République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master en Informatique.
Option : Adminstration et Sécurité des Réseaux.

Thème

Étude et mise en place d'une solution de virtualisation (Cas d'étude : Entreprise Cevital de Béjaïa)

Réalisé par :
Mlle . ZIANE Nadjet

Devant le jury composé de :

Président	**Dr. ALOUI Soraya**	**U. A/Mira Béjaïa.**
Examinateur	**Dr. MOHAMMEDI Mohamed**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. MEHAOUED Kamal**	**U. A/Mira Béjaïa.**

juin 2023

Remerciements

Tout d'abord, je souhaite exprimer ma gratitude envers Dieu le tout-puissant de m'avoir accordé le courage, la force et la patience nécessaires pour accomplir cette humble tâche. Je tiens à remercier chaleureusement Monsieur M. KAMEL pour son encadrement et ses précieux conseils. J'exprime également de plus vive reconnaissance envers l'ensemble du personnel de l'entreprise Cevital, notamment l'équipe du service Informatique, pour le temps qu'ils ont consacré, leurs directives précieuses et la qualité de leur suivi tout au long de mon stage. Aux membres du jury, nous tenons à vous adresser nos sincères remerciements d'avoir accepté d'évaluer mon travail avec bienveillance.

Dédicace

Je dédie ce modeste travail à :

À mon père qui m'a toujours soutenu dans mes choix, en particulier en ce qui concerne mes études, grâce à sa présence, son sérieux et ses précieux conseils, j'ai pu atteindre où je suis aujourd'hui. Papa, tu es toujours là-derrière moi, et je ne saurais jamais assez te remercier pour tout ce que tu fais pour moi. Merci du fond du cœur.

À ma chère maman, qui ne cesse de me pousser encore plus loin, qui s'est sacrifiée pour moi et a toujours su m'épauler et me soutenir dans les moments difficiles, j'espère être à la hauteur de tes attentes, maman. Je t'aime.

À ma sœur Mounira, malgré la distance qui nous sépare, tu m'as beaucoup aidé et soutenu à ta manière, et tu restes un modèle à suivre pour la réalisation de mes projets professionnels. Je t'adore, chère sœur.

À mes frères et sœurs (Chafika, Lamia, Lila, Chabha et Messade), qui sont également loin, je vous remercie infiniment pour vos encouragements et vos conseils.

À toute ma famille, qui ne cesse de m'encourager au quotidien, je vous remercie, mes oncles, tantes et cousins(es).

À mes chères amies Kahina, Meriem, Rima, Nadjette et Lidia, qui m'ont véritablement épaulé, je n'oublierai jamais votre aide et votre soutien. Merci.

Ziane Nadjet.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AD	Active Directory
CMD	command prompt l'invite de commandes
DHCP	Dynamique Host Configuration Protocole
DNS	Demain Name Système
FTP	File Transfer Protocol (protocol de transfer de fichier)
HTTP	Hypertexte Transférè Protocole
IP	Internet Protocole
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NetBIOS	Network Basic Input Output System
OSI	Open Systems Interconnection
RAM	la mémoire vive Random Access Memory
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VM	virtual machines
Vmnic	Les cartes réseau physiques au niveau de l'hyperviseur.
vSwitch	virtual Switch. Un commutateur réseau standard
WAN	Wide Area Network

Introduction générale

Depuis les années 50, les entreprises ont adopté un système d'unités centrales de plus en plus complexe et en constante évolution pour traiter leurs données. Au début, ces unités centrales étaient massives et coûtaient cher.

Aujourd'hui, les entreprises sont confrontées au défi constant de devoir fournir davantage de services chaque année, tout en disposant de budgets réduits. Les systèmes informatiques des entreprises doivent donc être suffisamment flexibles et réactifs pour répondre efficacement aux exigences des métiers, qui sont la source de revenus de l'entreprise.
Les avancées technologiques de ces dernières années ont entraîné de grandes innovations dans le domaine des sciences informatiques. Celles-ci ont poussé les entreprises à effectuer d'importantes restructurations au sein de leurs structures et de leurs différentes infrastructures réseau.

Malgré la mise en place de techniques de réduction des coûts dans les réseaux informatiques, cela engendre de grandes contraintes en termes de gestion et de maintenance. Les administrateurs de ces réseaux sont confrontés à des défis majeurs pour appréhender les techniques de consolidation instaurées par les différentes entreprises.

Face à ces multiples problèmes auxquels sont souvent confrontés les administrateurs de systèmes informatiques, plusieurs méthodes ont été mises en place pour faciliter l'administration. Parmi ces méthodes, la virtualisation des serveurs est devenue une base essentielle, qui constitue également le sujet de notre étude. Il existe plusieurs approches de virtualisation, chacune offrant une convivialité particulière en ce qui concerne la manière dont elle est appréhendée par les administrateurs de systèmes informatiques[21][22].

Il est vrai que les avantages de cette technologie sont nombreux en termes de productivité, de coûts et d'exploitation.

La virtualisation permet de créer des environnements virtuels qui regroupent plusieurs machines virtuelles sur un seul serveur physique, ce qui permet une meilleure utilisation des ressources matérielles et une réduction des dépenses liées à l'infrastructure. Dans cette optique, cette étude se concentre sur l'implémentation d'une solution COMPUTING sur une infrastructure de virtualisation, en mettant l'accent sur les avantages, les défis et les considérations clés pour garantir une mise en œuvre réussie.

Ce mémoire est organisé en quatre chapitres :

Le premier chapitre, sera consacré sur Généralité des Réseaux et la Sécurité informatique

Le deuxième chapitre nous traite une introduction à la virtualisation

Dans **Le troisième**, est consacré à Présentation de l'organisme d'accueil

Le quatrième chapitre, sera consacré à la partie pratique de mon travail, dans laquelle nous défini les différentes configurations, réalisation et test.

Nous finalisons par une conclusion générale dans laquelle nous allons citer nos acquis durant la réalisation de notre projet.

Chapitre 1

Généralité sur les Réseaux et la Sécurité informatique

1.1 Introduction

les réseaux et la sécurité informatique sont deux domaines étroitement liés qui jouent un rôle essentiel dans la protection des systèmes informatiques et de l'information qu'ils contiennent. Les entreprises, les organisations et les individus doivent comprendre les risques et les mesures de protection appropriées pour garantir la sécurité de leurs systèmes informatiques.

Dans ce chapitre, j'ai abordé des notions théoriques essentielles en matière de réseaux et de sécurité informatique. j'ai débuté par la définition du concept de réseau informatique, pour ensuite, j'ai penché sur les modèles OSI et TCP/IP. En outre, j'ai discuté de la définition de la sécurité informatique, ainsi que des attaques potentielles et des mécanismes de défense associés.

1.2 GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUE

1.2.1 Qu'est-ce qu'un réseau informatique

Un réseau informatique est constitué d'une collection d'équipements tels que des ordinateurs portables ou fixes, des routeurs, des commutateurs, et d'autres dispositifs similaires, qui sont situés à des endroits éloignés les uns des autres. Ces équipements sont interconnectés par des liens filaires (câbles) ou sans fil, ce qui permet aux utilisateurs de partager des ressources matérielles et logicielles. Le partage de ces ressources peut inclure des fichiers, des imprimantes, des bases de données, des connexions Internet et bien plus encore.

1.2.2 Objectifs des réseaux informatiques

Les réseaux informatiques ont plusieurs objectifs, notamment :

1. **Le partage de ressources :** Les réseaux permettent de partager des ressources telles que des fichiers, des imprimantes, des connexions Internet, des logiciels, etc. Cela permet une utilisation plus efficace des ressources et réduit les coûts.
2. **La communication :** Les réseaux facilitent la communication entre les utilisateurs et les dispositifs connectés. Les utilisateurs peuvent échanger des informations en temps réel, collaborer sur des projets et communiquer par voie électronique.
3. **La centralisation de la gestion :** Les réseaux permettent la centralisation de la gestion des ressources et des utilisateurs. Les administrateurs système peuvent gérer l'accès aux ressources, assurer la sécurité du réseau et mettre à jour les logiciels depuis une seule et même interface.

1.2.3 Classification d'un réseau informatique

Il existe plusieurs façons de classer les réseaux informatiques en fonction de leur taille, de leur portée géographique et de leur architecture. Voici les principales classifications :

1. **Un réseau local (Local Area Network, ou LAN en anglais)** est un réseau informatique qui relie des ordinateurs, des périphériques et des ressources sur une zone géographique limitée, telle qu'un bureau, une entreprise, une école ou un foyer. Les LAN sont généralement privés et permettent aux utilisateurs de partager des fichiers, des imprimantes, des connexions Internet et d'autres ressources.[1]

Deux modes de fonctionnement peuvent être distingués :

— Dans un environnement "peer-to-peer", il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire.

— Dans un environnement "serveur/client", un ordinateur central fournit des services réseau aux utilisateurs.

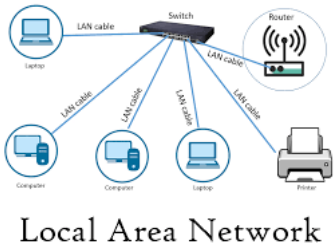


FIGURE 1.1 – Local Area Network [23]

2. **Un réseau étendu de zone métropolitaine (Métropolitain Area Network ou MAN en anglais)** est un type de réseau informatique qui couvre une zone géographique plus grande qu'un réseau local (LAN), mais plus petite qu'un réseau étendu (WAN). Les MAN connectent souvent plusieurs LANs situés dans des zones géographiques voisines, tels que des bâtiments d'une même entreprise ou des campus universitaires.[1]

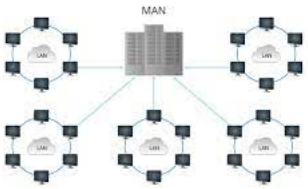


FIGURE 1.2 – Un réseau étendu de zone métropolitaine MAN[24]

Les MAN peuvent être utilisés pour fournir des services de communication rapides et fiables pour les entreprises, les organisations gouvernementales et les établissements d'enseignement situés dans une zone métropolitaine. Ils peuvent également être utilisés pour fournir des services de collectivité pour les fournisseurs d'accès Internet dans les zones urbaines.

3. **Un réseau étendu (Wide Area Network, ou WAN en anglais)** est un réseau informatique qui couvre une grande zone géographique, comme un pays, un continent ou même le monde entier. Les WAN connectent souvent plusieurs réseaux locaux (LAN) ou réseaux de zone métropolitaine (MAN) situés dans des zones géographiques éloignées.[1]

FIGURE 1.3 – Un réseau étendu WAN[25]

Les WAN peuvent être utilisés pour fournir des services de communication rapides et fiables pour les entreprises, les organisations gouvernementales, les établissements d'enseignement et les fournisseurs

d'accès Internet situés dans des zones géographiques éloignées. Les WAN peuvent également être utilisés pour connecter des centres de données, des succursales d'entreprises, des centres de recherche et des sites de production.

1.2.4 Les alternatifs de raccordements

1. **Les topologies Physique :**On distingue :

   (a) **TOPOLOGIE EN BUS :**La topologie en bus est un type de configuration de réseau dans lequel tous les périphériques sont connectés à une même ligne physique, appelé bus. Dans cette configuration, tous les périphériques partagent la même bande passante et communiquent en utilisant un protocole de communication commune. Dans l'ensemble, la topologie en bus est une méthode simple et peu coûteuse pour connecter des périphériques dans un réseau local. Cependant, elle peut ne pas être la meilleure solution pour les grands réseaux ou ceux qui nécessitent une haute disponibilité.

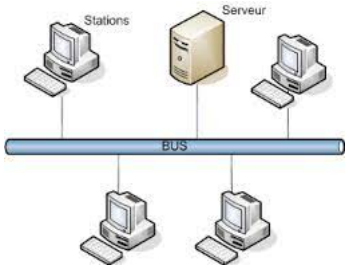


FIGURE 1.4 – Topologie en bus[26]

   (b) **TOPOLOGIE EN ANNEAU (RING) :** La topologie en anneau (ou Ring) est un type de configuration de réseau dans lequel tous les périphériques sont connectés les une aux autres pour former une boucle fermée. Dans cette configuration, les données sont transmises de nœud en nœud dans une direction unidirectionnelle autour de l'anneau jusqu'à ce qu'elles atteignent leur destination. Dans l'ensemble, la topologie en anneau est une méthode efficace pour connecter des périphériques dans un réseau local. Cependant, elle peut ne pas être la meilleure solution pour les grands réseaux ou ceux qui nécessitent une haute disponibilité.

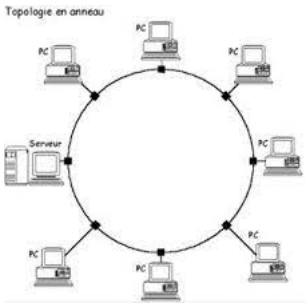


FIGURE 1.5 – Topologie en anneau[27]

   (c) **TOPOLOGIE EN ÉTOILE :** La topologie en étoile est un type de configuration de réseau dans lequel tous les périphériques sont connectés à un point central, souvent appelé concentrateur ou commutateur. Dans cette configuration, tous les périphériques communiquent avec le concentrateur, qui achemine les données vers leur destination. Dans l'ensemble, la topologie en étoile est une méthode efficace pour connecter des périphériques dans un réseau local et est largement utilisée dans les entreprises et les environnements professionnels. Elle offre une grande flexibilité et facile à gérer et est adaptée aux réseaux de toutes tailles.

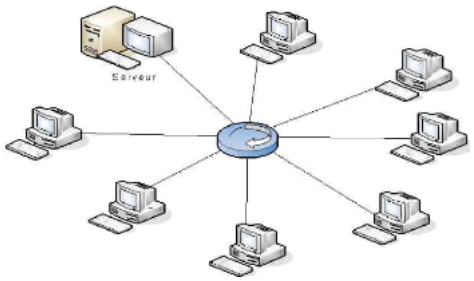


FIGURE 1.6 – Topologie en étoile[28]

(d) **TOPOLOGIES EN ARBRE** est un type de configuration de réseau qui combine les caractéristiques de la topologie en étoile et en bus. Dans cette configuration, les périphériques sont connectés à un nœud central appelé nœud racine, qui agit comme un point central pour la transmission de données. Les nœuds racines sont à leur tour connectés entre eux pour former une structure en arbre. Dans l'ensemble, la topologie en arbre est une option efficace pour les grandes entreprises et les organisations qui nécessitent un réseau de grande envergure. Elle offre une grande flexibilité et permet une gestion efficace du trafic de données, mais nécessite une planification minutieuse et peut-être plus coûteuse que d'autres topologies.

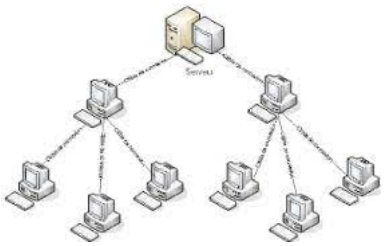


FIGURE 1.7 – Topologie en arbre[29]

2. **Les équipements physiques**

(a) **les terminaux (carte réseau @ MAC)** C'est une carte qui s'installe à l'intérieur de l'ordinateur. Elle constitue l'interface entre l'ordinateur et le câble du réseau, dont le rôle est de préparer et contrôler l'envoi de données sur le réseau. Les cartes possèdent par fois deux types de prises à l'arrière, RJ45 ou BNC, les prises BNC sont faites pour y connecter un câble coaxial, les prises RJ45 reçoivent les câbles à paire torsadée.

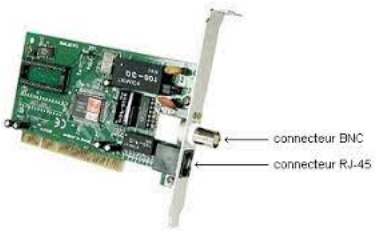


FIGURE 1.8 – Carte réseau[30]

(b) **Les équipements d'interconnexion :** Les équipements d'interconnexion sont des dispositifs qui permettent la connexion entre les différents segments d'un réseau. Ils assurent la communication entre les différents périphériques connectés au réseau. Voici quelques-uns des équipements d'interconnexion les plus couramment utilisés dans les réseaux :

— **Les commutateurs (Switch)** : ils sont utilisés pour connecter des ordinateurs et d'autres périphériques en utilisant des câbles Ethernet.

FIGURE 1.9 – Les Switch[31]

— **Concentrateur (hub)** : Appareil relié à plusieurs machines en réseau, et permettant de concentrer les données pour les transmettre par un unique canal

FIGURE 1.10 – Concentrateur (hub)[32]

— **Les routeurs (routeurs)** : Ils permettent la connexion entre différents réseaux, tels que l'Internet ou des réseaux d'entreprise.

FIGURE 1.11 – Le routeur[33]

— **Les pare-feux (firewalls)** : Ils sont utilisés pour sécuriser les réseaux en empêchant les accès non autorisés et les attaques de hackers. Les pare-feux peuvent être logiciels ou matériels.

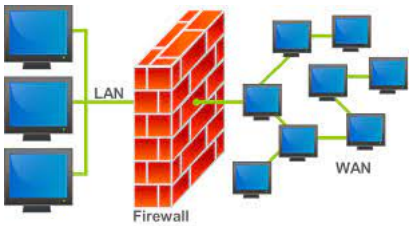


FIGURE 1.12 – Le Par-feu[34]

— **Les passerelles (gateways)** : Ils permettent la communication entre des réseaux différents, tels que la communication entre un réseau local et un réseau étendu. Les passerelles peuvent être des dispositifs matériels ou des programmes logiciels.

— **Les contrôleurs de domaine (domain controllers)** : Ils sont utilisés pour gérer les comptes d'utilisateur, les mots de passe et les permissions sur les réseaux d'entreprise. Les contrôleurs de domaine sont généralement utilisés avec des annuaires LDAP (Lightweight Directory Access Protocol).

FIGURE 1.13 – Les contrôleurs de domaine[35]

(c) **Les supports de transmission** Les supports de transmission sont les différents moyens physiques utilisés pour transmettre des données ou des signaux entre différents équipements de communication. Les supports de transmission les plus courants sont :

— **Le câble coaxial** est Les signaux électriques à haute fréquence, qu'il s'agisse de signaux audio, vidéo ou de données, sont transmis via un type de câble appelé câble coaxial.

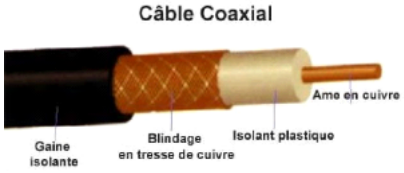


FIGURE 1.14 – câble coaxial[36]

— **Une paire torsadée** est un câble composé de deux fils de cuivre isolés torsadés ensemble pour former une paire. Ce type de câble est utilisé pour transmettre des signaux électriques basse fréquence, tels que des signaux téléphoniques, de données et de réseau.

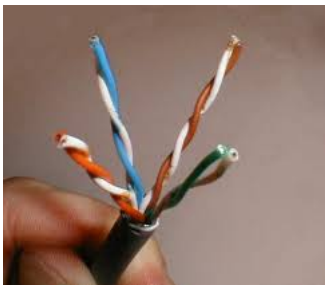


FIGURE 1.15 – Une paire torsadée[37]

— **Câble à Fibre optique**s sont des fils de verre très minces et très transparents, qui sont capables de transmettre des signaux lumineux à une vitesse très élevée et avec une qualité de transmission exceptionnelle sur de longues distances.

FIGURE 1.16 – Câble à Fibre optique[38]

1.2.5 Les modèles des références

1. **le modèle de référence OSI :**

   Le modèle OSI (Open Systems Interconnection) est un modèle de référence pour les réseaux informatiques. Il a été développé par l'ISO (Organisation internationale de normalisation) dans les années 1980 pour fournir une base commune pour la conception de réseaux ouverts [3].

   Le modèle OSI est souvent utilisé comme base pour la conception et la mise en œuvre de réseaux informatiques. Cependant, dans la pratique, de nombreux réseaux utilisent des protocoles qui ne correspondent pas exactement au modèle OSI, ou utilisent des versions simplifiées du modèle. Le modèle OSI se compose de sept couches, chacune étant responsable de fonctions spécifiques dans la transmission de données. Les couches sont les suivantes :[5]

Couche du modèle OSI	Description
1 - Physique	cette couche est responsable de la transmission des données brutes sur le support physique, tel que le câble ou la fibre optique.
2 - Liaison de données	cette couche est responsable de la gestion des erreurs de transmission et de l'acheminement des données sur le support physique.
3 - Réseau	cette couche est responsable du routage des données entre différents réseaux.
4 - Transport	cette couche est responsable de la fiabilité de la transmission des données entre deux points finaux.
5 - Session	cette couche est responsable de l'établissement, de la gestion et de la fin des sessions de communication entre deux applications.
6 - Présentation	cette couche est responsable de la représentation et de la conversion des données pour que les applications puissent les comprendre.
7 - Application	cette couche est responsable de la communication entre les applications et l'utilisateur final.

TABLE 1.1 – Modèle OSI
[5]

2. **Le modèle de référence TCP/IP :** Le modèle TCP/IP adopte une approche modulaire similaire à celle du modèle OSI, mais se compose uniquement de quatre couches. Ces couches ont des fonctions plus diverses car elles correspondent à plusieurs couches du modèle OSI. Les rôles des différentes couches sont les suivants, [3][4] :

La couche d'accès réseau : elle spécifie la manière dont les données doivent être acheminées, indépendamment du type de réseau utilisé, [3][4].

La couche Internet : elle est responsable de l'acheminement et du routage des données [2].

La couche de transport : elle fournit le paquet de données (datagramme) ainsi que les mécanismes nécessaires pour suivre l'état de la transmission. Les deux principaux protocoles utilisés pour les services de cette couche sont les suivants [2] :

TCP : il s'agit d'un protocole fiable qui garantit une communication sans erreur en utilisant un mécanisme de question/réponse, de confirmation et de synchronisation (orienté connexion).[7] **UDP :** il s'agit d'un protocole non fiable qui permet une communication rapide, mais qui peut contenir des erreurs en utilisant un mécanisme de question/réponse (sans connexion). La couche d'application : elle regroupe les applications standards du réseau [2]. L'acheminement des données entre l'émetteur et le récepteur au travers de différents réseaux se fait dans la couche réseau.

1.2.6 Adressage IP

L'adressage IP est un système d'identification et de localisation des ordinateurs et des périphériques sur un réseau informatique. Chaque appareil sur un réseau se voit attribuer une adresse IP unique, qui est une série de nombres décimaux séparés par des points.[6] Il existe deux versions principales du protocole IP : IPv4 et IPv6. IPv4 utilise des adresses 32 bits, ce qui limite le nombre d'adresses utilisables à environ quatre milliards. Cette limitation est devenue un problème avec l'augmentation d'Internet et du nombre d'appareils connectés. IPv6 utilise des adresses 128 bits, permettant plus d'adresses utilisables.

La notation CIDR et VLSM :

La notation CIDR (Classless Inter-Domain Routing) et le VLSM (Variable Length Subnet Masking) sont des approches permettant de fragmenter des réseaux de manière plus précise [6].

1. **La notation CIDR :** est une technique qui permet de représenter une adresse IP en y ajoutant un préfixe qui indique la longueur du réseau. Ce préfixe permet de déterminer le nombre de bits qui sont utilisés pour identifier le réseau dans l'adresse IP.
   Par exemple, une adresse IP avec un préfixe de /24 signifie que les 24 premiers bits de l'adresse sont réservés pour identifier le réseau, tandis que les 8 derniers bits sont utilisés pour identifier les hôtes.
   L'utilisation de cette méthode permet une allocation plus précise des adresses IP et une optimisation de l'utilisation des adresses disponibles.
2. **La notation VLSM :** est une technique qui permet de diviser un réseau en sous-réseaux de tailles variables, afin d'utiliser efficacement les adresses IP disponibles.
   Cette méthode est particulièrement utile pour les réseaux de taille moyenne à grande, où il est nécessaire de créer plusieurs sous-réseaux pour organiser les différents groupes d'utilisateurs ou de services.

1.3 la sécurité des réseaux informatique

1.3.1 Définition de la sécurité

La sécurité informatique est un domaine qui vise à protéger les systèmes informatiques et les données qu'ils contiennent contre les menaces internes et externes, telles que les attaques malveillantes, les virus, les logiciels malveillants, les pirates informatiques et les erreurs humaines. Elle comprend l'utilisation de diverses techniques, méthodes et outils pour prévenir, détecter et répondre aux incidents de sécurité informatique, ainsi que pour assurer la continuité des opérations et la récupération en cas de sinistre. La sécurité informatique est donc essentielle pour protéger la confidentialité, l'intégrité et la disponibilité des informations et des ressources informatiques.[8][20]

1.3.2 Terminologie de la sécurité

Voici quelques termes courants utilisés dans le domaine de la sécurité informatique :

1. **Pare-feu (Firewall) :** est un dispositif matériel ou logiciel qui contrôle le trafic réseau entrant et sortant d'un réseau.
2. **Authentification :** est le processus permettant de vérifier l'identité d'un utilisateur, d'un système ou d'une entité. Cela peut impliquer l'utilisation de mots de passe, de certificats numériques, de cartes à puce ou d'autres mécanismes d'identification.
3. **Vulnérabilité :** est une faiblesse ou une faille dans un système, une application ou un réseau qui peut être exploitée par un attaquant pour compromettre la sécurité. Les vulnérabilités peuvent résulter de défauts de conception, de bugs logiciels ou de mauvaises configurations.

1.3.3 Principe de la sécurité informatique

Les principes de la sécurité informatique sont les suivants :

1. **Confidentialité :** garantir que les informations ne soient accessibles qu'aux personnes autorisées.[20]
2. **Intégrité :** garantir que les informations ne soient pas modifiées ou altérées par des personnes non autorisées.[20]
3. **Disponibilité :** garantir que les informations soient disponibles en tout temps pour les personnes autorisées.[20]
4. **Authenticité :** garantir l'identité et la véracité des informations et des personnes qui y ont accès.[20]
5. **Non-répudiation :** garantir qu'une personne ne puisse nier avoir effectué une action ou avoir pris une décision.[20]

1.3.4 Attaque

1. **Définition d'une attaque :** Une attaque informatique est une action malveillante visant à exploiter une vulnérabilité ou une faiblesse dans un système informatique ou un réseau afin de compromettre la sécurité de ce système et d'y accéder, le perturber ou le détruire. Les attaques peuvent être menées par des individus mal intentionnés, des groupes organisés ou des États. Les attaques informatiques peuvent causer des pertes financières, des atteintes à la réputation, des violations de la vie privée et des perturbations de la vie quotidienne.[12]
2. **Les Types d'attaques :** Il existe plusieurs types d'attaques dans les réseaux informatiques. Voici quelques exemples courants :
   (a) **Attaques par déni de service (DOS) :** Ces attaques visent à rendre un service ou un système indisponible en submergeant les ressources du réseau ou du serveur ciblé, ce qui empêche les utilisateurs légitimes d'accéder aux services.
   (b) **Attaques par force brute :** Dans ce type d'attaque, un attaquant tente de deviner les identifiants d'accès en essayant différentes combinaisons de mots de passe jusqu'à ce qu'il en trouve un qui fonctionne.
   (c) **Attaques par hameçonnage (phishing) :** Les attaques de phishing impliquent l'utilisation de courriers électroniques, de sites web ou de messages instantanés trompeurs pour inciter les utilisateurs à divulguer des informations sensibles, telles que des mots de passe ou des numéros de carte de crédit.
   (d) **Attaques par injection SQL : :** Ces attaques exploitent les vulnérabilités des applications web pour injecter des commandes SQL malveillantes dans les requêtes de la base de données, ce qui peut permettre à un attaquant de manipuler les données ou d'accéder à des informations sensibles.
   (e) **Attaques par débordement de tampon (buffer Overleaf) :** Ces attaques exploitent une vulnérabilité dans un programme en envoyant des données excessives qui débordent la mémoire tampon, ce qui peut entraîner une exécution de code non autorisée ou un crash du système.

(f) **Attaques par interception de données (sniffing) :** Ces attaques consistent à intercepter et à surveiller le trafic réseau afin d'intercepter des informations sensibles telles que les identifiants d'accès ou les données confidentielles.

(g) **Attaques par injection de code malveillant :** Ces attaques consistent à injecter du code malveillant, tel que des virus, des vers ou des chevaux de Troie, dans un système ou un réseau afin d'endommager ou de compromettre les ressources ciblées.

1.3.5 Mécanisme de défense

1. **Antivirus :** est un logiciel de sécurité informatique qui a pour but de protéger les ordinateurs et les réseaux contre les virus, les logiciels malveillants et les menaces en ligne. L'antivirus utilise des techniques de détection pour identifier les virus connus et inconnus. Les techniques de détection incluent la comparaison de signatures de virus, l'analyse comportementale et la détection basée sur l'apprentissage automatique. L'antivirus peut également offrir d'autres fonctionnalités de sécurité, telles que la protection en temps réel, les pare-feux intégrés, la protection contre les logiciels espions et la vérification des e-mails et des pièces jointes.
2. **Chiffrement :** est une technique de sécurité informatique qui permet de protéger les données en les transformant en un format illisible pour toute personne qui n'a pas la clé de déchiffrement appropriée. Le chiffrement est utilisé dans de nombreux domaines, notamment pour protéger les communications en ligne, les transactions bancaires, les données personnelles et les fichiers sensibles. Il existe deux types de chiffrement :[11]
   - '**Le chiffrement symétrique :** utilise la même clé pour le chiffrement et le déchiffrement des données. Cette méthode est rapide et efficace, mais elle nécessite une transmission sécurisée de la clé pour éviter qu'elle ne soit interceptée par des tiers malveillants.
   - **Le chiffrement asymétrique :** utilise deux clés différentes : une clé publique pour le chiffrement des données et une clé privée correspondante pour le déchiffrement. Cette méthode est plus sécurisée, car la clé privée est gardée secrète et ne doit pas être transmise sur le réseau.[3][3.1]
3. **Pare-feu :** Un pare-feu est un dispositif matériel ou logiciel de sécurité informatique qui surveille et contrôle le trafic réseau entrant et sortant d'un système ou d'un réseau. Le pare-feu est conçu pour protéger le système ou le réseau contre les attaques provenant d'Internet ou d'autres réseaux, en filtrant le trafic en fonction de règles de sécurité prédéfinies. Le pare-feu peut également être utilisé pour restreindre l'accès à certaines ressources réseau ou applications en fonction des politiques de sécurité de l'organisation.
4. **Proxy :** est un serveur intermédiaire qui permet à un utilisateur ou à un groupe d'utilisateurs de se connecter à Internet de manière anonyme ou en utilisant une adresse IP différente de celle de leur réseau local. Le proxy agit comme un intermédiaire entre l'utilisateur et les sites Web qu'il visite, en transférant les requêtes de l'utilisateur vers les sites Web et en retournant les réponses des sites Web à l'utilisateur. Le proxy peut être configuré pour filtrer le trafic réseau en bloquant l'accès à certains sites Web ou en restreignant l'accès à certaines ressources réseau. Le proxy peut également être utilisé pour accélérer l'accès à Internet en mettant en cache les pages Web fréquemment consultées.
5. **Système de détection d'intrusion (IDS - Intrusion Detection System) :** est un outil de sécurité informatique conçu pour détecter les activités suspectes ou malveillantes sur un réseau ou un système informatique. L'IDS peut être déployé sous forme de logiciel sur un ordinateur ou sous forme de dispositif matériel sur un réseau. Il peut fonctionner de deux manières :
   - Dans le mode réseau : l'IDS surveille le trafic entrant et sortant sur un réseau et analyse les paquets de données à la recherche de signes d'activité malveillante.
   - Dans le mode hôte, l'IDS surveille l'activité sur un seul ordinateur et détecte les tentatives d'intrusion ou de compromission.

6. **Système de prévention d'intrusion (IPS - Intrusion Prévention System) :** est un outil de sécurité informatique qui surveille le trafic réseau pour détecter les tentatives d'intrusion et empêcher les attaques avant qu'elles ne réussissent.
   L'IPS fonctionne de manière similaire à un système de détection d'intrusion (IDS), mais il dispose en plus de la capacité de bloquer le trafic malveillant en temps réel.
   Lorsqu'une activité suspecte est détectée, l'IPS peut bloquer le trafic malveillant en temps réel pour empêcher une attaque réussie. Il peut également être configuré pour générer des alertes pour informer les administrateurs du système ou les équipes de sécurité de l'activité suspecte.

1.4 Conclusion

Dans ce chapitre, quelques notions de bases sur les réseaux informatiques ont été présentés, à savoir la définition des réseaux, ses différents types et leurs topologies. Nous avons vu le modèle de référence OSI et le modèle TCP/IP, Nous avons également examiné la question de la sécurité des réseaux informatiques, en résumant diverses informations sur les attaques et en présentant des mécanismes de défense essentiels. Dans le chapitre suivant, nous allons proposer quelques introductions sur la virtualisation.

Chapitre 2

INTRODUCTION À LA VIRTUALISATION

2.1 Introduction

Ces dernières années, l'informatique a connu un développement considérable, ce qui a poussé les entreprises à développer leurs datacenter. Cela a entraîné une augmentation du nombre de serveurs physiques, ainsi qu'une hausse du budget, de la consommation d'énergie et du personnel de maintenance. Heureusement, grâce à la virtualisation, les entreprises peuvent faire face à des besoins supplémentaires en termes d'infrastructure sans avoir besoin d'un ordinateur supplémentaire à chaque fois qu'elles veulent mettre en place un nouveau serveur. En effet, elles peuvent simplement démarrer un nouveau système d'exploitation. De plus, un système invité peut être dédié à une application unique et il peut être différent du système d'exploitation hôte. Les fonctionnalités telles que la virtualisation de stockage permet de déplacer les systèmes invités sans interruption de l'activité, exploitant ainsi au mieux le matériel informatique disponible.

La virtualisation est devenue une solution d'entreprise permettant de réduire le nombre de serveurs physiques tout en augmentant le nombre de serveurs virtuels sur chaque serveur physique, en vue d'optimiser leur utilisation, de réduire les dépenses sur le matériel serveur, de diminuer la consommation électrique, ainsi que de libérer beaucoup d'espace dans les salles serveur et de faciliter l'administration du système informatique. Dans cette étude théorique, nous explorerons l'histoire de la virtualisation, ses types, son impact sur les entreprises et ses avantages. Nous examinerons également les différents types d'hyperviseurs existants.

2.2 Le modèle en couches des systèmes d'informations

La représentation dans les systèmes d'information comporte un minimum de quatre niveaux selon les principes sous-jacents. La figure ci-dessous montre les quatre strates de systèmes d'information, dispersées dans le diagramme.[13]

2.2.1 Couche infrastructure

L'infrastructure informatique est l'ensemble des ressources et équipements informatiques utilisés pour stocker, traiter, gérer et transmettre des données et des informations dans une entreprise ou une organisation. Il comprend des éléments matériels tels que des ordinateurs, des serveurs, des routeurs, des commutateurs, des câbles, des périphériques, des périphériques de stockage et des dispositifs de sécurité, ainsi que des éléments logiciels tels que des systèmes d'exploitation, des applications, des bases de données et des outils de gestion.[13]

1. **Les équipements de sécurités :**
   Pare-feu : Un pare-feu, également connu sous le nom de firewall en anglais, est un système de protection pour les ordinateurs ou les réseaux d'ordinateurs contre les intrusions provenant d'un autre réseau tel qu'Internet. Le pare-feu agit comme une passerelle filtrante en contrôlant les paquets de données échangés avec le réseau.

Il est configuré pour filtrer au minimum les interfaces réseau suivantes :

— Une interface pour le réseau à protéger (réseau interne).

— Une interface pour le réseau externe.

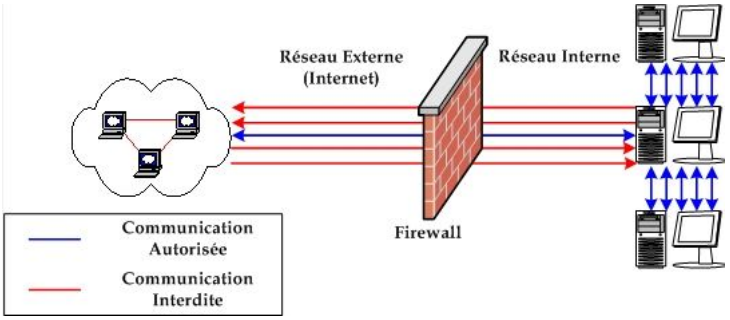


FIGURE 2.1 – Le fonctionnement d'un pare-feu[39]

2. **Les serveurs** : Un serveur informatique est un ordinateur dédié à la fourniture de services et de ressources à d'autres ordinateurs ou périphériques sur un réseau. Les serveurs sont conçus pour être robustes, fiables et puissants, et ils sont généralement équipés de matériel et de logiciels spécifiques pour répondre aux besoins des utilisateurs.[13]
   Les déférents types de serveurs :
   — Serveurs de fichiers
   — Serveurs d'impression
   — Serveurs d'applications
   — Serveurs DNS
   — Serveurs de messagerie
   — Serveurs de bases de données
   — Serveurs web
   — Serveurs virtuels
   — Serveurs proxy
   — Serveurs de supervision et d'administration
3. **Le rôle de la virtualisation :** La virtualisation joue un rôle important dans les entreprises en offrant une solution efficace pour gérer l'infrastructure informatique et répondre aux besoins des utilisateurs. Voici quelques-uns des rôles clés de la virtualisation dans les entreprises :[14]
   (a) Consolidation des serveurs.
   (b) Gestion des environnements de test et de développement.
   (c) Réduction des temps d'arrêt.
   (d) Isolation des environnements.
   (e) Utilisation efficace des ressources.

2.2.2 Couche Opérationnelle

La couche opérationnelle est la couche la plus basse du modèle hiérarchique de l'architecture d'un système d'information. Elle est responsable de la gestion des transactions quotidiennes de l'entreprise et de la collecte des données pour les autres couches du système. Les systèmes opérationnels sont conçus pour soutenir les processus opérationnels et sont généralement basés sur des bases de données relationnelles et des applications transactionnelles. Le choix de ne pas mettre en cache les informations de la couche métier repose sur plusieurs raisons. Tout d'abord, cette couche est souvent dynamique, ce qui signifie qu'elle ne peut pas être préalablement mise en cache. Ensuite, les utilisateurs attendent des réponses rapides de la couche opérationnelle. Ils souhaitent pouvoir dessiner rapidement, envoyer des informations détaillées en un seul clic de souris et visualiser les fonctions de manière précise. Enfin, la couche opérationnelle doit utiliser le même système de coordonnées que le service de fond de carte. Cette condition est essentielle pour éviter les superpositions et les problèmes de performance, ainsi que pour prévenir les erreurs dans les applications SIG Web. [14][15]

2.2.3 Couche Applicative

est la couche intermédiaire du modèle hiérarchique de l'architecture d'un système d'information. Elle est responsable de la gestion des processus métier et de la fourniture de services aux utilisateurs finaux. Elle utilise les données collectées par la couche opérationnelle pour soutenir les processus métier de l'entreprise. Les applications de cette couche sont souvent développées sur mesure pour répondre aux besoins spécifiques de l'entreprise et peuvent être exécutées sur des serveurs locaux ou sur le cloud. [14]

2.2.4 Couche décisionnelle

L'informatique décisionnelle (en anglais business intelligence (BI) 1 ou décision support système (DSS)). Elle est responsable de la création de rapports, d'analyses et de la prise de décision stratégique pour l'entreprise. Elle utilise les données collectées par la couche opérationnelle et traitées par la couche applicative pour fournir des informations de haut niveau pour la prise de décision. Les applications de cette couche sont conçues pour fournir des analyses et des rapports aux cadres de l'entreprise pour les aider à prendre des décisions éclairées.[14]

2.3 La virtualisation

2.3.1 la Définition de la virtualisation

La virtualisation est une technologie informatique qui permet de créer des versions virtuelles de systèmes informatiques, de serveurs, de réseaux ou d'applications. Par conséquent, il peut exécuter plusieurs systèmes d'exploitation ou applications sur un seul ordinateur physique ou un groupe de serveurs physiques.

Ainsi, la virtualisation permet à plusieurs utilisateurs ou applications de partager les mêmes ressources matérielles afin que les ressources informatiques puissent être utilisées au maximum. Il offre également la flexibilité de créer des environnements de test et de développement, de migrer facilement des applications entre différents environnements informatiques et d'isoler les applications les unes des autres pour une sécurité accrue « La virtualisation est une couche d'abstraction qui découple le système d'exploitation du matériel afin de délivrer une meilleure utilisation et flexibilité des ressources de traitement » (VMWare) Peut être vu comme une surcouche permettant de créer sur mesure un environnement correspondant aux spécifications de traitements.

On parle de :[14]

— Machine hôtes = machines exécutant différents systèmes virtuels.

— Machine invitée=Machine virtuelle s'exécutant dans un environnement virtualisé.

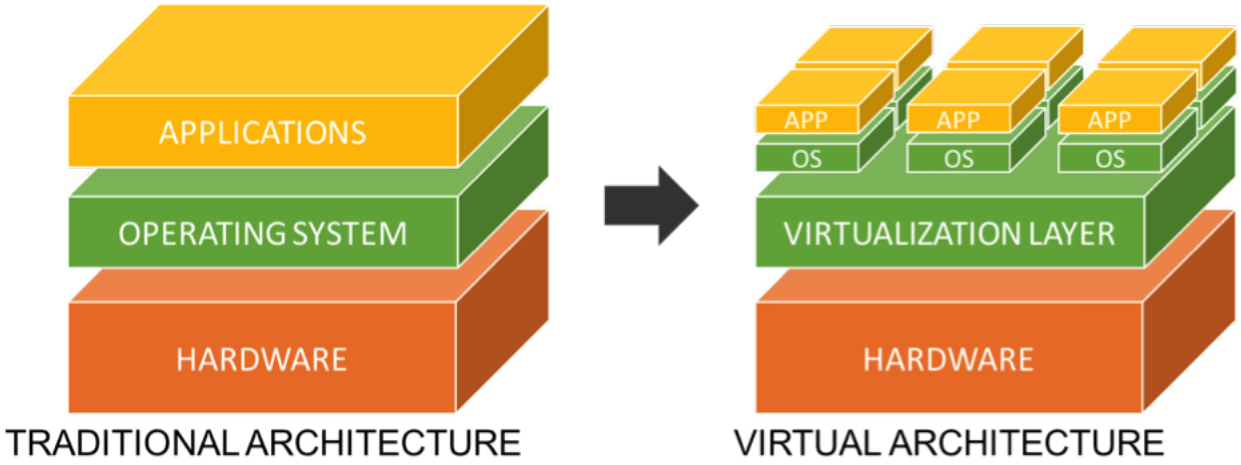


FIGURE 2.2 – La virtualisation[40]

2.4 Histoire de virtualisation

La virtualisation est une technologie développée pour les mainframes IBM dans les années 1960. Le système d'exploitation IBM System/370 CP/CMS a été la première plate-forme conçue pour la virtualisation.
Il permet à plusieurs instances de système d'exploitation de s'exécuter simultanément sur le mainframe. Cette combinaison de matériel et de logiciels compatibles avec la virtualisation a fait l'objet de recherches et est devenue la base de la famille de mainframes IBM. Les derniers mainframes IBM de la famille de systèmes Z continuent de fournir un support matériel pour la virtualisation à l'aide du logiciel z/VM (machine virtuelle). De nombreuses approches modernes de la virtualisation doivent beaucoup à l'implémentation originale du mainframe d'IBM.
Dans les années 1980, des embryons de virtualisation ont été créés pour les ordinateurs personnels, tels que l'Amiga qui pouvait démarrer des PC x386, des Macintosh 68 XXXe ou des solutions X11 multitâches.
Ces solutions sont purement logicielles ou associées à d'autres matériels. Big Unix a été suivi par les architectures Superdoué de HP et NUMA E10000/E15000 de Sun. Dans les années 1990, les émulateurs x86 pour machines plus anciennes des années 1980 connaissent un grand succès, notamment pour les ordinateurs Atari, Amiga, Amstrad et les consoles NES, SNES, Neo-Géo, AES. VMWare a popularisé la virtualisation logicielle pour les architectures de type x86 grâce à son système de virtualisation propriétaire développé à la fin des années 1990 et au début des années 2000.
Des logiciels libres tels que Xen, QEMU, Bochs, Linux-VServer, Virtual Box et des logiciels propriétaires gratuits tels que VirtualPC, VirtualServer et VMWare Serveur ont également contribué à populariser la virtualisation sur les architectures x86.

Les fabricants de processeurs x86 AMD et Intel ont implémenté la virtualisation matérielle dans leurs gammes de produits dans la seconde moitié des années 2000, VMWare a récemment rendu gratuit une version allégée de son hyperviseur phare ESX3i. [17][19].

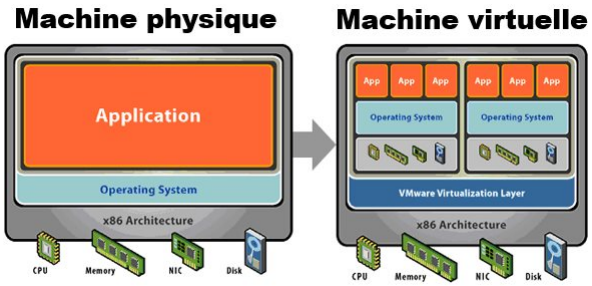


FIGURE 2.3 – Histoire de virtualisation[41]

2.5 Les hyperviseurs

Un hyperviseur (également appelé "moniteur de machine virtuelle" ou "VMM") est un logiciel de virtualisation qui permet de créer et de gérer des machines virtuelles (VM) sur un ordinateur physique. L'hyperviseur est la couche logicielle qui permet à plusieurs systèmes d'exploitation ou applications de fonctionner sur une même machine physique en les isolant les uns des autres. Il existe deux types d'hyperviseurs :[16]

1. **Les hyperviseurs de type 1** également appelés "hyperviseurs natifs" ou "hyperviseurs bare-metal", sont installés directement sur le matériel de l'ordinateur physique et sont capables de gérer les ressources matérielles directement. Les machines virtuelles fonctionnent donc directement sur le matériel, sans passer par un système d'exploitation hôte. Parmi les hyperviseurs de type 1 on trouve des solutions proposées par de grands éditeurs. Voici quelques noms de solutions : Hyper-V de chez Microsoft, ESXi de chez VMWare, Proxmox V qui se base sur Linux KVM et qui est open source, ou encore Citrix avec Citrix XenServer. VMWare est le leader sur le marché avec sa solution VMware ESXi, intégrée notamment dans sa suite vSphere [16].
2. **Les hyperviseurs de type 2** également appelés "hyperviseurs hébergés", sont installés sur un système d'exploitation hôte et utilisent les ressources matérielles de cet hôte pour créer et gérer les machines virtuelles. Par exemple, une machine sous Windows 10 sur lequel on va venir installer un hyperviseur (comme n'importe quel autre logiciel) dans le but de créer des VMs.

   Parmi les hyperviseurs de type 2, on retrouve les solutions suivantes : Oracle VirtualBox qui est gratuit et s'installe aussi bien sur Windows que Linux, VMWare Workstation (payant) ainsi que sa déclinaison gratuite VMWare Workstation Player. Sur macOS, on pourra installer VMWare Fusion. Clairement, ces hyperviseurs de type 2 sont idéals pour réaliser des tests sur une machine existante, tout comme peut l'être Hyper-V sur Windows 10.

Des tests à la maison ou en entreprise, dans tous les cas, l'hyperviseur de type 2 n'est pas destiné à la production [16].

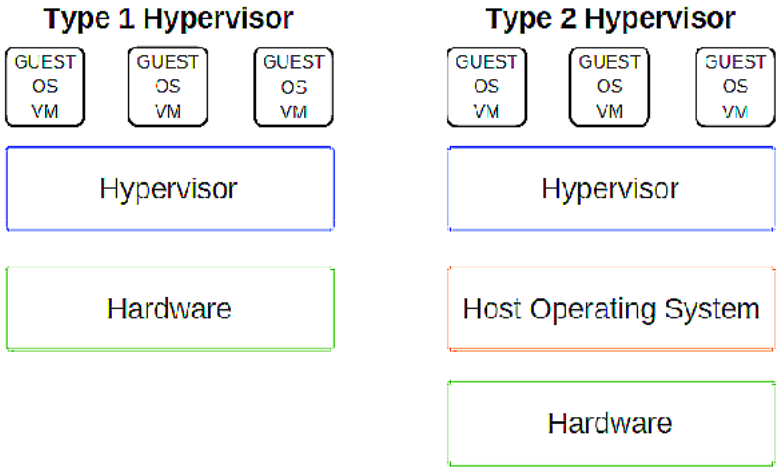


FIGURE 2.4 – Différence-hyperviseur-type-1-type-2[42]

2.6 Comment fonctionne la virtualisation

La virtualisation repose sur trois éléments clés : le système hôte, l'hyperviseur et le système invité. En combinant ces ingrédients, il est possible de créer une virtualisation. Pour ce faire, un système d'exploitation, également appelé système hôte, est installé sur un serveur unique. Il représente l'OS principal pour accueillir les autres systèmes d'exploitation. Ensuite, un logiciel de virtualisation, appelé hyperviseur, est installé sur le système hôte. Son rôle est de créer des environnements sur lesquels d'autres systèmes d'exploitation seront hébergés. Ces derniers sont appelés systèmes invités. Chaque environnement, appelé machine virtuelle, fonctionne de manière indépendante, mais peut disposer de capacités du serveur physique en termes de ressources matérielles. Ainsi, chaque machine virtuelle ou VM (Virtual Machine) peut bénéficier d'un accès à la mémoire, au processeur ou encore à l'espace disque. Des logiciels, appelés hyperviseurs, isolent les ressources physiques des environnements virtuels. Ces hyperviseurs peuvent reposer sur un système d'exploitation (ordinateur portable, par exemple) ou être directement installés sur un système physique (tel qu'un serveur), ce qui est l'option la plus souvent choisie par les entreprises qui ont recours à la virtualisation. Les hyperviseurs répartissent les ressources physiques pour permettre aux environnements virtuels de les utiliser.

La virtualisation repose sur trois éléments principaux : le système hôte, l'hyperviseur et le système invité. Sur un seul serveur physique, le système d'exploitation principal est installé et appelé système hôte. Il permet d'accueillir les autres systèmes d'exploitation invités. L'hyperviseur, un logiciel de virtualisation, est ensuite installé sur le système hôte. Son rôle est de créer des environnements virtuels sur lesquels les autres systèmes d'exploitation invités seront hébergés. Chaque environnement virtuel, appelé machine virtuelle, fonctionne de manière indépendante et peut disposer de ressources matérielles du serveur physique, telles que la mémoire, le processeur ou encore l'espace disque. Les hyperviseurs isolent les ressources physiques des environnements virtuels et répartissent les ressources physiques pour permettre aux environnements virtuels de les utiliser. Les machines virtuelles sont également appelées hôtes et permettent aux utilisateurs d'interagir et d'exécuter des calculs. Comme un fichier de données numériques, la machine virtuelle peut être transférée d'un ordinateur à un autre et utilisée de la même manière. Lorsqu'un utilisateur ou un programme émet une instruction nécessitant des ressources supplémentaires, l'hyperviseur transmet cette demande au système physique et en cache les modifications, offrant ainsi des performances presque identiques à celles d'un système natif.

2.7 Les types de virtualisations

2.7.1 Virtualisation de poste de travail

permet d'utiliser et de stocker des fichiers à des endroits auxquels tous les membres d'une équipe peuvent accéder facilement. Ainsi, plusieurs personnes peuvent accéder aux applications et aux systèmes d'exploitation d'un seul ordinateur, après qu'ils ont été installés sur un serveur qui centralisant données[18].

2.7.2 Virtualisation de systèmes d'exploitation

La virtualisation des systèmes d'exploitation, utilisée parfois à l'échelle domestique, permet d'exécuter sur une seule et même machine plusieurs OS différents, n'interférant pas les uns avec les autres. Exemple : naviguer sur un même ordinateur d'un environnement Windows à un environnement Linux. Les entreprises peuvent également transférer les systèmes d'exploitation virtuels vers des ordinateurs.[18]

2.7.3 Virtualisation des données

est une technologie qui permet de créer des copies virtuelles de données existantes, telles que des fichiers, des bases de données ou des systèmes de fichiers. Cette technique permet aux administrateurs de stocker et de gérer des données de manière plus efficace, en les regroupant et en les isolant les unes des autres.[18]

2.7.4 Virtualisation des applications

Grâce à la virtualisation des applications, les utilisateurs peuvent accéder à une application qui n'est pas installée sur leur ordinateur. Tout comme la virtualisation des bureaux, cette virtualisation est essentielle au travail à distance. Les employés peuvent ainsi travailler depuis chez eux en profitant de leurs outils professionnels. Cela signifie que les applications fonctionnent sur les ordinateurs comme si elles résidaient naturellement sur le disque dur de chacun d'eux, mais qu'elles sont exécutées sur un serveur centralisé.[18]

2.7.5 Virtualisations matérielles

La virtualisation matérielle est une technique de virtualisation qui permet à plusieurs systèmes d'exploitation de s'exécuter sur une seule machine physique. Cette technique permet d'optimiser l'utilisation des ressources matérielles en les partageant entre plusieurs machines virtuelles (VM). La virtualisation matérielle est réalisée à l'aide d'un logiciel appelé hyperviseur, également connu sous le nom de moniteur de machine virtuelle (VMM). [18]

2.8 Avantages de la virtualisation

De plus en plus d'entreprises ont adopté la technologie de la virtualisation en raison des nombreux avantages qu'elle offre. Parmi ces avantages, on peut citer :[19]

- La virtualisation permet de créer un environnement de test Plus d'obligation de réinstaller les serveurs
- Utiliser un autre système d'exploitation sans redémarrer son ordinateur
- Une flexibilité dans l'utilisation des différents systèmes d'exploitation. 1l est possible de travailler sous plusieurs environnements tels que Windows ou encore Linux sur un même poste.
- La souplesse de migration des VM sur un autre serveur physique plus puissant si besoin

— De diminuer les coûts de maintenance. Avec la virtualisation, le nombre de serveurs nécessaires diminement.

— Une meilleure exploitation des ressources : jusqu'alors souvent sous-exploitées, les capacités matérielles de T'entreprises sont fortement optimisées grâce à la virtualisation [181]

— Plus de disponibilité et Plus de portabilité.

— Tester des logiciels dans des environnements isolés et sécurisés

— Meilleure utilisation des ressources machines

— Gain de place physique, économie d'énergie

2.9 Consolidation, rationalisation et contraction

Afin d'éviter toute utilisation inappropriée de ces termes, j'ai redéfini chacun d'eux :

2.9.1 Consolidation

Il s'agit d'optimiser le taux d'utilisation des serveurs. Comme mentionné précédemment, exécuter une seule application sur des serveurs entraîne une perte. Ainsi, les serveurs ne sont exploités qu'à seulement 10 de leur performance (voire beaucoup moins dans certains cas). La consolidation permet d'atteindre des taux d'utilisation beaucoup plus élevés.[18]

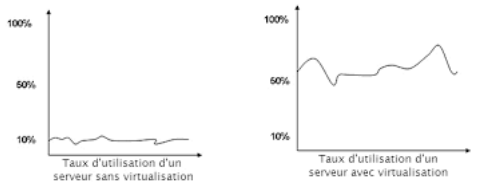


FIGURE 2.5 – Consolidation des serveurs.

2.9.2 Rationalisation

Il s'agit de supprimer les superflus et les équipements redondants inutiles. L'exemple le plus frappant concerne les différents composants d'un serveur tels que les cartes RAID, les cartes HBA et les disques durs. La rationalisation de l'infrastructure permet de réduire de manière drastique le nombre de ces équipements matériels. En plus des avantages financiers et des économies réelles apportées par la rationalisation, il y a également une réduction significative de la gestion quotidienne de ces équipements, ce qui est souvent une perte de temps.[18]

2.9.3 Concentration

La concentration permet de réduire l'espace pour accueillir davantage de serveurs dans un espace restreint. Il existe plusieurs niveaux de concentration : les formats Rack, les serveurs Lame et les formats Tour. Le nombre de U (1U équivaut à 44,45 millimètres) détermine la hauteur d'un serveur.

Les serveurs Lame (Bladeserveurs) sont les systèmes les plus optimisés en termes de concentration, car il est désormais possible d'héberger jusqu'à 16 serveurs Lame dans un châssis de 10U. Ils permettent également de rationaliser l'équipement en réduisant considérablement le câblage et les équipements redondants.

Cependant, ils n'offrent pas de consolidation, car le taux d'utilisation d'un serveur Lame est le même que celui d'un serveur Tour ou Rack.

L'association des serveurs Lame avec la virtualisation apporte consolidation, rationalisation et concentration. Pour certaines entreprises qui hébergent un grand nombre de serveurs (plusieurs centaines), l'association de Lame avec la virtualisation est un choix technique fondamental.[18]

2.10 Conclusion

Dans ce chapitre, nous avons vu la virtualisation et ses avantages, ainsi que les différents types de virtualisation avec leurs outils spécifiques et les hyperviseurs des deux types. Dans le chapitre suivant, nous allons Présenter l'organisme d'accueil

Chapitre 3

Présentation de l’organisme d’accueil

3.1 Introduction

Cevital est l'un des plus grands conglomérats privés en Algérie. Fondée en 1998 par Issad Rebrab, l'entreprise opère dans divers secteurs de l'économie, ce qui en fait un acteur majeur de l'industrie et du commerce en Algérie. Au fil des années, Cevital s'est développée et diversifiée, élargissant ses activités et étendant son influence tant en Algérie qu'à l'international.

3.2 Historique

Le groupe Cevital a une histoire qui remonte à sa fondation en 1998 par Issad Rebrab, un entrepreneur algérien. Depuis ses débuts, Cevital s'est développé rapidement et est devenu l'un des conglomérats les plus importants et les plus diversifiés d'Algérie.

Dans ses premières années, Cevital s'est concentré sur l'industrie agroalimentaire en investissant dans des secteurs tels que la transformation alimentaire, la production de sucre, d'huile végétale, de produits laitiers et de pâtes. Le groupe a également élargi ses activités dans d'autres secteurs, notamment la distribution, l'industrie automobile, la production d'acier, l'immobilier et la construction.

Au fil du temps, Cevital a cherché à se développer à l'international. En 2007, le groupe a acquis Groupe Brandt, une entreprise française spécialisée dans les appareils électroménagers. Cette acquisition a marqué l'entrée de Cevital sur le marché européen et a renforcé sa présence dans le secteur de l'électroménager.

En 2013, Cevital a poursuivi son expansion en Europe en acquérant Oxxo, un fabricant français de menuiseries en PVC. Cette acquisition a permis au groupe de diversifier ses activités dans le secteur de la construction et de renforcer sa position sur le marché européen.

Outre l'Europe, Cevital a également investi en Afrique et au Moyen-Orient. En 2015, le groupe a acquis le complexe sidérurgique El-Hadjar à Annaba, en Algérie, et a entrepris des investissements dans des projets d'exploitation minière en Mauritanie. Cevital a également développé des partenariats avec des entreprises en Égypte et a investi dans des projets agricoles au Soudan.

Au-delà de ses activités commerciales, Cevital a également mis en place des initiatives de responsabilité sociale des entreprises. Le groupe a lancé des programmes éducatifs et de formation professionnelle, soutenu des projets de développement communautaire et contribué à des initiatives humanitaires.

Avec son engagement constant envers l'expansion et la diversification, Cevital continue de jouer un rôle important dans l'économie algérienne et aspire à être un acteur majeur sur la scène internationale.

3.3 Organigramme du groupe Cevital

Voici le schéma général du groupe Cevital, dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre cette figure :

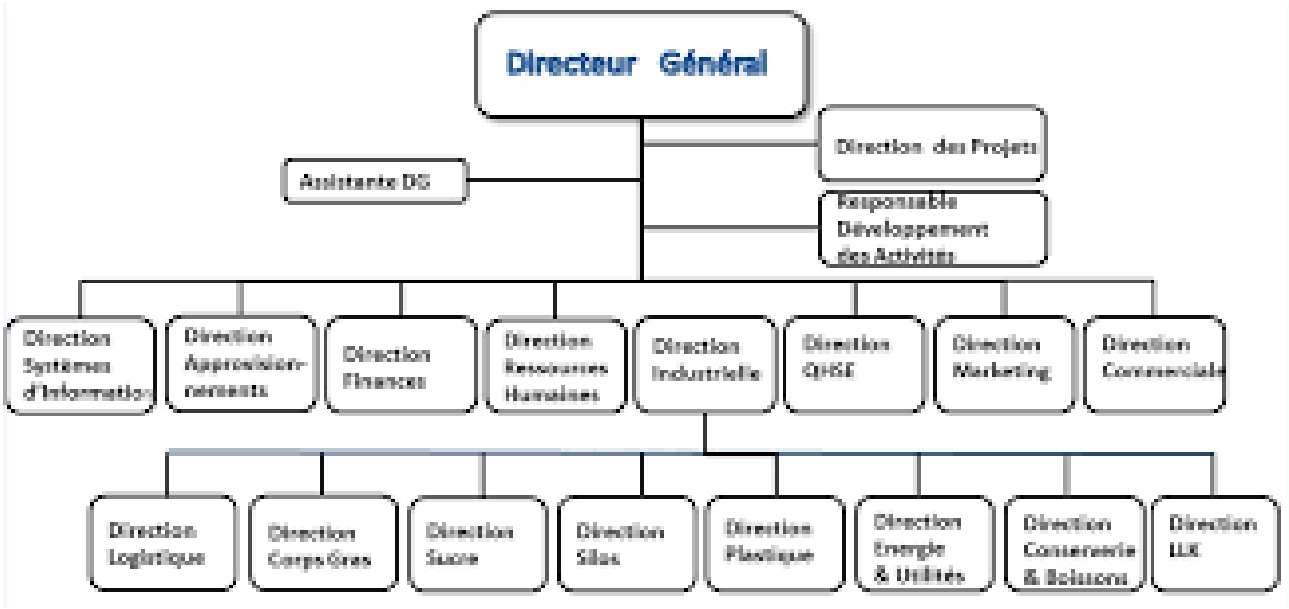


FIGURE 3.1 – Organigramme de cevital

3.4 Le département de Service Informatique de Cevital

est un département essentiel de l'entreprise chargé de fournir un soutien technique et informatique à l'ensemble de l'organisation. Son rôle principal est d'assurer le bon fonctionnement des systèmes informatiques, des logiciels et des équipements technologiques utilisés par les employés de l'entreprise.

Le département de Service Informatique est généralement composé d'une équipe d'experts en informatique, de techniciens et d'administrateurs système qui travaillent en étroite collaboration pour offrir un support technique efficace et résoudre les problèmes informatiques rencontrés par les utilisateurs.

Les principales responsabilités du département de Service Informatique comprennent :

1. Support technique : L'équipe de support Informatique est disponible pour aider les employés en cas de problèmes techniques tels que les pannes matérielles, les erreurs logicielles, les problèmes de connectivité Internet, etc. Ils fournissent une assistance par téléphone, par courrier électronique ou en personne, et cherchent à résoudre rapidement les problèmes pour minimiser les perturbations pour les utilisateurs.
2. Gestion des systèmes et des réseaux : Le département de Service Informatique est chargé de la gestion des systèmes d'exploitation, des serveurs, des réseaux et des infrastructures informatiques de l'entreprise. Ils assurent la configuration, la surveillance, la maintenance et la mise à jour régulière de ces systèmes pour garantir leur stabilité, leur sécurité et leur performance.
3. Gestion des logiciels et des licences : L'équipe gère également les licences logicielles de l'entreprise, en s'assurant que les logiciels utilisés sont légalement autorisés et correctement installés sur les ordinateurs des employés. Ils veillent également à ce que les logiciels soient régulièrement mis à jour pour bénéficier des dernières fonctionnalités et des correctifs de sécurité.

4. Sécurité informatique : Le département de Service Informatique joue un rôle crucial dans la sécurité des systèmes informatiques de l'entreprise. Ils mettent en place des mesures de sécurité telles que les pare-feu, les antivirus, les systèmes de détection des intrusions, les politiques de sécurité des mots de passe, etc. Ils effectuent également des sauvegardes régulières des données pour prévenir les pertes de données et planifient des plans de reprise après sinistre.

3.5 Missions de l'entreprise :

La mission principale de l'entreprise est de développer la production, garantir la qualité et le conditionnement des huiles, des margarines et du sucre à des prix compétitifs, dans le but de satisfaire et fidéliser les clients. Les objectifs poursuivis par Cevital peuvent être énoncés de la manière suivante :

1. **Diversification économique :** Cevital vise à promouvoir la diversification économique de l'Algérie en investissant dans différents secteurs, tels que l'agroalimentaire, l'industrie, la distribution et les services. En élargissant ses activités, l'entreprise contribue à la création d'emplois, au développement des industries locales et à la réduction de la dépendance à un seul secteur économique.
2. **Excellence opérationnelle :** Cevital s'efforce d'atteindre l'excellence opérationnelle dans toutes ses activités. Cela se traduit par des processus de production efficaces, une gestion rigoureuse de la qualité, l'adoption de normes internationales et une recherche constante d'innovation. L'entreprise vise à offrir des produits et des services de haute qualité qui répondent aux attentes des consommateurs.
3. **Expansion internationale :** Cevital a une ambition d'expansion internationale en investissant dans des marchés étrangers. L'entreprise cherche à acquérir des entreprises et à établir des partenariats stratégiques dans différents pays, ce qui lui permet de diversifier ses revenus et de renforcer sa présence sur la scène mondiale.
4. **Responsabilité sociale des entreprises :** Cevital reconnaît l'importance de la responsabilité sociale des entreprises et s'engage à contribuer au développement social et économique des communautés dans lesquelles elle opère. L'entreprise soutient des initiatives éducatives, des projets de développement durable, des programmes de santé et de bien-être, ainsi que des actions humanitaires pour améliorer les conditions de vie des populations locales.
5. **Leadership sectoriel :** Cevital aspire à être un leader dans les secteurs sur lesquels elle opère. L'entreprise vise à développer des produits innovants, à maintenir des normes élevées de performance et à jouer un rôle moteur dans la croissance de l'industrie. Cevital cherche également à favoriser la compétitivité de ses partenaires et à promouvoir des pratiques commerciales éthiques.

3.6 Problématique

Cevital est largement reconnue dans l'industrie agroalimentaire en Algérie et elle dispose également d'une infrastructure informatique étendue pour répondre aux exigences de ses diverses activités commerciales. Cependant, lors de mon stage à Cevital, nous avons constaté qu'il dispose d'un réseau local, de diverses plates-formes, de différents services, le service informatique dispose de plusieurs serveurs physiques, ce qui rend la gestion de ces derniers vraiment difficile et coûteuse.

3.7 Solution

VMware ESXi est une plateforme de virtualisation puissante et évolutive, conçue pour optimiser l'utilisation des ressources matérielles, simplifier la gestion des infrastructures et offrir des fonctionnalités avancées pour les environnements virtualisés, offre plusieurs avantages clés :

- Maximise l'utilisation des ressources matérielles et réduit les coûts associés à l'achat et à la maintenance de plusieurs serveurs.
- Les machines virtuelles peuvent être facilement redimensionnées, déplacées ou supprimées en fonction des exigences spécifiques,
- Les problèmes rencontrés au sein d'une machine virtuelle ne se répercutent pas sur les autres, ce qui contribue à renforcer la sécurité et la stabilité de l'environnement informatique en limitant les risques de propagation d'erreurs ou d'attaques.

3.8 conclusion

La présentation de la nature d'activité de l'entreprise cevital permettra de donner de façon plus claire l'obligation d'avoir une infrastructure réseau performante, flexible et sécurisé.
Dans ce qui suit, nous allons aborder les étapes de réalisation et configuration de solution de virtualisation.

Chapitre 4

RÉALISATION ET TEST

4.1 Introduction

Dans cette partie, nous parlerons de la réalisation de notre solution de virtualisation et de toutes les étapes d'installation et de configuration faute de matériels et d'infrastructure personnelle, on a juste pu créer : un serveur SER1 et une machine client pour jouer le rôle de l'utilisateur et un firewall pfSense pour assurer la connectivité entre les LAN serveur LAN clients et le trafic à l'extérieur (internet).

4.2 Présentation des outils de travail

4.2.1 VMWare Workstation

Le poste de travail VMWare (VMWare Workstation en anglais) est un hyperviseur de type 2 qui permet aux utilisateurs d'exécuter plusieurs systèmes d'exploitation sur une seule machine physique. Il a été développé par VMWare et a été initialement publié en 1999.

Le poste de travail VMWare prend en charge une large gamme de systèmes d'exploitation, notamment Windows, Linux et macOS. Il permet aux utilisateurs de créer des machines virtuelles, qui sont des environnements isolés qui imitent le matériel et les logiciels d'un ordinateur physique. Avec le poste de travail VMWare, les utilisateurs peuvent exécuter plusieurs machines virtuelles simultanément et passer de l'une à l'autre de manière transparente. Ils peuvent également partager des fichiers et des dossiers entre les machines virtuelles et le système d'exploitation hôte, ainsi que configurer des réseaux virtuels.

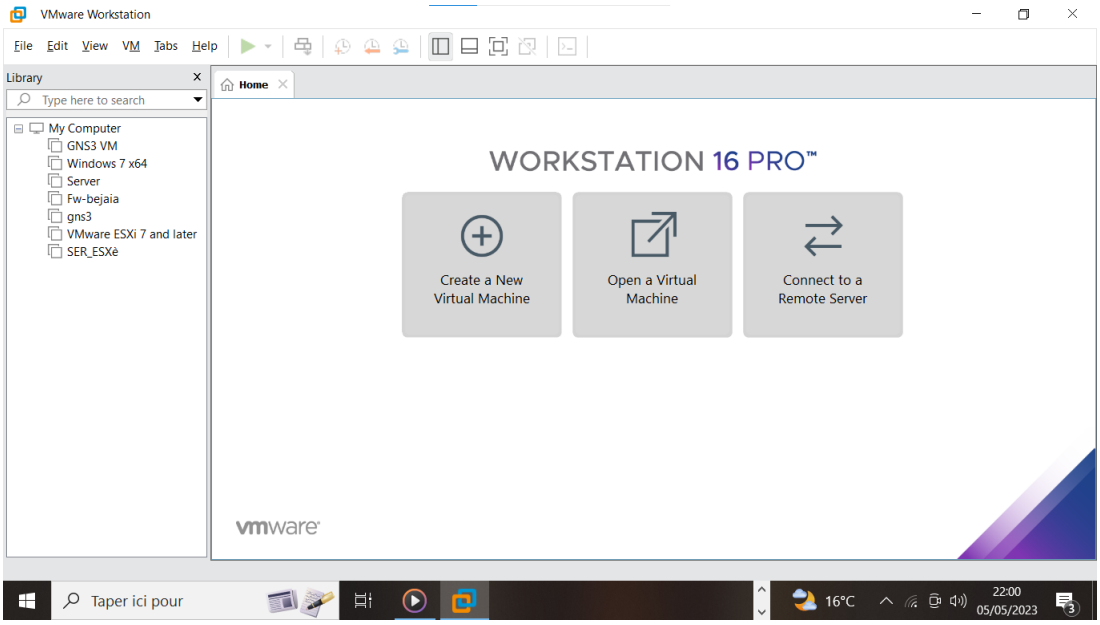


FIGURE 4.1 – VMWare Workstation.

4.2.2 ESXI

ESXi (prononcé "ess-eks-eye") est un hyperviseur de type 1, également appelé "bare-metal hyperviseur", qui permet de virtualiser des serveurs et des machines virtuelles sur des ressources matérielles dédiées. Il est développé par VMWare et est une version gratuite et légère de VMWare vSphere. Il a son propre système d'exploitation qui assure l'interface avec les agents dont il soutient l'exécution.

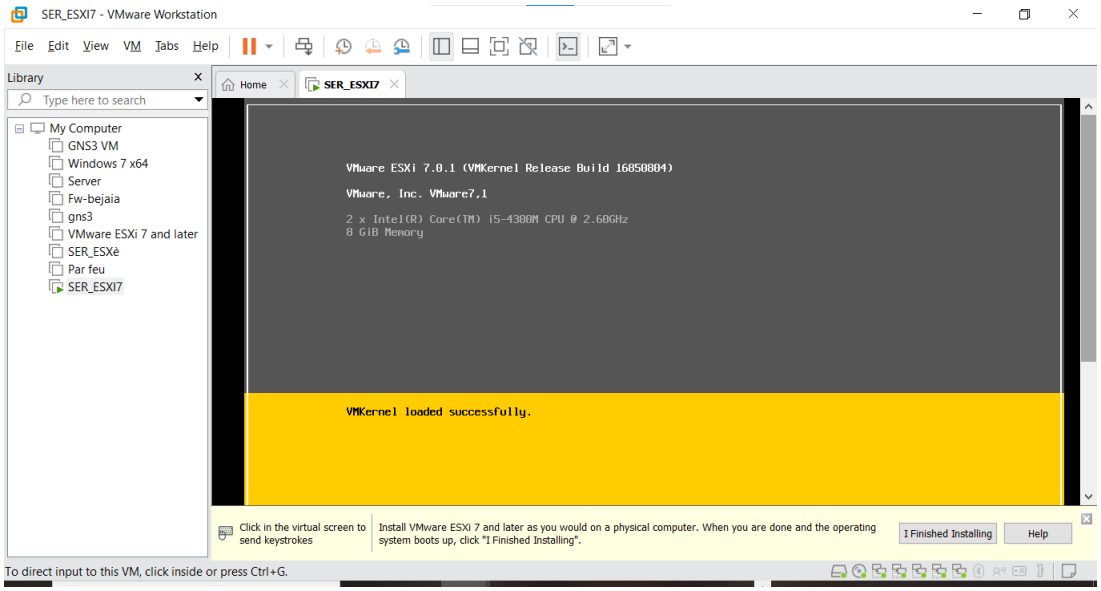


FIGURE 4.2 – ESXI.

4.2.3 Windows 10

Windows 10 est un système d'exploitation (OS) développé par Microsoft et lancé en juillet 2015. Il est la version la plus récente de la famille de systèmes d'exploitation Windows. Windows 10 est conçu pour fonctionner sur une grande variété de dispositifs, y compris les ordinateurs de bureau, les ordinateurs portables, les tablettes, les smartphones, les consoles de jeux, les appareils IoT et autres. Il est disponible en plusieurs éditions, notamment Windows 10 Home, Windows 10 Pro, Windows 10 Entreprise et Windows 10 Éducation, qui sont destinées à des utilisateurs et des entreprises ayant des besoins différents. Windows 10 est actuellement le système d'exploitation le plus utilisé dans le monde, avec une part de marché significative dans le monde des ordinateurs personnels. L'interface de l'OS s'adapte automatiquement au format et au mode de saisie (tactile ou bien clavier et souris).

4.2.4 Windows server 2022

Windows Server 2022 est un système d'exploitation serveur développé par Microsoft. Il s'agit de la dernière version de la plate-forme Windows Server, conçue pour répondre aux besoins des entreprises et des organisations en matière de gestion de serveurs, de stockage, de réseautage et d'autres services informatiques.

4.2.5 pfSense : firewall

pfSense est un système d'exploitation open-source basé sur FreeBSD qui est utilisé pour le pare-feu et les routeurs. Il fournit une plate-forme de sécurité réseau pour les entreprises, les fournisseurs de services et les utilisateurs finaux qui souhaitent sécuriser leurs réseaux.

4.3 Partie I : Configuration

4.3.1 Présentation de la solution de virtualisation

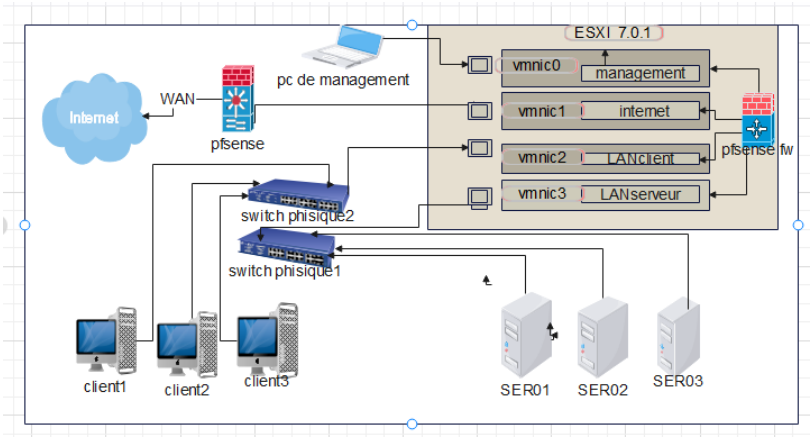


FIGURE 4.3 – La solution de virtualisation.

Tableau d'adressage des équipements

Équipements	Interfaces	Adresses IP
Firewall	LAN client LAN serveur WAN	10.1.10.1 10.1.20.1 DHCP
Serveurs	SER1	10.1.20.100
Client	Client1	10.1.10.10

TABLE 4.1 – Tableau d'adressage des équipements

Nom des segments	Adresse réseaux	Nic physique	Switch virtuel	Groupe de port
LAN Serveurs	10.1.20.1/24	Vmnic2	vSwitch2	Groupe serveur
LAN Clients	10.1.10.1/24	Vmnic1	vSwitch1	Groupe clients
WAN	DHCP	Vmnic3	vSwitch3	Internet
LAN Management	192.168.144.136/24	Vmnic0	vSwitch0	Management

TABLE 4.2 – Tableau des réseaux

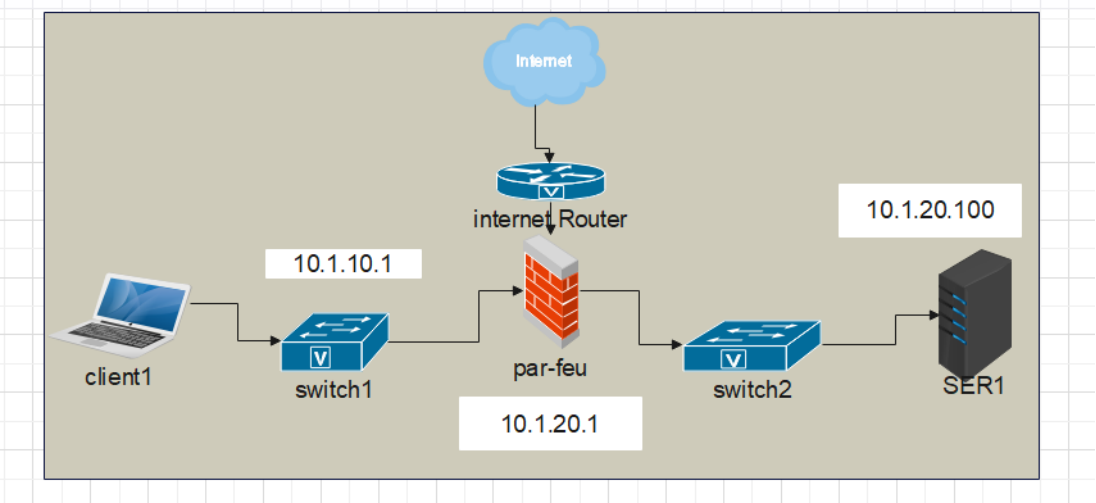
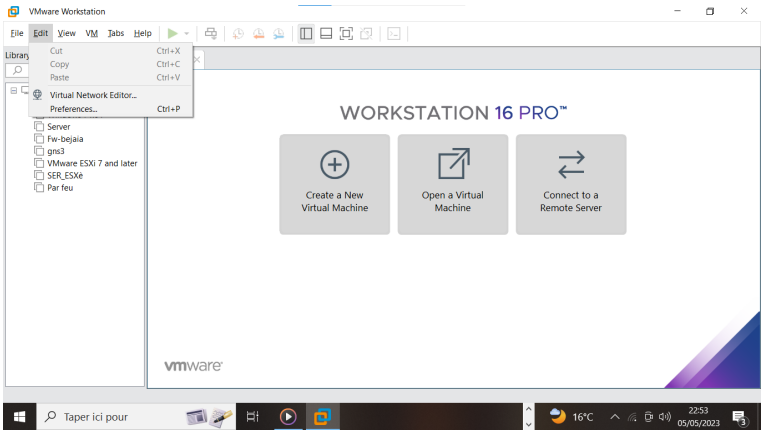


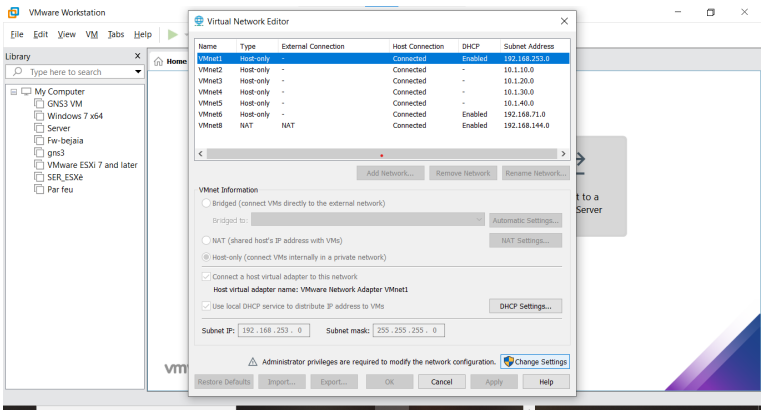
FIGURE 4.4 – Schéma architecture réseau proposé.

4.3.2 Création et paramétrage des cartes réseau physiques VMnet sur VMWare Workstation

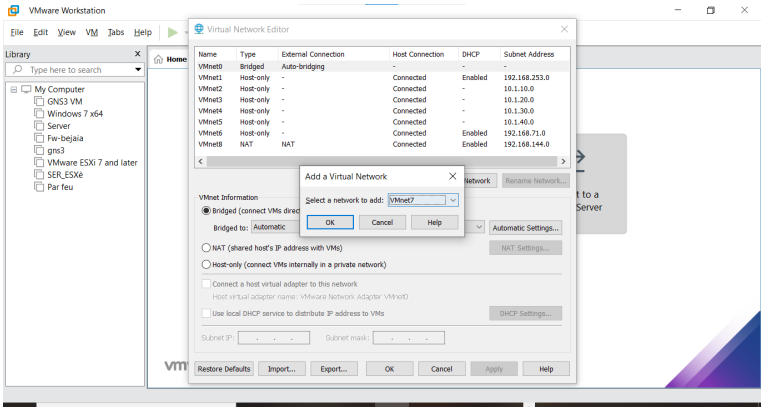
On lance le programme VMWare Workstation puis le menu Édit -> Virtual Network Editor de VMWare Workstation.



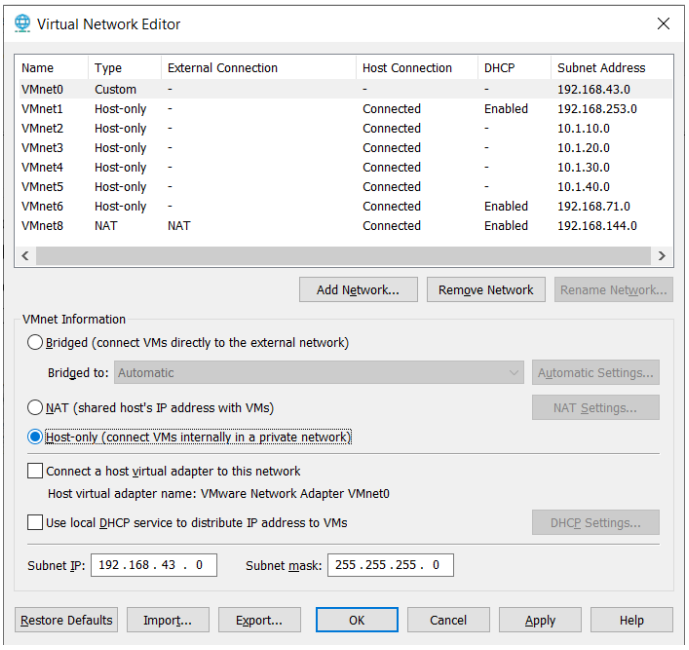
On doit cliquer sur Change Settings pour que Virtual Network Editor obtienne les droits administrateurs. Pour ajouter un nouveau réseau virtuel :



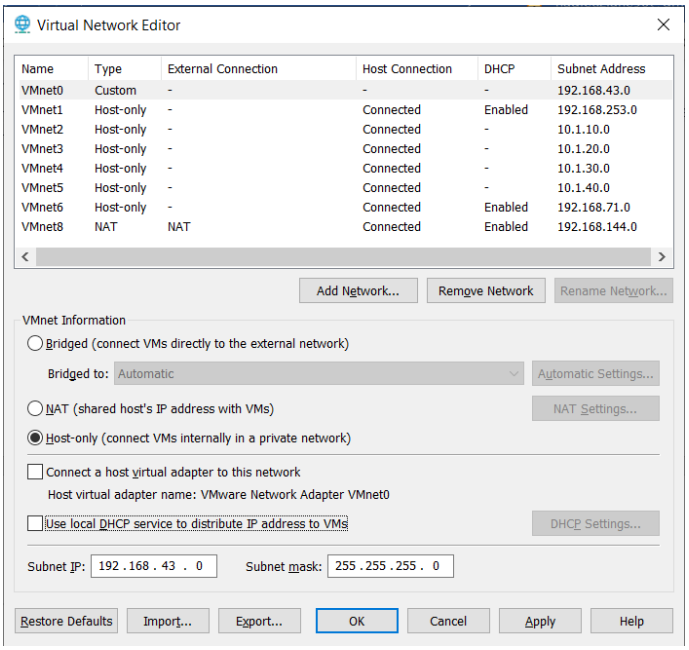
On Clique sur Add Network (exemple VMnet7 ici)



On Coche Host-only



On Décoche Use local DHCP



Subnet IP : on choisit un sous-réseau
Cliquez sur OK pour finir.

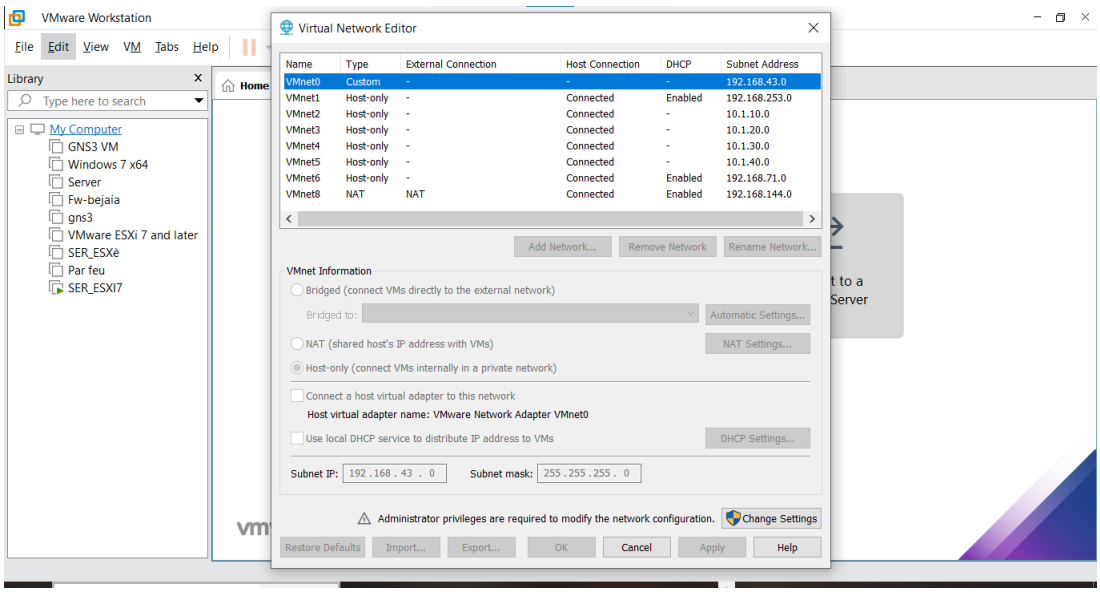


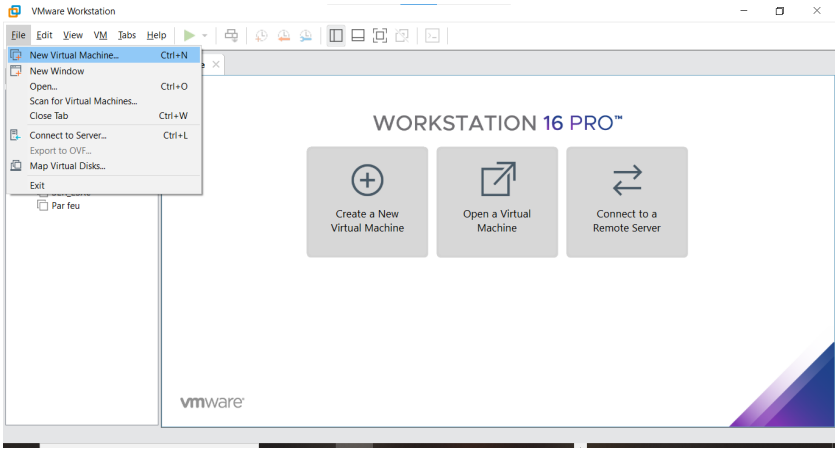
FIGURE 4.5 – Ajout d'une carte réseau.

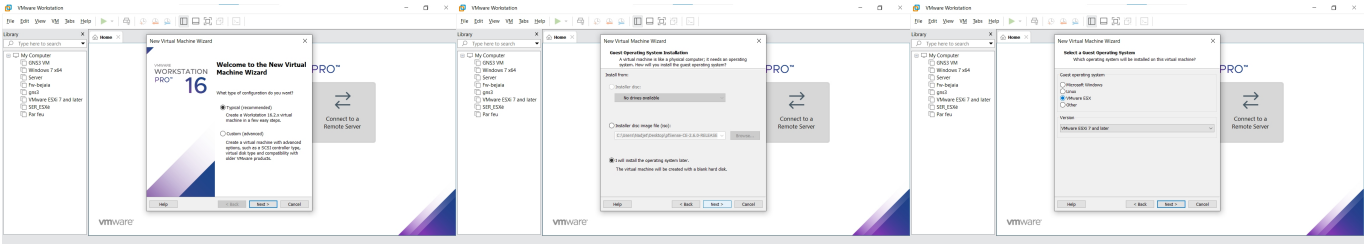
On a créé 4 Cartes réseau comme on l'a vu dans la figure précédente et dans le tableau des réseaux

- VMnet2 pour le management
- VMnet3 pour le LAN client
- VMnet4 pour le SERVEUR
- VMnet8 pour la connexion internet

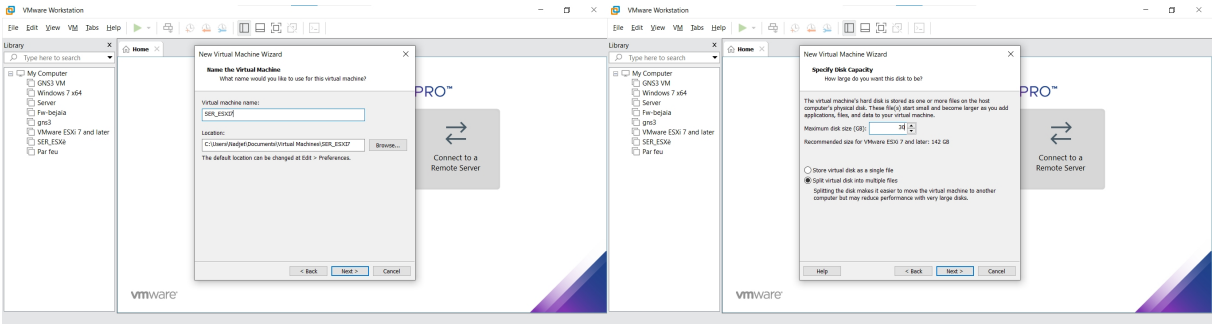
4.3.3 Installation ESXI

On a Choisi la version de notre ESXI ici, on travaille avec la version 7.0.1 On Clique sur New Virtual Machine->Custom après, on choisit la version de notre ESXI puis charger notre Image ISO de ESXI préalablement télécharger du site de VMWare dans les étapes à suivre :

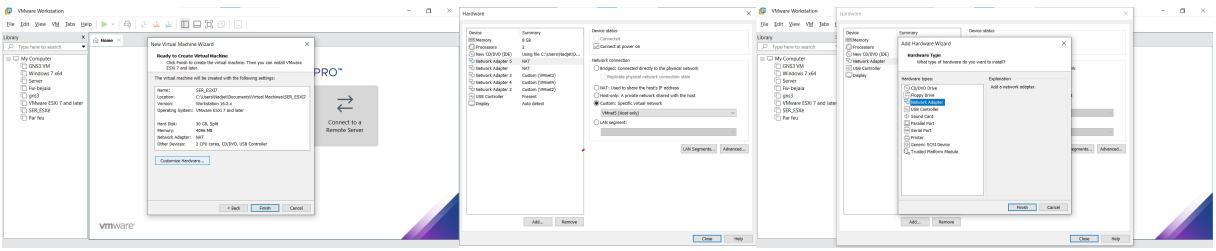




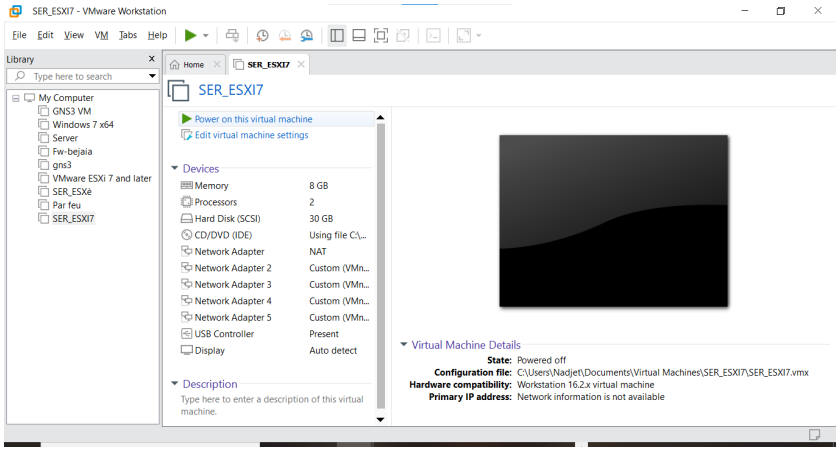
On va donner un nom à notre VM (c'est SER*ESXI7 ici) Sélectionner le nombre processeurs que l'on veut dédier à notre ESXI, la RAM (ici, c'est 8 Go) et la taille de l'espace de sauvegarde.

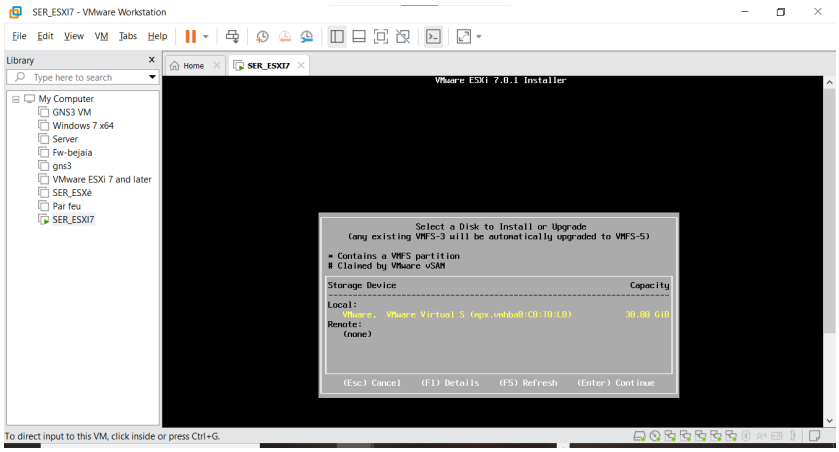


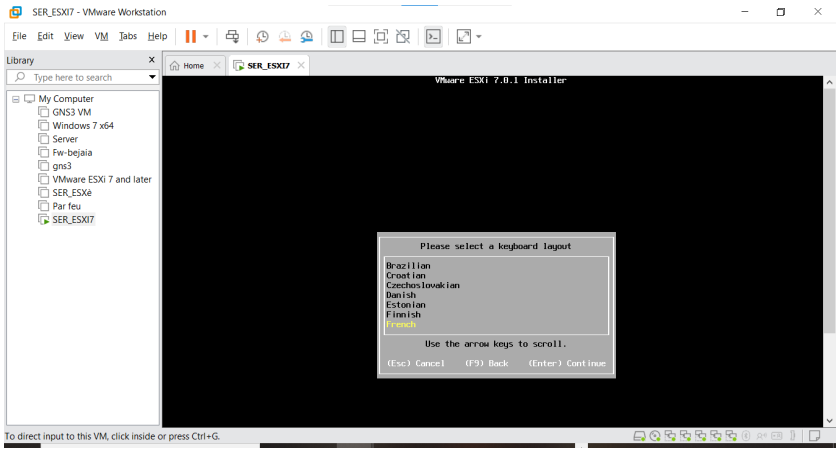
Avant de démarrer notre ESXI, on configure les paramètres de la VM dont l'ajout de nos VMnets, puis sur finish

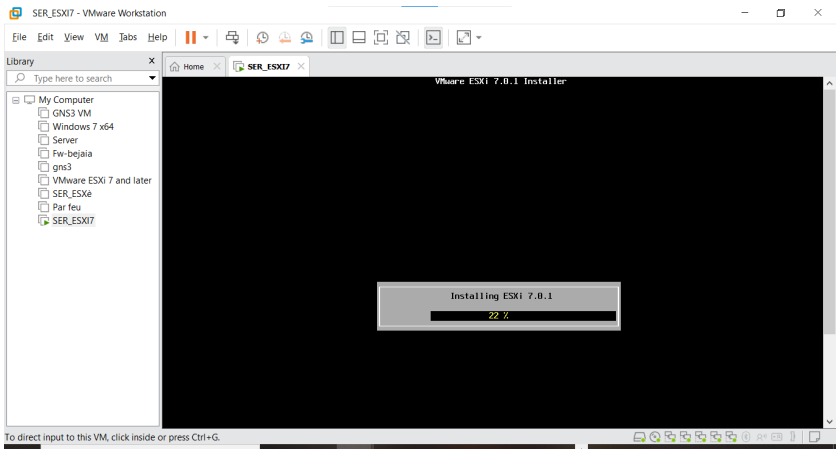


On Démarre la VM, après le chargement de l'ISO

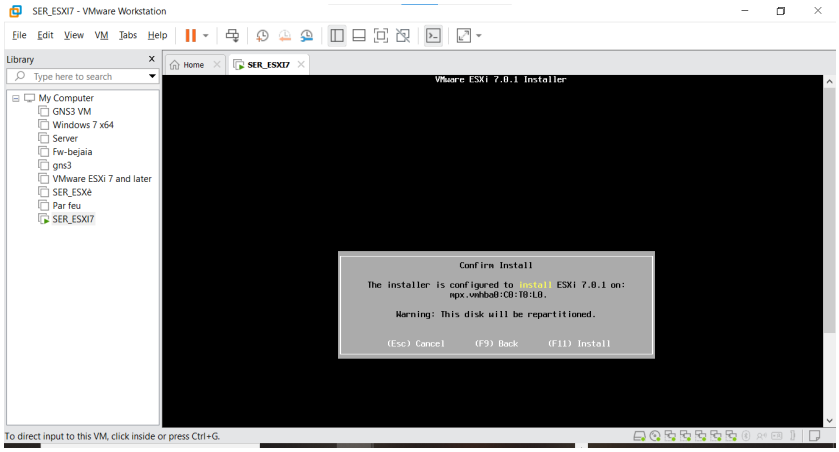


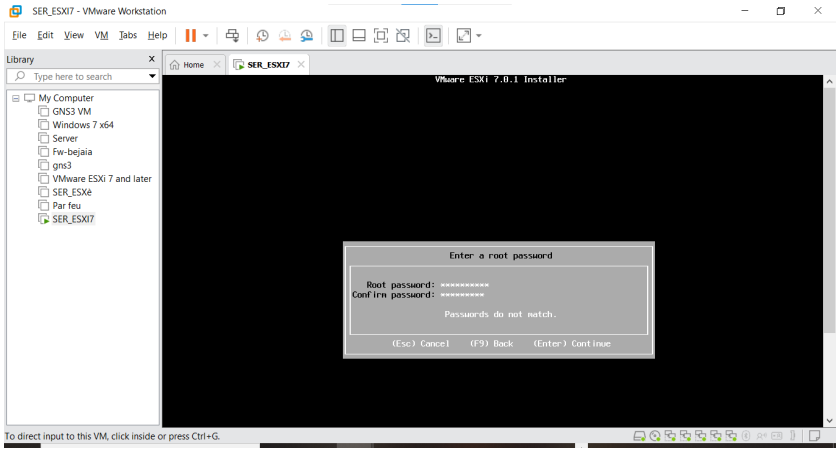


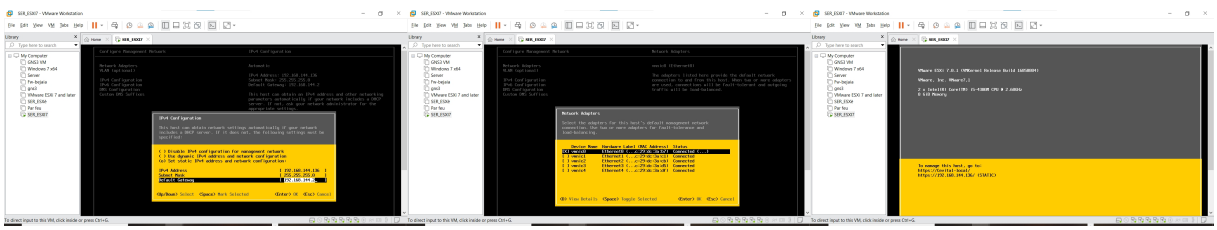




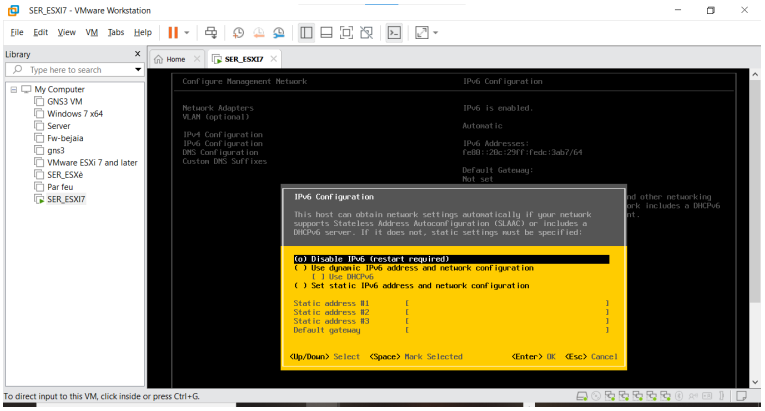
On clique sur F2 pour accéder au paramètre, nous avons entré notre mot de passe de (ASR**2023) ->Configure Management Network ->IPv4 Configuration -> Set Statique IPv4 adresse and network configuration



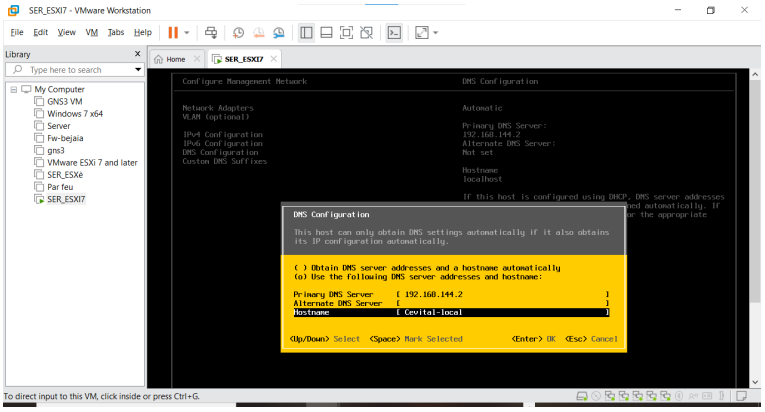




IPv6 Configuration ->espace (pour choisir disable IPv6)



->DNS Configuration ->hostname (Cevital-local)

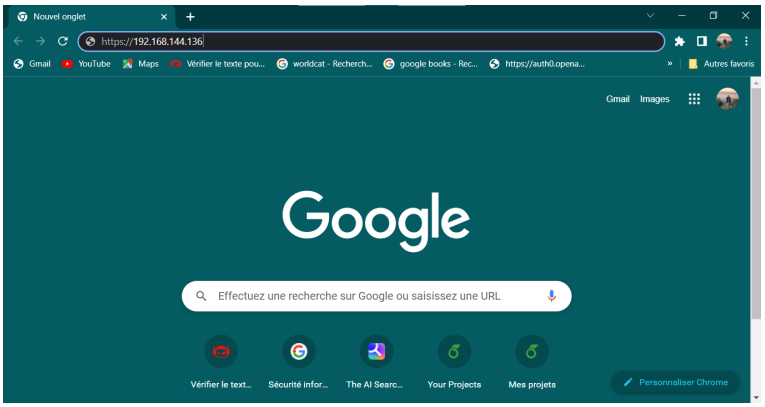


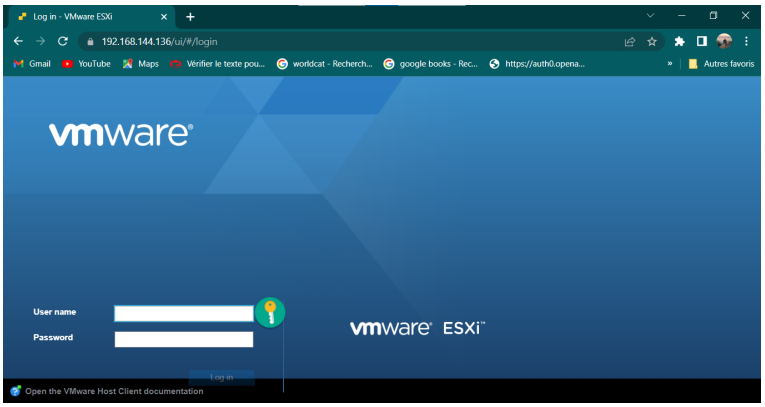
Renseigner l'adresse IP, Masque et la Passerelle en adéquation avec le sous-réseau du VMnet management créé au tout début Cliquez sur OK puis sur Yes pour redémarrer Configure Management Network.

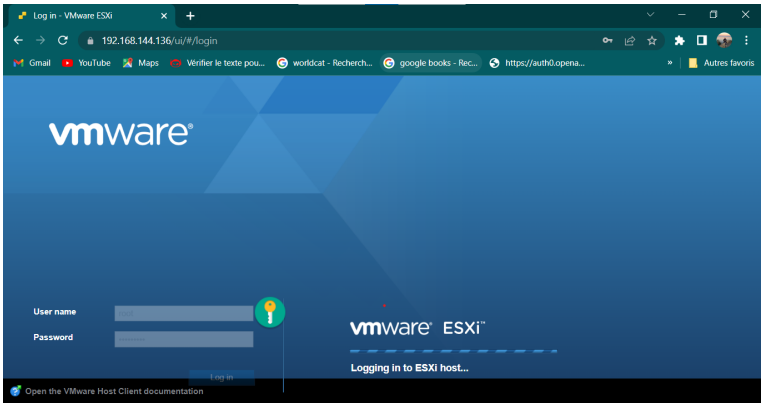
4.3.4 Création des commutateurs virtuelle vSwitchs

Un commutateur virtuel, également appelé vSwitch ou commutateur réseau virtuel, est un commutateur basé sur un logiciel qui fonctionne dans un environnement virtualisé. Il permet aux machines virtuelles (VM) de communiquer entre elles et avec le réseau physique.

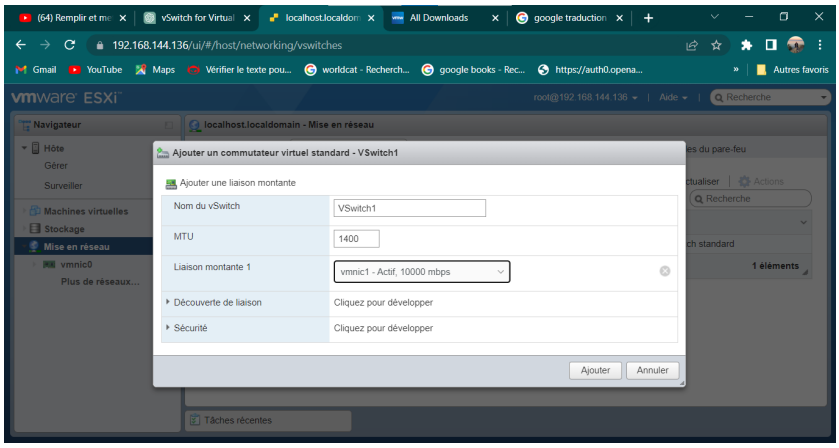
Un vSwitch crée des connexions de réseau virtuel entre les machines virtuelles et le réseau physique. Il permet également des configurations de réseau avancées, telles que le marquage VLAN, le façonnage du trafic et l'isolation de réseau. Sur l'interface graphique de notre ESXI (ça veut dire dans le navigateur) on doit donner l'adresse de notre SER*ESXI7 (ici, c'est https ://192.168.144.136) ->après saisir le nom et le mot de passe.

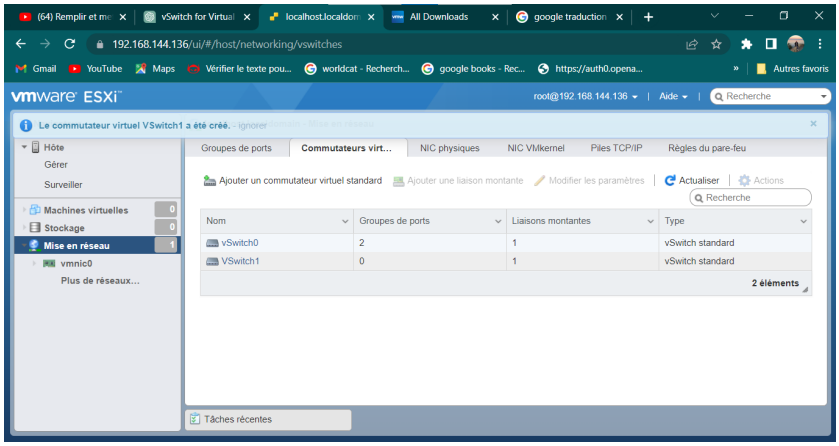




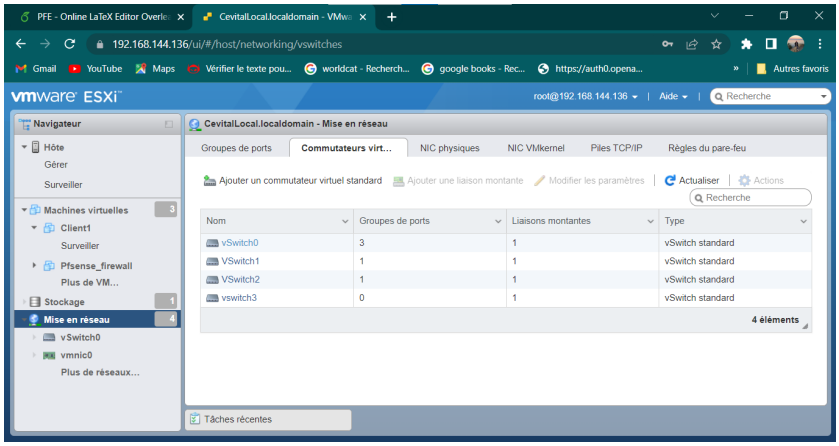


On va cliquer sur une mise en réseau -> commutateur virtuel, on clique sur ajouter un commutateur virtuel standard, une fenêtre va apparaitre (regarder la configure) on donne un nom à notre VSwitch (exemple ici VSwitch1) et on laisse tous les autres paramètres par défaut et l'on clique sur ajouter



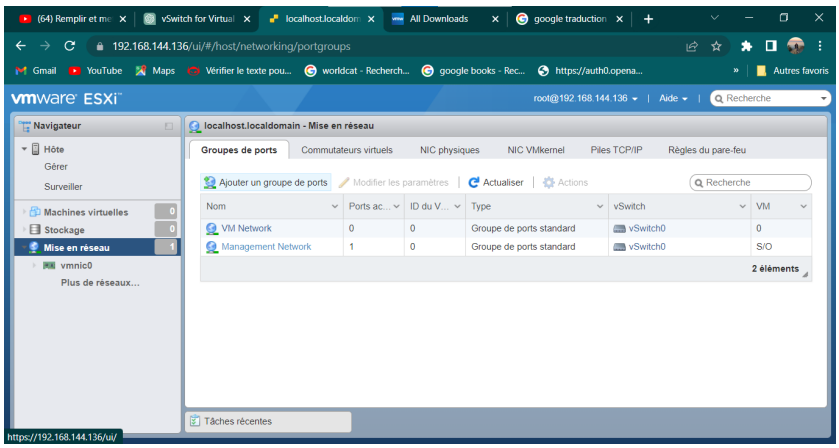


Voici tous les commutateurs virtuels que l'on a créés le vSwitch c'est le commutateur par défaut de l'ESXI (pour le management de notre ESXI).

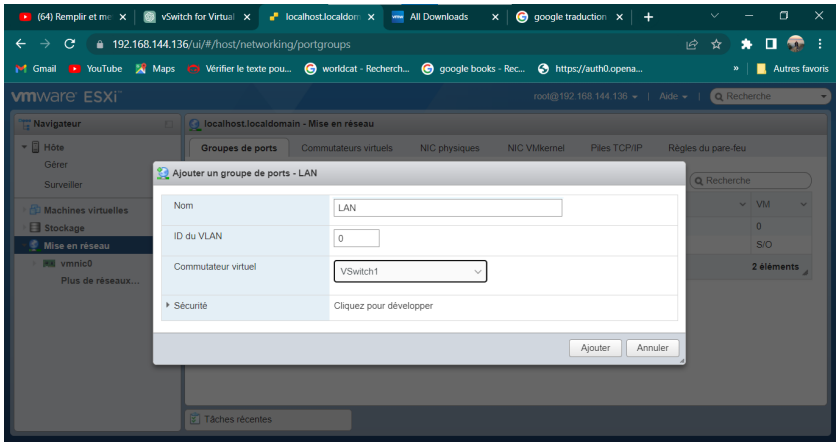


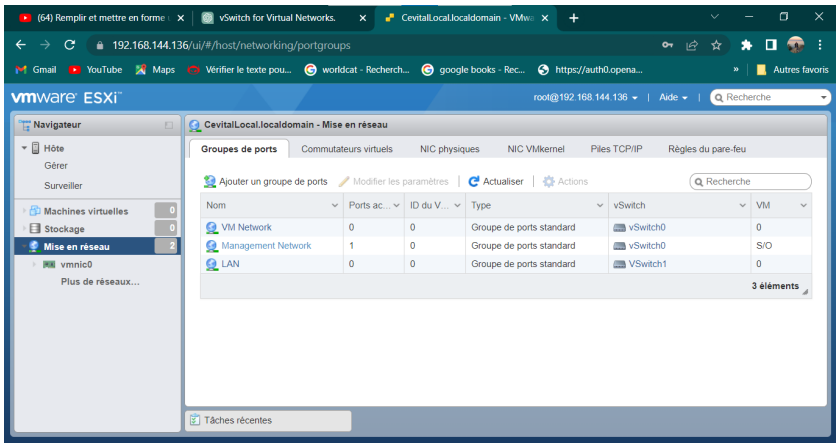
4.3.5 Création des groupes de port

Un réseau ou groupe de ports est connecté à un VSwitch, qui lui-même se connecte à une interface réseau physique. Les groupes de ports compartimentent une partie des ports du VSwitch.

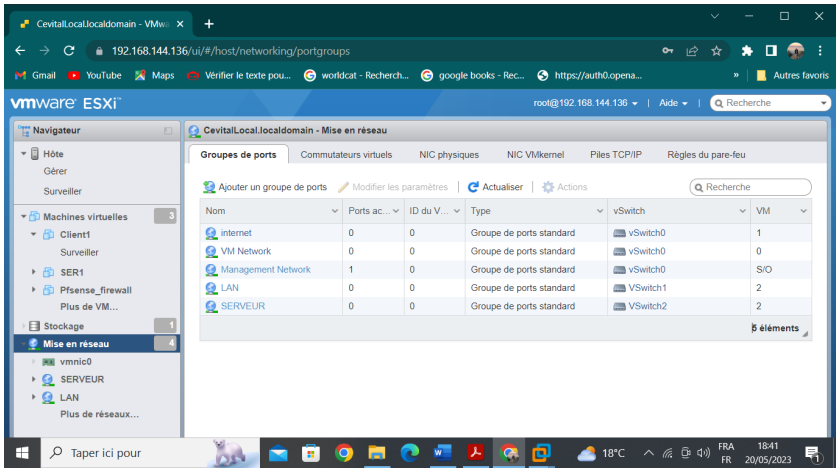


Ajout d'un groupe de port On clique sur ajouter un groupe de ports, dans la fenêtre suivante, on donne un nom à notre groupe de ports (ici le nom est LAN) et puis on lui affecte le vSwitch adéquat et on laisse tous les autres paramètres par défaut, ici, on n'utilise pas le vlan donc id vlan 0 Les groupe de port de notre ESXI sont comme suit (regarder la figure)





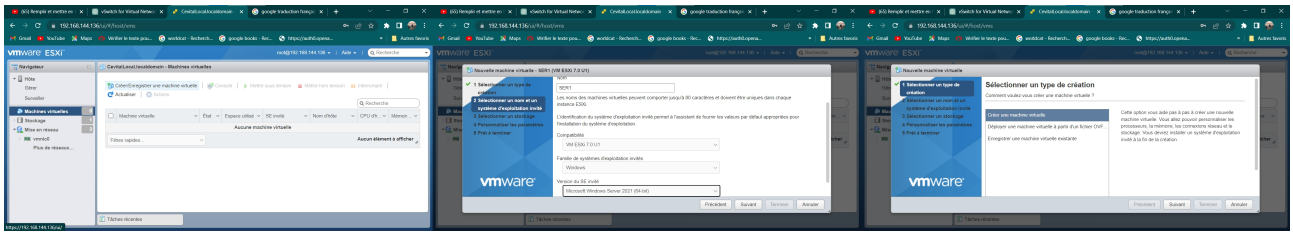
Voici tous les ports que l'on a créés :



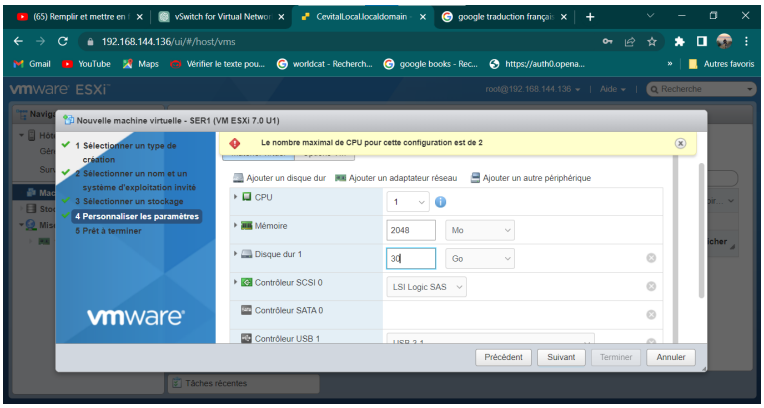
Une fois le vSwitch et le groupe de ports créés et configurés, on passe à la création machine virtuelle (VM)

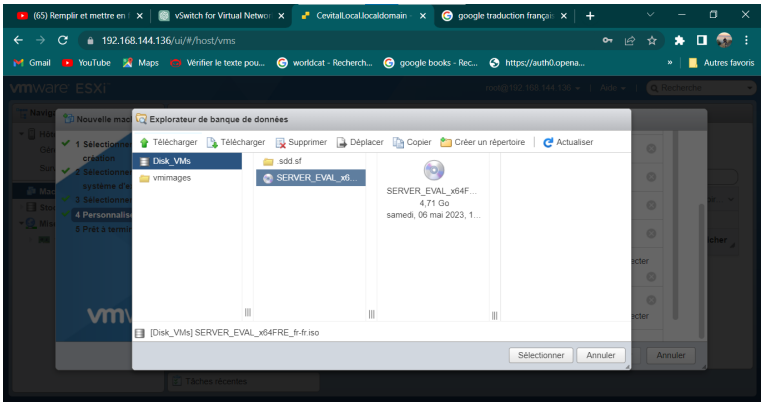
4.3.6 Création d'une machine virtuelle

Sur notre ESXI, on clique sur le bouton machine virtuelle. Puis, on clique sur créer une machine virtuelle, Ensuite, nous cliquons sur suivant dans la première fenêtre qui apparaît et nous entrons le nom VM, et sélectionnez le système d'exploitation que nous voulons installer sur la VM.

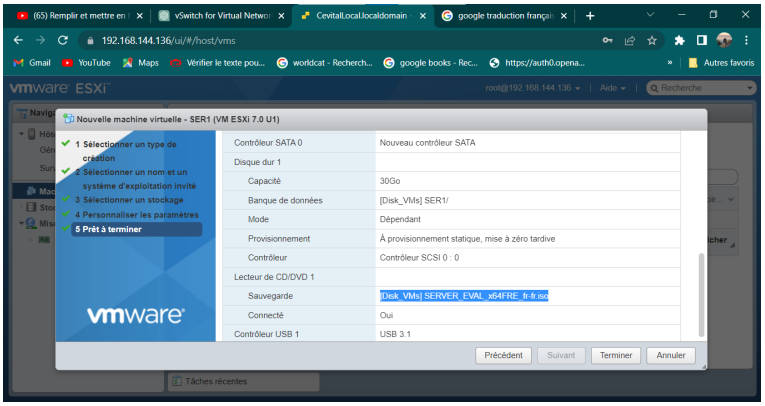


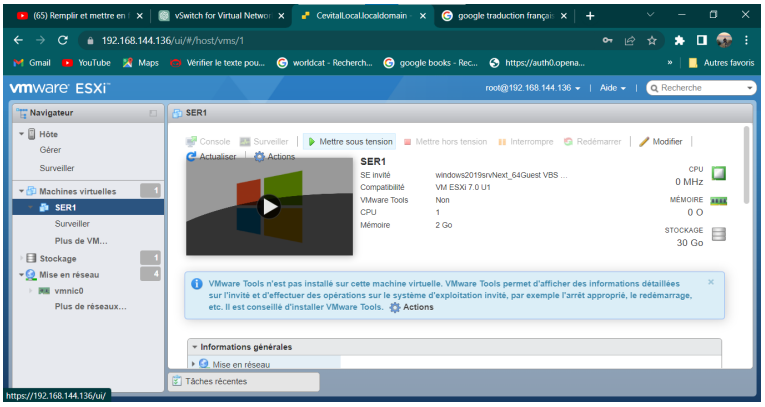
Ensuite, nous choisissons l'emplacement de stockage (data store) où nous voulons installer notre VM, et nous arrivons à l'écran avec lequel nous configurons le matériel de la VM. Configuration minimale recommandée pour votre système d'exploitation. Sur le lecteur de DVD, sélectionnez dans la liste déroulante "Fichier ISO banque de données", l'écran suivant apparaîtra afin que vous puissiez choisir l'ISO à utiliser avant le téléchargement.

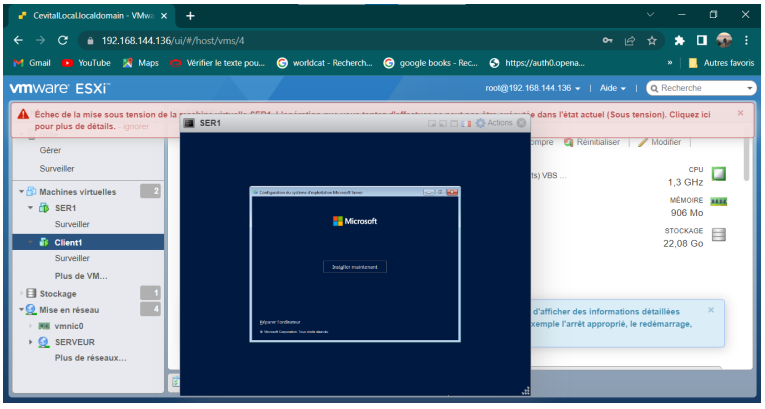


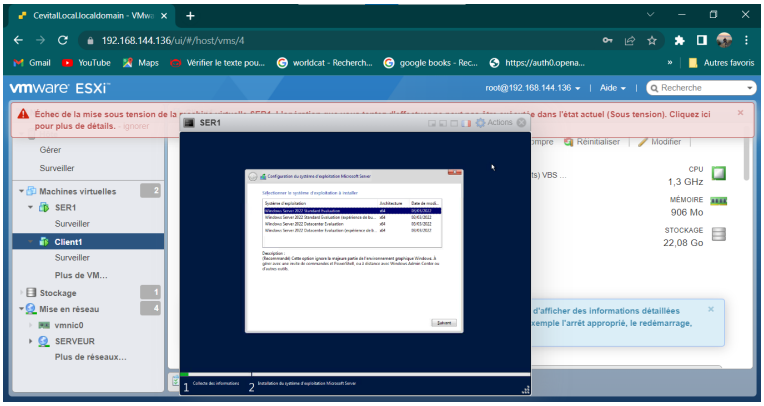


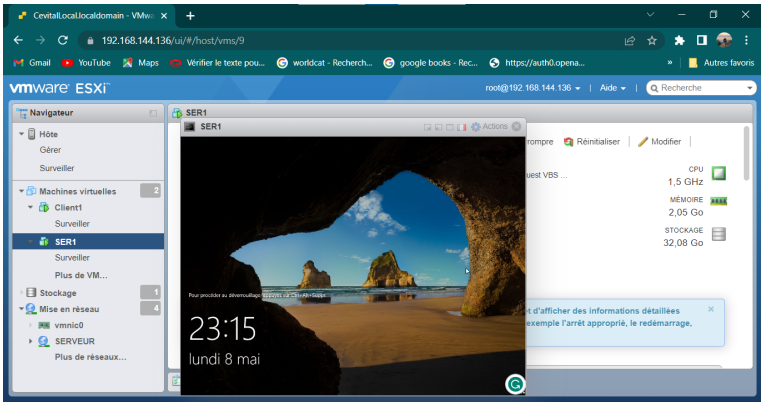
On clique une dernière fois sur Suivant et l'on arrive sur le résumé de notre machine, on clique sur Terminer. On met notre VM sous tension et l'on procède à l'installation de l'OS.

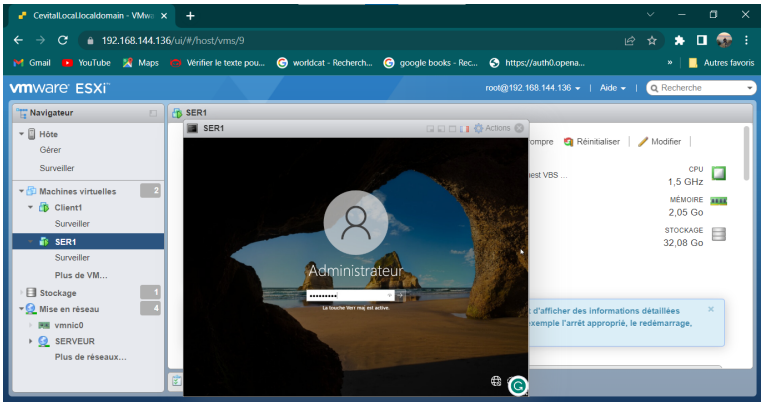




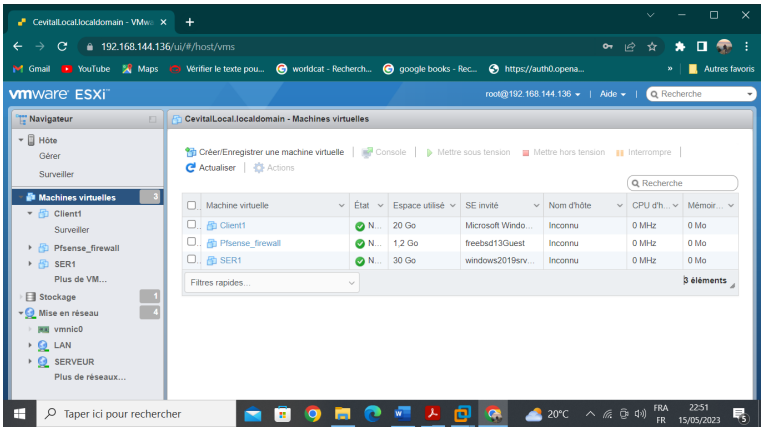






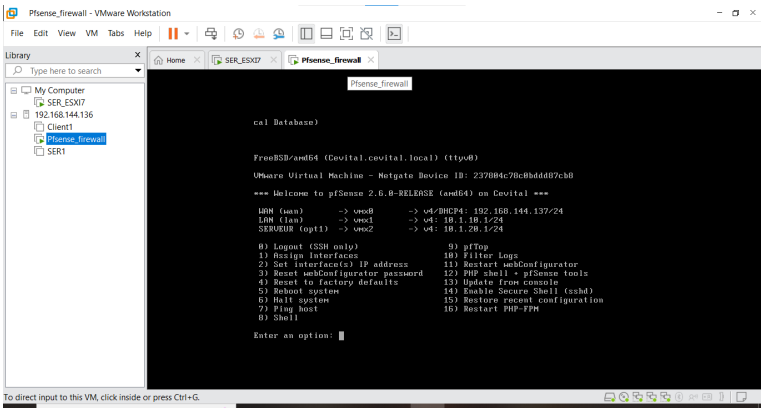


On a créé de la même façon nos VM, le client et le firewall pfSense et nous obtenons la figure suivante :

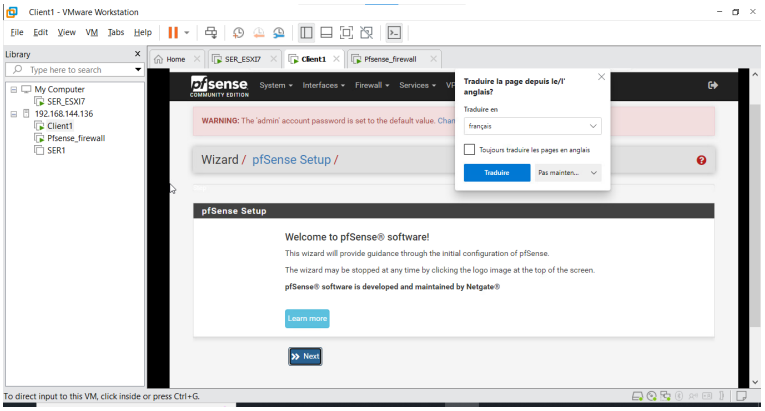


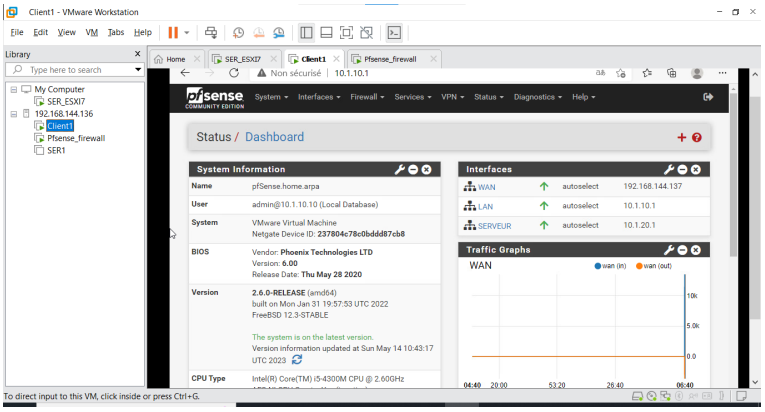
4.3.7 Paramétrage du firewall

Dans la Line de commande, on a attribué les adresses IP des trois interfaces du firewall comme suit :

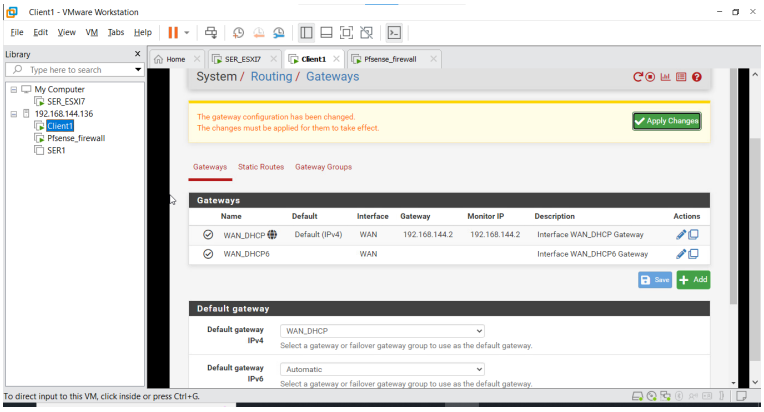


L'interface graphique de notre pare-feu pfSense est accessible depuis la machine cliente.

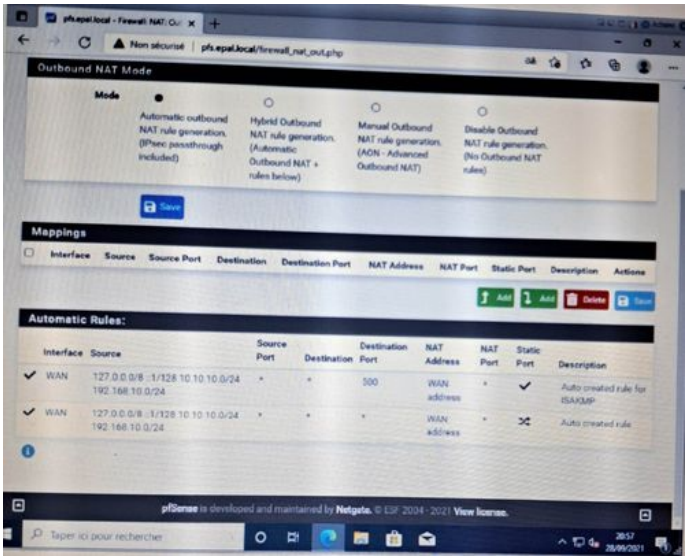




La passerelle de sortie est utilisée comme adresse par défaut pour le routage vers l'extérieur, ce qui signifie que tout le trafic réseau passe par celle-ci.



Une fonction de NAT automatique est mise en place pour le réseau vers l'extérieur (connexion Internet).



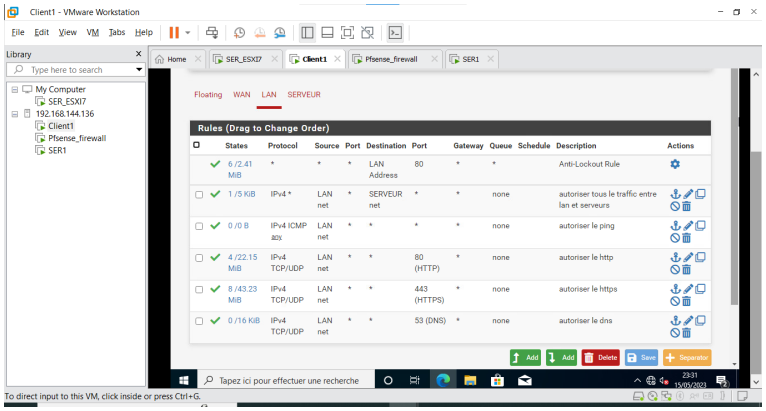
Filtrage : Autorisé trafic entre :

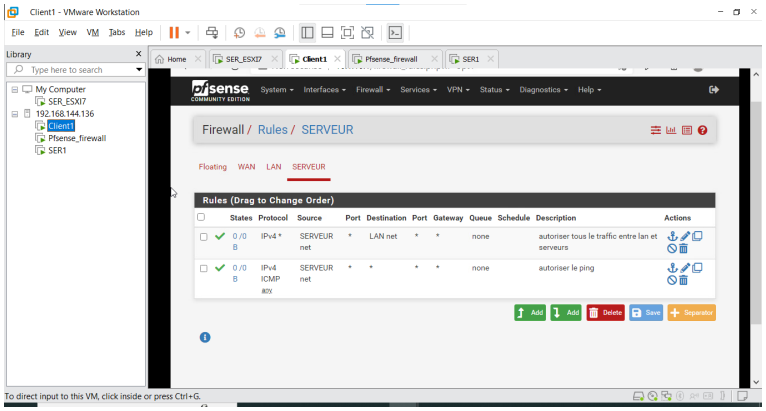
— LANclients et LANserveurs

— LANclient et WAN (autorise-le HTTP, HTTPS et DNS)

— LANserveur et LAN clients

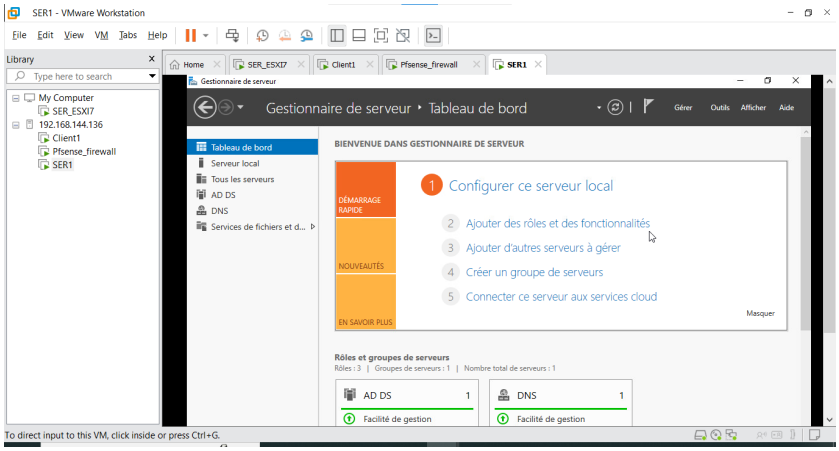
— LAN serveurs et WAN





4.3.8 Les serveurs

Serveur Active Directory

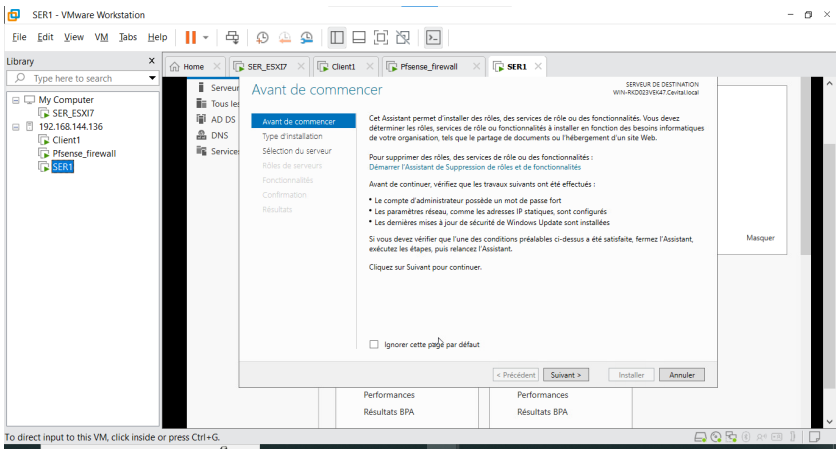


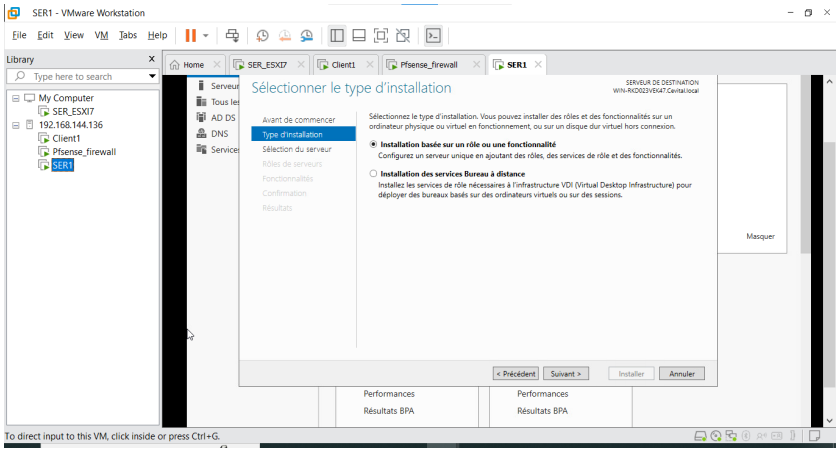
Installation d'Active Directory

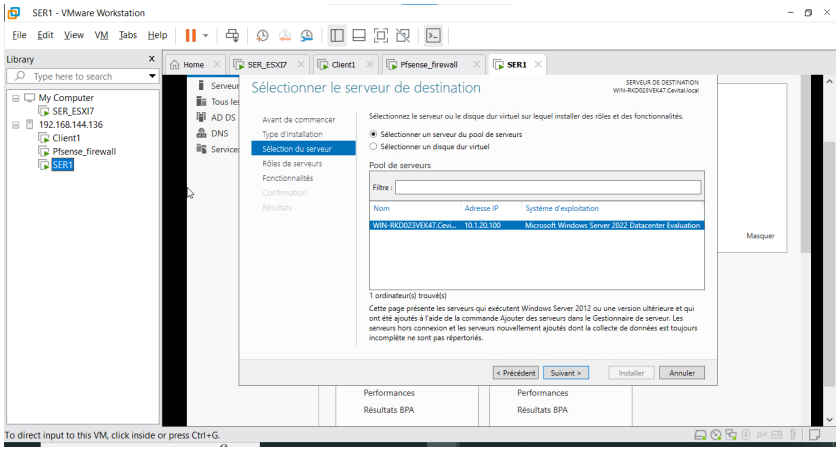
Active Directory est un service d'annuaire développé par Microsoft, utilisé pour gérer les ressources réseau dans un environnement Windows. Dans le contexte de VMWare, Active Directory peut être déployé en tant que machine virtuelle (VM) pour fournir des services d'annuaire centralisés aux machines virtuelles et aux utilisateurs du réseau.

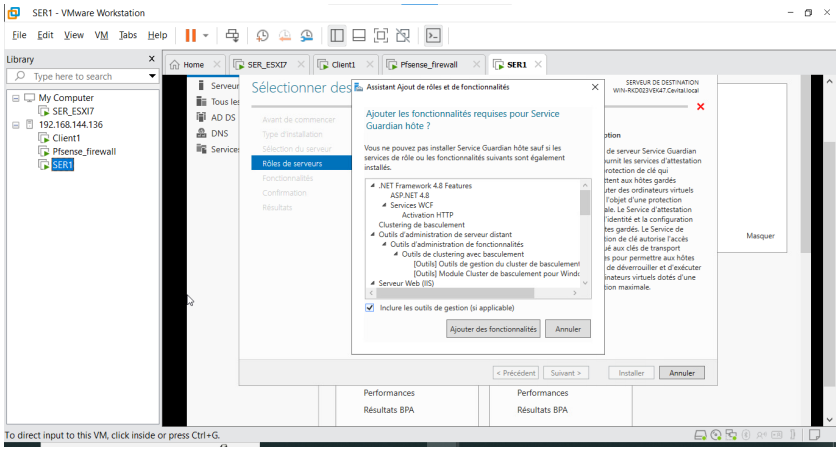
Il permet de centraliser l'authentification des utilisateurs, la gestion des comptes et des groupes, la politique de sécurité, ainsi que la gestion des ressources réseau telles que les imprimantes, les partages de fichiers et les autorisations.

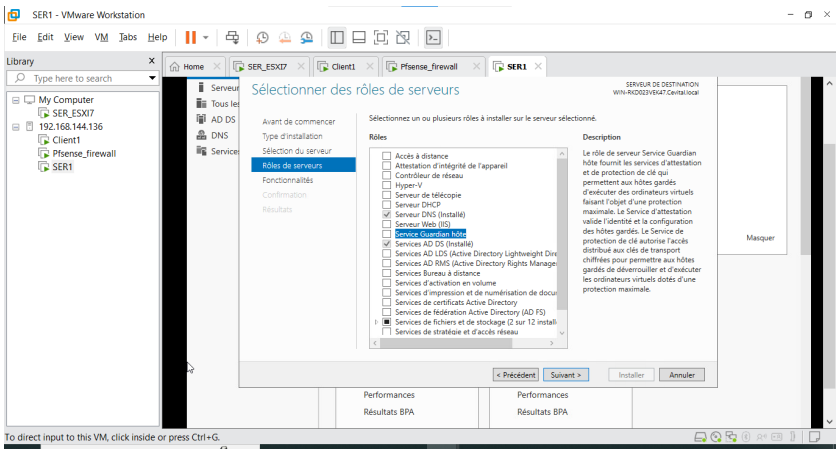
L'utilisation d'Active Directory dans VMWare permet de simplifier la gestion des ressources et des utilisateurs à travers l'infrastructure virtuelle. Pour ajouter Active Directory, il est nécessaire de passer par l'assistant de gestion des rôles. Il suffit de cocher la case "Serveur AD DS" et "Serveur DNS " puis on clique sur Ajouter des fonctionnalités, puis continuez l'assistant en cliquant sur Suivant.

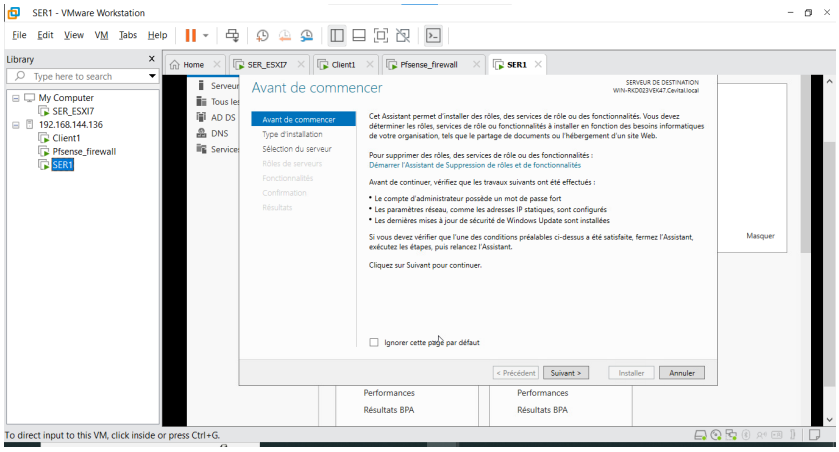




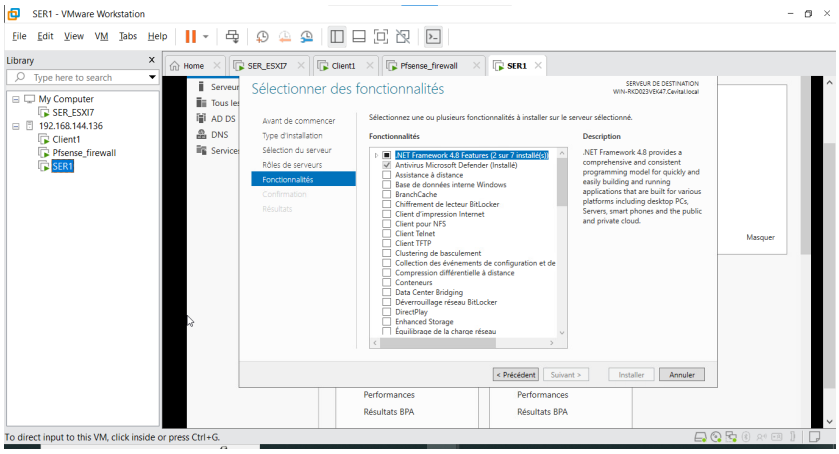

SER1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
SER_ESXI7
192.168.144.136
Client1
Pfsense_firewall
SER1
Home
SER_ESXI7
Client1
Pfsense_firewall
SER1
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
WIN-RKD023VEK47.Cevital.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
WIN-RKD023VEK47.Cevi...
10.1.20.100
Microsoft Windows Server 2022 Datacenter Evaluation
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler
Masquer
Performances
Résultats BPA
To direct input to this VM, click inside or press Ctrl+G.

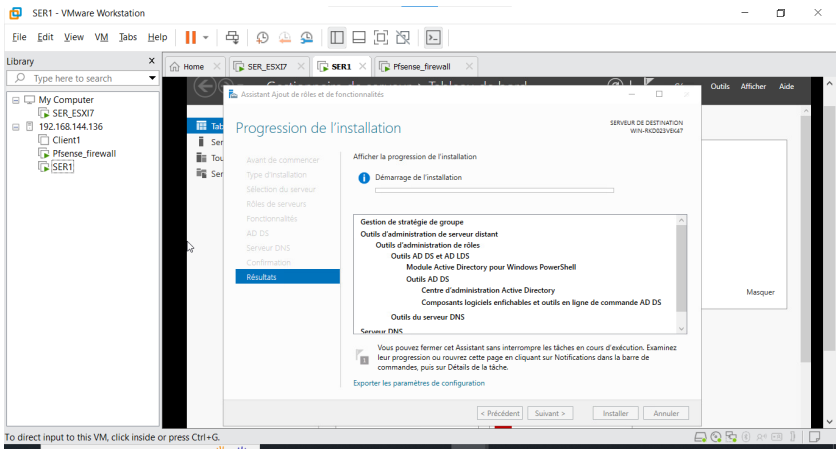

SER1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
SER_ESXI7
192.168.144.136
Client1
Pfsense_firewall
SER1
Home
SER_ESXI7
Client1
Pfsense_firewall
SER1
Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Service Guardian hôte ?
Vous ne pouvez pas installer Service Guardian hôte sauf si les services de rôle ou les fonctionnalités suivants sont également installés.
.NET Framework 4.8 Features
ASP.NET 4.8
Services WCF
Activation HTTP
Clustering de basculement
Outils d'administration de serveur distant
Outils d'administration de fonctionnalités
Outils de clustering avec basculement
[Outils] Outils de gestion du cluster de basculement
[Outils] Module Cluster de basculement pour Windo
Serveur Web (IIS)
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler
Masquer
Performances
Résultats BPA
To direct input to this VM, click inside or press Ctrl+G.


SER1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
SER_ESXI7
192.168.144.136
Client1
Pfsense_firewall
SER1
Home
SER_ESXI7
Client1
Pfsense_firewall
SER1
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
WIN-RKD023VEK47.Cevital.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS (Installé)
Serveur Web (IIS)
Service Guardian hôte
Services AD DS (Installé)
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (2 sur 12 install
Services de stratégie et d'accès réseau
Description
Le rôle de serveur Service Guardian hôte fournit les services d'attestation et de protection de clé qui permettent aux hôtes gardés d'exécuter des ordinateurs virtuels faisant l'objet d'une protection maximale. Le Service d'attestation valide l'identité et la configuration des hôtes gardés. Le Service de protection de clé autorise l'accès distribué aux clés de transport chiffrées pour permettre aux hôtes gardés de déverrouiller et d'exécuter les ordinateurs virtuels dotés d'une protection maximale.
< Précédent
Suivant >
Installer
Annuler
Masquer
Performances
Résultats BPA
To direct input to this VM, click inside or press Ctrl+G.

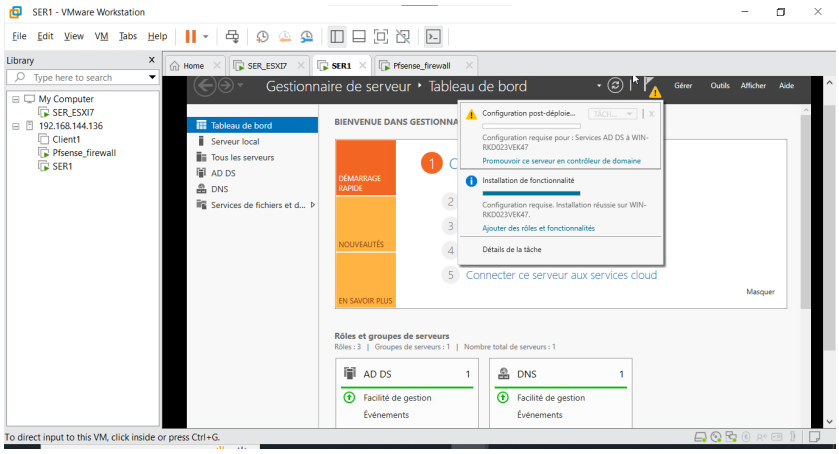


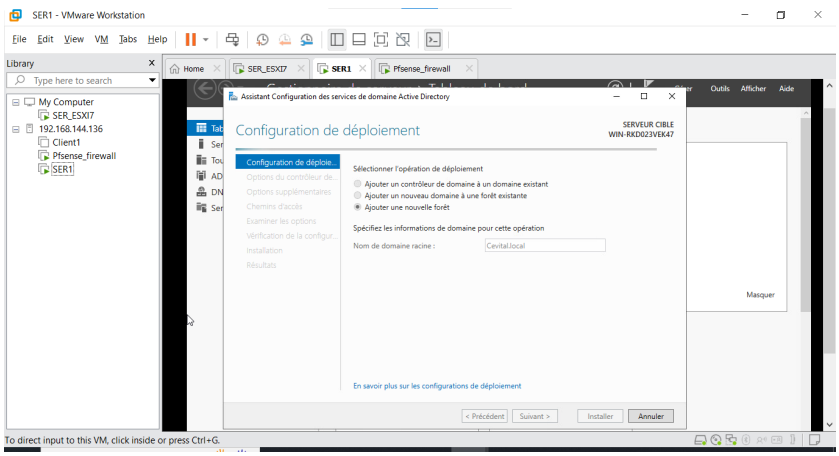
Dans les prochaines étapes, les fonctionnalités obligatoires ont été prés cochés. En cliquant sur "Suivant", tous les paramètres par défaut sont conservés. Ensuite, en cliquant sur "Installer", l'assistant procède à l'installation des services Active Directory Domain Services.



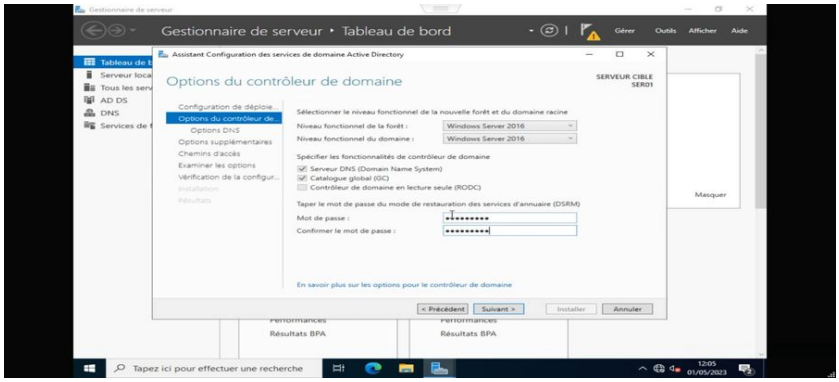


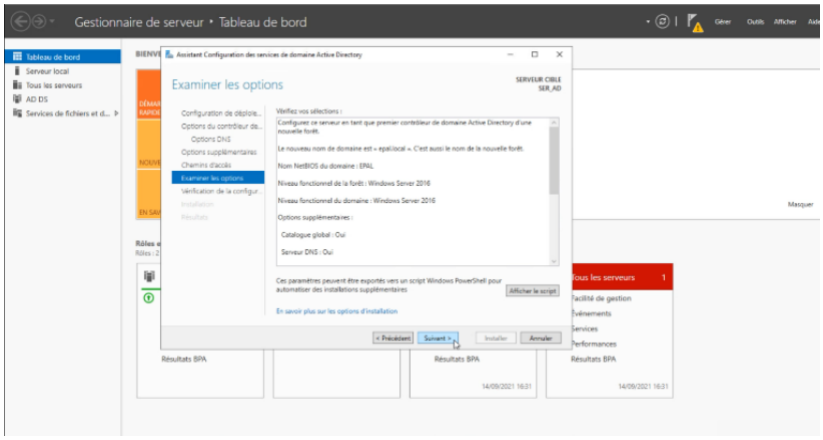
Pour transformer cet ordinateur en contrôleur de domaine, il est nécessaire de suivre des étapes supplémentaires. En cliquant sur "Promouvoir ce serveur en contrôleur de domaine", L'assistant de Configuration des services de domaine Active Directory se lance, on ajoute une forêt et on lui donne un nom de domaine.



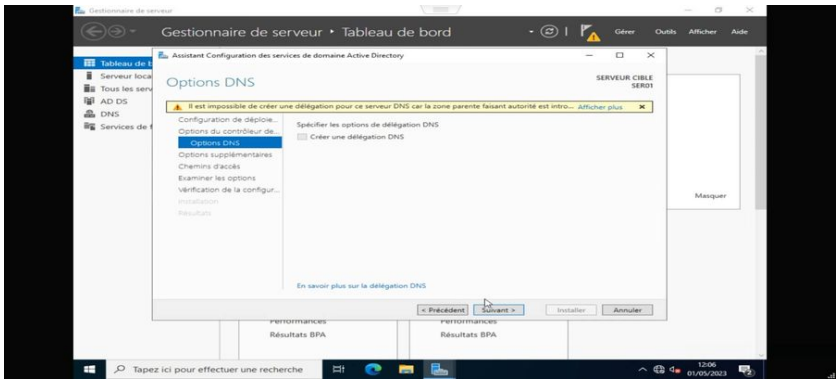


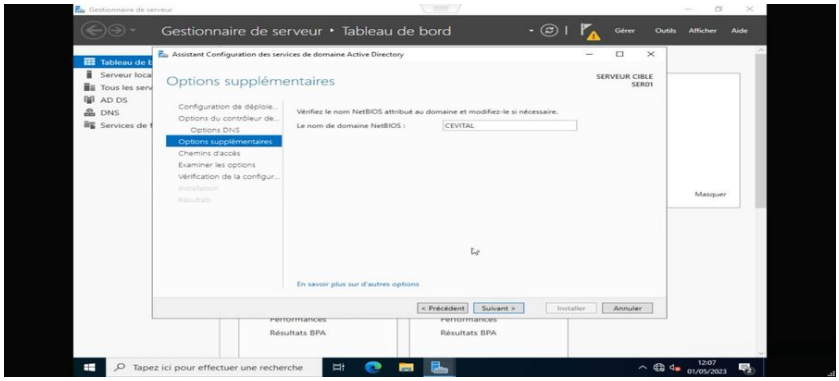
Ensuite, nous définissons le niveau fonctionnel de la forêt et du domaine, ainsi que le mot de passe. Ensuite, nous cliquons sur "Suivant".



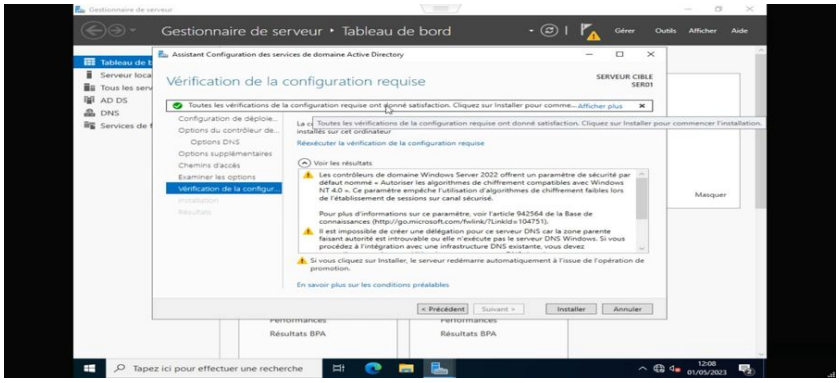


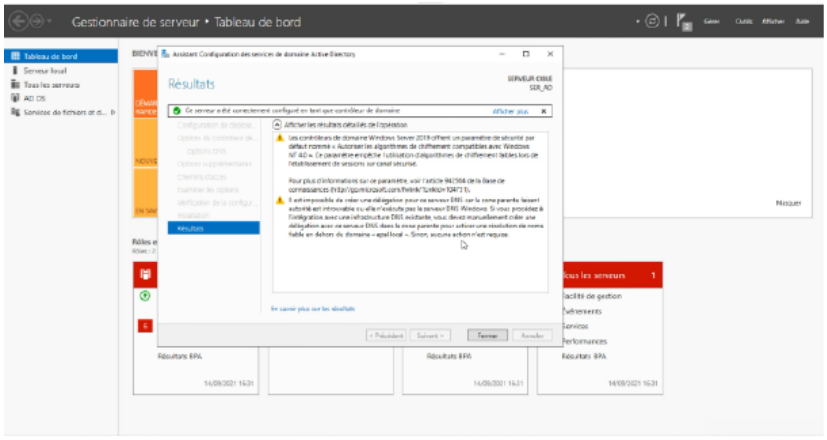
Dans toutes les étapes suivantes, on laisse les paramètres par défaut en cliquant sur suivant. Ici le nom NetBIOS de notre domaine est ensuite déterminé, on peut éventuellement le changer

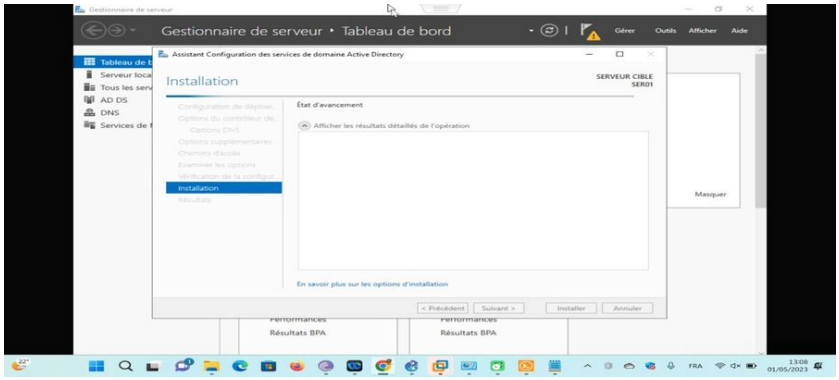




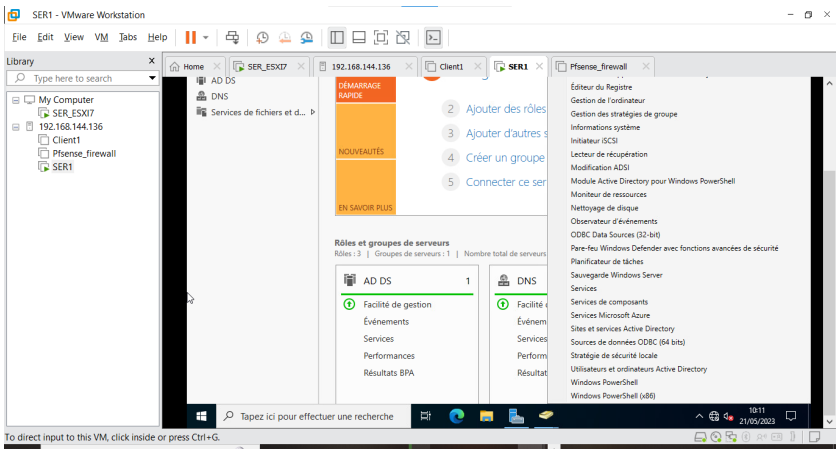
Un dernier écran récapitule notre configuration, puis nous cliquons sur "Installer" pour finaliser le processus. Une fois cette étape terminée, l'installation est achevée.

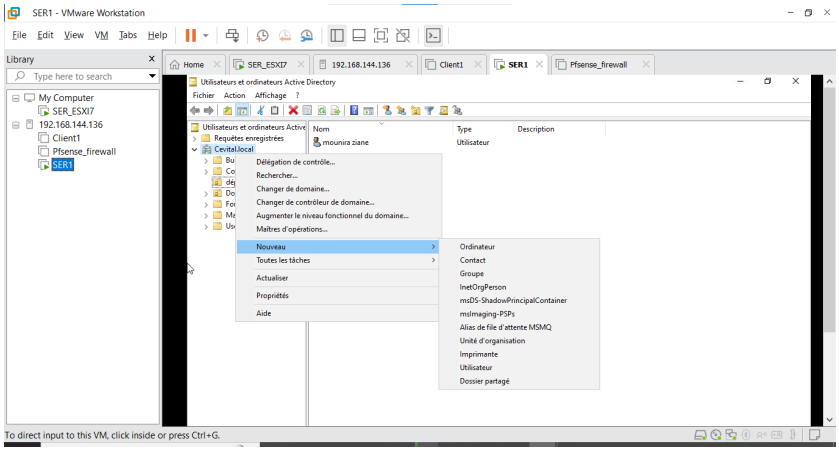




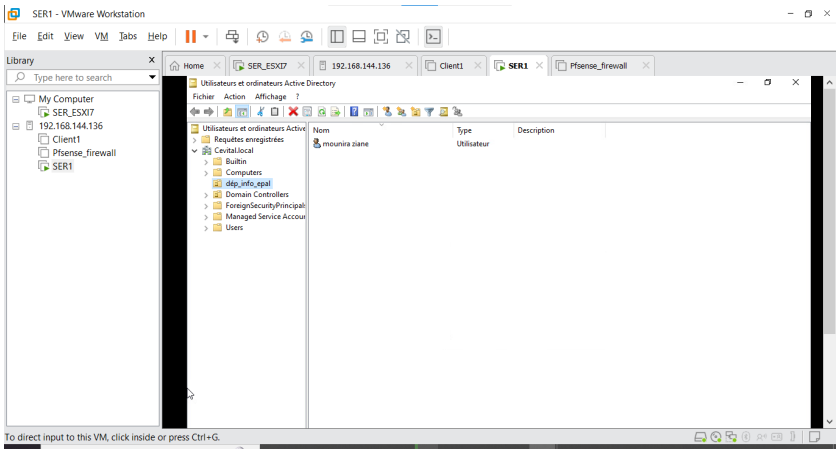


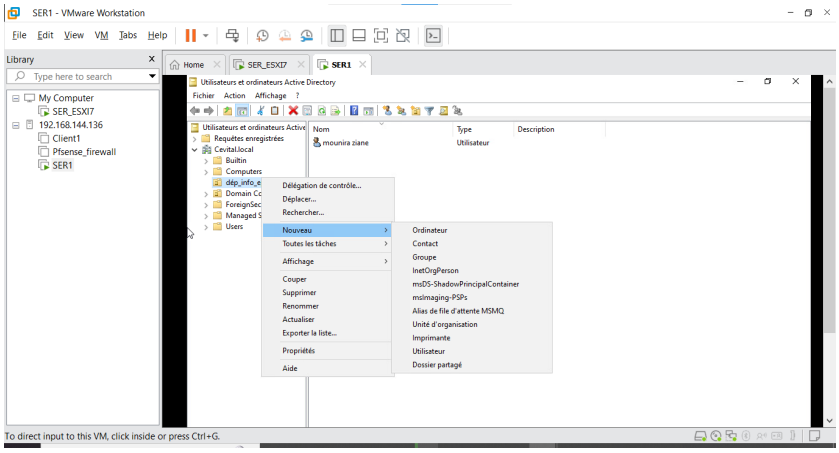
Création des utilisateurs, unité d'organisation et groupe : Ouvrir la console Utilisateurs et ordinateurs Active Directory. Faire un clic droit sur le domaine, aller sur Nouveau et l'on clique sur Unités d'organisation

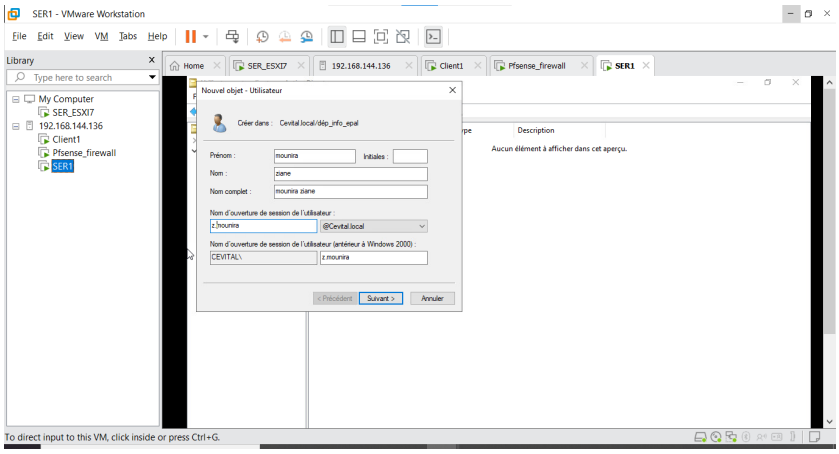


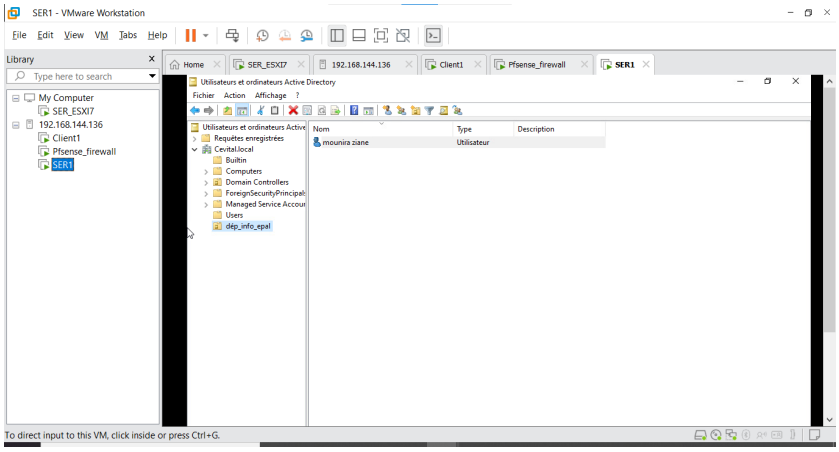


Nous commençons par attribuer un nom à notre unité d'organisation, puis nous cliquons sur "OK". Dans ce cas, nous avons créé une unité d'organisation appelée "dép-info-cev" (département informatique de cevital). À l'intérieur de cette unité, nous avons également créé une autre unité appelée "user" (utilisateurs), comprenant les utilisateurs Mounira et Nadjet (cette dernière étant créée dans une autre unité).

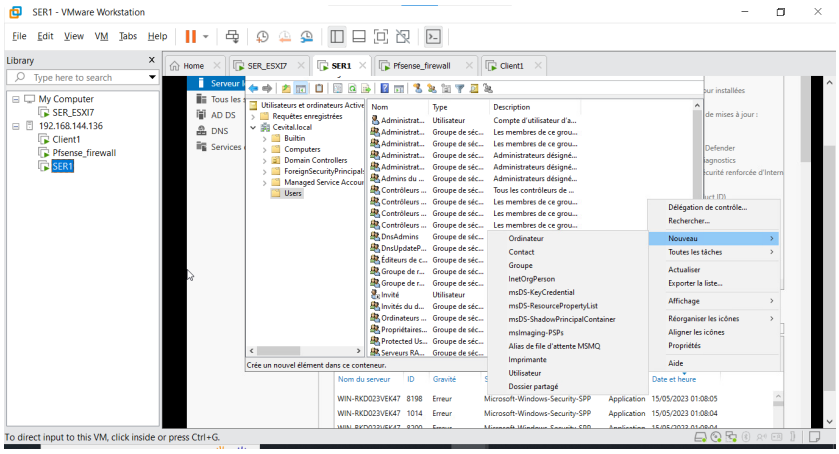


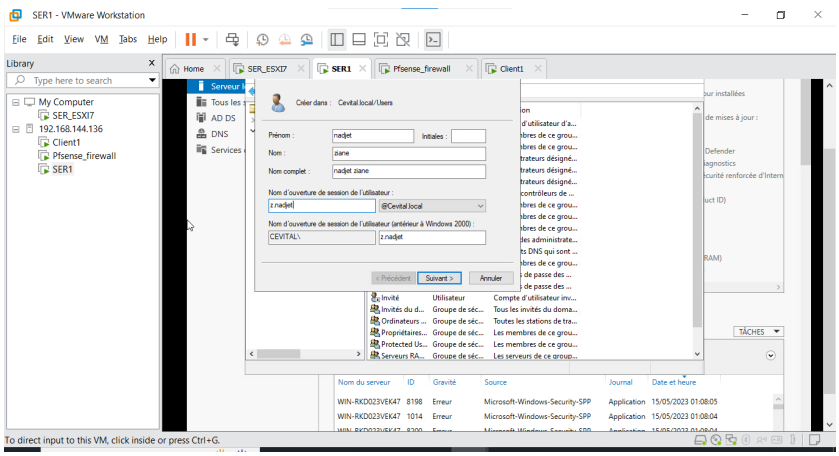




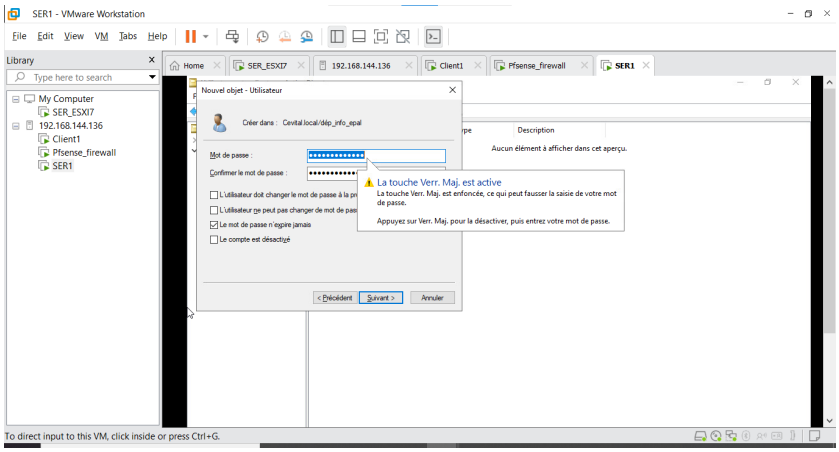


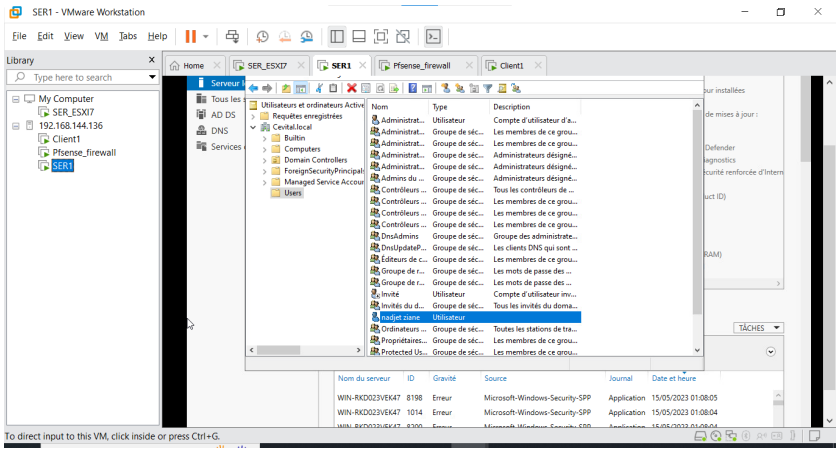
Clique droite sur user -> nouveau -> utilisateur, on entre le nom, prénom et l'identifiant de l'utilisateur qui est associé au domaine z.nadjet @Cevital.lovcal puis on clique sur suivant on (par la suite, on va ajouter cet utilisateur autant qu'administrateur de notre système depuis la machine client1)



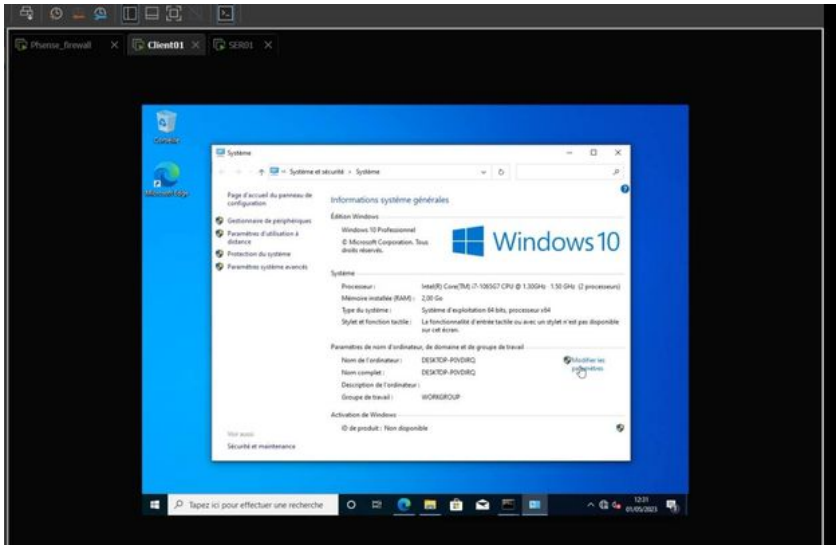


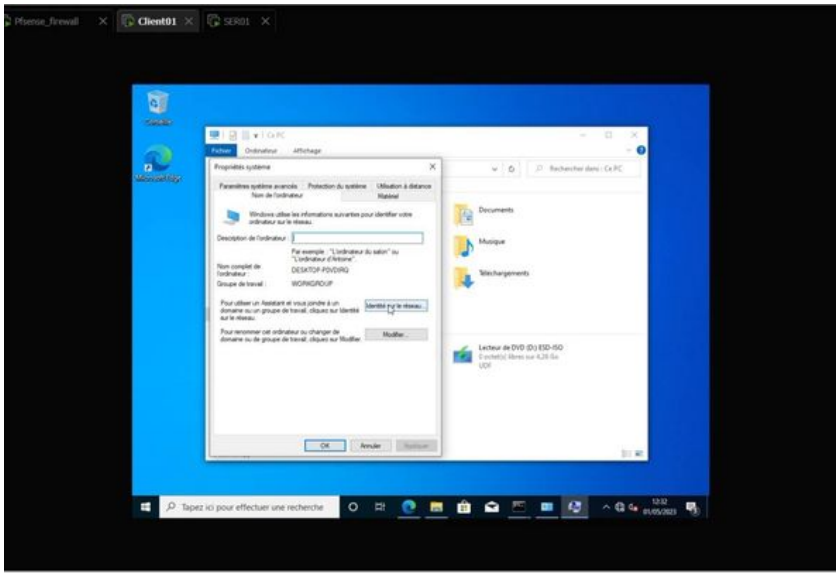
On choisit un mot de passe pour notre utilisateur et l'on choisit si le mot de passe reste fixe ou bien l'utilisateur pourra le changer puis on clique sur suivant et puis sur terminer pour ajouter notre utilisateur

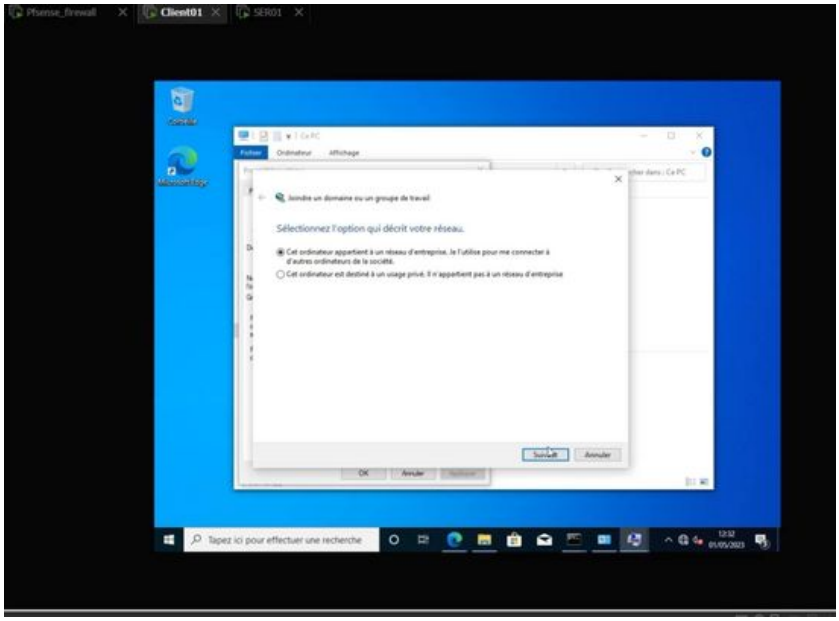


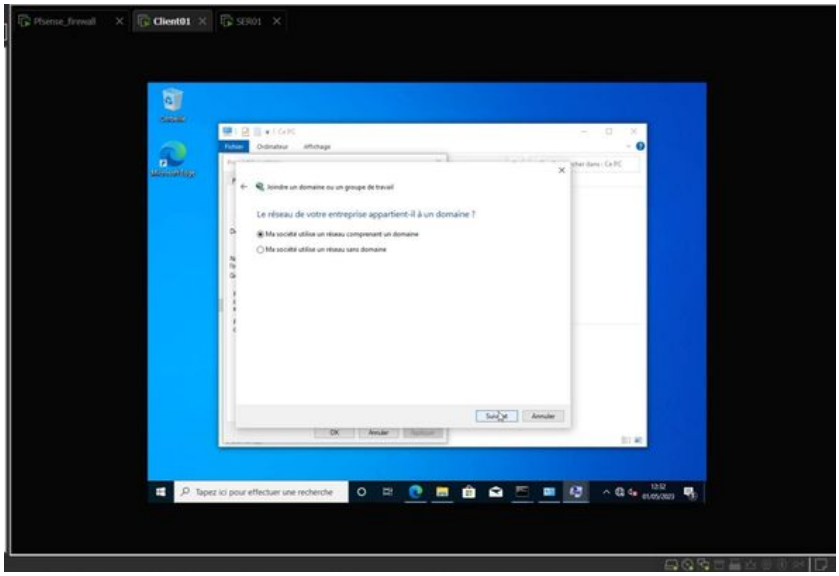


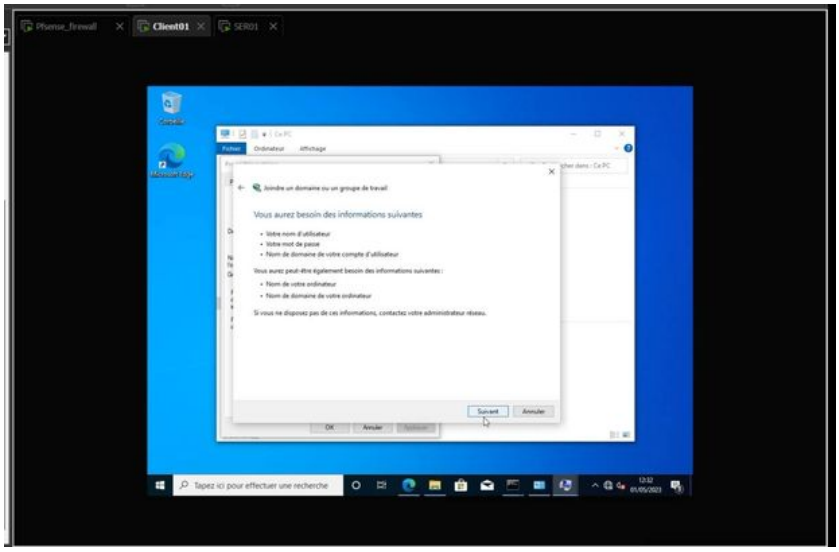
Ajouter client1 au domaine en tant qu'admin associé à un utilisateur : Lorsque nous cliquons sur "Identifier" sur le réseau, une fenêtre s'affiche, nous permettant de sélectionner les cases qui indiquent que notre ordinateur est connecté à un réseau d'entreprise et que notre entreprise possède un nom de domaine. Nous saisissons l'identifiant de notre utilisateur, préalablement créé dans l'Active Directory, ainsi que son mot de passe. L'utilisateur est ensuite associé à la machine "client1".

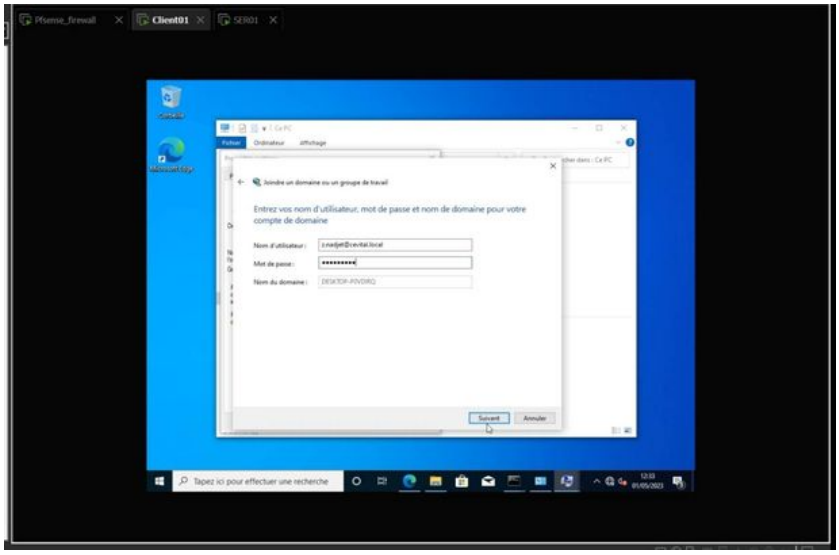



Pfsense_firewall
Client01
SER01
Propriétés système
Ce PC
Fichier
Ordinateur
Affichage
Documents
Musique
Téléchargements
Tapez ici pour effectuer une recherche

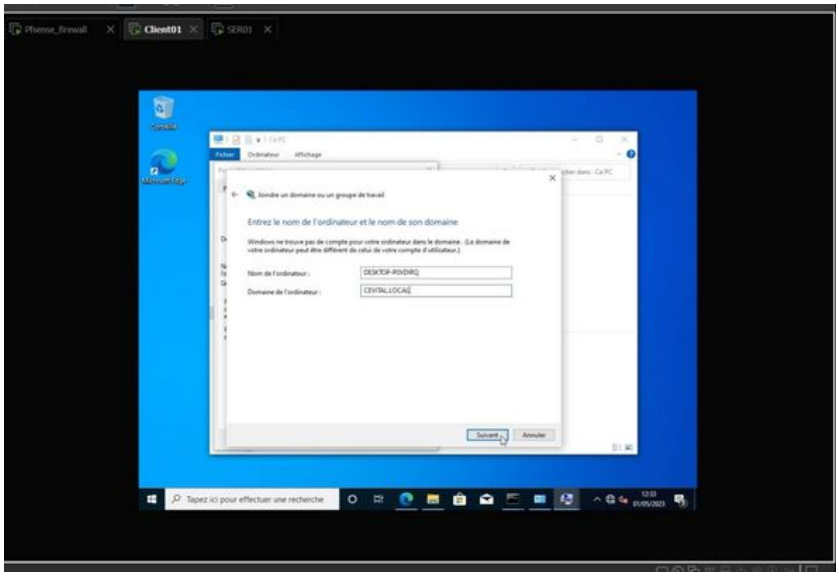

Pfsense_firewall
Client01
SER01
Joindre un domaine ou un groupe de travail
Sélectionnez l'option qui décrit votre réseau.
Cet ordinateur appartient à un réseau d'entreprise. Je l'utilise pour me connecter à d'autres ordinateurs de la société.
Cet ordinateur est destiné à un usage privé. Il n'appartient pas à un réseau d'entreprise
Suivant
Annuler
Tapez ici pour effectuer une recherche

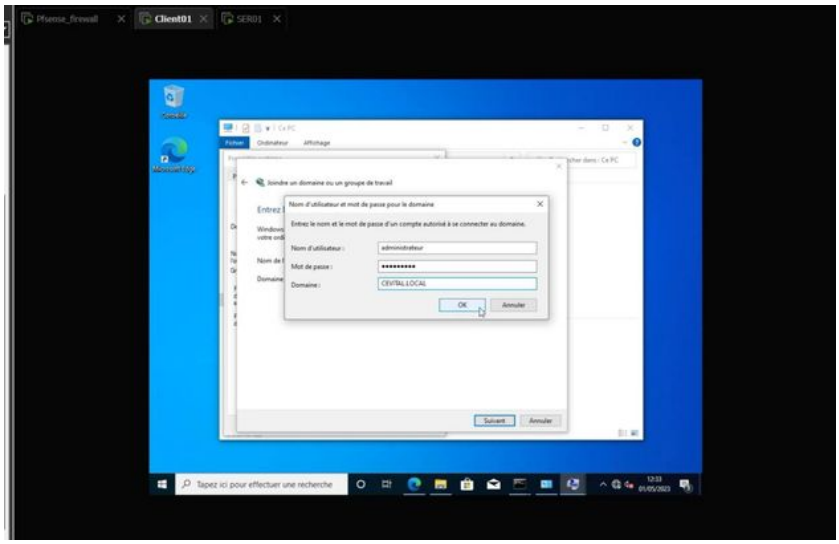

Pfsense_firewall
Client01
SER01
Joindre un domaine ou un groupe de travail
Le réseau de votre entreprise appartient-il à un domaine ?
Ma société utilise un réseau comprenant un domaine
Ma société utilise un réseau sans domaine
Suivant
Annuler
Tapez ici pour effectuer une recherche


Pfsense_firewall
Client01
SER01
Joindre un domaine ou un groupe de travail
Vous aurez besoin des informations suivantes
Votre nom d'utilisateur
Votre mot de passe
Nom de domaine de votre compte d'utilisateur
Vous aurez peut-être également besoin des informations suivantes :
Nom de votre ordinateur
Nom de domaine de votre ordinateur
Si vous ne disposez pas de ces informations, contactez votre administrateur réseau.
Suivant
Annuler
Tapez ici pour effectuer une recherche

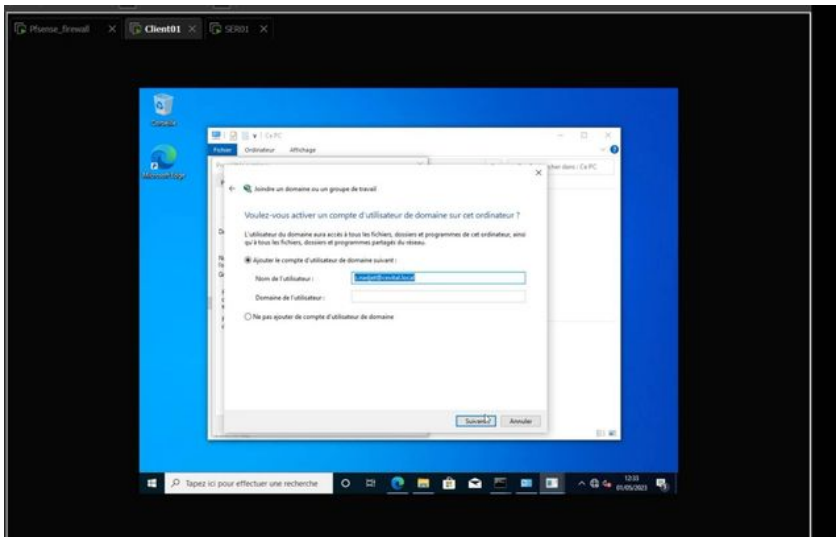

Pfsense_firewall
Client01
SER01
Joindre un domaine ou un groupe de travail
Entrez vos nom d'utilisateur, mot de passe et nom de domaine pour votre compte de domaine
Nom d'utilisateur :
Mot de passe :
Nom du domaine :
Suivant
Annuler
Tapez ici pour effectuer une recherche

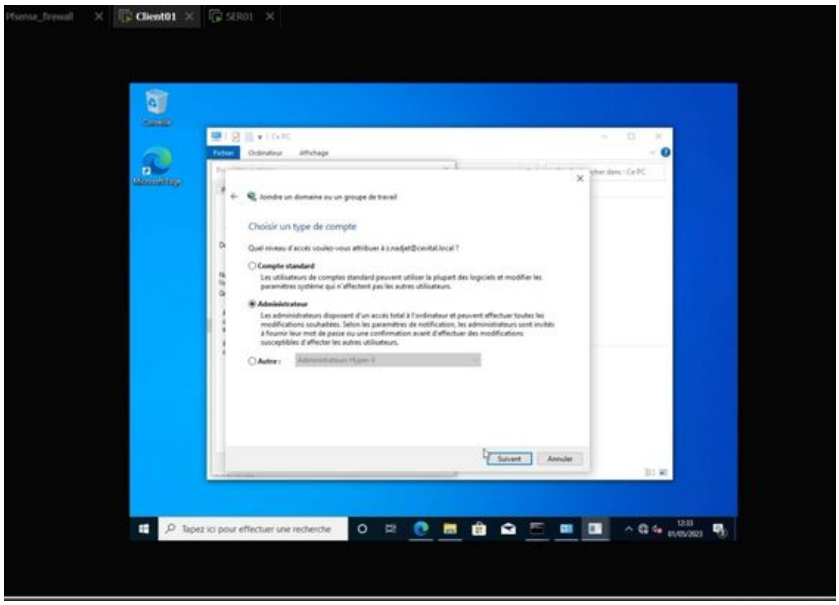
Après cela ont saisi le nom de notre domaine, s'authentifier pour autoriser à se connecter au domaine

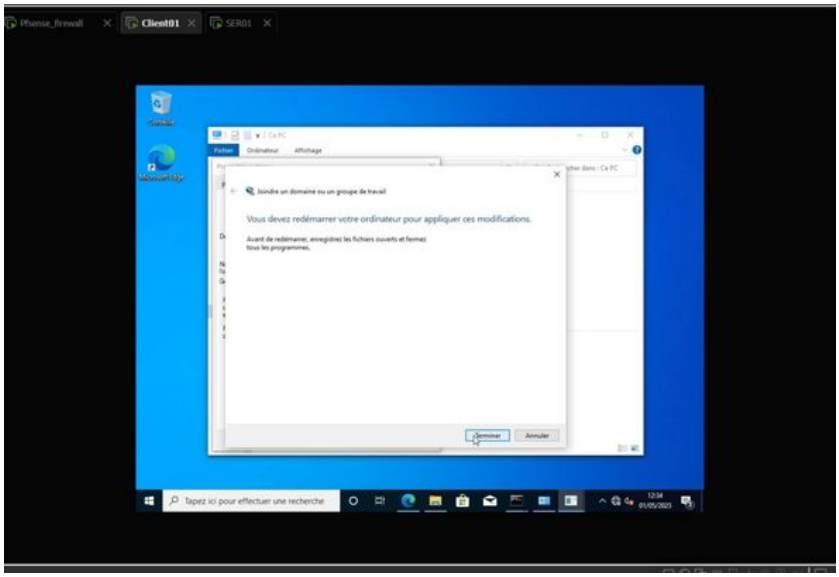


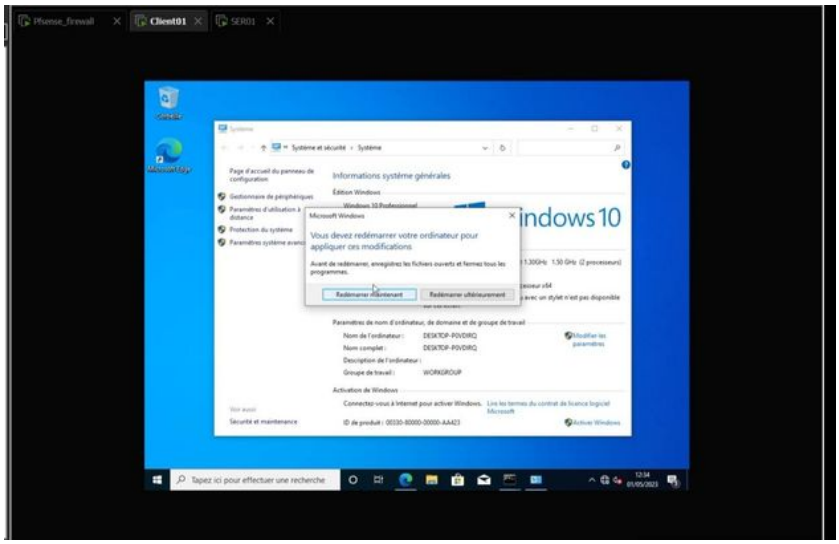


Nous activons le compte de l'utilisateur du domaine sur cet ordinateur (client1) et le sélectionnons comme administrateur. Ensuite, nous cliquons sur "Suivant", puis sur "Terminer", et redémarrons notre machine pour appliquer les configurations.





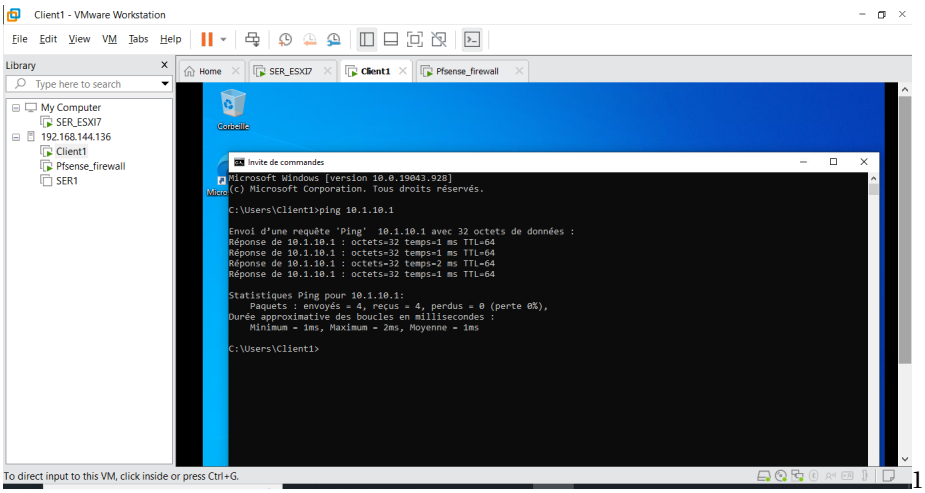

Pfsense_firewall
Client01
SER01
Joindre un domaine ou un groupe de travail
Vous devez redémarrer votre ordinateur pour appliquer ces modifications.
Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.
Terminer
Annuler
Tapez ici pour effectuer une recherche


Pfsense_firewall
Client01
SER01
Informations système générales
Microsoft Windows
Vous devez redémarrer votre ordinateur pour appliquer ces modifications
Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.
Redémarrer maintenant
Redémarrer ultérieurement
Paramètres de nom d'ordinateur, de domaine et de groupe de travail
Activation de Windows
Tapez ici pour effectuer une recherche

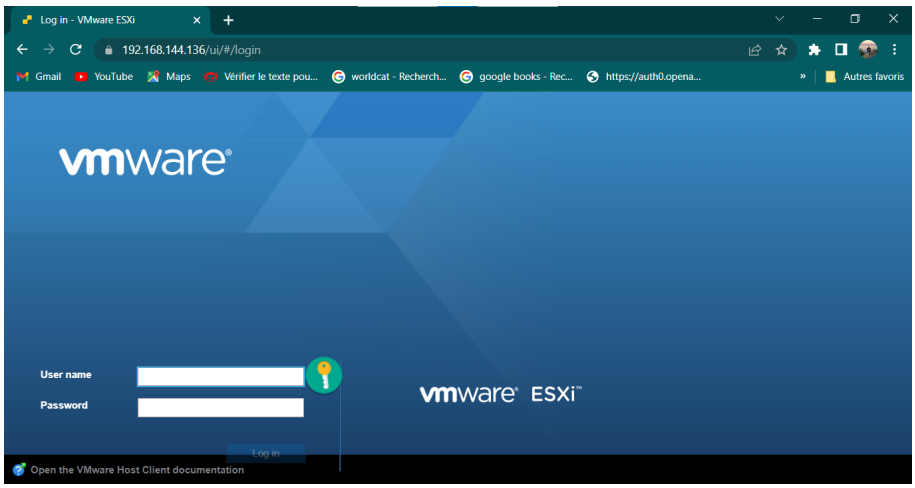
4.4 Partie II : Test

4.4.1 ESXI

On ping l'adresse de management pour tester notre ESXI.

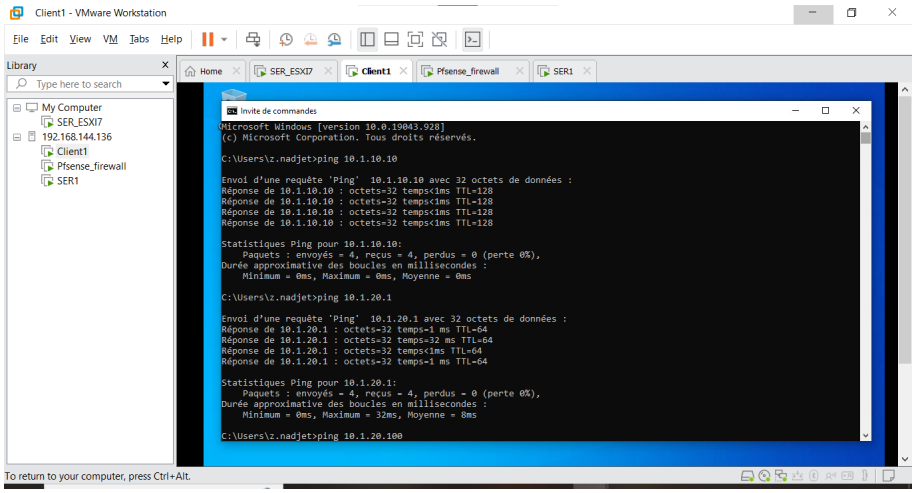

1

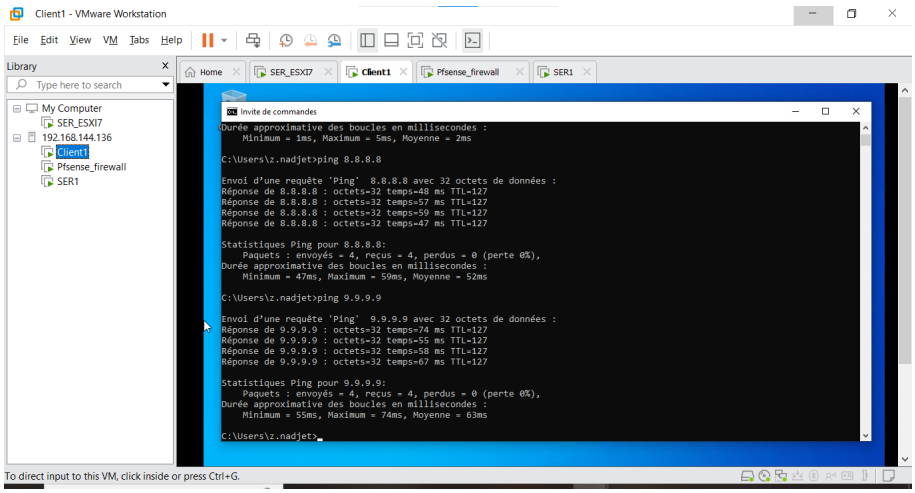
L'interface graphique de notre ESXI.



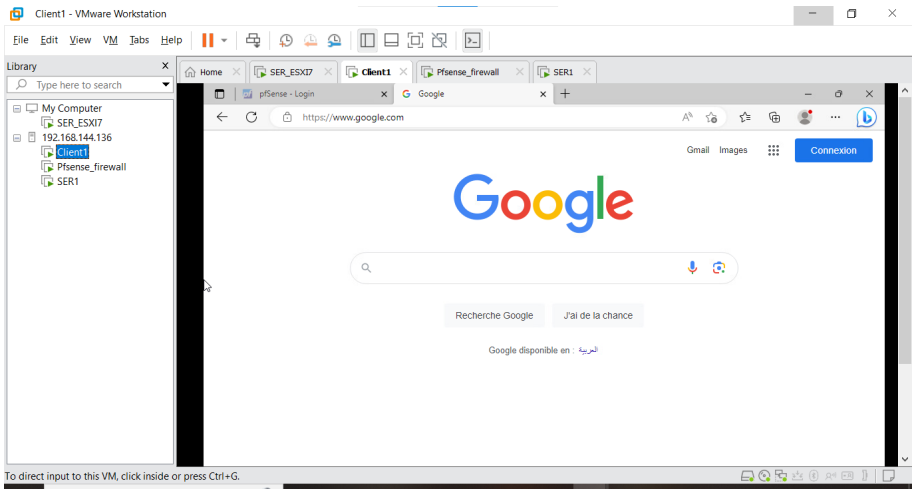
4.4.2 Firewall

Nous effectuons un ping sur toutes les interfaces de notre pare-feu. Notre pare-feu autorise le trafic entrant et sortant entre les segments client/serveur. Nous testons ensuite la connexion vers l'extérieur (Internet).



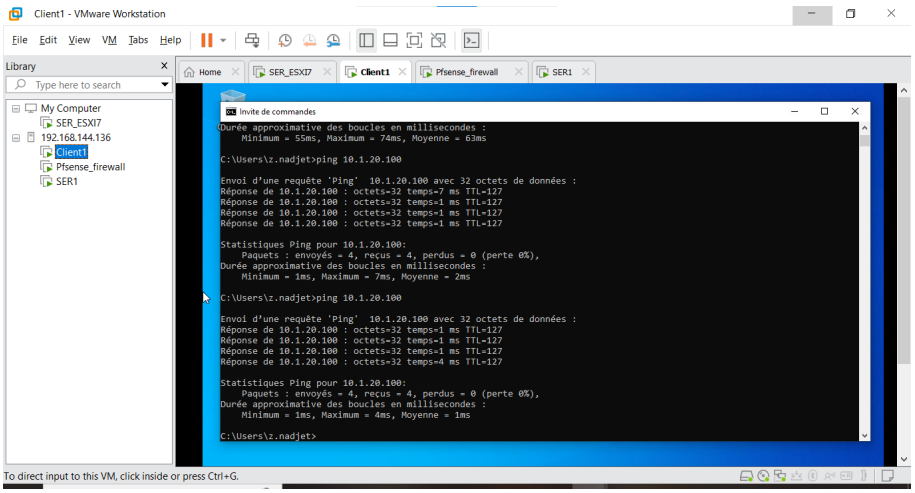


Test du trafic vers l'extérieur (connexion internet)

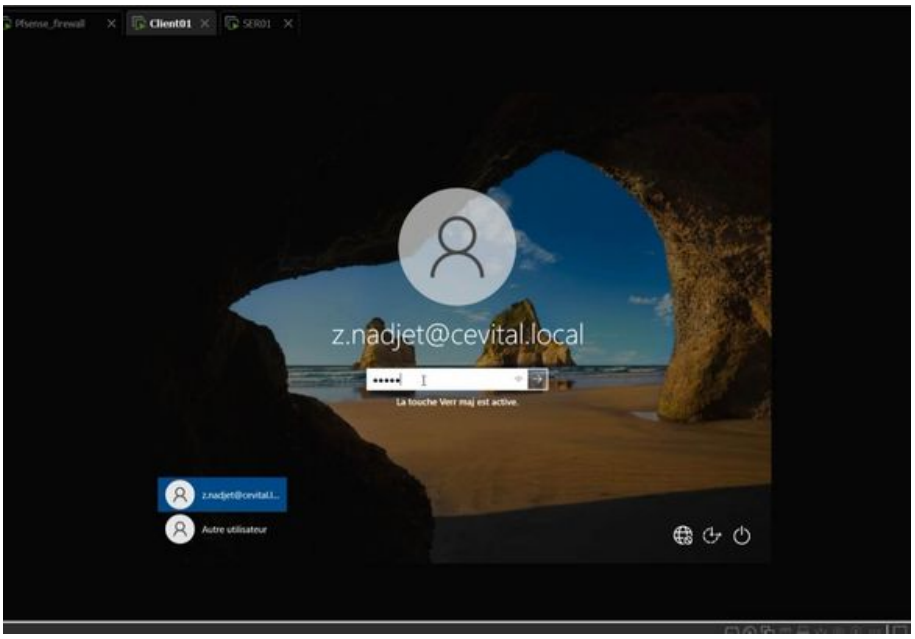


4.4.3 Les serveurs

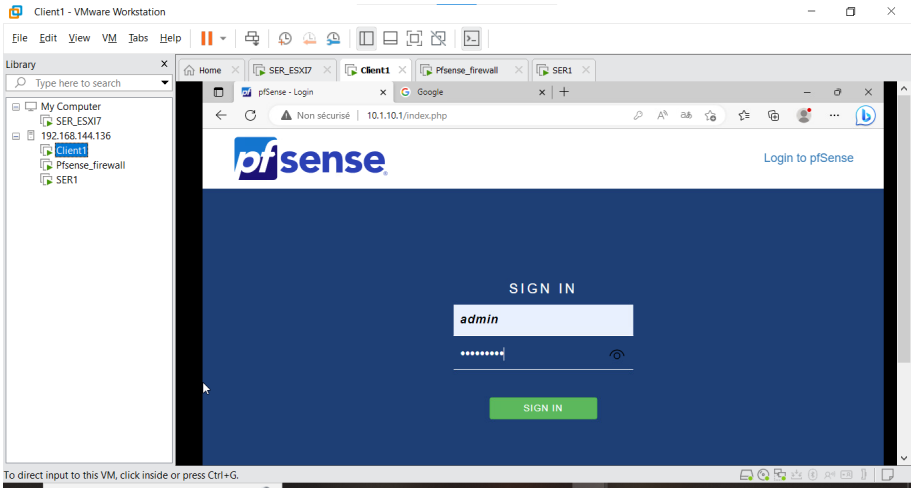
1. **Serveur Active Directory :** On ping le serveur AD-DNS depuis la machine clinet1 avec l'adresse 10.1.20.100



L'utilisateur peut s'authentifier en tant qu'administrateur depuis la machine client1.



2. **Serveur DNS :** Une fois que nous avons ajouté notre pare-feu à notre serveur DNS avec un nom d'hôte, nous pouvons actuellement accéder à notre pare-feu en utilisant son nom plutôt que son adresse IP depuis la machine client1.



4.5 conclusion

Dans ce chapitre, nous avons récemment déployé l'infrastructure réseau sur une plateforme virtuelle en utilisant la technologie de l'hyperviseur ESXi. Cette infrastructure prend en charge les différents systèmes d'exploitation, Windows serveur 2022, Windows 10 et free BSD, pfSense pour le firewall, les performances de chaque machine virtuelle sont optimisées, Nous avons in stallé, un serveur AD DNS DHCP : qui prend en charge les utilisateurs les trier par groupe dans une unité d'organisation, la distribution d'adresser IP et la connexion et accès avec le nom de domaine. Nous avons mis en place un pare-feu qui nous permet de contrôler le trafic entrant et sortant ainsi que la connectivité entre nos deux segments client et serveur. De plus, nous disposons d'une machine cliente sous Windows 10. Grâce à cette technique de virtualisation, les performances élevées de la machine physique sont désormais optimisées.

Conclusion générale

En conclusion, ce mémoire sur l'étude et la mise en place d'une solution de virtualisation a permis d'approfondir notre compréhension de cette technologie et de ses implications dans le domaine de l'informatique. La virtualisation offre de nombreux avantages, notamment en termes de sécurité, de stabilité et d'optimisation des ressources. L'étude nous a permis de comprendre comment la virtualisation permet d'isoler les systèmes d'exploitation et les applications au sein de machines virtuelles, minimisant ainsi les risques de propagation des erreurs ou des attaques. Nous avons également pu constater comment elle permet une meilleure utilisation des ressources matérielles, en consolidant plusieurs machines virtuelles sur une seule machine physique, ce qui entraîne des économies de coûts, d'espace et d'énergie.

La mise en place de la solution de virtualisation a été une étape importante de ce mémoire, nous permettant de mettre en pratique les connaissances acquises et de constater les résultats concrets. Nous avons pu observer les améliorations en termes de performances, de flexibilité et de gestion des ressources grâce à la virtualisation.

En termes de perspectives, la virtualisation continuera d'évoluer et de jouer un rôle crucial dans le domaine de l'informatique. Les avancées technologiques telles que la virtualisation des réseaux et des fonctions réseau ouvrent de nouvelles opportunités pour une gestion plus efficace des infrastructures informatiques. De plus, l'intégration de la virtualisation avec d'autres technologies émergentes telles que le cloud computing et l'intelligence artificielle offre des perspectives passionnantes pour l'innovation et la transformation numérique.

En conclusion, ce mémoire nous a permis de comprendre les avantages et les implications de la virtualisation, ainsi que d'acquérir une expérience pratique dans la mise en place d'une solution de virtualisation. La virtualisation continuera de façonner le paysage informatique à l'avenir, offrant des opportunités d'amélioration continue des performances, de la sécurité et de l'efficacité des systèmes informatiques.

Bibliographie

[1] Rziza Mohammed, université d'Angers, Cours des réseaux Informatiques (2010-2011), ouargla.dz.

[2] Jean-François Pillou, Tout sur les réseaux et Internet, DUNOD 2006.

[3] BOUIMEDJ Lynda, Étude et mise en place des réseaux locaux virtuels. Mémoire de Master en Informatique. Option : Réseaux et systèmes distribués : Université A/Mira de Bejaia, 2016/2017

[4] Pillou.J. Tout sur les réseaux et internet, Livre. Dunod, 2007, 5 édition.

[5] LAHDIR.M et MEZARI.R. Réseaux Locaux. Livre, Éditions Pages Bleus, 2006.

[6] https ://www.ionos.fr/digitalguide/serveur/know-how/cidr,04/04/2019 .

[7] http ://www.frameip.com/tcpip/, 2003

[8] https ://www.laboutiqueafricavivre.com/livres-specialises/174841-concevoir-la-securite-informatique-en-entreprise-9786202263252.html

[9] https ://pastel.archives-ouvertes.fr/pastel-00001492/document,2005

[10] GILBERT Held, les réseaux locaux virtuels, Conception, mise en œuvre et administration. Aout 1998.

[11] REMAZEILLES.V. La sécurité des réseaux avec Cisco, livre. Édition ENI, février 2009.

[12] B. Vachons. CCNA Security (210-260) Portable Command Guide. Global Édition-Pearson, 2016.

[13] http ://www.volle.com/travaux/couchessi.htm,2002

[14] MAILLÉ E, VMWare vSphere4,4 éme édition, Edition sENI, janvier 2010.

[15] https ://www.universalis.fr/encyclopedie/systemes-informatiques-systemes-d-aide-a-la-decision/2-differences-entre-un-systeme-operationnel-et-un-systeme-decisionnel

[16] FOURNEBERTONJHEURTINM, VMWare vSphere 6,6 éme édition, EditionsENI, janvier 2017.

[17] https ://www.hpe.com/ca/fr/what-is/virtualization.html,Copyright 2023

[18] MAILLÉ E, VMWare vSphere 4, 4 éditions, Éditions ENI, janvier 2010.

[19] https ://www.ws.afnog.org/afnog2014/ssf/docs/ssf(-) virtualisation-opensource.pdf

[20] Elies Jebri, « Introduction à la sécurité », support de cours, 2008

[21] https ://www.senat.fr/rap/r20-678/r20-678.mono.html,2021

[22] https ://journals.openedition.org/activites/4941,2020

[23] https ://www.heavy.ai/technical-glossary/local-area-network

[24] https ://community.fs.com/fr/blog/lan-vs-man-vs-wan-whats-the-difference.html

[25] https ://www.malekal.com/les-differents-types-de-reseaux-lan-wan-man/

[26] https ://www.quizz.biz/quizz-409783.html

[27] http ://sadky.ismail.free.fr/electrar/cours/reseaux/page2.htm

[28] http ://notionsinformatique.free.fr/reseaux/topologie.html

[29] https ://www.memoireonline.com/07/10/3707/m-Systeme-de-gestion-des-nouveau-nes-de-la-conception–la-mise-en-reseau0.html

[30] https ://fr.wikipedia.org/wiki/Carte-r

[31] https ://le-routeur-wifi.com/switch-ethernet-commutateur/

[32] http ://castilloje.free.fr/tsti2d/tsti2d-ett-tp/02-decouverte-des-reseaux/simul-hub/index.html?Commutateur.html

[33] https ://www.cnetfrance.fr/produits/meilleurs-routeurs-wifi-39869017.htm

[34] https ://www.bytecode.ch/produits-services-informatique/pare-feu/

[35] https ://www.tech2tech.fr/windows-server-2016-installer-un-controleur-de-domaine-adds-dns/

[36] https ://choquantecp.medium.com/c

[37] https ://fr.wikipedia.org/wiki/Paire-torsad

[38] http ://for-ge.blogspot.com/2015/05/fibre-optique.html

[39] https ://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/

[40] https ://www.weodeo.com/digitalisation/qu-est-ce-que-la-virtualisation-et-pourquoi-virtualise-t-on/

[41] https ://www.coeurduweb.com/blog/2014/03/28/virtualisation-serveur/

[42] http ://commentgeek.com/virtualbox-vmware-hyper-quelle-meilleure-machine/

Résumé

L'objectif principal de ce projet est de virtualiser les serveurs de Cevital, qui jouent un rôle essentiel dans la gestion de l'entreprise, la sécurité des données et la disponibilité des services.
Pour mettre en œuvre ce projet, nous avons opté pour la virtualisation de chaque serveur en utilisant l'hyperviseur ESXI (il existe deux types 1 et 2). nous avons créé deux machines virtuelles (SER01 et Client1) Après cela, nous avons procédé à la configuration de chaque serveur, en mettant l'accent sur des éléments clés tels que les serveurs AD DNS, WEB, ainsi que l'installation d'un pare-feu pfSense pour renforcer la sécurité de notre réseau.

Enfin, nous avons effectué des tests pour vérifier la connectivité et le bon fonctionnement de chaque serveur, ainsi que l'interaction entre eux et les services qu'ils fournissent, tout en assurant une gestion centralisée et des flux de données entrants et sortants sécurisés.

Mots clés : ESXI, AD, DNS, DHCP, WEB, serveur, firewall, hyperviseurs.

Abstract

The main objective of this project is to virtualize Cevital servers, which play a crucial role in the management of the company, data security, and service availability.

To implement this project, we opted for the virtualization of each server using the ESXI hypervisor (there are two types, type 1 and type 2). We created two virtual machines (SER01 and Client1). Afterward, we proceeded with the configuration of each server, focusing on key elements such as AD DNS servers, web servers, and the installation of a pfSense firewall to enhance network security.

Finally, we conducted tests to verify the connectivity and proper functioning of each server, as well as the interaction between them and the services they provide. We ensured centralized management and secure incoming and outgoing data flows.

Keywords : ESXI, AD, DNS, DHCP, WEB, server, FTP, firewall, hypervisor.