건 설정(임계치 설정) → 5) 통보 대상자 선택으로 이루어집니다.
- 1) 감시대상 상품은 VPC와 Classic 플랫폼이 상이하며 서버 로드밸런서 Cloud DB 등 다양한 상품에 대한 Event 설정이 가능합니다.
  - Server(Classic, VPC)
  - Loadbalancer Monitor(Classic, VPC)
  - Cloud search(Classic, VPC)
  - Cloud DB For My-SQL(VPC)
  - Cloud DB For MS-SQL(VPC)
  - Cloud DB For Redis(VPC)
  - Cloud DB For MongoDB(VPC)
  - Cloud Hadoop(VPC)
  - Autoscaling group(VPC)
  - Kubernetes(VPC)
  - Elasticsearch(VPC)

NAVER CLOUD PLATFORM

Cloud Insight

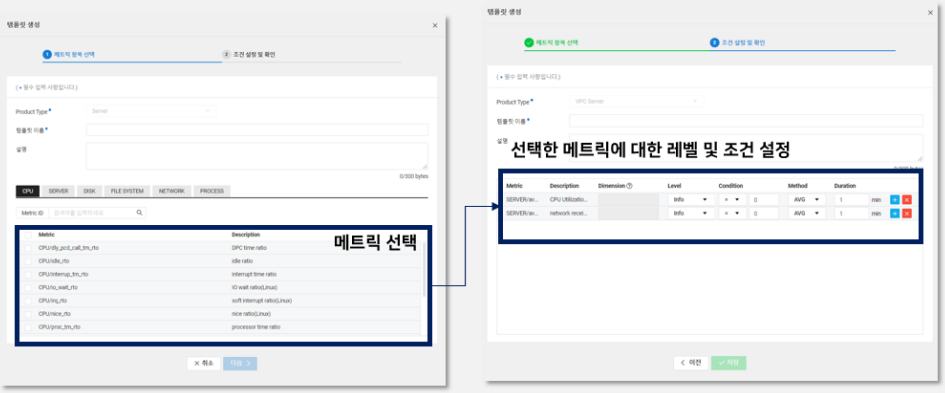
- 2) 감시 대상 선택에서는 감시 상품에 속한 실 인프라를 선택하는 과정입니다. (ex. 감시상품이 서버라면, 감시 대상은 계정 내에서 운영 중인 서버가 해당됩니다)
- 감시 대상은 감시 대상 그룹 관리를 통해 이루어집니다. Server(VPC) 상품의 경우 성능 지표 수집을 위해 agent가 필요하나, 서버 생성시 기본 탑재되기 때문에 사용자가 별도로 agent를 설치할 필요는 없습니다.
- 서버 상에서 아래의 명령어를 바탕으로 에이전트가 정상 동작하는지 확인이 가능합니다.
  - Linux : ps -ef | grep agent
  - Window : Window service에서 "nsight2_agent" 서비스의 상태를 확인



NAVER CLOUD PLATFORM

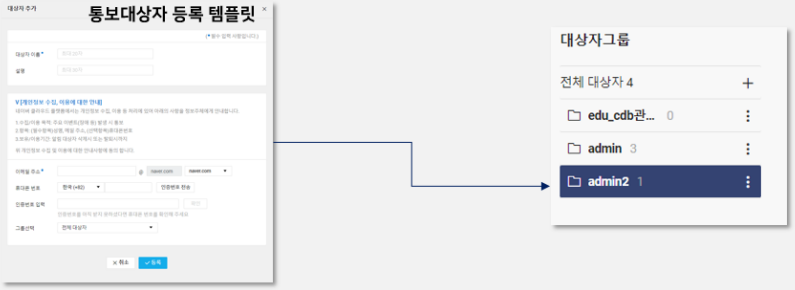
Cloud Insight

- 3) 감시 항목은 실제 통보 알람을 받을 항목(메트릭)을 선택하는 과정이며, 전체 목록에서 보여지는 Metric을 감시 항목으로 지정하거나, 감시 목적에 따라 감시 항목을 템플릿(Rule Template)으로 생성할 수 있습니다.
- 4) 메트릭 조건 설정 부분에서는 선택한 메트릭에 대하여 레벨(Info, Warning, Critical)을 선택할 수 있을 뿐만 아니라 실제 Event를 발생시킬 조건들을 설정합니다.



Cloud Insight

- 5) 통보 대상자 선택에서는 Event가 발생하였을 시 알람을 받을 관리 대상자를 선택할 수 있습니다.
- Notification Recipient 메뉴를 통해 Event Rule에 의한 Event 발생 시 SMS/Email로 통보를 받을 사용자의 이메일 주소와 연락처를 관리할 수 있습니다.
- 통보 대상자는 그룹으로 관리 가능하며, Event Rule 설정 시 통보 대상 그룹을 통보 대상자로 지정하여 Event 발생 시 그룹 내 사용자들에게 이벤트 알람이 전달되도록 구성이 가능합니다.



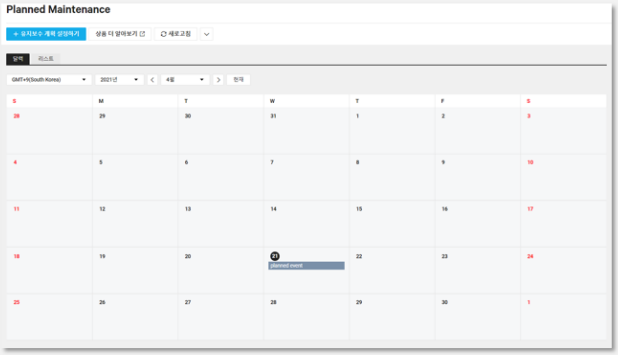
통보대상자들을 그룹핑하여 관리함으로써 인프라별 담당자 그룹을 설정할 수 있을 뿐만 아니라 다수의 관리자들이 동시에 통보알람을 받을 수 있도록 지원합니다.

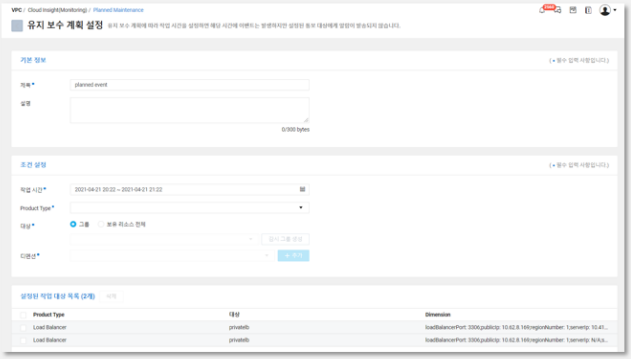
- Event 발생 시 통보 알람은 통보대상자 정보에 기입된 이메일, SMS뿐만 아니라 integration 내 Channel 생성을 통해 사용자가 지정한 Endpoint URL로 이벤트를 전송할 수 있습니다.

NAVER CLOUD PLATFORM

Cloud Insight

- 예정된 유지 보수, 배치 작업 등으로 특정 기간 동안 잠시 Event 발생에 따른 SMS/Email 통지와 같은 액션을 중단할 필요가 있는 경우, 이에 대한 일정을 등록해 해당 기간 동안 액션을 중지시킬 수 있습니다.
- 유지보수일정 등록을 위해, 유지보수 일정/기간/유지보수대상그룹 등을 기입합니다.

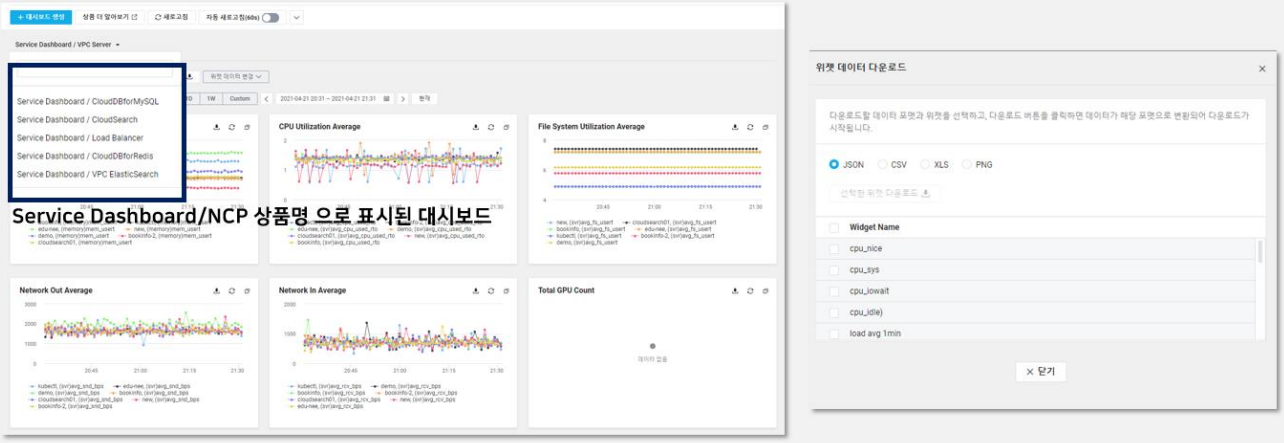




NAVER CLOUD PLATFORM

Cloud Insight

- Cloud insight 대시보드 메뉴에서는 Service Dashboard/NCP 상품명 으로 표시된 대시보드를 선택하면 해당 상품의 기본 메트릭을 한눈에 볼 수 있으며 위젯에 포함되어있는 데이터를 JSON, CSV, SLS, PNG 형태로 다운로드 받을 수 있습니다.



NAVER CLOUD PLATFORM

Cloud Advisor 개요

- Cloud Advisor 서비스는 네이버 클라우드 플랫폼 운영 노하우를 바탕으로 도출한 자체 모범 사례와 사용자의 이용 내용을 비교 분석하여 좀 더 안전하고 효율적으로 서비스를 이용할 수 있도록 사용자에게 권장 지침을 제공해주는 서비스입니다.
- 점검 결과에 대한 리포트를 제공하여 점검 항목에 대한 검사 결과를 확인할 수 있습니다.
  - **Sub Account 액세스키 관리**: SubAccount에 추가된 Access Key의 수명을 점검합니다.
  - **Sub Account 사용**: Sub Account 사용 여부를 검사합니다.
  - **Sub Account 비밀번호 관리**: Sub Account의 비밀번호 사용일을 점검합니다.
  - **Sub Account 2차인증 설정여부**: SubAccount에 2차 인증이 설정되어 있는지 점검합니다.
  - **Main Account 액세스키 관리**: 메인 계정이 사용하고 있는 Access Key의 사용일을 점검합니다.
  - **Main Sccount 비밀번호 관리**: 메인 계정의 비밀번호 사용일을 점검합니다.
  - **Main Account 2차인증 설정여부**: 메인 계정에 2차 인증이 설정되어 있는지 점검합니다.
  - **Load Balancer 리스너 보안 관리**: VPC LoadBalancer (Application, Network Proxy)에 권장하는 암호화 통신을 하는 리스너가 포함되어 있는지 검사합니다.
  - **Object Storage 버킷 권한** : 고객의 전체 버킷의 ACL을 확인하여, 외부에 공개된 경우 경고 합니다.
  - **Global DNS 레코드 SPF MX 점검**: MX 레코드에 대한 SPF, TXT 레코드가 존재하는지 확인합니다.
  - **Global DNS 레코드 TTL 점검**: 도메인에 연결된 레코드 세트의 TTL이 권장 TTL보다 높은지 검사합니다.
  - **Global DNS Authority NS점검**: 도메인 등록자 또는 DNS가 올바른 Global DNS 네임 서버를 사용하는지 검사합니다.
  - **ACG 포트 관리**: ACG 규칙 중 특정 포트에 대한 Any Open 규칙이 있는지 점검합니다.
  - **Cloud DB MYSQL 기본 PORT 점검**: Cloud DB for MySQL DB 서버 PORT를 점검합니다

NAVER CLOUD PLATFORM

Organization 개요

- **Organization 구성 및 비용 관리**
  - 조직의 IT 관리 담당자는 조직 내 각 부서 또는 개인이 사용 중인 네이버 클라우드 플랫폼 계정들을 초대하여 Organization을 생성할 수 있습니다.

- **서비스/부서/Workload 별 독립적인 클라우드 환경 제공**
  - 서비스/부서/Workload 별로 별도의 네이버 클라우드 플랫폼 계정을 생성하여 리소스를 효과적으로 분리하고 접근 가능한 사용자를 제한할 수 있습니다. 이렇게 계정이 분리된 환경에서도 Organization의 마스터 계정을 통해 하나의 계정을 사용하는 것처럼 모든 계정의 사용량 또는 비용을 확인하고 이에 대한 비용을 하나의 청구서로 지불할 수 있습니다.

- **이용 한도 관리**
  - Organization을 통해 조직의 클라우드 거버넌스 정책을 수립하고, 수립된 거버넌스 정책의 적용 범위를 지정할 수 있습니다. Organization의 마스터 계정은 사용할 수 있는 네이버 클라우드 플랫폼 서비스와 서비스 별 이용 한도를 정의한 이용 한도 정책을 생성하고, 이를 계정 그룹 또는 계정 별로 적용할 수 있습니다.

NAVER CLOUD PLATFORM

Organization 상품 용어 설명

항목	설명
마스터 계정	Organization 의 관리 권한을 가진 계정으로, Organization 을 생성한 계정이 해당 Organization 의 마스터 계정이 됩니다. 마스터 계정만이 다른 계정을 Organization 에 초대하거나, Organization 의 멤버 계정을 변경할 수 있습니다.
멤버 계정	Organization 에 소속된 계정으로, 각 멤버 계정은 반드시 하나의 Organization 에만 소속될 수 있습니다. Organization 마스터 계정의 초대를 받아 Organization 에 소속될 수 있으며, Organization 의 탈퇴를 위해서는 마스터 계정의 승인이 필요합니다.
계정 그룹	멤버 계정들의 집합으로 Organization 의 계층 구조를 관리하기 위해 사용됩니다. 계정 그룹 하위에 또다른 계정 그룹을 생성할 수 있으며, 계정 그룹에 멤버 그룹을 추가할 수 있습니다.
Quota Policy	마스터 계정이 계정 그룹에 부여한 이용 한도 정책으로, 계정 그룹 내 각 계정들은 마스터 계정이 부여한 이용 한도 내에서만 리소스를 생성할 수 있습니다. Quota Policy 를 통해 이용 한도를 제한하지 않은 리소스는 각 멤버 계정의 이용 한도에 따라 자유롭게 생성할 수 있습니다.

Organization 상품 이용 Flow

Organization 생성 -> 계정 초대 -> (자동)초대메일 발송 -> 초대받은 사람은 Pin Code 입력 -> 가입 승인

Lab 10

- SubAccount에 조직도 반영
- Cloud Insight에 조직도 반영
- Cloud Insight에 lnxsvr1에 대해 CPU 사용률이 80%를 넘으면 서버팀에 알람이 가도록 설정

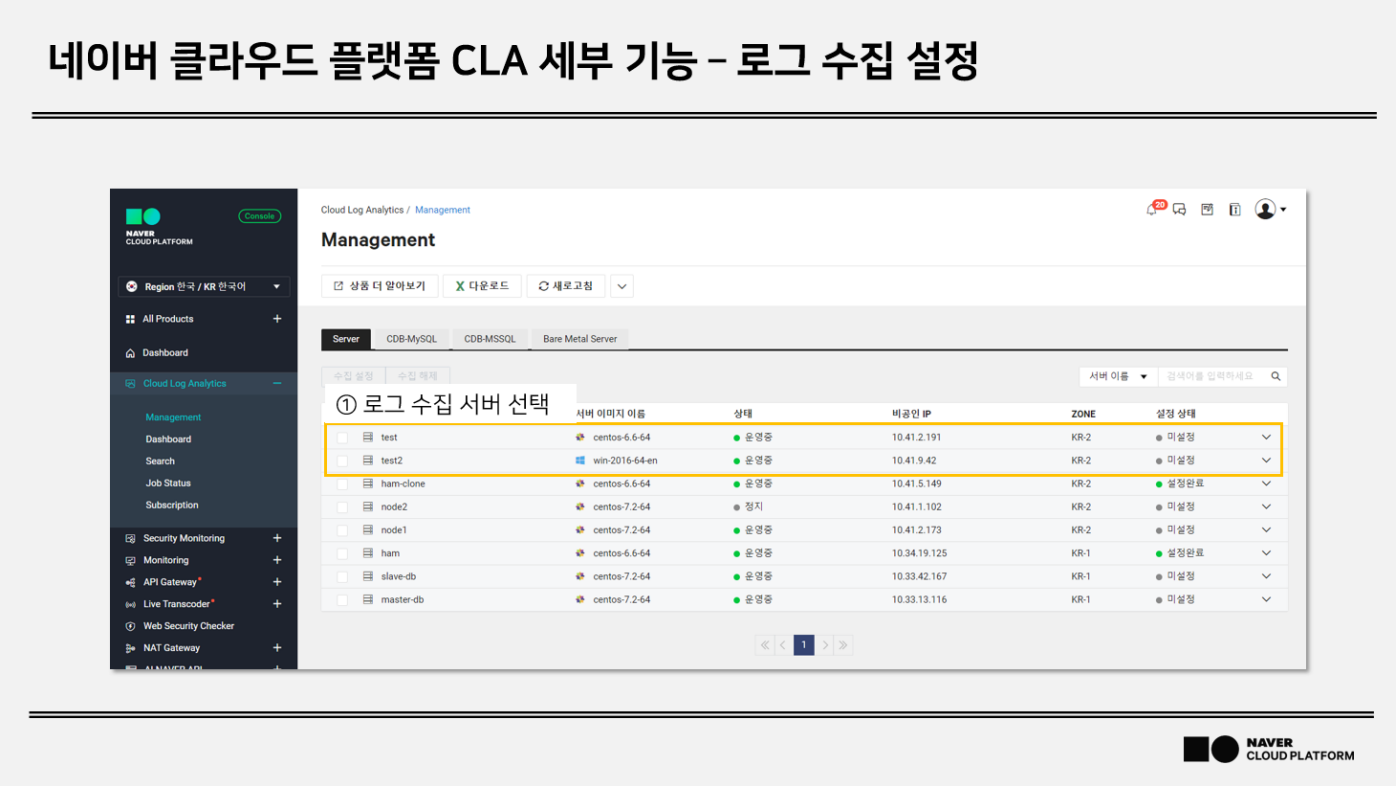
네이버 클라우드 플랫폼 Analytics - CLA

"CLA(Cloud Log Analytics)는 네이버 클라우드 플랫폼의 로그 관리 서비스입니다. "

서비스	구분	기능	설명
Cloud Log Analytics	Console	로그 수집 설정	웹 콘솔에서 로그 수집을 위한 모든 설정을 할 수 있습니다.
		에이전트 설치 및 실행	웹 콘솔에서 설정한 정보를 기준으로 스크립트를 수행하면 간편하게 에이전트가 설치 및 실행되어 바로 데이터를 수집할 수 있습니다.
		데이터 저장 및 검색	기본적으로 1주일간 1GB의 용량내에서 데이터가 무료로 수집/저장됩니다. 유료로 전환시 고객이 수집한 1달동안의 데이터가(최대 100GB) 다양한 방식의 검색을 통해 실시간으로 조회가 가능합니다.
		데이터 다운로드	필요한 데이터는 엑셀 등의 형식으로 대시보드에서 바로 다운로드 할 수 있습니다. 또한, CLA의 로그 검색 결과를 ObjectStorage로 내보낼 수 있습니다. 보유하고 계신 Object Storage를 선택하거나 신규 생성하여 저장이 가능합니다.
		대시보드	대시보드를 통해 다양한 항목의 데이터를 실시간으로 확인할 수 있습니다. -전체 / 일별 로그 발생 수 -최근 1분간 발생한 로그 현황 -현재 데이터 저장 용량 -데이터 타입별 사용 용량 -서버별 로그 발생 현황 등

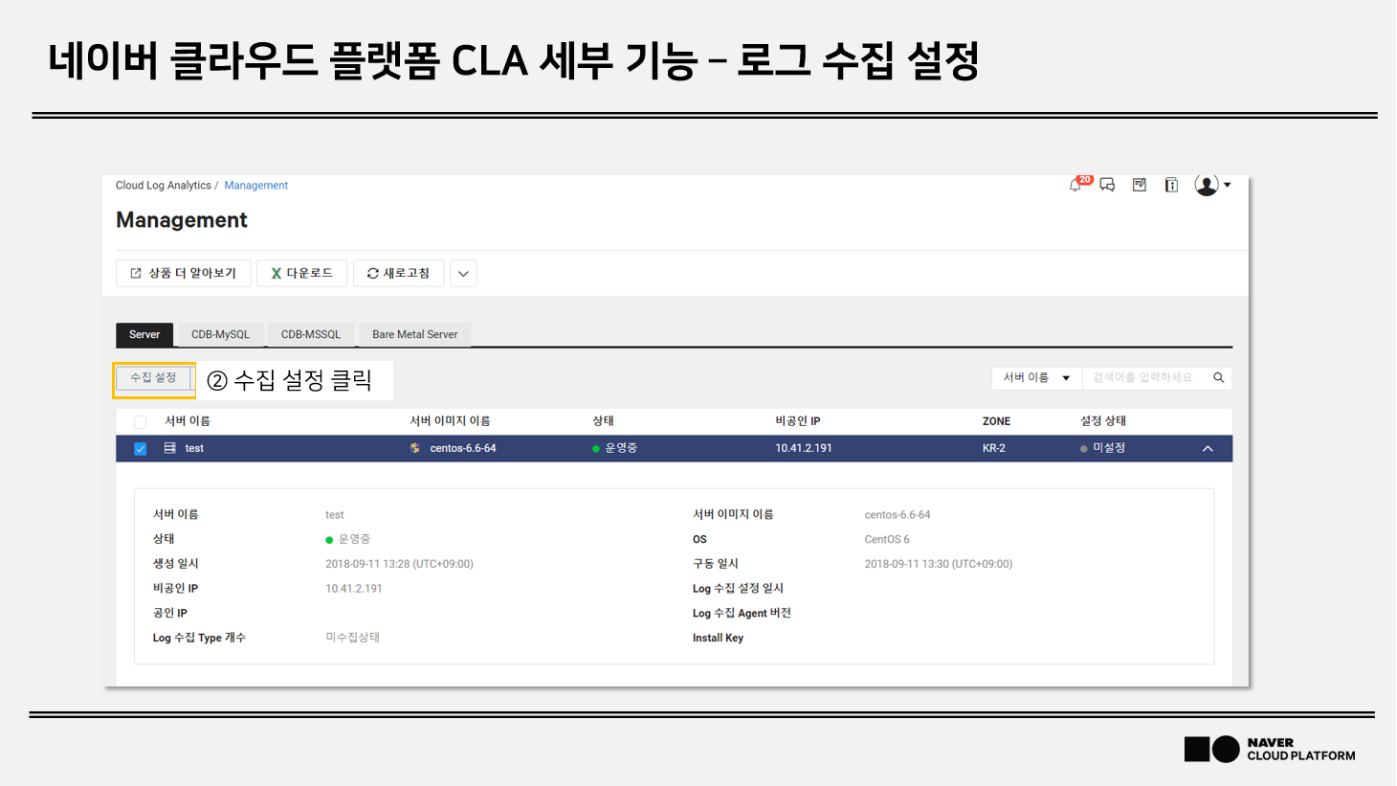
NAVER CLOUD PLATFORM

네이버클라우드플랫폼의 CLA는 서버에서 발생하는 모든 텍스트형태의 로그를 수집할 수 있습니다. 네이버클라우드플랫폼에서 제공하는 에이전트만 설치하면 바로 사용할 수 있으며 필요한 데이터는 엑셀 파일 형태로 다운로드하거나 검색된 로그에 대하여 Object Storage에 로그를 저장할 수 있도록 지원합니다. 만약 Object Storage 내에 버킷이 없다면, 미리 버킷을 생성한 후에 Export가 가능합니다.



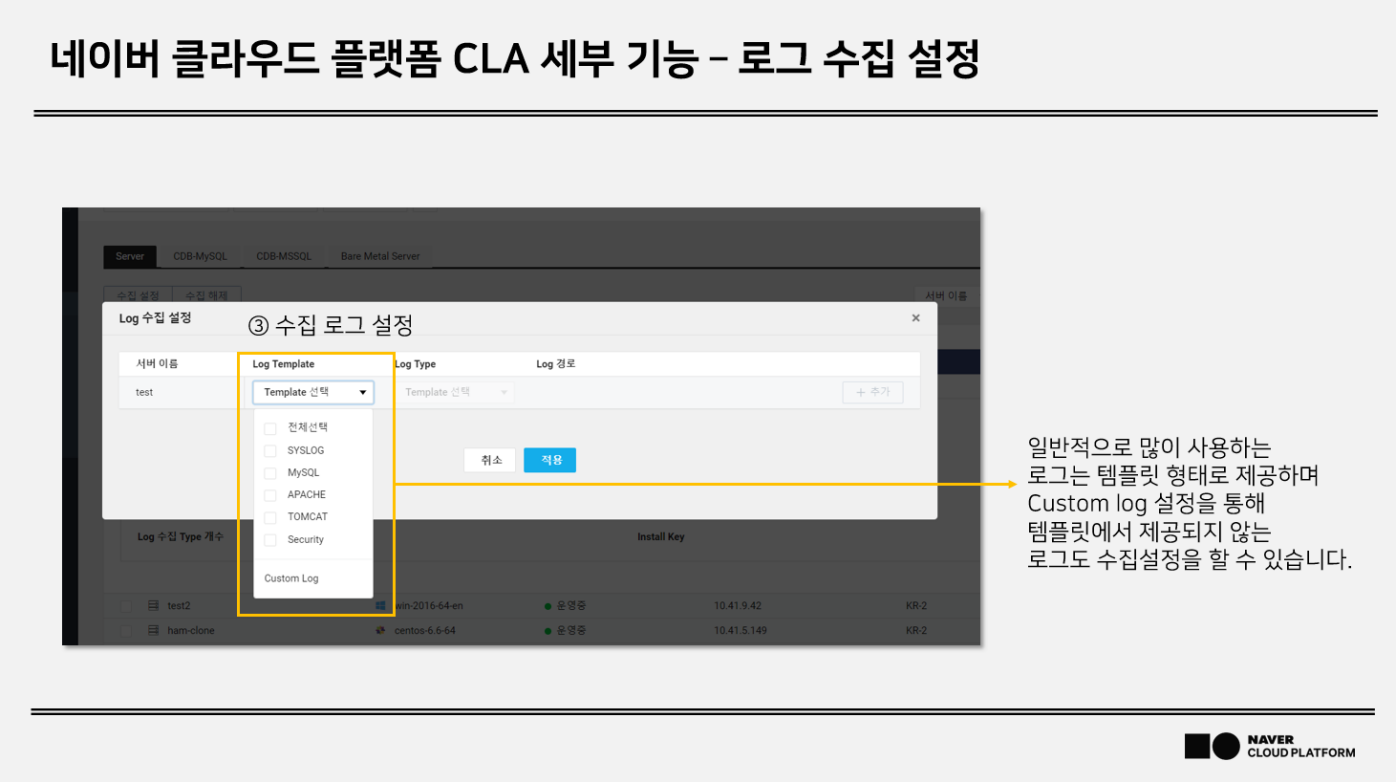
CLA 로그 수집 설정

네이버클라우드플랫폼 CLA를 사용하기위한 방법은 어렵지 않습니다. 가장 먼저 CLA로 로그를 수집하고자 하는 서버를 선택합니다.



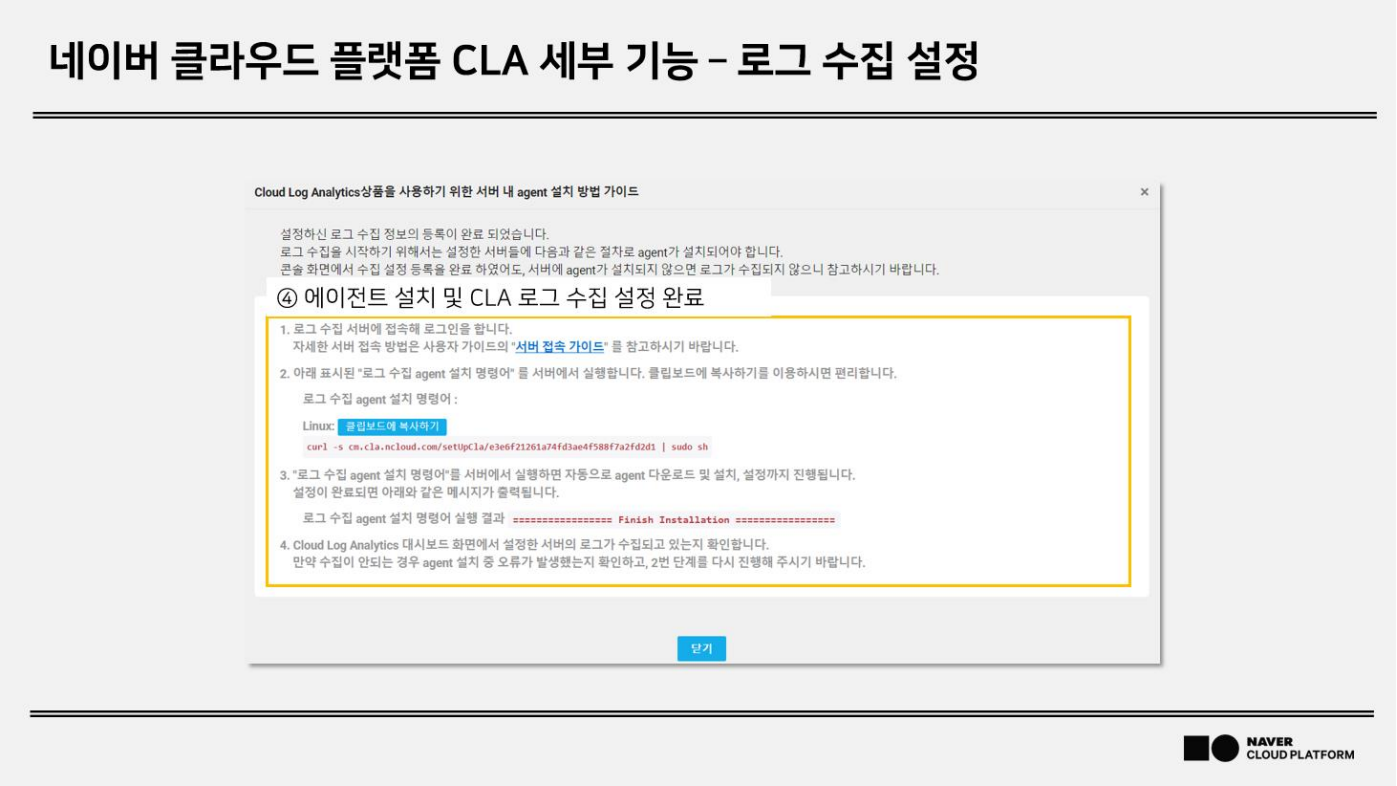
CLA 로그 수집 설정

다음으로 상단의 수집 설정 버튼을 클릭합니다.



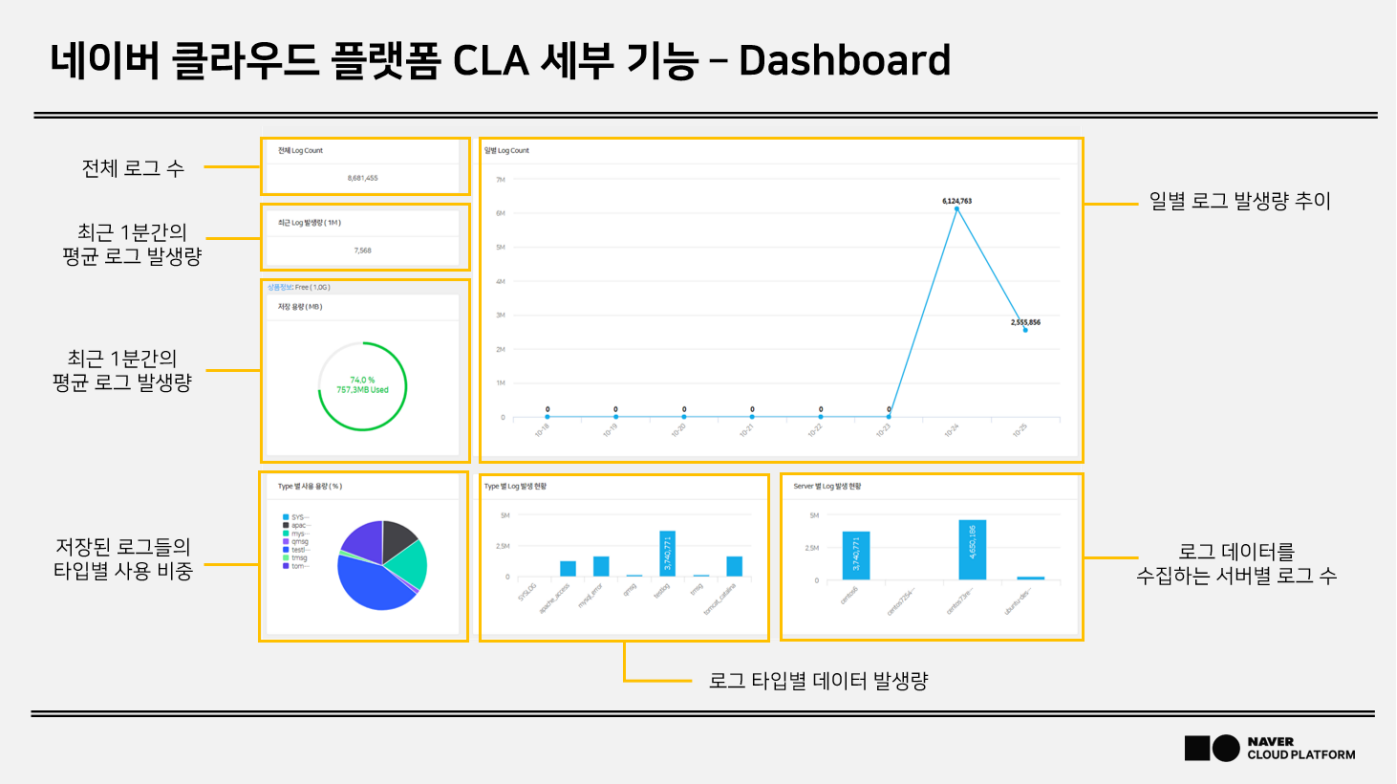
CLA 로그 수집 설정

마지막으로 수집 로그 템플릿을 선택합니다. 네이버클라우드플랫폼에서는 자주 사용되는 로그 타입을 템플릿 형태로 제공하고 있으며 템플릿으로 제공되지 않는 로그는 Custom log로 작성하여 사용하시면 됩니다.



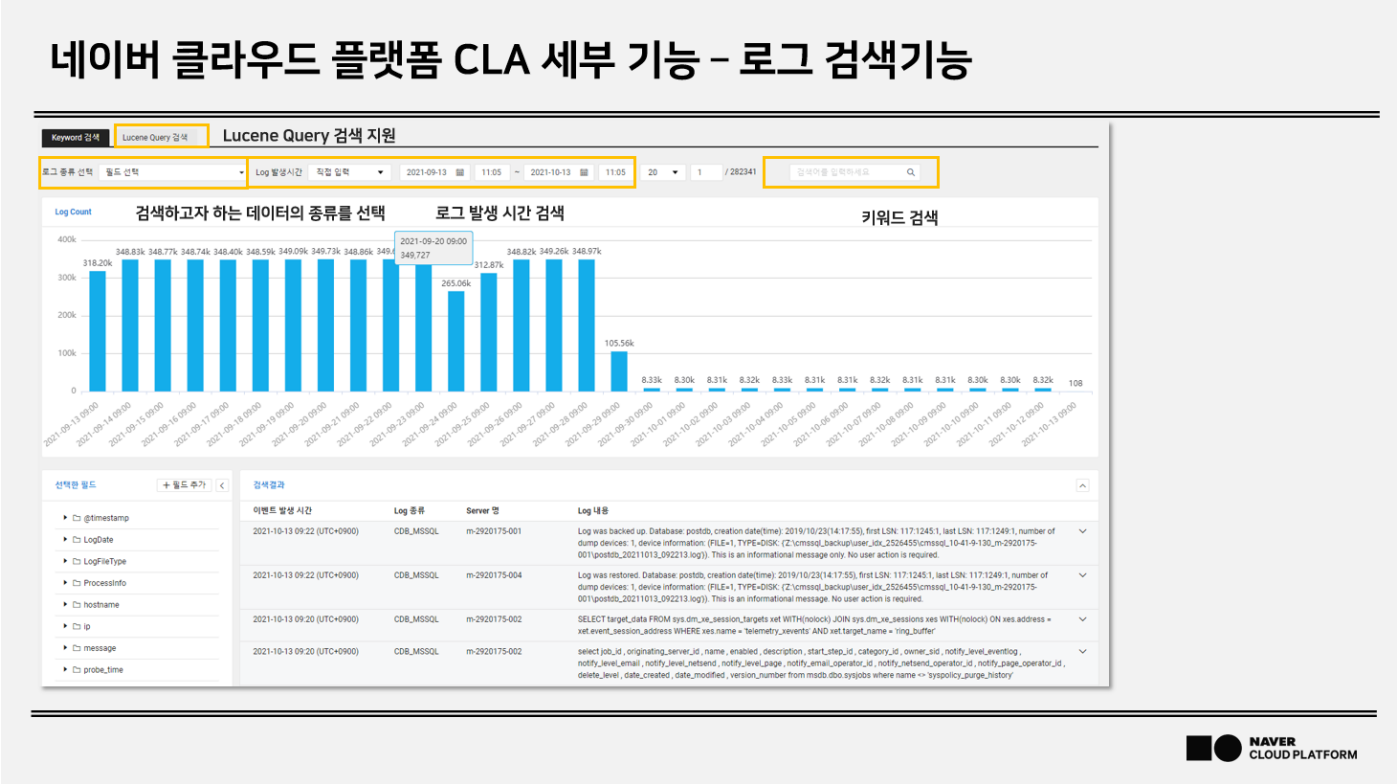
CLA 로그 수집 설정

마지막으로 CLA 로그 수집 에이전트만 설치해주면 됩니다. 로그 수집 에이전트 설치 명령어는 네이버클라우드플랫폼에서 제공하기 때문에, 명령어만 복사해서 서버에 설치해 주시면 됩니다.



CLA Dashboard

서버에 CLA 수집 에이전트를 설치하고 나면 대시보드를 통해 수집된 로그에 대한 현황을 살펴볼 수 있습니다. 대시보드에는 전체 로그 수, 최근 1분간의 평균로그 발생량, 저장된 로그타입별 비중, 일별 로그 발생량 추이, 로그 데이터를 수집하는 서버별 로그 수를 확인해 볼 수 있습니다.



CLA 로그 검색 기능

CLA에서는 수집된 로그에 대해서 필요한 로그만 검색이 가능하도록 키워드 기반의 로그 검색 기능과 Lucene Query 기능을 제공합니다. 로그의 종류나 로그 발생량에 따라서도 조회가 가능하며 기간별 검색도 지원합니다.

네이버 클라우드 플랫폼 Analytics - ELSA

" 애플리케이션 로그를 쉽게 저장하고 분석할 수 있는 서비스"

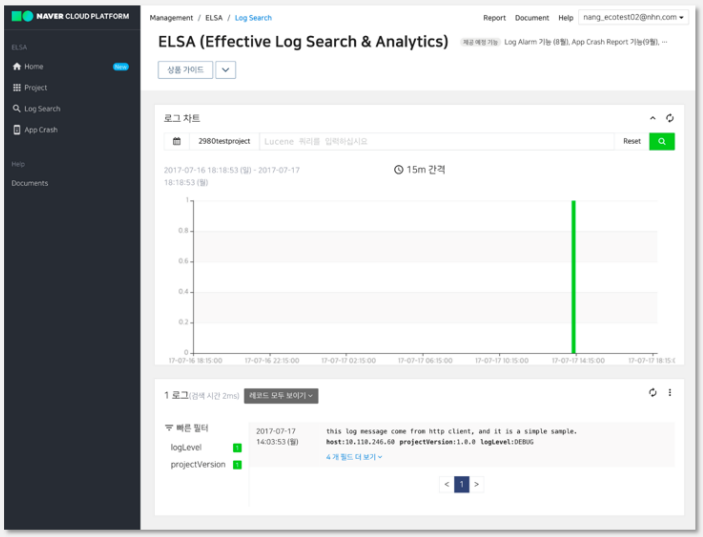
구분	기능	제공 기능 상세
Console	프로젝트 관리	손쉽게 프로젝트를 생성하고 관리할 수 있는 기능을 제공합니다.
	로그 검색	검색 기능을 통해 로그 정보를 조회하고 분석할 수 있습니다. 기간별(일/주/월 등)로 발생한 로그 이력을 확인할 수 있으며, 키워드를 직접 입력하거나 필터링 기능을 활용해 필요한 로그 정보를 편리하게 검색할 수 있습니다.
	모바일 크래시 로그 조회	앱 크래시 로그를 저장하고 분석할 수 있습니다. 등록된 프로젝트 단위로 비교 분석이 가능하며, 필터링 기능을 통해 크래시 로그의 세부 정보를 효율적으로 확인할 수 있습니다. 크래시 로그 발생 추이를 쉽게 파악할 수 있는 리포트 차트도 함께 제공합니다.
API	Log API	로그 전송 API와 관련된 상세한 가이드를 제공합니다. API 기능을 활용하여 실제 전송 정보를 입력한 후 로그를 저장할 수 있습니다. 추후 API 제공 기능을 점차 확대할 예정입니다.

NAVER CLOUD PLATFORM

네이버클라우드플랫폼 Analytics – ELSA

네이버클라우드플랫폼의 ELSA는 SDK 형태로 제공하여 앱에서 발생하는 실시간 로그를 확인할 수 있을 뿐만 아니라 앱크래시 정보를 저장하고 분석할 수 있기 때문에 빠르게 문제 상황을 파악하고 해결할 수 있도록 지원합니다.

네이버 클라우드 플랫폼 ELSA 상세 기능 – Log Search



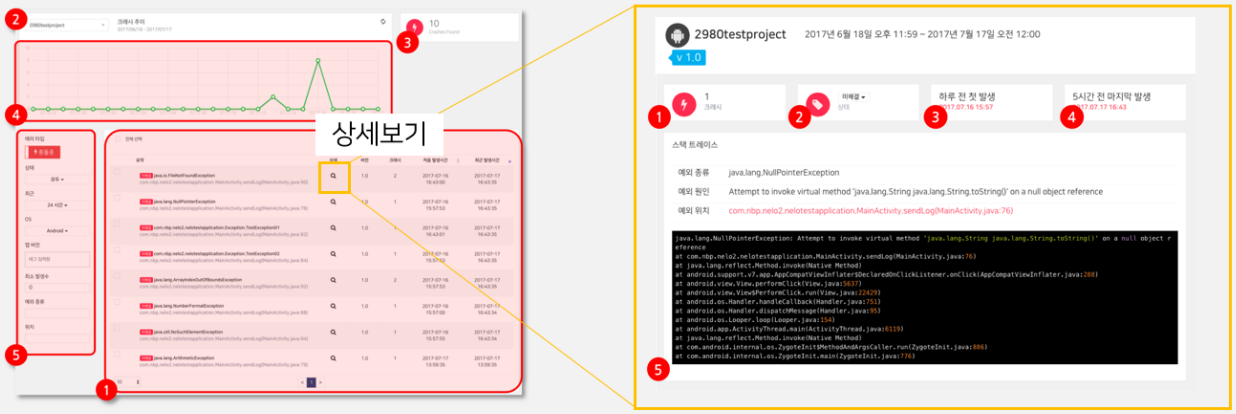
- MC화면의 Log Search에서는 기본값으로 현재 시간 기준으로 24시간 동안 발생한 로그에 대한 시간대별 로그 수집 개수 그래프와 상세 로그 형태로 제공됩니다.
- 실시간으로 저장되는 로그 정보를 로그레벨, 키워드, 기간 등 다양한 조건으로 통합 검색이 가능하며 발생되는 시간대 별로 저장하여 차트를 통해 확인할 수도 있습니다.
- 빠른 필터 기능도 제공하여 빠르게 로그 검색이 가능합니다.

항목명	설명
logLevel	레벨별로 로그를 출력합니다. (FATAL / ERROR / WARN / INFO / DEBUG)
logSource	사용자가 설정한 [로그 소스]로 구분합니다.
logType	사용자가 설정한 [로그 타입]으로 구분합니다.
projectVersion	사용자가 설정한 [프로젝트 버전]으로 구분합니다.

NAVER CLOUD PLATFORM

네이버 클라우드 플랫폼 ELSA 상세 기능 – Mobile App Crash

- MC의 App Crash에서는 iOS 와 Android 단말의 크래시 정보를 확인할 수 있습니다.
- 기본값으로 24시간 동안 발생한 크래시 상세 로그 및 크래시 횟수 그래프 형태로 나타납니다.
- 앱 크래시 조회화면에서 특정 예외 종류의 상세 버튼을 클릭하면 크래시의 스택 트레이스를 확인할 수 있습니다.



NAVER CLOUD PLATFORM

ELSA – Mobile App Crash

네이버클라우드플랫폼의 ELSA의 가장 강력한 기능은 모바일 앱크래시 정보를 쉽게 파악할 수 있다는 것입니다. ELSA 에서는 iOS와 안드로이드 단말의 크래시 정보를 확인할 수 있으며 기본적으로 24시간 이내에 발생한 크래시 상세로그 및 크래시 횟수를 그래프 형태로 나타납니다.

Lab 11

- CLA 서비스 생성하기
  - 서비스 구독
  - 로그 수집 대상 선정 및 로깅 데이터 정의
  - 에이전트설치

- Object Storage 백업설정하기
  - 버킷 생성하기
  - CLA로그백업설정

NAVER CLOUD PLATFORM

NAVER CLOUD PLATFORM

207 Trouble Shooting

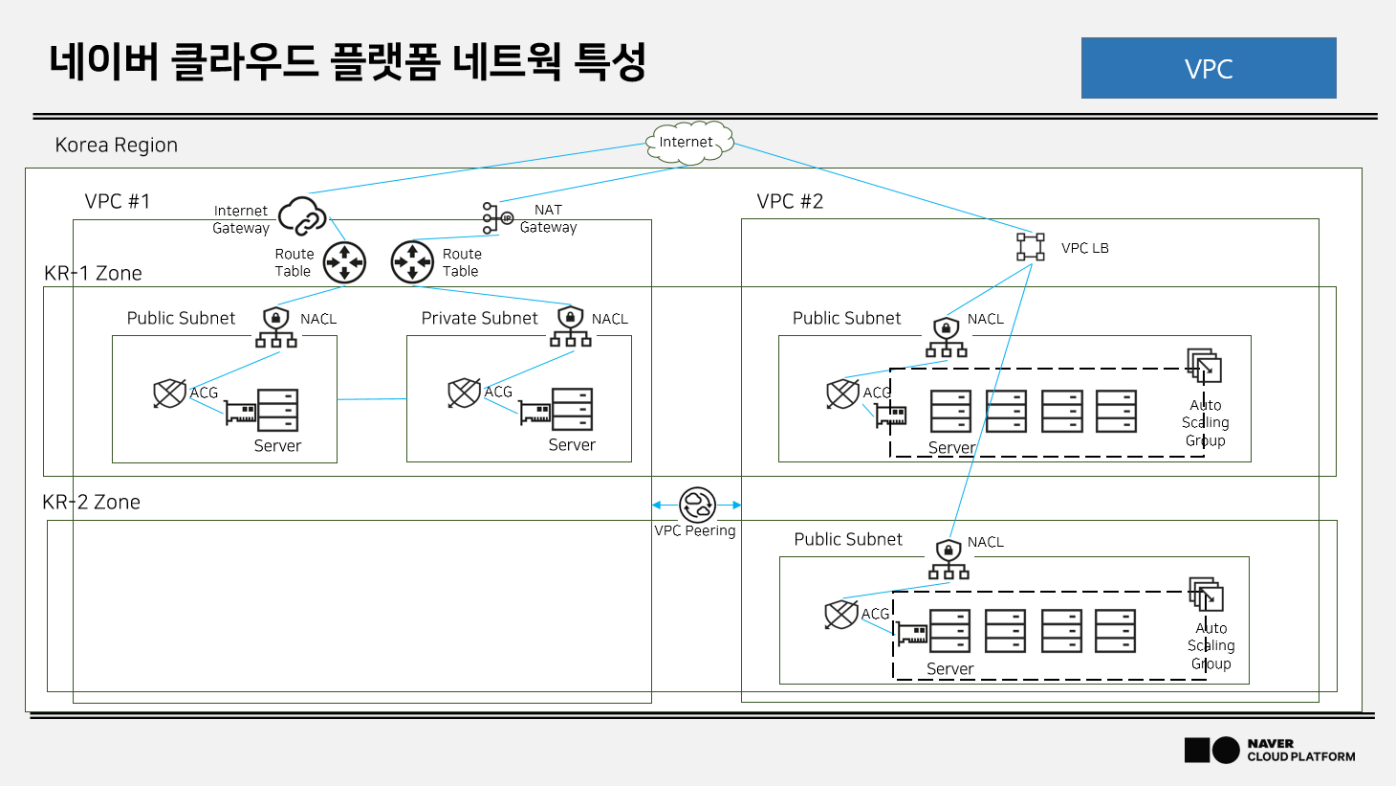
적절한 용량 산정

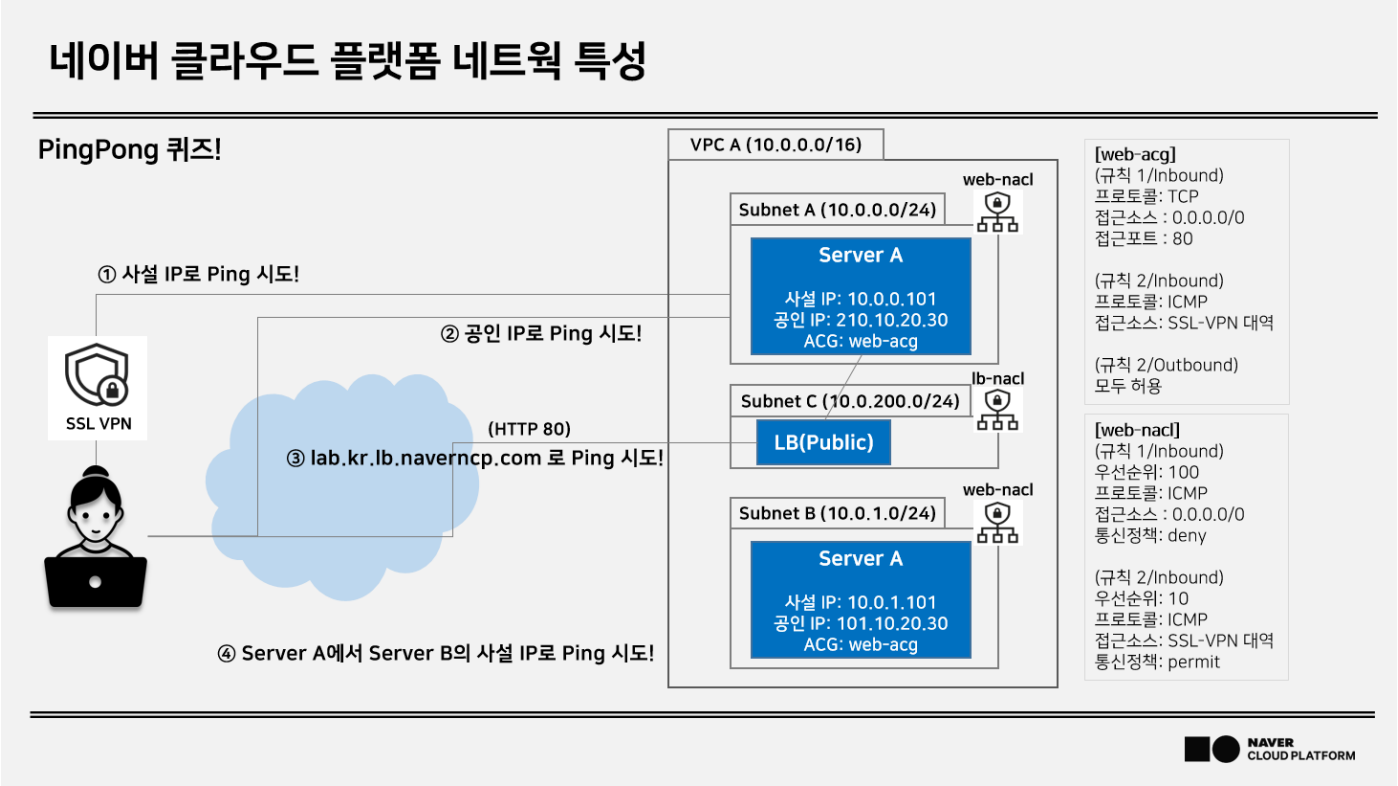
- 컴퓨팅 파워
  - IO Wait 이 발생하는 시점부터 서비스 품질은 떨어지기 시작
  - SWAP을 사용하는 경우 메모리 증설
  - 관련 명령어 : sar, ps, top
- 네트워크
  - 동접 기준으로 파일(페이지)를 기한내에 전송할 수 있을지를 가지고 산정
  - 서버의 경우 전송 속도 500Mbps 기준으로 서버 대수 산정
  - CDN의 경우 가용량 기준으로 산정
- 용량 산정 주요 지표
  - 파일(페이지) 크기
  - 동접

NAVER CLOUD PLATFORM

클라우드에서의 용량산정 전략

1. Scale Out 전략
   - 서버의 증감이 자유롭도록 설계
2. 초기에 과투입 후 서서히 리소스를 축소
   - 초기에 서비스가 필요로 하는 리소스보다 많은 리소스를 투입한 후 서비스 안정화 되면 리소스를 적정 수준까지 축소하는 전략


네이버 클라우드 플랫폼 네트워 특성
VPC
Korea Region
Internet
VPC #1
Internet Gateway
NAT Gateway
Route Table
Route Table
KR-1 Zone
Public Subnet
NACL
ACG
Server
Private Subnet
NACL
ACG
Server
VPC #2
VPC LB
Public Subnet
NACL
ACG
Server
Auto Scaling Group
KR-2 Zone
VPC Peering
Public Subnet
NACL
ACG
Server
Auto Scaling Group
NAVER CLOUD PLATFORM



문제풀이

① 서버 A의 사설 IP로 Ping 시도 => 성공

A. 사용자는 SSL VPN 클라이언트에 로그인을 하였기에, 사용자 PC에는 SSL VPN 대역의 IP가 한 개 부여된 상태입니다. 이 때 NACL 및 ACG에서 SSL VPN 대역에 대한 ICMP 프로토콜을 모두 허용하고 있기 때문에, 해당 통신은 정상적으로 성공합니다.

② 서버 A의 공인 IP로 Ping 시도 => 실패

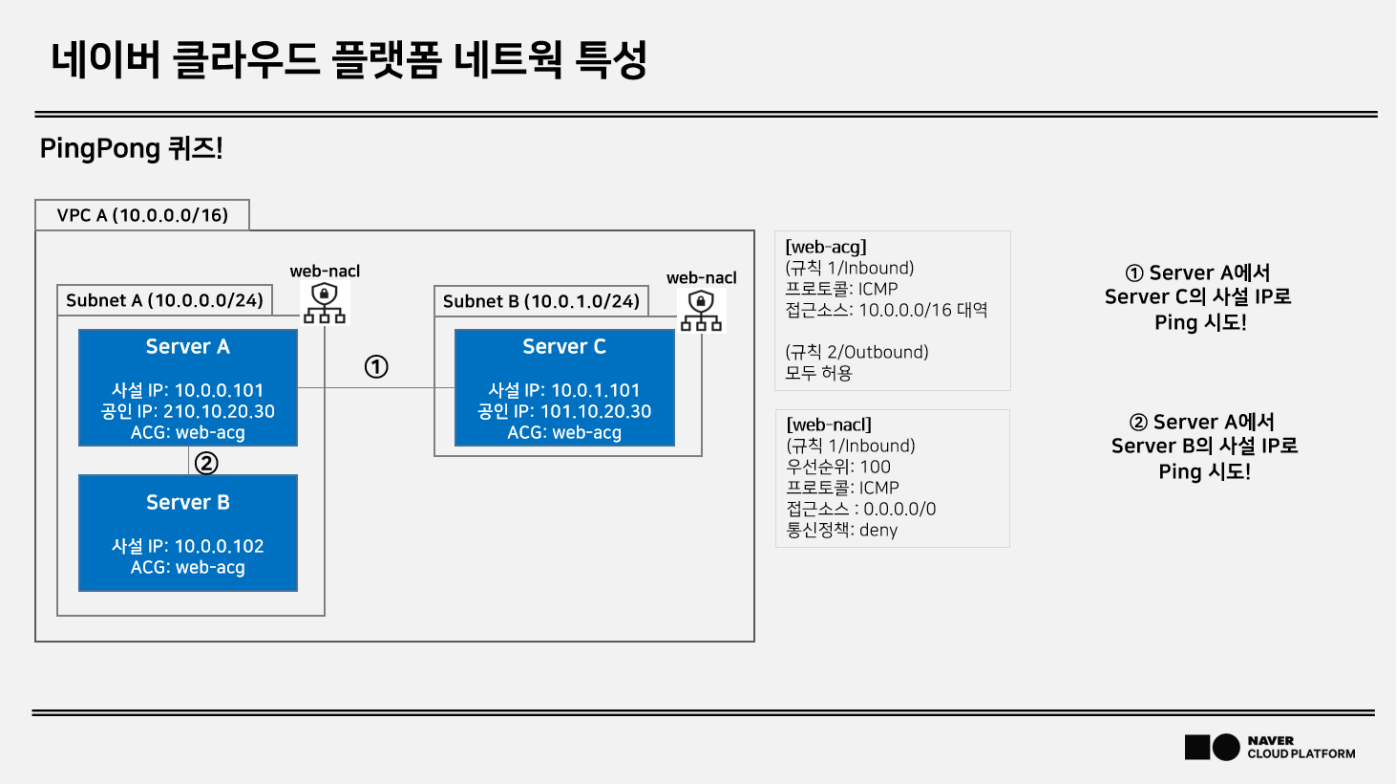
A. NACL 규칙에는 SSL VPN 대역을 제외한 나머지 모든 대역의 ICMP 프로토콜 인입을 거부하는 정책이 들어가있습니다. 따라서 사용자가 인터넷을 통해 Ping을 시도할 경우, 1차적으로 NACL에서 걸러지게 됩니다.

③ 서버 A와 연결된 LB의 도메인주소로 Ping 시도 => 실패

A. 로드밸런서의 도메인 주소로는 기본적으로 Ping이 나가지 않습니다.

④ 서버 A에서 서버 B의 사설 IP로 Ping 시도 => 실패

A. 서버 A와 서버 B가 서로 통신하기 위해서는 서버가 생성된 대역은 어느 곳인지(NACL 통과 여부), ICMP 허용 정책이 들어가있는지 확인이 필요합니다. 서버 A와 B는 다른 서브넷에 존재하는 서버로 NACL 규칙과 ACG 규칙을 모두 살펴볼 필요가 있습니다. NACL 규칙 및 ACG 규칙 모두 각 서버 대역에 대해 ping을 허용하는 정책이 들어가있지 않으므로, 정상적으로 통신이 불가능합니다.



문제풀이

① 서버 A에서 서버 C의 사설 IP로 Ping 시도 => 실패

② 서버 A에서 서버 B의 사설 IP로 Ping 시도 => 성공

성능 측정

- 웹서비스
  - WMS
  - Ngrinder
  - Pinpoint
  - AB

- MySQL 성능측정
  - Percona TPCC
  - sysbench
  - Apache Jmeter

NAVER CLOUD PLATFORM

성능 측정

- AB의 설치
  - Yum install httpd-tools

- AB 옵션
  - -n 요청 수
  - -c 동시에 요청하는 요청 수
  - -g 측정한 모든값을 gunplot 혹은 TSV 파일로 기록
  - -t 성능을 검사하는 최대 시간 (초단위)
  - -v 출력에 대한 상세한 정보 지정
    - 4 : 헤더에 대한 정보
    - 3 : 응답코드
    - 2: 정보
  - -X 프록시 서버를 사용하여 요청

NAVER CLOUD PLATFORM

AB 사용법

ab [-A *auth-username*:*password*] [-c *concurrency*] [-C *cookie-name*=*value*] [-d] [-e *csv-file*] [-g *gnuplot-file*] [-h] [-H *custom-header*] [-i] [-k] [-n *requests*] [-p *POST-file*] [-P *proxy-auth-username*:*password*] [-q] [-s] [-S] [-t *timelimit*] [-T *content-type*] [-v *verbosity*] [-V] [-w] [-x *<table>-attributes*] [-X *proxy*[:*port*]] [-y *<tr>-attributes*] [-z *<td>-attributes*] [http://]*hostname*[:*port*]/*path*

-A *auth-username*:*password*

서버에게 BASIC Authentication 정보를 제공한다. :으로 구분한 사용자명과 암호를 base64 인코딩하여 전송한다. 서버가 정보를 요구하는지 (*예를 들어*, 401 인증 필요를 보내는지) 관계없이 문자열을 전송한다.

-c *concurrency*

동시에 요청하는 요청수. 기본적으로 한번에 한 요청만을 보낸다.

-C *cookie-name*=*value*

요청에 Cookie: 헤더를 추가한다. 아규먼트는 보통 *name*=*value* 와 같은 쌍이다. 이 옵션은 여러번 사용할 수 있다.

-d

"percentage served within XX [ms] table"을 출력하지 않는다. (호환성을 위해).

-e *csv-file*

요청을 처리하는데 걸린 (밀리초 단위) 시간들의 (1%에서 100%) 누적백분율을 쉼표로 구분한 형식(CSV)으로 출력한다. 결과를 이미 '정리'하였기때문에 'gnuplot' 파일보다 보통 더 유용하다.

-g *gnuplot-file*

측정한 모든 값을 'gnuplot' 혹은 TSV (Tab separate values, 탭으로 구분한 값) 파일에 기록한다. Gnuplot, IDL, Mathematica, Igor, 심지어 Excel 같은 프로그램에서도 이런 파일을 쉽게 읽을 수 있다. 파일의 첫번째 줄에 항목이름이 나온다.

-h

사용법을 출력한다.

-H *custom-header*

요청에 헤더를 추가한다. 아규먼트는 보통 콜론으로 구분한 쌍인 (*예를 들어*, "Accept-Encoding: zip/zop;8bit") 유효한 헤더줄이다.

-i

GET 대신 HEAD 요청을 한다.

-k

HTTP KeepAlive 기능을 사용한다. *예를 들어*, 한 HTTP 세션에서 여러 요청을 한다. 기본적으로 KeepAlive 를 사용하지 않는다.

-n *requests*

성능을 검사하기위해 보내는 요청수. 기본값으로 요청을 한번만 보내기때문에 일반적인 성능검사 결과를 얻을 수 없다.

-p *POST-file*

POST 자료 파일.

-P *proxy-auth-username*:*password*

프록시를 통해 BASIC Authentication 정보를 제공한다. :로 구분한 사용자명과 암호를 base64 인코딩하여 전송한다. 프록시가 정보를 요구하는지 (*예를 들어*, 401 인증 필요를 보내는지) 관계없이 문자열을 전송한다.

-q

150 개 이상 요청을 보낼 때 ab 는 10% 혹은 매 100 요청당 표준오류에 진행상황을 출력한다. -q 옵션은 이 문구를 출력하지 않는다.

-s

기능을 추가하여 컴파일하였다면 (ab -h 로 확인할 수 있다) http 프로토콜 대신 SSL 을 사용한 https 프로토콜을 사용한다. 이 기능은 실험적이고 *매우* 기초적이다. 아마도 사용을 꺼려할 것이다.

-S

중간값과 표준편차를 출력하지 않고, 평균과 중간값의 차이가 표준편차보다 크더라도 경고/오류를 출력하지 않는다. 최소/평균/최대 값을 출력한다. (호환성을 위해).

-t *timelimit*

성능을 검사하는 최대 초단위 시간. 내부적으로 -n 50000 을 가정한다. 정해진 시간동안 서버 성능을 검사할 때 사용한다. 기본적으로 시간제한 없이 검사한다.

-T *content-type*

POST 자료의 Content-type 헤더.

-v *verbosity*

출력의 자세함 수준을 지정한다. 4 이상이면 헤더에 대한 정보를, 3 이상이면 (404, 202, 등) 응답코드를, 2 이상이면 경고(warning)와 정보(info)를 출력한다.

-V

버전을 출력하고 종료한다.

-w

결과를 HTML 표로 출력한다. 기본적으로 표를 흰 배경에 두 열로 작성한다.

-x *<table>-attributes*

<table>의 속성으로 사용할 문자열. 속성을 <table *여기에*> 추가한다.

-X *proxy*[:*port*]

프록시 서버를 사용하여 요청한다.

-y *<tr>-attributes*

<tr>의 속성으로 사용할 문자열.

-z *<td>-attributes*

<td>의 속성으로 사용할 문자열.

Sysbench를 이용한 MySQL 성능 측정법

```
sysbench --test=oltp --oltp-table-size=[테이블-레코드-건수]

--max-requests=[쿼리-요청-개수] --max-time=[테스트-시간]

--mysql-host=[호스트명] --mysql-db=[테스트-데이터베이스명] --mysql-user=[DB-USER] --mysql-
password=[DB-USER-비밀번호]

--mysql-table-engine=[테이블-엔진-종류] --myisam-max-rows=[MyISAM 인 경우-레코드-최대-건수]

--mysql-socket=[MySQL-소켓-파일-경로]

--mysql-port=[MySQL-포트-번호]

--oltp-test-mode=[simple|complex|nontrx] 테스트 모드 선택

--oltp-read-only=[on|off]

--oltp-read-only=off --db-driver=mysql

prepare
```

문제 진단을 위해 활용가능한 상품

- 웹서비스
  - WMS
  - Pinpoint

- DB
  - Cloud for MySQL
    - DB Dashboard
    - OS Dashboard
    - DB Logs
    - Query TimeLine

  - Cloud for MS-SQL
    - DB Dashboard
    - Performance
    - DB Logs

NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- Linux
  - tcpdump
  - Nmap
  - Traceroute
  - Sar
  - Ps
  - Lsof

- Windows
  - Microsoft Message Analyzer(https://www.microsoft.com/en-us/download/details.aspx?id=44226)
  - 이벤트 뷰어(eventvwr)
  - Performance Monitor(perfmon)
  - PSTools(https://docs.microsoft.com/en-us/sysinternals/downloads/pstools)

NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- sar
  - 리소스 사용량에 대한 로그 조회
  - Linux에서 시스템에 대한 광범위한 모니터링
  - CPU 사용률, 메모리, iowait, 로드 를 비롯한 다양한 정보를 확인 가능

- Demo
  - Sar –A
  - Sar –b (I/O)
  - Sar –n (network)
  - Sar –w (컨텍스위칭)

NAVER CLOUD PLATFORM

Sar 사용법

```
sar [ -A ] [ -b ] [ -B ] [ -C ] [ -d ] [ -h ] [ -i interval ] [ -m ] [
        -p ] [ -q ] [ -r ] [ -R ] [ -S ] [ -t ] [ -u [ ALL ] ] [ -v ] [ -V ] [
        -w ] [ -W ] [ -y ] [ -j { ID | LABEL | PATH | UUID | ... } ] [ -n {
        keyword [,...] | ALL } ] [ -I { int [,...] | SUM | ALL | XALL } ] [ -P
        { cpu [,...] | ALL } ] [ -o [ filename ] | -f [ filename ] ] [
        --legacy ] [ -s [ hh:mm:ss ] ] [ -e [ hh:mm:ss ] ] [ interval [ count
        ] ]
```

문제 해결을 위한 명령어들

- Ping
  - ICMP를 이용한 프로그램
  - 해당 호스트가 살아있는지 죽어 있는지
  - 방화벽에 의해 막혀 있는지 확인하기 위해 사용하는 기초적인 명령어
  - Windows와 Linux에서의 옵션은 서로 상이

NAVER CLOUD PLATFORM

Linux Ping 사용법

```
ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface or address] [-M mtu discovery hint] [-S sndbuf]
            [ -T timestamp option ] [ -Q tos ] [hop1 ...] destination
```

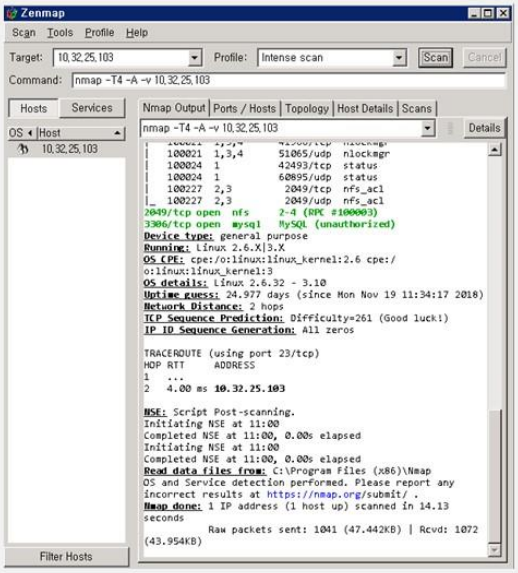
Windows Ping 사용법

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]    [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

문제 해결을 위한 명령어들

- nmap
  - 포트스캔용 툴
  - 오픈되어 있는 포트에 대해 스캔
  - 호스트 뿐만 아니라 대역으로도 탐지
  - 응용프로그램 버전 및 OS 탐지
  - Linux 와 Windows 버전 사용 가능



NAVER CLOUD PLATFORM

NMAP 사용법

```
nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -PR: ARP ping - does not need HW address -> IP translation
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

```
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  -sR: Check what service uses opened ports using RPC scan
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

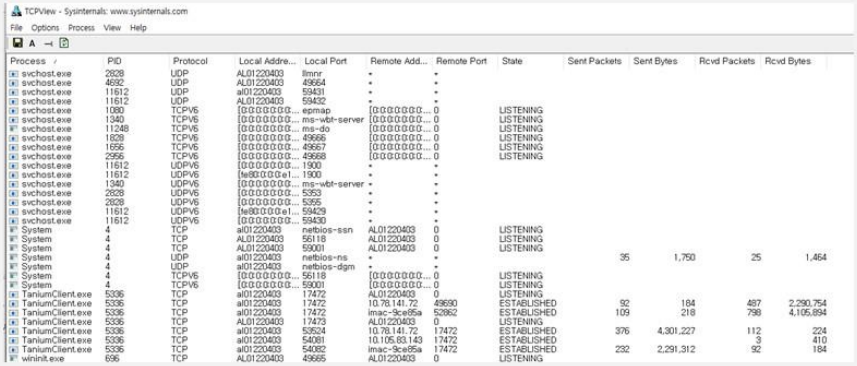
문제 해결을 위한 명령어들

- 단일 호스트 검색
  - Nmap 106.10.50.45, 10.41.83.101
  - Nmap -v 106.10.50.45, 10.41.83.101
- 대역으로 검색
  - Nmap 106.10.50.45-50, Nmap 106.10.50.*, Nmap 106.10.50.0/24, Nmap 10.41.83.101
- 방화벽 확인
  - Nmap -sA 106.10.50.45, 10.41.83.101
- 방화벽 으로 보호되는 호스트에 대한 스캔
  - Nmap -PN 106.10.50.45, 10.41.83.101
- 모든 패킷 표시
  - Nmap -packet-trace 106.10.50.45, 10.41.83.101

NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- TCPView
  - https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
  - Windows 시스템의 TCP/UDP에 대한 상세 정보 확인
    - Process, PID, Protocol, Address/Port, State, Packet Size
  - 작업중인 시스템의 오픈 된 네트워크 연결 프로세스 확인



Process	PID	Protocol	Local Addre...	Local Port	Remote Add...	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
svchost.exe	2828	UDP	AL01220403	llmnr	*	*					
svchost.exe	4692	UDP	AL01220403	49664	*	*					
svchost.exe	11612	UDP	al01220403	59431	*	*					
svchost.exe	11612	UDP	AL01220403	59432	*	*					
svchost.exe	1080	TCPV6	[0:0:0:0:0:0:...	epmap	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	1340	TCPV6	[0:0:0:0:0:0:...	ms-wbt-server	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	11248	TCPV6	[0:0:0:0:0:0:...	ms-do	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	1828	TCPV6	[0:0:0:0:0:0:...	49666	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	1656	TCPV6	[0:0:0:0:0:0:...	49667	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	2956	TCPV6	[0:0:0:0:0:0:...	49668	[0:0:0:0:0:0:...	0	LISTENING				
svchost.exe	11612	UDPV6	[0:0:0:0:0:0:...	1900	*	*					
svchost.exe	11612	UDPV6	[fe80:0:0:0:e1...	1900	*	*					
svchost.exe	1340	UDPV6	[0:0:0:0:0:0:...	ms-wbt-server	*	*					
svchost.exe	2828	UDPV6	[0:0:0:0:0:0:...	5353	*	*					
svchost.exe	2828	UDPV6	[0:0:0:0:0:0:...	5355	*	*					
svchost.exe	11612	UDPV6	[fe80:0:0:0:e1...	59429	*	*					
svchost.exe	11612	UDPV6	[0:0:0:0:0:0:...	59430	*	*					
System	4	TCP	al01220403	netbios-ssn	AL01220403	0	LISTENING				
System	4	TCP	AL01220403	56118	AL01220403	0	LISTENING				
System	4	TCP	AL01220403	59001	AL01220403	0	LISTENING				
System	4	UDP	al01220403	netbios-ns	*	*		35	1,750	25	1,464
System	4	UDP	al01220403	netbios-dgm	*	*					
System	4	TCPV6	[0:0:0:0:0:0:...	56118	[0:0:0:0:0:0:...	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:...	59001	[0:0:0:0:0:0:...	0	LISTENING				
TaniumClient.exe	5336	TCP	al01220403	17472	AL01220403	0	LISTENING				
TaniumClient.exe	5336	TCP	al01220403	17472	10.78.141.72	49690	ESTABLISHED	92	184	487	2,290,754
TaniumClient.exe	5336	TCP	al01220403	17472	imac-9ce85a	52862	ESTABLISHED	109	218	798	4,105,894
TaniumClient.exe	5336	TCP	AL01220403	17473	AL01220403	0	LISTENING				
TaniumClient.exe	5336	TCP	al01220403	53524	10.78.141.72	17472	ESTABLISHED	376	4,301,227	112	224
TaniumClient.exe	5336	TCP	al01220403	54081	10.105.63.143	17472	ESTABLISHED			3	410
TaniumClient.exe	5336	TCP	al01220403	54082	imac-9ce85a	17472	ESTABLISHED	232	2,291,312	92	184
wininit.exe	696	TCP	AL01220403	49665	AL01220403	0	LISTENING				

NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- traceroute
  - ICMP와 TTL을 이용하여 경로를 확인하는 프로그램
  - Windows에서는 tracert
  - 최근의 네트웍 장비들은 ICMP에 대해 응답하지 않음
  - 글로벌 환경에서 어떤 회선을 타고 가는지 확인이 필요할 경우 사용

NAVER CLOUD PLATFORM

Traceroute 사용법

```
traceroute [ -46dFITnreAUV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] host [ packetlen ]
```

문제 해결을 위한 명령어들

- ps
  - 현재 프로세스를 확인하는 명령어
  - Top과 유사

NAVER CLOUD PLATFORM

Ps 사용법

```
********* simple selection *********   ********* selection by list *********
-A all processes                        -C by command name
-N negate selection                     -G by real group ID (supports names)
-a all w/ tty except session leaders    -U by real user ID (supports names)
-d all except session leaders           -g by session OR by effective group name
-e all processes                        -p by process ID
                                        -q by process ID (unsorted & quick)
T   all processes on this terminal      -s processes in the sessions given
a   all w/ tty, including other users   -t by tty
g   OBSOLETE -- DO NOT USE              -u by effective user ID (supports names)
r   only running processes              U   processes for specified users
x   processes w/o controlling ttys      t   by tty
*********** output format **********   *********** long options ***********
-o,o user-defined   -f full             --Group --User --pid --cols --ppid
-j,j job control    s   signal          --group --user --sid --rows --info
-O,O preloaded -o   v   virtual memory  --cumulative --format --deselect
-l,l long           u   user-oriented   --sort --tty --forest --version
-F   extra full     X   registers       --heading --no-heading --context
                                        --quick-pid
                        ********* misc options *********
-V,V   show version         L   list format codes   f   ASCII art forest
-m,m,-L,-T,H   threads      S   children in sum     -y change -l format
-M,Z   security data        c   true command name   -c scheduling class
-w,w   wide output          n   numeric WCHAN,UID   -H process hierarchy
```

문제 해결을 위한 명령어들

- lsof
  - 현재 프로세스가 사용(오픈)하고 있는 파일 리스트 출력
  - 특정 프로세스가 CPU 점유율이 높을 경우 어떤 문제인지 확인하기 위해 사용

NAVER CLOUD PLATFORM

Lsof 사용법

```
Lsof [-?abhlnNoOPRtUvVX] [+|-c c] [+|-d s] [+D D] [+|-f[gG]] [+|-e s]
  [-F [f]] [-g [s]] [-i [i]] [+|-L [l]] [+m [m]] [+|-M] [-o [o]] [-p s]
[+|-r [t]] [-s [p:s]] [-S [t]] [-T [t]] [-u s] [+|-w] [-x [fl]] [--] [names]
```

-?|-h list help -a AND selections (OR) -b avoid kernel blocks

-c c cmd c ^c /c/[bix] +c w COMMAND width (9)

+d s dir s files -d s select by FD set +D D dir D tree *SLOW?*

+|-e s exempt s *RISKY* -i select IPv[46] files

-l list UID numbers -n no host names -N select NFS files

-o list file offset -O avoid overhead *RISKY* -P no port names

-R list paRent PID -s list file size -t terse listing

-T disable TCP/TPI info -U select Unix socket -v list version info

-V verbose search +|-w Warnings (+) -X skip TCP&UDP* files

-Z Z context [Z]

-- end option scan

```
+f|-f   +filesystem or -file names        +|-f[gG] flaGs

-F [f] select fields; -F? for help

+|-L [l] list (+) suppress (-) link counts < l (0 = all; default = 0)

                                          +m [m] use|create mount supplement

+|-M    portMap registration (-)          -o o    o 0t offset digits (8)

-p s    exclude(^)|select PIDs            -S [t] t second stat timeout (15)

-T qs TCP/TPI Q,St (s) info

-g [s] exclude(^)|select and print process group IDs

-i i    select by IPv[46] address: [46][proto][@host|addr][:svc_list|port_list]

+|-r [t[m<fmt>]] repeat every t seconds (15);   + until no files, - forever.

        An optional suffix to t is m<fmt>; m must separate t from <fmt> and

       <fmt> is an strftime(3) format for the marker line.

-s p:s   exclude(^)|select protocol (p = TCP|UDP) states by name(s).

-u s    exclude(^)|select login|UID set s

-x [fl] cross over +d|+D File systems or symbolic Links

names   select named files or files on named file systems
```

문제 해결을 위한 명령어들

- tcpdump
  - 트래픽 모니터링
  - 네이버 클라우드 플랫폼의 서버들의 경우 LB 로 연결된 구조의 경우 사용이 제한적
  - 일반적인 사용법
    - 호스트 관련
      - Tcpdump host
      - Tcpdump src
      - Tcpdump dst
      - Tcpdump net
    - 프로토콜 관련
      - Tcpdump port
      - Tcpdump src port
      - Tcpdump dst port

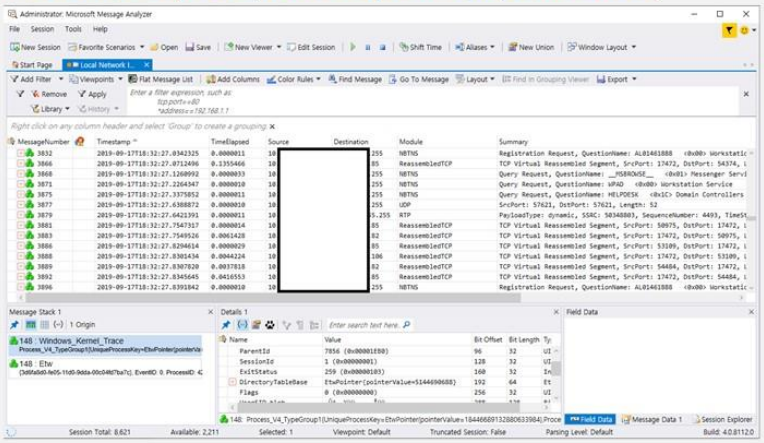
NAVER CLOUD PLATFORM

Tcpdump 사용법

```
tcpdump [-aAdDefIKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
        [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
        [ -i interface ] [ -M secret ] [ -r file ]
        [ -s snaplen ] [ -T type ] [ -w file ] [ -W filecount ]
        [ -y datalinktype ] [ -z command ] [ -Z user ]
        [ expression ]
```

문제 해결을 위한 명령어들

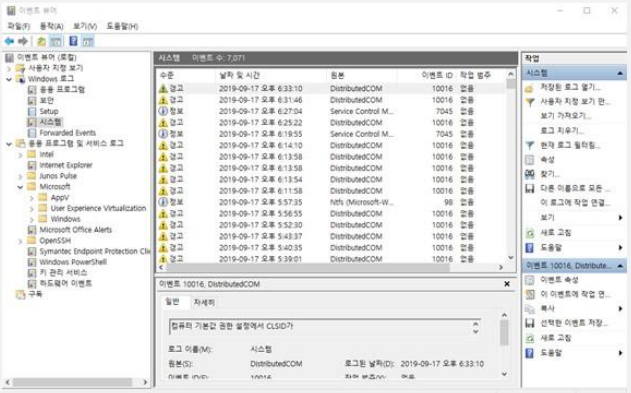
- Microsoft Message Analyzer
  - Netmon의 업그레이드 버전
  - https://www.microsoft.com/en-us/download/details.aspx?id=44226



NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- 이벤트 뷰어
  - Windows의 syslog
  - 주로 살펴봐야 하는 항목
    - Windows 로그 > 시스템
      - 시스템 Fault가 발생할 경우 이에 대한 로그 기록
    - Windows 로그 > 보안
      - 시스템 로그인 내역
    - Windows 로그 > 응용 프로그램
      - 응용 프로그램의 다양한 로그 기록
    - 응용 프로그램 및 서비스 로그
      - 응용 프로그램, 서비스에 대한 이벤트 로그 기록



NAVER CLOUD PLATFORM

Windows NT부터 사용되어진 이벤트 저장 및 뷰어

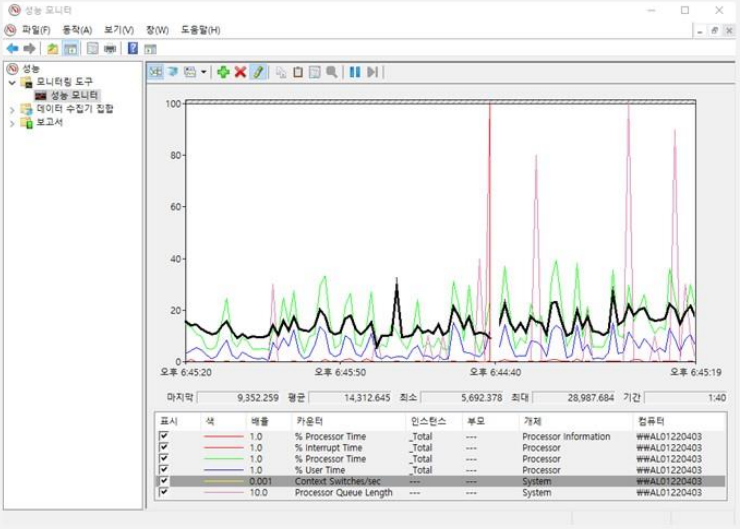
이벤트에 기록되는 내용들은 다음과 같다.

Property Name	Description
Source	The software that logged the event, which can be either a program name, such as "SQL Server", or a component of the system or of a large program, such as a driver name. For example, "Elnkii" indicates an EtherLink II driver.
Event ID	A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event Log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems.
Level	A classification of the event severity. The following event severity levels can occur in the system and application logs:
	Information. Indicates that a change in an application or component has occurred, such as an operation has successfully completed, a resource has been created, or a service started.
	Warning. Indicates that an issue has occurred that can impact service or result in a more serious problem if action is not taken.
	Error. Indicates that a problem has occurred, which might impact functionality that is external to the application or component that triggered the event.
	Critical. Indicates that a failure has occurred from which the application or component that triggered the event cannot automatically recover.

	The following event severity levels can occur in the security log:
	Success Audit. Indicates that the exercise of a user right has succeeded.
	Failure Audit. Indicates that the exercise of a user right has failed.
	In the Event Viewer normal list view, these are represented by a symbol.
User	The name of the user on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. Impersonation occurs when the server allows one process to take on the security attributes of another.
Operational Code	Contains a numeric value that identifies the activity or a point within an activity that the application was performing when it raised the event. For example, initialization or closing.
Log	The name of the log where the event was recorded.
Task Category	Used to represent a subcomponent or activity of the event publisher.
Keywords	A set of categories or tags that can be used to filter or search for events. Examples include "Network", "Security", or "Resource not found."
Computer	The name of the computer on which the event occurred. The computer name is typically the name of the local computer, but it might be the name of a computer that forwarded the event or it might be the name of the local computer before its name was changed.
Date and Time	The date and time that the event was logged.

문제 해결을 위한 명령어들

- 성능모니터
  - Windows 의 sar
  - Windows 시스템의 광범위한 리소스 모니터링
    - Processor
    - Process
    - Memory
    - System
    - Network Interface
    - Physical Disk / Logical Disk

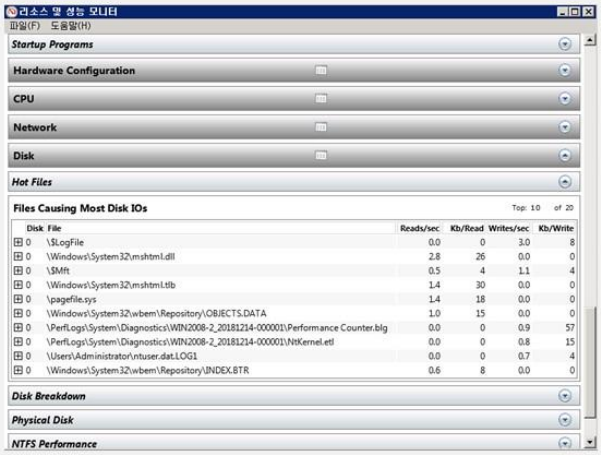


NAVER CLOUD PLATFORM

Windows 에서 제공되는 다양한 리소스 모니터링 뿐만 아니라 데이터 수집기 집합을 통해 원하는 항목에 대해 원하는 주기로 모니터링 데이터를 수집할 수 있다.

문제 해결을 위한 명령어들

- 리소스 및 성능모니터
  - Windows 시스템을 진단하고 보고서 작성

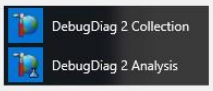


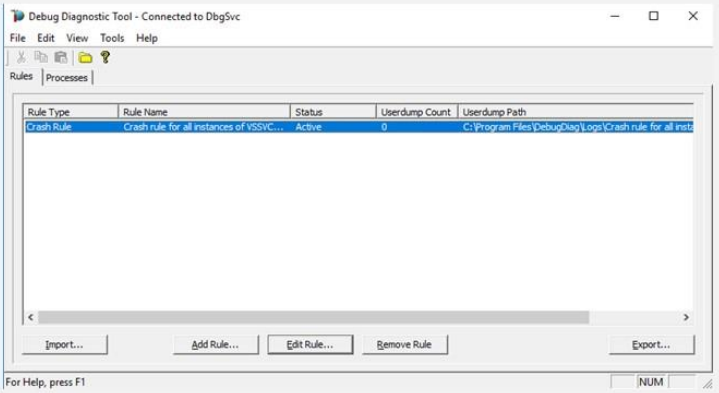
NAVER CLOUD PLATFORM

시스템에 대한 성능 지표를 진단하고 상세 보고서를 작성하여 어느 부분을 보완하여야 하는지 리포팅

문제 해결을 위한 명령어들

- Debug Diag
  - https://www.microsoft.com/en-us/download/confirmation.aspx?id=58210
  - Process의 Crash, Memory Leak 패턴을 확인하는 디버그 도구
  - Crash Dump에 대한 분석 도구

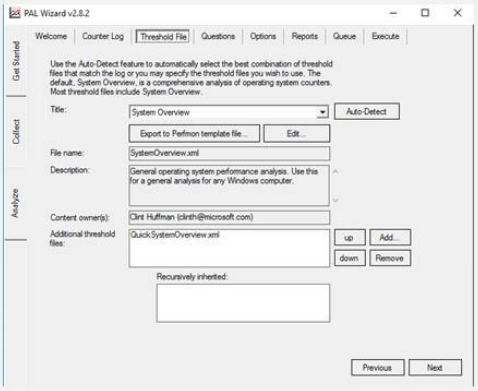




NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- PAL(*Performance Analysis of Logs (PAL) Tool)*
  - https://github.com/clinthuffman/PAL
  - 서버 타입 별 성능 카운터 오브젝트 제공
  - Threshold에 따른 성능 분석 리포트 제공



NAVER CLOUD PLATFORM

문제 해결을 위한 명령어들

- xPerf
  - Process의 Crash, Memory Leak 패턴을 확인하는 디버그 도구

NAVER CLOUD PLATFORM

문제 해결을 위한 Log

- Linux
  - 일반적인 시스템 로그
    - /var/log
  - HTTPD 로그
    - /var/log/httpd
- Windows
  - Eventvwr을 통한 로그 모니터링

NAVER CLOUD PLATFORM

Logrotate

- 시스템 연속성 보장을 위해 디스크 사용률 관리는 필수
  - 리눅스의 경우 / 파티션이 Full 이 되는 순간 서비스 정지
  - 디스크의 사용률을 높이는 요인
    - 로그
    - DB 데이터

- 로그에 대하여 정해진 처리 방식으로 삭제거나 파일을 바꿔주는 역할
  - 로그 파일을 바꿔줌으로써 시스템 성능을 높이는 역할 수행

NAVER CLOUD PLATFORM

/etc/logrotate.conf

로그로테이트 데몬의 기본적인 설정파일

/etc/logrotate.d/

로그로테이트로 처리할 다양한 데몬의 설정파일

커널 파라미터 변경

- Sysctl 명령어를 이용한 변경
  - Linux의 경우 커널 파라미터를 변경함으로써 성능을 변경할 수 있다.
- Sysctl.conf
  - 리눅스 커널 파라미터중 주요한 항목에 대한 설정
- Limits.conf
  - 사용자별 limit 설정
  - 프로세스, 오픈 파일 등이 sysctl.conf 파일과 함께 변경되어야 효과

NAVER CLOUD PLATFORM

CentOS 6.6 sysctl.conf

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
```

```
#net.ipv4.tcp_syncookies = 1

# Disable netfilter on bridges.
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0

# Controls the default maxmimum size of a mesage queue
kernel.msgmnb = 65536

# Controls the maximum size of a message, in bytes
kernel.msgmax = 65536

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 68719476736

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 4294967296
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.log_martians = 1
xen.independent_wallclock = 1
# Auto-enabled by xs-tools:install.sh
net.ipv4.conf.all.arp_notify = 1
```

Limits.conf

```
#*              soft    core        0
#*              hard    rss         10000
#@student        hard    nproc       20
#@faculty        soft    nproc       20
#@faculty        hard    nproc       50
#ftp             hard    nproc       0
#@student        -       maxlogins   4
```

주목하여야 하는 항목들

file-max 설정
fs.file-max

net.ipv4.tcp_rmem

net.ipv4.tcp_wmem

connection track max 설정
net.netfilter.nf_conntrack_max
net.ipv4.ip_local_port_range

network packet queue 설정
net.core.netdev_max_backlog
net.core.somaxconn
net.ipv4.tcp_max_syn_backlog

file limit max 설정 (root 계정)
root - nofile 999999

커널 파라미터 변경

- 파일 확인
  - 오픈할 수 있는 파일 개수 확인 cat /proc/sys/fs/file-nr
  - 변경
    - /etc/sysctl.conf
    - fs.file-max = 819200

- TCP 타임 아웃
  - 확인 sysctl -a | grep keep
  - net.ipv4.tcp_keepalive_time = 3600

- Limits.conf
  - 사용자별 limit 설정
  - 프로세스, 오픈 파일 등이 sysctl.conf 파일과 함께 변경되어야 효과

NAVER CLOUD PLATFORM

Workshop