République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme Master en Informatiques

Option :
Administration et sécurité des réseaux informatique

Thème

La mise en place d'un cluster haute disponibilité avec équilibrage de charge

Présenté par :
M^lle *KICHOU* Kenza
M^lle *SID* Nihad

Devant le jury composé de :

Présidente	**Dr. N. Bouadem**	**MCB**	**Université de Béjaia**
Promotrice	**Dr. S. Ouyahia**	**MCB**	**Université de Béjaia**
Examinatrice	**Dr. M. Yaici**	**MCB**	**Université de Béjaia**

Année universitaire 2022/2023

- Dédicaces -

Je rends grâce a dieu de m'avoir donné´ le courage et la volonté ainsi que la conscience d'avoir pu terminer mes ´études

Je dédie ce travail

À mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bienêtre. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis toujours. Puisse Dieu, le très haut, vous accorde santé, bonheur et longue vie.

À mes chers frères Sofiane, Walid et ma chère sœur Feriel qui ont su être là au moindre besoin.

À mes chers oncles et tantes pour leur soutien tout au long de mon parcours universitaire.

À mes chers cousins et cousines, pour leurs présence tout au long de ma préparation.

À ma chère binôme et amie Nihad, ta présence est remarquable tout au long de notre parcours et notre préparation de mémoire.

A tous les professeurs et enseignants qui ont collaboré a ma formation depuis mon cycle d'étude.

Je tiens également à exprimer ma profonde gratitude à toute ma famille et tous ceux qui ont participé du pré ou du loin à la réalisation de ce travail.

KENZA.

- Dédicaces -

Je rends grâce a dieu de m'avoir donné le courage et la volonté ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce travail

À mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bienêtre. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis toujours. Puisse Dieu, le très haut, vous accorde santé, bonheur et longue vie.

À mes chers mes frères Arezki ,Lyes, Mennad et ma chère sœur Yasmina qui ont su être là au moindre besoin.

À ma grande sœur, Dehia, Qui repose désormais en paix. Tu me manques énormément, mais je sais que tu es toujours avec moi en esprit.

À mes chères copines CHAHINAZ, DOUNIA, RIMA, ,ZAHRA merci de votre présence tout au long de l'élaboration du travail.

À ma chère binôme et amie Kenza, ta présence est remarquable tout au long de notre parcours et notre préparation de mémoire.

À tous les professeurs et enseignants qui ont collaboré a ma formation depuis mon cycle d'étude.

À toutes les personnes qui ont participé du pré et du loin à la réalisation de ce travail.

NIHAD.

- Remerciements -

Nos remerciements vont à Dieu le tout puissant de nous avoir donné la force, la volonté et le courage de réaliser ce modeste travail.

Nous tenons à remercier en premier lieu notre initiatrice ***Mme YESSAD SAMIRA****, pour son encadrement, sa disponibilité, son aide, ses encouragements, ses conseils et ses orientations qui nous ont permis de mener à bien ce travail.*

Nos remerciements les plus vifs vont tout particulièrement à notre maître de stage ***Mme BOUCHANA DALILA*** *pour son encadrement et orientation avec toute rigueur tout au long de notre stage au sein de* ***SONATRACH****.*

Nous tenons également à remercier les membres du jury d'avoir consacré leurs temps à la lecture et à la correction de ce mémoire.

Nous remerciements les plus particuliers à nos parents, en qui nous avons puisé tout le courage, la volonté et la confiance, nous leur serons éternellement reconnaissants.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AD	Active Directory
ARP	Address Resolution Protocol
ASL	Administration et Social
ATR	Approvisionnement et transport
AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
BDG	Budget et contrôle de gestion
BDM	Business Development Marketing
CDN	Content Delivery Network
CIDER	Classless Inter-Domain Routing
CME	Call Manager Express
COM	Commercialisation
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Dental of Service
DRGB	Direction Régionale de Bejaia
EP	Exploitation-Production
EXG	Exploitation Gaz
EXL	Exploitation liquide
FHRP	Hop redundancy Protocols
FIN	Finances
FTP	File Transfer Protocol
GEM	Gazoduc Espagne/Maroc
GLBP	Gateway LoadBlancing Protocol
GNL	Gaz Naturel Liquéfié
GPDF	Gazoduc Tunisie/Italie
GPL	Gaz de Pétrole Liquéfié
HA	High Availability
HRM	Gazoduc Hassi R'mel
HSE	Hygiène Sécurité Environnement

HSRP	Hot Standby Router Protocol
HTIP	Home network Topology Identifying Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LQS	Liquéfaction et Séparation
MAC	Media Access Control
MAN	Metropolitan Area Network
MNT	Maintenance
MOG	Moyens généraux
NAS	Network Attached Storage
OS	Operating System
OSI	Open Systems Interconnection
PAN	Personal Area Network
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
RAID	Redundant Array of Independent Disks
RHC	Ressources Humaines et Communication
RLE	Réseau Local d'Entreprise
RP	Raffinage et Pétrochimie
RSTP	Rapid Spanning-Tree Protocol
RTC	Région Transport Centre-Bejaia
RTE	Région Transport Est-Skikda
RTH	Région Transport de Haoud-el-Hamra
RTI	Région Transport d'Inaminas
RTO	Région Transport Ouest-Arzew
SAN	Storage Area Network
SDAF	Sous-direction Administration et Finances
SDE	Sous-direction Exploitation
SDT	Sous-direction Technique
SGBD	Système de Gestion de Bases de Données
SNMP	Simple Network Management Protocol
SONATRACH	Société Nationale de Transport et de Commercialisation des Hydro- carbure
SOPEC	Société Pétrolière de Gérance.
STC	Système de Transport par Canalisation
STP	Spanning-Tree Protocol
TCPTCP/IP	Transmission Control Protocol /Internet Protocol
TELNET	Terminal Network ou Télécommunication Network

TNF	Travaux neufs
TRC	Transport Par Canalisations
UDP	User Datagram Protocol
URL	Uniform Resource Locatar
VLAN	Virtuel Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

L'influence et l'évolution de la technologie informatique ont eu un effet transformateur sur tous les aspects de la vie humaine, y compris l'impact significatif des réseaux informatiques sur nos routines quotidiennes, en particulier dans la sphère de l'entreprise. De plus, les réseaux informatiques ont été affinés pour simplifier les opérations des utilisateurs et fournir un système qui répond aux demandes des clients. Ces améliorations portent tant sur la qualité que sur la quantité des solutions proposées. Les entreprises tirent parti de techniques telles que le clustering pour améliorer leurs services et anticiper les défaillances potentielles du système. Le clustering, une technologie qui assure la haute disponibilité des ressources partagées dans un réseau informatique, est l'une de ces techniques.

Le terme "clustering" est dérivé du mot "cluster" qui signifie groupe. Cependant, dans le domaine des réseaux informatiques, un cluster est un ensemble d'ordinateurs qui sont tous interconnectés dans le but de partager des ressources informatiques. Cela va au-delà de la définition de base trouvée dans les dictionnaires.

L'une des entreprises leader dans l'utilisation d'outils informatiques puissants pour la gestion des systèmes et des services est SONATRACH à Bejaia. Notre projet de fin d'études vise à mettre en place un cluster haute disponibilité avec load balancing.

Pour mener à bon port notre étude, nous avons élaboré un plan de travail qui s'articule sur quatre chapitres, Le premier intitulé «Présentation de l'organisme d'accueil» a pour but en premier lieu de présenter la société nationale des hydrocarbures (SONATRACH) généralement et la RTC de Bejaia, son système informatique ainsi qu'une étude sur notre thème en abordant la problématique et les différentes solutions permettant de mettre en oeuvre un cluster haute disponibilité avec un équilibrage de charge. Le deuxième intitulé « Généralités sur les réseaux et la sécurité informatiques » consiste à définir brièvement quelques notions de bases sur les réseaux et la sécurité informatiques. Dans le troisième «La haute disponibilité et le clustering», nous nous concentrerons sur le concept de haute disponibilité, notre étude comprendra une analyse complète des diverses méthodologies et technologies qui ont été créées à des fins de mise en œuvre de la haute disponibilité, afin de s'assurer qu'un système ou un service est disponible en permanence.

Le dernier intitulé « Réalisation, simulation et test » est consacré à la définition des différents

outils et logiciels ayant servis à l'élaboration de notre implémentation, tout en expliquant les configurations établies ainsi que les tests.

Enfin, nous terminerons notre travail par une conclusion générale qui résumera les points accomplis dans ce travail et nos perspectives.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les différents départements qui la constituent et donner quelques informations qui nous seront utiles pour notre approche sur le domaine et le milieu où nous souhaitons travailler.

1.2 Création et évolution de la SONATRACH

L'entreprise SONATRACH est l'acronyme de « Société Nationale pour le Transport et la Commercialisation des Hydrocarbures » est une compagnie algérienne pour la recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures et de leurs dérivés.

Elle intervient également dans d'autres domaines tels que la génération électrique, les énergies nouvelles et renouvelables et le dessalement d'eau de mer. Elle exerce ses métiers en Algérie Et partout dans le monde ou des opportunités se présentent, elle emploie 120 000 personnes dans l'ensemble du groupe. La SONATRACH, créée par décret N° 63/491 du 31 décembre 1963, dispose d'un capital social de 350 milliards de Dinars entièrement et exclusivement souscrit et libéré par l'État. Son activité a débuté le 01/01/1964.

SONATRACH, avec sa stratégie d'internationalisation, opère également dans plusieurs pays du monde tels que le Mali, le Niger, la Libye, l'Egypte, l'Espagne, l'Italie, le Portugal, la Grande Bretagne, le Pérou et les USA [1].

SONATRACH, avec ses chiffres d'affaires assez importants, est classée comme suit [1] :
- 1ère compagnie en Afrique ;
- 3ème exportateur mondial de GPL ;
- 6ème Compagnie Mondiale en matière de Gaz Naturel (réserves et production) ;

• 5ème exportateur mondial de Gaz Naturel ;
• 4ème exportateur mondial de Gaz Naturel Liquéfié (GNL) ;
• 13ème Compagnie Mondiale concernant les hydrocarbures liquides (réserves et production).

1.3 Organisation et activité de la SONATRACH

SONATRACH est divisée en cinq activités, chaque activité exerce ses métiers, développe son portefeuille d'affaires et contribue dans son domaine de compétences au développement des activités internationales de la société, qui sont représentées par l'organigramme suivant [1] :

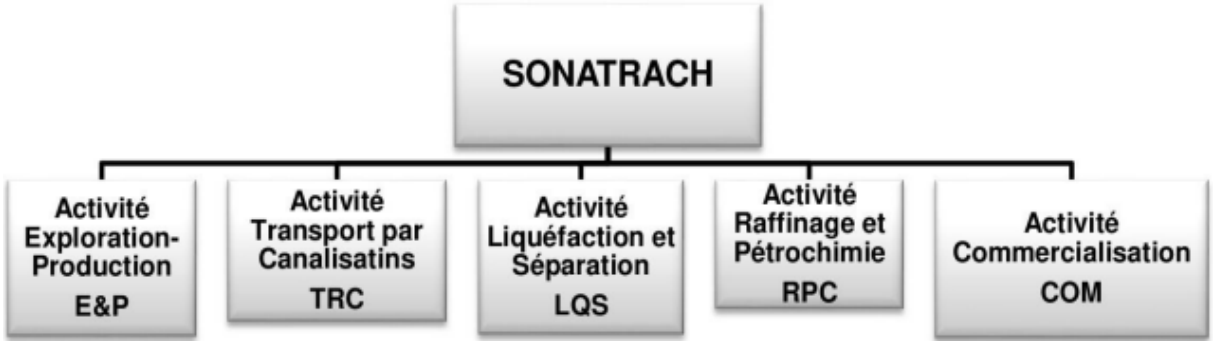

FIGURE 1.1 – Les activités de SONATRACH.
[1]

Les activités de base de SONATRACH portent sur toute la chaîne des hydrocarbures, en commençant par la recherche et l'exploration, jusqu'à la transformation des hydrocarbures et leur commercialisation aux consommateurs finaux. Il est possible de regrouper ces activités en cinq activités globales [1] :

A. L'Activité Exploration-Production (EP) : Elle s'articule autour de trois axes :
• Le développement et l'exploitation des gisements pour une valorisation optimale des ressources ;
• La gestion des activités en partenariat dans les phases d'exploration, de développement et d'exploitation des gisements ;
• La recherche, la négociation et le développement de nouveaux projets sur le territoire national et à l'international.

B. Activité Liquéfaction et Séparation (LQS) :l'activité liquéfaction et séparation s'est affirmée en tant que maillon important dans la chaine de valeur de SONATRACH s'érigeant en activité à part entière, dont sa mission principale est :
• Liquéfaction du gaz nature ;
• Séparation des GPL ;
• Optimisation de l'outil de production.

C. Activité Raffinage et Pétrochimie (RP) : L'activité raffinage et pétrochimie à pour mission essentielle l'exploitation et la gestion de l'outil de production du raffinage et de la pétrochimie, pour répondre principalement à la demande du marché national en produits pétroliers.

D. Activité Transport Par Canalisations (TRC) : Couvre plusieurs domaines :
• L'exploitation des ouvrages de transport des hydrocarbures et des installations portuaires à quai et en haute mer ;
• La maintenance des ouvrages de transport des hydrocarbures et des installations de chargement portuaires à quai et en haute mer ;
• Les études et développement, à l'exception des études relevant de la direction corporate Business Development et Marketing (BDM) et la réalisation de projets relevant de la Direction Centrale Engineering et Project Management.

SONATRACH exploite un réseau de transport par canalisation des hydrocarbures (Pétrole Brut, Condensat, Gaz Naturel et Gaz Pétrole Liquéfié) composé de 22 Systèmes de Transport par Canalisation (STC) d'une longueur totale de 20 705 km. Un STC est constitué d'une ou plusieurs canalisation(s) transportant des Hydrocarbures, y compris les installations intégrées, et les capacités de stockage liées à ces ouvrages, notamment les stations de compression, les stations de pompage, les postes de coupure, les postes de sectionnement, les lignes d'expédition, les postes de chargement à quai et en mer ainsi que les systèmes de protection cathodique, de comptage, de régulation, de télécommunications et de télé-contrôle [1].

La gestion des STC s'opère à travers six (06) Directions Régionales (RTO, RTH, RTE, RTI, RTC, HRM) et deux (02) Directions Opérationnelles (GEM et GPDF).

- Région Transport Ouest-Arzew (RTO) ;
- Région Transport de Haoud-el-Hamra(RTH) ;
- Région Transport Est-Skikda (RTE) ;
- Région Transport d'Inaminas (RTI) ;
- Région Transport Centre-Bejaia (RTC) ;
- Gazoduc Hassi R'mel (HRM) ;
- Gazoduc Espagne/Maroc (GEM) ;
- Gazoduc Tunisie/Italie (GPDF).

La branche transport par canalisations a pour mission [1] :

• La gestion et l'exploitation des ouvrages et le transport des hydrocarbures ;

• La coordination et le contrôle de l'exécution des programmes de transport arrêtent en fonction des impératifs de production et de commercialisation ;

• La maintenance, l'entretien et la protection des ouvrages et canalisation ;

• La conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations ;

• Augmenter les capacités de production et d'acheminement des hydrocarbures de près de 30% ;

• Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement.

E) Activité Commercialisation (COM)

• Commercialisation extérieure ;

• Commercialisation sur le marché intérieur ;

• Transport maritime des hydrocarbures [1].

1.4 Présentation de la Région Transport Centre (RTC)

La RTC est l'une des huit directions régionales de Transport par canalisations des hydrocarbures. Sa mission consiste en le transport, le stockage, et la livraison des hydrocarbures liquides et gazeux de la région centrale du pays via les pipelines. Elle fut fondée le 12 mars 1957 par la société Française des pétroles de gérance (SOPEG). La Région Transport Centre Bejaïa est chargée de l'exploitation de deux oléoducs et d'un gazoduc [1].

1.4.1 Situation géographique de l'organisme

La RTC de Bejaia est l'une des 5 directions régionales de la SONATRACH, qui a pour tâche le transport, le stockage et la livraison du pétrole brut et le condensât.

La RTC se situe à 2Km de la ville de Bejaia qui est devisée en deux terminaux, le terminal nord possédant 12 bacs de stockage de 35000M3, et le terminal sud avec 4 bacs de 50000M3 (Le 5éme bac est prévu). Elle comprend également un port pétrolier qui se trouve à 8Km nord de la

DRGB possédant 3 postes de chargement [1].La figure suivante montre la situation géographique de SONATRACH

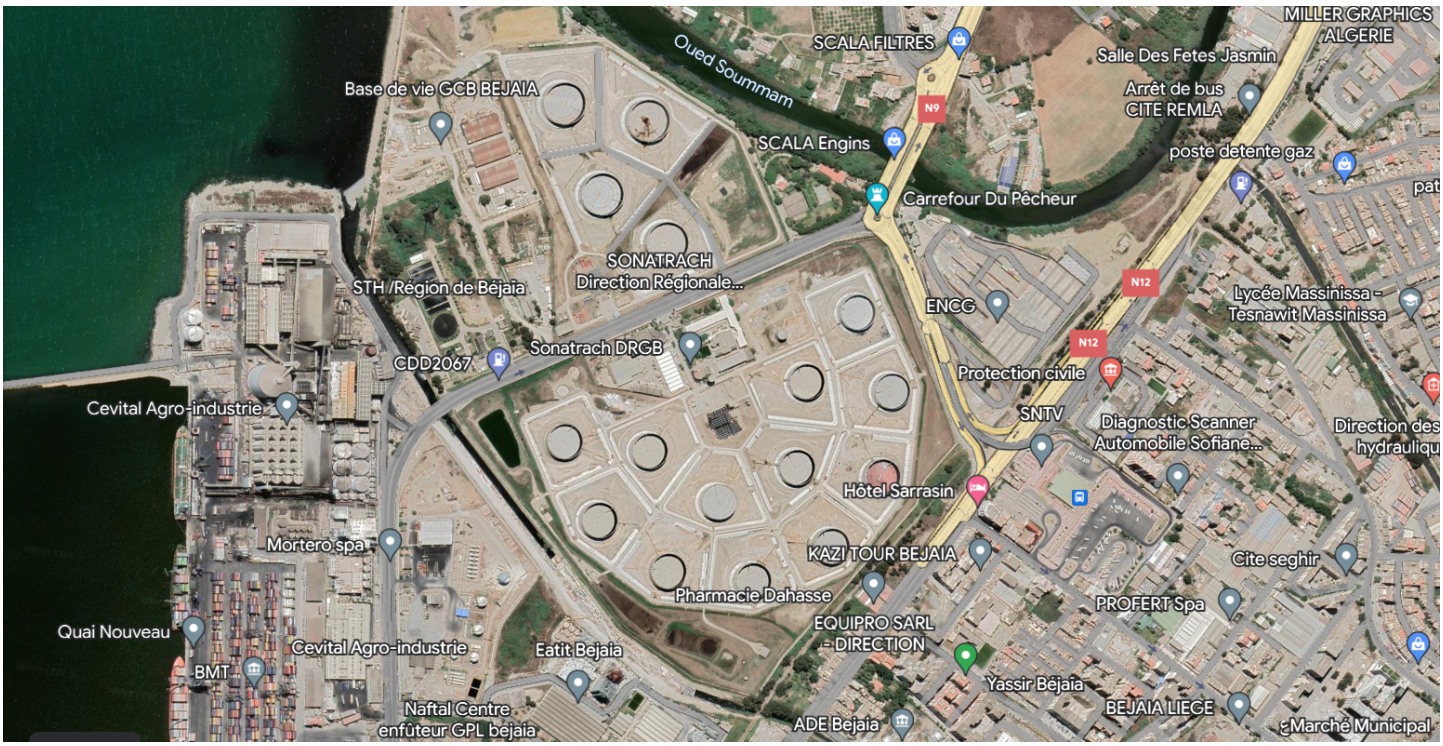

FIGURE 1.2 – vue satellitaire de SONATRACH.
[2]

1.4.2 La fiche technique

Le tableau ci-dessous représente quelques informations relatives au SONATRACH :

Dénomination	RTC (**Région Transport Centre**)
Logo	سوناطراك sonatrach
Secteur d'activités	Exploration, Production, transport et commercialisation
Siège	Arrière-port - BP 19 - 06000 Bejaïa
Secteur d'activités	Production, Import/ export
Numéro de Fax	+213 34 21 16 54
Numéro de Téléphone	+213 34 21 16 61
Email	rtc.bejaia@sonatrach.dz
Site Internet	www.sonatrach-dz.com

TABLE 1.1: Identifications sur SONATRACH Bejaia . [1]

1.4.3 Carte du Réseau de Transport RTC Bejaïa

La figure suivante montre la carte réseaux de transport de la RTC :

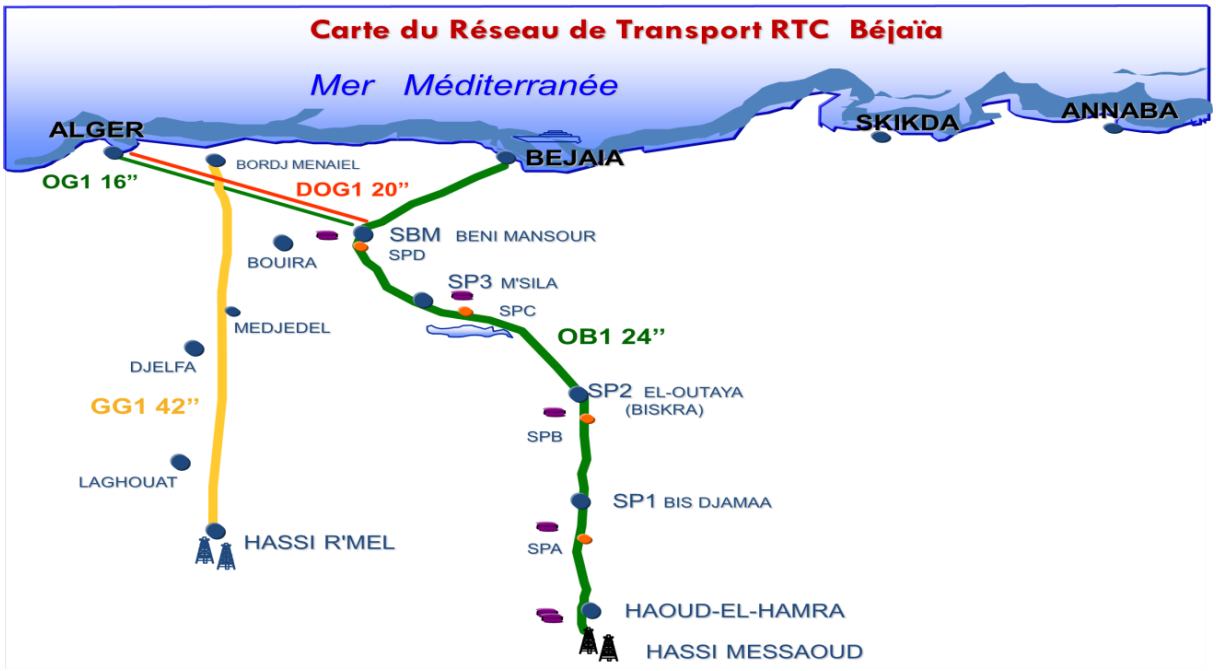

FIGURE 1.3 – Carte du Réseau de Transport RTC Bejaïa.
[1]

1.4.4 Organigramme de la RTC Bejaia

La RTC est composée de trois sous-directions qui sont elles-mêmes décomposées en départements.la figure suivantes montre Les différentes sous-directions et départements de la RTC :

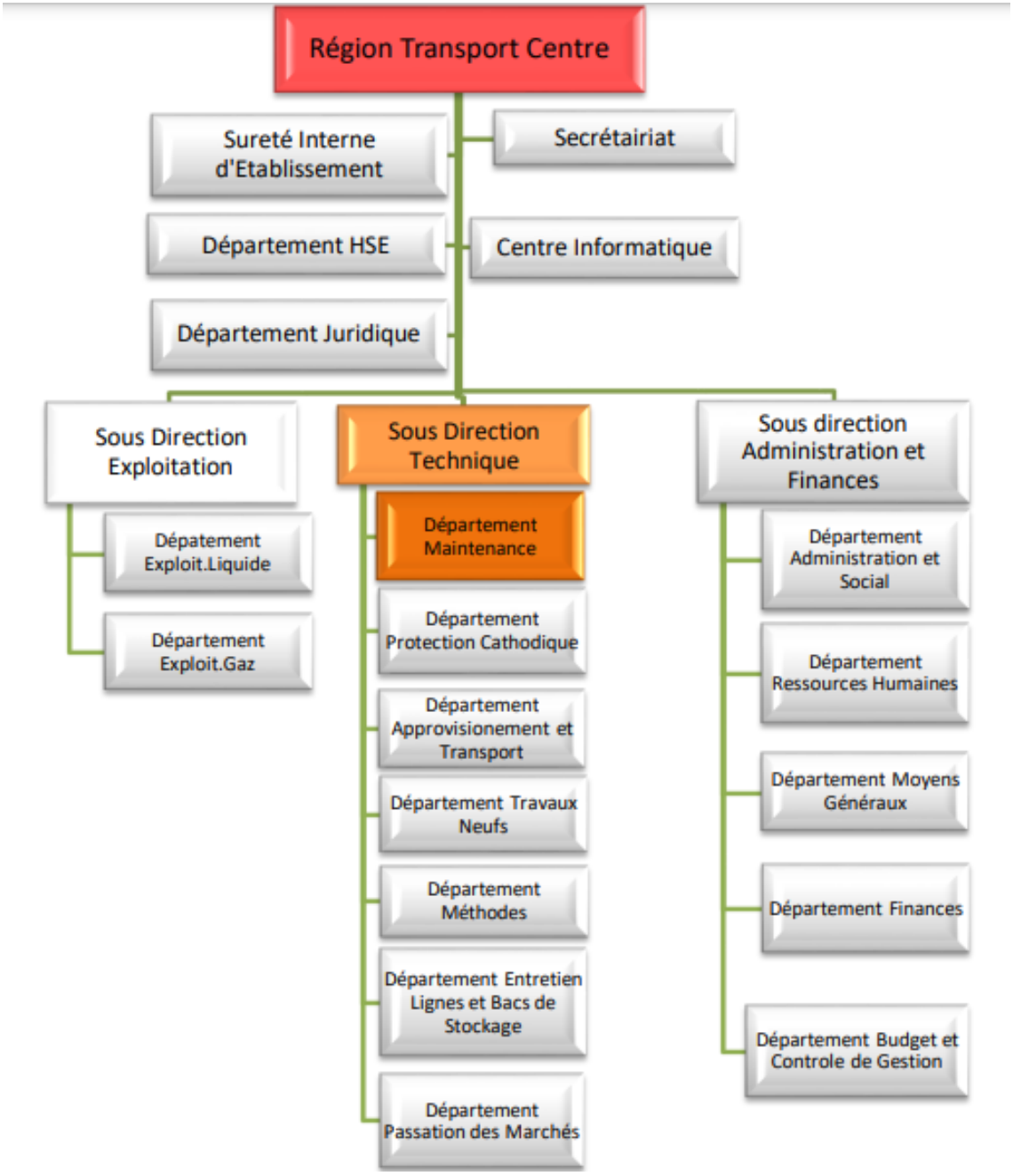

FIGURE 1.4 – Organigramme de la RTC .
[1]

a) Différentes sous directions

1. Sous-direction Exploitation « SDE »

La SDE est chargée de l'exploitation des installations de la région.Sa structure est représentée sur la figure suivante :

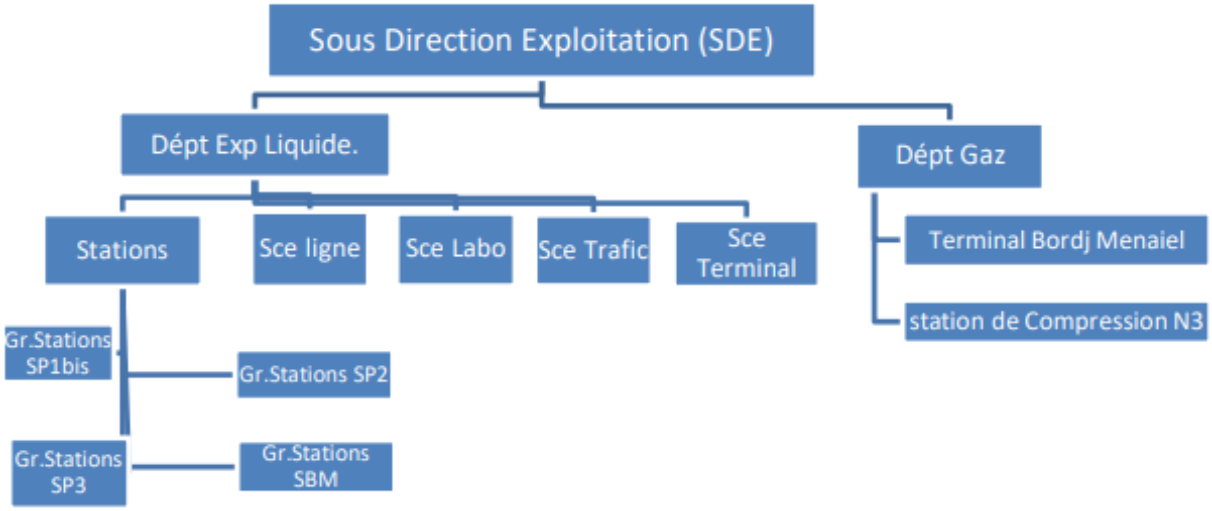

FIGURE 1.5 – organigramme qui montre la structure de SDE.
[1]

2. Sous-direction Technique « SDT »

La SDT a pour mission d'assurer la maintenance et la protection des ouvrages, ainsi que l'approvisionnement, l'étude et le suivi de projets de réalisation de travaux neufs.Sa structure est représentée sur la figure suivante :

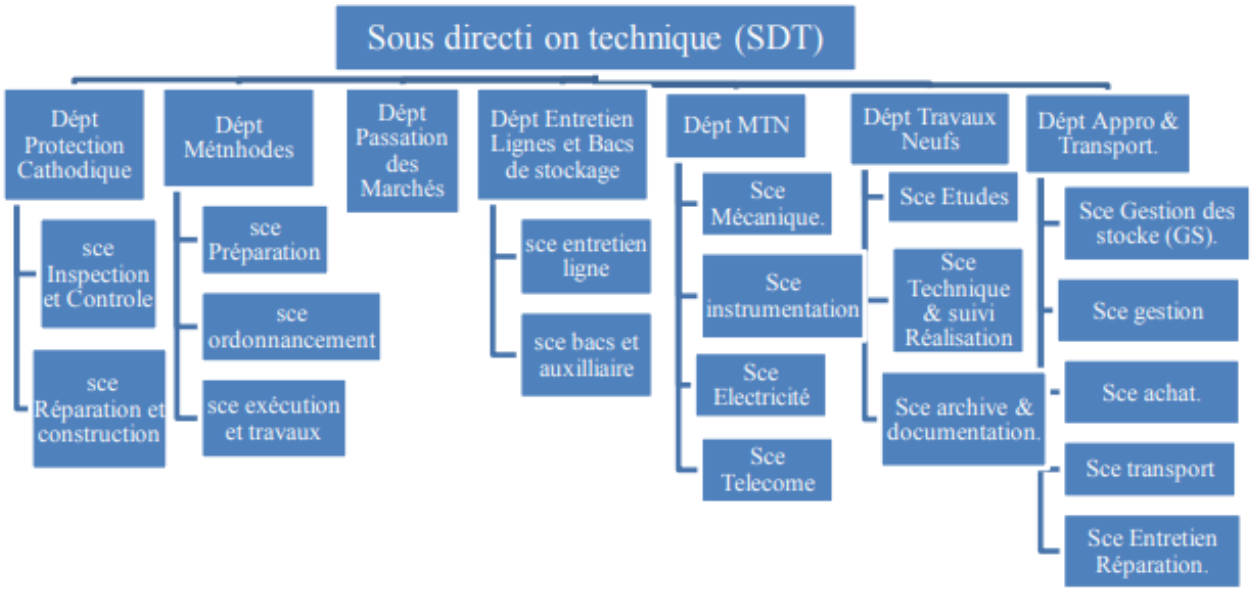

FIGURE 1.6 – organigramme qui montre la structure de SDT.
[1]

3. La Sous-direction Administration et Finances « SDAF »

Elle a pour mission de mettre en œuvre les recommandations de la commission hygiène et sécurité, élaborer et exécuter les plans emploi et formation de la Direction, Assurer la gestion administrative de son personnel.Sa structure est représentée sur la figure suivante :

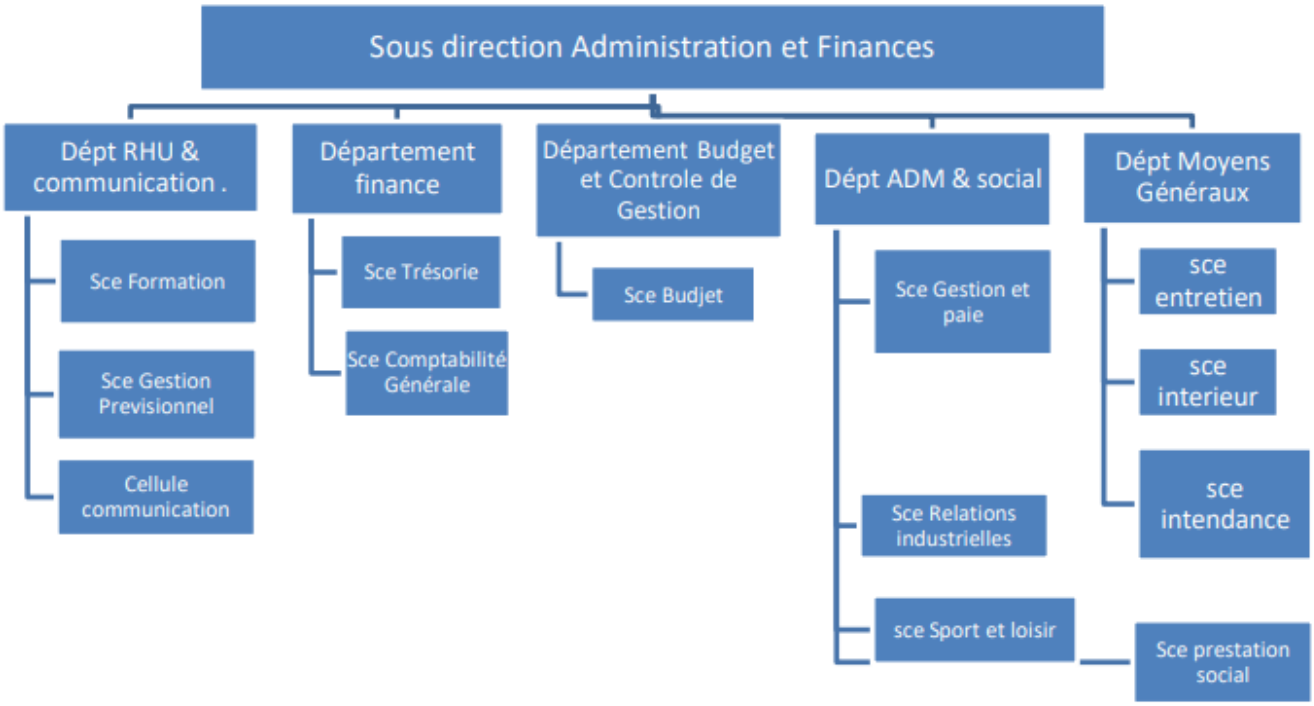

FIGURE 1.7 – organigramme qui montre la structure de SDAF.
[1]

b) Différents départements

1. Le Département Hygiène sécurité environnement « HSE » : Il a pour mission la Protection et la sauvegarde du patrimoine humain et matériel de la TRC, veille au respect, stricte des normes et standards en matière d'hygiène, et aussi le bon cheminement du transport des hydrocarbures.

2. Département maintenance « MNT » : Il est chargé de l'entretien des lignes (OB1, DOG1 et GG1) et vise à maintenir ou à rétablir les équipements de ces lignes dans un état spécifié afin de les garder en mesure d'un bon service en permanence.

3. Département Approvisionnement et transport « ATR » : Ce département comme son nom l'indique assure les approvisionnements nécessaires pour la bonne exploitation des installations, il assure la disponibilité des pièces de rechanges et équipements ainsi que les moyens de transport [1].

4. Département Travaux neufs « TNF » : Le département Travaux Neufs est chargé des études et le suivi des projets d'investissement de la RTC dans les distincts domaines. Il prend aussi en charge les travaux de rénovation des installations demandés.

5. Département Exploitation liquide « EXL » : Ce département est chargé par le Transport de pétrole brut et du condensât de Haoud El Hamra vers les terminaux de Bejaïa et de la raffinerie de sidi Arcine-Alger, Gestion des stations de pompage et des terminaux, Stockage de pétrole brute et condensât.

6. Département Exploitation Gaz « EXG » : Ce département, créé à partir de 2004, est

chargé de l'exploitation du gazoduc entre HassiR'mel et Bordj Menaiel. Le gaz est livré directement à la SONALGAZ pour l'alimentation des centrales électriques, des citoyens et des usines.
7. Département Finances « FIN » : Il prend en charge la gestion comptable et financière de RTC, il assure l'enregistrement chronologique des informations en comptabilité et la gestion de la trésorerie comme Il fait des appels de fonds à la division de commercialisations des hydrocarbures.
8. Département Juridique : Ce département veille sur la légalité des transactions, lance des appels d'offre nationaux et internationaux, les litiges nés entre RTC et les tiers et assurer le contrôle de gestion et de prise en charge des affaires juridiques de l'entreprises.
9. Département Budget et contrôle de gestion « BDG » : Ce département était l'un des services du département finances, devenu département dans le cadre du nouvel organigramme.
10. Département Administration et Social « ASL » : Ce département veille au respect des lois en vigueur qui régissent les relations de travail. Il est aussi chargé de la gestion du personnel de la RTC (pointage, remboursement des frais de mission, congé).
11. Département Ressources Humaines et Communication « RHC » : La mission de ce département est d'acquérir des ressources humaines en nombre et en qualité, d'assurer l'évolution de leur carrière et de planifier les besoins à court et moyen terme, tant en effectif qu'en besoins de formation, de perfectionnement et de recyclage.
12. Département Moyens généraux « MOG » : Ce département assure le soutien logistique de l'entreprise et assure la restauration du personnel ainsi que la prise en charge des missionnaires lors de leur déplacement [1].

1.5 Présentation du service d'accueil (Centre informatique)

Il est chargé de développer et d'exploiter des applications pour le compte de la RTC ainsi que la maintenance des équipements informatiques.Sa structure est représentée sur la figure suivante :

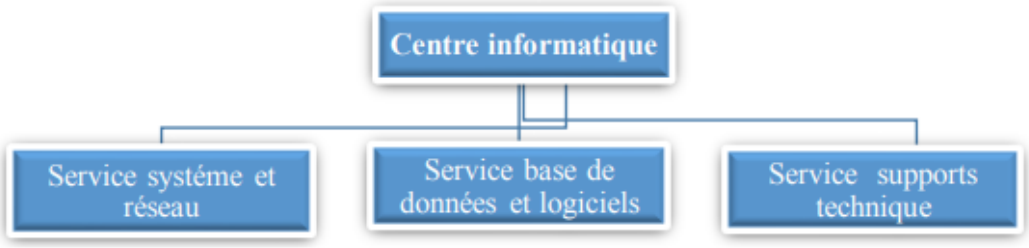

FIGURE 1.8 – Organigramme qui montre la structure du centre informatique.
[1]

1.5.1 Le rôle du service informatique

– **Service système et réseau**

1. Système

• Sélection du matériel informatique et des logiciels de base ;

• Mise en œuvre de solutions matérielles et logicielles sélectionnées ;

• Installer et configurer le système ;

• Diriger le travail de l 'équipe de développement en utilisant au mieux les ressources informatiques ;

• Implémentation de nouvelles versions logicielles [1].

2. Réseau

• Assurer le fonctionnement normal, la fiabilité des communications, la gestion du réseau et organiser le développement de sa structure ;

• recherche pour sélectionner l' architecture réseau à installer ;

• Participer au réseautage ;

• Définir les droits d' accès pour l 'utilisation du réseau ;

• Assurer une surveillance permanente pour détecter et prévenir les pannes ;

• Gérer les pannes et les événements qui se produisent sur le réseau [1].

–Service base de données et logiciels

1. Base de données

• Concevoir des bases de données et assurer l'optimisation et le suivi de la gestion informatisée des données ;

• Installer, configurer et exploiter un SGBD et ses bases de données ;

• Mettre en place et gérer les procédures de sécurité (accès, intégrité) ;

• Gérer la sauvegarde, la restauration et la migration des données.

2. Logiciels

• Recherche et conception de systèmes d'information ;

• Développer et maintenir les applications informatiques de RTC ;

• Déploiement de l 'application et formation des utilisateurs [1] .

– **Service supports technique**

• Assister les utilisateurs en cas de problèmes logiciels et matériels ;

• Installation de logiciels de gestion, techniques et bureautiques ;

• Formation à l' installation de nouveaux produits [1].

1.5.2 État des lieux

1.5.2.1 Présentation du réseau RTC

Le réseau informatique de la RTC de Bejaia est constitué de deux bâtiments, l'ancien bâtiment qui dispose de topologie physique en étoile étendue et le nouveau bâtiment dont la topologie physique est hybride (en étoile et en anneaux). Le type de lien entre ces deux derniers est la fibre optique [1].

1.5.2.2 Infrastructure réseau

L'architecture physique du réseau LAN de SONATRACH RTC est installée suivant le modèle hiérarchique qui divise le réseau en trois couches ou niveaux distinctes : couche cœur ou noyau (Core layer), couche distribution (Distribution layer) et couche d'accès (Access layer). Au niveau des stations rattachées à la SONATRACH RTC un réseau LAN est réalisé afin de faciliter la communication entre les utilisateurs des stations et l'utilisation des ressources centralisées au niveau de la DRGB. Le raccordement des stations au réseau SONATRACH RTC est réalisé à travers une ligne spécialisée de boucle fibre optique propriété de la SONATRACH [1].

1.5.2.3 Analyse du parc informatique

Le tableau suivant montre les différents équipements informatiques existant au niveau de l'entreprise SONATRACH RTC Bejaïa.

Périphériques utilisés	Appellation
Commutateur cœur	Cisco Catalyst 9407
Commutateur distribution	Cisco Catalyst 3850
Commutateur accès	Cisco Catalyst 9200
	Cisco Catalyst 2960
	Cisco Catalyst 3550
	Cisco Catalyst 3850
CME(Call Manager Express)	Routeur 2900
ISP(Internet Service Provider)	Cloud PT
Terminal PC	PC bureau DELL, Laptop
Téléphonie IP	IP Phone 7960
Autres équipements	Serveurs, imprimantes, Access Point

TABLE 1.2: Tableau du parc informatique existant . [1]

1.6 Problématique et solutions proposées

1.6.1 Problématique

La mise en place d'un cluster haute disponibilité avec équilibrage de charge est cruciale pour assurer la stabilité et la performance du réseau de SONATRACH de Bejaia. Au cours de mon stage pratique au sein de l'entreprise, on a identifié plusieurs anomalies liées à la sécurisation du réseau. Ces lacunes incluent l'absence d'une infrastructure de haute disponibilité réseau, ainsi que des risques de surcharge réseau dus à un seul domaine de diffusion. Par conséquent, la problématique de notre projet de fin d'études se formule comme suit :
- Comment mettre en place efficacement un cluster haute disponibilité avec équilibrage de charge pour améliorer la disponibilité, la sécurité et les performances du réseau de SONATRACH de Bejaia ?

1.6.2 Solution proposée

Pour résoudre ces lacunes et atteindre les objectifs de disponibilité et de performance du réseau, les solutions suivantes sont suggérés :

• Mise en place d'une infrastructure de cluster haute disponibilité : Installation et configuration de serveurs de cluster pour assurer une redondance et une continuité de service en cas de

défaillance d'un nœud.

• Mise en place de protocoles de redondance : Utilisation de protocoles tels que GLBP (GetwayLoad Balancing Protocol) pour équilibrer les charges entre les équipements réseau et assurer une redondance des chemins de communication.

• Mise en place de protocoles d'agrégation de liens : L'implémentation du LACP (Link Aggregation Control Protocol)qui permet de regrouper plusieurs liens physiques en un seul lien logique, augmentant ainsi la bande passante, la disponibilité et la résilience du réseau. De plus, l'utilisation d'EtherChannel, une technologie de Cisco Systems, offre une méthode de regroupement et de gestion des liens pour optimiser la performance et la redondance.

• Sécurisation de la DMZ : Implémentation de privates VLANs pour renforcer la sécurité de la zone démilitarisée (DMZ) et limiter la propagation des attaques potentielles.

• Utilisation de mécanismes de synchronisation et de réplication des données pour maintenir la cohérence entre les nœuds du cluster, évitant les incohérences et les conflits lors des mises à jour ou des modifications simultanées.

En mettant en œuvre ces solutions, la SONATRACH de Bejaia pourra améliorer la disponibilité, la sécurité et les performances de son réseau grâce à la mise en place d'un cluster haute disponibilité avec équilibrage de charge.

1.7 Conclusion

Dans ce chapitre, nous avons présenté les différentes structures de l'entreprise SONATRACH et plus précisément la Région Transport Centre de Bejaïa, dans laquelle nous avons effectuer notre stage au sein du centre informatique. En suite, nous avons posé la problématique.

Chapitre 2

Généralités Sur Les Réseaux Et La Securite Informatiques

2.1 Introduction

À l'époque contemporaine, les réseaux informatiques sont devenus indispensables. Les réseaux permettent l'utilisation d'une gamme variée d'applications, allant des plus élémentaires aux plus complexes. Les réseaux sont désormais omniprésents et impactent tous les propriétaires d'ordinateurs. Les réseaux offrent aux utilisateurs l'accès à d'innombrables fonctions, y compris le partage de ressources, ainsi que des fichiers.
Un réseau qui néglige la protection de ses données et de ses communications peut avoir des grands risques, c'est la raison pour laquelle la sécurité informatique s'occupe de toute protection.

Pour acquérir une compréhension globale de l'environnement réseau et sécurité, il est impératif de définir les termes fondamentaux. Notre discussion commencera par un aperçu des réseaux informatiques, y compris leurs définitions, objectifs et classifications, ainsi que les modèles OSI et TCP/IP, ainsi que les divers équipements d'interconnexion. Dans un deuxième temps, nous approfondirons le sens et les objectifs de la sécurité informatique dans son ensemble. Ensuite, nous examinerons les différentes attaques utilisées pour perturber les systèmes de réseau. Enfin, nous explorerons les mécanismes utilisés pour la sécurité informatique.

2.2 Généralité sur les réseaux informatiques

2.2.1 Définition

Un réseau informatique est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services. Un réseau est constitué d'équipements appelés nœuds, en fonctions de leurs étendues et de leur domaine d'application, ces réseaux sont catégorisés. Pour communiquer entre eux, les nœuds utilisent des protocoles, ou langages, compréhensibles par tous [3].

2.2.2 L'intérêt des réseaux informatiques

Un réseau informatique peut servir plusieurs buts distincts [4] :
- Le partage de ressources (fichiers, applications ou matériels) ;
-La communication entre personnes (courrier électronique, discussion en direct, etc.) ;
-La communication entre processus (entre des machines industrielles par exemple) ;
-La garantie de l'unicité de l'information (bases de données) ; -Le jeu vidéo multi-joueurs.

2.2.3 Architecture des réseaux

2.2.3.1 Architecture d'égal à égal

Dans une architecture d'égal à égal (ou poste à poste), contrairement à une architecture de réseau de type client-serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources [4].
- ***Avantage :*** l'architecture d'égal à égal a tout de même quelque avantage parmi lesquelles [4] :
• Un cout réduit (les couts engendrés par un tel réseau sont le matériel, les câbles et la maintenance) ;
• Une simplicité à toute épreuve.
- ***Inconvénients :*** Les réseaux d'égal à égal ont énormément d'inconvénients [4] :
• Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;
• La sécurité est très peu présente ;
• Aucun maillon du système n'est faible.
La figure suivante (figure 2.1) montre une architecture de type poste à poste :

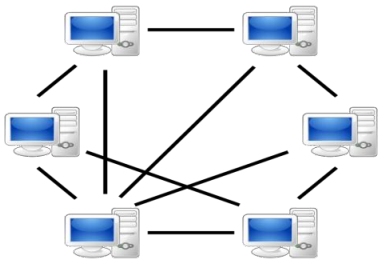

FIGURE 2.1 – Architecture poste à poste.
[5]

2.2.3.2 Architecture de type client-serveur

De nombreuses applications fonctionnent selon un environnent client-serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services [4].

- Avantage : Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont [4] :

• **Des ressources centralisées :** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction ;

• **Une meilleure sécurité :** car le nombre de points d'entrée permettant l'accès aux données est moins important ;

• **Une administration au niveau serveur :** les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés ;

• **Un réseau évolutif :** grâce à cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeurs.

- Inconvénients : cette architecture a tout de même quelques lacunes parmi lesquelles [4] :

• **Un cout élevé :** dû à la technicité du serveur ;

• **Un maillon faible :** le serveur est le seul maillon faible du réseau client/serveur.
La figure suivante (figure 2.2) montre une architecture de type client/serveur :

FIGURE 2.2 – Architecture client/serveur .
[6]

2.2.4 Type des réseaux

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes [3] :

a. Le réseau personnel (PAN) : la plus petite étendue de réseau est nommée en anglais **Personal AreaNetwork** (PAN). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celuici, le Personal Operating Space (POS). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique [3].

b. Le réseau local (LAN) : de taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français Réseau Local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs... Il est couramment utilisé pour le partage de ressources communes comme des périphériques, des données ou des applications [3].

c. Le réseau métropolitain (MAN) : Le réseau métropolitain ou Metropolitan AreaNetwork (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètres [3].

d. Le réseau étendu (WAN) : les étendues de réseaux les plus conséquentes sont classées en **Wide Area Network** (WAN). Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux [3].

La figure suivante (figure 2.3) montre les différents types des réseaux informatiques :

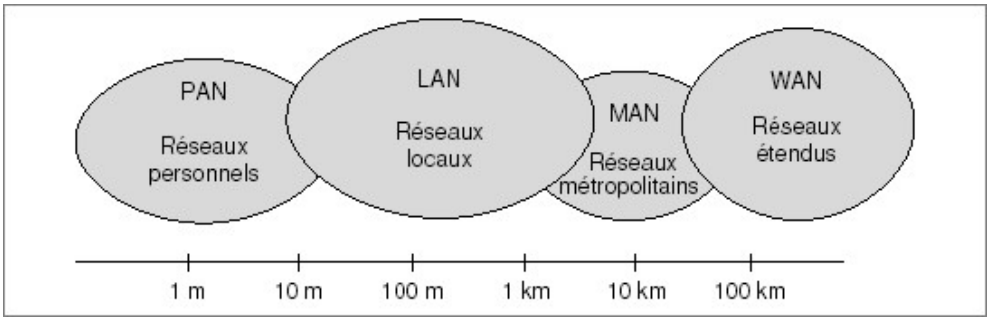

FIGURE 2.3 – Les types des réseaux.
[7]

2.2.5 Les Topologies d'un réseau

Une topologie caractérise la façon dont les différents équipements réseaux sont positionnés les uns par rapport aux autres [8].

On distingue la topologie physique, relative au plan du réseau, de la topologie logique, qui précise la façon dont les informations circulent au plus bas niveau [8].

a. Le bus : La topologie en bus (support linéaire) repose sur un câblage, sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexion, périphériques). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux. L'inconvénient majeur repose sur le fait qu'une seule coupure du câble empêche toute station d'échanger des informations sur le réseau [8].

La figure suivante (figure 2.4) montre une topologie en bus :

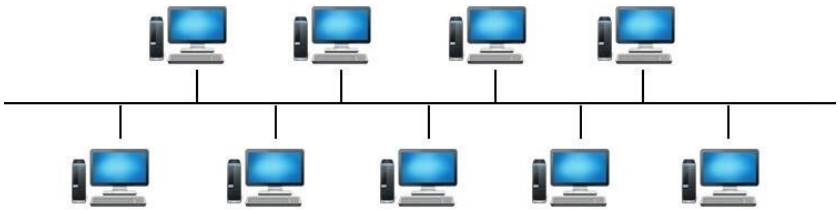

FIGURE 2.4 – Topologie en bus.
[9]

c. L'anneau : Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud, qui se compte comme un répéteur (élément actif). Les concentrateurs en anneau permettent l'insertion de station dans un réseau [8].

La figure suivante (figure 2.5) montre une topologie en anneau :

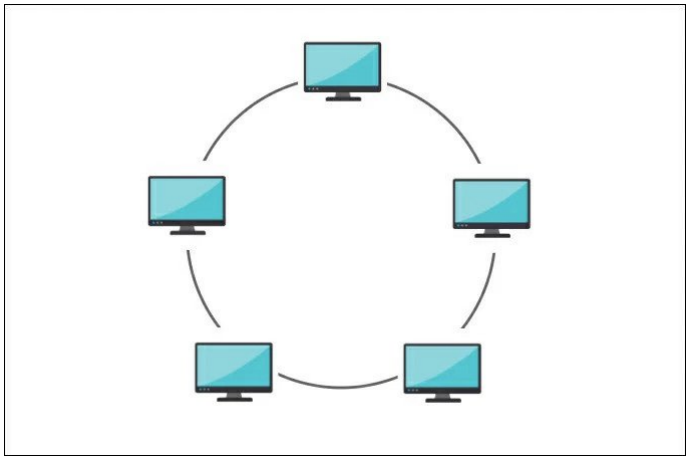

FIGURE 2.5 – Topologie en anneau.
[10]

b. L'étoile : La topologie en étoile repose, quant à elle, sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère. Il intègre une fonction de répéteur [8].
La figure suivante (figure 2.6) montre une topologie en étoile :

FIGURE 2.6 – Topologie en étoile.
[9]

d. L'arbre : Dans l'architecture en arbre, les postes sont reliés entre eux de manière hiérarchique, à l'aide de concentrateurs cascadables (stackable hubs). Cette connexion doit être croisée [8].
La figure suivante (figure 2.7) montre une topologie en arbre :

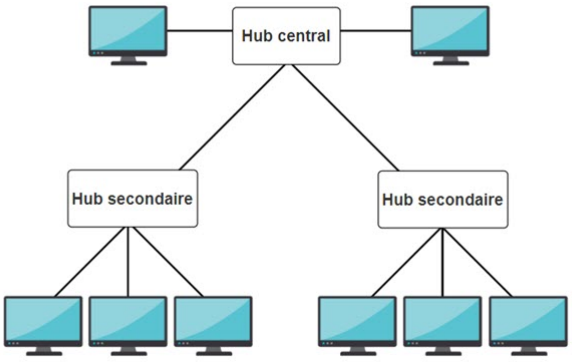

FIGURE 2.7 – Topologie en arbre.
[10]

2.2.6 Norme de communication

2.2.6.1 Le modèle OSI

OSI signifie (Open Systems Interconnection, Interconnexion de Systèmes Ouvert). Ce modèle a été défini par l'ISO afin de mettre en place un standard de communication entre les ordinateurs d'un réseau, c'est-à-dire des règles gérant les communications entre les ordinateurs [11]. Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI) [11].

Le modèle OSI comprend sept couches, Les couches du modèle OSI sont les suivantes [11] :
• **La couche Application - Application Layer (C7) :** Cette couche a pour objectif de fournir des services aux utilisateurs d'un réseau. Elle contient l'application informatique (le programme) qui désire communiquer avec un ordinateur distant [11].
• **La couche Présentation - Presentation Layer (C6) :** Elle permet de fournir une représentation des données, autrement dit une représentation qui ne dépend pas des ordinateurs, systèmes d'exploitation, etc. et inclut des services tels que le cryptage, la compression et le formatage des données [11].
• **La couche Session - Session Layer (C5) :** Cette couche offre la possibilité d'organiser les échanges en unités indépendantes. Elle offre aussi une structure de contrôle pour la communication entre application. Elle établit, maintient et clôt les sessions entre les applications. L'un des points forts de cette couche est la sécurité [11].
• **La couche Transport - Transport Layer (C4) :** Elle est chargée d'établir les connexions, de maintenir la qualité de la connexion et d'interrompre cette dernière de manière ordonnée, une fois la conversation terminée. Cette couche transporte des blocs d'octets de longueur quelconque. Elle s'assure que les données sont délivrées sans erreur et dans l'ordre [11].
• **La couche Réseau - Network Layer (C3) :** Elle transporte des blocs d'octets de taille limitée. Elle s'occupe de l'adressage et du routage des paquets a leurs destinations et a donc besoin d'un plan d'adressage, ainsi que du contrôle de flux. Elle est aussi responsable de l'établissement d'une connexion logique entre une source et une destination sur un réseau [11].
• **La couche Liaison de données - Data Link Layer (C2) :** Cette couche fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions entre entités de réseaux et est chargée d'acheminer sans erreur les données sur chaque liaison du réseau (Ethernet, Token Ring, etc.), en masquant aux autres couches les différences physiques du réseau. Elle assemble les données en blocs, auxquels elle ajoute des informations de contrôle pour constituer une trame de données : l'adresse de destination, la longueur du message, l'information de synchronisation, de détection d'erreur, etc. [11].
• **La couche Physique - Physical Layer (C1) :** elle permet de véhiculer l'information et de transformer des séquences de bits (0 ou 1) en séquences de grandeur physique appropriée au média de communication [11].
La figure suivante (figure 2.8) montre les couches du modèle OSI :

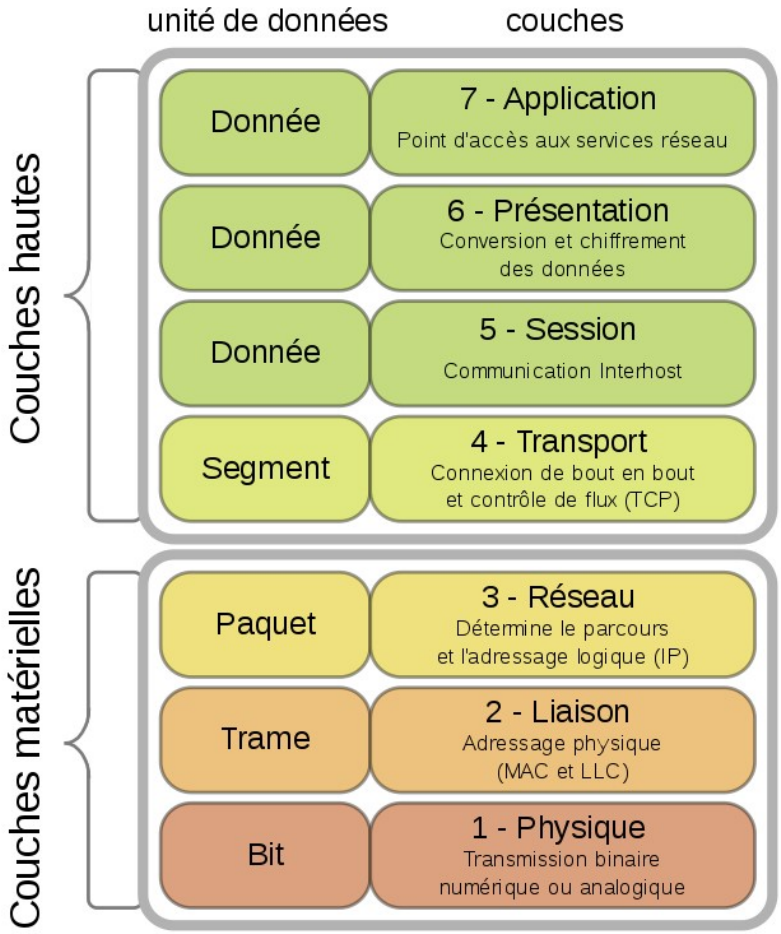

FIGURE 2.8 – le Modèle OSI.
[12]

2.2.6.2 Le modèle TCP/IP

TCP/IP : Transmission Control Protocol/Internet Protocol. Il s'agit d'un ensemble de protocoles utilisés par les ordinateurs pour communiquer sur un réseau. Il est en fait constitué de deux protocoles majeurs : TCP et IP et se caractérise entre autres par [13] :

- Le fractionnement des communications en paquets ;

- Son système d'adressage (par IP) ;

- Un acheminement correct des paquets ;

- Le contrôle des erreurs de transmission.

En fait, TCP/IP est ce qu'on appelle un modèle en couches, c'est-a-dire que les données traversent plusieurs niveaux de protocoles, ajoutant ainsi une information (en-tête) au paquet pour chaque couche. Le modèle TCP/IP s'appuie sur le modèle OSI (7 couches) mais ne comporte que 4 couches. Comme vous pouvez le voir, les couches TCP/IP regroupent plusieurs couches du modèle OSI [13].
La figure suivante (figure 2.9) montre les couches du modèle TCP/IP :

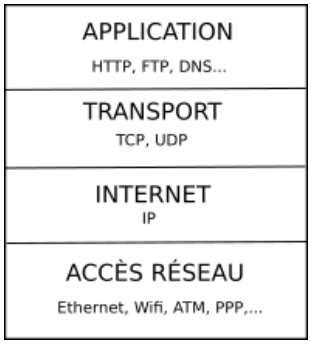

FIGURE 2.9 – Le modèle TCP/IP .
[14]

• **Couche Accès réseau (Link Layer) :** La couche Accès réseau spécifie la forme sous laquelle les données doivent être acheminées, quel que soit le type de réseau utilisé [13].
• **Couche Internet (Internet Layer) :** La couche Internet est chargée de fournir le paquet de données (datagrammes) [13].
• **Couche Transport (Transport layer) :** La couche Transport assure l'acheminement des données, ainsi que les mécanismes permettent de connaitre l'état de la transmission [13].
• **Couche Application (Application Layer) :** La couche Application englobe les applications standard du réseau (Telnet, SNMP, FTP...) [13].

2.2.7 Périphériques d'interconnexion

• **Le commutateur (Switch) :** est apparu en 1990, sur Ethernet, et en 1994, pour Token Ring. Il intègre à la fois une fonction de concentrateur et une fonction de pont. Il se comporte comme un pont multibrin. Il permet d'introduire une architecture centralisée d'interconnexion d'autres LAN. Etant au cœur de la topologie, il constitue un moyen privilégié de suivre l'utilisation du réseau [3].

• **Le routeur :** est un matériel d'interconnexion qui a accès à toutes les informations des couches 1,2 et 3 notamment aux adresses logiques qui sont indépendantes de toute méthode d'accès et toute topologie physique. Il permet de choisir le meilleur chemin possible au sens des

adresses logiques [3].

• **La passerelle :** Il s'agit d'une machine, en générale un serveur dédié, qui opère au niveau des couches 3 à 7 en tant que traducteur des couches moyennes et hautes, notamment pour la mise en forme des données [3].

• **Le répéteur (transceiver) :** agit au niveau de la couche physique du modèle OSI. Il reconditionne les données reçues et les retransmet, afin d'accroître la distance de transmission. En effet, les signaux numériques étant sujets à une forte atténuation, il est nécessaire de retransformer le signal en données, puis les données en signaux [3].

• **Le pont (bridge) :** agit au niveau de la couche liaison de données. Il permet ainsi de lier deux ou plusieurs supports physiques différents, à condition que les mêmes formats d'adresses MAC soient utilisés des deux côté [3].

2.2.8 Les classes d'adresses IP

Classe	**Bits de départ**	**Début**	**Fin**	**Notation CIDR**	**Masque de sous-réseau par défaut**
Classe A	0	0.0.0.0	126.255.255.255 (127 est réservé)	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		255.255.255.255
Classe E (réservée)	1111	**240**.0.0.0	255.255.255.255		non défini

TABLE 2.1: Les classes d'adresses IP . [15]

2.3 Généralité sur la sécurité informatique

2.3.1 Définition

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles [16].

2.3.2 Les objectifs de la sécurité

• **L'intégrit**é qui garantit que les données sont bien celles que l'on croit être, qu'elles n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle)[17] ;

• **La confidentialité** qui consiste à rendre l'information inintelligible d'autres personnes que les seuls acteurs de la transaction [17] ;

• **La disponibilité** qui permet de garantir l'accès à un service ou à des ressources [17] ;

• **La non-répudiation** de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction [17] ;

• **L'authentification** qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être [17].

2.3.3 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini. L'objectif est de mieux comprendre les risques possibles des attaques informatiques. Et évidemment, pour pouvoir mieux s'en défendre par la suite, il est nécessaire de définir certains termes :
• **Une ressource :** tout objet qui a une valeur pour une organisation et qui doit être protégé [18] ;
• **Une vulnérabilité :** c'est la faiblesse d'un système qui pourrait être exploitée par une menace [18] ;
• **Une menace :** un danger potentiel pour une ressource ou pour le fonctionnement du réseau [18] ;
• **Une attaque (exploit) :** c'est une action prise pour nuire à une ressource [18] ;
• **Un risque :** c'est la possibilité de perte, altération, destruction ou autres conséquences négatives de la ressource d'une organisation [18] ;
• **Une contre-mesure :** une protection qui atténue une menace potentielle ou un risque [18].

2.3.4 Les attaques informatiques

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables [17].

Nous présentons dans ce qui suit quelques types d'attaque.

2.3.4.1 Programme malveillant

On appelle malware (ou programme malveillant, maliciel) un programme ou une partie de programme destiné à perturber, altérer ou détruire tout ou partie des éléments logiciels

indispensables au bon fonctionnement d'un système informatique [17].

On distingue principalement sept types de programmes malveillants : les virus informatiques, les bombes logiques, les vers, les chevaux de Troie, les ***rootkits***, les ***keyloggers*** et les ***spywares***. [17].

2.3.4.2 Attaques de reconnaissance

Une attaque de reconnaissance ou « attaque passive » a pour objectif de regrouper des informations sur le réseau cible pour déceler toutes les vulnérabilités [18]. Cette attaque utilise, en général, les méthodes de base suivantes [18] :

• **Un balayage de « ping » :** l'attaquant envoie des paquets « ping » à une plage d'adresses IP pour identifier les ordinateurs présents dans un réseau ;

• **Le balayage de port :** l'attaquant procède a une analyse de port (TCP et UDP) permettent de découvrir les services s'exécutant sur un ordinateur cible ;

• **Une capture de paquets (sniffing) :** la capture de paquets permet de capturer les données (généralement des trames Ethernet) qui circulent sur le réseau en vue d'identifier des adresses MAC, des adresses IP ou des numéros de ports utilisés dans le réseau cible.

2.3.4.3 Les attaque d'accès

Ces attaques ont pour objectif d'essayer de récupérer des informations sensibles sur les éléments du réseau. Les méthodes suivantes sont courantes pour effectuer une attaque d'accès [18] :
• **Le phishing :** le phishing est une tentative de récupérer des informations sensibles en envoyant des e-mails non sollicités avec des URL truqués ;
• **Le pharming :** est une autre attaque de réseau visant à rédiger le trafic d'un site web vers un autre site web ;
• **L'attaque de « Man-in-the –middle » :** un attaquant se place entre deux éléments réseaux pour essayer de tirer profit des données échangées.
• **Les attaques mélangées :** les attaques mélangées combinent les caractéristiques des virus, des vers et d'autres logiciels pour collecter des informations sur les utilisateurs.

2.3.4.4 Attaque par déni de service (DOS)

Une attaque par déni de service [Dos, Dental of Service] est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés [17]. On distingue habituellement deux types de dénis de service [17] :

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

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

2.3.5 Mécanismes de sécurité

2.3.5.1 Antivirus

Un antivirus est un programme capable de détecter la présence de malware sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur [17].

2.3.5.2 Chiffrement

Le chiffrement désigne la conversion des données depuis un format lisible dans un format codé. Les données chiffrées ne peuvent être lues ou traitées qu'après leur déchiffrement. Les deux principales techniques de chiffrement sont le chiffrement symétrique et asymétrique [19] :

• **Chiffrement symétrique :** Également appelé chiffrement à clé privée. La clé utilisée pour encoder est la même que celle utilisée pour décoder ;

• **Chiffrement asymétrique :** cette méthode utilise deux clés différentes (publique et privée) mathématiquement.

2.3.5.3 Pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall], est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers (notamment Internet]. Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes [17] :

• Une interface pour le réseau à protéger (réseau interne) ;

• Une interface pour le réseau externe.

La figure suivante (figure 2.10) montre un pare-feu dans un système informatique :

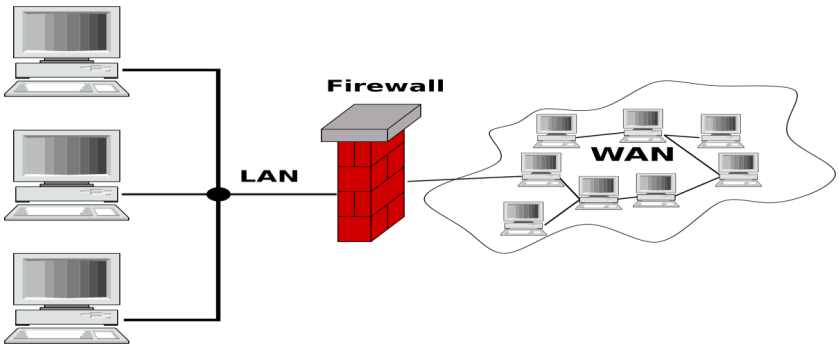

FIGURE 2.10 – Le pare-feu .
[20]

2.3.5.4 Zone démilitarisée (DMZ)

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie, serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise [17].

On parle ainsi de zone démilitarisée(notée DMZ, DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile [17].
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante [17] :
• Trafic du réseau externe vers la DMZ autorisé ;
• Trafic du réseau externe vers le réseau interne interdit
• Trafic du réseau interne vers la DMZ autorisé ;
• Trafic du réseau interne vers le réseau externe autorisé
• Trafic de la DMZ vers le réseau interne interdit ;
• Trafic de la DMZ vers le réseau externe interdit.
La figure suivante (figure 2.11) montre une zone démilitarisée :

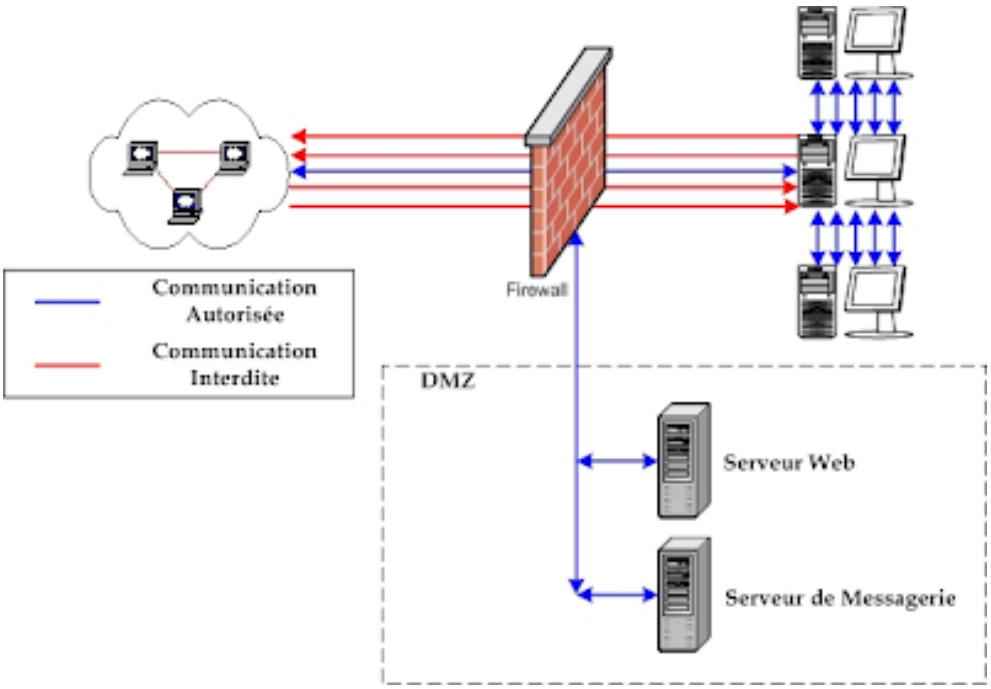

FIGURE 2.11 – La DMZ .
[21]

2.3.5.5 Proxy

Un serveur proxy (traduction française de proxy server, appelé aussi serveur mandataire] est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et Internet.La plupart du temps le serveur proxy est utilisé pour le Web, il s'agit alors d'un proxy HTIP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, etc.)[17].La figure suivante (figure 2.12) montre le serveur proxy :

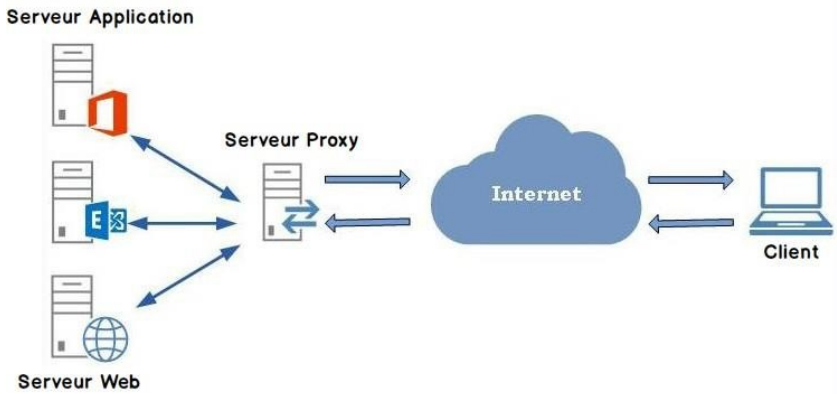

FIGURE 2.12 – Le proxy .
[22]

2.3.5.6 Système de détection d'intrusion (IDS)

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion [17].La figure suivante (figure 2.13) montre un système de détection d'intrusion :

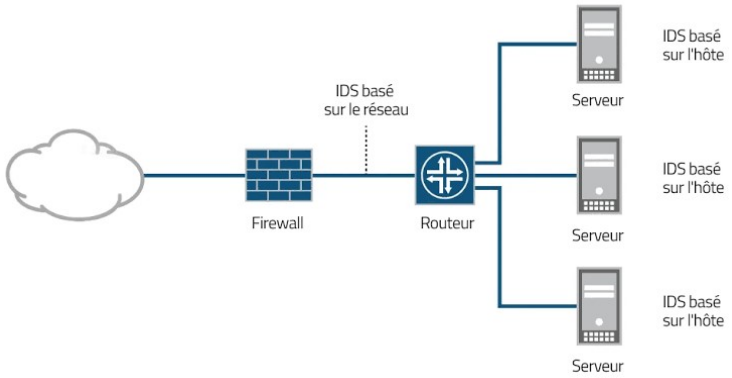

FIGURE 2.13 – Un système de détection d'intrusion .
[23]

2.3.5.7 Système de prévention d'intrusion (IPS)

Un système de prévention des intrusions (IPS) est un dispositif de sécurité réseau automatisé utilisé pour surveiller les potentielles menaces et y faire face. Tout comme les systèmes de détection des intrusions (IDS), les systèmes IPS sont capables de déterminer la présence de menaces en analysant le trafic réseau [24].La figure suivante (figure 2.14) montre un système de prévention d'intrusion :

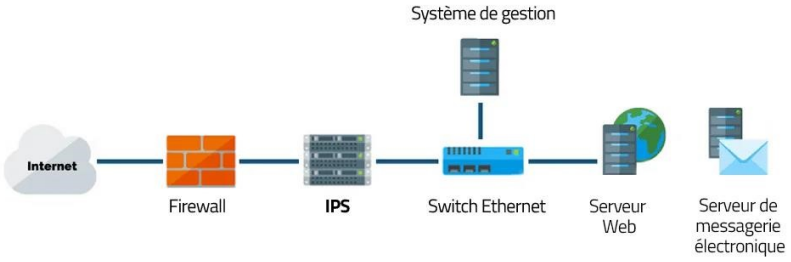

FIGURE 2.14 – Un système de prévention d'intrusion.
[25]

2.4 Conclusion

Dans ce chapitre nous avons présenté en premier lieu les réseaux informatiques d'une façon générale en citant les critères basiques qui montrent le rôle et la description d'un réseau informatique. Ensuite, nous avons défini la sécurité, les différentes attaques et les mécanismes utilisés pour la sécurité informatique

Chapitre 3

La Haute Disponibilité et le Clustering

3.1 Introduction

De nos jours, les activités dépendent de plus en plus des ressources informatiques. La disponibilité de ces ressources, c'est-à-dire leur capacité à fournir le service spécifié, ainsi que la confiance accordée par les utilisateurs aux services fournis par les systèmes informatiques, sont devenues des exigences primordiales. Ces éléments sont désormais considérés comme des propriétés essentielles de ces systèmes. Étant donné que les systèmes informatiques sont sujets à des défaillances, les concepteurs ont cherché des moyens de remédier à ces problèmes.

Nous serons ainsi conduits à aborder dans ce chapitre la haute disponibilité et le clustering dans un cadre général pour en cerner les différents concepts, puis, nous étudierons les différentes méthodologies et technologies élaborées pour la mise en place de la haute disponibilité.

3.2 Haute disponibilité

On appelle « haute disponibilité » (en anglais « high availability ») toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement d'un service 24H/24 [17].

Le terme « disponibilité » désigne la probabilité qu'un service soit en bon état de fonctionnement à un instant donné [17].

3.3 Définition et terminologie

Avant de présenter les concepts de la sûreté de fonctionnement et les systèmes à haute disponibilité, il est nécessaire d'introduire la terminologie associée [26] :

- **Elément :** c'est un sous-ensemble matériel et/ou logiciel assurant une fonction spécifique.

Il peut s'agir d'un dispositif, composant, sous-système, entité, module, unité, etc ;

• **Système Informatique :** ensemble cohérent et autonome d'éléments matériels, logiciel de base et d'applications, placé éventuellement dans un environnement réseau, son comportement est décrit dans un document de référence. Il offre des services à l'utilisateur dans un environnement donné ;

• **Service :** c'est l'ensemble des résultats et des conditions de leur délivrance que le système informatique fournit à l'utilisateur dans un environnement donné. La vie opérationnelle d'un système informatique est perçue, par ses utilisateurs, comme une alternance de trois états :
– **service rendu :** lorsque les résultats fournis et leurs conditions de délivrance sont conformes à ceux du service attendu ;
– **service dégradé (Degraded Service) :** lorsque les résultats fournis sont conformes à ceux du service attendu et leurs conditions de délivrance ne sont pas conformes à celles du service attendu ;
– **service non rendu :** lorsque les résultats fournis ne sont pas conformes à ceux du service attendu.

• **Défaillance :** discordance observée entre le service fournit à l'utilisateur et le service attendu. La défaillance peut être détectée par l'utilisateur (humain ou autre système) du système ou bien par le système lui même. On distingue différents niveaux de défaillance :
– **la défaillance complète (Complete Failure)** : c'est une discordance sur les résultats du service (par exemple, « plantage » (crash) du système d'exploitation) ;
– **la défaillance partielle (Partial Failure)** : c'est une discordance sur les conditions de la délivrance des résultats (par exemple, perte de performance, support d'un nombre moindre d'utilisateurs). Les défaillances sont causées par les erreurs.

• **Erreur :** c'est la discordance entre une valeur ou une condition, calculée ou observée, et la valeur ou la condition théorique correspondante ;

• **Plan de Reprise d'activité :** en anglais Disaster Recovery Plan ou DRP permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de l'infrastructure et la remise en route des applications supportant l'activité de l'organisation ;

• **Plan de continuité d'activité (PCA)** : Le plan de continuité d'activité quant à lui permet de poursuivre l'activité sans interruption du service. Le PCA est donc défini comme un ensemble de procédures et de dispositifs pouvant être appliqués avant, pendant ou après le déclenchement d'un sinistre.

3.4 Les concepts et composants

De nombreux facteurs peuvent avoir une incidence sur la disponibilité des données et des applications. Il est essentiel de prendre en considération tous ces éléments dans le cadre d'un concept de haute disponibilité.

3.4.1 La résilience matérielle

La disponibilité matérielle est une partie importante du concept de Haute disponibilité. Elle concerne les serveurs, disques durs, Switch sans oublier les PC, l'affichage ainsi que les chemins de communication à l'intérieur de l'infrastructure. Une façon simple de réduire le temps d'interruption d'un système d'information est de mettre en place une redondance au niveau des points critiques. Le matériel qui en constitue un, n'y échappe, et assuré sa disponibilité passe par la prise en compte de plusieurs paramètres [26].

3.4.1.1 La tolérance aux pannes

La tolérance aux pannes est la manière dont un système d'exploitation (OS) répond à une défaillance matérielle ou logicielle. Le terme se réfère essentiellement à la capacité d'un système à permettre des pannes ou des dysfonctionnements, et cette capacité peut être fournie par un logiciel, du matériel ou une combinaison des deux. Pour gérer les défauts avec élégance, certains systèmes informatiques ont deux ou plusieurs systèmes en double [27].

Principe

La tolérance aux pannes, permet de remplacer un serveur indisponible par un autre. Dans le cas étudié, le service génère une adresse IP qui redirigera les requêtes sur le serveur accessible. En fonctionnement normal, le client sera dirigé vers le serveur disponible. Les autres serveurs seront mis en attente. Tous les serveurs testent la présence des autres, la fréquence des tests est réglable ainsi que le temps pour considérer un serveur indisponible.

Dans le cas où le serveur principal devient indisponible, un des serveurs secondaires prend le relais. L'ordre de passage en mode actif est défini dans la configuration. Les services de type tolérance aux pannes sont à installer directement sur les serveurs. Certaines applications possèdent un service de tolérance aux pannes intégré, qui est parfois payant [28].
La figure suivante (figure 3.1) illustre le principe de tolérance aux pannes :

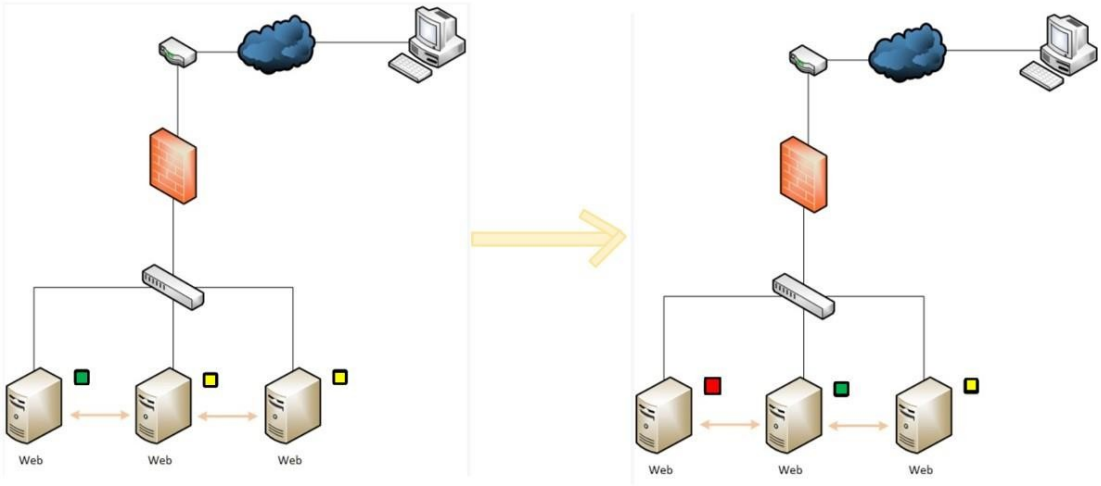

FIGURE 3.1 – schéma illustrant le principe de tolérance aux pannes.
[28]

3.4.1.2 Consolidation du Stockage

La consolidation du stockage est le processus de centralisation, de partage et d'optimisation des ressources de stockage de données entre plusieurs utilisateurs et applications. Il s'agit d'un concept large qui permet la conception et la construction d'une infrastructure de stockage pour une gestion efficace et une utilisation maximale, avec le matériel de stockage et les coûts de gestion les plus bas. La consolidation du stockage est également appelée convergence du stockage [29].

- SAN (Storage Area Network)

Un réseau de zone de stockage (SAN) est un réseau haut débit dédié et indépendant qui interconnecte plusieurs serveurs et leur offre des pools partagés de périphériques de stockage. Chaque serveur peut accéder à un stockage partagé comme s'il s'agissait d'un lecteur y étant directement rattaché. Un réseau SAN est généralement constitué de câbles, d'adaptateurs de bus hôte et de commutateurs SAN reliés à des baies de stockage et à des serveurs. Chaque commutateur et système de stockage du réseau de stockage doit être interconnecté [29].La figure suivante (figure 3.2) illustre un réseau de zone de stockage (SAN) :

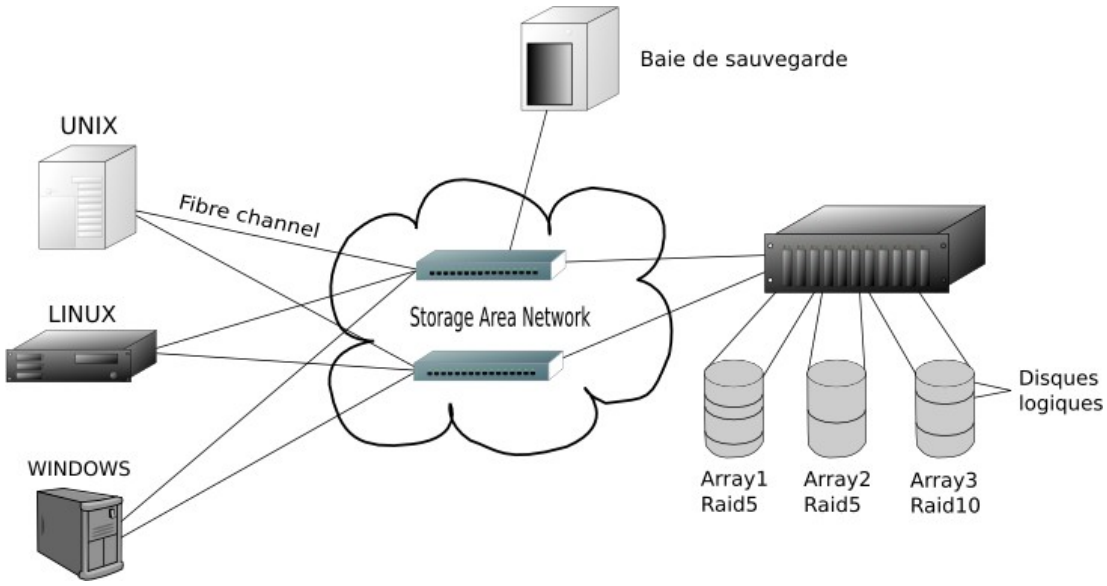

FIGURE 3.2 – Schéma illustrant un réseau de zone de stockage (SAN).
[30]

- NAS (Network Attached Storage)

Un NAS (Network Attached Storage, c'est à dire Stockage Raccordé au Réseau en français) est un serveur dont la vocation première est de servir de système de stockage de données déporté. En langage simple, il s'agit d'un (ou plusieurs) disque dur accessible sur un réseau [31].
La figure suivante (figure 3.3) illustre un stockage en réseau (NAS) :

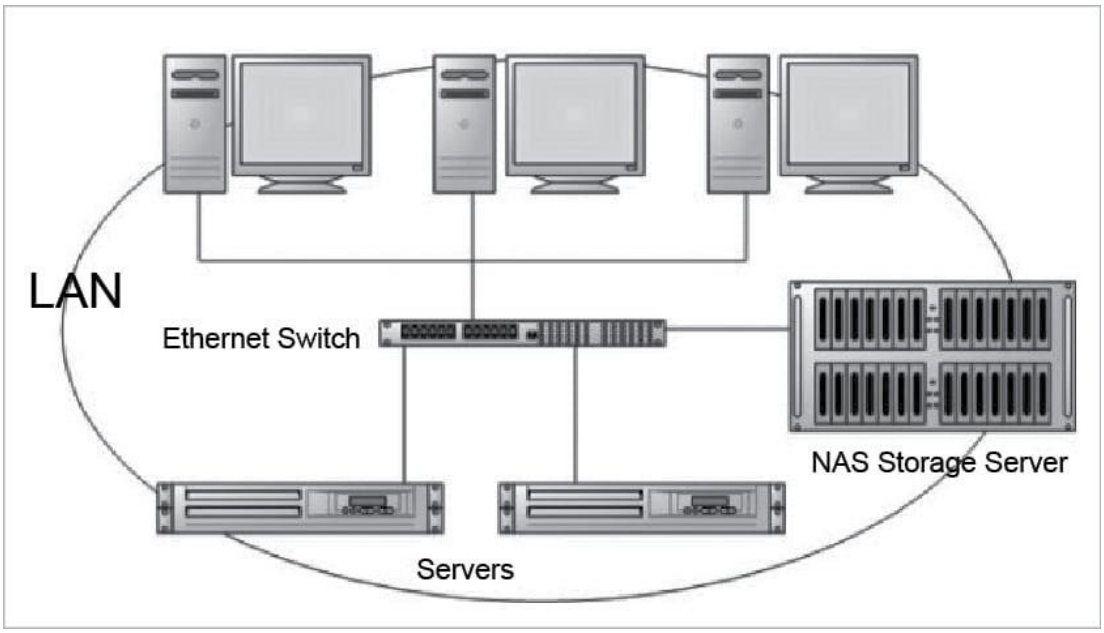

FIGURE 3.3 – Schéma illustrant un stockage en réseau (NAS).
[32]

3.4.1.3 Les solutions de virtualisation

En informatique, le processus de virtualisation consiste à attribuer les caractéristiques d'une machine physique à une ou plusieurs machines virtuelles, de manière à faire fonctionner différents systèmes d'exploitation sur un seul et unique serveur. Ce processus est aujourd'hui régulièrement utilisé pour augmenter la rentabilité des activités informatiques en entreprise [33].

Les avantages de la virtualisation [34] :

• **Des coûts réduits :** la virtualisation implique moins de serveurs, moins de place pour les héberger, moins de coûts de maintenance, etc. ;

• **Des économies d'énergie :** moins de serveurs = moins de pollution numérique ;

• **Une meilleure exploitation des ressources :** jusqu'alors souvent sous-exploitées, les capacités matérielles de l'entreprise sont fortement optimisées grâce à la virtualisation ;

• **Une continuité d'activité :** en cas de sinistre ou d'interruption, la virtualisation facilite le plan de reprise d'activité (ou PRA) ;

• **Une meilleure agilité :** en permettant de s'affranchir des contraintes matérielles, la virtualisation encourage la flexibilité des processus et la mobilité des équipes.

3.4.2 La résilience des données et des services

3.4.2.1 Système de sauvegarde & restauration

Le processus de sauvegarde et de restauration consiste à dupliquer des données et à les stocker dans un endroit sécurisé en cas de perte ou de dommage, puis à restaurer ces données dans un emplacement (que ce soit l'emplacement d'origine ou un emplacement sécurisé) afin qu'elles puissent être à nouveau utilisées dans le cadre des opérations. Dans l'idéal, cette copie de sauvegarde (souvent appelée « snapshot ») est immuable, c'est-à-dire qu'elle est non modifiable après sa création, afin de se protéger des menaces telles que les ransomwares par exemple [35].

3.4.2.2 Système de répartition de charge (équilibrage de charge)

- Définition

L'équilibrage de charge est la méthode qui permet de répartir le trafic réseau de manière égale sur un groupe de ressources prenant en charge une application. Les applications modernes doivent traiter des millions d'utilisateurs simultanément et renvoyer des données correctes comme du texte, des vidéos, des images et d'autres à chaque utilisateur de manière rapide et fiable. Pour gérer de tels volumes de trafic, la plupart des applications disposent de nombreux serveurs de ressources contenant des données en double. Un équilibreur de charge est un dispositif qui

se trouve entre l'utilisateur et le groupe de serveurs, et qui fait office de facilitateur invisible, garantissant que tous les serveurs de ressources sont utilisés de la même manière [36].
La figure suivante (figure 3.4) montre le principe de l'équilibrage de charge (Load Balancing) :

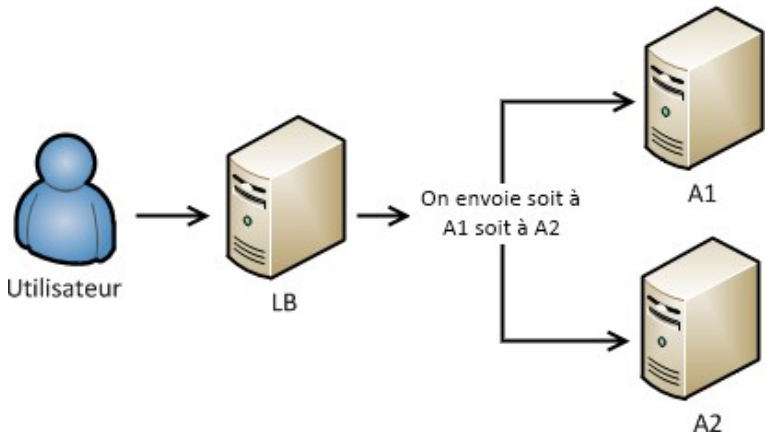

FIGURE 3.4 – Schéma illustrant le principe d'équilibrage de charge .
[37]

- Fonctionnement
L'équilibrage de la charge est assuré par un outil ou une application appelé "équilibreur de charge". Un équilibreur de charge peut être matériel ou logiciel. Les équilibreurs de charge matériels nécessitent l'installation d'un dispositif d'équilibrage de charge dédié.

Les équilibreurs de charge logiciels peuvent fonctionner sur un serveur, sur une machine virtuelle, ou dans le nuage. Les réseaux de diffusion de contenu (CDN) comprennent souvent des fonctions d'équilibrage de charge.

Lorsqu'une requête arrive d'un utilisateur, l'équilibreur de charge l'assigne à un serveur donné, et ce processus se répète pour chaque requête. Les équilibreurs de charge déterminent quel serveur doit traiter chaque demande en se basant sur un certain nombre d'algorithmes différents. Ces algorithmes se répartissent en deux grandes catégories : statiques et dynamiques [38].

- Algorithmes d'équilibrages de charge Il existe deux approches principales pour l'équilibrage de la charge :

L'équilibrage dynamique de la charge utilise des algorithmes qui prennent en compte l'état actuel de chaque serveur et distribuent le trafic en conséquence ;

L'équilibrage de charge statique distribue le trafic sans effectuer ces ajustements. Certains algorithmes statiques envoient une quantité égale de trafic à chaque serveur d'un groupe, soit dans un ordre précis, soit de manière aléatoire [39] :

*** Algorithmes d'équilibrage statique de la charge**

• **Round robin :** L'équilibrage de charge round robin distribue le trafic vers une liste de serveurs en rotation en utilisant le Domain Name System (DNS). Un serveur de noms faisant autorité possède une liste de différents enregistrements A pour un domaine et en fournit un différent en réponse à chaque requête DNS ;

• **Round robin pondéré :** Permet à un administrateur d'attribuer des poids différents à chaque serveur. Les serveurs jugés capables de gérer plus de trafic en recevront un peu plus. La pondération peut être configurée dans enregistrements DNS ;

• **Hachage IP :** Combine les adresses IP source et destination du trafic entrant et utilise une fonction mathématique pour les convertir en un hachage. Sur la base de ce hachage, la connexion est attribuée à un serveur spécifique.

*** Algorithmes d'équilibrage dynamique de la charge**

• **Least connection :** Vérifie quels serveurs ont le moins de connexions ouvertes à ce moment-là et envoie le trafic vers ces serveurs. Cela suppose que toutes les connexions nécessitent une puissance de traitement à peu près égale ;

• **Weighted least connection :** Donne aux administrateurs la possibilité d'attribuer des poids différents à chaque serveur, en partant du principe que certains serveurs peuvent gérer plus de connexions que d'autres ;

• **Temps de réponse pondéré :** Il calcule la moyenne du temps de réponse de chaque serveur et la combine avec le nombre de connexions ouvertes sur chaque serveur pour déterminer où envoyer le trafic. En envoyant le trafic vers les serveurs dont le temps de réponse est le plus rapide, l'algorithme garantit un service plus rapide aux utilisateurs ;

• **Basé sur les ressources :** Distribue la charge en fonction des ressources dont chaque serveur dispose à ce moment-là. Un logiciel spécialisé (appelé agent "") exécuté sur chaque serveur mesure le CPU et la mémoire disponibles de ce serveur, et l'équilibreur de charge interroge l'agent avant de distribuer le trafic vers ce serveur.

- Avantages et inconvénients de l'équilibrage de charge

Avantage : parmi lesquelles on a [40] :
- Augmentation de la quantité des services ;
- Amélioration des temps de réponse des services ;
- Capacité a palier la défaillance d'une ou de plusieurs machines ;
- Possibilité d'ajouter des serveurs sans interruption de service.

Inconvénient : parmi les lacunes on a [41] :
- Mise en place et configuration parfois complexe nécessitant une expertise technique ;
- Nécessite une protection spécifique contre les attaques par déni de service (DoS).

- Le basculement (failover)

Le failover, ou basculement est un mode de fonctionnement de secours qui consiste à basculer automatiquement sur une base de données, un serveur ou un réseau placé en attente si le système principal tombe en panne ou est arrêté le temps d'une maintenance. Le failover est une fonction extrêmement importante sur les systèmes critiques qui doivent rester accessibles à chaque instant. La fonctionnalité de failover redirige de manière transparente toutes les requêtes au système injoignable vers le système de secours, lequel imite l'environnement du système initial [42].

Caractéristiques

Cette capacité existe pour tout type d'équipement réseau : du serveur au routeur en passant par les pare-feux et les commutateurs réseau (Switch). Le basculement intervient généralement sans action humaine et même bien souvent sans aucun message d'alerte. Le basculement est conçu pour être totalement transparent [43].
Il existe deux modes principaux de basculement [43] :

actif/actif qui s'apparente plus à de l'équilibrage de charge (load-balancing) ;

Le mode classique couramment répandu, **actif/passif** où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.

3.4.3 La résilience de l'environnement

La résilience de l'environnement peut être divisée en deux parties : l'environnement physique et l'environnement logique [44] :

- Environnement physique : se compose de fonctions de disponibilité adaptées à un système unique et d'utilitaires requis pour la maintenance correcte d'un environnement informatique. Ces fonctions de disponibilité pour système unique sont essentielles pour préserver un environ-

nement à haute disponibilité. Le système comporte de nombreuses fonctions qui le protègent des pannes matérielles. Le premier composant à protéger est le sous-système de disques. RAID 5, RAID 6, RAID 10 et la protection par disque miroir sont les mécanismes de protection possibles ;

- Environnement logique : est l'environnement d'exécution des applications. Il comprend les attributs système, les valeurs système, les attributs de configuration de réseau, la configuration de la gestion des travaux et les profils utilisateur. Ces éléments doivent être identiques sur le système de secours et sur le système principal de production pour assurer un fonctionnement correct de l'environnement d'application.

3.5 Les caractéristiques d'un système à haute disponibilité

La sûreté de fonctionnement d'un système se caractérise par un certain nombre de propriétés [26] :

• **la fiabilité (reliability)** qui correspond à la continuité du service rendu. C'est une caractéristique commune des systèmes dits critiques tels que les systèmes de contrôle des vols aériens (au sol ou embarqués), les systèmes d'échanges monétaires, les systèmes de contrôle militaires... ;

• **la disponibilité (availability)** qui correspond à l'aptitude du système à être prêt à rendre le service pour lequel il a été conçu. La disponibilité d'un système dépend non seulement des caractéristiques du système mais aussi de celles de sa maintenance ;

• **la maintenabilité (maintenability)** est l'aptitude d'un système à être maintenu en condition opérationnelle ; c'est aussi l'aptitude du système à recevoir des réparations et des modifications, éventuellement en phase opérationnelle ;

• **l'innocuité (safety)** ou encore sécurité vis-à-vis de l'environnement qui correspond à l'absence d'occurrences de phénomènes ayant des conséquences non désirées sur l'environnement du système ; c'est une propriété à laquelle les utilisateurs sont de plus en plus sensibles ;

• **L'immunité (immunity)** qui correspond à la résistance d'un système aux agressions externes.

3.6 Mesure de la haute disponibilité

La disponibilité s'exprime la plupart du temps sous la forme de taux de disponibilité, exprimé en pourcentage, en ramenant le temps de disponibilité sur le temps total [17].

Le tableau suivant présente le temps d'indisponibilité (en anglais downtime) sur une base d'une année (365 jours) en fonction du taux de disponibilité [17] :

Taux de disponibilité	**Durée d'indisponibilité**
97%	11 jours
98%	7 jours
99%	3 jours et 15 heures
99,9%	8 heures et 48 minutes
99,99%	53 minutes
99,999%	5 minutes
99,9999%	32 secondes

TABLE 3.1: Le niveau de la disponibilité . [17]

3.7 Les principales sources d'indisponibilité

3.7.1 Arrêt planifiée

La maintenance planifiée signifie que le système doit être arrêté pour permettre l'exécution de mises à niveau d'applications, de logiciels et de matériels. Lorsque les horaires d'activité rendent impossible la programmation de la maintenance planifiée, l'implémentation d'une solution à haute disponibilité permettant la maintenance hors ligne peut être envisagée. Avec la maintenance hors ligne, le système de secours est mis à niveau en premier. Lorsque l'environnement de production est basculé vers le système mis à niveau, l'ancien système de production est alors mis à niveau à son tour [44].

3.7.2 Arrêts non planifiés

Un arrêt non planifié est un temps d'indisponibilité survenant pendant les horaires d'activité. Il peut être du à une erreur humaine, à des échecs d'applications ou de logiciels, à des pannes matérielles ou des défaillances d'utilitaires, et a pour conséquence un arrêt du système de production. La solution à haute disponibilité vous donne la possibilité de basculer l'environnement de production vers un système de secours [44].

3.8 Les protocoles de redondance

la redondance informatique concerne principalement la sécurité des centres de données et la disponibilité des systèmes. Il s'agit de données et de composants système en plusieurs exemplaires, qui existent en parallèle, en double ou en miroir et sont disponibles à profusion. Selon le contexte informatique, elle peut être connotée de manière aussi bien positive que négative. Au sens positif du terme, la redondance désigne les multiples ensembles de données critiques enregistrés ou répartis

sur plusieurs serveurs.au sens négatif du terme, la redondance désigne plutôt les « doublons » de données involontaires qui vous font perdre en espace de stockage [46].
parmi les protocoles de redondance, on trouve :

3.8.1 VRRP (Virtual Router Redundancy Protocol)

Le protocole VRRP (Virtual Router Redundancy Protocol) est un protocole de gestion de réseau utilisé pour augmenter la disponibilité des hôtes de service de passerelle par défaut sur le même sous-réseau. VRRP améliore la fiabilité et les performances du réseau hôte en permettant à un routeur virtuel d'agir comme passerelle par défaut pour ce réseau.

VRRP est spécialement conçu pour permettre le routage, le transfert et la commutation de données parmi un pool de routeurs virtuels. VRRP a été créé pour résoudre le problème des adresses statiques, qui s'avéraient inefficaces lorsque la route ou le chemin n'était pas disponible [47].

3.8.2 HSRP (Hot Standby Router Protocol)

HSRP, Host Standby Router Protocol est un protocole de redondance du premier saut (FHRP, First Hop redundancy Protocols), propriétaire Cisco. De multiples passerelles de réseau local s'entendent sur une adresse IP virtuelle et élisent un routeur "Active" qui prend en charge le trafic comme passerelle par défaut en répondant au trafic ARP. Un autre routeur reste en état "Standby" alors que tous les autres sont en état "Listen". HSRP converge endéans les dix secondes par défaut en Cisco IOS. Ses messages sont transportés dans des messages embarqués dans de l'UDP 1985 [48].

3.8.3 GLBP (Gateway LoadBlancing Protocol)

Gateway Load Balancing Protocol est un protocole propriétaire Cisco qui permet de faire de la redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles .

Le protocole GLBP élit un Active Virtual Gateway (AVG) qui va répondre aux requêtes ARP pour l'adresse IP virtuelle. GLBP permet de donner un poids variable à chacun des routeurs participants pour la répartition de la charge entre ces routeurs. La charge est donc répartie par hôte dans le sous-réseau [49].

Fonctionnement de GLBP

Tous les routeurs du groupe GLBP participent activement au routage alors que dans VRRP ou HSRP, il n'y en a qu'un qui est en mode actif, tandis que les autres patientent. Plus concrètement, à l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus haute adresse IP

du groupe prendra le statut de « AVG » (active virtual gateway). Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP. C'est d'ailleurs le Routeur AVG qui va assigner les adresses MAC virtuelles aux routeurs du groupe, Ainsi ils ont le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de backup en cas de défaillance des AVF [49].
La figure suivante (figure 3.5) montre et explique le fonctionnement du protocole GLBP :

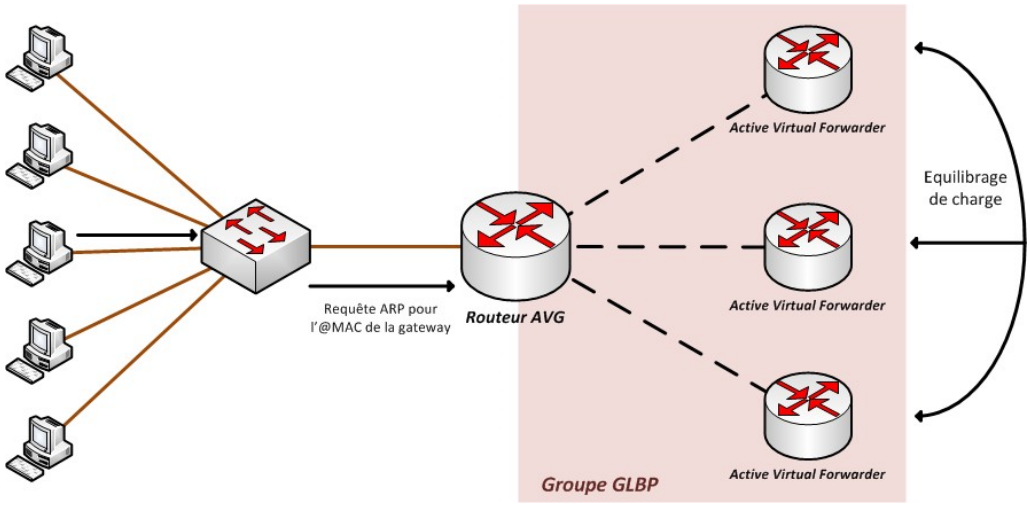

FIGURE 3.5 – schéma illustrant le fonctionnement du protocole GLBP . [49]

3.8.4 STP (Spanning-Tree Protocol)

Le protocole STP (Spanning Tree Protocol) est un protocole de gestion de liaison qui empêche les boucles de pont de contrôle d'accès au support (MAC) et les retards de diffusion sur tout réseau local (LAN). Les boucles de pont sont des boucles de réseau créées par plusieurs chemins de station actifs. STP est un protocole de couche liaison de données normalisé par l'Institut des ingénieurs électriciens et électroniciens (IEEE) 802.1D.

Le protocole Spanning Tree permet aux concepteurs de réseaux de maintenir la redondance automatique des chemins en cas de défaillance de la liaison active, tout en empêchant les boucles de pont. Les boucles de pont se produisent lorsque plusieurs ordinateurs d'un réseau tentent de répondre à un signal, ce qui peut entraîner une saturation du réseau. STP détermine quelle machine doit recevoir - et donc répondre à - chaque signal entrant. Le protocole Spanning Tree a été remplacé par le protocole Rapid Spanning Tree (RSTP) en 2001. RSTP est beaucoup plus rapide que STP, mais conserve toujours une compatibilité descendante avec le protocole d'origine [49].

3.8.5 VTP

Le protocole VTP (VLAN Trunking Protocol) est un protocole de gestion de VLAN utilisé dans les réseaux informatiques. Il permet la propagation des informations VLAN à tous les équipements du réseau, facilitant ainsi la gestion des VLAN dans un réseau étendu. Le protocole VTP (VLAN Trunking Protocol) permet une gestion centralisée des VLAN dans un réseau étendu. Il est important de comprendre les différents modes de configuration pour assurer une gestion efficace et sécurisée des VLAN.

• **Le mode ‘’SERVEUR ‘’** permet un contrôle total pour la création, suppression et renommage des VLAN dans le domaine. il peut y avoir plusieurs switchs en mode ‘’ serveur” dans un domaine VTP, permettant une gestion centralisée et cohérente des VLAN.

• **Le mode ‘’client”** ne permet pas de créer, supprimer ou renommer des VLAN, mais il apprend les créations et les modifications de VLAN du serveur VTP. Il relaie également des trames VTP par tous ses autres ports trunks.

• **Le mode ‘’transparent”** ne crée ni ne supprime de VLAN, mais relaie les informations provenant du serveur VTP vers ses ports trunks. Dans le cas de VTP v1, il relaie uniquement si le domaine et la version VTP sont respectés. Dans le cas VTP v2/3, il relaie les informations en toute circonstance.

• **Le mode ‘’OFF ‘’** ignore complétement le VTP et est disponible uniquement avec le VTP version 3. Cela peut être utile dans des scénarios ou le VTP n'est pas nécessaire ou s'il est désactivé pour des raisons de sécurité.[50]

3.9 Les systèmes de clustering

3.9.1 Définition

Les systèmes de clustering sont une combinaison de clusters matérielles et de clusters logicielles. Les clusters matériels permettent de partager des disques à haute performance entre les systèmes. Les clusters logiciels permettent à tous les systèmes de fonctionner ensemble.
Le clustering est généralement utilisé pour fournir un service à haute disponibilité, c'est-à-dire un service qui continuera même si un ou plusieurs systèmes du cluster échouent. Généralement, on obtient une haute disponibilité en ajoutant un niveau de redondance dans le système [51].

3.9.2 Avantage

La grappe de serveurs offre de nombreux avantages en informatique. Elle permet d'offrir une disponibilité totale, une répartition des charges et des fonctionnalités des calculs parallèles. Le cluster permet de simplifier la montée en charge, mais également la gestion des ressources (mémoire vive, bandes passantes, disques durs, processeurs...) [51].

3.9.3 Fonctionnement

En règle générale, une grappe de serveurs est constituée de nœuds de calcul, de nœuds de stockage de nœuds frontaux. On compte parfois des nœuds additionnels dédiés au monitoring. Les nœuds sont reliés entre eux par plusieurs réseaux. Les tâches d'administration comme le chargement des systèmes sur les nœuds, le suivi et la mesure de charge sont généralement pris en charge par le réseau dont le débit est le plus lent. Le second réseau, dont la bande passante est largement supérieure, se joint au premier réseau. Son débit peut atteindre 40 Gigabits par seconde. Il repose sur des technologies comme Quadrics, Myrinet et Infiniband.
Les programmes exécutés sur les clusters de serveurs reposent sur une API standard : Message Passing Interface. Cette API assure la communication entre les divers processus répartis sur les nœuds par le biais de messages. En cas de défaillance de l'un des serveurs, le logiciel de clustering isole le système en question. Lorsque les ressources sont partagées entre plusieurs tâches, si un serveur est surchargé, les tâches sont partagées avec un autre serveur.
Au sein d'une grappe de serveurs, chaque serveur possède et gère ses propres appareils locaux et repose sur une copie du système d'exploitation, des applications et des services qu'il gère. Les appareils communs de la grappe, comme les disques et le média de connexion permettant d'accéder à ces disques, sont détenus et gérés par un seul serveur à la fois [52].

3.9.4 Types de systèmes de clustering

Il existe principalement deux types de systèmes de clustering, à savoir le système de clustering asymétrique et le système de clustering symétrique [53] :

• **Dans le clustering asymétrique**, une machine est en mode de secours (tandis que l'autre exécute les applications. La machine hôte de secours (hot-standby) ne fait que surveiller le serveur actif. Si ce serveur tombe en panne, l'hôte de secours devient le serveur actif ;

• **Dans le clustering symétrique**, deux hôtes ou plus exécutent des applications et se surveillent mutuellement. Cette structure est évidemment plus efficace, car elle utilise tout le matériel disponible. Cependant, elle exige que plus d'une application soit disponible pour fonctionner.

3.10 Conclusion

Dans ce chapitre, nous avons abordé les notions de base de la haute disponibilité ainsi que les systèmes de clustering.

Chapitre 4

Réalisation, simulation et test

4.1 Introduction

Dans le but d'éclaircir et de compléter ce qui a été traité auparavant, à travers ce chapitre nous allons présenter le simulateur Graphical Network Simulator ainsi que la VMWARE qui nous permettront d'effectuer les configurations nécessaires, et les tests dans l'intention d'arriver à notre objectif principal qui est la mise en place d'un cluster haute disponibilité avec équilibrage de charge.

Présentation de l'environnement de travail

L'environnement de travail désigne l'ensemble des conditions matérielles et humaines qui composent le cadre du travail.

4.2 Partie logiciels

4.2.1 Présentation du simulateur GNS3 (Graphical Network Simulator)

GNS3 (Graphical Network Simulator en anglais) est une application qui permet de simuler graphiquement et avec précision des réseaux informatiques. Ce logiciel libre est distribué gratuitement. Ce dernier est utilisé par de grandes sociétés et organisations. GNS3 autorise la combinaison de modules réels et virtuels. Il est associé au logiciel d'émulation Dynamips pour simuler le système d'exploitation pour la connexion des réseaux Cisco IOS. Il prend en charge également des outils comme VirtualBox, WMWare... Le logiciel supporte une grande variété de commutateurs et de routeurs de marques différentes. GNS3 permet de préparer avantageusement aux épreuves relatives aux certifications Cisco et Juniper [54].

FIGURE 4.1 – Gns3.
[54]

4.2.2 Présentation de VMWARE

VMware Workstation est une solution logicielle professionnelle, puissante et complète qui vous permettra de gérer l'ensemble de vos machines virtuelles locales ou sur le réseau. La solution ultime de virtualisation pour émuler et gérer plusieurs systèmes d'exploitation [55].

FIGURE 4.2 – VMware Workstation.
[55]

4.3 Partie hardware

4.3.1 Pare-feu FortiGate

FortiGate est une gamme de boitiers de sécurité UTM (appliance sécurité tout en un) comprenant les fonctionnalités firewall, Antivirus, système de prévention d'intrusion (IPS), VPN (IPSec et SSL), filtrage Web, Antispam et d'autres fonctionnalités : QoS, virtualisation, compression de données, routage, policy routing ...etc. Les récents modèles comportent des ports accélérés par ASIC qui permettent d'optimiser le trafic au niveau des ports. Les boitiers de cette gamme sont iso fonctionnels s'adaptant à chaque besoin depuis la TPE avec la famille des FG50 jusqu'à l'opérateur avec le FG5000, en passant par les FG110C, FG310B, FG620B pour les moyennes et grosses entreprises. Une sécurité ultra-rapide, de bout en bout [56].

FIGURE 4.3 – FortiGate.
[57]

4.3.2 Les équipements utilisés dans l'architecture

Le tableau suivant, montre les équipements utilisés afin de réaliser notre architecture, ainsi que leurs images.

Les équipements	Les images
Pare-feu FortiGate	FortiOS
Switchs Coeur	IOU L2
Switch d'accés	IOU L2
Switch distribution	IOU L2
Serveur Windows	Windows Server 2022

TABLE 4.1: Tableau des équipements utilisés dans l'architecture proposée

4.4 Partie software

4.4.1 Windows server 2022

Windows Server 2022 est l'actuel système d'exploitation commercialisé par Microsoft et destiné aux serveurs, sorti en août 2021 [58].

4.4.2 Windows 10

Windows 10 est le dernier système d'exploitation de Microsoft, qui ramène de nombreuses fonctionnalités perdues des éditions précédentes et introduit des fonctionnalités longuement attendues qui étaient déjà disponibles sur les logiciels rivaux depuis un bon moment déjà [59].

FIGURE 4.4 – Windows 10.
[59]

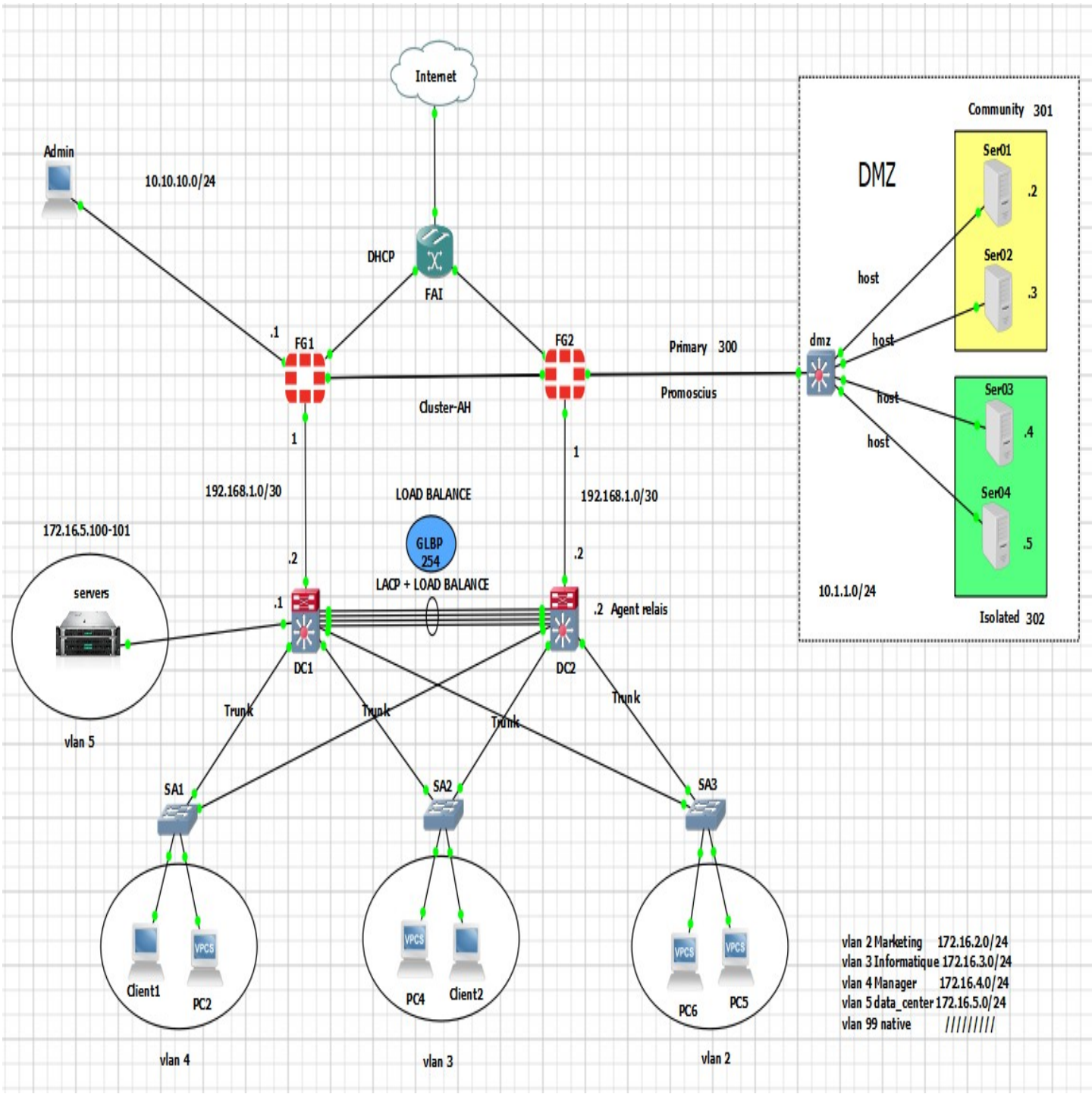

FIGURE 4.5 – Architecture proposée.

4.6 Plan d'adressage

4.6.1 Tableau d'adressage des VLANs

Les VLANs que nous avons proposés pour la RTC sont illustrés dans le tableau suivant, ainsi que les adresses IP.

VLAN ID	Nom du VLAN	Adresse IP
2	Marketing	172.16.2.0/24
3	Informatique	172.16.3.0/24
4	Manager	172.16.4.0/24
5	data_center	172.16.5.0/24
99	native	/

TABLE 4.2: Tableau d'adressage des VLANs.

4.6.2 Tableau d'adressage des équipements

Le tableau ci-dessous, montre l'attribution des adresses IP aux interfaces des différents équipements de l'architecture réseau proposée :

Equipements	Interface	Adresse IP
Switch CORE-DISTRIBUSON(DC1)	Gi0/0	192.168.1.2/30
	Gi0/1	Encapsulation dot1Q
	Gi0/2	Encapsulation dot1Q
	Gi0/3	Encapsulation dot1Q
	Po2	Encapsulation dot1Q
Switch CORE-DISTRIBUSON(DC2)	Gi0/0	192.168.1.2/30
	Gi0/1	Encapsulation dot1Q
	Gi0/2	Encapsulation dot1Q
	Gi0/3	Encapsulation dot1Q
	Po2	Encapsulation dot1Q
Switch ACCES(SA1)	E0/0 E0/1	Encapsulation dot1Q
Switch ACCES(SA2)	E0/0 E0/1	Encapsulation dot1Q
Switch ACCES(SA3)	E0/0 E0/1	Encapsulation dot1Q
Pare-feu FortiGate(FG1)	Port2 Port4 Port10	192.168.1.1/30 10.1.1.1/24 10.10.10.1/24
Pare-feu FortiGate(FG2)	Port2 Port4 Port10	192.168.1.1/30 10.1.1.1/24 10.10.10.1/24

TABLE 4.3: Tableau d'adressage des équipements.

4.7 Configuration des équipements

Commençant par la configuration des commutateurs qui se réalisera au niveau de la console de chacun d'entre eux,en introduisant des commandes spécifiques. Dans ce qui suit, nous allons présenter un exemple de chaque configuration qui nous permettra de mettre en œuvre l'architecture proposée.

4.7.1 Configuration de base

Elle consiste à effectuer ces configurations suivantes dans le mode de configuration globale des périphériques qu'on accède avec la commande « configure terminal » ou « conf t » :

— **Configuration du hostname et sécurisation du port console :**

Le port console d'un équipement sert à relier directement ce dernier à une station d'administration en utilisant un câble console pour effectuer sa configuration de base. Donc, il est très important de sécuriser le port console de tous les équipements pour empêcher tout accès à ces équipements, évidement lorsqu'il est définitivement installé sur dans une armoire de brassage.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname DC1
DC1(config)#line console 0
DC1(config-line)#password sonatrach
DC1(config-line)#login
DC1(config-line)#exit
DC1(config)#exit
DC1#
*Jun 24 07:46:39.309: %SYS-5-CONFIG_I: Configured from console by console
DC1#wr
Building configuration...
```

FIGURE 4.6 – Configuration du hostname et sécurisation du port console au niveau du switch cœur "DC1".

— **Sécurisation du mode Enable :**
Par ailleurs, le mode Enable sert d'un portail pour accéder à l'ensemble des modes de configuration des équipements géré. D'où la nécessité absolue de devoir sécurisé cette CLI pour empêcher tout affichage d'informations critiques ou tout changement de configuration de l'équipement administré.

```
DC1#enable
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#enable password sonatrach
DC1(config)#exit
DC1#
*Jun 24 07:47:37.362: %SYS-5-CONFIG_I: Configured from console by console
DC1#wr
Building configuration...
```

FIGURE 4.7 – sécurisation du mode Enable au niveau du switch cœur "DC1".

— **Configuration du SSH :**

SSH est parmi les configurations de base à effectuer, grâce à ces outils d'accès à distance, l'administrateur réseau pourra administrer à distance ses équipements.

```
DC1>enable
Password:
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#username sonatrach password sonatrach
DC1(config)#ip domain-name sonatrach.com
DC1(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
DC1(config)#crypto key generate rsa
The name for the keys will be: DC1.sonatrach.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: line vty 0 4
% A decimal number between 360 and 4096.
How many bits in the modulus [512]: transport input ssh
% A decimal number between 360 and 4096.
How many bits in the modulus [512]: login local
% A decimal number between 360 and 4096.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

DC1(config)#
*Jun 25 13:06:48.881:  RSA key size needs to be atleast 768 bits for ssh version 2
*Jun 25 13:06:48.889: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

FIGURE 4.8 – Configuration du SSH au niveau du switch cœur "DC1".

— **Bannière :**

```
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#banner motd c ACCES INTERDIT AU PERSONNES NON AUTORISEES c
DC1(config)#exit
DC1#
*Jun 24 07:48:36.442: %SYS-5-CONFIG_I: Configured from console by console
DC1#WR
Building configuration...
```

FIGURE 4.9 – Configuration de la bannière au niveau du switch cœur "DC1".

4.7.2 Configurations des interfaces trunks

Les liens en mode trunk représentent les liaisons entre les commutateurs ou entre un commutateur et un routeur. Les interfaces à configurer dans ce cas sont les liaisons entre l'ensemble des commutateurs de la couche d'accès et le commutateur cœur.

— **Le switch cœur**

```
DC1#enable
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#interface range gigabitEthernet 0/1-3,gigabitEthernet 3/0-3
DC1(config-if-range)#switchport trunk encapsulation dot1q
DC1(config-if-range)#switchport mode trunk
DC1(config-if-range)#switchport trunk native vlan 99
DC1(config-if-range)#switchport trunk allowed vlan 2-5,99
DC1(config-if-range)#end
DC1#wr
```

FIGURE 4.10 – Configuration des liens trunk au niveau du switch cœur "DC1".

— **Le switch d'accès**

```
SA1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SA1(config)#interface range ethernet 0/0-1
SA1(config-if-range)#switchport trunk encapsulation dot1q
SA1(config-if-range)#switchport mode trunk
SA1(config-if-range)#switchport trunk native vlan 99
SA1(config-if-range)#switchport trunk allowed vlan 2-5,99
```

FIGURE 4.11 – Configuration des liens trunk au niveau du switch d'accès "SA1".

4.7.3 Configuration du protocole VTP

Le serveur VTP : Il permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs clients du réseau. Il sera configuré au niveau du switch cœur.

```
DC1#enable
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#vtp mode server
Device mode already VTP Server for VLANS.
DC1(config)#vtp password sonatrach123
Password already set to sonatrach123
DC1(config)#vtp domain sonatrachvtp
Domain name already set to sonatrachvtp.
DC1(config)#vtp version 2
VTP version is already in V2.
DC1(config)#vtp pruning
Pruning already switched on
DC1(config)#end
DC1#wr
```

FIGURE 4.12 – Configuration du serveur VTP au niveau du switch cœur "DC1".

- Les clients VTP :

La configuration des clients VTP sera au niveau de tous les commutateurs de couche accès (switch d'accès) du réseau LAN.

```
SA1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SA1(config)#vtp password sonatrach123
Setting device VTP password to sonatrach123
SA1(config)#vtp domain sonatrachvtp
Changing VTP domain name from NULL to sonatrachvtp
SA1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SA1(config)#end
SA1#wr
Building configuration...
```

FIGURE 4.13 – Configuration du client VTP au niveau du switch d'accès "SA1".

4.7.4 Création des VLANs

La configuration des VLANs est faite au niveau du commutateur de la couche coeur c'est-à-direle switch cœur du réseau.

```
DC1#enable
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#vlan 2
DC1(config-vlan)#name Marketing
DC1(config-vlan)#vlan 3
DC1(config-vlan)#name Informatique
DC1(config-vlan)#vlan 4
DC1(config-vlan)#name Manager
DC1(config-vlan)#vlan 5
DC1(config-vlan)#name data_center
DC1(config-vlan)#vlan 99
DC1(config-vlan)#name native
DC1(config-vlan)#end
DC1#wr
```

FIGURE 4.14 – Création des VLANs au niveau du switch cœur "DC1".

4.7.5 Configuration des interfaces Access

Les ports auxquels nous connectons des PCs, sont dits des ports Access. Ces ports vont être assignésaux différents VLANs existants qui sont configuré sur tous les commutateurs d'accès.

```
SA1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SA1(config)#interface range ethernet 3/1-2
SA1(config-if-range)#switchport mode access
SA1(config-if-range)#switchport access vlan 4
SA1(config-if-range)#exit
SA1(config)#
```

FIGURE 4.15 – Configuration des ports access au niveau du switch d'accès "SA1".

4.7.6 Configuration de LACP et LOAD BALANCING

L'utilisation de LACP et la répartition de charge permet de créer des liaisons agrégées redondantes entre le commutateur de niveau 3 et d'autres périphériques réseaux, en distribuant équitablement le trafic entre les interfaces agrégées.

```
DC1>enable
DC1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DC1(config)#interface range gigabitEthernet 3/0-3
DC1(config-if-range)#channel-group 2 mode active
DC1(config-if-range)#exit
DC1(config)#port-channel load-balance src-dst-mac
DC1(config)#end
DC1#wr
```

FIGURE 4.16 – Activation du protocole LACP et le load balance au niveau du switch cœur DC1.

4.7.7 Routage inter-VLANs

La subdivision de l'interface reliant le switch d'accès et le switch cœur, a pour but, d'accomplir la communication entre les différents VLANs (communication entre- VLAN). En effet, subdiviser l'interface en un nombre de sous interfaces, dépendant du nombre de VLAN qui existent, en leur affectant, ainsi, des adresse IP et des masques de sous-réseaux pour chacune d'elles.

```
DC1(config)#ip routing
DC1(config)#interface vlan 2
DC1(config-if)#no shutdown
DC1(config-if)#ip address 172.16.2.1 255.255.255.0
DC1(config-if)#exit
DC1(config)#interface vlan 3
DC1(config-if)#no shutdown
DC1(config-if)#ip address 172.16.3.1 255.255.255.0
DC1(config-if)#exit
DC1(config)#interface vlan 4
DC1(config-if)#no shutdown
DC1(config-if)#ip address 172.16.4.1 255.255.255.0
DC1(config-if)#exit
DC1(config)#interface vlan 5
DC1(config-if)#no shutdown
DC1(config-if)#ip address 172.16.5.1 255.255.255.0
DC1(config-if)#exit
DC1(config)#end
DC1#wr
```

FIGURE 4.17 – Configuration des sub-interfaces au niveau du switch cœur "DC1 ".

4.7.8 Configuration du protocole GLBP

La configuration de GLBP sur un Switch de niveau 3 offre une répartition de charge équilibrée, une redondance et une haute disponibilité pour les passerelles par défaut.

```
DC1(config)#interface vlan 2
DC1(config-if)#glbp 2 ip 172.16.2.254
DC1(config-if)#glbp 2 priority 200
DC1(config-if)#glbp 2 preempt
DC1(config-if)#glbp 2 load-balancing round-robin
DC1(config-if)#glbp 2  authentication text sonatrach
DC1(config-if)#exit
DC1(config)#interface vlan 3
DC1(config-if)#glbp 3 ip 172.16.3.254
DC1(config-if)#glbp 3 priority 200
DC1(config-if)#glbp 3 preempt
DC1(config-if)#glbp 3 load-balancing round-robin
DC1(config-if)#glbp 3  authentication text sonatrach
DC1(config-if)#exit
DC1(config)#interface vlan 4
DC1(config-if)#glbp 4 ip 172.16.4.254
DC1(config-if)#glbp 4 priority 200
DC1(config-if)#glbp 4 preempt
DC1(config-if)#glbp 4 load-balancing round-robin
DC1(config-if)#glbp 4  authentication text sonatrach
DC1(config-if)#exit
DC1(config)#end
DC1#wr
Building configuration...
```

FIGURE 4.18 – Configuration du protocole GLBP au niveau du switch cœur "DC1 ".

4.7.9 Configuration de l'agent relais

On va configurer l'agent DHCP sur les Switch de niveau 3, il est utilisé pour relayer les messages DHCP entre les clients et les serveurs DHCP. Il peut intercepter les requêtes DHCP provenant des clients, les transmettre aux serveurs DHCP appropriés et acheminer les réponses de ces serveurs vers les clients correspondants.

```
DC1(config)#interface vlan 2
DC1(config-if)#ip helper-address 172.16.5.100
DC1(config-if)#ip helper-address 172.16.5.101
DC1(config-if)#exit
DC1(config)#interface vlan 3
DC1(config-if)#ip helper-address 172.16.5.100
DC1(config-if)#ip helper-address 172.16.5.101
DC1(config-if)#exit
DC1(config)#interface vlan 4
DC1(config-if)#ip helper-address 172.16.5.100
DC1(config-if)#ip helper-address 172.16.5.101
DC1(config-if)#exit
DC1(config)#end
DC1#wr
Building configuration...
```

FIGURE 4.19 – Configuration de l'agent relais au niveau du switch cœur "DC1 ".

4.7.10 Configuration de la DMZ et création des vlan de la Dmz

Le mode VTP transparent, est utilisé pour désactiver la propagation automatique des Vlan d'un commutateur. Cette configuration est souvent utilisée pour éviter les problèmes de configuration involontaire ou les modifications indésirables des VLANs dans un réseau. On va affecter les ports

```
dmz#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#vtp mode transparent
Device mode already VTP Transparent for VLANS.
dmz(config)#vlan 300
dmz(config-vlan)#private-vlan primary
dmz(config-vlan)#private-vlan association 301,302
dmz(config-vlan)#exit
dmz(config)#vlan 301
dmz(config-vlan)#private-vlan community
dmz(config-vlan)#exit
dmz(config)#vlan 302
dmz(config-vlan)#private-vlan isolated
dmz(config-vlan)#exit
```

FIGURE 4.20 – Configuration du mode transparent au niveau du switch distribution "dmz ".

aux VLANs de la DMZ :

```
dmz#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#interface range ethernet 0/0-1
dmz(config-if-range)#switchport mode private-vlan promiscuous
dmz(config-if-range)#switchport private-vlan mapping 300 301,302
dmz(config-if-range)#exit
dmz(config)#interface range ethernet 0/2-3
dmz(config-if-range)#switchport mode private-vlan host
dmz(config-if-range)#switchport private-vlan host-association 300 301
dmz(config-if-range)#exit
dmz(config)#interface range ethernet 1/0-1
dmz(config-if-range)#switchport mode private-vlan host
dmz(config-if-range)#switchport private-vlan host-association 300 302
dmz(config-if-range)#exit
dmz(config)#
```

FIGURE 4.21 – Affectation des ports aux VLANs au niveau du switch distribution "dmz ".

4.7.11 Configuration du pare-feu FortiGate

D'abord on configure les interfaces du pare-feu FortiGate au niveau de la console.

```
FG1 # config system interface

FG1 (interface) # edit port10

FG1 (port10) # set mode static

FG1 (port10) # set ip 10.10.10.1/24

FG1 (port10) # set allowaccess ping https http

FG1 (port10) #
```

FIGURE 4.22 – Configuration des interfaces du pare-feu FortiGate.

La prochaine étape consistera à configurer le pare-feu FortiGate que nous avons déjà installé ou la configuration de la page d'authentification est nécessaire : Tout d'abord il faut se rendre dans le site du pare-feu ou une configuration de la page d'authentification est nécessaire au début et ceux en y insérant quelques informations sur l'entreprise suivie du mot de passe avec lequel accédera l'administrateur à FortiGate.

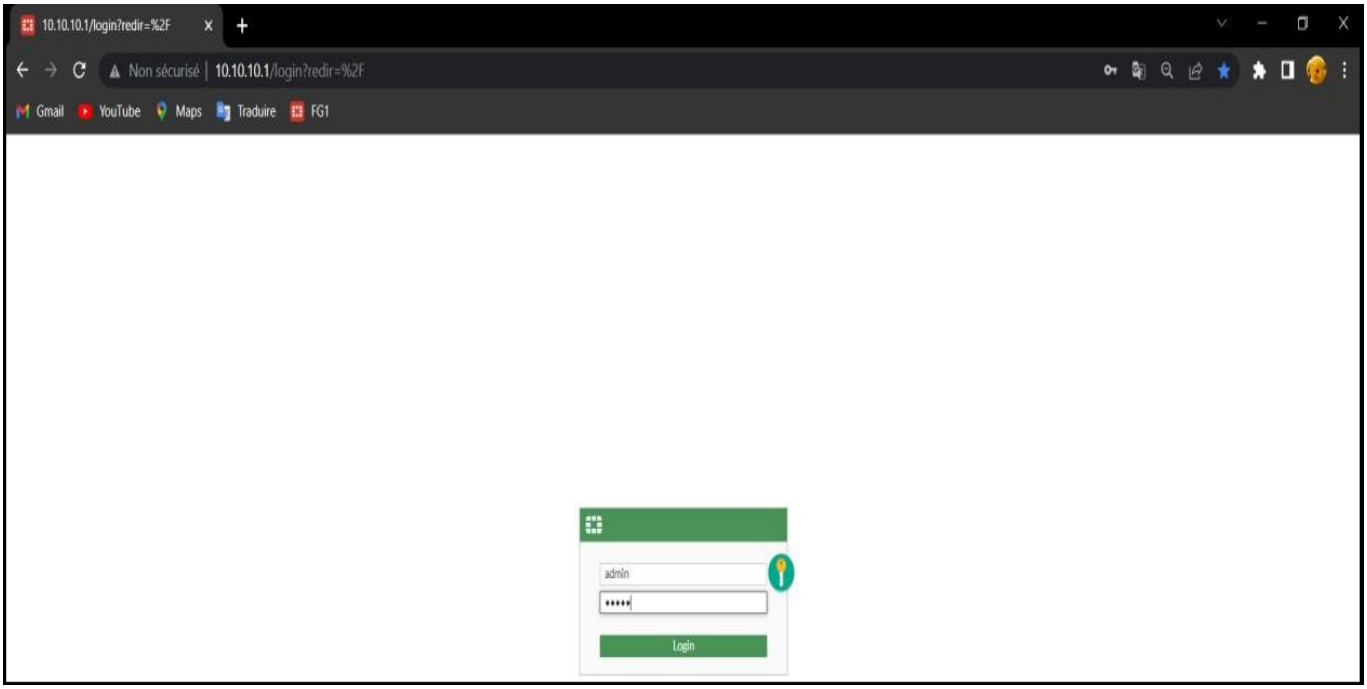

FIGURE 4.23 – L'interface d'authentification de FG1.

Après avoir introduit le mot de passe et le nom d'utilisateur (s'authentifier), l'interface d'accueil s'affichera comme suit :

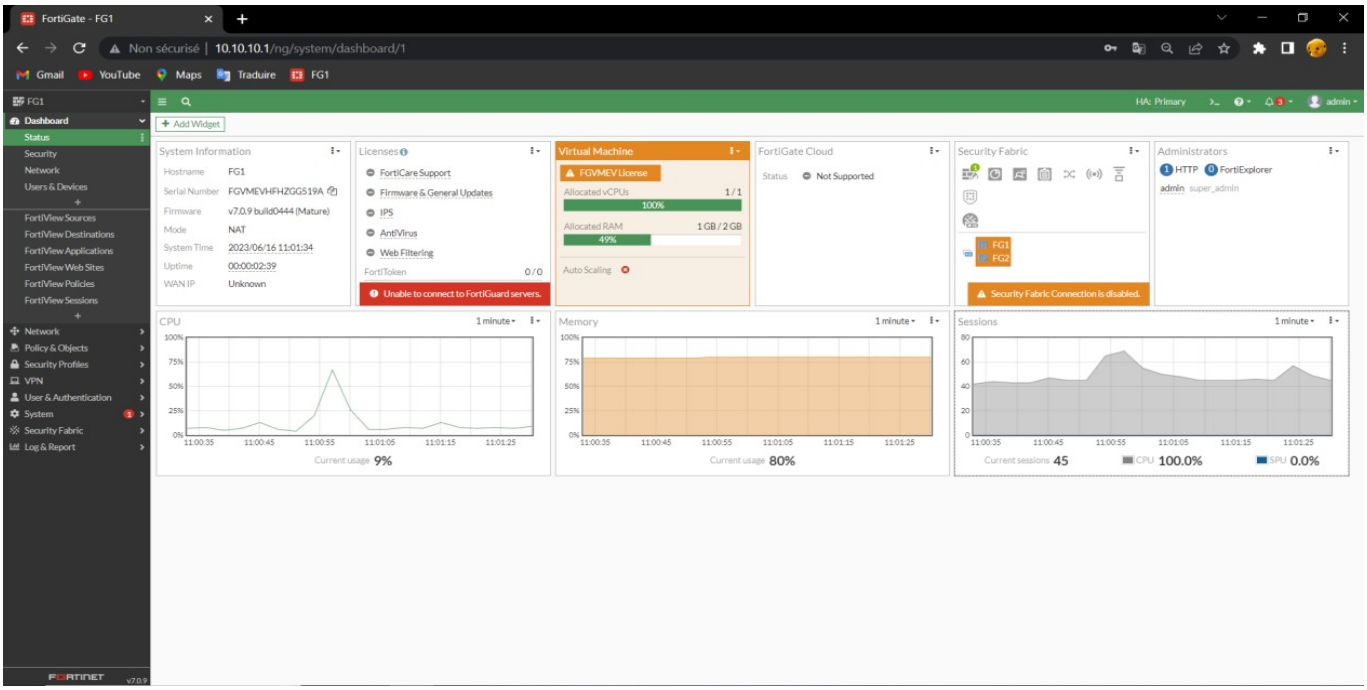

FIGURE 4.24 – L'interface d'accueil de FG1.

Ensuite, nous allons configurer les interfaces du FortiGate FG1

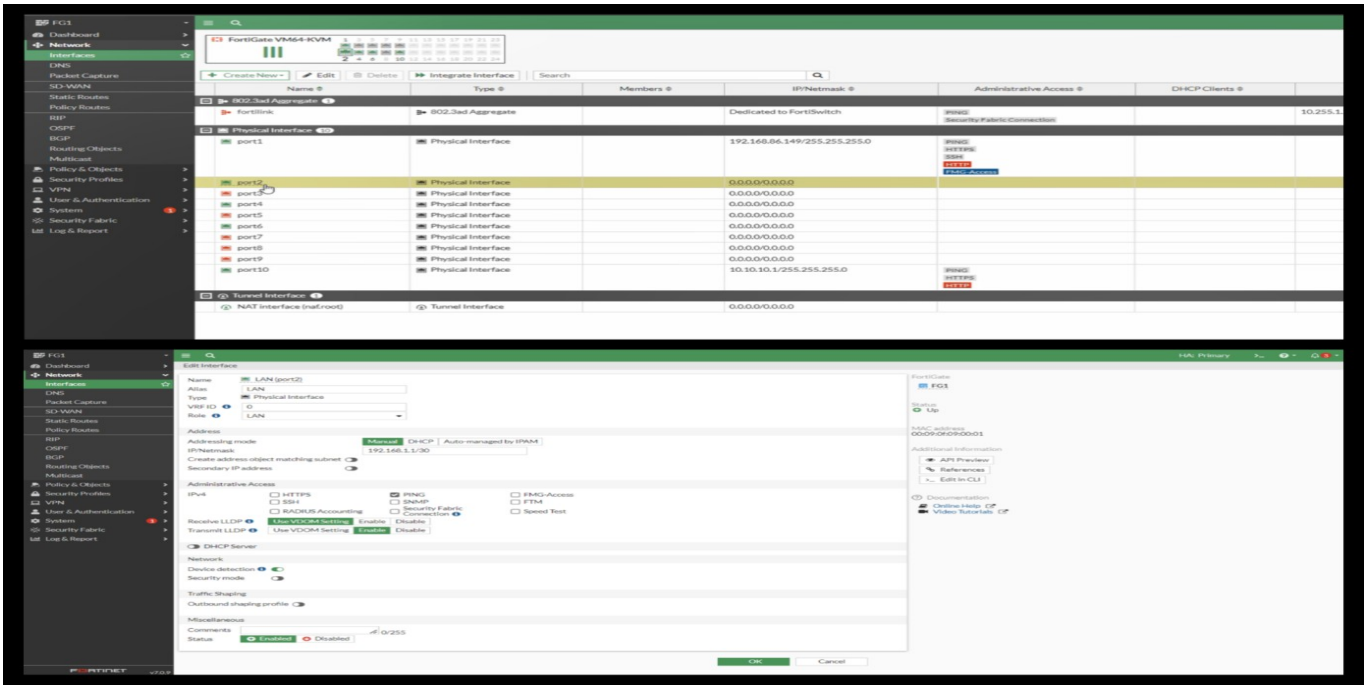

FIGURE 4.25 – Configuration des interfaces du FG1.

On va créer une zone pour interconnecter la DMZ et le LAN par la suite :

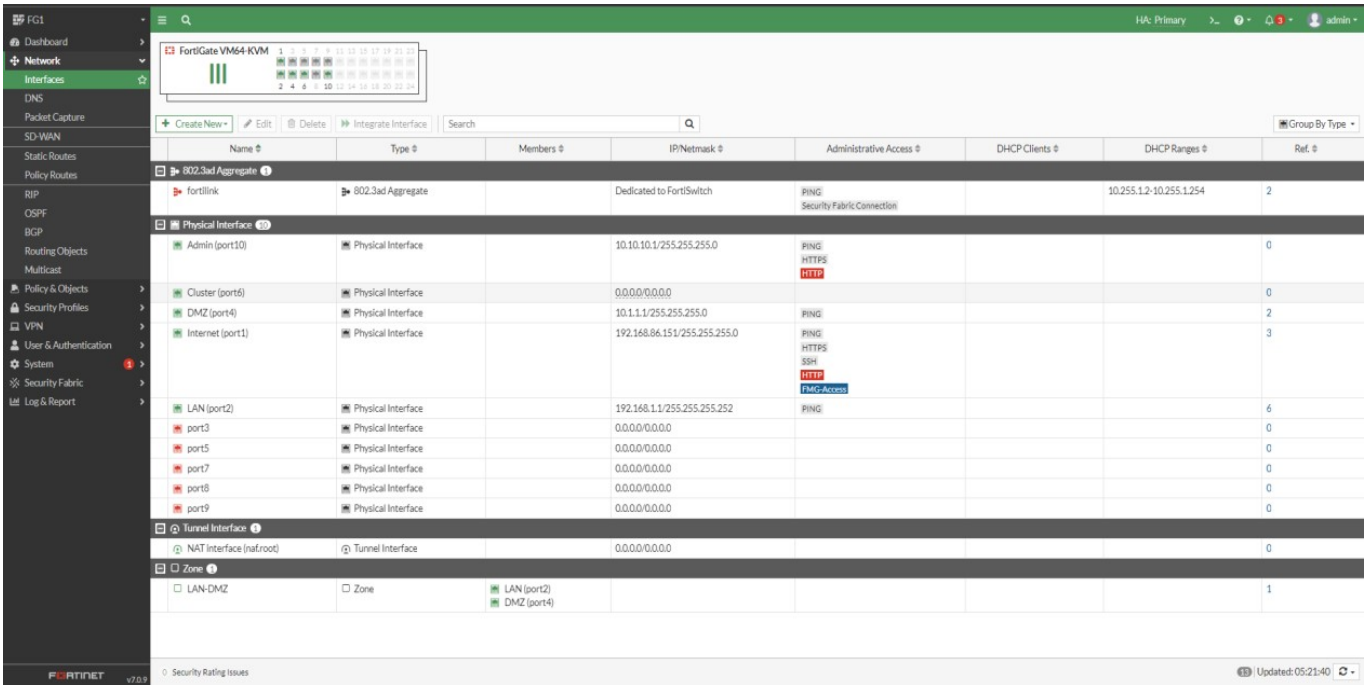

FIGURE 4.26 – Interconnexion de la DMZ et le LAN dans FG1.

Puis, on va router vers les vlan on créant des routes statiques :

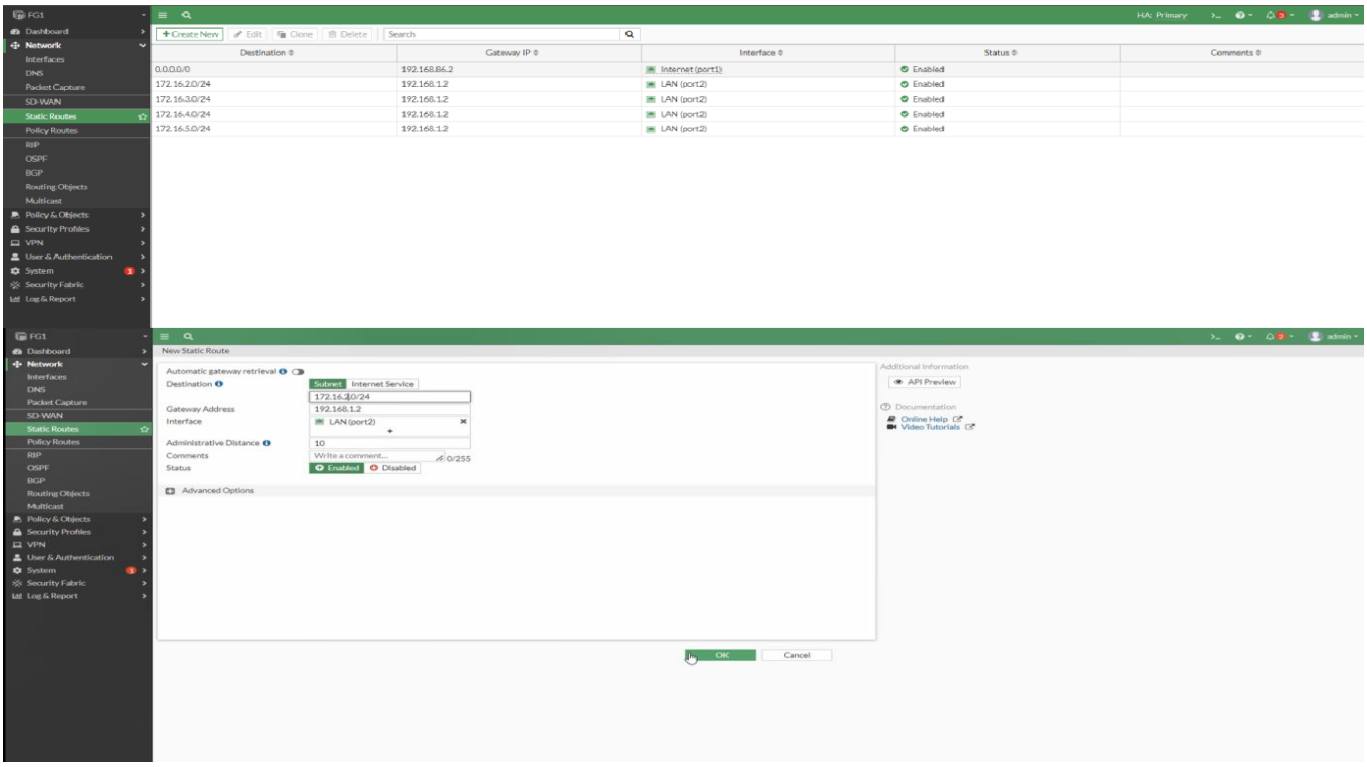

FIGURE 4.27 – Création des routes statiques du FG1.

Apres avoir créé les routes statiques, nous allons configurer la haute disponibilité dans le FG1 :

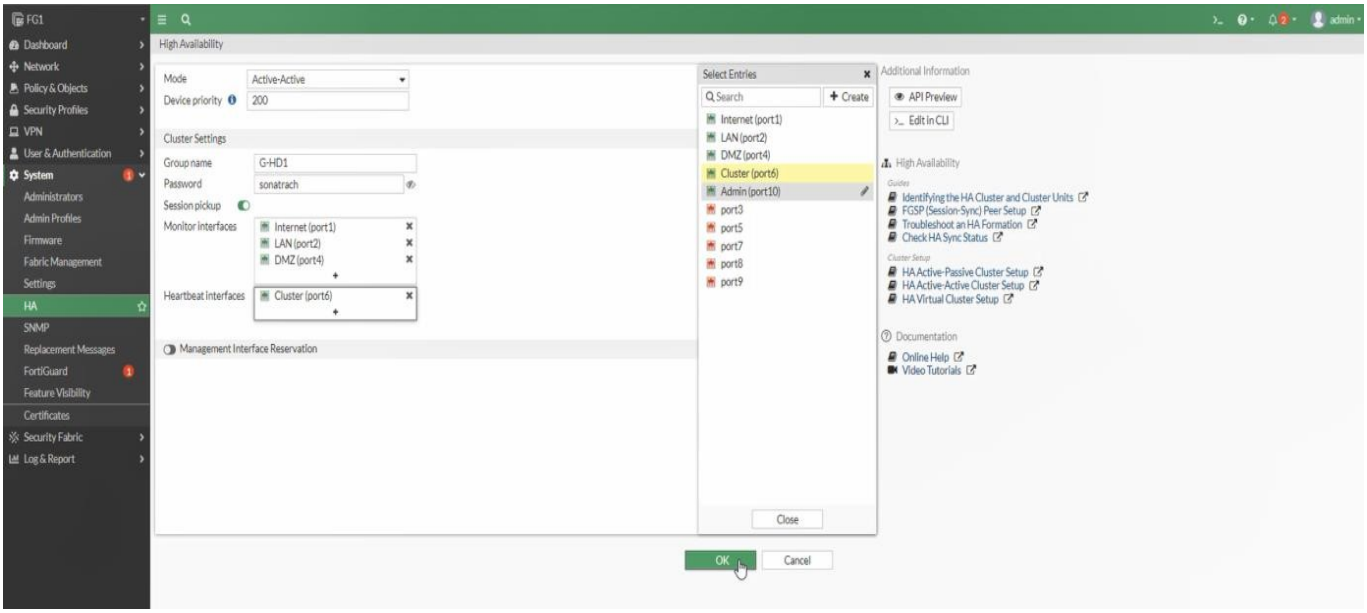

FIGURE 4.28 – Configuration de la haute disponibilité FG1.

Nous allons configurer la haute disponibilité sur FG2 par la ligne de commande CLI :

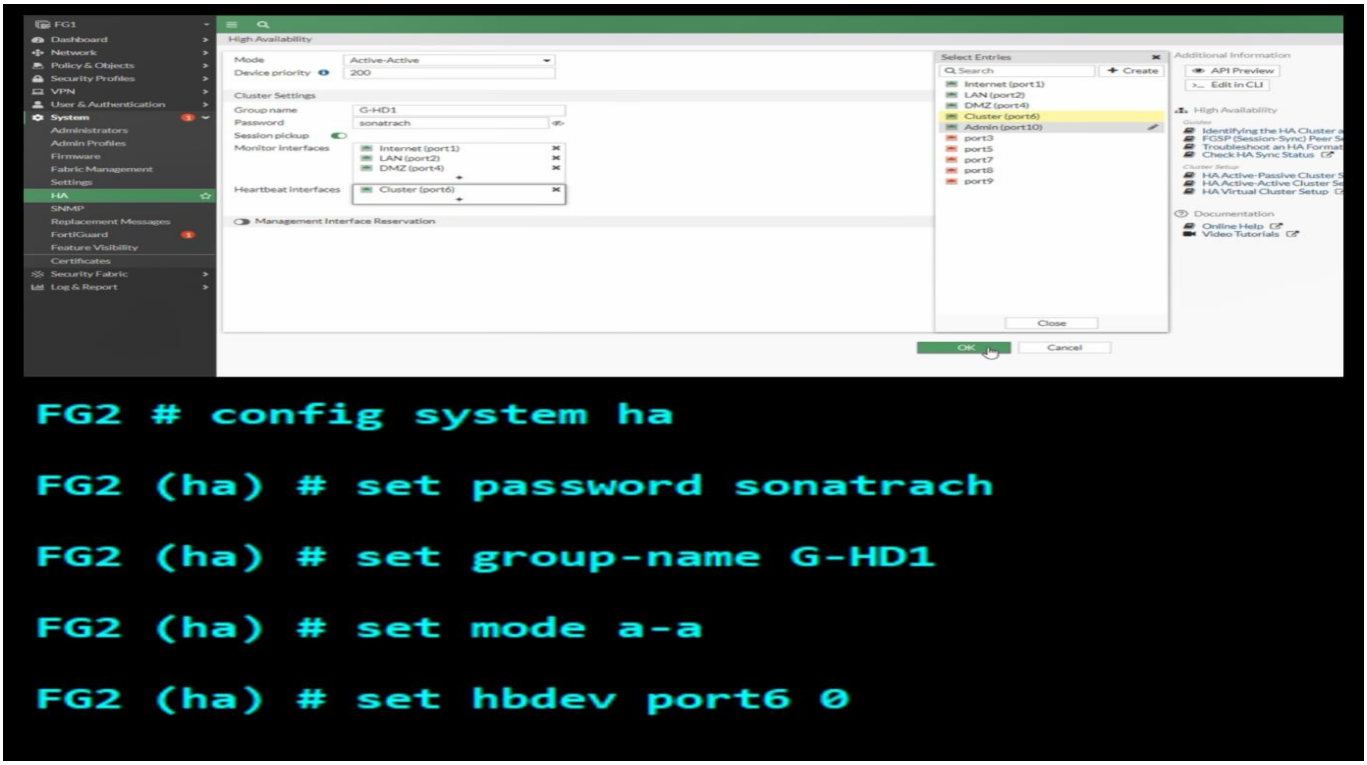

FIGURE 4.29 – Configuration de la haute disponibilité sur FG2.

Après la configuration de la haute disponibilité sur les deux FortiGate , on actualisera et on aura les deux FortiGate synchroniser :

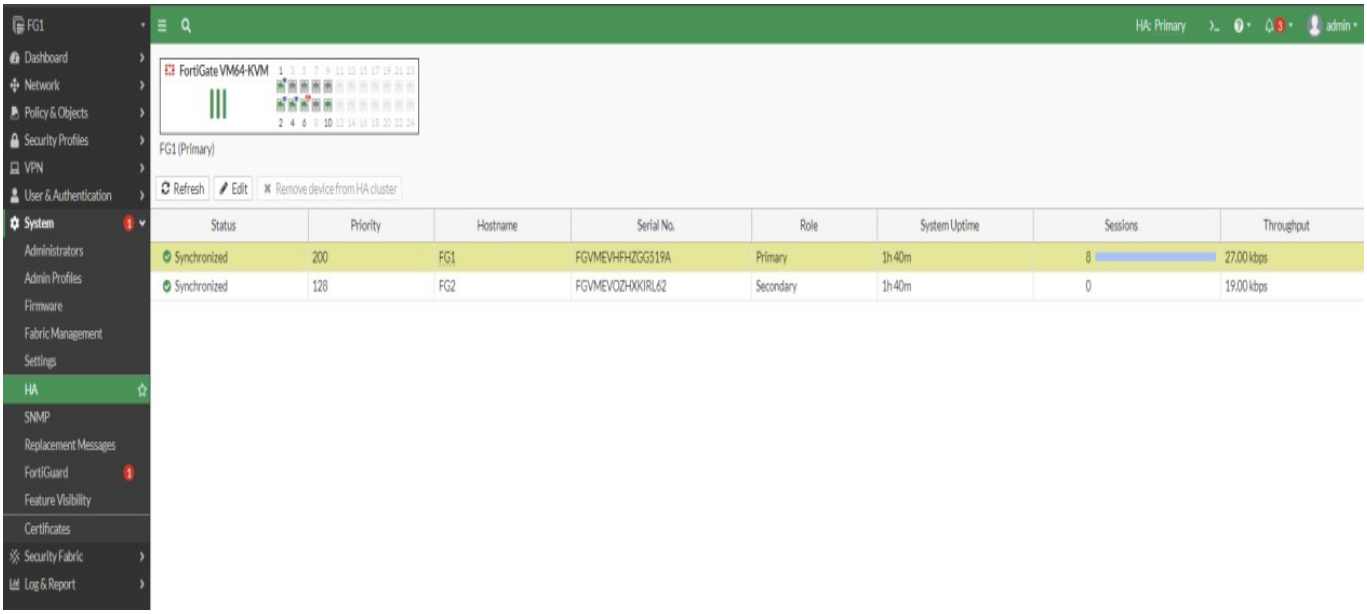

FIGURE 4.30 – Synchronisation de FG1 et FG2.

Configuration de l'interface entre les FortiGate et les commutateurs de Switch niveau 3 :

```
DC1(config)#interface gigabitEthernet 0/0
DC1(config-if)#no switchport
DC1(config-if)#ip address 192.168.1.2 255.255.255.252
DC1(config-if)#no shutdown
DC1(config-if)#description /// fortigate ///
DC1(config-if)#end
DC1#wr
```

FIGURE 4.31 – Configuration de l'interface du DC1.

4.7.12 Configuration des serveurs du cluster DHCP

Après avoir installé l'AD sur les serveurs, on va promouvoir le serveur SER01 en contrôleur de domaine, pour faire on va créer une forêt « sonatrach.dz » :

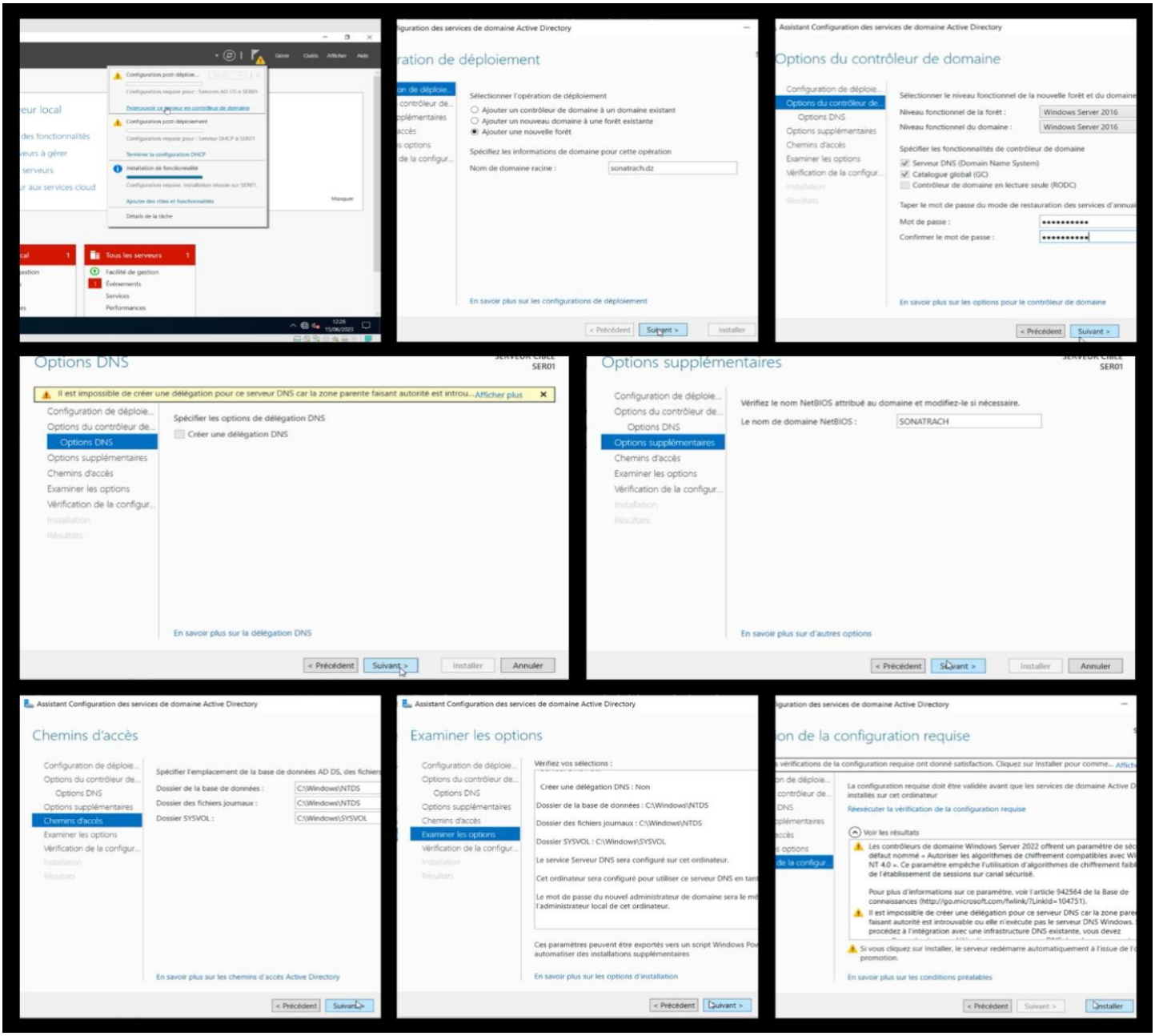

FIGURE 4.32 – Promouvoir du serveur SER01 en contrôleur de domaine.

Ensuite, on va relier le serveur SER02 au même nom de domaine que SER01, on a :

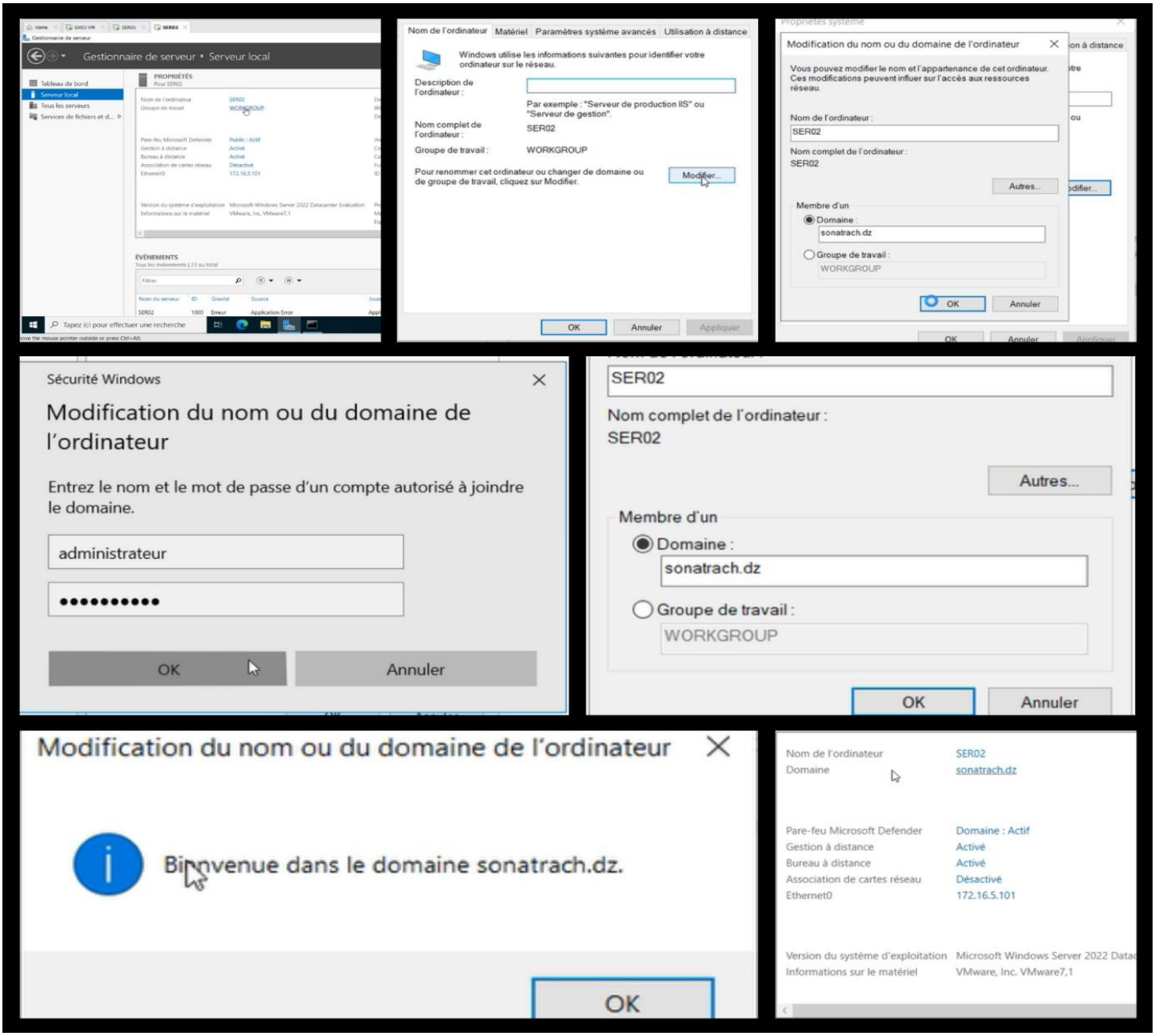

FIGURE 4.33 – Relier le serveur SER02 au même nom de domaine que SER01.

On va répliquer le cluster :

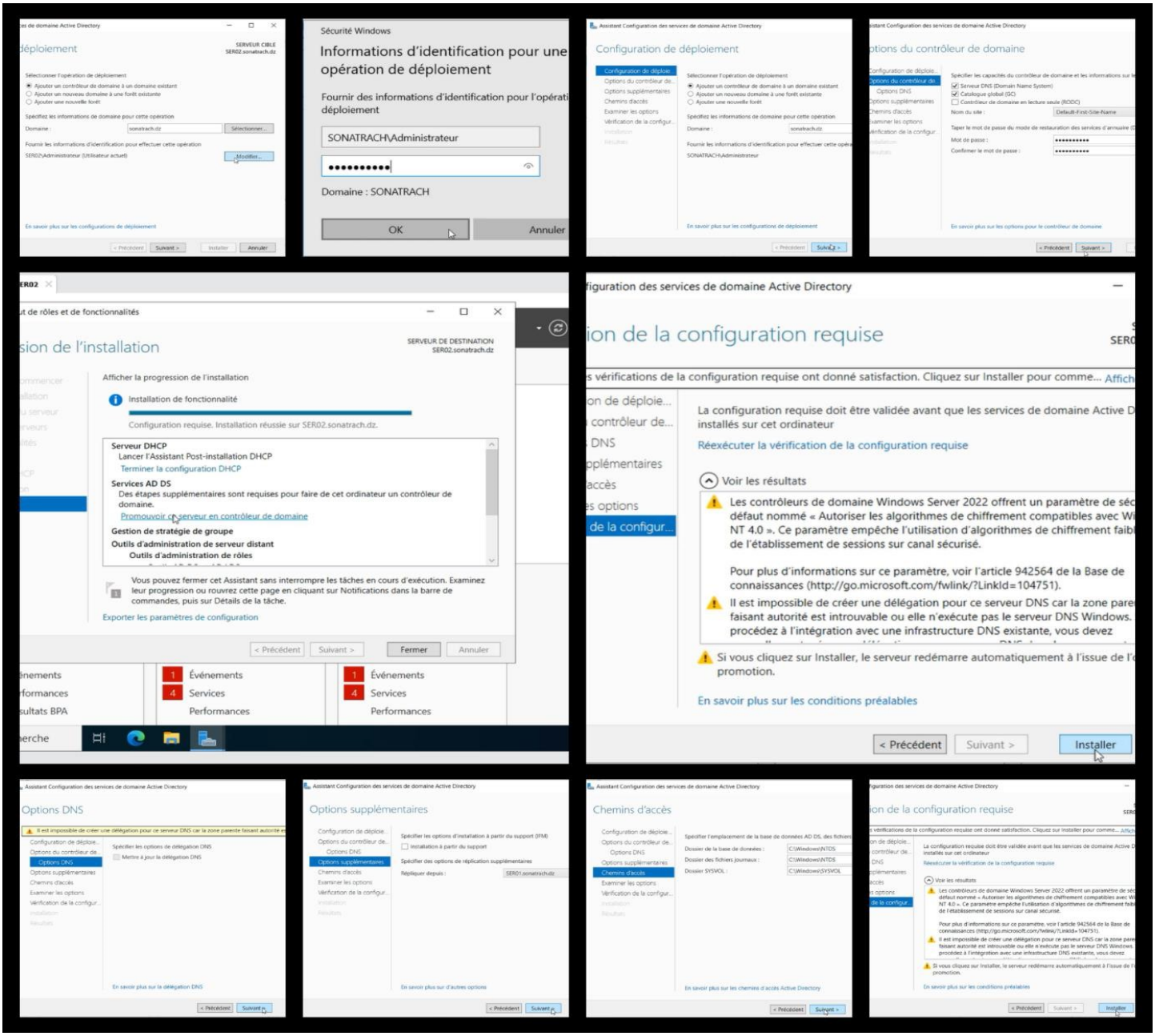

FIGURE 4.34 – La réplication du cluster.

On va créer une étendue pour chaque vlan dans le serveur SER01 :

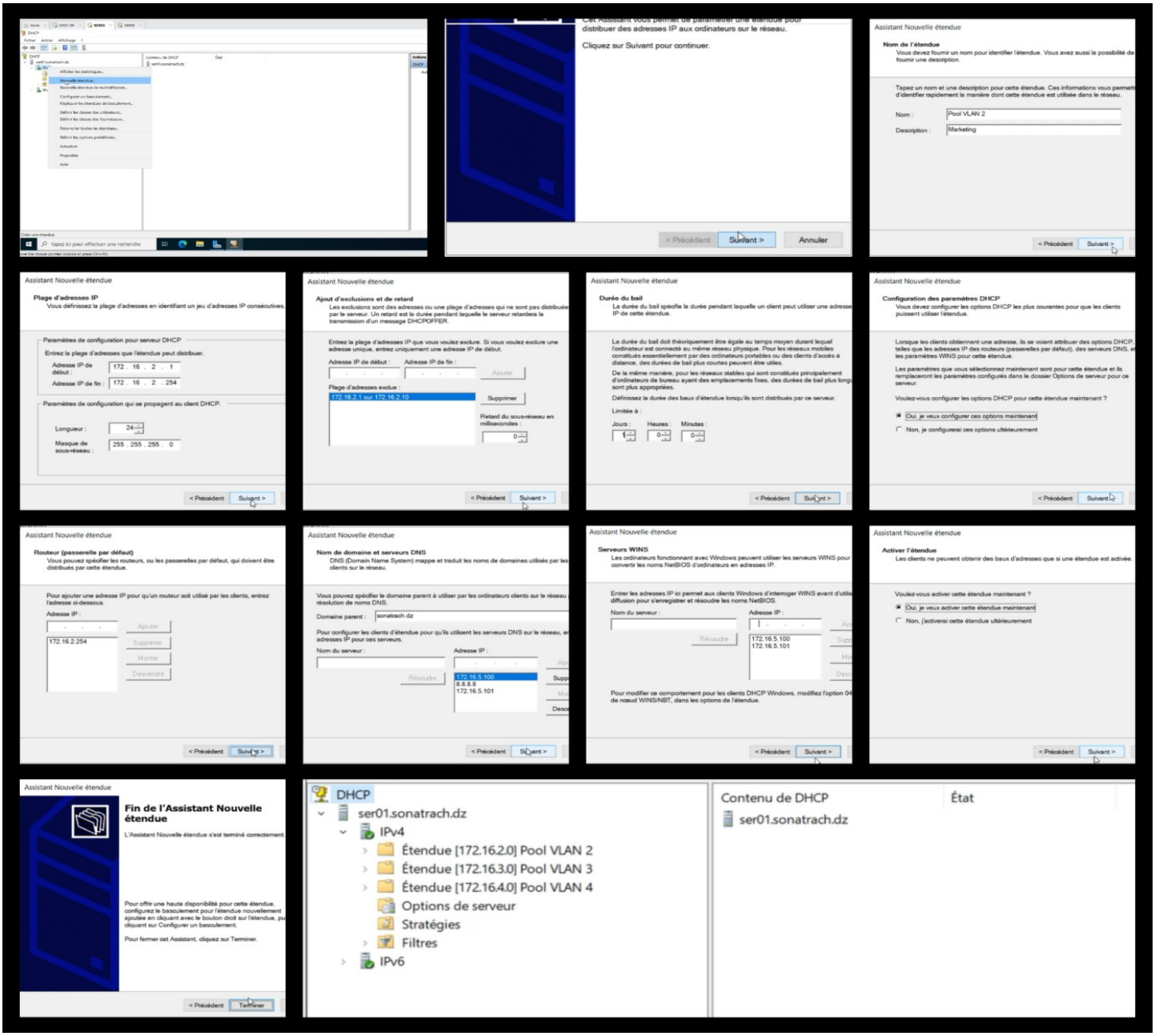

FIGURE 4.35 – Création des étendues pour chaque vlan dans le serveur SER01.

Ensuite, nous allons ajouter le SER02 au serveur SER01 :

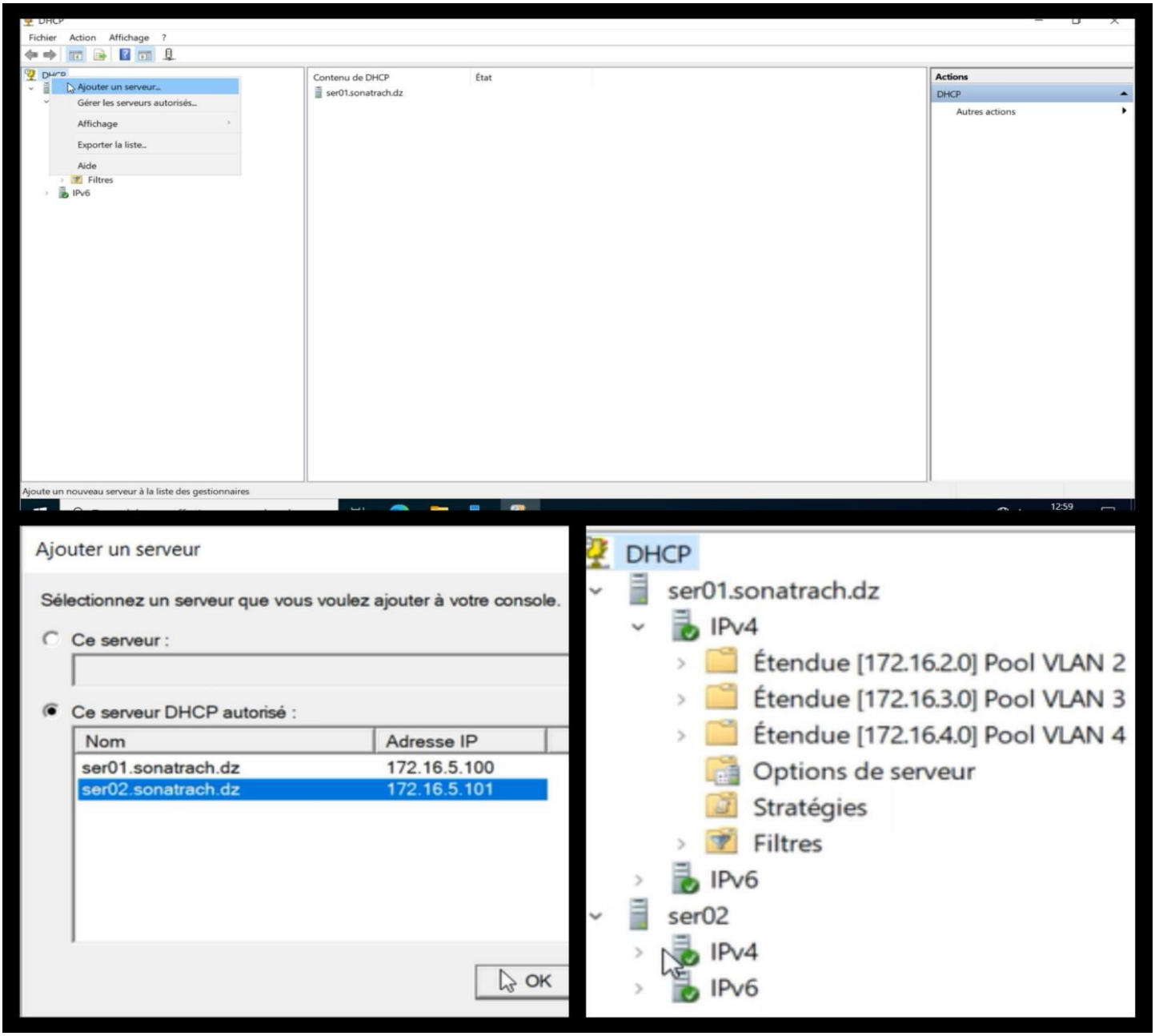

FIGURE 4.36 – Ajout du SER02 au serveur SER01.

Configurer un basculement pour chaque étendue du serveur SER01, en utilisant le mode de l'équilibrage de charge :

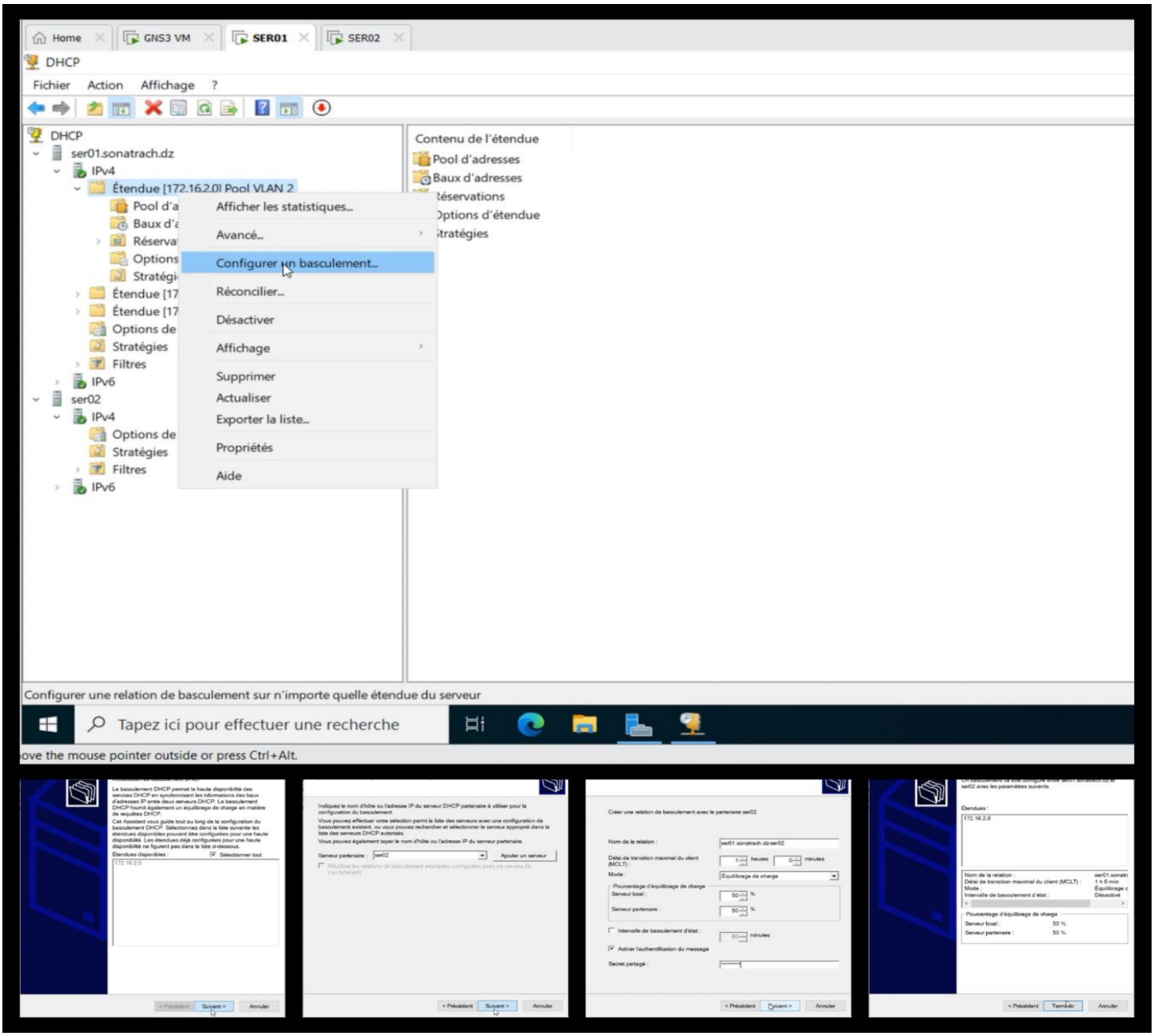

FIGURE 4.37 – Configuration du basculement pour chaque étendue du SER01.

4.8 Vérifications et Tests

Dans cette partie, l'ensemble des tests consiste à vérifier la validation des configurations en utilisant les commandes "Show" qui affiche selon la commande utilisé les différentes configurations effectuées sur les équipements, et une autre phase qui consiste à vérifier l'accessibilité et la communication entre les utilisateurs en utilisant la commande "Ping" qui teste la réponse d'un équipement sur le réseau.

4.8.1 Vérification des configurations

4.8.1.1 Vérification de la configuration du protocole VTP

On vérifie l'activation du protocole VTP sur les switchs de la couche cœur et accès avec la commande "Show vtp status" sur la console des équipements.
— Sur le switch cœur "DC1" en mode serveur :

```
DC1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrachvtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : 0c1a.9618.0000
Configuration last modified by 0.0.0.0 at 6-15-23 09:05:50
Local updater ID is 172.16.2.1 on interface Vl2 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
Configuration Revision          : 7
MD5 digest                      : 0x45 0x8F 0x3F 0x02 0x07 0x0F 0xDB 0x12
                                  0x09 0xF9 0x20 0x42 0x33 0xE4 0xE8 0x42
DC1#
```

FIGURE 4.38 – Vérification du protocole VTP en mode serveur sur "DC1".

— Sur le switch d'accès "SA1" en mode client :

```
SA1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrachvtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 6-15-23 09:05:50

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
Configuration Revision          : 7
MD5 digest                      : 0x45 0x8F 0x3F 0x02 0x07 0x0F 0xDB 0x12
                                  0x09 0xF9 0x20 0x42 0x33 0xE4 0xE8 0x42
```

FIGURE 4.39 – Vérification du protocole VTP en mode client sur "SA1".

4.8.1.2 Vérification de la création des VLANs

Pour vérifier que les VLANs sont bien crées, on lance la commande "show vlan brief" sur les commutateurs du la couche cœur et accès.

```
DC1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi1/1, Gi1/2, Gi1/3, Gi2/0
                                                 Gi2/1, Gi2/2, Gi2/3
2    Marketing                         active
3    Informatique                      active
4    Manager                           active
5    data_center                       active    Gi1/0
99   native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
DC1#
```

FIGURE 4.40 – Vérification de création des VLANs sur "DC1".

4.8.1.3 Vérification d'affectation des ports aux VLANs

Afin de vérifier que les ports ont était bien affecter aux VLANs, on lance la commande "show vlan brief" sur les commutateurs de la couche accès.

```
SA1#show  vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/3
2    Marketing                        active
3    Informatique                     active
4    Manager                          active    Et3/1, Et3/2
5    data_center                      active
99   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SA1#
```

FIGURE 4.41 – Vérification d'affectation des ports au VLAN Manager sur "SA1".

4.8.1.4 Vérification de protocole LACP

On vérifie l'activation du protocole LACP sur les switchs de la couche cœur avec la commande "Show etherchannel" sur la console du "DC1". et on doit avoir le "Port- channel" est à Po2(SU).

```
DC1#show  etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Gi3/0(P)    Gi3/1(P)    Gi3/2(P)
                                 Gi3/3(P)
 --More--
```

FIGURE 4.42 – Vérification d'activation de LACP sur "DC1".

4.8.1.5 Vérification de Load-Balancing

Afin de vérifier que la répartition de charge était bien configurée sur les commutateurs de la couche cœur, on utilise la commande "Show etherchannel load-balance" sur la console du "DC1".

```
DC1#show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination MAC address
  IPv6: Source XOR Destination MAC address
```

FIGURE 4.43 – Vérification de Load-Balancing sur "DC1".

```
DC1#show etherchannel
                Channel-group listing:
                ----------------------

Group: 2
----------
Group state = L2
Ports: 4   Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:   LACP
Minimum Links: 0


DC1#
```

FIGURE 4.44 – Vérification de l'état de l'agrégation de liens sur "DC1".

4.8.1.6 Affectation des interfaces aux VLANs (Routage interVlans)

On vérifie l'affectation des interfaces aux Vlans sur les switchs de la couche cœur et accès avec la commande "Show etherchannel" sur la console des switch cœur et accès.

```
DC1#show  ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  up                    up
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  up                    up
GigabitEthernet3/1     unassigned      YES unset  up                    up
GigabitEthernet3/2     unassigned      YES unset  up                    up
GigabitEthernet3/3     unassigned      YES unset  up                    up
Port-channel2          unassigned      YES unset  up                    up
Vlan2                  172.16.2.1      YES manual up                    up
Vlan3                  172.16.3.1      YES manual up                    up
Vlan4                  172.16.4.1      YES manual up                    up
Vlan5                  172.16.5.1      YES manual up                    up
```

FIGURE 4.45 – Affectation des interfaces aux VLANs sur "DC1".

On vérifie l'affectation des interfaces connecté aux VLANs sur les switchs de la couche cœur avec la commande "IP route" sur la console des switchs cœurs On voit bien que les interfaces ont été bien affecter aux Vlans :

```
DC1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Vlan2
L        172.16.2.1/32 is directly connected, Vlan2
C        172.16.3.0/24 is directly connected, Vlan3
L        172.16.3.1/32 is directly connected, Vlan3
C        172.16.4.0/24 is directly connected, Vlan4
L        172.16.4.1/32 is directly connected, Vlan4
C        172.16.5.0/24 is directly connected, Vlan5
L        172.16.5.1/32 is directly connected, Vlan5
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0
DC1#
```

FIGURE 4.46 – Affectation des interfaces aux Vlan sur "DC1".

4.8.1.7 Vérification de GLBP

On vérifie l'activation du protocole GLBP sur les switchs de la couche cœur avec la commande "Show glbp" sur la console du "DC1".

```
DC1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl2         2    -   200 Active   172.16.2.254    local           172.16.2.2
Vl2         2    1   -   Listen   0007.b400.0201  172.16.2.2      -
Vl2         2    2   -   Active   0007.b400.0202  local           -
Vl3         3    -   200 Active   172.16.3.254    local           172.16.3.2
Vl3         3    1   -   Listen   0007.b400.0301  172.16.3.2      -
Vl3         3    2   -   Active   0007.b400.0302  local           -
Vl4         4    -   200 Active   172.16.4.254    local           172.16.4.2
Vl4         4    1   -   Listen   0007.b400.0401  172.16.4.2      -
Vl4         4    2   -   Active   0007.b400.0402  local           -
Vl5         5    -   200 Active   172.16.5.254    local           172.16.5.2
Vl5         5    1   -   Listen   0007.b400.0501  172.16.5.2      -
Vl5         5    2   -   Active   0007.b400.0502  local           -
DC1#
```

FIGURE 4.47 – Vérification de GLBP sur "DC1".

4.8.1.8 Vérification d'affectation des interfaces de la DMZ

On vérifie l'affectation des interfaces sur la DMZ avec la commande "ip interface brief " sur la console du "dmz".

```
dmz#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
dmz#
```

FIGURE 4.48 – Affectation des interfaces aux Vlan sur "dmz".

4.8.1.9 Vérification de HA

On vérifie l'activation de la haute disponibilité sur les FortiGate avec la commande "get system ha status" sur la console du "FG1" ou bien "FG1".

```
Secondary    : FG2              , FGVMEVOZHXKIRL62, HA cluster index = 0
Primary      : FG1              , FGVMEVHFHZGG519A, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.2
Secondary: FGVMEVOZHXKIRL62, HA operating index = 1
Primary: FGVMEVHFHZGG519A, HA operating index = 0
```

FIGURE 4.49 – Vérification de la haute disponibilité sur "FG1".

4.8.2 Tests

La phase des tests consiste à effectuer des commandes "Ping" entre les équipements du réseau pour tester l'accessibilité. Un utilisateur qui veut communiquer avec un autre émet avec le ping des paquets au destinataire. Si ce dernier les reçoit alors le ping est réussi, sinon il a échoué.

4.8.2.1 Test de LACP et load-balance

On enlève un câble entre DC1 et DC2, et on affiche avec la commande « show ethernetchannel summary », on voit bien que les ports sont toujours actifs ce qui implique l'agrégation des liens est activée :

```
DC1#show  etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Gi3/0(P)    Gi3/1(P)    Gi3/2(P)
                                 Gi3/3(P)
 --More--
```

FIGURE 4.50 – Test de l'agrégation de lien sur "DC1".

4.8.2.2 Test de la DMZ

On va tester la communication entre les différents serveurs de la dmz, on a les serveurs du VLAN community se communique entre eux , mais ne se communique pas avec les serveurs du VLAN isolated.
Et pour les serveurs du VLAN isolated ne se communique ni entre eux ni entre les serveurs du VLAN community .

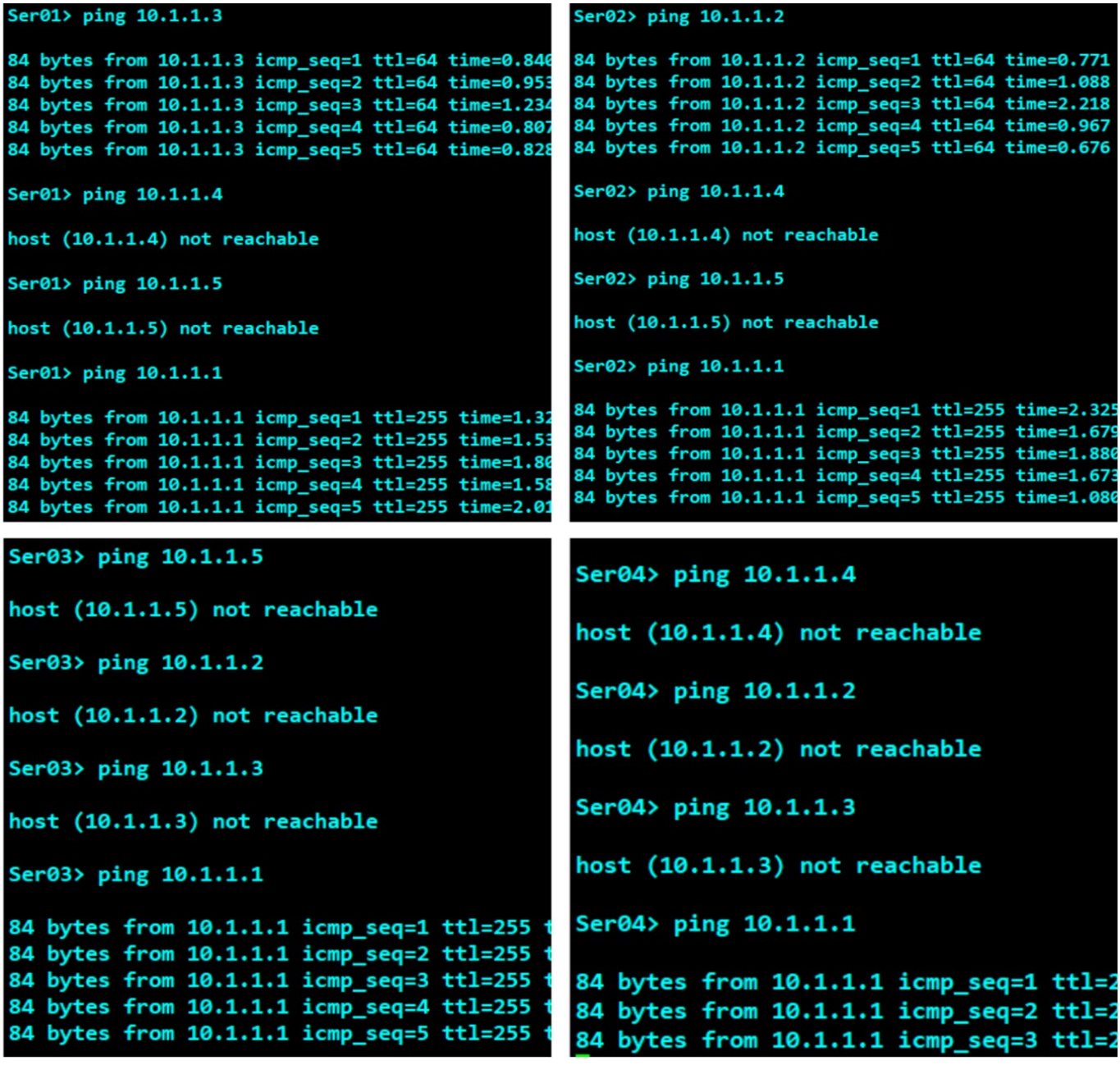

FIGURE 4.51 – Ping entre les serveurs de la "DMZ ".

4.8.2.3 Test du cluster Fortiget

On va désactiver le Forti Gate FG 1 qui est le Forti Gate primaire, on va regarder le statu du FG2 on voit qu'il a pris le relai et il est devenu primary. On va taper la commande « get system ha status ».

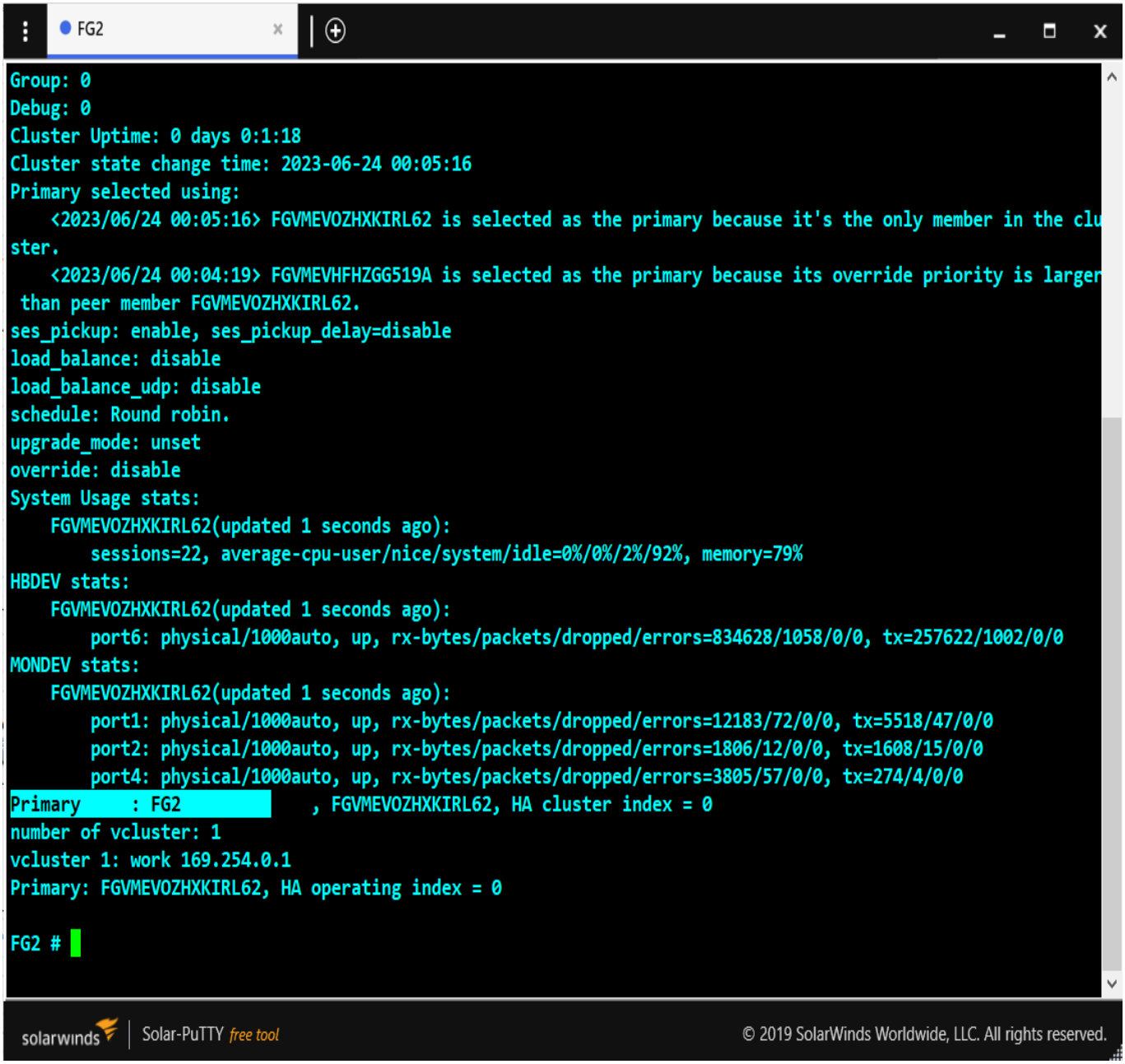

FIGURE 4.52 – Test de cluster FortiGate sur "FG2 ".

4.8.2.4 Test de réplication des données

On voit bien que les VLANs créés dans le serveur SER01 ont été répliqués dans le serveur SER02 .

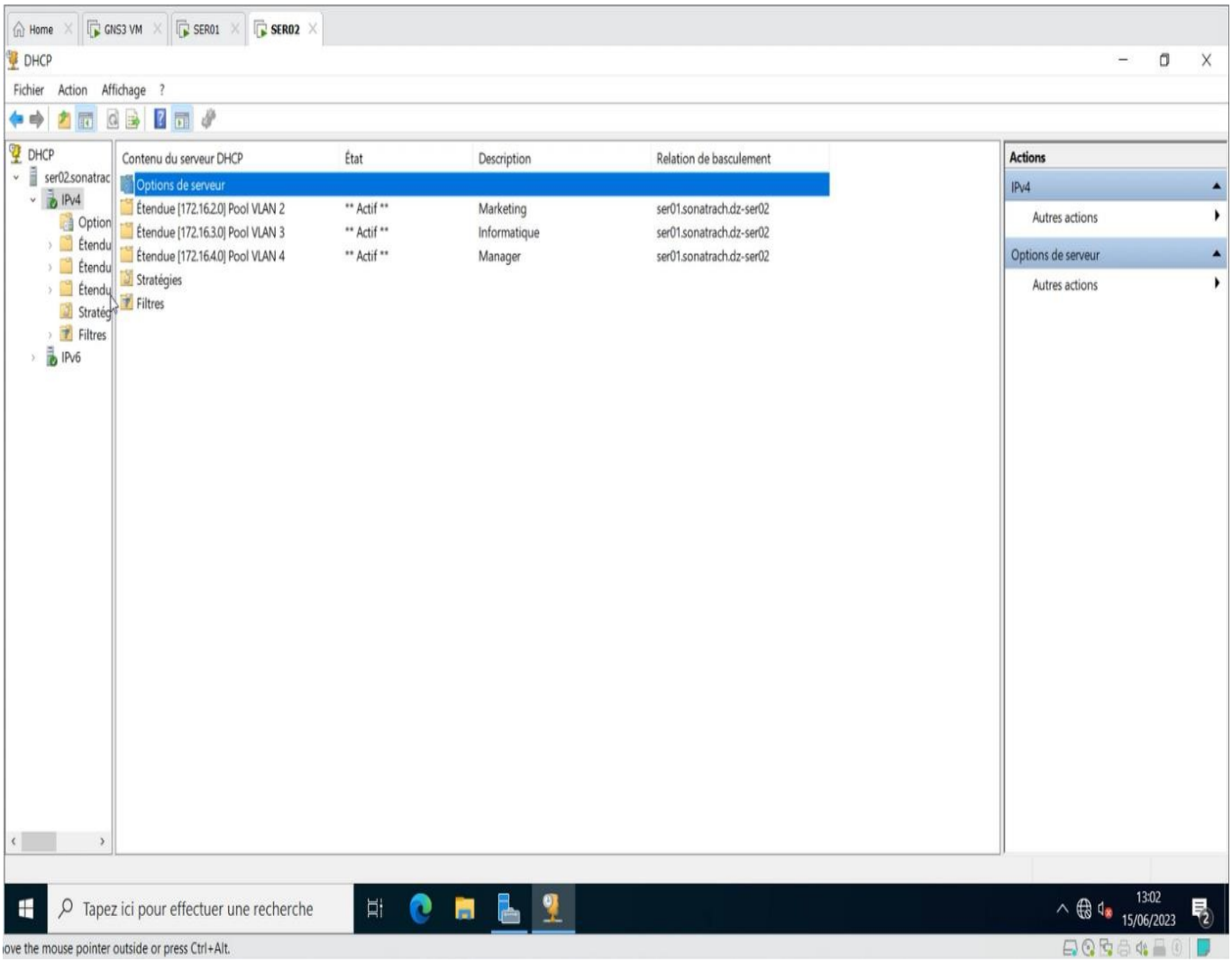

FIGURE 4.53 – Test de réplication des VLAN dans le serveur "SER02 ".

4.8.2.5 Test du cluster serveur DHCP

Comme premier test, on va voir si le cluster DHCP attribue des adresses IP , on tape la commande « ip dhcp » sur PC 4, on voit bien que cluster DHCP lui a attribué une adresse IP « 172. 16. 3. 133 ».

```
PC4> ip dhcp
DORA IP 172.16.3.133/24 GW 172.16.3.254

PC4>
```

FIGURE 4.54 – Test d'attribution des adresses par le cluster DHCP sur " PC 4".

On vérifier dans les baux d'adresses du SER01, on voit bien qu'il a attribué une adresse IP pour le PC 4 :

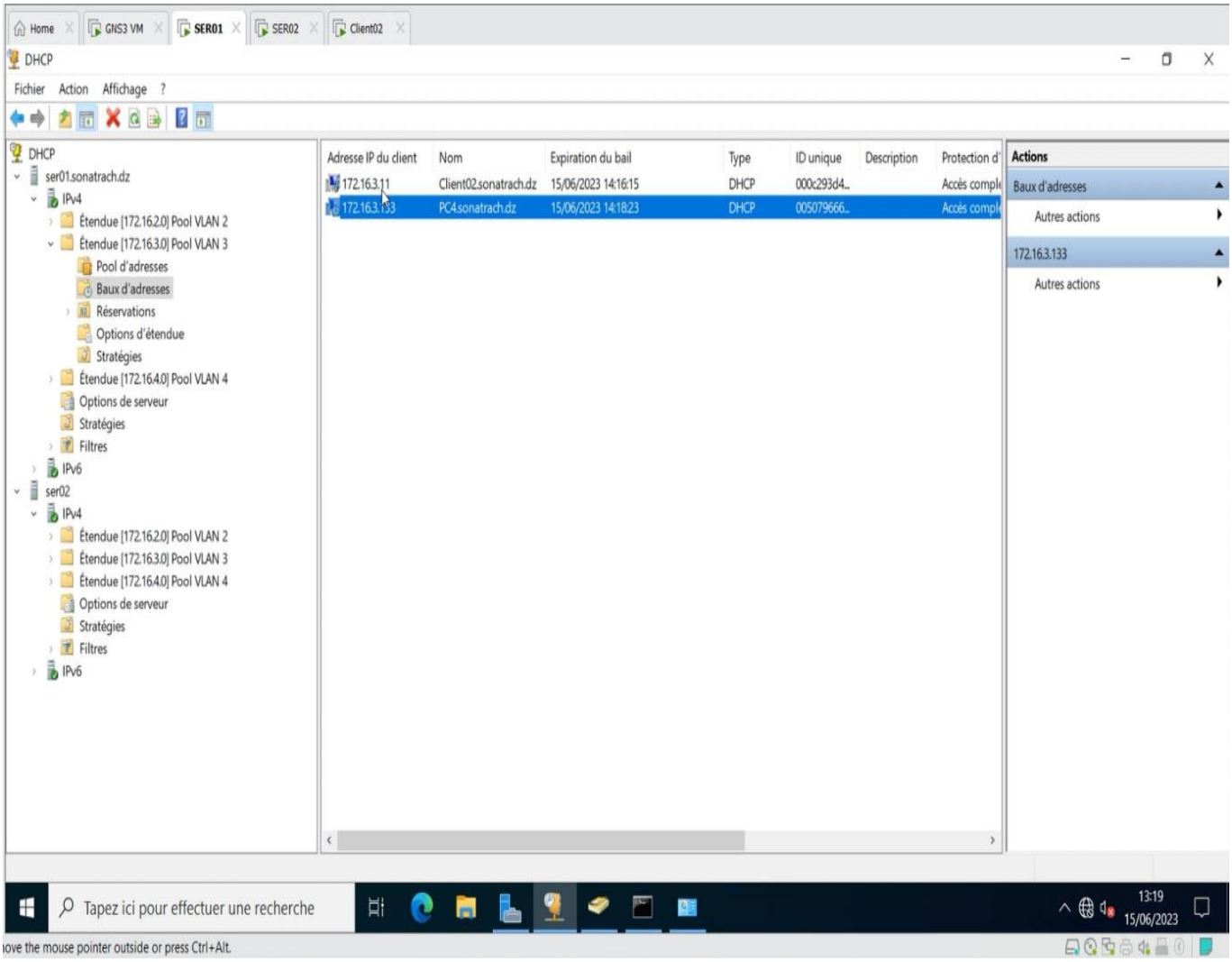

FIGURE 4.55 – Attribution d'une adresse IP pour " PC 4".

Maintenant, on va désactiver le serveur SER01 du cluster, et on va désactiver la carte réseau du client2 du VLAN 2, et on récupère l'adresse IP attribuée.

On voit bien que le client02 a une adresse IP attribué par le serveur SER02 qui a l'adresse IP 172.16.5.101, le SER02 a repris le relais directement lorsque le SER01 est tombé en pannes.

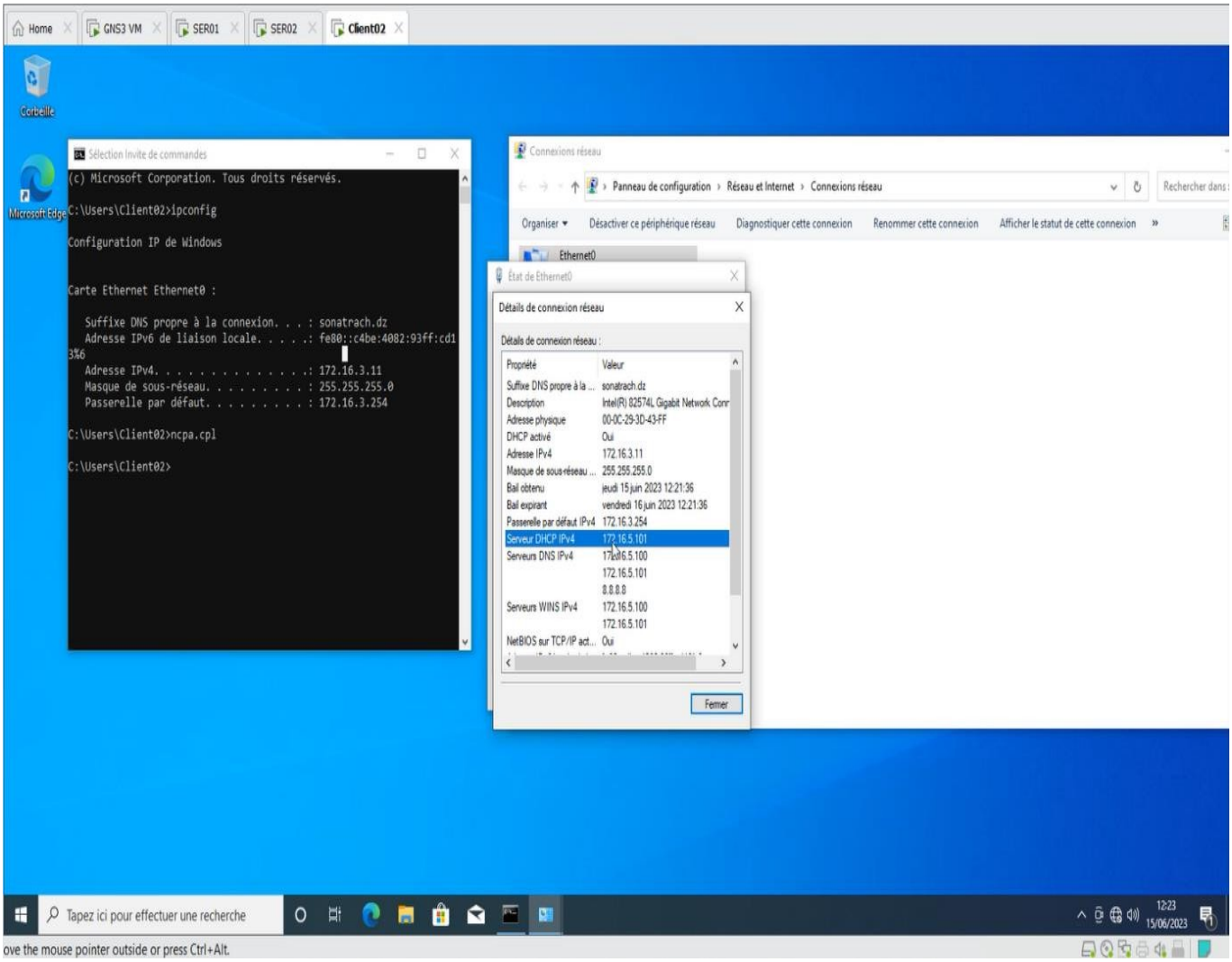

FIGURE 4.56 – L'attribution d'une adresse IP pour " Client02 ".

4.8.2.6 Test du cluster serveur AD

Ensuite, nous allons créer des utilisateurs sur SER01, on actualise et on voit qu'ils sont créés aussi dans SER02 :

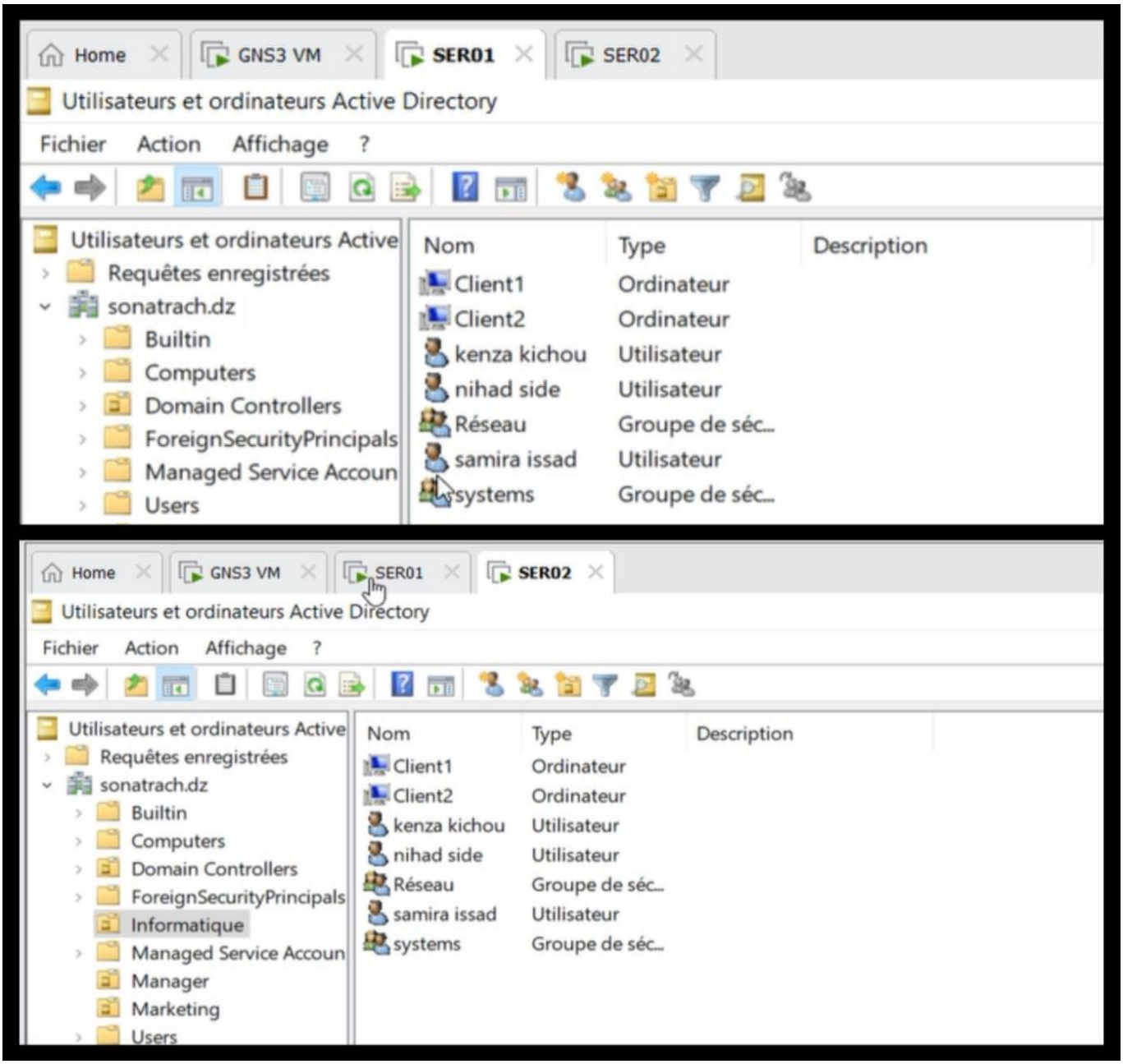

FIGURE 4.57 – Création des utilisateurs sur " SER01 ".

Nous allons ajouter un utilisateur, on a :

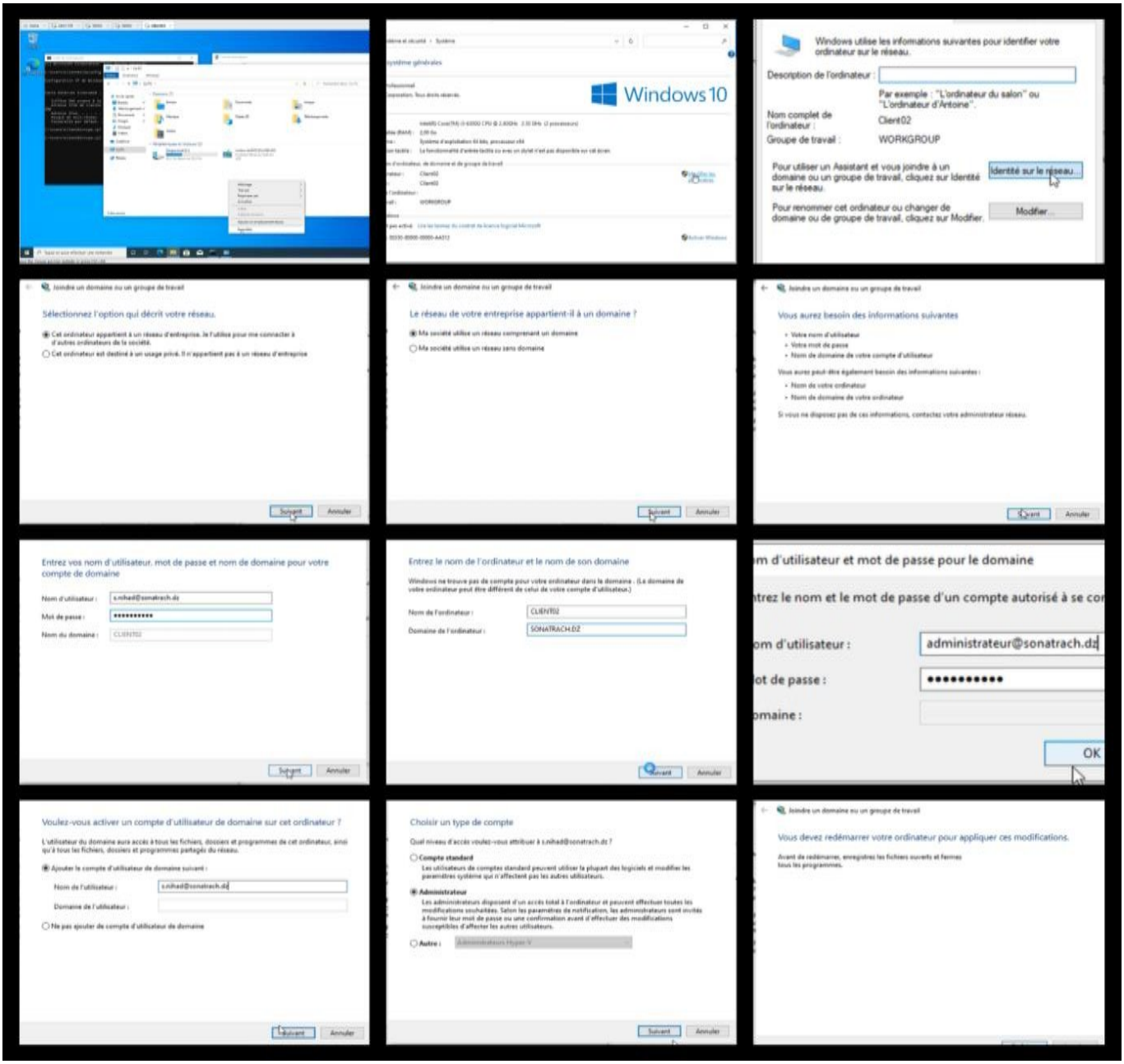

FIGURE 4.58 – Création d'un utilisateur sur " Client02 ".

On va pinger au DNS :

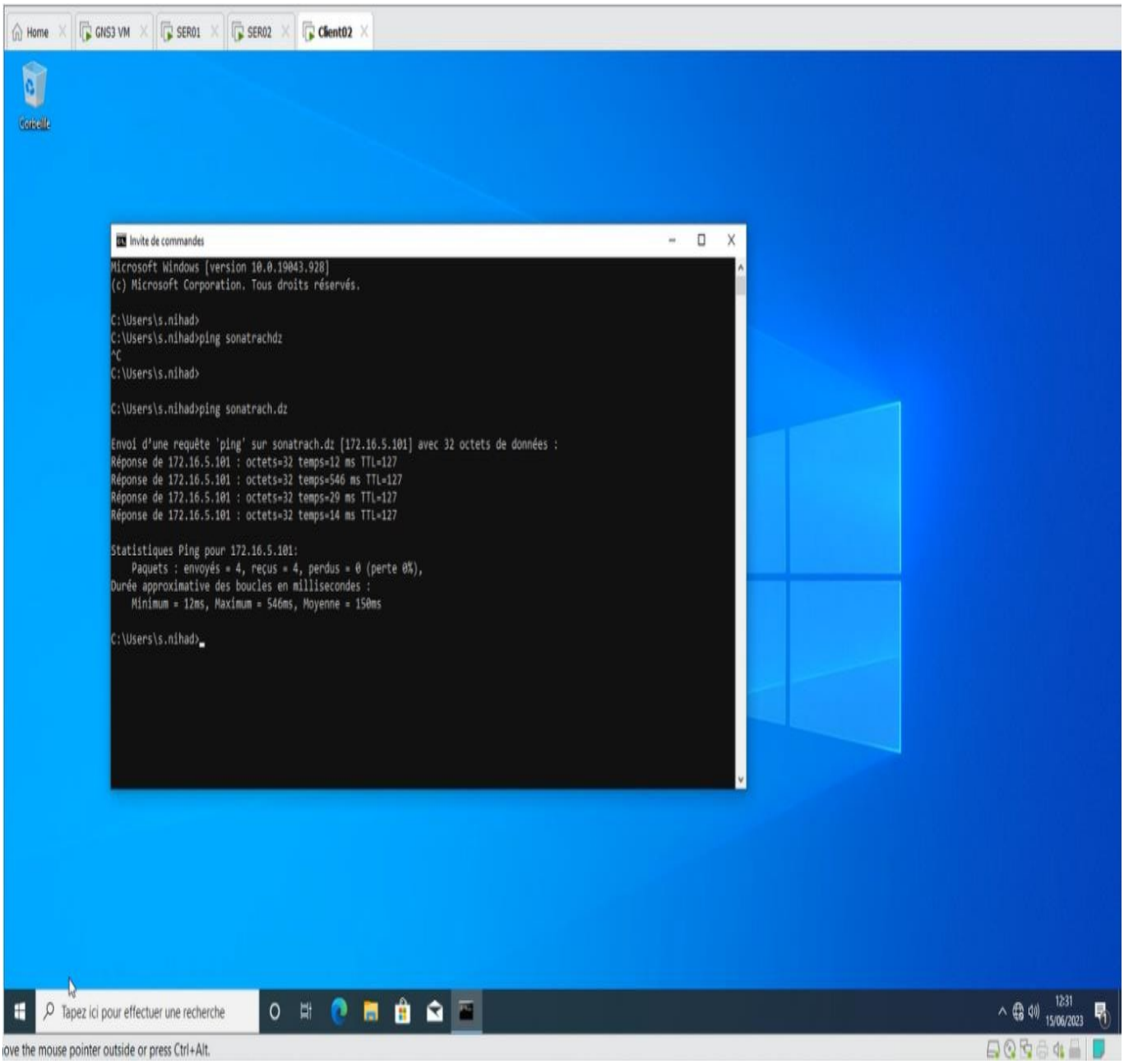

FIGURE 4.59 – Tester le DNS sur " Client02 ".

Nous allons entrer à une autre session d'utilisateur :

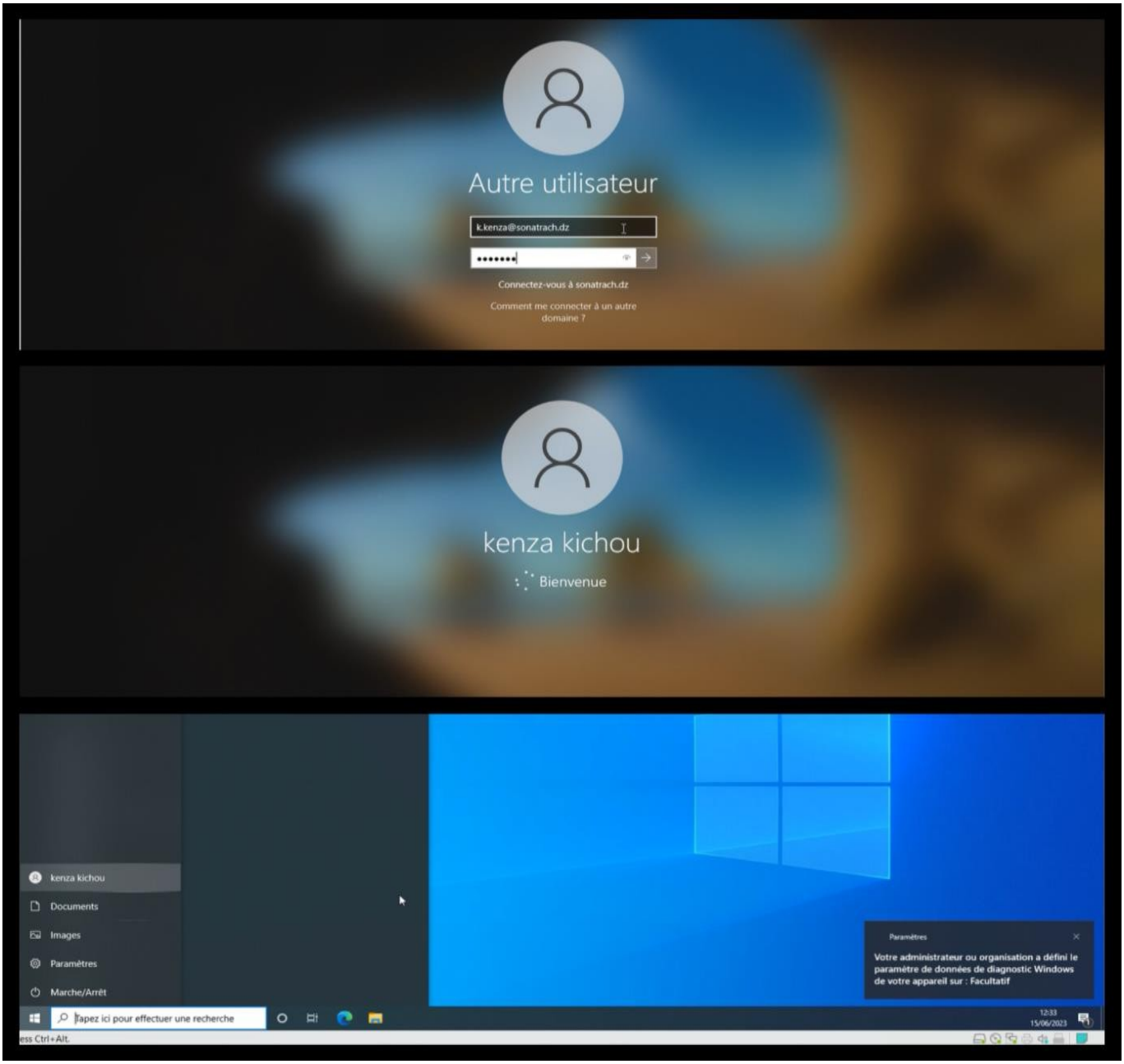

FIGURE 4.60 – Session d'un autre utilisateur.

4.9 Conclusion

Dans ce chapitre, nous avons présenté les différentes étapes de configuration qui nous ont aidé à mettre en place un cluster haute disponibilité avec un équilibrage de charge .

Enfin nous avons effectué un ensemble de tests de validation et de vérification afin de prouver l'efficacité des solutions.

Conclusion générale et perspectives

Ce projet de fin d'études consiste à proposer une solution pour assurer la disponibilité des services en réduisant les risques de surcharge et d'optimiser les performances à la RTC de Bejaia en mettant en pratique les connaissances théoriques à travers des méthodes professionnelles utilisées dans l'entreprise SONATRACH.

Le projet vise à améliorer la résilience et la disponibilité des applications critiques en créant un cluster robuste et performant. L'objectif est d'assurer une continuité opérationnelle et de garantir des performances optimales même en cas de défaillance d'un noeud du cluster.

Nous avons mis en oeuvre des techniques avancées d'équilibrage de charge pour répartir efficacement les requêtes et les charges de travail entre les différents noeuds du cluster. Cela permet d'optimiser l'utilisation des ressources et d'éviter les surcharges, assurant ainsi une expérience utilisateur fluide et réactive. En parallèle, des mécanismes de haute disponibilité ont été configurés pour garantir la redondance et la tolérance aux pannes. Cela comprend la réplication des données, la surveillance constante de l'état des noeuds et la mise en place de mécanismes de basculement automatique en cas de défaillance.

Ce projet a également nécessité une attention particulière à la sécurité. Des mesures appropriées ont été mises en place pour protéger le cluster contre les attaques potentielles, en assurant l'intégrité des données et la confidentialité des informations échangées.

La mise en place d'un cluster haute disponibilité avec équilibrage de charge au sein de l'entreprise Sonatrach de Béjaïa constitue une avancée significative pour améliorer la résilience, la performance et la disponibilité des applications critiques. Ce projet démontre l'engagement de l'entreprise à rester à la pointe de la technologie et à garantir des services fiables pour soutenir ses activités opérationnelles.

Pour la réalisation de ce travail, nous avons utilisé le GNS3 avec la VMWARE WORKSTATION PRO 16 pour simuler l'architecture étudiée. Aussi nous avons présenté notre environnement de travail et les outils qui nous ont servi pour implémenter notre simulation et vérifier son bon fonctionnement.

En termes de perspectives, nous envisageons d'améliorer notre travail en implémentant d'autres mécanismes de protection tels que des certificats SSL/TLS pour garantir que connexions autorisées sont établies avec le cluster.

Bibliographie

[1] *Présentation de l'Entreprise SONATRACH, Documents internes de SONATRACH.*

[2] earth.google.com/web/search/SONATRACH-wilaya-de-Bejaia/, consulté le 18/06/2023.

[3] Atelin, P. (2009). *Réseaux informatiques : notions fondamentales : normes, architecture, modèle OSI, TCP/IP, Ethernet, Wi-Fi,. .Editions ENI.*

[4] Pillou, J., Lemainque, F. (2012). *Tout sur les réseaux et Internet - 3e éd. Dunod.*

[5] fr.m.wikipedia.org/wiki/Fichier :P2P-network.svg, consulté le 08/06/2023.

[6] fr.m.wikipedia.org/wiki/Pair-à-pair, consulté le 11/06/2023.

[7] M. Boudiaf, *« Rcom-chapitre1-partie1.pdf », cours deuxième année LMD/s4, Université des sciences et de la technologie d'oran, 2022.*

[8] Dordoigne, J. (2013). *Réseaux informatiques : Notions fondamentales (protocoles, architectures, réseaux sans fil, virtualisation, sécurité, IP /,. . .).*

[9] sti2d.ecolelamache.org/ii-rseaux-informatiques-7-topologie-des-rseaux.html, consulté le 08/06/2023.

[10] gitmind.com/fr/topologie-reseau.html, consulté le 11/06/2023.

[11] Huet, F., Verhille, C. (2007). *GNU/Linux Fedora : Sécurité du système, sécurité des données, pare-feu, chiffrement, authentification. Editions ENI.*

[12] sti2d.ecolelamache.org-ii-rseaux-informatiques-4-le-modle-de-rfrence-osi.html, consulté le 11/06/2023.

[13] Pirio, M. (2004). *Linux-Debian :TCP/IP-Les services réseaux. Editions ENI.*

[14] pixees.fr/informatiquelycee/n-site/nsi-prem-modele-tcpip.html, consulter le 15/06/2023.

[15] stid2d.ecolelamache.org/ii-rseaux-informatiques-3-adresses-des-Iments-dun-rseau.html, consulter le 14/06/2023.

[16] Natkin, S. (2002). *Les protocoles de sécurité d'Internet.*

[17] Pillou, J., Bay, J. (2013). *Tout sur la sécurité informatique - 3e édition. Dunod.*

[18] Zaidoun, A. S. (2023). *Sécurité informatique : Concepts et outils. ISTE Group.*

[19] www.kaspersky.fr/resource-center/definitions/encryption, consulté le 14/06/2023.

[20] fr.m.wikipedia.org/wiki/Pare-feu-(informatique), consulter le 17/06/2023.

[21] Sécurité informatique : DMZ - NAT sécurité réseau FIREWALL - DMZ - NAT | Examens, Exercices, Astuces tous ce que vous Voulez (mrproof.blogspot.com)/, consulté le 17/06/2023.

[22] waytolearnx.com/2018/09/difference-entre-proxy-et-firewall.html, consulter le 12/06/2023.

[23] iotindustriel.com/glossaire-iiot/systeme-de-detection-dintrusion-ids , consulté le 16/06/2023.

[24] fr.barracuda.com/support/glossary/intrusion-prevention-system, consulté le 14/05/2023.

[25] iotindustriel.com/glossaire-iiot/systeme-de-prevention-dintrusion-ips/, consulté le 12/06/2023.

[26] www.clicours.com/etude-et-mise-en-place-dune-haute-disponibilite-en-base-de-donnees-oracle consulté le 25/05/2023.

[27] www.purestorage.com/fr/knowledge/what-is-active-active.html, consulté le 26/05/2023.

[28] fr.theastrologypage.com/storage-consolidation, consulté le 26/05/2023.

[29] www.1min30.com/dictionnaire-du-web/serveur-nas, consulté le 26/05/2023.

[30] fr.wikipedia.org/wiki/RC3A9seau-de-stockage-SAN, consulté le 19/06/2023.

[31] blog.hubspot.fr/marketing/virtualisation-informatique, consulté le 26/05/2023.

[32] Le meilleur logiciel open source pour le stockage en réseau (opensourceforu.com), consulté le 20/06/2023

[33] www.appvizer.fr/magazine/services-informatiques/virtualisation/type-virtualisation, consulter le 26/05/2023.

[34] www.cohesity.com/fr/glossary/backup-and-recovery/, consulté le 27/05/2023.

[35] www.cohesity.com/fr/glossary/backup-and-recovery/, consulté le 17/06/2023.

[36] aws.amazon.com/fr/what-is/load-balancing/, consulté le 17/06/2023.

[37] lightcode.fr/article/clusters/, consulté le 20/06/2023.

[38] www.cloudflare.com/fr-fr/learning/performance/what-is-load-balancing, consulté le 17/06/2023.

[39] www.cloudflare.com/fr-fr/learning/performance/types-of-load-balancing-algorithms/, consulté le 17/06/2023.

[40] www.2000serveur.com/hauteDisponibiliteLoadBalancing.aspx, consulté le 10/07/2023.

[41] datascientest.com/network-load-balancing-tout-savoir, consulté le 10/07/2023.

[42] fr.barracuda.com/support/glossary/failover, consulté le 27/05/2023.

[43] www.wikiwand.com/fr/Basculement-(informatique), consulté le 27/05/2023.

[44] www.ibm.com/docs/fr/i/7.3topicavailability-environment-resilience, consulter le 28/05/2023.

[45] www.ibm.com/docs/fr/i/7.1 ?topic=criteria-outage-coverage, consulté le 17/06/2023.

[46] www.ionos.fr/digitalguide/serveur/securite/redondance/, consulté le 10/07/2023.

[47] forum.huawei.com/enterprise/fr/qu-est-ce-que-le-protocole-de-redondance-de-routeur-virtuel-vrrp/thread/, consulté le 20/06/2023.

[48] cisco.goffinet.org/ccna/disponibilite-lan/redondance-de-passerelle-host-standby-router-protocol-hsrp/, consulté le 20/06/2023.

[49] fr.theastrologypage.com/spanning-tree-protocol, consulté le 20/06/2023.

[50] www.fingerinthenet.com/vtp/ , consulté le 20/06/2023.

[51] www.50a.fr/0/clustering, consulté le 17/06/2023.

[52] www.lebigdata.fr/cluster-definition, consulté le 17/06/2023.

[53] developpement-informatique.com/article/541/introduction-aux-systemes-de-clustering, consulté le 17/06/2023.

[54] gns3.fr.softonic.com/, consulté le 25/06/2023.

[55] www.clubic.com/telecharger-fiche121950-vmware- workstation.html, consulté le 25/06/2023.

[56] dz.kompass.com/p/ipkol-telecom/fr6148486/boitier-de- securite-fortigate/10863/, consulté le 25/06/2023.

[57] www.fortinet.com/products/endpoint-security/forticlient, consulté le 25/06/2023.

[58] fr.wikipedia.org/wiki/Windows-Server-2022, consulté le 26/06/2023.

[59] windows-10.fr.uptodown.com/windows, consulté le 26/06/2023.

Annexe A

Annexe

A.1 Installation de GNS3

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton « Finish ». La figure suivante représente l'interface de GNS3.

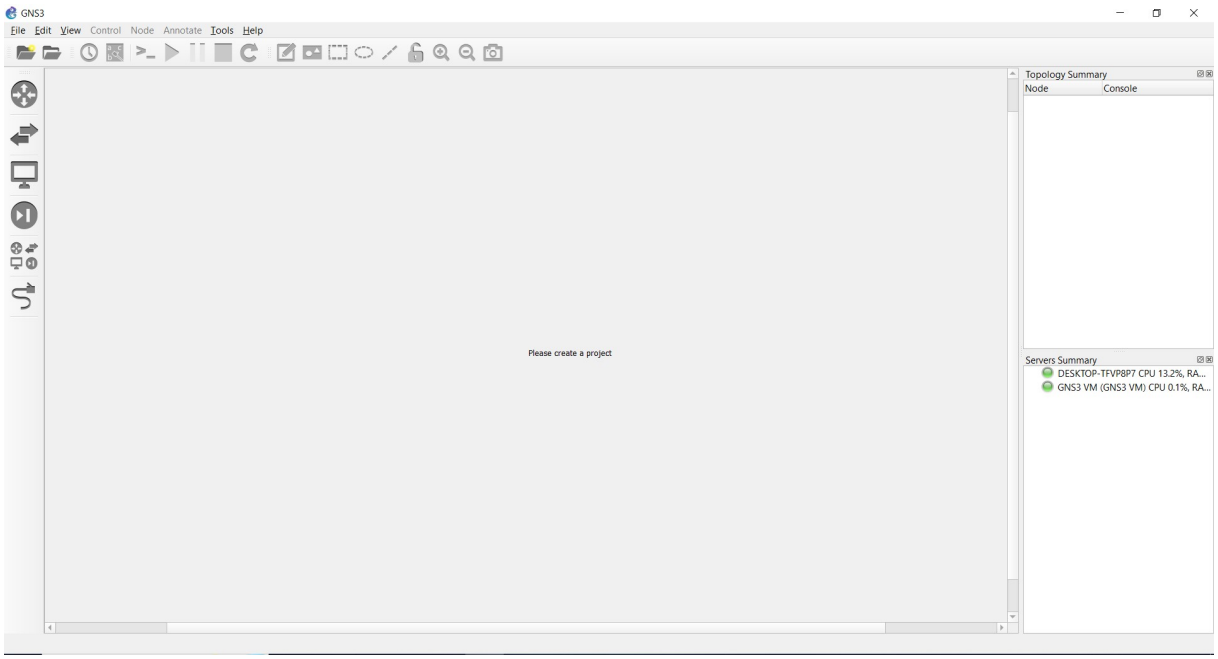

FIGURE A.1 – Interface de GNS3.

A.2 Installation du VMWare Workstation PRO 16

Pour installer le logiciel VMWare Workstation, il faut d'abord télécharger le fichier exécutable et lancer, après on suit les étapes d'installation jusqu'à la fin puis on clique sur "Finish". La figure suivante représente les différentes étapes :

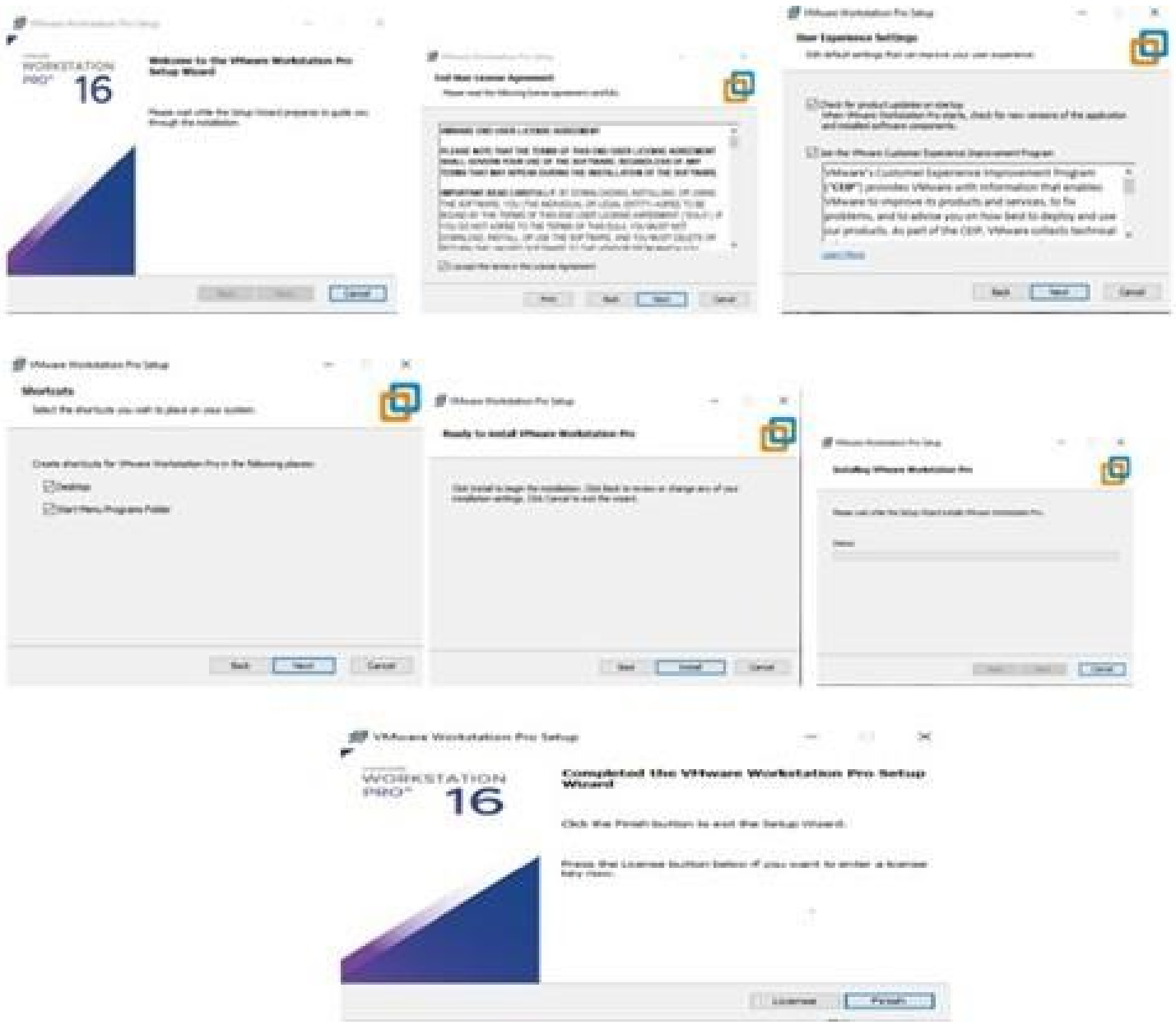

FIGURE A.2 – Les étapes d'installation du VMWare Workstation PRO 16.

A.3 Installation de la machine virtuelle serveur 2022

On va Téléchargez l'image ISO du serveur 2022, ensuite nous allons créer une nouvelle machine virtuelle avec les paramètres requis puis on va monter l'image ISO et démarrez la machine virtuelle. Et suivre les instructions à l'écran pour installer le serveur 2022. Une fois l'installation terminée configurer les paramètres réseau et autres selon vos besoins. La figure suivante représente les différentes étapes :

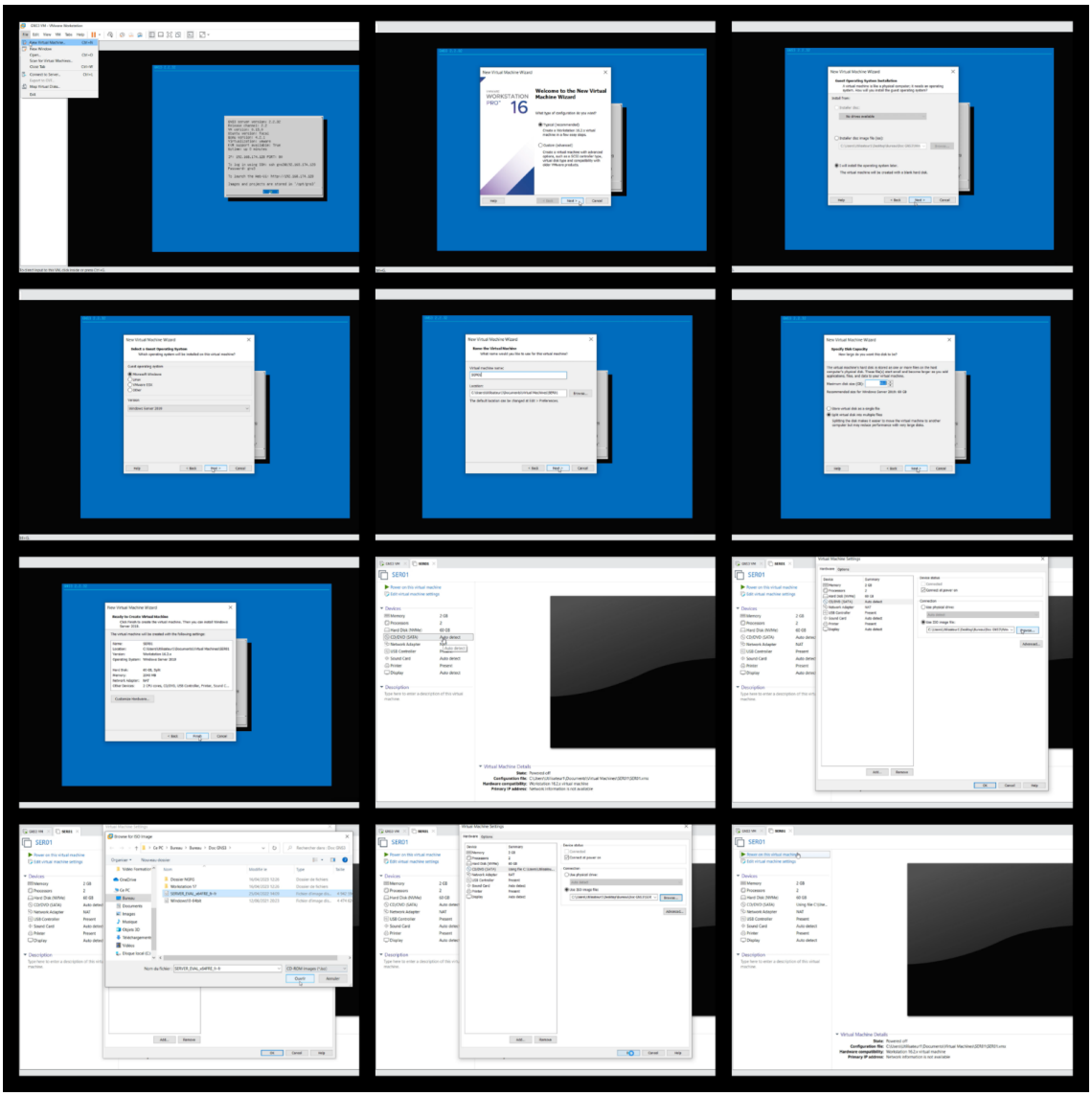

FIGURE A.3 – Les étapes d'installation de la machine virtuelle serveur 2022.

A.4 Installation de l'active directory sur Windows Server 2022

L'active Directory est un annuaire système hiérarchique. Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire.
Sur la machine virtuelle on installe le contrôleur de domaine "Active Directory". Pour commencer l'installation, il va falloir ajouter le Service de Rôle Active Directory. Lancer l'installation et ajouter les fonctionnalités qui manquent.

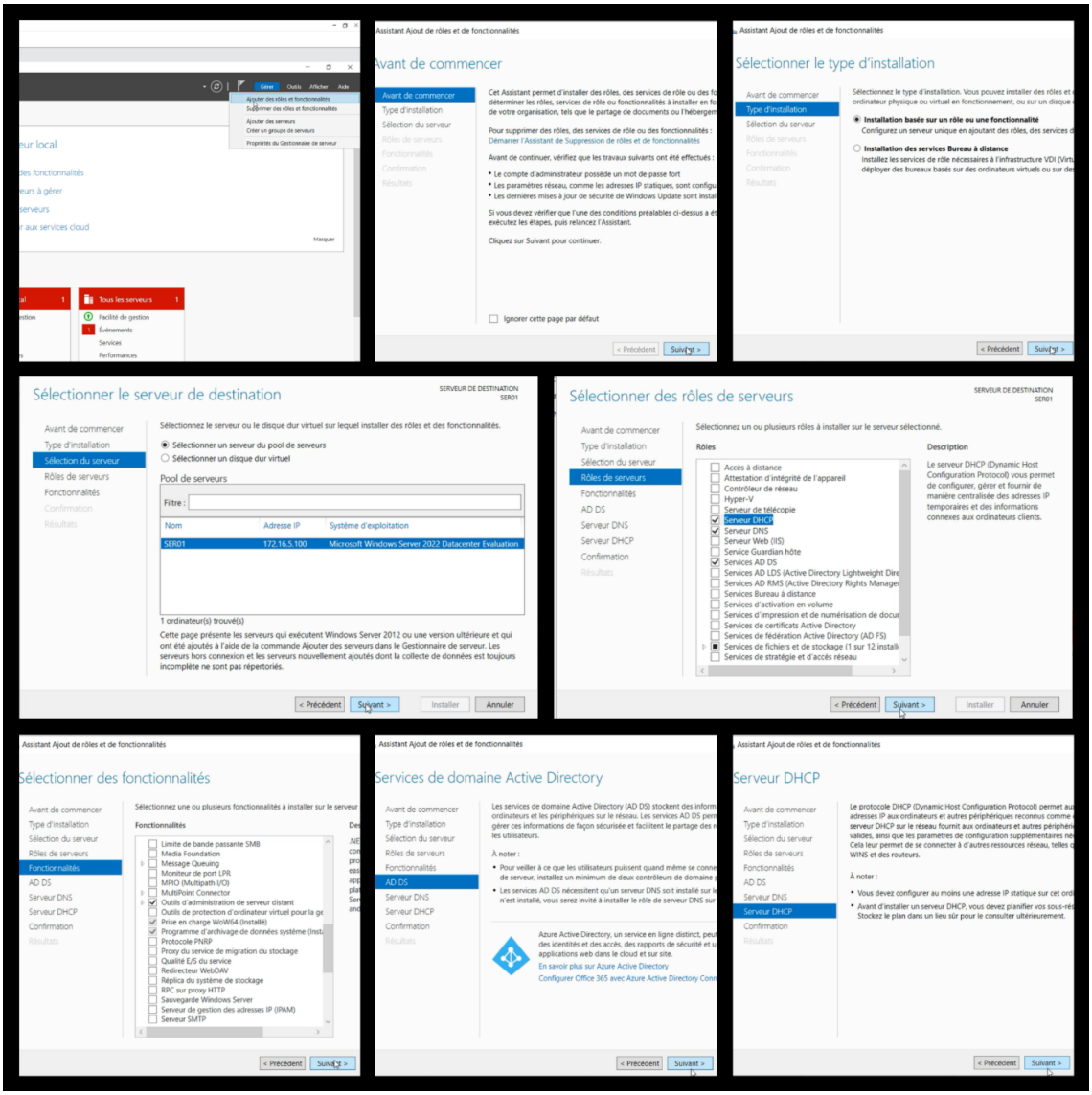

FIGURE A.4 – Installation de l'active directory.

A.5 Installation de DHCP sous Windows Server 2022

Sur la machine virtuelle Windows Server 2022, Nous avons installé DHCP server Pour commencer l'installation, il va falloir ajouter le Service de DHCP Server et ajouté les fonctionnalités. Les figures suivantes montrent les étapes de l'installation :

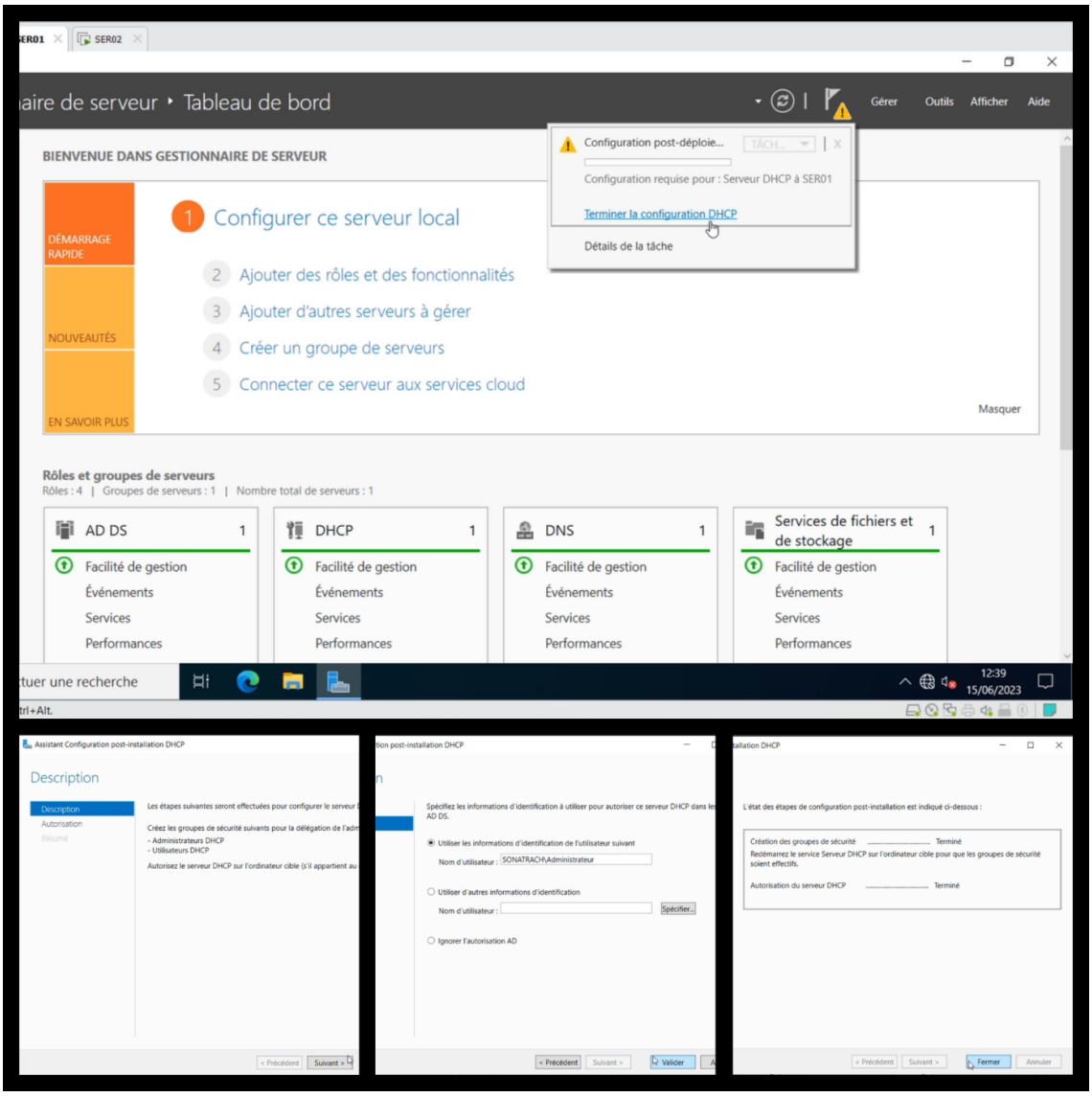

FIGURE A.5 – Installation du DHCP.

A.6 Installation de la machine virtuelle Windows 10

Afin d'installer une machine virtuelle Windows 10, on a les étapes suivantes :

Il va falloir téléchargez l'image ISO de Windows 10, ensuite nous allons créer une nouvelle machine virtuelle avec les paramètres requis. Monter l'image ISO et démarrez la machine virtuelle et suivre les instructions à l'écran pour installer Windows 10. Une fois l'installation terminée, configurez les paramètres de base et installez les pilotes nécessaires.

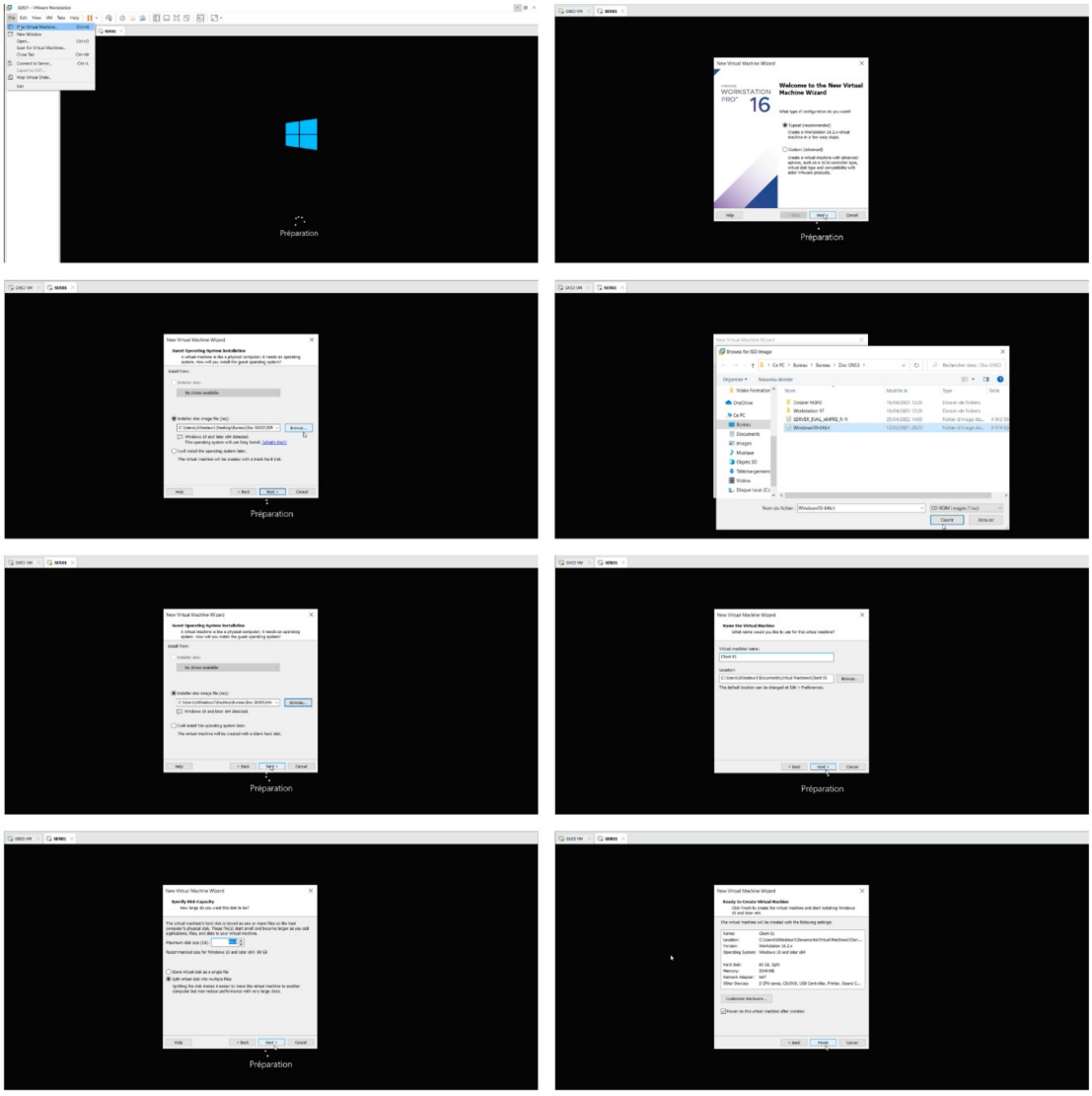

FIGURE A.6 – Les étapes d'installation de la machine virtuelle Windows 10.

RESUME

Le réseau informatique est le pilier essentiel de toute entreprise, indépendamment de son secteur d'activité. Il est donc primordial de garantir la continuité des opérations de l'entreprise. Dans notre travail, nous nous focalisons sur l'une des plus importantes technologies de haute disponibilité, c'est la mise en place d'un cluster haute disponibilité avec équilibrage de charge. L'objectif principal est d'assurer une continuité opérationnelle et de garantir des performances optimales des systèmes informatiques ainsi que la haute disponibilité des services cruciaux pour les entreprises dépendant de leurs infrastructures en répartissant la charge de travail. À cet effet, nous avons illustré concrètement ces concepts, nous avons décrit les étapes de configuration, en tenant compte des différents aspects tels que la création de VLAN, la configuration du DHCP et l'active directory, l'utilisation de protocoles de routage comme GLBP, et l'agrégation de liens avec LACP.

Pour la réalisation, notre simulation est faite à base du simulateur GNS3 et VMWARE.

Mots clés : la haute disponibilité, le clustering, l'équilibrage de charge, RTC, VLAN, DHCP, VTP, GLBP, LACP, GNS3 et VMWARE.

.

ABSTRACT

The computer network is the essential pillar of any company, regardless of its sector of activity. It is therefore essential to guarantee the continuity of business operations. In our work, we focus on one of the most important high availability technologies, it is the establishment of a high availability cluster with load balancing. The main objective is to ensure operational continuity and to guarantee optimal performance of IT systems as well as the high availability of crucial services for companies dependent on their infrastructures by distributing the workload. To this end, we have concretely illustrated these concepts, we have described the configuration steps, taking into account different aspects such as the creation of VLANs, the configuration of DHCP and the active directory, the use of protocols routing like GLBP, and link aggregation with LACP.For the realization, our simulation is made based on the GNS3 and VMWARE simulator.

Key words : high availability, clustering, load balancing, RTC, VLAN, DHCP, VTP, GLBP, LACP, GNS3 and VMWARE.