

## 베스트 질문 [가상화 클라우드]

Q1. 관리를 위해 잠시 컴퓨터를 끄고 새벽시간에 점검을 한다든가 하는 작업이 AWS에서도 일어나나요? (AWS를 사용하는 서비스가 도중에 사용불가한 상태가 일어날 수도 있는 건가요?)

답변:AWS에서도 점검과 관리를 위해 물리적인 서버를 종료하긴 하지만, 종료하기 전에 먼저 고객의 서버를 다른 물리적인 서버로 이전하고(설정이 변경되지 않는 선에서)진행할 것입니다. 따라서 AWS의 관리를 위해 고객의 서버를 끄는 행위는 일어나지 않습니다. 보통 AWS의 문제로 서비스가 내려가지는 않고 이를 사용하는 고객이 설정을 잘못된 경우라고 봐야 할 것입니다.

Q2. 모든 용량을 무료로 제공해주는 것이 아닌 제한적으로 지원을 해주는 것이라고 알게 되었습니다. 예를 들어 '카페, 블로그'같은 경우는 웹 서버 형태로 지원해주는 것인데 어느정도 사용 용량이 정해져 있지 않을 까요? 사용자가 1G미만이 영상이나 이미지를 매일 같이 수십, 수백 개를 업로드하게 되어도 문제가 되지 않나요?

답변:퍼블릭 클라우드 대표적으로 AWS의 경우에는 사용용량을 퍼블리셔(웹서버를 배포하는 사람)가 사용하고 싶은 컴퓨터의 성능이나 용량 등을 직접 설정하고 프라이빗 클라우드의 경우에는 기업의 자원 크기 또는 기업에서 정해진 자원만큼만 사용할 수 있도록 되어있습니다. 수십 수백개를 업로드 해도 문제가 되지 않도록 서버를 구성할 수도 있고 제한할 수도 있습니다. 기업이 돈을 더 내고 더 큰 용량을 빌릴 용량이 있다면 예시에서 수십 수백개를 업로드 해도 괜찮도록 서버를 구성할 것이고 기업이 그 만큼의 자본을 가지고 있지 않다면 수십 수백개를 올리지 못하도록 할 것입니다. 그것을 클라우드 서비스에 퍼블리싱 하는 웹 퍼블리셔가 설정합니다.

Q3. 내부 IP도 같이 지정해줘서 들어가야 한다고 설명하셨던거 같은데 service 설명부분에서 포트 IP가 변경되었을 때 제대로 연결이 안되었을 때 그것을 해결하는 것이라고 들었는데 제가 이해를 잘 못해서 자꾸 헷갈립니다. 외부에서 특정 노드 포트로 접속하면 그거에 맞게 나누어 준다고 보면 되는 건가요?

답변:Service 유형 중 Nodeport에 대해서 질문을 주셨는데요  
외부에서 노드 IP의 Port로 접속을 하면 서비스와 연결되어 있는 Pod에 접근할 수 있습니다. 즉, Nodeport를 비롯한 Service는 연결된 Pod에 L4 로드밸런싱 역할을 해주는 것이지요  
NodePort를 사용하는 경우 (포트 IP가 변경되었을 때 제대로 연결이 안되었을 때 그것을 해결한다는 것)은 연결을 하려면 주소를 알아야 연결을 할 수 있는데, Pod의 주소인 IP는 Pod가 재배포 되면 변경이 됩니다. 따라서 IP는 연결성이 끊어질 위험이 있습니다.  
Service를 사용하면, Pod의 IP로 접근하는 것이 아닌 Service로의 접근을 통해 Pod로 연결을 할 수 있는 것입니다. (포트 포워딩 설정, Selector : app=test와 Label : app=test가 동일해야 Pod와 Service가 연결)

Q4. api와 워크노드 큐블렛등의 역할은 이해했는데 k-proxy는 무엇인가요?

큐블렛을 작업반장과 같이 비유한 것처럼 비유하자면 어떤 역할로 들어가나요?

답변:AWS 클라우드를 배우시면서 VPC에 대해서도 학습을 하셨을 겁니다.  
kube-proxy는 vpc와 같이 네트워크 동작을 관리하는 구성요소라고 보시면 됩니다.  
작업반장들끼리 통신할 수 있는 핸드폰이 될 수도 있고 봉화 정도가 될 수도 있겠죠  
즉 노드들의 통신을 담당한다고 보시면 됩니다.

Q5. 각각의 서브넷을 가지는 가용영역이 여러개가 되도록 하는게 가용성이랑 관련이 있는 것으로 이해했는데 이게 맞을까요?

답변:네. 맞습니다.  
설명:여러 가용영역을 사용하면 가용성이 높아지게 됩니다. 가용영역은 사용하는 리소스의 물리적인 장소입니다. 서로 다른 가용영역은 각각 물리적으로 분리되어 있어 개별 가용영역의 물리적 장애는 다른 가용영역에 영향을 주지 않기 때문에 서로 다른 가용영역을 사용하면 가용성이 높아진다고 할 수 있습니다.

Q6. vpc, 가용범위와 서브넷 관련하여 질문 드립니다. vpc는 결국 회사의 개인적인 네트워크(다른 외부인의 접속을 제어하는)인 것이고, 서브넷은 다른 부서가 들어오지 못하게 접속을 제어하는 것이죠? 그렇다면 가용범위 하나 당 서브넷은 하나인 건가요? 아니면 그 이상이 될 수 있는 것인가요?

답변:VPC는 구성에 따라 개인적인 네트워크로 볼 수 있으나, 서브넷은 다른 부서가 들어오지 못하게 접속을 제어하는 것이 아니라 개인적인 네트워크(VPC) 내부에 구성하는 서브 네트워크이며 말씀하신 다른 부서가 들어오지 못하게 접속 제어를 위해서는 보안그룹이나 NACL로 구현 가능합니다.  
설명:간단하게 질문과 관련한 용어를 살펴보면 VPC는 AWS 내부에 만드는 개인적인 네트워크 환경, 서브넷은 VPC 내부에 만들어지는 세부 네트워크, 가용영역은 서브넷(가상네트워크)이 배치되는 물리적인 위치, 보안그룹은 다른 네트워크에서 들어오거나 나가는 트래픽 관리를 하기위한 제어수단 정도로 정리할 수 있습니다.

Q7. 0.0.0.0은 모든 ip라는 의미인가요?

답변:네. 맞습니다.  
설명:정확하게는 특정하지 않은 임의의 주소 즉 모든 주소라는 의미입니다. 0.0.0.0은 위 의미와 더불어 라우팅 테이블에서 대상 주소에 사용 가능한 특정 경로가 없을 때 사용되는 기본 경로로 사용되기도 하고, 노드의 모든 Local address를 의미하기도 합니다. 각 상황에 따라 여러가지 의미가 있다는 것을 참고하여 각 의미를 구분하여 사용해야 할 것입니다.

Q8. layer 4는 transport 계층인데 왜 TLB(Transport LoadBalancer)라 하지 않고 NLB(Network LoadBalancer)라고 하나요?

답변:NLB(Network LoadBalancer)는 AWS에서 정한 서비스 명칭입니다.

설명:처음 Load Balancer를 만들 때 Network의 부하를 분산하기 위한 목적으로 만들었기 때문에 Network 라는 용어를 사용할 뿐 OSI 3계층의 Network계층을 의미하는 것은 아닙니다.

또한 NLB, ALB 등의 서비스 명칭은 클라우드 서비스 사업자가 선정하는 내용이기에 사업자에 따라 달라 질 수 있습니다.

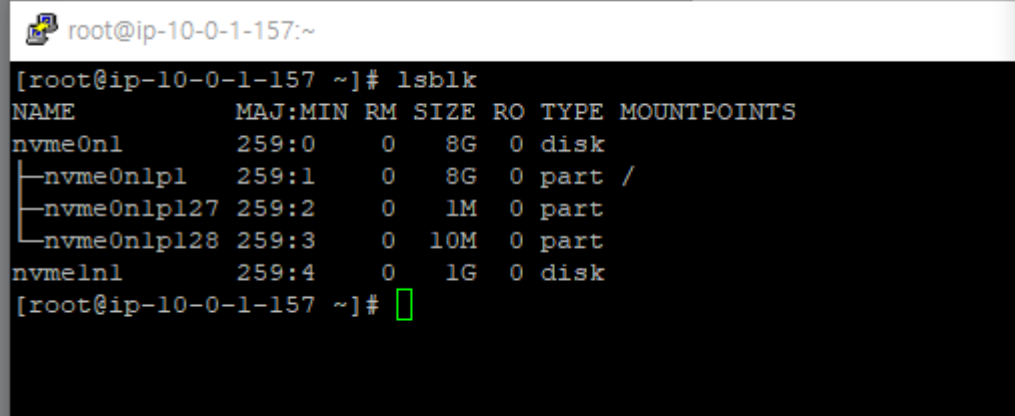
로드밸런서의 경우 네트워크 로드밸런서, 어플리케이션 로드밸런서라는 표현도 사용되지만 L4, L7 로드밸런서라는 표현으로 구분하는 경우도 많습니다.

Q9. 데이터 주고받을 때 로드밸런서가 없어도 목적지 사설IP에 데이터가 잘 도착할텐데 왜 굳이 로드밸런서를 사용해서 트래픽 처리를 하나요?

답변:로드밸런서를 사용해 트래픽을 처리하는 이유는 부하분산과 타겟그룹 내 개별 서버장애에도 외부서비스를 유지하기 위한 가용성 증가를 위하여 사용합니다.

설명:가용성은 실제 서비스중인 환경에서 필수적으로 고려되는 사항으로 로드밸런서라는 구성요소는 기본 구성요소로 보셔도 무방합니다. 위 목적 이외에도 외부 요청에 따라 적절한 서버로 전달하기위한 유사 라우팅 환경 구성 등의 목적으로도 사용합니다.

Q10. AWS 실습 Lab 3번에서, 여기서 강의 자료에 나온 것처럼 lsblk을 실행하면 xvdf란 디스크가 없어서 이 이후로 실습을 진행하지 못 하고 있습니다, 어떻게 진행해야 하나요?



```
root@ip-10-0-1-157:~  
[root@ip-10-0-1-157 ~]# lsblk  
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS  
nvme0n1              259:0    0   8G  0 disk  
├─nvme0n1p1          259:1    0   8G  0 part /  
├─nvme0n1p127        259:2    0  1M  0 part  
└─nvme0n1p128        259:3    0 10M  0 part  
nvme1n1              259:4    0  1G  0 disk  
[root@ip-10-0-1-157 ~]#
```

답변:저장공간이 nvme로 되어있어서 코드를 조금 수정해야 할 것 같네요.

sudo -i

lsblk

mkfs -t xfs /dev/nvme1n1

mkdir /data

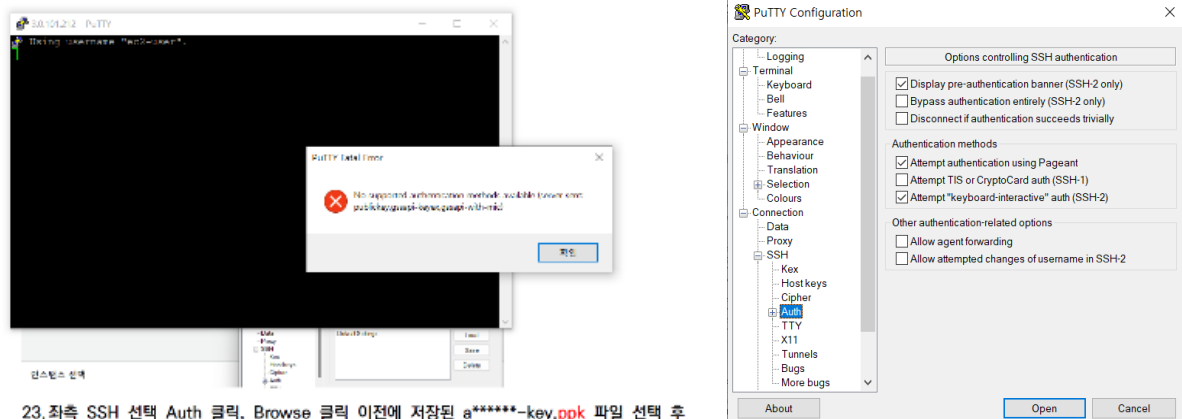
mount /dev/nvme1n1 /data

df -h

로 nvme로 볼륨 마운트 진행해주시면 되겠습니다.

설명:인스턴스 세대가 달라서 발생하는 문제, xvdf 대신 nvme1n1로 코드를 수정해야 됩니다.

Q11. AWS 실습 Lab 2의 23번에서 browse버튼이 없어서 키파일 선택하지 못하고 그냥 open했습니다. 그랬더니 알림창 뜨면서 accept가 있었는데 강사님이 그냥 accept하셔도 된다고 하셔서 눌렀더니 에러경고창이 뜹니다. 확인 눌렀는데 26번 계속 진행해도 되는 건가요?

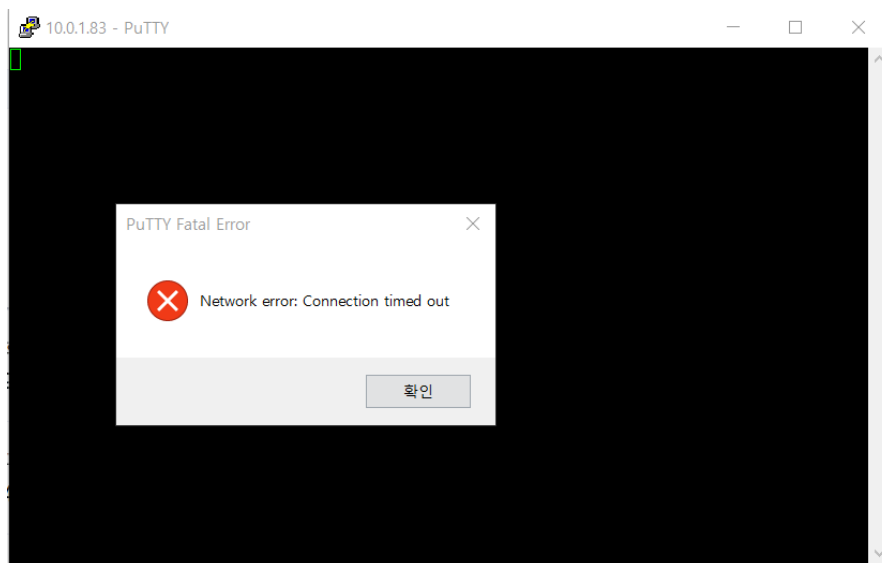


23. 좌측 SSH 선택 Auth 클릭, Browse 클릭 이전에 저장된 a\*\*\*\*\*-key.ppk 파일 선택 후

답변:PuTTY -> connection -> SSH -> Auth -> Credentials 에 private key file for authentication에 아까 저장하신 a\*\*\*-key.ppk를 불러오시면 됩니다.

설명:PuTTY 버전이 달라서 발생하는 문제, Credentials 경로가 더 추가됨, 키파일이 무조건 있어야 open이 됩니다.

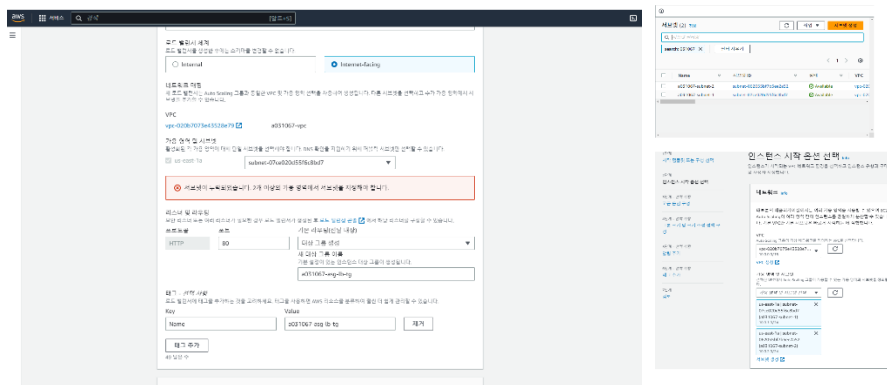
Q12. AWS 실습 Lab 2에서 .ppk를 첨부하고 open을 눌렀는데 putty창이 뜬 후 아무런 글자가 타이핑이 안되고 time out이 나옵니다. 어떻게 진행해야 하나요?



답변:IP가 제대로 설정되지 않는 등의 이유로 응답이 없을 때 time out 에러가 발생합니다. 이전 과정에서 EIP로 설정하신 IP로 접속 시도한 게 맞는 지 다시 확인해 보시기 바랍니다.

설명:인스턴스 생성시 허용된 My IP가 다르거나 설정이 되지 않았을 때, PuTTY로 접근할 시 발생하는 문제, 인스턴스 보안 그룹 설정을 다시 해야 됩니다.

**Q13. AWS 실습 Lab 5에서 Auto Scaling 구성에 대한 답변으로 subnet 을 2개 생성해줘야 한다고 하셨는데 이미 2개가 생성되어 있고 auto scaling 13번에서도 서브넷 2개를 모두 선택하였습니다. 이런 경우 어떤 점이 문제일까요?**



답변:현재 두subnet의 가용영역이 같아서 그렇습니다. 두subnet 가용영역을 다르게 생성해주세요.

설명:Auto Scaling을 구성할 때 AZ가 같은 두 subnet에 구성하는게 아니라, 서로 다른 AZ의 두 서브넷으로 구성해야 됩니다.

**Q14. K8s 실습 Lab 2-13번 Cloud9에서 아래 +버튼을 클릭, 터미널을 추가하여 Worker 1 에 접속**  
**에서 저의 맞는 worker 1 ip를 입력 하고 실행했는데 time out이 됩니다, 어떻게 진행해야 하나**  
**요?**

답변:콘솔에서 마스터 노드의 인스턴스 시작했던 것처럼, 나머지 두 개의 워커 노드도 ip로 검색해서 시작하셔야 됩니다. 그 후 다시 진행하시면 됩니다.

설명:마스터 노드에서 워커 노드로 접속하는 것이 아니라, 마스터 노드 1개, 워커 노드 2개를 각각 C9 환경에서 접속해야 합니다.

**Q15. AWS에서 네트워크를 구성할 때, 서브네팅을 하는 이유가 무엇인가요?**

답변:AWS 에서의 서브네팅이란 IP 블록을 더 작은 그룹으로 분할하는 것을 말합니다. 이렇게 서브넷을 나누는 이유는 용도별로 네트워크의 관리적인 측면도 있지만 가장 큰 이유는 보안의 이슈 때문 입니다.

서브네팅을 통해서 VPC 안에서도 외부에서 접근가능한 Public subnet, 외부에서 접근이 불가능한 Private subnet 으로 구분할 수가 있게 되는 것입니다.

설명:참고로 일반적인 네트워크에서의 서브네팅과 AWS의 서브넳 생성 개념은 다릅니다. 일반적인 네트워크의 서브넳이란, IP주소 낭비를 방지하기 위해 네트워크를 분할하여 효율적으로 사용하는 개념입니다.

**Q16. AWS의 ALB(Application Load Balancer)와 NLB(Network Load Balancer)의 역할을 정확히 이해 못했는데 차이점이 무엇인가요?**

답변:ALB 는 OSI 7 계층에서 L7 영역 즉, HTTP/HTTPS 에서의 부하를 분산시켜 주는 LB 이고, NLB 는 L4, TCP/IP 에서 부하를 분산 시켜주는 LB 입니다. 그리고 성능 비교를 하자면 NLB 가 ALB 보다 지연속도가 더 짧은 대신 부하 분산 시 IP 주소의 변경이 없습니다.

설명:ALB 와 NLB 의 차이점은 프로토콜에 있습니다. ALB 는 TCP, UDP 프로토콜을 지원하며, NLB 는 HTTP(S) 프로토콜을 지원합니다. 그렇기 때문에, NLB 는 VPC 와 같은 Private 한 네트워크 환경에서 사용되며, ALB 는 HTTP 통신이 이루어지는 Public 환경에서 동작합니다.

**Q17. 쿠버네티스 클러스터 설정 명령어 입력 시 Join 명령어 대신 Port in use 라는 오류가 발생하는데 어떻게 해결해야하나요?**

답변:[ERROR Port-6443]: Port 6443 is in use

[ERROR Port-10259]: Port 10259 is in use

[ERROR Port-10257]: Port 10257 is in use

이 에러를 보시면, 현재 커넥션을 걸려고 하는 포트의 일부분이 사용 중이어서 다음 과정을 진행하지 못해 뜨는 에러로 보입니다. 이런 경우 두 가지를 시도해볼 수 있을 것 같습니다.

1) 해당환경에서 kubeadm reset 명령어를 진행해보세요.

2) AWS 홈페이지에 Cloud9 환경 대쉬보드에서 생성하신 Cloud9 인스턴스의 이름을 클릭하신 뒤, 오른쪽 아래에 EC2 인스턴스 관리로 갑니다. 이 때 해당 Cloud9 인스턴스와 연동된 EC2 인스턴스로 가는데, 이 인스턴스를 재가동해주세요.

설명: 쿠버네티스 환경을 구축할 때, 오타나 실수로 인해 발생한 에러는 kubeadm reset 명령어로 클러스터를 초기화 해준 뒤, Cloud9 인스턴스도 재부팅하고 다시 세팅하면 됩니다. (본 과정 진행하면서 채팅창, 1:1 문의 게시판, 공유 시트 합쳐 10 번 이상은 본 질문입니다.)

**Q18. 쿠버네티스에서 하나의 YAML 파일로 default Namespace만 있는 상태에서 새 Namespace 와 그 안에 pod를 한번에 만드는 방법은 없나요?**

답변:YAML 파일안에 "---" 로 구분해서 한 파일안에 여러 오브젝트를 생성하게 세팅할 수 있습니다.

설명:두개의 쿠버네티스 리소스를 만드는 YAML 파일을 하나로 합칠 수 있습니다.