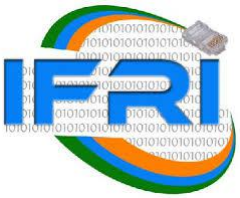


RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj



MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Darius Dorcalos Gbokanle **AFORA**

Etude et mise en place d'une solution cloud privé avec OpenStack

Sous la supervision de :
Mr AKPAKI **Marien**
(Consultant IT)
....

Membres du jury :

ASSOGBA Emery	Docteur	IFRI	Président
SAHO Nelson	Docteur	IFRI	Examinateur
AKPAKI Marien	Consultant IT	IFRI	Rapporteur

Année Académique : **2021-2022**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes 1

Introduction 2

1 Revue de littérature 4

2 Analyse et choix techniques 15

3 Mise en place, tests et résultats 31

Conclusion 42

Webographie 43

Table des matières 44

Dédicace

À mes chers parents, aucune dédicace ne peut exprimer mon amour, mon respect et mon souci pour vos sacrifices. Votre générosité et votre gentillesse ont toujours été mon modèle. Retrouvez les fruits de la patience et de la confiance que vous m'avez accordé dans ce travail.

A mes professeurs, à mes chers amis.

A tous ceux qui m'ont aidé de près ou de loin, je vous dédie ce travail.

Remerciements

Nous rendons grâce au tout puissant de nous avoir donné l'opportunité de réaliser ce modeste projet. Mes remerciements s'adressent aussi à toutes les personnes qui de près ou de loin ont contribué à la réalisation de ce mémoire.

Je tiens à remercier particulièrement :

- Le Professeur Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI) ;
- Mon encadreur Mr AKPAKI Marien (Consultant IT)
- Tous les enseignants de notre institut pour avoir accepté de partager avec dévouement une partie de leurs connaissances avec nous ;
- Ma famille pour tout le soutien qu'elle m'a apporté durant ces trois années de formation ;
- Mes proches et mes amis

Résumé

Avec le développement continu de la technologie dans le monde de l'informatique, les entreprises de divers domaines commencent à se tourner principalement vers la technologie de virtualisation et le cloud pour bénéficier des avantages offerts par cette dernière. De la même manière, nous rencontrons des clouds privés, dont l'implémentation dans les architectures d'entreprise se développe, même si leurs éditeurs existent depuis quelques années. Cet article présente un projet qui ajoute une plate-forme de cloud privé appelée openstack pour optimiser et maximiser l'utilisation des ressources tout en maintenant le contrôle et la gestion globale du réseau.

Mots clés : Virtualisation , Cloud privé , OpenStack , Open source ,VMware , Haute disponibilité.

Abstract

With the continuous development of technology in the world of IT, companies in various fields are beginning to turn mainly to virtualization technology and the cloud to benefit from the advantages offered by the latter. In the same way, we encounter private clouds, whose implementation in enterprise architectures is growing, even though their vendors have been around for a few years. This article presents a project that adds a private cloud platform called openstack to optimize and maximize the use of resources while maintaining control and overall management of the network

Key words : Virtualization, Private cloud, OpenStack, Open source, VMware, High availability.

Table des figures

1.1 Illustration du cloud . . . 5
1.2 Présentation cloud public . . . 7
1.3 Présentation du cloud privé . . . 8
1.4 Hyperviseur type 1 . . . 13
1.5 Hyperviseur type 2 . . . 14

2.1 Logo openstack . . . 23
2.2 Architecture conceptuel OpenStack . . . 26

3.1 Installation de microstack . . . 32
3.2 List microstack . . . 32
3.3 Microstack Init . . . 32
3.4 L'image par défaut . . . 33
3.5 Flavors liste . . . 33
3.6 Création de l'instance test . . . 33
3.7 HHorizon OpenStack . . . 34
3.8 Vue d'ensemble overview . . . 35
3.9 Paramètre OpenStack . . . 35
3.10 Création du rôle membre . . . 36
3.11 Création d'un utilisateur . . . 36
3.12 Création de sous réseau . . . 37
3.13 Création du Routeur1 . . . 37
3.14 Vue générale d'une partie du réseau . . . 38
3.15 Création d'un groupe de sécurité . . . 40

Liste des tableaux

2.1 Tableau compararif des solutions cloud opensource 22

Liste des acronymes

API : Application Programming Interface
AWS : Amazon web Services

DSI : Directeur du System d'Information

EC2 : Elastic Compute Cloud

HTML : HyperText Markup Language
HTTPS : HyperText Transfer Protocol Secure

IAAS : Infrastructure As A Service
IBM : International Business Machines
IoT : Internet of Things
IP : Internet Protocol
IT : Information Technologigy

KVM : Kernel-based Virtual Machine

MDGL : Ministère de la Décentralisation et de la Gouvernance Locale

OS : Operating System

PAAS : Platform as a Service

SAAS : Software as a service
SQL : Structured Query Language

VCPU : Virtual Central Processing Unit
VLAN : Virtual Local Area Network
VM : Virtual Machine

Introduction Générale

Contexte et justification

Au cours des dernières décennies, la société a connu une croissance technologique exponentielle, atteignant ce que nous appelons la révolution numérique. Cette vague a touché aussi bien le privé que le public dans tous les secteurs d'activité (santé, agriculture et éducation). Cette révolution numérique a augmenté le flux d'informations à traiter et la quantité de supports de stockage nécessaires. Les organisations gouvernementales ne font pas exception et sont confrontées aux défis uniques d'accomplir des tâches complexes avec des ressources limitées. Pour faire face à l'évolution des systèmes d'information en termes de ressources spatiales et de coûts, le cloud
computing se présente comme un candidat idéal. En effet, il offre la possibilité d'utiliser la puissance de calcul et la capacité de stockage fournies par des serveurs distants.
Le cloud computing est une technologie basée sur la virtualisation qui permet la mise en commun des ressources et l'utilisation des applications, les environnements de développement et de l'infrastructure matérielle en tant que services.
Certains fournisseurs open source comme openstack, opennebula et même d'autres propriétaires comme Amazon, Google Cloud, IBM Cloud, offrent des options très prometteuses pour résoudre plusieurs problèmes de longue date. Le but de notre travail est d'apporter la lumière sur le cloud computing , puis de choisir entre différents fournisseurs afin de proposer la meilleure solution disponible. C'est dans cette optique que notre sujet de recherche s'intitule "Étude et mise en place d'une solution cloud privé avec d'OpenStack ».

Problématique

Le Ministère de la Décentralisation et de la Gouvernance Locale est une institution qui prône l'efficacité dans tout son sens et détient des données vitales, pour la plupart confidentielles, qui circulent en ligne. Actuellement, ils disposent de plusieurs sites (C.M.S.I.C, CONAFIL, C.M.A.I, etc.) où les agents travaillent sur leur ordinateur personnel et stockent donc des données sur ce dernier .En cas de pannes leur données sont perdues. Dans le même temps quand l'administrateur dois installer une application il est obligé de parcourir tous les étages et de faire l'installations sur chaque poste utilisateur et ceux des autres sites se déplacent également pour avoir accès à ce dernier. Ce qui entraine une perte de temps et de productivité considérable. Il se pose alors ici deux problèmes :l'un

concernant la gestions des ressources de stockage et l'autre la gestion des pannes et incidents. La problématique de ce sujet consiste à tirer profit des avantages de la solution OpenStack, en minimisant les inconvénients pour assurer une infrastructure de production organisée, optimale et hautement disponible.

Objectifs

L'objectif Principale de notre projet est de présenter une étude et une mise en place d'une solution cloud privé avec OpenStack. Nous allons d'abord définir le cloud computing et OpenStack, puis nous allons analyser les avantages et les inconvénients de la mise en place d'une solution cloud privé avec OpenStack. Enfin, nous allons présenter les étapes à suivre pour mettre en place une solution cloud privé avec OpenStack.

Environnement de stage

0.1 Présentation du MDGL

0.1.1 Attributions et Organisation

Le Ministère de la Décentralisation et de la Gouvernance Locale a pour missions la définition, la mise en œuvre et le suivi-évaluation de la politique de l'État en matière de décentralisation, de déconcentration, de gouvernance locale et de développement à la base, conformément aux lois et aux règles en vigueur en République du Bénin et aux visions et politique de développement du Gouvernement.

A ce titre, il est chargé de :

- Coordonner la mise en œuvre de la réforme de l'administration territorial ;
- De mettre en œuvre la politique nationale de décentralisation et de déconcentration ;
- D'assurer l'administration des circonscriptions administratives et la tutelle des collectivités territoriales décentralisées ;
- De veiller à la qualité de la gouvernance dans la conduite des affaires locales ;
- De veiller à la qualité de l'offre des services publics locaux aux populations en collaboration avec les autres ministères.

Organisation du mémoire

Notre travail est structuré en trois chapitres. Le premier est consacré à une revue de littérature. Dans le second nous ferons des choix de solutions parmi les propositions après analyse. Le dernier chapitre est consacré à la mise en place des solutions, la présentation des tests effectués ainsi que les différentes perspectives d'amélioration de notre travail.

Chapitre 1

Revue de littérature

Introduction

Pour s'assurer que les entreprises ont non seulement un accès rapide aux informations, mais aussi l'intégrité de celles-ci, tout doit être fait avec une infrastructure adéquate et sécurisée. Ce chapitre définit certains concepts de base permettant d'établir l'état de l'art en matière de cloud computing et de virtualisation.

1.1 Présentation du cloud computing et des services

1.1.1 Le cloud computing

Il est assez complexe de donner une simple définition du cloud. Selon le NIST [10] , le cloud est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurable. Mais pour faire simple on peut dire que le cloud est une mise à disposition de plusieurs ressources (bases de données, fichier, application, stockage) informatiques sur demande avec une grande vitesse de réponse à travers un réseau étendu : Internet. Le cloud est composé de plusieurs caractéristiques et offres plusieurs services.

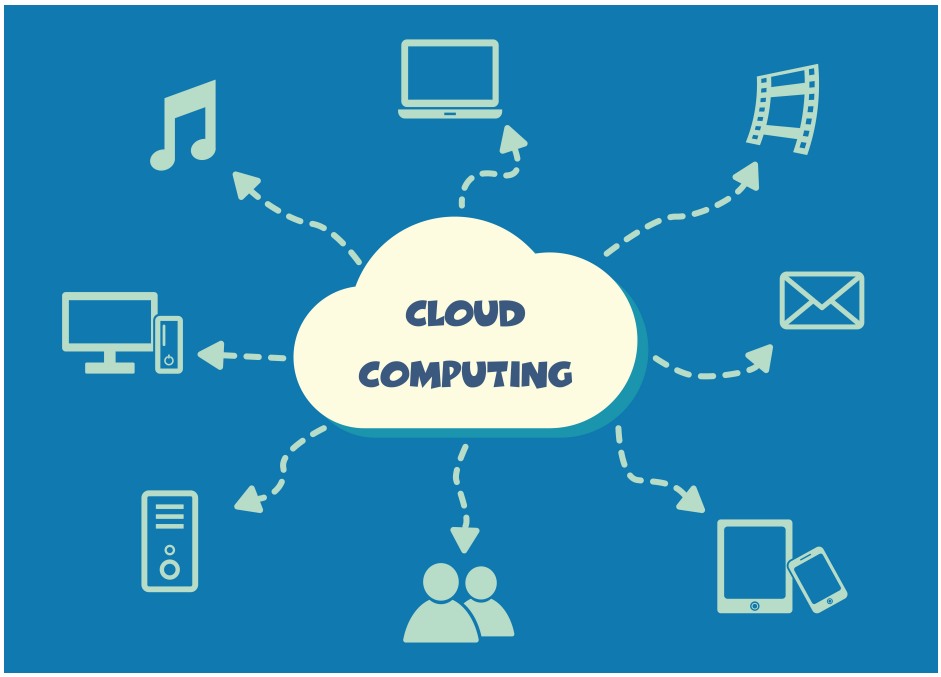


FIGURE 1.1 : Illustration du cloud

1.2 Avantages et inconvénients du cloud computing

Les solutions basées sur le cloud offrent de nombreux avantages. En fonction de votre entreprise et de vos besoins en matière de données, le passage à un environnement cloud peut présenter des avantages et des inconvénients :[1]

1.2.1 Les Avantages de l'utilisation du cloud

Comme nous le savons tous, le cloud computing est une technologie tendance. Une grande partie des entreprises ont déplacé leurs services vers le cloud pour la croissance de leurs activités. Ici, nous allons discuter de certains avantages importants du cloud computing.

- **Sauvegarde et restauration des données** Une fois les données stockées dans le cloud, il est plus facile d'obtenir une sauvegarde et de restaurer ces données.
- **Amélioration de la collaboration** Les applications cloud améliorent la collaboration en permettant à des groupes de personnes de partager rapidement et facilement des informations dans le cloud via un stockage partagé.
- **Excellente accessibilité** Le cloud nous permet d'accéder rapidement et facilement aux informations stockées n'importe quand, n'importe où dans le monde entier, en utilisant une connexion Internet. Une infrastructure cloud Internet augmente la productivité et l'efficacité de l'organisation en garantissant l'accessibilité des données.
- **Faible coût de maintenance** Le cloud computing réduit les coûts de maintenance matérielle et logicielle pour les organisations.

- **Services dans le modèle de paiement à l'utilisation** :Le cloud computing offre des interfaces de programmation d'applications (API) aux utilisateurs pour accéder à des services sur le cloud et le paiement des frais se fait en fonction de l'utilisation du service.
- **Capacité de stockage illimitée** Le cloud nous offre une énorme capacité de stockage pour stocker nos données importantes telles que des documents, des images, des l'audio, des vidéo, etc ... en un seul endroit.
- **Sécurité des données** La sécurité des données est l'un des plus grands avantages du cloud computing. Le cloud offre de nombreuses fonctionnalités avancées liées à la sécurité et garantit que les données sont stockées et traitées en toute sécurité.

1.3 Les inconvénients du cloud

Les inconvénients du cloud sont cités ci-dessous :

- **Connectivité Internet** Comme nous le savons, dans le cloud computing, toutes les données (image, audio, vidéo, etc.) sont stockées sur le cloud, et nous accédons à ces données via le cloud en utilisant la connexion Internet. Si vous ne disposez pas d'une bonne connectivité Internet, vous ne pouvez pas accéder à ces données. Cependant, nous n'avons aucun autre moyen d'accéder aux données à partir du cloud.
- **Verrouillage du fournisseur** Le verrouillage du fournisseur est le plus grand inconvénient du cloud computing. Les organisations peuvent rencontrer des problèmes lors du transfert de leurs services d'un fournisseur à un autre. Comme différents fournisseurs proposant des plates-formes différentes, cela peut entraîner des difficultés pour passer d'un cloud à un autre.
- **Contrôle limité** Comme nous le savons, l'infrastructure cloud est entièrement détenue, gérée et surveillée par le fournisseur de services, de sorte que les utilisateurs du cloud aient moins de contrôle sur la fonction et l'exécution des services au sein d'une infrastructure cloud.
- **Sécurité** Bien que les fournisseurs de services cloud mettent en œuvre les meilleures normes de sécurité pour stocker des informations importantes , nous savons que nous enverrons toutes les informations sensibles de notre organisation à un tiers, c'est-à-dire un fournisseur de services du cloud computing. Lors de l'envoi des données sur le cloud, il peut y avoir une chance que les informations de notre organisation soient interceptées par des pirates.

1.3.1 Les caractéristiques du cloud

D'après recherches, le cloud dispose de plusieurs caractéristiques majeures qui sont :

- **Agilité** :Le cloud fonctionne dans un environnement informatique distribué. Il partage les ressources entre les utilisateurs et fonctionne très rapidement.
- **Haute disponibilité et fiabilité** : La disponibilité des serveurs est élevée et plus fiable car les risques de défaillance de l'infrastructure sont minimes.
- **Haute évolutivité** : Le cloud offre un approvisionnement « à la demande » des ressources à grande échelle, sans avoir d'ingénieurs pour les pics de charge.

- **Multi-partage** :Avec l'aide du cloud computing, plusieurs utilisateurs et applications peuvent travailler plus efficacement avec des réductions de coûts en partageant une infrastructure commune.
- **Indépendance de l'appareil et de l'emplacement** :Le cloud computing permet aux utilisateurs d'accéder aux systèmes à l'aide d'un navigateur Web, quel que soit leur emplacement ou l'appareil qu'ils utilisent, par exemple un PC, un téléphone mobile, etc. Comme l'infrastructure est hors site (généralement fournie par un tiers) et accessible via Internet, les utilisateurs peuvent se connecter de n'importe où.
- **Entretien** :La maintenance des applications de cloud computing est plus facile, car elles n'ont pas besoin d'être installées sur l'ordinateur de chaque utilisateur et sont accessibles à partir de différents endroits.
- **Coût réduit** : En utilisant le cloud computing, le coût sera réduit car la charge matérielle de l'entreprise ainsi allégée, les dépenses liées aussi.

Services en mode de paiement à l'utilisation :Les interfaces de programmation d'applications (API) sont fournies aux utilisateurs afin qu'ils puissent accéder aux services sur le cloud en utilisant ces API et payer les frais en fonction de l'utilisation des services.

1.3.2 Les types de déploiement du cloud

Nous pouvons déployer les 3 types de cloud suivants en fonction des besoins des organisations [9] :

1.3.2.1 Le Cloud public

Le cloud public est ouvert à tous pour stocker et accéder à des informations via Internet en utilisant la méthode de paiement à l'utilisation.

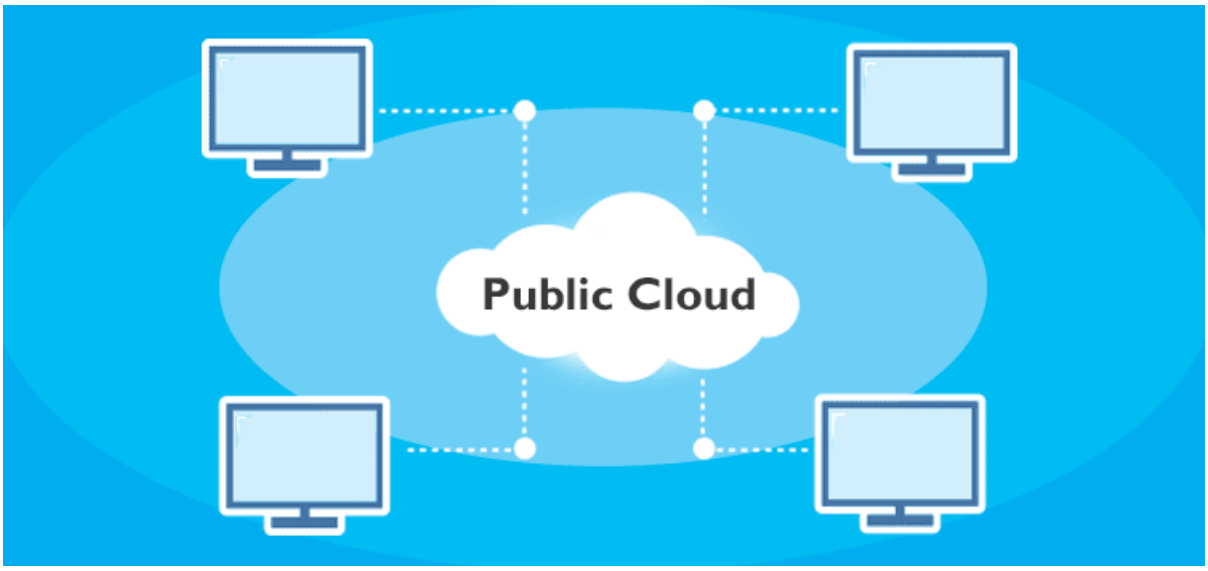


FIGURE 1.2 : Présentation cloud public

Dans le cloud public, les ressources informatiques sont gérées et exploitées par le fournisseur de services cloud (CSP).

Exemple :Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.

Avantages du Cloud Public

- Le cloud public est détenu à un coût inférieur à celui du cloud privé et hybride.
- Le cloud public est maintenu par le fournisseur de services cloud, vous n'avez donc pas à vous soucier de la maintenance.
- Le cloud public est plus facile à intégrer. Par conséquent, il offre une meilleure approche de flexibilité aux consommateurs.
- Le cloud public est indépendant de l'emplacement car ses services sont fournis via Internet.
- Le cloud public est hautement évolutif selon les besoins en ressources informatiques.
- Il est accessible au grand public, il n'y a donc pas de limite au nombre d'utilisateurs.

Inconvénients du Cloud Public

- Le Cloud public est moins sécurisé car les ressources sont partagées publiquement.
- Les performances dépendent de la liaison réseau Internet haut débit vers le fournisseur de cloud.
- Le Client n'a aucun contrôle sur les données.

1.3.2.2 Le Cloud privé

Un cloud privé fournit des services informatiques à des réseaux internes privés (au sein d'une organisation) et à des utilisateurs sélectionnés, plutôt qu'au public. Les clouds privés offrent des niveaux élevés de sécurité et de confidentialité des données grâce à des pare-feu et à un hébergement interne.

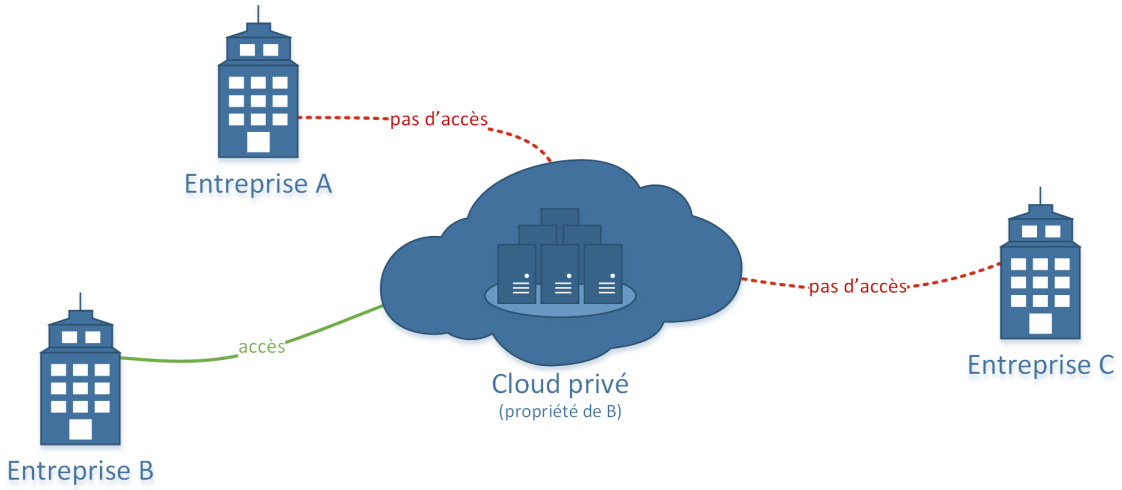


FIGURE 1.3 : Présentation du cloud privé

Il garantit également que les données opérationnelles et sensibles ne sont pas accessibles à des fournisseurs tiers.

Exemple : HP Data Centers, Microsoft, Elastra-private cloud et Ubuntu sont l'exemple d'un cloud privé.

Avantages du Cloud Privé

- Les clouds privés ont plus de contrôle sur leurs ressources et leur matériel que les clouds publics, car ils ne sont accessibles qu'à des utilisateurs sélectionnés.
- La sécurité et la confidentialité sont l'un des grands avantages du cloud computing. Le cloud privé a amélioré le niveau de sécurité par rapport au cloud public.
- Le cloud privé offre de meilleures performances avec une vitesse et une capacité d'espace améliorées.

Inconvénients du Cloud Privé

- Coût élevé Le coût est plus élevé qu'un cloud public car la configuration et la maintenance des ressources matérielles sont coûteuses.
- Zone d'opérations restreinte Comme nous le savons, le cloud privé est accessible au sein de l'organisation, de sorte que la zone d'opérations est limitée.
- Évolutivité limitée Les clouds privés ne sont mis à l'échelle que dans la limite de la capacité des ressources hébergées internes.
- Personnes qualifiées Des personnes qualifiées sont nécessaires pour gérer et exploiter les services cloud.

1.3.2.3 Le Cloud hybride

Le cloud hybride est une combinaison de clouds publics et privés. Cloud hybride = cloud public + cloud privé . L'objectif principal de la combinaison de ces clouds (publics et privés) est de créer un environnement informatique unifié, automatisé et bien géré. Dans le cloud hybride, les activités non critiques sont effectuées par le cloud public et les activités critiques sont effectuées par le cloud privé. Principalement, un cloud hybride est utilisé dans la finance, la santé et les universités.

Les meilleures sociétés de fournisseurs de cloud hybride sont
Exemple : Amazon, Microsoft, Google, Cisco et NetApp

Avantages du Cloud Hybride

- Il fournit des ressources flexibles en raison du cloud public et des ressources sécurisées en raison du cloud privé.
- Il offre les fonctionnalités du cloud public et privé. Un cloud hybride est capable de s'adapter aux exigences dont chaque entreprise a besoin en espace, en mémoire et en système.
- Le cloud hybride est sécurisé car les activités critiques sont effectuées par le cloud privé.
- Le cloud hybride offre aux entreprises un excellent moyen de gérer le risque.

Inconvénients du Cloud Hybride

- Dans le Cloud hybride, la mise en réseau devient complexe en raison du cloud privé et du cloud public.

- La compatibilité de l'infrastructure est le problème majeur dans un cloud hybride. Avec deux niveaux d'infrastructure, un cloud privé contrôle l'entreprise et pas un cloud public, il est donc possible qu'ils s'exécutent dans des piles séparées.
- La fiabilité des services dépend des fournisseurs de services cloud.

1.4 Quelques services du Cloud

Il existe les trois types de modèles de services cloud [5]

1.4.1 Le IAAS

Le IAAS ou (Infrastruture AS A Service) Infrastructure en tant que service représente la couche technique prise en charge par le fournisseur du cloud. Iaas est également connu sous le nom de Hardware as a Service (HaaS). C'est l'une des couches de la plate-forme de cloud computing. Il permet aux clients d'externaliser leurs infrastructures informatiques telles que ;les serveurs, la mise en réseau, le traitement, le stockage, les machines virtuelles et d'autres ressources. Les clients accèdent à ces ressources sur Internet à l'aide d'un modèle de paiement à l'utilisation.

L'IaaS est proposé en trois modèles : cloud public, privé et hybride. Le cloud privé implique que l'infrastructure réside chez le client. Dans le cas du cloud public, il est situé dans le centre de données du fournisseur de la plate-forme de cloud computing, et le cloud hybride est une combinaison des deux dans laquelle le client sélectionne le meilleur du cloud public ou du cloud privé.

Le fournisseur IAAS fournit les services suivants

- **Calculer** : L'informatique en tant que service comprend des unités de traitement centrales virtuelles et une mémoire principale virtuelle pour les machines virtuelles qui est provisionnée pour les utilisateurs finaux.
- **Stockage** : Le fournisseur IaaS fournit un stockage back-end pour le stockage des fichiers.
- **Réseau** :Le réseau en tant que service (NaaS) fournit des composants réseau tels que des routeurs, des commutateurs et des ponts pour les machines virtuelles.
- **Équilibreurs de charge** : Il fournit une capacité d'équilibrage de charge au niveau de la couche d'infrastructure.

1.4.2 Le PAAS

La plate-forme en tant que service (PaaS) fournit un environnement d'exécution. Il permet aux programmeurs de créer, tester, exécuter et déployer facilement des applications Web. Vous pouvez acheter ces applications auprès d'un fournisseur de services cloud sur une base de paiement à l'utilisation et y accéder à l'aide de la connexion Internet. Dans le PaaS, l'évolutivité back-end est gérée par le fournisseur de services cloud, de sorte que les utilisateurs finaux n'ont pas à se soucier de la gestion de l'infrastructure.

Le PaaS comprend une infrastructure (serveurs, stockage et mise en réseau) et une plate-forme (intergiciel, outils de développement, systèmes de gestion de bases de données, business intelligence, etc.) pour prendre en charge le cycle de vie des applications Web.

Exemple : Google App Engine, Force.com, Joyent, Azure.

Les fournisseurs PaaS fournissent les langages de programmation, les frameworks d'application, les bases de données et d'autres outils .

1.4.3 SAAS

Le SaaS est également connu sous le nom de « logiciel à la demande ». Il s'agit d'un modèle de distribution de logiciels dans lequel les services sont hébergés par un fournisseur de services cloud. Ces services sont disponibles pour les utilisateurs finaux sur Internet, de sorte que les utilisateurs finaux n'aient pas besoin d'installer de logiciel sur leurs appareils pour accéder à ces services.

1.4.3.1 Les inconvénients du cloud

- Centres de données existants : Dans de nombreuses entreprises, les applications et processus importants sont toujours exécutés dans des datacenters sur site, et non dans le cloud. Cela rend la migration vers un modèle NaaS légèrement plus difficile .
- Compatibilité : L'infrastructure du fournisseur de NaaS peut ne pas être compatible avec les systèmes existants qui sont encore en place, matériel plus ancien, applications sur site, etc.
- Verrouillage du fournisseur : Le passage à un service cloud présente toujours le risque qu'une entreprise devienne trop dépendante de ce fournisseur de services particulier. Si l'infrastructure du fournisseur de services tombe en panne ou s'il augmente ses prix, le verrouillage du fournisseur peut avoir des répercussions majeures.

1.5 La virtualisation

La virtualisation est une technique qui simule grâce à des machine virtuelles le comportement d'une ressources physique à l'aide d'un logiciel. Les machines virtuelles sont des programmes qui peuvent imiter un ordinateur complet pour prendre en charge un système d'exploitation conventionnel et utilise les mêmes fonctionnalités qu'un ordinateur physique .Une machine virtuelle n'est qu'un programme informatique , hébergée sur une machine physique [8] .
La virtualisation consiste , à exécuter sur une machine hôte, dans un environnement isolé, des systèmes d'exploitation pour générer des ressources virtuelles.
La virtualisation implique trois composant principaux qui sont :

- Un système d'exploitation installé sur la machine physique, appelé système hôte, car il joue le rôle d'hôte à d'autres systèmes d'exploitations
- Un hyperviseur un outil de virtualisation installé sur le système hôte qui fournit l'environnement dans lequel différentes machines virtuelles s'exécutent
- Un système d'exploitation installé dans la machine virtuelle appelé système pour invités .

1.5.1 Les différents types de Virtualisation

Nous avons quatre types de virtualisation :

- La virtualisation de stockage
- La virtualisation de réseau
- La virtualisation des postes de travail
- La virtualisation de serveurs

1.5.1.1 La virtualisation de stockage

Elle forme une couche de virtualisation active et transparente entre les périphériques de stockage sur disque pour optimiser la disponibilité, les performances et l'utilisation des grands et petits centres de données. L'intégration globale des fonctions de protection, d'approvisionnement, de mise en cache, de réplication et de migration gérées de manière centralisée vise à masquer les caractéristiques physiques des unités de stockage. Les avantages de ce type de virtualisation sont :

- Prolongement du cycle de vie de vos investissements en matière de stockage et ce de manière rentable.
- Bénéficie d'un premier niveau de Plan de Reprise d'Activité.

1.5.1.2 La virtualisation de réseau

consiste à recréer un réseau physique et ses différentes composantes : passerelles, switchs, routeurs, firewalls, load balancers... cela permet de faire tourner les applications sur un réseau virtuel comme sur un réseau physique, tout en profitant de l'indépendance matérielle inhérente à toute forme de virtualisation.

1.5.1.3 La virtualisation des postes de travail

La virtualisation des postes de travail permet aux administrateurs système et réseau de gérer plus facilement les postes de travail de l'entreprise et de répondre avec souplesse aux besoins des utilisateurs. Un poste de travail ou un poste de travail virtualisé peut être hébergé directement sur votre ordinateur ou sur un serveur dans notre centre de données .

1.5.1.4 La virtualisation des serveurs

Un serveur est un ordinateur conçu pour gérer un certain nombre de tâches spécifiques afin que d'autres ordinateurs (tels que des ordinateurs portables et de bureau) puissent effectuer diverses autres tâches . La virtualisation de serveur crée plusieurs serveurs virtuels sur un seul serveur physique. Ces serveurs créés s'exécutent sur la même machine physique et ont les mêmes propriétés que ce dernier . Les avantages de ce type sont :

- Consolidation des serveurs et optimisation de l'infrastructure.
- Augmentation de la flexibilité et de l'efficacité opérationnelle
- Disponibilité accrue des applications et amélioration de la continuité d'activité.

1.5.2 Les Hyperviseurs

Un hyperviseur est un logiciel qui vous permet de créer et d'exécuter des machines virtuelles. Un hyperviseur sépare le système d'exploitation et les ressources des machines virtuelles et permet la création et la gestion de ces machines virtuelles. L'hyperviseur alloue une ressource à chaque machine virtuelle et gère sa planification de ressources sur la base de la ressource physique . Le matériel physique utilisé comme hyperviseur est appelé un hôte , et toutes les machines virtuelles utilisant ses ressources sont appelées "invités". Deux types d'hyperviseurs peuvent être utilisés pour virtualiser les ressources : l'hyperviseur de type 1 et l'hyperviseur de type 2.[3]

1.5.2.1 Les hyperviseurs de type 1

Un hyperviseur de type 1, également appelé hyperviseur de système nu ou natif, s'exécute directement sur le matériel de l'hôte pour gérer les systèmes d'exploitation invités. Il prend la place du système d'exploitation de l'hôte et planifie directement les ressources des machines virtuelles sur le matériel. Ce type d'hyperviseur est fréquemment utilisé dans les datacenters d'entreprises et dans d'autres environnements basés sur des serveurs. Nous citons comme exemples : Hyper-V, XenServer, VMware ESXi.

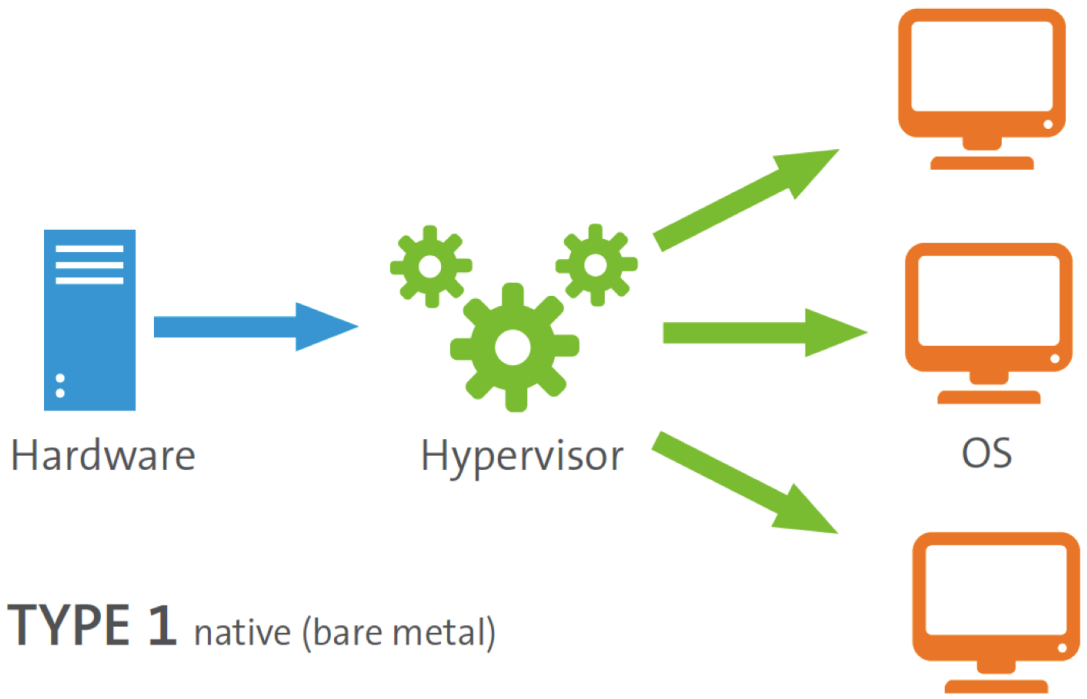


FIGURE 1.4 : Hyperviseur type 1

1.5.2.2 Les hyperviseurs de types 2

Un hyperviseur de type 2, également appelé hyperviseur hébergé, s'exécute sur un système d'exploitation traditionnel en tant que couche logicielle ou application. Il fonctionne en dissociant les systèmes d'exploitation invités du système d'exploitation hôte. Les ressources des machines virtuelles sont planifiées au niveau d'un système d'exploitation hôte, lui-même exécuté sur le matériel. Nous citons comme exemples : KVM, VMware Workstation, VirtualBoX.

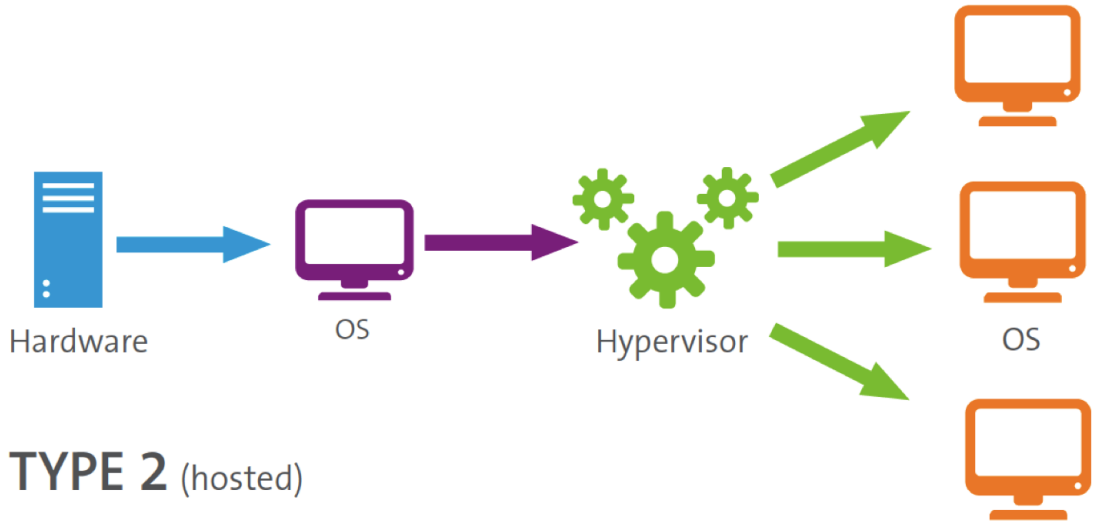


FIGURE 1.5 : Hyperviseur type 2

Conclusion

Le cloud computing est donc un moyen de délivrer un service informatique ciblé et quantifié à une clientèle précise sans que cette dernière n'ait à investir dans un système d'information dédié à ce service. Plusieurs services sont mis en places pour répondre aux besoins des utilisateurs simples mais aussi pour les petites et grandes entreprises. Dans ce chapitre nous avons présenté les notions de base et les points essentiels pour comprendre le cloud computing.

Chapitre 2

Analyse et choix techniques

Introduction

Le cloud computing, toujours en expansion, est une alternative efficace pour surmonter les problèmes internes et externes à l'entreprise. Dans ce chapitre, après une brève description de MDGL, nous aborderons des études de cas de clouds privés, principalement la création de VPC, et une étude comparative des meilleures offres pour mettre en évidence les meilleures solutions en termes de sécurité, mais aussi de performances structurelles.

2.1 Pourquoi utiliser un Cloud privé ?

2.1.1 Différence entre Cloud Privé et public

Un cloud privé est un cloud qui est géré par une organisation et qui est exclusivement utilisé par cette organisation. Les données sont stockées sur des serveurs physiques ou virtuels qui sont gérés et contrôlés par l'organisation. Les données sont généralement stockées dans un environnement sécurisé et isolé, ce qui permet à l'organisation de contrôler l'accès aux données et de les protéger contre les menaces externes.

Un cloud public est un cloud qui est géré par une entreprise et qui est accessible à tous les utilisateurs. Les données sont stockées sur des serveurs physiques ou virtuels qui sont gérés et contrôlés par l'entreprise. Les données sont généralement stockées dans un environnement partagé, ce qui permet aux utilisateurs d'accéder aux données à partir de n'importe quel endroit. Cependant, les données sont moins sûres car elles sont stockées sur des serveurs qui peuvent être accessibles à des tiers.

2.1.2 Choix du cloud Privé

Un cloud privé offre aux entreprises une plus grande flexibilité et un meilleur contrôle sur leurs données et leurs applications. Il permet aux entreprises de déployer des applications et des services à l'échelle de leur entreprise, sans avoir à se soucier des problèmes de sécurité et de confidentialité liés à l'utilisation d'un cloud public. Les entreprises peuvent également bénéficier d'une plus grande évolutivité et d'une meilleure disponibilité des services, car elles peuvent facilement ajouter ou sup-

primer des ressources en fonction de leurs besoins. Enfin, un cloud privé peut offrir aux entreprises des coûts plus faibles et une meilleure gestion des ressources.

Pour mettre en place un cloud privé il nous faut essentiellement des data center

2.1.2.1 Les exigences d'un cloud privé en matière de data center

Pour mettre en place un cloud privé il nous faut un data center qui puisse :

- Une infrastructure réseau robuste et sécurisée pour assurer la confidentialité des données et des applications.
- Des serveurs puissants et fiables pour gérer les charges de travail critiques.
- Des systèmes de stockage sécurisés et à haute disponibilité pour garantir la sécurité des données.
- Des solutions de sauvegarde et de récupération des données pour assurer la continuité des activités.
- Des systèmes de gestion des performances pour surveiller et optimiser les performances du cloud privé.
- Des solutions de sécurité avancées pour protéger le cloud privé contre les menaces externes.
- Des outils de gestion des identités et des accès pour gérer les utilisateurs et leurs autorisations.
- Des solutions de surveillance et d'audit pour surveiller et vérifier les activités du cloud privé.

2.2 Les solutions du cloud computing public

Actuellement, il existe trois acteurs potentiels sur le marché du cloud computing public. Windows via sa plate-forme Azure, Google via sa plateforme de développement d'applications AppEngine et Amazon via son service informatique virtuel EC2.

2.2.1 Google Cloud Virtual Private Cloud (VPC)

Google VPC dispose d'un réseau couvrant 27 régions et 200 autres régions et pays avec un temps d'arrêt minimal pour ses utilisateurs.

Un VPC peut couvrir plusieurs zones sans avoir à se connecter à Internet. Les utilisateurs locaux peuvent se connecter à un VPC avec des ressources locales et VPC avec toutes les régions d'un VPC.

Avec un VPC qui couvre l'ensemble de l'entreprise, les équipes peuvent être isolées au sein de leurs projets avec des quotas et des factures différents tout en ayant un espace IP partagé par tous et un accès aux services les plus couramment utilisés.

Il vous permet d'augmenter l'espace IP pour tous les sous-réseaux sans interruption ni arrêt de la charge de travail en configurant des plages de préfixes pour vos sous-réseaux et stratégies réseau en les configurant vous-même. Les utilisateurs peuvent également étendre les zones CIDR sans interruption. [2] Déploiement – Cloud, SaaS, basé sur le Web. Principales caractéristiques - Réseau VPC, journaux de flux VPC, appairage VPC, pare-feu, routes, VPC partagé, hybride et multi-cloud, Internet des objets, outils de gestion, informatique sans serveur et stockage, mise en miroir de paquets,

VPN, architectures simples et complexes, reprise après sinistre, médias et jeux, migration, mise en réseau, sécurité et identité, accès privé, Apigee, Firebase, Orbitera, Google Hardware, Google Identity, Chrome Enterprise, Android Enterprise. L'environnement de déploiement des serveurs sur Google cloud est Cent OS, une distribution linux qui est un des systèmes les plus utilisés dans le déploiement des serveurs web. Aussi ce choix constitue un défi personnel puisque ce sera mon premier contact avec cet environnement.

2.2.2 Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC permet aux utilisateurs de provisionner une partie isolée et logique dans le cloud AWS qui leur permet de démarrer des ressources AWS sous la forme d'un réseau virtuel.

Les utilisateurs contrôlent l'environnement de réseau virtuel en sélectionnant les adresses IP spécifiques au sous-réseau, en les créants et en configurants des itinéraires, des tables et des passerelles réseau. Il utilise IPv4 et IPv6 au sein du VPC pour sécuriser un accès rapide aux ressources et aux applications. [4] Il offre également un contrôle total sur leur réseau virtuel. Les utilisateurs peuvent configurer un réseau open source pour les sites Web connectés à Internet tout en plaçant leurs systèmes back-end dans des sous-réseaux privés sans connexion Internet, tels que des bases de données ou des serveurs d'applications. Principales caractéristiques

- Analyse, gestion de base de données
- Machines virtuelles personnalisées
- Configuration de console
- Gestion du réseau et des machines virtuelles
- Sécurité, maintenance, évolutivité ,connectivité sécurisée

2.2.3 Microsoft Azure virtual private cloud

Service de cloud computing créé par Microsoft pour la création, le test, le déploiement et la gestion d'applications et de services via des centres de données gérés par Microsoft. Il fournit des logiciels en tant que service (SaaS), une plate-forme en tant que service (PaaS) et une infrastructure en tant que service (IaaS) et prend en charge de nombreux langages, outils et Framework de programmation différents, y compris des logiciels et des systèmes spécifiques à Microsoft et tiers.[7]

2.3 Les solutions open source

Les solutions open source du cloud computing sont destinées au déploiement de l'architecture en privé pour un usage en interne. Toutefois, les solutions proposées peuvent être utilisées pour fournir les services du cloud public. Les solutions de cloud privé implémentent généralement les services IaaS. Leur rôle consiste à gérer un ensemble de machines physiques et virtuelles dans un réseau local ou une interconnexion de plusieurs réseaux. L'architecture de supervision des nœuds d'exécution des machines virtuelles de ces solutions est généralement composée d'un nœud central appelé cloud controller (CLC), de plusieurs nœuds d'exécution des services du cloud appelés Node controllers et parfois d'un ensemble de nœuds intermédiaires de supervision appelés cluster controllers. Les

terminologies utilisées dans les différentes solutions existantes telles que Eucalyptus, OpenNebula, Cloudstack et Openstack peuvent varier mais le principe de fonctionnement de ces différents nœuds reste approximativement le même.

2.3.1 Openstack

OpenStack est un système d'exploitation cloud qui contrôle de grands pools de ressources de calcul, de stockage et de mise en réseau dans un centre de données, le tout géré via un tableau de bord qui donne aux administrateurs le contrôle tout en permettant à leurs utilisateurs de provisionner des ressources via une interface Web. OpenStack est un ensemble de logiciels open source permettant de déployer des infrastructures de cloud Computing (IaaS et Naas).

2.3.2 Cloudstack

Apache CloudStack est une plate-forme open source d'infrastructure en tant que service qui gère et orchestre des pools de ressources de stockage, de réseau et informatiques pour construire un cloud de calcul IaaS public ou privé.

Avec CloudStack, vous pouvez :

Configurez un service de cloud computing élastique à la demande.

Autoriser les utilisateurs finaux à provisionner des ressources

CloudStack configure automatiquement les paramètres de réseau et de stockage pour chaque déploiement de machines virtuelles. En interne, un pool d'Appliance virtuelles prend en charge l'opération de configuration du cloud lui-même. Ces appareils offrent des services tels que : pare-feu, routage, DHCP, VPN, console proxy, stockage l'accès et la réplication du stockage. L'utilisation intensive de scalables horizontalement machines virtuelles simplifie l'installation et le fonctionnement continu d'un cloud.

2.3.3 Eucalyptus

Eucalyptus signifie Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems.Eucalyptus dans le cloud computing est une programmation open source qui réalise un cloud AWS viable, financièrement avisé, sécurisé et flexible . Il est développé en C, Java et Python et est disponible sous deux licences. Une licence GPL gratuite qui prend en charge les hyperviseurs Xen et KVM, et une licence commerciale avec des fonctionnalités avancées telles que la prise en charge de VMware. Cela vous permet de créer à la fois des solutions de cloud computing privées et des solutions publiques. Son gros avantage est qu'il s'intègre aux distributions Ubuntu et Debian. Eucalyptus fournit une interface compatible avec le service EC2 d'Amazon. Cela lui permet d'être utilisé pour des solutions de cloud computing hybrides.

2.3.4 OpenNebula

Contrairement aux solutions de cloud computing traditionnelles, OpenNebula fournit une boîte à outils complète pour gérer de manière centralisée des infrastructures virtuelles hétérogènes. Il s'agit d'une plate-forme open source pure pour les déploiements de cloud privé, public et hybride. Cependant, l'idée de base de la solution d'OpenNebula est une implémentation privée qui permet aux utilisateurs de se connecter à des ressources internes via une interface Web. La solution OpenNebula est strictement centralisée autour d'un nœud appelé le frontend, qui est chargé de surveiller l'ensemble

de l'architecture. Il repose sur un haut degré de personnalisation en proposant plusieurs modules paramétrables et adaptables à vos besoins. Ce haut degré de modularité a à la fois l'avantage de vous permettre de construire votre propre architecture et l'inconvénient d'introduire des difficultés de configuration qui entraînent des erreurs et des échecs de mise en œuvre, et l'hyperviseur VMware en option. L'architecture interne d'OpenNebula se compose de trois couches d'éléments, chacun appelé Tools, core et drivers.

2.3.5 Étude comparative des principales Solutions existantes

Précédemment, nous avons présenté les solutions existantes dans le domaine du cloud computing. Ces solutions se répartissent en deux catégories. Les solutions publiques et les solutions open source pour le cloud computing privé. Le Ministère étant une institution gouvernementale et donc public ces ressources ne peuvent être contrôler par un tiers en plus du coût que ça implique. Nous nous sommes alors tourner vers les solutions Open sources Une comparaison est effectuée dans le tableau suivant afin de ressortir la meilleure offre.

Solutions de clouds	**Critères de sécurité**	**Protocole de transmission des données**	**Coût d'installation**
Eucalyptus	Sécurité avancée avec des options de chiffrement et de contrôle d'accèsContrôle d'accès Authentification chiffrement des données	Utilise des protocoles comme SOAP et REST	Faible à moyen
CloudStack	• Faiblesse des outils de sécurité • Faiblesse de la surveillance des activités • Journalisation des activités • Contrôle d'accès limité • Authentification Sécurité renforcée avec des fonctionnalités de pare-feu et de VPN	Supporte des protocoles comme HTTP, HTTPS, et SNMP	Gratuit, mais des coûts peuvent s'ajouter pour le support et les services professionnels

Continued on next page

Table 2.1 Continued from previous page

Solutions de clouds	**Critères de sécurité**	**Protocole de transmission des données**	**Coût d'installation**
OpenNebula	• Contrôle d'accès • Authentification • Chiffrement des données • Journalisation des activités • Problèmes de configuration • Faiblesse des outils de sécurité • Contrôle d'accès limité • Faiblesse de la surveillance des activités	Utilise des protocoles comme XML-RPC et OCCI	Gratuit, avec des coûts potentiels pour le support et les services professionnels

Continued on next page

Table 2.1 Continued from previous page

Solutions de clouds	**Critères de sécurité**	**Protocole de transmission des données**	**Coût d'installation**
OpenStack	• Contrôle d'accès basé sur les rôles • Audit des activités • Problèmes de configuration • Chiffrement des données • Gestion des clés : OpenStack prend en charge la gestion des clés qui permet aux utilisateurs de contrôler l'accès aux données en fonction des clés. • Outils de sécurité intégrés • Faiblesse de la surveillance des activités : La surveillance des activités est essentielle pour détecter les tentatives d'accès non autorisées et les activités suspectes. Cependant, la surveillance des activités peut être faible dans le nuage OpenStack.	Supporte divers protocoles comme HTTP, HTTPS, et AMQP	Gratuit, mais les coûts peuvent varier en fonction de l'infrastructure et des services supplémentaires

TABLE 2.1 : Tableau compararif des solutions cloud opensource

2.4 Motivation du choix d'Openstack

En termes de services proposés, les quatre solutions open source que nous avons étudiées sont : Eucalyptus, OpenNebula, OpenStack et cloudstack offrent presque les mêmes fonctionnalités en termes de gestion VMS, gestion des utilisateurs, etc., mais diffèrent en termes de sécurité, de stockage, de modes réseau, etc. Chacun a ses avantages et ses inconvénients. OpenStack est la solution la plus utilisée par rapport à Eucalyptus, OpenNebula et Cloudstack, a un fort développement et est mise à jour chaque année, dernière version publiée le 30 mars 2022 par la version YOGA. Il Offre plus de flexibilité et de fonctionnalités avancées pour le déploiement de cloud . OpenStack s'est avéré être un excellent choix en termes de simplicité et, grâce à un tableau de bord riche en fonctionnalités, a été un facteur clé dans le contrôle de la santé de l'infrastructure et les opérations de VM peuvent être surveillées. Après avoir examiné quatre solutions et un tableau comparatif que j'ai créé, j'ai décidé d'installer OpenStack, une plate-forme entièrement gratuite et open source.

2.5 Presentation d'Openstack



FIGURE 2.1 : Logo openstack

2.5.1 Presentation

OpenStack est un projet de Cloud Computing prive, public et hybride sous licence Apache2.0, écrit en Python. La NASA a développé spécialement la partie calcul d'OpenStack et Rackspace Cloud a contribué à la partie stockage. À partir de juillet 2010, ces deux sociétés ont ensuite été rejoints par Cloud.com, Canonical, Cisco et autre pour le développement d'OpenStack. OpenStack est une architecture qui fournir la flexibilité pour concevoir un nuage, sans matériel propriétaire ou logiciel requis et la capacité d'intégrer avec les systèmes existants et des technologies tierces. Il est conçu pour gérer et automatiser des pools de ressources de calcul et peut travailler avec des technologies de virtualisation largement disponibles, ainsi le calcul haute performance (HPC). OpenStack est package dans Ubuntu Serveur et dans Debian. D'autres distributions telles que RedHat Enterprise Linux et

Cent OS sont maintenant supportées. OpenStack supporte la plupart des solutions de virtualisation du marché : ESX, Hyper-V, KVM, LXC, QEMU, UML, Xen et XenServer[11]

2.5.2 Modularité d'OpenStack

OpenStack est conçu selon un modèle modulaire, ce qui signifie qu'il est constitué de différents composants interopérables, chacun remplissant un rôle spécifique. Cette approche modulaire permet aux utilisateurs de sélectionner les composants nécessaires à leur infrastructure en fonction de leurs besoins, évitant ainsi la surcharge inutile. Parmi les composants essentiels d'OpenStack, on trouve :

2.5.2.1 Nova

Le module Nova est chargé de la gestion des instances de machines virtuelles (VM) et de leur provisionnement. Il sert de couche d'abstraction pour les ressources informatiques sous-jacentes. Il permet :

- La La gestion des instances serveurs
- La gestion du réseau
- Le contrôle des accès

Nova ne nécessite pas de pré-requis et est totalement indépendant de l'hyperviseur.Il est l'équivalent d'EC2 d'Amazon Elastic Compute Cloud.

2.5.2.2 Swift

Object Storage sert à la création d'espace de stockage redondant pour le stockage de plusieurs pétaoctet de données. Il ne s'agit pas réellement d'un système de fichier traditionnel, mais plutôt un système de stockage distribué conçu pour le stockage à long terme de gros volumes de données telles que les images de machines virtuelles, stockage photo, stockage e-mail, etc. Son architecture distribuée offre plusieurs points d'accès pour éviter les SPOF. C'est l'équivalent d'Amazon Simple Storage Service.

2.5.2.3 Glance

Fournit les services de stockage, de découverte, d'enregistrement et de distribution pour les images disques de machines virtuelles. Il fournit également une API compatible REST permettant d'effectuer des requêtes pour obtenir des Informations sur les images hébergées par les différents magasins de stockages. Glance offre les mêmes caractéristiques que le catalogue d'Amazon AMI

2.5.2.4 keystone

Keystone est le module d'authentification et d'autorisation, gérant les identités des utilisateurs, des projets et des rôles.

2.5.2.5 Cinder

Cinder est responsable de la gestion des volumes de stockage et de leur attachement aux instances de VM.

2.5.2.6 Horizon

Horizon est l'interface web d'OpenStack, offrant une expérience conviviale pour les utilisateurs et les administrateurs.

Il fournit une interface utilisateur modulaire fondé sur le Web pour tous les Services OpenStack. Cette interface graphique Web, permet aux administrateurs de nuages et aux utilisateurs de contrôler leur infrastructure (instances, Stockage et les ressources réseau). En tant qu'administrateur de nuage, le Dashboard fournit une vue d'ensemble sur la taille et l'état du nuage. Il permet de créer des utilisateurs et des projets, affecter des utilisateurs à des projets et fixer des limites sur les ressources pour ces projets (quotas), en revanche il fournit aux utilisateurs un Portail self-service et met à leur disposition leur propres ressources dans les limites fixées par les administrateurs. Le projet OpenStack est conçu pour fournir un nuage hautement évolutif. Pour ce faire, chacun des services constitutifs sont conçus pour fonctionner ensemble pour Fournir une infrastructure complète en tant que service (IaaS et Naas). Cette intégration est facilitée par des interfaces de programmation d'applications publiques (API) qui Permettent à chacun de ces services d'utiliser un autre service, ce sont les mêmes API qui sont disponibles pour les utilisateurs finaux du nuage

2.5.2.7 Neutron

OpenStack Networking (neutron) gère toutes les facettes de mise en réseau pour l'infrastructure de réseau virtuel (VNI) et l'accès aspects de couche de l'infrastructure de réseau physique (PNI) dans OpenStack.

réseau fournit des réseaux, des sous-réseaux et des routeurs en tant qu'abstractions d'objets. Chaque abstraction a une fonctionnalité qui imite son homologue physique : les réseaux contiennent des sous-réseaux et les routeurs acheminent le trafic entre différents sous-réseaux et réseaux.

Toutes configurations de mise en réseau donnée comporte au moins un réseau externe. Contrairement aux autres réseaux, le réseau externe ou le réseau du fournisseur n'est pas simplement un réseau virtuellement défini. Au lieu de cela, il représente une vue dans une tranche du réseau physique externe accessible en dehors d'OpenStack. Les adresses IP sur le réseau externe sont accessibles par n'importe qui physiquement à l'extérieur réseau.

2.5.2.8 Heat

Heat est le composant d'orchestration d'Openstack. Il permet de décrire une infrastructure sous forme de modèles. Dans Heat, ces modèles sont appelés des stack . Heat consomme ensuite ces modèles pour aller déployer l'infrastructure décrite sur Openstack. Il peut aussi utiliser les métriques fournies par Ceilometer pour décider de créer des instances supplémentaires en fonction de la charge d'une application par exemple.

2.5.2.9 Ceilometer

Le service de télémétrie d'OpenStack s'appelle Ceilometer. Il permet de collecter différentes métriques sur l'utilisation du cloud. Par exemple il permet de récolter le nombre d'instances lancé dans un projet et depuis combien de temps. Ces métriques peuvent être utilisées pour fournir des informations nécessaires à un système de facturation par exemple. Ces métriques sont aussi utilisées dans les applications ou par d'autres composants d'Openstack pour définir des actions en fonction de certains seuils comme avec le composant d'orchestration.

2.5.3 Flexibilité et Personnalisation

OpenStack offre une flexibilité exceptionnelle, permettant aux organisations de personnaliser leur infrastructure de cloud computing en fonction de leurs besoins spécifiques. Cette flexibilité découle de la modularité d'OpenStack, car les organisations peuvent choisir les composants qui correspondent le mieux à leurs exigences.

De plus, la nature open-source d'OpenStack signifie que les utilisateurs peuvent apporter des modifications au code source pour créer des fonctionnalités personnalisées ou résoudre des problèmes spécifiques. Cela offre un degré de contrôle et de personnalisation que les solutions propriétaires ne peuvent pas toujours offrir.

2.5.4 L'architecture et les relation entre les composant de openstack

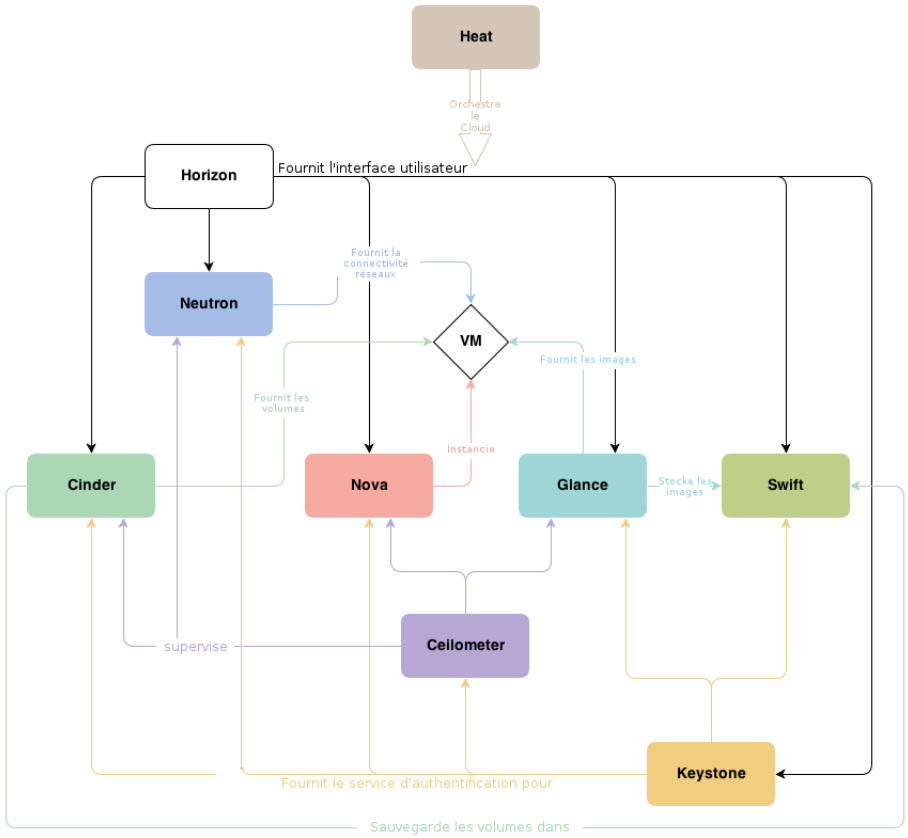


FIGURE 2.2 : Architecture conceptuel OpenStack

- **Horizon ou Dashbord** : Les utilisateurs se connectent à l'interface utilisateur et spécifie les paramètres de la machine virtuelle (machine virtuelle) tels que le nom, la saveur, les clés.
- **Nova**gère le cycle de vie des instances de calcul dans un environnement OpenStack. Il comprend le Spawning, la planification et la décomposition des machines virtuelles à la demande.
- **Cinder** Il fournit un stockage de bloc persistant aux instances en cours d'exécution
- **Neutron**Il fournit une connectivité entre l'interface d'autres services OpenStack tels que Nova .
- **Glance** Il stocke et récupère les images disque des machines virtuelles . Les images peuvent

être utilisées comme modèle lors de la configuration d'un nouveau serveur. Habituellement, les images sont stockées dans Swift (objet) .

- **Swift**il stocke et récupère des objets de données arbitraires non structurés via une API basée sur HTTP . Il est hautement tolérant aux pannes avec sa réplication de données et son architecture évolutive.
- **Keystone**Il fournit un service d'authentification et d'autorisation pour tous les autres services .

2.5.4.1 Évolution d'OpenStack

OpenStack est en constante évolution, avec des versions majeures publiées régulièrement pour introduire de nouvelles fonctionnalités et améliorations. Les versions d'OpenStack portent des noms de code, comme "Liberty," "Newton," "Pike," "Queens," "Rocky," "Stein," "Train," "Ussuri," "Victoria," "Wallaby," et ainsi de suite. Chaque version apporte des améliorations significatives à la plateforme, notamment en termes de sécurité, de performances et de convivialité.

La Fondation OpenStack joue un rôle central dans le développement d'OpenStack, coordonnant les efforts de milliers de contributeurs et garantissant que la plateforme reste un projet open-source actif et en constante évolution.

2.6 Confidentialité dans OpenStack

Dans ce section, nous nous concentrons sur un aspect critique de notre infrastructure de cloud privé basée sur OpenStack : la confidentialité des données. Nous explorerons les enjeux de la confidentialité, les mesures de sécurité mises en place dans OpenStack, et les meilleures pratiques pour gérer les données sensibles.

2.6.1 Enjeux de la Confidentialité

La confidentialité des données est un enjeu majeur dans l'environnement du cloud computing. Les organisations qui stockent et traitent des données sensibles, telles que des informations personnelles, des secrets commerciaux et des données financières, sont confrontées à plusieurs défis en matière de confidentialité.

- **Accès Non Autorisé** : L'un des principaux risques pour la confidentialité est l'accès non autorisé aux données. Dans un environnement OpenStack, plusieurs acteurs interviennent, des administrateurs aux utilisateurs finaux. Les vulnérabilités dans ces couches peuvent entraîner des accès non autorisés aux données, exposant ainsi l'organisation à des risques.
- **Fuite d'Informations Sensibles** : Les fuites d'informations sensibles sont une préoccupation constante. Elles peuvent résulter d'erreurs humaines, d'attaques malveillantes ou de vulnérabilités de sécurité. Les impacts de ces fuites peuvent être dévastateurs sur le plan financier, juridique et réputationnel.
- **Vulnérabilité des Données** : La vulnérabilité des données fait référence à la facilité avec laquelle les données peuvent être compromises. Les failles de sécurité dans OpenStack ou les mauvaises pratiques de gestion des données peuvent rendre les données vulnérables aux attaques.

2.7 Mesures de Sécurité dans OpenStack

OpenStack propose un certain nombre de mesures de sécurité pour répondre aux enjeux de confidentialité mentionnés ci-dessus.

2.7.1 Authentification et Autorisation

OpenStack utilise le composant Keystone pour gérer l'authentification et l'autorisation. Cela garantit que seules les personnes autorisées ont accès aux ressources et aux données sensibles.

2.7.2 Chiffrement des Données

Le chiffrement des données est une pratique courante dans OpenStack. Les données au repos et en transit sont chiffrées pour garantir leur confidentialité.

2.7.3 Politiques de Sécurité

OpenStack permet de définir des politiques de sécurité granulaires. Les administrateurs peuvent spécifier qui a accès à quelles ressources et quelles données, renforçant ainsi la sécurité.

La gestion des données sensibles est un élément essentiel de la préservation de la confidentialité. Les organisations doivent mettre en place des politiques et des procédures pour garantir la protection des données sensibles stockées dans OpenStack.

2.7.4 Surveillance et Audit

OpenStack offre des outils de surveillance, comme Ceilometer, pour détecter les activités suspectes. Les journaux d'audit enregistrent les actions des utilisateurs pour une traçabilité complète

2.8 Sécurité avec OpenStack

Cette section se penche sur l'aspect de la sécurité dans l'infrastructure OpenStack que nous mettons en place. Nous explorerons les composants d'OpenStack dédiés à la sécurité, les mécanismes de gestion des vulnérabilités, la surveillance de la sécurité et l'importance de la sécurisation des réseaux.

2.8.1 Authentification et Autorisation

2.8.1.1 Keystone : Le Gardien de l'Authentification

Keystone est le composant central d'OpenStack pour l'authentification et l'autorisation. Il gère les identités des utilisateurs, des projets et des rôles au sein de l'infrastructure. L'authentification est le processus de validation de l'identité de l'utilisateur, tandis que l'autorisation détermine les actions que cet utilisateur est autorisé à effectuer. Keystone utilise des mécanismes tels que le nom d'utilisateur et le mot de passe, mais peut également être intégré avec des systèmes d'authentification externes tels que LDAP ou SAML.

2.8.1.2 Gestion des Rôles

OpenStack utilise un modèle basé sur les rôles pour définir les politiques de sécurité. Les rôles déterminent ce qu'un utilisateur est autorisé à faire dans l'environnement OpenStack. Par exemple, un utilisateur peut être un administrateur, un opérateur ou un simple utilisateur final, chaque rôle ayant des privilèges différents. Cette granularité permet de définir des politiques de sécurité précises.

2.8.2 Gestion des Vulnérabilités

2.8.2.1 Surveillance des Vulnérabilités

La sécurité d'OpenStack est maintenue grâce à une surveillance active des vulnérabilités. Des équipes dédiées au sein de la communauté OpenStack surveillent en permanence les rapports de vulnérabilités et publient des correctifs. Cela garantit que les failles de sécurité connues sont rapidement corrigées, réduisant ainsi les risques potentiels.

2.8.2.2 Processus de Mise à Jour

OpenStack a établi un processus de mise à jour régulier pour garantir que les composants restent sécurisés. Les mises à jour régulières permettent de corriger les vulnérabilités, d'améliorer les performances et d'ajouter de nouvelles fonctionnalités. La communauté OpenStack encourage les administrateurs à maintenir leurs déploiements à jour pour bénéficier des dernières améliorations de sécurité.

2.8.3 Surveillance et Audit de Sécurité

2.8.3.1 Collecte de Données de Surveillance

La surveillance constante de l'activité dans OpenStack est essentielle pour détecter les comportements suspects ou les tentatives d'accès non autorisé. OpenStack utilise des outils tels que Ceilometer pour collecter des données sur les opérations effectuées au sein de l'infrastructure. Ces données comprennent les ressources allouées, les accès aux données, les modifications de configuration, etc.

Dans un environnement cloud, la sécurité est d'une importance capitale. Les principes de sécurité, tels que la confidentialité, l'intégrité et la disponibilité, doivent être intégrés à chaque niveau de l'infrastructure. Des outils tels que le cryptage des données, les pare-feu et la gestion des identités peuvent être utilisés pour renforcer la sécurité. De plus, la mise en place de bonnes pratiques de sécurité, telles que des politiques de gestion des mots de passe et des mises à jour régulières, est essentielle. La gestion des risques et la conformité aux réglementations en vigueur doivent également être prises en compte, notamment en ce qui concerne la protection des données sensibles. En fin de compte, la sécurité et la gestion des risques doivent être des préoccupations constantes dans la mise en place d'une solution cloud privé avec OpenStack.

2.8.3.2 Journaux d'Audit

Les journaux d'audit enregistrent toutes les actions effectuées par les utilisateurs et les administrateurs au sein de l'infrastructure OpenStack. Ces journaux fournissent une traçabilité complète des opérations, ce qui est essentiel pour la détection des comportements malveillants ou des erreurs humaines.

2.8.4 Sécurisation des Réseaux

2.8.4.1 Segmentation de Réseau

OpenStack permet de créer des segments de réseau isolés pour séparer les flux de données. Cela réduit le risque d'attaques réseau en limitant la surface d'attaque.

2.8.4.2 Pare-feu et VPN

OpenStack intègre des fonctionnalités de pare-feu pour filtrer le trafic réseau et d'accès VPN pour garantir une connexion sécurisée aux ressources. Ces outils contribuent à renforcer la sécurité des communications réseau.

2.8.5 Gestion des Menaces

La communauté OpenStack collabore avec des experts en sécurité pour faire face aux menaces émergentes. Cette collaboration permet de renforcer la sécurité d'OpenStack en tenant compte des dernières menaces et des meilleures pratiques. La sécurité dans OpenStack offre une protection robuste des données et des ressources. Les avantages incluent :

- Réduction des risques d'accès non autorisé.
- Détection précoce des menaces grâce à la surveillance.
- Chiffrement des données pour préserver la confidentialité.
- Gestion proactive des vulnérabilités.
- Respect des normes de conformité.

Conclusion

Dans ce chapitre nous avons étudié les solutions cloud qui permettent la mise en place d'un cloud de type IAASS et NAAS mais principales open source dont openstack,opennebula,cloudstarcket eucalytus.Ces dernières répondent à plusieurs besoin , mais openstack possède de récente mise a niveau et offre une meilleur expérience

Chapitre 3

Mise en place, tests et résultats

Introduction

Dans ce chapitre nous allons aborder la partie pratique de notre travail. Nous allons tout d'abord nous intéresser aux principales étapes pour installer Openstack Yoga.

Nous allons commencer par la préparation du système sur lequel il sera déployée et ceci par la configuration réseau , ainsi qu'a l'installation des paquets nécessaires pour le bon fonctionnement des différents services. Puis nous allons faire l'installation et la configuration de keystone,glance,Nova et des autres services nécessaire pour une bonne gestion d'Openstack .

3.1 Installation d'OpenStack

Il existe deux(2) manières pour installer OpenStack

- **LE Single Node("All in one")Déploiements** :Dans cette configuration , tous les services sont installés sur un même système.
- **Multi Node** : Dans cet déploiement les diverses composant d'OpenStack sont installés sur plusieurs noeuds différents.

Dans notre cas nous allons installer Openstack sur une seule machine donc le déploiement "All in One"[6]

3.1.1 Pré-requis pour installer OpenStack

Nous allons citer ceux d'on nous avons besoin pour installer OpenStack

- VirtualBox
- Système d'exploitation Ubuntu 18.04.4
- serveur Apache 2
- les bases de données MySQL et RabbitMQ

- le paquet Microstack-Openstack
- Un disque d'au moins 50Go et une mémoire vive de 4gb

3.1.2 Installation d'openstack

Tout d'abord nous avons installer microstack qui est un moyen simple pour tester OpenStack sur notre machine virtuelle avec la commande :

```
udo snap install microstack --beta
```

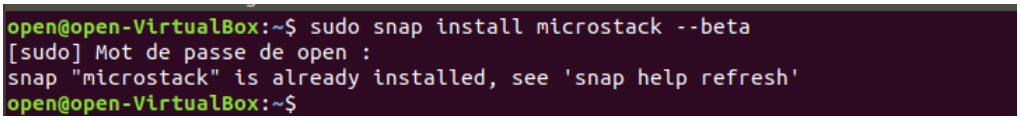


FIGURE 3.1 : Installation de microstack

Ensuite on peut voir les informations sur le composant logiciel installé avec la commande :

```
nap list microstack
```

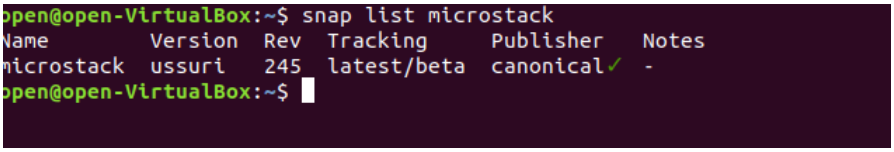


FIGURE 3.2 : List microstack

Nous allons a présent lancer l'installation d'OpenStack

```
sudo microstack init --auto --control
```

L'étape d'initialisation déploie ,configure et démarre automatiquement les services d'OpenStack .Il crée en particulier la base de données,les réseaux ,une image et les groupes de sécurité ICMP/SSH

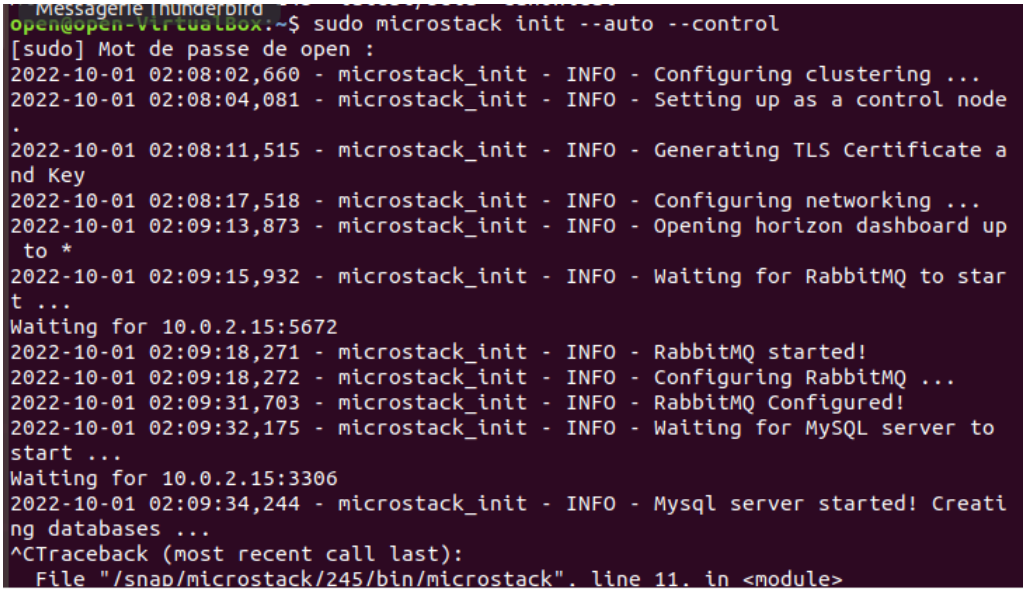


FIGURE 3.3 : Microstack Init

Le standard openstack client est ainsi pré-installé et on peu y accéder avec :

```
icrostack.openstack image list
```

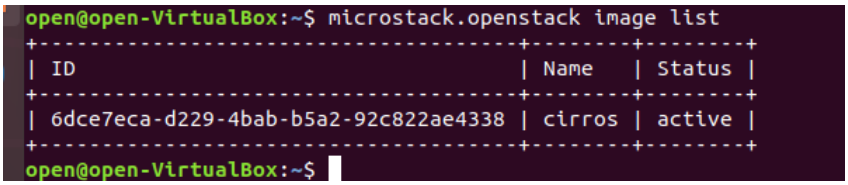


FIGURE 3.4 : L'image par défaut

Pour obtenir la liste des saveurs c'est a dire la capacité de calcule,de mémoire et de stockage d'un serveur virtuel ou d'une instance .On y accède avec la commande :

```
icrostack.openstack flavor list
```

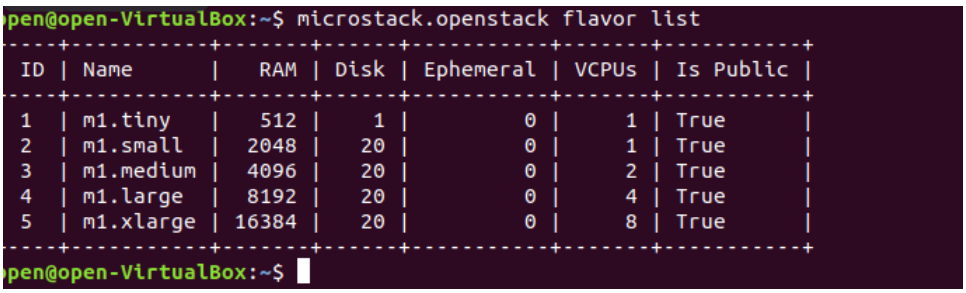


FIGURE 3.5 : Flavors liste

Création d'une instance Microstack est doté d'une commande de création d'instance pratique appelée microstack launch qui utilise les valeurs par défaut suivantes pour ses instances

- paire de clé "micropile"
- saveur "m1.tiny"
- adresse ip flottante sur le sous-réseau "10.20.20.0/24"

Pour créer une instance sur l'image 'cirros' on utilise la commande

```
icrostack launch cirros –n test
```

Nous venons de créer l'instance nommée test

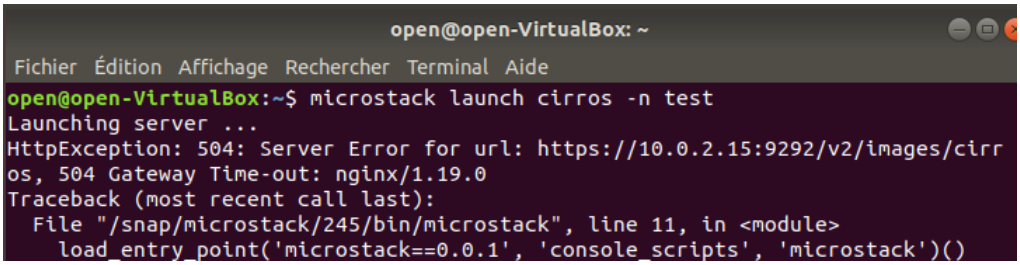


FIGURE 3.6 : Création de l'instance test

A cet étape nous pouvons déjà avoir accès à l'interface utilisateur Web avec l'URL : **https ://10.0.2.15** le nom d'utilisateur est "admin et le mot de passe est généré avec

```
do snap get microstack config.credentials.keystone–password
```

3.2 Test et Utilisation d'OpenStack

Il existe deux types d'utilisation du cloud , administrateur ou membre d'un projet. Selon le type d'utilisateur des interfaces ou d'autre s'affichent après authentification **Authentification**
La première étape qui devrait être effectué par l'administrateur pour qu'il puisse se connecter , a horizon est l'authentification comme le montre la figure ci-dessous

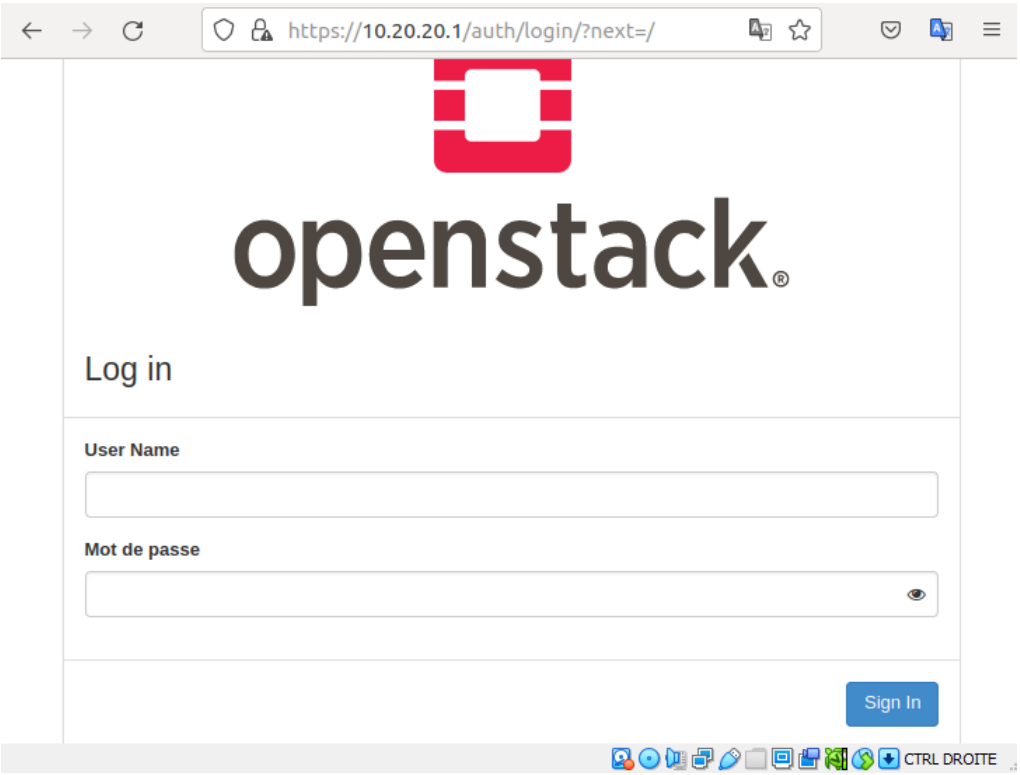


FIGURE 3.7 : HHorizon OpenStack

Overview ou Vue d'ensemble Une fois connecté , en fonction des privilèges d'accès , l'utilisateur est autorisé à accéder à des projets spécifiques .ce qui suit est une page d'aperçu pour un projet appartenant a l'administrateur "test"

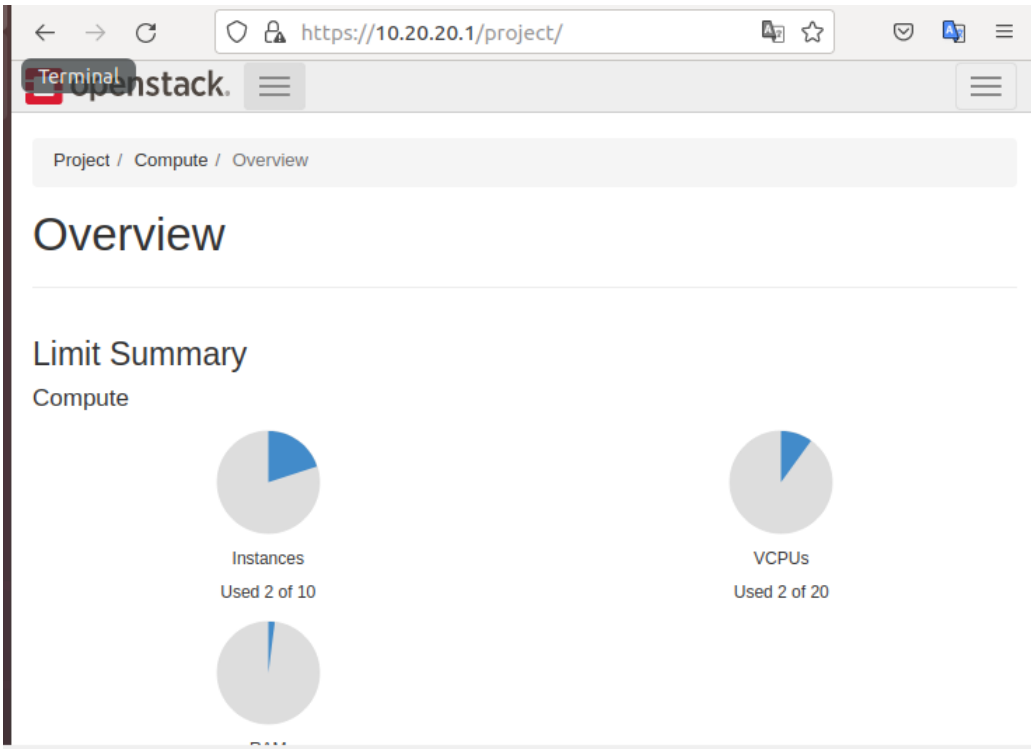


FIGURE 3.8 : Vue d'ensemble overview

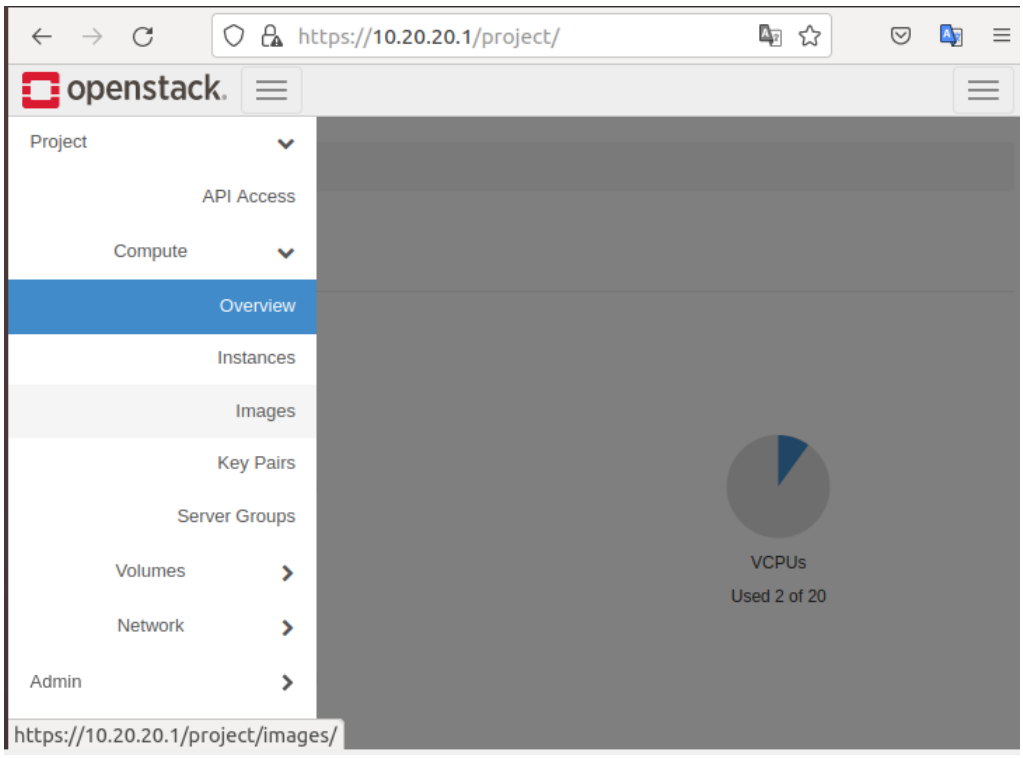


FIGURE 3.9 : Paramètre OpenStack

3.2.1 Les étapes pour le mise en place du serveur

Pour mieux tester le fonctionnement de la nouvelle technologie dans le dans , l' administrateur(le DSI) est responsable de la nouvelle solution cloud, il gérera donc le projet "admin" via la plate-forme Openstack. • Tout d'abord, il va s'occuper de la gestion des des instances en créant les utilisateurs

ainsi que leurs rôles selon les privilèges qu'il leur accorde .Ensuite, il allouera une adresse IP dynamique au projet, enfin, configurera et lancera une instance de serveur.

Création de rôles

l'administrateur principale va créer deux rôles , celui du lecteur et des membres . Le lecteur ne peut effectuer aucune modification dans le système . Pour créer un rôle on accède à l'onglet : identity->Roles – Create Role, puis le renommer et cliquer sur le bouton "submit" :



FIGURE 3.10 : Création du rôle membre

Création d'utilisateurs :

Pour créer un utilisateur, on se rend dans l'onglet : Identity->Users – Create User, puis le configure en l'associant à un rôle et un projet et en lui attribuant un mot de passe :

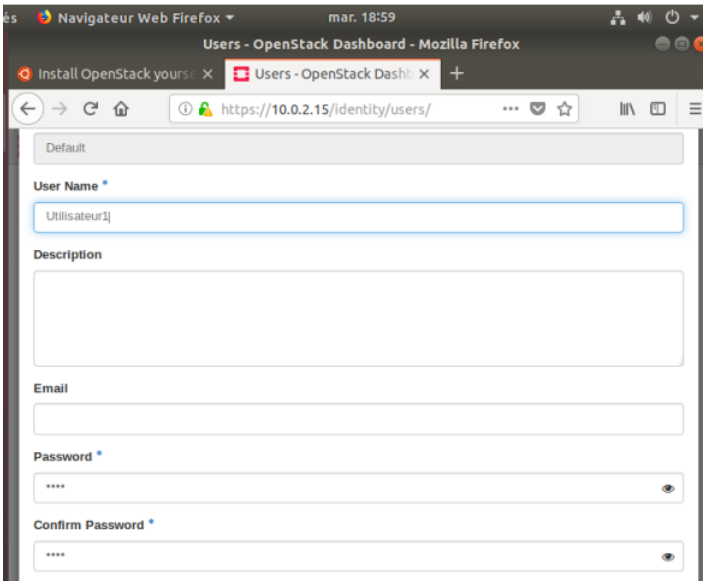


FIGURE 3.11 : Création d'un utilisateur

3.2.2 Lancement de l'instance de machine virtuelle

Création de réseaux et routeur

Maintenant, nous allons créer deux réseaux, un réseau public pour le siège officiel de la société et l'autre réseau dédié aux annexes du Ministère avec des adresses IP différentes.Puis vérifiez la possibilité de connectivité entre les deux postes en les reliant à un routeur virtuel via le Openstack Platforme. La création de se fait en suivant le chemin Admin->Réseau->Réseaux–Créer un réseau et en remplissant le formulaire selon la configuration souhaitée :

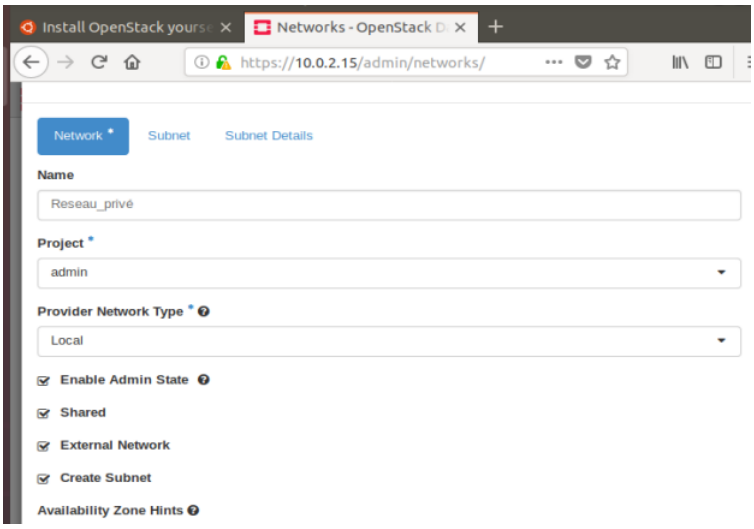


FIGURE 3.12 : Création de sous réseau

Pour passer la connexion entre les deux chaises, nous allons connecter les deux réseaux à un routeur en utilisant la commande

```
1 icrostack.openstack router create Routeur1
```

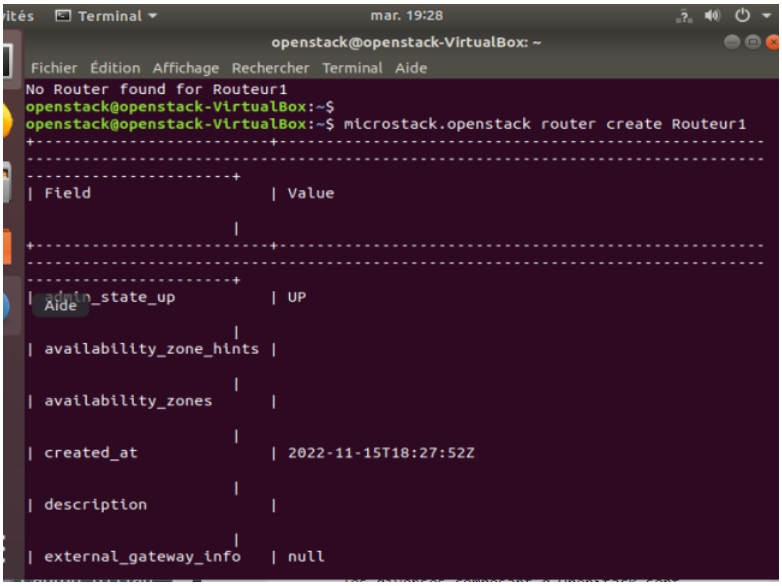


FIGURE 3.13 : Création du Routeur1

Une fois qu'ont a créé le routeur il nous faut cliqué sur le nom "Routeur1" puis sur le bouton [Interfaces] puis [ajouter des Interfaces] et il a choisi le réseau privé de l'annexe

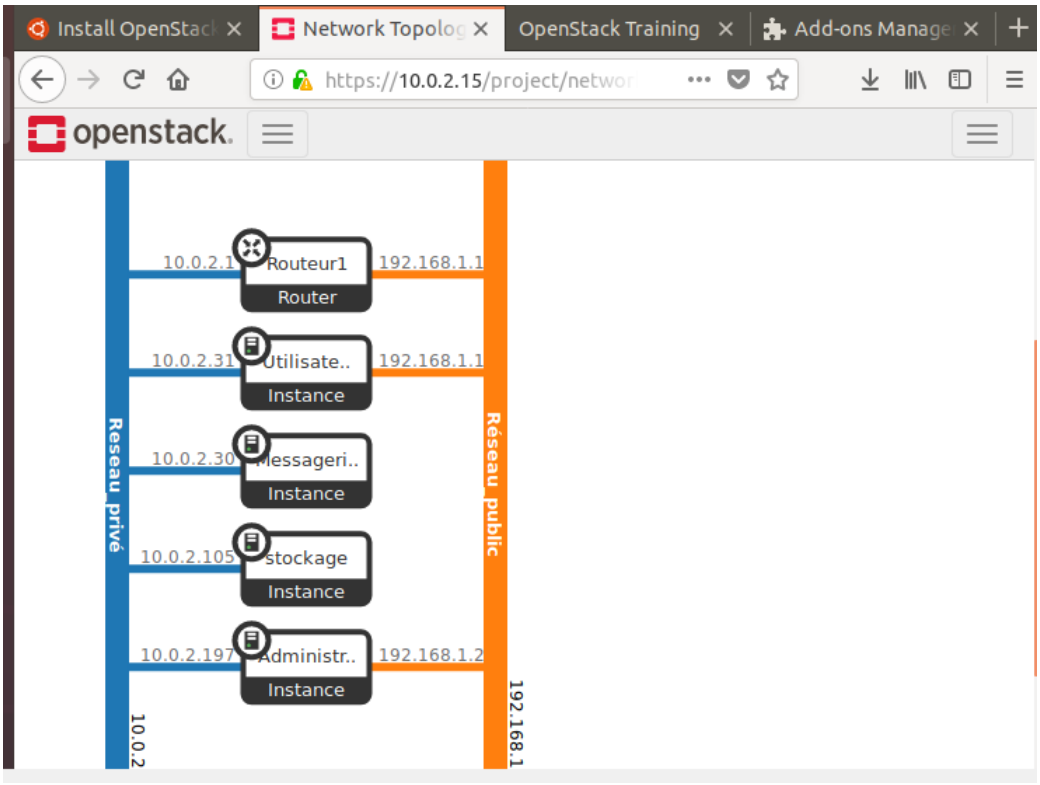


FIGURE 3.14 : Vue générale d'une partie du réseau

Ce travail pourrait être encore beaucoup plus élargir et améliorer à travers les principales perspectives qui sont :

- Mettre en place un serveur de redondance et un annuaire ;
- Penser à la solution sur un cloud privé virtuel pour réduire les coûts de matériaux ;
- Améliorer la sensibilité des ressources humaines pour renforcer la sécurité du système ;
- Élaboration de politiques de sécurité au sein de l'entreprise ;

Ces informations contribueront à améliorer le système et à accroître son efficacité. Ils contribueront également à améliorer la qualité du service et l'expérience utilisateur.

Après la mise en place du serveur l'administrateur réseau mets en place un Acces list pour contrôler qui peut avoir accès aux ressources ce qui garantie la confidentialité et la disponibilité en temps voulu.Par ailleurs les protocoles comme le HTTPS permet l'authentification ,la protection de la confidentialité et l'intégrité des données qui sont échangées .Il protège contre les attaques de l'interception et le chiffrement bidirectionnel des communications entre un client et un serveur protège les communications contre les écoutes et les falsifications.

3.2.2.1 Création d'un groupe de sécurité pour l'acces list

Un groupe de sécurité OpenStack permet aux administrateurs réseau de contrôler l'accès à leurs instances OpenStack en créant des règles spécifiques qui s'appliquent à un groupe spécifique d'instances. Les règles peuvent s'appliquer à des protocoles et des ports spécifiques et peuvent être configurées pour n'autoriser l'accès qu'à partir d'adresses IP spécifiques. Les groupes de sécurité permettent aux administrateurs réseau d'accorder ou de bloquer l'accès aux instances OpenStack en fonction des exigences de sécurité.

Pour la creation acces list sur openstack on fait comme suit :

- Connectez-vous à votre instance OpenStack avec vos informations d'identification.
- Utilisez la commande openstack security group list pour afficher la liste des groupes de sécurité existants.
- Utilisez la commande

```
1        openstack security group create [NOM_DU_GROUPE_DE_SECURITE]
```

  pour créer un nouveau groupe de sécurité.

- Utilisez la commande

```
1        openstack security group rule create [NOM_DU_GROUPE_DE_SECURITE] --protocol [PROTOCOLE] --dst-port
```

  pour créer une règle d'accès pour le nouveau groupe de sécurité.

- Utilisez la commande

```
1 nstack security group rule list  [NOM_DU_GROUPE_DE_SECURITE]
```

  pour vérifier la règle d'accès que vous avez ajoutée.

- Utilisez la commande

```
1        openstack security group rule delete [NOM_DU_GROUPE_DE_SECURITE] --protocol [PROTOCOLE] --dst-port
```

  pour supprimer la règle d'accès que vous avez ajoutée.

- Utilisez la commande

```
1        openstack security group delete [NOM_DU_GROUPE_DE_SECURITE]
```

  pour supprimer le groupe de sécurité que vous avez créé.

on obtien le resultat suivant :

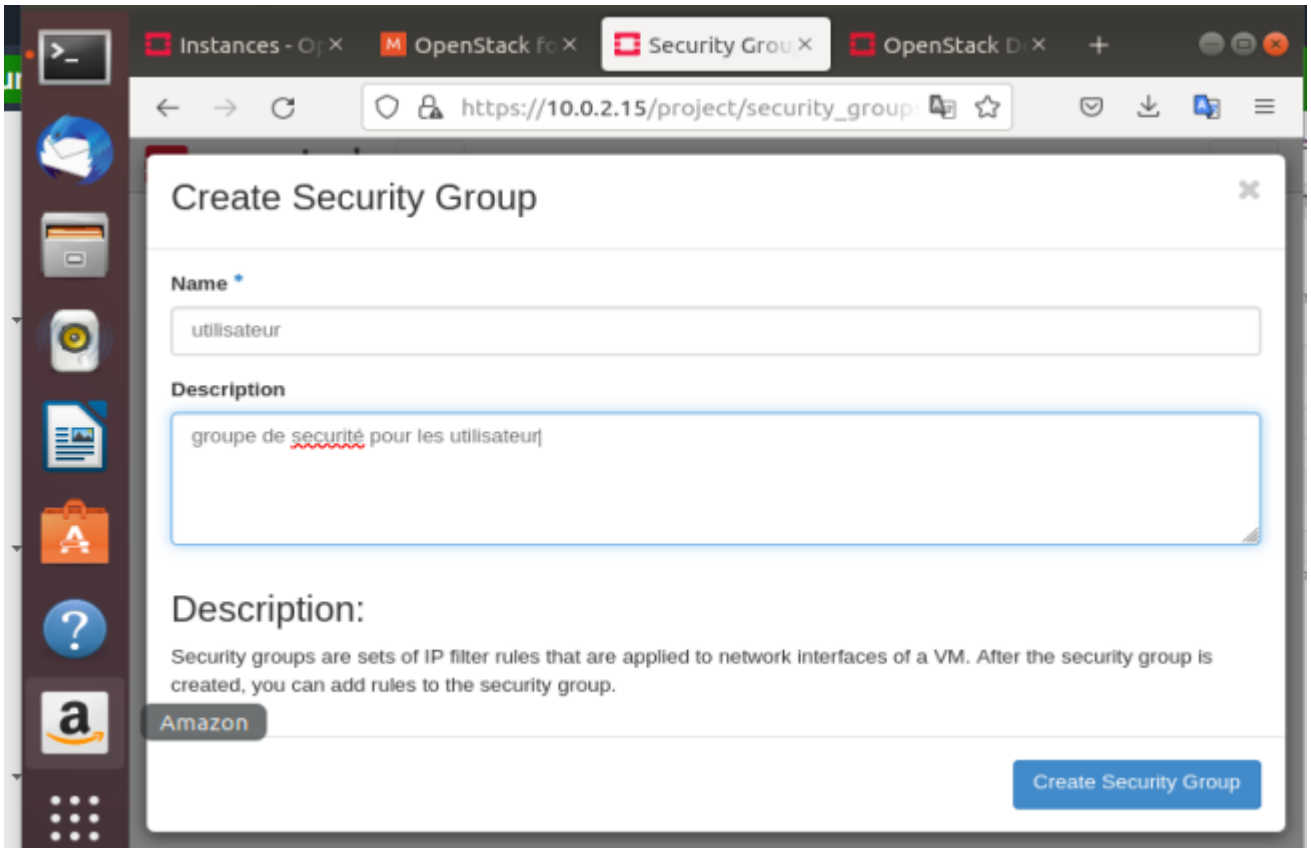


FIGURE 3.15 : Création d'un groupe de sécurité

3.2.3 les apports de Openstack au niveau de la confidentialité et de la sécurité

OpenStack offre une confidentialité et une sécurité accrues grâce à différentes caractéristiques et fonctionnalités. Ces caractéristiques et fonctionnalités incluent :

- Les rôles et les utilisateurs : OpenStack offre un contrôle des utilisateurs et des rôles qui permettent aux administrateurs de définir les autorisations et les fonctionnalités dont chaque utilisateur peut disposer.
- La sécurité du réseau : OpenStack offre une sécurité du réseau grâce à des technologies telles que le filtrage des ports et le chiffrement des données.
- Les outils de surveillance : OpenStack propose des outils de surveillance tels que Nagios et Zabbix qui surveillent les performances et l'état des services cloud.
- La sécurité des données : OpenStack offre une sécurité des données grâce à des technologies telles que le chiffrement des données et le cryptage des disques.
- Les systèmes de détection d'intrusion : OpenStack offre des systèmes de détection d'intrusion intégrés qui surveillent les activités suspectes et alerte les administrateurs en cas de détection d'une activité suspecte.
- Cryptage : OpenStack prend en charge le cryptage des données et des communications pour protéger les données sensibles.
- Surveillance : OpenStack surveille les activités des utilisateurs et des applications et génère des alertes en cas de comportements inhabituels.

- Contrôle d'accès : OpenStack fournit des contrôles d'accès aux données et aux applications, tout en offrant une authentification et une autorisation robustes pour protéger vos données.

3.2.4 Limites de l'étude

L'étude présentée dans ce document se concentre principalement sur la mise en place d'une solution cloud privé avec OpenStack, en mettant l'accent sur la conception, la planification, la mise en place pratique, la sécurité, la surveillance, la gestion des mises à jour et des évolutions, ainsi que les études de cas et retours d'expérience. Cependant, il est important de reconnaître que cette étude comporte certaines limites. Par exemple, elle ne couvre pas en détail les aspects financiers liés à la mise en place d'un cloud privé, ni n'aborde exhaustivement les implications légales et réglementaires. De plus, les recommandations présentées sont basées sur les meilleures pratiques actuelles, mais pourraient nécessiter des ajustements en fonction de l'évolution de la technologie et des exigences spécifiques des entreprises. Enfin, les limites liées à la taille et à la portée de l'étude impliquent qu'il existe d'autres aspects du cloud privé avec OpenStack qui pourraient bénéficier d'une attention supplémentaire dans le cadre de futures recherches.

Conclusion

Dans ce chapitre, nous avons établi nos fondations pour construire un cloud privé au sein d'une entreprise, grâce à ce paramètre, nous avons pu identifier les préférences de cloud et ce qui pourrait être rentable pour nous et augmenter les performances. Mais la mise en œuvre de cette technologie nécessite un matériel puissant et une prise en charge de la virtualisation avec un bon accès Internet.

Conclusion générale et perspectives

Le cloud computing est une technologie émergente et innovante qui permet la fourniture de ressources informatiques en tant que service à la demande. Accessible de n'importe où, n'importe quand et par n'importe qui. La fiabilité et la robustesse de ces services sont primordiales. A l'occasion de cet recherche, nous avons recherché et implémenté une Solution Cloud Open Source pour une entreprise, nous avons commencé par donner les définitions de base nécessaires pour comprendre le Cloud, l'architecture et ses services (IaaS, PaaS, SaaS) ainsi que différents types d'implémentations (privé, public, hybride) alors nous avons mentionné que la plate-forme du cloud est la virtualisation. Et nous avons présenté et détaillé différentes solutions de déploiement Cloud, ce qui nous permet d'avoir une idée précise et complète des solutions Cloud existantes et surtout de choisir la solution la plus adaptée pour nous. Dans notre projet, Openstack correspond le mieux à nos critères, car son objectif principal est de construire un cloud privé pur. Pour mettre en place cette solution, nous procédons à la création d'un environnement Cloud sur Openstack, cette étape est la plus longue et la plus compliquée à cause du manque d'installations et nécessite surtout une bonne connaissance du réseau Linux et des lignes de commande. Tous ces problèmes nous ont montré la complexité d'utilisation d'une des plateformes et de leurs solutions qui souvent nous retardent et nous pénalisent mais nous font trouver et essayer de nombreuses méthodes ainsi que l'expérience de travail d'un informaticien digne de ce nom qui propose des solutions à tout quel que soit la complexité du problème. Ce projet nous offre une belle opportunité d'explorer un nouvel environnement informatique complexe et vaste, nous permettant d'acquérir de l'expérience en administration système et réseau, et d'approfondir nos connaissances de l'industrie informatique en matière de virtualisation et de cloud computing.

Webographie

[1] Migration dans le cloud data integrity. , https://www.a3p.org/migration-dans-le-cloud-data-integrity/.

[2] Présentation du cloud privé virtuel. , https://cloud.google.com/vpc/docs/overview.

[3] Virtualisation : Hyperviseur. Publié le 10 Janvier 2020, https://www.redhat.com/fr/topics/virtualization/what-is-a-hypervisor.

[4] Amazon. Amazon virtual private cloud. , https://docs.aws.amazon.com/fr_fr/vpc/latest/userguide/what-is-amazon-vpc.html.

[5] Avi. modèles de services cloud - paas, saas, iaas, faas. Publié le 14 Septembre 2022, https://geekflare.com/fr/cloud-service-models/.

[6] Canonical. Openstack installation et configuration. , https://ubuntu.com/openstack/install.

[7] Sudhanshu D. Microsoft azure cloud computing services. , https://www.cisin.com/coffee-break/fr/enterprise/microsoft-azure-cloud-computing-services-how-it-helps-enterprises.html.

[8] Bastien L. Virtualisation : qu'est-ce que c'est et à quoi ça sert? Publié le 13 Mai 2019, https://www.lebigdata.fr/virtualisation-definition.

[9] Stacklima. Modèles de déploiement cloud. Publié le 5 juillet 2022, https://stacklima.com/modeles-de-deploiement-cloud/.

[10] Aina Strauss. Définition du cloud computing selon nist. Publié le 13 septembre 2022, https://www.hebergeurcloud.com/definition-cloud-computing-selon-nist/.

[11] Wikipedia. Openstack. , https://fr.wikipedia.org/wiki/OpenStack.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes 1

Introduction 2

0.1 Présentation du MDGL . . . 3

0.1.1 Attributions et Organisation . . . 3

1 Revue de littérature 4

Introduction . . . 4

1.1 Présentation du cloud computing et des services . . . 4

1.1.1 Le cloud computing . . . 4

1.2 Avantages et inconvénients du cloud computing . . . 5

1.2.1 Les Avantages de l'utilisation du cloud . . . 5

1.3 Les inconvénients du cloud . . . 6

1.3.1 Les caractéristiques du cloud . . . 6

1.3.2 Les types de déploiement du cloud . . . 7

1.3.2.1 Le Cloud public . . . 7

1.3.2.2 Le Cloud privé . . . 8

1.3.2.3 Le Cloud hybride . . . 9

1.4 Quelques services du Cloud . . . 10

1.4.1 Le IAAS . . . 10

1.4.2 Le PAAS . . . 10

1.4.3 SAAS . . . 11

1.4.3.1 Les inconvénients du cloud . . . 11

1.5 La virtualisation . . . 11

1.5.1 Les différents types de Virtualisation . . . 11

1.5.1.1 La virtualisation de stockage . . . 12

1.5.1.2 La virtualisation de réseau . . . 12

1.5.1.3 La virtualisation des postes de travail . . . 12
1.5.1.4 La virtualisation des serveurs . . . 12
1.5.2 Les Hyperviseurs . . . 13
1.5.2.1 Les hyperviseurs de type 1 . . . 13
1.5.2.2 Les hyperviseurs de types 2 . . . 13
Conclusion . . . 14

2 Analyse et choix techniques **15**
Introduction . . . 15
2.1 Pourquoi utiliser un Cloud privé ? . . . 15
2.1.1 Différence entre Cloud Privé et public . . . 15
2.1.2 Choix du cloud Privé . . . 15
2.1.2.1 Les exigences d'un cloud privé en matière de data center . . . 16
2.2 Les solutions du cloud computing public . . . 16
2.2.1 Google Cloud Virtual Private Cloud (VPC) . . . 16
2.2.2 Amazon Virtual Private Cloud (Amazon VPC) . . . 17
2.2.3 Microsoft Azure virtual private cloud . . . 17
2.3 Les solutions open source . . . 17
2.3.1 Openstack . . . 18
2.3.2 Cloudstack . . . 18
2.3.3 Eucalyptus . . . 18
2.3.4 OpenNebula . . . 18
2.3.5 Étude comparative des principales Solutions existantes . . . 19
2.4 Motivation du choix d'Openstack . . . 23
2.5 Presentation d'Openstack . . . 23
2.5.1 Presentation . . . 23
2.5.2 Modularité d'OpenStack . . . 24
2.5.2.1 Nova . . . 24
2.5.2.2 Swift . . . 24
2.5.2.3 Glance . . . 24
2.5.2.4 keystone . . . 24
2.5.2.5 Cinder . . . 24
2.5.2.6 Horizon . . . 25
2.5.2.7 Neutron . . . 25
2.5.2.8 Heat . . . 25
2.5.2.9 Ceilometer . . . 25
2.5.3 Flexibilité et Personnalisation . . . 26
2.5.4 L'architecture et les relation entre les composant de openstack . . . 26
2.5.4.1 Évolution d'OpenStack . . . 27
2.6 Confidentialité dans OpenStack . . . 27
2.6.1 Enjeux de la Confidentialité . . . 27
2.7 Mesures de Sécurité dans OpenStack . . . 28
2.7.1 Authentification et Autorisation . . . 28
2.7.2 Chiffrement des Données . . . 28
2.7.3 Politiques de Sécurité . . . 28

2.7.4 Surveillance et Audit . . . 28
2.8 Sécurité avec OpenStack . . . 28
2.8.1 Authentification et Autorisation . . . 28
2.8.1.1 Keystone : Le Gardien de l'Authentification . . . 28
2.8.1.2 Gestion des Rôles . . . 29
2.8.2 Gestion des Vulnérabilités . . . 29
2.8.2.1 Surveillance des Vulnérabilités . . . 29
2.8.2.2 Processus de Mise à Jour . . . 29
2.8.3 Surveillance et Audit de Sécurité . . . 29
2.8.3.1 Collecte de Données de Surveillance . . . 29
2.8.3.2 Journaux d'Audit . . . 29
2.8.4 Sécurisation des Réseaux . . . 30
2.8.4.1 Segmentation de Réseau . . . 30
2.8.4.2 Pare-feu et VPN . . . 30
2.8.5 Gestion des Menaces . . . 30
Conclusion . . . 30

3 Mise en place, tests et résultats **31**
Introduction . . . 31
3.1 Installation d'OpenStack . . . 31
3.1.1 Pré-requis pour installer OpenStack . . . 31
3.1.2 Installation d'openstack . . . 32
3.2 Test et Utilisation d'OpenStack . . . 34
3.2.1 Les étapes pour le mise en place du serveur . . . 35
3.2.2 Lancement de l'instance de machine virtuelle . . . 36
3.2.2.1 Création d'un groupe de sécurité pour l'acces list . . . 38
3.2.3 les apports de Openstack au niveau de la confidentialité et de la sécurité . . . 40
3.2.4 Limites de l'étude . . . 41

Conclusion **42**

Webographie **43**

Table des matières **44**