IMPLEMENTATION DE LA SOLUTION OPENSTACK ET GESTION DE LA SECURITE

CHAPITRE 4 : IMPLEMENTATION DE LA SOLUTION OPENSTACK ET GESTION DE LA SECURITE

Introduction

OpenStack est un logiciel libre qui permet la construction de Cloud privé et public. OpenStack est aussi une communauté et un projet en plus d'un logiciel qui a pour but d'aider les organisations à mettre en œuvre un système de serveur. Il s'installe sur un système d'exploitation libre comme Ubuntu ou Debian et se configure entièrement en ligne de commande. C'est un système robuste et qui a fait ses preuves auprès des professionnels du domaine. Son principal inconvénient est qu'il est assez difficile à installer.

IV.1 Installation de la solution OpenStack

IV.1.1 Prérequis

- Disposer des droits d'administration
- Disposer d'une connexion Internet configurée et activée
- Mise à jour des paquets et système
- Un processeur supportant la virtualisation matérielle
- Disposer d'un disque dur ou d'une partition non formatée pour LVM
- Avoir installé les dépendances
- Il est nécessaire de configurer le réseau en IP Fixe.
- Tous les services OpenStack seront installés sur la même machine.
- La configuration abordée suppose l'utilisation de 2 interfaces réseau.

IV.1.2 Architecture de notre système

CSI avez mis à notre disposition deux serveurs (Serveur de Test+Serveur Production) avec les caractéristiques suivantes :

- Modèle PC: HP ProLiant ML370.
- Type de système d'exploitation : Linux.
- Version : Ubuntu 12.04 LTS Server 64bits.
- Mémoire (RAM) : 24 GB.

- 6 Disques Dur: 300 GB pour chaque disque.
- Processeur (facultatif mais conseillé) : 1

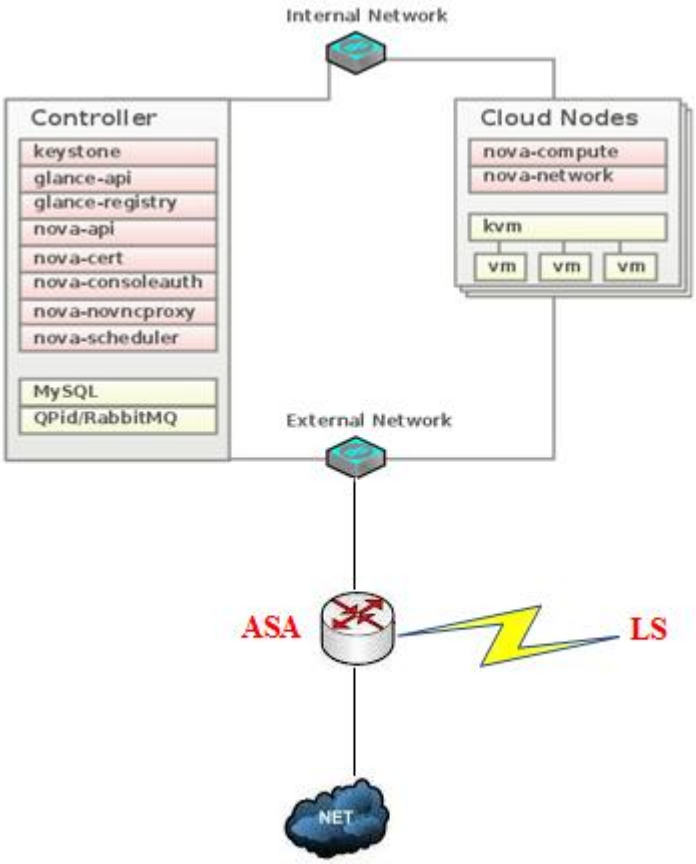


***Figure 13:** Architecture de notre maquette de Test*

IV.1.3 Configuration Réseaux

Modifiez avec les droits d'administration votre fichier */etc/network/interfaces* comme ci-dessous en adaptant à votre configuration.

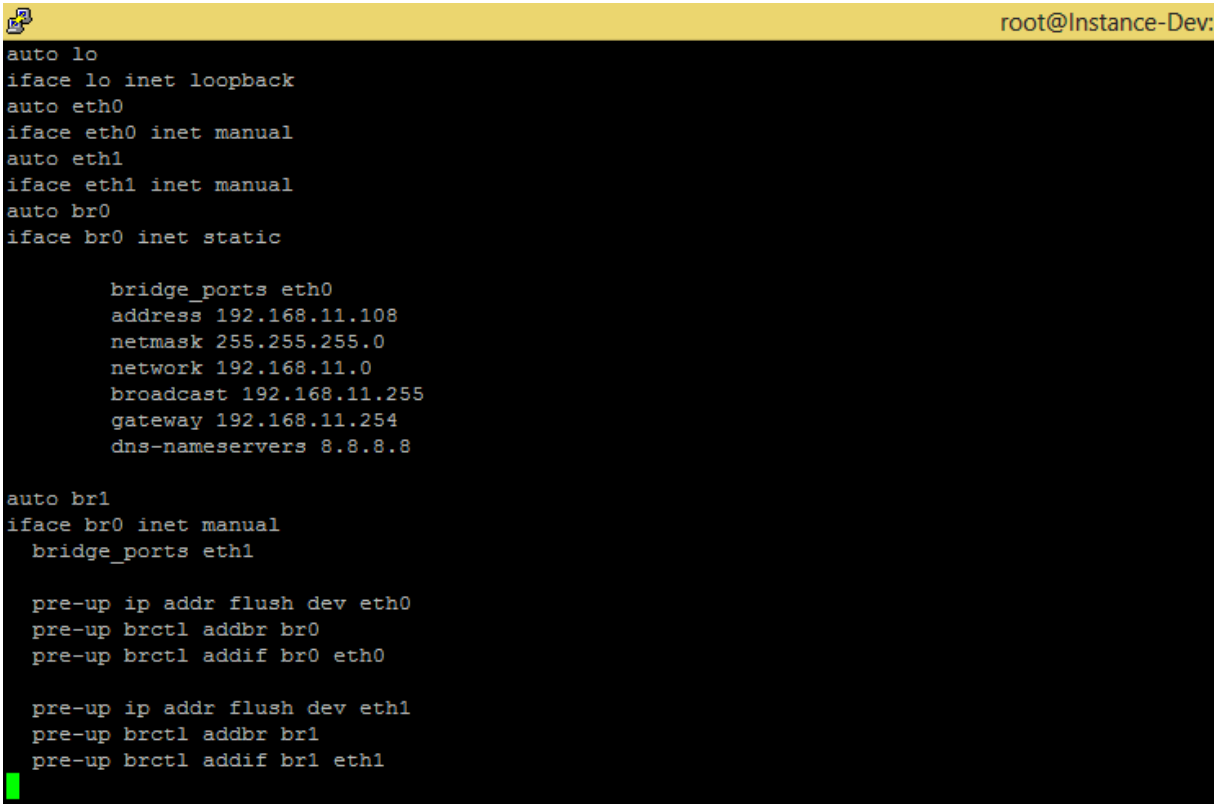


Figure 14: ***Configuration des interfaces réseaux***

IV.1.4 Installation des dépendances

Pour installer OpenStack on a besoin d'une machine qui a deux interfaces réseaux performante avec un processeur qui supporte la virtualisation matérielle, avoir un disque dur ou une partition non formate et installer les paquets suivantes.

kvm, libvirt-bin, virtinst mysql-server, python-mysqldb bridge-utils

Activer le routage : Editer le fichier ***/etc/sysctl.conf*** et décommenté la ligne net.ipv4.ip_forward=1

```
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4

net.ipv4.ip_forward=1
```

```
root@Instance-Dev: ~
root@Instance-Dev:~# apt-get install kvm libvirt-bin virtinst mysql-server python-mysqldb bridge-utils ntp
Lecture des listes de paquets... Fait
Construction de l'arbre des dÃ©pendances
Lecture des informations d'Ã©tat... Fait
Les paquets supplÃ©mentaires suivants seront installÃ©sÂ :
  acl cgroup-lite cpu-checker dnsmasq-base ebtables gawk kvm-ipxe libaio1 libapparmor1 libasound2 libasyncns0
  libcaca0 libcap2 libdbd-mysql-perl libdbi-perl libflac8 libhtml-template-perl libjson0 libmysqlclient18 libi
  libnuma1 libogg0 libopts25 libplrpc-perl libpulse0 librados2 librbd1 libsdl1.2debian libsigsegv2 libsndfile
  libxenstore3.0 libxml2-utils libyajl1 msr-tools mysql-client-5.5 mysql-client-core-5.5 mysql-common mysql-s
  python-libxml2 python-pycurl python-urlgrabber qemu-common qemu-kvm qemu-utils seabios vgabios
Paquets suggÃ©rÃ©sÂ :
  libasound2-plugins libasound2-python libipc-sharedcache-perl pulseaudio policykit-1 pm-utils radvd lvm2 tin
  python-mysqldb-dbg libcurl4-gnutls-dev python-pycurl-dbg mol-drivers-macosx openbios-sparc ubuntu-vm-builde
Les NOUVEAUX paquets suivants seront installÃ©sÂ :
  acl bridge-utils cgroup-lite cpu-checker dnsmasq-base ebtables gawk kvm kvm-ipxe libaio1 libapparmor1 libas
  libavahi-common3 libcaca0 libcap2 libdbd-mysql-perl libdbi-perl libflac8 libhtml-template-perl libjson0 libi
  libnspr4 libnss3 libnuma1 libogg0 libopts25 libplrpc-perl libpulse0 librados2 librbd1 libsdl1.2debian libsi
  libvirt0 libvorbis0a libvorbisenc2 libxenstore3.0 libxml2-utils libyajl1 msr-tools mysql-client-5.5 mysql-c
  mysql-server-core-5.5 ntp python-libvirt python-libxml2 python-mysqldb python-pycurl python-urlgrabber qemu
0 mis Ã  jour, 65 nouvellement installÃ©s, 0 Ã  enlever et 121 non mis Ã  jour.
Il est nÃ©cessaire de prendre 40,2 Mo dans les archives.
AprÃ¨s cette opÃ©ration, 144 Mo d'espace disque supplÃ©mentaires seront utilisÃ©s.
Souhaitez-vous continuer [O/n]Â ?
```

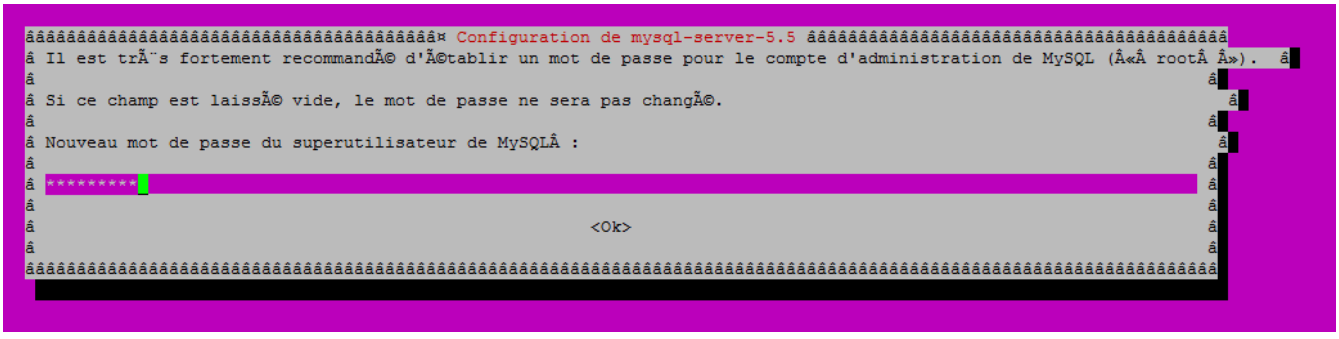
IV.1.5 Installation du serveur de temps NTP

Le serveur de temps **NTP** va nous permettre une bonne synchronisation du Cloud.

Pour cela éditer le fichier ***etc/ntp.conf*** en ajoutant les lignes suivantes

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server ntp.ubuntu.com iburst
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

Entrez le mot de passe pour la base de données MYSQL



IV.1.6 Préparation de la base de données MYSQL

Commencez d'abord par créer la base de données **MySQL**

La configuration de MySQL est un peu simple, il suffit d'indiquer à MySQL qu'il doit écouter sur toutes les adresses et pas seulement l'adresse de la boucle locale. Pour faire éditer le fichier ***/etc/mysql/my.conf*** comme suit.

```
[mysqld]
#
# * Basic Settings
#
user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
```

IV.1.7 Installation et configuration du composant Keystone

➢ Installation

D'abord on installe les paquets qui permettent le bon fonctionnement du composant Keystone.

```
root@Instance-Dev: ~
root@Instance-Dev:~# apt-get install  keystone python-keystone python-keystoneclient python-mysqldb
Lecture des listes de paquets... Fait
Construction de l'arbre des dÃ©pendances
Lecture des informations d'Ã©tat... Fait
python-mysqldb est dÃ©jÃ  la plus rÃ©cente version disponible.
Les paquets supplÃ©mentaires suivants seront installÃ©sÂ :
  dbconfig-common libjs-sphinxdoc libjs-underscore libxslt1.1 python-decorator python-eventlet python-formencode
  python-migrate python-openid python-passlib python-paste python-pastedeploy python-pastescript python-prettytabl
  python-sqlalchemy python-sqlalchemy-ext python-tempita python-webob ssl-cert
Paquets suggÃ©rÃ©sÂ :
  javascript-common python-egenix-mxdatetime python-dns python-greenlet-doc python-greenlet-dev python-greenlet-dl
  python-pastewebkit libapache2-mod-wsgi libapache2-mod-python libapache2-mod-scgi python-pgsql libjs-mochikit pyt
  python-sqlalchemy-doc python-psycopg2 python-kinterbasdb python-pymssql openssl-blacklist
Les NOUVEAUX paquets suivants seront installÃ©sÂ :
  dbconfig-common keystone libjs-sphinxdoc libjs-underscore libxslt1.1 python-decorator python-eventlet python-fo
  python-keystone python-keystoneclient python-lxml python-migrate python-openid python-passlib python-paste pytho
  python-routes python-scgi python-setuptools python-sqlalchemy python-sqlalchemy-ext python-tempita python-webob
0 mis Ã  jour, 28 nouvellement installÃ©s, 0 Ã  enlever et 121 non mis Ã  jour.
Il est nÃ©cessaire de prendre 4 140 ko dans les archives.
AprÃ¨s cette opÃ©ration, 19,6 Mo d'espace disque supplÃ©mentaires seront utilisÃ©s.
Souhaitez-vous continuer [O/n]Â ?
```

➢ Configuration

Création d'un utilisateur Keystone avec un mot de passe de votre choix dans la base de données Mysql.

```
root@Instance-Dev:
root@Instance-Dev:~# service mysql restart
mysql stop/waiting
mysql start/running, process 5134
root@Instance-Dev:~# mysql -u root -p <<EOF
> CREATE DATABASE keystone;
> GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' IDENTIFIED BY 'ousseynou';
> FLUSH PRIVILEGES;
> EOF
Enter password:
root@Instance-Dev:~#
```

Pour la configuration de keystone on doit éditer le fichier ***/etc/keystone/keystone.conf***

```
root@Instance-Dev:
[DEFAULT]
#bind_host = 0.0.0.0
public_port = 5000
admin_port = 35357
admin_token = ousseynou
compute_port = 8774
verbose = True
debug = True
log_config = /etc/keystone/logging.conf

# ================= Syslog Options ============================
# Send logs to syslog (/dev/log) instead of to file specified
# by `log-file`
use_syslog = False

# Facility to use. If unset defaults to LOG_USER.
# syslog_log_facility = LOG_LOCAL0
[sql]
connection = mysql://keystone:ousseynou@192.168.11.108:3306/keystone
idle_timeout = 200
```

redémarrer le service keystone et faire la synchronisation avec la base de données pour prendre en compte les données récemment modifié.

```
root@Instance-Dev:~# service keystone restart
keystone stop/waiting
keystone start/running, process 6618
root@Instance-Dev:~# keystone-manage db_sync
root@Instance-Dev:~#
```

➢ Connexion à la plateforme d'OpenStack

Pour se connecter à la plateforme d'OpenStack il suffit de tapez l'adresse IP du serveur su un navigateur web.

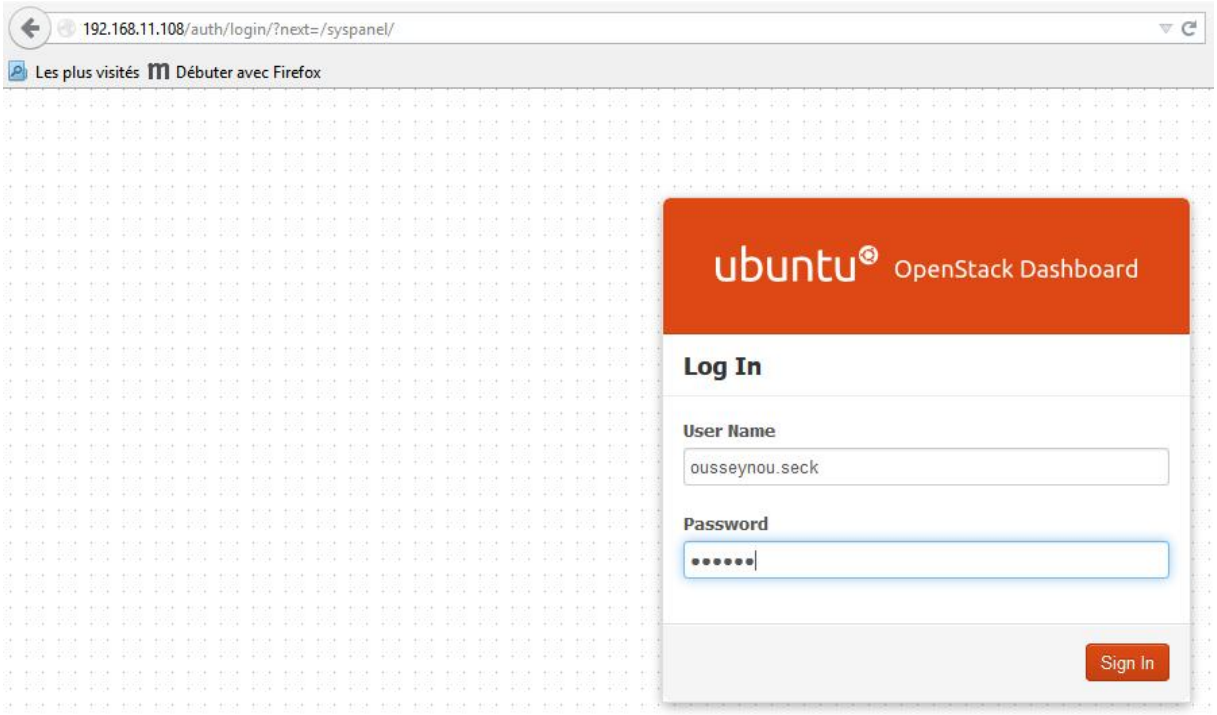


***Figure 15:** Page de connexion à la plateforme OpenStack*

La gestion des services du Cloud est aussi gérer par cette interface web

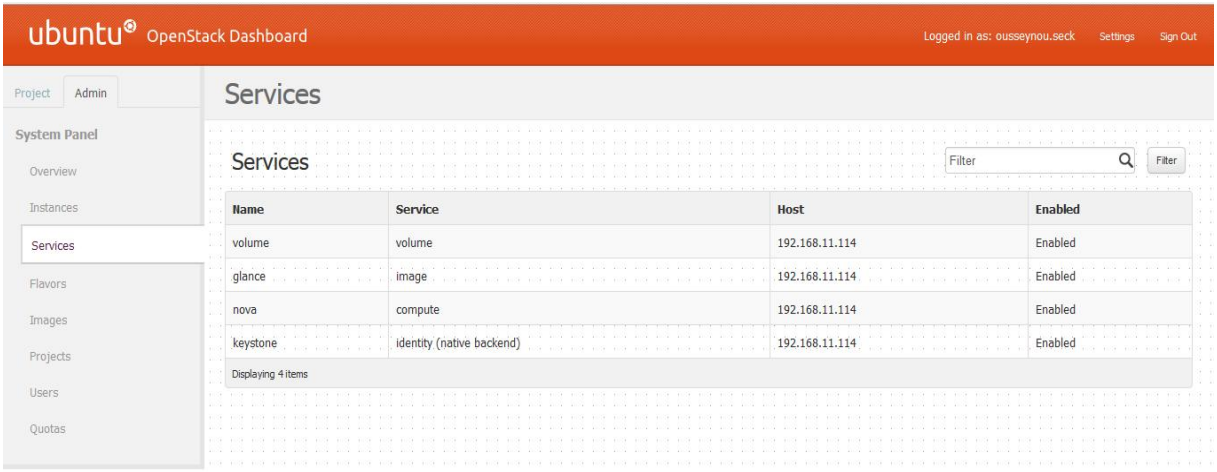
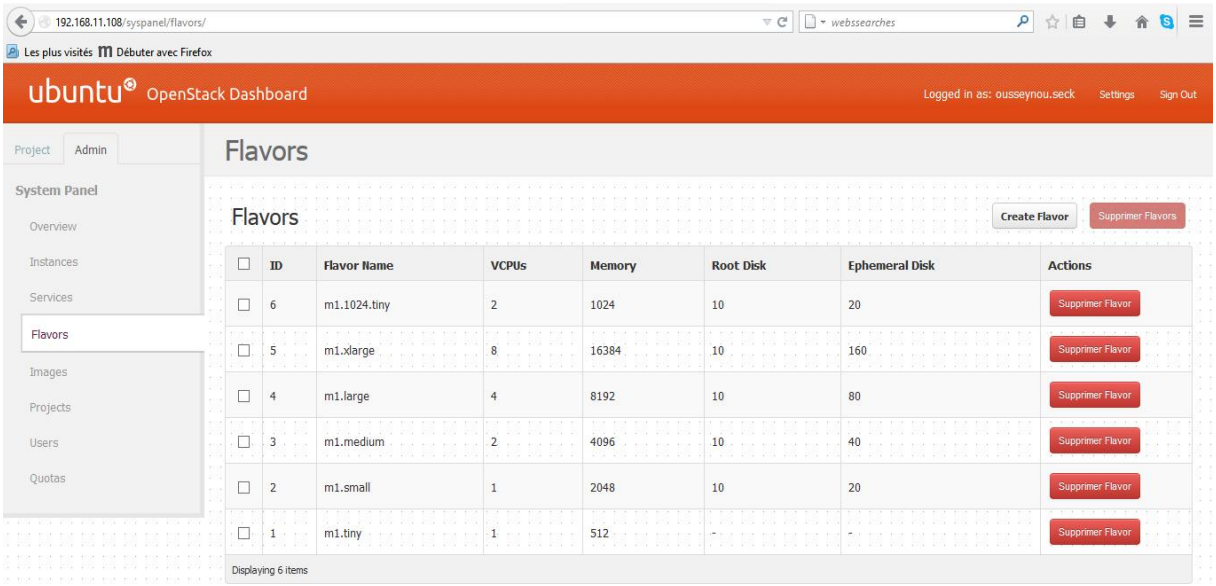


***Figure 16:** Les services du cloud OpenStack*

Cette interface nous permet la définition des flavors qui vont être utilisé par le service Nova d'OpenStack pour la création des machines virtuelles.



Cette interface nous permet la gestion des instances et volumes

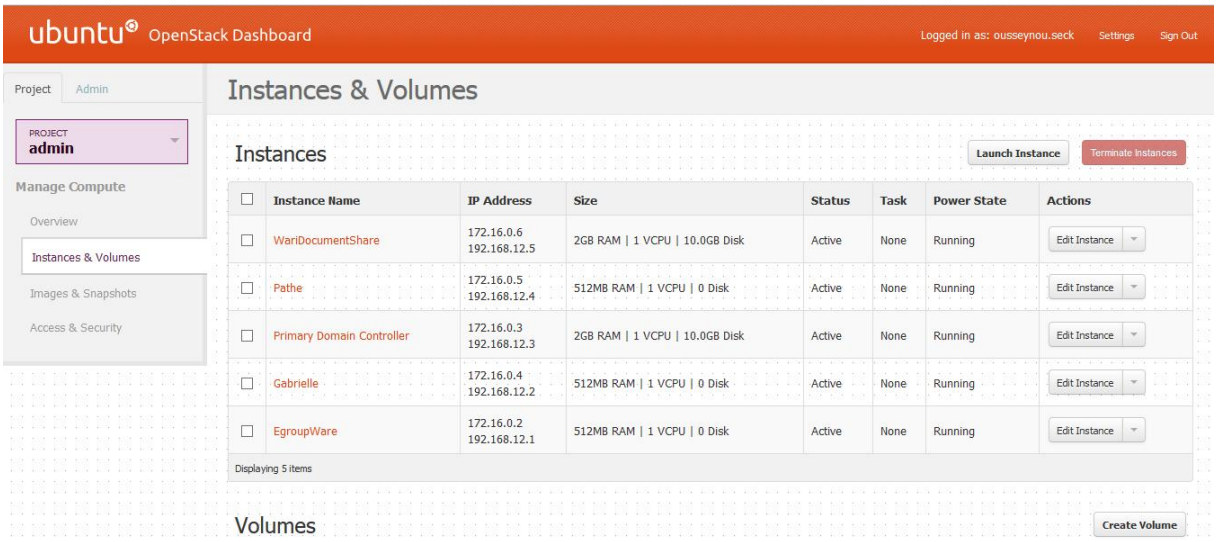


***Figure 17:* Interface de gestion des Instances et Volumes**

.

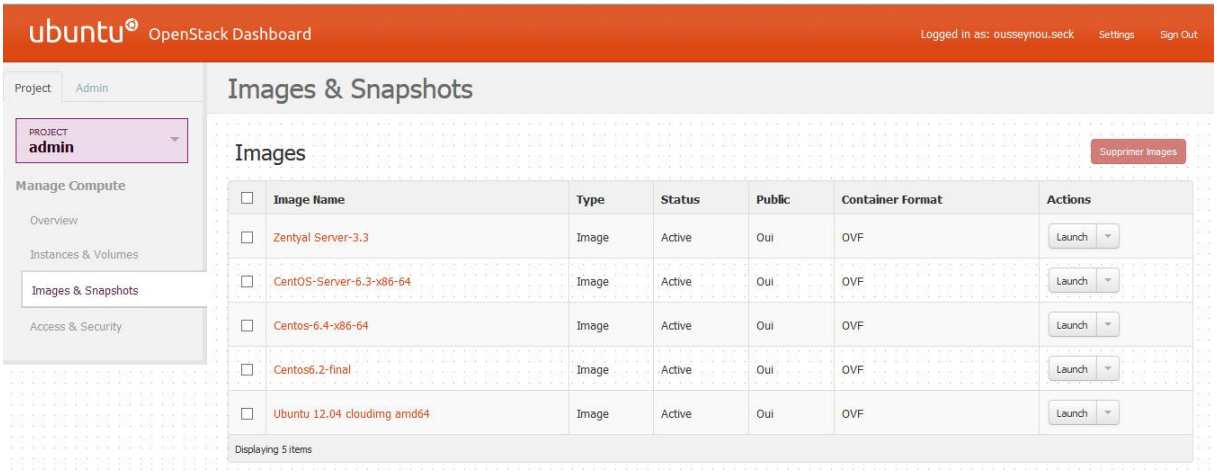


Figure 18: ***Gestion des images du service glance d'OpenStack***

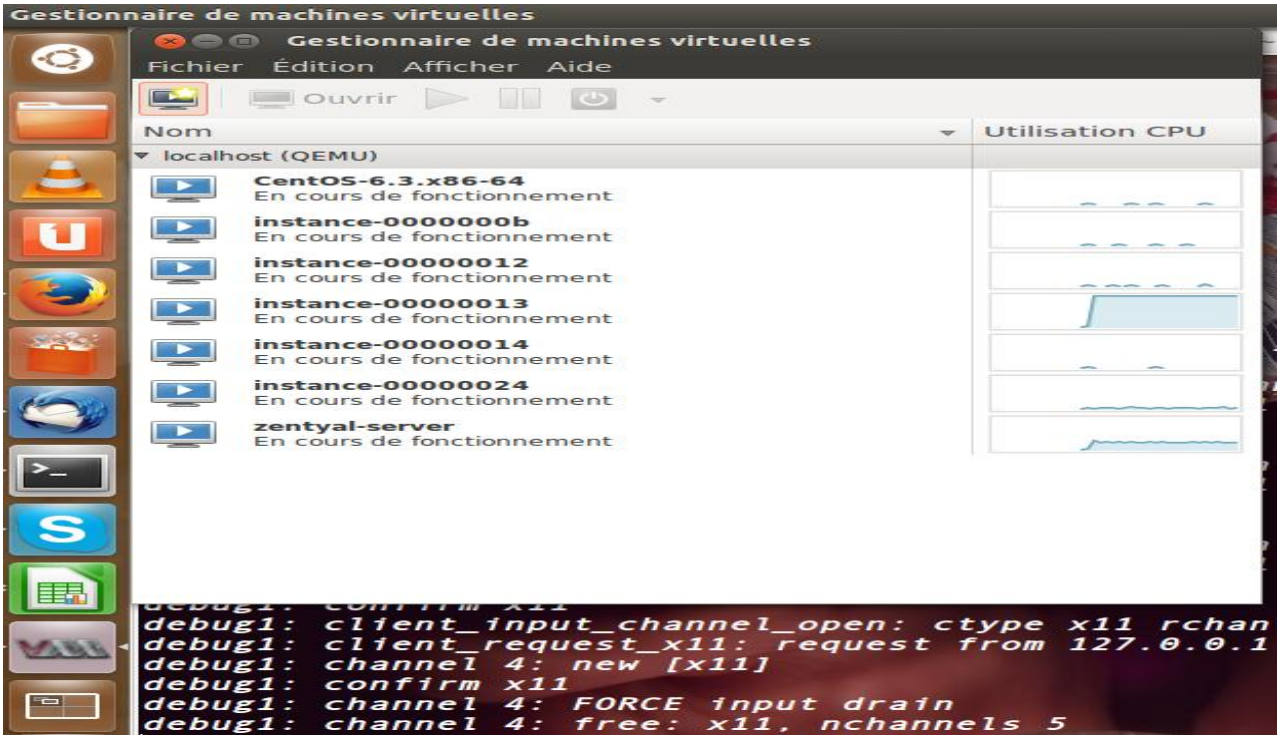
IV.1.8 Dashboard Horizon

L'interface graphique, le Dashboard Horizon, a été développée pour simplifier l'administration du serveur et des projets. L'accès se fait à partir d'un navigateur web pointant à l'adresse du serveur.

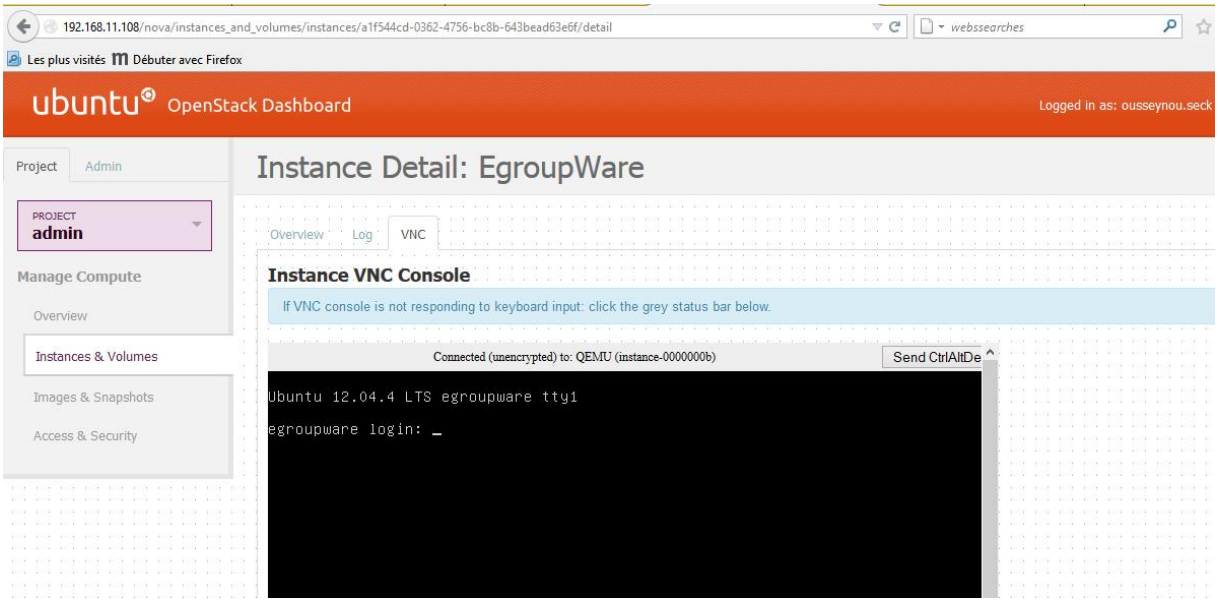
Les différents services doivent être installés et configurés avant de pouvoir l'utiliser. Une grande partie des commandes est alors à portée d'un clic de souris.

```
root@Instance-Dev:
root@Instance-Dev:~# apt-get install apache2 libapache2-mod-wsgi openstack-dashboard
Lecture des listes de paquets... Fait
Construction de l'arbre des dÃ©pendances
Lecture des informations d'Ã©tat... Fait
apache2 est dÃ©jÃ  la plus rÃ©cente version disponible.
Les paquets supplÃ©mentaires suivants seront installÃ©sÂ :
  memcached openstack-dashboard-ubuntu-theme python-cloudfiles python-django python-django-ho
Paquets suggÃ©rÃ©sÂ :
  libcache-memcached-perl libmemcached python-psycopg2 python-psycopg python-flup python-sqli
Les NOUVEAUX paquets suivants seront installÃ©sÂ :
  libapache2-mod-wsgi memcached openstack-dashboard openstack-dashboard-ubuntu-theme python-c
  python-memcache
0 mis Ã  jour, 9 nouvellement installÃ©s, 0 Ã  enlever et 119 non mis Ã  jour.
Il est nÃ©cessaire de prendre 5 152 ko dans les archives.
AprÃ¨s cette opÃ©ration, 41,0 Mo d'espace disque supplÃ©mentaires seront utilisÃ©s.
Souhaitez-vous continuer [O/n]Â ?
```

Redemarez le service apache et verifiez



<u>Figure 19:</u> Les différentes Instances de notre plateforme OpenStack



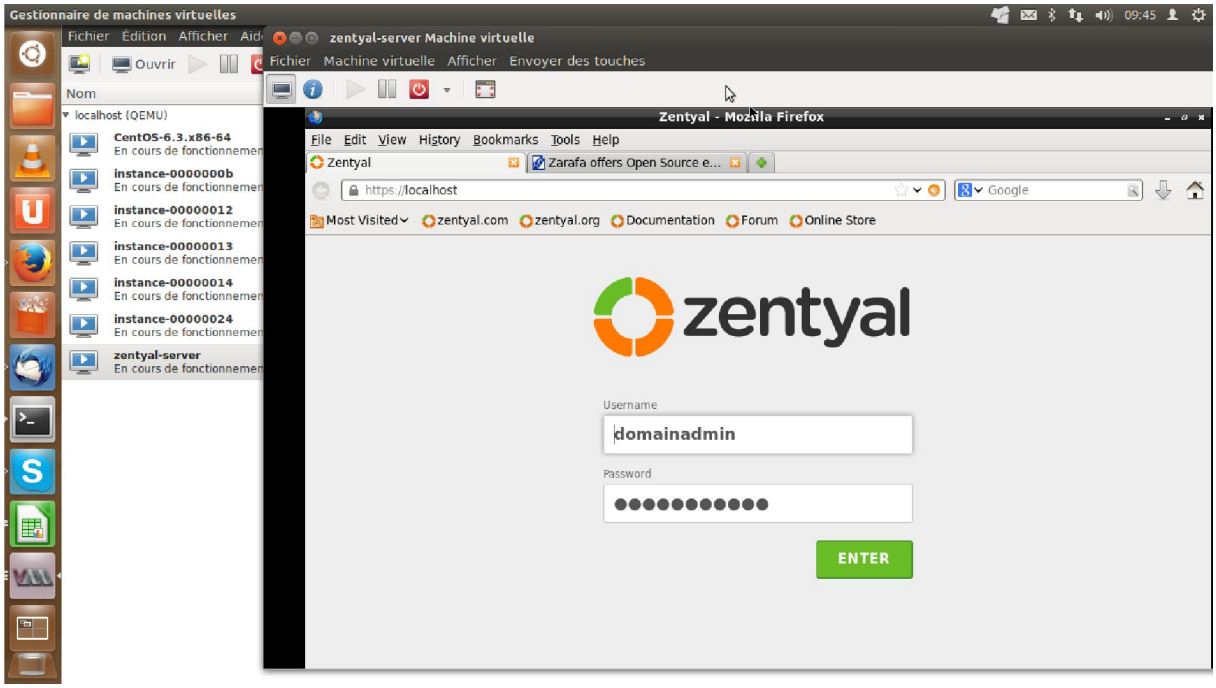


Figure 20: ***Connexion des Instances par la console VNC***

IV.2 Sécurité du Cloud Computing

La sécurité et la conformité émergent systématiquement comme les principales préoccupations des responsables informatiques lorsqu'il est question de Cloud Computing, des préoccupations encore plus accentuées lorsqu'il s'agit de Cloud public. La sécurité permet de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations.

IV.2.1 Menaces

Une menace est par définition toute action ou évènement susceptible de compromettre la sécurité d'un système informatique. C'est une violation potentielle de sécurité.

✓ Abus et utilisation malveillante

Les grands avantages du cloud se retournent contre lui sur ce point. En effet, cette technologie puissante et ouverte permet à de nombreux utilisateurs d'utiliser ses services gratuitement pendant une durée déterminée. C'est assez pour permettre aux hackers d'utiliser la bande passante pour commettre des actes malveillants. Spams, codes malicieux, chevaux de Troie cachés dans les applications cloud. Ce sont là quelques exemples d'abus et de malveillance inhérents au cloud. De plus, le cloud n'est pas doté de systèmes antifraudes performants et le

contrôle d'enregistrement de clients est assez laxiste. Ce qui laisse le champ libre aux cybers criminels pour décortiquer les programmes et craquer des mots de passe impunément.

- ✓ **Interfaces et API non sécurisés**

Pour accéder au cloud, les clients passent généralement par des API et des Interfaces graphiques. De ce fait, la sécurité de ces éléments est cruciale. Ils sont censés proposer un certain contrôle pour l'authentification, du chiffrement et de l'intégrité. Si elles sont mal protégées (et c'est le cas pour beaucoup d'API), c'est la porte ouverte à toute sorte d'attaques malveillantes qui mettrons en péril la confidentialité.

- ✓ **Malveillances internes**

A cause du caractère insidieux mais aussi de la difficulté à les détecter à temps, ce type d'attaque est très dangereux. Il s'agit d'attaques menées de l'intérieur par des employées ou des personnes familières avec le service. Ces malveillances consistent à obtenir des mots des passes et des informations confidentielles qui filtrent à travers le cloud. Ces malveillances peuvent briser les relations fournisseur/client car elles brisent la confiance établie. Les attaquants peuvent aussi prendre le contrôle des ressources des deux côtés et causer des dégâts financiers et matériaux graves.

- ✓ **Perte ou fuite de données**

Ce type de menace résulte de beaucoup de causes : failles opérationnels, stockage non fiable ou utilisation inadéquate (insuffisante) de clés de chiffrement. Pour le premier cas, il s'agit d'une mauvaise manipulation qui modifie les enregistrements alors qu'ils n'ont pas été sauvegardés. La seconde cause est liée à l'utilisation de media non fiables pour le stocker, ce qui peut s'avérer si on arrive plus à restaurer les données. En ce qui concerne l'utilisation des clés, une mauvaise manipulation ou une sécurité insuffisante ouvrent la voie à des accès non autorisés et de violations diverses. Une perte de donnée peut affecter non seulement les secrets de l'entreprise cliente, mais aussi le fournisseur de cloud dont la réputation de sécurité peut être détruit. Une mauvaise publicité qui peut générer des pertes considérables.

- ✓ **Détournement de compte ou de service**

Accès non autorisé, contrôle des comptes utilisateurs (phishing, fraude, falsification). Les credentials volés ouvrent tout un pan de vulnérabilités et peuvent devenir une base d'attaque. Cela fragilise la confidentialité, l'intégrité et la disponibilité. Solution : rôle et mots de passe (insuffisant).

✓ **Profil de risque inconnu**

Les utilisateurs doivent connaitre les technologies cloud auxquels ils font face. Le manque d'information représente un danger sinon ils ne peuvent se préparer en connaissance, ne sachant pas comment sont traitées leurs données et où elles sont stockées.

✓ **Virtualisation**

Une des technologies Cloud consiste à placer les applications des utilisateurs dans des machines virtualisées à partir des machines physiques du fournisseur. Ces MV sont isolées les unes des autres et gérées par un hyperviseur. Il est une cible de choix pour les pirates. Une attaque sur l'hyperviseur peut sérieusement endommager les machines virtuelles et réelles. La sécurité de cette entité doit être renforcée.

IV.2.2 Vulnérabilités

✓ **Détournement de session**

Il s'agit du fait d'utiliser une clé de session pour avoir un accès non autorisé sur les informations et les services. Cela permet d'envoyer des commandes illégales, manipuler et supprimer des données.

✓ **Virtual Machine escape**

Les attaques sur machines virtuelles ne sont pas encore pleinement étudiées et des protections sur mesure n'existent pas encore. Les IDS et IPS devront être configurés afin de prendre en charge ce type d'attaque.VM escape est la vulnérabilité permettant à une MV d'attaquer son hôte. Des codes malicieux peuvent être lancés de sortent que la ligne entre virtuel et réel soit mince et perméable.

✓ **Disponibilité et sureté du service**

Une coupure dans la disponibilité du Cloud entraine des pertes considérables. Plus il y a d'applications basées sur Cloud plus la disponibilité deviens essentielle.

✓ **Cryptographie non sure**

Une cryptographie non sure est toute cryptographie considérée comme sure alors que ses faiblesses ne sont pas encore découvertes. La cryptographie moderne se base sur la génération de nombre aléatoires, issues de sources nombreuses comme le mouvement de la

souris, le clavier etc… Chez le Cloud (MV sous linux), il n'y a qu'une seule source : le temps de traitement des horloges interne. Ce qui n'est pas suffisant pour faire du chiffrement à haute efficacité.

- ✓ **Protection de données et portabilité**

Il s'agit ici des données utilisateur laissés à l'abandon suite à une rupture de contrat ou cessation de service. Le fournisseur supprime-t-il ces données ? Les passe-t-il à un autre fournisseur ? Si oui, le client peut-il faire confiance à ce dernier ? Protection et portabilité des données font partie des plus grandes faiblesses du Cloud.

- ✓ **Vendor lock in**

Cette vulnérabilité réside de la politique et du business model d'un fournisseur qui empêche le client d'aller voir ailleurs. Et s'il accepte, cela engendre un cout considérable au client. Ces fournisseurs risquent de faire faillite et d'échec, d'où une prise d'otage des données.

- ✓ **Internet dependency**

Le Cloud est fortement dépendant d'internet, le client accède au service du fournisseur via un navigateur web. Que se passe-t-il lorsqu'internet est indisponible ? Pour certains services critiques (banque, hôpital), une indisponibilité d'internet peut jouer sur des opérations importantes et engendrés des pertes non négligeables.

IV.2.3 Risques

RISQUE = MENACE * IMPACT * VULNERABILITE

Il y'en a 35 identifiés par l'ENISA en tout. On peut citer **:**

- **Risques politiques et organisationnels :** pertes de données conduisant à effondrement de l'organisation
- **Risques techniques :** indisponibilité de services
- **Risques juridiques :** violation de la loi sur la vie privée et la confidentialité

Les risques les plus élevés :

- **Perte de gouvernance :** le client cède le contrôle au fournisseur sur plusieurs domaines qui ne sont pas encore maitrisés, ce qui laisse une brèche de sécurité.

- **Enfermement dans une solution** : lorsqu'on dépend entièrement d'un fournisseur Cloud, il n'y a plus de portabilité de données.
- **Echec isolation** : pour la plupart des fournisseurs, le partage de ressources et services est très courant. Ceci peut jouer sur l'isolation, qui est un aspect primordial de la sécurité. Les risques ici concernent les mécanismes de séparation entre stockage, mémoire vive et routage.

Défis conformité

- **Juridiques :** ordonnance de tribunal, citation, mandat de perquisition, saisie par le gouvernement local, changement de juridictions (manque de transparence) Malveillance interne : bien que ce soit un risque moindre, son impact est le plus grand pour le Cloud Computing.
- **Protection de données :** lorsqu'il s'agit d'une grande structure Cloud, qui communique avec d'autres Cloud, il est impossible de faire un suivi exact des données échangées (quantité, chemins). Le fait que le client ne puisse contrôler les flux est un gros risque pour la sécurité.
- **Réseau** (congestion, mauvaise utilisation)
  Les attentes : si la sécurité offerte est moins importante que celle attendue par le client, ce non synchronisation peut entrainer de grosses failles de sécurité.

IV.2.4 Mesures de contrôle

✓ **Contrôle et preuve :** le déploiement d'un dispositif de contrôle interne adapté est rendu complexe par les difficultés à mettre en place une relation contractuelle équilibrée, à auditer le prestataire (multiplicité des intervenants, localisation géographique potentiellement mondiale, …) et à identifier la réglementation applicable aux données.

✓ **Urbanisme et organisation :** le recours à une prestation informatique de type Cloud est susceptible de provoquer des problèmes d'intégration dans le système d'information et d'en diminuer à moyen terme sa flexibilité et sa capacité d'évolution. Les difficultés induites sont à la fois techniques (intégration potentiellement inadéquate d'un composant très standardisé dans un système d'information) et parfois

organisationnelles (capacité de l'organisation informatique à s'adapter à des évolutions du service *Cloud* parfois très fréquentes). Avant de s'engager envers une solution particulière de Cloud Computing, il est important de bien connaitre les risques associés et de maitriser ces technologies. Plusieurs règlements existent en la matière : Codes des Assurances (R.336-1f), code de la Mutualité (R. 211-28f) et code de la sécurité sociale (CRBF n°97-02).

- ✓ **Juridique** : l'encadrement contractuel de la prestation est impératif. Les mesures de protection des données mises en œuvre par le prestataire doivent être évaluées avant souscription du service. Concernant la protection des données personnelles, la prestation doit se conformer à la Directive européenne 95/46/CE et plus largement aux règles de protection de la propriété intellectuelle. Certains éléments transférés dans le *Cloud* sont susceptibles d'entrer dans le capital de la propriété intellectuelle de l'entreprise et doivent faire l'objet d'une clause contractuelle. Par ailleurs, tout changement dans la nature de la prestation doit être maîtrisé, y compris dans les versions logicielles. Le client se doit procéder à un pilotage contractuel en continu, en se basant sur les clauses qui régissent les pénalités et qu'il peut utiliser en cas de manquement par rapport au service rendu. Une certaine visibilité est requise de la part du prestataire, surtout s'il y a de la sous-traitante.

- ✓ **Contrôle du prestataire** : Il s'agit ici de la capacité et du droit à l'audit. Le prestataire doit s'attendre un audit régulier et à ce que son système subisse des tests d'intrusion et de vulnérabilité. Une documentation de l'ancien audit est aussi nécessaire et doit être mise à jour. La seule parole du prestataire ne peut pas être considérée comme une garantie suffisante.

IV.2.5 Impacts

Par définition, l'impact équivaut à l'évaluation des dommages causés par un évènement. Une fuite de données peut par exemple amener à des divulgations d'informations confidentielles de clients. Ce qui peut conduire à des pertes financières mais aussi à faire à l'entreprise victime sa crédibilité aux yeux des clients.

✓ **Confidentialité des données :**

La protection des données sensibles et personnelles, de même que le respect du secret bancaire, sont particulièrement difficiles au sein d'infrastructures mutualisées et potentiellement accessibles aux régulateurs locaux. Le manque de visibilité sur la localisation des données et donc sur la réglementation applicable ainsi que le nombre de parties prenantes dans une solution de *Cloud Computing* accentuent ce risque. La question de la confidentialité des données se pose également en termes d'assurance de leur destruction effective en cas d'arrêt de la prestation, y compris sur les sauvegardes dans des sites qui peuvent être dispersés.

✓ **Intégrité des données** :

A la longue, une sorte de dépendance s'installe pour le client envers le fournisseur. Celui-ci, consciemment ou non peut ainsi modifier le fonctionnement des services, les traitements de données sans que le client ne s'en aperçoive.

IV.3 Gestion de la sécurité du Cloud

Un processus d'identification continu est une alternative efficace contre les risques, évitent ainsi de mauvaises surprises (nouveaux risques). La transparence et la communication libre entre prestataire et client permettent de mieux évaluer les risques.

La sécurité des données est un enjeu primordial pour les entreprises. Avec le « cloud Computing », la gestion de la sécurité se trouve fortement déléguée au prestataire pour couvrir les risques portant sur :

- la confidentialité et l'intégrité des données (y compris lors de l'arrêt de la prestation),
- la perte de données,
- la continuité de service,
- la qualité de service.

IV.3.1 Techniques de sécurisations

Techniques :

Parmi les mesures techniques de sécurité, le **chiffrement systématique des données** est la mesure qui revient le plus souvent, notamment pour protéger les données dont la localisation n'est pas connue. Un grand groupe bancaire précise toutefois que si le chiffrement des données

lors du transport est obligatoire, il est plus complexe à mettre en œuvre pour le stockage. De grands groupes internationaux souhaitent que le chiffrement soit mis en œuvre par le déploiement d'une infrastructure à clés publiques qui ne serait pas gérée dans le *cloud*. Un groupe international (secteur assurance et banque) considère que le chiffrement n'est utile que pour les données sensibles (sans toutefois en donner de définition) et que l'anonymisation peut être utilisée dans les environnements hors production. Des assureurs souhaitent que les habilitations soient gérées par le donneur d'ordre et exigent le cloisonnement des données entre les différents clients du fournisseur.

Les entreprises doivent prendre des mesures de maîtrise des risques concernant les points suivant :

- Juridique : il faut un encadrement contractuel des prestations Cloud
- Technique : Chiffrement de données pendant le transport et le stockage
- Contrôle : grâce à l'audit du prestataire ;
- Continuité de la prestation : les attentes du client doivent être formalisées dans les contrats ;
- Réversibilité de la prestation : les conditions de réversibilité doivent être disponibles ;

1. Contrôle des risques

Pour contrôler les risques, il faut avant tout comprendre les données, leur nature et leur organisation. La faillite d'un prestataire peut tout à fait engendrer une privation critique des données pour une entreprise.

La perte de contrôle est un problème récurrent dans le débat sur le Cloud. L'abonné se retrouve « à la merci » du prestataire car elle dépend presque entièrement du prestataire.

Vol, destruction de matériel, incendie, problème technique, perte de contrôle sont autant de risques possibles.

Une mise à jour de la politique sur les achats permet de s'assure qu'une équipe compétente est présente et capable d'effectuer des analyses des risques. Cela permettra d'évaluer la sécurité et la confidentialité de la solution offerte. L'étape suivante est la définition d'objectifs de sécurité que le prestataire sera amené à atteindre.

La surveillance de ses objectifs ainsi que de leurs indicateurs permettra à l'entreprise abonnée de veiller à la sécurité durant l'utilisation du service.

Avec le Cloud, la sécurité est déléguée au fournisseur, il doit donc garantir :

- la confidentialité et l'intégrité des données (Y compris lors de l'arrêt de la prestation),

- la perte de données,
- la continuité de service,
- la qualité de service

La sauvegarde entière et externalisée est recommandée contre ces risques. Une entreprise qui héberge ses données elle-même a plus de contrôle dessus que celle qui bascule en Cloud.

2. Aspects juridiques

Les risques juridiques liés au Cloud découlent principalement de l'abstraction de la localisation des données: sur quel serveur, dans quel centre et, surtout, depuis quel pays ? Les données placées dans le Cloud sont forcément hébergées sur un serveur physique. Ce serveur peut être localisé dans n'importe quel pays du monde sans que le client en soit averti. Il faut être conscient que c'est la juridiction du pays ou sont hébergées les données qui s'appliquent.

Les juridictions de chaque pays sont différentes et il peut parfois être interdit, voire dangereux, d'héberger des données personnelles à l'étranger. Il convient donc d'être particulièrement vigilant car les fournisseurs sont très vagues sur leurs obligations légales et règlementaires et sur leurs engagements

Il y a évidemment aussi les aspects juridiques, liés notamment à la protection des renseignements personnels qui représente un des plus gros défis légaux du Cloud Computing à cause de l'indépendance de la localisation et de son caractère multi-tenant.

Comme les données peuvent être localisées, partagées et emmagasinées dans plusieurs pays, il peut devenir difficile d'assurer adéquatement la protection des renseignements personnels en raison des différentes lois ou de l'absence de loi qui régissent ces différents pays.

La rédaction d'un contrat de Cloud Computing s'appuie sur les aspects légaux et juridiques du contrat de services, c'est-à-dire que les contractualisant sont tenus par le respect de certaines obligations du droit ainsi que par une obligation de résultats.

Dans la plupart des cas, la législation appliquée en matière de contrat de services est celle du pays qui héberge les données. Il faut donc connaitre ces législations non seulement pour le stockage courant, mais au cas où il y aura une externalisation vers un autre pays.

Donc il faut assurer:

- Le SLA (Service Level Agreement) ou convention de niveau de services
- La Protection des données
- La Récupération de données
- La Réversibilité

IV.4 Quelques outils de supervision pour améliorer la sécurité

IV.4.1 EtherApe

EtherApe est un logiciel libre qui permet de surveiller un réseau informatique, il est muni d'une interface graphique qui permet de visualiser ce qui se passe sur un réseau (local et/ou relié à internet). Chaque transfert de donnée est représenté par un trait ainsi qu'un disque de couleur au point d'origine. Les protocoles sont représentés par des couleurs différentes et plus le transfert n'est important plus le disque et le trait sont grands. EtherApe fait visualiser les transferts par IP de destination ou bien par ports TCP. Il est possible d'enregistrer les activités du réseau afin de les étudier après. La destination des transferts d'informations sont affichées soit par son adresse IP soit par l'appellation courante (utilisation d'un serveur DNS). L'utilisateur peut obtenir des informations supplémentaires sur le transfert (port, origine et destination, taille, date...) si il clique sur le trait marquant. On peut configurer EtherApe afin de ne visualiser qu'une partie du trafic (par exemple le trafic vers internet seul).

Installation

apt-get install etherape *puis lancer la commande* ***etherape -i eth0*** *(selon l'interface d'écoute)*

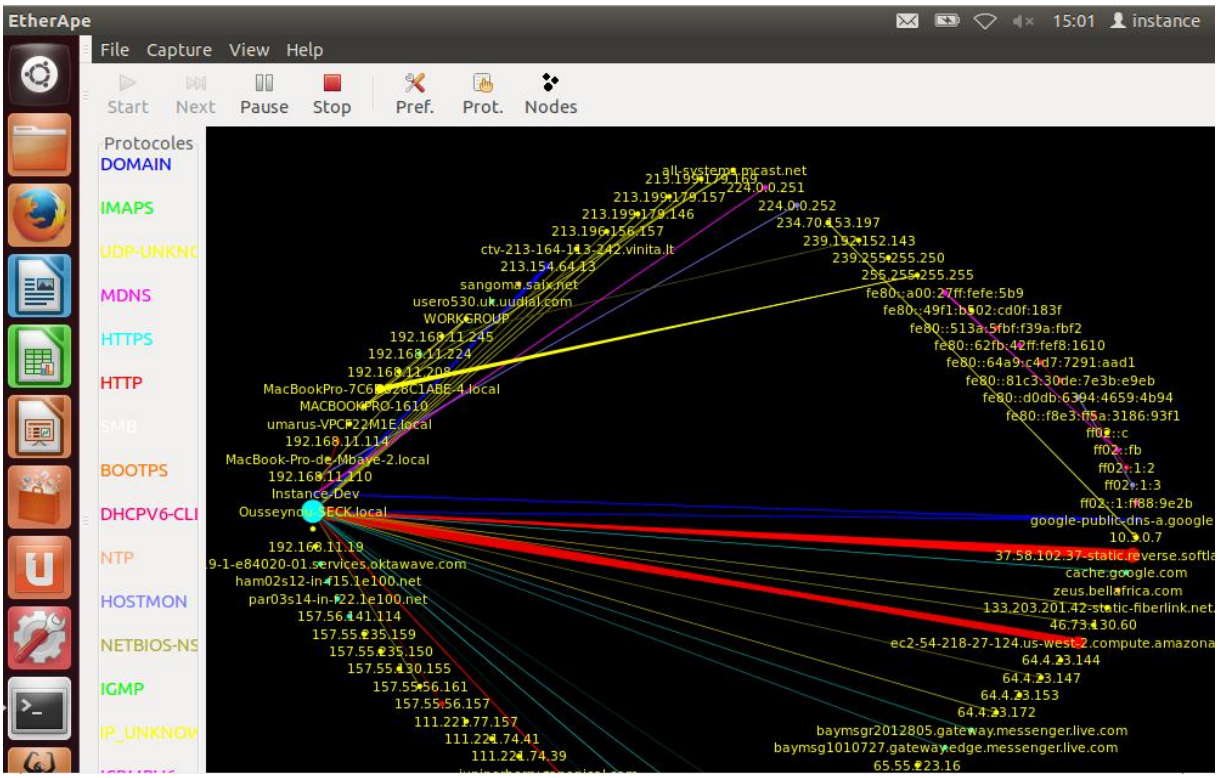


Figure 21: Capture des trafics donnés dans le réseau du Cloud

IV.4.2 IPtraf

C'est un outil de monitoring réseau qui fonctionne sous linux. Nous l'avons utilisé pour mesurer l'activité des interfaces réseau. Voici une liste non-exhaustive de ces capacités:

- Total, IP, TCP, UDP, ICMP, and non-IP byte counts
- TCP source and destination addresses and ports
- TCP packet and byte counts
- TCP flag statuses
- UDP source and destination information
- ICMP type information
- OSPF source and destination information
- TCP and UDP service statistics
- Interface packet counts
- Interface IP checksum error counts
- Interface activity indicators
- LAN station statistics

Installation

apt-get install iptraf *puis lancer la commande* ***iptraf -i eth0*** *(selon votre interface d'écoute)*

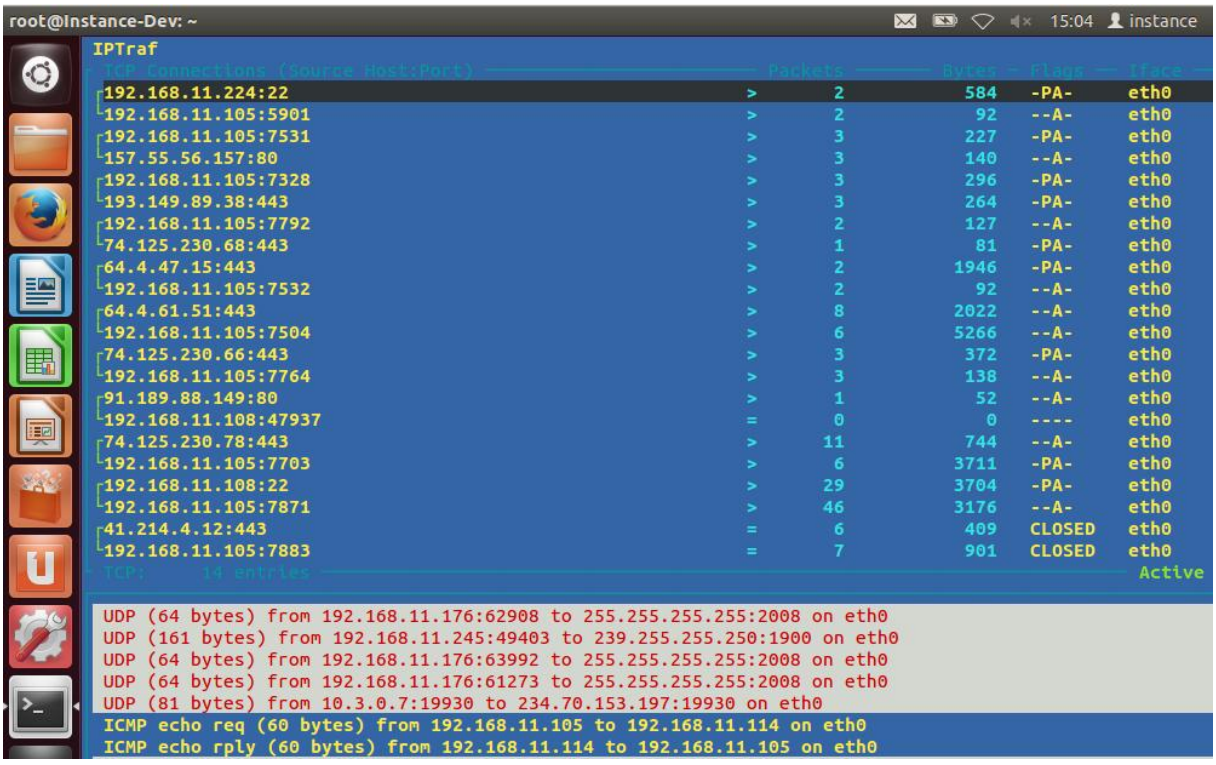


Figure 22: Analyse du réseau avec IPtraf