KOREAN STUDENT VERSION

Beginning Kubernetes

Byungwook Hyeon
&
Dongwan Kang

Begining Kubernetes

“Begining Kubernetes” is for kubernetes beginers who want to leran using korean, not a expert. We hope that this book will be a ESSENTIAL for kubernetes beginners.

Byungwook Hyeon & Dongwan Kang

About the Authors.

현병욱 Byungwook Hyeon

- 소속 : 한양대학교 ERICA 소프트웨어융합대학 소프트웨어학부
- 이력 :

2007. 03 ~ 2007. 11 : 홍콩 어학연수
2009. 03 ~ 2012. 02 : 창동고등학교 졸업
2014. 03 ~ 2019. 02 : 청주대학교 컴퓨터정보공학과 학사(중퇴)
2016. 02 ~ 2017. 10 : 705 특공연대 특공병, 병장 만기 전역
2019. 03 ~ 2021. 02 : 한양대학교 ERICA 소프트웨어학부 학사
2019. 03 ~ 2019. 06 : (주)대양엔바이오 컨설팅
2019. 09 ~ 2020. 06 : 클라우드 네이티브 컴퓨팅 플랫폼 개발 With KTds
2020. 08 ~ 2020. 12 : 최강학원 수학 강사
2020. 09 ~ 2020. 12 : AWS기반 호텔정보시스템(PMS) 개발, Agora
2020. 10~ 2020. 12 : 대한민국 증권시장에서 거래되는 주식에 대한 R기반 리스크 측도 및 평균 수익률 분석
2020. 11 ~ 2020. 12 : 콜옵션 소유자와 발행자 각각의 거래일에 대한 R기반 현금 흐름과 만기 수익 분석

- 자격 :

Microsoft - Azure Fundamental : AZ-900
Linux Foundation - Certified Kubernetes Administrator : CKA

About the Authors.

강동완 Dongwan Kang

- 소속 : 한양대학교 ERICA 소프트웨어융합대학 소프트웨어학부
- 이력 :

2007. 03 ~ 2010. 02 : 광성고등학교 졸업
2010. 03 ~ 2014. 02 : 유한대학교 컴퓨터소프트웨어공학과 전문학사
2011. 02 ~ 2012. 10 : 3사단 직할 전차대대, 병장 만기 전역
2013. 03 ~ 2017. 01 : 웹플러스 근무, 대리
2019. 03 ~ 2021. 02 : 한양대학교 ERICA 소프트웨어학부 학사
2019. 09 ~ 2020. 06 : 클라우드 네이티브 컴퓨팅 플랫폼 개발 With KTds
2019. 10 ~ 2020. 07 : GS25 안산신안점 근무
2020. 09 ~ 2020. 12 : AWS기반 호텔정보시스템(PMS) 개발, Agora

- 자격 :

Microsoft - Azure Fundamental : AZ-900
대한민국 한국산업인력공단 - 정보처리 산업기사

Table of Contents

시작하면서..

저자인 현병욱과 강동완은 클라우드 엔지니어로의 진출을 준비중인 한양대학교 ERICA 소프트웨어학부 학생입니다. 현병욱과 강동완은 KTds Architecture CoE팀과 클라우드 네이티브 컴퓨팅 플랫폼 개발을 주제로 프로젝트를 수행하여 종합 플랫폼인 Agora를 개발했습니다. 또한, 현병욱은 LInux Foundation과 CNCF사의 kubernetes 운용 능력 검증 시험인 'Certified Kubernetes Administrator : CKA'를 취득했습니다.

'Beginning Kubernetes'는 저자가 프로젝트 수행과 자격 취득 준비 과정에서 경험한 어려웠던 점들을 쉽게 설명하여 입문자들이 쉽게 kubernetes에 접근할 수 있도록 하기위해 집필하게 되었습니다. 이 과정을 통해 kubernetes 오픈 소스 프로젝트가 활성화되길 바랍니다.

저자 현병욱

저자 강동완

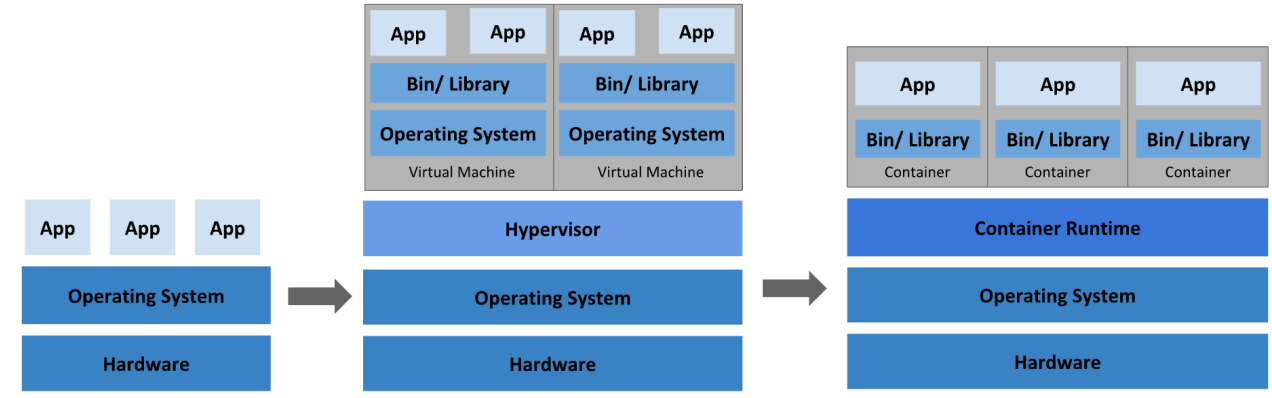
Chapter 1.

Kubernetes 소개

Kubernetes란?

Kubernetes는 컨테이너화된 애플리케이션의 자동 디플로이, 스케일링 등을 제공하는 오픈 소스 기반의 관리 시스템이다. 시스템의 초기 버전은 Google에 의해서 개발되어 2014년 중순에 공개되었다. 프로젝트 당시 kubernetes는 “프로젝트 세븐”으로 시작하였으나, 그리스어로 키잡이(helmsman)를 뜻하는 kubernetes로 2015년 7월 21일에 v1.0이 정식 출시되었다. 현재는 Linux Foundation에서 서비스를 주관하고 있다.

Why Kubernetes?



초창기 대부분의 애플리케이션은 기본적인 시스템의 물리 서버에서 서비스되었다. 그러나 여러개의 애플리케이션을 구동하고자 한다면 그에 상응하는 수의 물리 서버가 필요하다는 한계가 존재했는데, 이는 서비스 측면에 있어서 어플리케이션의 성능을 저하시킬 수 있다는 치명적인 단점으로 작용했다.

이를 해결하기 위해 VirtualBox, VMware와 같은 가상화 환경이 등장하게 된다. 가상환경은 기존의 단일 물리 서버의 CPU에서 다중으로 실행이 가능하도록하여 애플리케이션의 각 리소스들을 격리하여 성능 저하를 방지할 수 있다. 또한, 격리된 리소스는 서로간의 접근에 있어서 자율성을 제한하여 보안 측면까지 해결이 가능했다. 가상화의 등장은 기존에 요구된 많은 수의 물리 서버의 필요성을 감소시킴으로써 하드웨어 비용의 절감을 효과를 기대할 수 있다. 이는 동적 확장에 자율성을 보장해줄 수 있음은 물론이거니와, 기존 각 물리 서버에서 요구하는 독립적 운영체제의 도입에서 발생하는 비용을 감축킬 수 있기에 다수의 기업들이 가상환경을 도입하기 시작했다.

가상 환경의 도입으로 기존 물리 서버의 시대보다 효율적인 애플리케이션 운용이 가능해졌지만, 가상 환경에도 단점이 존재했다. 바로 리소스간의 접근 제한으로인한 개발 복잡성의 증가이다. 개발 단계에서 가상 환경내의 독립적인 리소스간는 정보를 주고받는 통신에 제약사항을 유발하여 개발 단계를 지연시키는 경우가 발생한 것이다. 이를 해결하기위해 등장하게 된 것이 바로 '컨테이너'기술이다. 컨테이너는 VM과 유사하지만 리소스간의 통신 제약사항을 완화하여 애플리케이션 간의 리소스 공유가 가능하도록 구상되었다. 또한, 컨테이너의 가장 큰 장점은 기존의 로우 레벨의 인프라와의 연결 고리가 끊어짐에따라 클라우드나 기타 다른 운영체제로의 이식이 가능해졌다는 점이다.

입문서의 메인 주제인 kubernetes는 컨테이너를 쉽게 관리할 수 있도록 고안된 플랫폼이다. Kubernetes는 분산 시스템에 대한 접근성 강화와 운영 단계를 단축시킬 수 있는 프레임 워크를 제공한다. 이를 통해 Kubernetes는 컨테이너에 대해 애플리케이션의 배포, 확장, 장애 조치, 모니터링, 스케쥴링 등을 신속하고 편리하게 처리할 수 있다. 결론적으로 Kubernetes는 컨테이너 시대를 총괄하는 플랫폼인 것이다.

Kubernetes 운용 능력 확보는 4차 산업혁명 흐름에 맞춰 변화중인 애플리케이션 개발 환경에 필수 역량으로 자리잡게 될 것이다.

Kubernetes 구성 요소

Kubernetes 운용 능력을 향상시키기 이전에 기본적으로 알아야 할 Kubernetes의 구성 요소는 다음과 같다.

1. 노드 (Node)

도커와 같은 패키징 프로그램을 통해 컨테이너화된 애플리케이션을 실행하는 단위이다.

2. 파드 (POD)

파드는 kubernetes에서 생성할 수 있는 가장 작은 단위의 오브젝트로, 애플리케이션의 작은 Instance 이다.

3. 클러스터 (Cluster)

클러스터는 컨테이너화된 애플리케이션을 실행하는 노드의 집합니다.

4. Kube-apiserver

Kube-apiserver는 kubernetes를 전반적으로 관리하는 메인 server이다. kuber-apiserver를 통해 클러스터 안의 모든 동작의 오케스트레이션을 관리할 수 있다.

5. Kubelet

Kubelet은 kube-apiserver로부터 커맨드를 받아 현재 컨테이너, 노드, 파드 등에 대한 정보를 받거나 노드에 컨테이너를 배포 혹은 삭제하는 기능을 수행한다.

6. Kube-proxy

Kube-proxy는 서비스와 클러스터 사이의 통신을 보조한다.

7. Kube-scheduler

Kube-scheduler는 현재 필요한 컨테이너를 가져오는 작업을 수행한다.

8. ETCD

ETCD는 reliable한 key-value를 간단하게 저장하여 보관할 수 있는 기능을 수행한다. 또한, 현재 클러스터에 존재하는 컨테이너, 파드, 노드 등에 대한 정보를 일괄적으로 백업하여 보관할 수 있다.

9. Replication-controller

Replication-controller는 노드를 새로운 클러스터에 가져오거나, 사용 불가 상태의 노드를 삭제할 수 있는 작업을 수행한다.

이 이외에도 kubernetes를 구성하고있는 수많은 요소들이 존재하지만, 다음 9가지는 kubernetes를 운용하는데 있어서 가장 기본적으로 숙지하고 있어야 할 구성 요소이다. 자세한 설명은 다음 장에서 진행하도록 한다.

Chapter 2.
Kubernetes 컨셉

✔ kube-apiserver

kubectl은 kube-apiserver에 접근한다.

api server가 노드에 접근하지 않고 POD를 생성하는 방법
1. ETCD server에 이미 생성되어진 POD를 업데이트한다.
2. 스케쥴러는 지속적으로 API server를 모니터링해서 새로운 POD가 노드에 생김을 인지한다.
3. API server는 2에서 받은 정보를 토대로 ETCD 클러스터를 업데이트한다.
4. 3에서의 업데이트 정보를 토대로 Node의 Kubelet에 정보를 전달한다.
5. kubelet은 API server로 정보를 업데이트해준다.
6. API Server는 ETCD 클러스터에 정보를 업데이트한다.
7. 클러스터의 모든 정보는 API server가 중심이 된다.

즉, Kube-api server의 역할
1. Authenticate User
2. Validate Request
3. Retrieve data
4. Update ETCD
5. Scheduler
6. Kubelet

※ Kube-api server는 ETCD Datastore와 직접적으로 상호작용하는 유일한 요소이다.
※ Kubelet, Kube-controller-manager, Scheduler는 kube-api server를 통해 클러스터 정보를 업데이트할 수 있다.

· 존재하는 클러스터의 kube-api server options 보는 방법
kubectl get pods -n kube-system

· kubeadm tool로 설정하면 kubeadm이 kube-api server를 pod로써 master node의 kubesystem name에 deploy한다.

· Pod definition file과 관련된 options를 보는 방법
cat /etc/kubernetes/manifests/kube-apiserver.yaml

· runnig process와 effective options의 list 보는 방법
ps -aux | grep kube-apiserver

✔Kube Controller manager

Node-controller는 kube-api server를 통해 정보를 받는다.

replication-controller는 레플리카 셋의 상태를 모니터링하고 필요한 수의 PODS를 셋에서 필요한 만큼 사용 가능하게 해준다. -> pods가 죽으면 다른 하나를 생성한다.

Kube Controller Manager에 Node-Controller, Replication-Controller, Deployments-Controller 등의 k8s에 존재하는 모든 Controller가 포함되어 있으므로, 따로 설치 할 필요 없이 Kube Controller Manager만 설치하면 일괄적으로 설치된다.

· Kube-Controller-Manager 설치 방법
wget https://storage.googleleapis.com/kubernetes-release/release/v1.13.0/bin/linux/amd64/kube-controller-manager

※ 설치 후 중요한 값 :
—node-monitor-periods=5s
-node-monitor-grace-periods=40s
-pod-eviction-timeout=5m0s

· Kube-Controller-Manager server Options 보는 법
7. Kubeadm tool 쓰는 경우
kubeadm이 kube-controller-manager를 Master Node의 kube-system namespace에 Pod로 Deployments한다.

cat /etc/kubernetes/manifests/kube-controller-manager.yaml

✔ Kube Scheduler
Kube Scheduler는 오직 어떤 Pod가 어떤 Node로 갈지를 정한다.

단, Node의 Pod로 이동시키지는 않는다. → Kubelet 역할

※ Nodes가 Pods에 필요한 충분한 CPU와 Memory를 갖고 있지 않다면 처음 두개의 작은 Nodes가 filtered out된다.

· Kube-Scheduler 설치 방법
wget https://storage.googleapis.com/kubernetes-release/release/v1.13.0/bin/linux/amd64/kube-scheduler

· Kube-scheduler server options 보는 방법
8. Kubeadm tool로 설정한 경우
kubeadm은 kube-scheduler를 Master Node의 Kube-system namespace에 Pod로 deploy한다.

cat /etc/kubernetes/manifests/kube-scheduler.yaml

✔ Kubelet
Kubelet은 배의 선장과 같다.
Kubelet은 컨테이너를 올릴지 말지를 결정하고 컨테이너의 상태를 체크한다.

· k8s의 Worker Node의 Kubelet은 k8s cluster에 Node를 등록한다.

· Container나 Node의 Pod를 불르라는 명령을 받게되면 Container run time engine인 Docker에 명령받은 image를 불러오라고 요청하고 불러와서 그 instance를 실행시킨다. 이후, Kubelet은 pods와 containers에 대한 지속적인 모니터링을 하고 그 결과를 kube-api server에 시간에 따라 정보를 전달한다.

· Kubelet 설치 방법
wget https://storage.googleapis.com/kubernetes-release/release/v1.13.0/bin/linux/amd64/kubelet

cluster에 deploy하기위해 kubeadm tool을 통해서 kubelet을 설치하면 자동적으로 kubelet을 deploy하는 것이 아니다. 이것이 다른 설치 요소들과의 차이점이다.
worker nodes에 수동으로 설치해줘야한다.

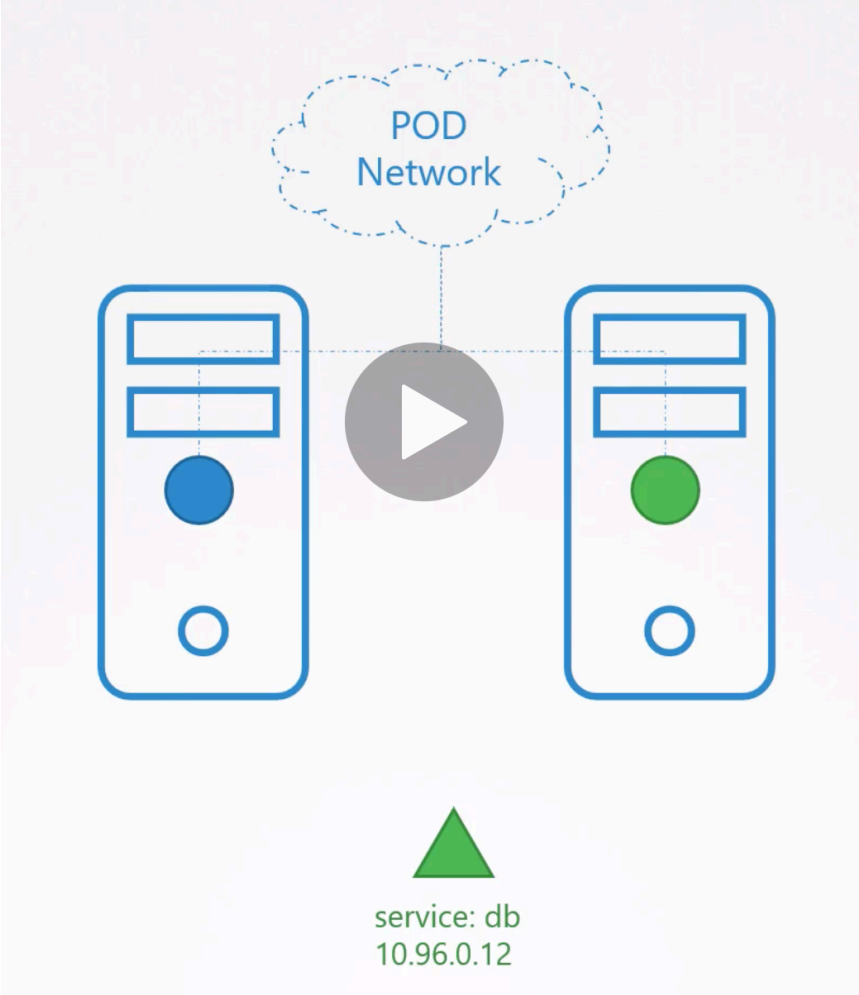
✔ Kube-proxy
k8s의 cluster는 모든 pods가 서로 다른 pods에 접근할 수 있도록 해준다.
이는 POD networking solution을 cluster에 deploy해줌으로써 가능하다.

※ 예제
상황 : Node1에 Web Application이 deploy되있고, Node2에 database application이 deploy 되어있다.

Web app은 database Pod의 IP를 통해 database에 접근할 수 있다.
하지만, database Pod의 IP가 항상 같은 상태로 남아있다고는 보장이 되지 않는다.

따라서, Web app이 database에 접근하고자 할 때의 최고의 방법은 service를 사용하는 것이다.

database application을 노출시키기 위해 cluster 밖에 Service: db를 생성한다.
이렇게 되면 web application은 service db를 통해 database에 접근할 수 있게 된다.



Service: db는 Pod가 service에 접근해서 IP나 name을 요청할때 마다 database에 할당된 IP 주소를 받아온다.

여기서 Service는 actual thing이 아닌 memory의 cabinet에 위치한 가상의 요소로 Pod networking에 접속할 수 없다.
따라서 service는 pod같은 container가 아니므로 interface가 없고, 능동적으로 process를 알 수 없다.

※ 그렇다면 Service는 database의 IP를 어떻게 받아오는가?
Kube-proxy를 통해 받아올 수 있다.
Kube-proxy는 k8s의 Cluster의 각각의 Node에서 동작하면서 항상 새로운 Service가 생성된게 있는지를 확인한다. 만약, 생성된게 있다면 적절한 IP Table Rules를 각각의 Node에 생성한다.

· Kube-proxy 설치
wget https://storage.googleapis.com/kubernetes-release/release/v1.13.0/bin/linux/amd64/kube-proxy

Kubeadm tool은 kube-proxy를 pods의 각각의 Node에 daemon set으로 deploy한다. 따라서 single Pod는 항상 cluster의 각각의 node에 배포된다.

✔ POD
POD는 application의 작은 instance이다.
POD는 k8s에서 생성할 수 있는 가장 가장 작은 단위의 object이다.

k8s는 worker node에 직접적으로 컨테이너를 deploy하지 않는다.

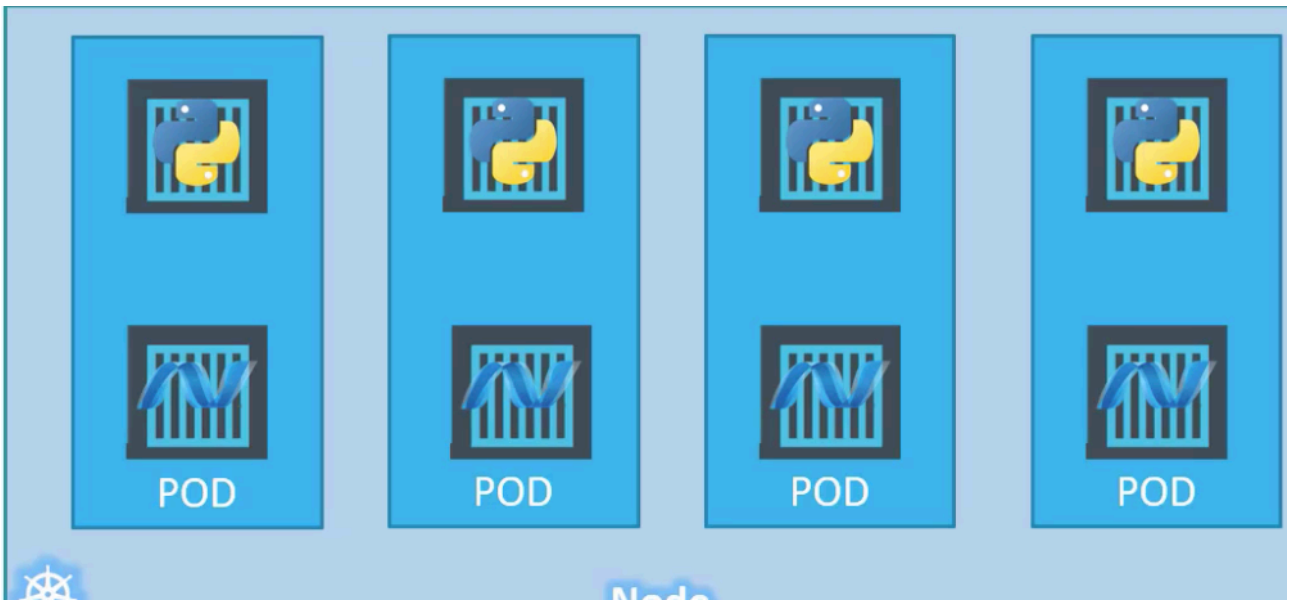
컨테이너는 POD라 알려진 k8s 오브젝트로 압축되서 들어간다.

새로운 컨테이너 instance를 같은 POD로 불러올 수 없다.

POD는 컨테이너와 1:1 관계이다.

싱글 POD는 멀티플 컨테이너를 가질 수 있다.

새로운 application 컨테이너가 POD에 생성되면 helper 컨테이너도 동시에 생성되고, 컨테이너가 삭제되면 helper 컨테이너도 삭제된다.



두개의 컨테이너는 같은 network namespace에 위치한다면 서로 직접적으로 localhost를 통해서 통신할 수 있다. 또한, storage도 공유할 수 있다.

· POD를 Deploy하는 방법
1. kubectl run nginx -> POD를 생성함으로써 docker 컨테이너를 deploy한다.
이 과정에서 POD를 자동으로 생성하고 nginx docker images의 instance를 deploy한다.

2. 1을 실행하게되면 다양한 application이 저장되어있는 docker hub(Public repository)로부터 최신 버전의 images를 가져온다.

3. kubectl get pods → 사용 가능한 POD를 확인하는 방법.

✔ POD with YAML

· YAML based configuration file을 사용해서 POD를 생성하는 방법

k8s definition files는 항상 4가지의 top-level field를 갖는다.

1. apiVersion : k8s api version을 말한다. → String
- POD를 생성하고자 할 때 : v1
- Service를 생성하고자 할 때 : v1
- ReplicaSet을 생성하고자 할 때 : apps/v1
- Deployment를 생성하고자 할 때 : apps/v1

2. kind : 생성하고자 하는 object의 type을 말한다. → String

Kind	Version
POD	v1
Service	v1
ReplicaSet	apps/v1
Deployment	apps/v1

3. metadata : name labels같은 object에대한 data를 말한다. → Dictionary
metadat의 child에는 k8s에서 인지 가능한 metadata만 넣을 수 있다. 하지만, labels의 child에는 내가 생각하기에 적합하다고 생각하는 것들을 넣을 수 있다.

4. spec : → Dictionary

ex)
apiVersion: v1 → String
kind: Pod → String
metadata: → Dictionary
        name: myapp-pod
        labels:
                app: myapp
                type: front-end

spec: → Dictionary

containers: → List/Array
- name: nginx-container → “-“ 는 첫번째 list item을 말한다.
  image: nginx

kubectl create -f pod-definition.yml

· kubectl get pods : Pods 확인하는 방법
· kubectl describe pod myapp-pod : 특정 pod의 정보를 보여주는 것