République Algérienne Démocratique Et Populaire Ministère De L'enseignement supérieur Et De La Recherche Scientifique
Université Abderrahmane Mira - Bejaia
Faculté de technologie
Département génie électrique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire de fin d'études
En vue d'obtention du diplôme de master
Options réseaux et systèmes de télécommunications

Etude et mise en place d'une solution d'automatisation Réseaux et systèmes

Réalisé par :
Ameziane Dihia
Amrane Nedjma

Encadré par :
M.

Membre de jury :

M.

M.

Promotion 2023 - 2024

Remerciements

En premier lieu, nous souhaitons exprimer notre reconnaissance envers Dieu le Tout-Puissant pour nous avoir accordé la force, le courage et la patience nécessaire pour mener humblement à bien ce travail.

Nous remercions sincèrement notre encadrant, **Mr Berrah Smail**, pour ses précieux conseils, orientations, disponibilité, sympathie et le temps qu'il nous a accordé tout au long de notre projet.

Nos remerciements à notre tuteur de stage, **Mr Yassine DJEBBARI**, pour son encadrement rigoureux et ses orientations tout au long de notre stage au sein du **CAMPUS NTS**.

Nous adressons également nos remerciements aux membres du jury d'avoir accepté d'assister à cette soutenance et d'évaluer notre travail.

Nous tenons aussi a exprimé toute notre gratitude, remercîment du fond du cœur à nos cher parents qui nous ont suivi et soutenue tout au long de nos études.

On remercie également toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce projet de fin d'études.

Dédicace

Je dédie humblement ce travail à mes chers parents, qui ont été mes piliers, mon inspiration et ma motivation tout au long de ce parcours. À **mon père**, pour son soutien inébranlable, et à **ma mère**, pour sa lumière, son amour inconditionnel et sa patience infinie. Que Dieu les protège et les bénisse.

À **Mr Berrah.S**, mon encadrant, dont les conseils avisés, les orientations précieuses et le soutien constant ont été d'une aide inestimable dans l'élaboration de ce mémoire.

À mes frères et sœurs, **Yassine, Zinou, Kahina, Asma**, qui ont été mes complices, mes confidents et mes meilleurs supporters. Votre présence a été un réconfort constant.

À mon Binôme, **Dihia** avec qui j'ai partagé ce voyage académique. Merci pour notre collaboration fructueuse et notre soutien mutuel.

À mes amies **Yousra , Khaoula , Imane, Ghouzlane** qui ont partagé mes joies, mes peines et mes succès Votre amitié est un trésor que je chérirai toujours.

Je remercie spécialement un ami **Tarek.M** qui m'a soutenu tout au long de la réalisation de mon projet qui n'aurait pu aboutir sans son aide précieuse et sa disponibilité .

Enfin, je dédie ce travail à toutes les personnes qui m'ont aimée et soutenue qui ont cru en moi et m'ont encouragée Votre confiance en moi a été ma plus grande motivation et je vous en suis infiniment reconnaissante.

Nedjma

Dédicace

Je dédie ce travail et ma profonde gratitude à **mon père** et **ma mère** pour L'éducation qu'ils m'ont prodiguée, au prix de tous Les sacrifices qu'ils ont Consentis à mon égard, pour le sens du devoir qu'ils m'ont Enseigné depuis mon enfance, Pour leur amour, leur soutien et leurs prières tout au long de Mes étude.

À **Mr Berrah.S**, mon encadrant, dont les conseils avisés, les orientations précieuses et le soutien constant ont été d'une aide inestimable dans l'élaboration de ce mémoire.

À ma sœur et mes frères **Ghaya, Mehdi, Massil, Samy et Idris**, qui ont été mes complices, mes confidents et mes meilleurs supporteurs. Votre présence a été un réconfort constant.

À mon Binôme, **Nedjma** avec qui j'ai partagé ce voyage académique. Merci pour notre collaboration fructueuse et notre soutien mutuel.

Je remercie spécialement un ami **Tarek.M** qui m'a soutenu tout au long de la réalisation de mon projet qui n'aurait pu aboutir sans son aide précieuse et sa disponibilité

À mes proches aimés et mes amis, merci d'avoir été là pour moi à chaque étape de ma vie. Votre amour, votre soutien et votre amitié ont été une source de réconfort et de joie pour moi, particulièrement dans les moments difficiles.

Dihia

Table des matières

Table des figures

Liste des abréviations

AD	Active Directory
APT	Advanced Packages Tool
CAT	Concatenate
CMDB	Configuration Management Data Base
DevOps	Developpement Operations
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FTTH	Fiber to the Home
FTTX	Fiber to the X
GNS3	Graphical Network Simulator-3
HTTP	Hypertext Transfer Protocol
IA	Intelligence Artificielle
IOS	Internetwork Operating System
IP	Internet Protocol
JSON	JavaScript Object Notation
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MKDIR	MaKe DIRectory
NTS	New Technology et Solutions
PING	Packet Internet Groper
PPA	Personal Package Archive
RSA	Rivest, Shamir, Adleman
SLA	Service Level Agreement
SSH	Secure Shell
SU	Super User
SUDO	Super User Do
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VTY	Virtual Terminal Lines
WAN	Wide Area Network

WINRM Windows Remote Management
YAML Yet Another Markup Language

Introduction générale

L'informatique est devenue essentiel afin de permettre aux utilisateurs d'accéder aux services et aux informations. À mesure que les centres de données se sont développés et que les applications hébergées se sont complexifiées, les administrateurs ont réalisé l'importance d'une collaboration dans la gestion des systèmes. C'est de cette manière que les outils de gestion de configuration et de provisionnement ont commencé à se développer.
Plutôt que de déployer, corriger ou gérer manuellement chaque serveur, les administrateurs ont accordé une grande importance à l'automatisation de la gestion des serveurs. C'est de cette manière que les développeurs d'applications ont commencé à communiquer avec les employés d'exploitation.
De nos jours, on regroupe les développeurs de logiciels et les experts en opérations informatiques sous le terme de DevOps. Quand les administrateurs collaborent étroitement avec les développeurs, cela permet d'améliorer la vitesse de développement et de gagner du temps. Une des premières étapes vers un environnement DevOps est de sélectionner des outils qui peuvent être utilisés à la fois par les développeurs et les ingénieurs d'exploitation.
Lorsqu'on évoque l'automatisation avec des DevOps, il est très probable que les termes Chef et Puppet soient évoqués. Cependant, ces dernières années, le moteur d'automatisation open source le plus mentionné est Ansible. On peut utiliser cette plate-forme à différentes fins : de la gestion de la configuration au déploiement d'applications procédurales, en passant par l'orchestration de plusieurs composants. Elle est sans agent, simple à mettre en place, à configurer et à maintenir.
Durant notre stage au sein de Compus NTS de Bejaia et après avoir étudier les différents aspects et besoins de cette entreprise, nous constatâmes que leur architecture réseau est constituée d'une centaine d'équipements. Notre objectif sera donc de concevoir une architecture avec un nœud d'automatisation, qui aura le rôle d'un serveur de gestion, de configuration, d'orchestration et de déploiement.

Ce mémoire est divisé en quatre chapitres :
Le premier chapitre « les fondamentaux des réseaux informatiques » cette partie examine ces défirent type et topologies, le modèle OSI, TCP/IP et la sécurité de ce dernier.
Le deuxième chapitre aborde « l'automatisation des réseaux et system, Ansible » cette partie explore les différentes solutions d'automatisation des réseaux, telles qu'Ansible, Puppet , Chef. Nous allons fait une comparaissant entre ces solutions et la raison pourquoi on a choisi l'outil de notre solution puis on a bien présenté cet outil.
Le troisième chapitre « Présentation de l'entreprise », concernera le Campus NTS au sein de laquelle nous avons effectué notre stage. Nous allons y présenter sa structure hiérarchique, son réseau informatique ainsi que son architecture.
Le quatrième chapitre « Simulation », portera notre environnement de travail et Nous aborderons l'automatisation des tâches en utilisant Ansible et nous expliquerons les différents exemples abordés.
Finalement, nous conclurons par une synthèse globale récapitulative des éléments clés de notre travail et nous examinerons les perspectives à venir.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Dans le monde numérique d'aujourd'hui, les réseaux informatiques sont devenus un élément indispensable pour les entreprises et les organisations de toutes tailles. Ils permettent une communication fluide, le partage de données et l'accès aux ressources, ce qui améliore la productivité, la collaboration et l'efficacité au sein des organisations. Cependant, la mise en œuvre et la maintenance d'un réseau informatique robuste nécessitent une compréhension approfondie des concepts, des technologies et des principes de sécurité réseau.
Ce chapitre explore les fondamentaux des réseaux informatiques, jetant les bases pour une exploration plus approfondie de l'administration et de la sécurité réseau. Nous examinerons les différents types de réseaux, leurs topologies sous-jacentes, ainsi que les protocoles de communication qui régissent l'échange de données. De plus, nous introduirons le concept de sécurité réseau et décrirons les critères essentiels pour protéger les réseaux contre les menaces potentielles.

1.2 Les réseaux informatiques

Un réseau informatique est composé d'une série de dispositifs électroniques connectés les uns aux autres, permettant ainsi le partage de ressources et de données. Ces réseaux facilitent la communication et la collaboration entre les utilisateurs, tout en offrant un accès à des services et des applications à distance. [TW11]

1.2.1 Rôles et importance des réseaux informatiques

Les réseaux informatiques jouent un rôle crucial dans le fonctionnement des organisations modernes. Ils permettent non seulement d'interconnecter des dispositifs, mais aussi de transformer la manière dont les ressources sont utilisées, les communications sont effectuées et les coûts sont gérés. Voici quelques aspects essentiels qui illustrent leur importance :

Partage des ressources

Les réseaux permettent un partage efficace des ressources informatiques, ce qui inclut les données, les applications et le matériel :

1. Accès aux Données et Applications, Les réseaux permettent aux utilisateurs d'accéder aux mêmes données et logiciels, indépendamment de leur emplacement physique. Cela signifie que les fichiers stockés sur un serveur central peuvent être consultés et modifiés par plusieurs utilisateurs simultanément, facilitant la collaboration et la gestion des informations.[Sta]
2. Partage du Matériel,Les ressources matérielles telles que les imprimantes, les scanners et les serveurs peuvent être partagées au sein du réseau. Par exemple, une seule imprimante peut être utilisée par plusieurs ordinateurs, ce qui réduit les coûts et améliore l'efficacité.[Sta]

Augmentation de la Fiabilité

Les réseaux informatiques augmentent la fiabilité des systèmes en permettant la redondance des données :

1. Tolérance aux Pannes, Les fichiers peuvent être copiés sur plusieurs machines, assurant leur disponibilité même en cas de panne.
2. Equilibrage de Charge, Si un serveur tombe en panne, d'autres peuvent prendre le relais pour éviter les interruptions.[Sta]

Réduction des Coûts

L'utilisation de réseaux informatiques permet des économies significatives à plusieurs niveaux :

1. Coût du Matériel, plutôt que d'investir dans de gros serveurs coûteux, les entreprises peuvent utiliser plusieurs petits ordinateurs en réseau, ce qui est souvent plus rentable pour des performances équivalentes.
2. Maintenance et Gestion, Centraliser les données et les applications dans un réseau facilite leur gestion et leur mise à jour, ce qui réduit les coûts de maintenance et de support.[Sta]

Facilitation de la Communication

Les réseaux sont des outils puissants pour améliorer la communication et la collaboration au sein des organisations.

1. Communication Instantanée : Grâce aux technologies de réseau, telles que la messagerie instantanée et la vidéoconférence, les employés peuvent communiquer en temps réel, indépendamment de leur localisation.
2. Collaboration à Distance : Les outils de collaboration en ligne permettent aux équipes de travailler ensemble sur des projets en temps réel, même si elles sont réparties sur différents sites géographiques.[Sta]

1.2.2 Classification des réseaux informatiques

Les réseaux informatiques peuvent être classifiés selon leur étendue géographique, leur topologie et leur méthode de transmission de données. En ce qui concerne l'étendue géographique : [Cyb24]

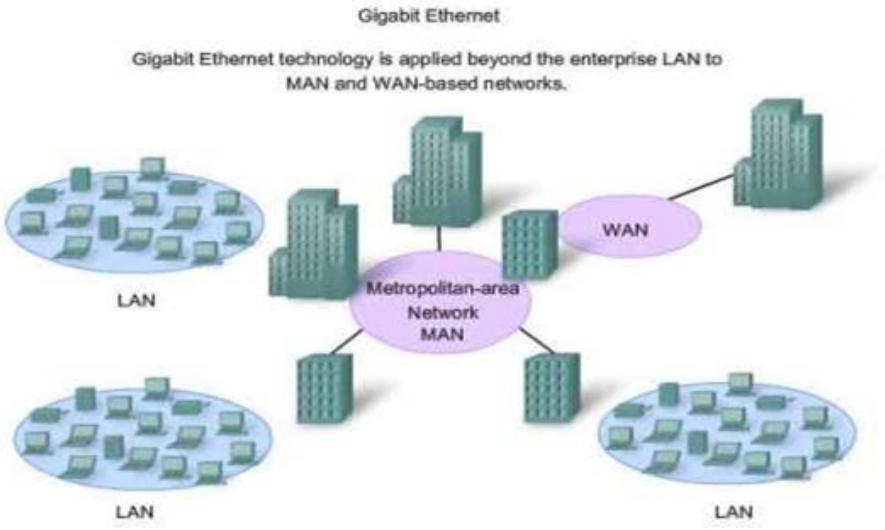

FIGURE 1.1 – Classification des réseaux informatiques

LAN (Local area network)

Il s'agit d'un réseau local qui relie des équipements situés dans un même bâtiment ou campus, souvent utilisé par une entreprise ou une organisation.

MAN (Métropolitain area network)

Le réseau étendu est similaire à un LAN en plus grand, et peut être public ou privé, couvrant un campus, une ville ou même une région géographique.

WAN (Wide area network)

Le réseau métropolitain permet de connecter des réseaux locaux sur de longues distances, souvent utilisé par des entreprises ayant des succursales situées dans différentes villes ou pays.

1.3 Les normes de communication réseau

1.3.1 Le modèle OSI

Est une norme établie par L'International Standard Organisation, afin de permettre aux systèmes ouverts (ordinateur, terminal, réseau, ...) d'échanger des in-

formations avec d'autres équipements hétérogènes. Cette norme est constituée de 7 couches, dont les 4 premières sont dites basses et les 3 supérieures dites hautes. Le principe est simple, la couche la plus basse (directement au dessus du support physique) ne peut communiquer directement avec une couche n +1 : chacune des couches est composée d'éléments matériels et ou logiciels chargés de « transporter » le message à la couche immédiatement supérieure.[J D23] [Sta]

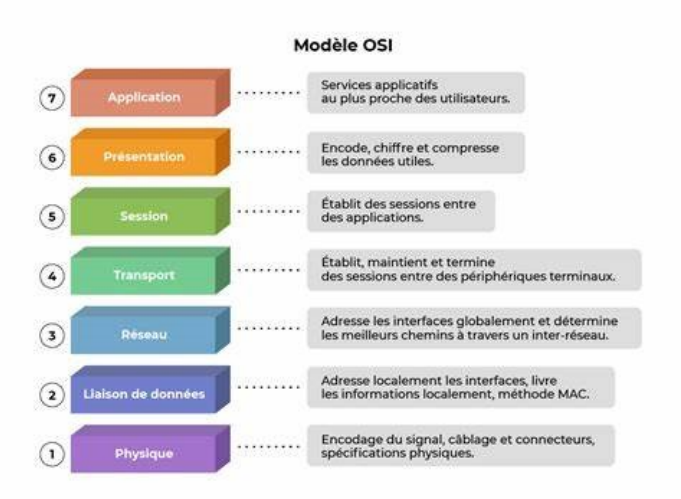

FIGURE 1.2 – Le modèle OSI

Il définit 7 couches :

La couche physique

cette couche comporte les éléments physiques appliqués dans le transfert des données, elle définit donc l'interface, les connecteurs et le câblage utilisés. L'unité de données manipulées à ce niveau est le bit.

La couche liaison

fournis les moyens d'établir et de maintenir les connexions entre les entités de réseau et les méthodes de contrôle d'accès au support (MAC) et de contrôle de liaison logique (LLC). De plus, elle détecte et elle corrige les erreurs de la couche physique. La trame est l'unité de données manipulées par cette couche.

La couche réseau

assure l'adressage et le routage des trames de données regroupées en paquets à travers le réseau, elle permet aussi l'interconnexion de réseau hétérogène.

La couche transport

responsable de la transmission des données de bout en bout, elle assure les fonctions de contrôle de flux, la résolution des pertes et le réassemblage des paquets en

message.

La couche session

responsable de l'ouverture et la fermeture des sessions de communication entre les machines du réseau ainsi elle organise et synchronise le dialogue entre les systèmes d'extrémité.

La couche présentation

s'occupe de la préparation et de la mise en forme des données afin qu'elles puissent être utilisées par la couche application, elle se charge aussi de la conversion, la compression de données et de la sécurité des informations (chiffrement/déchiffrement).

La couche application

c'est le point d'accès aux services réseaux (navigateur web, la messagerie électronique, etc.). Elle présente donc le niveau le plus proche des utilisateurs.

1.3.2 Le modèle TCP/IP

Le modèle TCP/IP est le modèle de référence utilisé par Internet ainsi que la plupart des réseaux informatiques actuels. Il comprend 4 couches principales :[Com14]

La couche liaison

Tout comme le modèle OSI, le modèle TCP/IP gère l'accès au support physique et les adresses MAC.

La couche internet

Le modèle TCP/IP gère l'adressage IP des machines, l'acheminement et le routage des paquets de données. Cette gestion correspond aux couches réseau et transport du modèle OSI.

La couche transport

Elle assure la fiabilité de la transmission des données entre les hôtes du réseau, en utilisant les protocoles TCP et UDP.

La couche application

Le modèle TCP/IP définit les protocoles utilisés par les applications réseau, tels que HTTP, FTP, SMTP, etc. Cette gestion correspond aux couches session, présen-

tation et application du modèle OSI.

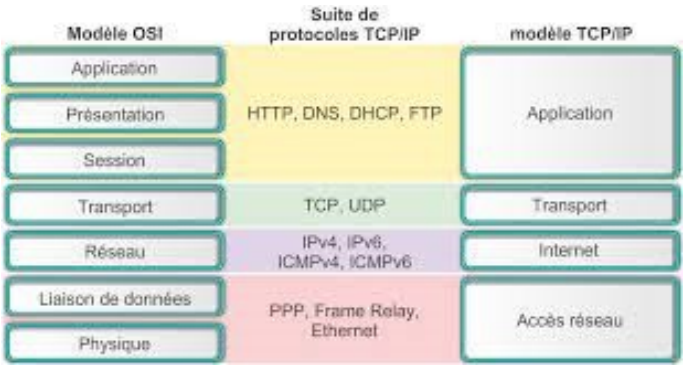

FIGURE 1.3 – Modèle TCP/IP compare au modèle OSI

Le modèle TCP/IP est largement utilisé dans les réseaux informatiques, notamment sur Internet. Il est plus simple que le modèle OSI et est mieux adapté aux réseaux IP, ainsi, il est moins rigoureux en matière de normalisation et de définition des couches. Parmi les organisations utilisant TCP/IP : Les opérateurs de centres de données qui utilisent le modèle TCP/IP pour gérer et contrôler le trafic réseau au sein de leurs centres de données. [TW11]

1.4 Analyse des besoins et de la topologie du réseau

L'analyse des besoins et de la topologie du réseau est une étape très importante dans la planification d'un réseau informatique en entreprise. Elle permet de comprendre les exigences spécifiques de l'entreprise en termes de communication, de partage de données et d'accès aux ressources. L'analyse des besoins de l'entreprise consiste à identifier les types d'appareils connectés au réseau, les types de données partagées et les utilisateurs et départements de l'entreprise. Cela permet de dimensionner adéquatement le réseau, de prévoir la capacité nécessaire et de mettre en place des autorisations d'accès appropriées. Une fois l'analyse des besoins effectuée, il est temps de planifier la topologie du réseau. La topologie du réseau détermine la façon dont les appareils sont connectés les uns aux autres et permet le flux des données. [SB15]

1.4.1 Topologie de réseau physique

Il illustre la réelle organisation des câbles et des équipements physiques dans le réseau. Elle souligne les interrupteurs, les routeurs, les serveurs et les autres équipements réseau, ainsi que les connexions câblées ou sans fil.

1.4.2 Topologie de réseau logique

Est un diagramme qui illustre la perception des appareils du réseau, sans prendre en compte la disposition physique des équipements. Les adresses IP, les sous-réseaux, les VLAN et les protocoles de communication entre les appareils sont mis en avant. Ce schéma offre une compréhension du parcours des données, des itinéraires suivis et des règles de communication établies.[Ins24]
La topologie du réseau définit la structure et les connexions entre les différents appareils du réseau. Voici quelques topologies couramment utilisées :

Topologie en Bus

C'est une configuration de réseau très simple qui relie tous les appareils à un câble commun, permettant ainsi des liaisons de transmission et une seule liaison sur laquelle un seul ordinateur peut envoyer des données à la fois. [Sta]

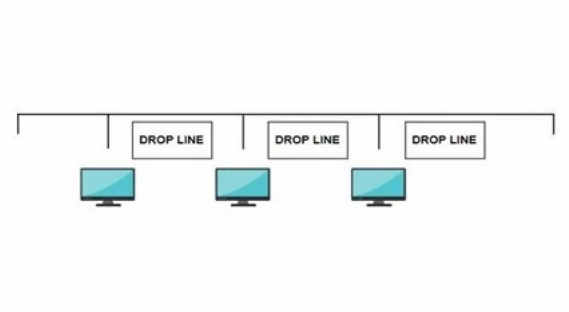

FIGURE 1.4 – Topologie en bus [Hat24]

Topologie en Anneau

Les équipements sont connectés les uns aux autres performer un anneau dans cette topologie. Cette configuration est plus résiliente car elle permet de maintenir la connectivité du réseau même si un lien tombe en panne.

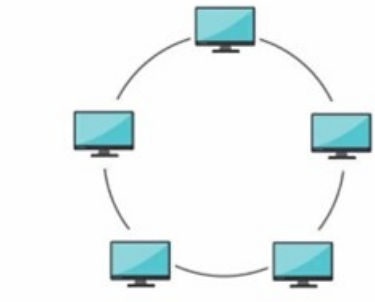

FIGURE 1.5 – Topologie en Anneau [Hat24]

Topologie en etoile

Tous les équipements sont connectés à un point central, qui est généralement un commutateur ou un concentrateur. Cette topologie est actuellement la plus courante, en particulier dans les réseaux Ethernet.

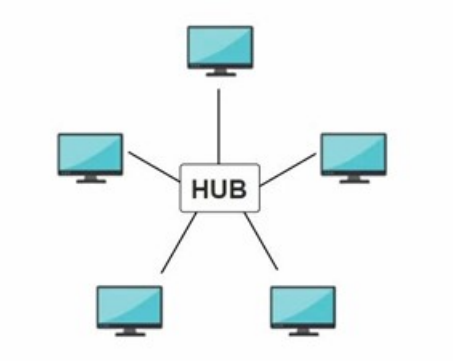

FIGURE 1.6 – Topologie en étoile [TW11]

Topologie en Arbre

Il s'agit d'une topologie multi-niveau, où les équipements sont connectés à différents niveaux. Cette configuration est souvent utilisée dans les grands réseaux d'entreprise.

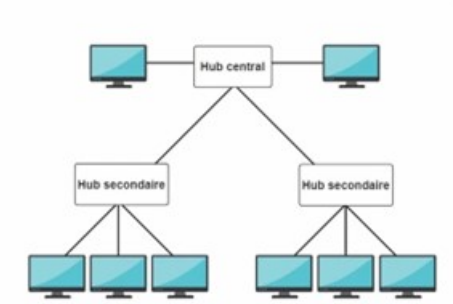

FIGURE 1.7 – Topologie en arbre [Hat24]

1.5 Architecture réseau

L'architecture réseau est la conception structurale qui détermine comment les différents composants d'un réseau sont interconnectés et communiquent entre eux. Elle inclut les principes, les modèles et les protocoles qui assurent l'efficacité, la sécurité et la scalabilité du réseau. [TW11]

1.5.1 L'architecture poste à poste

Une structure de réseau où chaque ordinateur, appelé "poste" ou "pair", fonctionne à la fois comme client et serveur. Contrairement aux architectures basées sur des serveurs centralisés, tous les postes dans un réseau P2P ont des capacités et des responsabilités similaires. Les postes communiquent directement entre eux sans passer par un serveur central. [Sta20]

1.5.2 L'architecture client/serveur

Elle implique la présence d'un serveur central auquel tous les clients (postes de travail) sont connectés via un réseau local. Le serveur centralise les ressources partagées telles que les fichiers, les imprimantes et les applications, et les rend accessibles aux clients.
L'architecture client/serveur est beaucoup plus puissante que l'architecture poste à poste et convient mieux aux besoins des organisations modernes, au détriment d'une plus grande complexité. Elle nécessite la mise en place d'un serveur central et d'un réseau local.[TW11]

FIGURE 1.8 – Comparaissant entre l'architecture client-serveur et l'architecture paire

1.6 La sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité.[PB13] [Sta20]

Confidentialité

Elle vise à garantir que seules les personnes autorisées ont accès aux informations et aux systèmes en utilisant des mécanismes d'authentification et de chiffrement. [SB15]

L'intégrité

Elle assure que les informations et les systèmes ne sont pas modifiés de manière inappropriée ou sans autorisation en utilisant des contrôles d'intégrité et des mécanismes de détection de modifications. [SB15]

La disponibilité

Elle garantit que les utilisateurs autorisés ont accès aux informations et systèmes quand ils en ont besoin. Elle implique la mise en place de redondances, de plans de reprise après sinistre et d'une surveillance de la disponibilité des services.[24]

La traçabilité

Elle permet de retracer les actions effectuées sur un système en identifiant qui a fait quoi, quand et comment. Elle utilise des journaux d'événements détaillés et des techniques d'authentification forte. [Ver24]

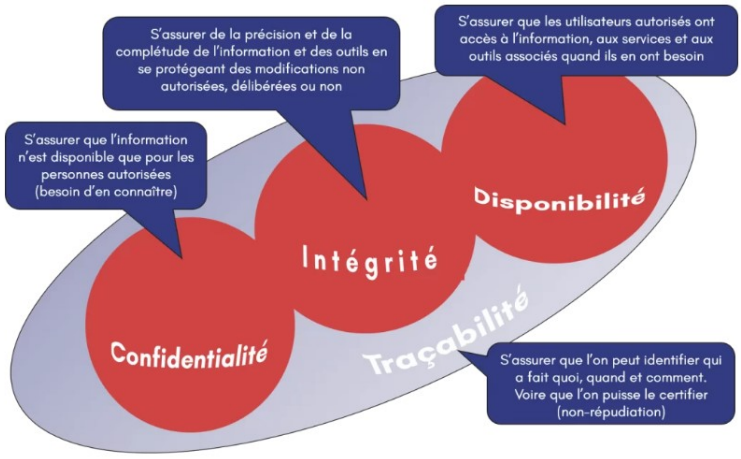

FIGURE 1.9 – La sécurité informatique. [Sta20]

1.6.1 Terminologie de la sécurité informatique

En sécurité informatique, il est essentiel de comprendre certains termes clés pour évaluer et gérer efficacement les risques liés aux systèmes d'information. Voici les définitions des termes mentionnés, avec des exemples pour clarifier chaque concept : [SB15]

Ressource

Toute entité ou élément ayant une valeur pour une organisation et nécessitant une protection. Les ressources peuvent inclure des données, des systèmes informatiques, du matériel, des logiciels, et même des services ou des informations sensibles.

Vulnérabilité

Une faiblesse ou un défaut dans un système ou une ressource qui pourrait être exploité par une menace pour causer des dommages ou obtenir un accès non autorisé.[Cyb24]

Menace

Tout danger potentiel pouvant exploiter une vulnérabilité pour nuire à une ressource ou perturber le fonctionnement d'un réseau. [Sta20]

Attaque

Une action délibérée menée par un acteur malveillant pour exploiter une vulnérabilité dans le but de nuire à une ressource ou de perturber un système.

Risque

La probabilité qu'une menace exploite une vulnérabilité, entraînant une perte, une altération, une destruction ou d'autres conséquences négatives pour une ressource ou un système. [Sta20]

1.7 Stratégies Avancées pour la Maintenance et le Support des Réseaux Informatiques

Assurer la maintenance et le support efficaces d'un réseau informatique est crucial pour la continuité opérationnelle et la performance d'une entreprise. Voici les principaux aspects à considérer pour optimiser ces processus : [Sta20] [All17]

Planification et Prévention : Une Approche Proactive

Élaboration d'un Plan de Maintenance, un plan de maintenance détaillé est essentiel pour prévenir les dysfonctionnements. Cela inclut des tâches telles que :

1. Mises à jour logicielles et firmware
2. Vérification et nettoyage du matériel

Surveillance Continue et Réactive : Garder un Œil sur le Réseau

Surveillance du Réseau, utiliser des outils avancés de monitoring pour :

1. Suivi en temps réel
2. Alerte proactive
3. Analyse des tendances

Gestion des Incidents : Une Réponse Rapide et Efficace

Analyse et Résolution des Problèmes :

1. Diagnostic approfondi
2. Actions correctives immédiates
3. Documentation des incidents

Sécurité Renforcée : Protéger le Réseau Contre les Menaces

Gestion des Mises à Jour de Sécurité :

1. Application régulière des patchs
2. Surveillance des menaces
3. Tests de sécurité réguliers

Support Utilisateur : Fournir une Assistance Réactive et Humaine

Assistance aux Utilisateurs :

1. Centre de support dédié
2. Base de connaissances
3. Suivi des demandes

Développement Continu des Compétences : Se Former pour l'Avenir

Formation Continue :

1. Mise à jour des compétences
2. Certifications professionnelles
3. Partage de connaissances

Évaluation et Amélioration Continues : Mesurer et Optimiser

Évaluation des Performances :

1. Indicateurs de performance clés (KPI)
2. Retour d'expérience
3. Processus d'amélioration continue

1.8 Conclusion

Dans ce chapitre nous avons présenté les réseaux et la sécurité informatique d'une façon générale, nous avons cité les critères basiques qui montrent le rôle d'un réseau informatique et la nécessité de le sécurisé, pour l'objectif de bien définir le concept d'administration et la sécurité d'un réseau au sein d'une entreprise. Le chapitre suivant sera consacré pour l'automatisation des réseaux, system et l'outil ansible.

Chapitre 2

Automatisation des réseaux et systèmes, Ansible

2.1 Introduction

Les équipements réseau ainsi que leurs natures hétérogènes ne cessent d'augmenter au fil du temps. Les administrateurs utilisaient des méthodes traditionnelles pour gérer le réseau, ce qui entraînait une configuration plus complexe, moins rapide, exposée aux erreurs humaines et qui nécessite beaucoup de moyens financiers.
L'Automatisation vient résoudre tous ces problèmes pour des centaines de milliers d'utilisateurs dans le monde entier.
Un ingénieur DevOps choisit les outils qui peuvent être utilisés par les développeurs et les ingénieurs d'opérations. Ansible est l'outil de choix pour réunir. Afin de pourvoir simuler un cas d'automatisation en utilisant l'outil Ansible.

2.2 Automatisation du réseau

L'automatisation en terme général correspond à l'utilisation de technologies pour effectuer certaines taches avec une intervention humaine réduite.
L'automatisation du réseau quant à elle est le processus d'automatisation de la configuration, de la gestion, des tests, du déploiement et du fonctionnement des périphériques physiques et virtuels au sein d'un réseau. Ce processus permet en outre d'exécuter ces tâches de façon fiable et répétée afin d'en améliorer l'efficacité, de réduire les erreurs humaines, et de diminuer les frais d'exploitation. [O0024] [Smi18]

2.2.1 Utilité de l'automatisation

L'automatisation permet non seulement d'accélérer les processus mais aussi de réduire les erreurs humaines, d'améliorer la précision et d'assurer une gestion plus proactive et réactive des ressources. Voici quelques-unes des utilités clés de l'automatisation dans le contexte des réseaux : [Smi18]

1. La planification et la conception du réseau, y compris la planification de scénarios et la gestion des inventaires
2. Le test des équipements et la vérification de la configuration.
3. Le provisionnement des équipements et services physiques déployés, ainsi que le déploiement et le provisionnement des équipements virtuels.
4. La collecte de données réseaux relatifs aux équipements, systèmes, logiciels, topologies réseau, trafic et services en temps réel.
5. L'analyse des données, y compris l'analyse prédictive basée sur l'IA , pour déterminer le comportement actuel et futur du réseau.
6. La conformité de la configuration, qui garantit le bon fonctionnement de tous les équipements et services réseau.
7. La mise à jour des logiciels, y compris la restauration si besoin.
8. La résolution en boucle fermée des incidents réseaux, y compris des pannes et des défaillances masquées.
9. La production de données de rapports, de tableaux de bord, d'alertes et d'alarmes
10. L'application des règles de sécurité.
11. La surveillance du réseau et de ses services pour garantir le respect des SLA et la satisfaction des clients.

2.2.2 Rôle de l'automatisation pour les entreprises

L'automatisation est devenue un élément crucial de la transformation numérique des entreprises, car elle leur permet de gagner en efficacité, en productivité et en agilité. Voici quelques-uns des avantages clés de l'automatisation pour les entreprises : [All17] [Smi18]

Réduction des coûts de production

Grâce à l'automatisation, il est possible de réduire les coûts en éliminant les tâches manuelles répétitives, en améliorant la qualité et la précision des processus, et en limitant les erreurs humaines. Cette optimisation peut entraîner des économies considérables en termes de temps, de main-d'œuvre et de ressources pour l'entreprise.

Augmentation de la productivité

Grâce à l'automatisation, les employés peuvent être libérés des tâches répétitives et chronophages, et ainsi se concentrer sur des tâches à plus forte valeur ajoutée. Cette optimisation peut augmenter la productivité globale de l'entreprise, ainsi que la satisfaction et la motivation des employés.

Amélioration de la qualité

L'automatisation permet d'améliorer la qualité des processus en limitant les erreurs humaines et en assurant la cohérence et la précision des résultats. Cette op-

timisation peut améliorer la satisfaction des clients et renforcer la réputation de l'entreprise. [Smi18]

Accélération des délais

Grâce à l'automatisation, les délais de traitement peuvent être réduits en éliminant les tâches manuelles répétitives et en accélérant les processus. Cette optimisation peut améliorer la réactivité de l'entreprise et lui permettre de répondre plus rapidement aux demandes des clients.

Renforcement de l'agilité

L'automatisation permet de rendre les processus plus flexibles et adaptables aux changements, en permettant une modification facile et rapide des processus et des workflows. Cette optimisation peut aider les entreprises à s'adapter plus rapidement aux changements de marché et à maintenir leur compétitivité.

2.2.3 Gestion de l'automatisation

Auparavant, les administrateurs système géraient les serveurs manuellement, installaient les logiciels, changeaient les configurations et administraient les services sur des serveurs individuels. À mesure que les Datacenter se développaient et que les applications hébergées devenaient plus complexes, les administrateurs ont réalisé qu'ils ne pouvaient pas faire évoluer leur gestion manuelle des systèmes aussi rapidement que les applications qu'ils activaient. Cela a également entravé la vitesse du travail des développeurs car l'équipe de développement était agile et publiait fréquemment des logiciels, mais les opérations informatiques passaient plus de temps à configurer les systèmes. C'est pourquoi que des outils de provisionnement de serveur et de gestion de la configuration automatique ont prospéré.[All17] [LK21]

2.3 Outils et technologies d'automatisation

Il existe plusieurs outils pour faciliter la gestion de la configuration. L'objectif de ces outils est de réduire la complexité et le temps de configuration et de maintenance des réseaux surtout les gros réseaux avec des certaines de périphériques. Dans la catégorie des outils de gestion de configuration et automatisation, il y'a trois outil NetDevops qui sont les plus connus et utilisés par les entreprises : Ansible, Puppet, Chef [Don11] [Sta20]

2.3.1 Ansible

Ansible, est un outil d'automatisation informatique Open Source qui automatise le provisionnement, la gestion des configurations, le déploiement des applications, l'orchestration et bien d'autres processus informatiques. Il fonctionne sur de nom-

breux systèmes de type Unix et peut configurer aussi bien des systèmes de type Unix que Microsoft Windows. [Doc24]

FIGURE 2.1 – Ansible [Gof24]

2.3.2 Puppet

Puppet, est un outil de gestion de configuration qui assure un moyen standard de livrer et d'exploiter les logiciels, quel que soit l'endroit où il s'exécute deux éditions de l'outil : Open source et professionnelle. [Doc21]
Il est construit sur une architecture serveur-client qui comprend un master (serveur centralisé) et plusieurs nœuds (clients). Dans chaque nœud, un agent Puppet est installé pour communiquer avec le master Puppet.

FIGURE 2.2 – Puppet [Ver24]

L'objectif de cette outil est de mettre en œuvre une manière flexible et standard d'automatiser le déploiement et la mise en production des applications.
Avec Puppet, les administrateurs peuvent définir l'état désiré de leurs systèmes en utilisant du code, généralement écrit dans un langage spécifique appelé Puppet DSL (Domain-Spécifique Langage). Puppet se charge ensuite de garantir que les systèmes maintiennent cet état désiré au fil du temps.

2.3.3 Chef

Chef, est un outil de gestion de configuration et une plateforme d'automatisation conçu pour rationaliser les tâches de provisionnement, de configuration et de maintenance des serveurs d'une entreprise. Il transforme l'infrastructure en code, la rendant souple, vision nable, lisible et testable, quelle que soit la plateforme ou il

s'exécute ou la taille du réseau. Ecrit en Ruby et Erlang, il peut s'intégrer avec une grande variété de plateformes cloud. Chef permet d'automatiser le déploiement, la configuration et la gestion des infrastructures informatiques.[RO21]

FIGURE 2.3 – Chef

2.4 Comparaison des fonctionnalités

Dans le cadre de la gestion des systèmes et de l'automatisation des déploiements, les outils de gestion de configuration tels que Ansible, Chef et Puppet sont devenus indispensables. Ils facilitent le processus de configuration, de gestion et de déploiement des infrastructures, permettant aux équipes d'assurer la cohérence et la rapidité des opérations IT.
Le tableau ci-dessous compare ces trois outils selon plusieurs critères clés : [**b19**]

Outils Critères	ANSIBLE	CHEF	puppet
Système de communication	Rapide	Très lent	Lent
Exécution de Configuration	Facile	Difficile	Difficile
Langage de configuration	YAML : permet de représenter des Données structurées	DSL (Ruby)	DSL(Puppets) : Propre à Puppet
Installation	Facile	Compliqué	Compliqué
Architecture	Client	Client/serveur	Client/serveur
Mécanisme de transport	SSH/Netconf	Rest	Rest
Evolutivité	Très haut	Haut	Haut
Déplacement client	Python, ssh, Bash	Ruby, ssh, Bash	Ruby
Capacités	-orchestration simple - Provisionnement rationalisé -Livraison continus avec flux de travail automatisé -Déploiement d'applications -Intégration de la sécurité et de la conformité dans les processus automatisés	-Livraison continus avec flux de travail automatisé - Gestion de la conformité et de la sécurité	-orchestration -Provisionnement rationalisé -Visualisation et reportant simples -Transparence élevée -Contrôle d'accès basé sur les rôles

FIGURE 2.4 – Comparaison des fonctionnalités [Ver24]

2.5 Choix de l'outil d'automatisation

Il s'agit de décider quel outil nous devons utiliser pour automatiser les actions des serveurs en fonction de nos besoins et de nos contraintes. En se basant sur l'étude comparative, nous avons opté Ansible. Ce choix est pour les raisons suivantes : [LT17] [LK21]

1. **Gratuit** Ansible est un outil open source.
2. **Simple** Ansible utilise une syntaxe simple écrite en YAML. Aucune compétence en programmation particulière n'est nécessaire pour créer les playbooks d'Ansible. Il est également simple à installer.
3. **Puissant** Ansible vous permet de modéliser des workflows très complexes.
4. **Flexible** Ansible vous fournit des centaines de modules prêts à l'emploi pour gérer vos tâches, quel que soit l'endroit où ils sont déployés. Vous pouvez réutiliser le même playbook sur un parc de machines Red Hat, Ubuntu ou autres.
5. **Client** vous n'avez pas besoin d'installer d'autres logiciels ou d'ouvrir des ports de pare-feu supplémentaires sur les systèmes clients que vous souhaitez automatiser. Ansible réduit encore l'effort requis pour que votre équipe commence à automatiser immédiatement.
6. **Efficace** Parce que vous n'avez pas besoin d'installer de logiciel supplémentaire, il y a plus de place pour les ressources d'application sur votre serveur.
7. **Capacité** une révision des capacités de chaque outil d'automatisation, peut vous aider à choisir l'outil de mieux adapté à nos besoins. Chaque outil possède son propre ensemble de capacités qui sont meilleures à leur manière.

L'outil Ansible vise à fournir des gains de productivité importants à une grande variété de défis d'automatisation. C'est un outil qui se veut simple à l'utilisation mais suffisamment puissant pour automatiser des environnements d'applications complexes à plusieurs niveaux. [RO21]

2.6 Ansible

Ansible est un utile open-source pour l'automatisation des tâches informatiques permettant de réaliser des communications à une vitesse superluminique (supérieure à la vitesse de la lumière) imaginé en 1966 par Ursula K. Son créateur est Michael Dean ; la première version d'Ansible date de 2012. Le nom Ansible est tiré d'un roman de science-fiction écrit par Ursula Le Guin, qui désigne un moyen de communication plus rapide que la lumière. Entre-temps, Ansible a été racheté en 2015 par Red Hat qui a été racheté par IBM (international business machines) en 2018. Donc, Ansible appartient désormais à IBM.
Le nom Ansible a été choisi en référence au terme « Ansible » a été inventé par Ursula K. Le Guin dans son roman de science-fiction Rocandons World en 1966 pour désigner un moyen de communication plus rapide que la lumière. [Doc24]

2.6.1 Concepts clés

Ansible est un outil NetDevOps d'automatisation informatique écrit en python. Il fonctionne sur de nombreuse distribution de type Linux/Unix. Ansible s'est progressivement imposé comme le principal outil d'automatisation dans le monde de réseau. Elle combine le déploiement de logiciels multi-nœuds, l'exécution des tâches ad-hoc, et la gestion de configuration, et l'automatisation des tâches. Elle gère les différents nœuds à travers SSH et ne nécessite l'installation d'aucun logiciel supplémentaire sur ceux-ci. [Doc24]
Ansible présente en sortie standard les résultats de ses actions en format JSON, mais Ansible utilise le format YAML pour exprimer des descriptions réutilisables de systèmes modèle, appelées ' Playbook'. Enfin, les variables peuvent se présenter dans Ansible grâce aux modèles Jinja2.

2.6.2 Utilisation de langage de programmation et Protocol utilisés pour Ansible

Techniquement, Ansible se base sur les langages ou protocoles suivants : [SB15]

1. La plate-forme et les modules sont développés en langage Python
2. YAML (Yet Another Markup Language) a été proposé pour la première fois par Clark Evans en 2001, qui l'a conçu avec Ingy dot Net et Oren Ben-Kiki. Il est un langage de sérialisation de données lisible par l'homme qui est souvent utilisé pour les fichiers de configuration et dans les applications où des données sont stockées ou transmises. Il vise un grand nombre des mêmes applications de communication que le langage de balisage extensible (XML) mais possède une syntaxe minimale. C'est un sur-ensemble strict de JSON, un autre langage de sérialisation des données. [LT17]
3. Le protocole SSH (secure shell) est enfin utilisé pour la communication avec les machines cibles.

2.6.3 Architecture d'Ansible

Ansible est un outil d'automatisation de la configuration et de l'orchestration sans agent qui utilise une architecture simple et efficace. Voici les composants clés de son architecture : [Doc24]

Nœud de Contrôle

C'est le serveur central où Ansible est installé et à partir duquel toutes les commandes et scripts sont exécutés.Il orchestre les opérations, gère les inventaires, et exécute les playbooks pour gérer les nœuds distants.

Nœuds Gérés

Ce sont les machines (serveurs, postes de travail, équipements réseau) sur lesquelles les tâches d'automatisation sont effectuées.Reçoivent et exécutent les com-

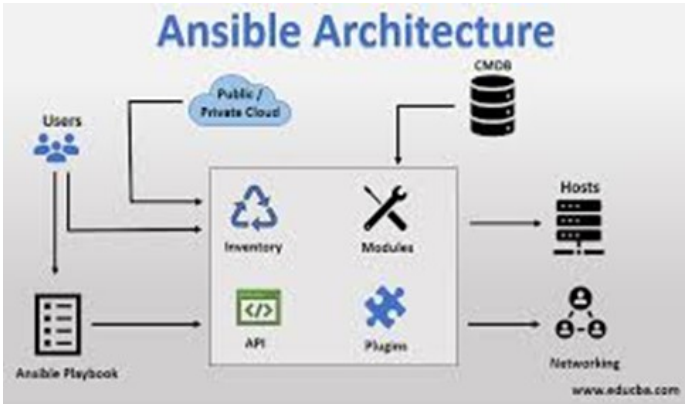

FIGURE 2.5 – Architecture d'Ansible

mandes envoyées par le nœud de contrôle via SSH (ou WinRM pour les machines Windows).

Inventaire

Une liste ou une base de données des nœuds gérés par Ansible. Organise les nœuds en groupes pour faciliter la gestion ciblée des tâches.

Modules

Petits programmes autonomes qui accomplissent des tâches spécifiques sur les nœuds gérés.et gére des aspects comme l'installation de paquets, la gestion de fichiers, la configuration réseau, etc.

Plugins

Fichiers YAML qui définissent les tâches à exécuter sur les nœuds gérés, Orchestrent des séquences d'actions complexes et décrivent l'état désiré des systèmes.

Playbooks

Rôle : Extensions qui ajoutent des fonctionnalités supplémentaires à Ansible. Gèrent les connexions, modifient l'inventaire, enregistrent les journaux, et bien plus encore.

2.6.4 Domaine d'application d'Ansible

Ansible est un outil polyvalent utilisé dans de nombreux domaines de l'administration système et du développement logiciel. Son architecture sans agent, sa simplicité et sa flexibilité en font un choix populaire pour une variété de tâches. Voici les principaux domaines d'application d'Ansible : [Doc24] [LT17]

La gestion des configurations

La gestion des configurations est un processus qui permet de maintenir les systèmes informatiques, les serveurs et les logiciels dans l'état souhaité et d'en préserver la cohérence. C'est une façon de s'assurer qu'un système fonctionne comme prévu au fil des changements effectués. Par exemple elle peut configurer un serveur, puis créer ses systèmes et en assurer le bon fonctionnement. Ansible nous permet d'accélérer les changements et les déploiements, de nous éviter les risques d'erreur humaine et de rendre la gestion des systèmes plus prévisible et évolutive. De plus, il permet de suivre l'état des ressources et évite de répéter des tâches, telles que l'installation d'un même paquet deux fois.

L'orchestration

L'orchestration permet de décrire comment automatiser un processus constitué de nombreuses étapes réalisées sur plusieurs systèmes différents. Ansible permet d'orchestrer le déploiement en exécutant les tâches du playbook dans l'ordre dans lequel elles ont été rédigées, tout en nous garantissant que le processus se déroule comme prévu.

Le déploiement d'application

L'automatisation du déploiement permet de déplacer les logiciels entre les environnements de test et de production à l'aide de processus automatisés. Ainsi, elle assure la reproductibilité et la fiabilité des déploiements tout au long du cycle de distribution.

Le provisionnement

La première étape de l'automatisation du cycle de vie des applications consiste à automatiser le provisionnement des infrastructures. Avec Ansible, on peut provisionner des plates, formes Cloud, des hôtes virtualités, des périphériques réseau et des serveurs barre métal

2.7 Conclusion

Dans ce chapitre, nous avons d'abord établi une vue générale sur les points essentiels de notre projet. Ensuite, une vue globale sur les différents domaines et outils de l'automatisation a été présenté. Enfin, nous nous sommes approfondis sur le cœur de notre sujet ; Ansible, en expliquant son principe de fonctionnement et pourquoi nous avons fait le choix de cet outil.

Chapitre 3

Présentions de l'organisme d'accueil

3.1 Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology § Solutions) où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

3.2 Présentation de l'entreprise, Campus NTS

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil.

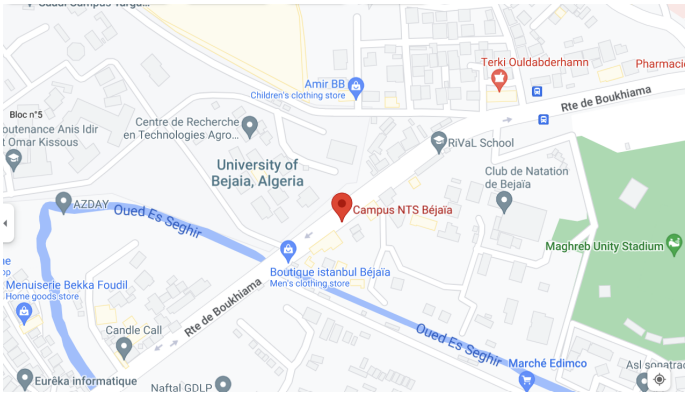

FIGURE 3.1 – Localisation de l'entreprise NTS

Elle a été créée en 2020 à Bejaia par Yassine DJEBBARI, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

1. Air Algérie
2. Retelem Alger.
3. Poste d'Algérie.
4. Adèle.
5. RATP ALJAZAIR.
6. La technologie.
7. Géant de l'électronique BBR.
8. Morsi.
9. Université de Bejaïa.
10. Cité universitaire à Bejaïa (targa ouzamour, 17 octobre...etc).
11. SARL Alphas Bejaïa.
12. Providentia Béjaïa.

3.2.1 Fiche technique de l'entreprise

Le tableau ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

Dénomination	Campus NTS
Logo	CAMPUS NTS INNOVATION TECHNOLOGY
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Bejaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

FIGURE 3.2 – Identification sur campus NTS

3.2.2 Objectifs, Missions et activités de l'Entreprise N.T.S

Les objectifs, les missions et les activités sont représentées dans la figure

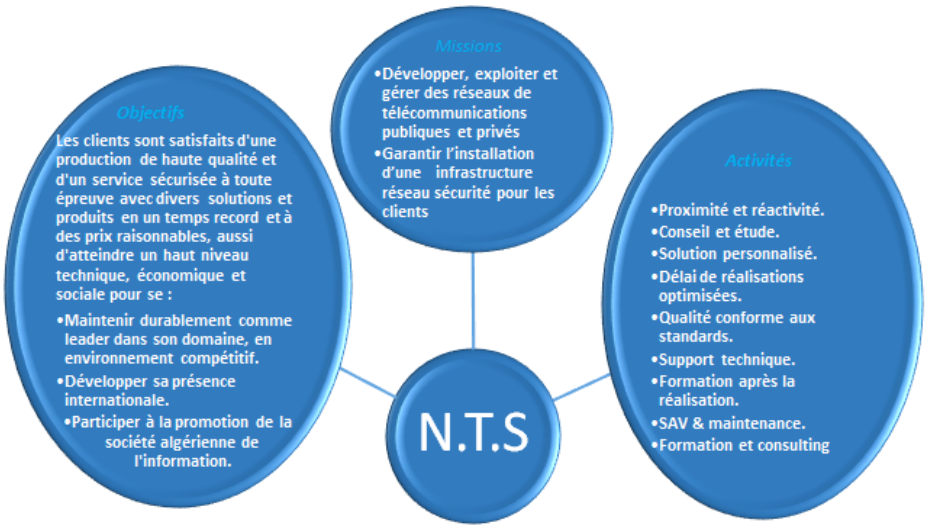

FIGURE 3.3 – Objectifs, Missions et Activités de l'NTS

3.3 Organigramme général de l'organisme d'accueil

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS dans lequel cet apprentissage termine le stage :

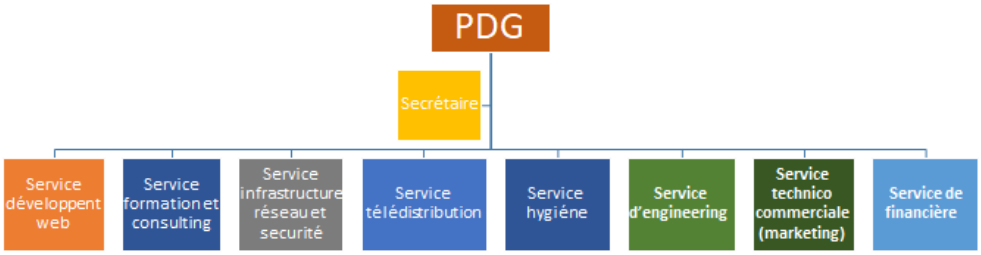

FIGURE 3.4 – L'organigramme de campus NTS.

3.3.1 Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

3.3.2 Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

1. Installation et configuration des réseaux informatiques.
2. Installation et configuration des réseaux informatiques.
3. Administration et sécurité des réseaux et système.
4. Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto...).
5. Installation et configuration des réseaux sans fil professionnel.
6. Installation et configuration des caméras de surveillance analogique et numérique.
7. Fibre optique les réseaux d'accès FTTH/FTTX.
8. Création des sites web.
9. Programmation (C, C++, C#, Java, Python...etc.).
10. Electricités Bâtiments et industriels.
11. Formation `Cisco CCNA`, `CCNP S&R`.
12. Virtualisation.
13. Microsoft server, SQL.
14. Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

3.3.3 Service d'accueil

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

Service réseau informatique

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :
Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

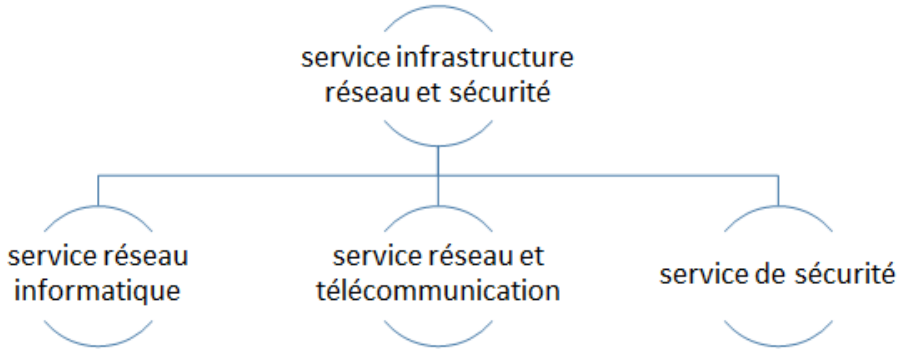

FIGURE 3.5 – Organigramme de service d'accueil

Service réseau et Télécommunication

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

1. Pose de fibre optique.
2. Emplacement du site de la tour cellulaire.
3. Test d'antenne radio.
4. Installation d'équipements téléphoniques standards et réseau de données.
5. Téléphonie standard

Service de sécurité

Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.
Les services qu'elle réalise sont les suivants :

1. Caméras de surveillance
2. Alarme anti- intrusion
3. Détection incendie
4. Pointeuse et Contrôles d'accès
5. Vidéophonie

3.3.4 Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

1. Rediffusion de programmation par satellite.
2. Transmission de chaînes de télévision par abonnement.
3. Services interactifs.
4. Programmation locale.

3.3.5 Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.
L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

1. D'ingénieurs en télécommunications.
2. D'informaticiens en gestion et sécurité des réseaux.
3. D'administrateurs de systèmes d'information.
4. D'informaticiens en programmation.
5. De techniciens fibre.
6. De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

3.3.6 Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

3.3.7 Service de financière

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :
Les tâches principales du Service des finances :

1. Assurer une saine gestion des ressources financières de l'entreprise par la planification.
2. La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
3. La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

Le rôle du service financier :

1. Le rôle du service financier :
2. La préparation et du suivi des budgets de fonctionnement et d'investissement.
3. La préparation des états financiers.
4. La gestion de la trésorerie et de des encaissements.
5. La rémunération des employés, des comptes à payer.
6. De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
7. La réception des marchandises et du courrier.

3.3.8 Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

1. Des actions de prévention des risques professionnels et de la pénibilité au travail.
2. La mise en place d'une organisation et de moyens adaptés.

3.4 État des lieux (Client Collable)

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte ces vlans à une connexion L.S (Ligne Spécialisée publique symétrique) en fibre optique fournie par Algérie télécom, Le schéma ci-dessous nous montre l'infrastructure du réseau Collable :

3.4.1 Présentation de l'architecture réseau existant dans l'entreprise

Collable construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure suivante :

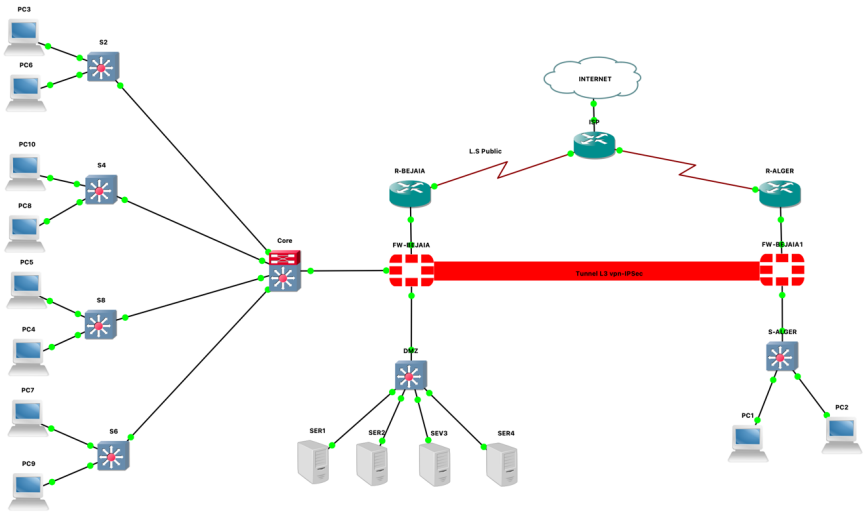

FIGURE 3.6 – Architecture de réseau Collable

3.4.2 Analyse du parc informatique

Présentation d'environnement hard et soft :

Nom de l'équipement	Le hardware (hard)	Software (soft)
Routeur	ISR 4331	IOS (International Organisation For Standardisation)
Pare-feu	PfSense	FREEBSD
Switch	• HPE 1820-24G Managed L2 • HPE 1920-24G Managed L3	LINUX
server	ESHP ProLiant DL380P génération 10	• ESXI • GOAUTODIAL • SERVER WINDOWS 2022
PC portable	Dell IAER 35 R	Windows 10

FIGURE 3.7 – Présentation d'environnement hard et soft

Les caractéristiques des équipements par niveaux :

Nom de l'équipement	Modèle	Caractéristique
Router 	ISR 4331	• **RAM :** 4 G0 (installé) /16 GO (maximum) • **Mémoire Flash :** 4000 MO • **Débit :** 100 Mb/s • **Protocole de liaison de données :** Ethernet, fast Ethernet et gigabit-Ethernet
Pare-feu 	PFSENSE	• **Débit :** 4000 Mbit/s • **Débit IPS :** 2700Mbit/s • **Débit VPN IP sec :** 560 Mbit/s • **@ IP/Numéro de port**
Switch 	HPE 1920	• **Ports :** 24 ports • **Mémoire Flash :** 16MO • **Mémoire RAM :** 128MO • **Capacité de commutation :** 32 Gbit/s
Switch 	HPE 1820	• **Ports :** 24 ports • **Mémoire Flash :** 128MO • **Mémoire RAM :** 512MO • **Capacité de commutation :** 56 Gbit/s
server 	HP ProLiant DL380P génération 10	• Processor Intel Xeon Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo) • 16 G0 DDR4 RDIMM (1x 16 GO - 12 slots)

FIGURE 3.8 – Présentation d'environnement hard et soft

3.5 Problématiques et Solutions proposées

Lorsque les équipes de Réseaux et Sécurité sont confrontées à des tâches, elles rencontrent certains problèmes qu'elles résolvent manuellement. Ce processus devient ainsi une boucle, ce qui peut entraîner des contraintes de temps et, surtout, des erreurs dans la configuration.
Dans l'ensemble, compte tenu des problèmes mentionnés ci-dessus, il est nécessaire de trouver une solution évolutive capable de résoudre ces problèmes. C'est pourquoi, dans ce projet, nous avons adopté l'outil NetDevOps Ansible.

3.6 Conclusion

Dans ce chapitre, nous avons donné un aperçu de l'infrastructure de client collable du fournisseur de solution IT campus nts, puis nous avons découvert un problème qui nous a amenés à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant

Chapitre 4

Environnement de travail et simulation

4.1 Introduction

Ce chapitre consistera en la préparation de notre environnement, en expliquant toutes les étapes qui contribueront au bon fonctionnement de notre projet.
On abordera des exemples d'automatisation avec Ansible. Le but est d'avoir la capacité de concevoir un programme et de l'intégrer en utilisant des lignes de commandes sur les nœuds de notre réseau. Tout d'abord, nous allons établir un document qui enregistrera toutes les machines que nous devrons automatiser.'
Ensuite, nous rédigerons des manuels au format YAML qui renfermeront toutes les informations concernant les nœuds à gérer et les tâches à effectuer sur ces nœuds.
En fin de compte, nous installerons ces programmes sur nos machines et vérifierons l'efficacité de ces scripts.

4.2 Présentation de l'environnement de travail

En termes de logiciels, nous avons utilisé plusieurs systèmes d'exploitation,notamment Windows10 et Ubuntu . Nous avons installé les outils nécessaires sur ces systèmes d'exploitation, tels que :

4.2.1 GNS3

GNS3 est une plateforme de simulation réseau open-source qui permet de créer des topologies complexes en intégrant des équipements réseaux virtuels. Dans notre étude, GNS3 est utilisé comme base pour la création et la gestion des réseaux virtuels, incluant les routeurs, les commutateurs et autres périphériques réseau. Nous détaillerons les configurations spécifiques et les choix de topologie effectués pour nos expérimentations. [GNS23] [Wel17]

FIGURE 4.1 – GNS3 [GNS23]

4.2.2 VMware Workstation

VMware Workstation est une plateforme de virtualisation permettant de créer et de gérer des machines virtuelles sur un système hôte. Dans notre environnement de simulation, VMware Workstation est utilisé pour exécuter les machines virtuelles nécessaires pour simuler des serveurs, des postes de travail ou d'autres dispositifs spécifiques à notre étude. Nous discuterons des configurations matérielles et logicielles utilisées pour chaque machine virtuelle. [VMw23]

FIGURE 4.2 – VMware Workstation [VMw23]

4.2.3 pfSense

Ce système d'exploitation open source est basé sur FreeBSD. Il est conçu pour configurer des routeurs et pare-feu robustes. pfSense offre une large gamme de fonctionnalités de sécurité et de gestion réseau, ce qui en fait un choix idéal pour nos besoins en matière de sécurité informatique.Ansible : Cet outil open-source d'automatisation simplifie la gestion des configurations, le déploiement d'applications et l'automatisation des tâches informatiques. [Lin20]

FIGURE 4.3 – pfSense [Lin20]

4.2.4 Ansible

Cet outil open-source d'automatisation simplifie la gestion des configurations, le déploiement d'applications et l'automatisation des tâches informatiques. Ansible est apprécié pour sa capacité à orchestrer facilement les opérations sur de nombreux systèmes, ce qui améliore notre efficacité opérationnelle. [Doc24]

FIGURE 4.4 – Ansible [Doc24]

4.3 Installation des systèmes et préparation du lab

4.3.1 Installation de GNS3

Pour installer GNS3, il vous suffit de télécharger son fichier exécutable, de le lancer et de suivre les étapes d'installation présentées dans l'annexe jusqu'à la fin, pour obtenir l'interface illustrée dans la figure suivante : [Bom23]

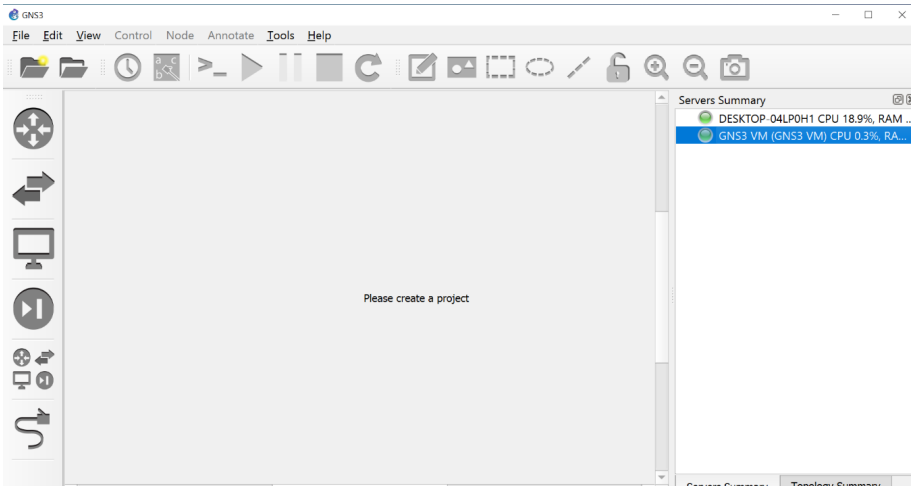

FIGURE 4.5 – Interface de GNS3

Une fois l'installation terminée, nous lançons GNS3 sur notre machine locale pour le configurer et y ajouter les dispositifs requis pour la mise en place de notre infrastructure : des routeurs Cisco ainsi que nos machines virtuelles Ansible et Node1.

4.3.2 Installation de VMware Workstation

Afin de pouvoir héberger plusieurs machines virtuelles pour nos serveurs sur un seul ordinateur, nous devons procéder à l'installation détaillée de VMware Workstation, comme expliqué en annexe. Cette démarche nous permettra d'obtenir à la fin l'interface utilisateur configurée comme illustrée dans la figure ci-dessous : [VMw23]

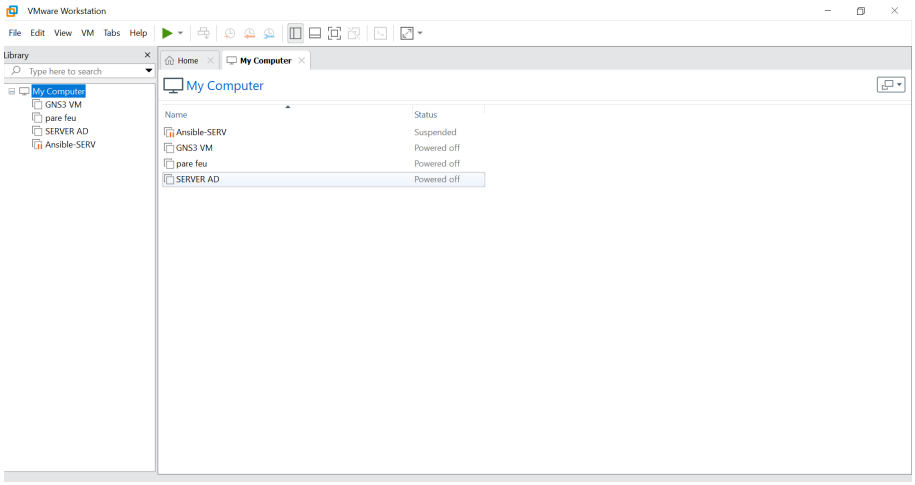

FIGURE 4.6 – Interface de VMWare Workstation version 17

4.3.3 Installation de Windows Server AD

Pour déployer Windows Server 2022, nous débutons par l'intégration de son image dans la machine virtuelle, puis suivons méticuleusement chaque étape jusqu'à l'achèvement du processus d'installation. À la fin, notre objectif est d'accéder à l'interface graphique finale illustrée dans la capture d'écran suivante : [Cor23]

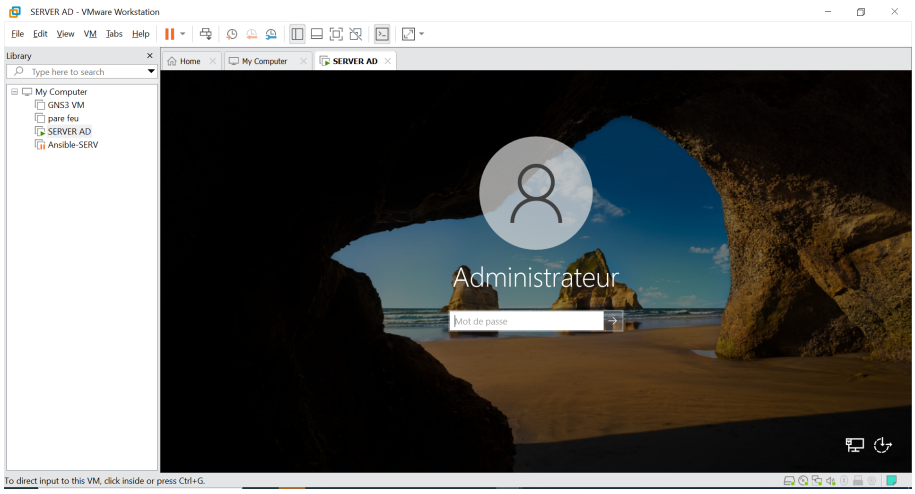

FIGURE 4.7 – Interface de Windows Server AD

4.4 Réalisation de l'architecture réseau

La figure ci-dessous représente l'architecture du réseau que nous avons créépour visualiser notre solution à l'aide du logiciel GNS3, cette configuration est basée sur le DMZ et le serveur AD afin de permettre une meilleure solution de virtualisation. par ailleurs, une configuration des différents équipements a été effectuée.
Le système en question, contient :

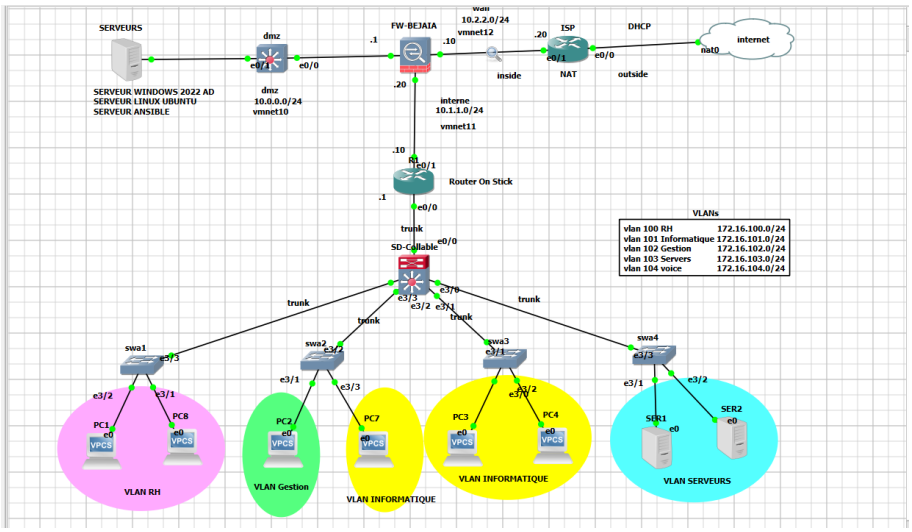

FIGURE 4.8 – Architecture proposée

4.4.1 Attribution des adresses IP aux équipements

Nom de la machine	Interface	Adresse IP	Masque de sous réseau	Passerelle
internat	VMnet11	10.1.1.0	255.255.255.0	10.1.1.1
WAN	VMnet12	10.2.2.0	255.255.255.0	10.2.2.20
DMZ	VMnet10	10.0.0.10	255.255.255.0	10.0.0.1
ISP	F0/0	10.2.2.20	255.255.255.0	/
	F0/1	192.168.122.255	255.255.255.0	/
R1	F0/0	10.1.1.1	255.255.255.0	/
	F0/1	10.1.1.10	255.255.255.0	/
PC1	/	172.16.100.11	255.255.255.0	172.16.100.1
PC2	/	172.16.102.11	255.255.255.0	172.16.102.1
PC3	/	172.16.101.11	255.255.255.0	172.16.101.1
PC4	/	172.16.101.12	255.255.255.0	172.16.101.1
PC5	/	172.16.102.12	255.255.255.0	172.16.102.1
PC6	/	172.16.100.12	255.255.255.0	172.16.100.1

FIGURE 4.9 – Attribution des adresses IP aux équipements

4.5 Installation d'Ansible

Ansible est un outil d'automatisation sans agent que vous installez sur un seul hôte (appelé nœud de contrôle).
À partir du nœud de contrôle, Ansible peut gérer à distance une flotte entière de machines et d'autres appareils (appelés nœuds gérés) avec SSH, Powershell remoting et de nombreux autres transports, le tout à partir d'une simple interface de ligne de commande sans base de données ni démons requis.

4.5.1 Installation des Packages APT

Il est essentiel de mettre à jour et d'installer les packages APT qui nous seront bénéfiques dans nos prochaines opérations lorsque nous commençons sur UBUNTU. La solution de gestion de paquets avancée Advanced Packaging Tool offre une solution de recherche facile et efficace, une installation simple et une désinstallation propre de logiciels et utilitaires .
Il facilite également la mise à jour de la distribution Ubuntu avec les paquets les plus récents et permet de passer à une nouvelle version de Ubuntu, dès qu'elle est accessible.
Les commandes à implémenter pour charger APT se présentent comme suit :

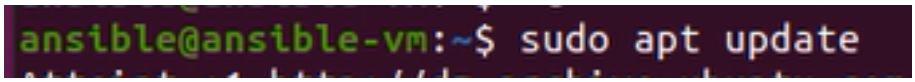

FIGURE 4.10 – Mise a jour système

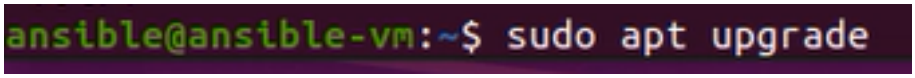

FIGURE 4.11 – Mise a jour l'ensemble des paquet installes sur notre PC

Software Properties Common

C'est un logiciel qui fournit une abstraction des référentiels APT utilisés. Il permet de gérer facilement des sources de logiciels de distribution et de fournisseurs de logiciels indépendants. En pratique, cela signifie qu'il fournit des scripts utiles pour ajouter et supprimer des PPA

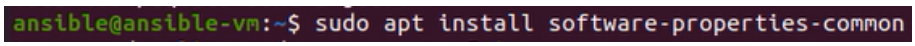

FIGURE 4.12 – Installation de software-properties-common

Personal package archive (PPA)

En utilisant une compilation de packages personnels (PPA), il est envisageable de fournir directement des logiciels et des mises à jour aux utilisateurs d'Ubuntu. La création de notre paquet source, le téléchargement et la création de fichiers binaires par Launchpad, puis leur hébergement dans notre propre référentiel APT.

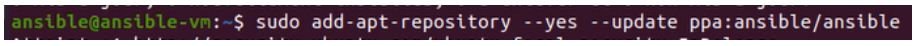

FIGURE 4.13 – Mise a jour de répertoire PPA Ansible

Installation de l'outil Ansible

En utilisant la commande suivante :

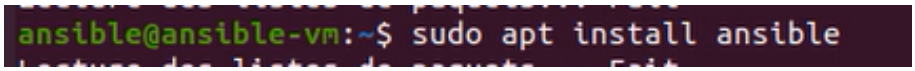

FIGURE 4.14 – Installation complète de ansible

Installation de Python3-PIP

Pip est un système de gestion de paquets utilisé pour installer et gérer des librairies écrites en Python.
Python 3 est installé par défaut dans la distribution Linux Ubuntu. Nous devrons donc installer le paquet python3-pip en utilisant la commande suivante.

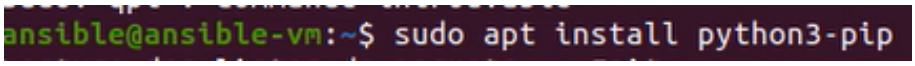

FIGURE 4.15 – Installation de Python3-PIP

La commande pip install argcomplete installe la bibliothèque argcomplete qui améliore l'expérience utilisateur des scripts Python en fournissant la complétion automatique des arguments de ligne de commande. Une fois installée et configurée, elle rend les scripts plus faciles à utiliser et réduit les erreurs de saisie.

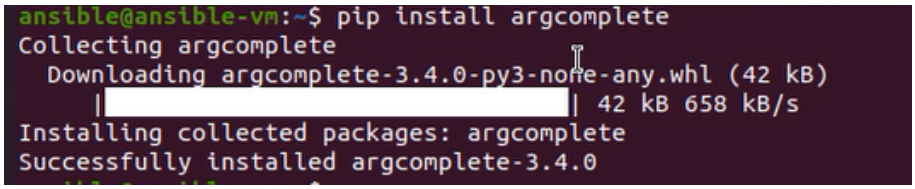

FIGURE 4.16 – Installation le packages argcomplete

4.6 Le protocole Secure ShelI

Le protocole Secure Shell (SSH) est un protocole de réseau cryptographique qui permet d'assurer une communication sécurisée entre deux systèmes sur un réseau non sécurisé. Il est principalement utilisé pour se connecter à des serveurs à distance de manière sécurisée, pour exécuter des commandes et pour transférer des fichiers. [YL06]

4.6.1 Activation du protocole SSH sur les VMs

Pour activer le protocole SSH sur une machine UBUNTU il suffit de télécharger « Open SSH Server », pour cela, nous avons besoin d'une seule commande «sudo apt install openssh-server» comme illustré sur la figure 4.8 , Cette commande sera exécutée sur toutes les machines UBUNTU que nous souhaitons connecter via SSH. cole SSH sur les VMs

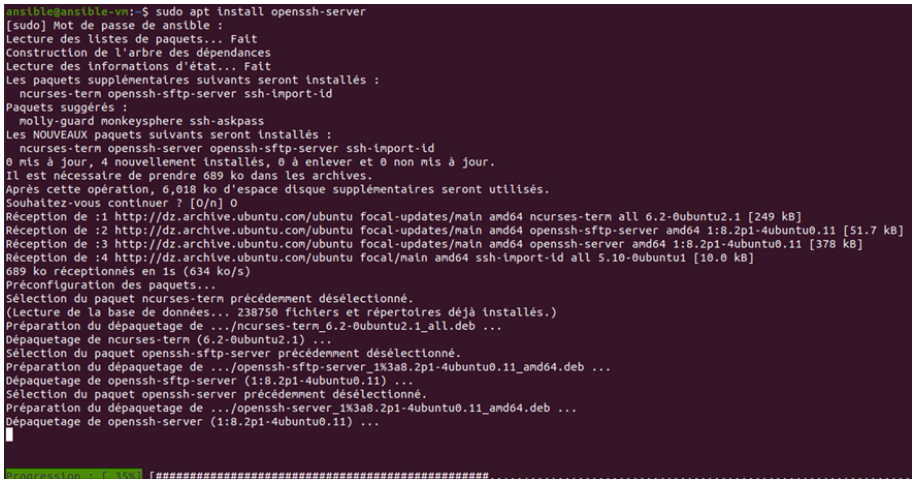

FIGURE 4.17 – Installation de l'open SSH server

4.6.2 SSH User Equivalence

L'objectif de cette configuration est de pouvoir utiliser Ansible via SSH et non pas par password. L'inconvénient de la méthode « password » est que le mot de passe peut être plus difficile à retenir ; lorsqu'on sécurise une session ou une machine d'un réseau privé, on doit créer un mot de passe long et contenant des caractères d'usage inhabituel ce qui fait que l'utilisateur aura du mal à écrire à chaque fois ce mot de passe, de plus c'est une méthode moins sécurisée par rapport au SSH User Equivalence.

4.6.3 SSH User Equivalence

L'objectif de cette configuration est de pouvoir utiliser Ansible via SSH et non pas par password. L'inconvénient de la méthode « password » est que le mot de passe peut être plus difficile à retenir ; lorsqu'on sécurise une session ou une machine d'un réseau privé, on doit créer un mot de passe long et contenant des caractères d'usage inhabituel ce qui fait que l'utilisateur aura du mal à écrire à chaque fois ce mot de passe, de plus c'est une méthode moins sécurisée par rapport au SSH User Equivalence.

4.6.4 Activer SSH sur des routeurs Cisco

Ici nous allons configurer SSH sur nos routeurs, pour cela, nous allons suivre les étapes suivantes :

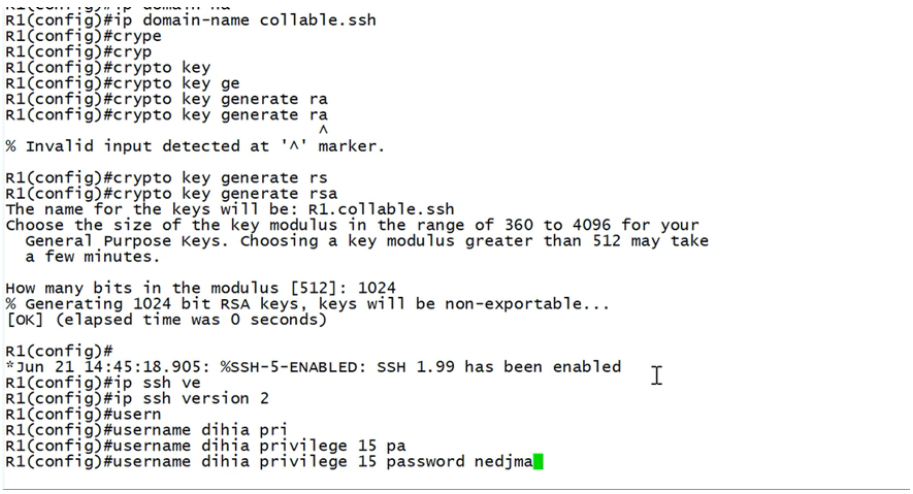

FIGURE 4.18 – Configuration du protocole SSH sur un router Cisco

1. Renommer notre équipement
2. Créer un compte utilisateur avec le mot de passe
3. Définir un nom de domaine
4. Générer les clés « RSA » et choisir le nombre de bits a 1024 (longueur de clés
5. Définir la version SSH que nous allons utiliser
6. Configurer la ligne virtuelle VTY
7. Utiliser le compte utilisateur que nous avons créé
8. Désactiver le protocole Telnet en activant SSH

Les configurations sont montrées sur la figure suivante et doivent être exécutées sur tous les routeurs du réseau.

Testes de connectivité entre la machine Ansible et le router Cisco

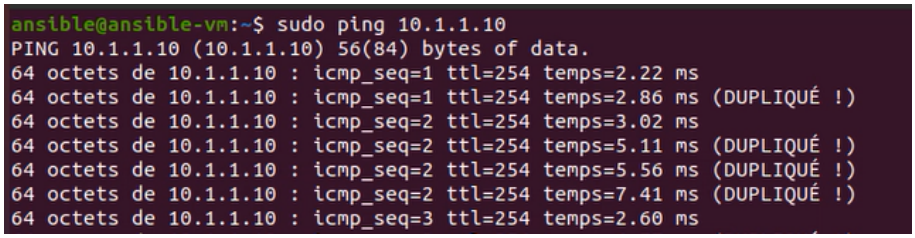

FIGURE 4.19 – Ping entre la machine ansible et le router

4.6.5 Connexion à distance via SSH

Dans notre cas nous avons déjà un « agent SSH » ajouté par défaut par notre système d'exploitation UBUNTU. Il suffit alors d'introduire les commandes comme illustrées sur la figure

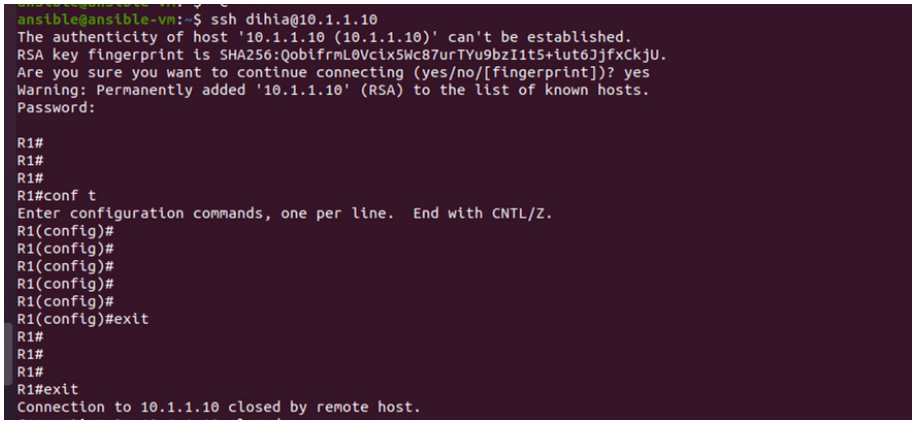

FIGURE 4.20 – Test de connectivité via SSH

Nous avons pu accéder à notre machine via le protocole SSH. Il est important de noter que le serveur demande le mot de passe de l'utilisateur uniquement lors de la première connexion. Par la suite, les connexions peuvent être établies sans mot de passe, à condition que l'authentification par clés SSH soit configurée.

4.6.6 Activer SSH sur DMZ

Pour activer le protocole SSH sur une machine située dans une zone DMZ, voici les étapes générales à suivre :

FIGURE 4.21 – configuration du protocole SSH sur DMZ

Configuration de l'Accès SSH sur un Routeur via les Lignes VTY

Voici une session de configuration sur un routeur Cisco ou similaire où l'on configure l'accès SSH via les lignes VTY (Virtual Teletype). Les lignes VTY sont des interfaces virtuelles qui permettent les connexions telnet ou SSH à distance.

```
dmz(config)#line vty ?
  <0-4>  First Line number

dmz(config)#line vty 0 4
dmz(config-line)#tr
dmz(config-line)#transport in
dmz(config-line)#transport input ssh
dmz(config-line)#login lo
dmz(config-line)#login local
dmz(config-line)#end
dmz#
```

FIGURE 4.22 – Configuration de l'Accès SSH sur un Routeur via les Lignes VTY

Configuration d'une Interface sur le DMZ

La configuration d'une interface VLAN sur un routeur ou un commutateur Cisco :

```
dmz(config)#interface  vlan 1
dmz(config-if)#no shu
dmz(config-if)#no shutdown
dmz(config-if)#ip a
*Jun 21 12:31:28.442: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 21 12:31:29.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to upg
dmz(config-if)#ip add
dmz(config-if)#ip address 10.0.0.3 255.255.255.0
dmz(config-if)#exit
dmz(config)#end
```

FIGURE 4.23 – Configuration d'une Interface

4.6.7 Copie de la clé sur le nœud géré

En premier lieu il est préférable de faire un test de connectivité entre les deux machines en utilisant la commande ping :

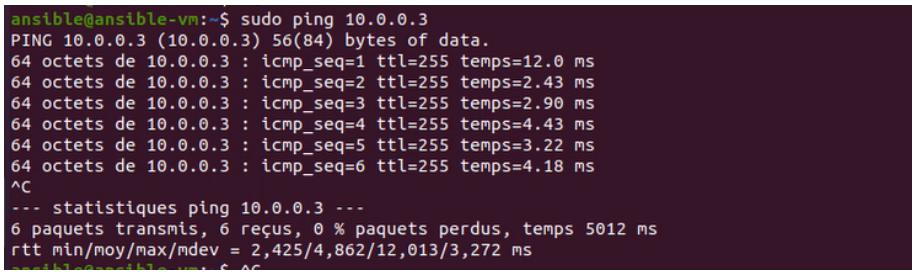

FIGURE 4.24 – Ping entre la machine ansible et DMZ

Gestion des Permissions lors de la Génération des Clés Hôtes SSH et du Redémarrage du Service SSH

Lors de la génération de nouvelles clés hôtes SSH et du redémarrage du service SSH, des problèmes de permissions peuvent survenir, empêchant la sauvegarde des clés générées. ici on illustre la résolution de tels problèmes de permissions.

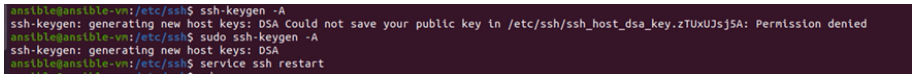

FIGURE 4.25 – Gérer et redémarrer le SSH

4.7 Configurations de base

4.7.1 Configuration de Windows Server

La gestion et la configuration des serveurs Windows nécessitent souvent l'automatisation et le contrôle à distance. PowerShell, avec ses puissantes capacités de scripting, et Windows Remote Management (WinRM), qui permet la gestion à distance des serveurs, sont des outils essentiels pour tout administrateur système.

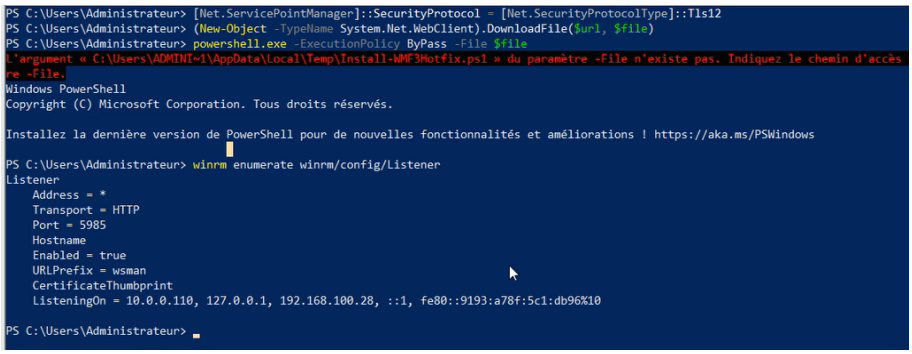

FIGURE 4.26 – Configuration de Windows Server avec PowerShell et WinRM

Étapes Détails

Pour assurer une configuration efficace de Windows Server, vous devez d'abord télécharger et exécuter un script PowerShell, puis configurer WinRM pour permettre la gestion à distance.

Téléchargement et Exécution du Script PowerShell

1. Ouvrez PowerShell en tant qu'administrateur.
2. Configurez le protocole de sécurité pour utiliser TLS 1.2.
3. Téléchargez le script PowerShell à partir d'un URL spécifié.
4. Exécutez le script avec une politique d'exécution qui permet le contournement.

Configuration de WinRM

1. Vérifiez les écouteurs WinRM existants.
2. Configurez de nouveaux écouteurs pour HTTP et HTTPS si nécessaire.
3. Assurez-vous que WinRM est configuré correctement et que les ports nécessaires sont ouverts dans le pare-feu Windows.

4.7.2 Configuration sur le fichier ansible.cfg

Le fichier de configuration par défaut, ansible.cfg, est fourni par l'installation de l'outil Ansible sur le nœud de contrôle situé dans le répertoire actuel. Ce fichier offre la possibilité de changer certains paramètres d'Ansible.

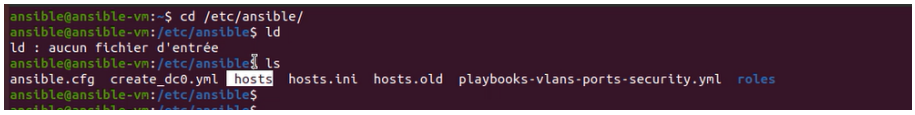

FIGURE 4.27 – Accéder au fichier ansible.cfg

Souvent, la configuration de base est adéquate, mais il est possible que des ajustements des paramètres soient requis pour garantir la connectivité et le bon fonctionnement de l'automatisation.
Le chemin du fichier et la manière d'y accéder en mode super utilisateur (sudo ou root) sont illustrés dans la figure suivante.

Fichiers hosts Le fichier "host" est un fichier important sur les systèmes Linux. Il est utilisé pour mapper les adresses IP aux noms de domaine.

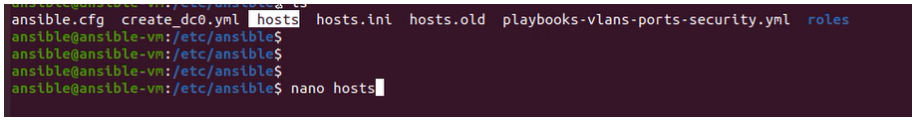

FIGURE 4.28 – Création des fichiers hosts

Ensuite, la déclaration de routeur de switch :

```
[routers]
R1

[switchs]
dmz

[all:vars]
ansible_connection=network_cli
ansible_network_os=ios
ansible_become=yes
ansible_become_method=enable
ansible_become_password=cisco
```

FIGURE 4.29 – La déclaration de routeur de switch

La commande **sudo nano host** peut être utilisée pour éditer le fichier "host" sur un système Linux. Ce fichier est utilisé pour mapper des adresses IP à des noms de domaine. En utilisant la commande "nano host", tu peux ouvrir et modifier ce fichier en utilisant l'éditeur de texte nano directement dans le terminal. Cela te permet de gérer les associations entre adresses IP et noms de domaine sur le système.

```
ansible@ansible-vm:/etc$ sudo nano hosts
```

FIGURE 4.30 – Fichiers modifies

Gestion des Fichiers Modifiés et test de Ping vers DMZ

```
127.0.0.1       localhost
127.0.1.1       ansible-vm

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.0.0.3 dmz
10.1.1.10 R1
```

FIGURE 4.31 – Ping vers DMZ

```
ansible@ansible-vm:/etc$ ping dmz
PING dmz (10.0.0.3) 56(84) bytes of data.
64 octets de dmz (10.0.0.3) : icmp_seq=1 ttl=255 temps=3.43 ms
64 octets de dmz (10.0.0.3) : icmp_seq=2 ttl=255 temps=3.68 ms
64 octets de dmz (10.0.0.3) : icmp_seq=3 ttl=255 temps=3.00 ms
64 octets de dmz (10.0.0.3) : icmp_seq=4 ttl=255 temps=3.68 ms
64 octets de dmz (10.0.0.3) : icmp_seq=5 ttl=255 temps=3.21 ms
64 octets de dmz (10.0.0.3) : icmp_seq=6 ttl=255 temps=4.23 ms
^C
--- statistiques ping dmz ---
6 paquets transmis, 6 reçus, 0 % paquets perdus, temps 5010 ms
rtt min/moy/max/mdev = 2,999/3,537/4,230/0,392 ms
```

FIGURE 4.32 – Modification des hosts

4.8 Création du fichier d'inventaire Ansible

Dans le répertoire « ansible », il faut créer un sous-répertoire « Playbook », celui-ci contiendra le fichier « hosts.yml » ou seront enregistrés nos nœuds .
Un rôle : Un rôle est une structure arborescente constituée de répertoires et de

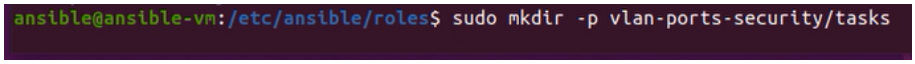

FIGURE 4.33 – Création de répertoire

fichiers de configuration YAML ,qui vont avoir pour fonction d'installer tel ou tel système. Les rôles peuvent être imbriqués et interdépendants" les uns des autres. Un rôle est donc un ensemble de fichiers organisés dans une structure arborescente.
Une tache (task) : Une täche est une instruction décrite en YAML dans un fichier de configuration. Chaque täche utilise un module ainsi que quelques éventuels arguments supplémentaires.

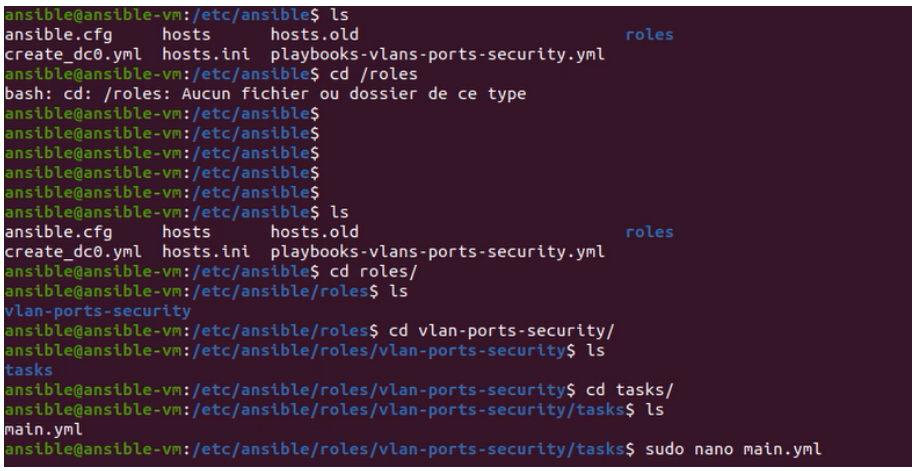

FIGURE 4.34 – Inventaire

mkdir : Cette commande est utilisée pour créer un nouveau répertoire dans le système de fichiers.
ls : La commande ls est utilisée pour lister le contenu des répertoires. Par défaut, elle affiche les noms des fichiers et des répertoires dans le répertoire courant.
nano : Cette commande est un éditeur de texte simple en ligne de commande. Elle est souvent utilisée pour créer de nouveaux fichiers ou modifier le contenu des fichiers texte comme ceux avec l'extension .txt, .ini, .yml, etc.

4.9 Injection des configurations sur les équipements réseau avec Ansible

4.9.1 Création des taches

On a modifier les tasks dans le langage YAML en utilisant la commande suivante :

```
ansible@ansible-vm:/etc/ansible/roles/vlan-ports-security$ cd tasks/
ansible@ansible-vm:/etc/ansible/roles/vlan-ports-security/tasks$ ls
main.yml
ansible@ansible-vm:/etc/ansible/roles/vlan-ports-security/tasks$ sudo nano main.yml
```

FIGURE 4.35 – Modification de tasks

Ensuite, nous avons créé un script pour créer les VLANs en utilisant le site officiel de la documentation d'Ansible :

```
 GNU nano 4.8                                                    main.yml
---
  - name: Configuration du VLAN 10 et 20 sur les switchs
    cisco.ios.ios_vlans:
      config:
        - name: Vlan_10
          vlan_id: 10
          state: active
          shutdown: disabled

        - name: Vlan_20
          vlan_id: 20
          state: active
          shutdown: enabled

        - name: Vlan_30
          vlan_id: 30
          state: suspend
          shutdown: enabled
```

FIGURE 4.36 – Création des vlans pour les interfaces

```
 GNU nano 4.8                                  main.yml                                  Modifié
---
  - name: Configuration du VLAN 10 et 20 sur les switchs
    cisco.ios.ios_vlans:
      config:
        - name: Vlan_10
          vlan_id: 10
          state: active
          shutdown: disabled

        - name: Vlan_20
          vlan_id: 20
          state: active
          shutdown: enabled

        - name: Vlan_30
          vlan_id: 30
          state: suspend
          shutdown: enabled

  - name: Merge provided configuration with device configuration
    cisco.ios.ios_l2_interfaces:
      config:
        - name: Ethernet2/3
          mode: access
          access:
            vlan: 10
          voice:
            vlan: 30
        - name: Ethernet3/0
          mode: trunk
          trunk:
            allowed_vlans: 10,20,40
            native_vlan: 20
            pruning_vlans: 10,20
            encapsulation: dot1q


Nom du fichier à écrire: main.yml
^G Aide                 M-D Format DOS          M-A Ajout (à la fin)    M-B Copie de sécu.
^C Annuler              M-M Format Mac          M-P Ajout (au début)    ^T Parcourir
```

FIGURE 4.37 – Création des vlans pour les interfaces

4.9.2 Structure du Playbook Ansible

Un playbook est structuré comme suit, Un fichier YAML commence toujours par trois tirets :

La première partie du playbook contient :

1. name : Le nom du playbook.
2. hosts : Les machines cibles.
3. gatherfacts : Ce module est utilisé par le playbook pour collecter les variables nécessaires sur les nœuds distants. La valeur booléenne "true" est attribuée lorsque nous voulons qu'Ansible exécute automatiquement les tâches, tandis que "false" est utilisé pour ajouter manuellement les modules.

La deuxième partie concerne les variables utilisées par notre playbook pour accéder aux aux machines cibles via SSH.
La troisième et dernière partie concerne les "tasks", détaillant les différentes tâches exécutées sur les nœuds.

FIGURE 4.38 – Playbook avec tasks

Ensuite, la vérification les pings pour les utilisateurs Cisco :

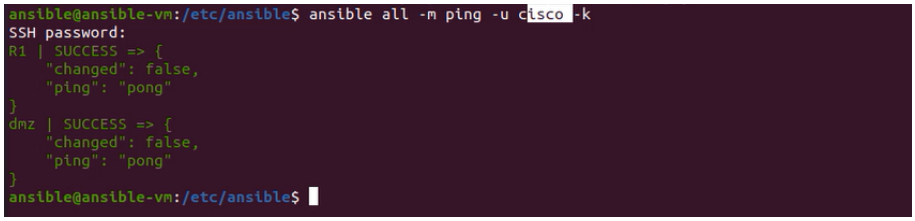

FIGURE 4.39 – Testes de connectivité

4.10 Exécution et résultat du Playbook

Nous déployons le playbook nommé "task.yml" sur un groupe de nœuds spécifiés dans le fichier d'inventaire "cisco", en utilisant la commande ansible-playbook, comme illustré dans la figure ci-dessous :

```
ansible@ansible-vm:/etc/ansible$ ansible-playbook playbooks-vlans-ports-security.yml -u cisco -k
SSH password:
```

FIGURE 4.40 – Commande d'exécution du playbook

Les résultats de cette automatisation apparaissent quelques secondes après l'exécution de la commande dans le terminal de la machine Ansible, comme indiqué dans la figure ci-dessous :

FIGURE 4.41 – Résultats du playbook

Visualisation des VLANs Configurés

L'image ci-dessous montre le résultat de la commande show vlan brief exécutée. Cette commande fournit un aperçu des VLANs configurés, leur statut, ainsi que les ports associés à chaque VLAN :

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et3/1, Et3/2, Et3/3
10   Vlan_10                          active    Et2/3
20   Vlan_20                          act/lshut
30   Vlan_30                          sus/lshut Et2/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
dmz#sho
dmz#show  in
dmz#show  int
dmz#show  interfaces tr
dmz#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        n-isl          trunking      1
Et0/1       desirable        n-isl          trunking      1
Et3/0       on               802.1q         trunking      20

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094
Et3/0       10,20,40

Port        Vlans allowed and active in management domain
Et0/0       1,10
Et0/1       1,10
Et3/0       10

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10
Et0/1       none
Et3/0       none
dmz#
```

FIGURE 4.42 – Visualisation des VLANs Configurés

4.11 Conclusion

En résumé, on peut affirmer que l'objectif initial de ce chapitre a été atteint. Nous avons démontré qu'il était envisageable d'injecter des configurations, d'installer des applications et de gérer le réseau en utilisant l'outil d'automatisation Ansible. L'implémentation des VLANs et la gestion de leur configuration montrent clairement les avantages de l'automatisation dans un environnement réseau.
Ainsi, nous pouvons conclure qu'Ansible représente une excellente solution pour l'automatisation des infrastructures, offrant à la fois simplicité d'utilisation, flexibilité et efficacité. Cela permet non seulement de réduire les erreurs humaines mais aussi d'améliorer la cohérence et la rapidité des déploiements et des configurations réseau.

Conclusion générale

L'essor fulgurant des technologies de l'information et de la communication a profondément modifié le paysage des réseaux informatiques, imposant aux entreprises des défis de gestion toujours plus complexes. Face à ces défis, l'automatisation des réseaux est devenue une nécessité incontournable pour garantir une gestion efficace, flexible et réactive des infrastructures. Dans ce cadre, ce mémoire a exploré l'application d'Ansible, un outil d'automatisation sans agent, au sein de l'infrastructure réseau de Campus NTS à Béjaïa.

En utilisant Ansible, nous avons montré comment cette plateforme peut simplifier la gestion, la configuration et l'orchestration des infrastructures réseau, tout en répondant aux besoins spécifiques d'une organisation moderne. Ansible se distingue par sa facilité d'implémentation et sa capacité à opérer sans l'installation d'agents sur les systèmes cibles, ce qui en fait un choix particulièrement adapté pour les environnements diversifiés et complexes.

Nous avons commencé notre étude par une exploration des fondamentaux des réseaux informatiques. Cette analyse comprenait une vue d'ensemble des types de réseaux et de leurs topologies, ainsi qu'une étude des modèles OSI et TCP/IP, qui sont essentiels pour comprendre les mécanismes de communication réseau. Nous avons également abordé les aspects critiques de la sécurité réseau, soulignant les défis constants que les entreprises doivent relever pour protéger leurs données et leurs services.

Par la suite, nous avons procédé à une analyse comparative des solutions d'automatisation des réseaux, en nous focalisant sur Ansible, Puppet et Chef. Ansible a émergé comme l'outil le plus adapté à notre projet, grâce à sa simplicité d'utilisation, sa flexibilité et sa capacité à s'intégrer facilement dans des environnements existants. Ce choix a été justifié par la nécessité de répondre de manière efficace aux exigences spécifiques de Campus NTS.

La présentation détaillée de l'organisation et de l'architecture réseau de Campus NTS a fourni le contexte nécessaire pour comprendre les besoins en automatisation de l'entreprise. Nous avons illustré comment Ansible peut être utilisé pour automatiser des tâches variées, allant de la gestion de la configuration à l'orchestration de déploiements complexes.

À travers nos simulations, nous avons démontré les avantages tangibles de l'utilisation d'Ansible : une gestion plus efficiente des ressources, une réduction significative du temps et des efforts nécessaires pour les opérations courantes, et une amélioration globale de l'agilité opérationnelle de Campus NTS. Ces résultats soulignent non seulement l'efficacité d'Ansible en tant qu'outil d'automatisation des réseaux, mais aussi son potentiel pour transformer la manière dont les entreprises gèrent leurs infrastructures informatiques.

En conclusion, ce mémoire met en évidence l'importance cruciale de l'automatisation des réseaux dans un monde de plus en plus connecté et complexe. Ansible, avec ses caractéristiques uniques et ses capacités robustes, représente une solution puissante pour les entreprises cherchant à optimiser leurs opérations et à se préparer aux défis futurs. L'expérience acquise à travers ce projet nous offre des perspectives prometteuses pour l'expansion et l'amélioration continue des pratiques d'automatisation au sein de Campus NTS et au-delà.

Annexe A

Installation de GNS3

A.1 Téléchargement du fichier GNS3 Client

Pour procéder à l'installation de GNS3, le premier pas consiste à télécharger le fichier client depuis le site officiel de GNS3.

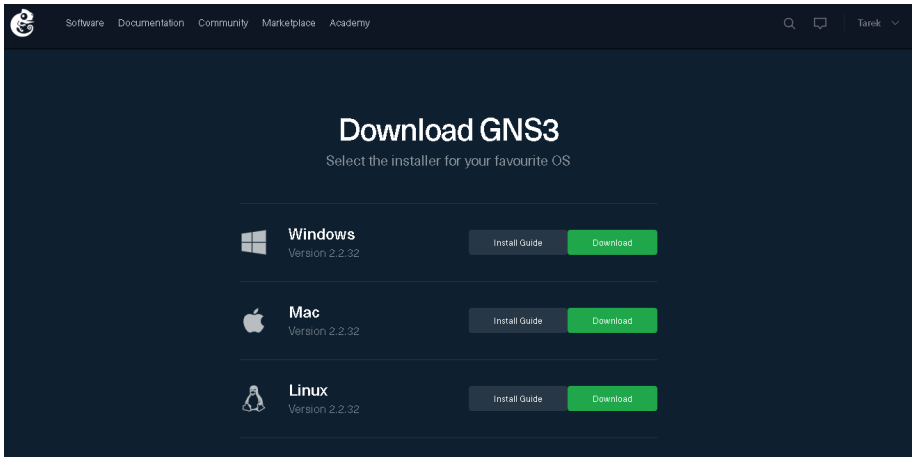

FIGURE A.1 – Téléchargement du fichier GNS3 Client

A.2 Installation de GNS3 Client

Sous Windows, l'installation de GNS3 est généralement simple et directe. Après avoir lancé le programme d'installation, la fenêtre de configuration s'affiche. Les instructions ont été suivies pas à pas, comme décrit ci-dessous :

FIGURE A.2 – Installation de GNS3 Client -1-

Préférant laisser toutes les options cochées, toutes les mises à jour nécessaires pour les logiciels sont effectuées automatiquement. En cliquant sur "Suivant", l'assistant d'installation demande d'accepter les conditions d'utilisation.

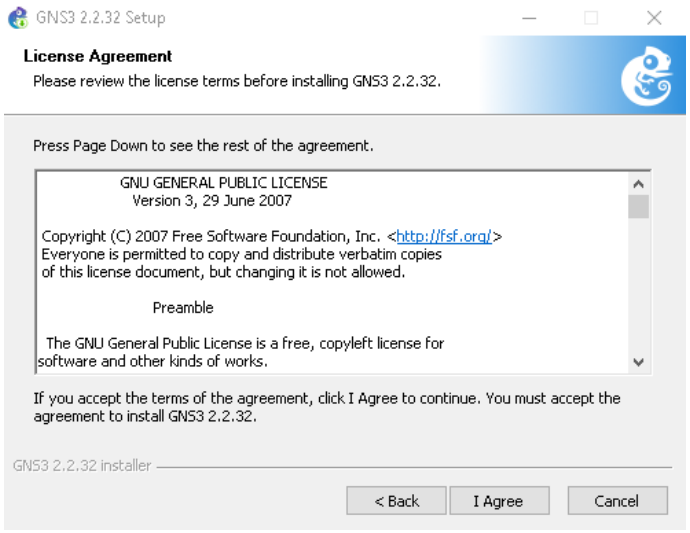

FIGURE A.3 – Installation de GNS3 Client -2-

Après avoir modifié le chemin d'installation du fichier, cliquez sur "Installer". Ensuite, vous devrez choisir le type de GNS3 VM :

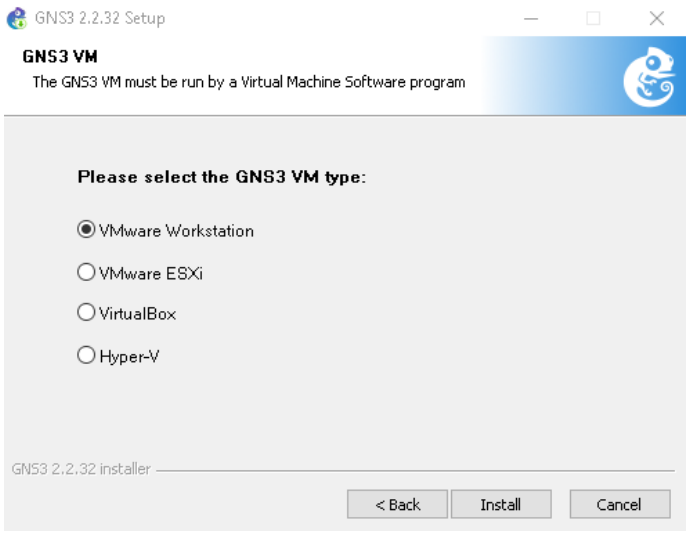

FIGURE A.4 – Installation de GNS3 Client

Une fois l'installation complétée, l'application démarre automatiquement :

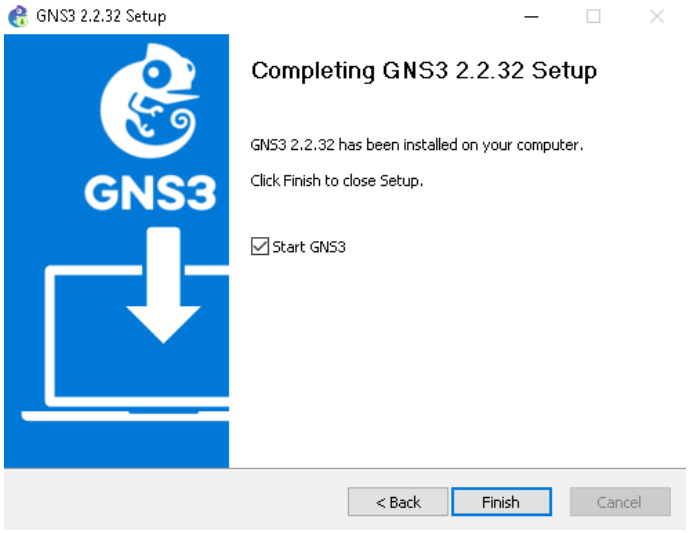

FIGURE A.5 – Téléchargement du fichier GNS3 Client

A.3 Importation de GNS3 VM dans VMware

Une fois le fichier téléchargé, je l'ai importé dans l'outil de virtualisation. Après l'avoir décompressé pour obtenir un fichier .ova, j'ai ouvert VMWare Workstation, déjà installé sur l'ordinateur. Ensuite, j'ai sélectionné le fichier .ova en utilisant les options "File" > "Open".

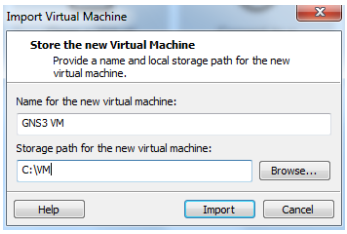

FIGURE A.6 – Importation de GNS3 VM dans VMware

A.4 Liaison entre GNS3 VM et GNS3 Client

Lors du lancement du client GNS3, l'assistant d'installation a affiché une fenêtre où l'option "Run modern IOS (IOSv or IOU), ASA and Appliance from Cisco manufacturers" a été sélectionnée, puis "Next" a été cliqué.

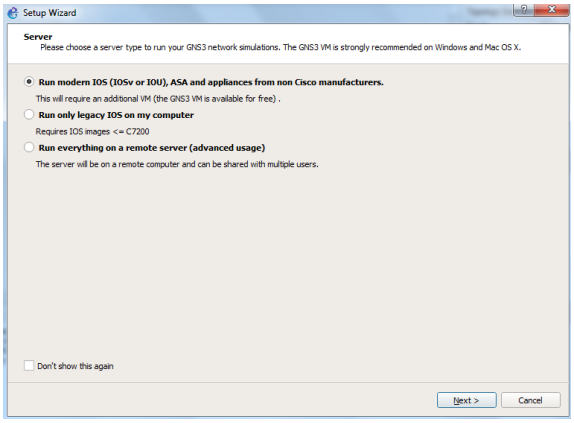

FIGURE A.7 – Intégration de GNS3 VM avec GNS3 Client -1-

Dans la fenêtre suivante, l'IP de l'interface réseau connectée à la VM a été sélectionnée dans « Host binding » :

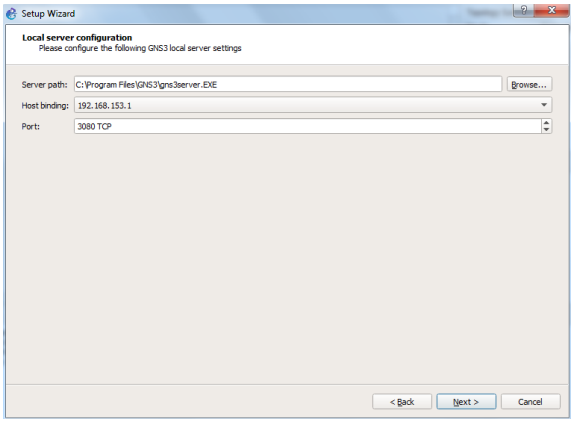

FIGURE A.8 – Intégration de GNS3 VM avec GNS3 Client -2-

La plateforme de virtualisation VMware a été sélectionnée. Ensuite, la fenêtre récapitulative de la configuration s'est présentée :

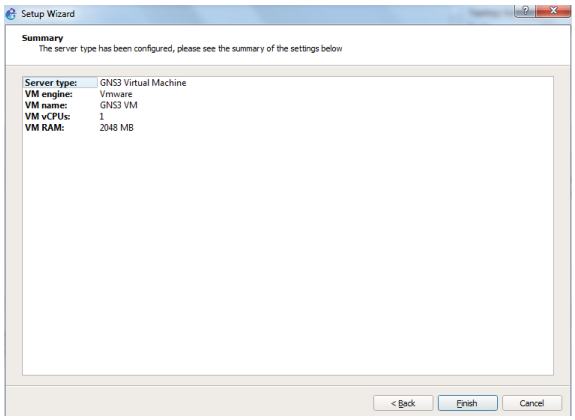

FIGURE A.9 – Intégration de GNS3 VM avec GNS3 Client -3-

A.5 Importation des images IOS

Pour télécharger les images IOS, il est nécessaire d'avoir un numéro de contrat renseigné sur votre compte, qui inclut l'équipement dont vous souhaitez télécharger l'IOS.
Dans notre cas, nous avons déjà en notre possession les images IOS des routeurs Cisco 3725 et Cisco 7200, que nous importerons dans notre GNS3 Client. Nous avons utilisé l'IOS du routeur Cisco 7200 comme illustration pour l'importation.
Après avoir cliqué sur "Edit" puis sur "Preferences..." dans le client GNS3, sélectionnez "IOS routers", puis cliquez sur "New" :

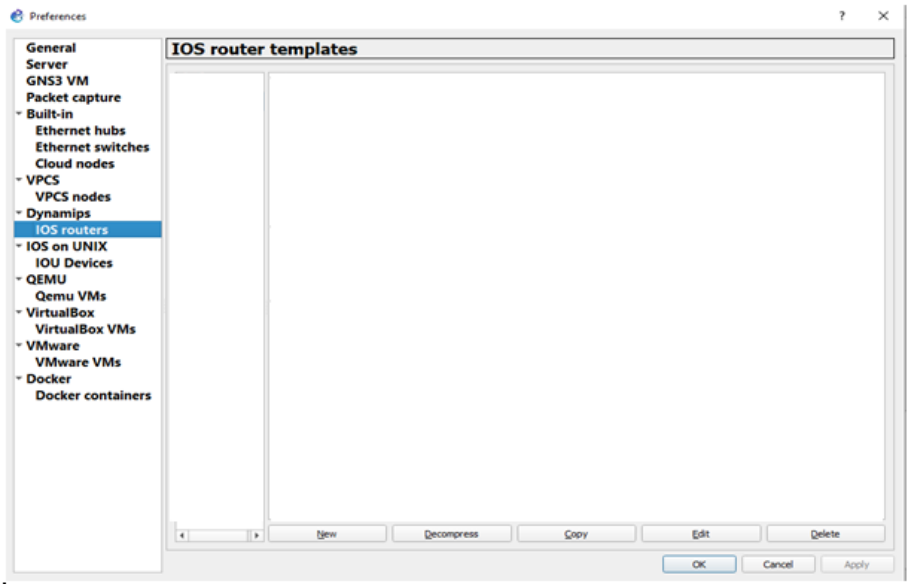

FIGURE A.10 – Importation des images IOS -1-

Dans la fenêtre suivante, l'option « Run this IOS router on my local computer » a été sélectionnée. Cette option permet d'utiliser le routeur IOS localement, même si l'environnement virtuel est désinstallé, bien qu'elle nécessite un espace de stockage sur l'ordinateur local. Ensuite, cliquez sur « Next ».

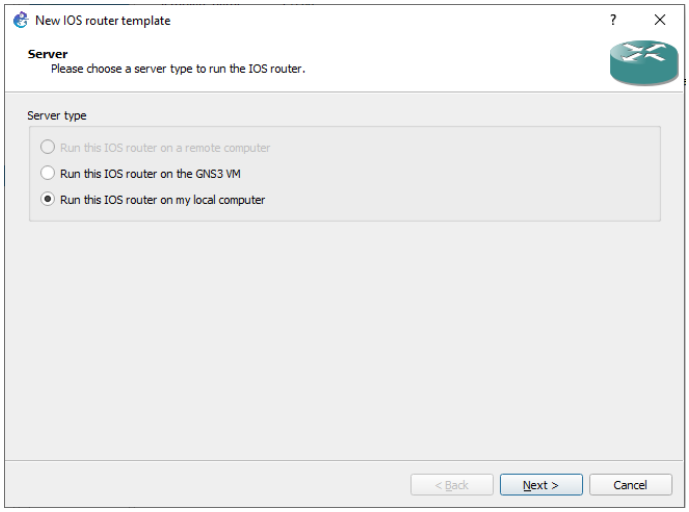

FIGURE A.11 – Importation des images IOS -2-

Ensuite, dans la fenêtre suivante, sélectionnez « New Image », puis cliquez sur « Browse... ». Naviguez pour choisir l'IOS téléchargé précédemment et cliquez sur « Ouvrir ».
Une fois l'IOS sélectionné, une série d'options de personnalisation s'ouvre. Il est possible de configurer la quantité de RAM, les adaptateurs réseau, les modules WIC, et d'autres paramètres spécifiques au routeur. Après avoir défini ces paramètres selon les besoins, cliquez sur « Finish » pour finaliser l'importation du routeur dans GNS3.

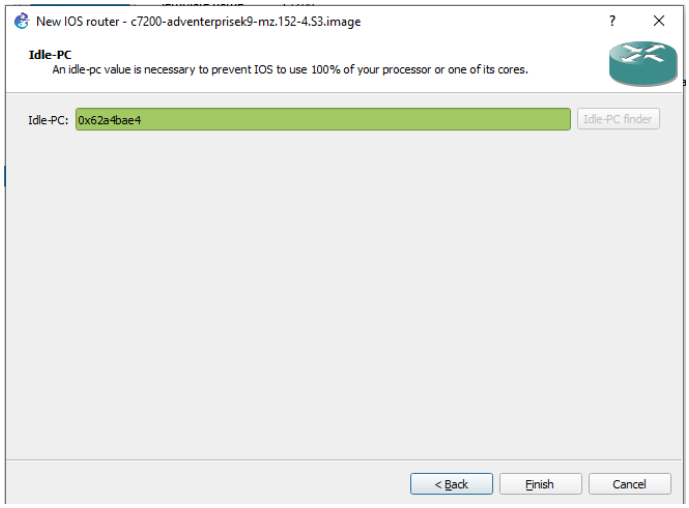

FIGURE A.12 – Importation des images IOS -3-

Vérification et test

Afin de vérifier que nos équipements ont bien été créés, nous avons cliqué sur l'icône du routeur et vérifié qu'ils sont apparus dans la liste. besoins, cliquez sur « Finish » pour finaliser l'importation du routeur dans GNS3.

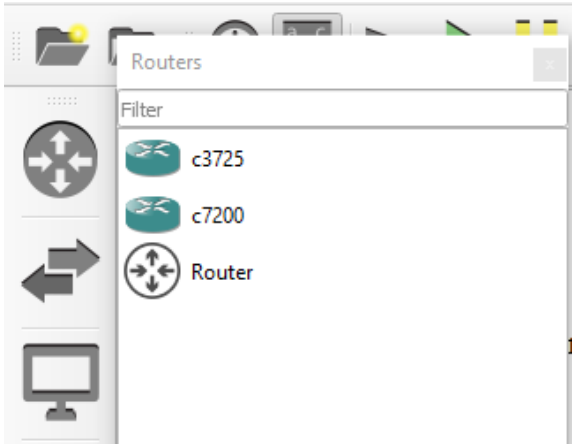

FIGURE A.13 – Vérification et test c7200

Bibliographie

[YL06] T. Ylonen et C. Lonvick. *The Secure Shell (SSH) Protocol Architecture*. Internet Engineering Task Force, 2006.

[Don11] Gary A Donahue. *Network Warrior*. 2nd. Sebastopol : O'Reilly Media, 2011.

[TW11] Andrew S. Tanenbaum et David J. Wetherall. *Computer Networks*. 5th. Boston : Pearson, 2011.

[PB13] Jean-François Pillou et Jean-Philippe Bay. *Sécurité informatique*. 3e. Paris : Dunod, 2013.

[SB15] John Smith et Jane Brown. « Cybersecurity Challenges in a Digital World ». In : *Proceedings of the 10th International Conference on Cybersecurity*. ACM. 2015, p. 100-110.

[All17] Neal Allen. *Network Maintenance and Troubleshooting Guide*. 2nd. Indianapolis : Cisco Press, 2017. isbn : 978-1-58714-431-3.

[LT17] Mischa Taylor Lau et Tina. *Learning Chef : A Guide to Configuration Management and Automation*. Sebastopol : O'Reilly Media, 2017. isbn : 978-1-491-95010-8.

[Wel17] Chris Welch. *Mastering GNS3*. Packt Publishing, 2017. isbn : 978-1788399128.

[Smi18] John Smith. *Automation in Network Management : Principles and Practice*. New York : TechPress, 2018. isbn : 978-1-234-56789-0.

[Lin20] D. Lindberg. *Mastering pfSense : A Comprehensive Guide to pfSense for Network Security*. Packt Publishing, 2020. isbn : 978-1789801934. url : https://www.packtpub.com/product/mastering-pfsense/9781789801934.

[Sta20] William Stallings. *Network Security Essentials : Applications and Standards*. 6th. Boston : Pearson, 2020. isbn : 978-0-13-453924-9.

[LK21] T. Larsen et S. Kalvala. « DevOps Tools and Automation : A Survey ». In : *Journal of Software Engineering* 19.3 (2021), p. 245-258.

[RO21] A. Rocha et T Oliveira. *Network Automation at Scale with NetDevOps*. Sebastopol : O'Reilly Media, 2021. isbn : 978-1-098-10237-8.

[Cor23] Microsoft Corporation. *Windows Server Documentation*. Microsoft, 2023. url : https://docs.microsoft.com/en-us/windows-server/.

Webographie

[Doc21] Puppet Documentation. *Puppet Enterprise User Guide*. Accessed : 2024-06-22. 2021. URL : https://www.puppet.com/docs/pe/2021.7/pe_user_guide.html.

[Bom23] David Bombal. *GNS3 Tutorials and How-To Videos*. Available at : https://www.youtube.com/user/ConfigByte. 2023. URL : https://www.youtube.com/user/ConfigByte.

[Cyb24] Orange Cyberdefense. *Vulnérabilités, de quoi parle-t-on ?* 2024. URL : https://www.orangecyberdefense.com/fr/insights/blog/gestion-des-vulnerabilites/vulnerabilites-de-quoi-parle-t-on (visité le 24/05/2024).

[Doc24] Ansible Documentation. *Ansible Documentation*. Accessed : 2024-06-22. 2024. URL : https://docs.ansible.com/.

[Gof24] Linux Goffinet. *Présentation du produit Ansible*. 2024. URL : https://linux.goffinet.org/ansible/presentation-produit-ansible/ (visité le 14/04/2024).

[Hat24] Red Hat. *Virtualization*. 2024. URL : https://www.redhat.com/fr/topics/virtualization (visité le 21/05/2024).

[Ins24] Infosec Institute. *VLAN Network - Chapter 5*. 2024. URL : https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/ (visité le 25/02/2024).

[O0024] O00o.org. *Monitoring Solutions*. 2024. URL : http://www.o00o.org/monitoring/solutions.html (visité le 21/05/2024).

[24] *Tout sur la sécurité informatique*. 2024. URL : https://www.pdfdrive.com/tout-sur-la-s%C3%A9curit%C3%A9-informatique-e186515890.html (visité le 07/02/2024).

[Ver24] Veritis. *Comparaison Chef vs Puppet vs Ansible*. 2024. URL : https://www.veritis.com/blog/chef.ys-puppet.vs.ansible-comparisan.of (visité le 23/03/2024).

[Sta] International Organization for Standardization (ISO). *ISO/IEC 27001 :2013 Information security management systems – Requirements*. URL : https://www.iso.org/fr/standard/80585.html (visité le 13/05/2024).

Résumé

Ce mémoire explore l'importance croissante de l'automatisation des réseaux dans les environnements informatiques modernes, en se concentrant sur l'application d'Ansible au sein de l'infrastructure réseau de Campus NTS à Béjaïa. Ansible se distingue par sa simplicité d'utilisation et sa capacité à orchestrer efficacement les déploiements sans nécessiter l'installation d'agents sur les systèmes cibles. À travers une étude approfondie des fondamentaux des réseaux informatiques et une analyse comparative des outils d'automatisation, ce mémoire démontre comment Ansible répond spécifiquement aux besoins de gestion et de flexibilité de Campus NTS. Cette approche a permis non seulement d'améliorer l'efficacité opérationnelle et la sécurité, mais aussi de préparer l'entreprise aux défis technologiques à venir.

Abstract

This thesis explores the growing importance of network automation in modern IT environments, focusing on the application of Ansible within the network infrastructure of Campus NTS in Béjaïa. Ansible stands out for its ease of use and its ability to effectively orchestrate deployments without requiring the installation of agents on target systems. Through an in-depth study of computer network fundamentals and a comparative analysis of automation tools, this thesis demonstrates how Ansible specifically meets the management and flexibility needs of Campus NTS. This approach has not only improved operational efficiency and security, but also prepared the organization for future technological challenges.