

커뮤니티 오픈소스를 활용한 금융, 공공권의 IaaS & PaaS 구축 사례

클라우드 마이그레이션 팀
김호진 상무



Contents

01. 커뮤니티 오픈소스와 재단
02. OIF/CNCF 프로젝트 사용하기
03. 커뮤니티 오픈소스를 활용한
금융, 공공 IaaS & PaaS 구축 사례

01

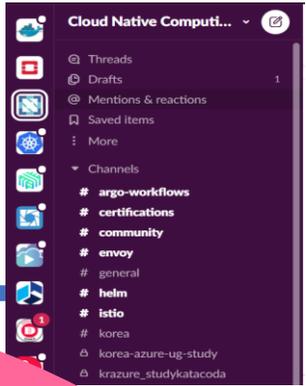
커뮤니티 오픈소스와 재단



OIF(Open Infrastructure Foundation (구 openstack Foundation))

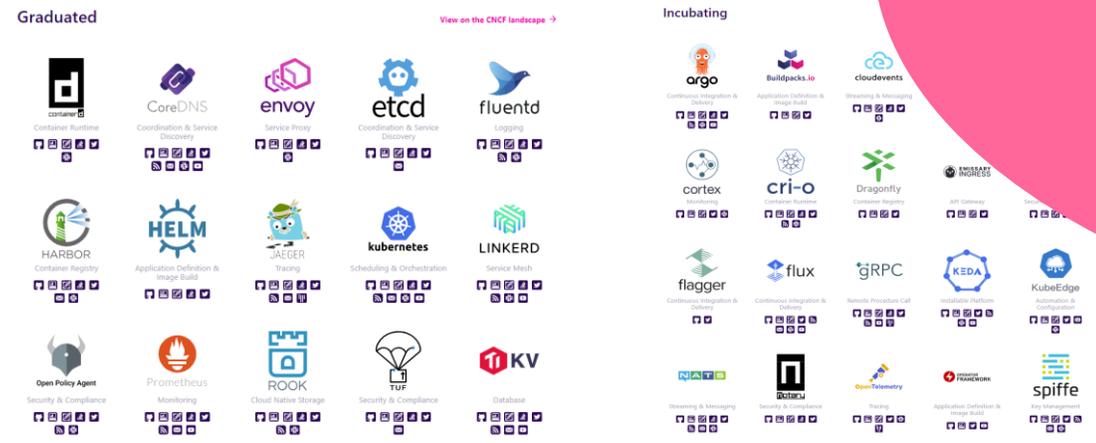


인프라 벤더 주도의 오픈소스 프로젝트 오픈스택

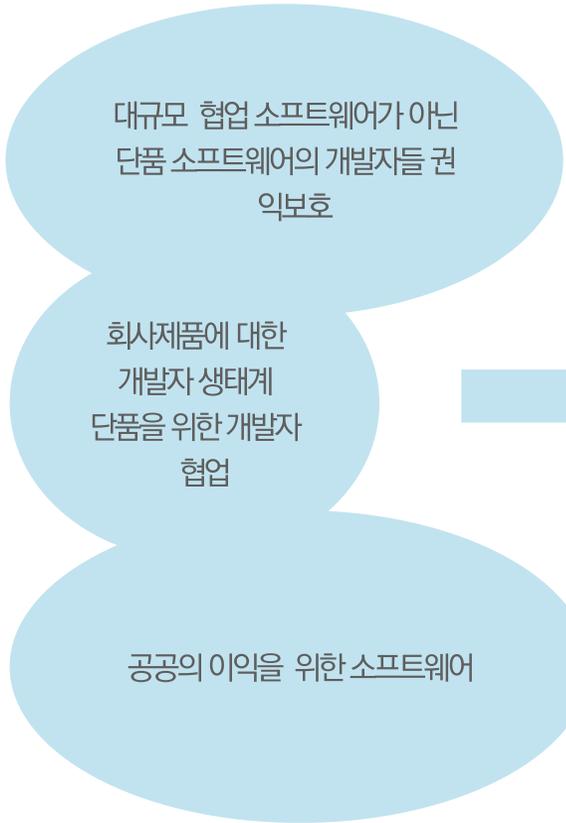


1. 어떤 특정 벤더가 유지보수 하는것이 불가능함
2. 특정 벤더의 제품을 추가할 경우, 벤더 락인이 걸림
3. 벤더 락인이 걸릴 경우 전체 제품의 안정성과 업그레이드 담보 불가

CNCF(Cloud native computing Foundation)



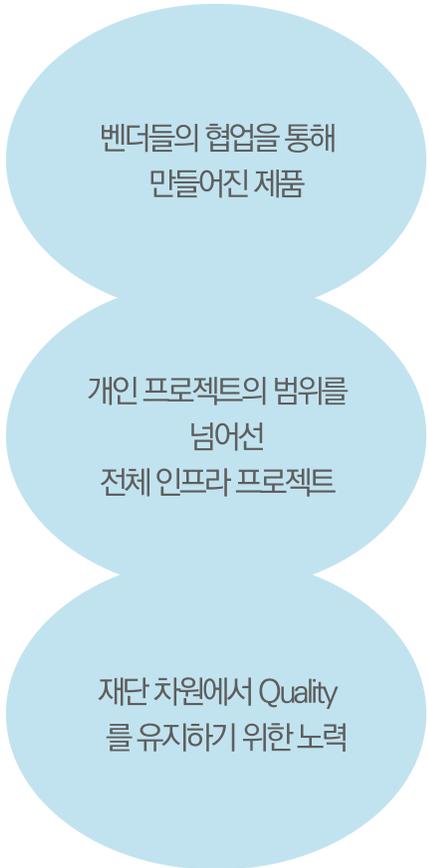
오픈소스 역사상 가장 많은 업체가 참여한 대규모 인프라 프로젝트



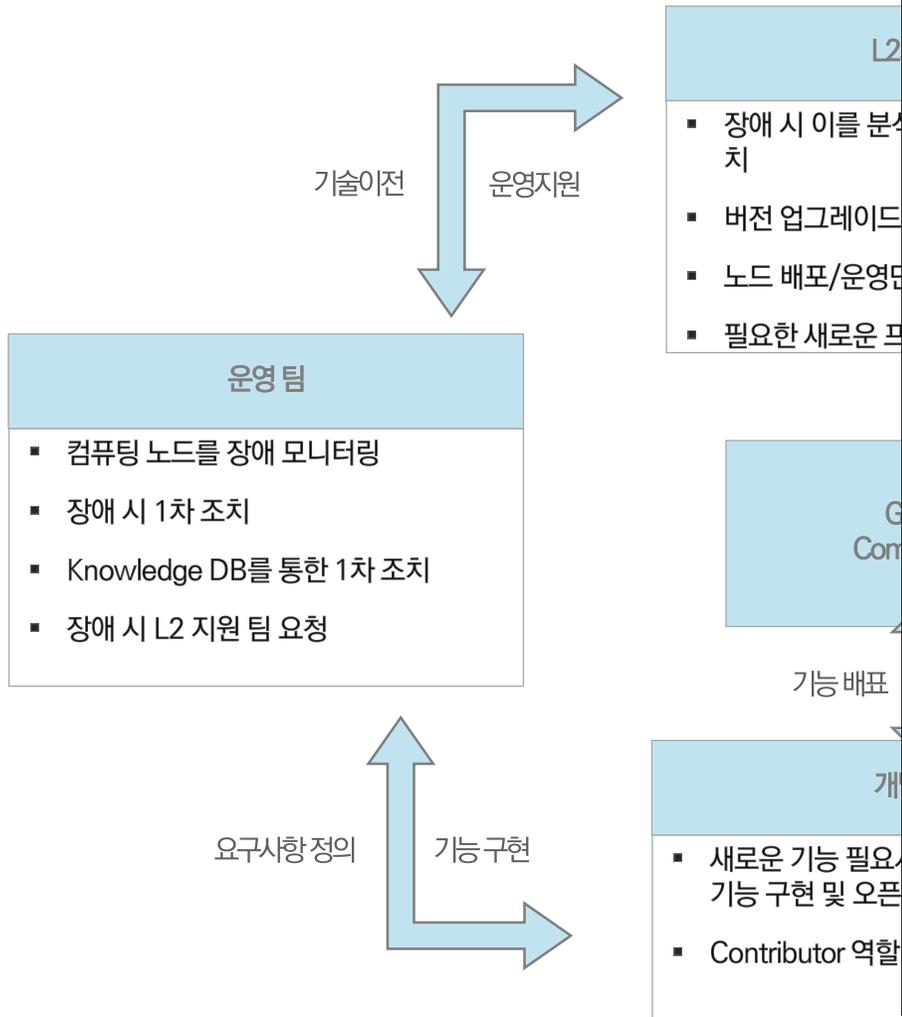
- 2010년 NASA가 클라우드 컴퓨팅 솔루션을 오픈하기로 결정
- 클라우드 인프라오픈소스에 열광한 대규모 벤더의 참여
- 자신의 제품을 클라우드 인프라에 맞추려는 노력들
- 핵심 프로젝트



- 구글이 쿠버네티스에 대한 통제권을 양도 하고 이를 리눅스 재단에서 운영하게 될 CNCF(Cloud Native Computing Foundation)라는 새로 설립된 재단에 기부



팀을 만들어 글로벌하게 소통하는 회사 → 운영 필요 인력 및 자



Linkerd

- Threads
- Mentions & reactions
- Slack Connect
- More
- Channels
 - # announcements
 - # linkerd2
 - Add channels
- Direct messages
 - Slackbot
 - Ho-Jin Kim you
 - Add teammates

Threads

Ho-Jin Kim 2 months ago

Hi guys. In istio, we used to have a solution as the envoy for getting dedicated ip which is used for firewall .

Are there any solution for linkerd.?

How about to use envoy for only egress with linkerd?

It is productionenv. And we cannot adopt poc egress (edited)

Matei David 2 months ago

Hey @Ho-Jin Kim, would you be able to expand? I'm not familiar with this particular feature, you'd like to get the IP of a service programatically?

You could use envoy as an egress controller (I'm not sure how it would work as opposed to something like an nginx proxy). We have a [POC on how to do egress with Linkerd](#) -- not sure you've seen it already. Linkerd will terminate TLS at an egress level, so basically:

```

+-----+ +-----+
|SVC A --> outbound-proxy| => |inbound-proxy --> egress-proxy |
+-----+ +-----+
```

Linkerd will mTLS from A to egress-proxy, egress-proxy will TLS call to external API. Linkerd only provides metrics for http calls (since we need to peek into the stream to get metrics; can't do it for an encrypted call).

We might support egress more natively in the future, but this would be after 2.11 (the next planned stable release) which will put in authz policies. (edited)

grampelberg/k8s-egress

Stars	Last updated
14	3 days ago

Added by GitHub

Ho-Jin Kim 2 months ago

Thanks for ur sincere answer. unfortunately because It's production env, we cannot test k8s-egress, I will test envoy and linkerd..Thanks

👍 1 🗨️

Matei David 2 months ago

Yup, so the k8s-egress repo I sent does this using nginx, if you follow the POC but replace nginx with envoy you might be able to get the same result 😊

✅ 1 👍 1 🗨️

02

OIF/CNCF 프로젝트 사용하기

→ Playce Cloud



■ Playce Cloud는 벤더 종속성을 모두 삭제한 100% 커뮤니티 오픈소스를 패키징 하여, 컨설팅하고, 구축하고, 운영, 장애처리 하는 노하우를 공유하고, 지원하는 솔루션입니다.

마치 자사에 오픈소스 팀이 있는 것처럼 오픈소스를 구축 / 운영하 실수 있는 노하우를 전수해 드립니다.



IaaS & PaaS 클라우드 플랫폼 PlayceCloud

☑ 컨테이너화 된 솔루션



PlayceOpenStack

오픈스택을 중심으로 패키징 한
프라이빗 IaaS 솔루션



PlayceKube

쿠버네티스를 중심으로 패키징 한
프라이빗 PaaS 솔루션

가장 많이 사용하는 아래 9가지 패키징을 기본으로 구성



인프라수명관리



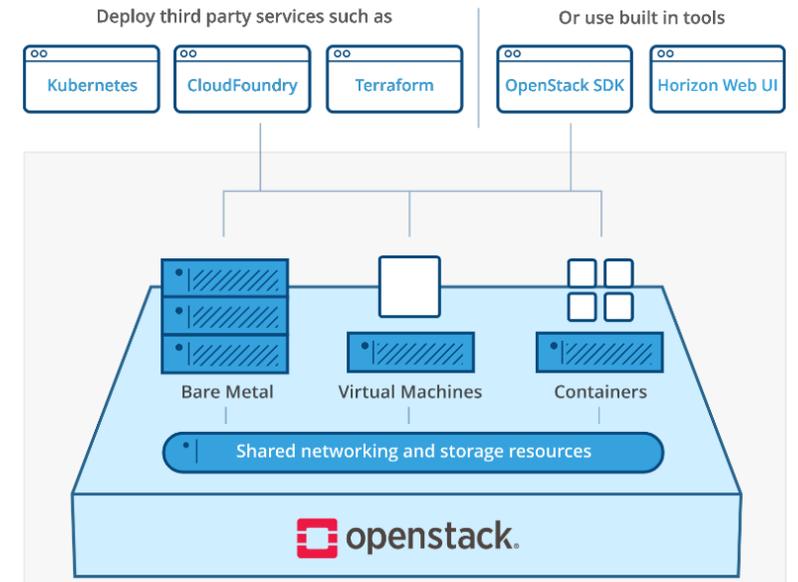
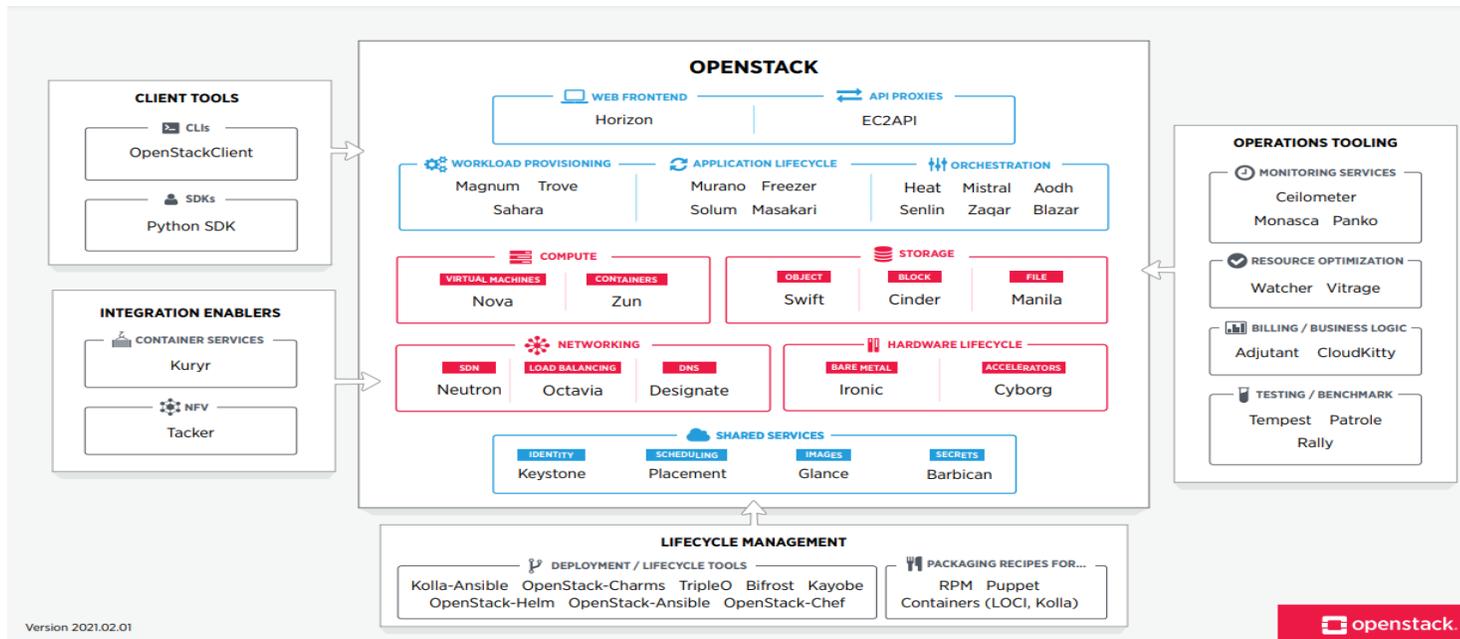
가상화컨테이너



모든 인프라 관리



게이팅 CI/CD



Landscape: <https://www.openstack.org/software/>

오픈스택은 점점 더 큰 규모의 인프라에 적합한 구조로 변화되고 있음. (SMB보다는 Enterprise에서 활용도가 높음)
 컴퓨팅 8452대 서버에 3만5천개의 VM / 그리고 개별 서버 3592대로 운영중인 사이트.

Activity Log



Surya Seetharaman (CERN)

20 Aug 2019 20:00:03 UTC in nova

Blueprint "Support server power state update through external event" (nova-support-instance-power-update)

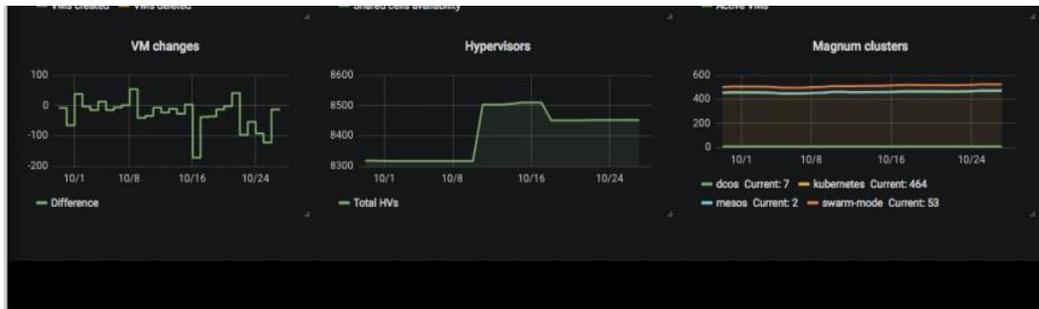
During the regular power sync between ironic and nova, physical instances going down will be marked down in nova's DB. However, physical instances coming up "unexpectedly" (via IPMI or power button) will be shut down again if they are marked as SHUTDOWN in nova. This can cause operational issues, e.g. if there was a power outage or when doing system repairs.

This blueprint proposes to make the power sync "source of truth" configurable, in particular to allow the physical instance to be the source of truth (and make nova update its DB rather than enforcing the DB state onto the physical instance).

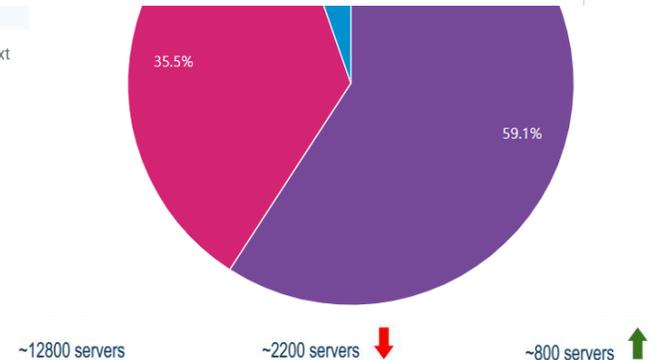
The basic idea is to add a "power-update" option/event to the existing os-server-external-events nova API, and then add code to ironic to call that API when a node changes power state and comes back-up.

Priority: Undefined

Status: Complete (Approved, Implemented)



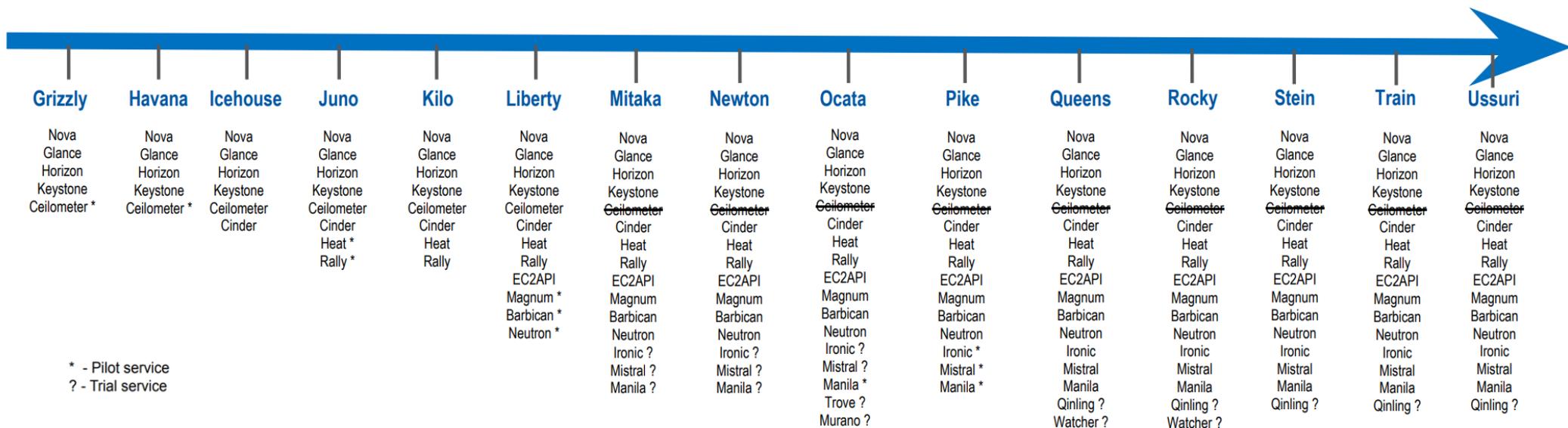
Showing 1 to 3 of 3 entries



■ 현재 오픈스택 서비스 프로젝트는 아래와 같으며 모두 42개의 프로젝트로 세분화됨

adjutant	aodh	barbican	blazar	ceilometer	cinder	cloudkitty	cyborg	designate	ec2-api	freezer	glance
heat	horizon	ironic	karbor	keystone	magnum	manila	masakari	mistral	monasca-api	monasca-events-api	
murano	neutron	nova	octavia	panko	placement	qinling	sahara	searchlight	senlin	solum	storlets
swift	tacker	trove	vitrage	watcher	zaqar	zun					

• 42개의 현재 프로젝트 중 필요한 프로젝트를 찾아서, 이를 적용하는 노력 필요 → CERN은 15개 프로젝트로 인프라를 운영 중



■ 기준 : Are vulnerability issues managed by the OpenStack security team?

• Playce OpenStack 기본 패키징

#	Code	서비스
1	Horizon	Dashboard
2	Keystone	인증
3	Neutron	네트워크
4	Cinder	블록 스토리지
5	Nova	컴퓨팅
6	Glance	이미지

• Playce OpenStack 추가 패키징

#	Code	서비스
7	Ironic	Bare Metal 프로비저닝
8	Manila	Shared File System
9	Octavia	loadbalancer



vulnerability:managed



vulnerability:managed

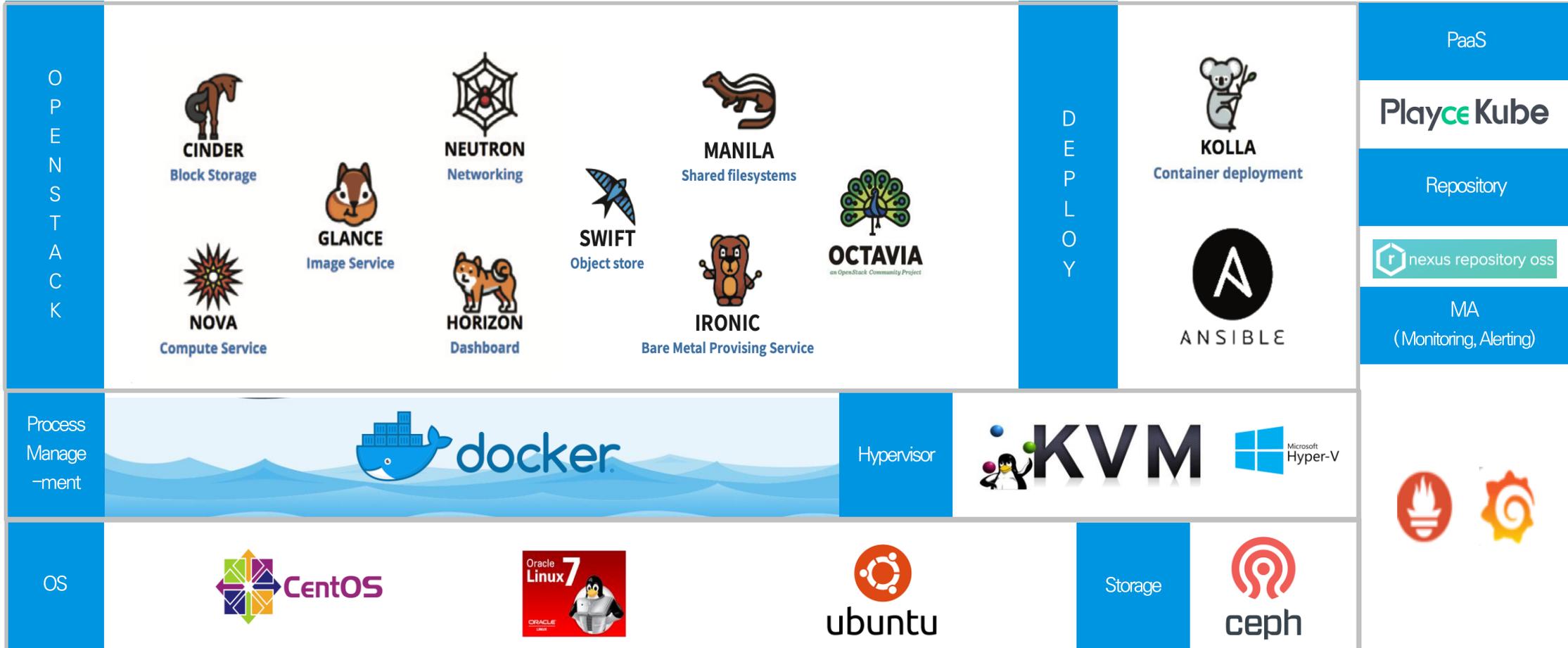
This tag is part of the vulnerability-classification system for vulnerability reporting and tracking across project deliverables. **vulnerability:managed** indicates that a deliverable's vulnerability report reception and disclosure are handled directly by the OpenStack Vulnerability Management team (VMT).

Application to current deliverables

- [Barbican \(Key Manager service\)](#): barbican, python-barbicanclient
- [Cinder \(Block Storage service\)](#): cinder, os-brick, python-cinderclient
- [Glance \(Image service\)](#): glance, glance-store, python-glanceclient
- [Heat \(Orchestration service\)](#): heat, python-heatclient
- [Horizon \(Dashboard\)](#): horizon
- [Keystone \(Identity service\)](#): keystone, keystonemiddleware, python-keystoneclient
- [Neutron \(Networking service\)](#): neutron, neutron-lib, python-neutronclient
- [Nova \(Compute service\)](#): nova, python-novaclient
- [Oslo \(Common libraries\)](#): castellan, oslo.config
- [Sahara \(Data Processing service\)](#): python-saharaclient, sahara, sahara-dashboard, sahara-extra, sahara-image-elements, sahara-plugin-ambari, sahara-plugin-cdh, sahara-plugin-mapr, sahara-plugin-spark, sahara-plugin-storm, sahara-plugin-vanilla
- [Swift \(Object Storage service\)](#): python-swiftclient, swift
- [Trove \(Database service\)](#): python-troveclient, trove

출처: <https://governance.openstack.org/tc/reference>

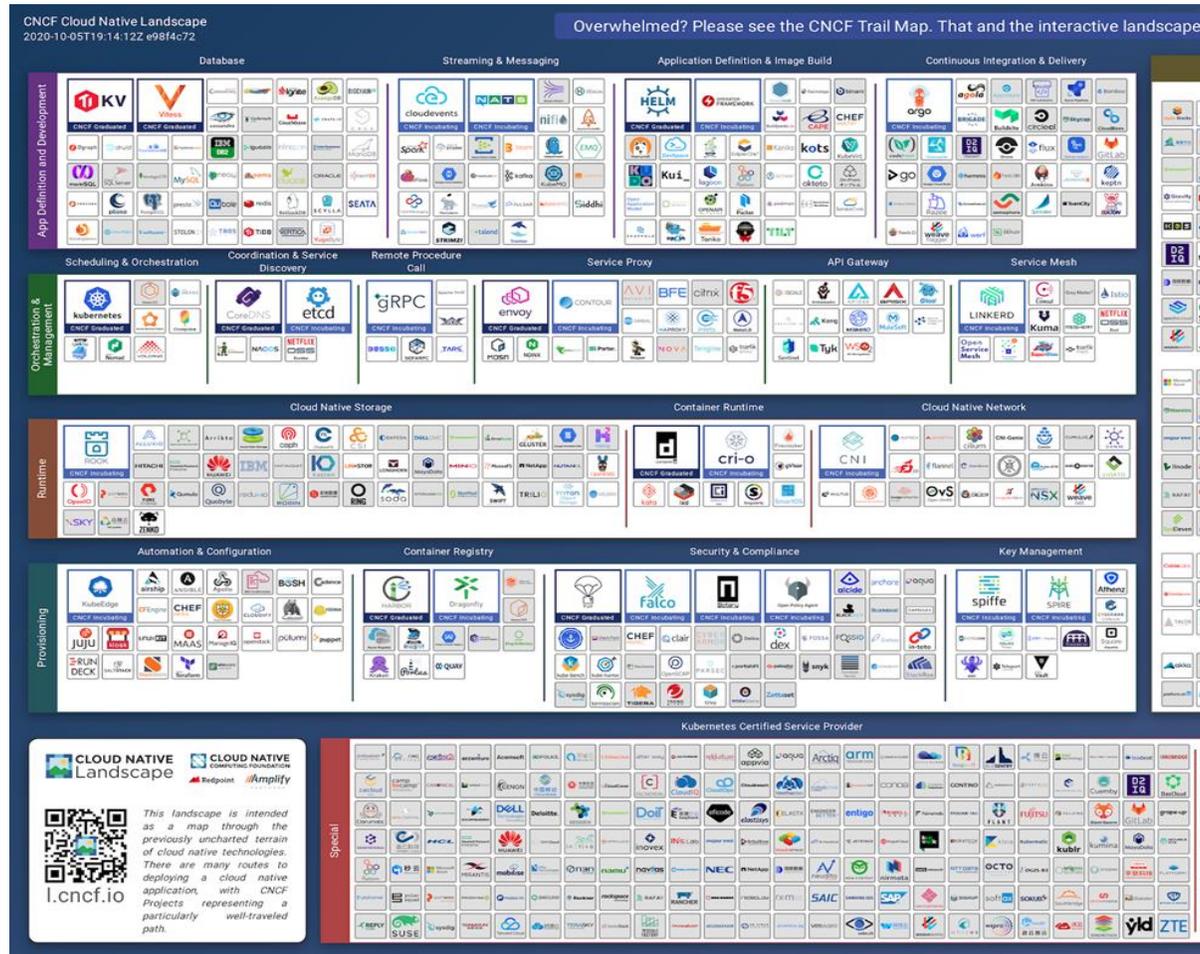
Playce OpenStack은 벤더 종속성에서 탈피하고 IaaS에서 필요한 오픈소스 패키지를 추가하여, 안정적인 인프라를 제공해 주기 위한 IaaS 솔루션임



필요시 요청할 수 있는 프로젝트 내용

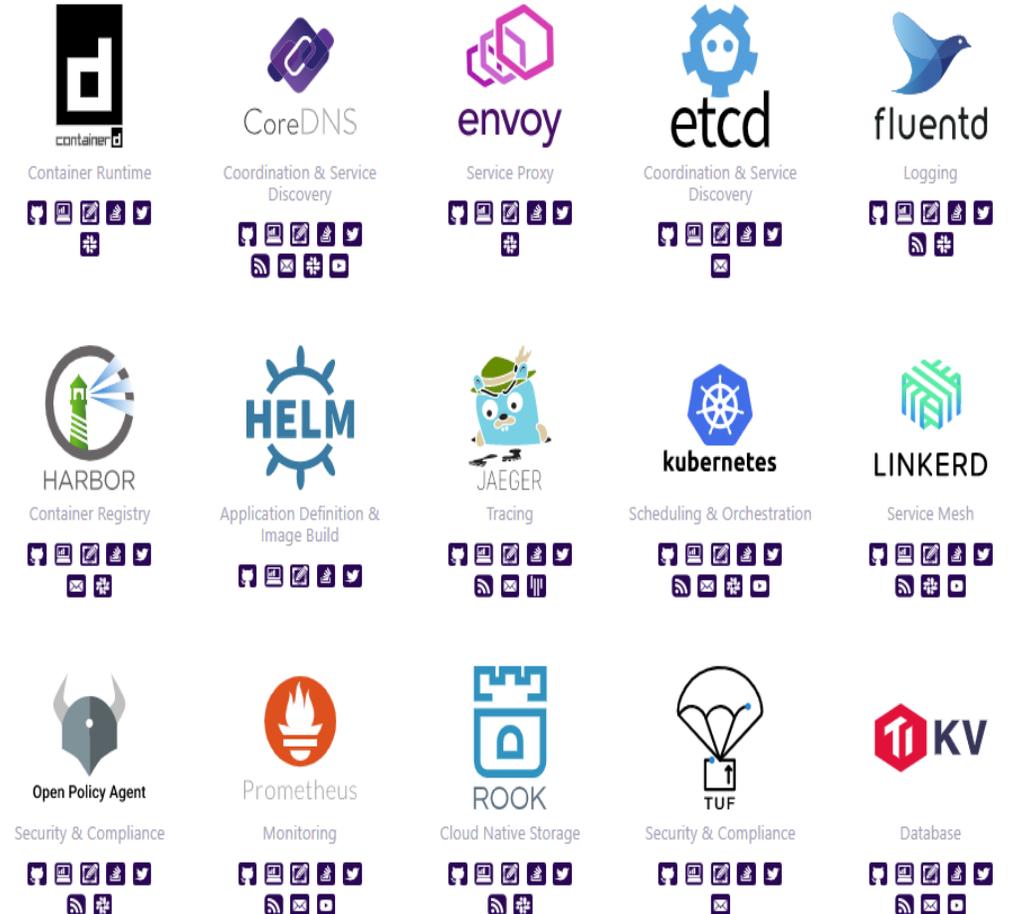
	Rally	Benchmarking tool Openstack 성능 분석 및 벤치 마킹 도구
	EC2API	EC2 API Openstack Nova 의 Amazon EC2 호환 API 제공
	Magnum	Container Orchestration Engine Provisioning Kubernetes 과 같은 Container Orchestration. Heat 를 사용하여 OS 이미지를 관리함
	Barbican	Openstack Key Manger Service. 암호, 암호화 키, X.509 인증서 그리고 raw binary data 에 보안을 제공함
	Mistral	Workflow Service. 실행 순서, 병렬 처리, 동기화 및 고가용성 처리 (Yaml 기반)

CNCF에서 오픈소스, 벤더 중립적인 프로젝트 생태계를 정리하고 이를 도표화 함



Graduated

View on the CNCF landscape →



Landscape: landscape.cncf.io/

CNCF (재단)의 Cloud Native 프로젝트들

-- Cloud Native Trail Map

클라우드 네이티브 여정에 대한 개요를 제공

- Github 300개 이상의 클라우드 네이티브 프로젝트를 기반으로 정리
- 오픈소스 소프트웨어의 상용버전은 제외

1. Containerization
2. CI/CD
3. Orchestration & Application Definition
4. Observability & Analysis
5. Service Proxy, Discover, & Mesh
6. Networking, Policy, & Security
7. Distributed database & storage
8. Streaming & Messaging
9. Container Registry & Runtime
10. Software Distribution

Trail Map: l.cncf.io

1. CONTAINERIZATION

- Commonly done with Docker containers
- Any size application and dependencies (even PDP-11 code running on an emulator) can be containerized
- Over time, you should aspire towards splitting suitable applications and writing future functionality as microservices

3. ORCHESTRATION & APPLICATION DEFINITION

- Kubernetes is the market-leading orchestration solution
- You should select a Certified Kubernetes Distribution, Hosted Platform, or Installer: cncf.io/ck
- Helm Charts help you define, install, and upgrade even the most complex Kubernetes application



5. SERVICE PROXY, DISCOVERY, & MESH

- CoreDNS is a fast and flexible tool that is useful for service discovery
- Envoy and Linkerd each enable service mesh architectures
- They offer health checking, routing, and load balancing



7. DISTRIBUTED DATABASE & STORAGE

When you need more resiliency and scalability than you can get from a single database, Vitess is a good option for running MySQL at scale through sharding. Rook is a storage orchestrator that integrates a diverse set of storage solutions into Kubernetes. Serving as the "brain" of Kubernetes, etcd provides a reliable way to store data across a cluster of machines. TiKV is a high performant distributed transactional key-value store written in Rust.



9. CONTAINER REGISTRY & RUNTIME

Harbor is a registry that stores, signs, and scans content. You can use alternative container runtimes. The most common, both of which are OCI-compliant, are containerd and CRI-O.



2. CI/CD

- Setup Continuous Integration/Continuous Delivery (CI/CD) so that changes to your source code automatically result in a new container being built, tested, and deployed to staging and eventually, perhaps, to production
- Setup automated rollouts, roll backs and testing
- Argo is a set of Kubernetes-native tools for deploying and running jobs, applications, workflows, and events using GitOps paradigms such as continuous and progressive delivery and MLOps



4. OBSERVABILITY & ANALYSIS

- Pick solutions for monitoring, logging and tracing
- Consider CNCF projects Prometheus, Fluentd for logging and Jaeger for Tracing
- For tracing, look for an OpenTracing-compatible implementation like Jaeger



6. NETWORKING, POLICY, & SECURITY

To enable more flexible networking, use a CNI-compliant network project like Calico, Flannel, or Weave Net. Open Policy Agent (OPA) is a general-purpose policy engine with uses ranging from authorization and admission control to data filtering. Falco is an anomaly detection engine for cloud native.



8. STREAMING & MESSAGING

When you need higher performance than JSON-RPC, consider using gRPC or NATS. gRPC is a universal RPC framework. NATS is a multi-modal messaging system that includes request/reply, pub/sub and load balanced queues. CloudEvents is a specification for describing event data in common ways.

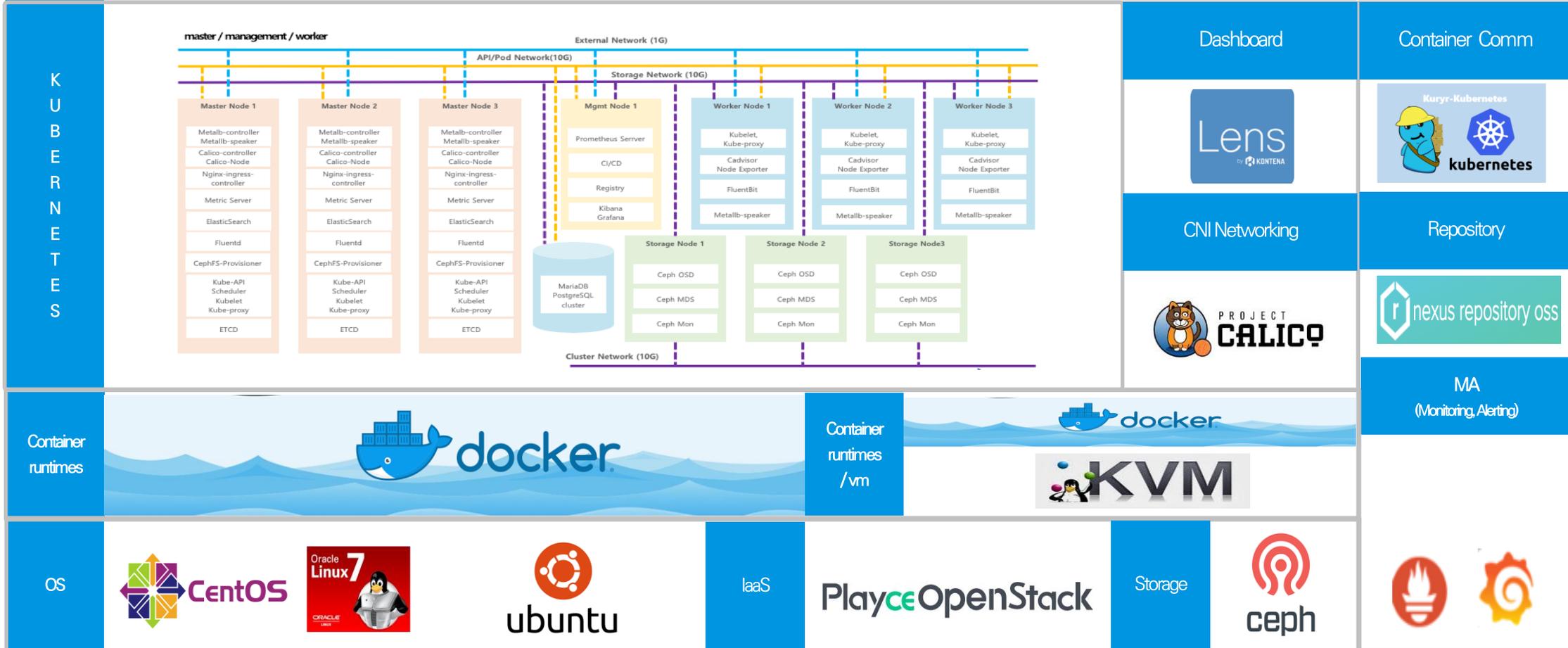


10. SOFTWARE DISTRIBUTION

If you need to do secure software distribution, evaluate Notary, an implementation of The Update Framework.

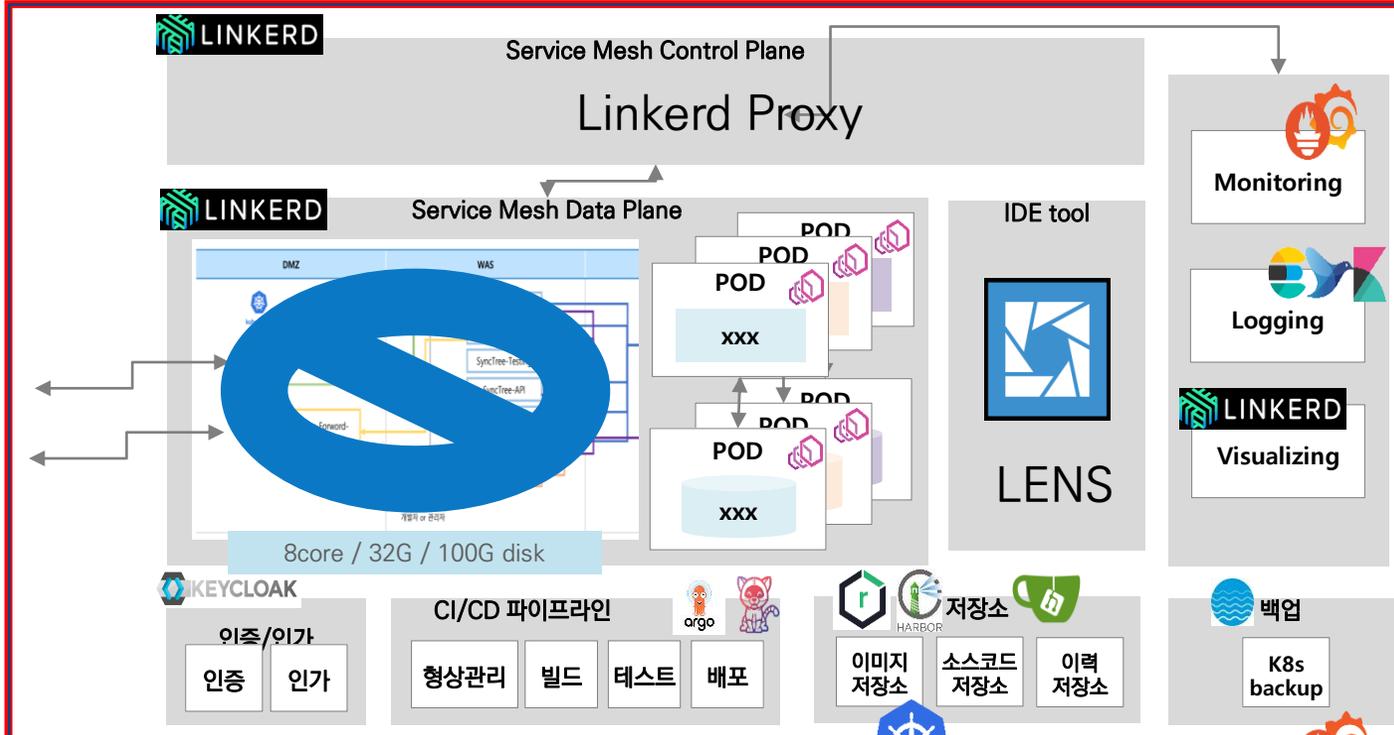


Playce Kube는 벤더 종속성에서 탈피하고 PaaS에서 필요한 오픈소스 패키지를 추가하여, 컨테이너 베이스의 애플리케이션에 최적화된 Kubernetes 솔루션입니다.

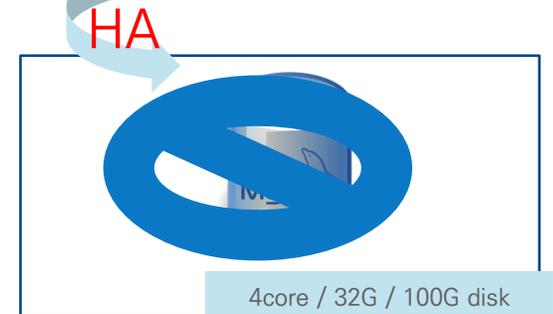


오픈소스컨설팅은 Cloud Native Trail Map에 따라 CNCF에서 검증된 incubating/graduated된 안정적인 프로젝트들을 컨설팅 및 구축을 합니다.

추가 패키징

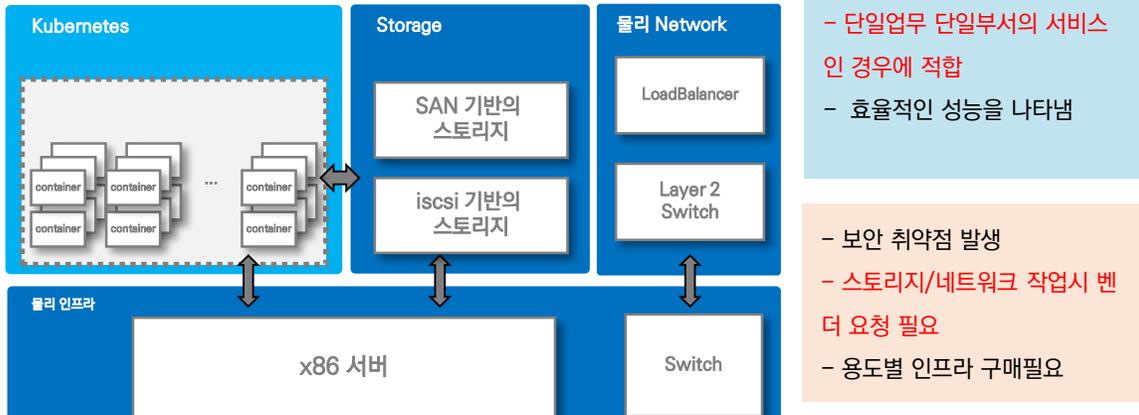


기본 패키징

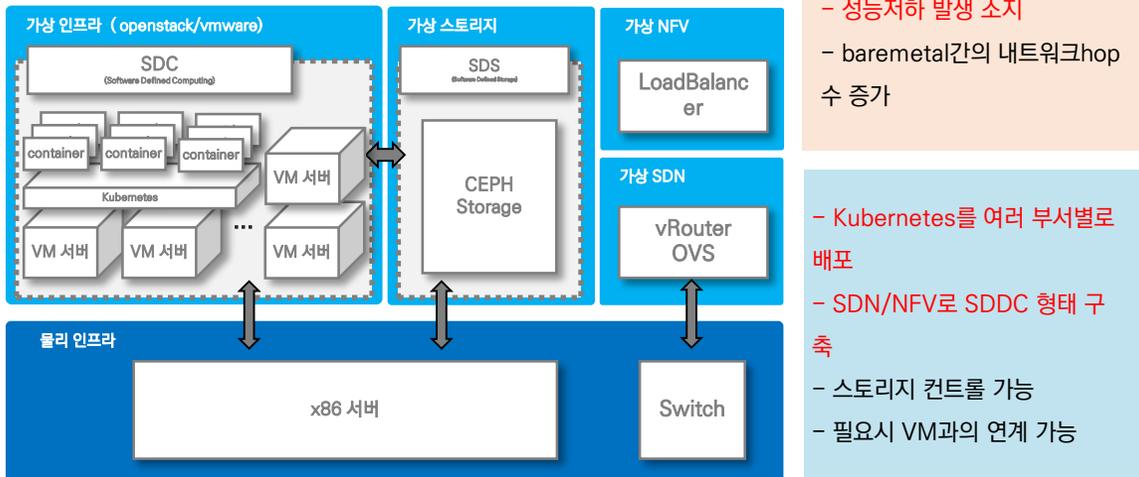


SDDC 형태의 베어메탈서버와 VM과 K8s에 최적화를 위해서 인프라 구성

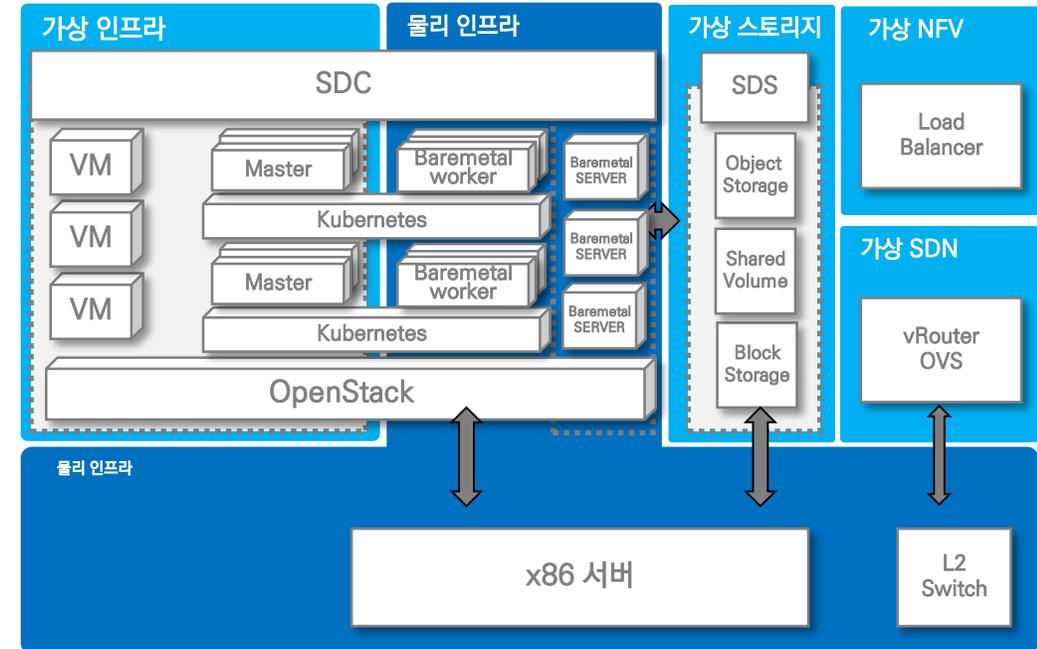
1. Legacy 형태 (기존 IaaS가 없는 상태에서 k8s 구축)



2. SDDC 형태 (cloud 구성 / 필요시 IaaS가 있는 상태에서 k8s 구축)



3. SDDC 형태 (Private cloud의 장점에 최적화된 구성)



- 오픈스택에서 모든 종류의 인프라 전체 관리 가능
- 부서별 용도별 Kubernetes 배포
- VM과의 연계하여 운영가능
- 성능/보안/신뢰성을 위한 테넌트 분리
- VM부터 컨테이너 베어메탈 전체의 라이프사이클 관리
- 하이브리드 클라우드에 최적화된 구성 환경

- Playce Cloud는 벤더 종속성을 모두 삭제한 100% 커뮤니티 오픈소스를 패키징 하여, 컨설팅하고, 구축하고, 운영, 장애처리 하는 노하우를 공유하고, 지원하는 솔루션입니다.
마치 자사에 오픈소스 팀이 있는 것처럼 오픈소스를 구축 / 운영하 실수 있는 노하우를 전수해 드립니다.



오픈소스컨설팅
OPEN SOURCE CONSULTING

IaaS & PaaS 클라우드 플랫폼

PlayceCloud

컨테이너화 된 솔루션



openstack.

PlayceOpenStack

오픈스택을 중심으로 패키징 한
프라이빗 IaaS 솔루션



kubernetes

PlayceKube

쿠버네티스를 중심으로 패키징 한
프라이빗 PaaS 솔루션

03

커뮤니티 오픈소스를 활용한
금융, 공공권의 IaaS & PaaS
구축 사례

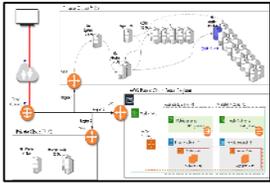
PlayceCloud

PlayceOpenStack

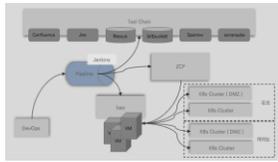
PlayceKube

2021

Playce Kube
사 하이브리드 쿠버네티스



Playce kube XX은행



Playce OpenStack/Kube TAX system



2020

PlayceCloud Ubuntu pkg 추가

Playce OpenStack/Kube 기상청 DR
Playce OpenStack/Kube 기상청 분청



Playce OpenStack/Kube
현대일렉트릭 (hybrid)



2019

CNCF 회원사 가입

Playce Kube 기상청



Community OpenStack
한국고용정보원

Playce OpenStack
씨아랩



2018

국내사례 발표 in 베트남 OpenStack day
OpenStackkorea summit 참가 및 후원
매년 해외 Summit / PTG 참가

Playce OpenStack 코인제스트
(hybrid)

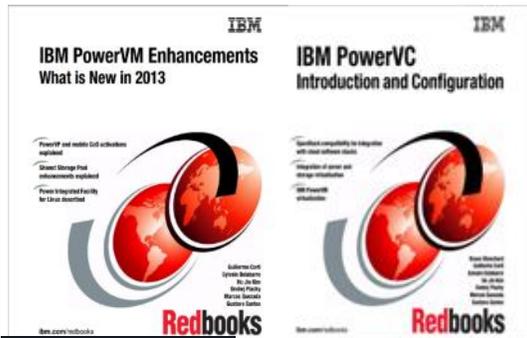


Playce OpenStack 비트탑



2014

IBM의 가상화 - PowerVM
IBM의 오픈스택 - PowerVC



2015

오픈스택 패키징



trystack

05. OSC 사내 OpenStack 구축 및 TryStack 구현 프로젝트

가상 서버에 openstack 구축 (2)

[repository 구축(1)]

[trystack module(Facebook 계정 연동, 자동 초기화) (2-)]

2016

L 공공기관



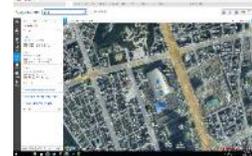
GIS DATA PORTAL 행정안전부

부동산청

기업입지지원

WIKI

Playce OpenStack 국토부 Vworld



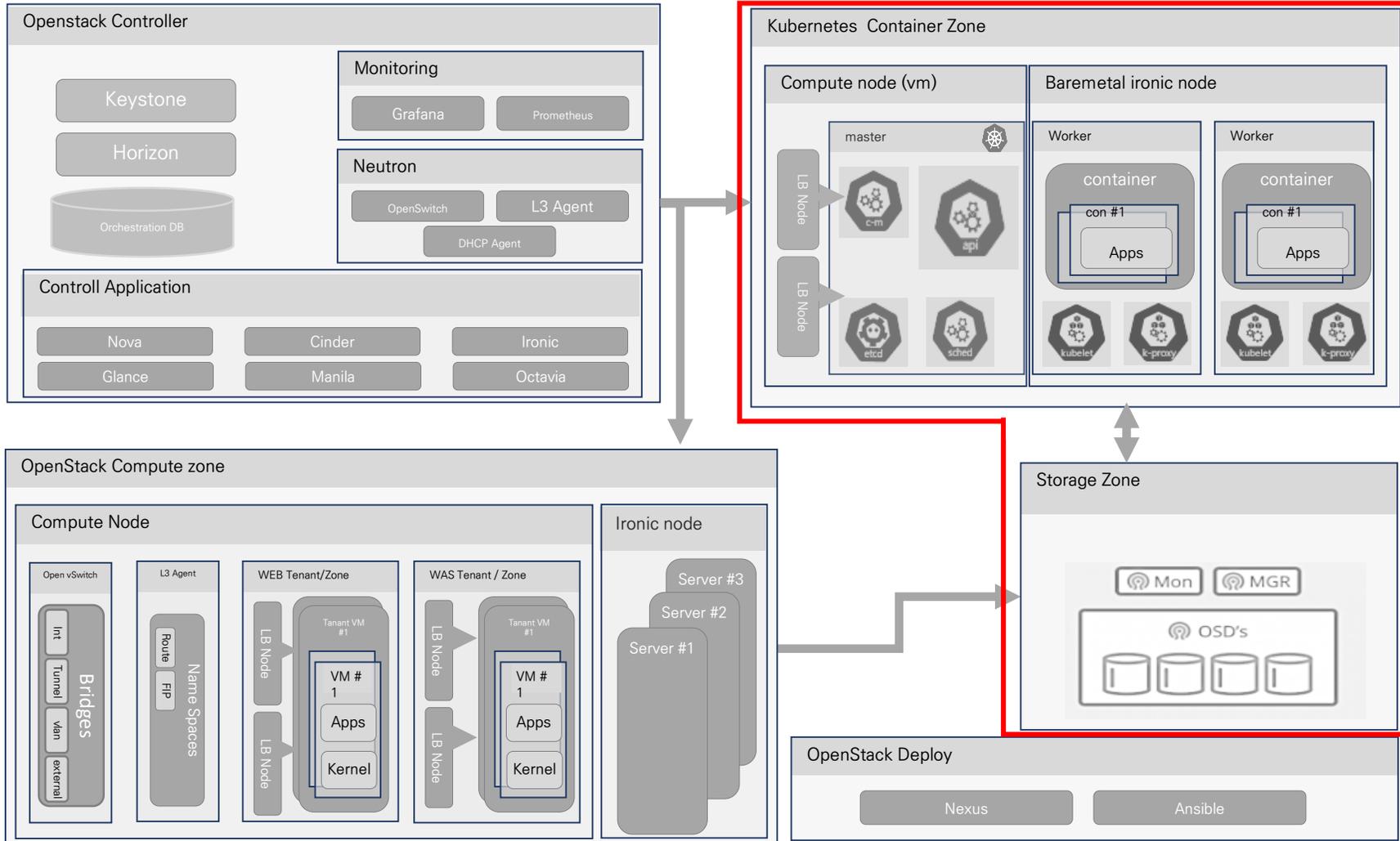
2017

Playce OpenStack 다우기술



구분	업체	내용	playce openstack	playce kube	수행기간	규모	비고
금융	XX은행	쿠버네티스와 DevOps 환경 구축		O	2021	60대	
공금융	XX	XX 클라우드 시스템 구축	O	O	2021	100대	
IT	XX	소프트웨어센타 하이브리드 클라우드		O	2021	60대	
공공	기상청	기상청 종합기상정보시스템(COMIS-5)의 오픈스택/쿠버네티스 기반 클라우드 구축	O	O	2020	250대	
금융	XX	하이브리드(AWS- 오픈스택)으로 가상화폐거래소 구축	O	O	2019	60대	
IT	XX	미란티스 오픈스택에서 자사 오픈스택으로 마이그레이션 및 컨설팅	O		2019	100대	
공공	기상청	기상청 종합기상정보시스템(COMIS-5)에 기 구축된 벤더 PaaS를 마이그레이션		O	2019	60대	
IDC	XX	GPU 가상화 서버 IaaS 서비스 구축	O		2019	50대	
금융	XX	가상화폐거래소 구축	O		2018	15대	
공공	국토부	공간정보 오픈플랫폼 오픈스택 가상화 구축 및 오픈소스 SW 도입 및 유지보수	O		2017	60대	
SMB	XX택배	배송시스템 클라우드 구축		O	2017	20대	
SMB	현대일렉트릭	인티그릭 클라우드 환경 구축	O	O	2017	30대	

VM과 컨테이너와 베어메탈등의 인프라 데이터를 모으고, 그것을 관리하며, 같은 스토리지 / 같은 네트워크를 사용하게 만들어 주는 인프라 필요



인프라 구축 내용 (선택 가능)

- 1 전체 인프라를 컨트롤할 IaaS solution (SDC* -베어메탈/VM/컨테이너 SDN* -L4 router / L4,7 LB / security SDS* -RBD / NFS(cephfs)/ Object Storage)
- 2 필요시 언제든지 확장가능한 PaaS Solution 높은 성능을 위해 baremetal에 worker구성가능
- 3 순수 커뮤니티 기반 소스로 업그레이드시 커뮤니티 소스 100% 반영 가능
- 4 오픈스택의 경우, on-line upgrade와 장애시 조치 편의성을 위해 모두 컨테이너로 패키징 필요
- 5 Database나 보안툴을 위한 관리가능한 baremetal을 관리가능
- 6 오픈소스 기반의 모니터링/ADMIN 툴 제공

* SDC (software Defined Compute)/ SDN(software Defined Network/ SDS(Software Defined Storage) / RBD(Raw Block Device)



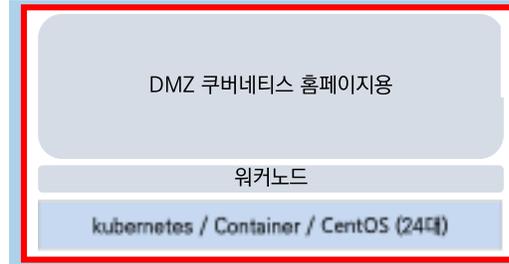
프라이빗 오픈스택 / 쿠버네티스 사례 - 기상청



- 기존의 x86 서비스를 확장가능한 오픈스택 / 쿠버네티스로 변경
- 클라우드 기반 전산자원 확충 및 운영 환경 조성
- 전산자원 할당·회수 자동화 및 시스템 부하에 따른 자동 시스템 확장이 용이한 클라우드 운영 관리 환경 적용
- 오픈스택(Openstack), 도커(Docker) 등과 같이 인터넷에 자유롭게 공개된 소프트웨어로 기존 벤더제품을 대체하여 기상정보시스템 환경으로 최적화
- 타사의 IaaS / PaaS → Playce Cloud로 대체

형태1. 컨테이너 기반의 단일 업무 환경의 PaaS 환경 : 쿠버네티스 단독 구축

기상청 홈페이지를 위한 쿠버네티스 (40대)



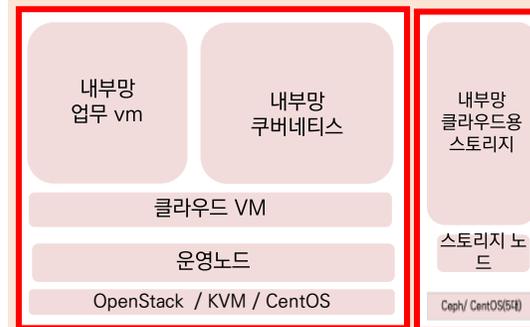
형태2. 여러 업무 환경의 IaaS 환경 : 오픈스택 단독 구축

기상청 업무망과 VM을 위한 오픈스택 (84대)



형태3. 컨테이너 기반의 여러 업무의 멀티 기상 환경의 IaaS + PaaS 환경 : 오픈스택 + 쿠버네티스 구축

기상청 업무망 vm과 연계를 위한 쿠버네티스 (12대)



개발 환경을 위한 쿠버네티스 (140대)



기상정보서비스를 위한 COMIS-5 통합 서비스 구축 사업

2018

- 기상청 상세 설계
- 도입 타당성 검토
- 설계 시범 구축

2019

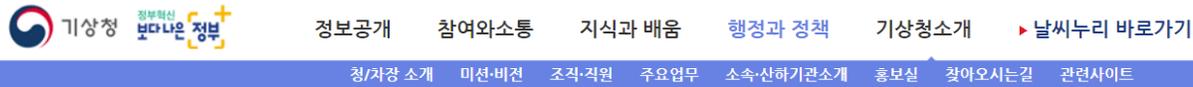
- 응용시스템 개발
- 기상정보 체계
- 인프라 확장
- 대국민서비스 오픈

2020

- 클라우드 확충
- 원격지 부하분산 체계 구축
- 병행 운영

2021

- COMIS-5 현업화 및 안정화



보고자료

본청
소속기관(각 지방청)

○ (컨테이너) 기상청 누리집은 연평균 2억 명 이상 방문하며, 위험기상 시 접속자가 폭증하는 등 급격한 사용자 증가에 대처하기 위해 60여종의 대국민 서비스 운영 환경을 자동 확장이 가능한 클라우드 컨테이너 환경으로 올해 말부터 단계적으로 전환할 계획이다.

※ 클라우드 컨테이너 서비스: 화물을 나누어 담아 편하게 수송하는데 쓰이는 컨테이너처럼, 하나의 소프트웨어를 독립적 기능을 하는 여러 개의 하는 클라우드 서비스

○ (플랫폼) 대용량 기상자료 분석, 수치모델 및 알고리즘 개발 등 비정형적 지식 기반 업무를 보다 체계적으로 지원하기 위해 K-DASH* 플랫폼 서비스를 올해 말까지 구축한다.

* K-DASH(KMA Data & SW Hub): 기상청의 클라우드 서비스의 고유 명칭으로서 대용량 기상자료 분석, 알고리즘 개발에 요구되는 전산자원, 기상자료, 라이브러리 및 분석·협업도구, 계산자원 등을 필요에 따라 통합적으로 구성하여 제공

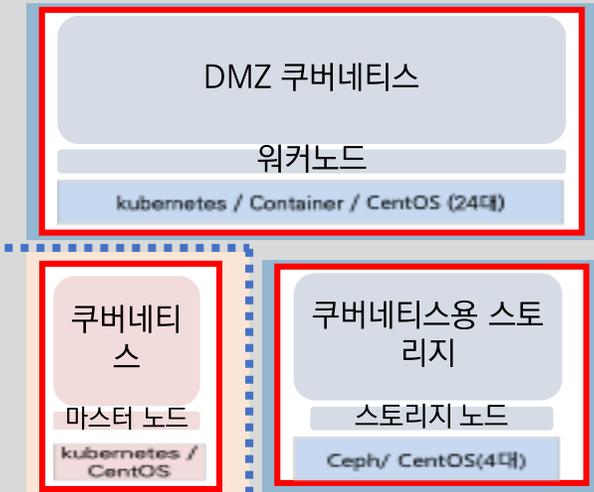
※ 클라우드 플랫폼 서비스: 프로그램 개발이나 각종 데이터 분석에 필요한 전산자원, 데이터, 라이브러리 등을 통합적인 플랫폼 형태로 필요에 따라 자유롭게 제공하는 서비스

기상정보서비스를 위한 COMIS-5 통합 서비스 구축 사업 (2019)

2019

- 응용시스템 개발
- 기상정보 체계
- 인프라 확장
- 대국민서비스 오픈

기상청 홈페이지를 위한 쿠버네티스 (40대)



컨테이너 플랫폼 구축 내용

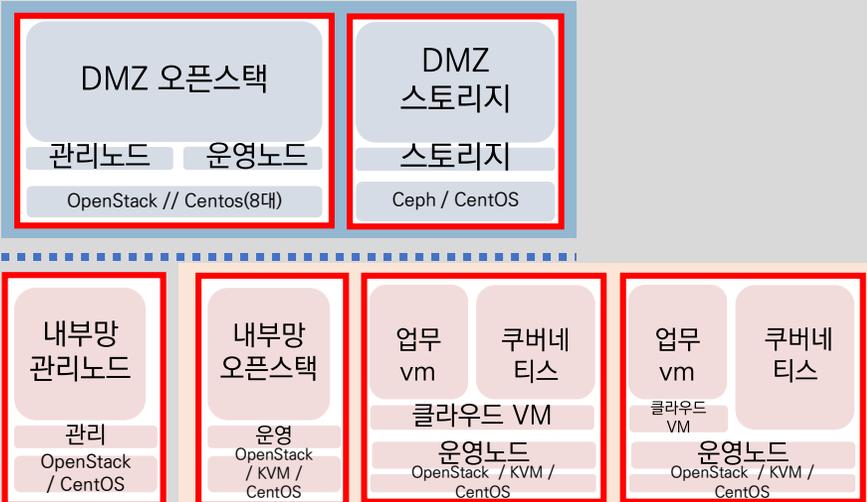
- 1 타사의 PaaS 제품을 커뮤니티 쿠버네티스로 변경
[망분리 요건 / L4 switch / S2I image 변환]
- 2 부서 요구사항에 따른 구성
부서업무는 한 부서의 쿠버네티스 클러스터만 요청
- 3 PaaS의 장점을 살려, 기존업무의 변경을 최소화하여 단시간 시스템 교체
- 4 오픈소스기반의 모니터링/ADMIN 툴 제공
담당자 교육 및 기술전수로 내재화 제공
- 5 담당자 1명 / 오픈후 서비스 무장애

기상정보서비스를 위한 COMIS-5 통합 서비스 구축 사업 (2019)

2020~2021

- 클라우드 확충
- 원격지 부하분산 체계 구축
- 병행 운영

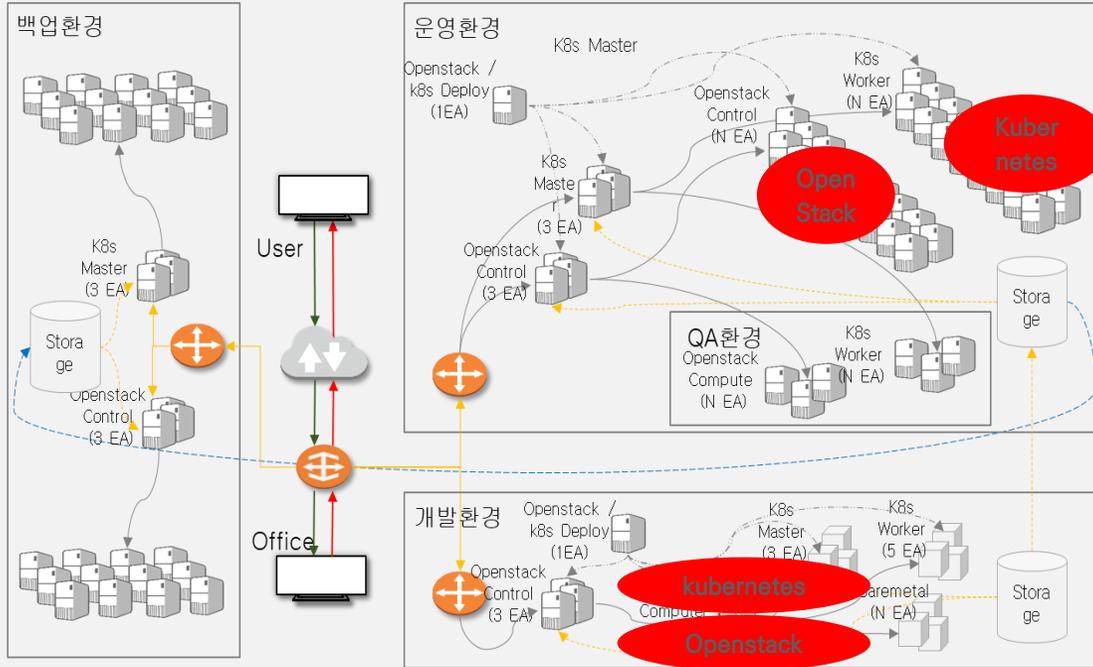
기상청 홈페이지를 위한 쿠버네티스 (40대)



컨테이너 플랫폼 구축 내용

1. 타사의 IaaS 제품을 커뮤니티 오픈스택으로 변경
[망분리 요건 / VM위에 K8S / IRONIC K8S]
2. 최신 오픈스택 LTS 버전 Ussuri 채택
3. 부서에 따른 요구사항 3가지 충족
 1. 일반 부서업무는 오픈스택 VM
 2. 빅데이터처리는 k-dash라는 프로젝트로 vm위에 쿠버네티스를 구성
 3. 연구용 vm과 컨테이너들은 vm은 오픈스택위에 컨테이너들은 오픈스택이 베어메탈 서버를 관리하면서 쿠버네티스가 최상의 성능을 낼수 있도록 구성
4. 쿠버네티스는 오픈스택의 LB와 cephfs(shared FS)를 사용
5. 담당자 1명 / 교육 및 기술전수로 내재화 성공 / 무장애

오픈스택 / 쿠버네티스 구축

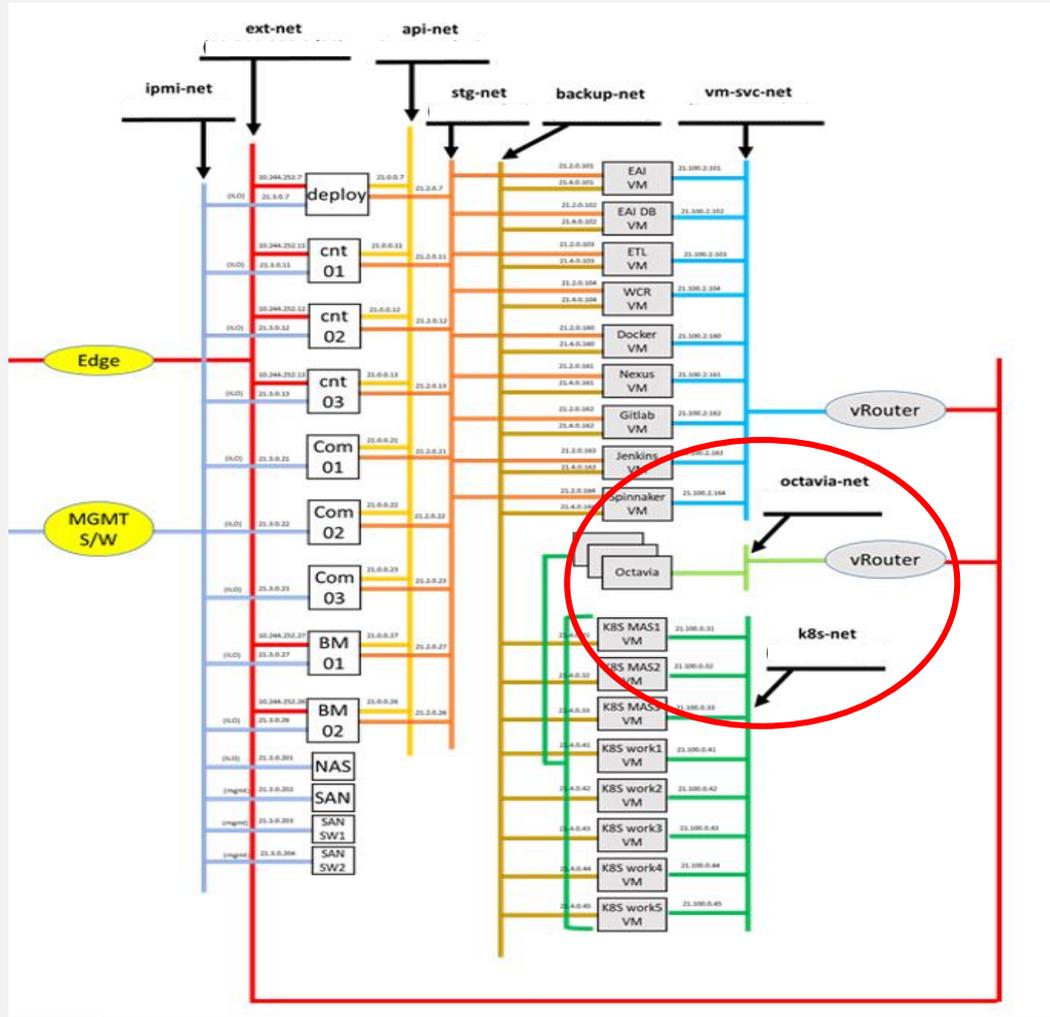


- Openstack VM 을 이용한 Kubernetes 구현한 개발존
- Openstack / Kubernetes 별도 구성으로 PRD + QA 구현한 운영존
- DRC - DR 구성으로 운영 안정성 보안
- Application CI/CD 구축으로 효율적인 배포 관리
- Openstack - Kubernetes 의 구성을 이용한 A-A, A-S, A-B 구성

백업 / 운영환경 구축

- 1 Active-Active(Standby) 전산센타를 구축하고자 함
업무별로 VM과 Container로 구분
- 2 GSLB를 통한 운영환경 이중화 (일부 A-A/ 일부 A-S)
- 3 개발환경은 오픈스택 위에 VM으로 master/worker를 두고, ironic으로 DB 구성(MS-SQL)
- 4 운영환경내에 서버와 스토리지를 분리하여 QA환경을 구축
- 5 스토리지만 복제 솔루션 사용
- 6 DevOps환경을 위한 CI/CD 구축
(spinnaker/gitlab/Jenkins)

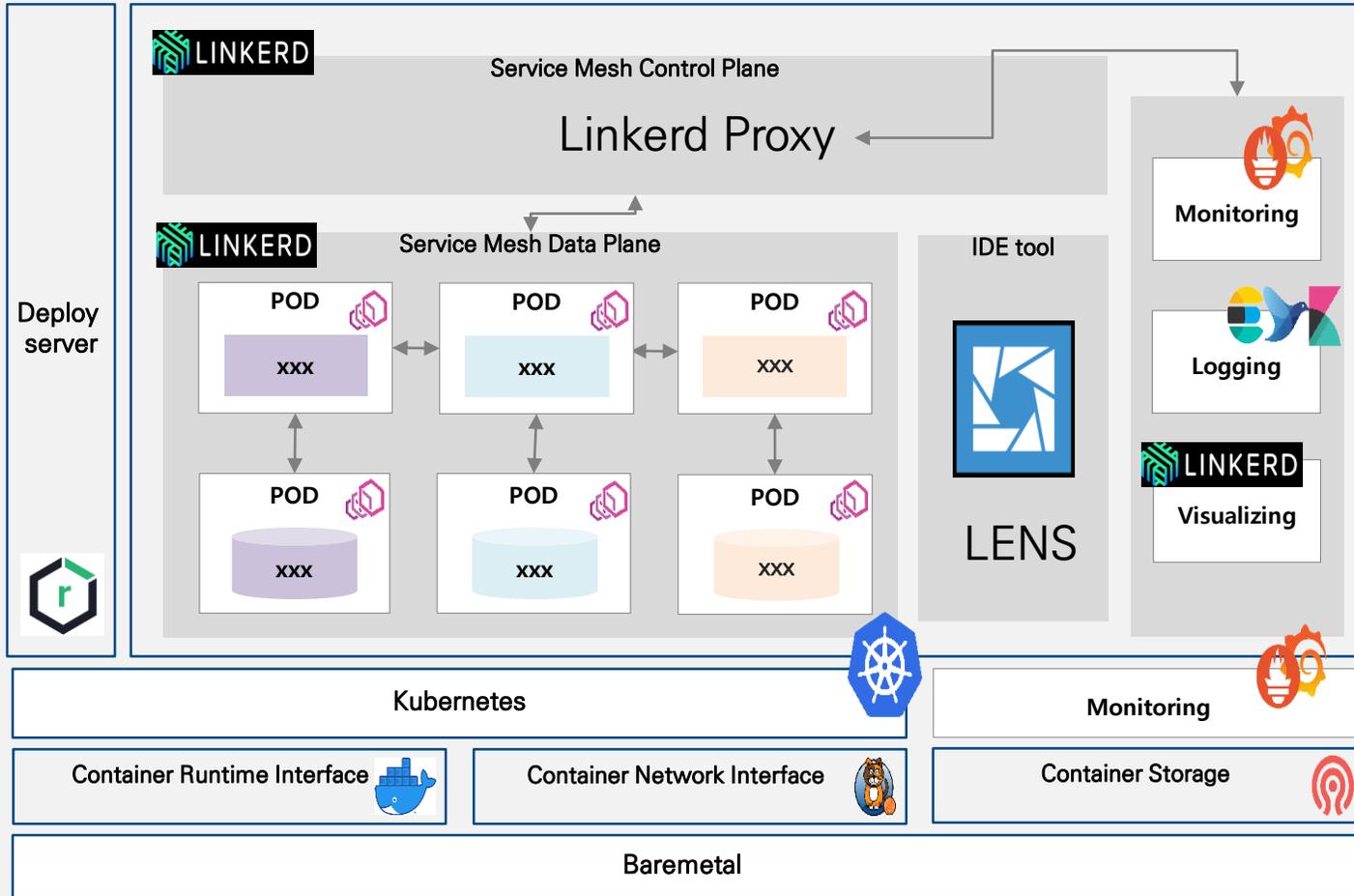
개발환경 Network구조



네트워크

- 1 Kubernetes가 octavia를 사용하여, LB가 가능하도록 구현
- 2 외부네트워크는 하드웨어 아답터단에서 분리하여 보안이슈제거
- 3 부하분산을 위해 스토리지 네트워크와 백업 네트워크 구분
- 4 어드민을 위한 mgmt. 네트워크 구성

계열사별 클라우드 PaaS 환경 구축



커뮤니티 오픈소스를 선택한 이유

- 1 기존 벤더의 지원체계와 가격체계에 이슈 (내부 직원들의 요청)
- 2 모든 DevOps 환경에 대한 연계된 서비스를 제공하지 못함

사례 요약

- 1 커뮤니티 오픈소스로 제1금융권 구축
- 2 Linkerd로 service mesh 구성 (egress 추가구성)
- 3 EFK(Elasticsearch/Fluentd/Kibana) Prometheus/Grafana 구성

Q & A

sales@osci.kr



Cloud & Collaboration

T. 02-516-0711 E. sales@osci.kr

서울시 강남구 테헤란로 88길 32, 5층 (삼성동, 나우키움삼성동A빌딩)

www.osci.kr

THANK YOU

감사합니다



Cloud & Collaboration

T. 02-516-0711 E. sales@osci.kr

서울시 강남구 테헤란로 88길 32, 5층 (삼성동, 나카우삼성동사빌딩)

www.osci.kr