Gestion de cluster *Kubernetes* dans le Cloud

Jérôme Pansanel

Strasbourg – 20 septembre 2018

cnrs IN2P3 Les deux infinis

IPHC Institut Pluridisciplinaire Hubert CURIEN STRASBOURG

Université de Strasbourg

Sommaire

- Kubernetes dans le Cloud ?
- Cloud commerciaux
- Cloud académiques
- Interaction avec OpenStack

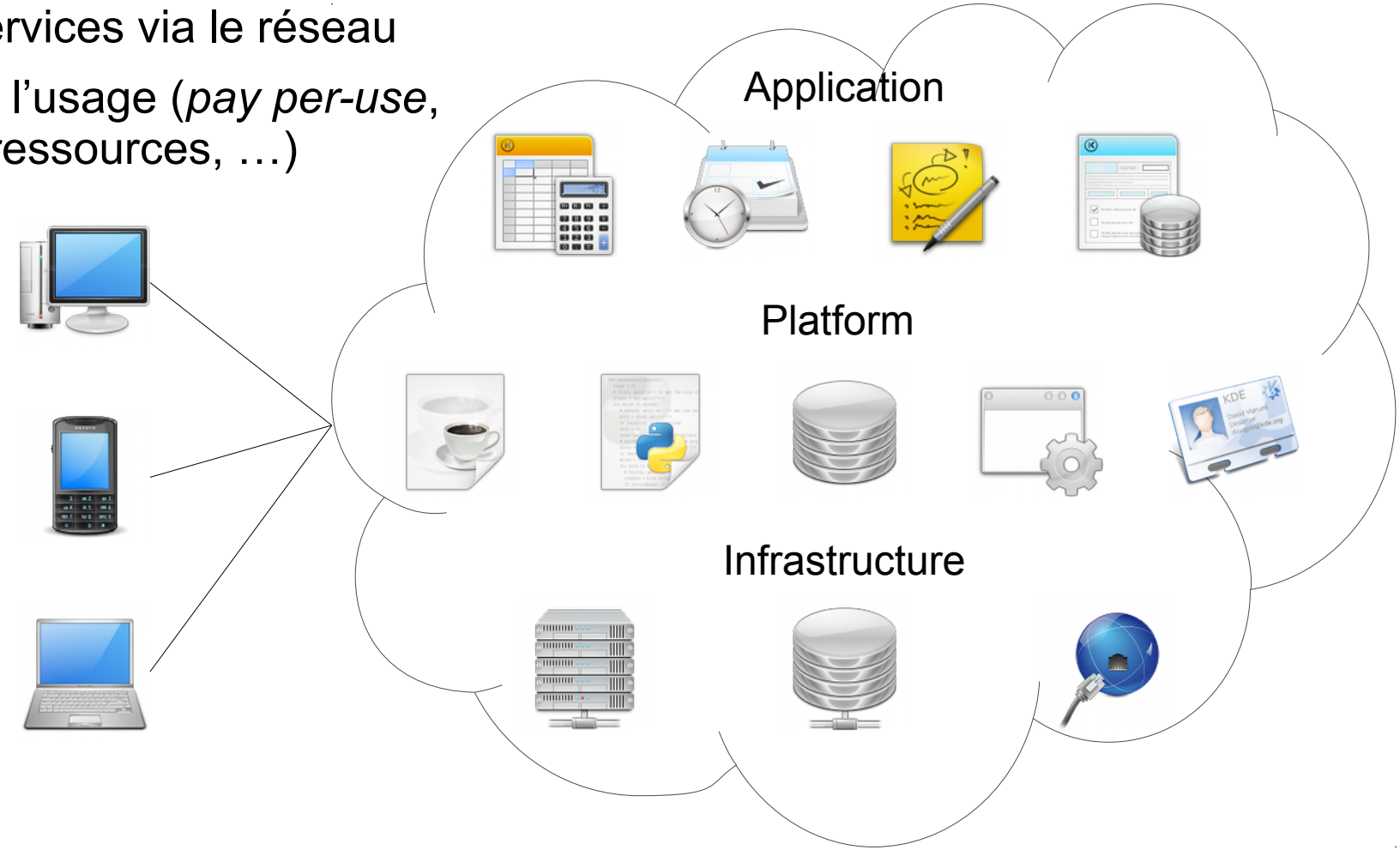
Sommaire

- Kubernetes dans le Cloud ?
- Cloud commerciaux
- Cloud académiques
- Interaction avec OpenStack

Cloud IaaS ?

Le Cloud IaaS

- Composition à base de CPU, RAM, disque et OS
- Accès aux services via le réseau
- Facturation à l'usage (*pay per-use*, partage des ressources, …)



Cloud IaaS ?

Des avantages intéressants …

- Utiliser un OS ou des outils spécifiques
- Déployer des infrastructures de test (rapidement et simplement)
- Intégration avec des outils supportant le Cloud nativement
- Anticiper les besoins (conteneurs, …)
- Effectuer des tâches longues
- Savoir facilement intégrer les réponses aux besoins de calcul hors norme
- Gestion des logiciels propriétaires par équipe
- Pouvoir déborder sur les centres partenaires / cloud commerciaux

Infrastructures de production

Différents types d'infrastructure

- Cloud commerciaux
  - Amazon, Google, Azur, … (US)
  - OVH, Outscale, Cloudwatt, Open Telekom Cloud, … (UE)
- Cloud académiques
  - Cloud du laboratoire
  - Plateforme régionale
  - CC-IN2P3
  - Fédération de Cloud (FG-Cloud, EGI FedCloud)

Choix de l'infrastructure

Accès

- Facilité d'utilisation et fiabilité
- Coût, contraintes / facilités d'accès (partenariats, type d'accès, ...)
- Compatibilité des APIs avec l'outil de gestion de conteneurs
- Ressources suffisantes pour votre projet, interopérabilité

Gestion des images

- Disponibilité d'images spécifiques (CoreOS, Fedora Atomic)
- Possibilité de charger ses propres images

Gestion du réseau

- Définition des groupes de sécurité / pare-feu
- Création de réseaux
- Accès à son *registry* Docker

Sommaire

- Kubernetes dans le Cloud ?
- Cloud commerciaux
- Cloud académiques
- Interaction avec OpenStack

Cloud Act

Clarifying Lawful Overseas Use of Data Act

- Divulgation des informations personnelles dans le cadre d'enquêtes
- Les données n'ont pas besoin d'être stockées sur le territoire américain
- Pas de validation des demandes par un juge
- Normalement encadré par un protocole cadre d'échange des données

Fournisseur commercial

https://www.ovh.com/fr/public-cloud

OVH

- Société française fondée en 1999
- Offre IaaS disponible depuis 2015
- 20 datacentres
- API et CLI OpenStack
- Images Ubuntu, CentOS, RedHat, Suse, Debian, Fedora, Windows server , ...
- Possibilité de charger ses propres images
- Kubernetes-as-a-Service (*alpha*), OVH Docker registry, GPU
- 8 VMs 16 cœurs / 56 GB RAM → ~ 12 € / jour

Fournisseur commercial

Cloudwatt (Orange)

- Société appartenant à Orange depuis mars 2015 (projet Andromède – Cloud souverain)
- Offre IaaS disponible depuis 2014
- 2 datacentres dans l'ouest de la France
- API et CLI OpenStack
- Images Ubuntu, CentOS, RedHat, Suse, Debian, Fedora, Windows server , ...
- Règlement par CB pour les commandes sur Internet, possibilité de fonctionner par bon de commandes
- Hadoop, Docker (CoreOS), Kubernetes HA multi-tenant multi-région
- 8 VMs 16 cœurs / 64 GB RAM → ~ 22 € / jour

Pas d'activité visible depuis juin 2017 … (→ stratégie Orange / Huawei?)

http://www.cloudwatt.com

Fournisseur commercial

Open Telekom Cloud (T-System)

- Cloud public de T-Systems (filiale Deustche Telekom)
- Datacentres en Allemagne et géré par T-Systems
- API et CLI OpenStack
- Images Linux, Windows, ...
- CB, bon de commande
- Retenu par le CERN dans le cadre du ….
- MapReduce, Kubernetes-as-a-Service, ...
- 8 VMs 16 cœurs / 64 GB RAM → ~ 19 € / jour

https://cloud.telekom.de/en/

Sommaire

- Kubernetes dans le Cloud ?
- Cloud commerciaux
- Cloud académiques
- Interaction avec OpenStack

Cloud académique

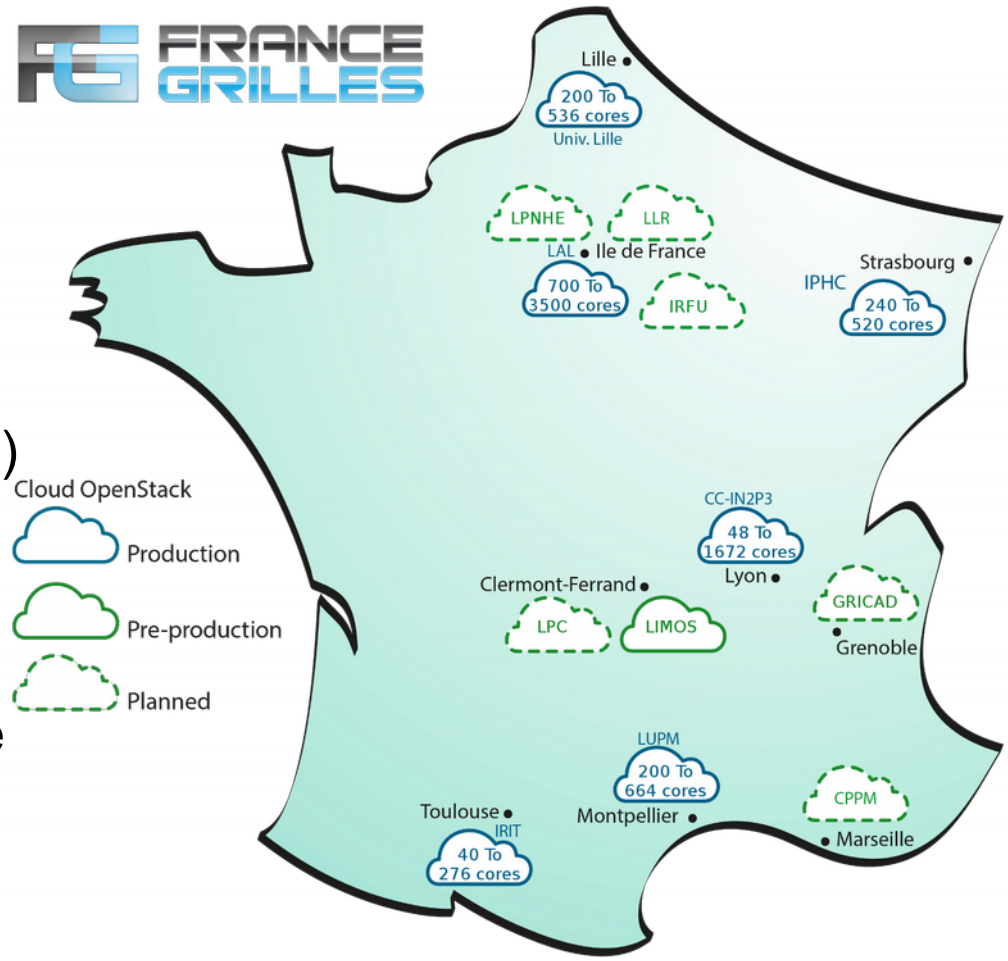
Plateforme SCIGNE

- Hébergée à Strasbourg et gérée par l'IPHC
- Labellisée par l'IN2P3
- Plateforme également accessible via EGI et l'IFB
- OpenStack / CEPH / iRODS
- 520 cœurs
- Gabarit jusqu'à 48 cœurs et 512 Go de RAM
- Kubernetes-as-a-service, calcul scientifique, formation, …
- Demande d'accès : scigne@iphc.cnrs.fr

Cloud académique

FG-Cloud

- Infrastructure fédérative de Cloud
- Pilotage par le groupe FG-Cloud
- En accord avec les stratégies locales
- Accessible via le catalogue de services France Grilles
- Géré avec OpenStack (API & CLI, Web)
- 7 sites en production, 7500 cœurs, 1500 To de stockage
- Surveillance fonctionnelle, distribution des images, authentification centralisée (outils non invasifs)



Cloud académique

FG-Cloud

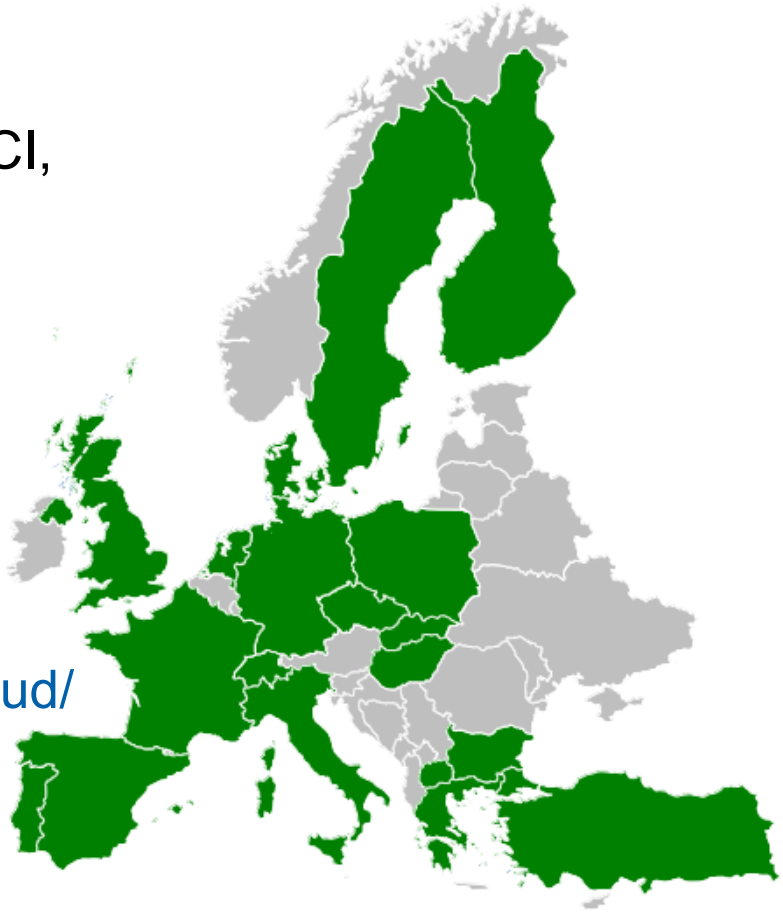
- Documentation, formation
- Cas d'utilisation :
  - Calcul scientifique (hors norme)
  - R&D
  - Projets nationaux
  - Web + analyse
  - …
- Possibilité de mutualisation (hébergement)
- Accès : contact@france-grilles.fr
- Retour des utilisateurs importants pour l'évolution de l'offre de services !

Cloud académique

Fédération de Cloud EGI

- Fédération de Clouds privés académiques
- Disponible en tant que Cloud IaaS pour les scientifiques en Europe et au-delà
- Basé sur l'utilisation de standards ouverts : OCCI, CDMI, OVF, GLUE, ...
- Implémentation hétérogène (API commune)
- Surveillance centralisée des infrastructures
- Équipe de sécurité internationale
- Catalogue important de VMs (par discipline)

→ https://www.egi.eu/federation/egi-federated-cloud/



Cloud académique

Fédération de Cloud EGI

- Possibilité de déployer des images pré-configurées avec Docker
  → https://wiki.egi.eu/wiki/Federated_Cloud_Containers
- Base Ubuntu 14.04 et Ubuntu 16.04
- NVIDIA Docker
- Accès par VO / formulaire en ligne
- Ressources accessibles par défaut en mode opportuniste
- Interface Web de gestion des déploiements :
  → https://appdb.egi.eu

Sommaire

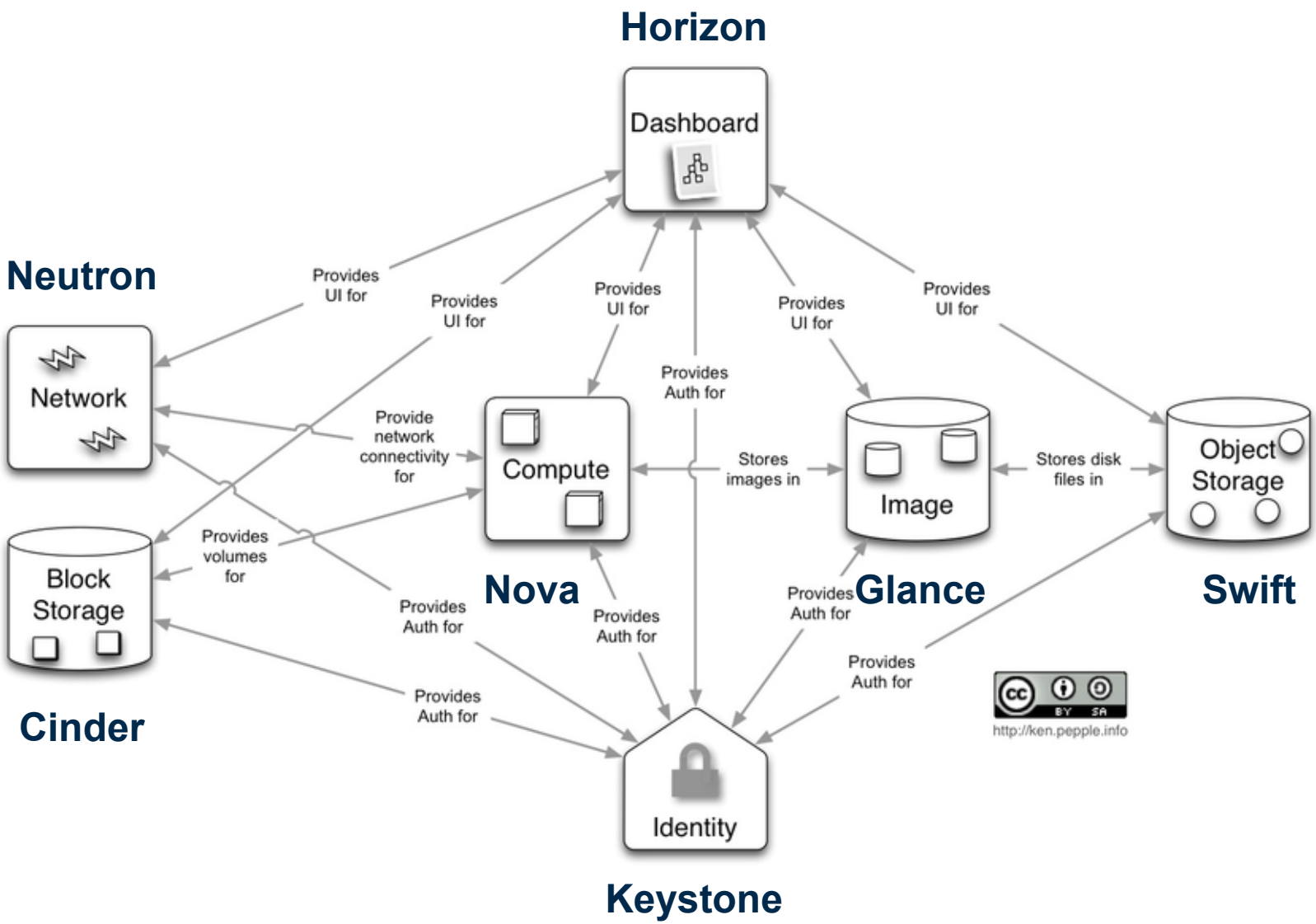
- Kubernetes dans le Cloud ?
- Cloud commerciaux
- Cloud académiques
- Interaction avec OpenStack

OpenStack

En quelques mots

- Middleware Cloud ouvert et libre
- Licence Apache 2.0
- Rackspace (stockage) + NASA (calcul) en 2010
- Développé en python
- Fondation (600 organisations, 85 k personnes)
- Composé de modules (un module ↔ une tâche)
- Largement déployé dans le monde professionnel (académique et privé)
- Version actuelle Pike et Queens (Ocata dans plusieurs distribution)
- Cycle rapide de développement (6 mois)

OpenStack


Horizon
Dashboard
Neutron
Network
Provides UI for
Provides UI for
Provides UI for
Provides UI for
Provides UI for
Provides Auth for
Provide network connectivity for
Compute
Stores images in
Image
Stores disk files in
Object Storage
Block Storage
Provides volumes for
Nova
Glance
Swift
Provides Auth for
Provides Auth for
Provides Auth for
Provides Auth for
Cinder
Identity
Keystone
http://ken.pepple.info

Docker Machine

Un outil multi-plateforme

- Déploiement et gestion de conteneurs dans le Cloud
- Compatible VMware Fusion, VirtualBox, AWS, Azure, Google Compute Engine, OpenStack …
- Installation :
  → https://docs.docker.com/machine/install-machine/
- Exemple d'utilisation :

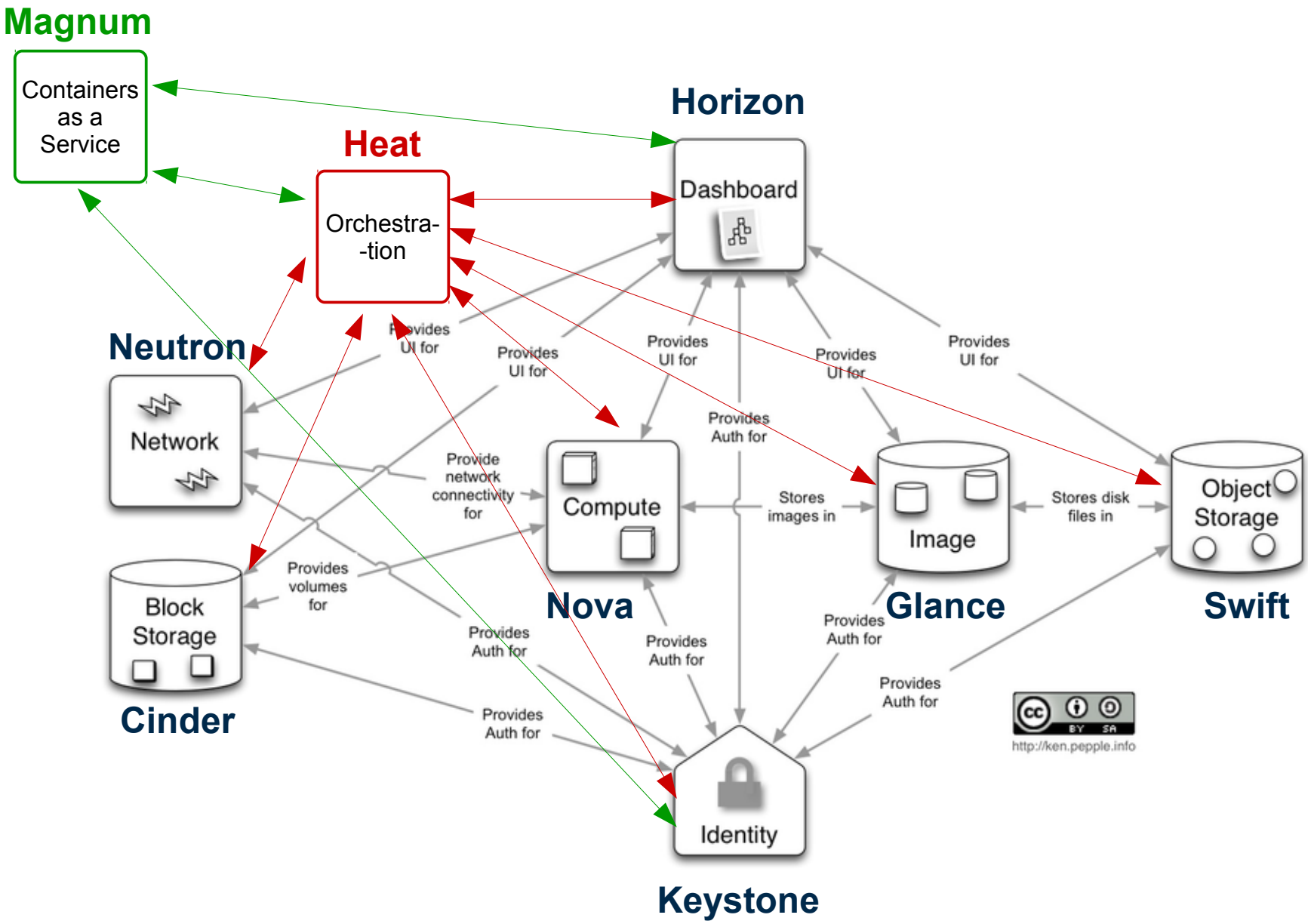
```
$ docker-machine create -d openstack –openstack-domain-name \
  Default --openstack-username myusername –openstack-password \
  changeme --openstack-tenant-name formation \
  --openstack-auth-url https://sbgcloud.in2p3.fr:5000/v3 \
  --openstack-flavor-id 2 --openstack-net-name formation-net \
  --openstack-floatingip-pool ext-net –openstack-image-id \
  88c8d1d0-6819-11e8-a370-ff5b2da2a487 –openstack-keypair-name \
  securekey --openstack-private-key-file path/securekey \
  --openstack-ssh-user centos
  mydockervm
```

Magnum

Conteneurs à la demande

- Module pour le déploiement de Docker Swarm, Kubernetes et Apache Mesos
- Basé sur le module Heat (orchestration)
- Module Ironic optionnel (déploiement *bare metal*)
- Sécurisation par projet
- Taille ajustable
- Système de *template* (Heat)
- Basé sur CoreOS ou Fedora Atomic
- Composant encore jeune

Magnum


Magnum
Containers as a Service
Heat
Orchestra--tion
Horizon
Dashboard
Neutron
Network
Provides UI for
Provides UI for
Provides UI for
Provides UI for
Provides UI for
Provides Auth for
Provide network connectivity for
Compute
Stores images in
Image
Stores disk files in
Object Storage
Block Storage
Provides volumes for
Nova
Glance
Swift
Provides Auth for
Provides Auth for
Provides Auth for
Provides Auth for
Cinder
Identity
Keystone
http://ken.pepple.info

Magnum

Exemple d'utilisation

```
$ openstack coe cluster template list
+--------------------------------------+--------------------------------------+
| uuid                                 | name                                 |
+--------------------------------------+--------------------------------------+
| 1d6fcc5e-104e-475f-9254-f1e6f9a71896 | swarm-fedora-atomic26                |
| eb8c8d8f-7359-4177-bcb8-3abe7d0ec3b8 | k8s-fedora-atomic26-cluster-template |
+--------------------------------------+--------------------------------------+

$ openstack coe  cluster create  --cluster-template k8s-fedora-atomic26 \
  --node-count 2 --name monclusterk8s
   Request to create cluster 07e has been accepted.


$ openstack coe cluster list
+------------+--------------+-----------+-------------+--------------------+
| uuid       | name         | node_count | master_count | status             |
+------------+--------------+-----------+-------------+--------------------+
| 07e9f716... | monclusterk8s |          2 |            1 | CREATE_IN_PROGRESS |
+------------+--------------+-----------+-------------+--------------------+
```

Magnum

Exemple d'utilisation

```
$ openstack coe cluster show monclusterk8s
```

Field	Value
status	CREATE_COMPLETE
cluster_template_id	eb8c8d8f-7359-4177-bcb8-3abe7d0ec3b8
node_addresses	[u'134.158.151.143', u'134.158.151.134']
uuid	77da102e-14a6-4b35-8e27-f9ce4237760d
stack_id	915373e8-83d7-47bb-a2ef-e9dd02aa5c63
status_reason	Stack CREATE completed successfully
created_at	2018-05-28T08:02:29+00:00
updated_at	2018-05-28T09:06:12+00:00
coe_version	v1.7.4
faults	
keypair	cloudkey
api_address	https://134.158.151.109:6443
master_addresses	[u'134.158.151.109']
create_timeout	60
node_count	2
discovery_url	https://discovery.etcd.io/393491e97871b13c2e3b8b78420858d9
master_count	1
container_version	1.12.6
name	monclusterk8s

Magnum

Export de la configuration

```
$ openstack  coe cluster config monclusterk8s
export KUBECONFIG=/home/user/config

apiVersion: v1
 clusters:
 - cluster:
     certificate-authority: /home/user/ca.pem
     server: https://134.158.151.109:6443
   name: monclusterk8s
 contexts:
 - context:
     cluster: monclusterk8s
     user: monclusterk8s
   name: monclusterk8s
 current-context: monclusterk8s
 kind: Config
 preferences: {}
 users:
 - name: monclusterk8s
   user:
     client-certificate: /home/user/cert.pem
     client-key: /home/user/key.pem
```

Magnum

Exemple d'utilisation

```
$ [fedora@monclusterk8s ~]$ kubectl cluster-info

Kubernetes master is running at http://localhost:8080
CoreDNS is running at http://localhost:8080/api/v1/namespaces/kube-
system/services/kube-dns/proxy
[fedora@monclusterk8s ~]$ kubectl get nodes
k8-lbcpd7kagr-0-e62qarrc5asx-kube-minion-4or6eo443za4   Ready                      44m
     v1.7.4
k8-lbcpd7kagr-1-635t36ajymyj-kube-minion-nhfuxaviylxc   Ready                      45m
     v1.7.4
k8-qdg4chvdta-0-3tx4dcdhn2p6-kube-master-ju7tz7oued7j   Ready,SchedulingDisabled   49m
     v1.7.4
```

Magnum

Exemple d'utilisation

```
$ openstack coe cluster update monclusterk8s replace node_count=4


$ openstack coe cluster list
+----------+------+----------+------------+--------------+--------------------+
| uuid     | name | keypair  | node_count | master_count | status             |
+----------+------+----------+------------+--------------+--------------------+
| 07e9f716 | k8s  | cloudkey |          4 |            1 | UPDATE_IN_PROGRESS |
+----------+------+----------+------------+--------------+--------------------+
```

Magnum

Des avantages

- Déploiement simple de cluster Kubernetes
- Une certaine élasticité
- Suite logiciel maintenu
- Aspect sécurité bien traité (chiffrement et authentification)
- Accessible via le dashboard

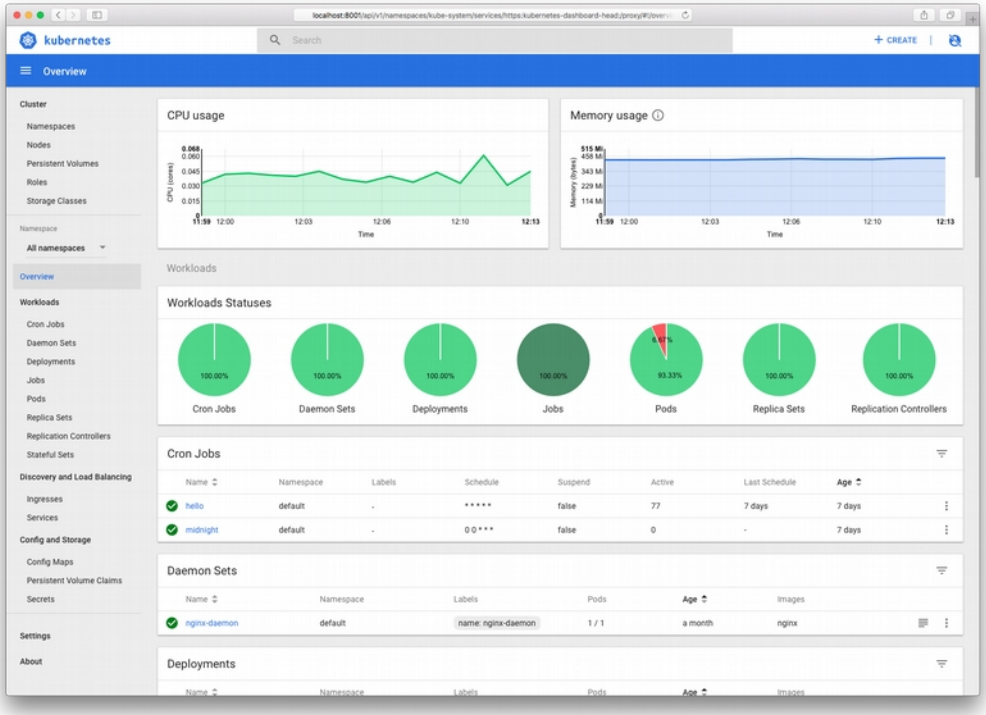
Et des inconvénients

- Projet jeune
- Stress important sur le service de messagerie RabbitMQ
- Nombre de couches importantes ne facilitant pas l'analyse des problèmes
- Toutes les versions de Fedora Atomic ne sont pas supportées

Sécurité

Il faut protéger son déploiement Kubernetes

- Vérifier les *security group*
- Mettre en place un système d'authentification sur tableau de bord Kubernetes
- Vérifier les images Docker disponibles



Questions ?