République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou

Faculté De Génie Electrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes de

MASTER ACADEMIQUE

Spécialité :

Réseaux & Télécommunications

Filière :

Télécommunications

Par
BEN MEDJEBER Lounas
FALI Amel

Thème

Conception et implémentation d'une solution d'automatisation de migration des services réseaux avec un accès distant sécurisé

Soutenu le : 26/06/2024

Devant le jury :

Présidente :	Mme. BOUALLEG Samira	MCB	UMMTO
Promoteur :	Mr. BACHIR M'hamed Saadi	MCB	UMMTO
Co-promoteur :	Mr. MEDDANE Redouane	Consultant	MICROTEL
Co-promoteur :	Mr. DJEBBARI Mohamed lamine	Consultant	MICROTEL
Examinateurs :	Mme. BOUSSOUM Ouiza	MCB	UMMTO

Remerciement

Au terme de ce travail, nous souhaitons tout d'abord exprimer notre profonde gratitude au Tout-Puissant Allah, le Créateur de toutes choses, pour nous avoir accordé la vie, les bénédictions et la force nécessaires à l'accomplissement de cette tâche.

Nous adressons nos sincères remerciements à Madame la Présidente du jury ainsi qu'aux membres du jury pour avoir accepté d'évaluer notre travail et pour le partage généreux de leurs précieuses connaissances.

Nous exprimons notre immense gratitude à notre promoteur, Monsieur Bachir, dont les efforts, la patience et les judicieux conseils ont été d'une importance capitale dans l'élaboration de notre réflexion.

Nos remerciements vont également à nos Co-encadrants, Monsieur Redouane Meddane, Monsieur Mohamed Lamine Djebbari, Madame Sara Bediaf.

Monsieur Djebbari Mohamed Lamine a fait preuve d'une grande patience et d'un engagement remarquable, nous offrant son soutien à toute heure. Nous le remercions pour ses conseils avisés, les informations et formations qu'il nous a prodigués, ainsi que pour le courage qu'il nous a insufflé pour continuer d'avancer et d'acquérir de nouvelles connaissances.

Grâce à Monsieur Meddane, nous avons eu l'opportunité d'effectuer un stage enrichissant au sein d'une grande entreprise, où il a mis à notre disposition tous les matériels nécessaires ainsi que de nombreuses informations et formations. Sa patience et ses encouragements ont été inestimables.

Nous tenons également à remercier Madame Sara Bediaf pour son aide précieuse durant cette période, ainsi que pour les efforts et les formations qu'elle nous a dispensés.

Nos remerciements s'adressent également à l'ensemble des enseignants et à toutes les personnes ayant contribué à notre formation.

Enfin, nous exprimons notre gratitude à toutes les personnes, de près ou de loin, dont les contributions ont rendu possible la réalisation de ce projet.

Dédicaces

Je dédie ce travail a

À mes chers parents, Avec tout mon amour et ma gratitude. Vous avez toujours été là pour moi, me soutenant et m'encourageant dans toutes mes épreuves. Vous avez sacrifié tant de choses pour me garantir une meilleure situation. Je vous exprime ici toute ma reconnaissance. Vous êtes les meilleurs parents du monde, et je vous serai éternellement reconnaissante. Que cette dédicace soit l'expression de mon amour infini pour vous.

À mes chères sœurs, cher frère et beau-frère, Kenza Imène, Mounia, Mélissa, Ryma, Youcef et Omar vos encouragements et votre présence ont été un phare dans les moments sombres, votre confiance en moi m'encourage à poursuivre mes objectifs, Vous êtes mes compagnons de vie et mes plus grands soutiens, merci d'être la meilleure famille que l'on puisse avoir.

Je dédie ce mémoire à mes chers et meilleurs amis Sofiane, Juba Dahmani, Rayane, Amel, Juba, Mehdi et sa femme Asma ainsi qu'à leur petit bébé, Assia, Naoual, Cirta, Mamah, Lina.

Mes instructeurs, Mr Meddane, Mr Djebbari et Mlle Bediaf, Je vous dédie cette œuvre avec une profonde gratitude. Grâce à vous, nous sommes arrivés jusqu'ici. Votre guidance, vos précieux conseils et votre soutien ont été essentiels à notre réussite. Ce projet est le fruit de nos efforts collectifs et de votre expertise. Merci pour votre dévouement et votre engagement tout au long de ce parcours. Votre contribution a été indispensable à notre apprentissage et à notre développement professionnel. Vous êtes des instructeurs exceptionnels et formidables.

A Mon Binôme, Lounas merci pour ton énorme soutien, notre collaboration a été précieuse et efficace, notre succès est le fruit de notre partenariat solide et de notre engagement mutuel.

À ma très chère Tata Fella, à Tonton Karim et à leurs petits-enfants, je vous dédie ce travail Grâce à toi tata, nous avons fait des rencontres en or, tout comme toi.

À mes chers neveux Racha, Melina et Hichem, vous apportez lumière et joie à ma vie chaque jour. Vos sourires et rires sont une source constante d'inspiration et de bonheur.

À tous ceux qui m'ont soutenu et cru en moi, je dédie ce travail avec gratitude. Merci pour votre confiance et votre encouragement tout au long de ce parcours.

Dédicaces

Je dédie ce mémoire de fin d'études à

Mes parents, pour leur amour inconditionnel, leur soutien constant et leurs sacrifices, qui m'ont permis de réaliser mes rêves et d'atteindre ce jalon important. Leur confiance en moi et leur encouragement ont été des sources inépuisables de motivation.

Mon grand frère, **Massinissa** à qui je dédie ce mémoire de fin d'études en signe de gratitude et de reconnaissance pour ton soutien indéfectible. Ton encouragement constant, tes conseils avisés et ta confiance en mes capacités ont été des piliers essentiels de ma réussite. Tu as toujours été un modèle d'inspiration et de persévérance, me montrant par l'exemple que tout est possible avec détermination et travail acharné.

Mes professeurs et encadrants, pour leur guidance précieuse, leur expertise partagée et leur dévouement. Leur passion pour l'enseignement et leur engagement envers notre réussite académique ont été des inspirations constantes.

Mes instructeurs, Mr Meddane, Mr Djebbari et Mlle Bediaf Je vous dédie ce mémoire de fin d'études en signe de profonde gratitude et de reconnaissance pour votre travail acharné et votre dévouement. Votre engagement sans relâche, vos conseils éclairés et votre patience ont été essentiels à ma réussite. Vous avez su me guider, m'encourager et me pousser à donner le meilleur de moi-même. Merci pour votre soutien constant et votre disponibilité. Votre passion pour l'enseignement et votre souci de la réussite de vos étudiants m'ont profondément inspiré. Ce mémoire est autant le fruit de votre travail que du mien.

Ma binôme, Amel Merci pour ta collaboration et ton soutien indéfectible tout au long de ce projet. Ce mémoire est le fruit de notre travail acharné et de notre esprit d'équipe.

Mes amis, **Said, Nasser, Sidali, Nassim, Merzouk, Takfarinas, Djahid, Rania et Cherifa** pour leur soutien moral, leurs encouragements et les moments de détente partagés qui ont équilibré les périodes de travail intense. Leur amitié sincère a enrichi cette aventure académique.

Enfin, je dédie ce mémoire à tous ceux qui ont cru en moi et m'ont soutenu d'une manière ou d'une autre tout au long de mon parcours académique. Leur contribution, qu'elle soit grande ou petite, a été précieuse et inestimable.

Table des matières

Chapitre II Étude et spécification des besoins

Chapitre III Conception de la solution

Chapitre IV Implémentation de la solution

Conclusion Générale

Liste des tableaux

Liste des figures

Acronymes

Acronyme	Signification
AAA	Authentication Authorization Accounting
ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
ADCS	Active Directory Certificate Services
ADDS	Active directory Domain System
ADFS	Active Directory Federation Services
ADLDS	Active Directory Lightweight Directory Services
ADRMS	Active Directory Rights Management Services
ASA	Adaptive Security Appliance
CD-ROM	Compact Disc Read Only Memory

CLI	Command Line Interface
CMD	Command Prompt
DACL	Discretionary Access Control List
DC	Domain Contrôleurs
DCUI	Console Directed User Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRS	Distributed Resource Scheduler
FMC	Firepower Management Center
FQDN	Fully Qualified Domain Name
FTP	File Transfert Protocol
FTPS	File Transfer Protocol Secure
FTD	Firepower Threat Defense
GPO	Groupe Policy
HA	High Avaibility
HCI	Human Computer Interaction
HR	Human Ressources
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAAS	Infrastructure As A Service
IIS	Internet Information Services
IP	Internet Protocol
IPS	Internet Protocol Security
ISE	Identity Services Engine
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MAN	Metropolitain Area Network
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
NTP	Ntework Time Protocol
OS	Operating System

PAAS	Platform As A Service
PAN	Personnal Area Network
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
SAAS	Software As A Service
SAN	Storage Area Network
SCSI	Small Computer System Interface
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
TCP	Transport Control Protocol
TELNET	Teletype Network
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VCSA	Virtual Center Server Appliance
VDS	Virtual Distributed Switch
VLAN	Virtual Local Area Network
VNIC	Virtual Network Interface Card
VM	Virtual Machine
VMCP	Virtual Machine Component Protection
VPN	Virtual Private Network
VSAN	Virtual Storage Area Network
VSS	Virtual Standard Switch
WAN	Wide Area Network

Mots clés

Virtualisation la virtualisation est une technique permettant de créer des environnements informatiques simulés à partir d'une seule infrastructure physique, améliorant l'efficacité et la gestion des ressources.

Data Center un datacenter est une installation dédiée à héberger des systèmes informatiques et leurs composants, tels que des serveurs, des dispositifs de stockage et des équipements réseau, assurant la gestion et la sécurité des données critiques.

Services réseaux les services réseaux sont des fonctionnalités fournies par des infrastructures de réseau pour assurer la communication, la gestion des données et le support applicatif, incluant des services comme le DNS, DHCP et les pare-feu.

Automatisation l'automatisation est le processus de rendre les systèmes, les tâches ou les processus opérationnels autonomes à l'aide de technologies et de logiciels, réduisant ainsi l'intervention humaine et améliorant l'efficacité.

Migration la migration est le processus de déplacement de données, d'applications ou d'infrastructures d'un environnement à un autre, souvent pour des raisons de mise à niveau, de consolidation ou d'optimisation des ressources.

Sécurité la sécurité est la protection des systèmes, des réseaux et des données contre les accès non autorisés, les attaques, les dommages ou les pertes, garantissant ainsi leur confidentialité, intégrité et disponibilité.

Serveur Radius est un serveur d'authentification centralisée qui vérifie les identités des utilisateurs et gère les autorisations d'accès aux ressources réseau.

Accès distant l'accès distant permet aux utilisateurs de se connecter et d'interagir avec des systèmes informatiques ou des réseaux à distance, en utilisant des technologies telles que VPN ou des logiciels de bureau à distance, pour faciliter le travail hors site et la gestion à distance.

Introduction Générale

Dans le cadre de ce projet, nous explorons l'automatisation de la migration et la haute disponibilité des machines virtuelles et des services réseaux. Ces éléments sont devenus essentiels pour répondre aux exigences croissantes des entreprises modernes. Notre approche innovante combine une stratégie de virtualisation avec une infrastructure matérielle robuste, garantissant une disponibilité maximale des services et une gestion agile des ressources.

Nous avons conçu une solution qui virtualise les ressources RAM et CPU, intégrant une couche de stockage pour créer une infrastructure hyperconvergée et un cloud privé au sein d'un data center. Cette configuration permet la migration automatisée des machines virtuelles et assure la continuité des services en cas de panne, répondant ainsi aux besoins de haute disponibilité.

La sécurité et l'accès à distance occupent également une place centrale dans notre projet. Nous avons intégré des réseaux privés virtuels (VPN) et une gestion centralisée des identifiants utilisateurs via un serveur RADIUS, en coordination étroite avec le pare-feu CISCO ASA. Cette intégration souligne l'importance de la protection des données et des communications dans un environnement de plus en plus interconnecté.

Pour mener à bien ce projet, nous avons approfondi nos connaissances dans divers domaines, notamment la virtualisation, le stockage, les réseaux, la sécurité, l'automatisation et la migration. Nous avons également étudié les technologies les plus avancées du moment et mis en place une plateforme de tests regroupant toutes ces technologies pour atteindre les résultats escomptés.

Chapitre I
Administration des services réseaux

I. Introduction

Dans un monde où la connectivité et la sécurité des réseaux revêtent une importance capitale, les réseaux sont élaborés selon une architecture exclusivement physique, Ces structures intègrent des éléments tels que des serveurs en tant qu'entité unique dédiée à un service spécifique entraînant des performances limitées et des pertes de performances et d'argents.

C'est à ce stade que la virtualisation des infrastructures se positionne comme un pilier essentiel pour répondre aux besoins croissants des entreprises en matière d'efficacité opérationnelle et de gestion des ressources. En nous permettant la création d'environnements informatiques virtuels

Dans la première partie de ce premier chapitre, nous exposons les concepts fondamentaux des réseaux informatiques et de connectivité, ainsi que de la virtualisation, du Cloud et de la migration.

Nul ne peut nier le fait que la sécurité des réseaux est un enjeu majeur dans notre société moderne, une ère numérique en constante évolution d’autant plus avec la montée en puissance du travail à distance ou le télétravail qui a fortement augmenté ces dernières années, les entreprises sont confrontées à des défis croissants en matière de protection de leurs infrastructures et de leurs données contre les menaces cybernétiques toujours plus sophistiquées.

L'essor de l'accès à distance, en particulier, a considérablement transformé la manière dont les entreprises opèrent. Les employés, les partenaires et même les clients accèdent désormais aux ressources et aux applications de l'entreprise de n'importe où et à tout moment, ce qui nécessite une vigilance accrue en matière de sécurité.

Dans la deuxième partie de ce même chapitre, nous examinerons de plus près les défis spécifiques posés par l'accès à distance et les solutions innovantes mises en œuvre pour garantir la sécurité des connexions distantes. Nous explorerons les technologies telles que les VPN (Virtual Private Network), les pare-feu avancés, les outils de gestion des identités et des accès (ISE), ainsi que les meilleures pratiques de sécurité des réseaux pour assurer une protection robuste contre les cybermenaces tout en permettant une connectivité flexible et sécurisée.

I.1 Les réseaux informatiques

Les réseaux informatiques représentent un écosystème dynamique et interconnecté de systèmes, d'appareils et de protocoles conçus pour permettre la communication et le partage de ressources entre des entités distantes. Fondamentalement, ils agissent comme des infrastructures numériques qui facilitent l'échange d'informations à travers divers médias de transmission, tels que les câbles, les fibres optiques et les ondes radios. Ces réseaux se structurent selon une architecture complexe, intégrant des éléments clés tels que les commutateurs, les routeurs et les serveurs, qui orchestrent le flux de données avec précision et efficacité.

Au-delà de leur fonction de transmission, les réseaux offrent également des fonctionnalités avancées telles que la sécurité, la gestion des données et la résilience, garantissant ainsi une connectivité robuste et fiable dans des environnements variés, allant des réseaux locaux (LAN) aux réseaux étendus (WAN) et à l'Internet global. En résumé, les réseaux informatiques constituent le fondement invisible mais essentiel de la société numérique moderne, permettant la collaboration, l'innovation et la connectivité à l'échelle mondiale.

I.1.1 Les équipements principaux d'un réseau

a. **Routeur** Un routeur est un périphérique de réseau responsable du transfert des données entre différents réseaux. Il analyse les adresses de destination des paquets de données et détermine le meilleur chemin pour les acheminer vers leur destination [2].

b. **Commut ateur (Switch)** Un commutateur est un dispositif de réseau qui connecte plusieurs périphériques au sein d'un réseau local (LAN). Il fonctionne en transférant les données uniquement vers les périphériques destinataires, améliorant ainsi l'efficacité du réseau [2].

c. **Firewall** Un pare-feu est un dispositif de sécurité réseau qui contrôle et filtre le trafic entrant et sortant d'un réseau. Il vise à protéger le réseau contre les accès non autorisés et les attaques informatiques [2].

d. **Serveur** Un serveur est un ordinateur puissant dédié au stockage et à la distribution de ressources et de services aux utilisateurs d'un réseau. Il peut héberger des fichiers, des

applications, des sites web, ou d'autres services réseau, on note trois formats de serveurs physiques [2].

- **Serveur Tour** similaire aux unités centrales d'un PC fixe, ce serveur peut être installé à divers endroits, mais il requiert une source électrique appropriée [1].
- **Serveur Rack** caractérisé par son format plat, ce serveur est conçu pour s'installer dans une baie. Les configurations de ce type de serveur surpassent généralement celles des serveurs Tour en termes de performances. L'accès est simplifié, car ces serveurs sont généralement logés dans des armoires situées dans des salles dédiées [1].
- **Serveur Lame (ou serveur Blade)** représentant le format le plus récent, ce serveur ne peut fonctionner de manière autonome. Il s'insère dans un châssis intégrant d'autres serveurs lames. La particularité de ce format réside dans le fait que le châssis est connecté aux réseaux et aux alimentations électriques [1].

e. **Ordinateur personnel** Un ordinateur personnel est un terminal de traitement de données individuel, utilisé pour exécuter des applications logicielles et accéder aux ressources partagées sur un réseau [2].

I.1.2 Support de transmission

Ces périphériques échangent des données à travers différents liaison de transmission Qui sont

a. **Liaison Filaire** La liaison filaire est une méthode de transmission de données qui utilise des câbles physiques pour acheminer les signaux entre les périphériques. Les types de liaisons filaires incluent les câbles Ethernet, les câbles coaxiaux et les câbles à fibre optique. Ces liaisons offrent généralement une grande fiabilité et des débits élevés, mais peuvent être limitées par la longueur du câble et les interférences électromagnétiques [3].

b. **Liaison Sans Fil** La liaison sans fil est une méthode de transmission de données qui utilise des ondes radio ou des signaux infrarouges pour communiquer entre les périphériques, sans l'utilisation de câbles physiques. Les technologies sans fil courantes incluent le Wi-Fi, le Bluetooth, et les réseaux cellulaires. Les liaisons sans fil offrent une grande flexibilité et une facilité de déploiement, mais peuvent être sujettes aux interférences et à la perte de signal [3].

c. **Liaison Optique** La liaison optique est une méthode de transmission de données qui utilise la lumière pour transmettre les signaux à travers des fibres optiques. Ces fibres sont généralement composées de verre ou de plastique, et permettent des débits de données élevés sur de longues distances. Les liaisons optiques sont largement utilisées dans les réseaux à haut débit, tels que les réseaux de télécommunications et les réseaux informatiques à fibre optique [3].

d. **Liaison Satellite** La liaison satellite est une méthode de transmission de données qui utilise des satellites en orbite pour relayer les signaux entre les émetteurs et les récepteurs. Ces liaisons sont souvent utilisées pour fournir une connectivité dans les régions éloignées ou difficiles d'accès, ainsi que pour les communications à longue distance. Les liaisons satellite offrent une grande couverture géographique, mais peuvent être sujettes à des retards de latence et à des coûts élevés [3].

I.1.3 Types de Réseaux

a. **Réseau Personnel (PAN – Personal Area Network)** un PAN est un réseau interne destine à une utilisation domestique très limité en termes de portée, qui peut être filaire et comme sans fil mais possédant un débit plus élevé (Bluetooth, Zigbee, P2P) [4].

b. **Réseau Local (LAN – Local Area Network)** Un LAN est un réseau informatique limité à une zone géographique restreinte, comme un bureau, un bâtiment ou un campus. Il permet le partage de ressources telles que des imprimantes, des fichiers et des applications entre les utilisateurs [4].

c. **Réseau Métropolitain (MAN – Metropolitan Area Network)** Un MAN est un réseau de taille intermédiaire, couvrant une zone métropolitaine comme une ville ou une région suburbaine. Il offre des services de communication à haut débit sur une zone géographique étendue [4].

d. **Réseau Étendu (WAN – Wide Area Network)** Un WAN couvre une plus grande distance géographique, reliant plusieurs LAN sur de vastes territoires, souvent à l'aide de technologies telles que les réseaux cellulaires ou Internet. Les WAN permettent la communication entre des sites distants [4].

e. **Réseau Privé Virtuel (VPN - Virtual Private Network)** Un VPN établit une connexion sécurisée sur un réseau public tel qu'Internet, permettant aux utilisateurs d'accéder à des ressources distantes de manière sécurisée comme s'ils étaient directement connectés au réseau privé [4].

f. **Réseau Client-Serveur** Ce type de réseau est basé sur un modèle dans lequel les ressources et les services sont fournis par des serveurs centralisés à des clients individuels. Les clients demandent des ressources et les serveurs les fournissent en retour [4].

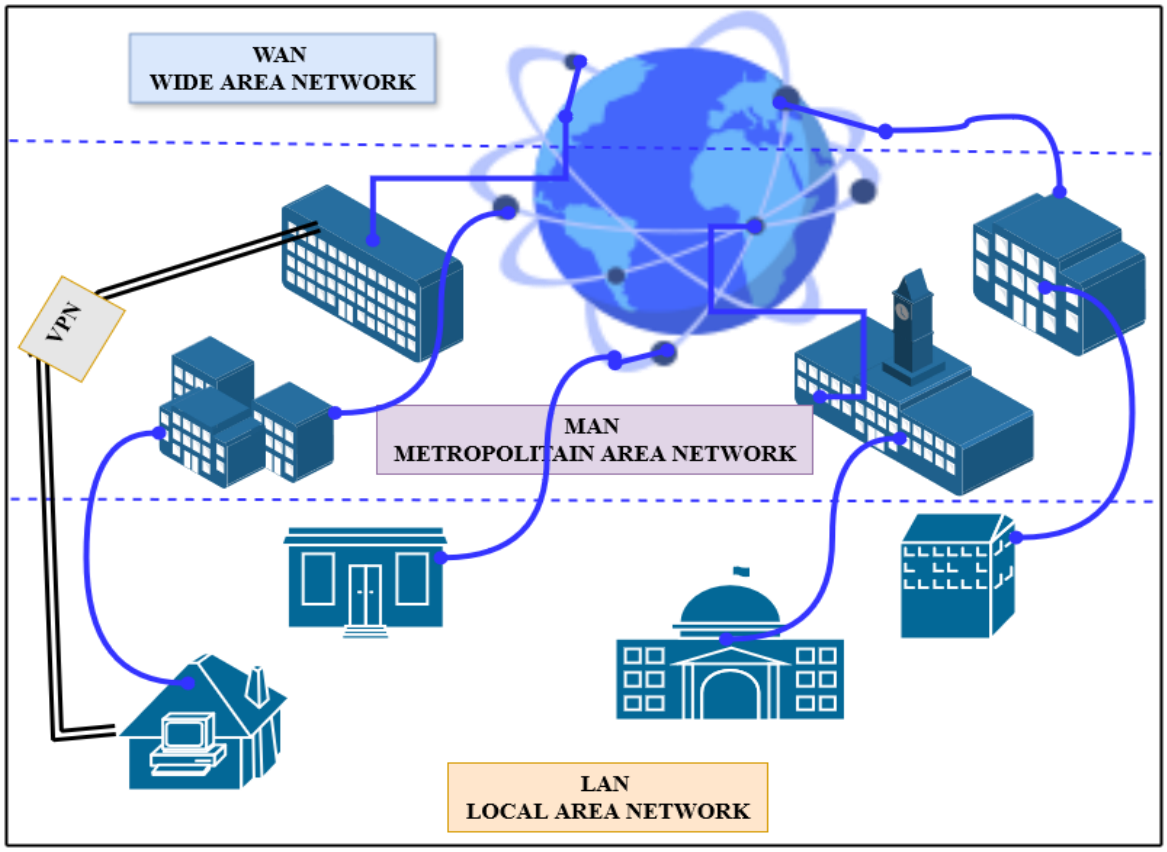

Figure I.1 Les types de réseaux.

I.2 Définition de la Virtualisation

La virtualisation représente l'exploitation ingénieuse d'un ensemble de ressources techniques, tant matérielles que logicielles. Elle permet l'exécution simultanée de plusieurs systèmes d'exploitation, appelés OS invités, sur une même machine serveur, abolissant ainsi le besoin d'un serveur distinct pour chaque application. Cette technologie novatrice nécessite simplement l'installation d'un logiciel de virtualisation sur une machine, ajoutant une couche d'abstraction

connue sous le nom d'hyperviseur. Cette séparation entre le matériel et les applications assure une indépendance totale, offrant une flexibilité sans précédent. Le logiciel de virtualisation peut alors simuler plusieurs machines virtuelles, chacune exécutant le système d'exploitation de son choix (Windows, Linux, Macintosh…) permettant ainsi une utilisation efficiente des ressources disponibles [5].

I.2.1 But de la Virtualisation

La virtualisation vise à révolutionner l'infrastructure informatique en permettant une utilisation plus flexible et efficiente des ressources matérielles et logicielles. Son objectif fondamental est de maximiser l'utilisation des ressources tout en minimisant les coûts et la complexité associés à la gestion des infrastructures informatiques. En créant des environnements virtuels, la virtualisation offre une solution innovante pour consolider les serveurs, améliorer la résilience et la disponibilité des systèmes, et faciliter le déploiement rapide des applications. En outre, elle favorise une meilleure utilisation des ressources énergétiques et une réduction de l'empreinte carbone, contribuant ainsi à une informatique plus durable.

La virtualisation transforme les opérations informatiques en offrant une flexibilité, une agilité et une efficacité accrues pour répondre aux besoins dynamiques des entreprises et des organisations modernes [5].

I.2.2 Les Avantages de la Virtualisation

La virtualisation comporte plusieurs avantages et bienfaits dont on peut citer

a. **Exploitation des ressources physique** elle nous permet l'utilisation accrue des ressources physique des machine (cpu, ram, mémoire, carte réseau) pour une exploitation maximale [6].

b. **Économies d'énergie** En consolidant les serveurs, la virtualisation contribue à une réduction de la consommation électrique nécessaire pour alimenter et refroidir les infrastructures informatiques. Cela se traduit par des économies significatives sur la facture mensuelle d'électricité [6].

c. **Réduction des coûts** La virtualisation permet une consolidation efficace des serveurs, ce qui réduit le besoin en équipements physiques. Cela se traduit par une diminution du

nombre de serveurs physiques nécessaires, ainsi que moins de périphériques réseau et une infrastructure sous-jacente moins complexe. En conséquence, les coûts de maintenance sont également réduits [6].

d. **Optimisation de l'espace** La combinaison de la consolidation des serveurs et de la virtualisation permet aux entreprises de réduire l'encombrement total du data center [6].

e. **En libérant de l'espace physique** Les entreprises peuvent mieux optimiser leur utilisation de l'espace et réduire les coûts associés à l'hébergement des équipements [6].

f. **Facilité de prototypage** La virtualisation permet la création rapide de laboratoires autonomes, opérant sur des réseaux isolés, pour tester et prototyper les déploiements réseau. En cas d'erreur, les administrateurs peuvent aisément revenir à une version antérieure, facilitant ainsi la gestion des tests et prototypes [6].

g. **Provisionnement rapide des serveurs** La création de serveurs virtuels est considérablement plus rapide que le provisionnement de serveurs physiques, ce qui accélère les processus de déploiement et de mise en production [6].

h. **Meilleure disponibilité des serveurs** Les plates-formes de virtualisation de serveurs offrent des fonctionnalités avancées de tolérance aux pannes, telles que la migration dynamique, la haute disponibilité et la planification des ressources distribuées, garantissant ainsi une disponibilité optimale des services [6].

i. **Reprise après sinistre efficace** La virtualisation propose des fonctions avancées de continuité d'activité, permettant une reprise rapide en cas de sinistre. L'abstraction matérielle élimine le besoin de disposer d'équipements matériels identiques, tandis que les logiciels de virtualisation permettent de tester et d'automatiser les basculements avant tout événement catastrophique [6].

j. **Compatibilité avec les systèmes existants** La virtualisation offre la possibilité de prolonger la durée de vie des systèmes d'exploitation et des applications existants, offrant ainsi aux entreprises un temps supplémentaire pour migrer vers de nouvelles solutions sans compromettre la stabilité et la continuité de leurs opérations [6].

I.2.3 Domaine de Virtualisation

Les différentes sphères où la virtualisation est appliquée englobent une gamme étendue d'applications et d'environnements où cette technologie est exploitée pour optimiser l'efficacité, la flexibilité et la gestion des ressources informatiques. Voici quelques-uns de ces domaines

I.2.3.1 Virtualisation des Applications

Il s'agit d'une technologie logicielle conçue pour améliorer la portabilité et la compatibilité des applications Cette approche permet d'exécuter des applications dans des environnements isolés, indépendamment du système d'exploitation sous-jacent, simplifiant ainsi leur gestion et leur déploiement [7].

I.2.3.2 Virtualisation des Serveurs

Cette pratique permet de regrouper plusieurs serveurs physiques en une seule et unique machine, améliorant ainsi l'utilisation des ressources et la gestion des charges de travail, elle comporte [1]

a. **Machine Hôte**

Une machine hôte dans le domaine de la virtualisation est le système physique sur lequel les machines virtuelles sont exécutées. Elle fournit les ressources matérielles nécessaires, telles que le processeur, la mémoire, le stockage et les périphériques, pour prendre en charge les instances virtuelles.

La machine hôte agit comme une plateforme de virtualisation, permettant aux machines virtuelles de fonctionner de manière isolée les unes des autres, tout en partageant les ressources de la machine physique sous-jacente [1].

b. **Machine Virtuelle**

Une machine virtuelle est une émulation d'un ordinateur ou d'un système informatique, fonctionnant comme une entité logicielle autonome sur une machine physique. Elle permet d'exécuter plusieurs systèmes d'exploitation et applications simultanément sur un seul matériel physique. En d'autres termes, une machine virtuelle crée un environnement virtuel isolé, offrant

une abstraction des ressources matérielles sous-jacentes et permettant une flexibilité et une gestion efficace des infrastructures informatiques [1].

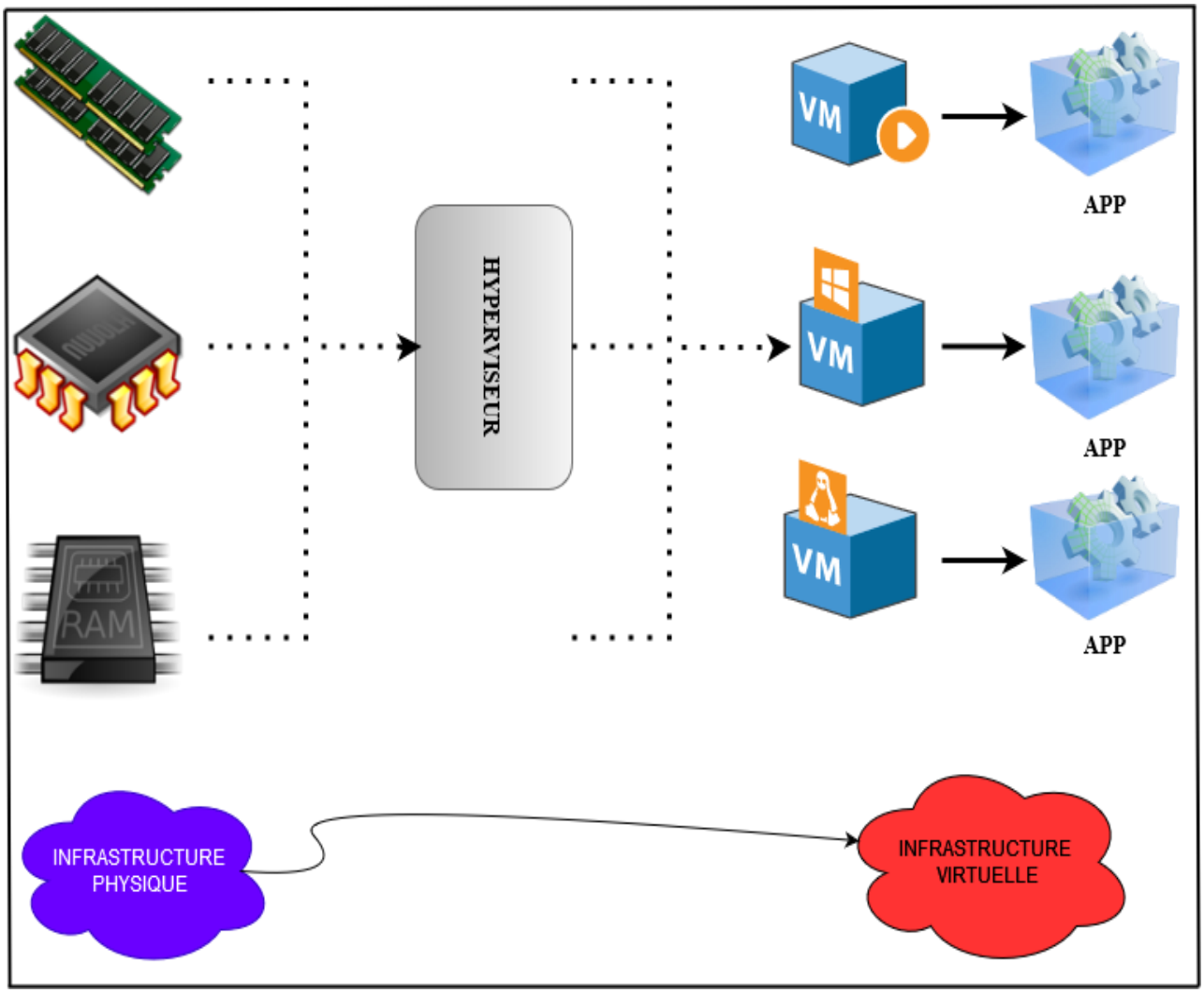

Figure I.2 Illustration de la virtualisation d'un serveur.

I.2.3.3 Virtualisation des Réseaux

La virtualisation des serveurs consiste à dissimuler les ressources physiques des serveurs (comme le nombre de serveurs, les processeurs et les systèmes d'exploitation) aux utilisateurs finaux. Cela peut poser des défis lorsque les data centers s'appuient sur des architectures réseau conventionnelles. Par exemple, les VLAN (réseaux locaux virtuels) utilisés par les machines virtuelles doivent être assignés au même port de commutation que le serveur physique hébergeant l'hyperviseur. Étant donné que les machines virtuelles peuvent être déplacées, les administrateurs réseau doivent pouvoir ajouter, supprimer et modifier les ressources et les

profils réseau de manière dynamique. Ce processus est souvent complexe avec les commutateurs réseau traditionnels. [8].

Les atouts de la virtualisation réseau comprennent [8]

- La capacité à héberger des machines virtuelles, offrant une liberté vis-à-vis du matériel. Les machines virtuelles peuvent ainsi migrer d'un domaine logique à un autre sans nécessiter de reconfiguration du réseau ni l'établissement de nouveaux liens physiques.

- Une meilleure flexibilité dans le réseau, car celui-ci est virtualisé au niveau de l'hyperviseur plutôt que sur un commutateur réseau physique.

- Une gestion simplifiée du réseau, puisque tous les composants et fonctionnalités sont déployés et gérés par des logiciels.

I.2.3.4 Virtualisation de Stockage

La virtualisation de stockage consiste à contrôler précisément l'accès des divers clients (serveurs, applications) aux équipements de stockage via différents protocoles. Les données sont organisées et stockées de manière cohérente sur un disque dur virtuel, permettant ainsi de regrouper et de partager de vastes quantités de stockage entre plusieurs applications et serveurs, indépendamment de la complexité de l'architecture physique sous-jacente.

Cette technologie offre la possibilité d'ajouter des périphériques de stockage supplémentaires sans interruption des services, ainsi que de regrouper des unités de disques durs de différentes vitesses, tailles et marques, tout en assurant une allocation dynamique de l'espace de stockage. Elle garantit une meilleure distribution et redondance des données grâce à divers mécanismes

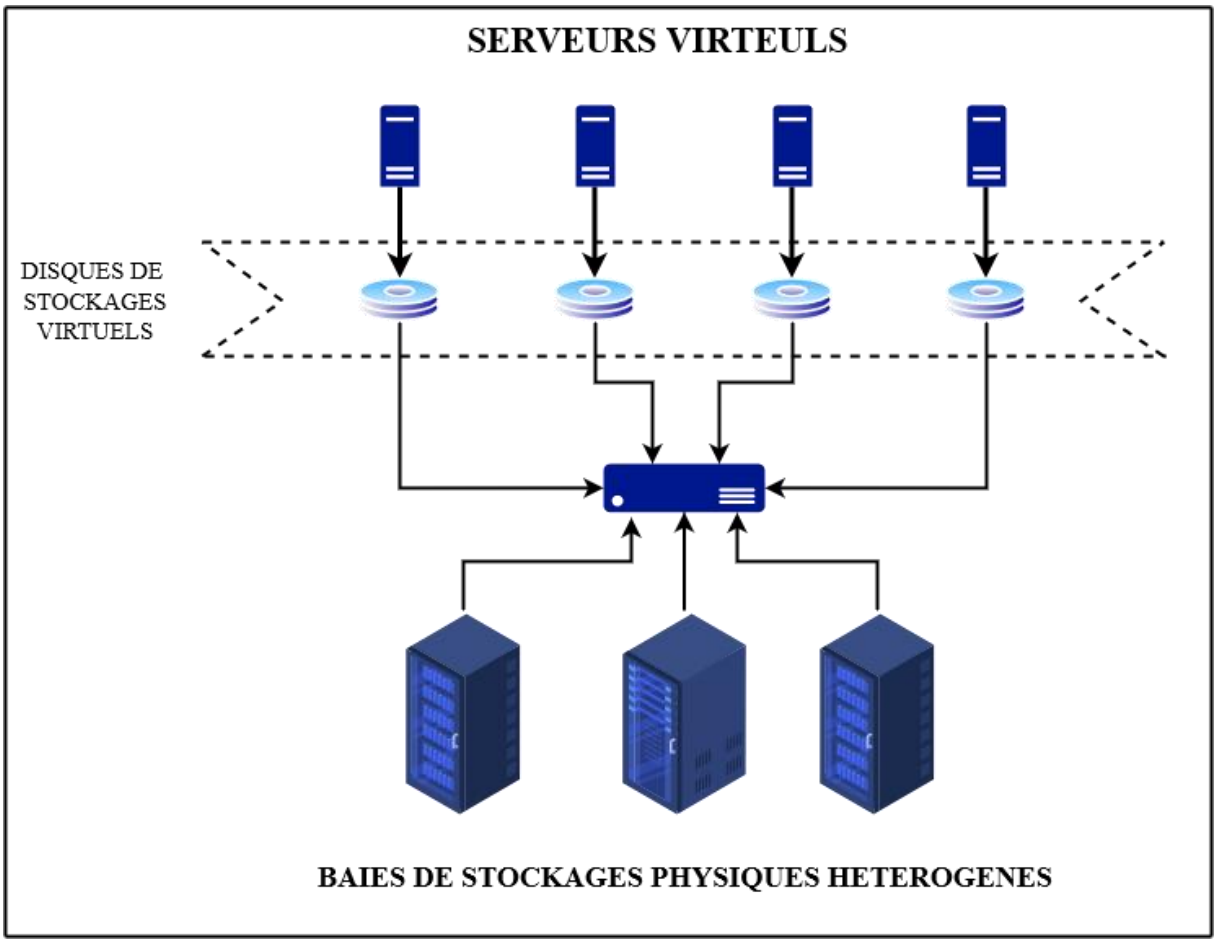

Figure I.3 Schéma représentatif de la virtualisation de stockage.

I.2.4 Hyperviseur

Un hyperviseur est un logiciel de gestion de virtualisation qui agit comme une couche d'abstraction entre le matériel physique d'un système informatique et les systèmes d'exploitation invités. Sa fonction principale est de créer et de gérer des machines virtuelles, offrant ainsi la possibilité d'exécuter plusieurs environnements informatiques isolés les uns des autres sur une seule infrastructure matérielle. Cette technologie permet une utilisation efficace des ressources matérielles en fournissant un partage sécurisé et contrôlé des ressources telles que le processeur, la mémoire, le stockage et les périphériques [1].

I.2.4.1 Types d'Hyperviseur

a. Un hyperviseur de type 1

L'hyperviseur de type 1 est installé directement sur le matériel physique ou les serveurs réseau, éliminant ainsi la nécessité d'un système d'exploitation intermédiaire. Typiquement déployés

dans les data centers des grandes entreprises, ces hyperviseurs offrent une gestion optimale des ressources matérielles en permettant l'exécution simultanée de plusieurs instances de systèmes d'exploitation sur le même serveur. Ils bénéficient d'un accès direct aux ressources matérielles, améliorant ainsi l'efficacité et les performances. Parmi les hyperviseurs de type 1 les plus répandus, on trouve VMware ESX et Microsoft Hyper-V [1].

b. Un hyperviseur de type 2

Aussi appelé "hyperviseur hébergé", fonctionne en étant installé au-dessus d'un système d'exploitation existant, comme Mac OS X, Windows ou Linux. Cette configuration permet l'exécution d'une ou plusieurs instances du système d'exploitation au-dessus de l'hyperviseur. L'un des avantages majeurs des hyperviseurs de type 2 est leur absence de nécessité d'une console de gestion logicielle, ce qui les rend très populaires aussi bien auprès des particuliers que des entreprises découvrant la virtualisation.

Des exemples courants d'hyperviseurs de type 2 incluent VMware Workstation et Oracle VM VirtualBox. Pour résoudre le problème de point de défaillance unique, les solutions de virtualisation intègrent généralement des fonctionnalités de redondance mises en œuvre de diverses manières. En cas de défaillance de l'hyperviseur, la machine virtuelle peut être redémarrée sur un autre hyperviseur. De plus, une même machine virtuelle peut être exécutée simultanément sur deux hyperviseurs, permettant ainsi la copie des instructions relatives à la mémoire vive et au processeur entre eux. Ainsi, si un hyperviseur tombe en panne, la machine virtuelle continue de fonctionner sur l'autre hyperviseur. D'autres fonctionnalités telles que l'exportation, l'importation et le clonage sont également disponibles pour les machines virtuelles [1].

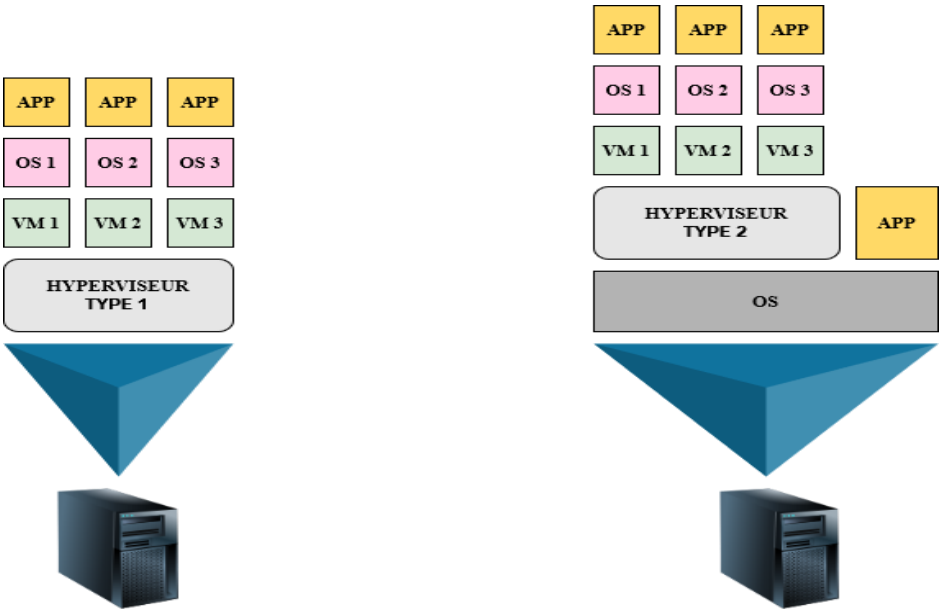

Figure I.4 Schéma représentatif des deux types d'hyperviseurs.

I.3. Data Center et Cloud Computing

Les termes "Data Center" et "Cloud Computing" sont parfois confondus. En réalité, le "Cloud Computing" repose sur l'infrastructure des data centers. Un data center est un espace physique où sont hébergés des systèmes informatiques et leurs composants, pouvant occuper une pièce ou même un bâtiment entier. Les grandes entreprises utilisent souvent des data centers privés pour stocker leurs données et fournir des services à leurs utilisateurs. En revanche, les entreprises de taille plus modeste, disposant de moins de ressources, ont souvent recours à la location de services de serveurs et de stockage auprès de data centers plus importants hébergés dans le cloud. Le "Cloud Computing" est généralement proposé sous forme de service par les data centers. Les fournisseurs de services cloud utilisent en effet les infrastructures des data centers pour héberger leurs services et leurs ressources basés dans le cloud. Ainsi, le "Cloud Computing" repose sur l'infrastructure physique des data centers pour offrir des services et des solutions informatiques à grande échelle [9].

I.3.1 Cloud Computing

Le Cloud Computing, selon la définition de l'Institut national américain des normes et de la technologie (NIST), offre un accès facile et à la demande, via le réseau, à un ensemble partagé de ressources informatiques configurables, telles que les réseaux, les serveurs, le stockage, les applications et les services. Ces ressources peuvent être provisionnées rapidement par les

utilisateurs ou libérées avec un minimum d'effort administratif de la part de l'entreprise ou du prestataire de services. Les caractéristiques principales du Cloud Computing comprennent un large accès réseau, une élasticité rapide, une facturation basée sur la consommation et la mise en commun des ressources [9].

I.3.1.1 Services Cloud Computing

Les services proposés dans le cloud offrent une gamme diversifiée d'options pour répondre aux besoins spécifiques des utilisateurs. Parmi les principales catégories de services de Cloud Computing figurent le SaaS (Software as a Service), le PaaS (Platform as a Service) et l'IaaS (Infrastructure as a Service) [9].

I.3.1.2 Modèles de Cloud Computing

Nous identifions quatre principaux modèles de Cloud Computing

a. **Clouds publics** Accessibles à tous, ces services peuvent être gratuits ou payants selon un modèle de tarification à l'utilisation. Le cloud public utilise Internet pour fournir ses services [9].

b. **Clouds privés** Dédiés à une entreprise ou à une entité spécifique, les Clouds privés peuvent entraîner des coûts élevés en termes de déploiement et de maintenance [9].

c. **Clouds hybrides** Intégrant au moins deux types de Clouds (par exemple, un cloud privé et un cloud public), les Clouds hybrides offrent aux utilisateurs des niveaux d'accès différenciés en fonction de leurs droits d'utilisateur [9].

d. **Clouds communautaires** Partagés par plusieurs organisations ayant des intérêts communs, les Clouds communautaires offrent une infrastructure partagée répondant aux besoins spécifiques de chaque communauté d'utilisateurs [9].

I.4 Cloud Computing et Virtualisation

Les termes "Cloud Computing" et "virtualisation", bien qu'associés, représentent des concepts distincts. La virtualisation constitue la fondation du Cloud Computing, jouant un rôle crucial dans sa mise en œuvre. En effet, sans la virtualisation, le modèle de Cloud Computing tel que nous le connaissons ne pourrait pas exister. Le Cloud Computing permet la séparation des

applications et du matériel, tandis que la virtualisation sépare le système d'exploitation et le matériel physique. De nombreux prestataires proposent des services de cloud virtuel qui permettent de provisionner dynamiquement des serveurs en fonction des besoins spécifiques [9].

I.5 La Migration

La migration dans le Domaine informatique implique le déplacement, la mise à niveau ou le transfert d'un système ou d'une application d'un état existant à un autre. Cela peut inclure le passage d'une architecture traditionnelle à une solution basée sur la virtualisation et l'hyper-convergence, la mise à jour d'un système d'exploitation vers une version plus avancée ou le déplacement d'une application en cours d'exécution d'une machine hôte à une autre [10].

La migration de données est un aspect essentiel de ce processus, et elle peut être classée en plusieurs types

a. **Migration de machine virtuelle** Ce type de migration implique le déplacement des données de mémoire vive et de processeur d'une machine virtuelle d'un hôte physique à un autre via un réseau [10].

b. **Migration de stockage** Cette migration implique le déplacement des données de stockage d'un nœud à un autre, qu'il s'agisse d'un nœud physique ou d'une machine virtuelle, sur site ou dans le cloud, via un réseau [10].

c. **Migration d'application** Plutôt que de déplacer une machine virtuelle entière, cette migration se concentre sur le déplacement d'une seule application vers une autre machine virtuelle. Cela peut inclure le transfert de bases de données, de dossiers d'installation et de données [10].

La migration peut être effectuée manuellement ou automatiquement. L'automatisation et l'orchestration sont important dans ce processus, permettant d'effectuer des migrations de manière efficace en libérant les ressources humaines des tâches fastidieuses [10].

I.6 Sécurité d’un Réseau Informatique

La sécurité des réseaux englobe un ensemble de stratégies, de dispositifs et de pratiques visant à prévenir les attaques, à protéger les données et les ressources, ainsi qu'à garantir le bon

fonctionnement des réseaux informatiques. Elle implique la mise en place de pare-feu, de systèmes de détection d'intrusion, de protocoles de chiffrement, et de mécanismes d'authentification pour contrer les menaces telles que les attaques par déni de service, les logiciels malveillants et les tentatives d'usurpation d'identité. En assurant la confidentialité, l'intégrité et la disponibilité des informations échangées, la sécurité des réseaux contribue à maintenir la confiance des utilisateurs et à préserver la continuité des activités des organisations [11].

I.6.1 But de la Sécurité

Le but de la sécurité réseau est de garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes au sein d'un réseau informatique. Cela implique de mettre en place des mesures de protection pour prévenir les cyberattaques, détecter les intrusions et y répondre de manière appropriée. En assurant la sécurité du réseau, les organisations peuvent réduire les risques liés aux violations de données, aux interruptions de service et aux dommages potentiels causés par des acteurs malveillants [11].

I.6.2 Différentes Méthodes de Sécurité

I.6.2.1 Virtual Local Area Network (VLAN)

Les VLANs sont des réseaux locaux virtuels qui permettent de segmenter un réseau physique en plusieurs sous-réseaux logiques distincts, même s'ils partagent la même infrastructure physique. Cela permet d’isoler les groupes de travail ou les types de trafic, de réduire les collisions de domaine de diffusion et d’améliorer la sécurité en limitant la portée des diffusions. Comme ils peuvent également être utilisés pour imposer des politiques de sécurité et simplifier l’administration du réseau [11].

I.6.2.2 Access Control List (ACL)

Les ACL sont des listes de contrôle d’accès qui spécifient quelles adresses IP sont autorisées ou refusées à traverser un point de contrôle réseau. Elles sont cruciales pour définir des politiques de sécurité granulaires et peuvent être appliquées à la fois aux interfaces entrantes et sortantes des routeurs et des commutateurs pour réguler le trafic [11].

Il y’a essentiellement deux types d’ACL

a. **ACL Standard** Les ACL standard sont les plus simples et les plus anciennes. Elles filtrent le trafic uniquement en fonction de l'adresse IP source. Cela signifie qu'une ACL standard peut autoriser ou refuser le trafic d'une adresse IP spécifique ou d'une plage d'adresses IP. Les ACL standard sont généralement utilisées pour des tâches simples de filtrage et sont appliquées aux interfaces pour contrôler le trafic entrant [11].

b. **ACL étendue** Les ACL étendues offrent une plus grande flexibilité et contrôle que les ACL standard. Elles peuvent filtrer le trafic non seulement en fonction de l'adresse IP source, mais aussi de l'adresse IP de destination, des numéros de port TCP/UDP source et celui de la destination. Cela permet aux administrateurs de définir des règles de sécurité plus précises et complexes. Les ACL étendues sont souvent utilisées pour des politiques de sécurité plus détaillées et peuvent être appliquées aux interfaces pour réguler le trafic entrant et sortant. Chaque entrée dans une ACL est appelée une ACE (Access Control Entry), et les ACL sont traitées séquentiellement par le dispositif de réseau jusqu'à ce qu'une correspondance soit trouvée. Si aucune règle ne correspond, le trafic est généralement refusé par défaut, ce qui renforce la sécurité du réseau [11].

I.6.2.3 Identity Services Engine (ISE)

ISE de Cisco est une plateforme de sécurité offrant une gestion centralisée des identités pour les utilisateurs et les appareils. Cette solution permet la création de politiques d'accès basées sur divers paramètres tels que le rôle, le contexte et l'emplacement. Elle intègre également des fonctionnalités essentielles telles que l'authentification, l'autorisation et la comptabilité (AAA) pour renforcer la sécurité du réseau. Grâce à ISE, les utilisateurs et les appareils sont authentifiés, ce qui détermine leurs droits d'accès au réseau ainsi que les ressources qu'ils sont autorisés à utiliser.

De plus, cette plateforme classe les appareils connectés au réseau, offrant ainsi une visibilité approfondie et un contrôle accru sur l'environnement réseau [11].

I.6.2.4 Triple A (Authentification, Autorisation, Comptabilité)

Le triple A est un ensemble de services ou de fonctions qui constituent la gestion d'accès aux réseaux et aux systèmes, chaque fonction joue un rôle spécifique et distinct mais complémentaire dans le contrôle et la sécurisation des ressources réseau [11].

a. **Authentification** C'est le 1er processus qui rentre en jeu en vérifiant les identités des utilisateurs qui tente d'accéder au réseau. Son principe est de s'assurer que la personne ou l'appareil est bien celui qui prétend être. Pour ce faire le moyen le plus courant est l'introduction d'un nom d'utilisateur suivi du mot de passe. L'authentification garantit ainsi que seuls les utilisateurs légitimes peuvent accéder aux ressources du réseau [11].
b. **Autorisation** L'autorisation intervient une fois que l'authentification a été réussie. Elle consiste à déterminer les actions et les ressources auxquelles l'utilisateur ou le périphérique authentifié est autorisé à accéder. Les décisions d'autorisation sont généralement basées sur les droits attribués à chaque utilisateur ou groupe d'utilisateurs, ainsi que sur les politiques de sécurité prédéfinies [11].
c. **Accounting (Comptabilité)** Ce processus concerne le suivi et l'enregistrement des activités des utilisateurs une fois qu'ils ont accédé au réseau. Cela inclut généralement la collecte de données telles que les heures de connexion, les ressources utilisées et les actions effectuées. La comptabilité est cruciale pour des raisons de sécurité, de conformité réglementaire et de gestion des performances du réseau. Les informations collectées peuvent être utilisées à des fins d'audit, de facturation ou pour générer des rapports sur l'utilisation des ressources réseau [11].

I.6.2.5 Système de Prévention des Intrusions IPS

C'est un composant qui optimise l'aspect sécuritaire des réseaux informatiques, offrant une protection proactive contre les menaces en ligne. Son principe de fonctionnement repose sur une surveillance en temps réel du trafic réseau, où il analyse le comportement du trafic ainsi que les signatures de menaces connues pour détecter et bloquer les activités qui représentent un risque. Les IPS fonctionnent en inspectant le contenu des paquets de données pour identifier les schémas ou les comportements suspects, tels que les tentatives d'intrusion, les attaques par déni de service distribué ou les exploits de vulnérabilités [11].

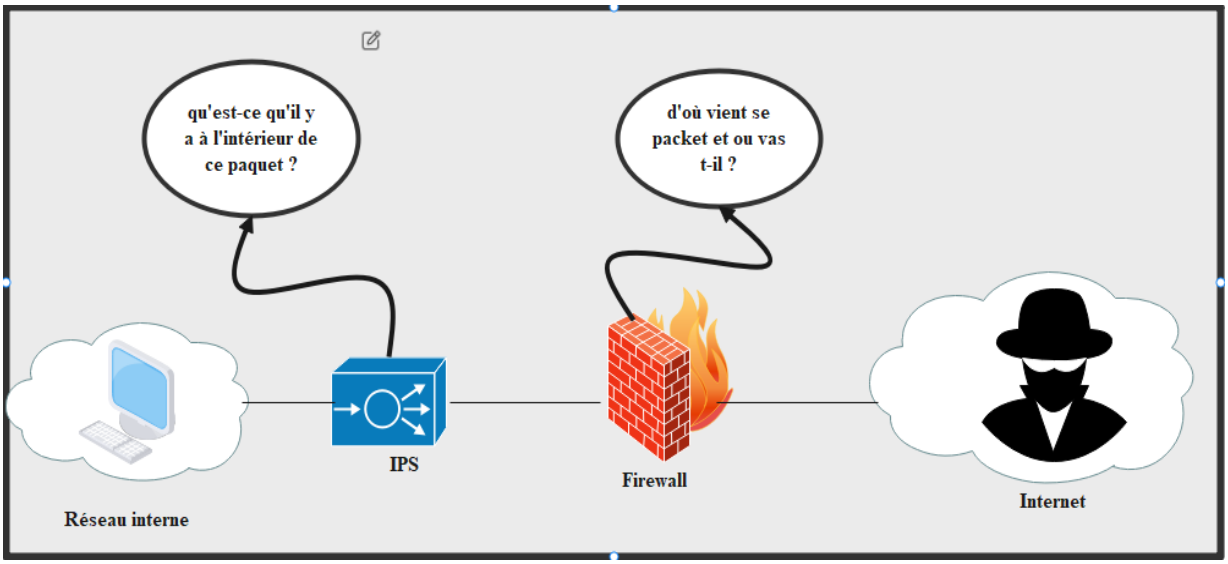

Figure I.5 Schématisation de la différence entre un pare-feu et un IPS.

I.6.2.6 Antivirus

Un logiciel antivirus est spécialement conçu pour identifier, bloquer et éliminer les logiciels malveillants comme les virus. Son objectif principal est de sécuriser les systèmes informatiques en surveillant en permanence les fichiers et les activités du système. Pour ce faire, il effectue régulièrement des analyses des fichiers, met à jour sa base de données de signatures de virus et prend des mesures telles que la mise en quarantaine ou de supprimer complètement les logiciels malveillants détectés [11].

I.7 L'accès à Distance

L'accès à distance désigne la capacité d'entrer dans un système informatique ou d'utiliser ses ressources depuis un emplacement éloigné, en utilisant des technologies telles que l'Internet ou des réseaux privés. Cela permet à un utilisateur de se connecter à un ordinateur ou à un réseau depuis n'importe où dans le monde, sans avoir besoin d'être physiquement présent à proximité de la machine ou des ressources qu'il souhaite utiliser.

En d'autres termes, c'est comme si vous pouviez contrôler un ordinateur ou accéder à des fichiers comme si vous étiez assis directement devant eux, même si vous êtes à des kilomètres de distance. Cette capacité est précieuse pour les professionnels qui doivent gérer des serveurs distants, fournir un support technique à distance, ou pour les personnes qui travaillent à distance et ont besoin d'accéder à leurs ressources professionnelles depuis chez elles [11].

Parmi les différentes techniques ou protocoles d'accès à distance :

I.7.1 Protocole Telnet

Terminal Network a été l'un des premiers protocoles utilisés pour permettre l'accès distant à des systèmes informatiques. Son fonctionnement repose sur le principe client-serveur. L'utilisateur se connecte à un serveur distant via le protocole Telnet, généralement en utilisant un logiciel client Telnet tel que PuTTY ou HyperTerminal. Une fois la connexion établie, l'utilisateur peut entrer des commandes à distance et recevoir les réponses du serveur.

L'inconvénient majeur de ce protocole est qu'il transmet les données, y compris les mots de passe, en texte clair, donc en cas d'attaque ou d'interception malveillantes nos données sont compromises [11].

I.7.2 Protocol SSH (Secure Shell)

La connexion SSH (Secure Shell) est un protocole de communication sécurisé qui permet à un utilisateur d'accéder à un ordinateur distant en ligne de commande. Cette méthode est couramment utilisée dans les environnements Linux/Unix pour gérer des serveurs à distance. Elle offre un moyen sécurisé d'interagir avec des systèmes distants et d'exécuter des commandes à distance. Ce protocole a apporté la touche manquante a Telnet puisque on effet les données transmises avec le SSH sont chiffrées [11].

I.7.3 VPN (Virtual Private Network)

Un VPN (Virtual Private Network) crée un tunnel sécurisé à travers Internet, permettant à un utilisateur distant de se connecter à un réseau privé comme s'il était localement connecté à ce réseau.

Cette méthode offre un accès sécurisé aux ressources internes d'une entreprise ou d'une organisation depuis n'importe quelle localisation géographique dans le monde, en préservant la confidentialité et la sécurité des données transitant sur le réseau [11].

On note deux types majeurs de VPN

a. **VPN Site a Site (Site-To-Site VPN)** ce type de VPN établit une connexion sécurisée entre deux réseaux locaux distincts via Internet. Les routeurs ou les pare-feu des deux

sites sont configurés pour créer un tunnel VPN sécurisé, permettant le transit sécurisé des données entre les deux réseaux distants. Les deux sites seront considérés ainsi comme un seul site [11].

b. **VPN D'accès Distant (Remote Access VPN)** Il permet aux utilisateurs individuels ou aux périphériques distants de se connecter de manière sécurisée à un réseau d'entreprise via Internet. Les utilisateurs utilisent généralement un logiciel client VPN comme Anyconnect pour établir une connexion cryptée avec un serveur VPN situé au sein du réseau de l'entreprise. Comme ils peuvent utiliser un simple navigateur internet, Cela leur permet d'accéder aux ressources du réseau interne comme s'ils étaient physiquement présents dans les locaux de l'entreprise [11].

I.8 Conclusion

Après avoir exploré en profondeur les différents aspects des réseaux informatiques, de la virtualisation, du cloud computing et de la sécurité des réseaux, il est clair que ces domaines sont essentiels pour comprendre et gérer l'infrastructure informatique moderne.

Dans ce premier chapitre, nous avons examiné les éléments constitutifs des réseaux informatiques, des équipements utilisés et les supports de transmission qui les sous-tendent. Nous avons exploré les différents types de réseaux, ainsi que les concepts fondamentaux de la virtualisation, tels que la virtualisation des applications, des serveurs, des réseaux et du stockage.

La virtualisation émerge comme une technologie clé pour optimiser l'utilisation des ressources matérielles et simplifier la gestion des infrastructures informatiques. Elle offre une flexibilité inégalée, permettant aux entreprises de déployer rapidement de nouveaux services et de s'adapter aux demandes changeantes.

Enfin, la sécurité des réseaux est un élément crucial de ce paysage technologique en constante évolution. La protection des données, la prévention des attaques et la gestion des vulnérabilités sont autant de préoccupations majeures pour garantir l'intégrité et la confidentialité des systèmes informatiques.

Ce premier chapitre nous a permis de comprendre l'importance vitale des réseaux informatiques, de la virtualisation et de la sécurité des réseaux dans le contexte de l'informatique

moderne. Ces domaines interconnectés façonnent le paysage technologique actuel et continueront de jouer un rôle central dans les entreprises et les organisations du monde entier.

Chapitre II
Étude et spécification des besoins

Introduction

Avec l'avènement de la virtualisation, de nouvelles architectures ont été conçues pour optimiser les performances, réduire l'encombrement physique et diminuer la consommation énergétique en consolidant les serveurs et en minimisant leur nombre. Dans le contexte des environnements virtualisés contemporains, il devient impératif pour les services informatiques d'adopter une approche novatrice, visant à lever les obstacles traditionnels et à exploiter pleinement les outils d'automatisation disponibles.

Dans ce chapitre, nous plongerons dans l'architecture que nous prévoyons de mettre en œuvre pour notre projet de fin d'études. Nous dresserons également le profil du personnel nécessaire au déploiement de notre environnement virtualisé, tout en détaillant le matériel essentiel requis pour la concrétisation de notre infrastructure. De plus, nous entreprendrons une étude comparative approfondie des divers fabricants et intervenants dans le domaine de la virtualisation.

Enfin, nous mettrons en lumière les différences entre les pare-feu traditionnels et modernes, dans le but d'illustrer l'importance de l'adaptation des mesures de sécurité aux évolutions technologiques contemporaines.

II.1 Etude de l’existant

Un client X dispose d’une infrastructure data center qui souhaite moderniser.

II.1.2 Matériels

- Cinq serveurs : un serveur web, deux contrôleurs de domaine, les deux sont aussi des serveurs DNS et l’un d’eux a DHCP comme un troisième rôle, un serveur d’application et un serveur de base de données.
- Un commutateur niveau 2.
- Un pare-feu physique qui assure la sécurité de l’infrastructure.
- Deux commutateurs SAN pour assurer le réseau de stockage.
- Une baie de stockage.

- Un routeur.

II.1.3 Personnels

a. Un administrateur réseau et sécurité : gère et assure la disponibilité du réseau et la connectivité entre les différents composants de l'infrastructure, ainsi que sa sécurité.

b. Un administrateur système : gère et assure la disponibilité des différents systèmes de l'infrastructure.

c. Un administrateur de stockage : gère et assure la disponibilité, le bon fonctionnement et la redondance du stockage et du réseau de stockage.

II.1.4. Infrastructure actuelle

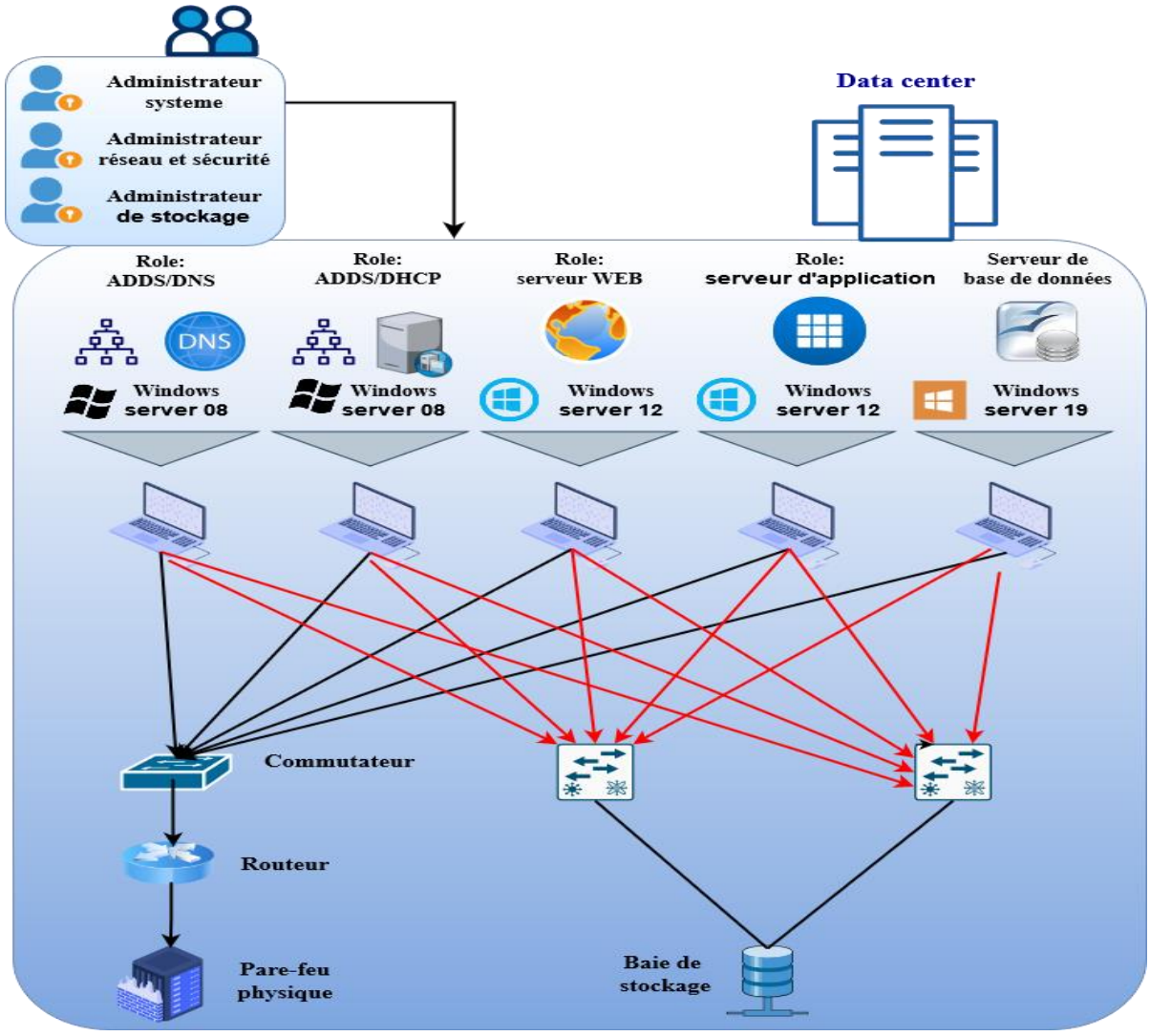

Figure II.6 Infrastructure actuelle du client.

II.2 Problématique

Parmi les critiques que nous pouvons apporter à cette architecture

- Architecture traditionnelle, Comme toute architecture non virtualisée, cette architecture utilise une relation d'un service ou un nombre extrêmement limité de services par serveurs physiques. Ce qui engendre un nombre élevé de serveurs dans le data center, ce qui implique
- Gaspillage énorme de ressources : l'utilisation de RAM, CPU...par un système d'exploitation unique sur un serveur est minime.
- Le coût de la maintenance des serveurs très élevé : ce qui est la conséquence de l'utilisation de beaucoup de serveurs.
- Le coût de la consommation électrique des serveurs est très élevé pour peu de services. Les systèmes de refroidissement sont aussi gourmands en termes de consommation d'électricité.
- Manque de redondance au niveau des équipements réseaux qui forment un point de défaillance unique ce qui nuit à la continuité du business.
- Risque d'arrêt des services : lié à l'absence de redondance sur les serveurs d'application, base de données, DHCP et web. Mis à part le ADDS et DNS, si un serveur physique tombe en panne, tous les services associés seront non disponibles.
- Une mauvaise exploitation de ressources et d'équilibrage de charge, par exemple le serveur hébergeant les rôles ADDS/DNS et DHCP utilise clairement beaucoup plus de ressources matérielles que d'autres serveurs physiques. Cela peut engendrer des durées de vie largement différentes du matériel.
- Manque d'automatisation des tâches, les administrateurs ont un énorme travail manuel au quotidien pour assurer la continuité du business.
- Migration de services difficile, la migration d'un service depuis un serveur physique à un autre en cas de panne ou de déséquilibrage de charge demande une planification, du temps et un effort humain considérable avec un risque élevé d'arrêt de service.
- Générations anciennes de système de serveur, ce qui peut engendrer une menace de sécurité, manque de conformité avec les nouvelles applications, et le manque de bénéfices des nouvelles fonctionnalités.

II.3 Cahier de charge

Notre client souhaite passer d'une infrastructure data center traditionnel vers une infrastructure virtualisé, cette transaction exige ce qui suit

- ✓ Passer vers une infrastructure moderne, automatisée et virtualisée.
- ✓ Assurer une meilleure disponibilité, redondance et gestion des ressources et des services.
- ✓ Minimiser le matériel.
- ✓ Garder les services déjà existants.
- ✓ Migrer les systèmes d'exploitation des services déjà existants vers de nouvelles versions.
- ✓ Assurer la sécurisé du réseau avec un pare-feu.
- ✓ Gestion centralisée des authentifications et autorisations avec un serveur Radius.
- ✓ Accès distant sécurisé au réseau.

Ⅱ.4 Tendance des solutions de virtualisation

Les sociétés informatiques fournisseuses de solution de virtualisation offres aux clients des technologies de mise en place d'infrastructure virtualisée, ainsi d'automatisation et de migration, selon le constructeur, ces solutions peuvent êtres gratuites on dit qu'elle est en open source et elles peuvent êtres sous licence donc "closed source".

II.4.1 Open source

C'est des solutions qui souvent ne demande pas de licence de la part du constructeur, ou qui sont fournies avec des licences gratuites, qui nous donne accès aussi au code source.

Parmi ces constructeurs on cite

a. **RED HAT** Red Hat est une entreprise de logiciels informatiques réputée dans le domaine de la virtualisation, proposant une plateforme de virtualisation open source aux utilisateurs conçue pour l'optimisation des ressources physiques déjà existantes [12].

b. **Citrix** est une société qui fournit des produits pour la collaboration, la virtualisation et le réseau afin de faciliter le travail mobile et l'adoption des services cloud. Citrix Xen Server, basé sur l'hyperviseur Xen, est une plateforme de virtualisation gratuite. Les solutions Xen Enterprise agissent comme des couches de coordination logicielle entre plusieurs applications logicielles sur différents serveurs virtuels, comprenant une console d'administration centralisée puissante [12].

c. **Proxmox** est une solution de virtualisation libre accès qui repose sur l'hyperviseur Linux KVM. Elle offre également une solution de conteneurs avec LXC. Elle propose un support payant. KVM (Kernel-based Virtual Machine) est un hyperviseur de type 1 pour Linux, intégré dans le noyau Linux depuis la version 2.6.20 [12].

II.4.2 Closed source

Cela signifie que les solutions proposées sont sous licences payantes, car ce n'est pas la solution elle-même qui est payante.

Seuls les auteurs originaux du logiciel peuvent accéder, copier et modifier ce logiciel [13].

Parmi ces solutions on cite

a. **VMware**

VMware est en tête du marché mondial dans le domaine de la virtualisation pour les serveurs et les postes de travail. En utilisant une approche inédite de la virtualisation, la technologie VMware sépare les logiciels des composants matériels. Un seul hôte peut ainsi faire tourner plusieurs systèmes d'exploitation et applications, proposant ainsi des solutions client qui rendent l'infrastructure informatique plus réactive en la simplifiant et en fournissant des services de façon plus flexible et évolutive. Les entreprises, qu'elles soient petites ou grandes, peuvent bénéficier des solutions VMware pour réduire leurs coûts et augmenter leur réactivité.

VMware propose des technologies élaborées pour offrir une infrastructure de systèmes plus automatisée et robuste, afin de répondre aux besoins changeants de l'entreprise. La solution proposée par VMware est basée sur l'hyperviseur "ESXi" [13].

b. Microsoft

Microsoft La société offre et met en vente différentes gammes de logiciels et services à usage professionnel et domestique. A l'occasion de son activité Windows Server, Microsoft présente Virtual Server. En 2008, Virtual Server devient Hyper-V, Également désigné sous le nom de Windows Server Virtualisation, ce système de virtualisation repose sur un hyperviseur 64 bits intégré à la version de Windows Server 2008. Ainsi, un serveur physique peut se transformer en hyperviseur, lui permettant la gestion et l'hébergement des machines virtuelles [13].

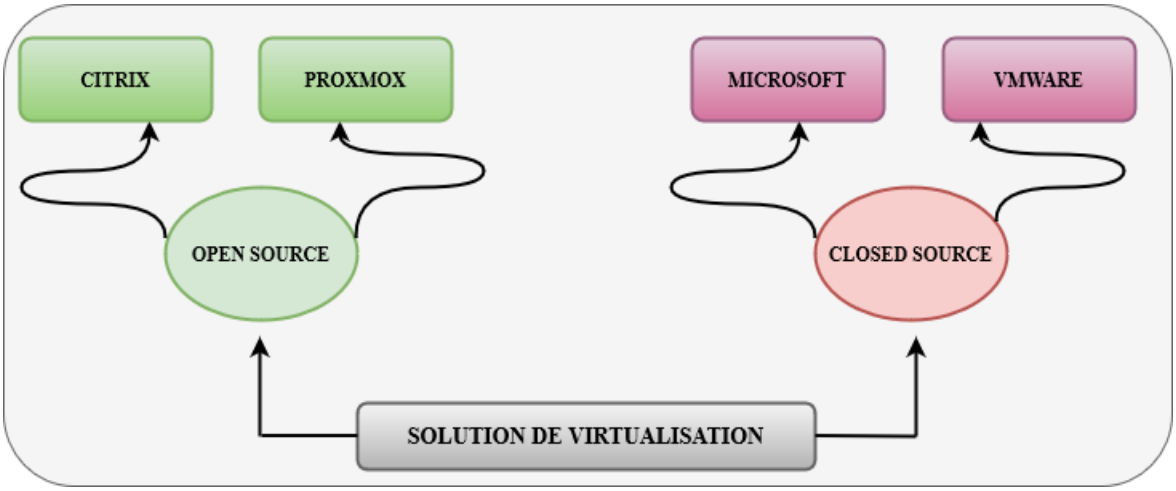

Figure II.7 Illustration des types de solutions.

II.5 Types d'infrastructure

II.5.1 Infrastructure non convergée

Dans une infrastructure informatique non convergée, les composants essentiels tels que le stockage, le réseau et les serveurs fonctionnent de manière autonome, avec peu ou pas de partage de ressources entre eux. Chaque élément est généralement géré séparément

Cela signifie que chaque composant nécessite son propre ensemble de matériel dédié et souvent des logiciels spécifiques pour son fonctionnement. Par conséquent, les ressources peuvent être sous-utilisées, car chaque domaine doit être dimensionné pour répondre à des charges de travail potentiellement maximales, même si elles ne surviennent que rarement.

Cette approche peut conduire à une complexité accrue de la gestion et à des coûts plus élevés, car il faut investir dans plusieurs infrastructures distinctes et former des équipes spécialisées

pour les gérer. De plus, elle peut rendre difficile l'évolutivité et l'adaptabilité de l'infrastructure pour répondre aux besoins changeants de l'entreprise [12].

II.5.2 Infrastructure convergée

Une infrastructure convergée représente une approche moderne et intégrée à la gestion des ressources informatiques au sein d'une organisation. Contrairement aux infrastructures traditionnelles où les composants tels que le stockage, le réseau et les serveurs sont gérés et provisionnés de manière distincte, une infrastructure convergée consolide ces ressources dans une seule plateforme unifiée.

Dans une infrastructure convergée, les ressources sont regroupées dans une architecture intégrée. Cela peut se faire à travers des solutions matérielles dédiées ou des logiciels de gestion qui orchestrent et automatisent les opérations sur différents composants. Parmi les avantages clés de l'infrastructure convergée est sa capacité à fournir une meilleure exploitation des ressources.

En consolidant les ressources dans une seule plateforme, les capacités peuvent être allouées de manière plus efficace et dynamique en fonction des besoins et simplifie le déploiement et l'évolutivité des application [12].

II.5.3 Infrastructure hyperconvergée

L'hyperconvergence (HCI) est une approche qui consolide les éléments essentiels de l'infrastructure, tels que le traitement, le stockage, le réseau et la virtualisation, dans un pool de ressources partagées au sein d'un même nœud, généralement des serveurs.

Cette intégration de toutes les fonctionnalités dans une couche logicielle distincte de l'infrastructure caractérise l'approche software defined [12].

Les avantages d'une infrastructure hyperconvergée sont multiples

- Réduction de la consommation énergétique grâce à une utilisation plus efficace des ressources.
- Simplification du data center en éliminant le besoin de stockage externe et de switches.

- Évolutivité de type "scale-out", permettant d'ajouter simplement de nouveaux nœuds pour augmenter la capacité du système.
- Fiabilité et sécurité accrues grâce à la redondance intégrée et à la réplication des données.
- Haute disponibilité pour garantir un accès continu aux applications et aux données.
- Simplification de la gestion grâce à une interface centralisée, ce qui permet d'optimiser l'utilisation des ressources et de réduire la complexité opérationnelle [12]

II.6 Tendance des solutions de stockage

vSAN (Virtual Storage Area Network) vSAN est une technologie de stockage définie par logiciel développée par VMware. Elle transforme les ressources de stockage locales des serveurs en un pool de stockage partagé et hautement disponible, créant ainsi une architecture de stockage virtualisée. Cette solution offre une gestion simplifiée, une évolutivité dynamique et une haute disponibilité pour les environnements virtualisés, tout en réduisant les coûts et en améliorant les performances [9].

ISCSI ISCSI offre une solution économique pour connecter des dispositifs de stockage et des serveurs. Cette approche simplifie la gestion du stockage, améliore l'accessibilité des données et permet une croissance évolutive sans investissements matériels majeurs. L'implémentation de l'iSCSI améliore les capacités de reprise après sinistre et garantit une haute disponibilité pour les applications critiques [9].

VxRail VxRail est une plateforme d'infrastructure hyperconvergée développée par Dell EMC en partenariat avec VMware. Elle intègre des serveurs, du stockage et des logiciels de virtualisation dans un seul appareil, offrant ainsi une solution de déploiement rapide et simplifiée pour les environnements virtualisés. VxRail assure une évolutivité linéaire, une gestion centralisée et une performance optimale, tout en réduisant la complexité opérationnelle et les coûts [9].

II.7 L'automatisation

L'automatisation informatique consiste à développer des instructions et des processus reproduisibles à l'aide de logiciels, dans le but de limiter ou de réduire l'interaction humaine

avec les systèmes informatiques. Par exemple, il est possible d'automatiser le provisionnement de nouveaux systèmes, de cloud ou de machines virtuelles (VM). Bien que cette tâche puisse être effectuée manuellement, l'automatisation est préférable et plus efficace, surtout à grande échelle. Elle représente un élément essentiel de l'optimisation et de la transformation numérique de l'environnement informatique [10].

Parmi les domaines clés de l'automatisation, on trouve

- **Migration automatisée** Cette approche permet à toute entreprise de se préparer à une variété de scénarios potentiels, comme les pannes matérielles, les problèmes virtuels ou la mauvaise utilisation des ressources, qui peuvent entraîner des temps d'arrêt. La migration automatisée garantit la disponibilité des ressources, optimise l'utilisation des ressources en équilibrant la charge et prolonge la durée de vie des ressources [10].

- **Déploiement de services** Le déploiement de services ou d'applications, ainsi que la création de tickets de service, sont réalisés de manière fiable en configurant les services requis dès le départ et en lançant les applications et leurs utilitaires de manière transparente et compréhensible [10].

- **Collecte de données** Interroger rapidement les équipements pour recueillir des données telles que le modèle et la version logicielle, qui sont utilisables pour planifier des mises à jour ou analyser des problèmes [10].

- **Configuration des équipements** Envoyer rapidement des modifications de configuration aux périphériques, qu'il s'agisse de modifications mineures telles que l'ajout de l'adresse IP d'un nouveau serveur, ou de modifications plus significatives [10].

- **Sécurité et conformité** Définir des politiques de sécurité, de conformité et de gestion des risques, puis les intégrer dans des étapes automatisées dans l'infrastructure pour garantir un niveau de sécurité et de conformité constant [10].

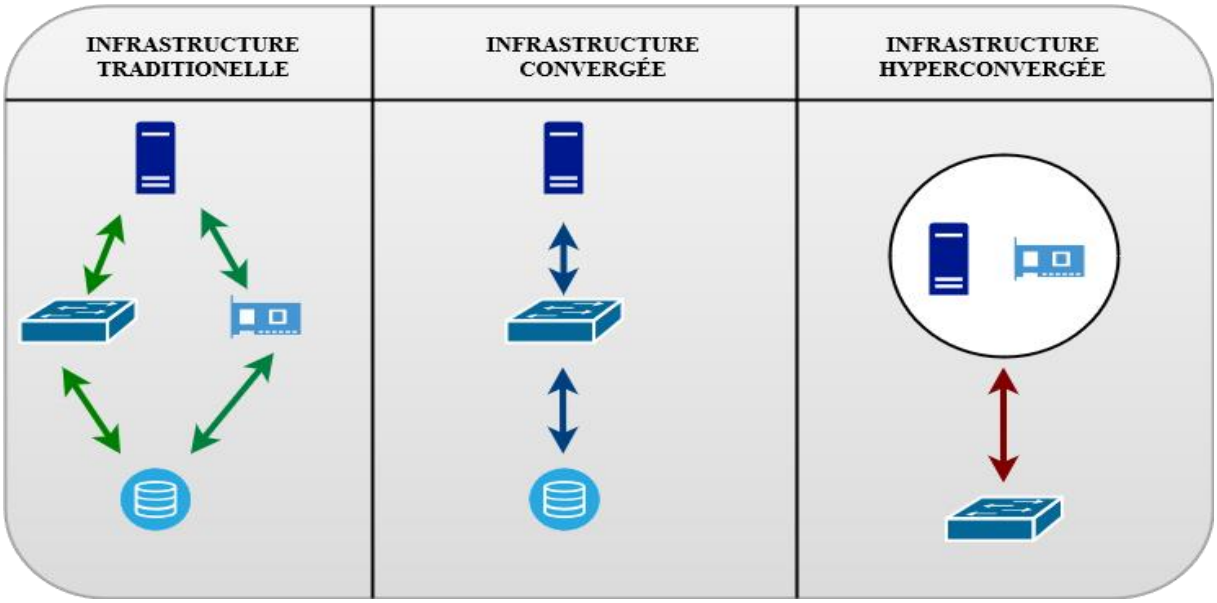

Figure II.8 Les différentes types d'infrastructure informatique.

II.8 Etude comparative

La mise en perspective entre les solutions favorisant la production et celles alignées avec les technologies et les exigences actuelles des entreprises est examinée dans le but de déterminer leur pertinence et leur adéquation aux besoins du marché contemporain et se fait selon plusieurs critères

II.8.1 Selon l'hyper-convergence

Les approches de l'hyperconvergence (HCI) varient selon les fournisseurs, certains privilégiant la virtualisation du stockage et la gestion des données, tandis que d'autres se concentrent d'abord sur la virtualisation des serveurs.Selon les évaluations récentes des principaux analystes de l'industrie, Gartner et Forrester, VMware et Nutanix restent des leaders dans le domaine du HCI en 2023/2024.

Les analystes reconnaissent la position de leader de VMware en matière de stratégie et de vision, tandis que Nutanix est salué pour ses solutions actuelles et ses offres, en particulier pour sa "gestion simplifiée et son extension de capacité sans interruption".

En outre, Dell EMC et HPE ont renforcé leur présence dans le HCI avec leurs solutions respectives VxRail et SimpliVity, toutes deux développées en partenariat avec VMware. En partenariat avec VMware) et SimpliVity (développée en collaboration avec VMware) [16].

II.8.2 Selon la virtualisation

Avant de prendre une décision sur l'hyperviseur à choisir, il est essentiel de réaliser une évaluation approfondie de chaque solution. Cette évaluation devrait se concentrer sur les besoins spécifiques de votre organisation en termes de performances, de fonctionnalités, de compatibilité et de coûts. Une fois que vous aurez analysé ces aspects, vous pourrez déterminer quelle solution répond le mieux à vos exigences opérationnelles et budgétaires [16].

Fournisseurs	**Microsoft**	**VMware**	**Citrix**
Produit	Windows Hyper-V 2023	VSphere 7	Citrix Hypervisor 9.1
RAM par Host	512 logiques	5 TB	288 logiques
CPU par Host	24 TB	16 TB	1000
VM par Host	1024	1024	32 pour 1 Gb 16 pour 10 Gb
Cartes réseaux physique par Host	32 pour 1 Gb 16 pour 10 Gb	16	1,5 TB
RAM par VM	1 TB pour génération 1 121 TB pour génération 2	6 TB	32
vCPU par VM	1 TB pour génération 1 121 TB pour génération 2	128	2 TB
Taille disque par VM	64 TB pour VHDX 2 TB pour VHD	62 TB	Produit de base Open Source gratuit : Uniquement pour la prise en charge de VM. Pour plus de fonctionnalités, des éditions premium sont disponible.
Prix	Entre 630,24 € et 3 607 €	Entre 501$ et 6 545 $	Le coût peut varier en fonction de la version de vSphere, des fonctionnalités choisies et du niveau de support, mais peut être plus élevé que autres solutions.

Tableau II.1 Etude comparative des acteurs de la virtualisation.

A partir de ces différentes comparaisons techniques qui montrent clairement que VMware assure

- Intégration étroite avec l'écosystème Windows pour une gestion simplifiée.
- Coût compétitif, notamment pour les entreprises utilisant déjà des licences Windows.
- Extensibilité pour une large gamme de scénarios d'entreprise, y compris la virtualisation des postes de travail et le cloud hybride.

La lumière de ces comparaisons techniques, il est évident que VMware offre plusieurs avantages

- Une flexibilité accrue grâce à un large choix de fonctionnalités et de licences.
- Des configurations physiques et virtuelles d'excellente qualité.
- Un support technique fiable pour les clients en cas de dysfonctionnement ou de pannes.
- Une gamme étendue de produits couvrant divers axes et technologies, ce qui permet aux clients de rester fidèles au même fournisseur à l'avenir, même s'ils optent pour la virtualisation du réseau ou la migration vers un cloud hybride, par exemple.
- VMware continue de dominer le marché mondial de la virtualisation, avec une part de marché estimée à 78,2 % en 2023.

Opter pour la solution VMware, en particulier vSphere, offre toujours à votre entreprise une infrastructure hautement disponible et continue, répondant ainsi à ses besoins actuels et futurs. Cette solution se distingue toujours par sa flexibilité, sa qualité, son support technique fiable, son évolutivité et sa durabilité, offrant ainsi une assurance pour le développement et la croissance de votre entreprise [16].

En outre, VMware a apporté des améliorations significatives à vSAN et vSphere dans ses dernières versions, notamment :

- **VSAN 8.0** Améliorations des performances, de l'efficacité et de la sécurité, ainsi qu'une prise en charge étendue des charges de travail conteneurisées.

- **VSphere 8.0** Nouvelles fonctionnalités de sécurité, de gestion et de performances, ainsi qu'une prise en charge améliorée des environnements multi-cloud.

Ces améliorations renforcent encore la position de VMware en tant que leader du marché HCI, offrant aux entreprises une solution fiable et évolutive pour leurs besoins d'infrastructure virtualisée [16].

II.8.3 Selon la sécurité

Comme nous l'avons vu dans le 1er chapitre l'aspect sécurité est un enjeu majeur dans une infrastructure informatique, dans ce même chapitre nous avons introduit les pare-feu, un dispositif incontournable qui assure la sécurité de notre réseau puisque rappelons-le il agit comme un filtre entre deux zone qui sont les zones interne "zone Trust" et les zones externe "zone Untrust", cependant avec l'évolution constante des technologies en général les pare-feu ont connu eux aussi une évolution on parle alors de pare-feu traditionnel et des pare-feu modernes ou "Next Generation".

Dans ce volet nous allons étudier le principe de fonctionnement de ces deux types de pare-feu ainsi que donner leurs spécifications et leurs différentes fonctions [16].

II.8.3.1 Pare-feu traditionnel

Pour cette étude nous allons prendre comme exemple le firewall ASA (Adaptive Security Appliance) de Cisco, c'est une solution de sécurité solide mise en place pour protéger les infrastructures des menaces émanant d'internet. Le Cisco ASA surveille, contrôle et filtre le trafic réseau entrant et sortant selon des règles prédéfinies.

Sa fonction principale est de prévenir les intrusions non autorisées en analysant le trafic réseau et en appliquant des politiques de sécurité strictes pour bloquer ou autoriser le flux de données.

Le firewall Cisco ASA permet la mise en œuvre d'un filtrage niveaux 3 et 4 avec des ACL, il permet aussi le filtrage niveau 7 sur la couche applicative mais seulement pour le trafic en clair (HTTP) c'est à dire un trafic non chiffré, avec l'avènement du protocole HTTPS, qui a apporté aspect sécuritaire et intégrité et authenticité qui manquais au protocole HTTP ce qui fait que ASA n'est pas en mesure de filtrer le trafic HTTPS dans la couche applicative [14]

Même si Cisco ASA est une solution robuste elle reste en quelque sorte vulnérable sur certain aspect à savoir

- Ne supporte pas la reconnaissance des applications (application awarness).
- Ne supporte pas l'inspection des fichiers pour la détection malware.
- Ne supporte pas le contrôle des utilisateurs ou groupe d'utilisateurs pour l'accès à internet (identity awarness).
- Le filtrage des URL n'est pas supporté pour le HTTPS.
- Ne supporte pas le décryptage (HTTPS) [14].

II.8.3.2 Pare-feu Next Generation

Le firewall de nouvelle génération (Next-Generation Firewall - NGFW) est une solution avancée de sécurité réseau conçue pour répondre aux défis croissants de la cybersécurité. Contrairement aux pare-feu traditionnels, les NGFW intègrent des fonctionnalités de sécurité supplémentaires telles que la prévention des intrusions, la détection des logiciels malveillants, le filtrage de contenu et la visibilité avancée sur le trafic réseau.

Ils sont venus compléter les lacunes des pare-feu traditionnel.

Comme nous l'avons vu dans le 1er chapitre l'aspect sécurité est un enjeu majeur dans une infrastructure informatique, dans ce même chapitre nous avons introduit les pare-feu, un dispositif incontournable qui assure la sécurité de notre réseau puisque rappelons-le il agit comme un filtre entre deux zone qui sont les zones interne (zone Trust) et les zones externe (zone Untrust), cependant avec l'évolution constante des technologies en général les pare-feu ont connu eux aussi une évolution on parle alors de pare-feu traditionnel et des pare-feu modernes ou (Next Generation).

Dans ce volet nous allons étudier le principe de fonctionnement de ces deux types de pare-feu ainsi que donner leurs spécifications et leurs différentes fonctions.

Ce qui rend les nouveaux firewall plus intéressants c'est leur capacité à inspecter et à analyser le trafic réseau à un niveau plus profond, en tenant compte non seulement des adresses IP et des ports, mais aussi du contenu des paquets de données eux-mêmes. Cela permet aux NGFW d'identifier et de bloquer les menaces sophistiquées telles que les attaques par exploitation de vulnérabilités, les attaques de phishing et les logiciels malveillants basés sur le contenu [15].

Les NGRW sont dotées de deux composants essentiels

- FMC (Firepower Management Center) Le Firepower Management Center est une plateforme de gestion centralisée qui permet aux administrateurs de configurer, surveiller et gérer efficacement leurs appareils de sécurité réseau Cisco Firepower, y compris les pare-feu de nouvelle génération (NGFW), les dispositifs de prévention des intrusions (IPS), et autres. Le FMC offre une interface utilisateur graphique conviviale qui permet une gestion unifiée des politiques de sécurité, la visualisation des événements de sécurité en temps réel, la gestion des signatures d'intrusion et des mises à jour logicielles, ainsi que des capacités avancées de reporting et de génération de rapports [15].

- FTD (Firepower Threat Defense) Firepower Threat Defense est le systè.me d'exploitation des appareils de sécurité réseau Cisco Firepower, y compris les pare-feu de nouvelle génération (NGFW) et les dispositifs de prévention des intrusions (IPS). Il combine la puissance du pare-feu traditionnel avec des fonctionnalités de sécurité avancées telles que la prévention des intrusions, la détection des logiciels malveillants, la visibilité du trafic réseau et la protection contre les menaces avancées. Le FTD offre une protection multicouche contre les cybermenaces, en utilisant à la fois des technologies de signature et de comportement pour détecter et bloquer les attaques en temps réel [15].

II.8.3.3 Choix du pare-feu

Les pare-feu ASA et les NGFW peuvent tous deux être utilisés pour fournir un accès à distance VPN sécurisé. Cependant, les pare-feu ASA peuvent être plus utiles lorsqu'une entreprise souhaite une solution VPN accès distant dédiée, certaines grandes entreprises préfèrent déployer un ou plusieurs firewalls pour le VPN seulement et dédier d'autres firewalls (NGWF) pour l'inspection et l'analyse approfondie du trafic contre les menaces internet, ce qui permet d'alléger le fonctionnement des firewalls en partageant les ressources, la charge et les taches, ainsi pour des raisons de couts, les entreprises continuent à investir sur le firewall ASA comme passerelle VPN dédiée et utiliser les autres fonctionnalités du firewall Next-Generation comme l'AMP (Advanced Malware Protection), IPS (Intrusion Prevention System), Security Intelligence, URL Filtering et SSL Decryption.

Bien que les NGFW offrent des fonctionnalités de sécurité avancées, les pare-feu ASA restent une option viable pour les déploiements d'accès à distance VPN nécessitant une faible consommation de ressources et un coût inférieur.

Et à cause des ressources en termes de CPU, RAM et Disque limitées dans notre station de travail et parce que l'objectif de notre déploiement est de mettre en place un VPN accès distant sécurisé, notre choix s'est porté sur le pare-ASA [15].

II.9 Conclusion

À la lumière de ce chapitre, il est évident que la virtualisation joue un rôle crucial dans l'optimisation des performances des serveurs. Dans le but de répondre efficacement aux besoins actuels des clients, plusieurs solutions ont été présentées, mettant en avant les différents acteurs majeurs de la virtualisation. Toutefois, le domaine de la virtualisation et de l'automatisation est fortement concurrentiel, avec la présence de multiples acteurs.

En outre la sécurité tel que nous l'avons vu reste nécessaire pour le bon fonctionnement des entreprises et garantir l'intégrité des données et des services.

Dans le prochain chapitre, nous aborderons la conception de la solution, en explorant plus en détail les stratégies et les outils nécessaires pour mettre en place une infrastructure virtualisée, automatisée et sécurisée répondant aux besoins spécifiques des entreprises.

Chapitre III

Conception de la solution

III. Introduction

L'évolution rapide des solutions de virtualisation a profondément remodelé le paysage des systèmes d'administration et des infrastructures d'entreprise, transcendant divers secteurs d'activité. Ces technologies, véritables catalyseurs de transformation, offrent un éventail de bénéfices allant bien au-delà de la simple réduction des coûts et de la flexibilité opérationnelle. Elles façonnent également la performance des systèmes, intimement liée à l'architecture physique sous-jacente, sa configuration et les composants qui la composent. Dans ce contexte, l'automatisation et la migration des machines virtuelles émergent comme des impératifs incontournables pour satisfaire les exigences évolutives des entreprises modernes, véritables moteurs de l'innovation.

C'est dans ce paysage en perpétuelle mutation que s'inscrit notre chapitre, focalisé sur une solution particulière. Cette solution combine une approche stratégique de virtualisation avec une configuration matérielle robuste, visant à garantir une disponibilité maximale des services et à automatiser le processus de migration des machines virtuelles. En explorant cette approche novatrice, notre objectif est de dévoiler les mécanismes essentiels permettant de maximiser l'efficacité opérationnelle et d'assurer une gestion agile des ressources informatiques.

Nous enrichirons ce chapitre d'une section dédiée à la sécurité et à l'accès à distance via des réseaux privés virtuels (VPN), soulignant l'importance cruciale de la protection des données et des communications dans un environnement de plus en plus interconnecté et exposé aux cybermenaces.

III.1 Architecture globale de la solution

La solution souhaitée s’articule sur une solution de virtualisation des ressources traditionnelles RAM, CPU avec une couche de stockage, une couche d’automatisation de migration de service et de haute disponibilité. Elle permet ainsi de couvrir tout le nécessaire pour la construction d’une infrastructure hyperconvergée et en formant le Cloud privé du client sur un data center avec un ensemble d’équipements qui s’intègre de manière harmonieuse avec cette dernière.

L’automatisation de migration des VM et les services fournis par les serveurs hébergés sur ces dernières, sera aussi assuré dans le cas de pannes ou de problèmes d’utilisation de ressources.

Toute l'infrastructure sera joignable via un accès privé virtuel à travers un pare-feu virtuel placé au même niveau que nos serveurs, ou les identifiant des différents utilisateurs seront hébergées dans un serveur ISE.

La solution comprend le réseau, les systèmes, le stockage, les services et la gestion en abordant tous les aspects

- Disponibilité et de continuité du business.
- Optimisation des ressources.
- Adaptabilité et évolutivité de la solution.
- Sécurité.
- Automatisation de migration des VM et de la haute disponibilité de services.
- Accès à distance sécurisé.

La conception globale de la solution est illustrée dans la figure ci-dessous.

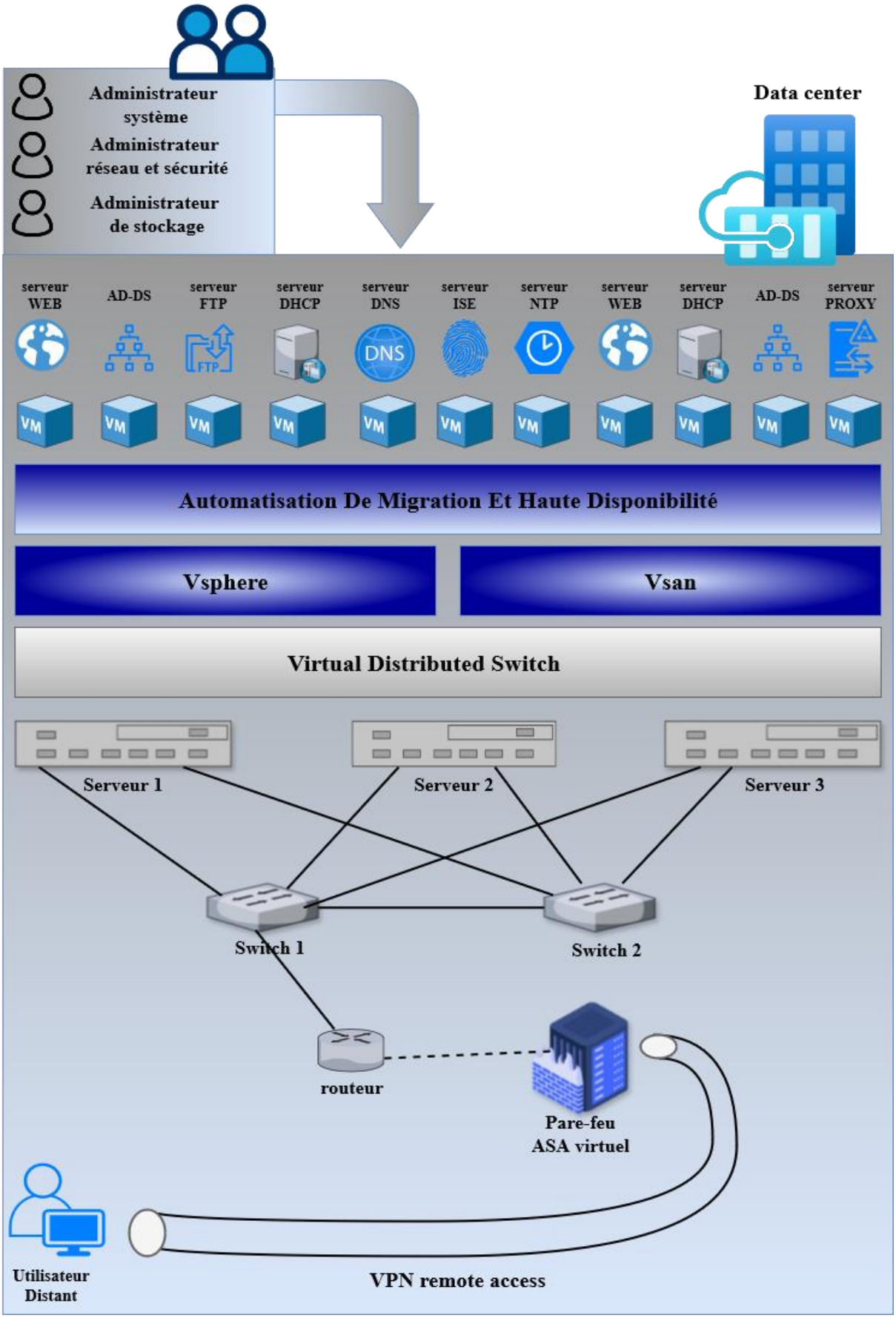

Figure III.9 Schéma de l'architecture globale.

III.1.2 Plan de segmentation niveau 3

Pour notre structure nous allons travailler avec la plage d'adresse privé 172.16.X.X/24 qui est recommandée par le constructeur VMware qui s'inscrivent dans les meilleures pratiques

Nos adresses seront attribuées comme indiqué dans le tableau ci-dessous

Réseau	Adresse IP	Description
Management	172.16.11.0/24	VLAN d'accès et de gestion
Production	172.16.12.0/24	VLAN de production et d'accès aux services des serveurs
vMotion	172.16.13.0/24	VLAN de production et d'accès aux services des serveurs
vSan	172.16.14.0/24	VLAN de service de Stockage

Tableau III.2 Plan d'adressage IP.

III.2 Composants physiques

Les composants physiques de l'architecture sont

- Trois serveurs physiques
- Deux switchs physiques
- Un routeur.

Dans le cadre de notre projet de fin d'étude nous allons utiliser pour le déploiement de notre infrastructure comme serveur un ordinateur portable DELL PRECISION 5510 avec une RAM de 64 GO et un stockage de 1 TO.

Et ceci grâce à un outil de virtualisation de poste de travail créé par la société VMware : VMware Workstation.

III.3 Infrastructure virtualisée

Pour la solution de virtualisation, nous opterons pour le logiciel VMware, reposant sur l'hyperviseur vSphere ESXi.

III.3.1 Vsphere

VMware vSphere constitue une plateforme de virtualisation réputée, redéfinissant les centres de données en des infrastructures informatiques virtualisées et simplifiées. Cette solution permet aux organisations informatiques de délivrer des services flexibles et fiables. VMware vSphere gère de vastes ensembles d'infrastructures, tels que les unités centrales, le stockage et les ressources réseau, en tant qu'environnement opérationnel dynamique et continu.

Le vSphere offre des fonctionnalités intégrées de gestion, d'optimisation des ressources, d'administration des centres de données et d'automatisation des opérations centralisées. Ces avantages se traduisent par des économies substantielles, une efficacité opérationnelle accrue, une polyvalence renforcée et une prestation de services informatiques améliorée.

Les principaux éléments de vSphere comprennent le client web vSphere, l'hyperviseur ESXi et le serveur vCenter. Ces composants interagissent de manière synergique pour offrir une expérience de virtualisation complète et performante [17].

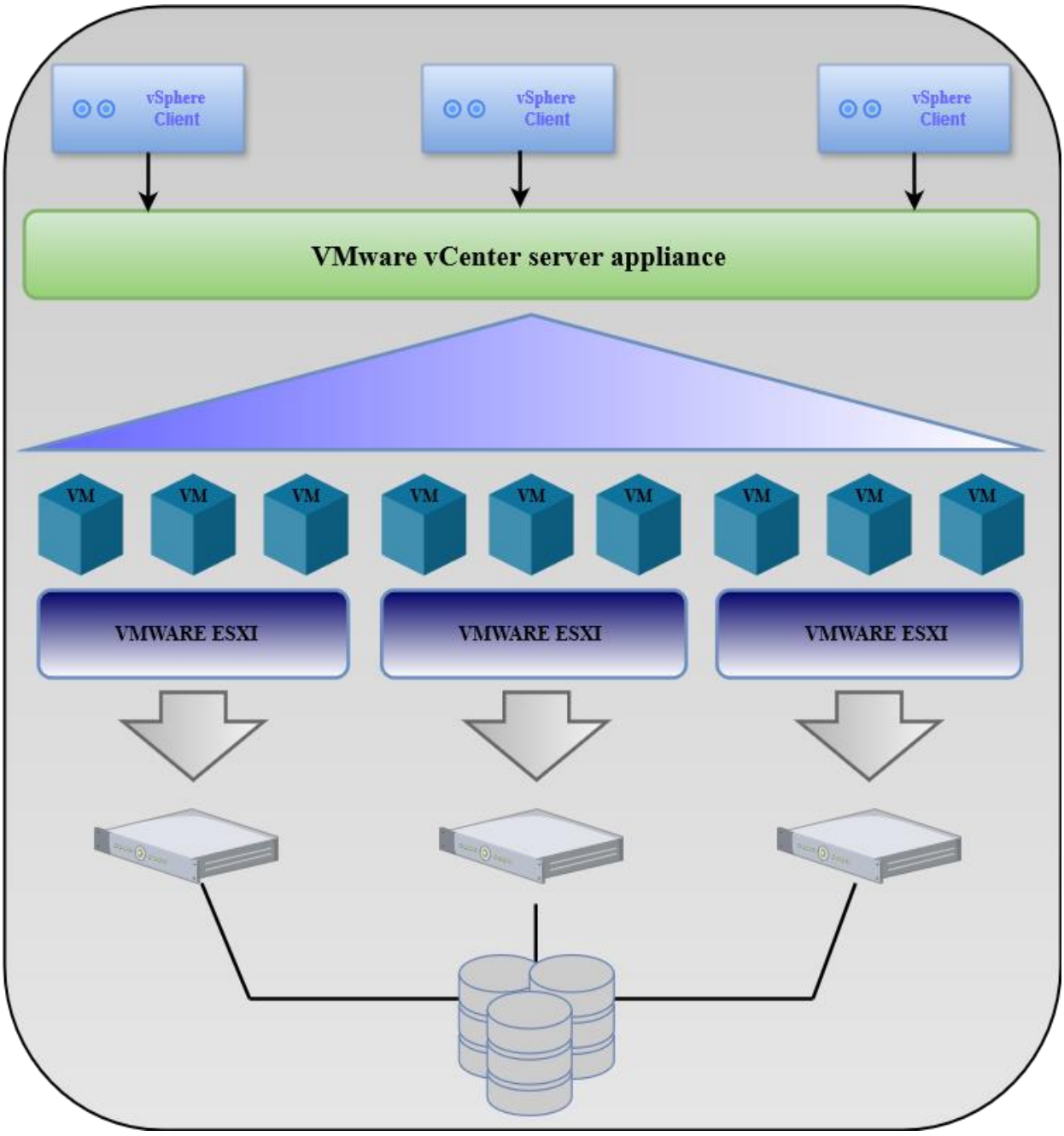

Figure III.10 Schéma de vSphere.

III.3.2 vShpere web client

Le vSphere Web Client se distingue comme une interface utilisateur graphique multiplateforme, offrant une gamme complète de fonctionnalités pour l'administration et la gestion des hôtes ESXi et du système vCenter Server. Dotée d'une architecture modulaire extensible, cette interface est conçue pour les administrateurs, les équipes de support et les propriétaires de machines virtuelles. Elle permet un accès à distance via différents navigateurs web [17].

III.3.3 VMware ESXi

ESXi représente un hyperviseur de type 1 développé spécifiquement par VMware, offrant la possibilité de créer et de faire fonctionner des machines virtuelles. Sa fonction principale consiste à partitionner les ressources matérielles, à consolider les serveurs et à allouer dynamiquement les ressources en fonction des besoins fluctuants.

Il permet une gestion flexible et efficace des ressources, garantissant une utilisation optimale des capacités disponibles tout en assurant une performance maximale des machines virtuelles [17].

III.3.4 VMware Virtual Center Server

Ce service joue le rôle d'administrateur central pour les hôtes ESXi connectés à un réseau, offrant à l'administrateur la capacité de gérer, configurer et provisionner les machines virtuelles à partir d'un emplacement centralisé. Il fournit une vue unifiée présentant toutes les machines physiques hébergeant les machines virtuelles, offrant ainsi une gestion simplifiée et efficace. Parmi ses fonctionnalités intégrées figurent vMotion, HA (High Availability), DRS (Distributed Resource Scheduler) et VDS (Virtual Distributed Switch), offrant une gamme étendue d'outils pour optimiser les performances et la disponibilité des machines virtuelles [17].

III.3.5 Clusters

Un cluster représente un regroupement d'hôtes, où l'ajout d'un hôte à ce cluster intègre automatiquement ses ressources dans un pool partagé comprenant processeurs, mémoire et stockage. Ce regroupement permet une gestion centralisée des ressources de chaque hôte. Les clusters VMware offrent la possibilité de mettre en œuvre des solutions avancées telles que la haute disponibilité et l'équilibrage de charge, ainsi que des solutions de stockage évolutives, garantissant ainsi une efficacité opérationnelle optimale et une capacité de traitement accrue [17].

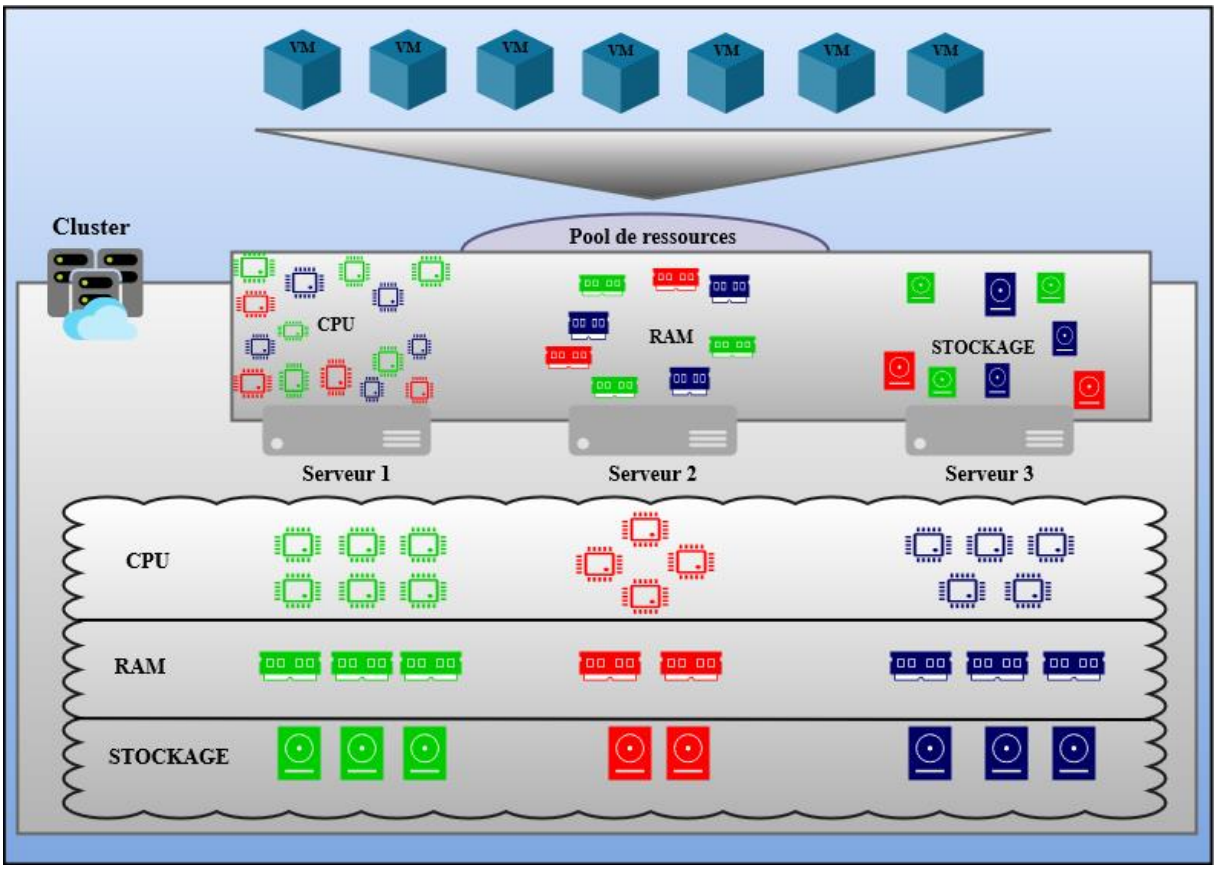

Figure III.11 Schéma de cluster.

III.4 Connectivité

Dans VMware vSphere, la mise en réseau virtuelle repose sur l'utilisation de deux types de commutateurs virtuels. Ces derniers facilitent la communication entre les machines virtuelles et leur connexion au réseau physique.

III.4.1 VMware VSS

Le Virtual Standard Switch (VSS) est un composant essentiel de l'infrastructure de virtualisation, assurant la connectivité réseau entre les hôtes et les machines virtuelles. Il fonctionne comme un commutateur Ethernet physique, contrôlant le flux de trafic réseau.

Le VSS détecte automatiquement les machines virtuelles connectées à ses ports virtuels. Pour étendre le réseau, il peut se connecter à des commutateurs physiques via des adaptateurs Ethernet physiques, appelés "ports de liaison montante". Les cartes réseau physiques des hôtes (vmnic) sont reliées à ces ports de liaison montante, établissant la connectivité réseau.

Les machines virtuelles possèdent des adaptateurs réseau (vNIC) connectés à des groupes de ports sur le VSS. Chaque groupe de ports utilise une ou plusieurs cartes réseau physiques pour gérer le trafic. Sans connexion à une carte réseau physique, les machines virtuelles d'un même groupe de ports ne peuvent communiquer qu'entre elles.

Les groupes de ports sont des ensembles logiques de ports virtuels dans le commutateur virtuel, permettant aux administrateurs d'appliquer des politiques spécifiques. Ils sont identifiés par des étiquettes de réseau uniques, définies au niveau de l'hôte. De plus, chaque groupe de ports peut être assigné à un VLAN (Virtual Local Area Network) pour segmenter efficacement le trafic réseau, les hôtes et les machines virtuelles, le VSS fournit une infrastructure réseau fiable et extensible, essentielle au fonctionnement efficace des environnements virtualisés [17].

III.4.2 VMware VDS

Le Virtual Distributed Switch (VDS) représente un commutateur unique opérant sur l'ensemble des hôtes reliés dans un data center, simplifiant ainsi la gestion du réseau pour plusieurs hôtes. Il centralise le provisionnement, l'administration et la surveillance des réseaux virtuels. La configuration du VDS est uniformément déployée à tous les hôtes associés au commutateur, offrant ainsi une cohérence réseau à l'échelle du data center.

Le VDS se compose d'un plan de gestion, situé dans vCenter Server, qui permet la configuration des VDS, des liaisons NIC, des adaptateurs uplink et des VLAN. Parallèlement, il inclut un plan de données, local sur chaque hôte, qui assure la mise en œuvre concrète des configurations réseau. Cette architecture introduit des concepts pour une configuration réseau homogène et cohérente, facilitant ainsi la gestion et l'administration des infrastructures virtuelles à grande échelle [17].

Les éléments fondamentaux du VDS comprennent plusieurs concepts clés essentiels à une configuration réseau harmonieuse :

Groupe de ports de liaison montante Ce groupe contient une ou plusieurs liaisons montantes (uplink), permettant de mapper les cartes réseau physiques des hôtes aux liaisons montantes configurées sur le commutateur distribué.

Groupe de ports distribués Ce groupe assure la connectivité réseau des machines virtuelles (VM) d'un côté, tout en gérant le trafic vmkernel de l'autre. Ces groupes de ports sont automatiquement répliqués pour chaque hôte à partir de vCenter Server.

VMkernel Cet adaptateur est dédié à la gestion du trafic des hôtes, notamment pour des fonctions telles que vMotion, le stockage réseau, Fault Tolerance et vSAN.

En raison de son efficacité, de sa gestion centralisée garantissant facilité et sécurité dans les manipulations, de son automatisation réduisant la charge de travail des administrateurs, de sa capacité d'extension aisée sur l'ensemble de l'infrastructure, ainsi que de son excellente interopérabilité avec le SDN, notre préférence se porte sur le VDS comme switch virtuel.

III.5 Migration

La migration des machines virtuelles (VM) est le processus de déplacement d'une VM d'un hôte physique vers un autre, au sein du même cluster ou d'un cluster différent. Cette opération est essentielle pour diverses raisons :

Équilibrage de la charge de travail La migration des VM permet d'optimiser l'utilisation des ressources en équilibrant la charge de travail sur les serveurs physiques. Cela garantit que tous les hôtes fonctionnent à des niveaux de performance optimaux [18].

Défaillance de l'hôte physique En cas de défaillance d'un hôte physique, les VM qui y sont hébergées doivent être migrées vers d'autres hôtes pour éviter les interruptions de service [18].

Maintenance Les opérations de maintenance planifiées, telles que les mises à jour du micrologiciel ou les réparations matérielles, nécessitent la migration des VM hors de l'hôte affecté [18].

Amélioration des performances La migration des VM vers des hôtes plus puissants ou dotés de fonctionnalités avancées peut améliorer les performances des applications et réduire la latence [18].

Consolidation des ressources La migration des VM vers un nombre réduit d'hôtes peut libérer des ressources sur d'autres hôtes, permettant une consolidation et une utilisation plus efficace de l’infrastructure.

Les techniques de migration des VM varient en fonction de l'environnement de virtualisation utilisé. Cependant, elles visent toutes à garantir un transfert transparent des VM, en préservant leur état et leur connectivité réseau [18].

VMware vMotion

VMware vMotion est une fonctionnalité essentielle de vCenter server qui permet aux entreprises de minimiser les temps d'arrêt en migrant des machines virtuelles en cours d'exécution d'un hôte ESXi vers un autre. Cela est possible grâce à deux types de migration :

Migration à chaud Déplace les VM en cours d'exécution sans interruption pour les utilisateurs ou perte de service [18].

Migration à froid Éteindre la VM avant de la migrer, ce qui est utile pour les opérations de maintenance planifiées.

VMotion permet aux administrateurs d'effectuer rapidement des opérations de maintenance sans impact sur les utilisateurs. Par exemple, ils peuvent migrer des VM vers des hôtes plus puissants pour améliorer les performances ou vers des hôtes différents pour équilibrer la charge de travail.

Parallèlement à VMotion, Storage vMotion permet de migrer les disques et le fichier de configuration d'une VM en service d'une banque de données à une autre, sans interruption de service. Cela est particulièrement utile pour les opérations liées au stockage, telles que l'équilibrage de la charge, la mise à niveau des baies de stockage ou la récupération après sinistre.

Ensemble, VMotion et Storage vMotion offrent une flexibilité et une disponibilité accrues aux environnements virtualisés, permettant aux entreprises de maintenir des opérations ininterrompues et d'optimiser l'utilisation des ressources [18].

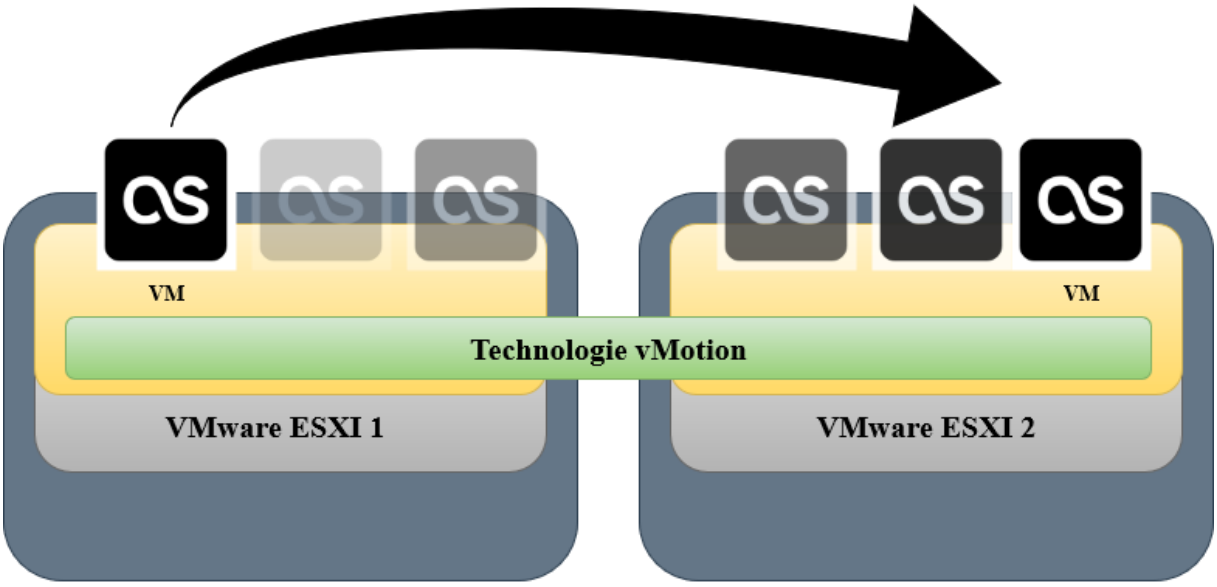

Figure III.12 Illustration de la migration.

III.6 Automatisation de Migration

La haute disponibilité des services est cruciale pour toute infrastructure informatique moderne. Pour y parvenir, l'automatisation de la migration des serveurs virtualisés est essentielle [18].

Ce mécanisme garantit la continuité des services en migrant automatiquement les machines virtuelles en cas de

- Pannes matérielles.
- Problèmes de virtualisation.
- Utilisation excessive des ressources.

L'automatisation de la migration se concentre sur deux aspects principaux

- **Continuité du service** Les VM sont migrées de manière transparente vers d'autres hôtes, minimisant les temps d'arrêt et assurant une disponibilité ininterrompue des applications [19].

- **Optimisation des ressources** En équilibrant la charge de travail entre les hôtes, l'automatisation de la migration optimise l'utilisation des ressources, prolongeant la durée de vie des serveurs et réduisant les coûts d'exploitation [19].

vCenter Server est le composant central de la gestion de l'infrastructure VMware. Il fournit un point de contrôle unique pour les administrateurs, leur permettant de gérer et de surveiller plusieurs hôtes VMware ESXi connectés sur un réseau.

- L'une des fonctions clés de vCenter Server est le contrôle d'admission. Il vérifie si un cluster dispose de ressources suffisantes pour prendre en charge de nouvelles machines virtuelles. Si ce n'est pas le cas, vCenter Server émet un message d'avertissement [19].

Pour faciliter la migration automatisée des VM, vCenter Server introduit deux fonctionnalités principales

III.6.1 DRS (Distributed Resource Scheduler)

VMware DRS (Distributed Resource Scheduler) est un composant essentiel de vCenter Server qui améliore l'allocation des ressources et la consommation d'énergie dans les environnements virtualisés. Il surveille en permanence l'utilisation des ressources sur tous les hôtes ESXi et les machines virtuelles d'un cluster [20].

Équilibrage de charge DRS optimise l'utilisation des ressources informatiques (CPU et RAM) en équilibrant la charge de travail entre les hôtes. Il détecte les déséquilibres de charge et recommande de migrer les VM vers des hôtes plus appropriés. Ces migrations sont effectuées de manière transparente à l'aide de vMotion, sans temps d'arrêt [20].

Règles d'affinité DRS permet également de contrôler le placement des VM sur les hôtes à l'aide de règles d'affinité. Ces règles peuvent être utilisées pour [20]:

• **Affinité** Maintenir des VM spécifiques ensemble sur le même hôte pour des raisons de performances ou de dépendance.

• **Anti-affinité** Séparer des VM spécifiques pour éviter de les perdre toutes les deux en cas de panne d'hôte.

Fonctionnement

DRS recueille des informations sur l'utilisation des ressources toutes les 5 minutes. Il génère ensuite des recommandations de migration si nécessaire. Ces recommandations peuvent être appliquées manuellement ou automatiquement, selon les paramètres configurés [20].

Avantages

DRS offre plusieurs avantages, notamment [20]

•Optimisation de l'utilisation des ressources, réduisant les coûts d'exploitation

•Amélioration des performances des VM en les plaçant sur des hôtes appropriés

•Réduction des risques de panne en séparant les VM critiques sur différents hôtes

Lien avec HA

Bien que DRS optimise l'allocation des ressources, il ne garantit pas la haute disponibilité. Pour cela, VMware HA (High Availability) est nécessaire. HA surveille en permanence la santé des hôtes ESXi et redémarre automatiquement les VM sur d'autres hôtes en cas de panne.

Le DRS et HA travaillent concomitamment pour fournir un environnement virtualisé hautement disponible et efficace, garantissant la continuité des services et l'optimisation des ressources [20].

III.6.2 HA (High Availability)

VMware HA (High Availability) veille à ce que les machines virtuelles (VM) restent opérationnelles en permanence, même en cas d'événements imprévus. Il regroupe les VM avec leurs hôtes respectifs dans des clusters étroitement surveillés.

Lorsqu'un hôte rencontre une défaillance, HA détecte rapidement l'incident et orchestre la reprise automatique des VM affectées sur d'autres hôtes sains du cluster. Ce processus transparent garantit une continuité de service ininterrompue, minimisant les temps d'arrêt et protégeant les applications critiques contre les interruptions.

Grâce à HA, les entreprises peuvent bénéficier d'une infrastructure virtualisée hautement disponible, assurant la fiabilité et la résilience de leurs systèmes informatiques essentiels [20].

Fonctionnement

Au sein d'un cluster HA, un hôte maître est désigné pour assurer une surveillance constante. Il communique en permanence avec vCenter Server, surveillant l'état de toutes les VM et des hôtes esclaves à un rythme d'une seconde [20].

Cette surveillance vigilante permet à l'hôte maître de détecter rapidement divers types de défaillances d'hôte [20] :

- **Panne soudaine** L'hôte devient inaccessible, ne répondant plus aux pings ou aux signaux de pulsation.
- **Isolation inattendue** L'hôte reste joignable par ping, mais son agent HA cesse de communiquer.
- **Partition réseau** L'hôte perd sa connexion avec l'hôte maître, mais continue d'échanger des signaux de pulsation avec une banque de données.

En cas de détection d'une défaillance, l'hôte maître réagit immédiatement en orchestrant la reprise des VM affectées sur des hôtes sains du cluster. Ce processus transparent garantit une continuité de service ininterrompue, protégeant les applications critiques contre les interruptions.

Surveillance des VM

HA utilise "VM Monitoring" pour détecter les défaillances au niveau des VM. Il vérifie les pulsations régulières et l'activité des E/S du processus VMware Tools exécuté dans chaque VM. Si aucune pulsation ou activité d'E/S n'est reçue, la VM est considérée comme ayant échoué et est redémarrée [18].

Protection des composants des VM

"VM Component Protection" (VMCP) protège les VM contre les défaillances d'accessibilité des banques de données. Si VMCP est activé, HA peut détecter ces échecs et récupérer automatiquement les VM affectées [18].

Avantages

VMware HA offre plusieurs avantages, notamment [20] :

- **Haute disponibilité** Les VM sont redémarrées automatiquement sur d'autres hôtes en cas de défaillance, garantissant la continuité des services.

- **Détection et récupération rapides** HA détecte les défaillances en temps réel et redémarre les VM rapidement, minimisant les temps d'arrêt.

- **Réduction des interventions manuelles** HA automatise le processus de récupération, réduisant la charge de travail des administrateurs.

III.7 Infrastructure de stockage

III.7.1 vSAN

Les solutions de stockage hyperconvergées regroupent les ressources matérielles pour former un pool de stockage partagé, éliminant ainsi les contraintes traditionnelles des réseaux SAN. VMware vSan est une solution de stockage hyperconvergée qui simplifie considérablement la configuration et le provisionnement du stockage.

vSan virtualise les ressources de stockage locales des hôtes ESXi, les transformant en pools de stockage partagés accessibles à tous les hôtes du cluster. Ces pools de stockage partagés sont utilisés par les machines virtuelles, les applications, les services et les fonctionnalités VMware nécessitant un stockage partagé, tels que HA, vMotion et DRS.

vSan est intégré directement dans l'hyperviseur ESXi. Il agrège tous les périphériques de stockage locaux dans une banque de données unique partagée par tous les hôtes du cluster vSan [21]

Groupes de disques

Au sein d'un cluster vSan, chaque hôte ESXi héberge des groupes de disques qui regroupent des périphériques de stockage locaux. Un groupe de disques représente une capacité de stockage sur un hôte, constituée de périphériques physiques offrant des performances et une capacité au cluster.

Tous les groupes de disques doivent obligatoirement inclure un périphérique de cache flash et au moins un périphérique de capacité. Les périphériques de cache sont exclusifs à chaque groupe de disques et ne peuvent être utilisés à d'autres fins [21].

Avantages de vSAN

vSAN offre plusieurs avantages, notamment [21]

- **Simplification du stockage** Élimine le besoin d'un stockage externe partagé, réduisant la complexité et les coûts d'administration.

- **Provisionnement rapide** Provisionnement instantané et automatisé du stockage pour les machines virtuelles, accélérant le déploiement des applications.

- **Haute disponibilité** Intégration étroite avec HA pour garantir la disponibilité continue des machines virtuelles en cas de défaillance d'un hôte.

- **Performances optimisées** Utilisation des périphériques flash pour améliorer les performances des E/S et réduire la latence.

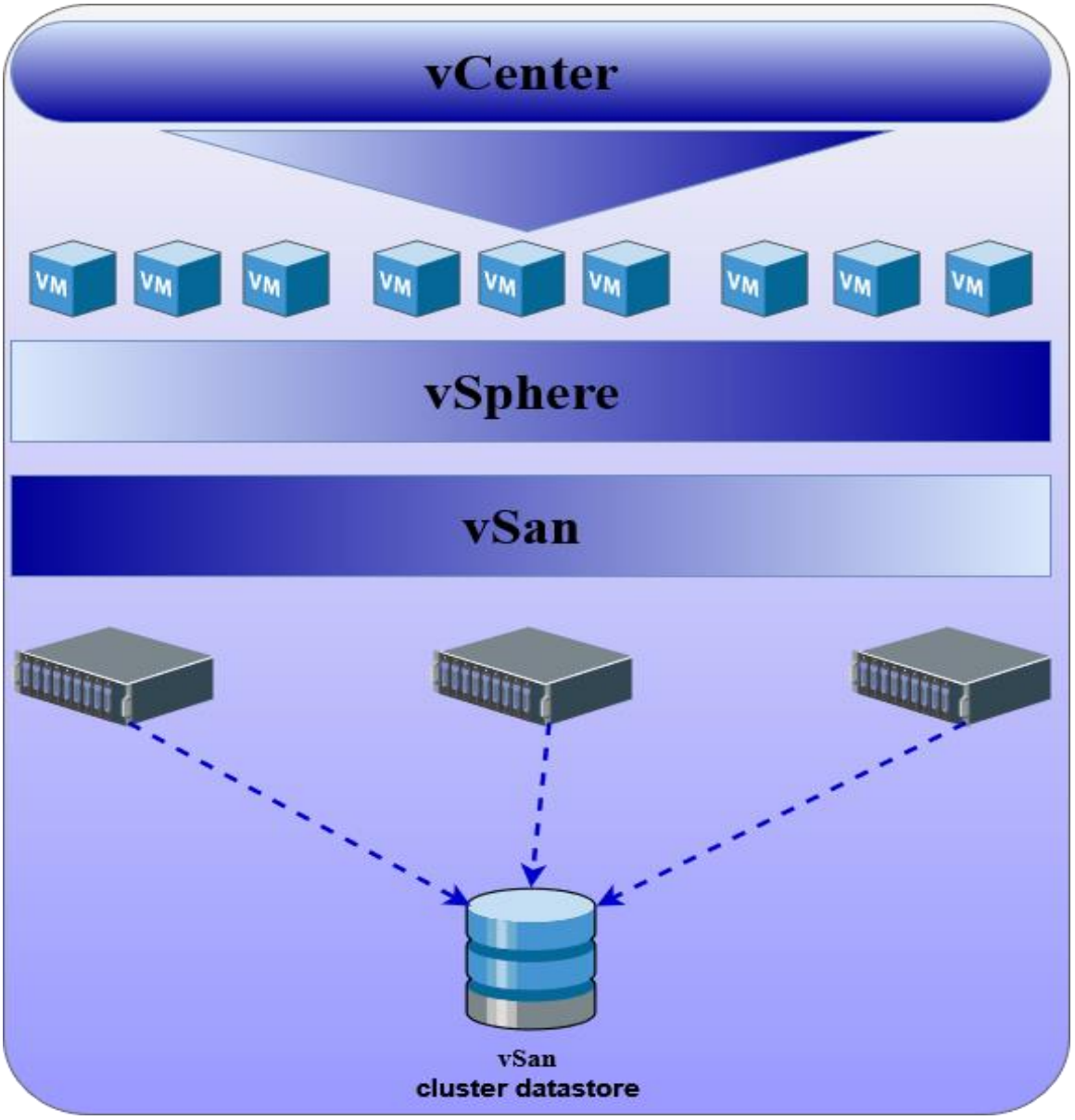

Figure III.13 Illustration du vSan.

III.7.2 ISCSI

Le stockage iSCSI (Internet Small Computer Systems Interface) est une technologie qui permet de transmettre des commandes SCSI sur des réseaux IP, créant ainsi un réseau de stockage évolutif et économique. Cette solution innovante permet de connecter des dispositifs de stockage à des serveurs en utilisant l'infrastructure Ethernet existante, sans nécessiter de matériel dédié coûteux comme dans les réseaux Fibre Channel traditionnels.

Principes de Fonctionnement du Stockage iSCSI

Le protocole iSCSI encapsule les commandes SCSI dans des paquets IP, permettant leur transmission sur un réseau TCP/IP. Cette encapsulation permet de transformer un réseau local (LAN) en un réseau de stockage (SAN).

Les principaux composants d'une infrastructure iSCSI

- **Initiateurs iSCSI** Logiciels ou matériels installés sur les serveurs qui initient les connexions SCSI.
- **Cibles iSCSI** Dispositifs de stockage, tels que les baies de disques ou les serveurs NAS, qui reçoivent et répondent aux commandes SCSI.
- **Réseau IP** Infrastructure Ethernet existante qui transporte les paquets iSCSI entre les initiateurs et les cibles.

III.8 Architecture de services

L'architecture de services, tant du point de vue physique que logique, représente la structure organisée par laquelle notre solution offre ses fonctionnalités.

Elle établit une hiérarchie précise et détermine le déploiement optimal des services. Ces derniers sont hébergés sur des serveurs, lesquels sont à leur tour déployés sur des machines virtuelles, éléments fondamentaux de l'architecture virtualisée que nous avons précédemment détaillée.

Composants de l’architecture de services

Parmi les éléments constitutifs de l'infrastructure des services, on peut évoquer divers composants essentiels

- **Système d'exploitation des serveurs**

Nous avons opté pour Windows Server 2019, l'une des dernières versions du système d'exploitation serveur de Microsoft, en raison de sa familiarité auprès des administrateurs, de ses fonctionnalités étendues et de son support technique fiable.

Ce choix stratégique nous permet d'optimiser les performances de nos serveurs et de bénéficier d'une assistance rapide en cas de problème [21].

- **AD (Active Directory)**

Active Directory est le service d'annuaire mis en œuvre par Microsoft pour les systèmes d'exploitation Windows. Il fournit un système de gestion unifié pour un domaine de sécurité partagé, permettant une authentification et une autorisation centralisées.

Active Directory gère tous les objets d'un réseau local, notamment [21] :

- Machines serveurs et postes de travail
- Ressources et applications
- Comptes d'utilisateurs
- Groupes de sécurité

Active Directory se compose de cinq rôles principaux [21]

- **ADDS (Active Directory Domain Services**) gère les domaines Active Directory et fournit des services d'authentification et d'autorisation. Permet aux utilisateurs d'accéder à des ressources externes en utilisant leurs informations d'identification Active Directory.
- **ADCS (Active Directory Certificate Services)** émet et gère des certificats numériques pour sécuriser les communications et l'authentification.
- **ADRMS (Active Directory Rights Management Services)** Protège les documents et les e-mails contre l'accès non autorisé.
- **ADLDS (Active Directory Lightweight Directory Services)** fournit un service d'annuaire léger pour les environnements où un contrôleur de domaine complet n'est pas nécessaire.

Dans ce travail, nous nous intéressons aux services suivants

- **ADDS (Active Directory Domain Service)**

Comme nous l'avons indiqué juste avant, le ADDS est le rôle d'Active Directory qui gère les comptes d'utilisateurs, les ressources et les applications utilisant les annuaires, telles que Microsoft Exchange Server. Il permet également d'organiser hiérarchiquement les éléments d'un réseau, notamment les utilisateurs, les ordinateurs et les périphériques.

ADDS assure la sécurité grâce à l'authentification d'ouverture de session unique et au contrôle d'accès aux ressources de l'annuaire. Le serveur qui exécute ADDS est appelé contrôleur de domaine.

- **DNS (Domain Name System)**

Dans l'écosystème Windows Server, un rôle essentiel est le DNS (Domain Name System). Ce service permet de convertir les noms de domaine en adresses IP, facilitant ainsi la communication sur le réseau. Dans un environnement Active Directory (AD), le DNS travaille en synergie avec les services de domaine. Pour assurer une intégration harmonieuse, il est recommandé de configurer le DNS sur les mêmes serveurs que ceux hébergeant Active Directory.

- **FTP (File Transfer Protocol)**

Le FTP (File Transfer Protocol) est un outil essentiel en matière de transfert de fichiers entre des ordinateurs connectés à un réseau. Il permet aux utilisateurs d'échanger des fichiers, que ce soit pour partager des données importantes ou accéder à des fichiers stockés à distance.

Cette configuration nous offre un contrôle accru sur l'accès aux fichiers et assure la sécurité de nos données sensibles [21].

Le serveur FTP offre plusieurs fonctionnalités clés [21] :

- **Sécurité renforcée** Tous les transferts de fichiers sont cryptés, garantissant ainsi la confidentialité des données contre tout accès non autorisé.

- **Authentification des utilisateurs** Avant d'accéder aux fichiers, les utilisateurs doivent s'authentifier, ce qui permet de sécuriser davantage l'accès aux données.

- **Gestion fine des autorisations** Les administrateurs peuvent définir des autorisations spécifiques pour chaque utilisateur, contrôlant ainsi précisément qui peut accéder à quels fichiers.

- **Prise en charge des transferts de fichiers volumineux** Le service FTP est capable de gérer efficacement le transfert de fichiers de grande taille, ce qui en fait une solution idéale pour partager des données volumineuses entre utilisateurs.

- **Le protocole NTP (Network Time Protocol)**

Le protocole NTP (Network Time Protocol) est un service crucial dans les environnements informatiques pour synchroniser l'horloge des équipements sur un réseau. Il permet de garantir que tous les appareils ont la même référence temporelle, ce qui est essentiel pour la coordination des activités, la gestion des journaux et la sécurité des systèmes.

Dans notre infrastructure, nous avons configuré le service NTP en tant que client. Cette mise en place nous permet de maintenir une horloge précise et synchronisée surtout entre notre serveur RADIUS et la machine virtuelle ou nous avons installé Active Directory, ce qui est essentiel pour garantir le bon fonctionnement de notre infrastructure [21].

- **IIS - WEB**

Le service web est un élément fondamental de toute infrastructure informatique moderne, permettant aux utilisateurs ou aux clients d'accéder à des ressources et des services via Internet. Dans notre environnement, nous avons déployé et configuré un serveur web dédié que pour répondre aux besoins de nos utilisateurs

Notre serveur web et exclusivement dédié que pour les utilisateurs interne de l’entreprise, ce qui signifie que notre site n’est pas accessible pour internet

En fournissant un service web fiable, sécurisé et performant, nous nous assurons que nos utilisateurs peuvent accéder aux ressources et aux services dont ils ont besoin de manière efficace et sécurisée.

C’est ici que la partie vSphere se termine, nous allons maintenant présenter la 2ème partie de notre projet, celle d’une gestion d’authentification et d’autorisation centralisé, géré par un serveur radius Cisco ISE et de la partie accès distance avec un tunnel VPN [21].

III.9 Intégration Active Directory avec Cisco ISE

Avant d'expliquer le rôle qu'a Cisco ISE dans notre solution, nous allons présenter les groupes et utilisateurs dans le client souhaite en disposer 6 groupes avec 6 utilisateurs afin d'utiliser les groupes Active Directory pour attribuer des privilèges d'accès spécifiques à chaque utilisateur, permettant de créer des politiques d'autorisation granulaires et adaptées aux besoins de chaque groupe [15].

Cependant il est important de noter que les utilisateurs que nous avons créés ne sont pas les vrais utilisateurs ce ne sont que des exemples

Voici les groupes et les utilisateurs correspondants

GROUPE	UTILISATEUR	IDENTIFIANT	SERVICES
IT-ADMIN	Chris meyer	cmeyer	ADDS/DNS/FTP/ISE/WEB
HR	John doe	jdoe	FTP/WEB/DNS
SALES	Anita perez	aperez	FTP/WEB/DNS
FINANCE	Charles connors	cconnors	FTP/WEB/DNS
MARKETING	James smith	jsmith	FTP/WEB/DNS
PARTNERS	Maria pierce	mpierce	WEB

Tableau III.3 Groupes et utilisateurs.

Dans le cadre de ce projet, Cisco ISE a été sélectionné comme solution centrale pour l'authentification, l'autorisation et la journalisation (AAA) du réseau. Cette centralisation vise à renforcer la sécurité et le contrôle d'accès, tout en simplifiant la gestion des utilisateurs et des appareils.

L'intégration de Cisco ISE avec Active Directory que nous allons voir dans le chapitre prochain permet de centraliser l'authentification des utilisateurs et de récupérer leurs informations de groupe. Cette approche permet de définir des politiques d'autorisation granulaires basées sur l'appartenance à un groupe, offrant un contrôle d'accès précis et personnalisé.

Par ailleurs, la journalisation centralisée des activités des utilisateurs par Cisco ISE permet d'obtenir une visibilité complète sur l'utilisation du réseau et de détecter les anomalies potentielles [21].

III.9.1 Authentification

L'authentification est le processus qui garantit que seuls les utilisateurs autorisés peuvent accéder au réseau. Cisco ISE joue un rôle essentiel dans ce processus en s'intégrant à Active Directory. Cette intégration permet à Cisco ISE de vérifier l'identité des utilisateurs en utilisant leurs identifiants et mots de passe stockés dans Active Directory. Grâce à cette intégration, le processus d'authentification est simplifié et sécurisé. Les utilisateurs n'ont plus besoin de mémoriser des identifiants multiples, et Cisco ISE peut garantir que seuls les utilisateurs authentifiés peuvent accéder au réseau. Elle offre une solution efficace et sécurisée pour contrôler l'accès au réseau et protéger les ressources sensibles [22].

III.9.2 Autorisation

Le processus d’autorisation quant à lui garantit que les utilisateurs authentifiés ne disposent que des privilèges d'accès nécessaires pour effectuer leurs tâches. Cisco ISE utilise les groupes Active Directory pour attribuer des privilèges d'accès spécifiques à chaque utilisateur, permettant ainsi de créer des politiques d'autorisation granulaires et adaptées aux besoins de chaque groupe. Par exemple, les membres du groupe "IT-admin" peuvent avoir un accès complet au réseau, leur permettant de gérer les systèmes et les ressources. En revanche, les membres du groupe "SALES" peuvent avoir un accès limité aux ressources de vente, leur permettant de se concentrer sur leurs tâches quotidiennes. Cette approche permet de simplifier la gestion des accès et de garantir que les utilisateurs ne disposent que des privilèges nécessaires pour effectuer leurs tâches, contribuant ainsi à la sécurité et à la productivité du réseau.

Dans le cadre de notre projet nous avons créés 6 groupes avec 6 utilisateurs afin d’utiliser les groupes Active Directory pour attribuer des privilèges d'accès spécifiques à chaque utilisateur, permettant de créer des politiques d'autorisation granulaires et adaptées aux besoins de chaque groupe.

III.9.3 Compatibilité

Accounting en anglais c'est pour la surveillance et l'audit des activités des utilisateurs sur le réseau. Cisco ISE enregistre les informations relatives aux connexions, aux déconnexions et aux accès aux ressources, permettant ainsi de suivre l'activité des utilisateurs et d'identifier les problèmes potentiels [23].

Ces informations peuvent être utilisées pour [23]

- Identifier via quel équipement une connexion a été établi (ordinateur, Smartphone…) ou quel système d'exploitation (Android, Windows, Linux…)
- Surveiller l'activité du réseau et identifier les anomalies ou les tentatives d'accès non autorisées.
- Auditer les activités des utilisateurs pour garantir la conformité aux politiques de sécurité et aux réglementations.

Résoudre les problèmes liés à l'accès au réseau en identifiant les causes des erreurs ou des pannes.

III.9.4 DACL pour les autorisations

Les autorisations d'accès au réseau sont gérées à l'aide de listes de contrôle d'accès téléchargeables (DACL). Ces listes définissent les actions que les utilisateurs sont autorisés à effectuer en fonction de leur appartenance à un groupe. Les DACL permettent de configurer des règles d'accès précises et granulaires, garantissant que les utilisateurs ne disposent que des privilèges nécessaires pour effectuer leurs tâches [22].

Les DACL vont être télécharger sur le pare-feu depuis le serveur radius ou nous les auront configurés au préalable

III.9.5 Scénario de déploiement

Voici le scénario de déploiement que nous prévoyons pour cette partie que nous allons voir étape par étape dans le prochain chapitre

1. Cisco ISE est installé et configuré pour l'intégration avec Active Directory.

2. Des politiques d'autorisation sont créées pour accorder différents niveaux d'accès aux utilisateurs en fonction de leur appartenance à un groupe.
3. Les utilisateurs sont configurés pour utiliser le client AnyConnect pour se connecter au VPN.
4. Lorsqu'un utilisateur tente de se connecter au VPN, Cisco ISE authentifie l'utilisateur auprès d'Active Directory et récupère ses informations de groupe.
5. En fonction de l'appartenance à un groupe de l'utilisateur, Cisco ISE applique la politique d'autorisation appropriée.

III.10 Intégration ASA avec Cisco ISE

Pour que notre firewall ASA puisse appliquer les directives et configuration implémentés sur active directory ains que Cisco ISE, il faut faire l'intégration entre notre pare-feu et notre serveur radius

Le pare-feu ASA et Cisco ISE vont travailler conjointement pour assurer l'authenticité des utilisateurs et pour donner les autorisations adéquates selon les groupes auxquels ils font partie et ce en téléchargeant les ACL que nous avons créé au niveau de Cisco ISE, pour chaque groupe chose que nous allons voir en détails lors du prochain chapitre.

III.11 VPN Remote Access

Notre accès distant sera configuré au niveau du pare-feu ASA, pour permettre aux utilisateurs d'accéder au réseau local et a ces ressources comme s'ils étais physiquement présent sur place

Pour ça on va activer le "web vpn" sur le firewall et configurer une ACL interne qui permet d'accepter une requête de connexion via internet au réseau local ainsi que créer les "group policy" et profile de connexion, ainsi que quelques autres configurations que nous allons voir dans le prochain chapitre [15].

III.12 Conclusion

Dans ce chapitre, nous avons présenté l'étude conceptuelle de notre projet à travers la description, de l'architecture physique et de l'architecture virtuelle. Nous avons également expliqué le processus d'automatisation de migration, le stockage ainsi que la façon dont les services sont fournis par notre solution

Nous avons aussi expliqué sans aller dans le détail du travail conjoint que va faire ASA, AD et Cisco ISE pour gérer les authentifications et les autorisations.

Pour finir, comment l'accès distant va être mis en place.

Dans le chapitre suivant, nous allons exposer les différentes étapes de configuration, et commencer l'implémentation.

Chapitre IV

Implémentation de la solution

IV. Introduction

Apres la présentation de l'architecture de la solution à déployer dans le chapitre précèdent, nous allons consacrer ce chapitre pour la partie implémentation en citant les différentes étapes d'installation et de configuration.

IV.1 Environnement de travail

Pour des raisons de disponibilité du matériel, nous n'avons malheureusement pas pu disposer des serveurs et des équipements réseau nécessaires pour le déploiement de notre solution, par conséquent nous avons opté pour une réalisation sous forme de "Nested Virtualisation" sur une seule machine assez puissante afin de supporter le bon fonctionnement du lab.

Nested Virtualisation ou virtualisation imbriquée, c'est une fonctionnalité qui permet la virtualisation d'une architecture déjà virtualisée. Ce qui signifie la création des machines virtuelles dans ou sur une autre machine elle-même virtuelle : Notons que cette approche n'est faisable que pour des environnements de lab ou d'essai, elle n'est pas du tout valable pour un environnement de production

La figure ci-dessous illustre parfaitement la solution implémentée :

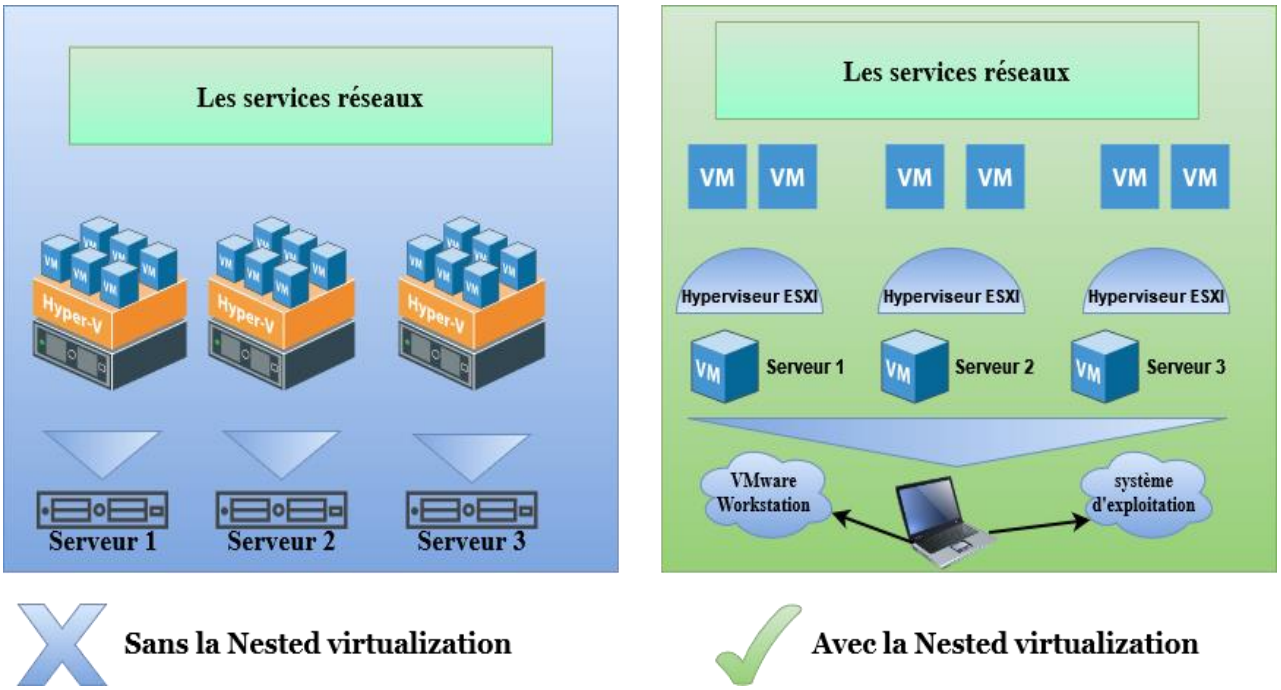

Figure IV.14 Schéma de la solution avec et sans Nested virtualisation.

Les 3 hôtes (serveurs physiques dans notre conception) et contenant les ESXI ou les hyperviseurs de type 1 seront virtualisés dans 3 VM s'exécutant sur un hyperviseur (VMware Workstation) de type 2. Les 3 machines virtuelles peuvent être exportées puis reconfigurées et installées sur des serveurs physiques pour un environnement de production.

IV.1.2 Outils

Comme indiqué précédemment, nous allons utiliser deux composante essentiels (matériel physique et logiciels) lors de notre déploiement.

IV.1.3 Matériel physique

La machine que nous allons utiliser pour cette réalisation est un ordinateur avec les caractéristiques suivants :

- **Fabricant** Dell Inc
- **Modèl** Precision-5510 Laptop.
- **Processeur** Intel(R) Core (TM) i7-6820HQ.
- **Mémoire installée (RAM)** 64 Go.
- **Stockage** interne SSD 1 To.
- **Système d'exploitation** Ubuntu 22.04

IV.1.4 Logiciels

VMware Workstation

C'est un hyperviseur de type 2 créé par la société VMware, Il peut être employé pour établir un cadre d'essai visant à élaborer de nouveaux logiciels ou des architectures complexes, avant leur déploiement effectif sur des équipements physiques.

Version VMware Workstation 17.5.1

FileZilla FileZilla est un logiciel de transfert de fichiers open source utilisé pour la gestion des transferts de fichiers entre un ordinateur local et un serveur distant via les protocoles FTP, FTPS et SFTP.

Version 3.58.0

Putty

Putty est un logiciel open source de client Telnet et SSH. Il offre une interface simple et légère permettant aux utilisateurs d'établir des connexions sécurisées avec des serveurs distants via différents protocoles de communication réseau.

Version Putty 3.24.30

AnyConnect

AnyConnect est une solution de connectivité sécurisée développée par Cisco. Il fournit un client VPN polyvalent, conçu pour permettre aux utilisateurs d'accéder de manière sécurisée aux ressources réseau depuis n'importe où, à tout moment, via Internet. AnyConnect offre une connectivité VPN basée sur les standards, tels que SSL (Secure Sockets Layer) et IPsec (Internet Protocol Security), offrant ainsi un accès sécurisé aux réseaux d'entreprise, aux applications et aux données sensibles.

IV.2 Etapes de configuration

Après la présentation de l'environnement de travail, nous allons passer à l'installation, la configuration et aux tests de la solution.

IV.2.1 Création et configuration des VMnet

Les vmnet sont des réseaux virtuels utilisés pour connecter les machines virtuelles entre elles et avec le réseau physique de l'ordinateur hôte.

Nous aurons besoin de quatre VMnet avec la configuration suivante

- **VMnet 1** pour le traffic management avec une plage d'adresse 172.16.11.0/24.
- **VMnet 2** pour le traffic production avec une plage d'adresse 172.16.12.0/24.
- **VMnet 3** pour le traffic vMotion avec une plage d'adresse 172.16.13.0/24.
- **VMnet 4** pour le traffic vSan avec une plage d'adresse 172.16.14.0/24.

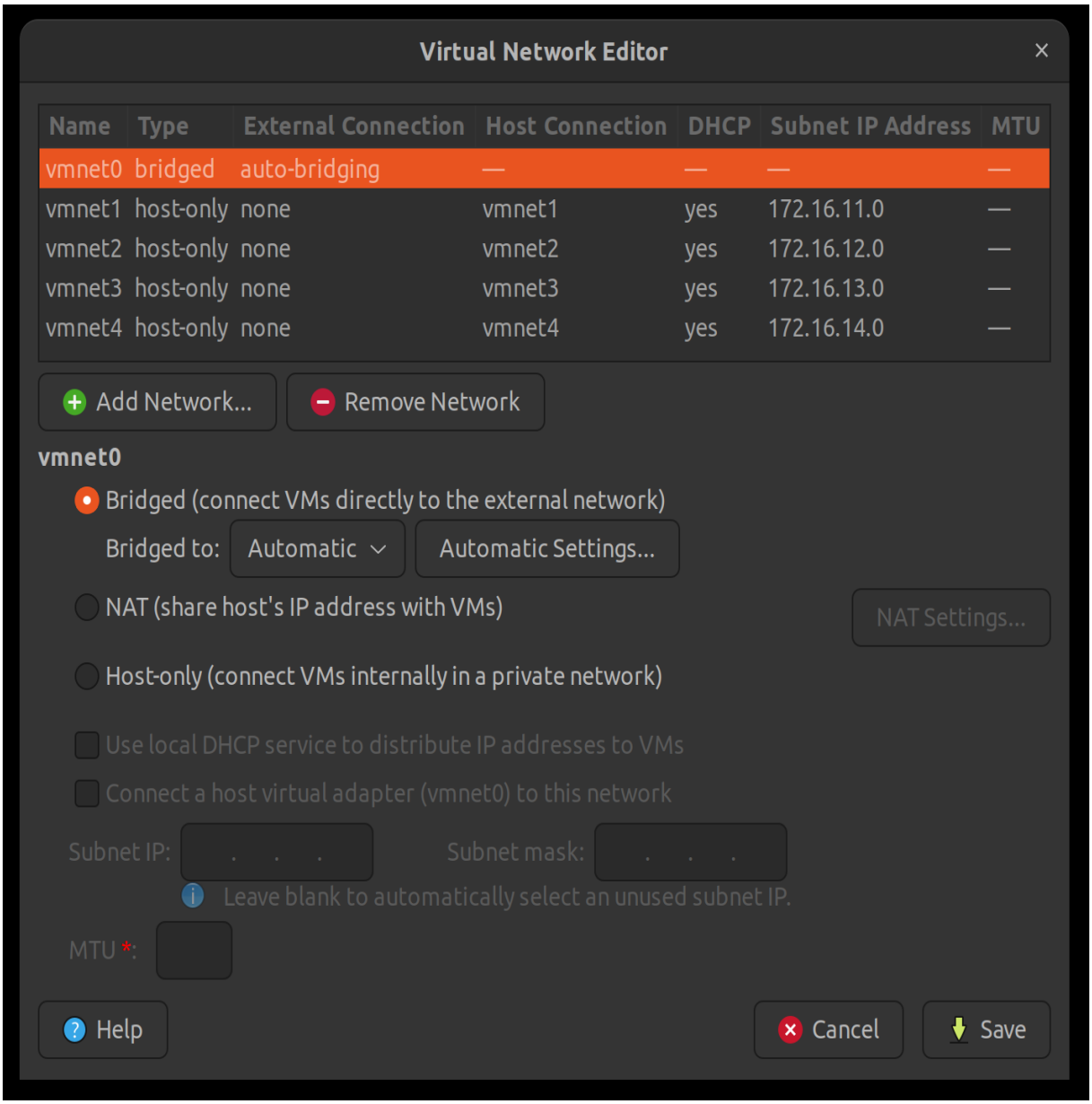

Figure IV.15 Configuration des VMnet sur Workstation.

La carte vmnet 0 est la carte par default qui est créer par le logiciel lui-même, qui est en mode "bridged" ce qui signifie qu'elle nous offre accès vers internet contrairement au vmnet 1, 2, 3 et 4 que nous avons-nous-mêmes créer et configurer en "Host-Only" pour le traffic interne.

IV.2.2 Adressage IP et FQDN

Durant le déploiement de notre solution nous avons suivi les bonnes pratiques recommandées par vmware en termes d'adressage IP, et nous avons fait cet adressage

NOM	ADRESSE IP	FQDN
ESXI 03	172.16.11.12	ESXI03.lab.local
ESXI 04	172.16.11.13	ESXI04.lab.local
ESXI 05	172.16.11.14	ESXI05.lab.local
vCenter	172.16.11.150	vcsa-demo.lab.local
Site IIS	172.16.12.132	Pfe.lab.local
Serveur DNS	172.16.12.132	/
Serveur ADDS	172.16.12.132	Lab.local
Serveur DNS secondaire	172.16.11.131	/
Serveur FTP	172.16.12.132	/
Cisco ISE	172.16.12.100	Ise-pfe.lab.local
ASA Outside	192.168.8.250	/
ASA Production	172.16.12.250	/

Tableau IV.4 Adressage IP et FQDN.

IV.2.3 Installation d'une machine virtuelle Windows server 2019

La structure d'une machine virtuelle repose sur une collection de fichiers qui résident sur un périphérique de stockage. Les principaux fichiers incluent le fichier de configuration (.vmx), le fichier de disque virtuel (.vmdk), le fichier de configuration NVRAM et le fichier journal (.log).

Dans le cadre de notre déploiement nous auront besoin de déployer une machine virtuelle temporaire DC (Domain contrôleurs) au même niveau que les trois serveurs ESXI pour des fins de connectivité de configuration DNS, pour cela nous avons créé une VM Windows server 2019 comme suit dans les figures suivantes :

Apres avoir choisi l'onglet création de nouvelle machine virtuelle nous avons cette interface :

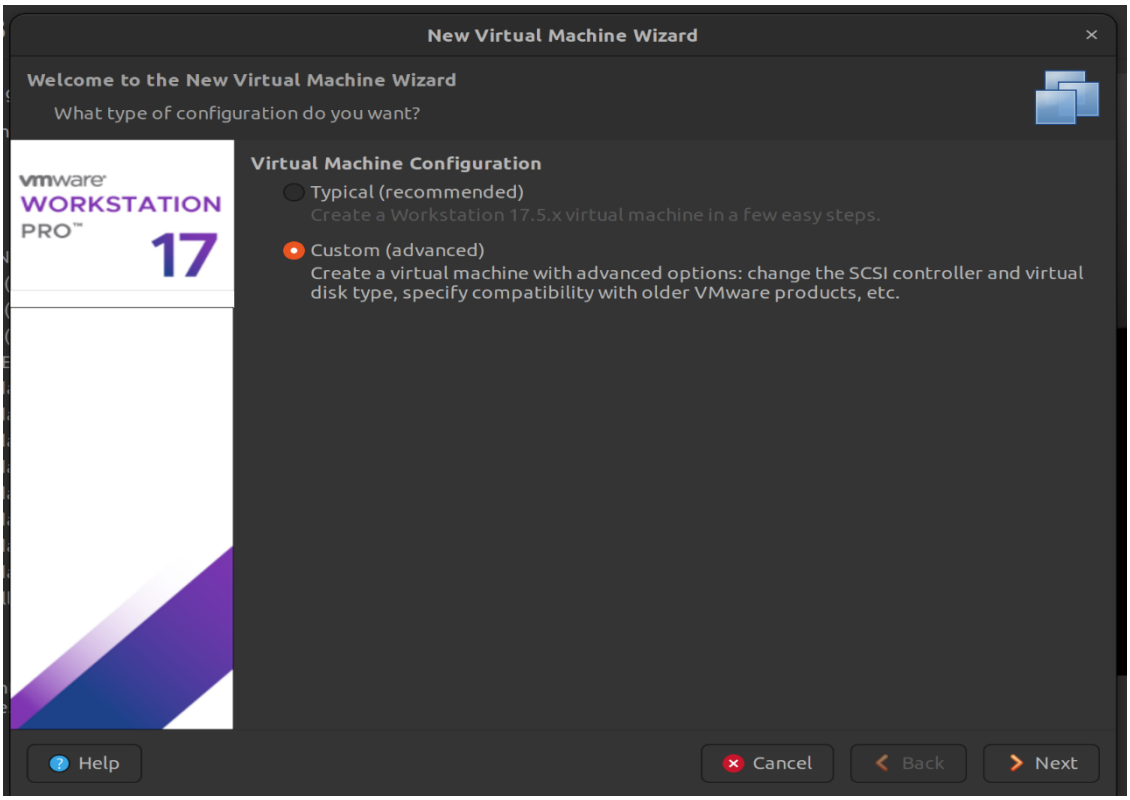

Figure IV.16 Wizard d'installation d'une nouvelle VM.

Cette interface consiste a choisi des parametre pour des fins de compatibilité

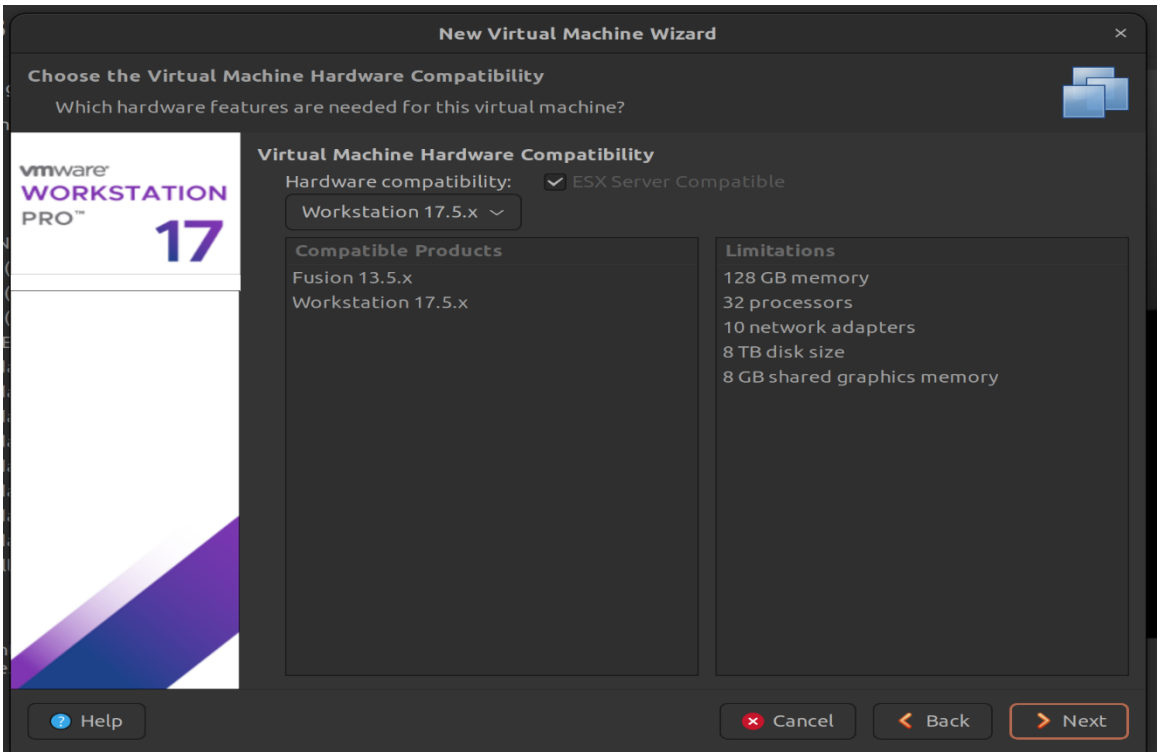

Figure IV.17 Hardware compatibilité.

Nous allons selectionner l'imagie iso Windows server que nous voulons deployer

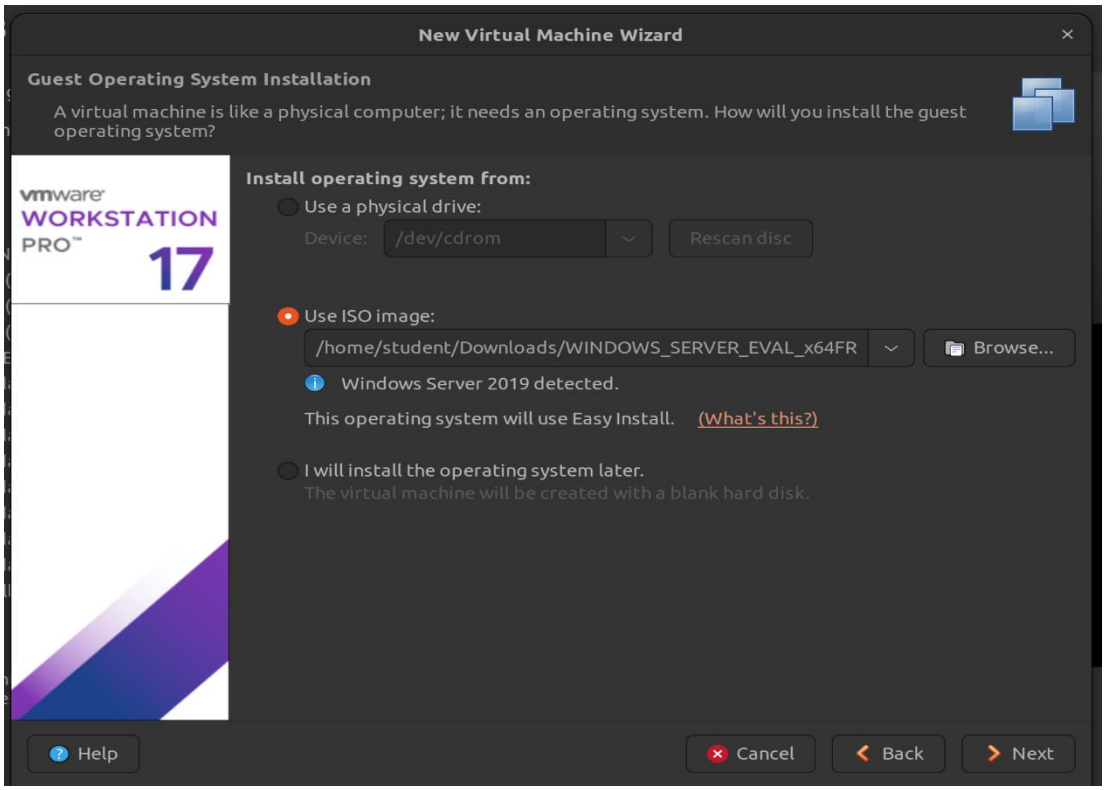

Figure IV.18 Sélectionner l'image iso Windows server 2019.

On nom notre VM et choisissons l'emplacement de sauvegarde

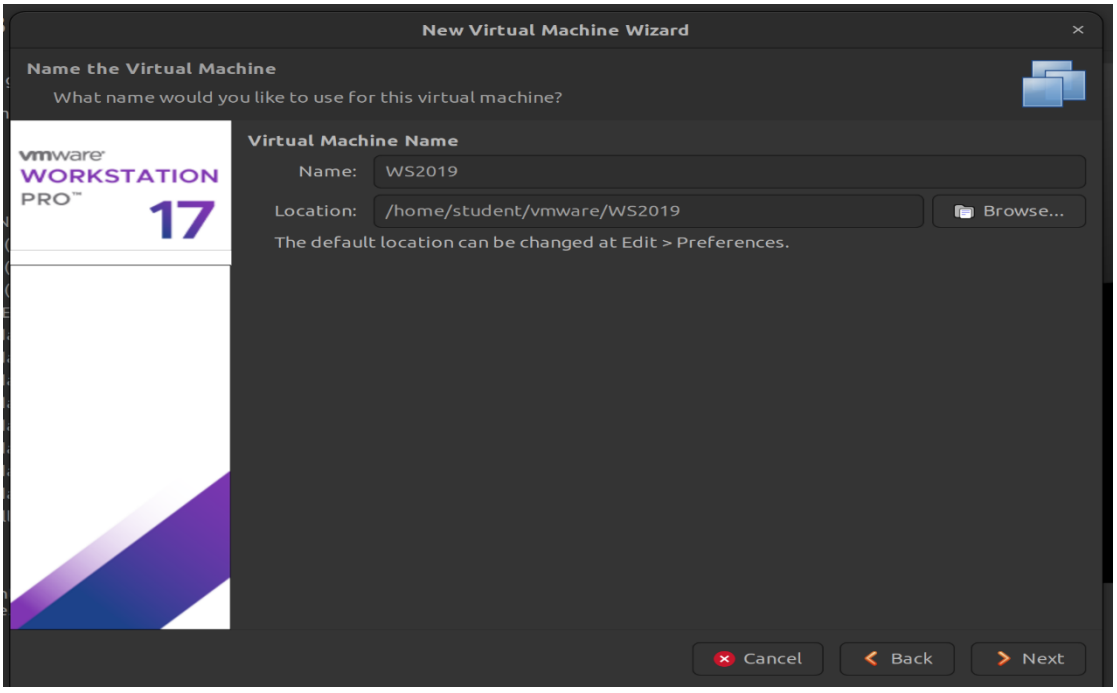

Figure IV.19 Nom et emplacement de la VM.

Pour l'installation on va l'installer à partir du bios

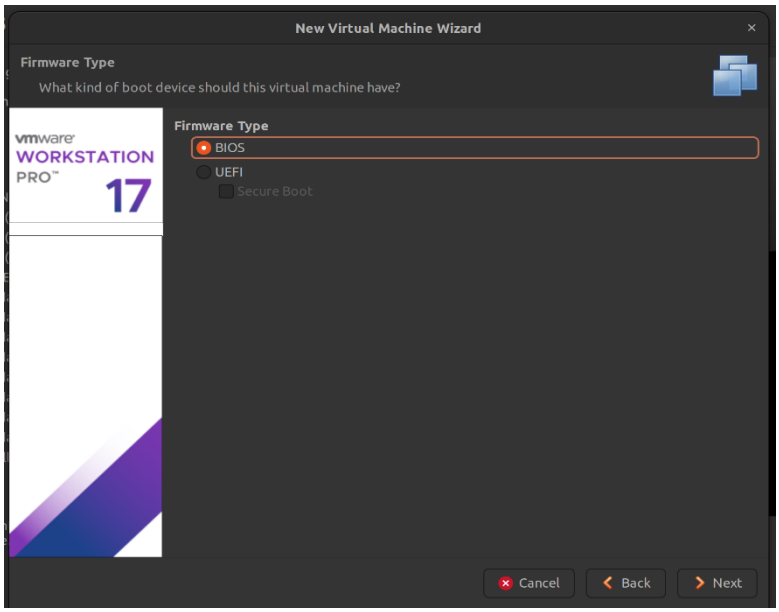

Figure IV.20 Type de boot pour l'installation de la VM.

Les figure suivantes representes l'assignement des ressources que nous voulons attribuer pour notre vm (cpu, ram, carte reseau, mémoire, type de disque)

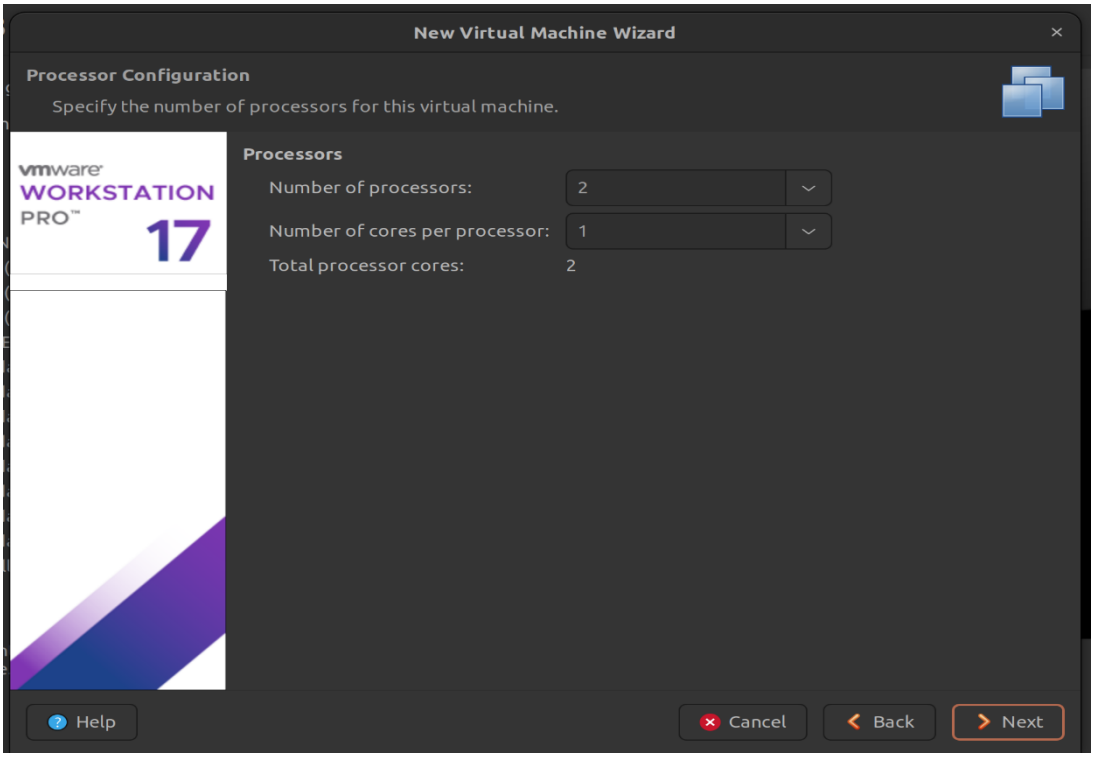

Figure IV.21 Nombre de Cores de processeurs.

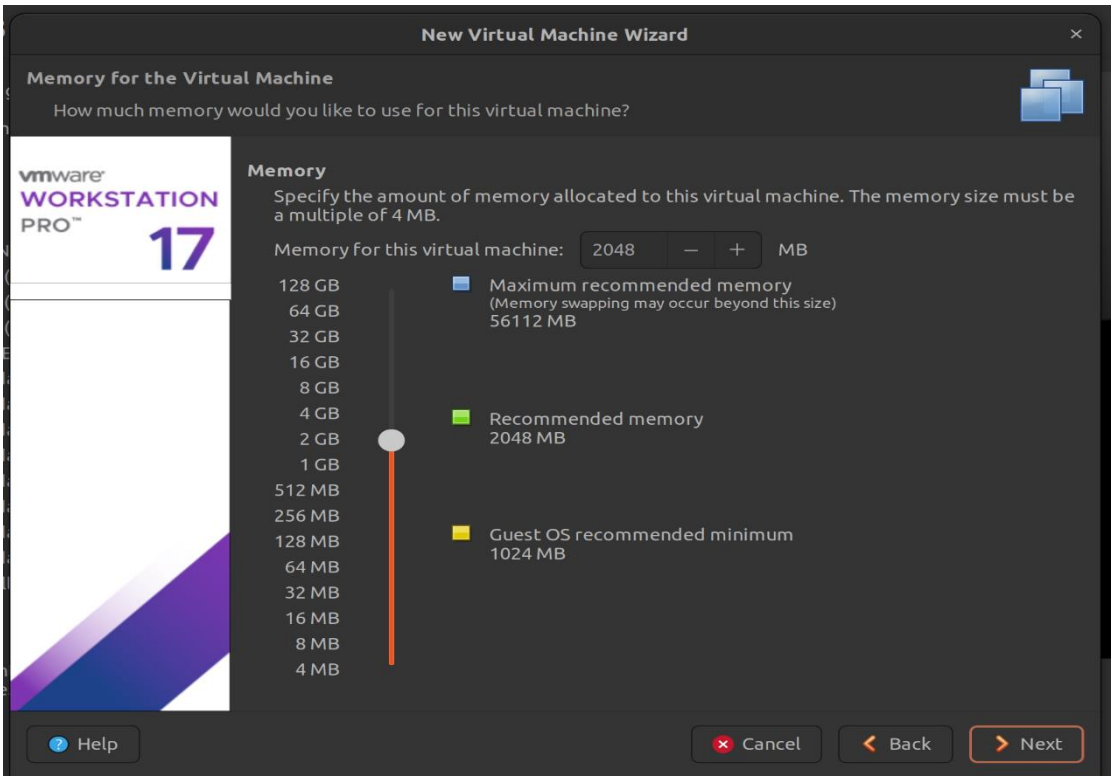

Figure IV.22 Quantité de RAM.

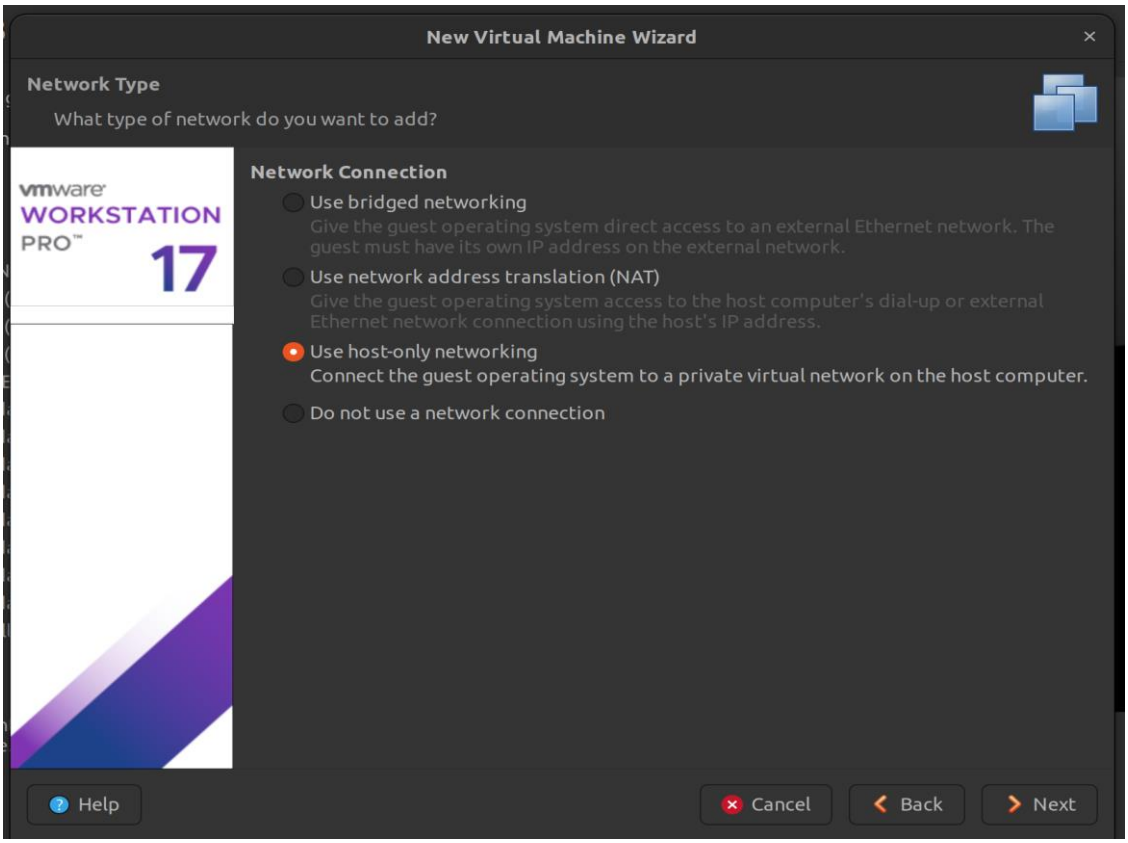

Figure IV.23 Type de la carte réseau.

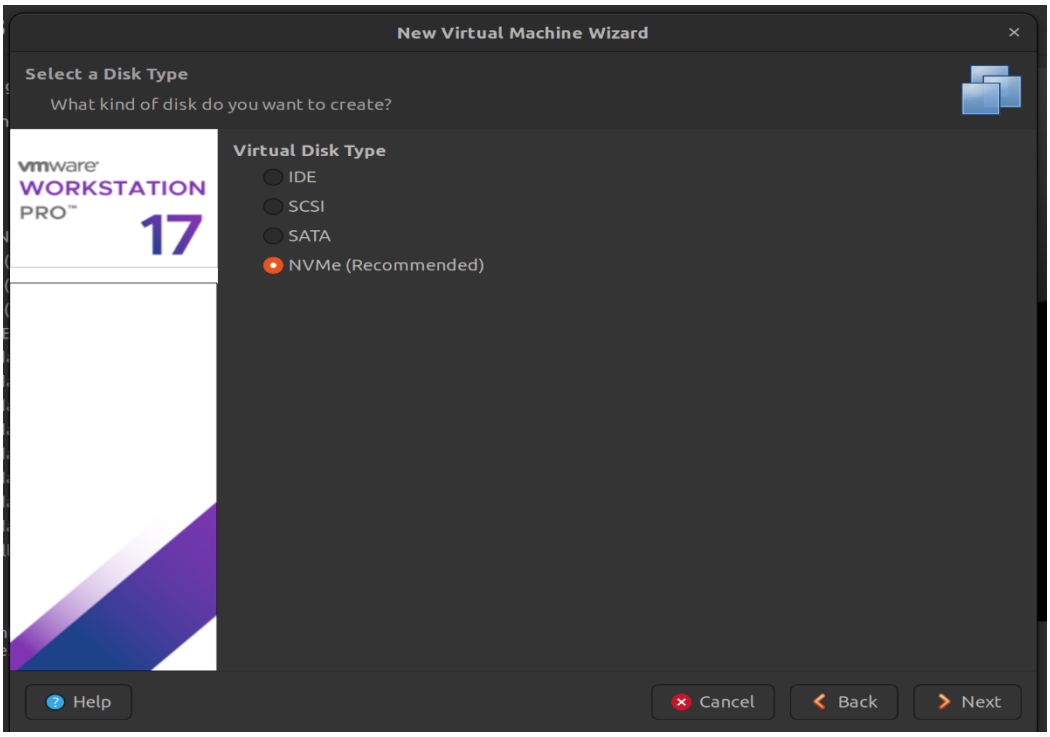

Figure IV.24 Type de disque de stockage.

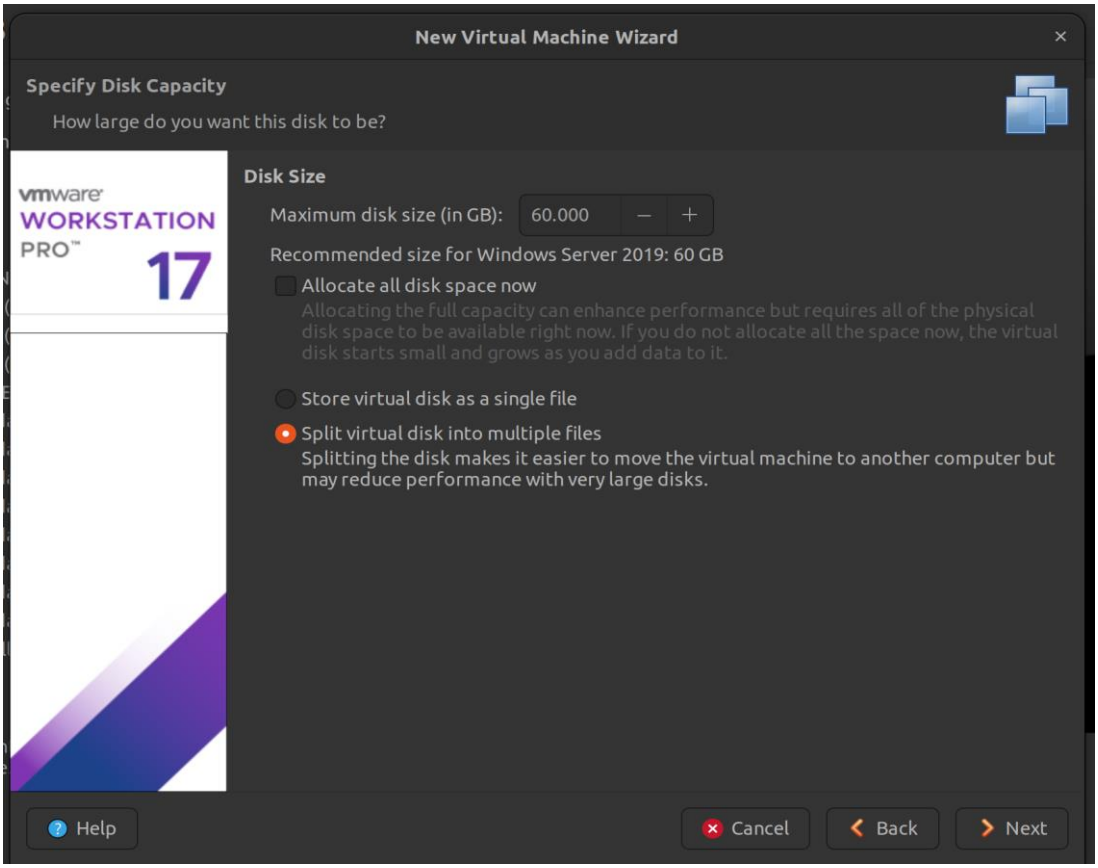

Figure IV.25 Capacité du disque de stockage.

Cette figure represente un recapetulatif de nos configurations, on clique sur finish pour finaliser la creation de notre nouvelle machine virtuelle

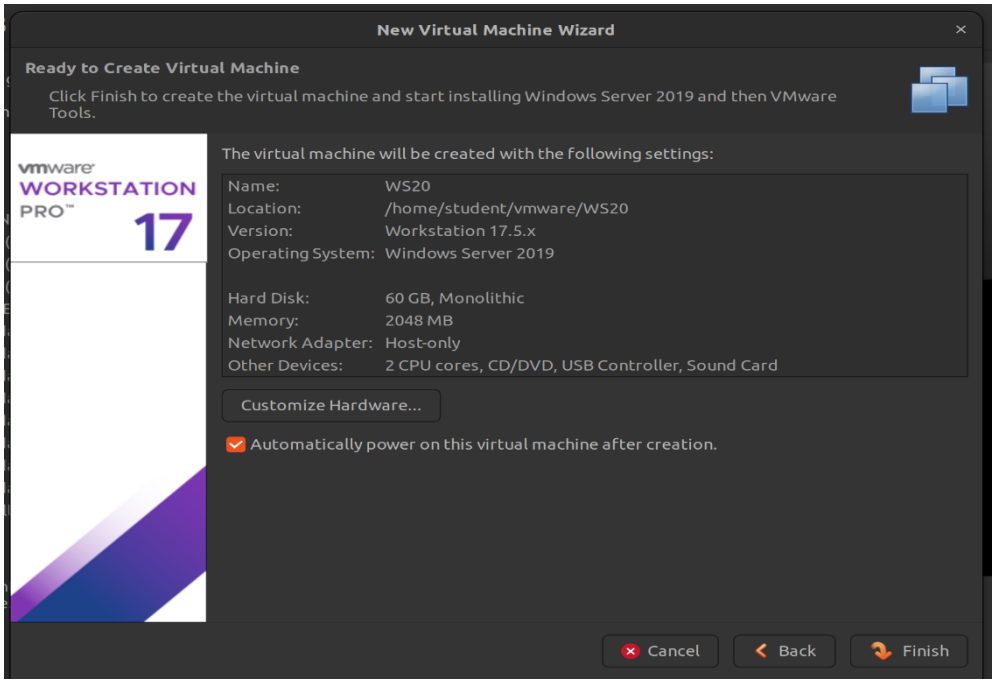

Figure IV.26 Récapitulatif des paramètres avant la création de la VM.

Voici les paramètres de la machine virtuelle une fois déployé

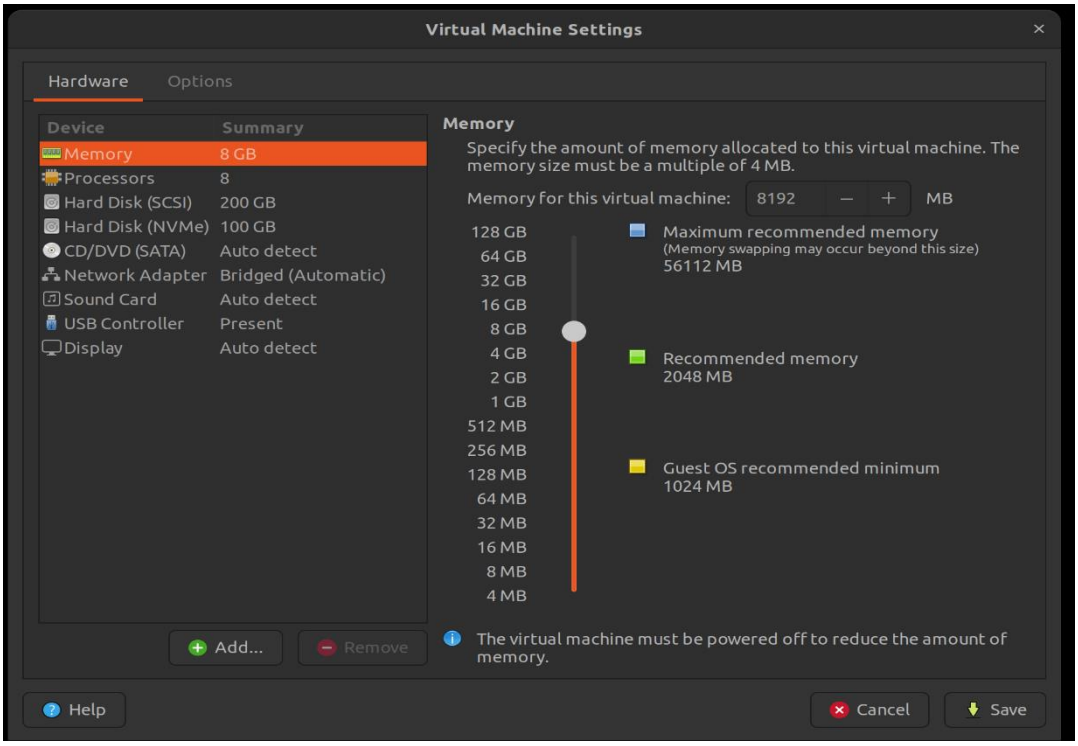

Figure IV.27 La configuration de notre machine virtuelle.

Les méthodes d'installation des machines virtuelles comprennent

- Création de la VM depuis le logiciel VMware Workstation.
- Utilisation de l'interface web Client de l'ESXi cette approche permet l'installation de la VM uniquement sur l'hôte spécifié. Par exemple, en se connectant à un hôte donné (serveur 1), il est possible de créer une VM exclusivement sur cet hôte. Cette méthode s'avère pratique lorsque vCenter n'est pas accessible ou n'est pas installé.
- Utilisation de l'interface web Client de vCenter : cette méthode offre la possibilité d'installer la VM sur n'importe quel hôte géré par vCenter.

Une fois la VM déployé nous allons poursuivre l'installation Windows comme suit

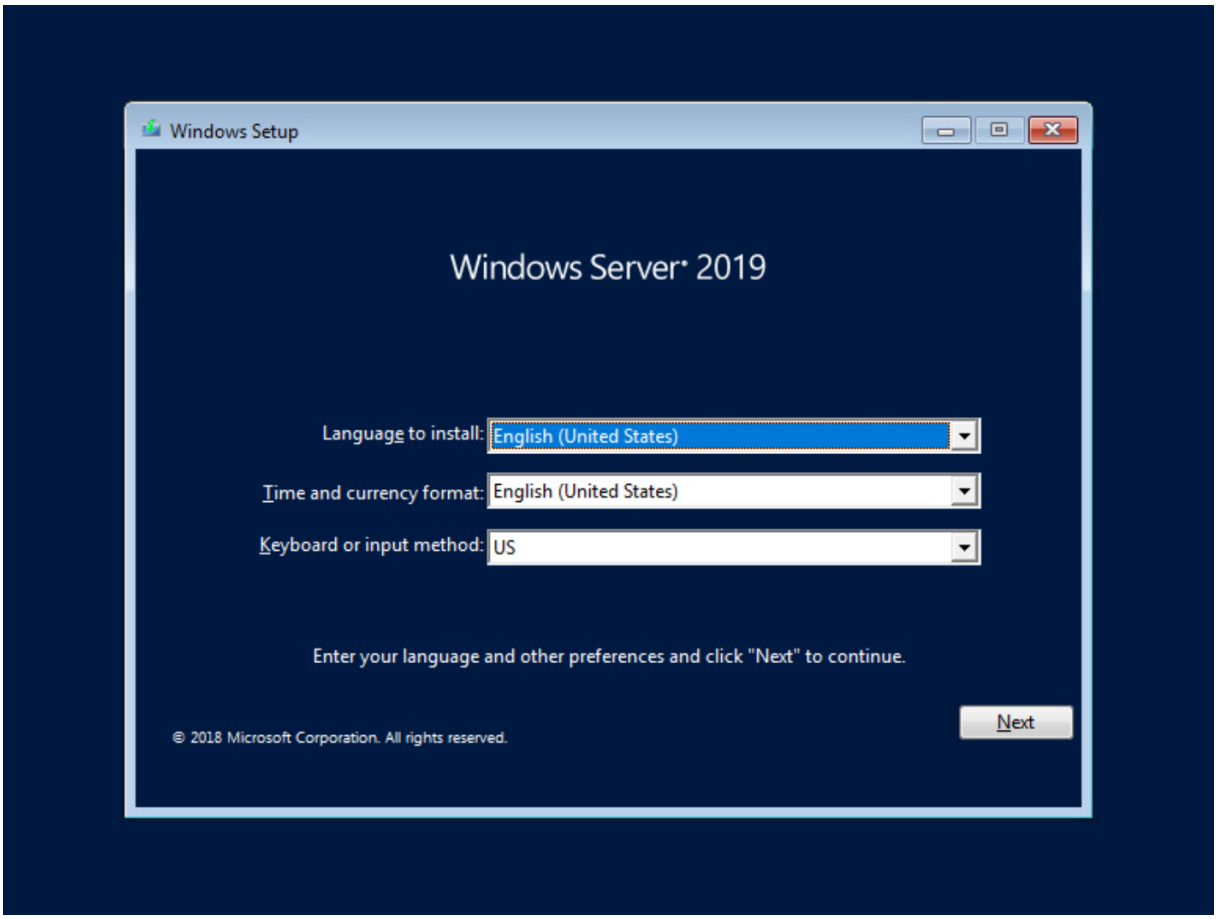

Figure IV.28 Choix de langue.

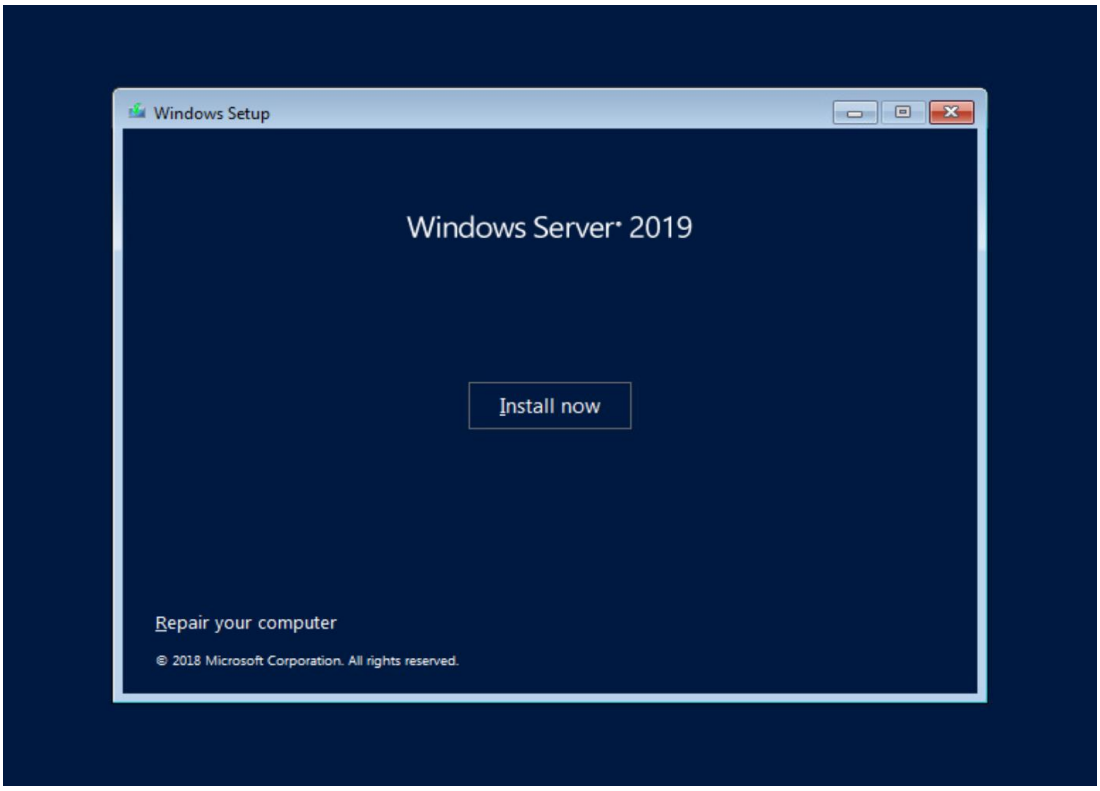

Figure IV.29 Lancement de l'installation finale.

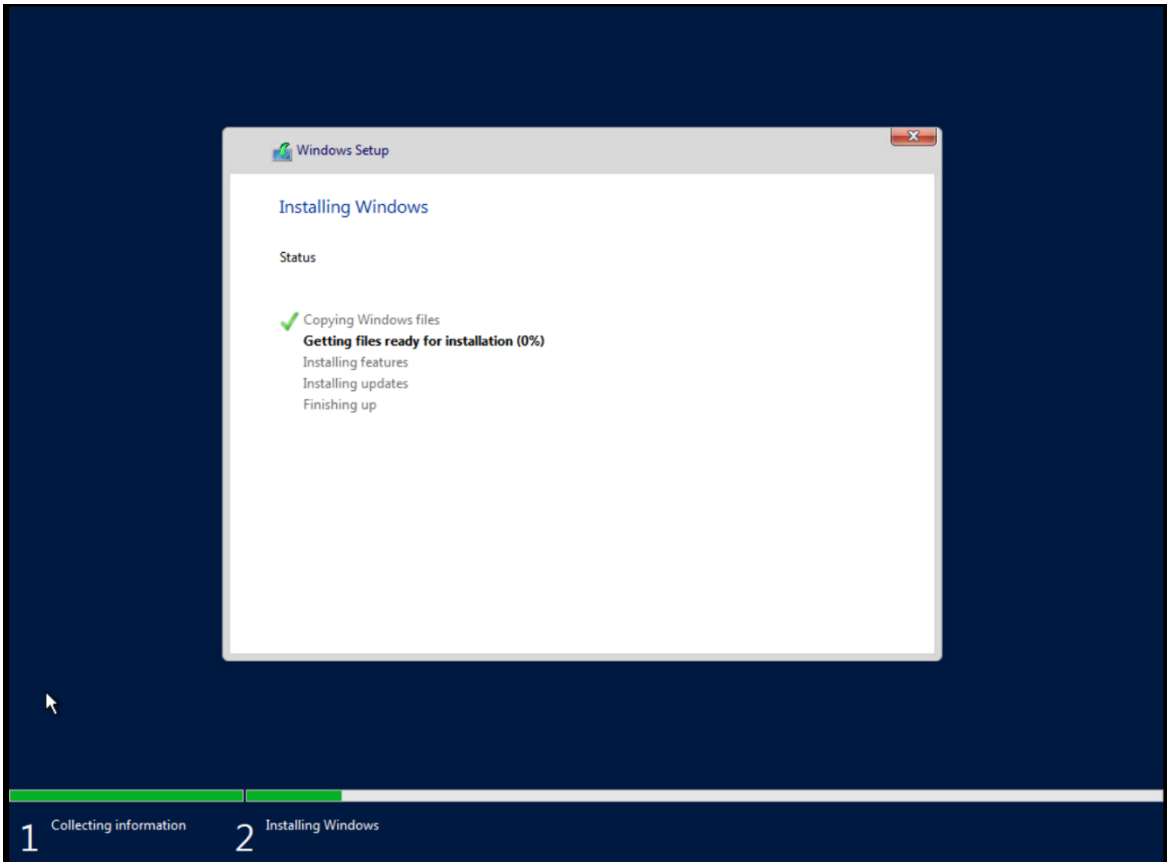

Figure IV.30 Finalisation de l'installation.

Lorsque l'installation s'achève la fenêtre de server manager s'affiche automatiquement

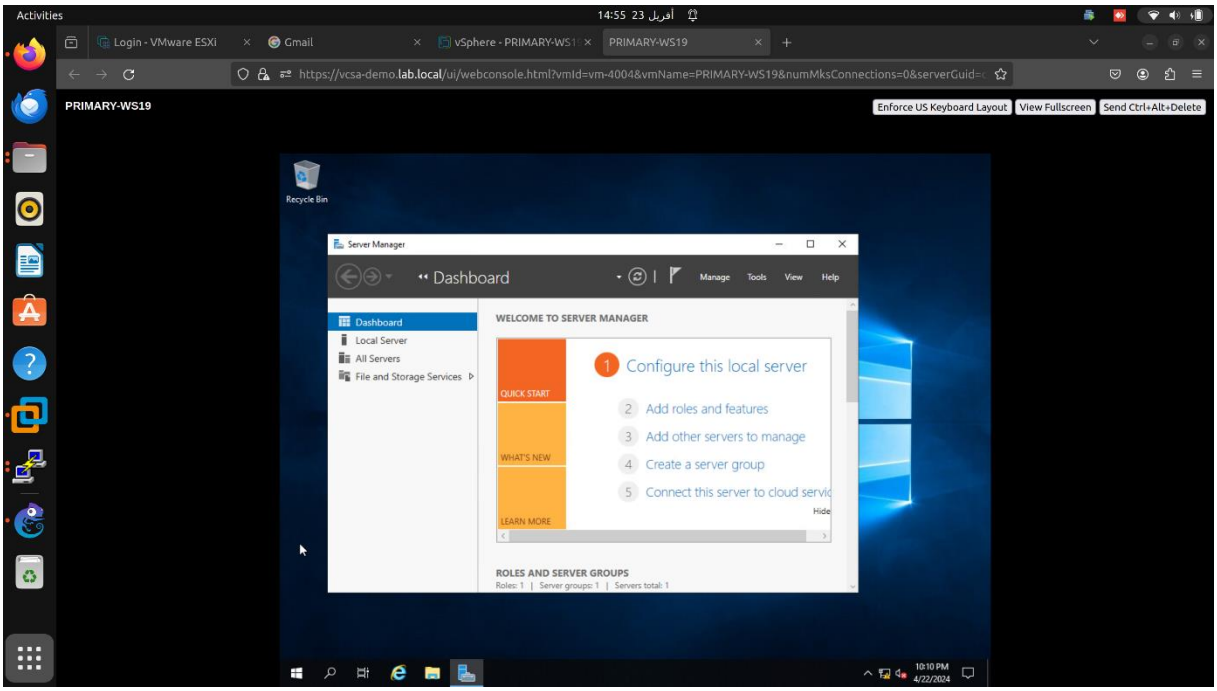

Figure IV.31 Fenêtre Server Manager.

IV.2.4 VMware Tools

Pour pouvoir utiliser pleinement notre VM nous allons procéder à l'installation de VMware Tools, avons de faire la démonstration de son installation nous allons définir ce que c'est VMware Tools.

VMware Tools C'est un ensemble de services et de pilotes logiciels essentiels fournis par VMware pour améliorer les performances et la gestion des machines virtuelles exécutées sur ses plates-formes de virtualisation. Ces outils facilitent l'interaction entre le système d'exploitation invité de la VM et l'hyperviseur, offrant des fonctionnalités telles que le partage de fichiers entre l'hôte et la VM, la synchronisation de l'horloge, des améliorations graphiques, une meilleure gestion des périphériques et des performances accrues.

Pour installer VMware Tools il faut suivre les étapes suivantes :

Clique droit sur la VM, et choisir l'onglet "Guest OS" Puis "Install" VMware Tools comme indiqué sur la figure ci-dessous

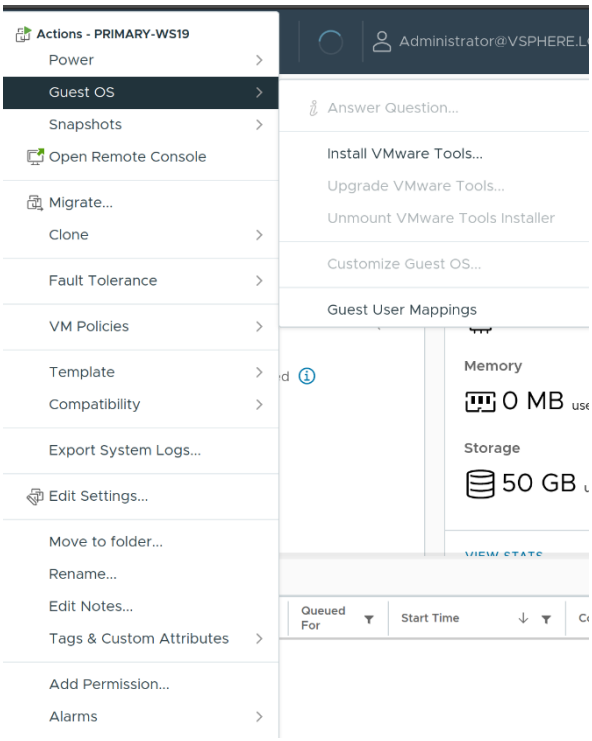

Figure IV.32 installer VMware Tools.

Suite à cella aune fenêtre va s'afficher disant que le fichier d'installation va être exporter vers la VM comme virtuel CD/DVD

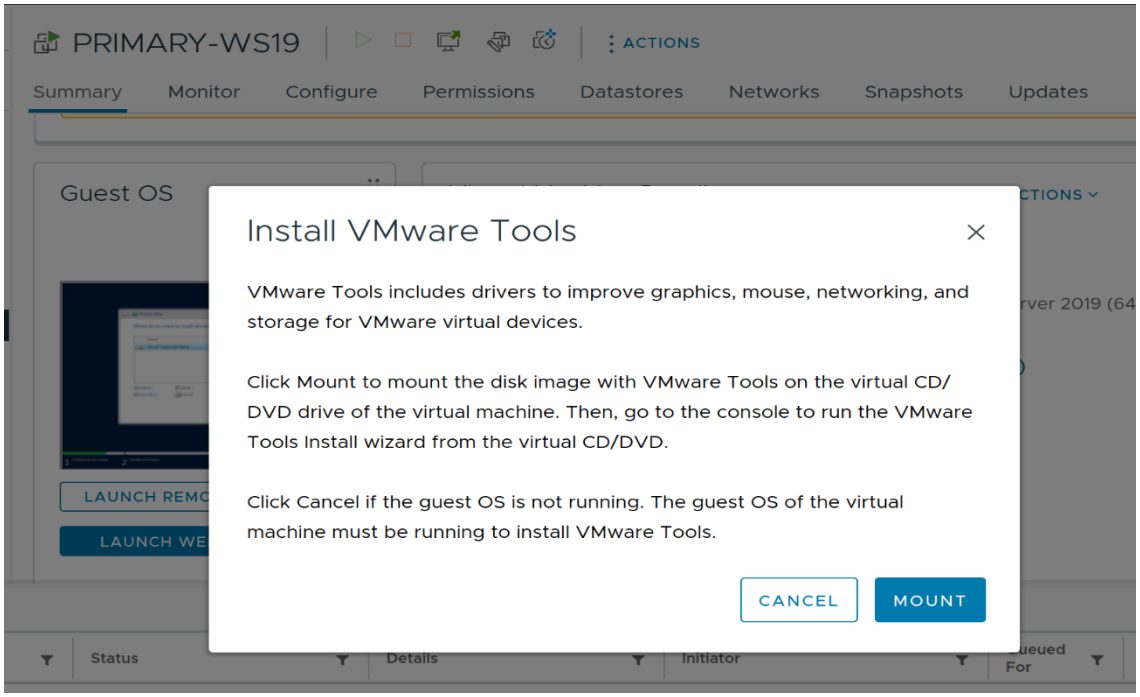

Figure IV.33 Chargement de l'exécutable d'installation VMware Tools.

Nous allons nous rendre au disque CD/DVD de la machine virtuelle et faire un double clique

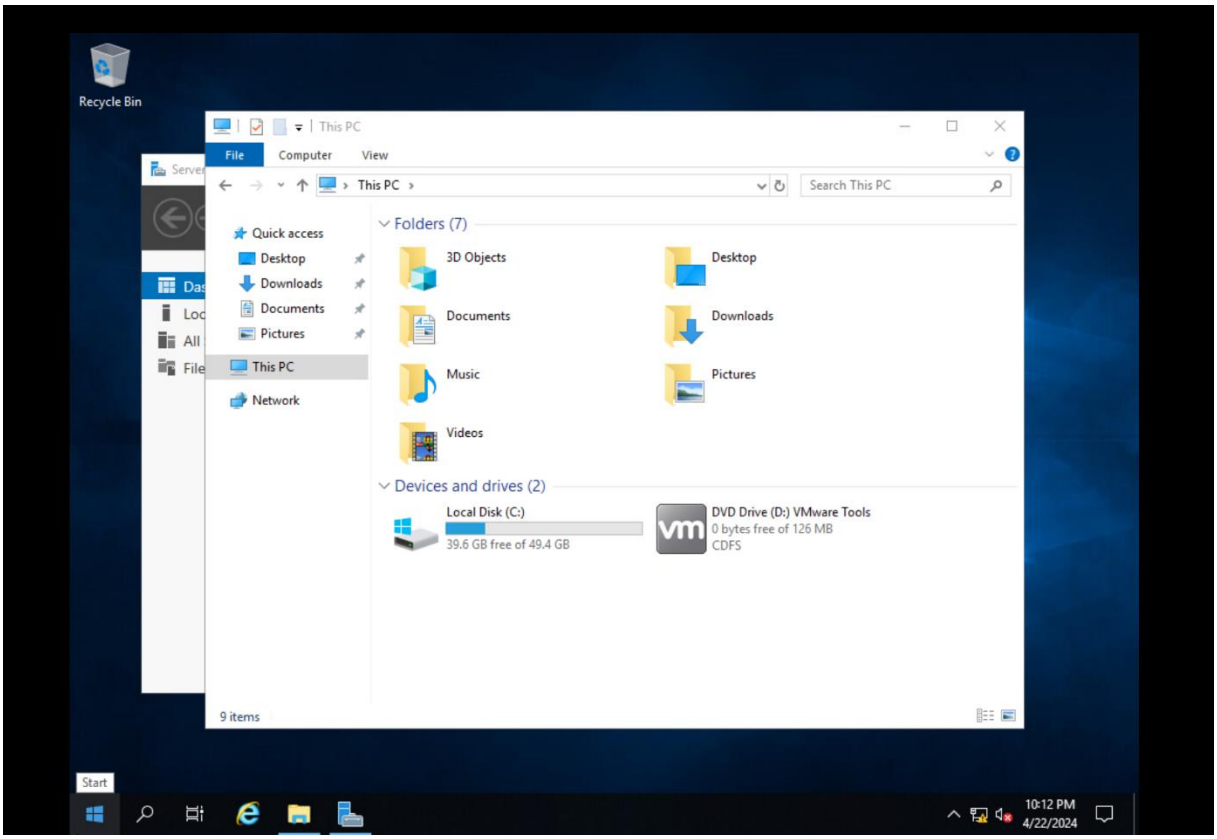

Figure IV.34 Emplacement d'où lancer l'installation de VMware Tools.

L'installation va démarrer comme le montre la figure suivante

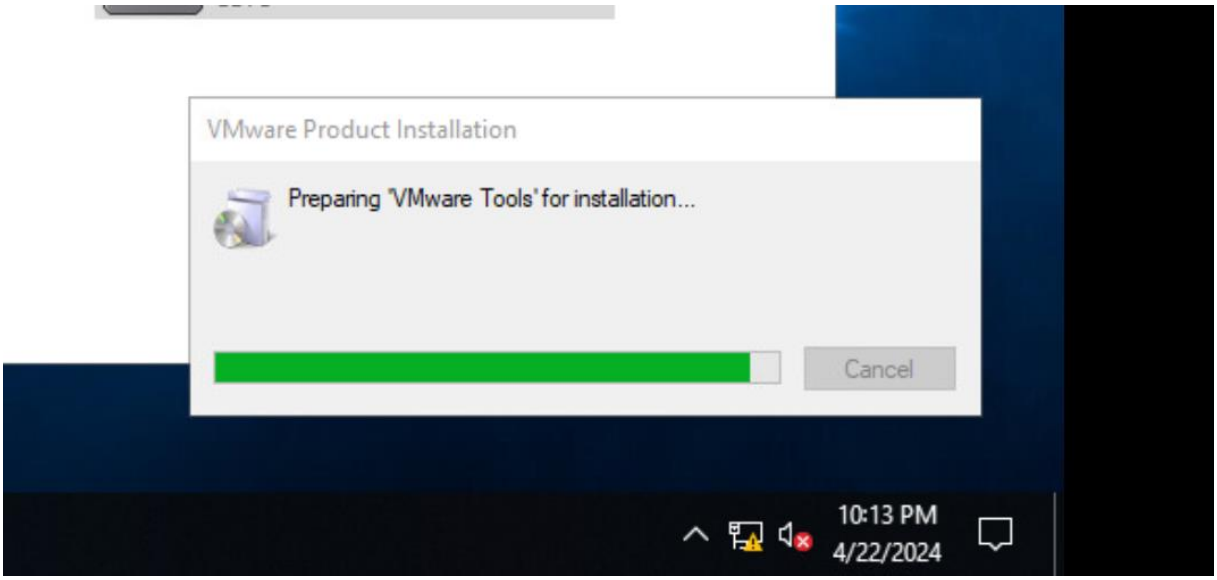

Figure IV.35 Préparation d'installation VMware Tools.

Il nous sera à présent désormais demandé quelle version souhaitons-nous installer, nous avons opté pour la version complète qui comprend toutes les fonctionnalités

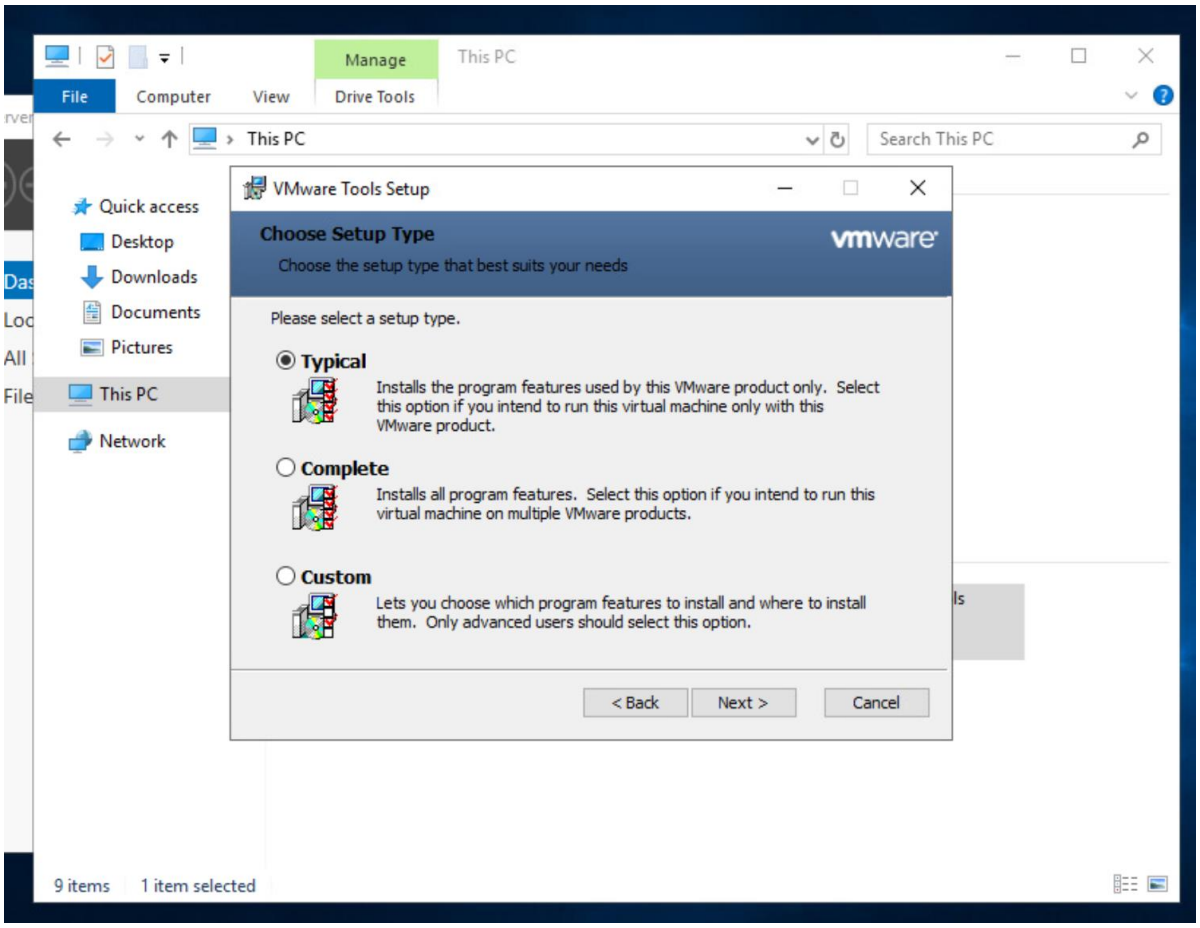

Figure IV.36 Type d'installation VMware Tools souhaité.

Une fois l'installation terminé, il nous sera demandé de redémarrer notre machine pour que l'installation prenne effet et pouvoir profiter des fonctionnalités qu'offre VMware Tools

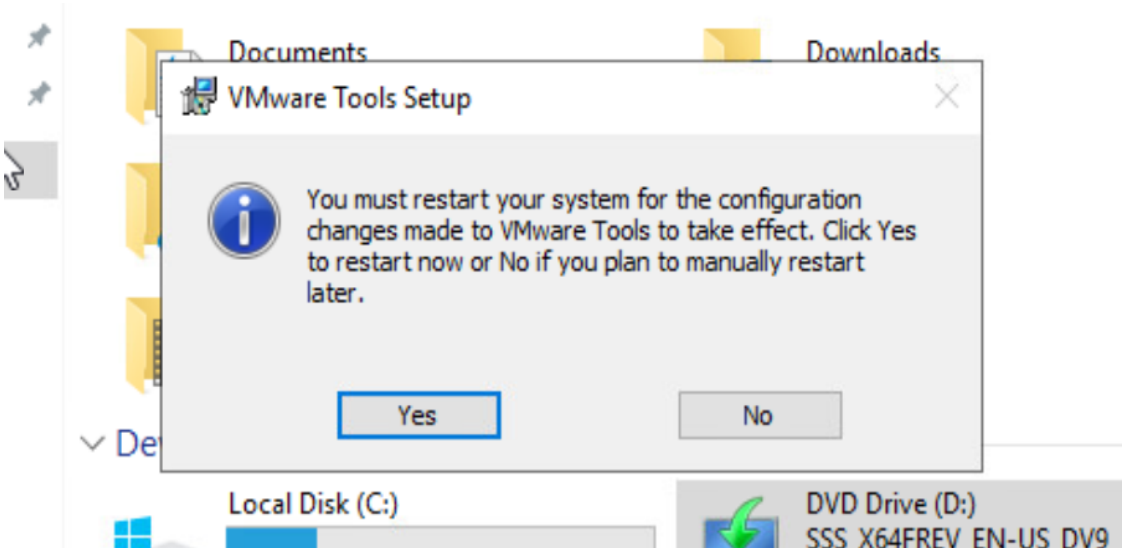

Figure IV.37 Redémarrage de la VM.

IV.2.5 Installation du rôle DNS

Nous allons maintenant installer le service DNS pour pouvoir installé l'instance vCenter en suivant ces étapes

Accéder à la carte réseau de la machine et lui assigner une adresse IP statiquemt dans notre plage d'adresse réservé au réseau management, une adresse qui sera celle du serveur DNS que nous allons installer juste après cette étape

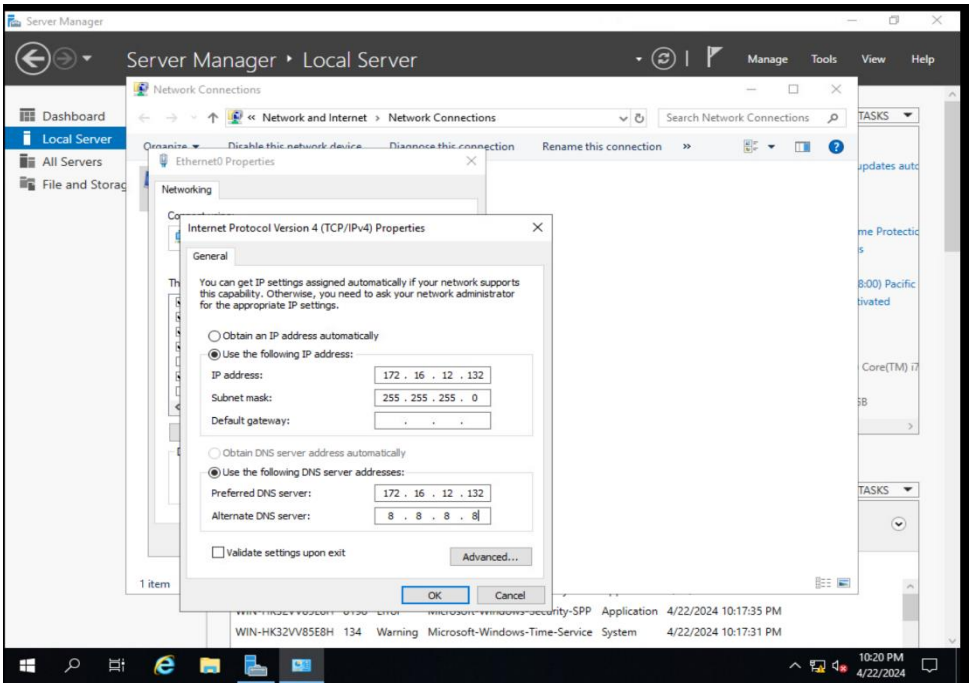

Figure IV.38 Adresse IP de la machine.

Une fois l'adresse IP attribué nous allons cliquer sur l'onglet Manage dans la fenêtre server manager pour créer le service DNS, en cliquant sur "Add Rôles and Features" nous allons lancer la procédure de création d'un nouveau service

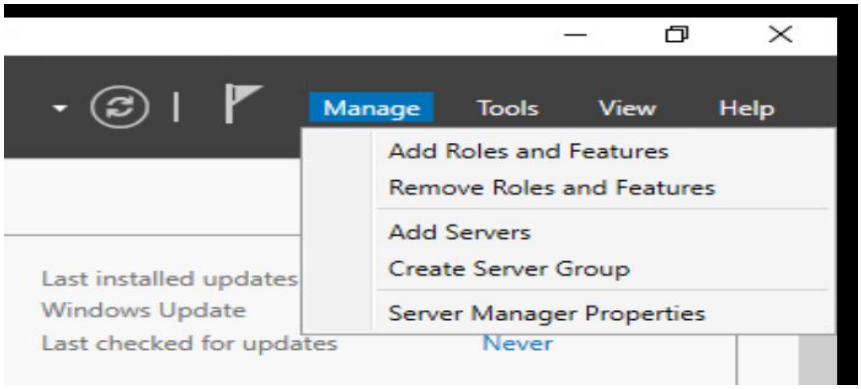

Figure IV.39 L'ajout d'un nouveau service.

Une fenêtre contenant une série de prérequis s'affiche, qui assurent la bonne installation de notre service

Les prérequis sont

- La machine doit avoir un mot de passe robuste.
- L'adresse IP de la machine doit être attribué d'une manière statique.
- Les pilote et driver de la machine doivent être mis à jour.

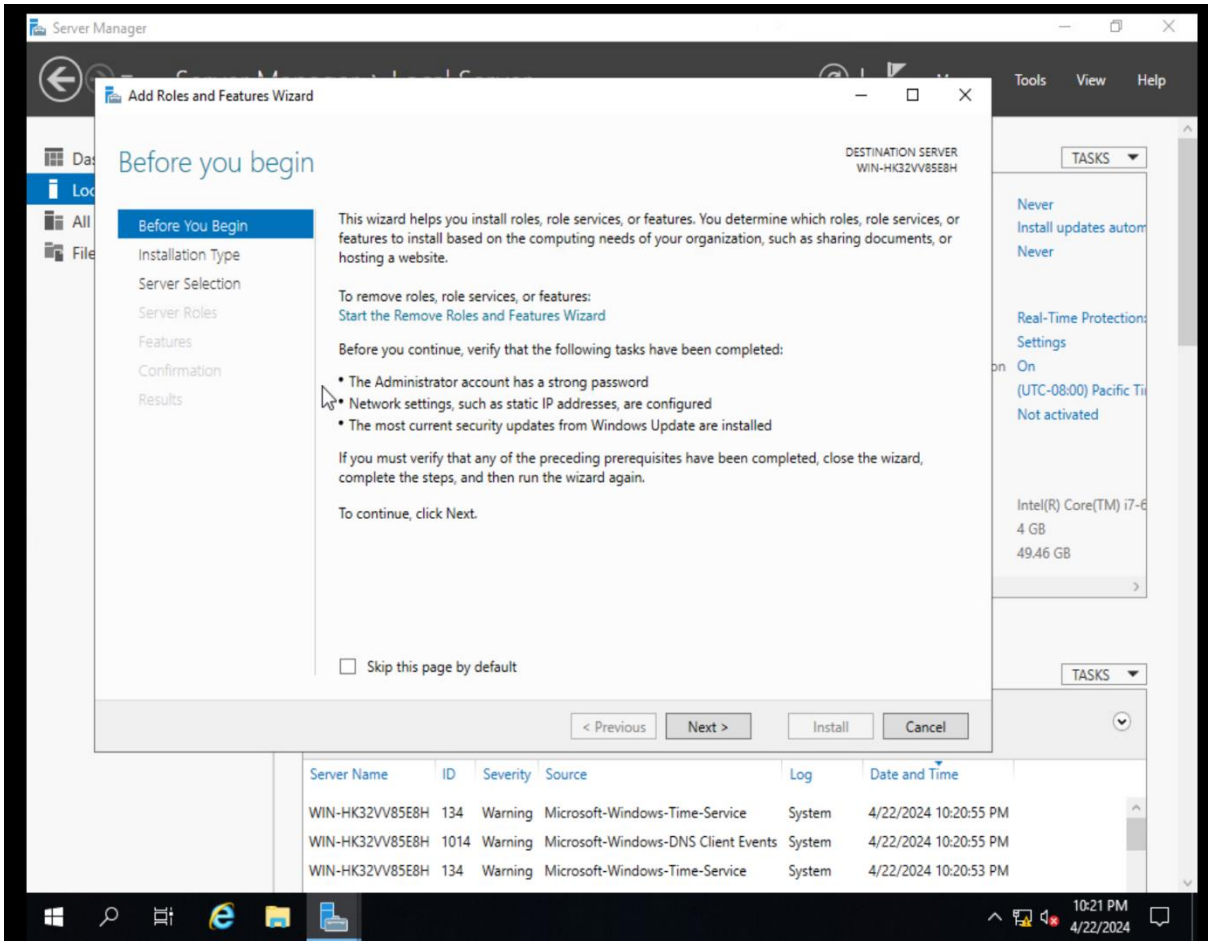

Figure IV.40 Prérequis avant installation.

A présent il nous sera demandé de choisi quel type d'installation nous souhaitons, ont choisi une installation dans un disque local non pas distant

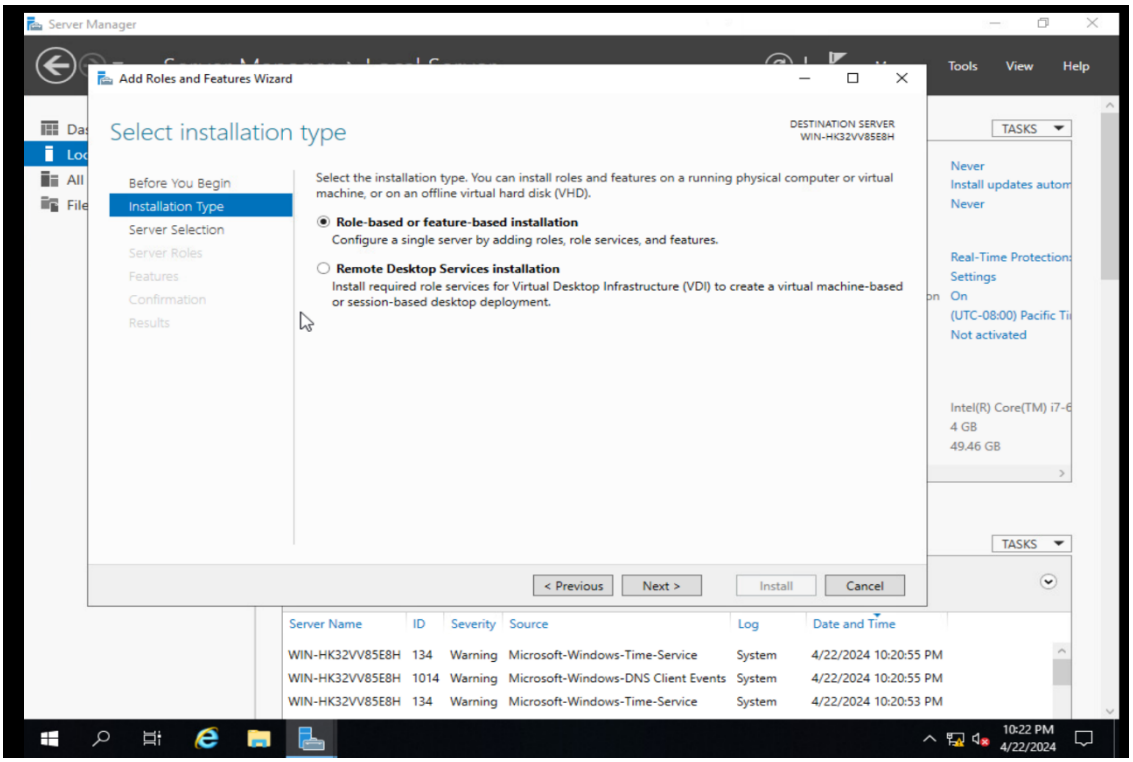

Figure IV.41 Type d'installation.

On sélectionne le disque de la machine ou on va installer notre service

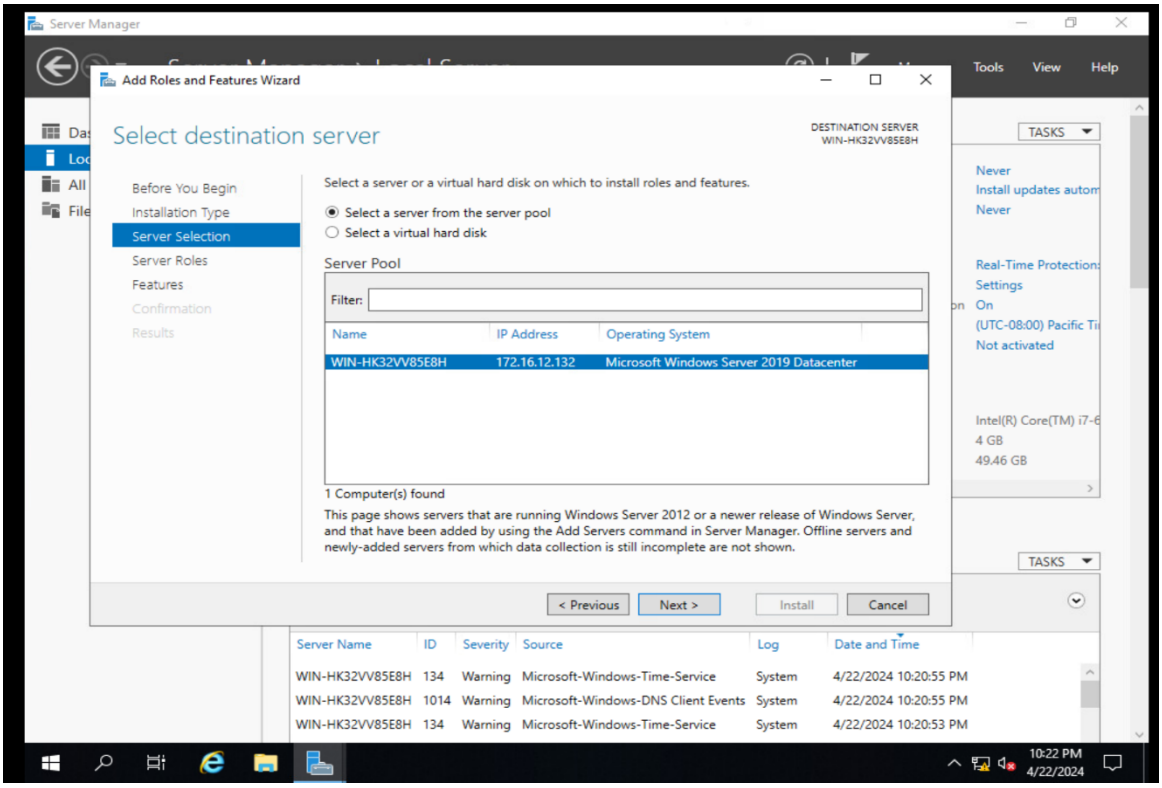

Figure IV.42 Choix de disque dur.

Celle lors de cette étape que nous allons choisir l'ajout les fonctionnalités DNS

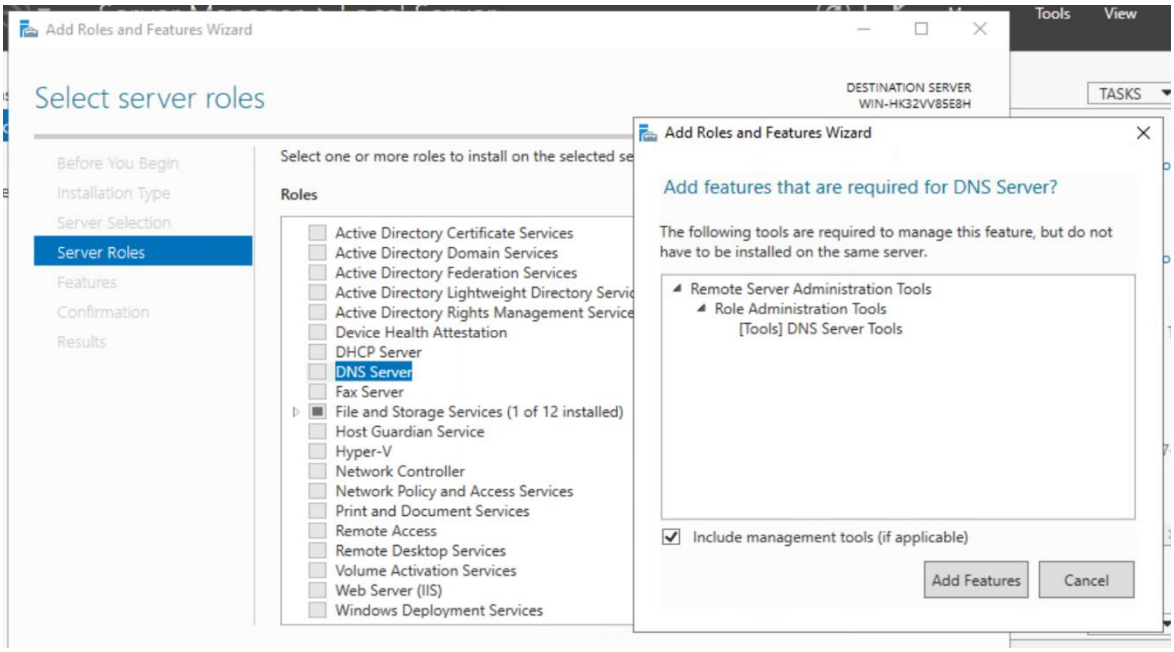

Figure IV.43 L'ajout les fonctionnalités DNS.

Une instance de confirmation de l'installation va s'afficher se a quoi on va cliquer sur "Install" et l'installation pourra débuter

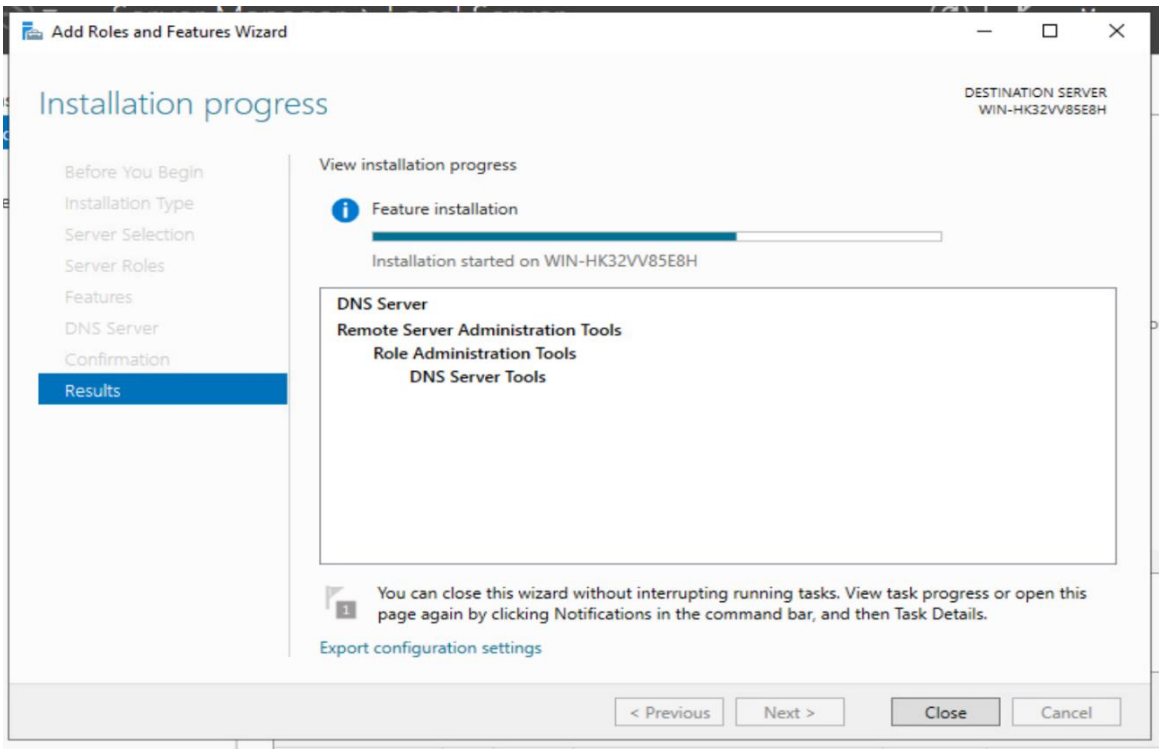

Figure IV.44 L'installation du service DNS.

Une fois l'installation terminé il suffit de s'y rendre au "Dashboard" du server manager pour confirmer l'installation du service DNS

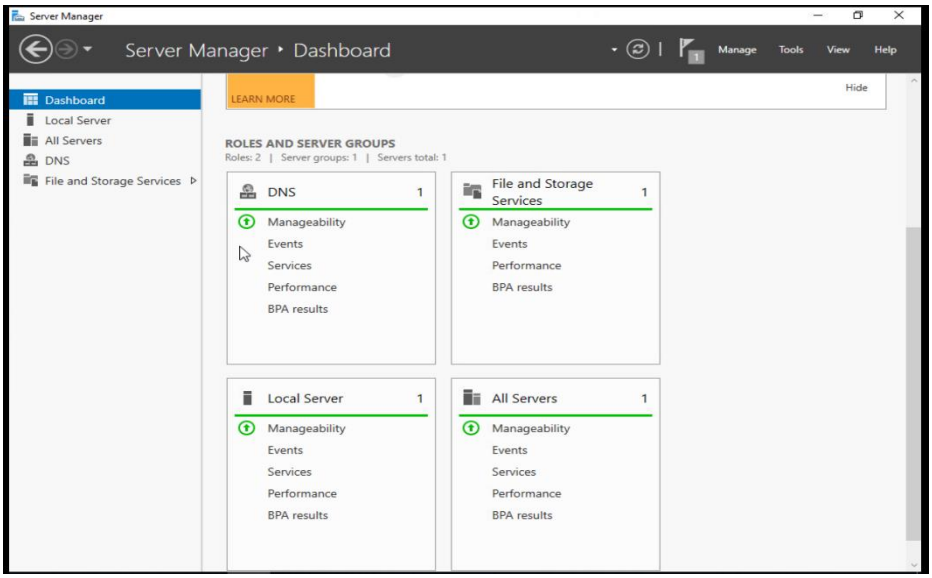

Figure IV.45 Confirmation de l'installation du service DNS.

Maintenant que nous avons installé notre rôle DNS avec succès, nous allons créer des zones "Forward" et "Reverse" à l'intérieur de ce service pour assurer la translation des adresses IP en FQDN et vice-versa

Pour ce faire on se rend sur l'onglet "Tools" de server manager

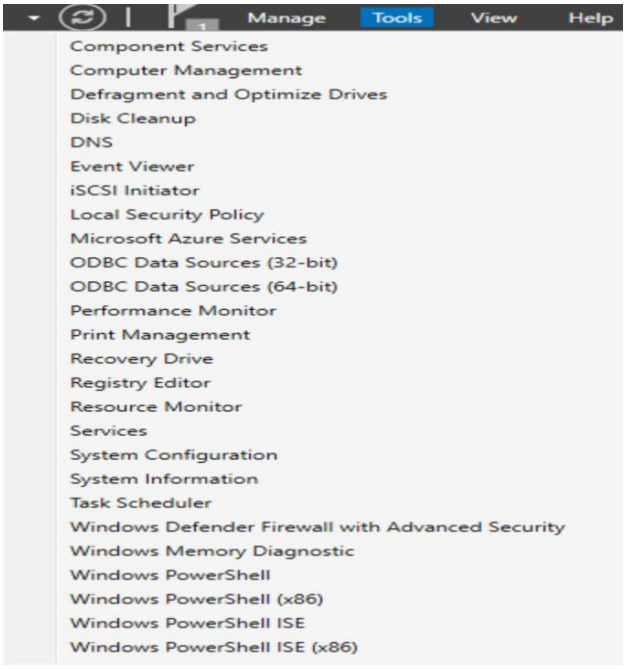

Figure IV.46 L'ajout des zones Forward et Reverse au service DNS.

Apres avoir choisi DNS on fait un clique droit sur l'instance "Forward Lookup Zones"

La zone forward est utilisé pour la résolution des noms de domaine en adresses IP

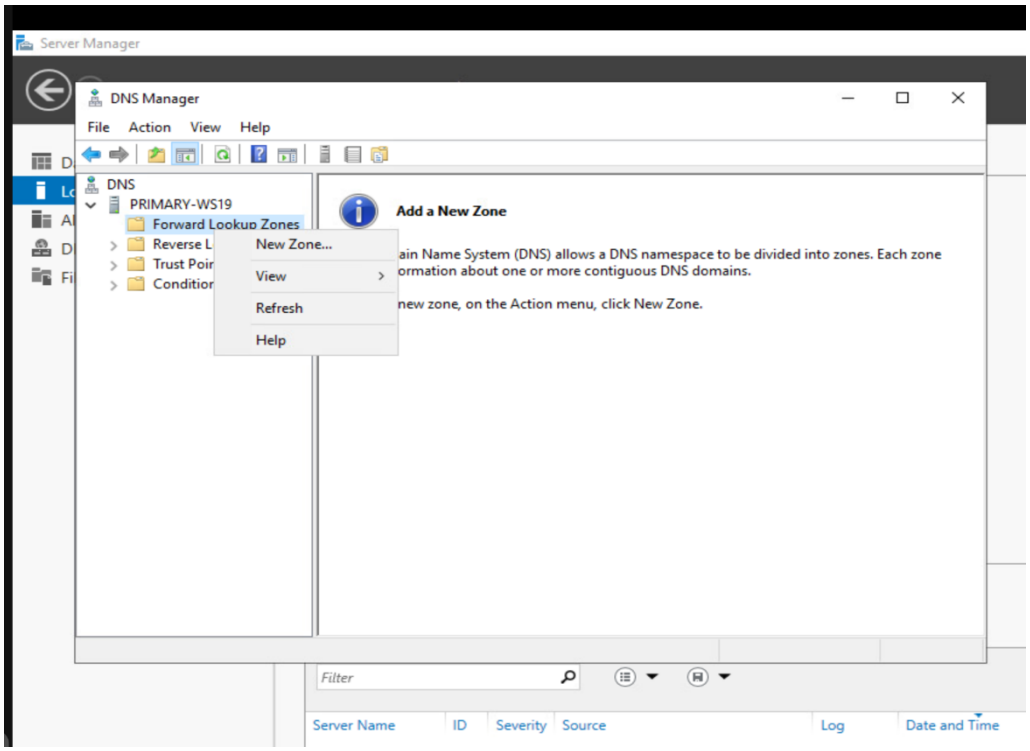

Figure IV.47 Créer les nouvelles zones de translation.

On choisit le type de zones souhaité, puisque c'est notre seul serveur DNS on choisit "Primary"

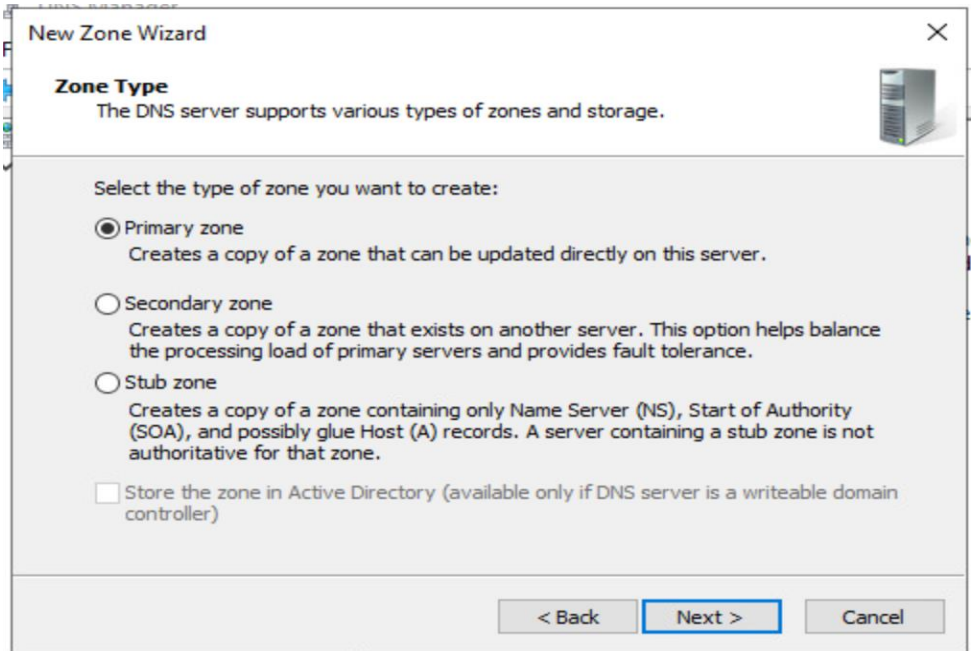

Figure IV.48 Choix du type de la zone.

On attribue un nom à notre nouvelle zone comme suit

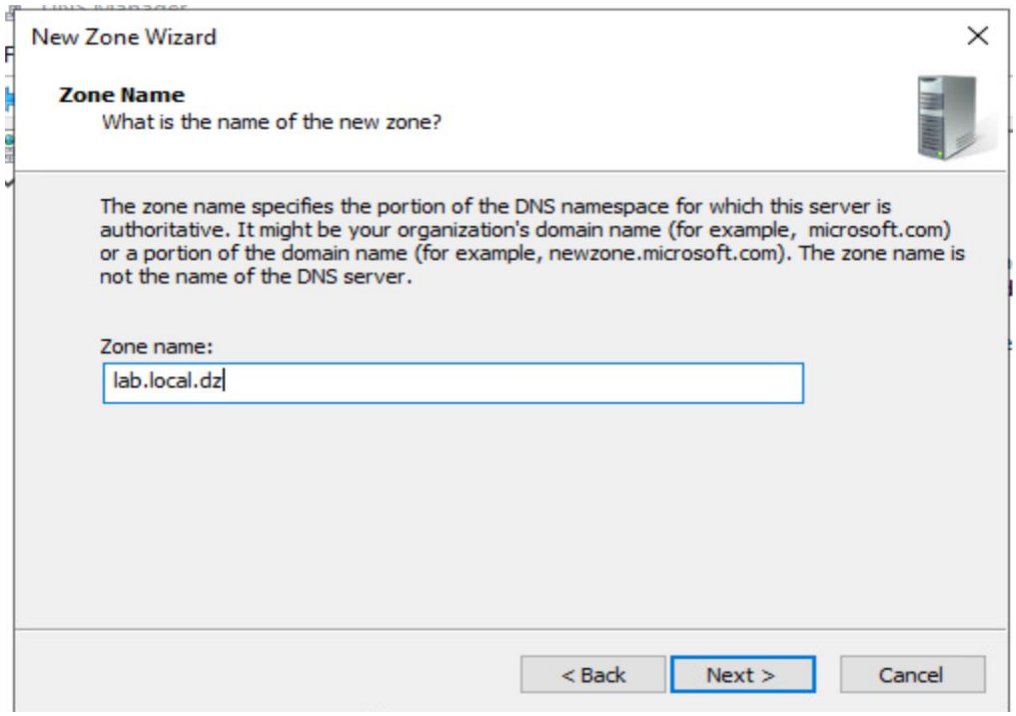

Figure IV.49 Nom de la zone.

On va créer aussi des nouveaux fichiers puisque on ne dispose pas d'un autre serveur DNS

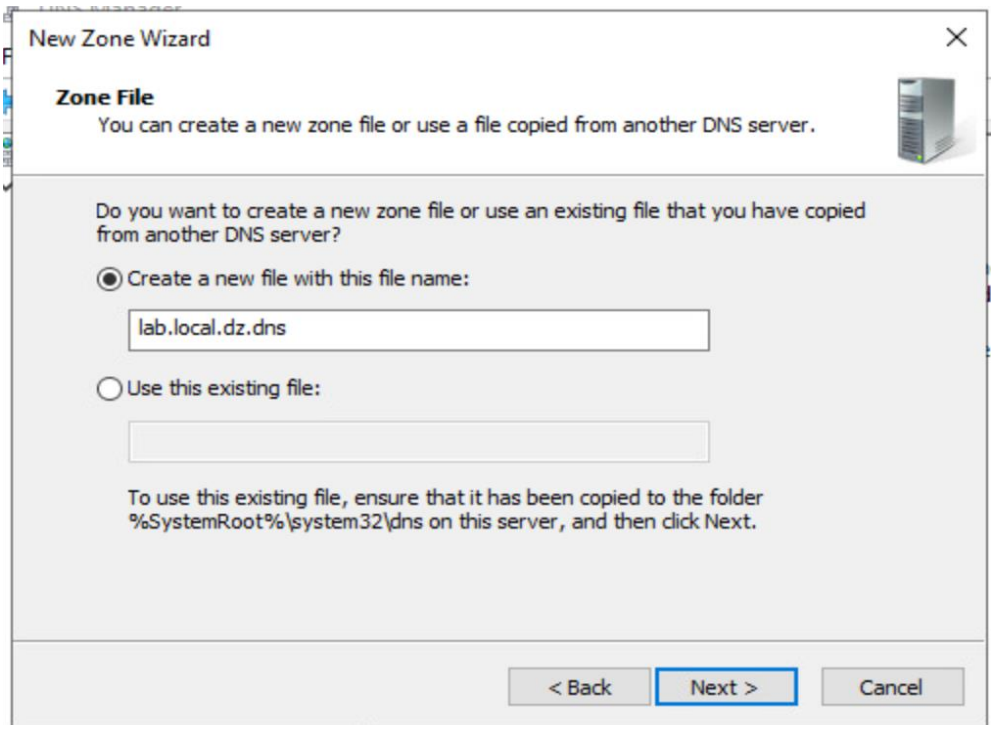

Figure IV.50 Création des fichiers de la zone Forward.

Une fenêtre récapitulative des configurations va s'afficher puis on clique sur finish, et ainsi notre zone a été créer avec succès

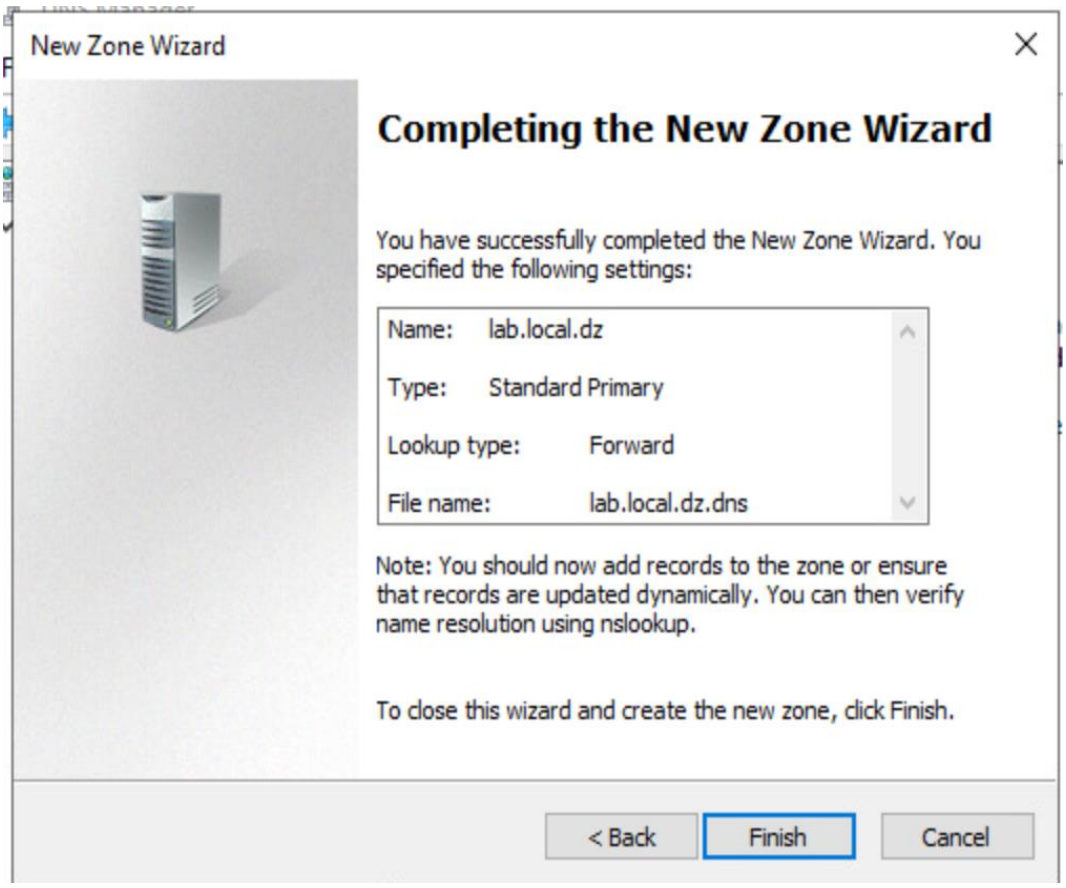

Figure IV.51 Créer les nouvelles zones de translation.

On va désormais faire la même chose pour créer une zone "Reverse"

La zone "Reverse" est utilisé pour l'inverse de la zone "Forward" c'est-à-dire la résolution des adresses IP en noms de domaine.

On commence par introduire les 3 premiers octets de notre adresse IP dédié au service DNS comme indiqué sur la figure suivante

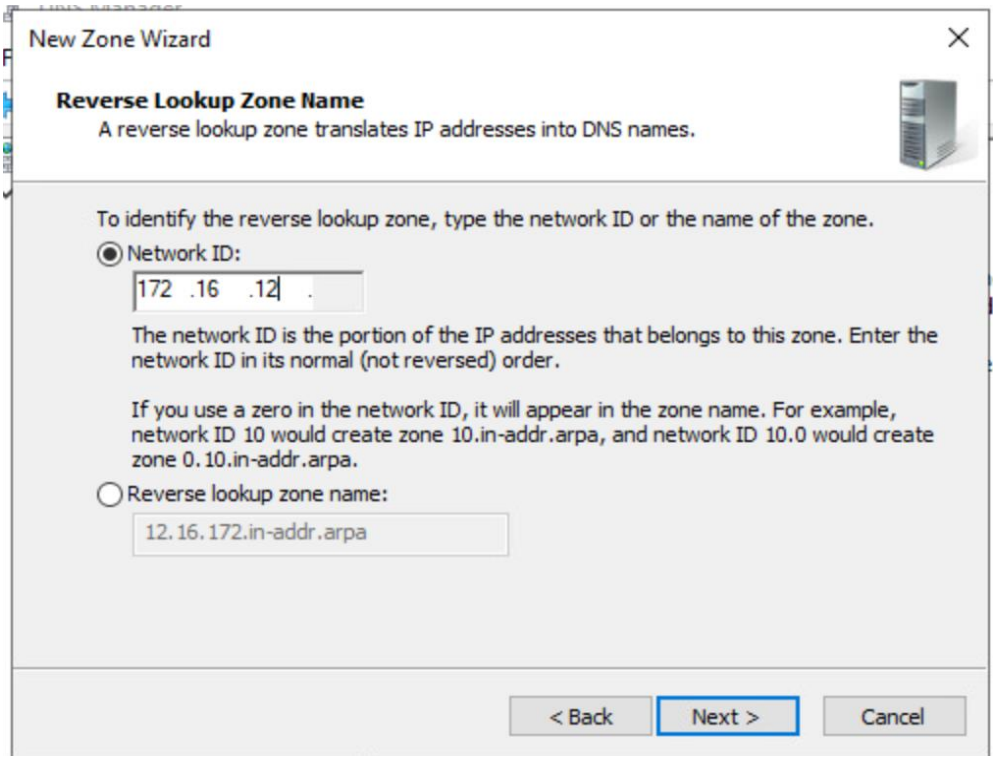

Figure IV.52 Introduire l'adresse IP du serveur DNS.

Il suffit de cliquer sur finish pour se voir la création de la zone Reverse créer avec succès

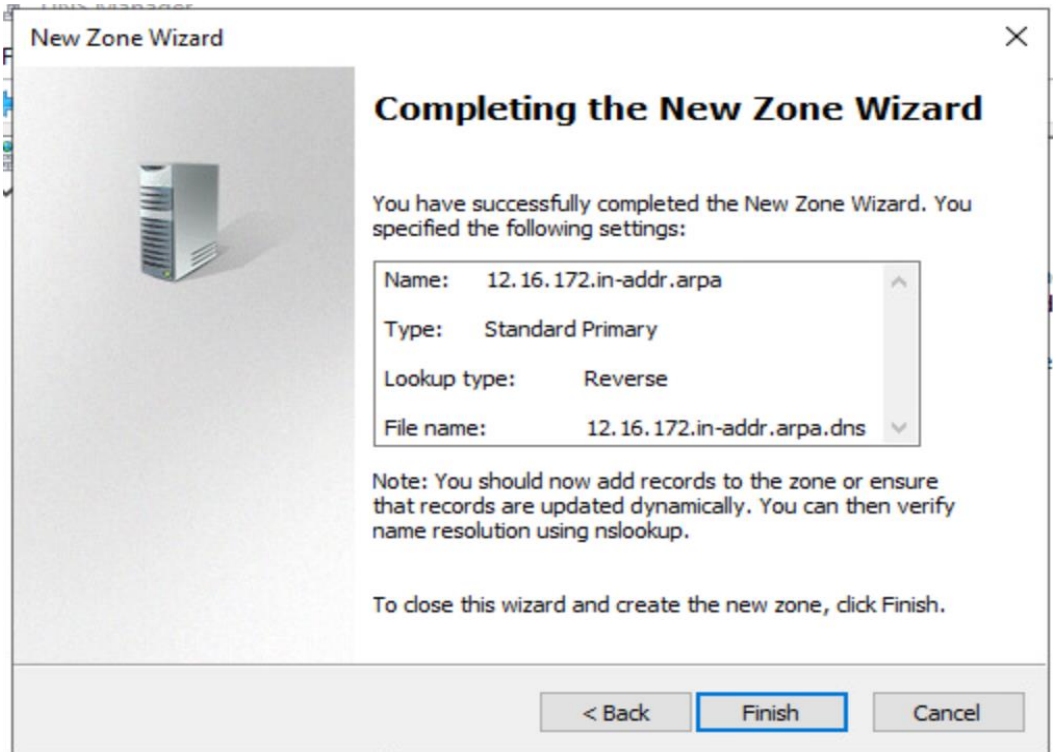

Figure IV.53 Créer les nouvelles zones de translation.

Une fois les deux zones créées, on doit ajouter à l'intérieur de ces zones les adresses et nom de domaine auxquels on souhaite faire la translation, et pour ce faire on suit ces étapes :

Clique droit sur la zone "Forward" créé et on clique sur "New Host"

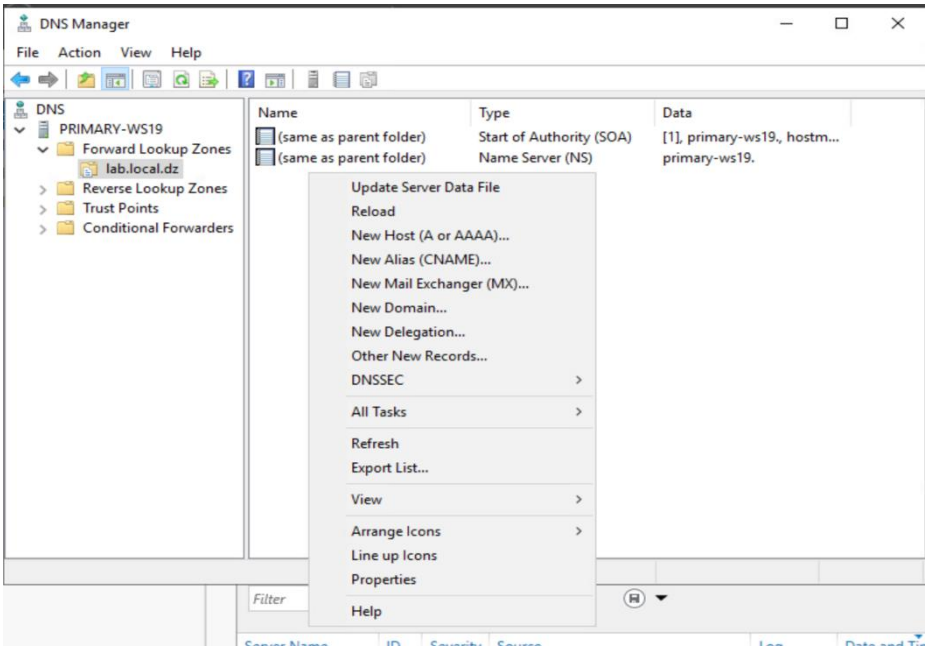

Figure IV.54 L'ajout d'un hôte à traduire.

On complète les champs requis nom, nom de domaine et adresse IP

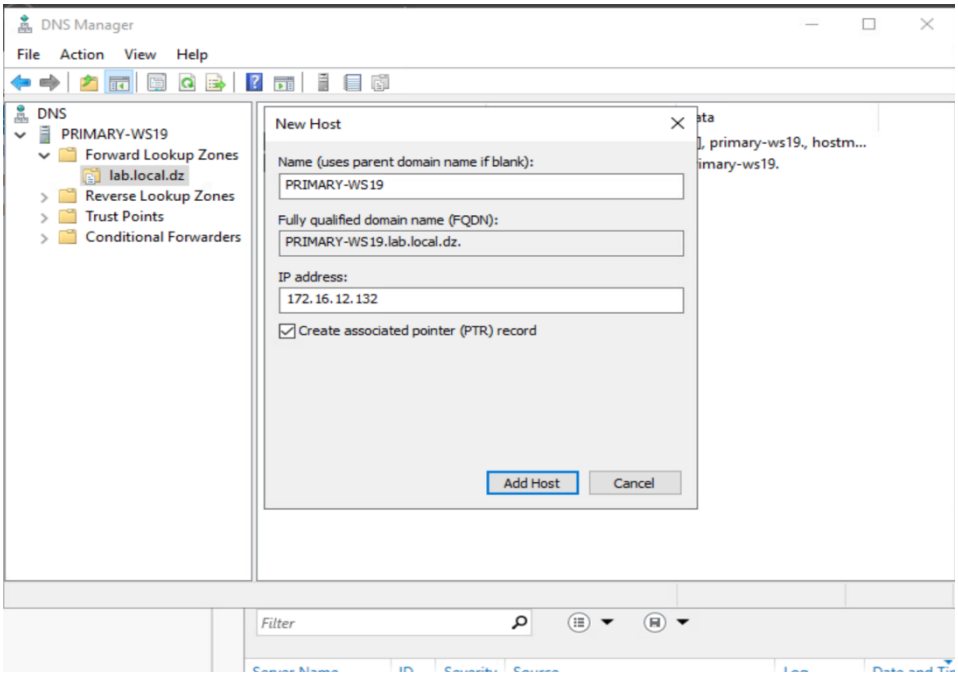

Figure IV.55 Information sur l'hôte.

Une fenêtre indiquant l'ajout de l'hôte s'affiche

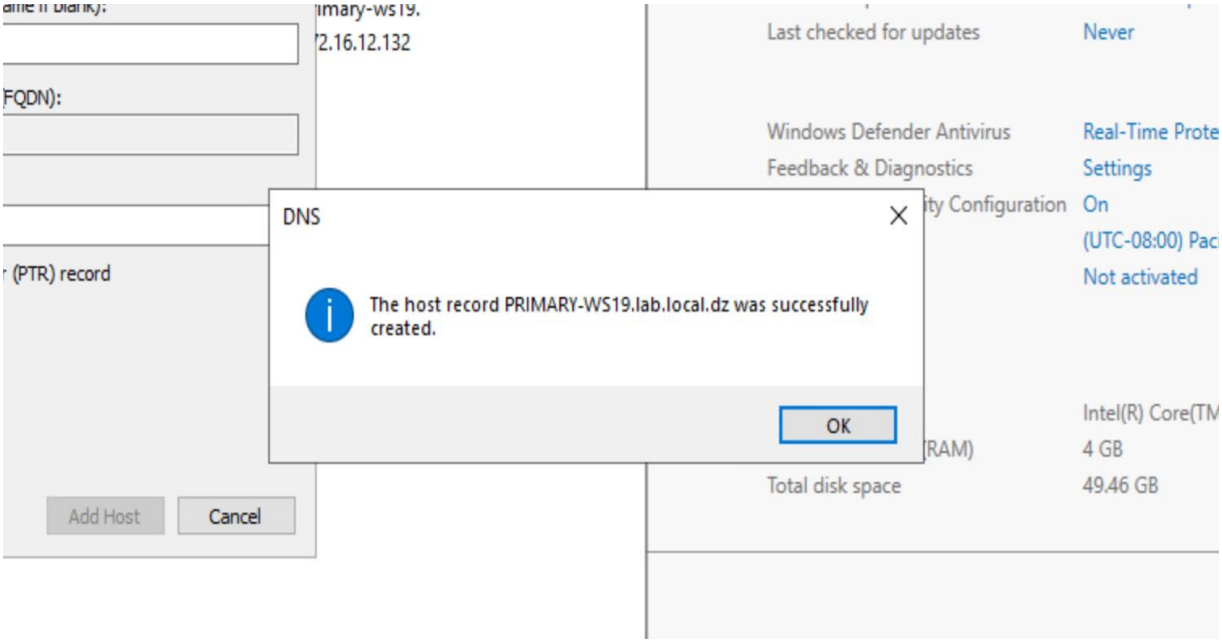

Figure IV.56 L'ajout de l'hôte est terminé.

Désormais on va tester si notre service est bel bien fonctionnel et pour cela on fait un clique droit sur le service DNS et on choisit "Launch nslookup"

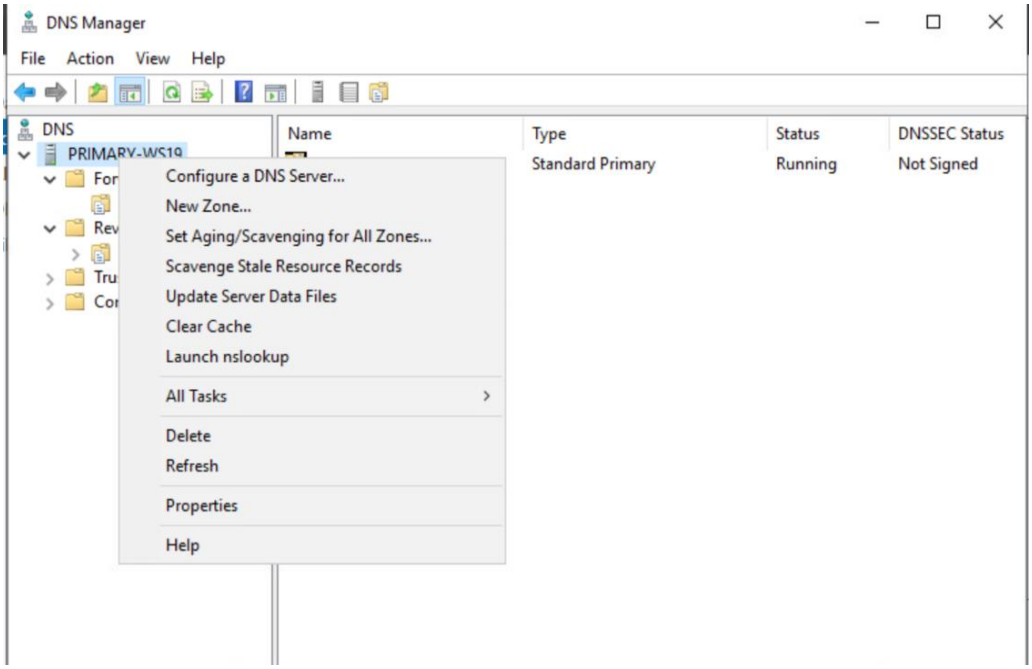

Figure IV.57 Lancer nslookup.

On test si le service DNS est joignable et ainsi tester le service on lui-même s'il fait les translations

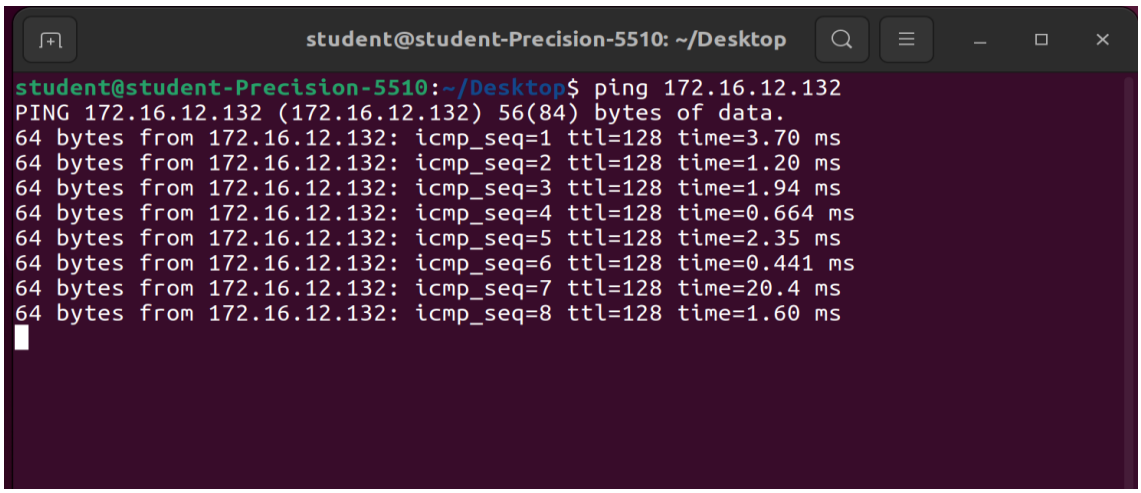

Figure IV.58 Test de connectivité du service DNS.

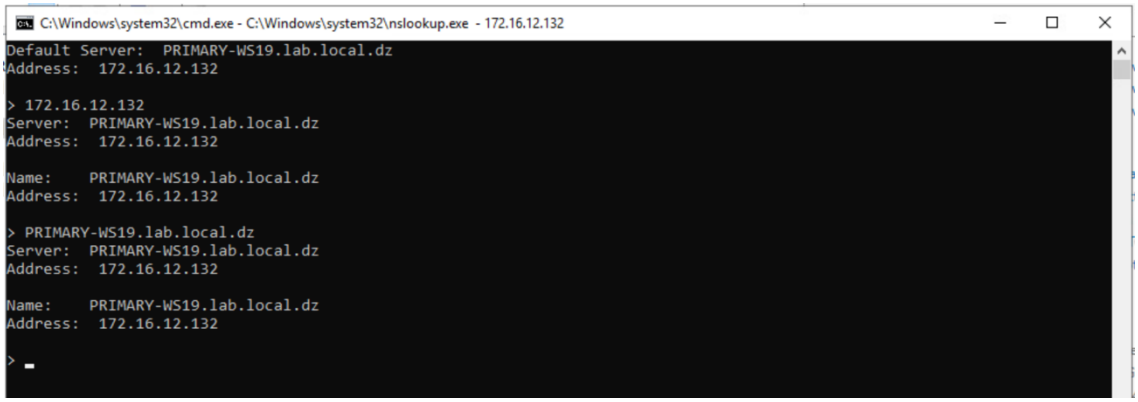

Figure IV.59 Test du service DNS.

Ainsi nous avons un service DNS déployé et fonctionnel.

IV.3 Installation des serveur ESXI

Pour chaque serveur, nous avons créé une machine virtuelle puis nous avons installé et exécuté l'hyperviseur ESXi de VMware au sein de cette dernière, avec l'image ISO correspondante

La configuration des 3 machines virtuelles est présentée dans la figure suivante

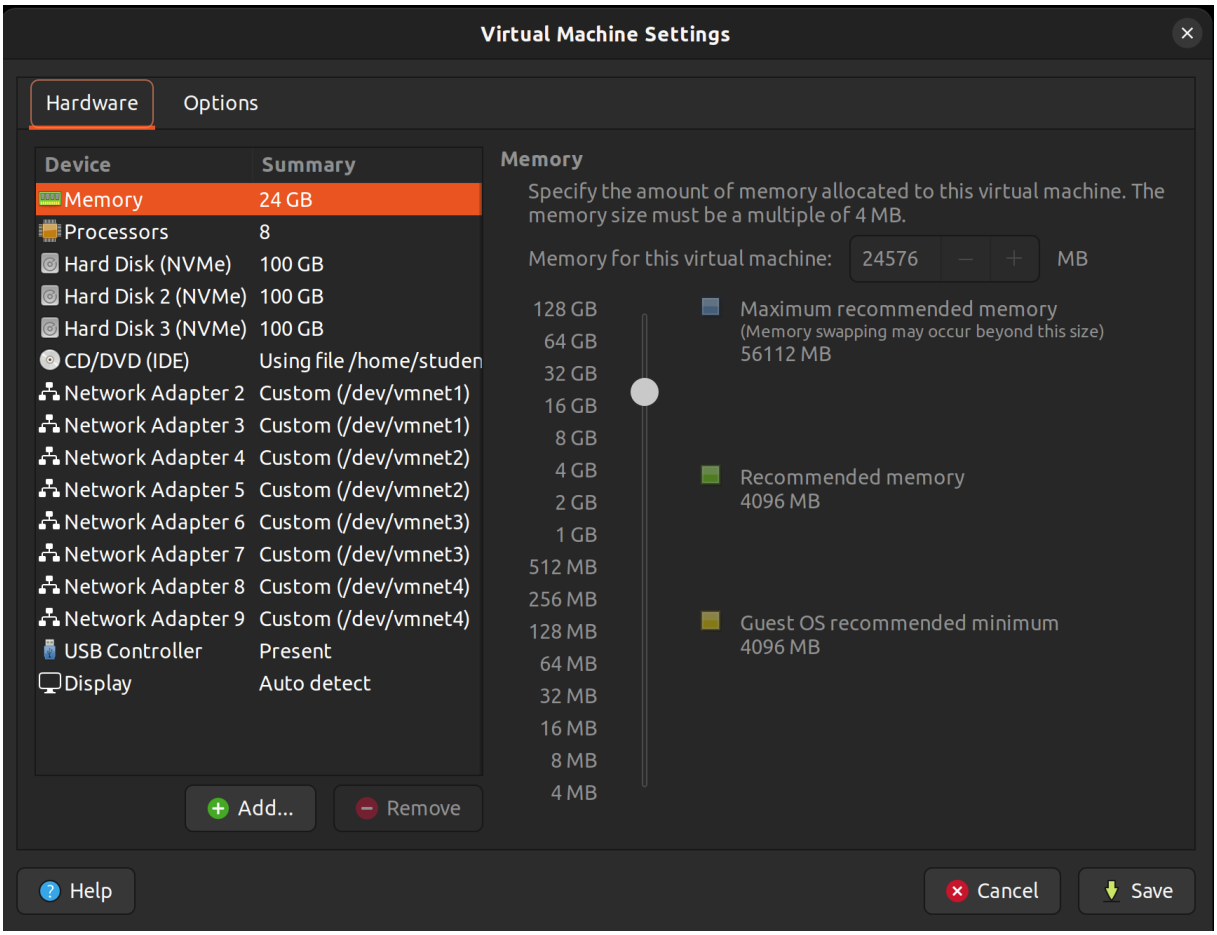

Figure IV.60 Configuration des serveurs ESXI.

Chaque serveur ESXI dispose principalement de

- 08 Cartes réseaux : nous avons doublé les cartes pour assurer la redondance
    - 02 pour le réseau management.
    - 02 pour le réseau de production.
    - 02 pour le réseau vMotion.
    - 02 pour le réseau vSan.
- Disques de stockage.
- 08 GB Processeur.

Pour l'installation, nous nous assurons que l'image (ISO) de l'ESXi sous le nom de (VMware-VMvisor-installer-8.0.0.update02-xxxxxxxx.iso) est montée et que le serveur est configuré pour démarrer sur CD-ROM dans le BIOS.

Une fois le CD démarré, le menu de démarrage de VMware ESXi s'affiche sous forme d'une interface de base appelée (DCUI) "Console-Directed User Interface" comme le montre la figure ci-dessous

Figure IV.61 Interface DCUI de l'installation de l'ESXI.

IV.3.1 Configuration des serveurs ESXI

La Console de l'interface utilisateur directe (DCUI) offre la possibilité d'engager des interactions avec l'hôte (le serveur ESXi) au niveau local, en se basant sur des menus textuels. Elle permet une configuration élémentaire des aspects tels que les paramètres réseau, les méthodes d'accès autorisées, le nom et le FQDN, tout en permettant également la visualisation des journaux, comme démontré dans la figure suivante

Figure IV.62 Interface d'accès de l'ESXI.

Pour pouvoir accéder à cette interface il nous faut introduire nos "Credentials"

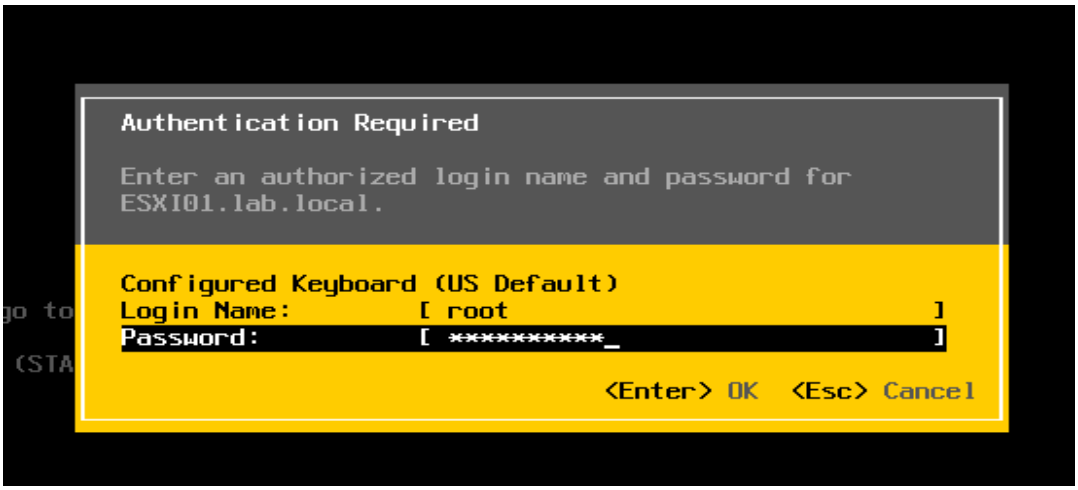

Figure IV.63 Fenêtre des informations d'identification.

Nous configurons les paramètres réseaux, le FQDN, les serveurs DNS et les noms d'hôtes.

La figure suivante illustre ces étapes

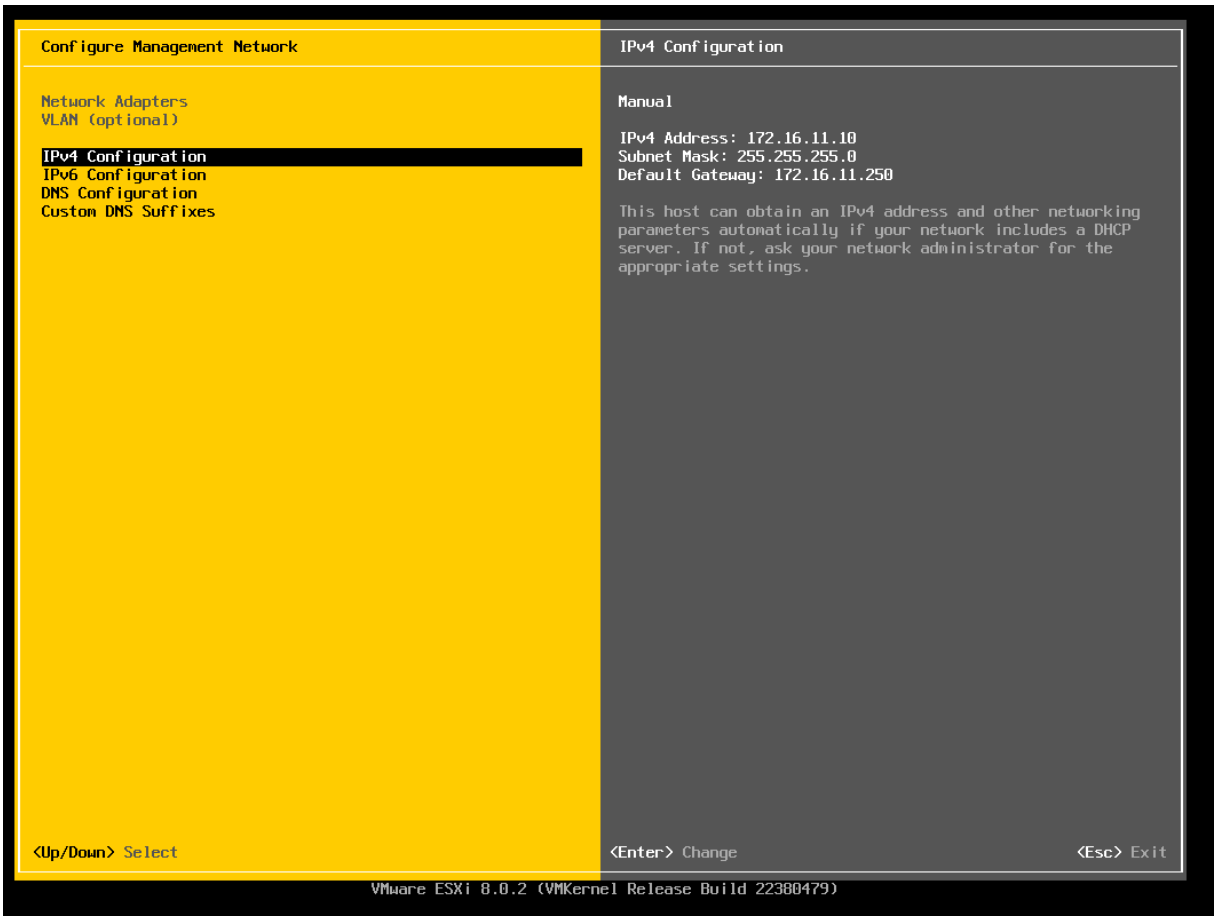

Figure IV.64 Interface de configuration des paramètres réseaux du serveur ESXI.

Une fois ces configurations achevées nous utilisons pour le reste des configurations, du monitoring et de l'utilisation des machines virtuelles, une autre interface appelée "ESXI Host Client".

Nous devons entrer l'adresse IP de l'hôte dans le navigateur, remplir les champs "Utilisateur" et "mot de passe" comme représenter dans la figure suivante

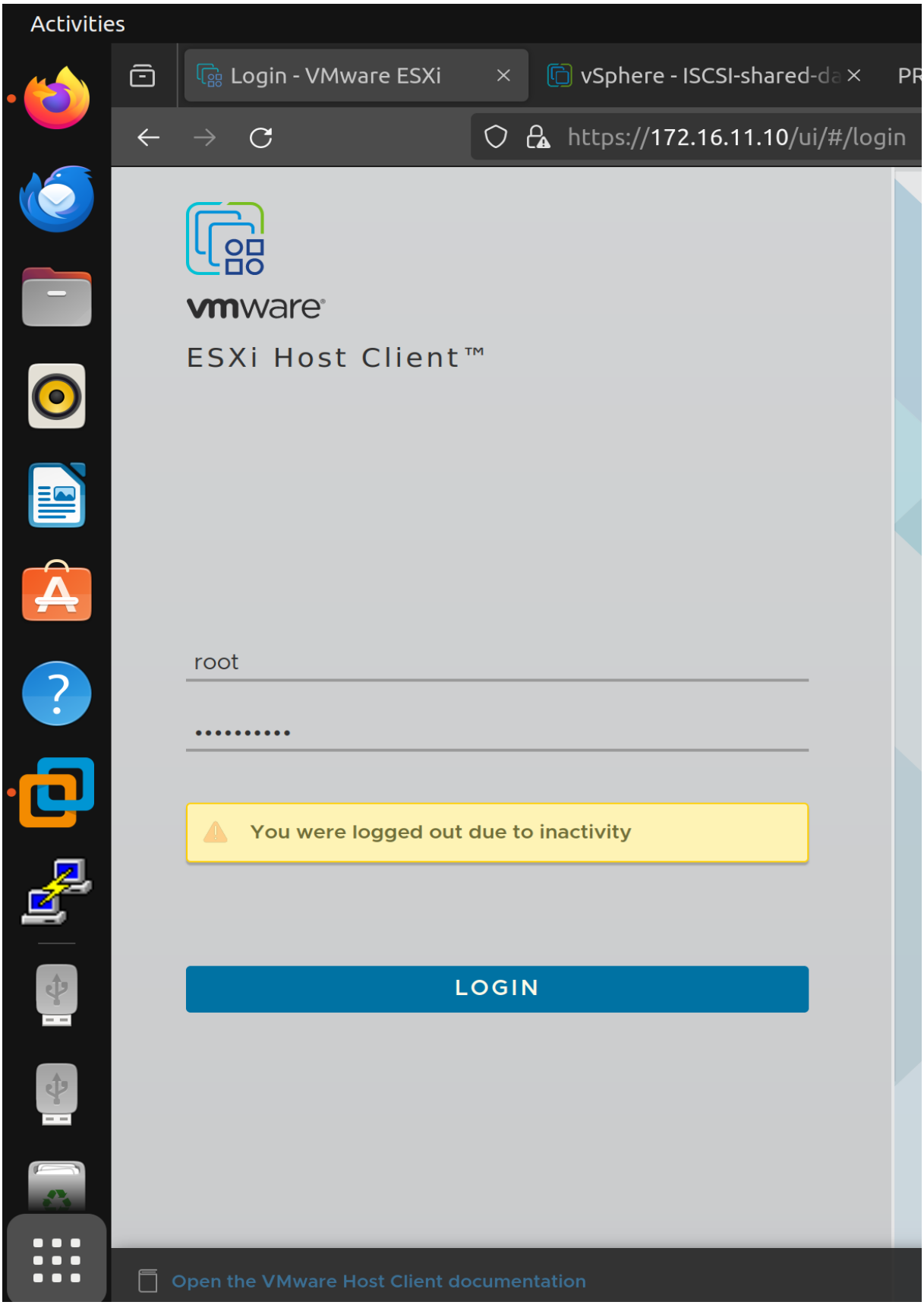

Figure IV.65 Accès au Host client via un navigateur.

La figure ci-dessous représente l'ESXI "Host Client"

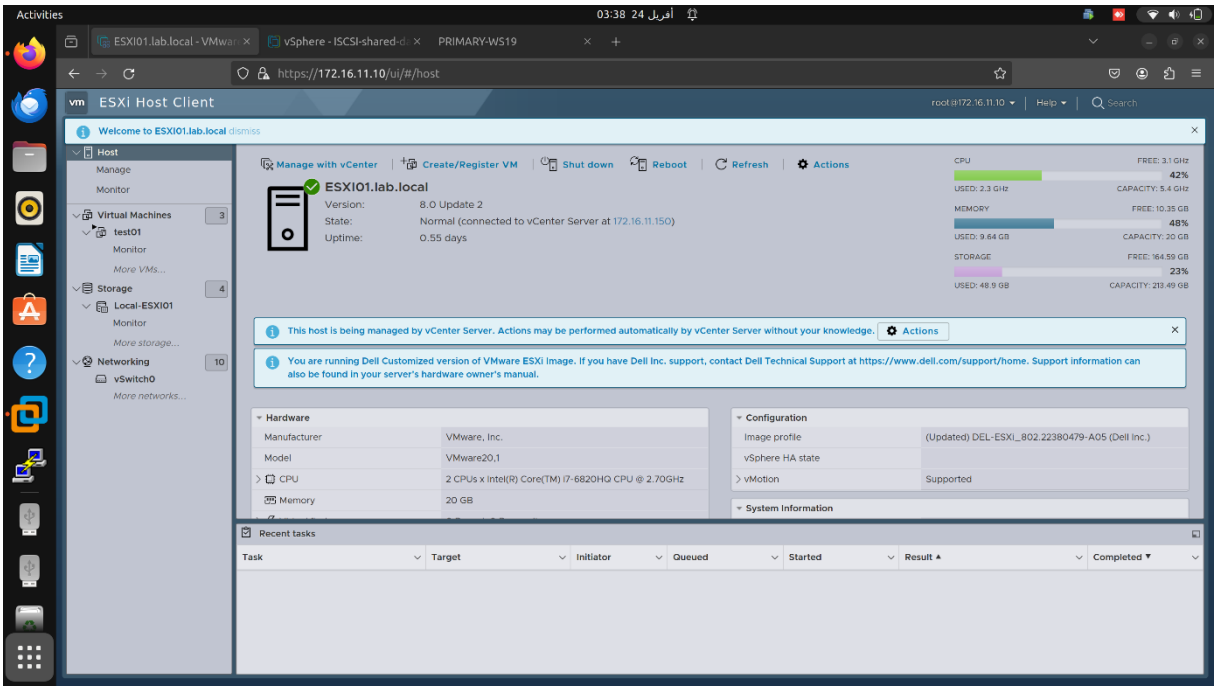

Figure IV.66 Interface d'accueil de l'ESXI Host Cient.

Comme le montre la figure, le "Host client" permet de tout manipuler sur un hôte ESXi : le stockage (banque de donnée ou data store), le réseau (VMkernel, vnic, port group), les machines virtuelles, le monitoring, le démarrage planifié, ainsi qu'une dizaine d'autres de manipulations.

IV.4 Installation vCenter sous forme de VCSA Appliance

Une fois nos trois serveurs ESXI bien installé et configuré nous avons procédé à l'installation du vCenter serveur. Pour lancer le programme d'installation, nous utilisons notre machine physique exécutant Ubuntu 22.04 puis nous accédons au contenu de l'image ISO du vCenter "VMware-VCSA-all- 8.0.2-XXXXX.iso" puis "vcsa-ui-installer lin64". A ce stade, nous lançons installer.exe.

A noter qu'il y a deux différents prototypes d'installation celle avec une interface graphique et celle avec une série de commande comme le montre la figure suivante

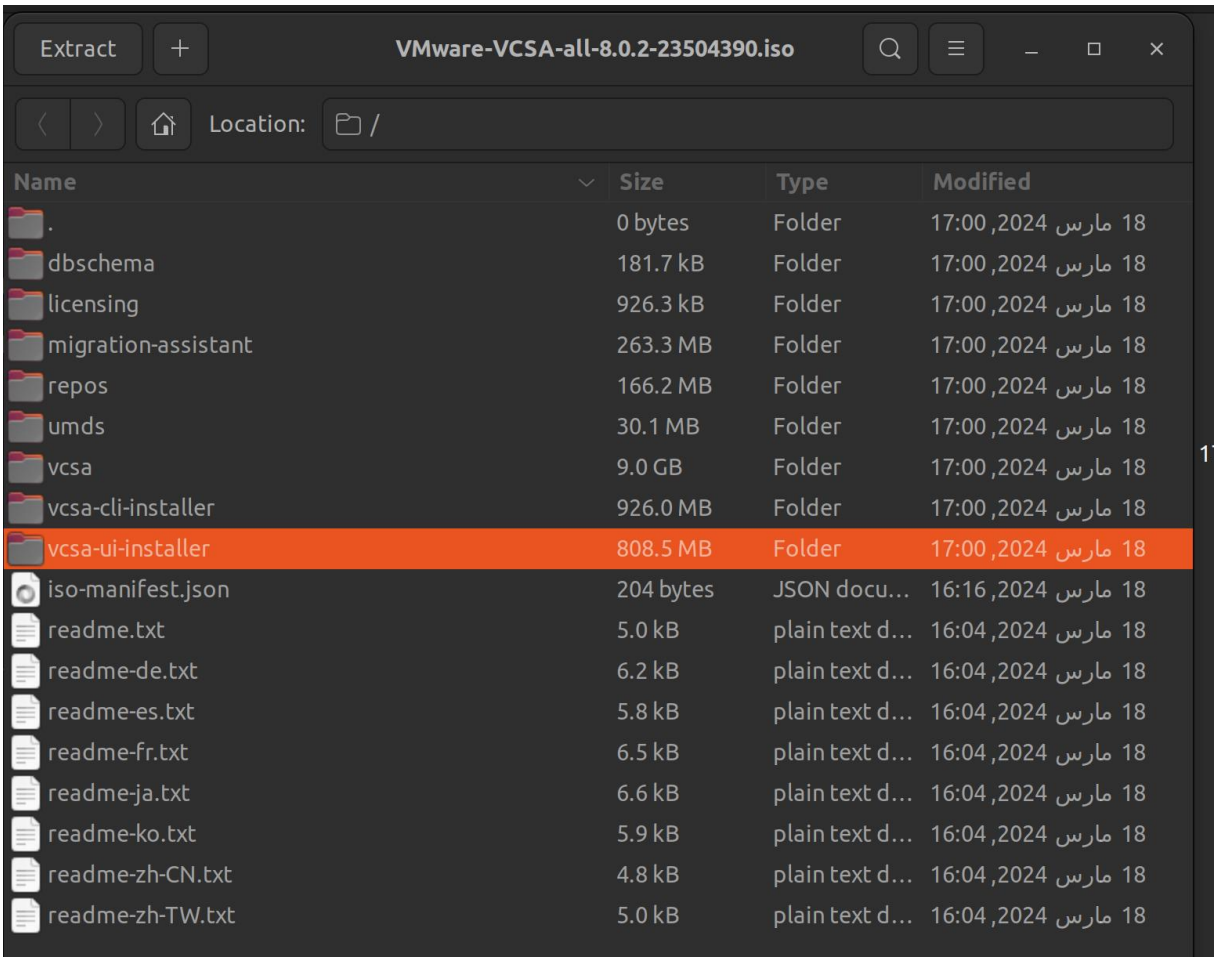

Figure IV.67 Les fichiers qui constituent l'image iso.

Nous avons opté pour l'installation via l'interface graphique qui est la méthode la plus simple.

Nous avons déployé notre vCenter sur une station de travail sous Ubuntu donc on a choisi le fichier d'installation adéquat

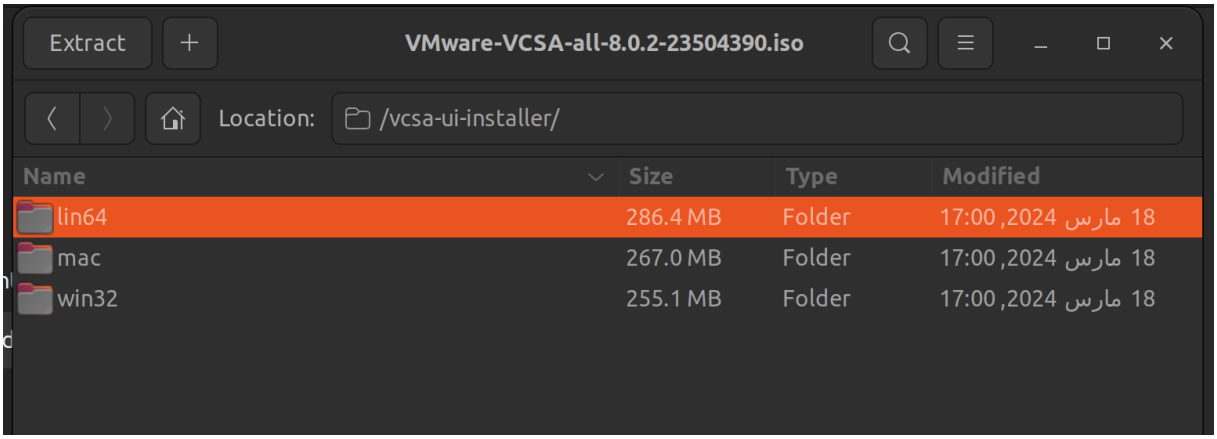

Figure IV.68 Fichier d'installation selon le type de système d'exploitation.

Le programme d'installation de vCenter Server Appliance 8.0.2 va démarrer après avoir double cliquer sur l'instance installer dans le fichier

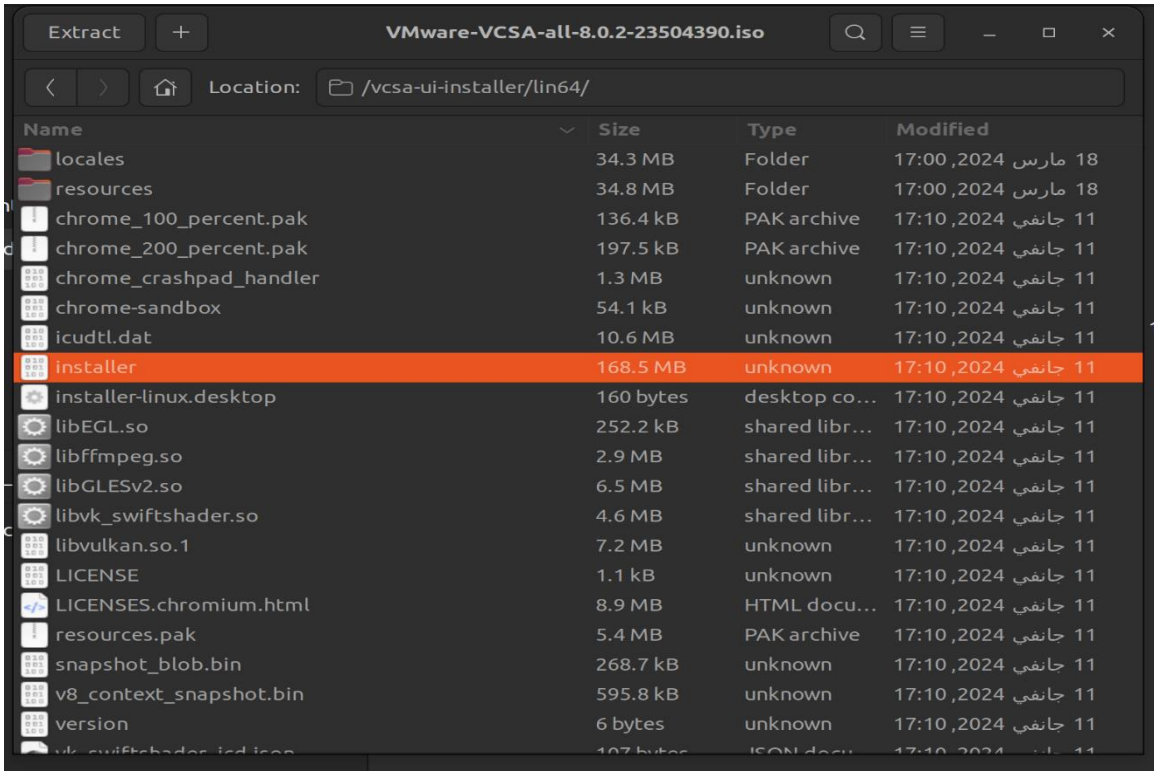

Figure IV.69 Fichier exécutable de l'installation.

Nous allons faire une installation pour la première fois donc nous choisissons "installer". Le processus d'installation consiste en deux étapes distinctes. Dans la première étape, nous allons déployer "l'Appliance", puis dans la deuxième étape, nous allons la configurer

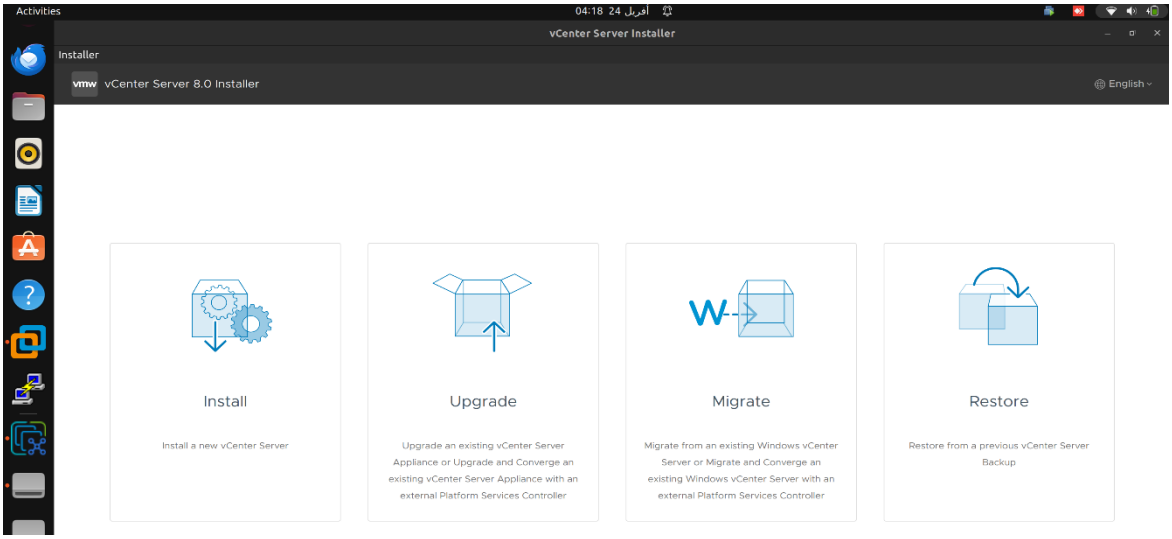

Figure IV.70 VMware vCenter installation.

Nous allons accepter les termes du contrat de licence, puis nous choisissons un type de déploiement standard "instance intégrée de plateforme service Controller" qui veut dire que le vCenter sera déployé dans un même dispositif. Les figures suivantes montrent ces étapes

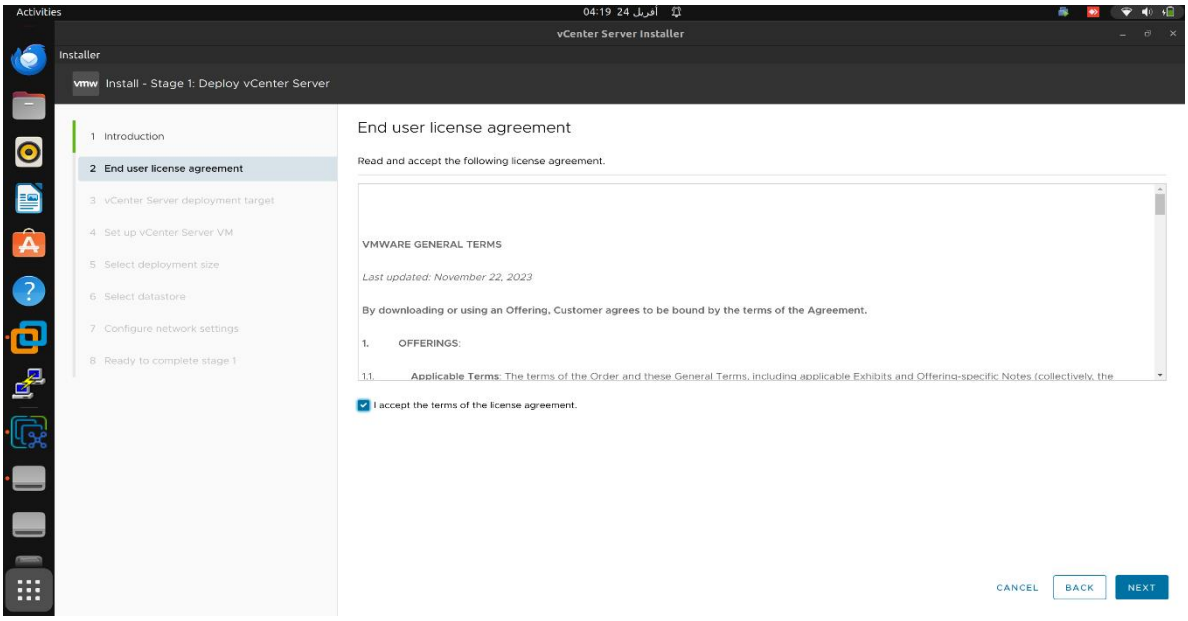

Figure IV.71 Termes du contrat de licence.

Le vCenter sera mis en place sous une machine virtuelle dans un des hôtes ESXi. Pour cela, nous devons maintenant entrer les détails du serveur cible ESXi sur lequel nous allons déployer l'Appliance "VCSA 8"

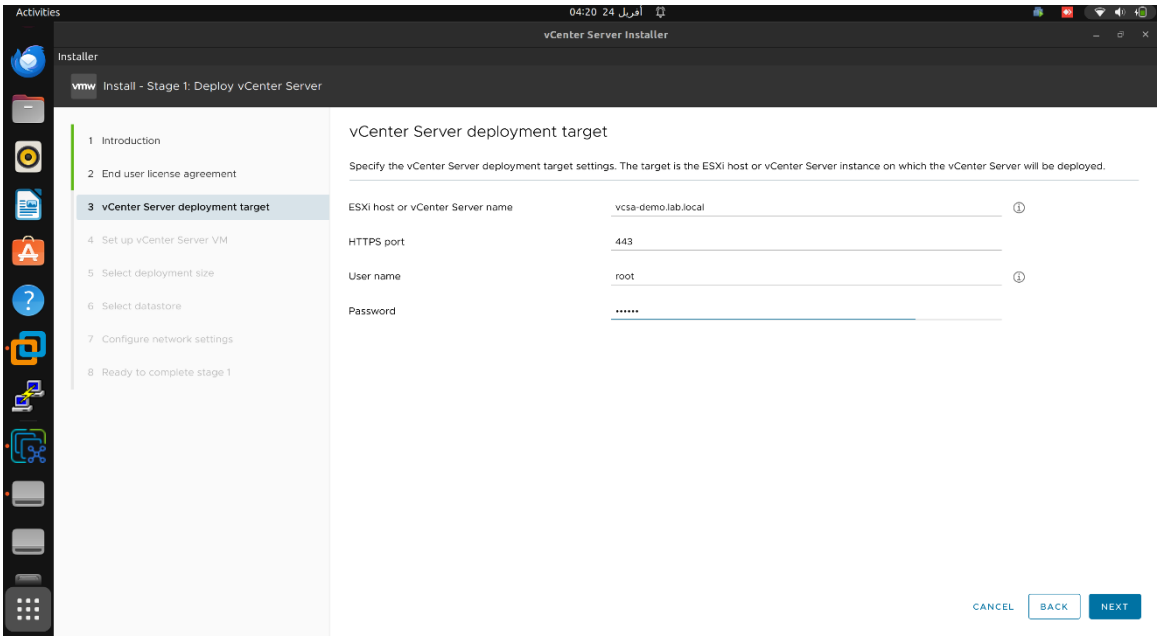

Figure IV.72 Information du serveur cible.

Nous devons maintenant configurer le nom de l'Appliance (il s'agit du nom de la VM déployée plus tard sur l'hôte ESXi et non du nom de domaine complet de vCenter) et le mot de passe du root

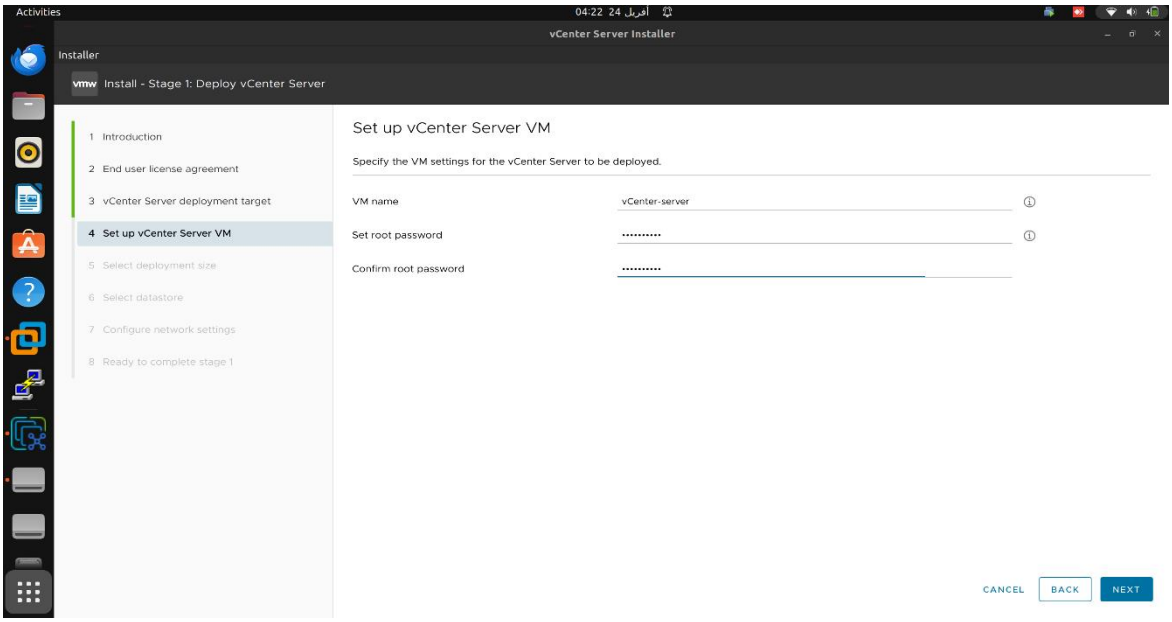

Figure IV.73 Configuration de la VM du vCenter.

Pour l'étape suivante, nous devons sélectionner la taille du déploiement. Comme notre infrastructure contient 3 hôtes, nous choisissons la configuration "Tiny" qui a comme fourchette (2-10) hôtes, puis pour le disque de stockage, nous choisissons le data store du serveur cible bien évidement

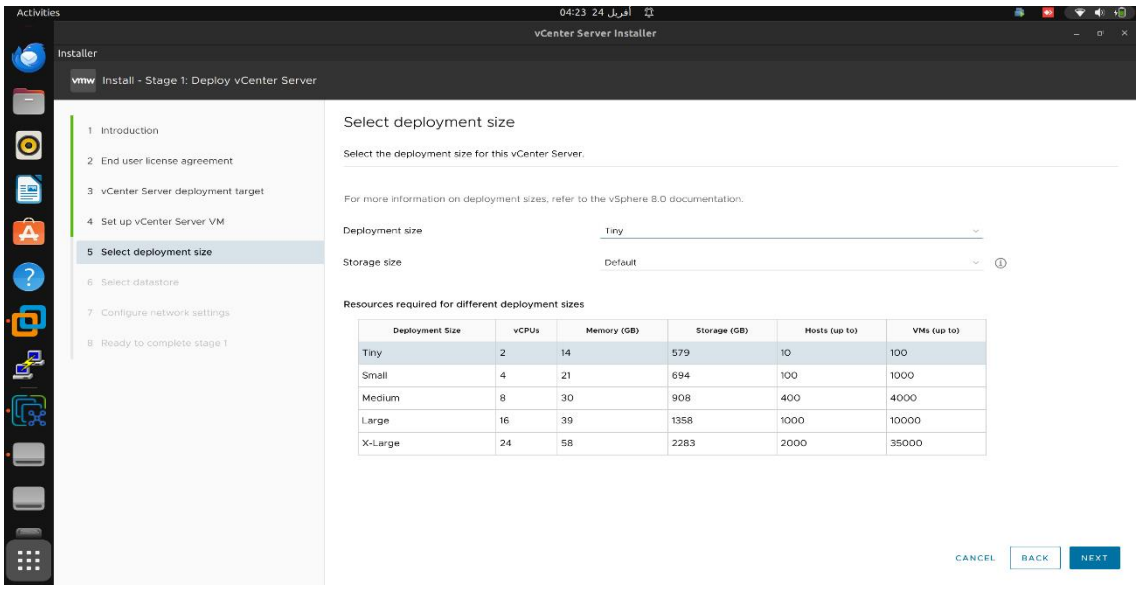

Figure IV.74 Taille de l'infrastructure.

Après avoir validé les étapes précédentes, nous devons sélectionner le datastore ciblé qui va héberger notre vCenter

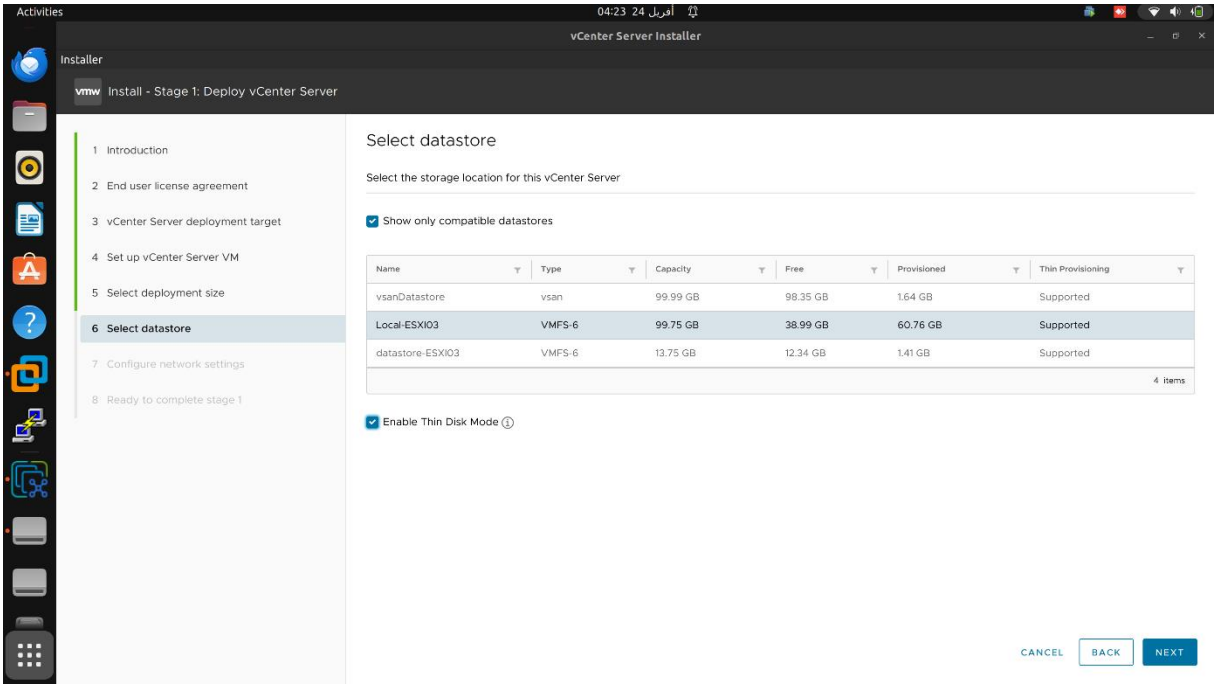

Figure IV.75 Sélection du Datastore.

Après avoir validé les étapes précédentes, nous devons configurer les paramètres réseaux

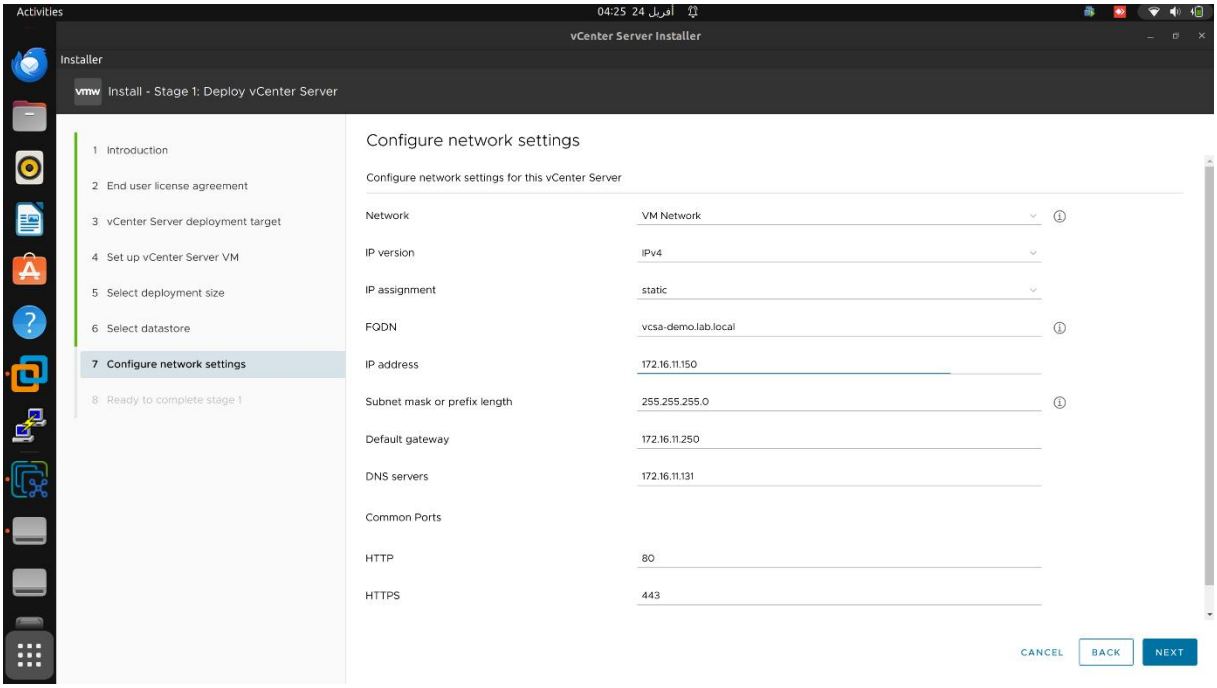

Figure IV.76 Configuration des paramètres réseaux.

Le port groupe par défaut se trouve sur le vSwitch0 qui est le vSS "virtuel standard switch" par défaut, cette configuration va être migrée plus tard vers un vDS "virtuel distributed switch".

L'assistant démarre maintenant pour déployer "vCenter Server Appliance 8" après avoir cliqué sur "Finish"

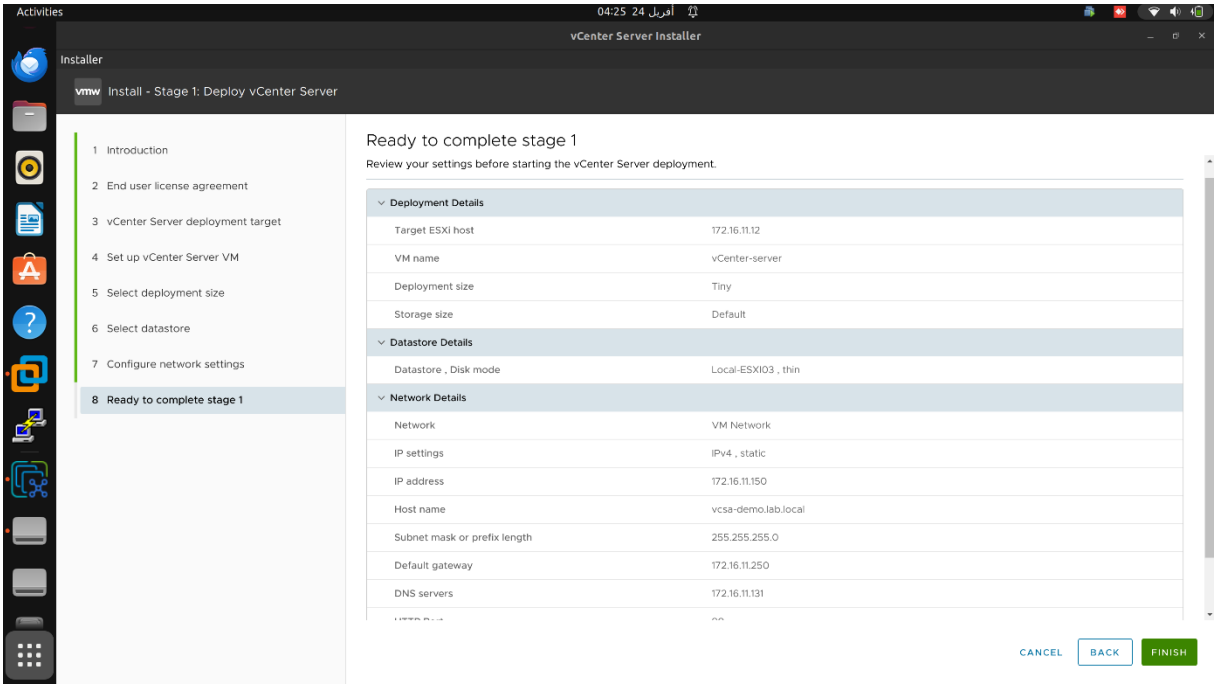

Figure IV.77 Récapitulatif des configurations établies.

La première étape est maintenant terminée. L'Appliance est prête et sous tension sur le serveur ESXi ciblé. Pour passer à la deuxième étape, cliquons sur Continuer.

L'assistant de l'étape 2 commence. Cliquons sur Suivant

Figure IV.7 Lancement de la 2ème phase d'installation.

A ce stade nous devons choisir

Le mode de synchronisation de l'heure : nous pouvons nommer le serveur NTP souhaité, mais nous optons pour la synchronisation avec l'hôte ESXi, car notre infrastructure ne contient pas de serveur NTP pour l'instant.

L'activation de SSH que nous laissons désactivé à l'instant puisque nous allons accéder par web client principalement.

La configuration SSO nous choisissons le nom de domaine "lab.local", le mot de passe et le nom du site

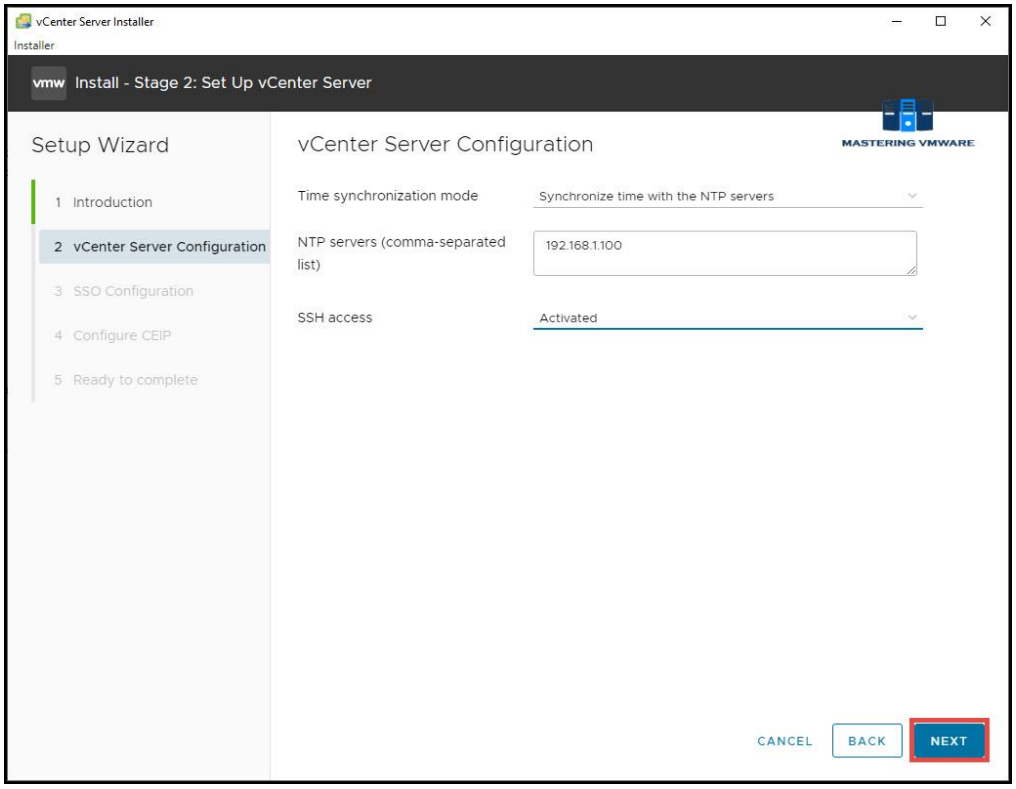

Figure IV.79 vSphere Client.

La décision de rejoindre le programme d'amélioration de l'expérience client VMware : nous choisissons non et cliquons sur Suivant.

La configuration de l'Appliance commence maintenant. Notons que nous n'avons pas de bouton pour annuler le processus

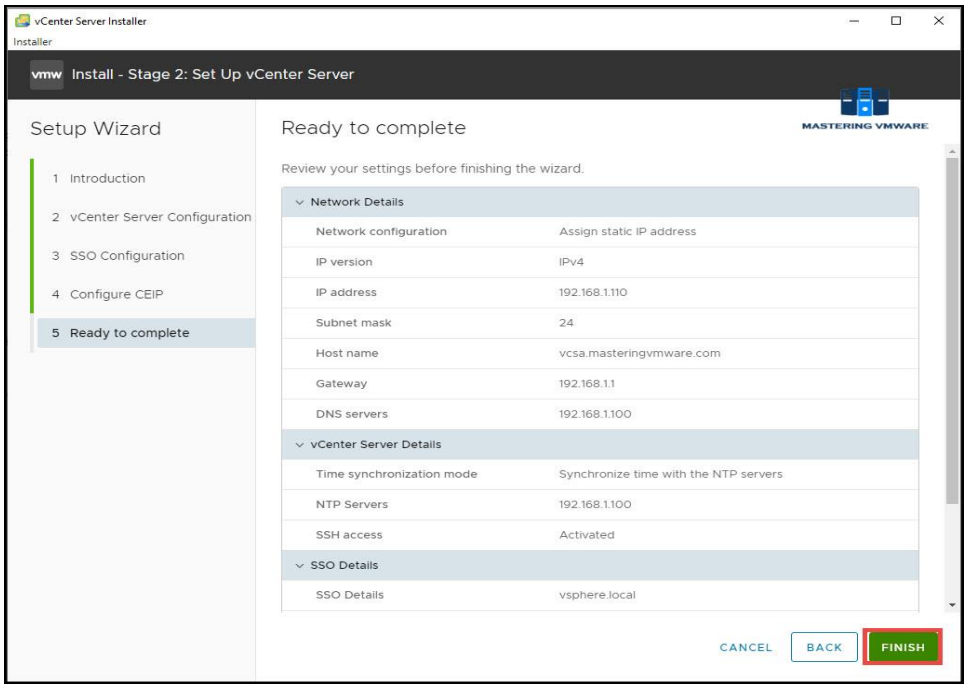

Figure IV.80 vSphere Client.

Maintenant que le vCenter et installé et prêt à être utilisé, pour y accéder on ouvre un navigateur internet et on tape l'adresse IP ou FQDN de ce dernier comme indiqué dans cette figure

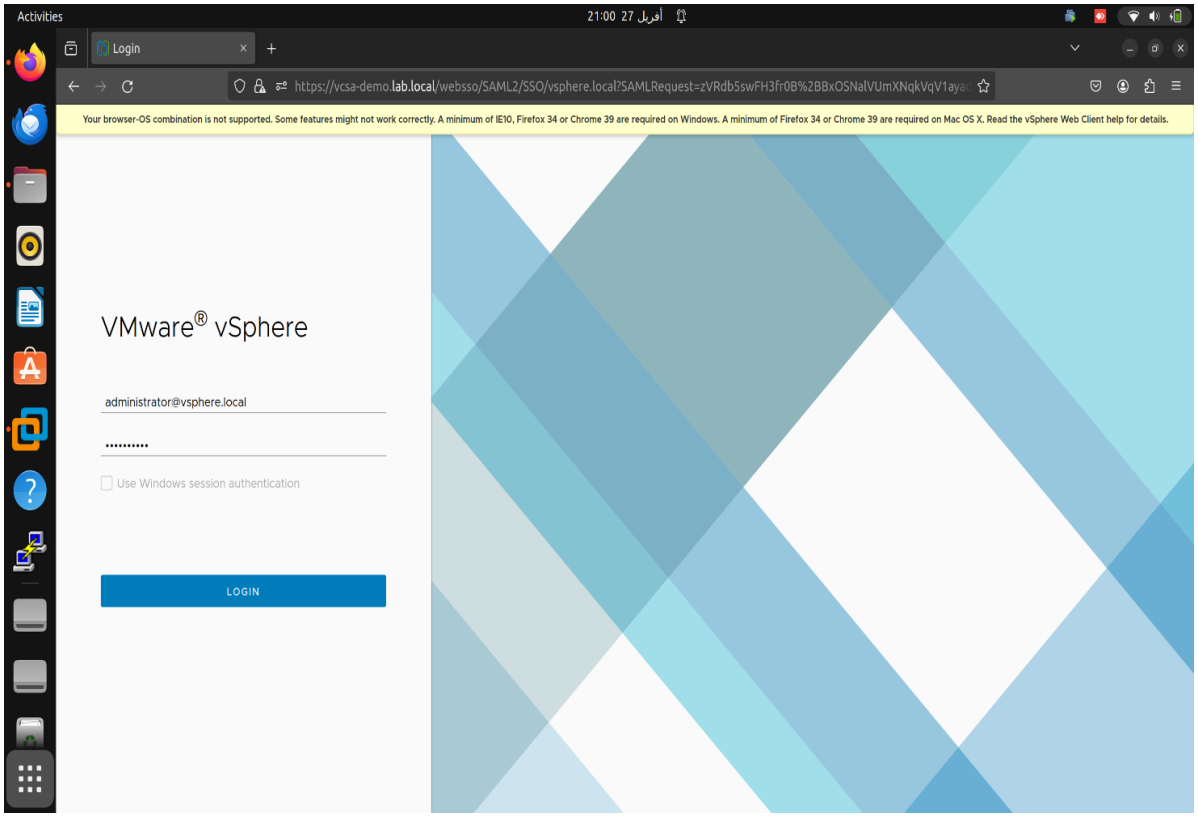

Figure IV.81 vSphere Client.

IV.4.1 Configuration du vCenter

Maintenant que notre vCenter est installé et opérationnel on pourra commencer les configurations

IV.4.2 Installation du Datacenter

Nous allons maintenant créer notre Datacenter comme indiqué sur ces figures

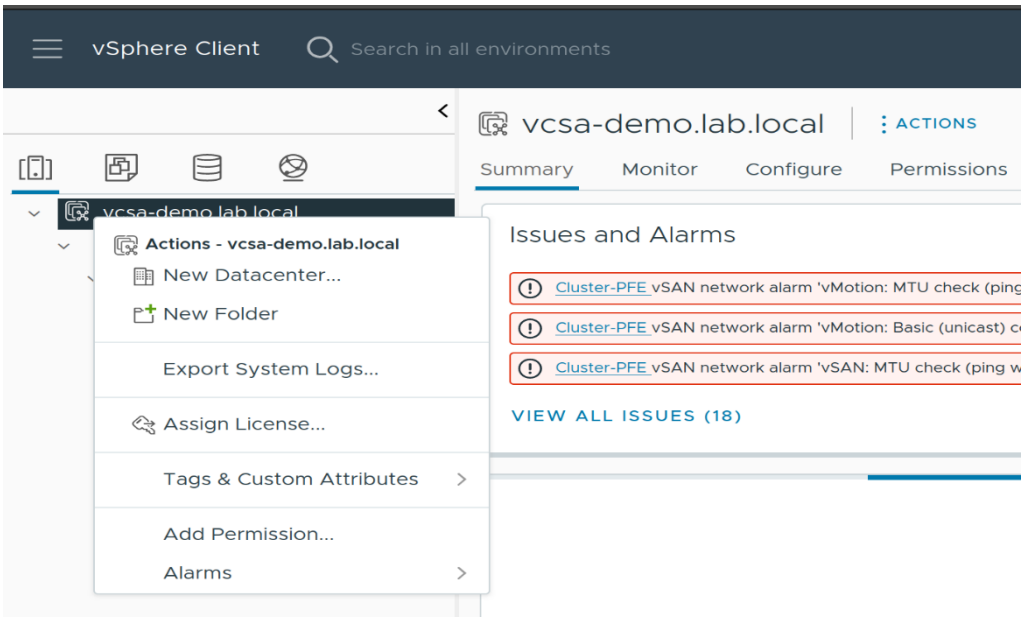

Figure IV.82 Créer un Datacenter.

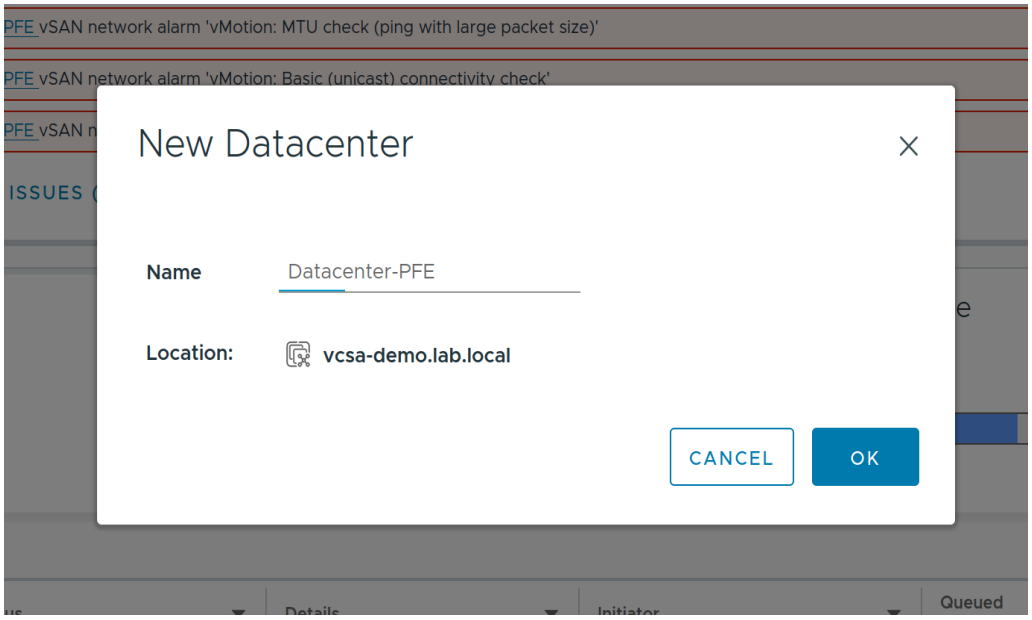

Figure IV.83 Nom du Datacenter.

Maintenant que le Datacenter a été créé on va ajouter nos hôtes ESXI dans le Datacenter

On va regrouper le tout dans un cluster et pour ce faire on va créer un

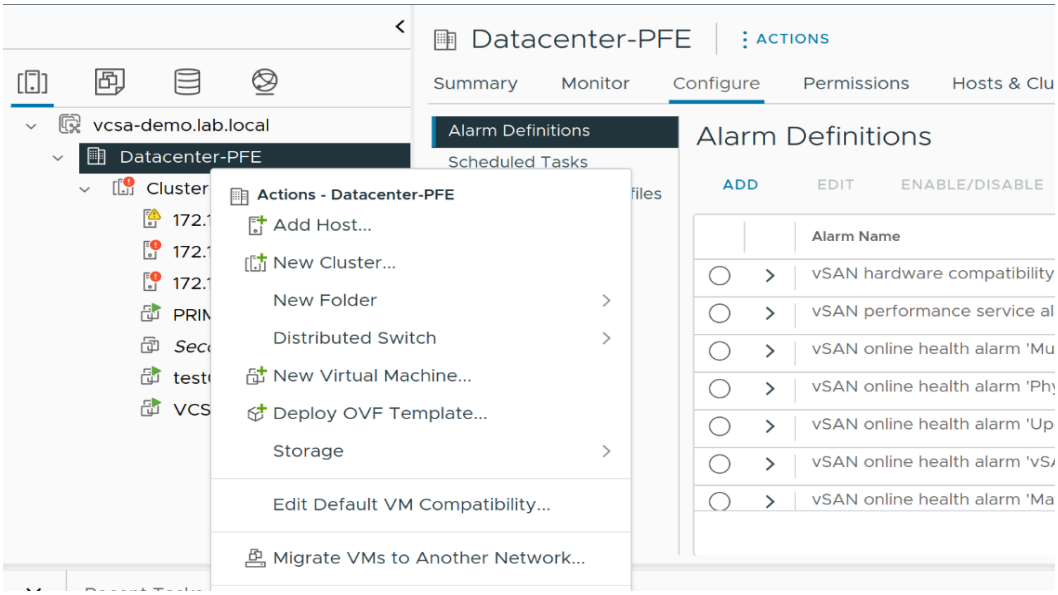

Figure IV.84 Création d'un cluster.

IV.4.3 Installation du Cluster

Afin de pouvoir utiliser les fonctionnalités vSAN, le DRS et HA nous allons mettre en place un cluster dans le data center. Nous activons ses fonctionnalités à la création

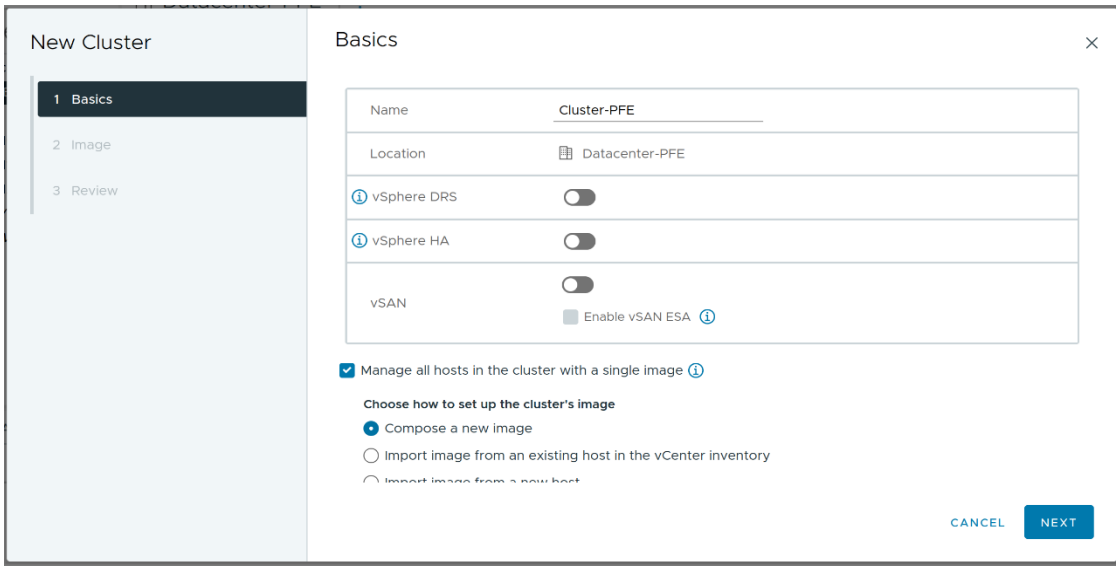

Figure IV.85 Paramétrage du cluster.

Nous ajoutons tous les hôtes (avec IP ou FQDN) au cluster afin de créer un pool de ressources

IV.4.4 Installation du Switch Virtuel Distribué

Une fois le Datacenter et le cluster créer et configurer on va créer le virtuel switch distribué

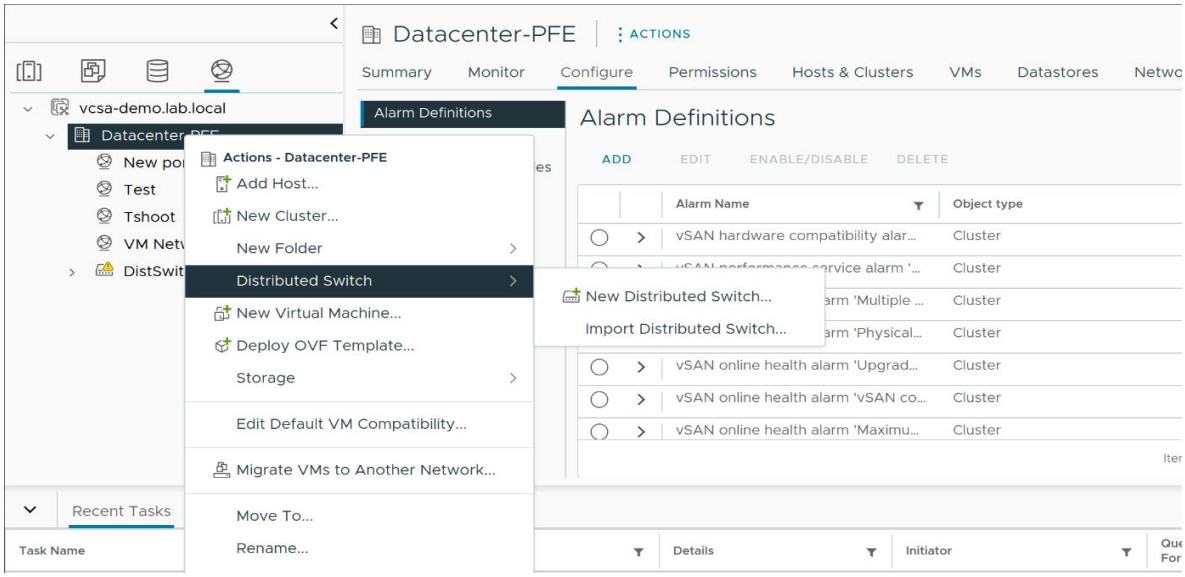

Figure IV.86 Créer un nouveau switch distribué**.**

Donner un nom au vDS

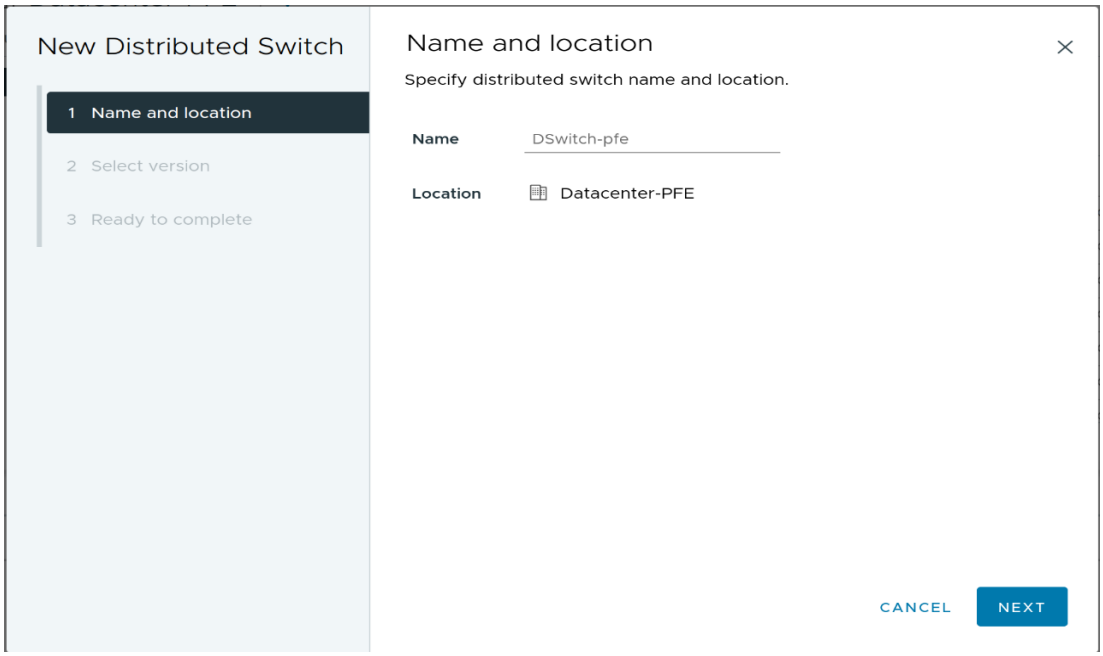

Figure IV.87 Nommer le VDS.

Sélectionner la version utilisée de l'ESXI

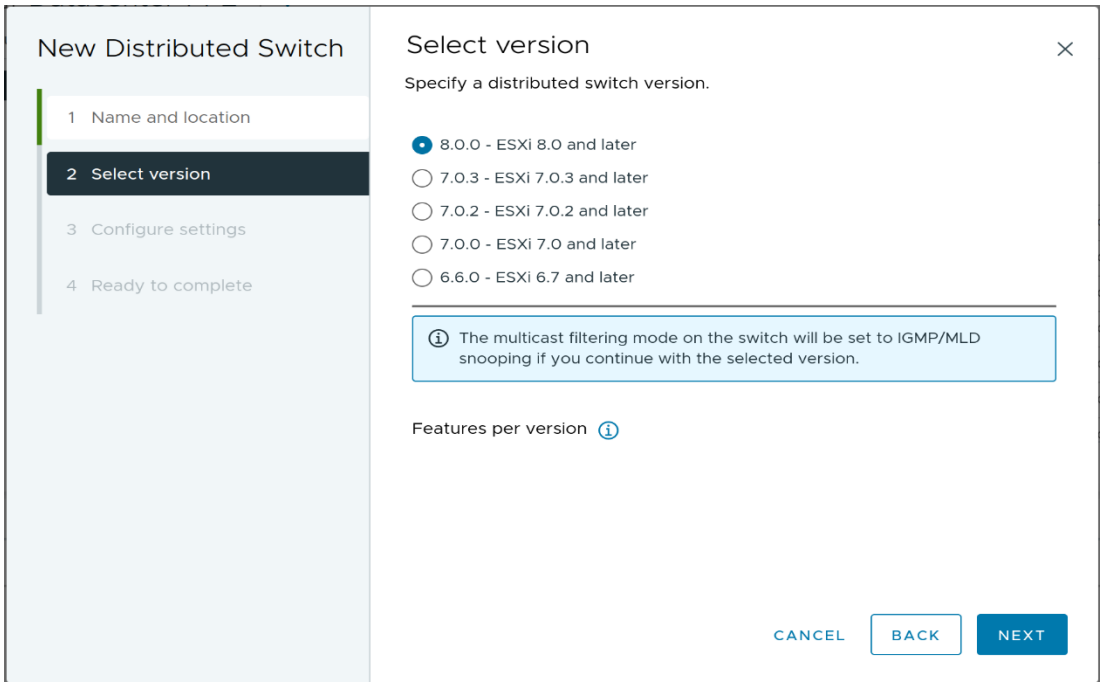

Figure IV.88 Sélectionner la version.

Paramétrer le vDS selon nos besoins

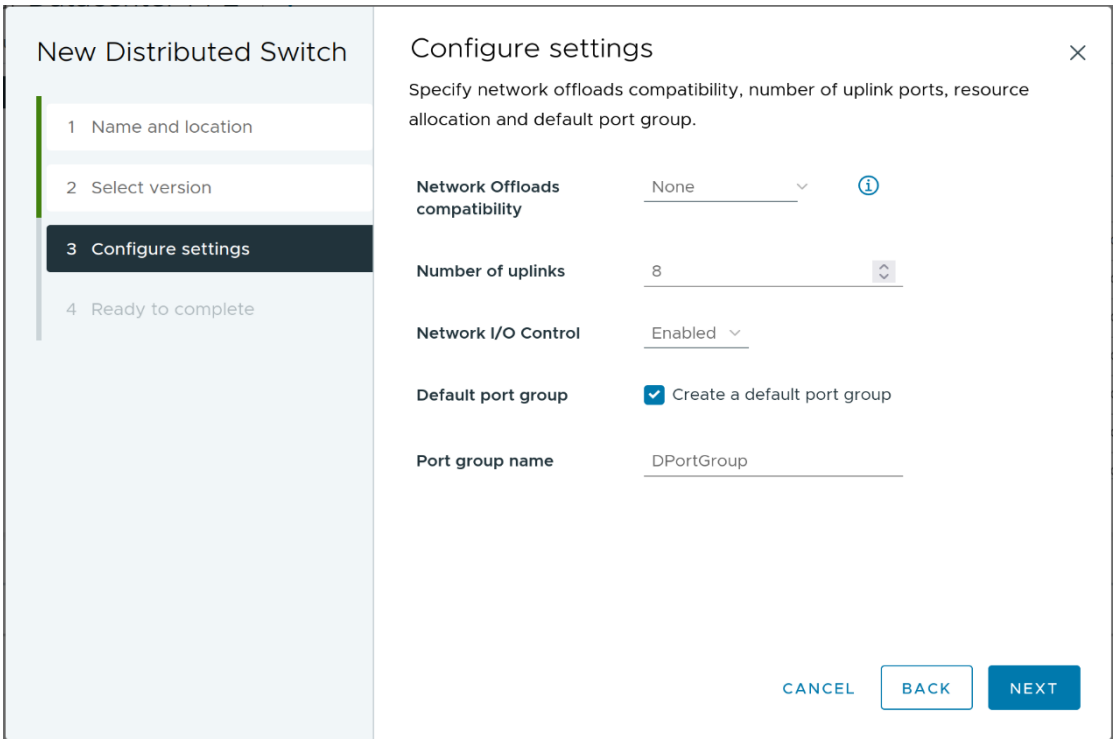

Figure IV.89 Paramétrage du vDS.

Terminer les configurations en cliquant sur "Finish"

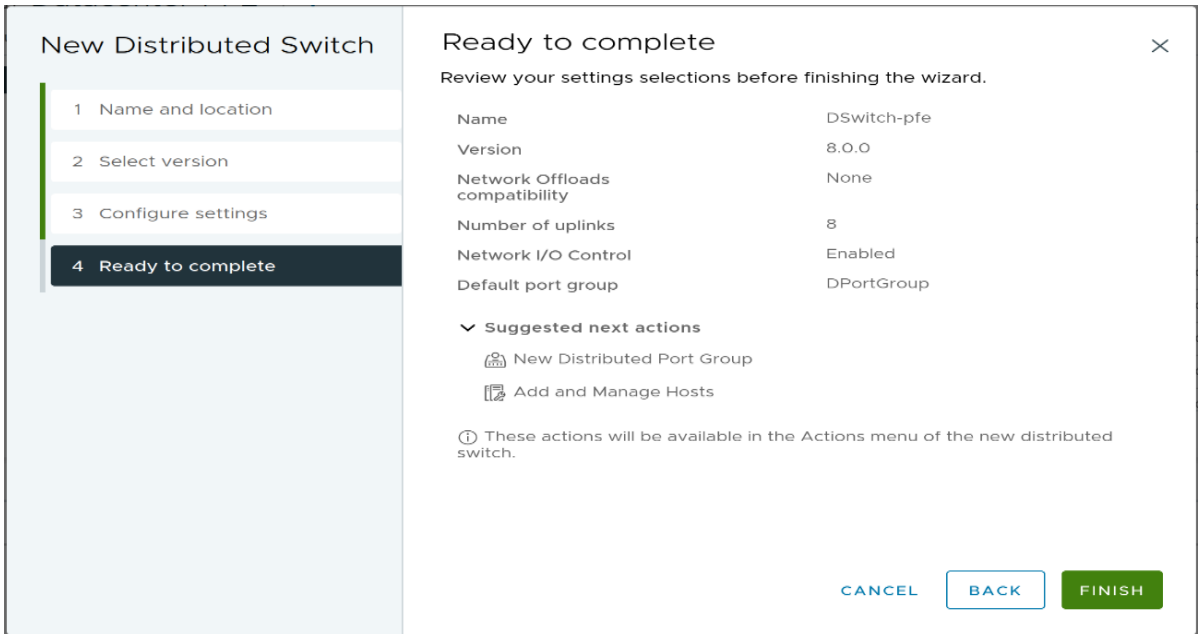

Figure IV.90 Récapitulatif des configurations établies.

Une fois notre vDS créer nous allons faire la migration des carte réseaux préalablement configuré sur le vSS, une fois la migration faite la topologie de vDS va être comme l'indique la figure ci-dessous

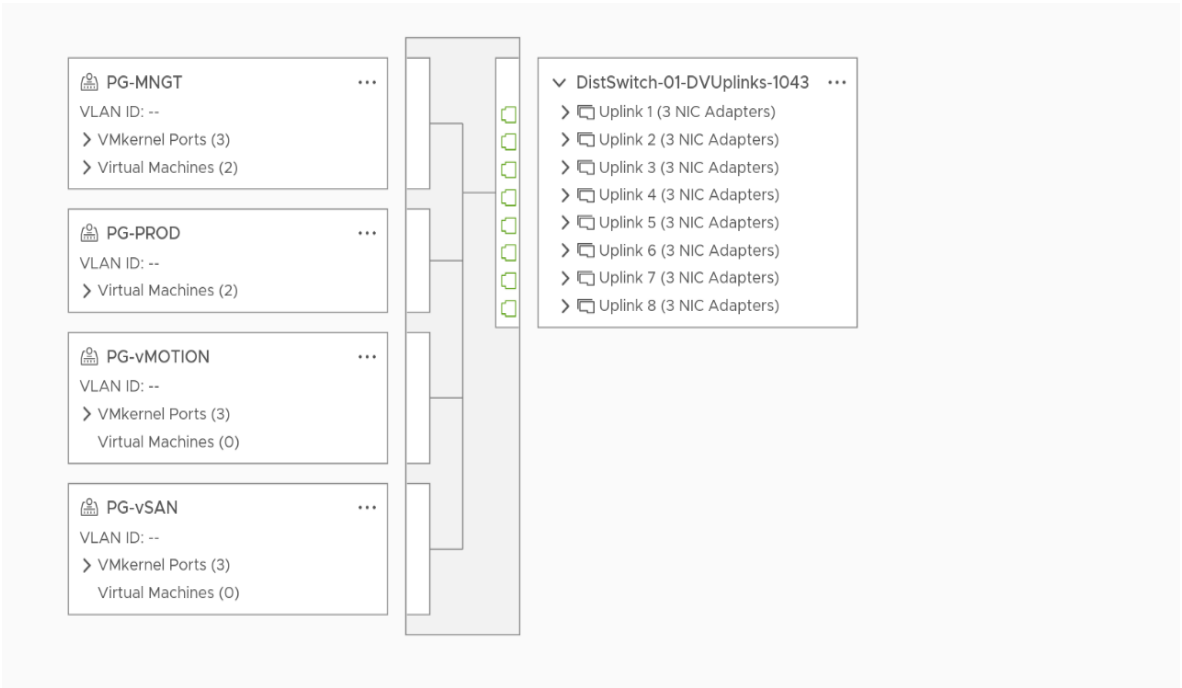

Figure IV.91 Topologie de vDS.

IV.5 Activation du DRS

DRS est une fonctionnalité Cluster, pour l'activer on fait un clique droit sur le cluster, dans l'onglet configuration on clique sur "Edit" et sélectionne DRS.

Cette interface va s'afficher

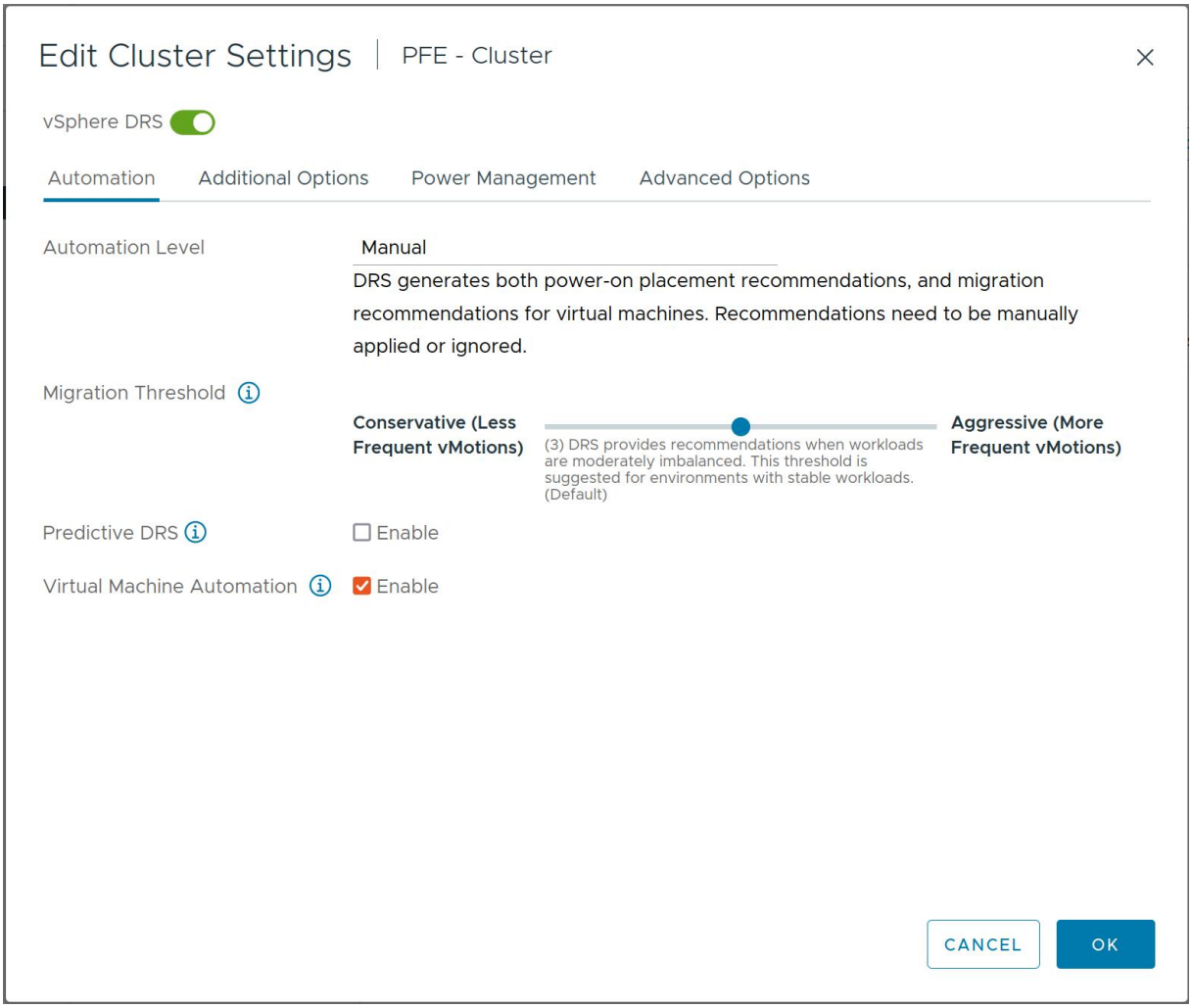

Figure IV.92 Activation du DRS.

Parmi 3 niveaux d'automatisation, nous avons choisi : Manuel, avec un seuil de migration qui est moyen, nous avons également activé l'option d'automatisation des VMs.

IV.5.1 Activation du HA

Après avoir activer DRS, nous allons activer HA qui viia cette interface

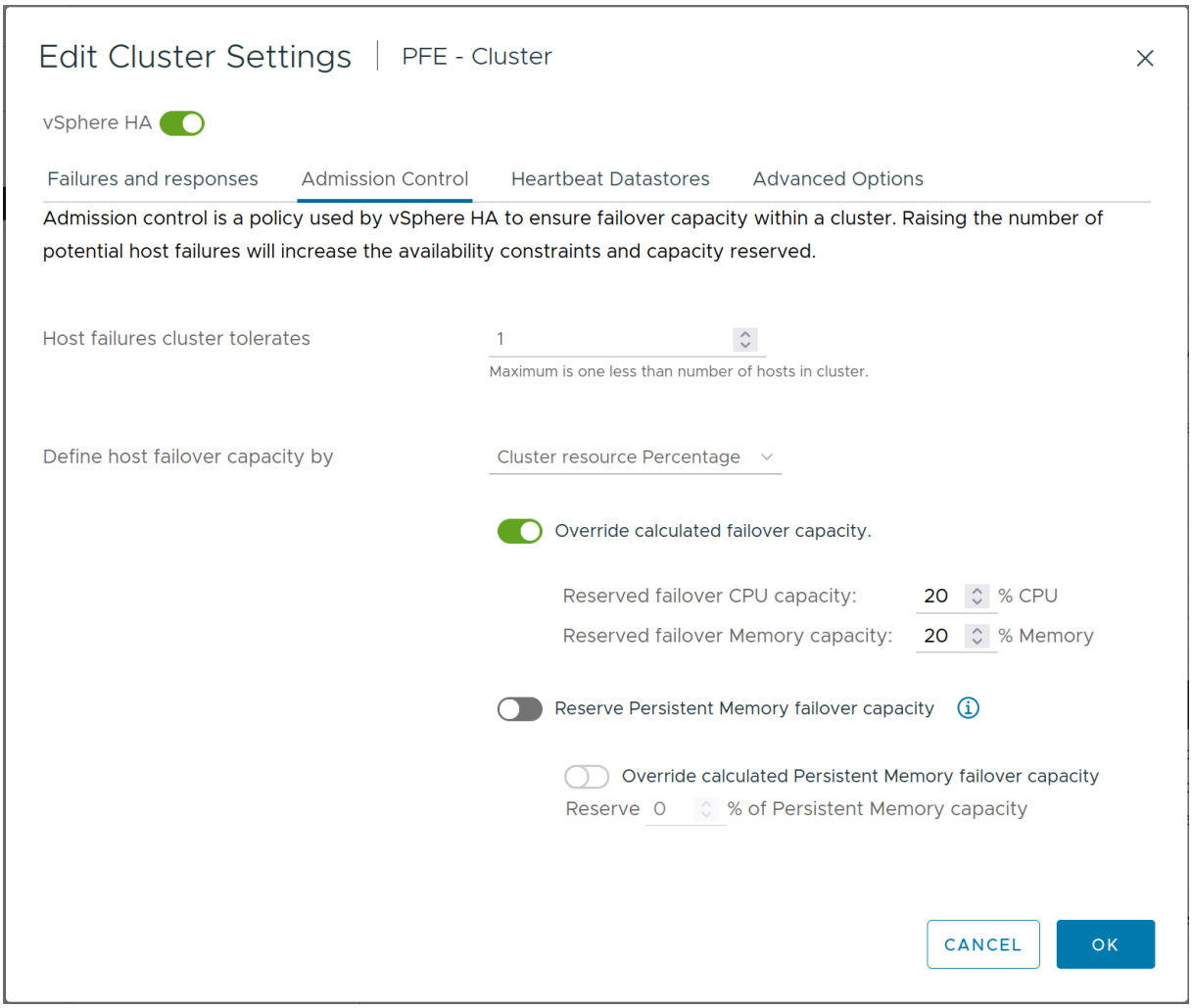

Figure IV.93 Activation du HA.

Nous allons spécifier les paramètres et les comportements liés aux pannes des hôtes et des VMs.

Nous spécifions ainsi le nombre de pannes à tolérer et le pourcentage de ressources dédié au service HA et le pourcentage de dégradation toléré.

IV.6 Installation, Configuration et mise en place des services

Nous allons installer et configurer tous nos services sur une seule et même machine virtuelle Windows server 2019.

IV.6.1 Active Directory Domain Service

On commence par le service "ADDS Active Directory Domain Services" en suivant ces étapes :

Premièrement la sélection du rôle et fonctionnalités

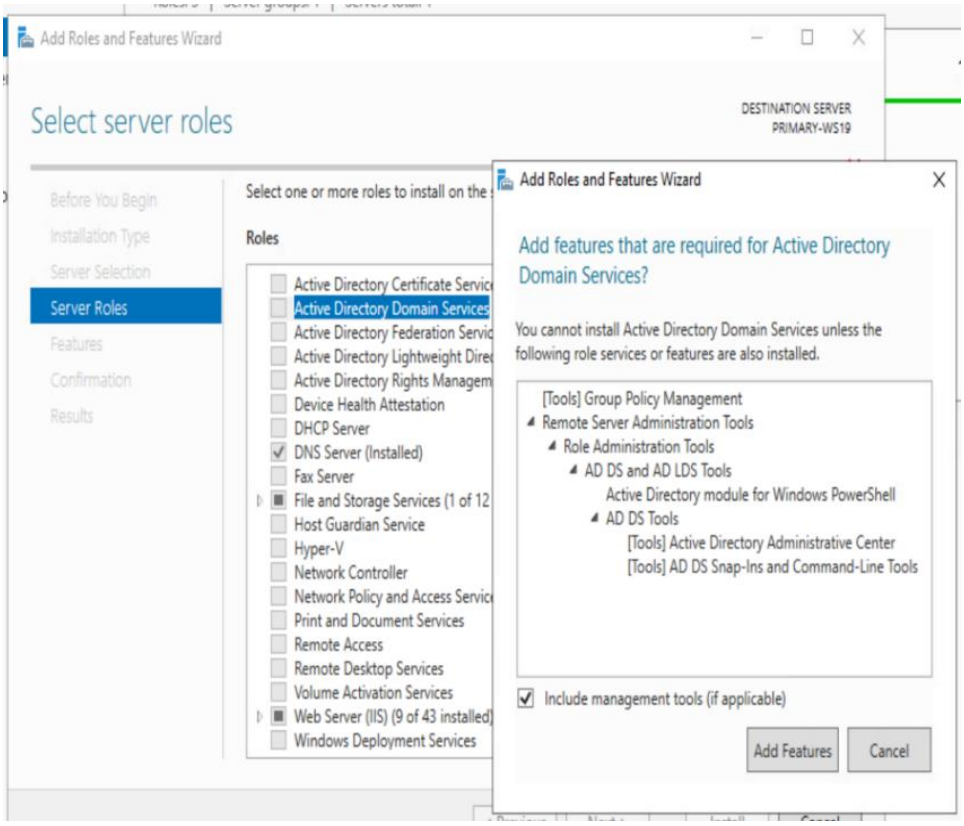

Figure IV.94 Ajout du rôle et fonctionnalités.

Lancer l'installation du rôle ADDS

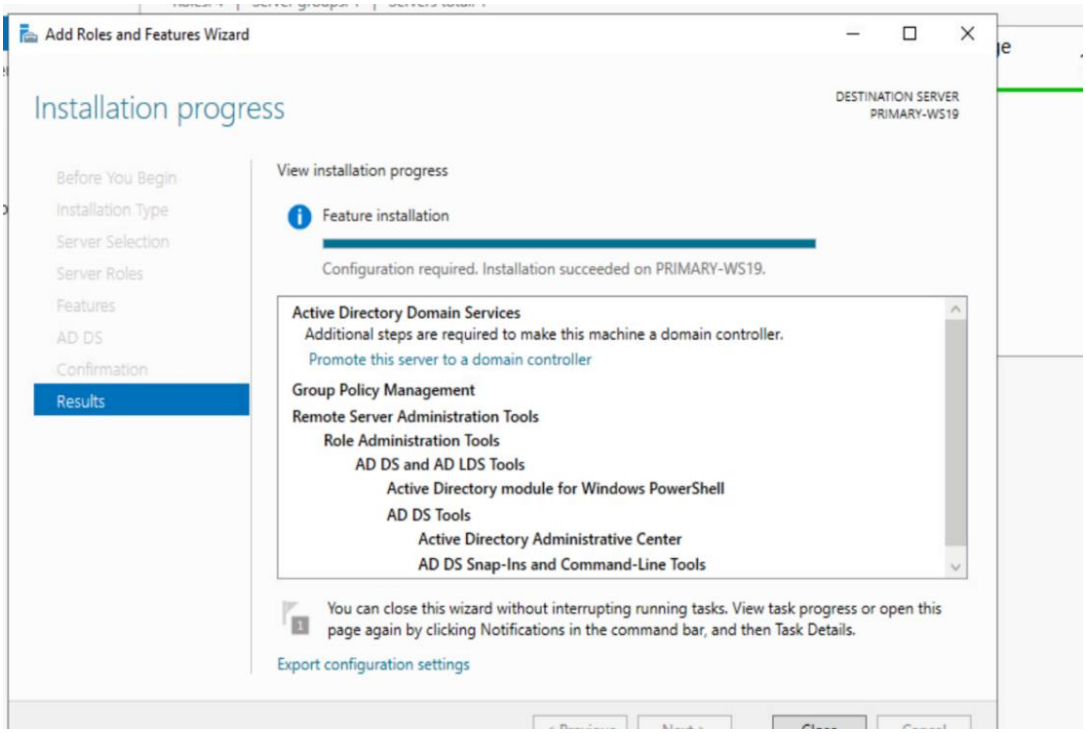

Figure IV.95 Installation du service.

On donne un nom de domaine, "lab.local" pour notre cas

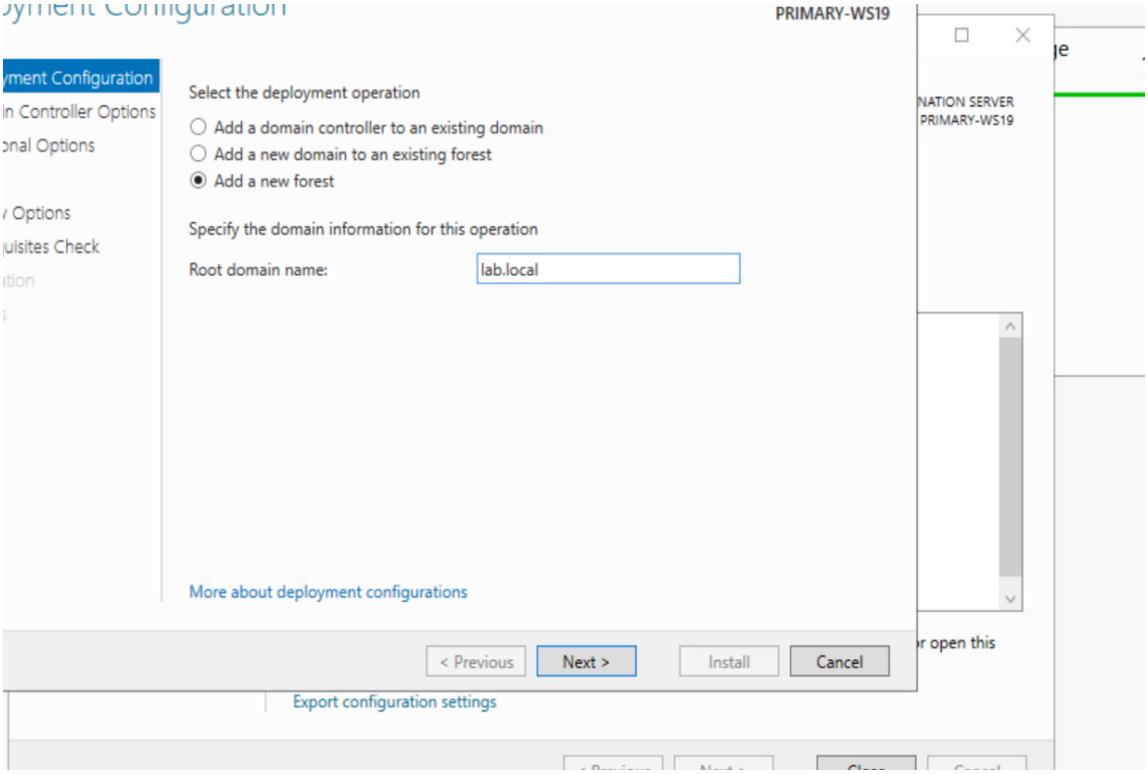

Figure IV.96 Définir un nom de domaine.

Etablir un mot de passe qui doit être assez robuste

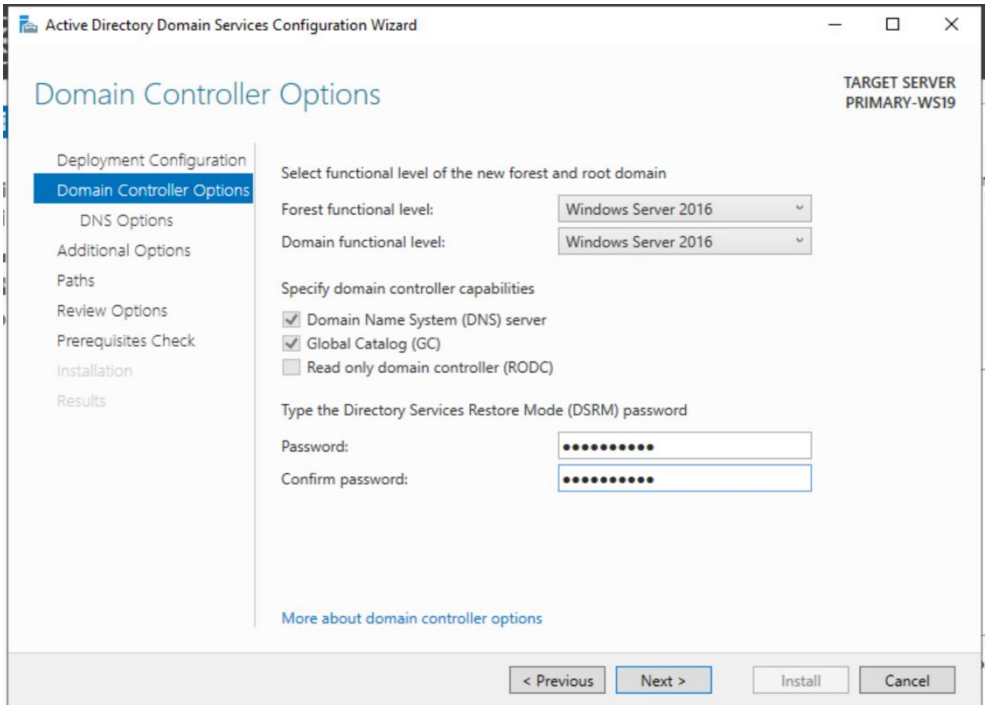

Figure IV.97 Mot de passe.

Récapitulatif des configurations établies

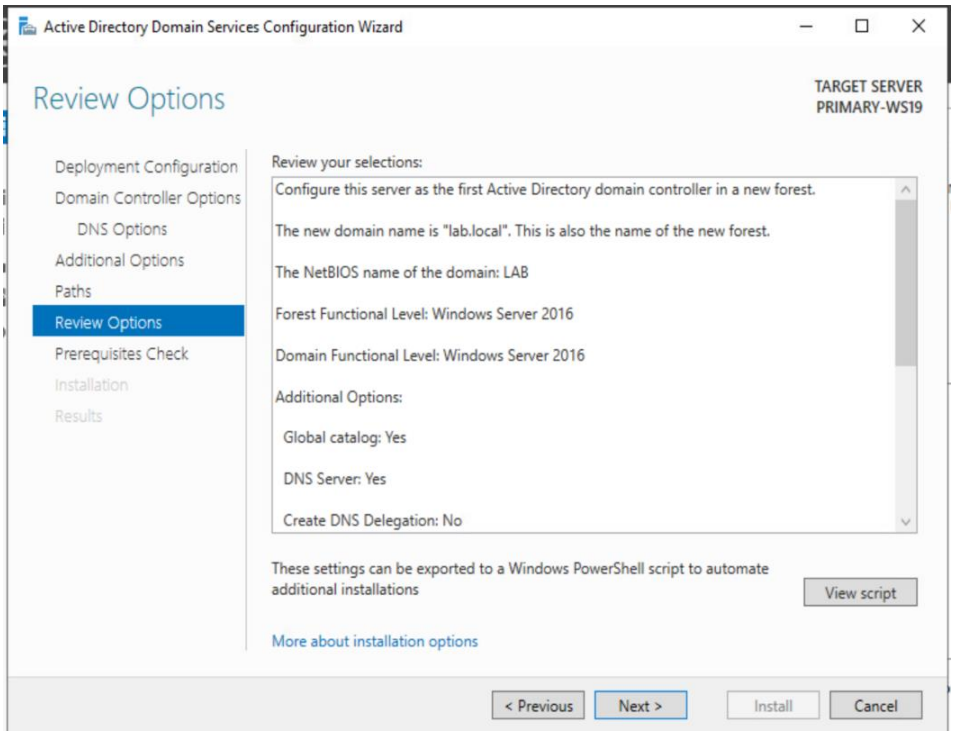

Figure IV.98 Récapitulatif des configurations.

Confirmation d'avoir bien respecté les prérequis indiqués

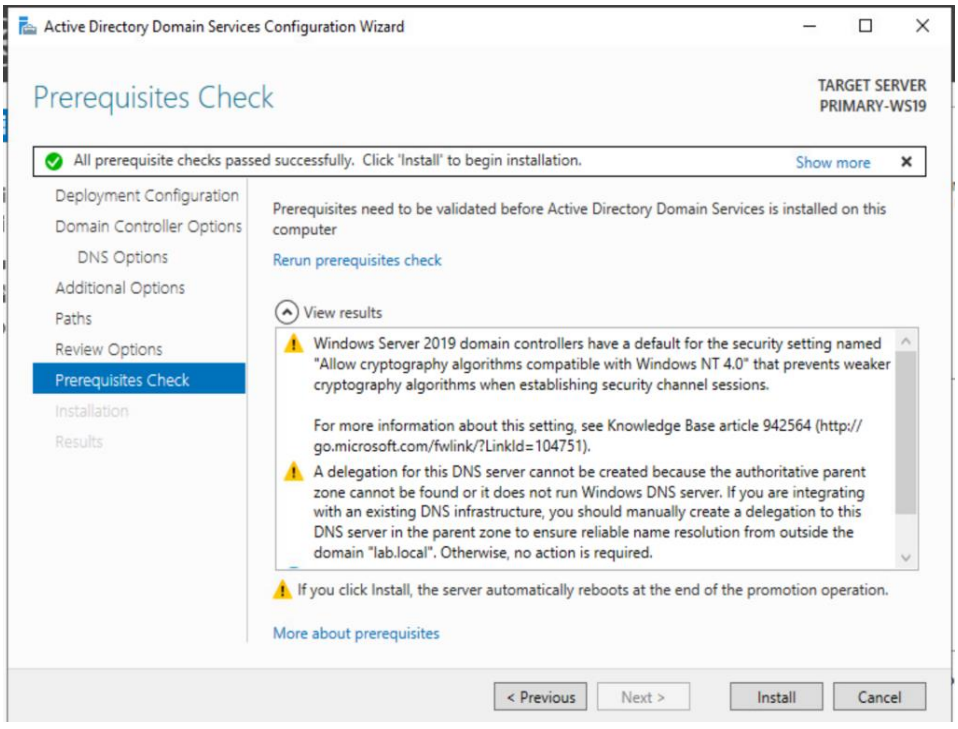

Figure IV.99 Vérification des prérequis.

Lancement de l'installation du service

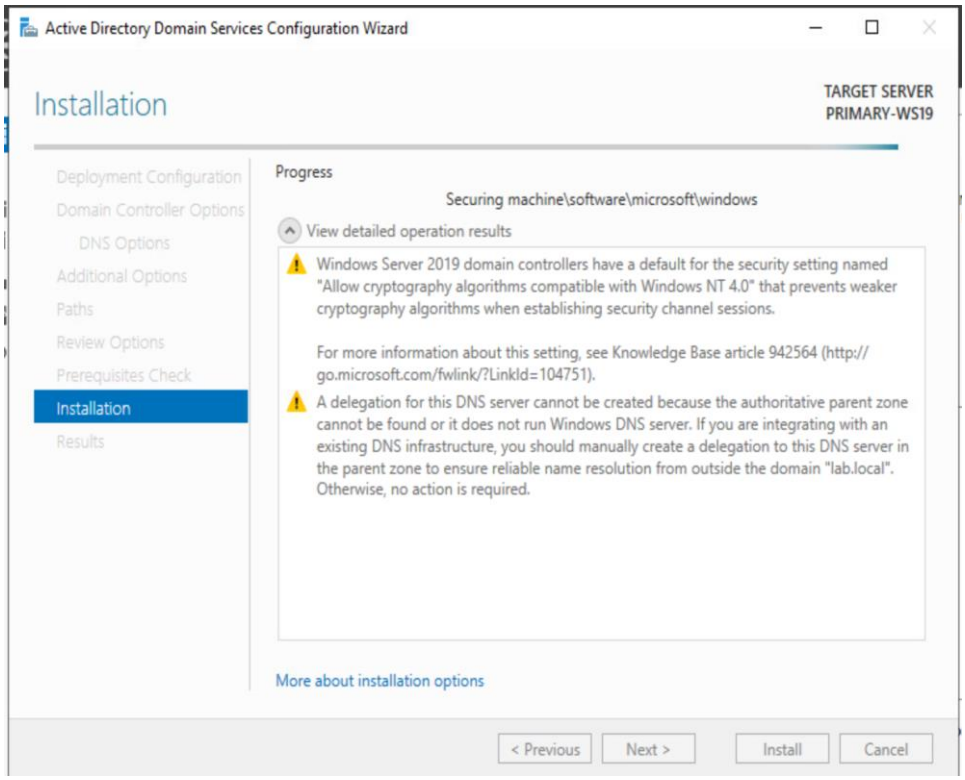

Figure IV.100 Installation du service.

Une fois l'installation terminé la machine va se redémarrer pour assurer le fonctionnement du service

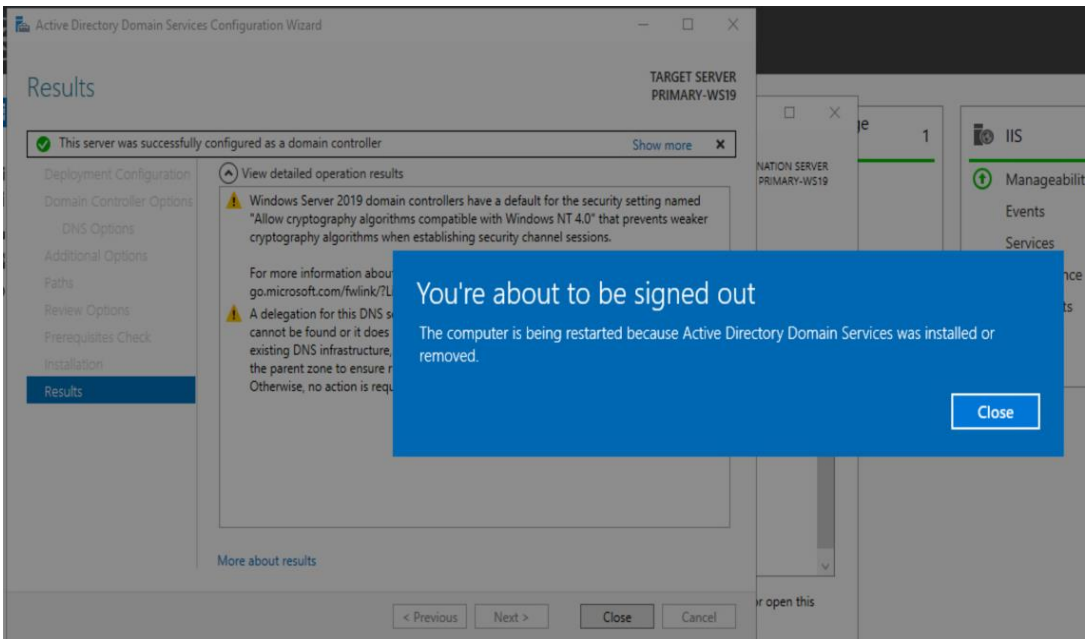

Figure IV.101 Redémarrage de la VM.

On voit sur le tableau du "Dashboard" des services que le service ADDS et bien installé

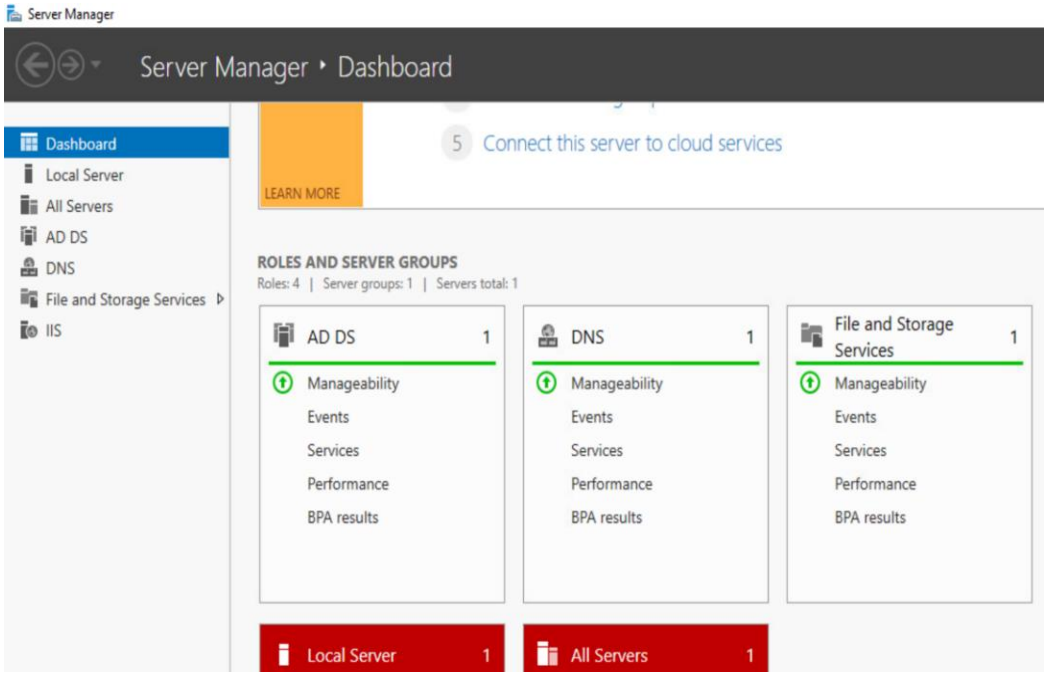

Figure IV.102 Visualisation du service sur le dashboard.

IV.6.2 Création des groups et des utilisateurs Active Directory

Maintenant que notre service et opérationnel on va créer les groupes et utilisateurs pour notre client que nous avons présenté dans le chapitre précèdent en suivant ces étapes :

Une fois dans l'instance de gestion de l'active directory on fait un clique droit et on choisit new puis group

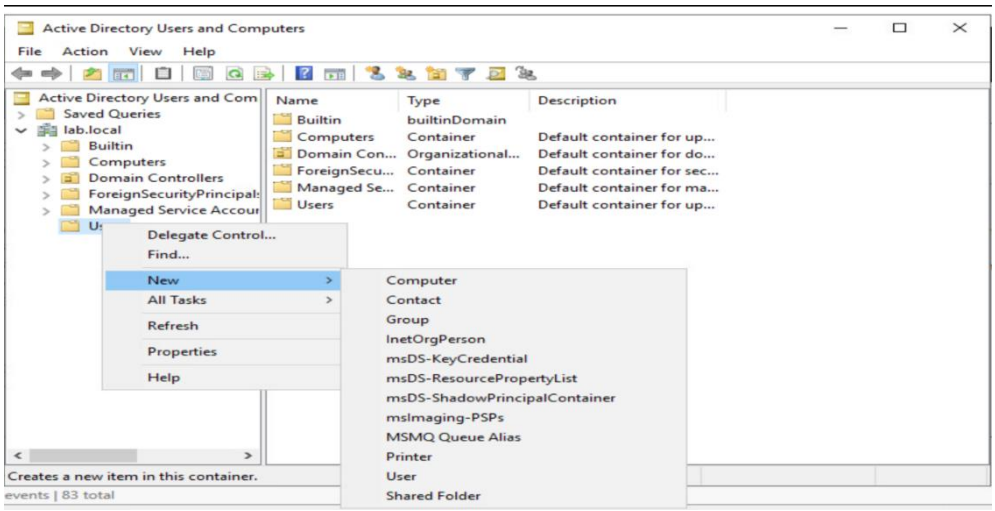

Figure IV.103 Créer un nouveau groupe.

On choisit le nom souhaité pour le groupe

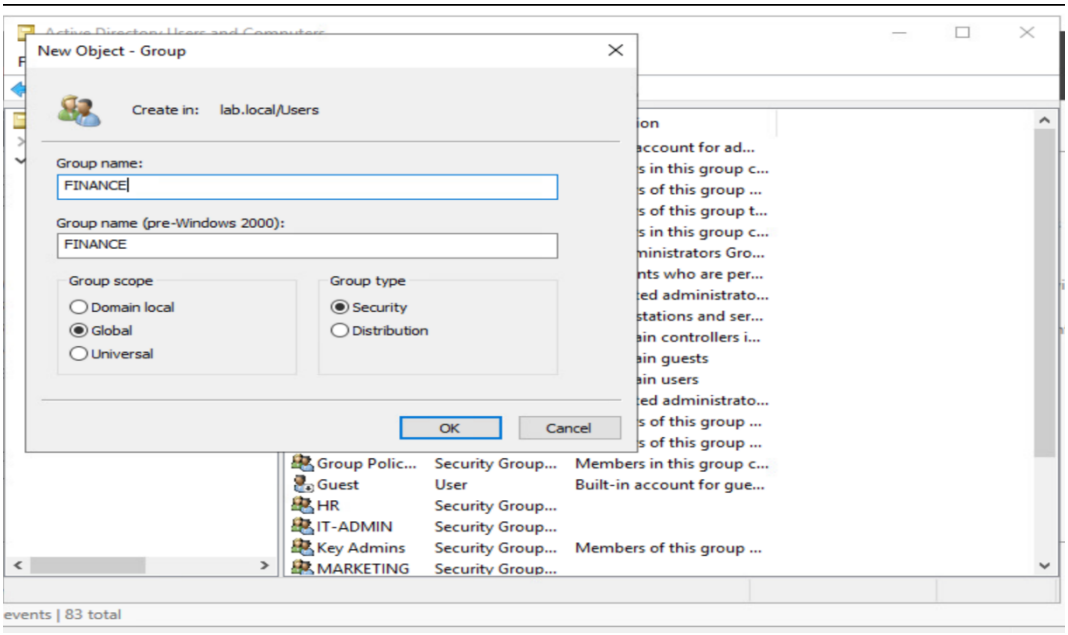

Figure IV.104 Nommer le groupe.

Compléter les informations de l'utilisateur

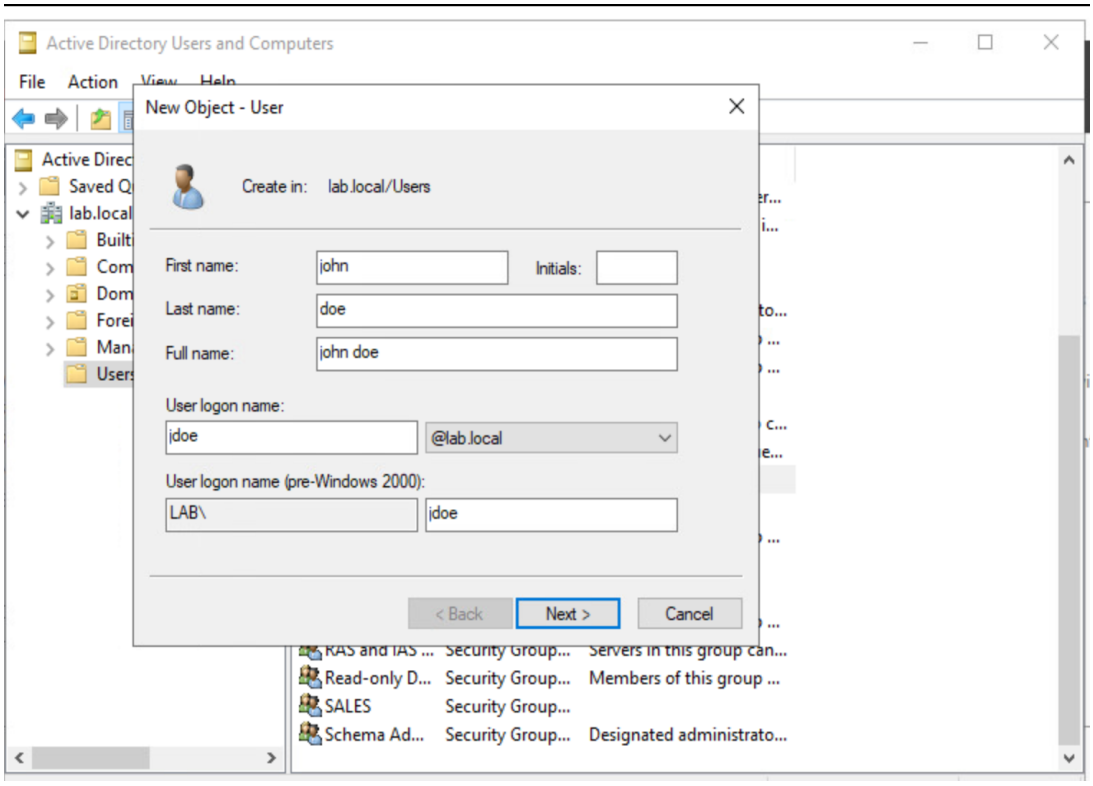

Figure IV.105 Créer un nouvel utilisateur.

On met on place le mot de passe de cet utilisateur, avec l'option que ce dernier n'expire jamais

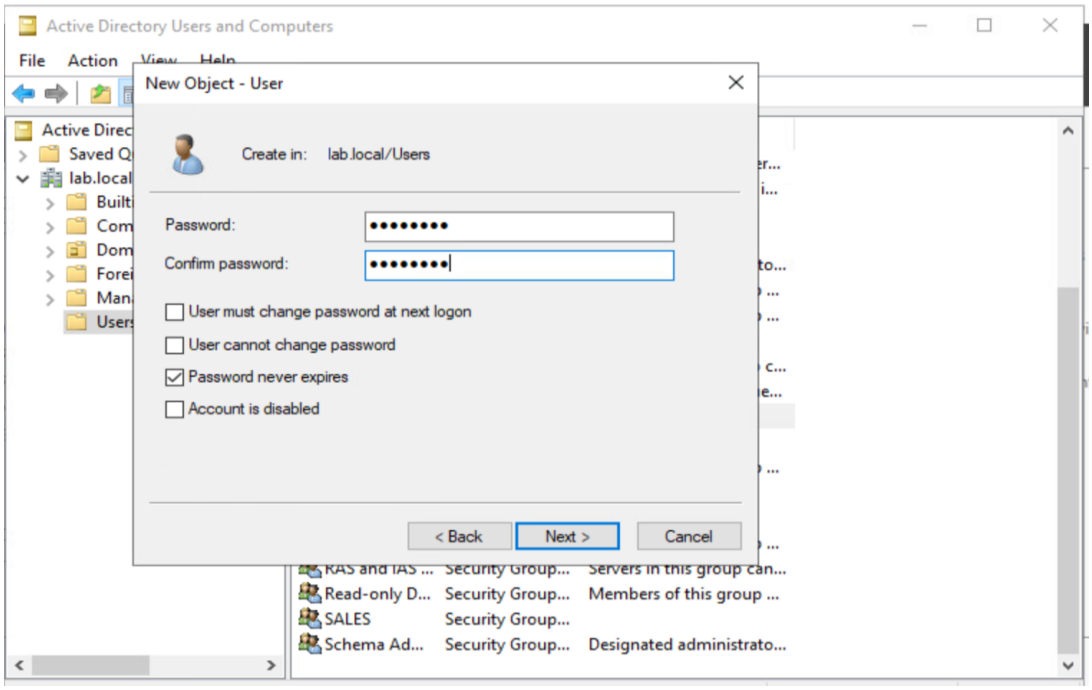

Figure IV.106 Etablissement d'un mot de passe.

Désormais on va associer cet utilisateur au groupe souhaité en effectuant un clique droit sur l'utilisateur puis "Add to a group"

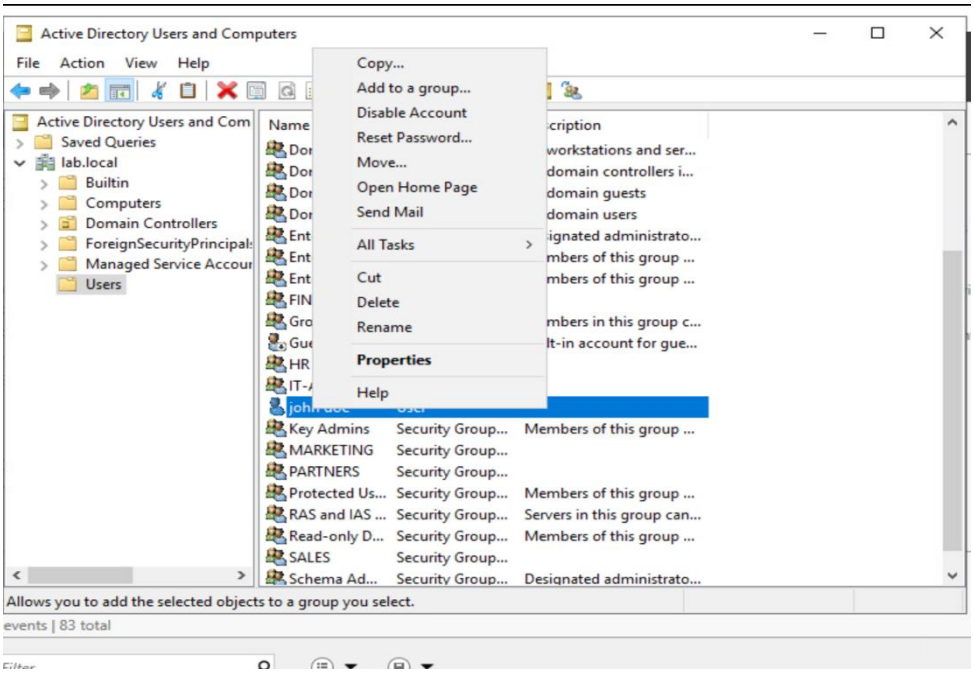

Figure IV.107 Associer l'utilisateur a son groupe.

Une fenêtre de recherche va apparaître et on va chercher le groupe souhaité

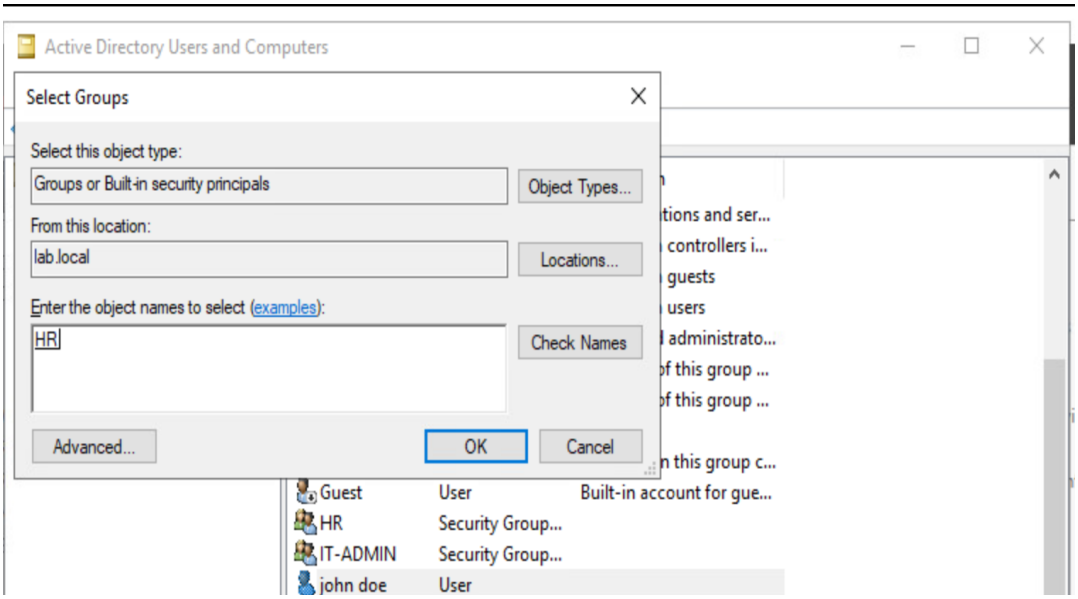

Figure IV.108 Trouver le groupe approprié.

En cliquant sur ok notre utilisateur et ajouter au groupe indiqué, on fait la même chose pour tous les groupe et tous les utilisateurs

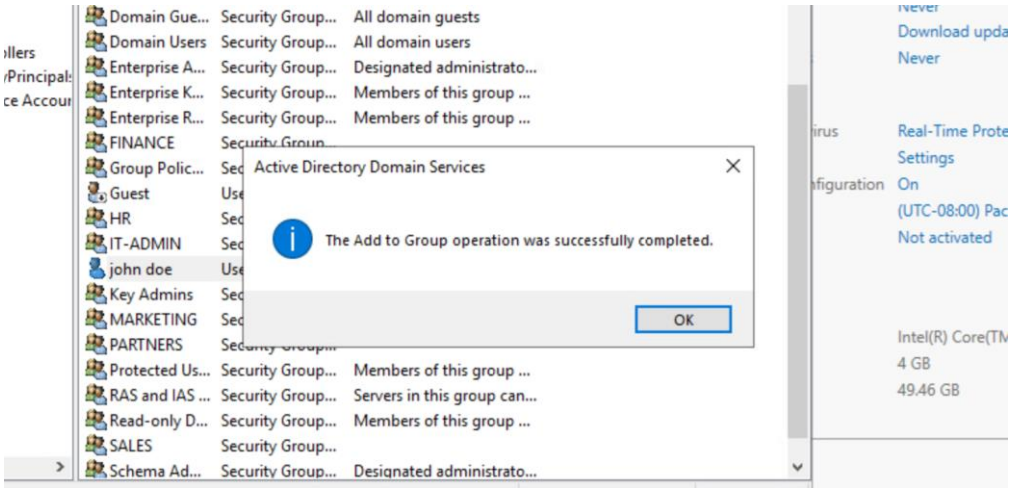

Figure IV.109 Utilisateur ajouté au groupe.

IV.6.3 Installation du service WEB et FTP

Après l'installation de Windows server, nous installons le rôle FTP et IIS de manière simultanée et nous accédons à l'interface de gestion de ce dernier.

Comme lors de l'installation du service DNS expliqué précédemment, et après avoir suivi les mêmes étapes pour les deux services web et ftp on ajoute leurs rôle et fonctionnalités

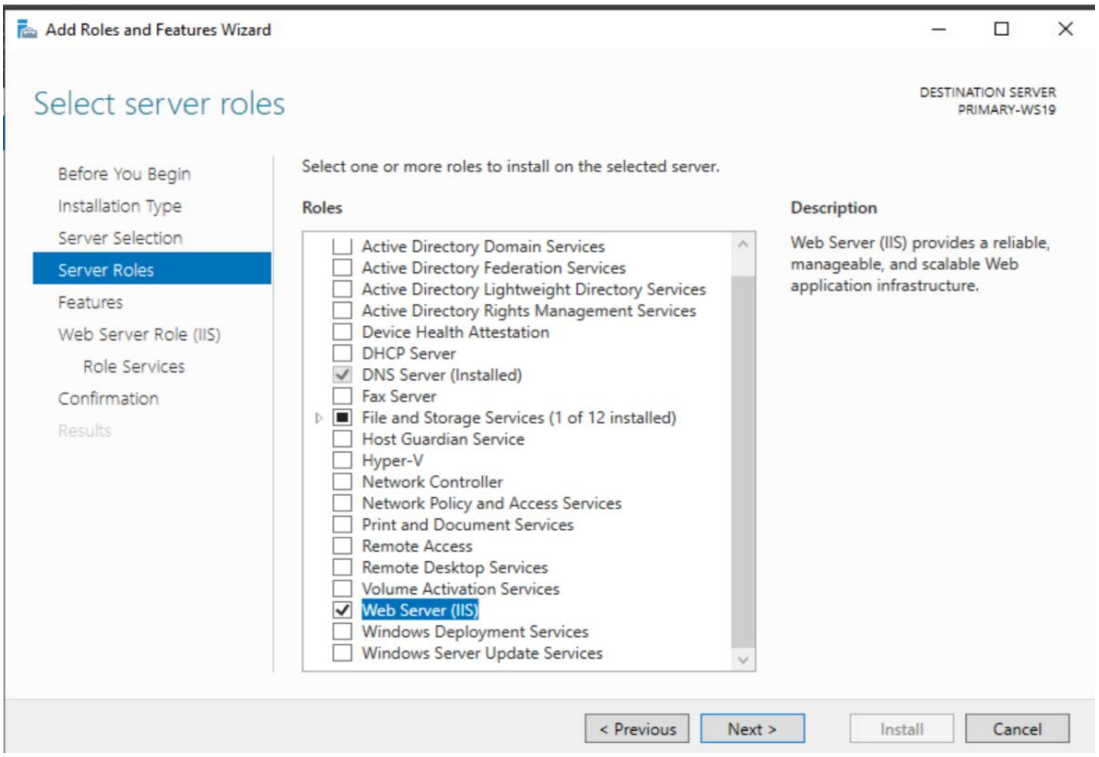

Figure IV.110 Choix du service.

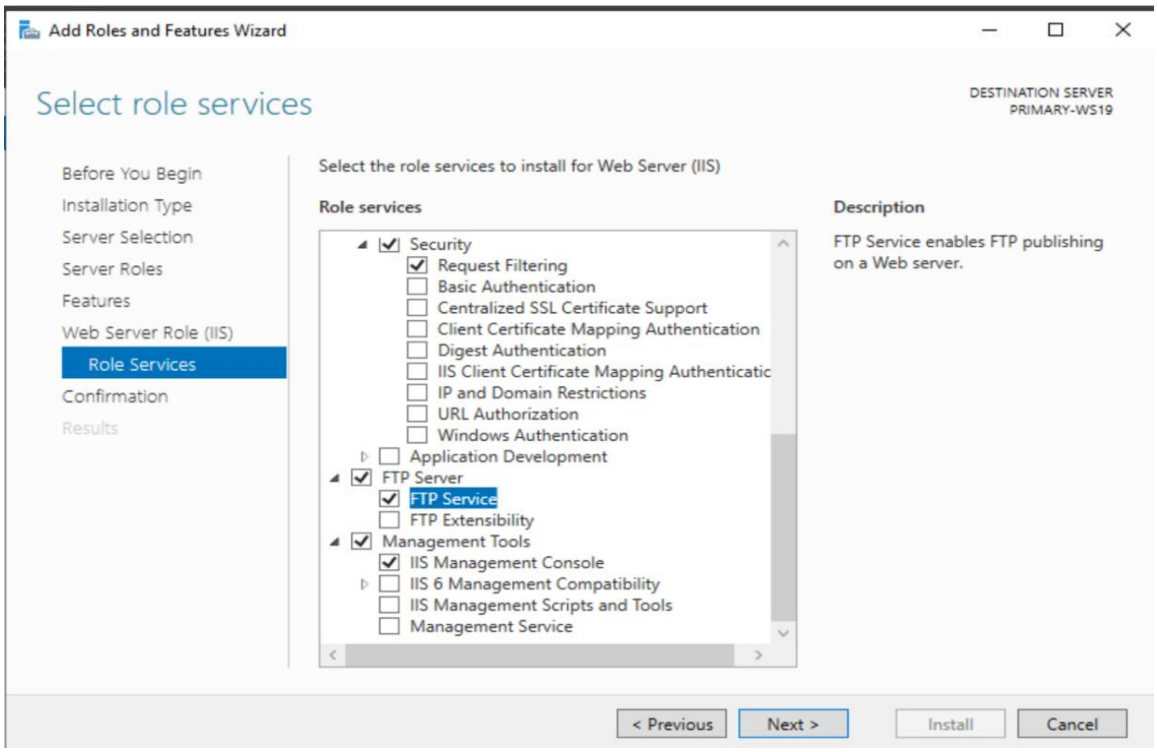

Figure IV.111 Installation de la fonctionnalité FTP.

Une fois le choix fait, une fenêtre de confirmation du choix s'affiche

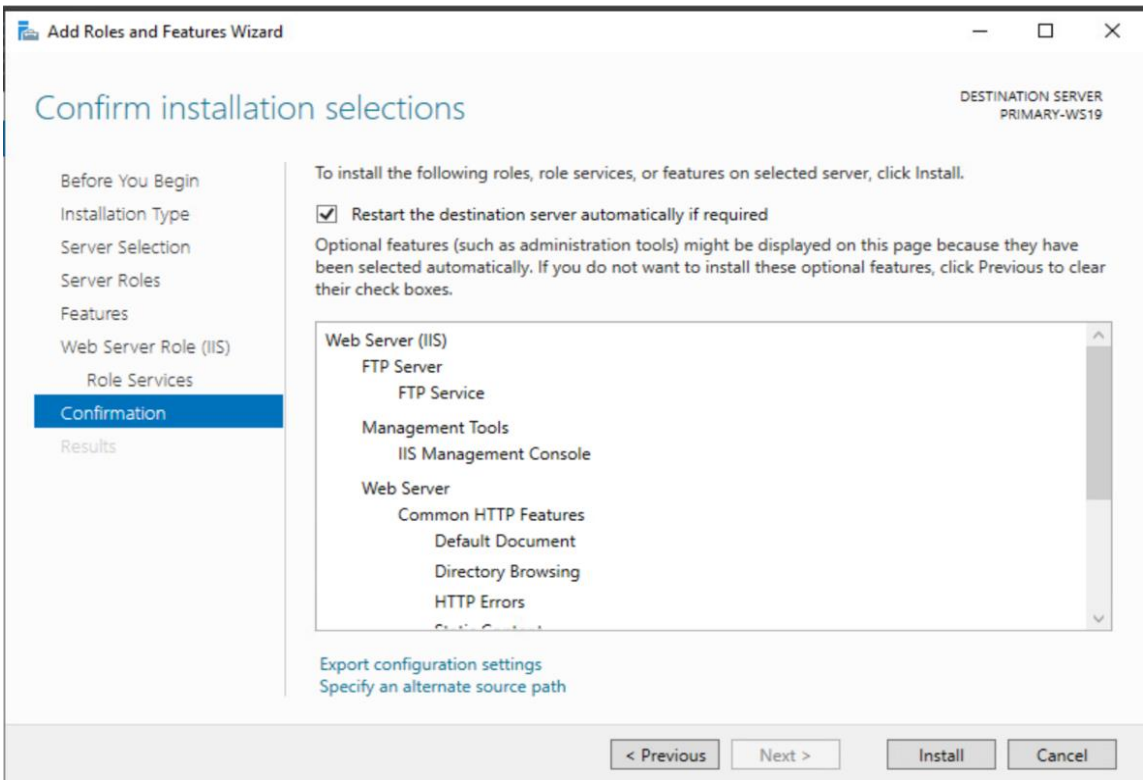

Figure IV.112 Confirmation de l'installation des services.

L'installation commence et ne prend pas énormément de temps en général

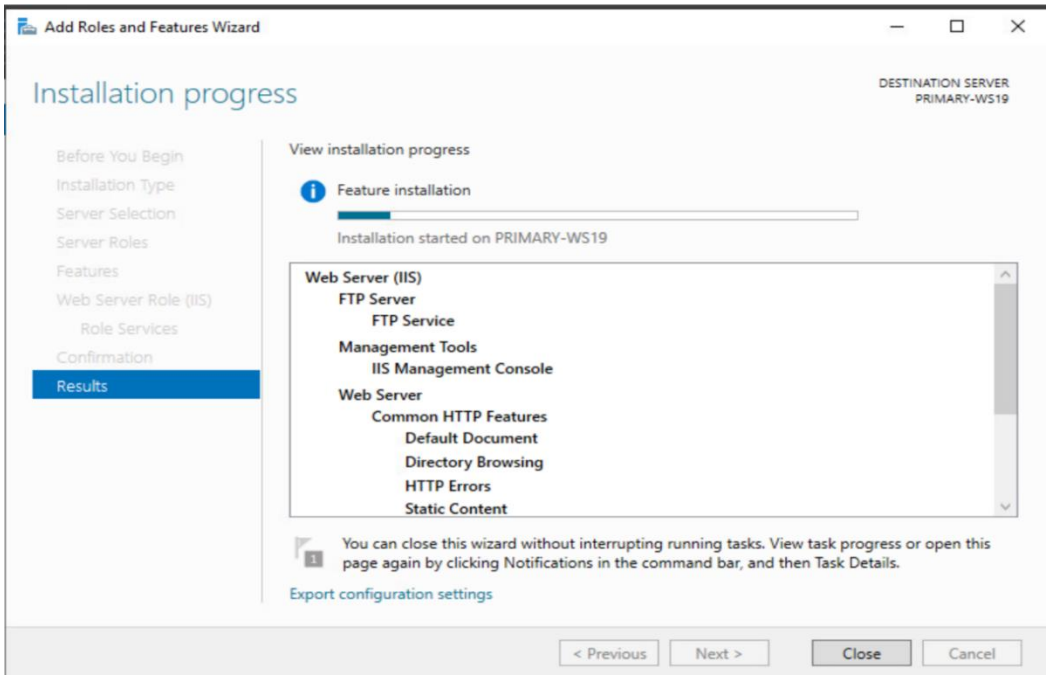

Figure IV.113 Lancement de l'installation.

On rejoint l'instance Tools pour la configuration des deux services

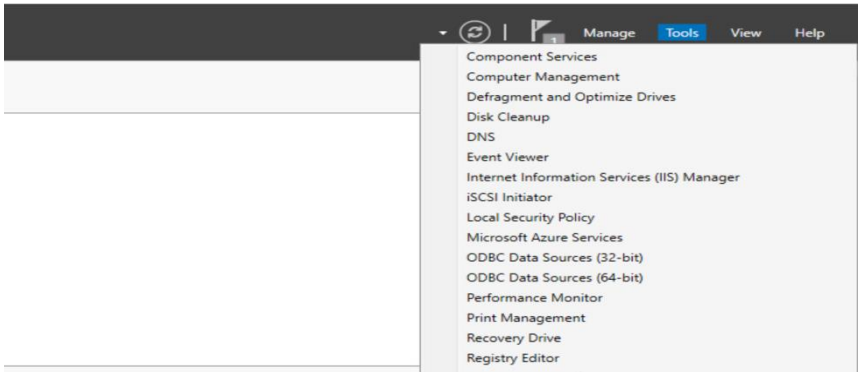

Figure IV.114 Configurer les services.

Une fois avoir cliqué sur internet information service, l'interface de gestion du service WEB s'affiche

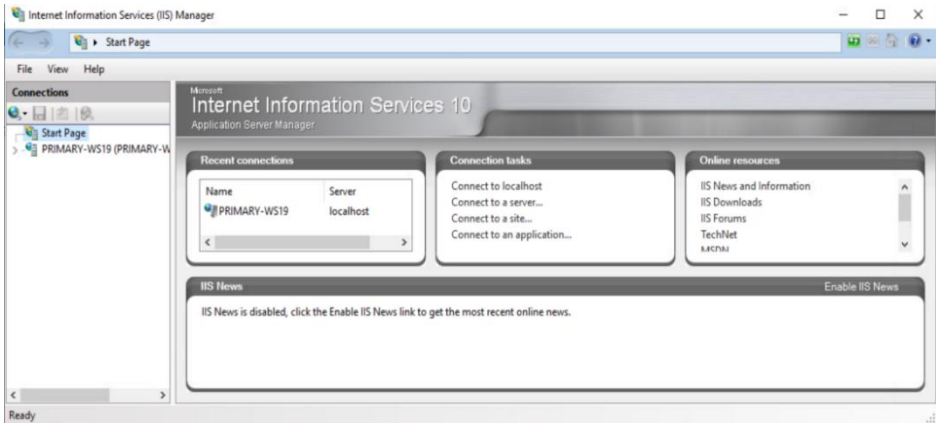

Figure IV.115 Interface de gestion.

Nous ajoutons un site FTP

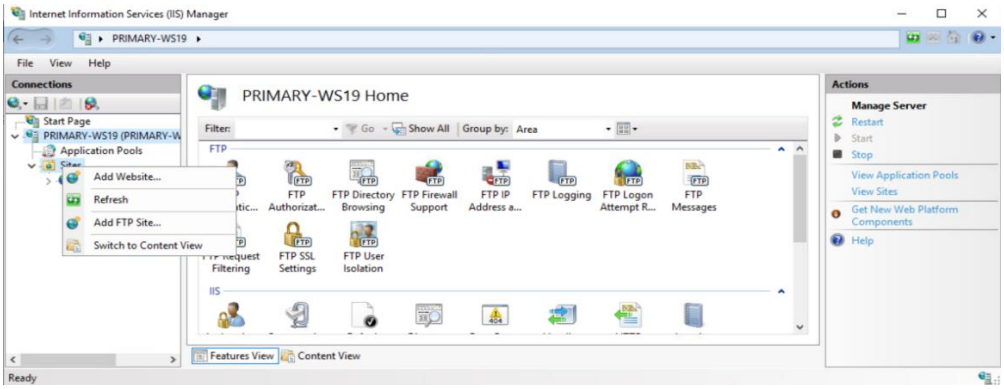

Figure IV.116 Ajout d'un site.

Une fois le site créé on lui donne et nom et son emplacement

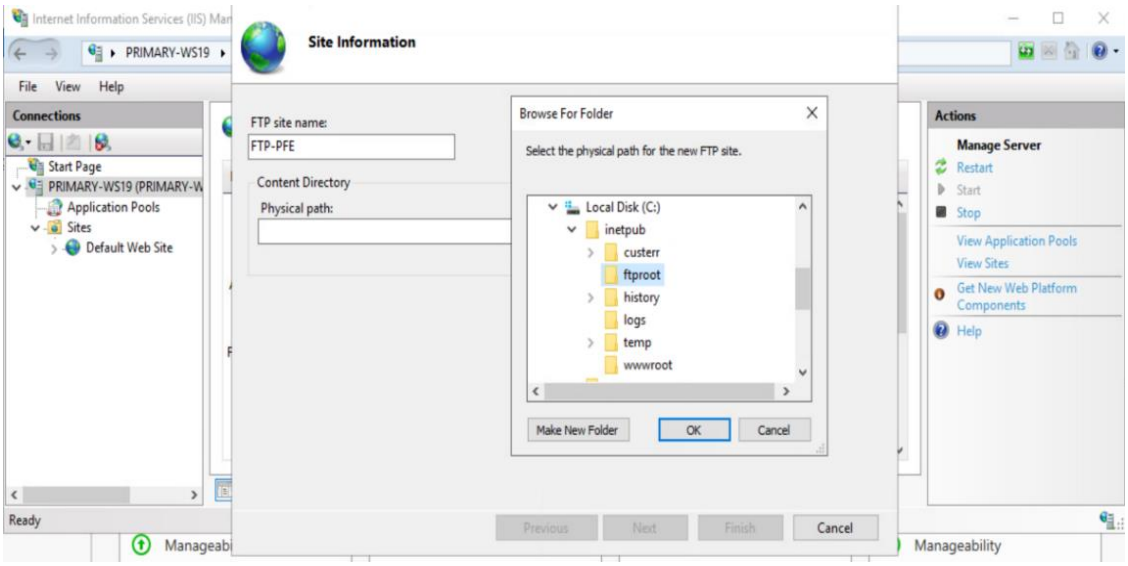

Figure IV.117 Details du site.

On lui attribue une adresse IP qui dans notre cas sera la même que le DNS puisque nous allons créer nos services sur la même machine virtuelle, et désactivé la fonction SSL dans on n'aura pas besoin

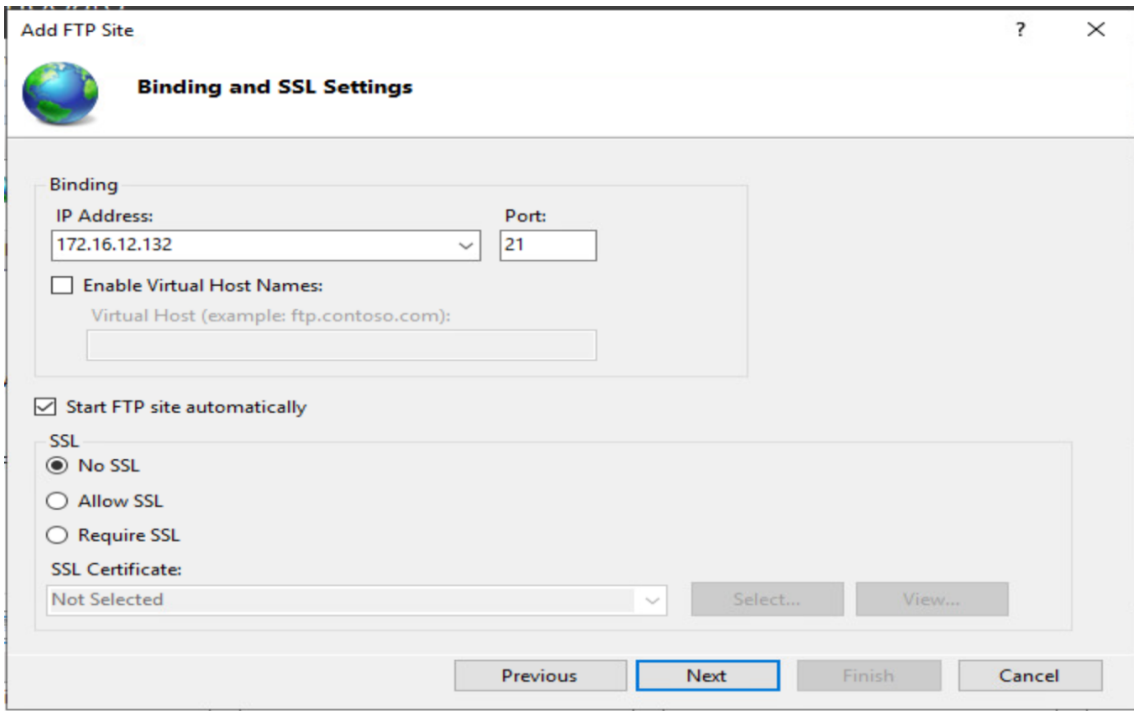

Figure IV.118 Paramètre du service.

Maintenait que nous avons fini les configurations du service il s'affiche sur le site que nous avons créé

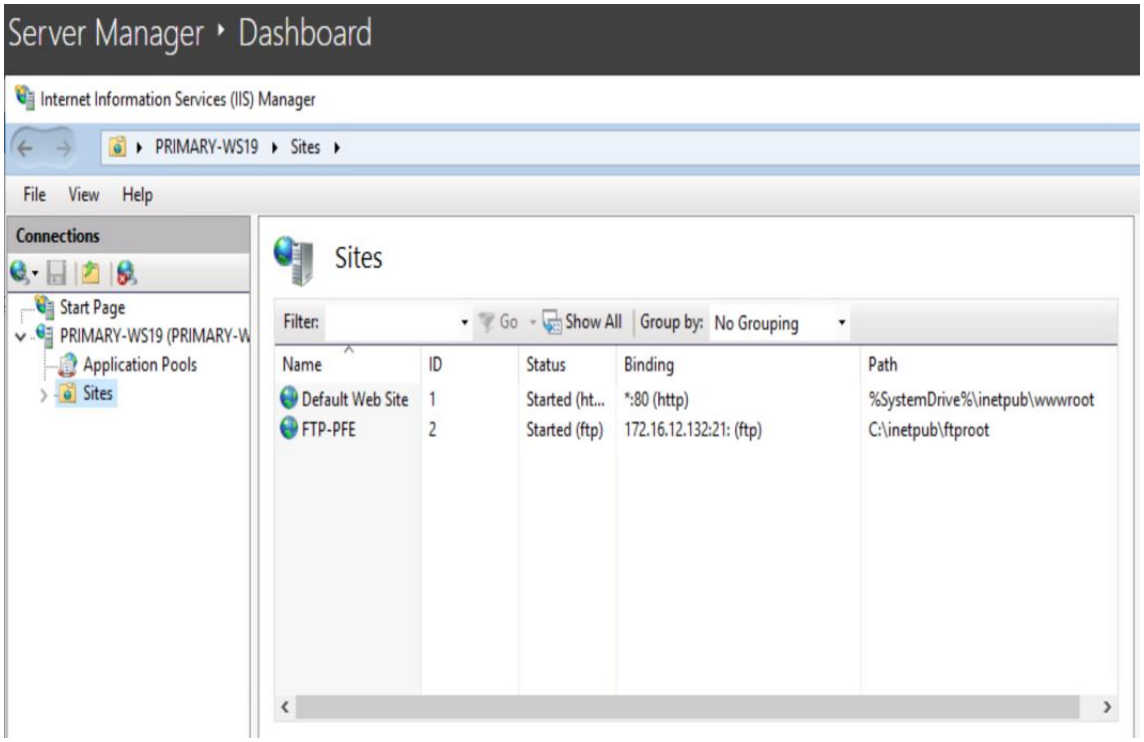

Figure IV.119 Service opérationnel.

Pour accéder au fichier partagé du service FTP et l'interface web on ouvrir le navigateur internet et on introduit ftp://172.16.12.132 dans la barre de recherche, une fenêtre nous demandons l'identifiant et le mot de passe de la machine qui héberge le service FTP s'affiche

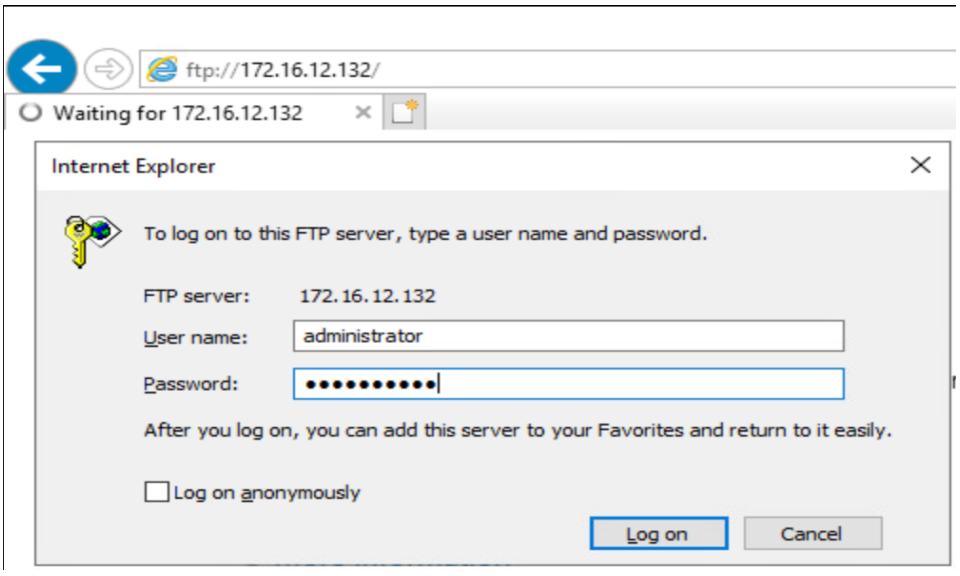

Figure IV.120 Accéder au service FTP.

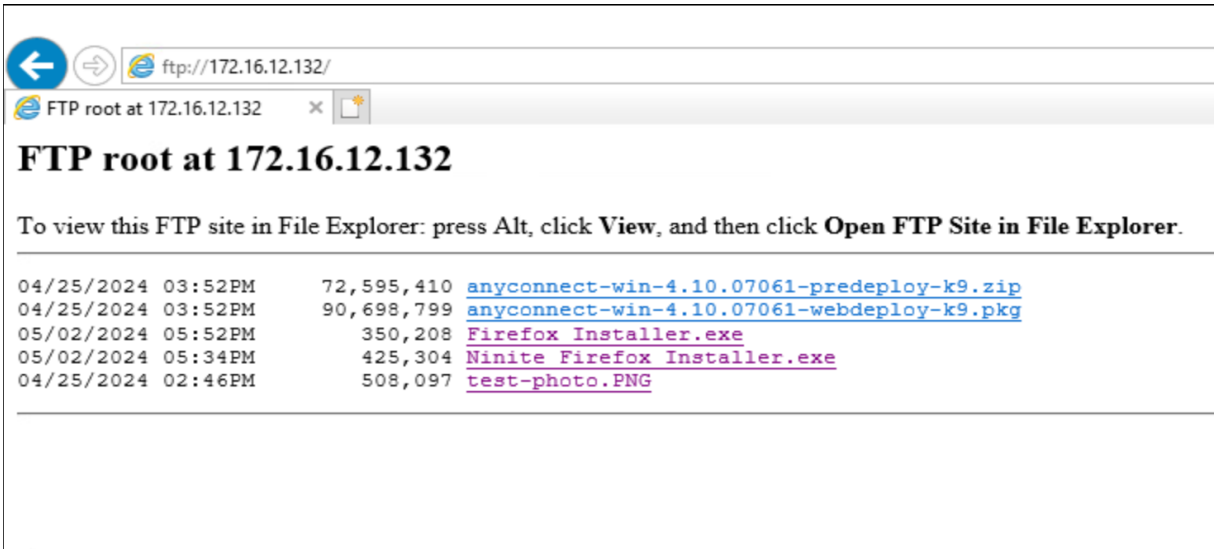

Figure IV.121 Fichier ajouté au service FTP.

Pour ajouter des fichiers au service FTP on utilise le logiciel FileZilla que nous avons présenté au début du chapitre

Il suffit d'accéder au logiciel, introduire l'adresse IP du service un utilisateur et son mot de passe et enfin le numéro de port du service FTP qui est 21, l'ajout des fichiers se fait par un simple "drag and drop"

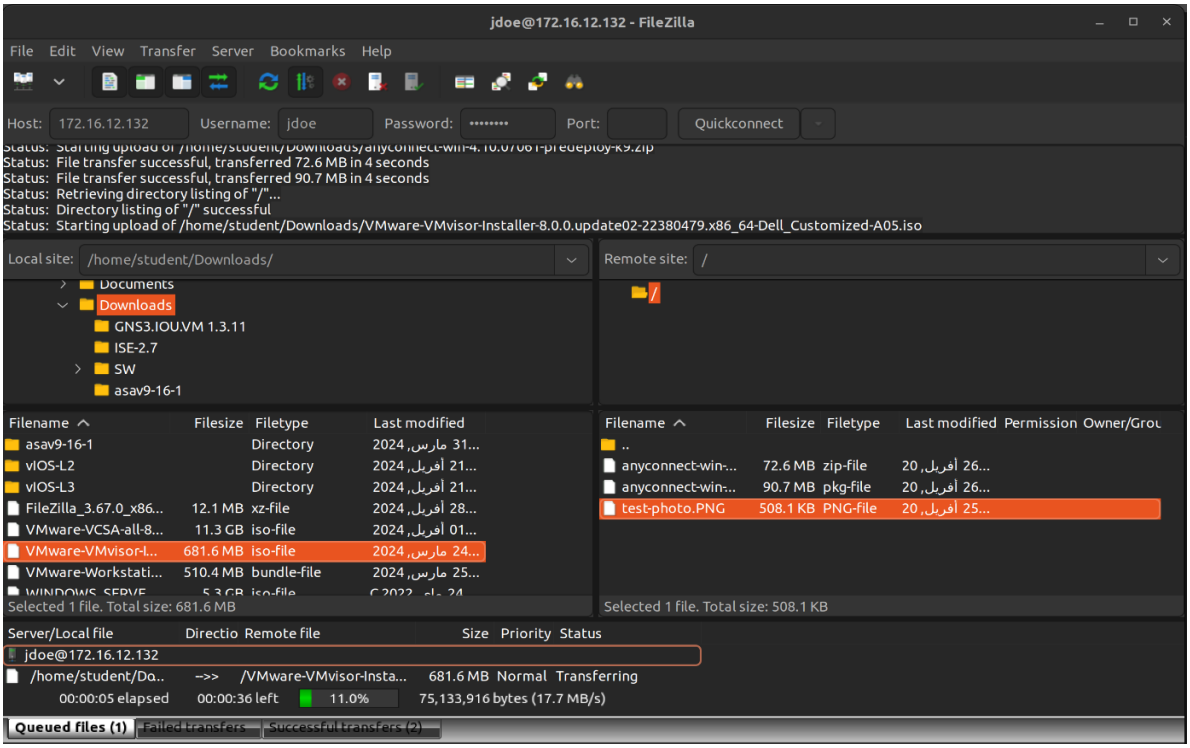

Figure IV.122 Ajout des fichiers au service FTP.

IV.6.4 Activation du client Network Time Protocol

Pour pouvoir faire l'intégration de Cisco ISE avec Active Directory ces deux services doivent être synchronisé et pour se faire on va pointer notre VM vers un serveur NTP publique comme client, chose que nous allons faire aussi pour Cisco ISE une fois cette étape atteinte

Les étapes qui nous permettent de pointer notre machine virtuelle vers un serveur NTP comme client sont les suivantes :

Via l'onglet Tools on accède à group Policy Management et on fait un clique droit sur Domain Controller et on sélectionne "create a GPO in this domain", cette démarche va nous permettre de créer une stratégie de groupe qui sont des directives de configuration pour les ordinateurs et utilisateurs

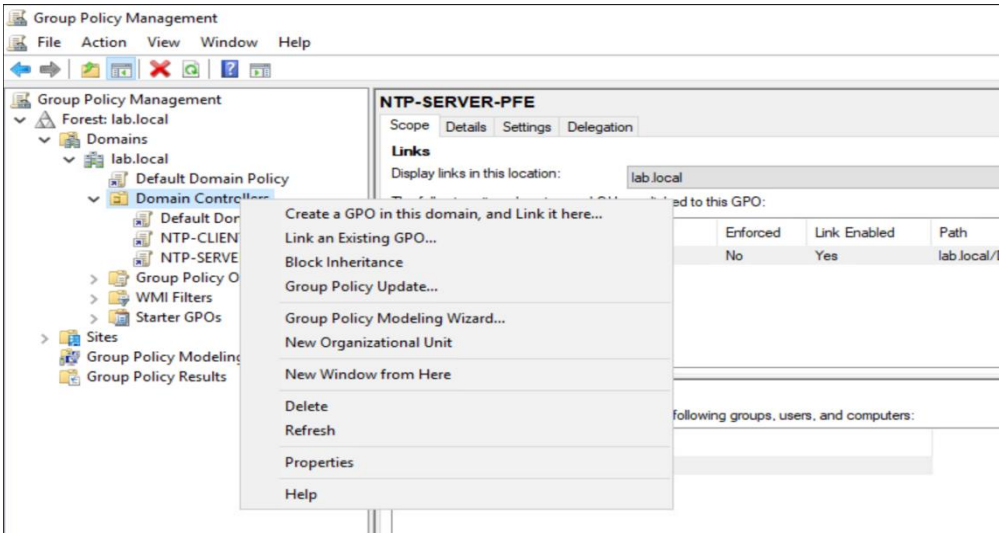

Figure IV.123 Interface Group Policy Management.

On va la nommer NTP-CLIENT

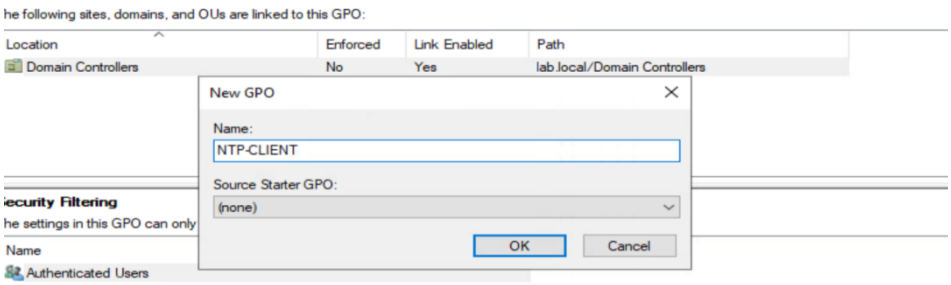

Figure IV.124 Créer l'instance Client NTP.

Pour pouvoir paramétrer cette instance créée on fait un clique droit dessus et on suit se chemin : "Policies, Administrative Templates, System, Windows Time Service et puis Time Providers"

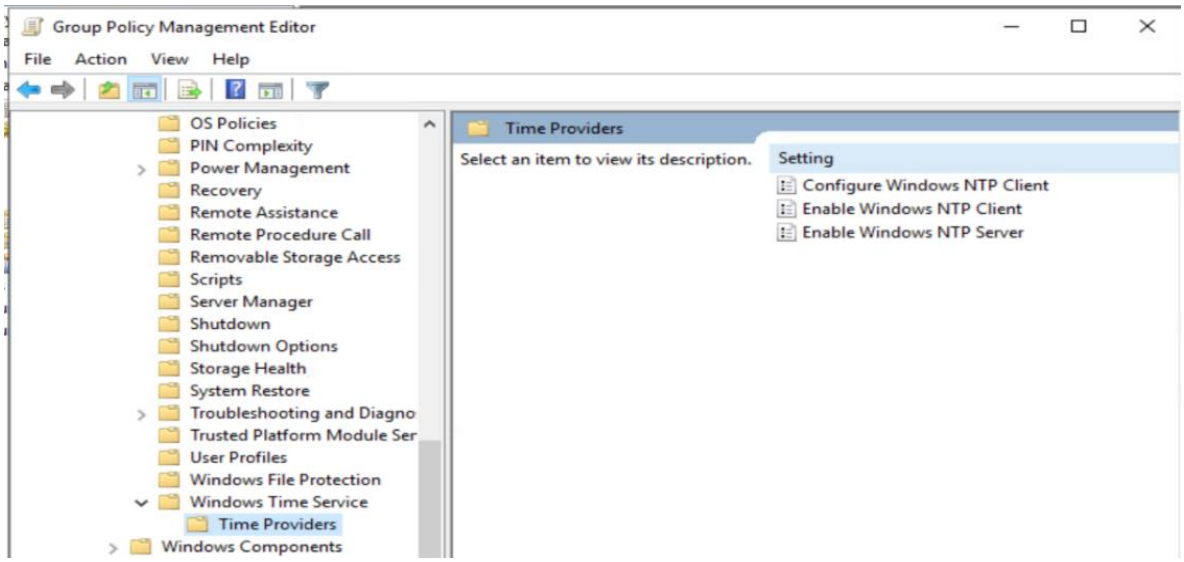

Figure IV.125 Activer le client NTP.

On va activer les options NTP Client et les configurer comme suit

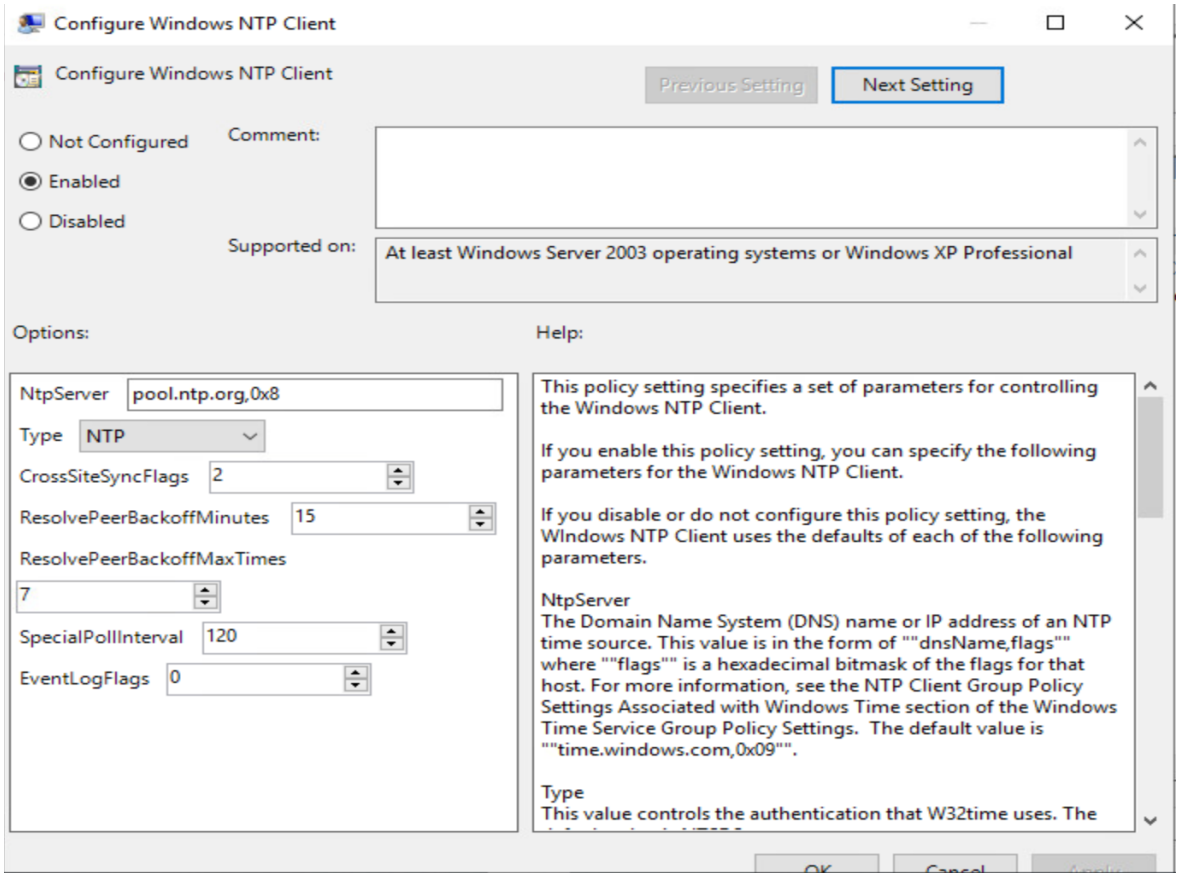

Figure IV.126 Paramétrage du Client NTP.

On point notre machine vers le serveur NTP : pool.ntp.org

On teste si notre machine a bien été synchronisé avec le serveur externe via le CMD

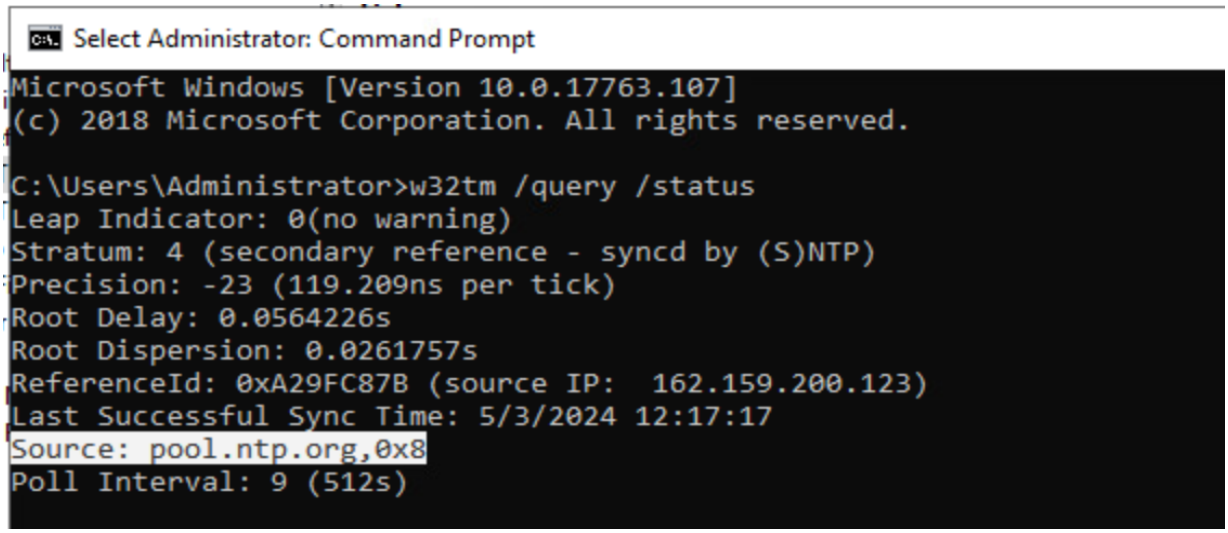

Figure IV.127 Tester la synchronisation.

IV.7 Installation de Cisco Identity Services Engine

On va des a présent commencer l'installation lourde de Cisco ISE comme convenue sur ESXI04, pour cela nous allons créer une VM et lui donner les ressources nécessaires pour assurer le bon fonctionnement de cette dernière

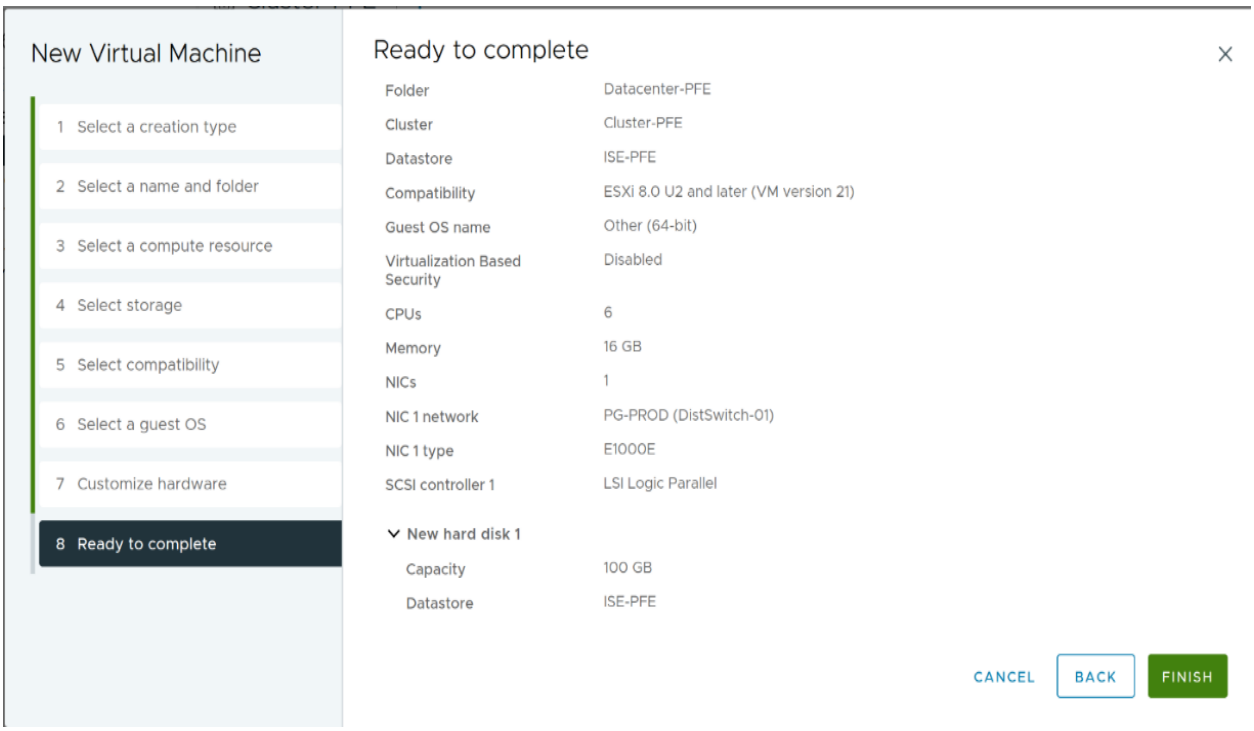

Figure IV.128 Configuration de la VM Cisco ISE.

Il faut noter que la version de ISE utilisé est 2.7.0.356 et pour assurer le bon fonctionnement il faut minimum

- 6 Cores CPU
- 16 GB de RAM
- Disque de stockage de 130 GB

Maintenant on allume la VM et on procède à l'installation comme le montre la figure suivante

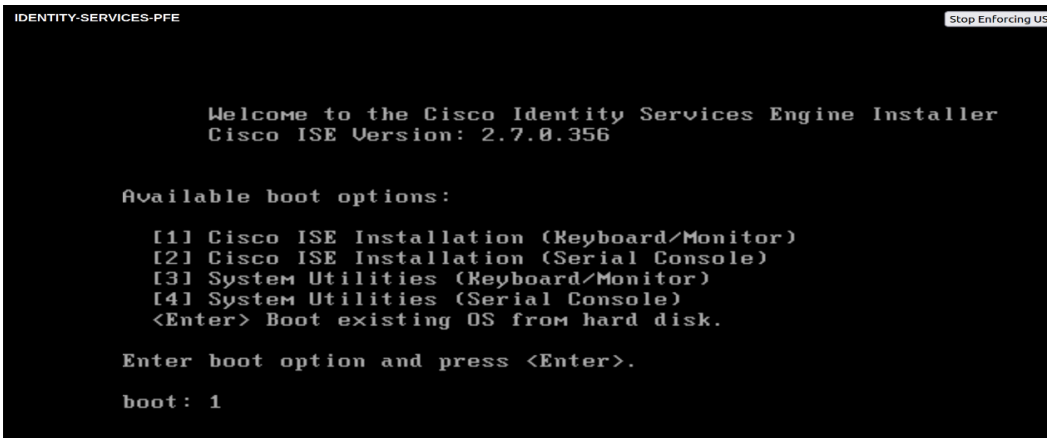

Figure IV.129 Option d'installation.

On choisit l'installation monitor pour suivre pas à pas l'installation et pouvoir intervenir en cas d'échec.

Une fois avoir fait ce choix l'installation débute

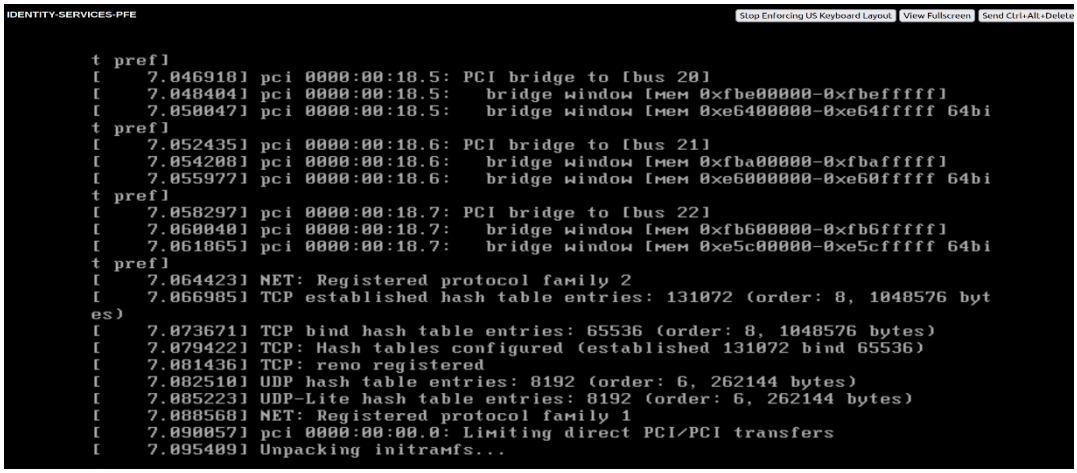

Figure IV.130 Installation de Cisco ISE.

A ce stade il va faire une vérification des ressources, si les prérequis de l'installation ne sont pas respectés, cette dernière s'interrompe

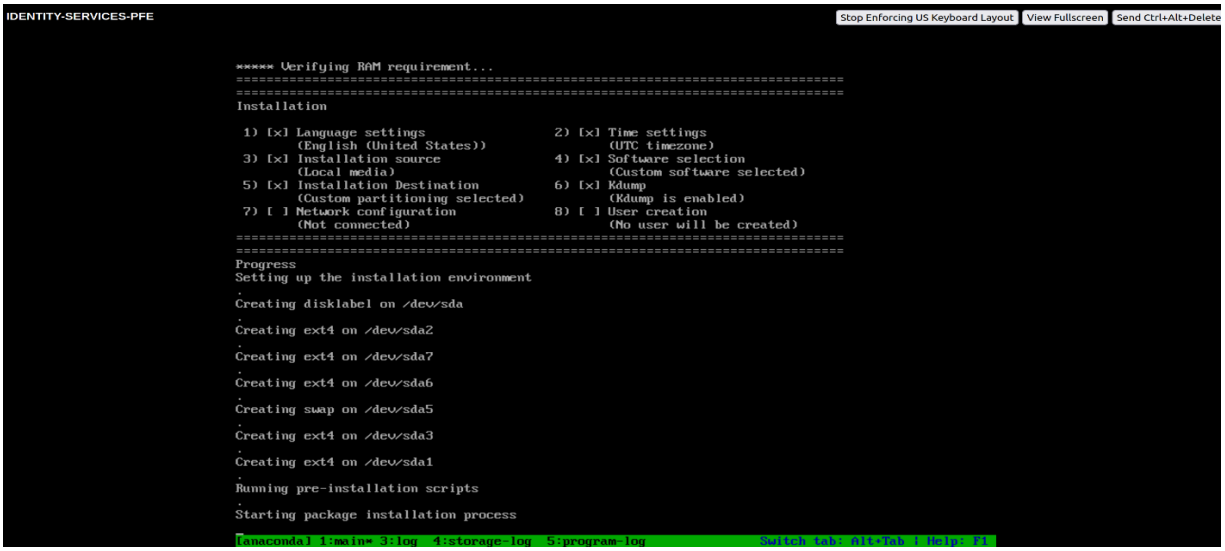

Figure IV.131 Vérification des prérequis.

Une fois l'installation touche à sa fin il nous sera demandé de configurer les paramètres réseaux de l'ISE tel que les adresses IP le masque de sous réseau, la passerelle et plein d'autres paramètres indiqués dans la figure suivante

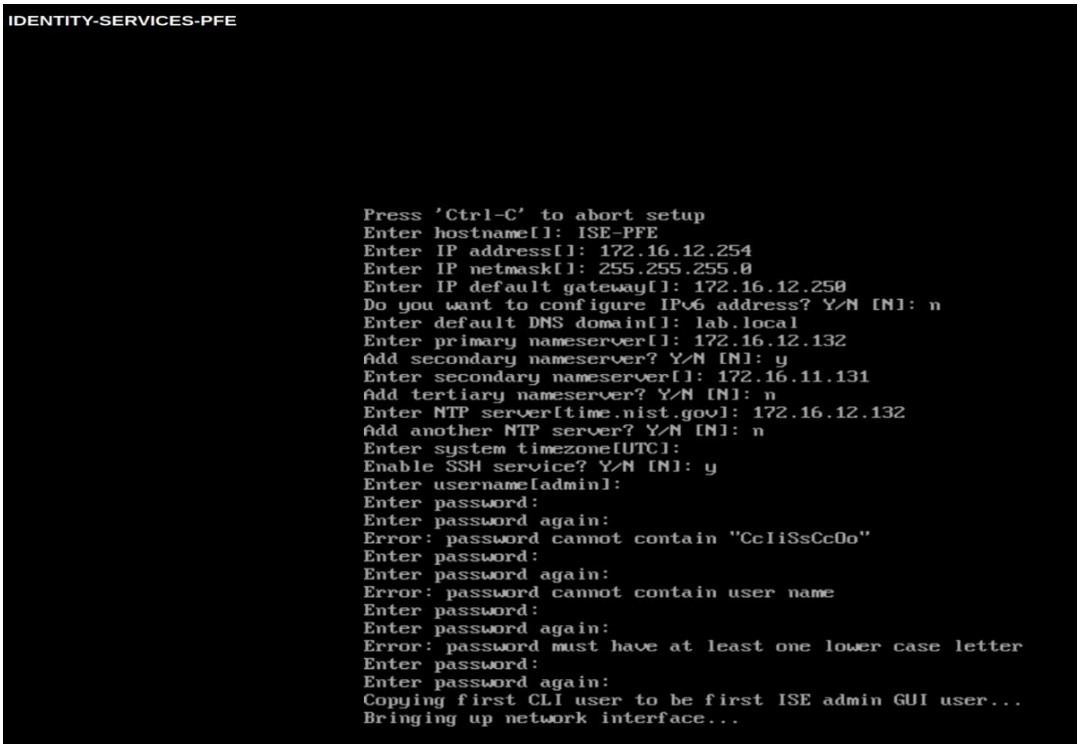

Figure IV.132 Configuration des paramètres réseaux.

Il nous sera aussi demandé d'établir un nom d'utilisateur et un mot de passe qui vont être demandé juste après les avoir configurés pour accéder au CLI de Cisco ISE

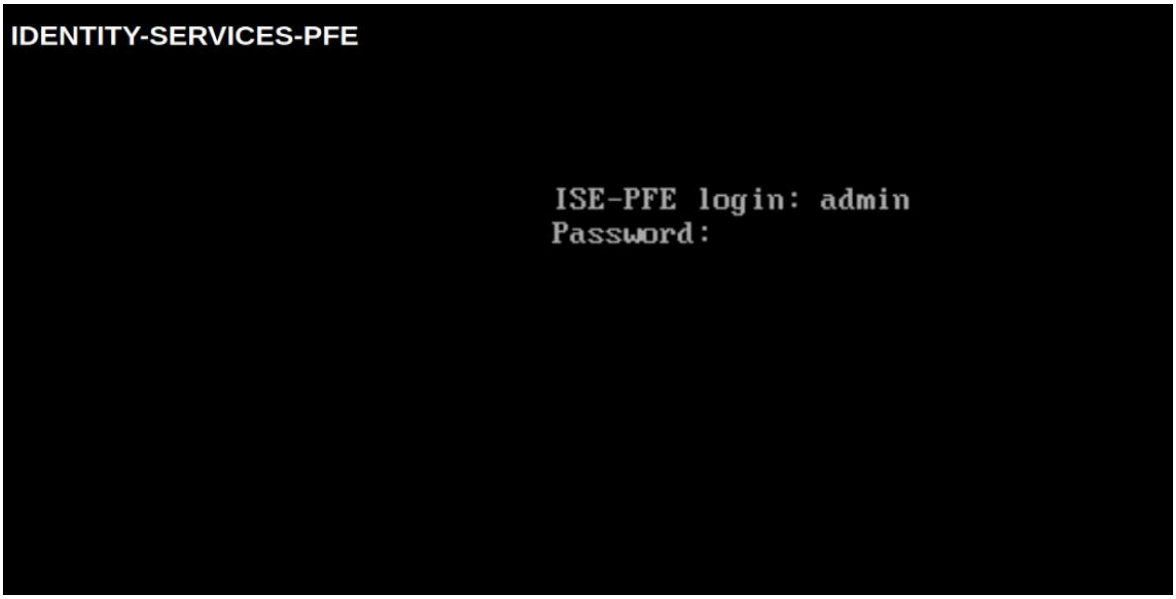

Figure IV.133 Etablissement des identifiants.

Nous pouvons des a présent accéder à l'interface graphique de Cisco ISE en tapant sur le navigateur l'adresse IP

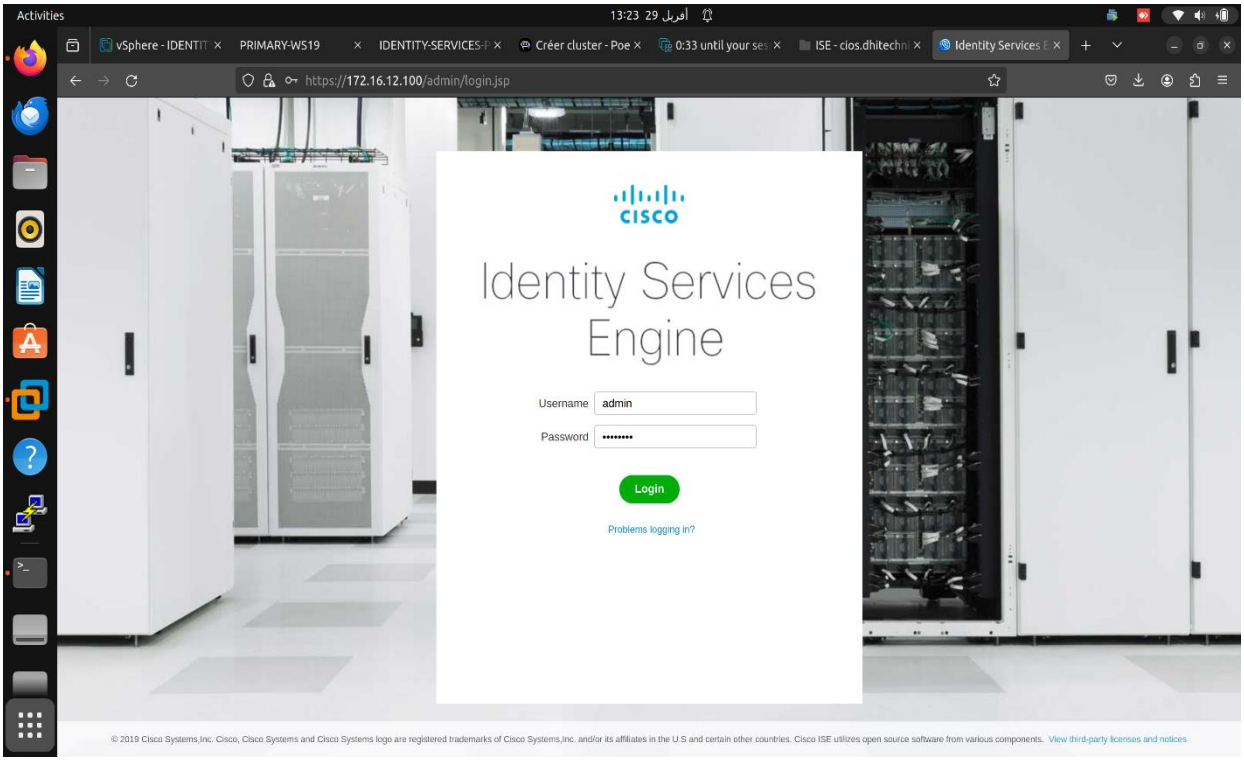

Figure IV.134 Comment accéder à Cisco ISE.

Un tableau de licence nous sera affiché, il faut savoir que la licence coute relativement cher, pour la simulation nous allons nous contenter de la licence d'essai qui dure 90 jours

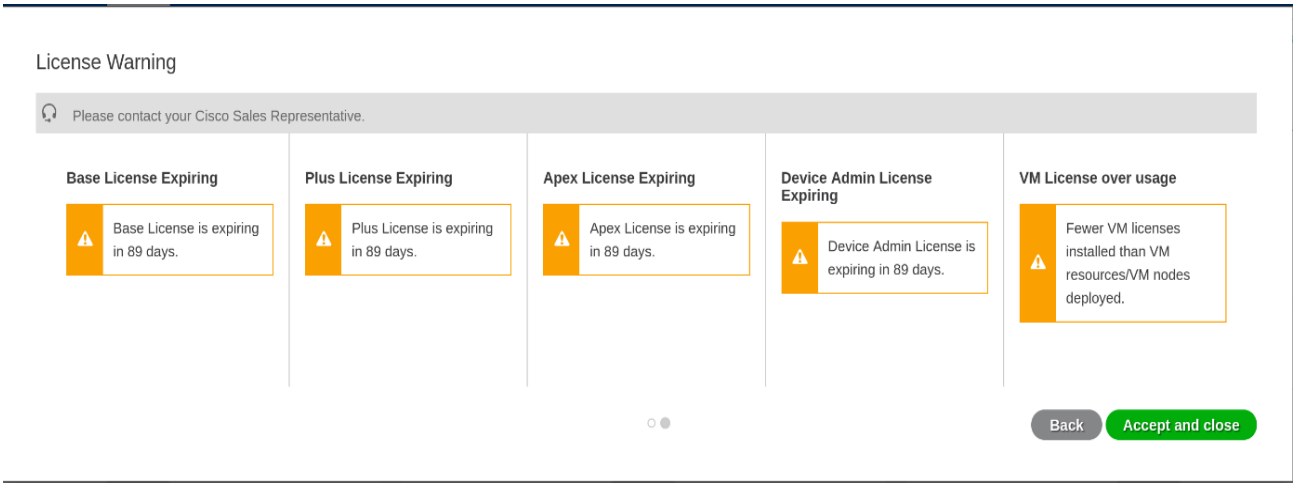

Figure IV.135 Licences relative à Cisco ISE.

Une fois avoir cliqué sur "Accept and Close", l'interface graphique de Cisco ISE va s'afficher, et c'est à partir de là que nous allons commencer l'intégration entre ISE et Active Directory dans nous avons parlé dans le chapitre précèdent

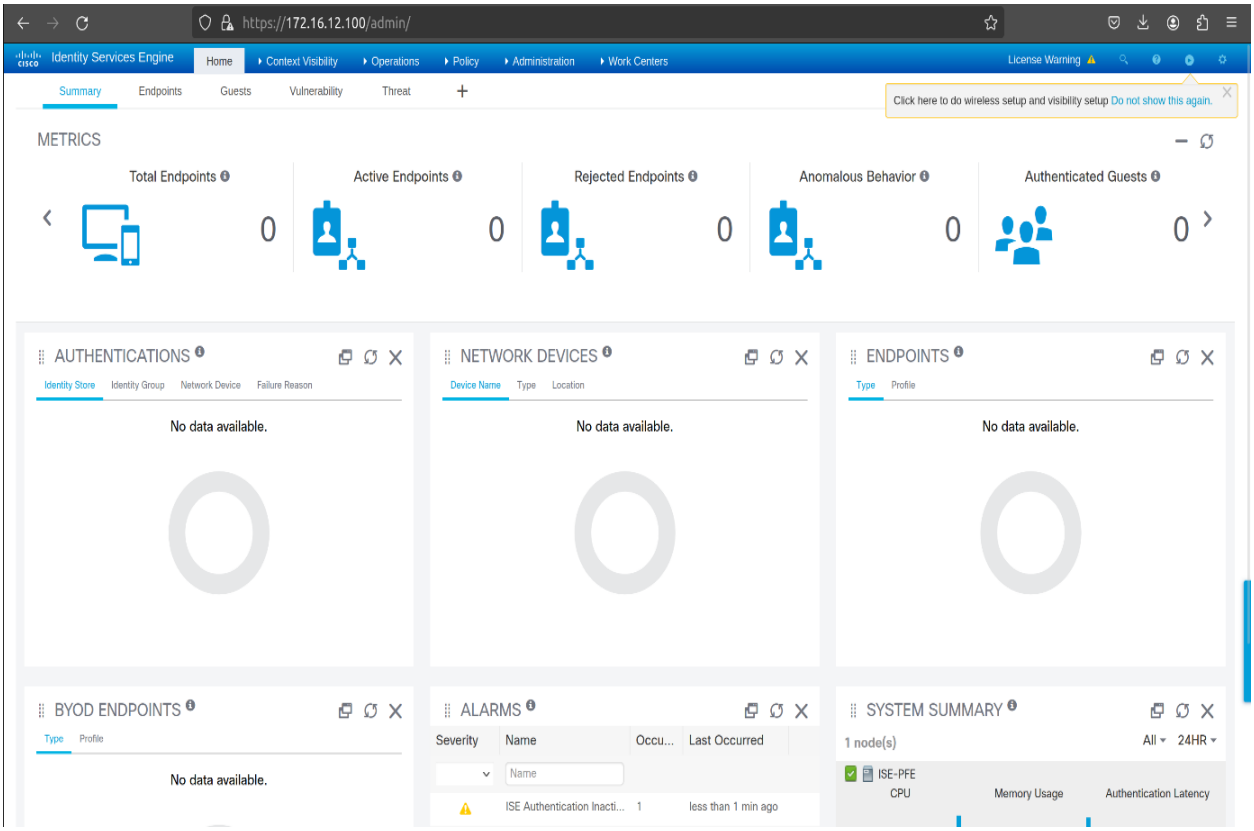

Figure IV.136 Interface graphique de Cisco ISE.

IV.7.1 Intégration de Cisco Identity Services Engine avec Active Directory

A l'aide du logiciel PuTTY que nous avons présenté précédemment nous allons accéder au CLI de Cisco ISE pour pouvoir configurer le serveur NTP et le pointé vers le serveur public comme suit

Les étapes d'intégration entre Cisco ISE et AD sont les suivantes

On se rend à l'onglet "Administration, External Identity Sources" puisque Active Directory s'agit d'un service externe

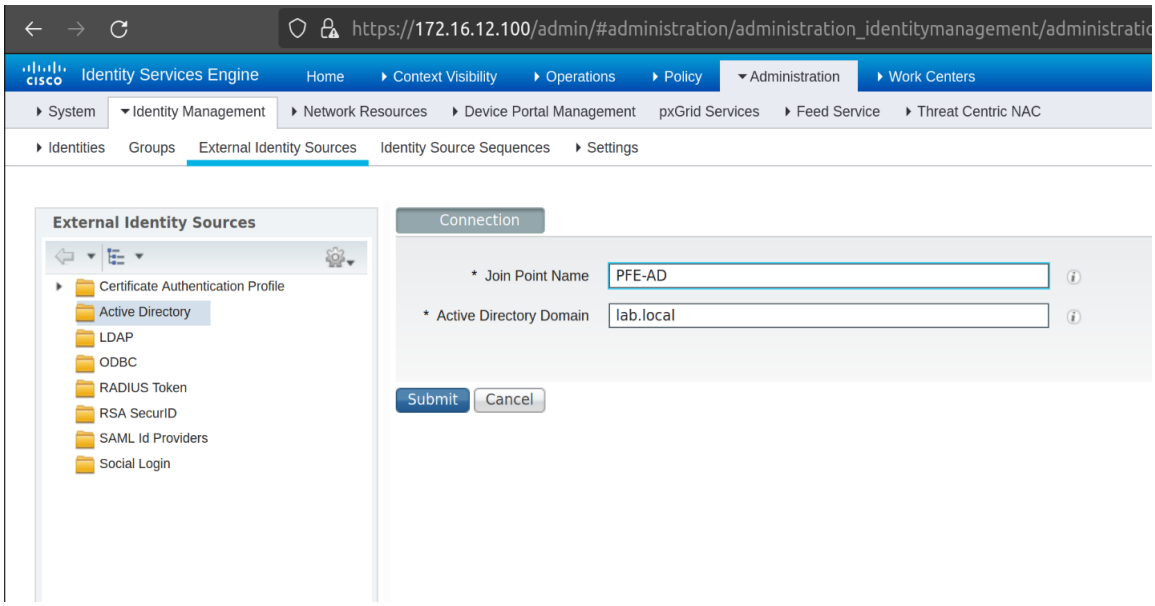

Figure IV.137 Faire appel à Active Directory.

On introduit le nom de domaine de Active directory et demander de joindre le domaine

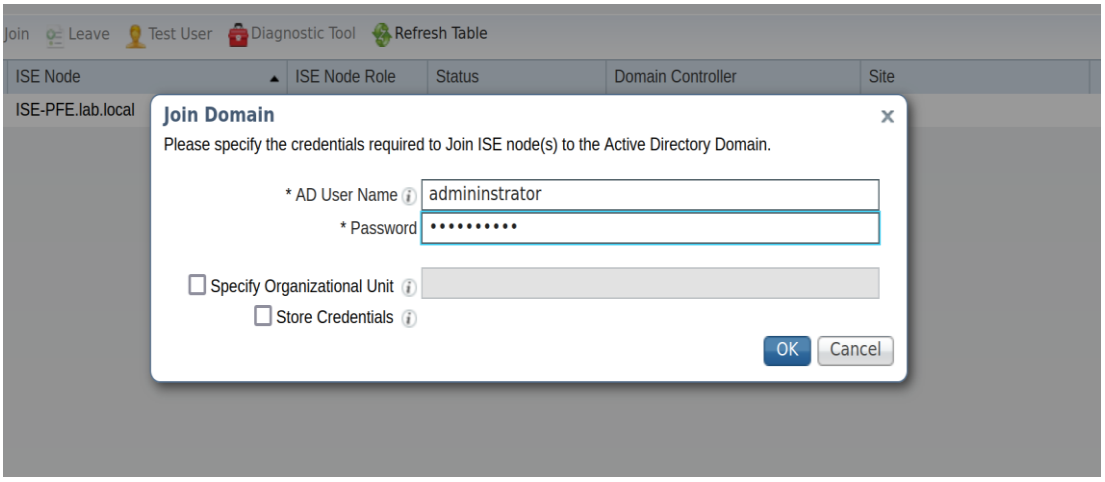

Figure IV.138 Joindre le domaine AD.

La figure suivante montre que nous avons rejoint avec succès le domaine AD

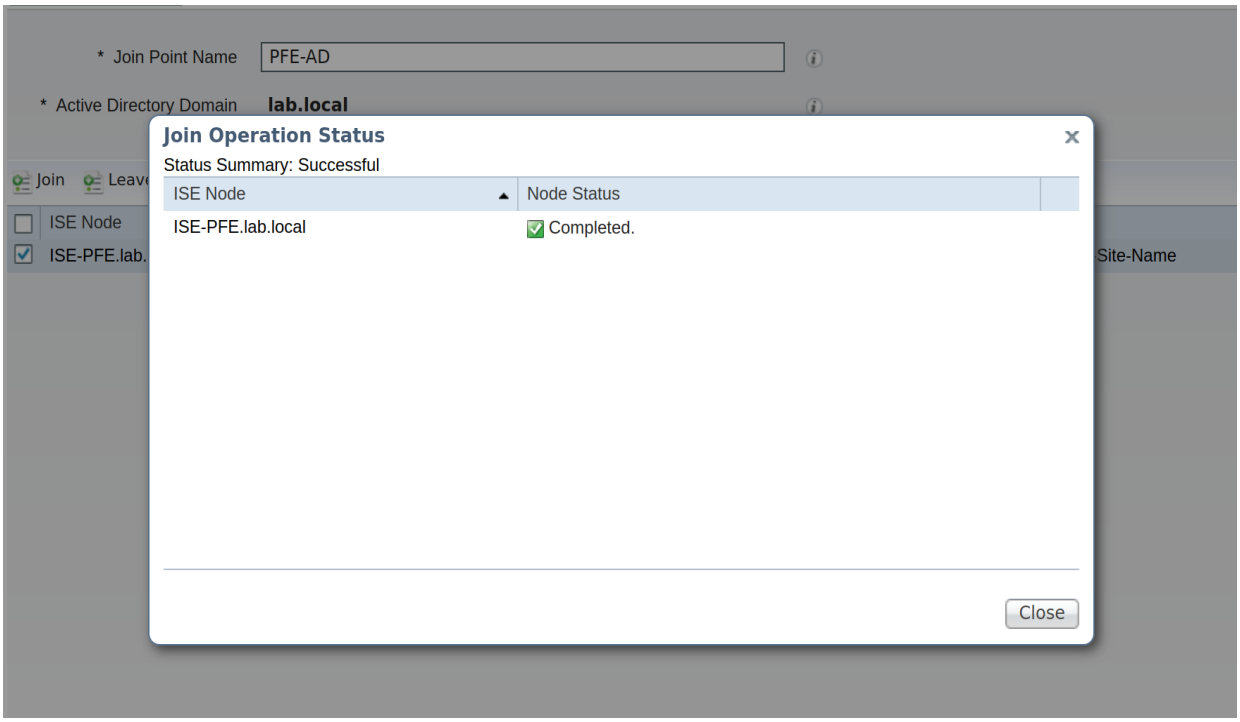

Figure IV.139 Confirmation de jointe du domaine AD.

A présent nous devons importer les groupes et utilisateurs depuis AD, et pour ce faire dans le domaine que nous avons créé on clique sur "ajouter"

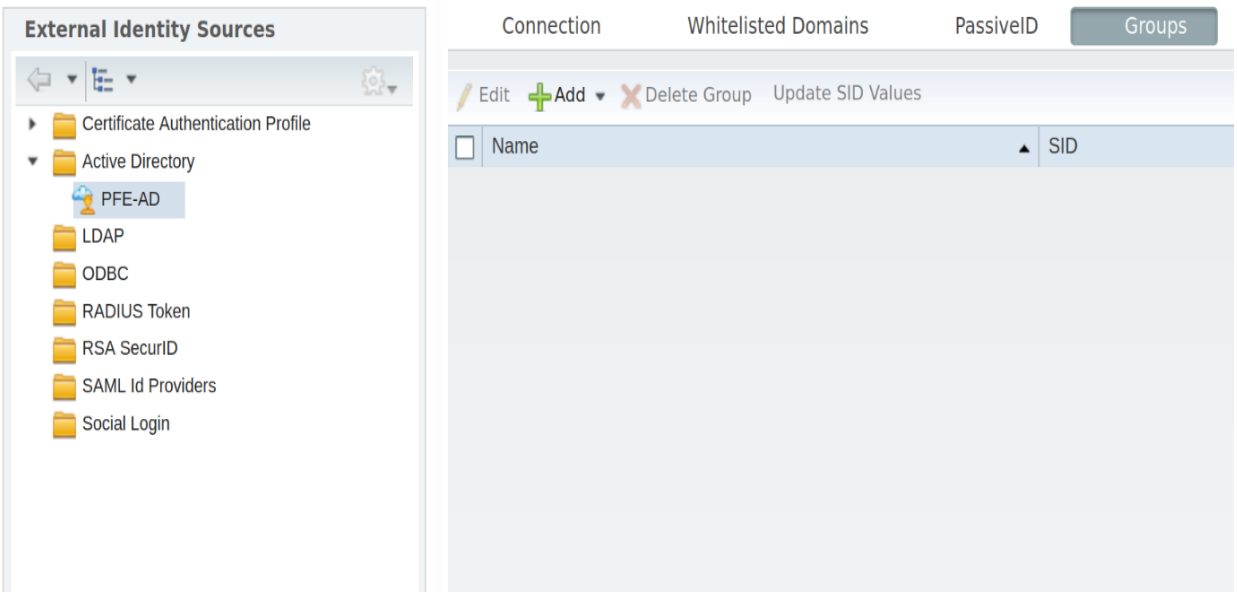

Figure IV.140 Ajouter les groupes.

On sélectionne les groupes que nous souhaitons importer, il est important de noter que les utilisateurs seront importés de manière automatique lors de l'importation des groupes dans lesquels font partie les utilisateurs

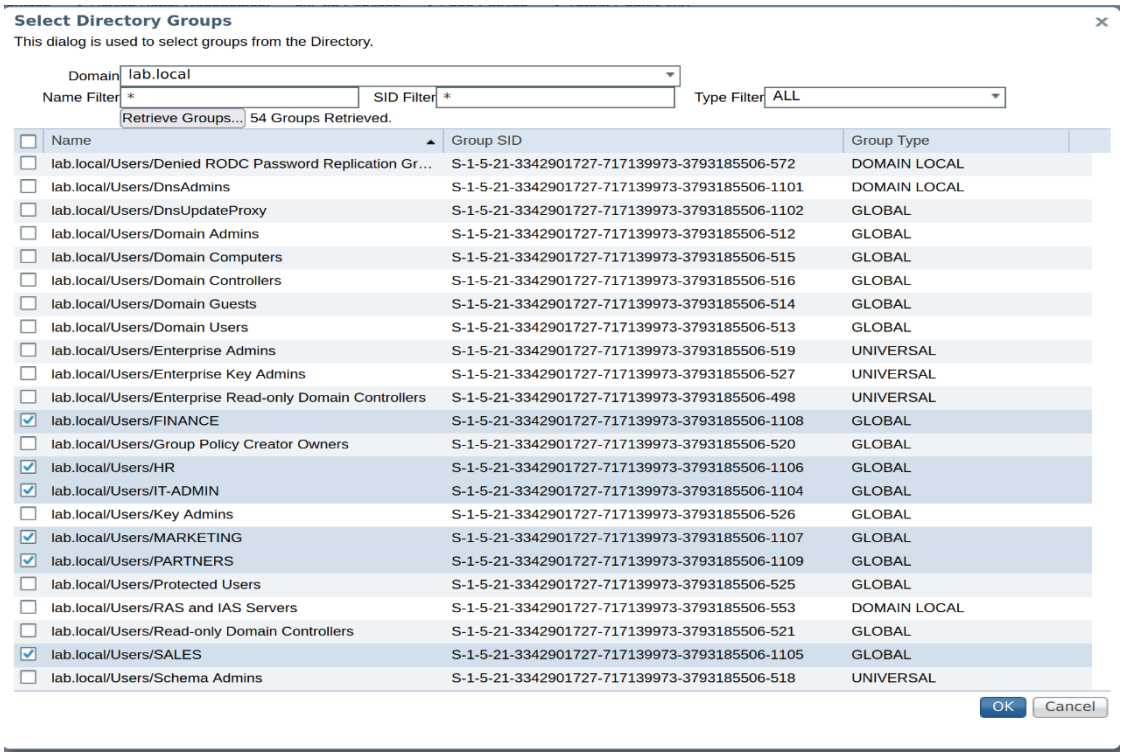

Figure IV.141 Choix des groupes à importer.

On s'aperçoit que nos groupes ont été importer avec succès depuis AD vers Cisco ISE

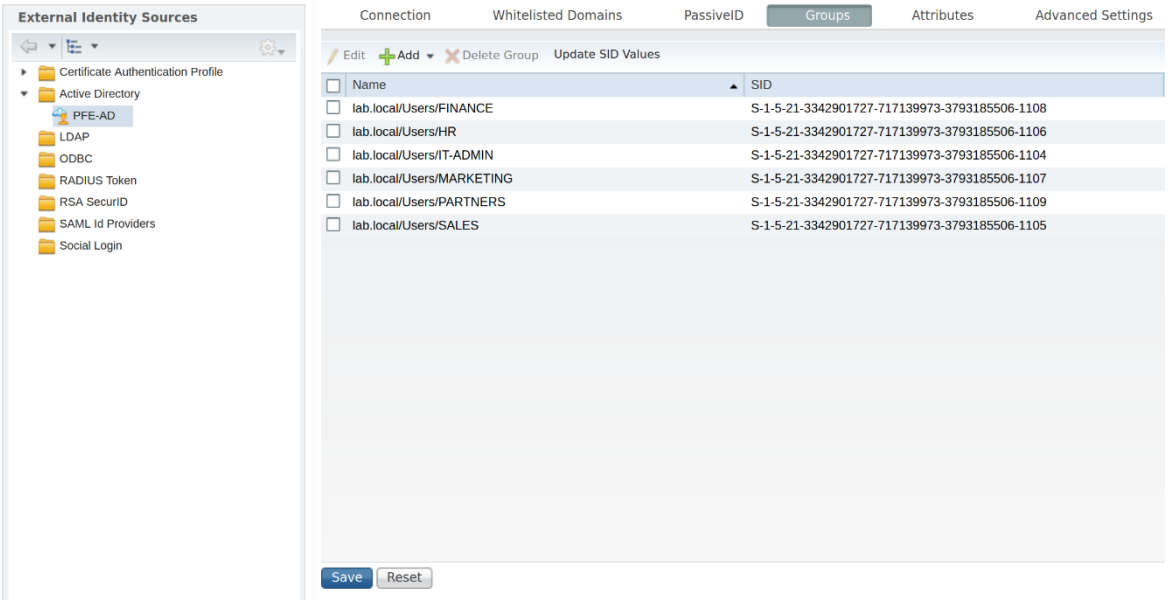

Figure IV.142 Groupes importer vers Cisco ISE.

IV.7.2 Intégration de Cisco Identity Services Engine avec le pare-feu ASA

Maintenait que l'intégration entre AD et Cisco ISE a été établit avec succès nous allons faire la même chose entre notre firewall ASA et Cisco ISE.

Nous devons aussi configurer des pools d'adresses pour les 6 groupes dans on dispose

Nous avons défini les pools d'adresses IP comme le montre le tableau suivant

GROUPE	ADRESSE RESEAU	PREMIÈRE ADRESSE	DERNIÈRE ADRESSE
IT-ADMIN	172.16.1.0/24	172.16.1.10	172.16.1.20
HR	172.16.2.0/24	172.16.2.10	172.16.2.20
SALES	172.16.3.0/24	172.16.3.10	172.16.3.20
FINANCE	172.16.4.0/24	172.16.4.10	172.16.4.20
MARKETING	172.16.5.0/24	172.16.5.10	172.16.5.20
PARTNERS	172.16.6.0/24	172.16.6.10	172.16.6.20

Tableau IV.5 Illustration des plages d'adresses des groupes via l'accès distant.

La configuration de ces dernières se fait avec le CLI du firewall comme suit

```
ciscoasa(config)# ip loca
ciscoasa(config)# ip local p
ciscoasa(config)# ip local pool IT-ADMIN-P
ciscoasa(config)# ip local pool IT-ADMIN-POOL 172.16.1.10-172.16.1.20 ma
ciscoasa(config)# ip local pool IT-ADMIN-POOL 172.16.1.10-172.16.1.20 mask 255$
ciscoasa(config)# ip local pool HR-POOL 172.16.2.10-172.16.2.20 mask 255.255.2$
ciscoasa(config)# ip local pool SALES-POOL 172.16.3.10-172.16.3.20 mask 255.25$
ciscoasa(config)# ip local pool FINANCE-POOL 172.16.4.10-172.16.4.20 mask 255.$
ciscoasa(config)# ip local pool MARKETING-POOL 172.16.5.10-172.16.5.20 mask 25$
ciscoasa(config)# ip local pool PARTNERS-POOL 172.16.6.10-172.16.6.20 mask 255$
ciscoasa(config)# sh run ip l
ciscoasa(config)# sh run ip local p
ciscoasa(config)# sh run ip local pool
ip local pool IT-ADMIN-POOL 172.16.1.10-172.16.1.20 mask 255.255.255.0
ip local pool HR-POOL 172.16.2.10-172.16.2.20 mask 255.255.255.0
ip local pool SALES-POOL 172.16.3.10-172.16.3.20 mask 255.255.255.0
ip local pool FINANCE-POOL 172.16.4.10-172.16.4.20 mask 255.255.255.0
ip local pool MARKETING-POOL 172.16.5.10-172.16.5.20 mask 255.255.255.0
ip local pool PARTNERS-POOL 172.16.6.10-172.16.6.20 mask 255.255.255.0
```

Figure IV.143 Configuration des pools d'adresses.

Désormais nous allons configurer les "group policy" ou nous allons créer six groupes pour les six existant sur Active Directory tout en ajoutant le DNS en adresse IP et en nom de domaine

```
ciscoasa(config)# group-policy IT-ADMIN-GR inter
ciscoasa(config)# group-policy IT-ADMIN-GR internal
ciscoasa(config)# group-policy IT-ADMIN-GR a
ciscoasa(config)# group-policy IT-ADMIN-GR attributes
ciscoasa(config-group-policy)# vpn-tunnel-pro
ciscoasa(config-group-policy)# vpn-tunnel-protocol ss
ciscoasa(config-group-policy)# vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)# dns-server value 172.16.12.132
ciscoasa(config-group-policy)# def
ciscoasa(config-group-policy)# default-domain v
ciscoasa(config-group-policy)# default-domain value
ERROR: % Incomplete command
ciscoasa(config-group-policy)# default-domain value lab.local
```

Figure IV.144 Configuration des policy group.

Il faut désormais associer les "group policy" aux profils de connexions correspondant et en spécifiant que le type d'accès est l'accès distant

```
ciscoasa(config)# tunnel-group IT-ADMIN-PROFILE type remote-access
ciscoasa(config)# tunnel-group IT-ADMIN-PROFILE gen
ciscoasa(config)# tunnel-group IT-ADMIN-PROFILE general-attributes
ciscoasa(config-tunnel-general)# def
ciscoasa(config-tunnel-general)# default-group-policy
ciscoasa(config-tunnel-general)# default-group-policy IT-ADMIN-GR
ciscoasa(config-tunnel-general)# add
ciscoasa(config-tunnel-general)# address-pool IT-ADMIN-POOL
ciscoasa(config-tunnel-general)# EXIT
```

Figure IV.145 Association des profils aux groupes.

Maintenant on va accéder à l'interface graphique de Cisco ISE pour ajouter notre pare-feu pour qu'il s'intègre et travail conjointement avec le serveur radius, on suit ces étapes :

On se rend dans l'objet Administration des groupes de périphériques réseaux pour pouvoir ajouter un groupe dédié au pare-feu

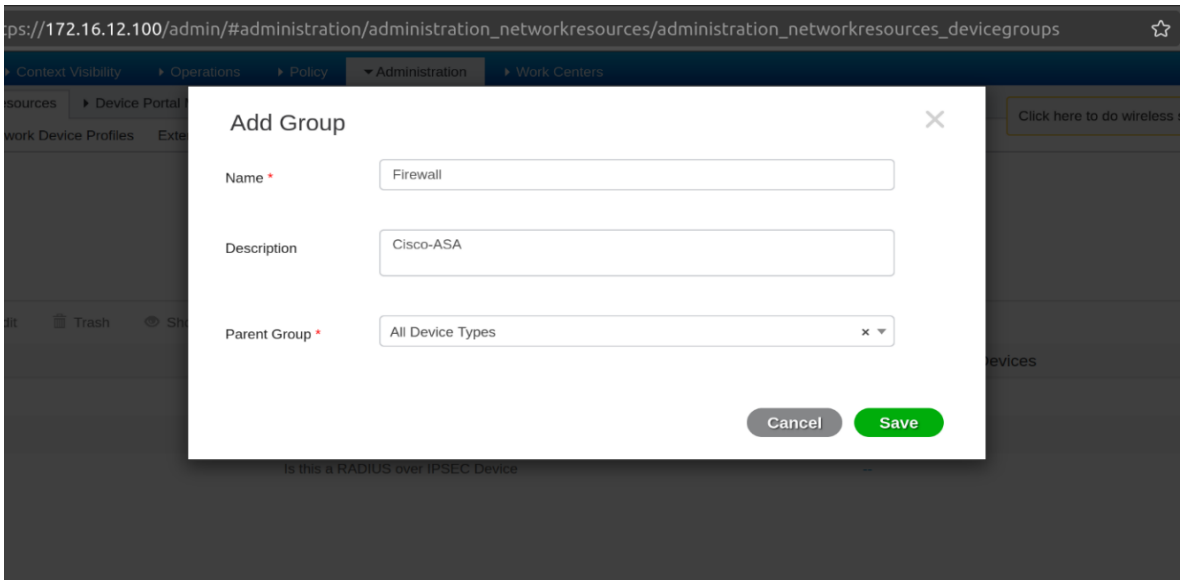

Figure IV.146 Ajout d'un groupe de pare-feu.

On va mettre les paramètres réseaux du firewall demandé comme le montre cette figure

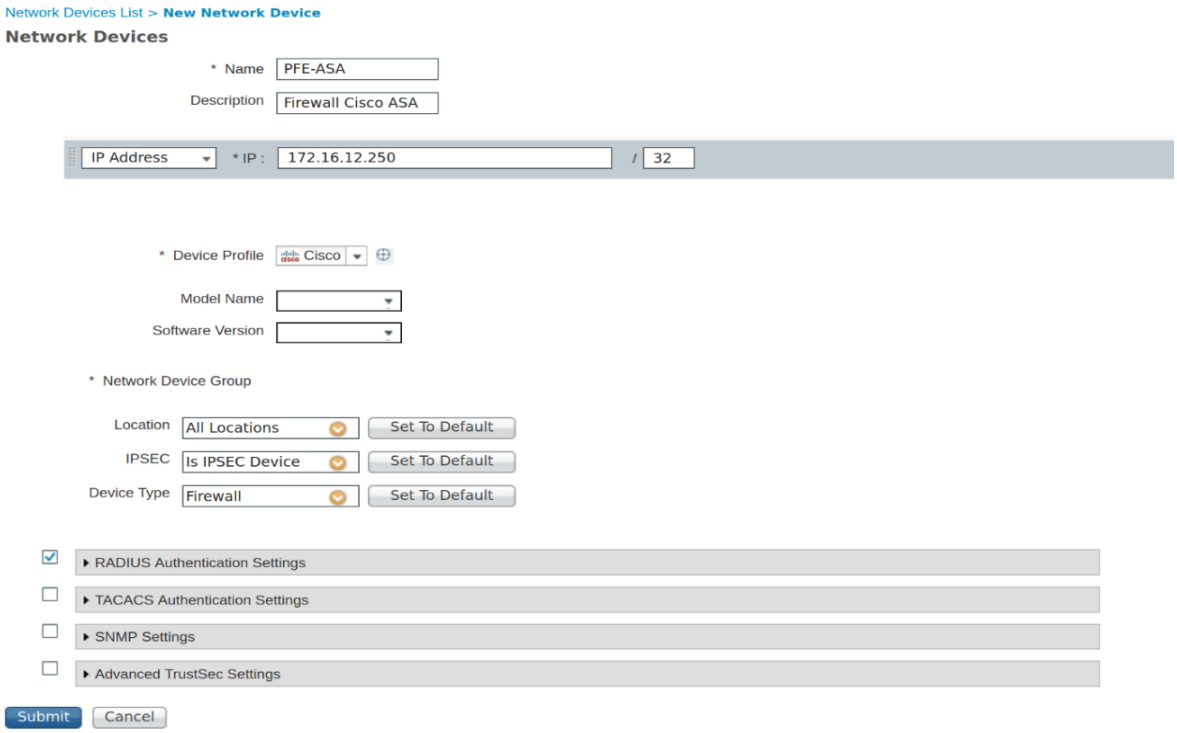

Figure IV.147 Paramètres réseaux.

On voit l'apparition de notre firewall, ce qui signifie que la première étape d'intégration du pare-feu est terminée

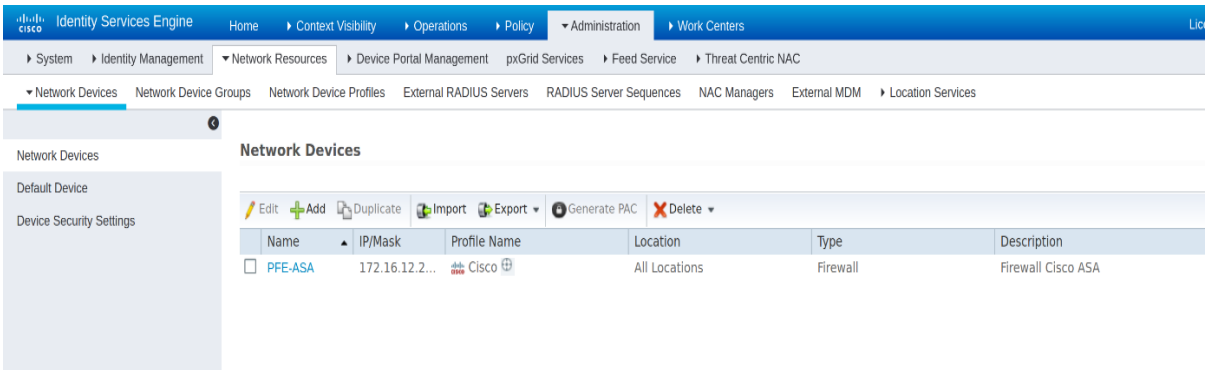

Figure IV.148 Association du pare-feu avec Cisco ISE.

Maintenant on doit faire l'inverse, c'est à dire intégrer ISE au pare-feu ASA

Pour commencer dans le mode configuration on va activer le protocol radius et paramétrer le triple A et mettre l'adresse IP de notre serveur ISE, puis mettre en marche le service triple A, le tout avec des lignes de commandes, qui sont les suivantes

```
ciscoasa# config t
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# aaa-server PFE-ISE protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server PFE-ISE (prod) host 172.16.12.100
ciscoasa(config-aaa-server-host)# key cisco
ciscoasa(config-aaa-server-host)#
ciscoasa(config-aaa-server-host)#
ciscoasa(config-aaa-server-host)# sh run aaa-server
aaa-server PFE-ISE protocol radius
aaa-server PFE-ISE (prod) host 172.16.12.100
 key *****
ciscoasa(config-aaa-server-host)#
```

Figure IV.149 Activation du service AAA.

On va créer des tunnel groupe pour les six groupes, c'est ainsi que l'authentification se fera par Cisco ISE, voici un exemple pour le groupe HR

```
ciscoasa(config)# tunnel-group HR-PROFILE general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group PFE-ISE
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)#
```

Figure IV.150 Gestion des authentifications par ISE.

IV.8 Configuration des ACL

Maintenant que nos deux équipements se sont parfaitement intégrés, on va procéder à la configuration des ACL, dans l'objet autorisation qui se trouve dans "policy".

Nous aurons trois ACL à créer, une ACL full accès pour le groupe "IT-ADMIN", une autre avec accès pour "FTP, WEB et DNS" pour les groupes : "HR, FINANCE, MARKETING et SALES", et enfin une ACL pour le groupe "PARTNERS" à qui on donnera accès que pour le site WEB

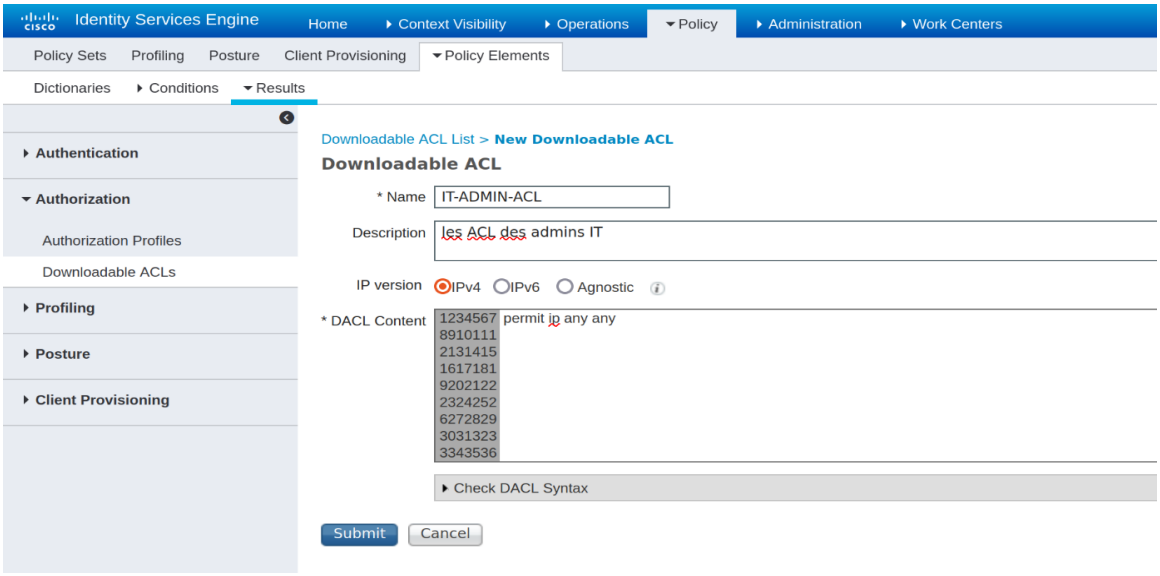

Figure IV.151 Création de l'ACL IT-ADMIN.

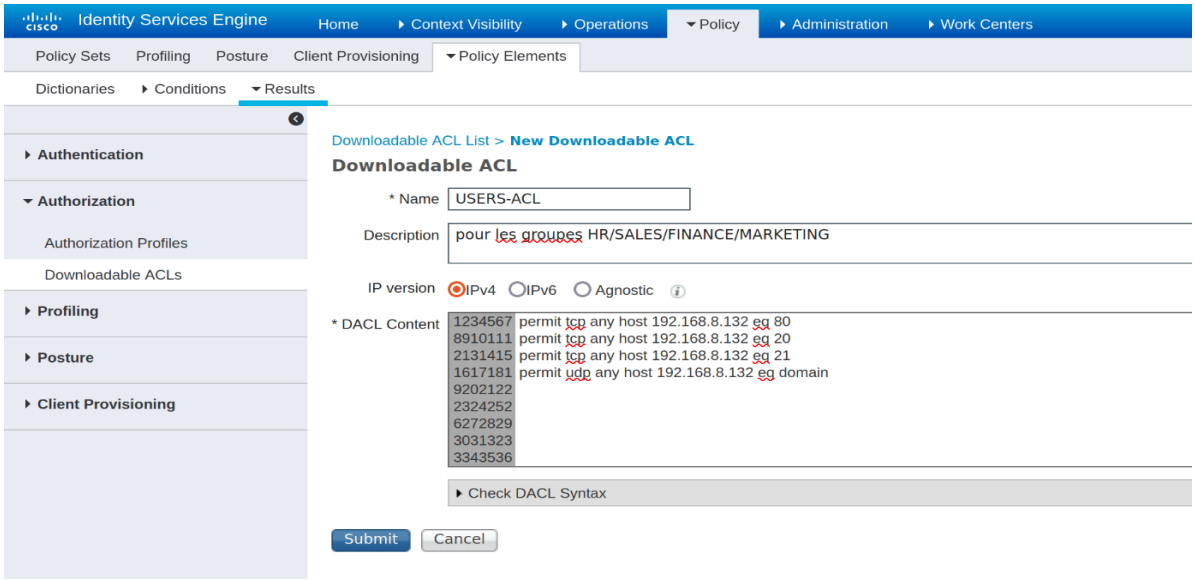

Figure IV.152 Création de l'ACL pour HR, FINANCE, SALES et MARKETING.

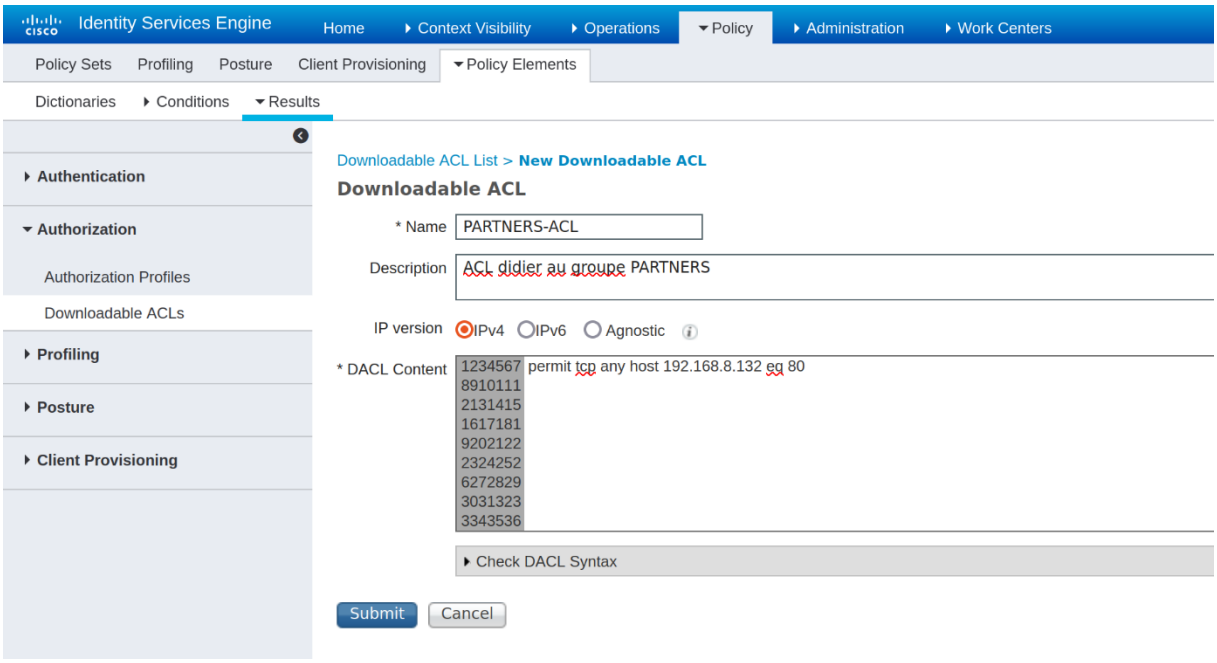

Figure IV.153 Création de l'ACL PARTNERS.

On va désormais attribuer les ACL aux profils correspondant, en passant par plusieurs étapes qui seront montrer dans les figures suivantes

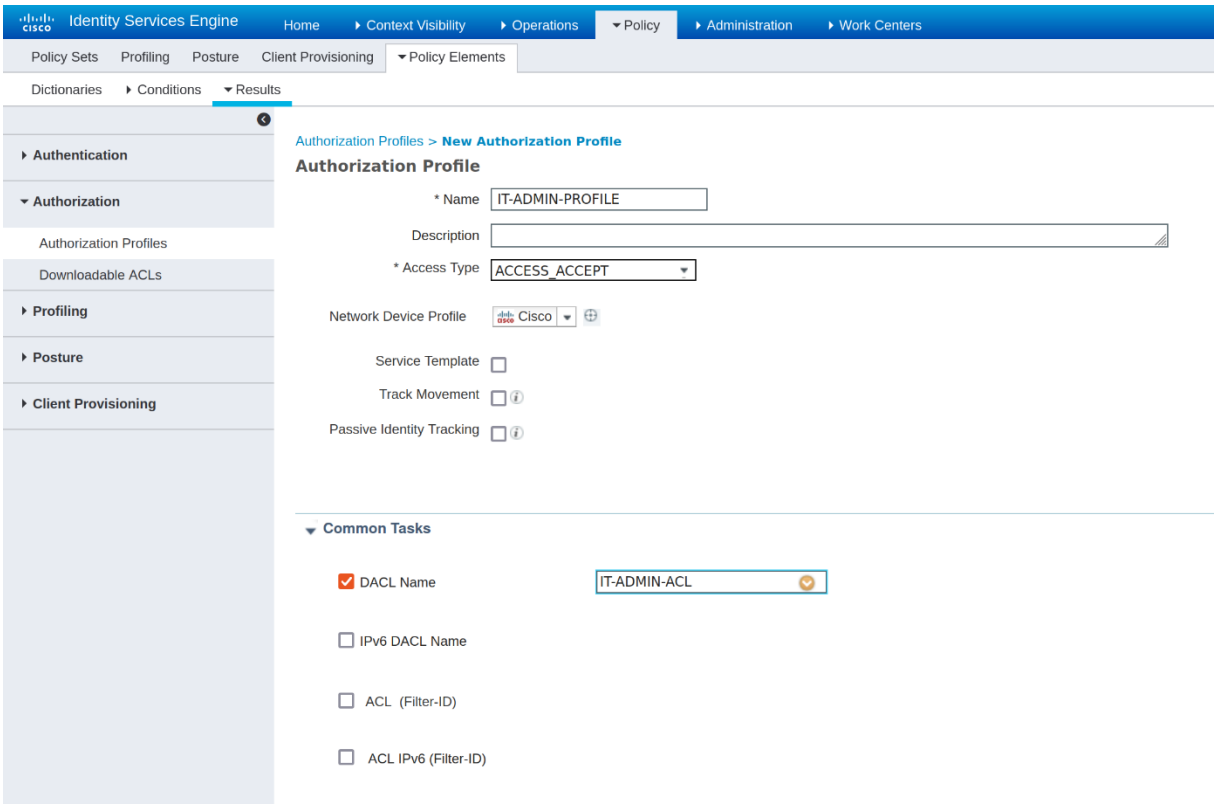

Figure IV.154 Association de l'ACL IT-ADMIN-ACL au profil IT-ADMIN.

Dans "policy set" on va cliquer sur "authorization"

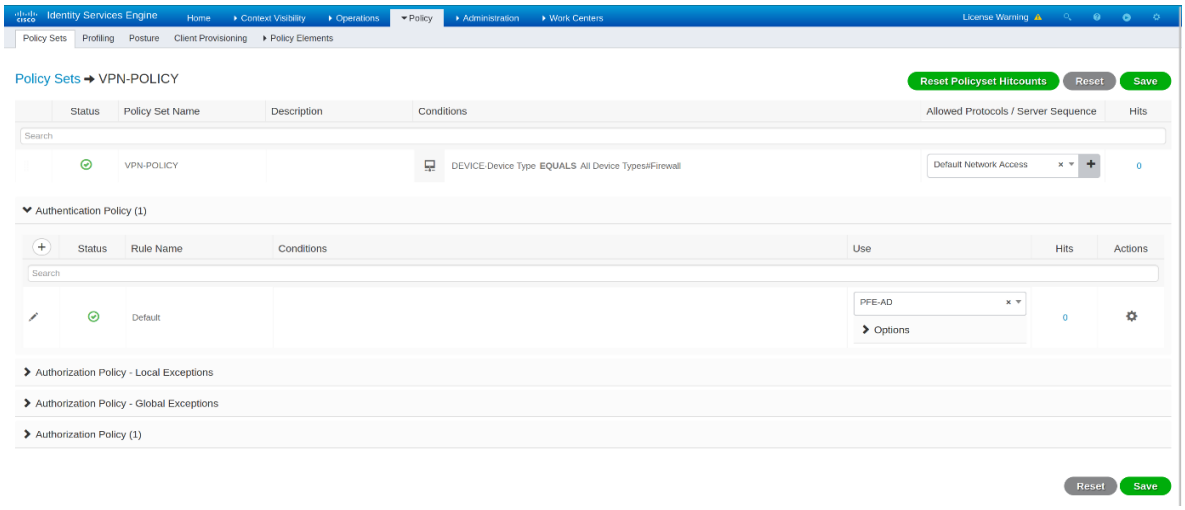

Figure IV.155 Association des profils aux groupes.

Pour chaque ACL ont choisi son groupe

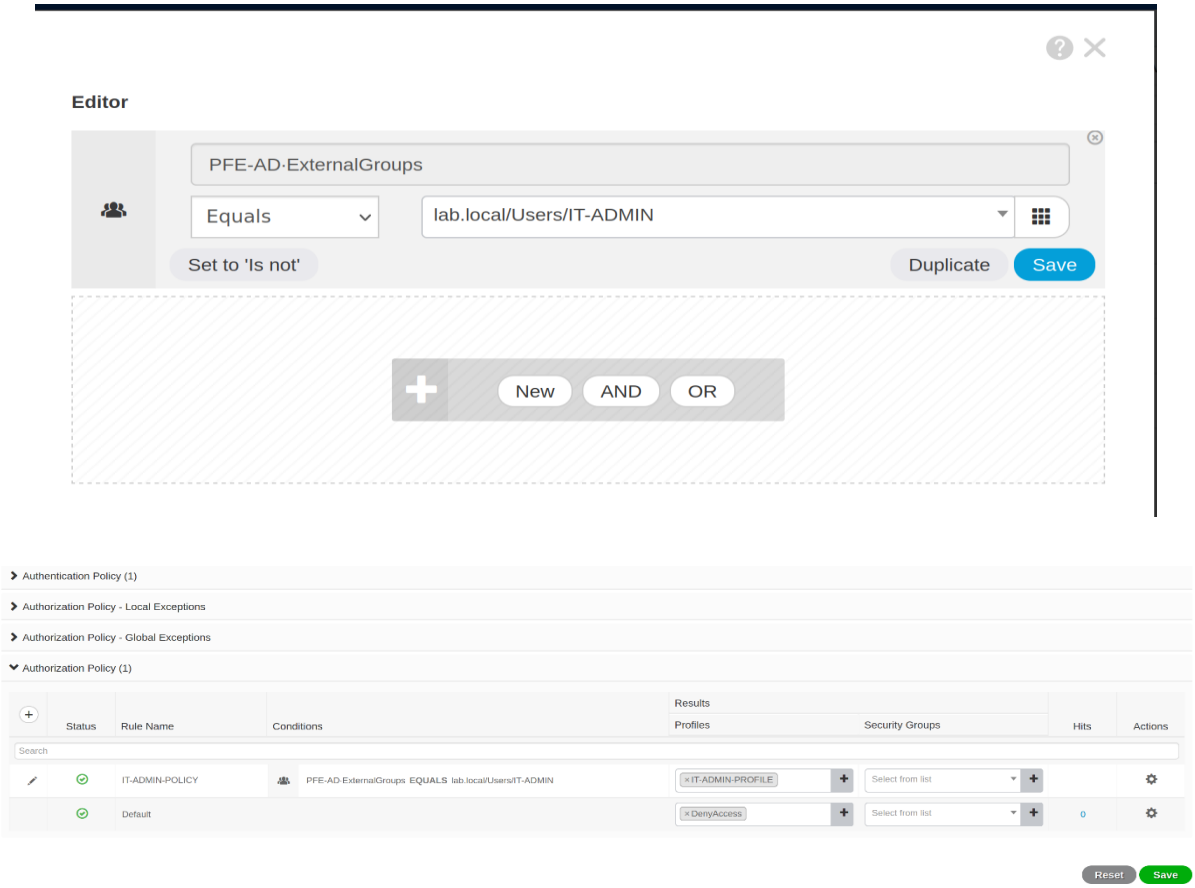

Figure IV.156 Association des ACL aux groupes.

Unr fois toutes les ACL attribues à leurs groupes on obtient cette figure qui nous montre que chaque groupe à ces ACL adéquates

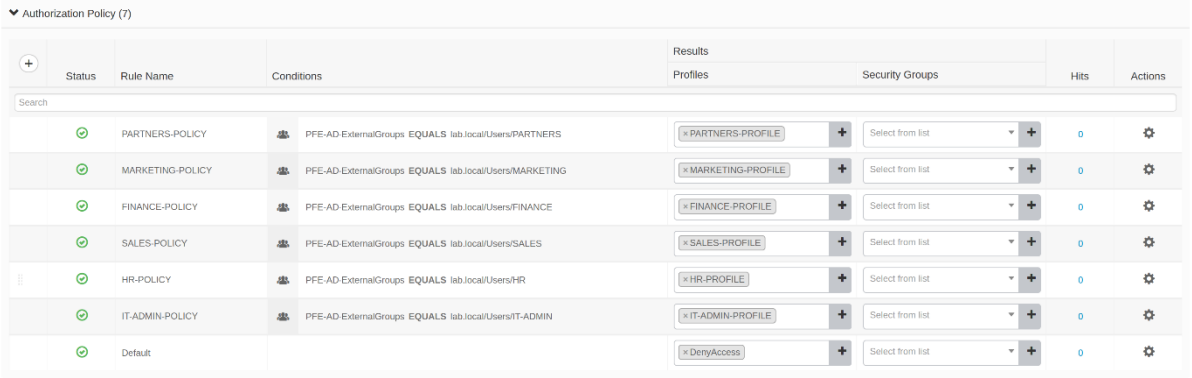

Figure IV.157 Visualisation des autorisations policy.

Nous allons aussi verrouiller les profils avec leurs groupes de connexion, ce qui signifie que l'utilisateur X faisant partie d'un groupe Y, ne peut accéder qu'avec son groupe

Pour activer cette fonctionnalité à partir de Cisco ISE on va dans "Policy Set – Results – authorization profiles"

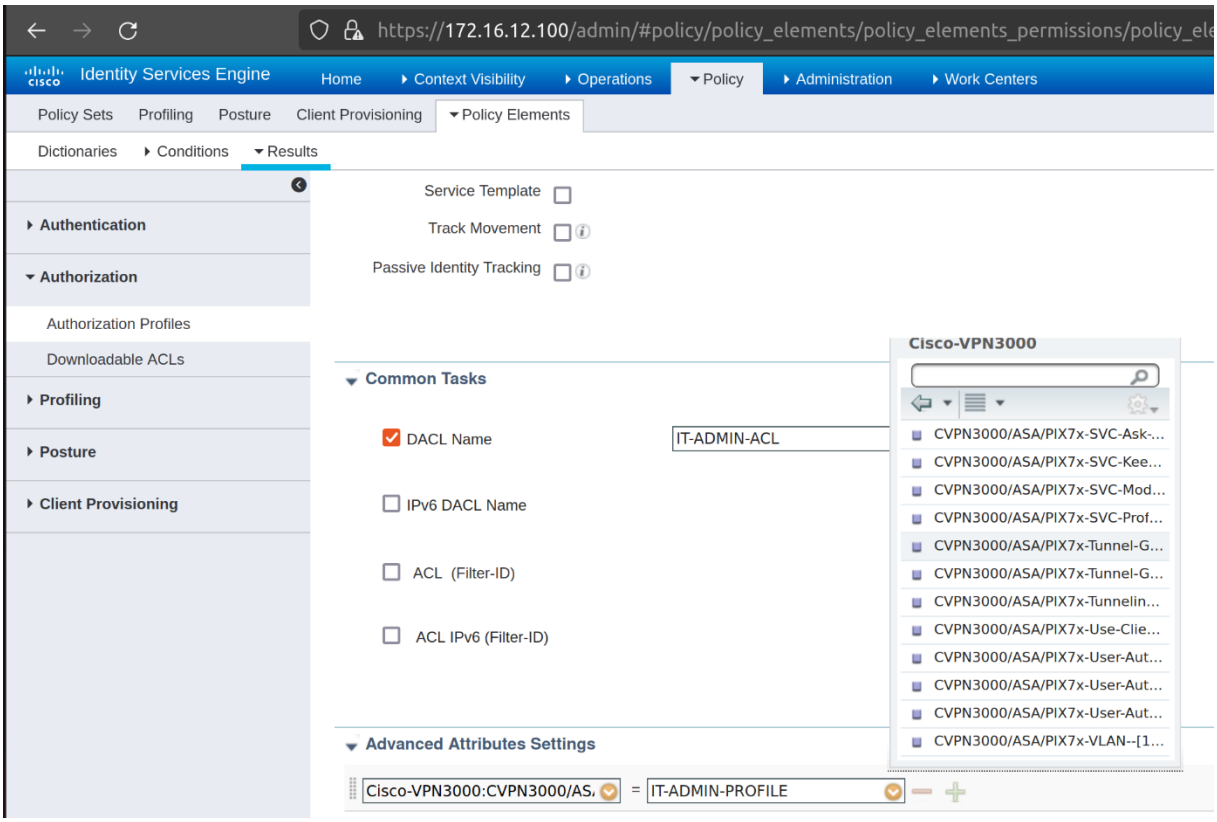

Figure IV.158 Chemin de Group-Lock.

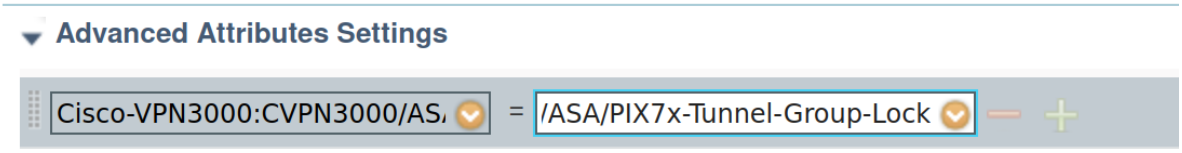

Figure IV.159 Verrouillage du Profile.

IV.9 Configuration du Port Forwarding

A ce stade notre accès distant a été configuré ave succès, il ne manque plus que configurer le "port forwarding" au niveau du Modem pour que le firewall laisse passer les requêtes émanent de internet via le tunnel VPN vers le réseau et les services locaux

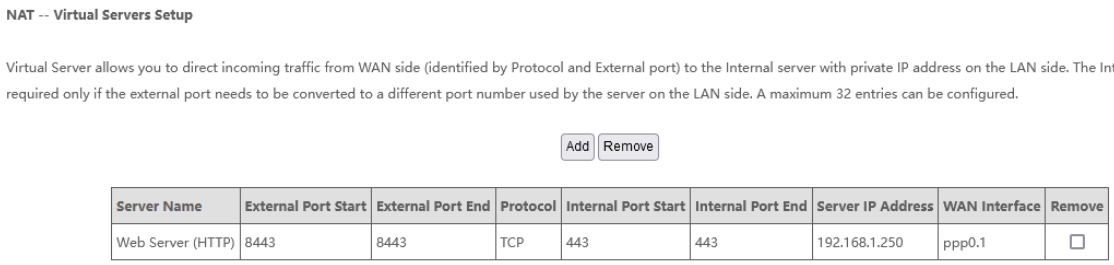

Figure IV.160 Configuration du port forwarding.

IV.10 Tests

Nous allons tester l'automatisation de migration

Le scenario de test est le suivant

Nous avons un serveur ESXI qui utilise quasiment toute ces ressources nous allons allumer une VM sur le même ESXI nous allons recevoir une notification DRS qui nous suggère ou nous pouvons allumer cette VM

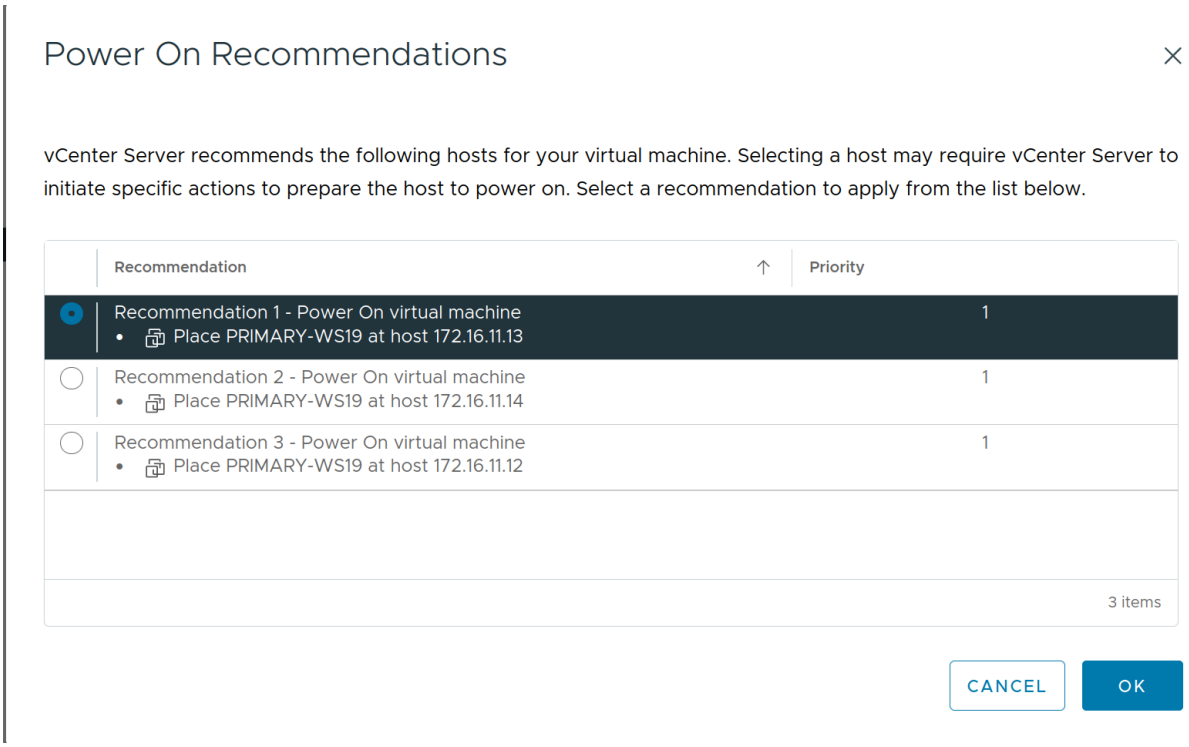

Figure IV.161 Suggestion DRS.

Nous avons une VM test que nous avons allumé sur l'ESXI 04 puis nous allons éteindre se serveur ESXI et nous allons voir que la VM va rester allumer est sera automatiquement migré vers un autre serveur ESXI

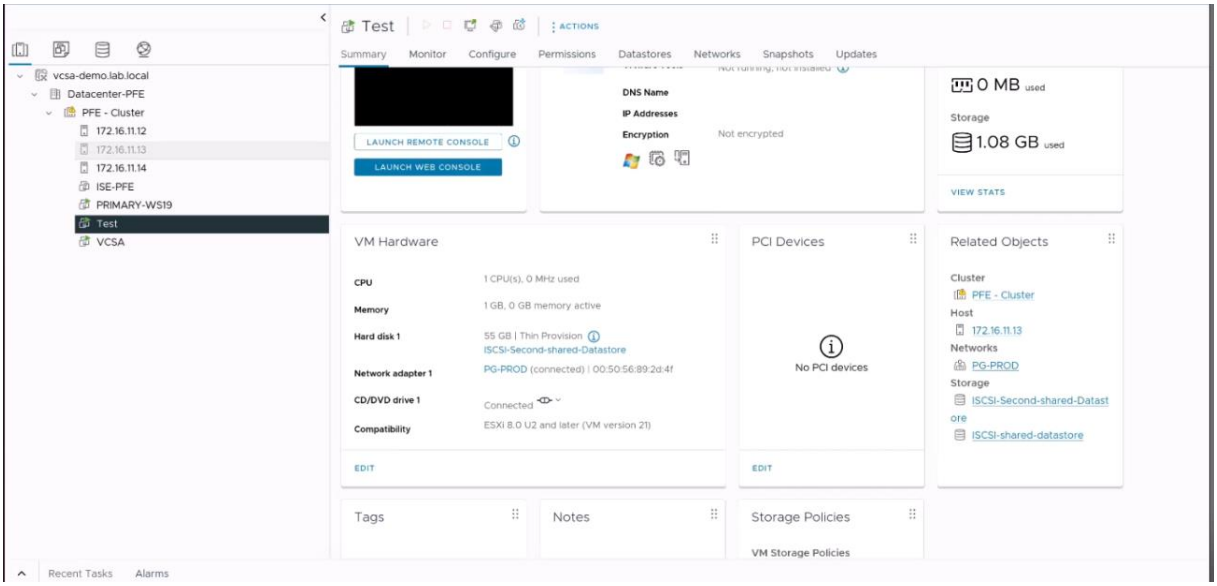

Figure IV.162 Test HA.

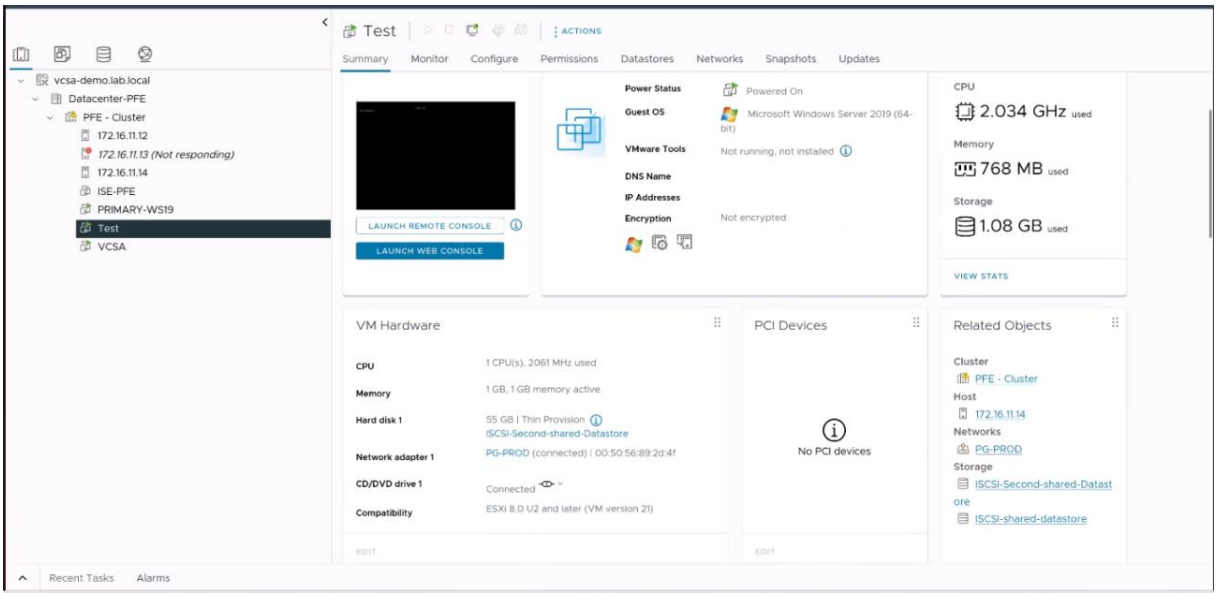

Figure IV.163 Test HA.

Désormais nous allons procéder aux tests du VPN

Le scenario des tests et le suivant

Je suis "cmeyer" je fais partie des administrateurs "IT" de l'entreprise, je souhaite faire des configurations sur mon serveur ISE depuis mon domicile, pour se faire je dois d'abord accéder à l'application "AnyConnect" et j'introduis l'adresse IP public de mon réseau local suivit du numéro de port "8443" comme indiqué sur cette figure

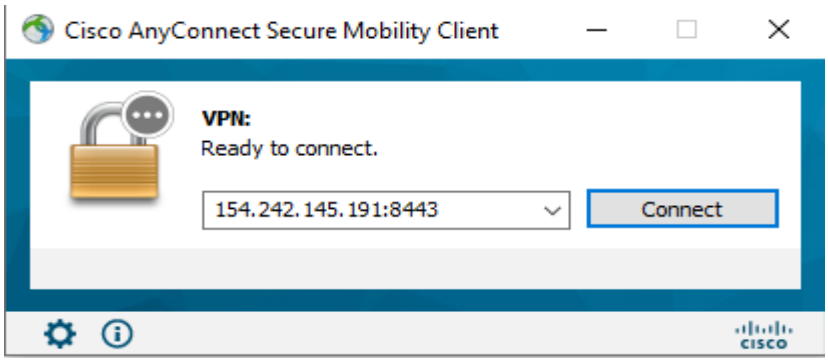

Figure IV.164 Connexion VPN.

Une fois avoir cliquer sur "connect", une fenêtre d'authentification va s'afficher comme le montre cette figure

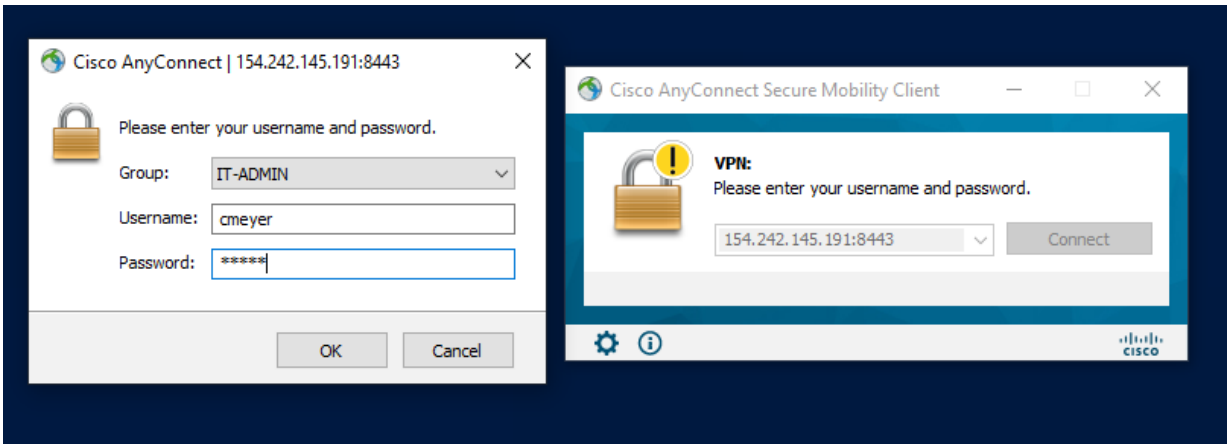

Figure IV.165 Authentification de l'utilisateur.

A cette étape le pare-feu, en collaboration avec Cisco ISE vont authentifier l'utilisateur et lui donner les autorisations nécessaires, l'utilisateur va être authentifier avec succès, et un chrono va s'afficher, il représente le temps d'ouverture de la session

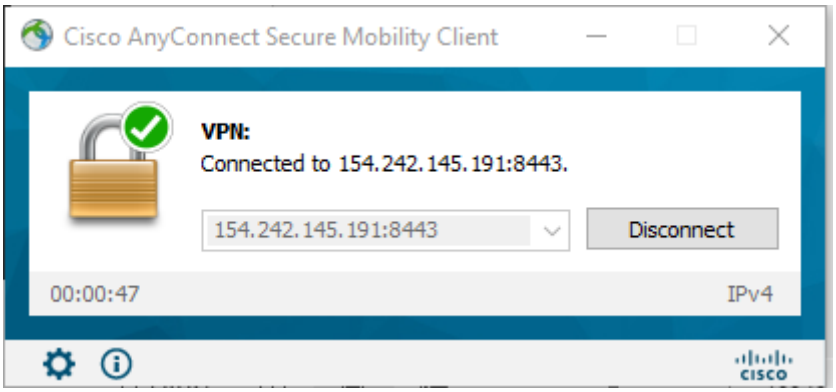

Figure IV.166 Utilisateur authentifier avec succès.

On procède à une vérification de l'adresse IP qui lui a été attribuer

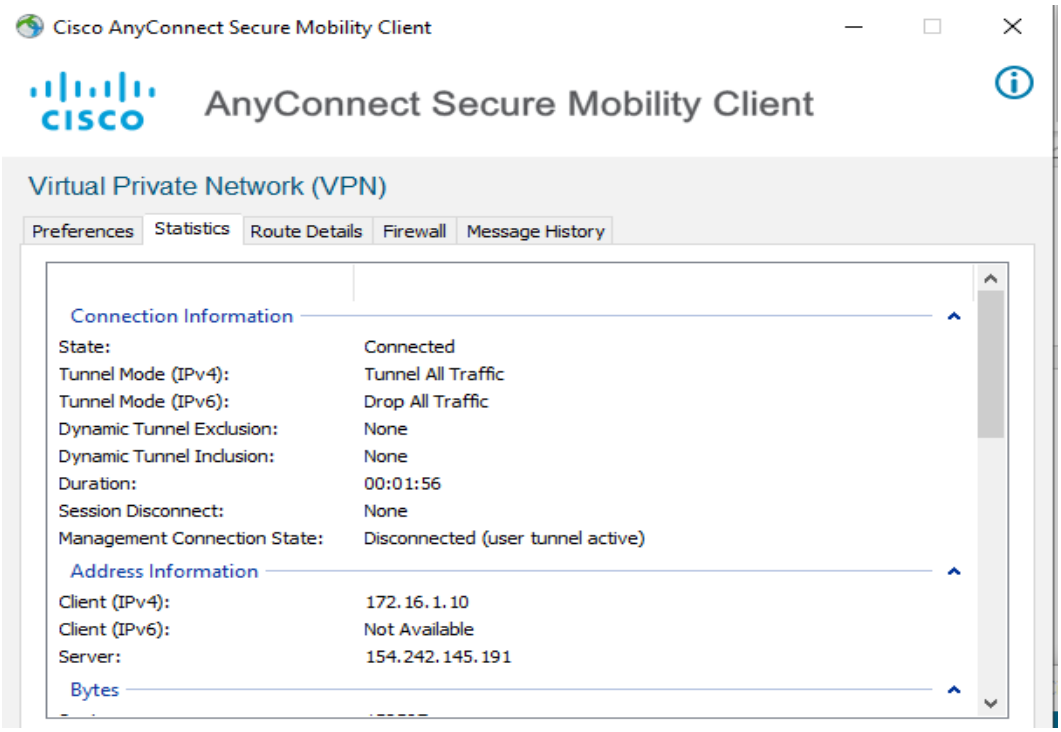

Figure IV.167 Statistiques de connexion.

On voit qu'effectivement il a récupéré une adresse IP du pool d'adresse auquel il appartient.

Nous pouvons vérifier le journal pour voir ce qui s'est passé lors de l'authentification

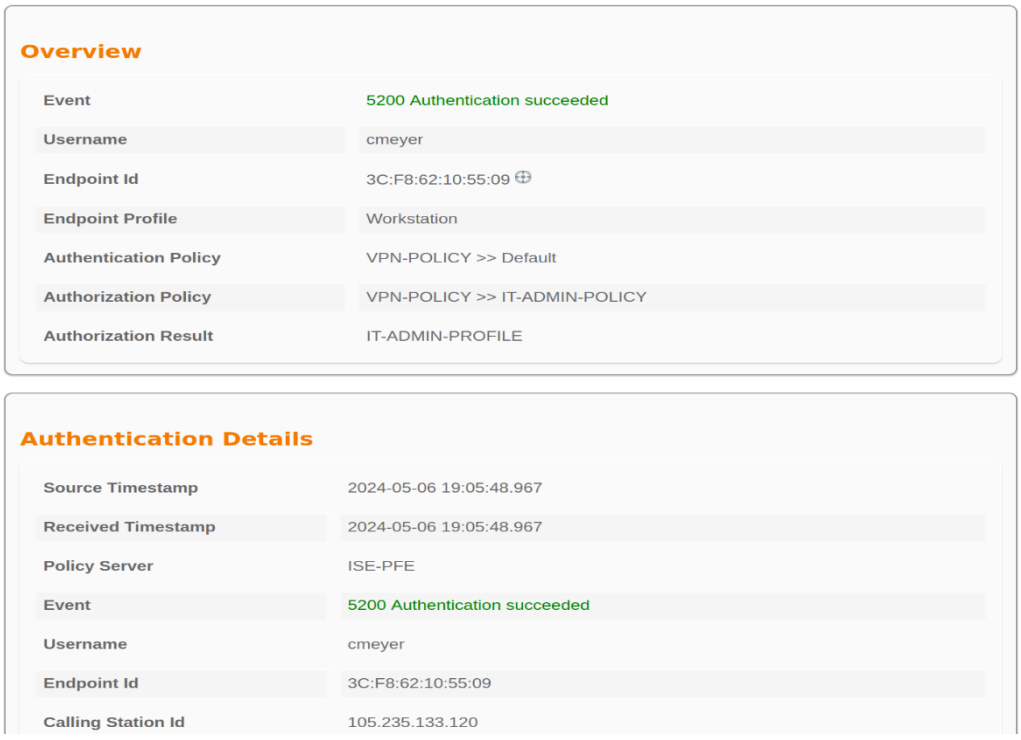

Figure IV.168 Authentification de l'utilisateur.

Nous avons les mêmes détails sur le pare-feu avec la commande "show vpn-sessiondb anyconnect"

```
Username     : cmeyer                  Index        : 58
Assigned IP  : 172.16.1.10             Public IP    : 105.235.133.120
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 20177                   Bytes Rx     : 30192
Group Policy : IT-ADMIN-GR             Tunnel Group : IT-ADMIN-PROFILE
Login Time   : 13:42:40 UTC Thu May 9 2024
Duration     : 0h:00m:39s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : ac100bfa0003a000663cd2d0
Security Grp : none
```

Figure IV.169 Details de la connexion sur ASA.

Et si un utilisateur tante de se connecter avec un groupe de profil auquel il n'appartient pas, la connexion ne s'établira pas, il va authentifier l'utilisateur mais ne le laisserai pas accéder au réseau

```
%ASA-6-113004: AAA user authentication Successful : server =  172.16.12.100 : user = cmeyer
%ASA-6-113009: AAA retrieved default group policy (FINANCE-GR) for user = cmeyer
%ASA-6-113008: AAA transaction status ACCEPT : user = cmeyer
%ASA-4-113040: Group <FINANCE-GR> User <cmeyer> IP <105.235.133.120> Terminating the VPN conne
ction attempt from <FINANCE-PROFILE>. Reason: This connection is group locked to <IT-ADMIN-PRO
FILE>.
```

Figure IV.170 Connexion échoué.

Maintenant il ne lui reste qu'à introduire l'adresse IP ou l'FQDN de Cisco ISE pour qu'il puisse accéder

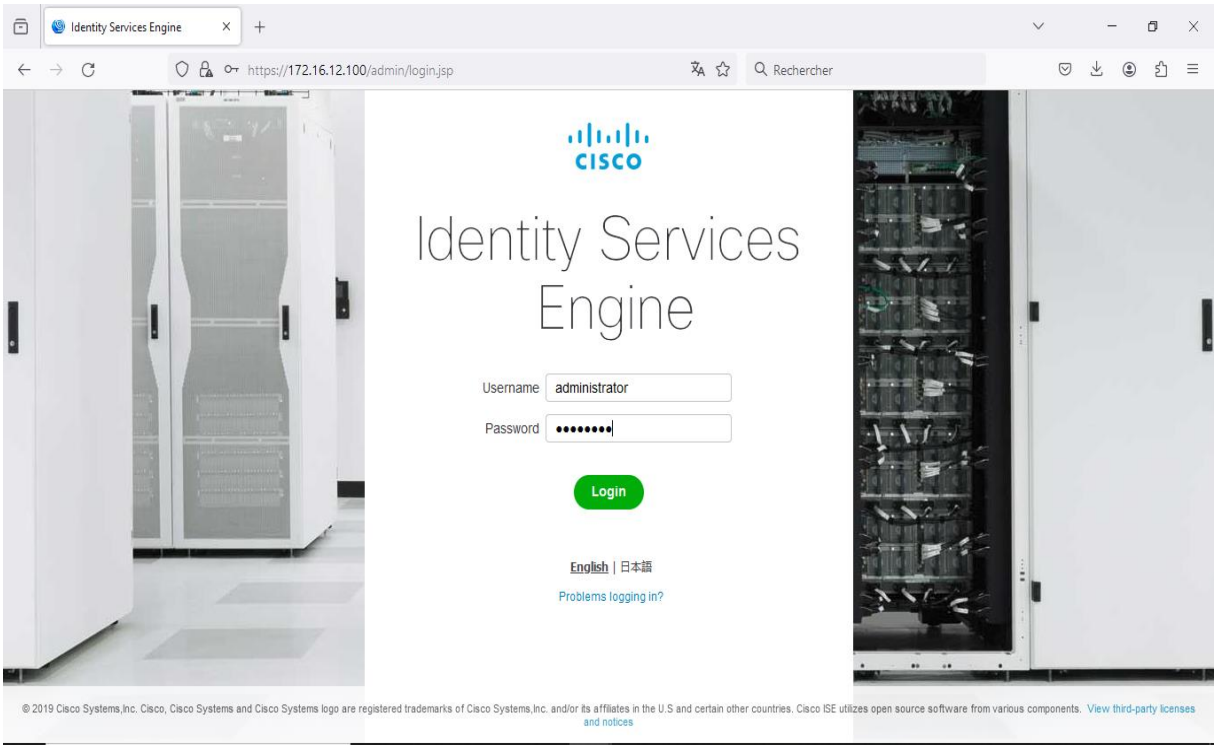

Figure IV.171 Accès distant au serveur ISE.

L'utilisateur souhaite à présent déposer des fichiers sur le serveur FTP, c'est simple, il ouvre une fenêtre sur le navigateur et introduit l'adresse IP du serveur FTP précédé de FTP://

La figure suivante le montre

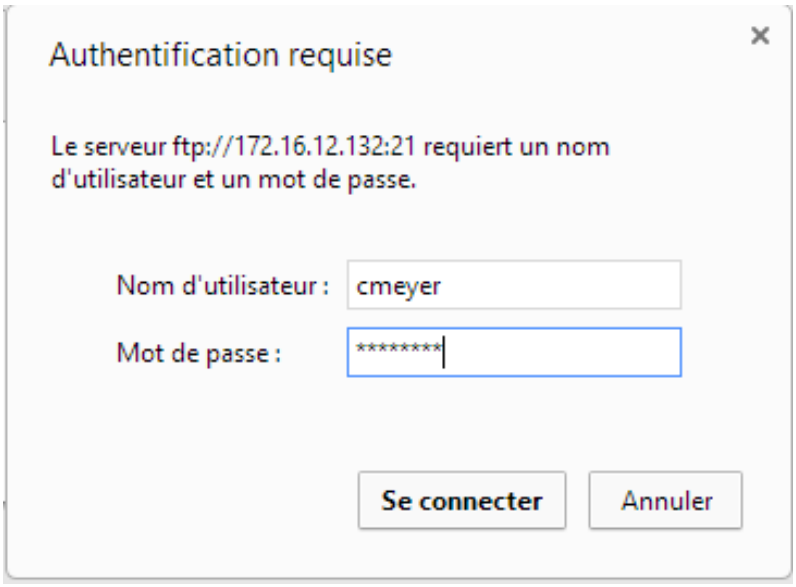

Figure IV.172 Accès distant au serveur FTP.

L'utilisateur souhaite accéder au site WEB de l'entreprise, dans une nouvelle fenêtre sur le navigateur il tape http://172.16.12.132 ou http://pfe.lab.local et la page web s'affiche comme suit

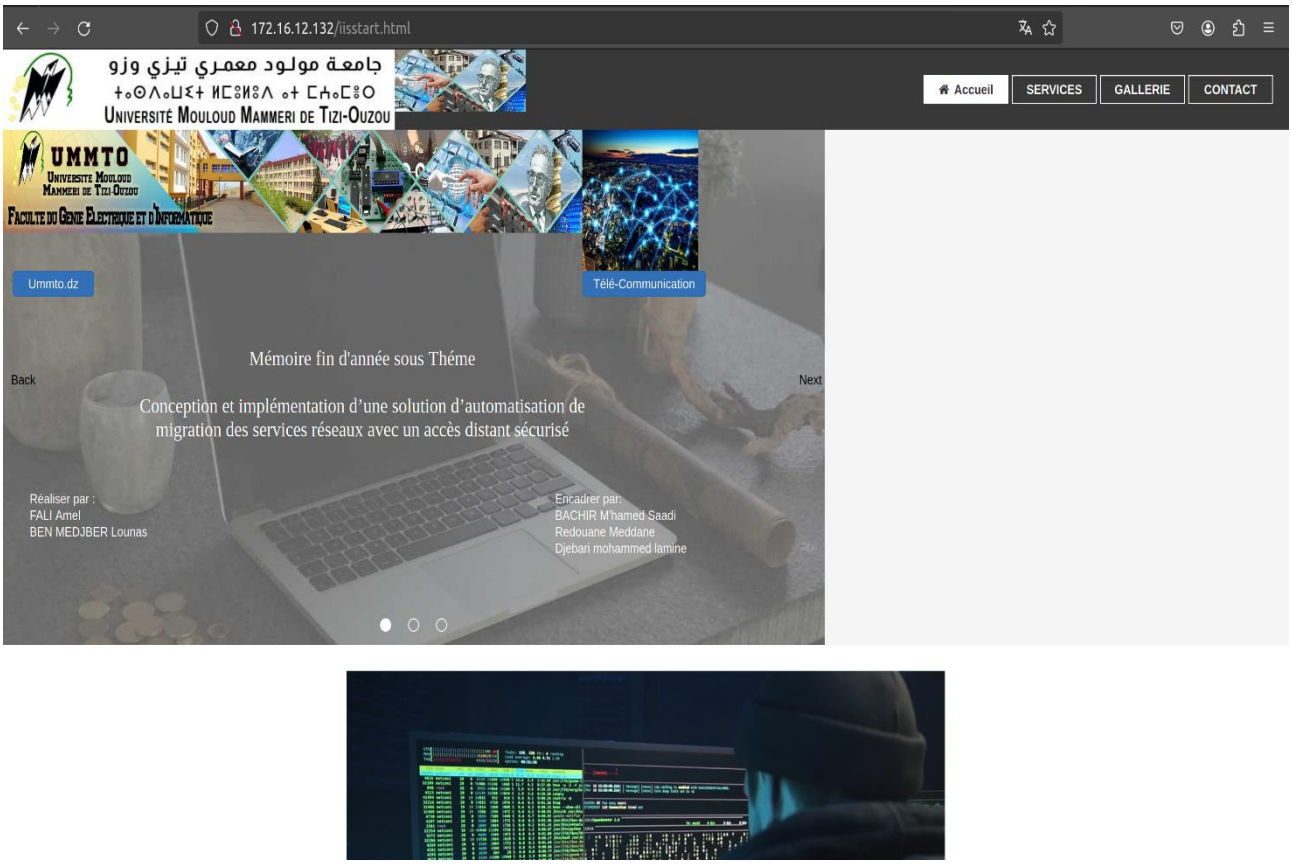

Figure IV.173 Accès au site WEB.

IV.11 Conclusion

Tout au long de ce chapitre, nous avons présenté l'environnement de travail ainsi que les outils utilisés. Nous avons mis en place notre solution en installant et en configurant l'hyperviseur VMware ESXi, VMware vSphere client et VMware vCenter, tout en explorant leurs différents services offerts. Nous avons également automatisé la migration dans le cas de panne ou de consommation excessive de ressources afin d'éviter les temps d'arrêt.

Nous avons aussi configuré notre accès distant sécurisé via le pare-feu qui travaille en collaboration avec notre serveur Radius Cisco ISE, Cette étape nous a permis de réaliser notre objectif de l'implémentation de la solution, et les résultats obtenus ont montré l'efficacité de notre conception.

Conclusion Générale

Conclusion Générale

L'étude réalisée a pour but de concevoir et d'implémenter une solution d'infrastructure réseau basée sur la virtualisation en formant un cloud privé et en offrant des services avec une couche d'automatisation de migration des services, ainsi que la sécurisation d'un accès distant.

Pour mettre en œuvre ce projet, nous avons été amenés dans un premier lieu à perfectionner nos connaissances dans les domaines, à savoir la virtualisation, le stockage, le réseau, la sécurité, l'automatisation et la migration. Pendant la réalisation, nous avons pu avoir un aperçu général sur les technologies les plus pertinentes du moment.

La mise en place de ce projet a été une occasion pour mieux comprendre d'une part le concept de la virtualisation et ses dérivées en l'implémentant, et pour aider d'autre part, les administrateurs grâce à l'automatisation des taches notamment la migration. Et de simplifier l'accès aux services via un VPN. Aussi, nous avons étudié l'existant au niveau de notre organisme d'accueil, nous avons fait des critiques ainsi que des propositions pour être à la hauteur du travail demandé. Afin d'accomplir ce projet, nous avons effectué une étude comparative entre les différents constructeurs de solutions et nous avons opté pour la solution mise en place par VMware pour les entreprises à savoir VMware vSphere comme hyperviseur et VMware vSAN pour le stockage partagé, le tout formant une infrastructure hyperconvergée.

Dans ce mémoire, nous avons présenté également les principaux outils, et les points importants concernant l'automatisation de migration, ainsi que la consommation des ressources.

Nous avons été amenés à mettre en place une plateforme de tests qui regroupe toutes ces technologies afin d'aboutir aux résultats voulus.

Enfin nous avons eu le plaisir de travailler sur un serveur Radius, responsable des authentifications et autorisations des utilisateurs au sein du réseau.

Bibliographie

[1] H.Noui, « Cloud Computing et Virtualization » chapitre 4, Université BATNA2 ,2016-2017.

[2] D.Oumar ,T. Hamadoun «Etude et Mise en place d'un réseau informatique sécurisé à l'hôpital de jour du centre Hospitalier Universitaire Sanou Souro de Bobo-Dioulasso» mémoire ,Université polytechnique DE BOBO-DIOULASSO(UPB) 2009-2010.

[3] L.SCHALKWIJK, «Cisco Commutation, routage et réseau sans-fil», ENI, 2022.

[4] W.Odom « CCNA 200-301 Official Cert Guide» Cisco Press ,2019.

[5] C.Hintz, CCIE® No. 15729 , C.OBEDIENTE, CCIE® No. 5620, O.KARAKOK, CCIE® No. 6331 «CISCO, CCNA Data Center DCICN 200-150. 2017». Cisco Press 800 East 96th Street Indianapolis, IN 46240, 2021.

[6] J.Raffre, all «Virtualisation et cloud open source» Copyright Smile, Edition décembre 2012.

[7] L.Berger , «La virtualisation des systèmes d'information» ,Mémoire de Bachelor, Haute Ecole de Gestion de Genève (HEG), 2012.

[8] A.Frikha, «Système de gestion des réseaux virtuels dans le contexte de l'informatique en nuage», Université du QUÉBEC À MO TRÉAL ,2015.

[9] G.Gauthey, all «Guide sur le Cloud Computing et les Datacenters à l'attention des collectivités locales» le portail de la direction générale des entreprises , 2015.

[10] K.Akila, «Migration de machine virtuelle en temps réel», mémoire, Faculté des sciences de l'ingénieur, 2018-2019.

[11] V.Remazeilles « La sécurité des réseaux avec Cisco», ENI, 2009.

[12] B.samira , C.zouina, «Étude de migration de l'infrastructure Hyper convergente», Mémoire ,Université de Bejaia, 2019/2020.

[13] Dr. D.Graziotin, «A Unified Open and Closed - Source Software Requirements Dataset», University of Stuttgart, 2021-2022.

[14] J.Musset, «Sécurité informatique ethical hacking», Edition ENI 2009.

[15] J.Frahim, all, «Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services» Cisco Press , 2014.

[16] N.Brookwood, «Comment l'hyperconvergence simplifie les choses et réduit les couts» ,Linsight, 2022.

[17] VMWARE, vSphere Storage Update 2, VMware vSphere 6.7, VMware ESXi 6.7, vCenter Server 6.7. VMware, Inc, 2019.

[18] V. MEDINA et J. M. GARCÍA, «A survey of migration mechanisms of virtual machines», ACM Computing Surveys (CSUR), t. 46, no 3, p. 1-33, 2014.

[19] J.Léon, «Histoire de l'automatisation des sciences du langage», ENS Edition, 2015.

[20] Adresse : http://www.vmware.com/fr/support.

[21] I.Lemagit, STORAGE,le magazine du stockage informatique professionnel. LEMAGIT, Inc, JUIN 2015.

[22] «Le livre blanc ; Pilotage réseaux passez a l'automatisation» ; Interdata, 2018.

[23] A.Woland , all, «Cisco ISE for BYOD and Secure Unified Access, 2nd» , Cisco Press, 2017.

Résumé

À travers les évolutions constantes, de nombreuses organisations ont privilégié les environnements virtualisés, tels que le Cloud, en raison de leurs avantages par rapport aux architectures traditionnelles. Ces dernières, soumises à des contraintes liées à des techniques éphémères d'exploitation de ressources, des coûts importants, et une complexité croissante des services, deviennent de plus en plus inacceptables. La virtualisation, notamment avec VMware, offre la possibilité de substituer les serveurs physiques par des terminaux légers, permettant une gestion centralisée et fine du datacenter, entraînant une réduction des coûts, une optimisation du système informatique, la haute disponibilité et plein d'autres avantages. Cependant, le concept de migration reste étroitement lié à la virtualisation, signalant la nécessité de migrer des machines virtuelles, des applications ou des services sans interruption. Même avec la virtualisation, les tâches manuelles persistent, représentant une charge quotidienne pour les administrateurs. Un autre enjeu a germé qui est la sécurité, en effet avec l'évolution des réseaux qui ne sont plus confinés, la mobilité des utilisateurs, le télétravail qui a explosé surtout après la pandémie mondiale covid-19, l'accès à distance aux services devient donc incontournable d'où la nécessité cruciale d'assurer une sécurité renforcée des accès. Dans ce contexte, notre projet de fin d'études vise à relever ces défis en proposant une infrastructure réseau virtualisée, un modèle hyperconvergé, et une solution de sécurité robuste. Cette approche conduit à la création d'un cloud privé offrant des services avec automatisation de la migration, haute disponibilité, et un accès sécurisé pour les utilisateurs mobiles. La sécurisation de l'accès distant est réalisée par la mise en place d'un VPN remote access, offrant authentification, confidentialité et intégrité des données. Cette solution repose sur le pare-feu de Cisco, assurant une implémentation intuitive et une gestion simplifiée des authentifications et des autorisations grâce à l'intégration avec un serveur Radius basé sur la solution Cisco ISE.

Mots clés : Virtualisation, Data Center, Services, Automatisation, Migration, Sécurité, accès distant.

Abstract

Throughout constant evolutions, many organizations have prioritized virtualized environments, such as the Cloud, due to their advantages over traditional architectures. The latter, subject to constraints related to ephemeral resource exploitation techniques, significant costs, and growing service complexity, are becoming increasingly unacceptable. Virtualization, particularly with VMware, offers the possibility of replacing physical servers within clients, enabling centralized and accurate management of the data center, resulting in cost reduction, system optimization, high availability, and many other benefits. However, the concept of migration remains closely linked to virtualization, highlighting the necessity of migrating virtual machines, applications, or services without interruption. Even with virtualization, manual tasks persist, representing a daily burden for administrators. Another emerging challenge is security; with the evolution of networks that are no longer confined, user mobility, and the trend to work remotely, especially after the global COVID-19 pandemic, remote access to services becomes essential, while enhancing security for access.

In this context, our final year project aims to address these challenges by proposing a virtualized network infrastructure, a hyper-converged model, and a robust security solution. This approach leads to the creation of a private cloud offering services with automated migration, high availability, and secure access for mobile users. Remote access security is achieved through the implementation of a remote access VPN, providing authentication, confidentiality, and data integrity. This solution relies on Cisco firewall, ensuring intuitive implementation and simplified management of authentications and authorizations through integration with a Radius server based on Cisco ISE solution.

Keywords: Virtualization, Data Center, Services, Automation, Migration, Security, Remote Access.