LA REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLAB DE BLIDA
FACULTE DES SCIENCES
DEPARTEMENT D'INFORMATIQUE

MEMOIRE

Présenté pour l'obtention du diplôme ***de Master 2***

En :***Informatique***

Option : ***Sécurité de Système d'information***

Thème

Conception et implémentation d'une solution sécurisée d'accès au « dossier patient »

Présenté par: Asma Rahmani

Dirigé par : Mme D.Bouaissa

Soutenu le 20/10/2020, devant le jury composé de :

N. Boustia, Professeur, USDB 1 — *Président*

M.Arkam, MAA, USDB 1 — *Examinateur*

2019/2020

Remerciement

Avant tout, je remercie Allah le TOUT PUISSANT de m'avoir donné le courage et la patience, pour l'accomplissement de ce travail.

Je tiens à remercier chaleureusement mon promoteur Mme.D.Bouaissa enseignante à l'université de Saad Dahleb Blida , pour m'avoir proposée ce sujet et de m'avoir guidée tout au long de ce travail.

Mes remerciements s'adressent également aux membres du Jury pour nous avoir honorées en consentant à juger mon modeste travail.

Un immense merci à Mr. M.Z.Rahmani pour sa patience, son optimisme et son soutien sans faille.

Merci à tous

Dédicaces

À mon très cher père

Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être. Ce travail représente peu, comparé aux lourds sacrifices que vous avez consentis pour mon éducation et ma formation.

À ma très chère mère

Tu es l'exemple de dévouement qui n'a pas cessé de m'encourager et de prier pour moi. Puisse Allah, le tout puissant, te préserver et t'accorder santé, longue vie et bonheur.

À mes frères et mes chères sœurs

qui sont ce que j'ai de plus cher et qui ont toujours été là pour moi et soutenue, cette année et tant d'autres.

À tous ceux que j'aime.

Je vous dédie ce modeste travail

ASMA

Résumé :

Dans les établissements de santé, le déploiement d'un dossier patient informatisé est un défi considérable. Il doit prendre en charge le patient depuis son admission au bureau des entrées, durant son séjour à l'hôpital, tous les actes médicaux, jusqu'à la fin de son séjour, il doit aussi permettre d'archiver toutes les informations de ce patient.

Parmi les défis, la sécurité d'accès au dossier patient non seulement au sein de l'établissement mais même en dehors. Delà vient l'idée de notre projet de fin d'étude intitulé « Conception et Implémentation d'une solution sécurisé d'accès ou « dossier patient » ».

La solution proposée dans notre travail contient deux partie la première est l'authentification par service d'annuaire gérer par un contrôleur de Domain, la deuxième partie consiste à permettre aux médecins et infirmiers de pouvoir se connecter de l'extérieur à travers Internet, il a fallu donc sécuriser la liaison via VPN.

Pour les outils, on a opté à l'utilisation des services de Windows server 2016.

Mots clés : Contrôleur de Domain, VPN, Windows server 2016.

ملخص

في مرافق الرعاية الصحية، يعد سجل المريض المحوسب تحديًا كبيرًا. يجب أن يحتوي على معلومات المريض من دخوله إلى مكتب الدخول، وأثناء إقامته في المستشفى، وجميع الأعمال الطبية، حتى نهاية إقامته، كما يجب أن يتيح إمكانية أرشفة جميع المعلومات الخاصة بهذا المريض.

ومن بين التحديات، أمن الوصول إلى ملف المريض ليس فقط داخل المؤسسة ولكن حتى خارجها. من هنا تأتي فكرة مشروع نهاية الدراسة بعنوان "تصميم وتنفيذ حل الوصول الآمن الى " سجل المريض ".

يحتوي الحل المقترح في عملنا على جزأين، الأول هو المصادقة عن طريق خدمة الدليل التي تدار بواسطة وحدة تحكم المجال، ويتكون الجزء الثاني من السماح للأطباء والممرضات بالقدرة على الاتصال من الخارج عبر الإنترنت. من VPN.

الكلمات الدالة مراقب وحدة ف ب ان وWindows Server 2016

abstract

In healthcare facilities, the deployment of a computerized patient record is a considerable challenge. He must take care of the patient from his admission to the entry office, during his stay in the hospital, all medical acts, until the end of his stay, he must also make it possible to archive all the information of this patient.

Among the challenges, the security of access to the patient file not only within the establishment but even outside. From this comes the idea of our end of study project entitled "Design and Implementation of a secure access solution or" patient record "".

The solution proposed in our work contains two parts the first is the authentication by directory service managed by a Domain controller, the second part consists of allowing doctors and nurses to be able to connect from the outside through the Internet. It was therefore necessary to secure the connection via VPN.

For tools, we opted to use Windows server 2016 services.

Keywords: Domain controller, VPN, Windows server 2016.

Table des matières

Liste des Figures :

INTRODUCTION GENERALE :

Les réseaux informatiques sont devenus, depuis plusieurs années, un élément très important dans toute institution : commerciale, industrielle, gouvernementale, éducative, etc. Ceci est dû notamment à la vulgarisation de l'outil informatique et l'apport extraordinaire qu'apportent les réseaux informatiques dans la circulation rapide de l'information.

Le domaine de la santé comme tous les autres domaines a connu une progression au niveau de la numérisation. Les informations liées à la prise en charge d'un patient autrefois conservées sous la forme d'un dossier médical papier et d'un dossier infirmier distinct ont été rassemblées sous la forme d'un dossier patient informatisé. Vu l'importance de ces informations qui sont souvent véhiculées dans le réseau, ceux-ci requièrent une bonne gestion du réseau, une souplesse d'utilisation et un certain degré de sécurité.

De cela, l'authentification est une démarche importante et présente plusieurs avantages. Elle permet en premier lieu de sécuriser le réseau de l'établissement sanitaire. Avec cette barrière de sécurité, on peut aussi interdire aux inconnus d'accéder au réseau.

À cet effet, la mise en place d'une infrastructure réseau comportant un service d'annuaire géré par le contrôleur de domaine afin d'harmoniser dans un environnement sécurisé tous les composants du système (les données patients, les utilisateurs et toutes les interactions)

D'une autre part, il est nécessaire de pouvoir consulter le dossier patient de n'importe quel endroit, par exemple un médecin doit avoir la possibilité de consulter le dossier de son patient qu'il soit dans un autre établissement ou en cas d'urgence.
Pour remédier à ce problème, il existe plusieurs technologies comme le Firewall, les listes de contrôle d'accès et le VPN (Virtual Private Network), les experts considèrent que le VPN est la technologie la plus sécurisée.

Dans notre travail on a proposé une solution qui permettra au médecin de consulter le dossier patient une fois authentifié par un contrôleur de Domaine même en dehors de l'établissement de santé en utilisant le VPN.

Le mémoire contient trois chapitres le premier présente une généralité sur les réseaux et VPN, le deuxième consacré au contrôleur de Domaine et aux services domaine active directory et le troisième chapitre à la conception et implémentation de la solution proposée.

CHAPITRE 1 : GENERALITES SUR LES RESEAUX ET LA SECURITE

1.1. Introduction

Les réseaux informatiques des entreprises constituent un ensemble d'équipements connectes entre eux afin de s'échanger tout type d'informations.
De cet effet une préoccupation est apparue celle de la sécurité du transport des données, ainsi que l'accès aux informations sur les différents postes de travail.
Alors, nous allons aborder dans ce premier chapitre, quelques notions sur les réseaux ainsi que les concepts de la sécurité informatiques.

1.2. Les réseaux informatiques

1.2.1. Définition

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue de partager des données, des ressources ou des informations. En d'autres termes, c'est une infrastructure de communication reliant des équipements informatiques qui permet de partager des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles). [1]

1.2.2. Type des réseaux

On peut distinguer trois types de réseaux selon la localisation, la distance et le débit,

- *LAN (Local Area Network) ou réseau local*

Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet) [2].
La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s [3].
La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs [3].

- *MAN (Metropolitan Area Network) ou réseau métropolitain*

Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants, supérieur à 100 Mbits/s. Ainsi Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [2].

- *WAN (Wide Area Network) ou réseau étendu*

Interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent

de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet [2].

1.2.3. Topologie des réseaux

Comme le nom de topologies implique, elles ont à voir avec la forme d'un réseau. Il en existe deux types :

- *Les topologies physiques* : se réfèrent à la mise en forme réelle des fils dans un réseau
- *Les topologies logiques* : se réfèrent plus à la façon dont les données se déplacent via le réseau. Elle peut être différente de la topologie physique. Les topologies physiques et logiques les plus classiques sont maillées, en anneau et en bus.

1.2.3.1. Le réseau maillé

En ce qui concerne les topologies maillées, Il y a en fait deux types. Il y a le maillage complet, et puis il y a aussi le maillage partiel. Dans la topologie maillée complète, tous les périphériques sont connectés directement à tous les autres appareils. Cela fournit une redondance complète pour le réseau. Alors que chaque appareil connecté à tous les autres appareils fournit une grande redondance, il augmente également le coût de manière significative. [4]

Figure 1 : Réseau maillé.

1.2.3.2. Le réseau en bus

La topologie du bus est la plus ancienne technologie de réseau disponible. Avec la technologie bus, tous les nœuds ou les ordinateurs sont connectés directement à un câble principal qui traverse le réseau appelé le bus. [4]

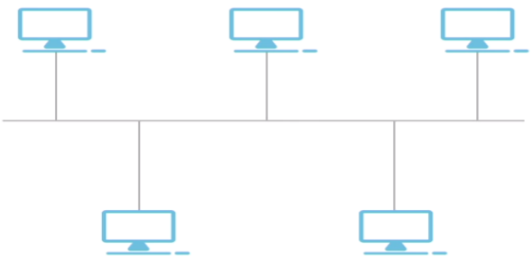

Figure 2 : Réseau en bus.

1.2.3.3. Le réseau en anneau

La topologie de l'anneau est également l'une des topologies réseaux les plus anciennes à notre disposition, et elle est similaire à la topologie de bus dans le sens où vous avez à câble dorsal unique auquel tous les nœuds ou tous les ordinateurs se connectent. La différence est qu'au lieu d'avoir ce câble dorsal juste déroulé comme dans la topologie du bus, ce câble dorsal est fondamentalement connecté à lui-même pour former un anneau ou un cercle. Les paquets sont alors capables de se déplacer autour du cercle, comme dans le motif de l'anneau. [4]

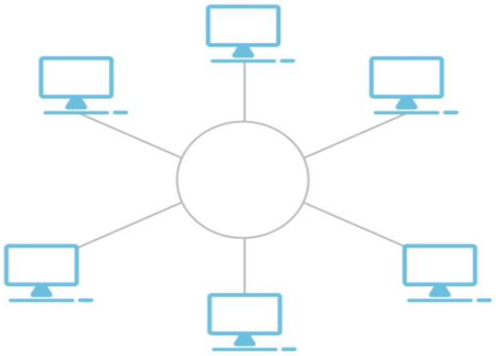

Figure 3 : Réseau en anneau.

1.2.3.4. Le réseau en étoile

Dans une topologie en étoile, tous les nœuds se connectent à un concentrateur ou à un commutateur central. Cela facilite grandement le dépannage d'une configuration en étoile hiérarchique. Le principal problème avec une configuration en étoile est qu'il est susceptible de connaître un seul point de défaillance. Cependant, si l'ensemble du réseau tombe en panne car un périphérique central a un problème, alors vous savez où est le problème, il vous suffit de regarder le périphérique central. [4]

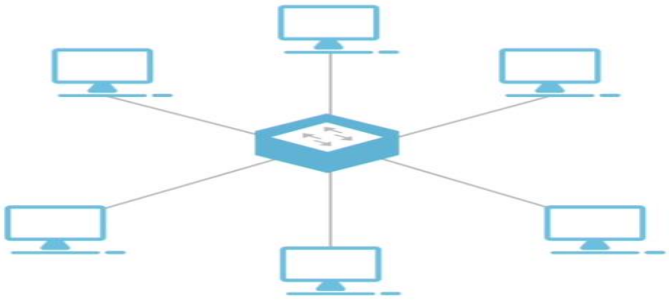

Figure 4 : Réseau en étoile.

1.2.3.5. Topologie hybride

Au-delà des types de topologie de base dont nous avons déjà parlé, nous avons également une topologie hybride. À la base, une topologie hybride combine une topologie avec une autre. Les topologies hybrides existent en plusieurs types. Un type est la topologie hybride physique. Un autre type est la topologie hybride physique-logique. Dans la topologie hybride physique, vous disposez essentiellement d'un réseau contenant deux topologies physiques ou plus au sein du réseau et dans la topologie hybride physique-logique, vous avez un réseau qui ressemble physiquement dans un sens ou qui ressemble physiquement à une topologie, mais fonctionne comme une technologie différente. [4]

1.2.4. Les connexions Client-Serveur et Peer-to-Peer

Il existe essentiellement deux modèles de gestion de réseau disponibles pour un réseau local :

1.2.4.1. Client-Serveur :

Le modèle de gestion réseau serveur client, tous les périphériques accèdent aux ressources du réseau via un serveur central. Dans ce cas, pour qu'un périphérique se connecte au réseau, il doit se connecter au serveur et chaque périphérique du réseau qui n'est pas le serveur est appelé client. Le ou les périphériques contrôlant l'accès au réseau et les ressources du réseau sont appelés serveurs. [4]

1.2.4.2. Peer-to-Peer

Dans un modèle poste à poste, chaque ordinateur du réseau est responsable de sa propre sécurité et de sa propre gestion. Fondamentalement, chaque ordinateur est géré comme un périphérique distinct et, par conséquent, la gestion repose sur des ordinateurs individuels [4]. Chaque poste peut être un client ou un serveur selon le poste est-ce qu'il demande ou fournit le service.

1.3. Sécurité de réseau

La sécurité informatique est l'ensemble des moyens outils, techniques et méthodes mise en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles [5]
Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent.

1.3.1. Objectifs de la sécurité

- *L'intégrité,* c'est-à-dire garantir que les données sont bien celles que l'on croit être.
- *La confidentialité,* consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- *La disponibilité,* permettant de maintenir le bon fonctionnement du système d'information.
- *La non répudiation,* permettant de garantir qu'une transaction ne peut être niée.
- *L'authentification,* consistant à assurer que seules les personnes autorisées aient accès aux ressources.

1.3.2. Les différents types de sécurité

Une sécurité couvre les éléments suivants :

- *Sécurité de l'infrastructure :* couvre la sécurité logique et physique des équipements et des connexions réseau.
- *Sécurité des accès :* couvre la sécurité logique des accès locaux et distants aux ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès aux systèmes d'information de l'entreprise.
- *Sécurité de l'Intranet face à Internet ou aux tierces parties de confiance :* couvre la sécurité logique des accès aux ressources de l'entreprise (Extranet) et l'accès aux ressources extérieurs (Internet).

1.3.3. Les protocoles d'authentification

Pour la sécurité des accès les organismes utilisent l'authentification pour contrôler quels utilisateurs ont accès aux réseaux et aux ressources de l'organisme, ainsi que pour identifier et contrôler les machines et les serveurs qui ont accès.

Le protocole d'authentification permet de contrôler l'accès aux systèmes en vérifiant si les informations d'identification d'un utilisateur correspondent aux informations d'identification d'utilisateurs autorisés sur un serveur d'authentification de données.

Les protocoles d'authentification les plus utilisés sont TACACS +, RADIUS, KERBEROS, LDAP et Active Directory

- *TACACS + :*

Terminal Access Controller Access Control System (TACACS) est le nom quelque peu redondant d'un protocole Cisco propriétaire pour gérer l'authentification et l'autorisation. Le signe plus distingue la version moderne du protocole d'une version très ancienne que personne n'utilise plus.

TACACS + présente quelques caractéristiques distinctives clés. Il permet le cryptage complet des paquets d'authentification lorsqu'ils traversent le réseau entre le serveur et le périphérique

réseau. Cela empêche un attaquant de voler vos identifiants de connexion lorsqu'ils traversent le réseau.

La caractéristique la plus importante et la plus utile de TACACS + est sa capacité à effectuer une autorisation de commande granulaire fine. Lorsque vous utilisez l'autorisation de commande avec TACACS + sur un périphérique Cisco, vous pouvez restreindre exactement les commandes que différents utilisateurs administratifs peuvent saisir sur le périphérique.

Par exemple, vous pouvez autoriser un utilisateur du service d'assistance à consulter la sortie de la commande « show interface brief», mais pas les autres commandes «show», ni même les autres options de commande «show interface». [6]

- *RADIUS :*

Le service RADIUS (Remote Authentication Dial-In User Service) est rarement utilisé pour authentifier les utilisateurs d'accès à distance, mais c'est pourquoi il a été développé à l'origine. C'est maintenant un protocole général pour l'authentification des utilisateurs.

Contrairement à TACACS +, RADIUS ne crypte pas le paquet entier. Au lieu de cela, il chiffre uniquement la partie du paquet qui contient les informations d'authentification de l'utilisateur. Ce niveau de sécurité est généralement considéré comme suffisant, bien que je ne recommanderais pas de le faire passer sur Internet public sans chiffrement supplémentaire tel qu'un VPN.

Bien que RADIUS puisse être utilisé pour authentifier les utilisateurs administratifs lorsqu'ils accèdent aux périphériques réseau, il est plus généralement utilisé pour l'authentification générale des utilisateurs accédant au réseau. Par exemple, RADIUS est le protocole sous-jacent utilisé par 802.1X pour authentifier les utilisateurs câblés ou sans fil accédant à un réseau. [6]

- *KERBEROS :*

Kerberos fonctionne en attribuant une clé unique (appelée ticket) à chaque client qui s'authentifie avec succès sur un serveur. Le ticket est crypté et contient le mot de passe de l'utilisateur, qui est utilisé pour vérifier l'identité de l'utilisateur lorsqu'un service réseau particulier est demandé. [7]

Le protocole Kerberos utilise une cryptographie forte afin qu'un client puisse prouver son identité à un serveur (et vice versa) via une connexion réseau non sécurisée. Une fois qu'un client et un serveur ont utilisé Kerberos pour prouver leur identité, ils peuvent également crypter toutes leurs communications pour garantir la confidentialité et l'intégrité des données au cours de leurs activités.

- *LDAP et Active Directory :*

Le LDAP ou Lightweight Directory Access Protocol est un protocole visant à interroger et manipuler de manière synchrone ou asynchrone les annuaires. Active Directory est un annuaire au format Microsoft qui a pour objectif de stocker des informations en centralisant les données. L'authentification Active Directory permet aux utilisateurs de se connecter au système s'ils ont un compte dans un domaine Active Directory.

Certains périphériques réseau, en particulier les périphériques sans fil, peuvent communiquer directement avec LDAP ou Active Directory pour l'authentification. Mais les commutateurs et routeurs Cisco ne parlent pas nativement LDAP et Active Directory. Si vous avez du matériel Cisco, vous devrez utiliser autre chose, généralement RADIUS, comme étape intermédiaire.[6].

1.3.4. Technologie utilisée pour sécuriser un Intranet face à Internet

Afin d'accéder au réseau interne depuis l'extérieur des technologies sont utilisées pour sécuriser un Intranet on a :

1.3.4.1. *Pare-feu* Un firewall (ou pare-feu) est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise) [15].

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

1.3.4.2. *Les zones démilitarisées* Une zone démilitarisée est un sous-réseau (DMZ) isolé par deux pare-feux (firewall). Ce sous-réseau contient des machines se situant entre un réseau interne (LAN - postes clients) et un réseau externe (typiquement, Internet).

La DMZ permet à ces machines d'accéder à Internet et/ou de publier des services sur Internet sous le contrôle du pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par le pare-feu interne.[16]

Le DMZ permet de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs.

Serveurs installés sur la DMZ :

– Les serveurs Web (http),
– Les serveurs de fichiers (ftp),
– Les serveurs d'e-mails (SMTP),
– Les serveurs de noms (DNS).

1.3.4.3. *Le RDP* RDP signifie Remote Desktop Protocol ou Protocole de Bureau à Distance, RDP permet de vous connecter directement à votre PC du bureau, de sorte que vous devez entrer votre nom d'utilisateur et votre mot de passe. Par la suite RDP chargera votre profil et votre bureau (desktop). Une fois chargé, l'écran de l'ordinateur distant affichera la

même image que votre ordinateur du bureau, tout comme si vous étiez assis devant votre ordinateur au bureau.

1.3.4.4. Le Réseau virtuel privé VPN

Pour faire face au problème de sécurité de l'interconnexion des réseaux d'organisme avec l'Internet, ou tout autre réseau, il est donc nécessaire de protéger les entrées et sorties sur le réseau.
Le VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Cette technologie, de plus en plus utilisée dans les organismes, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante, les données soient illisibles. [8]

1.3.4.4.1. Connexion

Il existe trois types de connexions VPN

1. ***Le VPN d'accès (poste à site) :*** Ce type nomade, également appelé "Road Warrior" permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services [9].

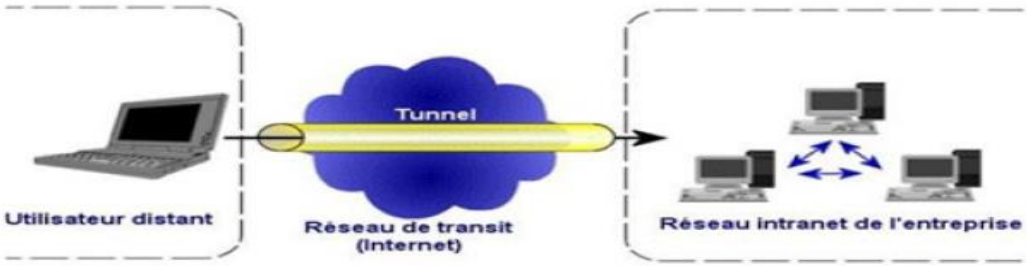

Figure 5 : Le fonctionnement d'un VPN poste à site [10].

2. ***Site à site (LAN to LAN) :*** qui permet de relier deux réseaux d'entreprises entre eux de façon transparente [9].

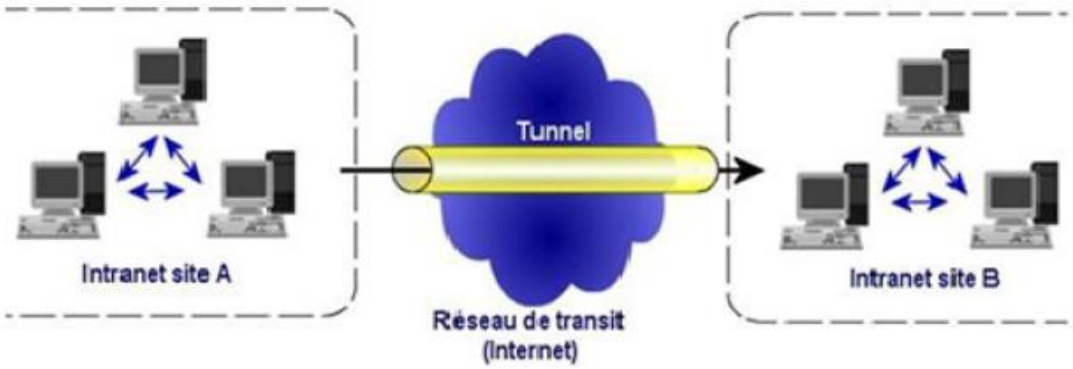

Figure 6: Architecture VPN LAN to LAN [10].

3. ***Poste à poste (Host to Host) :*** Ce type de VPN est utilisé par les entreprises afin de communiquer avec ses clients en ouvrant son réseau local à ses clients ou partenaires [9].

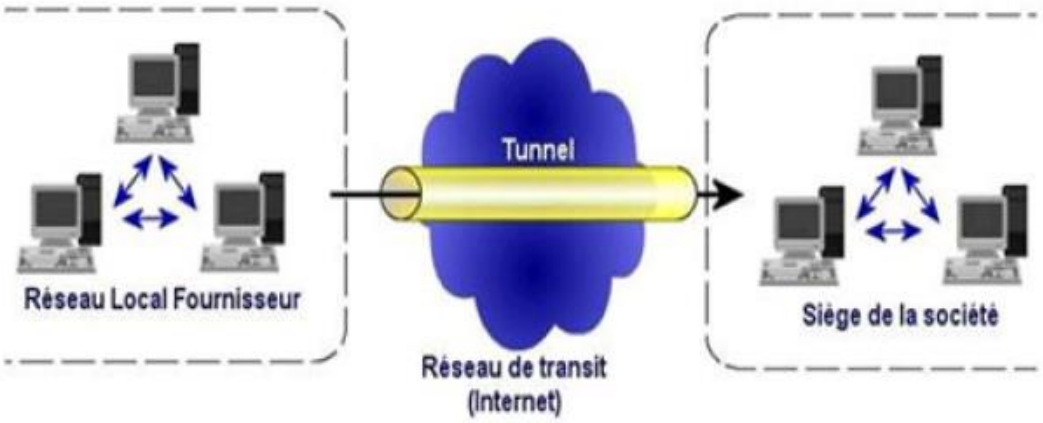

Figure 7 : Le fonctionnement de l'extranet [10].

1.3.4.4.2. Les fonctionnalités du VPN

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

- Authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa.
- Authentification des utilisateurs : seules les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.
- Gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveaux clients en obtenir une facilement.
- Cryptage du tunnel : les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa.
- Les clés de cryptage doivent être régénérées souvent (automatiquement).
- Le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

1.3.4.4.3. Les principaux protocoles de VPN

- *PPTP (Point-to-Point Tunneling Protocol)* est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.

- *L2F (Layer TwoForwarding)* est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- *L2TP (Layer Two Tunneling Protocol)* est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- *IPSec*est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP [10].

1.4. Conclusion

Au cours de ce chapitre, nous avons parcouru les notions générales des réseaux informatiques en présentant les différentes topologies des réseaux.
Par la suite nous nous sommes intéressés au principe de la sécurité informatique, ses objectifs, ses types et les topologies de l'authentification puis nous avons présenté les VPNs.

CHAPITRE 2 : LE CONTROLEUR DE DOMAINE

2.1. Introduction

De nos jours, la gestion du réseau se fait à travers un système d'exploitation serveur spécialement conçu pour répondre aux demandes des ordinateurs clients. Nous citons par exemple Windows Server, Unix, Linux, etc.

Windows server, propose de déployer des contrôleurs de domaine sous l'annuaire Active directory qui s'appuie sur la norme LDAP. Beaucoup d'améliorations ont été apportées depuis. Il comprend généralement l'ensemble des comptes nécessaires à l'authentification des ordinateurs et utilisateurs d'une entreprise. [13]

2.2. Les services de domaine Active Directory

Les AD DS (Active Directory Domain Services) constituent les fonctions essentielles d'Active Directory pour gérer les utilisateurs et les ordinateurs et pour permettre aux administrateurs système d'organiser les données en hiérarchies logiques.

AD DS fournit des certificats de sécurité, LDAP, et la gestion des droits. [11]

Le rôle Services de domaine Active Directory contient des composants physiques et logiques.

2.2.1. Les composants physiques qui englobent plusieurs éléments clés dans un domaine Active Directory. Ces derniers peuvent être matériels ou logiciels :

- *Le contrôleur de domaine :* qui est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs des réseaux informatiques. La mission première du DC est d'authentifier un utilisateur et de valider son accès au réseau. Lorsque les utilisateurs se connectent à leur domaine, le DC vérifie leur identifiant, leur mot de passe ainsi que d'autres authentifiant, afin de leur autoriser ou leur refuser l'accès.

  Le concept le plus important à comprendre est qu'AD DS est un cadre de gestion de domaine et que l'ordinateur que les utilisateurs utilisent pour accéder à AD est le DC.

- *Les sites :* sont des ensembles de plusieurs sous réseaux IP reliés entre eux par des liaisons à haut débit. Les liaisons entre sites peuvent être plus lentes ou plus coûteuses. La notion de site est indépendante de la notion de domaine, un domaine peut contenir plusieurs sites et un site peut contenir plusieurs domaines. [14]

- *La base de données et le dossier sysvol :* qui vont contenir l'ensemble des informations d'Active Directory (propriétés des comptes utilisateurs, ordinateurs…). Chaque contrôleur de domaine du domaine Active Directory en contient une copie.

2.2.2. L'Architecture de l'Active Directory :(composants logiques)

Les composants physiques fonctionnent avec des composants logiques, ces derniers permettent de mettre en place la structure Active Directory souhaitée.

– *Domaine (ou sous-domaine) :* est le composant logique principal .Un domaine Active Directory est un regroupement logique de comptes utilisateurs, ordinateurs ou de groupes. Les objets qui sont créés sont stockés dans une base de données présente sur tous les contrôleurs de domaine Active Directory. Cette base de données peut stocker plusieurs types d'objets.
.

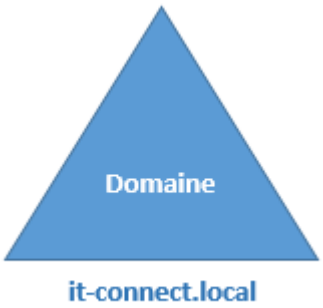

Figure 11 : Présentation d'un Domaine

Le **nom du domaine** est très important. Il doit correspondre à un nom **DNS résolvable** au sein du réseau de l'entreprise et à l'extérieur (sur internet).

– *Arborescence :* Ensemble de domaines appartenant à une même hiérarchie de nom DNS, le Domaine racine est le premier domaine créé, non renommable, non supprimable.
L'ajout d'un nouveau domaine se fait en créant un domaine enfant à un domaine existant de l'arborescence. Le nom complet (DNS) du nouveau domaine est obtenu en concaténant son nom au nom du domaine parent.

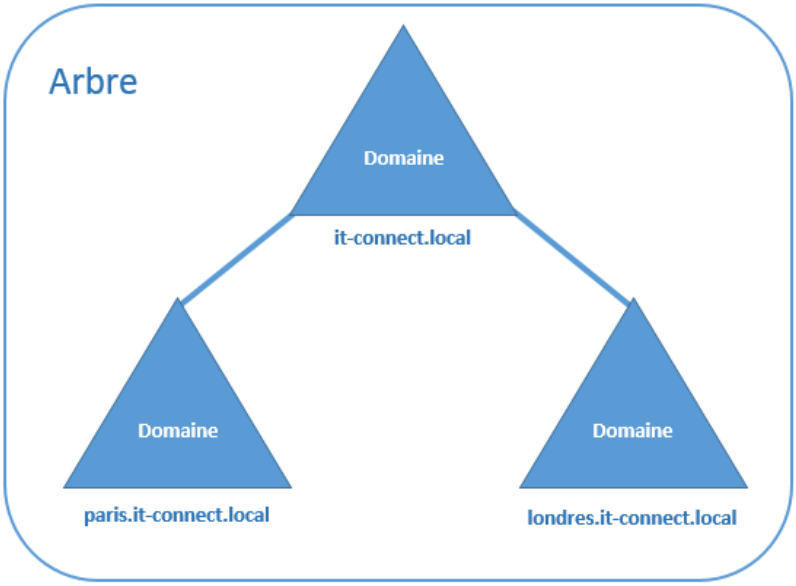

Figure 12 : Représentation d'une arborescence.

– *Forêt :* Ensemble d'arborescences qui appartient à la même organisation. Le nom de la forêt est le nom de l'arborescence racine (première arborescence créée dans la forêt). Une forêt peut ne contenir qu'une seule arborescence

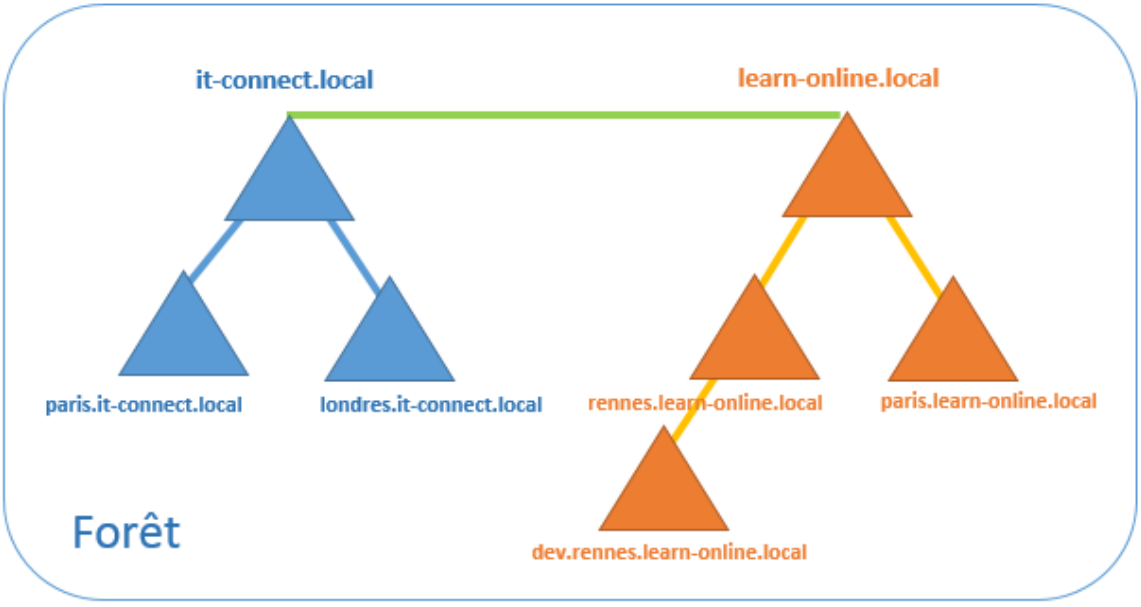

Figure 13 : Représentation d'une forêt.

Une architecture Active Directory repose sur des serveurs sur lesquelles sont installé les domaines contrôleurs.

2.3. Le DNS

Le DNS pour **Domain Name System** est obligatoire pour le fonctionnement d'AD DS. Un serveur DNS externe au serveur AD DS peut être utilisé (Windows ou Linux). Cependant, il est possible d'installer le rôle DNS en même temps qu'un Domain Controller. Cela permet à AD DS d'être directement intégré au DNS sans configuration supplémentaire.

L'AD DS utilise les services de résolution de noms DNS pour permettre aux clients de localiser les contrôleurs de domaine et aux contrôleurs de domaine qui hébergent le service d'annuaire de communiquer entre eux.

AD DS permet une intégration facile de l'espace de noms Active Directory dans un espace de noms DNS existant. Des fonctionnalités telles que les zones DNS intégrées à Active Directory facilitent le déploiement de DNS. [12]

2.4. Les services fournis par un Domaine active directory (AD DS)

Voici les services fournis par AD DS, qui constituent les fonctionnalités de base d'un système de gestion centralisée des utilisateurs.

- **Services de domaines** : stocke les données et gère les communications entre les utilisateurs et le contrôleur de domaine. Il s'agit de la principale fonctionnalité d'AD DS.

- **Services de certificat** : permet à votre contrôleur de domaine de servir des certificats et des signatures numériques, ainsi qu'un chiffrement à clé publique.

- **Lightweight Directory Services** : prend en charge LDAP pour des services de domaine multiplateformes, par exemple l'ensemble des ordinateurs Linux présents sur votre réseau.

- **Services de fédération d'annuaire** : dans la même session, fournit une authentification SSO pour plusieurs applications. Ainsi, les utilisateurs ne sont pas obligés de ressaisir les mêmes identifiants.

- **Gestion des droits** : contrôle les politiques en matière de droits à l'information et d'accès aux données. Par exemple, la gestion des droits détermine si vous pouvez accéder à un dossier ou envoyer un e-mail. [11]

2.5. Les avantages des services d'un domaine Active directory

Pour l'administration de base des utilisateurs et ordinateurs réseau, l'utilisation d'AD DS présente plusieurs avantages.

- Les données sont organisées de façon à répondre aux besoins de l'organisme.
- AD DS fournit une fonction intégrée de réplication et de redondance : si un contrôleur de domaine tombe en panne, un autre contrôleur de domaine prend la charge à son compte
- Tout accès aux ressources réseau passe par AD DS, ce qui assure une gestion centralisée des droits d'accès au réseau

- On peut inclure un ou plusieurs domaines, chacun avec un ou plusieurs contrôleurs de domaine, qui permettent de faire évoluer l'annuaire en fonction des besoins du réseau.

2.6. Les objets Active Directory et comment sont organisés

Active Directory stocke des informations sur les objets du réseau où chaque objet possède un ensemble d'attributs regroupant diverses informations permettant de le distinguer. Certains objets peuvent être des conteneurs d'autres objets. S'ils sont bien paramétrés, ils permettent de connaître très rapidement le détail des ressources spécifiques du système informatique d'une entreprise. Les objets active directory sont principalement regroupés en quatre types.

2.6.1. Utilisateurs

Un utilisateur dans ADDS correspond souvent à **un utilisateur physique**

Lors de la création d'un nouvel utilisateur, les informations essentielles seront demandées :

- Noms : prénom, nom, initiales et nom complet
- Noms d'ouverture de session
- Mot de passe
- Options de mot de passe

2.6.2. Ordinateurs

En effet, les utilisateurs vont dans beaucoup de cas se connecter sur un ordinateur en utilisant leur compte de domaine donc on **joindre** un ordinateur au domaine.
En cas de problème, il est toujours possible de s'authentifier sans un compte de domaine : on parle ici d'une **authentification locale**.

2.6.3. Unités d'organisation

Une unité d'organisation, Organizational Unit ou **OU** est une entité hiérarchique qui peut contenir des utilisateurs, des ordinateurs et d'autres OUs.
Une unité d'organisation a 3 rôles :

- ***L'organisation :*** permettre de retrouver rapidement les objets AD
- ***La délégation des droits d'administration*** sur les objets contenus dans l'OU à d'autres utilisateurs exemple Dans une entreprise assez conséquente, vous ne

serez probablement pas le seul à administrer le système d'information de l'entreprise. Il est également important de ne pas donner trop de droits à des utilisateurs.

- ***L'application des stratégies de groupe :*** GPO (group policy object). Les GPO permettent de restreindre des actions comme les accès restreints à toutes les ressources ou certains dossiers, la désactivation de certains exécutables etc.

Les GPO peuvent s'associer à l'ensemble des domaines et des UO.

2.6.4. Les Groupes

Un groupe c'est un ensemble d'utilisateurs ou d'ordinateurs ou d'autres groupes avec des droits spécifiques.
Puisqu'un objet hérite automatiquement des droits de son parent, il est intéressant de former des groupes, d'y placer des objets, et d'attribuer des permissions aux groupes. Cela évite de traiter chaque objet séparément.
Les groupes peuvent bénéficier de droits particuliers (comme par exemple le droit de sauvegarder, de gérer les imprimantes, etc ...) ou hériter des droits par imbrication du groupe dans un autre groupe.

Types de groupe : deux types de groupes sont disponibles :

- ***les groupes de sécurité*** utilisés pour gérer la sécurité des ressources du ou des domaines.

- ***les groupes de distribution*** utilisés par exemple pour envoyer des messages électroniques à l'ensemble des utilisateurs de ces groupes. Ces groupes ne peuvent pas être utilisés pour la sécurité.

L'étendue d'un groupe correspond à sa portée au niveau de l'arborescence Active Directory, les étendues peuvent aller d'une portée uniquement sur le domaine local, mais aussi s'étendre sur la forêt entière. Il existe trois étendues différentes :

- **Domaine local :**

Un groupe qui dispose d'une étendue « domaine local » peut être utilisé uniquement dans le domaine dans lequel il est créé.

- **Globale :**

Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base.

- **Universelle :**

Un groupe disposant de l'étendue « universelle » à une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

2.7. Conclusion

Dans ce chapitre nous avons présenté le domaine active directory en définissant ces composants physique et logique ainsi que ces services leurs avantages.
Dans les chapitres suivants, la mise en place d'un contrôleur de domaine sera détaillée avec une solution qui permit aux utilisateurs d'y accéder à distance.

CHAPITRE 3 : CONCEPTION ET IMPLEMENTATION

3.1. Introduction

Afin de bien mener notre objectif de permettre au médecin de consulter le dossier patient à l'intérieure de l'établissement de santé et même en dehors, nous allons définir l'architecture réseau proposée et les différents outils que nous utiliserons ainsi que les installations et les configurations requises.
Dans le cadre de notre travail, nous avons simulé le système en faisant appel au logiciel VirtualBox.

3.2. Architecture de la solution proposée

L'infrastructure réseau proposée est : un contrôleur de demain pour l'authentification des utilisateurs avec un serveur DHCP pour attribution automatique des adresses IP au niveau de LAN et pour l'accès externe via internet on recommande un serveur VPN qui créera un tunnel sécurisé internet-internat.

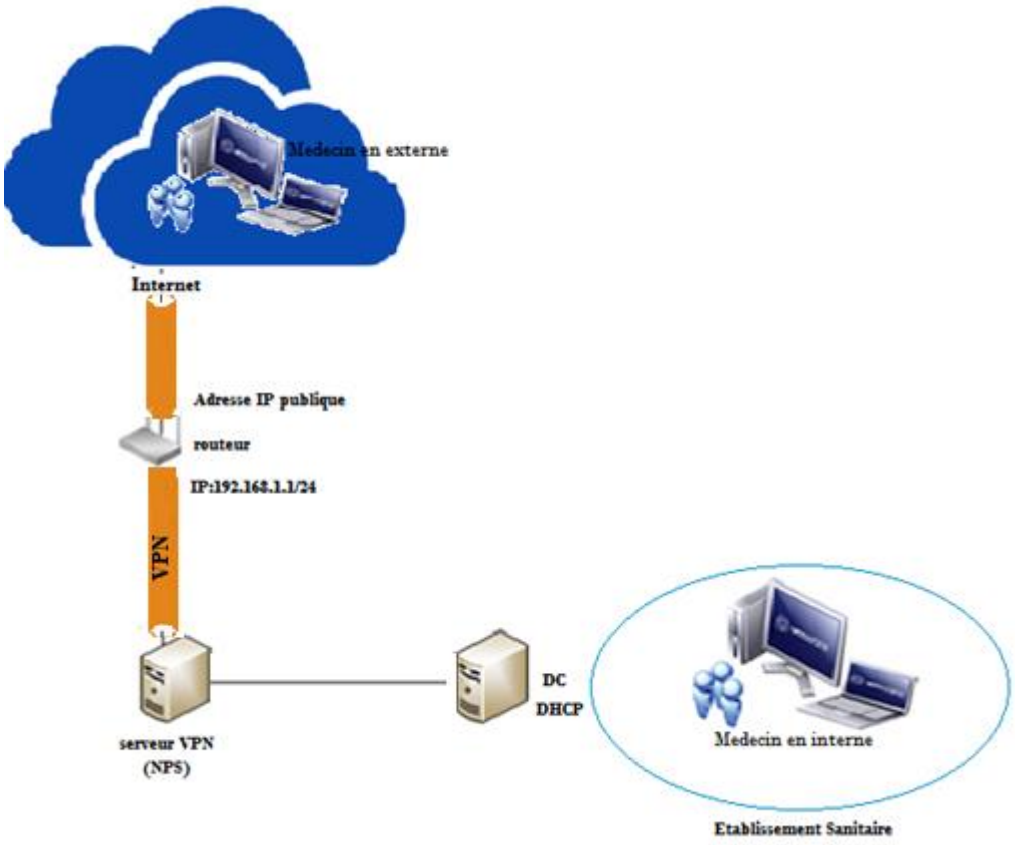

Figure 14 : Architecture de la solution proposée.

3.3. Implémentation de la solution proposée

3.3.1. Les outils de travail

Pour la solution proposée on a opté pour **Windows Server** ; c'est un choix incontournable pour les établissements et les entreprises, Windows Server est une option à étudier pour tout établissement désireuse d'avoir un outil familier pour gérer ses comptes utilisateurs, groupes et règles de partage. La solution serveur de Microsoft et grâce à ses différents services permet la gestion des utilisateurs et des ressources via le service **Contrôleur de Domaine**(voir chapitre 2), l'interconnexion sécurisé par le serveur **VPN** (voir chapitre 1) avec le rôle d'accès à distance et enfin le **NPS (Network Policy Server)** (NPS dans Windows server 2016 et 2019) qui permet la création et l'application des stratégies d'accès au réseau à l'échelle de l'organisation pour l'authentification et l'autorisation des demandes de connexion.

À l'activation du contrôleur de Domaine le service **DNS (Domain Name Server)** est automatiquement activé ce dernier correspond tout d'abord à un protocole permettant à des clients (du réseau) d'interroger une base de données contenant des informations sur les machines et les services hébergés par ces machines.
DNS est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine [12].

Serveur **DHCP (Dynamic Host Configuration Protocol)** a pour but de fournir une adresse IP et un masque à tout périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la configuration, d'autres paramètres tous aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser, des serveurs WINS et le suffixe de domaine pour ne citer que les principaux.
DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs [12].

Vu la situation sanitaire que vit notre pays et vu que le lieu de stage était un établissement sanitaire, j'étais contrainte de faire mes tests sur machines virtuelles « virtualBox ».

3.3.2. Pourquoi utiliser LDAP Active directory, Windows server et VPN

- *LDAP :*

LDAP peut être utilisé comme un répertoire central accessible sur tout le réseau. De plus, puisque LDAP prend en charge les fonctions Secure Sockets Layer (SSL) et Transport Layer Security (TLS), des données confidentielles peuvent être protégées contre toute intrusion.

LDAP prend aussi en charge diverses bases de données parallèles pour y enregistrer des répertoires. Ainsi, les administrateurs disposent de la flexibilité nécessaire pour déployer la base de données la plus adaptée au type d'informations que le serveur doit disséminer. De plus, comme LDAP comporte une interface de programmation d'application (ou API de l'anglais Application Programming Interfaces) bien définie, le nombre d'applications compatibles avec LDAP est vaste et croissant aussi bien en quantité qu'en qualité. D'après [17] et [18]

- *Windows Server :*

En comparant les deux systèmes les plus utiliser Windows et Linux, on peut supposer que Linux propose en principe des solutions moins chères que sous Windows pour héberger un serveur. Dans la pratique, cela s'avère parfois être une fausse conclusion. Selon les différentes distributions l'assistance est plus ou moins chère et son personnel plus ou moins qualifié. Le modèle complexe de licence Windows représente toutefois un léger désavantage. On ajoute les fonctions complexes de communication et de structuration du travail, la compatible avec des programmes courants et l'assistance long-terme pour toutes les versions. Dans notre cas établissement sanitaire le système d'exploitation Windows server relève le bon choix par son assistance et ça structure du travaille plus ça flexibilité qui permet l'utilisation dans une grande échelle. [19]

- *VPN :*

Le principal avantage d'une DMZ est qu'elle fournit un terrain neutre, généralement pour les services auxquels doivent accéder (par exemple, un service Web) par les utilisateurs internes et externes. Par conséquent, placer un contrôleur de domaine en DMZ n'est pas une solution préférable. [20]
Un VPN nous donnera accès à un réseau tandis que le bureau à distance (ou RDP) nous donnera le contrôle d'un ordinateur entier. Les experts en sécurité recommandent d'utiliser un VPN sur une connexion de bureau à distance en raison du niveau d'accès fourni par les connexions d'accès à distance. [21]

3.3.3. Les étapes d'implémentation de la solution proposée

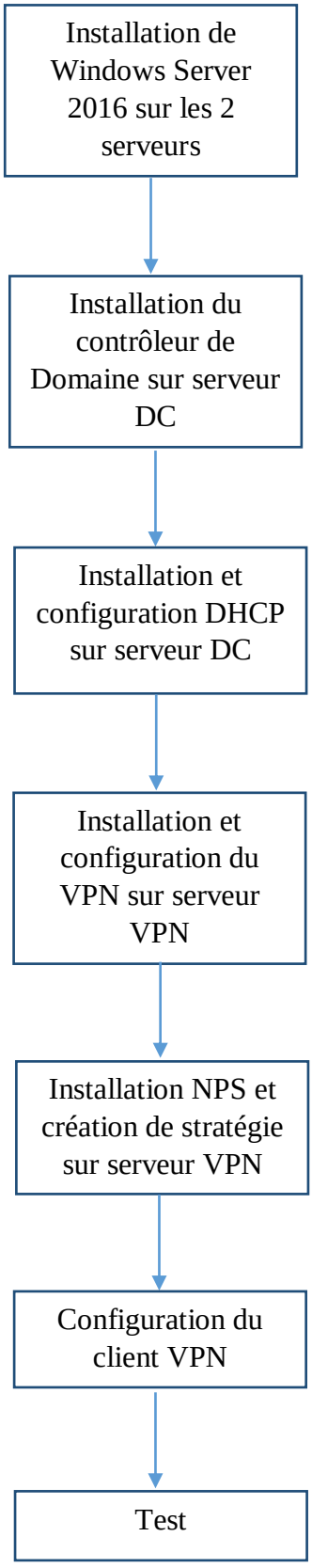

Figure 15 : Les étapes d'implémentation de la solution.

Pour simuler le système nous allons utiliser 2 serveurs dans des machines Virtual Box et pour le client PC avec Windows 8 :

1. Un serveur Active Directory ou le rôle DHCP sera installé nommé Serveur DC
2. Un autre serveur VPN plus le rôle NPS joint à cet Active Directory nommé Serveur VPN.

3.3.3.1. Installation Windows Server 2016

On commence par l'installation de Windows server dans les 2deux machines ***Serveur DC et Serveur VPN***

1. Insérer le support sur le serveur ou monter l'iso dans la MV.

2. Démarrer la machine.

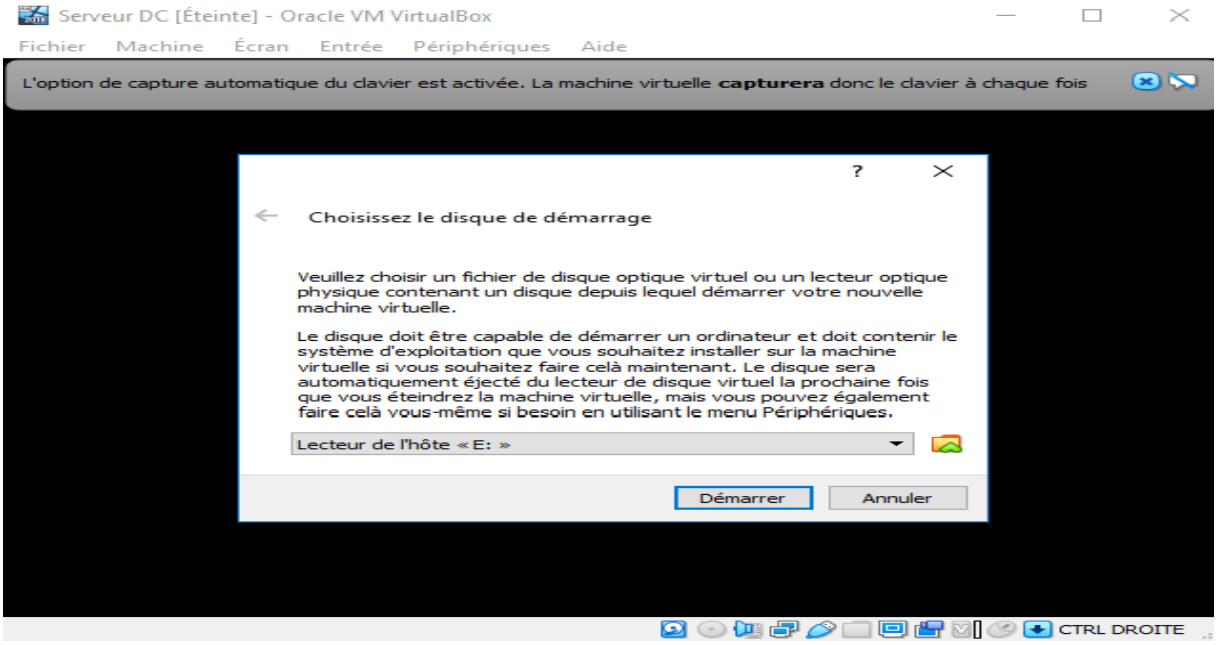

Figure 16 : Monter l'iso dans la VM

3. Premier écran, choisir la langue, le format de l'heure et le type de clavier.

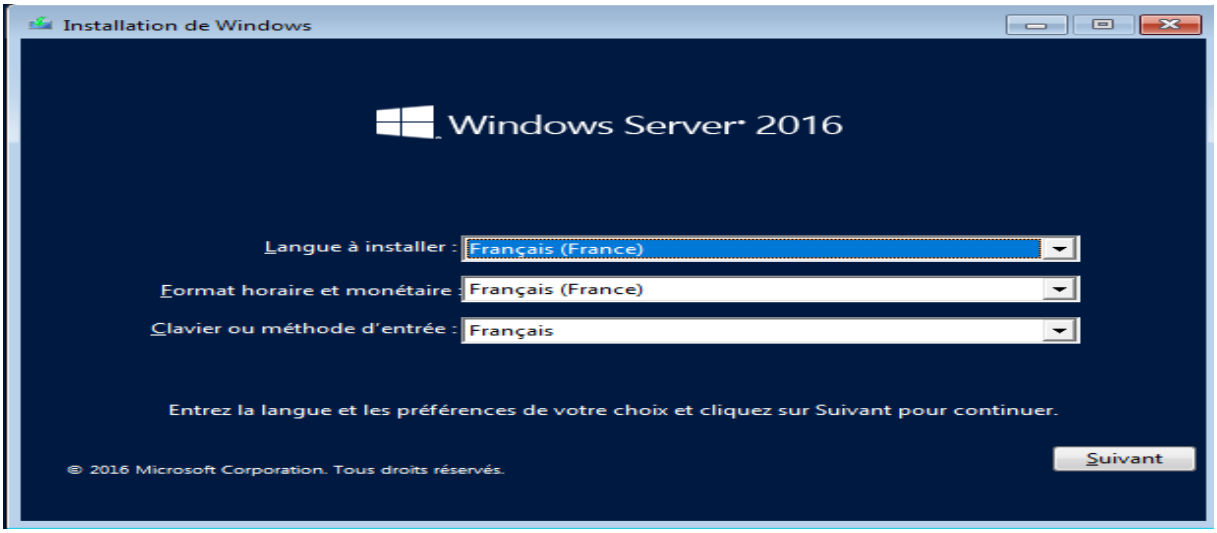

Figure 17 : Étape 1 d'installation Windows Server 2016

4. Cliquer sur Installer maintenant
5. **Indiquer la clé de produit** (numéro de licence) de Windows Server pour activer le système. Pour une version d'évaluation ou pour l'activer plus tard, cliquer sur « **Je n'ai pas de clé de produit (Product Key)** »

6. Choisir l'édition à installer : Windows Server Standard ou Datacenter : selon la licence achetée.« **Expérience utilisateur** » signifie interface graphique

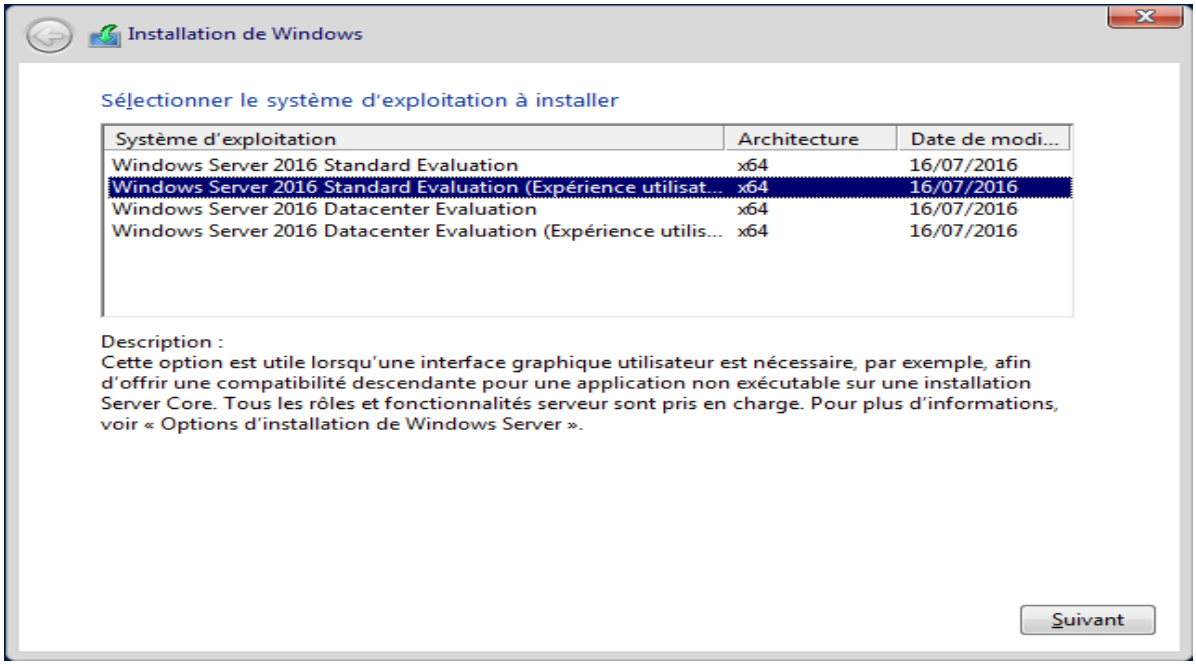

Figure 18 : Choix d'Edition Windows Server 2016

7. Accepter les termes de contrat de licence.

8. Sélectionner le type d'installation Personnalisé pour gérer les disques et partitions.

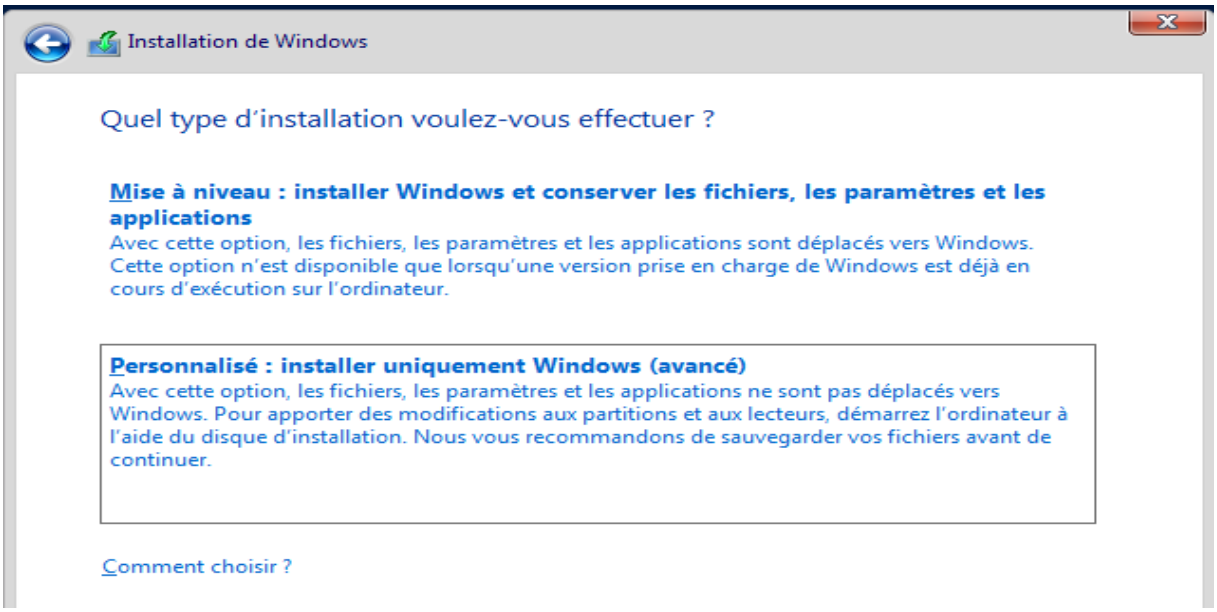

Figure 19: Type installation Windows Server 2016.

9. Choisir le disque dur ou la partition qui sera utilisée.

10. Le programme d'installation démarre et se terminera en demandant un mot de passe pour le compte administrateur.

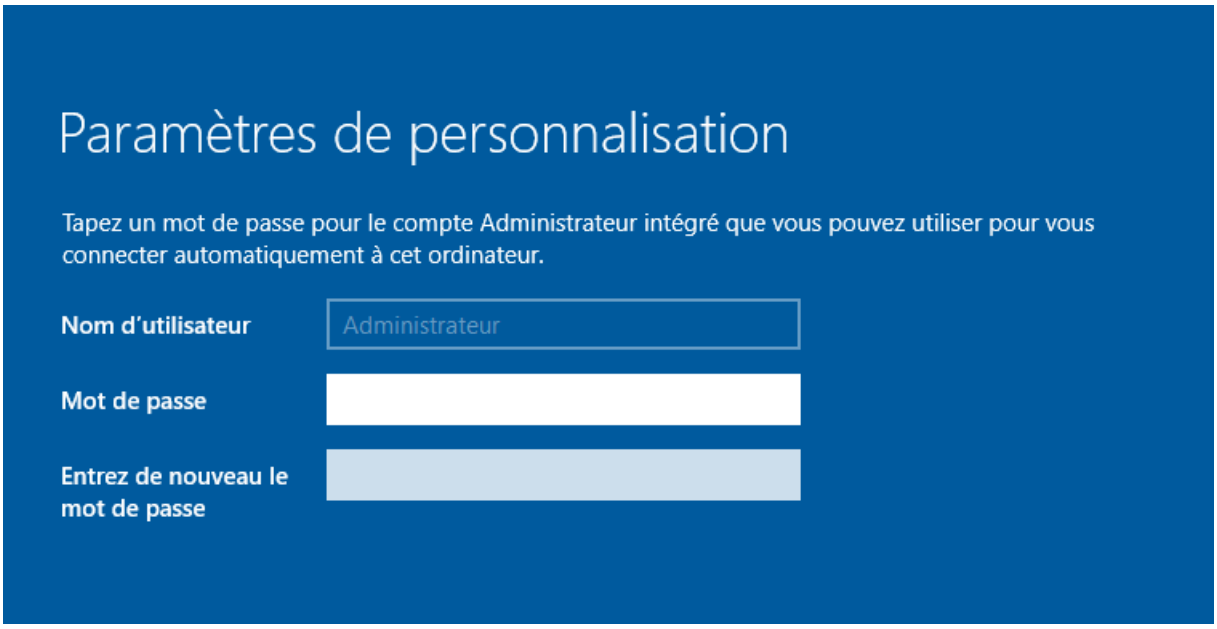

Figure 20 : Mot de passe compte administrateur

Une fois que vous avez choisi un mot de passe, vous vous retrouverez sur le bureau Windows. Le gestionnaire de serveur se lance une fois que vous vous serez connecté.

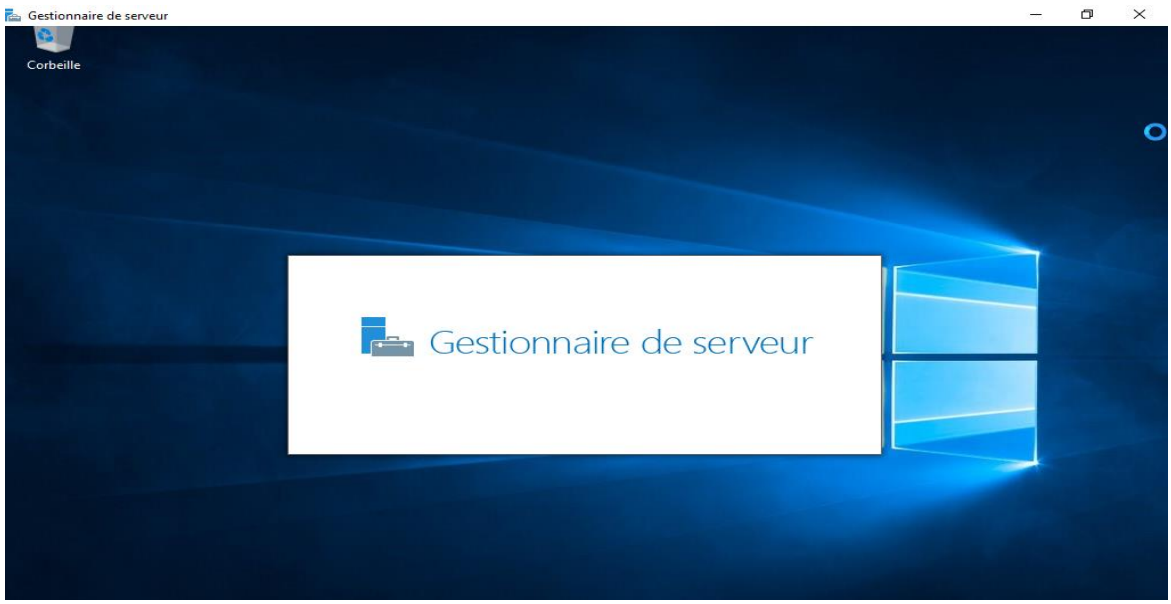

Figure 21 : Gestionnaire de serveur.

On installe le contrôleur de domaine dans la machine Serveur DC

3.3.3.2. Installation du Contrôleur de Domaine

En premier, il est nécessaire de configurer notre serveur en IP Fixe et de l'avoir renommé. Nommer le serveur en fonction de la convention de nommage de notre Domaine(ex : nom de l'organisme).

1. On clique sur « **Configurer ce serveur local** » pour paramétrer les premières informations de la machine :

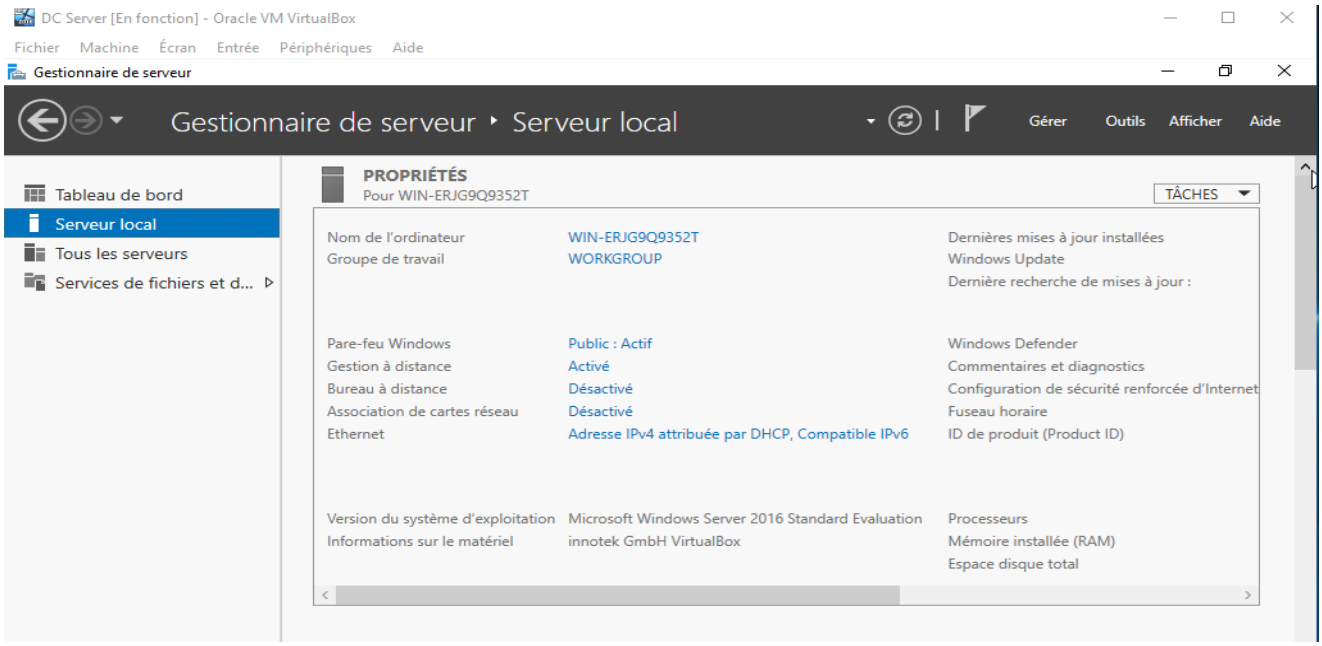

Figure 22 : Propriétés de serveur

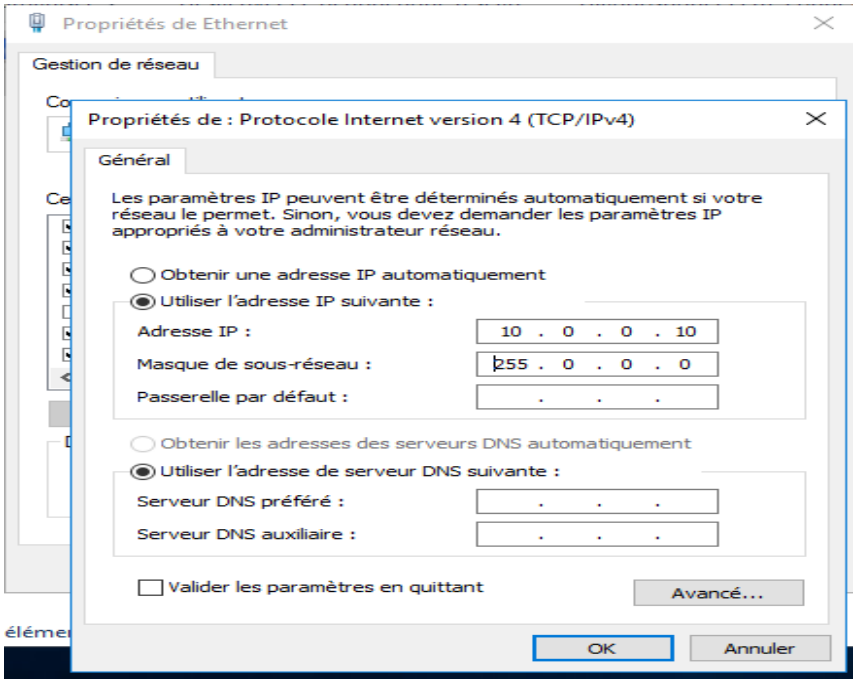

Figure 23 : Adresse IP serveur DC

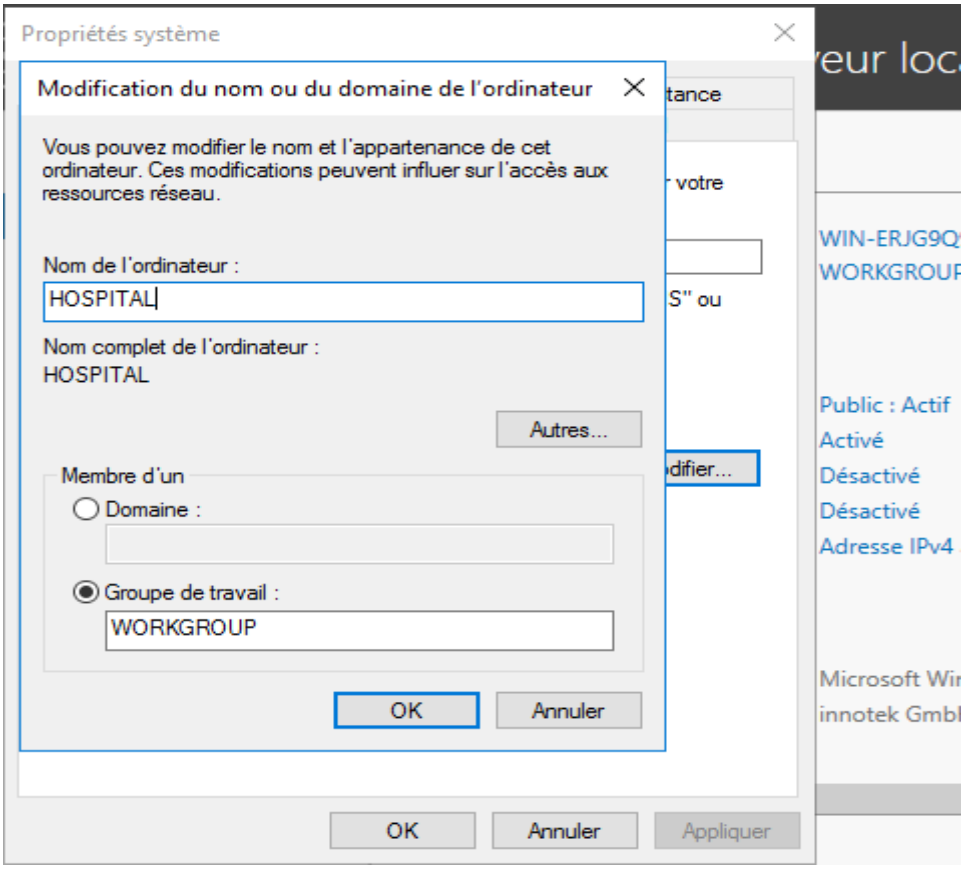

Figure 24 : Nommage de serveur DC

2. On va dans Gérer - › Ajouter des rôles et des fonctionnalités

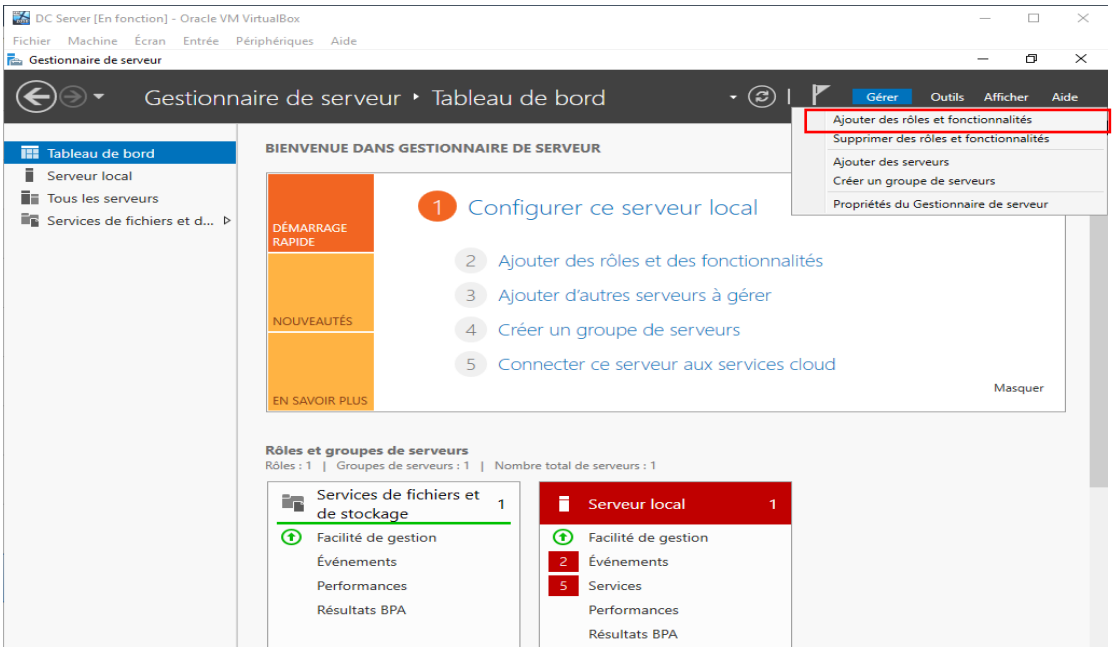

Figure 25 : Ajouter des rôles et des fonctionnalités

3. On sélectionne le type d'installation « **Installation basée sur un rôle ou une fonctionnalité** ».

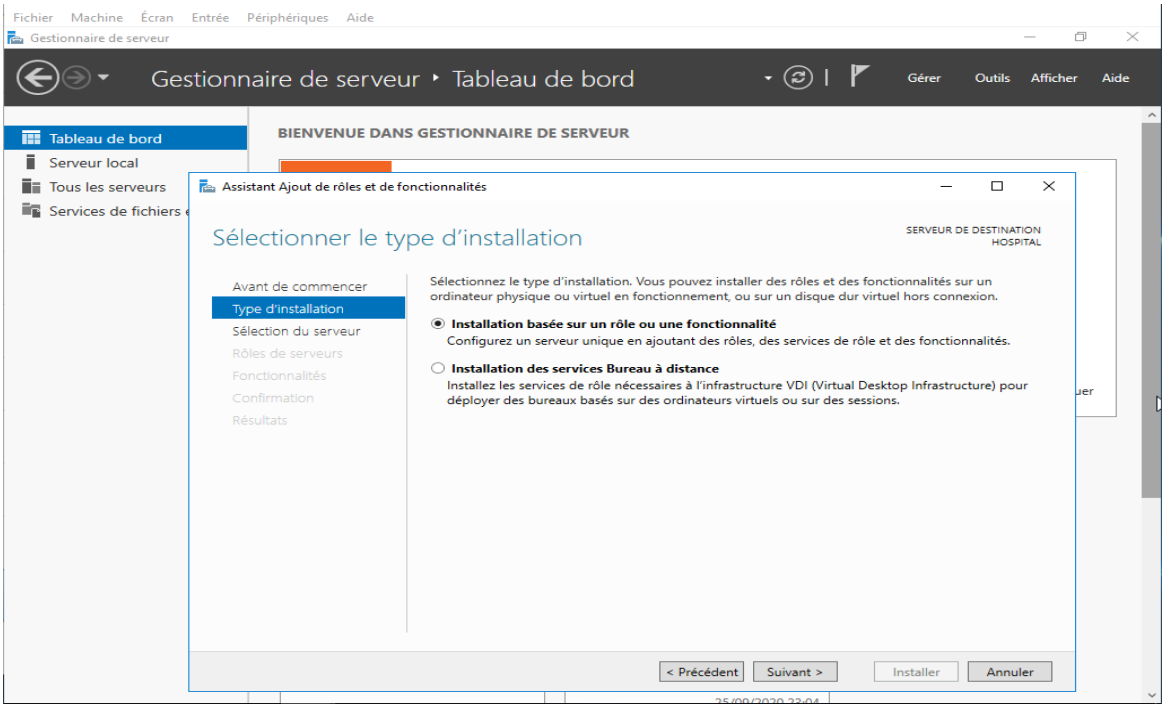

Figure 26 : Lancement d'installation d'AD DS

4. On Sélectionne le serveur et on clique sur **Suivant** :

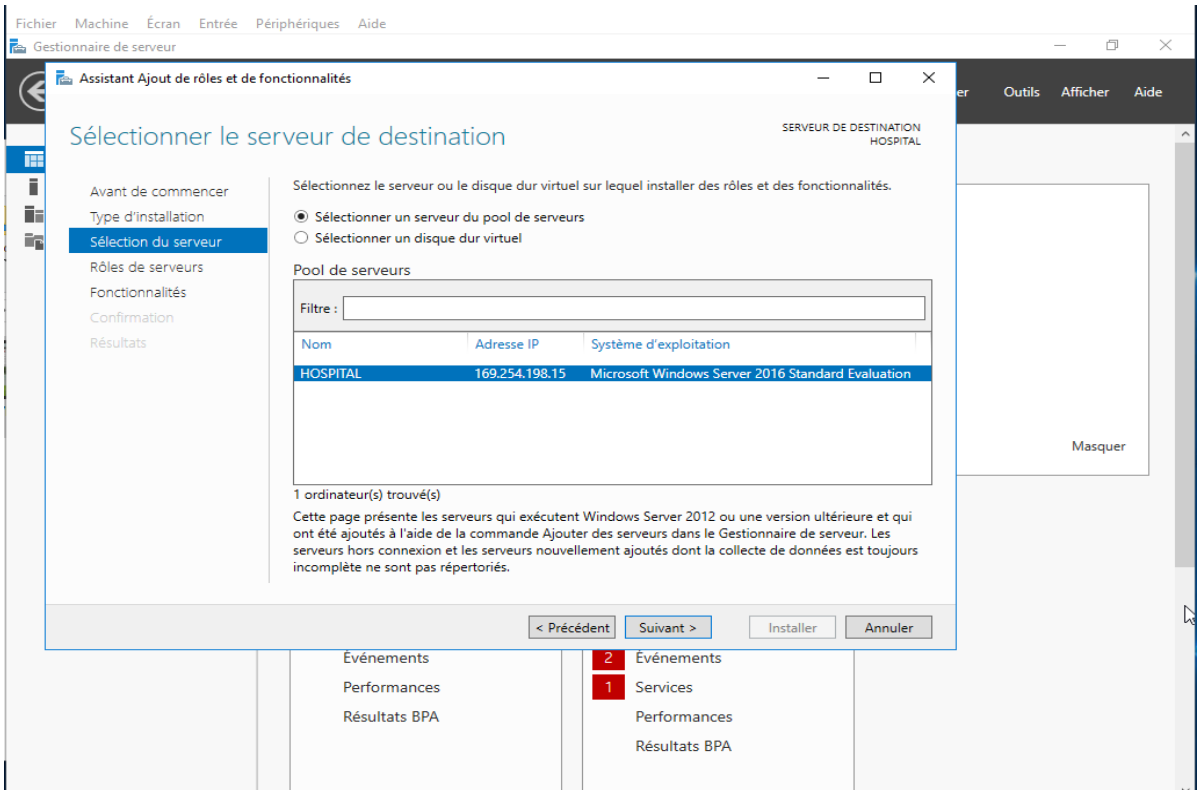

Figure 27 : Choix de serveur AD DS.

5. On clique sur Services de domaine Active Directory « AD DS » puis sur suivant. Ensuite, il nous demande d'ajouter des fonctionnalités supplémentaires. On clique sur ajouter des fonctionnalités:

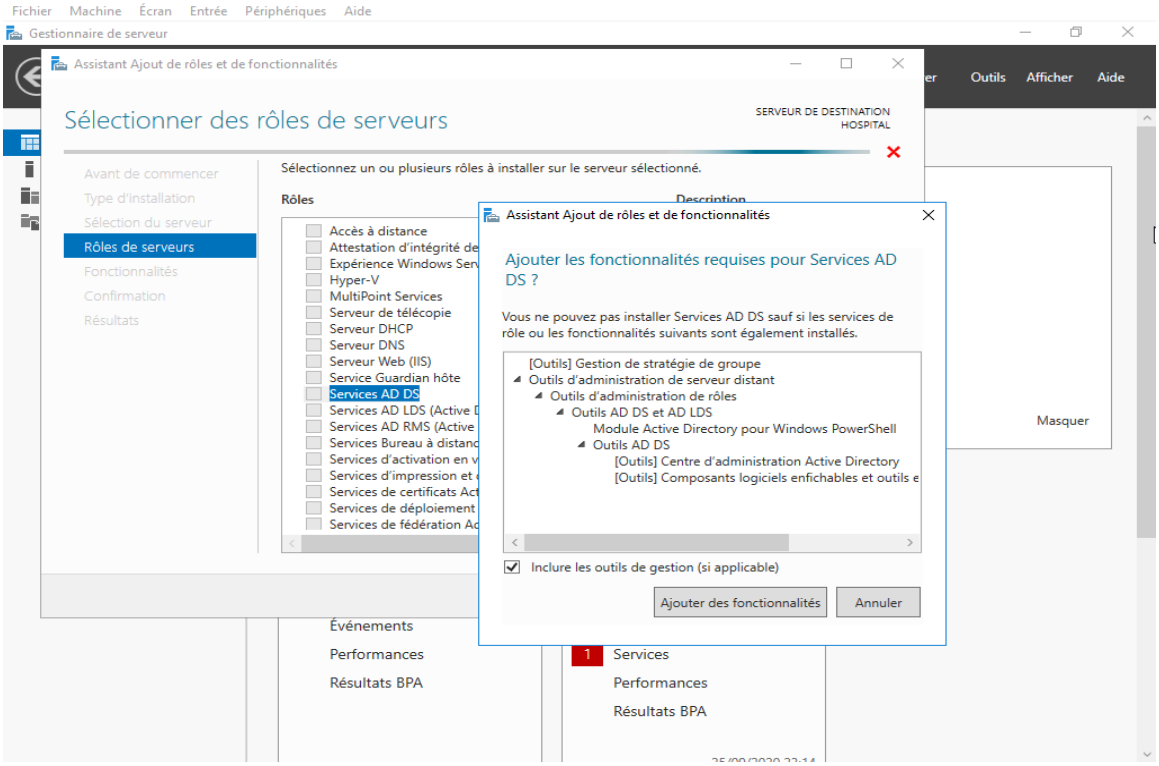

Figure 28 : L'ajout des fonctionnalités d'installation AD DS

6. On clique sur le bouton **Suivant** pour continuer, en général, toutes les caractéristiques qui sont nécessaires pour rôle cible sont déjà sélectionnées :

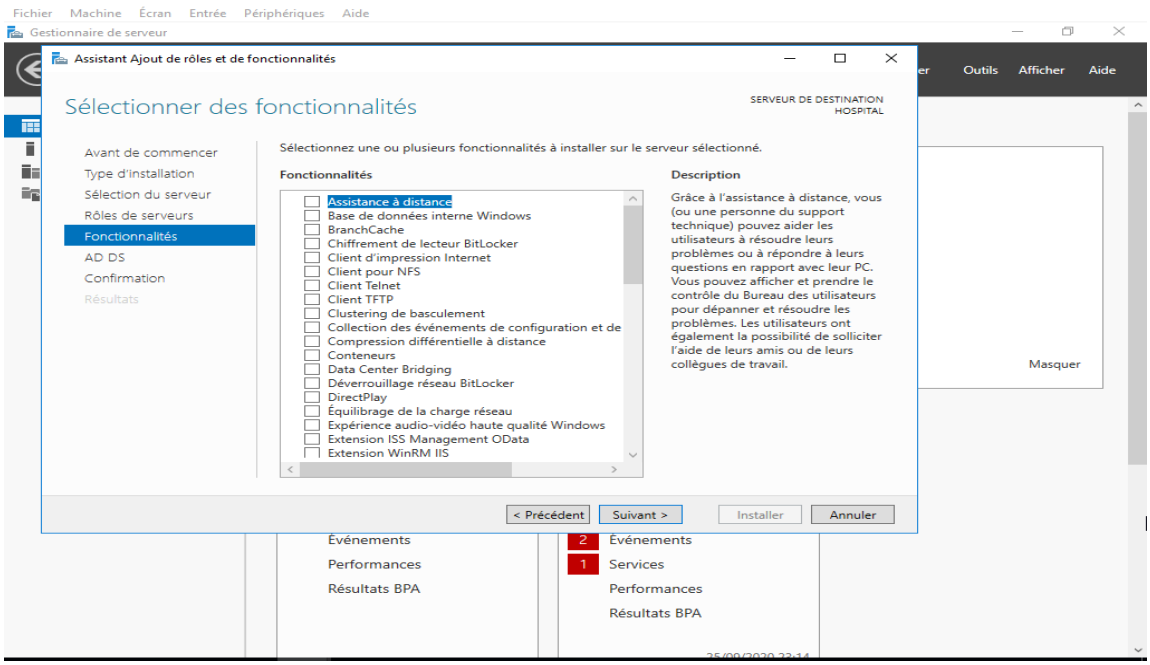

Figure 29 : Sélection des fonctionnalités AD DS.

7. Sur la page de description, on clique sur suivant pour continuer :

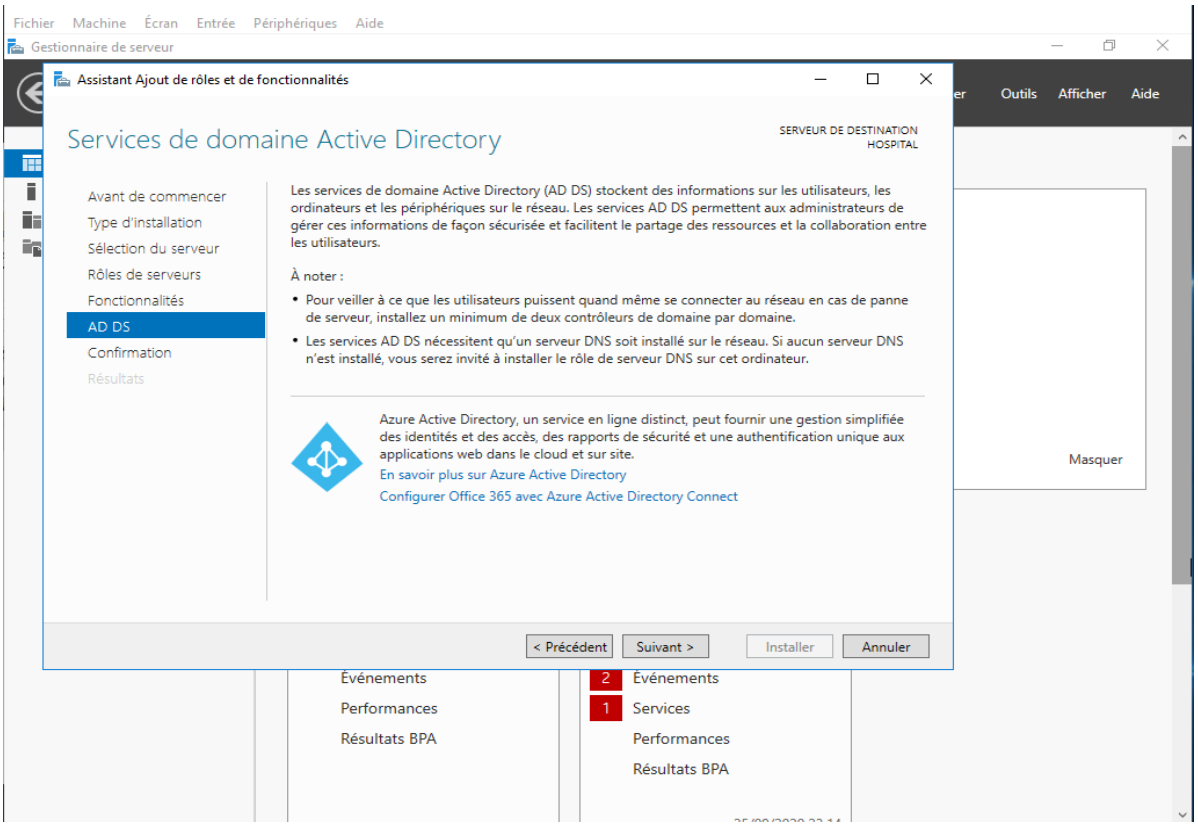

Figure 30 : Description d'AD DS.

8. Sur la page de confirmation, on clique sur installer :

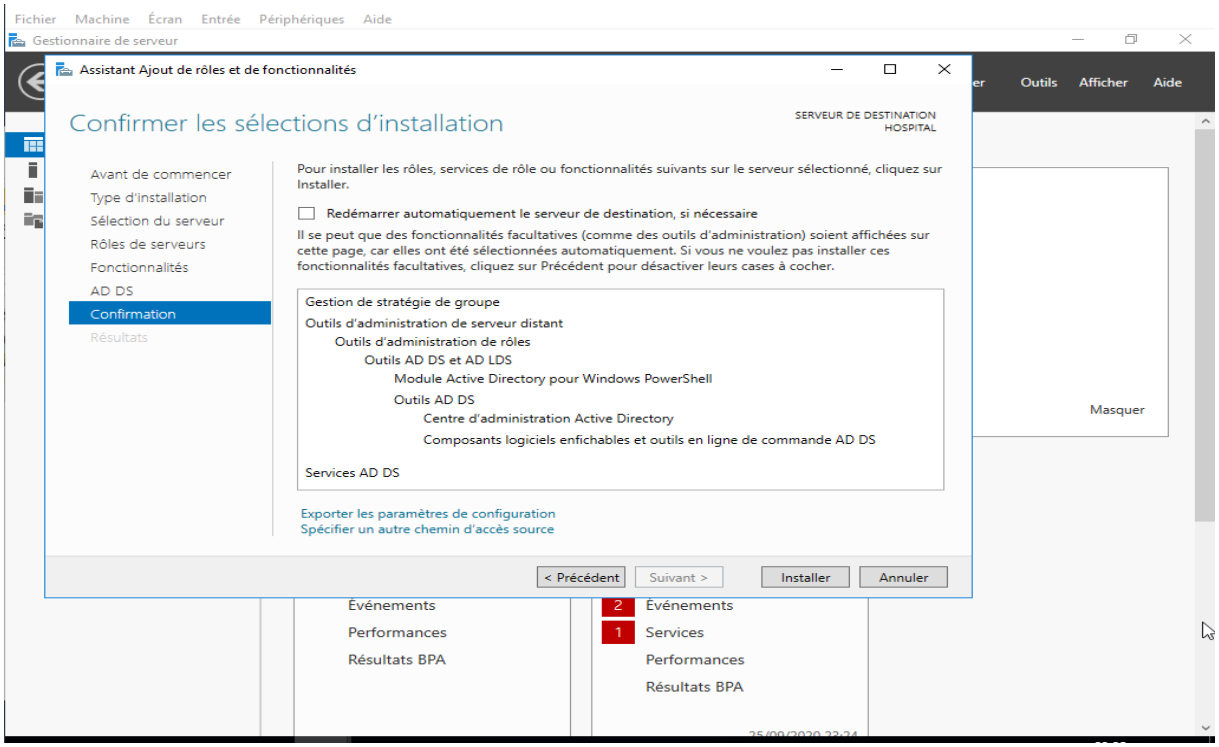

Figure 31 : Confirmation d'installation AD DS.

9. On clique sur Promouvoir ce serveur en contrôleur de domaine :

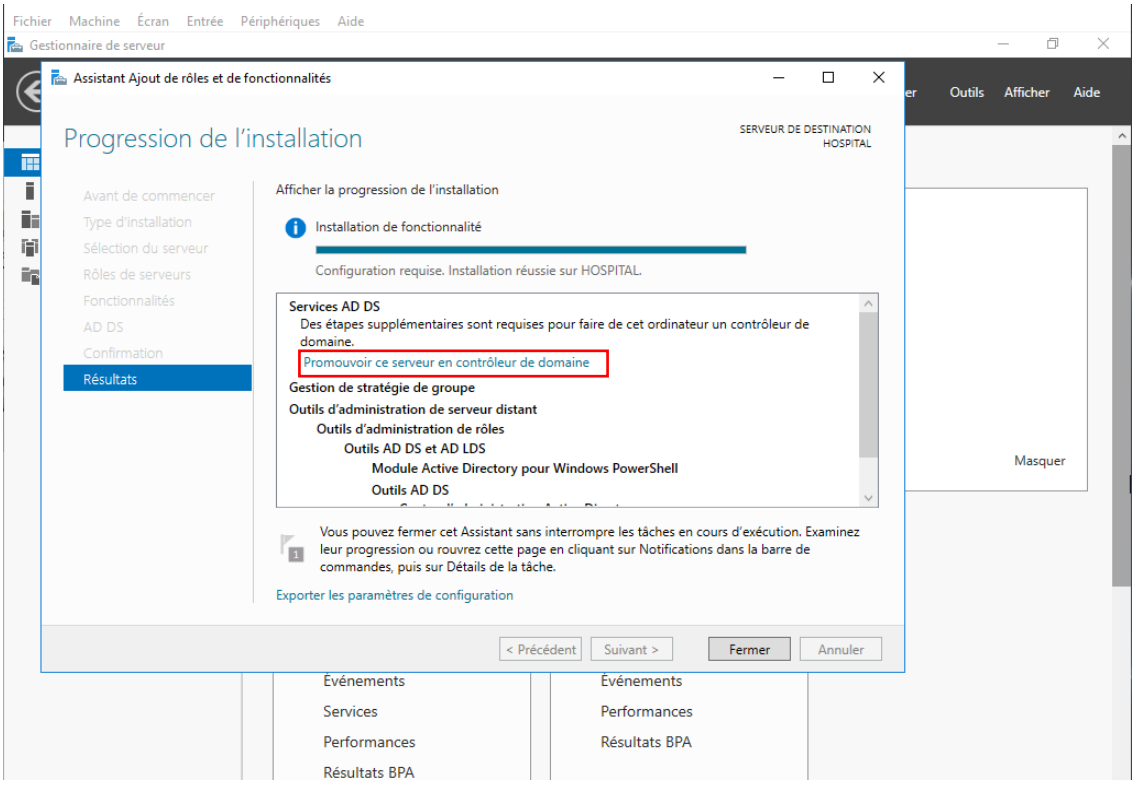

Figure 32 : Fin d'installation AD DS.

10. On déploie une nouvelle forêt dans notre cas « HOSPITAL » :

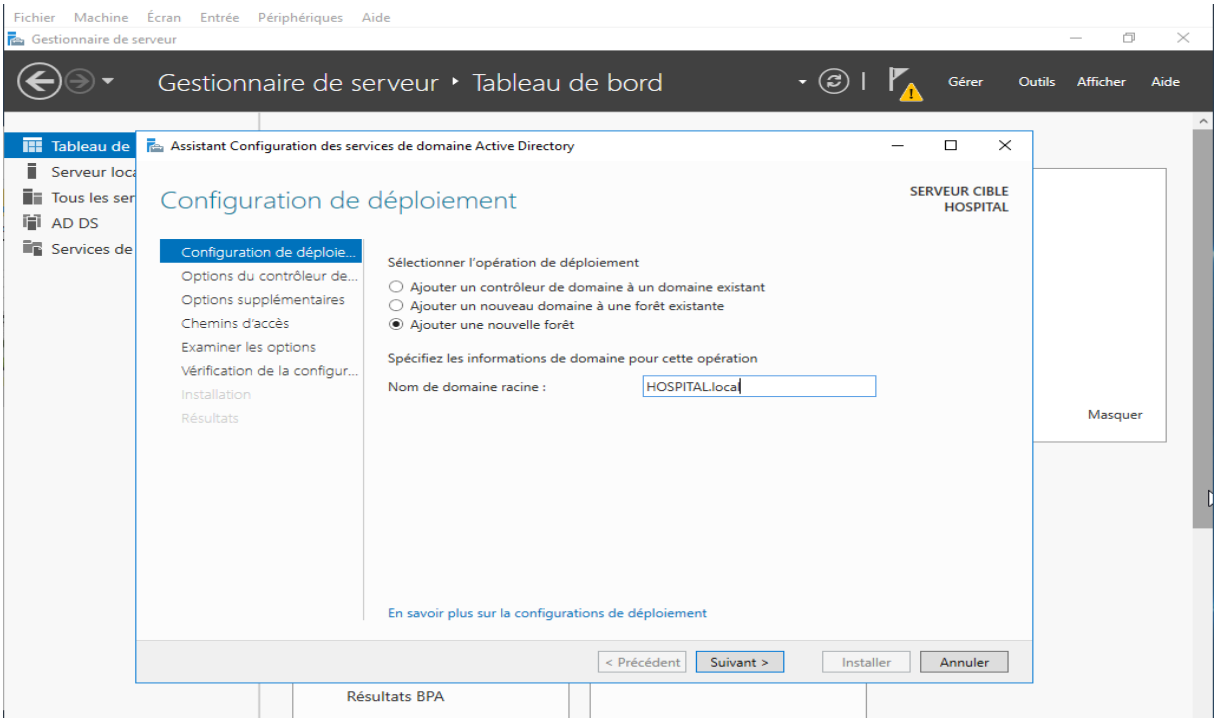

Figure 33 : Création du domaine.

On vient tout juste de créer un nouveau contrôleur de domaine et une nouvelle forêt, on a donc tout intérêt à laisser le niveau fonctionnel en Windows Server 2016. On aurait pu changer le niveau fonctionnel si ce serveur venait intégrer une architecture déjà existante dans un niveau fonctionnel inférieur.

11. On choisir un mot de passe de restauration des services d'annuaire (DSRM) **:**

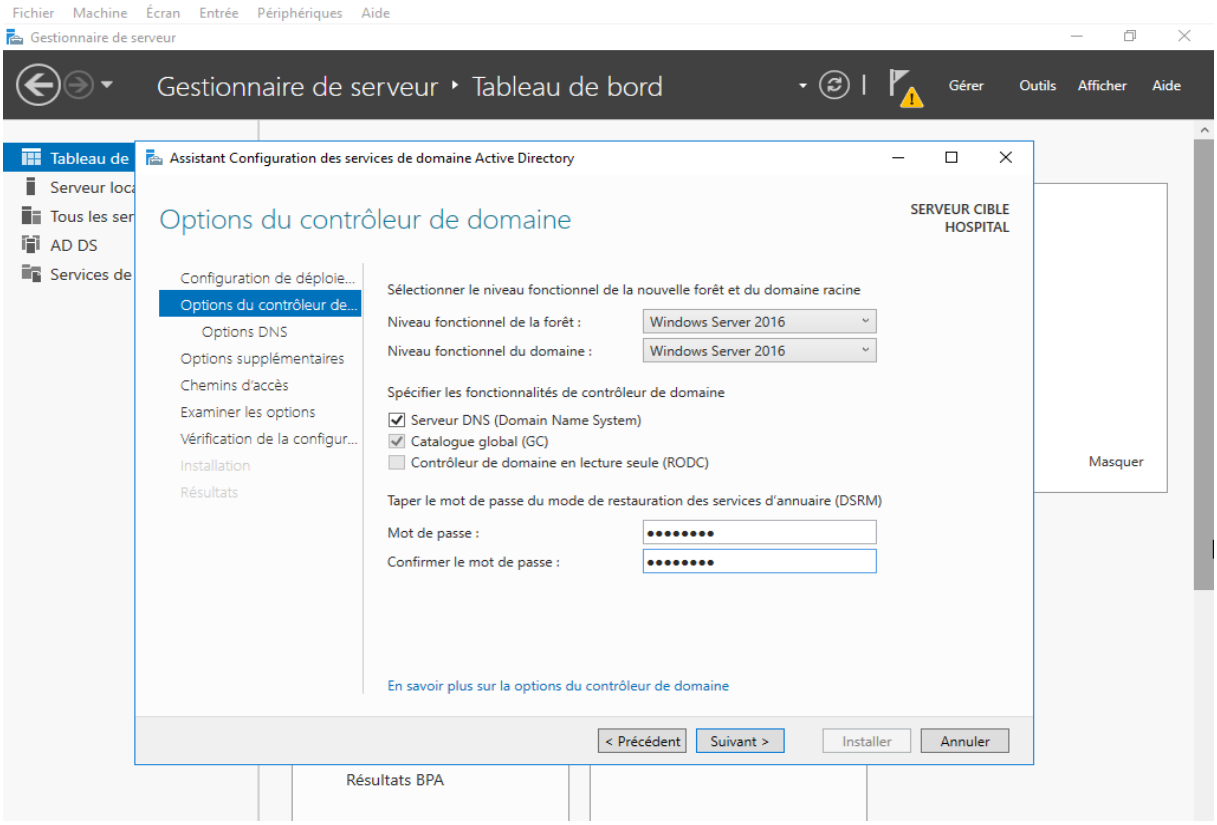

Figure 34 : Mot de passe de restauration.

Le mode de restauration des services d'annuaires (DSRM) est une option de démarrage en mode sans échec pour les contrôleurs de domaine Windows Server. Ce mot de passe fournit à l'administrateur une porte débordée vers la base de données en cas de problème plus tard, mais il ne donne pas accès au domaine ni à aucun service.

12. On peut créer une délégation DNS, ici, on n'a pas d'autres serveurs DNS dans ce domaine, il est donc logique d'avoir cet avertissement. On clique sur Suivant :

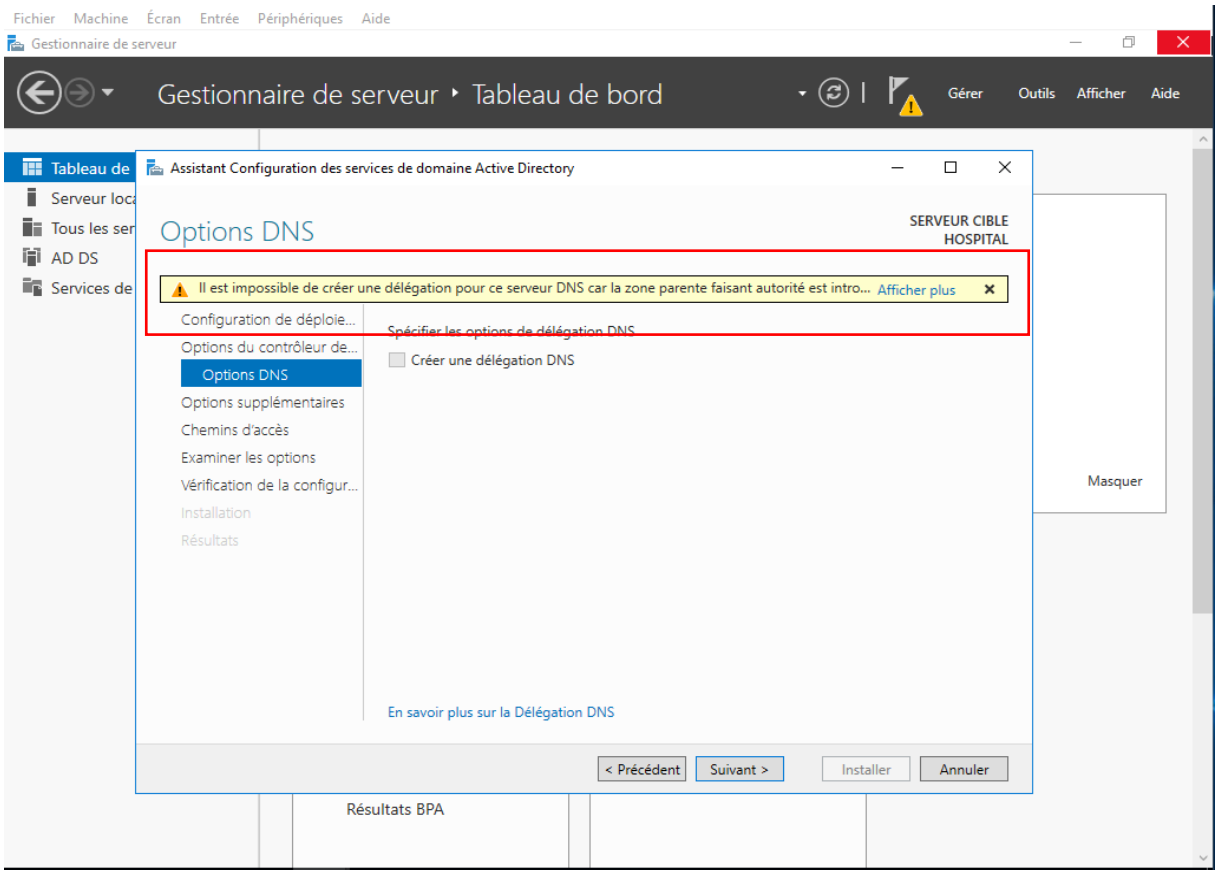

Figure 35 : Délégation DNS

13. Le NetBIOS sera automatiquement créé, on clique sur Suivant pour continuer :

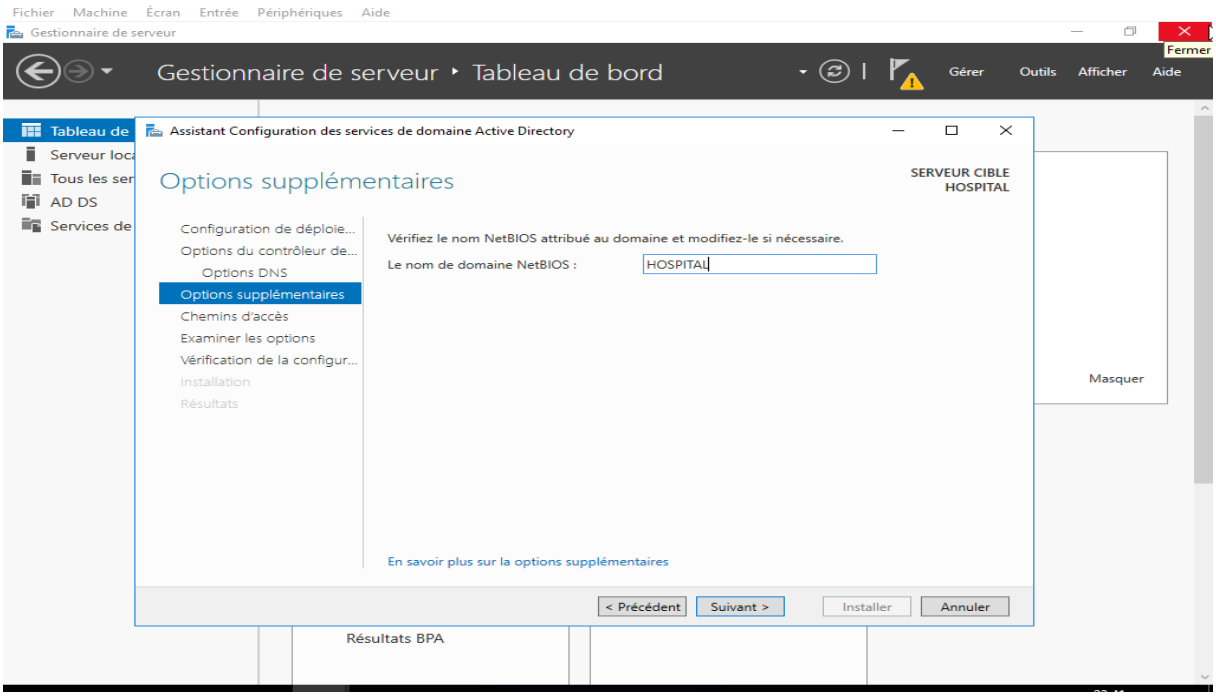

Figure 36 : Nom de domaine NetBios.

14. On clique sur Suivant pour continuer :

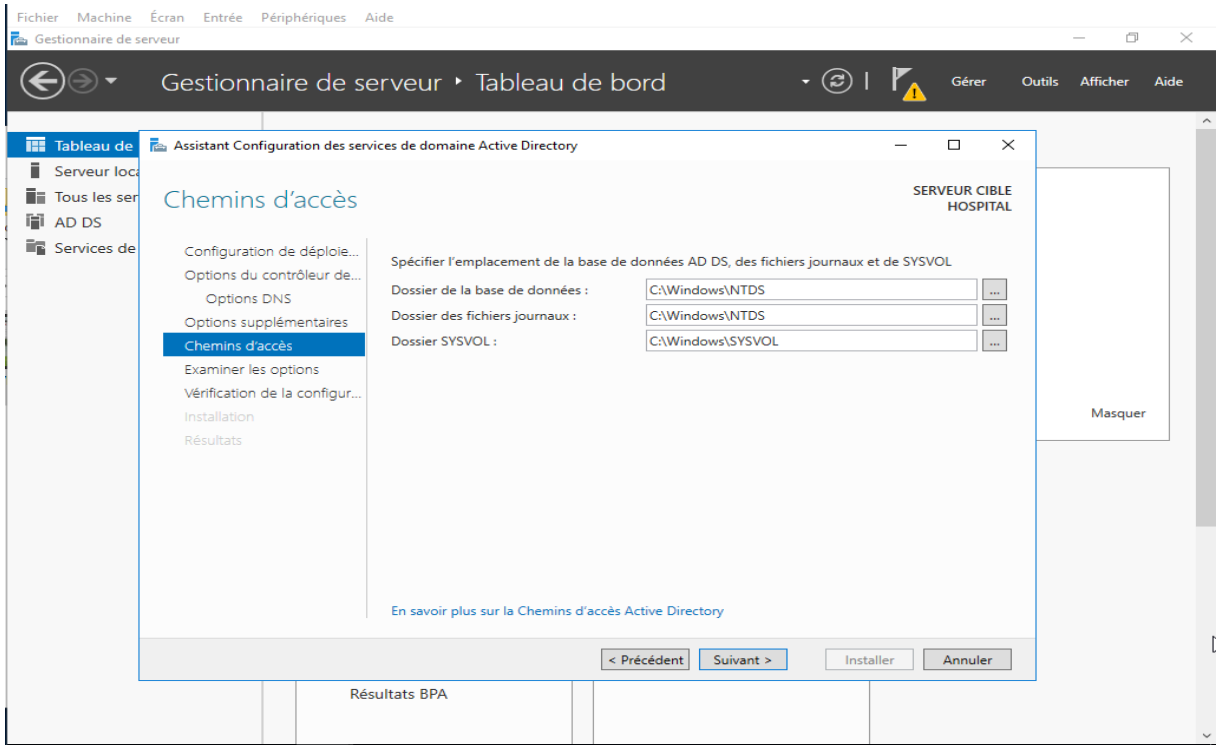

Figure 37 : Emplacement des fichiers.

On rappelle qu'Active Directory est le regroupement d'une base de données et de fichiers journaux. Si on le souhaite, on peut ici changer le chemin de la BDD, des logs ou encore de SYSVOL.

15. On clique sur suivant :

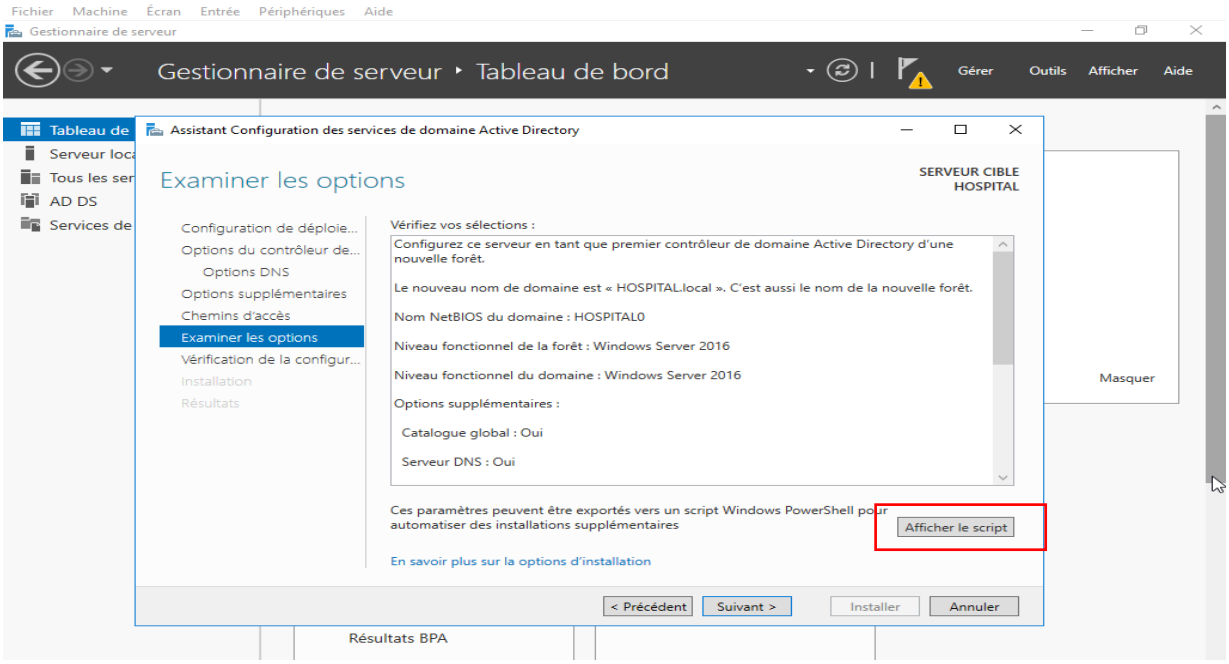

Figure 38 : Configuration en script.

On a la possibilité de revoir la configuration. En prime, lorsque on clique sur le bouton Afficher le script, le script PowerShell nous est fourni pour automatiser les futures installations.

16. On clique sur Installer pour enfin lancer l'installation du contrôleur de domaine :

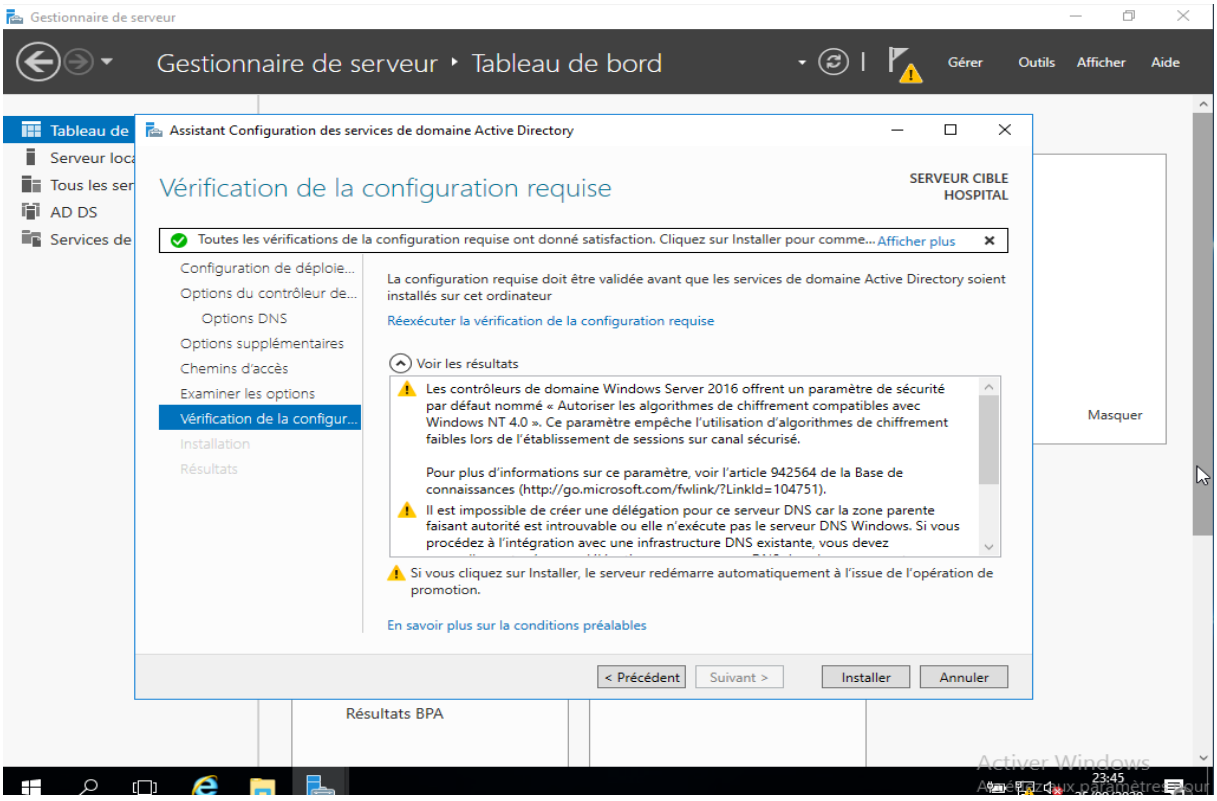

Figure 39 : Installation du Domain.

17. IL redémarre automatiquement le serveur une fois terminé.

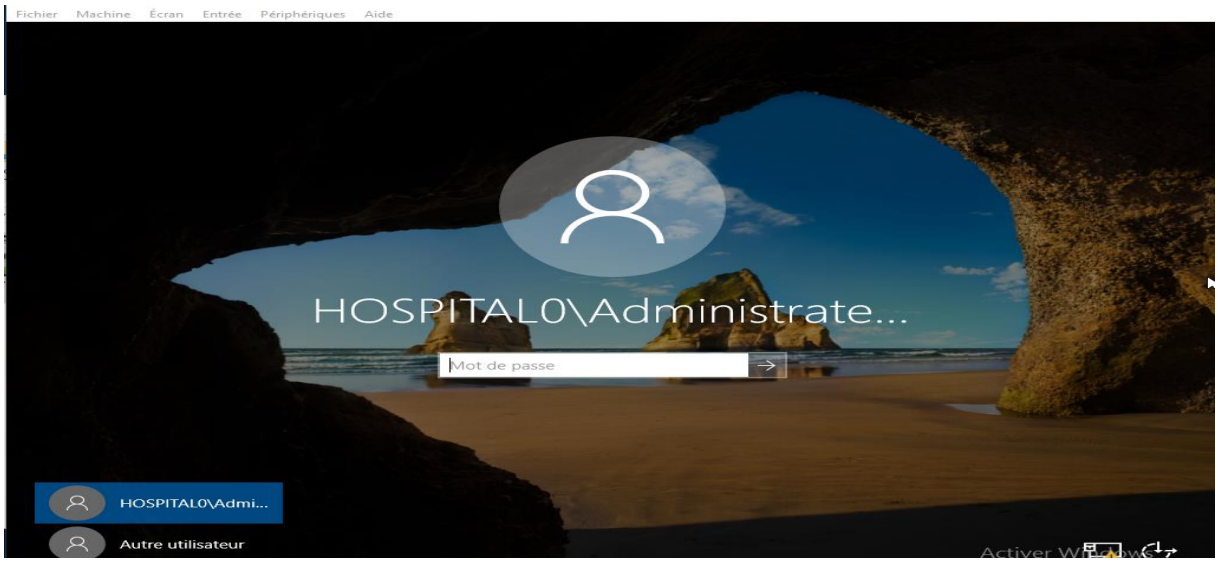

Figure 40 : Fin d'installation d'AD DS.

Maintenant que notre serveur est promu comme Contrôleur de Domaine, On voie les rôles ADDS & DNS sur le Gestionnaire de serveur :

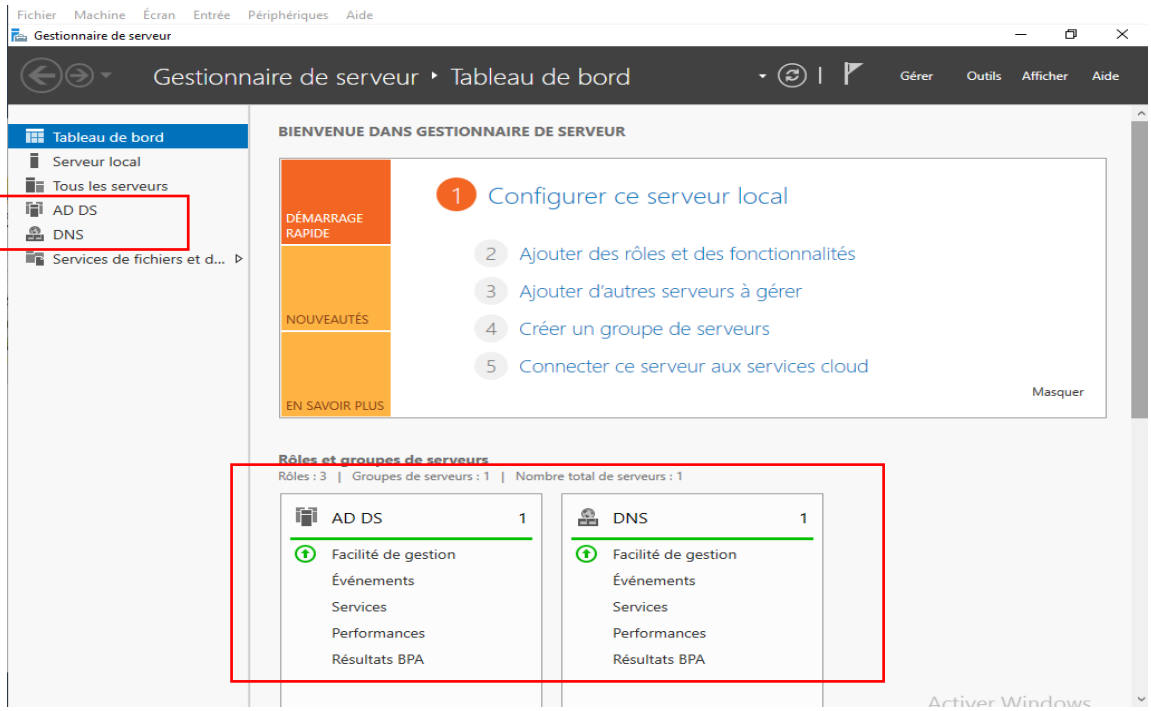

Figure 41 : Serveur DNS et AD DS

Un serveur DNS est automatiquement créé lors de l'installation d'une nouvelle forêt. Le DNS sert à résoudre les adresses IP en nom et inversement et permet aussi au réseau de pouvoir sortir sur internet grâce à des redirecteurs conditionnels.

3.3.3.3. Installation et configuration du DHCP

Pour la suite de l'implémentation, on requit la configuration réseau suivante :

Serveur DC :

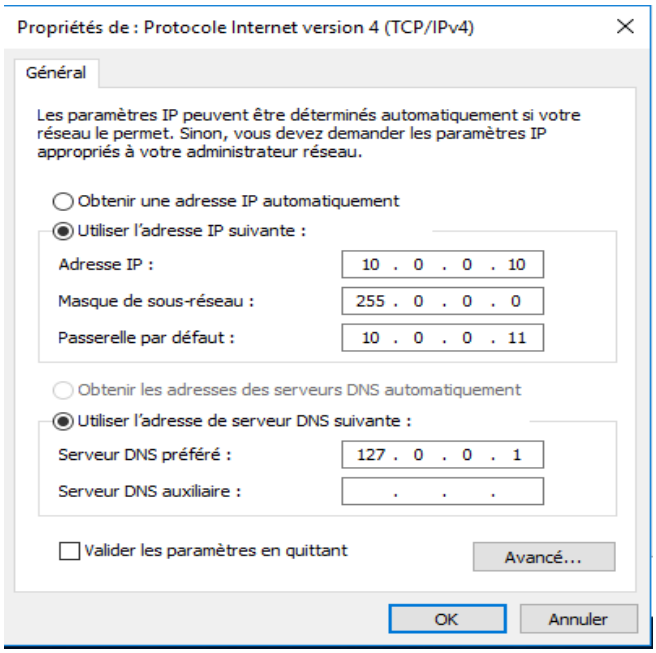

Figure 42 : Adresse IP de serveur DC.

Serveur VPN : ce serveur possède 2 cartes réseau

- La carte réseau LAN pour le réseau interne,
- La carte réseau WAN connecté à internet.

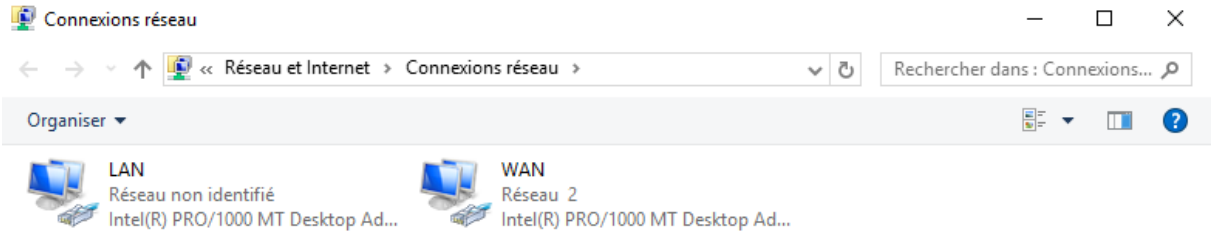

Figure 43 : Cartes réseau de serveur VPN.

Carte LAN :

Pas de passerelle et pour le DNS on utilise celui qui a été automatiquement installé lors de l'installation de l'Active Directory.

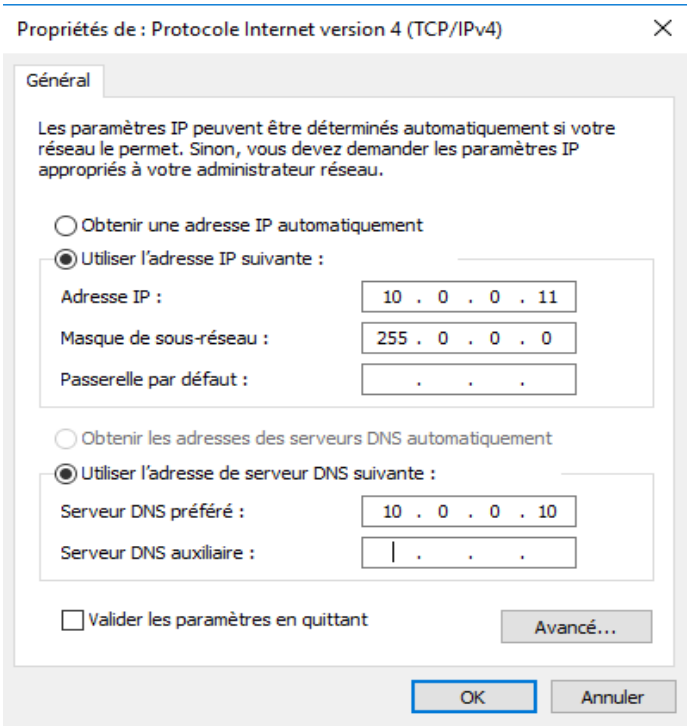

Figure 44 : Adresse IP LAN.

Carte WAN :

Notre routeur distribue des adresse IP du type : 192.168.X.X donc on a choisi une adresse IP de 192.168.1.10, la passerelle correspond à l'adresse IP de notre routeur : 192.168.1.1 et le DNS on utilise qui se trouve dans notre routeur ainsi que ceux de Google.

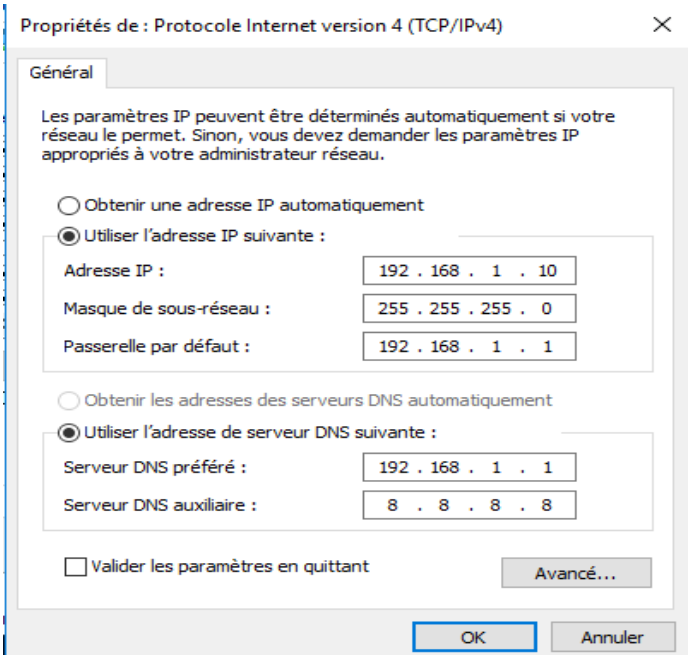

Figure 45 : Adresse IP WAN.

Installation du DHCP sur le serveur DC qui servira a distribué des adresses IP de type 10.0.0.X

1. À partir du Gestionnaire de serveur→ **ajoutez des rôles et des fonctionnalités.**

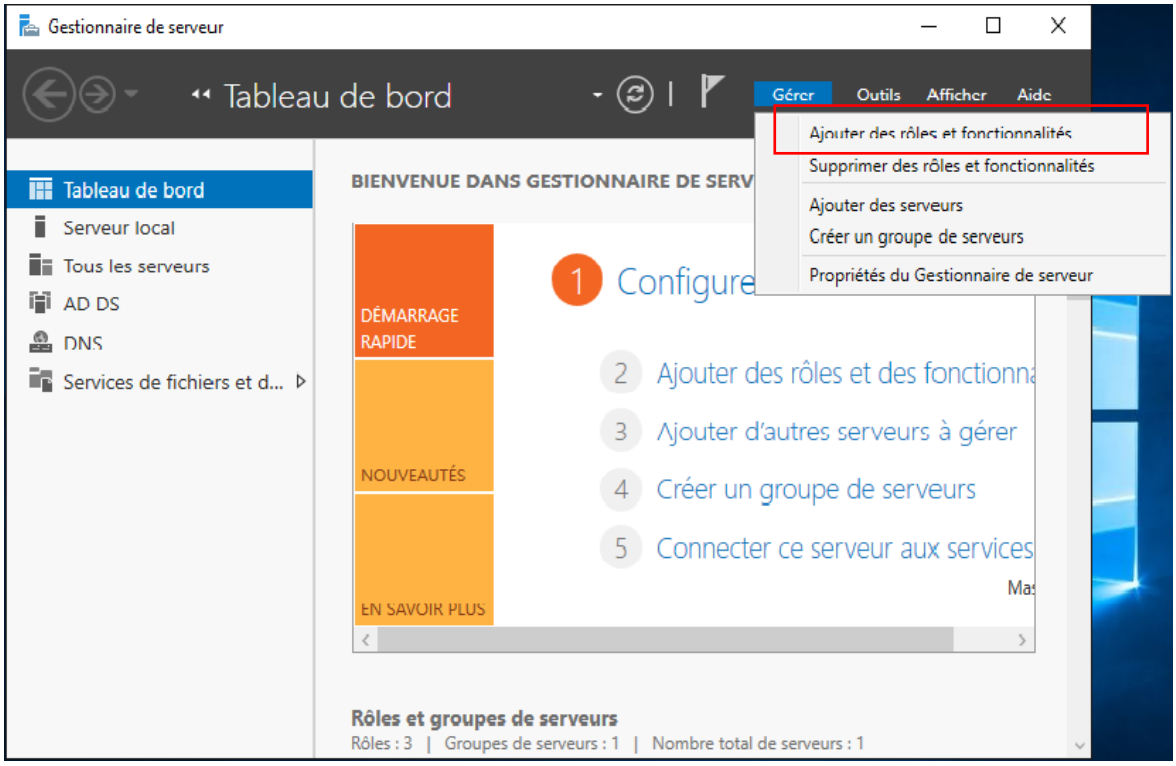

Figure 46: Ajouter le rôle de DHCP.

2. On sélectionne **Installation basée** sur les **rôles ou les fonctionnalités** et on clique suivant

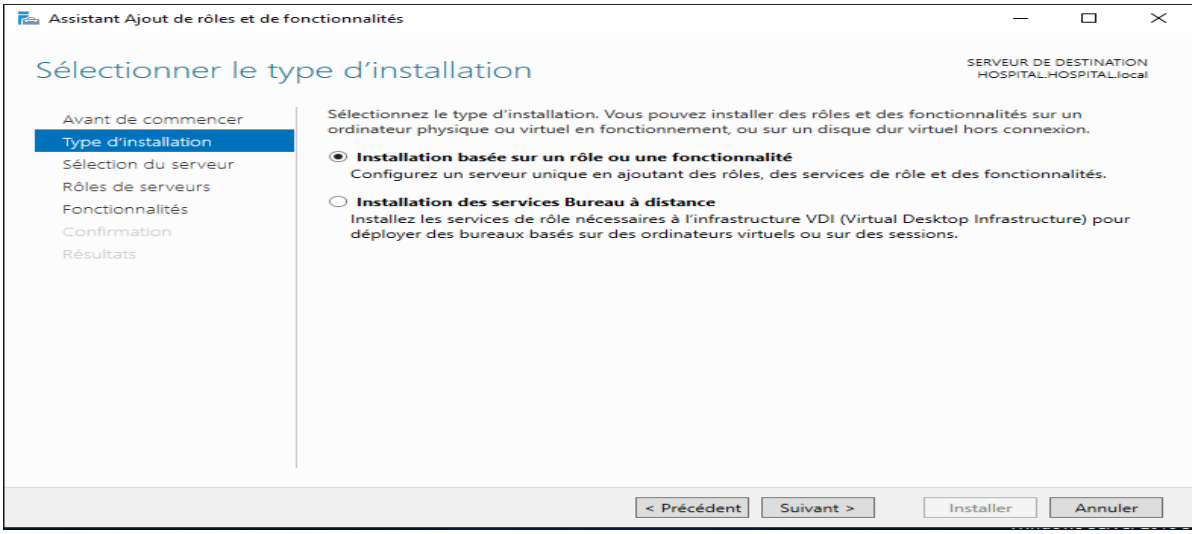

Figure 47 : Type d'installation DHCP.

3. On sélection le serveur :

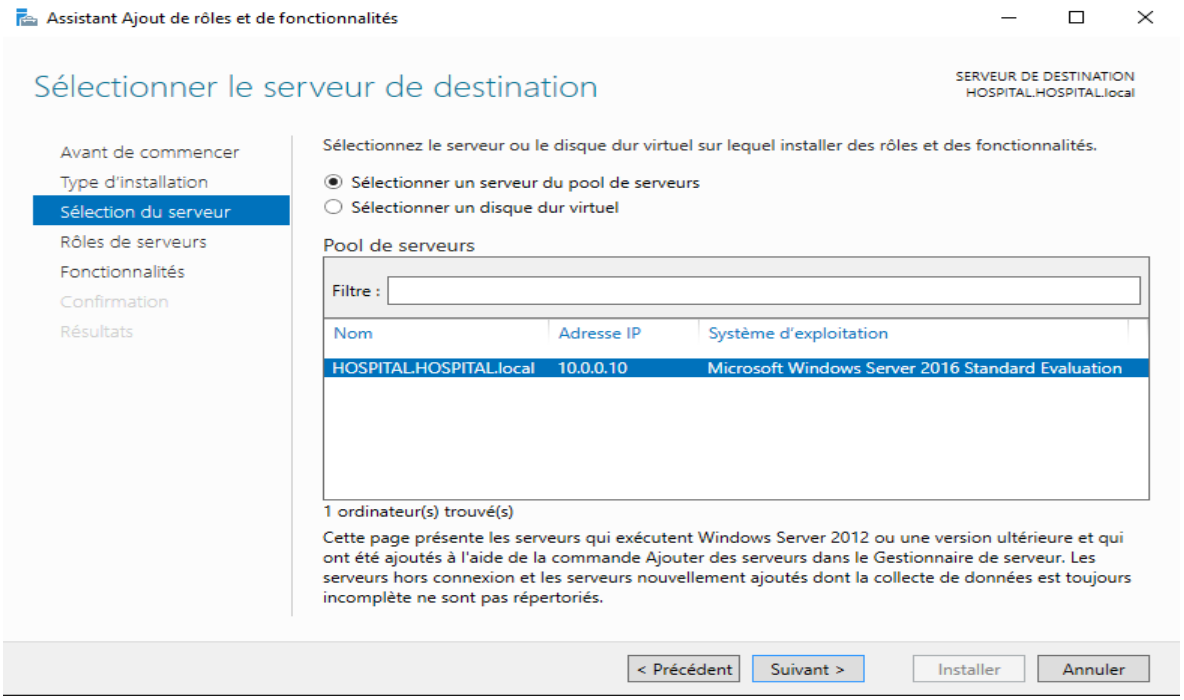

Figure 48 : Sélection du serveur DHCP.

4. Ensuite, sur les rôles de serveur de sélection, on clique sur le bouton **DHCP** et on clique sur suivant pour continuer.

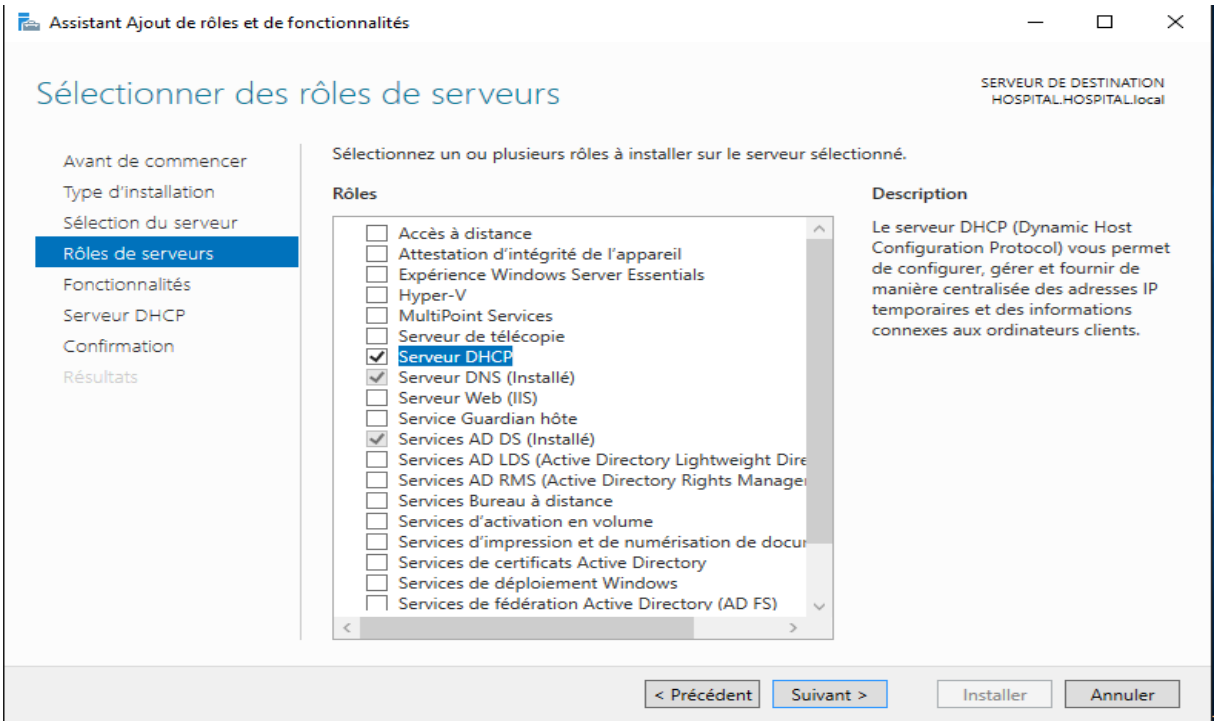

Figure 49 : Sélection du rôle DHCP.

5. Sur l'écran de sélection de la fonctionnalité**,** on clique sur Suivant

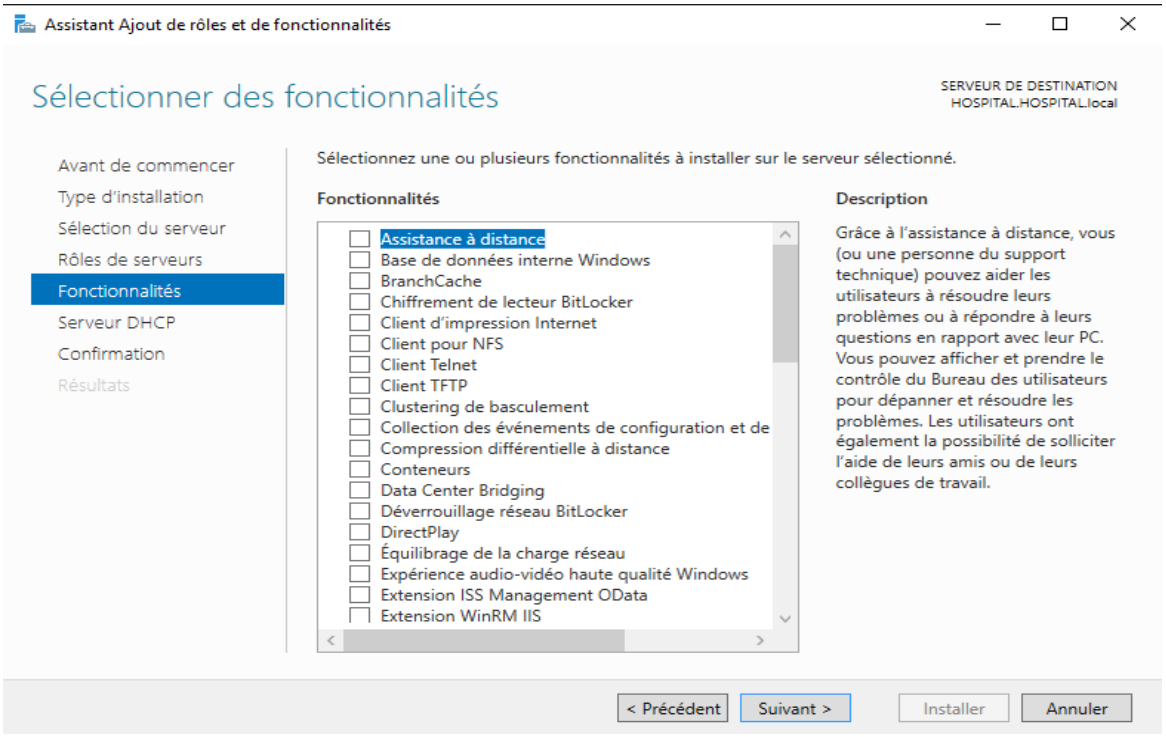

Figure 50 : Ajout des fonctionnalités DHCP.

6. Sur l'écran du serveur DHCP, on clique sur suivant pour continuer

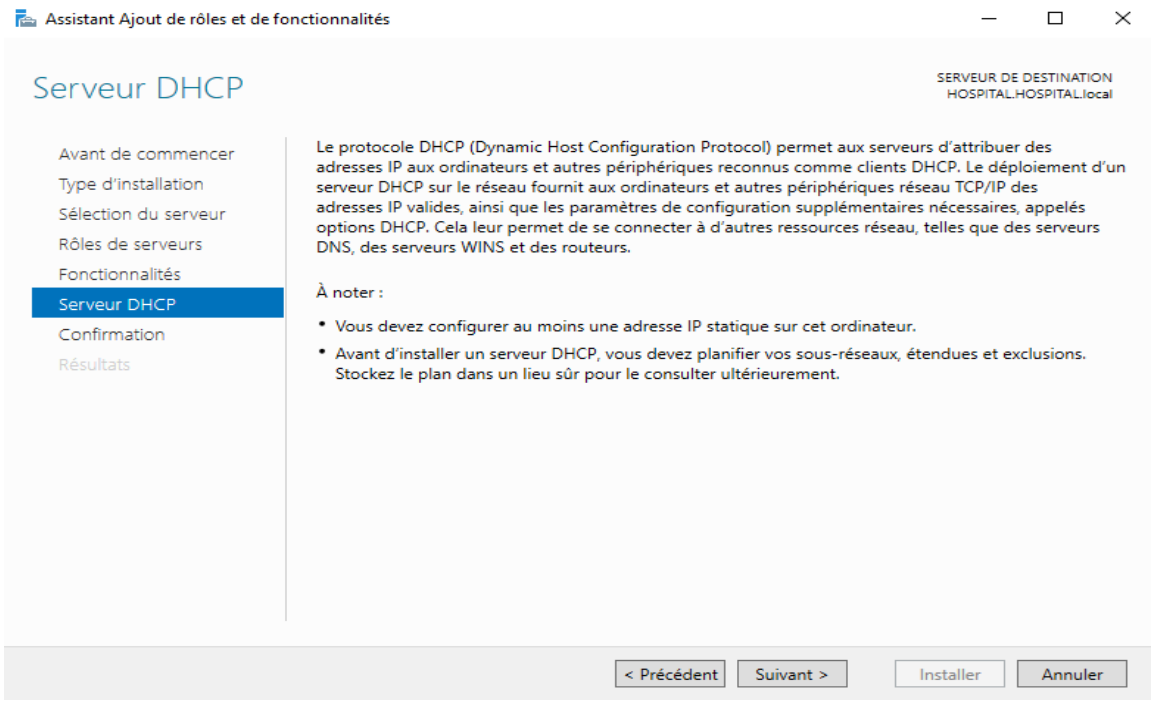

Figure 51 : Description de DHCP.

7. On clique sur Installer

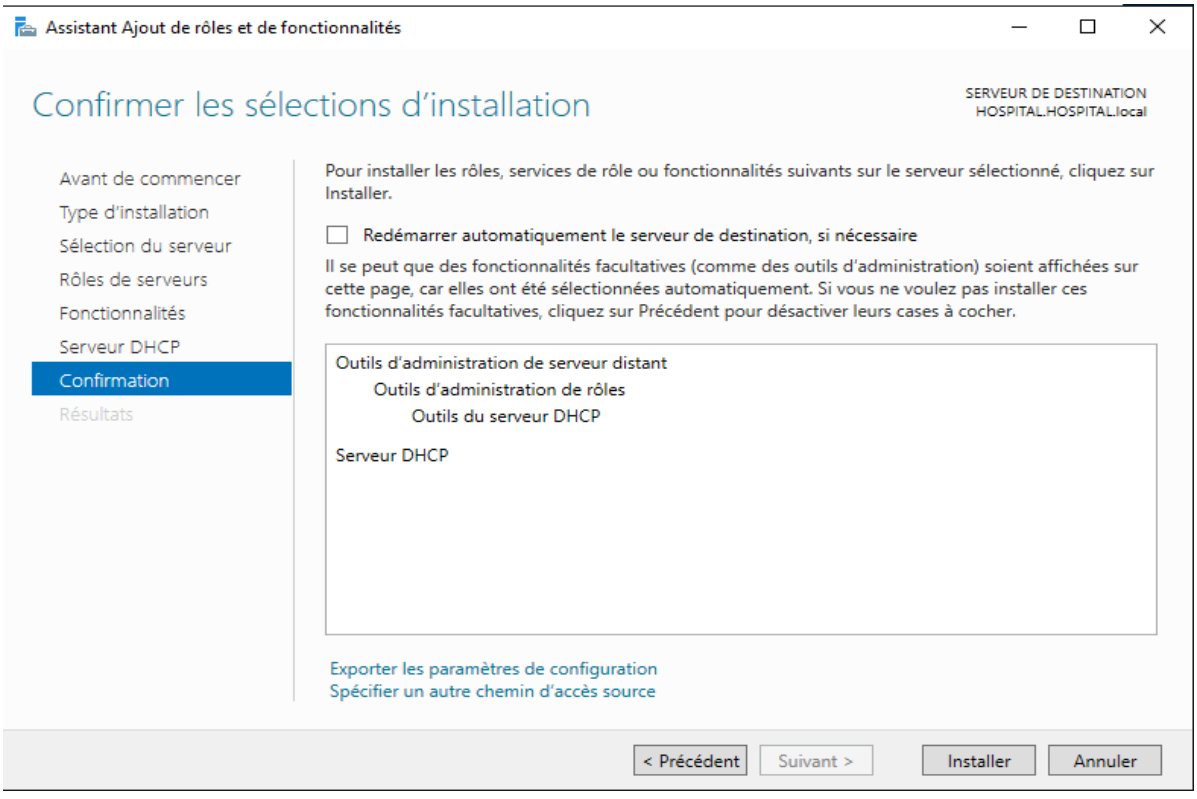

Figure 52 : Confirmer l'installation DHCP.

8. On attend la réussite de l'installation et on clique sur le bouton Fermer.

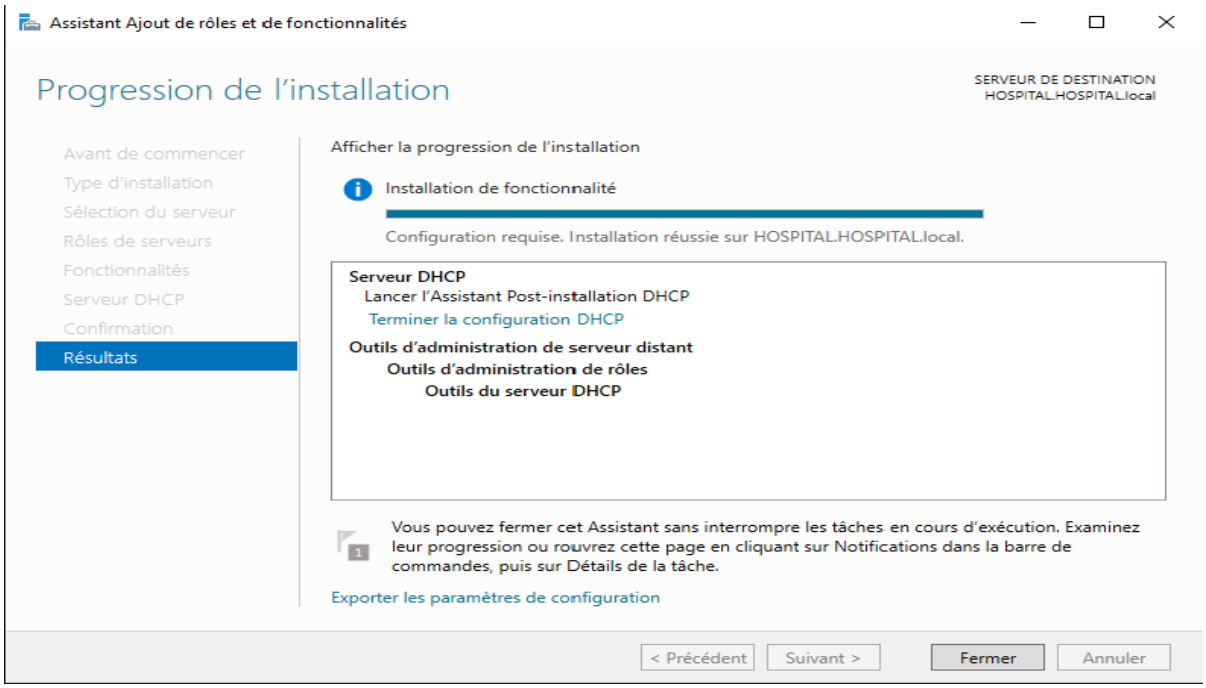

Figure 53 : Installation DHCP terminer.

9. Cliquez sur Terminer la configuration DHCP.

Maintenant on doit fournir un compte disposant de l'autorisation requise dans AD pour autoriser les serveurs DHCP. On peut utiliser un compte connecté (dans notre cas, l'administrateur du domaine) ou fournir un autre compte disposant des autorisations requises.

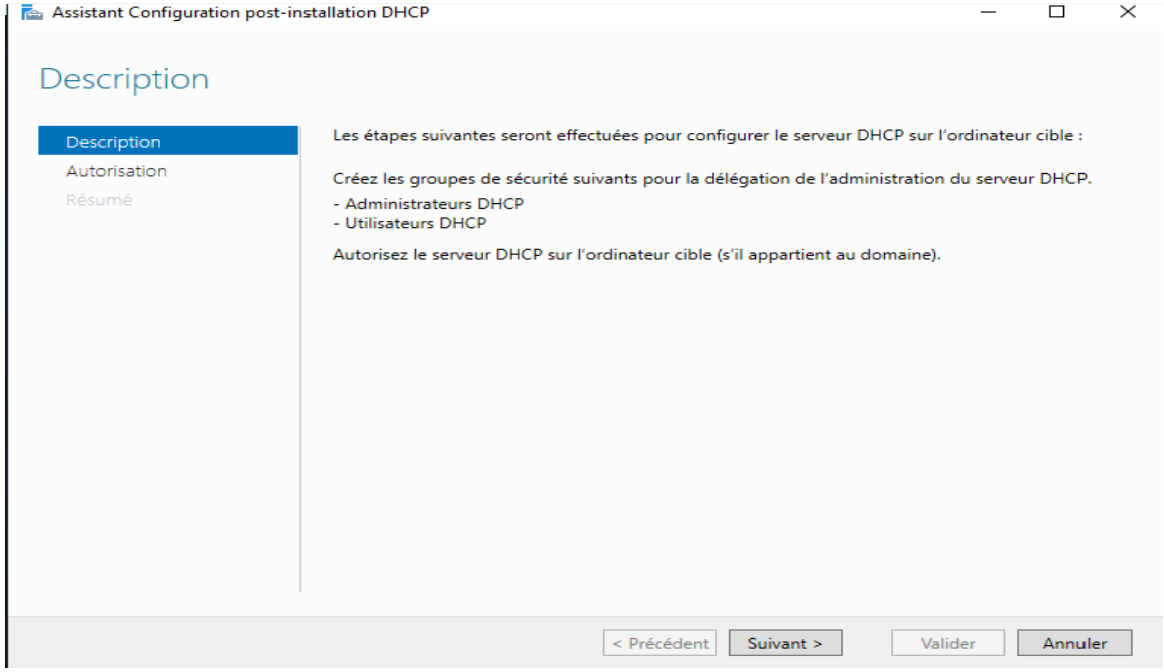

Figure 54 : Configuration DHCP.

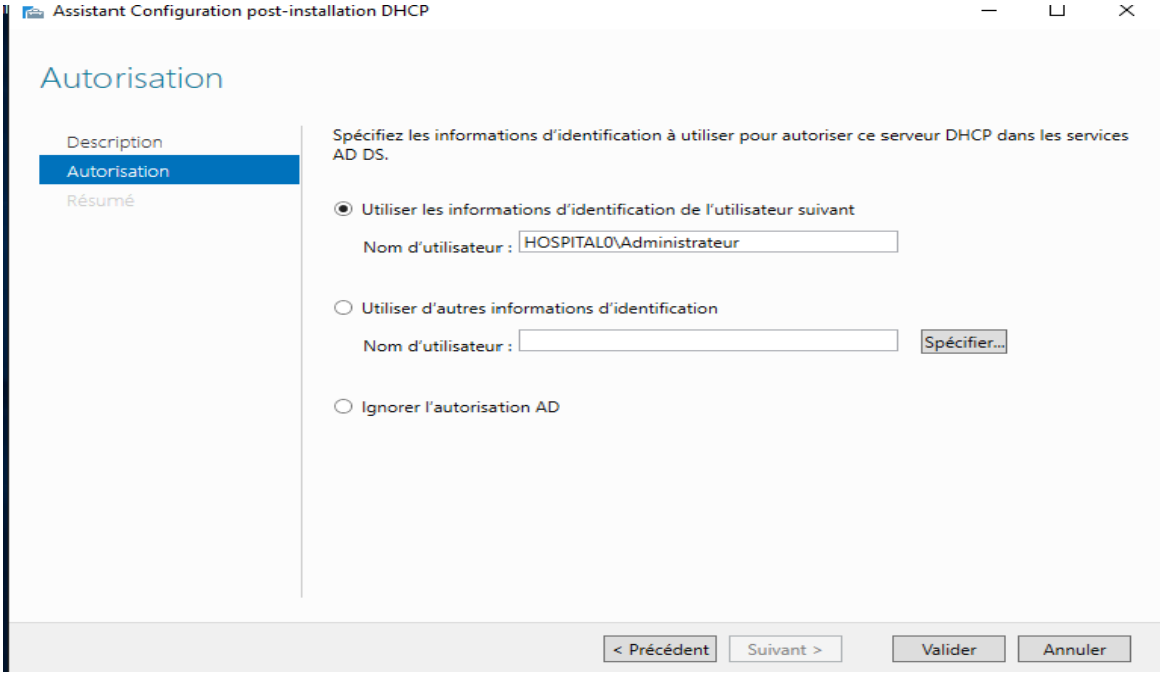

Figure 55 : Choix d'utilisateur de DHCP.

10. On clique sur Fermer et notre serveur DHCP est installé

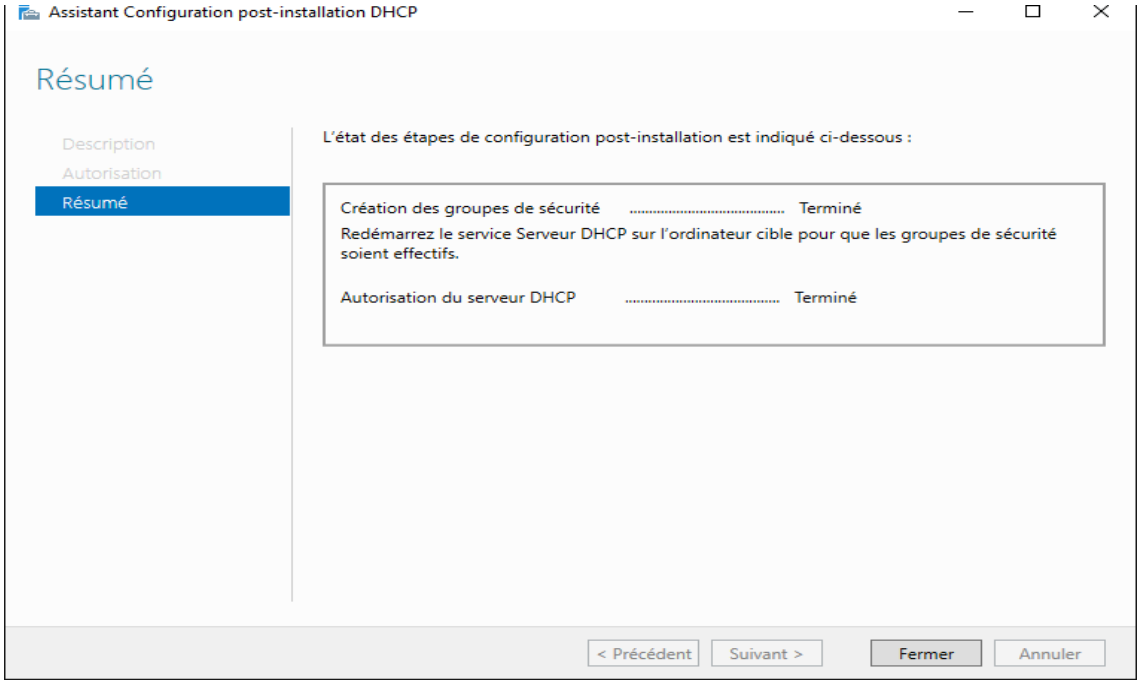

Figure 56 : Description de post installation DHCP.

Après l'installation, il faut passer à l'étape de configuration. Il faut indiquer au serveur quel est sa table d'adresses et quels sont les différentes valeurs qu'il doit proposer aux machines du réseau.

11. Dans Gestionnaire de serveur on clique sur Outils, on voie DHCP indiqué dans la liste, un clic sur DHCP pour ouvrir la console.

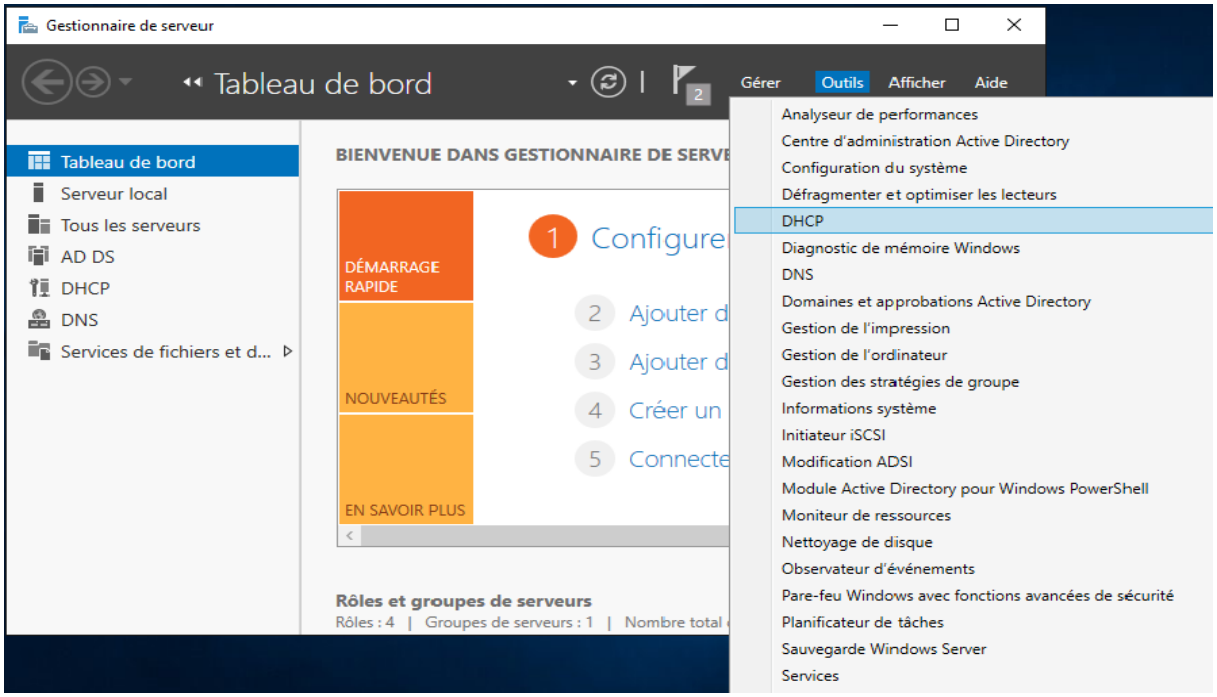

Figure 57 : Apparition du DHCP dans onglet Outils.

La console d'administration du service DHCP va s'ouvrir

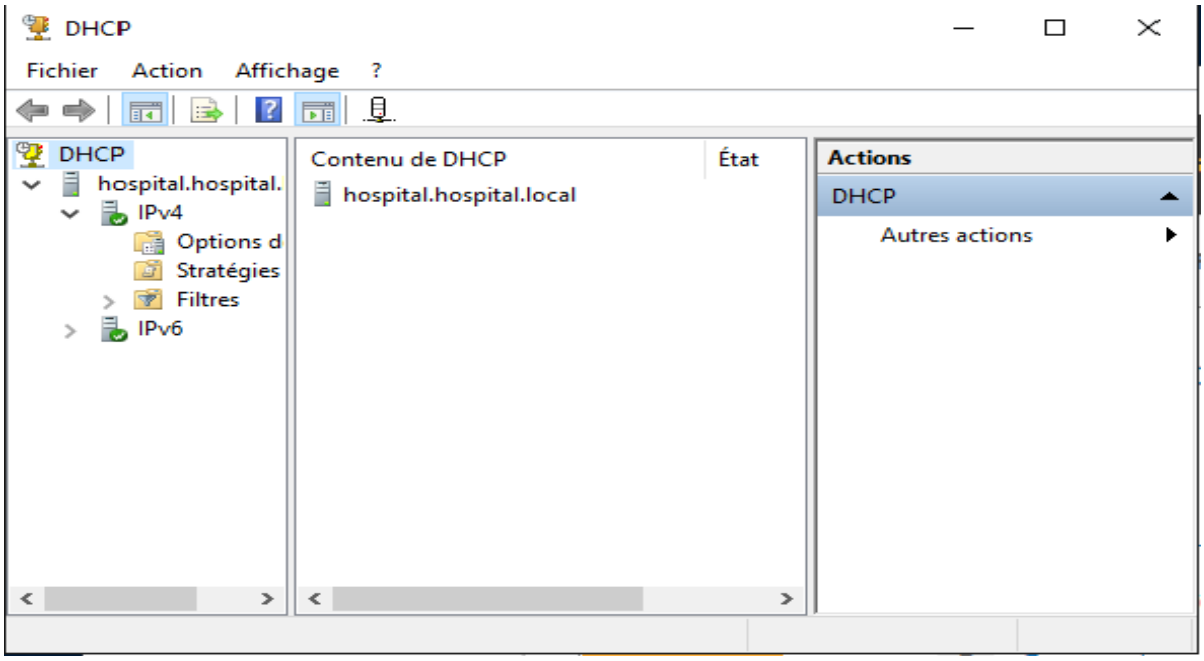

Figure 58 : Console d'administration DHCP.

12. Ensuite, on crée la portée afin que plus tard, nos clients obtiennent l'adresse IP de ce serveur. Alors on clique avec le bouton droit sur IPv4, on clique sur Nouvelle étendue.

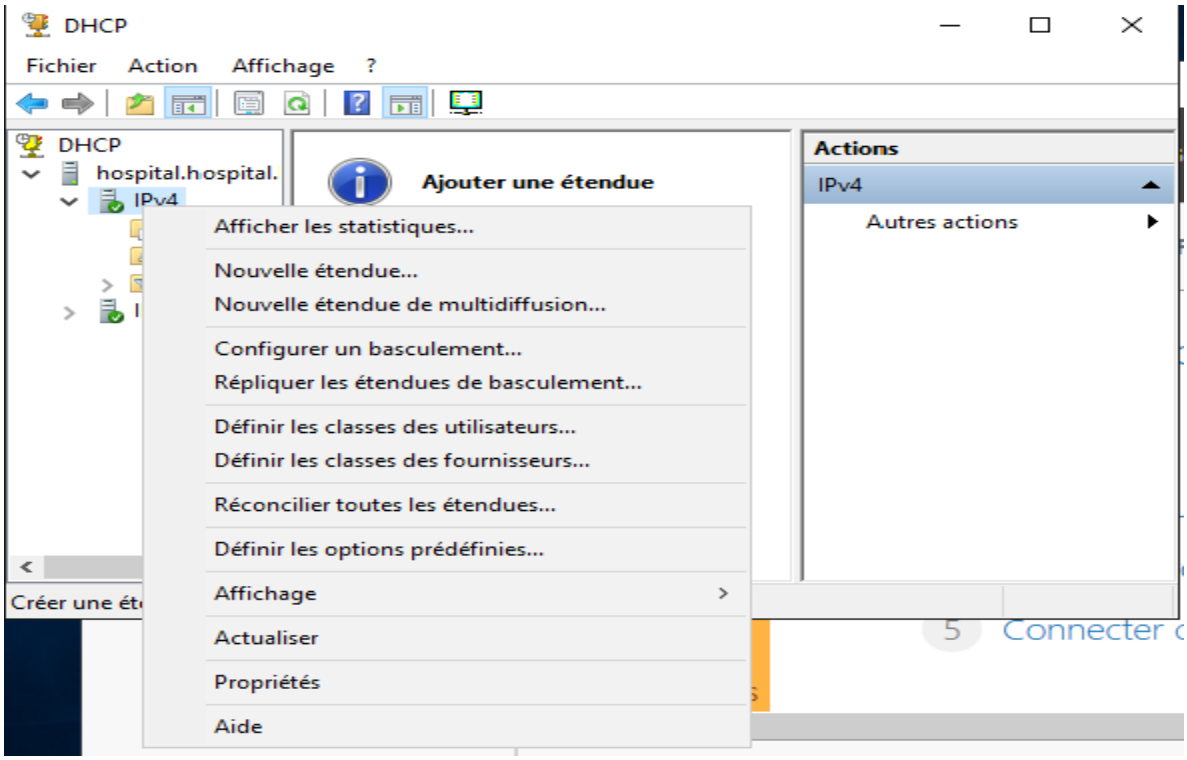

Figure 59 : Lancement de la Création d'étendu IPv4.

13. Une nouvelle fenêtre s'ouvre, on clique sur suivant

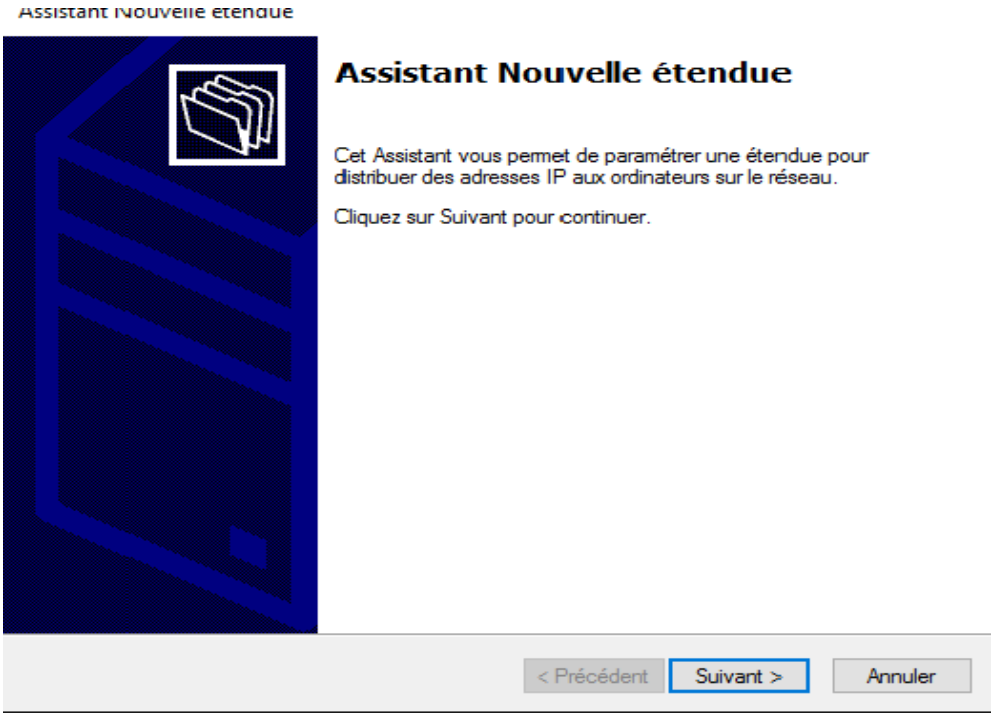

Figure 60 : Assistant de nouvelle étendu.

14. On indique le nom de l'étendu, il y a possibilité d'écrire une description

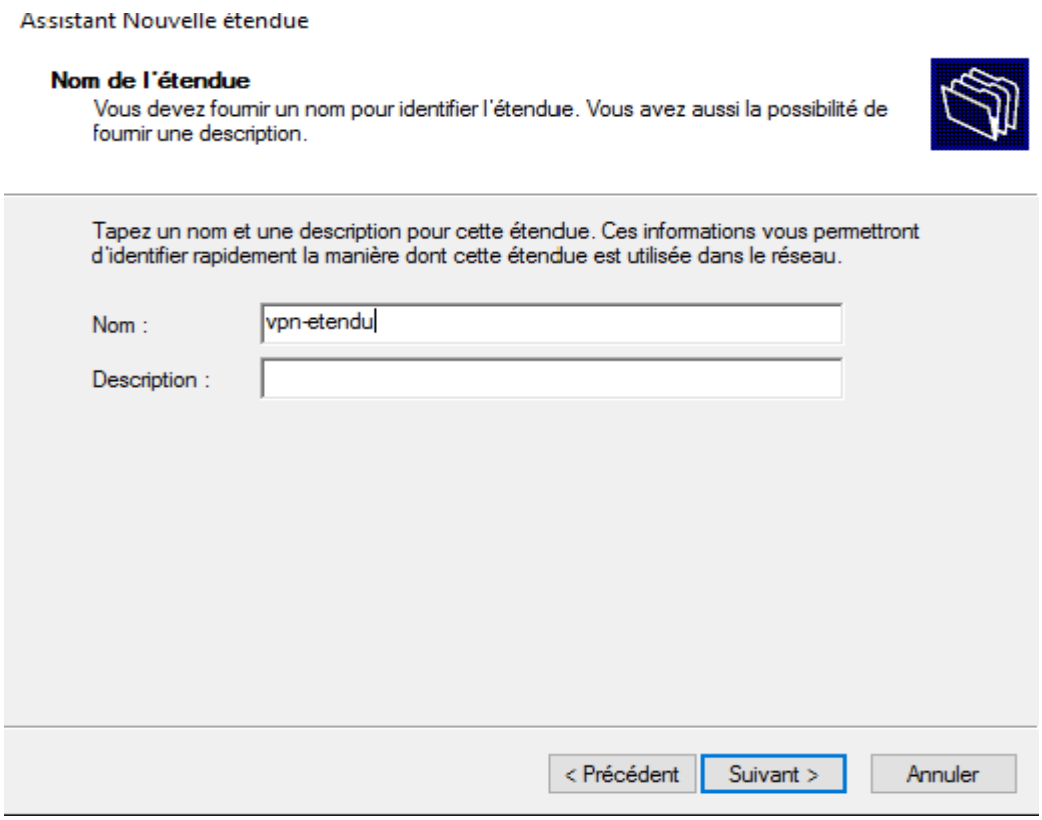

Figure 61 : Nom de l'étendu.

15. Sur l'écran **Plage d'adresses IP**, c'est ici qu'on fait entrer la plage d'adresses IP de nos clients,

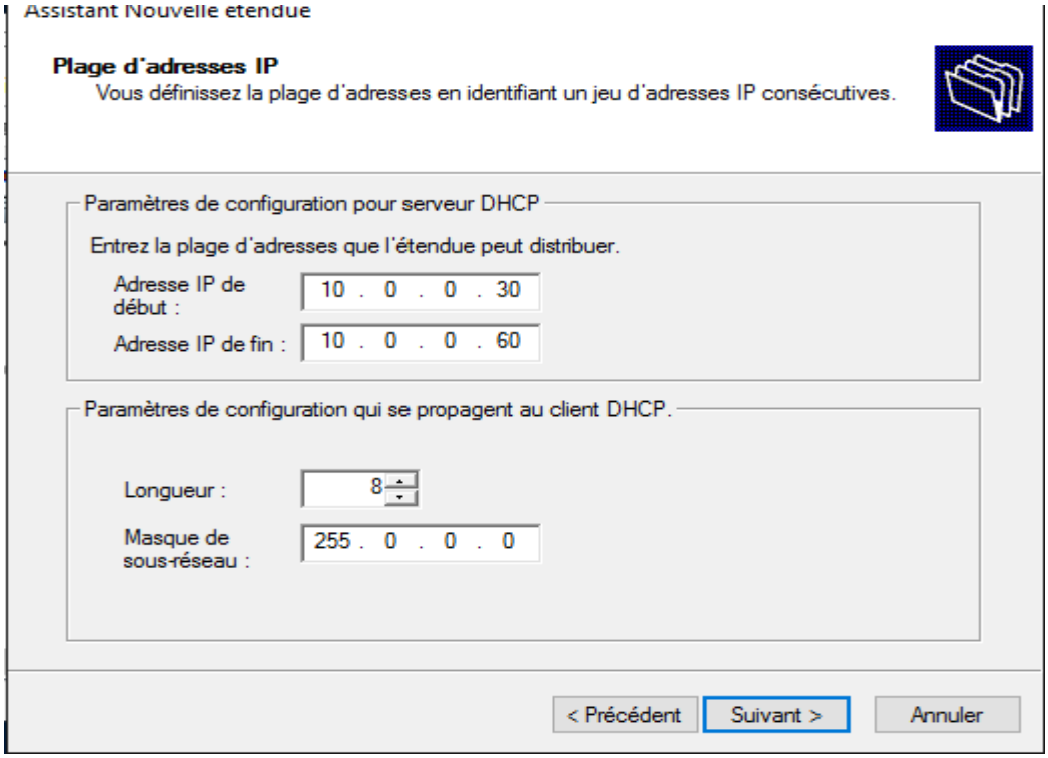

Figure 62 : La plage d'adressage de l'étendu.

16. Sur cette fenêtre on peut exclure des adresses IP, on clique sur suivant

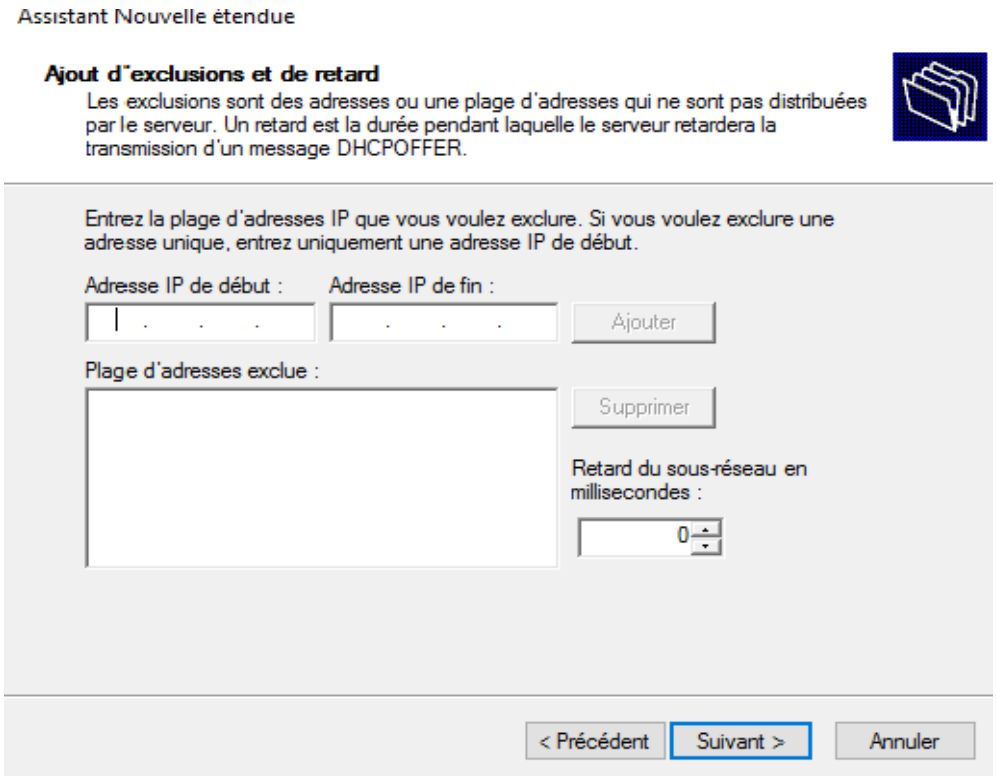

Figure 63 : Ajout d'exclusion.

17. Ici on peut spécifie combien de temps nos clients peuvent utiliser une adresse IP de cette étendue.

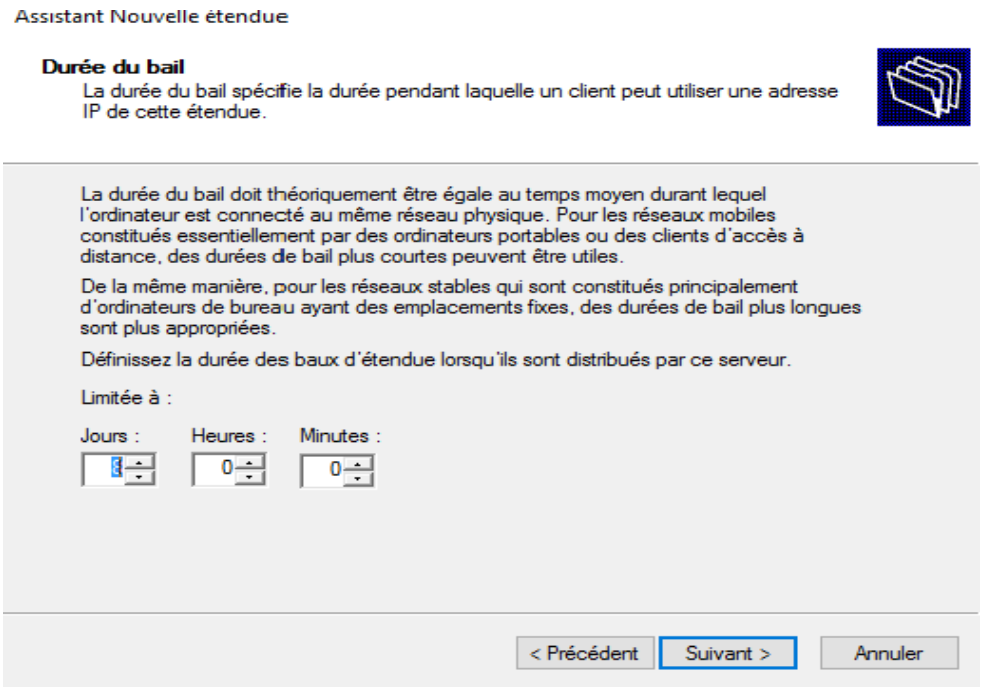

Figure 64 : Durée de connexion d'une adresse IP.

18. On clique sur « Oui, je veux configurer ces options maintenant ».

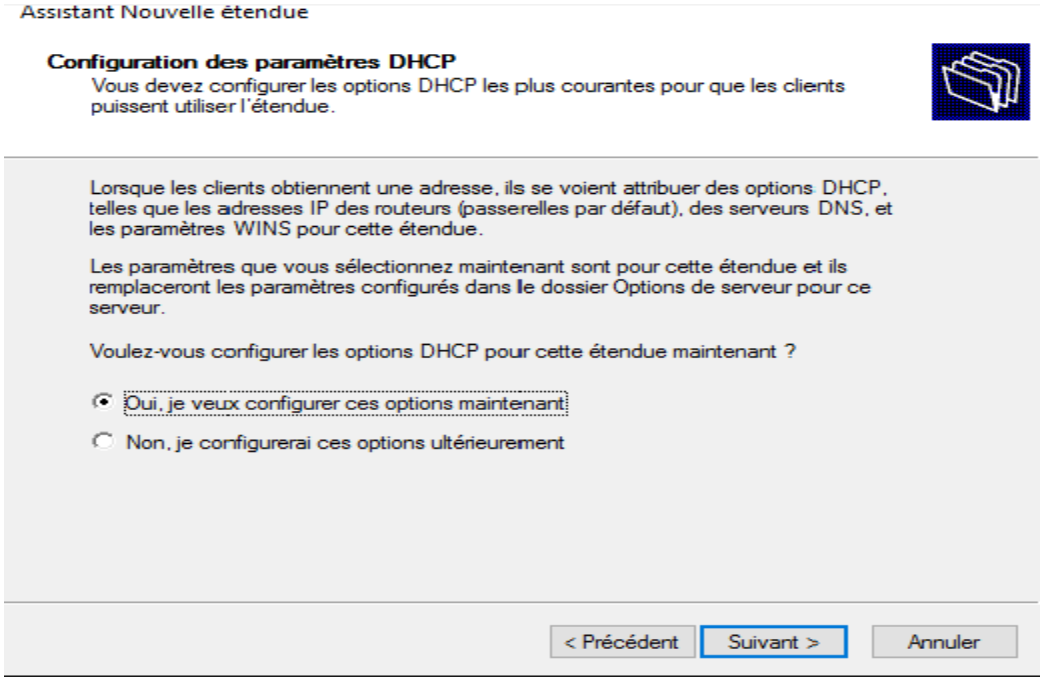

Figure 65 : Confirmer la configuration DHCP.

19. On indique au serveur DHCP quelle est l'adresse IP de passerelle par défaut.

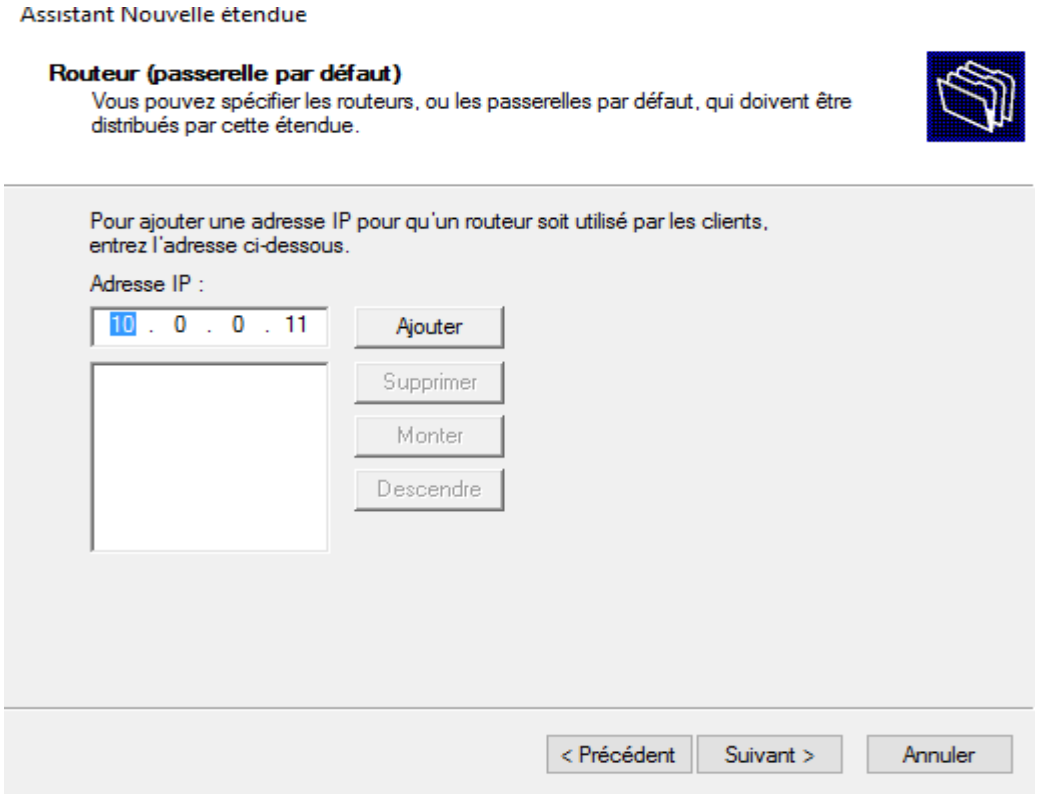

Figure 66 : Ajout d'adresse de routeur.

20. Ensuite sur l'écran Nom de domaine et serveurs DNS**,** on vérifie que le domaine parent détecte automatiquement le nom de domaine et l'adresse IP elle-même.

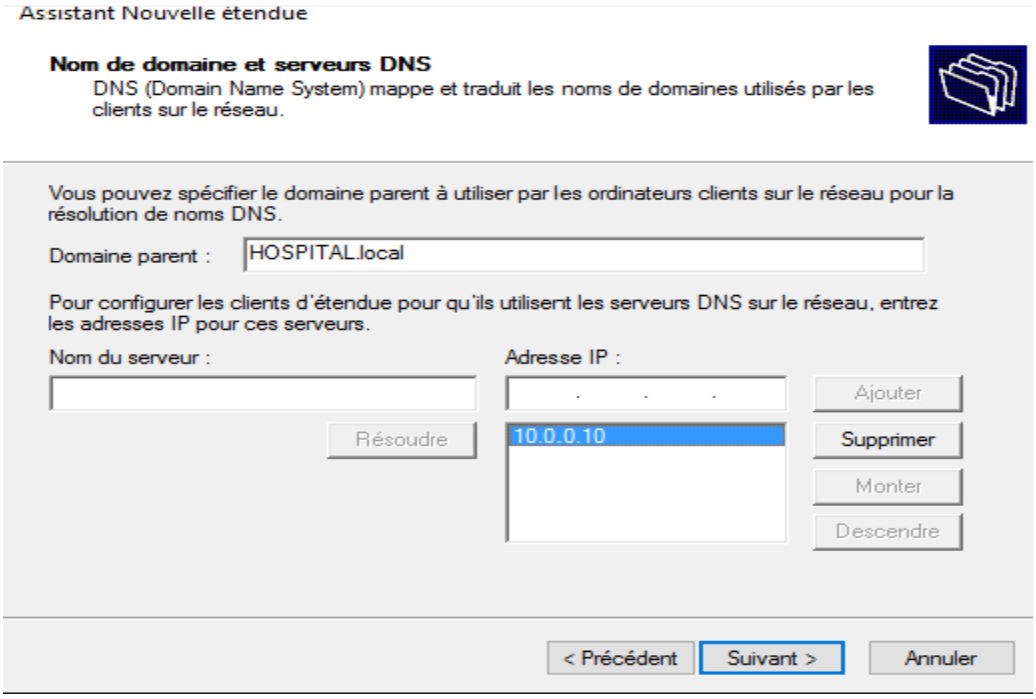

Figure 67 : Entrer le Domaine.

21. Sur les serveurs WINS**,** on clique simplement sur Suivant

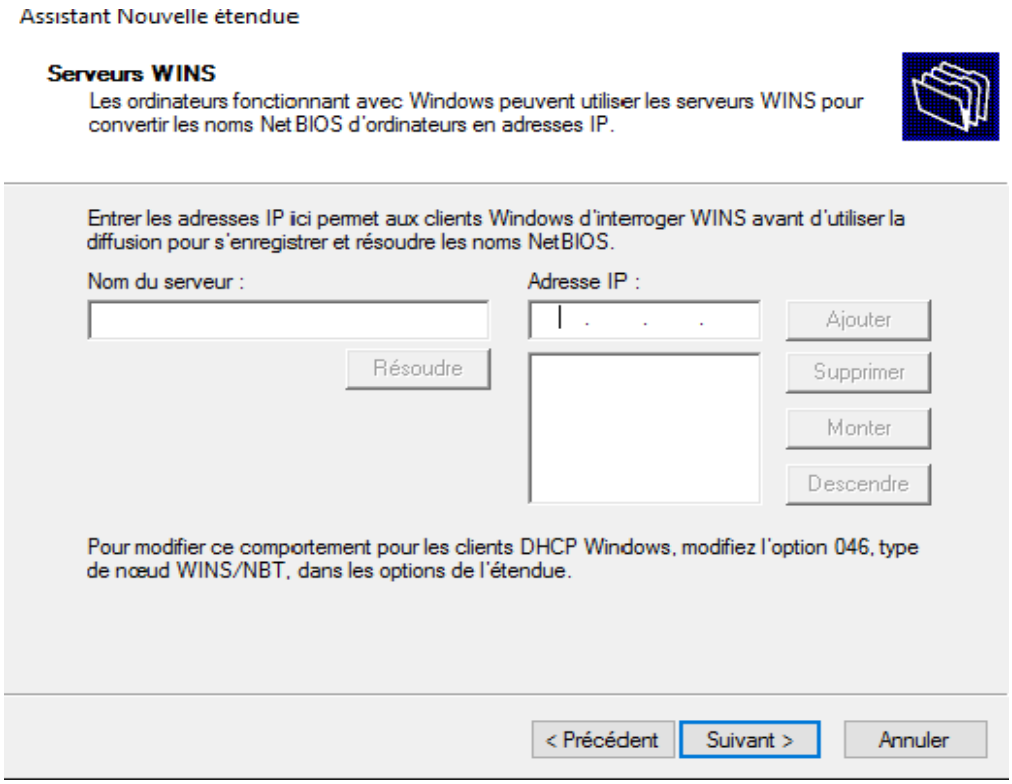

Figure 68 : Serveurs WINS.

22. On choisit « Oui**,** je veux activer cette étendue maintenant »et on clique sur suivant

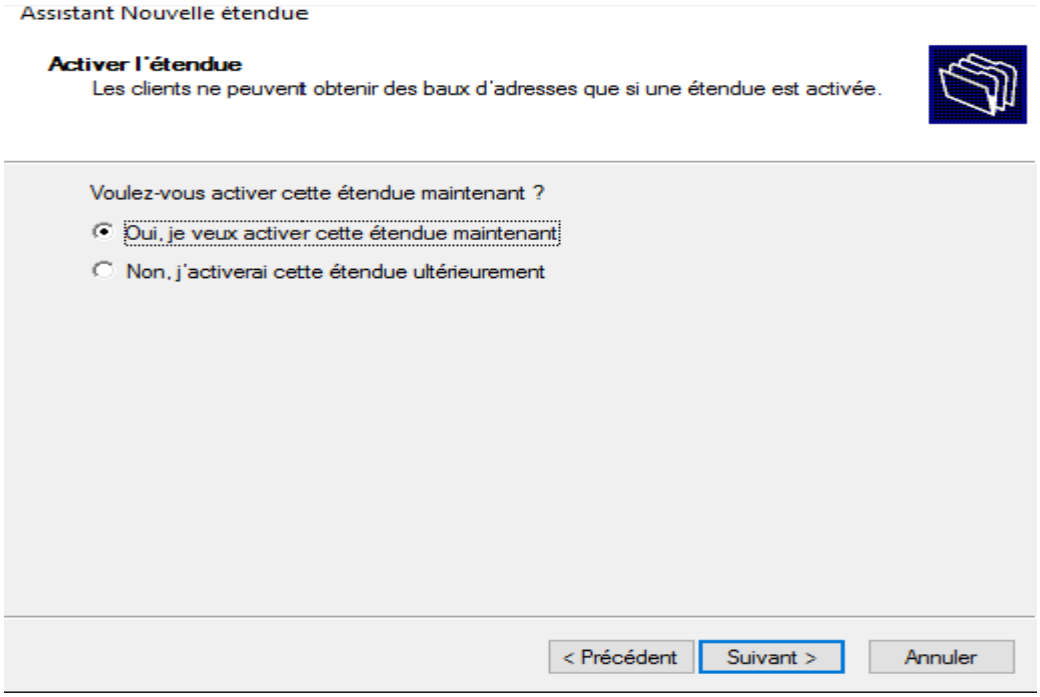

Figure 69 : Activer l'étendu.

23. Finalement on a la confirmation qu'on a bien terminé la création de l'étendu

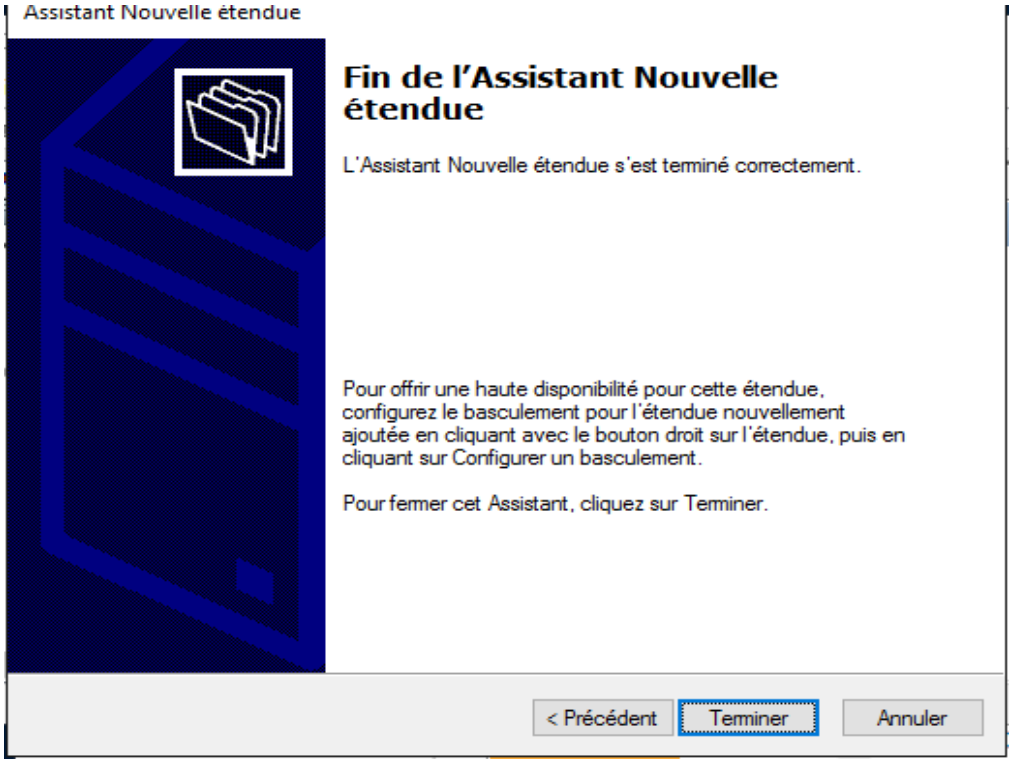

Figure 70 : Terminer la création de l'étendu.

L'étape suivante est l'installation du service VPN dans la machine serveur VPN

3.3.3.4. Installation et configuration du VPN

1. On lance l'assistant d'ajout de rôles et de fonctionnalités

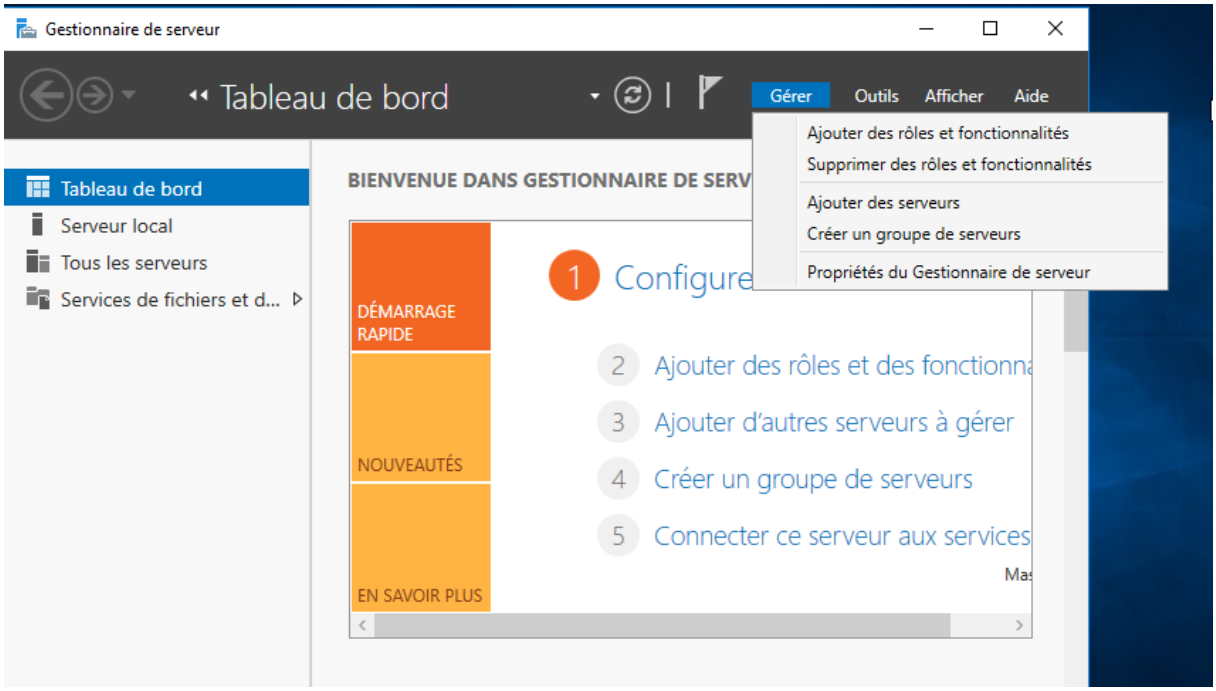

Figure 71 : Ajout de rôle VPN.

2. On peut voir que notre serveur possède 2 adresses IP, on clique sur suivant

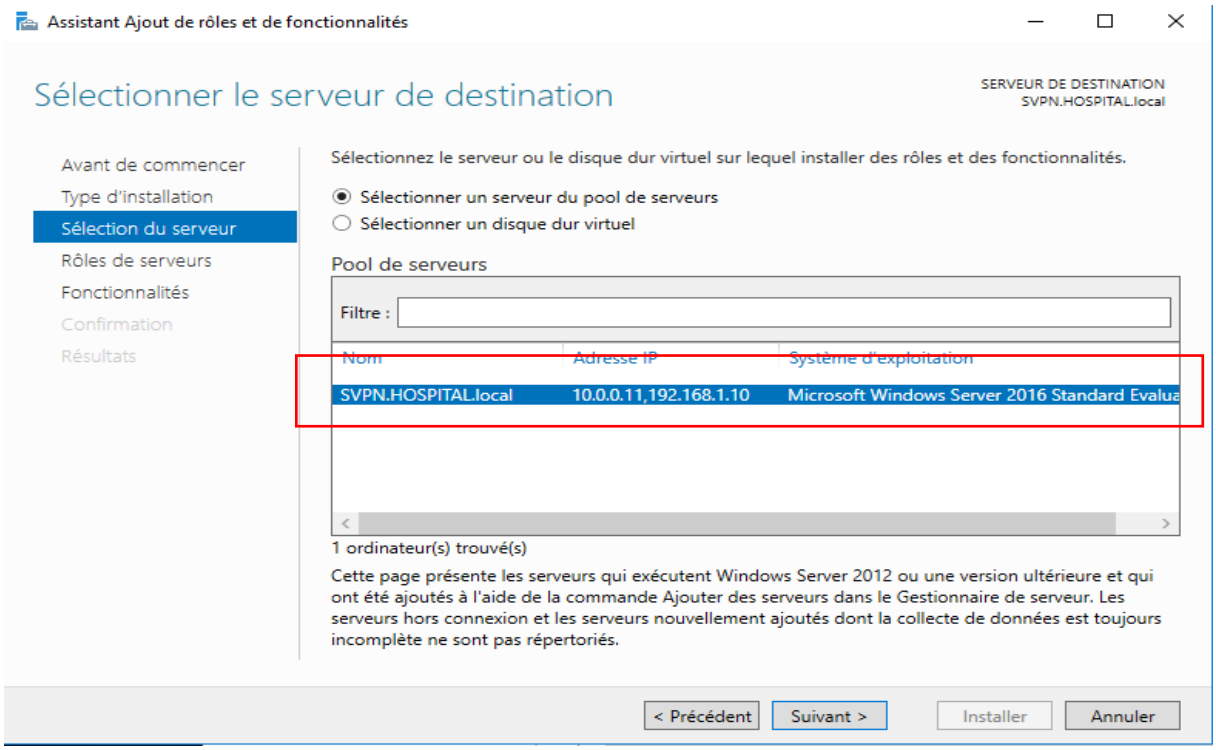

Figure 72 : Choix de serveur VPN.

3. On coche la case « Accès à distance » et on clique sur suivant

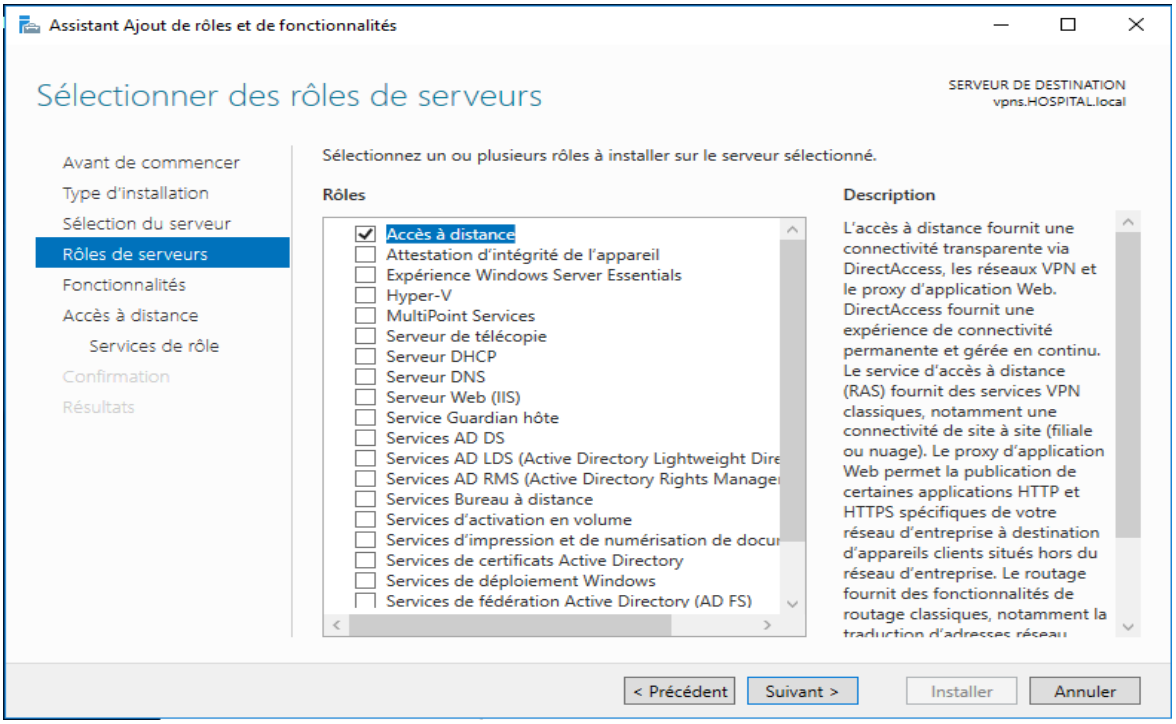

Figure 73:Sélection de rôle Accès à distance.

4. Aucune fonctionnalité nécessaire, on clique sur suivant

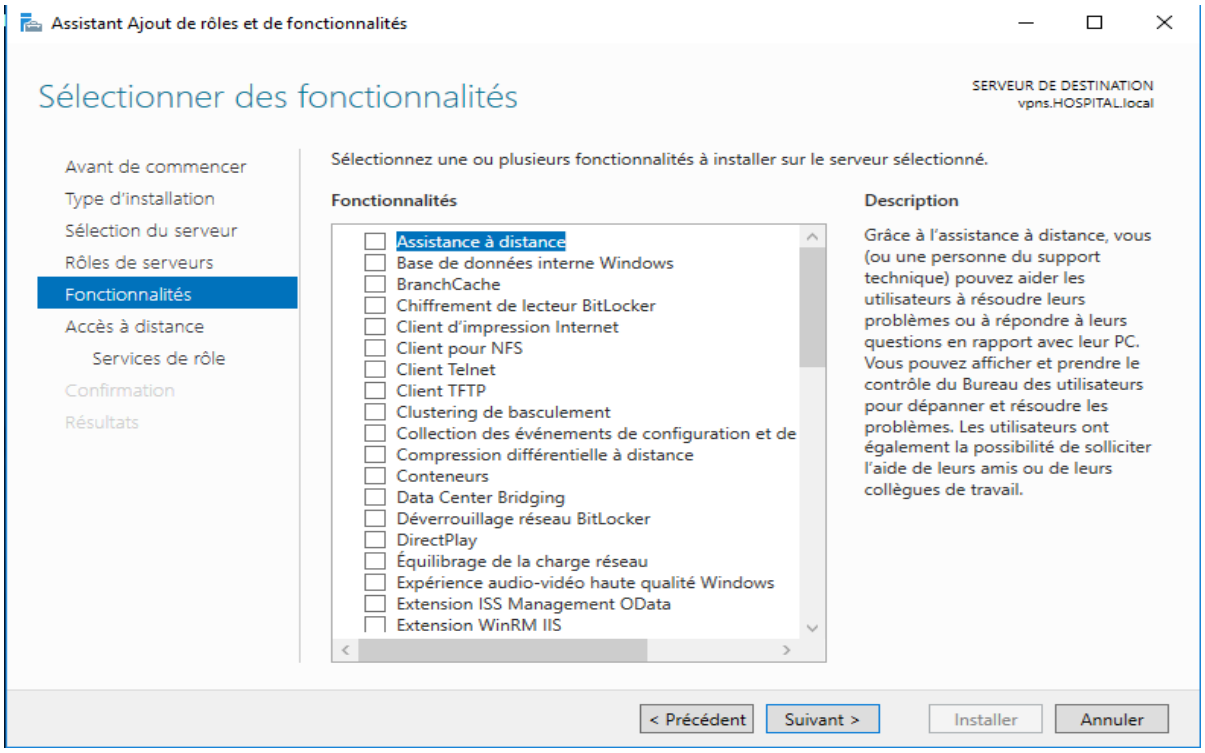

Figure 74 : Sélection de fonctionnalités VPN.

5. Sur l'écran une description du rôle « Accès à distance » s'affiche, on clique sur suivant

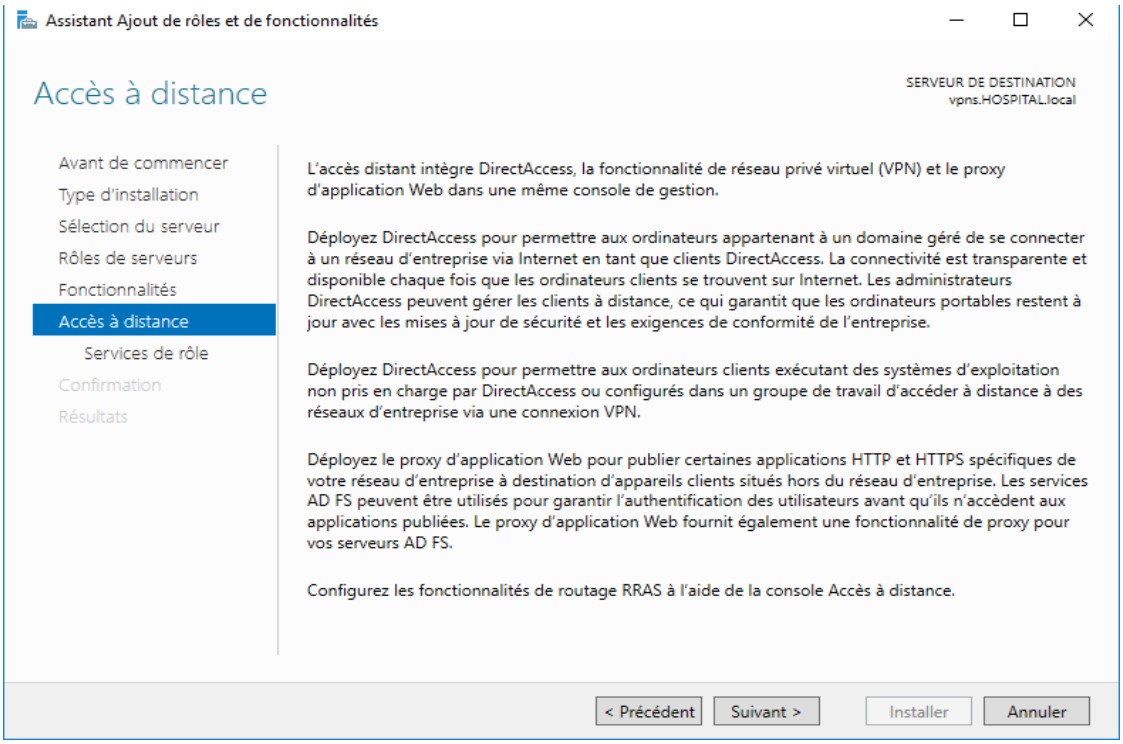

Figure 75 : Description de rôle Accès à distance.

6. On coche « Direct Access et VPN »

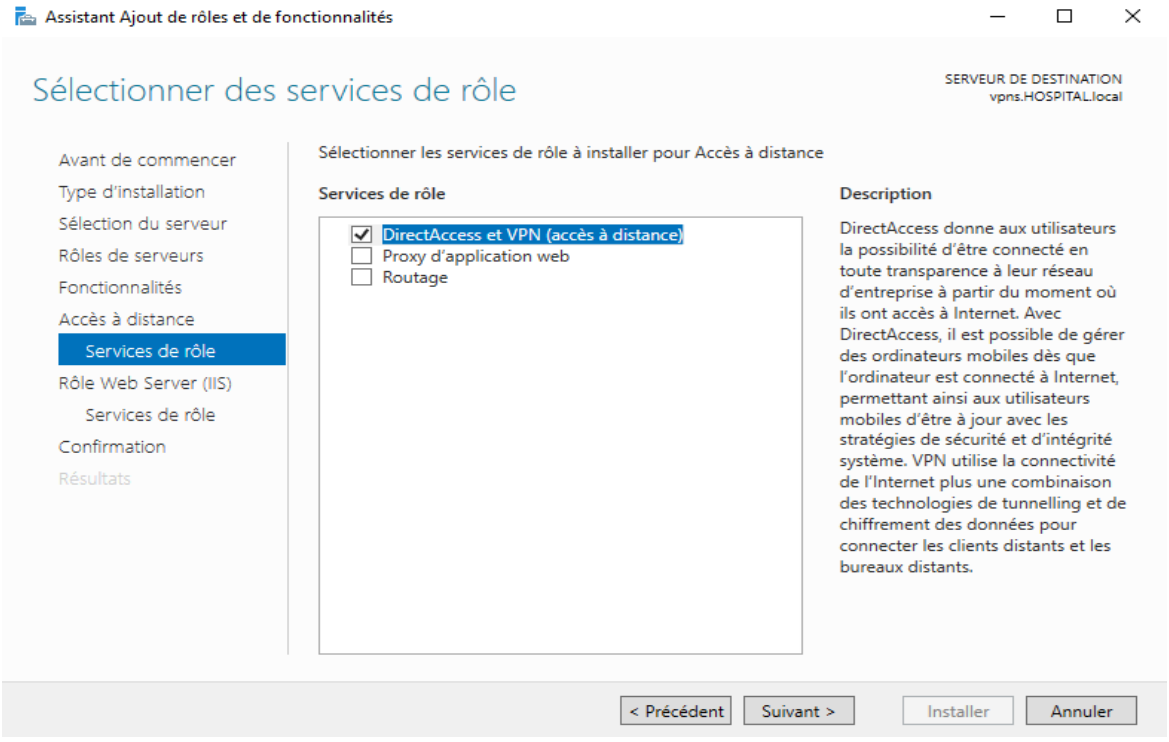

Figure 76 : Sélection des services de rôle Accès à distance.

7. Windows nous affiche une description du rôle « Web Server (IIS) », on clique suivant pour continue

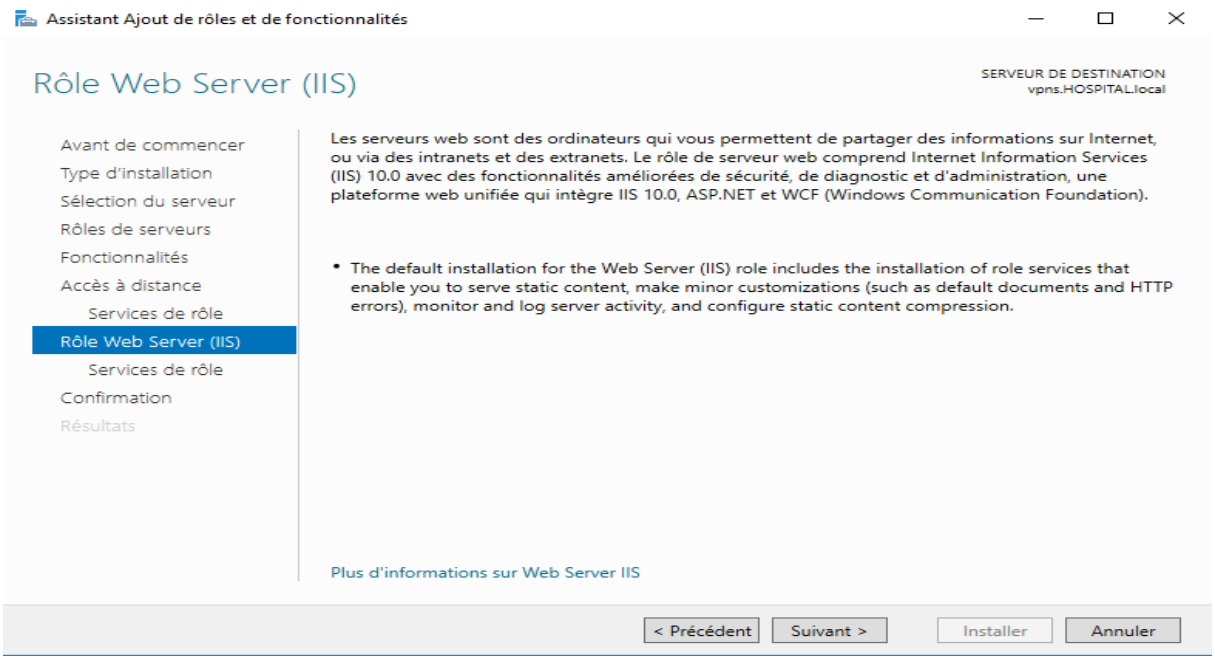

Figure 77:Description du rôle Web server IIS.

8. On clique sur suivant

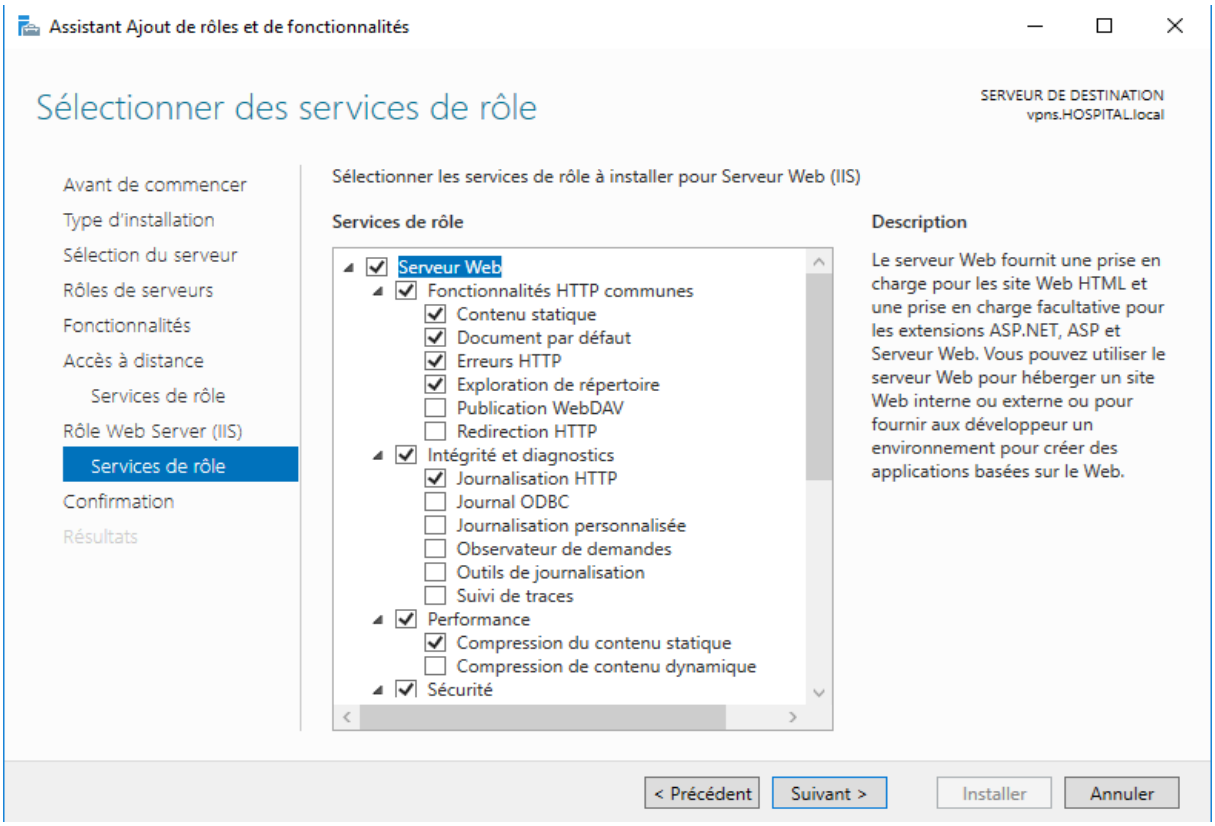

Figure 78 : Sélection des services de rôle IIS.

9. On clique sur installer

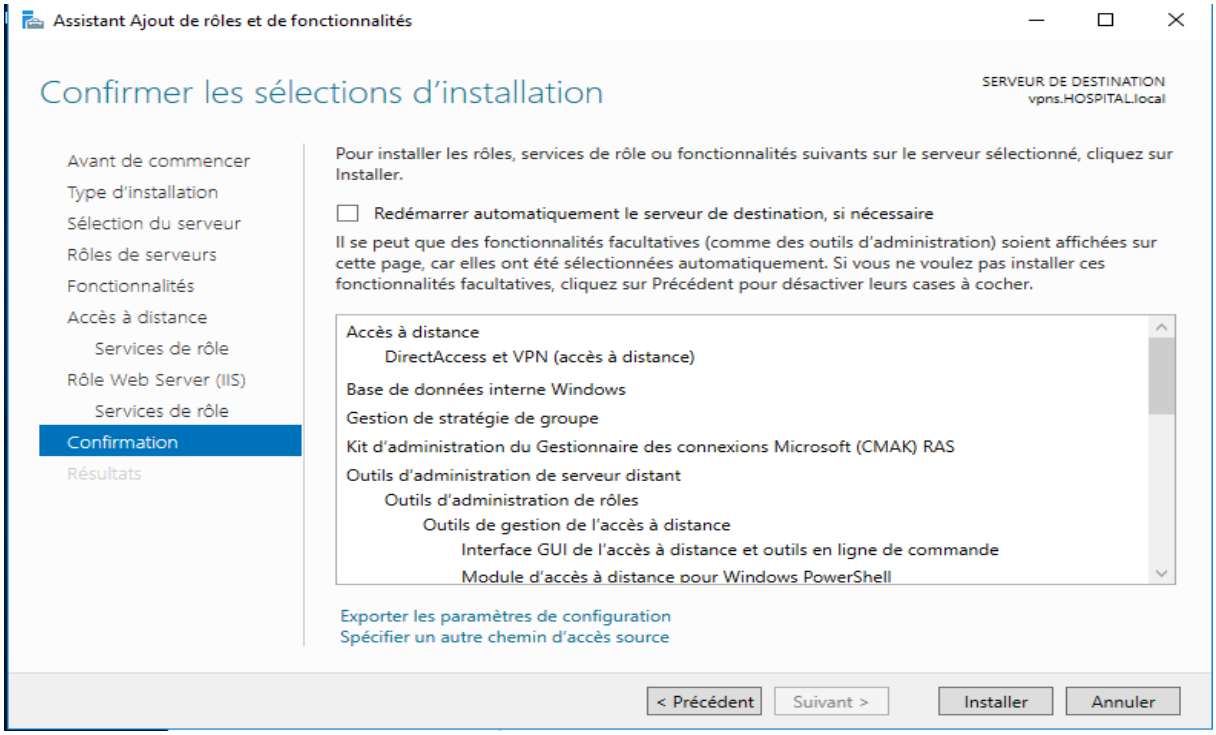

Figure 79 : Confirmation de l'installation de rôle Accès à distance.

10. Une fois l'installation terminée, on clique sur le lien « Ouvrir l'Assistant Mise en route »

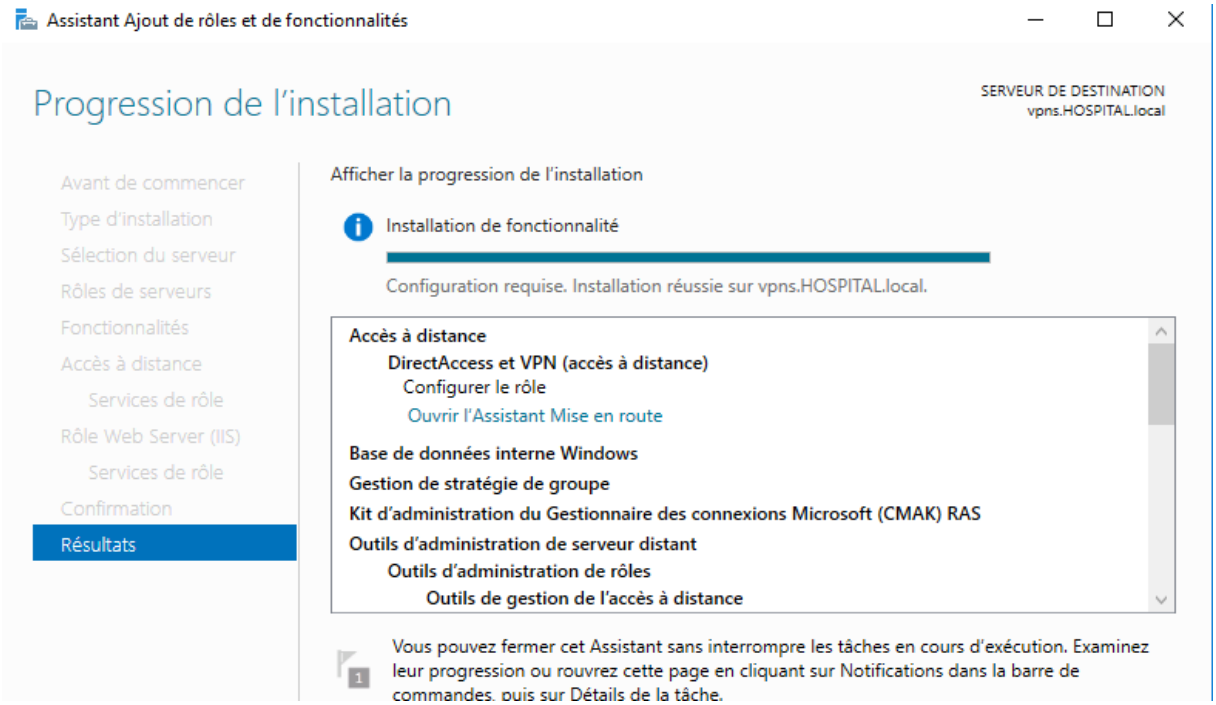

Figure 80 : Fin d'installation du rôle Accès à distance.

11. On commence la configuration de notre VPN, on choisit « Déployé VPN uniquement »

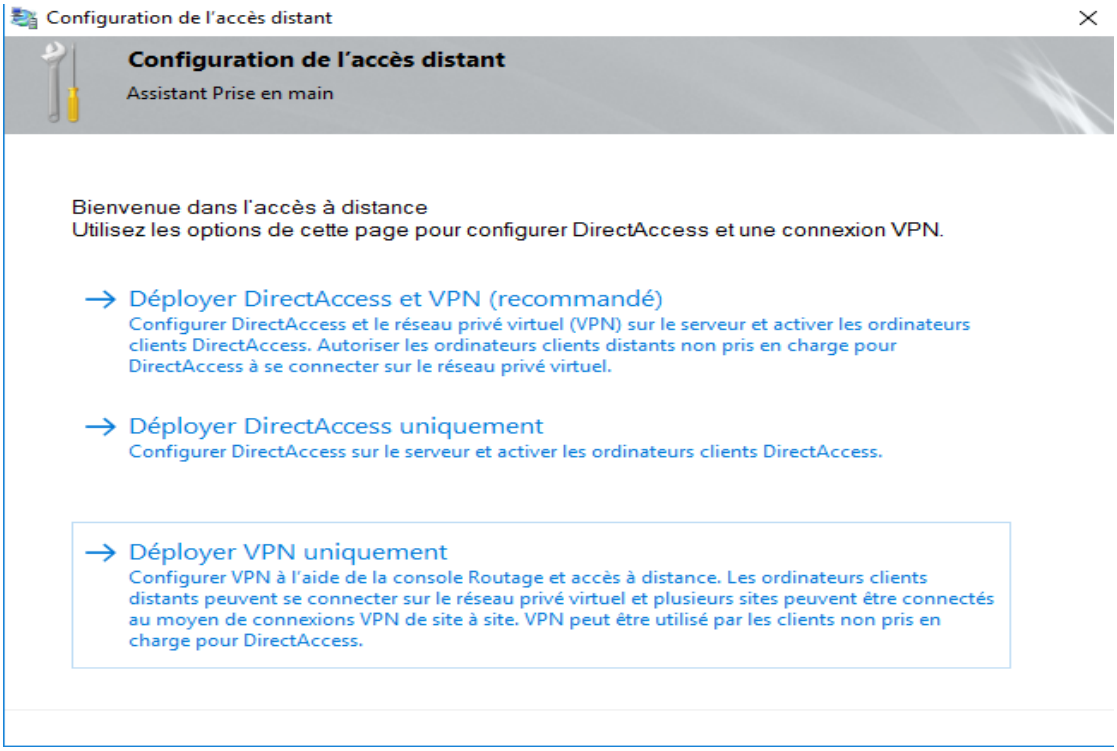

Figure 81 : Configuration du rôle Accès à Distance.

12. Ensuite, une fenêtre « Routage et accès distant » s'affiche, on fait un clic droit sur le nom de notre serveur, puis on clique sur « configurer et activer le routage et l'accès à distance »

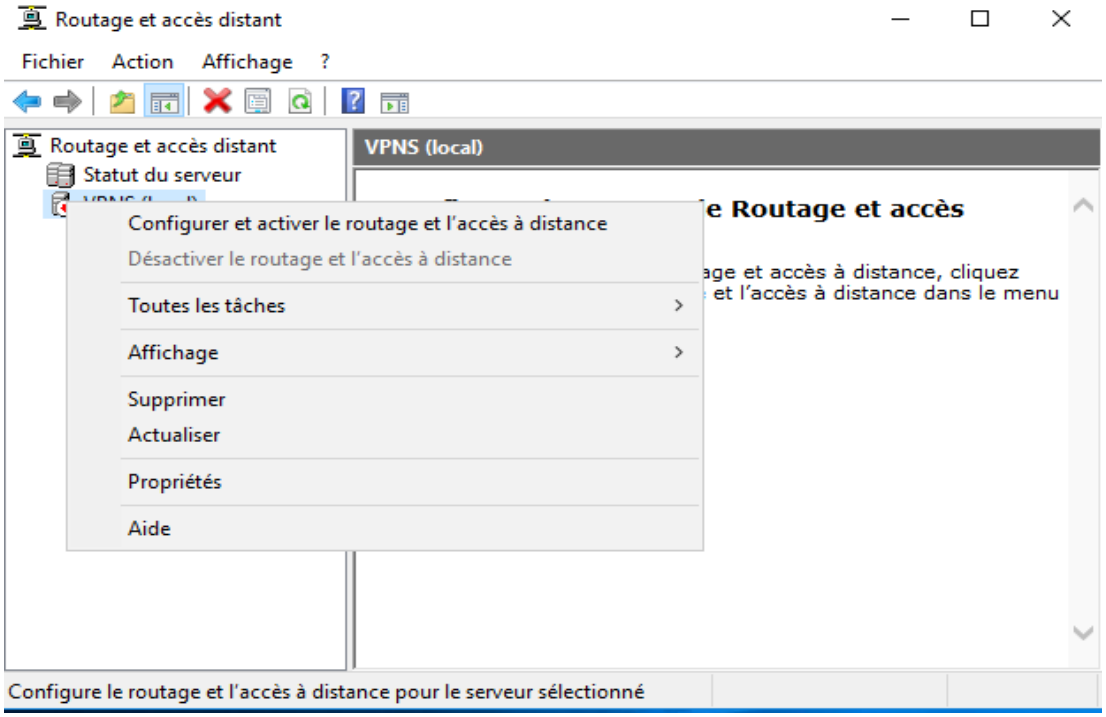

Figure 82 : Configuration de l'Accès à Distance.

13. L'assistant installation d'un serveur Routage et accès distant s'affiche, on clique sur Suivant

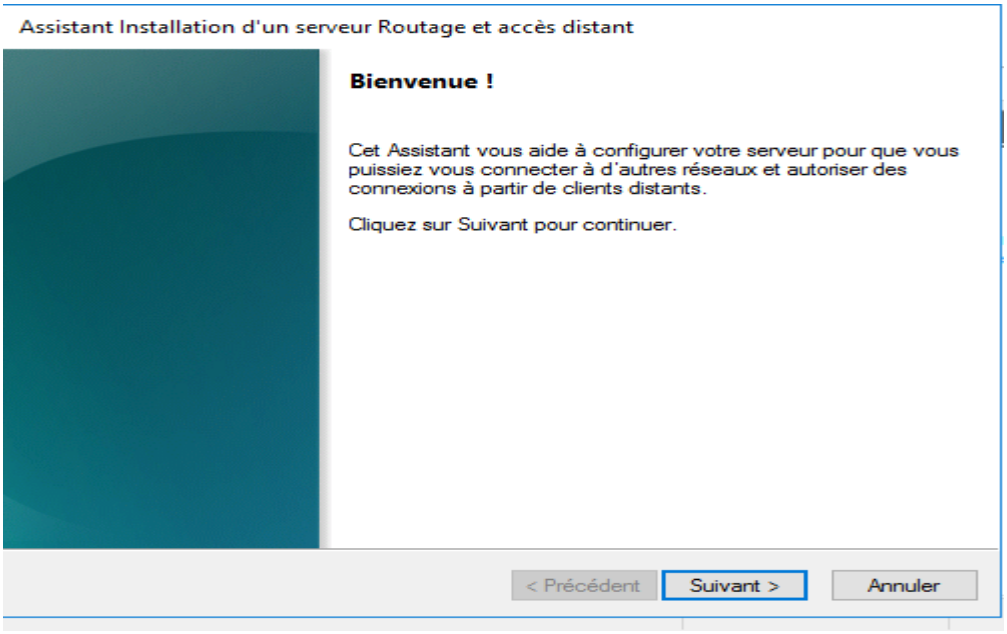

Figure 83 : Assistant installation d'un serveur Routage et accès distant.

14. On choisit « Accès à distance (connexion à distance et VPN) et on clique suivant

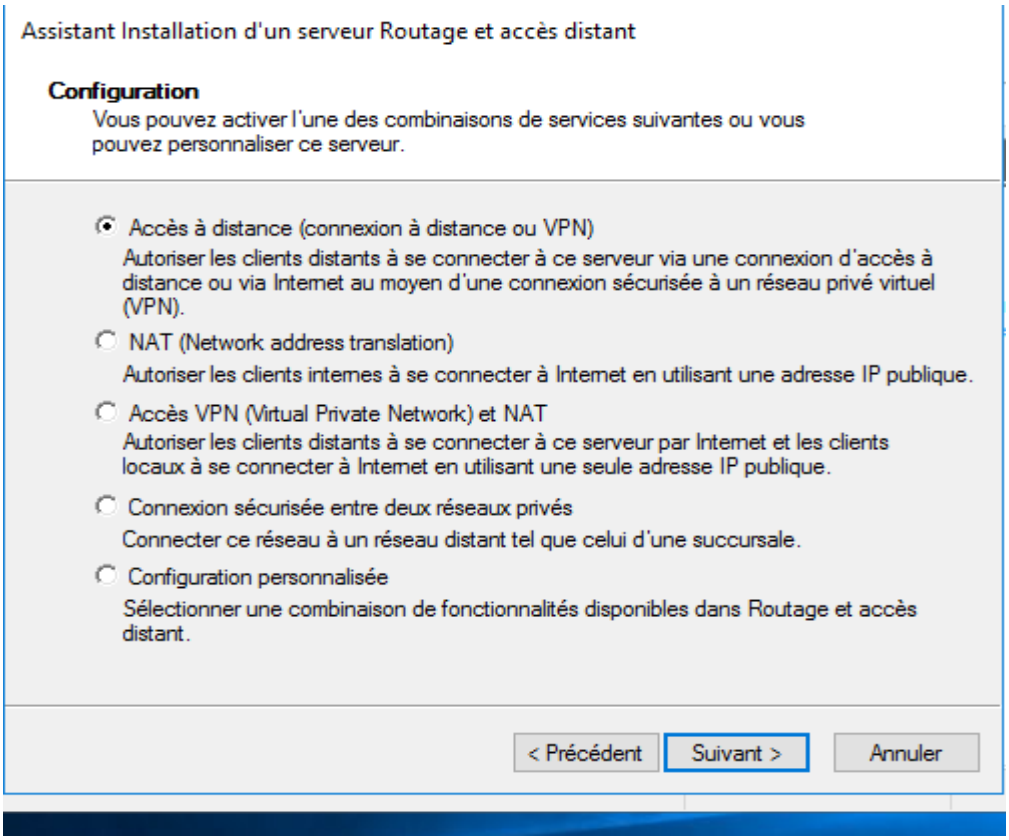

Figure 84 : Choix d'accès à distant connexion à distance ou VPN.

15. Sur la page suivante on clique VPN

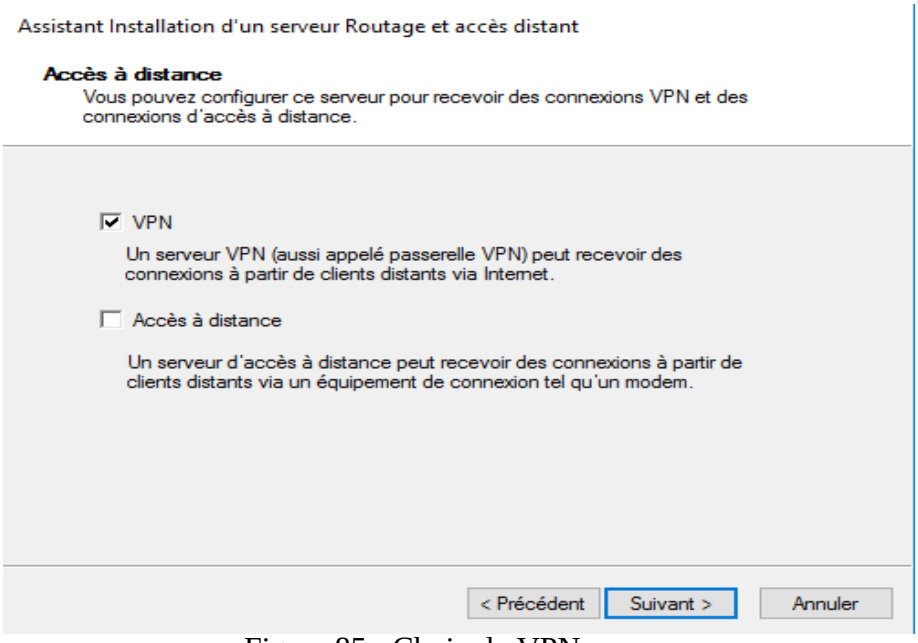

Figure 85 : Choix de VPN.

16. On sélectionne l'interface réseau de notre serveur qui est connectée à internet, on clique suivant

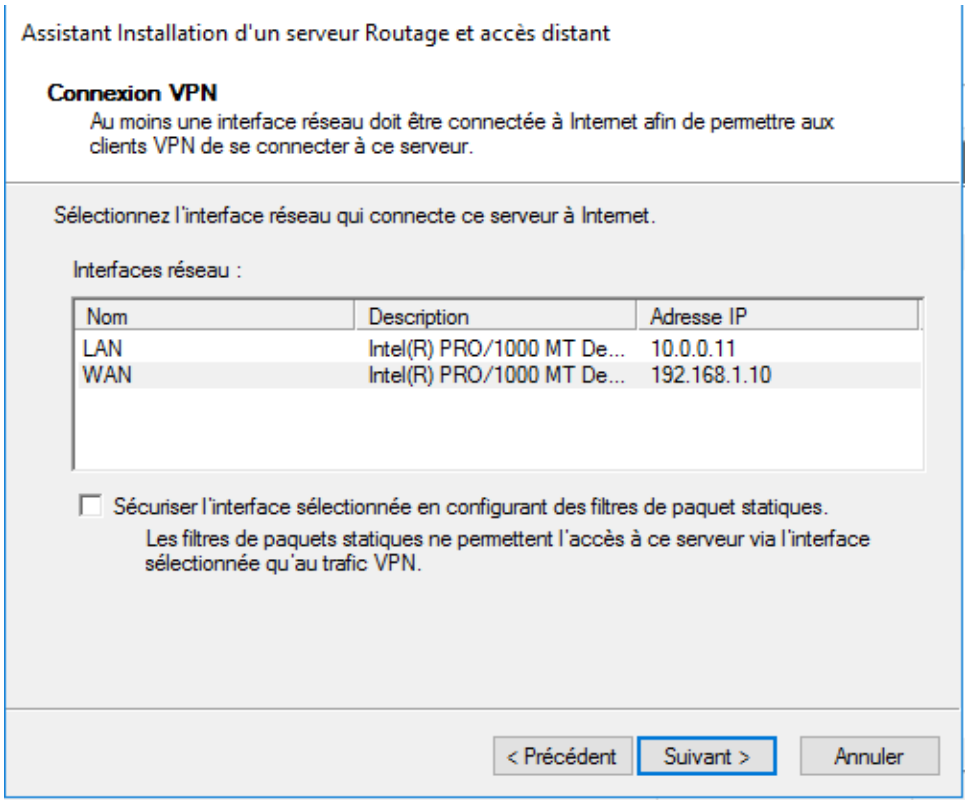

Figure 86 : Ajout d'interface WAN au connexion VPN.

17. On sélection aussi l'interface réseau à laquelle les clients VPN veulent se connecter (réseau interne) et on clique suivant

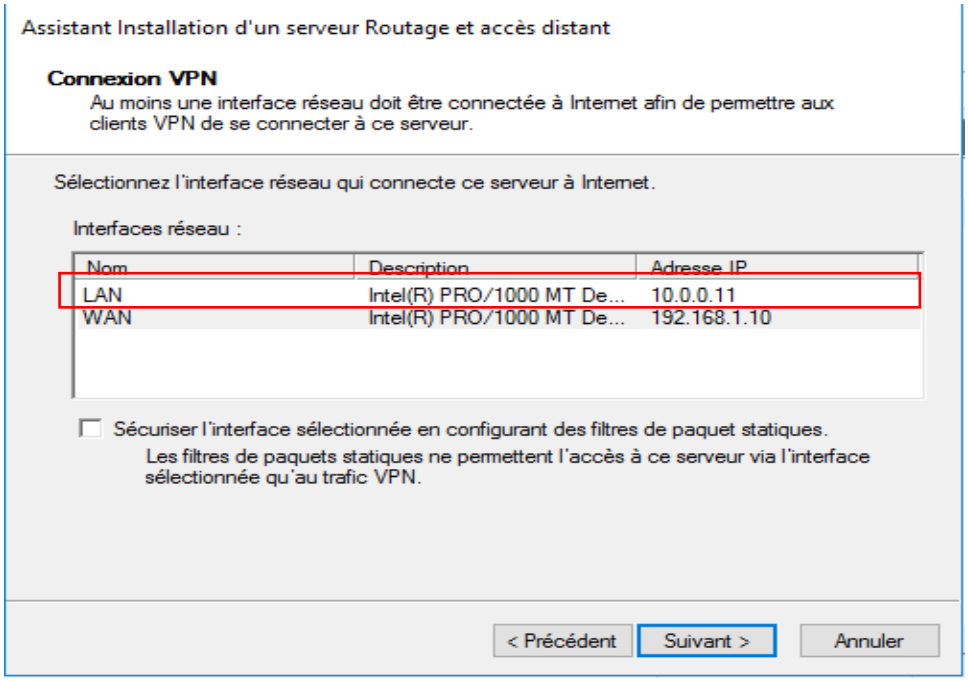

Figure 87 : Ajout d'interface LAN à la connexion VPN.

18. On sélectionne « automatique » Puis on clique sur Suivant.

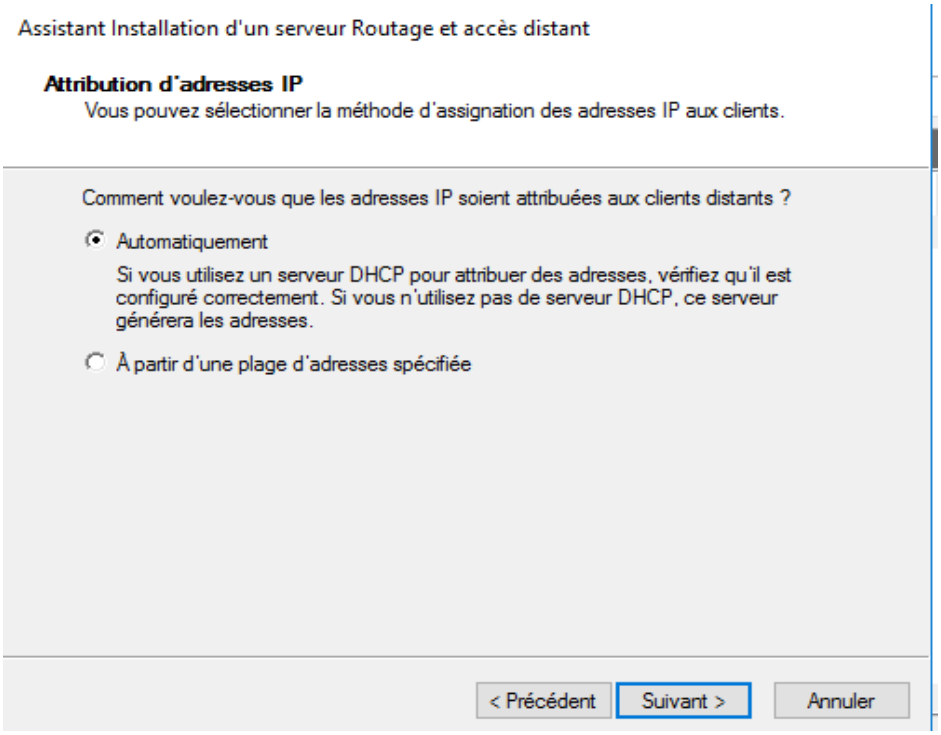

Figure 88 : Sélection méthode d'assignation des adresses IP au client.

19. On accepte la sélection par défaut sur cette page et on clique sur Suivant

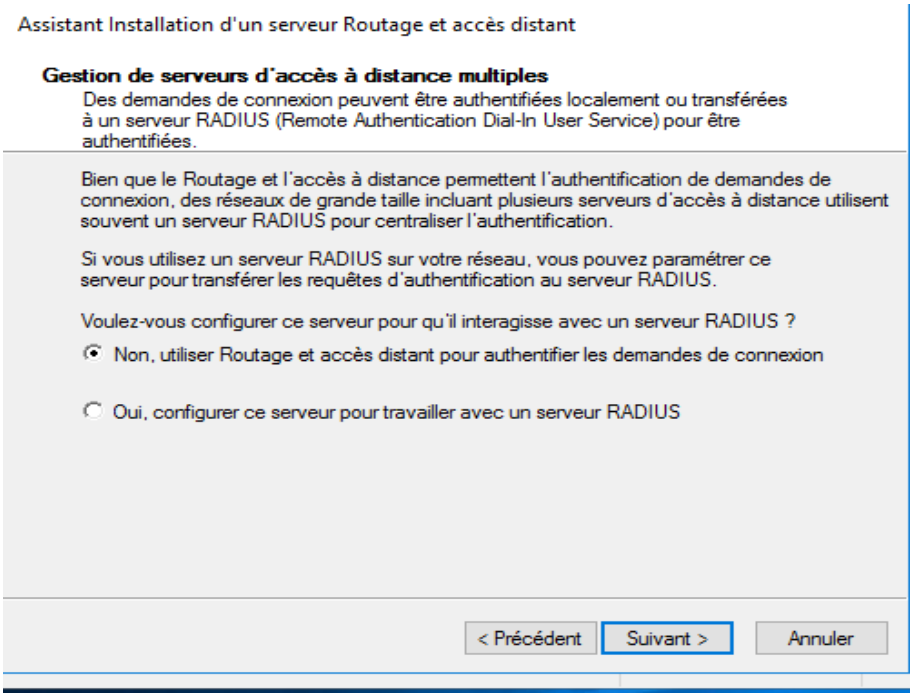

Figure 89 : Sélectionne de type des demandes.

20. Pour activer le VPN dans Windows Server 2016, on clique sur Terminer.

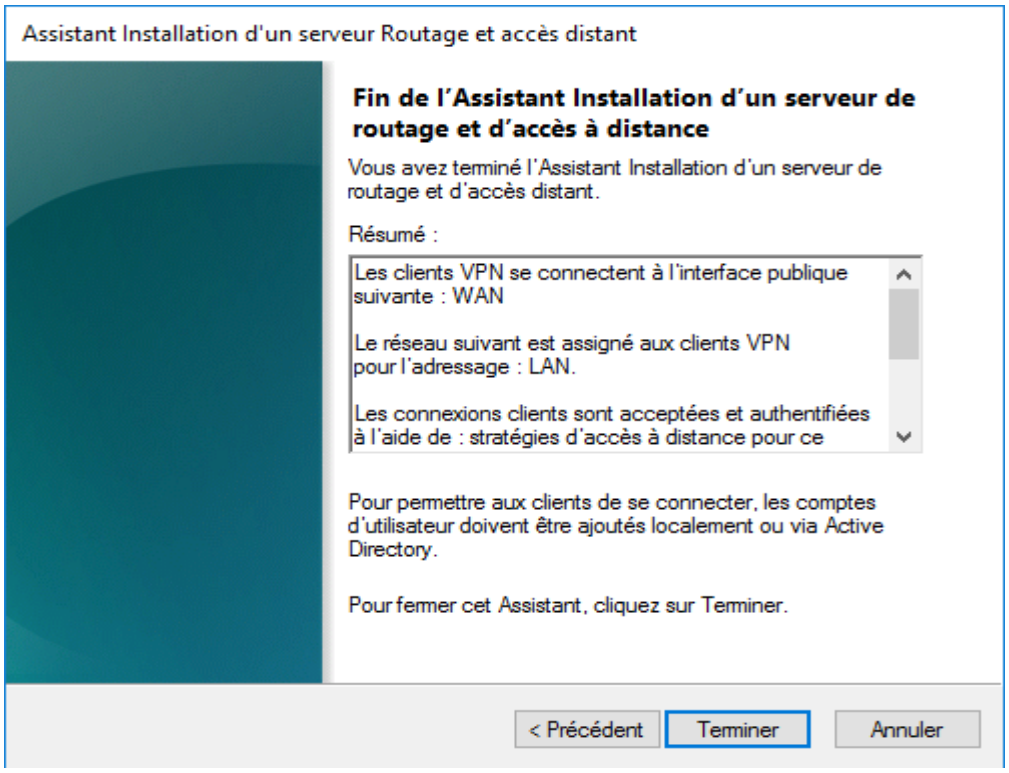

Figure 90 : Fin d'assistant Routage et accès distant.

21. On clique sur OK, la configuration des propriétés de l'agent de relais DHCP sera prise dans les prochaines étapes

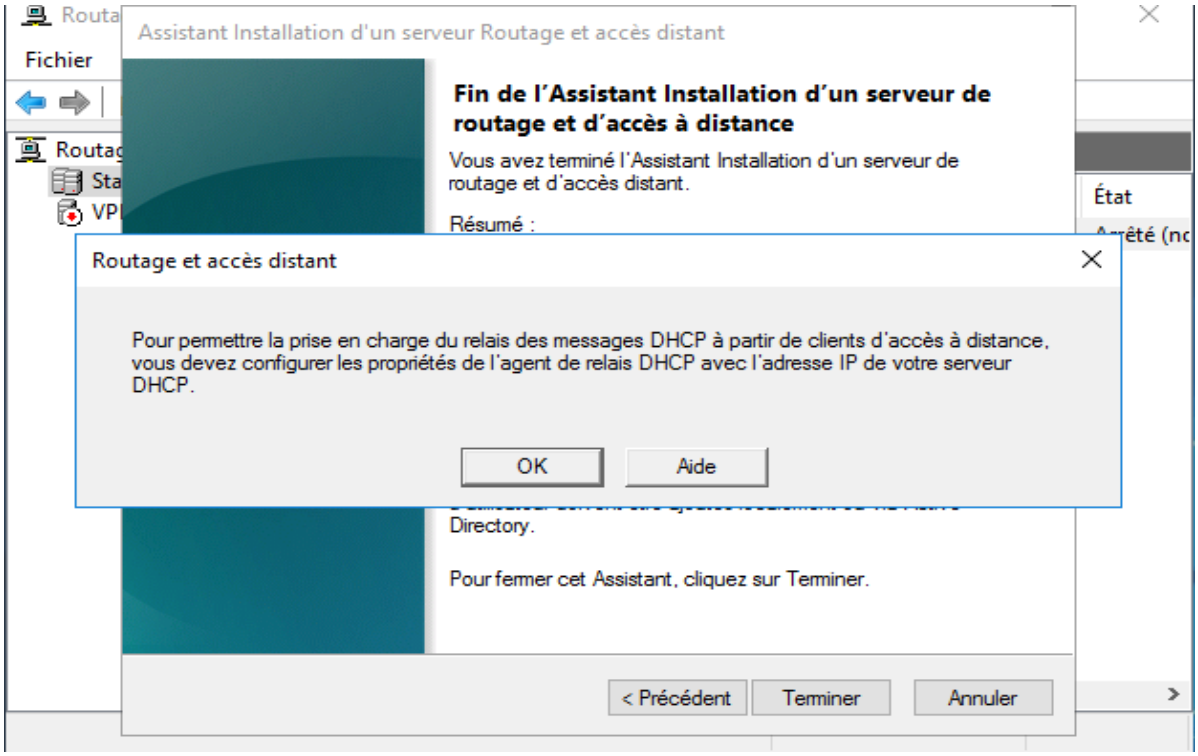

Figure 91 : Demande de configuration D'agent relais DHCP.

22. Enfin, notre serveur s'initialisera et démarrera le service

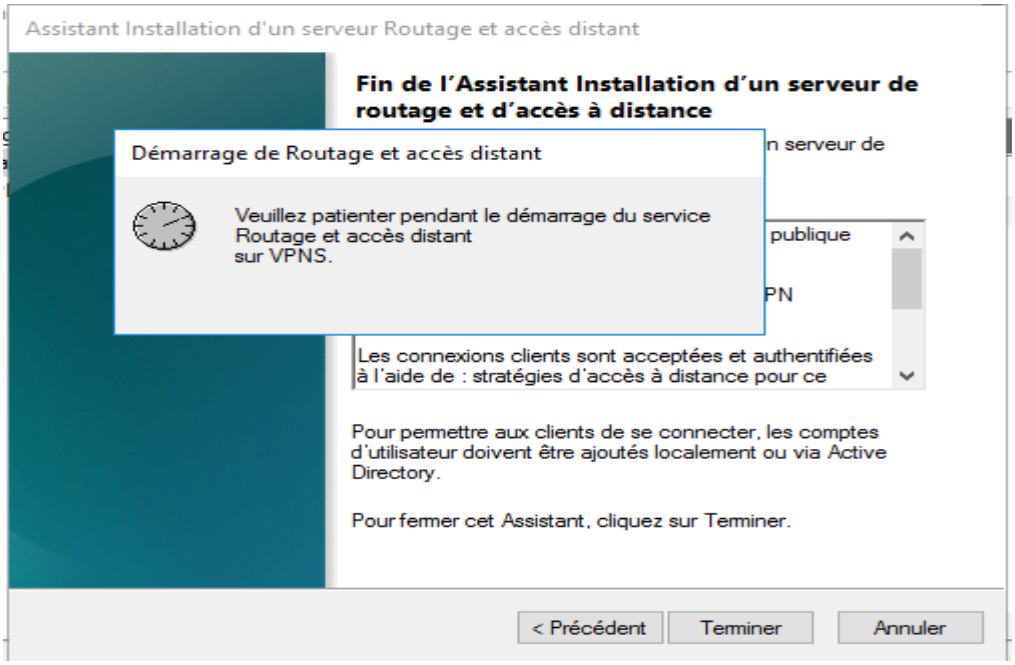

Figure 92 : Fin d'installation VPN.

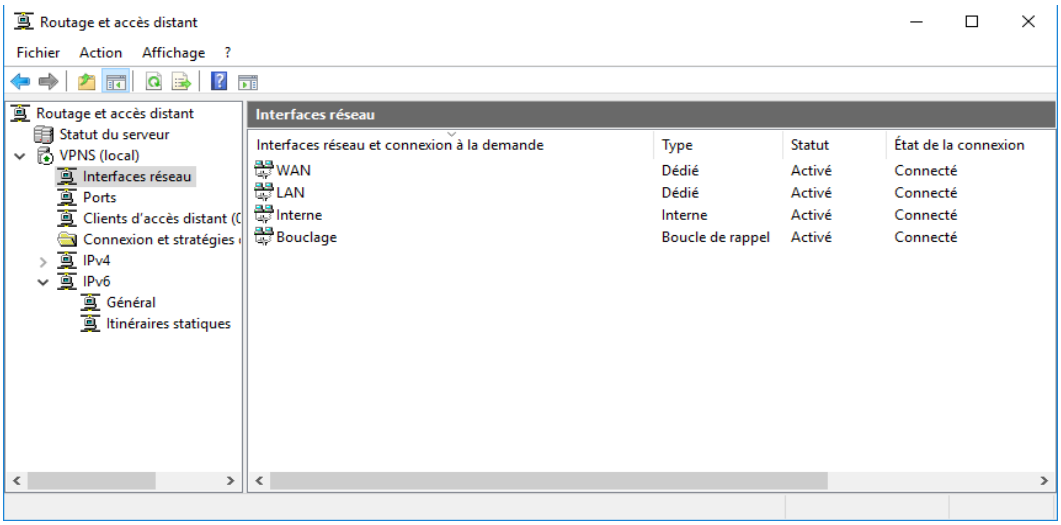

Figure 93 : Démarrage de serveur VPN.

23. Configuration d'agent de relais DHCP, Routage ouvert et accès à distance. On développe le serveur. Puis Clic droit sous IPv4 général et on sélectionne Nouveau protocole de route …

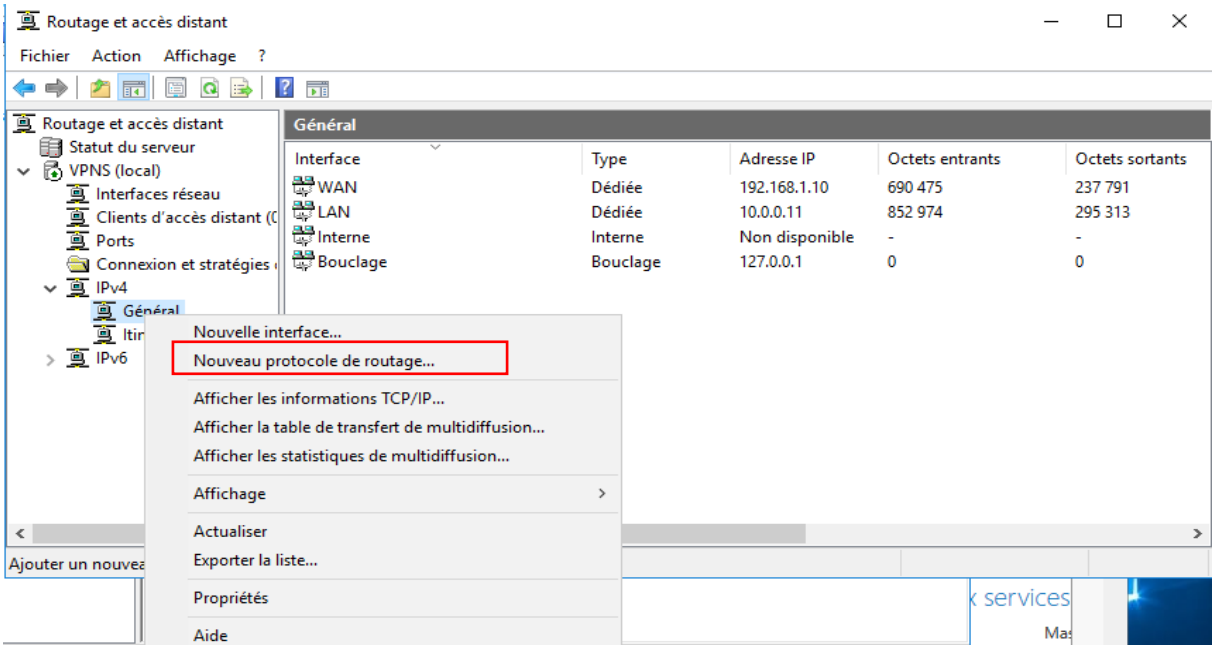

Figure 94 : Création de protocole agent de relais DHCP.

24. Dans la liste des protocoles de routage : on clique sur **Agent de relais DHCP**. Puis on clique sur OK. Le protocole est ajouté

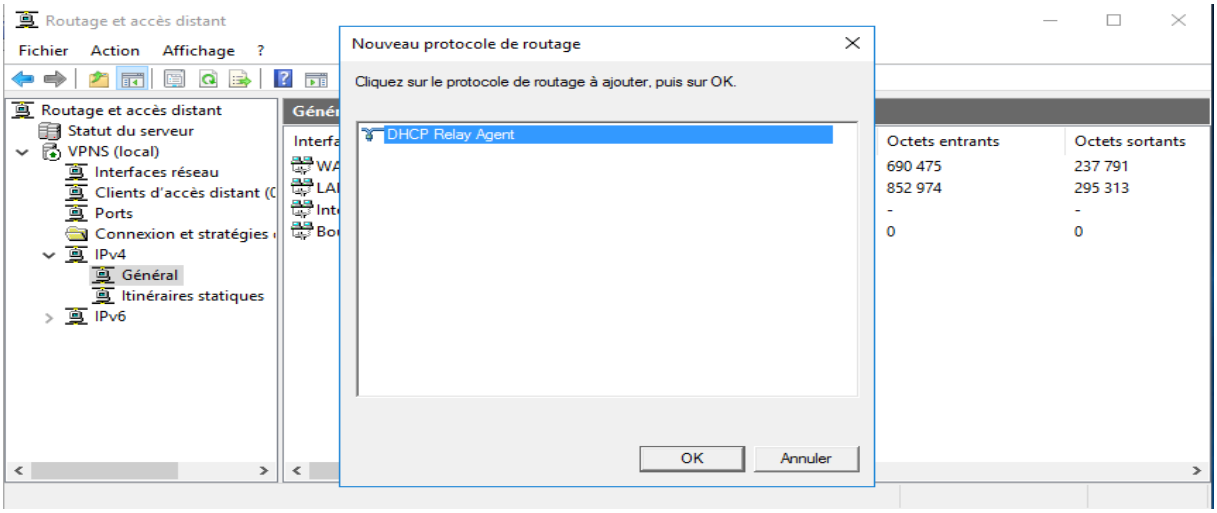

Figure 95 : Ajout d'agent de relais.

25. Clic droit sur Agent de relais DHCP et on sélectionne Nouvelle interface …Puis Dans la liste des interfaces, on sélectionne l'interface du réseau LAN et on clique sur OK. Lorsque les propriétés de la nouvelle interface apparaissent, cliquez sur OK (fenêtre 2)

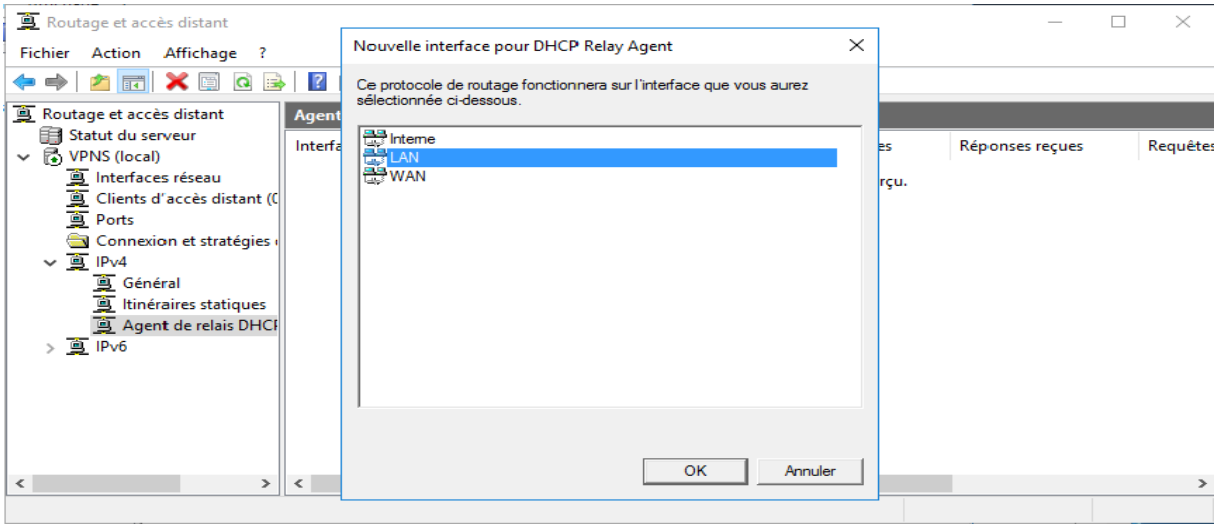

Figure 96 : Ajout d'interface LAN a l'agent de relais.

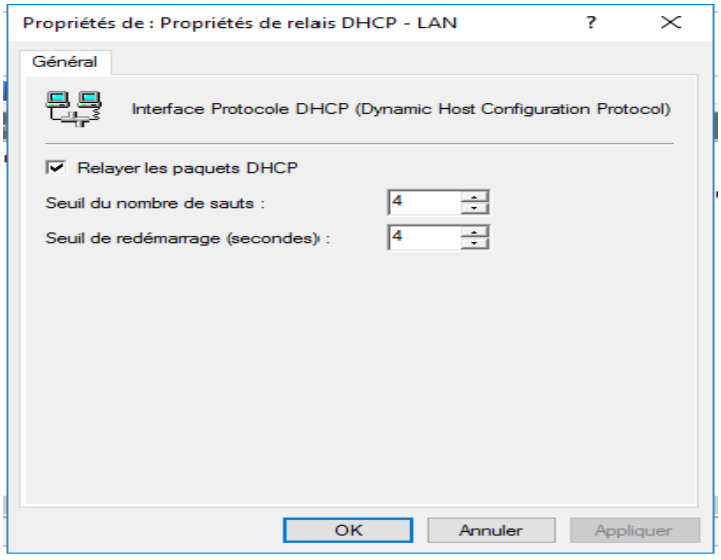

Figure 97 : Propriétés de l'interface LAN.

26. Du même pour l'interface réseau WAN

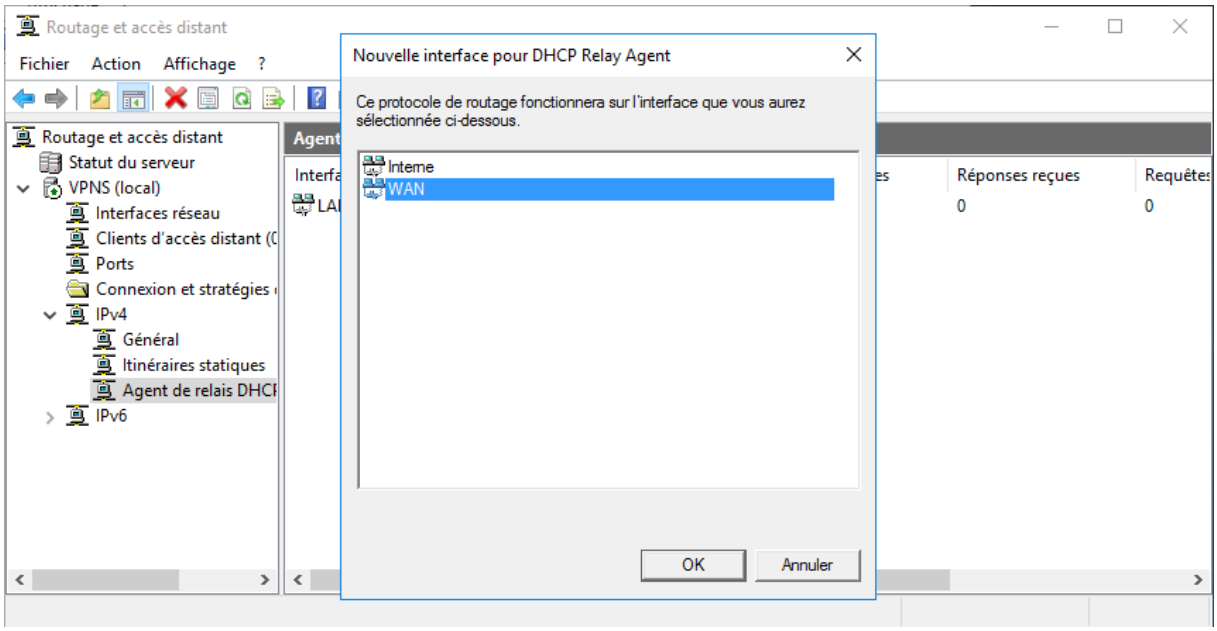

Figure 98 : Ajout de l'interface WAN a l'agent de relais.

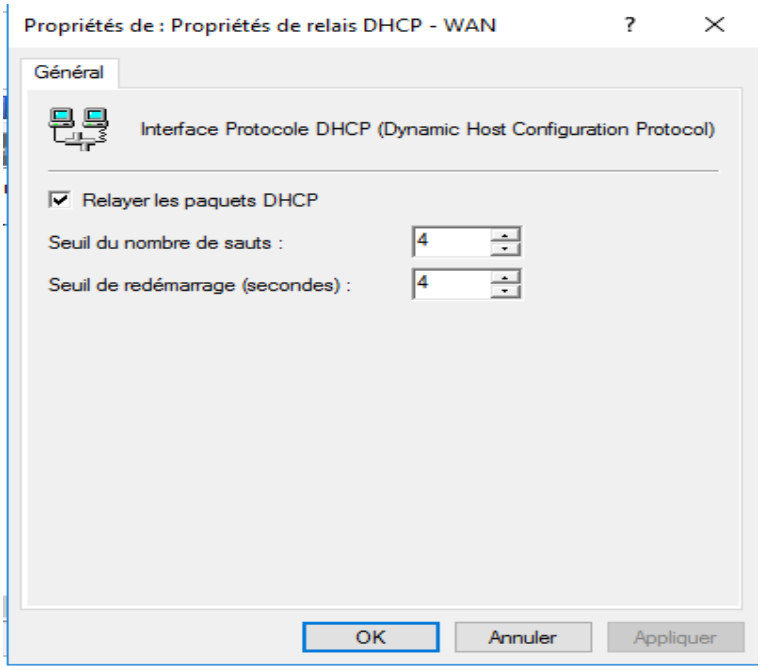

Figure 99 : Propriétés de l'interface WAN.

27. Un clic droit *Agent de relais DHCP* et on clique **propriétés puis** on ajoute l'adresse IP du serveur DHCP et on clique OK.

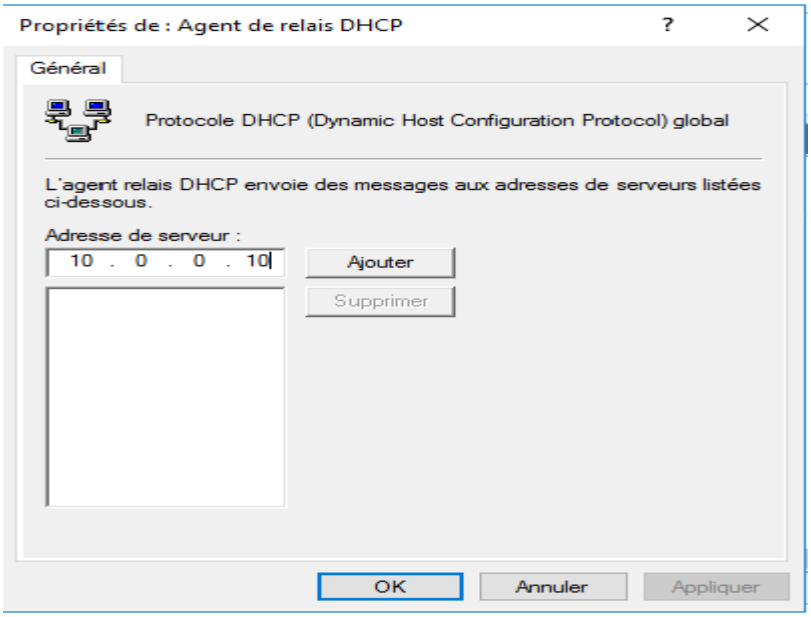

Figure 100 : L'adresse d'IP de l'agent de relais.

3.3.3.5. Installation et création de stratégie NPS

1. Maintenant, on va installer le serveur de stratégie réseau (NPS) pour le traitement des demandes de connexion envoyées par le serveur VPN. Dans la console « Routage et accès distant », on fait un clic droit sur « Connexion et stratégies d'accès à distance », puis on clique sur « Lancer NPS ».

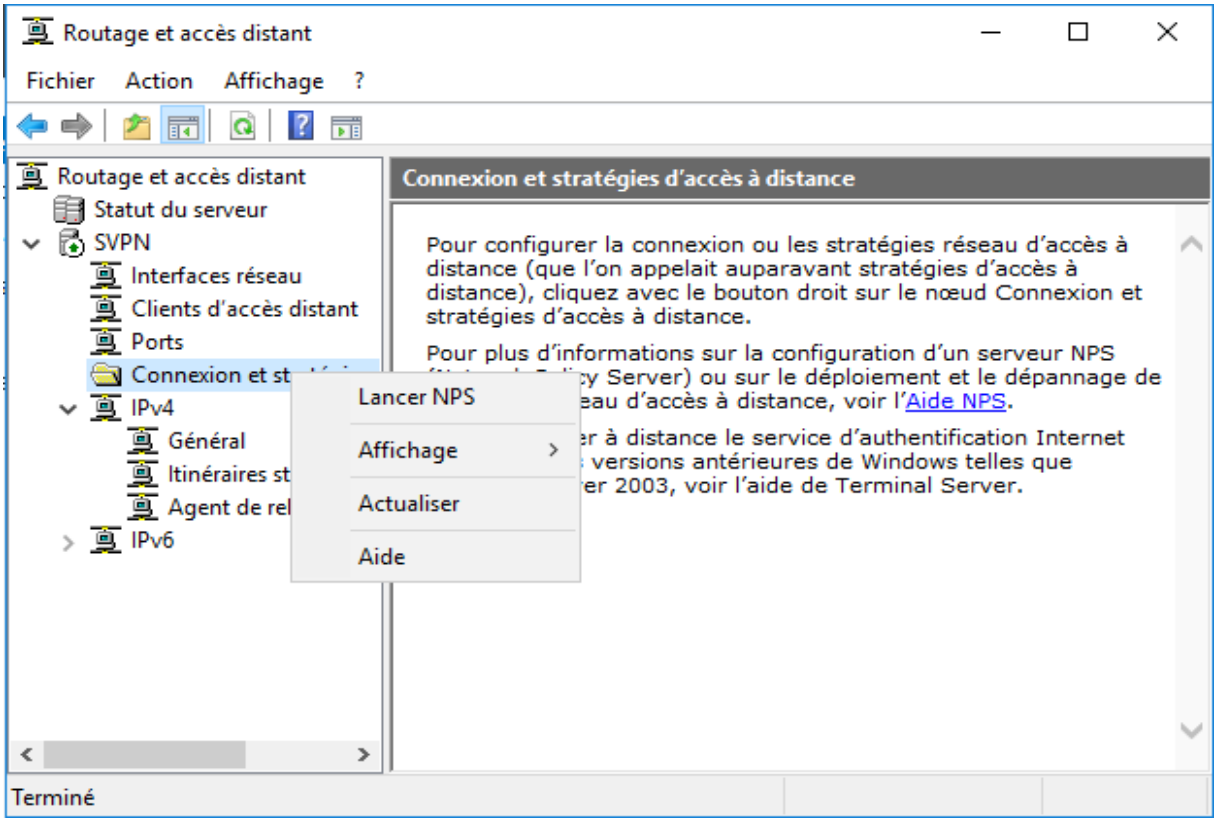

Figure 101 : Lancement de service NPS.

NPS est composé de 3 parties :

- Gestion (gestion du réseau, NAP...)
- Stratégie réseau : permet de choisir qui peut et qui ne peut pas accéder au réseau, se connecter au serveur VPN, …selon des conditions. (La partie utilisée dans notre configuration)
- Filtres IP : permet d'autoriser et/ou bloquer certains protocoles et/ou certains ports.

2. Avant de créer notre stratégie on va créer un groupe d'utilisateur dans notre domaine où les utilisateurs de ce groupe auront le droit d'utiliser le VPN. (Dans machine serveur DC)

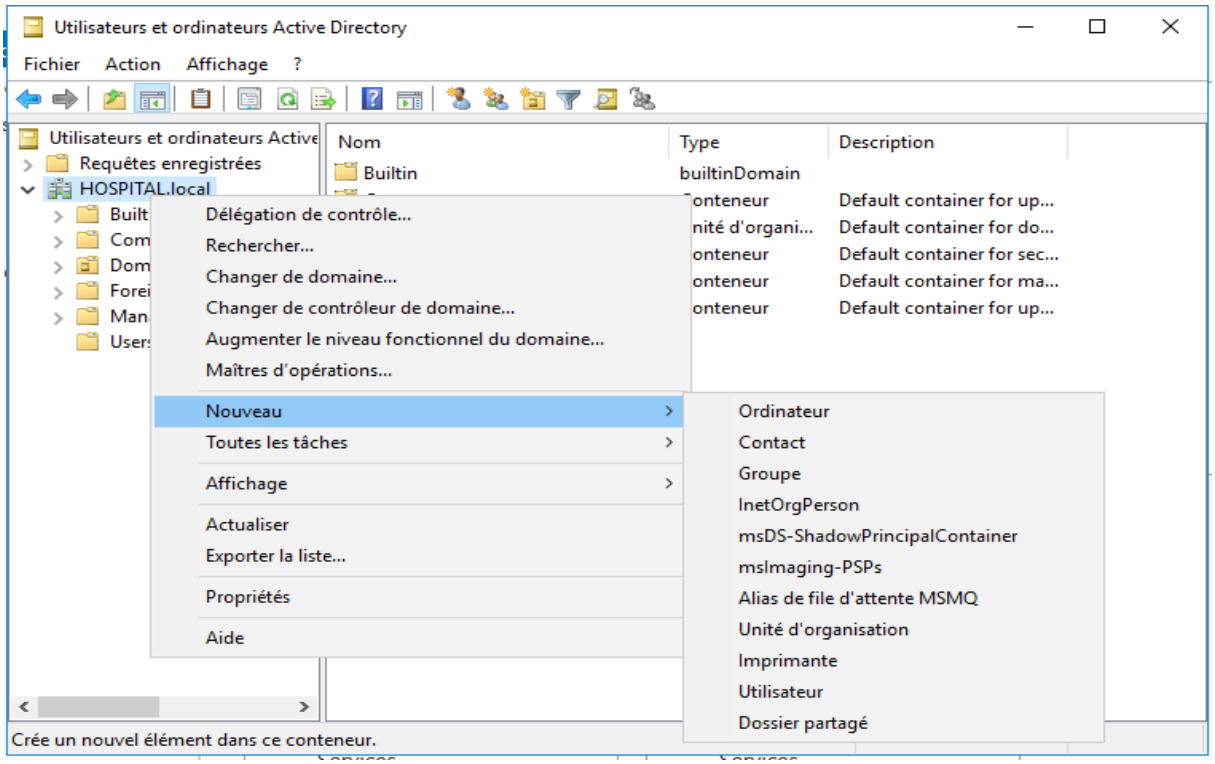

Figure 102 : Création du groupe dans le Domaine Hôpital.

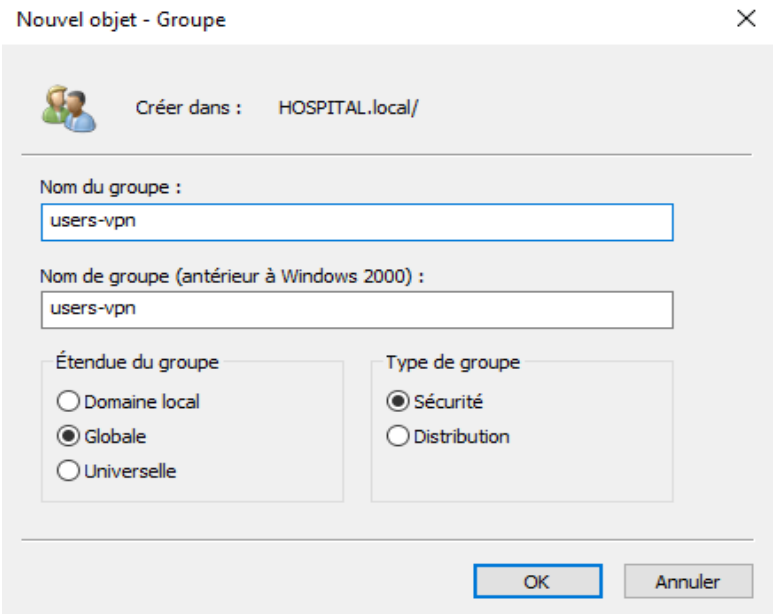

Figure 103 : Nom du groupe.

3. On associe un utilisateur au groupe users-vpn. Dans le dossier « **utilisateur et ordinateur Active Directory** », on choisit le dossier **« users »**, on fait clic droit sur un utilisateur donné pour l'ajouter à un groupe afin d'être autorisé par le VPN à accéder au système et on clique OK

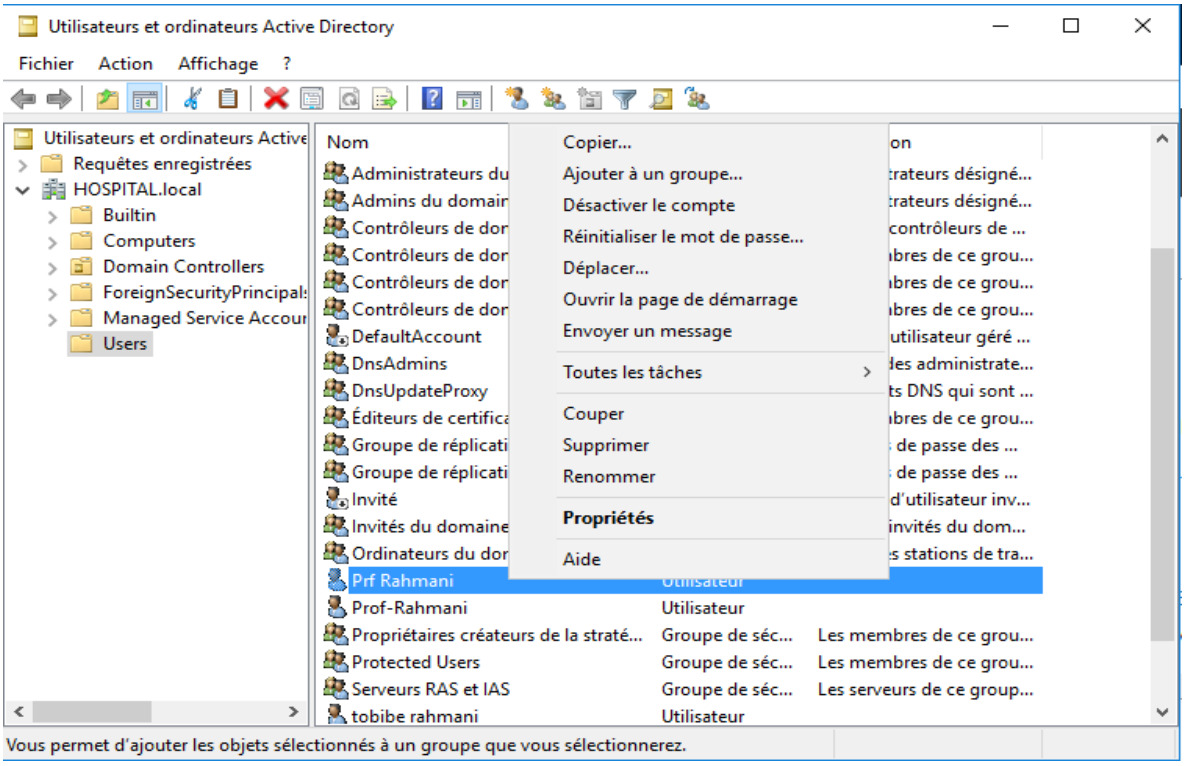

Figure 104 : Associe un utilisateur au groupe.

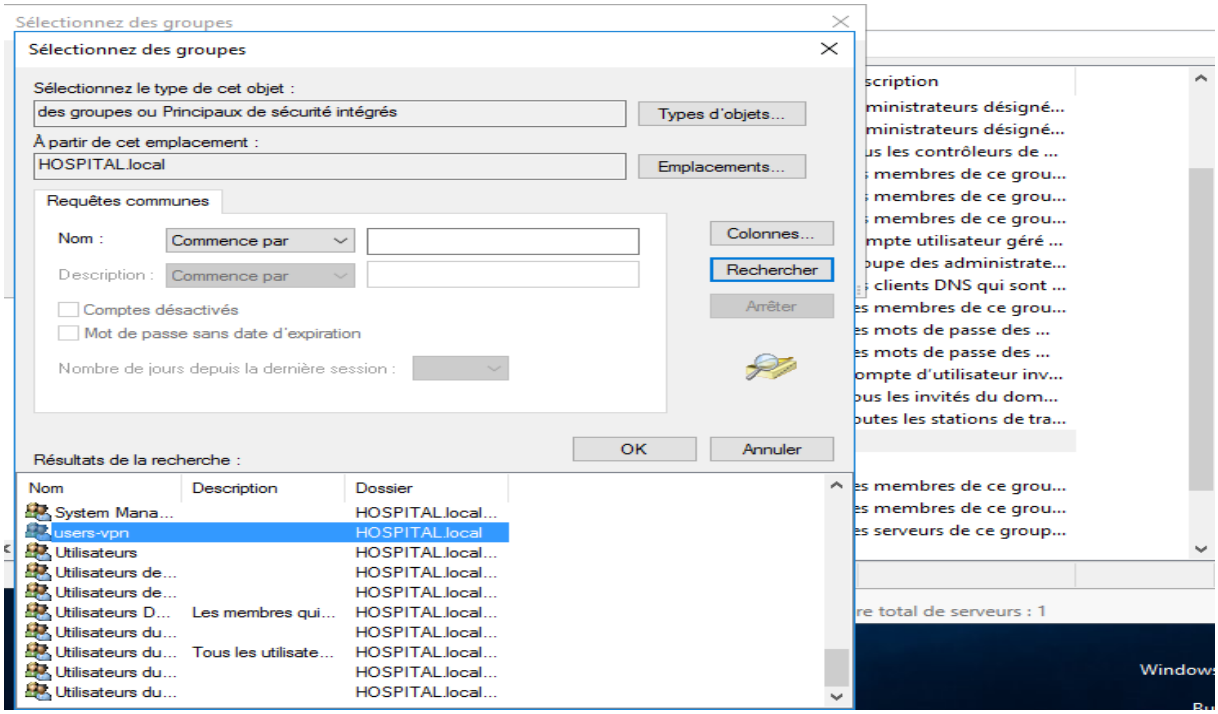

Figure 105 : Recherche du groupe.

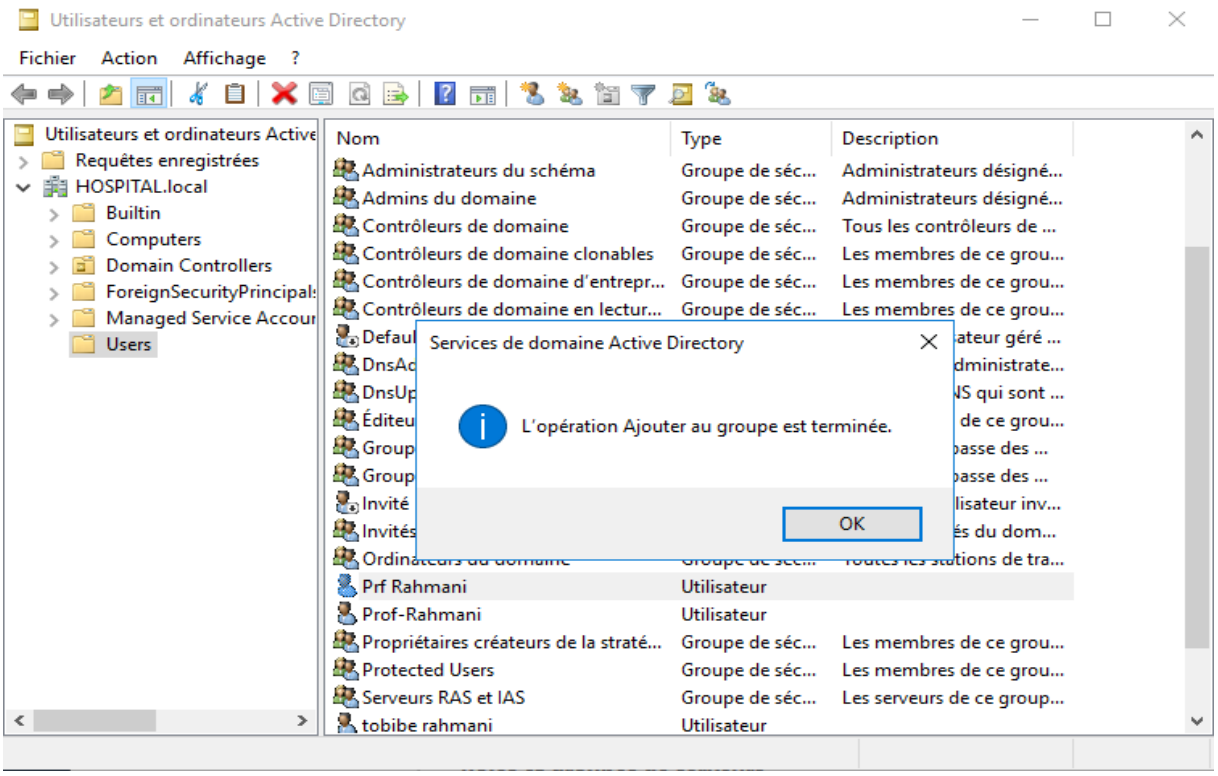

Figure 106 : Fin d'ajout d'utilisateur au groupe.

4. On va créer une nouvelle stratégie réseau, on fait un clic droit sur « Stratégie réseau » et on clique sur « Nouveau »

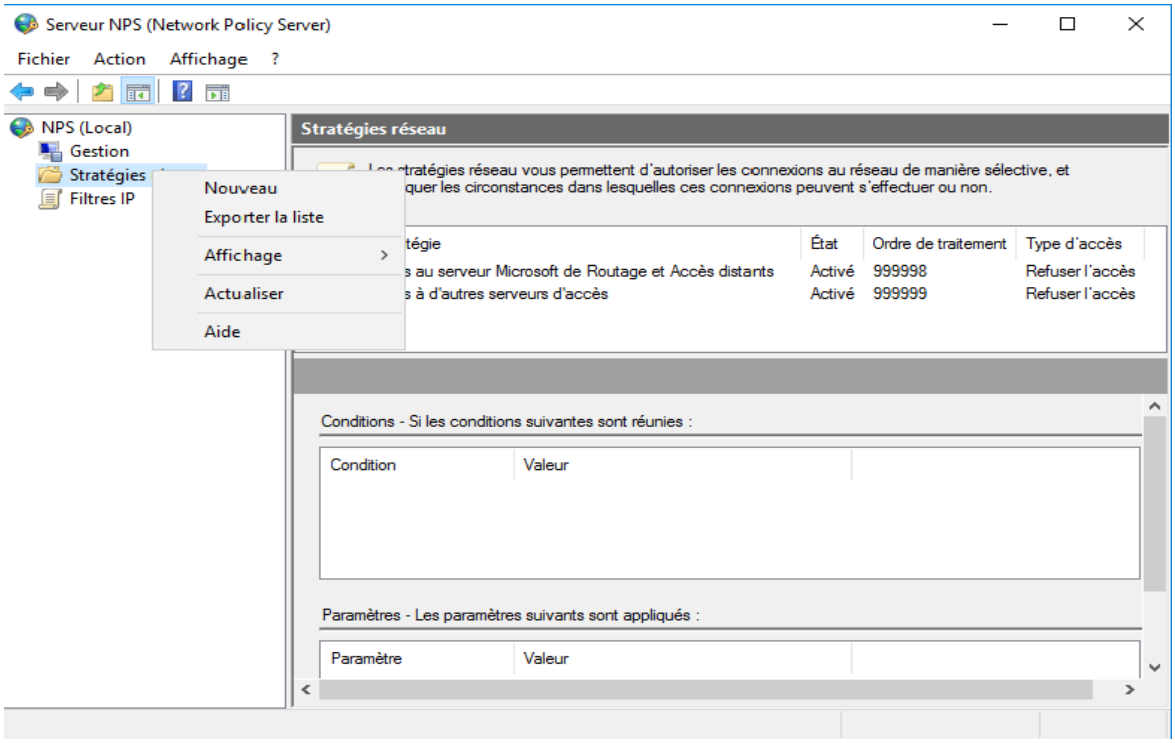

Figure 107 : Création d'une stratégie NPS.

5. On indique un nom pour cette nouvelle stratégie

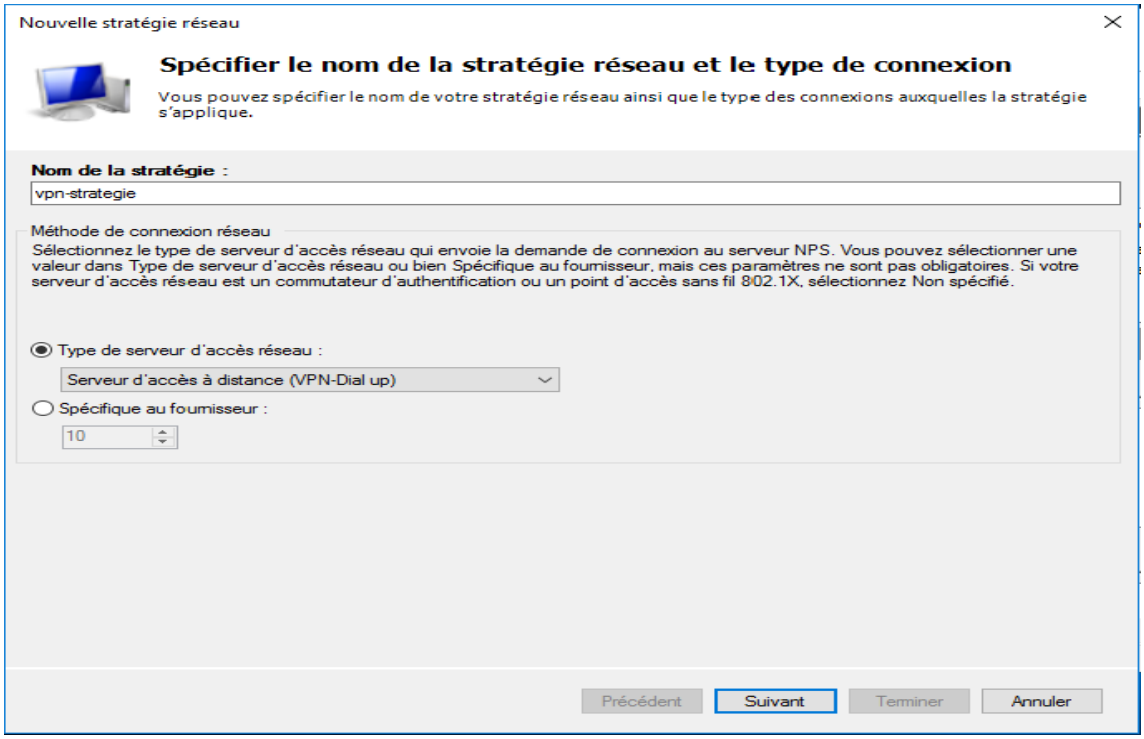

Figure 108 : Indication de nom de la stratégie.

6. On va autoriser les utilisateurs de l'Active directory à connecter à notre serveur VPN. Pour cela, on sélectionne « Groupes d'utilisateurs » et on clique sur Ajouter

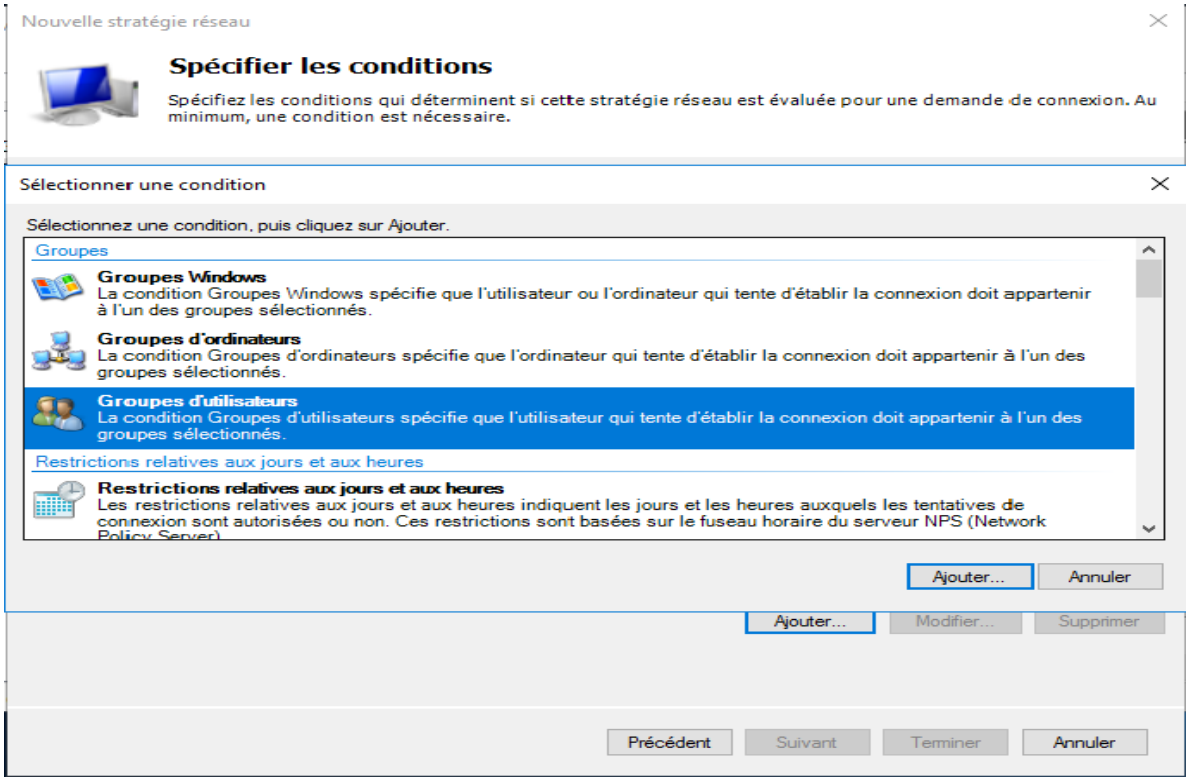

Figure 109 : Condition de stratégie.

7. On Clique sur « Ajouter des groups », on clique « avancé » puis on sélection le groupe

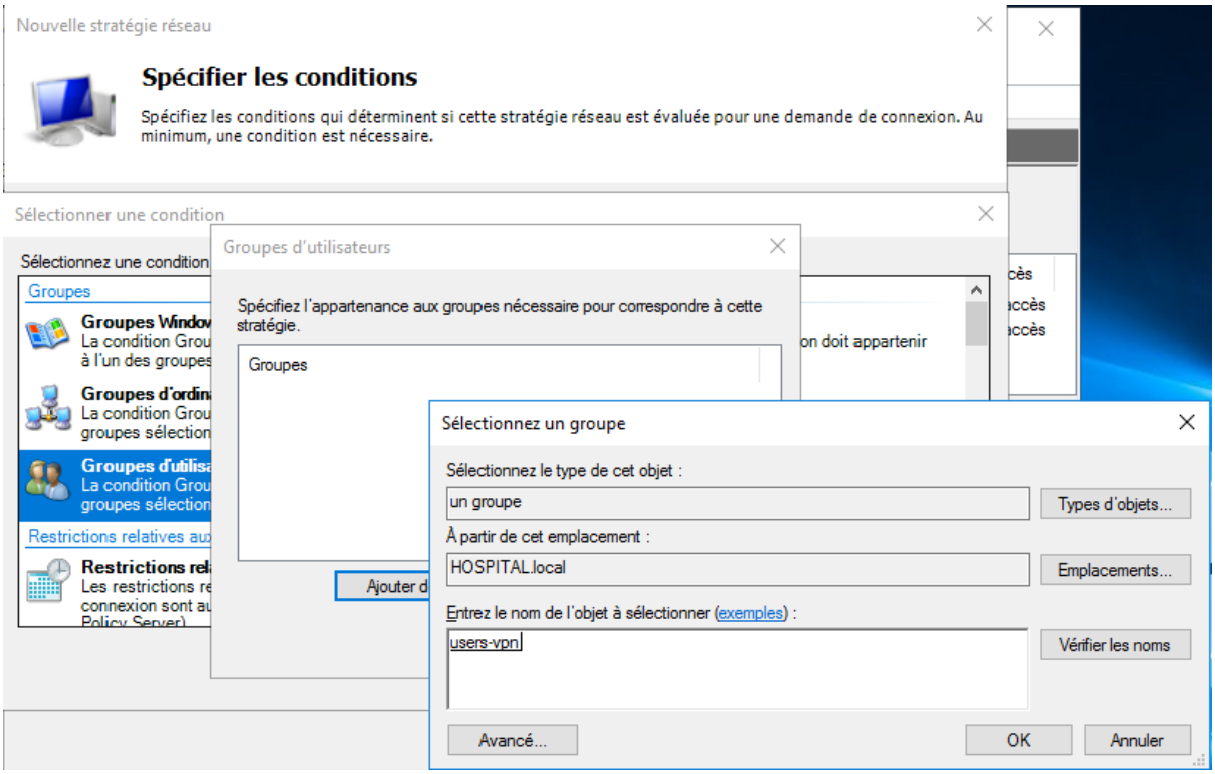

Figure 110 : Ajouter groupe d'utilisateur dans les conditions de stratégie.

8. Maintenait, cette stratégie de sécurité s'appliquera aux utilisateurs du domaine, on clique sur Suivant

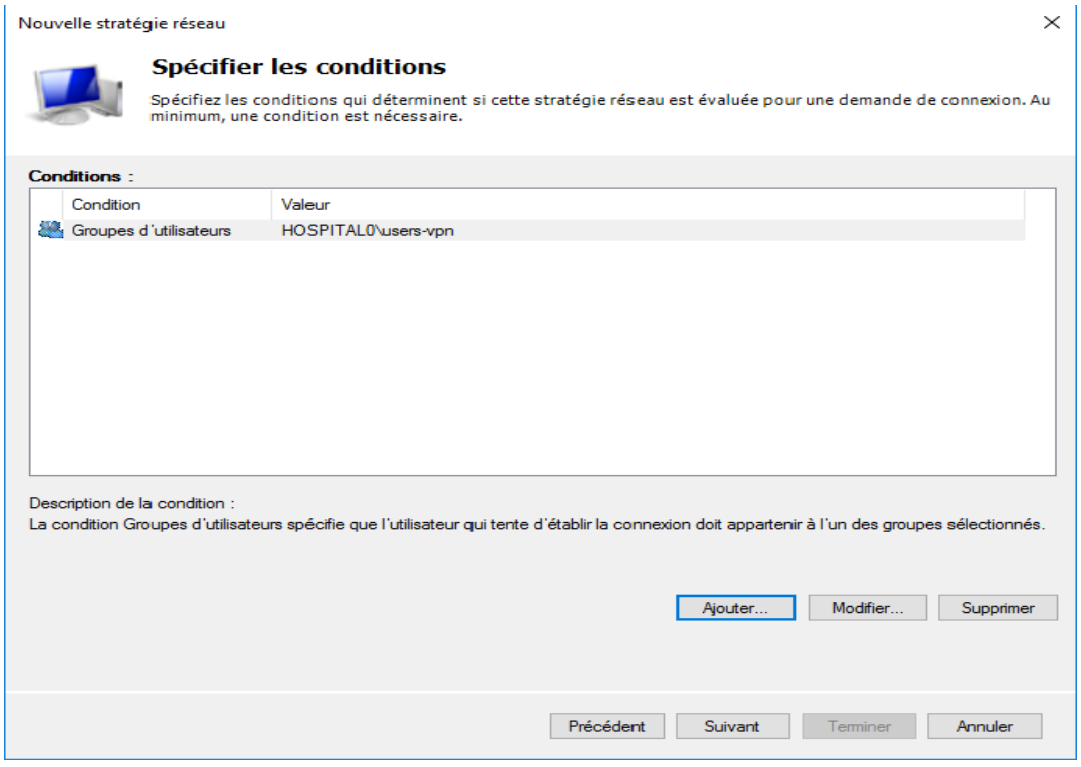

Figure 111 : Fin d'ajout du groupe à la stratégie.

9. On sélection « Accès accordé » et on clique sur suivant

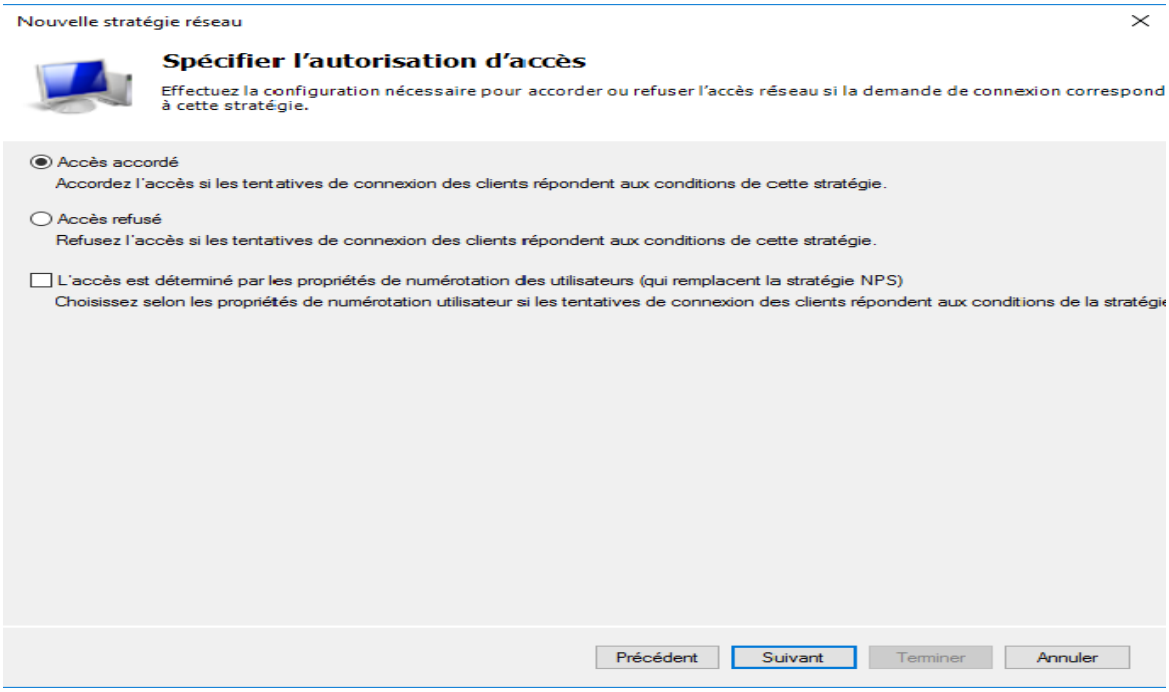

Figure 112 : Autoriser l'accès à la stratégie.

10. Pour les protocoles EAP on clique sur Ajouter

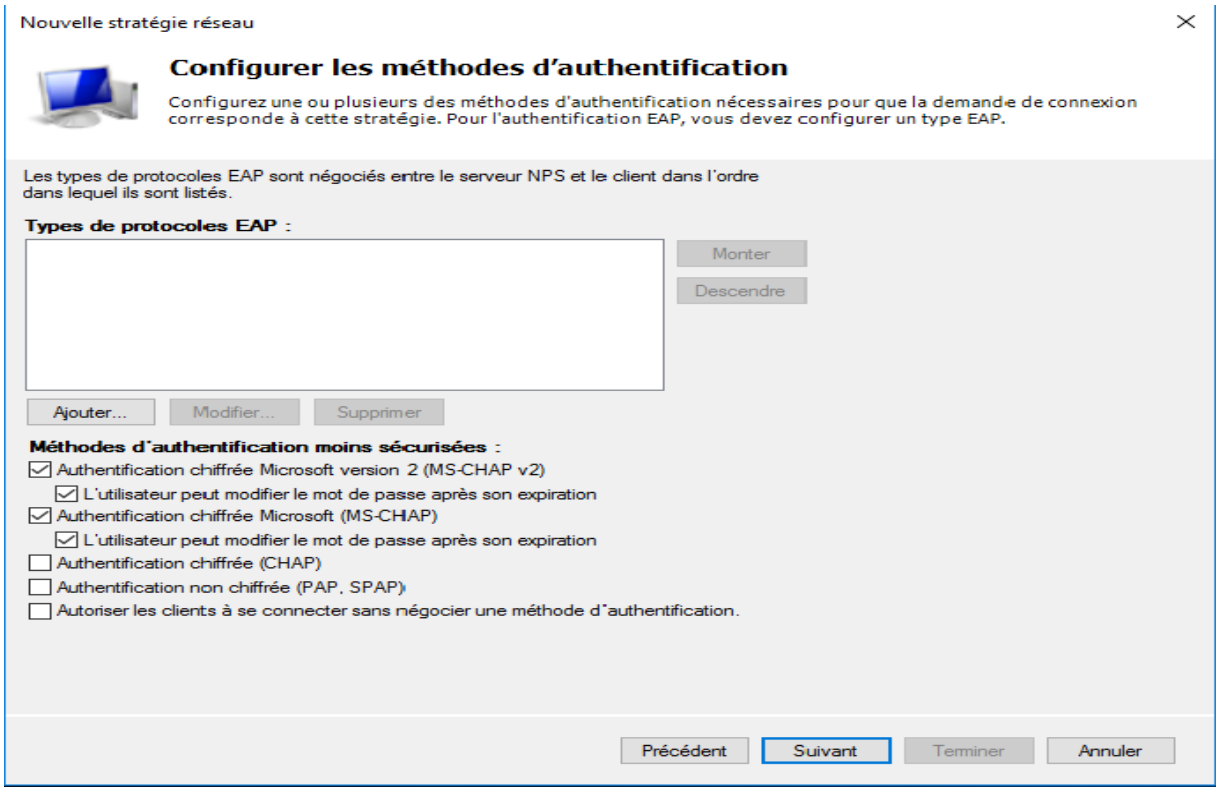

Figure 113 : Les protocoles d'authentification de la stratégie NPS.

11. Sur l'écran « Ajouter des protocoles EAP », on ajoute PEAP et EAP-MSCHAP un par un

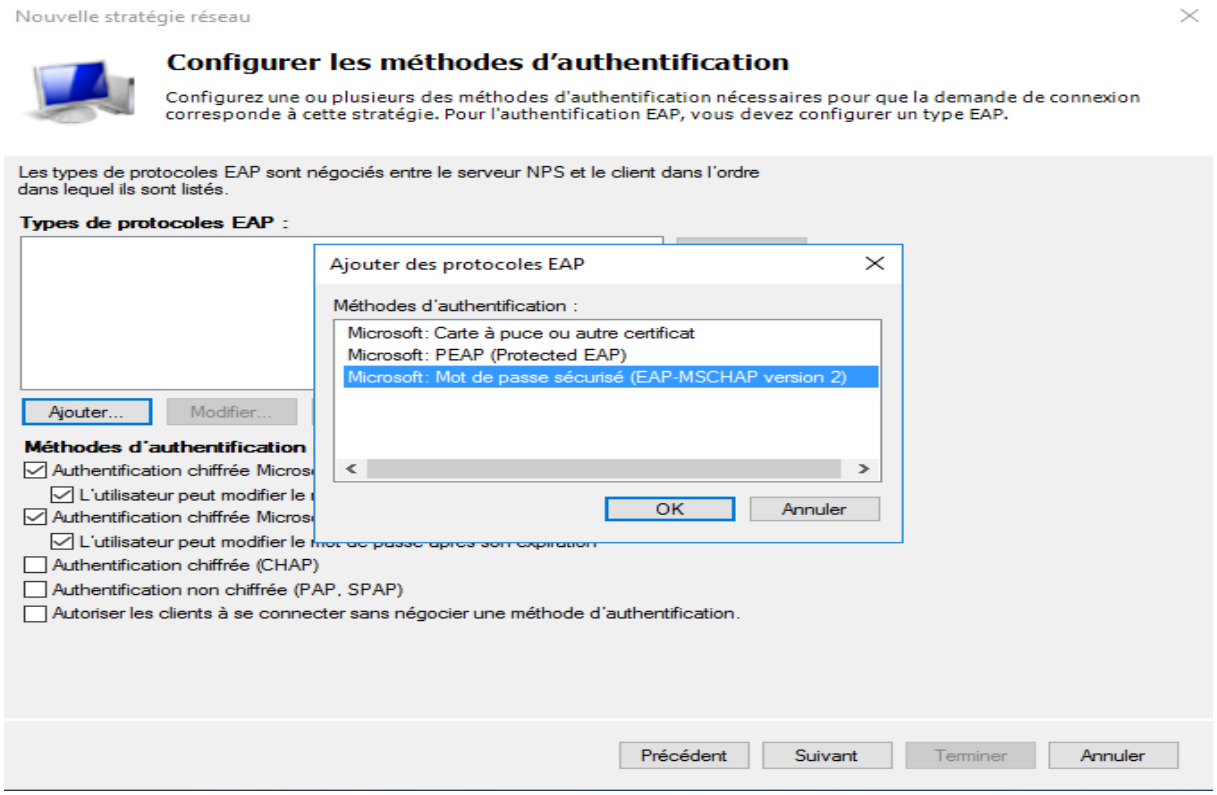

Figure 114 : Ajout des protocoles EAP.

12. Pour la partie contrainte, on peut définir un temps d'inactivité après lequel la connexion sera automatiquement fermée. On peut aussi définir des restrictions relatives à la date et à l'heure.

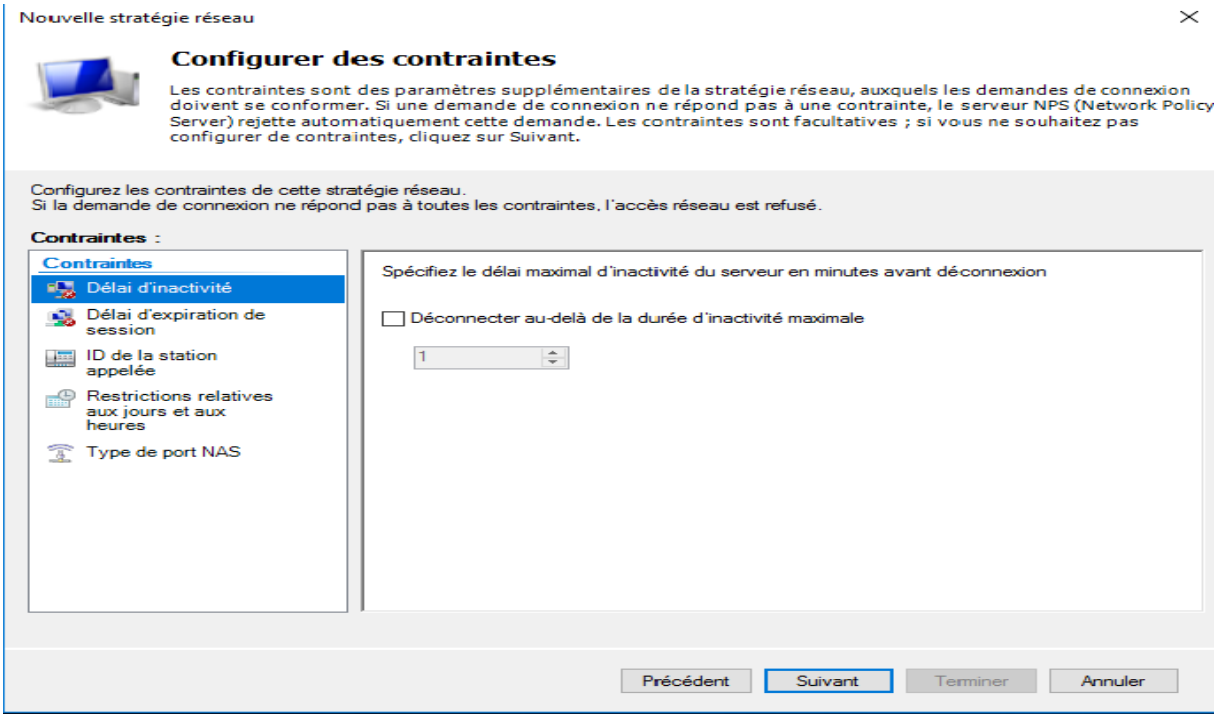

Figure 115 : Configuration des contraintes de stratégie.

13. On clique sur suivant

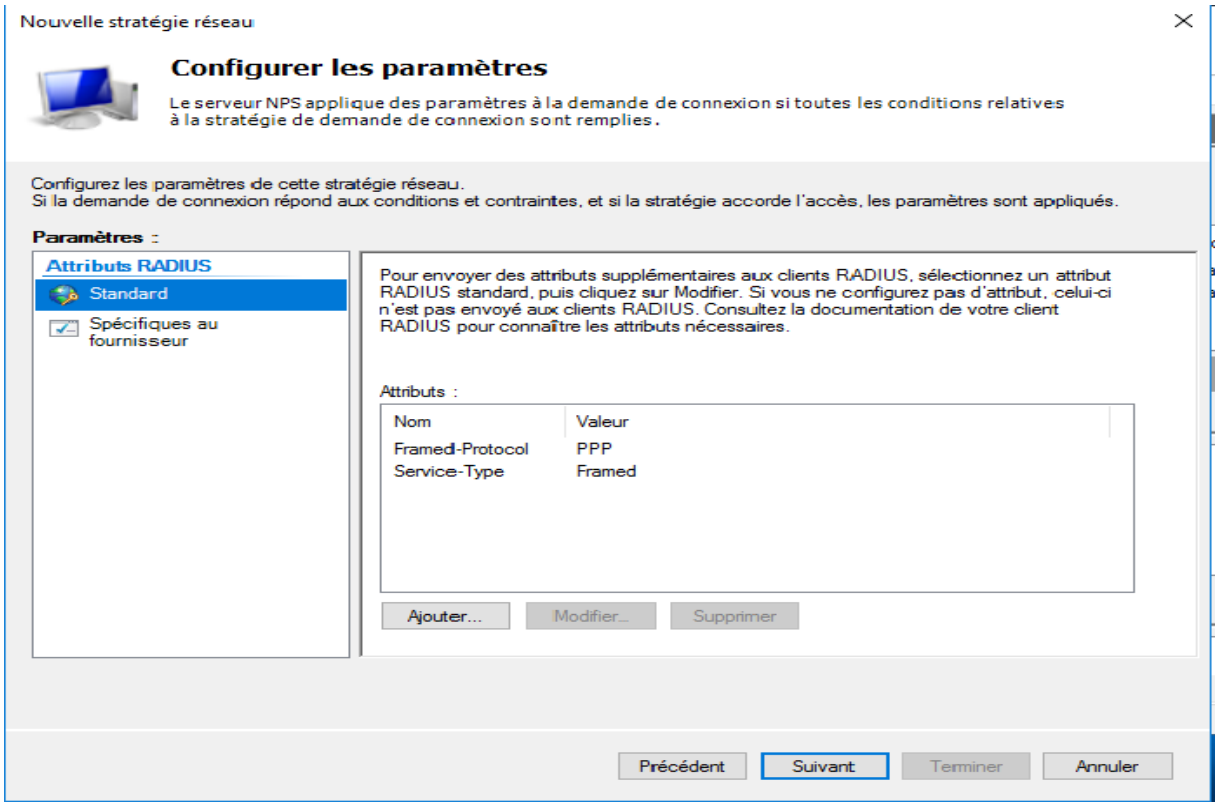

Figure 116 : Configuration des paramètres de la stratégie.

14. On clique sur terminé et notre stratégie est crée

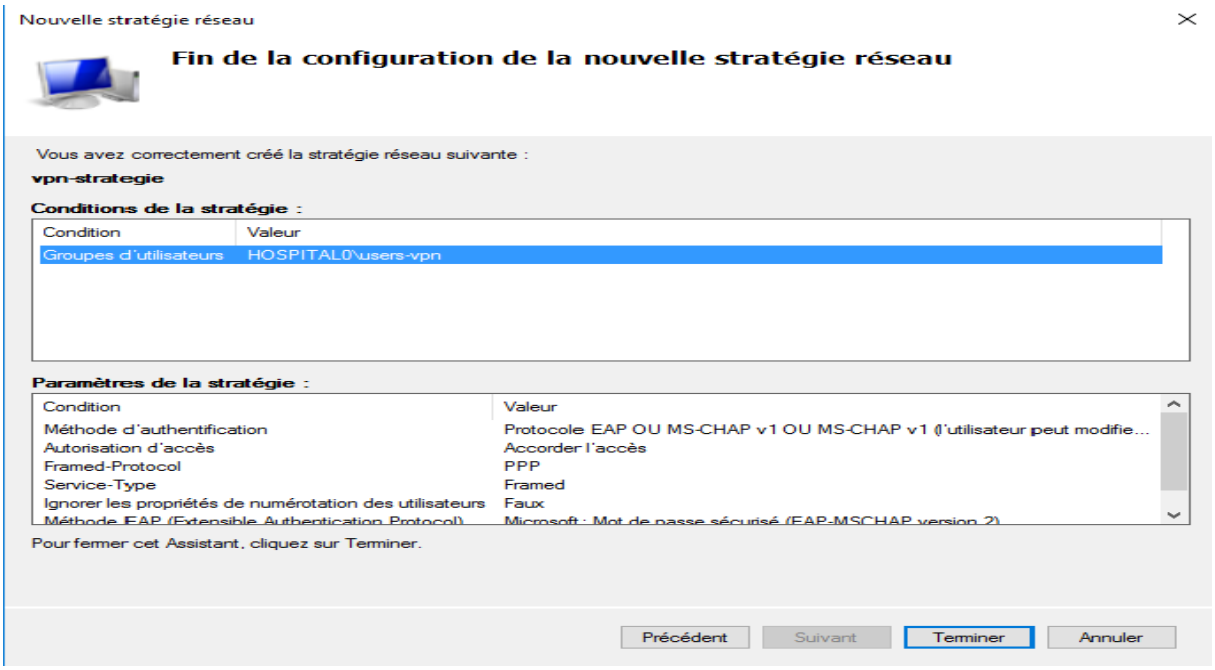

Figure 117 : Fin de configuration de la stratégie.

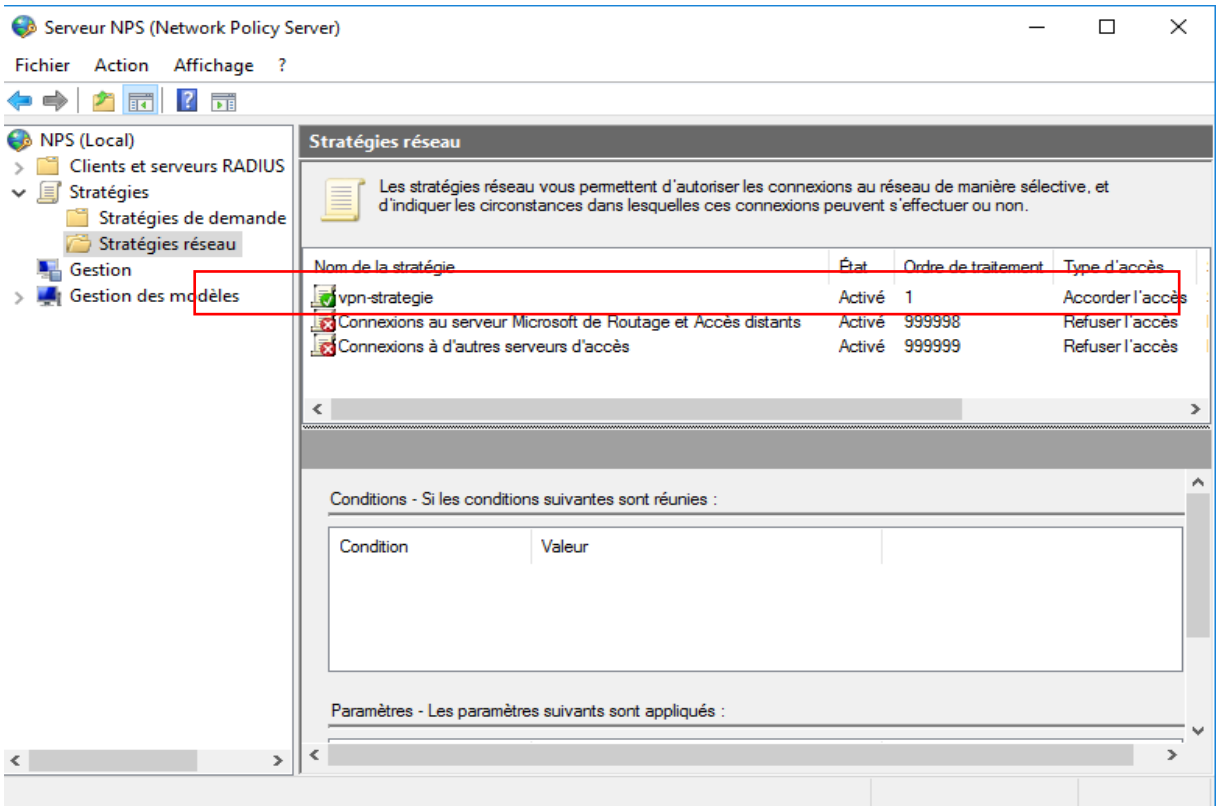

Figure 118 : Stratégie crée.

15. On va vérifier si les ports d'accès distance sont autorisés dans le pare feu de notre serveur VPN si ce n'est pas le cas on les autorise

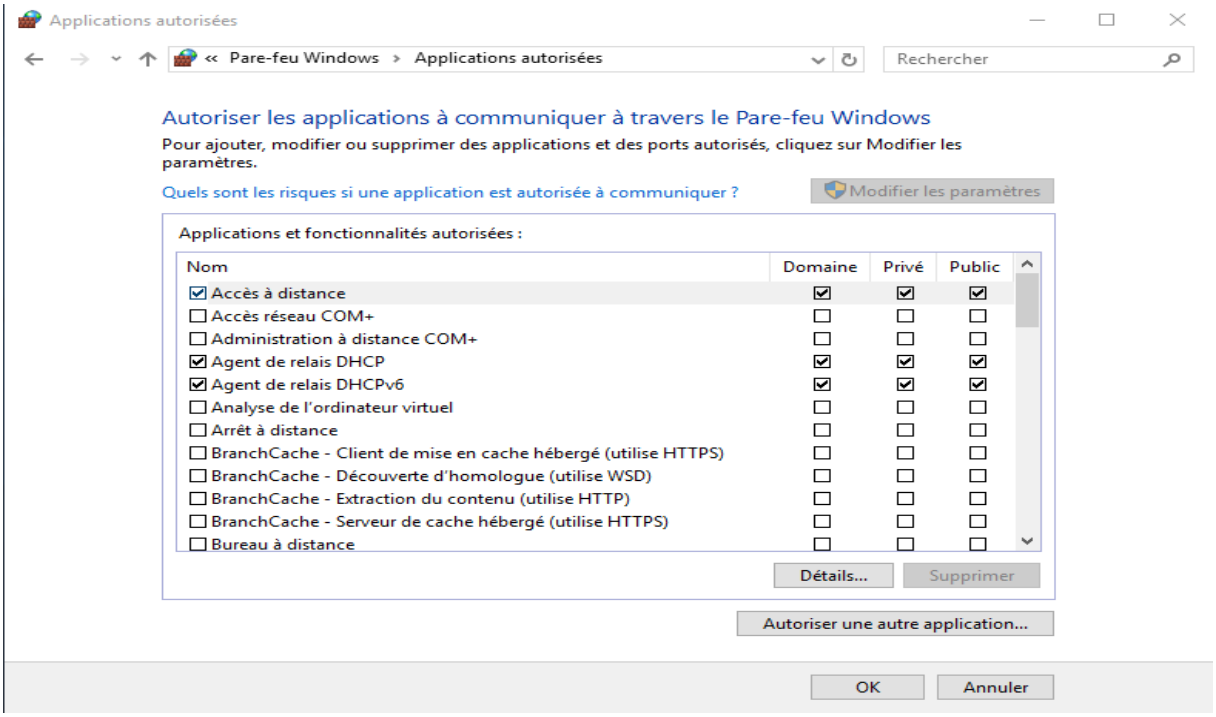

Figure 119 : Autorisation des ports.

3.3.3.6. Configuration du client VPN

Maintenant que notre serveur est entièrement configuré, on va tenter de se connecter à notre serveur VPN.

1. Pour cela, sous Windows 8, on fait un clic droit sur l'icône réseau présente dans la barre des tâches et on clique sur « Ouvrir le centre Réseau et partage ».
   Ensuite, on clique sur le lien « Configurer une nouvelle connexion ou un nouveau réseau »

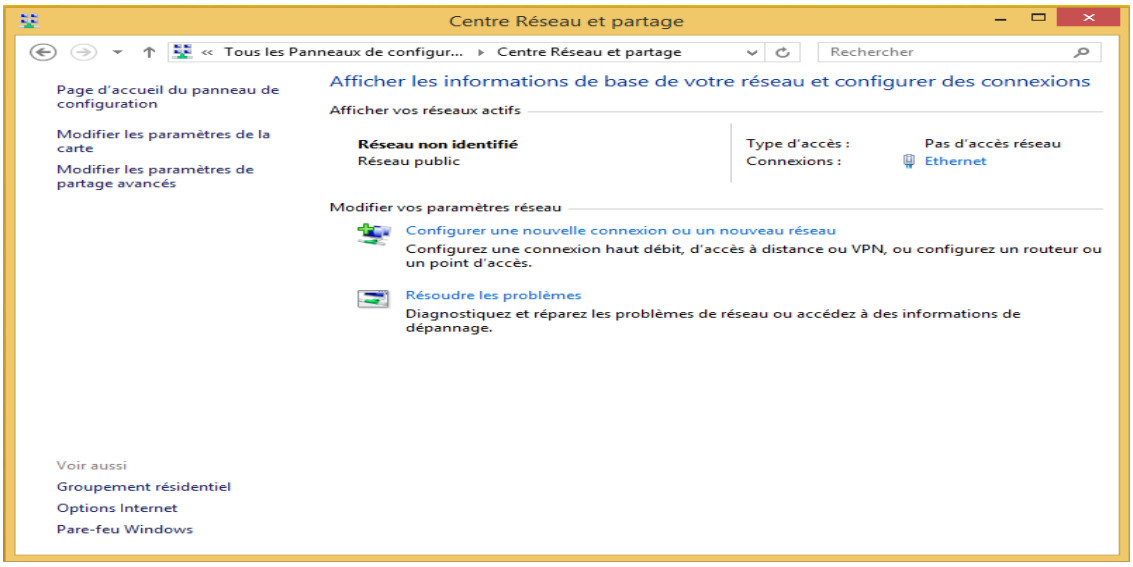

Figure 120 : Centre Réseau et partage Windows 8.

2. On sélectionne « Connexion à votre espace de travail » et on clique sur suivant :

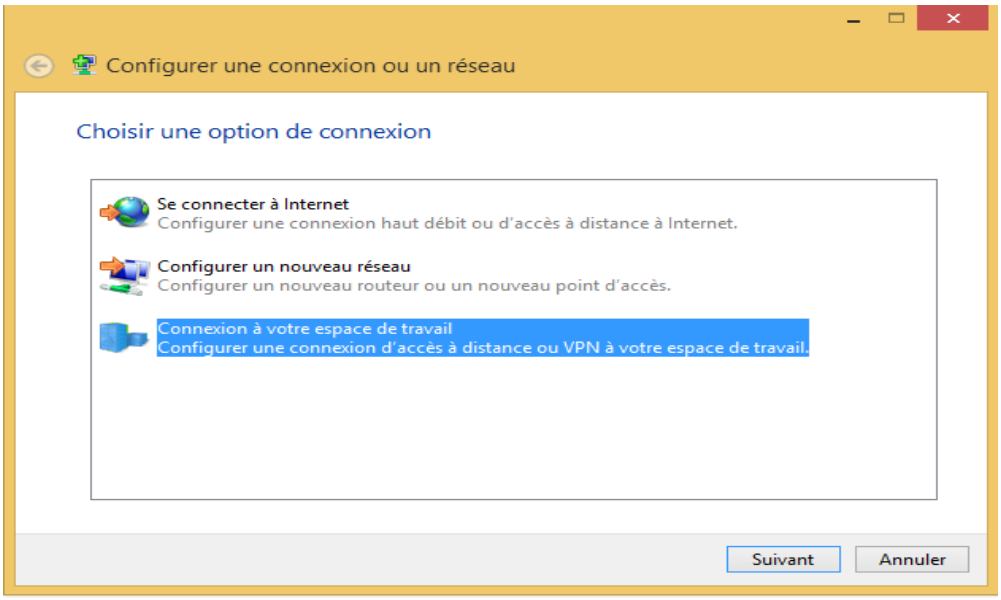

Figure 121 : Création d'une nouvelle connexion.

3. On clique sur « Utiliser ma connexion Internet (VPN) »

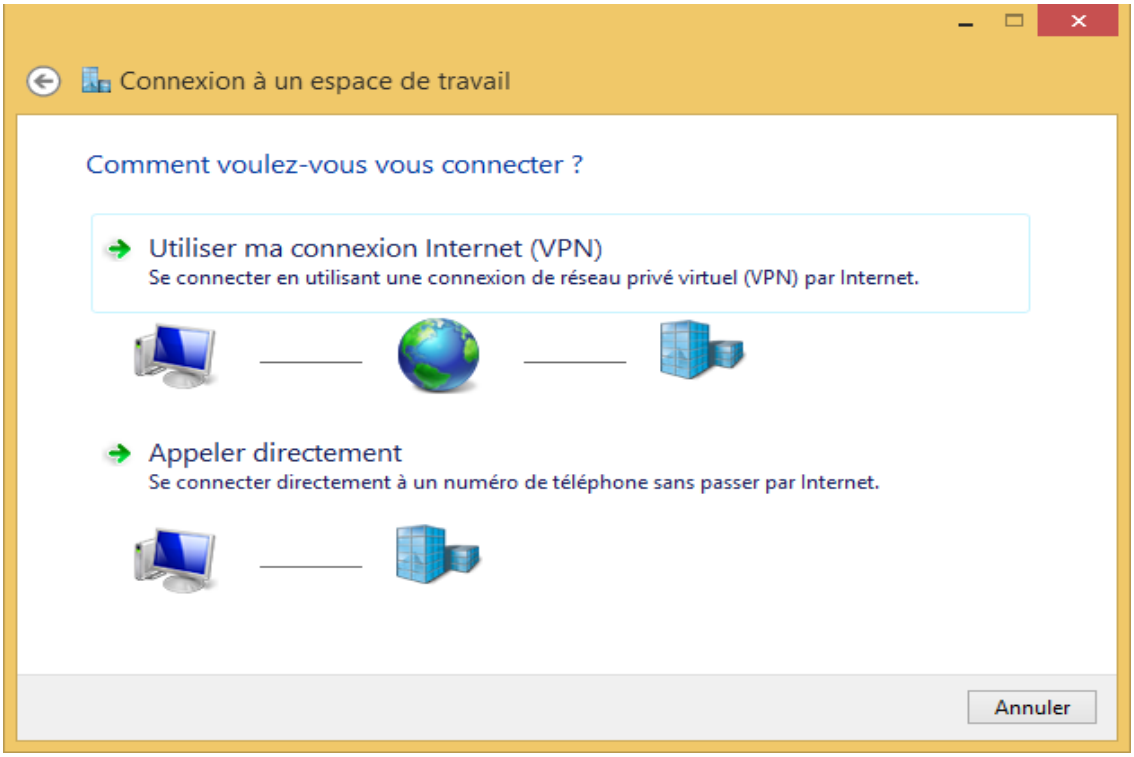

Figure 122 : Préciser type de connexion.

4. On indique l'adresse IP externe de notre serveur VPN

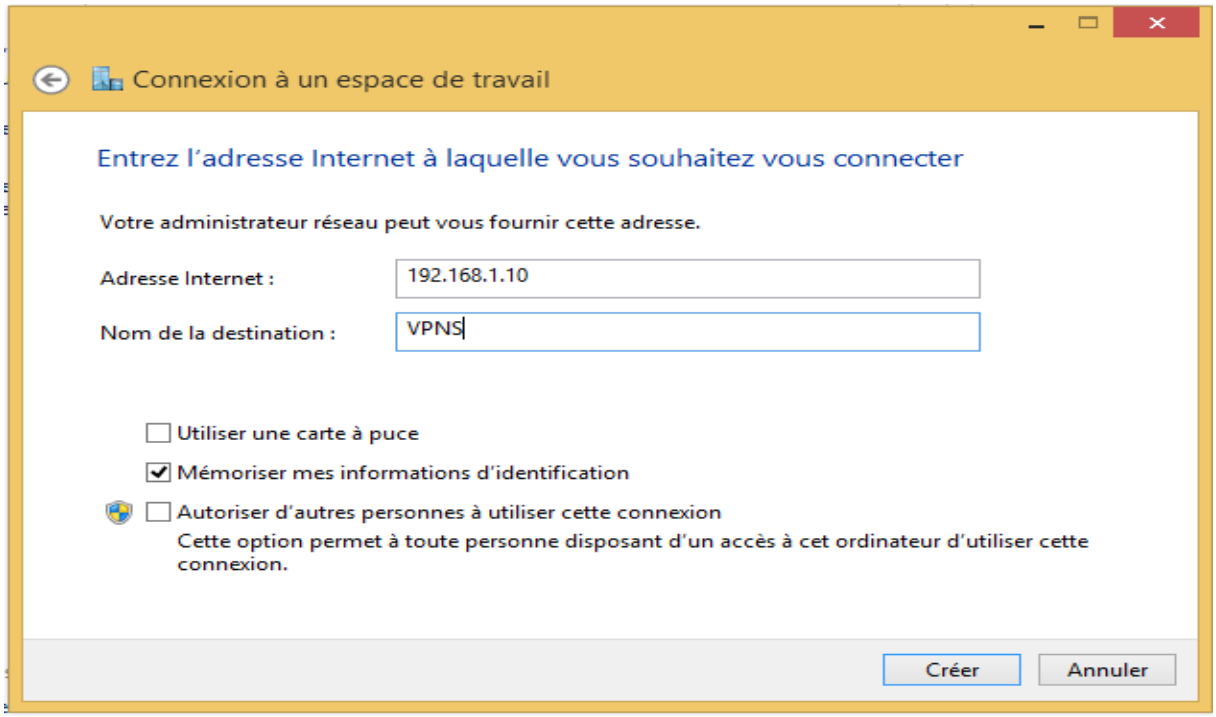

Figure 123 : Entrer adresse IP du serveur VPN.

5. Si on regarde dans nos connexions réseau, on verra qu'une nouvelle connexion réseau a apparu

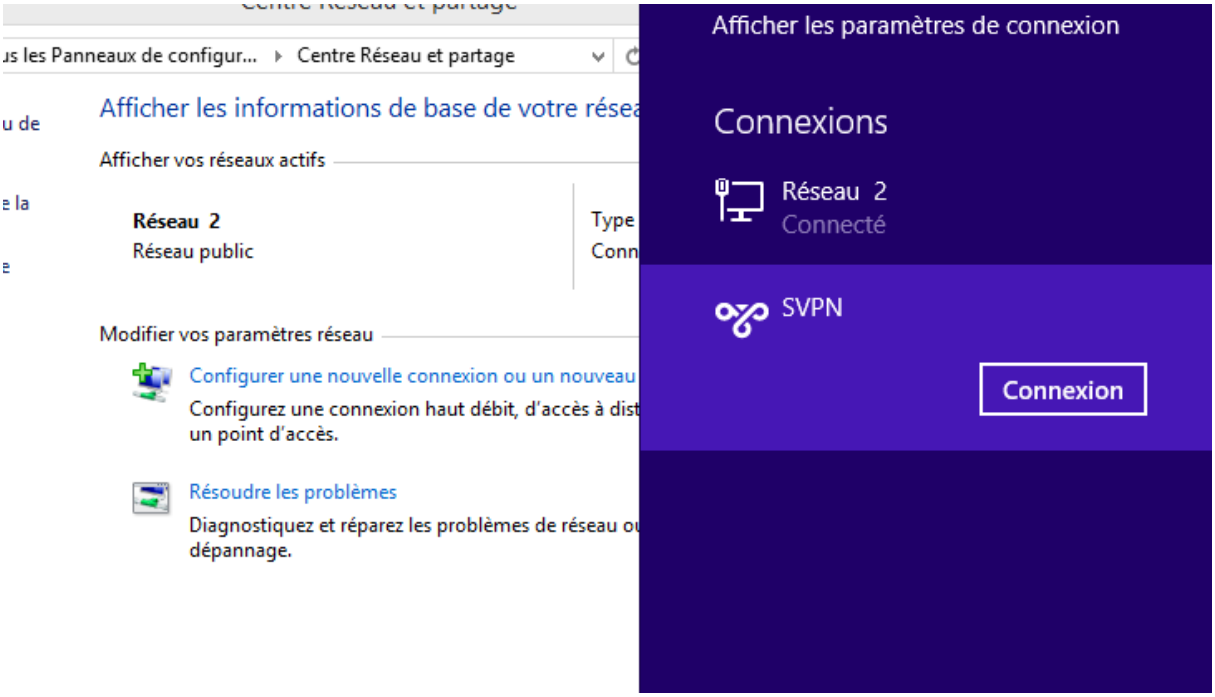

Figure 124 : Connexion crée.

3.3.3.7. Test

Dans ce test, on va accéder au Domaine en local à partir d'Internet via VPN, en utilisant un compte médecin

1. On ajoute le nom de Domaine dans le PC en local, puis on introduit le compte médecin.

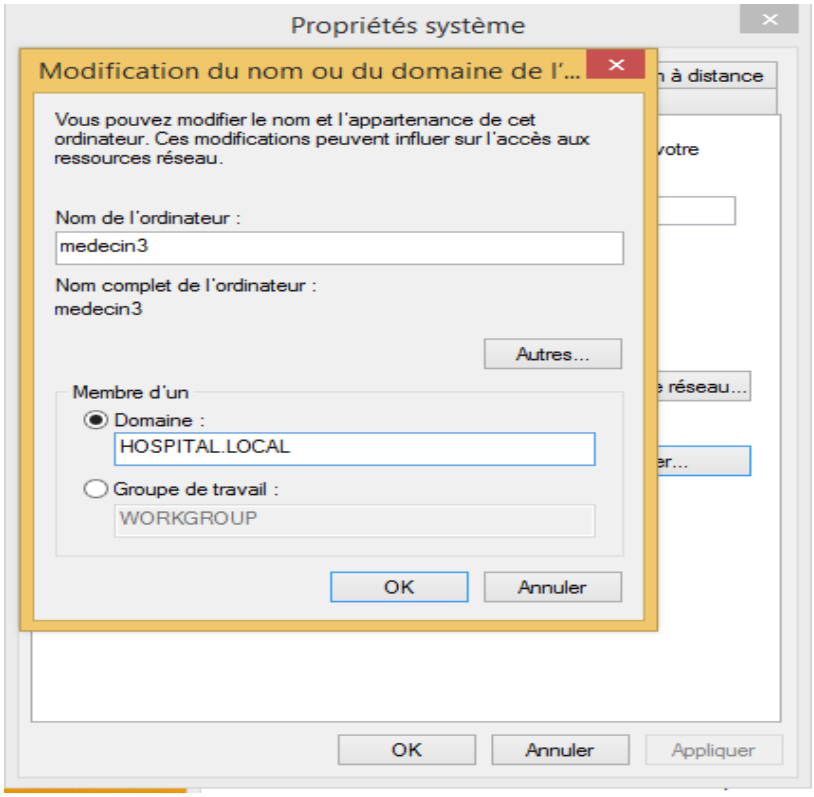

Figure 125 : Ajouter nom de Domaine dans un pc Windows 8 en LAN.

2. S'authentifié au Domaine en LAN au tant que médecin :

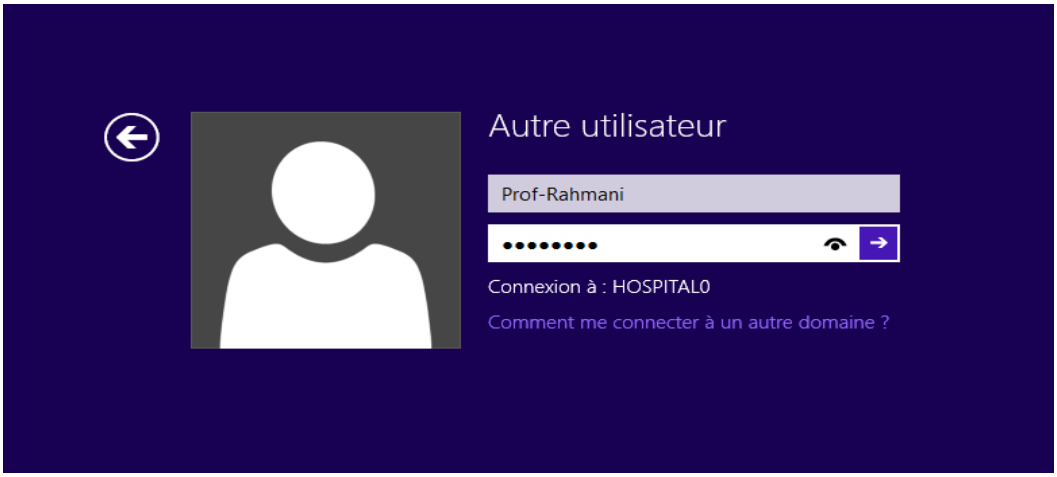

Figure 126 : Authentification du compte local en Domaine.

2. Le compte médecin se connecte au Domaine en local

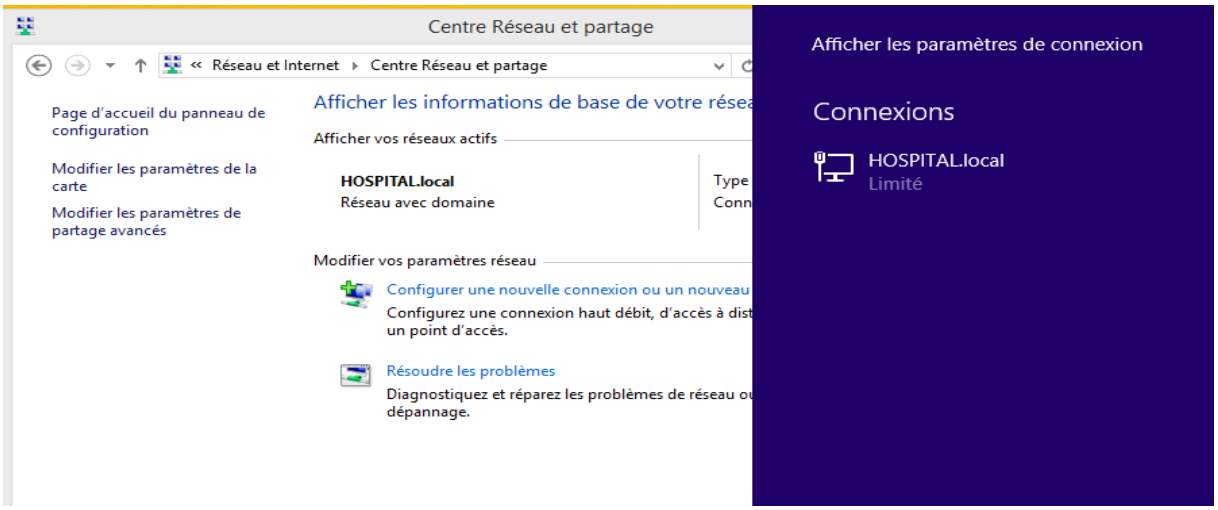

Figure 127 : Connexion établie en LAN.

4. Dans cet écran on retrouve l'adresse IP attribuée par le DHCP

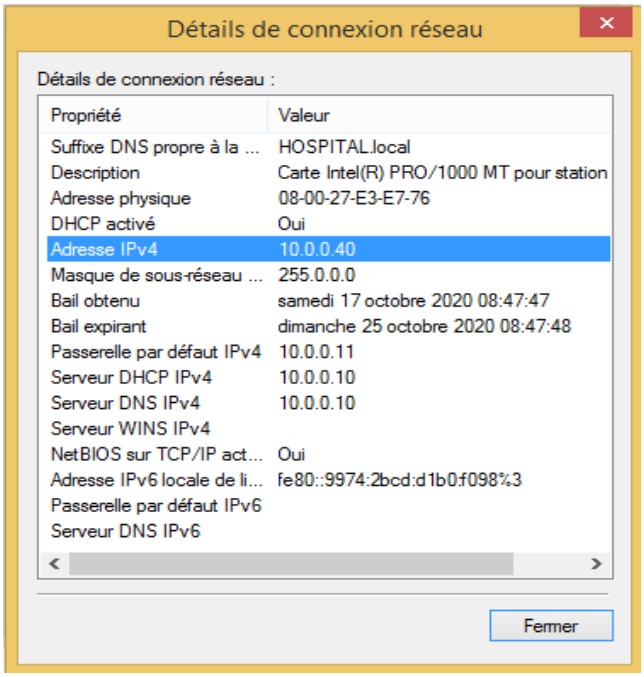

Figure 128 : Adresse IP d'un utilisateur en LAN.

5. On va se connecter au Domaine à distance à partir de la connexion VPN crée dans la configuration de client, on introduit les identifiants de médecin et on clique OK

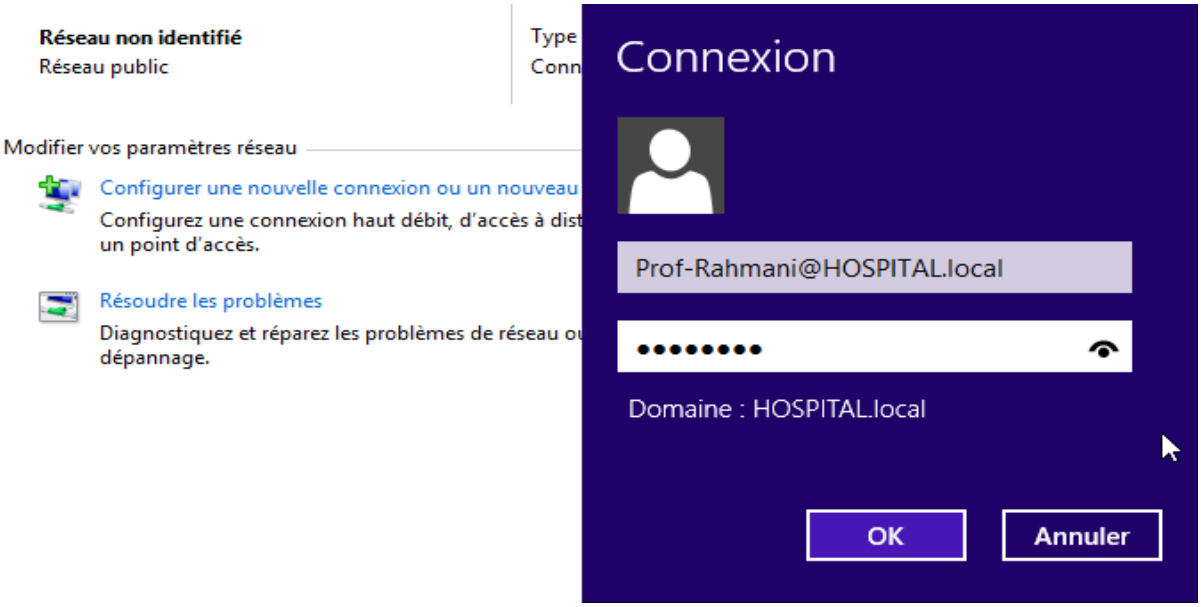

Figure 129 : Entrer le compte de Domaine.

6. La connexion est établie

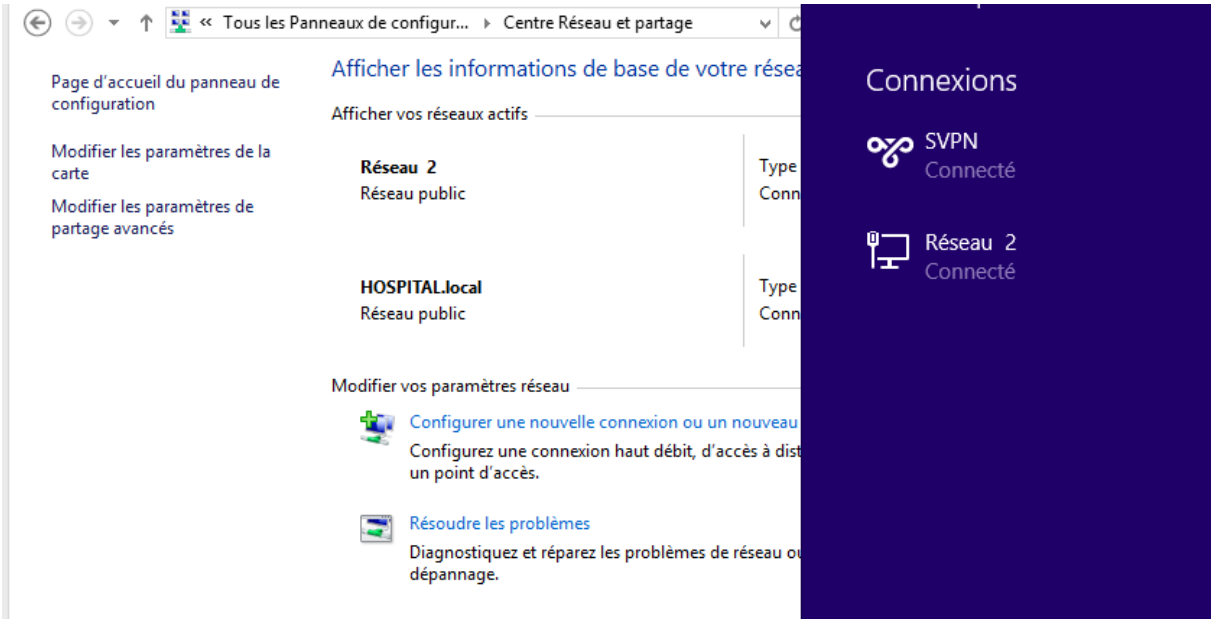

Figure 130 : Connexion VPN établie.

7. Dans la console de gestion de l'accès distant, on trouve notre médecin distant connecté avec le détail de la connexion

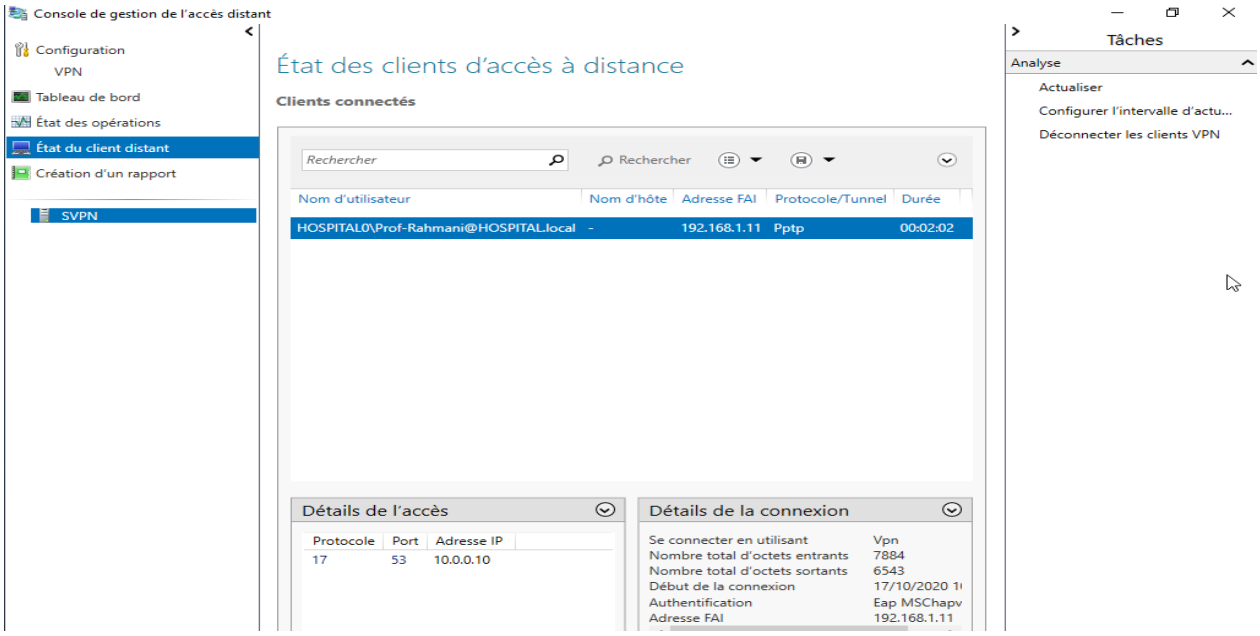

Figure 131 : Console de gestion de l'accès distant.

Remarque importante **:** Pour la configuration de client on a fait le test localement, mais si le PC est à l'extérieur, c'est l'adresse IP publique aussi appelé IP WAN qu'on devra utiliser.

Pour finir, c'est effectivement l'adresse IP indiquée par les sites du style « Mon IP » trouvés via Google qu'on devra utiliser. De plus, une redirection de port (port forwarding) dans le routeur physique sera nécessaire pour que le routeur redirige la demande de connexion vers notre serveur VPN.

5.1. Conclusion

Dans ce chapitre on a présenté la solution proposée et son implémentation en détaillant l'installation et la configuration du contrôleur de domaine, du VPN, l'ajout de service NPS avec une stratégie qui autorise les médecins de Domaine de se connecter via VPN et on a terminé par un test. Ainsi le médecin peut consulter le dossier patient avec toute sécurité dans l'établissement et par internet.

CONCLUSION GENERALE

Dans ce projet, nous avons procédé à la conception et l'implémentation d'une solution sécurisée afin d'accéder au dossier patient, cette solution est bâtie sur :

-le système d'exploitation Windows server 2016 à travers son contrôleur de domaine permettant une authentification sécurisée des utilisateurs ;

-Le VPN permet aux utilisateurs d'accéder à distance après leurs identifications via le contrôleur de Domaine.

Nous avons commencé par l'installation d'un contrôleur de Domaine pour l'authentification, l'organisation et la sécurité des comptes utilisateurs, les données et les ressources du réseau.

Par la suite, nous somme passer à l'installation et la configuration du VPN qui offre un moyen sécurisé et sûre qui permettra au médecin d'accéder au réseau interne par l'Internet, depuis l'extérieurs du réseau (autre établissement de santé) afin de suivre leurs patients sans pour autant risquer de compromettre la sécurité des données et ressources internes du réseau.

Ainsi, pour la sécurité de notre réseau nous avons mis en place un deuxième protocole d'authentification Radius en ajoutant le service NPS de Windows server 2016 et nous l'avons configuré pour vérifier toutes les connexions des comptes utilisateurs entrant de VPN.

Pour finir, nous pensons que la mise en œuvre de cette solution que nous proposons est d'une importance pour le bon fonctionnement du projet, notre travail reste ouvert à des extensions possibles telles que l'ajout d'un certificat de sécurité au serveur VPN.

Bibliographie

Ouvrage

[1] C. SERVIN, Réseaux et télécoms, Edition DUNOD. 2eme Edition.2013

[2] Dean.T. Réseaux Informatique, 2ème édition. LesÉditions RYNALD GOULET, 2001.

[3] LEMAINQUE Fabrice PILLOU Jean-François. Tout sur les Réseaux et Internet,3e édition. Dunod,2012.

[5] Yves LESCOP, "sécurité informatique", 2002

[8] J. ARCHIER, Les VPN : fonctionnement, mise en œuvre et maintenance des réseaux Privés virtuels. Edition ENI, 2010.

[9] Vincent Remazeilles. La sécurité des réseaux avec Cisco. Edition ENI.2009 60

[10] M. CHATEAU et autres, Windows Server 2008 R2 administration avancée, 2 IIème édition, Eni édition, 2011.

[14]B. MAMBENGA, Mise en Place d'un annuaire Active Directory, BTS SIO, 2016.

Site Web

[4] https://www.supinfo.com/articles/single/7300-differentes-topologies-reseaux

[6] https://www.auvik.com/franklymsp/blog/authentication-protocols/

[7] https://www.brainbell.com/tutorials/Networking/Remote_Authentication_Dial-In_User_Service_RADIUS.html

[10] www.frameip.com/vpn/

[11] https://blog.varonis.fr/services-de-domaine-active-directory-ad-ds-presentation-et-fonctions/

[12] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/dns-and-ad-ds

[13] https://www.editions-eni.fr/supports-de-cours/support-de-cours/windows-server-2012-r2-installation-et-configuration-9782746090095/extrait-du-livre.pdf

[15]https://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-firewall474.

[16]https://www.techno-science.net/definition/3836.html.

[17]http://www.ordinateur.cc/syst%C3%A8mes/fen%C3%AAtres/212340.html

[18]http://psonlinehelp.equallogic.com/fr/V6.0/Content/bomre/LDAP/ldap-taskref/ldap_ref_adv_disadv_ad_users_groups.htm

[19] https://www.ionos.fr/digitalguide/serveur/know-how/linux-vs-windows-le-grand-test-des-serveurs/

[20]https://www.capgemini.com/2011/07/domain-and-dmz-critical-consideration/

[21]https://blog.netop.com/vpn-vs-remote-desktop-main-difference