الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
المركز الجامعي لعين تموشنت
Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent
Institut de Technologie
Département de Génie Electrique

Projet de fin d'études
Pour l'obtention du diplôme de Master en :
Domaine : TECHNOLOGIE
Filière : GENIE ELECTRIQUE
Spécialité : Réseaux & Télécommunication
Thème

Etude des solutions de sécurité VMware pour le cloud computing entreprise et mise en place d'un serveur à base d'une carte raspberry pi

Présenté Par :

1) ABDELFATTAH Nadir
2) BENSAID Hanane

Devant le jury composé de :

Dr.DEBBAL Mohamed	MCB	C.U.B.B (Ain Temouchent)	Président
Dr.MERADI Abdelhafid	MCB	C.U.B.B (Ain Temouchent)	Encadrant
Dr.BEMMOUSSAT Chemseddine	MCB	C.U.B.B (Ain Temouchent)	Examinateur

Année universitaire 2018/2019

Remerciements

Au terme de ce travail, nous voudrions adresser nos sincères remerciements à Monsieur Meradi Abdelhafid pour son encadrement et ses encouragements tout au long de ce projet.
Nous tenons, également, à remercier les membres du jury
Dr.DEBBAL Mohamed et Dr BEMMOUSSAT Chemseddine
Qui ont accepté d'évaluer ce modeste travail.
Nous souhaitons témoigner notre gratitude à tous ceux qui ont contribué, de prés ou de loin à l'élaboration de ce travail.

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 soutient permanent venu de toi.

Mes frères et sœurs qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité.

Mes professeurs du centre universitaire Belhadj Bouchaib-Ain Temouchent qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

Abdelfattah Nadir
&
Bensaid Hanane

Résumé

Depuis sa naissance au début des années 70, internet est devenu le pilier de la vie professionnelle moderne, son apparition a évolué d'un réseau simple de taille limité à une infrastructure inépuisable à grandes dimensions. Alors qu'il était initialement développé pour établir une communication entre des différents ordinateurs , aujourd'hui il provoque une décentralisation de ces systèmes centraux , tout en offrant des services complexes , à la demande des utilisateurs et aux entreprises en particulier , vers la révolution d'une nouvelle tendance qu'elle s'agit du cloud computing .

Le Cloud computing est une solution économique et technologique, dans lequel les ressources informatiques sont partagées et la puissance de calcul est configurable en fonction des besoins. tel que le stockage et la gestion des applications qui peuvent être provisionnées et libérées avec un minimum effort de direction.

Cependant, La protection de la vie privée et la sécurité des données sont primordiales dans l'utilisation des applications et les services cloud, et les risques qui accompagnent leur déploiement deviennent plus complexe avec l'infrastructure de cet technologie .

Dans ce mémoire nous nous intéressons à l'étude de la sécurité et la gestion des plateformes du cloud computing, en présentant les plus récentes solutions VMware existantes dans ce domaine tel que la technologie container par docker.

Notre objectif dans ce travail est de proposer une solution d'un serveur cloud personnel déployé à partir de l'infrastructure de gestion docker tout en intégrant un système de sécurité honeypot conceptionnel à l'aide d'une carte raspberry pi.

Mots clés : cloud computing,VMware, container, docker, honeypot , raspberry pi.

Abstract

Since its birth in the 1970's, the Internet has become the pillar of the modern professional life, its emergence has went from being a simple network with a limited size to becoming an endless infrastructure with great dimensions.Though it was initially developped to establish a communication between different computers, today it induces a decentralization of these cetral systems, by offering complexed services, by demand from the user or the enterprise in particular,towards a revolution of a new trend that is the cloud computing.

The cloud computing is an economical and technological solution, in which data processing resources are shared and computing power is configurable in term of needs, such as storage and app management that can be previsioned and released with a minimum direction effort.

However, the protection of private life and data security are premordial when using cloud services and apps, and the risks that come with their deployment become more complexed with the infrastructure of this technologie.

In this memorandum we are interested by the study of the security and management of the platforms of cloud computing, by presenting the most recent solutions VMware existing in this field such as the container technology by docker.

Our objective in this work is to propose a solution : a personal cloud server deployed from the Infrastructure of the docker management by integrating a conceptional honeypot security system by the help of a raspberry pi card.

KEY WORS : cloud computing , VMware , container, docker, honeypot , raspberry pi.

ملخص

منذ نشأتها في أوائل السبعينيات ، أصبحت الإنترنت الدعامة الأساسية للحياة المهنية الحديثة ، تطور مظهرها من شبكة بسيطة من حجم محدود إلى بنية تحتية لا تنضب مع أبعاد كبيرة. في حين تم تطويرها في الأصل لتأسيس اتصال بين أجهزة كمبيوتر مختلفة ، واليوم تسببت في لامركزية هذه الأنظمة ، مع تقديم خدمات معقدة لطلب المستخدمين والشركات على وجه الخصوص ، نحو ثورة جديدة الاتجاه و التي تتمثل في الحوسبة السحابية.

الحوسبة السحابية هي الحل الاقتصادي والتكنولوجي ،و التي عبرها تتم مشاركة الموارد, وقوة الحساب مبرمجة حسب الاحتياجات . مثل تخزين وإدارة التطبيقات التي يمكن أن تكون مشروطة و مقدمة مع الحد الأدنى من الجهد الإداري. ومع ذلك ، فإن حماية الخصوصية وأمن البيانات أمر بالغ الأهمية في استخدام التطبيقات والخدمات السحابية والمخاطر التي تصاحبها تصبح أكثر تعقيدا مع البنية التحتية لهذه التكنولوجيا.

في هذه المذكرة نحن مهتمون بدراسة الأمن وإدارة منصات الحوسبة السحابية ، التي تقدم أحدث حلول الافتراضية الموجودة في هذا المجال مثل تكنولوجية الدوكر.
هدفنا في هذا العمل هو اقتراح حل تطبيقي لسيرفر سحابة شخصي مبرمج بطريقة البنية التحتية لدوكر مع ادماج نظام حماية Honeypot و يعني بالإنجليزية قدر العسل أو مصائد مخترقي الشبكات بواسطة ادات راسبيري باي.

الكلمات المفتاحية : الحوسبة السحابية ,الافتراضية, الحاوية , دوكر , قدر العسل

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Liste des figures

Liste des figures

Liste Des Tableaux

ACRONYMES

ADT :	Abstract data type
AmazonEC2 :	Amazon Elastic Compute Cloud
Amazon S3 :	Amazon Simple Storage Service
AMD :	Advanced Micro Devices
ARM :	Advanced Risk Machine
AoE :	Age of Empires
API :	Application programming interface
ARP :	Address Resolution Protocol
Cap Ex :	Capital expenditure
CC :	Contrôleur de cluster
CLC :	Contrôleur de nuage
CLI :	Command-line interface
CSA :	Cloud Security Alliance)
DDoS :	Distributed denial of service
Dfs :	Distributed filesystem
DHCP :	Dynamic Host Configuration Protocol
DNS :	Domain Name System
DDNS :	Dynamic DNS
DNSSEC :	Domain Name System Security Extensions
DoS :	Denial of Service
FTP :	File Transfer Protocol
HDMI :	High-Definition Multimedia Interface
HTML :	HyperText Mark-Up Language
HTTPS :	Hypertext Transfer Protocol Secure ou protocole de transfert hypertexte sécurisé
IaaS :	Infrastructure as a Service
IBM :	International Business Machines
IP :	Internet Protocol
IRC :	Internet Relay Chat
ISACA :	Information Systems Audit and Control Association)
iSCSI :	Internet Small Computer System Interface
IT :	Information Technology
KVM :	Kernel-based Virtual Machine
LDAP :	Lightweight Directory Access Protocol
LE :	Let's Encrypt
MITM :	Man in the Middle
NAS :	Network Attached Storage
NC :	Contrôleur de noeud
NES :	Nintendo Entertainment System
NIST :	National Institute of Standards and Technology
Op Ex :	Operational expenditure
OS :	Operating System
PaaS :	Platform as a Service
Pc :	Personal Computer
PME :	Petites et les moyennes entreprises
REST :	Representational state transfer
RFB :	Remote Frame Buffer
SaaS :	Software as a Service
SAN :	Storage Area Network

ACRONYMES

SC :	Contrôleur de stockage
SD	Secure Digital
SET :	Social engineering Toolkit
SLA :	Service Level Agreement
SMB :	Serveur Message Block
SQL :	Structured Query Language
SSH :	Secure shell
SSI :	La sécurité des systèmes d'information
SSL:	Secure Socket Layer
ST :	Sixteen/Thirty-two
TLS :	Transport Layer Security
URL :	Uniform Resource Locator
USB :	Universal Serial Bus
VE :	Virtual Environment
VLAN :	Virtual local area network
VM :	Machines virtuelles
VNC :	Virtual Network Computing
VPC :	Virtual Private Cloud
VPN :	Virtual Private Network
VPS :	Virtual Private Server
WINS :	Windows Internet Name Service
WSRF :	Web Services Resource Framework
WS3 :	Contrôleur de stockage Walrus
WWW :	World Wide Web

Introduction Générale

Introduction Générale

De nos jours, l'accès à l'information à tout moment et à travers les différents types d'appareils électroniques (téléphones mobiles, tablettes, ordinateurs portables ou bureautiques,…etc) via internet, qui, au fil des années est devenu un outil incontournable.

Cette connexion internet nous offre des services très attachants comme l'accès aux différents réseaux sociaux, les services bancaires permettant à effectuer des achats et des ventes ou d'autres fonctions en ligne. Cependant, l'accès aux différentes fonctionnalités de l'internet demande un espace de stockage considérable et une protection des données sensibles. Toutefois, ces paramètres sont devenus plus important que l'accès à l'information même.

La nécessité de stocker, traiter et analyser de grandes quantités de données a conduit de nombreuses organisations et entreprises mais aussi les individus à adopter le Cloud Computing, Ce dernier représente une révolution extraordinaire dans le domaine de l'informatique, assurant ainsi une restructuration inévitable des systèmes d'information et offre des capacités évolutives en matière de traitement de l'information.

Cependant, la sécurité des données en transit dans un Cloud public reste un challenge pour les fournisseurs de Cloud. En effet, ces données sont la cible de plusieurs attaques réseau, qui ont pour but d'interrompre, d'intercepter, de modifier et voler des informations. Par conséquent, il est essentiel de faire face à ces attaques en vue d'améliorer l'utilisation et l'adoption de Cloud.

Dans notre travail nous présentons une étude sur la conception et la sécurisation d'un cloud personnel en s'inspirant sur de nouvelles approches dans ce domaine.

Organisation de mémoire :

Chapitre I :

-Ce chapitre explicite les notions fondamentales, le mécanisme et les différents services du cloud computing, ainsi des généralités à propos de la virtualisation.

Chapitre II:

-Ce chapitre présente les différentes attaques et vulnérabilités du cloud avec leurs solutions de sécurité à travers des infrastructures et des plateformes existantes.

Chapitre III :

-Ce chapitre représente la nouvelle tendance de conteneurisation et ses nouveau modèles de solutions Vmware tel que docker et redhat.

Chapitre IV :

-Enfin dans ce dernier chapitre, nous présentons notre solution de simulation d'un fournisseur de service Cloud avec la conception d'un serveur cloud personnel open source doté d'une protection chiffrée avec un système de sécurité honeypot.

Finalement, nous finissons ce travail par une conclusion générale, avec de futures perspectives.

Introduction Générale

Finalement, nous finissons ce travail par une conclusion générale, avec de futures perspectives.

Chapitre I :

Généralités sur le cloud computing

I.1. Introduction

La croissance continuelle des coûts dus soit à la mise en place d'un système informatique ou due à la maintenance des équipements utilisés poussent bons nombres d'organismes à se tourner vers cette technologie appelée le cloud computing. Le sujet sur le cloud computing attire de plus en plus l'intérêt de plusieurs institutions spécialisées dans divers domaines d'activité car cette technologie leur offre un grand nombre d'avantages.

De nos jours, le cloud computing est un sujet phare dans le domaine des systèmes d'information et de communication. De nombreuse entreprises y voient un moyen pour améliorer leur performance, agilité et de gérer les coûts des systèmes d'information plus paisiblement. La disponibilité des services en ligne donne le moyen de s'approprier l'équipement informatique mais de payer les frais en fonctions de l'utilisation. Avec son modèle informatique elle offre la modularité des ressources informatiques, en termes de volume et en temps [1]. La question que nous nous posons donc est de savoir qu'est-ce que le cloud computing ?

I.2. Historique

Le concept de Cloud Computing est loin d'être nouveau. On en trouve les premières traces dans les années 1960, quand John McCarthy affirmait que cette puissance de traitement informatique serait accessible au public dans le futur. La première utilisation de l'expression « Cloud Computing » remonte à 1997, lorsque Ramnath Chellappa, professeur en systèmes d'information et en management, l'a utilisee pour decrire un nouveau modèle de gestion de l'informatique, dans lequel les limites ne seraient plus définies par des problématiques techniques mais par des choix économiques. L'intérêt de ce modèle réside notamment dans la transition d'une partie des coûts informatiques du Cap Ex vers l'Op Ex.

En 2002, Amazon lance le premier service clairement estampille « Cloud Computing ». Le leader de la vente de livres en ligne avait en effet investi dans un parc de serveurs largement surdimensionnés, capable d'absorber les pics de charge des commandes des fêtes de fin d'année. Ce parc de serveurs étant sous utilisé le reste de l'année, le cybercommerçant a alors eu l'idée de louer de la capacité de calcul inutilisée à d'autres entreprises afin de rentabiliser son investissement.

Le terme « Cloud Computing »sera rendu populaire en 2006 par le directeur exécutif de Google, Eric Schmidt, qui qualifiait ainsi le déport vers « le nuage Internet »de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers [2].

I.3. Définition

L'origine du terme cloud Computing est traduit littéralement par « informatique dans les nuages », ces nuages faisant référence à Internet et au web.

Le cloud Computing signifie donc que les ressources en ligne sont utilisées comme si elles étaient situées dans l'éther (figure I.1), dans un espace sans réalité physique. Certains acteurs du monde du cloud Computing jouent d'ailleurs sur cette immatérialité : ainsi Google entretient un certain mystère autour de l'emplacement de ses centres de données ou Datacenters [3].

Figure (I.1) : Cloud computing [4].

I.3.A. D'après Numergy :

« Le Cloud Computing (que l'on appelle aussi en France le nuage informatique) fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (Smartphone, PC de bureau, ordinateur portable et tablette). Pour être plus précis, le Cloud Computing permet de partager, chez un fournisseur d'offres Cloud, une infrastructure, une solution applicative ou encore une plateforme à tout utilisateur qui en fait la demande via un simple site internet (aussi appelé portail) en libre-service».

I.3.B. D'après NIST (National Institute of Standards and Technology):

« Le Cloud Computing est l'ensemble des disciplines, pratiques, technologies et modèles commerciaux utilisés pour délivrer comme un service à la demande et par le réseau des capacités informatiques (logiciels, plateformes, matériels) » [5].

I.3.C. D'après CISCO :

Pour CISCO 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. [CISCO 2009] [6].

Donc le Cloud Computing 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, accessible de n'importe où, n'importe quand et par n'importe qui.

I.4. Eléments constitutifs du cloud computing:

Les éléments pouvant constitué le système cloud sont les suivants :

I.4.A. Infrastructure:

L'infrastructure informatique du Cloud est un assemblage de serveurs, d'espaces de stockage et de composants réseau organisés de manière à permettre une croissance incrémentale supérieure à celle que l'on obtient avec les infrastructures classiques. Ces composants doivent être sélectionnés pour leur capacité à répondre aux exigences d'extensibilité, d'efficacité, de robustesse et de sécurité.

Les serveurs d'entreprise classiques ne disposent pas des capacités réseau, de la fiabilité ni des autres qualités nécessaires pour satisfaire efficacement et de manière sécurisée les accords de niveau de service SLA (service level agreement). Par ailleurs, les serveurs d'un Cloud affichent des coûts de fonctionnement moins élevés et ils peuvent être plus fiables s'ils ne sont pas tous équipés de disques internes [7].

I.4.B. Virtualisation:

La virtualisation est la principale technologie dans Cloud, est une manière pour partition un ressource physique en plusieurs ressources virtuelles, par exemple: un serveur, un espace de stockage ou un réseau lors de la création des machines virtuelles.

Elle permet intégrer les différentes serveurs en façons plus flexible pour facilite l'utilisation. Le but du virtualisation est faire la transparence d'utilisation et efficacité l'exploitation des ressources, d'assurer le fonctionnement des différents services et la séparation entre de multiples locataires (utilisateurs) impliqués dans d'un matériel physique [7].

I.4.C. Interfaces de service:

L'interface de service placée entre le fournisseur et le client est un élément de différenciation du Cloud. Elle représente un contrat qui fait respecter la proposition de valeur décrite par des SLA et des conditions tarifaires. Si le Cloud semble nouveau, c'est principalement en raison de cette interface. Elle représente la valeur d'un fournisseur et sert de base à la concurrence. Par l'ajout d'interfaces de libre service, nous obtenons d'autres optimisations. Les clients du Cloud sont en mesure d'engager des ressources de manière automatisée sans que le service informatique soit un obstacle. L'espace de stockage et les ressources sont présentés au travers d'une interface graphique que l'utilisateur peut manipuler de manière à obtenir et à instancier une infrastructure informatique virtuelle. Un navigateur web ou une carte bancaire à titre d'exemple [7].

I.4.D. Centre de données (Datacenter):

Un centre de traitement de données en anglais « data centre » est un site physique sur lequel se regroupés des équipements constituants du système d'information de l'entreprise (mainframes, serveurs baies de stockage, équipements réseaux et de télécommunications, etc.), Comme le montre la figue ci-dessous. Il peut être interne ou externe à l'entreprise, exploité ou non avec le soutien de prestataires.

Figure (I.2) : Data center [8].

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 utilisé 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 [9].

I.5. Principales caractéristiques

Les principales caractéristiques de l'informatique en nuage déterminées par le NIST dans «The Nist definition of cloud computing »:

- **Service à la demande :** Les services sont fournis au client automatiquement et sans intervention humaine.
- **Élasticité rapide :** Le stockage, la puissance computationnelle peuvent être rapidement ajustés, parfois systématiquement en fonction des besoins immédiats de chaque client.
- **Mise en commun des ressources :** Les différents utilisateurs bénéficient de ressources de serveurs alloués de manière dynamique et rapide dans le cadre d'un modèle de cloud communautaire.
- **Résilience :** Le cloud computing se doit d'apporter des mécanismes hétérogènes où les technologies présentes supportent une multitude de clients légers

(ordiphones, tablettes) et de clients lourds (ordinateurs).

- **Paiement à l'utilisation :** Les services se facturent en fonction de l'utilisation des ressources et en toute transparence Pour le client et le fournisseur de services en nuage [10].

I.6. Les Modèles de déploiement de Cloud Computing

On peut distingue quatre type principaux dans le Cloud sont : le Cloud privé, le Cloud public, le Cloud hybride (Mixte) et le Cloud communautaire, nous allons expliquer chaque type en détaille.

I.6.A. Cloud privé:

En anglais **"** Private Cloud **"** est un ensemble des services et des ressources disponible à un seul client par exemple un entreprise, le Cloud privé peut être géré par l'entreprise elle-même**,** ou bien avec sa branches, dans ce cas il s'appel "Le Cloud privé Interne", en d'autre façons il peut être géré par un prestataire externe qu'il est louée par l'entreprise, dans ce cas s'appel "Le Cloud privé Externe ", qu'il accessible via des réseaux sécurisés de type VPN (Virtual Private Network), par exemple Amazon Virtual Private Cloud (Amazon VPC).

I.6.B. Cloud public:

En anglais "Public Cloud" est un ensemble des services et des ressources accessibles par Internet et géré par un prestataire externe, ces ressources et services sont partagés entre plusieurs clients, qu'ils les utilisent à la demande et à tout moment sans savoir où elles existent, aussi ces services peuvent être gratuits ou payants.

On cas les services sont payants, il existe des contrats SLA (Service Level Agreement) entre les clients et les fournisseurs, SLA est un document qui définit la qualité de service requise entre les deux. Quelques exemples de Cloud public: Amazon Elastic Compute Cloud (EC2) et Amazon S3, Sun Cloud, IBM’s Blue Cloud, Google AppEngine et Windows Azure Services Platform [11].

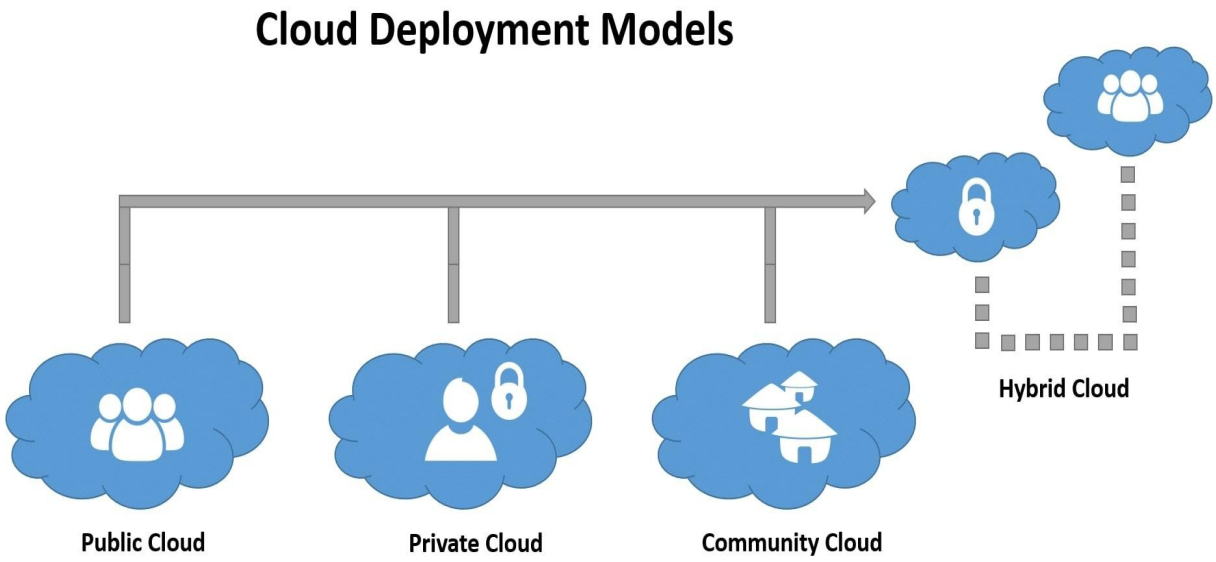
I.6.C. Cloud communautaire :

En anglais " Cloud Community" est un ensemble des infrastructures, qu'ils permettent à plusieurs clients ou organisations de partager les différentes ressources, ces ressources sont généralement spéciale à des organisations, ce type de Cloud peut être géré par ces organisation elles-mêmes ou par des fournisseurs externes.

Aussi il permet à un groupe des utilisateurs à créer leur propre Cloud avec des caractéristiques de Cloud privé tel que la sécurité, ressources dédiées et un coût réduit.

I.6.D. Cloud hybride :

En anglais " Hybrid Cloud" est une composition de deux types de Cloud Privé et public comme Par exemple l'utilisation des applications dans un Cloud public mais ces applications nécessitent des données stockées sur un Cloud privé [12].



Figure(I.3) : les modèles de déploiements du cloud computing [13].

I.7. Avantages et inconvénients du cloud par types:

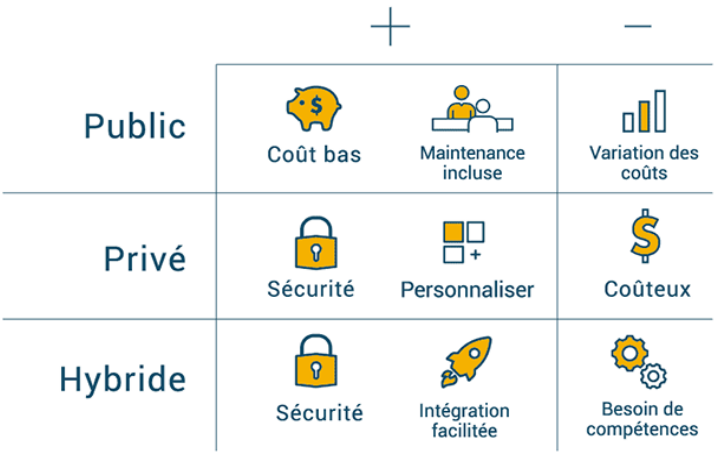


Tableau (I.1) : Avantages et inconvénients du cloud par types [14].

I.8. Les modèles des services 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).

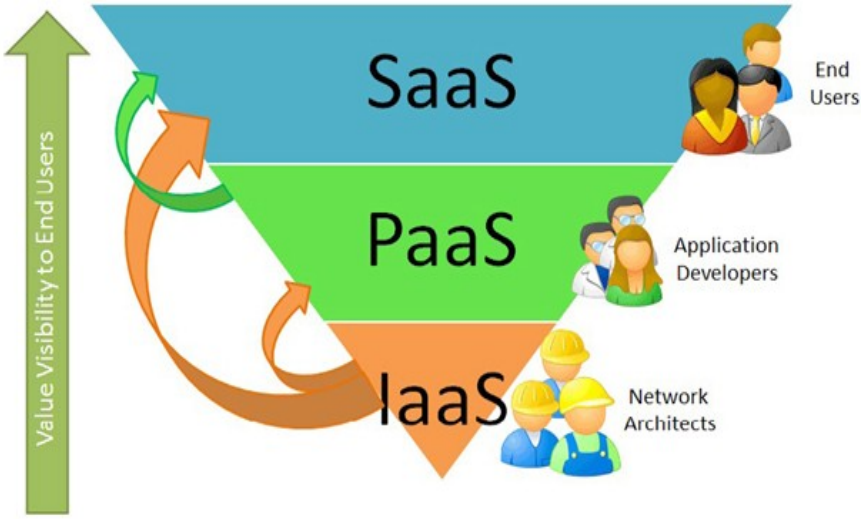


Figure (I.4): Les couches du Cloud computing [15].

La Figure ci-dessus 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 logicielle comme un service (SaaS) est le « produit final » pour les utilisateurs.

I.8.A. SAAS :

L'acronyme « SAAS » est le plus connu dans le monde du Cloud Computing. Sa signification est « Software as a Service », autrement dit, application en tant que service, c'est un modèle de déploiement d'application dans lequel un fournisseur loue une application clé en main à ses clients en tant que service à la demande au lieu de leur facturer des licences.

De cette façon, l'utilisateur final n'a plus besoin d'installer tous les logiciels existants sur sa machine de travail. Cela réduit également la maintenance en supprimant le besoin de mettre à jour les applications. Ce type de modèle transforme les budgets logiciels en dépenses variables et non plus

fixes et il n'est plus nécessaire d'acquérir une version du logiciel pour chaque personne au sein de l'entreprise [16].

I.8.B. PAAS :

Le PAAS qui signifie « Platform as a Service » est une architecture composée de tous les éléments nécessaires pour soutenir la construction, la livraison, le déploiement et le cycle de vie complet des applications et des services exclusivement disponibles à partir d'internet. Elle est également connue sous le nom de « CloudWare ».

Le PAAS offre des facilités à gérer le déroulement des opérations lors de la conception, du développement, du test, du déploiement et de l'hébergement d'applications web à travers des outils et des services tels que :

- Le travail collaboratif (« team collaboration »).
- L'intégration des services web et bases de données.

Ces services sont fournis au travers une solution complète destinée aux développeurs et disponible immédiatement via l'internet [16].

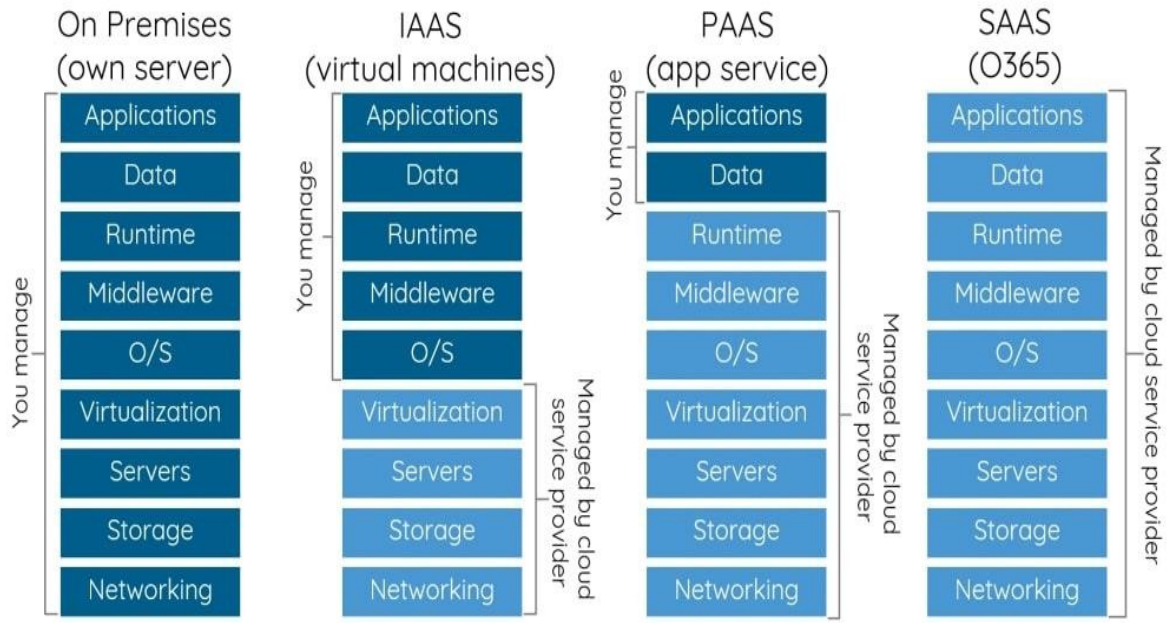
I.8.C. IAAS :

L'IAAS (Infrastructure as a Service) est un modèle qui permet de fournir des infrastructures informatiques en tant que service. Ce terme était originellement connu sous le nom de (Hardware as a Service).Ces infrastructures virtuelles composent un des domaines du « As a Service » en empruntant la même philosophie de fonctionnement et de tarification que la plupart des services du Cloud Computing.

Plutôt que d'acheter des serveurs, des logiciels, et l'espace dans un centre de traitement de données et/ou de l'équipement réseau, les clients n'ont plus qu'à louer les ressources auprès des prestataires de service. Le service est alors typiquement tarifé en fonction de l'utilisation et de la quantité des ressources consommées.

De ce fait, le coût reflète typiquement le niveau d'activité de chaque client. C'est une évolution de l'hébergement Internet qui se différencie des anciens modes de fonctionnement, on distingue :

- Hébergement mutualité : une machine pour plusieurs clients, gérée par un prestataire de service et dont les clients payent le même prix peu importe leur utilisation.
- Hébergement dédié : une machine pour un client, gérée le plus souvent par le client lui même et pour laquelle le client paye le même prix chaque mois peu importe son utilisation.
- Infrastructure as a Service : un nombre indéfini de machines pour un nombre indéfini des clients, dont les ressources sont combinées et partagées pour tous les clients. Chaque client paye en fonction de son utilisation de l'architecture [16].



Figure(I.5) : Répartition des charges [17].

I.9. Avantages et Inconvénients des services:

	Avantages	Inconvénients
Saas	➢ Pas d'installation ➢ Plus de licence ➢ Migration ➢ Accessible via un abonnement	➢ Logiciel limité ➢ Sécurité ➢ Dépendance de prestataire
Paas	➢ Pas d'infrastructure nécessaire ➢ Pas d'installation ➢ Environnement hétérogène	➢ Limitation des langages ➢ Pas de personnalisation dans la configuration des machines virtuelles
Iaas	➢ Administration ➢ Personnalisation ➢ Flexibilité d'utilisation ➢ Capacité de stockage infini	➢ Sécurité ➢ Besoin d'un administrateur système ➢ Demande pour les acteurs du cloud des investissements très élevés

Tableau (I.2) : Avantages et Inconvénients des services [18].

I.10. Avantages et Inconvénients du Cloud Computing

I.10.A. Les avantages du Cloud Computing

Le Cloud présente de nombreux avantages :

- Possibilité de partager ses contenus avec son réseau personnel.
- Possibilité de partager les ressources.

- Redondance de stockage de données en cas un disque dur tombe en panne, les données restent en sécurité et disponibles automatiquement sur un autre disque.
- Possibilité de spécifier des ressources.
- Aucune défaillance : est signifie qu'il n'ya ni de problèmes de matériel, ni de logiciel de la technologie.
- Dans Cloud où chaque utilisateur peut être isolé dans son propre environnement.
- Plus flexible.
- Augmente la collaboration.
- Mobilité : l'utilisateur peut à tout moment et à partir de n'importe quel appareil se connecter à ses applications (Any where - any time).
- Contrôle des coûts.

I.10.B. Les inconvénients de Cloud Computing:

- L'accès au Cloud passe nécessairement par une connexion internet : par conséquent, si votre connexion est coupée, momentanément ou durablement, vous n'avez plus accès à vos documents ou service.
- Sécurité : la plateforme Cloud, si elle est externe (non installée sur le réseau interne ou avec une ouverture extérieure) doit être suffisamment sécurisée pour éviter le risque d'intrusion, de vol des données par piratage [19].

I.11. Les fournisseurs du cloud computing:

Les fournisseurs de cloud sont des entreprises qui proposent des infrastructures, des plateformes et/ou des logiciels via un réseau. Ces services sont souvent regroupés dans le cloud, c'est-à-dire un pool de ressources virtuelles orchestrées par des logiciels de gestion et d'automatisation et accessibles à la demande via des portails en libre-service. Ces ressources sont redimensionnées automatiquement et allouées de façon dynamique. Un fournisseur de cloud vous permet de proposer des services informatiques que vous devriez sinon fournir vous-même.

- **Microsoft** : le leader du marché cloud computing en termes de revenus.

Figure (I.6) : Logo du Microsoft [20]

- **Amazon :** le doyen du marché cloud computing.

Figure(I.7) : Logo d'Amazon [21].

- **Google :** le géant du web et maintenant du cloud.

Figure (I. 8) : Logo du Google cloud [22].

- **IBM :** une transition réussie vers le marché cloud computing.

Figure (I.9) : Logo de l'IBM [23].

I.12. Différence fondamentale entre le service internet et le cloud computing:

Bien qu'assez similaire dans leur représentation et leur façon de fonctionner, les services Internet et les services Cloud Computing sont assez différents.Internet est bien plus ancien que le Cloud Computing. C'est grâce à Internet que le développement du Cloud Computing a été aussi rapide. En effet, on peut parler d'internet sans Cloud Computing, mais on ne peut pas parler de Cloud Computing sans Internet.

Internet est le moyen le plus utilisé par les fournisseurs de solution de Cloud Computing pour proposer leur service. Mais, internet peut être dans certains cas substitué à tout autre réseau (intranet, réseau téléphonique) comme nous le verrons dans la suite [24].

I.13. Le 100% Cloud dans les entreprises : une réalité dans un futur proche :

La grande majorité des entreprises considère l'adoption du Cloud computing comme étant essentielle à leur réussite à long terme et comme un outil efficace pour la mise en place de leur stratégie de développement. Pourtant, elles sont très nombreuses à affirmer qu'elles ne seront jamais à 100% dans le nuage. Alors, la généralisation du Cloud, info ou intox ?.

Avant le Cloud, les entreprises devaient acheter un serveur pour stocker leurs données et développent Leur propre infrastructure pour héberger leurs services, leurs applications. La mise en place de ces installations générait une perte de temps et d'argent. Les solutions Cloud offrent **plus de souplesse** aux entreprises tout en étant **plus économiques**. Elles permettent d'exploiter des services et des données en lignes via un simple navigateur web, 24h sur 24. Les entreprises tirent profit de cette technologie notamment pour l'hébergement, le développement et le déploiement rapide de nouvelles applications [25].

I.14. Comment le cloud révolutionne les entreprises de toutes les industries?

Depuis maintenant quelques années, le cloud transforme littéralement toutes les industries. Le modèle économique, la façon dont les services et logiciels sont créés et vendus, mais également la manière dont les entreprises fonctionnent sont en pleine transformation. Découvrez comment le cloud transforme les entreprises de toutes les industries [26].

Penchons-nous sur les services informatiques suivants :

- Le courrier électronique (Gmail, Hotmail, Yahoo…).
- Les sites Internet (portail et pages Web d'entreprise…).
- Les réseaux sociaux (Facebook, Twitter…).
- Les outils de productivité en ligne (Office 365, Google Apps…).

- Les services de stockage et sauvegarde en ligne (Dropbox, YouSendIt, Google Drive, SafeSync…).

Si une de ces technologies est utilisée dans votre société, c'est que vous profitez déjà des avantages du Cloud. Tous ces services capitalisent peu ou prou sur le Cloud pour satisfaire aux demandes de ses utilisateurs.

I.15. Le cloud, un moyen d'augmenter la notoriété des PME

Le Cloud computing n'est pas seulement un moyen de gérer des ressources internes mais va aussi permettre à une marque d'augmenter sa notoriété sur le web. Une petite entreprise, qui a un budget restreint pour financer son site Internet, ne pourra pas bénéficier d'un serveur dédié très puissant. Cela aura de fâcheuses conséquences sur la performance de la bande passante et provoquera certainement des encombrements. Quelle erreur stratégique ! Se faire connaître va être l'un des premiers objectifs pour une petite entreprise. Si les clients potentiels sont bloqués dès leur première visite, l'image perçue ne pourra qu'être mauvaise. Le Cloud computing va permettre d'y remédier et donner la possibilité à des petites structures de posséder un site efficace grâce à un hébergement mutualisé. Les sites seront capables d'accueillir de nombreux visiteurs, et les entreprises de réduire leurs coûts. Les internautes satisfaits pourront alors véhiculer une image positive de cette jeune marque. La loi du référencement naturel fera le reste, plus il y aura de visites, plus le site remontera dans les moteurs de recherche. La notoriété de l'entreprise augmentera alors [27].

I.16. Le cloud, une stratégie pour augmenter la performance des petites entreprises:

Le Cloud computing est aujourd'hui une vraie révolution et une bonne opportunité pour les entreprises, en particulier les plus petites. L'ensemble de leur système d'exploitation est pris en charge par des prestataires externes, impliquant des réductions budgétaires remarquables. Que ce soit l'hébergement, les logiciels, la bande Passante… tout est géré en externe sous forme de location.

Ce concept est très intéressant car les avantages sont nombreux. Le Cloud computing permet :

- Extensibilité et adaptabilité, nul besoin d'anticiper les ressources nécessaires, il décharge les entreprises de toute logistique, maintenance, mises à jour et permet un important stockage de données.
- Virtualisation et mobilité, peu importe le lieu où l'on se trouve, un simple navigateur et une connexion Internet suffisent pour retrouver sa session et ses documents.
- Mutualisation et réduction des coûts, la consommation est gérée par mutualisation, plus besoin d'investissement lourd dans du personnel compétent ou dans du matériel rapidement obsolète.

Là est la véritable opportunité pour une petite structure. Les serveurs deviennent virtuels, les entreprises ne payent que ce qu'elles utilisent réellement, comme elles le feraient avec leur

consommation électrique. Plus de problèmes techniques ou d'encombrements, les entreprises sont plus performantes face à la concurrence et bénéficient des mêmes ressources que les plus grandes.

Ce concept rentre vraiment dans la stratégie de développement, de compétitivité et de pérennisation des entreprises [27].

I.17.Conclusion

Au cours de cette première partie nous avons fourni une étude théorique sur l'état de l'art du cloud computing en arborant ses types, ses modèles de services (Iaas, Paas, Saas), ses éléments constitutifs,ainsi ses avantages et ses inconvénients.

Le cloud computing apparait donc comme une solution innovante, mais malgré ses avantages la sécurité des données reste un débat pour ses fournisseurs, et c'est ce qu'on va découvrir dans le chapitre suivant.

Références chapitre I

[1] Laribi, I. Etude et mise en place d'une solution cloudcomputing privée pour une entreprise (Doctoral dissertation).

[2] http:// connect.ed-diamond.com/MISC/MISC-060/Introduction-aucloudcomputing-risques-et-enjeux-pour-la-vie-privee,Juin 2017.

[3] Plouin, G. (2016). Cloud computing, 4e ed: Sécurité, gouvernance du SI hybride et panorama du marché. Dunod

[4] http://www.ipsoconsulta.it/

[5] URL : http://communication.sysdis.fr/2012/05/09/cloud-computing-dfinitions-etnotions-de-base/, Consulté le 01.04.2013.

[6] Akbi, k & Zehri, M**. (2013).** Etude et mise en place d'une solution cloud computing privé : Mémoire master en Informatique Fondamentale, au sein de l'université de ouargla.

[7] Winkler, J. R., & Soulard, H. (2011). La sécurité dans le Cloud:[techniques pour une informatique en nuage sécurisée]. Pearson.

[8] https://www.istockphoto.com/fr/photo/moniteur-terminal-dans-la-salle-des-serveurs-avec-des-racks-de-serveurs-dans-le-gm845069958-138261331

[9] Noumsi, L. F. (2012). Etude et mise en place d'une solution" cloud computing" privée dans une entreprise moderne: cas de CAMTEL. Mémoire ingénieur, Ecole nationale supérieure des postes et télécommunications-*Paris*.

[10] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. ([M13589.PDF] thèse du doctorat)

[11] Kuhn, A. L. Cloud Computing.

[12] AOUAMEUR, Z&TAHRINE, H. (2013). Comparaison et mise en place des plateformes de Cloud Computing : OpenStack et Eucalyptus : Mémoire de Magistère en Informatique Industrielle, Université Kasdi Merbah de Ouargla

[13] https://www.uniprint.net/en/7-types-cloud-computing-structures

[14] https://azure.microsoft.com/fr-fr/overview/what-is-cloud-computing/

[15] http://icp.ge.ch/sem/cms-spip/spip.php?article962

[16] N.Grevet. Le cloud computing : évolution ou révolution ? Pourquoi, quand, comment et surtout faut-il prendre le risque ?, Août 2009.

[17] Expert Thinking

[18] Hannachi, S. (2015). Etude et Mise en Place d'une Solution Cloud Computing Privé au sein de Tunisie Télécom : Rapport de stage de fin d'études, Réalisé au sein de Tunisie Télécom.

[19] AOUAMEUR, Z&TAHRINE, H.(2013). Comparaison et mise en place des plateformes de Cloud Computing : OpenStack et Eucalyptus : Mémoire de Magistère en Informatique Industrielle, Université Kasdi Merbah de Ouargla

[20] https://groupolivrer.com/rise-from-the-depths-azure-cloud-services-empower-organizations-to-transform/

[21] https://commons.m.wikimedia.org/wiki/File:AmazonWebservices_Logo.svg

[22] https://www.actua.com/actualite/google-cloud-annonce-des-nouveautes-ai-ml/

Références chapitre I

[23] https://ibmcloud.ideas.aha.io

[24] Noumsi, L. F. (2012). Etude et mise en place d'une solution" cloud computing" privée dans une entreprise moderne: cas de CAMTEL. Mémoire ingénieur, Ecole nationale supérieure des postes et télécommunications-*Paris*.

[25] https://www.oodrive.fr/blog/productivite/le-100-cloud-dans-les-entreprises-une-realite-dans-un futur-proche/

[26] https://www.lebigdata.fr/stockage-cloud-top-petites-entreprises

[27] https://fr.wikiversity.org/wiki/Cloud_computing_et_entreprise/Cloud_computing_au_sein_des_entreprises

Chapitre II :

Sécurité du cloud computing

II.1. Introduction

Devant la croissance accrue dans l'utilisation des réseaux et des systèmes informatiques et devant la nature sensible des données manipulées par ces systèmes, il est primordial de mettre en place des mécanismes de sécurité pour assurer l'intégrité, la confidentialité, la disponibilité ainsi que la non-répudiation .

La sécurité informatique en général et la sécurité des réseaux en particulier est devenue aujourd'hui, plus que jamais, un souci majeur au niveau international, et surtout à l'heure où les systèmes informatiques sont devenus de plus en plus complexes, avec des centaines d'applications qui s'exécutent en parallèle, et qui ont été développées par des acteurs dont le soucis majeur est de réduire au maximum le temps de délivrance de la marchandise au marché.

Les attaques informatiques représentent aujourd'hui le plus grand défi pour la plupart des entreprises, et des établissements, cependant, malgré les développements et les améliorations des méthodes et des outils de protection, le nombre des attaques succès s'augmente sans cesse, et des nouveaux formes d'attaques et de trous de sécurité sont publiés presque chaque jour. Néanmoins, ni l'augmentation d'utilisation des firewalls, ni celle des anti-virus ont pu stopper ces attaques, et encore les dommages des entreprises et des établissements et même des personnes restent en croissance à l'abri des systèmes actuels de protection, de détection et de prévention des attaques qui forment un simple point de protection contre les attaques connues qui sont enregistrées dans leurs bases de règles le problème crucial de ces derniers c'est comment mettre à jour leurs bases de signatures par les nouveaux types d'attaques avant que ces derniers peuvent faire des dégâts [1].

II.2. Les vulnérabilités du cloud computing:

Les avantages du cloud computing sont aujourd'hui une évidence, les plus notables sont la réduction des coûts de maintenance de son infrastructure informatique, la réduction de la consommation énergétique, la disposition rapide d'une plateforme prête à l'emploi pour le déploiement des applications, la disposition d'une solution de sauvegarde simple et accessible à tous, même aux non-informaticiens, etc…. .

Cependant, devant toutes les possibilités offertes par ce nouveau concept de l'informatique, il demeure des réticences dans son adoption. Ces réticences sont liées, pour la plupart, au facteur de sécurité, qui reste encore un véritable challenge.

Plusieurs études menées par des spécialistes tels qu'ISACA (Information Systems Audit and Control Association) et CSA (Cloud Security Alliance) ont permis d'identifier plusieurs points qui constituent les menaces majeures à la sécurité des données et à celles des applications en cloud [2].

Selon nos recherches et le nombre innombrable d'attaques existantes, nous les avons classifiés sous 3 catégories :

II.2.A. Les attaques web.

II.2.B. Le Social engineering.

II.2.C. Les attaques mobiles.

II.2.A. Les Attaque Web:

II.2.A.1. Les Malwares:

On appelle malware (ou programme malveillant, maliciel) un programme ou une partie de programme destiné à perturber, altérer ou détruire tout ou partie des éléments logiciels indispensables au bon fonctionnement d'un système informatique.

On distingue principalement sept types de programmes malveillants : les virus informatiques, les bombes logiques, les vers, les chevaux de Troie, les rootkits, les keyloggers et les spywares [3].

II.2.A.2. Attaque par déni de service (DOS):

Une attaque par déni de service (DOS, Denial Of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation.

Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés comme le montre la figure (II.1).

Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à Internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur Internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information.

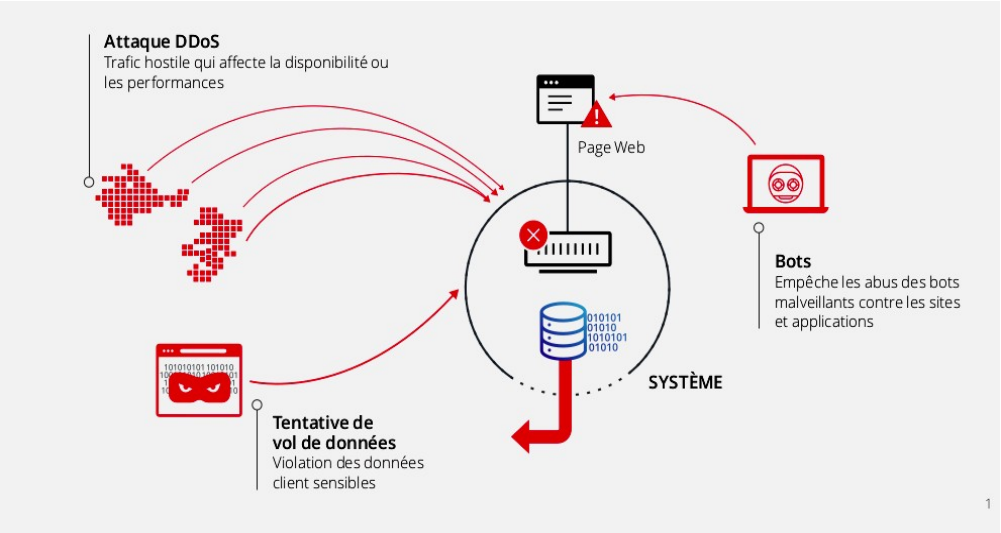


Figure (II.1) : Attaque DDoS [4].

On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation : consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles.

- Les dénis de service par exploitation de vulnérabilités : consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Le principe de ces attaques consiste à envoyer des paquets IP ou des données de taille ou de Constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent [5].

De plus en plus exposées, les entreprises doivent renforcer leurs défenses contre trois problèmes et risques principaux :

- Une attaque DDoS contre des applications, des sites Web ou des API affecte leur disponibilité et leurs performances, provoquant la chute des revenus, des coûts opératoires plus élevés et une dégradation de la réputation.
- La violation des données sensibles des clients et des entreprises, comme les renseignements personnels ou la propriété intellectuelle, peut entraîner la perte de clients et entacher leur confiance.
- Les bots malveillants emploient l'extraction de contenu, l'usurpation de compte et les fraudes au paiement pour s'attaquer aux applications client [6].

II.2.A.3. Les botnets:

Historiquement, botnet désignait des réseaux de robots IRC. Le sens de botnet s'est étendu aux réseaux de machines zombies, utilisés notamment pour le minage de crypto monnaies mais aussi des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS) [7].

II.2.A.4. Attaques man in the middle:

Une attaque man in the middle (littéralement « attaque de l'homme au milieu » ou « attaque de l'intercepteur »), parfois notée MITM, est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties [8] comme le montre la figue ci-dessous:

.

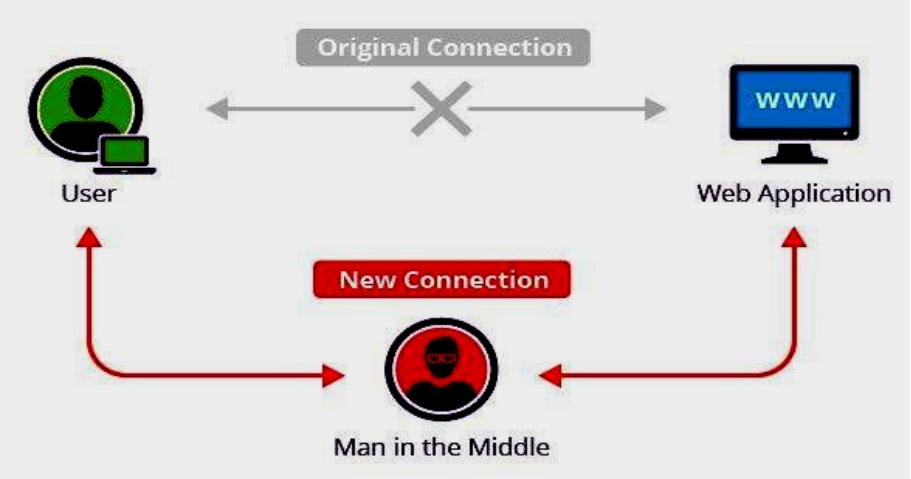


Figure (II.2) : Attaque Man in the Middle [9].

Une interception MITM cible généralement les utilisateurs de boîtes email professionnelles, d'applications bancaires, de sites marchands ou encore de solutions professionnelles SaaS dans le but de voler leurs identifiants, numéros de cartes et comptes bancaires, etc.… [10].

La plupart du temps, l'échange entre les deux parties est intercepté via une connexion Wi-Fi. Les malfaiteurs / pirates / hackers créent des réseaux publics libres d'accès utilisant des noms légitimes. Lorsque L'utilisateur connecte son terminal au réseau malveillant, toutes les données envoyées sur le réseau sont interceptées par le hacker.

Dans d'autres cas, des techniques de « IP, DNS ou ARP spoofing » sont exécutées afin d'afficher une copie d'un site authentique lorsqu'une URL légitime est recherchée. Pour ce faire, les assaillants cachent leur identité derrière une adresse IP de confiance (IP spoofing) ou répondent à des requêtes ARP ou DNS avec leur propre adresse IP (ARP/DNS spoofing). Ce type d'attaque cible généralement les sites de services financiers [10].

II.2.A.5. Détournement de DNS (Dns Hijacking):

Le détournement de DNS est une technique qui permet de contrôler complètement les sites Web affichés par les navigateurs d'un ordinateur. Il consiste à modifier le serveur DNS utilisé par défaut (voir la figure (II, 3)). De nombreux malwares utilisent cette technique car elle persiste même si l'utilisateur parvient à se défaire des programmes indésirables installés sur son PC. En effet, le DNS par défaut fait parti des paramètres du système. Il n'a donc a priori aucun niveau de dangerosité.

De plus, il n'existe aucune méthode automatique pour le système d'exploitation ou un logiciel antimalware de connaître le DNS du fournisseur d'accès utilisé pour accéder à Internet (le protocole DNS sec pourrait changer ce point).

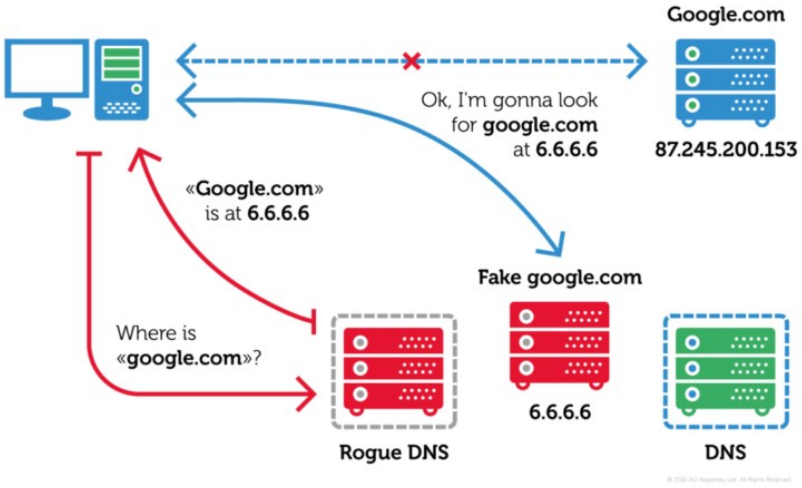


Figure (II.3) : Attaque Dns Hijacking [11].

Le détournement de DNS permet non seulement de rediriger un navigateur web vers le site du choix du pirate mais aussi d'insérer à la volée du code HTML dans les sites affichés. N'importe quel site peut alors servir à récupérer des données personnelles ou à rediriger l'utilisateur pour créer du trafic sur un site web [8].

II.2.A.6. Attaques par injection de commandes SQL:

La figure (II ,4) nous montre les attaques par injection de commandes SQL sont des attaques visant les sites web s'appuyant sur Des bases de données relationnelles.

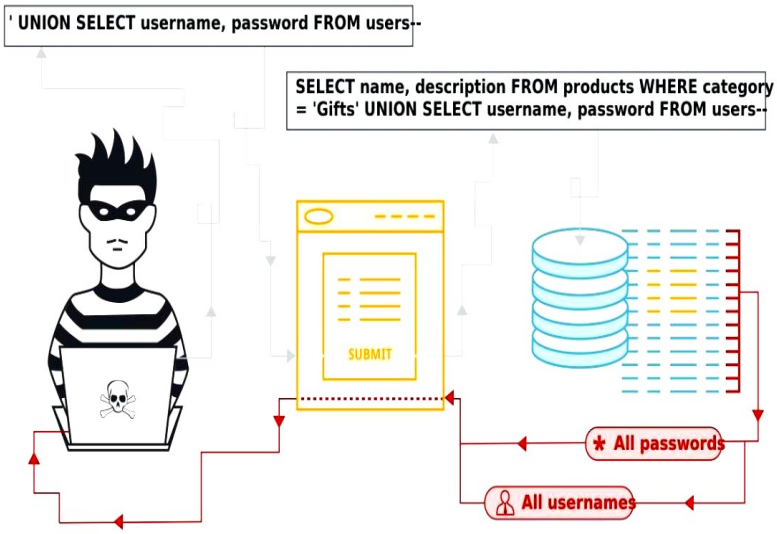


Figure (II.4) : Attaque par injection de commandes SQL [12].

Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire d'en modifier le contenu.

En effet, certains caractères permettent d'enchaîner plusieurs requêtes SQL ou bien ignorer la suite de la requête. Ainsi, en insérant ce type de caractères dans la requête, un pirate peut Potentiellement exécuter la requête de son choix.

Soit la requête suivante, attendant comme paramètre un nom d'utilisateur :

★ SELECT * FROM utilisateurs WHERE nom="$nom";

Il suffit à un pirate de saisir un nom tel que "toto" OR 1=1 OR nom ="titi" pour que la requête devient la suivante :

★ SELECT * FROM utilisateurs WHERE nom="toto" OR 1=1 OR nom ="titi"; Ainsi, avec la Requête ci-dessus, la clause WHERE est toujours réalisée, ce qui signifie qu'il Retourne les enregistrements correspondants à tous les utilisateurs [8].

II.2.A.7. 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.

Les attaques de détournement comprennent IP attaques Spoofing, numéro de séquence TCP 2 attaques, et DNS Spoofing [13].

II.2.A.8. Backdoor:

La figure (II.5) nous montre un backdoor, mot anglais qui se traduit en français par « porte dérobée » ou « trappe », est un cheval de Troie caché dans un logiciel, un service en ligne ou un système informatique entier et dont l'utilisateur n'a pas connaissance. Dans le meilleur des cas, il est créé dès la conception par le développeur du programme, un fournisseur de service ou un constructeur pour réaliser facilement des opérations de maintenance ou pour pouvoir couper l'accès en cas de litige avec un client [14].

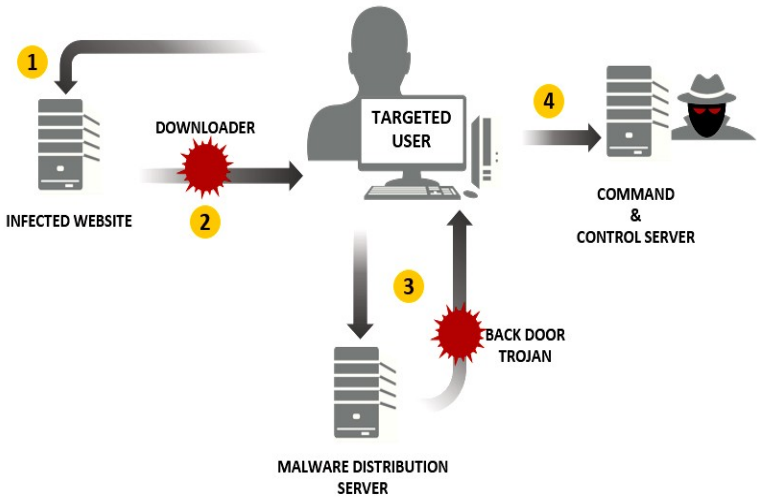


Figure (II.5) : Attaque par backdoor [15].

II.2.B. Le Social engineering:

II.2.B.1. Le concept du social engineering

C'est une technique qui a pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte. Contrairement aux autres attaques, elle ne nécessite pas de logiciel.

La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering: par téléphone, par lettre, par internet et par contact direct [16].

II.2.B.2. L'être humain: la pièce fragile:

De tout temps, on a fait confiance à l'être humain pour conserver des informations. Confiance plus ou moins exprimée : César envoyait ses mes sages de manière chiffrée (grâce au très célèbre algorithme dit "de César") mais partait du principe que seul le destinataire connaissait «la clé de déchiffrement ». Le problème avec l'être humain, c'est qu'il existe des tas de raisons de divulguer ses secrets, allant de la simple inattention à l'obligation sous la torture, deux extrêmes qui ont poussé les destinataires de César à révéler leur clé et les messagers à partager leur fardeau.

Ramy Badir, l'un des frères non-voyants, déclara un jour« qu'un ordinateur sécurisé est un ordinateur entreposé dans un hangar et débranché ».

Parmi les réponses à cette citation, l'une d'entre elles a retenu notre attention : son auteur, Kevin Mitnick, indique qu'il pourra toujours trouver une personne assez aimable pour brancher l'ordinateur!

Le social engineering, c'est donc ça : utiliser la pièce fragile qu'est l'humain pour avancer dans l'histoire,en lui demandant de brancher un ordinateur, de transmettre une fausse information,d'indiquer le mot de passe du Directeur général, voire même d'envoyer par courrier le plan confidentiel sur lequel ont travaillé les ingénieurs de l'entreprise durant plus de six mois.

Rien ne sert d'avoir des protections techniques infaillibles si une personne interne à votre système permet à son insu à un attaquant de déjouer toutes ces protections. L'humain est une faille qu'il faut surveiller [17].

II.2.B.3. Le processus et méthodes du social engineering:

Dans la pratique, le pirate exploite les vulnérabilités humaines et sa connaissance de la cible, de ses clients ainsi que de ses fournisseurs et sous-traitants en utilisant : la manipulation, la supercherie et l'influence Pour son exploitation, le pirate pourra utiliser tout média à sa disposition : rencontre IRL, téléphone, email, messagerie instantanée, réseaux sociaux...

- Se faire passer pour un fournisseur, un partenaire.
- Se faire passer pour un collègue.
- Se faire passer pour un supérieur hiérarchique.
- Se faire passer pour une administration [18].

II.2.B.4. Le Social engineering Toolkit (SET):

Le SET c'est l'ensemble des outils que peut contenir un logiciel d'ingénierie sociale, (voir la figure(II.6)).

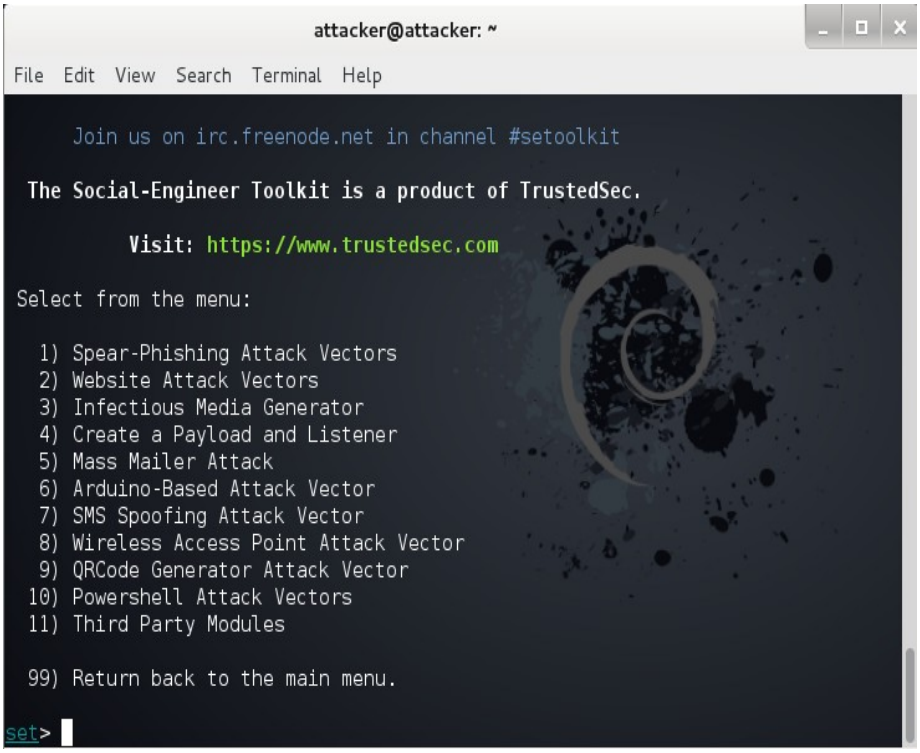


Figure (II.6) : The Social-engineering Toolkit [19].

II.2.C. Les attaques mobile

II.2.C.1. Vecteurs d'attaque réseaux Mobile:

Un terminal mobile est connecté, constamment. Les utilisateurs ont développé des usages de connexion systématique à tout et n'importe quoi. Dès qu'il trouve une connexion, il se connecte. L'important est de trouver de la bande passante.

L'autre problème c'est qu'aujourd'hui, beaucoup d'entreprises vont encourager leurs utilisateurs à se connecter depuis le Wifi. L'objectif est de faire des économies en termes de coût de

data. Or, il n'y a rien de plus facile pour un attaquant de se mettre entre un utilisateur et un terminal [20].On peut trouver aussi: l'application infectée (malwares) et le phishing sms.

II.2.C.2. Attaque Ios:

On ne peut pas être dans la course à l'innovation constante, aller vers de nouveaux connecteurs, s'intégrer de plus en plus au centre d'un écosystème qui va intégrer de plus en
Plus les objets connectés, de la domotique, etc. et fournir des OS robustes d'un point de vue sécurité.

On va avoir sur les OS mobiles un certain nombre de vulnérabilités. Il y a énormément de difficultés pour les entreprises à patcher ses vulnérabilités, à obtenir un niveau de sécurité conforme aux terminaux mobiles déployés [20].

Voici les statistiques des différentes attaques mobiles de l'année 2018 selon Kaspersky

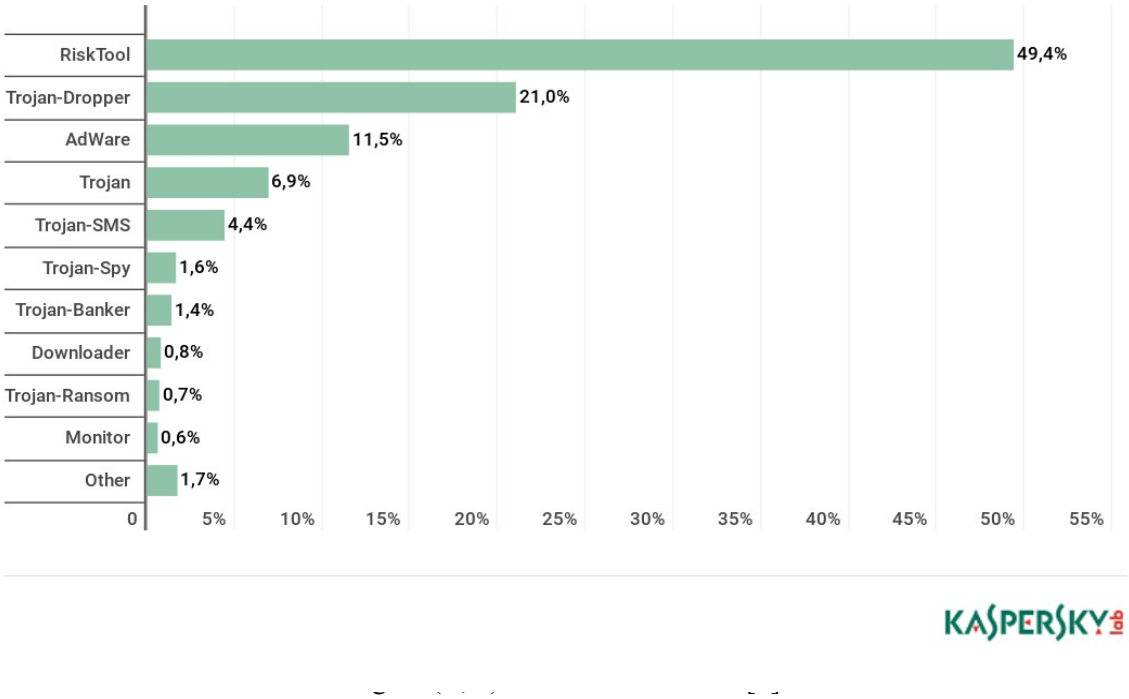


Figure (II.7) : les statistiques des différentes attaques mobile de l'année 2018 selon Kaspersky [21].

II.3. Les solutions de Sécurité du cloud computing

II.3.A. La virtualisation

II.3.A.1. Définition de la virtualisation:

La virtualisation est un ensemble de techniques matérielles et/ou logicielles qui autorisent l'exécution de plusieurs applications indépendantes sur une même machine hôte. Grâce à la virtualisation, il est possible d'exécuter plusieurs systèmes d'exploitation (OS invité) sur un même serveur. Ainsi, il n'est plus nécessaire d'utiliser un serveur par application. On parle souvent

d'environnement virtuel (Virtual Environnent – VE) ou de serveur privé virtuel (Virtual Private Server – VPS) lorsqu'une machine exploite la virtualisation.

La figure (II, 7) représente les différents technologies et produits de virtualisation Pour bénéficier de cette technologie, il suffit d'équiper une machine d'un logiciel de virtualisation permettant d'ajouter une couche de virtualisation, appelée hyperviseur. Cet hyperviseur masque les véritables ressources physiques de la machine afin de proposer des ressources différentes et spécifiques en fonction des applications qui tournent. Il y a donc une totale indépendance entre le matériel et les applications. Le logiciel de virtualisation simule autant de machines virtuelles que de systèmes d'exploitation souhaité. Chaque OS croit alors qu'il est installé seul sur une machine alors qu'en réalité, plusieurs OS peuvent fonctionner en parallèle en partageant les mêmes ressources [22].

Figure (II.8) : Technologies et produits de virtualisation[23].

II.3.A.2. Les différents types de virtualisation

Nous avons 4 types de virtualisations :

- La virtualisation de serveur
- La virtualisation d'application
- La virtualisation de postes de travails
- La virtualisation de stockage

II.3.A.2.1. La virtualisation de serveur :

La virtualisation de serveur permet de regrouper plusieurs serveurs physiques sous-employés sur un seul hôte qui exécute des systèmes virtuels comme illustrer sur la figure (II.8). Il permet aussi

de réduire la consommation électrique et le nombre d'administrateurs. Il participe beaucoup à la réalisation des économies (locaux, Consommation électrique).

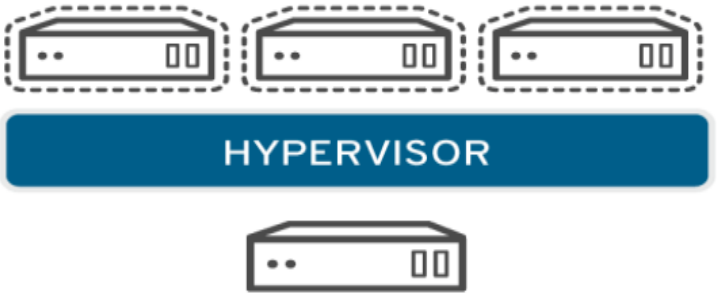


Figure (II.9) : Virtualisation de serveur [24].

II.3.A.2.2. La virtualisation d'application:

Elle permet de séparer complètement l'application du système d'exploitation hôte et des autres applications présentes afin d'éviter les conflits comme le montre la figure ci-dessous.

En outre elle peut être définie comme la technologie qui permet de séparer l'environnement du bureau et des applications associées de la machine physique.

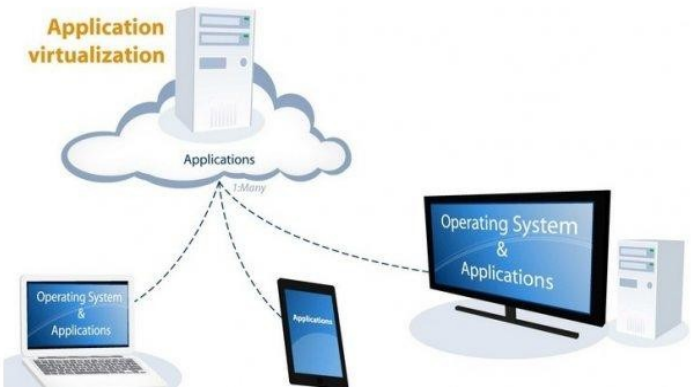


Figure (II.10) : Virtualisation des Applications [25].

II.3.A.2.3. La virtualisation des postes de travail:

La figure (II, 10) représente la virtualisation des postes de travails permet aux administrateurs systèmes et réseaux de gérer beaucoup plus facilement les postes de travail de l'entreprise et de répondre avec flexibilité aux demandes des utilisateurs.

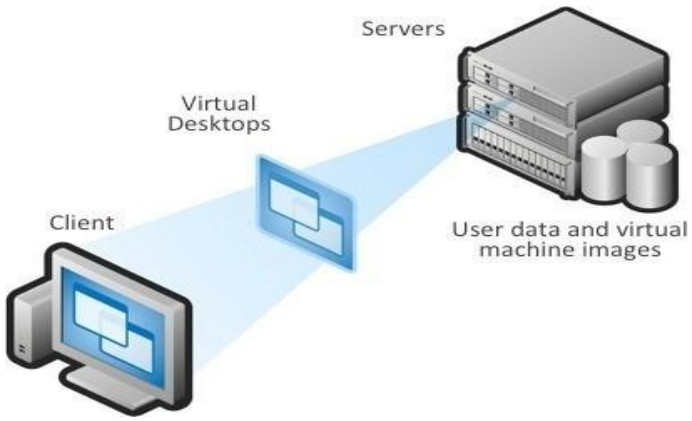


Figure (II.11) : Virtualisation des postes de travail [26].

Un poste de travail virtualisé ou bureau virtuel peut être hébergé soit directement sur l'ordinateur du client soit sur un serveur dans le centre de données.

II.3.A.2.4. La virtualisation de stockage :

La virtualisation des stockages permet d'exploiter au maximum les ressources, d'exploiter au mieux le stockage des disques durs. Dans un premier, temps pour centraliser et sécuriser les données, il faudrait que le centre de donnée s'équipe d'un SAN (Storage Area Network).

Un des plus grands défis de la virtualisation reste le stockage. Dans les faits, c'est le plus souvent le stockage qui fait exploser les coûts, et créer des engorgements et des pertes de performances.

L'infrastructure, en l'occurrence le stockage, s'il est mal dimensionné, ralentit les applications. Le NAS (Network Attached Storage) est effectivement un élément de stockage attaché directement au réseau local d'une entreprise. Il se configure par le biais d'une application web comme le navigateur par exemple [27].

II.3.A.3. L'évolution de la virtualisation :

Le concept de virtualisation est apparu autour des années 1960 lorsque des entreprises telles que IBM ont souhaité partitionner les ressources des mainframes (un mainframe ou ordinateur central est un ordinateur de grande puissance de traitement).

La virtualisation a perdu tout son intérêt dans les années 1980 – 1990 bien que certains projets comme Amiga, SideCar ou encore Implant ont essayé d'exploiter cette technologie. En effet, durant cette période, les systèmes client-serveur sont à la mode. Mais les problèmes de protection en cas de panne ainsi que le coût important de la maintenance des serveurs et des stations clientes seront des limites pour cette architecture à deux niveaux. Au milieu des années 1990, les émulateurs connaissent un réel succès (ordinateurs Atari, Amiga ; consoles NES). Ce n'est qu'au début des années 2000 que la virtualisation devient célèbre grâce à la société VMware qui développe des logiciels pour des serveurs de type x86. En 2003 apparaît la para-virtualisation avec Xen.

A partir de 2005, les fabricants de processeurs Intel et AMD implantent la virtualisation matérielle dans leurs produits. En 2007, les machines virtuelles KVM (Kernel-based Virtual Machine) débarquent sur Linux. Jusqu'alors, la virtualisation était utilisée pour tester des systèmes d'information avant leur déploiement la figure (II.11) dévoile l'axe d'évolution de la virtualisation.

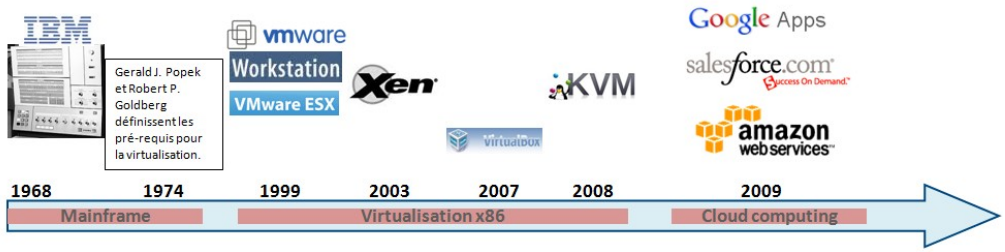


Figure (II.12) : L'axe d'évolution de la virtualisation [28].

Depuis peu, le monde informatique connaît une nouvelle mutation avec la virtualisation 3.0, utilisée principalement dans les technologies liées au cloud computing et à la gestion automatisée des déploiements internes [29].

II.3.A.4. Pourquoi virtualiser ?

La virtualisation est l'une des technologies majeure du cloud, applicable à plusieurs niveaux: stockage, réseau, processeur, mémoire, etc. tant sur des infrastructures serveur que poste de travail.
En tant d'entrepreneur, la virtualisation est une solution technologique qui peut permettre à votre entreprise d'améliorer ses ratios notamment qualité / performance / investissement, mais aussi de simplifier et sécuriser son mode de fonctionnement [30].

La virtualisation des systèmes informatiques présente de nombreux avantages :

- Déploiement rapide des applications
- Niveaux de service supérieur et disponibilité accrue des applications
- Taux d'utilisation supérieur des investissements dans l'infrastructure
- Évolutivité rapide et flexible
- Réduction des coûts énergétiques, d'infrastructure et des installations
- Diminution des frais de gestion
- Accès aux applications et aux données des bureaux en tout lieu
- Sécurité informatique renforcée [31].

II.3.A.5. Différence entre le cloud et la virtualisation :

Si virtualisation et Cloud Computing ne sont pas des termes similaires, ils reposent pourtant sur des fondamentaux communs, dans la mesure où aujourd'hui, la délivrance de services de Cloud Computing comporte quasi nécessairement de la virtualisation.

Parce que le Cloud consiste à délivrer des services disponibles dans un catalogue, le Cloud fonctionne en instanciant et en combinant de multiples ressources, qui seront des serveurs, des emplacements de stockage, des bases de données ou encore, des firewall par exemple. Ainsi, si la virtualisation est nécessaire, c'est l'automatisation de la mise à disposition de ces ressources, ainsi que le suivi de leur consommation à des fins de facturation qui constitue véritablement ce que l'on appelle le Cloud.

II.3.A.6.Cloud ou virtualisation, faut-il choisir ?

Puisque la virtualisation est un composant du Cloud, bien entendu, il ne s'agit donc pas de choisir. Tous deux permettent de maximiser les ressources informatiques et donc, de réduire les coûts et d'augmenter l'agilité de l'entreprise. Mais le Cloud et la virtualisation ne sont donc pas non plus synonymes : tandis que la virtualisation est une technologie, permettant de simuler plusieurs instances virtuelles au sein d'un même matériel physique, le Cloud Computing permet d'orchestrer facilement la gestion de ces instances virtuelles et de transformer la délivrance de ces ressources en un service, facturable à la consommation.

La virtualisation n'est donc pas le coeur du concept du Cloud, mais étant donné l'avancée technologique actuelle en matière de gestion d'infrastructure informatique, elle fait aujourd'hui partie intégrante de son fonctionnement. C'est en ce sens qu'il faut comprendre la complémentarité entre ces deux concepts [32].

II.3.B. Les plateformes du cloud computing (solutions open source):

Dans cette partie on va citer quelques solutions Open Source qui sont assignées au déploiement de l'architecture de leur différentes infrastructures. Bien entendu que les solutions proposées peuvent être utilisées pour la gestion des services du cloud public , Parmi eux, on trouve :

- OpenNebula.
- Eucalyptus.
- OpenStack.

II.3.B.1. La solution Openstack

Figure (II.13) : Logo d'OpenStack [33].

OpenStack est un ensemble de logiciels ''open source'' permettant de déployer des infrastructures cloud privé de type IaaS. Il est Composé de plusieurs projets corrélés (Nova,Swift, Glance...) et est structuré en une architecture modulaire lui permet de contrôler les différentes ressources telles que la puissance de calcul, le stockage ou encore la gestion de la connectivité réseau des machines virtuelles.Openstack est porté par une organisation non-commerciale appelée Fondation OpenStack qui a pour but de promouvoir le projet OpenStack ainsi que de protéger et d'aider les développeurs libres à travailler et contribuer à travers le monde entier [34].

II.3.B.1.1. Les composants d'Openstack:

OpenStack possède une architecture modulaire qui comprend de nombreux composants:

Services	Nom du code	Description
Les composants communs		
openStack Identity	**Keystone**	Gestion de l'identité
openStack Dashboard	**Horizon**	Interface web de paramétrage et gestion
Les composants de base		
OpenStack Compute	**Nova**	Gestion des instances(serveurs)
OpenStack Network	**Neutron**	Gestion des réseaux
OpenStack Imaging Service	**Glance**	Gestion des images
Les composants optionnels		
OpenStack Storage	**Swift**	Stockage d'objet

OpenStack Block Storage	**Cinder**	Service de disques persistants pour les machines virtuelles
OpenStack Telemetry	**Ceilometer**	Service de métrologie notamment pour la facturation
OpenStack Orchestration	**Heat**	Service d'orchestration à base de template

Tableau (II.1) : Les composants openstack [34].

II.3.B.2. OpenNebula:

Il s'agit d'une plateforme purement open-source permettant de déployer des Clouds privés, hybrides et publiques. Elle est écrite en C++, Ruby et Shell et elle supporte les hyperviseurs Xen, KVM et VMware. Le support de Virtualbox est prévu à partir de la version 4.0 de VirtualBox.

Sa puissance consiste dans ses connecteurs vers des fournisseurs d'IaaS sur les Clouds publics tels que : Amazon EC2 Web Service, Nimbus WSRF, ElasticHosts REST, etc. OpenNebula est soutenu par le projet européen RÉSERVOIR, qui propose une architecture complète pour la gestion de Datacenter et la création de services Cloud [35].

II.3.B.2.1. Architecture Cloud ouverte

Le cloud computing d'entreprise est la prochaine étape dans l'évolution de la virtualisation des centres de données. OpenNebula est une solution simple, riche en fonctionnalités et flexible, permettant de créer et de gérer des clouds d'entreprise et des contrôleurs de domaine virtualisé, associant les technologies de virtualisation existantes à des fonctionnalités avancées de multi-location, de fourniture automatique et d'élasticité.

OpenNebula suit une approche ascendante fondée sur les besoins des administrateurs système, des développeurs et des utilisateurs.

II.3.B.2.2. Aperçu architectural:

OpenNebula suppose que votre infrastructure physique adopte une architecture de type cluster classique avec une interface frontale et un ensemble d'hôtes sur Les quels les machines virtuelles (VM) seront exécutées. Il existe au moins un réseau physique reliant tous les hôtes au serveur frontal. comme le montre la figure ci-dessous.

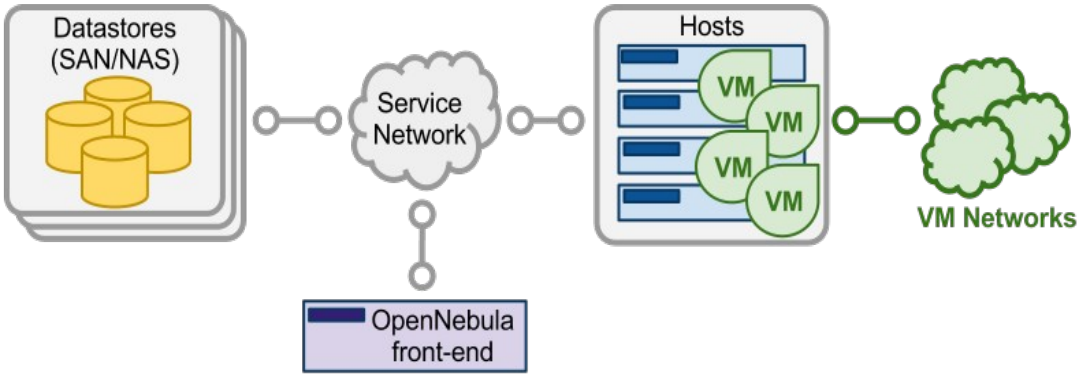


Figure (II.14) : Architecture D'OpenNebula [36].

Une architecture cloud est définie par trois composants: stockage, mise en réseau et virtualisation. Par conséquent, les composants de base d'un système OpenNebula sont les suivants:

- Frontal qui exécute les services OpenNebula.
- Des hôtes compatibles avec l'hyperviseur qui fournissent les ressources nécessaires aux ordinateurs virtuels.
- Magasins de données contenant les images de base des ordinateurs virtuels.
- Les réseaux physiques utilisés pour prendre en charge des services de base tels que l'interconnexion des serveurs de stockage et des opérations de contrôle OpenNebula, ainsi que les VLAN des ordinateurs virtuels [35].

II.3.B.3. Eucalyptus

Eucalyptus Son acronyme est : Elastic Utility computing Architecture for Linkingyour Programs To UsefulSystems ; est un outil open source issue d'un projet de recherche de l'université de Californie. Cette solution est la plus connue, car elle est intégrée dans les distributions Ubuntu Server et Debian. Eucalypti s'est écrit en C, Java et Python et permet de créer des Clouds IaaS de type privé ou hybride. Il supporte les machines virtuelles Linux ainsi que les hyperviseurs Xen et KVM. Son avantage majeur est le fait qu'il est compatible avec Amazon EC2 (Amazon Elastic Compute Cloud) [37].

II.3.B.3.1. Composants d'eucalyptus:

II.3.B.3.1.1. Contrôleur de cluster (CC):

Le contrôleur de cluster gère le ou les contrôleurs de noeud et est responsable du déploiement et de la gestion des instances sur ceux-ci. Il communique avec Node Controller et Cloud Controller simultanément.

CC gère également la mise en réseau des instances en cours sous certains types de modes de mise en réseau disponibles dans Eucalyptus.

II.3.B.3.1.2. Contrôleur de nuage (CLC) :

Le contrôleur de nuage est une interface frontale pour tout l'écosystème. CLC fournit une interface de services Web conforme à Amazon EC2 / S3 avec les outils clients d'un côté et interagit avec le reste des composants de l'infrastructure Eucalyptus de l'autre.

II.3.B.3.1.3. Contrôleur de noeud (NC) :

C'est le composant de base pour les noeuds. Le contrôleur de noeud conserve le cycle de vie des instances exécutées sur chaque noeud. Le contrôleur de noeud interagit avec le système

d'exploitation, l'hyperviseur et le contrôleur de cluster simultanément.

II.3.B.3.1.4. Contrôleur de stockage Walrus (WS3):

Le contrôleur de stockage Walrus est un système de stockage de fichiers simple. WS3 stocke les images de la machine et les instantanés. Il stocke et sert également des fichiers à l'aide des API S3.

II.3.B.3.1.5. Contrôleur de stockage (SC) :

Permet la création d'instantanés de volumes. Il fournit un stockage de bloc persistant sur AoE ou iSCSI aux instances. La figure ci-dessous résume l'architecture Eucalyptus.

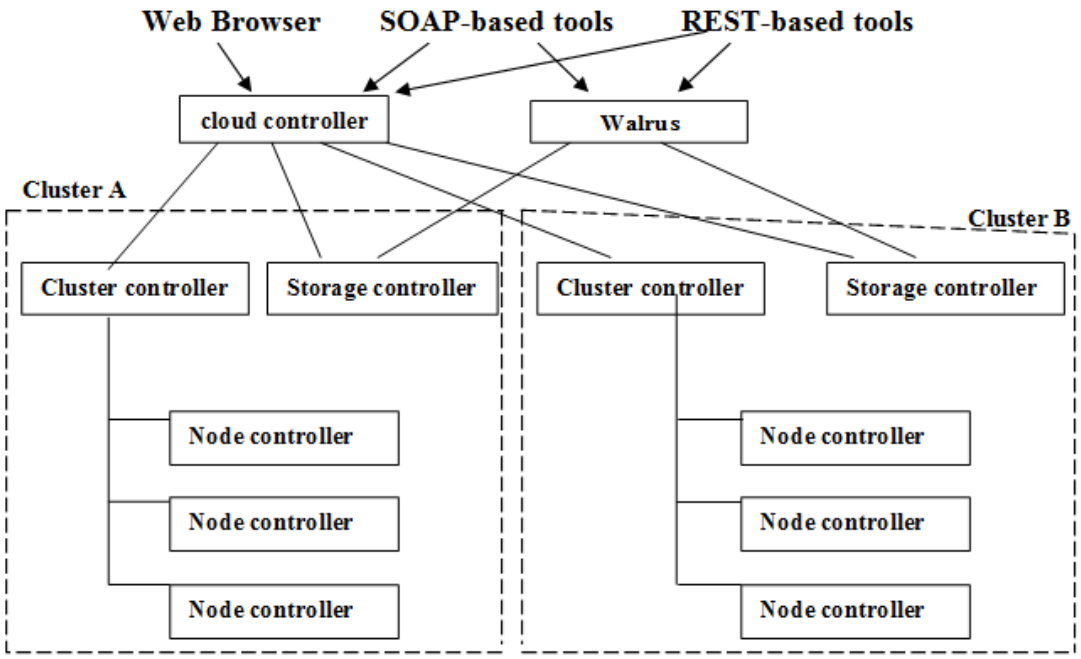


Figure (II.15) : Eucalyptus cloud architecture [38].

II.4. Conclusion

Dans ce chapitre , nous avons présenté les principales menaces et vulnérabilités du cloud computing tout en illustrant les différentes solutions et plateformes open source existantes : de la openNebula, Eucalyptus vers l'openStack , Sachant qu'avec le vaste monde de l'IT , le développement de ces dernières (plateformes) nous a conduit vers une nouvelle tendance appelée "la technologie par conteneurs" ou "container" en anglais, et qui a résolue pas de problèmes de : gestion , de stockage et sécurité en offrant une extensibilité pour les entreprises en particulier , et que nous allons voir dans le chapitre suivant comme choix de solution à déployer.

Références chapitre II

[1] BOULAICHE, A. (2006). TECHNOLOGIES HONEYPOTS : Mémoire de Magistère En Informatique, Université du Québec en Outaouais, Canada.

[2] https://cloud-computing.developpez.com

[3] Pillou, J. F .Tout sur la Sécurité informatique edition 2013

[4] https://pbs.twimg.com/media/D6a8vKXUwAAMZiQ.jpg

[5] Pillou, J. F., & Bay, J. P. (2016). *Tout sur la sécurité informatique-4e édition*. Dunod.

[6] GRANGE, P. (2010). Le livre blanc du Cloud Computing. *Paris: Syntec Informatique*

[7] wikipédia

[8] Pillou, J. F., & Bay, J. P. (2016). *Tout sur la sécurité informatique-4e édition*. Dunod.

[9] https://protfoliogd.fr/quest-ce-quune-attaque-mitm].

[10] https://blog.pradeo.com/fr/attaque-man-in-the-middle

[11] https://www.google.com/amp/s/wccftech.com/android-trojan-dns-hijacking/amp/

[12] https://portswigger.net/web-security/images/sql-injection.svg

[13] Moussa, M.(2014). Etude sur la sécurité du cloud computing : Mémoire master Technologie de L'information et de Communication, Université de Msila.

[14] https://www.futura-sciences.com

[15] https://news.softpedia.com/news/tick-cyber-espionage-group-targets-japanese-companies-with-dasrf-backdoors-503555.shtml

[16] www.securiteinfo.com

[17] livre : sécurité informatique ethical-hacking

[18] Social Engineering L'art de l'influence et de la manipulation Christoph Casalegno

[19] http://linuxtrack.net/img/2/1409298373_capture_d_ecran_-_290814_-_09_06_13.png

[20] article "FIC 2017 : cinq vecteurs d'attaque des smartphones professionnels"

[21] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/08/03175922/180803-it-threat-evolution-q2-2018-statistics-2-0.png

[22] http://www.bmcssi.ch

[23] http://www.capitalbureautique.com/wp-content/uploads/2013/06/Microsoft-virtualisation.jpg

[24] https://www.redhat.com/fr/topics/virtualization/what-is-virtualization

Références chapitre II

[25] https://www.google.com/amp/s/www.lemondeinformatique.fr/actualites/lireamp-la-virtualisation-une-bombe-a-retardement-en-matiere-de-licence-logicielles-51970.html

[26] https://www.supinfo.com/articles/single/2351-differents-types-virtualisation

[27] https://www.supinfo.com/articles/single/2351-differents-types-virtualisation

[28] https://upload.wikimedia.org/wikipedia/commons/7/72/Historique.png

[29] livre blanc sécurité et virtualisation

[30] https://www.journaldunet.com/solutions/expert/63557/5-raisons-de-choisir-la-virtualisation.shtml

[31] http://pf-mh.uvt.rnu.tn/867/1/plateforme-virtualisation-cloud-prive-open-source.pdf

[32] www.ivision.fr

[33] https://i.directioninformatique.com/wp-content/uploads/2014/04/Openstack_logo.jpg

[34] https://www.supinfo.com

[35] Opennebula. http ://opennebula.org/.

[36] https://docs.opennebula.org/5.8/deployment/cloud_desin/open_cloud_architecture.html

[37] Eucalyptus. http ://www.eucalyptus.com/

[38] https://upload.wikimedia.org/wikipedia/commons/2/2f/Eucalyptus_cloud_architecture-1.6.png

Chapitre III :

Sécurité du cloud computing : approches et solutions

III.1. Introduction:

Les conteneurs ont une longue et riche histoire en informatique. Contrairement à l'hyperviseur où une ou plusieurs machines indépendantes fonctionnent virtuellement sur matériel physique via une couche d'intermédiation, les conteneurs s'exécutent à la place dans l'espace utilisateur du noyau d'un système d'exploitation. En conséquence,la virtualisation de conteneur est souvent appelée virtualisation au niveau du système d'exploitation.

La technologie des conteneurs permet les instances d'espace utilisateur lattées à exécuter sur un seul hôte. En raison de leur statut d'invités du système d'exploitation, les conteneurs sont quelquefois considérés comme moins flexibles: ils ne peuvent généralement que le même client ou un invité similaire système d'exploitation en tant qu'hôte sous-jacent. Par exemple, vous pouvez exécuter Red Hat-Linux sur un serveur Ubuntu, mais vous ne pouvez pas exécuter Microsoft Windows sur le dessus d'un serveur Ubuntu.

Les conteneurs sont généralement considérés comme une technologie allégée parce qu'ils nécessitent des frais limités, contrairement aux technologies traditionnelles de virtualisation ou de paravirtualisation. Ils n'ont pas besoin d'une couche d'émulation ou d'une couche d'hyperviseur pour fonctionner et à la place il utiliser l'interface d'appel système normale du système d'exploitation, ce qui réduit à une nécessité pour faire fonctionner les conteneurs et peut permettre une plus grande densité de conteneurs.

Malgré leur histoire, les conteneurs n'ont pas atteint l'adoption à grande échelle, une grande partie de cela peut être posée aux pieds de leur complexité : les conteneurs peuvent être complexes, difficile à mettre en place, et difficile à gérer et à automatiser [1].

III.2. Définition: Que signifie la conteneurisation ?

La conteneurisation est un type de stratégie de virtualisation qui est apparue comme une alternative à la virtualisation traditionnelle basée sur un hyperviseur. Comme dans ce dernier cas, la virtualisation par conteneur implique la création d'éléments virtuels spécifiques d'une infrastructure matérielle. Toutefois, contrairement à l'approche traditionnelle, qui sépare complètement ces machines virtuelles du reste de l'architecture, la conteneurisation créer simplement des conteneurs distincts au niveau du système d'exploitation [2].

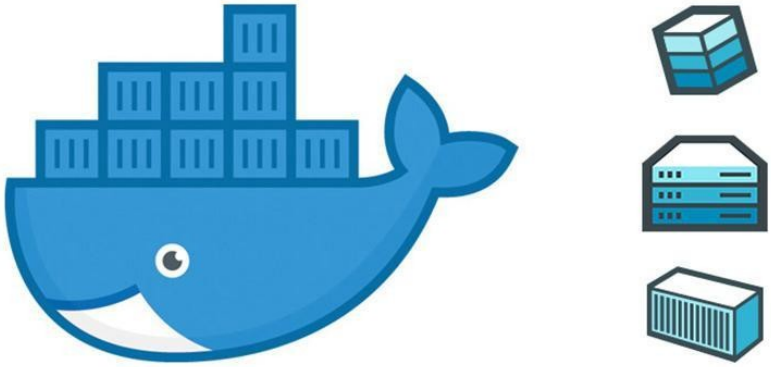


Figure (III.1) : Logo des conteneurs [3]

III.3. La conteneurisation selon Google Cloud:

De Gmail à YouTube en passant par le moteur de recherche, tout fonctionne sous forme de conteneurs chez Google. La mise en conteneur permet à nos équipes de développement d'agir rapidement, de déployer efficacement des logiciels et d'œuvrer à une échelle sans précédent. Nous recréons chaque semaine plus de deux milliards de conteneurs. Les dix dernières années nous ont beaucoup appris sur l'exécution des charges de travail en conteneur, et nous avons partagé nos connaissances avec la communauté tout au long du processus [4].

III.4. En quoi consistent les conteneurs ?

Les conteneurs proposent un mécanisme de regroupement logique qui permet d'extraire des applications de l'environnement dans lequel elles s'exécutent réellement. Une fois extraites, les applications basées sur des conteneurs peuvent facilement être déployées dans n'importe quel environnement, qu'il s'agisse d'un centre de données privé, du cloud public ou encore de l'ordinateur personnel d'un développeur. Grâce à la mise en conteneur, chaque tâche est clairement répartie. En effet, les développeurs peuvent se concentrer sur la logique et les dépendances de leur application pendant que les équipes informatiques se consacrent au déploiement et à la gestion, sans avoir à se soucier de détails tels que la version du logiciel ou la configuration spécifique à l'application.

Si vous avez déjà travaillé dans des environnements virtualisés, les conteneurs sont comparables à des machines virtuelles (VM). Vous connaissez peut-être le principe des VM : un système d'exploitation invité tel que Linux ou Windows est installé sur un système hôte, dont la configuration sous-jacente est accessible virtuellement.

À l'instar des machines virtuelles, les conteneurs vous permettent de regrouper votre application, des bibliothèques et d'autres dépendances en un seul package afin d'obtenir un environnement isolé pour l'exécution de vos services logiciels. La ressemblance s'arrête ici toutefois, car les conteneurs prennent la forme d'unités bien moins volumineuses qui offrent de nombreux avantages aux développeurs et aux équipes informatiques [4].

III.5. Différence entre les conteneurs et la virtualisation :

Avec la technologie de virtualisation, le package qui peut être transmis est une machine virtuelle, et comprend un système d'exploitation complet ainsi que l'application.

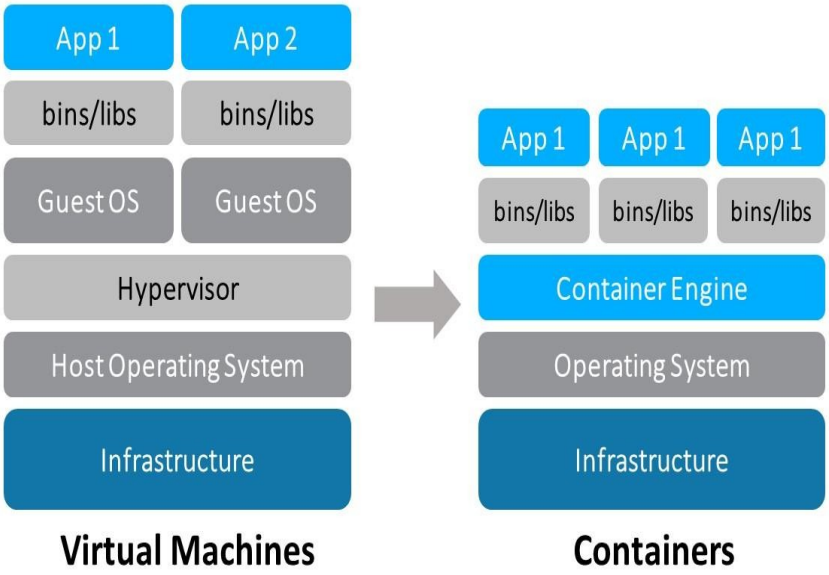


Figure (III.2) : la différence entre les machines virtuelles et les conteneurs [4].

Un serveur physique exécutant trois machines virtuelles aurait un hyperviseur et trois systèmes d'exploitation distincts [5].

III.5.A. Dans les VM:

Les systèmes d'exploitation («OS») et leurs applications partagent des ressources matérielles à partir d'un serveur hôte unique ou d'un pool de serveurs hôtes. Chaque machine virtuelle nécessite son propre système d'exploitation sous-jacent et le matériel est virtualisé comme le montre la figure (III.3) Un hyperviseur ou un moniteur de machine virtuelle est un logiciel, un micrologiciel ou un matériel qui crée et exécute des ordinateurs virtuels. Il se situe entre le matériel et la machine virtuelle et est nécessaire pour virtualiser le serveur.

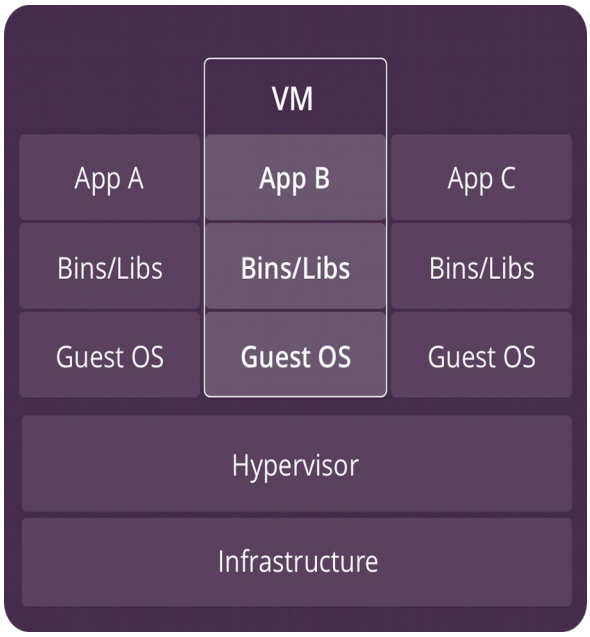


Figure (III.3) : Machine Virtuelle [6].

Depuis l'avènement de la technologie de virtualisation et des services d'infonuagique abordables, les services informatiques, grands et petits, ont adopté les machines virtuelles (VM) comme moyen de réduire les coûts et d'accroître l'efficacité [6].

III.5.B. Dans les conteneurs:

Avec les conteneurs, au lieu de virtualiser l'ordinateur sous-jacent comme une machine virtuelle, seul le système d'exploitation est virtualisé comme l'indique la figure (III.4).

Les conteneurs reposent sur le dessus d'un serveur physique et de son système d'exploitation hôte - généralement Linux ou Windows.

Chaque conteneur partage le noyau du système d'exploitation hôte et, généralement, les fichiers binaires et les bibliothèques. Les composants partagés sont en lecture seule. Le partage de ressources de système d'exploitation, telles que des bibliothèques, réduit considérablement le besoin de reproduire le code du système d'exploitation et signifie qu'un serveur peut exécuter plusieurs charges de travail avec une seule installation de système d'exploitation.

Les conteneurs sont donc exceptionnellement légers: leur taille ne dépasse pas les mégaoctets et ne prend que quelques secondes.

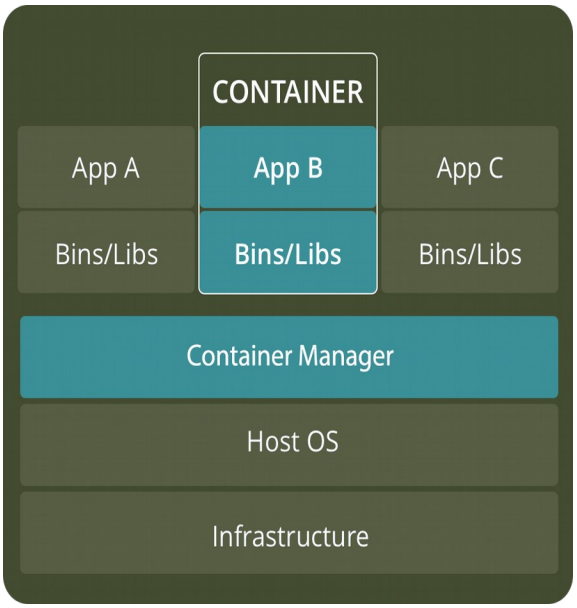


Figure (III.4) : Conteneurs [6].

Comparativement aux conteneurs, les VM prennent plusieurs minutes à fonctionner et sont d'un ordre de grandeur supérieur à un conteneur équivalent.

Contrairement aux ordinateurs virtuels, un conteneur nécessite uniquement un système d'exploitation, des programmes et des bibliothèques pris en charge, ainsi que des ressources système pour exécuter un programme spécifique [6].

Le tableau (III.1) résume les différences entre les machines virtuelles et les conteneurs :

Quelle est la Différence: VM vs Containers	
Les VM	**Les conteneurs**
Poids lourd	**Poids léger**
Performance limitée	**Performance native**
Chaque VM s'exécute dans son propre système d'exploitation	**Tous les conteneurs partagent le système d'exploitation hôte**
Virtualisation de niveau matériel	**Virtualisation de système d'exploitation**
Temps de démarrage en minutes	**Temps de démarrage en millisecondes**
Alloue la mémoire requise	**Nécessite moins d'espace mémoire**
Entièrement isolé et donc plus sécurisé	**Isolation au niveau du processus, éventuellement moins sécurisée**

Tableau (III.1) : Les différences entre les machines virtuelles et les conteneurs [6].

III.6. Pourquoi utiliser des conteneurs ?

Plutôt que de virtualiser le parc matériel comme le font les machines virtuelles, les conteneurs permettent une virtualisation au niveau du système d'exploitation, et de nombreux conteneurs s'exécutent directement au-dessus du noyau de cet OS.

Les conteneurs sont donc extrêmement légers : ils partagent le même noyau, démarrent très rapidement et leur exécution demande très peu de mémoire comparé au lancement d'un système d'exploitation [4].

III.7. Les avantages des conteneurs :

III.7.A. Indépendance de la plate-forme:

Un des principaux avantages des conteneurs est leur portabilité. Un conteneur encapsule une application avec tout ce dont elle a besoin pour s'exécuter, comme des fichiers de configuration et des dépendances. Cela vous permet d'exécuter facilement et de manière fiable des applications sur

différents environnements, tels que votre ordinateur de bureau local, vos serveurs physiques, vos serveurs virtuels, les tests, le transfert, les environnements de production et les clouds publics ou privés.

Cette portabilité offre aux entreprises une grande flexibilité, accélère le processus de développement et facilite le passage à un autre environnement Cloud ou à un autre fournisseur, le cas échéant [7].

III.7.B. Isolement efficace et partage des ressources:

Même si les conteneurs s'exécutent sur le même serveur et utilisent les mêmes ressources, ils n'interagissent pas entre eux. Si une application se bloque, d'autres conteneurs avec la même application continueront à fonctionner parfaitement et ne rencontreront aucun problème technique. Cette isolation réduit également les risques de sécurité: si une application devait être piratée ou violée par un logiciel malveillant, les effets négatifs en résultant ne seraient pas étendus aux autres conteneurs en cours d'exécution [7].

III.7.C. Sécurité:

Les conteneurs sont autonomes et n'interagissent pas les uns avec les autres. Cela signifie que si votre entreprise exploite une série de conteneurs sur les mêmes ressources et qu'un conteneur tombe en panne, les autres continueront à fonctionner sans interruption. C'est également un avantage en termes de sécurité - si un conteneur est piraté, l'impact devrait être - comme son nom l'indique – contenu.

Les conteneurs légers peuvent être démarrés et arrêtés en quelques secondes. Les conteneurs problématiques peuvent être arrêtés sans affecter les autres systèmes de l'entreprise. Les mises à jour, quant à elles, peuvent également être effectuées rapidement, ce qui signifie que des fonctionnalités peuvent être ajoutées facilement et que les bogues errants susceptibles de générer des problèmes de sécurité sont minimisés [8].

III.8. Les solutions containers

Les plates-formes de gestion de conteneurs facilitent l'organisation et la virtualisation des conteneurs de logiciels, également appelés virtualisations au niveau du système d'exploitation. Les développeurs utilisent des conteneurs pour lancer, tester et sécuriser des applications dans des environnements indépendants des ressources. Les conteneurs hébergent des composants d'applications, des bibliothèques ou des groupes de code source pouvant être exécutés à la demande.

Les plates-formes de gestion aident les utilisateurs à allouer des ressources pour optimiser l'efficacité et équilibrer les charges de travail du système.

Les conteneurs fournissent une plateforme flexible et portable pour organiser, automatiser et distribuer des applications. Les entreprises utilisent un logiciel de gestion des conteneurs pour rationaliser la livraison des conteneurs afin d'éviter les complexités d'architectures de systèmes

interdépendantes. Les outils sont évolutifs et peuvent grandement améliorer les performances d'applications largement distribuées.

De nombreuses solutions de gestion de conteneurs s'intègrent à un logiciel d'intégration continue pour accélérer le déploiement et l'intégration. De nombreuses solutions d'infrastructure informatique fonctionnent aussi bien à l'unisson qu'aux outils de gestion des conteneurs [9].

Pour pouvoir être inclus dans la catégorie gestion des conteneurs, un produit doit:

- Organiser les conteneurs et lancer des instances de conteneurs.
- Orchestrer et regrouper des conteneurs de cluster.
- Automatiser ou planifier l'exécution du conteneur.
- Répliquer les conteneurs pour une exécution simultanée.

III.8.A. La conteneurisation : quelle solution pour le cloud ?

Les conteneurs, peut aussi être défini comme une structure de données, ou également appelé ADT (type de donnée abstrait) et consiste en une collection de nombreux types de données différents. La taille de base de ces conteneurs dépend du nombre total de types de données qu'il contient. Dans un langage simple, il stocke une variété d'objets de manière organisée en fonction d'une règle ou d'une méthode d'accès particulière.

Cloud computing est l'une des technologies ou méthodologies les plus récentes utilisant un réseau de serveurs distants pour stocker, gérer ou traiter des données, via et suivant les protocoles de service Internet. Cette technique est très utile pour presque tous les types de services en ligne fournis aux utilisateurs via le WWW (World Wide Web), pour leur permettre d'avoir un accès complet aux informations, données ou objets, à n'importe quel lien ou en tout lieu, sans avoir à transporter ces objets partout avec eux [10].

III.8.B. Le classement des meilleures solutions containers 2019:

Selon "G2 Grid® pour la gestion des conteneurs" le meilleur classement des plates-formes containers de l'année 2019 est le suivant :

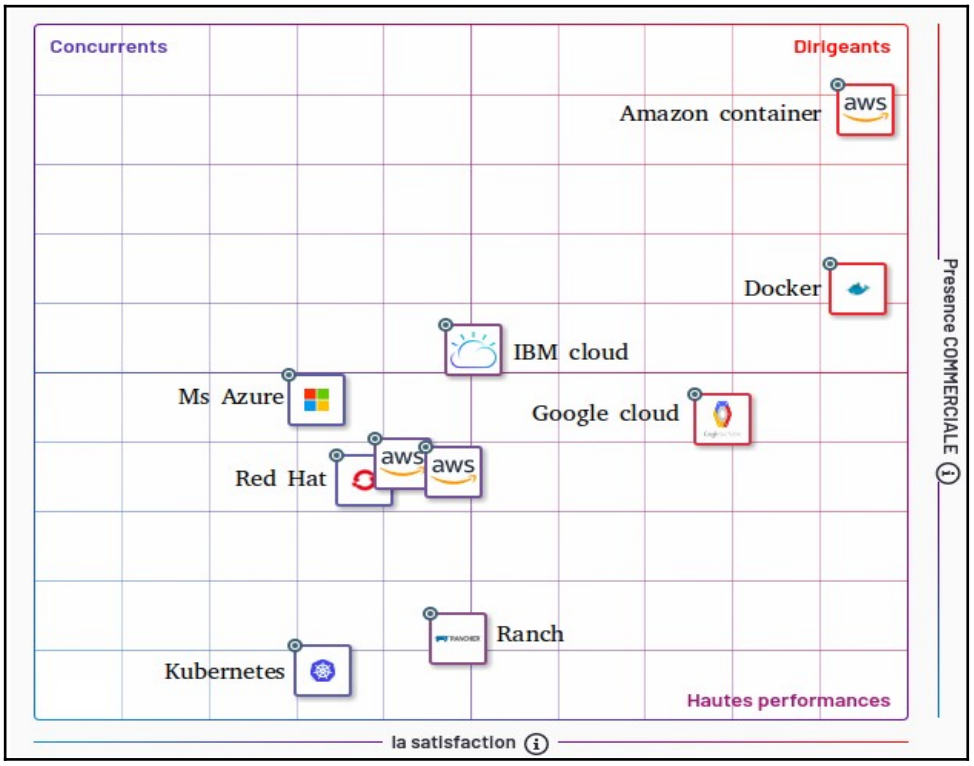


Figure (III.5) : Le meilleur classement des plates-formes containers de l'année 2019 [11].

Pour cela on va parler de la meilleure et la plus populaire plateforme de gestion des conteneurs qu'il s'agit de docker.

III.8.C. Docker:

III.8.C.1. Vue d'ensemble de docker:

Docker est une plate-forme ouverte de développement, d'exportation et d'exécution d'applications. Docker vous permet de séparer vos applications de votre infrastructure afin de pouvoir livrer des logiciels rapidement. Avec Docker, vous pouvez gérer votre infrastructure de la même manière que vous gérez vos applications. En tirant parti des méthodologies de Docker pour l'envoi, le test et le déploiement rapides de code, vous pouvez réduire considérablement le délai entre l'écriture du code et son exécution en production [12].

III.8.C.2. La plateforme docker:

Docker fournit des outils et une plateforme pour gérer le cycle de vie de vos conteneurs:

- Développez votre application et ses composants de support à l'aide de conteneurs.
- Le conteneur devient l'unité de distribution et de test de votre application.
- Lorsque vous êtes prêt, déployez votre application dans votre environnement de production, en tant que conteneur ou service orchestré. Cela fonctionne de la même manière, que votre environnement de production soit un centre de données local, un fournisseur de cloud ou un hybride des deux [12].

III.8.C.3. Moteur Docker:

Docker Engine est une application client-serveur avec les composants principaux suivants:

- Un serveur qui est un type de programme à exécution longue appelé processus démon.
- Une API REST qui spécifie les interfaces que les programmes peuvent utiliser pour communiquer avec le démon et lui indiquer quoi faire.
- Un client d'interface de ligne de commande (CLI).

La CLI utilise l'API REST Docker pour contrôler ou interagir avec le démon Docker via des scripts ou des commandes directes de la CLI. De nombreuses autres applications Docker utilisent les API et CLI sous-jacentes.

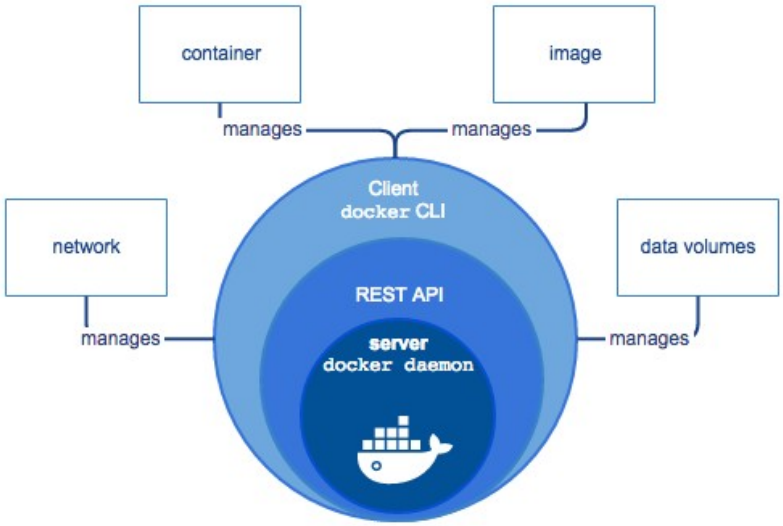


Figure (III.6) : Docker Engine [12].

Le démon crée et gère des objets Docker, tels que des images, des conteneurs, des réseaux et des volumes comme le montre la figure (III.6) [12].

III.8.C.4. L'architecture docker:

L'architecture Docker utilise un modèle client-serveur et comprend 3 composants (voir la figure (III.7)):

- Client Docker.
- Hôte Docker.
- Registre Docker.

Docker utilise une architecture client-serveur. Le **client Docker** communique avec le **démon Docker,** qui effectue le levage du bâtiment, l'exécution et la distribution de vos conteneurs Docker.

Le client et le démon Docker peuvent s'exécuter sur le même système ou vous pouvez connecter un client Docker à un démon Docker distant. Le client et le démon Docker communiquent à l'aide d'une **API REST**, via des sockets UNIX ou une interface réseau [13].

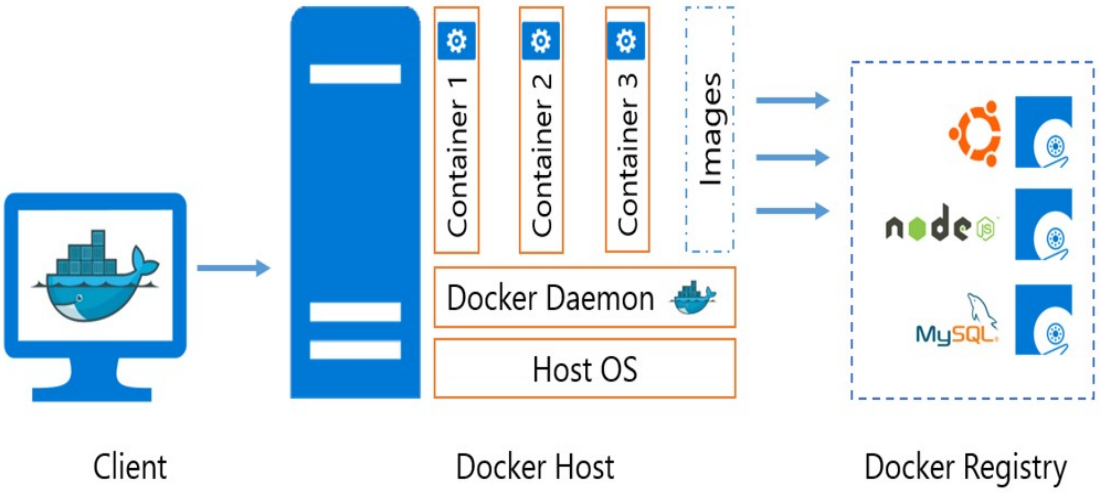


Figure (III.7) : L'architecture docker [13].

III.8.C.4.1. L'hôte Docker

Hôte Docker exécute le Docker DAemon. Docker Daemon écoute les demandes Docker. Les demandes de Docker peuvent être "exécution de docker", "construction de docker", n'importe quoi. Il gère les objets de menu fixe tels que les images, les conteneurs, les réseaux et les volumes [13].

III.8.C.4.2. Le client Docker

Docker Client est utilisé pour déclencher des commandes Docker. Lorsque nous envoyons une commande (construction de docker, exécution de docker, etc.), le client docker termine ces commandes vers le démon Docker qui les traitera ultérieurement.

Remarque : le client Docker peut communiquer avec plusieurs démons [13].

III.8.C.4.3. Registres Docker

Le registre est une application côté serveur hautement évolutive et sans état qui permet de stocker et de distribuer des images Docker. Vous pouvez créer votre propre image ou utiliser des registres publics, à savoir Docker Hub et Docker Cloud. Docker est configuré pour rechercher des images sur Docker Hub par défaut.

Ainsi, lorsque nous exécutons la commande **docker pull** ou **docker run** , les images requises sont extraites de votre registre configuré. Lorsque vous utilisez la commande **docker push** , votre image est transférée dans le registre configuré [13].

III.8.C.4.4. Un cluster:

Un cluster est composé d'un ordinateur maître et de plusieurs ordinateurs ou nœuds d'ouvrier. Le maître se coordonne entre tous les nœuds [14].

III.8.C.4.5. Un noeud:

Un nœud est un poste de travail, une machine virtuelle ou un ordinateur physique contenant des services permettant d'exécuter des pods. Il est contrôlé par un maître qui se coordonne entre tous les nœuds.

III.8.C.5. Référence d'exécution de Docker

Docker exécute les processus dans des conteneurs isolés. Un conteneur est un processus qui s'exécute sur un hôte. L'hôte peut être local ou distant. Lorsqu'un opérateur s'exécute docker run, le processus de conteneur qui s'exécute est isolé en ce sens qu'il possède son propre système de fichiers, son propre réseau et son propre arbre de processus isolé, distinct de l'hôte.

Cette page explique comment utiliser la docker run commande pour définir les ressources du conteneur lors de l'exécution [12].

III.8.C.6. Forme générale:

Le docker run commande de base prend cette forme:

$ docker run **[OPTIONS]** IMAGE**[:TAG|@DIGEST] [COMMAND] [ARG...]**

Le docker **run commande** doit spécifier une **IMAGE** pour dériver le récipient à partir. Un développeur d'image peut définir des images par défaut liées aux éléments suivants:

- Détaché ou courant au premier plan.
- Identification du conteneur.
- Paramètres réseau.
- Contraintes d'exécution sur le processeur et la mémoire.

Avec le, docker **run [OPTIONS]** un opérateur peut ajouter ou remplacer les valeurs d'image par défaut définies par un développeur. De plus, les opérateurs peuvent remplacer presque toutes les valeurs par défaut définies par le moteur d'exécution Docker lui-même.

La capacité de l'opérateur à remplacer les valeurs par défaut de l'image et de l'exécution de Docker est la raison pour laquelle **run** à plus d'options que toute autre docker commande le tableau Tableau (III.2) ci-dessous représente les commandes de base pour le docker [12].

III.8.C.7. Quelques commandes de base :

Commander	La description
attacher docker	Attachez les flux d'entrée, de sortie et d'erreur standard locaux à un conteneur en cours d'exécution
construction de docker	Construire une image à partir d'un fichier Docker
constructeur de docker	Gérer les builds
docker checkpoint	Gérer les points de contrôle
docker commit	Créer une nouvelle image à partir des modifications d'un conteneur
config docker	Gérer les configurations Docker
conteneur docker	Gérer les conteneurs
docker cp	Copier des fichiers / dossiers entre un conteneur et le système de fichiers local

Tableau (III.2) : Les commandes de base pour le docker [15].

III.8.C.8. Red Hat linux entreprise:

Figure (III.8) : logo du redhat [16].

III.8.C.8.1. Définition:

Red Hat Enterprise Linux (RHEL) est une distribution du système d'exploitation Linux développé pour le marché des entreprises. RHEL s'appelait auparavant Red Hat Linux Advanced Server.

RHEL est basé sur du code source libre et gratuit. Bien que Red Hat rend son code source disponible pour le téléchargement, la copie exacte de la distribution est interdite.

Le système d'exploitation RHEL (OS) prend en charge les charges de travail diverses dans physique, virtuels et cloud environnements. Les éditions RHEL sont disponibles pour les serveurs, les ordinateurs centraux, les ordinateurs de bureau et OpenStack [17].

III.8.C.8.2. Déploiement d'un cloud privé:

Un cloud privé permet de contrôler et de faire évoluer plus facilement les politiques de sécurité, les exigences en matière de conformité, le budget et les réglementations. La solution Red Hat®OpenStack® Platform fournit une infrastructure cloud qui crée rapidement et facilement des ressources virtuelles. En la déployant sur Red Hat Enterprise Linux®, le système d'exploitation natif d'OpenStack, vous obtenez une base solide pour créer, déployer et prendre en charge les environnements cloud au sein de votre entreprise.

Vous pouvez aussi partir de zéro avec la solution Red Hat Cloud Infrastructure qui vous offre tous les outils dont vous avez besoin pour mettre en place un cloud privé : le système d'exploitation, la plateforme de virtualisation, les outils de cloud computing et les fonctionnalités de gestion [18].

III.8.C.8.3. Déploiement de conteneurs dans le cloud:

Le déploiement de conteneurs dans le cloud revient plus ou moins à déployer une solution PaaS (qui fournit le langage, les environnements d'exécution et les applications) sur une IaaS (qui fournit les réseaux, le système de stockage, les serveurs et la technologie de virtualisation). Pris séparément, ils sont limités. D'un côté, l'environnement IaaS est flexible, mais il faut le configurer pour chaque application déployée.

De l'autre, la solution PaaS peut verrouiller un environnement, mais cela complique la personnalisation des environnements d'exécution des applications. En les déployant ensemble, vous pouvez limiter les contraintes [18].

III.8.C.8.4. Openshift container:

Un outil de gestion pour les infrastructures de cloud privé et virtuelles:

La solution Red Hat OpenShift Container Platform fournit des environnements d'entreprise pour la création, le déploiement et la gestion des applications conteneurisées dans tous les datacenters publics ou privés qui prennent en charge Red Hat Enterprise Linux.

Avec Red Hat OpenShift Container Platform, vous pouvez exploiter votre propre cluster, sur votre propre infrastructure, ce qui vous octroie le contrôle total de votre environnement de conteneurs [19].

III.8.C.8.5. L'architecture red hat :

La figure (III.9) représente l'architecture des conteneurs Linux dans Red Hat Enterprise Linux, Plusieurs composants sont nécessaires au bon fonctionnement des conteneurs Linux. La plupart d'entre eux sont fournis par le noyau Linux. Les espaces de noms de noyau garantissent l'isolation des processus et des groupes de contrôle sont utilisés pour contrôler les ressources système. SELinux est utilisé pour assurer la séparation entre l'hôte et le conteneur, ainsi qu'entre les conteneurs individuels.

L'interface de gestion forme une couche supérieure qui interagit avec les composants de noyau susmentionnés et fournit des outils pour la construction et la gestion de conteneurs [20].

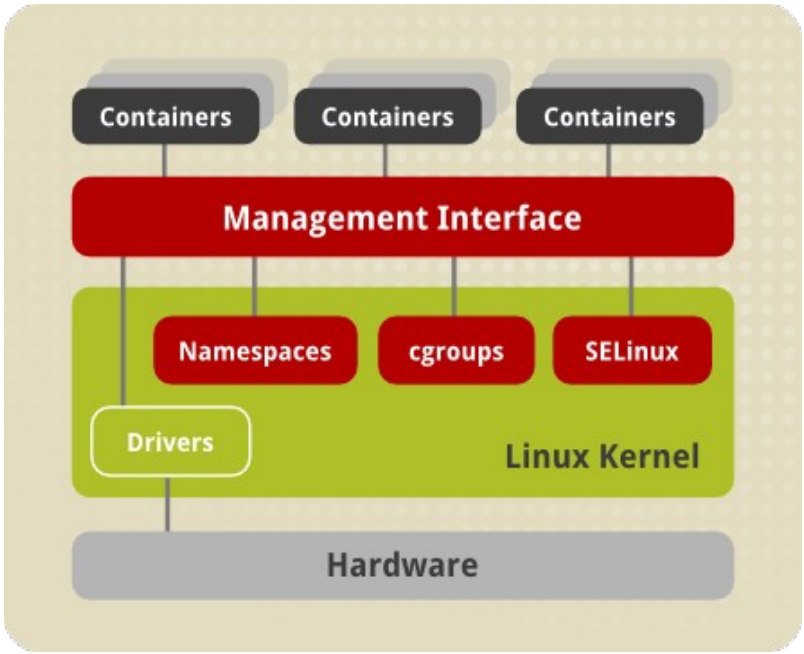


Figure (III.9) : l'architecture des conteneurs Linux dans Red Hat Enterprise Linux [21].

III.8.D. Kubernetes vs Docker:

Figure (III.10) : Logo du Kubernetes [22].

III.8.D.1. Définition:

Kubernetes Engine est un environnement géré et prêt à l'emploi pour le déploiement d'applications en conteneur. Il regroupe nos dernières innovations en matière de productivité des développeurs, d'efficacité des ressources, d'automatisation des opérations et de flexibilité Open Source pour accélérer vos temps de production.

Lancé en 2015, Kubernetes Engine s'appuie sur plus de 12 ans d'expérience de Google en matière de gestion de services tels que Gmail et YouTube sous forme de conteneurs. Grâce à Kubernetes Engine, configurez Kubernetes en un rien de temps. En effet, dans cet environnement, vous n'avez plus besoin d'installer, de gérer, ni d'exploiter vos propres clusters Kubernetes [23].

III.8.D.2. Kubernetes vs Docker:

On compare très souvent Kubernetes avec la plateforme de stockage de container Docker, et plus précisément avec Docker Swarm la solution de clustering native pour les containers Docker. Ces deux outils offrent en effet des fonctionnalités de création et de gestion de containers virtuels. Cependant, ces deux systèmes présentent de nombreuses différences.

Tout d'abord, Docker se révèle plus simple à utiliser que Kubernetes. L'un des défauts souvent reproché à Kubernetes est en effet sa complexité. Par exemple, Kubernetes est très long à installer et à configurer, et nécessite une certaine planification car les noeuds doivent être définis avant de débuter. La procédure diffère également pour chaque système d'exploitation.

De son côté, Docker Swarm utilise la CLI de Docker pour exécuter toutes les portions de son programme. Il suffit d'apprendre à maîtriser cet ensemble d'outils pour pouvoir créer des environnements et des configurations. Il n'est pas non plus nécessaire de cartographier les clusters avant de commencer [24].

En outre, Kubernetes peut être exécuté par dessus Docker mais nécessite de connaître les caractéristiques de leurs CLI respectives pour pouvoir accéder aux données via l'API. Il faut connaître la CLI de Docker pour naviguer au sein de la structure, et la CLI kubectl de Kubernetes pour exécuter les programmes. En comparaison, l'utilisation de Docker Swarm se rapproche de celle des autres

outils Docker comme Composé. On utilise la même CLI Docker, et il est même possible de lancer de nouveaux containers avec une simple commande. De par sa vitesse, sa polyvalence et sa simplicité d'utilisation, Docker prend donc un certain avantage sur Kubernetes en termes d'usabilité.

Les deux plateformes se distinguaient aussi jadis par le nombre de containers qu'il est possible de lancer, ainsi que par leur taille. Dans ce domaine, Kubernetes avait l'avantage. Cependant, les récentes mises à jour de Docker ont permis de réduire l'écart.

Désormais, les deux systèmes peuvent prendre en charge un maximum de 1000 clusters et 30 000 containers. Cependant, un test mené par Docker en mars 2016 révèle que Docker peut lancer le même nombre de containers que Kubernetes cinq fois plus rapidement. En revanche, une fois les containers lancés, Kubernetes conserve un avantage en termes de réactivité et de flexibilité.

Quoi qu'il en soit, rien n'empêche d'utiliser à la fois Kubernetes et Docker Swarm. Il est par exemple possible d'utiliser conjointement Docker et Kubernetes pour coordonner la programmation et l'exécution de containers Docker sur Kubelets. Le moteur Docker se charge d'exécuter l'image de container, tandis que la découverte de service, l'équilibrage des tâches et le networking sont gérés par Kubernetes. Ces deux outils sont donc très adaptés au développement d'architecture Cloud moderne malgré leurs différences [24].

III.9. Conclusion:

Dans ce chapitre, nous avons découvert la notion de conteneurisation et ses différentes solutions désignées comme nouvelles plateformes pour la gestion, la sécurité et le déploiement des applications sur plusieurs environnements dédiés au stockage voir au cloud computing, en partant du Docker vers Red hat au Kubernetes.

Références chapitre III

[1] the docker book by James Turnbull

[2] https://www.techopedia.com/definition/31234/containerization-computers

[3] https://nickjanetakis.com/assets/blog/cards/differences-between-a-dockerfile-docker-image-and-docker-container-001320c81dd8d2989df10d0bec36341fd6a94b043f6f9de1c26ee79eaf16e566.jpg

[4] https://cloud.google.com/containers/?hl=fr

[5] https://cloud.google.com/containers/?hl=fr

[6] article : "What's the Diff: VMs vs Containers" by Roderick Bauer

[7] article ;"Top 7 benefits of using containers" by kumina

[8] article : "Five business benefits of containers" by Mark Samuels for Build What's Next

[9] https://www.g2crowd.com/categories/container-management?segment=all

[10] article "Ease your cloud service working with cloud container technology" by sumant bag

[11] https://www.g2.com/categories/container-orchestration

[12] https://docs.docker.com/engine/docker-overview/

[13] article "Docker Architecture" by Ramandeep

[14] https://medium.com/devopslinks/understanding-nodes-pods-containers-and-clusters-778dbd56ade8

[15] https://docs.docker.com/engine/reference/commandline/docker/

[16] https://www.redhat.com/en/about/brand/standards/logo

[17] https://searchdatacenter.techtarget.com/definition/Red-Hat-Enterprise-Linux-RHEL

[18] https://www.redhat.com/fr/topics/cloud

[19] https://www.redhat.com/fr/technologies/cloud-computing/openshift

[20] livre "Red Hat Enterprise Linux Atomic Host 7"

[21] https://access.redhat.com/documentetion/enus/red_hat_entreprise_linux_atomic_host/7/html/overviw_of_containers_in_red_hat_systems/introduction_to_linux_containers

[22] https://www.ovh.com/fr/blog/why-ovh-managed-kubernetes/

[23] https://cloud.google.com/kubernetes-engine/

[24] article "Kubernetes – Tout savoir sur la plateforme d'orchestration de containers"par Bastien-L

Chapitre IV :

Matériels et Méthodes

IV.1. Introduction:

Dans les chapitres précédents, nous avons abordé une étude théorique et comparative du cloud computing, tout en expliquant son principe de fonctionnement et ses différentes plateformes et architectures.

Dans ce présent chapitre, nous présentons notre modèle de déploiement et mettons en œuvre notre solution proposée, une solution basée sur un serveur cloud personnel conçu à l'intérêt des entreprises en général et à l'individu en particulier.

IV.2. Etude de solution :

IV.2.A. Choix du matériel:

Nous avons utilisé une carte raspberry pi sur laquelle nous avons installé le serveur cloud, pour simuler le cas d'un fournisseur de services Cloud.

IV.2.B. Cloud open source

Afin de mettre en place notre serveur, nous avons opté pour "NextCloud" qui est une solution open sources, de manière à gérer nos propres services de partage, stockage et sécurité sans le moindre coût d'hébergement.

IV.2.C. Cloud sous docker

Pour la performance et le bon déploiement du serveur, nous allons utiliser la technologie des conteneurs citée dans le chapitre précédent et tout intégrer sous Docker.

IV.4.D. Serveur NAS externe

En vue de l'importance du service de stockage des données dans le cloud, nous avons ajouté un espace partagé en interne et en externe du réseau tout en gagnant la mobilité et le contrôle du volume

IV.5.E. Protection cloud:

La sécurité des données est un enjeu vital pour les utilisateurs cloud, pour cela nous avons renforcé la protection de notre serveur en adoptant un modèle d'environnement cloné et chiffré.

IV.3. Environnement :

IV.3.A. hardware utilisé:

Le Raspberry Pi n'est rien d'autre qu'un ordinateur réduit à sa plus simple expression: une unique carte à processeur ARM un poil plus grande qu'une carte de crédit. Son intérêt est de rendre l'informatique abordable et accessible à tous (comptez entre 5 et 35 € suivant

les modèles) tout en encourageant l'apprentissage de la programmation informatique et de ses différents langages [1].

Même si vous n'êtes pas un grand passionné de hardware et de programmation informatique, il y a fort à parier que vous avez déjà entendu parler du Raspberry Pi. Et en effet, comme nous allons le voir, ce nano-ordinateur novateur n'est pas seulement destiné à un public averti ! Débutants, amateurs, technophiles, petits et grands : le Raspberry Pi est à la portée de tous et ouvre un large champ de possibilités pour un tarif relativement léger [1].

IV.3.A.1. La fondation Raspberry Pi

Lancé en février 2012 (les premiers prototypes datent de 2006), le Raspberry Pi a été développé dans le cadre de la fondation Raspberry Pi avec le soutien de l'Université de Cambridge et du fabricant du semi-conducteurs Broadcom. Créée par David Braben (notamment connu pour avoir conçu le jeu vidéo Elite sur BBC Micro en 1984, puis sur Atari ST, Amiga et NES quelques années plus tard) ainsi que plusieurs professeurs de l'université de Cambridge, la fondation Raspberry Pi est une association caritative dont l'objectif est de promouvoir les bases de la programmation informatique dans les écoles [1].

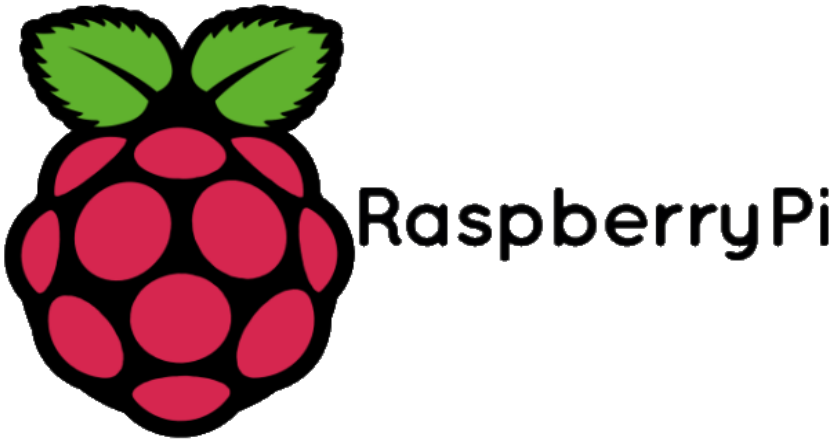


Figure (IV.1): Logo fondation Raspberry pi [2].

IV.3.A.2. Raspberry Pi : un succès largement mérité

Depuis le lancement en 2012 des premiers modèles A et B, respectivement vendu 25 et 35 $ et suivis par trois autres générations de cartes, **le Raspberry Pi s'est vendu a plus de 22 millions d'exemplaires** à travers le monde [1].

Le « Raspi » a, en effet, été initialement développé dans le but pédagogique d'encourager la jeunesse à s'intéresser à l'informatique et notamment à la programmation avec Scratch et Python. Fonctionnant avec un processeur ARM, les systèmes d'exploitation et logiciels aujourd'hui compatibles avec le Raspberry Pi sont légion, les tutoriels se multiplient et la communauté ne cesse de accroître au fil des années [3].

IV.3.A.3. Des milliers de projets envisageables

Des projets assez incroyables fleurissent chaque jour un peu partout sur le net. Néanmoins, parmi les usages les plus courants d'un Raspberry Pi, on peut trouver :

- L'apprentissage de la programmation et la découverte de systèmes d'exploitation open source.
- La création de média center et de console de rétrogaming, émulation de bornes d'arcade.
- L'utilisation comme matériel embarqué pour créer des robots ou autres appareils télécommandés.
- La mise en place de serveur web et mails, VPN, DNS, etc.
- La gestion d'un système domotique, le contrôle d'une imprimante 3D.

IV.3.A.4. Raspberry pi, c'est quoi:

Comme mentionné dans les paragraphes précédents, le Raspberry Pi est un nano-ordinateur mono-carte à processeur ARM et fait un peu penser à l'Arduino, ce circuit imprimé dont la plupart des composants sont sous licence libre.

Le Raspberry Pi est livré nu, c'est-à-dire sans boitier ni alimentation, et encore moins de clavier, souris ou écran. L'objectif ici est bien entendu de réduire les coûts au maximum et de permettre à son acquéreur de pouvoir recycler du matériel déjà en sa possession. Il est néanmoins possible de trouver des kits tout-en-un dans le commerce pour moins de 80 € [3].

IV.3.A.5. Modèles :

La Figure (IV.3) ci-dessous présente une illustration des différents modèles des cartes raspberry pi.

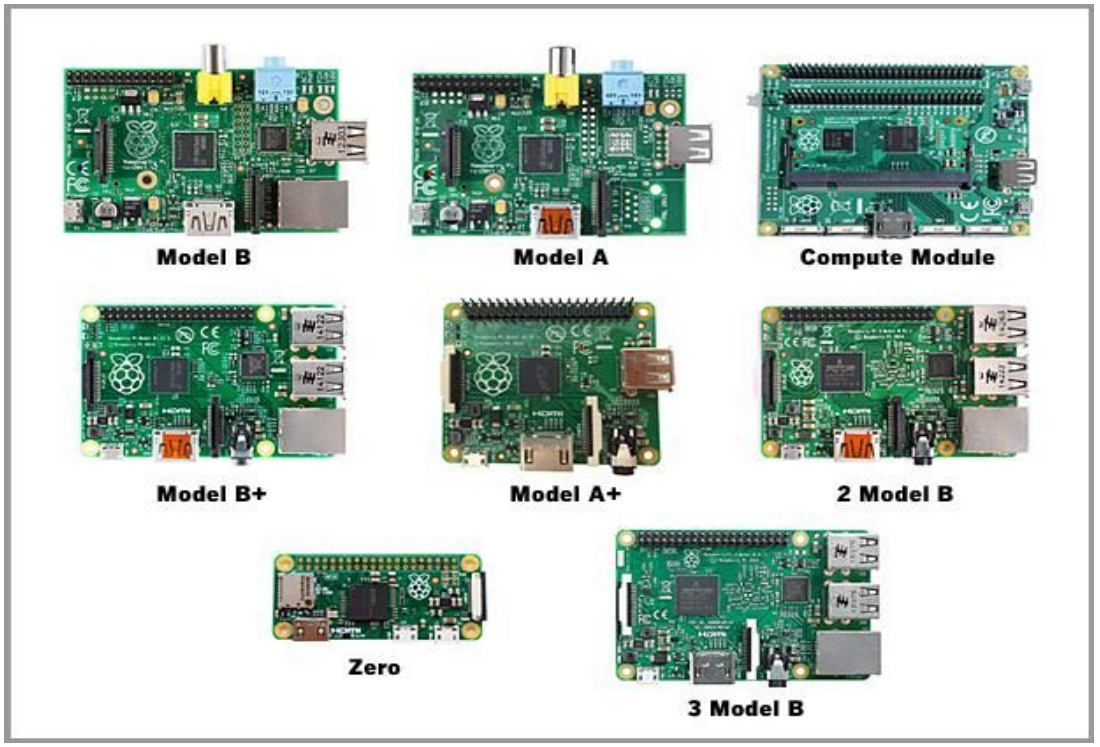


Figure (IV.2): Modèles Raspberry pi [5].

IV.3.A.6. Caractéristiques:

	Raspberry Pi 1 Model A	Raspberry Pi 1 Model A+	Raspberry Pi 1 Model B	Raspberry Pi 1 Model B+	Raspberry Pi 2 Model B	Raspberry Pi 3 Model B	Raspberry Pi Zero
USB 2.0 Ports	1	1	2	4	4	4	1 (Micro-USB)
Ethernet	None	None	10/100 Mbit/s	10/100 Mbit/s	10/100 Mbit/s	10/100 Mbit/s	None
Bluetooth	None	None	None	None	None	4.1	None
WiFi	None	None	None	None	None	802.11n	None
Audio In	I²S	I²S	I²S	I²S	I²S	I²S	I²S
Audio Out	I²S, analog (3.5mm jack), digital (HDMI)	I²S, analog (3.5mm jack), digital (HDMI)	I²S, analog (3.5mm jack), digital (HDMI)	I²S, analog (3.5mm jack), digital (HDMI)	I²S, analog (3.5mm jack), digital (HDMI)	I²S, analog (3.5mm jack), digital (HDMI)	Digital (mini-HDMI), analog GPIO PWM
Video In	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	None
Video Out	HDMI, Composite (RCA)	HDMI, Composite (TRRS)	HDMI, Composite (RCA)	HDMI, Composite (TRRS)	HDMI, Composite (TRRS)	HDMI, Composite (TRRS)	Mini-HDMI, GPIO Composite
External Storage	SD	MicroSD	SD	MicroSD	MicroSD	MicroSD	MicroSD

Tableau (IV.1) : Caractéristiques des différents modèles raspberry pi [6].

Pour notre projet nous allons travailler avec un Raspberry py 2 modèle B:

- 1GB RAM.
- 40pin GPIO.
- Micro SD.
- 4 Ports USB + HDMI + Vidéo+Caméra.

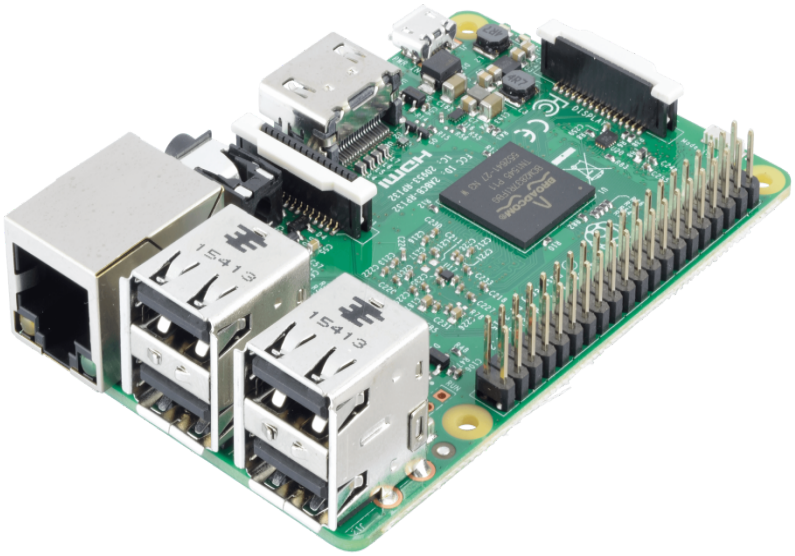


Figure (IV.3): Carte raspberry pi [4].

IV.3.B. Software utilisé:

Comme pour chaque ordinateur disposant d'un microprocesseur nécessite un système d'exploitation, pour le Raspberry pi il utilise diverses distributions basé sous linux, on compte parmi eux :

- Pidora
- Arch linux
- Kali linux
- Raspbian

Pour notre cas, on va utiliser la distribution “Raspbian” basé sous debian, car c’est la version la plus populaire et officielle de la fondation Raspberry pi.

IV.3.B.1. Installation de Raspbian:

Il faut se rendre sur le site officiel de raspberry pi et télécharger l’image iso raspbian , puis faire un montage de disque d’une carte SD 16 G avec le logiciel etcher .

IV.3.B.2. Etcher:

C’est un logiciel (libre) très simple d'utilisation qui permet de graver des fichiers images sur un disque USB ou sur une carte SD [7].

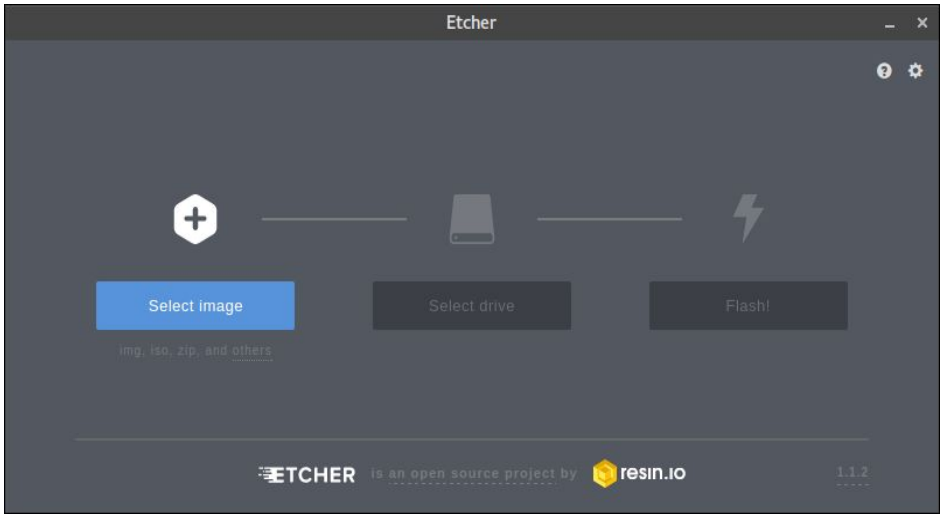


Figure (IV.4): Logiciel Etcher [8].

Après redémarrage de la carte, on fait notre choix du système à installer

Figure (IV.5) : Installation de raspbian [9].

IV.3.B.3. Mode de connexion :

Après avoir terminé l'installation, nous allons éliminer toutes sorte de périphérique, clavier, souris, moniteur ; câble rj45 afin d'avoir une meilleure manipulation et mobilité .Pour cela, nous allons nous connecter à distance à travers notre Pc hôte depuis un point d'accès du routeur via un dongle wifi placé dans le port usb de la carte raspberry pi.

IV.3.B.4. Mode VNC:

En informatique, Virtual Network Computing (VNC) est un système graphique de partage de postes de travail qui utilise le protocole RFB (Remote Frame Buffer) pour contrôler à distance un autre ordinateur . Il transmet les événements de clavier et de souris d'un ordinateur à un autre, en relayant les mises à jour de l'écran graphique dans l'autre sens, via un réseau [10].

IV.3.B.5. Mode ssh:

SSH pour secure shell est une solution logicielle de faible coût, permettant, sur un réseau de mettre vos données à l'abri des regards indiscrets. Il ne résout pas tous les problèmes de confidentialité et de sécurité mais il en élimine un certain nombre. Il offre essentiellement :

- Un protocole client/serveur sécurisé pour le chiffrement et la transmission des données sur un réseau.
- La possibilité de sécuriser des applications réseaux non sûres, comme Telnet, FTP et de nombreux autres programmes et protocoles reposant sur TCP/IP.
- Une transparence quasi complète pour l'utilisateur final.
- Des implémentations pour la plupart des systèmes d'exploitation [11].

Pour se connecter, on fait un scan réseau, afin d'obtenir les adresses ip des hôtes grâce à l'application Android "Fing".

IV.3.B.6. Configuration DHCP

Dans le but d'avoir une adresse IP fixe de la carte, nous allons la configurer en mode DHCP pour une connexion automatique au réseau pour chaque démarrage.

IV.3.B.7. Putty:

PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il permet également des connexions directes. À l'origine disponible uniquement pour Windows, il est à présent porté sur diverses plates-formes Unix [12].

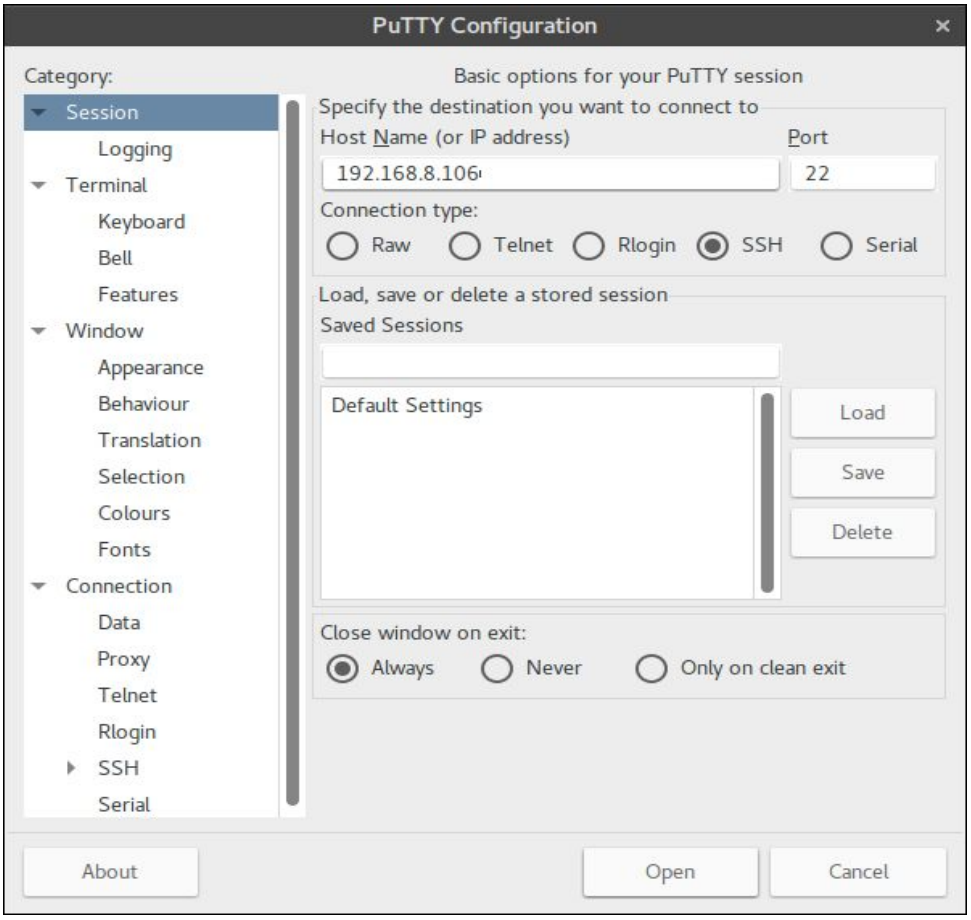


Figure (IV.6): Interface Putty [13].

IV.3.B.8. Mise à jour et mise à niveau du système d'exploitation Raspbian

Après une première connexion avec un login et un mot de passe, nous avons fait une mise à jour et une mise à niveau du système pour éviter toute sorte d'erreur, grâce à la commande :

```
sudo apt-get update && sudo apt-get upgrad
```

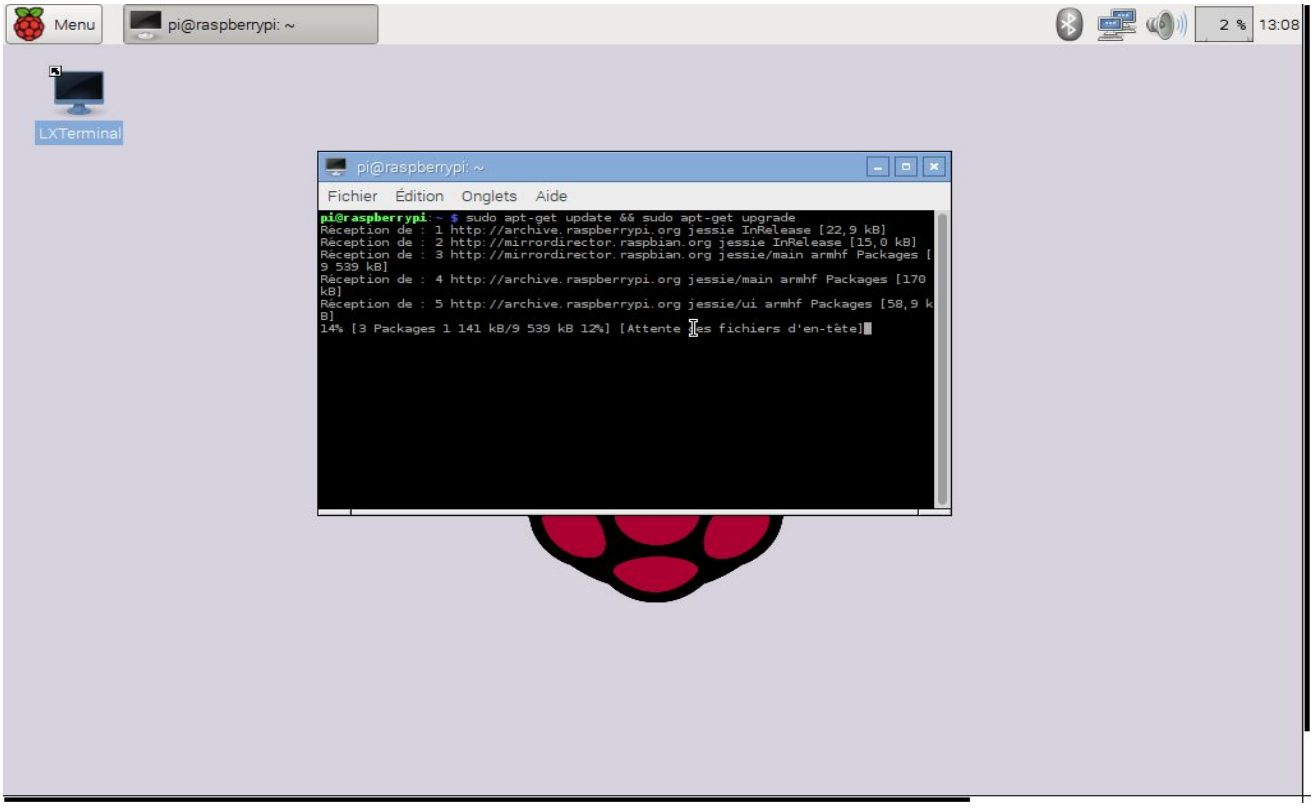


Figure (IV.7) : Mise à jour et à niveau du système [14].

Références chapitre iv

[1] Article: Matthieu Legouge “Qu'est-ce qu'un Raspberry Pi ? Introduction au nano-ordinateur

[2] https://pic.clubic.com/v1/images/1697249/raw

[3] http://formation.04sys.fr/le-raspberry-pi

[4] http://www.geekland-leblog.fr/wp-content/uploads/2015/07/raspberry-A-Copier.jpg

[5] https://cdn-reichelt.de/bilder/web/xxl_ws/A300/RASP_03_01.png

[6] https://images.techhive.com/images/article/2016/08/raspberry-pi-hardware-2016-2-100678887-gallery.idge.jpg

[7] https://doc.ubuntu.fr.org/etcher

[8] capture de logiciel etcher

[9] capture d'installation de Raspbian

[10] livre “Richardson, T .; Stafford-Fraser, Q .; Wood, KR; Hopper, A. (1998). "Informatique en réseau virtuel" ”

[11] Barrett, D. J., & Silverman, R. E. (2002). SSH, le shell sécurisé: la référence. " O'Reilly Media,
Inc.".

[12] https://fr.wikipedia.org/wiki/PuTTY

[13] capture d'interface putty

[14] capture de mise à jour et à niveau du système

Chapitre V :

Mise en place d’un serveur

V.1. Exécution du projet:

V.1.1. Installation de Docker :

Docker est un programme informatique qui effectue une virtualisation au niveau du système d'exploitation, également appelée "conteneurisation". Il a été libéré en 2013 et est développé par Docker, Inc.

Docker est utilisé pour exécuter des packages logiciels appelés "conteneurs". Les conteneurs sont isolés les uns des autres et regroupent leurs propres outils, bibliothèques et fichiers de configuration. Ils peuvent communiquer entre eux par le biais de canaux bien définis. Tous les conteneurs sont gérés par un seul noyau de système d'exploitation et sont donc plus légers que les ordinateurs virtuels. Les conteneurs sont créés à partir "d'images"qui spécifient leur contenu précis. Les images sont souvent créées en combinant et en modifiant des images standard téléchargées à partir de référentiels publics. [1]

Nous allons installer docker grâce à la commande suivante :

```
$curl -sSL https://get.docker.com | sh
```

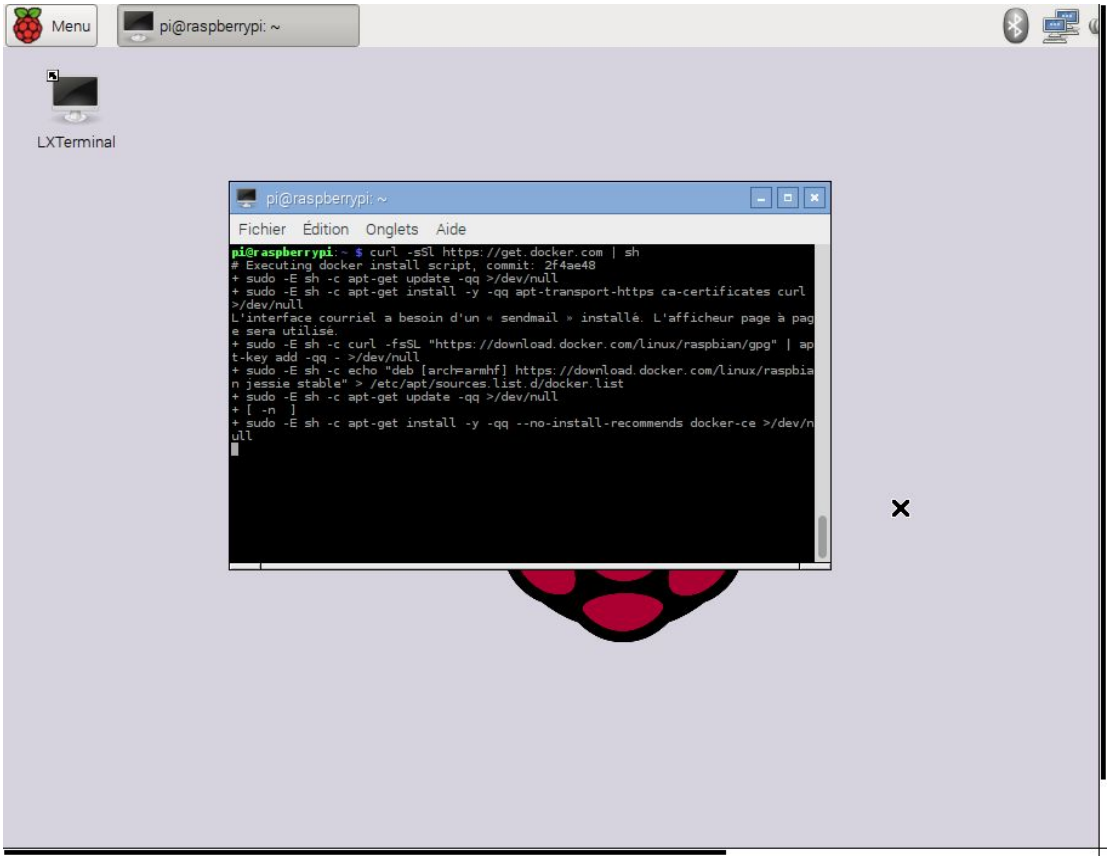


Figure (V.1) : Installation de docker [2].

Après que docker soit près à être utilisé, on va ajouter l'utilisateur "pi" au groupe docker pour lui donner la permission d'exécuter les commande docker :

V.1.2. L'ajout de la permission et la vérification de la version:

Pour ajouter la permission aux utilisateurs docker on lance la commande suivante :

```
$ sudo usermod -aG docker pi
```

On vérifie la version grâce à la commande :

```
$ docker version
```

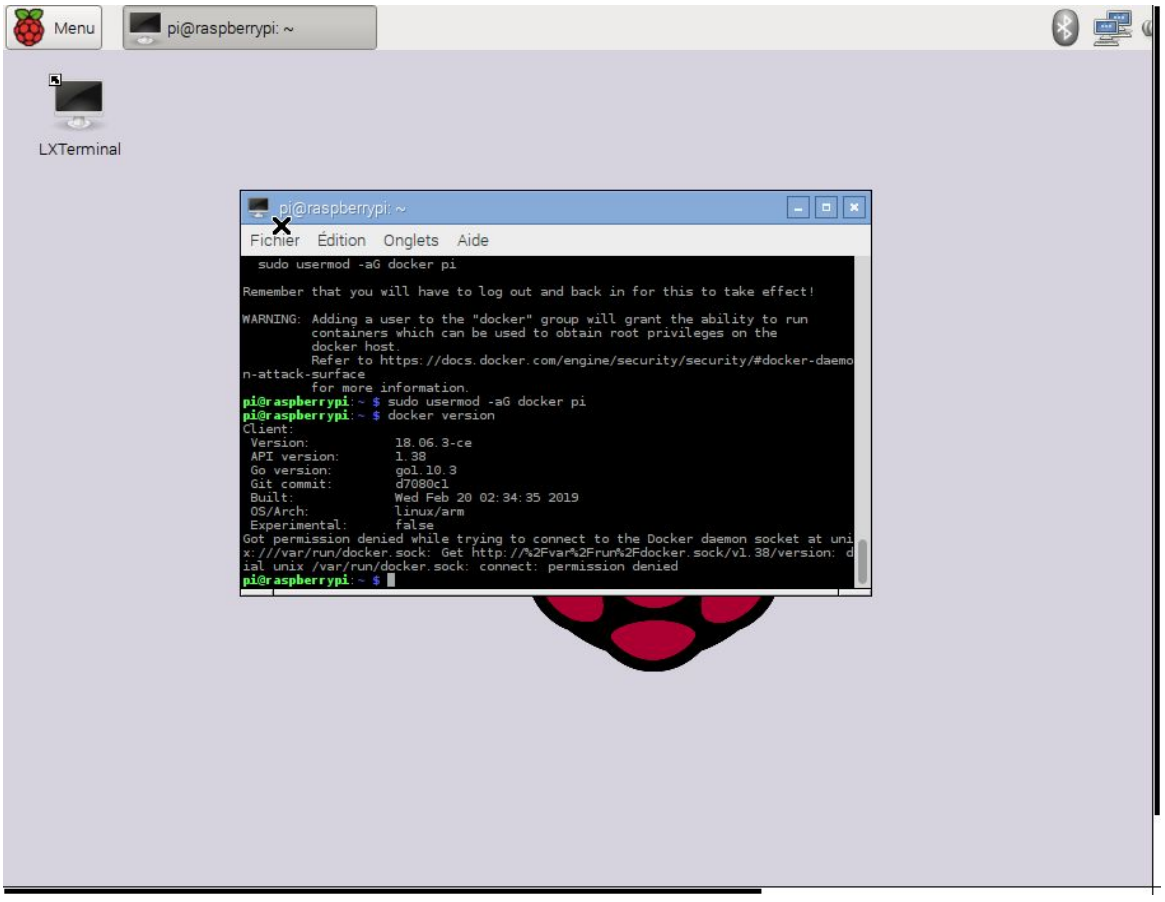


Figure (V.2) : Version docker [3].

Pour vérifier les informations et les erreurs du menu docker, nous devons taper:

```
$ docker info
```

V.1.3. Création du conteneur :

Maintenant nous allons passer à la création du fameux conteneur Hello-world pour assurer que notre installation a été bien déployée :

```
$ docker run hello-world
```

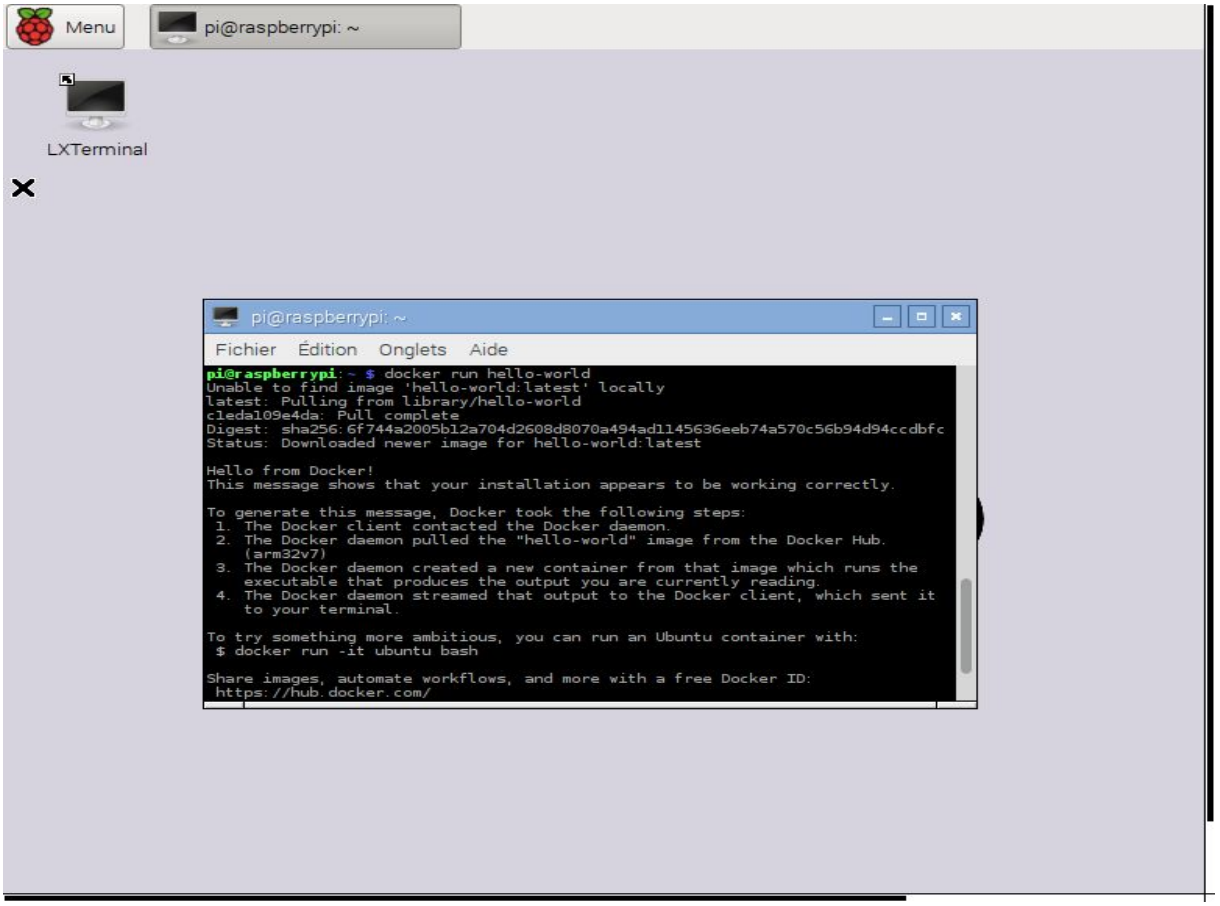


Figure (V.3): Création du conteneur [4].

V.1.4. Déploiement du serveur cloud :

Pourvu que le conteneur est prêt, nous procédons maintenant à la création d'image de notre serveur cloud personnel qui est nextcloudpi. Pour remédier à cela, nous téléchargeons l'image depuis le site officiel de nextcloudpi sur docker.

V.1.5. Nextcloud:

Nextcloud est une application d'auto-hébergement qui vous permet de sauvegarder vos contacts, vos images, et tous vos documents personnels dans un endroit centralisé. Avec Nextcloud, vous n'aurez pas besoin des solutions tierces comme Mega, DropBox, Box, Google Drive, etc.

Voici quelques caractéristiques de Nextcloud:

- La gestion des utilisateurs et groupes avec OpenID ou LDAP,
- L'accès de vos données existantes sur DropBox, un serveur FTP ou un NAS,
- Le support d'une authentification en deux étapes,
- La synchronisation des clients Nextcloud (mobiles, ordinateurs) avec le serveur,
- La possibilité de partager des documents avec les autres utilisateurs,
- La gestion depuis l'interface d'administration des appareils et applications connectés au serveur [5].

Figure (V.4): Logo nextcloud [5].

V.1.5.A. Nextcloud, à quoi ça sert ?

Nextcloud, est un logiciel libre, open source et gratuit de stockage de données. « A safe home for all your data. » Il s'installe sur le serveur que vous avez choisi (votre machine locale ou un serveur mutualisé loué auprès d'un fournisseur d'hébergement).

Une interface graphique permet de s'échanger facilement des fichiers ou des dossiers sans avoir besoin par ex. de joindre des pièces jointes dans des emails [6].

V.1.5.B. Quelle différence avec un « hébergement propriétaire » ?

Un « hébergement propriétaire » renvoie à une personne (physique ou morale) qui a opté pour un logiciel dont le code source n'est pas ouvert pour stocker des données. Cela peut également désigner un gros hébergeur – souvent soumis à la législation américaine proposant un quota d'espace disque gratuit en échange de certaines de vos données personnelles.

Si vous optez, pour l'installation sur votre machine (ou une machine louée dans un data center) d'un logiciel dont le code source a été analysé par une communauté, vous êtes dans le cadre d'un hébergement alternatif ou « libre »de données. Comme tout logiciel, il ne sera pas exempt de bugs, mais, vous aurez une garantie plus importante que le logiciel installé par vos soins ou celui d'un prestataire face uniquement ce qu'il est sensé faire. Par ailleurs, éviter un gros hébergeur permet de limiter le risque d'un crack massif très rémunérateur pour des délinquants numériques [6].

V.1.6. NextcloudPi:

NextCloudPi est une instance Nextcloud préinstallée et préconfigurée. Elle comprend une interface de gestion avec tous les outils nécessaires pour héberger soi-même vos données privées dans un seul package.

Il s'agit d'un projet officiel de la communauté open source qui vise à faciliter le contrôle de chacun sur ses propres données [7].

Figure (V.5): Logo NextcloudPi [8].

V.1.6.A. Installation de NextcloudPi sous doker:

Nous allons télécharger l'image de nextcloudpi grâce à la commande ci-dessous, depuis le site offciel d'ownyourbit², pour cela il faut se mettre au super utilisateur root pour avoir tous les droits d'exécutions.

$ sudo su

#docker run -d -p 4443:4443 -p 443:443 -p 80:80 -v ncdata:/data --name nextcloudpi ownyourbits/nextcloudpi-armhf $IP

Vous pouvez remarquer que l'adresse ip de la carte raspberry pi a changé de réseau, 192.168.1.x au 192.168.8.x, c'est juste parce qu'on a travaillé avec deux routeurs différents.

Figure (V.6) : Installation de nextcloudpi sous docker [9].

Après que l'image nextcloudpi a été téléchargée avec succès, nous pouvons vérifier son statut et faire un premier login comme le montre la figure (IV.1) :

$ sudo su : pour passer au supere utilisateur

docker ps –a :

```
# docker logs -f nextcloudpi
```

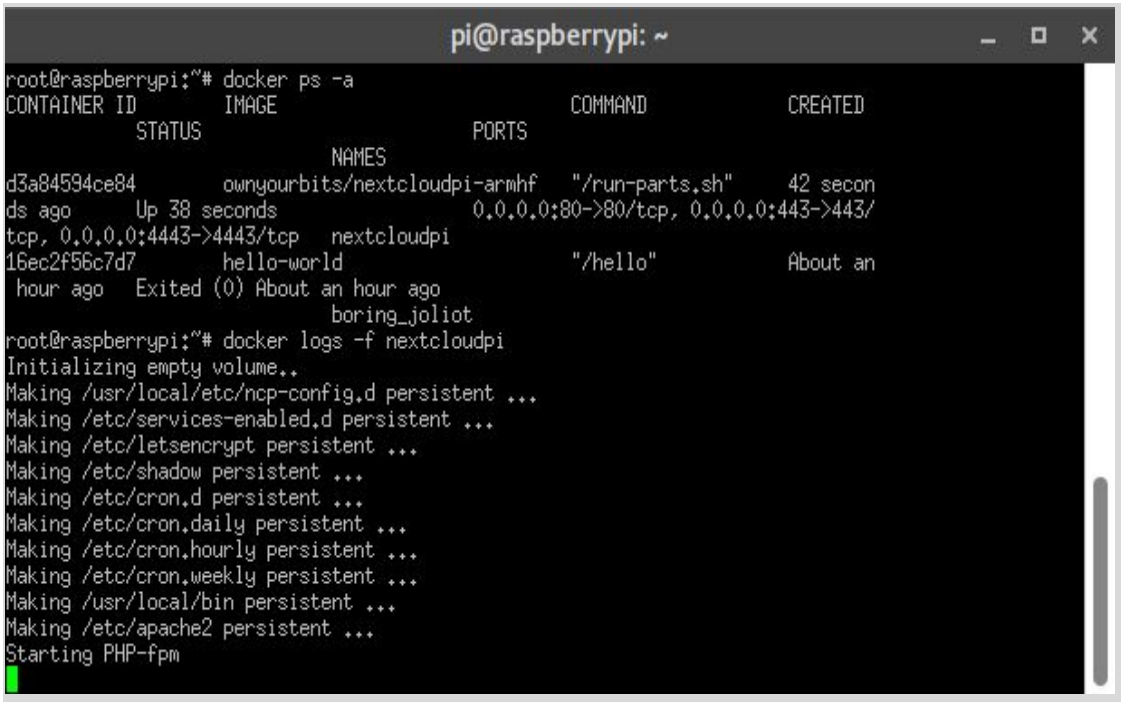


Figure (V.7) : Vérification du statut de l'image docker [10].

Maintenant, il nous reste qu'à exécuter le serveur sous docker avec la commande ci-dessous:

```
$ docker start nextcloudpi
```

V.1.6.B. Activation de Nextcloupi:

Enfin, il semble que les conteneurs de menu docker en montage pour x86 et ARM mettent en cache en termes de taille réduite. C'est une bonne nouvelle car cela allège le fardeau de la création et de la maintenance des images de base minidebian et miniraspbian car c'est le but principal de docker.

Il nous reste maintenant qu'à accéder à la plateforme nextcloudpi à partir du navigateur via l'adresse ip de raspberry pi comme montre la figure (IV, 2):

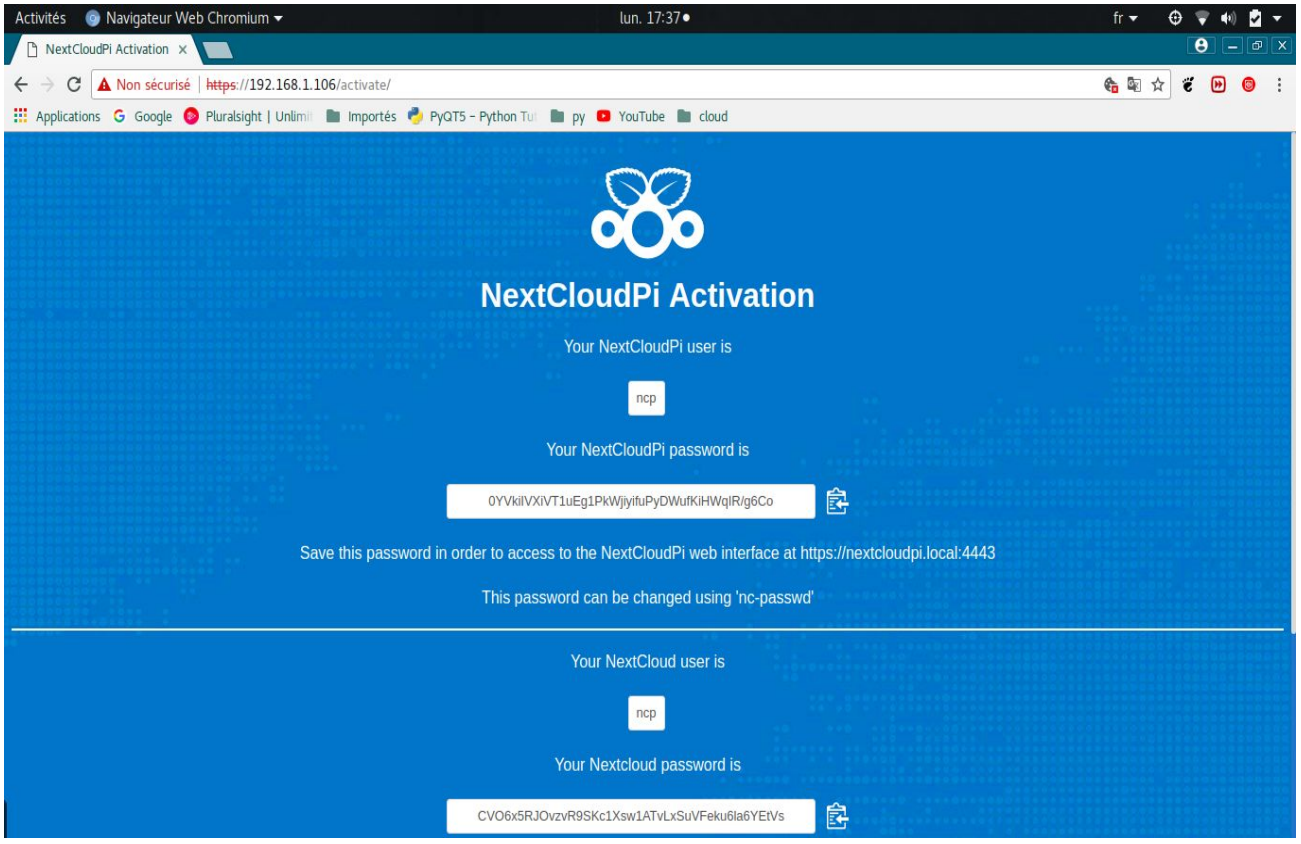


Figure (V.8): Plateforme nextcloudpi [11].

Comme vous pouvez le constater, notre domaine et sans protection https, pour cela on va se connecter au mode de configuration de nextcloudpi via le menu appelé “nextcloudpi -panel” grâce au nom d’utilisateur et le mot de passe donné via le port 4443 et exécuter l’activation comme mentionné dans la figure (IV.2).

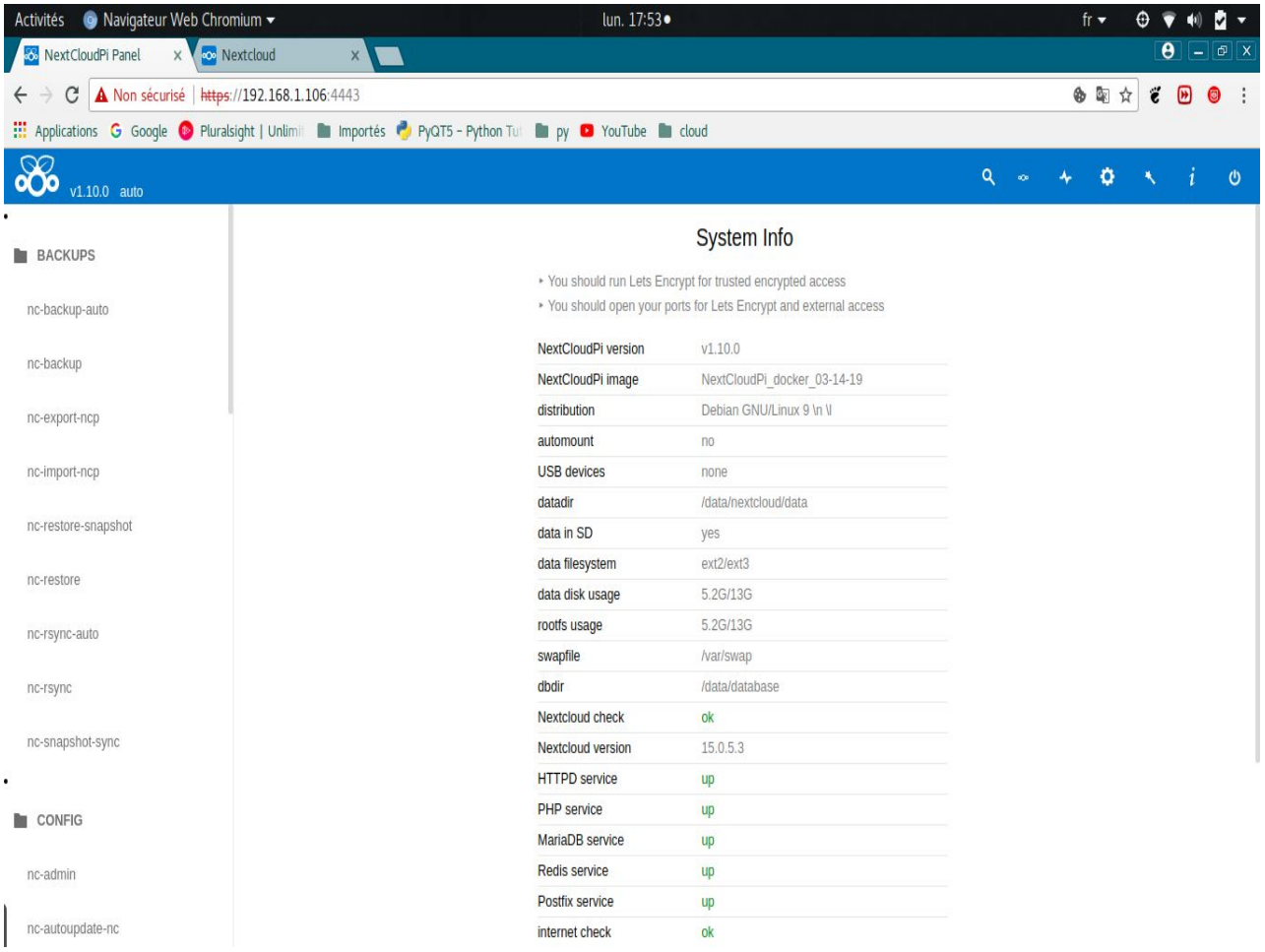


Figure (V.9): Panel nextcloudpi [12].

Après redirection vers la page principale, nextcloudpi nous indique que notre connecxion depuis la carte n'est pas reconnue comme domaine de confiance, pour remédier à cela, nous allons dans le menu panel et ajouter notre domaine comme étant autorisé :

nc-trusted-domain

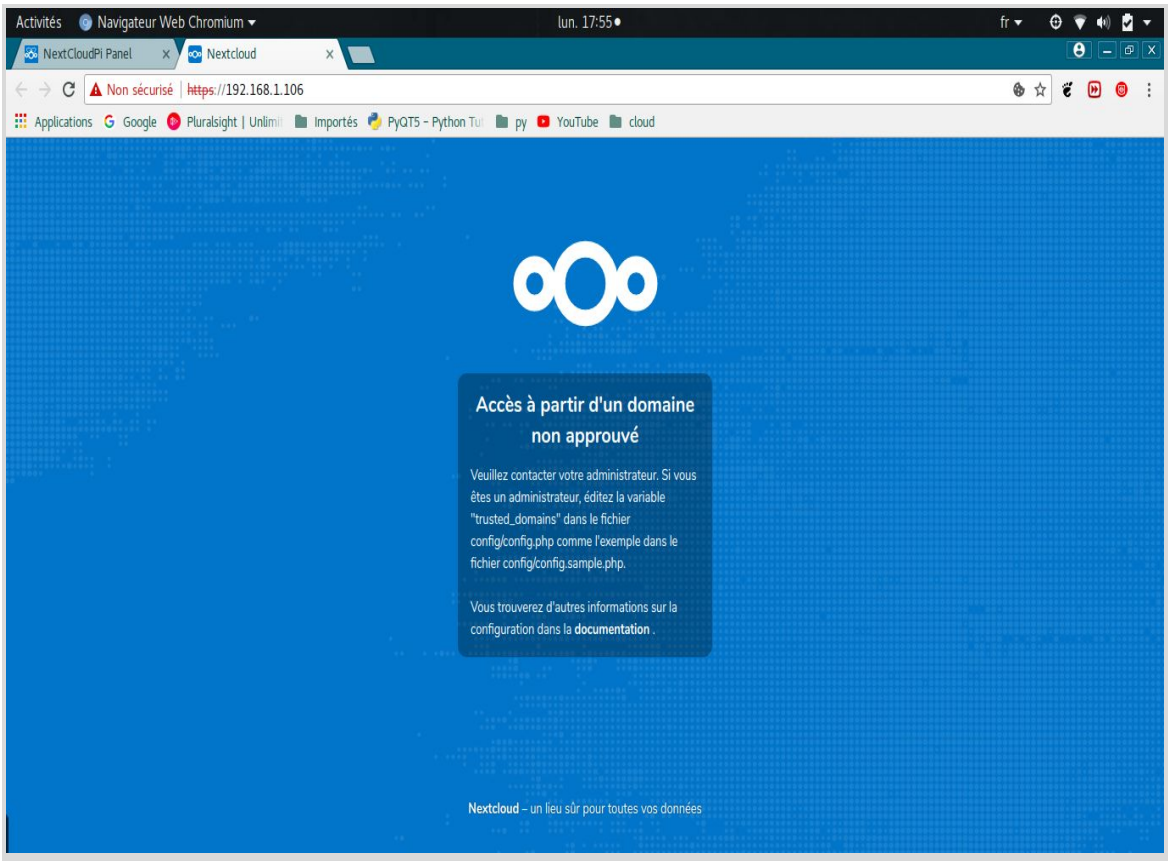


Figure (V.10): Connexion non approuvée de raspberry pi [13].

V.1.6.C. L'ajout des domaines de confiance :

Nextcloudpi nous donne la possibilité d'ajouter 3 différents domaines, comme pour notre cas, nous avions plusieurs connexions depuis de divers réseaux.

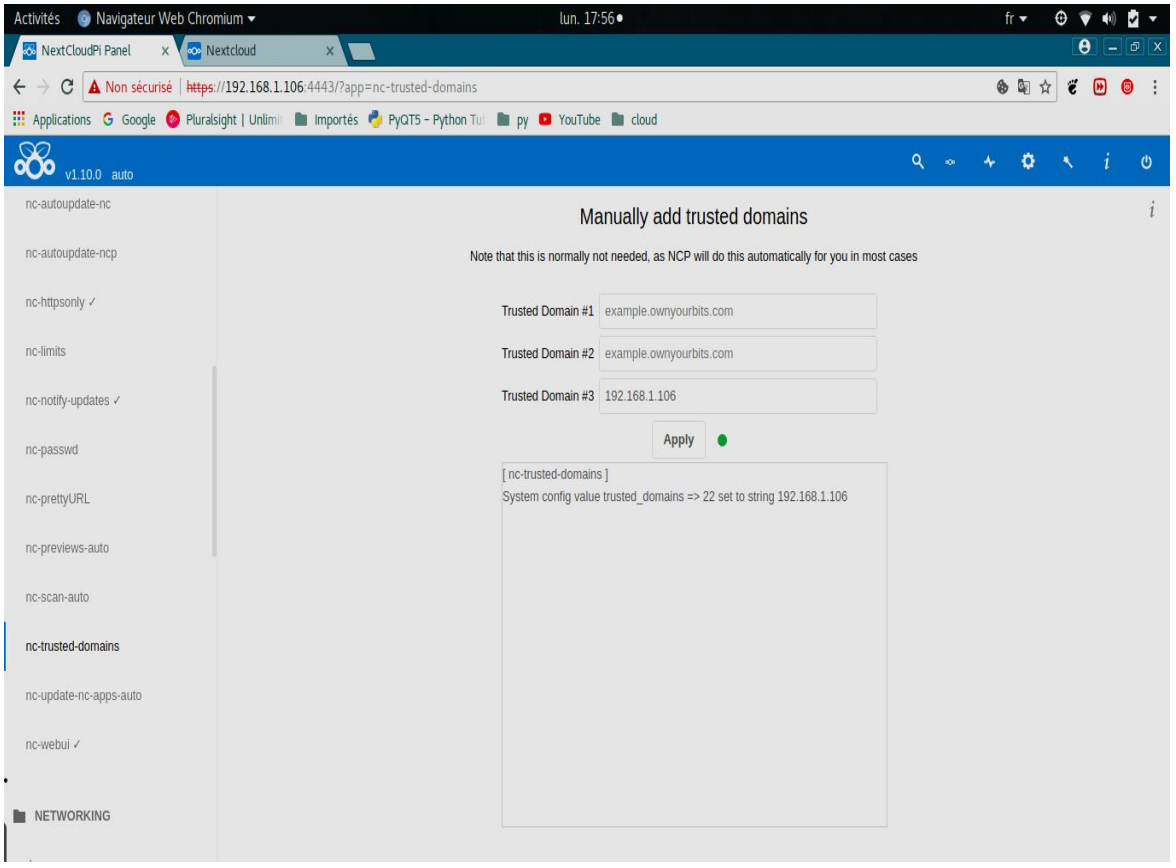


Figure (V.11): L'ajout des domaines de confiance [14].

Après l'ajout du domaine qui n'est rien d'autre que l'adresse ip de notre carte raspberry pi, nous allons à nouveau se connecter pour vérifier que la procédure à été bien mise en place.

Ensuite, il nous reste qu'à s'identifier grâce au nom d'administrateur et le mot de passe donné auparavant (figure (IV.2)).

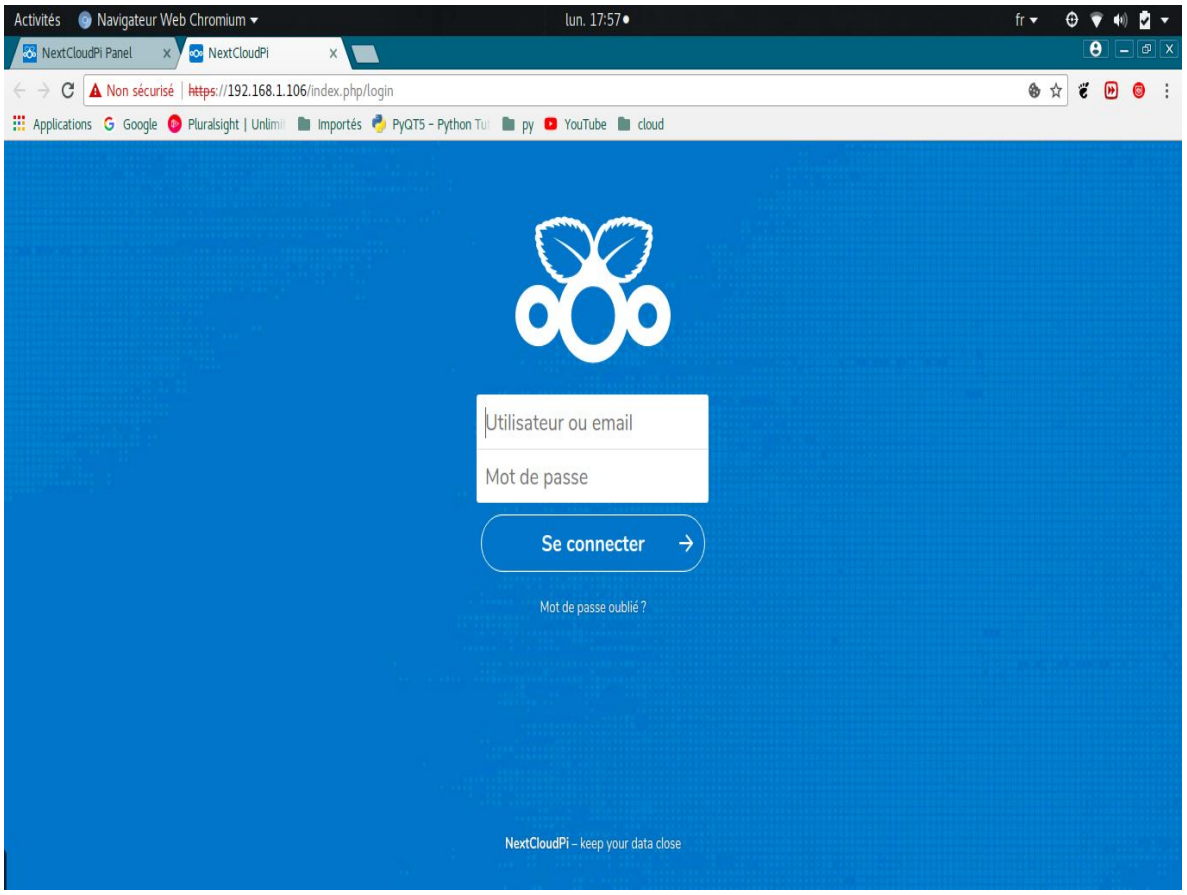


Figure (V.12): Plateforme de connexion nextcloudpi [15].

Puisque la sécurité est primordiale pour notre serveur, nous allons faire un changement de mot de passe depuis la commande du panel ci-dessous:

```
nc-password
```

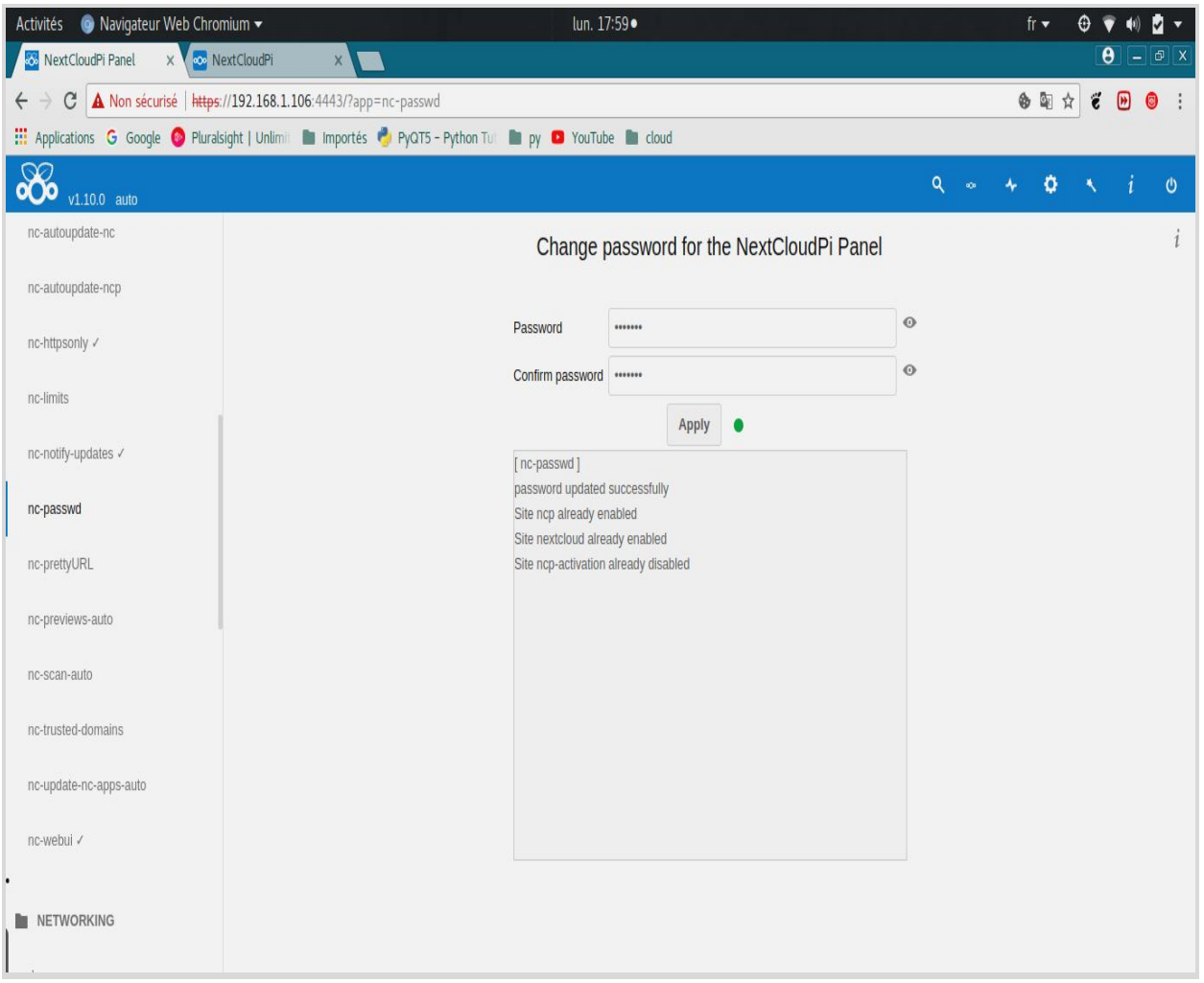


Figure (V.13): Changement de mot passe [16].

V.1.7. Configuration de base du serveur :

Notre objectif, consiste à fournir une image de menu docker stable qui tire parti du panneau Web NextCloudPi et du package de services associés, tels que Let's Encrypt, DDNS, les mises à niveau sans surveillance et les sauvegardes. Nextcloud a besoin de nombreux procédures, de la configuration et de la gestion de système, et notre objectif est de les simplifier.

À ce stade, la couche supplémentaire NextCloudPi contient un sous-ensemble des options disponibles dans l'image SD. Certaines options, telles que la gestion du wifi, n'ont aucun sens dans un conteneur, et d'autres nécessitent encore du travail pour être adaptées. Comme d'habitude, l'aide, les rapports de problèmes et les suggestions sont les bienvenus.

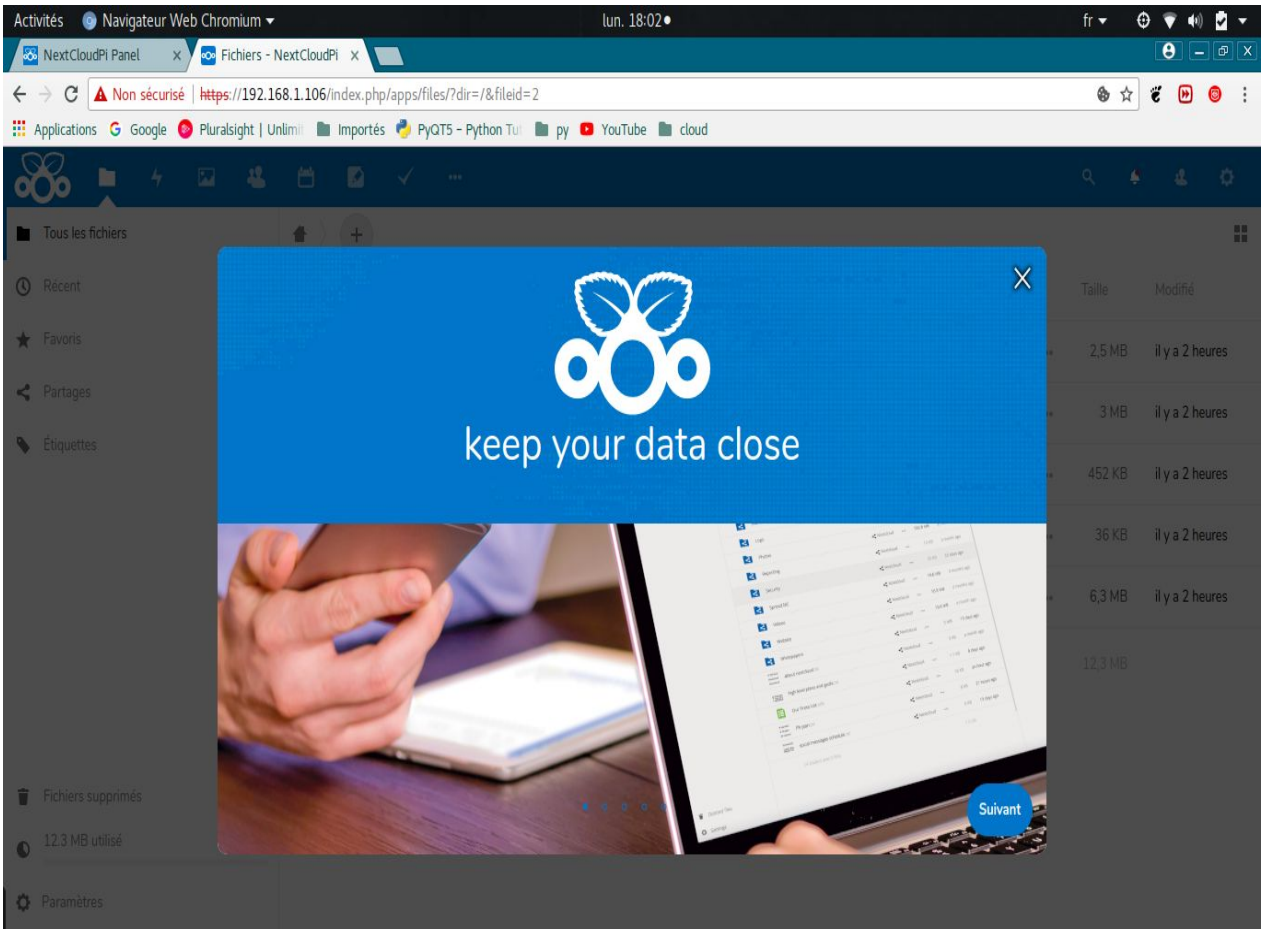


Figure (V.14): Plateforme nextcloudpi [17].

V.1.8. Configuration DNS:

V.1.8.1. C'est quoi un DNS:

Le serveur DNS (Domain Name System, ou Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau. [18].

V.1.7.3. Schéma du serveur DNS:

La figure (IV.19) nous présente le schéma typique du serveur DNS.

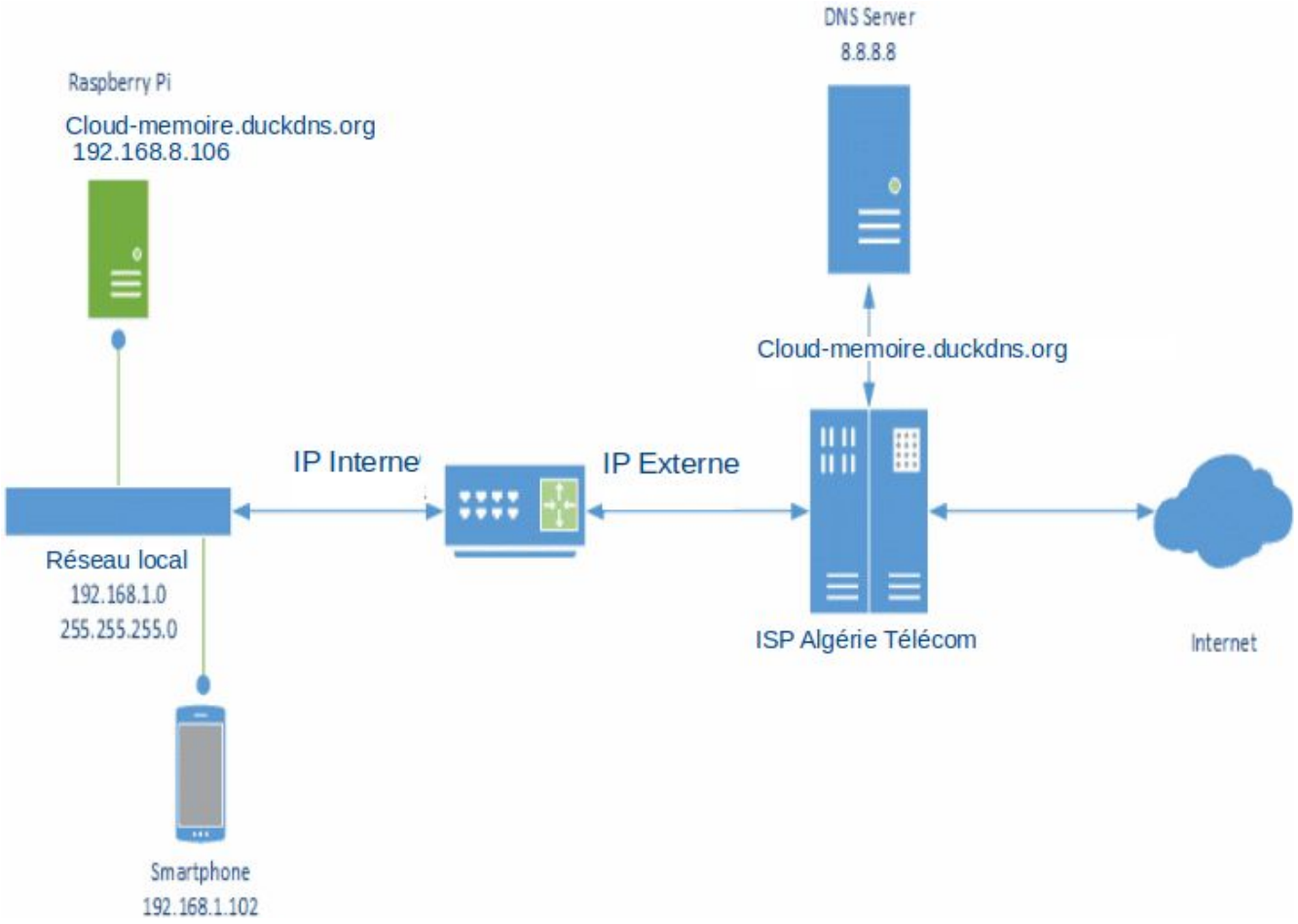


Figure (V.15): Schéma du serveur DNS [19].

V.1.4.3. Activation du DNS:

Comme citer auparavant, il faut donner une adresse ip fixe pour la carte grâce au dhcp pour que le serveur DNS puisse marcher avec chaque démarrage du serveur cloud.

Après cela, on active le serveur dns dans le panel du nextcloudpi avec l'ip du raspberry pi locale, pour que le trafic externe du serveur se redirige vers elle, et non pas vers d'autres hôtes connectés dans le réseau (pc, tablette,ext..).

Objectif désiré :

Notre but au début c'était de faire fonctionner le serveur cloud juste dans le réseau local, pourvu la mobilité de la carte qui n'est pas un atout pour son utilisateur.

Mais avec tout ça, nous voulons rendre la tâche encore plus facile sans aucun transport de matériels, et consulter ses données justes avec son smartphone ou tablette ou même pc portable alors que le serveur cloud tourne dans la carte raspberry pi depuis sa maison.

Ce qui nous a conduits à créer un réseau externe à travers un nom de domaine accessible depuis vers n'importe quel réseau dans le monde.

Pour cela, nous allons nous rendre vers le site de duckdns[3] et créer notre nom de domaine "cloud-memoire.duckdns.org"

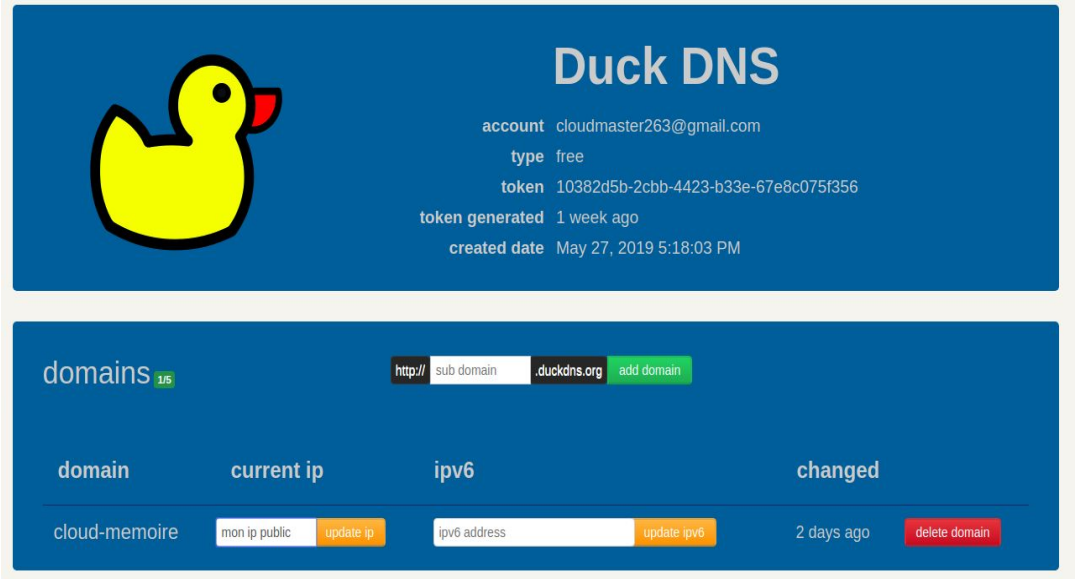


Figure (IV.16): Domaine duckdns [20].

Nous allons introduire la clé token et le nom de domaine dans nextcloudpi et l'activer depuis le panel :

Duckdns

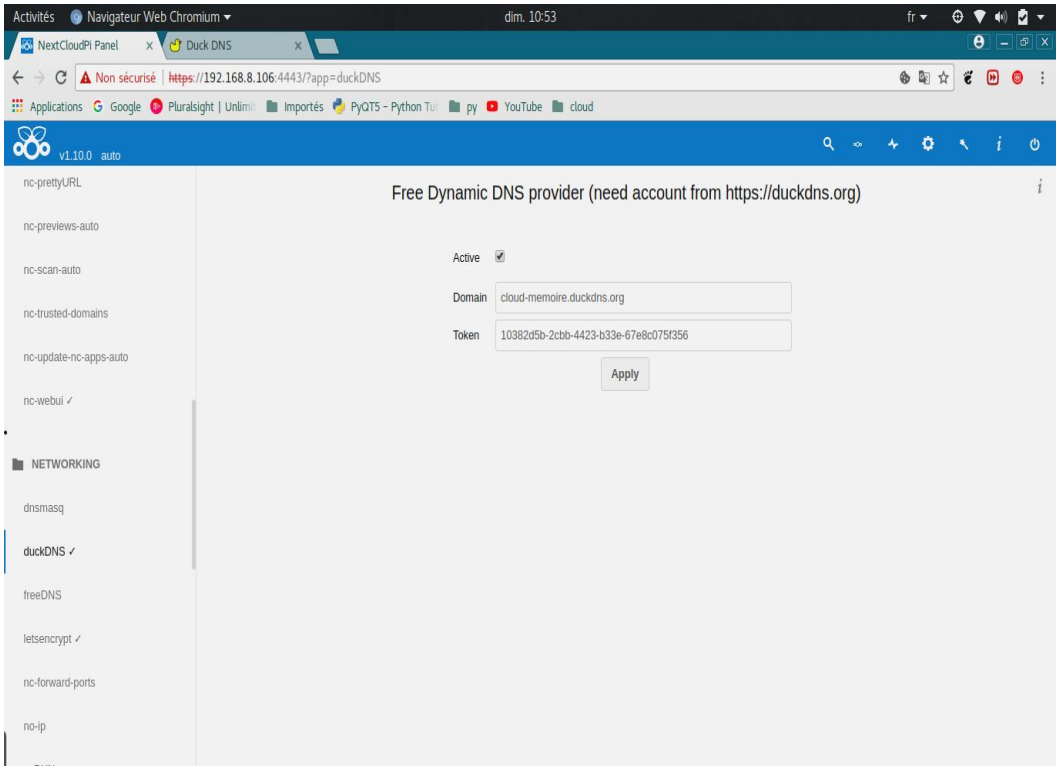


Figure (V.17): Activation du domaine [21].

V.1.5. Ip Forwarding :

IP Forwarding est le procédé qui fait le routage internet, il permet de déterminer la direction du réseau où les paquets IP, les datagrammes peut être envoyé (routage IP) [22].

En règle générale, les routeurs séparent les réseaux les uns des autres. Pour que les paquets puissent circuler entre les réseaux, ils doivent être «routés» d'un réseau à un autre. Ces routeurs contiennent une table de routage pouvant contenir des instructions spécifiques sur la manière d'envoyer des paquets à un réseau de destination (appelé route), ou un ensemble d'instructions génériques sur l'endroit où envoyer des paquets ne correspondant à aucune des autres routes spécifiées (appelées une route par défaut), ou les deux. Ces itinéraires peuvent être codés en dur dans le routeur par l'administrateur du réseau (appelé itinéraire statique) ou appris de manière dynamique via un protocole de routage.. Ces

itinéraires donnent aux routeurs des instructions sur la manière d'utiliser l'infrastructure de réseau physique en place pour acheminer les paquets jusqu'à leur destination, quel que soit le nombre de sauts qu'ils doivent effectuer pour y parvenir [23].

V.1.6. Configuration du routeur :

Nous allons vers la page web du routeur via l'adresse IP 192.168.1.1, vers l'onglet virtual server, et ajouter l'adresse ip local de raspberry pi avec le port 80 pour le protocole http et le port 443 pour le protocole https:

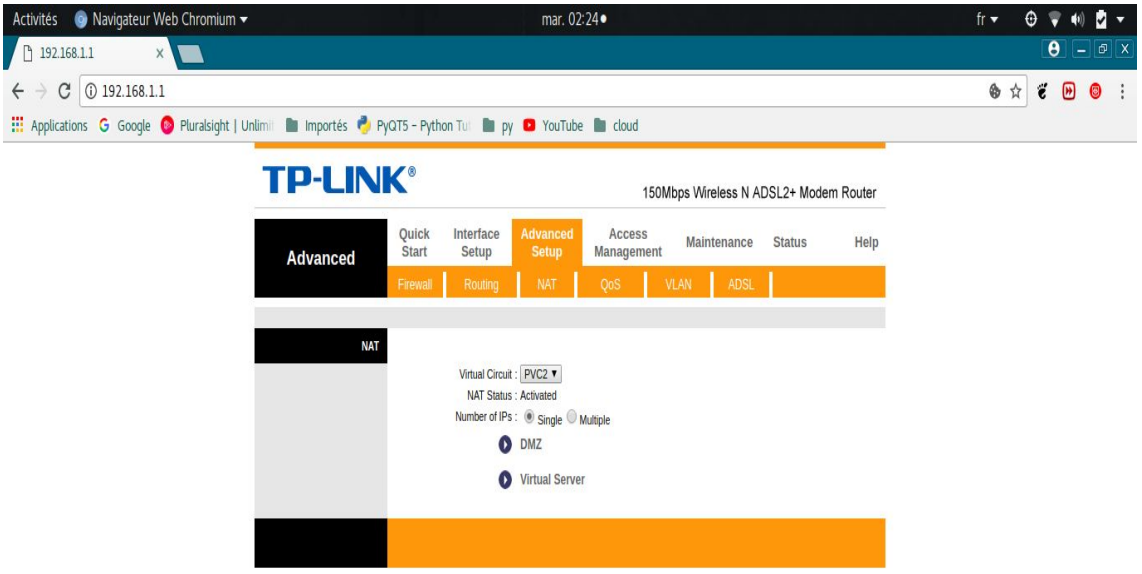


Figure (V.18): Configuration du serveur virtuel [24].

V.1.7. Protocole https:

HTTPS (Hypertext Transfer Protocol Secure ou protocole de transfert hypertexte sécurisé) est un protocole de communication Internet qui protège l'intégrité ainsi que la confidentialité des données lors du transfert d'informations entre l'ordinateur de l'internaute et

le site. Les internautes s'attendent à bénéficier d'une expérience en ligne sécurisée et confidentielle lorsqu'ils consultent un site Web.

Nous vous encourageons à adopter le protocole HTTPS afin de permettre aux internautes de consulter votre site Web en toute sécurité, quel que soit son contenu.

Les données envoyées à l'aide du protocole HTTPS sont sécurisées via le protocole Transport Layer Security(TLS), qui offre trois niveaux clés de protection :

- Le chiffrement : consiste à coder les données échangées pour les protéger des interceptions illicites. Cela signifie que lorsqu'un internaute navigue sur un site Web, personne ne peut "écouter" ses conversations, suivre ses activités sur diverses pages ni voler ses informations.
- L'intégrité des données : les informations ne peuvent être ni modifiées, ni corrompues durant leur transfert, que ce soit délibérément ou autrement, sans être détectées.
- L'authentification : prouve que les internautes communiquent avec le bon site Web.

Cette méthode protège contre les attaques des intercepteurs et instaure un climat de confiance pour l'internaute qui se traduit par d'autres retombées pour votre activité [25].

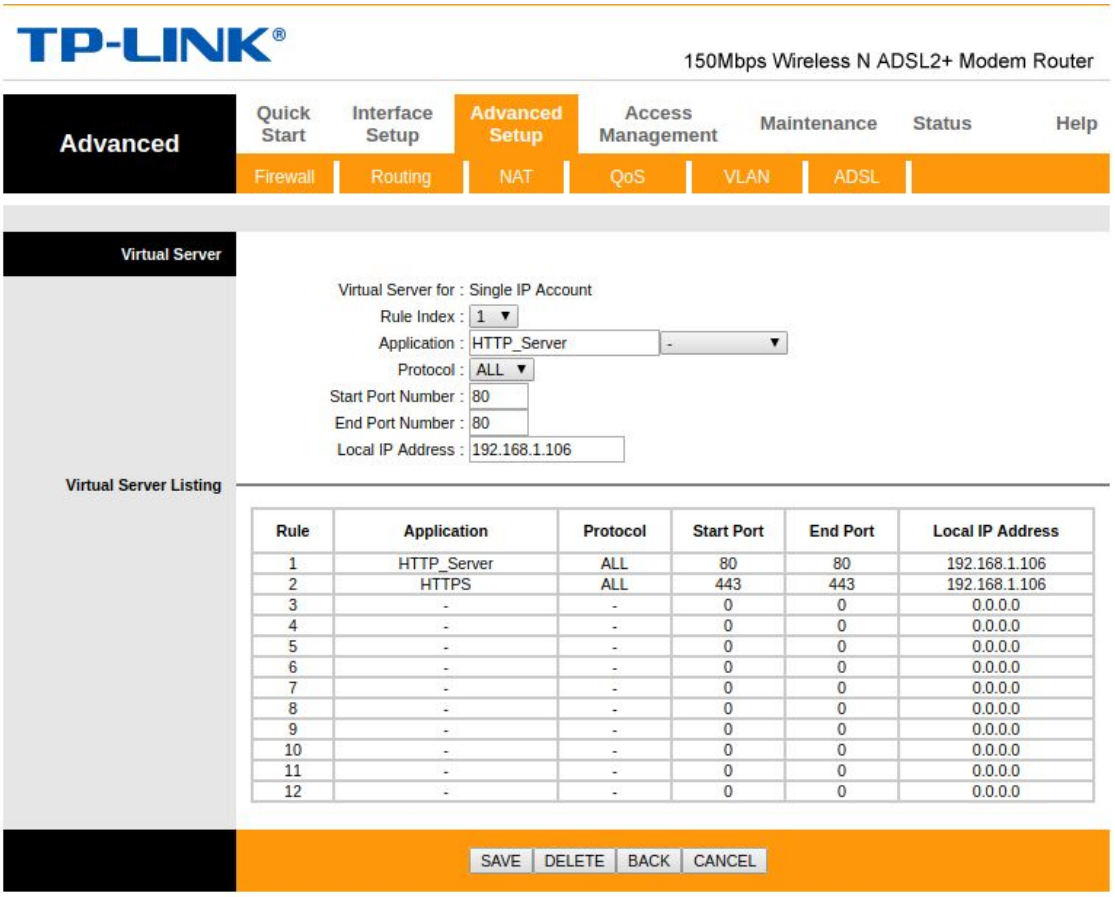


Figure (V.19): Configuration des ports 80 et 443 [26].

Aussi il faut faire les mêmes étapes au niveau du nextcloudpi en activant les ports via le panel :

nc-port-forward

V.1.8. Stockage externe:

Étant donné que le stockage est l'élément essentiel qui constitue le cloud, et pour des raisons de sécurité, nous allons créer notre propre espace de stockage avec un contrôle total de son environnement.

Pour cela, nous allons ajouter des disques durs externes (notre cas des clés usb de 16 G)

À la carte raspberry pi pour immigrer le serveur nextcloudpi vers le disque dur externe, pour réaliser cette procédure, nous allons créer un serveur NAS mais avec un aspect différent.

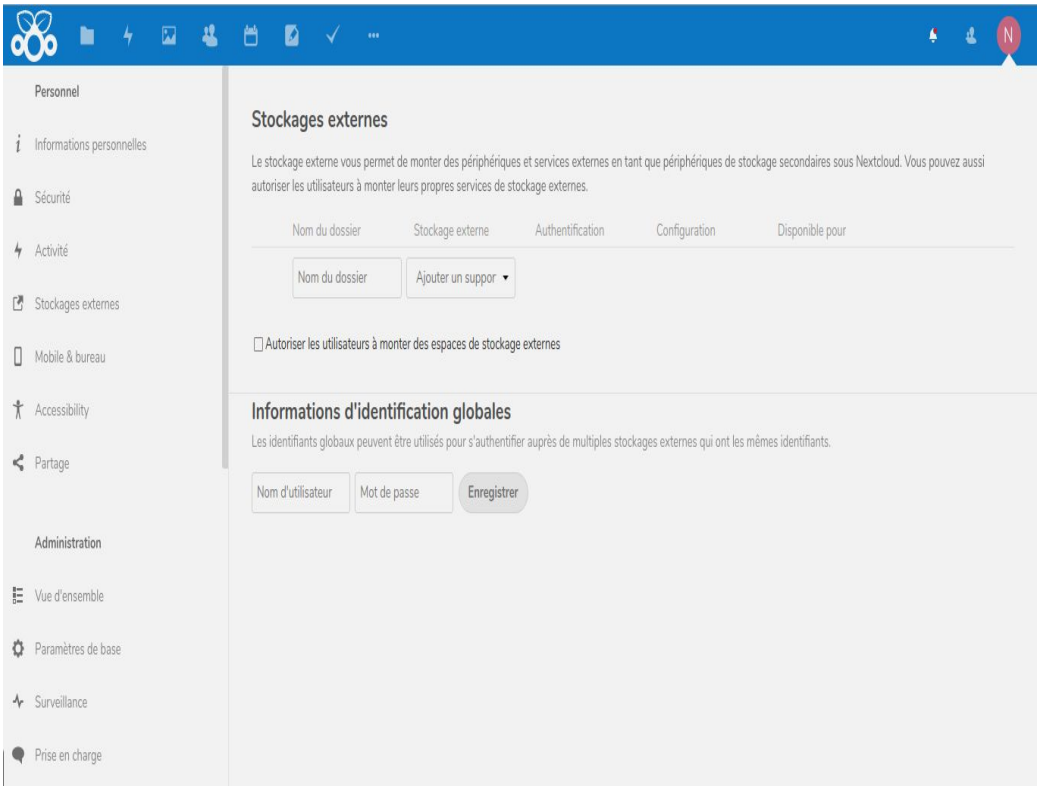


Figure (V.20): Menu stockage externe [28].

V.1.9. Serveur NAS :

Un serveur de stockage en réseau, également appelé stockage en réseau NAS (Network Attached Storage), ou plus simplement NAS, ou encore boîtier de stockage en

réseau, est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes. Le composant informatique principal de ce type de serveur est le disque dur [29].

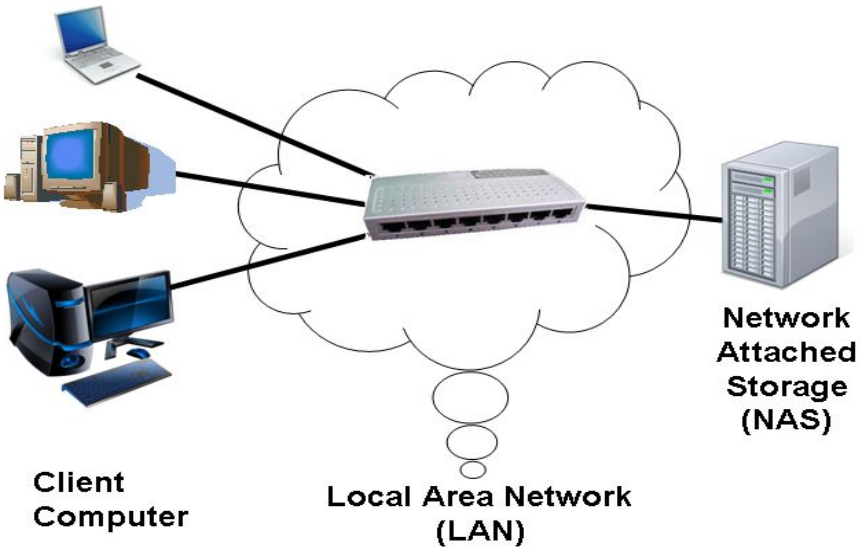


Figure (V.21): Serveur NAS [30].

Dans le but de faire un partage hors réseau local, et rendre le NAS accessible en externe, nous allons faire une deuxième migration vers le nouveau serveur samba.

V.1.10. Serveur Samba:

Samba est un ensemble d'applications Unix qui utilisent le protocole SMB (Serveur Message Block). Les systèmes d'exploitation Windows de Microsoft et OS/2 utilisent SMB dans les opérations client- serveur pour le partage de fichiers et d'imprimantes ainsi que pour les opérations associées.

En mettant en œuvre ce protocole Samba permet à des systèmes Unix de communiquer à l'aide du même protocole que Windows et du point de vu des clients windows de se présenter sur le réseau comme tout système Windows.

Un serveur Samba offre les services suivants :

- Partage d'une ou plusieurs arborescences de répertoires.

- Partage d'une ou plusieurs arbroscences Dfs (Distributed filesystem).
- Partage d'imprimante installée sur le serveur au profit des clients Windows du réseau.
- Participation à l'exploration des clients se connectant à un domaine Windows.
- Fourniture ou participation à la résolution de noms WINS (Windows Internet Name Service).

V.1.10.1. Montage du disque:

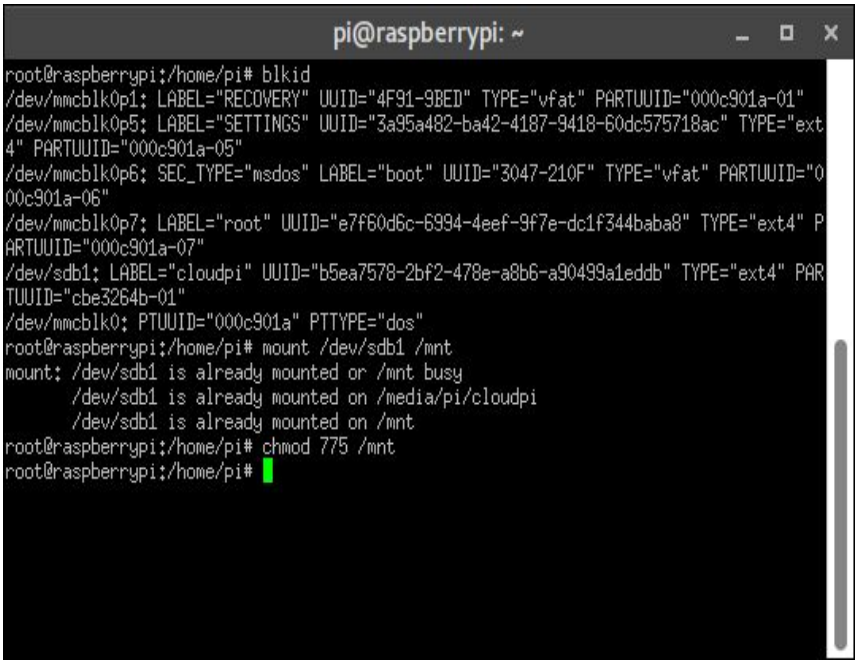


Figure (V.22): Montage du disque [31].

Les commandes :

Voici les commandes permettant le montage du disque externe :

`# blkid` pour lister les différents périphérique branchés dans les ports usb

`# mount /dev/sdb1 /mnt` pour monter le répertoire vers la clé usb

`# chmod 775` /mnt pour donner les droits de lecture

Pour des raisons de sécurité, nous avons créé un nouveau utilisateur “nadir” dans la carte dédié spécialement pour la clé usb :

```
#  adduser nadir
```
ajouter un nouveau utilisateur nadir

```
#  useradd -m -d /externe nadir
```
diriger le répertoire du montage vers l’utilisateur nadir

V.1.10.2. Installation de Samba :

On exécute l’installation de Samba grâce à la commande suivante :

```
# sudo apt-get install samba samba-common-bin
```

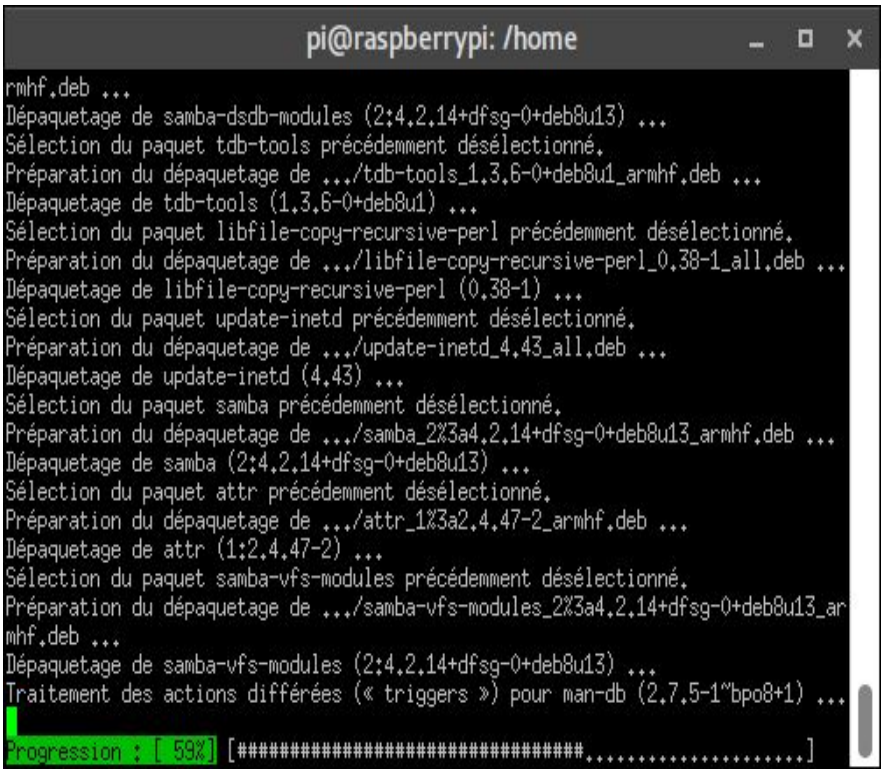


Figure (V.23): Installation de Samba [32].

V.1.10.3. Configuration de Samba :

```
#sudo leafpad /etc/samba/smb.conf
```
Fichier de configuration Samba

Ajouter le répertoire “/externe” pour le partage en externe

[EXTERNE]
Comment = Pi shared folder
Path = /externe
Browseable = yes
Writeable = Yes
only guest = no
create mask = 0777
directory mask = 0777
Public = yes
Guest ok = yes

sudo smbpassword -a nadir pour ajouter l’utilisateur “nadir” au serveur samba.

V.1.10.4. Configuration de samba sur nextcloudpi :

Afin d’accomplir la configuration, il faut se diriger vers le panel “external storage” de nextcloudpi en tant qu'administrateur et ajouter le disque monté (usb) avec l’identifiant de samba
(notre utilisateur créer c’est “nadir”) .

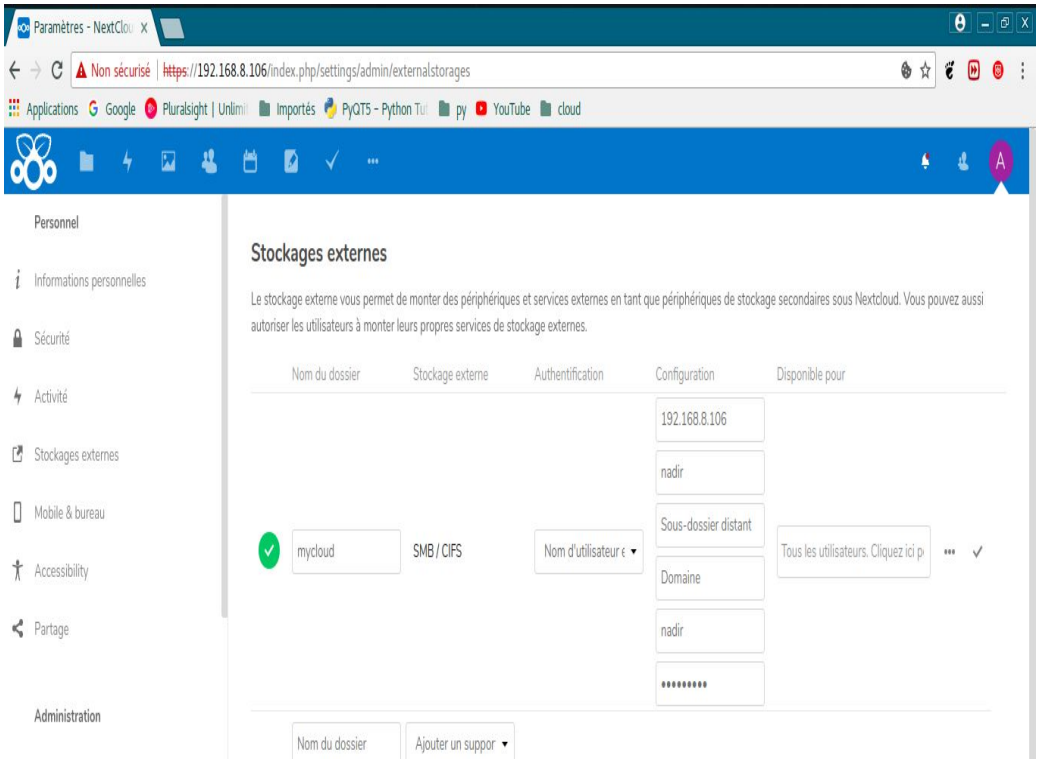


Figure (V.24): Configuration de Samba [34].

mycloud : le nom du dossier créé pour le partage.

SMB / CFS : serveur Samba avec identifiant “nadir” .

Localhost: 192.168.8.106 l’adresse ip de la carte raspberry pi .

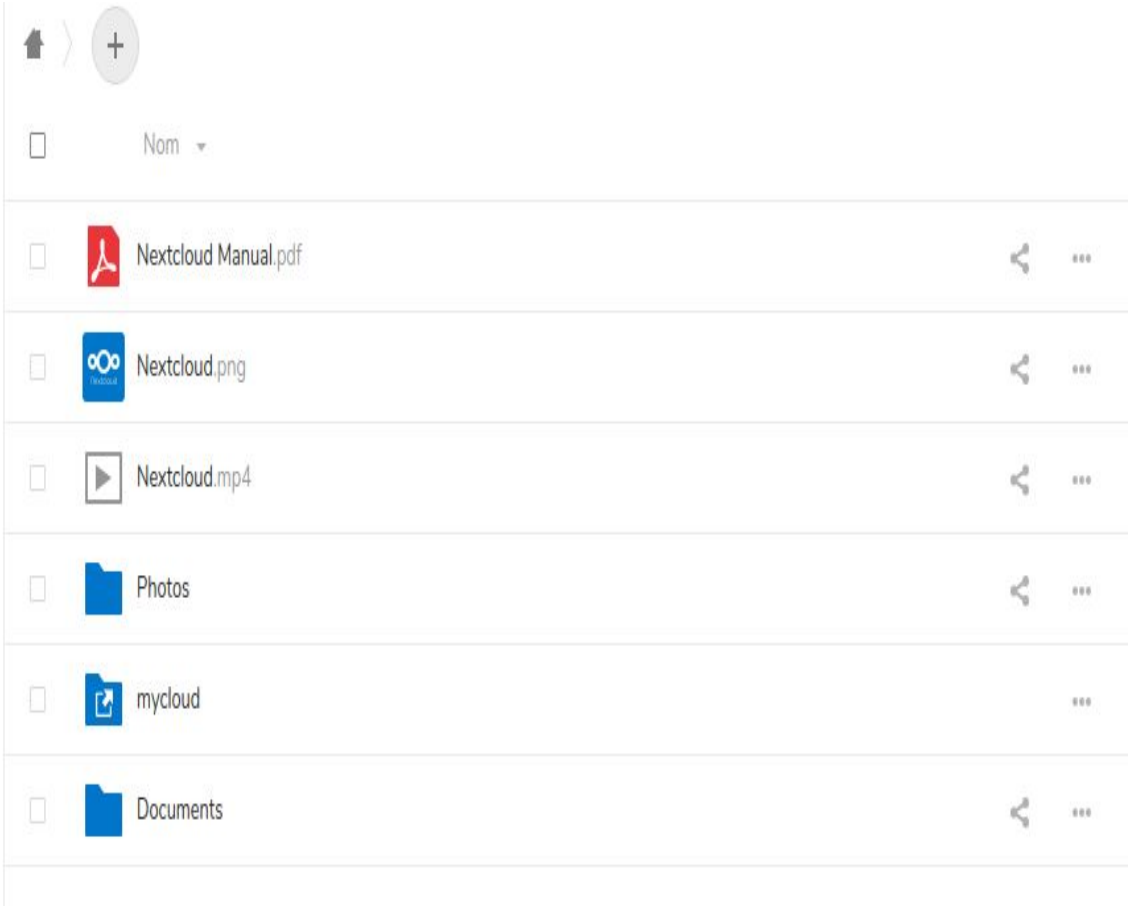
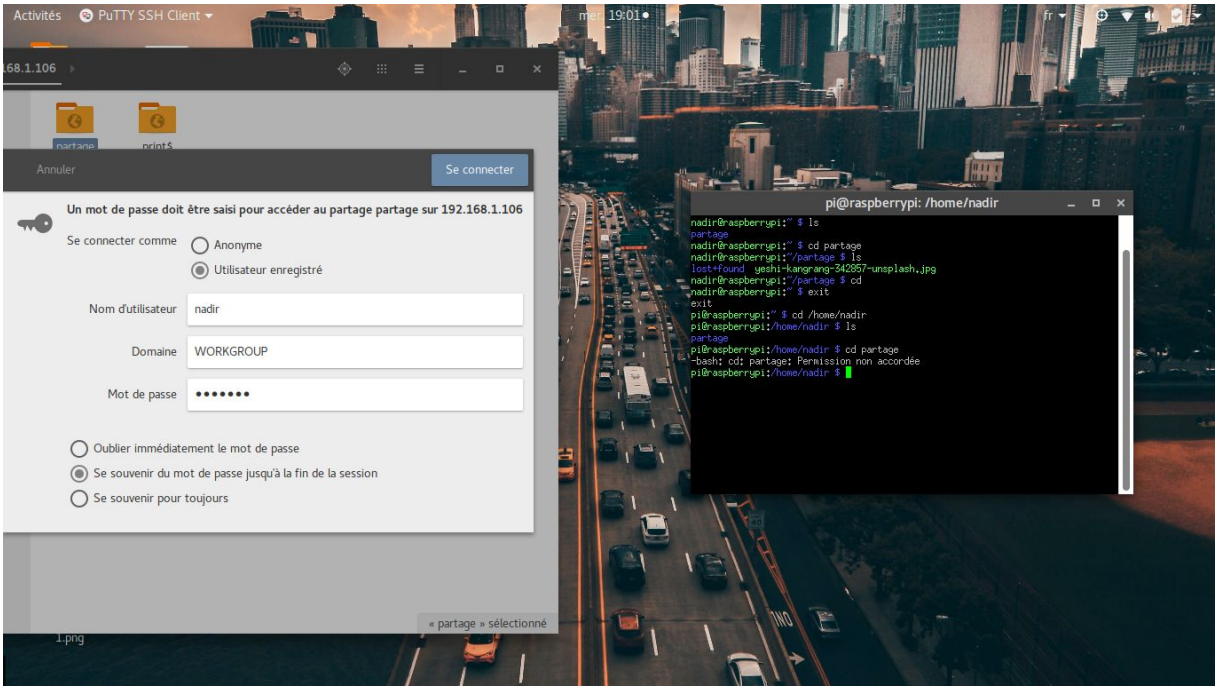


Figure (V.25) : Espace de stockage de nextcloudpi [35].

Maintenant, notre serveur est prêt à être déployé en interne via le réseau local de l'adresse ip de la carte 192.168.8.106 et en externe via le serveur DNS et le nom de domaine : cloud-memoire.duckdns.org.

V.2. Sécurité du serveur cloud :

Afin de mieux protéger notre serveur de stockage NAS, nous avons enlever ses permissions de partage en local, dans le but qu'il soit exécuté seulement via le serveur nextcloud, la figure ci-dessous nous montre le refus de connexion au serveur NAS via un autre hôte en local, nous avons fais le test avec une machine ubuntu :



Figure(V.26) : Le refus de la connexion NAS externe.[36]

Avec toute cette procédure, le serveur reste vulnérable aux attaques, c'est pourquoi nous allons renforcer notre sécurité avec deux méthodes différentes :

- Installer un certificat de chiffrement ssl pour sécuriser l'interface web du serveur cloud et protéger le trafic réseau.
- Installer un honeypot (pot de miel) pour piéger toutes tentatives d'attaques et les diriger vers un faux serveur cloud.

V.2.1. Qu'est-ce que le SSL ?

Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) est le protocole de sécurité le plus répandu qui créé un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne. Dans notre société centrée sur un Internet vulnérable, le SSL

est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web.

Techniquement parlant, le SSL est un protocole transparent qui nécessite peu d'interaction de la part de l'utilisateur final. Dans le cas des navigateurs, par exemple, les utilisateurs sont avertis de la présence de la sécurité SSL grâce à l'affichage d'un cadenas et du protocole « https » dans l'url, et, dans le cas du SSL à validation étendue, par la barre d'adresse verte. La clé du succès du SSL est donc son incroyable simplicité pour l'utilisateur final. (Voir la figure (IV.34)).

En pratique, le SSL devrait être utilisé dans les cas suivants :

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle.
- Pour sécuriser les applications et les messageries web, telles qu'Outlook Web Access, Exchange et Office Communications Server.
- Pour sécuriser les flux de production et les applications de virtualisation tels que Citrix Delivery Platforms et les plates-formes sur le Cloud.
- Pour sécuriser les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Pour sécuriser le transfert de fichiers au travers de services « https » et FTP, dans les cas de mise à jour de sites Internet par exemple [49].

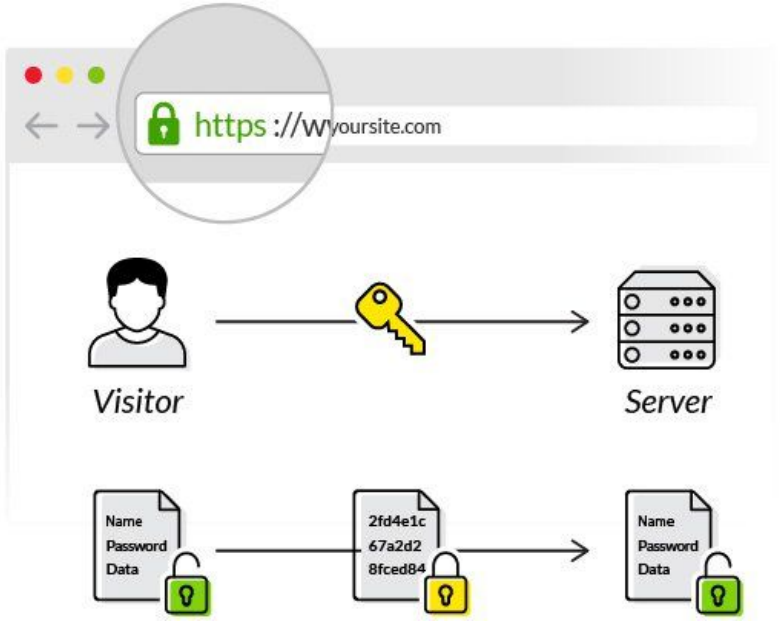


Figure (V.27): Certificat ssl [37].

V.2.2. SSL pour nextcloudpi :

Let's Encrypt (abrégé *LE*) est une autorité de certification lancée le 3 décembre 2015 (Bêta Version Publique). Cette autorité fournit des certificats gratuits pour le protocole cryptographique TLS (***Transport Layer Security*** ou Sécurité de la couche de transport) au moyen d'un processus automatisé destiné à se passer du processus complexe actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation des sites internet. En septembre 2016, plus de 10 millions de certificats ont été délivrés .En février 2017, Let's encrypt était utilisé par 13,70% du total des domaines français enregistrés. En avril 2018, Let's encrypt fournit 51,21 % des certificats [38].

Figure (V.28) : Logo let's Encrypt [39].

Activation de let's encrypt pour notre serveur nextcloudpi via le panel de configuration:

let's encrypt Nous allons maintenant se connecter depuis un réseau 3g (réseau externe) depuis le domaine créé, et vérifier le certificat ssl (https) quel a été bien installé.

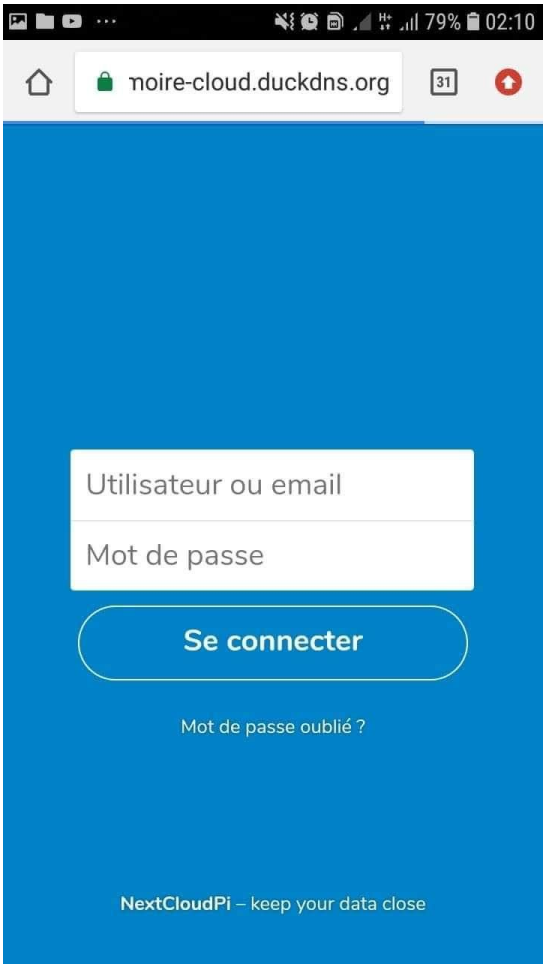


Figure (V.29): Connexion dns avec ssl [40].

V.2.3. Installation du honeypot:

V.2.3.A. Qu'est-ce qu'un honeypot :

On n'en entend pas souvent parler, mais les honeypots (pots de miel en français) sont des pièges à pirates qui remontent à une dizaine d'années.

Un honeypot est un concept mis au point par des experts en sécurité informatique dont le but n'est pas d'empêcher les pirates d'entrer sur leurs systèmes, mais au contraire de les piéger lorsqu'ils viennent.et donc d'étudier leur comportement pour mieux s'en protéger, en plus de leur restreindre l'accès à tout le système en production [41].

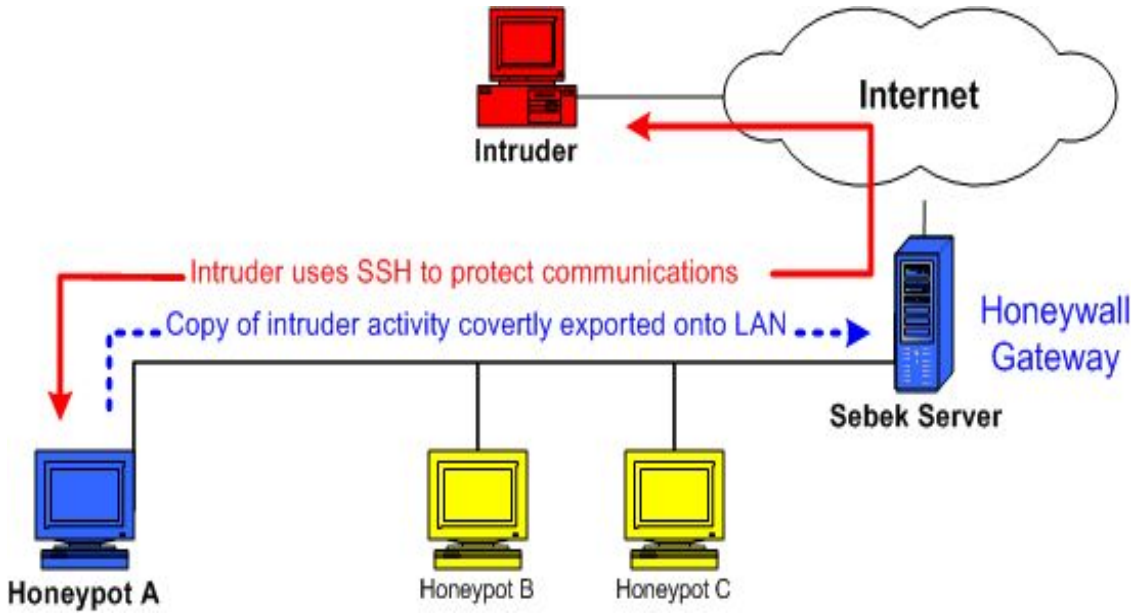


Figure (V.30): Attaque Honeypot [42].

V.2.3.B. Principes de fonctionnement:

Le but de ce leurre est de faire croire à l'intrus qu'il peut prendre le contrôle d'une véritable machine de production, ce qui va permettre à l'administrateur d'observer les moyens de compromission des attaquants, de se prémunir contre de nouvelles attaques et lui laisser ainsi plus de temps pour réagir.

Une utilisation correcte d'un pot de miel repose essentiellement sur la résolution et la mise en parallèle de trois problématiques [Ref] :

- La surveillance.
- La collecte d'information.
- L'analyse d'information [56].

Pour installer le honeypot dans notre serveur cloud, nous allons d'abord changer le port ssh pour sécuriser la session, on change le port ssh par défaut "22" en "5463"

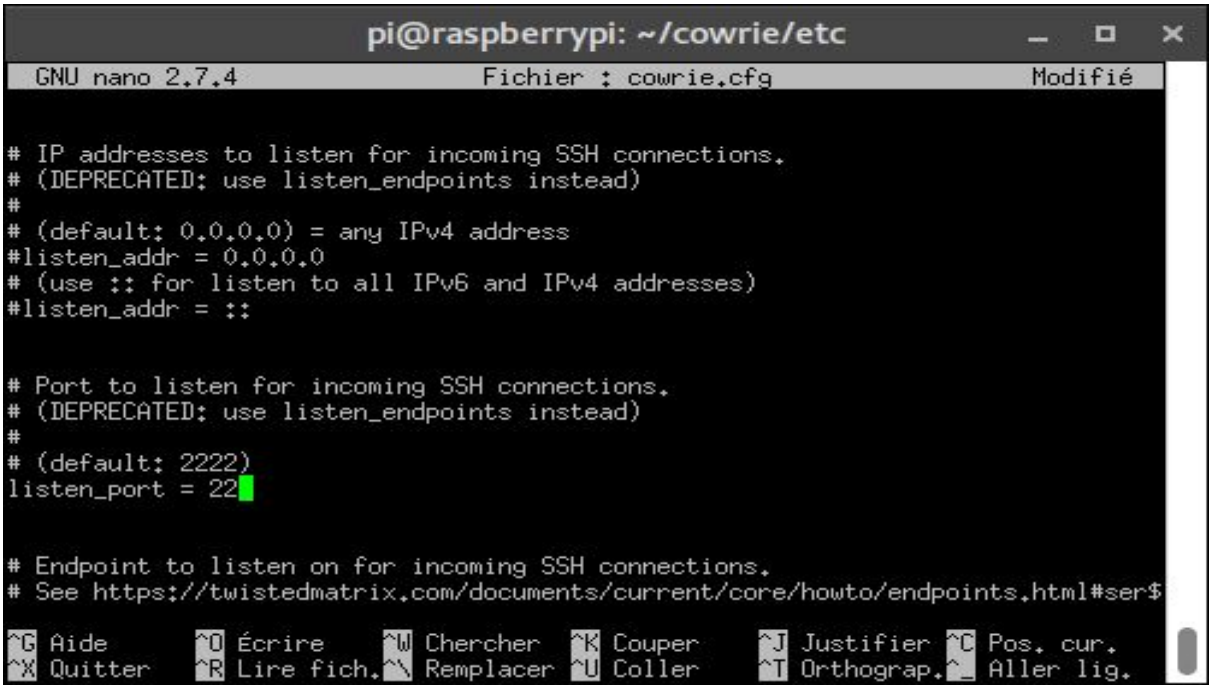


Figure (V.31) : Fichier de configuration ssh [43].

Après nous faisons un redémarrage du serveur ssh grâce à la commande :

```
sudo /etc/init.d/ssh restart
```

Après ça, nous allons nous déconnecter du serveur, puis reconnecter avec le nouveau port configuré “5463”.

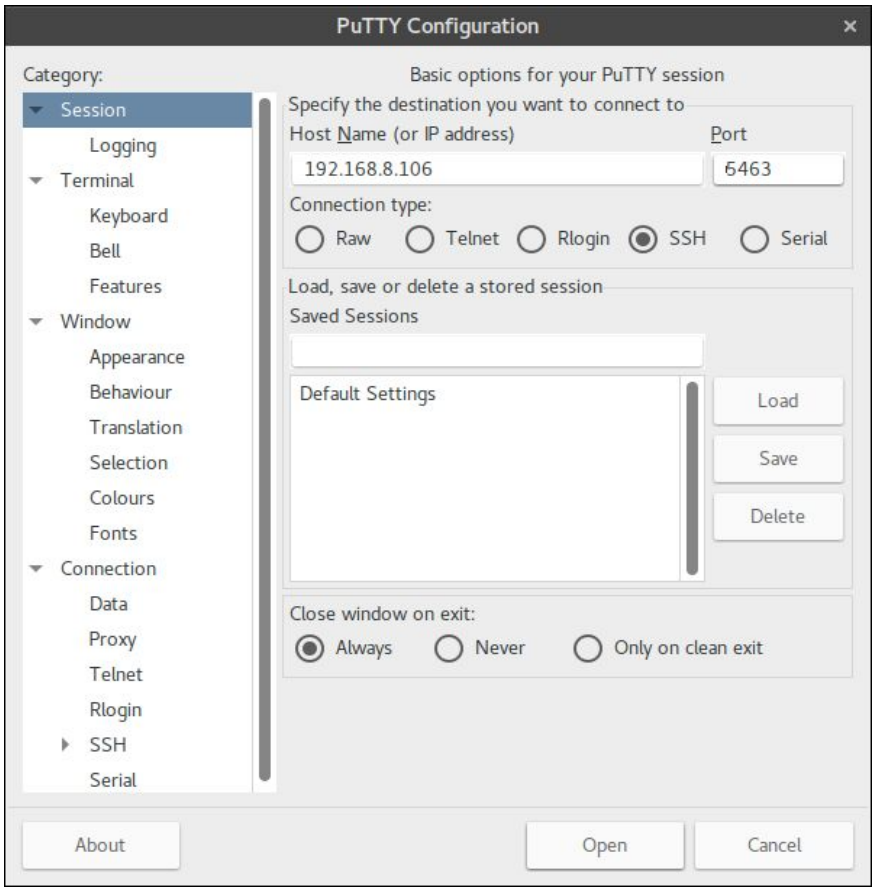


Figure (V.32): Connexion ssh depuis le nouveau port [44].

V.2.4. Kippo :

Kippo est un pot de miel SSH à interaction moyenne écrit en Python . Kippo est utilisé pour enregistrer les attaques par force brute et l'intégralité de l'interaction du shell effectuée par un attaquant [59].

Les étapes suivantes consistent à installer les paquets essentiels pour le bon fonctionnement du honeypot Kippo via la commande ci-dessous :

```
root@raspberrypi:# sudo apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted
```

Cette commande consiste à installer les librairies python et le openssl pour générer les clés de cryptographies rsa-key.

Ajouter l'utilisateur Kippo pour se rendre dans le serveur honeypot créé.

```
root@raspberry pi:/# sudo adduser kippo
```

Afin que l'utilisateur kippo puisse avoir tous les droits de lecture et la permission du super utilisateur, il faut exécuter les commande suivantes:

```
root@raspberry pi: /# touch /etc/authbind/byport/22
```

```
root@raspberry pi: /# chown kippo:kippo /etc/authbind/byport/22
```

```
root@raspberry pi: /# chmod 777 /etc/authbind/byport/22
```

Le port 22 c'est pour le mettre en ouverture réseau et faire croire au pirate que c'est le vrai port utilisé.
Téléchargement de kippo depuis github:

```
root@raspberry pi:/# clone git https://github.com/lambis7/raspberrypi3-honeypot-ids
```

Au final, il nous reste qu'à lancer le serveur honeypot et le faire tourner sous notre réseau cloud qui n'est d'autre que le nom de domaine et l'adresse ip de raspberry pi avec la commande suivante:

```
kippo@raspberrypi ~ /kippo$ ./start.sh
```

De manière à surveiller le serveur cloud et vérifier les attaques, on se dirige vers le fichier log de kippo et on observe les login et les mots de passes introduits par les pirates :

```
kippo@raspberrypi ~ /kippo$ cd log
```

```
kippo@raspberrypi ~ /kippo$/log cat logs.log
```

V.3. Conclusion

A la fin de ce chapitre, nous avions le plaisir de mettre en place notre solution , qui est basée sur des nouvelles tendances dans le monde du cloud computing tel que docker, et nous avons pu réaliser notre serveur cloud avec une meilleure protection en utilisant un honeypot et un chiffrement ssl afin de le rendre moins vulnérable, offrant une meilleure sécurité de données tout en espérant le commercialiser à la demande de l'individu et des startup surtout pour notre pays, qui présente un champ vierge dans ce domaine.

Références chapitre v

[1] article “Harish Kumar What is Docker ?”

[2] capture installation de docker

[3] capture version docker

[4] Création du conteneur

[5] https://homputersecurity.com/2017/08/15/comment-creer-votre-propre-service-cloud-avec-nextcloud/

[6] https://upload.wikimedia.org/wikipedia/commons/thumb/6/60/Nextcloud_Logo.svg/800px-Nextcloud_Logo.svg.png

[7] https://ownyourbits.com/nextcloudpi/#content_start

[8] https://ownyourbits.com/nextcloudpi/#content_start ² ownyourbit.com , ³ duckdns.org

[9] capture d'Installation de nextcloudpi sous docker

[10] capture de vérification du statut de l’image docker

[11] capture plateforme nextcloudpi

[12] capture panel nextcloudpi

[13] capture connexion non approuvée de raspberry pi

[14] Plateforme de connexion nextcloudpi

[15] capture changement de mot passe

[16] capture plateforme nextcloudpi

[17] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203373-dns-serveur-dns-domain-name-system-definition-traduction/

[18] capture schéma du serveur DNS

[19] capture domaine duckdns

[20] capture activation du domaine

[21] http://www.octetmalin.net/linux/tutoriels/ip-forward.php

[22] https://www.quora.com/What-is-IP-forwarding

[23] https://support.google.com/webmasters/answer/6073543?hl=fr

[24] capture configuration des ports 80 et 443

[25] capture menu stockage externe

[26] Razafy, N. R., Randriamaroson, R. M., & Rakotomiraho, S. (2016). Sécurisation de données. Éditions universitaires européennes

[27] https://upload.wikimedia.org/wikipedia/commons/2/29/NAS.png

[28] capture montage du disque

[29] Installation de Samba

Références chapitre v

[30] capture configuration de samba

[31] capture espace de stockage de nextcloudpi

[32] https://www.globalsign.fr/fr/centre-information-ssl/definition-ssl/

[33] https://www.it-ps.net/wp-content/uploads/diagram1.jpg

[34] https://fr.wikipedia.org/wiki/Let's_Encrypt

[35] https://i2.wp.com/travellingtechguy.eu/wp-content/uploads/2018/09/Letsencrypt.jpg?fit=583%2C360&ssl=1

[36] Capture connexion dsn avec ssl

[37] https://www.leblogduhacker.fr/les-honeypots-des-pieges-a-pirates/

[38] http://www.frameip.com/wp-content/uploads/honeypots-honeynet-roo-honeywall-2.png

[39] https://fr.wikipedia.org/wiki/Honeypot

[40] https://assets.digitalocean.com/tutorial_images/vYAoz8R.png

[41] Capture connexion ssh depuis le nouveau port

[42] https://en.wikipedia.org/wiki/Kippo

2 https://ownyourbits.com/

3 https://ownyourbits.com/

Conclusion Générale

Conclusion générale

Dans ce mémoire nous avons abordé la notion du cloud computing comme infrastructure numérique dématérialisée fournissant des services et des applications configurables à la demande de leurs usages.

A travers cela, nous avons présenté en premier lieu, une étude bibliographique sur les différentes architectures et modèles de déploiements Iaas Paas Saas ainsi que leurs éléments constitutifs. Cette étude donne donc un aperçu relativement large sur les ressources du cloud computing en se basant sur leurs multiples solutions et plateformes VMware.

Tandis que la sécurité des données reste le maillon faible des fournisseurs de services cloud nous avons effectué une analyse sur ses variantes menaces et vulnérabilités ainsi que leurs solutions existantes.

Notre objectif dans ce mémoire aborde principalement le concept de sécurité du cloud computing est se diriger vers une nouvelle approche plus confiante qu'offre les hébergeurs cloud.

Afin de mettre en place notre solution, nous avons commencé par la réalisation d'un serveur cloud personnel et open sources, tout en se basant sur la technologie des conteneurs docker pour un meilleur déploiement.

La configuration de notre solution nous a conduit à créer deux autres nouveaux serveurs, l'un d'eux est un serveur NAS mais avec un partage externalisé ce qui va offrir un contrôle total de gestion de données pour son utilisateur.

Le deuxième serveur vise la sécurité de cet espace de stockage, ce qui nous a ramené à intégrer un système de protection de type honeypot et un chiffrement ssl afin de réduire ses vulnérabilités et renforcer son trafic.

Cette solution étant très ambitieuse, nous nous sommes vite heurtés à de considérables Problèmes, que ce soit dû au déploiement du serveur ou à son configuration de sécurité, tous ces défis nous ont fourni la face complexe cachée pour la proposition d'une telle solution, et leurs démêlement nous a souvent retardé mais nous a amené à explorer le monde de télécommunication, crucial pour tout ingénieur digne de ce nom, qui propose une solution à tout problème quelques soit sa difficulté.

Ce projet a été pour nous un avantage et une magnifique opportunité de découvrir un environnement informatique nouveau, complexe et riche, ce qui nous accréditer d'acquérir une bonne connaissance en administration systèmes et réseaux et d'approfondir nos expérience dans le domaine de la sécurité et du Cloud Computing et surtout d'acquérir les bons techniques que doit avoir tout administrateur réseau.

Perspectives:

Cependant la solution qui a été mis en place est un prototype de test et démonstration qui sera par la suite redéployé en un environnement de production commercialisable et envisageable suite à son amélioration.

Conclusion générale

منذ نشأتها في أوائل السبعينيات ، أصبحت الإنترنت الدعامة الأساسية للحياة المهنية الحديثة ، تطور مظهرها من شبكة بسيطة من حجم محدود إلى بنية تحتية لا تنضب مع أبعاد كبيرة. في حين تم تطويرها في الأصل لتأسيس اتصال بين أجهزة كمبيوتر مختلفة ، واليوم تسببت في لامركزية هذه الأنظمة ، مع تقديم خدمات معقدة لطلب المستخدمين والشركات على وجه الخصوص ، نحو ثورة جديدة الاتجاه و التي تتمثل في الحوسبة السحابية.

الحوسبة السحابية هي الحل الاقتصادي والتكنولوجي ،و التي عبرها تتم مشاركة الموارد, وقوة الحساب مبرمجة حسب الاحتياجات . مثل تخزين وإدارة التطبيقات التي يمكن أن تكون مشروطة و مقدمة مع الحد الأدنى من الجهد الإداري. ومع ذلك ، فإن حماية الخصوصية وأمن البيانات أمر بالغ الأهمية في استخدام التطبيقات والخدمات السحابية والمخاطر التي تصاحبها تصبح أكثر تعقيدا مع البنية التحتية لهذه التكنولوجيا.

في هذه المذكرة نحن مهتمون بدراسة الأمن وإدارة منصات الحوسبة السحابية ، التي تقدم أحدث حلول الافتراضية الموجودة في هذا المجال مثل تكنولوجية الدوكر.
هدفنا في هذا العمل هو اقتراح حل تطبيقي لسيرفر سحابة شخصي مبرمج بطريقة البنية التحتية لدوكر مع ادماج نظام حماية Honeypot و يعني بالإنجليزية قدر العسل أو مصائد مخترقي الشبكات بواسطة ادات راسبيري باي.

الكلمات المفتاحية : الحوسبة السحابية ,الافتراضية, الحاوية , دوكر , قدر العسل.

Résumé :

Depuis sa naissance au début des années 70, internet est devenu le pilier de la vie professionnelle moderne, son apparition a évolué d'un réseau simple de taille limité à une infrastructure inépuisable à grandes dimensions. Alors qu'il était initialement développé pour établir une communication entre des différents ordinateurs , aujourd'hui il provoque une décentralisation de ces systèmes centraux , tout en offrant des services complexes , à la demande des utilisateurs et aux entreprises en particulier , vers la révolution d'une nouvelle tendance qu'elle s'agit du cloud computing .

Le Cloud computing est une solution économique et technologique, dans lequel les ressources informatiques sont partagées et la puissance de calcul est configurable en fonction des besoins. tel que le stockage et la gestion des applications qui peuvent être provisionnées et libérées avec un minimum effort de direction.

Cependant, La protection de la vie privée et la sécurité des données sont primordiales dans l'utilisation des applications et les services cloud, et les risques qui accompagnent leur déploiement deviennent plus complexe avec l'infrastructure de cet technologie .

Dans ce mémoire nous nous intéressons à l'étude de la sécurité et la gestion des plateformes du cloud computing, en présentant les plus récentes solutions VMware existantes dans ce domaine tel que la technologie container par docker.

Notre objectif dans ce travail est de proposer une solution d'un serveur cloud personnel déployé à partir de l'infrastructure de gestion docker tout en intégrant un système de sécurité honeypot conceptionnel à l'aide d'une carte raspberry pi.

Mots clés : cloud computing,VMware, container, docker, honeypot , raspberry pi.