



Présentation d'OpenStack

Vincent LEGOLL <vincent.legoll@idgrilles.fr>
Jérôme PANSANEL <jerome.pansanel@iphc.cnrs.fr>

IPHC – Décembre 2015

Histoire

- *Middleware Cloud* ouvert / libre
- Rackspace (stockage) + NASA (calcul)
- Développé en python
- Licence Apache 2.0
- Fondation :
 - Juridique
 - RH (dev, marketing, release manager)
 - Infrastructure
 - Organisation des *OpenStack summit* (4,5K participants)
 - *500 organisations*
 - *23K membres individuels*

Rythme des versions

6 mois d'intervalle (Avril ~ Octobre) :

- Austin (2010.1)
- Bexar (2011.1)
- [...]
- Havana (2013.2)
- Icehouse (2014.1)
- Juno (2014.2)
- Kilo (2015.1)
- Liberty (2015.2)
- Mitaka (2016.1)
- N... (2016.2)
- O... (2017.1)

Largement supporté

Pour la version kilo :

- ~1500 contributeurs
- 70 organisations
- + de 7K bogues corrigés
- 800K chaînes traduites
- RedHat, IBM, Dell, Intel, Cisco, Juniper, NetApp, HP, VMWare, Google, Yahoo...

Développement :

- Ouvert a tous
- Cycles courts (6 mois)
- Git, GitHub, Gerrit, Launchpad, Jenkins
- Très actif (17K commits / icehouse : havana + 25 %)

The background of the slide features a smiling woman on the left and a hand-drawn diagram on the right. The diagram shows a circular flow with arrows and some handwritten text, including 'grilles' and 'consignations'.

Largement utilisé

Secteur public :

- CERN
- Harvard
- INFN
- MIT
- Wikimedia
- FG-Cloud : fédération France Grilles
- EGI FedCloud : APIs occi, ooi

Secteur privé :

- OVH
- Paypal
- Seagate
- Orange
- Disney
- Sony
- American Express

Secteur Français, *cloud* souverain :

- Cloudwatt (Orange, Thalès)
- Numergy (SFR, Bull)

En 2012 : Caisse des dépôts et
Consignations : 2 * 75 M€ pour 2 * 33%

Début 2015 : Orange rachète Cloudwatt

Octobre 2015 : procédure de sauvegarde
pour Numergy.

Architecture en composants

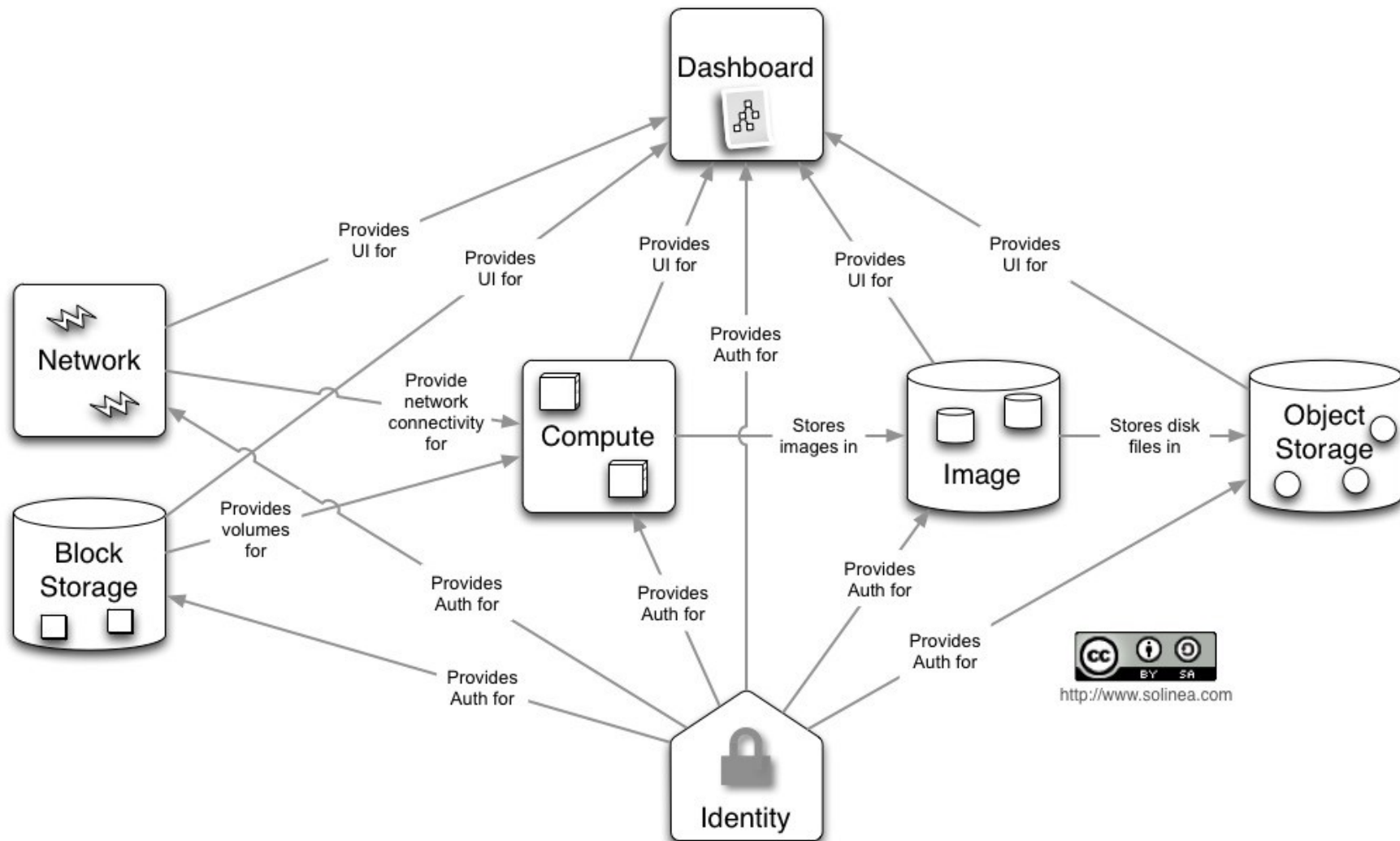
Chacun de ces composants est un projet séparé

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

Architecture en composants

- Chaque composant est découpé en services
- Communication par bus de messages AMQP : RabbitMQ, etc...
- Utilisation d'une base de données (MariaDB, MySQL, PostgreSQL)
- Ces composants supportent différentes API :
 - ReST
 - Librairies natives python
 - Amazon

Architecture



Keystone

- Annuaire d'utilisateurs et de groupes / projets (tenants)
- Catalogue de services
- Authentification
- Autorisation d'accès aux services
- Fonctionnement basé sur des « *tokens* »
- API admin : port 35357
- API utilisateur : port 5000

Les tenants ou projets

- Concept d'isolation des utilisateurs en groupes isolés
- Les utilisateurs ont des rôles sur des tenants
- Les ressources sont associées à un tenant
- Mais éventuellement partagées

Nova

Service de Calcul, fournit des instances de VM :

- Virtualisation : libvirt, KVM, Qemu, VMWare, Xen, vSphere
- Conteneurs : LXC, Docker, OpenVZ
- Instances éphémères (disque OS volatile)
- Les VMs sont instanciées par gabarits (flavor)
- Glance fournit les images
- Neutron fournit des ports réseaux
- Cinder fournit du stockage bloc

Nova²

Capacités :

- Redimensionnement d'une instance
- Migration possible d'une instance
- Groupes de sécurité : pare-feu pour chaque instance
- Service de méta-données personnalisées pour chaque instance
- Logs console de l'instance
- Accès console (VNC, Spice)

Nova++

Nova scheduler :

- Distribue les nouvelles instances sur les hyperviseurs
- Filtre en fonction des CPU, de la RAM, etc...
- Trie par poids en RAM (par défaut)

Nova conductor :

- Nœuds compute sont plus vulnérables
- Proxy entre nœuds compute et BDD
- Augmente la sécurité (évite des injections SQL, etc...)

Glance

- Catalogue d'images de VM
- Backend de stockage : disque local, swift, CEPH, etc...
- Les images ont des propriétés :
 - Format (type) : qcow2, iso, raw, vmdk, etc...
 - Taille disque minimum
 - Visibilité
 - RAM minimum
 - Publique ?
 - Etc...

Neutron

- Network as a Service
- Software Defined Networking
- IP flottantes
- Groupes de sécurité (firewall)
- Agents DHCP pour les instances
- Implémentation virtuelle : OpenVSwitch, etc...
- Implémentation matérielle : Cisco, Juniper, etc.
- L2, L3
- Équilibrage de charge (HAProxy)
- FwaaS
- VPN
- Utilise les namespaces réseau linux pour éviter les conflits d'IP
- Proxy metadata pour instances isolées

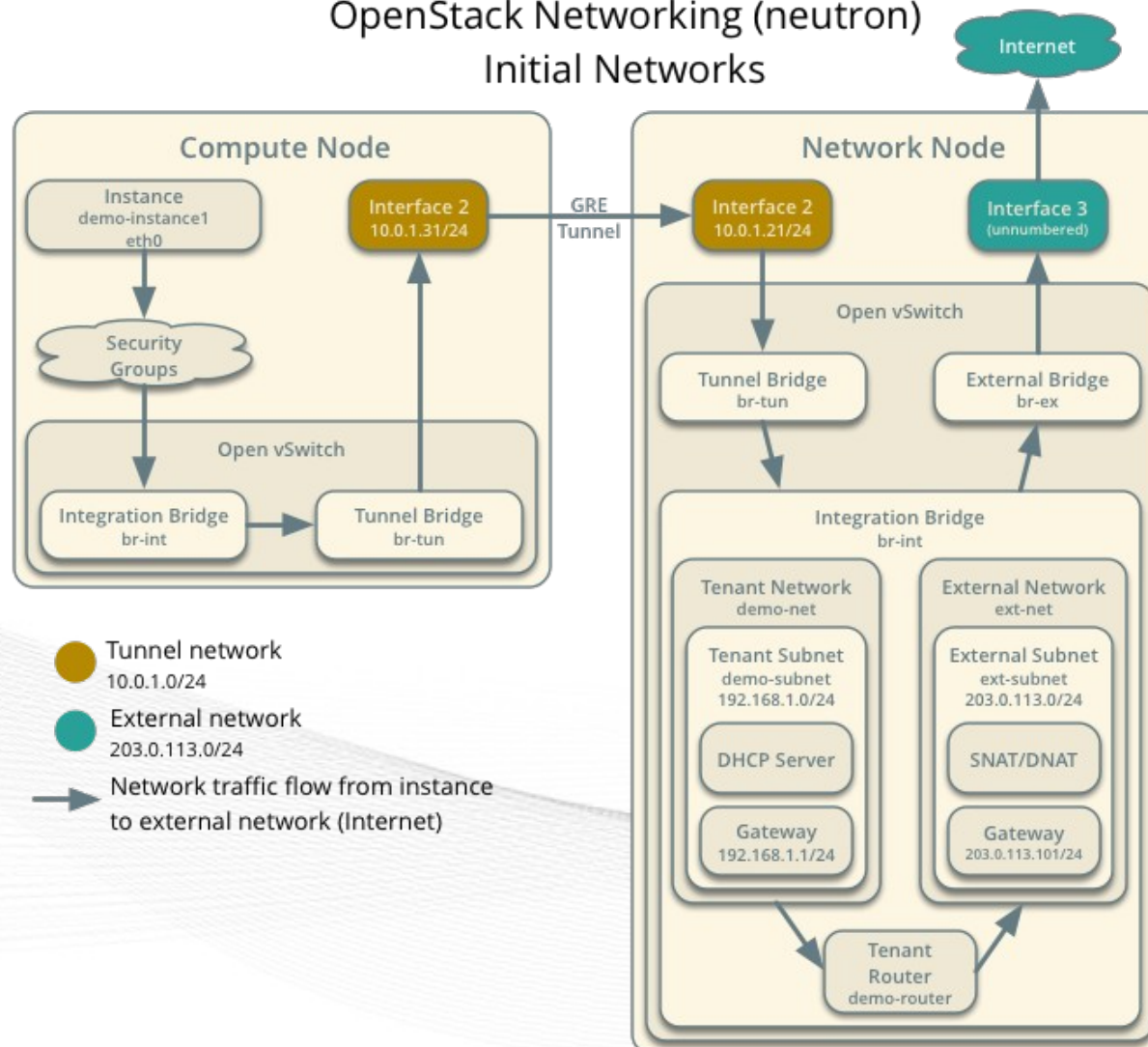
Neutron²

Les éléments présentés par l'API :

- Réseaux
- Sous-réseaux (plusieurs sur un réseau)
- Routeurs
- Ports qui connectent les éléments du réseau

Neutron

OpenStack Networking (neutron) Initial Networks

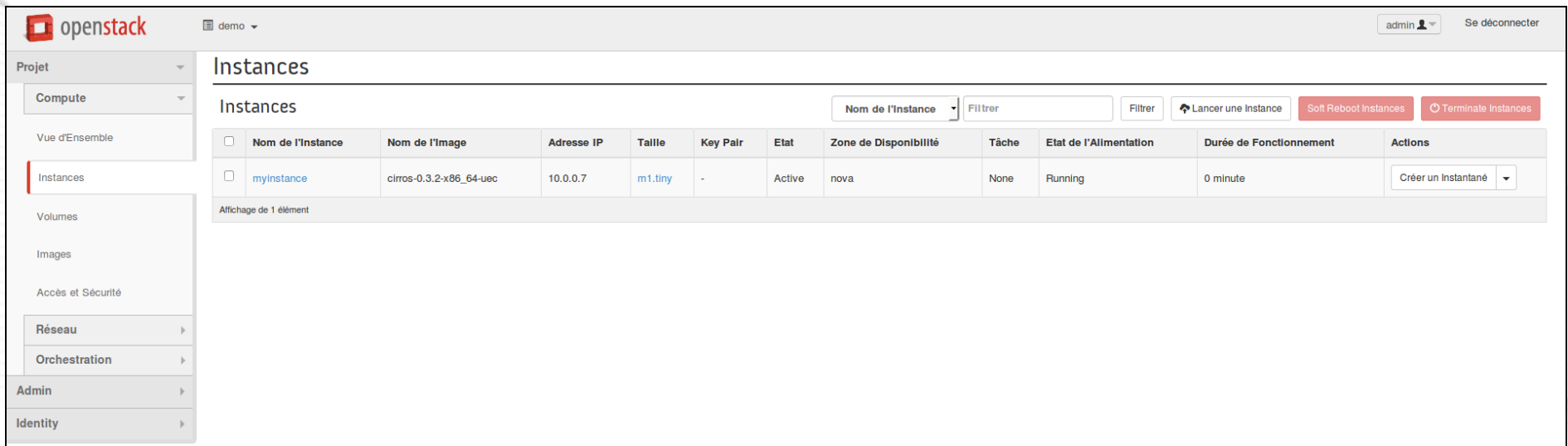


Cinder

- Volumes persistants
- Mode bloc (idem disques réels)
- Snapshots
- Backups
- Attachés par iSCSI aux instances
- Usage exclusif, pas partagé
- Bootable éventuellement
- Backends :
 - LVM (par défaut)
 - CEPH
 - GlusterFS
 - NetApp
 - Etc...

Horizon

- Interface utilisateur web
- Basée sur django et les APIs
- Dashboard est la version fournie
- Les services visibles sont ceux répertoriés dans keystone
- Zone spécifique pour « admin »
- Zone par « tenant » ou projet



The screenshot shows the OpenStack Horizon 'Instances' page. The table lists the following instance:

	Nom de l'Instance	Nom de l'Image	Adresse IP	Taille	Key Pair	Etat	Zone de Disponibilité	Tâche	Etat de l'Alimentation	Durée de Fonctionnement	Actions
☐	myinstance	cirros-0.3.2-x86_64-uec	10.0.0.7	m1.tiny	-	Active	nova	None	Running	0 minute	Créer un Instantané

Below the table, it indicates 'Affichage de 1 élément'.