Infrastructures de Cloud en production pour le déploiement

Jérôme Pansanel

ANF ADA – 30 septembre 2019

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

Types de déploiement

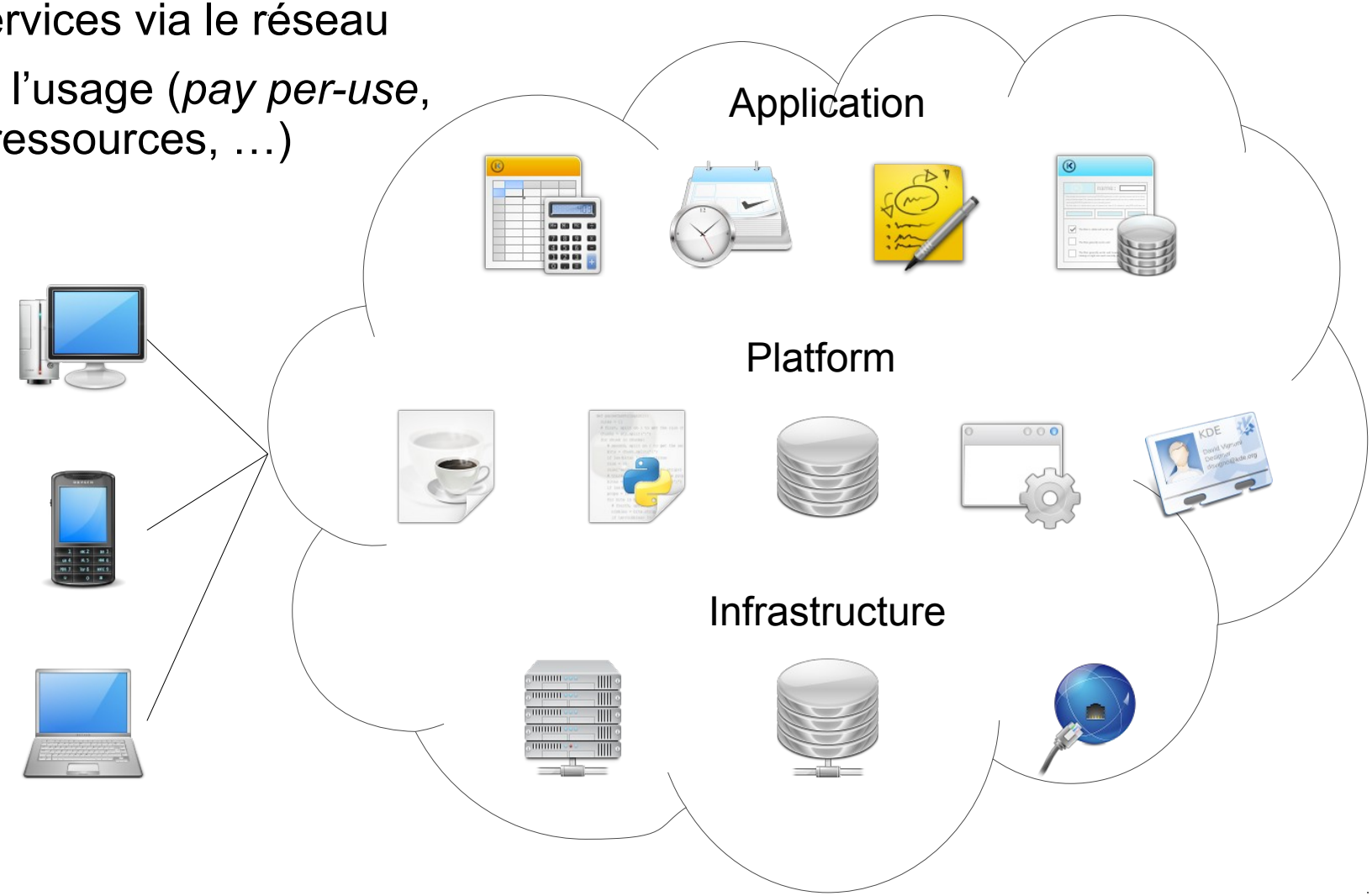
Où déployer un SI ?

- Sur vos serveurs (x86, rasberry, ...)
- Chez un prestataire (par ex. fournisseur de Cloud)
- Les deux
- Via des conteneurs hébergés dans les infrastructures citées ci-dessus

Cloud IaaS ?

Le Cloud IaaS

- 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 hors norme
- Gestion des logiciels propriétaires par équipe
- Pouvoir déborder sur les centres partenaires / cloud commerciaux

Ressources dans le Cloud IaaS

Différents types de ressource dans le Cloud

- Machine virtuelle (VM)
- Bare metal
- Conteneurs

VM vs bare metal

- Performance (coût CPU et mémoire, latence réseau)
- Roll-back / snapshot
- Sécurité (machine mono projet vs flash bios, re-configuration des hyperviseurs, sécurité réseau)

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
  - CC-IN2P3
  - Fédération de Cloud (FG-Cloud, EGI FedCloud)
  - Cloud communautaire (IFB, …)
  - Plateforme régionale

Choix de l'infrastructure

Accès

- Facilité d'utilisation et fiabilité
- Coût, contraintes / facilités d'accès (partenariats, type d'accès, ...)
- Compatibilité des APIs avec vos OS / déploiement
- Ressources suffisantes pour votre projet, interopérabilité

Gestion des images

- Disponibilité d'images spécifiques
- Possibilité de charger ses propres images

Gestion du réseau

- Définition des groupes de sécurité / pare-feu
- Création de réseaux

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

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 → ~ 4338 € / an

Fournisseur commercial

Outscale

- Société créée en 2010, soutenue par Dassault Systèmes
- Une réponse au problème de Cloud souverain
- Offre IaaS disponible depuis 2011
- Plusieurs datacentres
- API et CLI AWS
- Images Linux, Windows server , ...
- Image Docker, GPU
- 8 VMs 16 cœurs / 64 GB RAM → ~ 6812 € / an

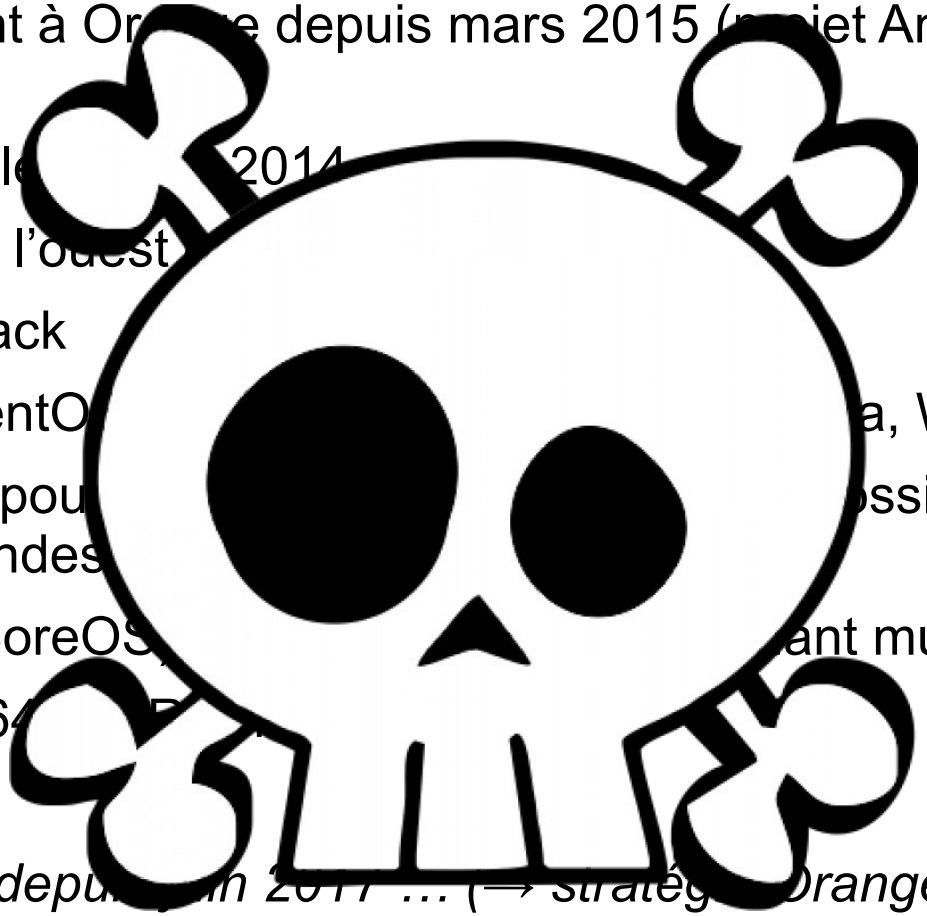
https://fr.outscale.com

Fournisseur commercial

Cloudwatt (Orange)

- Société appartenant à Or[illegible]e depuis mars 2015 (p[illegible]iet Andromède – Cloud souverain)
- Offre IaaS disponible[illegible]2014
- 2 datacentres dans l'ouest
- API et CLI OpenStack
- Images Ubuntu, CentO[illegible]a, Windows server , ...
- Règlement par CB pou[illegible]ssibilité de fonctionner par bon de commandes
- Hadoop, Docker (CoreOS[illegible]ant multi-région
- 8 VMs 16 cœurs / 64 [illegible]

Pas d'activité visible depu[illegible]in 2017 … (→ stratég[illegible]Orange / Huawei?)



http://www.cloudwatt.com

Fournisseur commercial

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

Ikoula

- Société française possédant ses propres infrastructures et datacentres (en France) créée en 1998
- 2 datacentres en France (Reims et Eppes)
- API et CLI CloudStack
- Images Ubuntu, CentOS, RedHat, Fedora, Windows server , ...
- Basé sur Apache CloudStack
- Gabarits d'instance en nombre limité, pas de GPU
- 8 VMs 32 cœurs / 64 GB RAM → ~ 3839 € / an

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 → ~ 4906 € / an

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

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

Cloud académique

CC-IN2P3

- Cloud basé sur OpenStack (CLI / API, Web, EC2)
- Infrastructure labellisé par l'IN2P3
- OpenStack
- ~ 6560 cœurs et 33,3 To de RAM
- Trois niveaux d'offre :
  - HA (haute disponibilité)
  - Calcul (performance CPU)
  - R&D
- Images Ubuntu, SL, CentOS, CernVM
- Possibilité d'ajouter ses propres images

→ https://doc.cc.in2p3.fr/infrastructure:cloud:start

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

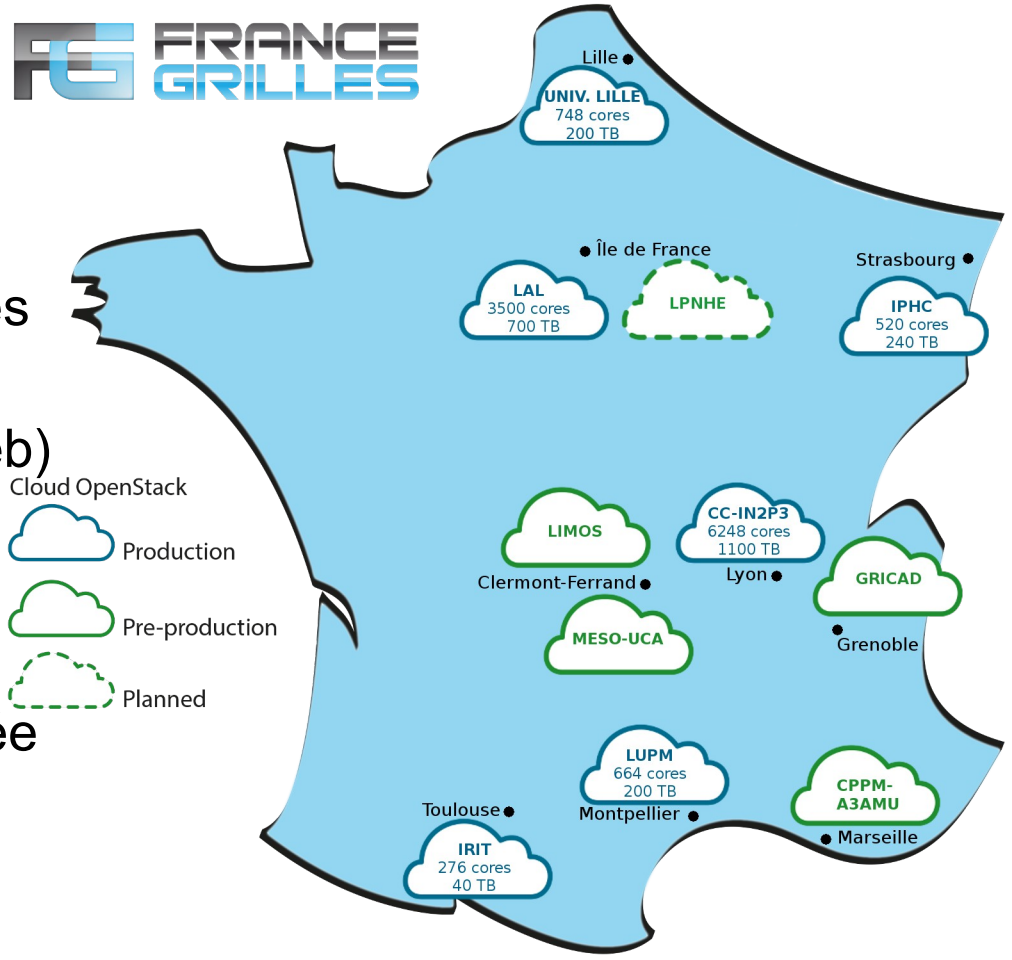
Plateforme Cloud @ Virtual Data

- Hébergée à P2IO (Orsay) et gérée par le LAL
- Labellisée par l'IN2P3
- OpenStack / CEPH
- ~ 3500 cœurs
- Hébergement d'infrastructure de calcul scientifique : Spark (300 cœurs / 40 To), JupyterHub (80 coeurs), DW4NP (Data Workflow 4 Nuclear Physics - projet CSNSM-IPNO)
- Contact: http://openstack.lal.in2p3.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)
- 6 sites en production, 7500 cœurs, 1500 To de stockage
- Surveillance fonctionnelle, distribution des images, authentification centralisée (outils non invasifs)



Cloud académique

FG-Cloud

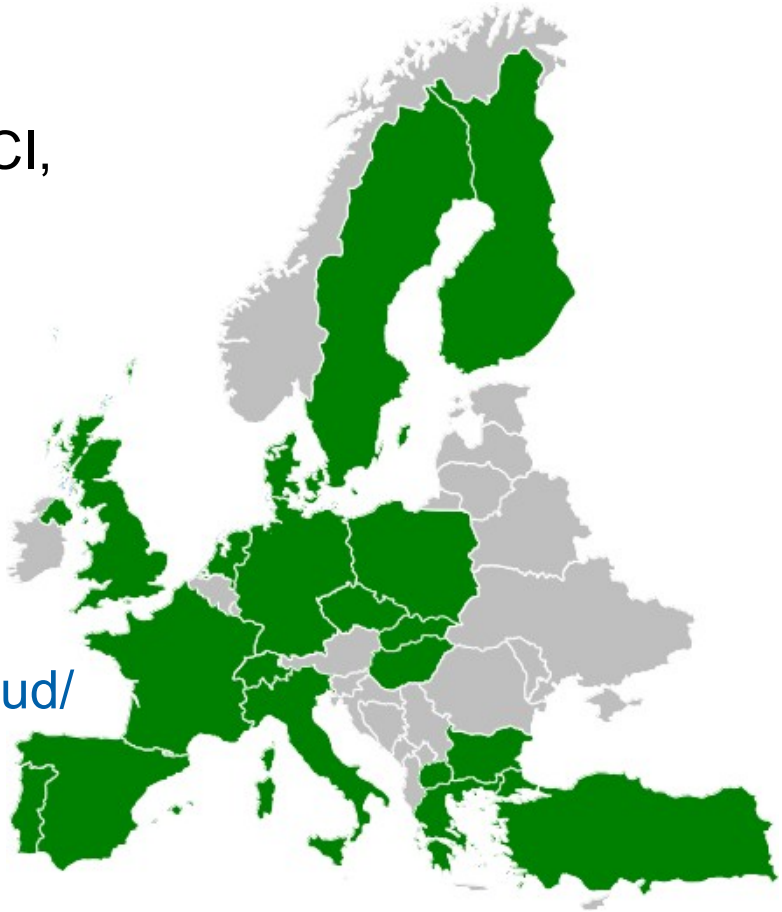
- Documentation, formation
- Cas d'utilisation :
  - Calcul scientifique (hors norme)
  - R&D
  - Projets nationaux
  - Web + analyse
  - …
- Possibilité de mutualisation (hébergement)
- Accès : contact@france-grilles.fr
- Retour des utilisateurs importants pour l'évolution de l'offre de services !

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 16.04 et Ubuntu 18.04
- NVIDIA Docker
- Accès par VO / formulaire en ligne
- Ressources accessibles par défaut en mode opportuniste
- Interface Web de gestion des déploiements :
  → https://dashboard.appdb.egi.eu/vmops

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

OpenStack

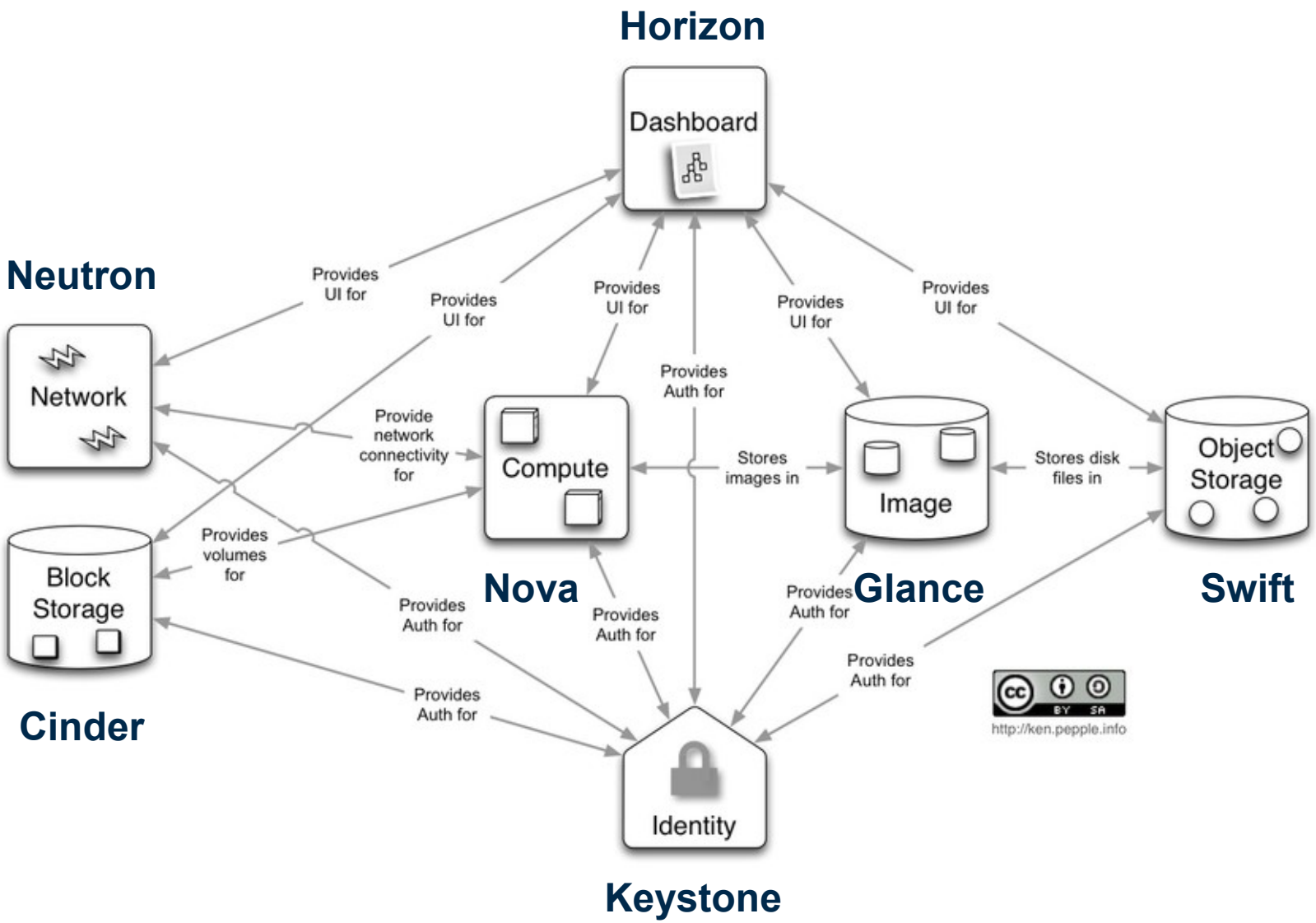
En quelques mots

- *Middleware* Cloud ouvert / libre (licence Apache 2.0)
- Rackspace (stockage) + NASA (calcul)
- Développement Python, très actif
- RedHat, IBM, Dell, Intel, Cisco, Juniper, NetApp, HP, VMWare, …
- Disponible dans de nombreuses distributions

Modules

- Nova : Calcul
- Cinder : Stockage bloc
- Neutron : Réseau (SDN)
- Glance : Images VM
- Keystone : Identité
- Horizon : UI web
- Swift : Stockage objet
- Heat : Orchestration
- Trove : Bases de données
- Ironic : Bare-metal
- Magnum : Conteneurs
- Sahara : traitement de données
- Barbican : Gestion de clés
- Manila : Systèmes de fichiers partagés

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
Provides Auth for
Cinder
Identity
Keystone
http://ken.pepple.info

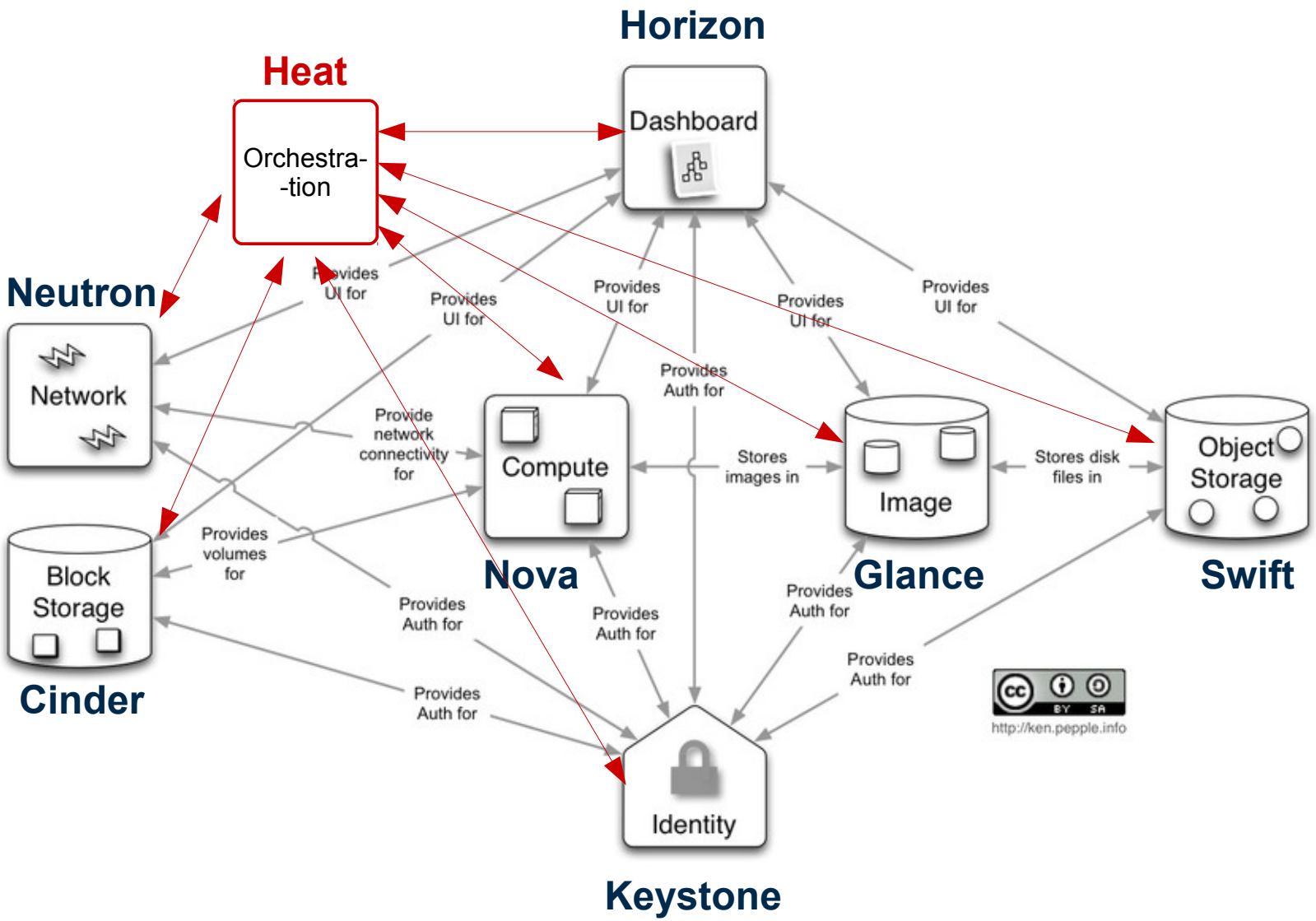
Heat

Orchestration de machines virtuelles

- Inspiré de CloudFormation (AWS)
- Description de l'infrastructure dans un fichier *template* structuré (YAML)
- Format HOT (Heat Orchestration Template)
- Ce fichier peut être instancié en stack (ensemble de ressources)
- Heat s'occupe de l'allocation des ressources en faisant les demandes auprès des différents services OpenStack
- Possibilité de passer des variables au lancement d'un stack
- Possibilité de récupérer des valeurs (IPs, …) à la fin du lancement
- Possibilité d'*auto-scaling* (interaction avec les outils de métrologie)

→ **https://docs.openstack.org/heat/latest/template_guide/**

Heat


Horizon
Heat
Orchestra-
-tion
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
Identity
Cinder
Keystone
http://ken.pepple.info

Heat

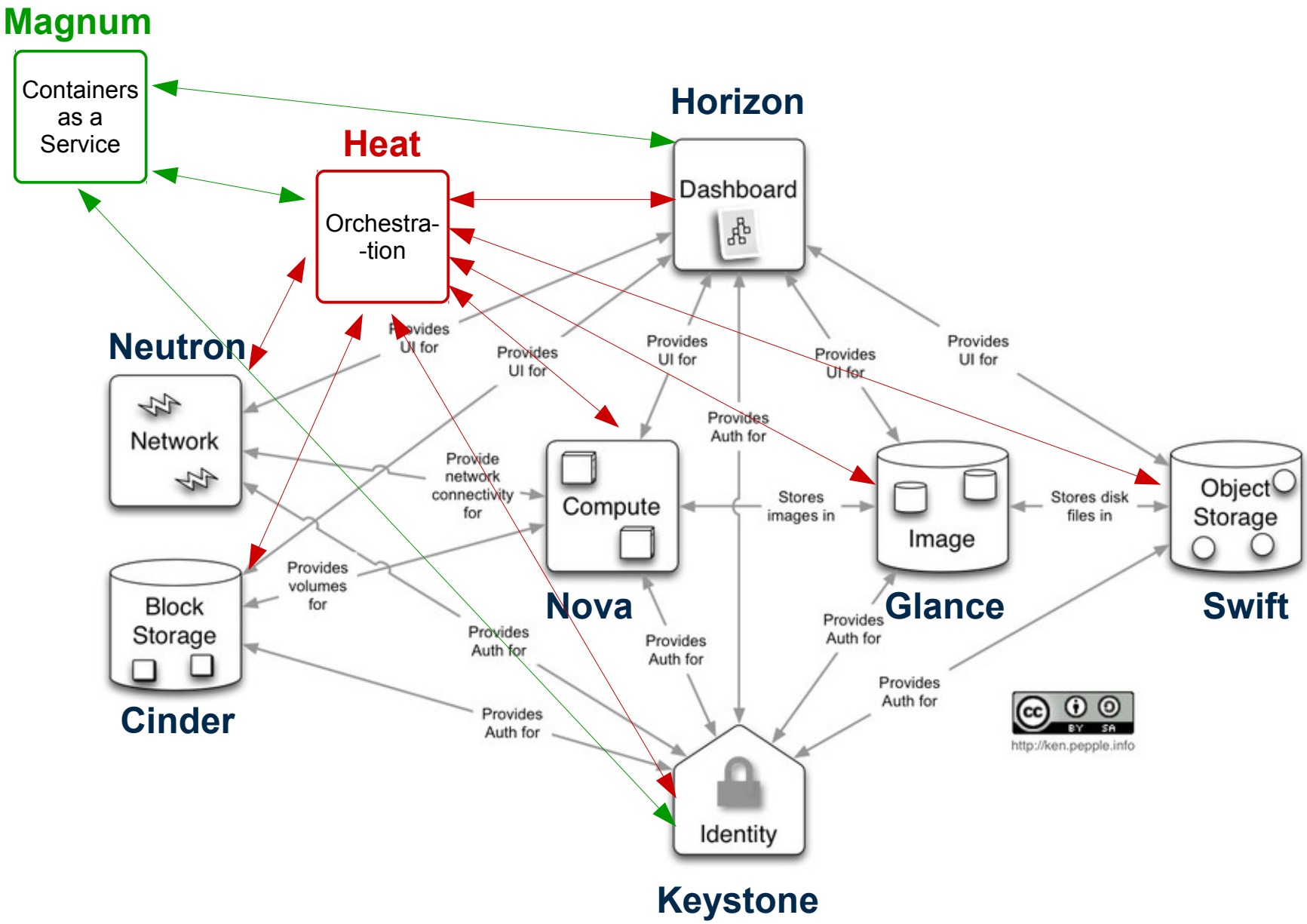
```
heat_template_version: rocky
description: >
    Simple template to deploy a single compute instance with an attached
    volume on the France Grilles Federated Cloud.
parameters:
    key_name:
        type: string
        description: Name of keypair to assign to servers
    name:
        type: string
        description: Name of the instance to create
resources:
    fg_instance:
        type: OS::Nova::Server
        properties:
            name: { get_param: name }
            key_name: { get_param: key_name }
            image: FG_Cloud-Ubuntu-16.04-x86_64
            flavor: m1.small
            networks:
                - port: { get_resource: fg_instance_port }
    fg_volume:
        type: OS::Cinder::Volume
        properties:
            size: 10
    fg_attachment:
        type: OS::Cinder::VolumeAttachment
```

Magnum

Orchestration de conteneurs à la demande

- Module pour le déploiement de Docker Swarm, Kubernetes et Apache Mesos
- Basé sur le module Heat (orchestration)
- Module Ironic optionel (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
Horizon
Heat
Dashboard
Orchestra--tion
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

SDKs et API

SDK

- Disponible dans de nombreux langages (Python, GO, Java, …)
- Possibilité d'utiliser des bibliothèques compatibles (Apache JClouds, …)
- Nombreux exemples pour les clients Python OpenStack : https://docs.openstack.org/openstacksdk/latest/

API

- Tous les modules accessibles via une API REST
- Documentation complète : https://docs.openstack.org/api-quick-start/index.html
- Accessible simplement avec **curl** ...

SDK Python : authentification

```
import sys

from keystoneauth1.identity import v3
from keystoneauth1 import session

auth_params = {
    'username': 'nom_utilisateur', 'password': 'super_mdp',
    'auth_url': 'https://sbgcloud.in2p3.fr:5000/v3',
    'project_name': 'FG_formation', 'user_domain_name': 'Default',
    'project_domain_name': 'Default'
}

auth = v3.Password(**auth_params)
sess = session.Session(auth=auth)

# Get Glance endpoint
glance_endpoint = sess.get_endpoint(service_type='image')
sys.stdout.write(glance_endpoint + "\n")
```

http://sbgcloud.in2p3.fr:9292

SDK Python : session

```
import sys

import openstack

auth_params = {
    'username': 'nom_utilisateur', 'password': 'super_mdp',
    'auth_url': 'https://sbgcloud.in2p3.fr:5000/v3',
    'project_name': 'FG_formation', 'user_domain_name': 'Default',
    'project_domain_name': 'Default'
}

cloud = openstack.connect(**auth_params)

for server in cloud.compute.servers():
    sys.stdout.write(server.id + "\n")
```

```
0d9046a0-ae42-42ee-99e5-ec29489b2835
dd23942b-cc51-4e7f-96e8-ad0dd9ba91a6
0c49b4fd-3a94-4015-91fe-dbe013bffabc
18c933c6-5abd-4095-b884-4949950de8b5
```

API

```
REQ=$(curl -i \
  -H "Content-Type: application/json" \
  -d '
{ "auth": {
    "identity": {
      "methods": ["password"],
      "password": {
        "user": {
          "name": "nom_utilisateur",
          "domain": { "id": "default" },
          "password": "super_mdp"
        }
      }
    }
  }
}' \
  "https://sbgcloud.in2p3.fr:5000/v3/auth/tokens")

OS_TOKEN=$(echo "${REQ}" | awk '/X-Subject-Token: /{print $NF}')

echo ${OS_TOKEN}
```

Sommaire

- Quelles solutions pour déployer vos infrastructures ?
- Cloud commerciaux
- Cloud académiques
- Automatisation des déploiements OpenStack
- Orchestration multi-cloud

Orchestration

Chaque fournisseur de technologie à ses propres

- APIs
- Langages
- Mécanicismes de fonctionnement
- Modèles de données
- Gestionnaires des erreurs
- Sémantiques
- Mécanismes de sécurité

Comment abstraire ces points pour faciliter le déploiement multi-Cloud ?

Orchestration

TOSCA

- Topology and Orchestration Specification for Cloud Applications
- Une spécification
- Standardisation du format de description de tous les types d'éléments pour déployer un SI (et le déployer dans un Cloud)
- Format YAML
- Compatible OpenStack (heat-translator), Cloudify, CloudFoundry et CloudFormation (TOSCAna)
- https://www.oasis-open.org/committees/tosca

Orchestration

```
tosca_definitions_version: tosca_simple_yaml_1_0

imports:
  - indigo_custom_types:
https://raw.githubusercontent.com/indigo-dc/tosca-types/master/custom_types.yaml

description: >
  TOSCA test for launching a Kubernetes Virtual Cluster.
topology_template:
  inputs:
    admin_username:
      type: string
      description: Username of the admin user
      default: kubeuser
    admin_token:
      type: string
      description: Access Token for the admin user
      default: not_very_secret_token

node_templates:
  lrms_front_end:
    type: tosca.nodes.indigo.LRMS.FrontEnd.Kubernetes
    properties:
      admin_username:  { get_input: admin_username }
      admin_token: { get_input: admin_token }
    requirements:
      - host: lrms_server
```

Déploiement multi-cloud

Outils d'orchestration

- Développement « maison » (par ex. https://dashboard.appdb.egi.eu/)
- Cloudify - https://cloudify.co/
- Morpheus – https://www.morpheusdata.com
- Occopus - https://github.com/occopus
- Platform 9 – https://platform9.com/
- Slipstream – https://github.com/slipstream
- Terraform – https://www.terraform.io

Déploiement de conteneurs

Docker-machine

- 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
```

Déploiement de conteneurs

Orchestration

- Crossplane
- Federation Kubernetes
- Mesosphere (D2iQ)
- Nuvla 2 (SixSq, *work in progress*)
- OpenShift (RedHat)
- Platform 9 – https://platform9.com/
- Rancher

→ **https://landscape.cncf.io/**

ANSIBLE

Automatisation de la configuration

- Logiciel libre pour le déploiement et la configuration des logiciels
- Support officiel par RedHat
- Gestion des nœuds à travers SSH sans agent
- *Playbook* rédigés en YAML décrivent les tâches à effectuer
- Pas de langage prédéfini pour les modules, mais nécessitent d'être idempotent
- Outil couramment utilisé pour la configuration des machines virtuelles et des infrastructures sous-jacentes
- API Python …

→ **https://www.ansible.com**

ANSIBLE

Déploiement d'une VM

- Utilisation du module *os_server* et du module Python openstacksdk
- https://www.cloudandheat.com/manage-openstack-vms-with-ansible/

```
- name: launch a compute instance
  hosts: localhost
  tasks:
    - name: launch an instance
      os_server:
        state: present
        auth:
          auth_url: https://sbgcloud.in2p3.fr:5000
          username: nom_utilisateur
          password: super_mdp
          project_name: FG_formation
        name: vm1
        region_name: IPHC
        image: 2ba4257c-eb25-4e0b-bf9e-38b2f10822b9
        key_name: cloudkey
        flavor: 2
        security_groups: default
        auto_ip: yes
```

Questions ?