République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications

Thème

Etude et conception de la haute disponibilité et du clustering dans un environnement de virtualisation.

Préparé par :

- M[lle] MAHINDAD Melissa
- M[lle] KERKOUR Melissa

Dirigé par :

M. BELLAHSENE Hocine

M.LATRECHE Sofiane

M.IMLOUL Fatah

Examiné par :

M.BERRAH Smail (Président)

Mme. MAMMERI Karima (Examinatrice)

Année universitaire : **2023/2024**

Remerciements

Avant d'entrer dans le vif du sujet, nous tenons à exprimer notre profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Nous remercions tout particulièrement notre superviseur, M.Bellahsene, pour son encadrement, ses conseils avisés et son soutien constant tout au long de ce travail. Ses suggestions précieuses et ses encouragements ont grandement contribué à la qualité de ce travail. Sans oublier M. Latreche pour son accompagnement.

Nous tenons également à remercier notre tuteur de stage, M.Imloul, pour son accompagnement attentif, et sa disponibilité tout au long de notre expérience en entreprise. Son expertise nous a été d'une aide précieuse dans la réalisation de ce mémoire.

Nous adressons nos remerciements sincères à l'ensemble des membres du jury pour avoir accepté d'évaluer ce mémoire.

Nous sommes reconnaissantes envers nos professeurs et collègues du département ATE pour leur soutien et leurs encouragements durant toute la durée de nos études.

Nous voudrions aussi exprimer notre gratitude à toutes les personnes qui ont participé à ce travail, notamment M.Djebarri, pour ses précieux conseils.

Nous tenons à exprimer notre gratitude particulière envers nos familles pour leur soutien inconditionnel et leurs encouragements tout au long de cette aven-

ture académique. Leur patience infinie et leur compréhension sans faille ont été d'un grand réconfort et ont joué un rôle crucial dans notre réalisation de cet accomplissement.

Enfin, nous tenons à remercier toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire.

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

AD DS : Active Directory Domain Services.
AES : Advanced Encryption Standard.
API : Application Programming Interface.
BDD : Base de Données.
CARP : Common Address Redundancy Protocol.
CLI : Command Line Interface.
CP/CMS : Control Program/Cambridge Monitor System.
CPU : Central Processing Unit.
DC : Domaine Controler.
DDN : Direction de la Digitalisation Numérique.
DH : Diffie-Hellman.
DHCP : Dynamic Host Configuration Protocol.
DMZ : Demilitarized Zone.
DNS : Domain Name System.
DSRM : Directory Services Restore Mode.
EPB : Entreprise Portuaire de Bejaia.
ESP : Encapsulating Security Payload.
FQDN : Fully Qualified Domain Name.
GED : Gestion Electronique de Document.
GNS3 : Graphical Network Simulator 3.
GUI : Graphical User Interface.
HA : High Availability.
HPC : High Performance Computing.
HTTP : HyperText Transfer Protocol.
HTTPS : HyperText Transfer Protocol Secure.

IBM : International Business Machines Corporation.

ICMP : Internet Control Message Protocol.

IEEE : Institute of Electrical and Electronics Engineer.

IKE : Internet Key Exchange.

IP : Internet Protocol.

IPsec : Internet Protocol Security.

IPv4 : Internet Protocol version 4.

ISP : Internet Service Provider.

ISO : International Organization for Standardization.

KVM : Kernel-based Virtual Machine.

LACP : Link Agregation Control Protocol.

LAN : Local Area Network.

LB : Load Balancing.

LVM : Logical Volume Manager.

LXC : Linux Containers.

MOTD : Message Of The Day.

MTBF : Mean Time Between Failure.

MTTR : Mean Time To Recovery.

NAS : Network Attached Storage.

NAT : Network Address Translation.

NFV : Network Function Virtualization.

OD : Objectif de Disponibilité.

OS : Operating System.

PVLAN : Private Virtual Local Area Network.

QoS : Quality of Service.

RAM : Random-Access Memory.

RPO : Recovery Point Objective.

RTO : Recovery Time Objective.

SAN : Storage Area Network.

SDN : Software-Defined Networking.

SHA : Secure Hash Algorithm.

SIP : Système d'Information Portuaire.

SPOF : Single Point Of Failure.

SSH : Secure SHell.

STONITH : Shot The Other Node In The Head.

STP : Spanning Tree Protocol.

Telnet : Teletype Network Protocol.

TCP : Transmission Control Protocol.

TLS : Transport Layer Security.

UDP : User Datagram Protocol.

VIP : Virtual Internet Protocol.

VLAN : Virtual Local Area Network.

VM : Virtual Machine.

VMM : Virtual Machine Monitor.

VPN : Virtual Private Network.

VRF : Virtual Routing and Forwarding.

VTP : VLAN Trunking Protocol.

WAN : Wide Area Network.

ZFS : Zettabyte File System.

Introduction générale

Dans un monde en constante évolution technologique, les entreprises se doivent d'ajuster régulièrement leurs infrastructures réseau afin de satisfaire les demandes croissantes en termes de performance et de disponibilité. Cette adaptation devient encore plus importante dans les contextes où les systèmes d'information jouent un rôle central dans les opérations quotidiennes. Dans le cadre de cette dynamique, ce mémoire examine diverses méthodes et technologies visant à améliorer et à protéger les infrastructures réseaux et systèmes des pannes potentielles.

Pour atteindre cet objectif, nous allons structurer ce travail en quatre chapitres. Le premier chapitre présentera l'organisme d'accueil de façon générale et se concentrera plus particulièrement sur les problématiques rencontrées dans la gestion de son infrastructure réseau, servant de justification pour les travaux menés dans le cadre de ce mémoire.

Le deuxième chapitre traitera la virtualisation des systèmes et des réseaux, en exposant les avantages, les concepts fondamentaux de la virtualisation ainsi que les différentes technologies utilisées pour créer un environnement de virtualisation et optimiser l'efficacité des infrastructures réseau.

Le troisième chapitre sera focalisé sur la haute disponibilité et le clustering. Il détaillera les différentes stratégies de haute disponibilité et de clustering utilisées pour améliorer la disponibilité des réseaux et des services critiques dans les environnements où les interruptions de service peuvent entraîner des répercussions importantes.

Enfin, le dernier chapitre nous proposerons une nouvelle architecture réseau

conçue pour améliorer la durabilité de l'infrastructure réseau dans un environnement de virtualisation, et ce en s'appuyant sur les problématiques identifiées ainsi que les connaissances acquises dans les chapitres précédents. Nous détaillerons les configurations ainsi que les résultats des simulations menées pour tester l'efficacité des changements proposés.

À travers ces quatre chapitres, ce mémoire vise à fournir un aperçu des défis auxquels l'organisme d'accueil est confronté ainsi que des solutions mises en place pour y faire face. En combinant théorie et pratique, nous espérons contribuer à une compréhension plus approfondie des enjeux liés à la gestion des infrastructures réseaux dans des contextes professionnels exigeants.

Chapitre 1

Contexte du travail

Introduction

Afin d'introduire notre travail, nous commençons par ce chapitre qui sera réservé à la présentation de l'entreprise portuaire de Béjaia (EPB), où nous avons effectué notre stage. Dans un premier temps, nous aborderons un aperçu concis de l'entreprise pour mieux comprendre sa structure et ses objectifs. Par la suite nous étudierons l'architecture réseau de l'EPB ainsi que ses composantes afin de pouvoir proposer d'éventuelles améliorations.

1.1 Présentation générale de l'organisme d'accueil

Au-delà de sa fonction d'accueillir des navires du monde entier, le port de Béjaïa possède une histoire riche qui remonte à l'époque phénicienne. Il a réussi à s'ajuster aux changements mondiaux et à se développer, devenant un moteur économique majeur pour la région. En raison de ses caractéristiques nautiques, de ses infrastructures performantes et de son nouveau modèle de gestion, il offre un accès privilégié aux diverses industries, proposant des terminaux compétitifs et des équipements modernes pour le traitement des produits.
Le rôle du port est crucial en tant que moteur de croissance économique, stimulant les affaires de ses clients et facilitant l'amélioration de la performance de la chaîne logistique. L'EPB vise également. à favoriser l'expansion du transport multimodal et des activités logistiques. Enfin, grâce à différentes initiatives, le port cherche à encourager une collaboration plus étroite entre tous les acteurs de l'industrie pour l'évolution du port et de ses communautés [2].

1.1.1 Structure de l'entreprise

L'entreprise EPB est constituée de diverses directions et services. L'ensemble de ces derniers sont dirigés par une direction générale chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise (voir la figure 1.1).

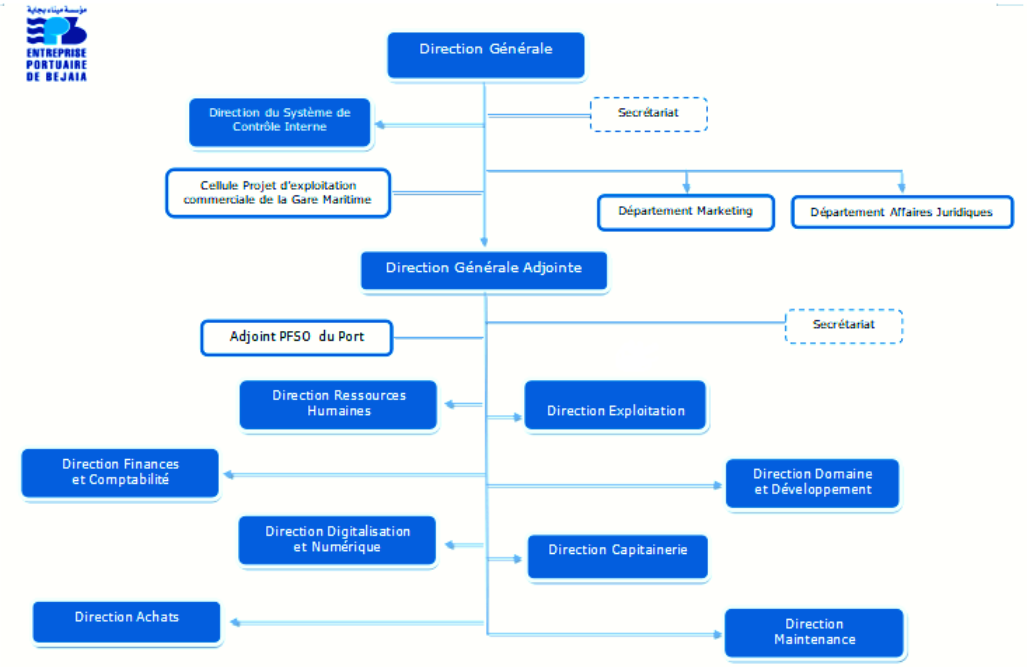


FIGURE 1.1 – Organigramme de l'EPB.

1.2 Présentation du service d'accueil

Le stage que nous avons effectué au sein de l'EPB s'est déroulé au niveau de la direction de la digitalisation numérique (DDN), plus précisément au département d'infrastructure informatique. Cette section est consacrée à sa présentation.

1.2.1 Organisation

La direction de la digitalisation numérique est une direction rattachée à la direction générale adjointe, elle est subdivisée en trois déparements (voir la figure 1.2) :

1. **Département génie logiciel :** Il se compose d'un seul service chargé d'études et de développement, c'est le département chargé de l'administration et du suivi des applications développées en interne ou acquises chez un fournisseur externe, du dépoilement et de l'assistance auprès des utilisateurs finaux.

2. **Département chargé de la gestion des programmes, méthodes et organisation :** C'est le département qui s'occupe des programme méthode et organisations, du suivi des archives, de l'affichage dynamique et des communications internes. Il est divisé en deux services :
    - **Le service de communication et d'information :** Un service qui s'occupe de l'étude des programmes et de la communication interne.
    - **Le service de gestion documentaire :** Ce service est constitué d'un documentaliste, de bibliothécaire, d'archiviste et de technicien informatique chargé de la GED (Gestion Electronique de Document) et de l'infographie.
3. **Département infrastructure informatique :** Ce département est chargé du déploiement et de l'administration du réseau et des systèmes, on retrouve un administrateur réseau principal ainsi que deux services élémentaires :
    - **Le service des infrastructures informatiques :** Un service qui se compose d'ingénieurs d'état maintenance et de techniciens informatique.
    - **Le service des systèmes :**Un service qui se compose d'ingénieurs d'état système et de chargés d'étude des bases de données.

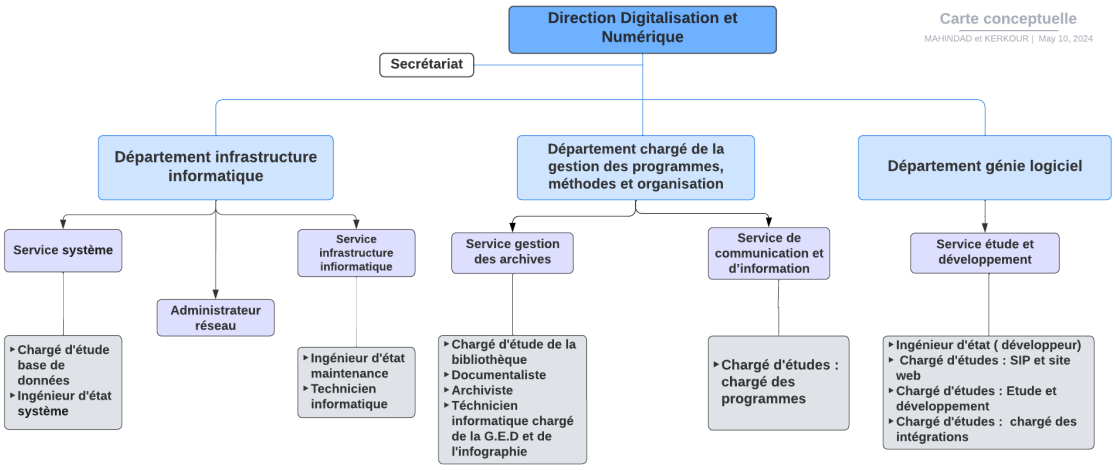


FIGURE 1.2 – Organisation du service d'accueil.

1.2.2 Activités de la Direction Digitalisation Numérique

Les activités principales menées par le département infrastructure informatique comprennent :

- L'élaboration du schéma directeur en pilotant les projets d'informatisation, en garantissant leur cohérence fonctionnelle et technique ainsi que la qualité et la sécurité des systèmes d'information.

- Le déploiement des systèmes d'information à la fois flexibles et fiables.
- La gestion de l'évolution des systèmes d'information et des projets informatiques.
- La mise en place et la supervision de l'infrastructure informatique.
- L'entretien et la maintenance du parc informatique.

1.3 Etude de l'existant

1.3.1 Présentation du réseau informatique de l'EPB

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 16 (Port à bois). Dans la salle machine du réseau local de l'EPB, on trouve principalement une armoire de brassage et une grande armoire optique. Éventuellement, cette salle abrite l'ensemble des serveurs. Ces deux armoires sont utilisées pour connecter les différents sites de l'entreprise au département informatique via des fibres optiques de 4, 6, 8 et 12 brins (voir figure 1.3), deux types de fibre optique sont utilisées : la fibre optique multimode pour le réseau local, qui relie les différents sites du port entre eux sur de courtes distances, ainsi que la fibre optique monomode pour les liaisons extérieures qui relie quant à elle le port à des sites distants. Chaque site dispose d'une armoire de brassage contenant un ou plusieurs convertisseurs de média et un ou plusieurs commutateurs, auxquels sont connectés les différents équipements par des câbles informatiques.

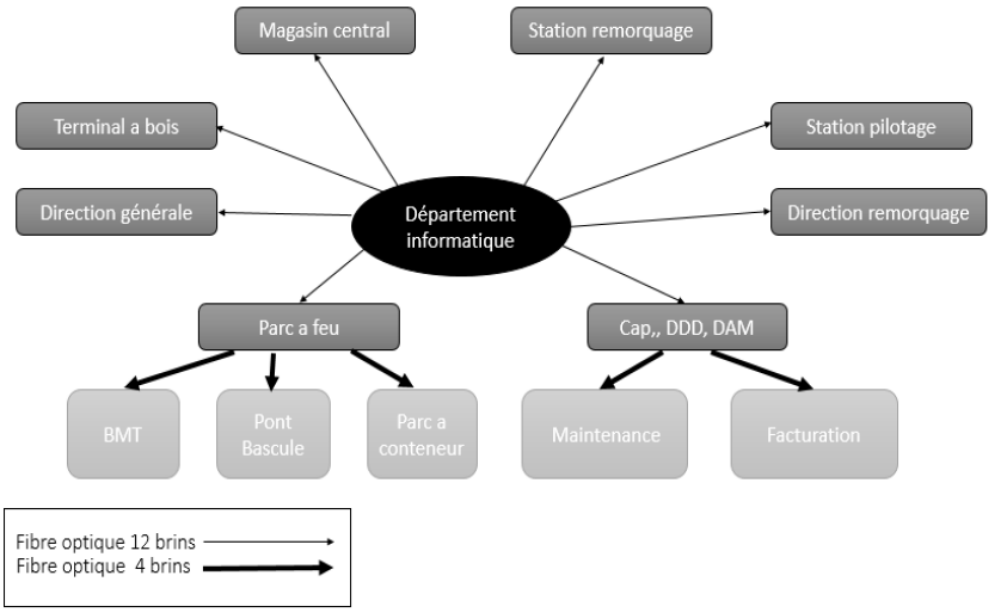


FIGURE 1.3 – Réseau informatique de l'EPB.

1.3.2 Présentation de l'environnement hard et soft

Les tableaux 1.1 et 1.2 représentent le matériel hard et soft utilisé par l'entreprise EPB.

Environnement hard :

Equipement	Marque	Description
Commutateur	Cisco Catalyst 2960x	Fournit une connexion Fast Ethernet et Gigabit Ethernet, prend en charge des services LAN avancés [11]. N'est plus pris en charge par Cisco depuis le 31/12/2019.
	D-Link	Offre des fonctionnalités de commutation de paquets et de gestion de la qualité de service.
	D-Link xStack	Switch optique, offre des fonctionnalités de commutation de paquets et de gestion de la qualité de service.
	KVM	Switch permettant d'accéder aux équipements à l'aide d'un seul clavier, souris et écran simplifiant leurs configurations.
Transmetteur optique	Huawei optiX OSN 500	Relié à deux liaisons internet (10 Mb/s et 30 Mb/s).
Serveur	HP ProLiant DL380 Gen 9	Serveur physique, répond aux besoins des entreprises en matière de virtualisation et gestion de données.
Stockage	NAS Synology	Unité de stockage connectée au réseau de l'entreprise permet de centraliser l'emmagasinage des données, configuré en RAID5.

TABLE 1.1 – Les équipements hard.

Environnement soft :

Rôle	Logiciel	Description
Hyperviseur	VMware ESXI	Hyperviseur propriétaire de type 1, pourvoit un environnement virtuel pour exécuter plusieurs VMs sur un seul serveur physique.
Sécurité	PfSense	Logiciel open source controle le trafic entrant et sortant de et vers le réseau LAN, joue aussi role de routeur.
	Kaspersky Administration Kit	outil de getion des produits Kaspersky.
Gestion utilisateurs	Active Directory	Logiciel de gestion d'identités et accés des utilisateurs.
Base de données	MySQL / MSSQL	Système de gestion de base de données open source.
Monitoring	Zabbix	Logiciel de surveillance réseau libre.
Application	Tomcat	Serveur d'application open libre utilisé pour héberger des applications web.

TABLE 1.2 – Les équipements soft.

1.3.3 Architecture du département informatique

L'EPB utilise le modèle hiérarchique pour la conception de son réseau (Figure 1.4), composé de trois couches distinctes :

- **La couche cœur :** Elle constitue le niveau le plus élevé de l'architecture, assurant la connectivité entre les différents réseaux locaux de l'organisation ou entre différentes entités.
- **La couche distribution :** Agissant comme une interface entre la couche cœur et la couche d'accès, elle assure la distribution efficace du trafic sur le réseau en agrégeant vers les différents serveurs.
- **La couche accès :** Cette couche représente le niveau le plus bas de la hiérarchie, connectant les périphériques finaux tels que les ordinateurs et les imprimantes au réseau local.

En complément du réseau interne, on utilise également des connexions distantes VPN (Virtual Private Network), largement adoptées en téléinformatique, pour créer des tunnels sécurisés afin de connecter des réseaux privés distants sur un réseau public, tel qu'Internet. Des protocoles de cryptage tel que IPsec (Internet Protocol Security) dans notre cas, sont utilisés pour sécuriser les communications, assurant ainsi la confidentialité et l'intégrité des données. On distingue deux types de liaisons :

1. **Liaison site-à-site :** Une liaison VPN site-à-site permet d'interconnecter deux réseaux d'entreprise entre eux. Cette interconnexion est utile afin de permettre le partage de ressources entre les deux réseaux. Dans le cas de l'EPB on dispose de deux sites distants, l'un situé à Ighil Ouberouak (IOB) et l'autre nommé TEXTER se trouvant au niveau de la wilaya de Bordj Bou Arreridj.
2. **Liaison poste-à-site :** Une liaison VPN poste-à-site ou client-à-site est utilisé lorsque des appareils individuels, tels que des ordinateurs, des smartphones ou des tablettes, se connectent au réseau d'entreprise depuis des emplacements distants. Idéal pour le télétravail ou pour les employés en déplacement, elle leur permet d'accéder aux ressources de l'entreprise, de manière sécurisée, peu importe leur emplacement.

Chaque site dispose d'un pare-feu pfSense, de switch de distribution et d'accès. Les postes de travail et les serveurs du même site communiquent directement entre eux, tandis que ceux qui se trouvent dans des sites différents communiquent via le VPN de manière sécurisée.
On retrouve également une DMZ (zone démilitarisée) qui représente un segment de réseau isolé, située entre le réseau interne et internet. Elle est utilisée pour héberger des serveurs, tels que le serveur SIP (Système d'informations portuaire) dans notre cas, et des applications qui doivent être accessibles depuis Internet, mais qui ne doivent pas avoir un accès direct au réseau interne. Cette architecture sera utilisée comme point de référence pour la comparer à une nouvelle architecture proposée dans le chapitre 4.

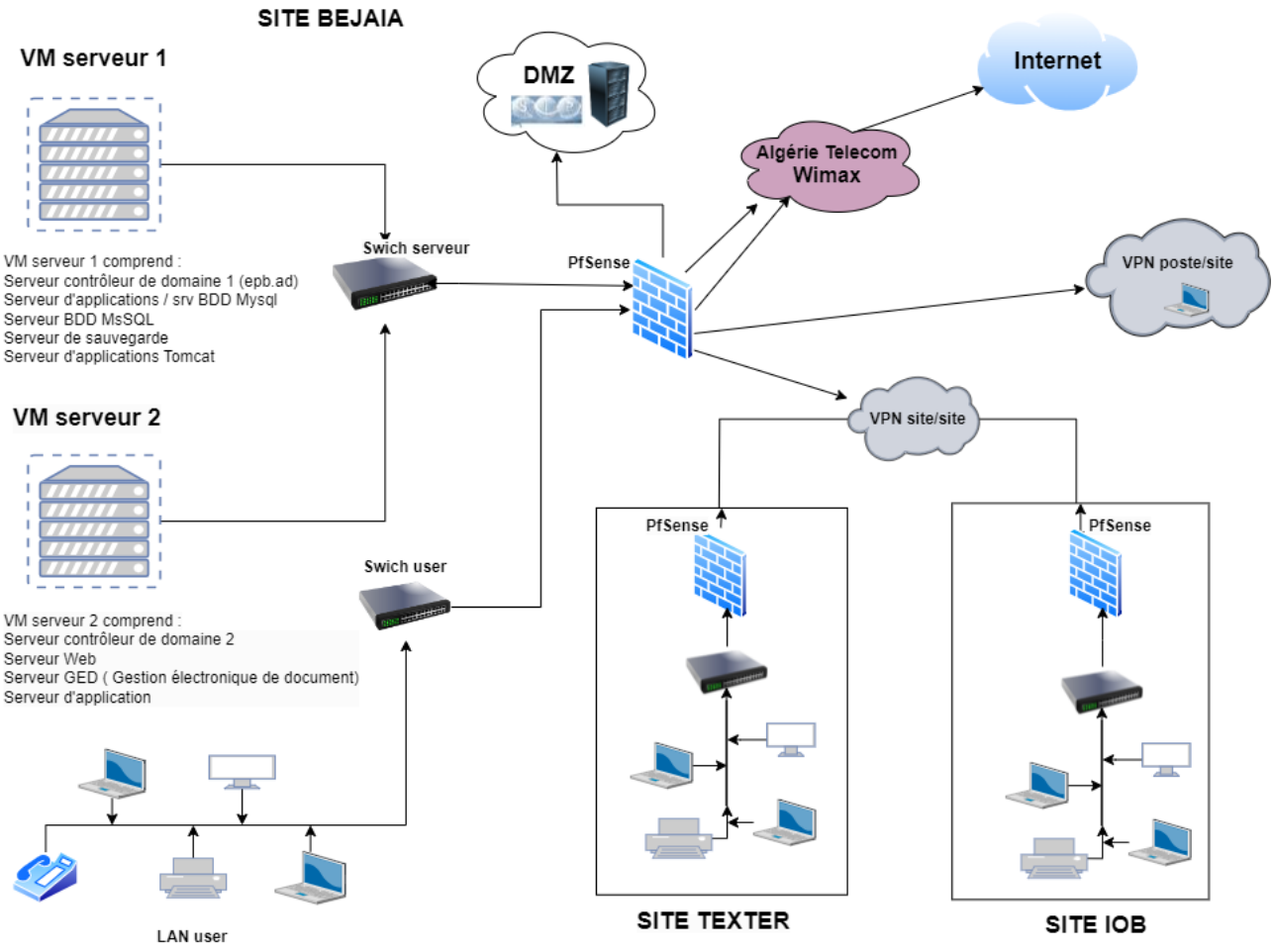


FIGURE 1.4 – Architecture du réseau de l'EPB

1.3.4 Présentation de la salle machine de l'EPB

La salle machine de l'EPB est équipée de deux armoires de brassage, dont l'une est l'armoire cœur du réseau. Un onduleur central gère tous les équipements et les armoires, y compris l'armoire optique et l'armoire câblée normalement.
À l'intérieur de l'armoire optique, on retrouve divers équipements, notamment des switchs Cisco Catalyst 2960, des switchs D-Link, un équipement de transmission optique Huawei OSN 500 Optique X alimenté par deux connexions optiques haut-débit (10 Mbps et 30 Mbps), ainsi que des switchs optiques D-Link xStack.
Le switch Cisco Catalyst 2960 assure la conversion de l'optique vers l'Ethernet, facilitant ainsi le passage d'Internet du switch optique vers le switch Ethernet, puis vers le switch serveur connecté aux serveurs. Du côté des serveurs, on retrouve des hyperviseurs VMware hébergeant des machines virtuelles, celles-ci incluent :

- Des serveurs Windows (Active Directory).
- Des serveurs EZet (serveur anti-virus).
- Des serveurs base de données (MySQL et MariaDB).

- Un serveur local SIP qui héberge un site internet en intranet.

Des switchs KVM (Kernel-based Virtual Machine) sont utilisés afin de permettre l'accès aux hyperviseurs, tandis que le logiciel VSphereClient permet de les superviser.
Il existe deux baies de stockage, l'une en mode NAS (Network Attached Storage) et l'autre en mode SAN (Storage Area Network). Toutes les données sont stockées dans la baie de stockage via des disques durs connectés au réseau NAS. Pour l'envoi des données, la couche cœur du réseau est sollicitée en les distribuant vers la couche distribution puis vers la couche accès, où se trouvent deux switchs Catalyst Cisco 2960 permettant l'accès au réseau global.

1.3.5 Problématiques et solutions proposées

Au cours de notre stage, nous avons observé plusieurs lacunes et défis rencontrés dans l'infrastructure réseau de l'entreprise, ce qui impactent négativement sa disponibilité, ses performances et sa sécurité. Ces défauts incluent :

- **Absence de configuration VLAN :** La non-utilisation de VLAN peut causer une congestion du réseau, des problèmes de sécurité ainsi que des difficultés dans la gestion des différentes catégories de trafic.
- **Manque de redondance des équipements :** En cas de défaillance d'un élément essentiel du réseau, il existe un risque potentiel d'interruption complète des services. La mise en œuvre de mécanismes de redondance est essentielle afin d'assure la continuité du service en cas de dysfonctionnement d'un élément.
- **Agrégation de liens non configurée :** L'absence d'agrégation de liens peut restreindre la capacité de bande passante disponible et créer des goulots d'étranglement, en particulier dans les environnements virtualisés où les besoins en bande passante sont élevés.
- **Manque de mécanismes de haute disponibilité :** Un manque de mécanismes de haute disponibilité signifie qu'un réseau ou un système ne dispose pas de mesures telles que le clustering, la répartition des charges, ou le basculement automatique pour assurer la continuité des services en cas de panne et limiter ces interruptions.

Les lacunes citées peuvent avoir des conséquences importantes sur l'entreprise et peuvent conduire à une perte de données, de productivité, une augmentation des coûts avec les pannes de réseau dont les réparation importants, mais surtout à une atteinte à l'image de marque de l'entreprise et affecter la confiance des clients. Afin de remédier à cela nous proposons comme solution de mettre en

place une infrastructure hautement disponibile en intégrant la notion du clustering, des mécanismes de redondance ainsi qu'une amélioration des performances avec l'intégration des VLAN et l'agrégation des liens.

Conclusion

Dans ce chapitre, nous avons donné une vue global de l'entreprise EPB, et nous avons découvert certains problèmes spécifiques qui nous ont amenés à rechercher comment mettre en œuvre une nouvelle architecture réseau hautement disponibile. En conclusion, nous prévoyons d'approfondir l'application des solutions proposées dans les chapitres suivants.

Chapitre 2

La virtualisation des systèmes et réseaux

Introduction

Dans le domaine des réseaux et des télécommunications, la virtualisation des réseaux et des systèmes connaît une croissance rapide. Les entreprises et les organisations font face à des défis de plus en plus complexes en ce qui concerne la gestion, la sécurité et les performances de leurs infrastructures réseaux en raison de l'évolution rapide des technologies de l'information et des communications. Dans ce contexte, la virtualisation est une solution prometteuse pour faire face à ces défis en offrant une plus grande souplesse et une meilleure exploitation des ressources.
Nous examinerons dans ce chapitre de manière brève les fondements de la virtualisation des réseaux et des systèmes, ses bénéfices, ainsi que les méthodes et techniques employées.

2.1 Introduction à la virtualisation

2.1.1 Historique

La première apparition de la virtualisation remonte vers la fin des années 1960 avec le développement des premières machines virtuelles. Avant cette révolution, on avait face à l'époque des gros ordinateurs centraux où chacune de ces machines physiques ne pouvait exécuter qu'un seul processus à la fois, ce qui limitait leur efficacité et ne répondait pas aux besoins des clients qui souhaitaient une utilisation plus optimale de leurs investissements.

C'est ainsi que IBM (International Business Machines Corporation) intervient et prend le mérite d'être la source d'une grande partie du travail sur la virtualisation, en développant le système expérimental CP/CMS (Control Program/Cambridge Monitor System), qui devient par la suite le produit connu maintenant sous le nom d'hyperviseur.
Malgré ces travaux, ce n'est qu'à partir des années 2000 que les entreprises commençaient à adopter la solution de la virtualisation réglant ainsi deux problèmes majeurs : ils pouvaient fractionner leur infrastructure de serveurs de façon optimale et exécuter leurs anciennes applications sur plusieurs types et versions de système d'exploitation, et ceux, en réduisant leur budget lié à l'achat et à la maintenance des serveurs [62].

2.1.2 Définition de la virtualisation système et réseau

La virtualisation consiste en la création d'une couche d'abstraction qui permet de présenter une ressource virtuelle comme étant identique à la ressource physique réelle qu'elle représente. Cela permet l'utilisation de multiples environnements ou de ressources dédiées à partir d'un seul système physique.
La virtualisation système implique donc la virtualisation des ressources physiques, comme les serveurs ou les dispositifs de stockage afin de permettre une utilisation plus efficace des ressources matérielles. De même, la virtualisation réseau permet la création de réseaux logiques indépendants du réseau physique sous-jacent, offrant une flexibilité accrue dans la configuration et la gestion des infrastructures réseau [22][33].

2.1.3 Importance de la virtualisation dans les environnements modernes

Face à la complexité croissante des infrastructures de nos jours, la virtualisation s'impose comme étant une solution incontournable, elle offre une multitude d'avantages significatifs aux entreprises et aux organisations, parmi eux on retrouve :

- **Des coûts d'investissement réduits :** En faisant coexister plusieurs machines virtuelles sur un seul serveur physique, les entreprises peuvent réduire considérablement les coûts matériels ainsi que les coûts de maintenance associés. Cela entraîne par la même occasion une réduction de la consommation d'énergie [42].
- **Une flexibilité et une évolutivité accrue :** La virtualisation permet une flexi-

bilité dans l'utilisation des ressources en maximisant leur efficacité. Les machines virtuelles peuvent être modifiées, supprimées, ajoutées ou déplacées en toute facilité permettant ainsi l'introduction de nouvelles technologies et de systèmes innovants [61].

- **Une isolation et une sécurité améliorée :** Les machines virtuelles sont isolées les unes des autres, ce qui améliore la sécurité en évitant la propagation des vulnérabilités. De plus, un gestionnaire de machine virtuelle peut contrôler et filtrer le comportement des programmes invités, prévenant ainsi toute opération malveillante potentielle [55].
- **Une haute disponibilité et une reprise après sinistre :** Les solutions de virtualisation offre des fonctionnalités de haute disponibilité qui garantissent la continuité de l'activité. En cas de panne d'une machine physique, les disques virtuels peuvent être déplacés vers une autre machine hôte et toutes les machines virtuelles restent disponibles, ce qui implique des temps d'arrêt réduits [45].

2.2 Fondements de la virtualisation système

2.2.1 Concepts fondamentaux de la virtualisation système

- **Machine virtuelle (VM) :** Une machine virtuelle est un environnement virtuel simulant une machine physique, et permet à plusieurs systèmes d'exploitation (OS) et applications de fonctionner simultanément sur un même serveur ou autre machine physique.
  Le fichier de configuration (qui expose les ressources matérielles disponibles pour la machine virtuelle) et le fichier du disque virtuel (qui stocke le système d'exploitation et les données de la machine virtuelle) sont les éléments clés d'une machine virtuelle [50].

- **Conteneurs :** Un conteneur est une unité logicielle [48] qui fait abstraction au niveau du système d'exploitation plutôt qu'au niveau du matériel, contrairement aux machines virtuelles, partageant ainsi le noyau du système hôte. C'est une forme légère de virtualisation qui regroupe une application et ses dépendances dans un seul paquet portable, indépendant de la plate-forme et peut être facilement déplacé et exécuté sur n'importe quel système d'exploitation compatible [50].

- **Hyperviseurs :** Un hyperviseur, ou moniteur de machine virtuelle (VMM, Virtual Machine Monitor), est la couche logicielle qui autorise la création et

l'exécution d'un grand nombre de machines virtuelles sur une même machine physique.
Le VMM prend en charge l'attribution des ressources allouées à chaque machine virtuelle ainsi que la gestion de leur planification en fonction des ressources disponibles [55]. On retrouve deux catégories d'hyperviseurs (voir la figure 2.1) :

1. **Hyperviseur de type 1 :** Appelé bare-metal, il s'exécute directement sur le matériel physique, permettant aux machines virtuelles d'exécuter leurs instructions directement sur ce matériel, dans le but de faciliter la prise en charge des systèmes d'exploitation invités [52].
   Parmi les hyperviseurs connus de cette catégorie on retrouve : VMware vSphere, VMware ESXi, Citrix XenServer, Microsoft Hyper-V Server.

2. **Hyperviseur de type 2 :** Aussi nommé hyperviseur hébergé, c'est un hyperviseur qui s'installe et s'exécute comme une application à l'intérieur d'un système d'exploitation existant. Il agit comme un intermédiaire entre les ressources offertes par le système d'exploitation hôte et les systèmes d'exploitation virtualisés, en gérant et en partageant les ressources du système hôte pour répondre aux besoins des machines virtuelles [52].
   Certains exemples des solutions proposées dans cette catégorie sont : VMware Workstation, Oracle VM VirtualBox, Microsoft Virtual Server.

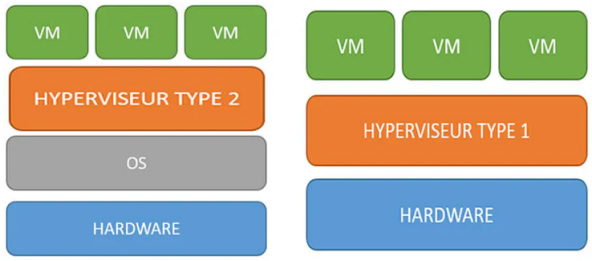


FIGURE 2.1 – Les différents types d'hyperviseurs [60].

2.2.2 Types de virtualisation système

1. **Virtualisation des serveurs :** C'est un processus qui consiste à diviser un seul serveur physique en plusieurs serveurs virtuels à l'aide d'une couche logicielle. Chaque serveur virtuel se comporte comme un seul périphérique physique, capable d'exécuter son propre système d'exploitation [21].
2. **Virtualisation de poste de travail :** La virtualisation des postes de travail offre la possibilité de déployer simultanément plusieurs environnements de

bureau simulés sur de multiples appareils physiques. Ce type de virtualisation permet aux administrateurs de réaliser des configurations, des mises à jour et des contrôles de sécurité de manière globale sur l'ensemble des postes de travail virtuels [21].

3. **Virtualisation de stockage :** C'est une technique qui permet de regrouper plusieurs serveurs à partir d'un seul système de stockage virtuel, permettant ainsi une gestion distribuée des données sans que les serveurs aient besoin de connaître leur emplacement précis [55].
4. **Virtualisation d'applications :** La virtualisation d'applications est une technologie qui permet de séparer les applications du système d'exploitation en isolant celles-ci dans des conteneurs. Cette approche permet d'éliminer les conflits entre applications sur une même machine [22].

2.3 Technologies de la virtualisation système

De ce que nous avons cité précédemment, on retrouve deux principes distincts, l'hypervision et la conteunerisation. Pour mieux les distinguer, le tableau 2.1 présente un résumé de ces principes :

Type	Hyperviseur type 1	Hyperviseur type 2	Conteneur
Fonctionnement	S'exécute directement sur le matériel physique, les VM fonctionnent directement sur cet hyperviseur.	Installé sur un système d'exploitation hôte, les VM fonctionnent comme des processus sur l'OS hôte.	Partage le noyau de l'hôte et isole les processus dans des environnements légers.
Avantages	-Performances élevées -Meilleure sécurité -Isolation complète des systèmes d'exploitation invités	-Simplicité dans l'installation et l'utilisation -Large choix de systèmes d'exploitation invités	-Portabilité et flexibilité -Meilleure utilisation des ressources -Développement et déploiement rapides
Inconvénients	-Complexité de gestion et de configuration -Coût plus élevé	-Dépendance à l'OS hôte -Performance légèrement inférieure	-Moins d'isolation que les machines virtuelles -Nécessite un système d'exploitation hôte compatible
Cas d'utilisation	-Environnements de production critiques -Virtualisation de serveurs	-Environnements de développement et de test -Virtualisation de postes de travail	-Déploiement d'applications cloud -Microservices

TABLE 2.1 – Comparaison entre les technologies de la virtualisation système

2.4 Déploiement et gestion de la virtualisation système

La virtualisation système joue un rôle clé dans la création d'une infrastructure hautement disponible et résiliente. Par conséquent, il est primordial d'aborder les aspects fondamentaux du déploiement et de la gestion de la virtualisation système.

2.4.1 Déploiement d'hyperviseurs et de conteneurs

Les hyperviseurs et les conteneurs sont des technologies de virtualisation couramment utilisées pour créer des environnements isolés et exécuter des applications de manière efficace. Pour garantir le bon fonctionnement de l'infrastructure virtuelle, une configuration et un déploiement minutieux sont essentiels. Pour réaliser ceci des étapes sont nécessaires :

- **Sélection de la plateforme :** La sélection d'un hyperviseur ou de la plateforme de conteunerisation est une étape importante lors de la mise en place d'une infrastructure virtuelle. Elle exige une évalution des besoins de l'infrastructure en termes de performances, de coût, de compatibilité matérielle, ainsi que de fonctionnalités avancées telle que la haute disponibilité, les migrations à chaud et le clustering.

- **Installation et configuration :** L'installation et la configuration d'un hyperviseur consistent à installer le logiciel sur le matériel physique ou sur une machine virtuelle, à configurer les paramètres de l'hyperviseur pour optimiser les performances et la fiabilité de l'infrastructure virtuelle, et à allouer les ressources matérielles, telles que le processeur, la mémoire, le stockage et le réseau, aux machines virtuelles. Ceci se fera en prenant en compte des besoins ainsi que des recommandations de la plateforme choisie.

2.4.2 Gestion des machines virtuelles et des conteneurs

Les machines virtuelles et les conteneurs sont désormais indispensables pour exécuter des applications et des services de manière flexible et évolutive. Par conséquent, une gestion efficace de ces environnements virtuels est importante afin d'assurer leur disponibilité, leurs performances et leur sécurité tout au long de leur évolution.

- **Allocation des ressources :** L'allocation de ressources consiste à allouer des ressources matérielles (CPU (Central Processing Unit), mémoire, stockage, bande passante réseau) aux machines virtuelles et aux conteneurs en fonction de leurs besoins et de leurs priorités, tout en veillant à ne pas surcharger les serveurs physiques ou virtuels [34].

- **Migrations :** On retrouve deux principaux types de migrations :
    1. **Migration à chaud :** Connue sous le nom "live-migration", la migration à chaud implique le déplacement d'une machine virtuelle ou d'un conteneur sans interrompre les services ou les applications en cours d'exécution, garantissant ainsi leur continuité et leur disponibilité. Elle

est particulièrement utilisée dans des environnements critiques où la disponibilité des applications est essentielle [31].

2. **Migration à froid :** La migration à froid est le processus de déplacement de machines virtuelles ou de conteneurs qui nécessite la mise hors tension ou l'arrêt de ces derniers. Ce processus est souvent utilisé lorsque des contraintes de compatibilité ou d'autres restrictions empêchent l'utilisation de la migration à chaud [43].

- **Sauvegardes :** Les sauvegardes consistent à enregistrer l'état d'une machine virtuelle ou d'un conteneur à un moment donné, pour pouvoir le restaurer en cas de panne ou de défaillance. Un plan de sauvegarde est nécessaire pour définir les fréquences, les types et les destinations des sauvegardes, ainsi que les procédures de restauration [39]. Selon les besoins, plusieurs types de sauvegardes seront détaillés dans le prochain chapitre.

2.4.3 Outils de gestion de la virtualisation système

Le choix d'un outil de gestion de la virtualisation système adapté est essentiel pour optimiser l'efficacité et la performance des infrastructures. De nombreux outils de gestion de la virtualisation système sont disponibles sur le marché, le tableau 2.2 présente une vue d'ensemble des principales solutions disponibles, où l'on retrouve parmi elles l'hyperviseur utilisé par l'EPB :

L'outil	Proxmox VE	VMware ESXi	Microsoft Hyper-V	Docker	Kubernetes
Approche de virtualisation	Conteneur, VM	VM	VM	Conteneur	Conteneur
Interface utilisateur	Web, Ligne de commande	vSphere Client, vCenter Server	Web, Hyper-V Manager	Web, ligne de commande	Web, ligne de commande
Gestion des VM/Conteneurs	Création, suppression, clonage, migration, snapshots	Création, suppression, clonage, migration, snapshots	Création, suppression, clonage, migration, snapshots	Création, suppression, clonage, migration, snapshots	Déploiement, mise à l'échelle, gestion des conteneurs
Gestion des ressources	Allocation dynamique des ressources	Allocation dynamique des ressources	Allocation dynamique des ressources	Allocation dynamique des ressources	Allocation dynamique des ressources
Haute disponibilité et clustering	Intégré	Intégré	Intégré	Non intégré	Intégré
Licence	Open-source	Payante	Payante	Open-source	Open-source

TABLE 2.2 – Comparaison des outils de gestion de la virtualisation système

2.5 Fondements de la virtualisation réseau

La virtualisation du réseau repose sur plusieurs principes fondamentaux :

- **Découpage d'un réseau physique en réseaux virtuels isolés :** Un des principaux fondements de la virtualisation réseau est le découpage. La virtualisation du réseau consiste à fragmenter un réseau physique en plusieurs réseaux virtuels distincts. Chaque fragment va donc agir comme s'il était un réseau physique séparé [18].
- **Abstraction et isolation des ressources réseau :** Chaque réseau virtuel est doté de ses propres ressources, telles que des interfaces et des liens, qui sont abstraites des autres réseaux virtuels. En outre, ces ressources sont séparées les unes des autres, assurant ainsi que chaque réseau virtuel opère de manière indépendante et sécurisée [18].
- **Partitionnement de la table de transfert de paquets :** Le partitionnement de la table de transfert de paquets dans la virtualisation réseau permet à

chaque réseau virtuel de fonctionner de manière autonome en attribuant un sous-ensemble spécifique de la table de routage à chaque réseau. Cela donne à chaque réseau virtuel l'illusion d'avoir ses propres adresses IP (Internet Protocol) et règles de routage de manière indépendante. Cette méthode garantit une isolation complète entre les réseaux virtuels en partageant les mêmes ressources physiques et en simplifiant la gestion globale du réseau [18].

2.6 Technologies de la virtualisation réseau

2.6.1 Virtualisation des commutateurs et des routeurs

Les commutateurs et routeurs virtuels, communément appelés vSwitch et vRouter, sont des logiciels qui virtualisent les fonctions réseau d'un commutateur et d'un routeur physique. Ils permettent de créer des réseaux virtuels qui peuvent être utilisés pour isoler le trafic réseau, améliorer la sécurité et optimiser l'utilisation des ressources.
Le vSwitch se charge de la commutation de trames entre les machines virtuelles connectées au même réseau local virtuel (VLAN), tandis que le vRouter est responsable du routage du trafic entre les différents réseaux virtuels et le réseau externe [66].
Pour segmenter efficacement les réseaux virtuels et garantir leur bon fonctionnement, des technologies virtuelles sont utilisées dans ces contextes :

- **Les VLAN (Virtual Local Area Network) :** C'est une technologie de segmentation local de couche 2 qui permet de créer des réseaux virtuels isolés sur un même commutateur physique. Le protocole VTP (VLAN Trunking Protocol), associé aux VLAN, simplifie la gestion et la distributions des informations sur les VLAN au sein d'un réseau.
- **le VRF (Virtual Routing and Forwarding) :** Cette technologie va plus loin en permettant l'exécution de plusieurs instances d'une table de routage de fonctionner simultanément sur un même nœud. Cela permet de segmenter le réseau en plusieurs domaines logiques indépendants, tout en utilisant un seul routeur physique. Le VRF utilise des VLAN pour identifier les différents réseaux virtuels où chaque réseau virtuel est associé à un VLAN spécifique [18].

2.6.2 Les réseaux définis par logiciel (SDN)

L'idée du SDN est de séparer la couche de données (matériel) de la couche de contrôle (logiciel) pour avoir un réseau programmable et virtualisable [32]. Il centralise la gestion du réseau en s'appuyant sur des contrôleurs logiciels ou des API (Application Programming Interface) pour créer et contrôler des réseaux virtuels, offrant ainsi une alternative aux réseaux traditionnels basés sur des périphériques matériels dédiés. Cela favorise l'automatisation et l'efficacité des ressources [54].

2.6.3 Virtualisation des fonctions réseau

La virtualisation des fonctions réseau (NFV) est une technologie prisée dans le domaine des télécommunications qui virtualise les fonctions réseau du matériel physique sur lequel ils s'exécutent traditionnellement. Cela permet de déplacer les logiciels qui exécutent ces fonctions vers des machines virtuelles standardisées et peuvent ainsi être orchestrées et gérées de manière flexible, en fonction des besoins spécifiques du réseau et des utilisateurs [52]. Parmi les fonctions que prend en charge la NFV on retrouve des fonctions de partage de fichiers, d'équilibrage de charge, de configuration d'adresses IP mais aussi [35] :

- **Les pare-feux virtuels :** Un pare-feu virtuel est un logiciel qui opère au niveau du VMM dans des environnements virtualisés, offrant des fonctionnalités similaires aux pare-feux matériels traditionnels, telles que le filtrage du trafic réseau et la protection des données sensibles pour sécuriser les machines virtuelles, les charges de travail conteneurisées, les applications web et les bases de données [9][59].
- **La traduction d'adresses réseau :** Le NAT (Network Address Translation) est une fonctionnalité qui traduit les adresses IP et les ports d'un réseau privé en adresses IP et ports valides sur un réseau public, et inversement, permettant à plusieurs appareils d'un réseau privé d'accéder à Internet en partageant une seule adresse IP publique [44].

2.7 Déploiement et gestion de la virtualisation réseau

La virtualisation réseau peut diviser un réseau physique en plusieurs réseaux virtuels isolés en utilisant des interfaces et des nœuds virtuels, tels que machines virtuelles ou conteneurs, ce qui améliore l'utilisation des ressources physiques. Pour garantir une mise en œuvre efficace de la virtualisation du réseau, il est important d'assurer un transfert optimal du trafic entre les machines virtuelles, en veillant à mettre en place un déploiement et une gestion performante de la

virtualisation réseau [65].

2.7.1 Déploiement et gestion de solutions de virtualisation réseau

Le déploiement et la gestion de solutions de virtualisation réseau impliquent plusieurs étapes, notamment :

- **Définition des besoins :** Avant de sélectionner une solution et de la mettre en œuvre, une clarification des exigences de l'organisation en matière de virtualisation réseau doit se faire. Cela implique une évaluation de l'infrastructure réseau existante en termes de topologie, de composants matériels et logiciels et de contraintes de sécurité, ainsi qu'une détermination des exigences en matière de performance en prenant en compte certains facteurs tels que la bande passante, la latence et la disponibilité pour chaque réseau virtuel envisagé.
- **Choix de la solution :** Après la définition des besoins, il est possible de commencer à évaluer les différentes solutions de virtualisation réseau, en prenant en compte la facilité d'utilisation, l'évolutivité ainsi que les différentes fonctionnalités proposées afin d'intégrer au mieux l'infrastructure physique déjà existante.
- **Conception et déploiement du réseau virtuel :** Le réseau virtuel doit être conçu en tenant compte des exigences en matière de performance, de sécurité et de scalabilité. Le déploiement de la solution de virtualisation réseau doit être réalisé de manière à minimiser les perturbations sur l'infrastructure physique sous-jacente.
- **Tests et validation :** Afin de s'assurer de leur bon fonctionnement, les réseaux virtuels doivent être soumis à des tests et à des validations des solutions choisies, en terme de : Fonctionnalité, sécurité, performance, intégrité et résilience avant le déploiement en production pour identifier et résoudre les problèmes potentiels.

2.7.2 Gestion des réseaux virtuels

La gestion des réseaux virtuels comprend plusieurs tâches, notamment :

- **Provisionnement des ressources réseau :** Les ressources réseau, telles que les adresses IP, les VLAN et les pools DHCP (Dynamic Host Configuration Protocol) doivent être allouées aux réseaux virtuels prévus.
- **Gestion de la sécurité :** Pour protéger au mieux les réseaux virtuels et l'infrastructure globale, il est primordial de mettre en place les configurations

de sécurité nécessaire telles que les pare-feux, le chiffrement, ainsi qu'une politique de sécurité, couvrant les droits d'accès, la gestion des données, la protection contre les logiciels malveillants et la réponse aux incidents.

- **Mise en place de mécanismes de QoS :** La configuration de mécanismes de qualité de service (QoS), tels que la classification et la priorisation du trafic, est nécessaire pour garantir un traitement prioritaire aux applications critiques.
- **Surveillance des performances :** Les performances des réseaux virtuels doivent être surveillées pour garantir que les besoins des utilisateurs sont satisfaits.
- **Mise à jour des logiciels :** Les logiciels de virtualisation réseau doivent être mis à jour régulièrement pour garantir la sécurité et les performances optimales. Une vérification de celles-ci est recommandée afin de s'assurer de leur compatibilité avec la solution de virtualisation employée.

2.7.3 Outils de gestion de virtualisation réseau

On retrouve sur le marché de nombreux outils de gestion de virtualisation réseau qui permettent aux administrateurs réseau de gérer de manière centralisée les réseaux virtuels. Le provisionnement automatisé des réseaux virtuels est l'une des fonctionnalités fréquentes de ces outils, elle permet de créer et de configurer rapidement des réseaux virtuels en automatisant les tâches manuelles, de permettre une surveillance en temps réel et de gérer centralement les politiques de sécurité et de QoS. Parmi les différents outils utilisés pour gérer la virtualisation réseau [16], on peut citer :

Outil de gestion de virtualisation réseau	**Description**
VMware NSX	Plateforme de virtualisation réseau pour la création et la gestion de réseaux virtuels dans des environnements virtualisés et cloud[26].
Linux Bridge et Open vSwitch	Pont et commutateur virtuels open source qui permettent de créer des réseaux virtuels sur des environnements Linux. Souvent utilisés dans les déploiements de virtualisation et de conteneurisation[38][46].
Cisco ACI	Solution SDN pour la gestion automatisée des réseaux de datacenters[27].

TABLE 2.3 – Outils de gestion de virtualisation réseau

Conclusion

Au cours de ce second chapitre, nous avons exploré les fondements de la virtualisation réseau et système, soulignant ses avantages et son importance dans les infrastructures modernes des télécommunications. En nous appuyant sur cette compréhension, nous sommes mieux préparés à aborder le chapitre suivant axé sur la haute disponibilité et le clustering, et nous étudierons comment ces technologies peuvent être intégrées pour assurer une infrastructure robuste et fiable.

Chapitre 3

La Haute Disponibilité et Clustering

Introduction

La dépendance aux communications numériques crée pour les entreprises la nécessité de mettre en place des mesures qui garantissent la continuité de leur opérations pour répondre à la demande croissante des services, même en cas d'interruptions. Dans ce chapitre, segmenté en deux sections, nous aborderons la haute disponibilité et le clustering. La première partie sera consacrée à la haute disponibilité. Nous verrons son importance et les principales solutions pouvant être mises en œuvre pour y pallier. Dans la deuxième section, nous explorerons le clustering, l'intérêt d'adopter cette technologies ainsi que les mécanismes qui facilite son déploiement et gestion.

3.1 La Haute Disponibilité

3.1.1 Introduction à la Haute Disponibilité

La haute disponibilité ou High Availability (HA), se définit comme la capacité d'un système à être opérationnel en permanence, avec un objectif qui tend vers 100% de disponibilité, même en cas de pannes. Le but est de minimiser les temps d'arrêt et les interruptions de services [53].

Cependant, la haute disponibilité ne se résume pas qu'à cette simple définition ; elle désigne également une approche de conception de systèmes et réseaux qui met en place un ensemble de techniques visant à garantir qu'un certain système ou service est continuellement opérationnel et accessible, avec un minimum de temps d'arrêt [7].

Mettre en place des mécanismes de haute disponibilité est essentiel et important (Importance de la haute disponibilité en section A.2) pour assurer la continuité des opérations et la protection contre les pannes. Cependant, il ne s'agit que d'une étape dans un processus plus large qui exige une planification rigoureuse. Les étapes de cette étude sont les suivantes :

1. **Identification des risques et causes d'indisponibilité potentiels :** Implique de saisir les types de risques auxquels l'organisation est exposée. Diverses menaces pourraient mettre en péril l'environnement telles que les pannes matérielles et les erreurs humaines [24].
2. **Énonciation des objectifs de disponibilité :** C'est une étape cruciale dans l'élaboration d'un plan d'architecture hautement disponible. Les OD (Objectifs de Disponibilité) définissent les exigences en matière de performances attendues pour les systèmes et applications critiques en termes de disponibilité et de perte de données acceptable. Les deux mesures à définir sont le Recovery Time Objective (RTO 3.1.4) et le Recovery Point Objective (RPO 3.1.4).
3. **Analyse de l'architecture actuelle de l'entreprise :** L'objectif est d'obtenir une compréhension complète de l'architecture de l'entreprise, en identifiant et cartographiant ses composants, services et données critiques, qui permettra de visualiser les interdépendances entre ces éléments, d'identifier les points de défaillance potentiels et de comprendre les besoins de la firme.
4. **Sélection des technologies et des solutions :** Le choix de la solution dépend des exigences spécifiques de l'environnement et des applications. Prendre en compte des facteurs tels que le coût et la complexité est aussi important.
5. **Définition des politiques de gestion :** Celà suscite de préciser la fréquence des sauvegardes, de maintenances et mise à jour des entités logicielles et matérielles.
6. **Mettre en œuvre et tester l'architecture HA :** Effectuer des tests approfondis pour valider la conception de l'architecture avant son installation définitive [63], et simuler des scénarios de défaillance pour s'assurer que les mécanismes sélectionnés répondent aux exigences et aux objectifs voulus.

3.1.2 Les principales sources d'indisponibilité

L'une des difficultés rencontrées lors de la création d'une solution à grande disponibilité réside dans l'analyse et le traitement de toutes les raisons potentielles d'interruptions. Lors de la création d'une infrastructure résiliente, il est capital de considérer les raisons d'indisponibilités, qu'elles soient planifiées 1 ou non planifiées 2, comme celles énumérées dans la figure 3.1 et expliquées dans la section A.1.

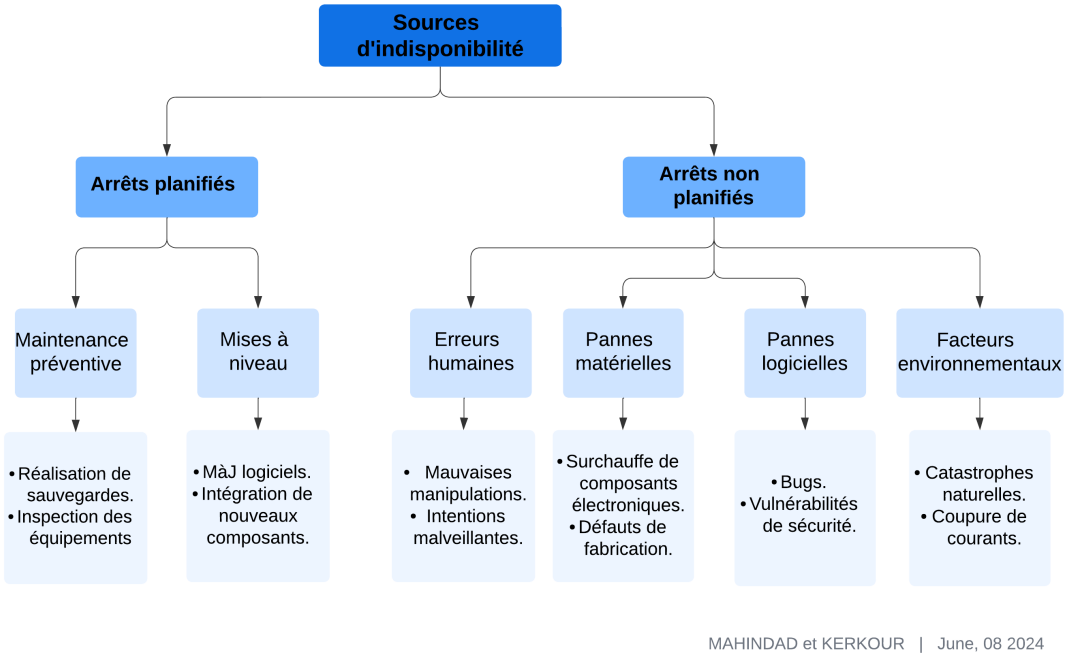


FIGURE 3.1 – Diagramme récapitulant les sources d'indisponibilité.

3.1.3 Méthodes et Technologies pour Assurer la Haute Diponibilité

Haute disponibilité matérielle :

Les technologies à implémenter pour une haute disponibilité matérielle sont les suivantes :

1. **La redondance matérielle :** Lors de la conception d'une infrastructure hautement disponible, l'éradication des points de défaillance uniques (Single Points of Failure (SPOF)) constitue un objectif primaire.

   Un SPOF se définit comme un élément singulier dont la défaillance est susceptible d'entraîner l'arrêt complet du système. En d'autres termes, il s'agit d'un maillon faible au sein de l'infrastructure qui, en cas de panne, peut mettre en péril l'ensemble des fonctionnalités. Afin de les limiter, voire de les éliminer, les organisations s'orientent vers la mise en place de solutions de redondance.

   La redondance matérielle vise à dupliquer les composants critiques de l'infrastructure, comme le montre la figure 3.2, afin de garantir une meilleure fiabilité et une connectivité persistante en cas de défaillance. Cela inclut le stockage, les sources d'alimentation, les cartes réseaux, les serveurs et les équipements et liaisons d'interconnexion.

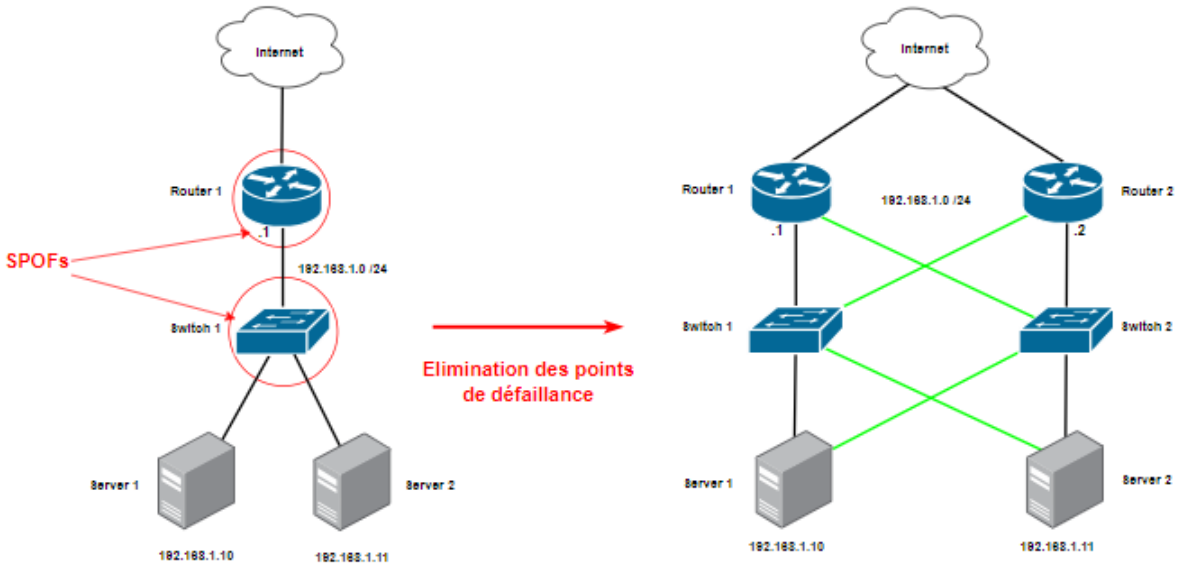


FIGURE 3.2 – Élimination des SPOFs par redondance des équipements critiques.

2. **Load Balancing :** L'équilibrage de charge ou LB (Load Balancing en anglais), illustré dans la figure 3.3, agit comme une méthode qui permet de répartir le trafic réseau de manière homogène et équitable, sur un groupe de ressources redondants effectuants les mêmes tâches, en vue de fluidifier le traffic et éviter des charges trop importantes sur les équipements[6].

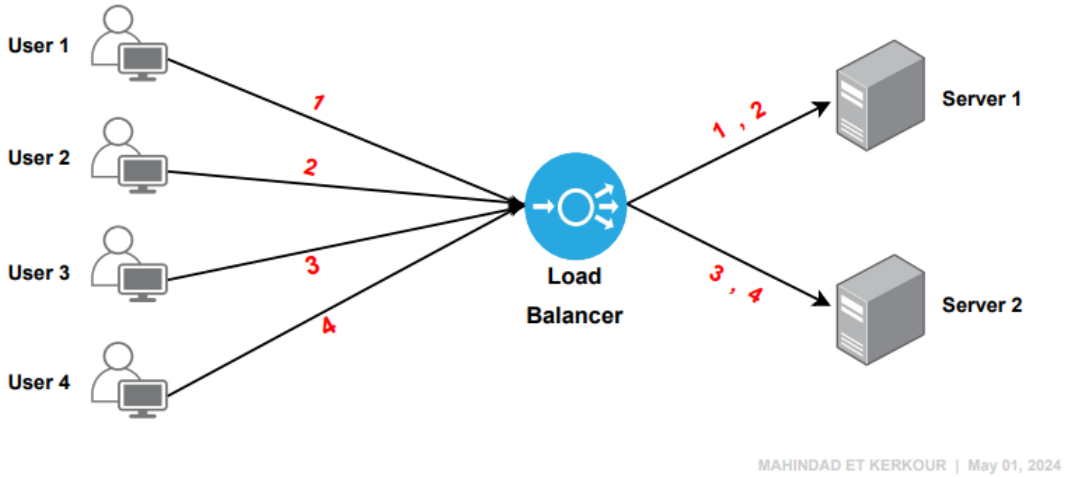


FIGURE 3.3 – Equilibrage de charge entre serveurs.

Haute disponibilité logicielle :

1. **Sauvegarde et restauration :** Une sauvegarde est une copie de données effectuée à un moment précis et de manière périodique (Quotidienne, hebdomadaire, annuelle...). Cette copie peut être utilisée pour restaurer des don-

nées en cas de perte, de suppression ou de corruption [39]. Le tableau 3.1 classe les trois niveaux de sauvegarde :

Niveaux de sauvegarde	Avantages	Inconvénients	Fréquence	Coût	Objectif
Sauvegarde complète	Simple à restaurer	Nécessite plus d'espace et temps de stockage	Régulière (ex : hebdomadaire, mensuelle)	Coûteuse en espace de stockage et temps	Protection complète du système
Sauvegarde incrémentielle	Petite, rapide et économe en espace de stockage	Complexe à restaurer	Plus fréquente (ex : quotidienne, journalière)	Économique	Sauvegarde de données modifiées depuis la dernière sauvegarde
Sauvegarde différentielle	Rapide et moins d'espace de stockage	Peut devenir plus difficile à restaurer	Plus fréquente (ex : quotidienne, journalière)	Économique	Sauvegarde de données modifiées depuis la dernière sauvegarde complète

TABLE 3.1 – Les niveaux de sauvegarde.

La restauration est le processus d'utilisation d'une sauvegarde pour restituer les données perdues ou endommagées à leur état d'origine [39].

2. **Réplication :** Cette technique fonctionne copiant en continu les données de production en direct, sur un support de stockage adapté de manières asynchrones donc périodiques, ou synchrones ; c'est à dire en temps réel. Dans ces deux cas, la réplication garantit que les données répliquées restent synchronisées et identiques ente un système et un autre [57] [58]. Dans l'outil Proxmox 4.1.1 de la partie simulation, c'est le gestionnaire de volumes logiques ZFS (Annexe D) qui assure cette opération.

   Bien que la sauvegarde et réplication impliquent toutes deux la création de copies de données, elles servent des objectifs différents et présentent des caractéristiques distinctes : La sauvegarde de données vise principalement à conserver les informations pour une utilisation future ou pour la récupération en cas de perte. D'autre part, le but de la réplication n'est pas de stocker les informations pour une période prolongée, mais plutôt de créer une ver-

sion exacte et actuelle, de la totalité ou de parties spécifiques des données [58].

3. **Synchronisation de données** : La synchronisation des données est le processus qui permet de maintenir la cohérence entre deux ou plusieurs copies de données. Cela se fait généralement en répliquant les modifications apportées aux données sources vers toutes les autres réplicas.
4. **Migration :** (Voir Chapitre 2.4.2).

Autres mécanismes de détection et de récupération des pannes :

1. **Failover :** En cas de panne ou de problème sur un des composants principaux, le principe de failover ou basculement garantit la continuité du système en redirigeant les requêtes des utilisateurs vers une instance de secours fonctionnant en parallèle. Le processus de failover peut être déclenché par diverses conditions, telles qu'une perte de connectivité réseau, un taux d'erreur élevé ou surcharge du système principal [1].
2. **failback** : Le failback veut dire "retour en arrière". Il s'agit de l'opération inverse du failover ; C'est le processus de basculement des opérations de l'élément de secours vers l'élément principal restauré. Ces deux mécanismes sont représentées dans la figure 3.4.

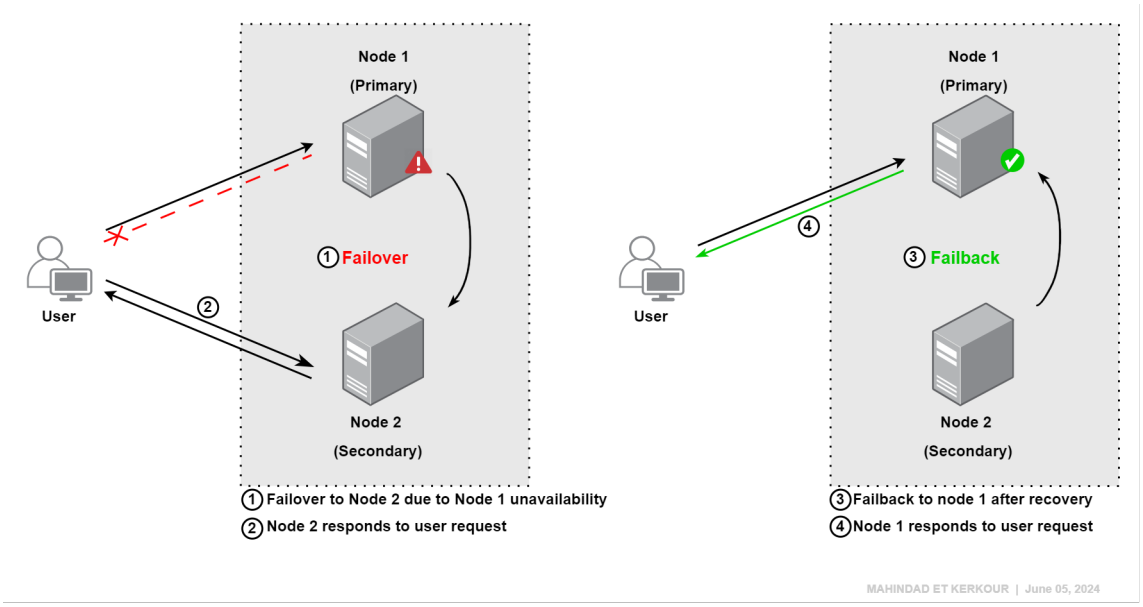


FIGURE 3.4 – Processus de basculement vers un serveur secondaire et restoration vers le serveur principal.

3.1.4 Évaluation de La Haute Disponibilité

Mesure de la disponibilité :

Dans les environnements à haute disponibilité, de nombreux indicateurs de mesures communs permettent aux équipes informatiques de déterminer si l'architecture à haute disponibilité remplit ses objectifs. Leur pertinence peut varier selon la structure et les types de services fournis par les organisations et entreprises, mais il reste utile de tous les évaluer afin de définir les attentes de base en matière de performances [53] :

- **Temps moyen entre les pannes (MTBF) :** C'est le temps moyen écoulé entre deux défaillances consécutives d'un système ou d'un composant pendant son fonctionnement normal. Un Mean Time Between Failure élevé indique une meilleure fiabilité du système, c'est-à-dire qu'il est susceptible de fonctionner plus longtemps sans panne.
- **Temps moyen de réparation (MTTR) :** Le Mean Time To Repair représente le temps moyen nécessaire pour réparer un système après une panne. Un MTTR plus bas indique une meilleure maintenabilité du système, c'est-à-dire qu'il peut être remis en service plus rapidement après une panne.
- **Objectif de délai de récupération (RTO) :** Durée maximale acceptable pendant laquelle un système peut être hors service sans pour autant causer des dommages à l'entreprise. Ou autrement dit ; la durée maximale acceptable pour restaurer une panne. Dans le réseau de l'EPB cet objectif est de 3 heures.
- **Objectif de point de récupération (RPO) :** Il s'agit de la fenêtre des données perdues, ou autrement dit, la quantité tolérable de données que l'entreprise peut se permettre de perdre sans qu'il y ait d'impacts irréversibles.

Calcul de la fiabilité :

- **Taux de disponibilité :** Le taux de disponibilité d'un système est une mesure de la probabilité qu'il soit opérationnel et accessible à un moment donné. Il est calculé de cette manière :

$$A = \frac{\text{MTBF}}{\text{MTTR} + \text{MTBF}} = \frac{\text{Temps de bon fonctionnement}}{\text{Temps total}}$$

Avec :

$$MTBF = \frac{1}{\lambda}$$

$$MTTR = \frac{\text{Temps total consacré aux réparations}}{\text{Nombre de réparations}}$$

- **Taux de défaillance :** Le taux de défaillance d'un système est une mesure de la probabilité qu'il tombe en panne pendant une période donnée. Ce paramètre est calculé comme suit :

$$\lambda = \frac{\text{Nombre de totale de pannes}}{\text{Temps total de fonctionnement}}$$

Pour améliorer la fiabilité d'un système et réduire son taux de défaillance, il est important de mettre en œuvre des stratégies similaires à celles visant à améliorer le taux de disponibilité telles ques les mécanismes et stratégies vus précédemment dans ce chapitre.

3.2 Le Clustering

3.2.1 Introduction au Clustering

Le clustering est une technique de conception et de gestion des systèmes et réseaux qui vise à améliorer la disponibilité, la fiabilité et la performance en regroupant plusieurs ressources similaires en un seul cluster. Un cluster, également appelé grappe, est essentiellement un groupe de serveurs ou de nœuds interconnectés qui travaillent ensemble à l'image d'une entité logique unique pour fournir des services ou des applications de manière cohérente et efficace. Ces serveurs sont configurés pour fonctionner de manière coordonnée, de sorte qu'ils puissent se soutenir mutuellement en cas de panne ou de surcharge de travail. Les noeuds de la grappe se partagent un disque de stockage qui fournit un référentiel central pour les données qui doivent être accessibles à tous les éléments du cluster comme illustré dans la figure 3.5.

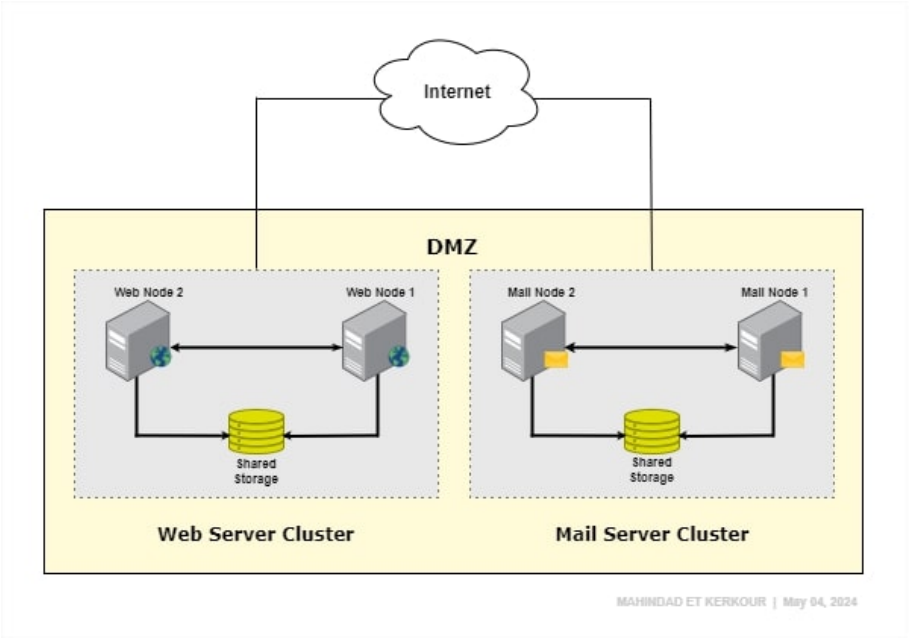


FIGURE 3.5 – Cluster de serveurs Web et messagerie dans une DMZ.

Importance du Clustering :

Le clustering a des avantages significatifs par rapport à l'utilisation d'ordinateurs individuels, tels que :

- **Haute disponibilité :** En regroupant plusieurs ressources informatiques en un seul ensemble cohérent, les clusters permettent d'assurer une disponibilité continue des services. En cas de défaillance d'un nœud ou d'un composant, les autres nœuds du cluster peuvent prendre le relais, assurant ainsi une continuité du service sans interruption.
- **Évolutivité :** Les clusters sont hautement évolutifs, permettant une expansion facile des ressources en ajoutant de nouveaux nœuds. Cette capacité garantit une performance optimale et une disponibilité continue dans des environnements en constante évolution.
- **Centralisation et simplificité de gestion :** En regroupant plusieurs ressources en un seul ensemble cohérent, les clusters simplifient la gestion et l'administration des systèmes. Les tâches de déploiement, de surveillance, de maintenance et de mise à jour peuvent être centralisées et automatisées, réduisant ainsi la complexité opérationnelle.
- **Performance accrue et optimisation des ressources :** En répartissant la charge de travail sur plusieurs nœuds, les clusters permettent de booster les performances globales du système. Cela se traduit par une augmentation des vitesses d'entrée/sortie, une diminution des délais de réponse et l'élimination des points de congestion. En conséquence, le système devient plus

réactif et offre une expérience utilisateur plus fluide.

Malheureusement, les clusters ne sont pas sans inconvénient car leur déploiement peut nécessiter un investissement initial important en matériel, logiciels et licences. On peut y remédier grâce à la virtualisation pour réduire le nombre de serveurs physiques.

3.2.2 Fondements du Clustering :

Modèles de Clustering :

Il existe trois (03) modèles de Clustering :

- **Clustering HA :** L'objectif principal de ce type de cluster est de fournir un niveau de disponibilité plus élevé, une résilience et une gestion centralisée des ressources. Un cluster HA peut migrer une tâche de travail vers l'autre nœud en cas d'erreur ou de mise hors service. Cela peut réduire les temps d'arrêt sans contrôle constant de l'administrateur [30].
- **Clustering load balancing :** Même si l'objectif principal de ce type de cluster est l'augmentation des performances, il offre également une fiabilité accrue. La structure de ce type de cluster n'est pas très différente de celle d'un cluster HA. De nos jours, les logiciels pour un clustering HA ont souvent une fonction d'équilibrage [30].
- **Clustering High Performance Computing :** Les clusters Calcul Haute performance (HPC) nécessite généralement un réseau à faible latence et un grand nombre de serveurs puissants pour accélérer considérablement les calculs et simulations complexes et intensifs [30].

Types de Clustering :

Les types de clustering sont les suivants :

- **Clustering de serveurs :** Le clustering de serveurs consiste à regrouper plusieurs serveurs physiques ou virtuels afin de les faire fonctionner comme une seule unité logique dans l'intention d'éviter la surcharge d'un seul noeud et améliorer les temps de réponse.
- **Clustering de stockage :** Conçu pour regrouper plusieurs unités de stockage en un système unique et centralisé afin de fournir une capacité de stockage élevée.
- **Clustering de pare-feu et de routeurs :** Le clustering de pare-feux et de routeurs est une pratique essentielle dans la gestion des équipements réseaux, visant à renforcer la sécurité, la disponibilité et la performance des

infrastructures. Des solutions comme CARP 4.5.4 (Common Address Redundancy Protocol) est utilisée plus bas dans ce projet.

- **Clustering de machines virtuelles et conteneurs :** Les environnements de virtualisation tirent parti du clustering pour regrouper plusieurs machines virtuelles sur des hôtes physiques. Cette approche procure de nombreux avantages comme une plus grande flexibilité qui permet d'optimiser et d'adapter la gestion des ressources de l'infrastructure aux besoins changeants des applications.

Modes de Clustering :

Il existe deux (02) modes de clustering :

- **Mode actif-actif :** Dans une architecture de cluster en mode actif-actif 3.6, il existe au moins deux nœuds, chacun exécutant simultanément le même service. L'objectif principal est de garantir un équilibrage optimal de la charge. Ce mécanisme intelligent répartit équitablement la charge de travail entre tous les éléments de la grappe, empêchant ainsi la surcharge d'un seul d'entre eux tout en améliorant le débit et les temps de réponse [29].

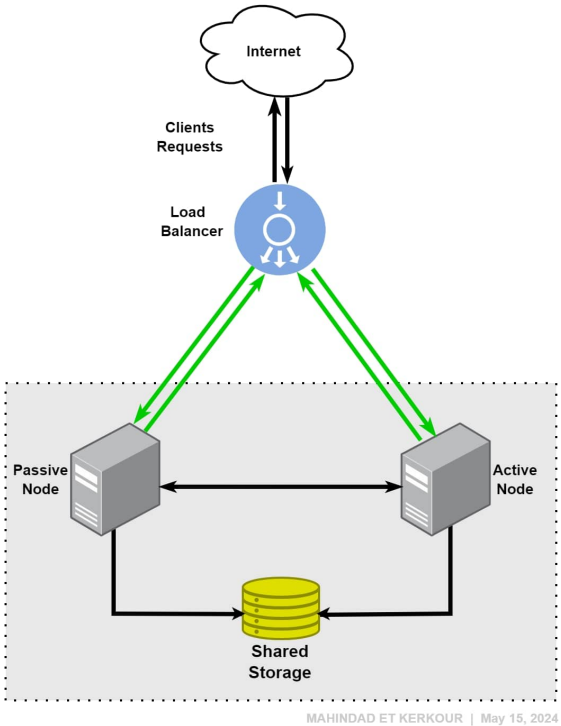


FIGURE 3.6 – Traitement des requêtes clients par les deux noeuds.

- **Mode actif-passif :** Les clusters en mode actif-passif comptent aussi au minimum deux nœuds. Cependant, contrairement aux clusters actifs-actifs où tous les nœuds sont en activité simultanée, ce mode implique qu'un seul

nœud est actif à un moment donné, tandis que les autres restent passifs, en veille, servent de sauvegarde prêtes à prendre le relais en cas de défaillance du nœud principal [29].

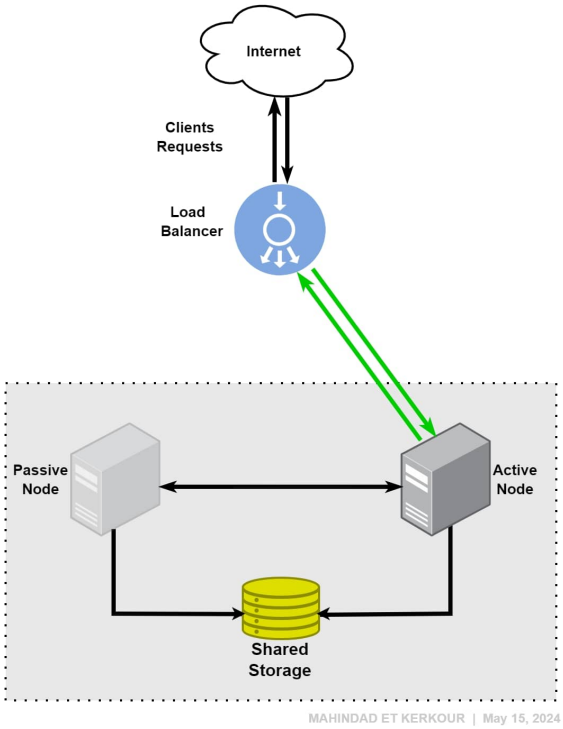


FIGURE 3.7 – Traitement des requêtes clients par le noeud actif du cluster.

3.2.3 Mécanismes et Technologies de Clustering :

Mécanismes de détection des pannes :

- **Quorum :** Le quorum désigne le nombre minimum de nœuds qui doivent être en état de fonctionnement et en communication pour que le cluster puisse prendre des décisions critiques et fonctionner correctement. Le quorum est essentiel pour le maintien de la disponibilité de la grappe, la préservation de l'intégrité des données et pour éviter les conditions de "split-brain" (division du cerveau en anglais) où différents segments du cluster pourraient prendre des décisions conflictuelles.
- **Fencing :** Le fencing est le processus d'isolement d'un nœud ou de protection des ressources partagées lorsqu'un nœud ne fonctionne pas correctement. Si un nœud tombe en panne, il peut contrôler les ressources partagées qui doivent être récupérées et le reste du système doit être protégé. La clôture s'effectue par : Désactivation du nœud ou blocage l'accès au stockage partagé au nœud [17]. La figure 3.8 reflète le fonctionnement du fencing.

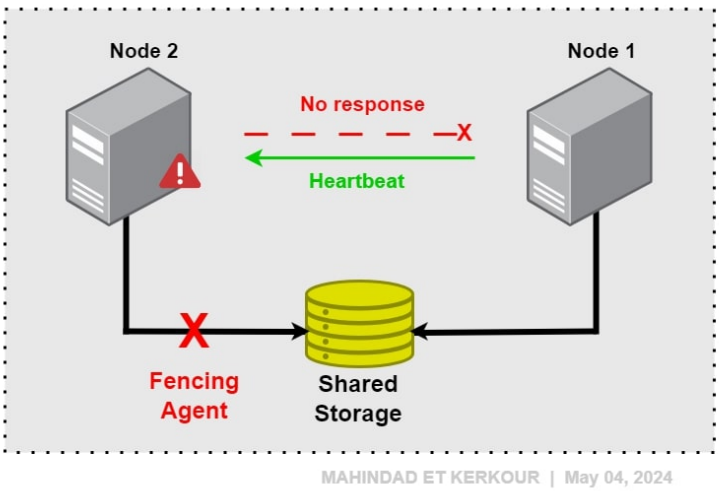


FIGURE 3.8 – Désactivation de l'accès au stockage par l'agent de Fencing après défaillance du noeud 2

- **Heartbeat :** Le gestionnaire de cluster utilise un mécanisme de communication spécifique sur chaque nœud afin de permettre à chaque système de déterminer l'état (actif ou inactif) des autres membres du cluster. Ce mécanisme, nommé Heartbeat, est sans doute le plus important du cluster. Sans cela, le système de sauvegarde n'a aucun moyen de connaître l'état du noeud actif et, par conséquent, aucun moyen de lancer un basculement en cas de panne du système actif. Il repose sur l'échange d'informations entre entités du cluster, qui servent d'indicateurs d'état système [8][25]. Dans l'hyperviseur ProxmoxVE qui sera utilisé plus tard, c'est le gestionnaire de cluster Corosync D qui orchestre les échanges entre membres de la grappe.
- **Pacemaker :** Pacemaker est un gestionnaire de ressources de grappe. Cette algorithme atteint une disponibilité maximale des services de cluster en détectant et en récupérant les pannes au niveau des nœuds et des ressources en utilisant les capacités de messagerie et d'adhésion fournies par le Heartbeat [47].

Outre les techniques précédemment citées, d'autres mécanismes 3.1.3 tels que le basculement, l'équilibrage de charge, la synchronisation et la réplication de données peuvent être déployés pour renforcer la haute disponibilité des clusters.

3.2.4 Conclusion

A travers ce chapitre, nous avons mis en évidence les principes de la haute disponibilité, l'importance d'implémenter les méthodes associées et leurs avantages

au sein d'un réseau d'entreprise. Nous avons aussi insisté sur l'une des technologies qui est le clustering, son fonctionnement, son fondement et les mécanismes relatives à cette solution.

Chapitre 4

Simulation de la nouvelle topologie et discussion des résultats

Introduction

Dans ce chapitre, nous allons procéder à la phase pratique qui constitue le dernier volet de notre travail et qui a pour objectif d'exposer notre mise en œuvre des solutions que nous proposons. Pour ce faire, nous présentons les différents outils que nous utiliserons, ainsi que les différentes configurations nécessaires à implémenter tout au long de ce projet.

4.1 Présentation de l'environnement de travail

4.1.1 Proxmox

L'un des outils principaux utilisé dans la partie pratique de ce projet est l'outil Proxmox Virtual Environment. Proxmox VE 4.1 est une plateforme de virtualisation open source de type 1 bare-metal 2.2 basée sur la distribution Debian Linux.

FIGURE 4.1 – Proxmox Virtual Environment [3].

Proxmox est disponible gratuitement sans aucune fonctionnalité verrouillée dans sa version Community. Cependant, une licence d'abonnement est toute aussi dis-

ponible pour accéder au référentiel d'entreprise, qui offre des correctifs et des mises à jour bien testés dans sa version Entreprise. Les abonnements sont recommandés pour un environnement Proxmox de niveau production. Les caractéristiques principales de Proxmox VE [5] sont :

- **Virtualisation et Réseau :**
  - Proxmox s'appuie sur le module **KVM (Kernel-Based Virtual Machine)** D pour exécuter des machines virtuelles indépendantes ; offrant ainsi une solution de virtualisation complète, et sur **LXC (Linux Containers)** pour gérer des conteneurs légers [51].
  - Virtualisation réseau avancée avec prise en charge des ponts, des VLAN et des fonctionnalités de sécurité grâce aux commutateur virtuel **Open vSwitch** et **Proxmox VE Firewall** F intégrés.
- **Gestion :**
  - Interface Web intuitive pour gérer les noeuds, les machines virtuelles et les conteneurs.
  - Authentification et autorisation granulaires pour gérer et contrôler l'accès aux ressources.
- **Haute disponibilité :** Proxmox VE supporte les technologies de Haute Disponibilité qui sont la clusterisation, la migration, le basculement automatique et la réplication.
- **Stockage :** Proxmox VE se distingue par le large choix de systèmes de stockage dont il dispose (comme LVM D et ZFS D) pour stocker des images de disque virtuel, des modèles ISO et des sauvegardes. En conséquence, il donne à l'utilisateur la flexibilité nécessaire pour exploiter le stockage existant sur le réseau [4].

4.1.2 GNS3

GNS3 (Graphical Network Simulator 3) (Figure 4.2) est une plateforme de simulation de réseaux graphique, libre et multiplateforme, compatible avec Windows, Mac OS et Linux. Cette application permet aux professionnels du domaine des télécommunications et des réseaux de modéliser une large gamme de topologies réseau, des plus simples aux plus complexes, et de tester le fonctionnement ainsi que de reproduire le comportement d'équipements, de services et de protocoles, le tout sans nécessiter de matériel physique.

FIGURE 4.2 – Graphical Network Simulator 3 [20].

4.1.3 Les machines virtuelles

PfSense :

L'ISO pfSense (Figure 4.3) est un fichier image disque contenant le système d'exploitation pfSense basé sur FreeBSD, entièrement géré via une interface Web et capable d'agir comme un routeur et un pare-feu pour protéger les réseaux informatiques [19]. Cette image ISO permet d'installer PfSense sur une variété de plates-formes, offrant des fonctionnalités avancées de filtrage, de routage, de NAT, de VPN, de serveur DHCP, de load balancing, ainsi que d'autres fonctionnalités réseau avancées [49].

FIGURE 4.3 – PfSense [49].

Serveur Windows 2022 :

Windows Server 2022 (Figure 4.4) est la version la plus récente du système d'exploitation serveur de Microsoft, spécialement conçue pour satisfaire les exigences des entreprises de toutes tailles. Il propose une plateforme fiable pour gérer différentes charges de travail, allant des applications classiques aux environnements cloud et hybrides. Il fournit des fonctionnalités telles que la virtualisation et divers services de gestion et de surveillance [64].

FIGURE 4.4 – Serveur Windows 2022 [56].

4.2 Architecture proposée

La figure 4.5 représente l'architecture proposée basée sur le modèle hiérarchique. Elle met en évidence diverses pratiques visant à garantir une haute disponibilité du réseau, en intégrant des principes de redondance pour éviter les SPOF, l'ajout des VLAN et de l'agrégation des liens, ainsi que de l'utilisation d'un hyperviseur open source pour la gestion des machines virtuelles. De plus, une approche de clustering sera utilisée, non seulement pour les serveurs mais également pour les pare-feux afin de garantir la continuité du service même en cas de panne matérielle.

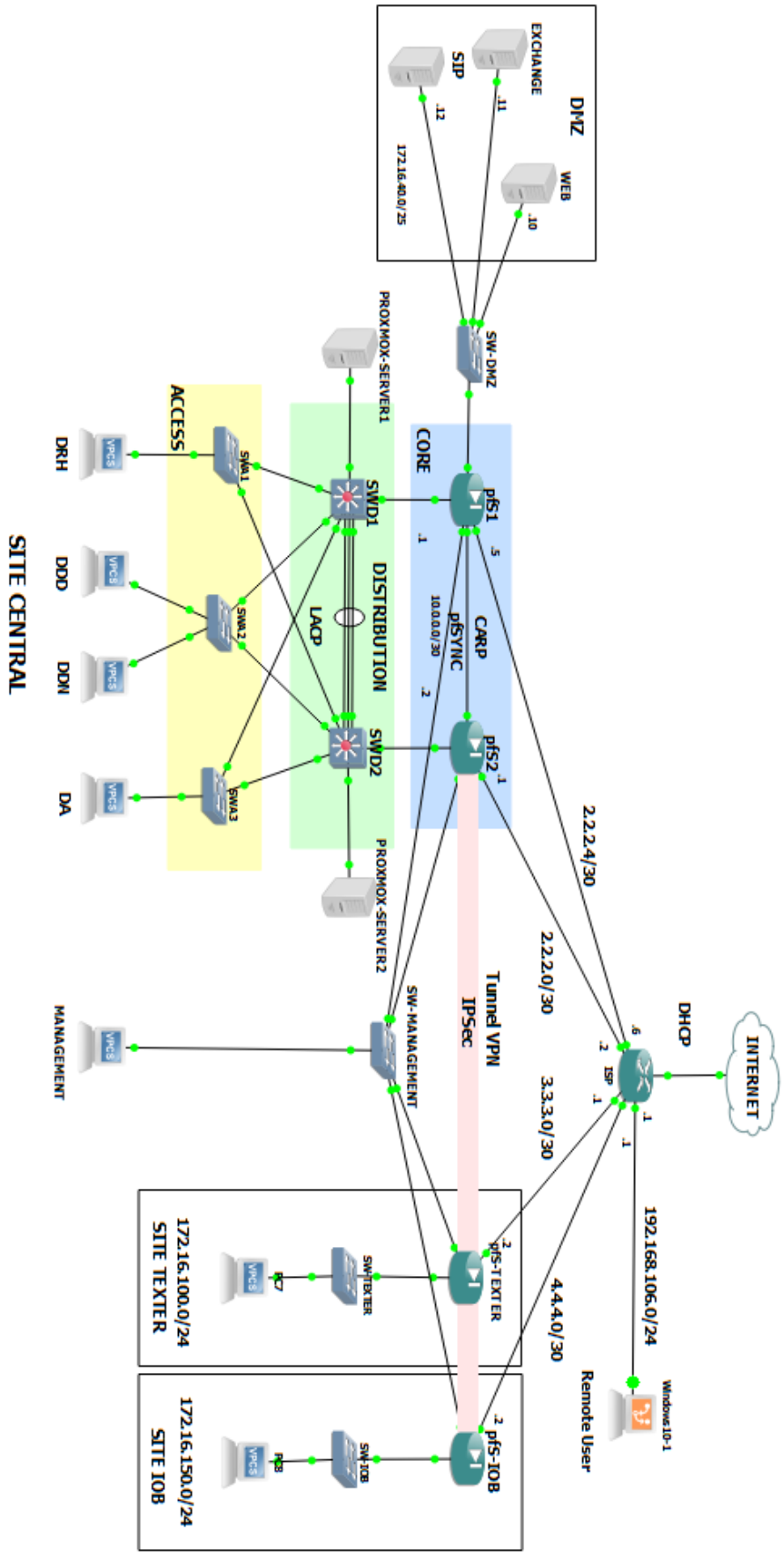


FIGURE 4.5 – Architecture Proposée.

4.3 Méthodologie

Pour mettre en œuvre l'architecture améliorée, nous avons structuré notre travail en trois phases (installation, configuration et tests) suivant les étapes décrites par le diagramme 4.6. Chacune de ces étapes sera détaillée dans la suite de ce chapitre.

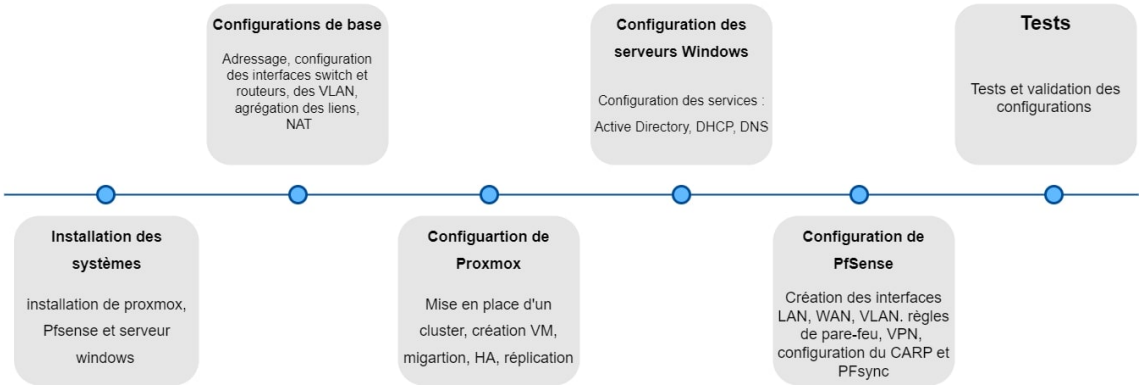


FIGURE 4.6 – Méthodologie de travail.

4.4 Phase 1 : Installation

Dans cette première phase, nous allons présenter principalement l'installation de l'hyperviseur Proxmox VE. Le reste des parties de l'installation se trouve dans l'annexe B.

4.4.1 Proxmox

Matériel minimum recommandé :

Composant	Spécifications minimales
Processeur	Intel Core i3 avec prise en charge la virtualisation matérielle (Intel VT-x ou AMD-V).
Mémoire	1 Go de RAM (Préconiser plus de mémoire dans le cas de la création de machines virtuelles).
Stockage	64 Go SSD

TABLE 4.1 – Matériel minimum recommandé pour le fonctionnement du noeud Proxmox VE.

Nous entamons l'installation de l'hyperviseur en allumant la machine virtuelle pve1, l'assistant d'installation s'affiche : par défaut le mode **graphical** est sélec-

tionné comme le montre la figure 4.7. Il est préférable de lancer l'installation en mode graphique pour facilité le paramètrage du noeud.

FIGURE 4.7 – Assistant d'installation Proxmox VE.

Dans la fenêtre suivante, on indique le disque sur lequel le système sera installé. Par défaut, le système de fichiers ext4 est sélectionné. Le programme d'installation utilise LVM D si ext4 est choisit comme systèmes de fichiers. Il convient de vérifier qu'il y ait bien deux disques (Figure 4.8).

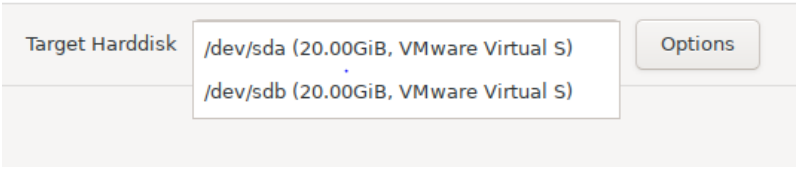


FIGURE 4.8 – Disques du serveur Proxmox.

La page suivante (Figure 4.9) demande des options de configuration de base telles que l'emplacement de l'administrateur, le fuseau horaire et la disposition du clavier.

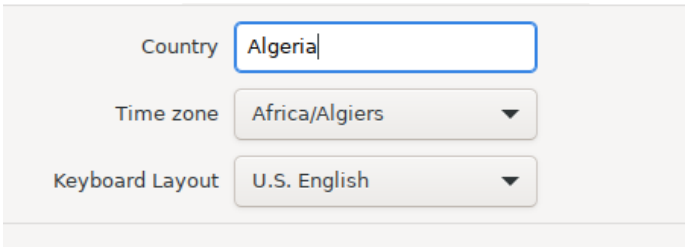


FIGURE 4.9 – Options de configurations (a).

Pour sécuriser le serveur Proxmox, on choisit un mot de passe robuste qui sera attribué au compte du super utilisateur (root) et saisit une adresse email valide

pour recevoir les notifications ; comme des informations sur les mises à jour de packages disponibles et/ou des messages d'erreurs (Figure 4.10).

FIGURE 4.10 – Options de configurations (b).

La dernière étape est la configuration du réseau (Figure 4.11) :

- Choix de l'interface de gestion qui permettera, un peu plus tard, d'accéder à l'interface graphique pour effectuer des tâches d'administration. Les interfaces réseau **UP** affichent un cercle plein devant leur nom.
- Attribution d'un nom de domaine (hostname (FQDN)) au serveur Proxmox.
- Allocation d'une adresse IP, d'une passerelle et d'un serveur DNS (Domain Name System). Il faut faire attention à adapter l'adressage IP du noeud à celle de la carte réseau virtuelle retenue lors de la création de la machine virtuelle dans VMware Workstation. Ces paramètres peuvent être modifiés même après installation définitive du logiciel.

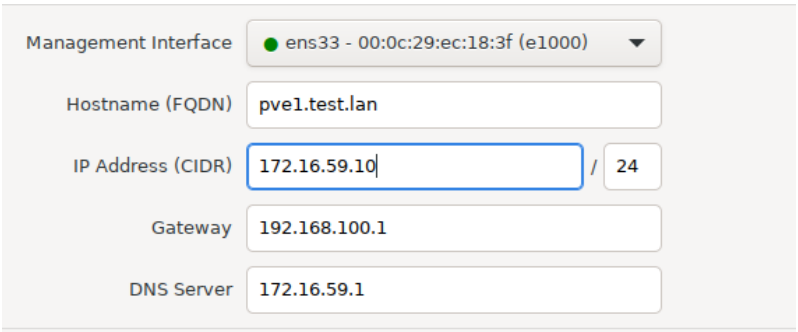


FIGURE 4.11 – Configuration réseau du serveur pve1.

La figure 4.12 représente un tableau récapitulatif des configurations effectuées. Si les paramètres sont corrects, nous pouvons lancer l'installation de l'hyperviseur. En cliquant sur **Install**, la machine redémarrera pour finaliser l'installation. Il est à noter de l'importance des adresses.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Algeria
Timezone:	Africa/Algiers
Keymap:	en-us
Email:	melissa.kerrkour@tech.univ-bejaia.dz
Management Interface:	ens33
Hostname:	pve1
IP CIDR:	172.16.59.10/24
Gateway:	192.168.100.1
DNS:	172.16.59.1

FIGURE 4.12 – Tableau récapitulatif des configurations.

Après le reboot de la machine, l'écran d'accueil s'affiche comme dans la figure 4.13. Nous y accèderons en tant que super utilisateur en saisissant devant le login **root** et le mot de passe associé à ce compte.

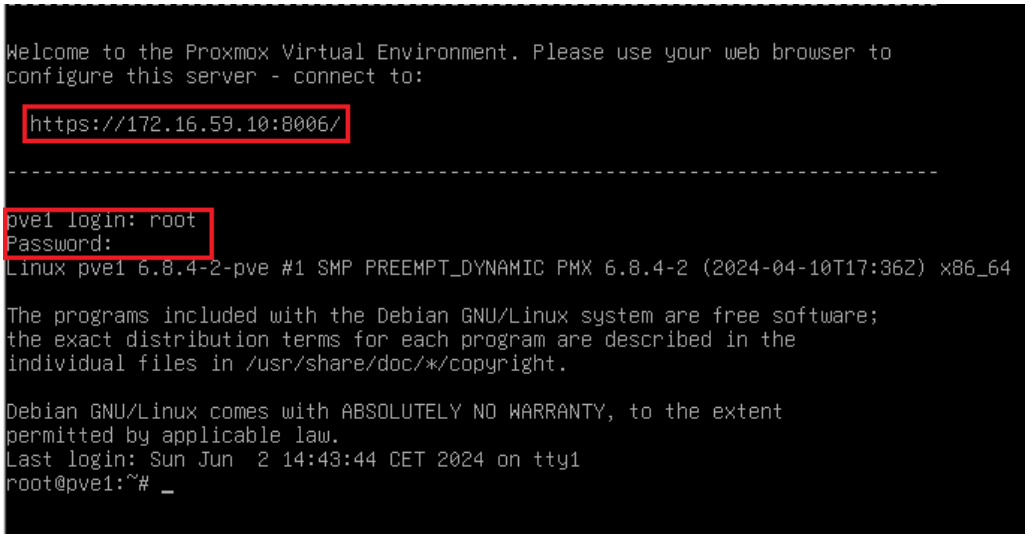


FIGURE 4.13 – Ecran d'accueil de l'interface de ligne de commande de pve1.

Maintenant il est possible de lancer l'interface graphique de la machine sur un navigateur en entrant l'adresse IP et le numéro de port affiché sur l'écran d'accueil précédent de la manière exposée dans la figure 4.14 : **http :// [@IP] :8006/**.

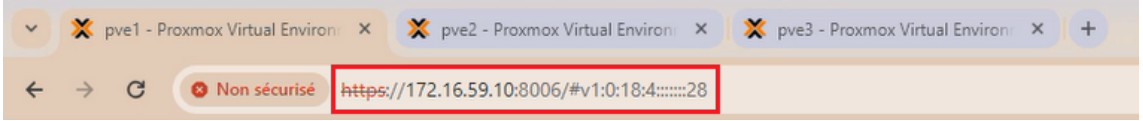


FIGURE 4.14 – Lancement de l'interface graphique en entrant l'adresse IP du serveur pve1.

Dans la figure 4.15 on nous demande d'entrer le nom d'utilisateur et le mot de passe.

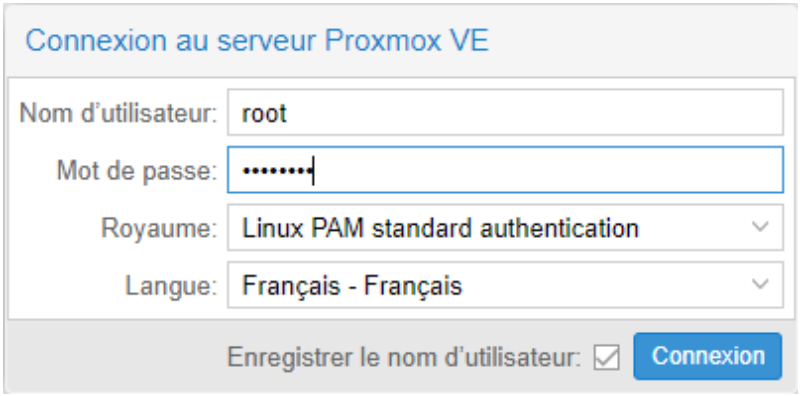


FIGURE 4.15 – Connexion au serveur pve1.

Nous effectuons les mêmes étapes deux fois pour installer pve2 et pv3, pour par la suite, créer un cluster de trois machines virtuelles 3.2.2.

4.5 Phase 2 : Configuration

4.5.1 Configuration de base

1. **Table d'adressage générale :** Le tableau 4.2 représente toutes les adresses IP attribuées pour les différentes interfaces de notre nouvelle topologie.

Equipement	Interface - Id	Adresse réseau	Passerelle
Pare-feu pfS1	em0 - wan em1 - lan em2 - vlan em3 - dmz em4 - pfSync	2.2.2.5/30 172.16.0.2/24 172.16.40.1/25 10.0.0.1/30	2.2.2.6
Pare-feu pfS2	em0 - wan em1 - lan em2 - vlan em3 - dmz em4 - pfSync	2.2.2.1/30 172.19.0.3/24 172.16.40.2/25 10.0.0.2/30	2.2.2.2
Pare-feu TEX-TER	em0 - wan em1 - lan em2 - LOCAL	3.3.3.2/30 172.16.0.4/24 172.16.100.1/24	3.3.3.1
Pare-feu IOB	em0 - wan em1 - lan em2 - LOCAL	4.4.4.2/30 172.16.0.5/24 172.16.150.1/24	4.4.4.1
Routeur ISP	e0/0 e0/1 e0/2 e0/3 e1/0	DHCP 2.2.2.2/30 2.2.2.6/30 3.3.3.1/30 192.168.106.254/24	

TABLE 4.2 – Table d'adressage générale.

2. **Table d'adressage des VLAN :** Le tableau 4.3 présente l'ensemble des VLAN créés pour chaque département de l'EPB, ainsi que les adresses réseaux associées.

Nom VLAN	Id	Adresse réseau	Nom VLAN	Id	Adresse réseau
DRH	50	172.16.50.0/24	DA	56	172.16.56.0/24
DG	51	172.16.51.0/24	DC	57	172.16.57.0/24
DFC	52	172.16.52.0/24	DM	58	172.16.58.0/24
DE	53	172.16.53.0/24	Datacenter	59	172.16.59.0/24
DDD	54	172.16.54.0/24	Management	60	172.16.60.0/24
DDN	55	172.16.55.0/24	Native	99	/

TABLE 4.3 – Table d'adressage VLAN.

3. **Configuration de l'agrégation des liens :** L'agrégation des liens se fera au niveau des deux switchs de distribution pour les trois liens qui les relient, en utilisant le protocole standard LACP (Link Aggregation Control Protocol) en mode **actif**. Avant cela, il est conseillé d'activer le protocole STP (Spanning Tree Protocol) (Annexe D) en mode rapide afin de permettre une

convergence plus rapide, réduisant le temps de récupération après une modification ou une défaillance du réseau (Voir figure 4.16).

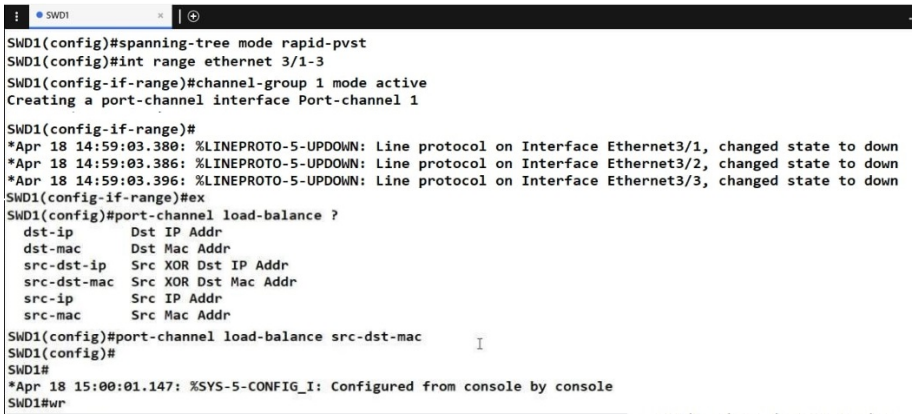


FIGURE 4.16 – Agrégation des liens.

La commande **port-channel load-balance src-dst-mac** permettra d'équilibrer la charge entre les deux commutateurs.

4. **Configuration du VTP :** La configuration du protocole VTP représentée par les figures 4.17 et 4.18 se fera au niveau des switchs. Tous les switchs devront avoir le le même nom de domaine VTP ainsi que le même mot de passe pour qu'ils puissent se synchroniser et partager les informations VLAN. Pour les switchs de distribution, le SWD1 sera en mode serveur et le SW2 en mode client :

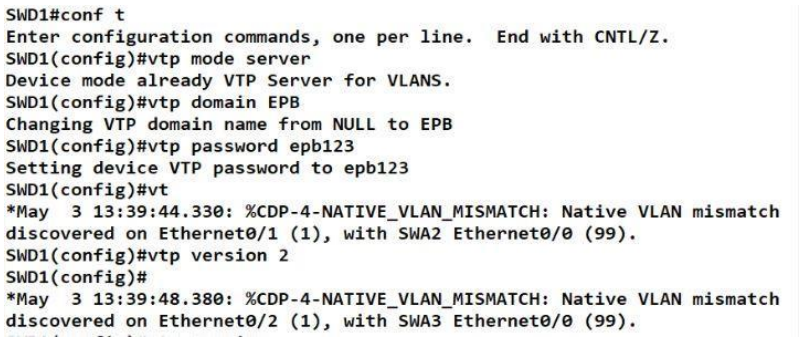


FIGURE 4.17 – Serveur VTP.

```
SWD2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWD2(config)#vtp domain EPB
Changing VTP domain name from NULL to EPB
SWD2(config)#vtp p
*May  3 13:40:35.148: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/2 (1), with SWA3 Ethernet0/1 (99).
SWD2(config)#vtp password epb123
Setting device VTP password to epb123
SWD2(config)#vtp version 2
SWD2(config)#no vtp mode server
Device mode already VTP server for VLAN feature
Resetting device to VTP SERVER mode.
SWD2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWD2(config)#vtp domain EPB
Domain name already set to EPB.
SWD2(config)#vtp password epb123
Password already set to epb123
```

FIGURE 4.18 – Client VTP.

Les switchs d'accès, quant à eux, seront en mode client et auront la même configuration faite au niveau du SWD2 (Figure 4.18).

5. **Configuration des VLAN :**
   - **Création des VLAN :** Après la configuration du VTP, la création des VLAN pourra se faire uniquement sur le switch configuré en tant que serveur VTP. Ainsi, il distribue automatiquement les informations de configuration des VLAN aux clients VTP. Cela se fait avec les commandes suivantes :

     ```
     SWD1(config)#vlan id_VLAN
     SWD1(config-vlan)#name nom_VLAN
     ```

Le résumé de la création des VLAN sur le switch SWD1 est donnée par la figure 4.19. On y constate que tous les VLAN sont actifs et opérationnels. En complément, des VLAN privés ont été configurés au niveau de la DMZ, comme détaillé dans l'annexe C.

FIGURE 4.19 – Résumé des VLAN créés.

- **Configuration des ports d'accès :** Nous devons désormais assigner les

ports aux VLAN correspondants, pour cela les commandes données par la figure 4.20 (a, b et c) sont exécutées.

```
SWA1(config)#interface ethernet 0/2
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport acces vlan 50
```

(a) Ports d'accès au niveau du SWA1.

```
SWA2(config)#interface ethernet 0/2
SWA2(config-if)#switchport mode access
SWA2(config-if)#switchport access vlan 54
SWA2(config-if)#ex
SWA2(config)#interface ethernet 0/3
SWA2(config-if)#switchport mode access
SWA2(config-if)#switchport access vlan 55
```

(b) Ports d'accès au niveau du SWA2.

```
SWA3(config)#interface ethernet 0/2
SWA3(config-if)#switchport mode access
SWA3(config-if)#switchport access vlan 60
```

(c) Ports d'accès au niveau du SWA3.

FIGURE 4.20 – Configuration des ports d'accès.

- **Configuration des liens trunk :** Pour faire transiter le trafic des VLAN vers les couches supérieures de notre architecture, il est essentiel de configurer des liens trunk. Ces derniers permettent de transporter le trafic de plusieurs VLAN sur une seule liaison physique entre switches. Les figures 4.21 et 4.22 présentent les étapes requises pour configurer des liens trunk sur nos switches.

```
SWD1(config)#interface range ethernet 0/0-3
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
*May  3 13:44:06.057: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/1 (1), with SWA2 Ethernet0/0 (99).
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#
*May  3 13:44:08.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet0/3, changed state to down
SWD1(config-if-range)#switchport trunk native vlan 99
SWD1(config-if-range)#do wr
SWD1(config)#interface range ethernet 1/1-3
SWD1(config-if-range)#switchport mode trunk
*May  3 13:45:13.778: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/0 (99), with SWA1 Ethernet0/0 (1).
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#switchport trunk native vlan 99
SWD1(config-if-range)#end
```

FIGURE 4.21 – Trunk des liens du SWD1.

```
SWA1(config)#interface range ethernet 0/0-1
SWA1(config-if-range)#switchport trunk encapsulation dot1q
*May  3 13:47:45.852: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/1 (1), with SWD2 Ethernet0/0 (99).
*May  3 13:47:46.064: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/0 (1), with SWD1 Ethernet0/0 (99).
SWA1(config-if-range)#switchport trunk encapsulation dot1q
SWA1(config-if-range)#switchport mode trunk
SWA1(config-if-range)#switchport trunk native vlan 99
SWA1(config-if-range)#ex
SWA1(config)#interface range ethernet 1/1-3
SWA1(config-if-range)#switchport trunk encapsulation dot1q
SWA1(config-if-range)#switchport mode trunk
SWA1(config-if-range)#switchport trunk native vlan 99
```

FIGURE 4.22 – Trunk des liens du SWA1.

Les mêmes configurations seront reproduites sur le SWD2 pour les liens connectés aux interfaces du SWD1 et des autres switches d'accès, mais aussi sur les switches d'accès pour les liens connectés aux switches de distribution.
Pour plus de sécurité, des commandes supplémentaires seront ajoutées afin de sélectionner les VLAN autorisés sur le tronc. La configuration des switches d'accès est présentée dans la figure 4.23, mais elle sera également appliquée aux interfaces des switches SWD1 et SWD2.

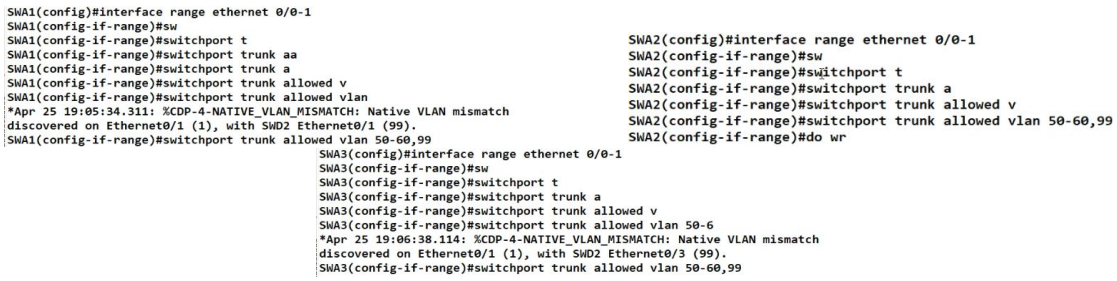


FIGURE 4.23 – Autorisation du trafic sur les liens trunk.

6. **Configuration du routeur ISP :**
   - **Configuration des interfaces :** La configuration des interfaces du routeur se fait en activant l'interface concernée avec la commande **no shutdown** et en attribuant l'adresse et le masque du sous-réseau statiquement avec la commande **ip address** telle que le montre la figure 4.24 (Voir la table 4.2 pour les adresses de chaque interface) :

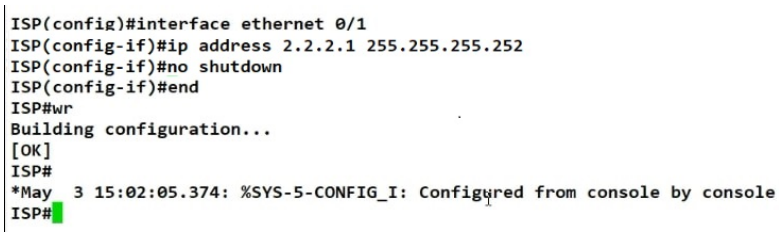


FIGURE 4.24 – Configuration de l'interface e0/1.

Une configuration du service DHCP sera ajoutée à l'interface e1/0 (Figure 4.25) pour permettre à chaque utilisateur distant d'accéder à internet en recevant une adresse IP dynamique à partir de la plage d'adresse **[192.168.106.11 192.168.106.253]**. Cette configuration inclura donc l'adresse du réseau et de son masque, l'adresse de la passerelle par défaut, les adresses des serveurs DNS (Domain Name System), et spécifiera les adresses à exclure pour des raisons de gestion et de sécurité.

```
ISP(config)#interface ethernet 1/0
ISP(config-if)#no shu
ISP(config-if)#no shutdown
ISP(config-if)#ip address 192.168.106.254  255.255.255.0
ISP(config-if)#
ISP(config-if)#exit
ISP(config)#ip dhcp
ISP(config)#ip dhcp ex
ISP(config)#ip dhcp excluded-address 192.168.106.1 192.168.106.10
ISP(config)#ip dhcp pool
ISP(config)#ip dhcp pool lanvpn
ISP(dhcp-config)#net
ISP(dhcp-config)#netw
ISP(dhcp-config)#network 192.168.106.0 255.255.255.0
ISP(dhcp-config)#def
ISP(dhcp-config)#default-router 192.168.106.254
ISP(dhcp-config)#dns
ISP(dhcp-config)#dns-server 8.8.8.8
ISP(dhcp-config)#dns-server 8.8.4.4
```

FIGURE 4.25 – Configuration de l'interface e1/0.

- **Configuration du NAT :** La configuration du NAT se fait au niveau du routeur ISP représentant le fournisseur d'accès à Internet (Figure 4.26). Nous indiquons l'interface qui sera désignée comme extérieure (outside) et les interfaces qui seront désignées comme intérieures (inside), tout en permettant aux réseaux internes d'accéder à l'extérieur via le NAT, cela garantirait une communication fluide et sécurisée avec Internet.

```
ISP(config)#interface e0/0
ISP(config-if)#ip nat outside
ISP(config-if)#ex
ISP(config)#ip access-list standard NAT1
ISP(config-std-nacl)#permit 2.2.2.0 0.0.0.3
ISP(config-std-nacl)#permit 3.3.3.0  0.0.0.3
ISP(config-std-nacl)#permit 2.2.2.4  0.0.0.3

ISP(config)#ip nat inside source list NAT1 interface ethernet0/0 overload
ISP(config)#ex
% Ambiguous command:  "ex"
ISP(config)#end
ISP#wr
Building configuration...
[OK]
ISP#
ISP(config)#interface  ethernet0/2
ISP(config-if)#ip nat inside
ISP(config)#interface Ethernet0/3
ISP(config-if)#ip nat inside
ISP(config)#interface  ethernet 0/1
ISP(config-if)#ip nat inside
ISP(config-if)#end
```

FIGURE 4.26 – Configuration du NAT.

4.5.2 Configuration de Proxmox

Cette partie est consacrée à la configuration de l'hyperviseur proxmox où nous appliquerons les principes de clustering, gestion des ressources, de VM et de haute disponibilité.

Mise en place d'un cluster en mode actif-passif :

La création du cluster en mode actif-passif 3.2.2 se fera à partir de l'interface graphique. Dans le **Centre de données** du noeud pve1, nous nous dirigeons vers la rubrique **Grappe de serveurs** et sélectionnons **créer une grappe de serveurs** comme montré en rouge dans la figure 4.27.

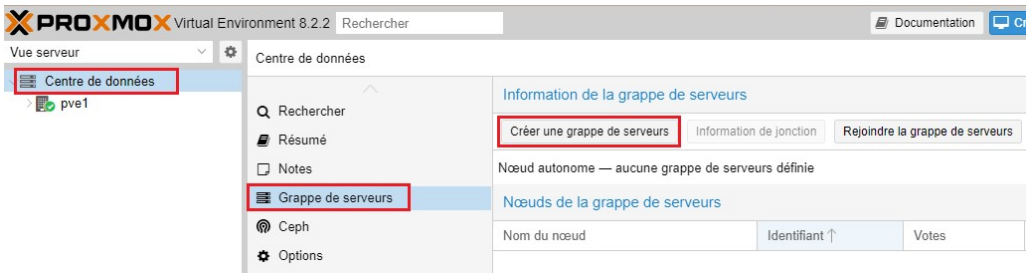


FIGURE 4.27 – Début de création du cluster.

À compter de là, nous affectons un nom et une adresse réseau au cluster (Figure 4.28). Nous garderons l'adresse par défaut.

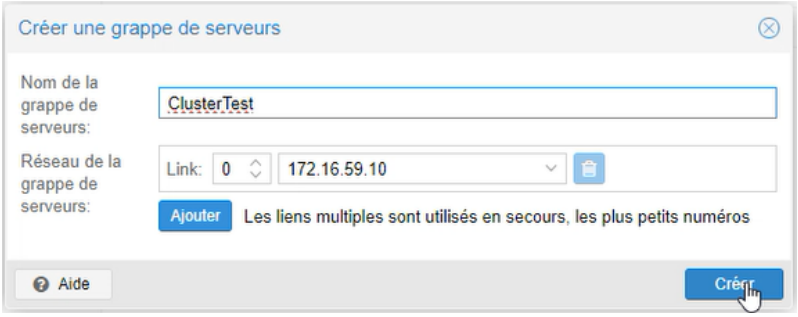


FIGURE 4.28 – Affectation d'un nom et d'un réseau au cluster.

Une fenêtre qui indique le statut de création 4.29 s'affiche :

FIGURE 4.29 – Affichage du statut de création du cluster.

À ce niveau, **Corosync Cluster Engine** (Annexe D) génère une clé d'authentification qui sera enregistrée dans un fichier nommé authkey situé dans le répertoire **/etc/corosync**. Cette clé garantit une communication protégée entre les nœuds et que seuls les nœuds la possédants sont autorisés à rejoindre le cluster. Le message **TASK OK** devrait apparaitre, ce qui témoigne de la bonne création de la grappe. Nous notons que le statut de Corosync affiche **running** (Figure 4.30) qui veut dire en marche.

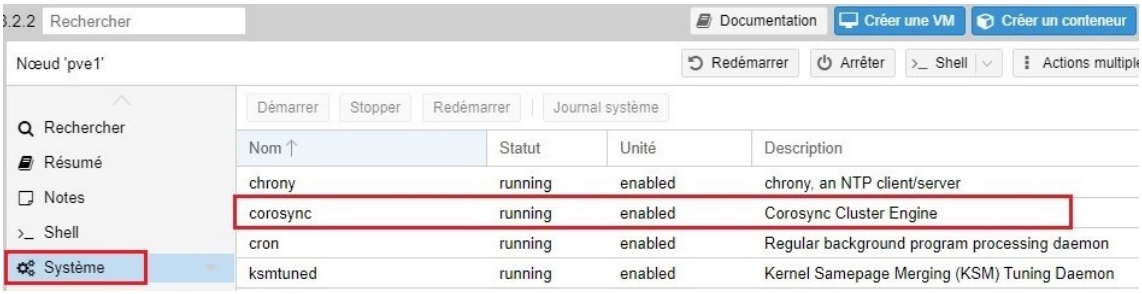


FIGURE 4.30 – Statut de Corosync après création du cluster

Pour regrouper les noeuds, nous copions **'information de jonction** qui est la clé générée auparavant (Figure 4.31),

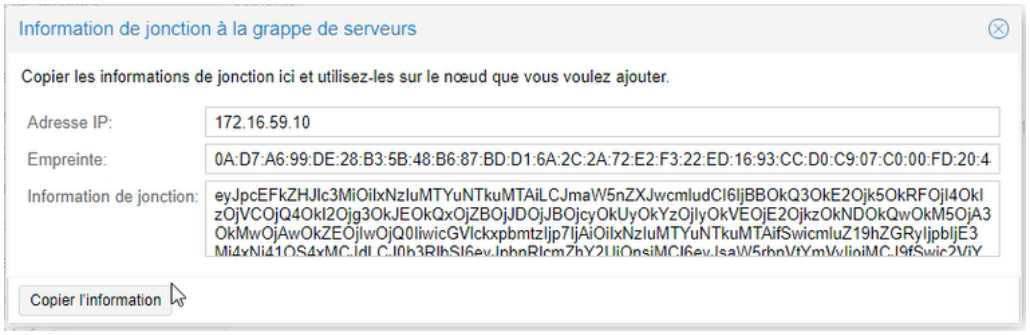


FIGURE 4.31 – Génération de la clé d'authentification.

Nous collons dans **Rejoindre la grappe de serveurs** au niveau du node pve2 en indiquant le mot de passe du serveur pve1 et cliquons sur **Rejoindre 'Cluster-Test'** tel qu'indiqué dans la figure 4.32.

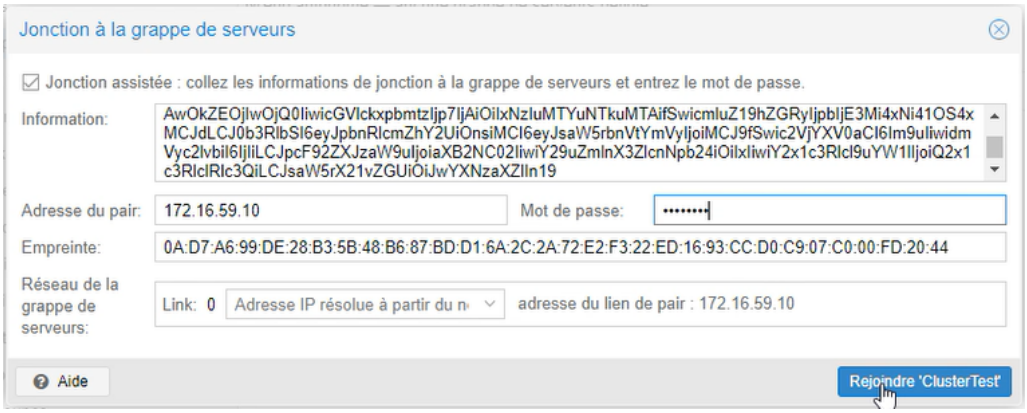


FIGURE 4.32 – Jonction du noeud pve2 à la grappe ClusterTest.

À ce stade, nous remarquons dans la figure 4.33 que dans le menu situé à gauche de la GUI (Graphical User Interface), pve1 et pve2 sont réunis, ce qui offre une gestion centralisée et une meilleure visibilité sur l'état de la grappe. Si ce n'est pas le cas, il suffit de rafraîchir la page du navigateur. Idem pour les ressources des serveurs qui ont été réunis. Nous réiterons les étapes similaires pour le pve3.

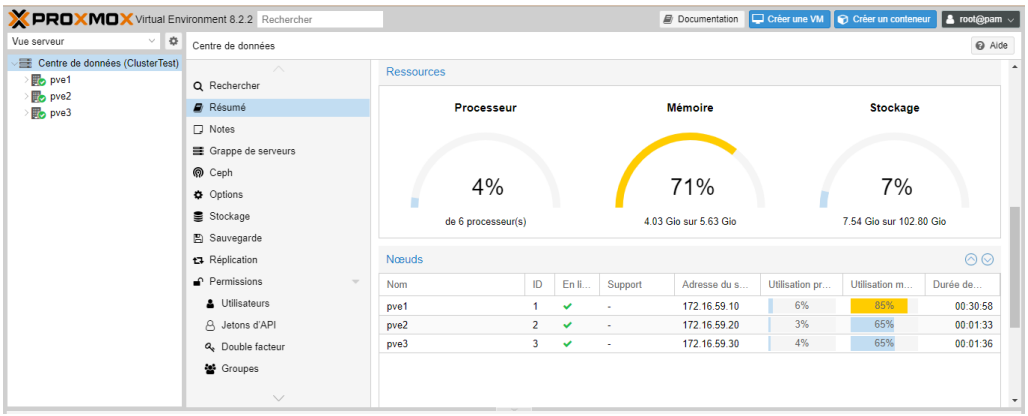


FIGURE 4.33 – Résumé du centre de données après création du cluster.

La configuration ne s'arrête pas là, il est temps de concevoir un disque de stockage partagée. Ce disque de stockage partagé va servir, d'une part, à emmagasiner les VMs, et d'autre part à ce que ces machines virtuelles puissent être accessibles par les tous serveurs Proxmox du cluster, ce qui assure la haute disponibilité [10].

Voyons d'abord l'état de nos disques .

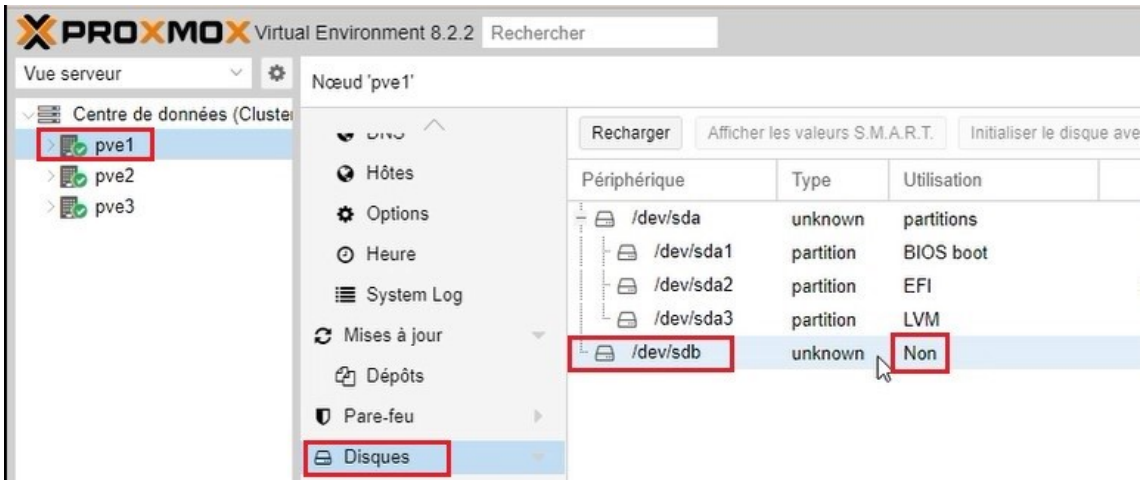


FIGURE 4.34 – Vérification de l'état des disques.

Le disque **dev/sdb** non utilisé, encadré en rouge dans la figure 4.34, est le disque ajouté lors de l'installation la machine virtuelle Proxmox en annexe B.1 ; c'est là qu'il nous sera utile. Nous choisissons de créer un stockage **ZFS** sur chacun des serveurs et qui porterons le même identifiant. Cette uniformité est essentielle pour permettre aux machines virtuelles migrées vers de nouveaux nœuds de localiser et d'accéder correctement au disque virtuel partagé. Si les noms des stockages ZFS diffèrent, les VM migrées ne pourront pas identifier le chemin approprié pour accéder à leurs données, ce qui entraînerait des erreurs et des interruptions de service.

Dans **ZFS** localisé dans la rubrique **Disques** de pve1, nous cliquons sur **Créer :ZFS**. Une fenêtre apparait, nous y affectons un nom et le disque dev/sdb tel que dans la figure 4.35. Nous cocherons la case **Ajouter un stockage** que cette fois-ci.

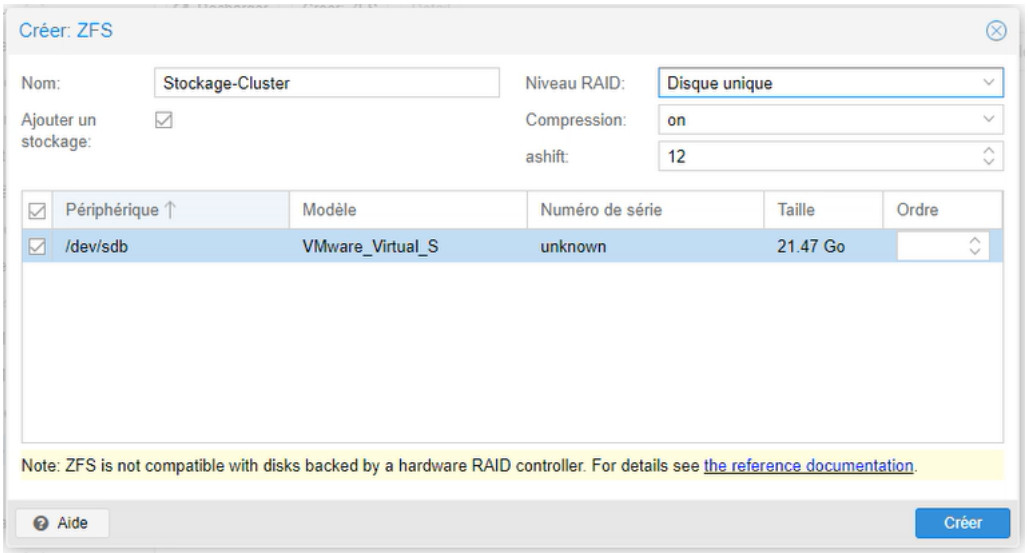


FIGURE 4.35 – Création du stockage ZFS.

Comme on peut le voir dans la figure 4.36, le volume de stockage est créé. Il faudra suivre les mêmes étapes pour le restes des noeuds. les stockages ne s'affichent pas pour pve2 et pve3 pour l'instant. Pour que ce volume de stockage soit entièrement opérationnel et les VMs stockées hautements disponibles, il est nécessaire de regrouper les 3 serveurs dans le pool ZFS depuis **Centre de données > stockage**. Notre plage de stockage devrait y être. Dans le cas contraire on clique sur le **Volume ZFS** ensuite **Ajouter** pour l'établir (Figure 4.37).

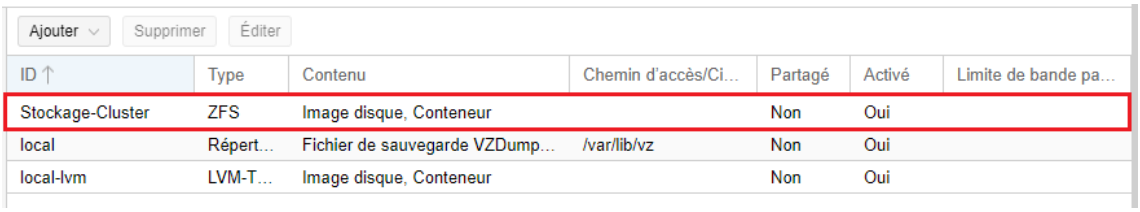


FIGURE 4.36 – Fin de la création du stockage ZFS.

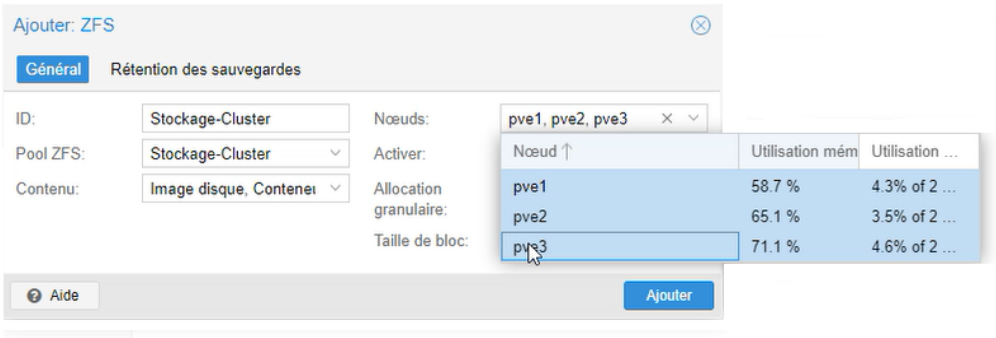


FIGURE 4.37 – Ajout des trois noeuds au volume ZFS.

Création d'une VM :

Avant d'entamer cette section, il est à noter que les paramètres de création diffèrent d'une VM à une autre est ce en raison du système d'exploitation invité et des fonctionnalités spécifiques que l'on souhaite activer. il est donc recommandé d'exploiter la documentation officielle de l'hyperviseur Proxmox avant toute manipulation (`https://pve.proxmox.com/pve-docs/chapter-qm.html`).

À droite de l'interface graphique se trouve **Créer une VM**. En cliquant dessus l'assistant de création apparait (Figure 4.38) : Elle demande d'attribuer un nom et un ID unique à la VM. En sélectionnant suivant (Figure 4.39), il introduire une image de média du logiciel que l'on souhaite intallé sur l'hyperviseur et choisir le système d'exploitation adéquat à l'ISO. Pour notre part, nous choisissons de ne pas ajouter d'image média ; Cette VM servira seulement à effectuer des tests.

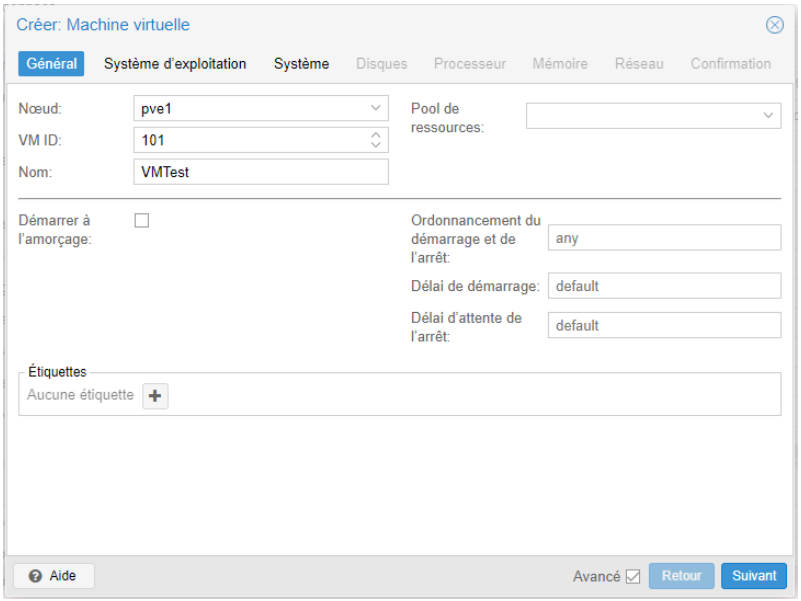


FIGURE 4.38 – Configurations générale.

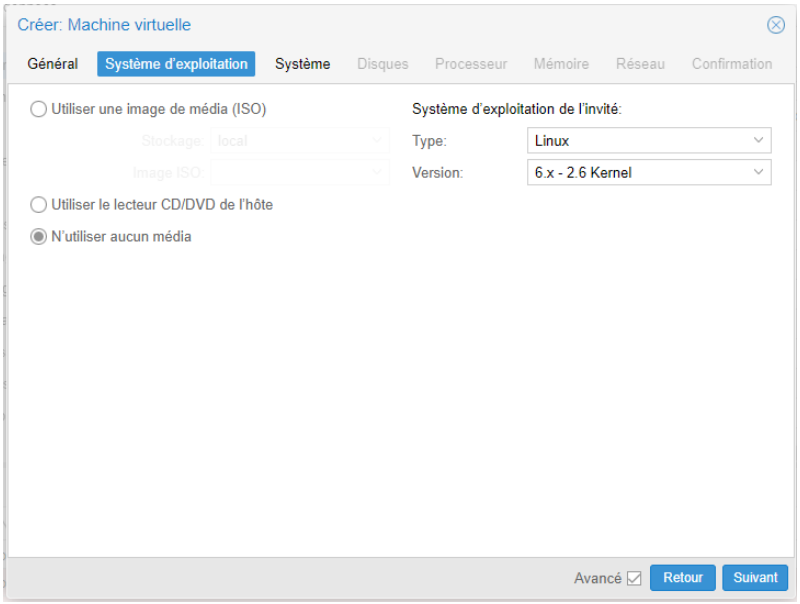


FIGURE 4.39 – Configurations système.

Dans la partie **Système** (Figure 4.40), les paramètrees par défaut sont gardés.

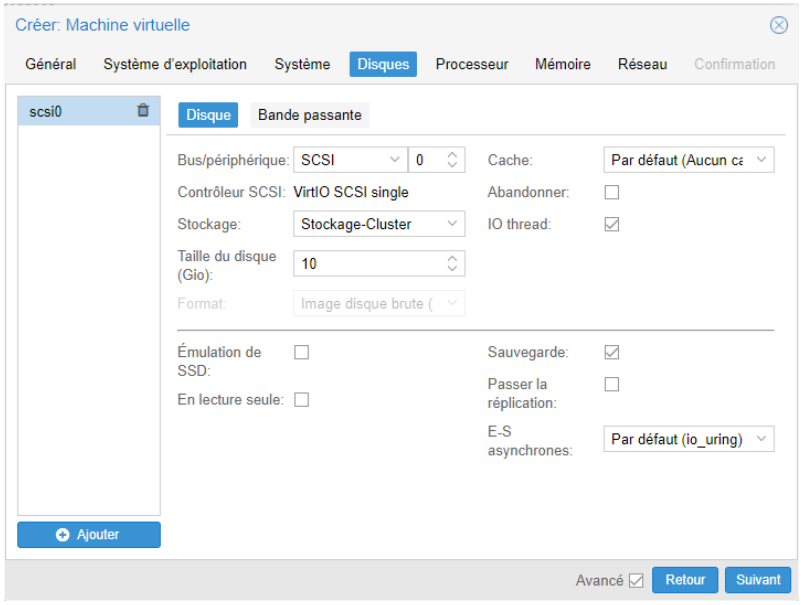


FIGURE 4.41 – Configurations Disques.

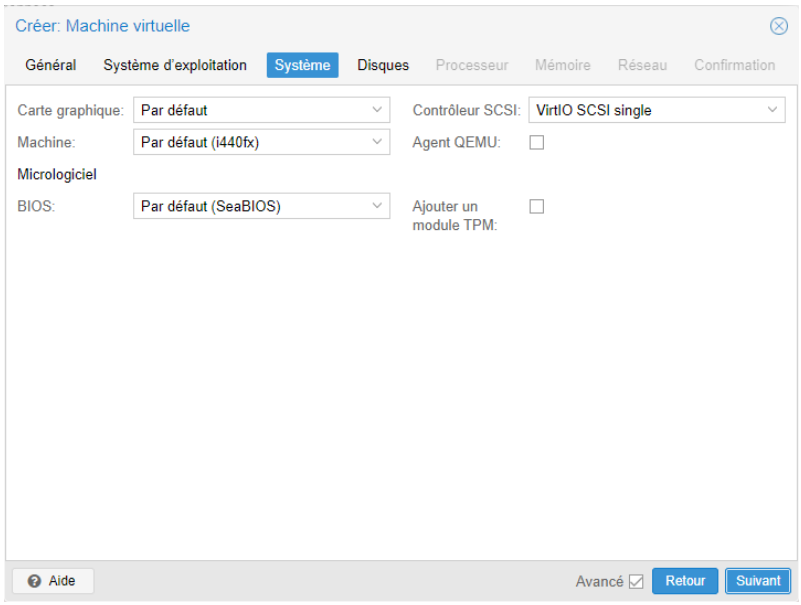


FIGURE 4.40 – Configurations système d'exploitation.

La VM doit impérativement être stocker dans le volume précédemment créé (Figure 4.41). La taille du disque de la machine est de 10Go comme indiqué par la figure 4.41. Le reste des paramètres seront laissés par défaut ainsi que pour les configurations **Processeur** (Figure 4.42) .

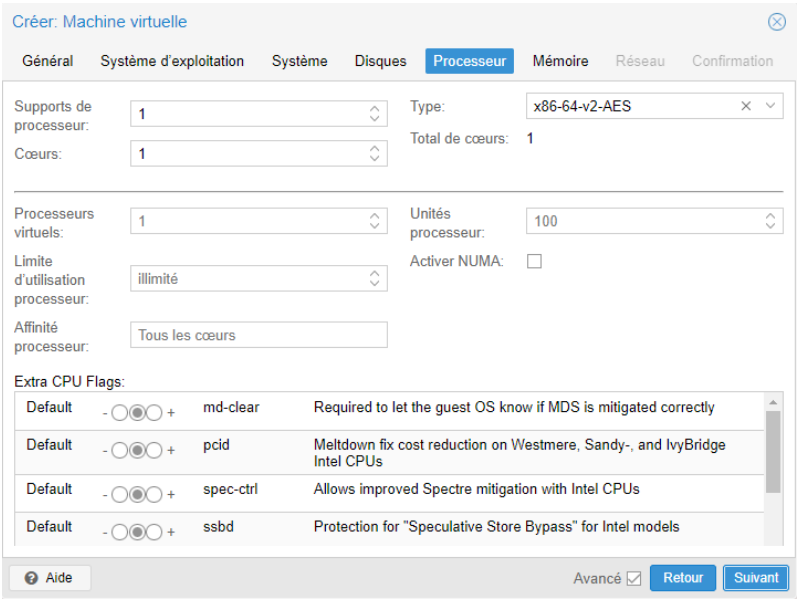


FIGURE 4.42 – Configurations Processeur.

Aucun changement n'ait effectué dans la figure 4.43.

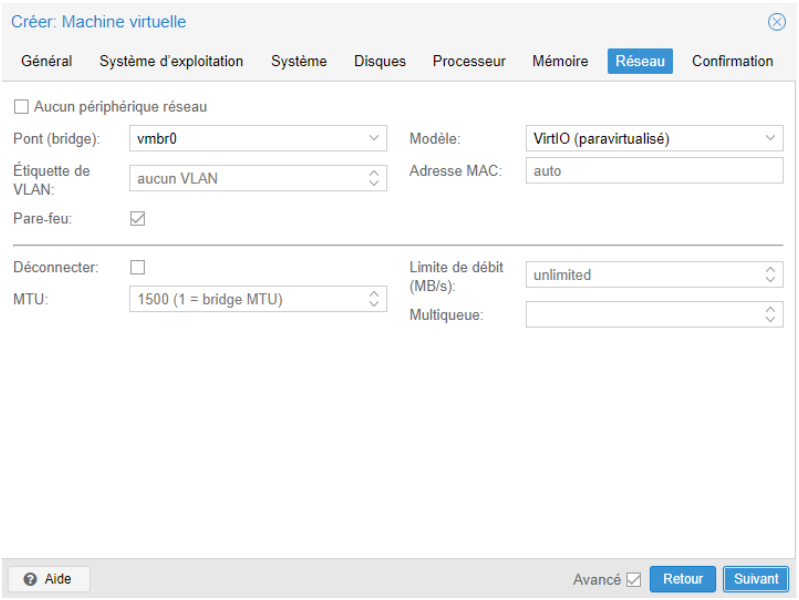


FIGURE 4.43 – Configurations Réseau.

Enfin, un tableau récapitulant toutes les configurations s'affiche (Figure 4.44). La machine virtuelle apparait dans le noeud pve1 en terminant la création (Figure 4.45).

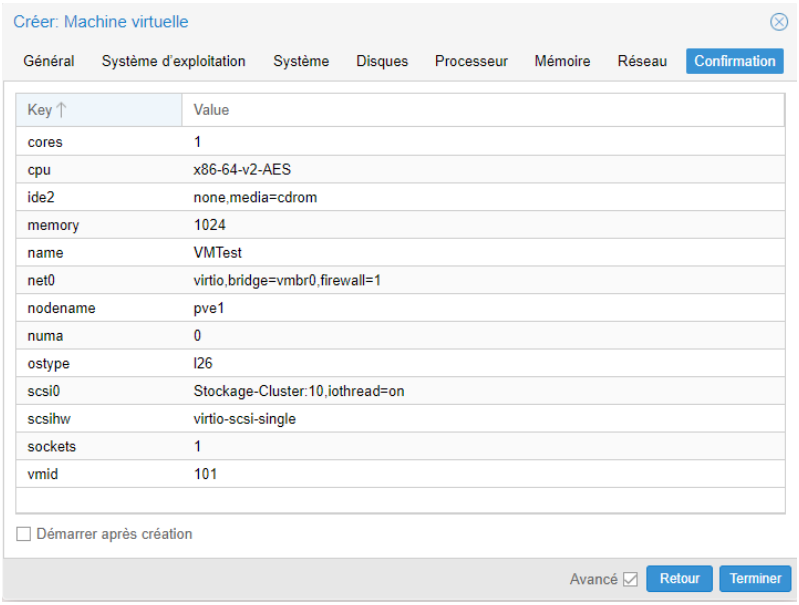


FIGURE 4.44 – Tableau récapitulatif des configurations.

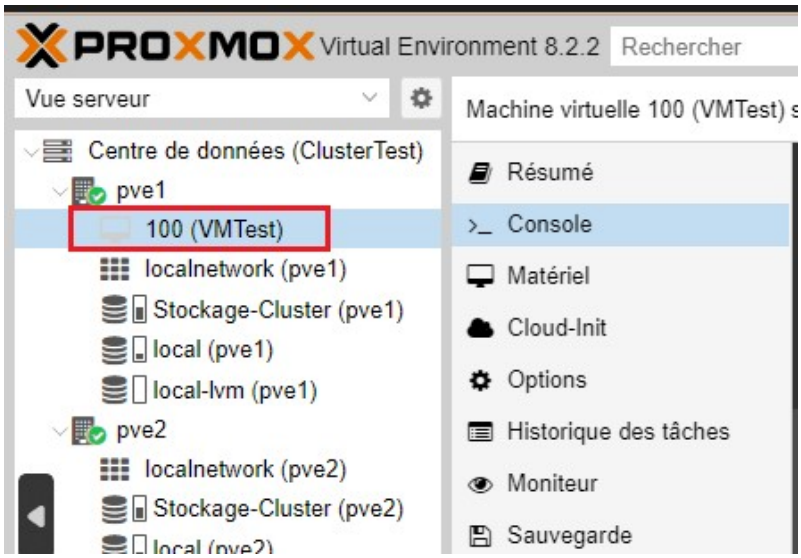


FIGURE 4.45 – Fin de la création de la machine virtuelle.

L'adresse IP allouée à la VM est 172.16.59.134/24. Nous en aurons besoin pour nos tests.

Réplication de la VM :

Il est important de garder à l'esprit que la réplication est une opération gourmande en bande passante, il est donc recommandé d'ajouter des liens entre les noeuds pour fluidifier le trafic.

La réplication se fait à partir de la machine virtuelle dans la catégorie **Réplication**, on ajoute une tâche de réplication (Figure 4.46) ; choisit le nœud cible, la fréquence

de synchronisation 3 et terminer la création (Figure 4.47). On réitére cette tâche pour le troisième nœud du cluster.

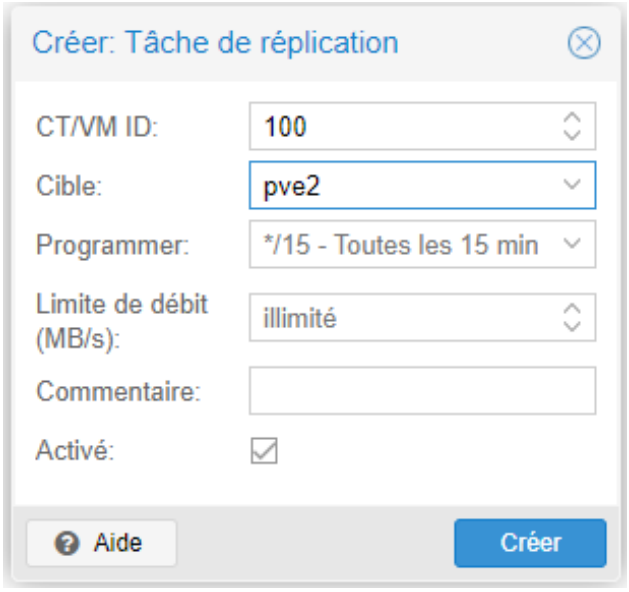


FIGURE 4.46 – Programmation de la réplication de la machine VMTest dans le noeud pve2.

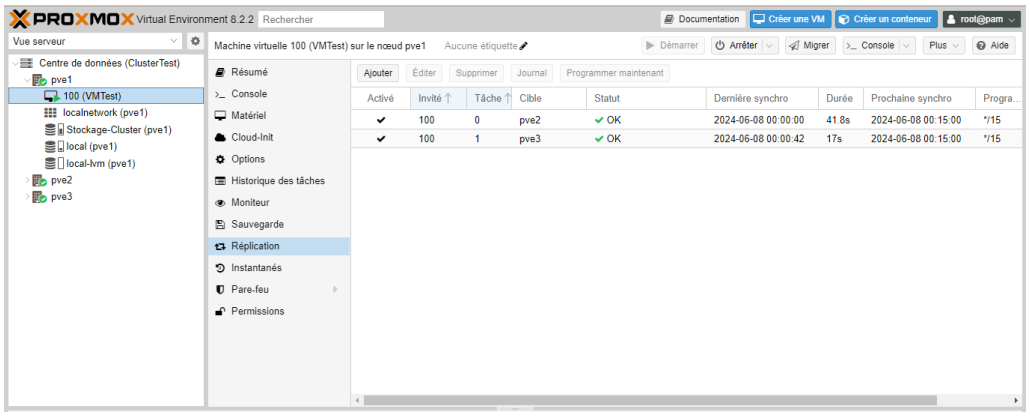


FIGURE 4.47 – Fin de la réplication.

Activation de la HA :

L'activation de la HA assure la continuité de service de la VM en cas de défaillance de son serveur en la migrant automatiquement vers l'un des autres noeuds du cluster et l'allumant. La HA dans Proxmox exige d'avoir au minimum trois noeuds dans un cluster pour être activée et pour que le quorum 3.2.3 fonctionne correctement. Les données de cette machine ne seront à jour qu'à la dernière réplication effectuée.

Dans le centre de données, on clique sur **HA**. Sous **Ressources**, on sélectionne **Ajouter** puis la VM concernée comme dans la figure 4.48.

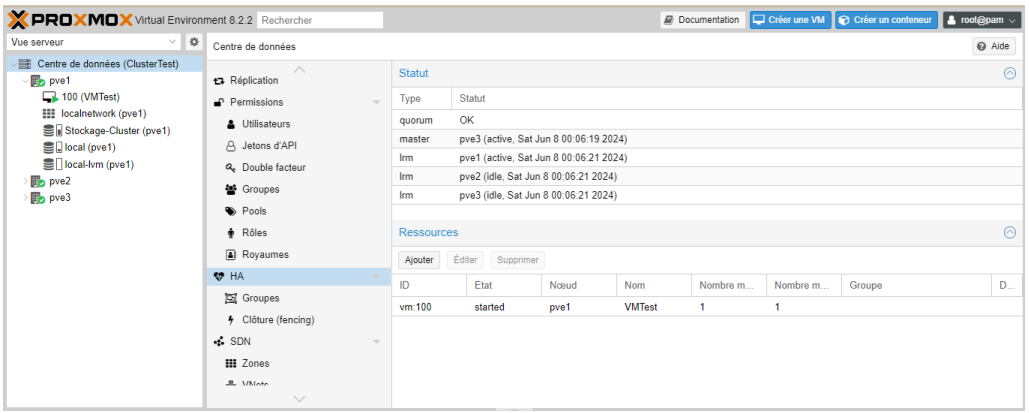


FIGURE 4.48 – Activation de la HA.

On constate qu'il est impossible de démarrer la machine virtuelle si tous les noeuds ne sont pas en marche après activation de la HA (Figure 4.49), celà est dû aux règles de quorum 3.2.3 qui permet la prise de décision correcte en cas de défaillance d'un nœud.

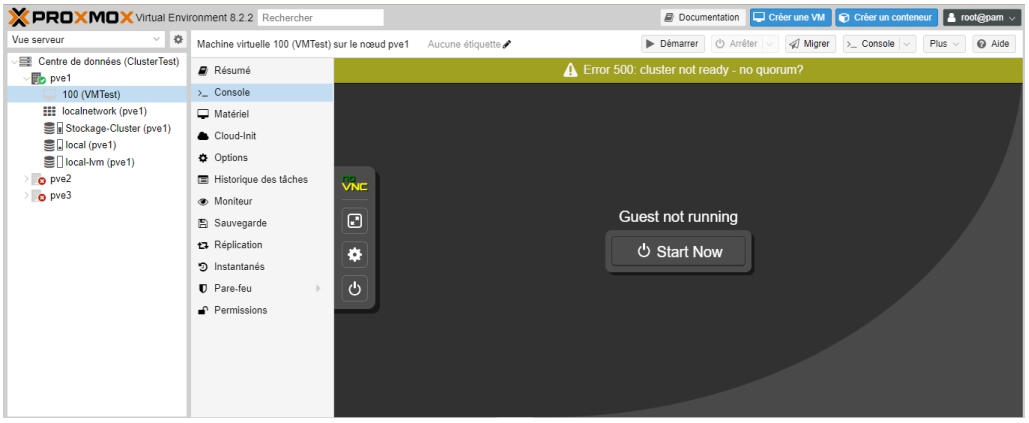


FIGURE 4.49 – Inactivité de la machine VMTest dû aux règles de quorum.

4.5.3 Configuration des serveurs Windows

Cette partie est consacrée à la configuration de deux serveurs Windows 2022 en cluster avec l'ajout des services Active Directory Domain Services (AD DS), DNS et DHCP. L'objectif est d'assurer des services critiques ininterrompus en centralisant la gestion des utilisateurs et des ressources, tout en fournissant des services de nommage et d'adressage IP redondants.

Configuration du serveur principal :

Pour débuter ces configurations, nous devons d'abord configurer un serveur principal. Il est important d'attribuer une adresse IP statique ainsi qu'un nom signi-

ficatif (Figure 4.51) en allant sur le gestionnaire des serveurs qui se trouve à l'acceuil (Figure 4.50).

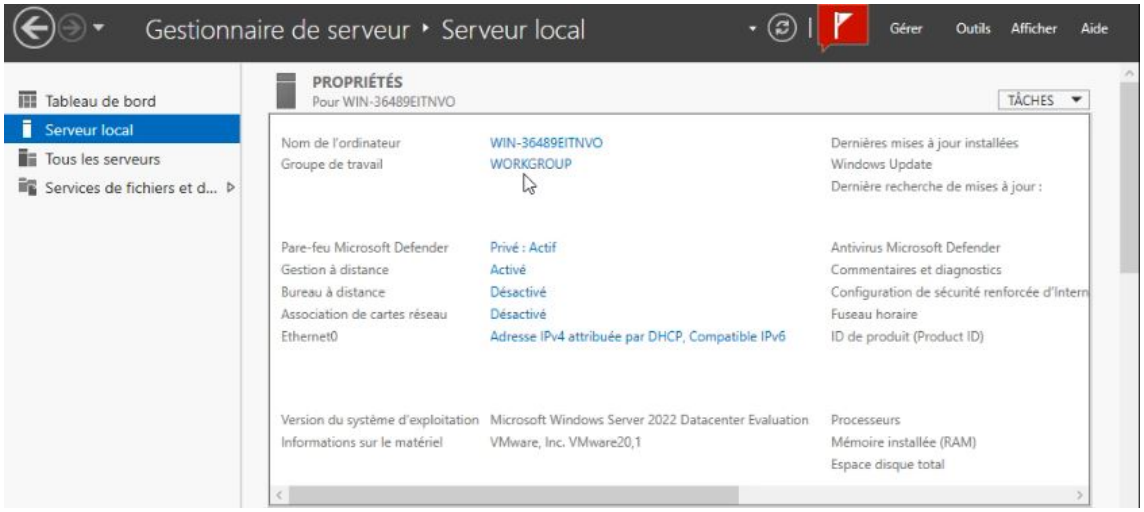


FIGURE 4.50 – Gestionnaire des serveurs.

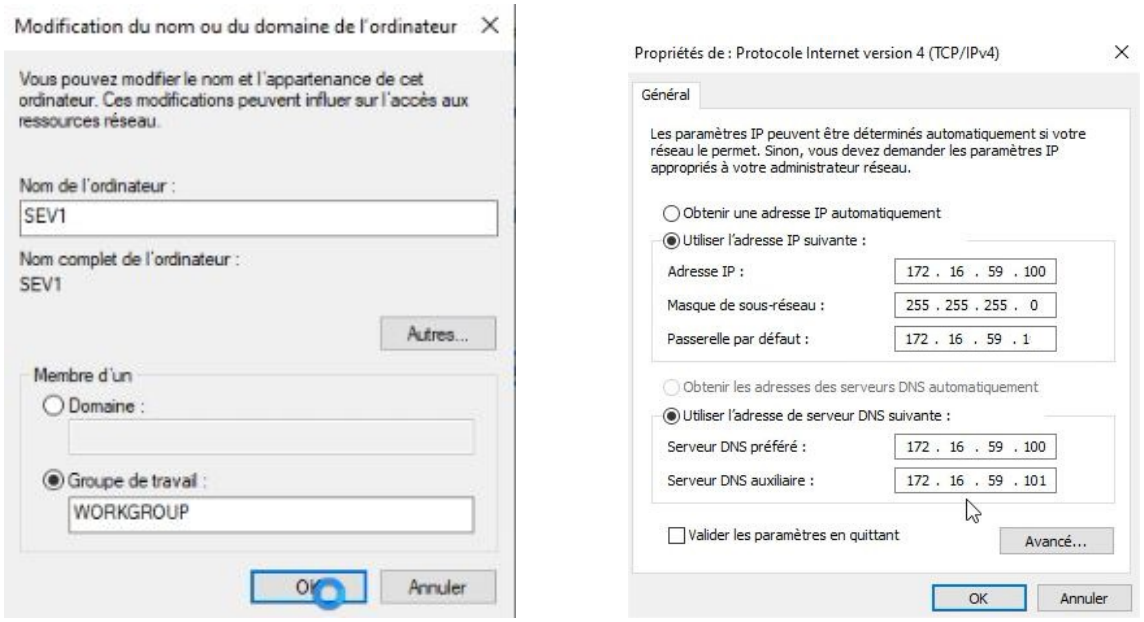


FIGURE 4.51 – Configuration du nom et de l'adressage IP du serveur principal.

Il est à remarquer que pour la partie adressage du serveur DNS (Figure 4.51), nous avons attribué l'adresse IP du serveur principal comme adresse DNS préférée et l'adresse IP du futur serveur secondaire comme adresse auxiliaire qui sera utile dans des cas de défaillance.

Pour ajouter les services AD DS, DNS et DHCP (Figure 4.53), il suffit de cliquer sur **Ajouter des rôles et des fonctionnalités** en accédant au tableau de bord du serveur Windows (Figure 4.52).

FIGURE 4.52 – Tableau de bord du serveur Windows.

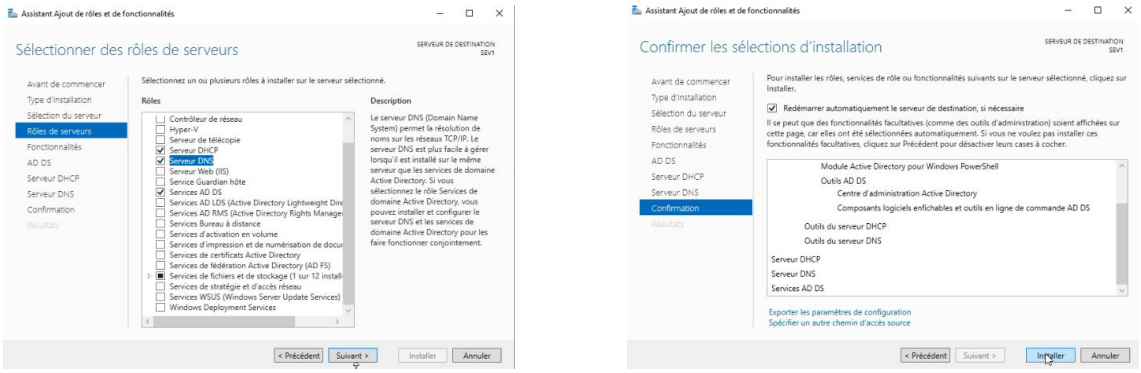
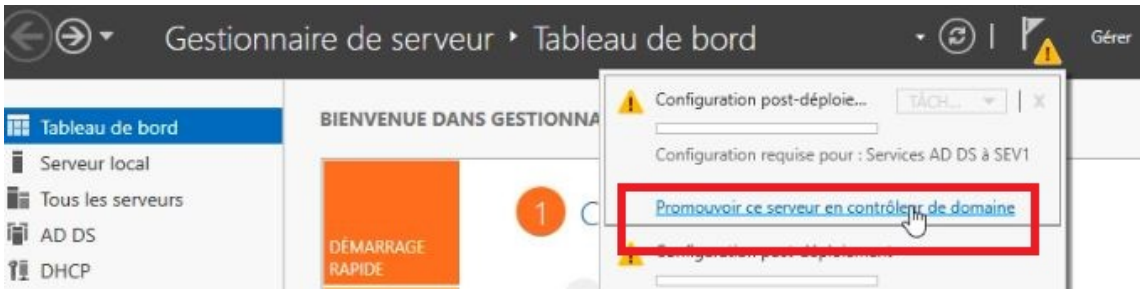
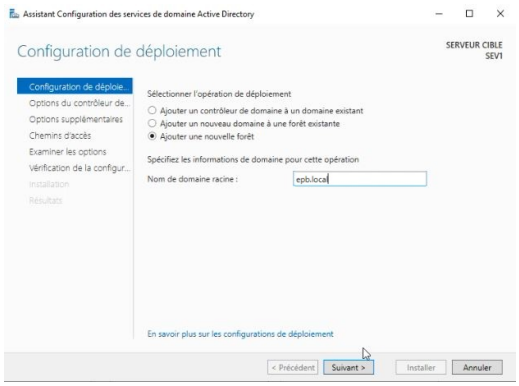


FIGURE 4.53 – Ajout des services.

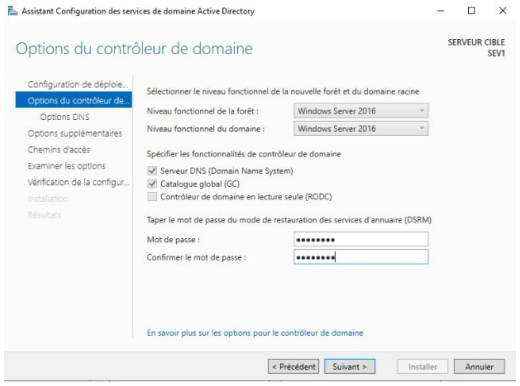
Par la suite, il faudrait promouvoir le serveur en tant que contrôleur de domaine (DC) (Figure 4.54a). Dans l'Assistant de Configuration de l'AD DS (Figure 4.54b), nous ajoutons une nouvelle forêt en lui attribuant le nom de domaine racine **epb.local**. Il est possible de sélectionner des options pour ce contrôleur de domaine (Figure 4.54c), nous cochons "Serveur DNS" afin qu'il soit également serveur DNS. Il est impératif d'ajouter, en plus de cela, un mot de passe pour le mode de restauration des services d'annuaire (DSRM) qui est essentiel pour les opérations de maintenance et de récupération. Le reste des options seront gardées par défaut.



(a) Promouvoir le serveur en contrôleur de domaine.



(b) Ajout du contrôleur de domaine à une nouvelle forêt.



(c) Options du contrôleur de domaine.

FIGURE 4.54 – Promotion du serveur principal en contrôleur de domaine.

Configuration du serveur secondaire :

Tout comme pour le serveur principal, nous allons changer le nom du serveur secondaire tout en lui attribuant le nom de domaine que nous avons créer auparavant **epb.local**, nous lui attribuerons également des adresses IP appartenant au même réseau que le premier serveur (Figure 4.55).

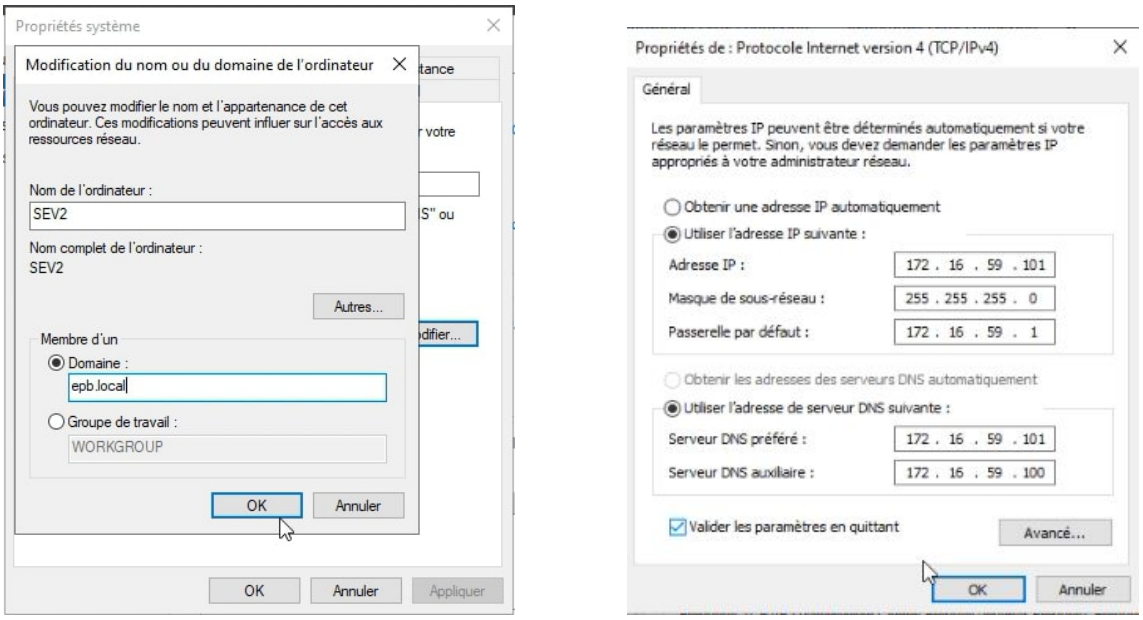


FIGURE 4.55 – Configuration du nom et de l'adressage IP du serveur secondaire.

Nous allons répéter les mêmes étapes (Figures 4.53 et 4.54) pour ajouter les rôles AD DS, DNS et DHCP, tout en promouvant ce deuxième serveur en tant que contrôleur de domaine. Cela assure la redondance des services d'annuaire, pérennise la base d'annuaire par réplication entre les DC, et répartit les requêtes pour un meilleur équilibrage de la charge. Il suffit d'ajouter cette fois ce DC dans un domaine existant (Figure 4.54b) et de rajouter une option supplémentaire pour choisir une réplication depuis le serveur principal (Figure 4.56).

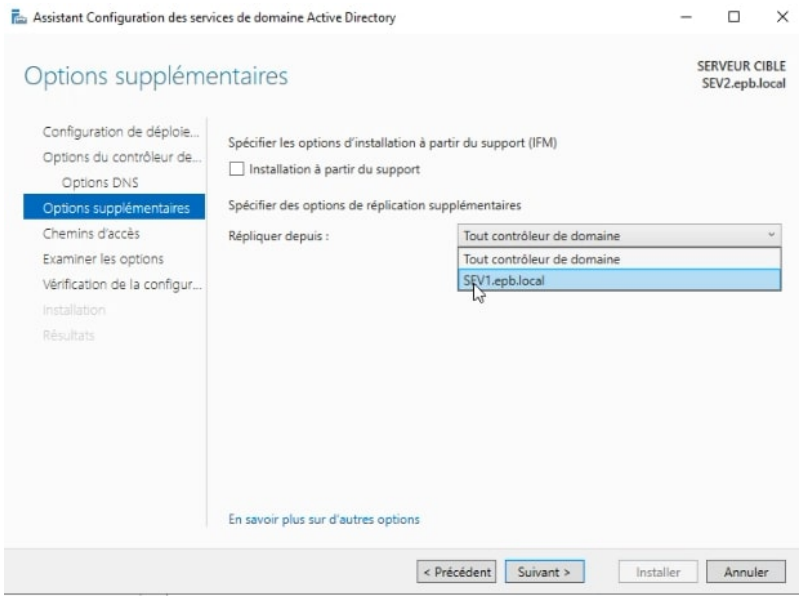


FIGURE 4.56 – Option supplémentaire du second DC.

Configuration des structures Active Directory :

Le rôle AD DS permet de structurer notre domaine en créant des unité d'organisation, des utilisateurs, des groupes, des équipements terminaux et d'autres encore. Nous allons procéder à la création et à la configuration de ces éléments pour optimiser la gestion et l'administration de notre infrastructure réseau, et ce, en passant par **outils -> utilisateurs et ordinateurs Active Directory**.

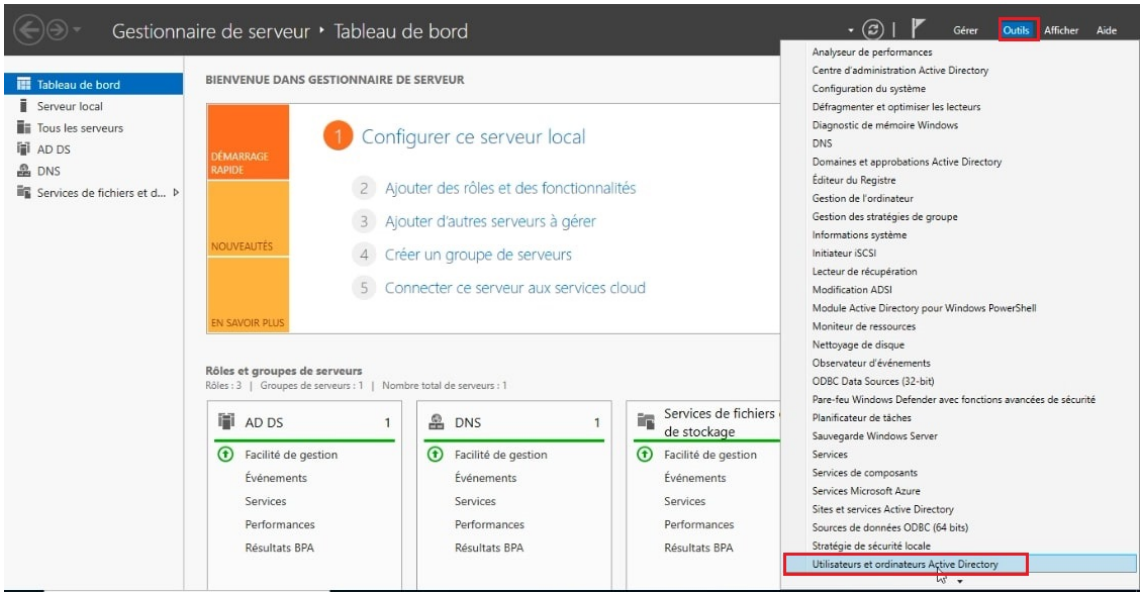


FIGURE 4.57 – Accès à la configuration des éléments mentionnés.

- **Création d'une unité d'organisation :** Sur l'interface obtenue, on retrouve notre domaine. Pour ajouter une nouvelle unité d'organisation, les étapes indiquées dans la figure 4.58 seront suivies.

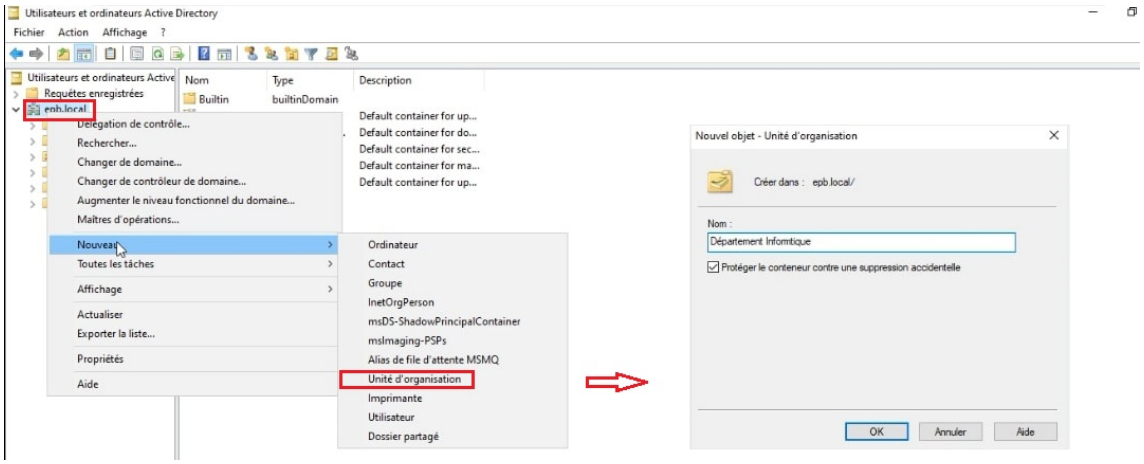


FIGURE 4.58 – Création d'une unité d'organisation.

- **Création des groupes et utilisateurs :** Au sein de l'unité d'organisation, il

est possible d'ajouter des groupes d'utilisateur telle que le montre la figure 4.59 :

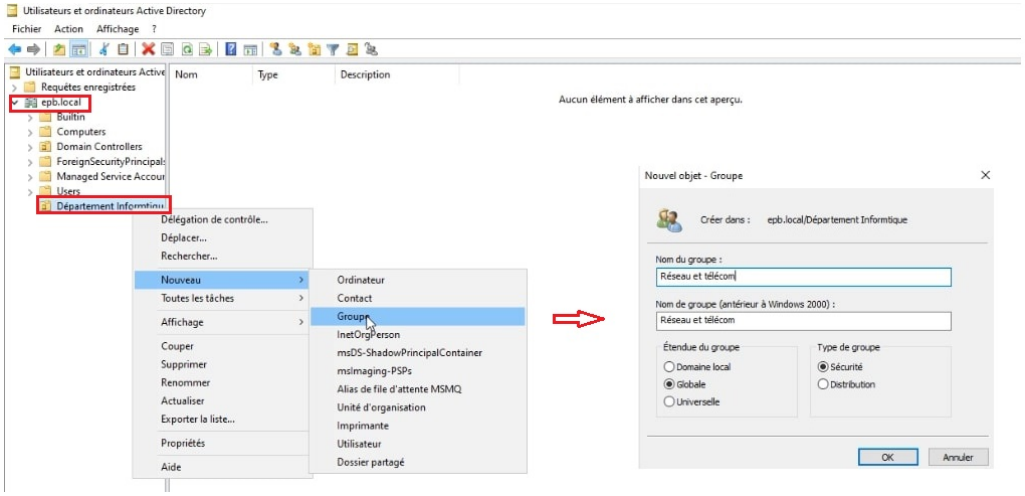


FIGURE 4.59 – Création d'un groupe.

De la même manière, nous allons ajouter deux utilisateurs :

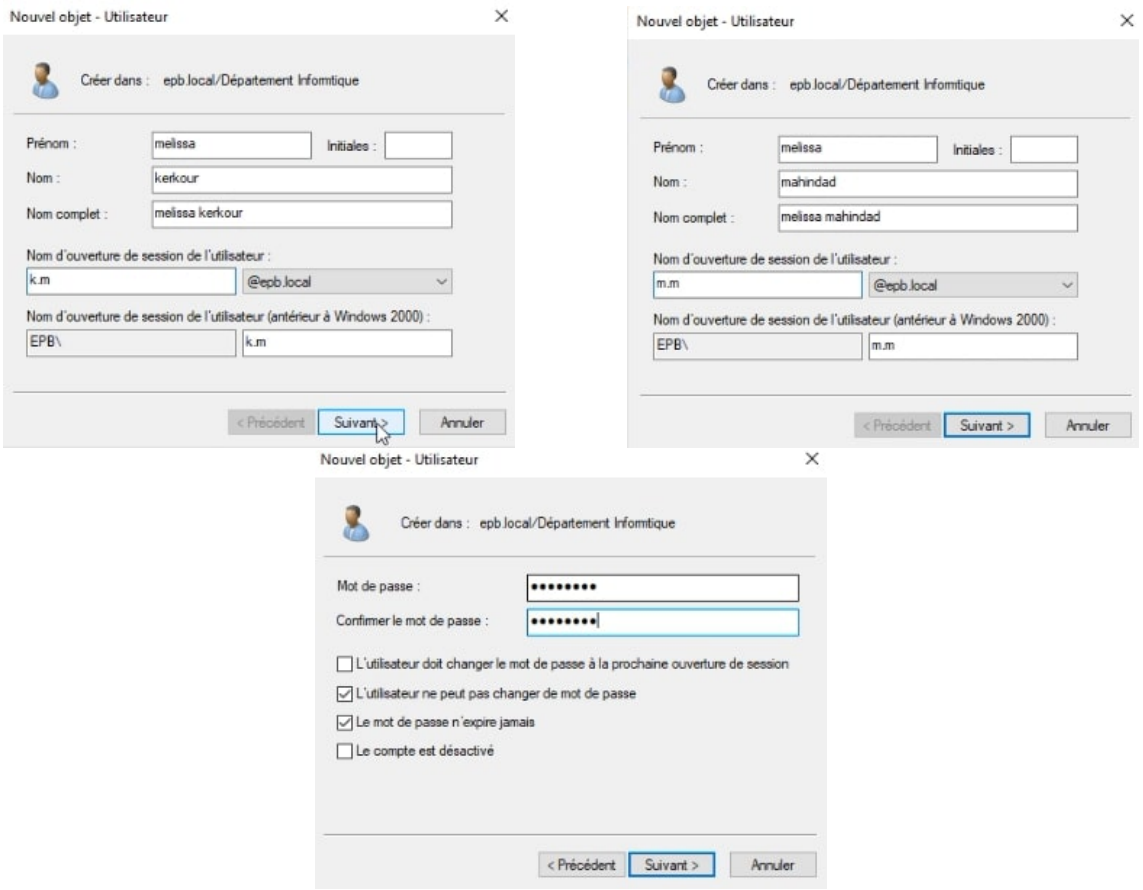


FIGURE 4.60 – Création des utilisateurs.

- **Ajout des utilisateurs à un groupe :** Pour joindre les utilisateurs au groupe

créé auparavant, il faut accéder aux propriétés du groupe, et sélectionner les deux utilisateurs et les ajouter sur l'onglet "Membre".

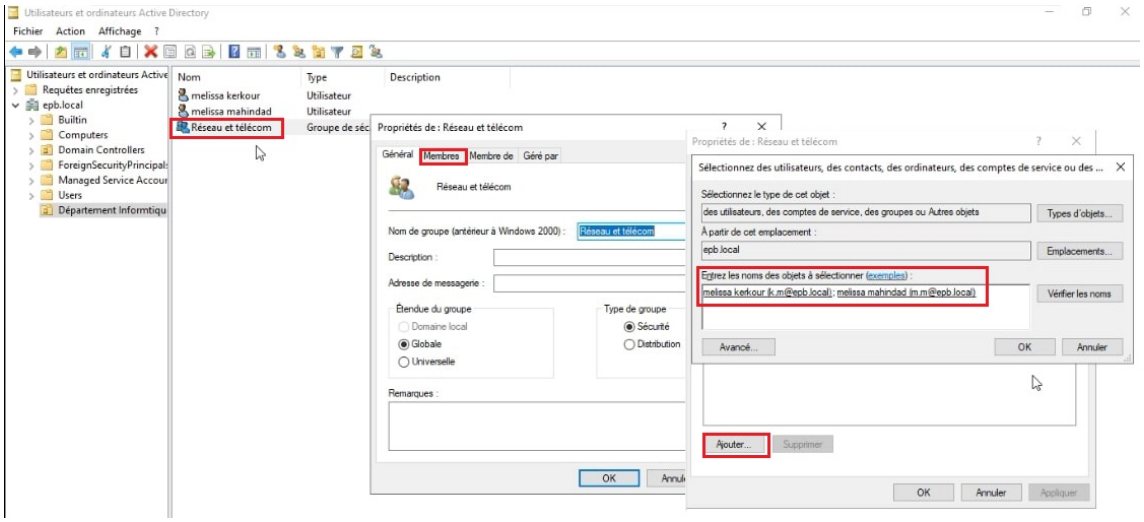


FIGURE 4.61 – Ajout des utilisateurs au groupe.

On applique les changements pour que les utilsateurs deviennent membres du groupe.

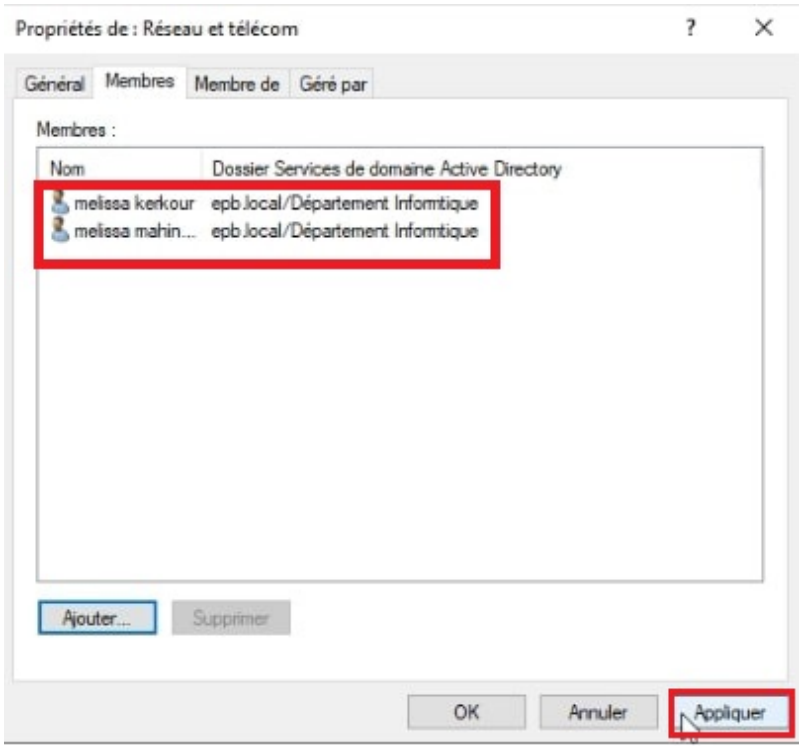
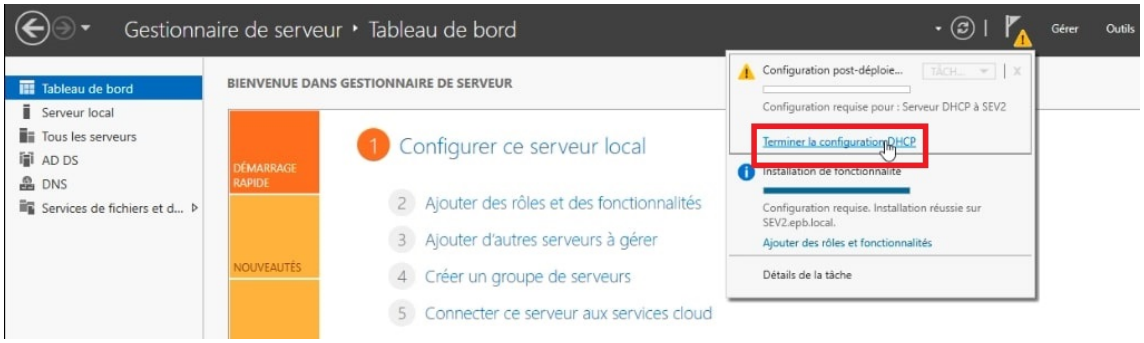


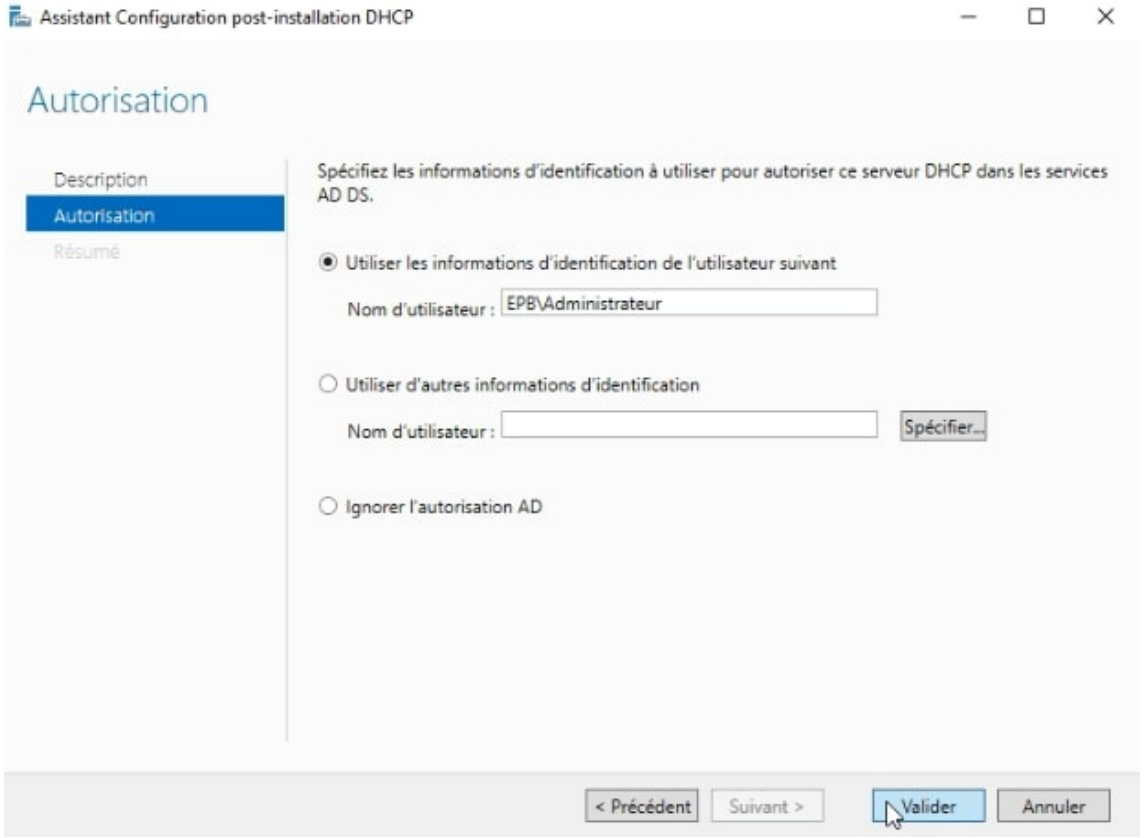
FIGURE 4.62 – Application des changements.

Configuration du DHCP :

Pour utiliser efficacement notre rôle DHCP, il est essentiel de l'intégrer au service AD DS déjà configuré :



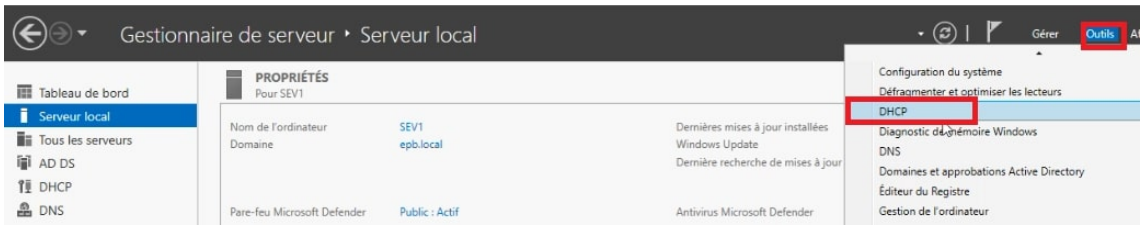
(a) Continuation de la configuration du DHCP.



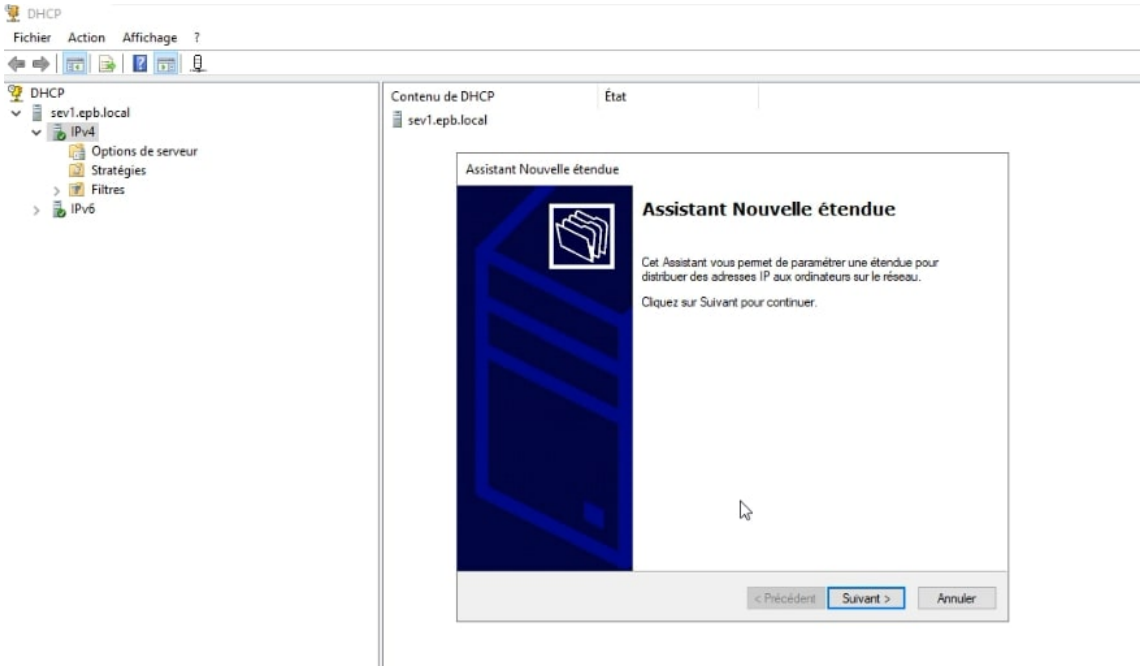
(b) Autorisation de lu serveur DHCP au niveau de AD DS.

FIGURE 4.63 – Finalisation de configuration du DHCP.

- **Création d'une étendue DHCP :** Pour déclarer une plage d'adresses IP que le service DHCP pourra distribuer, il faut accéder à l'espace **outils -> DHCP** d'un de nos deux serveurs synchronisés et configurer une nouvelle étendue comme le montrent les figures 4.64a et 4.64b :



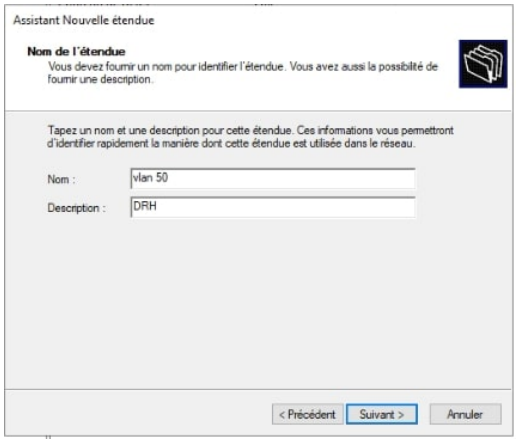
(a) Accès à l'espace outils.



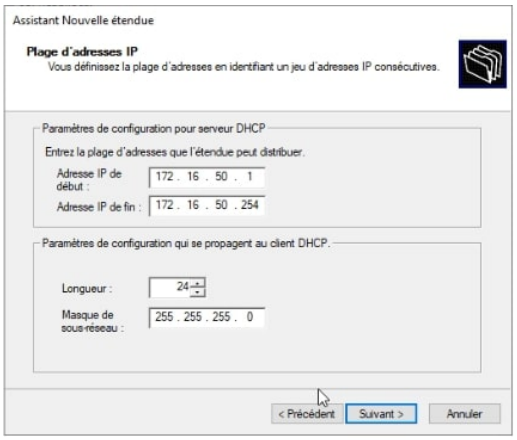
(b) Assistance de création de l'étendue.

FIGURE 4.64 – Création d'une nouvelle étendue.

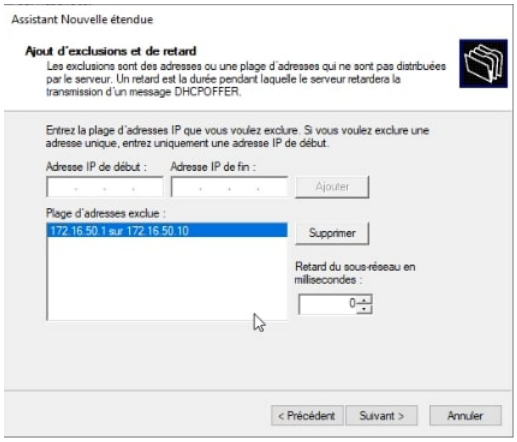
Une nouvelle étendue sera créée pour chacun des VLAN configurés, en leur attribuant des noms, des plages d'adressage, une durée de bail pendant laquelle les utilisateurs pourront utiliser leurs adresses, en spécifiant également les adresses à exclure, et en configurant l'adresse de la passerelle par défaut. Pour ce faire, nous allons procéder suivant les étapes de la figure 4.65 :



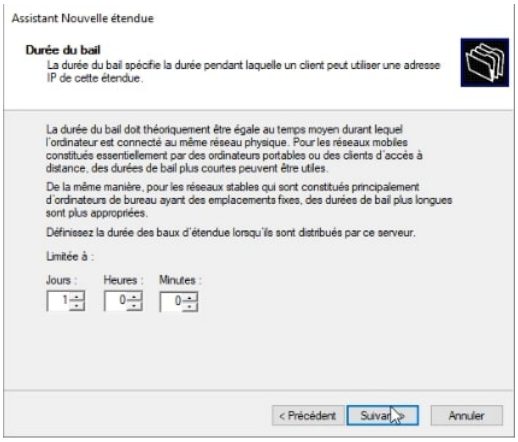
(a) Nom de la nouvelle étendue.



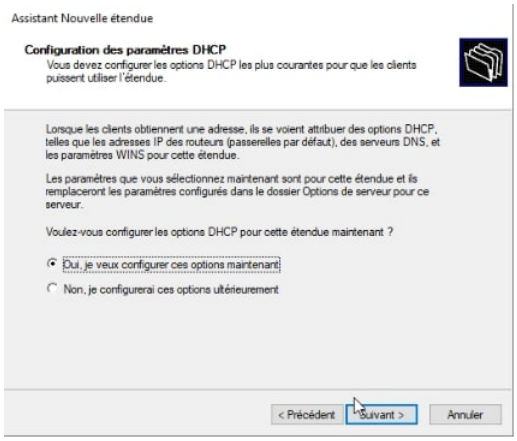
(b) Plage d'adressage de la nouvelle étendue.



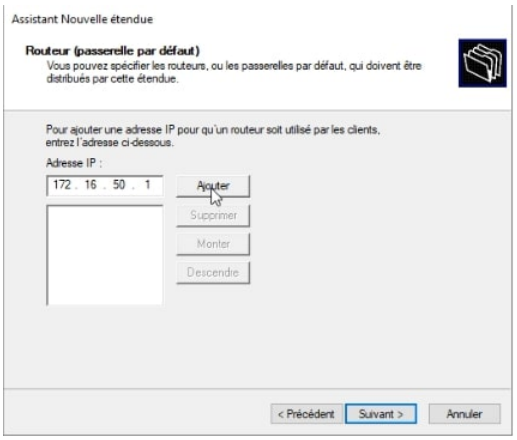
(c) Intervalle d'adresse IP à exclure.



(d) Durée du bail des adresses.



(e) Confirmation de la configuration des options DHCP.

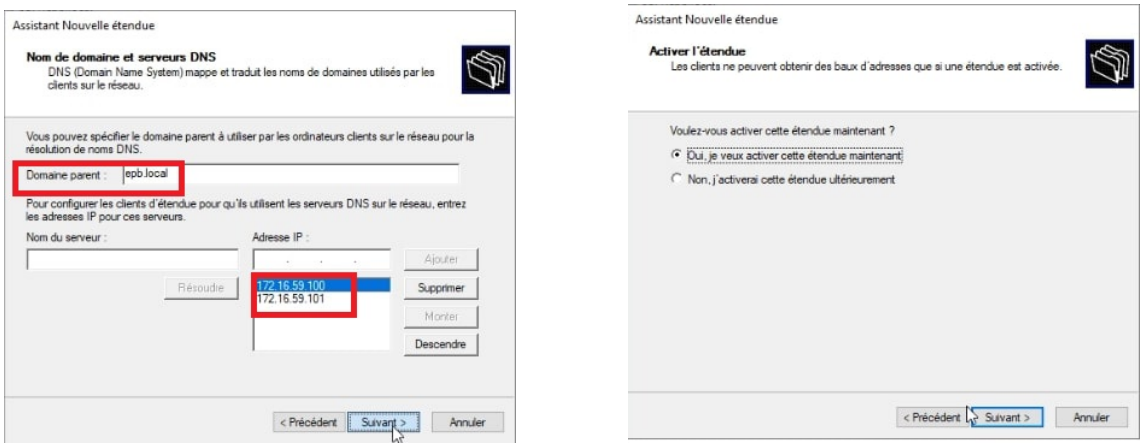


(f) Adresse de la passerelle par défaut.

FIGURE 4.65 – Configuration d'une étendue DHCP pour un VLAN

En arrivant à la dernière étape avant d'activer la configuration de cette nouvelle étendue, nous retrouvons l'option de configuration du nom de domaine et des serveurs DNS, en spécifiant les adresses de nos deux serveurs, que le DHCP at-

tribuera :



(a) Option du DNS. (b) Activation de l'étendue.

FIGURE 4.66 – Finalisation de l'étendue.

Ainsi, notre étendue "VLAN 50" est désormais visible dans la console DHCP et est active. À partir de ce moment-là, les postes clients de ce VLAN peuvent obtenir une adresse IP à partir de notre serveur.

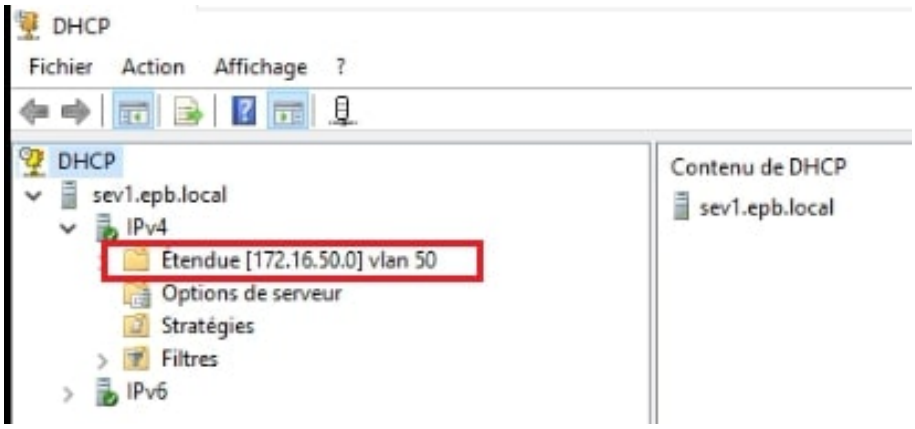
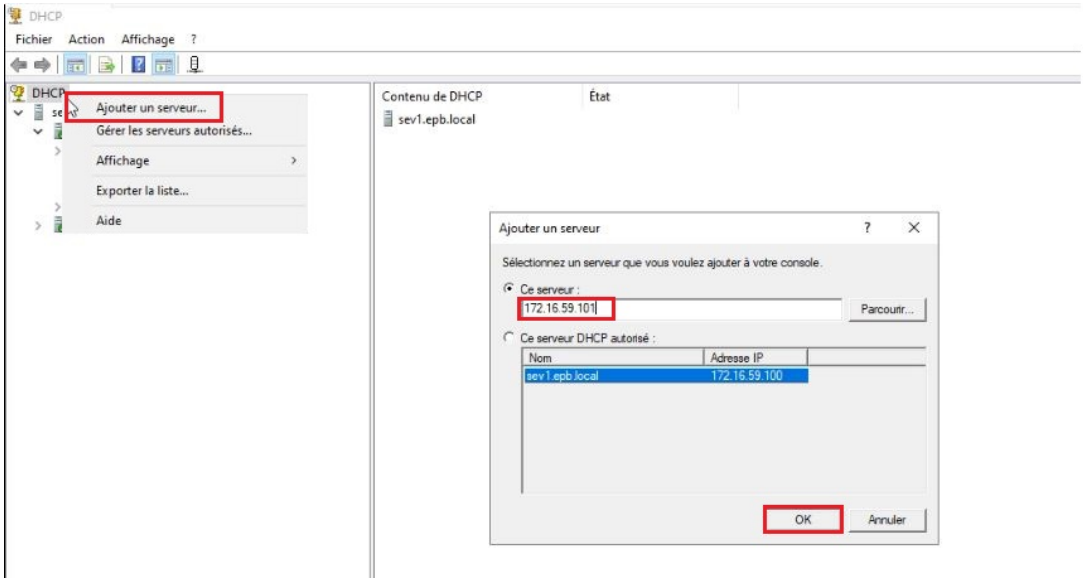
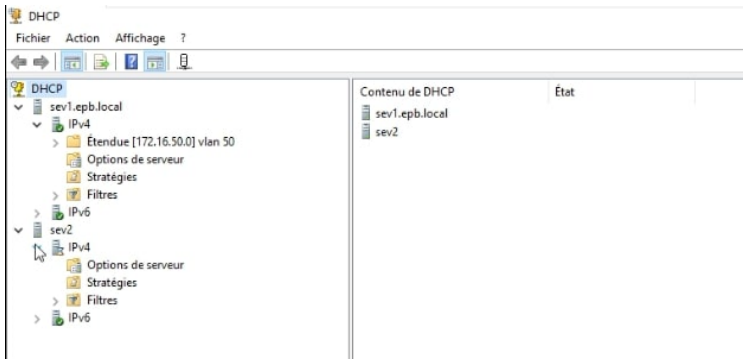


FIGURE 4.67 – Affichage de l'étendue.

- **Configuration du basculement :** Pour garantir une haute disponibilité du service DHCP, le second serveur sera intégré à la console DHCP du premier serveur afin d'avoir un serveur de secours en cas de panne. Cela est considéré comme un cluster du service DHCP.



(a) Ajout du deuxième serveur.



(b) Résultat de l'ajout.

FIGURE 4.68 – Cluster des deux serveur.

À présent, il est possible de mettre en place un basculement, en prenant comme exemple l'étendue du VLAN 50, et commencer les étapes de configuration pour cette procédure.

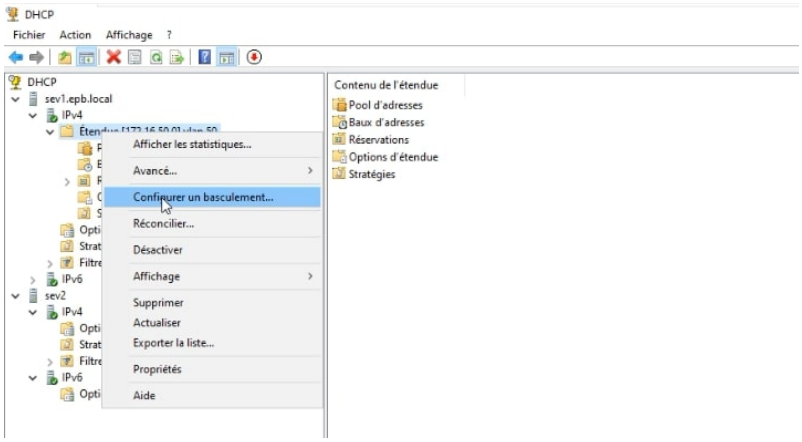
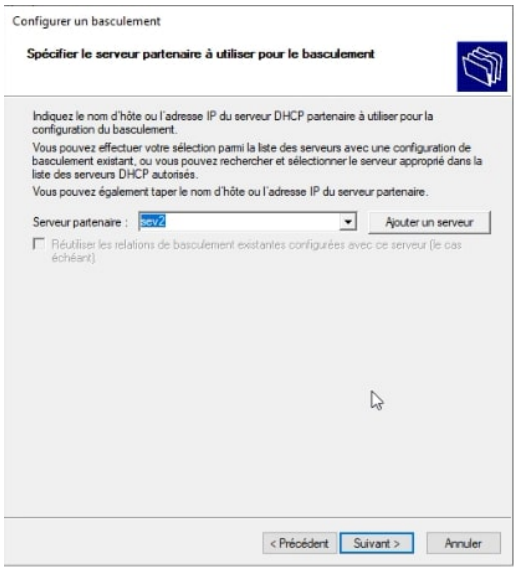
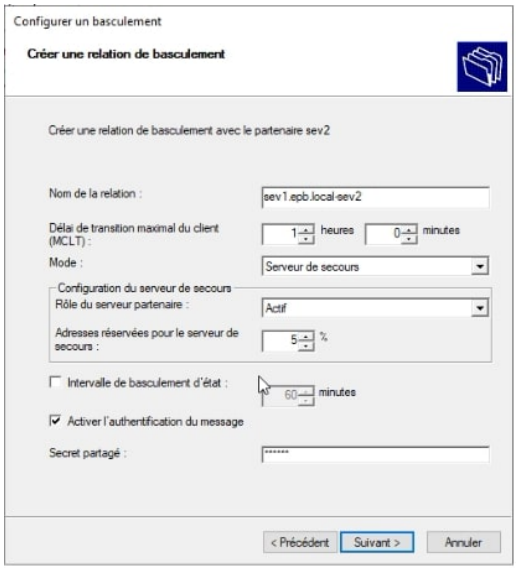


FIGURE 4.69 – Sélection de l'étendue à faire basculer.

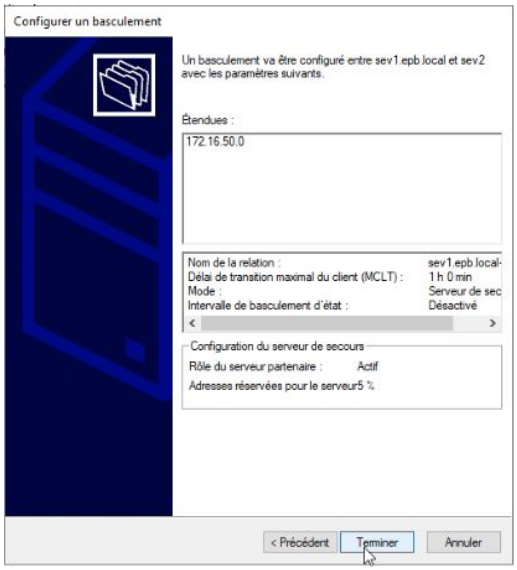
(a) Introduction au basculement.



(b) Spécification du serveur partenaire.



(c) Configuration du Mode Serveur de Secours et Activation du Rôle Partenaire.



(d) Fin de la configuration.

FIGURE 4.70 – Étapes de configuration du basculement.

La configuration est maintenant terminée. La même configuration sera reproduite sur le deuxième serveur (Le serveur secondaire), en désignant cette fois le serveur 1 (sev1- serveur principal) comme serveur partenaire.

4.5.4 Configuration de pfSense

Cette partie concerne toutes les configuations faites au niveau de nos pare-feux, concernant les interfaces, les règles de filtrage du trafic, ainsi que l'application d'un cluster pour les deux pare-feux du site principal de l'EPB.

Configuration des interfaces :

Pour configurer les liens des différents pare-feux, des interfaces ont été créées au niveau de ces derniers, incluant les adresses IP et leurs passerelles. Ces interfaces sont présentées comme suit sur les tableaux de bords de chacun d'eux :

Interfaces			
WAN	↑	1000baseT <full-duplex>	2.2.2.5
LAN	↑	1000baseT <full-duplex>	172.19.0.2
VLAN	↑	1000baseT <full-duplex>	n/a
VLAN50	↑	1000baseT <full-duplex>	172.16.50.1
VLAN51	↑	1000baseT <full-duplex>	172.16.51.1
VLAN52	↑	1000baseT <full-duplex>	172.16.52.1
VLAN53	↑	1000baseT <full-duplex>	172.16.53.1
VLAN54	↑	1000baseT <full-duplex>	172.16.54.1
VLAN55	↑	1000baseT <full-duplex>	172.16.55.1
VLAN56	↑	1000baseT <full-duplex>	172.16.56.1
VLAN57	↑	1000baseT <full-duplex>	172.16.57.1
VLAN58	↑	1000baseT <full-duplex>	172.16.58.1
VLAN59	↑	1000baseT <full-duplex>	172.16.59.1
VLAN60	↑	1000baseT <full-duplex>	172.16.60.1
DMZ	↑	1000baseT <full-duplex>	172.16.40.1

(a) Interfaces du pare-feu pf1.

Interfaces			
WAN	↑	1000baseT <full-duplex>	2.2.2.1
LAN	↑	1000baseT <full-duplex>	172.19.0.3
VLAN	↑	1000baseT <full-duplex>	n/a
VLAN50	↑	1000baseT <full-duplex>	172.16.50.2
VLAN51	↑	1000baseT <full-duplex>	172.16.51.2
VLAN52	↑	1000baseT <full-duplex>	172.16.52.2
VLAN53	↑	1000baseT <full-duplex>	172.16.53.2
VLAN54	↑	1000baseT <full-duplex>	172.16.54.2
VLAN55	↑	1000baseT <full-duplex>	172.16.55.2
VLAN56	↑	1000baseT <full-duplex>	172.16.56.2
VLAN57	↑	1000baseT <full-duplex>	172.16.57.2
VLAN58	↑	1000baseT <full-duplex>	172.16.58.2
VLAN59	↑	1000baseT <full-duplex>	172.16.59.2
VLAN60	↑	1000baseT <full-duplex>	172.16.60.2
DMZ	↑	1000baseT <full-duplex>	172.16.40.2

(b) Interfaces du pare-feu pf2.

Interfaces			
WAN	↑	1000baseT <full-duplex>	3.3.3.2
LAN	↑	1000baseT <full-duplex>	172.19.0.4
LOCAL	↑	1000baseT <full-duplex>	172.16.100.1

(c) Interfaces du pare-feu TEXTER.

Création des règles de pare-feu :

Dans la conception et la configuration efficace des pare-feux, il est primordial de définir des règles spécifiques pour les principaux protocoles réseaux : ICMP, TCP et UDP (voir annexe C pour comprendre leurs rôles) et ce, au niveau de chaque interface (WAN, LAN, DMZ, VLAN). Ces règles seront appliquées pour le trafic entrain et sortant pour une sécurité optimale du réseau.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐ ✓	0 /0 B	IPv4 TCP	*	*	*	*	*	none			
☐ ✓	0 /0 B	IPv4 UDP	VLAN50 net	*	VLAN50 address	67 - 68	*	none			
☐ ✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			

FIGURE 4.72 – Règles de pare-feu.

Configuration du CARP et pfsync :

Les protocoles CARP et pfsync (Packet Filter Synchronization) sont utilisés afin de mettre en place une configuration de haute disponibilité dans un environnement réseau. CARP permet de partager une adresse IP virtuelle (VIP) entre deux pare-feux pfSense sur un même réseau. Ainsi, en cas de défaillance du pare-feu principal, la VIP bascule automatiquement vers le pare-feu secondaire.
Le pfsync, quant à lui, synchronise l'état des connexions en cours entre les deux pare-feu pfSense. De cette manière, lorsque le pare-feu secondaire prend le relais, il conservera l'état des connexions établies. Ces protocoles évitent alors toute interruption, assurant une continuité de service transparente pour les utilisateurs connectés.

Pour commencer ces configurations, il est primordial de créer d'abord un utilisateur pfsync au niveau du pf2 en tant que pare-feu secondaire, et le pare-feu principal pf1 prendra en charge l'activation de la HA et de la synchronisation, ainsi toutes les configurations qui suivent ne seront pas répétées au niveau de chaque pare-feu. Cet utilisateur sera ajouté au menu **System -> User manager**.

FIGURE 4.73 – Création de l'utilisateur pfsync.

Il faudrait également lui ajouté le privilège de synchronisation de la haute disponibilité.

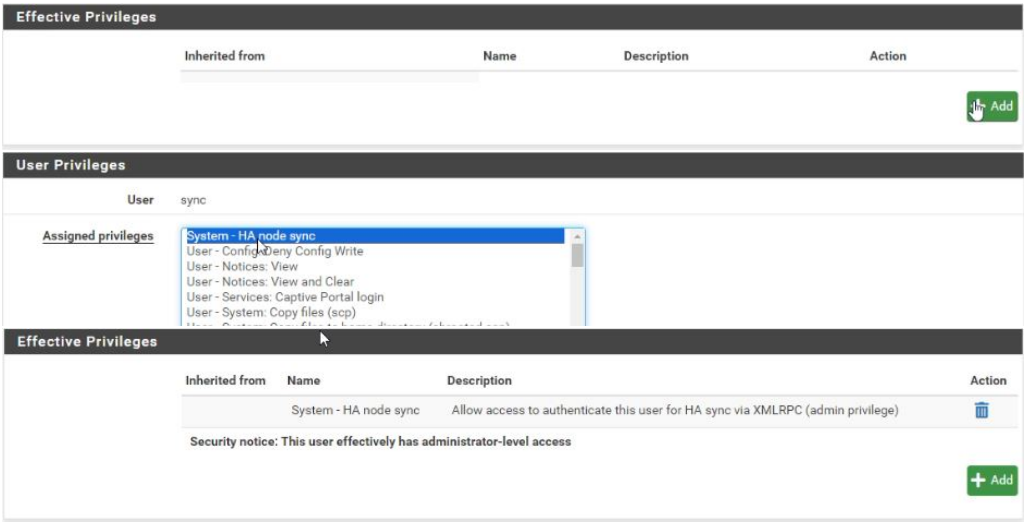


FIGURE 4.74 – Ajout du privilège HA.

La configuration se poursuit avec l'ajout d'une interface pfsync au niveau des deux pare-feux pf1 et pf2 tout en leur créant une règle autorisant tous les protocoles de IPV4.

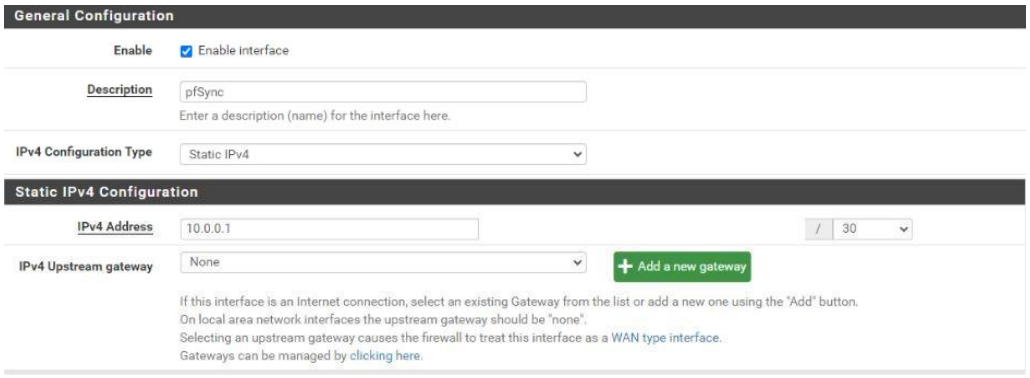


FIGURE 4.75 – Création de l'interface pfsync sur pf1.

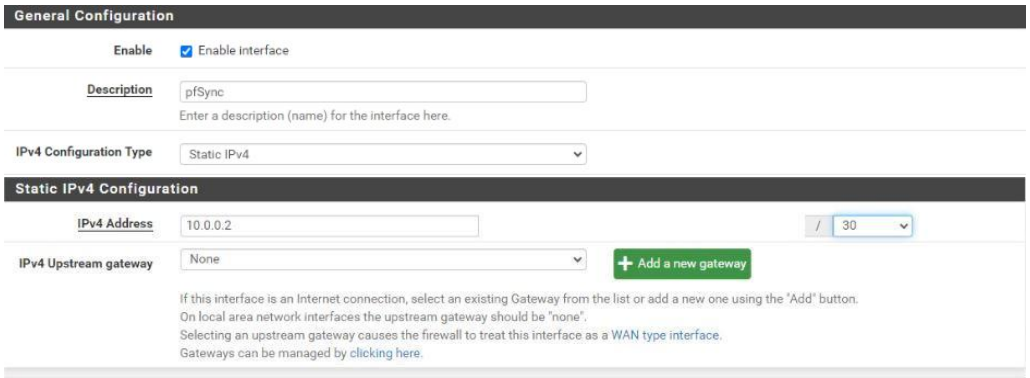


FIGURE 4.76 – Création de l'interface pfsync sur pf2.

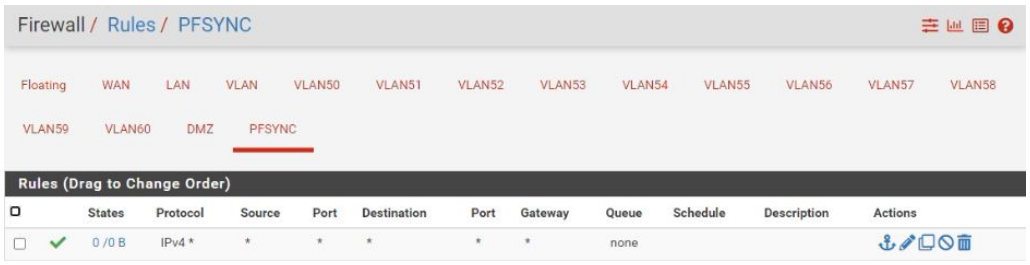


FIGURE 4.77 – Création de la règle.

En revenant au pare-feu principal, sur le menu **System -> High Avail.Sync** il faudrait cocher la synchroniation des états de connexion avec l'interface pfsync du pare-feu secondaire dont l'adresse IP est **10.0.0.2**, tout en insérant les informations d'authentification de l'utilisateur "sync".

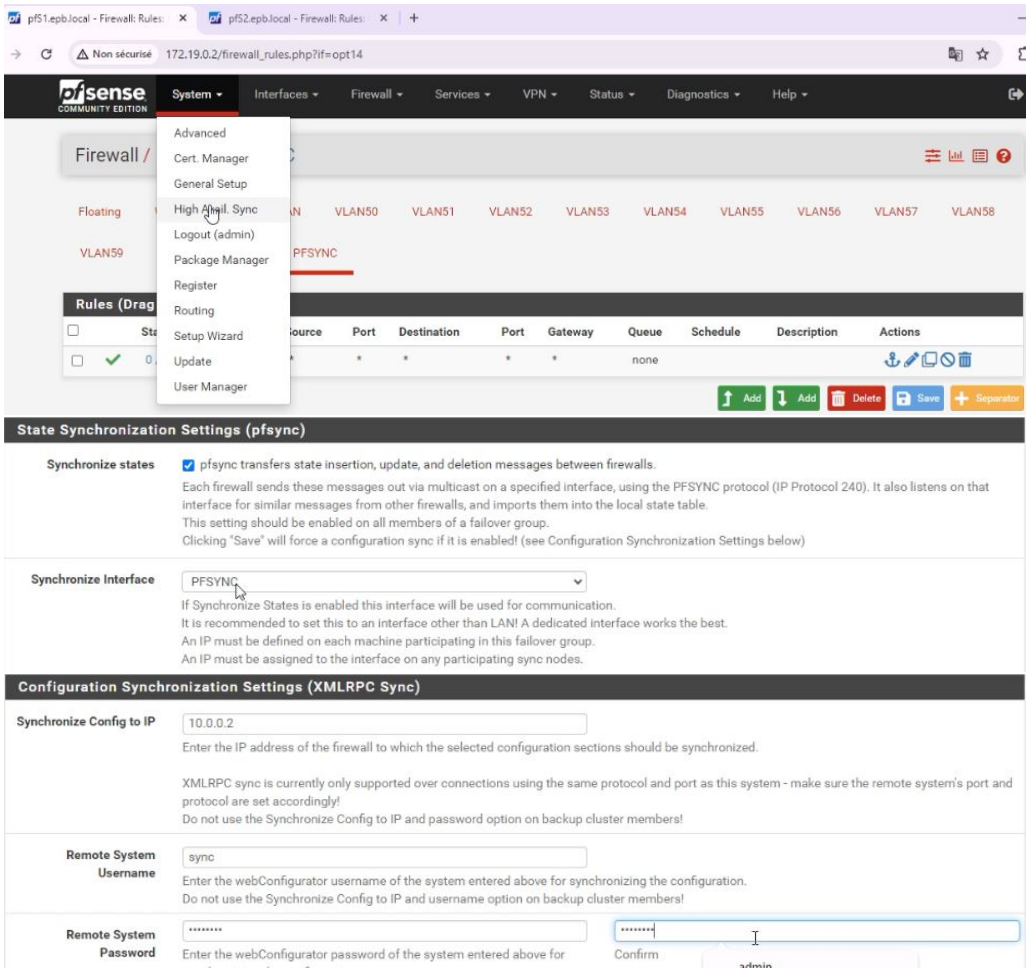


FIGURE 4.78 – Activation de la synchronisation.

Une liste d'options de synchronisation est affichée, il est possible de sélectionner l'ensemble des options disponibles pour garantir une synchronisation optimale.

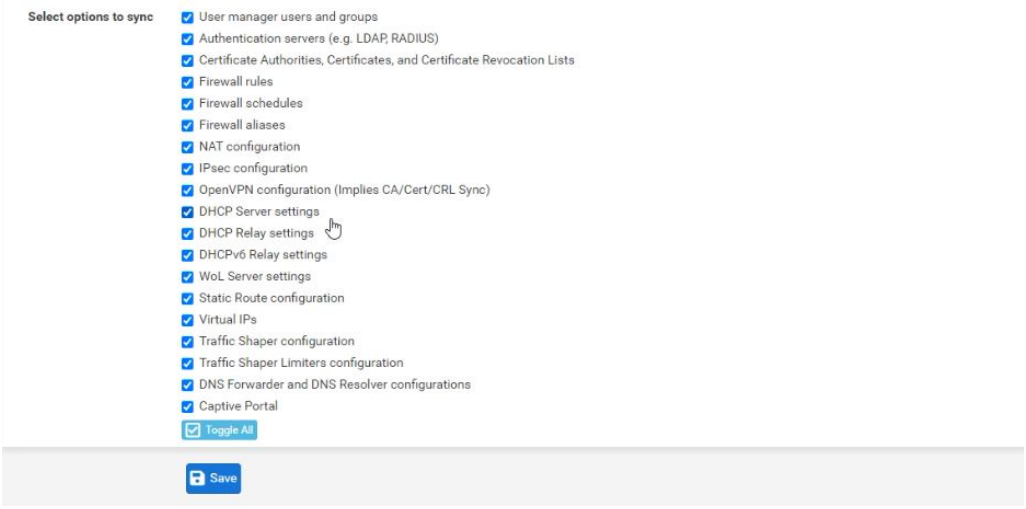


FIGURE 4.79 – Sélection des options de synchronisation.

En terminant avec cette partie, il faudrait créer des VIP de type CARP pour chaque VLAN en accédant au menu **Firewall-> Virtual IPs** d'un des deux pare-feux.

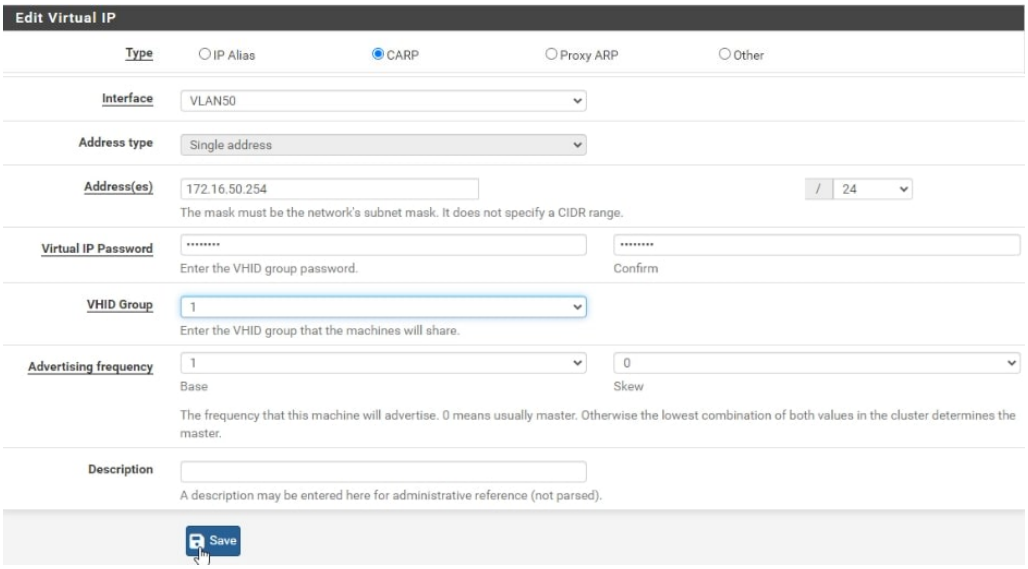


FIGURE 4.80 – Création d'une VIP.

L'ensemble des VIP configurées sont représentés dans la figure 4.81.

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
172.16.50.254/24 (vhid: 1)	VLAN50	CARP		
172.16.51.254/24 (vhid: 2)	VLAN51	CARP		
172.16.52.254/24 (vhid: 3)	VLAN52	CARP		
172.16.53.254/32 (vhid: 4)	VLAN53	CARP		
172.16.54.254/24 (vhid: 5)	VLAN54	CARP		
172.16.55.254/24 (vhid: 6)	VLAN55	CARP		
172.16.56.254/24 (vhid: 7)	VLAN56	CARP		
172.16.57.254/24 (vhid: 8)	VLAN57	CARP		
172.16.58.254/32 (vhid: 9)	VLAN58	CARP		
172.16.59.254/24 (vhid: 10)	VLAN59	CARP		
172.16.60.254/24 (vhid: 11)	VLAN60	CARP		

FIGURE 4.81 – Affichage des VIP.

Configuration du VPN :

1. **VPN site-à-site :** Pour entamer la configuration d'un VPN site-à-site, il faudrait accéder au menu **VPN** et sélectionner **IPsec** sur l'un des deux pare-feux du site principal pour effectuer les configurations nécessaires (Annexe E.1) afin de créer un tunnel IPsec (Internet Protocol Security) vers le site distant TEXTER.

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
Disable	1	V2	WAN 3.3.3.2		AES (256 bits)	SHA256	2 (1024 bit)	Connexion VPN	

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
Disable	1	tunnel	VLAN60	172.16.100.0/24	ESP	AES (256 bits), AES128-GCM (128 bits)	SHA256	Connexion VPN IPSEC	

Add P2

FIGURE 4.82 – Configuration du VPN du site principal vers le site TEXTER.

De la même façon, nous allons mettre en place un tunnel IPsec entre le site TEXTER et le site principal.

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
Disable	1	V2	WAN 2.2.2.1		AES (256 bits)	SHA256	14 (2048 bit)	Connexion VPN IPSEC 1	
Show Phase 2 Entries (1)									
Disable	2	V2	WAN 2.2.2.5		AES (256 bits)	SHA256	2 (1024 bit)	Connexion VPN IPSEC 2	
Show Phase 2 Entries (1)									

FIGURE 4.83 – Configuration du VPN du site TEXTER vers le site principal.

2. **VPN poste-à-site :** Pour la configuration d'un VPN poste-à-site, il faudrait accéder au menu **VPN** et sélectionner **Open VPN** au niveau du pare-feu

choisi tout en intégrant une intégrant une autorité de certification interne et un certificat dédié au serveur pour la sécurisation de notre tunnel VPN. (Annexe E.2). Un résumé des configurations faites à ce niveau est représenté dans la figure 4.84.

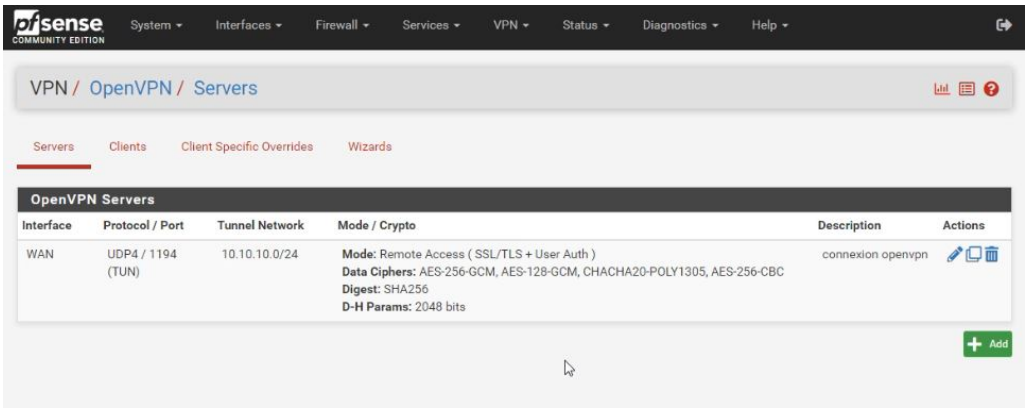


FIGURE 4.84 – Configuration du VPN du site TEXTER vers un poste externe.

Par la suite, un utilisateur VPN doit être créé sur le menu **User Manager**, en lui attribuant un nom ainsi qu'un mot de passe pour se connecter au VPN.

FIGURE 4.85 – Ajout de l'utilisateur VPN.

Pour l'authentification VPN, il faudrait créer à cet utilisateur un certificat interne de type "user" en lui attribuant une description significative et en sélectionnant l'autorité de certification (CA) appropriée pour le certificat interne, le type et la longueur de la clé à utiliser pour assurer la sécurité du certificat.

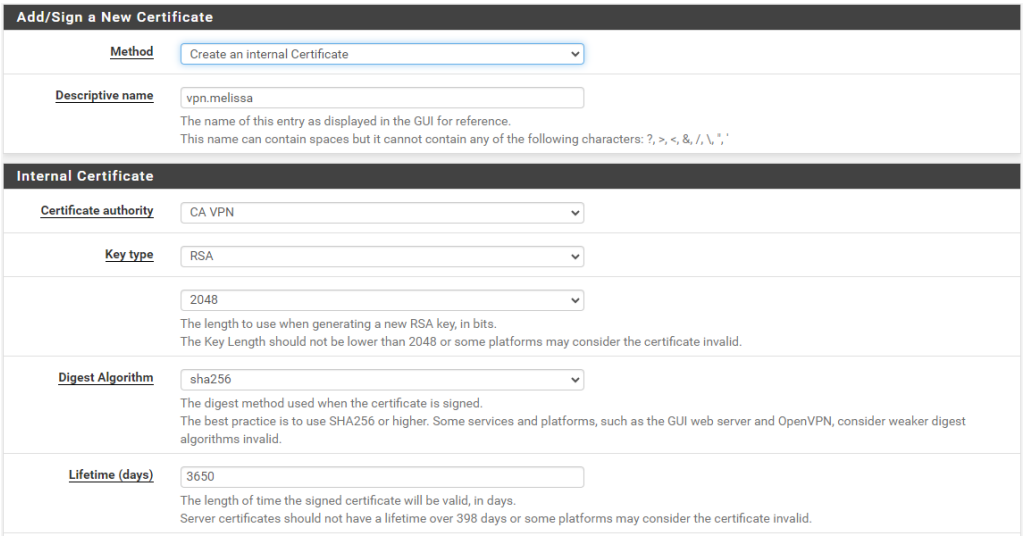


FIGURE 4.86 – Ajout du certificat interne dédié à l'utilisateur VPN.

En se basant sur nos configurations précédentes, il est essentiel de préciser, le nom de domaine de l'organisation, les détails de la région géographique ainsi que le département sur lequel on aimerait l'intégrer.

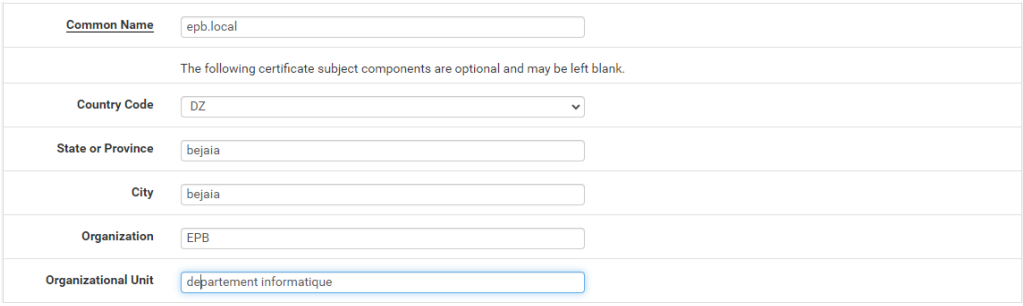


FIGURE 4.87 – Informations supplémentaires du certificat utilisateur.

Il est primordial de télécharger la configuration de certification au format ".ovpn" et de l'exporter vers nos clients VPN, et ce, en installant un paquet supplémentaire sur notre pare-feu. Il suffit de se rendre dans le menu **System -> Package Manager -> Available Packages** (Figure 4.88).

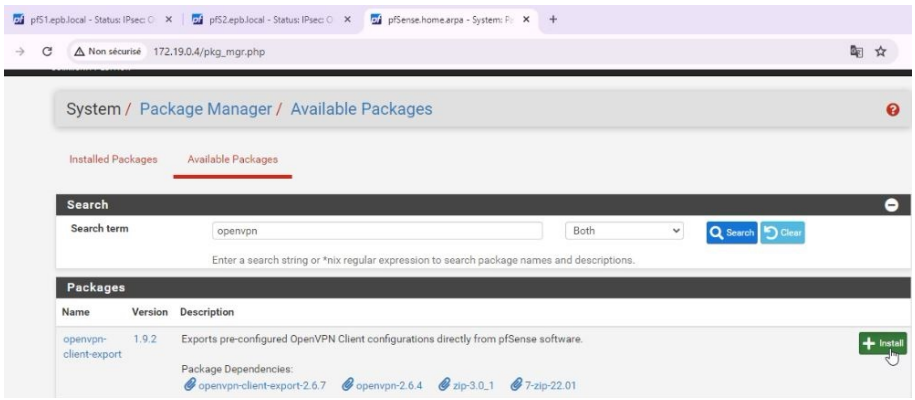


FIGURE 4.88 – Paquet à installer.

Après son installation et son exportation vers notre client OpenVPN, il suffit d'extraire le contenu de l'archive ZIP téléchargée sur ce dernier. L'utilisateur distant devra installe l'application OpenVPN (Figure 4.89).

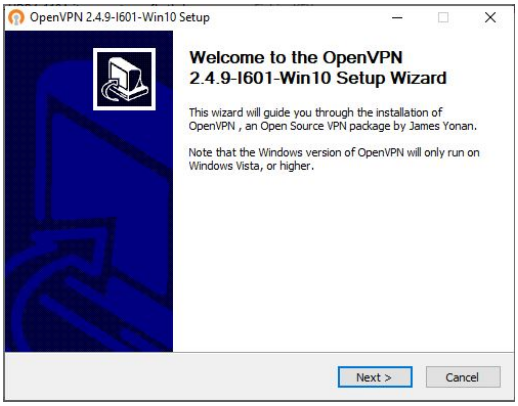


FIGURE 4.89 – Application OpenVPN.

Une règle sur l'interface WAN du pare-feu TEXTER pour autoriser le trafic VPN est nécessaire à mettre en place pour établir le tunnel VPN entre le site et l'utilisateur distant. Celle-ci est encadré en rouge dans la figure 4.90

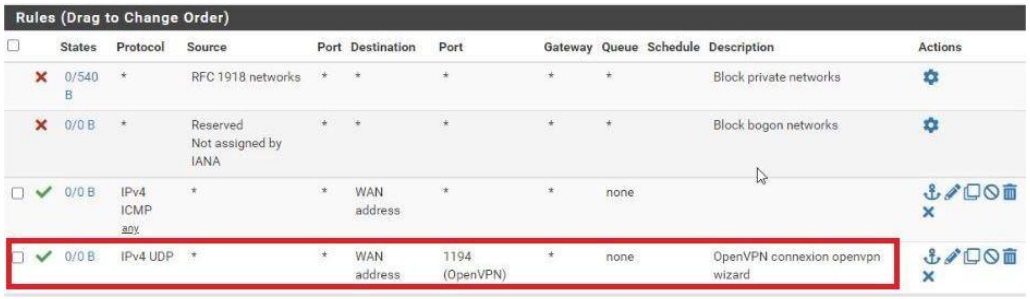


FIGURE 4.90 – Configuration de la règle pare-feu sur l'interface WAN.

4.6 Phase 3 : Tests

4.6.1 Test de la Haute Disponibilité du Cluster ProxmoxVE :

Pour tester la fiabilité du cluster, nous simulons une panne au niveau du nœud pve1 ; celui-ci hébergeant la machine virtuelle. Le serveur est mis hors de service en l'éteignant à partir de l'hyperviseur VMware Workstation (Figure 4.91). Cette panne cause l'arrêt de la machine virtuelle VMTest (Figure 4.92).

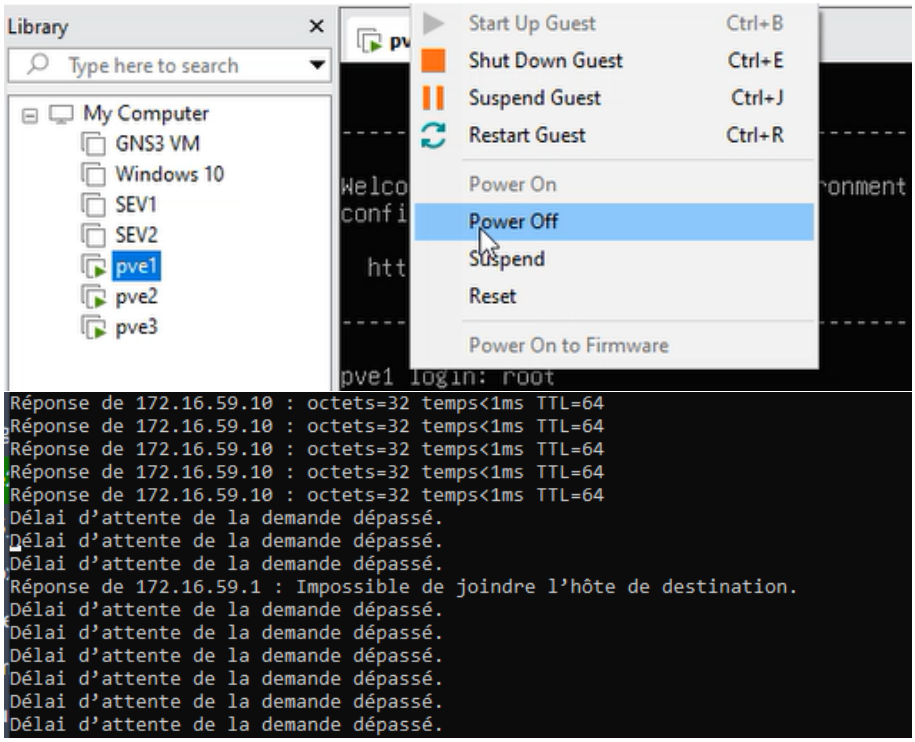


FIGURE 4.91 – Mise hors service du noeud pve1 (b).

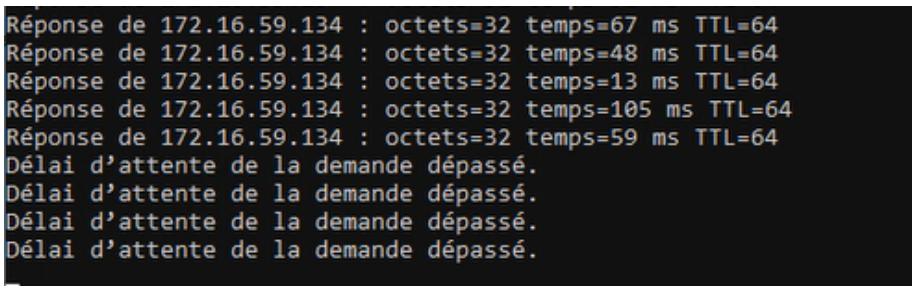


FIGURE 4.92 – Indisponibilité de la machine virtuelle VMTest

Après quelques secondes, la détection de l'inactivité de pve1 a lieu. Pve2 est alors élu comme master du cluster (Figure 4.93).

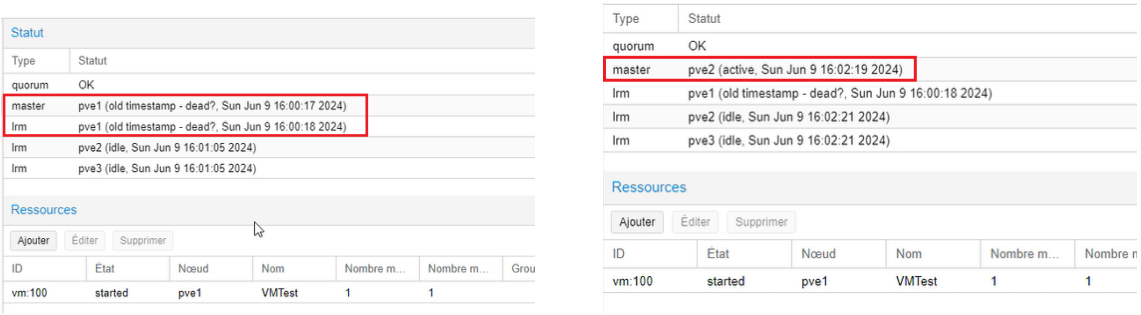


FIGURE 4.93 – Détection de l'inactivité de pve1 (à gauche) et élection de pve2 en tant que master (à droite).

L'opération a pris au total environ 3 mins, cette durée appelée RTO 3.1.4, comprend la détection de la panne du serveur pve1, l'élection de pve2 en tant que noeud leader du cluster, migration de la VM et réactivation de cette dernière (Figure 4.94 et 4.95). Cette durée peut être réduite dans le cas d'utilisation de machine plus performante.

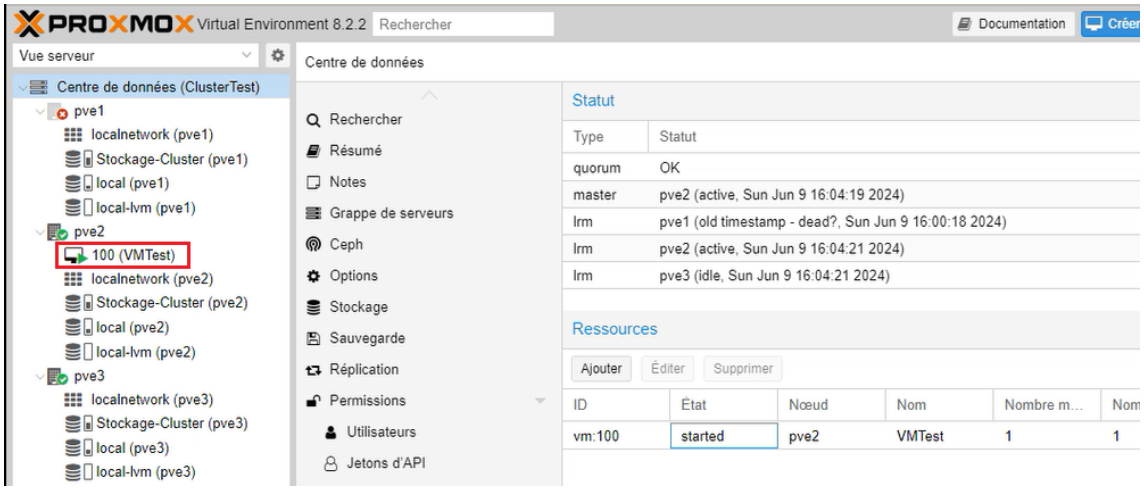


FIGURE 4.94 – Migration de la machine virtuelle vers pve2.

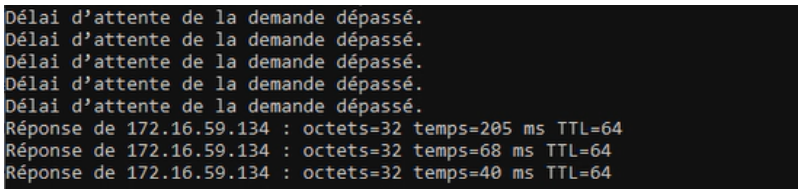


FIGURE 4.95 – Réactivation de la machine virtuelle.

4.6.2 Test du Cluster du service DHCP :

Pour tester la configuration effectuée en rapport avec notre service DHCP, une simulation d'une panne d'un de nos deux serveurs sera faite. Nous commencons

par vérifier l'état du service DHCP sur les deux serveurs SEV1 et SEV2. D'après la figure 4.96, les deux services fonctionnent correctement.

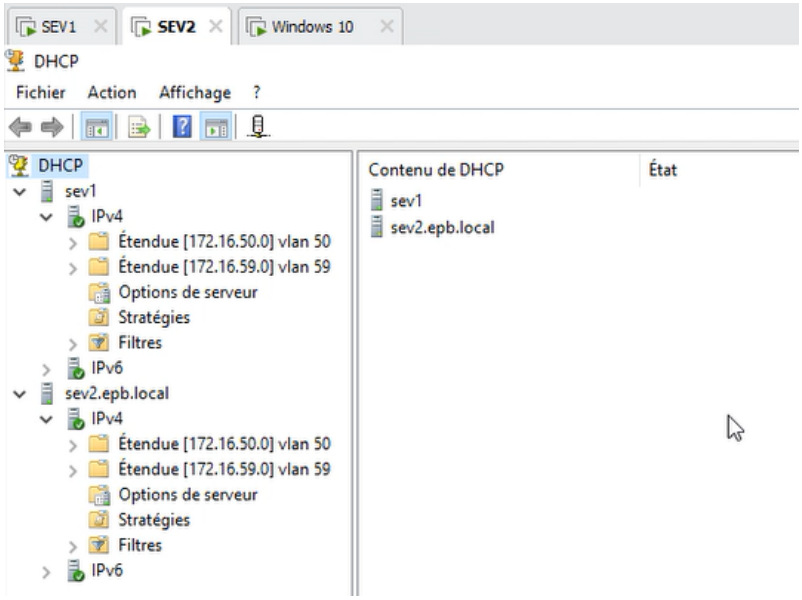


FIGURE 4.96 – État des services DHCP.

Nous nous connectons à présent à une machine Windows. La première chose à faire est de supprimer l'adresse IP attribuée à ce poste avec la commande :

```
C:Users/admin>ipconfig/release
```

Pour en demander une nouvelle, allouée par le serveur DHCP 172.16.59.100 qui devrait être acceptée avec la commande :

```
C:Users/admin>ipconfig/renew
```

En utilisant la commande :

```
C:Users/admin>ipconfig/all
```

L'adresse IP que nous apercevons dans la figure 4.97 est 172.16.59.135/24 et a été allouée par le serveur 172.16.59.100, ce qui témoigne de la bonne configuration du service DHCP.

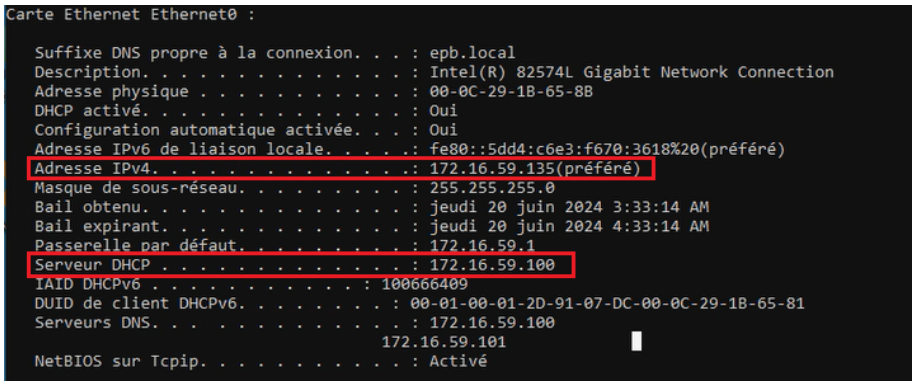


FIGURE 4.97 – Adresse IP de la machine Windows attribuée par SEV1.

La prochaine phase est de simuler une panne au niveau du serveur DHCP de SEV1. Il suffit de faire un clique droit sur le serveur DHCP de SEV1 et choisir **Toutes les tâche > Arrêter** (Figure 4.98).

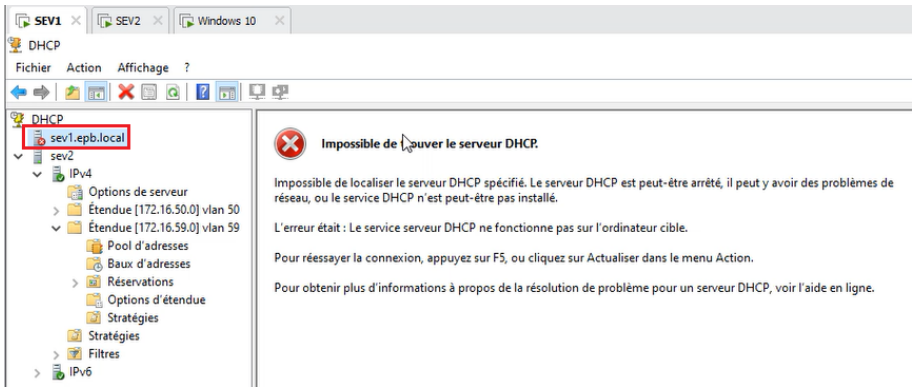


FIGURE 4.98 – Arrêt du serveur DHCP de SEV1.

Nous réutilisons la première et la deuxième commande pour mettre fin au bail puis renouveler l'adresse logique du poste Windows puis la troisième pour s'assurer du bon déroulement du test.

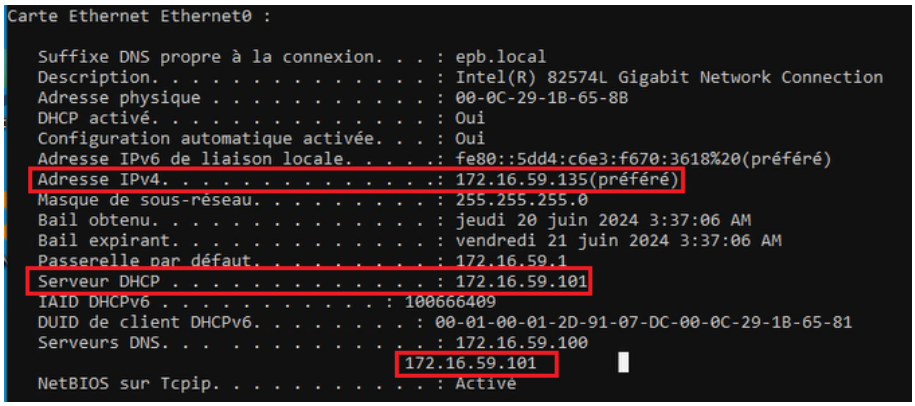


FIGURE 4.99 – Arrêt du serveur DHCP de SEV1.

La figure 4.99 illustre qu'il y a eu basculement et que le serveur secondaire SEV2 a pris le relai, ce qui atteste de la réussite du test.

4.6.3 Test des VPN :

Pour vérifier la fonctionnalité de nos tunnels VPN, il suffit d'établir la connexion à une extrémité et de vérifier si elle est établie à l'autre extrémité.

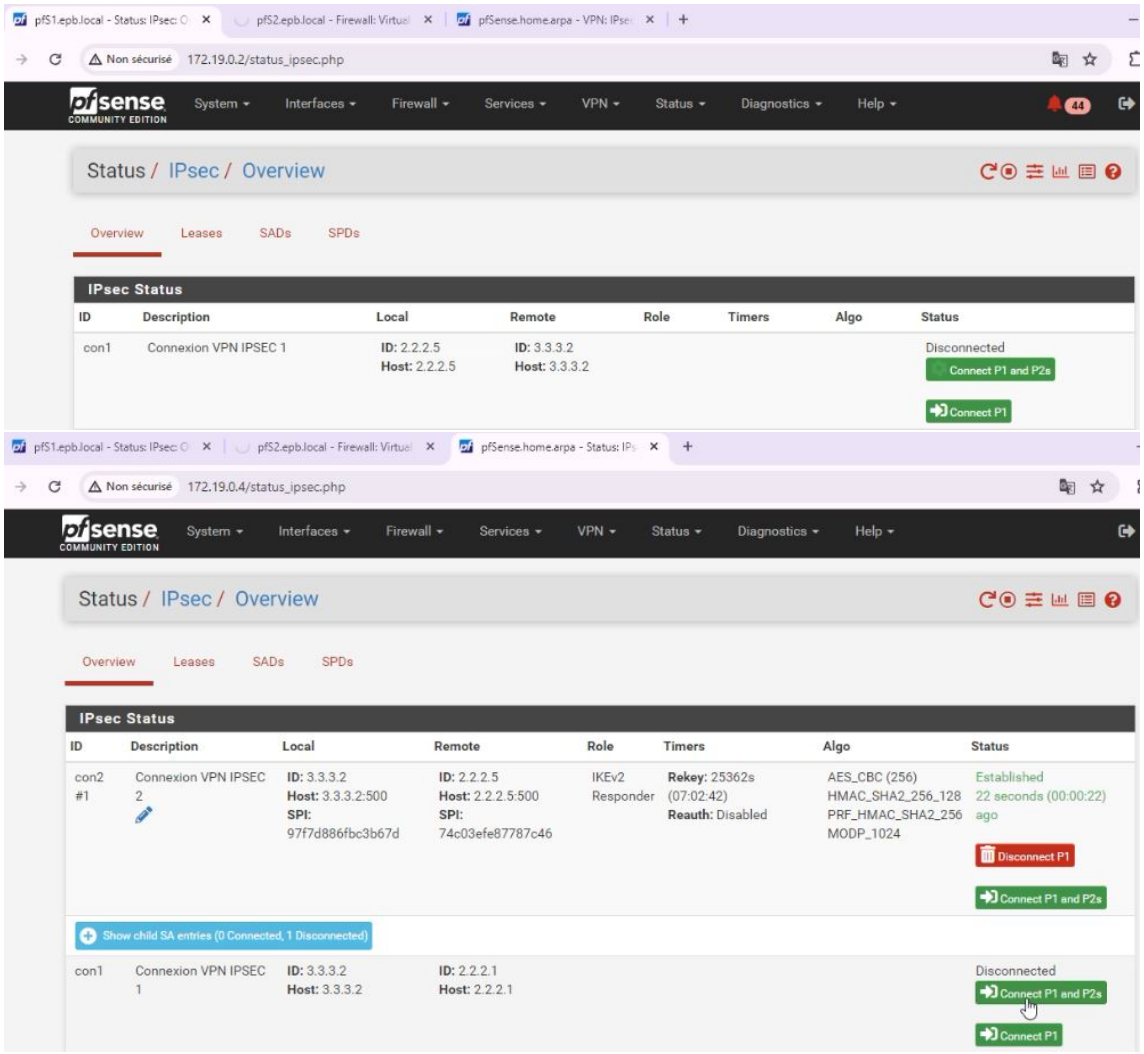


FIGURE 4.100 – Test du tunnel VPN site-à-site.

Le tunnel VPN site-à-site est donc fonctionnel.
Avant de vérifier le bon fonctionnement de notre tunnel poste-à-site, il est nécessaire de vérifier si le service DHCP configuré à l'interface e1/0 a attribué une adresse IP pour le poste distant.

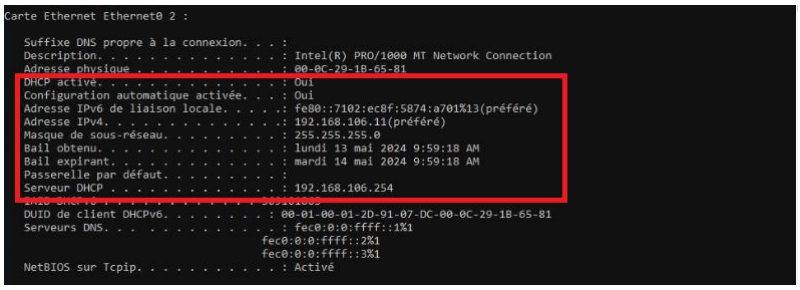


FIGURE 4.101 – Vérification de la connectivité avec le poste distant.

Le service DHCP à attribué une adresse IP à ce poste, il est donc possible de vérifier s'il a l'accès à notre réseau. Sur le poste de l'utilisateur distant, une icône OpenVPN apparaît dans la barre des tâches (Figure 4.102), avec un clic droit dessus et un autre sur "Connecter" nous allons vérifier si le tunnel entre l'utilisateur distant sera établi.

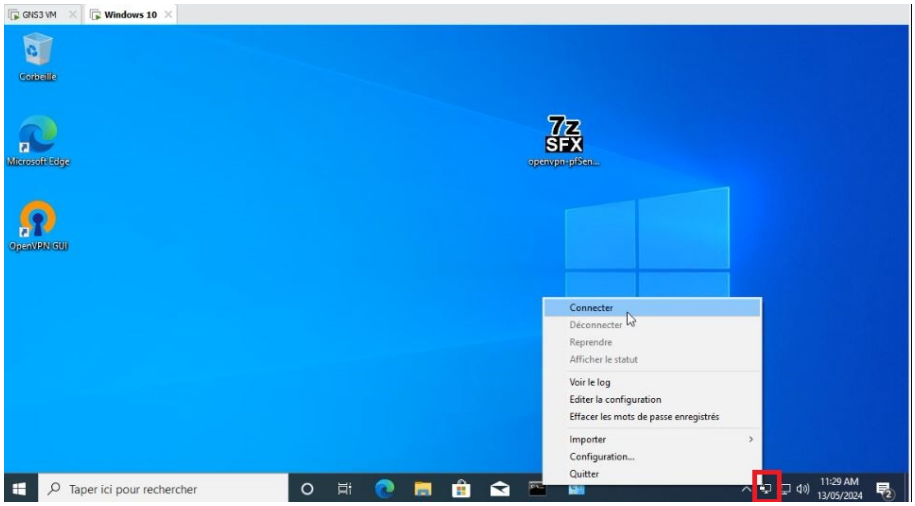
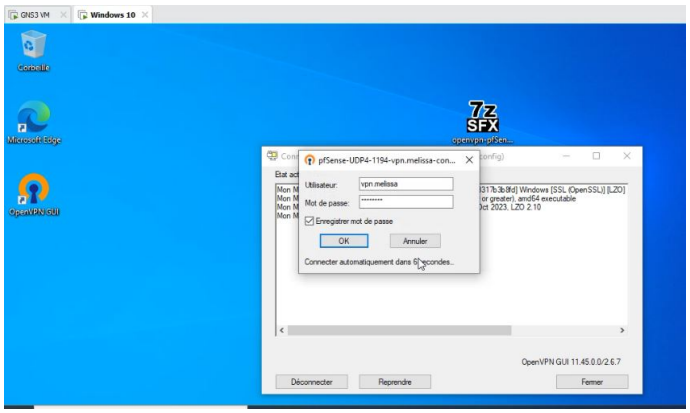
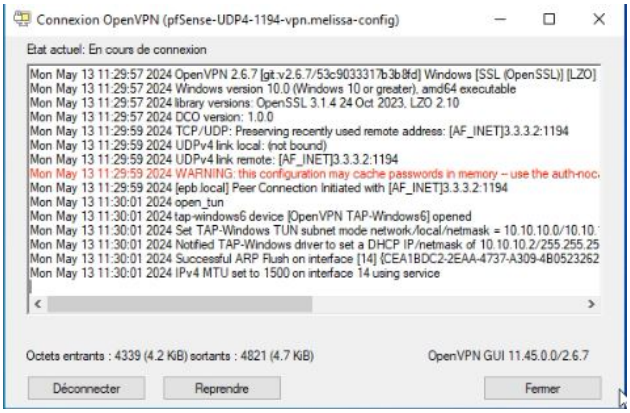


FIGURE 4.102 – Icône de connexion OpenVPN.

En insérant le nom d'utilisateur et le mot de passe associé au compte utilisateur créé au niveau du pare-feu (Figure 4.103a), le tunnel VPN client-à-site sera établi (Figure 4.103b).



(a) Authentification de l'utilisateur.



(b) Connexion du client OpenVPN.

FIGURE 4.103 – Etablissement du tunnel client-à-site.

Le tunnel a été établi avec succès, l'utilisateur externe peut désormais accéder au site distant.
Pour verifier encore la connectivté avec les terminaux du site TEXTER, nous allons demander une adresse IP pour le PC7 (Figure 4.104a) puis nous lancerons un ping pour confirmer la communication.

```
PC7> ip 172.16.100.10/24 172.16.100.1
Checking for duplicate address...
PC7 : 172.16.100.10 255.255.255.0 gateway 172.16.100.1
```

(a) Adresse IP du PC7.

```
C:\Users\admin>ping 172.16.100.10

Envoi d'une requête 'Ping'  172.16.100.10 avec 32 octets de données :
Réponse de 172.16.100.10 : octets=32 temps=11 ms TTL=63
Réponse de 172.16.100.10 : octets=32 temps=5 ms TTL=63
Réponse de 172.16.100.10 : octets=32 temps=7 ms TTL=63
Réponse de 172.16.100.10 : octets=32 temps=4 ms TTL=63

Statistiques Ping pour 172.16.100.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 11ms, Moyenne = 6ms
```

(b) Ping du PC distant au PC7.

FIGURE 4.104 – Connectivité entre le PC distant et le PC du site TEXTER.

Il est à remarquer que tous les paquets destinés au PC7 ont été envoyés avec succès, confirmant encore que notre VPN client-à-site est opérationnel.

Conclusion

L'objet de ce dernier chapitre à été la simulation de la nouvelle topologie, une étape essentielle pour assurer une infrastructure plus efficace et résiliente. En utilisant les configurations existantes et les concepts de réseau avancés, nous avons élaboré et expérimenté une nouvelle architecture qui répondra aux besoins actuels et futurs de l'organisme d'accueil. Les performances et la disponibilité ont été considérablement améliorées grâce aux simulations, confirmant le bon fonctionnement des modifications suggérées. Cette nouvelle configuration offre une base solide pour la croissance constante de l'infrastructure réseau de l'entreprise, garantissant une meilleure préparation face aux défis technologiques à venir.

Conclusion générale

Au terme de ce travail, nous avons examiné la problématique de la haute disponibilité et du clustering dans un environnement de virtualisation. L'analyse de l'entreprise d'accueil et de ses défis nous a permis de prendre conscience des enjeux spécifiques liés à la haute disponibilité. Nous avons exploré en détail les différentes technologies de virtualisation des systèmes et des réseaux, tout en poursuivant avec une étude approfondie des stratégies de haute disponibilité et de clustering, ce qui nous a permis par la suite d'identifier les solutions les plus adaptées pour garantir la fiabilité et la tolérance aux pannes dans notre environnement. Nous avons notamment passé en revue les concepts de redondance, de basculement et de répartition de charge, ainsi que les technologies de clustering et de virtualisation des ressources.

La phase de simulation de la nouvelle topologie du réseau a été l'occasion de mettre en pratique les connaissances acquises et de concevoir une architecture idéale pour notre environnement de virtualisation. Celle-ci nous a permis de valider les choix techniques et d'identifier les éventuels points de fragilité à renforcer. Pour avoir atteint notre objectif, nous avons simulé notre réseau à l'aide du logiciel GNS3 pour sa capacité à simuler et à reproduire des réseaux complexes. Nous avons appliqué au sein de notre architecture différents concepts tels que la configuration des liens agrégés, l'intégration d'une redondance matérielle pour l'élimination des SPOF, ainsi que l'utilisation d'un hyperviseur type 1, où l'on a pu créer des serveurs en tant que machines virtuelles sur lesquelles nous avons pu intégrer principalement le clustering ainsi que la gestion de la haute disponibilité. Ces principes ont également été revus au niveau de nos pare-feux à l'aide des protocoles CARP et pfsync.

En effet, nous avons pu tester le comportement de notre réseau et de nos VM en

cas de panne, en terme de basculement, de migration et de réplication, ce qui nous a conduit à confirmer nos résultats et à nous rendre compte que des temps d'arrêt minimisés en utilisant les pratiques adaptées. Bien que ces pratiques couvrent de nombreux avantages, la mise en place de la haute disponibilité et du clustering est souvent associée à des coûts onéreux. Cependant, notre choix d'outils est à souligner, en vue de l'utilisation des solutions principalement open-source pour ne pas impacter le plan budgétaire de l'entreprise.

Concernant l'aspect sécuritaire, nous avons pu mettre en place un système d'annuaire ainsi que des règles de pare-feu pour la gestion des accès et le filtrage du trafic réseau entrant et sortant. Toutefois, des mécanismes de détection d'intrusion pourraient être pris en compte pour des travaux futurs. Au-delà de cela, cette étude met en avant l'importance de la planification, de la mise en place de procédures de maintenance et de surveillance pour assurer la continuité et la fiabilité des systèmes virtualisés.

En conclusion, ce travail a permis d'acquérir une expertise approfondie dans le domaine des réseaux pour ses aspects de haute disponibilité, clustering et virtualisation, offrant ainsi des perspectives intéressantes pour l'avenir.

Annexe A

Complément du chapitre 3

A.1 Principales sources d'indisponibilité

1. **Arrêt planifié :** C'est une période prédéterminée pendant laquelle un système, un service ou une application est mis hors ligne pour les raisons suivantes :
   - **Maintenance Préventive :** Des périodes d'interruption peuvent être prévues pour effectuer des opérations de maintenance préventive, comme la mise à jour des logiciels et le remplacement du matériels défectueux.
   - **Mises à niveau :** Lorsque de nouveaux équipements matériels sont installés, des arrêts planifiés peuvent être nécessaires pour intégrer ces composants dans l'infrastructure existante.
2. **Arrêt non planifié :** un arrêt non planifié est un temps d'indisponibilité impondérable survenant pendant les horaires d'activité. Les arrêts non planifiés peuvent être classés en quatre catégories :
   - **Erreurs humaines :** L'erreur humaine est l'origine principale des arrêts imprévus. Le manque de formation, mauvaises manipulation, avertissements négligés ou mêmes des intentions malveillantes d'employés peuvent être à l'origine d'arrêts [23].
   - **Pannes matérielles :** La surchauffe de composants électroniques, l'humidité, les décharges d'électrostatique, défauts de fabrication ou autres facteurs sont des formes de dégradations matérielles qui sont susceptible de conduire à la défaillance et dysfonctionnements d'équipements physiques [23].
   - **Pannes logicielles :** Les arrêts lies aux pannes logicielles sont généralement liés à des vulnérabilités de sécurité, bugs, mauvaises configu-

rations ou à des problèmes de compatibilité.

- **Facteurs environnementaux :** Les évènements aléatoires suivants : coupure de courants, catastrophes naturelles...etc, sont de taille à interrompre la disponibilité des réseaux d'entreprise.

A.2 Importance de la Haute Disponibilité

- **Minimisation des pertes financières :** Pour les entreprises, les temps d'arrêts se traduisent en perte de revenus conséquentes. L'investissement dans des technologies assurant fiabilite et performance est un moyen rentable de protéger les pertes financières.
- **Protection contre les pertes de données :** En cas panne ou de sinistre, des mécanismes assurent que les données sont sauvegardées et accessibles, ce qui permet de minimiser les risques de perte et de corruption.
- **Renforcement de la crédibilité de l'entreprise :** Les pannes informatiques peuvent nuire à la réputation d'une entreprise. La haute disponibilité permet de maintenir une image de fiabilité et de professionnalisme ce qui attire de nouveaux clients et partenaires.
- **Gain en productivité :** Une infrastructure hautement disponible permet de maintenir un environnement de travail fluide et sans interruption même en cas de pannes,favorisant ainsi la performance et l'efficacité des équipes.
- **Satisfaction des clients :** Les clients s'attendent à pouvoir accéder aux services 24h/24 et 7j/7. Une entreprise qui dispose d'un système informatique hautement disponible est perçue comme étant fiable et professionnelle, ce qui contribue à la satisfaction des clients envers l'entreprise.

Il est important de considérer que le besoin en termes de disponibilité peut varier considérablement d'un secteur d'activité à un autre, en fonction des exigences spécifiques de chaque domaine. Les facteurs qui peuvent influencer cette variation sont : la criticité des opérations, la demande des clients, le type de service offert. Bien que les infrastructures hautement disponibles offrent de nombreux avantages, elles présentent également certains inconvénients :

- **Complexité d'implémentation :** La complexité croissante des infrastructures haute disponibilité est attribuable à plusieurs facteurs, notamment la variété des composants logiciels et matériels et les configurations redondantes. utiliser des outils de gestion automatisés, et investir dans la formation et le développement des compétences de l'équipe chargée de l'administration réseau et système de l'entreprise.

- **Impact budgétaire élevé :** La mise en place et la maintenance d'une infrastructure HA sont généralement plus coûteuses que celles d'une infrastructure traditionnelle, dû aux services supplémentaires nécessaires pour assurer la redondance. Il est possible d'atténuer cet impact en optant pour des solution de virtualisation et open source pour réduire les coûts de licence des logiciels et éliminer le besoin d'investissements massifs en matériel.

A.3 Principes fondamentaux de la haute disponibilité

- **Fiabilité et résilience :** La fiabilité est l'aptitude d'un système à fonctionner sans interruption pendant une période donnée. Quant à la résilience, c'est sa capacité de maintenir accès aux données et la disponibilité des processus opérationnels malgré un événement perturbateur [15].
- **Récupération rapide :** Il existe de nombreuses façons de se remettre d'échecs ; il est donc important que l'on puisse déterminer quels types de pannes peuvent survenir dans un environnement haute disponibilité et comment récupérer rapidement de ces pannes afin de répondre aux besoins d'entreprise et clients [14].
- **Continuité des opérations :** Fournir un accès continu à vos données est essentiel lorsque le temps d'arrêt est inacceptable pour effectuer des activités de maintenance. Dans une architecture haute disponibilité, les activités telles que les mises à jour de d'application ou le replacement d'un matériel défectueux doivent être transparentes pour l'utilisateur [14].

Annexe B

Installation des machines virtuelles

B.1 Installation de la machine virtuelle Proxmox VE :

Nous débutons l'installaton de Proxmox VE en téléchargeant son image ISO à partir du site officiel https://www.proxmox.com/en/downloads (Figure B.1). La version utilisée dans cette partie pratique est la version 8.2-1 (dernière MàJ le 24 avril 2024) .

FIGURE B.1 – Image ISO Proxmox VE.

Une fois le fichier ISO téléchargé, nous devons créer une machine virtuelle sur l'outil de virtualisation de poste de travail VMware Workstation 17 pro (Figure B.2).

FIGURE B.2 – Assistant de création de machine virtuelle.

Comme déclaré antérierement, Proxmox VE étant basé sur Debian Linux, nous sélectionnons les paramètres appropriés pour un système d'exploitation Linux (Figure B.3).

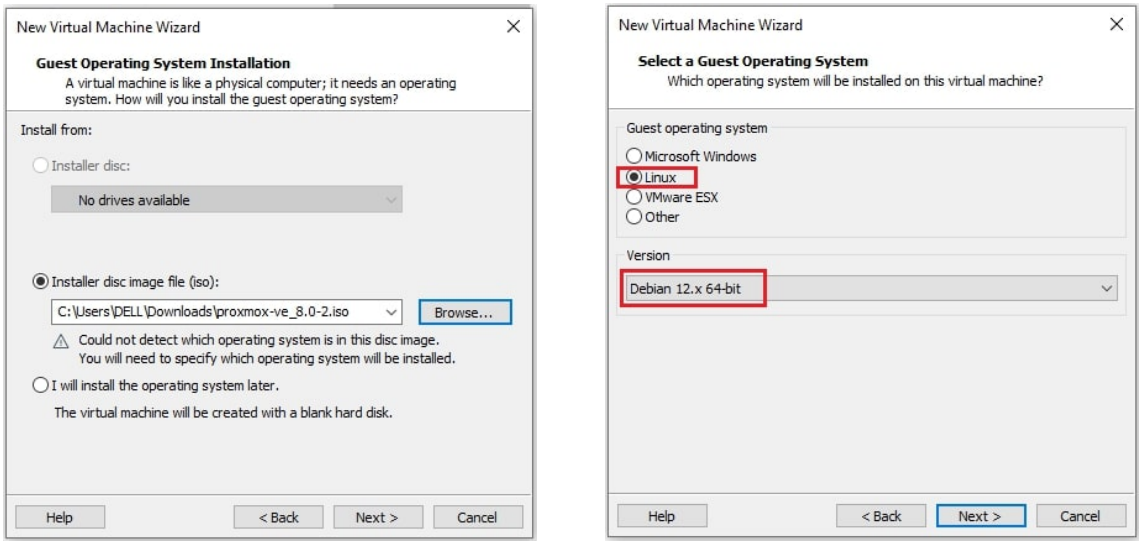


FIGURE B.3 – Création de la machine virtuelle Proxmox VE (a).

Nous cliquons sur **Next**, dans la figure B.4 l'utilisateur doit introduire un nom à son noeud, ainsi que sa localisation. La prochaine étape est d'insérer la taille maximale du disque en gigaoctets. Dans le cas de cette étude, le volume alloué est de 20 Go dû aux ressources limitées que nous avons à disposition.

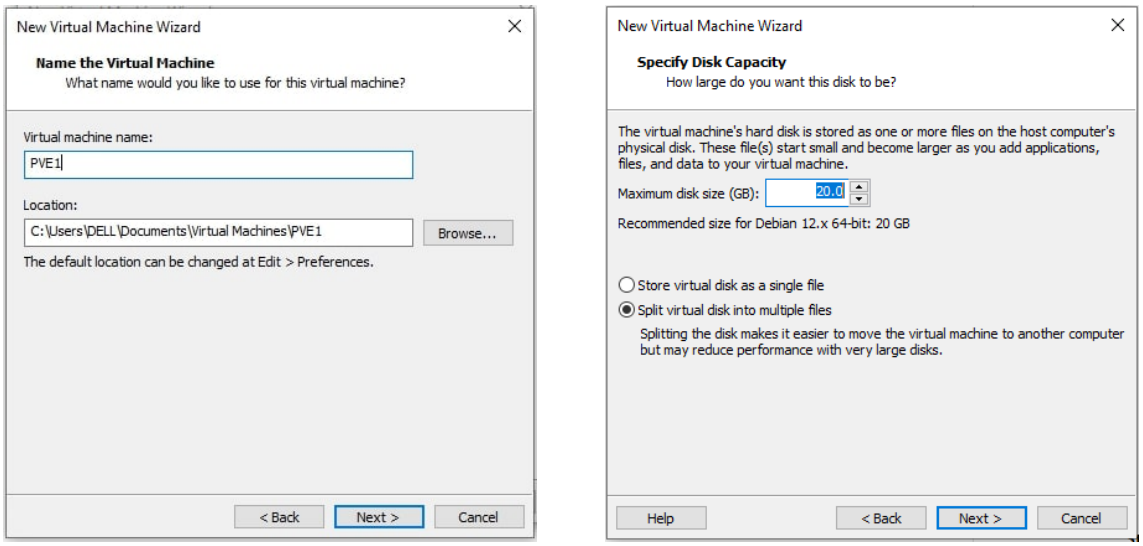


FIGURE B.4 – Création de la machine virtuelle Proxmox VE (b).

Dernière halte de la création de la VM est la vérification et la personnalisation des paramètres. Pour ce faire, nous sélectionnons **Customize Hardware** indiqué rouge dans la figure B.5.

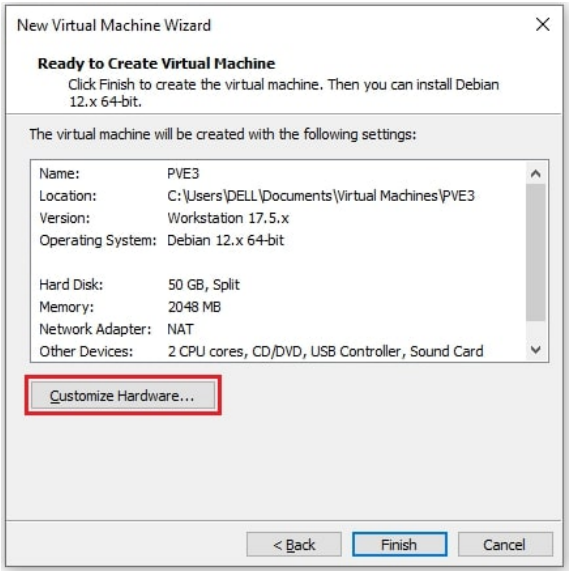


FIGURE B.5 – Création de la machine virtuelle Proxmox VE (c).

Il est impératif de cocher la case **Virtualize Intel VT-x/EPT or AMD-V/RVI** (la figure B.6) pour activer la virtualisation imbriquée et qui s'avérera nécessaire pour la création d'une machine virtuelle dans le serveur Proxmox. Nous aurons aussi besoin d'ajouter un autre disque identique au premier en cliquant sur **add...**, nous y reviendrons plus tard. Nous aurons besoin de 3 machines virtuelles Proxmox dans ce projet.

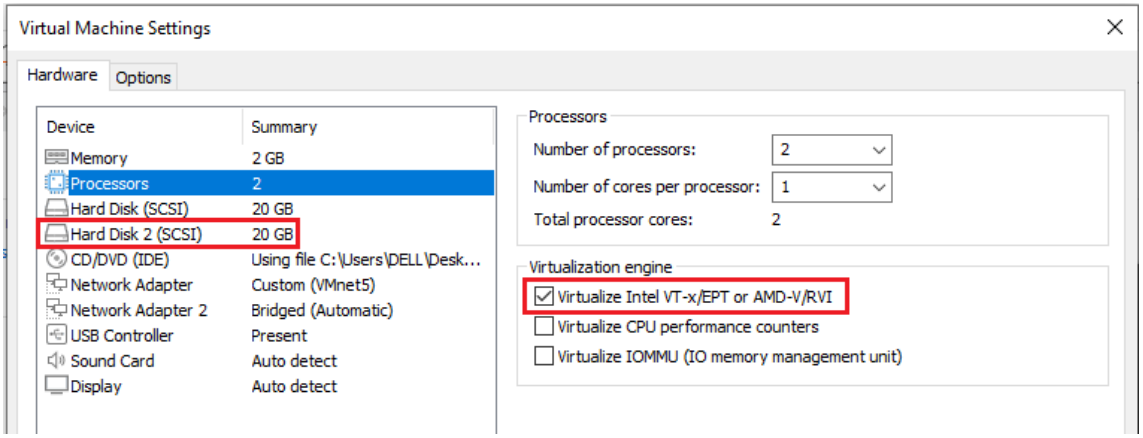


FIGURE B.6 – Paramétrage de la machine virtuelle Proxmox VE.

Pour finaliser la création, on clique sur **Finish**.

B.2 Installation de la machine virtuelle PfSense :

Pour installer l'iso de pfsense nous avons décidé de l'intégrer directement sur le logiciel GNS3 en suivant les étapes suivantes [28] :

1. Pour commencer nous allons sur **All devices**> **New template** et nous allons sélectionner le choix recommandé qui est l'installation de l'équipement à partir du serveur GNS3 VM.

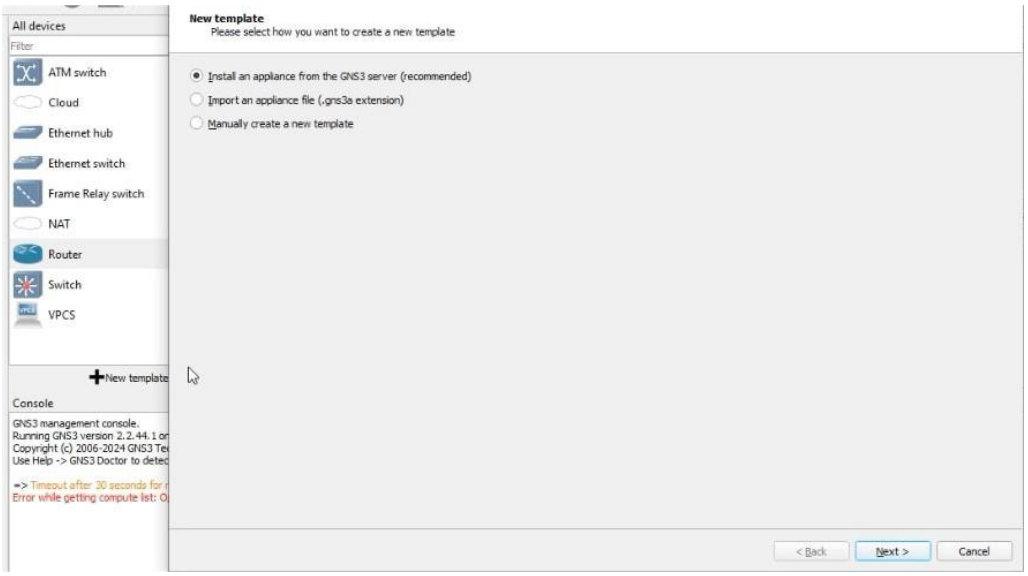


FIGURE B.7 – Interface d'ajout d'un nouvel équipement.

2. Il suffit ensuite de chercher le nom pfSense parmi la liste des appareils disponibles, puis sélectionner la version adaptée afin de lancer son installation.

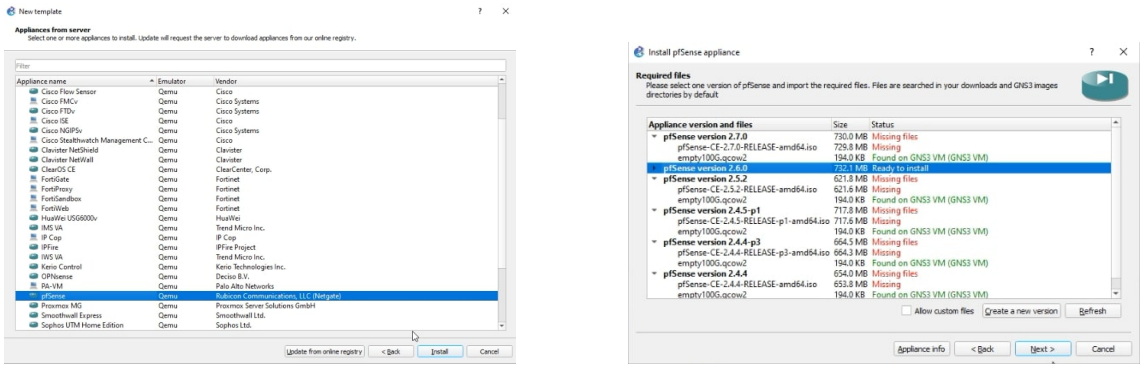


FIGURE B.8 – Recherche de la version adaptée de pfSense.

3. Un premier écran s'ouvre à nous, présentant les conditions de licence pour le logiciel pfSense que nous devons accepter pour poursuivre l'installation.

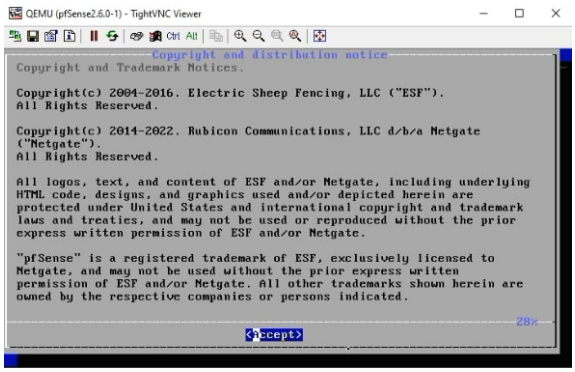


FIGURE B.9 – Licence d'installateur.

4. Le programme d'installation nous invite à lancer les options de secours ou à démarrer le processus d'installation. Dans notre cas, nous continions vers l'installation du logiciel.

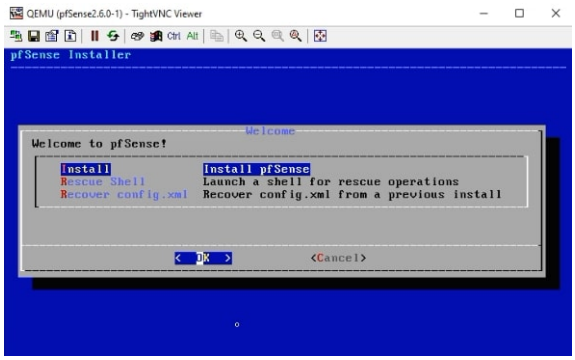


FIGURE B.10 – Options de secours ou d'installation.

5. Dans cette étape, il est demandé de choisir le système de fichiers voulu pour le disque cible du pare-feu. Le type de système de fichiers ZFS (Zettabyte

File System) est plus fiable et possède plus de fonctionnalités c'est pour cela que nous allons le séléctionner.

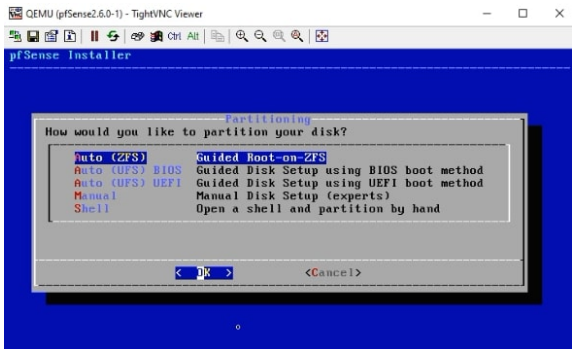


FIGURE B.11 – Sélection du système de fichiers.

6. Le programme d'installation nous présente l'écran de configuration ZFS, nous sélectionnons donc **Pool type/Disks** pour choisir le type de périphérique virtuel que nous utiliserons. Parmi les disponibilités, le type **stripe** qui convient aux pare-feux avec un seul disque cible sera choisi.

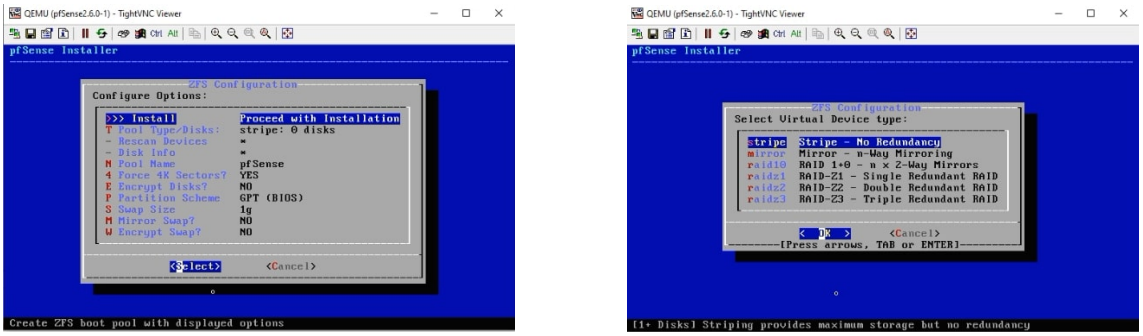


FIGURE B.12 – Sélection du périphérique virtuel.

7. Enfin, l'installation sera finalisée en cliquant sur **Reboot** afin de redémarrer sur le système de pfSense.

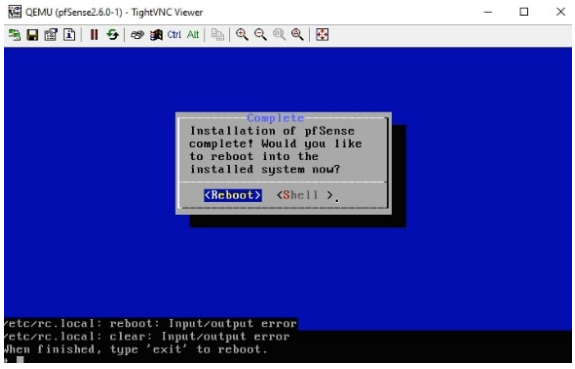
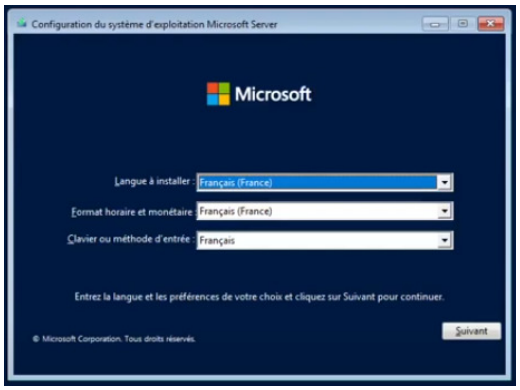


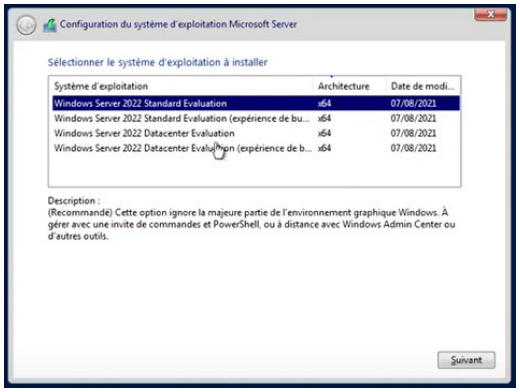
FIGURE B.13 – Fin de l'installation.

B.3 Installation de la machine virtuelle Windows serveur 2022 :

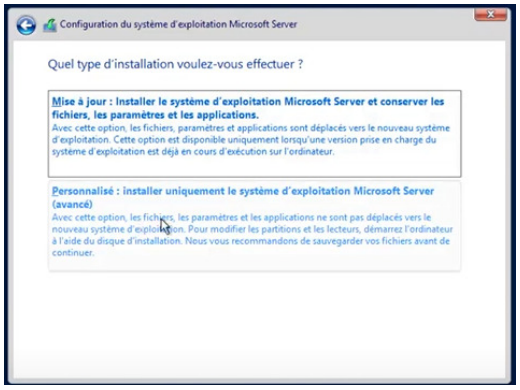
Pour installer la VM du serveur Windows 2022 nous allons suivre les étapes représentées par la figure B.14 :



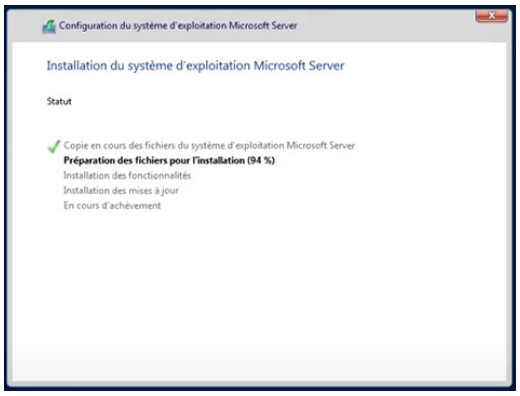
(a) Choix de la langue.



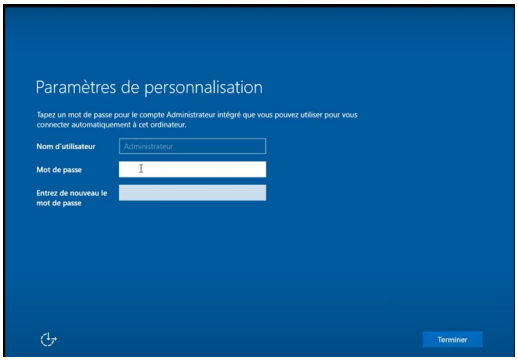
(b) Sélection du système d'exploitation.



(c) Choix du type d'installation.



(d) Installation en cours.

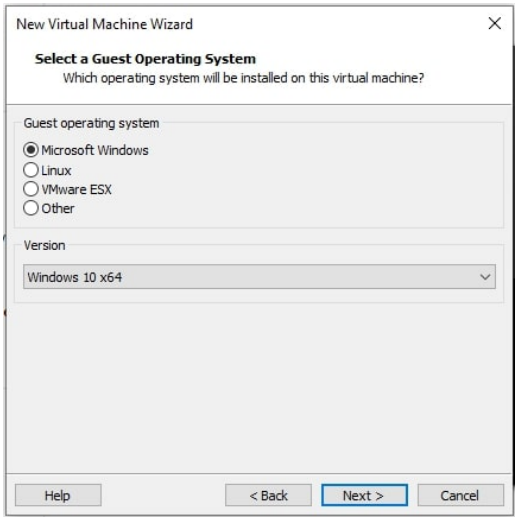


(e) Saisie du nom d'utilisateur et du mot de passe.

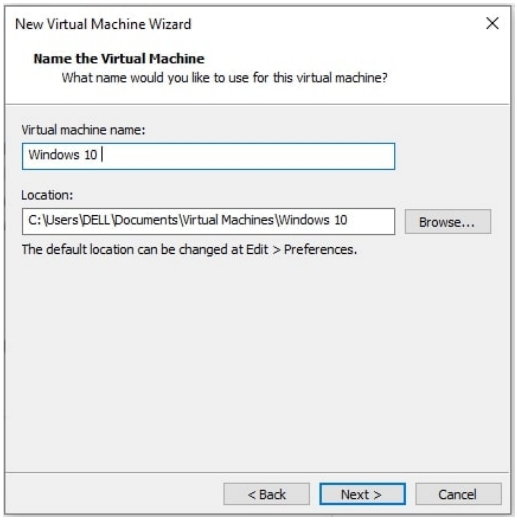
FIGURE B.14 – Installation du serveur Windows 2022.

B.4 Installation du système d'exploitation Windows 10 :

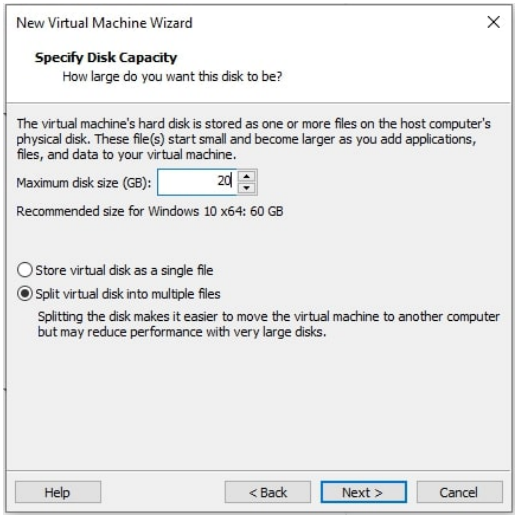
Pour installer la machine virtuelle du système d'exploitation Windows 10 nous allons suivre les étapes de la figure B.15 faites à partir du logiciel VMware Workstation Pro 17 :



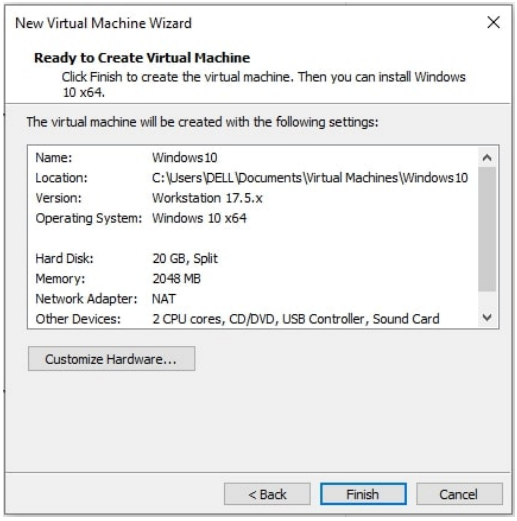
(a) Sélection du sysème d'opération.



(b) Nom de la nouvelle VM.



(c) Attribution de l'espace disque.



(d) Fin de création de la nouvelle VM.

FIGURE B.15 – Installation du système d'exploitation Windows 10.

Après cela, nous allons rajouter des paramètres afin de compléter l'installation. Cela inclut la sélection de la carte réseau utilisée ainsi que l'ajout de l'ISO de cette VM.

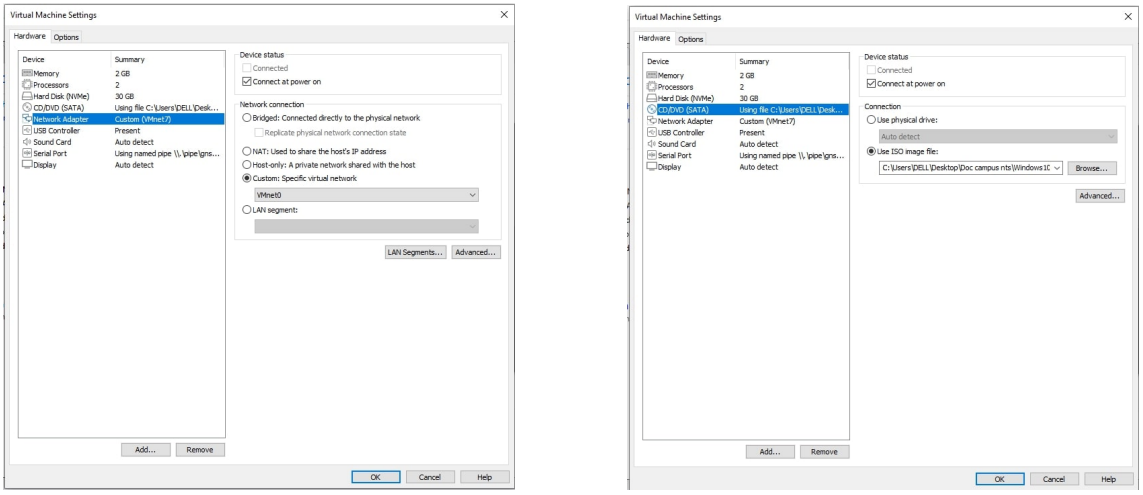


FIGURE B.16 – Paramètres supplémentaires.

Nous pouvons ainsi finir l'installation de notre notre VM et la redémarrer :

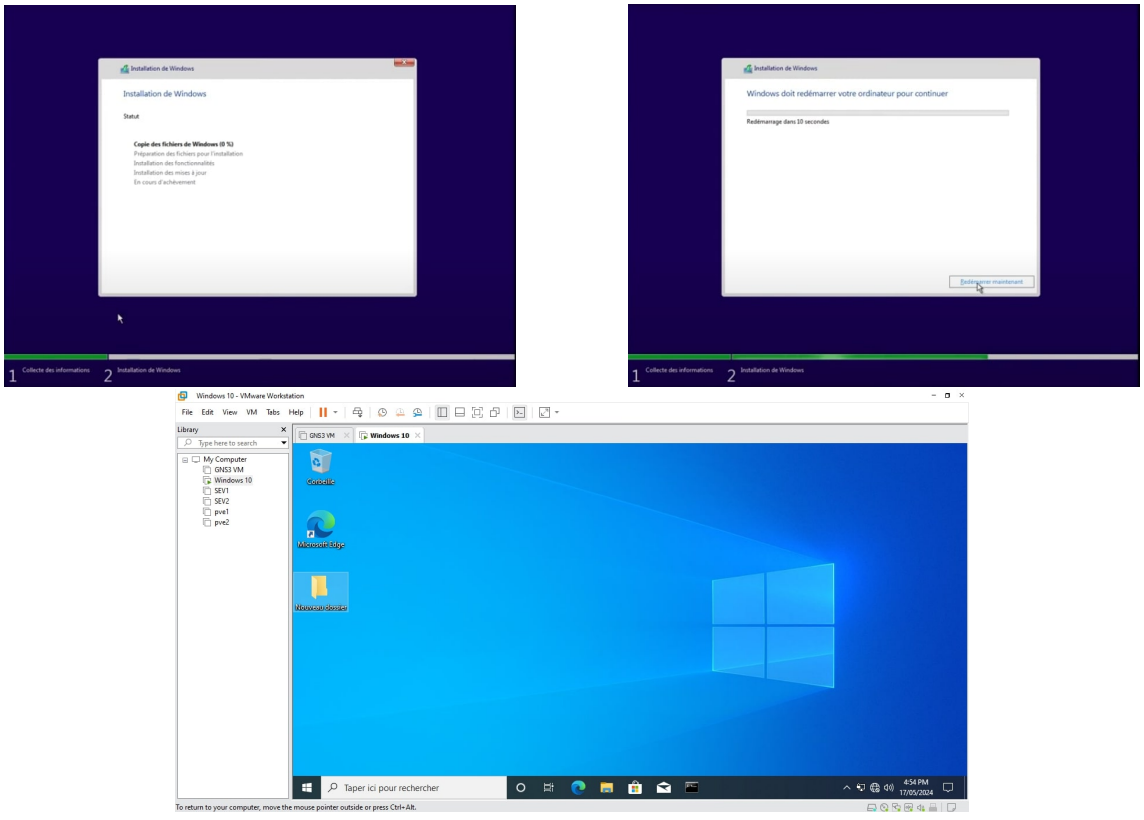


FIGURE B.17 – Fin de l'installation.

Annexe C

Les VLAN privés

Contrairement à un VLAN traditionnel qui fonctionne comme un domaine unique de diffusion, les VLAN privés permettent d'avoir un même VLAN principal (connu sous le nom de VLAN primaire) qui sera subdivisé en plusieurs sous-domaines de diffusion séparés (connus sous le nom de VLAN secondaires). Cette méthode permet moins de gaspillage d'adresses IP, une meilleure isolation et une sécurité encore plus renforcée, elle est souvent utilisée dans des zones démilitarisées ou pour créer des réseaux invités sécurisés, en isolant les appareils des invités du réseau interne de l'entreprise.
De ce que nous avons mentionné on retient deux types de VLAN : primaire et secondaire. Les VLAN secondaires à leurs tours se composent également de deux types :

- **VLAN isolé :** Les ports d'un VLAN isolé ne peuvent pas communiquer entre eux au niveau couche 2.
- **VLAN communautaire :** Les ports d'un VLAN communautaire peuvent communiquer uniquement entre eux et ne peuvent donc pas communiquer avec les ports d'autres communautés au niveau couche 2.

Il existe alors trois types de ports de VLAN privé :

1. **Port promiscuous :** Un port promiscuous appartient au VLAN primaire et a la capacité de communiquer avec toutes les interfaces, y compris les ports hôtes appartenant aux VLAN secondaires associés au VLAN principal.
2. **Port isolé :** Le port isolé est un port hôte (host en anglais) qui fait partie d'un VLAN secondaire isolé. Ce port dispose d'une couche 2 entièrement séparée des autres ports du même domaine VLAN privé, hormis les ports promiscuous. Le trafic vers les ports isolés est bloqué par les VLAN privés, à l'exception du trafic provenant des ports promiscuous.

3. **Port de communauté :** Un port de communauté est un port hôte qui appartient à un VLAN secondaire de communauté. Ces interfaces sont isolées au niveau de la couche 2 de toutes les autres interfaces des autres communautés et des ports isolés au sein de leur domaine VLAN privé [36].

Dans la configuration de notre nouvelle architecture, nous avons utilisé les VLAN privés au niveau de la DMZ. Pour ce faire, les étapes suivantes ont été suivies :

1. Configuration du VTP en mode transparent pour que les informations sur les VLAN ne soient pas propagées entre les commutateurs via les trunks, cela veut dire que chaque commutateur peut avoir sa propre configuration VLAN, indépendamment des autres commutateurs du réseau [12].
2. Création du VLAN 103 comme VLAN primaire à qui on lui a associé le VLAN isolé 100 et le VLAN communautaire 101.

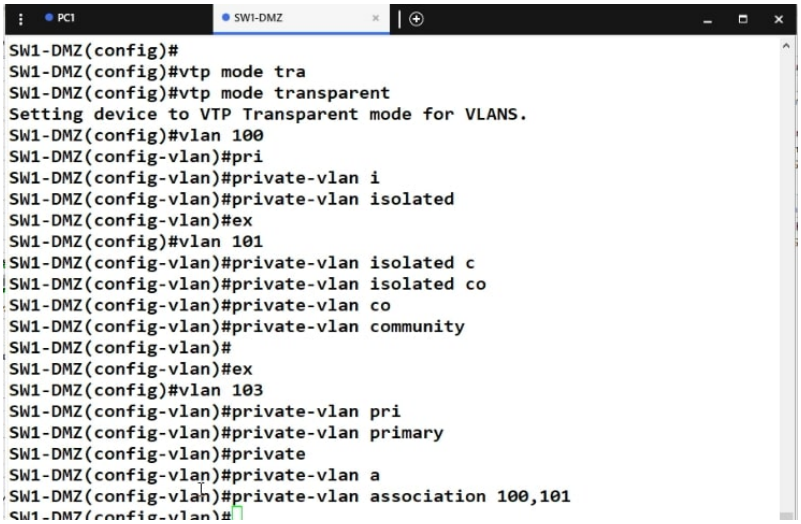


FIGURE C.1 – Configuration du vtp et création des VLAN privés.

3. Configuration des ports hôtes communautaires liés aux serveurs web et Exchange.

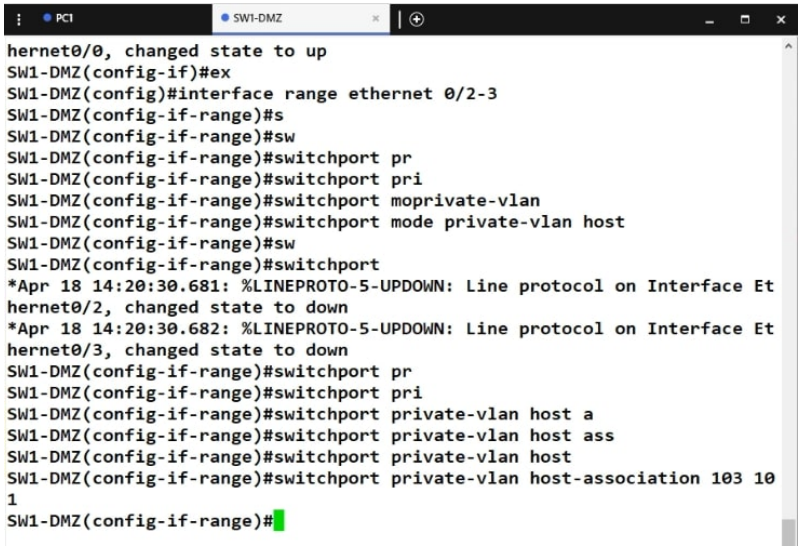


FIGURE C.2 – Configuration des ports hôtes communautaires.

4. Configuration du port lié aux serveur SIP en tant que port hôte isolé.

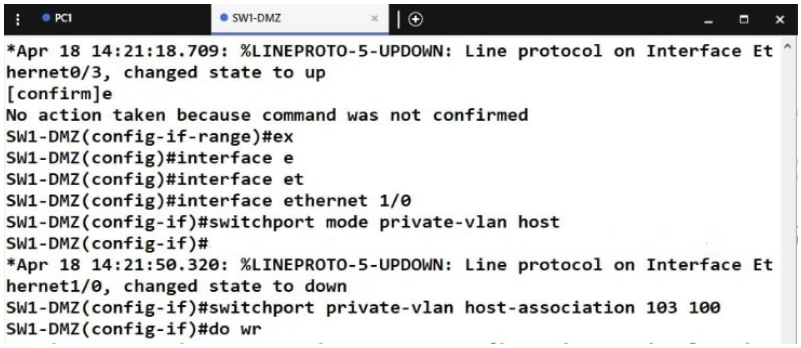


FIGURE C.3 – Configuration du port hôte isolé.

5. Nommination du port promiscuous au niveau de l'interface e0/0 qui relie le switch DMZ au parfeu et mappage des VLAN secondaires au VLAN primaire.

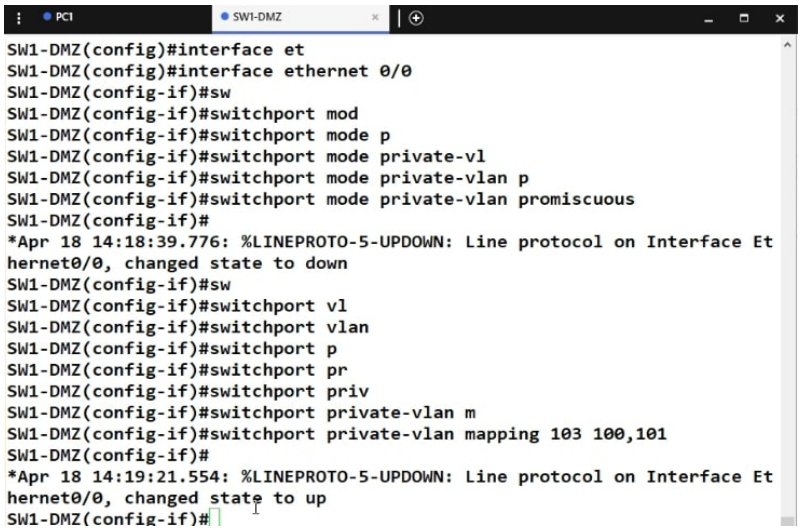


FIGURE C.4 – Nommination du port promiscuous.

Annexe D

Généralités

- **Le protocole LACP (Link Aggregation Control Protocol :** Norme définie par IEEE 802.3ad (Institute of Electrical and Electronics Engineers), permet d'agréger plusieurs connexions réseau physiques en une seule liaison logique. Son objectif est d'augmenter la bande passante disponible et d'assurer la redondance des liens en cas de défaillance [37].
- **Le protocole STP (Spanning Tree Protocol) :** C'est un protocole de couche 2 qui permet de concevoir des topologies sans boucle dans les réseaux LAN à l'aide de commutateurs.
  Son algorithme « spanning tree » détermine le meilleur chemin entre les points du réseau tout en assurant la redondance des câbles. Il bloque certains ports de commutation pour garantir l'unicité du chemin et éviter les tempêtes de diffusion susceptibles de perturber le réseau [13].
- **Les règles de pare-feu :**
  - **Règle ICMP (Internet Control Message Protocol) :** L'ICMP est un protocole important pour le dépannage et le diagnostic réseau. Il permet d'envoyer des messages de contrôle et d'erreur entre les hôtes. Les règles ICMP doivent permettre le trafic ICMP entrant et sortant afin de faciliter l'identification et la résolution des problèmes de connectivité. Cela inclut les messages ping, les messages d'erreur de destination injoignable, etc. Une configuration adéquate des règles ICMP contribue à la maintenance et à la surveillance efficaces du réseau.
  - **Règle TCP (Transmission Control Protocol) :** Le TCP est un protocole orienté connexion, largement utilisé par les applications essentielles comme le web, les courriels et les transferts de fichiers. Les règles TCP doivent autoriser le trafic TCP entrant et sortant afin de permettre le bon fonctionnement de ces applications. De plus, le pare-feu peut

suivre et gérer les sessions TCP établies, ce qui permet d'appliquer des règles de sécurité plus granulaires et de détecter certaines attaques.

- **Règle UDP (User Datagram Protocol)** Le protocole UDP est un protocole sans connexion, principalement utilisé par les applications en temps réel comme les jeux en ligne, la VoIP et la diffusion multimédia. Les règles UDP doivent autoriser le trafic UDP entrant et sortant afin de prendre en charge ces applications sensibles aux délais. De plus, de nombreux services réseau e Remerciements Avant d'entrer dans le vif du sujet, nous tenons à exprimer notre profonde gra- titude à toutes les personnes qui ont contribué à la réalisation de ce mémoire. Nous remercions tout particulièrement notre superviseur, M.Bellahsene, pour son encadrement, ses conseils avisés et son soutien constant tout au long de ce travail. Ses suggestions précieuses et ses encouragements ont grandement contri- bué à la qualité de ce travail. Sans oublier M. Latreche pour son accompagnement. Nous tenons également à remercier notre tuteur de stage, M.Imloul, pour son accompagnement attentif, et sa disponibilité tout au long de notre expérience en entreprise. Son expertise nous a été d'une aide précieuse dans la réalisation de ce mémoire. Nous adressons nos remerciements sincères à l'ensemble des membres du jury pour avoir accepté d'évaluer ce mémoire. Nous sommes reconnaissantes envers nos professeurs et collègues du département ATE pour leur soutien et leurs encouragements durant toute la durée de nos études. Nous voudrions aussi exprimer notre gratitude à toutes les personnes qui ont participé à ce travail, notamment M.Djebarri, pour ses précieux conseils. Nous tenons à exprimer notre gratitude particulière envers nos familles pour leur soutien inconditionnel et leurs encouragements tout au long de cette aven- 1 FIGURE E.5 – Paramètres d'associations de sécurité. Le temps de négociation du tunnel sera gardé par défaut. FIGURE E.6 – Temps de négociation du tunnel. Les deux phases sont donc configurées, il ne reste plus qu'à rajouter une règle de pare-feu pour le protocole IPsec au niveau de nos pare-feux pour autoriser le trafic au niveau du tunnel VPN. FIGURE E.7 – Autorisation du trafic IPsec. E.2 VPN client-à-site Pour la configuration du VPN client-à-site, il faudrait créer une autorité de certification interne sur le pfSense TEXTER, puis créer un certificat dédié au ser- veur qui servira pour sécuriser notre tunnel VPN. il faudrait suivre les étapes qui suivent : 121 ssentiels, comme les serveurs DNS, utilisent le protocole UDP, rendant ainsi les règles UDP cruciales pour le bon fonctionnement du réseau.

- **Linux Containers :** LXC est une technologie de virtualisation légère qui ne nécessite pas d'émulation du matériel. Au lieu de cela, elle partage le même noyau de système d'exploitation que l'hôte, ce qui permet une utilisation plus efficace des ressources [41]. Voir Conteneurs 2.2.1 pour plus de détails.
- **Kernel-based Virtual Machine :** KVM est une technologie de virtualisation complète open source pour Linux. Contrairement à LXC, KVM offre une virtualisation matérielle complète, permettant de créer et de gérer des machines virtuelles exécutant des systèmes d'exploitation complets.
- **Logical Volume Manager :** LVM (ou gestionnaire de volumes logiques en français) permet de créer et de gérer des volumes logiques sous Linux. Les volumes logiques remplacent en quelque sorte le partitionnement traditionnel des disques, offrant un système beaucoup plus flexible. Par exemple, il est possible de réduire la taille d'un système de fichiers pour en augmenter un autre sans se soucier de leur emplacement sur le disque. LVM permet notamment de redimensionner les partitions sans nécessiter de reformatage et de rajouter des disques à la volée [40].
- **Zettabyte File System :** ZFS et un gestionnaire de volumes logiques et un système de fichiers open source conçu pour fournir un stockage haute capacité avec des fonctionnalités importantes, telles que la protection, la compression et la réplication 2 de données. [5].
- **Corosync Cluster Engine :** Corosync Cluster Engine est un gestionnaire de cluster open source intégré à Proxmox utilisé pour coordonner les actions des différents noeuds du cluster. Il utilise également un système de quorum pour garantir la prise de décision cohérente en cas de défaillance d'un noeud et éviter les états conflictuels.

Annexe E

Configuration des VPN

E.1 VPN site-à-site

Pour établir un tunnel vpn site-à-site, deux phases doivent être configurées :

1. **Phase 1 :** La phase 1 du VPN établit une connexion sécurisée entre les extrémités du tunnel en négociant les paramètres de sécurité et en authentifiant mutuellement les parties. Elle crée un canal sécurisé pour la communication.
2. **Phase 2 :** Cette phase traite le trafic à travers le tunnel, définissant les sous-réseaux encapsulés, les algorithmes de chiffrement, de hachage, et les clés utilisées, ainsi que la durée de vie et le renouvellement des clés, permettant l'utilisation de multiples sous-réseaux dans un seul tunnel.

- **Configuration de la phase 1 :** La configuation débute en mettant une description ainsi que l'adresse IP de l'interface WAN menant vers le site TEXTER, tout en choisissant la version la plus récente du protocole IKE (Internet Key Exchange) qui sert à négocier les paramètres de sécurité entre les deux parties pour établir un canal sécurisé.

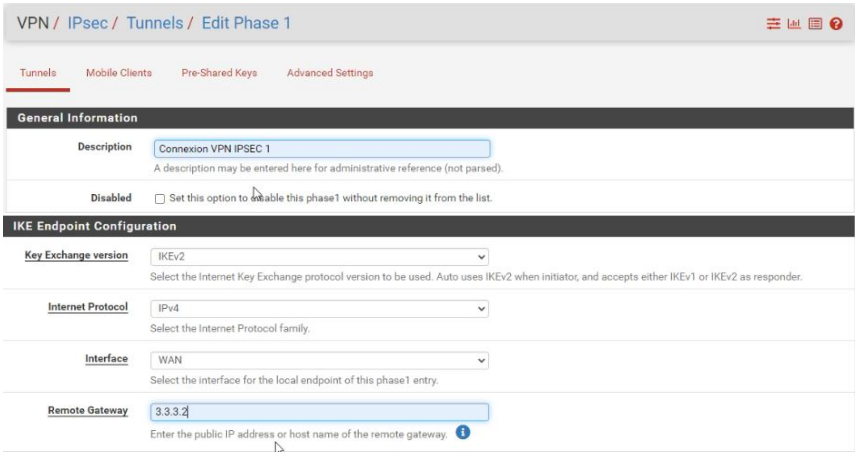


FIGURE E.1 – Insertion de l'adresse IP de l'interface WAN vers TEXTER.

Dans cette étape, il faudrait choisir la méthode d'authentification des deux pairs. PSK (Pre-Shared Key) est une méthode d'authentification par clé pré-partagée.

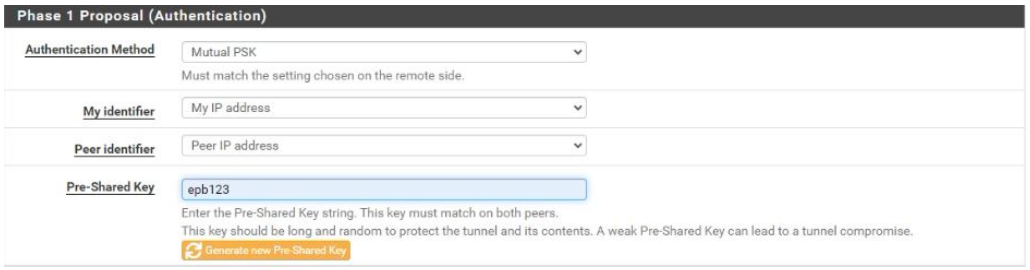


FIGURE E.2 – Méthode d'authentification.

Enfin, il faudrait finir par choisir quel algorithme de chiffrement sera utilisé à travers le tunnel VPN. Pour bénéficier d'un bon niveau de chiffrement, il est recommandé d'utiliser l'AES (Advanced Encryption Standard) avec une longueur de 256 bits. La fonction de hachage SHA256 (Secure Hash Algorithm 256) sera gardée par défaut, et la valeur du groupe Diffie-Hellman (DH group), utilisé pour l'échange de clés, sera fixée à 2 pour avoir un bon équilibre entre sécurité et débit. Quant à la fréquence de renouvellement de la connexion, sa valeur sera gardée par défaut.

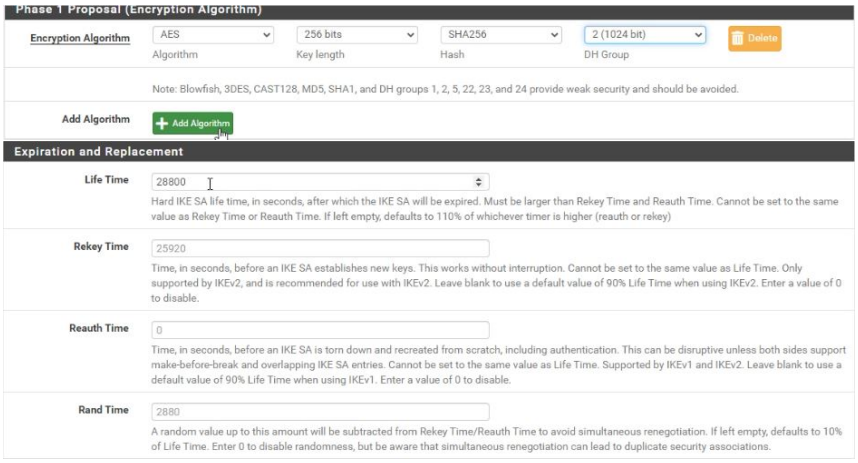


FIGURE E.3 – Algorithmes de chiffrement.

- **Configuration de la phase 2 :** Pour initier la phase 2 liée à la phase 1, il est possible d'insérer une nouvelle fois une description pour celle-ci. Par la suite, il faudrait préciser le réseau-local joignable par l'hôte distant sur ce VPN IPsec. Dans notre cas, il a été choisi de mettre le VLAN management (VLAN 60) ainsi que l'adresse réseau du site distant sur la partie **Remote Network**.

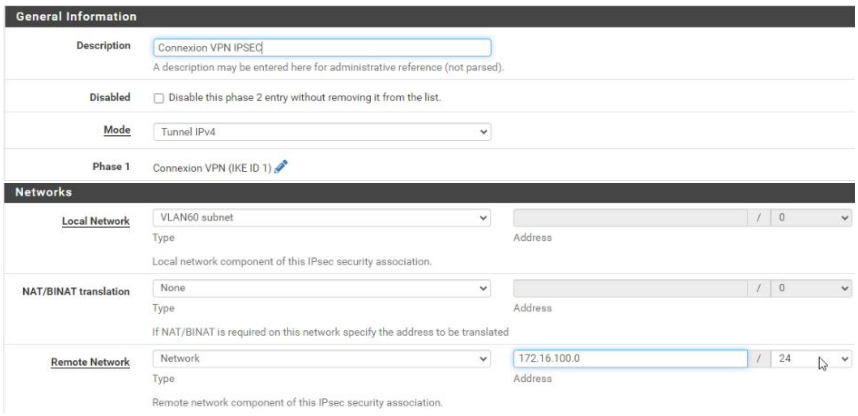


FIGURE E.4 – Configuration réseau de la phase 2.

Dans la section **Protocol** le protocole ESP (Encapsulating Security Payload) à été sélectionné. Ce dernier permet de chiffrer l'intégralité des paquets échangés, garantissant ainsi l'authentification, l'intégrité et la confidentialité. Quant aux reste des paramètres, ils seront configuréss de la même manière que pour la phase 1.

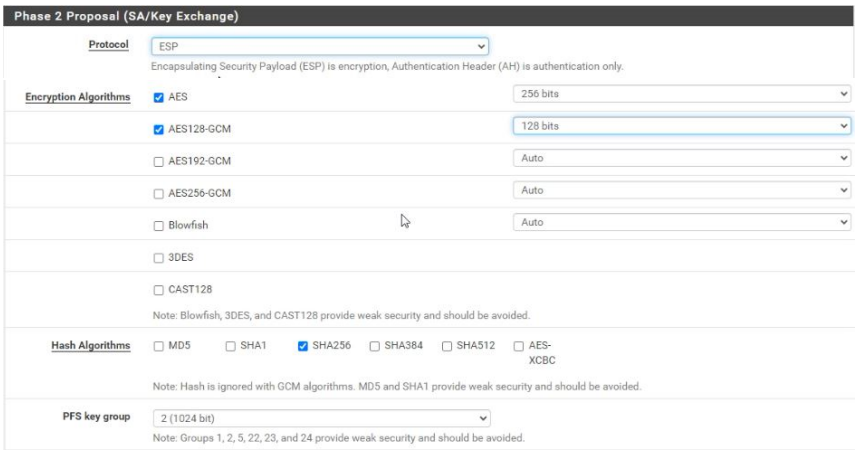


FIGURE E.5 – Paramètres d'associations de sécurité.

Le temps de négociation du tunnel sera gardé par défaut.

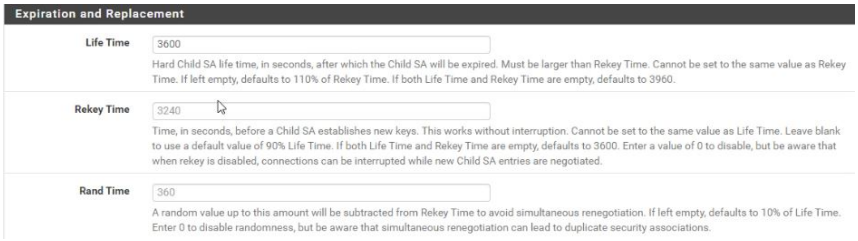


FIGURE E.6 – Temps de négociation du tunnel.

Les deux phases sont donc configurées, il ne reste plus qu'à rajouter une règle de pare-feu pour le protocole IPsec au niveau de nos pare-feux pour autoriser le trafic au niveau du tunnel VPN.

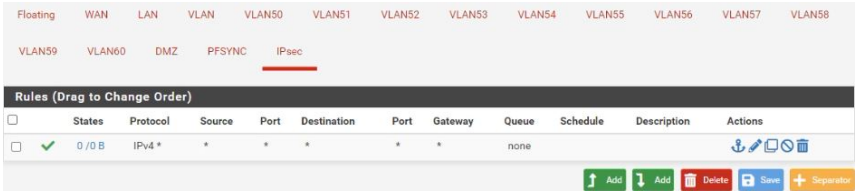
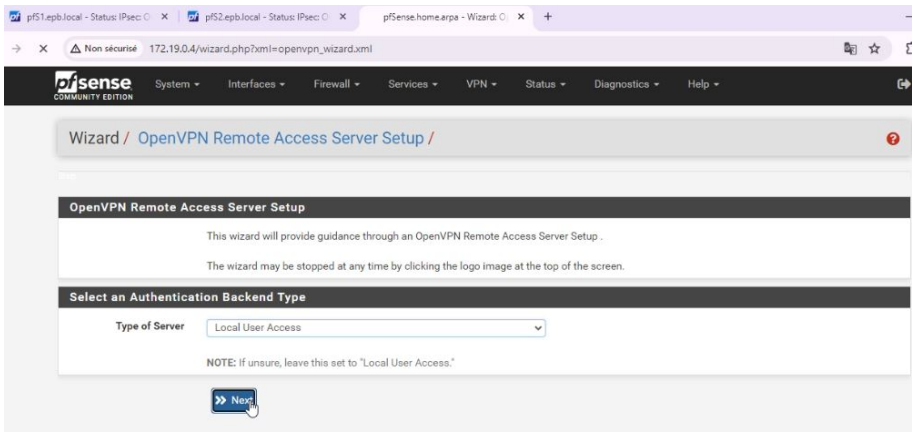


FIGURE E.7 – Autorisation du trafic IPsec.

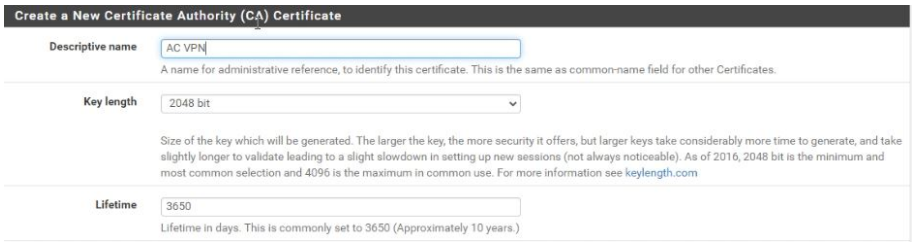
E.2 VPN client-à-site

Pour la configuration du VPN client-à-site, il faudrait créer une autorité de certification interne sur le pfSense TEXTER, puis créer un certificat dédié au serveur qui servira pour sécuriser notre tunnel VPN. il faudrait suivre les étapes qui suivent :

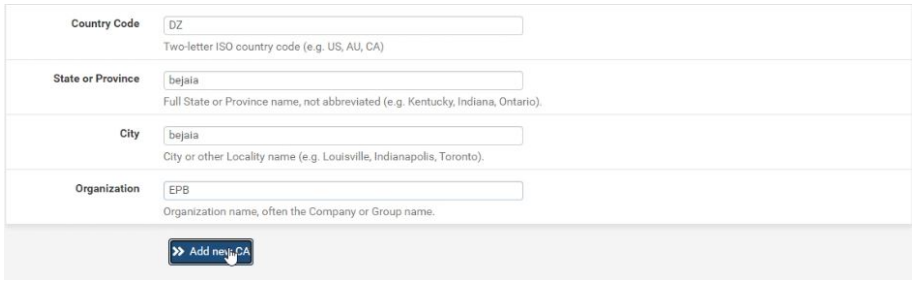
1. **Création de l'autorité de certification :** Pour créer une autorité de certification, il est essentiel de préciser où l'on souhaite retrouver la base de donnée, les détails de la région géographique ainsi que la longueur et la durée de validité la clé qui sera échangée tout en lui attribuant un nom significatif.



(a) Définition de la base de données en local.



(b) Nom de la CA, longueur et durée de vie de la clé.



(c) Sélection des détails de la région et de l'organisation.

FIGURE E.8 – Création d'une autorité de certification.

2. **Création du certificat pour le serveur VPN :** Tout comme pour la création de l'autorité de certification, il est nécessaire de préciser les mêmes paramètres que dans les figures E.8b et E.8c.

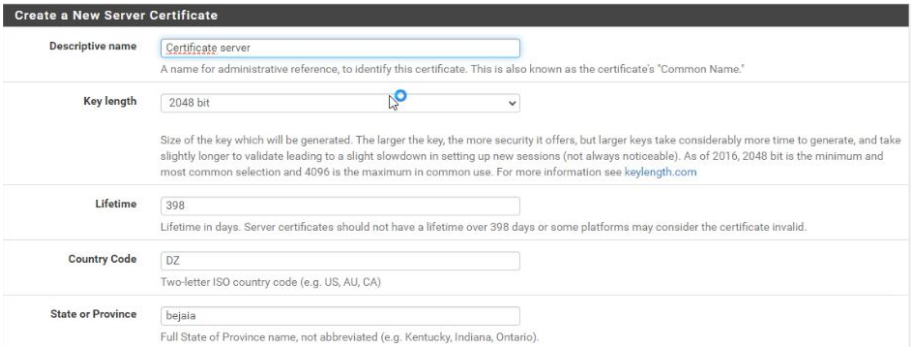


FIGURE E.9 – Nom du certificat pour le serveur et paramètres par défaut.

L'interface concernée par le tunnel pour bénéficier de l'accès distant est l'interface WAN. En ce qui concerne le protocole, le VPN repose sur l'UDP avec le port 1194 par défaut.

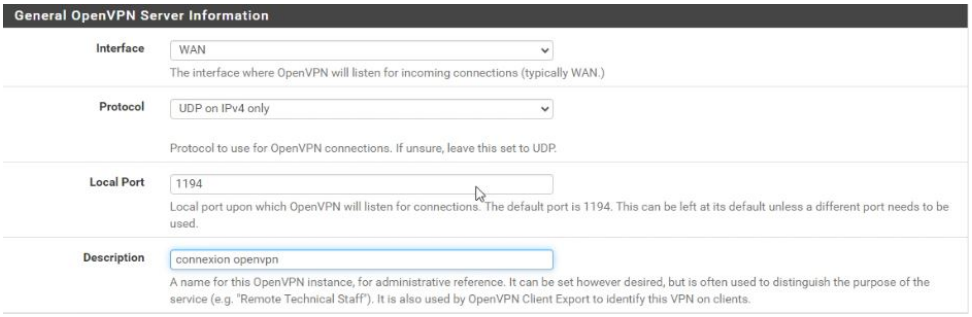


FIGURE E.10 – Informations du serveur.

Dans la section de chiffrement, nous cochons l'authentification TLS (Transport Layer Security) pour valider l'identité des pairs et la génération automatique des clés robustes pour chaque instance VPN.
Concernant les paramètres DH qui garantissent que seules les parties autorisées peuvent accéder aux données échangées, la valeur de leur longueur sera gardée par défaut et l'option de négociation de chiffrement sera activée pour assurer que les données soient chiffrées convenablement, en utilisant un algorithme de chiffrement supporté à la fois par le client et le serveur.

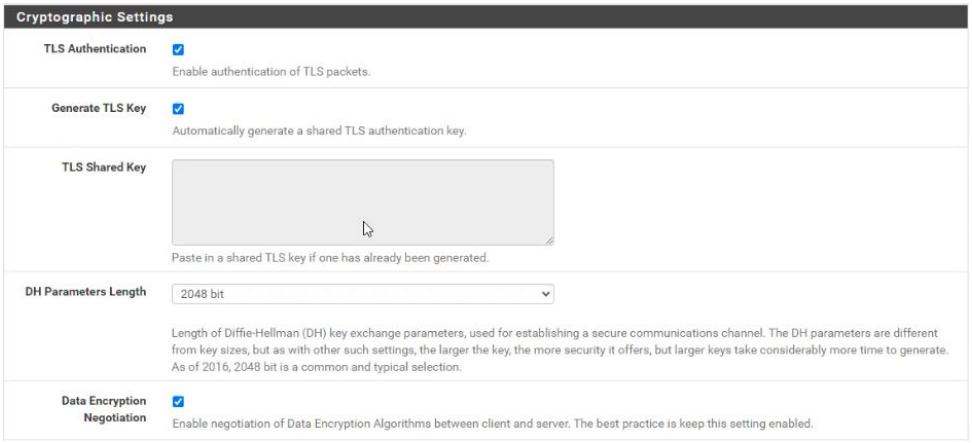


FIGURE E.11 – Paramètres de chiffrement.

Pour la configuration du tunnel VPN, il suffit de mettre l'adresse IP du réseau VPN ainsi que l'adresse réseau du réseau LAN que nous souhaitons rendre accessible via ce tunnel.

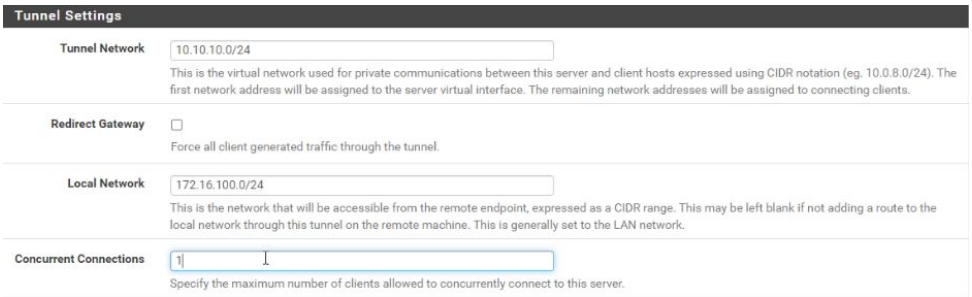
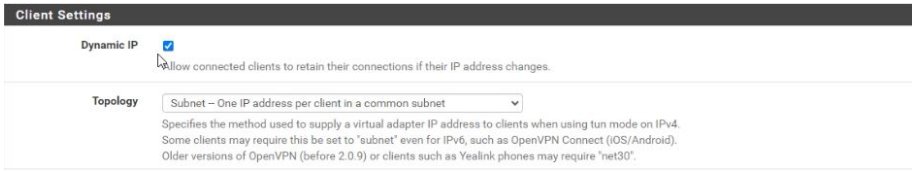


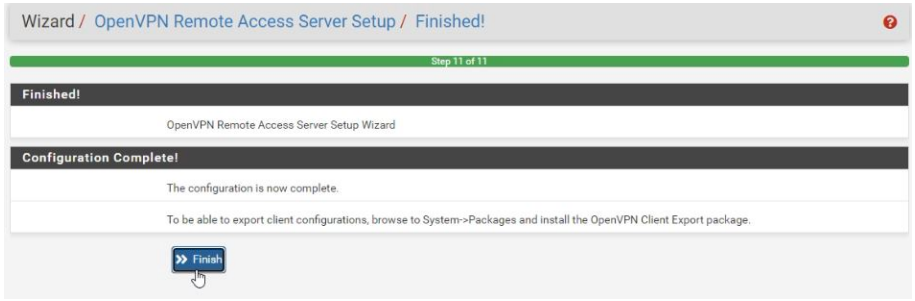
FIGURE E.12 – Adresse réseau du tunnel et du réseau local.

Dans les paramètres clients, il est recommandé de cocher l'option **Dynamic IP**, cela permettra à un client de maintenir sa connexion VPN si son adresse IP publique change. Il est également essentiel d'autoriser le trafic provenant des clients vers le serveur VPN ainsi que le trafic des clients à travers le tunnel.



(a) Activation de l'attribution des adresses dynamiques.

(b) Autorisation du trafic des clients vers le serveur et du trafic client à travers le tunnel.



(c) Fin de la création.

FIGURE E.13 – Finalisation de la configuration du serveur VPN et de son certificat.

Annexe F

Règles de filtrage du pare-feu Proxmox

Dans Proxmox VE, le pare-feu virtuelle fonctionne selon une hiérarchie à trois zones :

1. **Pare-feu du centre de données :** Les règles de cette zone définissent le trafic vers et depuis tous les hôtes et invités [4].
2. **Pare-feu de l'hôte ou noeud :** Les règles de ce niveau définissent le flux de trafic entrant et sortant d'un cluster et de ses nœuds [4].
3. **Pare-feu de la VM ou conteneur :** Les règles de cette zone déterminent comment le trafic entre et sort de chaque machine virtuelle ou conteneur [4].

Les paquets sont évaluées dans cette ordre là. Cette division en zones permet une gestion granulaire ; c'est à dire qu'on à la capacité de définir des règles de manière très détaillée et spécifique comme la définition de règles applicables à des sous-ensembles spécifiques de données ou d'utilisateurs.

Dans **Centre de données > Pare feu > Options**, le pare-feu est désactivé par défaut comme le montre la figure F.1. Si on l'active sans configurer notre première règle, on perdera l'accès à l'interface graphique car la **Politique d'entrée** est en mode **DROP** (signifie que toutes les connexions entrantes sont bloquées par défaut).

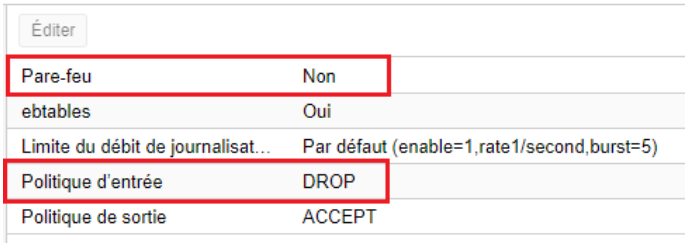


FIGURE F.1 – Pare-feu Proxmox VE désactivé.

La toute première règle à établir se fait dans la première zone ; On autorise le trafic **in** (Entrant) depuis le port **8006** à travers l'interface de management **vmbr0** et le protocole doit être **TCP** car l'accès se fait via **HTTP** (Figure F.2).

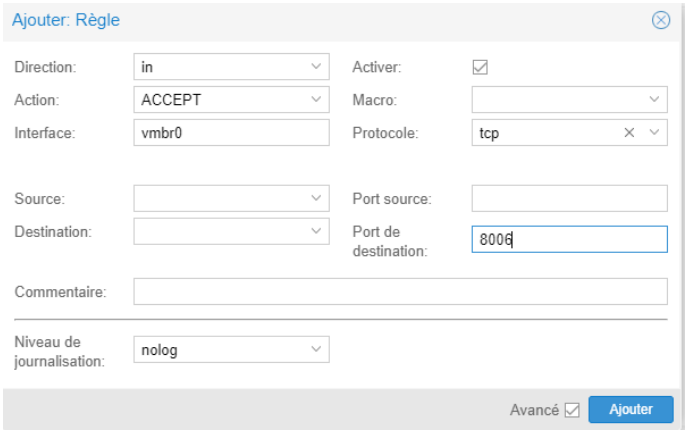


FIGURE F.2 – Établissement de la première règle de pare-feu.

Il est à présent possible d'activer le pare-feu du centre de données (Figure F.3).

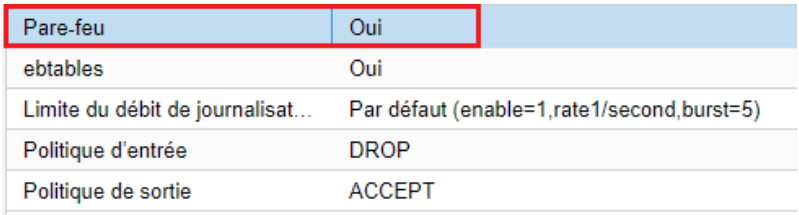


FIGURE F.3 – Activation pare-feu Proxmox VE.

Nous testons la connectivité vers le noeud pve1 (Figure F.4).

```
C:\Users\DELL>ping 172.16.59.10

Envoi d'une requête 'Ping'  172.16.59.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 172.16.59.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

FIGURE F.4 – Activation pare-feu Proxmox VE.

Cette fois il faut mettre en place des règles de firewall dans la zone deux ; Dans **pve1 > Pare-feu**, on configue comme la figure F.5 en indiquant l'adresse **Source** du pc administrateur et répète cette étape pour le restes des nodes du cluster.

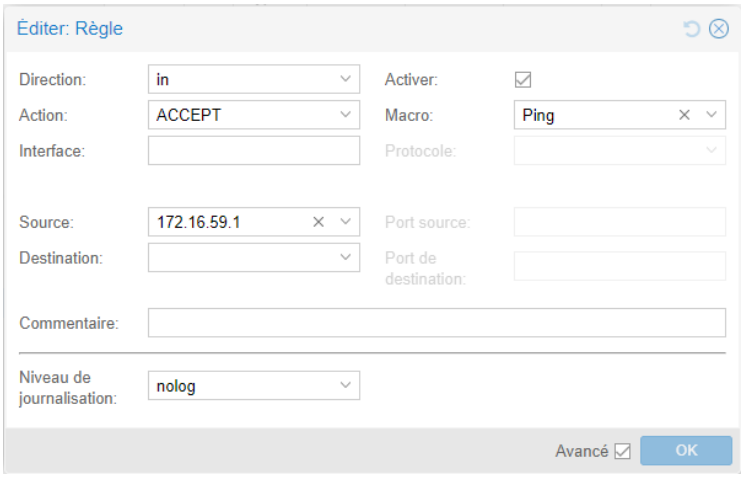


FIGURE F.5 – Règle de pare-feu pve1.

Nous faisons le test à nouveau. (Figure F.6).

```
C:\Users\DELL>ping 172.16.59.10

Envoi d'une requête 'Ping'  172.16.59.10 avec 32 octets de données :
Réponse de 172.16.59.10 : octets=32 temps<1ms TTL=64
Réponse de 172.16.59.10 : octets=32 temps<1ms TTL=64
Réponse de 172.16.59.10 : octets=32 temps<1ms TTL=64
Réponse de 172.16.59.10 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.16.59.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

FIGURE F.6 – Établissement de la connectivité entre pve1 et le pc administrateur.

La dernière étape sécuriser la machine virtuelle test avec le pare-feu de la troisième zone et autorise les requêtes Ping entrantes, en suivant les mêmes paramètres, sont effectuées dans pve1 (Voir figure F.5).

Bibliographie

[1] *106 System Design Patterns for Interview Preparation*. (visité le 05/04/2024). Mostafa Gamil, 2023. URL : https://www.google.dz/books/edition/106_System_Design_Patterns_for_Interview/pbOpEAAAQBAJ?hl=fr&gbpv=0.

[4] Wasim AHMED. *Mastering Proxmox*. en. (visité le 20/05/2024). Packt Publishing, mai 2016. ISBN : 978-1-78588-950-9.

[5] Wasim AHMED. *Proxmox Cookbook*. en. (visité le 27/05/2024). Packt Publishing, 2015. ISBN : 978-1-78398-090-1.

[8] *Blueprints for High Availability : Designing Resilient Distributed Systems*. 2003.

[9] R. BOTWRIGHT. *TCP/IP : Network+ Protocols And Campus LAN Switching Fundamentals*. (visité le 30/03/2024). Rob Botwright, 2024. ISBN : 978-1-83938-664-0. URL : https://books.google.dz/books?id=DurxEAAAQBAJ.

[10] Simon M. C. CHENG. *Proxmox High Availability*. en. (visité le 27/05/2024). Packt Publishing Ltd, oct. 2014. ISBN : 978-1-78398-089-5.

[14] Oracle CORPORATION. *Oracle Database High Availability Overview 12c Release 2*. (visité le 20/03/2024). URL : https://docs.oracle.com/en/database/oracle/oracle-database/12.2/high-availability.html.

[16] DR.V.KUMARESAN et al. *VIRTUALIZATION FOR SERVER, NETWORK, STORAGE & TOOLS*. en. (visité le 28/04/2024). SK Research Group of Companies, jan. 2024. ISBN : 978-81-19-98044-4.

[17] Anastasiia DUDNIK. *Creating a high-availability cluster with two physical servers and virtual machines*. 2017. URL : https://www.theseus.fi/handle/10024/127326.

[18] D.G. DUTT. *Cloud Native Data Center Networking : Architecture, Protocols, and Tools*. (visité le 23/03/2024). O'Reilly Media, 2019. ISBN : 978-1-4920-4557-1. URL : https://books.google.dz/books?id=79i_DwAAQBAJ.

[21] E. HAQUE. *The Ultimate Modern Guide To The Internet Of Things (IoT) : From Connecting Devices to Human Value Creation*. Lulu Press, Incorporated, 2022. ISBN : 978-1-4478-0525-0. URL : https://books.google.dz/books?id=MX-0EAAAQBAJ.

[22] *How To Do Virtualization : Your Step By Step Guide To Virtualization*. (visité le 27/03/2024). Hot Methods, 2011. ISBN : 978-1-64758-971-4. URL : https://books.google.dz/books?id=GGTcDwAAQBAJ.

[24] IBM. *High Availability and Disaster Recovery Configurations for IBM SmartCloud Control Desk and IBM Maximo Products*. IBM Redbooks.

[25] IBM. *High Availability and Disaster Recovery Configurations for IBM SmartCloud Control Desk and IBM Maximo Products*. (visité le 20/04/2024). IBM Redbooks. URL : https://www.redbooks.ibm.com/.

[26] Palash IJARI. *Comparison between Cisco ACI and VMWARE NSX*. T. 19. Fév. 2017, p. 70-72. DOI : 10.9790/0661-1901047072.

[30] Ekaterina KALOSHINA. *Proxmox HA virtualization cluster | Bachelor's thesis | Information Technologies*.

[31] Vincent KHERBACHE, Fabien HERMENIER et Eric MADELAINE. *Ordonnancement contrôlé de migrations à chaud*. (visité le 17/04/2024). Juill. 2015. DOI : 10.13140/RG.2.1.5100.2649.

[32] R. KHONDOKER. *SDN and NFV Security : Security Analysis of Software-Defined Networking and Network Function Virtualization*. Lecture Notes in Networks and Systems. (visité le 21/03/2024. Springer International Publishing, 2018. ISBN : 978-3-319-71761-6. URL : https://books.google.dz/books?id=vK9JDwAAQBAJ.

[33] D. KUSNETZKY. *Virtualization : A Manager's Guide*. Real Time Bks. (visité le 31/03/2024). O'Reilly Media, Incorporated, 2011. ISBN : 978-1-4493-0645-8. URL : https://books.google.dz/books?id=dV_L5CbsDscC.

[39] Cybellium LTD. *Mastering Backup and restore*. en. (visité le 05/04/2024). Cybellium Ltd, sept. 2023.

[42] E. MAILLÉ. *VMware vSphere 4 : mise en place d'une infrastructure virtuelle*. Expert IT. Editions ENI, 2010. ISBN : 978-2-7460-5287-1. URL : https://books.google.dz/books?id=F8zBB96KOLYC.

[45] G.K. NUTI. *CompTIA Cloud+ Certification Guide (Exam CV0-003) : Everything you need to know to pass the CompTIA Cloud+ CV0-003 exam (English Edition)*. Bpb Publications, 2023. ISBN : 978-93-5551-384-7. URL : https://books.google.dz/books?id=pFTJEAAAQBAJ.

[48] L. PARZIALE et al. *The Virtualization Cookbook for IBM Z Volume 2 : Red Hat Enterprise Linux 8.2*. (visité le 24/03/2024). IBM Redbooks, 2021. ISBN : 978-0-7384-6006-2. URL : https://books.google.dz/books?id=FqBIEAAAQBAJ.

[50] M. PORTNOY. *Virtualization Essentials*. (visité le 24/03/2024). Wiley, 2023. ISBN : 978-1-394-18157-5. URL : https://books.google.dz/books?id=_xi3EAAAQBAJ.

[52] Guy PUJOLLE. *Réseaux logiciels : Du Cloud Networking à la 5G - 2e édition revue et augmentée*. fr. (visité le 23/03/2024). ISTE Group, juin 2020. ISBN : 978-1-78405-686-5.

[54] K.S. SAHOO et al. *SDN-Supported Edge-Cloud Interplay for Next Generation Internet of Things*. Chapman & Hall/CRC Internet of Things. (visité le 21/03/2024). CRC Press, 2022. ISBN : 978-1-00-081483-5. URL : https://books.google.dz/books?id=K5yaEAAAQBAJ.

[55] Mrs Lavanya SELVARAJ et al. *Building Cloud and Virtualization Infrastructure : A Hands-on Approach to Virtualization and Implementation of a Private Cloud Using Real-time Use-cases (English Edition)*. en. (visité le 27/03/2024). BPB Publications, sept. 2021. ISBN : 978-93-90684-47-2.

[63] Peter S. WEYGANT. *Cluster for High Availability - A Prime for HP Solutions - Second Edition*. Prentice Hall PTR.

[65] Yimeng ZHAO. *Software switch deployment in SDN-enabled network virtualization environment*. en. Mai 2016. URL : https://pastel.hal.science/tel-03752344 (visité le 20/04/2024).

[66] Nur ZINCIR-HEYWOOD, Marco MELLIA et Yixin DIAO. *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning*. en. (visité le 23/03/2024). John Wiley & Sons, oct. 2021. ISBN : 978-1-119-67550-1.

Webographie

[2] *Accueil - Entreprise Portuaire de Bejaia*. fr-FR. URL : https://www.portdebejaia.dz/ (visité le 04/06/2024).

[3] *Add Proxmox icon · Issue #337 · andOTP/andOTP*. en. URL : https://github.com/andOTP/andOTP/issues/337 (visité le 18/05/2024).

[6] AMAZONAWS. *Qu'est-ce que la répartition de charge ?* (visité le 29/03/2024). URL : https://aws.amazon.com/fr/what-is/load-balancing/.

[7] APPMASTER. *qu'est-ce que la haute disponibilite ?* (visité le 23/03/2024). URL : https://appmaster.io/fr/blog/quest-ce-que-la-haute-disponibilite.

[11] *Commutateur - Cisco Catalyst 2960*. fr-FR. URL : https://www.cisco.com/web/FR/documents/pdfs/datasheet/switching/Catalyst2960.pdf (visité le 04/06/2024).

[12] *Comprendre le protocole VTP (VLAN Trunk Protocol)*. fr. URL : https://www.cisco.com/c/fr_ca/support/docs/lan-switching/vtp/10558-21.html (visité le 09/05/2024).

[13] *Configurer les paramètres du protocole STP sur un commutateur par l'interface de ligne de commande (CLI) - Cisco*. URL : https://www.cisco.com/c/fr_ca/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html (visité le 15/06/2024).

[15] *Cybersecurity - Le royaume des cinq neuf*. (visité le 04/04/2024). URL : https://community.cisco.com/t5/blogues-de-s%C3%A9curit%C3%A9/cybersecurity-le-royaume-des-cinq-neuf/ba-p/4668985.

[19] *En savoir plus sur le projet pfSense*. URL : https://www.pfsense.org/about-pfsense/ (visité le 07/05/2024).

[20] Jeremy GROSSMANN. *Español : Logo de GNS3English : GNS3 logo*. Août 2014. URL : https://commons.wikimedia.org/wiki/File:GNS3_logo.png (visité le 25/05/2024).

[23] IBM. *Haute disponibilité*. (visité le 09/03/2024). URL : https://www.ibm.com/docs/fr/i/7.3topic=availability-high.

[27] *Infrastructure axée sur les applications (ACI) - Cisco Application Centric Infrastructure Solution Overview - Cisco*. URL : https://www.cisco.com/c/fr_fr/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html (visité le 01/05/2024).

[28] *Installation et mise à niveau — Effectuer l'installation — Procédure d'installation pas à pas — ZFS | Documentation pfSense*. URL : https://docs.netgate.com/pfsense/en/latest/install/install-zfs.html (visité le 24/05/2024).

[29] JSCAPE. (visité le 14/04/2024). URL : https://www.jscape.com/blog/active-active-vs-active-passive-high-availability-cluster.

[34] *La virtualisation avec VMware vSphere 8 - Comprendre les hyperviseurs*. URL : https://www.editions-eni.fr/livre/la-virtualisation-avec-vmware-vsphere-8-notions-fondamentales-9782409041877/comprendre-les-hyperviseurs (visité le 20/04/2024).

[35] *La virtualisation des fonctions réseau, qu'est-ce que c'est ?* fr. URL : https://www.redhat.com/fr/topics/virtualization/what-is-nfv (visité le 05/06/2024).

[36] *LAN Switching - Configuring Private VLANs [Support]*. en. URL : http://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/pvlans.html (visité le 09/05/2024).

[37] *Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces*. en. URL : https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html (visité le 25/06/2024).

[38] *Linux on IBM Systems*. fr. Nov. 2023. URL : https://www.ibm.com/docs/en/linux-on-systems?topic=choices-using-linux-bridge (visité le 01/05/2024).

[40] *lvm [Wiki ubuntu-fr]*. URL : https://doc.ubuntu-fr.org/lvm (visité le 05/06/2024).

[41] *LXC containers*. en. URL : https://ubuntu.com/server/docs/lxc-containers (visité le 12/06/2024).

[43] *Migration à froid*. fr. URL : https://docs.vmware.com/fr/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-98C18721-A4B0-4BD2-96BF-1BBC29391B3E.html (visité le 17/04/2024).

[44] *Network Address Translation Definition | How NAT Works | Computer Networks*. en. URL : https://www.comptia.org/content/guides/what-is-network-address-translation (visité le 05/06/2024).

[46] *Open vSwitch*. URL : https://www.openvswitch.org/ (visité le 01/05/2024).

[47] *Pacemaker*. (visité le 21/06/2024). URL : https://clusterlabs.org/pacemaker/doc/deprecated/en-US/Pacemaker/1.1/html/Clusters_from_Scratch/_what_is_emphasis_pacemaker_emphasis.html#:~:text=Pacemaker%20is%20a%20cluster%20resource,and%20driven%20by%20prescribed%20rules..

[49] *pfSense Documentation | pfSense Documentation*. URL : https://docs.netgate.com/pfsense/en/latest/index.html (visité le 07/05/2024).

[51] *PROXMOX – TUTOS-info.fr*. fr-FR. URL : https://tutos-info.fr/index.php/proxmox/ (visité le 17/05/2024).

[53] REDHAT. *What is high availability?* (visité le 23/03/2024). URL : https://www.redhat.com/en/topics/linux/what-is-high-availability.

[56] Satish SHETHI. *10 New Things in Windows Server 2022 to Know*. en-US. Nov. 2021. URL : https://geekflare.com/new-features-in-windows-server-2022/ (visité le 22/05/2024).

[57] STONEFLY. (visité le 13/04/2024). URL : https://stonefly.com/blog/mirroring-vs-replication-vs-clustering-comparison/.

[58] STONEFLY. (visité le 21/06/2024). URL : https://stonefly.com/blog/backup-vs-replication-whats-the-difference/.

[60] *Type de virtualisation : définition et avantage de chaque type*. URL : https://www.appvizer.fr/magazine/services-informatiques/virtualisation/type-virtualisation (visité le 25/03/2024).

[61] *Un hyperviseur, qu'est-ce que c'est ?* fr. URL : https://www.redhat.com/fr/topics/virtualization/what-is-a-hypervisor (visité le 06/05/2024).

[62] *Virtualisation avec VirtualBox - Ian's Web Page*. URL : https://www.morere.eu/spip.php?article122#outil_sommaire_3 (visité le 26/05/2024).

[64] *Windows Server 2022 | Centre d'évaluation Microsoft*. fr-FR. URL : https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022 (visité le 07/05/2024).

Résumé

Dans le monde actuel, la disponibilité des systèmes et réseaux est devenue une exigence du fait qu'ils occupent une place importante dans les entreprises modernes. La virtualisation a rendu ces Infrastructures plus faciles à gérer et l'introduction de nouvelles technologies de haute disponibilité et clustering ont amélioré leur résilience et leur efficacité.

La présente étude vise à améliorer la disponibilité des services de l'entreprise portuaire de Bejaia, et à prévenir les temps d'arrêts, en mettant en place des mécanismes de haute disponibilité et clustering en environnement virtuel.

Dans la partie configuration et simulation de ce projet, nous aurons recours à des outils, tels que l'hyperviseur Proxmox VE, l'émulateur GNS3, le pare-feu pfSense et le serveur Windows 2022, dans le but de concevoir une architecture pour l'EPB qui soit fiable et résiliente.

Mots clés : Virtualisation, systèmes, réseaux, haute disponibilité, clustering, résilience, temps d'arrêt, hyperviseur Proxmox VE, GNS3, pfSense, serveur Windows 2022, EPB.

Abstract

In today's world, the availability of systems and networks has become a requirement because of modern businesses. Virtualisation has made these Infrastructures easier to manage and the introduction of new high availability and clustering technologies have improved their resilience and efficiency.

The aim of this study is to improve the availability of services at the Bejaia port company. and prevent downtime, by implementing high availability and clustering mechanisms in a virtual environment.

In the configuration and simulation part of this project, we will be using tools such as the Proxmox VE hypervisor, the GNS3 emulator, the pfSense firewall and the Windows 2022 server, with the aim of designing a reliable and resilient architecture for the EPB.

Key words : Virtualisation, systems, networks, high availability, clustering, resilience, downtime, Proxmox VE hypervisor, GNS3, pfSense, Windows Server 2022, EPB.