
openmaru
APM
쿠버네티스의 필요성과 도입의 어려운 난이도

GOOGLE 과 컨테이너

openmaru

- **Google의 업무 방식**

Gmail에서 YouTube, 검색에 이르기까지 Google의 모든 제품은 컨테이너에서 실행됩니다.

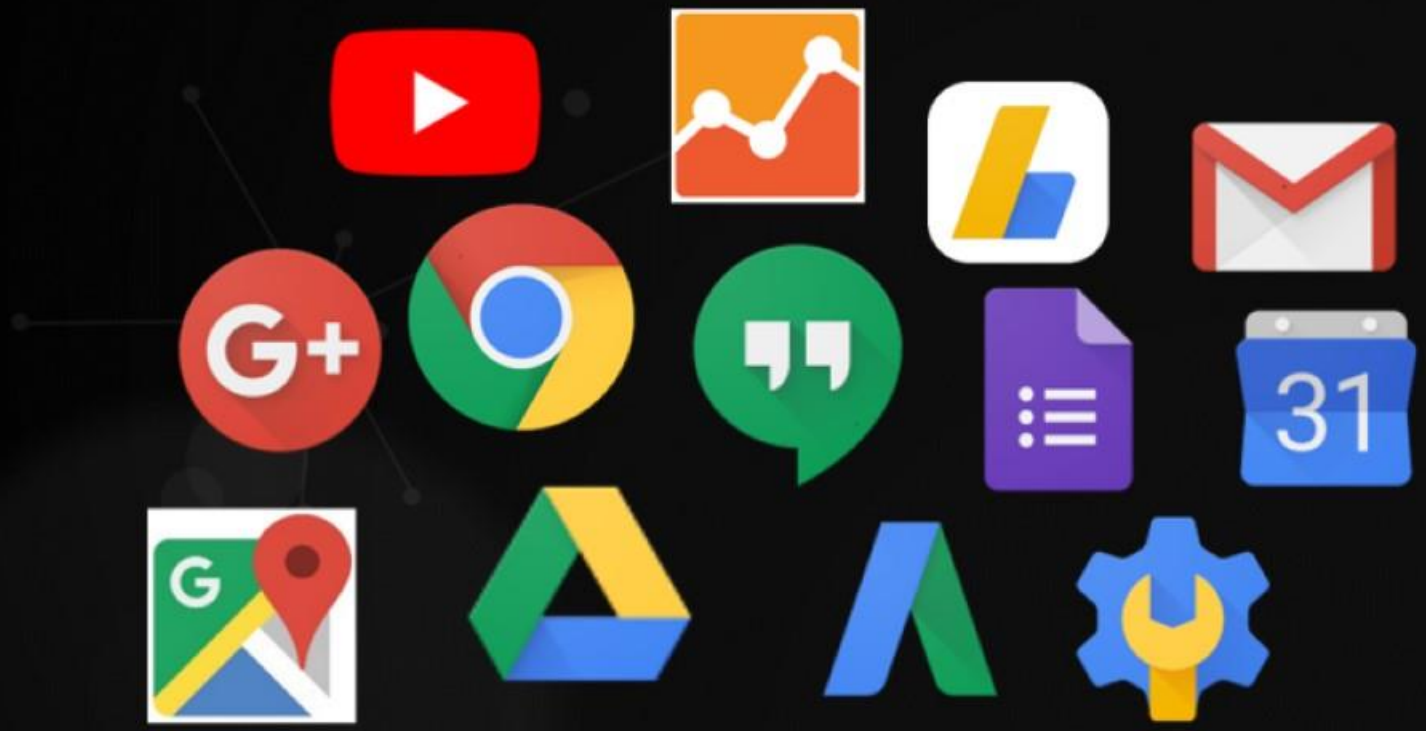
개발팀은 컨테이너화를 통해 더욱 신속하게 움직이고, 효율적으로 소프트웨어를 배포하며 전례 없는 수준의 확장성을 확보할 수 있게 되었습니다. **Google은 매주 수십억 개가 넘는 컨테이너를 생성**합니다. **지난 10여 년간 프로덕션 환경에서 컨테이너화된 워크로드를 실행하는 방법에 관해 많은 경험**을 쌓으면서 Google은 커뮤니티에 계속 이 지식을 공유해 왔습니다.

초창기에 cgroup 기능을 Linux 커널에 제공한 것부터 **내부 도구의 설계 소스를 Kubernetes 프로젝트로 공개**한 것까지 공유의 사례는 다양합니다. 그리고 이 전문 지식을 Google Cloud Platform으로 구현하여 개발자와 크고 작은 규모의 회사가 최신의 컨테이너 혁신 기술을 쉽게 활용할 수 있도록 하였습니다.

Source - https://cloud.google.com/containers/

Google 는 모두 컨테이너에서 실행

- Gmail , 검색, 지도 ...
- MapReduce , GFS , Colossus ...
- Google Compute Engine 가상 머신도 컨테이너에서 실행!
- 매주 20 억개 이상의 컨테이너를 실행 중



About Kubernetes

- 쿠버네티스(K8s)는 컨테이너화된 애플리케이션을 자동으로 배포, 스케일링 및 관리해주는 오픈소스 소프트웨어
- 쿠버네티스", "쿠베르네테스","K8s", "쿠베", "쿠버", "큐브"라고 부르며 Apache License 2.0 라이선스로 리눅스 재단 (Linux Foundation)산하 Cloud Native Computing Foundation (CNCF) 에서 관리
- Go로 작성된 오픈 소스 , OSS (Apache License 2.0) 라이선스
- 구글에서 개발하고 설계한 플랫폼으로서 사내에서 이용하던 컨테이너 클러스터 관리 도구인 "Borg"의 아이디어를 바탕으로 개발

> "Kubernetes is open source-a contrast to Borg and Omega, which were developed as purely Google-internal systems. "
>
> - *Borg, Omega, and Kubernetes*

시스템 비대화로 작업 폭증과 인력 부족 어떻게 할까요?

장애의 65 %는 Human Error이며,시스템 복잡도와 난이도 증가

시스템 운용 업무의 45 %는 정기적으로 수행해야하는 반복 작업

운영 효율화를 통한 비용 절감의 요구

시스템의 대규모 화

높은 수준의 엔지니어 부족

지속적인 시스템 통합 요구

동일한 작업 반복

운영 품질 향상

운영 비용 (TCO) 절감 요구

업무 확대와 관련 데이터양의 비약적인 증가

가상화, 클라우드 등 다양한 운영 환경의 증가와 관리 효율화 요구

운영 품질에 대한 지속적인 향상 요청

컨테이너 오케스트레이션을 통한 IT 인프라 운영 자동화

- IT 인프라의 대규모화, 고도화에 따라 IT 장비에 대한 환경설정 및 정보 취합이 복잡하고 어려움
- 작업 계획시간과 현장 작업 시간의 증가와 휴먼 에러의 증가

Before OpenShift

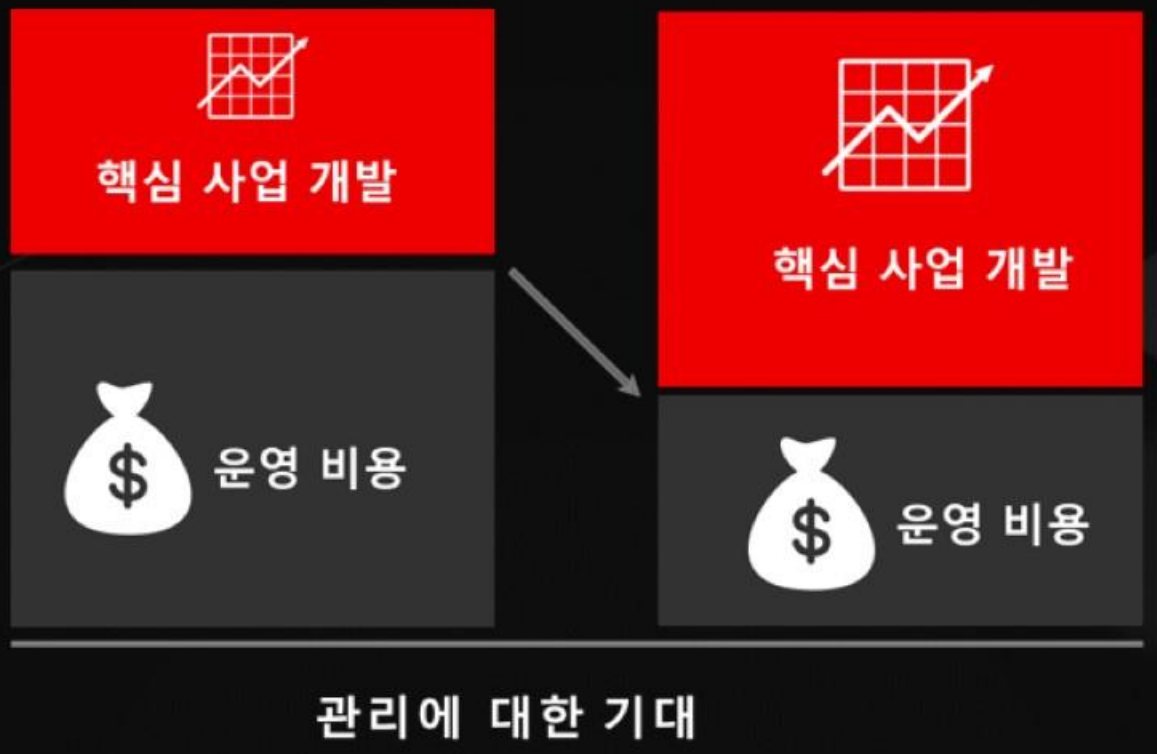
- 시스템 운영을 위한 관리 작업 증가
- 현장 작업 시간 증가
- Human Error 증가

After OpenShift

- 운영 기술 표준화를 통한 준비 시간 및 작업 시간 감소
- 시스템 일괄 설정 작업 시간 단축
- 시스템을 통한 작업으로 Human Error감소

PaaS 를 통한 사업 비용 절감

- 매니지드 서비스로 운영 비용을 줄이고 귀중한 인적 자원을 핵심 사업의 개발에 집중



Container와 Kubernetes의 역사

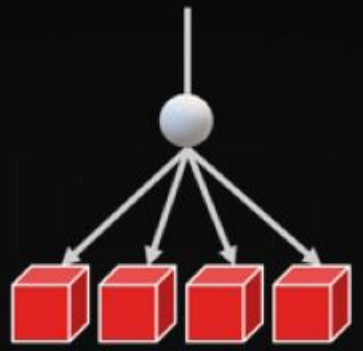
chroot
FreeBSD jail
Virtuozzo
200
OpenVZ
2005
2008
LXC
Red Hat OpenShift Online
2011
Kubernetes
2013
docker
RED HAT ENTERPRISE LINUX 7
2014
rkt
2015
Red Hat OpenShift 3.0
OCI
2016
CNCF
skopeo
Moby
moby project
2017
cri-o
Buildah
2018
Red Hat Enterprise Linux 8
2019
Podman
Red Hat OpenShift 4.5
2020

Kubernetes 주요 기능

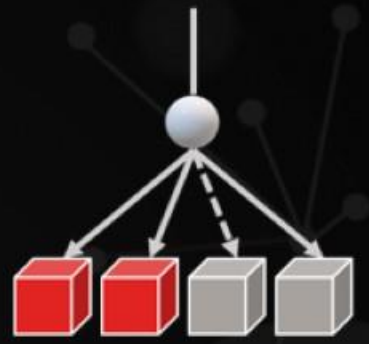
openmaru

Scale Out / In

Load Balancer

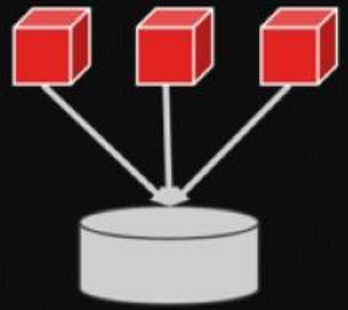


Rolling Update

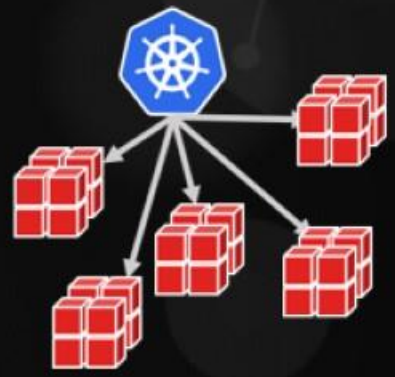


Auto Healing

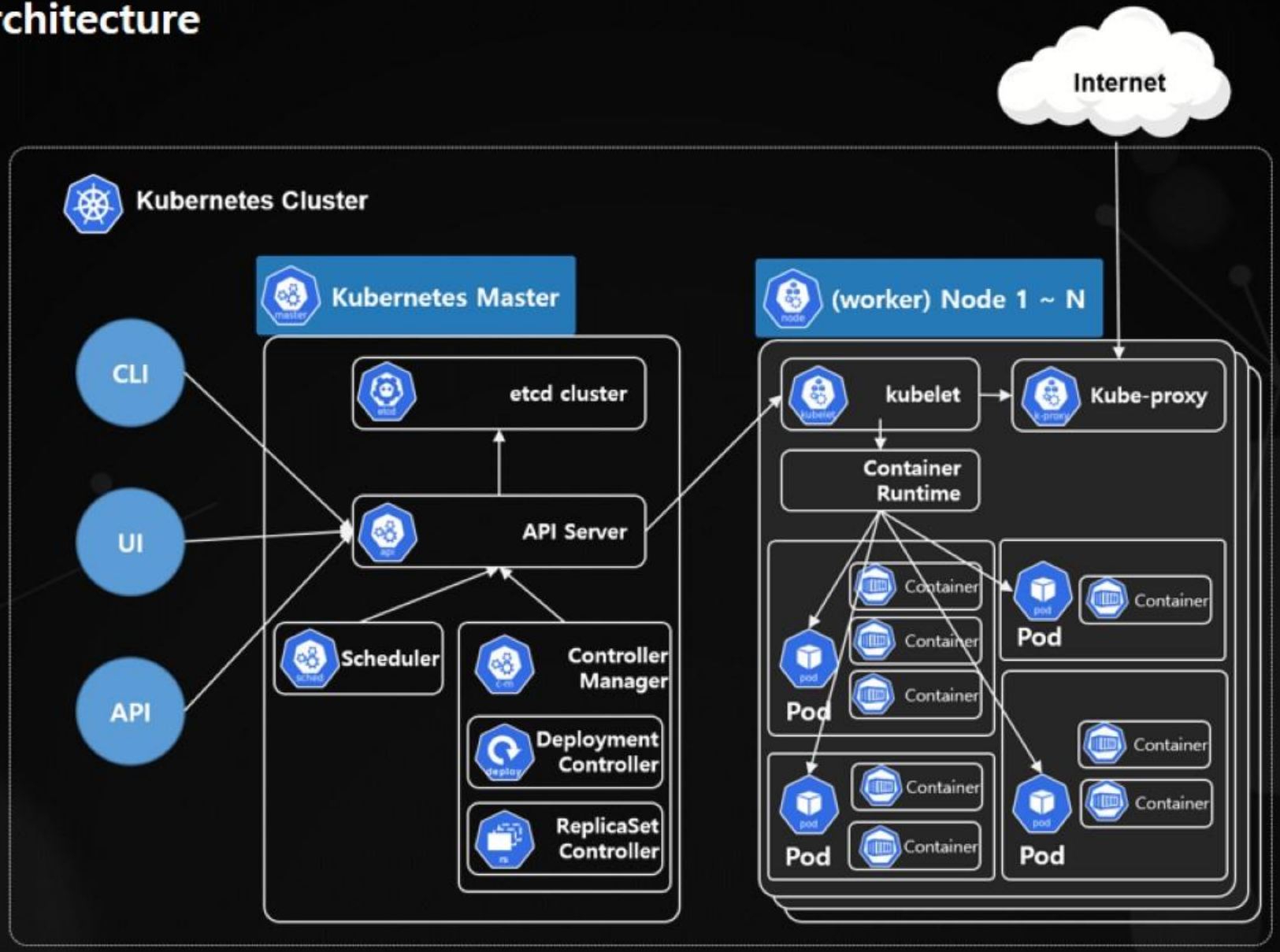
Persistence Volume



Container Orchestration



Kubernetes Architecture



쿠버네티스, 정확한 이해 없이 성공적인 도입 어려워...

VM웨어가 매년 실시하고 있는 쿠버네티스 실태 조사 보고서에 의하면 지난해에 이어 올해도 많은 기업이 쿠버네티스를 채택하고 있다는 것을 증명했지만, 그 과정에서 여러 과제들도 안고 있는 것으로 나타났다.

https://www.datanet.co.kr/news/articleView.html?idxno=174878

- 검증된 기술지원 역량 고려
  - 핸들링할 역량이 충분한지 PoC를 통해서 검증
  - 대부분의 업체들이 고객 요구사항에 대응이 가능하다고 하지만, 정작 그렇지 못한 경우들도 많으니 주의

- 엔터프라이즈용 쿠버네티스 지원
  - 순수 커뮤니티를 이용해서 운영하는 것은 자체 고급인력 확보, 보안, 버그, 짧은 라이프사이클로 인한 업그레이드 이슈 등을 안고 같이 가야 하는 것과 마찬가지
  - 기술 자체의 이슈에 대한 지원을 받을 수 있어야만 그 기반의 문제에 대한 빠른 대응과 극복이 가능
  - 순수 쿠버네티스로는 도입 후 성공적으로 운영하기는 많은 어려움

KUBERNETES 를 제대로 운영하기 어려운 이유는?

- Kubernetes 훌륭한 기초 기술이지만, 스토리지, 네트워킹, 보안, 애플리케이션 프레임 워크 등을 통합하고 이를 분기별로 갱신하는 것은 큰 부담입니다

- Ashesh Badani, Red Hat

Why running your own Kubernetes deployment could be a terrible idea

Kubernetes is hard, but becomes doubly so when you take on the burden of supporting this fast-moving project.

By Matt Asay | June 21, 2018, 11:23 AM PST

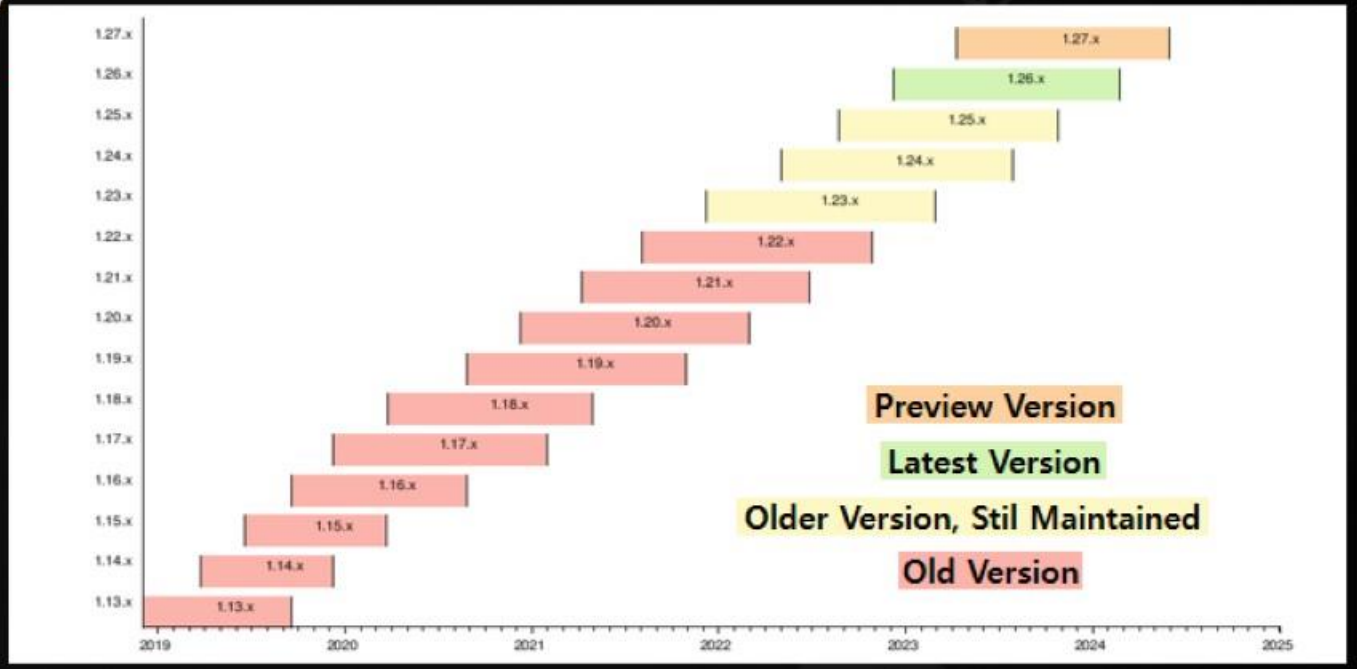
https://www.techrepublic.com/article/why-running-your-own-kubernetes-deployment-could-be-a-terrible-idea/

K8S의 업그레이드 주기

- Kubernetes의 경우 1년에 3~4 버전의 Major Release
- 2023년시점 21년 중반에 release한 1.22.x 버전 역시 maintain 종료
- 업그레이드 버전간 Dependency에 대한 명확한 설명이 부족함.

https://kubernetes.io/docs/tasks/administer-cluster/kubeadm/kubeadm-upgrade/

  - Make sure you read the release notes carefully.
  - The cluster should use...
  - Make sure to back up...
  - Swap must be disabled...



https://en.wikipedia.org/wiki/Kubernetes

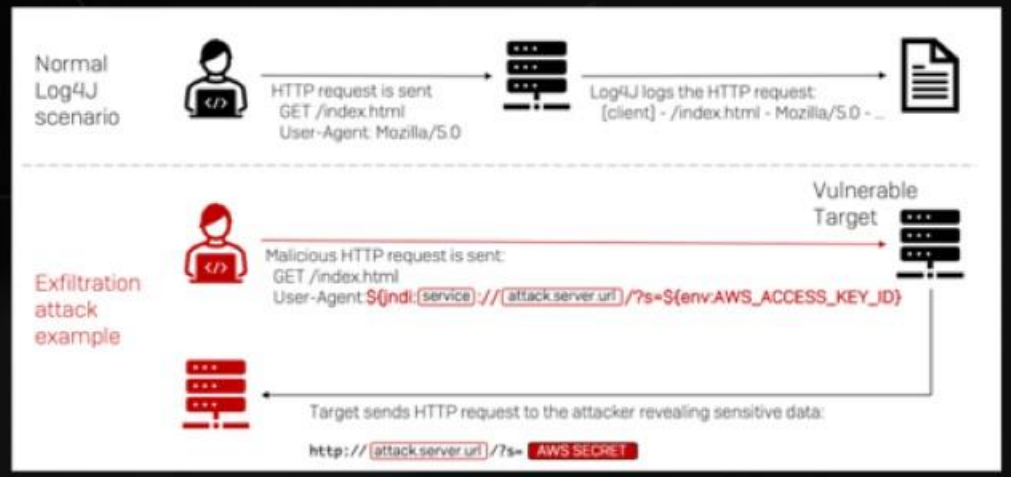
(참고)Elasticsearch Log4j 보안취약점 이슈

- 2021년 12월 9일 식별된 CVE-2021-44228 취약점

  RCE(Remote Code Execution)라고 일컬어지는 이 취약점은 공격자가 원격 서버에서 코드를 실행할 수 있게 합니다.

- Kubernetes의 자체적인 컴포넌트들은 대부분 Go언어이나 그 위에 동작하는 운영을 위한 시스템들은 JAVA와 같은 여러가지 언어로 작성된 프로그램

- 로깅 스택의 Elastic Search의 경우 CVE-2021-44228 취약점을 조치한 버전을 release 했으나, 그것을 운영중인 Kuberentes 클러스터에 적용시키는 것은 Kubernetes 클러스터 관리자의 몫



AWS환경에서 CVE-2021-44228 취약점을 활용한 공격 구성 (출처 : SOPHOS Labs)

Introducing 7.16.2 and 6.8.22 releases of Elasticsearch and Logstash to upgrade Apache Log4j2

By Tom Callahan, Quin Hoxie, Rajiv Raghunarayan

2021년 12월 19일

한국어

https://www.elastic.co/kr/blog/new-elasticsearch-and-logstash-releases-upgrade-apache-log4j2

Kubernetes 구축과 운영의 복잡성

openmaru

Kubernetes 사용자 중 **75 %** 는

구축과 운영의 복잡성으로 도입하기 어렵다고 함

INSTALL
• Templating
• Validation
• OS Setup

DEPLOY
• Identity & Security Access
• App Monitoring & Alerts
• Storage & Persistence
• Egress, Ingress & Integration
• Host Container Images
• Build / Deploy Methodology

HARDEN
• Platform Monitoring & Alerts
• Metering & Chargeback
• Platform Security Hardening
• Image Hardening
• Security Certifications
• Network Policy
• Disaster Recovery
• Resource Segmentation

OPERATE
• OS Upgrade 및 Patch
• Platform Upgrade 및 Patch
• Image Upgrade 및 Patch
• App Upgrade 및 Patch
• Security Patches
• Continuous Security Scanning
• Multi-environment Rollout
• Enterprise Container Registry
• Cluster & App Elasticity
• Monitor, Alert, Remediate
• Log Aggregation

Source : The New Stack, The State of the Kubernetes Ecosystem, August 2017

OpenShift가 아닌 K8S를 구축할 때 고려해야할 것들

openmaru

1. 보안

- 인증서 관리
- 컨테이너 이미지 신뢰성
- Runtime 신뢰성
- 플랫폼 계정관리
- Host OS 보안
- 컨테이너 보안

2. 운영/관리

- Web Console
- Cloud Native 3rd Party
- 서비스 라우팅
- 기술지원
- Cluster Upgrade
- Software Defined Network
- 모니터링

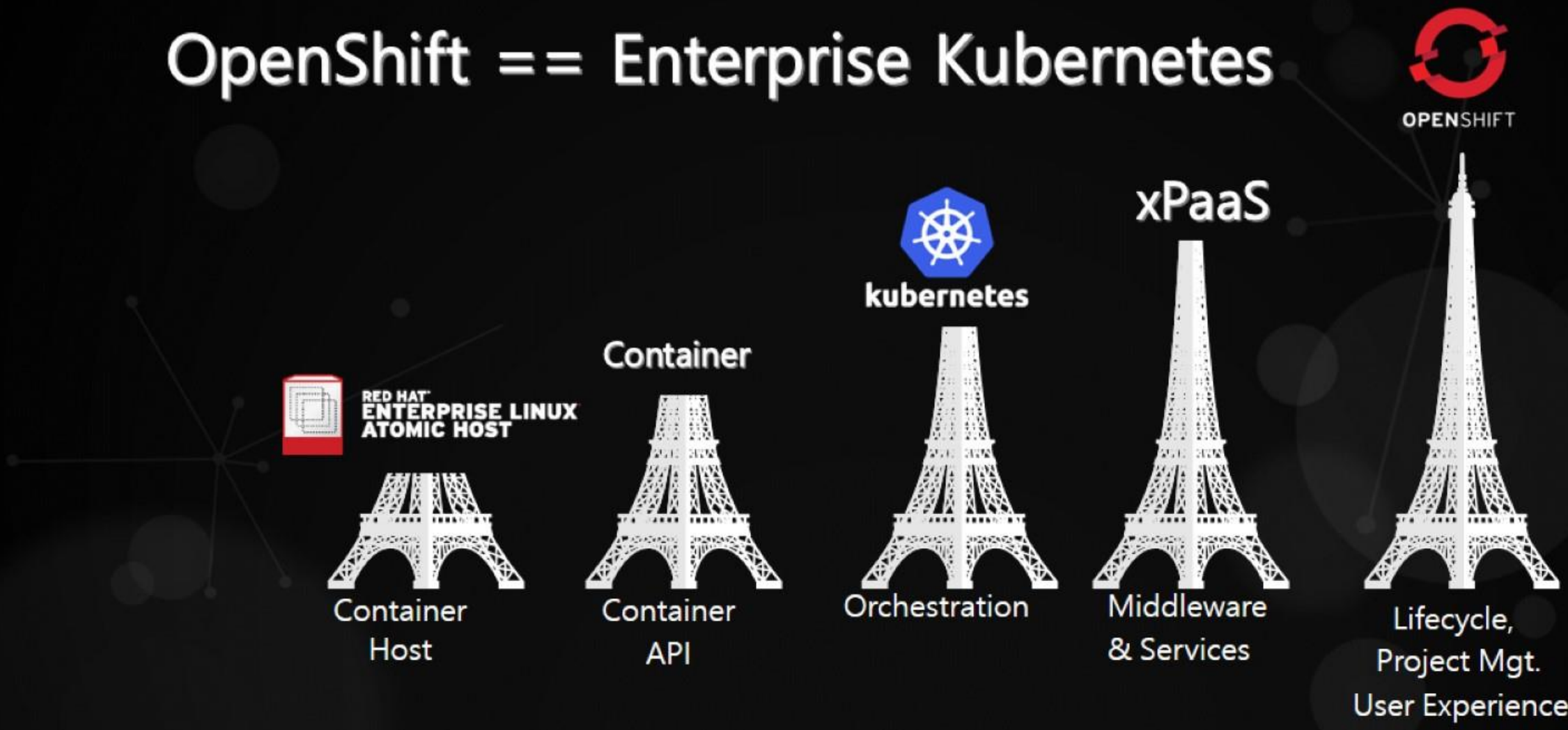
3. 애플리케이션

- 애플리케이션 컨테이너화
- 애플리케이션 로깅
- 애플리케이션 빌드배포
- 서비스메시

What is OpenShift ?

openmaru

OpenShift == Enterprise Kubernetes



부족한 Kubernetes vs 완벽한 OpenShift

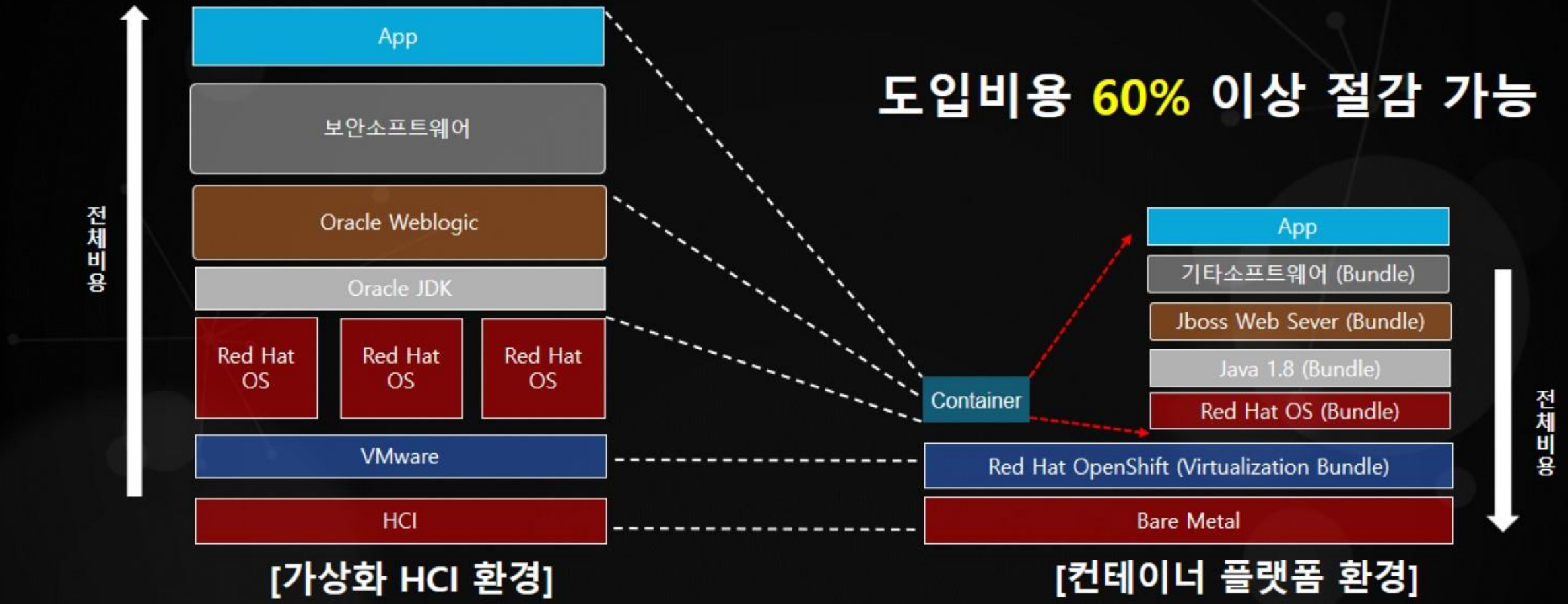
분류	Kubernetes	Openshift
이미지 레지스트리	• 별도 솔루션 필요- 담당 엔지니어가 직접 설치/구성/업데이트 진행	• Openshift 포함 – Openshift 전문 자격증을 보유한 고급엔지니어가 지원
로그관리	• 별도 솔루션 필요- 담당 엔지니어가 직접 설치/구성/업데이트 진행	• Openshift 포함 – Openshift 전문 자격증을 보유한 고급엔지니어가 지원
SDN (Software-Defined Network)	• 별도 솔루션 필요- 담당 엔지니어가 직접 설치/구성/업데이트 진행	• Openshift 포함 – Openshift 전문 자격증을 보유한 고급엔지니어가 지원
운영체제	• Linux 라이선스 별도 구매	• 번들로 포함하여 무료 (CoreOS)
컨테이너 런타임	• DOCKER/Containerd/CRI-O 직접선택필요	• 표준 컨테이너인 CRI-O
보안	• 별도 솔루션 필요- 담당 엔지니어가 직접 보안 책임	• OS 레벨에서 보안/취약점 대응 • 안전한 컨테이너 사용을 위한 이미지 스캐닝, 암호화, 실행 사용자 제한등 각종 기능 제공
운영관리	• 별도 솔루션 필요-담당 엔지니어가 직접 운영관리	• 앤서블을 사용한 설치 및 설정 • 레드햇이 제공하는 클라우드 시스템 관리 제품과의 연계
CI / CD	• 별도 솔루션 필요-담당 엔지니어가 직접 설치/구성	• Openshift에 포함된 Jenkins로 원활한 CI/CD 통합 가능

Openshift는 레드햇과 공식파트너 오픈나루가 책임!

Kubernetes는 제품직접선택/직접설치/직접구성/직접업데이트진행/회사책임

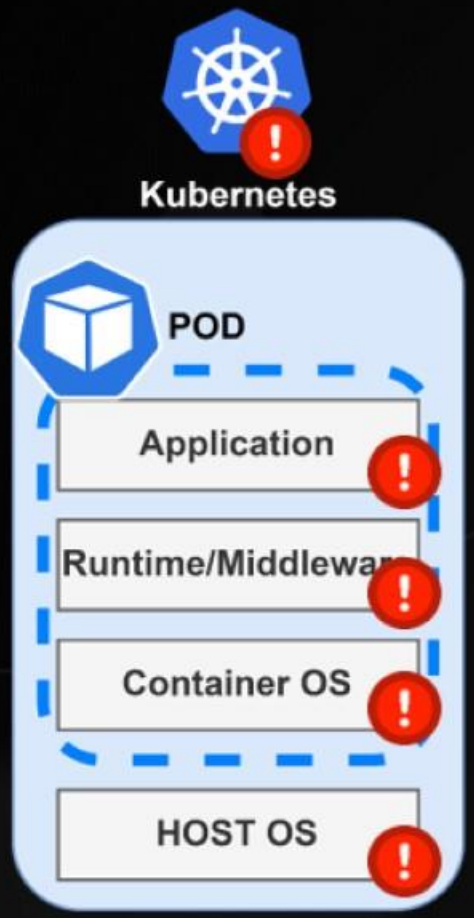
HCI 가상화 VS 컨테이너 플랫폼 금액 비교(2)

- 컨테이너 환경에서의 가상화소프트웨어 / WAS / 보안소프트웨어 비용 제거
- 1 Bare Metal (1 Worker Node - 2 socket / up to 64 cores) 1 copy 기준은 2 Core 1 Copy 기준 대비 90% 비용 절감



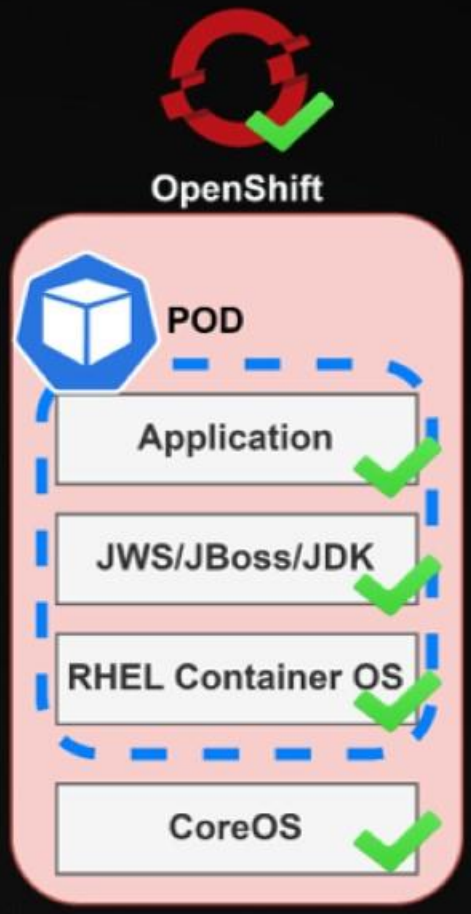
신뢰할 수 있는 Software 스택 제공

openmaru



Kubernetes + DIY Stack

- 신뢰할 수 없는 컨테이너 이미지
  - 컨테이너 보안 업데이트 X
- QA팀을 통한 안정화 테스트 X
- HOST OS 유지보수
  - 업그레이드
  - 패치
  - 트러블슈팅
  - 구매비용 발생
- Runtime/Middleware 유지보수
  - 업그레이드
  - 패치
  - 트러블슈팅
  - 구매비용 발생



OpenShift Container Platform

- 신뢰할 수 있는 컨테이너 이미지
  - Quay, red hat registry
- QA팀을 통한 안정화 테스트
- Red Hat Core OS
  - 업그레이드 지원
  - 버그 패치 지원
  - 트러블슈팅 지원
  - 컨테이너 특화 OS
  - 구매비용 발생 X
- OpenJDK / JBoss Web Server, EAP
  - 업그레이드 지원
  - 패치 지원
  - 트러블슈팅 지원
  - 구매비용 발생 X
    (EAP의 경우 구매비용 발생)

레거시 환경에서 필요한 서버 보안

- OS 보안, 서버 접근제어 등 보안 5종 S/W를 OS 설치
  - OS 마다 설치하기 때문에 물리서버는 1Copy이고, 가상화는 VM 개수 만큼 설치
- 서비스에 따라 부가적인 보안 소프트웨어 필요(개인정보 검출, 비정형 암호화 등)
- 법적인 근거로 인해 서버보안 – 전자금융법, ISMS 등의 요건

컨테이너 환경에서 필요한 보안

왜 AS-IS 환경의 보안들이 필요하지 않을까?

기존의 보안 소프트웨어가
필요하지 않은 환경

실질적으로 컨테이너환경에서 필요한 보안들

- 컨테이너 실행 권한에 대한 보안 : SCC
  - Container breakout
- 취약한 Container Image 사용
  - 악성코드, 채굴 프로그램이 포함된 이미지
- Role Base Access Controle : RBAC
  - 사용자별 필요 권한 부여
- 컨테이너 플랫폼의 Audit 로깅
  - EFK
- 신뢰할 수 있는 컨테이너 런타임 보안
  - Capabilities, SELinux, Seccomp & Namespace
- 컨테이너간의 네트워크 격리
  - Network Policy

필수 보안 프로그램 설치 방안

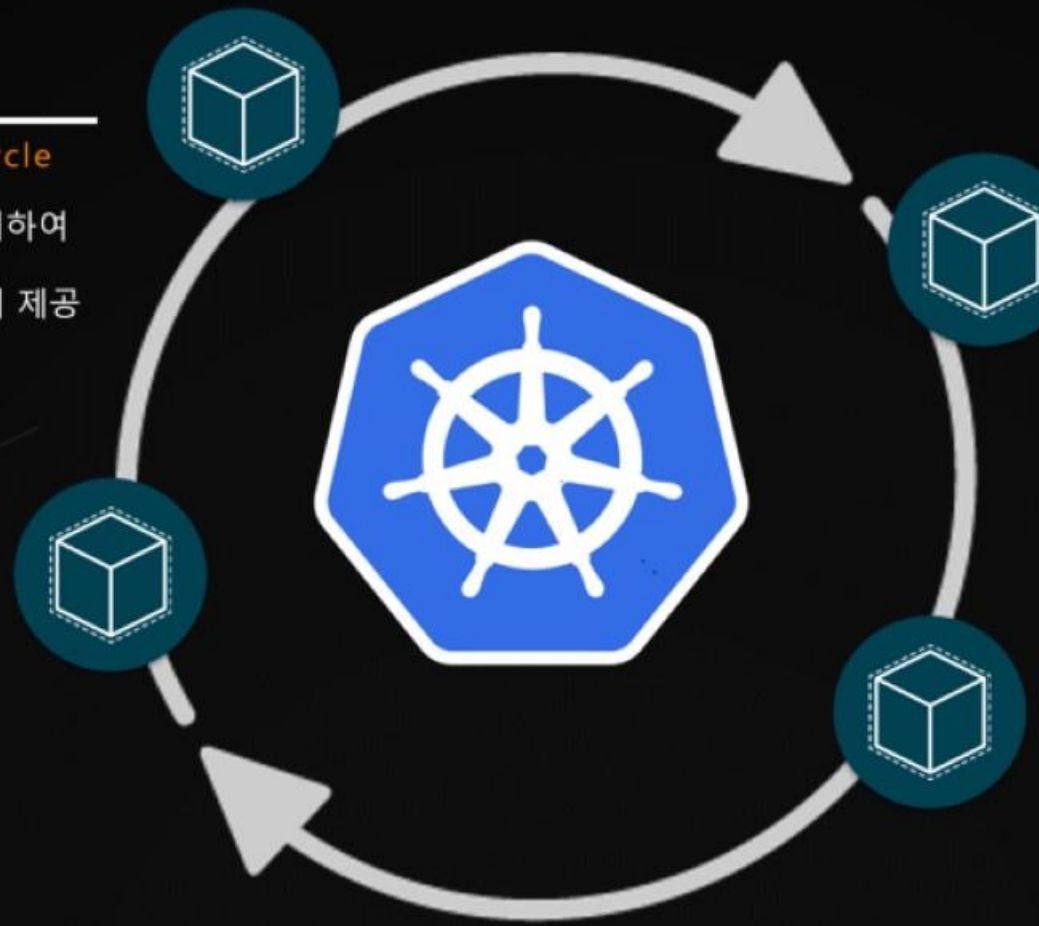
기업에서 필요한 Kubernetes 기술지원

openmaru

장기 수명주기

Predictable and long lifecycle

예측 가능한 라이프 사이클을 제시하여 운영하는 애플리케이션과 비즈니스에 필요한 장기 지원 체계 제공



교육

Training

장기적인 지원 뿐만 아니라 제품 교육과 자격증 제도를 제공하여 기술 내재화를 통한 서비스의 지속적인 운영을 지원

SLA 와 기술 지원

SLA and support

장애에 대한 응답 및 복구 할 수 있는 기한에 따라 SLA 을 지원하며, 벤더를 통한 명확한 지원 체계 제공

파트너 인증

Certification

ISV 가 제공하는 3rd party 소프트웨어를 포함하여 쿠버네티스 상에서 동작을 확인하고 비즈니스에 중요한 워크로드에 적합한 지 보장

제품 / 서비스에 관한 문의

- 콜 센터 : 02-469-5426 (휴대폰 : 010-2243-3394)
- 전자 메일 : sales@opennaru.com