Guillaume PHILIPPON

Mise en place d’un cloud privé et publique

Sommaire

- Genèse du projet
- Présentation de StratusLab
- Infrastructures hebergées au LAL
  - Expériences
- La sécurité dans un cloud publique
- Conclusions

La genèse du projet

Pour mieux répondre aux demandes des utilisateurs

- Les utilisateurs veulent plus de souplesse dans les services fournis en particulier dans les configurations des serveurs Web
- Les configurations requises par les expériences sont souvent incompatibles entres elles

Pour mieux gérer les ressources

- De nombreuses ressources sont sous utilisées

Le choix du Cloud

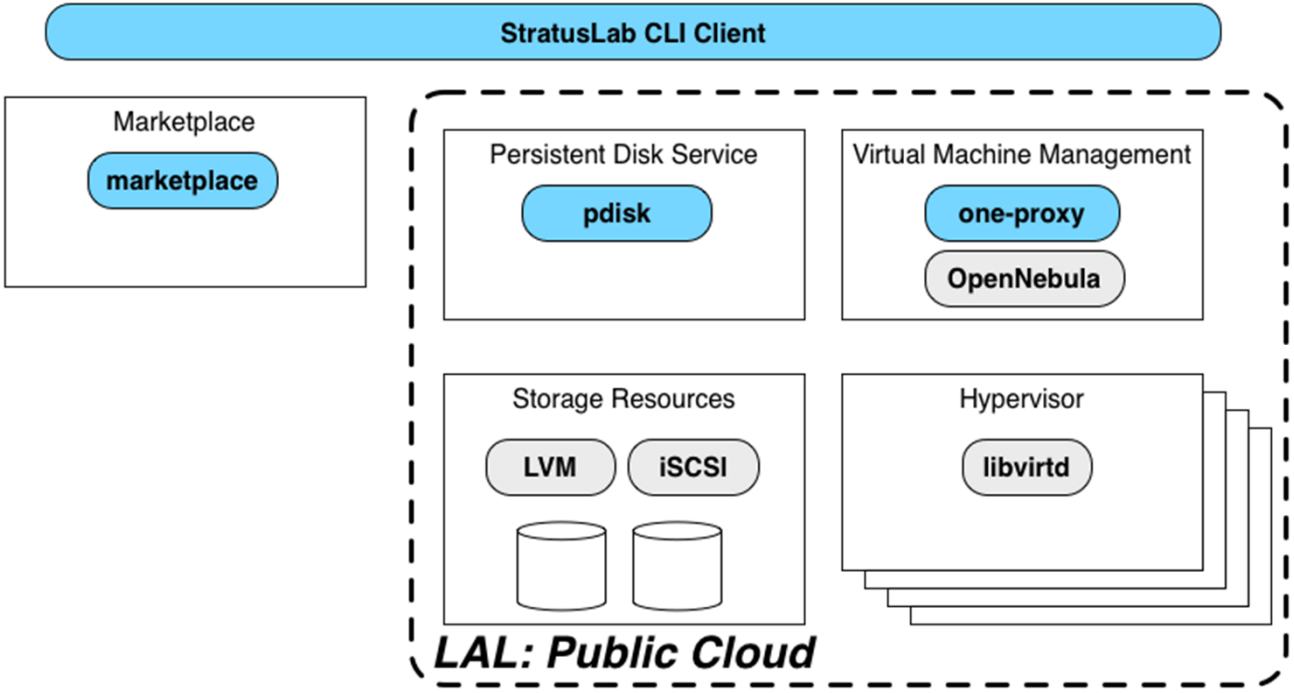
- L'allocation dynamique des ressources

StratusLab

- Logiciel « open source » de déployement de cloud IaaS créé dans le cadre d'un projet Européen
- Une collaboration durable du LAL, IBCP, SixSq et TCD
- Le maitre mot : simple à utiliser, installer et maintenir

Cloud publique du LAL

- En production depuis fin 2010
- Ouvert à toutes les communautés



Ressources	
machines	16
cœurs	440
mémoire (Go)	772
stockage (To)	15

Cloud publique du LAL

- Sert de démonstrateur du logiciel StratusLab
- Plus de 350 utilisateurs différents
  - D'une une 100n très régulier
- Cette infrastructure publique va continuer de croitre en lien avec l'université et le groupe « VirtualData » du LabEx P2IO
- Objectif de doubler la capacité en 2015

Expériences positives

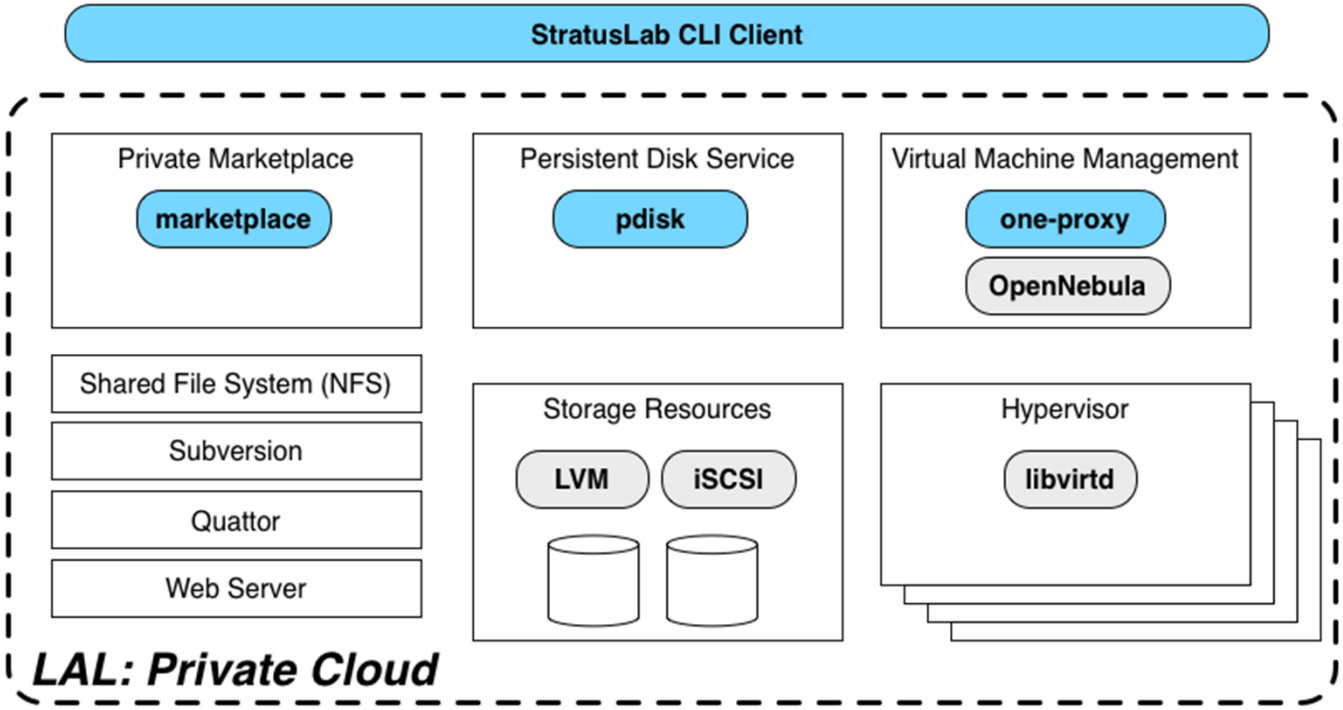
- Infrastructure très stable sauf pour les problèmes physique
- Ressources clouds fortement utilisées
- Peu de support nécessaire après la formation initiale
- Autopsie des machines simplifié
  - En cas d'alerte de sécurité

Les points faibles

- Administration du cloud nécessite une bonne connaissance des technologies sous-jacente
  - iSCSI
  - Virtualisation
  - Bridge réseau

Cloud privé

- En production depuis 3 ans
- Dédié aux besoins d'exploitations



Ressources	
machines	2
cœurs	96
mémoire (Go)	72
stockage (Go)	300

Expériences positives

- Infrastructure très stable
- Utilisation au mieux des capacités des machines (6 services différents sur 2 machines physiques)
- Possibilité de tester les nouveaux services avant mise en production
- Retour en arrière simplifié

Les points faibles

- La gestion des images est longue et difficile
  - On ne gère plus des machines mais des appliances
- L'utilisation du cloud nécessite toujours le savoir-faire de l'administrateur système
  - Limite la souplesse d'utilisation

Et ensuite…

- On va continuer d'étendre le cloud privée pour les services du laboratoire
- Ouvrir la possibilité de lancer des VMs qui peuvent accéder aux volumes NFS des expériences
- Heberger des nœuds grille dans l'infrastructure

La sécurité dans le Cloud

- On ne maitrise plus que l'environnement d'éxécution
  - Je ne sais pas qui utilise quoi
- Les utilisateurs administrateurs des machines
  - Pas d'authentification login / password
  - SSH forcement ouvert

Quelques principes

- Ne pas savoir qui fait quoi ce n'est pas laisser tout le monde faire n'importe quoi
  - Accès aux ressources contrôlé
  - On doit être en mesure quelle image fonctionne et qui a créer cette image
    - Signature des images, hashé et identifiable

Contrôler l'environnement

- Etre proactif dans la detection des attaques
  - Analyser le flux réseaux
  - Etre capable de blacklister une image
  - Etre capable d'autopsier les images
    - Ne pas détruire une image dès que son utilisateur arrête la machine
    - Travail largement facilité par la manipulation d'image et non plus de disque

Après 4 ans d'expériences

- 3 problèmes de sécurité sur l'infrastructure publique
  - Lié à des images incorrect
  - 1 alerte remonté par le site ciblé (avant la mise en place de la quarantaine et de l'analyseur de flux)
  - 1 alerte remonté par l'analyseur de flux. Après autopsie moins de 20 mins entre la prise de contrôle et la mise en quarantaine
  - 1 alerte de « bitcoin mining »

Conclusions

L'expérience StratusLab est positive

- IaaS solide
- Nécessite de gérer les problèmes éventuels de « poule et d'œuf »

Gestion et cycle de vie des images « virtuelles »

- Permet de gérer les images virtuelles comme des serveurs physiques
- Demande néanmoins plus de coordination afin de mettre en place un « cycle de mise à jour »

Nécessite encore beaucoup de connaissance dans l'infrastructure cloud pour gérer un service

- Difficile de déléguer la création des images