docker 在 openstack 的應用

高國棟

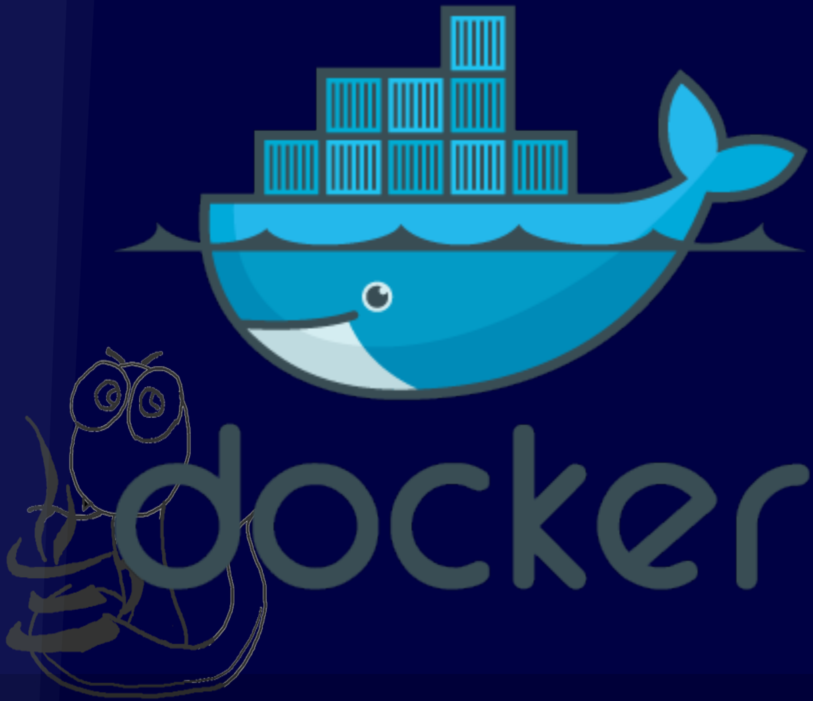
簡介

- 任職於 inwinstack
- Conference speaker
- Openstack contributor
- Python, django, linux, openstack, docker, scala
- http://www.blackwhite.tw/

大綱

- docker 介紹
- nova-docker
- kolla
- heat-docker
- murano
- magnum

docker



- lightweight, portable, self-sufficient containers.
- the process running in the container is isolated from the process running in the other container.

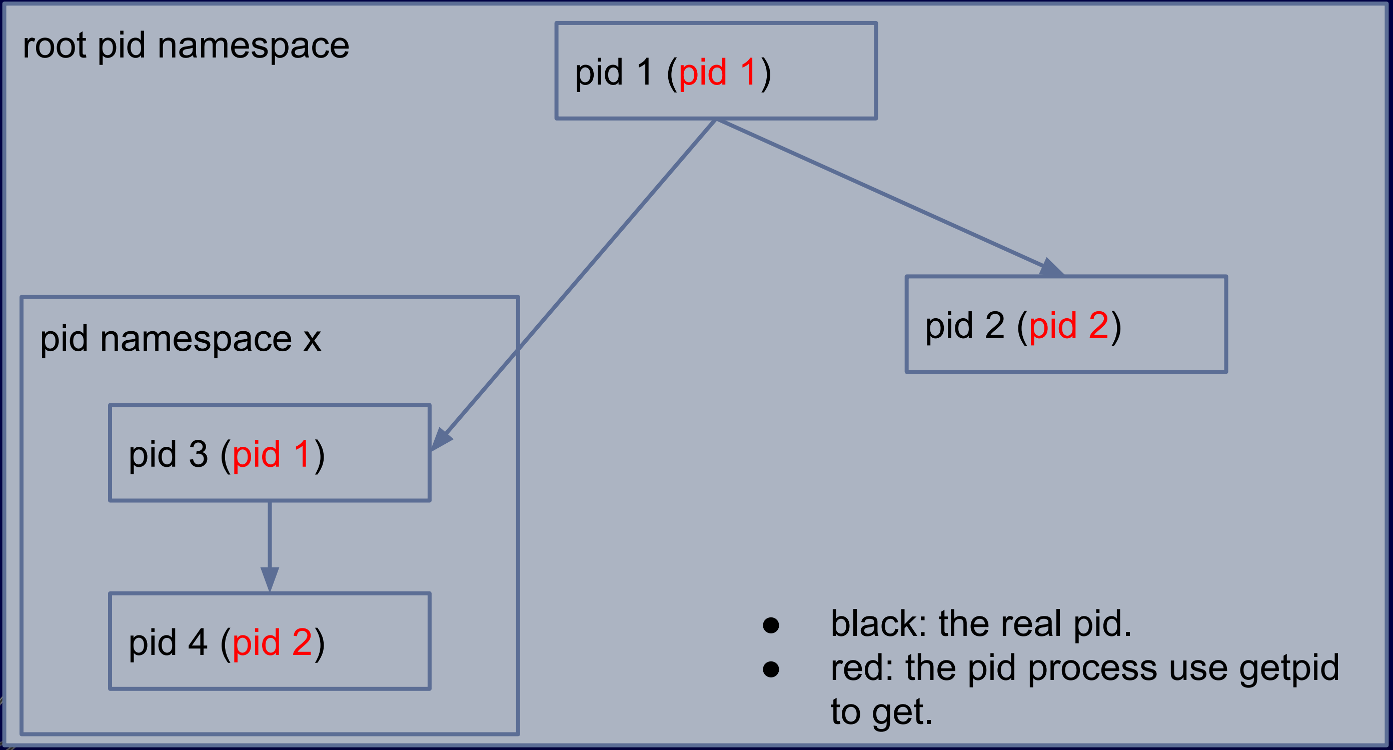
Docker

- Based on
    - lxc
        - linux kernel namespace
        - Apparmor and SELinux profiles
        - Seccomp policies
        - Control groups
        - Chroots
    - Autofs

Kernel namespace

- The purpose of each namespace is to wrap a particular global system resource in an abstraction that makes it appear to the processes within the namespace that they have their own isolated instance of the global resource.
- Private view

kernel pid namespace



- black: the real pid.
- red: the pid process use getpid to get.

Kernel namespace

1. UTS: hostname
2. IPC: inter-process communication
3. PID: processes in different PID namespaces can have the same PID
4. MOUNT: mount points, first to land in Linux
5. NET: network access, including interfaces
6. USER: map virtual, local user-ids to real local ones

kernel namespace

Mount namespaces

UTS namespaces

PID namespaces

Network namespaces

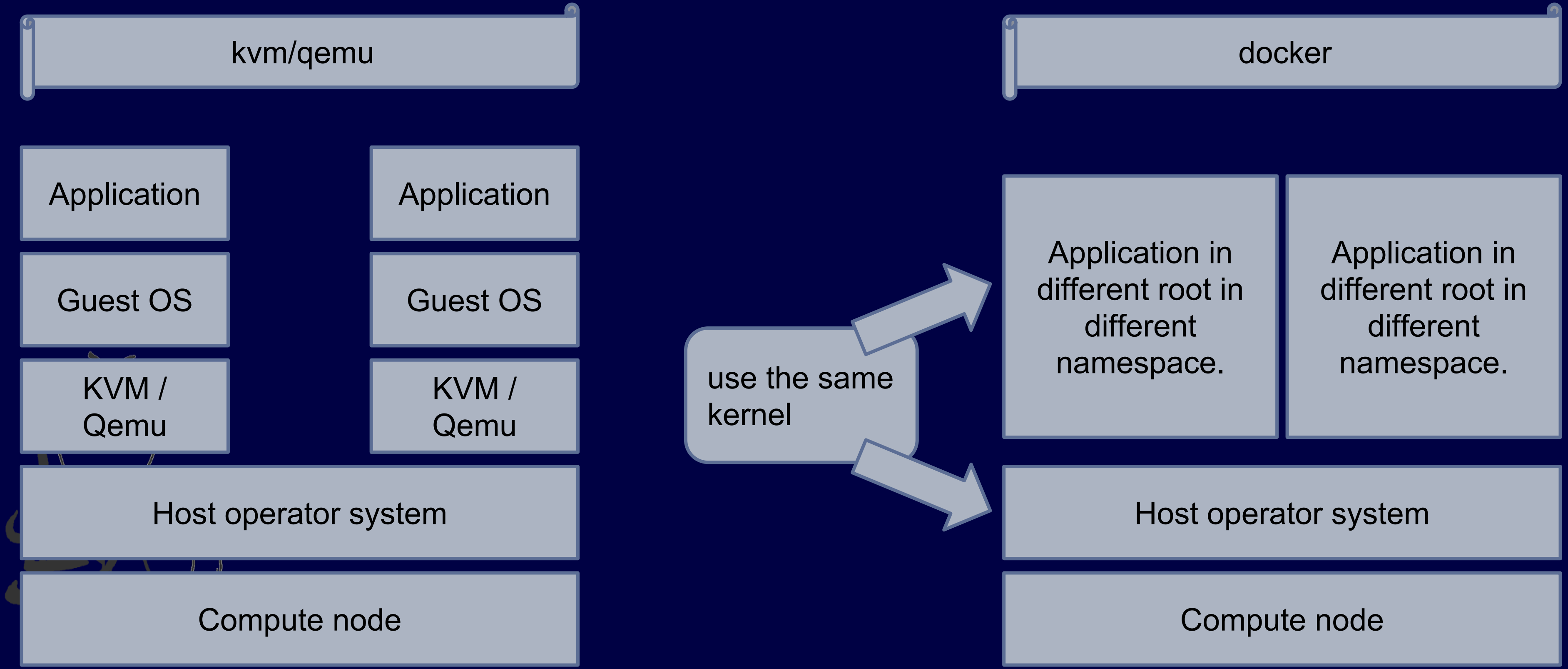
User namespaces

IPC namespaces

nova-docker

- nova:
  - provide vm
- experimental:
  - It was introduced with the Havana release
  - It lives out-of-tree for Icehouse and Juno.
- inactivity

Nova - kvm/qemu vs docker



kvm/qemu

Application

Guest OS

KVM / Qemu

Application

Guest OS

KVM / Qemu

Host operator system

Compute node

docker

use the same kernel

Application in different root in different namespace.

Application in different root in different namespace.

Host operator system

Compute node

Summary for nova-docker

- 優點：
  - 快速啟動
  - 較好效能
- 缺點：
  - 與其他元件水土不合
  - inactivity

kolla

- deploying OpenStack services using Docker containers.
- https://hub.docker.com/u/kollaglue/
  - Glance
  - Keystone
  - Nova
  - Neutron
  - Horizon

kolla

- https://github.com/stackforge/kolla/blob/master/docs/minimal-environment-vars.md
  - sudo docker run -e "KEYSTONE_PUBLIC_SERVICE_HOST=10.0.2.15" -e "GLANCE_API_SERVICE_HOST=10.0.2.15" -e "NOVA_API_SERVICE_HOST=10.0.2.15" -p 5566:80 -d kollaglue/fedora-rdo-horizon

- support ansible (working)

kolla

- Upgrade or rollback OpenStack deployments atomically.
- Upgrade or rollbackOpenStack based by component.
- make more platform-dependent

nova-compute in container

- The container’s processes wants to utilize the host network namespace
    - specifically –net=host flag.
- The container’s processes wants to utilize bind mounting
    - that is mounting a directory from the host file-system

- The container’s processes wants to utilize the host pid namespace

nova-compute in container

- /sys: To allow libvirt to communicate with systemd in the host process
- /sys/fs/cgroup: To allow libvirt to share cgroup changes with the host process
- /var/lib/libvirt: To allow libvirt and nova to share persistent data
- /var/lib/nova: To allow libvirt and nova to share persistent data

nova-compute in container 測試結果

- libvirt 可以在 container 執行
- nova-compute 可以在 container 執行
    - 用 nova-compute container 替換 devstack 的 nova-compute
    - 但是無法執行 instance

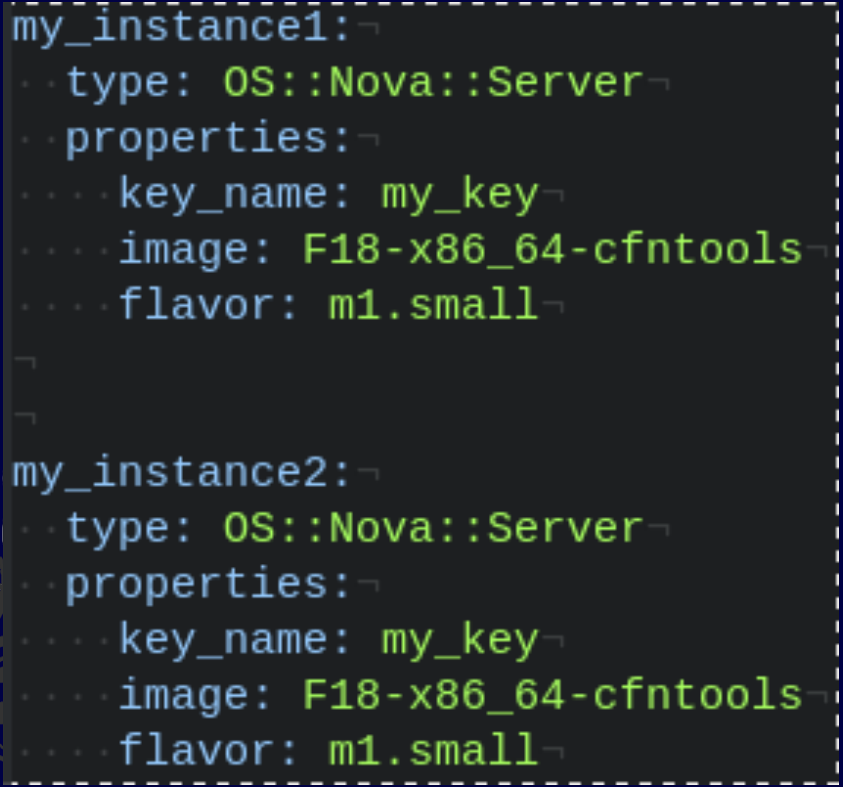
Summary for kolla

- 很有潛力的專案
- 如果配上 ansible 如虎添翼
- 現在在 container 內除錯也更容易
    - 因 1.3 版引進 docker exec

Heat

- 提供一個語言，讓你更方便使用與管理 openstack 資源。
- yaml
- 應用：
  - auto scaling, alarm system

heat script sample



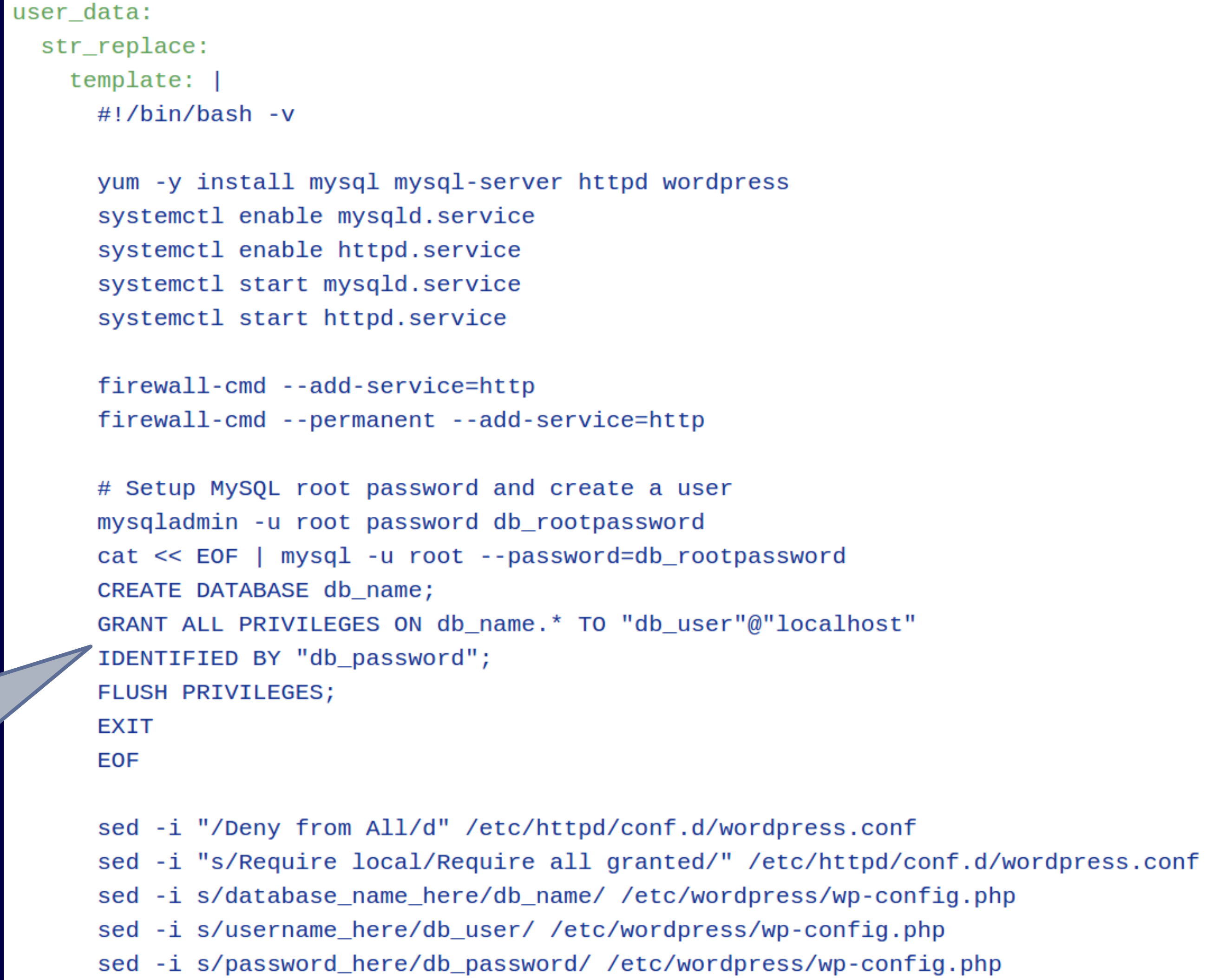
```
my_instance1:
  type: OS::Nova::Server
  properties:
    key_name: my_key
    image: F18-x86_64-cfntools
    flavor: m1.small


my_instance2:
  type: OS::Nova::Server
  properties:
    key_name: my_key
    image: F18-x86_64-cfntools
    flavor: m1.small
```

- 建立兩個 instance
- instance 的 image 是 F18-x86_64-cfntools
- flavor 是 m1.small

heat script sample to deploy application

- 客製化 vm image，讓 vm 啟動後就做你期望的事情
  - website
  - mysql
  - website1
  - website2
  - website3

heat script sample to deploy application



```
user_data:
  str_replace:
    template: |
      #!/bin/bash -v

      yum -y install mysql mysql-server httpd wordpress
      systemctl enable mysqld.service
      systemctl enable httpd.service
      systemctl start mysqld.service
      systemctl start httpd.service

      firewall-cmd --add-service=http
      firewall-cmd --permanent --add-service=http

      # Setup MySQL root password and create a user
      mysqladmin -u root password db_rootpassword
      cat << EOF | mysql -u root --password=db_rootpassword
      CREATE DATABASE db_name;
      GRANT ALL PRIVILEGES ON db_name.* TO "db_user"@"localhost"
      IDENTIFIED BY "db_password";
      FLUSH PRIVILEGES;
      EXIT
      EOF

      sed -i "/Deny from All/d" /etc/httpd/conf.d/wordpress.conf
      sed -i "s/Require local/Require all granted/" /etc/httpd/conf.d/wordpress.conf
      sed -i s/database_name_here/db_name/ /etc/wordpress/wp-config.php
      sed -i s/username_here/db_user/ /etc/wordpress/wp-config.php
      sed -i s/password_here/db_password/ /etc/wordpress/wp-config.php
```

write many code in user data

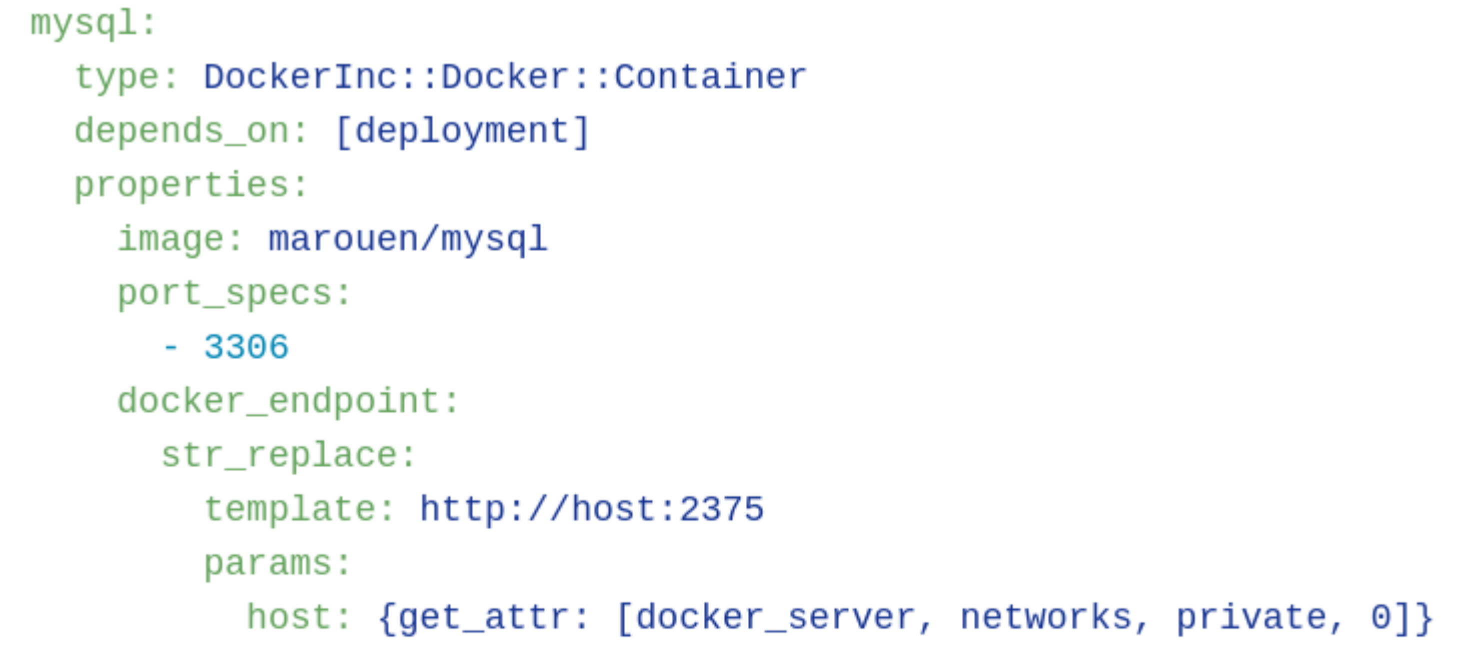
heat-docker

- 讓 heat script 可以控制 docker（透過 docker remote api)
- 讓你更容易使用 heat script 去佈署應用程式

Openstack heat property

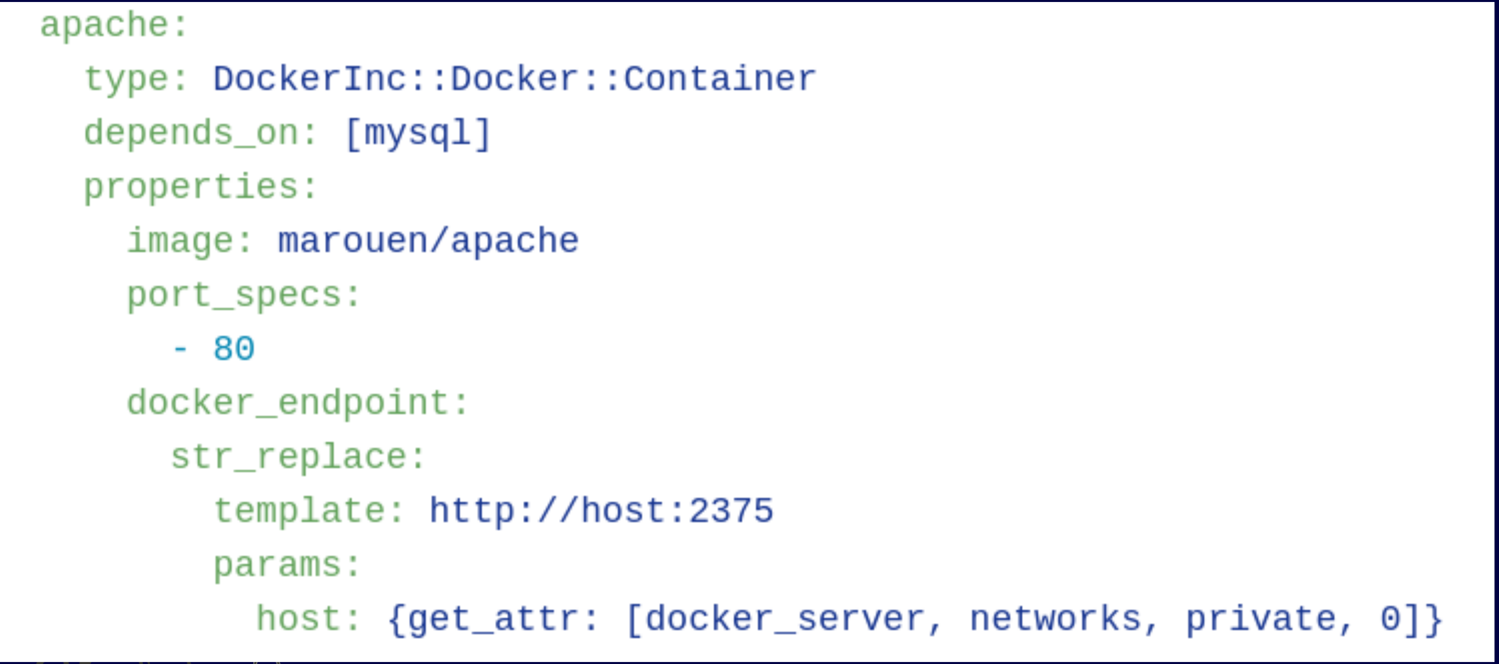
- cap_add
- cap_drop
- cmd
- cpu_set
- cpu_shares
- devices
- dns
- docker_endpoint
- env
- hostname
- image
- links
- memory
- name
- open_stdin
- ...

Openstack heat



```
mysql:
  type: DockerInc::Docker::Container
  depends_on: [deployment]
  properties:
    image: marouen/mysql
    port_specs:
      - 3306
    docker_endpoint:
      str_replace:
        template: http://host:2375
        params:
          host: {get_attr: [docker_server, networks, private, 0]}
```

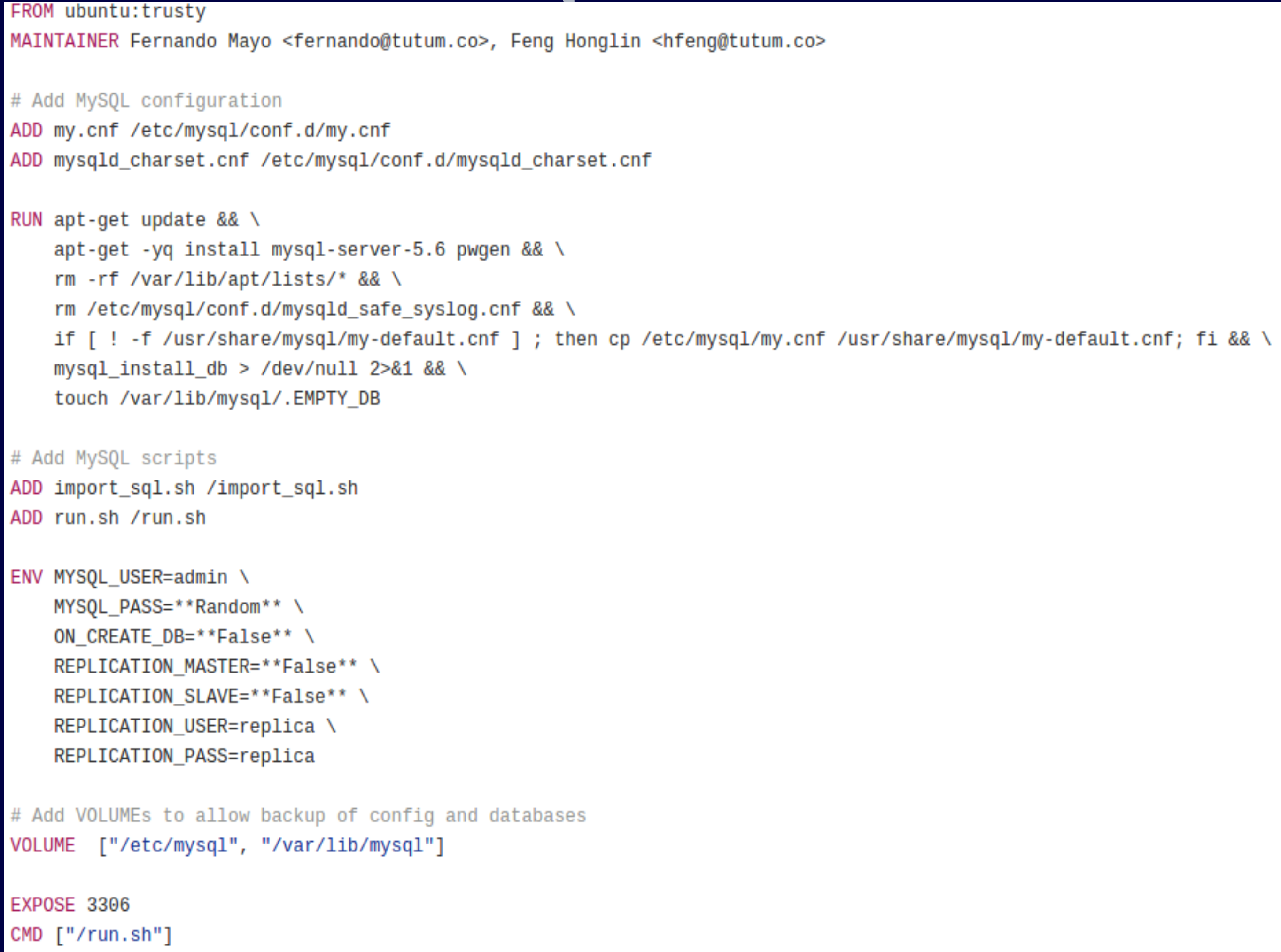
Openstack heat



```
apache:
  type: DockerInc::Docker::Container
  depends_on: [mysql]
  properties:
    image: marouen/apache
    port_specs:
      - 80
    docker_endpoint:
      str_replace:
        template: http://host:2375
        params:
          host: {get_attr: [docker_server, networks, private, 0]}
```

How about docker image version control?

Thanks to Dockerfile



```
FROM ubuntu:trusty
MAINTAINER Fernando Mayo <fernando@tutum.co>, Feng Honglin <hfeng@tutum.co>

# Add MySQL configuration
ADD my.cnf /etc/mysql/conf.d/my.cnf
ADD mysqld_charset.cnf /etc/mysql/conf.d/mysqld_charset.cnf

RUN apt-get update && \
    apt-get -yq install mysql-server-5.6 pwgen && \
    rm -rf /var/lib/apt/lists/* && \
    rm /etc/mysql/conf.d/mysqld_safe_syslog.cnf && \
    if [ ! -f /usr/share/mysql/my-default.cnf ] ; then cp /etc/mysql/my.cnf /usr/share/mysql/my-default.cnf; fi && \
    mysql_install_db > /dev/null 2>&1 && \
    touch /var/lib/mysql/.EMPTY_DB

# Add MySQL scripts
ADD import_sql.sh /import_sql.sh
ADD run.sh /run.sh

ENV MYSQL_USER=admin \
    MYSQL_PASS=**Random** \
    ON_CREATE_DB=**False** \
    REPLICATION_MASTER=**False** \
    REPLICATION_SLAVE=**False** \
    REPLICATION_USER=replica \
    REPLICATION_PASS=replica

# Add VOLUMEs to allow backup of config and databases
VOLUME  ["/etc/mysql", "/var/lib/mysql"]

EXPOSE 3306
CMD ["/run.sh"]
```

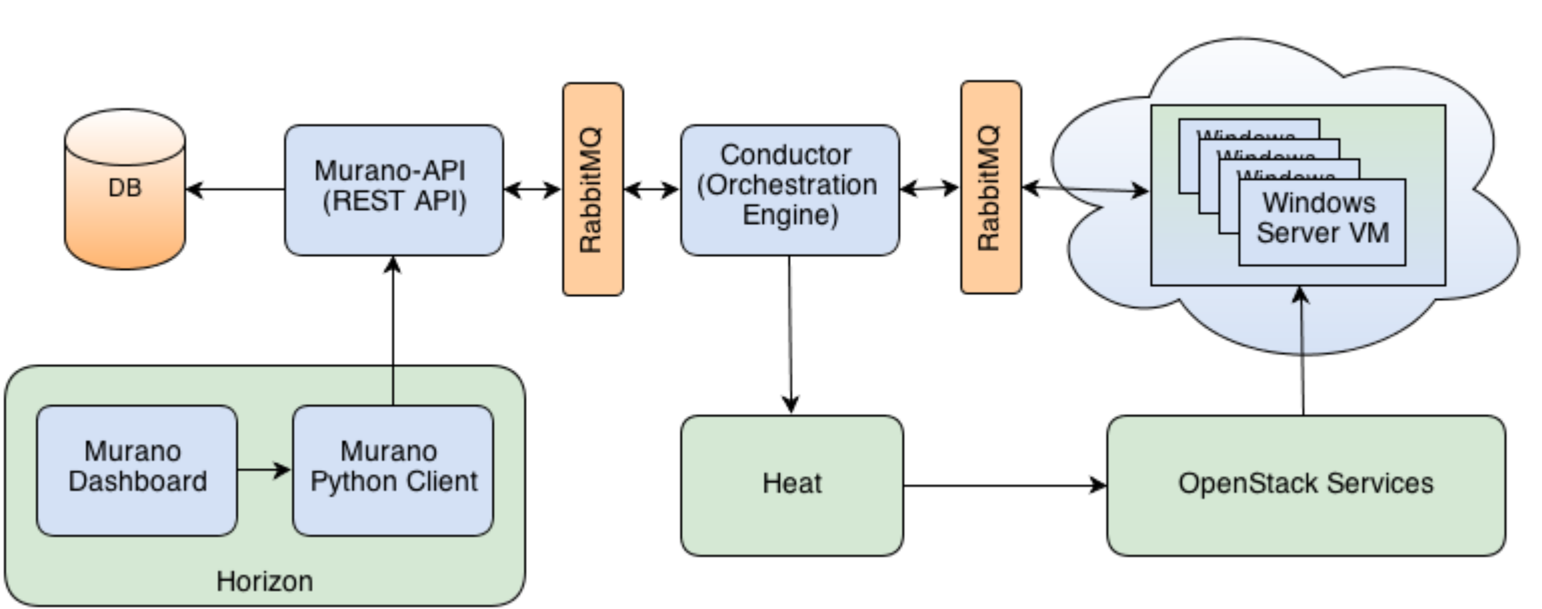
Summary for heat-docker

- 各司其職，各盡所能
  - heat script 只要負責將各種功能(Application)接起來，至於功能(Application)如何被實作出來，他不在意。
  - docker 負責把功能做出來，至於別人要怎麼用他不在意。docker 也讓環境可以受到版本控制

Murano

- Enabling application developers and cloud administrators to publish various cloud-ready applications in a browsable categorized catalog.
- https://github.com/openstack/murano-apps
- 在 vm 裡安插 agent，接受來自 murano-conductor 指令

Murano


DB
Murano-API
(REST API)
RabbitMQ
Conductor
(Orchestration
Engine)
RabbitMQ
Windows
Server VM
Murano
Dashboard
Murano
Python Client
Horizon
Heat
OpenStack Services

How do murano-conductor send message to murano-agent ?

- Murano create environment’s network. And add instance to environment’s network.

murano app（without docker）

- https://github.com/openstack/murano-apps/tree/master/MySQL/package
- 18 files, 695 lines
- steps:
    - initialize
    - deploy
    - createDatabase
    - createUser
    - assignUser
    - getConnectionString

murano app (with docker)

- https://github.com/openstack/murano-apps/blob/master/Docker/Applications/MySQL/package
- 8 files, 334 lines
- steps:
  - initialize
  - getContainer
  - onInstallationStart
  - onInstallationFinish

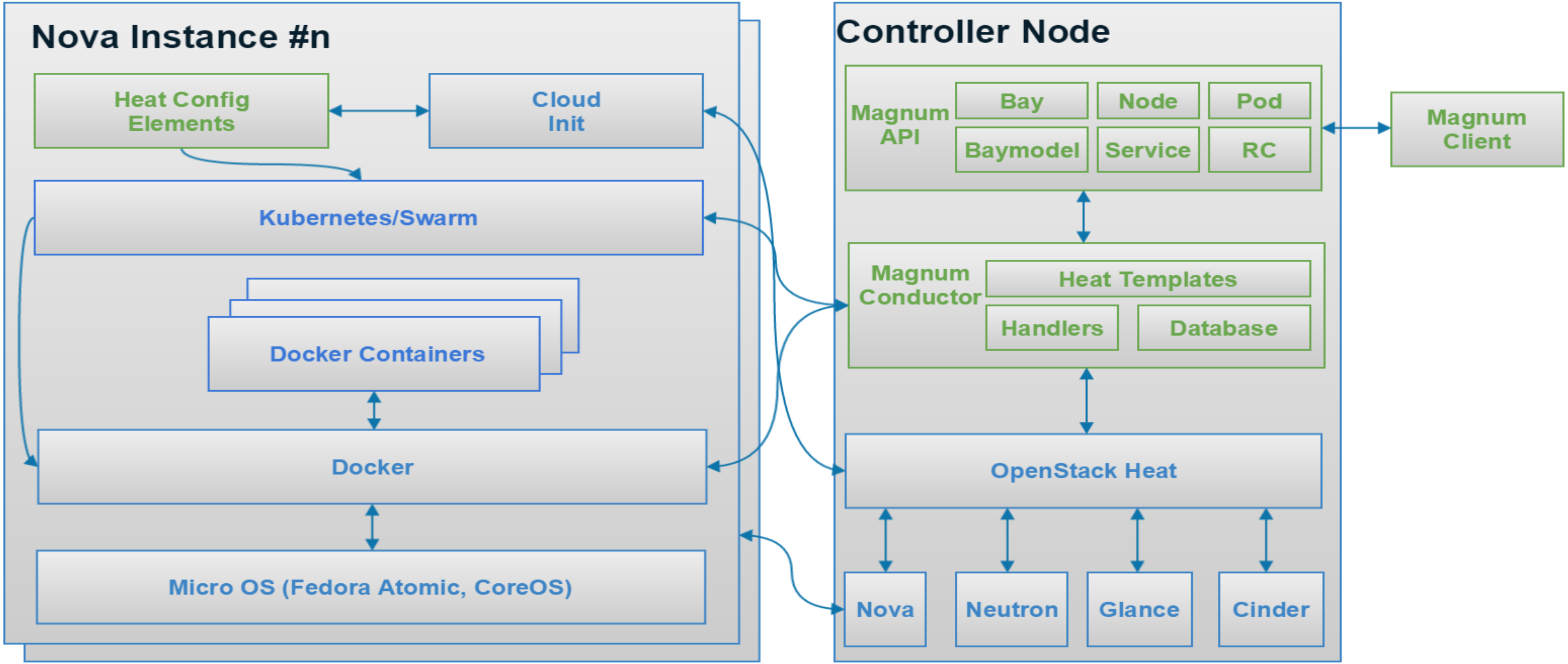
Summray for murano

- We can write less code to deploy app when using docker.
- 14 apps without using docker
- 20 apps using docker
- If I have seen farther than others, it is because I was standing on the shoulders of giants

Magnum

- Based on
  - kubernetes or
  - swarm
- Provide:
  - asynchronous API
  - compatible with Keystone
  - multi-tenancy implementation
- magnum 幫你整合好 openstack 與 kubernets (or swarm)

Magnum


Nova Instance #n
Heat Config Elements
Cloud Init
Kubernetes/Swarm
Docker Containers
Docker
Micro OS (Fedora Atomic, CoreOS)
Controller Node
Magnum API
Bay
Node
Pod
Baymodel
Service
RC
Magnum Client
Magnum Conductor
Heat Templates
Handlers
Database
OpenStack Heat
Nova
Neutron
Glance
Cinder

Will I get the same thing if I use the Docker resource in Heat?

- No, heat-docker poor in:
  - Replication
  - Service

Summary for magnum

- Still developing
- Poor document
- useful for the people who want to use openstack and kubernetes

Summary

- nova-docker
- kolla
- heat-docker
- murano
- mugnum