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 vu de l'obtention du diplôme de Master
en Informatique

Option

Administration et sécurité des réseaux

Thème

Administration et supervision des réseaux en utilisant un cluster d'équilibrage de charge sous windows server 2016

Cas pratique : Entreprise Portuaire de Bejaia

Réalisé par : M. IBARISSEN Toufik & Mlle. RABAHI Fatima Zahra

Soutenu le 03 Juillet 2018 devant le jury composé de :

Président	**M^{r} AKILAL Abdellah**	**M.A.A**	**U. A/Mira Béjaia.**
Examinatrice	**M^{me} BOUADEM Nassima**	**M.A.A**	**U. A/Mira Béjaia.**
Encadreur	**M^{me} HOUHA Amel**	**M.A.A**	**U. A/Mira Béjaia.**

Béjaia, Juillet 2018.

⁕ *Remerciements* ⁕

$\mathcal{N}$ous remercions tout d'abord Dieu, le tous puissant de nous avoir accordé santé, courage et foie.

$\mathcal{N}$ous exprimons nos gratitudes les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire et qui ont accepté de répondre à nos questions avec gentillesse.

$\mathcal{O}$n tient à remercier sincèrement Mme HOUHA Amel, qui en tant qu'encadreur, s'est toujours montré à l'écoute ainsi que ses précieux conseils et son aide durant toute la période du travail.

$\mathcal{N}$os remerciements s'étendent également à notre maitre de stage Mr TOUATI ainsi qu'à tous nos professeurs et examinateurs de la Faculté des sciences exactes pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

$\mathcal{N}$ous remercions les membres du jury pour l'honneur qu'ils nous font en participant au jugement de ce travail.

$\mathcal{S}$ans oublier nos parents pour leur contribution, leur soutien et leur patience.

$\mathcal{E}$nfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours Soutenue et encouragée au cours de la réalisation de ce mémoire.

$\mathcal{M}$erci à tous et à toutes.

⁕ *Dédicaces* ⁕

C'est avec profonde gratitude et sincères mots, que nous dédions ce modeste travail de fin de cycle à nos chers parents ; qui ont sacrifié leur vie pour notre réussite et nous ont éclairé le chemin par leurs conseils judicieux. Nous espérons qu'un jour, nous pourrons leurs rendre un peu de ce qu'ils ont fait pour nous, que dieu leur prête bonheur et longue vie. Nous dédions aussi ce travail à nos frères et sœurs, nos amis, tous nos professeurs qui nous en enseignés et à tous ceux qui nous sont chers.

MLLE. ***Rabahi Fatima Zahra*** *&* *M.* ***Ibarissen Toufik***

Table des matières

Table des figures

Liste des abréviations

AD	**A**ctive **D**irectory
AD DS	**A**ctive **D**irectory **D**omain **S**ervices
AD FS	**A**ctive **D**irectory **F**ederation **S**ervices
ASCE	**A**ssociation **C**ontrol **S**ervice **E**lement
CAN	**C**ontroller **A**rea **N**etwork
CMIP	**C**ommon **M**anagement **I**nformation **P**rotocol
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ystem
EPB	**E**ntreprise **P**ortuaire **B**ejaia
ERP	**E**ntreprise **R**esource **P**lanning
FDDI	**F**ctive **D**istributed **D**ata **I**nterface
FTP	**F**ile **T**ransfer **P**rotocol
GED	**G**estion **E**lectronique des **D**ocuments
GMAO	**G**estion de **M**aintenance **A**ssistée par **O**rdinateur
HAN	**H**ome **A**rea **N**etwork
HTTP	**H**yper **T**text **T**ransfer **P**rotocol
HTTPS	**H**yper **T**text **T**ransfer **P**rotocol **S**ecure
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IP	**I**nternet **P**rotocol
ISO	**I**nternational **S**tandards **O**rganization
LAN	**L**ocal **A**rea **N**etwork
MAN	**M**etropolitan **A**rea **N**etwork
MIB	**M**anagement **I**nformation **B**ase
NAS	**N**etwork **A**ttached **S**torage
NIC	**N**etwork **I**nterface **C**ard
NLB	**N**etwork **L**oad **B**alancing
NMS	**N**etwork **M**anagement **S**tation
OID	**O**bject **I**dentifier
OSI	**O**pen **S**ystems **I**nterconnection
OSPF	**O**pen **S**hortest **P**ath **F**irst
PKI	**P**ublic **K**ey **I**nfrastructure
POP	**P**ost **O**ffice **P**rotocol
RAID	**R**edundant **A**rray **I**ndependent **D**isks
RDP	**R**emote **D**esktop **P**rotocol
RDS	**R**emote **D**esktop **S**ervices
RIP	**R**outing **I**nformation **P**irectory
ROSE	**R**emote **O**perations **S**ervice **E**lement

SAN	**S**torage **A**rea **N**etwork
SCSI	**S**mall **C**omputer **S**ystem **I**nterface
SI	**S**ystem **I**nformation
SMFA	**S**pecific **M**anagement **F**unctional **A**rea
SMI	**S**tructure of **M**anagement **I**nformation
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SSD	**S**olid **S**tate **D**rive
STP	**S**hielded **T**wisted **P**air
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
UTP	**U**nshielded **T**wisted **P**air
VPN	**V**irtual **P**rivate **N**etwork
WAN	**W**ide **A**rea **N**etwork
WDS	**W**indows **D**eployment **S**ervices

Introduction générale

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en œuvre. Le nombre des machines dans ces réseaux peut parfois devenir extrêmement élevé, la maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux importants, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.

Un réseau a donc nécessairement besoin d'un administrateur réseau et parfois même d'une équipe informatique de gestion de réseau. Son rôle est d'une telle importance et sa responsabilité est si grande que parfois on le considère comme la clef de voûte de l'économie de l'entreprise. Car si le réseau tombe en panne ou à des problèmes, l'entreprise est en danger.

Produire des systèmes stables demande de passer beaucoup de temps en études et en analyses. Heureusement, il existe des techniques simples permettant de pallier à la fiabilité des systèmes complexes, qu'ils soient matériels ou logiciels. Plutôt que de chercher à rendre ces systèmes stables, on peut inverser la démarche et intégrer à la source la notion de panne dans l'étude de ces systèmes : si l'on peut prévoir la panne d'un composant matériel ou logiciel, on peut alors l'anticiper et mettre en œuvre une solution de substitution. On parle alors de disponibilité du service, voire de Haute Disponibilité selon la nature de l'architecture mise en place.

C'est pour cela que nous avons opté pour la mise en place d'une solution avec tolérance aux pannes pour l'Entreprise Portuaire de Bejaia.

Le premier chapitre sera consacré à présenter des généralités sur les réseaux locaux, ainsi qu'au critère de disponibilité dans le réseau et le système d'information.

Le deuxième chapitre portera sur la présentation des notions de base de l'administration des réseaux et leur supervision informatique.

Par la suite, nous nous intéresserons dans le troisième chapitre, à la description de l'environnement de notre travail, en outre, notre organisme d'accueil qui est l'Entreprise Portuaire de Bejaia et nous nous étalerons sur l'étude de son réseau informatique, D'où nous tirerons une problématique.

Enfin, le quatrième chapitre, nous le consacrons pour la mise en place de notre travail qui consiste à mettre en place une solution d'équilibrage de charge que nous avons recommandé. L'exécution de la solution se fera dans un environnement virtuel sur VmWare sous Windows Serveur 2016.

Chapitre 1

Généralités sur les réseaux locaux

1.1 Introduction

Dans ce premier chapitre, nous allons présenter quelques notions de base sur les réseaux informatiques, les concepts et les modèles les plus utilisés, ainsi que les équipements d'interconnexion nécessaires et leurs caractéristiques, ensuite nous allons aborder la notion de haute disponibilité ainsi que la solution du Cluster.

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs terminaux en vue d'échanger, de partager des données, des ressources ou des informations. En d'autre terme c'est une infrastructure de communication reliant des équipements informatiques (ordinateurs, imprimantes...) par l'intermédiaire d'un support de communication et équipements d'interconnexion (concentrateur, commutateurs, , routeurs,...), permettant de partagé des ressources communes, en respectant des règles bien définies. Il existe plusieurs types de réseaux comme les réseaux industriels, informatiques, locaux.

1.2 Classification des réseaux

- **Selon la distance**

Un réseau est défini comme un groupe de deux ou plusieurs systèmes informatiques reliés entre eux. Il existe plusieurs types de réseaux informatiques, notamment :

Réseaux locaux (LAN) : Les ordinateurs sont géographiquement proches (c'est-à-dire dans le même bâtiment).

Réseaux étendus (WAN) : Les ordinateurs sont plus éloignés et sont connectés par des lignes téléphoniques ou des ondes radio.

Réseaux de campus (CAN) : Les ordinateurs se trouvent dans une zone géographique limitée, telle qu'un campus ou une base militaire.

Réseaux métropolitains (MAN) : Un réseau de données conçu pour une ville.

Réseaux domestiques (HAN) : Réseau contenu dans le domicile d'un utilisateur qui connecte les appareils numériques d'une personne.

On s'intéressera dans ce qui suit aux réseaux locaux.

1.3 Réseau local

Un réseau local (LAN) est un réseau informatique qui s'étend sur une zone géographiquement limité de quelques mètres à plusieurs centaines de mètres. Le plus souvent, un réseau local est confiné à une seule pièce, bâtiment ou groupe de bâtiments, cependant, un réseau local peut être connecté à d'autres réseaux locaux sur n'importe quelle distance via des lignes téléphoniques et des ondes radio. Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet standard) à 1 Gbps (Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1 000 machines[1].

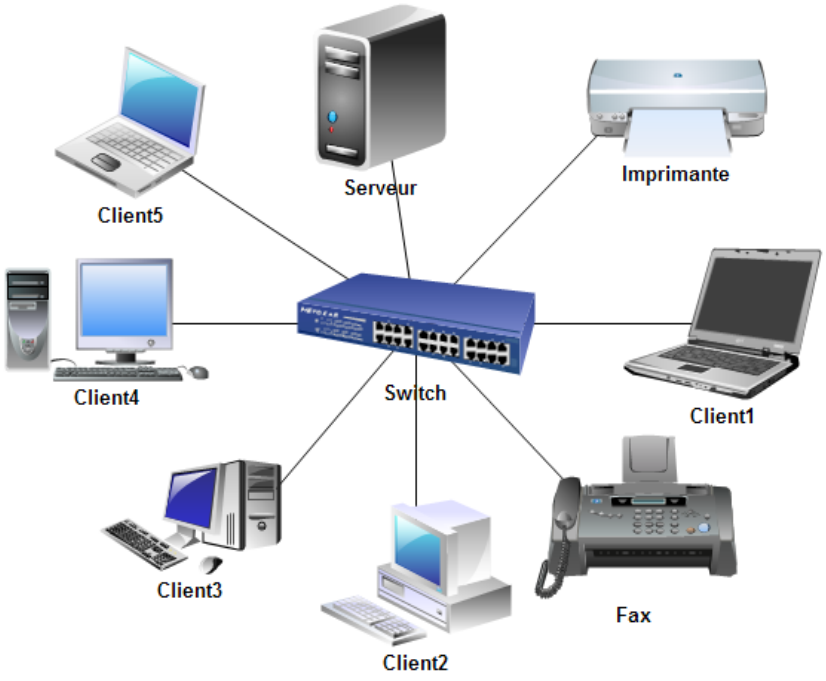


FIGURE 1.1 – Réseau local

1.3.1 Topologies des réseaux locaux

La topologie logique : représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token-ring et FDDI(Fiber Distributed Data Interface).

La topologie physique : désigne l'arrangement géométrique des dispositifs sur le réseau. Dans cette topologie nous avons trois grandes topologies qui sont :

- **Topologie en Bus**

Une topologie de bus est un réseau local dans lequel chacun des périphériques en réseau est connecté à un seul câble ou lien, comme illustré à la **Figure 1.2**. Dans cette topologie, une station (ordinateur) en panne ne perturbe pas le reste du réseau. Par contre, en cas de rupture du câble, le réseau est inutilisable, c'est l'ensemble du réseau qui ne fonctionne plus. Ce réseau utilise la technologie Ethernet 10 base 2.

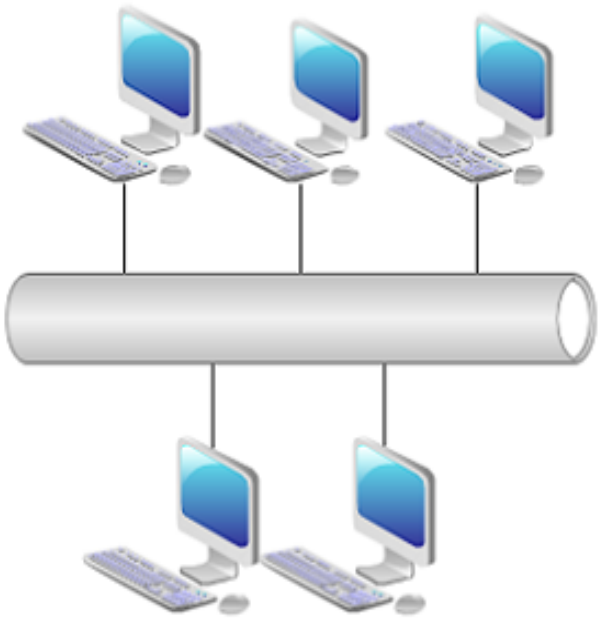


FIGURE 1.2 – Topologie en bus[2]

- **Topologie en Etoile**

La topologie en étoile est la topologie la plus répandue dans les réseaux actuels et inclut Ethernet, Fast Ethernet et Gigabit Ethernet. Chaque nœud dans une topologie en étoile se connecte à un lien dédié où l'autre extrémité se connecte à un commutateur ou un concentrateur. Dans ce réseau (illustré à la **Figure 1.3**), plusieurs périphériques sont connectés à un commutateur ou un concentrateur.

L'une des meilleures raisons d'utiliser une topologie en étoile est qu'une perte d'un nœud ne perturbe pas les opérations réseau. Il est également facile d'ajouter ou de supprimer un nœud du réseau. Du câblage à l'installation, il est particulièrement facile de configurer un réseau de topologie en étoile. mais les inconvénients sont : que le coût est un peu élevé, la panne du concentrateur centrale entraine le disfonctionnement du réseau. La technologie utilisée est l'Ethernet 10 base T, 100 base T.

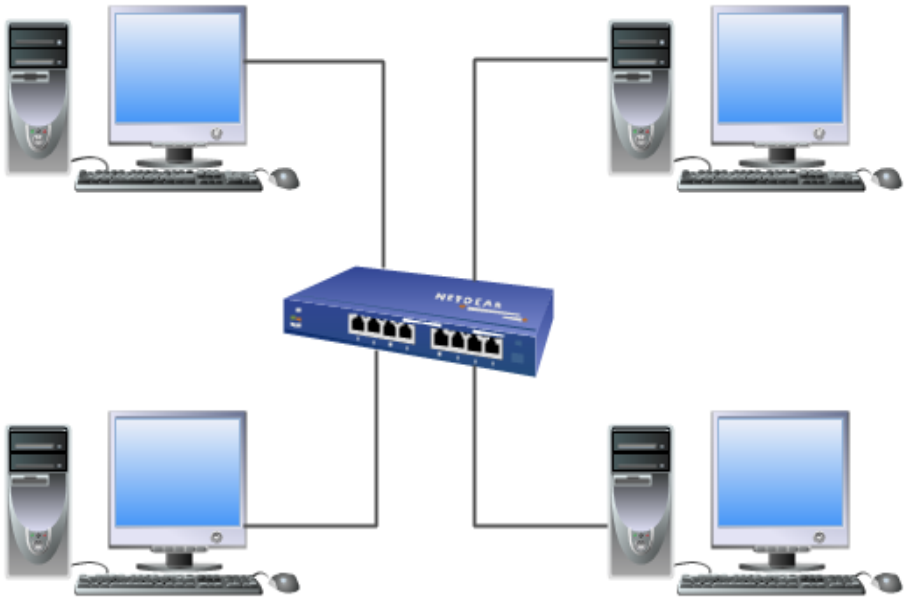


FIGURE 1.3 – Topologie en étoile[2]

- **Topologie en Anneau**

Dans une topologie en anneau LAN (illustrée à la **Figure 1.4**), comme dans un réseau local à topologie de bus, tous les nœuds ou périphériques du réseau sont connectés au réseau sur le même câble ou la même liaison. La différence est qu'une topologie en anneau fait un cercle complet. Token Ring et FDDI utilisent une topologie en anneau.

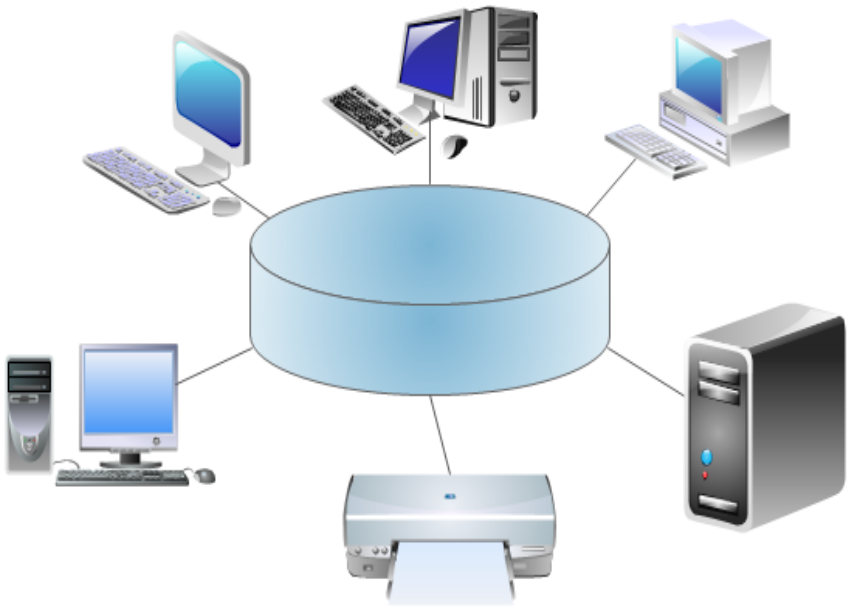


FIGURE 1.4 – Topologie en anneau[2]

1.3.2 Types de câbles

Les réseaux locaux sont connectés via différents supports [2] :

- **Coaxial** est constitué d'un noyau de fil de cuivre entouré d'isolant, d'un blindage métallique tressé et d'un couvercle extérieur.

- **Paire torsadée** dans sa forme la plus simple, le câble à paire torsadée (en anglais Twisted-pair cable) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants. On distingue généralement deux types de paires torsadées : les paires blindées (STP : Shielded Twisted-Pair) et les paires non blindées (UTP : Unshielded Twisted-Pair).

- **Fibre optique** fait circuler un faisceau lumineux qui est le support de l'information, ce qui permet au signal d'être isolé des perturbations extérieures.

1.3.3 Equipements d'interconnexion d'un réseau local

Il existe plusieurs équipements. Mais nous allons citer les plus importants :

- **Répéteur :** c'est un équipement électronique simple permettant d'amplifier un signal et d'augmenter la taille d'un réseau.
- **Concentrateur (Hub) :** il permet de concentrer le trafic réseau provenant de plusieurs hôtes, il agit au niveau de la couche physique du modèle OSI (Open Systems Interconnection).
- **Commutateur(Switch) :** c'est un pont multiport c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau de la couche 2 du modèle OSI.
- **Routeur :** c'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.
- **Passerelle(Gateway) :** c'est un système matériel et logiciel permettant de faire la liaison entre deux réseaux afin de faire l'interface avec le protocole du réseau différent.

1.4 Modèle OSI

1.4.1 Définition

Le modèle OSI (Open Systems Interconnection) est un outil de référence pour la compréhension des communications de données entre deux systèmes en réseau. La norme ISO (International Organization for Standardization) 7498-1 a défini ce modèle. Ce dernier permet à tous les éléments du réseau de fonctionner ensemble, peu importe qui a créé les protocoles et quel fournisseur d'ordinateurs les prend en charge. Il divise les processus de communication en sept couches. Chaque couche effectue à la fois des fonctions spécifiques pour supporter les couches au-dessus et offre des services aux couches situées en dessous. Les trois couches les plus basses se concentrent sur le passage du trafic à travers le réseau vers un système final. Les quatre couches supérieures entrent en jeu dans le système final pour compléter le processus [3].

Un tel modèle de fonctionnalité en couches est également appelé «pile de protocoles» ou «suite de protocoles».

Les protocoles, ou règles, peuvent faire leur travail dans le matériel ou le logiciel ou, comme avec la plupart des piles de protocoles, dans une combinaison des deux. La nature de ces piles est que les couches inférieures font leur travail dans le matériel ou le micro logiciel (logiciel qui fonctionne sur des puces matérielles spécifiques) tandis que les couches supérieures fonctionnent dans le logiciel.

1.4.2 Couches du modèle OSI

- **Couche physique :** la couche 1 définit les spécifications de connecteur et d'interface, ainsi que les exigences de support (câble). Des spécifications électriques, mécaniques, fonctionnelles et procédurales sont fournies pour l'envoi d'un train de bits sur un réseau informatique. Les composants de la couche physique comprennent :
  - Composants du système de câblage
  - Adaptateurs qui connectent les médias aux interfaces physiques
  - Conception du connecteur et affectations des broches
  - Spécifications du concentrateur, du répéteur et du panneau de brassage
  - Composants du système sans fil
  - SCSI parallèle (Small Computer System Interface)
  - Carte d'interface réseau (NIC)

- **Couche liaison :** la couche 2 du modèle OSI fournit les fonctions suivantes :
  - Permet à un périphérique d'accéder au réseau pour envoyer et recevoir des messages
  - Offre une adresse physique pour que les données d'un appareil puissent être envoyées sur le réseau
  - Fonctionne avec le logiciel réseau d'un appareil lors de l'envoi et de la réception de messages
  - Fournit une capacité de détection d'erreur

  Les composants réseau courants qui fonctionnent au niveau 2 incluent :
  - Cartes d'interface réseau
  - Commutateurs Ethernet et Token Ring
  - Des ponts

- **Couche réseau :** la couche 3, fournit un système d'adressage logique de bout en bout de sorte qu'un paquet de données peut être acheminé sur plusieurs réseaux de couche 2 (Ethernet, Token Ring, Frame Relay, etc.). Les adresses de couche réseau peuvent également être appelées des adresses logiques.

  Les routeurs communiquent entre eux en utilisant des protocoles de routage, tels que RIP (Routing Information Protocol) et OSPF (Open Version of Shortest Path First), pour connaître les autres réseaux présents et calculer la meilleure façon d'atteindre chaque réseau en fonction d'une variété de critères (tels que le chemin avec le moins de routeurs).

- **Couche transport :** la couche 4, offre une communication de bout en bout entre les équipements terminaux via un réseau. En fonction de l'application, la couche de transport peut être fiable, orientée connexion ou sans connexion. Certaines des fonctions offertes par la couche de transport comprennent :

  - Identification de l'application
  - Identification de l'entité côté client
  - Confirmation que le message entier est arrivé intact
  - Segmentation des données pour le transport en réseau
  - Contrôle du flux de données pour éviter les dépassements de mémoire
  - Établissement et maintenance des deux extrémités des circuits virtuels
  - Détection d'erreur de transmission
  - Réalignement des données segmentées dans le bon ordre du côté récepteur
  - Multiplexage ou partage de plusieurs sessions sur un seul lien physique

  Les protocoles de couche de transport les plus courants sont le protocole TCP (Transmission Control Protocol) orienté connexion et le protocole UDP (User Data Protocol) sans connexion.

- **Couche session :** la couche 5, fournit divers services, y compris le suivi du nombre d'octets que chaque extrémité de la session a accusé réception de l'autre extrémité de la session. Cette couche de session permet aux applications fonctionnant sur des périphériques d'établir, de gérer et de terminer une boîte de dialogue via un réseau. La fonctionnalité de la couche Session comprend :

  - Connexion virtuelle entre les entités d'application
  - Synchronisation du flux de données
  - Création d'unités de dialogue
  - Négociations de paramètres
  - Partitionnement des services en groupes fonctionnels
  - Remerciements des données reçues pendant une session
  - Retransmission de données si elles ne sont pas reçues par un périphérique

- **Couche présentation :** la couche 6, est responsable de la façon dont une application met en forme les données à envoyer sur le réseau. La couche de présentation permet essentiellement à une application de lire (ou de comprendre) le message.

Des exemples de fonctionnalités de couche de présentation incluent :

- Cryptage et décryptage d'un message pour la sécurité
- Compression et expansion d'un message afin qu'il se déplace efficacement
- Formatage graphique
- Traduction de contenu
- Traduction spécifique au système

- **Couche application :** la couche 7, fournit une interface pour l'utilisateur final qui exploite un périphérique connecté à un réseau. Cette couche est ce que l'utilisateur voit, en termes de chargement d'une application (comme un navigateur Web ou un e-mail), c'est-à-dire que cette couche d'application est la donnée que l'utilisateur visualise lors de l'utilisation de ces applications. Des exemples de fonctionnalités de couche d'application incluent :

  - Prise en charge des transferts de fichiers
  - Possibilité d'imprimer sur un réseau
  - Courrier électronique
  - Messagerie électronique
  - Parcourir le World Wide Web

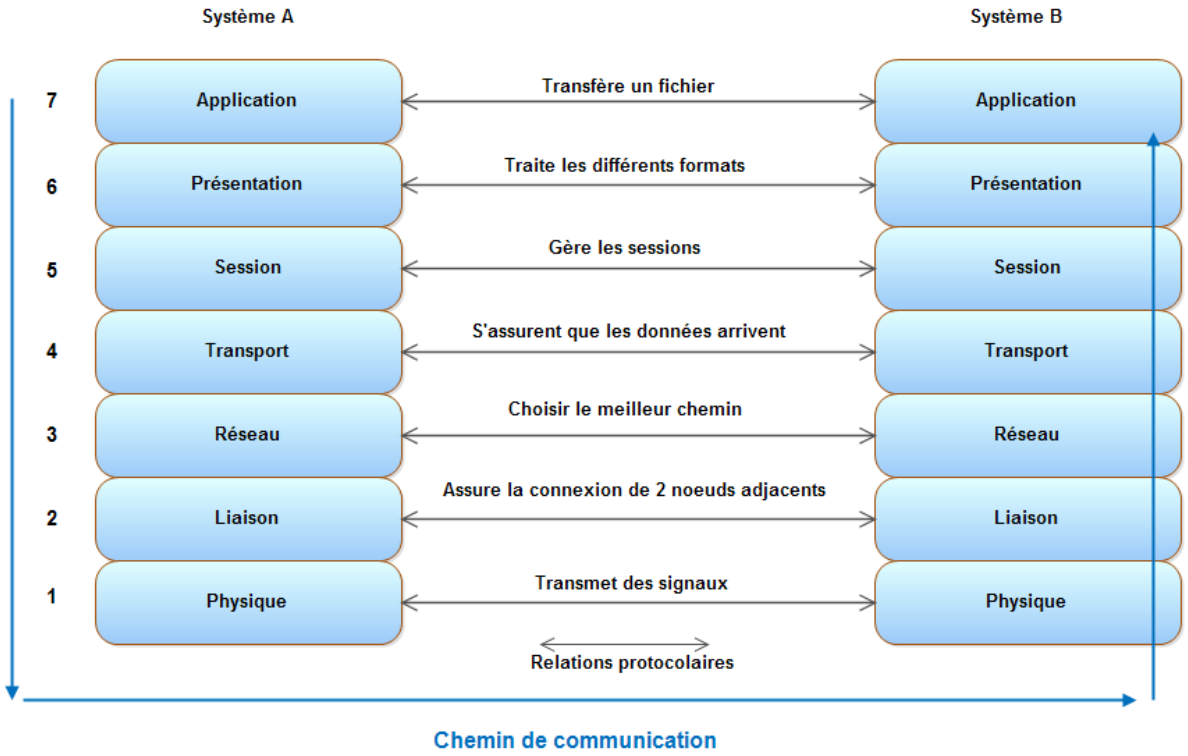


FIGURE 1.5 – Les couches du modèle OSI[3]

1.5 Modèle TCP/IP

1.5.1 Définition

TCP / IP ou "protocole de contrôle de transmission / protocole Internet", est une suite de protocoles de communication utilisés pour interconnecter des périphériques réseau sur Internet. TCP / IP peut également être utilisé comme protocole de communication dans un réseau privé (intranet ou extranet).

TCP / IP spécifie comment les données sont échangées sur Internet en fournissant des communications de bout en bout qui identifient comment elles doivent être divisées en paquets, adressées, transmises, acheminées et reçues à destination. TCP / IP nécessite peu de gestion centrale, et il est conçu pour rendre les réseaux fiables, avec la capacité de récupérer automatiquement à partir de la défaillance de n'importe quel périphérique sur le réseau.

Les deux protocoles principaux de la suite de protocoles Internet ont des fonctions spécifiques. TCP définit la manière dont les applications peuvent créer des canaux de communication sur un réseau. Il gère également la manière dont un message est assemblé en paquets plus petits avant d'être transmis sur Internet et réassemblé dans le bon ordre à l'adresse de destination.

IP définit comment adresser et acheminer chaque paquet pour s'assurer qu'il atteint la bonne destination. Chaque ordinateur passerelle sur le réseau vérifie cette adresse IP pour déterminer où transférer le message [4].

1.5.2 Architecture en couche du modèle TCP/IP

- **Accès réseaux**

La couche accès réseaux est la première couche du modèle TCP / IP. Elle définit la manière dont les données sont envoyées physiquement à travers le réseau, En fonction du type de réseau, des protocoles différents peuvent être utilisés à ce niveau. La couche d'accès réseau TCP / IP peut englober les fonctions des deux couches inférieures du modèle de référence OSI

- **Couche Internet(IP)**

La couche au-dessus de la couche accès réseau dans la hiérarchie de protocole est la couche Internet. Cette couche a pour rôle de traiter les paquets et connecter les réseaux indépendants pour transporter les paquets à travers les frontières du réseau. IP est le protocole le plus important de cette couche.

- **Couche Transport(TCP)**

La couche TCP correspond à la couche 4 de l'OSI et est responsable du maintien des communications de bout en bout à travers le réseau. TCP gère les communications entre les hôtes et assure le contrôle du flux, le multiplexage et la fiabilité. Les protocoles de transport incluent TCP et le protocole UDP, qui est parfois utilisé à la place de TCP à des fins spéciales.

- **Couche Application**

Enfin, la couche application (équivalente aux couches 5, 6 et 7 de l'OSI), fournit aux applications un échange de données standardisé. Ses protocoles comprennent le protocole HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), POP3 (Post Office Protocol), SMTP (Simple Mail Transfer Protocol) et SNMP (Simple Network Management Protocol).

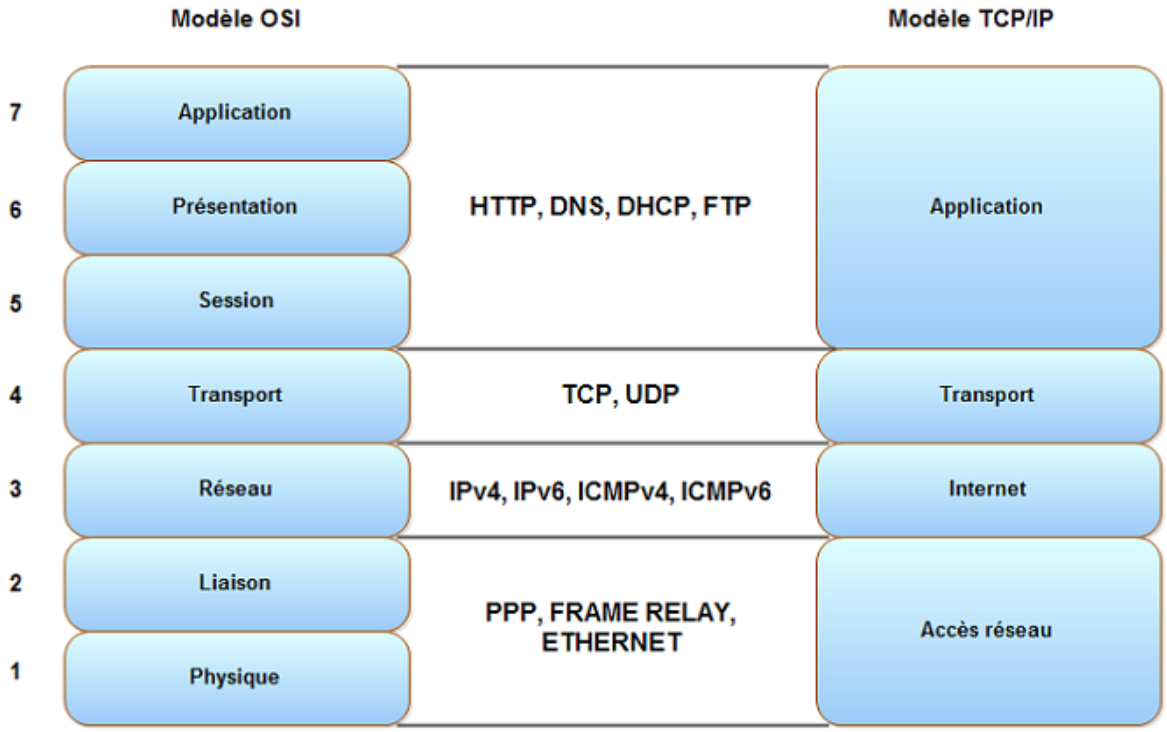


FIGURE 1.6 – Comparaison entre le modèle OSI et le modèle TCP/IP[5]

1.6 Critères de sécurité

Les critères de sécurité de base sont la disponibilité, l'authentification, l'intégrité et enfin la confidentialité. Dans ce qui suit, nous allons nous concentrer sur la disponibilité qui est un critère important. La disponibilité d'une ressource signifie que l'information est accessible lorsque les utilisateurs autorisés en ont besoin. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée.

1.7 Continuité opérationnelle

La continuité opérationnelle fait référence à la capacité d'une entreprise à résister aux événements critiques, et à faire fonctionner normalement et sans interruption des services importants, tout en ayant la capacité à continuer à remplir sa mission.

L'exigence la plus élémentaire en matière de continuité des opérations est de maintenir les fonctions essentielles en service durant les temps d'indisponibilité (arrêts planifiés ou non, pannes, sinistres) et de les rétablir avec le moins de temps d'arrêt possible (inférieur à 0,001 % de la durée du service totale).

Un environnement à haute disponibilité se caractérise par des objectifs qui sont plus exigeants en matière de temps de reprise (quelques secondes à quelques minutes) et de point de reprise [6].

1.8 Haute disponibilité

La haute disponibilité est une caractéristique d'un système qui vise à assurer un niveau de performance opérationnel convenu, généralement en temps de disponibilité, pour une période supérieure à la normale.

1.8.1 Critères de la haute disponibilité

Toute entreprise qui conçoit et met en œuvre une stratégie de haute disponibilité doit commencer par effectuer une analyse approfondie des pilotes métier nécessitant une haute disponibilité.

Une analyse des exigences de l'entreprise pour la haute disponibilité combinée à une compréhension du niveau d'investissement requis pour mettre en œuvre différentes solutions de haute disponibilité permet le développement d'une architecture à haute disponibilité qui atteindra les objectifs commerciaux et techniques.

Les éléments de ce cadre d'analyse sont [6] :

- **Budget**

Chaque solution à haute disponibilité implique un coût. Son coût doit être comparé aux avantages qu'elle apporte à l'entreprise.

Comprendre ce coût est essentiel car cela permet de prioriser l'investissement en haute disponibilité et a une influence directe sur les technologies de haute disponibilité choisies pour minimiser le risque d'indisponibilité.

- **Besoins en temps de disponibilité**

Les besoins en temps de disponibilité désignent la durée totale de disponibilité du système pour les applications des utilisateurs finaux. La valeur est exprimée en pourcentage du total des heures de travail planifiées.

- **Vue d'ensemble des types d'indisponibilité**

Prendre en compte les événements (panne, maintenance planifiée, arrêts non prévus) qui peuvent survenir est primordial pour choisir une solution à haute disponibilité.

- **Objectif de temps de reprise (RTO)**

L'objectif de temps de reprise est la durée maximale d'interruption admissible. Il s'agit du temps maximal acceptable pour effectuer la reprise d'une ou plusieurs ressources informatique (serveur, réseau, ordinateur, application) suite à une interruption majeure de service (planifiée, non planifiée ou sinistre), et relancer son fonctionnement normal.

- **Objectif de point de reprise (RPO)**

L'objectif de point de reprise désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne. Les modifications des données précédant la panne ou le sinistre et qui interviennent au moins dans cette plage de temps sont préservées grâce au processus de reprise.

- **Besoins en résilience**

Identification des entités qui doivent être disponibles même en cas de panne du système qui les hébergent.

- **Performance du système**

La solution de haute disponibilité choisie a souvent des implications sur les performances, c'est pour cela que l'entreprise doit choisir la technologie de résilience des données en fonction de ses besoins.

1.8.2 Avantages de la haute disponibilité

Les avantages de la haute disponibilité sont [6] :

- **Protection contre les temps d'arrêt**

Si un serveur critique tombe en panne, tous les serveurs qui interagissent avec lui s'arrêtent. Si un serveur tombe en panne, les solutions haute disponibilité vous permettent de migrer de manière transparente les opérations vers un serveur hôte. De cette façon, les relations avec la clientèle peuvent encore être maintenues, les employés peuvent continuer à faire leur travail, et les temps d'arrêt ne peuvent pas paralyser le fonctionnement critique de l'entreprise.

- **Simplifier la maintenance**

Les temps d'arrêt imprévus d'une catastrophe ne sont pas le seul type de temps d'arrêt auquel les entreprises sont confrontées. Les mises à jour matérielles et logicielles ou les mises à niveau sont d'autres exemples où les entreprises peuvent faire face à des temps d'arrêt coûteux. Avec les solutions haute disponibilité, ces temps d'arrêt peuvent être minimisés. Les entreprises peuvent planifier la restauration de leur serveur sur le site hôte et y exécuter la production pendant la modification de leurs opérations internes. De cette façon, les entreprises ne doivent pas être empêchées d'apporter les améliorations nécessaires et peuvent toujours mettre à jour leurs environnements informatique sans perdre de temps.

- **Réduction de la fenêtre de sauvegarde**

Les solutions à haute disponibilité permettent de réduire le temps d'indisponibilité du système ou des services pendant les sauvegardes. Le temps nécessaire à l'exécution d'une sauvegarde, de A jusqu'à Z, est appelé une fenêtre de sauvegarde. La difficulté consiste à sauvegarder la totalité des données dans cette fenêtre de temps.

- **Reprise après incidente**

Il s'agit d'un plan qui permet la reprise des applications suite à un sinistre. Cela permet de minimiser l'impact du sinistre sur l'activité de l'entreprise.

- **Équilibrage de charge**

Les solutions à haute disponibilité peuvent être utilisées pour l'équilibrage de charge. Les technologies les plus courantes d'équilibrage de charge consistent à déplacer le travail vers les ressources disponibles.

1.9 Cluster

Les solutions à haute disponibilité se basent sur la technologie de grappe(Cluster).

Un cluster haute disponibilité est un groupe d'hôtes qui agissent comme un seul système et fournissent une disponibilité permanente.

Par conception, le cluster est capable de détecter l'état de non disponibilité de l'un des serveurs par le principe du Heartbeat ou vérification de fonctionnement réciproque des serveurs. Selon la configuration mise en place, ce système pourra faire basculer automatiquement les ressources. Cette fonctionnalité offre ainsi une continuité de service des applications aux utilisateurs, elle permet aussi aux clients d'accéder aux applications et ressources lors d'arrêts planifiés de l'un des serveurs. Celles ci sont basculées automatiquement vers le serveur opérationnel [7].

Les clusters à haute disponibilité sont souvent utilisés à des fins d'équilibrage de la charge, de sauvegarde et de basculement.

Il existe deux modes de fonctionnement :

-Equilibrage de charge (Actif/actif) : NLB (Network Load Balancing)(**Figure 1.7**).

-Cluster avec basculement (Actif/passif)(**Figure 1.8**).

- **Equilibrage de charge**

En mode actif / actif, deux ou plusieurs serveurs regroupant la charge de trafic réseau. En cas de panne d'un des serveurs, une répartition dynamique de la charge et les connexions gérées par ce dernier se fera sur les autres serveurs [8]. La répartition de charge réseau fonctionne en trois modes différents de répartition :

La répartition manuelle : Elle permet de répartir le poids pour chaque noeud du cluster basé sur un poids de charge. Si trois serveurs sont configurés avec le poids 50, 30 et 20 ; le premier va recevoir la moitié des requêtes, le second 30 % et le dernier 20 %.

La répartition égale : Elle permet de répartir de façon égale les requêtes sur l'ensemble des serveurs composant le cluster. S'il y a trois serveurs dans la ferme du cluster, chacun recevra 33 % des requêtes.

La répartition prioritaire : Elle permet de mettre en place la notion de tolérance de panne en spécifiant un serveur prioritaire. L'ensemble du trafic est tout d'abord acheminé sur l'hôte ayant la priorité 1. Si celui-ci tombe en panne, l'ensemble du trafic sera envoyé au serveur de priorité 2 et ainsi de suite.

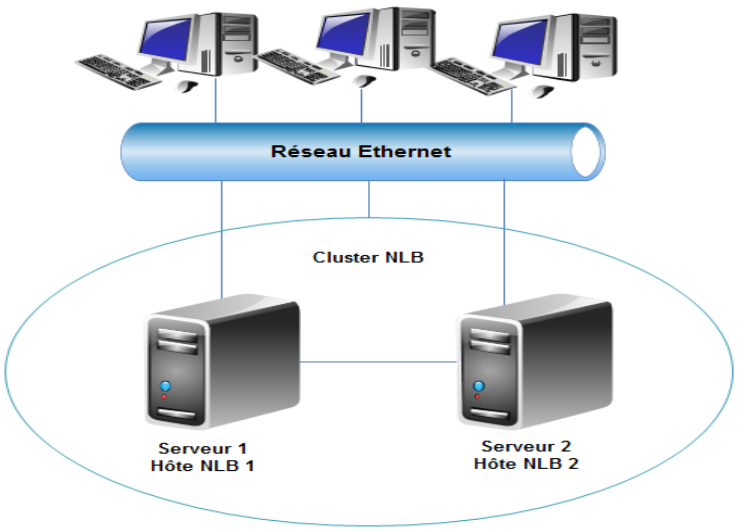


FIGURE 1.7 – Cluster avec équilibrage de charge

- **Cluster avec basculement**

Comme le mode actif-actif, actif-passif comprend également au moins deux nœuds. Cependant, comme l'indique le nom "actif-passif", tous les nœuds ne seront pas actifs. Dans le cas de deux nœuds, par exemple, si le premier nœud est déjà actif, le deuxième doit être passif ou en attente. Le serveur passif (failover) sert de sauvegarde prêt à prendre le relais dès que le serveur actif (primary) est déconnecté ou incapable de servir [9].

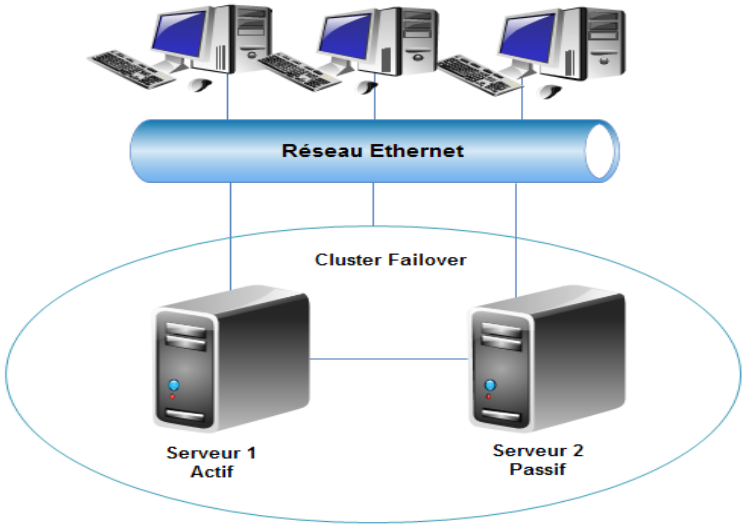


FIGURE 1.8 – Cluster avec basculement

1.10 Conclusion

Dans ce chapitre nous avons présenté les notions et les aspects élémentaires des réseaux informatiques et en particulier les réseaux locaux. Une panne ou même des travaux de maintenance entraîne une indisponibilité du réseau ou de l'un de ses composants, mais des mécanismes fondamentaux de sécurité et de disponibilité ont été mise en œuvre afin de rendre le réseau plus fiable. Dans le chapitre suivant, nous allons aborder l'administration et la supervision des réseaux, qui s'avère un domaine primordial pour la maintenance et la gestion d'un parc informatique.

Chapitre 2

Administration et supervision des réseaux

2.1 Introduction

Dans ce chapitre, nous allons présenter l'administration des systèmes est des réseaux qui repose fondamentalement sur la connaissance de l'infrastructure des réseaux et celle du fonctionnement des systèmes informatiques, ensuite, nous définirons les protocoles d'administration du réseau et les outils les plus utilisés pour réaliser les tâches d'administration.

2.2 Définition de l'administration réseaux

L'administration du réseau implique un large éventail de tâches opérationnelles qui aident un réseau à fonctionner de manière fluide et efficace. Sans administration de réseau, il serait difficile de maintenir le réseau.

Les principales tâches associées à l'administration du réseau comprennent :

- Conception, installation et évaluation du réseau.
- Exécution et administration de sauvegardes régulières.
- Création de documentation technique précise, telle que des schémas de réseau, des documents de câblage réseau, etc.
- Provision pour une authentification précise pour accéder aux ressources réseau.
- Provision pour assistance de dépannage.
- Sécurité du réseau, y compris la détection d'intrusion.

Il existe trois modèles d'administration des systèmes et des réseaux :

- Le modèle organisationnel, qui fournit les moyens de transfert des informations de gestions entre les objets administrés. Il définit également un dialogue (le CMIP : Common Management Information Protocol ISO 9596).
- Le modèle informationnel, qui décrit une méthode de définition des données d'administration. L'ensemble des éléments gérés est orienté objet et constitue une MIB (Management Information Base : ISO 10165).
- Et le modèle fonctionnel SMFA (Specific Management Functional Areas) qui définit des domaines fonctionnels d'administration et leurs relations. Il consiste en 5 domaines de compétence : la gestion des performances, la gestion des fautes, la gestion de la configuration, la gestion des informations comptables, et la gestion de la sécurité.

Dans la suite de cette section, nous allons détailler ces 5 modèles [10] :

2.2.1 Gestion des performances

La gestion des performances permet d'évaluer les performances des ressources(et la disponibilité) du réseau et de ses composants. Les performances du réseau sont calculées à l'aide de quatre paramètres bien précis :

- Le temps de réponse ;
- Le débit ;
- Le taux d'erreur ;
- La disponibilité(en terme de temps) ;

Le traitement des statistiques se déroule en quatre étapes :

- La collecte ;
- Le contrôle ;
- La présentation des informations ;
- L'archivage.

La collecte des informations consiste à mettre à jour les compteurs associés à chaque interface d'un élément actif(commutateur Ethernet ou routeur). les appareils du réseau, s'ils sont considérés comme supervisables (auquel cas ils intègrent toutes les fonctionnalités nécessaires) permettant à une station de supervision d'avoir une vue globale de leur fonctionnement (nombre de trames émises et reçues, volumétrie exprimée en octets, taux d'erreurs, collisions, répartitions du trafic par tailles de trames Ethernet...).

Dans le cas d'un systèmes TCP/IP, ces variables sont intégrées à une base de données MIB.

2.2.2 Gestion des fautes

Une fois connu l'état des composants (en terme de disponibilité ou de configuration) du réseau, il convient d'être informé des évènements qui peuvent perturber son fonctionnement.

Deux types de défauts peuvent alors se présenter et, pour optimiser le traitement, il convient de bien les différencier :

- Les défauts internes résultant d'une panne de l'élément actif lui-même (interface hors service), ou d'un état fortement dégradé (mémoire saturée entraînant une perte de données) ;
- Les défauts externes indépendants des appareils eux-mêmes, mais liés à l'environnement propre du réseau (alimentation électrique défaillante, lien inter-réseau coupé).

Le traitement d'une panne est composé de quatre étapes :

1. La signalisation du fonctionnement anormal d'un élément actif ou d'un lien inter-réseau ;
2. La localisation du défaut sur l'infrastructure ;
3. La réparation ;
4. La confirmation du retour à un comportement normal du réseau.

L'historisation des incidents peut aider le technicien ou l'ingénieur dans la compréhension des dysfonctionnements du réseau.

2.2.3 Gestion de la configuration

La gestion des configurations représente l'inventaire des ressources nécessaires au fonctionnement du réseau. On peut trouver par exemple le plan d'adressage et de routage IP du réseau, la gestion des noms de domaine...

On trouvera aussi dans la gestion des configurations un état du système : charge CPU ou mémoire, paramètres d'environnement tels la température dans le boîtier ou la consommation électrique d'un appareil.

2.2.4 Gestion des informations comptables

La gestion d'informations comptables permet d'établir les taxes d'utilisation des ressources et de définir les coûts correspondants. La gestion d'informations comptables comprend les fonctions suivantes :

- Informer les utilisateurs des coûts encourus et des ressources utilisées ;
- Permettre de fixer des limites comptables et d'associer des barèmes à l'utilisation des ressources ;
- Permettre de combiner les coûts quand plusieurs ressources sont utilisées pour atteindre un objectif de communication donné.

2.2.5 Gestion de la sécurité

La gestion de la sécurité est une fonction de gestion qui concerne le contrôle et la distribution des informations utilisées pour la sécurité. Elle englobe le cryptage et la liste des droits d'accès.

Voici les fonctionnalités qui doivent être mises en œ uvre :

- Il faut dans un premier temps assurer la sécurité relative à l'administration de réseau elle même, c'est-à-dire gérer les droits d'accès aux postes de travail, les autorisations d'accès aux informations de gestion.
- Ensuite, il faut garantir la sécurité des accès au réseau géré ; pour cela, il faut mettre en place des mécanismes qui impliquent des fonctions telles que :
  1. La définition des conditions d'utilisation
  2. L'activation ou la désactivation des mécanismes
  3. Effectuer un contrôle des accès et une détection des tentatives d'accès frauduleuses
- Enfin, il faut garantir la sécurité de l'information par la gestion de mécanismes de protection, de cryptage et de décryptage, et par la détection d'incidents, exemple : détection d'intrusion et détection de virus.

2.3 Disciplines de l'administration d'un système

L'administration de réseaux ne peut pas être isolée de son environnement. En effet il s'agit d'une partie intégrante d'un système plus général constitué de trois parties fondamentales qui sont :

- Les utilisateurs ou consommateurs de services.
- Les serveurs d'applications ou fournisseurs de services.
- La machine de transport reliant les utilisateurs aux fournisseurs.

Ces trois groupes déterminent les trois disciplines d'administration d'un système :

□ **Administration des utilisateurs**

Qui fournit l'ensemble des mécanismes pour :

- L'accessibilité et la connexion aux applications. En effet, l'utilisateur doit pouvoir se connecter aux différentes applications et, pour cela, il doit disposer d'un ensemble d'outils qui lui assurent la transparence des méthodes d'accès et de connexion aux différentes applications.
- L'accès aux serveurs de noms, afin de permettre la localisation des ressources et d'assurer à l'utilisateur l'existence et l'utilisation de ces ressources.
- La confidentialité et la sécurité : le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.
- La qualité de service, qui est la perception du réseau ressentie par l'utilisateur. Son exigence majeure concerne la disponibilité et les performances du système ainsi que sa capacité à assurer un service convenable.

□ **Administration des serveurs**

Qui recouvre l'ensemble des mécanismes à mettre en place pour :

- La connexion et la distribution des applications, cela afin de permettre l'interrelation des services
- La Gestion et la Distribution des données, doivent garantir la fiabilité de transmission des informations et offrir des outils permettant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes

- La gestion des applications, correspond essentiellement au contrôle et la protection des accès à ces applications par la distribution de droits, ainsi qu'à la fourniture de mécanismes de contrôle d'utilisation de ressources concernant l'application

□ **Administration de la machine de transport**

Qui consiste à fournir des mécanismes sur :

- Des opérations de réseau, dont le rôle est de permettre l'intervention sur le fonctionnement du réseau et la modification si nécessaire.
- L'inventaire, qui a pour rôle de tenir à jour en permanence la liste des éléments (logiciels et matériels) qui constituent un système réseau.
- L'évolution et les changements, dont l'objectif est de fournir un certain nombre d'informations permettant de déterminer les nouveaux besoins à prendre en compte et les parties du système concernées.
- La configuration, dont le but est de déterminer la meilleure configuration du réseau améliorant ainsi les performances du système, et par la même, sa qualité de service.

2.4 Surveillance du réseau

La surveillance du réseau fait référence à la pratique consistant à superviser le fonctionnement d'un réseau informatique à l'aide d'outils logiciels de gestion spécialisés. Les systèmes de surveillance de réseau sont utilisés pour garantir la disponibilité et les performances globales des ordinateurs (hôtes) et des services réseau. Ils permettent aux administrateurs de surveiller l'accès, les routeurs, les composants lents ou défaillants, les pare-feux, les commutateurs principaux, les systèmes clients et les performances du serveur parmi d'autres données réseau.

Ping est l'un des outils de surveillance de réseau les plus basiques.

Il est disponible sur la plupart des ordinateurs qui envoient des messages de test IP entre deux hôtes. N'importe qui sur le réseau peut exécuter des tests Ping de base pour vérifier que la connexion entre deux ordinateurs fonctionne et également pour mesurer les performances de connexion en cours.

2.5 Quelques outils de supervision

Il existe différent types d'outils de supervision ayant chacun leurs qualités et leurs défauts.

- Solutions propriétaires couteuses.
- Utilisation d'outils open source qui ont fait leurs preuves.

Néanmoins, lorsque l'on commence une étude afin de mettre en place un système de supervision, il est indispensable de se demander ce que l'on souhaite superviser :

Serveurs : CPU, mémoire, processus, espace disque, services,...

Matériels : Disques, cartes Raid, cartes réseau, température, alimentations, onduleurs,...

Réseaux : Bande passante, protocoles, switchs, routeurs, firewall, accès externes, bornes wi-fi,...

Dans ce qui suit, nous allons présenter quelques outils de supervision :

- **Solutions propriétaires**

Hp open view : est un outil de supervision reconnu sur le marché. Son principal avantage est la centralisation des informations sur un seul poste. Il a pour rôle de gérer et de surveiller entre autre les infrastructures et services réseaux. Ce logiciel est donc destiné aux moyennes et grandes entreprises qui souhaitent avoir une vue globale de leur réseau et de son état.

Ibm tivoli monitoring itm : les solutions ibm tivoli monitoring sont conçues pour une meilleure gestion des applications en ligne essentielles à l'entreprise en :

-Surveillant de manière proactive les ressources système vitales.

-En détectant efficacement les goulets d'étranglement et les problèmes potentiels.

-En répondant automatiquement aux événements.

- **Outils open source**

Zabbix : permet de superviser réseau, systèmes (processeur, disque, mémoire, processus,...). Zabbix offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. Le « serveur ZABBIX » peut être décomposé en 3 parties séparées : Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque... Le logiciel peut réaliser le monitoring via SNMP. Fonctionnalité intéressante, il est possible de configurer des "proxy Zabbix" afin de répartir la charge ou d'assurer une meilleure disponibilité de service.

Nagios (anciennement Netsaint) : est un logiciel qui permet de superviser un système d'information. Nagios est, avant toute chose, un moteur gérant l'ordonnancement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective). L'interface web est la partie graphique visible, via un serveur web tel que Apache, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activité.

Windows server 2016 : est un système d'exploitation pour serveurs x64 de Microsoft, faisant partie de la famille Windows NT destinée aux serveurs d'entreprise. Il est connu aussi sous le nom "Windows Server vNext". La première version en Technical Preview est sortie le 1er octobre 2014 en même temps que System Center 2016. La cinquième version de preview est disponible depuis fin avril 2016. Windows Server 2016 est sorti le 5 octobre 2016. Parmi les nouvelles fonctionnalités figurent l'utilisation de containers, les microservices et le cloud hybride.

Notre choix s'est porté sur Windows server 2016, que nous allons détailler plus en profondeur dans le chapitre 4.

2.6 Protocoles d'administration réseaux

2.6.1 SNMP (Simple Network Management Protocol

Dans ce qui suit nous allons présenter SNMP (Simple Network Management Protocol) [11], un protocole de gestion qui inclut un logiciel de surveillance réseau. SNMP proposé par l'IETF (Internet Engineering Task Force) en 1988 pour la gestion des réseaux TCP/IP est le protocole de surveillance et de gestion réseau le plus déployé et utilisé. Il comprend :

- Les appareils du réseau surveillé.
- Logiciel agent sur les périphériques surveillés.
- Un système de gestion de réseau (NMS), qui est un jeu d'outils sur un serveur qui surveille chaque périphérique sur un réseau et communique des informations sur ces périphériques à un administrateur informatique.

Les administrateurs peuvent utiliser le moniteur SNMP et gérer les aspects de leurs réseaux en :

-Recueillir des informations sur la quantité de bande passante utilisée sur le réseau.

-Sondage actif des périphériques réseau pour demander un statut à des intervalles spécifiés.

-Notifier l'administrateur par SMS d'une panne de l'appareil.

-Collecter les rapports d'erreurs, qui peuvent être utilisés pour le dépannage.

-Email une alerte lorsque le serveur atteint un niveau d'espace disque faible spécifié.

SNMP v3 est la version actuelle. Il doit être utilisé car il contient des fonctionnalités de sécurité qui manquaient dans les versions 1 et 2.

- **Fonctionnement du protocole SNMP**

SNMP a une architecture simple basée sur un modèle client-serveur. Les serveurs, appelés gestionnaires, collectent et traitent les informations sur les périphériques du réseau.

Les clients, appelés agents, sont tous les types de périphériques ou de composants de périphériques connectés au réseau. Ils peuvent inclure non seulement des ordinateurs mais également des commutateurs réseau, des téléphones, des imprimantes, etc.

Les agents fonctionnent à certain niveaux du modèle OSI (sur des couches choisies) et stockent les informations dans des bases MIB. De nombreuses MIB existent offrant un panel de fonctionnalités assez importantes[11].

SNMP permet le dialogue entre le gestionnaire et les agents afin de recueillir les objets souhaités dans la MIB (**Figure 2.1**).

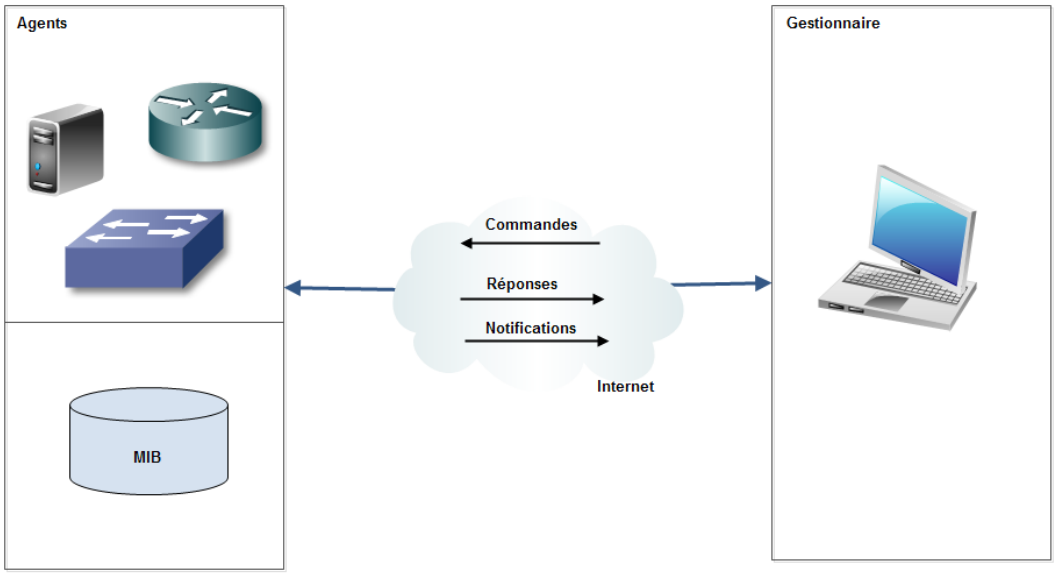


FIGURE 2.1 – Fonctionnement SNMP

Le protocole SNMP utilise le protocole UDP et communique sur les ports 161 et 162. Il est constitué de plusieurs commandes différentes, échangées entre agent et gestionnaire :

- Obtention de valeur courante d'un objet du MIB géré par un agent : requête get-request (GET) ;
- Obtention de la valeur courante du prochaine objet du MIB géré par un agent à partir d'un objet courant : requête get-request (GETNEXT) ;

- Mise à jour de la valeur courante d'un objet du MIB géré par un agent : requête setrequest (SET) ;
- Renvoi de la valeur d'un objet du MIB géré par un agent : requête get-reponse. C'est la réponse à un GET, GATNEXT ou SET. On voit que SNMP est un protocole de type commande/réponse sans états ;
- Signal émis par un agent en direction d'un manager (pour remonter une alarme par exemple) : message trap (TRAP).

- **Différentes versions de SNMP**

  - **SNMPv1** C'est la première version de SNMP qui a été très utilisée et qui l'est encore mais qui a un défaut majeur : une sécurisation très faible. il n'y a pas de cryptage des données et aucune authentification.
  - **SNMPv2** Cette seconde version [12] est une évolution de la version SNMPv1. De nombreuses évolutions ont existé : SNMPv2p, SNMPv2c, SNMPv2u.

    Le développement de SNMPv2c a permis de résoudre certaines limitations de SNMPv1. L'amélioration la plus remarquable a été l'introduction du type de message GetBulk et l'ajout de compteurs sur 64 bits à la MIB. La récupération d'informations à l'aide de GetRequest et de GetNextRequest constituait une méthode peu efficace de collecte. Avec SNMPv1, il était seulement possible de solliciter une variable à la fois. GetBulkRequest résout cette faiblesse en permettant de recevoir plus d'informations à la suite d'une seule requête. Cette version est toujours restée expérimentale et a laissé place à la version 3.
  - **SNMPv3 [13]** Cette version permet le cryptage des données. Il permet également aux administrateurs de spécifier des exigences d'authentification différentes sur une base granulaire pour les gestionnaires et les agents. Cela empêche l'authentification non autorisée et peut éventuellement être utilisé pour exiger le chiffrement pour les transferts de données.

  L'essentiel est que, bien que les problèmes de sécurité dans SNMPv1 aient valu à SNMP un mauvais nom dans certains cercles, SNMPv2 et surtout SNMPv3 ont résolu ces problèmes. Les nouvelles versions de SNMP fournissent un moyen sécurisé et à jour de surveiller le réseau.

- **Modèle SMI (Structure of Management Information**

La structure SMI (Structure of Management Information)décrit les règles de description de l'information et permet d'identifier de façon unique un objet de la MIB géré par un agent SNMP.

Chaque objet est identifié par ce que l'on appelle un OID (Object IDentifier). La hiérarchie de ces objets se représente sous la forme d'un arbre, les branches constituent les différents OIDs et les feuilles les variables.

Une variable peut donc être référencée par la liste ordonnée des différents OIDs parcourus à partir de la racine de l'arbre.

Le modèle SMI définit également les types de données utilisables pour les variables : entier, réel, durée, compteur, etc.

- **Structure MIB (Management Information Base**

La MIB (Management Information Base) est une base de donnée gérée par un agent SNMP regroupant les objets gérés en respectant les règles SMI. Elle possède une structure d'arbre similaire à celui employé dans le DNS (Domain Name System). On retrouve une racine non nommée à partir de laquelle on référencie de façon absolue un objet par son OID (nœd de l'arbre).

2.6.2 CMIP (Common Management Information Protocol)

CMIP (Common Management Information Protocol) est un protocole de gestion développé par ISO. Il peut être comparé au SNMP car les deux protocoles utilisent des tables MIB pour effectuer leur travail. Mais CMIP n'interroge pas les composants actifs, ce sont eux qui émettent des informations. Cette technique permet donc de réduire sensiblement le trafic sur le réseau. En contrepartie, la gestion de CMIP est beaucoup plus complexe, ce qui a été un frein à son expansion dans les petits réseaux et il est quasi exclusivement utilisé dans les réseaux opérateurs.

De plus, le protocole CMIP est défini pour fonctionner sur la pile du protocole OSI. Cependant, le standard utilisé de nos jours dans la majorité des environnements de réseaux locaux est le protocole TCP/IP [10].

CMIP fonctionne avec deux autres protocoles OSI de couche 7, ASCE (élément de service de contrôle d'association) et ROSE (protocole d'élément de service d'opérations distantes). Le premier gère les associations entre les applications de gestion, c'est-à-dire les connexions entre les agents CMIP, et le second gère les interactions d'échange de données.

Les applications utilisant CMIP on été divisé en 5 domaines fonctionnels : gestion des configurations, gestion des anomalies, gestion des performances, gestion de la comptabilité et sécurisation des données.

CMIP est un protocole totalement orienté « connexion » c'est-à-dire que chaque message est acquitté. Il est basé sur un principe de notification et d'évènements en gérant chaque variable comme étant un objet.

la structure CMIP comprend les composants suivants :

- Objet géré : caractéristiques d'un périphérique géré pouvant être surveillées, modifiées ou contrôlées et pouvant être utilisées pour effectuer des tâches.
- Agent de gestion : envoie les notifications et les alarmes à l'application de gestion de réseau.
- Application de gestion de réseau : initie des transactions avec l'agent de gestion en utilisant les opérations suivantes : action, cancel_get, create, delete, get et set.

Pour indiquer le passage à un sous-objet on utilise le point (.). Chaque nœud a un nom et un numéro unique.

2.7 Conclusion

Dans ce chapitre nous avons présenté les 5 domaines fonctionnels du modèle SMFA qui répartit les fonctions d'administration.

L'administration de réseau peut s'avérer un travail complexe. Pour aider l'administrateur dans sa tâche, nous avons illustré certains outils de supervision et des protocoles spécifiques tel que SNMP ou CMIP.

Le chapitre suivant va se porter sur la présentation de l'Entreprise Portuaire de Bejaia, l'étude de son réseau ainsi que ses différents équipements.

Chapitre 3

Présentation de l'organisme d'acceuil

3.1 Introduction

Ce chapitre a pour but de présenter l'organisme d'accueil EPB (Entreprise Portuaire de Bejaïa) qui nous a accueillis dans le cadre de notre stage de fin d'études, nous allons évoquer un bref aperçu de l'entreprise pour mieux connaitre sa structure et ses objectifs. Ensuite, nous allons étudier le réseau et ses composants pour pouvoir proposer d'éventuelles améliorations.

3.2 Présentation de l'entreprise

Le port de Bejaïa joue un rôle très important dans les transactions internationales vu sa place et sa position géographique.

L'EPB a été créé le 14 août 1982 suite au décret n° 82-285, elle est l'une des entreprise socialiste à caractère économique ; elle est transformée en Entreprise Publique économique, Société par Actions (EPE-SPA).

Aujourd'hui, il est classé 2e port d'Algérie en marchandises générales, et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir installé un système de management de qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire de Bejaïa a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail [14].

3.2.1 Ses missions

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de l'Entreprise Portuaire de Béjaïa, dans le but de promouvoir les échanges extérieurs du pays.

Les missions de l'EPB consiste en [14] :

- Le traitement, dans les meilleures conditions de délais, de coût et de sécurité, l'ensemble des passagers, des marchandises et des navires.
- La gestion et l'exploitation des infrastructures et des superstructures portuaires.
- La manutention et l'acconage des marchandises en transit par le port de Béjaïa.
- Le transit des passagers et leurs véhicules par la gare maritime du port de Béjaïa.
- La mise à disposition d'infrastructures nécessaires aux activités relatives aux hydrocarbures (exportation pétrole et de cabotage national des produits raffinés et gaz de pétrole liquéfié). Le pilotage, le remorquage et le lamanage des navires dans les limites de la zone de pilotage dans le port de Béjaïa.

3.2.2 Ses activités

Les principales activités de l'entreprise peuvent être énumérées comme suit [14] :

- L'exploitation de l'outillage et des installations portuaires.
- L'exclusion des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- L'exercice du monopole des opérations d'acconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.
- Le remorquage portuaire et hauturier.
- L'assistance-sauvetage des navires et engins en péril.
- La location de remorqueurs, l'avitaillement et le transport du matériel.
- La protection de l'environnement, la lutte contre les incendies.
- La réception des marchandises.
- Le transfert vers les aires d'entreposage des marchandises.
- La préservation ou la garde des marchandises sur terre-plein ou hangar.
- Marquage des lots de marchandises.
- Livraison aux clients.

3.3 L'organigramme de l'EPB

La **Figure 3.1** illustre la hiérarchie des différentes directions de l'EPB :

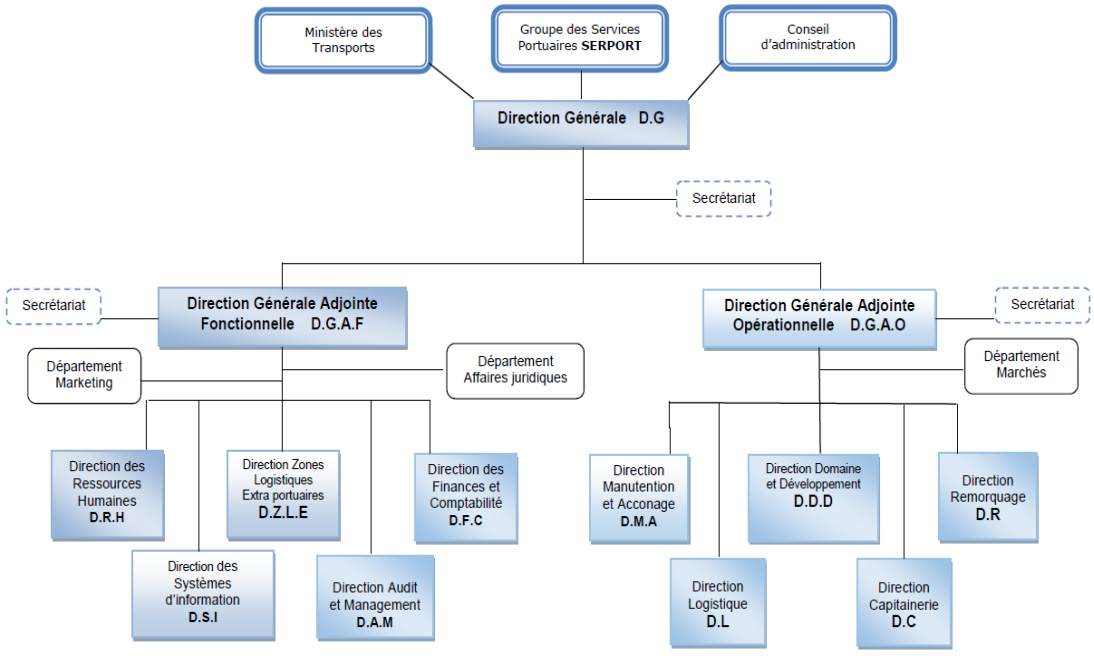


FIGURE 3.1 – Organigramme de l'EPB

3.4 Présentation du centre des systèmes et réseaux d'information de l'EPB

3.4.1 Organisation humaine du centre informatique

Le centre informatique se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI(Système d'information), chaque département est structuré en services comme le montre l'organigramme (**Figure 3.2**) [15] :

Département Infrastructure informatique : chargé de l'administration du réseau, des systèmes, de la sécurité, des serveurs, des bases de données ; des équipements (dotation, suivi, maintenance & helpdesk...)

Département Génie Logiciel : c'est le département chargé de l'administration et du suivi des applications développées en interne ou achetées chez un fournisseur externe, dépoilement et assistance chez les utilisateurs finaux. Exemple d'applications existantes : GMAO (gestion de la maintenance assistée pour ordinateurs), application escale, GED (gestion électronique de document), ERP (Enterprise Resource Planning) etc.

Département Programme Méthode et Organisation : c'est une administration qui s'occupe des programme méthode et organisations suivi des archives de l'affichage dynamique, communications interne, etc.

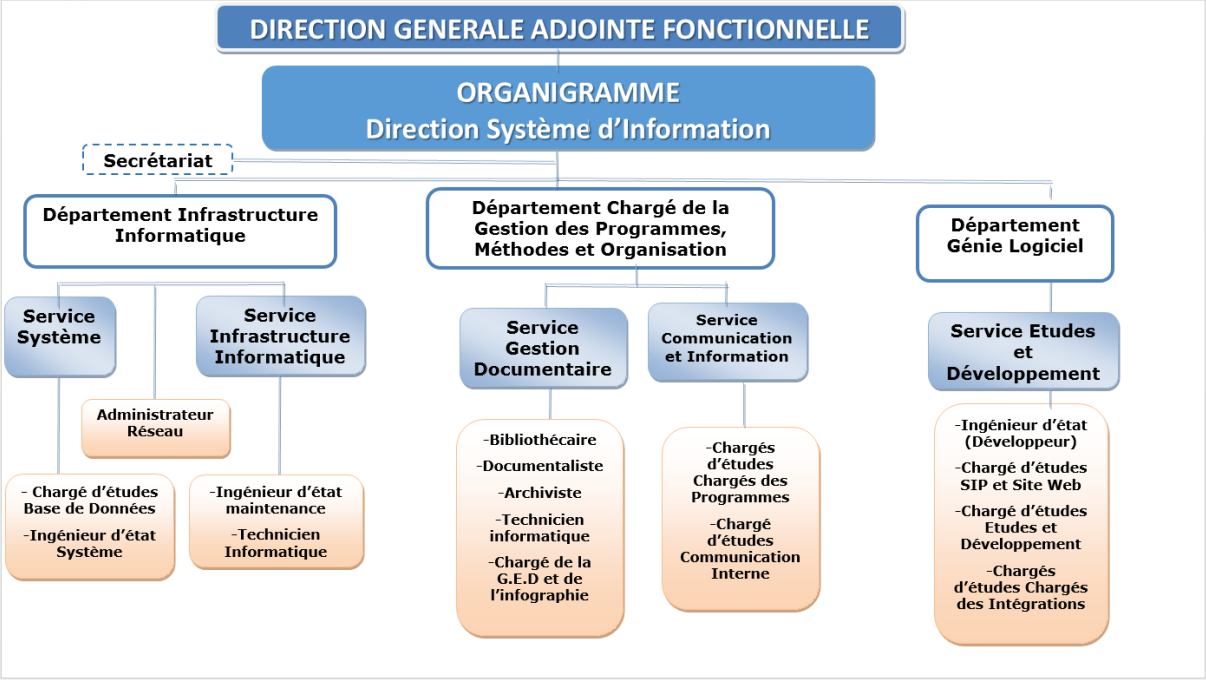


FIGURE 3.2 – Organigramme de la structure informatique

3.4.2 Missions du centre informatique

- L'informatique a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaia, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information.
- L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs.
- Le réseau apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

3.5 Parc informatique de l'EPB

La **Figure 3.3** représente l'architecture réseau de l'EPB.

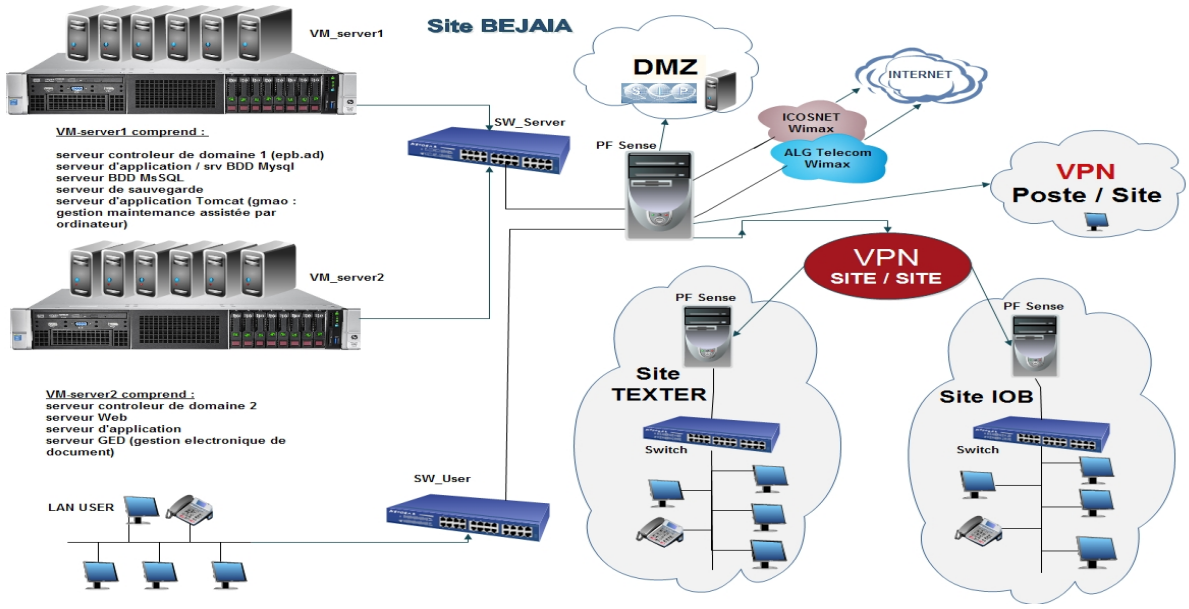


FIGURE 3.3 – Architecture réseaux de l'EPB

L'architecture du réseau de l'entreprise portuaire de Béjaïa est une architecture client-serveur plate. L'armoire de brassage constitue l'essence même du réseau de l'EPB elle contient les équipements réseau permettant aux employés de l'entreprise d'accéder à Internet et de faire de l'Intranet. On y distingue plusieurs switchs et platines où arrivent les câbles qui sont connectés aux différentes armoires de brassage de petite taille placées dans chaque étage du bâtiment, reliées aux prises murales où les employés connectent leurs ordinateurs. Les différents serveurs offrent des services aux différents postes clients.

Connexion internet : l'Entreprise Portuaire de Béjaïa s'est dotée de deux connections Wimax à savoir Algérie Télécom et Icosnet, Ce type de connexions permet de se connecter à Internet haut débit grâce à une antenne outdoor qui communique par des ondes hertzienne via une station de base située au mont Gouraya, d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

Sécurité : ces deux connexions sont reliées directement à un pare-feu PFSense configuré pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet.

Salle machine : la salle machine est le coeur du réseau toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des Switchs elle comporte les différentes machines serveurs :

- ☐ Deux contrôleurs de domaines DC1 et DC2 et également serveur DNS en plus l'infrastructure de clés publiques PKI hébergées dans DC1, DC2 hébergera un serveur DHCP et aussi un serveur WDS (Windows Déploiement Services).
- ☐ Serveur de base de données : qui répond à des demandes de manipulation de données stockées dans une ou plusieurs base de données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données.
- ☐ Un serveur de sauvegarde en réseau NAS(Network-attached storage) intégrant le système RAID : ce serveur, en collaboration avec la baie de stockage, ont pour rôle de sauvegarder en continu les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y ait un dysfonctionnement d'un ordinateur, le serveur est en mesure de rétablir le fichier perdu.
- ☐ Un serveur d'Application : c'est un serveur sur lequel sont installées quelques applications.
- ☐ Un serveur de messagerie externe Microsoft Outlook.

Il est à noter que l'entreprise s'appuie notamment sur l'utilisation de produits Microsoft sous licence particulièrement pour les systèmes d'exploitation.

L'EPB dispose de 220 PC HP et ACER répartis à travers les différentes directions de l'entreprise et interconnectés à un réseau informatique par fibre optique et câbles à paires torsadés. On y retrouve Windows 7 et XP pour les postes clients et Windows server 2012 pour les serveurs, elle favorise aussi l'exploitation de logiciels Open source.

- La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).

- Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.

- Tous les PC sont dotés d'un anti-virus ESET END point.

3.6 Problématique

L'étude que nous avons menée sur l'architecture nous a permis de retirer des faiblesses réseaux et qui sont les suivantes :

- L'utilisation de windows server 2012

  La date de fin du support standard est le 10/9/2018 et le support étendu est pour le 10/10/2023.

Il y a deux périodes de supports et donc deux dates de fin de support :

- ☐ La période de support standard durant laquelle sont disponibles les mises à jours fonctionnelles et celles ayant trait à la sécurité.
- ☐ La période de support étendu où seules les mises à jours de sécurité continuent à être proposées.

- Plan d'adressage

  Gaspillage d'adresse : les adresses sont de classe A avec un masque réseau de 8 bits ce qui n'est pas un choix judicieux compte tenu de la structure de l'entreprise.

- Architecture plate

  Absence de segmentation, donc un seul et unique domaine de diffusion ce qui implique une surcharge énorme du réseau, des machines surchargées mais non sollicitées.

- Absence d'équipements de secours

  Si un des ordinateurs de l'un des services de l'entreprise tombe en panne son utilisateur sera dans l'inaptitude de travailler et ce qui provoquera un retard ou un arrêt de ce service si l'ordinateur en lui-même contient un logiciel critique. Pour assurer la disponibilité et la continuité des données et des ressources dans une entreprise un serveur en redondance est important.

3.7 Solutions proposées

Notre travail consiste à mettre en œuvre d'autres améliorations à cette architecture pour un meilleur fonctionnement et pour assurer la disponibilité et la continuité de quelques services.

- ☐ Mise à niveau du système d'adressage : revoir le système d'adressage IP du réseau.
- ☐ Stockage des données dans un Cloud (Serveur virtuel distant), ce dernier garantie l'accessibilité, facilite la flexibilité et le partage, optimise les coût et automatise les mises à jour. L'entreprise n'a pas accepté cette solution à cause des temps d'arrêt qui sont souvent cités comme l'un des plus grands désavantages du cloud computing. Puisque les systèmes du cloud sont basés sur internet, les interruptions de services sont toujours une possibilité regrettable et peuvent survenir pour n'importe quelle raison. Si l'utilisateur n'a pas de connexion internet, ou une connexion insuffisante, il ne pourra accéder à sa plate forme de travail, ce qui fait qu'il ne pourra pas faire des sauvegarde au moment voulu.
- ☐ Mise à niveau des contrôleurs de domaines : migration vers une nouvelle plateforme Active Directory (système et paramétrages réseaux) sur les deux contrôleurs.

- ☐ Déploiement de deux serveurs RDS (Remote Desktop Services) qui donne la possibilité d'accéder à distance, faciliter les mises à jour des applications installées sur ces serveurs et l'administration des droits de chaque utilisateur.
- ☐ Proposition d'une solution de haute disponibilité qui va résoudre la contrainte de continuité opérationnelle de l'entreprise, augmenter la capacité totale ou les performances du système et réduire le risque de panne.

3.8 Conclusion

L'étude de l'existant nous a permis de nous familiariser avec notre structure d'accueil et aussi de bien nous imprégner dans le thème d'étude. Le réseau existant de l'EPB est assez conséquent et utilise une technologie avancée, mais présente des carences au niveau de la disponibilité (manque de redondance suffisante pour quelques ressources critiques).

Dans ce chapitre, nous avons commencé par présenter l'entreprise d'accueil, puis nous avons positionné la problématique et enfin nous avons défini nos objectifs principaux qui visent à apporter les solutions escomptées. Dans le chapitre suivant, nous allons détailler les solutions préconisées et leur mise en place.

Chapitre 4

Mise en œuvre de la solution

4.1 Introduction

Dans ce chapitre, nous allons détailler les différentes étapes pour la mise en place de notre solution au sein de l'EPB.

4.2 Présentation de Windows Server 2016

Windows Server 2016 est un système d'exploitation serveur développé par Microsoft, faisant partie de la famille de systèmes d'exploitation Windows NT (New Technology) destinée aux serveurs d'entreprise. Il présente de nombreux avantages, notamment pour les entreprises qui recherchent toujours la sécurité mais surtout pour la création de profits tout en réduisant les coûts.

4.2.1 Nouveautés de Windows Server 2016

- Nano server

Windows Server 2016 offre trois choix d'installation : Serveur avec Desktop Experience, Server Core et Nano Server, La taille de cette dernière option est réduite de 93 % par rapport aux installations Windows Server classiques. Le déploiement léger du Nano Server va plus loin que la simple installation du Core. Il réduit au minimum l'empreinte du système d'exploitation, en supprimant l'interface utilisateur graphique. Les activités administratives s'exécutent à distance via Core PowerShell, Microsoft Management Console ou les outils de gestion de serveur Web.

- Containers

Les containers sont des systèmes isolés qui sont mis à disposition pour des applications. ils vont donc s'appuyer sur les ressources de l'hôte, par exemple (le système d'exploitation, la mémoire). Ils démarrent donc beaucoup plus vite que les machines virtuelles classiques.

on retrouve deux types de conteneurs : Windows Server Containers et Hyper-V Containers.

- Espace de stockage direct

C'est une fonctionnalité Windows Server qui permet aux administrateurs de créer un stockage sur disque redondant et flexible avec une haute disponibilité. Espaces de stockage Direct dans Windows Server 2016 étend les espaces de stockage pour permettre aux nœuds de cluster de basculement d'utiliser leur stockage local à l'intérieur de ce cluster, évitant ainsi la nécessité préalable d'un stockage partagé.

- Réplication de stockage

Nouvelle fonctionnalité qui permet une réplication synchrone de niveau bloc et indépendante des ressources de stockage, entre serveurs ou clusters pour anticiper les désastres et effectuer une récupération.

- Administration

Windows PowerShell 5.0 intègre plusieurs nouvelles fonctionnalités importantes qui, en plus d'étendre et de simplifier son utilisation, permet de contrôler et de gérer les environnements Windows plus facilement et de façon plus poussée.

On retrouve également un système de corbeille dans l'AD (Active Directory), très utile lors d'une fausse manipulation, par exemple supprimer la mauvaise personne dans l'AD. Grâce à la corbeille, nous pourrons restaurer l'utilisateur dans l'AD. Cette fonctionnalité était manquante aux anciennes versions de Windows Server, mais peut s'avérer très utile en cas de mauvaises manipulations.

- Sécurité

Les services de domaines (AD DS) ajoutent la possibilité de définir une expiration d'appartenance à un groupe. Cela permet d'ajouter un utilisateur à un groupe pour une période de temps limitée (Exemple : fournir des privilèges d'administration pendant l'installation d'une application).

Les services de fédérations (AD FS) permettent notamment aux applications et services dans le cloud de s'authentifier à l'aide de l'annuaire local.

4.2.2 Avantages de Windows Server 2016

- Windows Server 2016 fournit la sécurité au niveau du système d'exploitation, y compris la résistance aux intrusions intégrée qui permet de repousser les attaques sur les systèmes. Des couches de sécurité supplémentaires détectent et limitent toute activité suspecte qui parvient à pénétrer l'environnement.

- Protection des machines virtuelles : permet l'utilisation de BitLocker pour chiffrer les machines virtuelles et veiller à ce qu'elles ne fonctionnent uniquement que sur des hôtes approuvés par le service Host Guardian Service (Service de gardien d'hôte).

- Sécurisation des informations d'identification de l'administrateur : aide à la protection des informations d'identifications des comptes administrateurs en utilisant les fonctionnalités Credential Guard et Remote Credential Guard . Il est aussi possible de contrôler les privilèges administrateur.

- Protection du système d'exploitation : résiste aux infractions en utilisant la fonctionnalité de sécurité Contrôleur de débit (Control Flow Guard) qui contribue à prévenir les attaques de corruption de mémoire et Windows Defender. Avec le dispositif de protection (Device Guard), nous pouvons nous assurer que seuls les applications de confiance seront exécutés sur le serveur.

- Amélioration de la capacité de détection des attaques : les fonctions d'audit avancées aident à détecter les programmes et comportements malveillants.

- Réduction des coûts : possibilité de créer des solutions évolutives de stockage définies par des logiciels selon le prix du SAN (Storage Area Network) ou du NAS (Network Attached Storage). En incluant la fonctionnalité Espace de stockage direct dans Windows Server 2016, Microsoft permet aux utilisateurs d'utiliser des serveurs standard avec un stockage local ou des disques à grande vitesse tels que les SSD (Solid State Drive).

- Création d'une continuité économique abordable : la réplication de stockage synchrone permet la récupération après sinistre, des centres de données. Cette fonctionnalité permet aux entreprises d'éviter le pire en termes financiers et matériel informatique.

4.3 Remote Desktop Services

RDS (Remote Desktop Services) autrement dit Service Bureau à distance permet à des utilisateurs d'accéder à leur bureau et applications de n'importe où que ce soit sur un poste ou un périphérique mobile, elle permet donc une meilleure efficacité de travail tout en permettant de sécuriser son infrastructure.

Le service RDS a évolué, anciennement nommé Terminal Services, nous retrouvons donc un service de bureau à distance plus simple avec des améliorations et des fonctionnalités en plus.

Les clients peuvent accéder à un serveur RDS par le biais d'une connexion bureau à distance ou à l'aide de programmes RemoteApp.

4.3.1 Rôles RDS

Par défaut, RDS propose tous les sous-rôles suivants :

- Remote Desktop Connection Broker (Courtier de connexion Bureau à distance)

Le courtier de connexion connecte les utilisateurs avec des postes de travail distants. Ce rôle permet d'équilibrer la charge entre les différents services. De plus, si un utilisateur perd la connectivité à un poste de travail distant, le courtier de connexion permet de rétablir la connexion sans perdre l'état du bureau virtuel.

- Remote Desktop Web Access (Accès Web Bureau à distance)

Ce composant permet aux utilisateurs d'accéder à des bureaux distants ou à des programmes RemoteApp via un navigateur web ou le menu démarrer. Il s'agit d'un site IIS avec une mire d'authentification pour permettre aux utilisateurs de s'identifier sur le portail et de sélectionner quelles ressources ils souhaitent exécuter.

- Remote Desktop Session Host (Hôte de session Bureau à distance)

Il s'agit du (ou des) serveur(s) qui hébergent les ressources qui sont exécutées par les utilisateurs. C'est notamment sur ce composant que seront hébergés les RemoteApps.

- Remote Desktop Gateway (Remote Desktop Gateway)

Ce composant permet la connectivité aux bureaux virtuels et aux programmes RemoteApp sur Internet.

L'utilisation du rôle RD Gateway apporte son lot d'avantages, notamment autour de la sécurité :

- ☐ L'encapsulation des flux RDP (Remote Desktop Protocol) (vidéo, souris, clavier, ...) dans HTTPS offrant ainsi les avantages de la sécurité, de l'intégrité et de la confidentialité associés au TLS(Transport Layer Security).
- ☐ La possibilité de configurer les politiques d'autorisations et de contrôles d'accès pour limiter les risques associés aux connexions d'Internet.
- ☐ La possibilité pour vos utilisateurs d'accéder à des ressources internes de votre entreprise sans besoin de mettre en place de VPN, en temps et en maintenance.

- Remote Desktop Virtualization Host (Hôte de virtualisation de bureau à distance)

Il s'agit du composant qui héberge les bureaux virtuels.

- Remote Desktop Licensing (Licence de bureau à distance)

C'est le rôle qui gère les licences RDS. Il en existe 2 types différents : licences par utilisateur ou licences par appareil.

Les applications et les bureaux de RDS sont accessibles à partir de divers périphériques clients, systèmes d'exploitation et facteurs de forme, ainsi que de navigateurs HTML5 et de clients Java. Les utilisateurs visualisent et interagissent avec les ressources RDS via un protocole d'affichage à distance. Microsoft fournit le protocole RDP avec Windows et les sociétés tierces peuvent également créer leurs propres protocoles, Citrix HDX et VMware PC-over-IP, par exemple.

4.3.2 Avantages de l'utilisation des RDS

- Travailler à distance

Les dirigeants d'entreprise et les employés ont besoin d'un accès fiable à leurs contacts, calendriers et documents, quel que soit l'endroit où ils se trouvent et l'heure à laquelle ils se trouvent. Remote Desktop Services est une excellente solution pour les besoins de mobilité actuels. Cela permet au personnel d'être productif à partir de n'importe quel endroit.

- Seul point de maintenance

Dans un environnement RDS, les applications sont installées sur un serveur RDS plutôt que sur des postes de travail individuels. En conséquence, les mises à jour d'applications deviennent beaucoup plus faciles car il n'y a qu'une seule copie de chaque application. Plus besoin d'assurer que les correctifs au niveau de l'application sont appliqués à tous les postes de travail de l'organisation.

- Le matériel de bureau a une durée de vie plus longue

En utilisant les services RDS, les entreprises peuvent réduire la durée de vie de leurs ordinateurs de bureau. Parce que tout le traitement se produit à la fin du serveur, les postes de travail agissent essentiellement comme des terminaux muets.

Cela signifie que l'utilisation du matériel de bureau existant reste une option viable bien plus longtemps que si les applications étaient exécutées localement. De même, l'exécution d'applications sur un serveur RDS peut permettre aux entreprises d'acheter du matériel de bureau bas de gamme, ce qui entraînerait des économies de coûts.

- Les PC de bureau ont une surface d'attaque plus petite

Étant donné que les services RDS impliquent des applications ou des sessions de bureau hébergées de manière centralisée, il n'est pas nécessaire d'installer des applications sur des postes de travail individuels.

Les administrateurs réseau peuvent verrouiller l'accès aux fichiers et au système à partir d'un seul point. Les serveurs RDS limitent considérablement la possibilité pour les sites distants de prendre des données d'une organisation.

Cela permet de réduire la surface d'attaque (comme dans les logiciels malveillants et les virus) des postes de travail de l'organisation. Généralement, les ordinateurs de bureau nécessitent un système d'exploitation, certains logiciels antivirus et un client RDS (fourni avec Windows). Tout le reste peut être exécuté sur le serveur.

- Performance, évolutivité et redondance

En plus d'augmenter l'utilisation des ressources d'un serveur pour prendre en charge de nombreux utilisateurs, lors de la détermination des spécifications matérielles d'un serveur RDS, un serveur "haut de gamme" avec une capacité supérieure à la moyenne sera généralement utilisé. Il existe des formules et des directives pour déterminer quelles sont les ressources nécessaires pour un serveur RDS en fonction du nombre d'utilisateurs, des types d'applications en cours d'exécution, etc.

Un autre aspect de la performance est dans le système d'exploitation lui-même. Les services Microsoft Remote Desktop ont été spécialement conçus pour accueillir de nombreux utilisateurs et sont spécialement adaptés à cette fin.

Dans les très grandes installations où un serveur RDS unique ne gère pas la charge, le clustering de serveurs RDS entre en jeu. Le clustering regroupe plusieurs serveurs RDS dans un cluster avec la possibilité de répartir automatiquement la charge entre les utilisateurs sur différents serveurs RDS. En utilisant cette méthode, la mise à l'échelle est presque illimitée quant au nombre d'utilisateurs pouvant être pris en charge.

Outre l'utilisation de la mise en cluster pour l'évolutivité, elle peut également être utilisée pour la redondance. En cas de défaillance d'un serveur RDS, les serveurs RDS restants du cluster sont toujours disponibles pour prendre en charge ses utilisateurs.

4.4 RemoteApp

Remoteapp est une solution d'application virtuelle qui permet aux utilisateurs d'exécuter des applications basées sur Windows, quel que soit le système d'exploitation qu'ils utilisent. Il permet aux utilisateurs de lancer des applications virtuelles à partir d'un serveur qui apparaît sur leur ordinateur comme s'il était installé localement, mais qui fonctionne en réalité sur un serveur distant.

Le programme RemoteApp s'exécute dans sa propre fenêtre redimensionnable, peut être déplacé entre plusieurs moniteurs et possède sa propre entrée dans la barre des tâches.

4.5 Explication du travail

Dans le cadre de notre travail, nous avons fait appel au logiciel VMware qui permet de simuler plusieurs machines.

Dans un premier temps, nous allons installer un environnement virtuel qui simule l'environnement logique de l'entreprise EPB. L'installation de Windows Server 2016 est très classique et ressemble à celle de Windows 10. ensuite nous allons créer un contrôleur de domaine auquel nous affecterons les rôles de serveur DNS et DHCP. Le nom de domaine est V-EPB.

Après cela, nous mettrons en place deux machines qui vont contenir nos RDS (RDS01 et RDS02) pour l'accès à distance et le cluster qui va assurer l'équilibrage de la charge.

Et enfin, nous installerons une machine cliente sous Windows 7 pour les tests de basculement entre les RDS.

Toutes ces machines seront introduites dans le domaine afin de communiquer entre elles.

4.6 Installation de Windows Server 2016

Après avoir suivi les étapes d'installation du système qui se fais soit en démarrant depuis un DVD, ou depuis une image ISO, la console Gestionnaire de serveur (**Figure 4.1**) se lance par défaut à l'ouverture de session sur le serveur.

Cette console permet de regrouper les outils essentiels liés à l'administration d'un serveur Windows local ou distant. Grâce à celle-ci, un administrateur système peut rapidement avoir accès aux éléments suivants :

-La gestion des fonctionnalités de serveur.

-La gestion de certains rôles de serveur.

-La gestion des serveurs distants.

-La gestion de la configuration du serveur local.

-La gestion des services de fichiers et de stockage...etc.

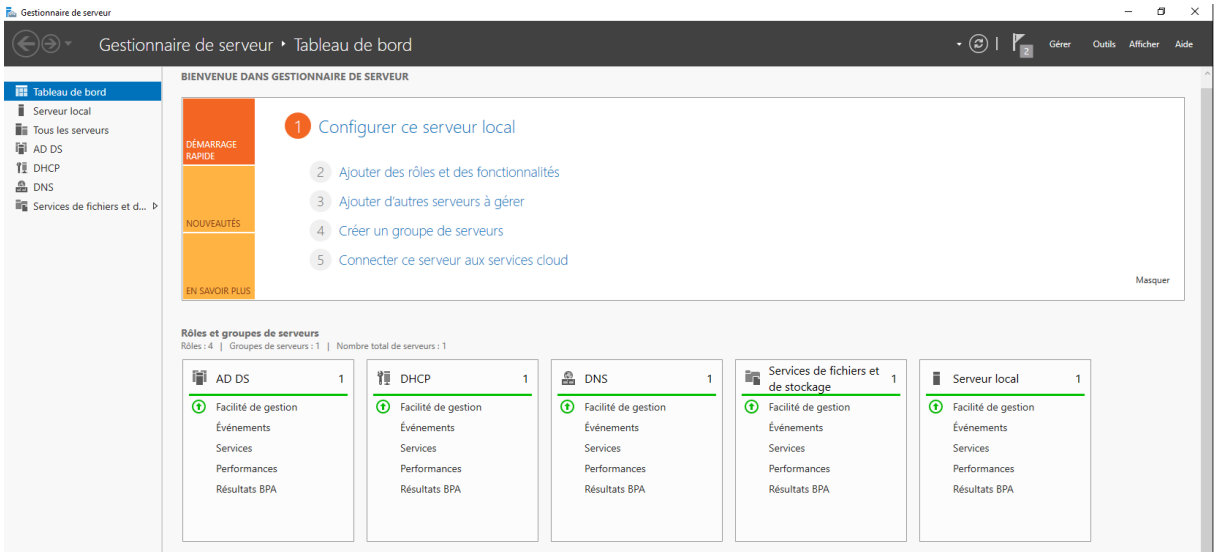


FIGURE 4.1 – Gestionnaire de serveur

Avant d'entamer l'installation de l'AD, nous avons configuré notre serveur local en lui définissons les propriétés de base (**Figure 4.2**).

FIGURE 4.2 – Configuration du serveur local

L'adresse IP statique est nécessaire pour le serveur, parce que les autres ordinateurs doivent avoir accès au serveur. Si elle est modifiée, les ordinateurs clients ne peuvent pas trouver le serveur.

Nous avons attribuer l'adresse IP du DNS (Domain Name System) car lorsque nous installerons AD sur le serveur Windows, il va automatiquement installer le DNS.

- **Installer le rôle "services de domaine AD"**

En cliquant sur "ajouter des rôles et des fonctionnalités", l'assistant d'ajout s'ouvre, ensuite on sélectionne le serveur local et le rôle AD DS (Active Directory Domain Services), Une fenêtre va apparaitre pour indiquer que d'autres éléments requis AD DS doivent être installés.

Une fois les fonctionnalités d'AD DS installées, le serveur va redémarrer automatiquement. Nous devons promouvoir ce serveur en tant que contrôleur de domaine (**Figure 4.3**), sinon le domaine ne sera pas crée.

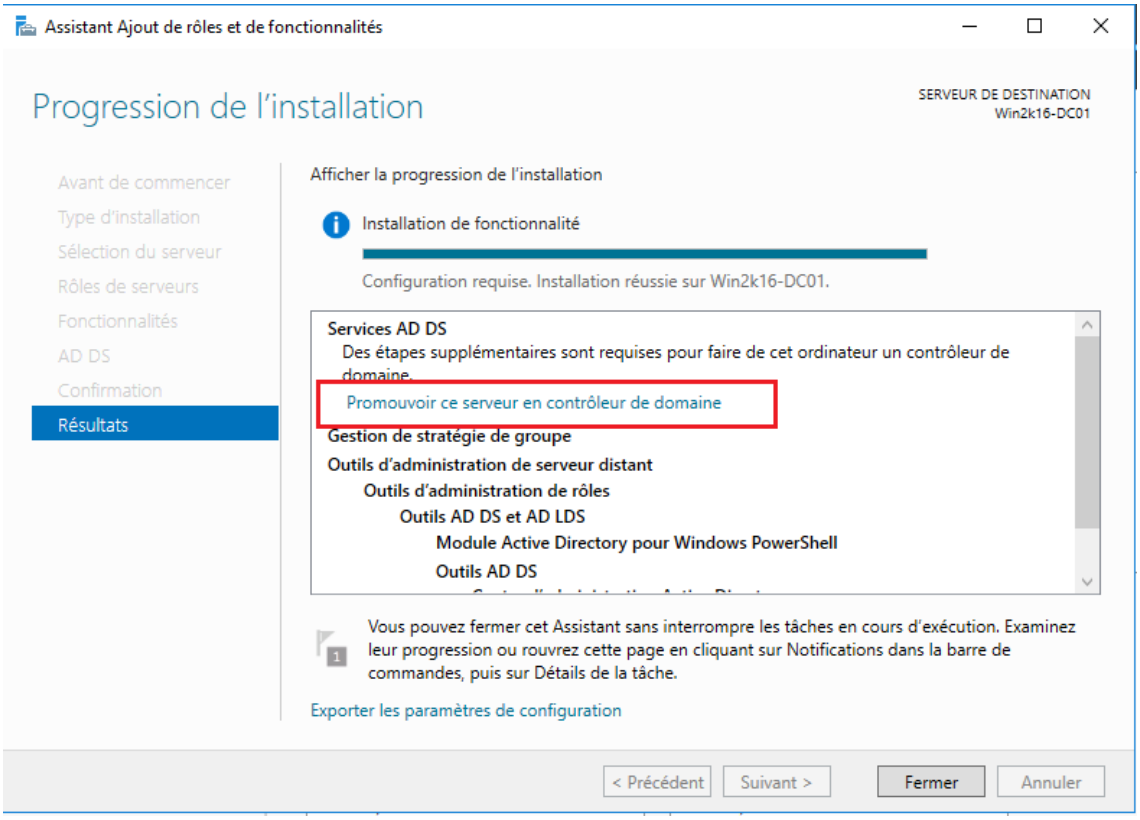


FIGURE 4.3 – Promouvoir le serveur

Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en cochant sur "Ajouter une nouvelle forêt" et en spécifiant le nom de note domaine appelé V-EPB.LOCAL (**Figure 4.4**).

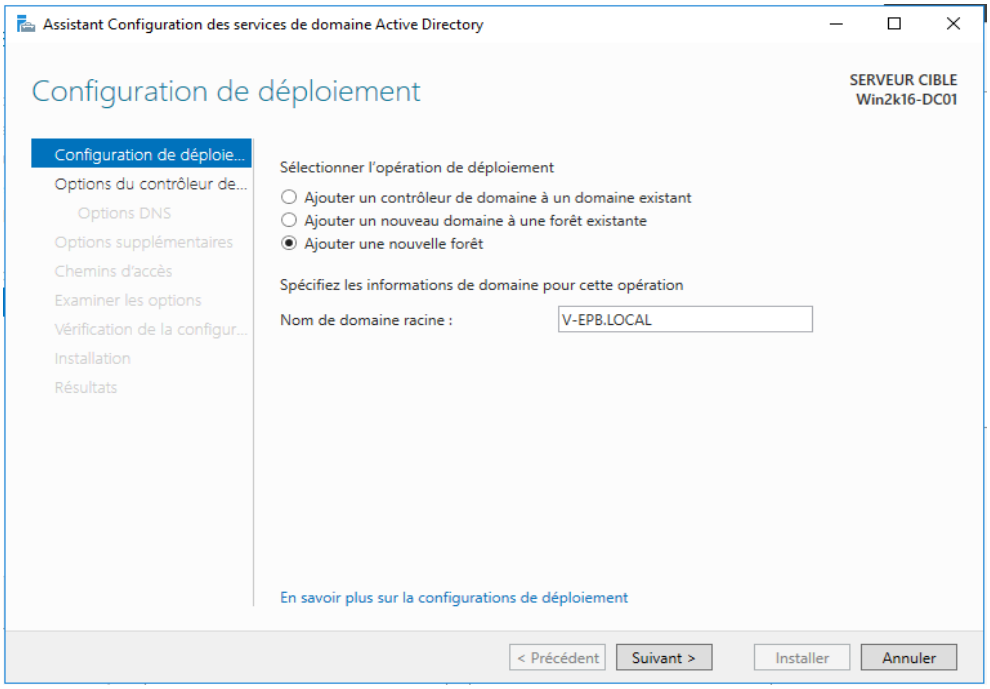


FIGURE 4.4 – Création du domaine V-EPB

L'étape suivante (**Figure 4.5**) consiste à choisir le niveau fonctionnel de domaine et de forêt, et le mot de passe pour DSRM (Directory Services Restore Mode).

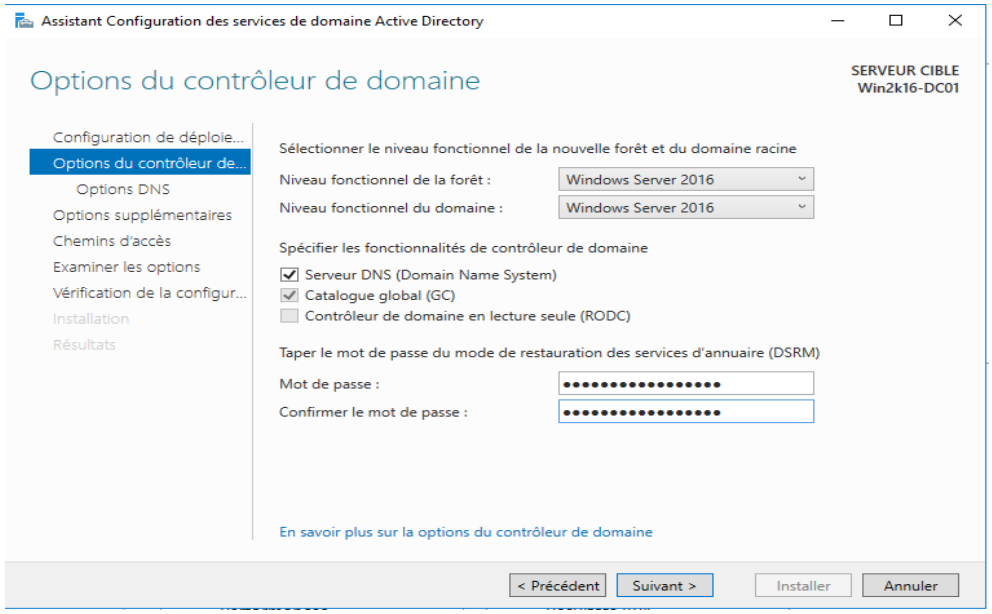


FIGURE 4.5 – Sélection du niveau fonctionnel de la forêt et du domaine

Lorsque nous installons les services de domaine Active Directory (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS. La zone DNS résultante est intégrée à AD DS contrôlé par le serveur Win2K16-DC01. Pour les options DNS, cela va être le premier serveur DNS dans la nouvelle forêt. Donc pas besoin de modifications.

Apres configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu outils.

Notre domaine est crée et l'ouverture d'une session s'effectue avec le compte d'administrateur du domaine V-EPB (**Figure 4.6**).

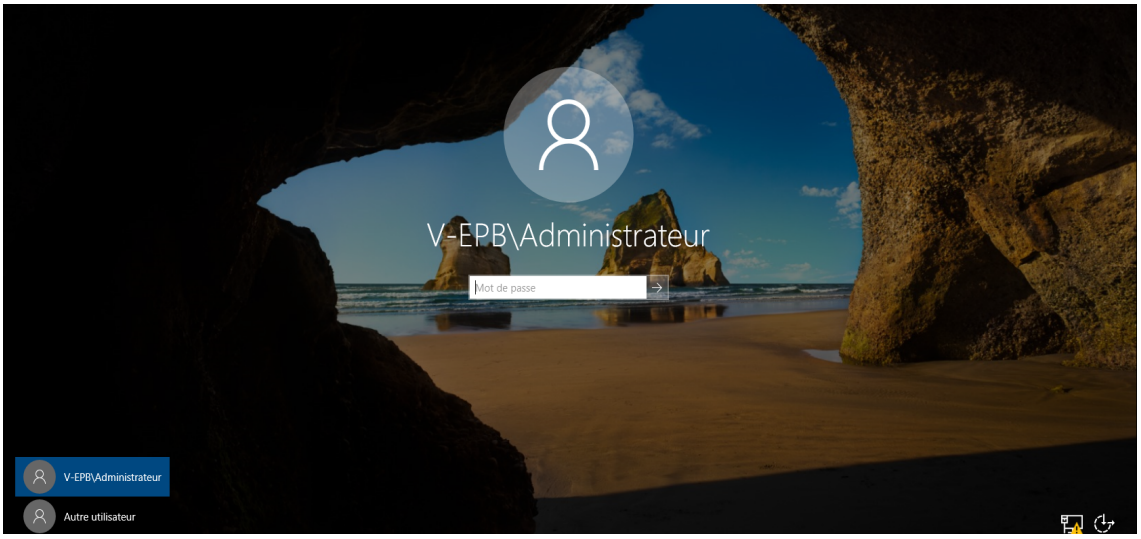


FIGURE 4.6 – Ouverture de la session Administrateur

En ouvrant le PowerShell (en tant qu'administrateur) et en introduisant la commande dsac.exe le centre administratif du répertoire actif s'ouvrira. Là, on pourra commencer à gérer les ressources.

Les deux commandes Get-ADDomain | fl Nom, DomainMode et Get-ADForest | fl Nom, ForestMode servent à confirmer les niveaux fonctionnels de domaine et de forêt (**Figure 4.7**).

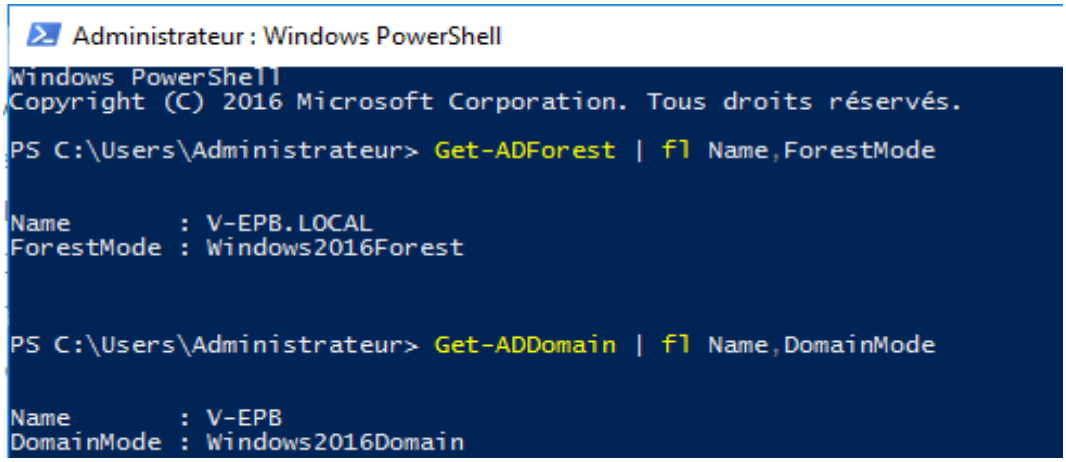


FIGURE 4.7 – Vérification du domaine et de la fôret

- **Installation et configuration du service DHCP(Dynamic Host Configuration Protocol)**

La principale fonctionnalité du serveur DHCP est de fournir aux clients une adresse IP, un masque de sous-réseau, une adresse DNS et une adresse de passerelle à chaque fois que les clients demandent dans le réseau en mode de configuration automatique.

Dans l'assistant de gestion des rôles, on ajoute le rôle DHCP. Après l'installation du rôle DHCP, la section suivante est la configuration, comment et quelles plages d'adresses IP utiliser, quel routeur passerelle et serveur DNS peuvent être utilisés et pendant combien de temps il doit être utilisé.

Création de nos étendues DHCP à l'aide de la console d'administration DHCP qui a été lancée depuis le menu Outils du gestionnaire de serveur (**Figure 4.8**).

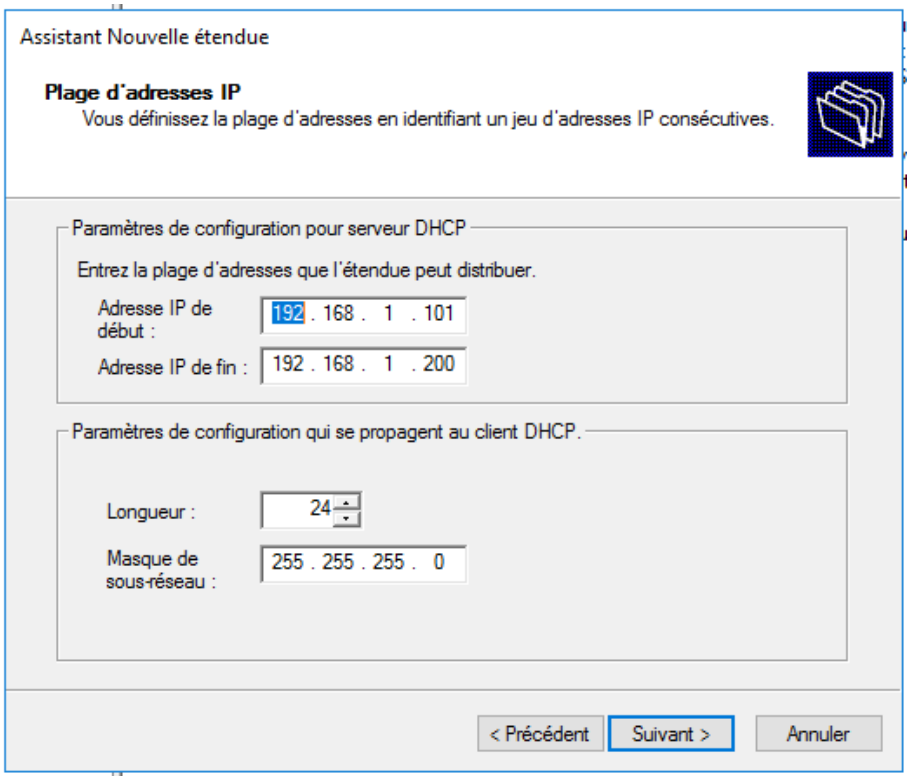


FIGURE 4.8 – Création des étendues DHCP

La portée DHCP a une plage valide de pool d'adresses IP à donner aux clients par crédit-bail, l'option de réservation d'adresse mac, d'exclusion et d'autres possibilités peut être effectuée (**Figure 4.9**).

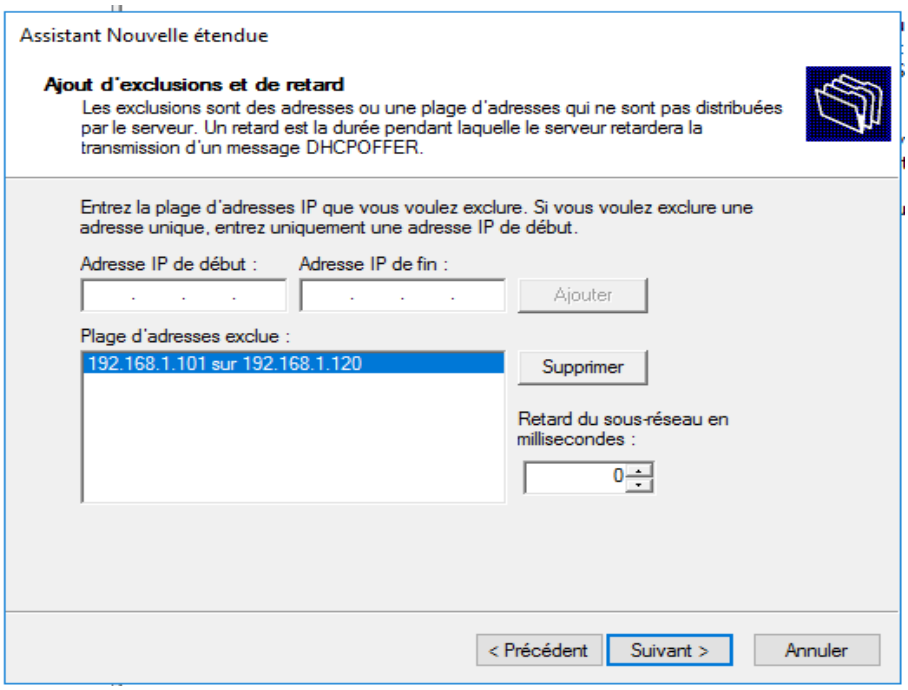


FIGURE 4.9 – Ajout d'exclusion DHCP

Ici (**Figure 4.10**), nous pouvons spécifier les routeurs, les passerelles par défaut à distribuer par cette portée.

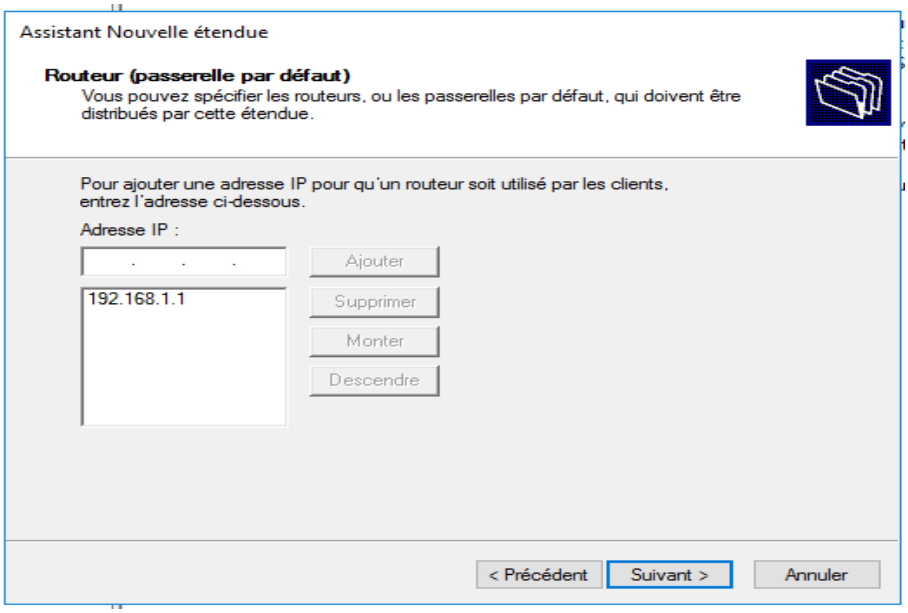


FIGURE 4.10 – Ajout de l'adresse IP de la passerelle

Nous avons mentionner les adresses IP du serveur DNS en fonction de la configuration que nous voulons que notre client utilise (**Figure 4.11**).

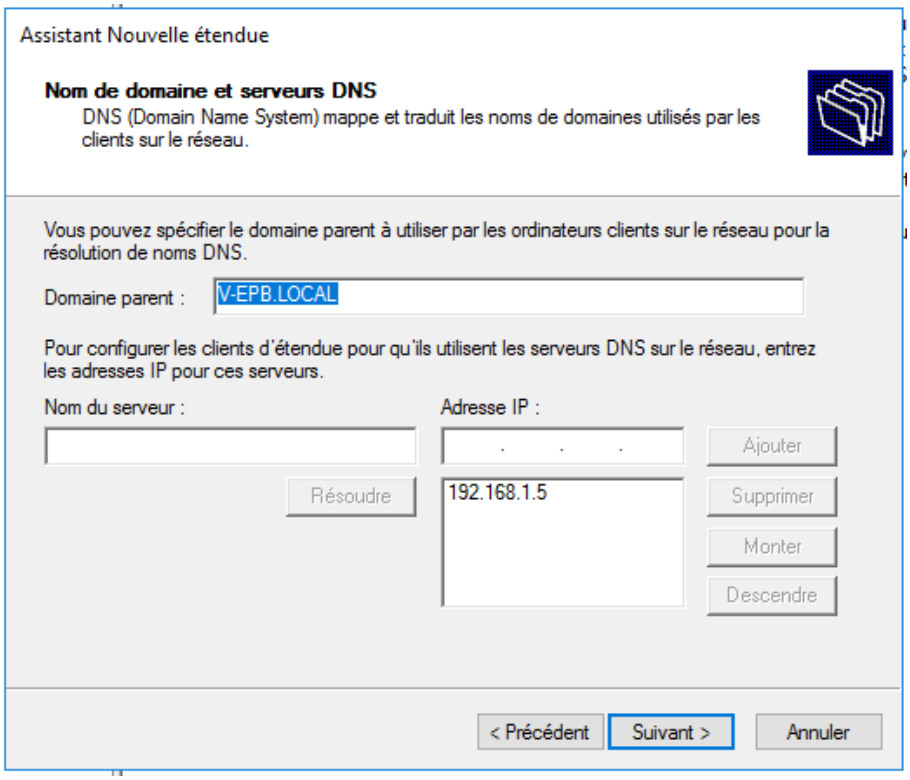


FIGURE 4.11 – Nom de domaine et serveur DNS

L'exécution du nouvel assistant d'étendue indique que nous avons terminé avec succès la création d'une nouvelle portée.

La portée est créée et activée comme le montre la **Figure 4.12**.

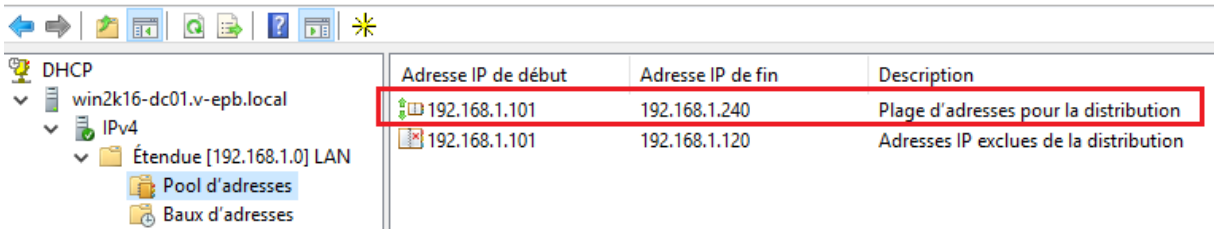


FIGURE 4.12 – Aperçu de l'étendue DHCP

4.7 Installation du rôle RDS01

Nous allons passer à l'installation du rôle RDS sur le serveur RDS01. Depuis le server manager et sur l'ajout de rôles et de fonctionnalités, on clique sur suivant et on choisit "installation des services Bureau à distance". (**Figure 4.13**)

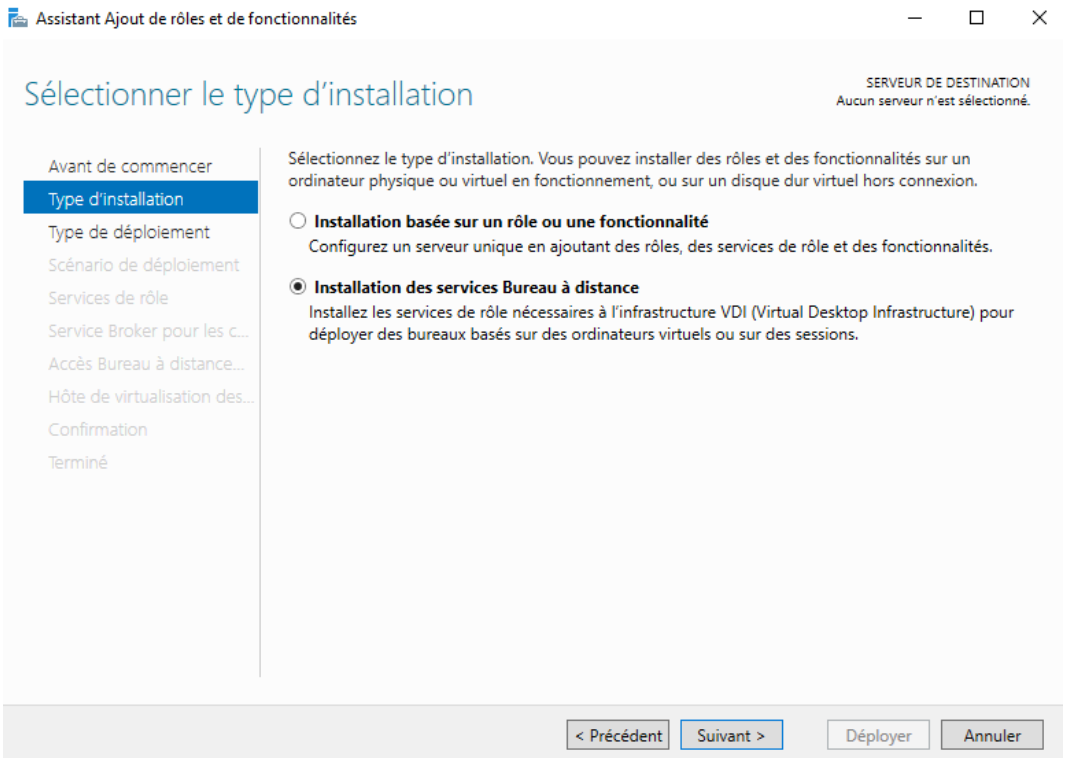


FIGURE 4.13 – Choix du type d'installation

Le rôles RDS peut être déployé via trois modes différents et sous deux scénarios différents :

Déploiement standard : déploiement des Services de rôles RDS sur plusieurs serveurs.

Déploiement rapide : déploiement des Services de rôles RDS sur un seul et même serveur.

Multipoint Services : il s'agit d'un nouveau rôle, désormais natif dans Windows Server 2016. Il a pour but de permettre à des postes clients économiques et à des clients légers de se connecter à un serveur via USB ou via Ethernet pour proposer à plusieurs utilisateurs des sessions individualisées sur un même serveur. L'idée est de fournir un bureau Windows 10 à de multiples utilisateurs sur un seul et même serveur Windows.

Étant donné que nous avons sélectionné le démarrage rapide (**Figure 4.14**), la collection et les programmes RemoteApp seront configurées automatiquement et les rôles Connection Broker, Web Access et Hôte de session seront installés sur le serveur unique.

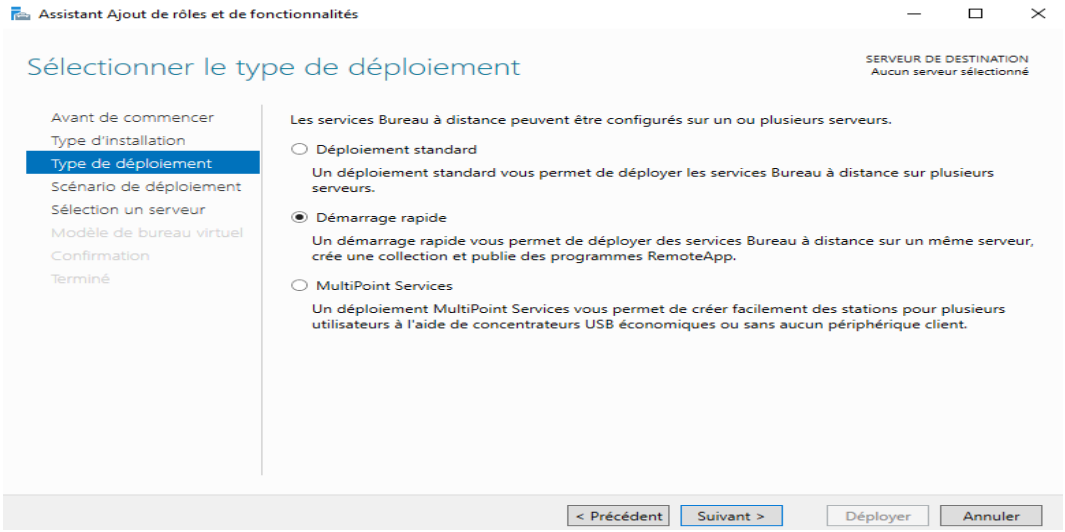


FIGURE 4.14 – Choix du type de déploiement

Les scénarios existants sont :

Déploiement sur une session : Présentation de Bureau Windows & Publication d'applications.

Déploiement basé sur une machine virtuelle : VDI (Virtual Desktop Infrastructure). On sélectionne le déploiement de bureaux sur une session (**Figure 4.15**).

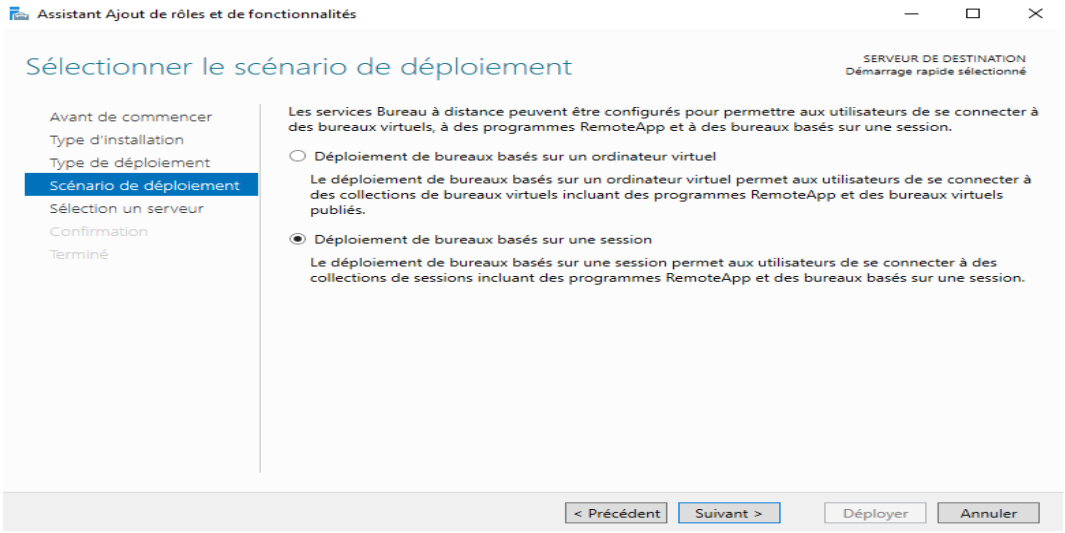


FIGURE 4.15 – Choix du scénario de déploiement

Dans la zone "Sélectionner un serveur", on vérifie notre serveur RDS et l'adresse IP (dans notre cas, notre serveur RDS est Win2K16-RDS01 / 192.168.1.122).

À la fin de l'installation et après le redémarrage du système, Nous pouvons accéder aux services bureau à distance via le gestionnaire de serveur si nous cliquons sur le lien service bureau à distance dans le volet de gauche (**Figure 4.16**).

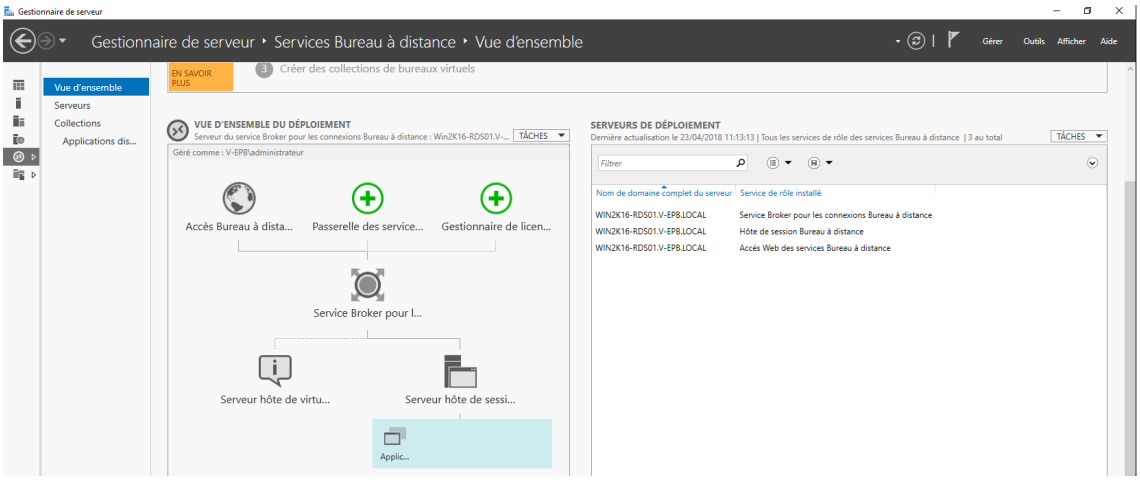


FIGURE 4.16 – Interface RDS

Les collections séparent les hôtes de sessions RD dans des batteries distinctes et permettent aux administrateurs d'organiser les ressources (**Figure 4.17**).

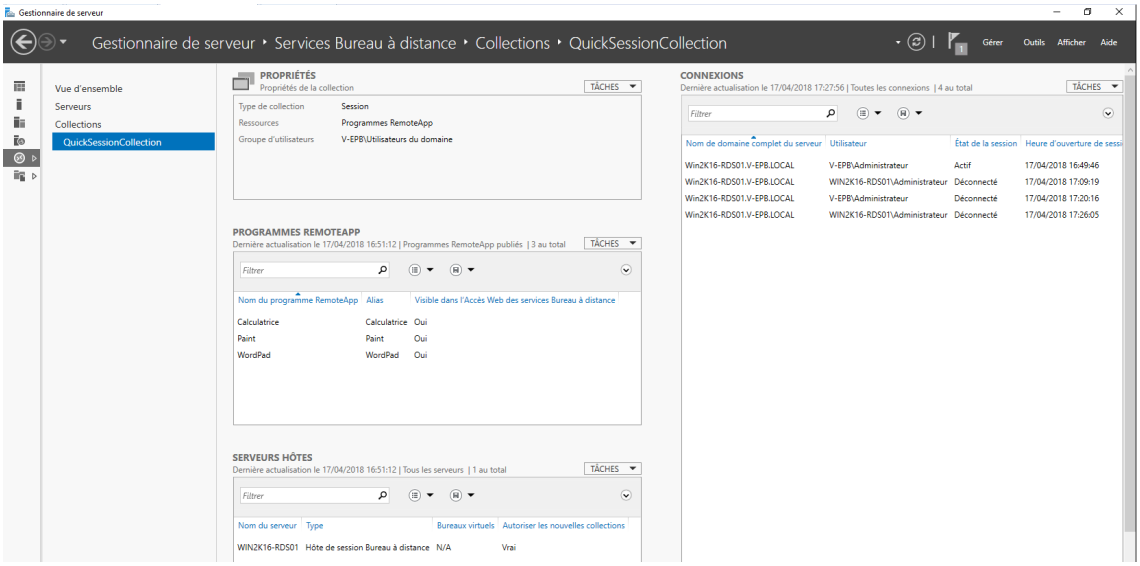


FIGURE 4.17 – Interface de la collection par défaut

- Création d'une collection de sessions

Maintenant que les services de bureau à distance sont installés, nous allons passer à la création de notre collection de sessions pour permettre aux utilisateurs d'un groupe d'accéder aux applications.

Toujours dans l'onglet "Collection", on clique sur le bouton tâches puis sur "Créer une collection de sessions". Nous avons donner un nom à notre collection (**Figure 4.18**).

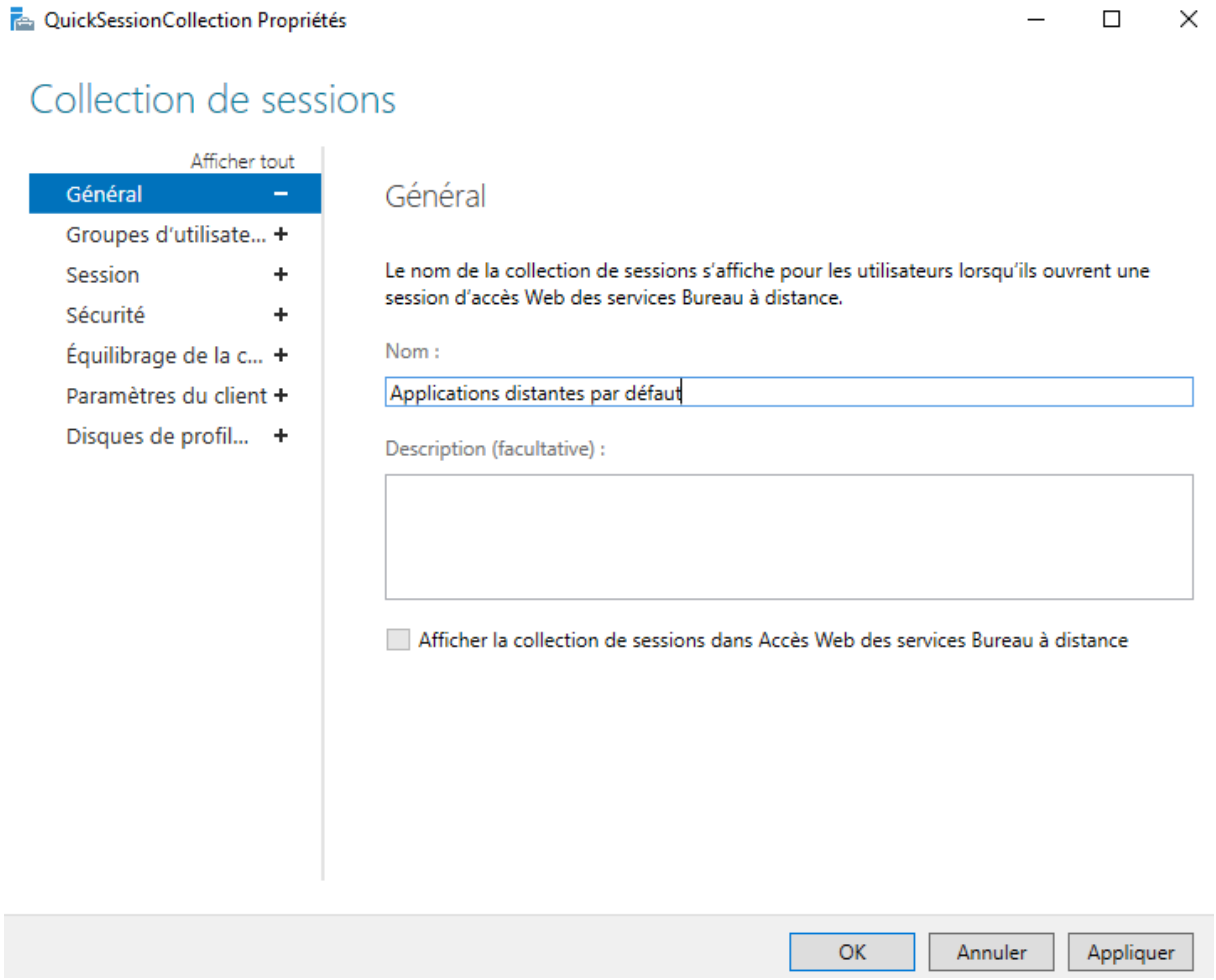


FIGURE 4.18 – Création d'une collection de session

Ensuite, nous avons sélectionner notre serveur et le groupe d'utilisateur autorisé à accéder à la collection (que nous avons créer sur notre serveur AD). Notre collection est à présent créée.

Nous allons maintenant ajouter des applications à notre collection, toujours dans le Gestionnaire de serveur (Server Manager). On clique sur la collection crée. Puis au niveau du panneau "Programmes RemoteApp", on clique sur "Publier des programmes RemoteApp".

L'assistant va automatiquement rechercher toutes les applications disponibles sur les serveurs "Session Host" concernés et la liste apparaît. On sélectionne le ou les programmes à publier (**Figure 4.19**).

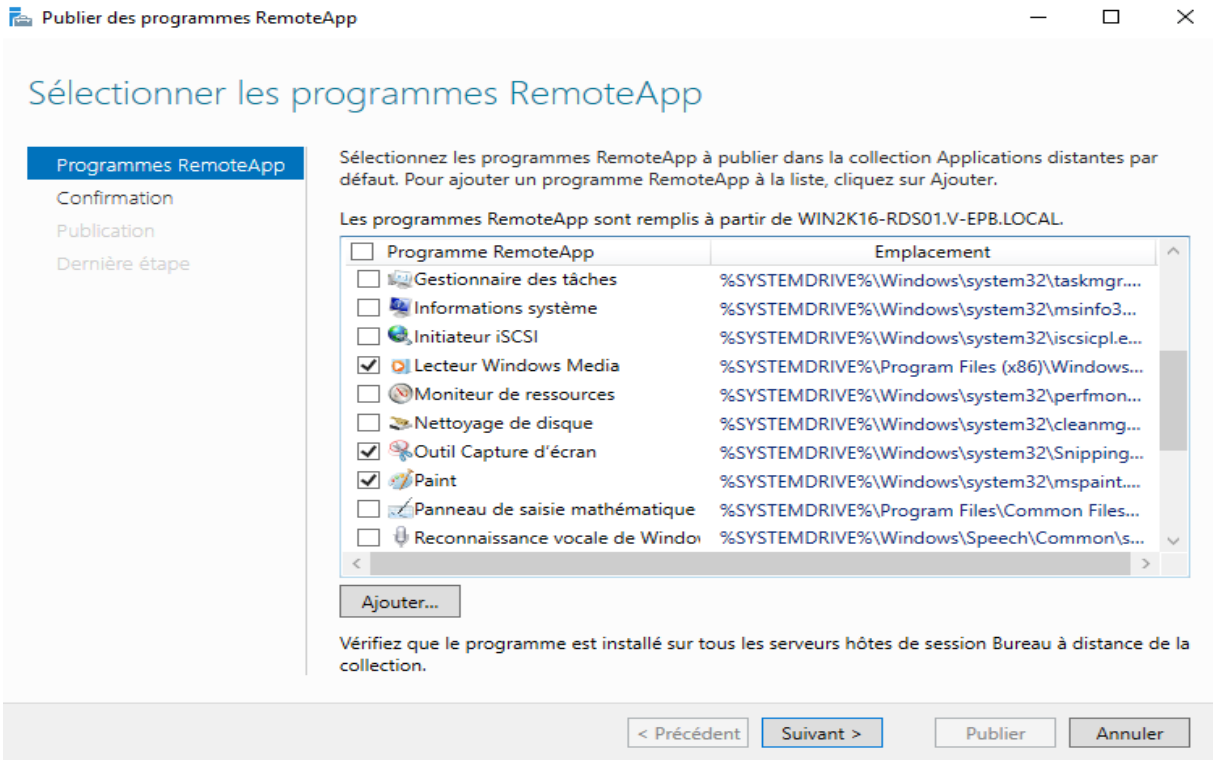


FIGURE 4.19 – Choix des applications à publier

Une fois la publication terminée, on clique sur fermer.

4.7.1 Différents accès au serveur

- **Accès via le web**

Pour vérifier que nous accédons bien à nos RemoteApp, nous allons utilisé une machine cliente.

On démarre le navigateur internet et on tape le lien serveur complet, dans notre cas https ://Win2K16-RDS01.V-EPB.LOCAL/RDWEB (à adapter en fonction de notre domaine AD et du nom de notre serveur qui héberge le rôle RD Web Access).

La fenêtre suivante s'ouvre (**Figure 4.20**), saisir un nom d'utilisateur et un mot de passe autorisés à se connecter aux services Bureau à distance, puis cliquer sur s'inscrire.

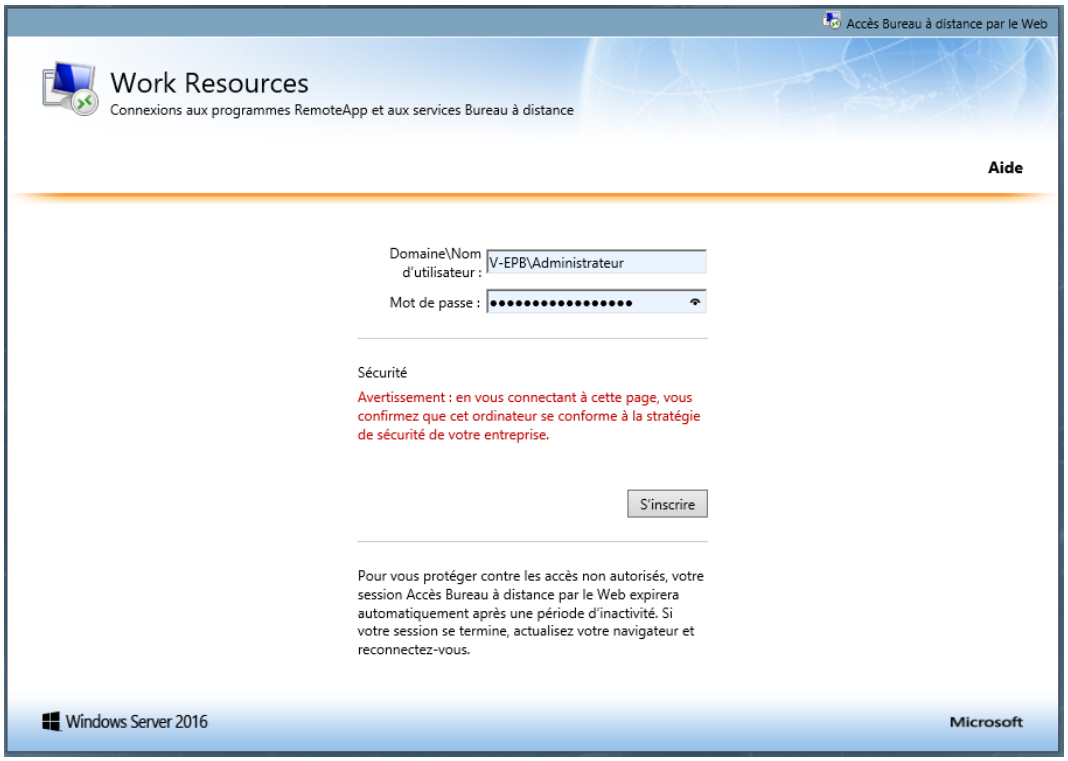


FIGURE 4.20 – Accès via web : Authentification

Enfin, nos applications RemoteApp sur la page RDWEB (**Figure 4.21**).

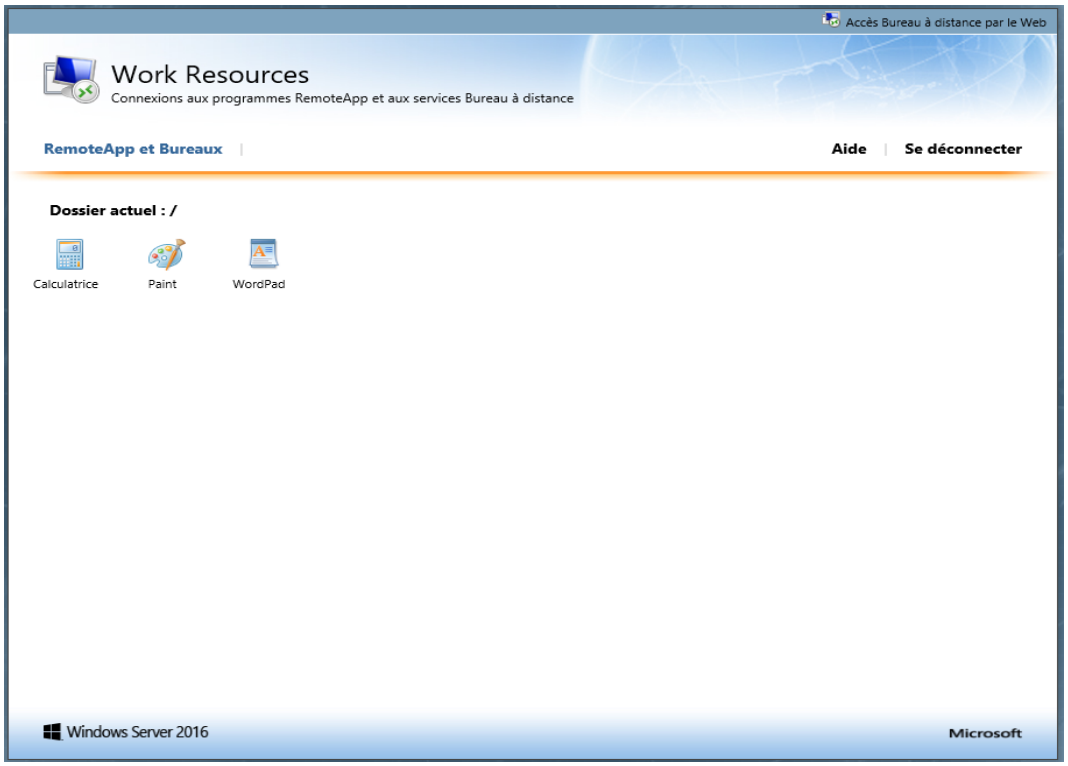


FIGURE 4.21 – Accès via web : Applications publiées

- **Accès via le bureau à distance**

Pour accéder au programme RemoteApp via un accès à distance, nous allons utiliser le Bureau à distance de Windows. Il suffit d'aller sur le bureau du système, ouvrir le menu Démarrer, dans le sous-menu Accessoires, choisir "Connexion Bureau à distance" (**Figure 4.22**).

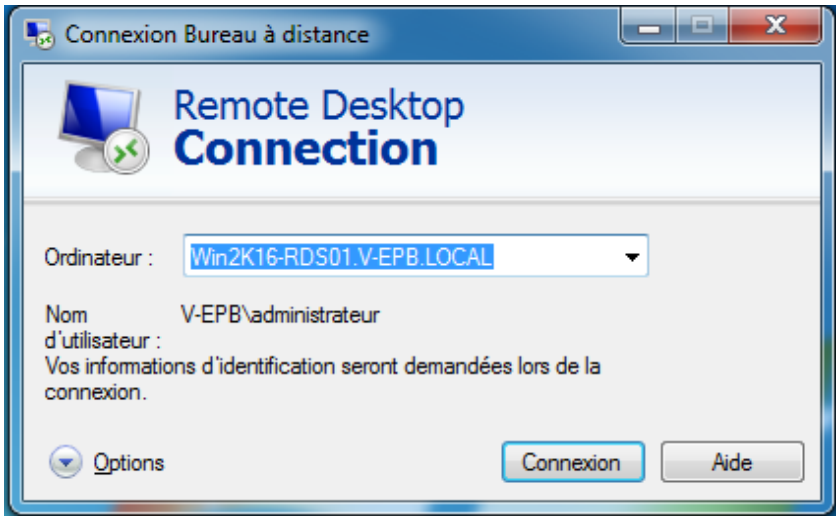


FIGURE 4.22 – Connexion au bureau à distance

4.8 Installation du RDS02

Pour l'installation du RD02 et sa configuration, nous avons suivi les mêmes étapes que celles faites précédemment pour RDS01.

4.9 Mise en place de la solution d'équilibrage de charge

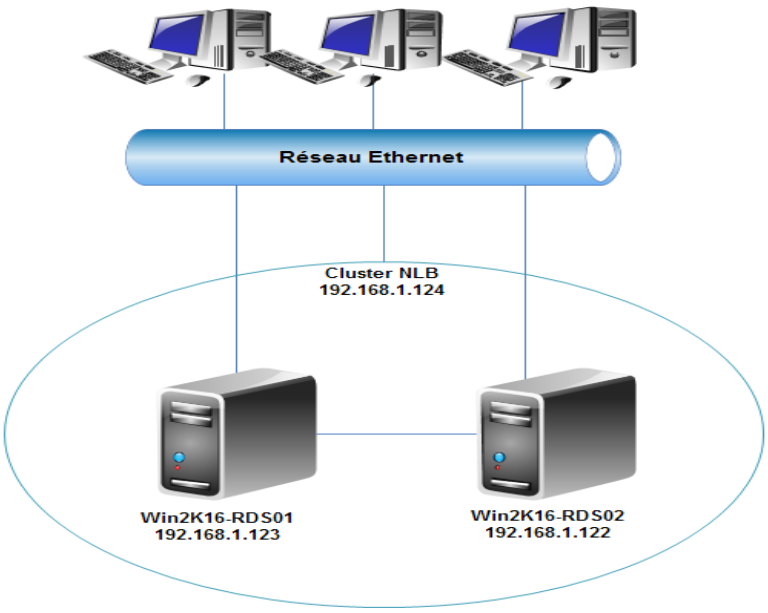


FIGURE 4.23 – Fonctionnement du Cluster NLB

Dans un cluster chaque hôte exécute une copie distincte des applications de serveur souhaitées. NLB (Network Load Balancing) distribue les connexions entrantes entres les hôtes actif du cluster. L'ajout d'hôtes peut se faire de manière dynamique lors d'une charge accru du réseau. De même il est possible de configurer autant de fois que nécessaire le poids de charge que chaque hôte doit traiter.

L'équilibrage de la charge réseau permet d'adresser au cluster une adresse IP globale tout en conservant des adresses IP fixe sur chacun des membres du cluster. Dans notre cas l'adresse IP du cluster est 192.168.1.124. Si on se connecte au server web à cette adresse, la connexion sera dirigée vers l'un des deux membres du cluster.

En cas d'échec sur une application équilibrée, ou de passage hors connexion (serveur éteint pour maintenance ou panne technique), la charge est alors automatiquement redistribuée entre les serveurs toujours en fonctionnement. Pour éviter d'interrompre les connexions actives, nous utiliserons la commande drainstop, ce qui permet à l'hôte de continuer à gérer les connexions actives, mais désactive tout nouveau trafic vers cet hôte.

En permanence des heartbeats (pulsations) sont envoyés entre les serveurs du cluster, si aucun heartbeat ne parvient pendant 5 secondes, le serveur en question est considéré comme en échec.

4.9.1 Installation de Network Load Balancing

Avant d'installer la fonctionnalité d'équilibrage de la charge réseau, il est nécessaire de respecter quelques points indispensables au niveau logiciels :

-L'adresse IP des serveurs doivent être fixes.

-Les serveurs doivent tous utiliser DNS.

-Les serveurs doivent être dans le même AD.

-Les serveurs doivent tous être membres du domaine.

Nous allons installer la fonctionnalité NLB depuis la console Windows PowerShell (**Figure 4.24**), pour se faire il faut introduire la commande suivante :

Invoke-Command -Computername nomduserveur -command Install-WindowsFeature NLB,RSAT-NLB

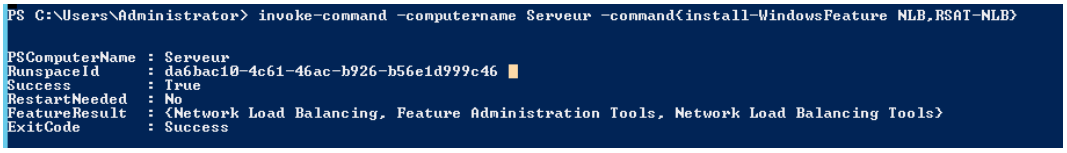


FIGURE 4.24 – Console Windows PowerShell

Une fois le processus terminé, ouvrir le "Gestionnaire de serveur", cliquer sur "Outils" et vérifier que le gestionnaire d'équilibrage de la charge réseau est installé (**Figure 4.25**).

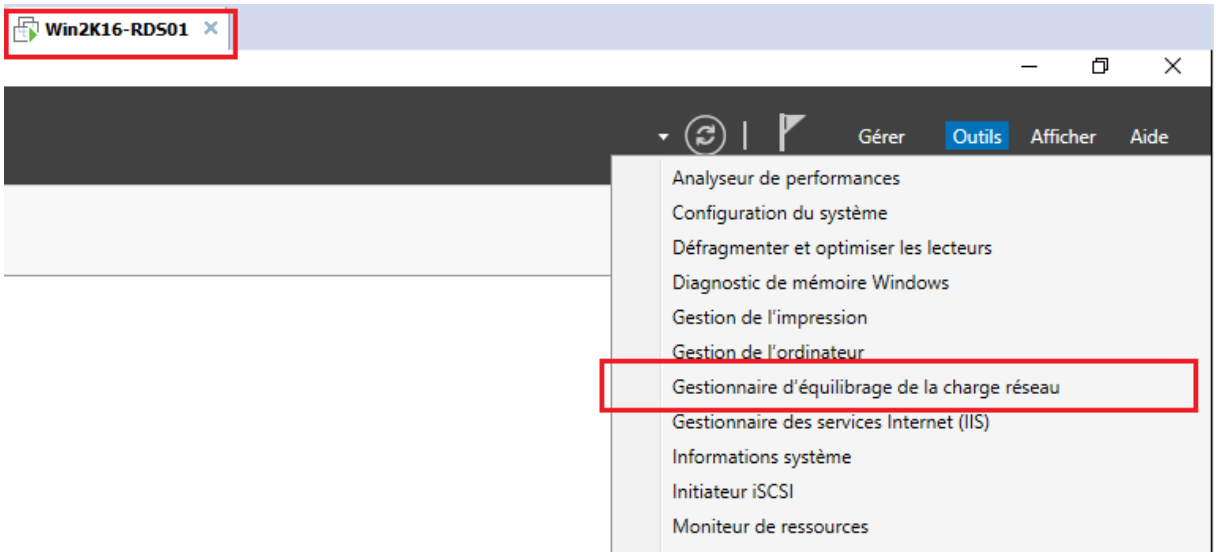


FIGURE 4.25 – Vérification de l'installation 1

La même vérification pour RDS02 (**Figure 4.26**).

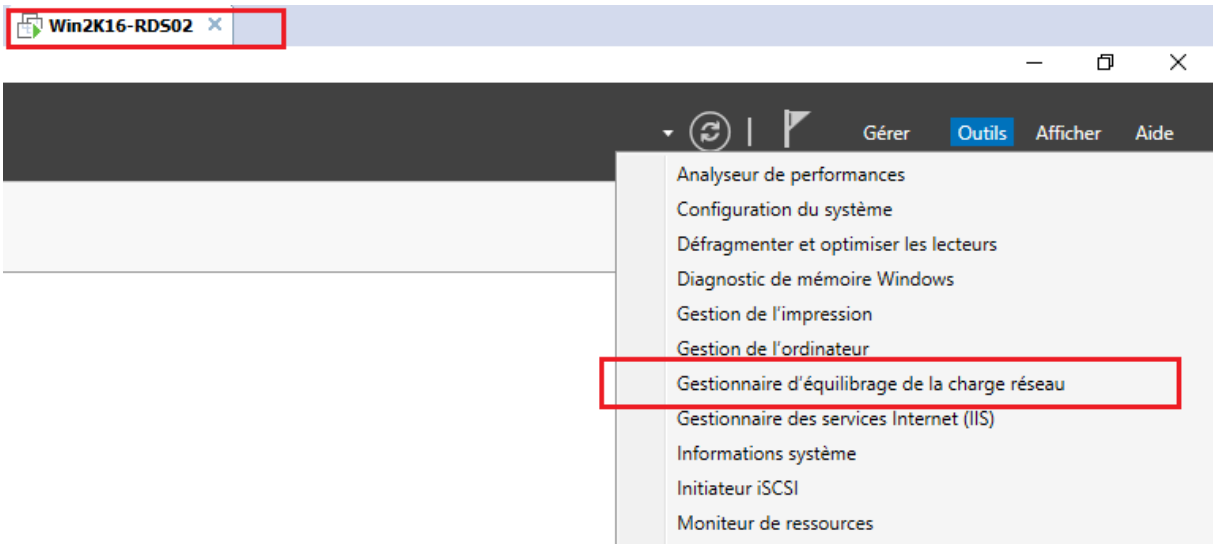


FIGURE 4.26 – Vérification de l'installation 2

4.9.2 Création et configuration du Cluster

Pour créer et configurer notre Cluster, nous allons suivre les étapes suivantes :

A partir du gestionnaire de serveur dans l'onglet outils on ouvre le gestionnaire d'équilibrage de la charge réseau.

Dans la fenêtre qui s'affiche, faire un clic droit puis "Nouveau cluster" sur l'onglet Clusters d'équilibrage de la charge réseau (**Figure 4.27**).

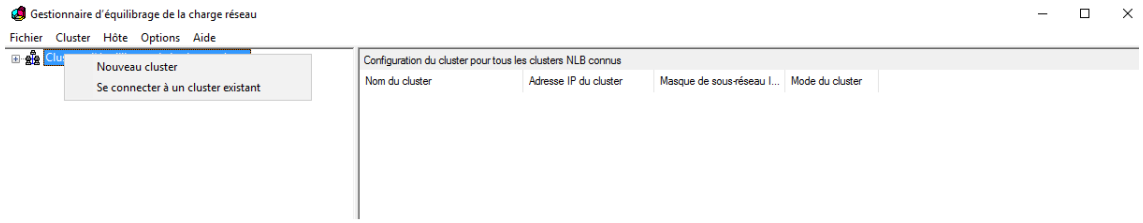


FIGURE 4.27 – Création du Cluster

On va dans un premier temps choisir un nœud à ajouter au cluster, dans notre cas "RDS01" avec son adresse IP qui sera 192.168.1.123. Si le nœud en question est trouvé, toutes ses connexions réseaux sont affichées en dessous (**Figure 4.28**).

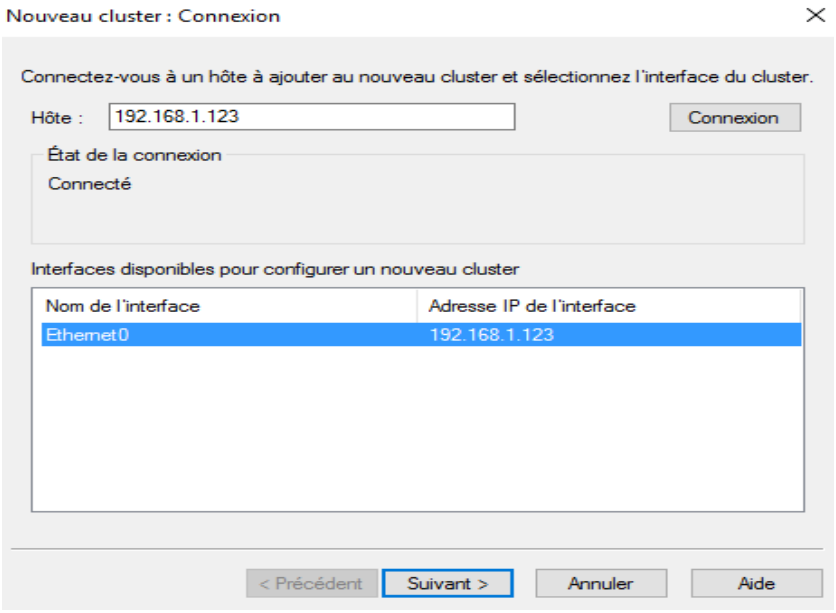


FIGURE 4.28 – Ajout du premier nœud

Par la suite, il va falloir définir la priorité du nœud sur le cluster. Cette priorité est basée sur le plus petit nombre. Nous laisserons la priorité à 1 dans notre cas ainsi que l'état démarré par défaut (**Figure 4.29**).

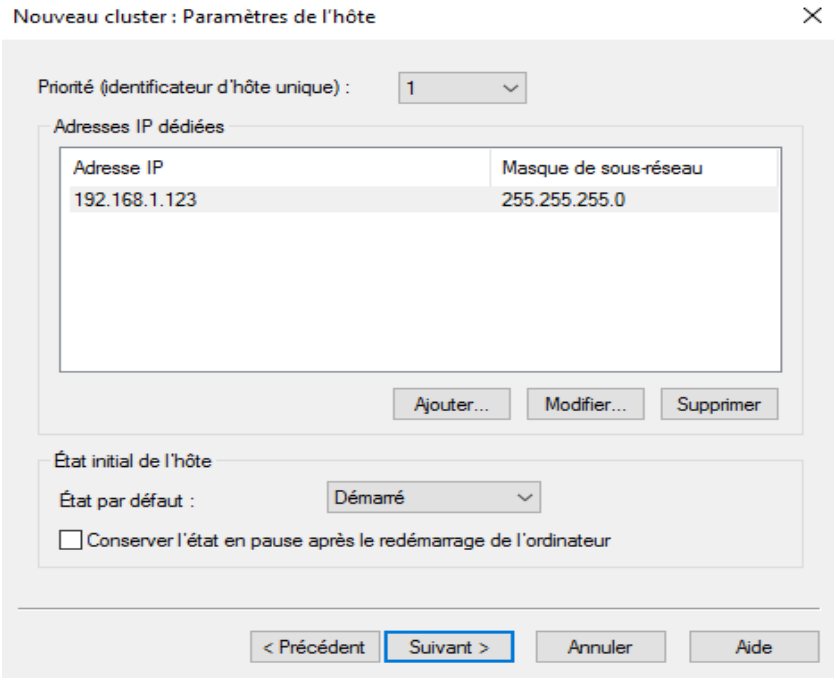


FIGURE 4.29 – Configuration de la priorité de l'hôte

Dans le champ suivant, on va ajouter l'adresse IP qu'on va dédier pour notre cluster ainsi que le masque. Cette adresse est aléatoire (**Figure 4.30**).

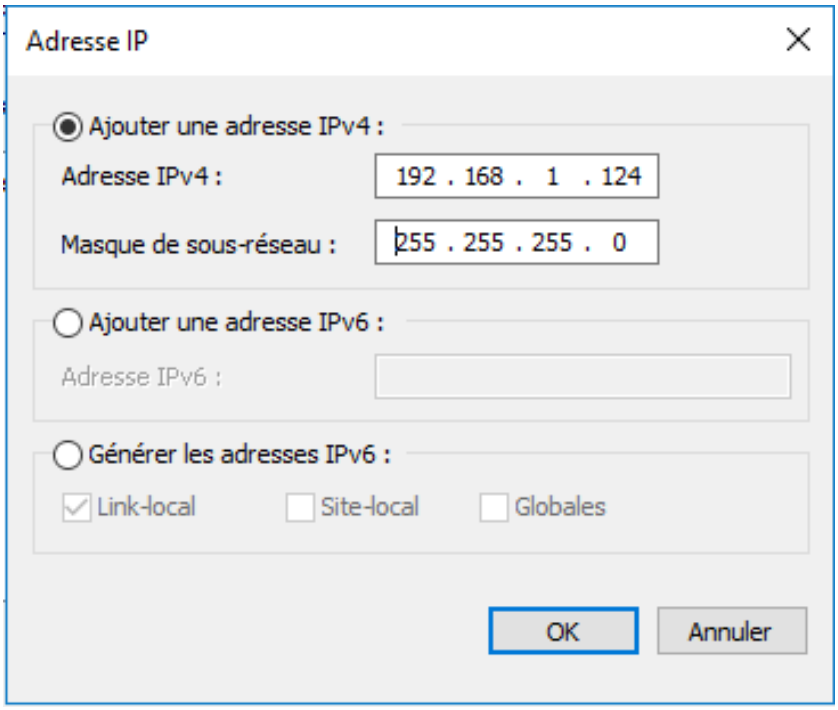


FIGURE 4.30 – Paramétrage de l'adresse IP du cluster

Chaque fois qu'un client se connecte à l'adresse IP du cluster qui est une adresse IP virtuelle, cette dernière redirigera le client vers le serveur approprié.

Après avoir définit les paramètres réseaux du cluster, nous allons lui donner un "Nom Internet Complet" et un mode d'opération.

Le paramètre "Nom Internet complet" indique un nom global au cluster NLB, Dans notre cas "Cluster". Ce nom est utilisé pour accéder au cluster dans son ensemble.

Monodiffusion : assigne la même adresse mac sur tous les nœuds du cluster, cela va à l'encontre des switches, qui mémorisent l'adresse mac par port, et pour lesquels avoir deux fois la même adresse mac n'est pas possible.

Multidiffusion : règle le problème de l'adresse mac en ajoutant une adresse mac de type multi-diffusion et en empêchant les équipements réseaux de mémoriser l'adresse mac du cluster.

Multidiffusion IGMP(Internet Group Management) : ce mode se comporte comme le précédent, mais les nœuds s'enregistrent également sur une adresse IP IGMP de classe D. Cela impose que les équipements réseaux supportent la multidiffusion IGMP. Chaque nœud a sa propre adresse mac, l'adresse IP de multidiffusion et seulement les nœuds reçoivent le trafic réseau du cluster.

Dans notre cas nous avons décidé de choisir le mode multidiffusion (**Figure 4.31**).

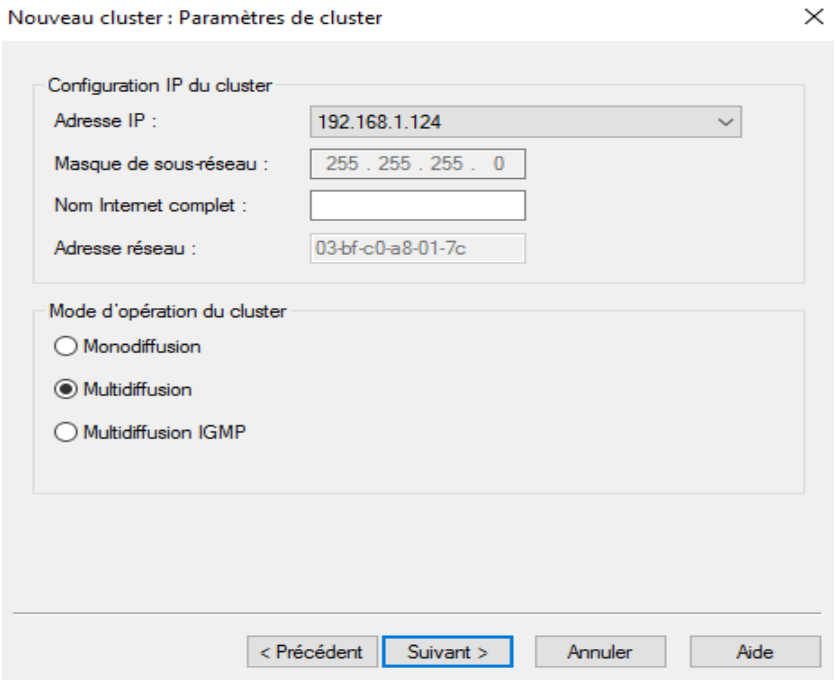


FIGURE 4.31 – Configuration du Cluster

Sur la fenêtre suivante, nous avons la possibilité de définir des règles de port (**Figure 4.32**).

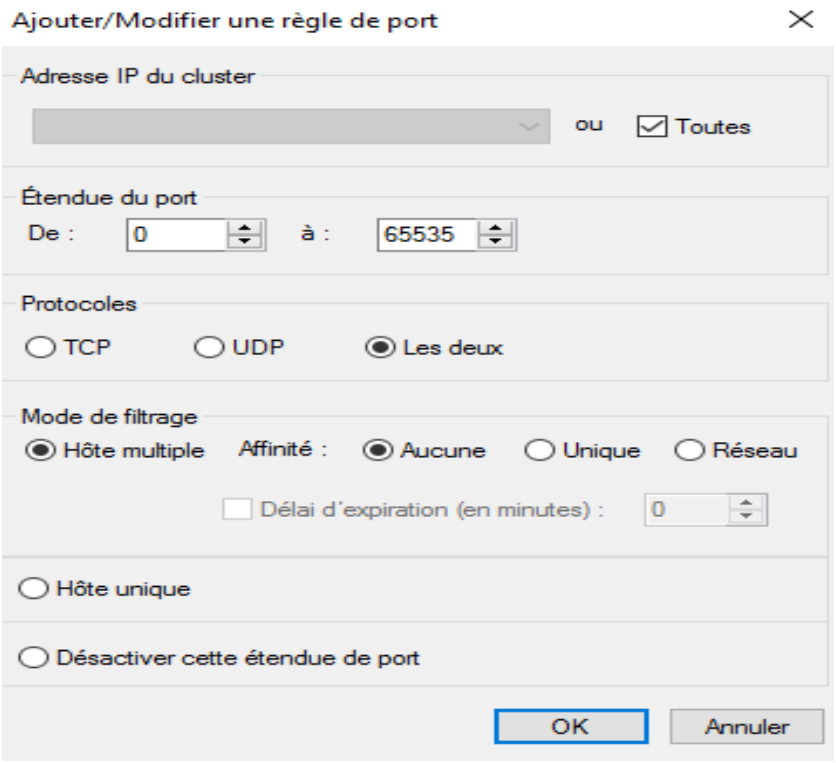


FIGURE 4.32 – Définition des règles de port

Par défaut le cluster utilise les ports de 0 à 65535.

-Le mode "Hôte unique" est de type actif/passif, avec le nœud qui a le plus petit ID en actif.

-Le mode de filtrage "Aucun" permet quant à lui de bloquer le trafic sur certain ports, notamment pour protéger les nœuds.

-En mode hôte multiple, trois choix d'affinité son possibles :

Aucun : à chaque connexion TCP d'un même client, celui-ci sera dirigé vers le nœud ayant le moins de clients. Ce mode assure la meilleure répartition possible, surtout lorsqu'il n'y a pas de spécificité cliente à maintenir (panier, session...)

Unique : permet de maintenir un client (son adresse IP) sur le même nœud tant que la topologie de la ferme n'est pas modifiée (ajout/suppression de nœud). Chaque client doit avoir une adresse IP unique afin d'avoir une répartition efficace (pas de Nat, proxy...)

Réseau : se comporte comme le filtrage précédent, mais au lieu d'utiliser directement l'adresse IP du client, il calcule l'adresse du réseau. Ce filtrage est pertinent lorsqu'il faut maintenir un ensemble de client venant d'un même réseau sur un même nœud.

Si l'état est sur "convergé" cela signifie que le premier nœud de notre cluster est opérationnel, pour ajouter un deuxième nœud, il suffit de faire un clic droit sur le nom du cluster puis de sélectionner "Ajouter l'hôte au cluster" (**Figure 4.33**).

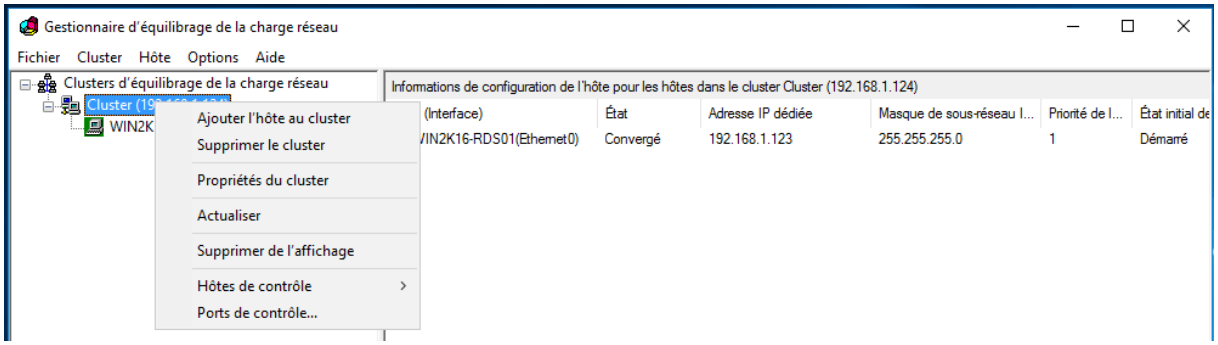


FIGURE 4.33 – Ajout du deuxième nœud

Nous allons configurer les paramètres du nœud (notamment la priorité et les adresses IP dédiées) supplémentaire en suivant les mêmes instructions que celles que nous avons utilisées pour configurer l'hôte initial. étant donné que nous ajoutons des nœuds à un cluster déjà configuré, tout les paramètres à l'échelle du cluster restent les mêmes (**Figure 4.34**).

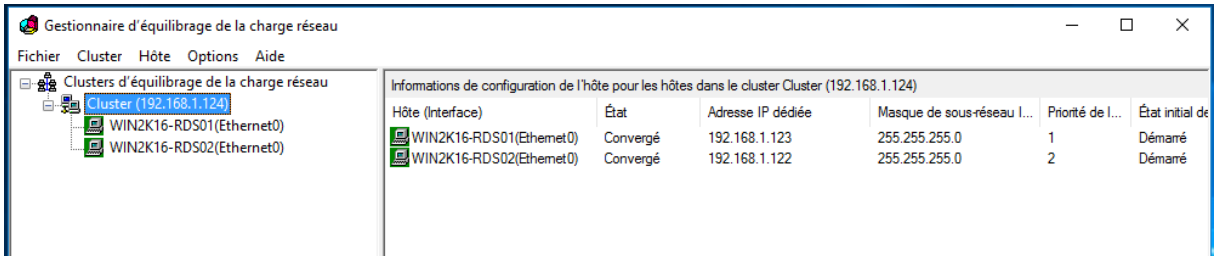


FIGURE 4.34 – Etats des nœuds sur le Cluster

Maintenant que notre cluster est configuré, on passe à notre contrôleur de domaine pour ajouter un enregistrement DNS pour le cluster (**Figure 4.35**).

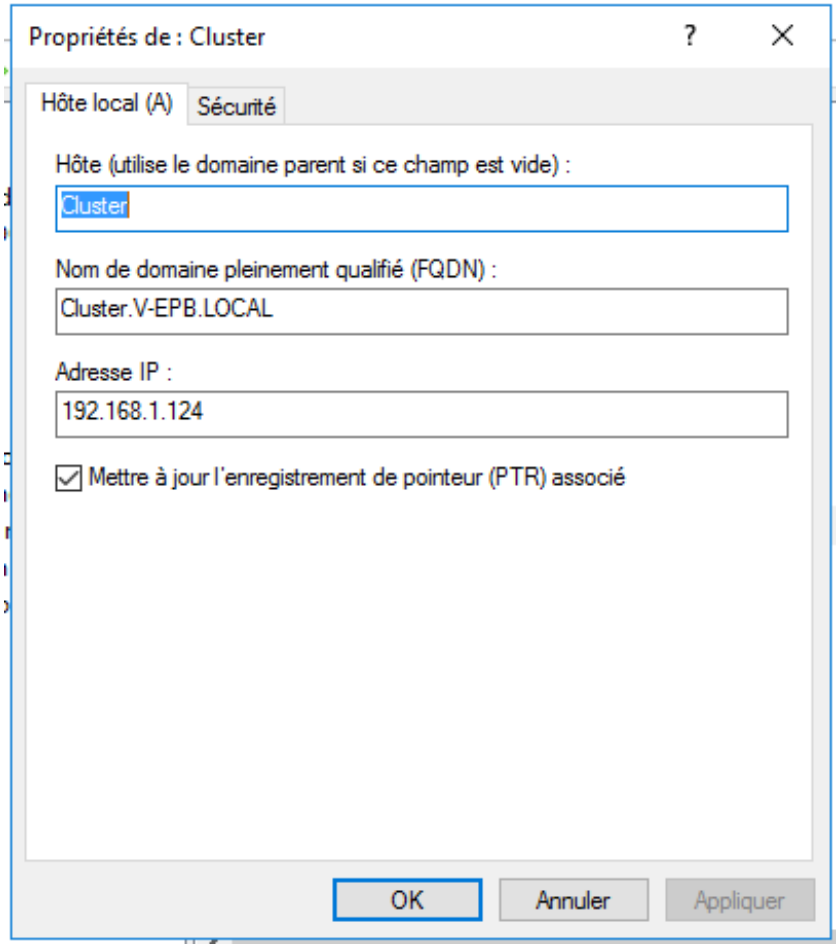


FIGURE 4.35 – Ajout d'un enregistrement DNS pour le Cluster

4.10 Test

4.10.1 Test du fonctionnement NLB

Taper à l'invite de commande nlb dispaly all sur les deux nœuds du cluster. Nous y trouvons le statut de chaque nœud.

RDS01 :

```
C:\Users\Administrateur>nlb display all
NLB Utilitaire de contrôle de cluster V2.6
Cluster 192.168.1.124

=== Configuration : ===

Current time                = 03/06/2018 16:51:49
ParametersVersion           = 6
CurrentVersion              = V2.6
EffectiveVersion            = 00000201
InstallDate                 = 0x5ADE23CE
HostPriority                = 1
ClusterName                 = Cluster
ClusterIPAddress            = 192.168.1.124
ClusterNetworkMask          = 255.255.255.0
DedicatedIPAddresses/       = 192.168.1.123/255.255.255.0
DedicatedNetworkMasks
McastIPAddress              = 0.0.0.0
ClusterNetworkAddress       = 03-bf-c0-a8-01-7c
IPToMACEnable               = ENABLED
MulticastSupportEnable      = ENABLED
```

FIGURE 4.36 – Statut du nœud RDS01

RDS02 :

```
C:\Windows\system32>nlb display all
NLB Utilitaire de contrôle de cluster V2.6
Cluster 192.168.1.124

=== Configuration : ===

Current time                = 03/06/2018 16:53:02
ParametersVersion           = 6
CurrentVersion              = V2.6
EffectiveVersion            = 00000201
InstallDate                 = 0x5ADE2612
HostPriority                = 2
ClusterName                 = Cluster
ClusterIPAddress            = 192.168.1.124
ClusterNetworkMask          = 255.255.255.0
DedicatedIPAddresses/       = 192.168.1.122/255.255.255.0
DedicatedNetworkMasks
McastIPAddress              = 0.0.0.0
ClusterNetworkAddress       = 03-bf-c0-a8-01-7c
IPToMACEnable               = ENABLED
MulticastSupportEnable      = ENABLED
```

FIGURE 4.37 – Statut du nœud RDS02

4.10.2 Test du basculement NLB

Afin de tester le bon fonctionnement de notre solution, nous allons passer à notre machine cliente.

- Via un navigateur web

Entrer l'adresse URL "https ://Cluster/", nous remarquerons que notre premier serveur répond (**Figure 4.38**).

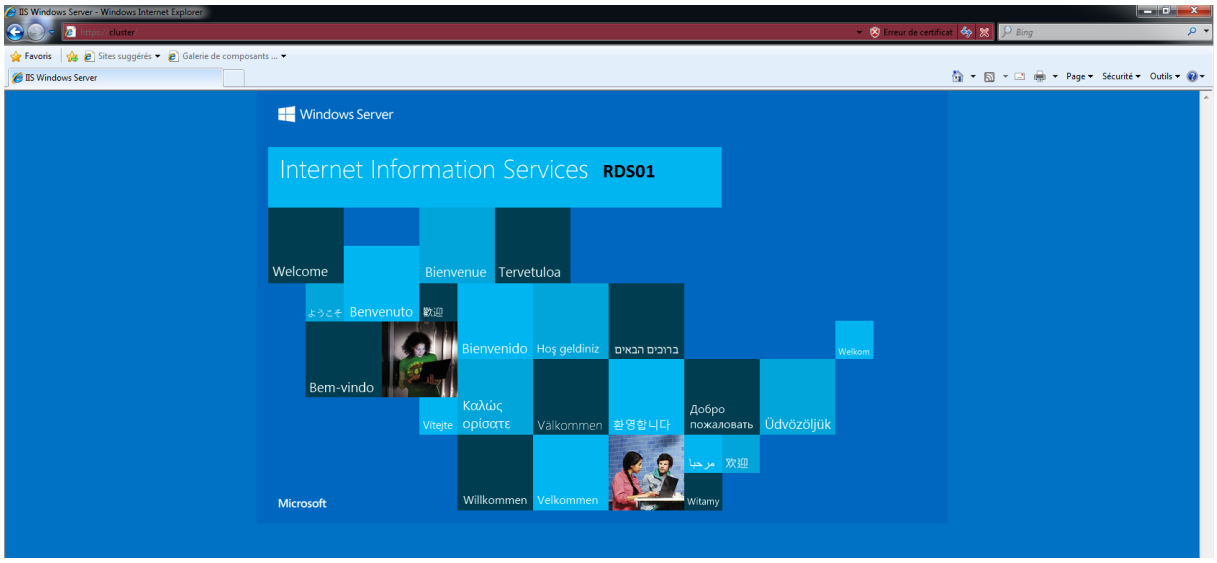


FIGURE 4.38 – Site web IIS du serveur RDS01

A ce moment là, nous arrêtons l'hôte RDS01 (**Figure 4.39**).

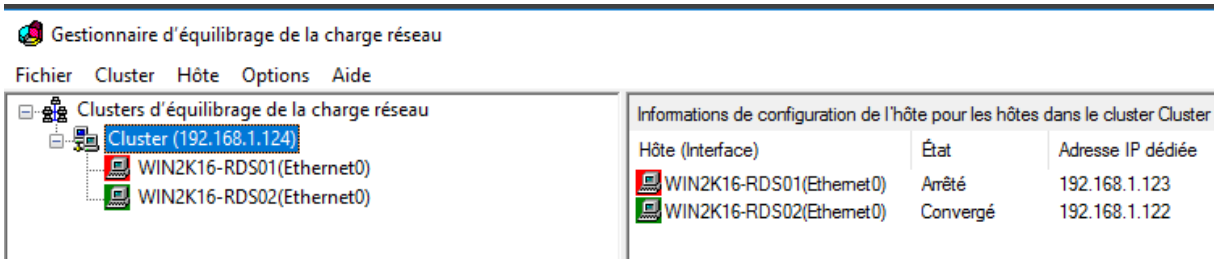


FIGURE 4.39 – Arrêt du serveur RDS01

En actualisant, on voit que notre cluster fonctionne bien car la page par défaut de IIS s'affiche. La requête du client a été dirigée vers le serveur RDS02(**Figure 4.40**).

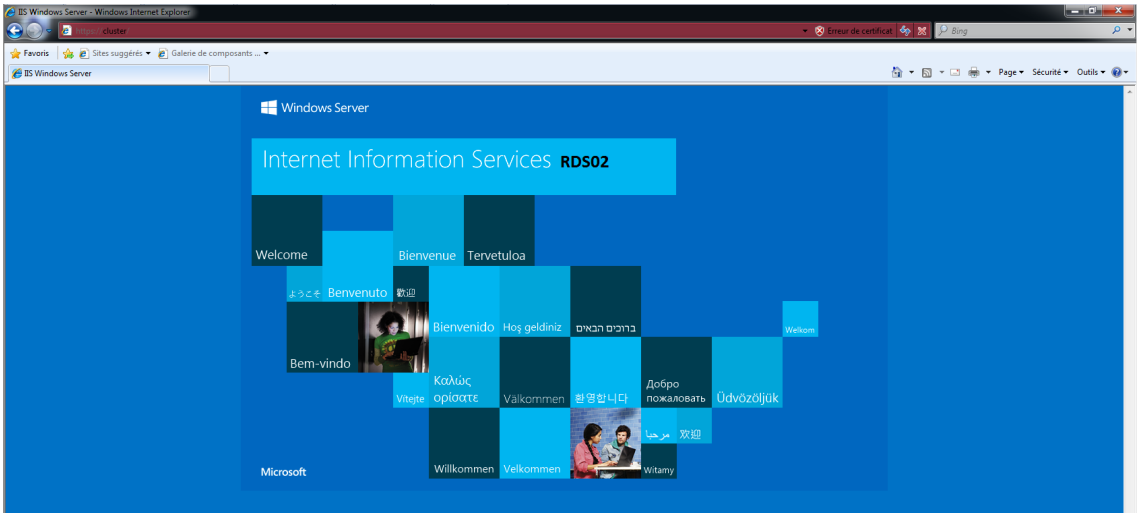


FIGURE 4.40 – Site web IIS du serveur RDS02

- Via l'invite de commande :

Dans ce qui suit nous prendre comme exemple d'application une calculatrice. Nous allons lancer notre programme RemoteApp (**Figure 4.41**).

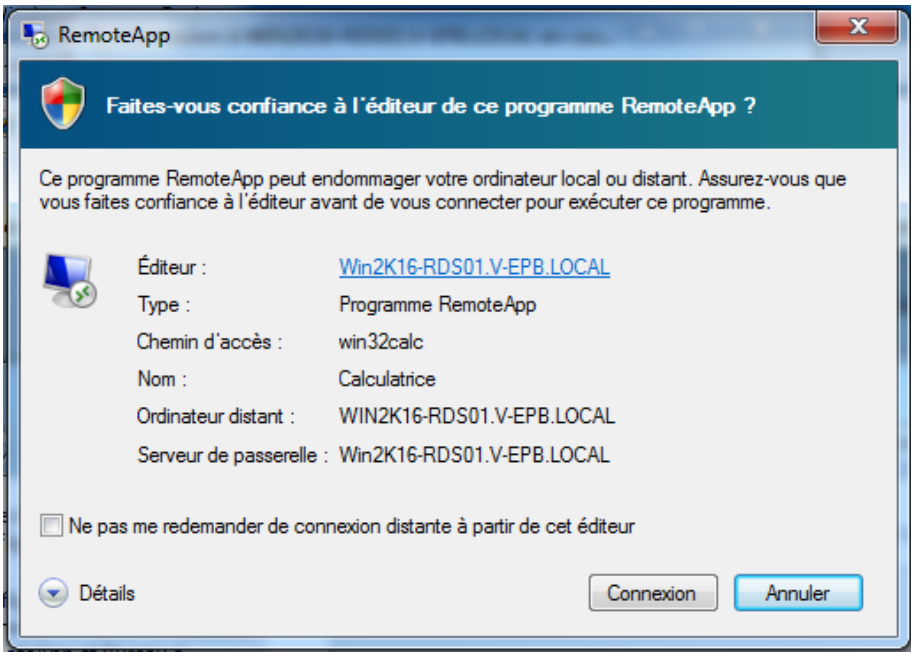


FIGURE 4.41 – Connexion au programme RemoteApp

Ensuite, nous allons introduire nos données d'identification (**Figure 4.42**).

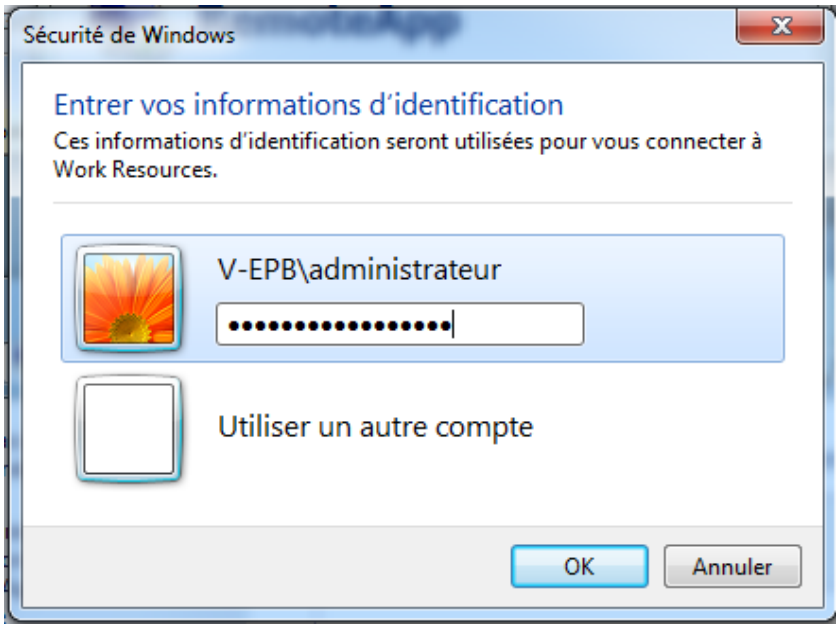


FIGURE 4.42 – Authentification

Lancement du programme RemoteApp (**Figure 4.43**).

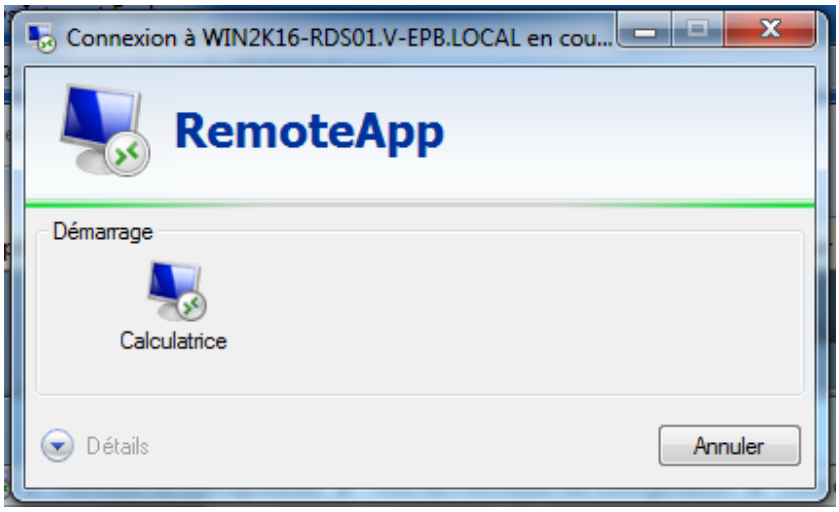


FIGURE 4.43 – Lancement du programme RemoteApp

La calculatrice Remote App est lancée (**Figure 4.44**).

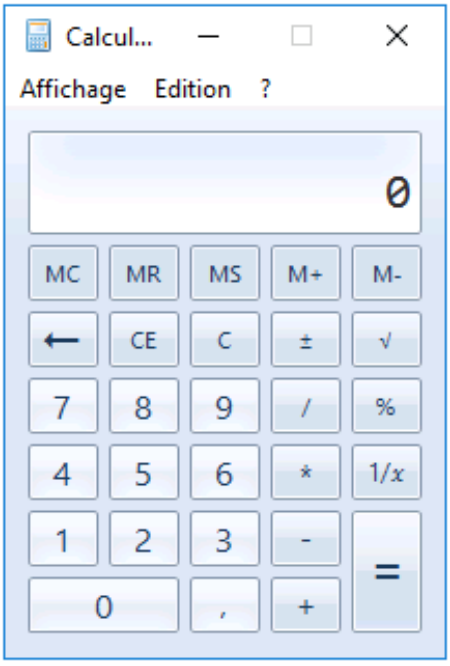


FIGURE 4.44 – Calculatrice RemoteApp

En tapant à l'invite de commande "netstat" sur la machine cliente. Nous y trouvons les connexion TCP en cours qui démontre que le client est connecté sur RDS01 (**Figure 4.45**).

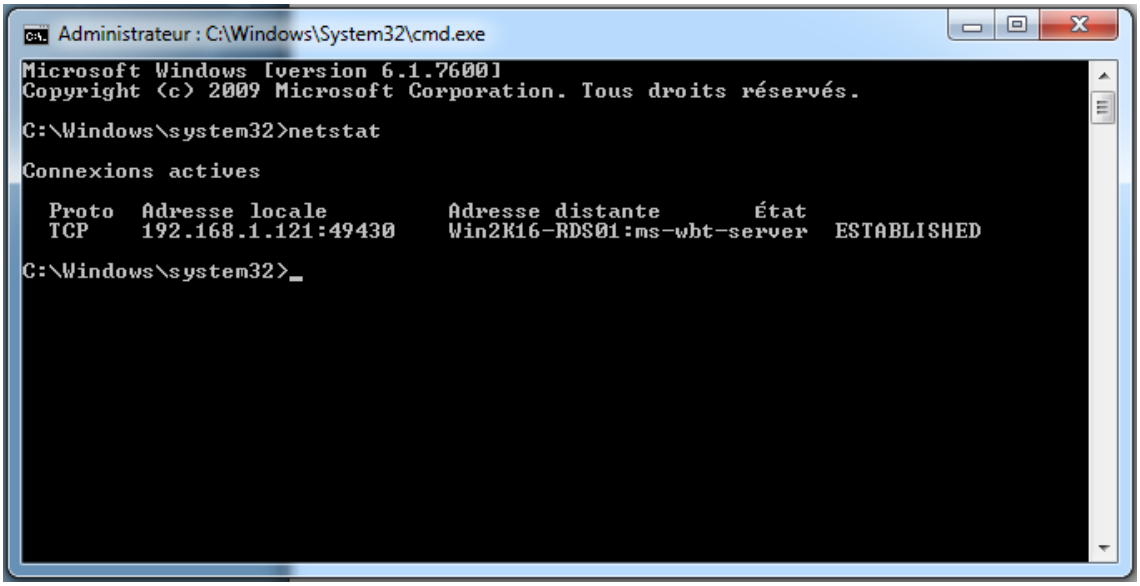


FIGURE 4.45 – Connexion TCP 1

Pour tester le basculement, nous allons arrêter le serveur RDS01 (**Figure 4.46**).

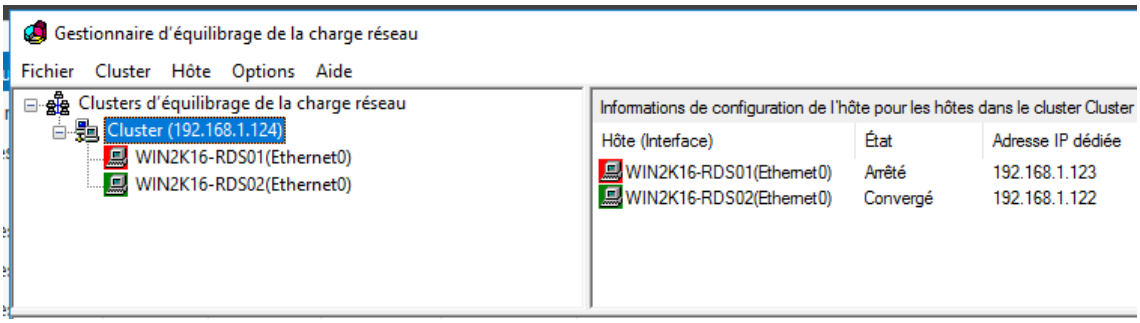


FIGURE 4.46 – Arrêt du serveur RDS01

Ensuite, nous taperons à l'invite de commande "netstat". Nous remarquerons que le basculement vers le serveur RDS02 est réussi (**Figure 4.47**).

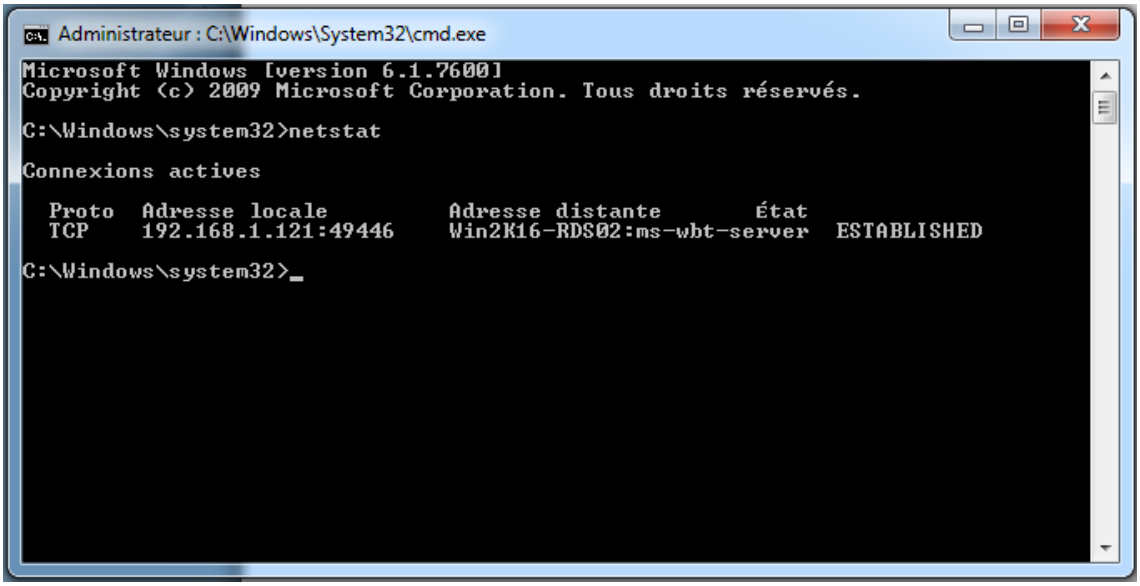


FIGURE 4.47 – Connexion TCP 2

4.11 Simulation avec SimEvents

Afin de simuler notre solution, nous avons choisi comme logiciel SimEvents (Matlab), qui est l'outil de simulation d'événements discrets de la famille de produits mathworks.

SimEvents fournit un moteur de simulation à événements discrets et une bibliothèque de composants pour analyser les modèles de systèmes pilotés par les événements et optimiser les caractéristiques de performance telles que la latence, le débit et la perte de paquets. Les files d'attente, les serveurs, les commutateurs et d'autres blocs prédéfinis nous permettent de modéliser le routage, les délais de traitement et la hiérarchisation pour la planification et la communication.

Avec SimEvents, nous pouvons étudier les effets de la synchronisation des tâches et de l'utilisation des ressources sur les performances des systèmes de contrôle distribués, des architectures logicielles et matérielles et des réseaux de communication. Nous pouvons également effectuer des recherches opérationnelles pour les décisions relatives à la prévision, à la planification de la capacité et à la gestion de la chaîne d'approvisionnement.

Nous allons représenter notre solution de haute disponibilité comme suit :

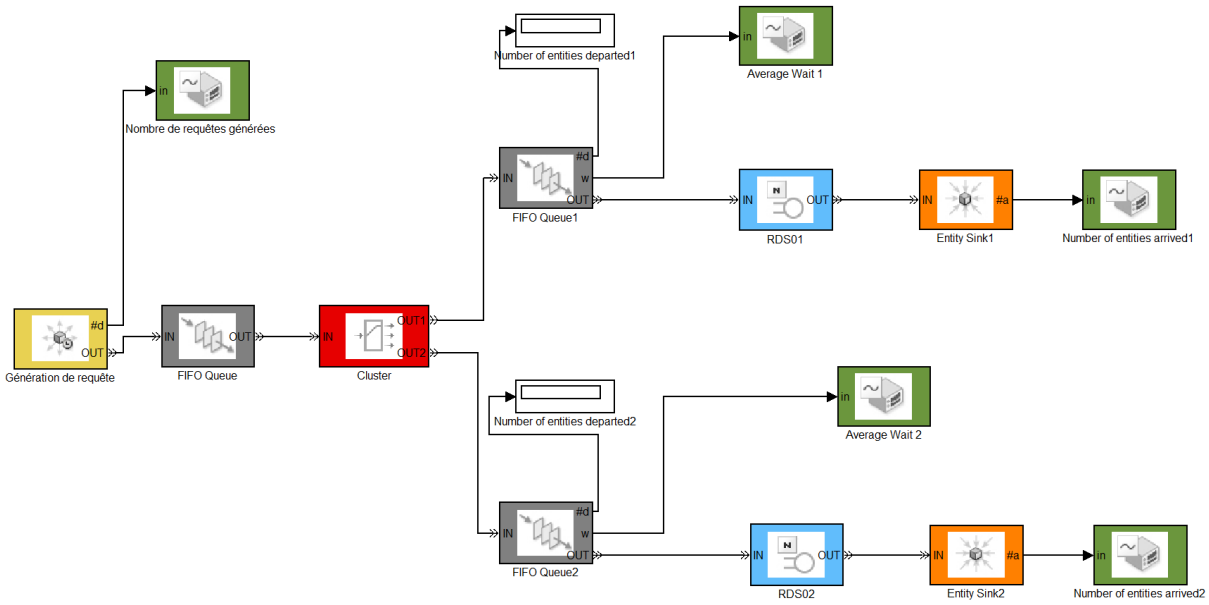


FIGURE 4.48 – Modèle de simulation

Le modèle (illustré dans la **Figure 4.48**) fournit les résultats suivants :

1er cas : Le deuxième port sera choisit seulement si le premier est bloqué (serveur en panne, surchargé..).

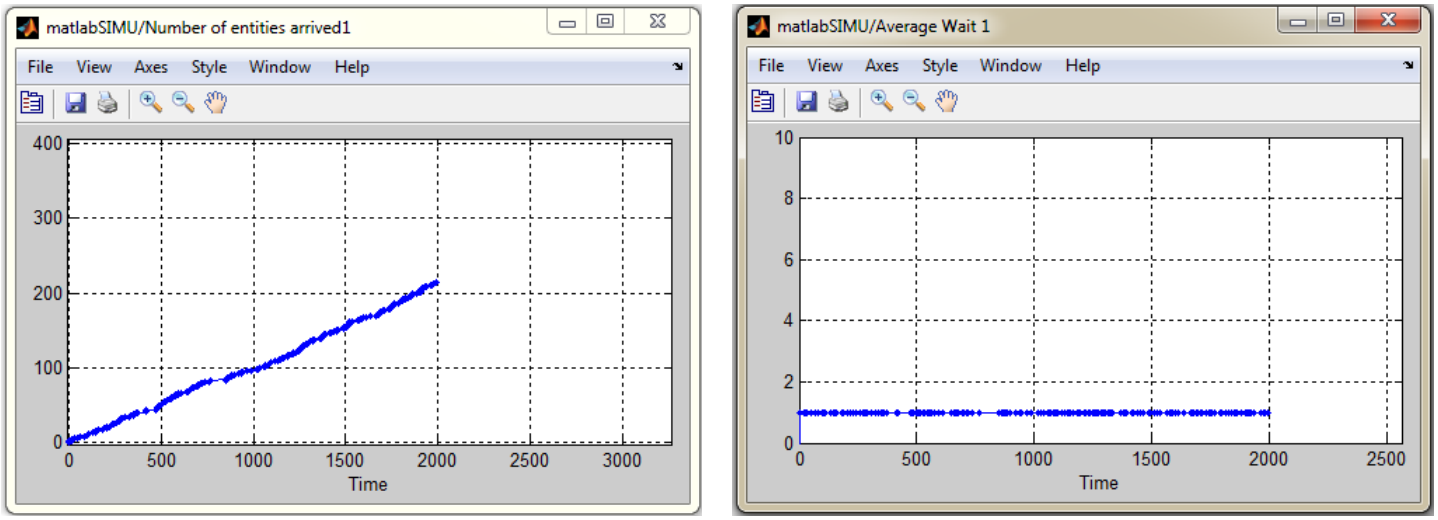


FIGURE 4.49 – Résultats graphique(1er cas) a) Nombre de requêtes reçues (RDS01) b) Temps d'attente moyen(RDS01)

Dans ce premier cas, toutes les requêtes sont passées par la première file. Nous constatons que la courbe (**Figure 4.49**) "a" augmente avec le nombre d'entités générées dans le temps et le temps d'attente moyen est constant à 1.

2e cas : Nous supposerons que la première file est pleine(panne ou surcharge du serveur RDS01). Les résultats sont comme suit :

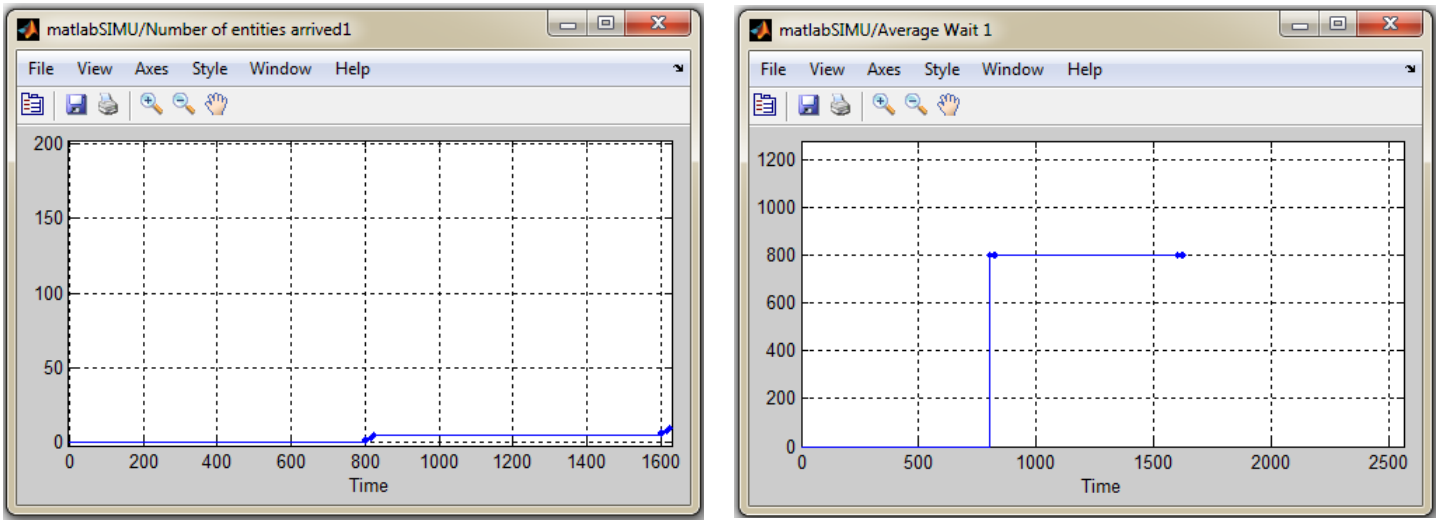


FIGURE 4.50 – Résultats graphique(2e cas) a) Nombre de requêtes reçues (RDS01) b) Temps d'attente moyen(RDS01)

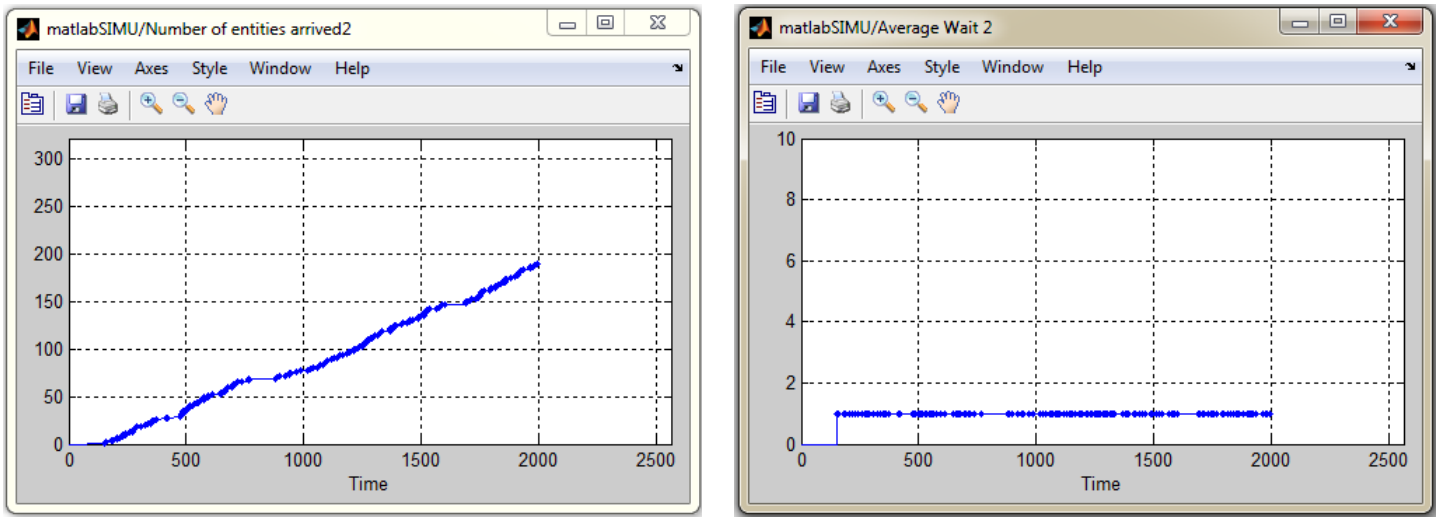


FIGURE 4.51 – Résultats graphique(2e cas) a) Nombre de requêtes reçues (RDS02) b) Temps d'attente moyen(RDS02)

Le serveur RDS01 a reçu quelques requêtes avant de tomber en panne **Figure 4.50** "a", les autres requêtes sont passer par la deuxième file **Figure 4.51** "a". Les temps d'attente moyens pour les requêtes du serveur RDS01 à 800 unités.

3e cas : recevoir le même nombre de requêtes

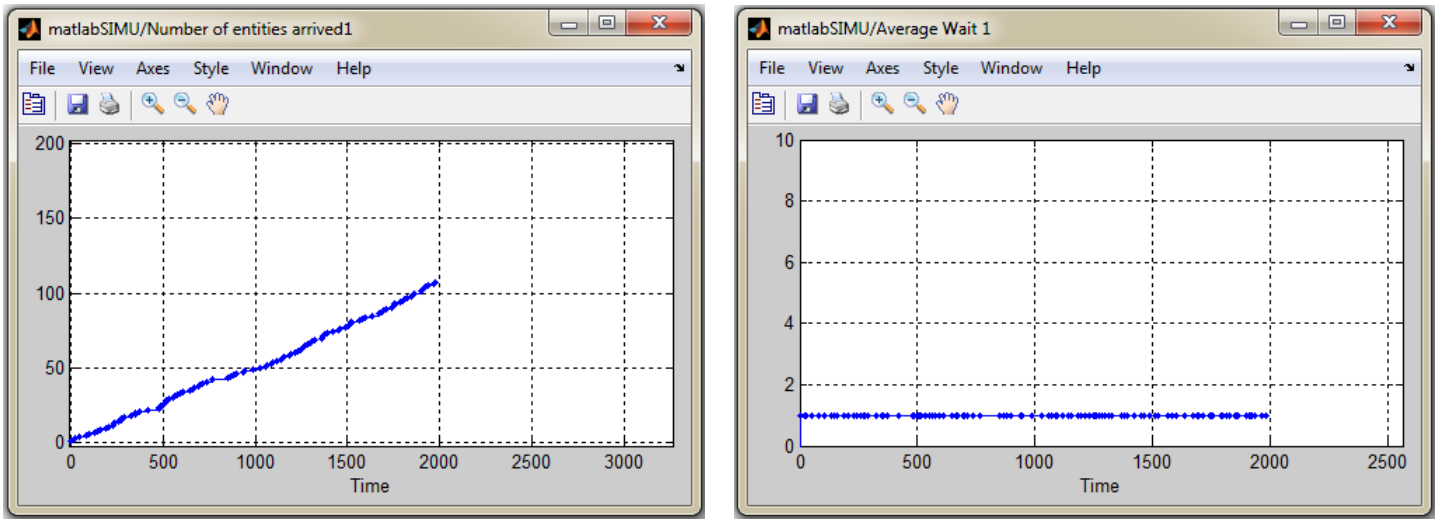


FIGURE 4.52 – Résultats graphique(3e cas) a) Nombre de requêtes reçues (RDS01) b) Temps d'attente moyen(RDS01)

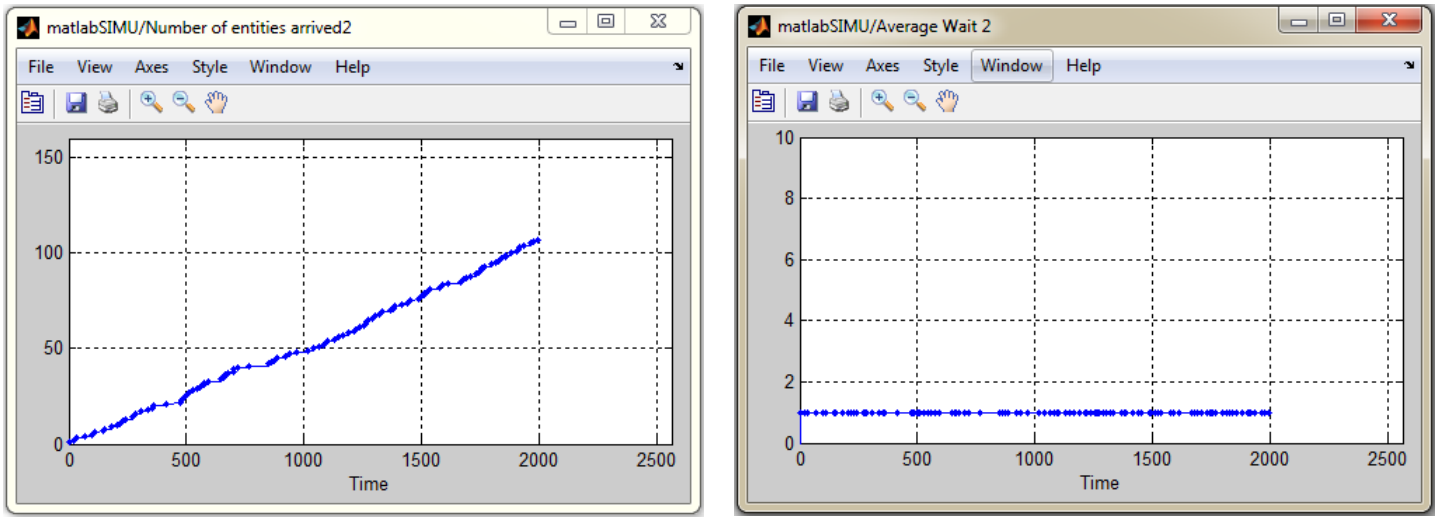


FIGURE 4.53 – Résultats graphique(3e cas) a) Nombre de requêtes reçues (RDS02) b) Temps d'attente moyen(RDS02)

Nous constatons dans la **Figure 4.52** "a" et la **Figure 4.53** "a" que les deux serveurs reçoivent le même nombre de requêtes, La première requête arrivant dans la simulation quitte le port OUT1. A chaque arrivée suivante, le bloc sélectionne le port de sortie de l'entité à côté du dernier port sélectionné. Après avoir épuisé tous les ports de sortie d'entité, le bloc retourne au premier, OUT1. Les temps d'attente moyens sont constants.

La **Figure 4.54** représente la description de chaque blocs utilisés précédemment.

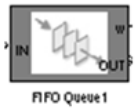
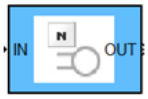
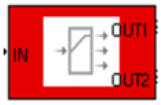
Bloc	Representation	description
Générateur d'entité basé sur le temps		Générer des entités en utilisant des temps d'inter génération à partir d'une distribution de signaux ou de statistiques
FIFO Queue		Stocker les entités en séquence pour une durée indéterminée
Serveur		Servir une entité pour une période de temps
Entity Sink		Accepter ou bloquer des entités
Output Switch		Sélectionnez le port de sortie de l'entité pour le départ
signal scope		Création d'un graphique à l'aide des données d'un signal basé sur un événement.

FIGURE 4.54 – Description des blocs Simevents

4.12 Conclusion

Dans ce chapitre, nous avons présenté la partie essentielle de notre travail, à savoir la mise en place d'une solution de haute disponibilité sous Windows Server 2016 au sein de l'EPB.

Cette étape nous a permis de réaliser notre objectif de répondre à la continuité opérationnelle que s'est fixé l'entreprise EPB. La solution apportée n'est certes pas optimale, mais c'est une étape que nous considérons importantes et que l'entreprise devra mettre en place dans les plus bref délais afin d'optimiser son réseau informatique.

Conclusion générale

Ce document a été rédigé au terme du projet de fin de cycle réalisé au sein de l'EPB.

Il s'agit en effet de mettre en place une solution de haute disponibilité en utilisant un cluster d'équilibrage de charge, qui devrait assurer la continuité opérationnelle de l'entreprise.

Pour cela, nous avons été amenés dans un premier lieu à perfectionner nos connaissances dans le domaine système informatique dans une entreprise, ainsi que l'administration et la supervision réseaux, ensuite, nous avons étudier l'existant au niveau de notre organisme d'accueil, ce qui nous a permis de poser une problématique, ainsi que nos objectifs.

Afin d'accomplir ce travail et d'aboutir au résultat prévu, nous avons choisi la solution mise en place par Microsoft pour les entreprise a savoir Windows server 2016. Ce système nous a permis de répondre aux besoin de l'EPB.

Ce projet nous a été très bénéfique, car nous avons enrichi nos connaissances sur les deux plans : théorique et pratique. Il nous a aussi permis de découvrir et d'acquérir de nouvelles connaissances et d'améliorer nos méthodes de travail. Nous avons été confrontés à des problèmes que nous n'avons pas envisagés. Le fait de l'avoir mené à son terme nous a apporté satisfaction qui a été complétée par le fait de répondre par une solution efficace à un besoin de l'entreprise. Durant la mise en place de ce projet, nous avons effectué de nombreuses recherches.

De plus, avoir eu l'opportunité de travailler dans une entreprise tel que l'EPB nous a permis de prendre conscience de la nécessité d'avoir un système informatique sans interruption.

Pour les perspectives, nous souhaitons implémenter une solution VPN et VLAN afin d'améliorer la securité du réseau de l'entreprise.

Bibliographie

[1] DROMARD Danièle et Dominique SERET. *Architecture des réseaux.* Pearson Education France, Collection Synthex, 2006, 256 pages.

[2] MONTAGNIER J. *Réseaux d'entreprise par la pratique.* Eyrolles, Paris, 2004, 548 pages.

[3] DEAN Tamara. *Network+ Guide to Networks.* Cengage Learning, New York, 2012, 896 pages.

[4] GORALSKI Walter. *The Illustrated Network : How TCP/IP Works in a Modern Network.* Morgan Kaufmann, Burlington, 2009, 832 pages.

[5] ATELIN philippe. *Réseaux informatique notion fondamentales.* Edition ENI, Paris, 2009, 407 pages.

[6] IBM Knowledge Center. Disponibilité haute disponibilité - présentation. [en ligne]. `https://www.ibm.com/support/knowledgecenter/fr/ssw_ibm_i_72/rzarj/rzarjgetstarted.htm`, [Consulté en Avril 2018].

[7] CARPENTIER Jean François. *La sécurité informatique dans la petite entreprise.* Edition ENI, Paris, 2016, 444 pages.

[8] RICHET Antoine, THOBOIS Loïc, and POPOTTE Sammy. Network load balancing. [en ligne]. `https://labo-microsoft.supinfo.com/articles/nlb/`, [Consulté en Mai 2018].

[9] Dr. HIGHLEYMAN Bill, HOLENSTEIN Paul, and Dr. HOLENSTEIN Bruce. Achieving century uptimes part 6 : Active/active versus clusters. [en ligne]. `https://shadowbasesoftware.com/articles/archive/achieving-century-uptimes-as-seen-in-the-connection/`, [Consulté en Mai 2018].

[10] REUTER Emmanuel. *Agents Mobiles : itinéraires pour l'administration système et réseau, Thèse de doctorat en Informatique.* PhD thesis, Université de Nice Sophia Antipolis, Soutenu le 28 Mai 2004.

[11] J. Case, M. Fedor, M. Schoffstall, and J. Davin. Rfc 1157 : Simple network management protocol (snmp). `https://tools.ietf.org/html/rfc1157`, Mai 1990.

[12] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser. Rfc 1441. introduction to snmp v2. `https://tools.ietf.org/html/rfc1441`, Avril 1993.

[13] J. Case, D. Partain, and B. Stewart. Rfc 3410 : Snmp v3. `https://tools.ietf.org/html/rfc3410`, Décembre 2002.

[14] Entreprise portuaire de bejaia. [en ligne]. `https://www.portdebejaia.dz/`, [Consulté en Mai 2018].

[15] Présentation de l'entreprise portuaire de béjaïa, documents internes de l'epb.

[16] Pr MOKDAD lynda. Cours : Modéliser, simuler avec simevent(matlab).

RÉSUMÉ

L'administration des réseaux informatiques évolue sans cesse et elle s'affirme aujourd'hui comme une activité clé de toute entreprise. En plus d'être constamment en fonction, ces outils d'échange de données et de partage d'information en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve.

Les opérations 24 heures sur 24 et la nécessité d'avoir des infrastructures toujours disponibles impliquent la disponibilité permanente des applications critiques. C'est ceci qui nous a poussés à mettre en place une solution de cluster avec équilibrage de la charge. Notre travail consiste à installer et configurer deux serveurs Remote Descktop Services avec équilibrage de la charge pour l'Entreprise Portuaire de Bejaia, ce qui permet d'une part, la facilité d'accéder aux applications publiées grâce au RemoteApp. D'une autre part, permettre à l'administrateur réseau de gérer ou dépanner le parc informatique de son entreprise, dans un plus bref délai et cela depuis son poste de travail ou bien tout poste qui est configuré pour l'accès distant. Le déploiement de cette solution a été mise en œuvre en utilisant différents logiciels informatiques tel que Windows serveur 2016, VMWare.

Mots clés : administration réseau, windows server 2016, cluster, disponibilité, équilibrage de charge.

ABSTRACT

The administration of computer networks is constantly evolving and is now becoming a key activity of any company. In addition to being constantly in operation, these tools for real-time data exchange and information sharing must be able to offer maximum privacy and foolproof security.

24-hour operations and the need for always-available infrastructures mean that critical applications are always available. This is what pushed us to implement a cluster solution with load balancing. Our job is to install and configure two load-balancing Remote Descktop Services servers for the Bejaia Port Company, which makes it easy to access published applications through the RemoteApp. On the other hand, allow the network administrator to manage or troubleshoot the computer park of his company, in a shorter time and that from his workstation or any post that is configured for remote access. The deployment of this solution has been implemented using various computer software such as Windows server 2016, VMWare.

Key words : network administration, windows server 2016, cluster, availability, load balancing.