NUCLEO CLOUD NATIVE PLATFORM BASED ON KUBERNETES

Choe, Cheng-Dae
charlie.choe@linecorp.com

Agenda

- OpenStack at Line
- Cloud Native Platform base on kubernetes

Verda

- Private Cloud for Line Corporation
- OpenStack + Inhouse components

Verda: OpenStack

- Keystone: Custom Authentications/ Roles/ Kerberos Integration
- Glance: Ceph
- Nova: Custom Scheduling
- Neutron: Custom Network Architecture, No overlays
- Designate: with some customization
- Horizon: custom panels —> inhouse dashboard

Verda: Non OpenStack

- LBaaS not Neutron LBaaS: bpf, xdf, bgp… docker…
- DBaaS not Trove: MySQL, Redis, HBase(todo)
- BareMetal not Ironic: Integrated with internal kickstart
- Object Storage: Ceph
- CDN: poppy with customize
- Container Orchestration: ****, Nucleo

Verda - status

- Mitaka
- Dev/ Prod Clusters
- In Tokyo
- 70% of vm, 30% of bm

	Dev	Prod
VM	2500+	400+
PM	200+	300+
Projects	500+	150+
Launched	16. 8	17. 4

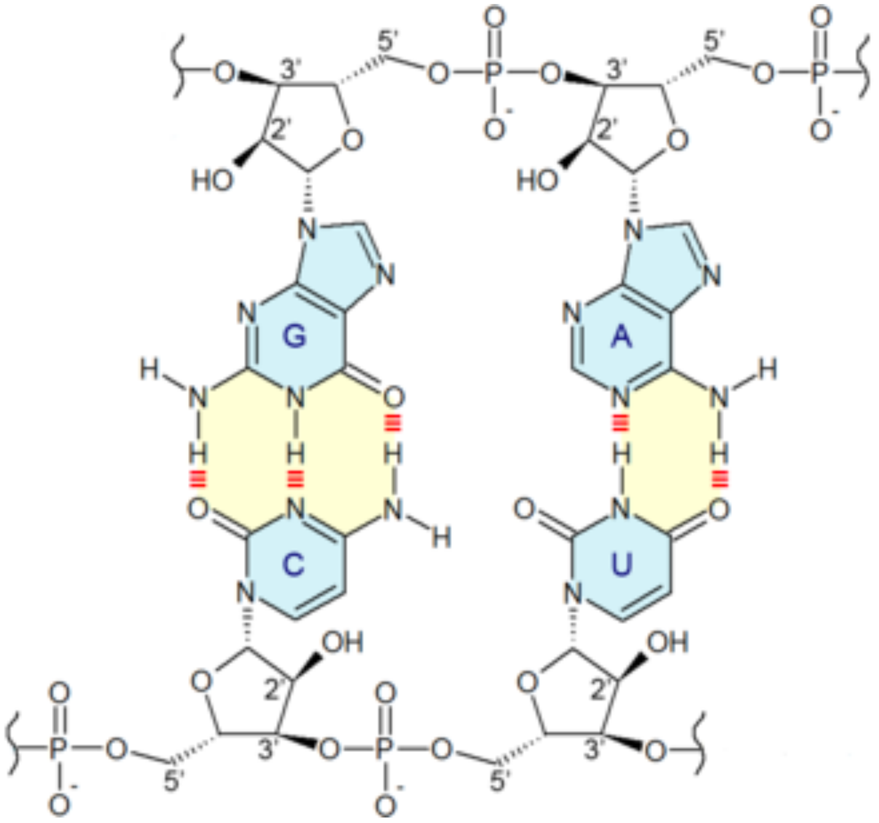
Verda - deploy

- all automated just one click.
- to enable this...
    - on push master or release branch
    - deploy to stage {dev|prod} on verda
    - run automated functional test & QA

Verda Plan

- More Region
    - Osaka(2018. 1), Singapore, Korea, Germany, USA…
- More Features
    - HBase as a Service…
    - Backups
    - More Platform/ Supporting Services
- More Developers :D

Nucleo - The Cloud Native Platform



Cloud native?

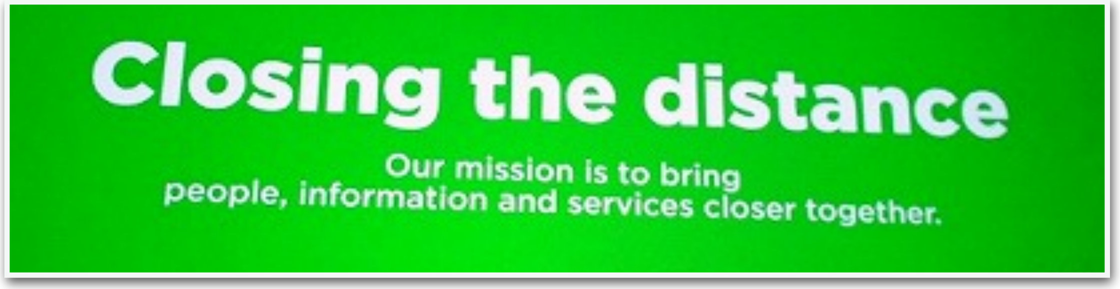
- https://12factor.net/ko/: codebase, dependencies, **config**, backing service, build/ release/ run, **processes**, port binding, concurrency, **disposability**, **dev/prod parity**, logs, admin processes

- service that supports Continuous Deploy, DevOps, Infra agility

- Micro Service Architecture

- Stateless Protocol: http, gRPC…

- time to business:



Closing the distance

Our mission is to bring
people, information and services closer together.

Why….?

- why container?… is there any doubt?
- why not magnum?
    - magnum provides container cluster itself.
    - user should familir to kubernetes, mesos, swarm…
    - multiple clusters… make difficult to manage, updates…
    - our goal is provide a platform service not a container cluster.
- Why kubernetes?

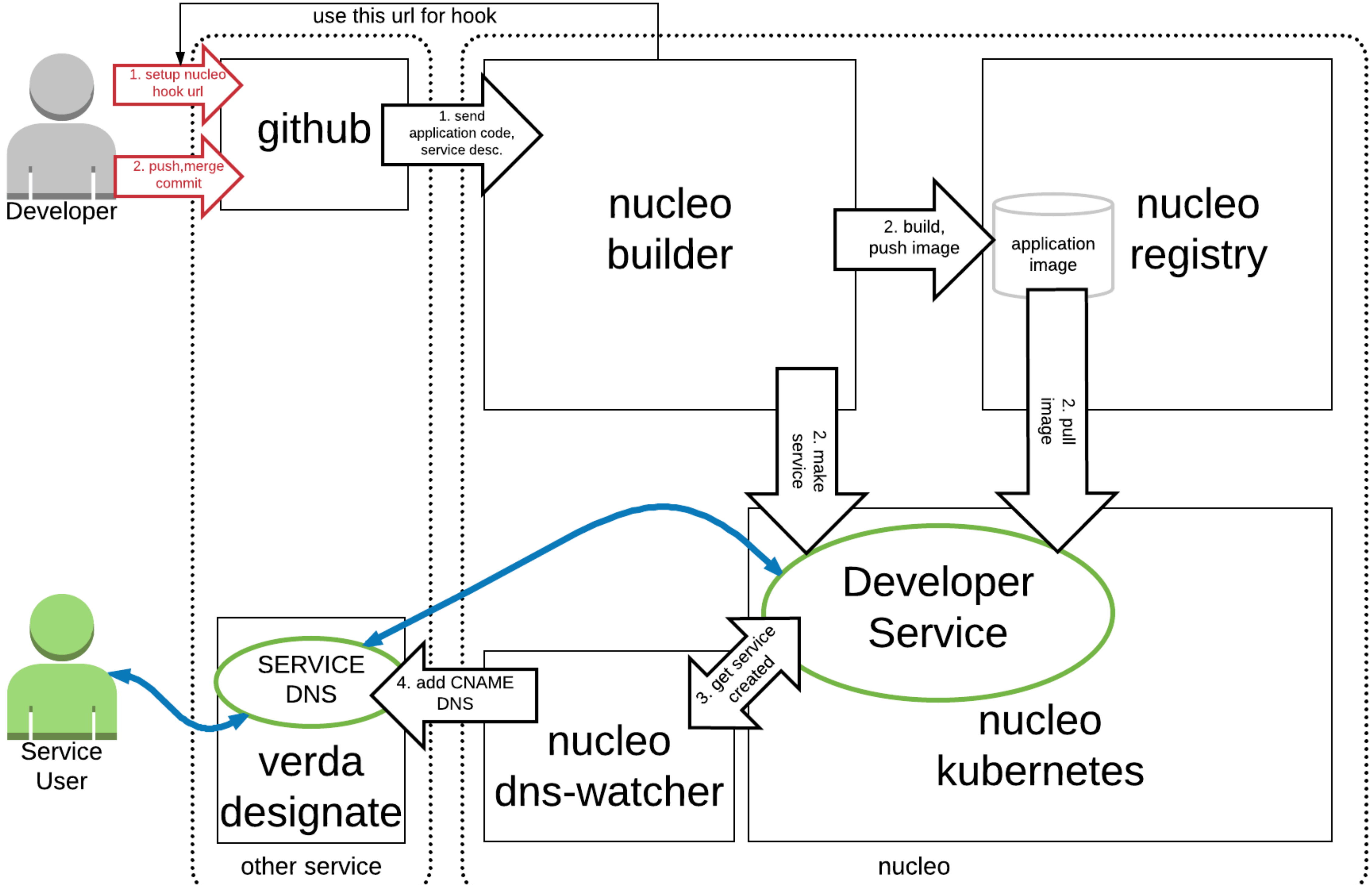
Why platform?

- user get a freedom of getting infra resources...
    - also get a role for mange resources...
- there is no changes but BM -> VM
- fragmentation: each service team has their own way
- DevOps != Dev(Ops), DevOps = (Dev + Ops)
- Provide a another infra is not a solution.

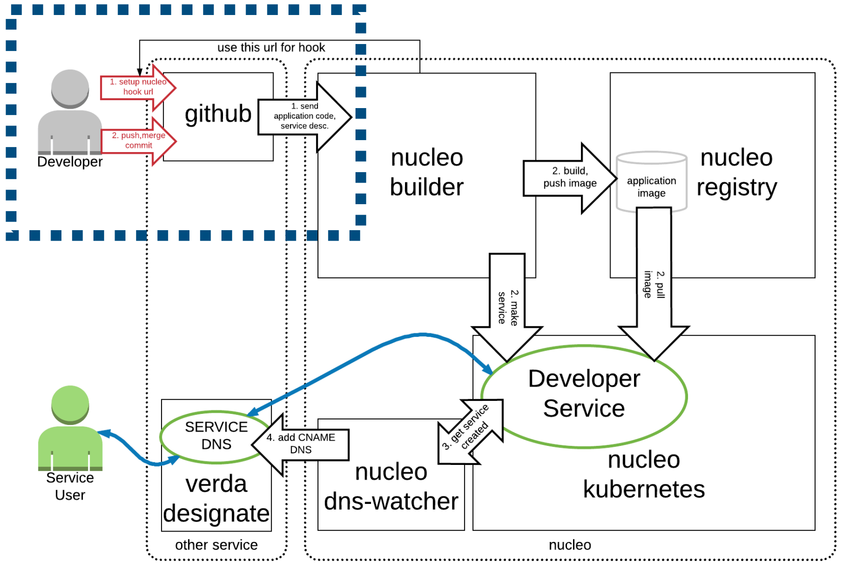
Goal

- Continuous Delivery: Closing the distance
- Sharing codebase between Dev and Ops
- Sharing knowhow with platform

Nucleo: Architecture



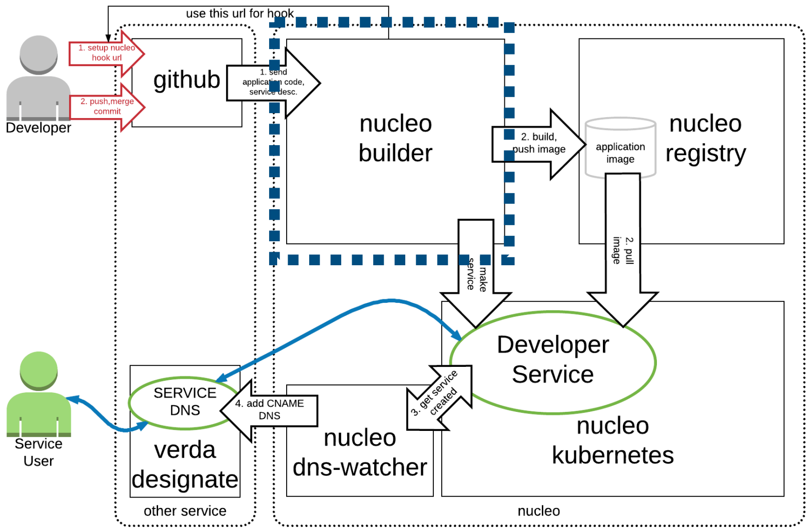
github



- codebase
- continuous delivery
- configuration as a code
- operation as a code
- push to service —> reduce business delivery time

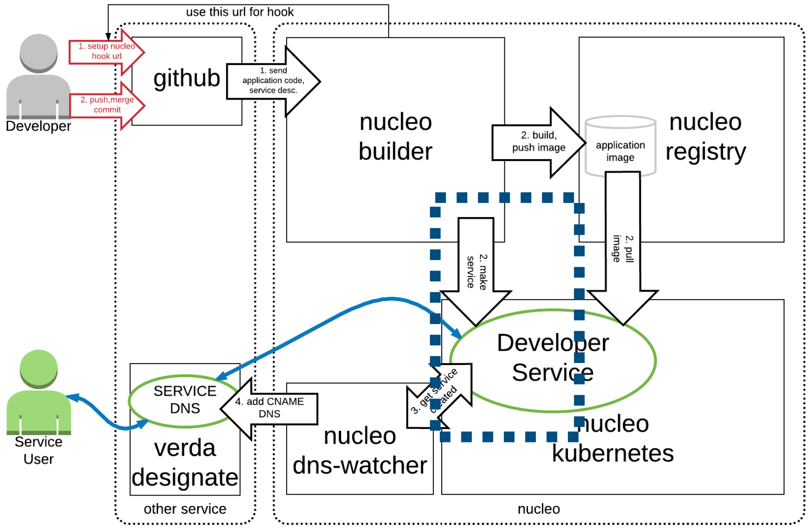
```
platform: python

ports:
  # <internal port>:<external port>
  - 8080:80
  # does not expose public port
  # only accessible in nucleo cluster
  # - 8080

cmd:
  start: nucleo/start.sh
  pre_stop: nucleo/pre_stop.sh

scale:
  # static replicas, scaling manually
  replicas: 4

  # auto scaling
  # replicas: 2-20
  # cpu_threshold: 50

kernel:
  key: value
```

image builder

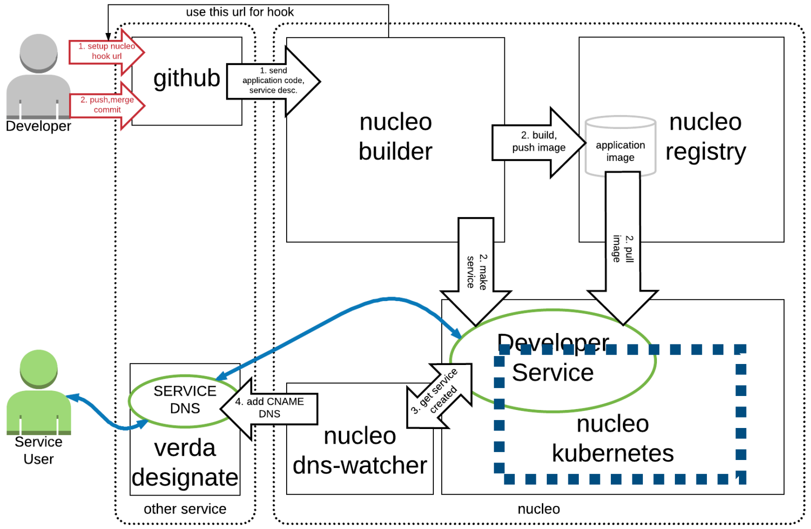


- triggered by push webhook
- build container image from source like buildpack..
    - restrict to provided platforms..
- Dockerfile or Container Image built by user makes...
    - security: If base image has security hole? Who is he for defeat hole?
    - not all developer are familiar to build docker image…
    - not automated means that we can’t ensure running image is built from latest code.
- Taking build image role..
    - we can rebuild image anytime. security updates, base image updates, tunings... etc
    - no need to manage huge private image repository. only needs latest images.
    - as a platform: spread knowhow to others... without any conscious effort..

Helm: The kubernetes package manager



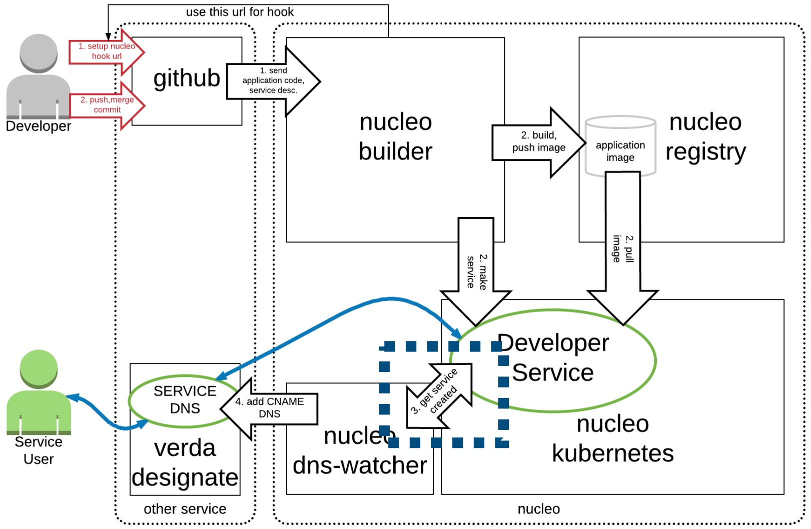
- All nucleo apps are helm instances
- Templating resources
- Managing resource updates, versioning
- Share packages: charts
- gives us convenient way updating resources



Cilium

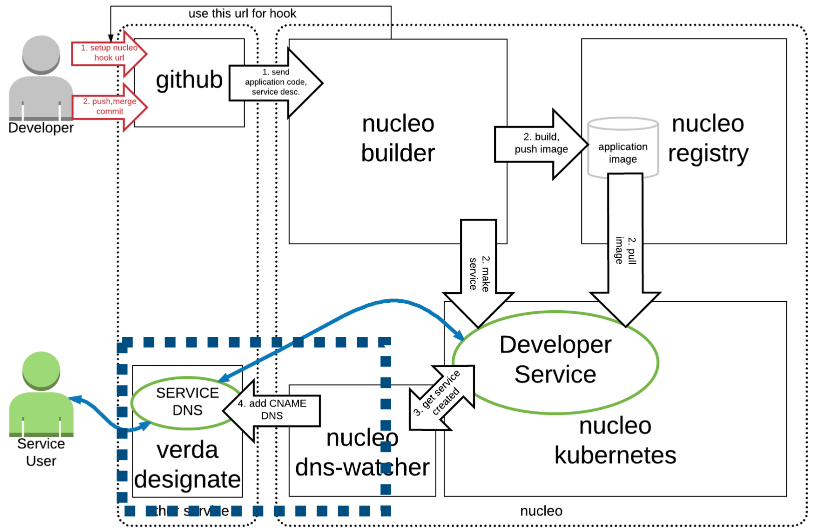
- https://www.cilium.io/
- bpf: a bytecode runs in kernel level enables hook incoming, outgoing packets, system calls, kprobes, uprobes, tracepoints… cilium leverages bpf to preform data path filtering, mangling, monitoring and redirection.
- xdp: run bpf program in network driver with direct access to packet’s DMA buffer.
- > kernel 4.11
- not DPDK

Ingress controller



- L4, L7 service gateway
- implemented as k8s deployment
- nginx, haproxy, traefik…

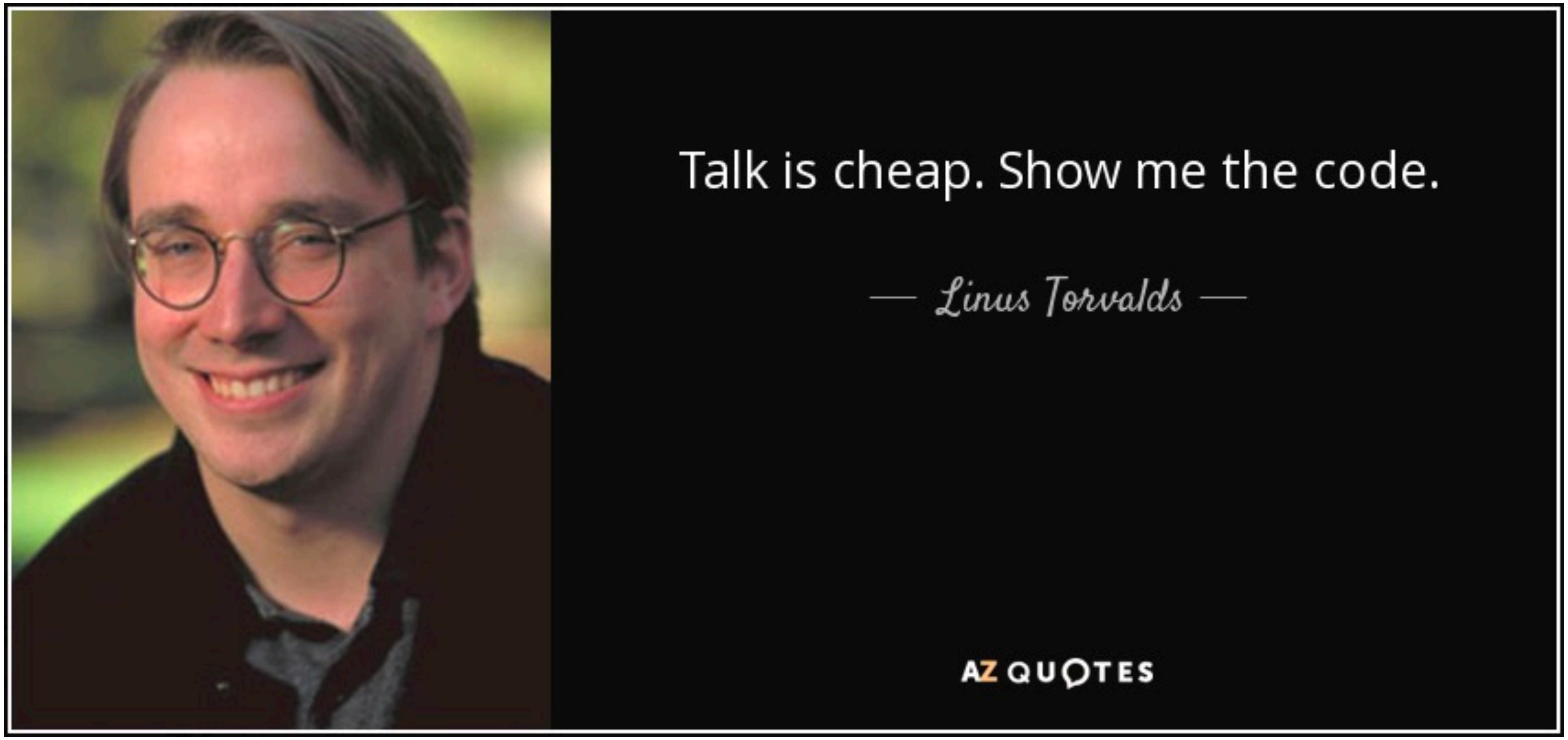
edge router



- nucleo-dns
  - watch k8s service changes
- FabricLB
  - create vip and set backend to ingress controller
- Designate
  - create record to FabricLB

Misc

- Notification: HipChat
- Metric: Heapster + InfluxDB(Prometheus) + Grafana
- Logging: fluentd + (Kafka, HDFS) + ES + Kibana
- Alerting: Inhouse



Talk is cheap. Show me the code.

— Linus Torvalds —

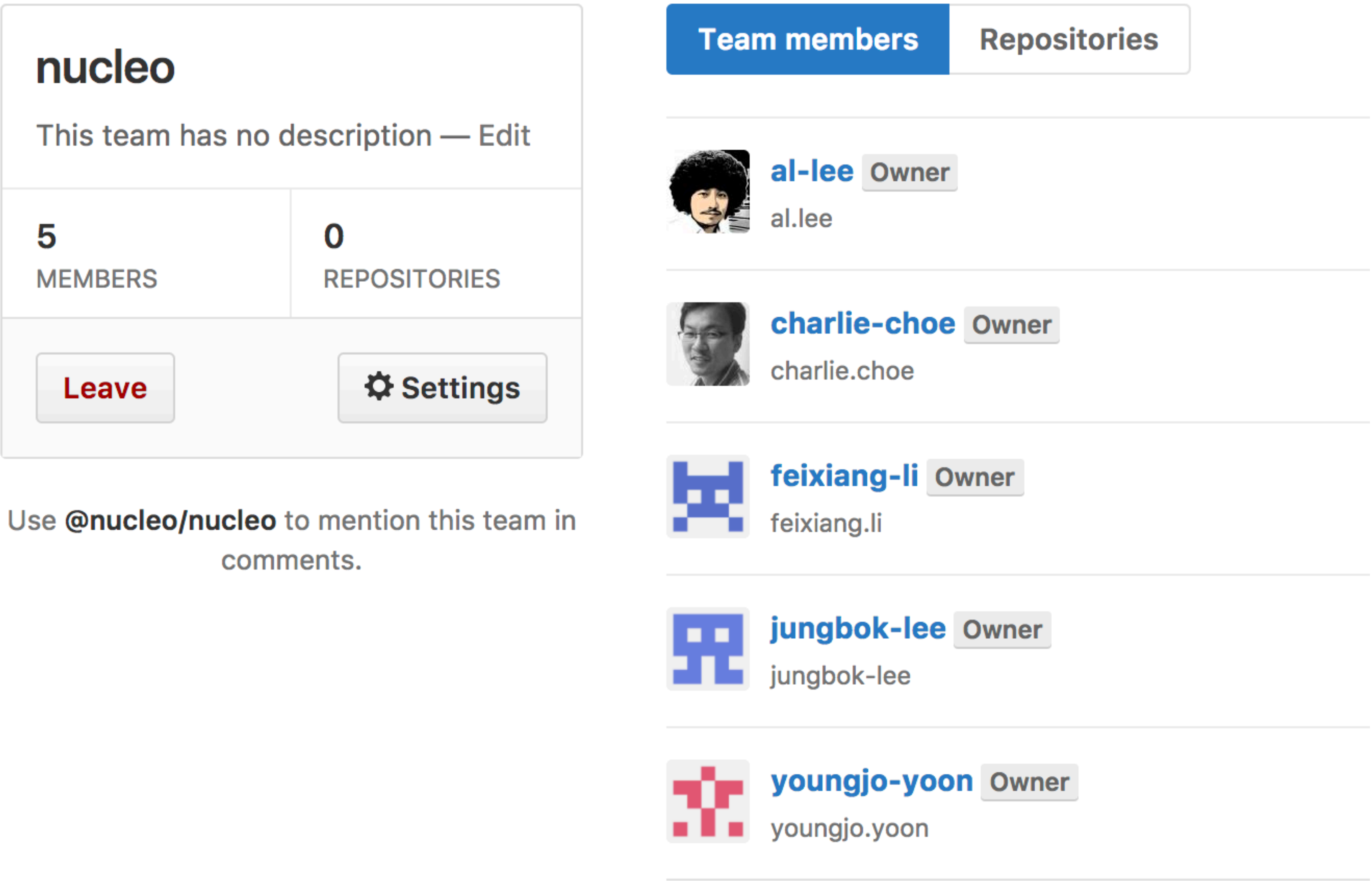
Nucleo

- Continuous Delivery
- Developer Develops
- Operator Operate
- Me make it works well

Plan

- CI Integration
- Platform Services:
  - More Language Supports: Java, …
  - More Platforms: DB, Cache, Queue
  - Inhouse Platforms
- FaaS, APIGateway
- CronJob, Batch Job
- More Developers…

Thanks



nucleo

This team has no description — Edit

5 MEMBERS

0 REPOSITORIES

Use @nucleo/nucleo to mention this team in comments.

al-lee Owner
al.lee

charlie-choe Owner
charlie.choe

feixiang-li Owner
feixiang.li

jungbok-lee Owner
jungbok-lee

youngjo-yoon Owner
youngjo.yoon