
openmaru
APM
왜 Kubernetes 프로젝트가 어려운가?
- K8S를 운영환경에 맞게 갖추기 위해 고려해야하는 것들

Summary

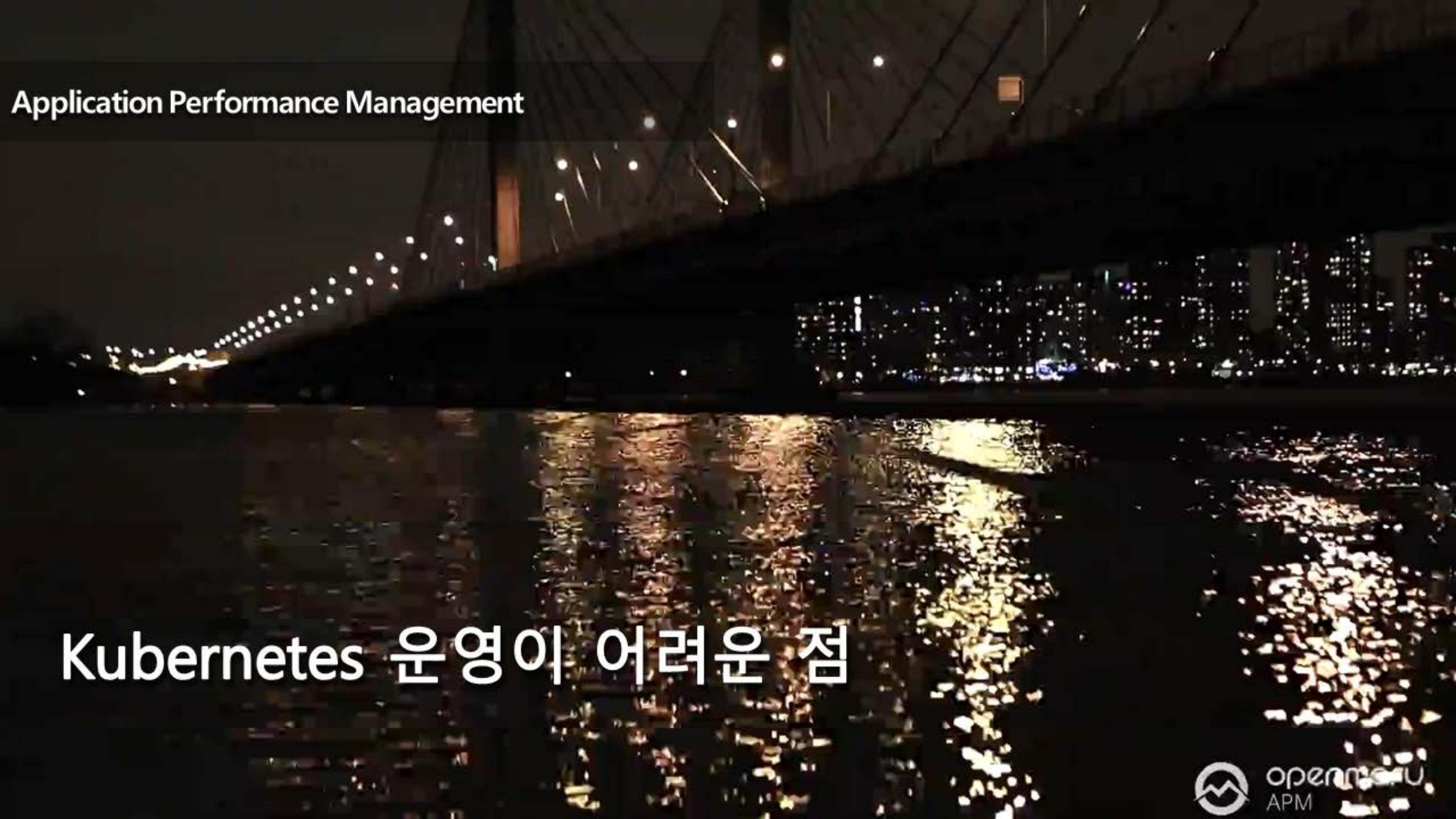
openmaru

1. Kubernetes 운영이 어려운 점

- Kubernetes 소개
- Kubernets 운영의 어려운 점

2. Kubernetes 운영시 필요한것들을 제공하는 PaaS

- OpenShift 소개
- K8S에서 고려되어야 하는 OpenShift의 컴포넌트


Application Performance Management
Kubernetes 운영이 어려운 점
openmetric
APM

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

클라우드 네이티브 환경의 애플리케이션 모니터링 어려움

openmaru

6. Monitor, log and troubleshoot from the start

The construction of applications from a set of microservice Legos considerably complicates how to monitor and troubleshoot systems and their performance. Various microservices often trigger a cascade of events that leads to an application failure. To minimize failures -- which aren't a *maybe*, but a reality -- incorporate monitoring and troubleshooting into microservices design.

https://www.techtarget.com/searchitoperations/tip/Follow-these-6-steps-to-deploy-microservices-in-production

- 마이크로 서비스 아키텍처일수록 **모니터링 방법이 상당히 복잡**해 집니다.
- 마이크로 서비스 아키텍처에 **모니터링과 트러블 슈팅 방법이 고려**되어야 합니다.

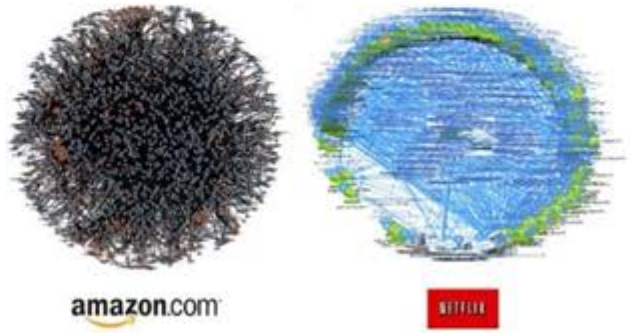
- **Uber는 2014년 말 에 4,000개가 넘는 독점 마이크로 서비스와 점점 더 많은 수의 오픈 소스 시스템이 모니터링 시스템에 문제를 제기했다고 보고**
- **컨테이너 인프라는 모니터링 시스템이 필수적인 환경**
- **마이크로 서비스에 특화된 모니터링 시스템이 필요**

2. Microservices instead of a monolith

Following a microservice architecture, a typical monolith application would be broken down into a dozen or more microservices, each one potentially running its own programming language and database, each one independently deployed, scaled and upgraded.

Uber for example reported in late 2014 over 4,000 proprietary microservices and a growing number of open source systems which posed a challenge for their monitoring system.

The Challenge: A surge in the number of discrete components you need to monitor.



https://www.infoq.com/articles/microservice-monitoring-right-way

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

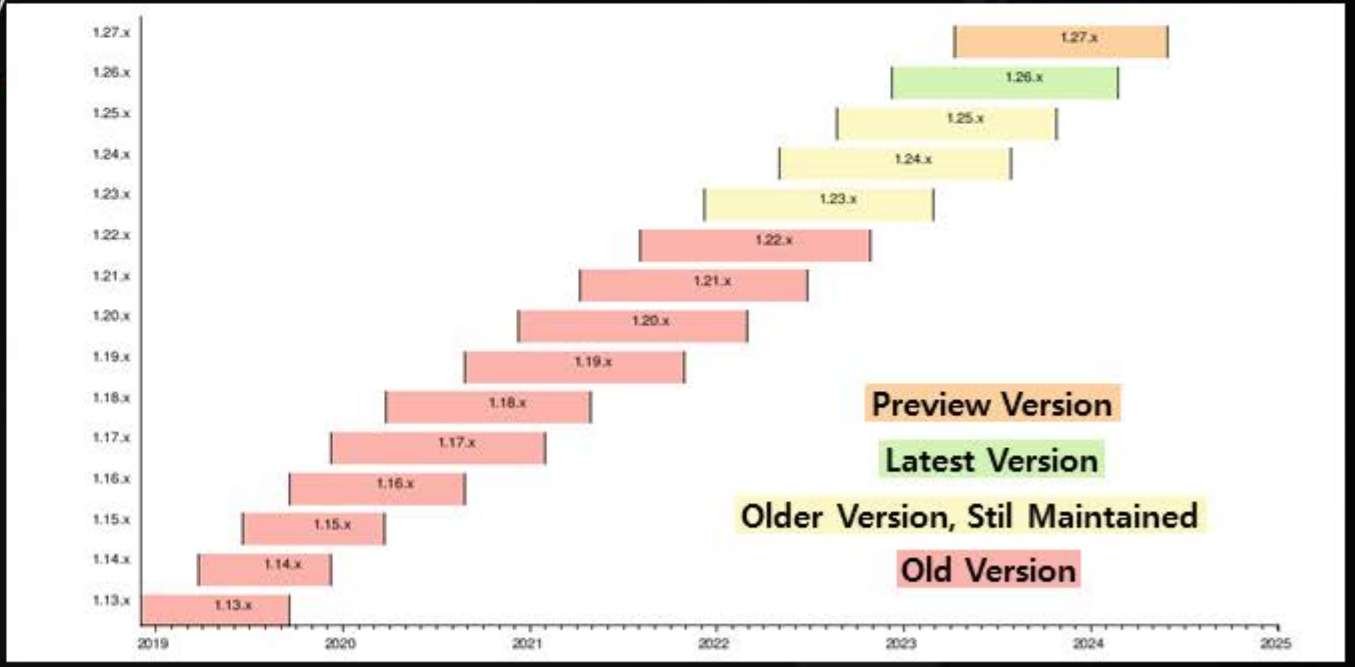
https://www.techrepublic.com/article/why-running-your-own-kubernetes-deployment-could-be-a-terrible-idea/

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

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

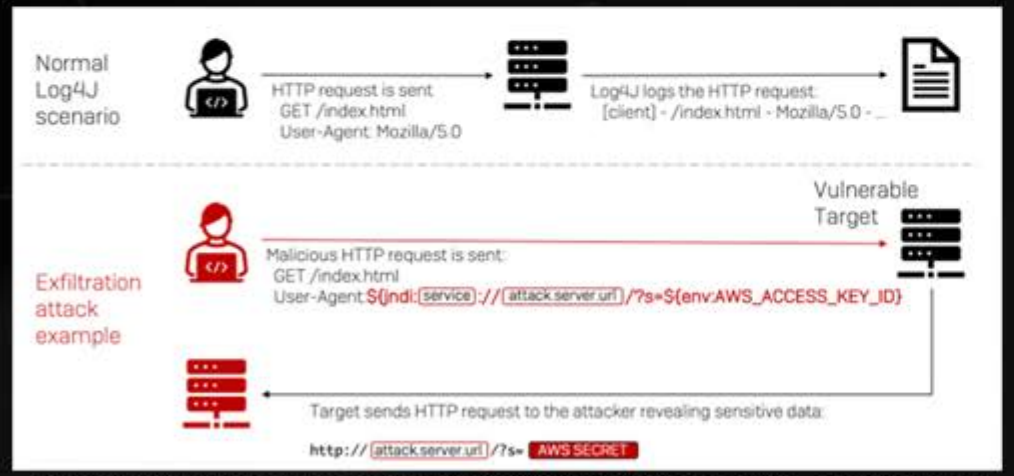
(참고)Elasticsearch Log4j 보안취약점 이슈

- 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

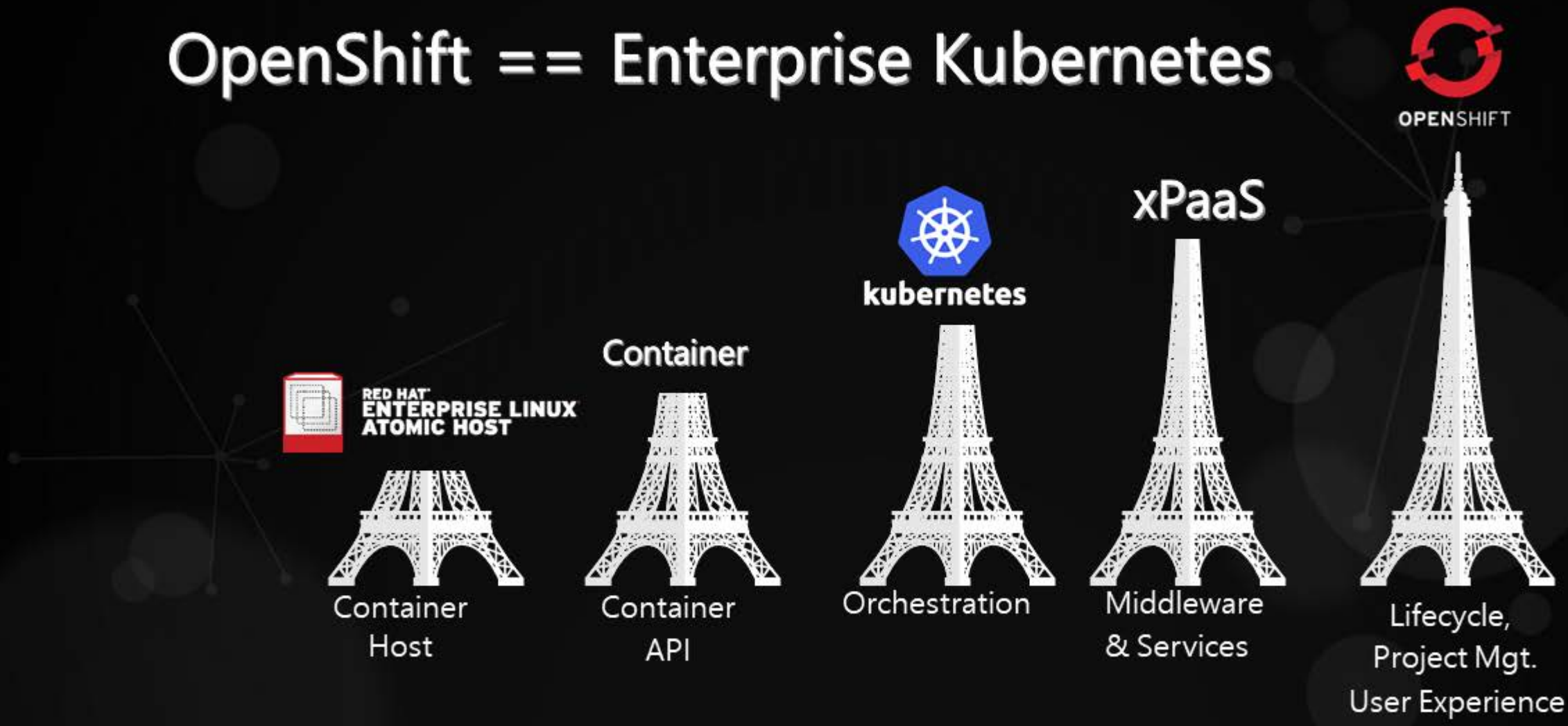
https://www.elastic.co/kr/blog/new-elasticsearch-and-logstash-releases-upgrade-apache-log4j2


Kubernetes 운영시 필요한것들을 제공하는 PaaS
openmaru
APM

What is OpenShift ?

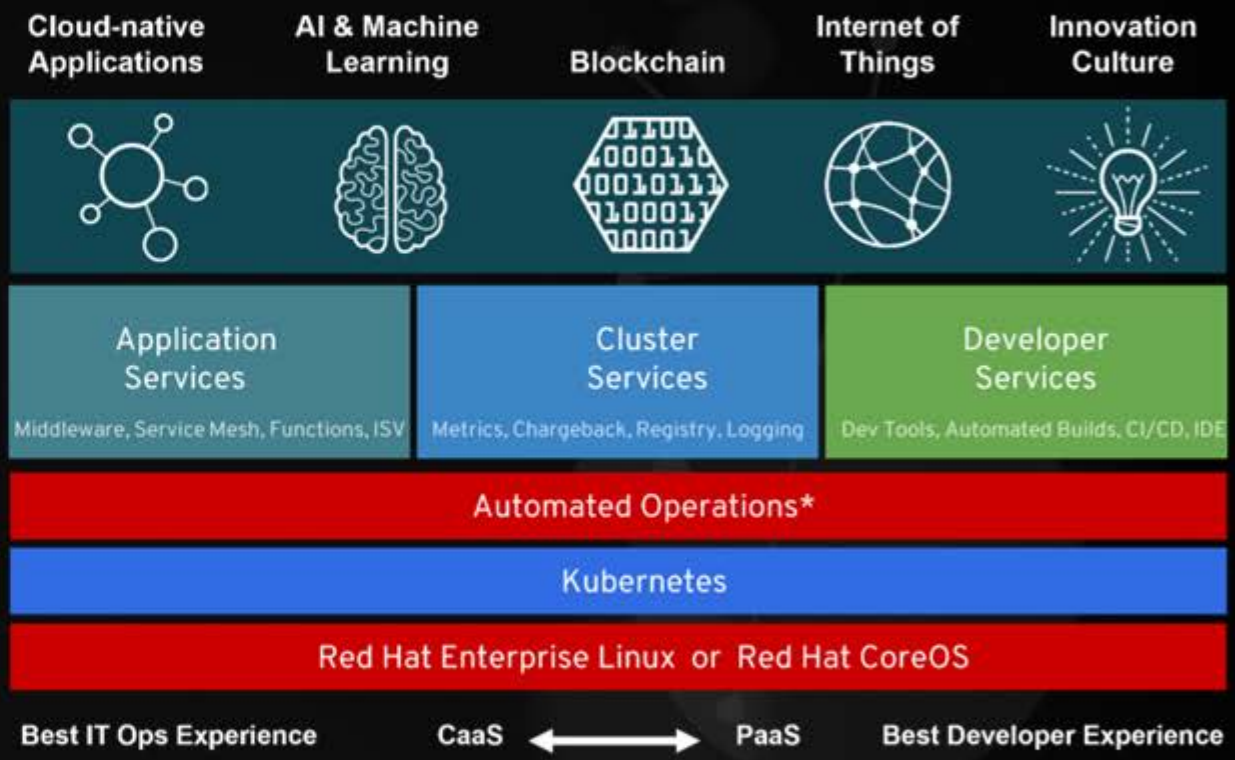
openmaru

OpenShift == Enterprise Kubernetes



Enterprise Kubernetes

- 신뢰할 수 있는 Enterprise Kubernetes
  - 신뢰할 수 있는 호스트, 컨텐츠, 플랫폼
  - Full-Stacked (전자동) 설치
  - Over the Air Updates & Day 2 management
- 어떤 환경에서도 클라우드를 경험
  - 하이브리드, 멀티 클러스터 관리
  - 오퍼레이터 (Operator) 프레임 워크
  - Operator Hub 와 certified ISVs
- 혁신을 위한 개발자 지원
  - OpenShift Service Mesh (Istio) – 서비스 메쉬
  - OpenShift Serverless (Knative) - Serverless
  - CodeReady (Che) - k8s native 개발 환경



Red Hat OpenShift

How Do We Deliver OpenShift?

Community Distribution of Kuberne
tes 100+ Integrations
Align time with OSS trunk

okd

Integrate OSS projects Partner int
egration platform
No-cost validations for innovation

Red Hat
OpenShift
Container Platform

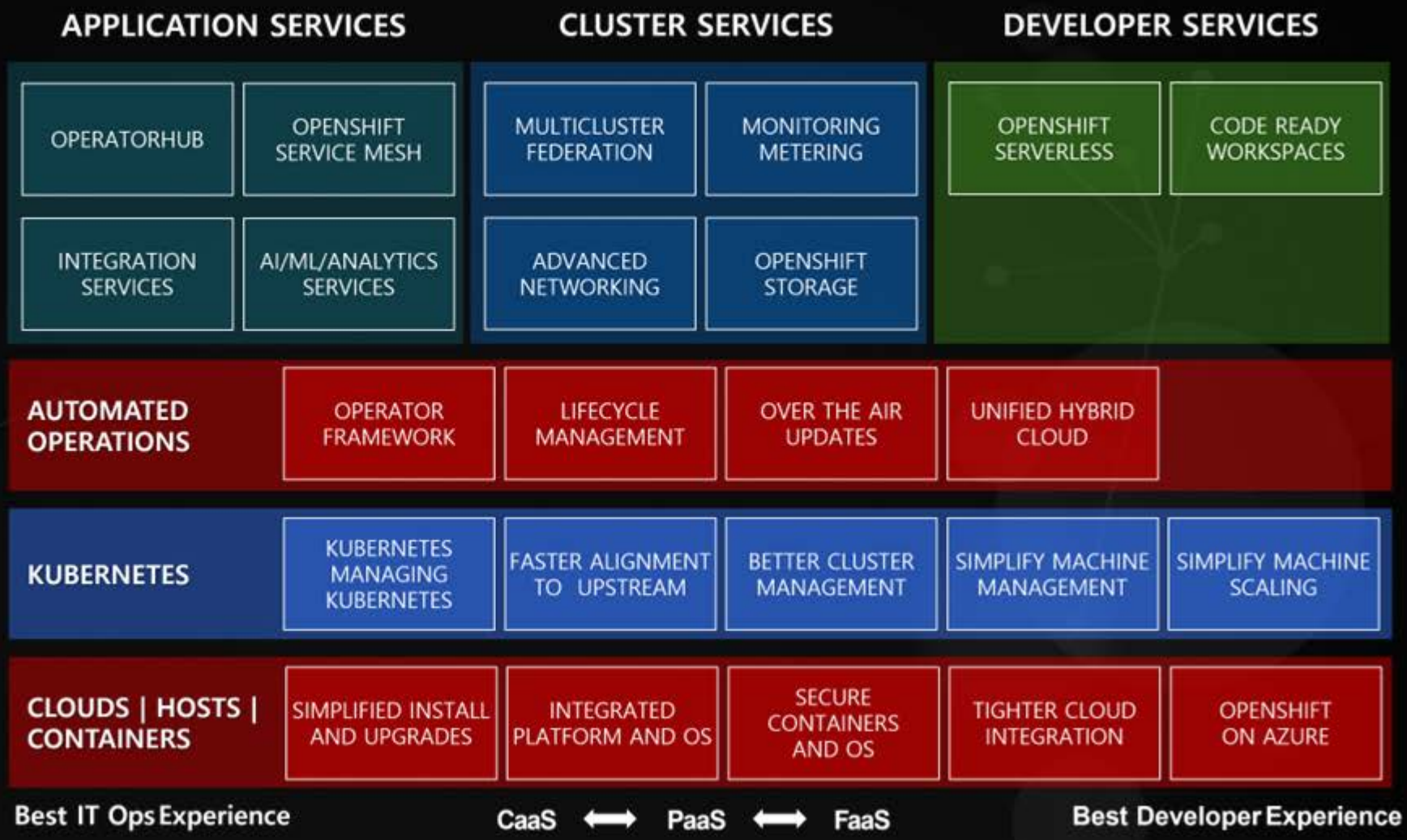
Red Hat
OpenShift Dedicated

Red Hat
OpenShift Online

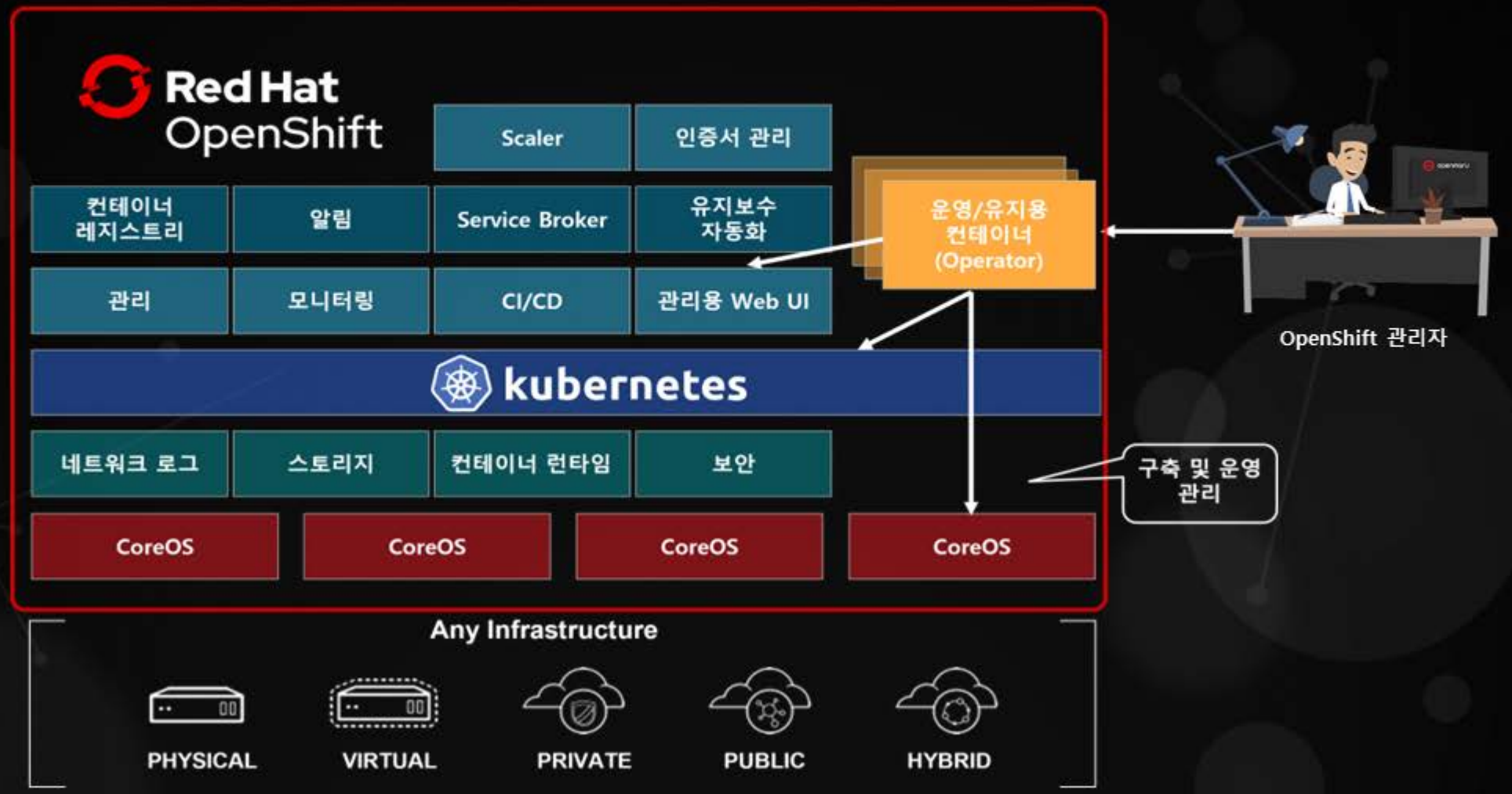
OpenShift 4 Platform

openmaru

Red Hat OpenShift



컨테이너 플랫폼 구축 및 관리 – OpenShift4



Why OpenShift?

- 엔터프라이즈 급 애플리케이션 지원
  - 기존의 애플리케이션 (상태)에서 클라우드 네이티브 애플리케이션 (무상태, 12 Factor App) 까지
- 업계 표준을 기반
  - CRI-O, Kubernetes, RHEL
- 기업용 미들웨어 서비스
  - JBoss EAP, JWS A-MQ, Fuse, BRMS, BPMS, JDG, Mobile, SSO
- 다양한 운영 환경 지원
  - 물리적 환경, 가상 환경, 프라이빗 클라우드, 퍼블릭 클라우드
- 하이브리드 클라우드 용 애플리케이션 플랫폼
  - 퍼블릭 / 프라이빗 클라우드 간 이동성 보장, 클라우드 프로바이더 간 관리
- Red Hat 을 통한 기술지원
  - 검증된 오픈 소스 리더

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. 설치/구성/관리

- Web Console
- Cloud Native 3rd Party
- 서비스 라우팅
- 기술지원
- Cluster Upgrade
- 빌드/배포
- 모니터링

Private 인증서 적용으로 각 컴포넌트에 대한 인증 처리

- 국내/외 K8S 보안가이드는 통신의 SSL을 적용하도록 가이드
- 인증서는 다음 구성요소와의 보안 연결(secure connections)을 위해 사용

MASTER	ETCD
NODES	INGRESS CONTROLLER
CONSOLE	REGISTRY

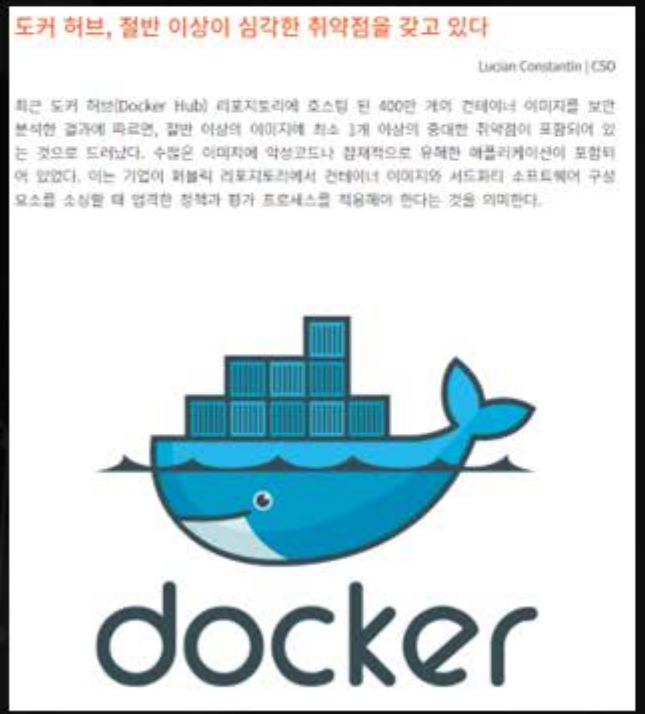
- 인증서 갱신 자동화 (Automated Certificate rotation)
  - Kubeadm의 경우 인증서 생성까지만 됨

- 커스텀 인증서를 사용하기 위한 외부 엔드포인트 설정 가능
  Requesting and Installing Let's Encrypt Certificates for OpenShift 4

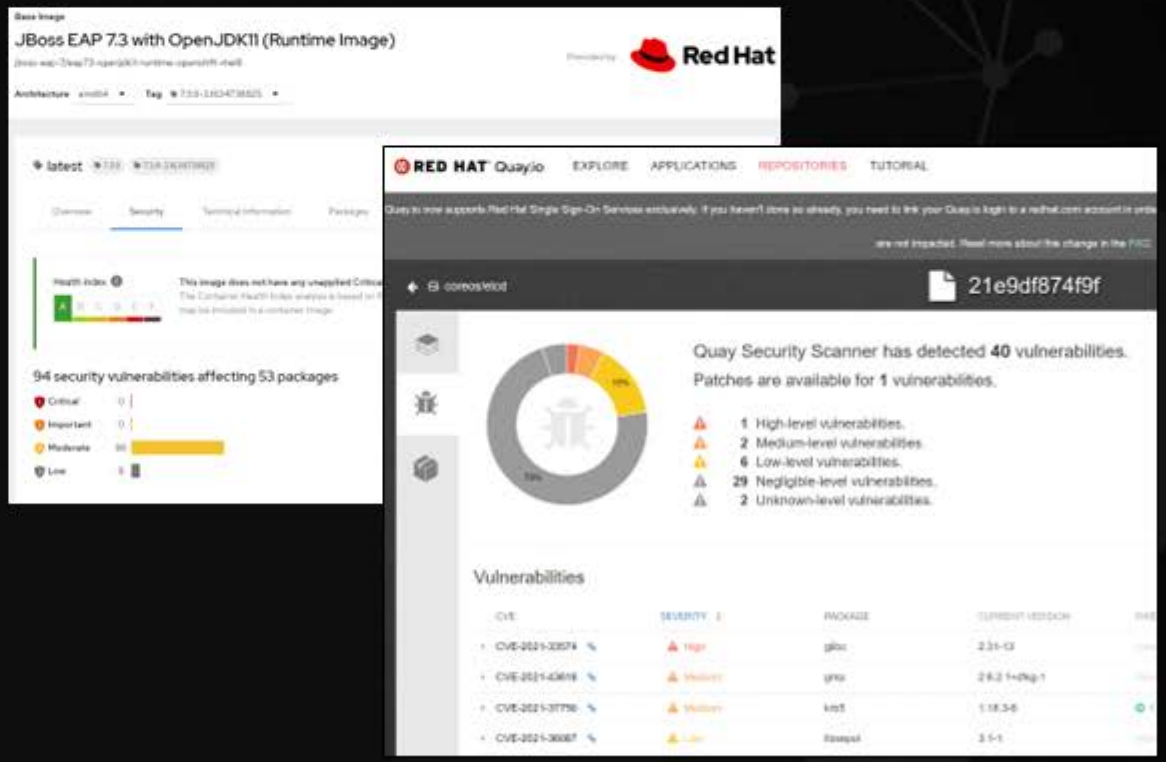
국내/외 보안단체의 K8S 보안 가이드

신뢰할 수 있는 컨테이너 이미지 제공

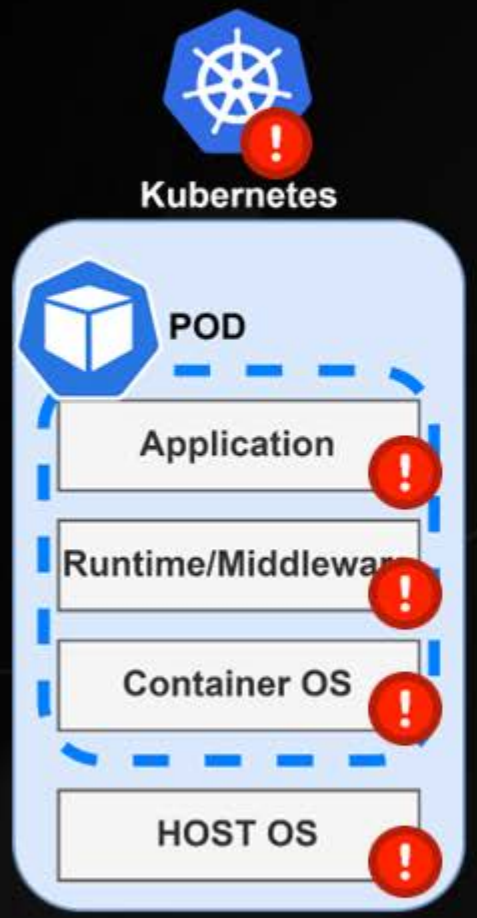
- DockerHub의 경우 개방되어 있어 다양한 Container Image가 많지만, 신뢰할 수 없는 이미지들도 대거 존재
- Red Hat의 경우 Quay.io와 registry.redhat.com을 운영하며
  OS, Middleware 소프트웨어들 뿐만 아니라 OCP에 Certi된 3rd Party 이미지도 제공(OperatorHub, ex: efk, servicemesh)



https://www.itworld.co.kr/news/174679

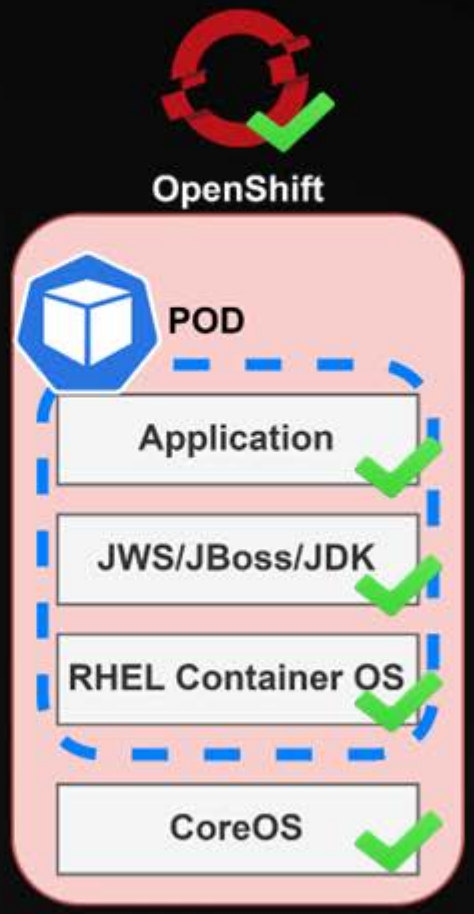


신뢰할 수 있는 Software 스택 제공



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

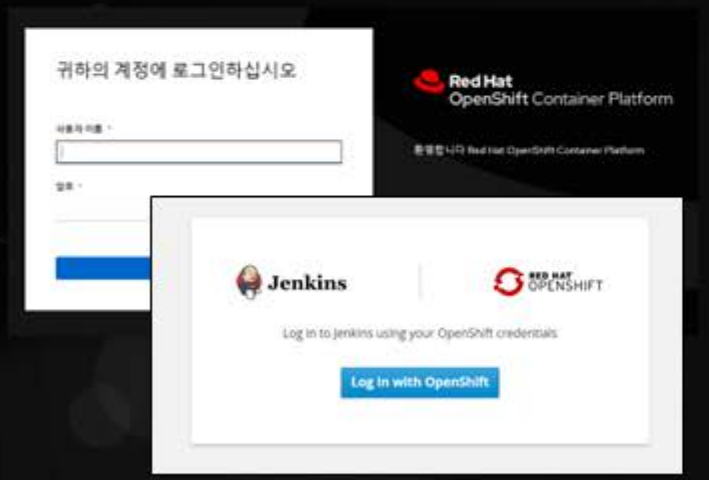


OpenShift Container Platform

- 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)

OAUTH를 통한 통합계정관리 제공

- OpenShift는 OAUTH를 제공하여 기존 시스템의 Identity Provider를 이용한 계정관리 가능
  - 별도 없을 시 HTPasswd를 이용한 연동
- OpenShift Web Console뿐만 아니라 OperatorHub를 통해 설치되는 3rd Party 솔루션의 Console도 연동 가능
  - Kibana Console
  - Jaeger, Kali Console



다양한 RBAC Role 제공

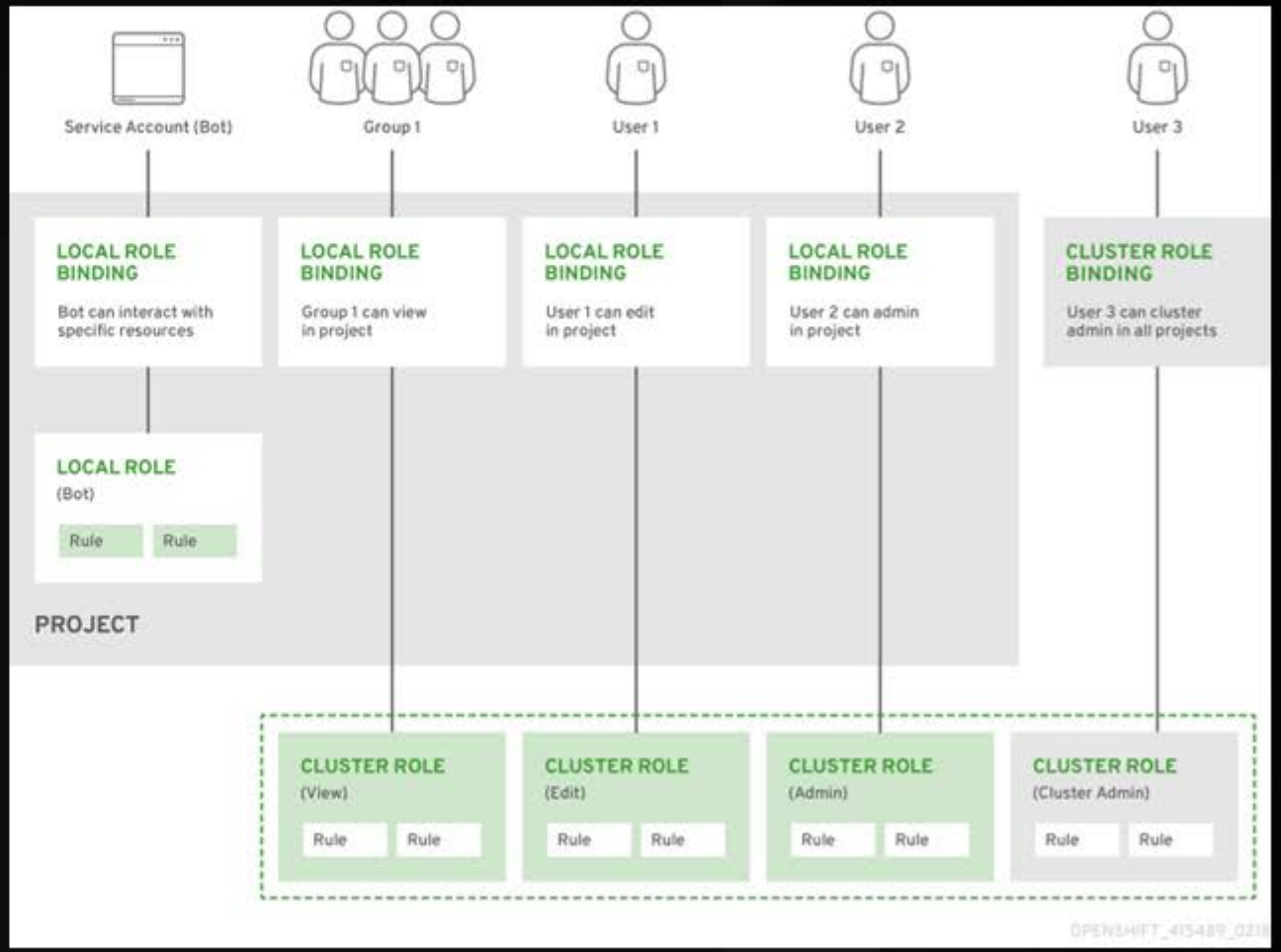
openmaru

Role based authorization

- Project scope & cluster scope available
- Matches request attributes (verb,object,etc)
- If no roles match, request is denied (deny by default)
- Operator- and user-level roles are defined by default
- Custom roles are supported

OpenShift RBAC VS K8S RBAC

- 사전에 정의된 OpenShift RBAC 약 160개.
  (System RBAC 제외)
- 사전에 정의된 K8S은 5개
  (System RBAC 포함 15개)



컨테이너를 기동시키기 위한 CoreOS

Immutable Infra Structure, Red Hat CoreOS

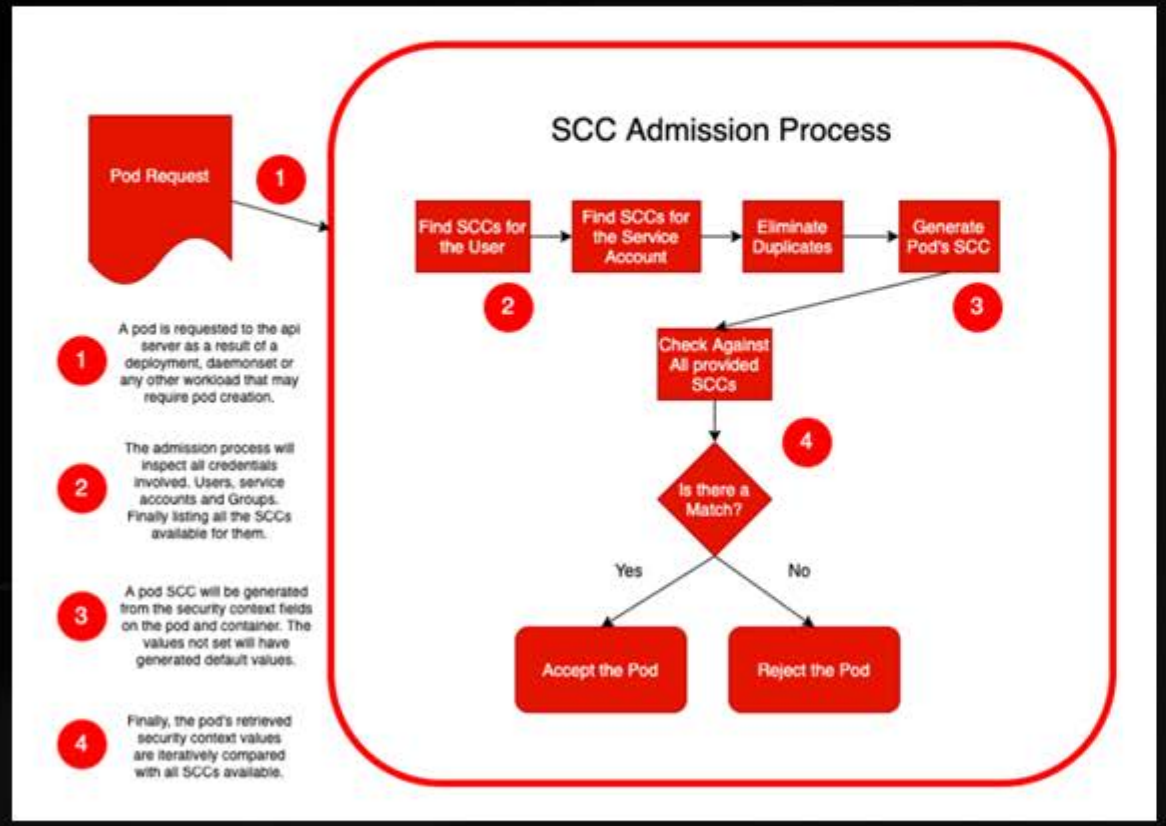
기존 OS에 필요한 Host OS 보안 프로그램

- 취약점 스캐너
- 서버접근제어
- OS 보안
- 백업 Agent
- 로그 수집
- VM 혹은 Baremetal 대수 만큼 필요

Red Hat CoreOS는 Immutable Infrastructure

- RHCOS는 플랫폼에 포함된 Compliance 시스템
  - 1금융권 사례
- Immutable Infrastructure 특성으로 Read-Only OS

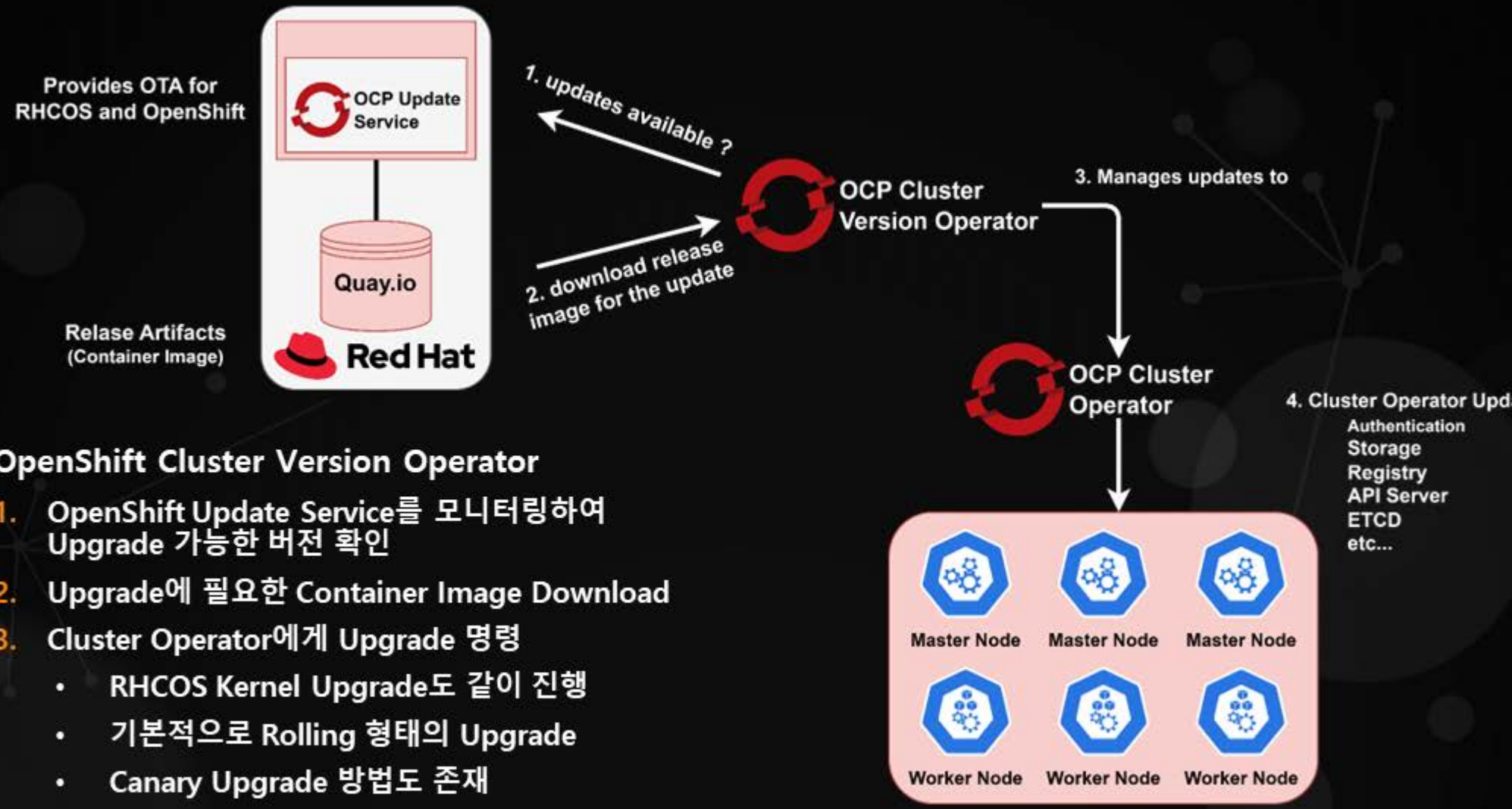
컨테이너 보안 SCC



Security Context Constraints

- 컨테이너가 기동할 때 컨테이너가 수행할 수 있는 기능 권한 제어
- Cluster 관리자가 컨테이너 ServiceAccount 별로 권한을 관리
  - 컨테이너가 Port를 Bind 하는지
  - 컨테이너 기동 계정 UID가 고정되어 있는지
  - Root로 컨테이너를 기동하는지
  - Host volum을 사용하는지
  - ...
- 대표적인 예시로 root 계정으로 실행되는 Container들은 OpenShift에서 기동되지 않음
  - Root 계정으로 기동하는 컨테이너는 Host OS의 root 계정을 탈취할 수 있음. (Container breakout 취약점)
- 일반적인 WEB Application의 경우 Port를 Bind할 수 있는 권한만 있음.

Cluster, Host OS Upgrade 방안



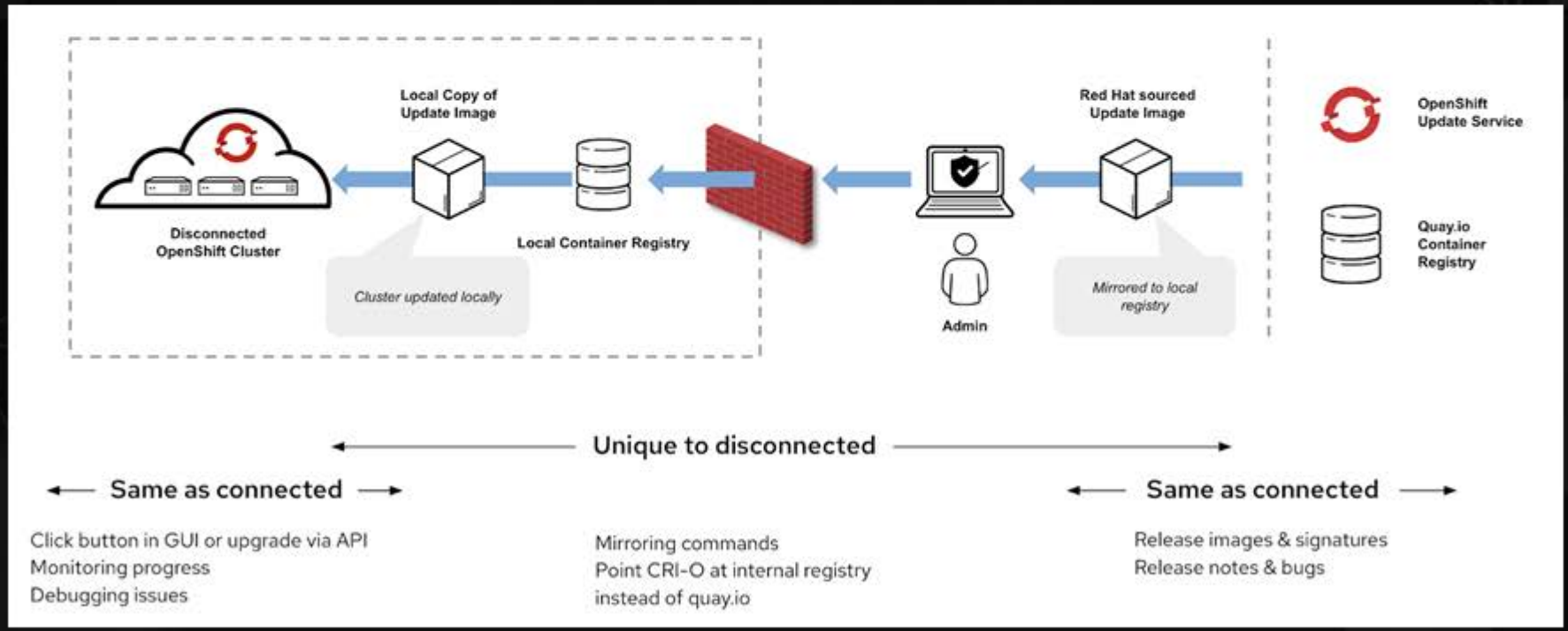
OpenShift Cluster Version Operator

1. OpenShift Update Service를 모니터링하여 Upgrade 가능한 버전 확인
2. Upgrade에 필요한 Container Image Download
3. Cluster Operator에게 Upgrade 명령
   - RHCOS Kernel Upgrade도 같이 진행
   - 기본적으로 Rolling 형태의 Upgrade
   - Canary Upgrade 방법도 존재

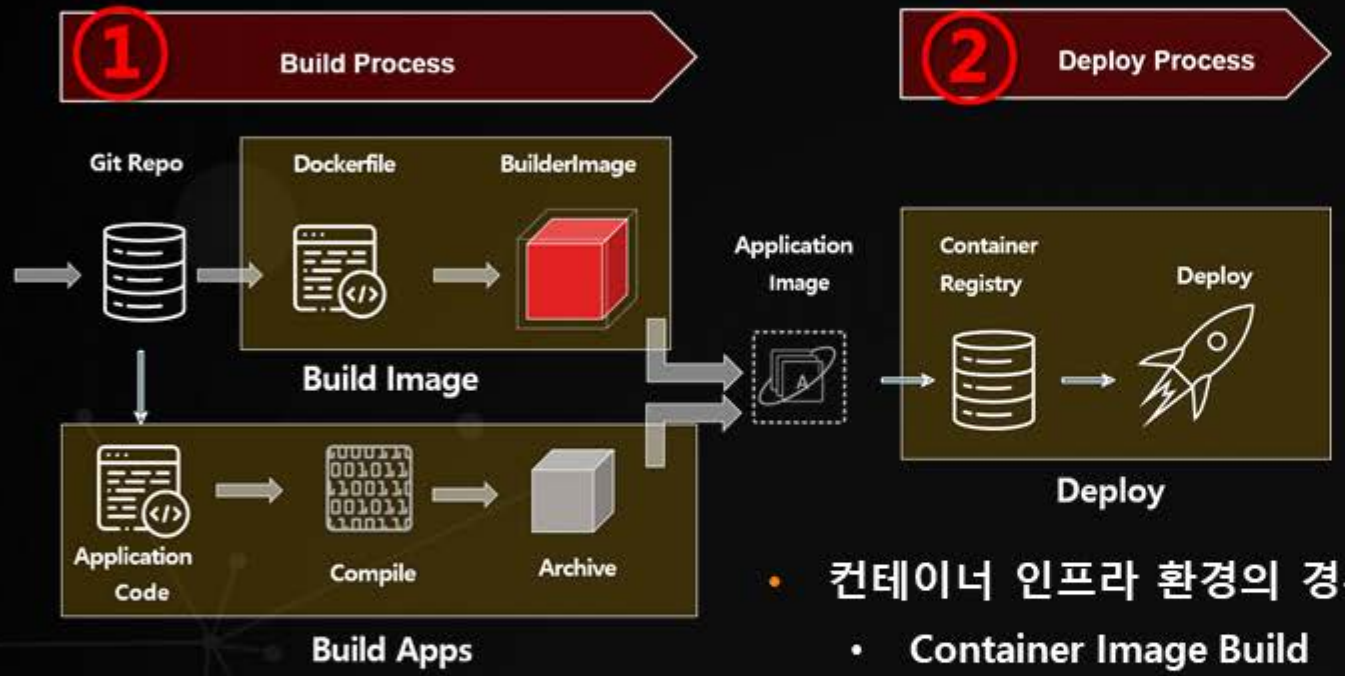
Disconnected 환경의 Upgrade 방안

Disconnected에서의 Upgrade 방안

- Connected Upgrade와 유사하나 Cluster 관리자의 Image Mirroring 작업이 필요
  - Mirror Image를 저장할 별도의 Image Registry가 필요
    ex: Quay, Harbor, Docker-registry



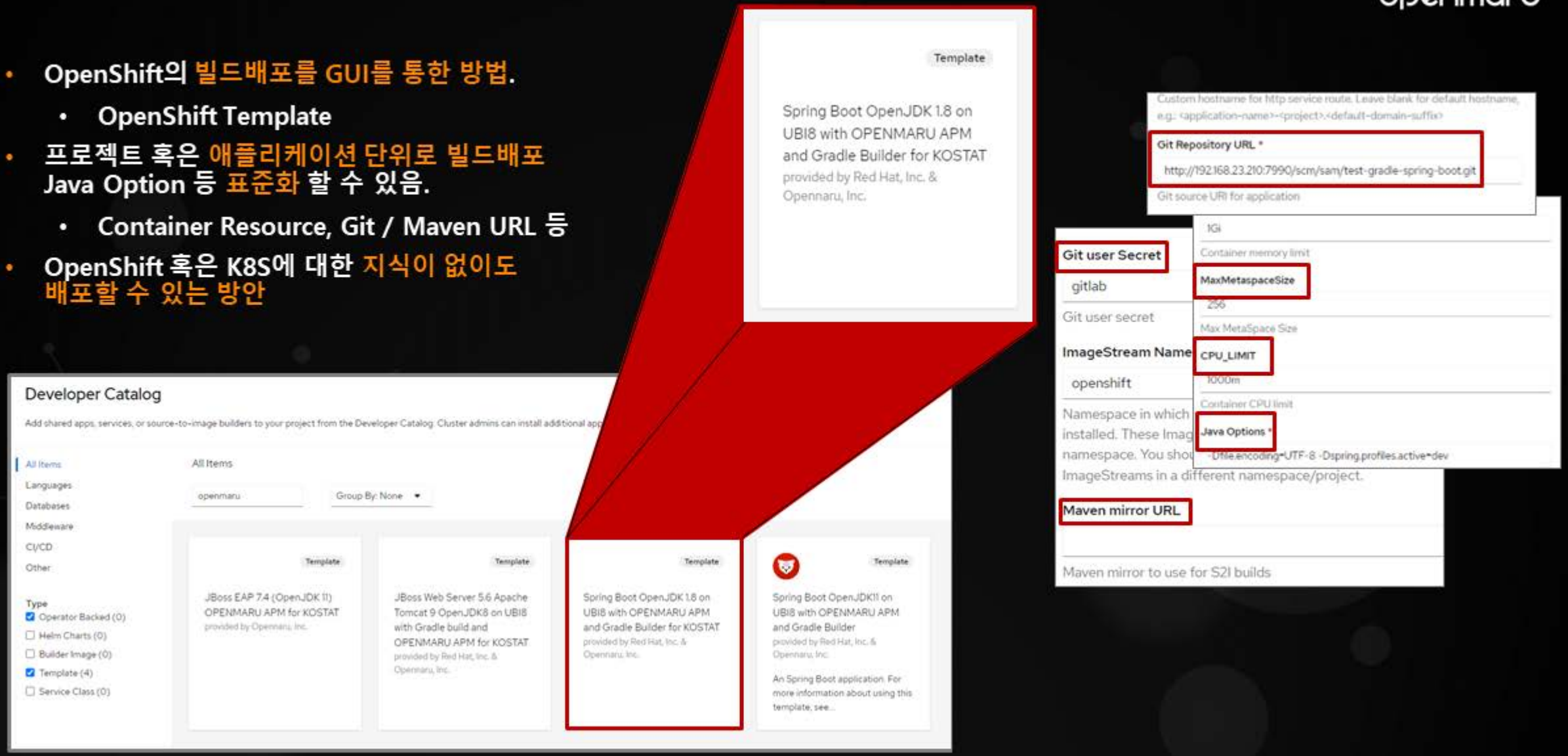
소스 빌드 / 컨테이너 이미지 빌드 / 배포 자동화



- 컨테이너 인프라 환경의 경우 기존환경보다 1가지 이상의 빌드과정이 추가 됨.
  - Container Image Build
  - 빌드된 애플리케이션을 Container Image와 결합하는 과정
- 많은 수의 MSA 애플리케이션과 잦은 빌드배포가 일어나기 때문에 자동화하는 방안이 필수.
- OpenShift에서는 Source To Image를 통해 지원

GUI 환경의 빌드 배포, OpenShift Template

- OpenShift의 빌드배포를 GUI를 통한 방법.
  - OpenShift Template
- 프로젝트 혹은 애플리케이션 단위로 빌드배포 Java Option 등 표준화 할 수 있음.
  - Container Resource, Git / Maven URL 등
- OpenShift 혹은 K8S에 대한 지식이 없이도 배포할 수 있는 방안

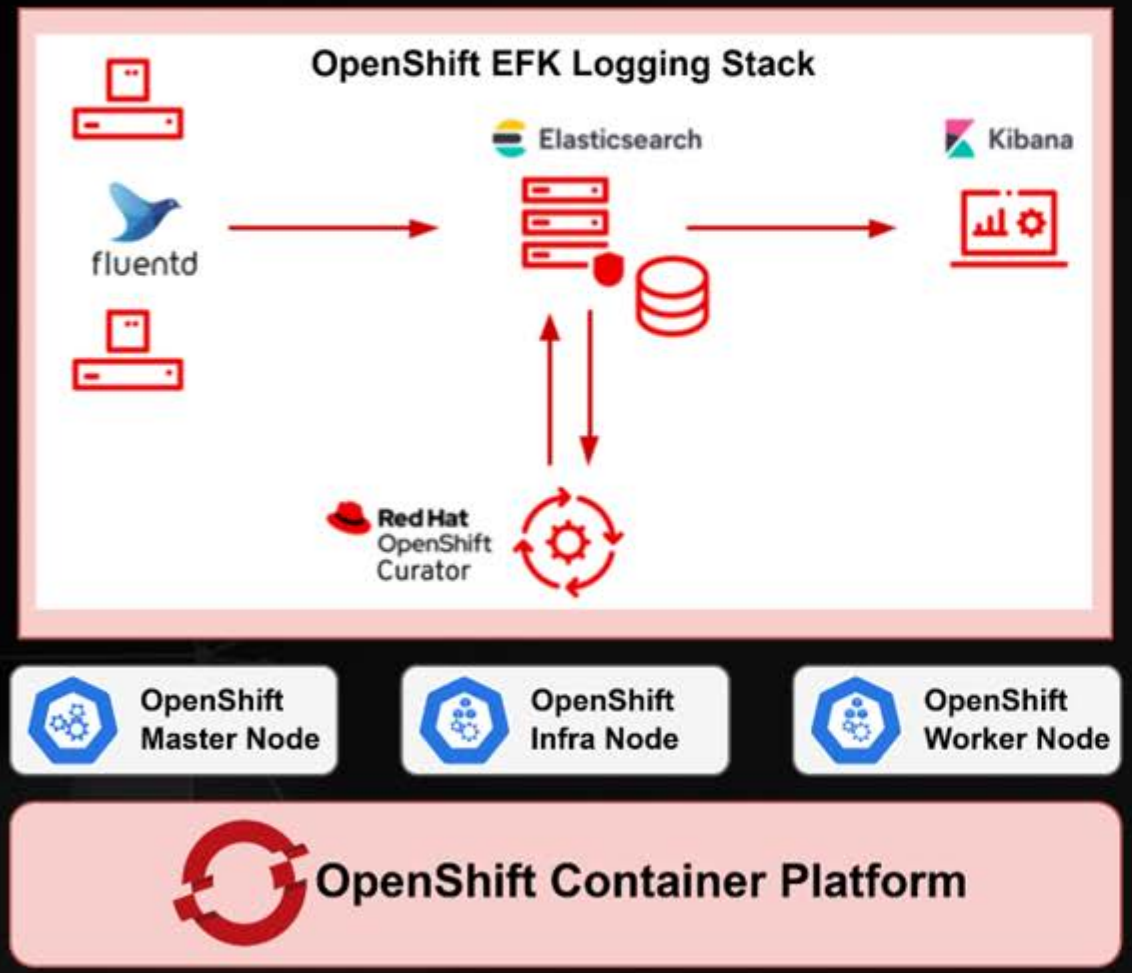


OpenShift Template 카탈로그 리스트

- OpenShift 에서는 각 서비스들을 프로비저닝 할 수 있는 템플릿을 제공
- CI/CD, Databases, Languages, Middleware, 기타 항목의 총 79 개의 템플릿을 제공

CI/CD	Databases	Languages	Middleware	Etc..
jenkins	PostgreSQL MariaDB MySQL	Java Ruby PHP Python Node.js Dancer	JWS HTTPD A-MQ 3-scale Wildfly BPM BRMS Keycloak JDG Fuse Data Virtualization	Nginx Redis

Cloud Native Logging Stack, EFK 제공



Elasticsearch + Fluentd + Kibana Logging Stack

- 컨테이너 인프라 환경, Cloud Native 환경 같은 경우 로그 집중화 스택이 필요함
  - 수 많은 Container 기동
  - Container 삭제시 로그데이터 삭제
- Cloud Native에 적합한 로그 스택, EFK
  - Elasticsearch : 로그 데이터 저장소
  - Fluentd : 로그 데이터 전송
    (logstash 대체하는 경우도 있음)
  - Kibana : 로그 데이터 시각화
  - Curator : 로그 메타데이터 rotate
- K8S 운영시 자체적으로 클러스터에 통합해야함.

3rd Party 시스템의 간단한 설치 구성 지원, OPERATOR HUB

openmaru

- 3rd Party 시스템을 OperatorHub 를 통해 손쉽게 설치와 구성
- AI/Machine Learning, Integration & Delivery, Logging & Tracing, Networking 등의 18 가지 항목의 426 가지 Operator 를 제공

etcd Prometheus kafka dynatrace

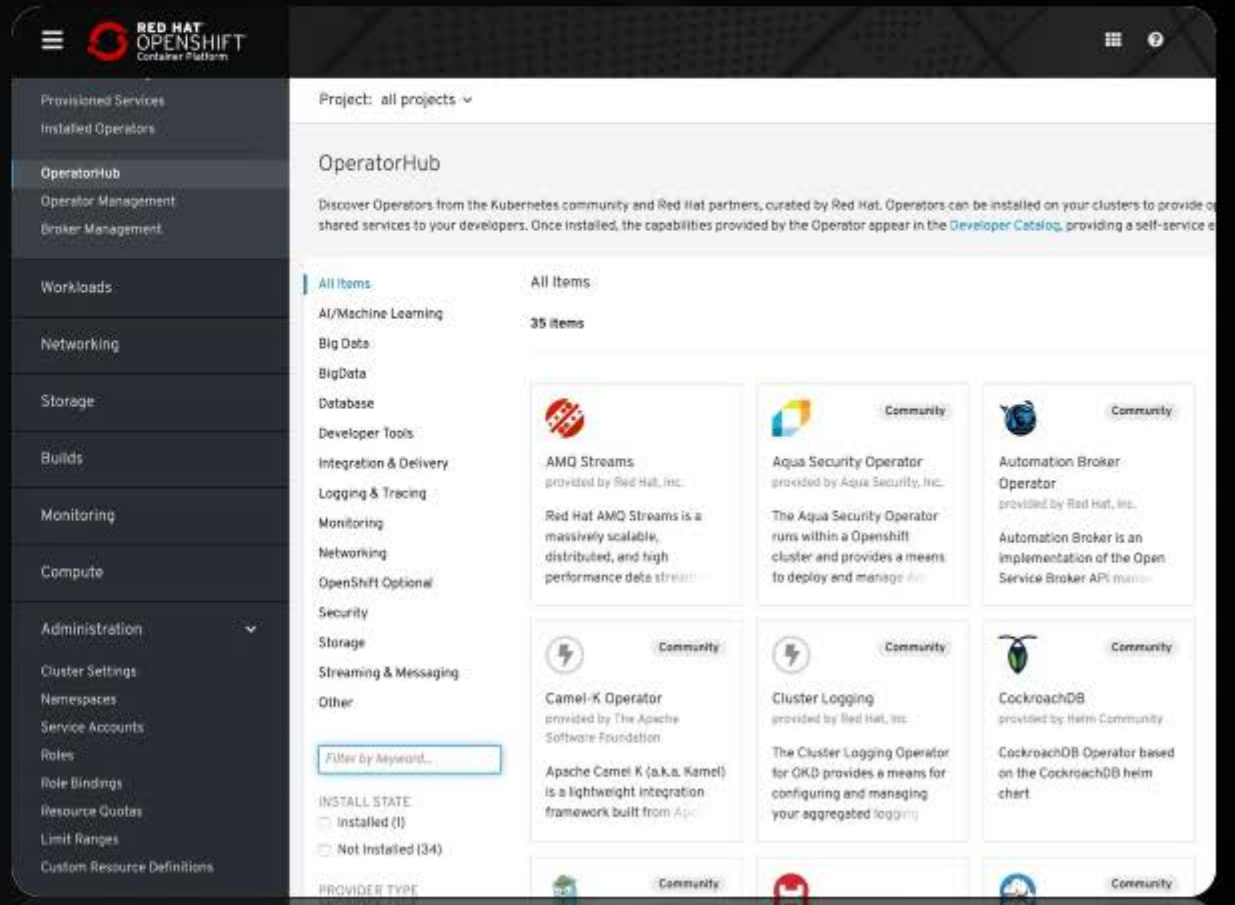
Couchbase StackRox elasticsearch

JAEGER TEKTON redis fluentd

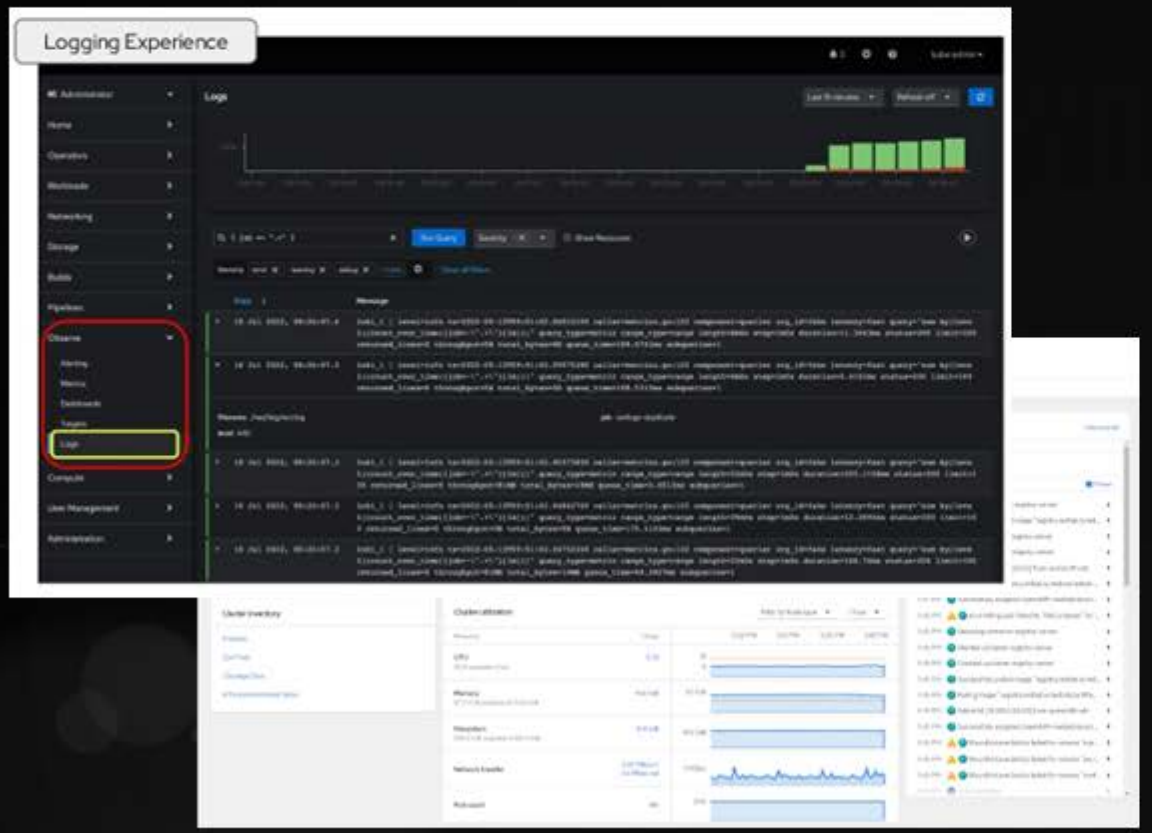
mongoDB. STRIMZI argo kibana

cassandra CRUNCHY Enterprise PostgreSQL Spark ROOK

...and many more



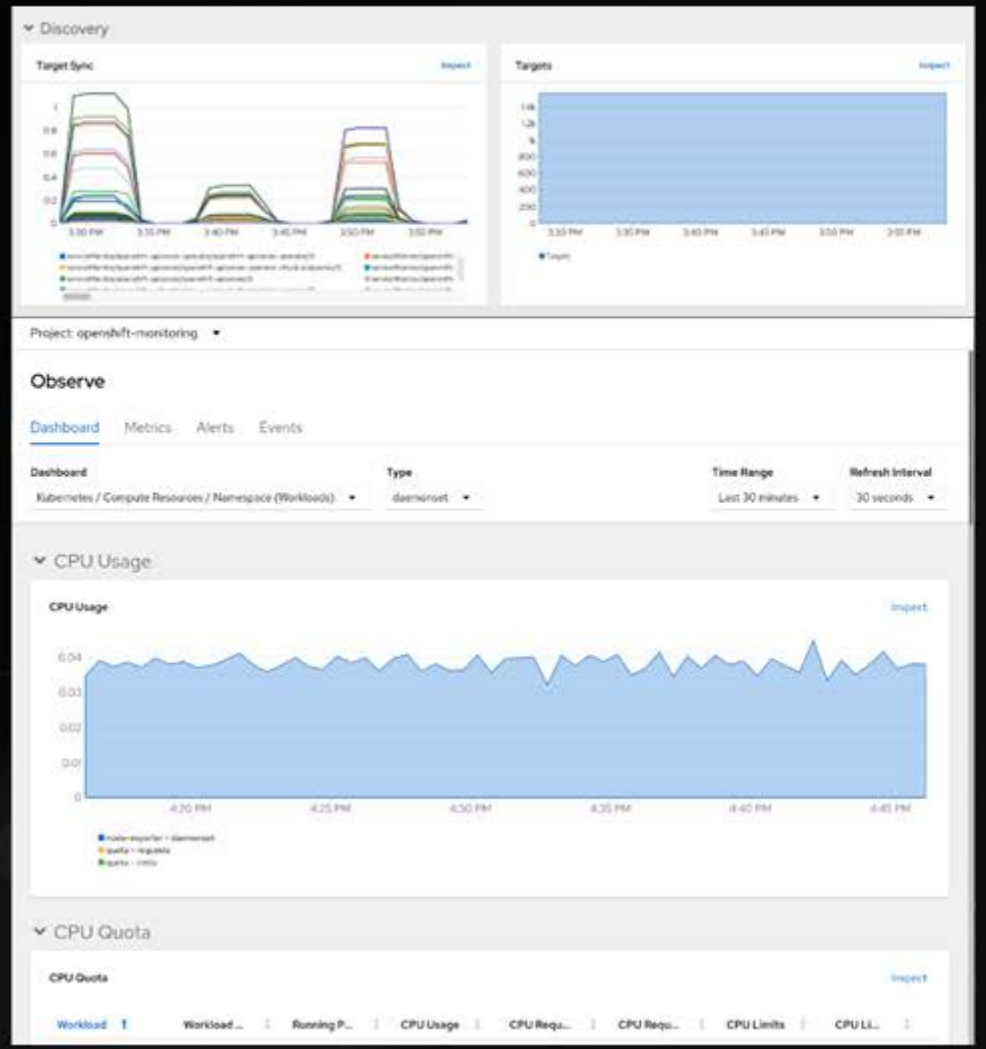
시스템 메트릭, 로그 모니터링이 통합된 Web Console 제공



OpenShift Web Console

- 웹 콘솔은 프로젝트 데이터를 시각화하고 관리 및 문제 해결 작업을 수행할 수 있는 그래픽 사용자 인터페이스를 제공
- OAuth를 통해 다른 OpenShift Web Console들과 통합 계정관리
- 시스템 모니터링이 Web Console에 통합되어 있으며, 최신버전의 경우 로깅 모니터링도 통합

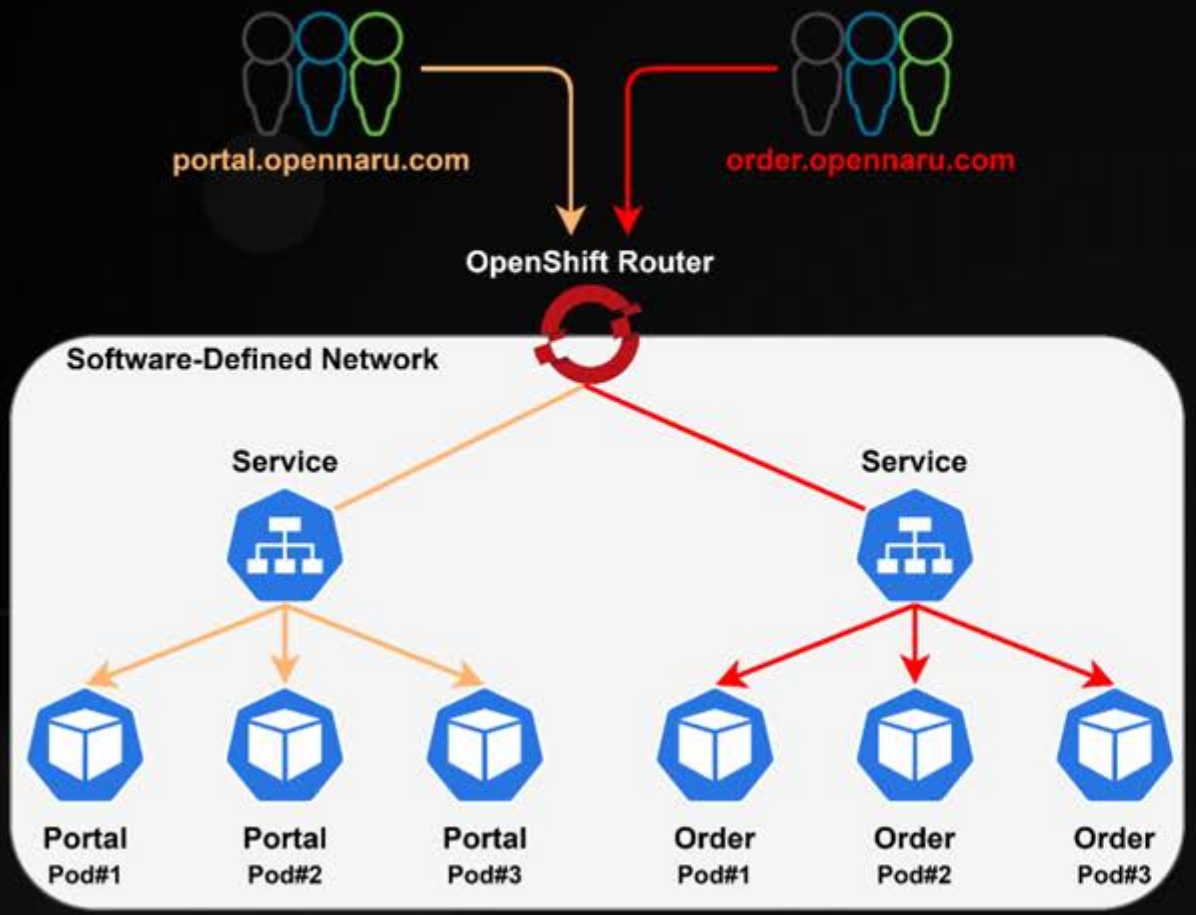
시스템 메트릭 모니터링



- **OpenShift에는 Default로 시스템 메트릭 정보들을 수집하는 Prometheus가 포함**
  - 필요에 따라 사용자가 정의한 프로젝트에 대해서 별도의 시스템 모니터링도 가능

- **수집된 메트릭 정보를 OpenShift Web Console로 확인**
  - **Administrator perspective**
    - API performance
    - etcd
    - Kubernetes compute resources
    - Kubernetes network resources
    - Prometheus
    - USE method dashboards relating to cluster and node performance
  - **Developer perspective**
    - CPU usage
    - Memory usage
    - Bandwidth information
    - Packet rate information

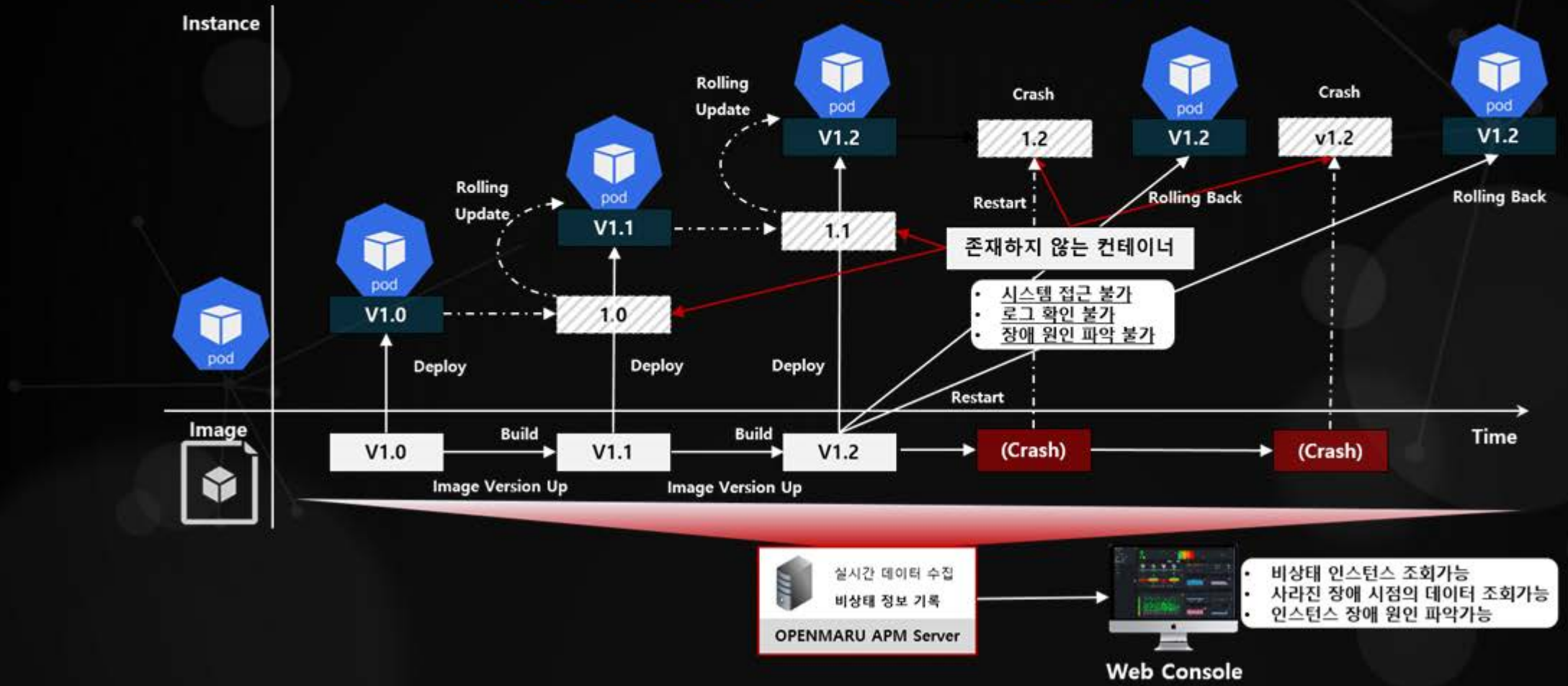
컨테이너 환경의 애플리케이션 노출 방안, OpenShift Router



- K8S와 OpenShift 같은 컨테이너 인프라 환경은 SDN으로 네트워크가 구성됨.
  - SDN 네트워크는 Cluster 외부에서 접속 할 수 없음.
- 애플리케이션(Pod)에 접속할 수 있도록 설정하는 것이 Ingress
  - OpenShift의 경우 Router
  - Domian Name 기반으로 애플리케이션(Pod)를 찾아가는 방식
  - Weight 설정으로 Service 별 트래픽 부하 조절 가능
- K8S의 경우 별도로 Ingress를 구성 및 유지보수 해야함

PaaS 환경의 비상태 WAS 인스턴스에 대한 모니터링 기능

- 컨테이너가 중지된 후 장애원인을 파악을 위한 정보를 파악할 수 있어야 함.
- 존재하지 않는 컨테이너 즉, 장애 혹은 업데이트로 인한 과거의 컨테이너의 정보를 분석 가능해야 함.



기업에서 필요한 Kubernetes 기술지원

openmaru

장기 수명주기

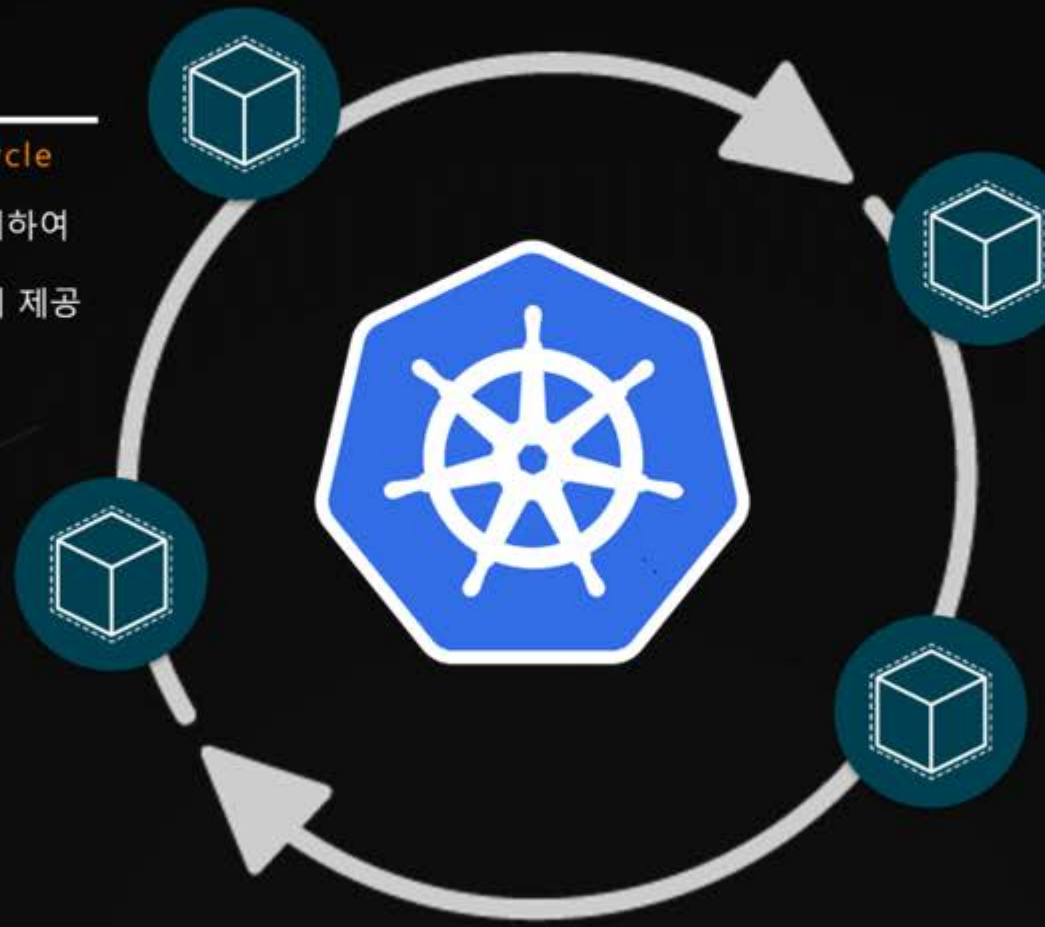
Predictable and long lifecycle

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

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



교육

Training

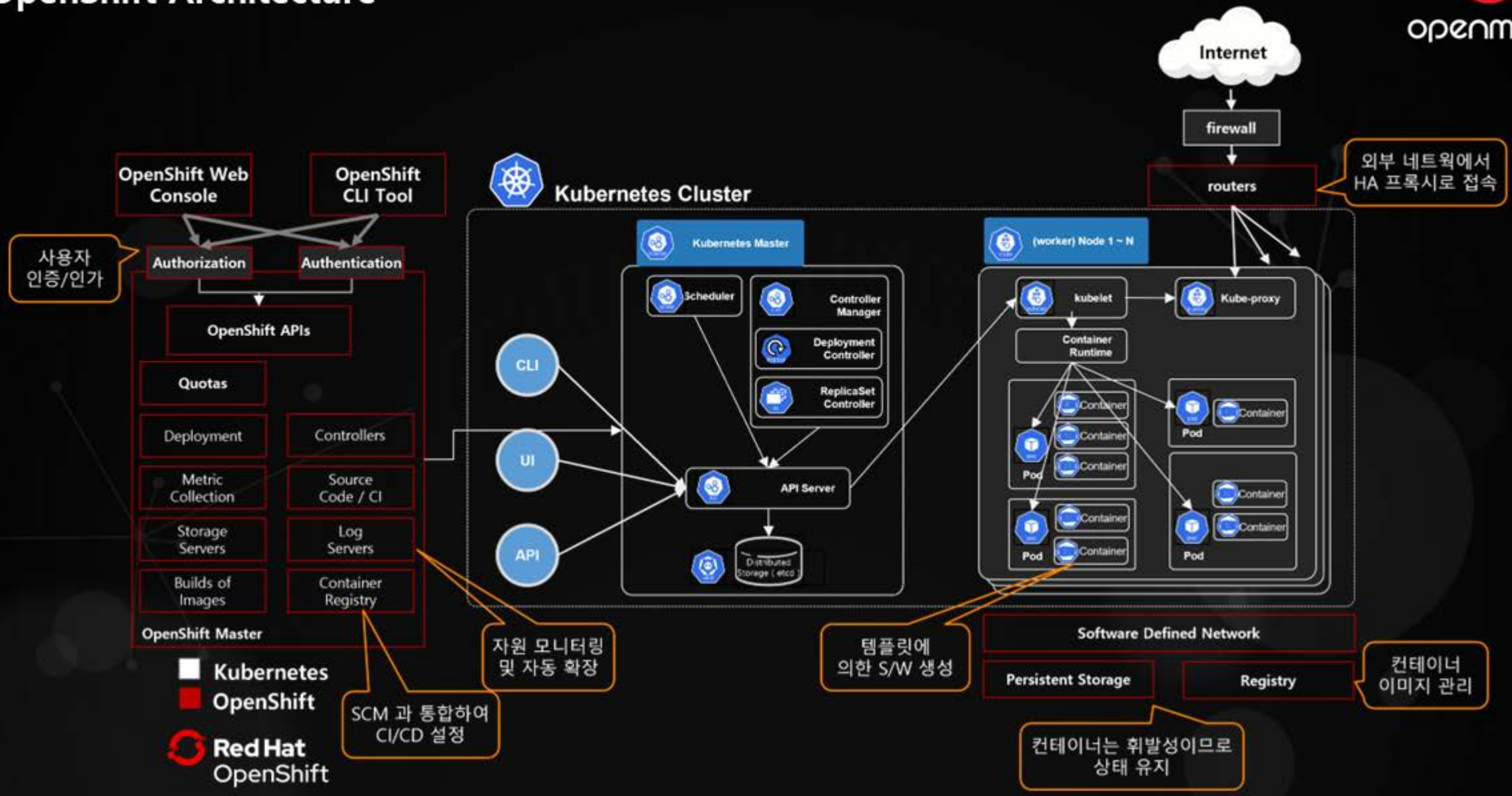
장기적인 지원 뿐만 아니라 제품 교육과 자격증 제도를 제공하여 기술 내재화를 통한 서비스의 지속적인 운영을 지원

파트너 인증

Certification

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

OpenShift Architecture



Kubernetes와 OpenShift의 비교 요약

openmaru

Kubernetes	비교 항목	OpenShift
K8S Community 활용 혹은 자체적으로 해결	기술지원	24/7 Red Hat 기술지원
일부 자동 생성되나 이후 관리 필요	인증서 관리	자동 생성, 자동 갱신
보안에 취약한 컨테이너 이미지 활용 가능성	컨테이너 이미지	Quay.io, Red Hat Registry를 통한 신뢰할 수 있는 컨테이너 이미지 제공
Runtime을 자체적으로 유지보수	Runtime 관리	플랫폼에 미들웨어, OS 포함되어 기술지원 제공
별도의 관리 시스템이 필요	계정관리	OAUTH 시스템 제공
기존 환경과 같이 많은 수의 보안 프로그램 필요	Host OS 보안	Compliance OS(CoreOS) 제공
컨테이너 실행 보안에 대한 방안 필요	컨테이너 보안	Security Constraints Context(SCC) 제공
서비스 라우팅을 위한 방안 필요	서비스 라우팅	OpenShift Router 제공
업그레이드 의존성 및 자체적인 수행	Cluster Upgrade	OTA 업그레이드, Disconnected 업그레이드, 업그레이드 의존성 리스트 지원
별도의 빌드배포 Pipeline 구성이 필요	빌드/배포	OpenShift Source To Image, Template 지원
시스템, 로그 등 모니터링 스택이 필요	모니터링	시스템 모니터링, 로그 모니터링 설치 지원

제품 / 서비스에 관한 문의

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