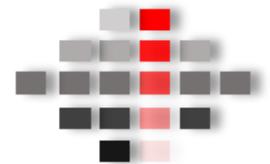


# From Infra to Services: LBAAS and K8S

Mingjun Shan

June 12, 2018 Ottawa OpenStack  
Meetup



[www.computingstack.com](http://www.computingstack.com)

# About ComputingStack.com



ComputingStack is a development and engineering focused business. We contribute to upstream Open Source, create our own package and deliver the services of those to enterprise user for those data and cloud solution. In meanwhile we partner up with solution providers to accelerate their solution portfolios.

IntOS is a self-maintained package by ComputingStack, composed of IntOS OpenStack, Ceph Storage, Kubernetes as well IntOS Cloud Management. The ground up packaging with “0” dependencies on third parties component makes it possible to depoy anywhere anytime any device.

**95%** generic upstream codes of openstack, ceph, K8s, monitoring, high availability components

**5%** in-house developed codes: automation, packaging , bug fix, HA , security engineering, customizations, tools

IntOS targets at Enterprise Ready for high complex cloud, while incrementally incorporating Cloud 2.0 services for NFV, Edge, IoT etc.

# Pre-Conclusions



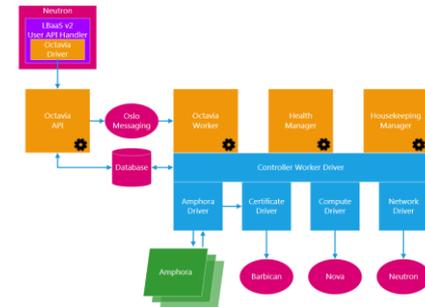
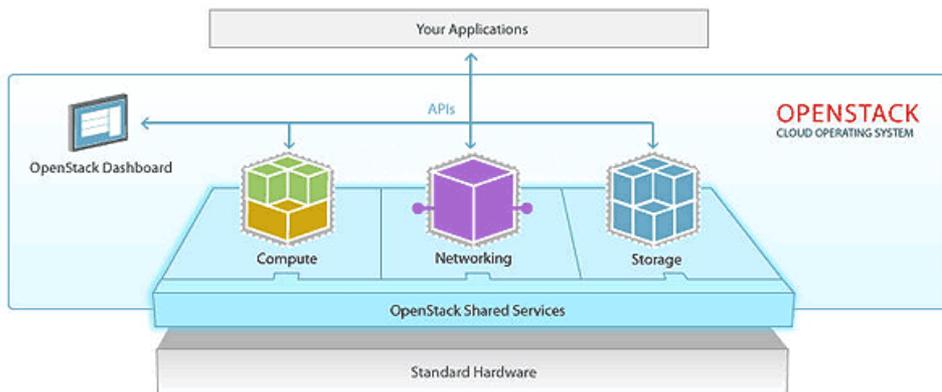
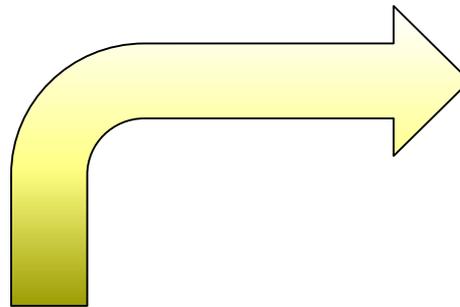
## Benefits:

- No EXPENSIVE ~~\$\$\$~~ public cloud
- Magnum+Octavia+Barbican provide super experience of Kubernetes clustering: High Secure, Scalable, and High Available
- A comparable to AWS EKS
- Just a natural step forward, when OpenStack in place,
- Truly community driven “OPEN”: issues resolvable

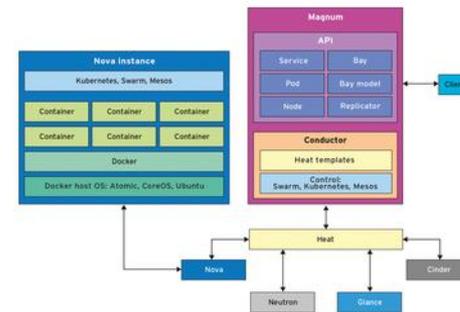
## Drawbacks:

- Integration is not a small work, expert openstack + solid Kubernetes knowledge, but with community, it can be simple 😊
- Both OpenStack and Kubernetes are dynamic, so keeping changing is a challenge for reaching a best balance (functionality vs stability) of this marriage.
- Octavia is over HAProxy, a rather stable, approachable, usable backend

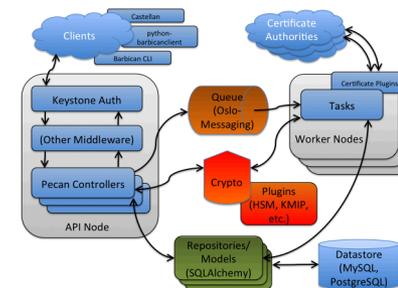
# Value add on: From stack to services



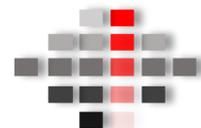
Octavia



Magnum  
Kubernetes

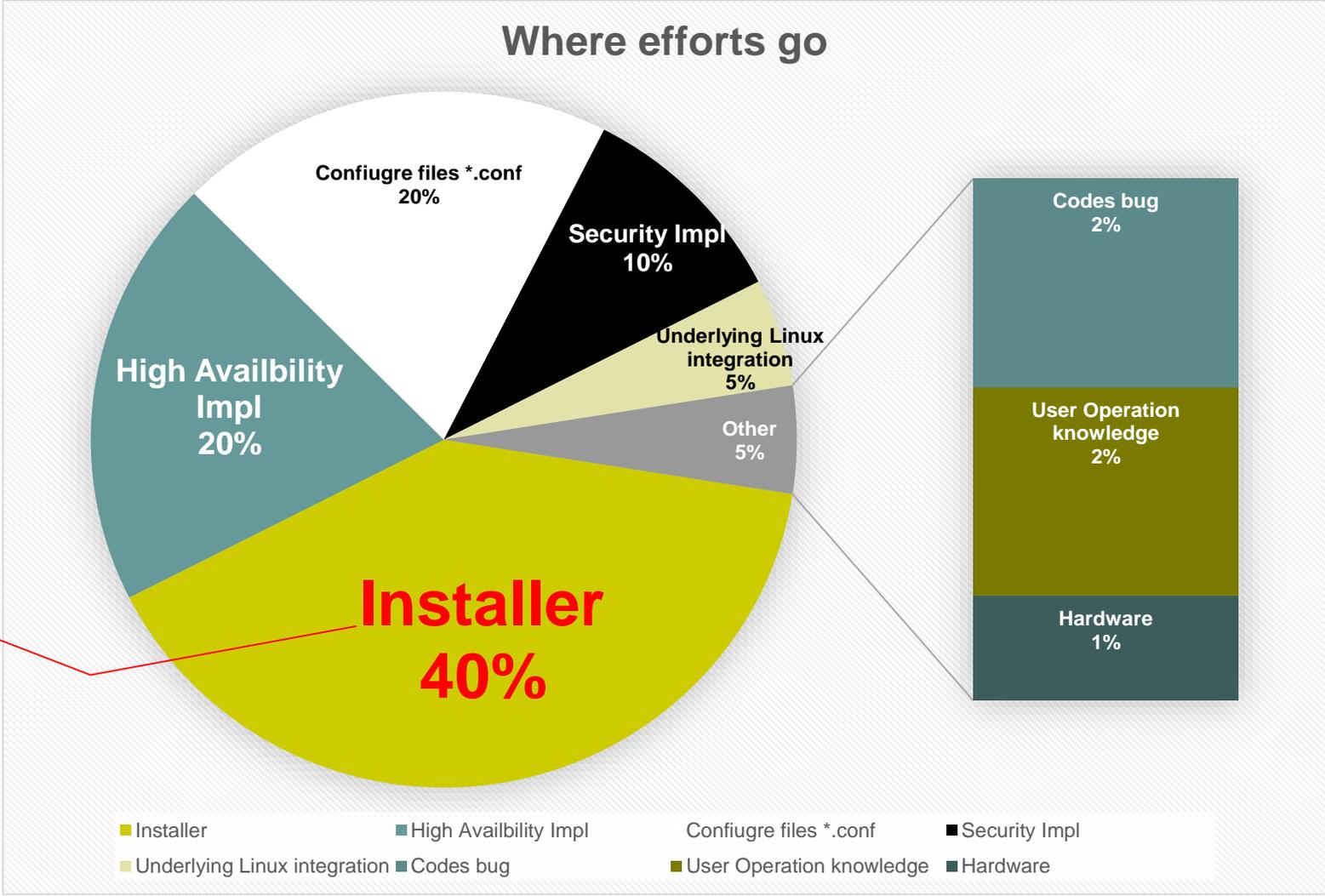
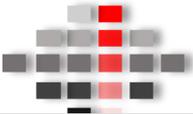


Barbican



**DEMO**

# Understand the complexity of building such



# Which Installer



## Community



Apt package  
Yum package

....

## Vendor specific



....

- Kolla
- Helms
- Ansible
- IntOS
- Redhat OSP
- Mirantis MOS
- Wind River Titanium
- Ubuntu conjure up
- Yum package
- Apt package
- Vendor specific:  
Rackspace, Huawei  
etc

# Three Versions of load balancers by OpenStack



| LBAAS V1                                                                                                                                                           | LBAASV2                                                                                                                                                                                                                                                                                                                                        | OCTAVIA                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Deprecated in Liberty                                                                                                                                              | Deprecated in Pike                                                                                                                                                                                                                                                                                                                             | Only option of Load Balancer in Queens |
| Agent support:<br>neutron_lbaas.services.loadbalancer.plugin.LoadBalancerPluginv2<br>neutron_lbaas.drivers.haproxy.plugin_driver.HaproxyOnHostPluginDriver:default | Agent support:<br>neutron_lbaas.services.loadbalancer.plugin.LoadBalancerPluginv2<br>neutron_lbaas.drivers.haproxy.plugin_driver.HaproxyOnHostPluginDriver:default<br>Octavia Support:<br>neutron_lbaas.services.loadbalancer.plugin.LoadBalancerPluginv2<br>LOADBALANCERV2:Octavia:neutron_lbaas.drivers.octavia.driver.OctaviaDriver:default | ZERO neutron dependencies              |

# Queens Version Major Change



Queens has no significant change, but is a cut off alike change, as it is separated completely from Neutron

- stopped github/neutron-lbaas repo
  - stopped github/neutron-lbaas-dashbaord
  - Continue: github/octavia
  - New: github/octavia-dashboard
  - Stopped as plugin/service provider to neutron, but level 1 service
  - Stopped cli: neutron-lbaas-xxxx
  - Octavia doesnot read neutron.conf
  - Api CALL change
  - CLI: only ocatavia neutron-lbaas
- How is it causing compatibility problem?
    - Configuration
    - Database
    - Upgrading
    - Magnum

# Network and Image Prep



LB CONSUMES a lot of IP and Compute resources!!!

Lb-mgmt-net has to be a public network, through which Octavia conductor talks with LB instances

In dev, external\_network (which floating-ip uses) can be used as lb-mgmt-net

Image: amphora with: tags: amphora

Flavor: amphora is Ubuntu, so can't be too small, but our env shows 1 core 2G ram performs well

# Certificates in Octavia



Notes: Certificates dealing can be daunting

The bi-directional TLS authentication is only security measure for network between HAproxy and OpenStack controller, hence a must, either CA signed or self-signed.

[https://github.com/openstack/octavia/blob/master/bin/create\\_certificates.sh](https://github.com/openstack/octavia/blob/master/bin/create_certificates.sh)  
works

```
openssl genrsa -passout pass:foobar -des3 -out private/cakey.pem (A)2048
openssl req -x509 -passin pass:foobar(B) -new -nodes -key private/cakey.pem \
  -config $OPEN_SSL_CONF \
  -subj "/C=US/ST=Denial/L=Springfield/O=Dis/CN=www.example.com" \
  -days $VALIDITY_DAYS \
  -out ca_01.pem (C)
openssl x509 -in ca_01.pem -text -noout
openssl req \
  -newkey rsa:2048 -nodes -keyout client.key (D) \
  -subj "/C=US/ST=Denial/L=Springfield/O=Dis/CN=www.example.com" \
  -out client.csr (E)
openssl ca -passin pass:foobar -config $OPEN_SSL_CONF -in client.csr \
  -days $VALIDITY_DAYS -out client-.pem -batch
cat client-.pem client.key > client.pem (F)
```

```
Vi /etc/Octavia/Octavia.conf
[certificates]
ca_private_key = /home/intos/certificates/private/cakey.pem (A)
ca_private_key_passphrase = foobar(B)
```

```
[haproxy_amphora]
client_cert = /etc/octavia/certs/server_ca.pem (F)
server_ca = /etc/octavia/certs/client.pem (C)
```

```
[amphora_agent]
agent_server_ca = /etc/octavia/certs/client_ca.pem(D)
agent_server_cert = /etc/octavia/certs/server.pem(F)
```

# Migration to Octavia from neutron-lbaas: work around



<https://wiki.openstack.org/wiki/Neutron/LBaaS/Deprecation>

Octavia DB replaces previous neutron DB  
addon

Manual deletion might be needed on neutron  
db, but it won't hurt

neutron.conf: no service\_provider, no plugin

# Integration with Magnum



- Octavia is a MUST for kubernetes over OpenStack
- Integration might be straightforward as only API call in between
- However:
  - Magnum k8s master: kube-controller-manager.service may not be well compatible with new API change of Octavia to create external LB service to expose pods
  - Manual LB works well
  - Workaround: `service_plugins = router,lbaasv2-proxy`

# Some lessons



- OpenStack is far beyond network/computing/storage, but SERVICES
- OpenStack Doc provides an idea, but far from being correct, sometimes misleading 😞
- Codes, codes, dive more, more insights!
- DevStack is fairly easy to learn many codes details, highly recommended as a tool handy
- OpenStack is high complex, and be prepared for long install journey, but eventually worth it
- Fortunately we have community and support 😊



Q&A

Contact: [dangxiaoxing@computingstack.com](mailto:dangxiaoxing@computingstack.com)