



Université Catholique de l'Afrique de l'Ouest
Faculté des Sciences de Gestion
INSTITUT SUPERIEUR DE GESTION SAINT MICHEL
Science – Foi – Action



Agrément : n° 05/AG/SAC/MESUCURRS/DES/DFS

Habilitation : N° RepSEN/Ensup-priv/HA/015-2017

SPECIALITE : INFORMATIQUE DE GESTION

MEMOIRE

Présenté par

EL HADJI CHEIKH ASSANE SARR

Pour l'obtention du diplôme de

Master en Informatique de gestion

SUJET

Etude de la vulnérabilité des données dans le Cloud Computing

Et gestion de la sécurité avec OpenStack

Soutenu à UCAO/Saint Michel le 30/03/2019 devant le jury composé de :

Président : Pr Cheikh Amadou Bamba GUEYE	Professeur Titulaire en Informatique	UCAD
Directeur de mémoire : Pr Samba NDIAYE	Professeur Titulaire en Informatique	UCAD
Co-encadreur : Dr Edouard Ngor SARR	Assistant en Informatique	UCAO
Examineur : Dr Reine Marie MARONE	Assistante en Informatique	UCAO

Année 2016-2017

Dédicaces

Je dédie ce mémoire à :

- Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.
- Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutien permanent venu de toi.
- Mes sœurs qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité. Mes professeurs de l'UCAO qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

Remerciements

Nous tenons à exprimer nos vifs remerciements à :

- Dieu le tout puissant, pour la volonté, la santé et la patience qu'il nous a données durant toutes ces années d'études afin que nous puissions en arriver là.
- Le Directeur General
- Le Directeur des études : Monsieur Remy Bass
- Encadreurs : Monsieur Edouard Sarr, Mdm Ndiaye Yacine Dieye Sarr
- les enseignants et les personnes que j'ai eu à côtoyer durant la rédaction de ce mémoire pour leurs aides judicieuses, les moyens qu'ils ont mises à mon disposition pour réaliser ce travail.
- ma famille plus particulièrement mes parents qui m'ont accompagnés durant toute mon cursus.
- Enfin à toute personne qui a collaborée à la réalisation Du présent mémoire.
Puisse dieu vous bénir et descends sa miséricorde sur vous et vos proches.

Résumé

Cloud Computing nouveau modèle de technologie de l'information, il peut fournir à la fois l'infrastructure matérielle et logicielle ainsi que tous les services sont à la demande et via internet. Cependant, l'une des préoccupations importantes de ce service aujourd'hui est de garantir la sécurité de l'infrastructure du cloud. Le travail attendu dans Ce sujet porte sur **L'Étude de la vulnérabilité des données dans le cloud computing et gestion de la sécurité avec OpenStack**. OPENSTACK une solution open source. Le projet *OpenStack* est une plateforme de cloud computing open source qui supporte tous types d'environnements cloud. Le projet vise une implémentation simple, une scalabilité massive, et un ensemble varié de fonctionnalités notamment la sécurisation des VM (Virtual Machine) etc.

Mot clés : vulnérabilité, cloud computing, sécurité, OpenStack

Abstract

Cloud computing is the new model of IT department, it can provide both physical infrastructure and software as well as all services are on demand and via internet. However, one of the major concerns of this service today is to ensure the security of the cloud infrastructure. The expected work in this topic is a study on the security of cloud computing. The expected work in this topic is on the study of data **vulnerability in cloud computing and security management with OpenStack**. OPENSTACK an open source solution. The OpenStack project is an open source cloud computing platform that supports all types of cloud environments. The project aims at a simple implementation, a massive scalability, and a varied set of functionalities including VM security (Virtual Machine) etc.

Mot clés : vulnérability, cloud computing, sécurité, OpenStack

Table des matières

Introduction générale.....	-1-
CHAPITRE 1 : LES NOTIONS FONDAMENTALES DU CLOUD COMPUTING.	3
1.1 Introduction :	3
1.2 Définition de Cloud Computing :	3
1.3 Eléments constitutifs du Cloud Computing :	5
1.3.1 La virtualisation :	5
1.3.2 Le Datacenter :	5
1.3.3 La Plateforme collaborative :	5
1.4 Type de Cloud Computing :	6
1.4.1 Cloud public :	6
1.4.2 Cloud privé :	7
1.4.3 Cloud hybride :	7
1.4.4 Cloud communauté :	8
1.5 Architecture du Cloud Computing :	8
1.5.1 Infrastructure As A Service (IAAS) :	9
1.5.2 Platform As A Service (PAAS) :	10
1.5.3 Software As A Service (SAAS) :	10
1.6 Avantages et inconvénients du Cloud Computing :	12
1.6.1 Les avantages :	12
1.6.2 Les inconvénients :	13
1.7 Conclusion :	14
CHAPITRE 2 :	15
LES MECANISMES DE SECURITE D'UN CLOUD COMPUTING	15
2.1 Introduction :	15
2.2 Les attaques et l'impact sur le Cloud :	15

2.2.1 DoS : Attaques par déni de service :	15
2.2.2 Les Attaques de Session Hijacking :	16
2.2.3 Les attaques SQL injection :	16
2.2.4 Les attaques XSS (Cross Site Scripting) :	17
2.2.5 Les attaques de fragmentation :	18
2.2.6 Les attaques de Spoofing:	18
2.2.7 Balayage de port:	18
2.2.8 L'isolation:	19
2.3 Historique des attaques dans le Cloud:	19
2.4 La sécurité d'infrastructure	20
2.4.1 La sécurité physique d'un Cloud :	20
2.4.2 La virtualisation et la sécurité:	20
2.4.3 La sécurité des flux de données:	21
2.5 La sécurité des données dans le Cloud :	21
2.5.1 Confidentialité :	21
2.5.2 L'intégrité:	22
2.5.3 La disponibilité :	22
2.5.4 Les services de chiffrement (Cryptage)	23
2.6 Le contrôle de sécurité d'un Cloud :	27
2.6.1 Contrôles dissuasifs :	27
2.6.2 Contrôles préventifs :	27
2.6.3 Contrôles correctives :	27
2.6.4 Les contrôles de détection :	28
2.7 Conclusion :	28
CHAPITRE 3 - La mise en place d'OpenStack	29
LA MISE EN PLACE D'OPENSTACK	29
3.1 Introduction :	29

3.2 Présentation d'Openstack:.....	29
3.2.1. Historique :	29
3.2.2. Définition :.....	29
3.3 Architecture d'Openstack :.....	31
3.4 Installation d'Openstack :.....	34
• Installation de Linux :.....	34
• Prérequis du système.....	35
3.5 Création d'un espace Cloud:	39
3.5.1. Création de projet et manipulation de quotas:	39
3.5.2. Création d'un utilisateur:.....	41
3.5 Conclusion:.....	43
CHAPITRE 4 : LA SECURITE DANS L'OPENSTACK	44
4.1 Introduction :	44
4.2 Création d'un Groupe de sécurité:	44
4.2.1. La rédaction des règles d'un groupe :	45
4.2.2. La création des instances :	48
4.2.3. Une vue d'ensemble sur le système :	49
4.3 Les scanners des vulnérabilités:.....	50
4.3.1. Nessus :	51
4.3.2. Nmap :	54
4.4 Les techniques d'attaque :	55
4.4.1. Foot printing :	55
4.4.2. DOS Le déni de service:	56
CONCLUSION GENERALE.....	57
BIBLIOGRAPHIE.....	58
WEB GRAPHIE	60
ANNEXES:.....	61

Cigles

NIST : National Institute of Standards and Technology

CISCO : Est une Systems et entreprise informatique américaine spécialisée.

CIGREF: Le Club Informatique des Grandes Entreprises en Françaises.

SOA : Service Oriented Architecture.

DOS: Denial of Service Attack.

TCP : Transmission Control Protocol

DNS : Domain Name System

SMTP : Simple Mail Transfer Protocol

SAN : Storage Area Network

NAS : Network Attached Storage

EMC : Est une entreprise américaine de logiciels et de systèmes de stockage fondée en 1979 à Newton.

SSH : Secure Shell un protocole de communication sécurisé.

Liste des figures

Figure 1.1 : les services du Cloud Computing.....	4
Figure 1.2 : Les types de Cloud Computing.	8
Figure 1.3 : Les 3 couches du Cloud Computing.	9
Figure 1.4 : Les différents niveaux des services du Cloud Computing.....	11
Tableau 1.1 : Avantages et inconvénients des services.	12
Figure 2.1 :L'attaque par déni de service.	16
Figure 2.2 : L'attaque XSS.....	18
Tableau 2.1 Historique des attaques dans le Cloud	20
Figure 2.3 : La méthode de Chiffrement d'un disque.	26
Figure 3.1: Le rôle d'OpenStack	30
Tableau 3.1 : Les versions d'OpenStack	31
Tableau 3.2 : Services d'openstack	2
Figure 3.2 : l'installation à partir de DevStack.....	34
Figure 3.3 : upgradé et mettre à jour votre système	36
Figure 3.4 : création d'un user pour installation.....	36
Figure 3.5 : téléchargement le devstack	37
Figure 3.6: configuration du fichier local.conf.....	38
Figure 3.7: lancement de l'installation d'openstack	39
Figure 3.8: résumé et fin de l'installation.....	39
Figure 3.9: interface d'administration d'openstack Horizon.....	39
Figure 3.10: Création d'un projet. On remplit les champs comme montré:.....	40
Figure 3.11: Informations nécessaires pour un projet.	40
Figure 3.12: Ressources nécessaire pour le projet.....	41
Figure 3.13: Création d'un utilisateur.	42
Figure 3.14: Page d'accueil pour les membres de projet.	43
Figure 4.1: L'interface de la page Access & Security.....	45

Figure 4.2: L'interface de la fenêtre Create Security Groupe.....	45
Figure 4.3: La liste des groupes de sécurité.....	45
Figure 4.4: L'interface de la page pour ajouter des règles.....	46
Figure 4.5: La liste des règles.....	46
Figure 4.6: L'interface de création le pair de clés.....	47
Figure 4.7: La fenêtre de téléchargement le fichier de clé.....	47
Figure 4.8: L'interface de création des instances.....	48
Figure 4.9: L'interface de l'ajout de la clé et du groupe.....	49
Figure 4.10: La liste des instances.....	49
Figure 4.11: Une vue d'ensemble sur le système.....	50
Figure 4.12: La page login sur Nessus.....	52
Figure 4.13: La page de la nouvelle Policy.....	53
Figure 4.14: La configuration de Policy.....	53
Figure 4.15: La configuration de scan.....	54
Figure 4.16: Nmap.....	55
Figure 4.16 : Maltego Footprinting.....	56
Figure 4.17 : Utilisation de Slowloris.....	56

Liste des tableaux

Tableau 1.1 : Avantages et inconvénients des services.....	56
Tableau 2.1 Historique des attaques dans le Cloud	56
Tableau 3.1 : Les versions d'OpenStack.....	56
Tableau 3.2 : Services d'OpenStack.....	5632-

Introduction générale

La technologie de l'information (TI) est un Ensemble d'outils et de ressources technologiques permettant de transmettre, enregistrer, créer, partager ou échanger des informations, notamment les ordinateurs, l'internet (sites web, blogs et messagerie électronique, Cloud Computing).

Les systèmes d'information sont un enjeu stratégique dans plusieurs domaines Parmi les évolutions récentes, le développement du Cloud Computing et la sécurité est devenu un sujet d'attention.

Le Cloud Computing est maintenant le fondement, de plus l'utilisation d'Internet. Email, moteurs de recherche, réseaux sociaux, médias en streaming, et d'autres services sont désormais hébergés dans "le Cloud «. Les collections des grands serveurs des produits de base en cours d'exécution de coordination logicielles qui rend des hôtes individuels largement disponible. Alors que le Cloud Computing à coûts réduits et une commodité accrue, l'accessibilité et la centralisation du Cloud Computing crée également de nouvelles opportunités pour les failles de sécurité.

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information (SI) . Assurer la sécurité du système d'information est une activité du management du système d'information. Il existe des chercheurs en sécurité qui ont étudié divers aspects de la sécurité du Cloud Computing à la fois une offensive et une perspective défensive.

L'objectif de notre travail est de faire une **Etude de la vulnérabilité des données dans le cloud computing et gestion de la sécurité avec OpenStack**. Dans ce mémoire, nous adopterons une organisation comportant quatre différents chapitres.

Les deux premiers chapitres présentent l'état de l'art sur les notions fondamentales du Cloud Computing et Les mécanismes d'attaques, et de sécurité d'un Cloud Computing. Dans le premier chapitre, nous définirons le Cloud Computing et éléments constitutifs du Cloud Computing, ainsi qu'un aperçu des types de Cloud Computing. A la fin de ce chapitre nous donnons une description sur l'architecture du Cloud Computing.

Dans le deuxième chapitre, il sera consacré pour présenter une étude sur les mécanismes d'attaques et de sécurité d'un Cloud Computing, nous commençons cette étude par les attaques et l'impact courant sur le Cloud. Puis nous introduisons les différentes techniques utilisées pour la sécurité de données du Cloud, en présentant aussi l'historique des attaques dans le Cloud. Nous terminons ce chapitre par le contrôle de sécurité d'un Cloud.

Le troisième chapitre, la réalisation du système, en présentant le système open source OPENSTACK, ainsi nous expliquons les différentes étapes pour l'installation de l'OPENSTACK puis on expliquera comment créer un espace Cloud sur OPENSTACK.

Le quatrième chapitre, nous allons présenter une étude sur la sécurité dans l'OpenStack, puis on expliquera comment on utilise les outils de l'analyse des vulnérabilités d'un Cloud, et les outils de l'attaque. A la fin de ce chapitre nous allons présenter les outils de la sécurité.

Notre travail sera achevé par la conclusion générale qui va résumer nos objectifs estimés et les limites de notre réalisation tout en évoquant les problèmes que nous avons rencontrés et les améliorations envisageables.

CHAPITRE 1 : LES NOTIONS FONDAMENTALES DU CLOUD COMPUTING.

1.1 Introduction

Indéniablement, la technologie de l'internet se développe d'une manière exponentielle depuis sa création. Actuellement, une nouvelle "tendance" a fait son apparition dans le monde de l'IT (information Technologies : Technologies de l'information et de la communication), il s'agit du Cloud Computing. Cette technologie, s'appuie sur le WEB 2.0, offre des occasions aux sociétés de réduire les coûts d'exploitation des logiciels par leurs utilisations directement en ligne. [L2]

Dans ce chapitre nous allons présenter les notions fondamentales du Cloud Computing, ses enjeux, ses évolutions et son utilité ainsi que la technologie qui la constitue et les différents acteurs du secteur. Nous devons dans un premier temps étudier le Cloud Computing de manière générale, dans un second temps nous allons étudier les trois services principaux, sur lesquels le Cloud Computing repose: applicatif, plateforme, infrastructure, qui ont donné naissance aux fameux SaaS/PaaS/IaaS. Et la dernière partie de ce chapitre présente les différents avantages et inconvénients du Cloud Computing.

1.2 Définition de Cloud Computing

Le Cloud Computing traduit de l'anglais « informatique dans les nuages » est devenu un mot à la mode populaire, littéralement l'informatique dans les nuages est un concept qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur. Il consiste à proposer des services informatiques sous forme de service à la demande, accessibles de n'importe où, n'importe quand et par n'importe qui, grâce à un système d'identification, via un PC et une connexion à Internet. Cette définition est loin d'être simple à comprendre, toute fois l'idée principale à retenir est que le Cloud n'est pas un ensemble de technologies, mais un modèle de fourniture, de gestion et de consommation de services et de ressources informatiques. Pour (NIST)^{w1} Le Cloud Computing est un modèle pour permettre, un accès pratique omniprésente au réseau sur demande à un pool partagé de ressources informatiques configurables (réseaux, serveurs, stockage, applications et services) qui Peuvent être

provisionnés rapidement et libérés avec un effort de gestion minimale ou interaction de fournisseur de service. [L2]

La figure ci-dessous (Fig. 1.1) présente les services du Cloud Computing.

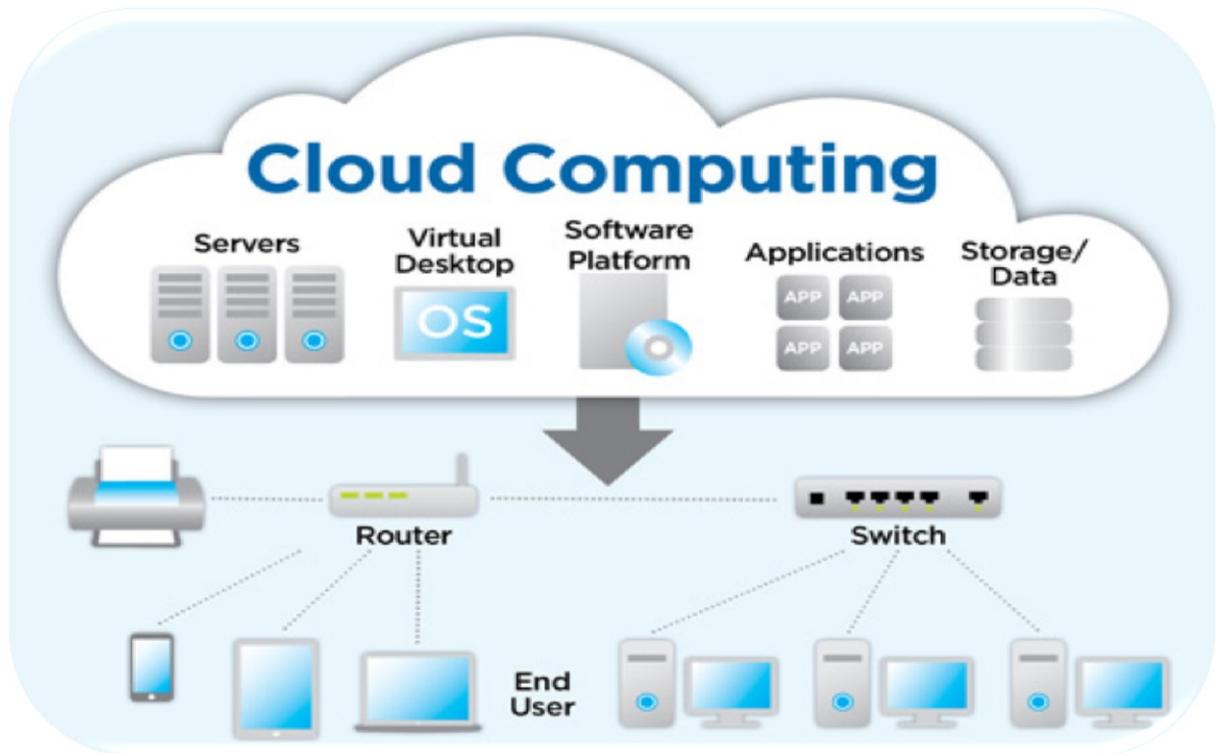


Figure 1.1 : les services du Cloud Computing.

Pour CISCO^{w2} : (Est un Système et entreprise informatique américaine spécialisée). Le Cloud Computing est une plateforme de mutualisation informatique fournissant aux entreprises des services à la demande avec l'illusion d'une infinité de ressources. Pour le groupe de travail CIGREF^{w3} : (Le Club Informatique des Grandes Entreprises en Françaises). Le Cloud Computing est défini par les quatre points suivants :

- Un Cloud est toujours un espace virtuel.
- Contenant des informations qui sont fragmentées.
- Dont les fragments sont toujours dupliqués et répartis dans cet espace virtuel, lequel peut être sur un ou plusieurs supports physiques.
- Qui possède « une console (programme) de restitution » permettant de reconstituer l'information

1.3 Eléments constitutifs du Cloud Computing

Les éléments pouvant constitué le système Cloud sont les suivants:

1.3.1 La virtualisation

Se définit comme l'ensemble des techniques matérielles et/ou logiciels qui permettent de faire fonctionner sur une seule machine, plusieurs systèmes d'exploitation (appelées machines virtuelles (VM), ou encore OS invitée) [L3]

La virtualisation des serveurs permet une plus grande modularité dans la répartition des charges et la reconfiguration des serveurs en cas d'évolution ou de défaillance momentanée. Les intérêts de la virtualisation sont multiples, on peut citer :

- L'utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives).
- L'économie sur le matériel (consommation électrique, entretien physique, surveillance).
- L'installation, tests, développements sans endommager le système hôte.

1.3.2 Le Datacenter

Un centre de traitement de données (data center en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituant le système d'information de l'entreprise (mainframes, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien des prestataires. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Cette infrastructure peut être propre à une entreprise et utilisée par elle seule ou à des fins commerciales. Ainsi, des particuliers ou des entreprises peuvent venir y stocker leurs données suivant des modalités bien définies [L3].

1.3.3 La Plateforme collaborative

Une plate-forme de travail collaborative est un espace de travail virtuel. C'est un site qui centralise tous les outils liés à la conduite d'un projet et les met à disposition des acteurs.

L'objectif du travail collaboratif est de faciliter et d'optimiser la communication entre les individus dans le cadre du travail ou d'une tâche.

Les plates-formes collaboratives intègrent généralement les éléments suivants :

- Des outils informatiques.
- Des guides ou méthodes de travail en groupe, pour améliorer la communication, la production, la coordination.
- Un service de messagerie ;
- Un système de partage des ressources et des fichiers ;
- Des outils de type forum, pages de discussions ;
- Un trombinoscope, ou annuaire des profils des utilisateurs ;
- Des groupes, par projet ou par thématique ;
- Un calendrier. [L6]

1.4 Type de Cloud Computing

Nous distinguons quatre formes de Cloud Computing :

- Cloud public ;
- Cloud privé ;
- Cloud hybride ;
- Cloud communauté.

1.4.1 Cloud public

Un Cloud public est basé sur un modèle standard de Cloud Computing, dans lequel un prestataire de service met les ressources, tels que les applications, ou le stockage, à la disposition du grand public via internet. Le Cloud public peut être gratuit ou fonctionner selon paiement à la consommation.

L'avantage de ce genre d'architecture est d'être facile à mettre en place, pour des coûts relativement raisonnables. La charge du matériel, des applicatifs, de la bande passante étant couverte par le fournisseur. De cette manière ce modèle permet de proposer une souplesse et une évolutivité accrue afin de répondre rapidement au besoin. Il n'y a pas de gaspillage de ressources car le client ne paye que ce qu'il consomme.

Ce type est :

- Demande de lourds investissements pour le fournisseur de services;
- Offre un maximum de flexibilité;
- N'est pas sécurisé.

1.4.2 Cloud privé

C'est un environnement déployé au sein d'une entreprise. Ainsi, elle doit gérer toute seule son infrastructure. Dans ce cas, implémenter un Cloud privé signifie transformer l'infrastructure interne en utilisant des technologies telles que la virtualisation pour enfin délivrer, plus simplement et plus rapidement, des services à la demande. L'avantage de ce type de Cloud par rapport au Cloud public réside dans l'aspect de la sécurité et la protection des données. [L3]

En effet, l'ensemble du matériel est conservé au sein de votre propre emplacement. De ce fait, les ressources sont détenues et contrôlées par votre propre département informatique. Eucalyptus, OpenNebula et OpenStack (Chapitre 3) sont des exemples de solution pour la mise en place du Cloud privé. Ce type est:

- Cher pour le client ;
- Dédié et sécurisé;
- Moins flexible comparé au Cloud public.

1.4.3 Cloud hybride

En général, on entend par Cloud hybride la cohabitation et la communication entre un Cloud privé et un Cloud public dans une organisation partageant des données et des applications (Par exemple, un Cloud dédié pour les données et un autre pour les applications). [L3]

Ce modèle :

- Permet d'allier les avantages des deux modèles de déploiement;
- Permet la gestion de deux Cloud qui peut s'avérer plus contraignant.

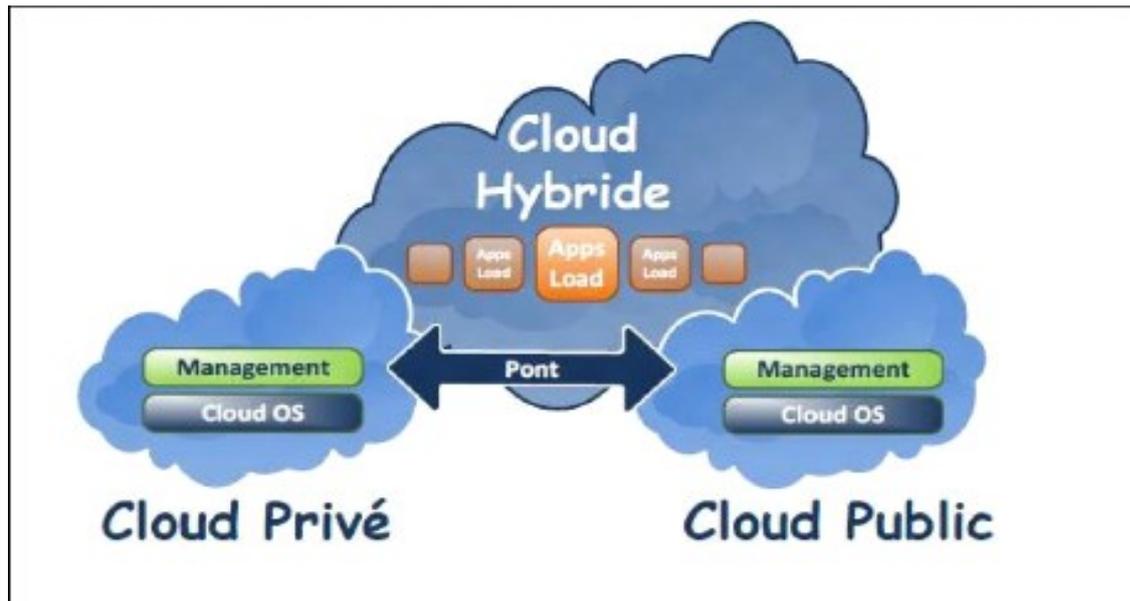


Figure 1.2 : Les types de Cloud Computing.

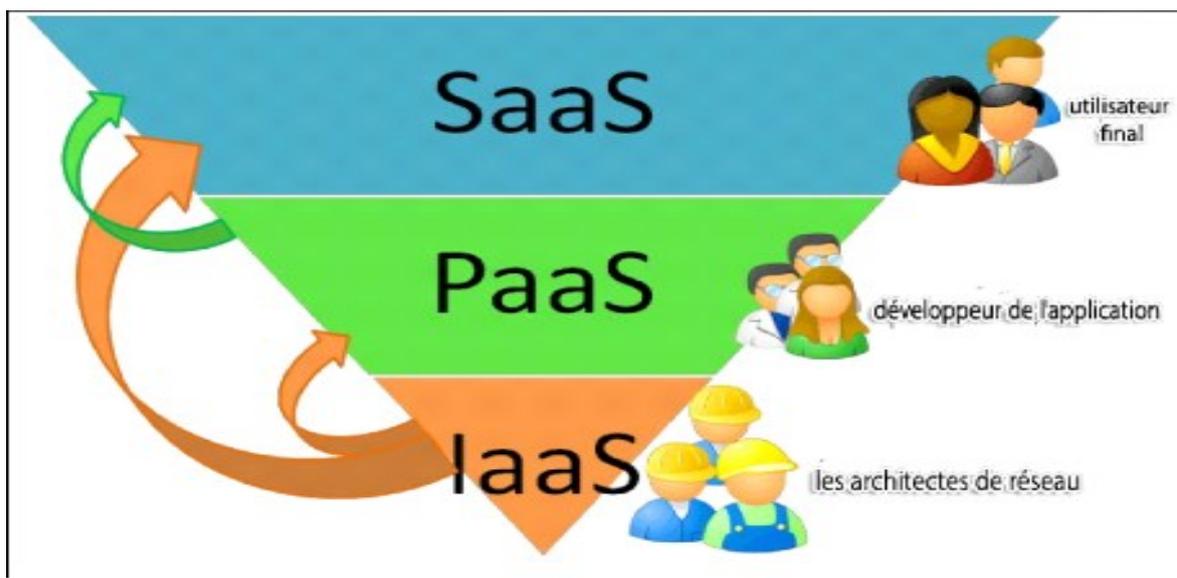
1.4.4 Cloud communauté

L'infrastructure de Cloud est partagé par plusieurs organisations et soutient une communauté spécifique qui a des préoccupations communes (considérations par exemple, la mission, les exigences de sécurité, de la politique, et de conformité). Il peut être géré par les organisations ou un tiers et peut exister sur site ou hors prémisses. [L3]

1.5 Architecture du Cloud Computing

Le Cloud Computing peut être décomposé en trois couches :

- Applicative (SAAS, Software as a Service) ;
- Plateforme (PAAS, Platform as a Service) ;



- Infrastructure (IAAS, Infrastructure as a Service).

Figure 1.3 : Les 3 couches du Cloud Computing.

La Figure 1.3 ci-dessous représente les différentes couches du Cloud Computing de la couche la moins visible pour les utilisateurs finaux à la plus visible. L'infrastructure as a Service (IaaS) est plutôt gérée par les architectes réseaux, la couche PaaS est destinée aux développeurs d'applications et finalement le logiciel comme un service (SaaS) est le « produit final » pour les utilisateurs. [L4]

1.5.1 Infrastructure As A Service (IAAS)

L'IaaS couche du Cloud Computing, la plus complexe en termes de gestion est l'infrastructure comme un service (IaaS). L'infrastructure fournit des capacités de calcul, de stockage et une bande passante suffisante. Cette infrastructure est mise à disposition de façon à gérer automatiquement la charge de travail requise par les applications. Il y a très peu de limitation pour le client si ce n'est la partie matérielle qui peut être contournée grâce aux systèmes de virtualisation. Les applications vont dès lors pouvoir être déployées sans être liées à un serveur spécifique. La virtualisation répond de manière dynamique là où les serveurs physiques fournissent un ensemble de ressources allouées selon les besoins, et où la relation entre les applications et les ressources de calcul, de stockage et de réseau pourront

s'adapter de manière automatique pour répondre à la charge de travail et aux exigences demandées.

Pour simplifier ces différentes définitions, on peut retenir qu'avec le SaaS on utilise une application, avec le PaaS on construit ses applications et finalement l'IaaS permet d'héberger le tout. [L4]

- **Avantage :** Grande flexibilité, contrôle total des systèmes qui permettent d'installer tout type de logiciel métier.
- **Inconvénient :** Besoin d'administrateurs système comme pour les solutions de serveurs classiques sur site.

1.5.2 Platform As A Service (PAAS)

La plateforme comme un service (PaaS), est la plateforme d'exécution, de déploiement et de développement des applications. Le client maintient ses applications, le fournisseur maintient : les runtimes, l'intégration **SOA**, les bases de données, le logiciel serveur, la virtualisation, le matériel serveur, le stockage et les réseaux.

Un service PaaS met à disposition des environnements de développement prêts à l'emploi, fonctionnels et performants. Parmi les solutions : Windows Azure de Microsoft, AppEngine de Google, Force.com de Salesforce. Chaque fournisseur de PaaS propose des environnements de développement différents, Google AppEngine se limite à Java et Python, tandis Windows Azure permet de travailler avec les langages .NET, PHP, Python, Ruby et Java. [L4]

1.5.3 Software As A Service (SAAS)

Ce type de service, des applications sont mises à la disposition des consommateurs. Les applications peuvent être manipulées à l'aide d'un navigateur web ou installées de façon locale sur un PC, et le consommateur n'a pas à se soucier d'effectuer des mises à jour, d'ajouter des patches de sécurité et d'assurer la disponibilité du service.

Gmail est un exemple de tel service. Il offre au consommateur un service de courrier électronique et le consommateur n'a pas à se soucier de la manière dont le service est fourni.

- **Avantage :**

Plus d'installation, plus de mise à jour (elles sont continuées chez le fournisseur), plus de migration de données etc. Paiement à l'usage. Test de nouveaux logiciels avec facilité.

- Inconvénient :

Limitation par définition au logiciel proposé. Pas de contrôle sur le stockage et la sécurisation des données associées au logiciel. Réactivité des applications Web pas toujours idéale. [L3]

La figure ci-dessous (Fig. 1.4) présente les trois couches du Cloud Computing ainsi que leurs acteurs en donnant un compromis flexibilité/simplicité. En Cloud, la flexibilité est obtenue grâce à la virtualisation des systèmes d'exploitation.

La plateforme est exécutée via des machines virtuelles et les ressources peuvent être allouées et délibérées à la demande. Ainsi, l'IaaS est considéré comme le service le plus flexible.

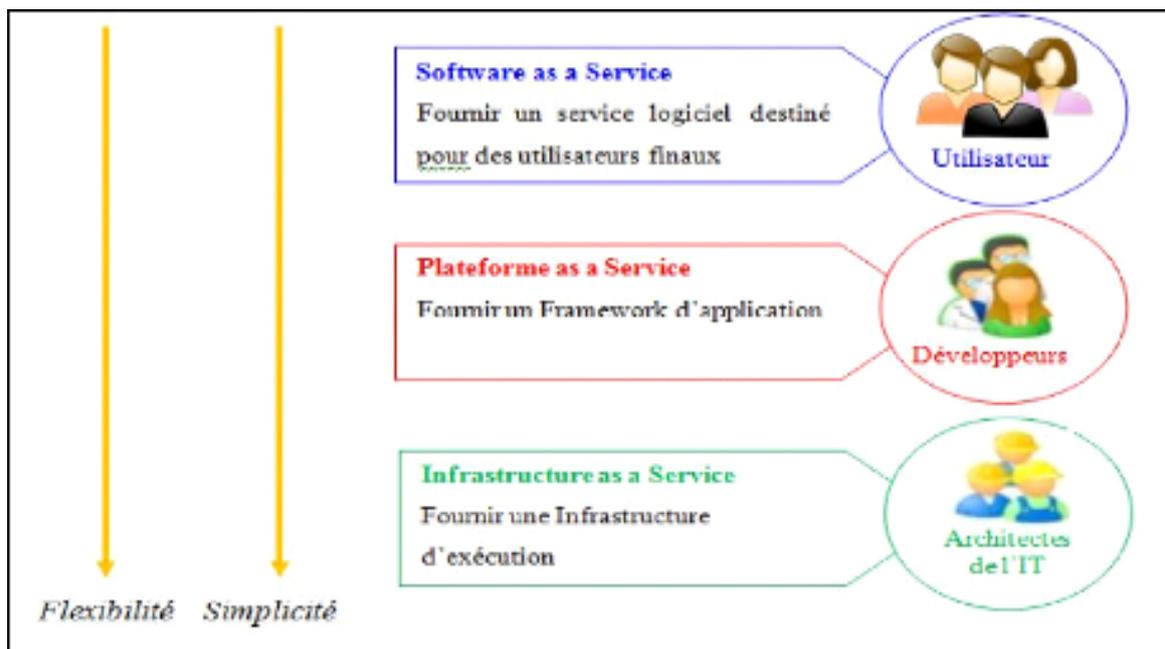


Figure 1.4 : Les différents niveaux des services du Cloud Computing.

- Avantages et inconvénients des services :

Du point de vue économique, le Cloud Computing est essentiellement une offre commerciale d'abonnement économique à des services externes. Selon le National Institute of

Standards and Technologie, il existe trois catégories de services qui peuvent être offertes en Cloud Computing: IaaS, PaaS et SaaS. Les avantages et les inconvénients de ces services ce

	Avantage	Inconvénient
SaaS	<ul style="list-style-type: none"> ✓ Pas d'installation ✓ Plus de licence ✓ Migration ✓ Accessible via un abonnement 	<ul style="list-style-type: none"> ✓ Logiciel limité ✓ Sécurité ✓ Dépendance des prestataires
PaaS	<ul style="list-style-type: none"> ✓ Pas d'infrastructure nécessaire ✓ Pas d'installation ✓ Environnement hétérogène 	<ul style="list-style-type: none"> ✓ Limitation des langages ✓ Pas de personnalisation dans la configuration des machines virtuelles
IaaS	<ul style="list-style-type: none"> ✓ Administration ✓ Personnalisation ✓ Flexibilité d'utilisation ✓ Capacité de stockage infini 	<ul style="list-style-type: none"> ✓ Sécurité ✓ Besoin d'un administrateur système ✓ Demande pour les acteurs du Cloud des investissements très élevés

résume dans le tableau ci-dessous.

Tableau 1.1 : Avantages et inconvénients des services.

1.6 Avantages et inconvénients du Cloud Computing :

1.6.1 Les avantages

Le Cloud Computing peut permettre d'effectuer des économies, notamment grâce à la mutualisation des services sur un grand nombre de clients. Certains analystes indiquent que 20 à 25 % d'économies pourraient être réalisées par les gouvernements sur leur budget informatique s'ils migraient vers le Cloud Computing. Comme pour la virtualisation, l'informatique dans le Cloud peut être aussi intéressante pour le client grâce à son évolutivité. En effet, le coût est fonction de la durée de l'utilisation du service rendu et ne nécessite aucun investissement préalable (homme ou machine). L'« élasticité » du nuage permet de fournir des services évolutifs et peut permettre de supporter des montées en charge. Inversement, le fournisseur a la maîtrise sur les investissements, est maître des tarifs et du catalogue des offres, et peut se rémunérer d'autant plus facilement que les clients sont captifs.

L'abonnement à des services de Cloud Computing peut permettre à l'entreprise de ne plus avoir à acquérir des actifs informatiques et nécessitant une durée d'amortissement. Les dépenses informatiques peuvent être comptabilisées en tant que dépenses de fonctionnement. La maintenance, la sécurisation et les évolutions des services étant à la charge exclusive du prestataire, dont c'est généralement le cœur de métier, celles-ci ont tendance à être mieux réalisées et plus rapidement que lorsque sous la responsabilité du client (principalement lorsque celui-ci n'est pas une organisation à vocation informatique).

1.6.2 Les inconvénients

Plusieurs catégories d'inconvénients existent :

L'utilisation des réseaux publics, dans le cas du Cloud public, entraîne des risques liés à la sécurité du Cloud (chapitre 2). En effet, la connexion entre les postes et les serveurs applicatifs passe par le réseau internet, et expose à des risques supplémentaires de cyber attaques, et de violation de confidentialité. Le risque existe pour les particuliers, mais aussi pour les grandes et moyennes entreprises, qui ont depuis longtemps protégé leurs serveurs et leurs applications des attaques venues de l'extérieur grâce à des réseaux internes cloisonnés.

Le client d'un service de Cloud Computing devient très dépendant de la qualité du réseau pour accéder à ce service. Aucun fournisseur de service Cloud ne peut garantir une disponibilité de 100 % Par exemple, des défaillances sur les services Cloud sont référencées par l'International Working Group of Cloud Résilience. Les entreprises perdent la maîtrise de l'implantation de leurs données. De ce fait, les interfaces inter-applicatives (qui peuvent être volumineuses) deviennent beaucoup plus complexes à mettre en oeuvre que sur une architecture hébergée en interne. Les entreprises n'ont plus de garanties (autres que contractuelles) de l'utilisation qui est faite de leurs données, puisqu'elles les confient à des tiers. Les questions juridiques posées notamment par l'absence de localisation précise des données du Cloud Computing Les lois en vigueur s'appliquent, mais pour quel serveur, quel data center, et surtout quel pays ? Tout comme les logiciels installés localement, les services de Cloud Computing sont utilisables pour lancer des attaques (craquage de mots de passe, déni de service...).

En 2009, par exemple, un cheval de Troie a été utilisé illégalement dans un service du Cloud public d'Amazon pour infecter des ordinateurs. [L2]

1.7 Conclusion

Au cours de cette première partie, nous avons fourni une base théorique sur le Cloud Computing, en présentant ses types, ses services (IaaS, PaaS, SaaS), ses avantages et inconvénients, afin d'appliquer ses concepts à notre contexte.

CHAPITRE 2 : LES MECANISMES DE SECURITE D'UN CLOUD COMPUTING

2.1 Introduction

La sécurité du Cloud (Cloud Security en anglais) est un sous domaine du Cloud Computing en relation avec la sécurité informatique. Elle implique des concepts tels que la sécurité des réseaux, du matériel et les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure associées au Cloud Computing. Un aspect important du Cloud est la notion d'interconnexion avec divers matériels qui rend difficile et nécessaire la sécurisation de ces environnements. [L5]

2.2 Les attaques et l'impact sur le Cloud

Les composants de sécurité telle que les pare feu ou les systèmes de détection d'intrusion, ne sont pas adaptés pour détecter les attaques distribuées, Ces attaques sont donc subdivisées en sous attaques afin d'être indétectable par de tel système de sécurité. Dans ce chapitre nous allons présenter les attaques actuelles sur le Cloud Computing.

2.2.1 DoS : Attaques par déni de service

L'attaque par déni de service a pour but de rendre un service indisponible par une surcharge réseau. L'attaque (Dos¹) pourrait utiliser certaines des techniques suivantes de submerger les ressources d'une Cloud :

- Remplissage de l'espace disque de stockage d'entraînement d'une Cloud à l'aide d'énormes pièces jointes ou les transferts des fichiers ;
- Envoi d'un message qui réinitialise un masque de sous-réseau de l'hôte cible, provoquant une perturbation de sous-réseau de routage du Target ;
- D'utiliser tous les moyens d'un Target pour accepter les connexions réseau, ce qui entraîne des connexions réseau supplémentaires étant refusée.

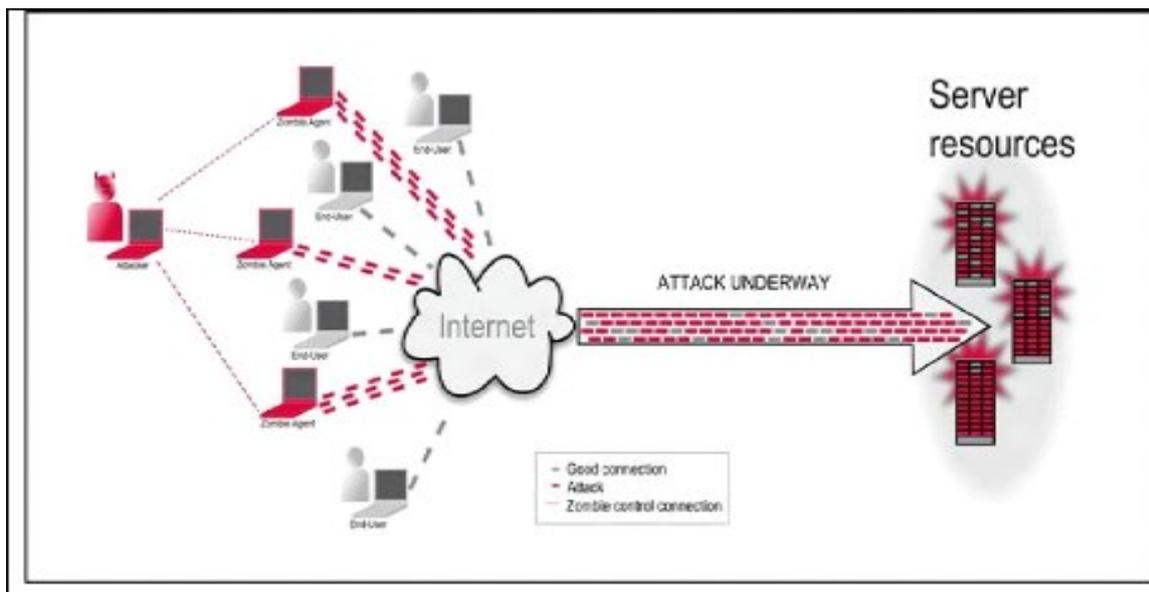


Figure 2.1 :L'attaque par déni de service.

2.2.2 Les Attaques de Session Hijacking

L'accès non autorisé à un système peut être réalisé par le détournement de session. Dans ce type d'attaque, un attaquant détourné une session entre un client de confiance et de serveur Cloud. L'ordinateur attaquant remplace son adresse IP à celle du client de confiance et le Cloud poursuit le dialogue, estimant qu'il communique avec le client de confiance. Attaques de détournement comprennent IP attaques Spoofing, numéro de séquence TCP et DNS. [L6]

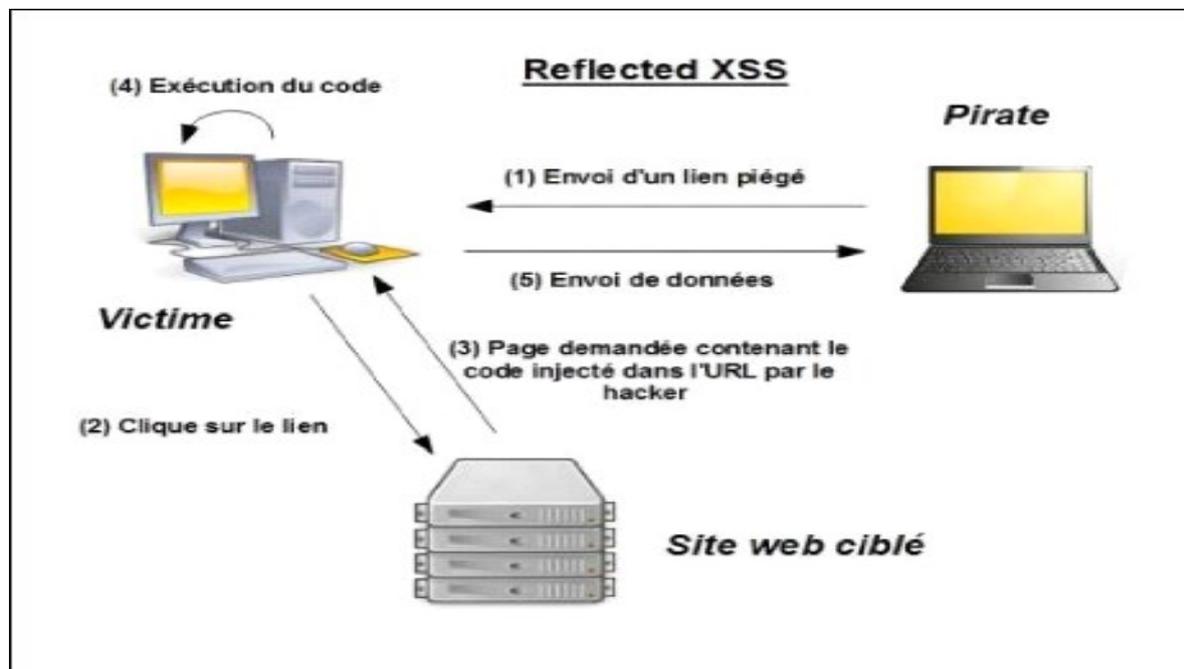
2.2.3 Les attaques SQL injection

Injection SQL est une méthode d'attaque où un attaquant peut exploiter code vulnérable et le type de données d'une application acceptera, et peut être exploitée dans ne importe quel paramètre d'application qui influe sur une requête de base de données. Les exemples incluent des paramètres dans l'URL elle-même, les données de poste, ou la valeur du cookie. En cas de succès, SQL injection peut donner un attaquant d'accéder au contenu de base de données d'arrière-plan, la capacité d'exécuter des commandes à distance du système, ou dans certaines circonstances, les moyens de prendre le contrôle du serveur hébergeant la base de données.

Nous avons vu dans certains des commentaires précédents sur la conception de base de données multiples locataire, que le stockage de la base de données des locataires multiples dans la même table séparés par l'ID de locataire agissant comme une clé primaire est un modèle de conception valide. Par exemple, si il y'a un détail applications SaaS qui permet plusieurs détaillants d'héberger leurs produits et de les vendre à travers l'application de SaaS en ligne, alors la mesure du possible une conception de la table de locataire pour table qui accueille toutes les commandes pourraient l'être. Si l'application SaaS est sujette à l'injection SQL, alors il est très facile pour certains une exploitation forestière au nom de One locataire peut afficher les commandes appartenant à un autre client. [L6]

2.2.4 Les attaques XSS (Cross Site Scripting)

Le cross site Scripting (abrégié XSS), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java, Flash...) et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML5. Il est par exemple possible de voler la session en



récupérant les cookies.

Figure 2.2 : L'attaque XSS

2.2.5 Les attaques de fragmentation

Attaques par fragmentation IP utilisent variée datagramme IP fragmentation de déguiser leurs paquets TCP à partir des dispositifs de filtrage IP d'une cible. Voici deux exemples de ces types d'attaques sont les suivantes:

- Une attaque de fragment minuscule se produit lorsque l'intrus envoie un très petit fragment qui oblige une partie de la tête TCP champ dans un second fragment. Si le dispositif de filtrage de la cible n'applique pas la taille des fragments minimum, ce paquet illégal peut alors être transmis via le réseau de la cible.

- Une attaque de fragment de chevauchement est une autre variation sur le zéro-offset modification d'un datagramme. Les paquets suivants écrasent les informations d'adresse de destination du paquet initial, puis le deuxième paquet est passé par le dispositif de filtrage de la cible. Cela peut se produire si le dispositif de filtrage de la cible n'applique pas un fragment décalage minimum pour les fragments avec des décalages de zéro.

2.2.6 Les attaques de Spoofing

Les intrus utilisent IP Spoofing pour convaincre un système qu'il est en communication avec une entité connue de confiance afin de fournir l'intrus avec un accès au système. Usurpation d'adresse IP implique la modification d'un paquet au niveau de TCP, qui est utilisé pour attaquer les systèmes connectés à Internet qui offrent divers services TCP / IP. L'attaquant envoie un paquet avec une adresse IP source de, un hôte connu de confiance au lieu de sa propre adresse IP source à un hôte cible. L'hôte cible peut accepter le paquet et agir sur elle. [L7]

2.2.7 Balayage de port

L'attaque par balayage de port permet à celui-ci de découvrir des ports de communication exploitables. Cette attaque peut être évitée grâce à des systèmes de sécurité comme un pare-feu ou encore un système de détection d'intrusion ((en) IDS : Intrusion System Detection). Les infrastructures du Cloud sont sensibles à ce type d'attaque si celle-ci est effectuée en parallèle. Un système tel que l'IDS analyse une partie du trafic et ne détecte donc pas une

attaque par scan de port si celle-ci est effectuée avec différents scanners. Les solutions de sécurité actuelle ne sont pas adaptées pour ce type d'attaque sur une telle infrastructure. [L7]

2.2.8 L'isolation

Le Cloud Computing introduit le partage de ressources, ce qui peut potentiellement mener à des attaques de type attaque par canal auxiliaire (écoute passive d'informations) ou canal caché (envoi d'informations) entre différentes machines virtuelles évoluant dans le même environnement. Le problème d'isolation réside dans le fait que l'environnement (machine virtuelle) d'un attaquant peut potentiellement se retrouver sur la même machine physique d'un utilisateur cause que cette dernière héberge de multiples machines virtuelles. Cela lui permet de mettre en place différentes attaques matérielles ou logicielles pour écouter ou perturber les autres machines virtuelles. [L8]

2.3 Historique des attaques dans le Cloud

La plupart des attaques sur le Cloud Computing au cours des dernières années (2014,2015) sont des attaques par déni de service DDOS. Mais dans les années (2011, 2012,2013) il existe plusieurs attaques le tableau suivant représente historique des attaques dans le Cloud.

Victime	Date	Type d'attaque	Description
Dropbox	Octobre 2012	Analyse du client Dropbox	Analyse du client Dropbox et démonstration de vulnérabilités exploitables localement et à distance. http://archive.hack.lu/2012/Dropbox%20security.pdf [archive]
Epsilon	Mars 2012	Hameçonnage par e-mail	Récupération des noms et e-mail de plus de 20 entreprises clientes de la société Epsilon.
Dropbox	Juin 2012	Vol de mot de passe et ingénierie sociale	Vol de mot de passe de compte Dropbox d'un employé et récupération d'informations concernant un projet confidentiel. Menant à une large campagne de spam.
Rackspace	Juin 2012	Prédiction de mot de passe administrateur	Plusieurs failles de sécurité ont permis de prédire ou modifier le mot de passe administrateur de compte rackspace. http://mesoscale-convective-vortex.blogspot.fr/2012/06/multiple-rackspace-security.html [archive]
iCloud	Août 2012	Vol de mot de passe et ingénierie sociale	Un journaliste possédant un compte iCloud a été victime du vol de plusieurs de ses comptes y compris l'effacement de ses données sur des périphériques Apple en utilisant iCloud.
CloudFlare	Mai 2012	Exploitation d'une vulnérabilité Google Apps/Gmail	AT & T trompés en redirigeant un message vocal à une boîte vocale frauduleuse. Processus de récupération de compte Google a été exploité par la boîte vocale frauduleuse, ce qui permet d'atteindre des craquelins Gmail PIN de récupération de compte, et pour réinitialiser le compte Gmail. Une vulnérabilité dans le processus de récupération de Google Enterprise Applications qui a permis aux pirates de contourner l'authentification à deux facteurs de l'adresse URL utilisateur CloudFlare.com. Vulnérabilités BCCing CloudFlare a permis aux cybercriminels pour réinitialiser un mot de passe client une fois qu'ils avaient eu accès à un compte de messagerie administrative.
PlayStation Network	Avril 2011	Injection SQL	Le service PlayStation Network de Sony victime d'une attaque par injection sql et exploitation d'un défaut de chiffrement des données utilisateurs du PSN, obligeant la société à arrêter complètement son réseau en ligne de jeux vidéo et PlayStation Store.
VMWARE	Juin 2009	Exécution de code à l'extérieur du VMWARE Guest	CLOUDBURST A VMware Guest to Host Escape Story http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf [archive]

Tableau 2.1 Historique des attaques dans le Cloud

2.4 La sécurité d'infrastructure

2.4.1 La sécurité physique d'un Cloud

La sécurité physique est rompue avec le modèle du Cloud, à cause de la notion de partage de ressources et de virtualisation. Une machine physique partage ses ressources avec les différentes machines virtuelles qu'elle héberge et ceci indépendamment du client de la machine. Il revient logiquement au fournisseur de choisir ou mettre en place son architecture et quelle sécurité physique est déployée, mais aussi protéger et documenter l'accès aux données utilisateur. [L7]

2.4.2 La virtualisation et la sécurité

La virtualisation est liée au Cloud Computing. En effet, le fournisseur de Cloud propose à ces clients d'acquérir son propre serveur autrement dit sa propre machine virtuelle. Le

fournisseur de Cloud, propose ce service sans prendre connaissance du système d'exploitation installé sur cette machine virtuelle, ni de la configuration de celui-ci. Néanmoins, ce dernier propose un système de sécurité comme service (Security as a service) basé sur l'introspection des machines virtuelle. [L9]

Une machine virtuelle peut subir une attaque basée sur la modification de la mémoire. L'attaquant peut soit y introduire un Rootkit ou des données dans les zones protégées de celle-ci. Quelques implémentations de protection pour la mémoire :

- CoPilot, un noyau de système d'exploitation basé sur le contrôle d'intégrité et la détection des modifications illégales d'un noyau Linux ;
- Paladin, un composant qui utilise la virtualisation pour la détection et le contrôle d'une attaque par Rootkit ;
- Xenkimono, Un composant qui détecte les violations des règles de sécurité en utilisant l'introspection de la machine virtuelle (VMI). Il implémente un contrôle d'intégrité, pour détecter la modification du code du noyau système ;
- SecVisor, un petit hyperviseur qui assure que le code exécuté par le noyau système est approuvé par l'utilisateur. Il utilise pour cela la virtualisation de la mémoire physique.

2.4.3 La sécurité des flux de données:

Une attaque sur les machines virtuelles peut agir sur des flux de données par exemple. C'est pour cela que la mise en place de système de contrôle et d'intégrité doit permettre d'éviter la modification des flux de donnée. Lares est un exemple de composant permettant via l'introduction d'un outil sur le système d'exploitation cible, de vérifier si la machine virtuelle est sécurisée. Il utilise pour cela la vérification des règles de sécurité et l'introspection de la machine virtuelle. [L7]

2.5 La sécurité des données dans le Cloud

Confidentialité, l'intégrité et la disponibilité sont parfois connues comme la triade CIA de la sécurité du système d'information, et sont des piliers importants de l'assurance de Cloud.

2.5.1 Confidentialité

Se réfère à la prévention de la divulgation non autorisée intentionnelle ou involontaire d'informations. Confidentialité dans les systèmes de Cloud Computing est liée aux domaines des droits de propriété intellectuelle, canaux cachés, analyse le trafic, cryptage et l'inférence:

- **Droits de propriété intellectuelle** : La propriété intellectuelle (IP) comprend les inventions, les dessins, et artistiques, musicales et œuvres littéraires. Les droits de propriété intellectuelle sont protégés par les lois de droits d'auteur, qui protègent les créations de l'esprit, et les brevets, qui sont accordés pour les inventions nouvelles ;
- **Les canaux cachés** : Un canal caché est une voie de communication non autorisée et involontaire qui permet l'échange d'informations, Canaux cachés peuvent être réalisés par le calendrier des messages ou l'utilisation inappropriée des mécanismes de stockage ;
- **L'analyse du trafic** : est une forme de violation de confidentialité qui peut être accompli en analysant le volume, la vitesse, la source et la destination du trafic de message, même si elle est cryptée. L'activité de message accrue et rafales élevés de trafic peuvent indiquer un événement majeur se produit. Contre-mesures à l'analyse du trafic comprennent le maintien d'un taux quasi-constante de trafic et un message déguiser les emplacements source et destination du trafic ;
- **l'inférence** : est généralement associée à la sécurité de base de données. Inférence est la capacité d'une entité d'utiliser et de corréler des informations protégées à un niveau de sécurité pour découvrir des informations qui est protégé à un niveau de sécurité plus élevé.

2.5.2 L'intégrité

Le concept de l'intégrité des informations de Cloud exige que les trois principes suivants soient remplis:

- Les modifications ne sont pas faites pour les données par le personnel ou des processus non autorisés ;
- Les modifications non autorisées ne sont pas faites à des données par le personnel ou processus autorisés ;
- Les données est interne et externe cohérente - en d'autres termes, l'information interne est conforme à la fois entre tous les sous-entités et avec le monde réel, la situation extérieure.

2.5.3 La disponibilité

Disponibilité assurer l'accès fiable et rapide aux données en nuage ou Cloud Computing ressources par le personnel approprié. Disponibilité garantit que les systèmes fonctionnent correctement en cas de besoin. En outre, ce concept garantit que les services de sécurité du système de Cloud sont en ordre de marche. Une attaque par déni de service est un exemple d'une menace contre la disponibilité. [L8]

2.5.4 Les services de chiffrement (Cryptage)

Le Cryptage de la Cloud Computing est sur les données et les bases de données. Les principales manifestations de cryptage des données sur le mouvement sont:

- **Secure Socket Layer (SSL) :** Cela a été une procédure d'exploitation standard depuis des années, nous n'allons pas exposer à ce sujet dans une grande longueur, sauf ces quatre points:

1. Mettre en œuvre SSL chaque fois qu'il y'a du trafic confidentielles sur les serveurs Web ou des lignes non garantis ;

2. Avoir un moyen systématique de manipulation expiration et la délivrance des certificats SSL de sorte que vous ne avez pas a perturbé les opérations commerciales ;

3. Mettre en oeuvre le protocole SSL pour le trafic Web de la console d'administration ;

4. Assurez-vous d'utiliser les normes SSL acceptées par l'industrie. En cas de doute, reportez-vous aux dernières mises à jour de l'Institut National des Standards and Technologie (NIST). Les orientations actuelles dans NIST SP 800-522 recommande SSL v3. [L7]

- **Les Réseaux privés virtuels (VPN) :** Dans le contexte de Cloud privé, VPN pourrait être utilisé pour fournir les fonctionnalités suivantes:

1. Connexion de site à site: Cette fonctionnalité assure deux points de communication. Dans une mise en œuvre de Cloud privé, vous pourriez avoir à autoriser les connexions de partenaires d'affaires pour transférer des données ou offrent des services partagés ;

2. L'utilisateur final un accès à distance: Vos utilisateurs finaux pourraient vouloir accéder à votre capacité de Cloud privé de l'extérieur de votre réseau. Utiliser un VPN ou le client

IPsec pour sécuriser les communications dans votre réseau. Appliquer posture contrôle sur la connexion VPN de sorte que vous pouvez valider le client à la source ;

3. Administrateur VPN: Une passerelle VPN peut être établie pour fournir un point de passage obligé pour tous les accès administratifs dans le Cloud privé.

- **Secure Shell (SSH)** : est couramment utilisé par les administrateurs pour l'accès distant à la console. Il peut sembler que VPN et SSH sont redondants. Toutefois, si Telnet est autorisée au lieu de SSH, le trafic de la Cloud sera clair. Une session Telnet contenant les informations d'identification d'administrateur peut être reniflée en texte clair. Se débarrasser de Telnet tous ensemble et l'application SSH comme une norme minimale est nécessaire, même avec la superposition des VPN ; [L7]

- **Secure File Transfer Protocol (SFTP)** : Si il ya des exigences pour transférer des fichiers en toute sécurité vers et depuis votre Cloud privé, se assurer que vous établissez un processus de SFTP :

1. Établir un processus de gestion des utilisateurs d'identifier clairement et l'accès de l'utilisateur de commande ;

2. Établir de provisionnement, et les processus de certification de l'utilisateur ;

3. Établir des autorisations d'accès appropriées et dossier isolement pour les utilisateurs SFTP ;

4. Appliquer nettoyage de données de dossiers SFTP sur une base périodique ;

- **Transport Layer Security (TLS)** : Chiffrement TLS est généralement utilisé pour crypter le trafic SMTP : (*Simple Mail Transfer Protocol*) sur deux passerelles de messagerie. Cela pourrait ne pas être spécifique à votre mise en œuvre de Cloud privé, mais il est traité ici d'être exhaustif ;

- **Le cryptage de la base de données** : le majeur té de base de données telle qu'Oracle et Microsoft SQL ont intégré dans les capacités de cryptage au sein de leurs applications. La méthodologie de cryptage de base de données de premier plan est appelé chiffrement transparent des données (TDE). TDE fournit des systèmes de gestion de base de données avec la possibilité de crypter l'ensemble de base de données, ou pour seulement crypter certaines colonnes ;

- **Les Appareils de chiffrement** : sont un moyen pour les fonctions cryptographiques à exécuter sur le réseau. La logique de l'application fait un appel de programmation vers le module de chiffrement sur le dispositif pour chiffrer les données avant de les stocker dans la base de données. Voici quelques-uns des facteurs clés à considérer lors de l'utilisation d'un appareil de chiffrement:

1. Performance: dispositifs de cryptage attachés réseau sont des appareils spécialisés construits dans le but d'exécuter des fonctions cryptographiques ;

2. Centralisée: L'appareil de chiffrement peut être utilisé par différents locataires sur notre Cloud privé ;

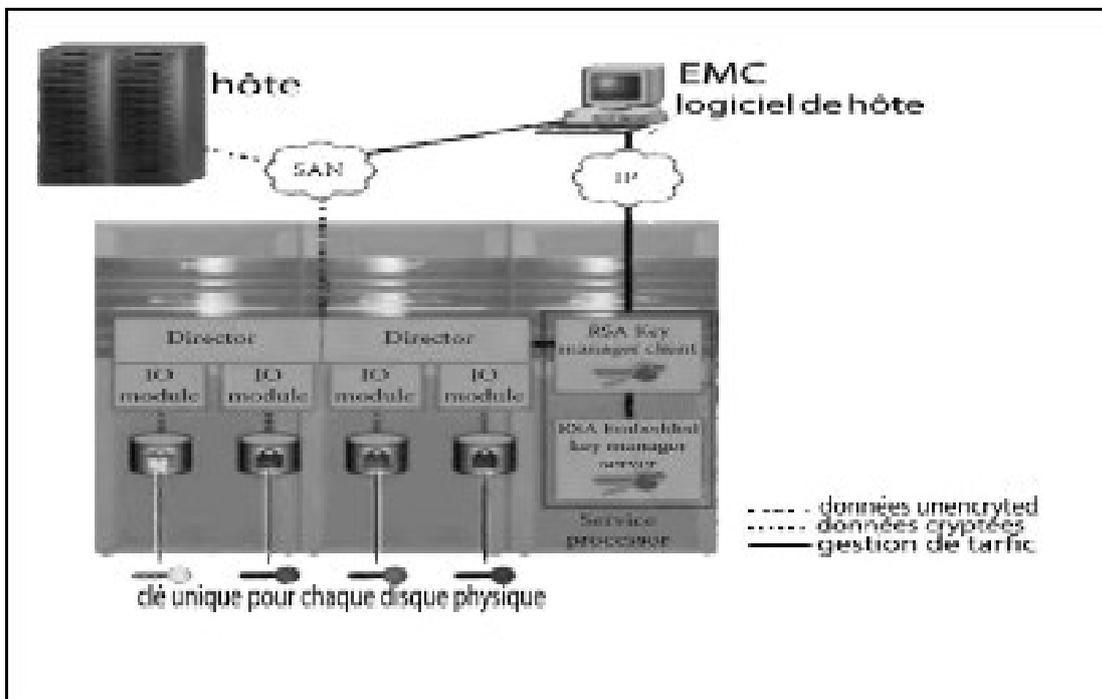
3. Impact applications: Ces solutions offrent plusieurs façons d'appeler la fonction de cryptage, il peut être un appel de programmation qui envoie un champ à chiffrer avant le stockage dans la base de données ;

4. Les coûts de licence: Ces appareils peuvent être agréés par connecteur, par des fonctions cryptographiques, ou une taxe de l'appareil une fois l'entretien ;

- **Chiffrement de disque** : est une fonction matérielle de cryptage de la totalité du disque au lieu de crypter des fichiers, les volumes ou les espaces table. Ceci est analogue à chiffrement de disque dur déployé au niveau d'ordinateur portable; Toutefois, aux fins de Cloud, nous transposant sa capacité à réseau de stockage SAN et de stockage en réseau NAS Déploiements varient selon le fournisseur. Certains fournisseurs, comme EMC, intègrent.

La solution comme un module supplémentaire au sein de la solution de gestion de stockage (figure 2.3).

Figure 2.3 : La méthode de Chiffrement d'un disque.



- La mise en œuvre basée sur un agent est similaire à pré cryptage de disque de démarrage. Fondamentalement, l'agent est chargé dans la machine virtuelle et intercepte la séquence de l'instance virtuelle démarrage. L'agent s'exécute alors une séquence d'authentification de pré-lancement pour valider et appliquer le domaine de cryptage approprié pour cette instance virtuelle. Essentiellement, le domaine de cryptage peut agir comme un mécanisme de segmentation sur votre Cloud privé pour vos unités ou des environnements commerciaux conformité lourd. En enveloppant un domaine de cryptage autour de ces systèmes, vous pouvez répondre à l'exigence de crypter les données pour l'ensemble de la pile. Comme pour les autres technologies de cryptage, tout crypter les données seule n'est pas suffisante pour répondre à la plupart des exigences de conformité. Assurez-vous que le fournisseur peut répondre aux exigences de gestion des clés de chiffrement et de l'ensemble de la. En cas de doute, valider avec notre vérificateur ou évaluateur de sécurité qualifié. Tenez compte des facteurs suivants lors de l'examen de cryptage instance virtuelle à base d'agents:

1. les mécanismes de gestion des clés pour la solution de cryptage ;

2. Assurez-vous que les clés sont distribuées en toute sécurité lors de l'exécution ;
3. Veiller à ce que des clés de cryptage sont protégées lorsqu'ils sont stockés ;
4. Valider contrôle d'accès pour utilisation de la clé ;
5. Assurer la vérifiabilité et la traçabilité de l'utilisation des clés.

Certains fournisseurs ont la possibilité d'étendre les modules de cryptage pour les deux Cloud privés et publics. L'aspect basé sur un agent de cette solution facilite un déploiement plus facile car il est dépendant le moins possible sur l'extrémité arrière de Cloud public. La gestion des clés peut être retenue à l'intérieur de l'entreprise avec un appareil de distribution de clé qui se trouve dans le Cloud public. [L8]

2.6 Le contrôle de sécurité d'un Cloud

L'objectif des contrôles de sécurité de nuage est de réduire les vulnérabilités à un niveau tolérable et de minimiser les effets d'une attaque. Pour ce faire, une organisation doit déterminer quel impact pourrait avoir une attaque, et la probabilité de perte. Exemples de perte sont compromission d'informations sensibles, malversations financières, perte de réputation, et la destruction physique des ressources. Le processus d'analyse différents scénarios de menace et de produire une valeur représentative de la perte potentielle estimée est connu comme une analyse des risques (RA). Contrôles fonctionnent comme des contre-mesures pour les vulnérabilités. Il existe plusieurs types de commandes, mais ils sont généralement classés dans l'un des quatre types suivants:

2.6.1 Contrôles dissuasifs

Réduire la probabilité d'une attaque délibérée.

2.6.2 Contrôles préventifs

Protéger les vulnérabilités et faire une attaque infructueuse ou réduire son impact. Contrôles préventifs inhibent tentatives de violation de la politique de sécurité.

2.6.3 Contrôles correctives

Réduire l'effet d'une attaque.

2.6.4 Les contrôles de détection

Découvrez les attaques et déclenchent des contrôles préventives ou correctives. Les contrôles de détection avertissent des violations ou tentatives de violations de la politique de sécurité et comprennent des contrôles que les systèmes de détection d'intrusion, les politiques organisationnelles, des caméras vidéo et des détecteurs de mouvement.

2.7 Conclusion

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.

Chapitre 3 - LA MISE EN PLACE D'OPENSTACK

3.1 Introduction

Le Cloud Computing représente un nouveau défi dans le monde informatique. Plusieurs solutions sont proposées : des solutions propriétaires et des solutions open sources. Dans ce chapitre, nous allons présenter OPENSTACK une solution open source. Le projet *OpenStack* est une plateforme de cloud computing open source qui supporte tous types d'environnements cloud. Le projet vise une implémentation simple, une scalabilité massive, et un ensemble varié de fonctionnalités.

3.2 Présentation d'OpenStack

3.2.1. Historique

Créé en juillet 2010 par la NASA et l'hébergeur américain Rackspace, OpenStack est une offre d'IaaS 100% open-source encore en développement qui a livré son code source récemment et qui permet aux sociétés de développer leurs propres solutions d'infrastructure du Cloud Computing. Plus de trente fournisseurs soutiennent ce projet tels que: AMD, Intel, Dell et Citrix. OpenStack devrait également être intégré dans les prochaines versions d'Ubuntu comme c'est le cas pour Eucalyptus. Il comprend le logiciel OpenStack Compute pour la création automatique et la gestion de grands groupes de serveurs privés virtuels et le logiciel OpenStack Stockage pour optimiser la gestion de stockage, répliquer le contenu sur différents serveurs et le mettre à disposition pour une utilisation massive des données [W9]

3.2.2. Définition

OpenStack est un logiciel libre qui permet la construction de Cloud privé et public de type IaaS sous licence Apache qui a pour but d'aider les organisations à mettre en œuvre un système de serveur et de stockage virtuel. 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.

OpenStack joue le rôle d'une couche de management de Cloud qui assure la communication entre la couche physique où se trouvent des serveurs physiques occupés par des hyperviseurs différents (VMware ESX, Citrix Xen, KVM, qemu...) et la couche applicative (Applications, utilisateurs, administrateurs...). Elle fournit une solution d'Infrastructure-as-a-Service (IaaS) à travers un éventail de services complémentaires. Chaque service offre une Application Programming Interface (API) qui facilite cette intégration. [W13]

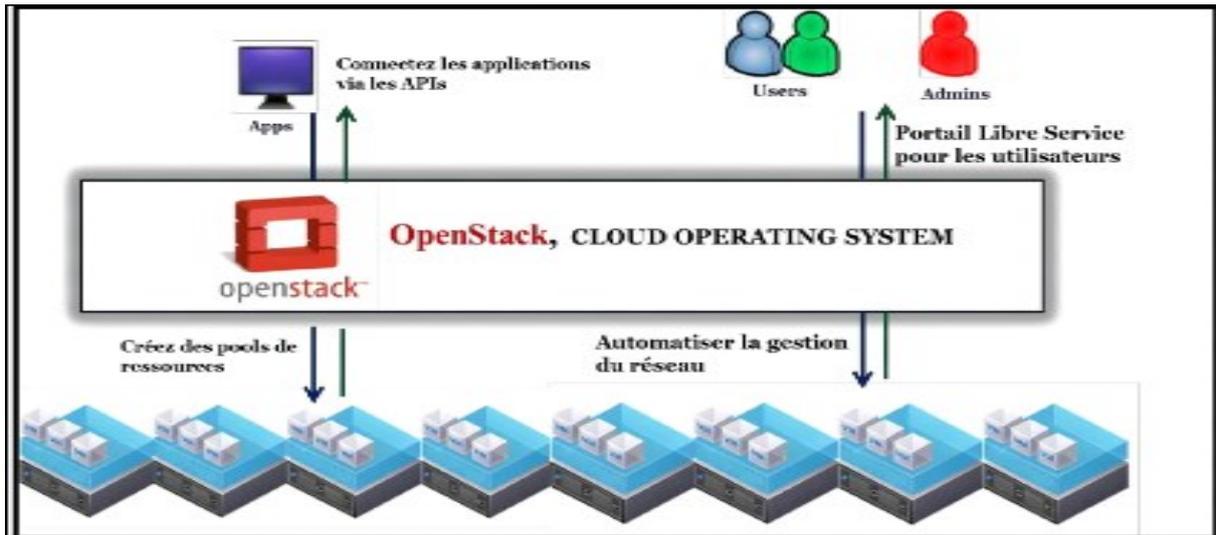


Figure 3.1: Le rôle d'OpenStack

OpenStack est développé et publié autour de cycles de 6 mois. Après la publication initiale, des versions de points stables supplémentaires seront publiées dans chaque série de versions. Vous pouvez trouver le détail des différentes versions comme indiqué dans le tableau ci-dessous:

Nom	Date	Composants inclus
Austin	21 octobre 2010	Nova, Swift
Bexar	3 février 2011	Nova, Glance, Swift
Cactus	15 avril 2011	Nova, Glance, Swift
Diablo	22 septembre 2011	Nova, Glance, Swift
Essex	5 avril 2012	Nova, Glance, Swift, Horizon, Keystone
Folsom	27 septembre 2012	Nova, Glance, Swift, Horizon, Keystone, Quantum, Cinder
Grizzly	4 avril 2013	Nova, Glance, Swift, Horizon, Keystone, Quantum, Cinder
Havana	22 octobre 2013	Nova, Glance, Swift, Horizon, Keystone, Neutron, Cinder, Heat, Ceilometer
Icehouse	17 avril 2014	Nova, Glance, Swift, Horizon, Keystone, Neutron, Cinder, Heat, Ceilometer, Trove
Jun0	16 Octobre 2014	Nova, Glance, Swift, Horizon, Keystone, Neutron, Cinder, Heat, Ceilometer, Trove, Sahara
Kilo	30 Avril 2015	Nova, Glance, Swift, Horizon, Keystone, Neutron, Cinder, Heat, Ceilometer, Trove, Sahara, Ironic

Tableau 3.1 : Les versions d'OpenStack

OpenStack est composé d'une série de logiciels et de projets au code source libre qui sont maintenus par la communauté incluant: OpenStack Compute (nommé Nova), OpenStack Object Storage (nommé Swift), OpenStack Image Service (nommé Glance)... .

3.3 Architecture d'OpenStack

Elle s'articule autour de ces services : [W10]

Services	Nom du projet	Description
Tableau de Bord	Horizon	Fournit un portail de self-service basé web qui sert aux interactions avec les services sous-jacents d'OpenStack, comme le lancement d'une instance, la distribution d'adresses IP ou la configuration des contrôles d'accès.
Compute	Nova	Gère le cycle de vie d'instances de compute dans un environnement OpenStack. Les responsabilités incluent la génération dynamique, la planification et la mise hors service de machines virtuelles à la demande.
Réseaux<http://www.openstack.org/software/releases/liberty/components/neutron>	Neutron	Permet Network-Connectivity-as-a-Service pour d'autres services d'OpenStack, comme Compute d'Openstack. Fournit une API pour que les utilisateurs puissent définir les réseaux et les pièces jointes dedans. Possède une architecture enfichable compatible pour la plupart des fournisseurs connus de réseaux et de technologies.
		Stockage
Object Storage	Swift	Stocke et récupère arbitrairement des objets data non structurés via une API RESTful basée sur HTTP. Le service est hautement tolérant aux pannes avec sa réplication de données et son architecture de type scale-out. Son implémentation diffère des serveurs de fichiers avec répertoires montables. Dans ce cas, le service écrit les objets et les fichiers vers plusieurs disques, en s'assurant que les données soient répliquées à travers le cluster de serveurs.
Stockage par Blocs	Cinder	Fournit un stockage de blocs persistants aux instances en cours d'exécution. Son architecture

Services	Nom du projet	Description
		de pilote enfichable facilite la création et la gestion des périphériques de stockage en blocs.
		Services partagés
Service d'identification	Keystone	Fournit un service d'authentification et d'autorisation pour les autres services d'OpenStack. Donne un catalogue de points de terminaison pour tous les services d'OpenStack.
Service d'Image	Glance	Stocke et récupère des images de disques de machines virtuelles. Compute d'Openstack en fait usage lors de la mise en service d'instances.
Télémetrie	Ceilometer	Surveille et mesure le nuage OpenStack pour la facturation, l'analyse comparative, l'évolutivité et les statistiques.
		Services de plus haut niveau
Orchestration	Heat	Orchestre de nombreuses applications de cloud composées en utilisant soit le format de template natif <i>HOT</i> ou le format Cloud Formation d'AWS, à travers soit une API REST native OpenStack ou soit par une API de Requête compatible avec Cloud Formation.

Tableau 3.2 : Services d'OpenStack

3.4 Installation d'OpenStack



Nous avons choisie l'installation à partir de DevStack qui est une compilation de scripts utilisés pour mettre en place rapidement un environnement OpenStack complet. DevStack est basé sur les dernières versions des modules OpenStack. Il est utilisé comme un environnement de développement et constitue la base des tests fonctionnels du projet OpenStack.



Figure 3.2 : l'installation à partir de DevStack

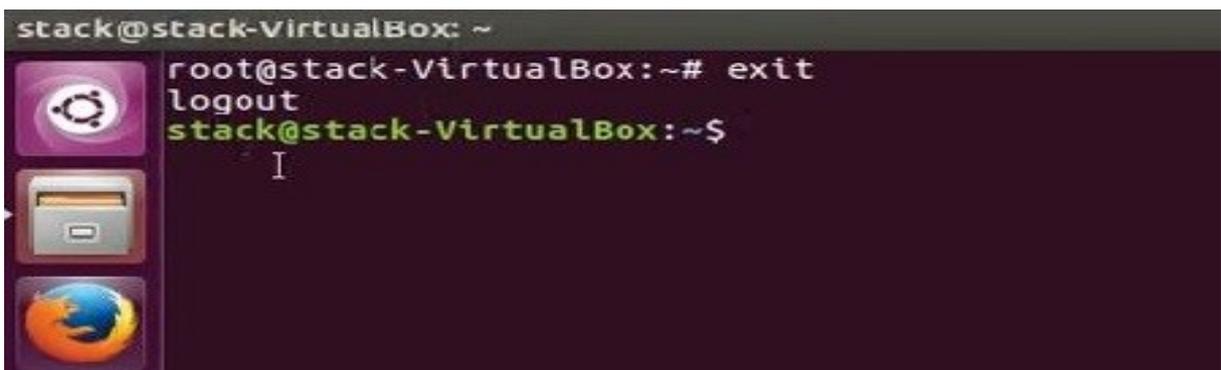
• Installation de Linux

Commencez avec une installation propre et minimale d'un système Linux. Devstack supporte Ubuntu 16.04 / 17.04, Fedora 24/25, CentOS / RHEL 7, ainsi que Debian et OpenSUSE.

Pour notre projet nous avons utilisé Ubuntu 16.04 qui le plus testé et le plus recommandé. Mais au préalable il nous faut un bon débit de connexion, une bonne configuration matérielle sur l'ordinateur 14 Go de RAM est le minimum recommandé ,100 Go d'espace disque, au moins, vituelbox pour pouvoir créer la machine virtuelle sous win10 qui tourne sur Ubuntu16.04 pour l'installation de DEVSTACK.

- **Prérequis du système**

1. Avant de commencer le processus d'installation, nous avons upgradé et mettre à jour votre système ;



```
stack@stack-VirtualBox: ~  
root@stack-VirtualBox:~# exit  
logout  
stack@stack-VirtualBox:~$  
I
```

```
stack@stack-VirtualBox: ~
stack@stack-VirtualBox:~$ sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:2 http://bd.archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [212 kB]
Get:4 http://bd.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [88.8 kB]
Get:6 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metadata [68.1 kB]
Get:7 http://bd.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:8 http://bd.archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main DEP-11 64x64 Icons [47.6 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [6,828 B]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/restricted Translation-en [2,272 B]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 DEP-11 Metadata [200 B]
Get:13 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [74.7 kB]
Get:14 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [42.1 kB]
Get:15 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 DEP-11 Metadata [32.1 kB]
Get:16 http://security.ubuntu.com/ubuntu xenial-security/universe DEP-11 64x64 Icons [37.0 kB]
Get:17 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [2,748 B]
Get:18 http://security.ubuntu.com/ubuntu xenial-security/multiverse Translation-en [1,232 B]
Get:19 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 DEP-11 Metadata [212 B]
Get:20 http://security.ubuntu.com/ubuntu xenial-security/multiverse DEP-11 64x64 Icons [29 B]
Get:21 http://bd.archive.ubuntu.com/ubuntu xenial/main Translation-en [568 kB]
Get:22 http://bd.archive.ubuntu.com/ubuntu xenial/main amd64 DEP-11 Metadata [733 kB]
Get:23 http://bd.archive.ubuntu.com/ubuntu xenial/main DEP-11 64x64 Icons [409 kB]
Get:24 http://bd.archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [8,344 B]
Get:25 http://bd.archive.ubuntu.com/ubuntu xenial/restricted Translation-en [2,908 B]
Get:26 http://bd.archive.ubuntu.com/ubuntu xenial/restricted amd64 DEP-11 Metadata [186 B]
Get:27 http://bd.archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
51% [27 Packages 1,450 kB/7,532 kB 19%]
```

Figure 3.3 : upgradé et mettre à jour votre système

2. créer un nouvel utilisateur et donner la permission de démarrer l'installation OpenStack

```
stack@stack-VirtualBox: ~
stack@stack-VirtualBox:~$ sudo -i
root@stack-VirtualBox:~# echo "stack ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
root@stack-VirtualBox:~# exit
logout
stack@stack-VirtualBox:~$
```

Figure 3.4 : création d'un user pour installation

3. téléchargez le devstack sur github.com

```

stack@stack-VirtualBox: ~
stack@stack-VirtualBox:~$ sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
git-man liberror-perl
Suggested packages:
git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb git-arch git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 336 not upgraded.
Need to get 3,760 kB of archives.
After this operation, 25.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://bd.archive.ubuntu.com/ubuntu xenial/main amd64 liberror-perl all 0.17-1.2 [19.6 kB]
Get:2 http://bd.archive.ubuntu.com/ubuntu xenial/main amd64 git-man all 1:2.7.4-0ubuntu1 [735 kB]
Get:3 http://bd.archive.ubuntu.com/ubuntu xenial/main amd64 git amd64 1:2.7.4-0ubuntu1 [3,006 kB]
Fetched 3,760 kB in 2min 16s (27.6 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 172622 files and directories currently installed.)
Preparing to unpack ../liberror-perl_0.17-1.2_all.deb ...
Unpacking liberror-perl (0.17-1.2) ...
Selecting previously unselected package git-man.
Preparing to unpack ../git-man_1%3a2.7.4-0ubuntu1_all.deb ...
Unpacking git-man (1:2.7.4-0ubuntu1) ...
Selecting previously unselected package git.
Preparing to unpack ../git_1%3a2.7.4-0ubuntu1_and64.deb ...
Unpacking git (1:2.7.4-0ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up liberror-perl (0.17-1.2) ...
Setting up git-man (1:2.7.4-0ubuntu1) ...
Setting up git (1:2.7.4-0ubuntu1) ...
stack@stack-VirtualBox:~$

```

```

stack@stack-VirtualBox:~$ git clone https://git.openstack.org/openstack-dev/devstack
Cloning into 'devstack'...
remote: Counting objects: 37199, done.
remote: Compressing objects: 100% (17979/17979), done.
remote: Total 37199 (delta 26443), reused 29036 (delta 18696)
Receiving objects: 100% (37199/37199), 7.53 MiB | 245.00 KiB/s, done.
Resolving deltas: 100% (26443/26443), done.
Checking connectivity... done.
stack@stack-VirtualBox:~$

```

Figure 3.5 : téléchargement le devstack

4. configure le fichier local.conf file

```

stack@stack-VirtualBox:~$ cd devstack
stack@stack-VirtualBox:~/devstack$ ls
clean.sh  exerciserc  extras.d  functions-common  HACKING.rst  LICENSE  openrc  run_tests.sh  setup.py  tests  unstack.sh
data     exercises  files    FUTURE.rst      inc         MAINTAINERS.rst  pkg     samples  stackrc  tools
doc      exercise.sh  functions  gate           lib         Makefile        README.md  setup.cfg  stack.sh  tox.ini
stack@stack-VirtualBox:~/devstack$ cd samples
stack@stack-VirtualBox:~/devstack/samples$ ls
local.conf  local.sh
stack@stack-VirtualBox:~/devstack/samples$ cp local.conf ../
stack@stack-VirtualBox:~/devstack/samples$ cd ..
stack@stack-VirtualBox:~/devstack$ ls
clean.sh  exerciserc  extras.d  functions-common  HACKING.rst  LICENSE  Makefile  README.md  setup.cfg  stack.sh  tox.ini
data     exercises  files    FUTURE.rst      inc         local.conf  openrc  run_tests.sh  setup.py  tests  unstack.sh
doc      exercise.sh  functions  gate           lib         MAINTAINERS.rst  pkg     samples  stackrc  tools
stack@stack-VirtualBox:~/devstack$

```

```

stack@stack-VirtualBox:~/devstack$ sudo nano local.conf

```

```

=====
DevStack Component Timing
=====
Total runtime          5366

run_process            71
test_with_retry        5
apt-get-update         27
pip_install            691
restart_apache_server  14
wait_for_service       23
git_timed              1942
apt-get                1571
=====

This is your host IP address: 192.168.1.1
This is your host IPv6 address: ::1
Horizon is now available at http://192.168.1.1/dashboard
Keystone is serving at http://192.168.1.1/identity/
The default users are: admin and demo
The password: p1

stack@stack-virtualBox: ~/devstack
GNU nano 2.5.3 File: local.conf

[[local|localrc]]

# Minimal Contents
# -----

# While ``stack.sh`` is happy to run without ``localrc``, devlife is better when
# there are a few minimal variables set:

# If the ``*_PASSWORD`` variables are not set here you will be prompted to enter
# values for them by ``stack.sh`` and they will be added to ``local.conf``.
ADMIN_PASSWORD=p1
DATABASE_PASSWORD=p1
RABBIT_PASSWORD=p1
SERVICE_PASSWORD=p1

HOST_IP=192.168.1.1
FLOATING_RANGE=192.168.1.224/27

# ``HOST_IP`` and ``HOST_IPV6`` should be set manually for best results if
# the NIC configuration of the host is unusual, i.e. ``eth1`` has the default
# route but ``eth0`` is the public interface. They are auto-detected in
# ``stack.sh`` but often is indeterminate on later runs due to the IP moving
# from an Ethernet interface to a bridge on the host. Setting it here also
# makes it available for ``openrc`` to include when setting ``OS_AUTH_URL``.
# Neither is set by default.
#HOST_IP=w.x.y.z
#HOST_IPV6=2001:db8::7

# Logging
# -----

```

Figure 3.6: configuration du fichier local.conf

5. maintenant vous pouvez commencer votre processus d'installation.

Figure 3.7: lancement de l'installation d'OpenStack

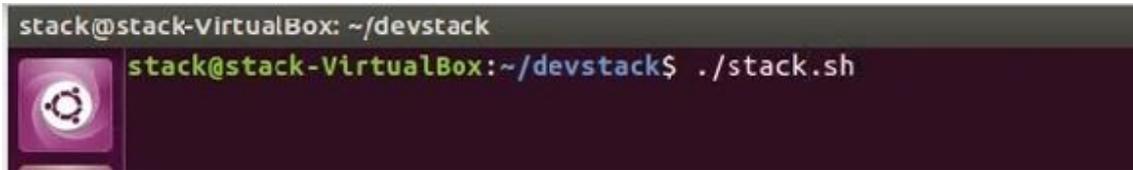


Figure 3.8: résumé et fin de l'installation

Maintenant nous pouvons accéder à l'interface d'administration OpenStack avec Horizon:

<https://192.168.1.1>

User : **admin**

Password: **p1**

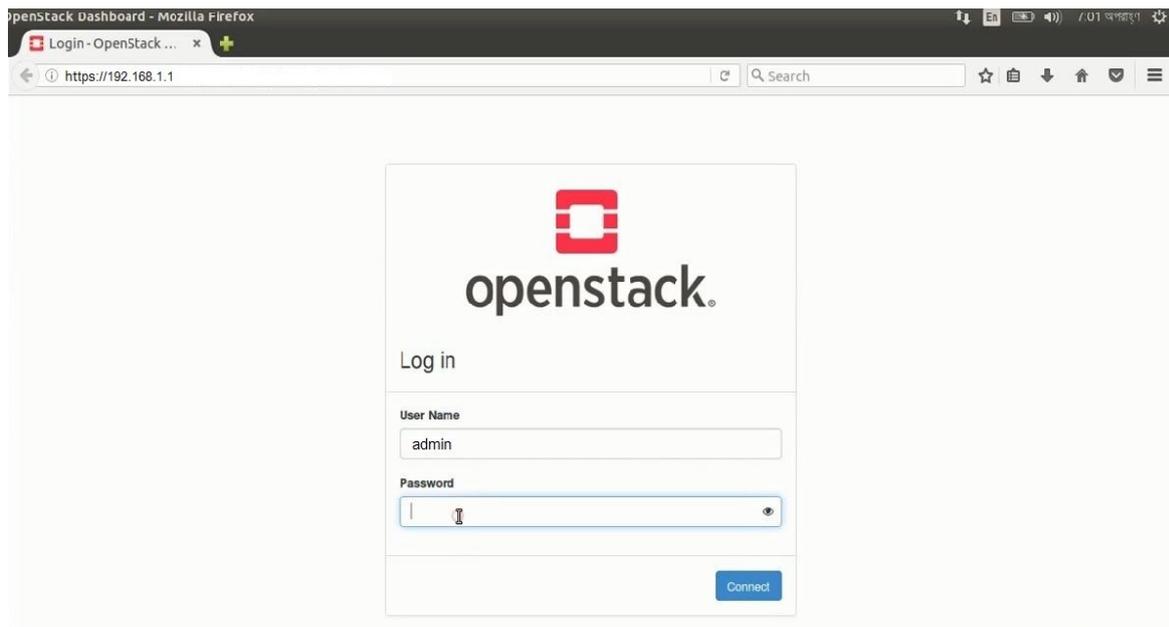


Figure 3.9: interface d'administration d'OpenStack Horizon

3.5 Création d'un espace Cloud

Après avoir accédé à l'interface d'administration d'OpenStack, on peut maintenant créer un projet qui contient les ressources (CPU, RAM, réseau et espace de stockage). On va créer aussi un compte utilisateur, qu'ils vont utiliser pour accéder à leur espace Cloud.

3.5.1. Création de projet et manipulation de quotas

Dans l'interface d'administration, on va créer un nouveau projet. Les deux figures ci-dessous montrent un aperçu de cette première étape:

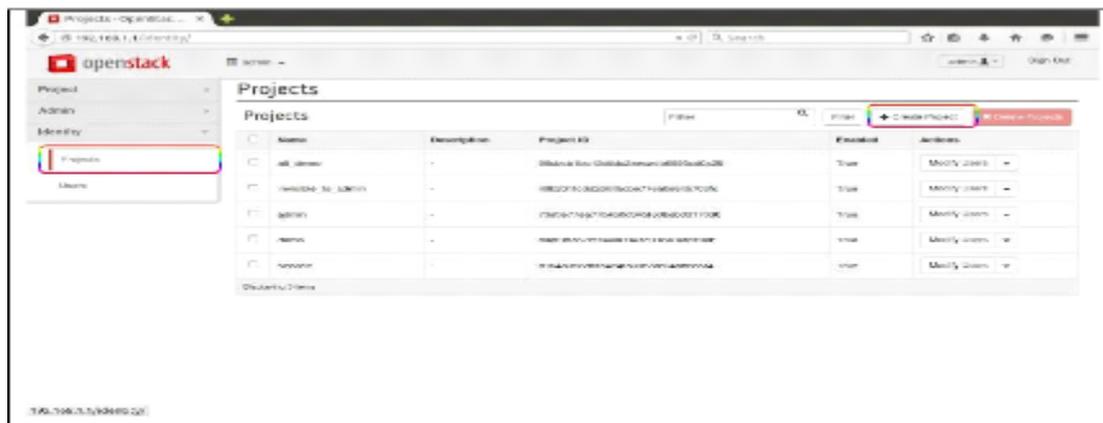


Figure 3.10: Création d'un projet. On remplit les champs comme montré:

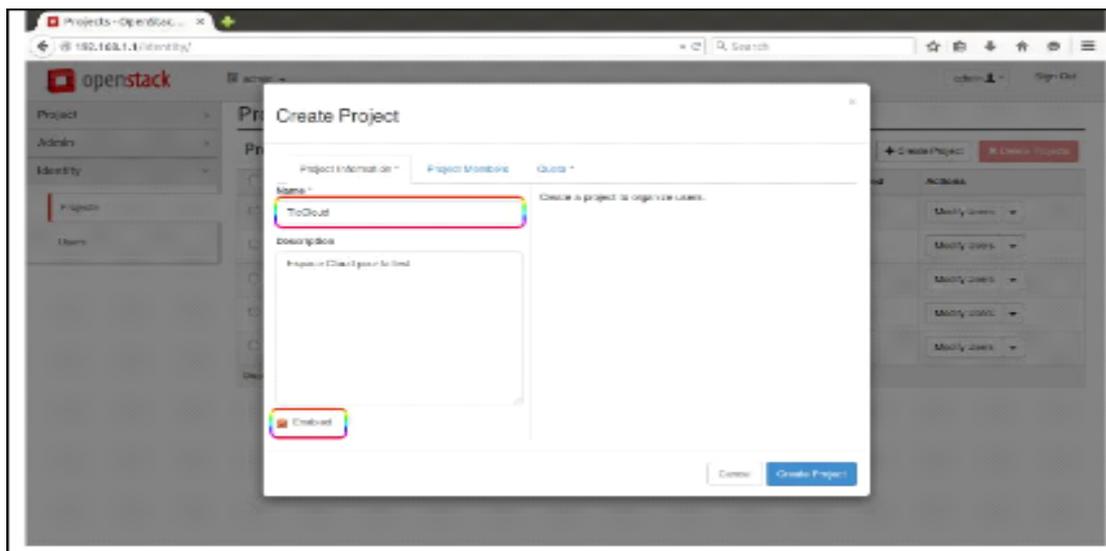


Figure 3.11: Informations nécessaires pour un projet.

L'onglet « Quota » nous permet de définir les ressources, comme montré dans la figure suivante puis on clique sur le bouton « Create Project » :

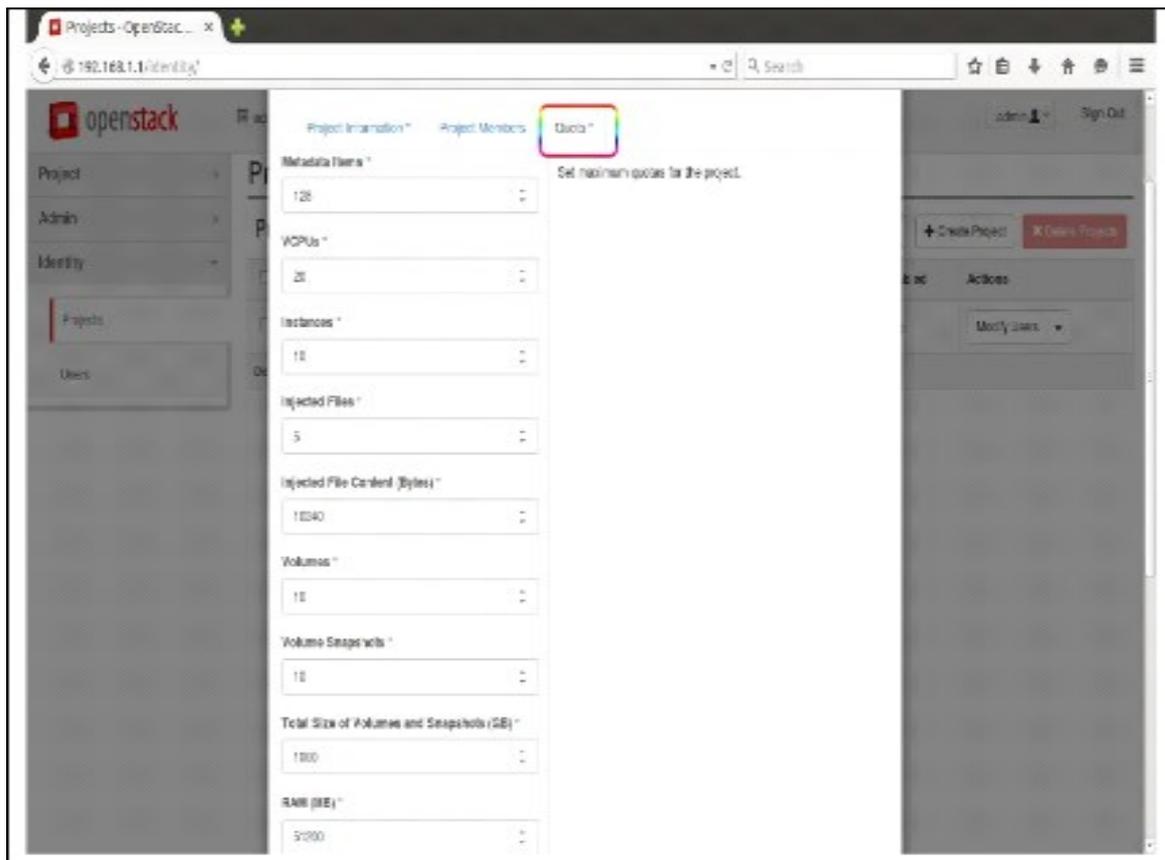


Figure 3.12: Ressources nécessaire pour le projet.

3.5.2. Création d'un utilisateur

On clique sur « User », puis sur « Create User » pour créer un utilisateur qui sera membre de ce projet, il peut exploiter et manipuler les ressources (quotas) qu'on lui a affecté seulement.

On remplit les champs comme montrés ci-dessous, puis on valide.

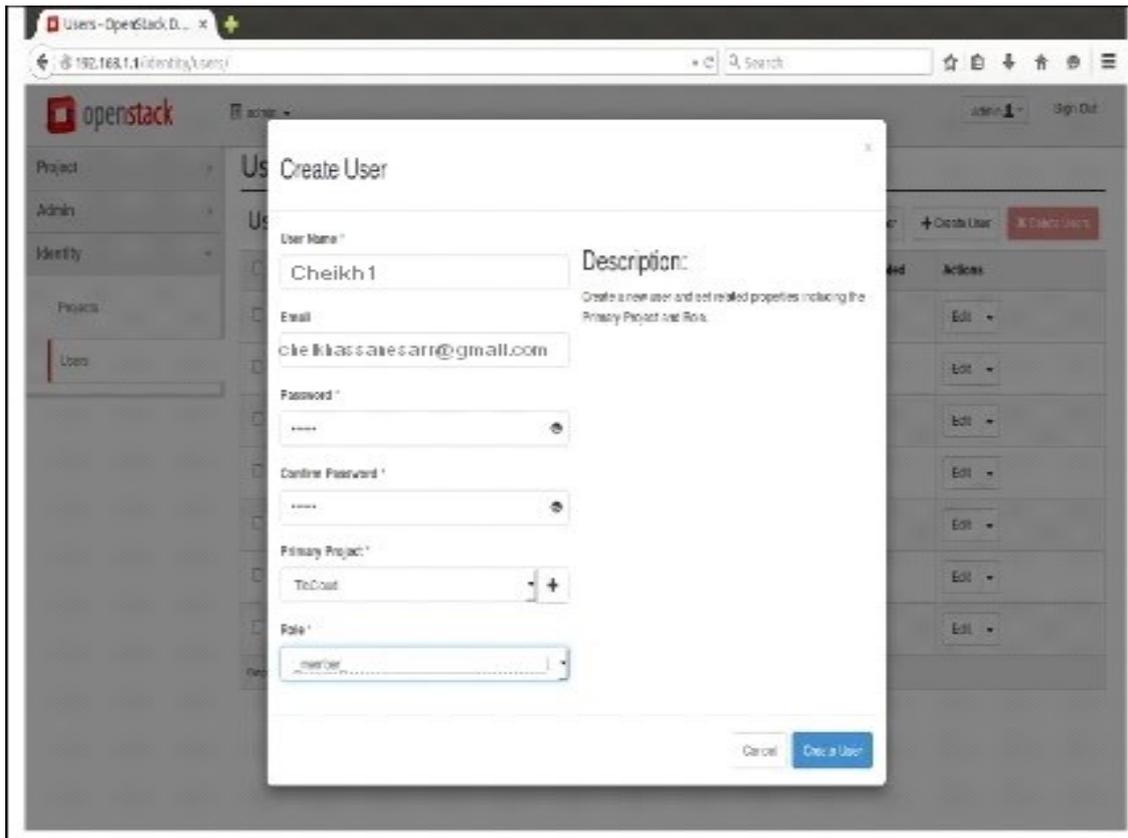


Figure 3.13: Création d'un utilisateur.

Maintenant pour accéder et exploiter les ressources affectées, on ferme la session admin, et on rentre avec l'utilisateur membre de ce projet. Dans la page d'accueil, on peut voir les ressources affectées, et leur taux d'utilisation. On peut aussi exploiter ces ressources.

La figure 3.14 représente la page d'accueil pour les utilisateurs de projet.

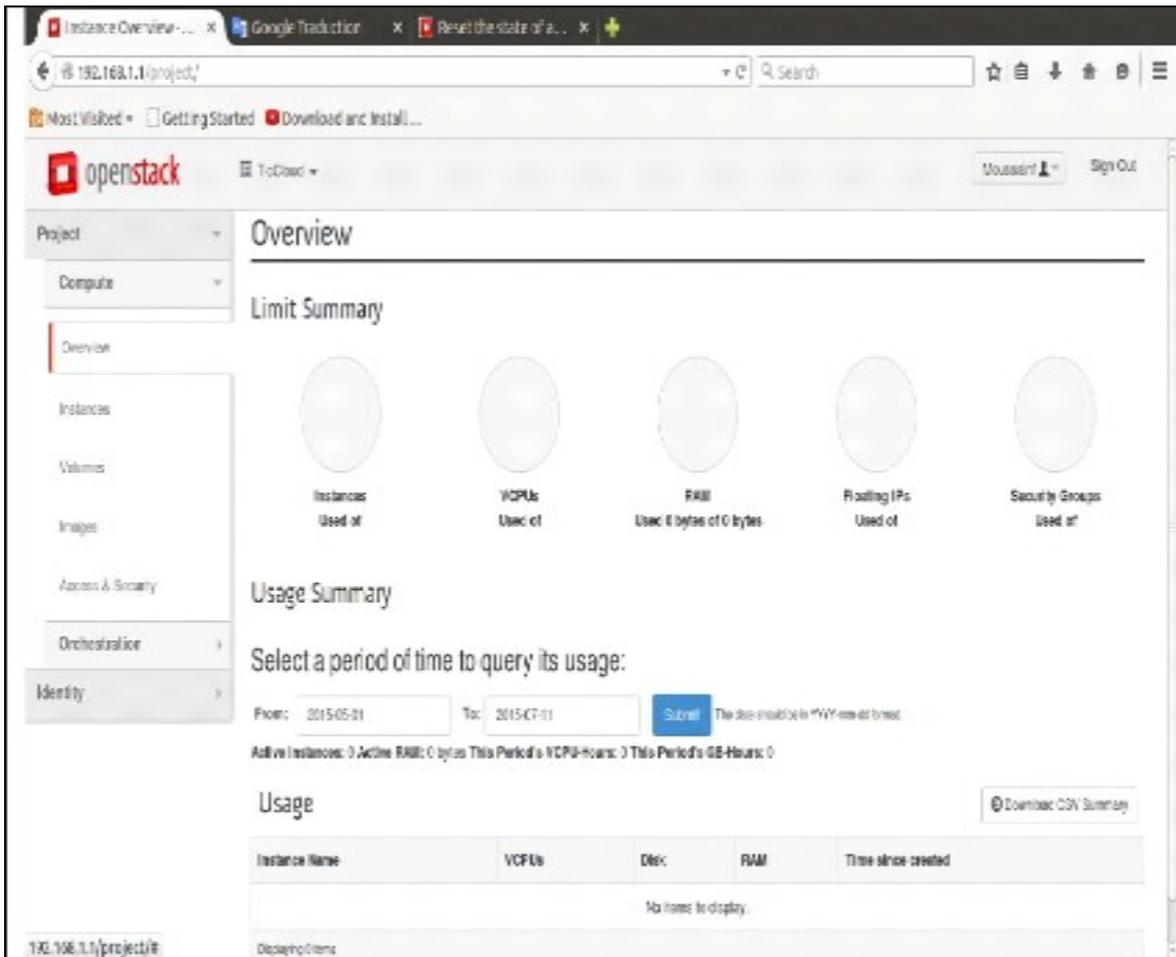


Figure 3.14: Page d'accueil pour les membres de projet.

3.5 Conclusion

Dans ce chapitre, on a présenté les outils logiciels et matériels ainsi que toutes les étapes et la démarche à suivre pour installer les différents composants d'OpenStack. Bien que l'installation semble facile à première vue, mais on a beaucoup cherché avant de la finaliser avec succès, car à chaque fois un problème survenait, qu'il fallait résoudre pour passer à l'étape suivante. En plus du fait que certaines informations ne sont pas évidentes à trouver, comme on a pu le constater. Nous avons choisie l'installation à partir de DevStack qui est une compilation de scripts utilisés pour mettre en place rapidement un environnement OpenStack complet. Qu'il est bon de connaître, pour mener à bien cette laborieuse installation et configuration.

CHAPITRE 4 : LA SECURITE DANS L'OPENSTACK

4.1 Introduction

Dans ce chapitre nous allons présenter une étude sur la sécurité dans l'OpenStack, et puis en a expliqué comment utilise les outils de l'analyse les vulnérabilités et les outils de l'attaque d'un Cloud.

4.2 Création d'un Groupe de sécurité

Les questions de sécurité, au sein d'OpenStack sont de la responsabilité du projet de sécurité. Le projet de sécurité est un effort horizontal au sein d'OpenStack qui est composé de ce qui était auparavant appelé le Groupe de sécurité OpenStack. L'équipe de gestion des vulnérabilités est également une partie du projet de sécurité.

Pour créer et configurer un groupe de sécurité on suit les étapes suivantes :

- Cliquez sur l'onglet Accès et Sécurité et sélectionnez Groupes de sécurité, et puis cliquez sur le bouton Créer groupe de sécurité ;

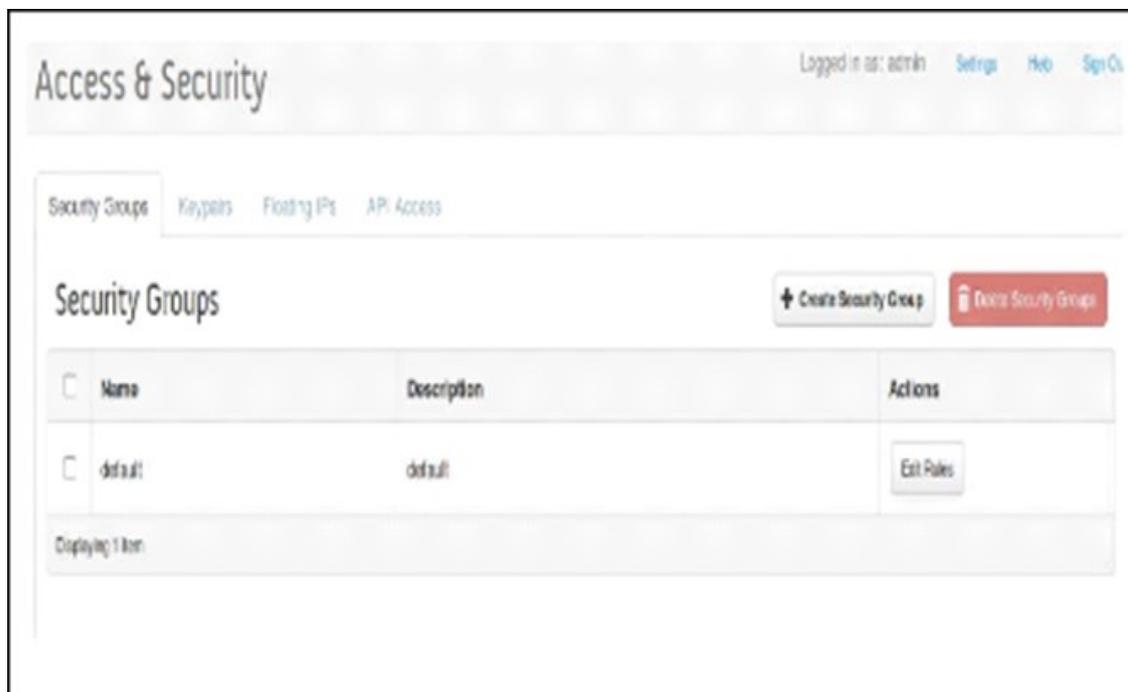
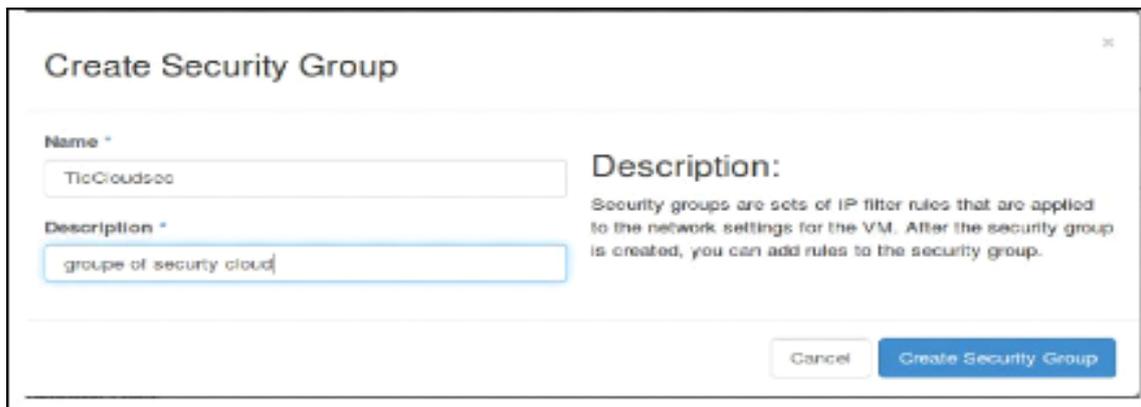


Figure 4.1: L'interface de la page Access & Security

- Entrez le nom de votre nouveau groupe de sécurité et de la description, Cliquez sur le bouton Créer groupe de sécurité ;



Create Security Group

Name *

TicCloudsec

Description *

groupe of security cloud

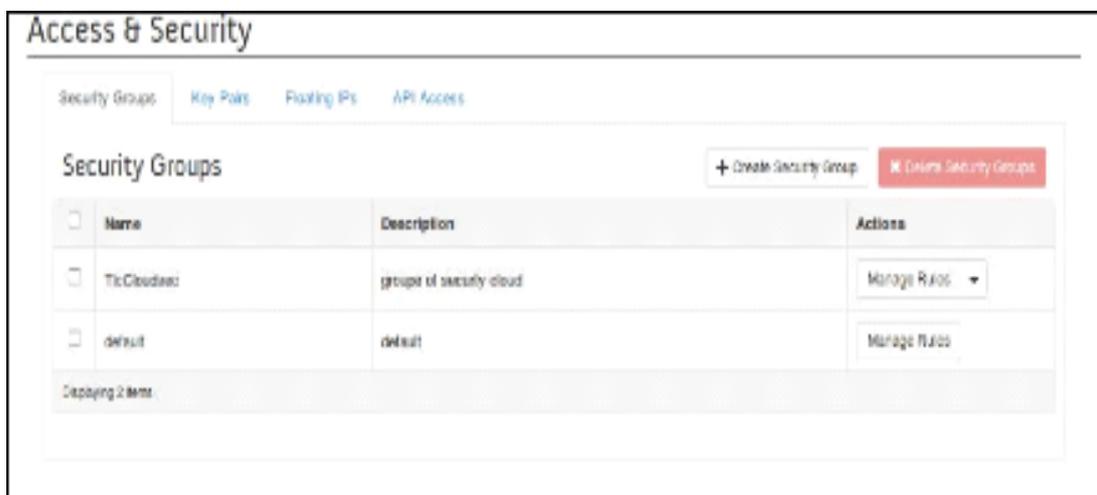
Description:

Security groups are sets of IP filter rules that are applied to the network settings for the VM. After the security group is created, you can add rules to the security group.

Cancel Create Security Group

Figure 4.2: L'interface de la fenêtre Create Security Groupe.

- Après cela, nous pouvons voir le nouveau groupe de sécurité dans la liste des groupes.



Access & Security

Security Groups Key Pairs Floating IPs API Access

Security Groups + Create Security Group - Delete Security Groups

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	TicCloudsec	groupe of security cloud	Manage Rules
<input type="checkbox"/>	default	default	Manage Rules

Deploying 2 VMs

Figure 4.3: La liste des groupes de sécurité.

4.2.1. La rédaction des règles d'un groupe

Appuyez sur le bouton Modifier les règles à côté du groupe de sécurité que vous souhaitez ajouter des règles / modifier. Nous allons utiliser le TicCloudsec Groupe de sécurité, d'abord ajouter une règle pour permettre les connexions SSH¹ entrantes sur le port 22.

Add Rule

Rule *
SSH

Remote *
Security Group

Security Group
TicCloudsec (current)

Description:
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:
Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.
Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.
Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

Figure 4.4: L'interface de la page pour ajouter des règles.

Maintenant, l'accès ssh est activé provenant de l'adresse IP spécifiée à toutes les machines virtuelles qui ont ce groupe de sécurité associé avec elles. La figure ci-dessous montre la liste de tous les règles qui sont ajoutées ;

Manage Security Group Rules: TicCloudsec

Security Group Rules + Add Rule X Delete Rules

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Ingress	-	ICMP	-1 (All ICMP)	TicCloudsec	Delete Rule
<input type="checkbox"/>	Ingress	-	TCP	1 - 65535	TicCloudsec	Delete Rule
<input type="checkbox"/>	Ingress	-	TCP	22 (SSH)	TicCloudsec	Delete Rule

Displaying 3 items

Figure 4.5: La liste des règles.

Ensuite, nous avons à générer une paire de clés qui seront utilisés pour authentifier les utilisateurs dans les machines virtuelles. Cliquez sur l'onglet "paires de clés" sur "l'accès et la sécurité" et cliquez sur "Créer une paire de clés" ;

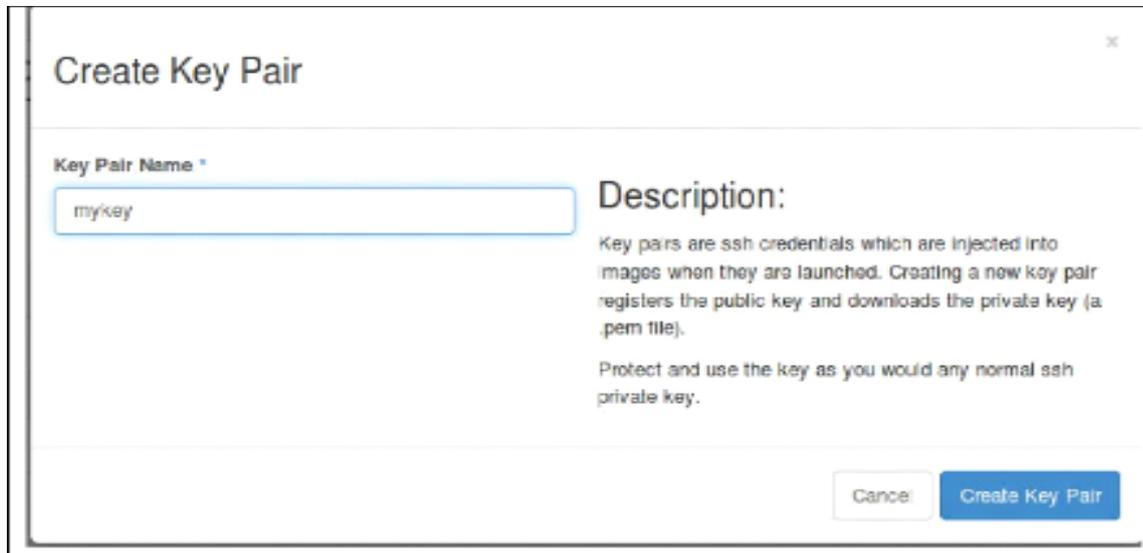


Figure 4.6: L'interface de création le pair de clés.

Téléchargez et enregistrez le fichier de clé. Il sera utilisé pour se connecter à des machines virtuelles à partir de l'extérieur.

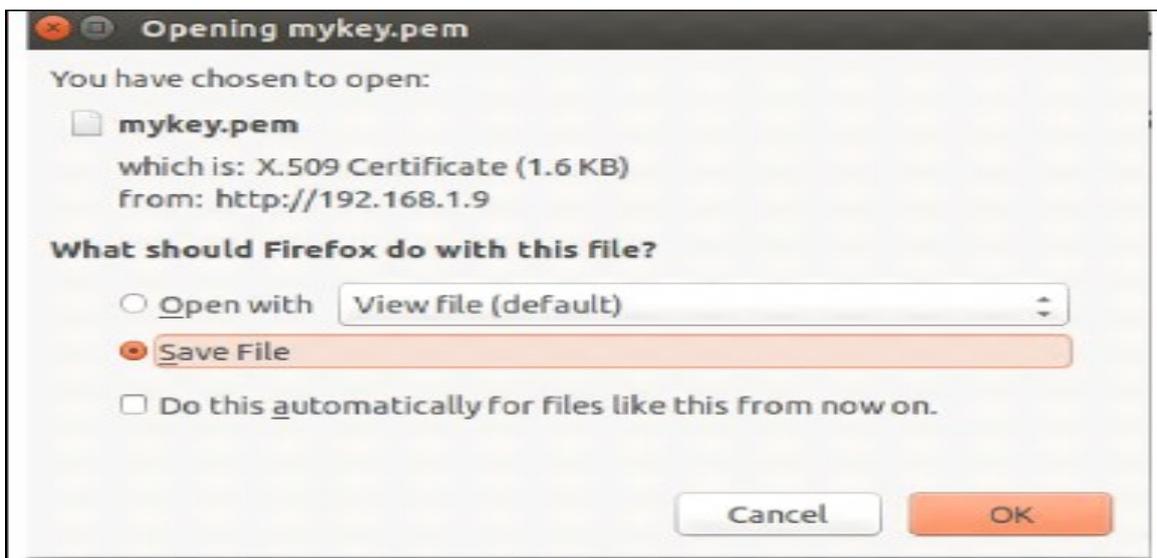


Figure 4.7: La fenêtre de téléchargement le fichier de clé.

4.2.2. La création des instances :

Une instance est une machine virtuelle qu'OpenStack dispose sur un nœud de calcul. Maintenant, nous pouvons créer une instance en utilisant le groupe de sécurité et la paire de clés que nous avons créés. Cliquez sur le lien "Instances" sous l'onglet "Project" et cliquez sur "Lancer instance" ;

Flavor Details	
Name	m1.nano
VCPUs	1
Root Disk	0 GB
Ephemeral Disk	0 GB
Total Disk	0 GB
RAM	64 MB

Project Limits
Number of Instances: 0 of 10 Used

Figure 4.8: L'interface de création des instances.

Dans l'interface utilisateur, vous pouvez configurer l'exemple en fournissant un nom, taille, etc.... sous l'onglet "Détails". Sous l'onglet "Accès et Sécurité" nous pouvons choisir la paire de clés et le groupe de sécurité que nous créons ci-dessus ;

Keypair
mykey

Confirm Admin Pass

Security Groups
 default

Figure 4.9: L'interface de l'ajout de la clé et du groupe.

Après avoir configuré l'instance, cliquez sur "Lancer". Puis attendre l'instance entre un état "Running" .

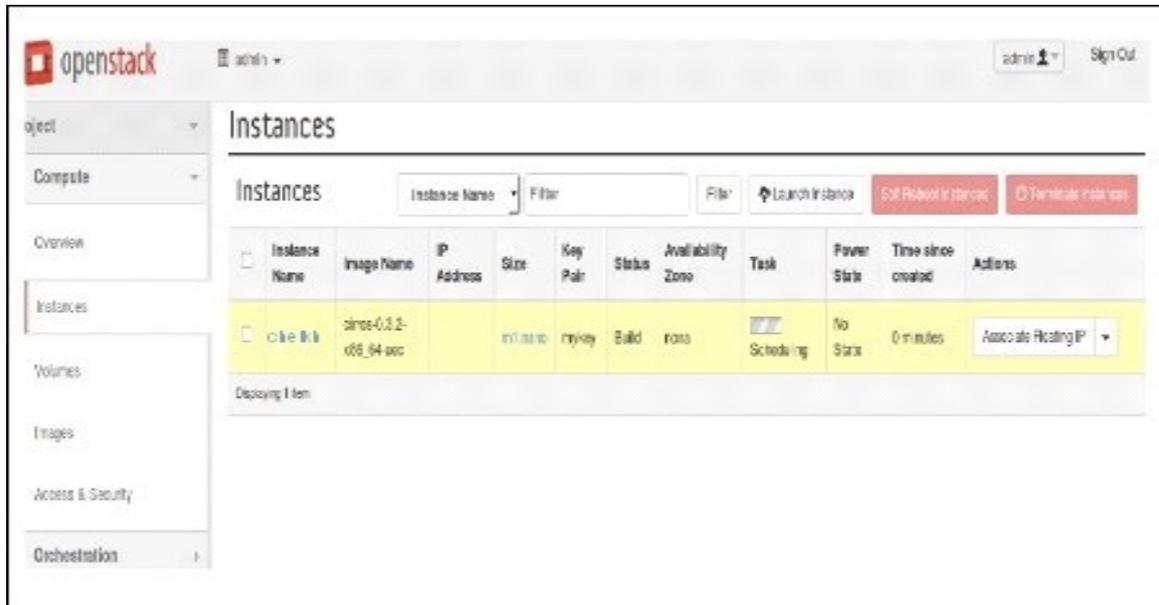


Figure 4.10: La liste des instances.

4.2.3. Une vue d'ensemble sur le système :

Dans la figure 4.11 une vue d'ensemble "overview" sur les ressources utilisées dans ce système.

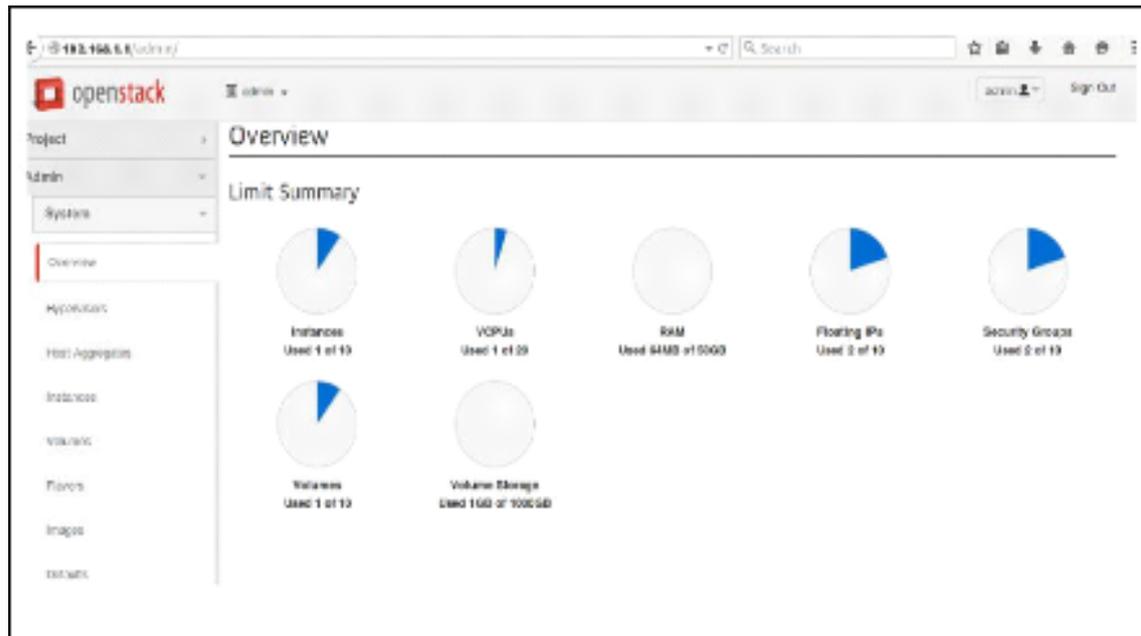


Figure 4.11: Une vue d'ensemble sur le système.

4.3 Les scanners des vulnérabilités

Un scanner de vulnérabilité est un programme conçu pour identifier des vulnérabilités dans une application, un système d'exploitation, ou un réseau Cloud.

Les scanners de vulnérabilité peuvent être utilisés dans des objectifs licites ou illicites :

- objectifs licites : les experts en sécurité informatique des entreprises utilisent les scanners de vulnérabilité pour trouver les failles de sécurité des systèmes informatiques et des systèmes de communications de leurs entreprises dans le but de les corriger avant que les pirates informatiques ne les exploitent.

- objectifs illicites : les pirates informatiques utilisent les mêmes équipements pour trouver les failles dans les systèmes des entreprises pour les exploiter à leur avantage. Il existe plusieurs programmes :

Nexpose un scanner de vulnérabilité de Rapid7 (propriétaire de Metasploit) ;

Nessus ;

OpenVAS un scanner de vulnérabilité libre ;

Snort un système de détection d'intrusion ;

Nmap un scanner de ports ;

Nous allons présenter une petite explication sur le meilleur scanneur dans ce chapitre (Nessus, Nmap).

4.3.1. Nessus

Nessus est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :

- Les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles (lecture de fichiers confidentiels par exemple), des dénis de service ;
- Les fautes de configuration (relais de messagerie ouvert par exemple) ;
- Les patchs de sécurité non appliqués, que les failles corrigées soient exploitables ou non dans la configuration testée ;
- Les mots de passe par défaut, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. Nessus peut aussi appeler le programme externe Hydra pour attaquer les mots de passe à l'aide d'un dictionnaire ;
- Les services jugés faibles (on suggère par exemple de remplacer Telnet par SSH) ;
- Les dénis de service contre la pile TCP/IP ;
- Scan les vulnérables des Cloud Computing ;

Pour utiliser Nessus suivre les étapes suivantes :

Une fois Nessus installé et tous les plugins installés, lancez cette commande via le terminal :

```
/etc/init.d/nessusd start
```

Nessus est maintenant lancé. Rendez-vous à l'adresse **http://127.0.0.1:8834** ou **http://votremachine:8834** pour vous connecter à Nessus. Laissez-le s'initialiser, puis vous serez redirigés vers la page de login où vous devrez vous identifier.

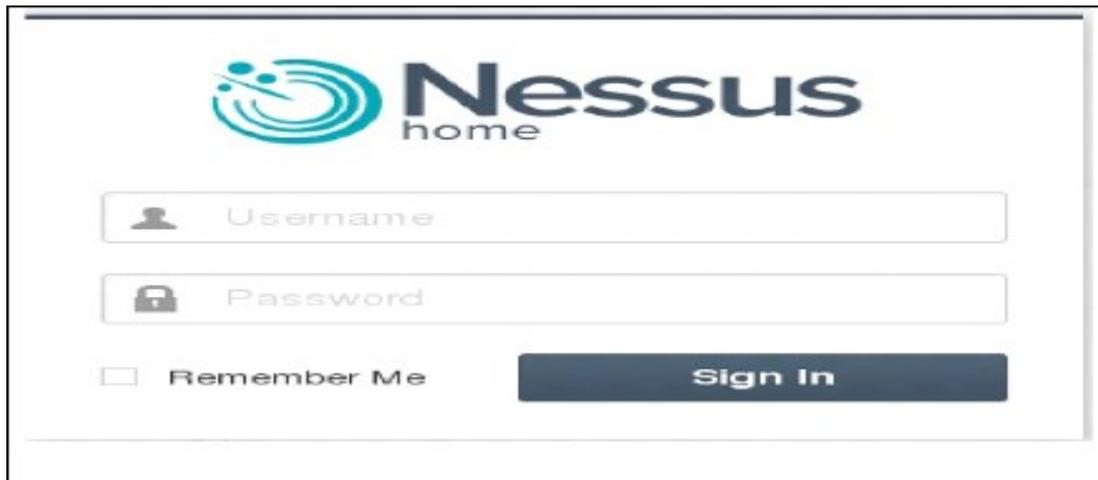


Figure 4.12: La page login sur Nessus.

Une fois identifié, vous serez amenés sur la page d'accueil, où il faudra en premier temps créer une nouvelle Policy. Cliquez sur le bouton en haut à gauche et cliquez sur Policy. et puis choisir le type de scan puis créez en une nouvelle avec les paramètres par défauts ;

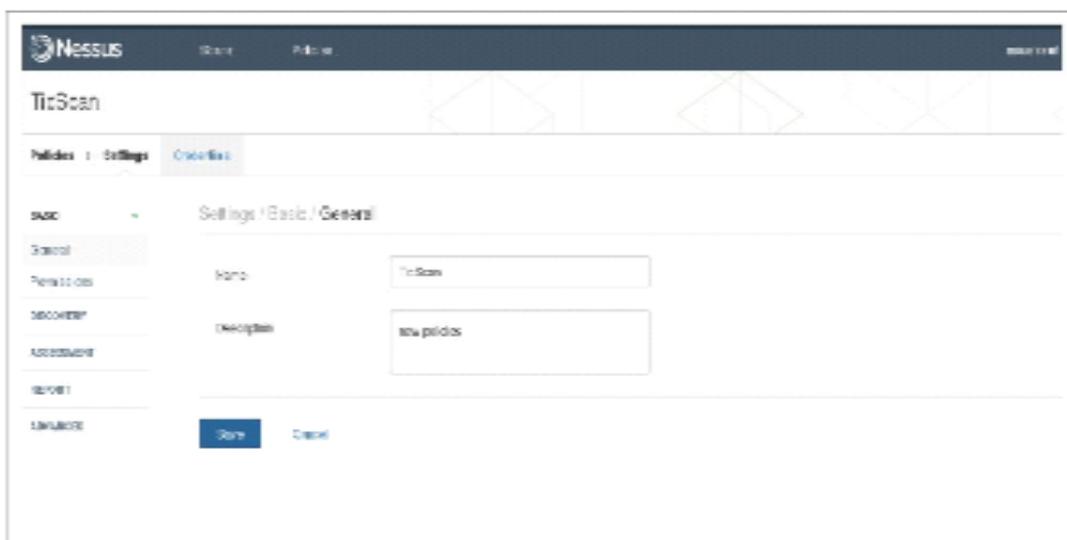
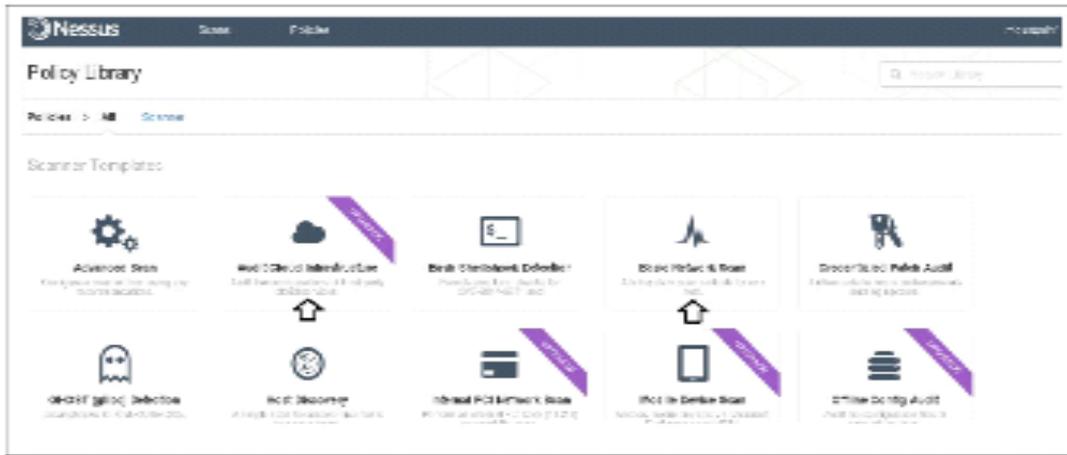


Figure 4.13: La page de la nouvelle Policy.

Figure 4.14: La configuration de Policy.

La description, la police (celle que nous avons créé tout à l'heure) et la liste des hôtes à scanner ;

Ici, mettez l'adresse IPv4 de la Target, pour nous ce sera 192.168.1.1 Le scan devrait se lancer. Attendez un moment, le temps que Nessus scan la machine(Cloud), puis une fois que Nessus vous indiquera que le scan est terminé, cliquez sur le scan pour afficher le résultat du scan.

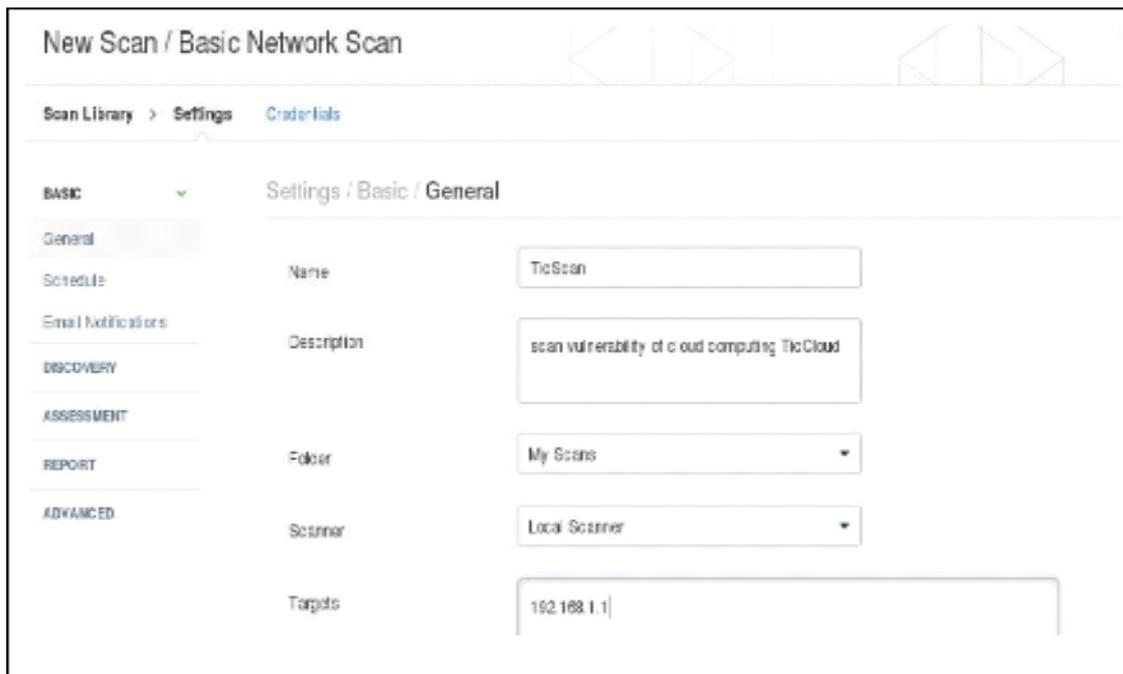


Figure 4.15: La configuration de scan.

4.3.2. Nmap

Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'une machine distante. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris. On utilise le Nmap parce que le OpenStack est installé sur une machine Virtual, donc La figure 4.15 montré le scan de Nmap :

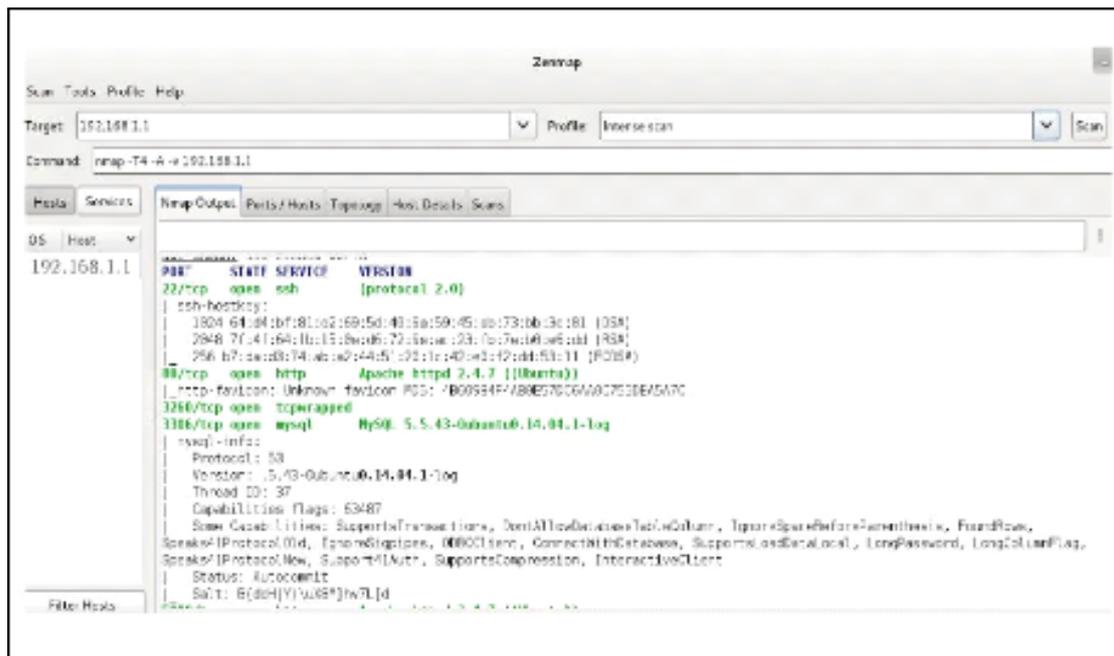


Figure 4.16: Nmap.

4.4 Les techniques d'attaque

Il existe deux types d'attaques :

- **Attaques passives** : elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues ;
- **Attaques actives** : elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critiques que les passives.

4.4.1. Foot printing

Le Footprinting est la technique consistant à récolter des informations sur des systèmes informatiques et toutes les entités auxquelles ils sont rattachés. Cela est effectué par le biais de plusieurs techniques, Dans le jargon de la sécurité informatique, le Footprinting se réfère généralement aux étapes précédant une attaque. Pour faire du Footprinting, nous allons utiliser :

- **Maltego** : est une application de l'intelligence de la source et la criminalistique ouverte. Il vous offrira une manière facile de la collecte des informations ainsi que la représentation de ces informations dans un format facile à comprendre. [14] Exemple qui nous présente sur le cloud [dropbox.com](https://www.dropbox.com), dans la figure 4.16.

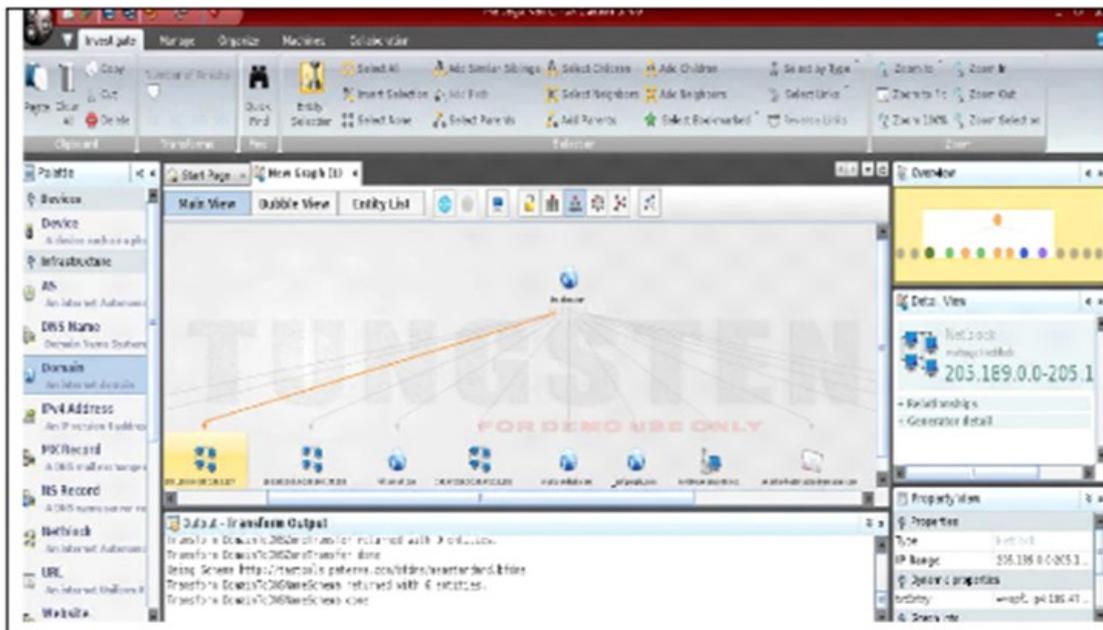


Figure 4.16 : Maltego Footprinting.

4.4.2. DOS Le déni de service

Les attaques par déni de service ont pour seul but d'empêcher le bon fonctionnement d'un cloud et non de récupérer des informations.

Exemple : Slowloris est un script écrit en Perl utilise une attaque de type DoS (attaque par déni de service), il affecte en particulier les serveurs Apache 1.x et 2.x qui représentent 67% des serveurs sur le net.

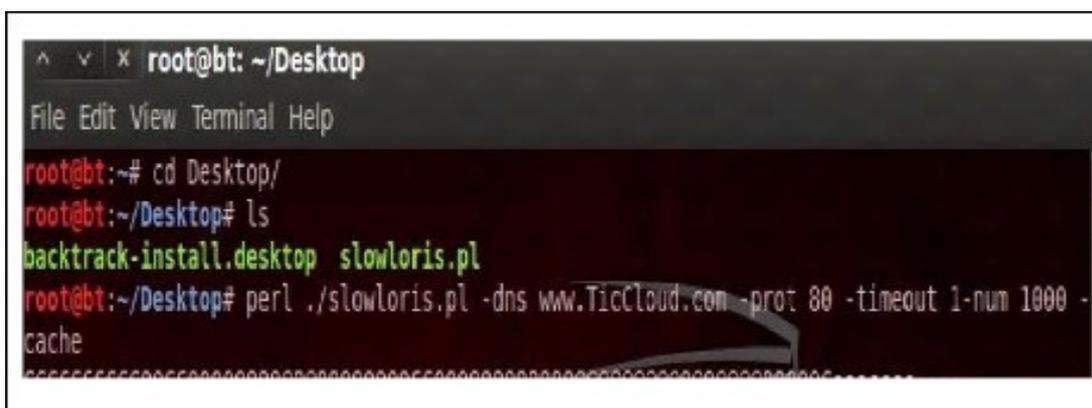


Figure 4.17 : Utilisation de Slowloris.

CONCLUSION GENERALE

Au cours de ce mémoire, nous avons fait une étude sur la sécurité d'un Cloud Computing, on a commencé par donner les définitions de base nécessaires à la compréhension du Cloud, son architecture et ses différents types (privée, public, hybride) et services (IaaS, PaaS, SaaS), et puis on a présenté et détaillé les différents mécanismes de gestion de sécurité d'un Cloud Computing. Le système qui on a utilisé dans cette projet qui s'appelle OpenStack, Nous avons fait par la suite l'installation et la configuration d'OpenStack qui a nécessité des prérequis matériels et logiciels. La configuration de notre solution a été réalisée sous le système d'exploitation Ubuntu 16.04 qui a été installé sur une machine virtuelle, le logiciel de virtualisation utilisé est Virtual Box. Le dernier point évoqué dans ce mémoire est un test de la sécurité de ce système 'OpenStack'. Nous avons été confronté à certains problèmes durant implantation du system de test : installation qui nécessite un bon débit, problème de mise à jour des paquets, problèmes de stockage.

En somme, et pour clore ce mémoire, nous espérons que les objectifs fixés au départ ont été en grande partie réalisés et que les résultats obtenus trouveront un bon écho. Ainsi plusieurs questions se posent

- Comment marche le cloud?
- Quels environnements sont proposés sur les plates-formes de Cloud Computing ?
- Quelle est la différence entre un Cloud privé et un Cloud public ?
- Comment choisir mon fournisseur de Cloud Computing ?
- Comment savoir si mes données sont sécurisées ?
- Le Cloud Computing est-il conforme à la législation sur la préservation des données ?

BIBLIOGRAPHIE

- L 1. *Fondamentaux du Cloud Computing* SYNTHÈSE Les travaux passés du CIGREF <https://www.slideshare.net/.../fondamentaux-du-cloud-computing>
- L 2. Vincent Kherbache, Mohamed Moussalih, Yannick Kuhn, Allan Lefort, *Cloud Computing*, Edition Eucalyptus, 2010. <https://members.loria.fr/lnussbaum/files/ptasrall2010-cloud-computing-rapport.pdf>
- L 3. Sosinsky, *Cloud Computing Bible*, Edition Wiley Publishing, 2011.
- L 4. George Reese, *Cloud Application Architectures*, Edition O'Reilly Media, 2009. <https://ameensheriffmca.files.wordpress.com/2014/07/text-book1.pdf>
- L 5. Damien Riquet, Gilles Grimaud et Michaël Hauspie, Étude de l'impact des attaques distribuées et multi-chemins sur les solutions de sécurité réseaux, 9ème Conférence Internationale Jeunes Chercheurs, Lille, France, Octobre 2012.
- L 6. Lee newcombe, *Securing Cloud Services*, Edition ITGP, 2012.
- L 7. Ronald L, Krutz et Russell dean vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Edition Wiley Publishing, 2010.
- L 8. Yanpei Chen, Vern Paxson et Randy H. Katz, *What's New About Cloud Computing Security*, Edition Université of California, 2010. <https://www.owasp.org/images/d/d1/Cloud-security.pdf>
- L 9. Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra et Diego Zamboni, « Cloud Security Is Not (Just) Virtualisation Security », Edition ACM, 2009.
- L 10. **Évaluation et analyse des mécanismes de sécurité des réseaux** réseaux dans les infrastructures virtuelles de cloud computing. Thibaut Probst. To cite this version: Thibaut Probst. Évaluation et analyse des *mécanismes de sécurité* des réseaux dans les infrastructures virtuelles de *cloud computing*. <https://tel.archives-ouvertes.fr/tel-01216609/document>
- L 11. Alain-B TCHANA, système d'administration autonome adaptable : application au Cloud, L'institut national polytechnique de Toulouse, 2011. <https://zxr.io/teaching/stonybrook/CSE509.2012.F/p97-christodorescu.pdf>
- L 12. L'état de l'art de la sécurité dans le Cloud Computing : Hassan EL ALLOUSSI, LAILA FETJAH, Abderrahim SEKKAKI Département Mathématique & Informatique

Securite dans le Cloud Computing.pdf

L 13. L'installation OpenStack

<https://fredericfaure.wordpress.com/2013/07/05/introduction-a-openstack-2-sur-2-installation-devstack-et-utilisation-via-console-web-horizon/>

file:///C:/Users/CHEIKH%20ASSANE%20SARR/Downloads/Documents/Etude et mise en place dune solution cloudcomputing privee pour une entreprise.pdf

L 14. La sécurité dans OpenStack

https://indico.in2p3.fr/event/12140/contributions/8164/attachments/6515/8079/OpenStack_Security.pdf

etude_et_mise_en_place_dune_solution_cloudcomputing_privee_pour_une_entreprise.pdf

WEBOGRAPHIE

- [W1] <https://csrc.nist.gov/publications/detail/sp/800-145/final>, visite le 02/12/2017.
- [W2] www.cisco.com , visite le 09/12/2017.
- [W3] www.cigref.fr/cigref_publications/RapportsContainer/Parus2010/Impact_du_Cloud_Computing_sur_la_DSI_2010_CIGREF.pdf , visite le 09/12/2017.
- [W4] azure.microsoft.com , visite le 15/01/2018.
- [W5] www.clusif.asso.fr , visite le 15/01/2018.
- [W6] https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_cloud visite le 18/01/2018
- [W7] www.cloudmagazine.fr , visite le 25/01/2018.
- [W8] www.securitecloud.com , visite le 25/01/2018.
- [W9] www.openstack.org , visite le 03/02/2018.
- [W10] <https://docs.openstack.org/liberty/fr/install-guide-rdo/overview.html> (03/02/2018)
- [W11] www.lucasvidelaine.wordpress.com/2018/02/05/installation-de-devstack , visite le 28/01/2018
- [W12] www.inzeCloud.fr , visite le 03/02/2018.
- [W13] www.techterms.com , visite le 03/02/2018.
- [W14] www.futura-sciences.com , visite le 03/02/2018.
- [W15] www.nessus.com , visite le 20/03/2018.
- [W16] www.Insecure.org , visite le 20/03/2018.
- [W17] www.paterva.com , visite le 20/03/2018.
- [W18] <https://cloud-computing.developpez.com/actu/97105/Quels-sont-les-risques-de-securite-majeurs-du-cloud-computing-Une-etude-du-CSA-en-revele-douze> visite le 01/04/2018

ANNEXES:

Lien du projet : <https://git.openstack.org/cgit/openstack-dev/devstack>

Sources et docs anglophones : <https://docs.openstack.org/developer/devstack/>

Attention : DevStack effectuera des modifications importantes sur votre système pendant l'installation. N'utilisez que DevStack sur des serveurs ou des machines virtuelles dédiés à cet effet.

Démarrage Rapide

Installation de Linux :

Commencez avec une installation propre et minimale d'un système Linux. Devstack supporte Ubuntu 16.04 / 17.04, Fedora 24/25, CentOS / RHEL 7, ainsi que Debian et OpenSUSE.

Si vous n'avez pas de préférence, Ubuntu 16.04 est le plus testé et le plus recommandé.

Pré-requis du système :

```
# Mettre à jour les dépôts
```

```
$ sudo apt-get --yes update
```

```
# Outils basiques utilisés par DevStack
```

```
$ sudo apt-get install --yes sudo vim vim-nox lynx zip binutils wget
```

```
$ sudo apt-get install --yes openssl ssl-cert ssh
```

```
# Installation de NTP
```

```
$ sudo apt-get install --yes ntp
```

```
    # Prérequis pour le script de DevStack
```

```
$ sudo apt-get install bridge-utils
```

```
$ sudo apt-get install --yes git
```

```
$ sudo apt-get install --yes python-pip
```

```
$ sudo pip install --upgrade pip
```

```
$ sudo pip install -U os-testr
```

Création de l'utilisateur :

DevStack doit être exécuté par un utilisateur non root mais ayant les permissions sudo.

Il faut donc créer un utilisateur, appelé ici « stack ».

```
$ sudo groupadd stack
```

```
$ sudo useradd -s /bin/bash -d /opt/stack -m stack
```

Comme l'utilisateur exécute DevStack et que ce dernier apporte des changements majeurs au système il faut le doter des permissions sudo. Exécuter ces commandes en tant que root pour plus de facilités.

```
$ cd /etc/sudoers.d
```

```
$ umask 226 && echo "stack ALL=(ALL) NOPASSWD:ALL" > /etc/sudoers.d/50_stack_sh
```

Téléchargement de DevStack :

Nous allons donc récupérer les fichiers de DevStack contenant le script d'installation.

```
$ su stack
```

```
$ cd
```

```
$ git clone https://git.openstack.org/openstack-dev/devstack
```

```
$ cd devstack
```

```
$ git checkout stable/ocata
```

Création du fichier de configuration local.conf :

Il va falloir créer dans le dossier devstack/ le fichier local.conf qui va contenir la configuration minimale pour pouvoir lancer le script.

```
[[local|localrc]]
```

```
ADMIN_PASSWORD=openstack
```

```
DATABASE_PASSWORD=openstack
```

```
RABBIT_PASSWORD=openstack
```

```
SERVICE_PASSWORD=openstack
```

```
GIT_BASE=https://git.openstack.org
```

Le fichier définira donc les mots de passe des différents modules de DevStack.

Si vous souhaitez installer des modules supplémentaires rajoutez à la suite du fichier local.conf :

```
enable_plugin heat https://git.openstack.org/openstack/heat stable/ocata
```

```
enable_plugin murano https://git.openstack.org/openstack/murano stable/ocata
```

Adaptez les modules en fonction de vos besoins.

Démarrage de l'installation :

Pour lancer l'installation il faut démarrer le script se trouvant dans le dossier devstack/

```
./stack.sh
```

Le script mets entre 15 et 20 minutes pour totalement installer DevStack, tout dépendra de la puissance de votre machine et de votre connexion internet puisque de nombreux fichiers et paquets seront installés pendant le processus.

Si une erreur ce produit, exécuter ce script et recommencez :

```
./clean.sh
```

Profitez !

Vous avez maintenant un environnement DevStack fonctionnel.

Normalement votre DevStack aura installé les modules Keystone, Nova, Cinder, Neutron et Horizon par lui-même.

Attention : Si vous arrêter votre machine il faudra recommencer ! DevStack ne prévoit de redémarrer...

Vous avez donc accès à Horizon depuis l'interface web afin de gérer vos instances, vos réseaux, vos volumes et vos images.

Évidemment vous pouvez également employer les commandes d'OpenStack depuis la console de votre serveur DevStack.

Puisque DevStack et OpenStack sont libre et communautaire vous pouvez exposer vos modifications au sein du code et les faire valider depuis [cette page](#).

Résumé

Cloud Computing nouveau modèle de technologie de l'information, il peut fournir à la fois l'infrastructure matérielle et logicielle ainsi que tous les services sont à la demande et via internet. Cependant, l'une des préoccupations importantes de ce service aujourd'hui est de garantir la sécurité de l'infrastructure du cloud. Le travail attendu dans Ce sujet porte sur **L'Étude de la vulnérabilité des données dans le cloud computing et gestion de la sécurité avec OpenStack**. OPENSTACK une solution open source. Le projet *OpenStack* est une plateforme de cloud computing open source qui supporte tous types d'environnements cloud. Le projet vise une implémentation simple, une scalabilité massive, et un ensemble varié de fonctionnalités notamment la sécurisation des VM (Virtual Machine) etc.

Mot clés : vulnérabilité, cloud computing, sécurité, OpenStack

Abstract

Cloud computing is the new model of IT department, it can provide both physical infrastructure and software as well as all services are on demand and via internet. However, one of the major concerns of this service today is to ensure the security of the cloud infrastructure. The expected work in this topic is a study on the security of cloud computing. The expected work in this topic is on the study of data **vulnerability in cloud computing and security management with OpenStack**. OPENSTACK an open source solution. The OpenStack project is an open source cloud computing platform that supports all types of cloud environments. The project aims at a simple implementation, a massive scalability, and a varied set of functionalities including VM security (Virtual Machine) etc.

Mot clés : vulnerability, cloud computing, security, OpenStack