OFPPT

Projet de fin de formation

Mise en Œuvre d'un Serveur VPN sous Windows Server 2008

Réalisé par :

Rachid BOUHADI

Sofiane DAHBI ESSAKALI

El kaouri LAMTI

Encadré par :

Abdraheman BOULAL

Sommaire :

Remerciement :

Tout d'abord, je profite de cette occasion pour exprimer toute ma gratitude à tous ceux qui ont contribué à la réalisation de ce Modest travail, tenant compte à la bonne stratégie de l'institut ISTA qui nous offre une occasion d'attaquer le secteur pratique suite à celui de la théorie, afin d'améliorer nos connaissances dans le domaine.

Nous tenons à remercier nos formateurs de l'institut, pour leur bien vaillance et leur disponibilité pour nous fournir leurs Soutiens et en plus des conseils.

Nous tenons à remercier tout particulièrement ceux qui, de près ou de loin, nous ont aidés à élaborer ce travail. Nous les remercions également pour leurs pilotages efficaces, pour leurs conseils les plus précieux, leurs commentaires les plus pertinents tout au long de cette période.

Ensuite, nous souhaitons que ce travail soit à la hauteur de nos ambitions et à l'attente de notre encadreur.

Introduction :

Les réseaux locaux d'entreprise (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel**(noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.
Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

Le système de *VPN* permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

Partie 1

VPN

(Virtual Private Network)

Qu’est-ce que VPN ?

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau (Internet par exemple). Il permet de faire transiter des informations, entre les différents membres de ce VPN, de manière sécurisée.

VPN permet à deux bureaux distants d’être liés ensemble à travers Internet et ainsi de partager des ressources entre tous les postes faisant partie du réseau local (LAN).
Il s’adresse particulièrement aux employés en déplacement qui pourront ainsi profiter des ressources de l’entreprise à distance.

Pour schématiser, on peut considérer qu'une connexion VPN revient à se connecter en LAN en utilisant Internet. On peut ainsi communiquer (ping, tous protocoles IP) avec les machines de ce LAN en appelant leurs IP locales (la plupart du temps, elles ressemblent à ça : 192.168.X.X ou bien 10.X.X.X ou bien 172.16.X.X, etc...).

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant Ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'Ip. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Cas d'utilisation de VPN

On peut trouver plusieurs cas d'utilisation d'un VPN dont :

- Le Télétravail. Il existe des entreprises sans locaux, ou les employés travaillent chez eux. Quand ce type de travail est possible, pourquoi dépenser plus pour des locaux, des problèmes de transport, etc ... ? Le VPN apporte la possibilité pour tous ses employés de travailler sur un même réseau privé virtuel. Il doit alors évidement disposé d'une connexion internet qui lui permet de travailler à distance, et d'utiliser les différents services du réseau, et même exploiter des outils de travail collaboratif.

- Connexion de sites distants. Pour en entreprise possédant plusieurs sites, il est parfois avantageux de les relier. Une première solution serait d'utiliser une LS. Mais cette solution à un coup, et le VPN ne coûte pas plus que 2 connexion d'accès à internet.

Les moyens techniques de VPN :

Le VPN est ne représente donc qu'un concept, derrière lui, plusieurs implémentations ont vu le jour, selon l'utilisation que l'on veut en faire, le niveau de sécurité, la taille du réseau, etc. ...

Plusieurs moyens techniques peuvent être utilisés et couplés pour mettre en œuvre des VPN : le chiffrement, l'authentification, le contrôle d'intégrité et les tunnels.

Chiffrement : Utilisé pour que les données traversant le réseau ne puissent pas être lu par une autre personne. On utilise pour cela notre baguage mathématique et surtout arithmétique. Les deux principaux types de cryptage utilisés sont : le chiffrement asymétrique et symétrique. Le chiffrage symétrique utilisé la même clé pour chiffrer et pour déchiffrer. L'inconvénient, est clair : chaque partie de la communication devra avoir la même clé, et la communiquer à la partie adverse sans que les autres puissent le récupérer. Plusieurs algorithmes de cryptage peuvent être utilisés : DES, AES, RC4/5. Le cryptage asymétrique n'a pas cette inconvénient la : deux clés sont utilisées : une clé publique et une clé privée. La clé public est disponible par tout le monde. Elle sert à crypter des données. Si on veut communiquer avec un autre, on doit récupérer sa clé publique et seul lui pourra la décrypter avec sa clé privé. Bien sur le cryptage et le décryptage se font de manière précise suivant la méthode utilisée.

Authentification : On veut garantir qu'a chaque instant de la communication, on parle au bon interlocuteur. Dans le cadre du VPN, on parle des deux passerelles qui sont séparé par internet.

Contrôle d'intégrité : il garantit que les données transmit entre les interlocuteur n'ont pas été modifié.

Tunnel : le tunnel consiste à établir un canal entre 2 points sans ce soucier des problématique d'interconnexion (de façon transparente). Nous verrons plus en détail cet aspect important du VPN.

Avantages et inconvénients du VPN :

Les avantages :

- La possibilité de réaliser des réseaux privés à moindre coût par rapport à tout autre type de connexion, l'entreprise ne paye que l'accès à Internet, il n'est pas nécessaire de payer une communication nationale ou internationale.

- La mise en œuvre d'un Intranet étendu et homogène permettant à tous les utilisateurs d'accéder à distance à des ressources partagées ou des services de types ASP, quelle que soit leur localisation.
- L'accès de vos partenaires ou vos clients à votre réseau ainsi que la possibilité de communiquer entre eux.
- L'extension de votre réseau local en toute sécurité par l'utilisation de tunnels de communication cryptés.

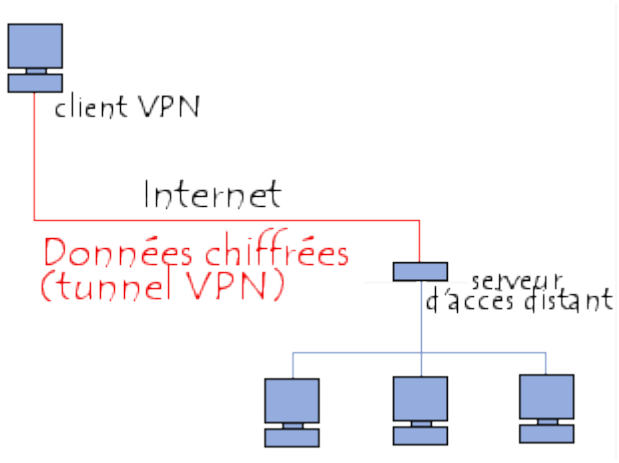
Les inconvénients :

- **Dépendant du réseau** : a contrario des connexions à la demande, les performances de l'abonnement Internet de l'un ou l'autre des deux parties (société ou nomade) ont un impact non négligeable sur la qualité des transmissions. Tout problème chez le fournisseur d'accès de l'un ou de l'autre peut provoquer une incapacité totale à communiquer.
- **Confidentialité des données** : bien qu'utilisant des systèmes de chiffrement il n'en reste pas moins que les données transitent au travers d'Internet. Du coup, elles sont potentiellement visibles de tous et ce bien qu'elles soient chiffrées.

Principe de fonctionnement :

Fonctionnement d'un VPN :

Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunnelisation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un *VPN* établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur VPN* (ou plus généralement

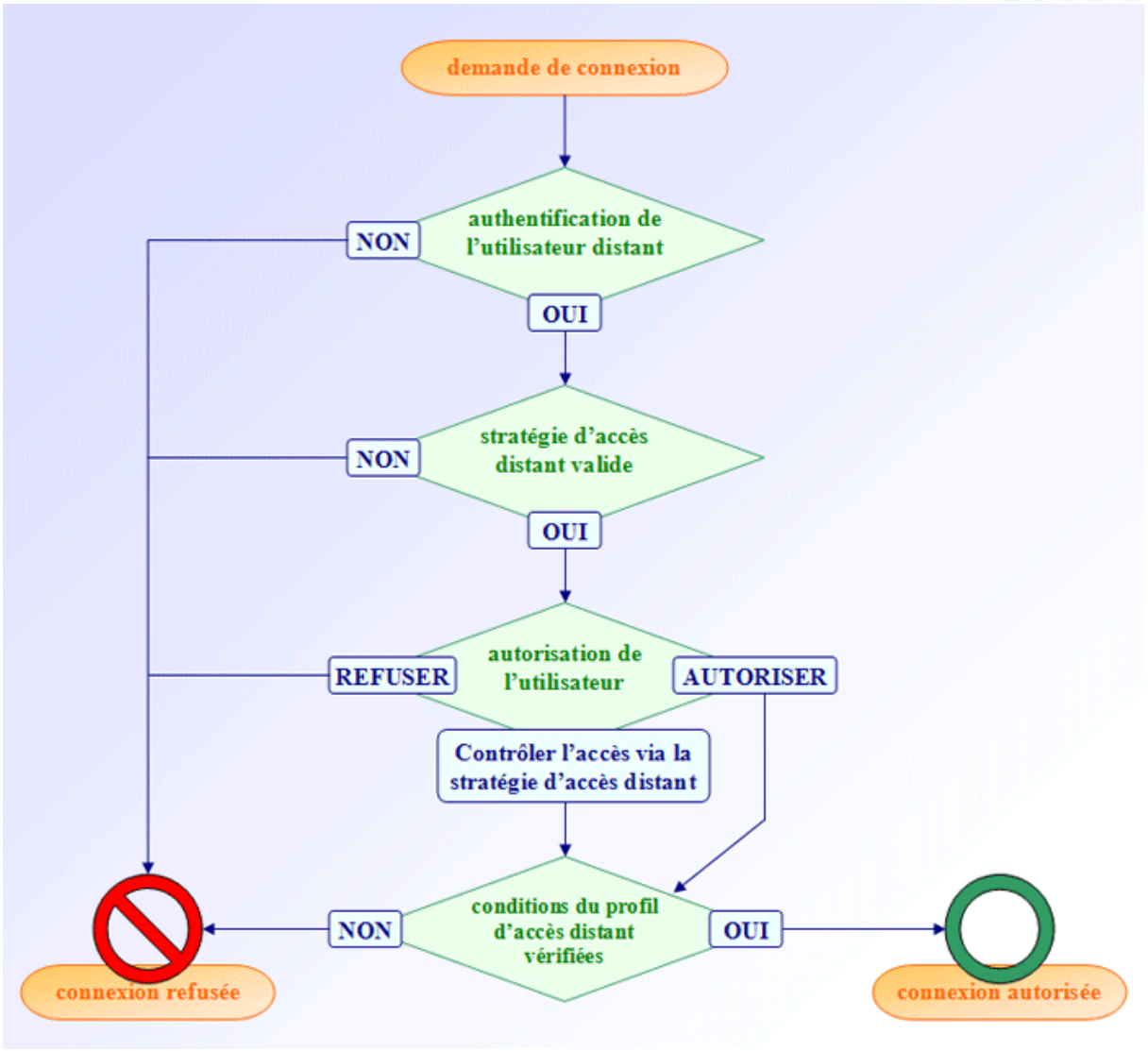
serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

Principe de fonctionnement de l'accès à distance :

L'établissement d'une connexion d'accès à distance passe par plusieurs étapes :

1. Un client contacte le serveur d'accès distant et lui envoie un identifiant avec un mot de passe pour tenter de s'authentifier.
2. Le serveur d'accès distant commence par vérifier si l'identifiant et le mot de passe correspondent à un utilisateur de l'annuaire Active Directory : c'est la phase d'authentification.
3. Si l'utilisateur s'est authentifié avec succès, alors le serveur d'accès distant compare les paramètres de la demande de connexion avec toutes les stratégies d'accès distant existantes.
4. Si les conditions d'une stratégie d'accès distant correspondent avec les paramètres de la demande de connexion, alors le serveur d'accès distant vérifie si l'utilisateur a l'autorisation de se connecter à distance au réseau de l'entreprise : c'est la phase d'autorisation.
5. Si l'utilisateur est autorisé à se connecter à distance au réseau de l'entreprise, alors les conditions du profil d'accès distant de la connexion sont vérifiées.
6. Si toutes les conditions du profil d'accès distant sont vérifiées alors la connexion est autorisée et le client reçoit une adresse IP.



Les protocoles de tunnelisation :

Les principaux protocoles de tunneling sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) 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.

Le protocole PPTP

Le **P**oint-**T**o-**P**oint **T**unneling **P**rotocol (PPTP) travaille que sur des réseaux IP.

Le principe du protocole PPTP (*Point To Point Tunneling Protocol*) est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.

Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectés par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP.

De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP, qui est lui-même encapsulé dans un message IP.

Le protocole PPTP consiste en deux flux de communication entre le client et le serveur, s'appuyant directement sur le protocole IP :

- Le premier flux a pour rôle la gestion du lien entre les deux parties, il s'agit là d'une connexion sur le port 1723 du serveur en TCP.
- Le second flux concerne les données échangées entre les deux parties, bien entendu ce flux peut et doit être chiffré, ce dernier transite en utilisant le protocole **GRE**.

PPTP ne concerne que le transport des données, un de ces deux protocoles intervient ensuite pour sécuriser l'authentification

- **P**assword **A**uthentification **P**rotocol (PAP): consiste à mettre en place une authentification entre le client et le serveur VPN. Les informations d'authentification (nom d'utilisateur et mot de passe) transitent en clair, Ce qui n'est pas l'idéal si l'on veut sécuriser au maximum...
- **C**hallenge **H**andshake **A**uthentification **P**rotocol (CHAP): consiste en un mécanisme d'authentification crypté, il est donc sécurisé.

Le protocole L2TP

Le protocole L2TP est un protocole standard de tunnelisation (standardisé dans un RFC) très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS).

Le protocole IPSec

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la

sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

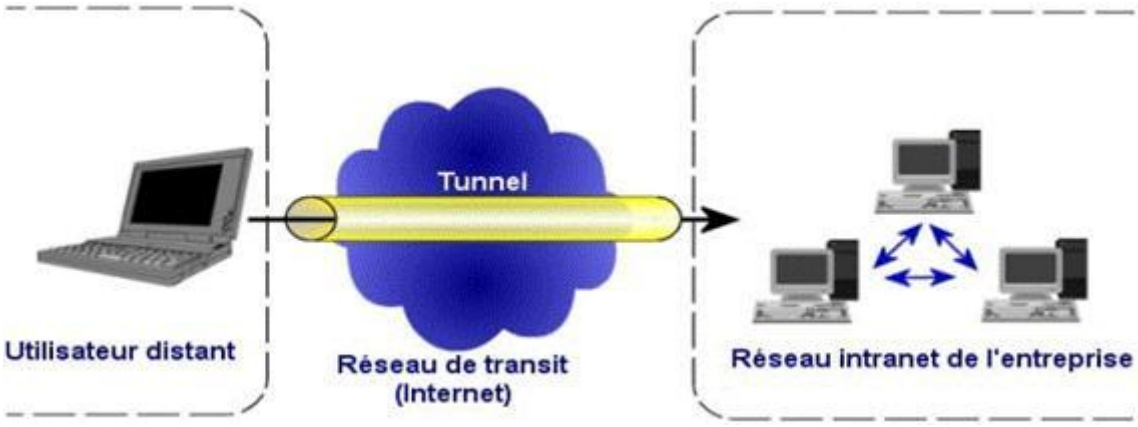
Le protocole IPSec est basé sur trois modules :

- *IP Authentification Header* (**AH**) concernant l'intégrité, l'authentification et la protection contre le rejeu. des paquets à encapsuler
- *Encapsulating Security Payload* (**ESP**) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu.
- *Security Assocation* (**SA**) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algo de sécurité utilisés par les protocoles, les clés utilisées,...). L'échange des clés se fait soit de manière manuelle soit avec le protocole d'échange IKE (la plupart du temps), qui permet aux deux parties de s'entendre sur les SA.

Fonctionnalités des VPN

Il existe 3 types standards d'utilisation des VPN. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des VPN.

Le VPN d'accès



Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas:

L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

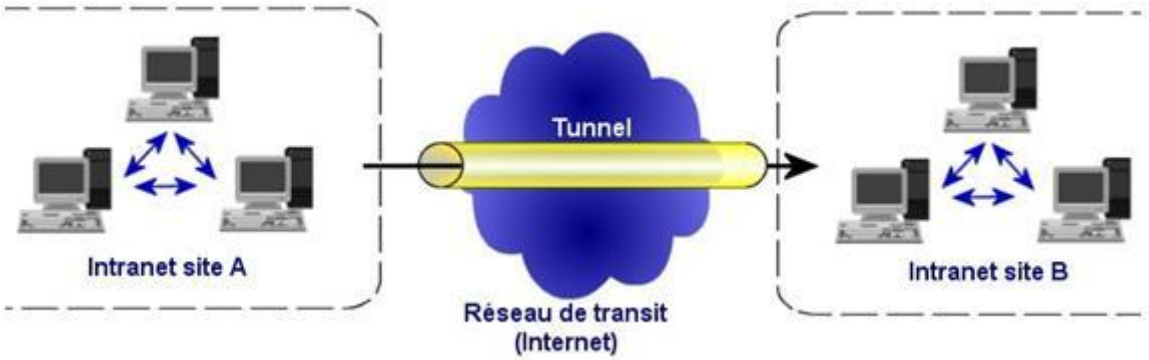
Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.

Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier Ce problème certaines entreprises mettent en place des VPN à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.

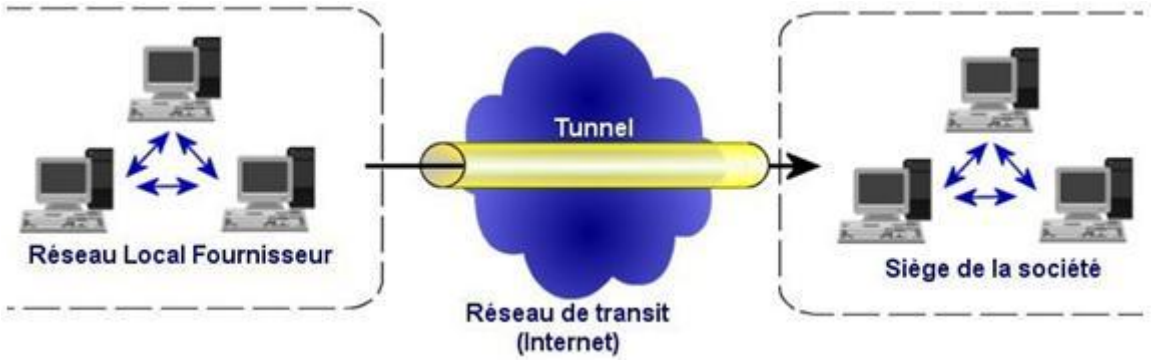
Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

L'intranet VPN



L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

L'extranet VPN



Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

Bilan des caractéristiques fondamentales d'un VPN :

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
- Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clés. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multiprotocole. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Le VPN est un principe : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

Partie 2

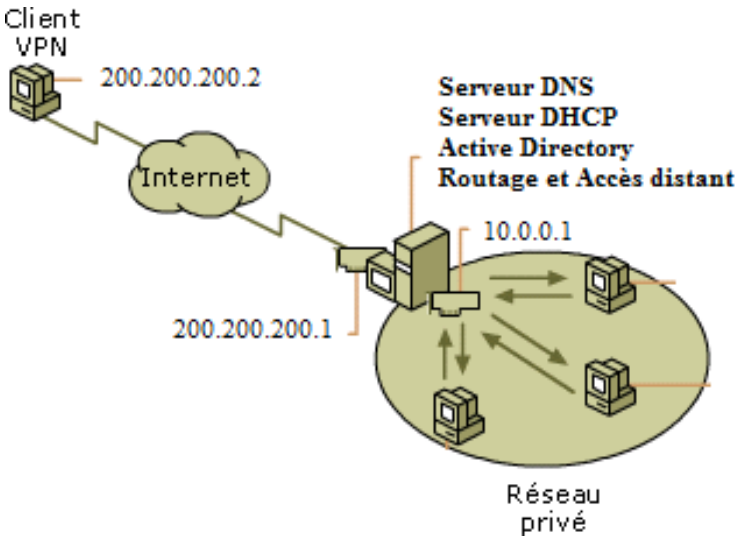
Mise en place d'un serveur VPN sous Windows 2008 Server

Introduction :

Comme nous le savons, l'internet n'a pas été créer dans un optique de confidentialité, c'est pour cela qu'ont été mis au point ces fameux VPN, ils permettent de créer une liaison entre deux points (deux pairs connectés à l'internet) tout en rendant cette connexion privé et cryptée donc inaccessible à autrui qui ne serait pas autorisé afin de protéger ces données.

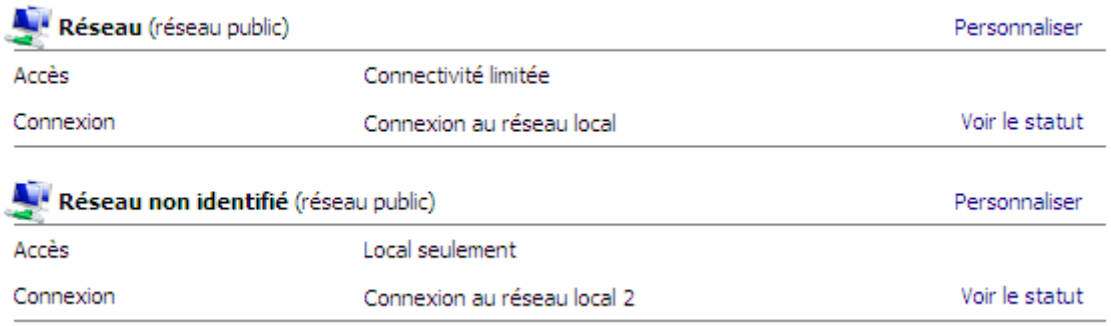
Dans cette partie de ce projet en va parler sur l'installation d'un serveur VPN sous Windows 2008 Server. Exemple dans un réseau local d'une entreprise pour permet à des utilisateurs de l'entreprise d'accéder d'après l'internet en tant que client VPN au réseau local pour permet d'assurer la confidentialité des données transmises.

Et cette topologie présente l'exemple d'une entreprise qu'on va le travailler dans ce projet :

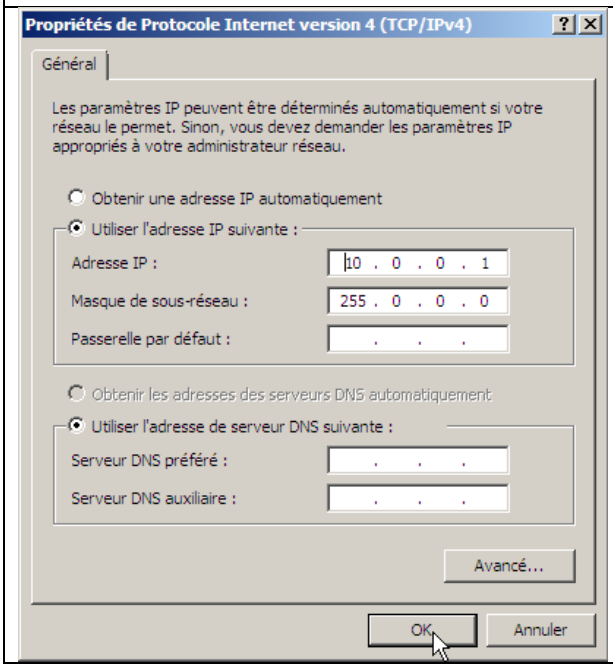
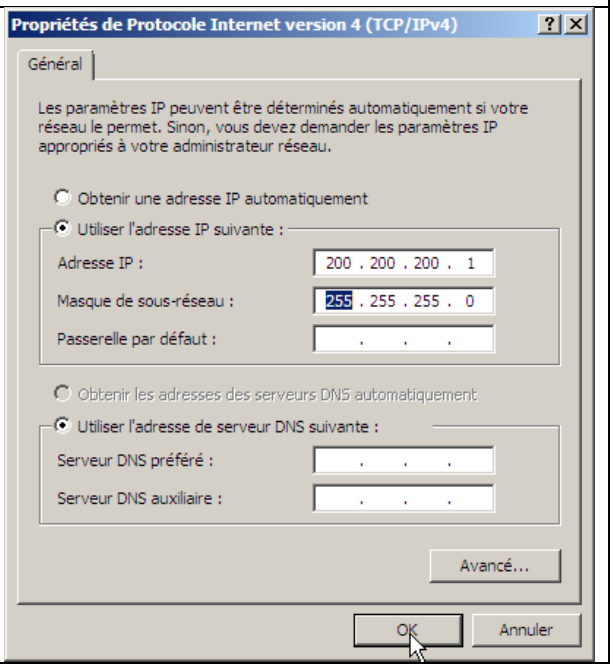


Pour installer un serveur VPN a cette entreprise il est d'abord nécessaire d'installer les serveurs suivant :

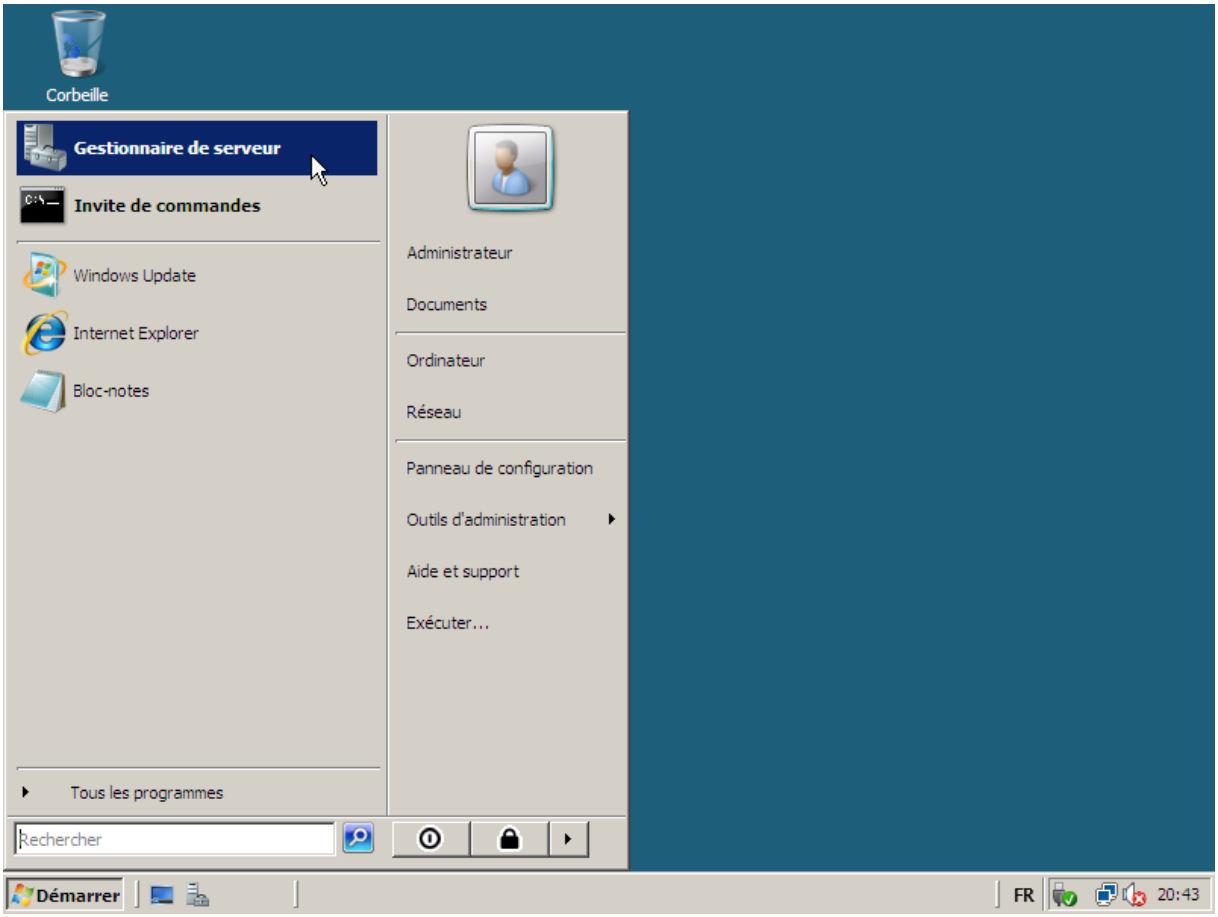
- Serveur DNS (Domaine Name Système).
- Serveur DHCP (Dynamic Host Configuration Protocol).
- Services de domaine Active Directory.



Dans notre serveur qui appartient aux système d'exploitation Windows 2008 server avec deux cartes réseau :

La première carte avec une adresse IP privé : 10.0.0.0/8	**La deuxième carte avec une adresse IP public : 200.200.200.0**
	

Installation des serveurs sous Windows 2008 Server :

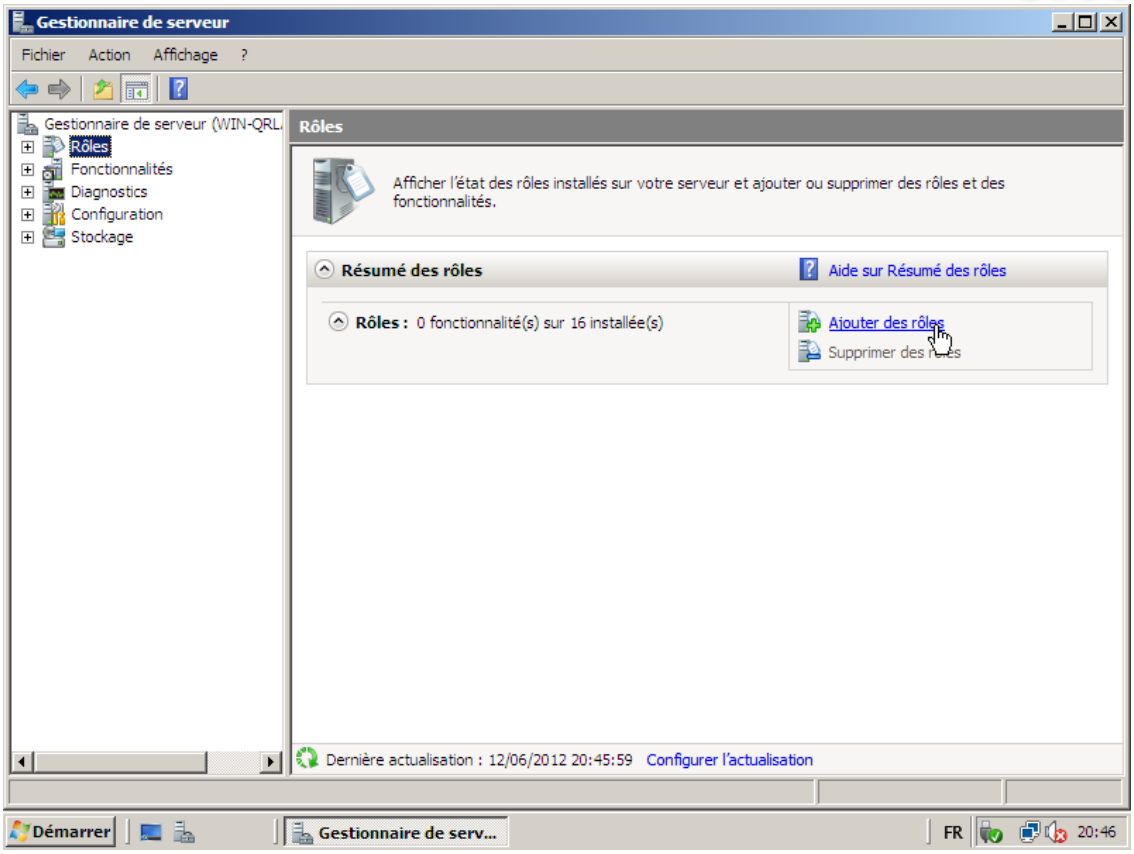


Pour l'ajoute d'un rôle on clique sur **Démarrer** puis **Gestionnaire de serveur**.

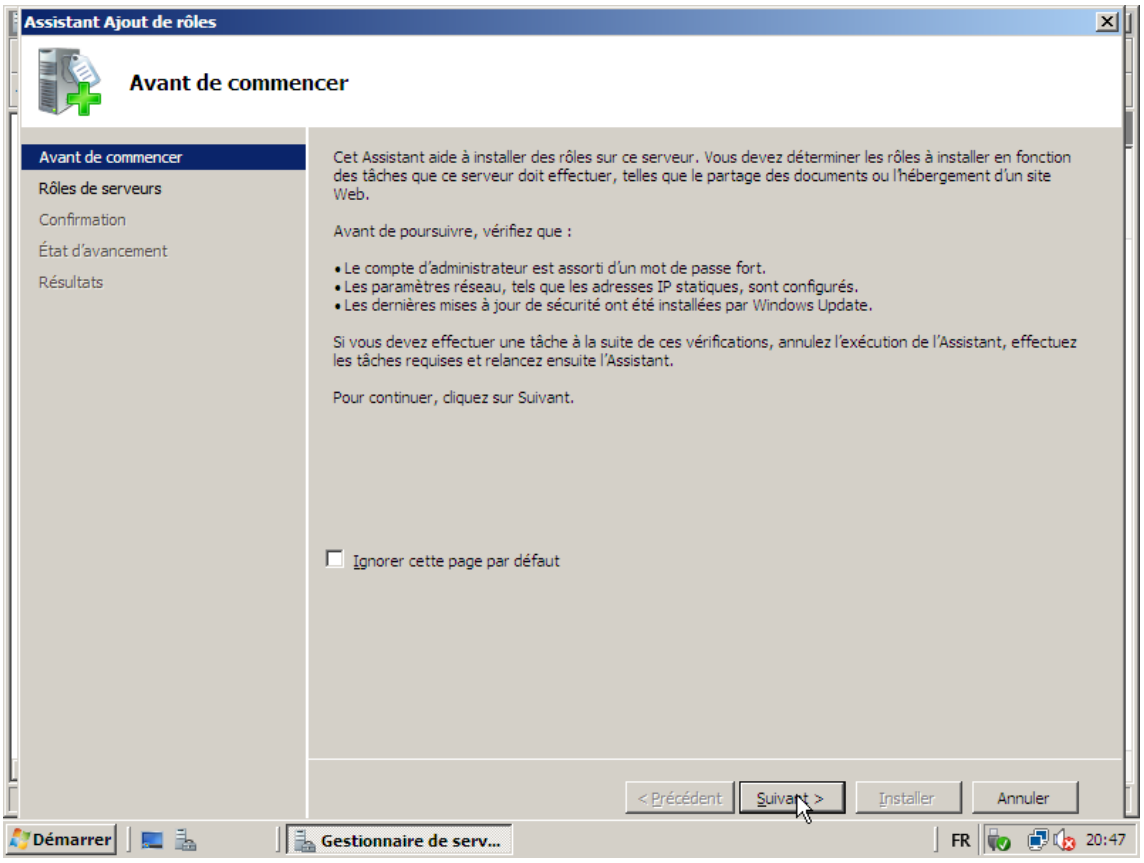
DNS :

Le serveur DNS (Domain Name System) fournit la résolution de noms pour les réseaux TCP/IP. Ce serveur est plus facile à gérer s'il est installé sur le même serveur que les services de domaine Active Directory. Si vous sélectionnez le rôle services de domaine Active Directory, vous pouvez installer et configurer le serveur DNS et les services de domaine Active Directory pour qu'ils fonctionnent ensemble.

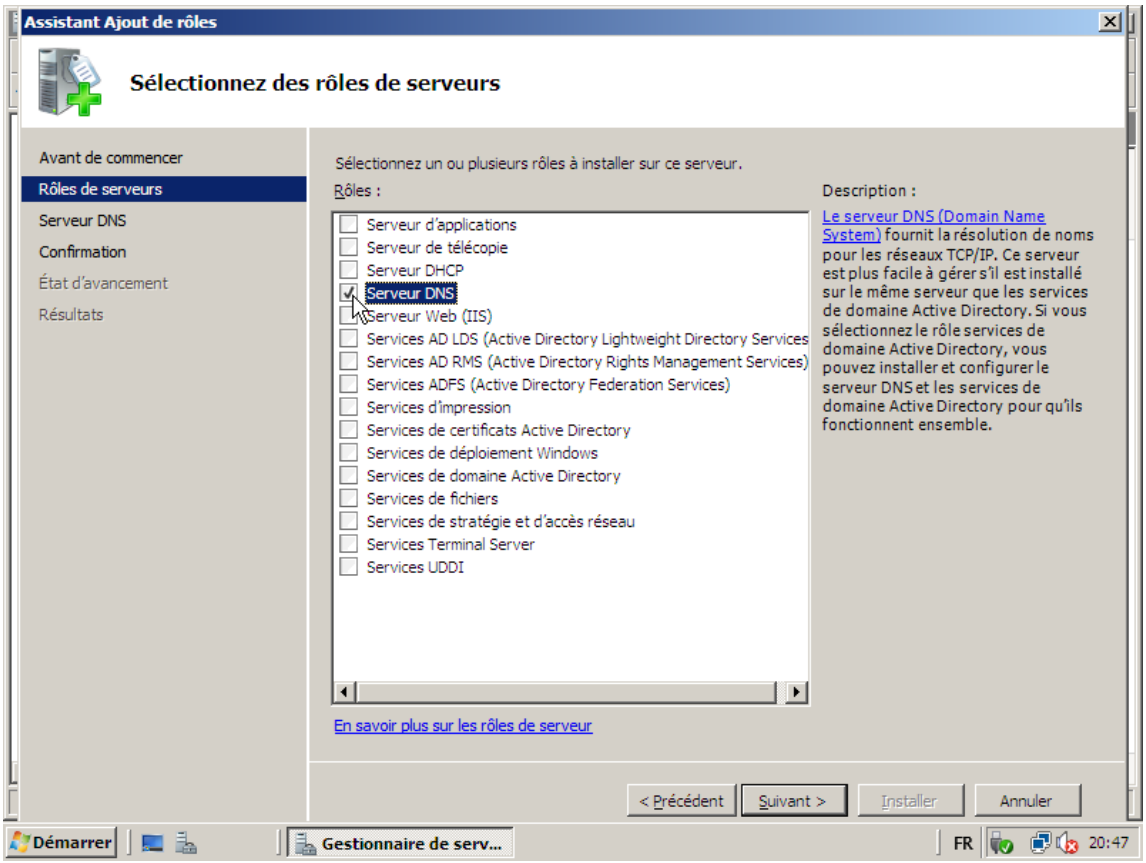
Pour ajouter le rôle Serveur DNS on choisit le menu **Rôles** puis on clique sur **Ajouter un rôle**.



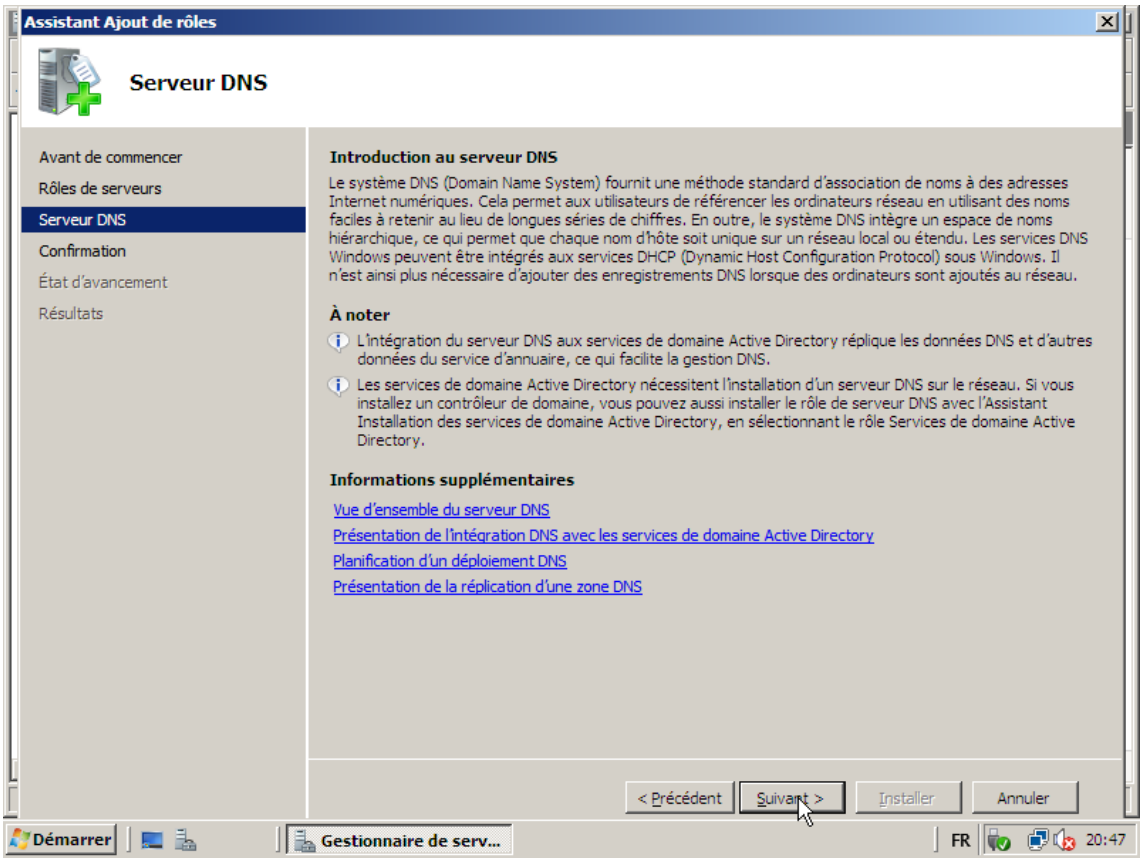
Dans l'**Assistant ajout de rôles** on clique sur **Suivant**



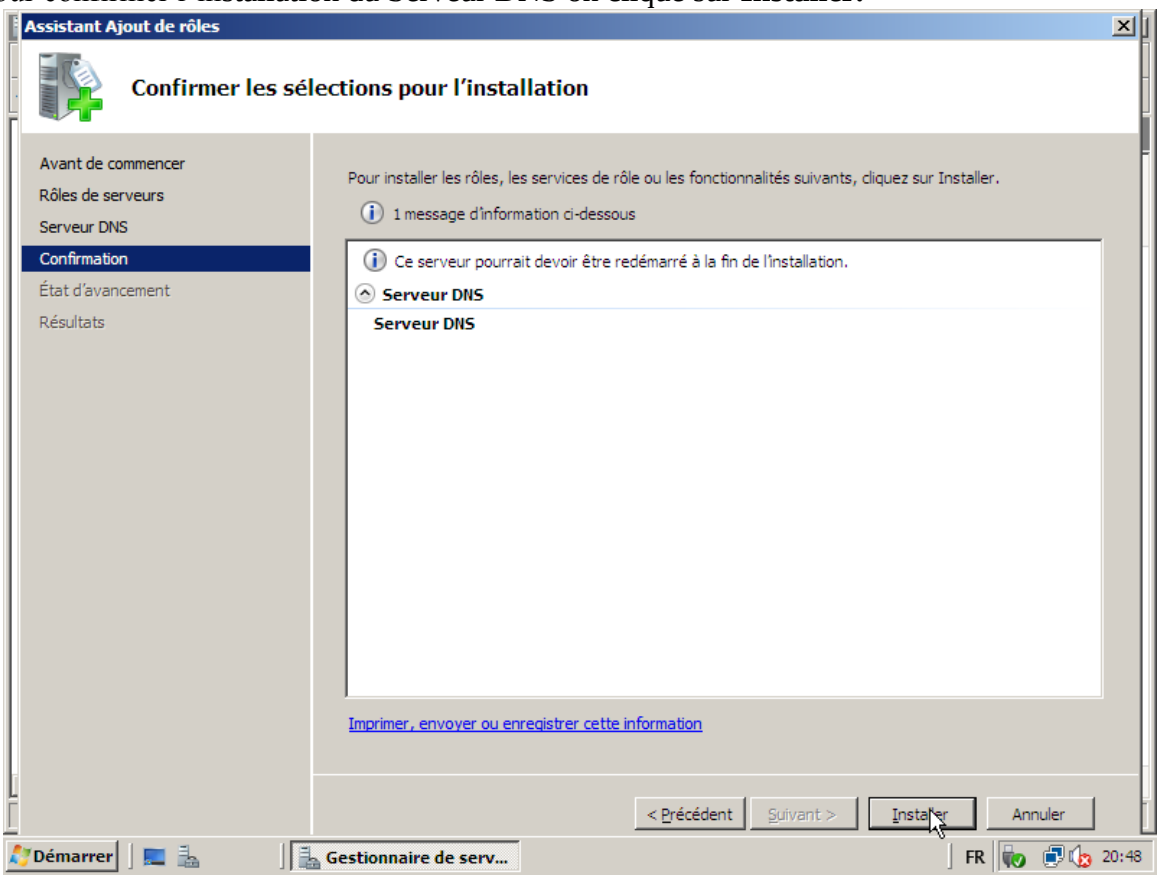
On sélectionne le rôle **Serveur DNS** dans la liste des rôles puis on clique sur **Suivant**



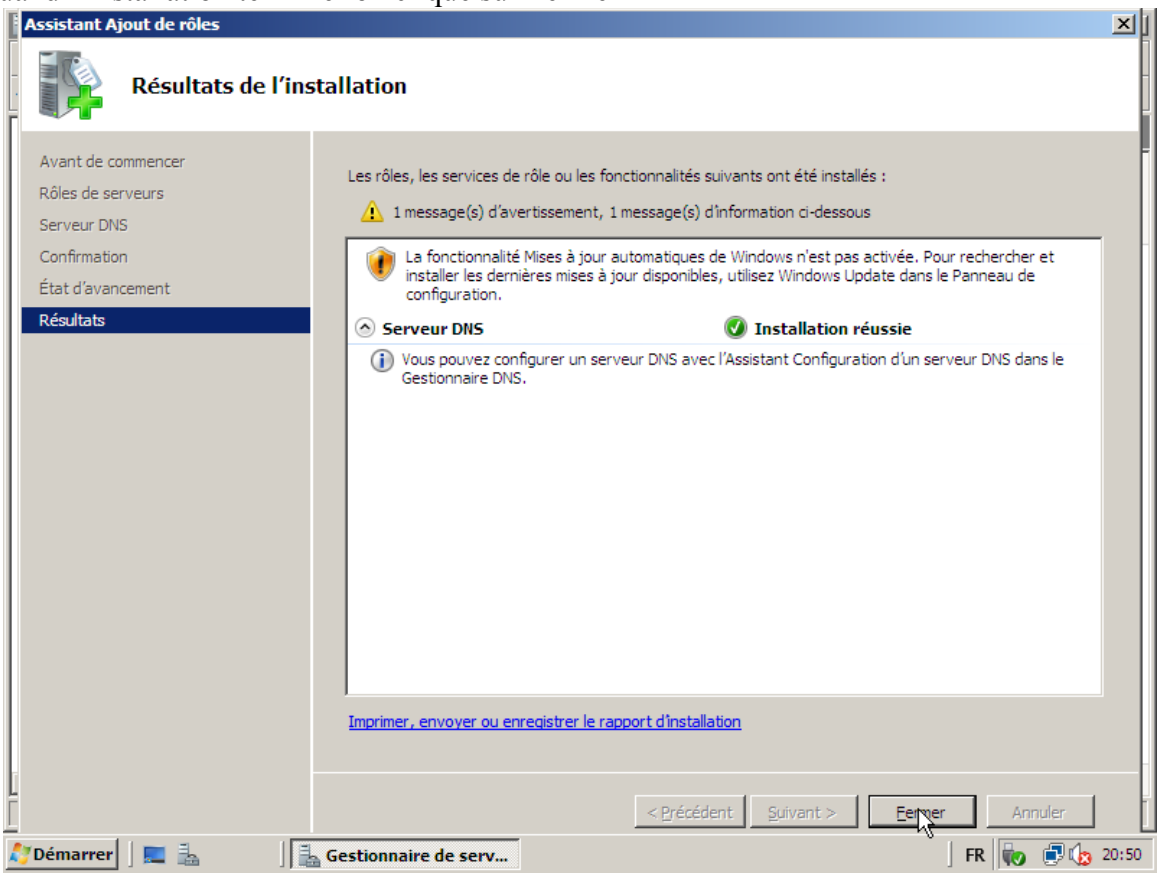
Puis on clique sur **Suivant**



Pour confirmer l'installation du Serveur DNS on clique sur **Installer.**



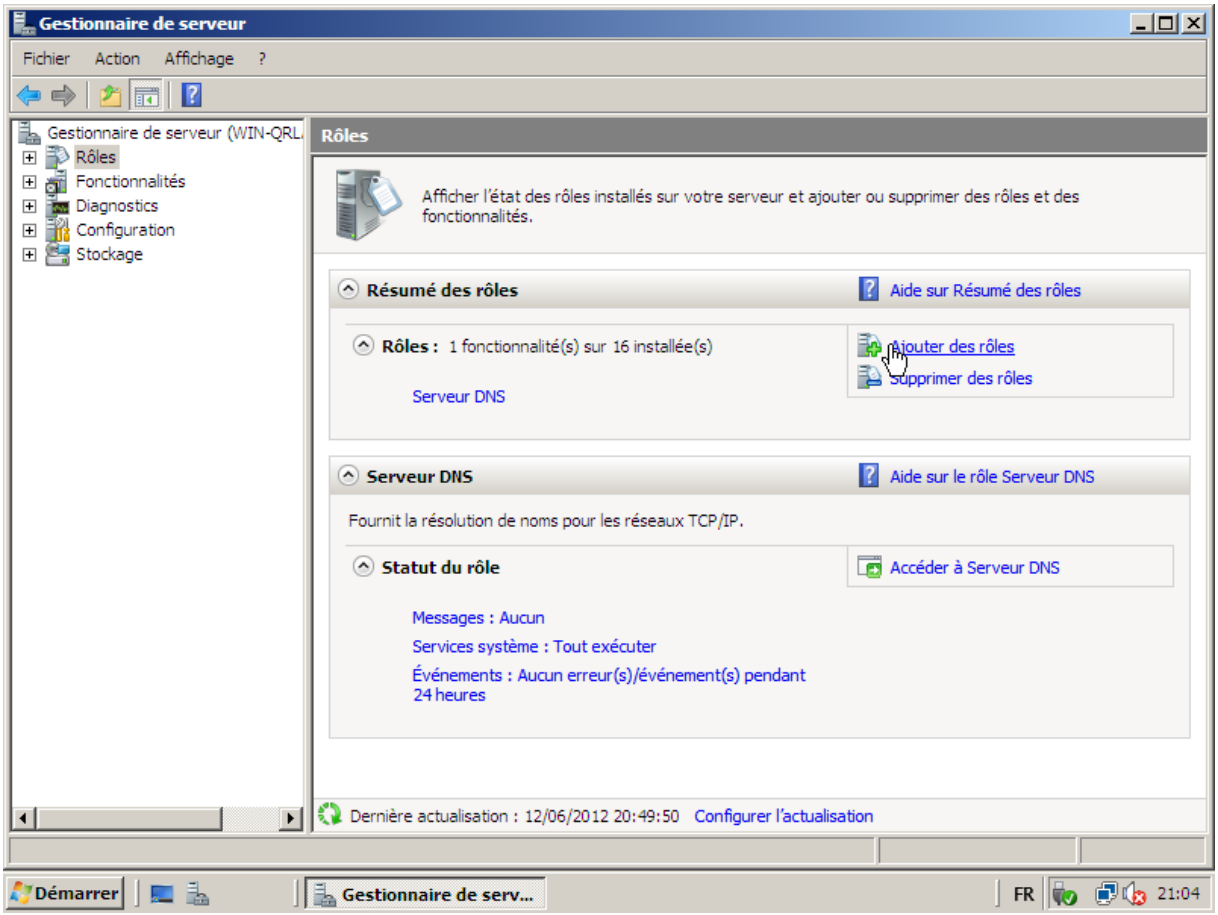
Quand l'installation terminer on clique sur Fermer



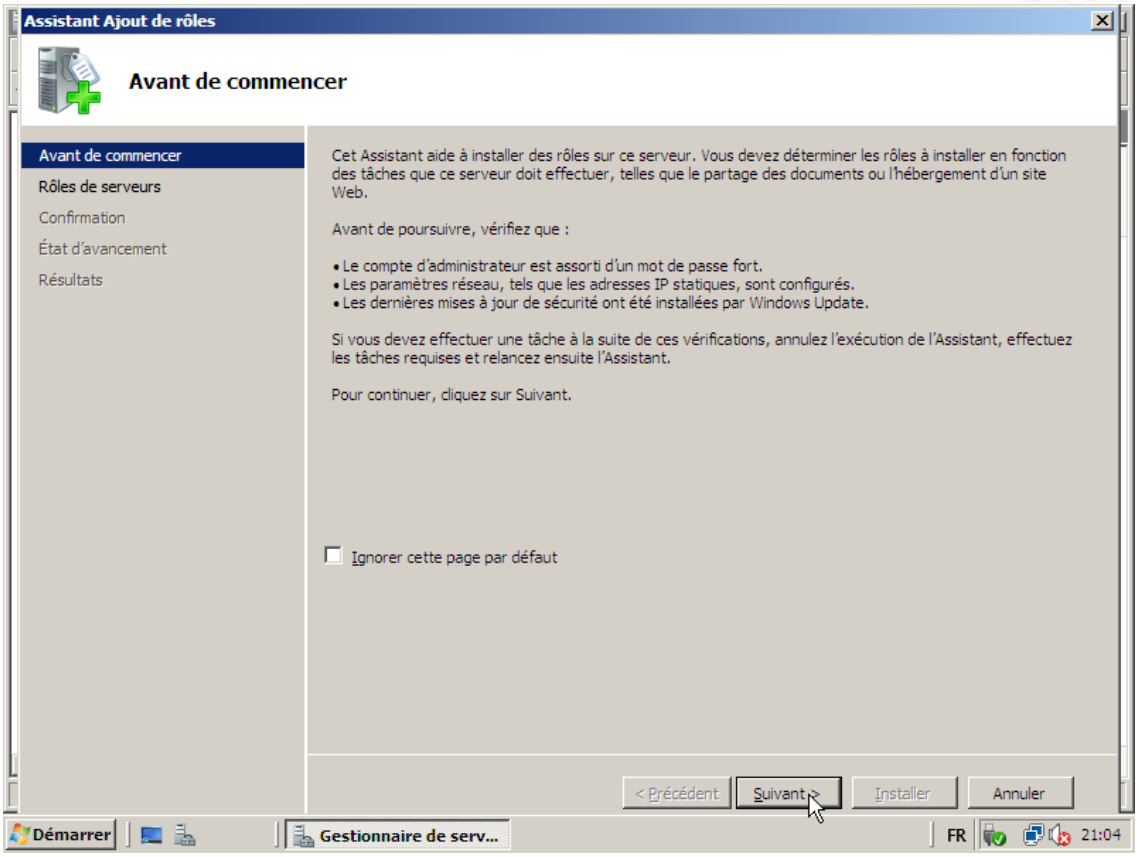
Active Directory :

Les services de domaine Active Directory (AD DS) stockent des informations sur les objets sur le réseau et les rendent disponibles aux utilisateurs et aux administrateurs réseau. Ces services utilisent des contrôleurs de domaine pour donner accès aux ressources autorisées aux utilisateurs réseau n' importe où sur le réseau via un processus d'ouverture de session unique.

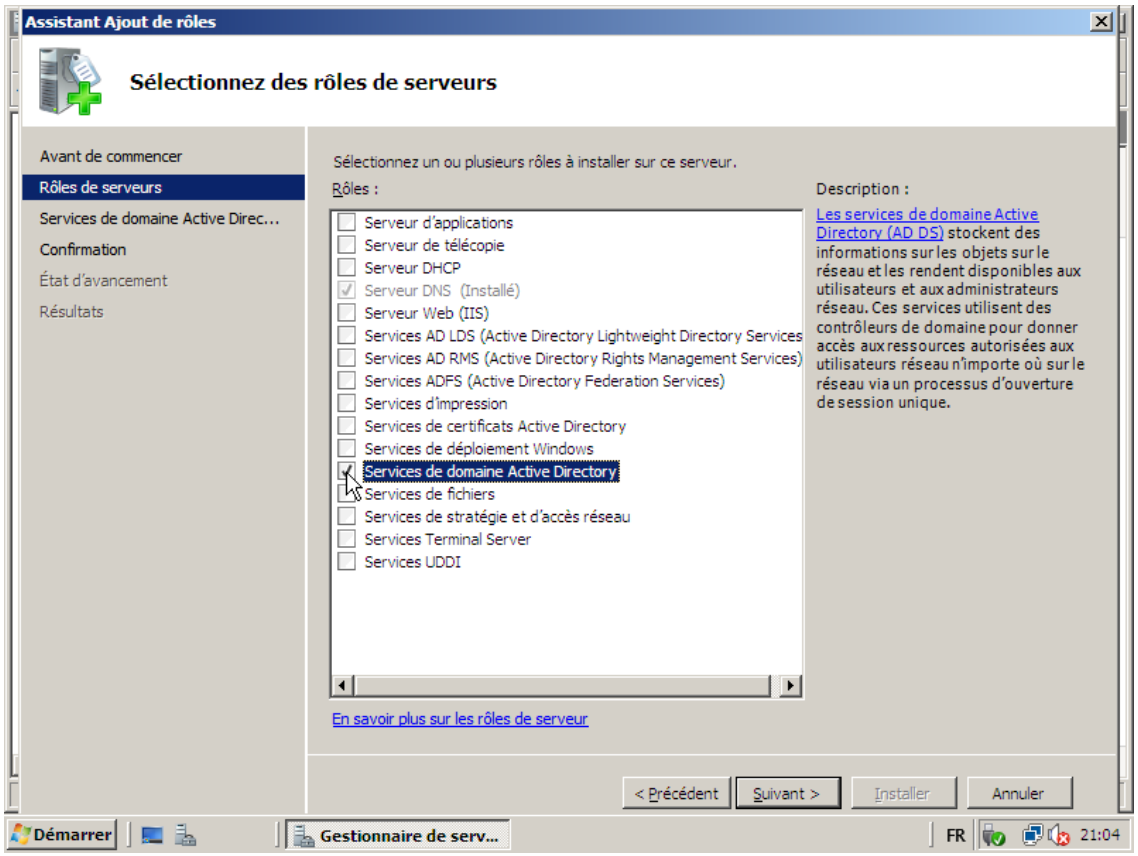
Pour ajouter le rôle Services de domaine Active Directory on choisit le menu **Rôles** puis on clique sur **Ajouter un rôle**.



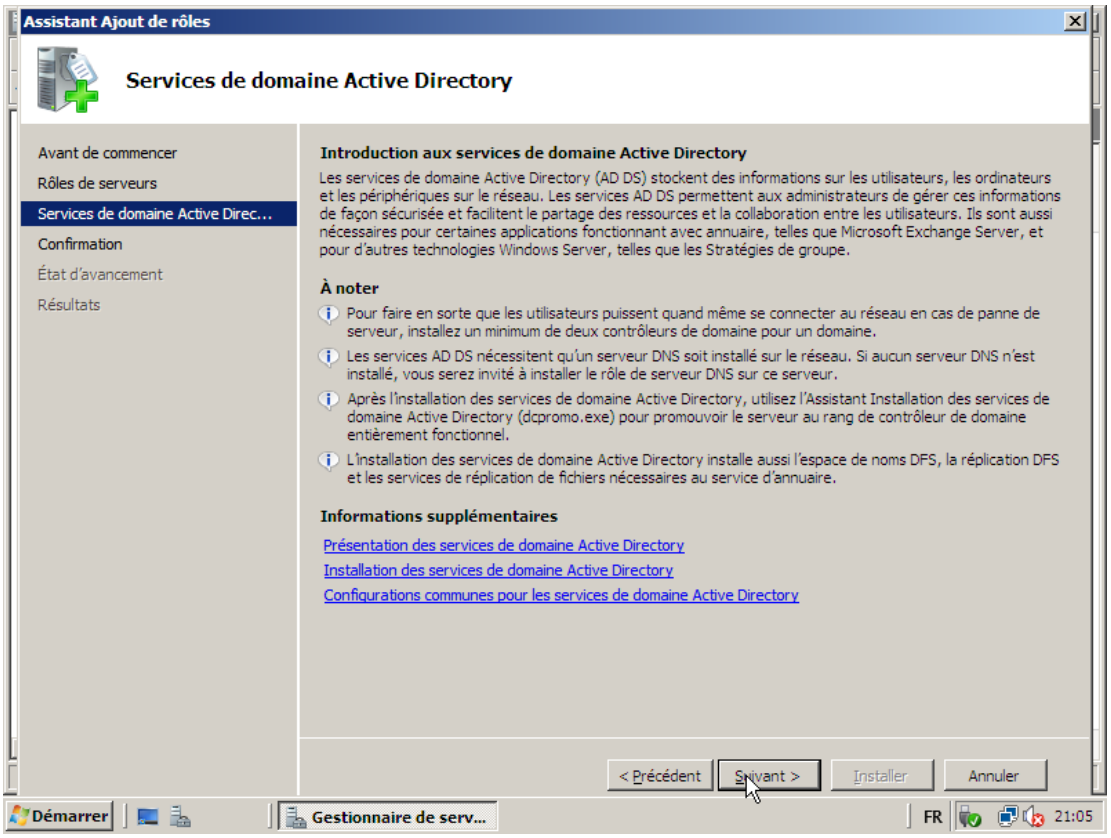
Dans l'**Assistant ajout de rôles** on clique sur **Suivant**



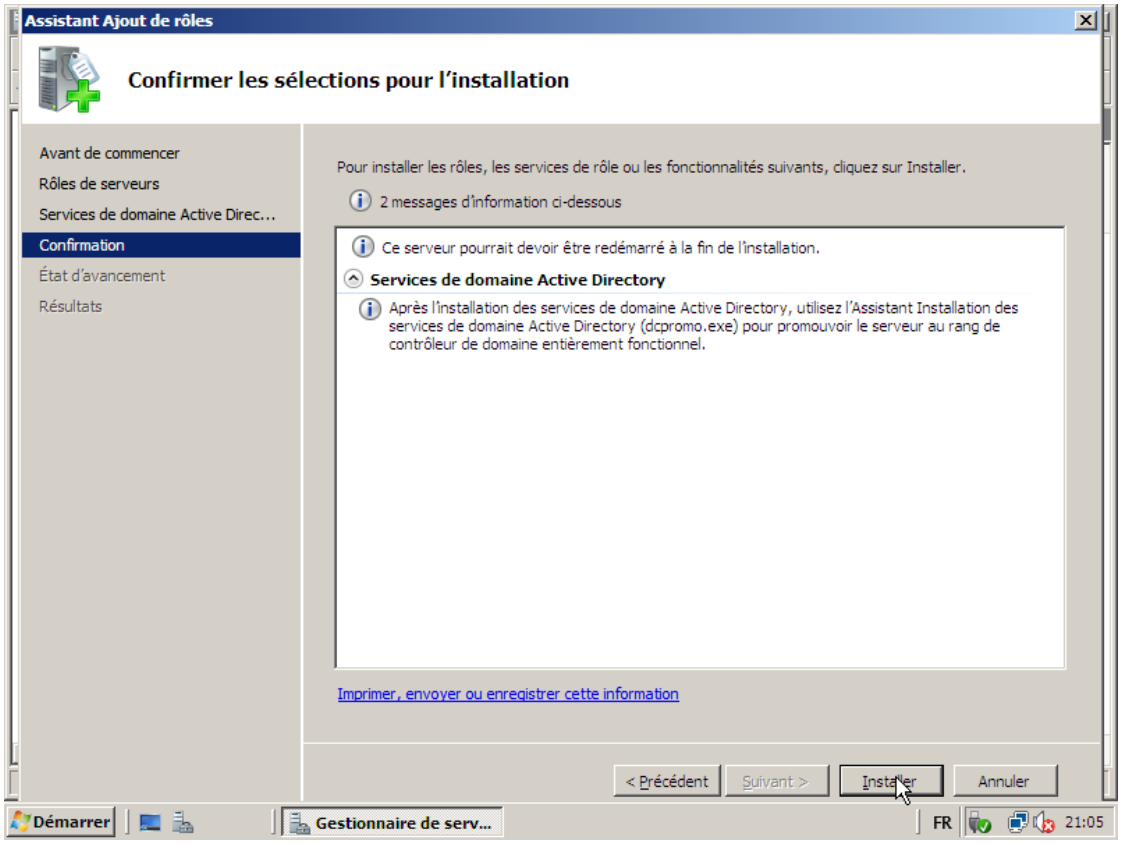
On sélectionne le rôle **Service de domaine AD** dans la liste puis on clique sur **Suivant**.



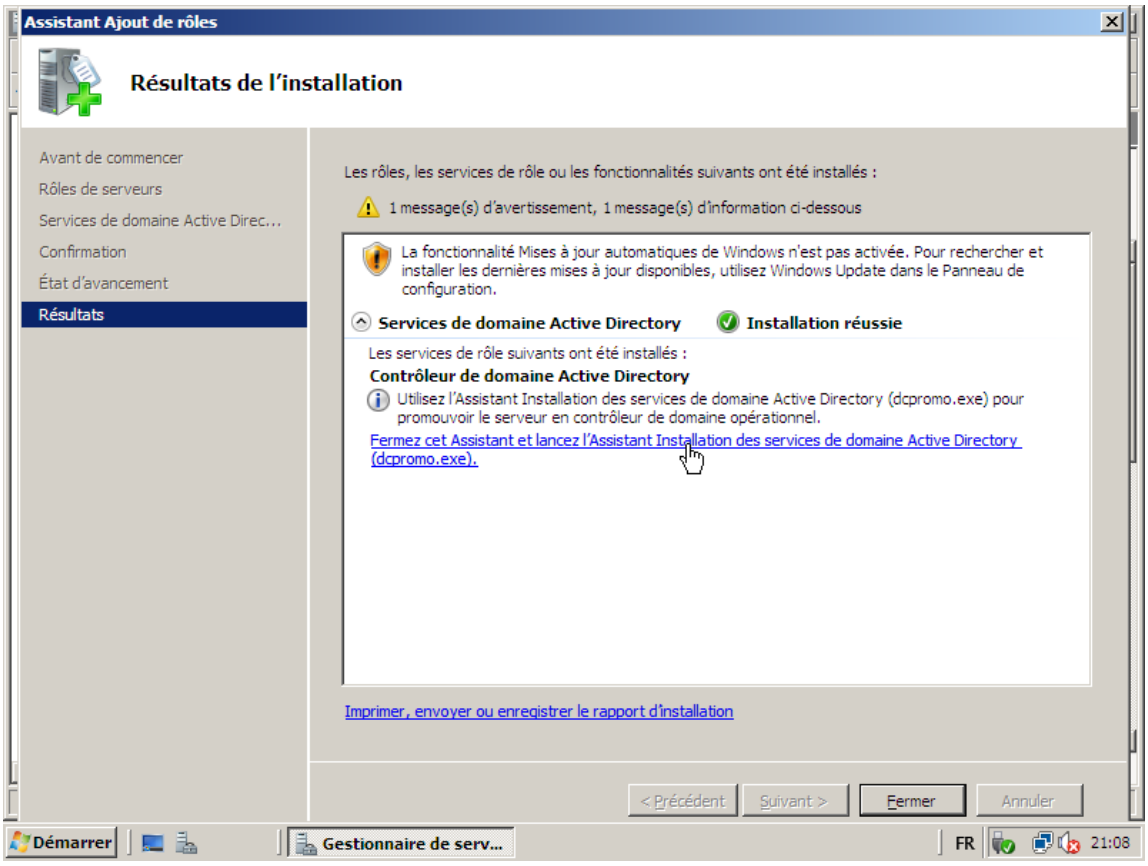
Puis cliquer sur **Suivant**.



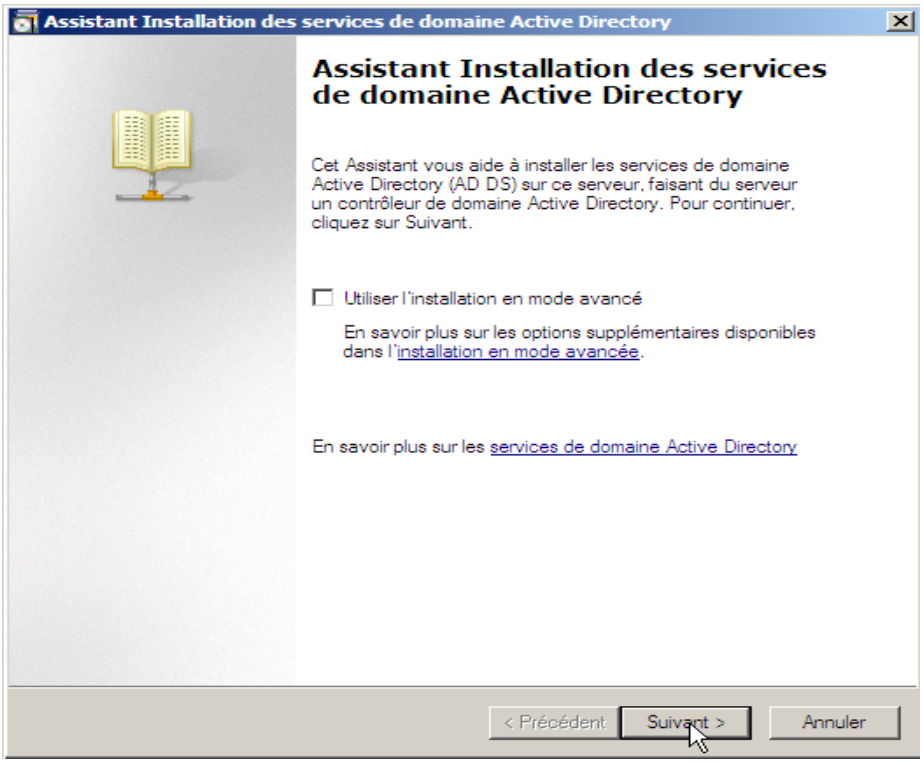
Pour confirmer l'installation du Services de domaine Active Directory on clique sur **Installer.**



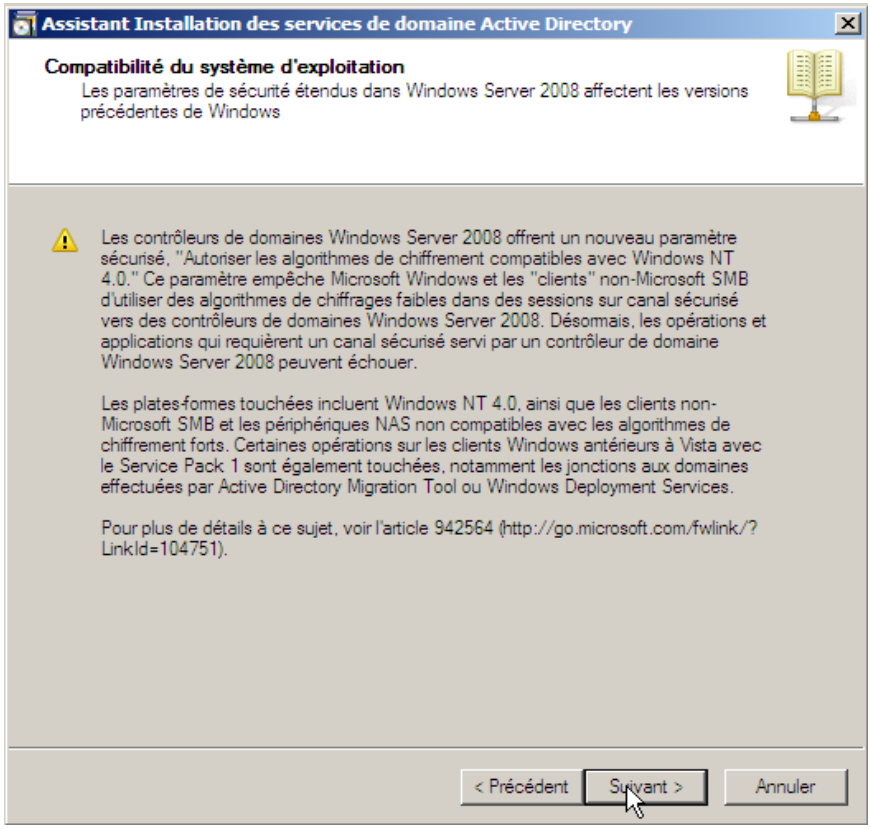
Puis on clique sur **Fermez cet Assistant et lancez l'assistant Installation des services de domaine Active Directory (dcpromo.exe).**



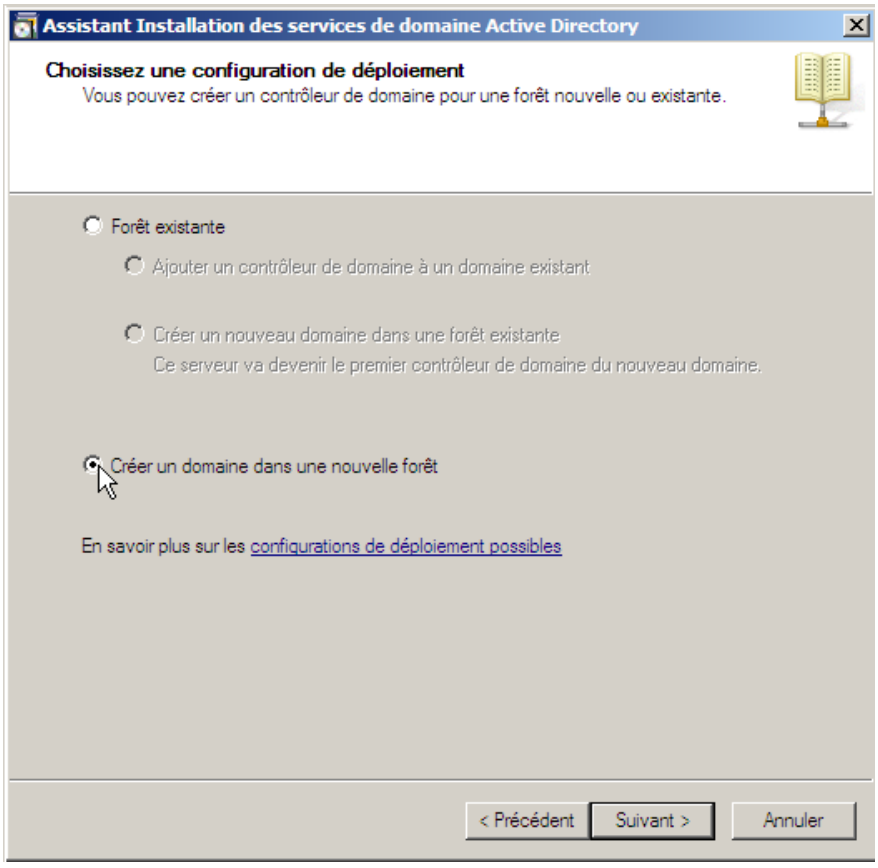
Assistant Installation des services de domaine Active Directory.



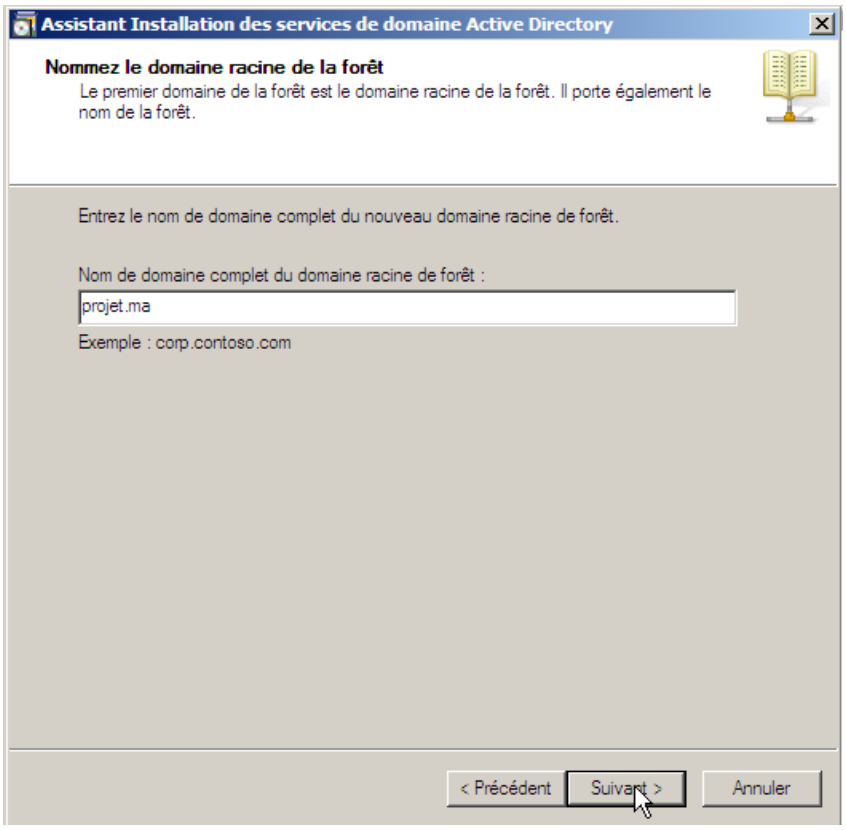
Cliquer sur **Suivant**.

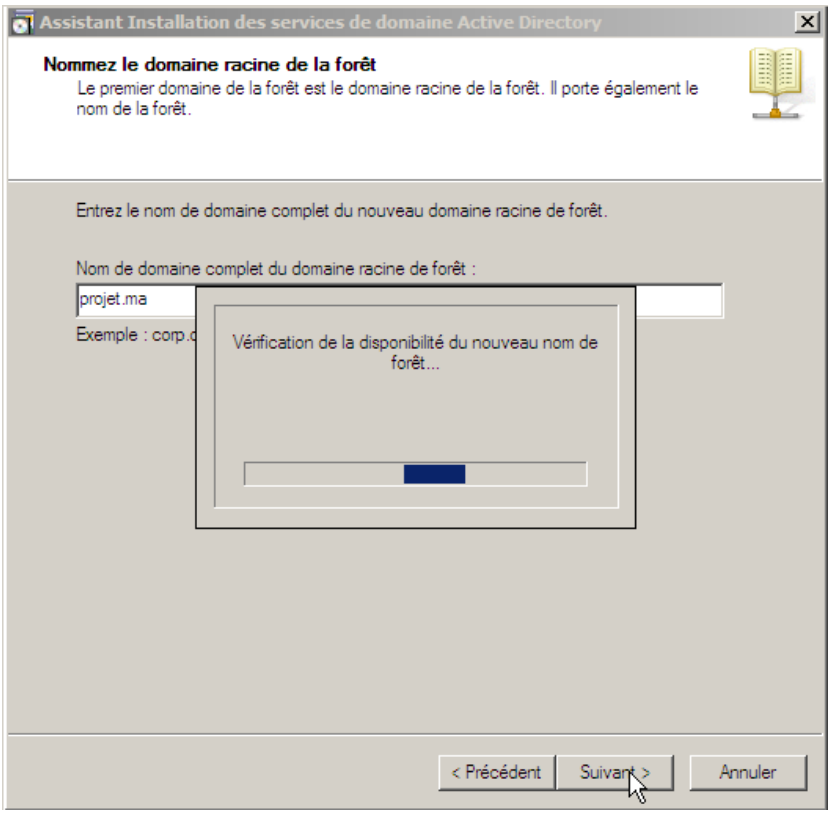


Créer un controleur de domaine dans une nouvelle forêt.

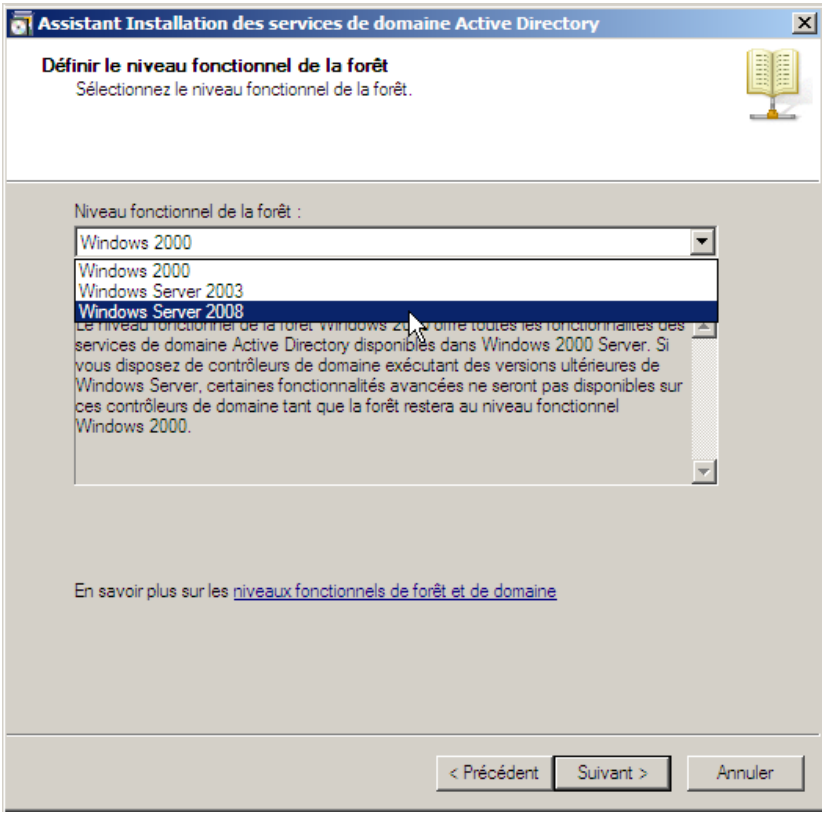


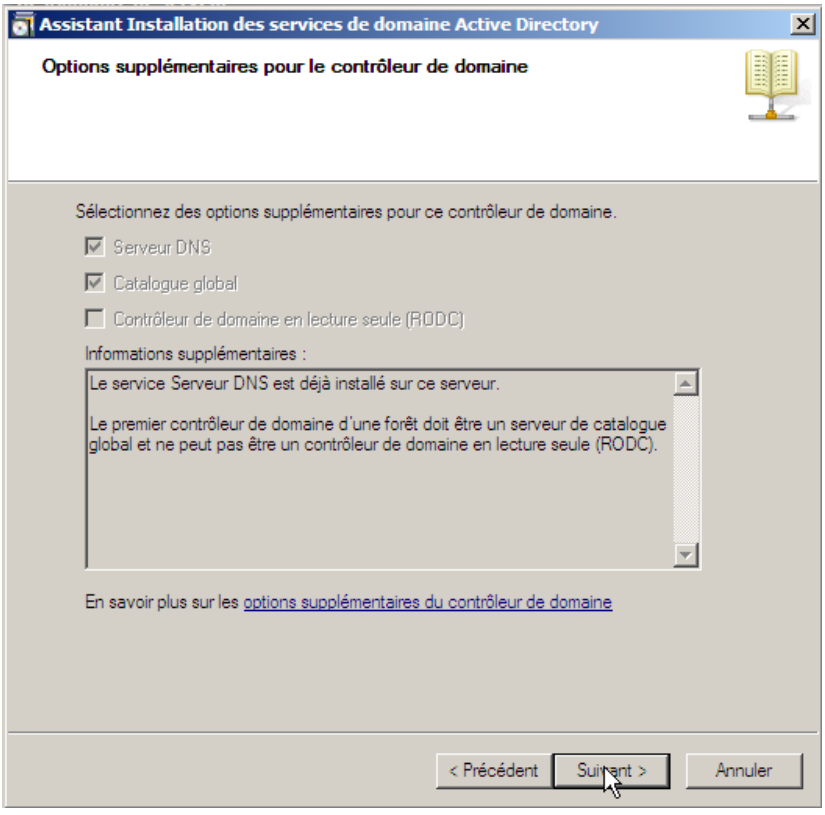
Entrez le nom de domaine complet du domaine racine de forêt .

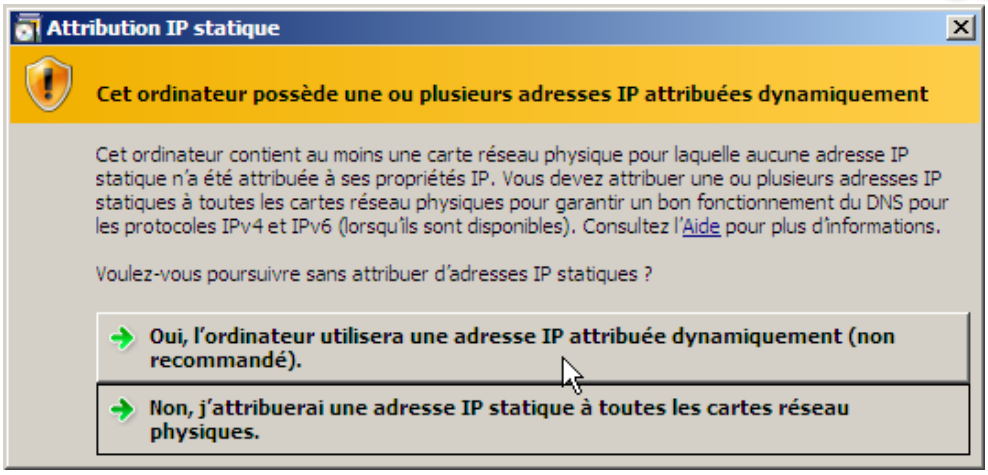


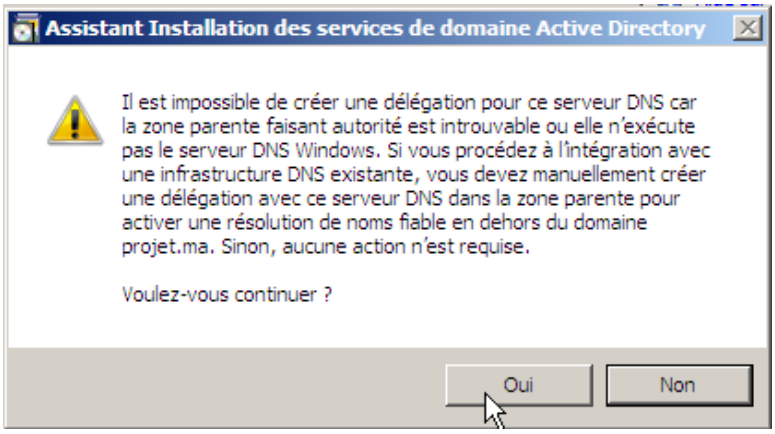


Sélectionnez le niveau fonctionnel de la foret

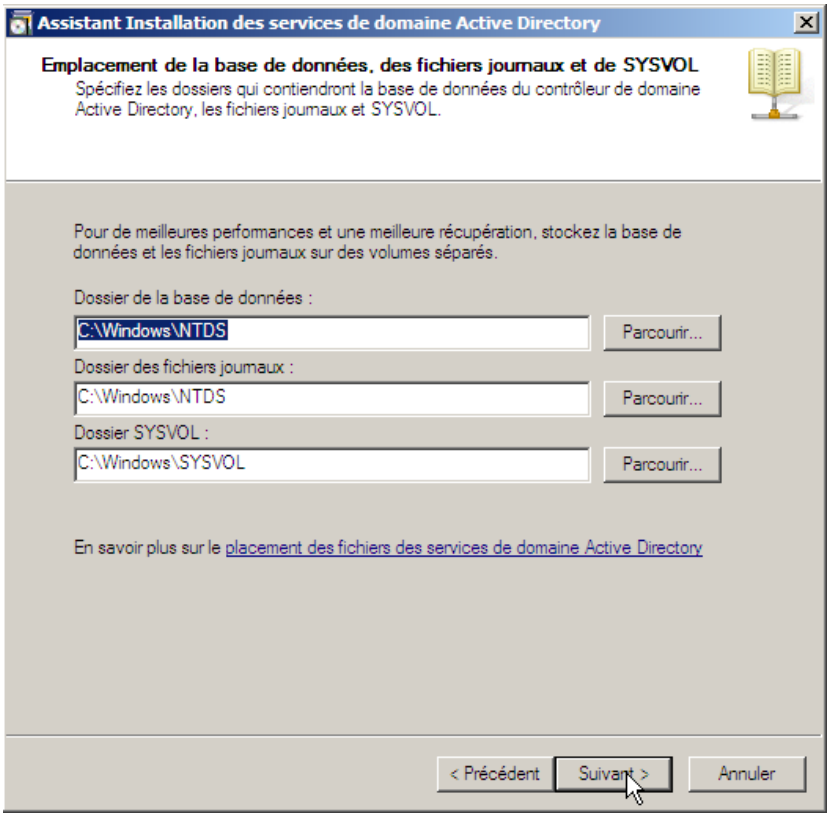




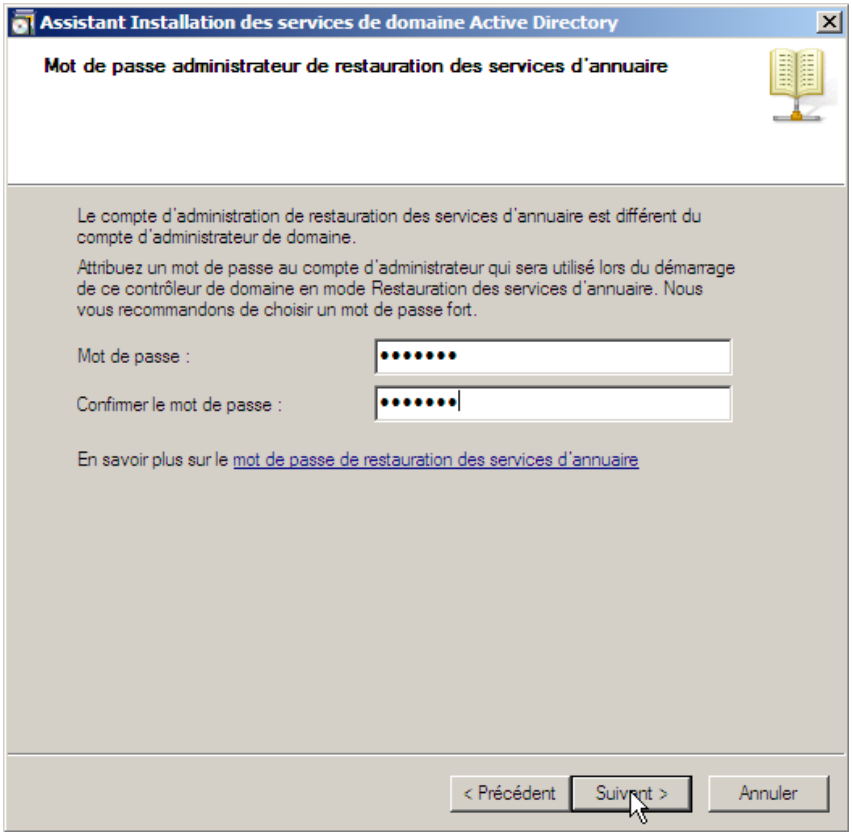


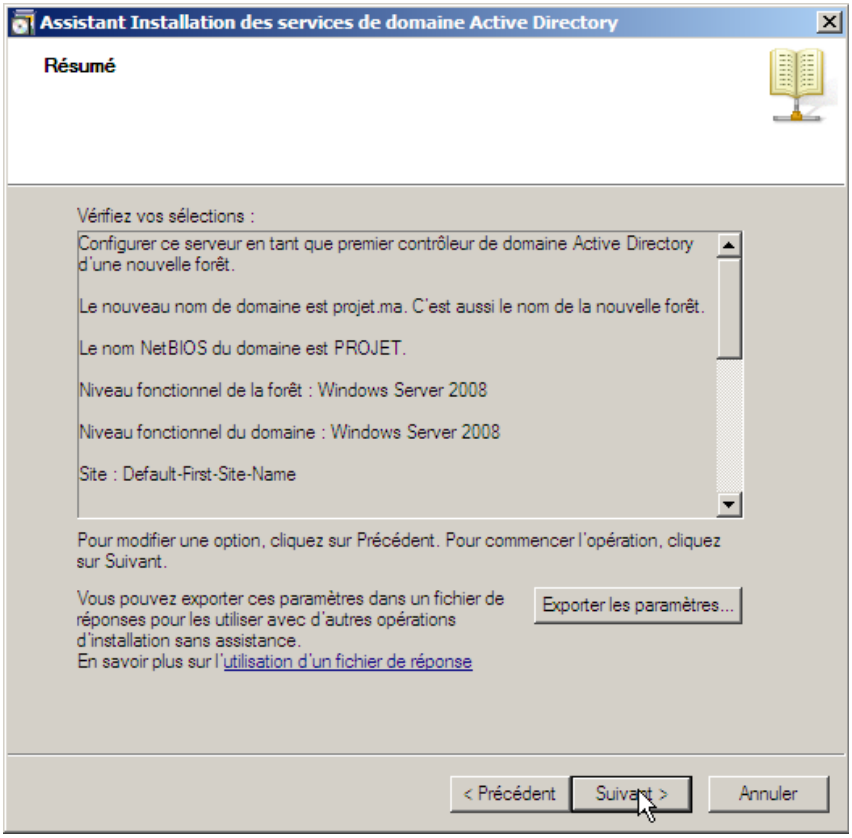


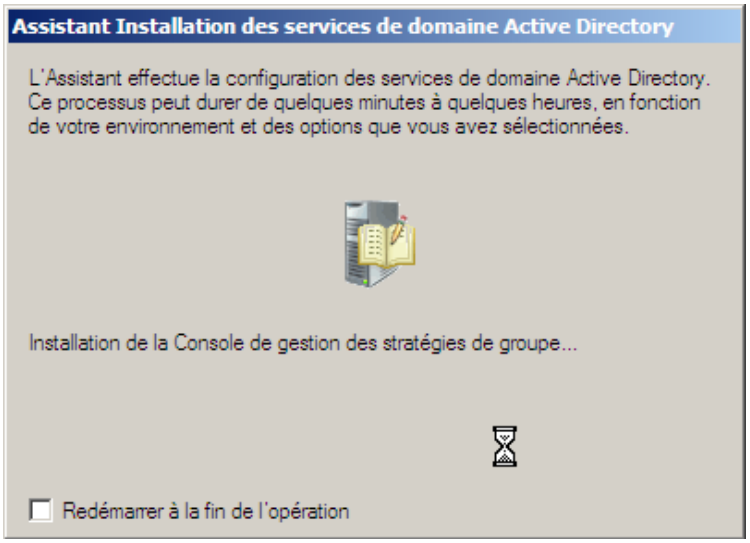
Définir l'emplacement de la base de données et des fichiers journaux et de SYSVOL



Mot de passe administrateur de restauration des services d'annuaire

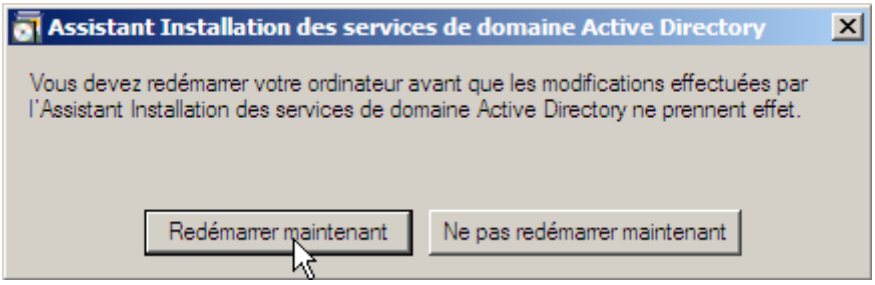






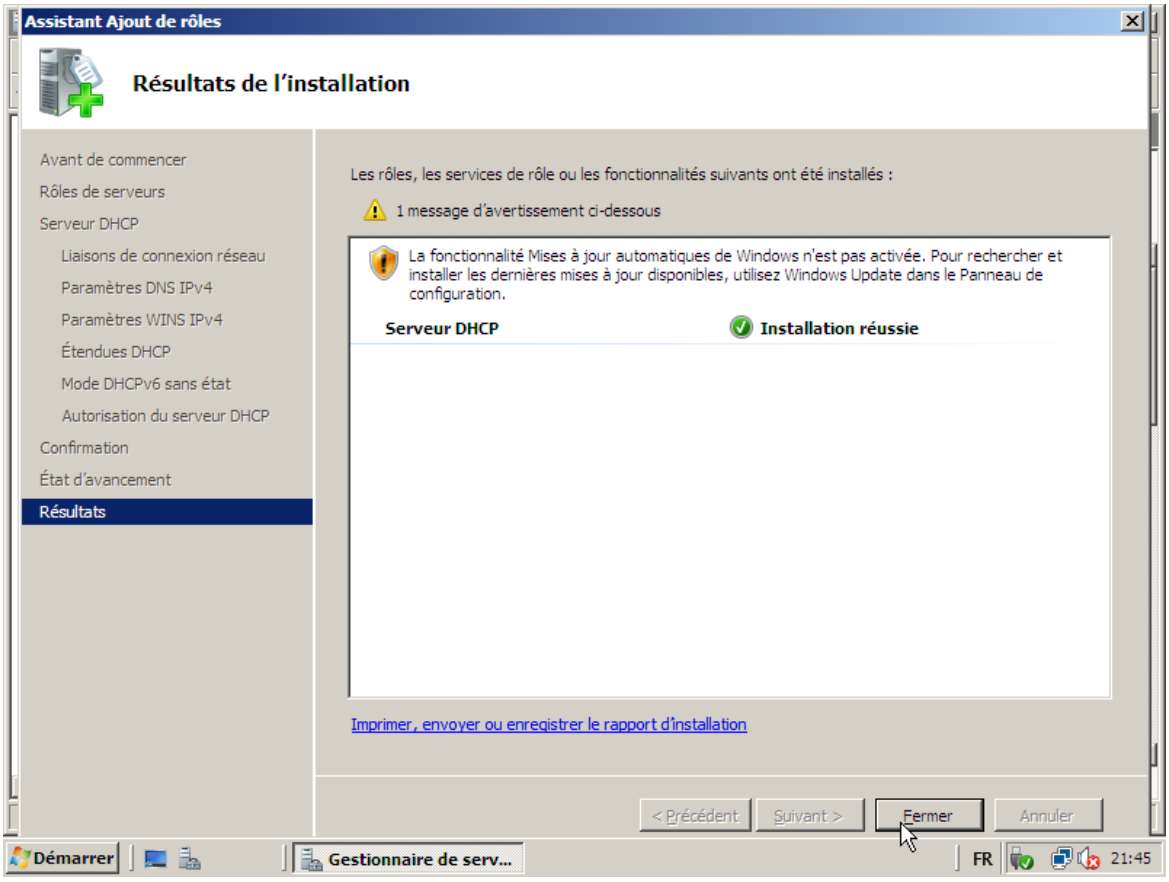
Cliquer sur Terminer.

Cliquer sur Redémarrer maintenant.

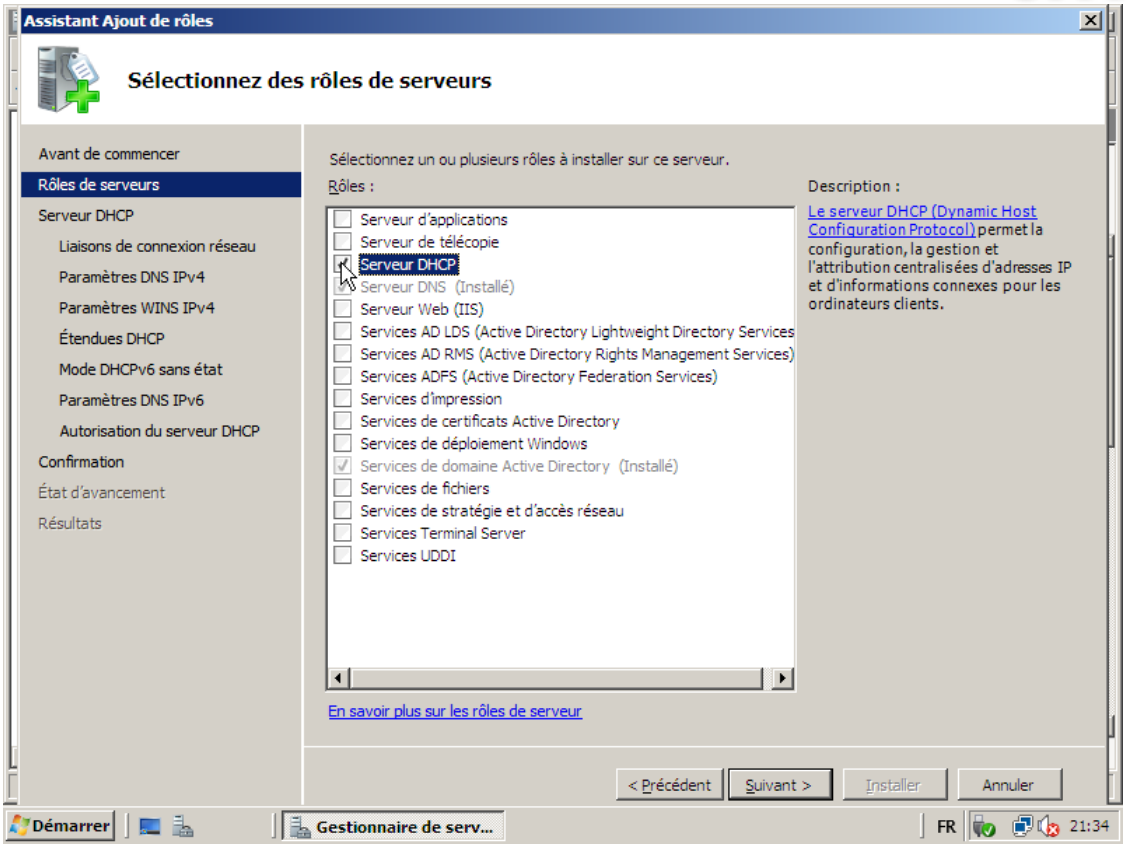


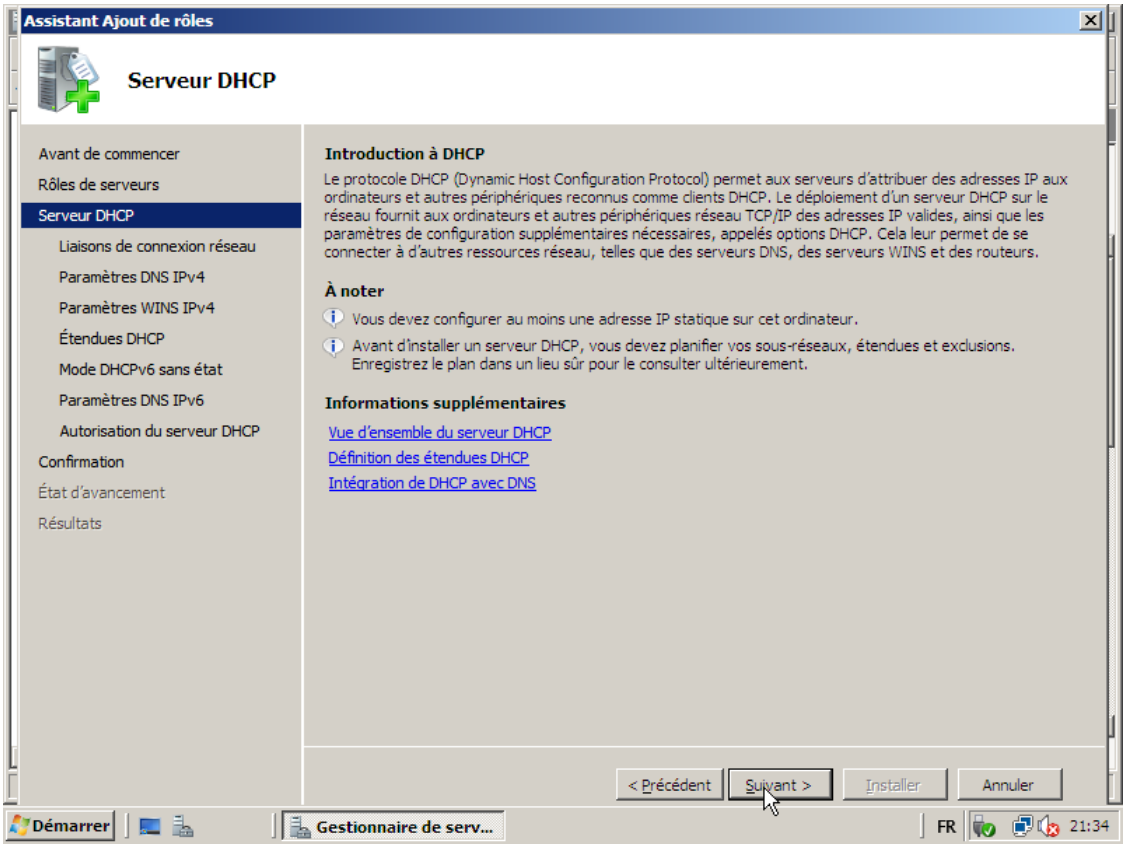
DHCP :

Le serveur DHCP (Dynamic Host Configuration Protocol) permet la configuration, la gestion et l'attribution centralisées d'adresse IP et d'informations connexes pour les ordinateurs clients.

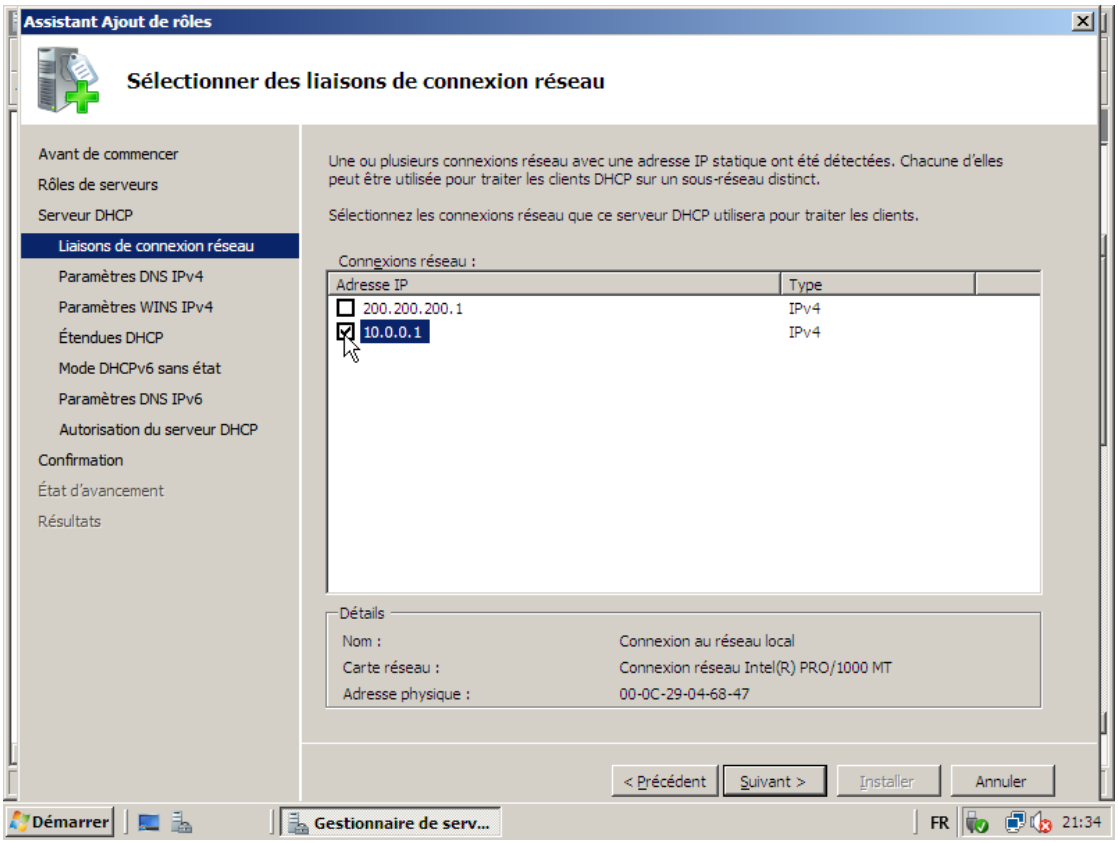


Choisi le rôle Serveur DHCP dans la liste des rôles puis cliquer sur Suivant

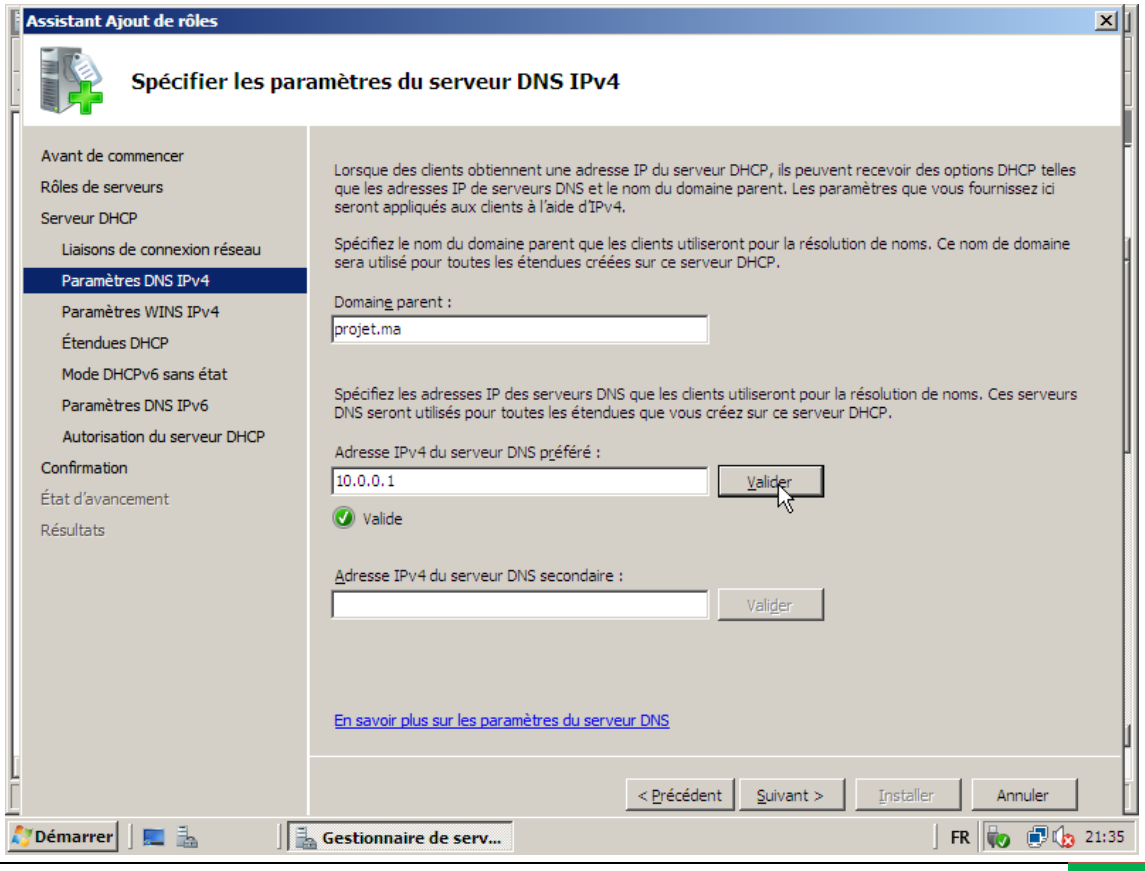

Assistant Ajout de rôles
Sélectionnez des rôles de serveurs
Avant de commencer
Rôles de serveurs
Serveur DHCP
Liaisons de connexion réseau
Paramètres DNS IPv4
Paramètres WINS IPv4
Étendues DHCP
Mode DHCPv6 sans état
Paramètres DNS IPv6
Autorisation du serveur DHCP
Confirmation
État d'avancement
Résultats
Sélectionnez un ou plusieurs rôles à installer sur ce serveur.
Rôles :
Serveur d'applications
Serveur de télécopie
Serveur DHCP
Serveur DNS (Installé)
Serveur Web (IIS)
Services AD LDS (Active Directory Lightweight Directory Services)
Services AD RMS (Active Directory Rights Management Services)
Services ADFS (Active Directory Federation Services)
Services d'impression
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory (Installé)
Services de fichiers
Services de stratégie et d'accès réseau
Services Terminal Server
Services UDDI
Description :
Le serveur DHCP (Dynamic Host Configuration Protocol) permet la configuration, la gestion et l'attribution centralisées d'adresses IP et d'informations connexes pour les ordinateurs clients.
En savoir plus sur les rôles de serveur
< Précédent
Suivant >
Installer
Annuler
Démarrer
Gestionnaire de serv...
FR
21:34


Assistant Ajout de rôles
Serveur DHCP
Avant de commencer
Rôles de serveurs
Serveur DHCP
Liaisons de connexion réseau
Paramètres DNS IPv4
Paramètres WINS IPv4
Étendues DHCP
Mode DHCPv6 sans état
Paramètres DNS IPv6
Autorisation du serveur DHCP
Confirmation
État d'avancement
Résultats
Introduction à DHCP
Le protocole DHCP (Dynamic Host Configuration Protocol) permet aux serveurs d'attribuer des adresses IP aux ordinateurs et autres périphériques reconnus comme clients DHCP. Le déploiement d'un serveur DHCP sur le réseau fournit aux ordinateurs et autres périphériques réseau TCP/IP des adresses IP valides, ainsi que les paramètres de configuration supplémentaires nécessaires, appelés options DHCP. Cela leur permet de se connecter à d'autres ressources réseau, telles que des serveurs DNS, des serveurs WINS et des routeurs.
À noter
Vous devez configurer au moins une adresse IP statique sur cet ordinateur.
Avant d'installer un serveur DHCP, vous devez planifier vos sous-réseaux, étendues et exclusions. Enregistrez le plan dans un lieu sûr pour le consulter ultérieurement.
Informations supplémentaires
Vue d'ensemble du serveur DHCP
Définition des étendues DHCP
Intégration de DHCP avec DNS
< Précédent
Suivant >
Installer
Annuler
Démarrer
Gestionnaire de serv...
FR
21:34

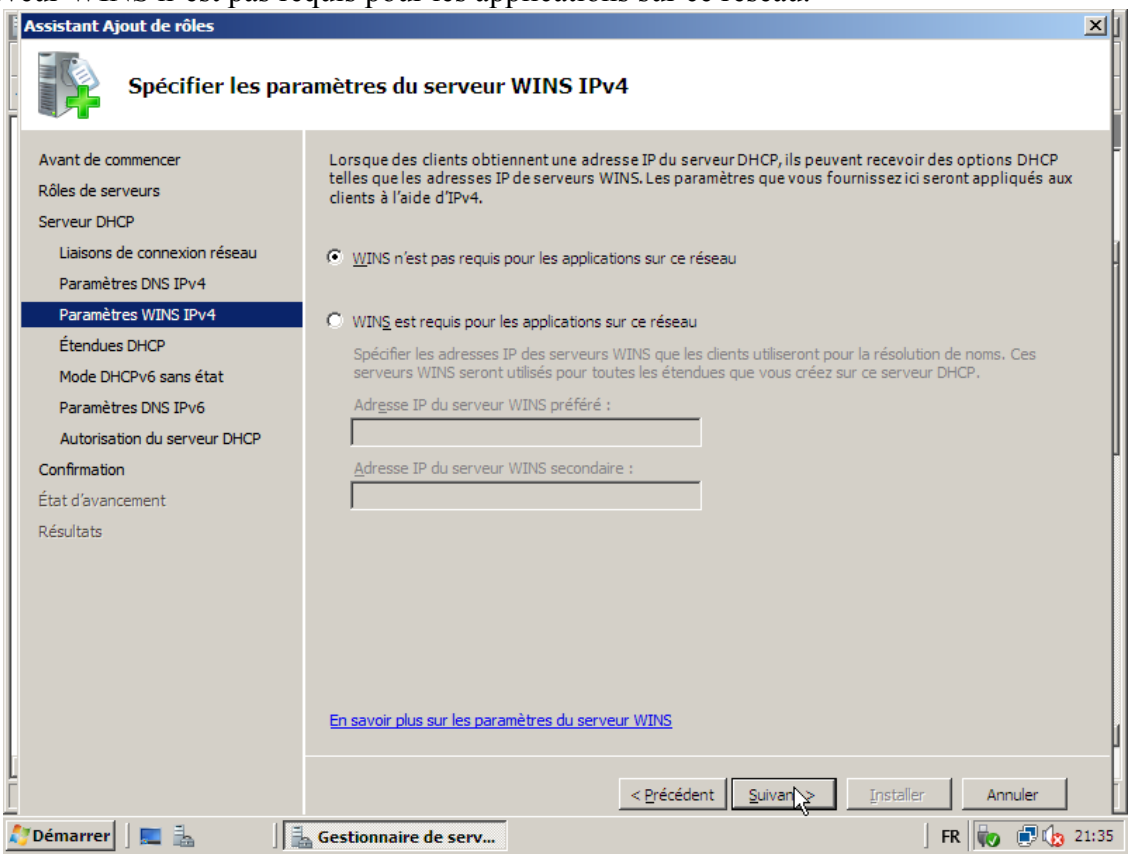
Sélectionnez l'adresse IP privée



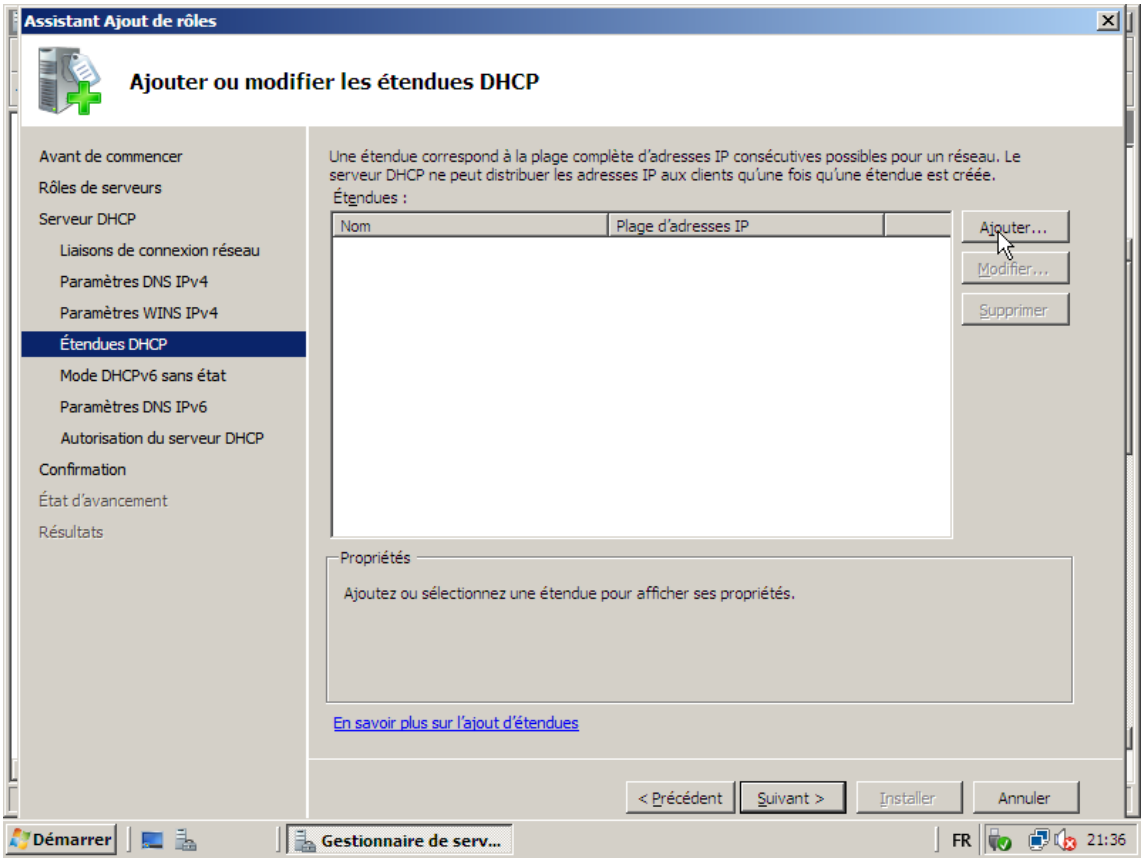
Donner le nom de domaine parent DNS et l'adresse IPv4 du serveur DNS préférer



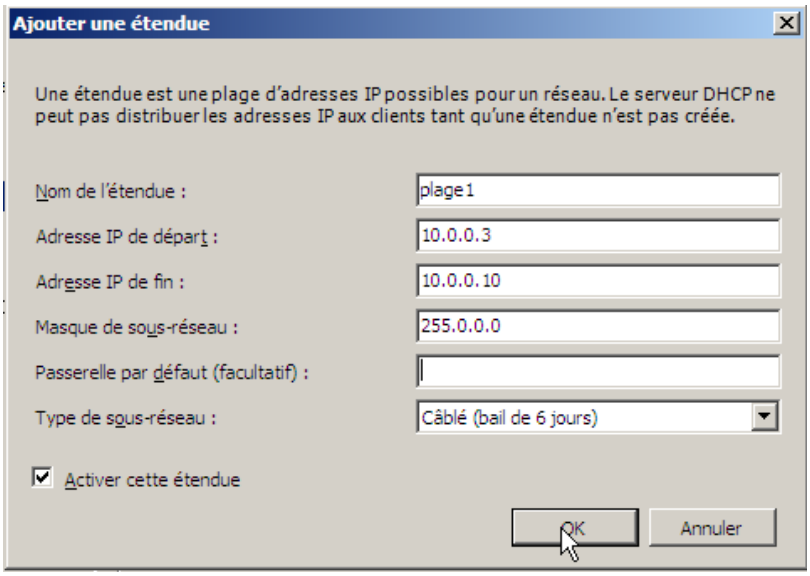
Serveur WINS n'est pas requis pour les applications sur ce réseau.

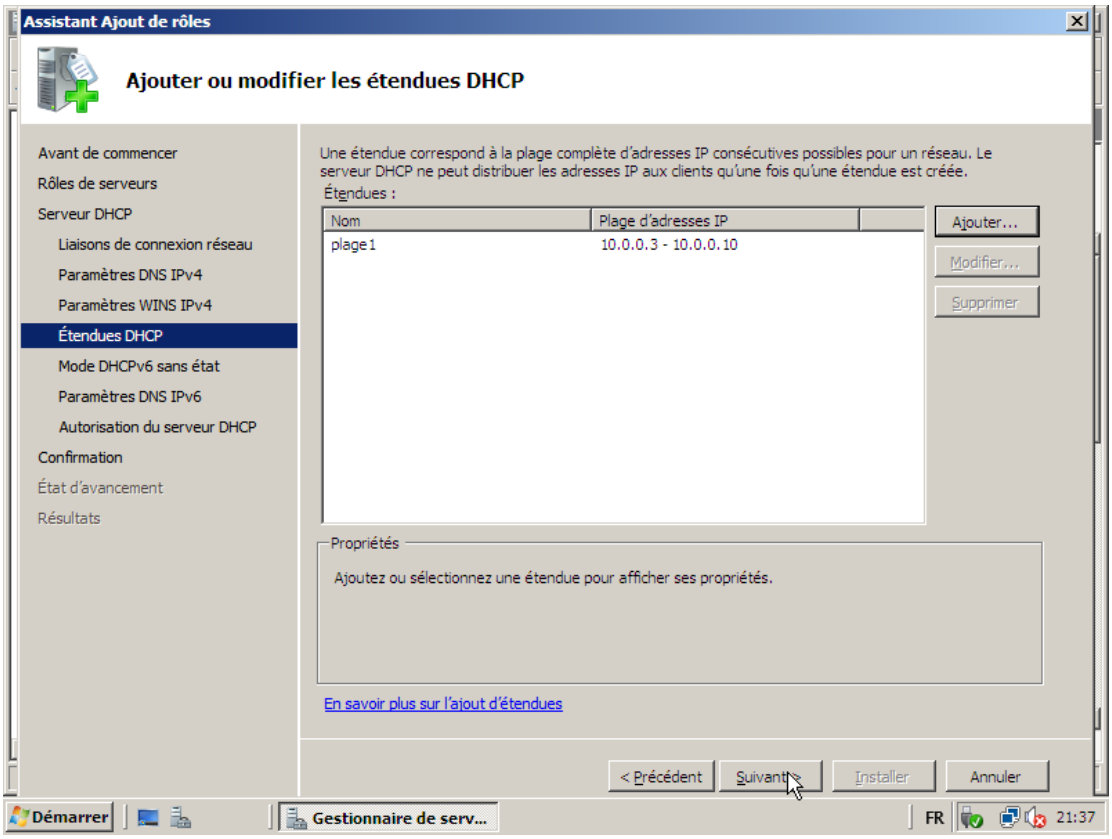


Cliquer sur Ajouter pour ajouter une plage étendue DHCP

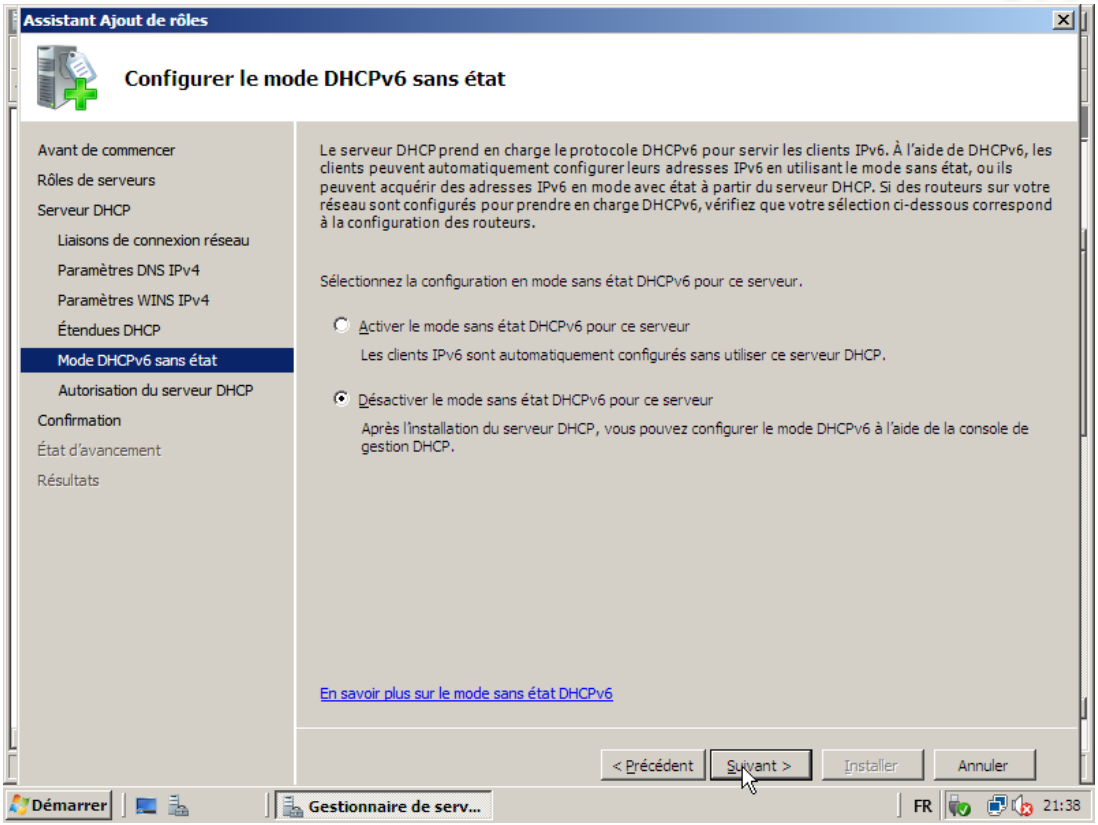


Donner un nom à la plage et l'adresse IP de départ et fin de la plage.

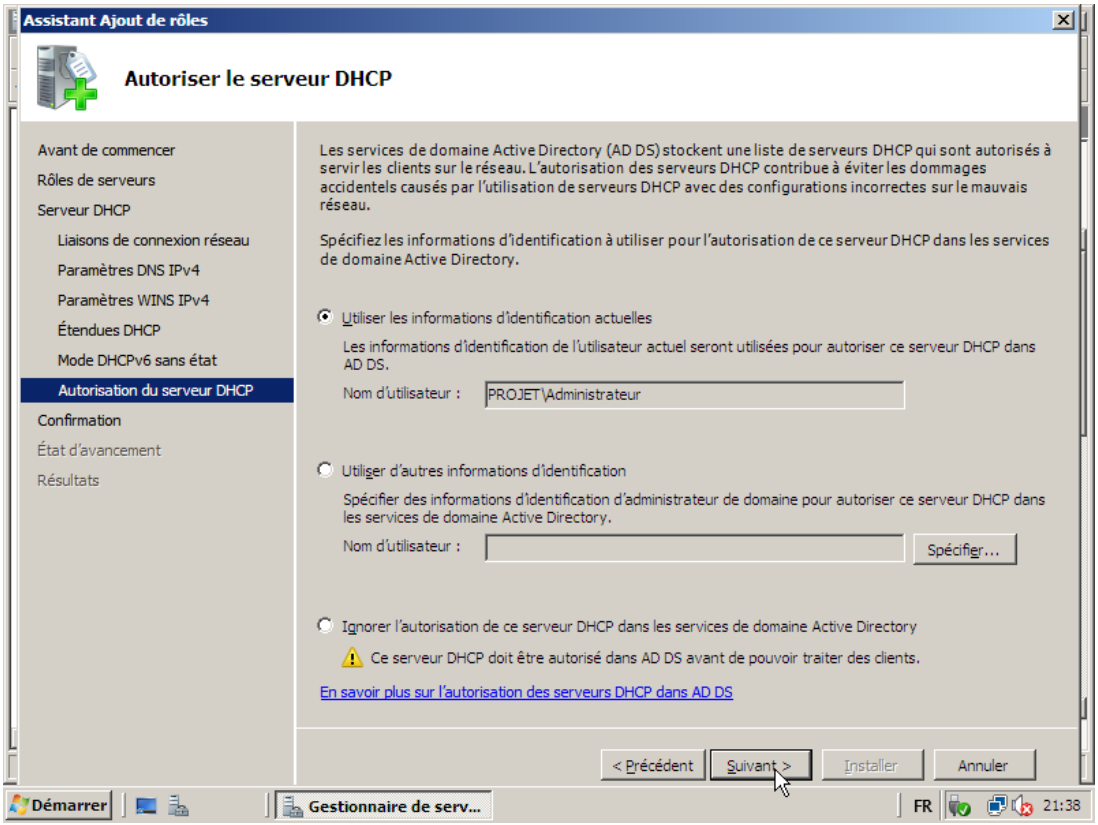




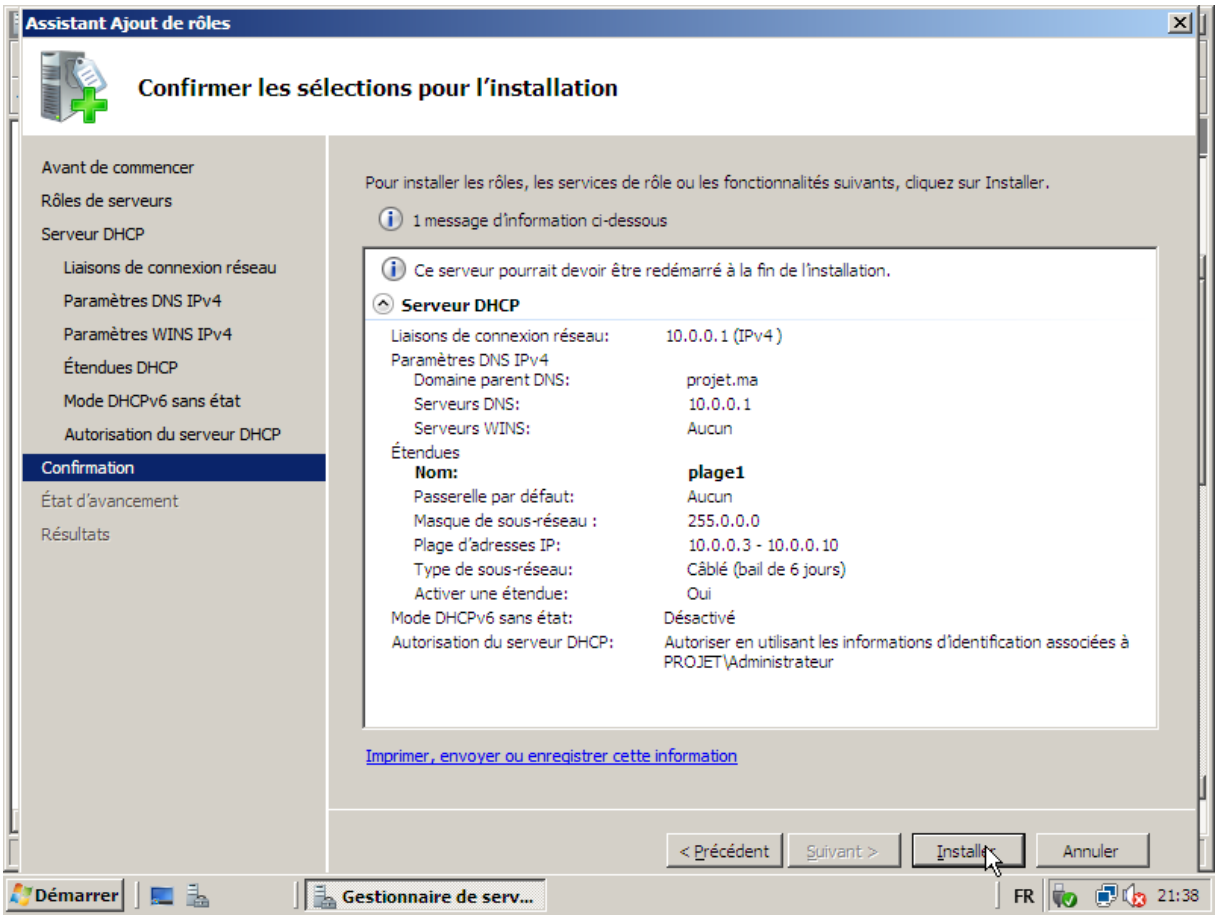
Désactiver le mode sans état DHCPv6 pour ce serveur



Autoriser le serveur DHCP pour utiliser les informations d'identification actuelles

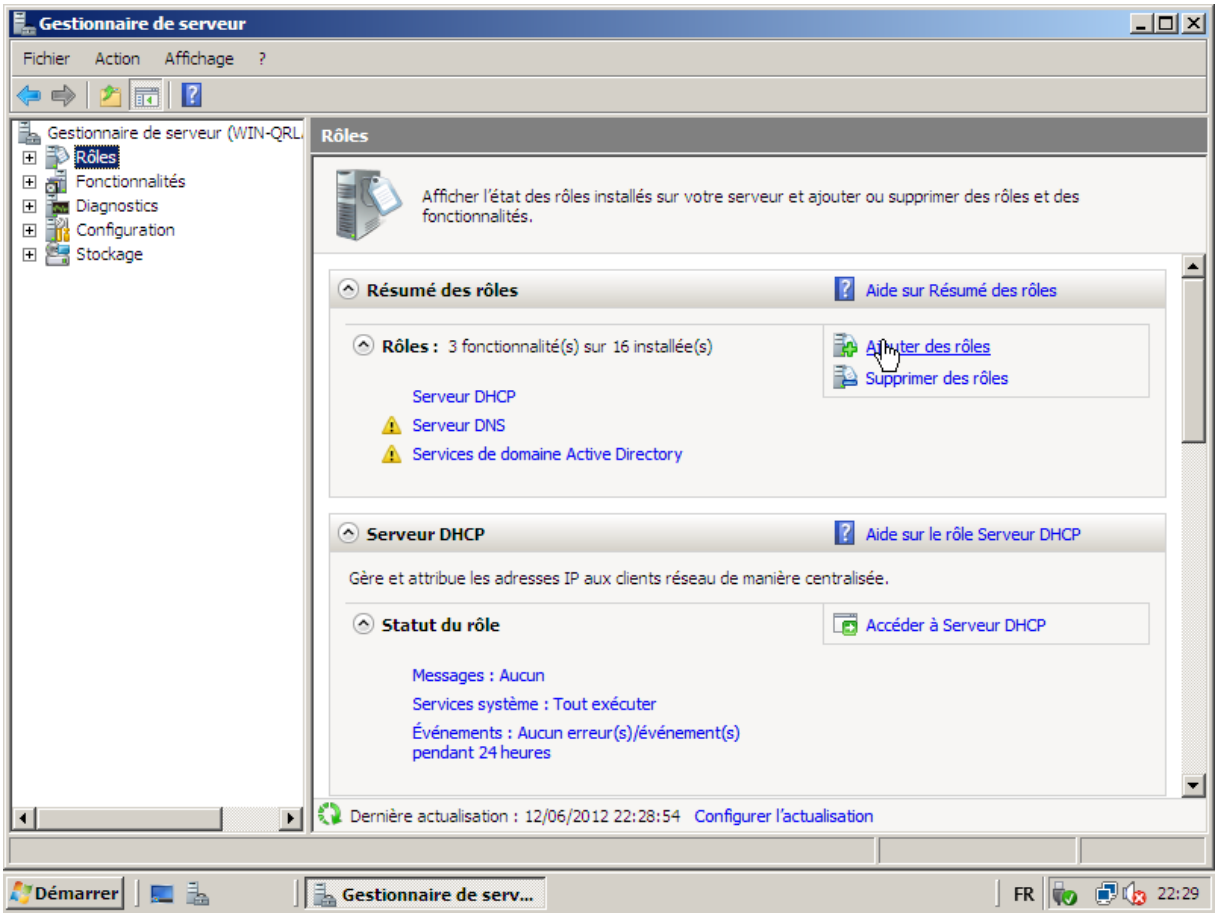


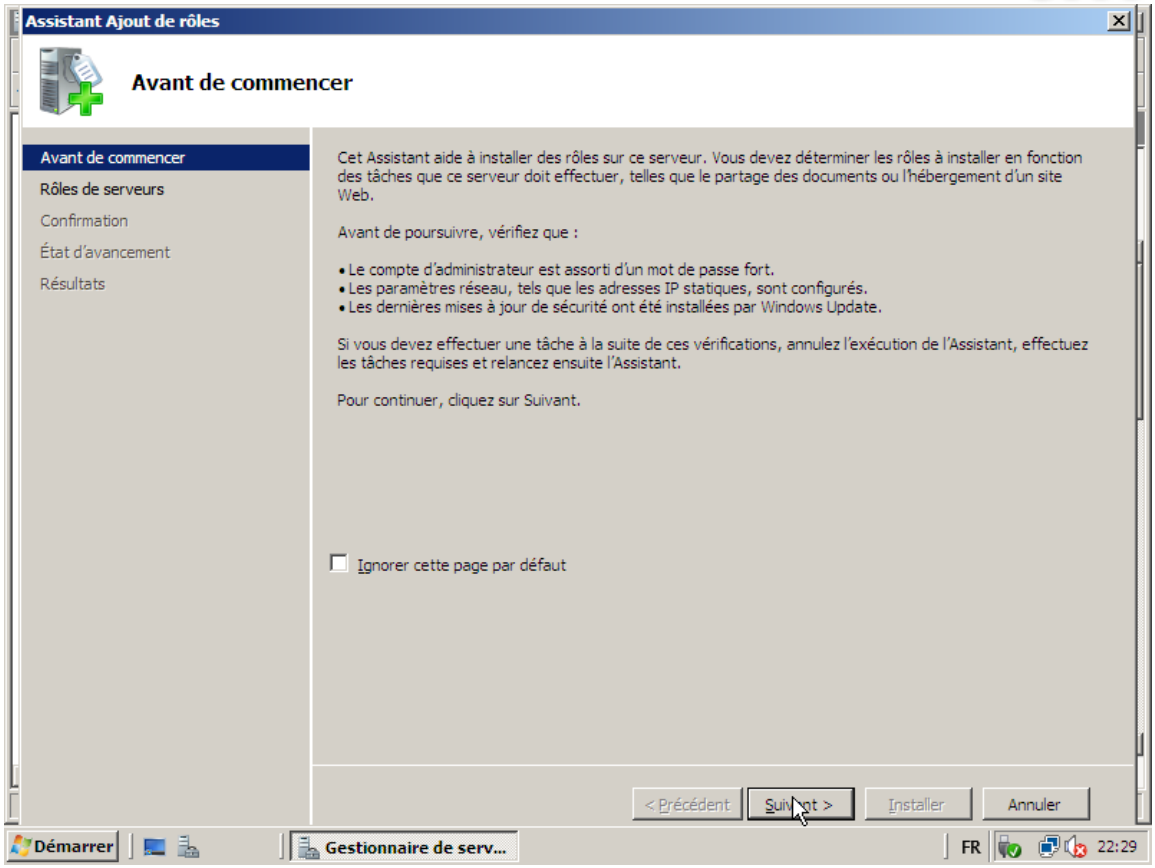
Cliquer sur Installer pour confirmer l'installation du serveur DHCP.



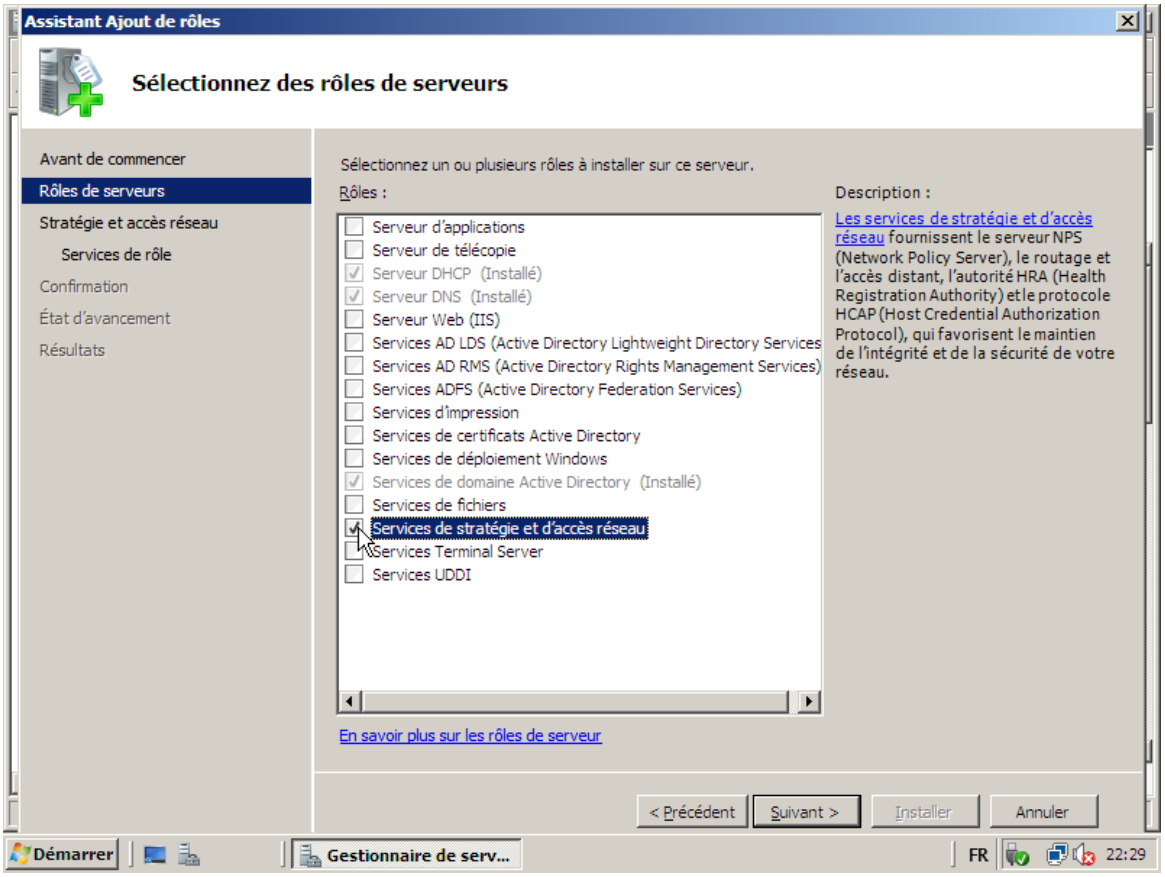
Services de stratégie et d'accès réseau :

Les services de stratégie et d'accès réseau fournissent le serveur NPS (Network Policy Server), le routage et l'accès distant, l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.

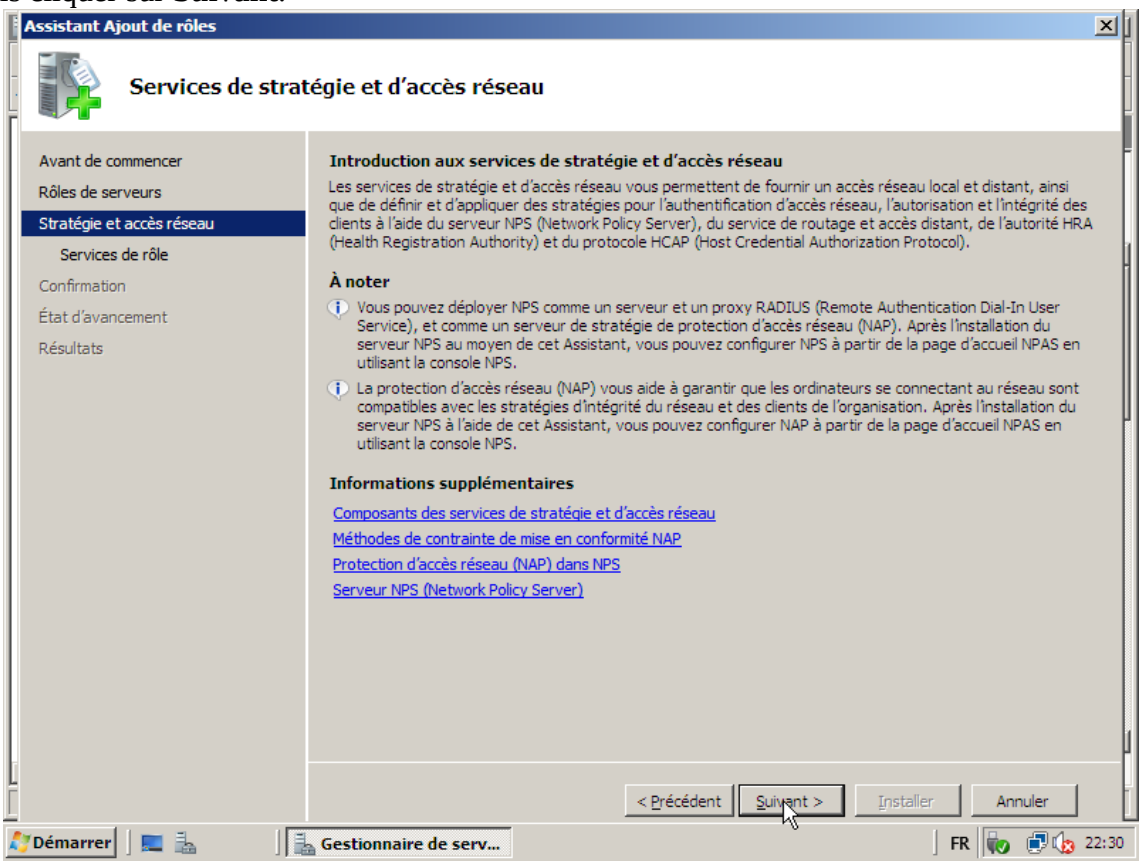




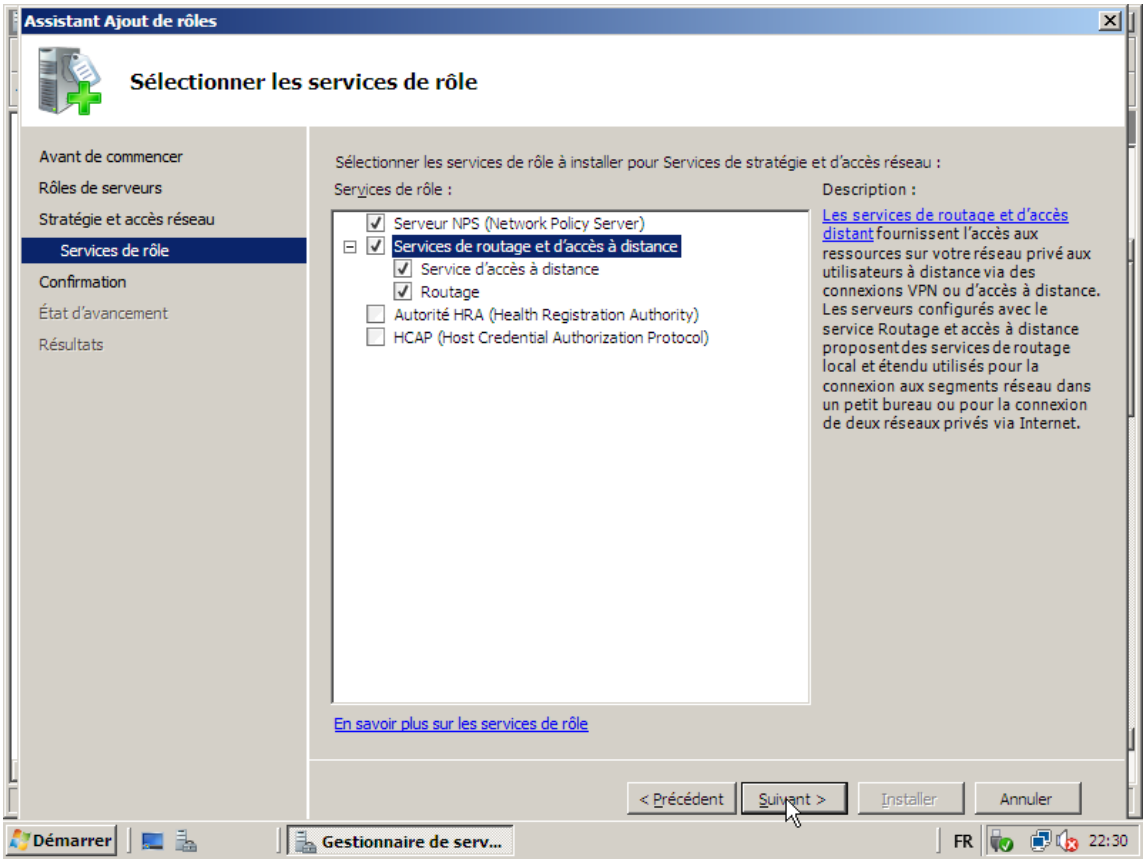
Choisi le rôle Services de stratégie et d'accès réseau puis cliquez sur Suivant.



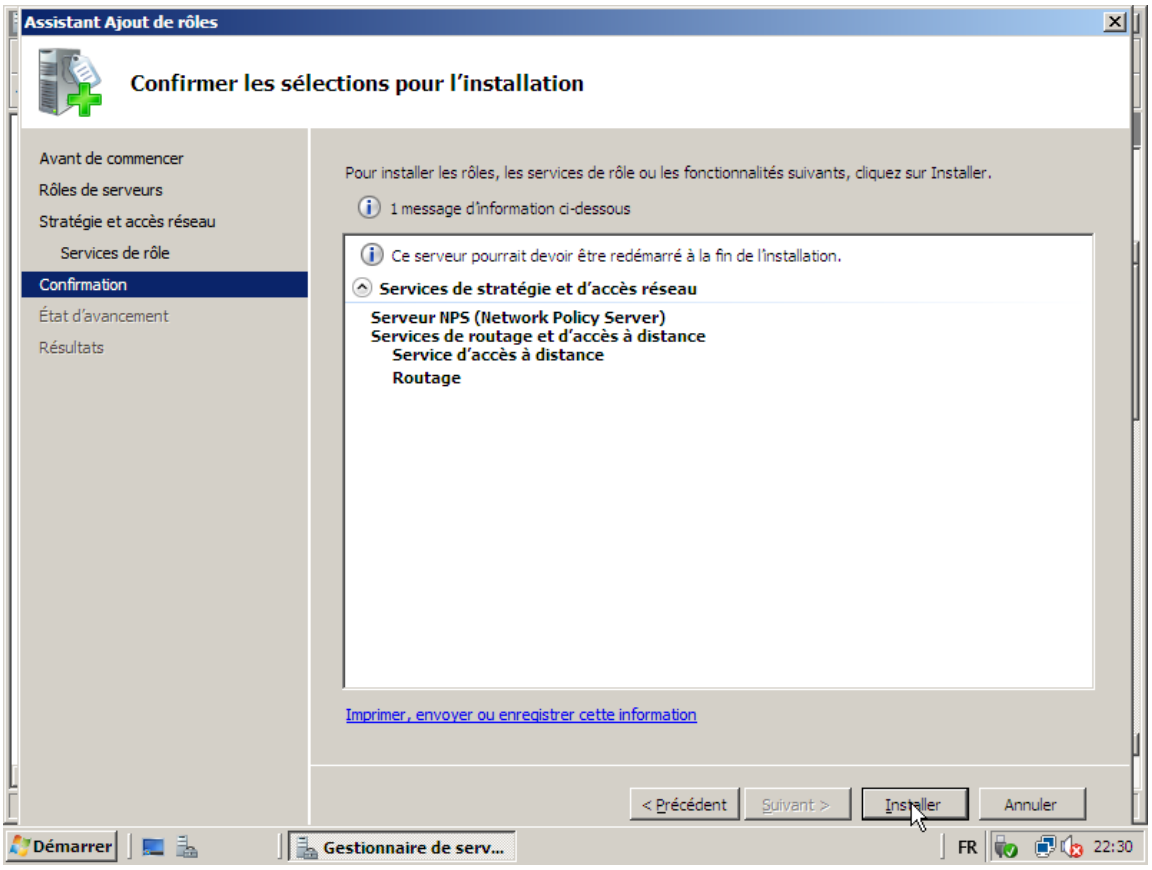
Puis cliquer sur **Suivant**.

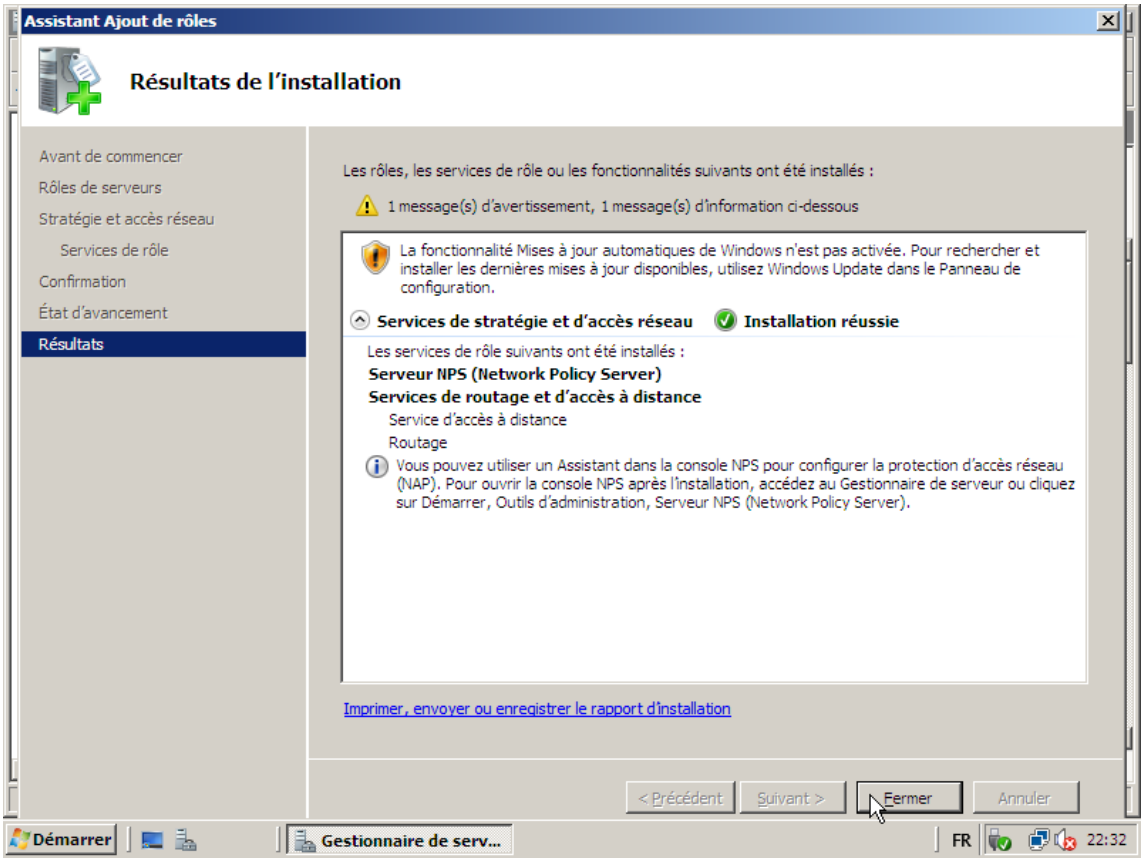


Choisi le serveur NPS et le service de routage et d'accès à distance

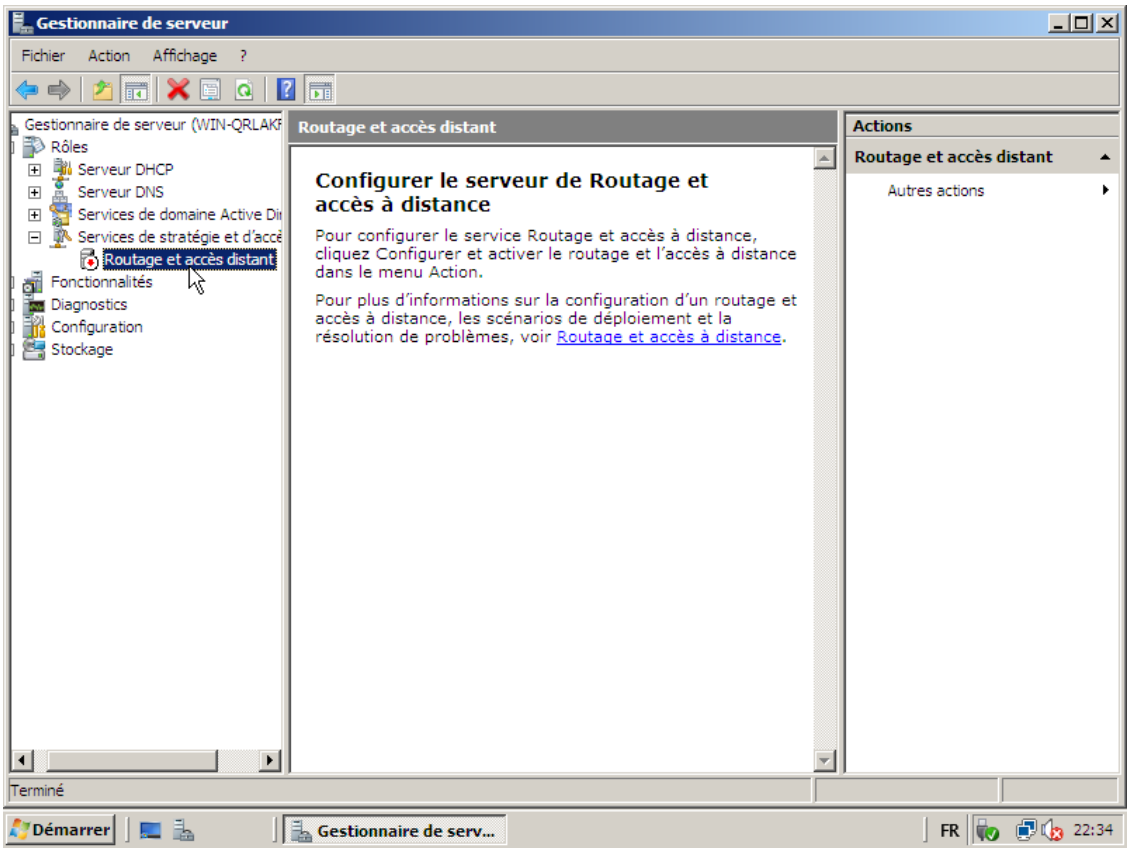


Pour confirmer l'installation cliquer sur Installer.

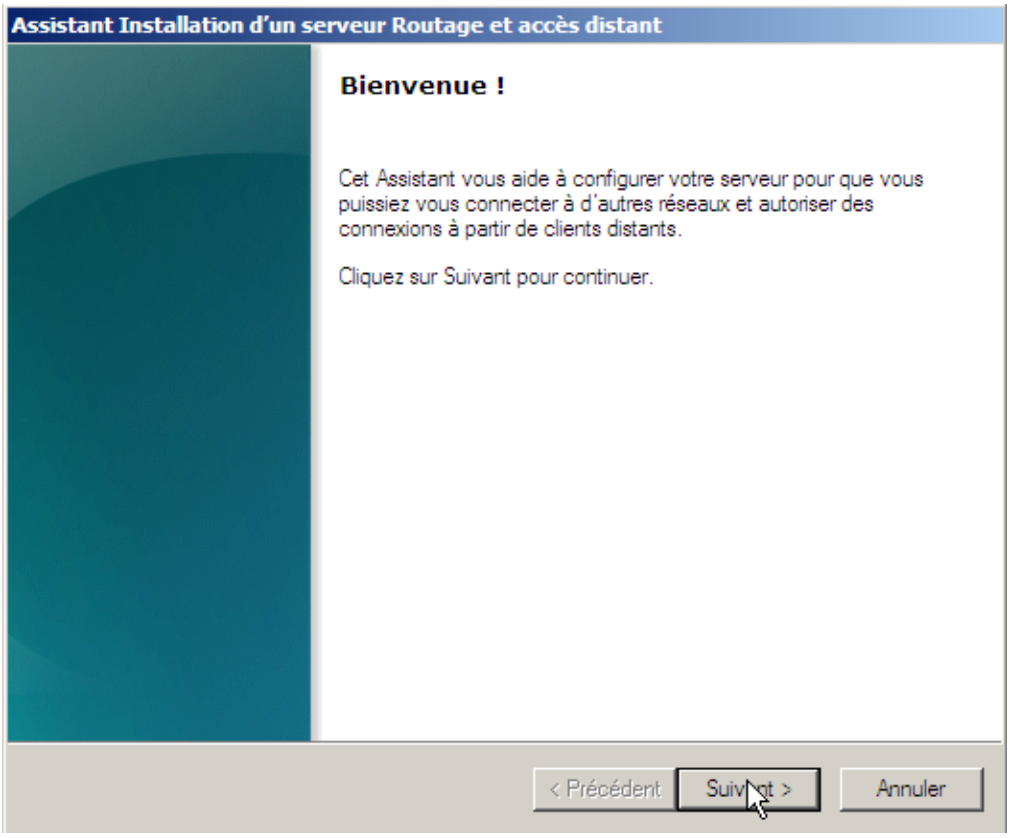




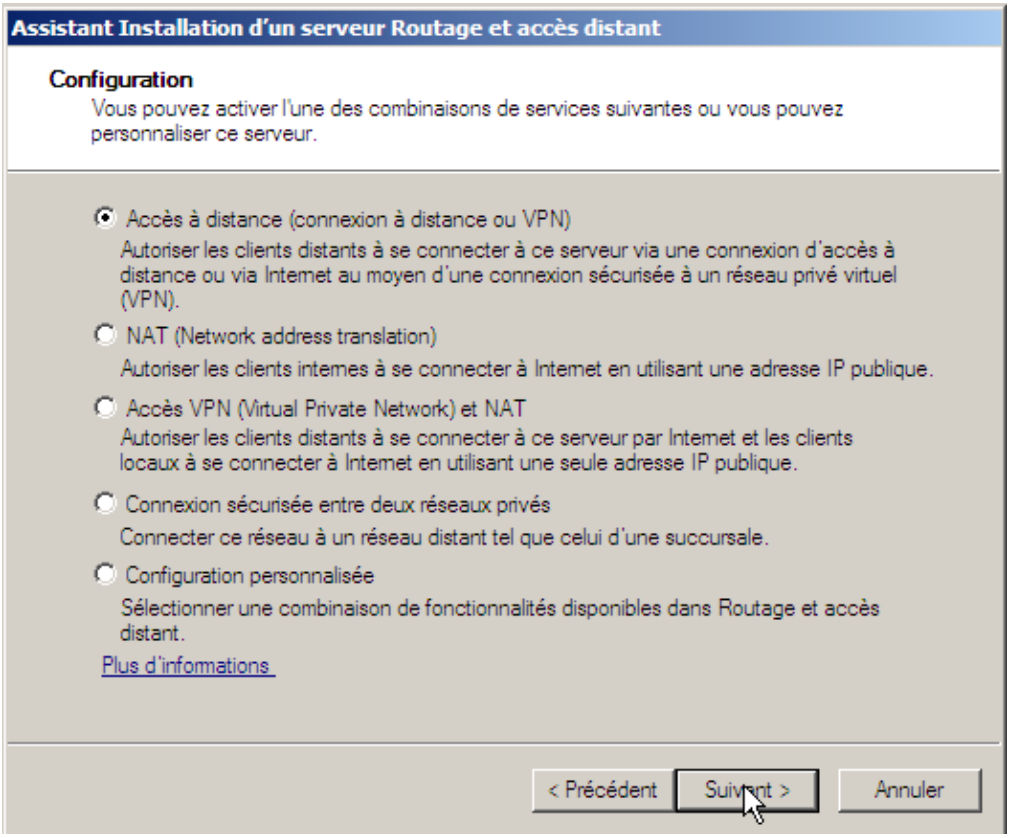
Clic droit sur Routage et accès distant puis Installation d'un serveur routage et accès distant



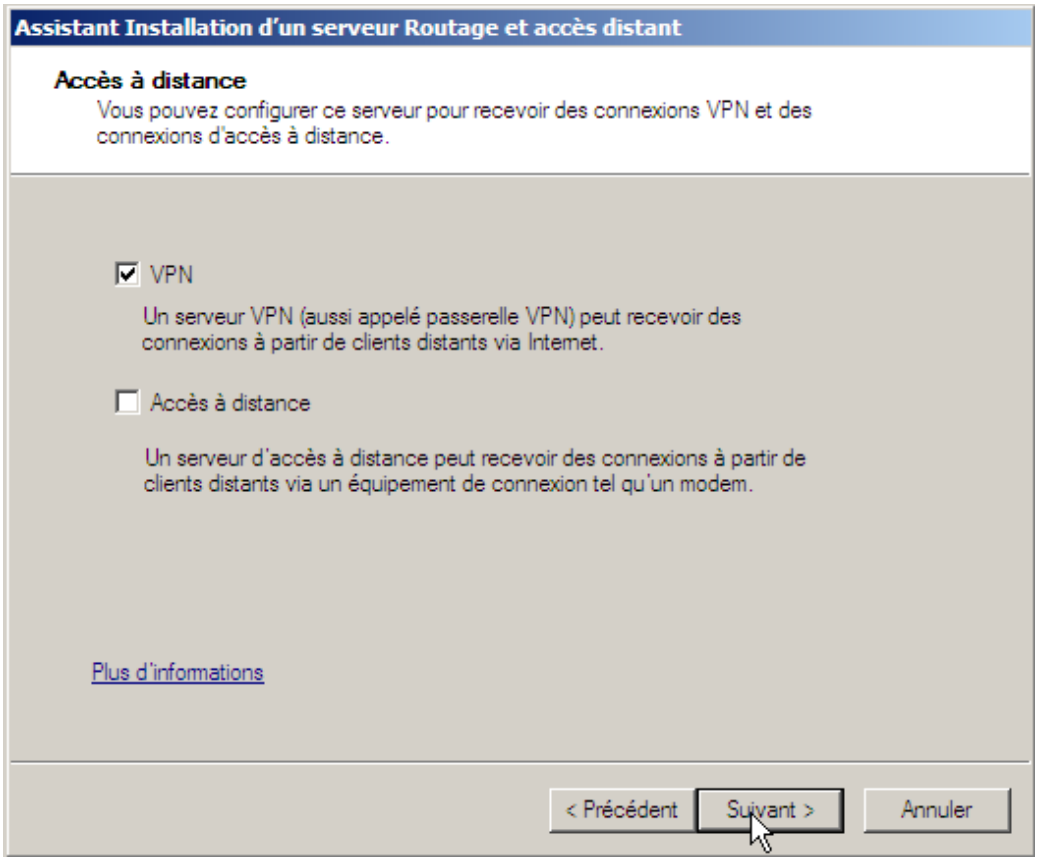
Clique sur suivant pour continuer l'installation



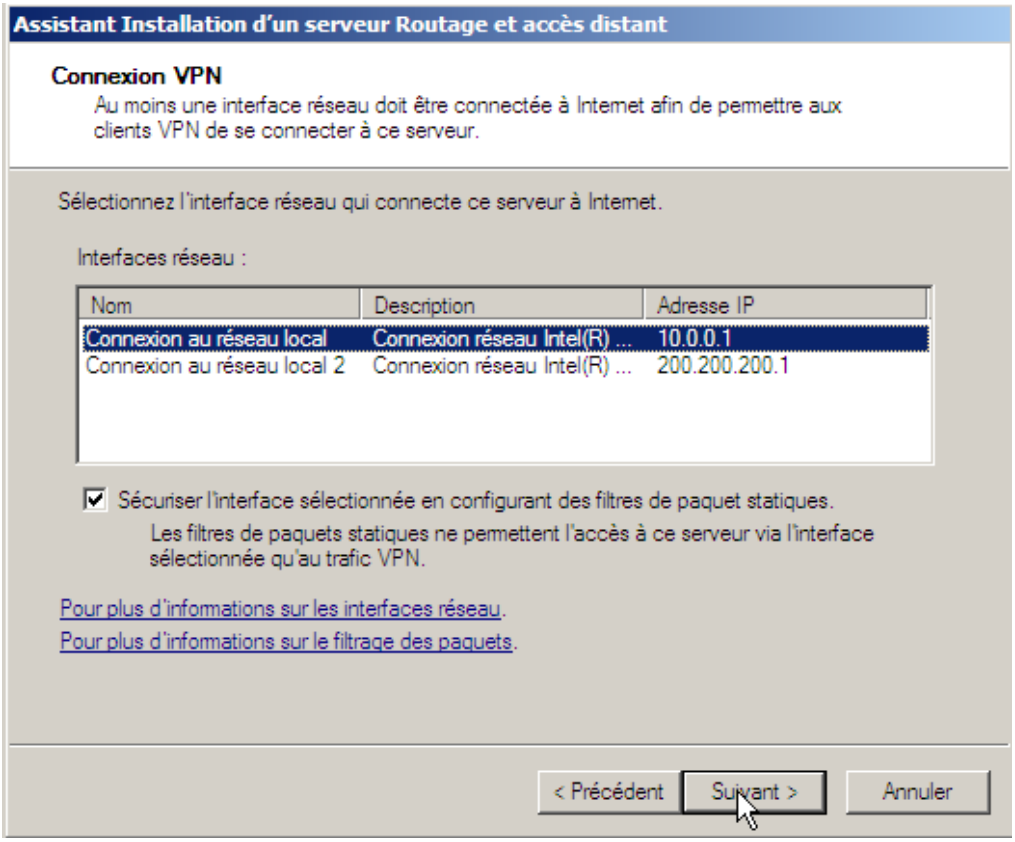
Choisi Accès à distance (connexion à distance ou VPN) puis clique sur Suivant



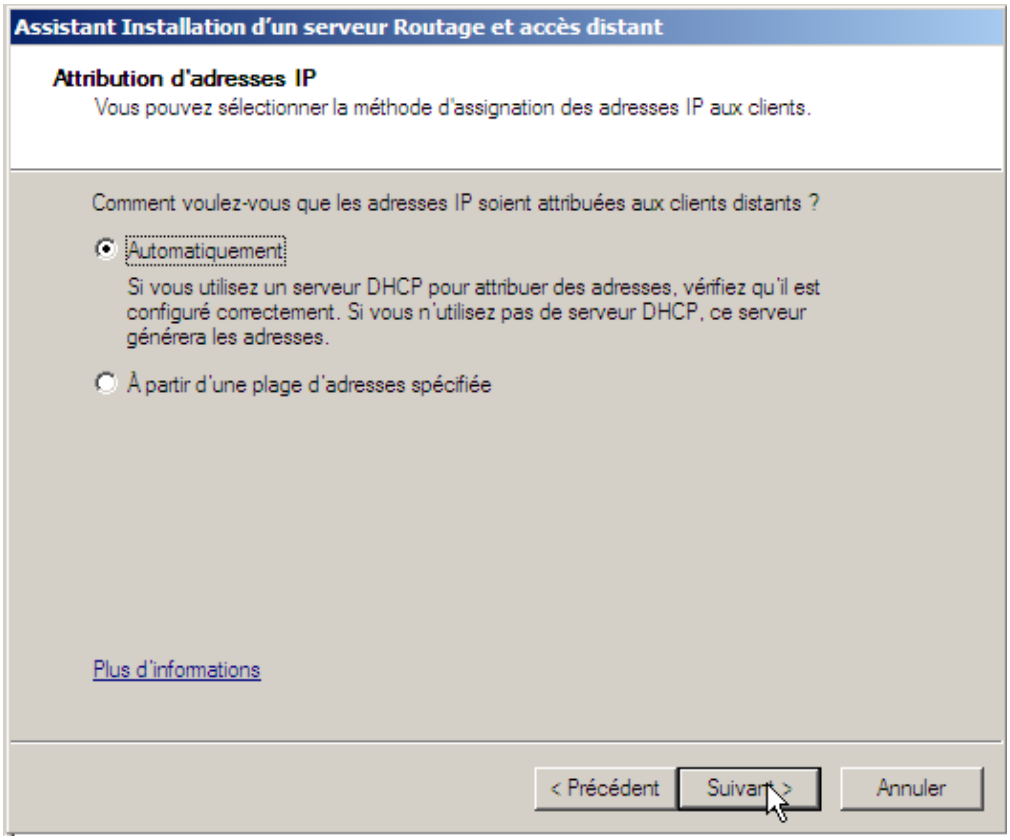
On choisit VPN puis cliquer sur Suivant



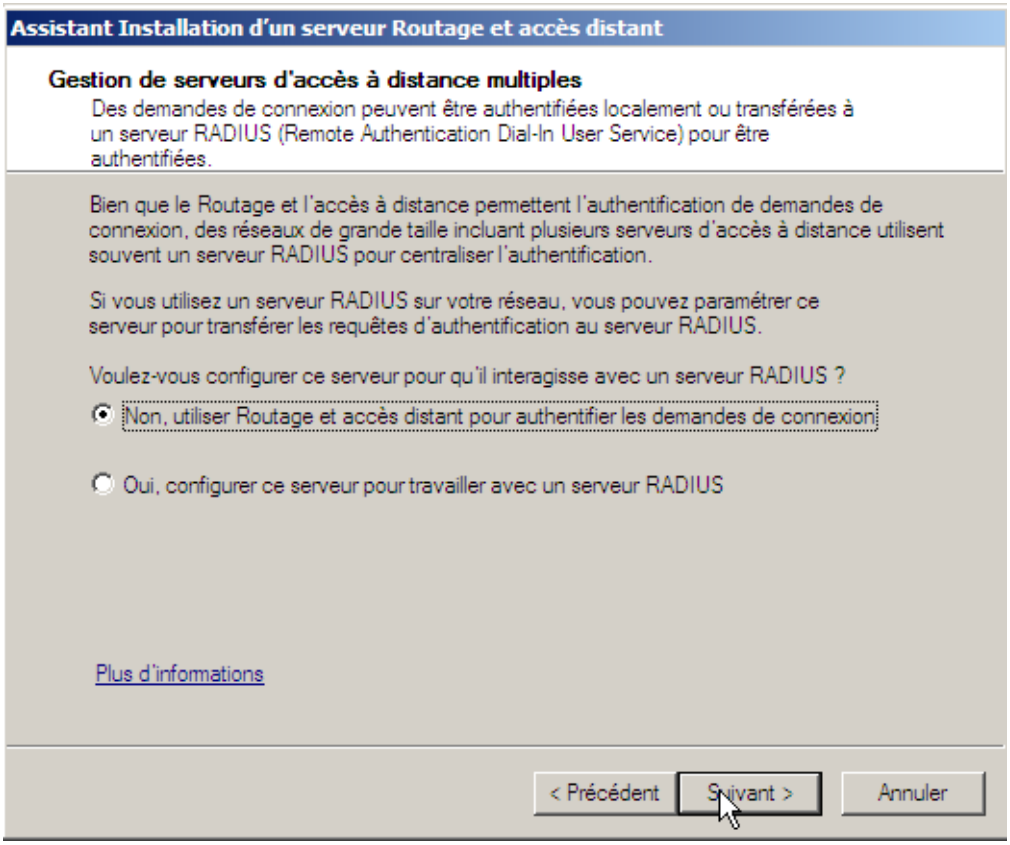
Sélectionnez l'interface qui appartient l'adresse local.



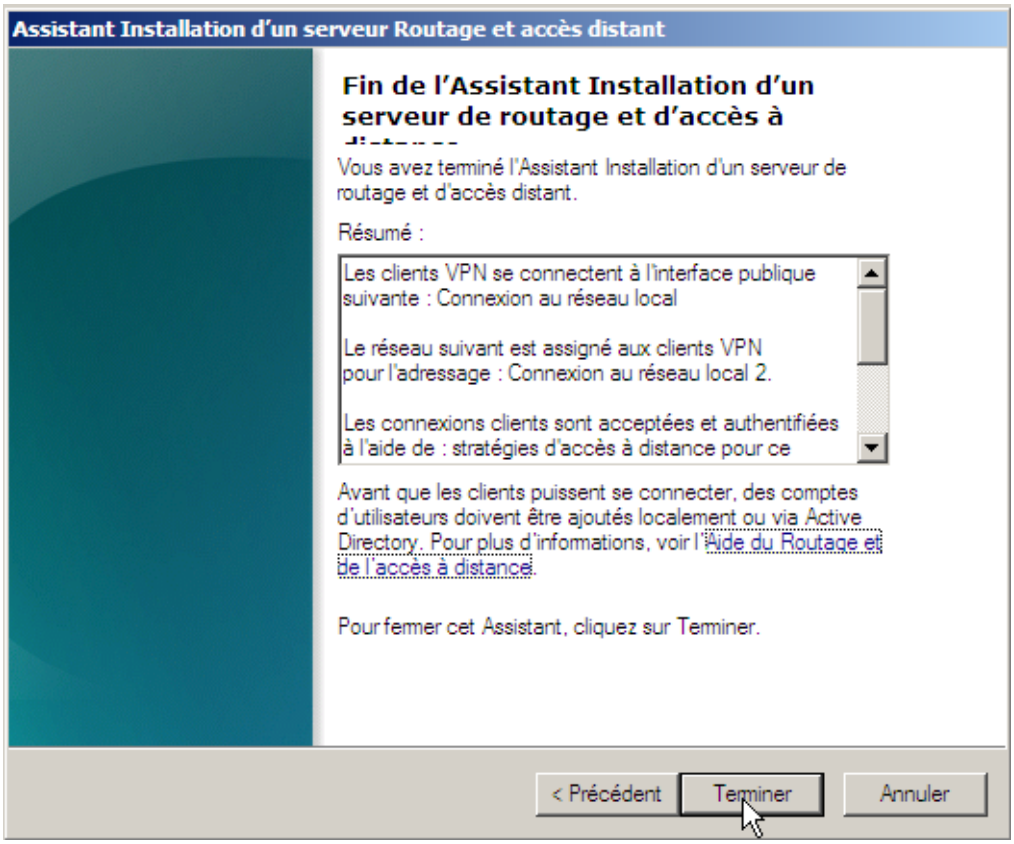
Attribution d'adresse IP est automatique parce que il a un serveur DHCP.



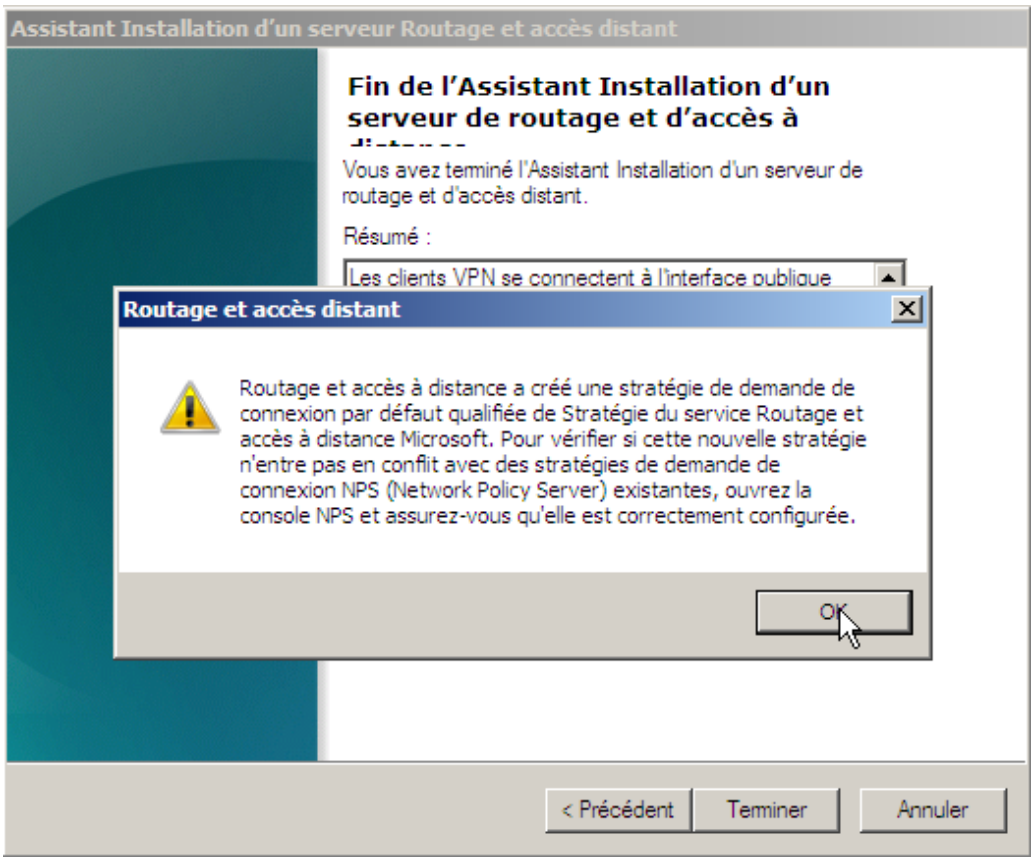
Utiliser routage et accès distant pour authentifier les demandes de connexion



Cliquer sur terminer pour terminer l'installation.



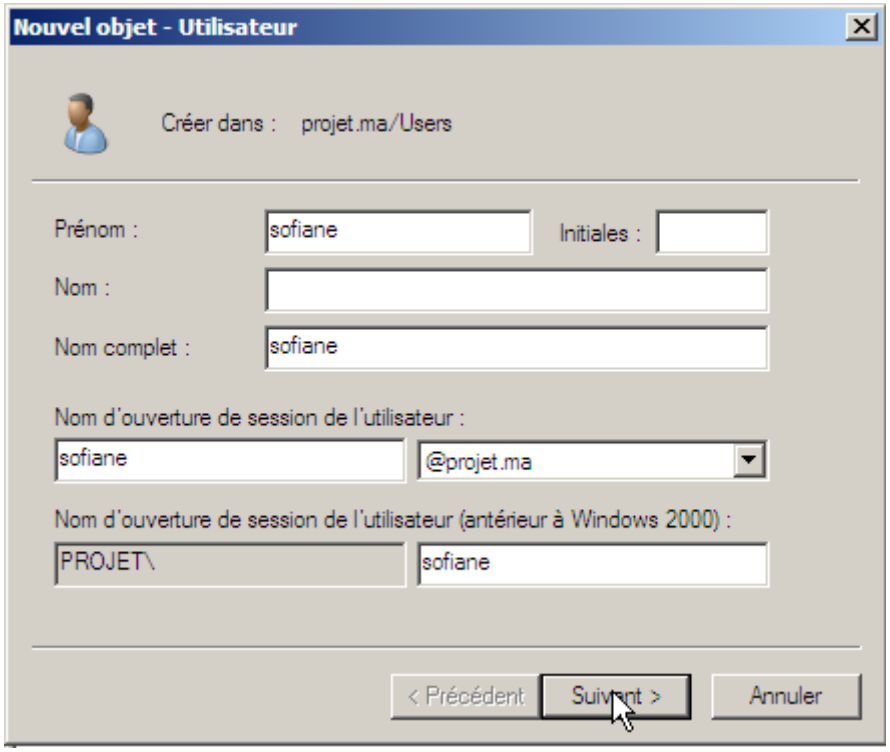
Cette fenêtre affiche que le routage et accès à distance a créé une stratégie de demande de connexion par défaut qualifiée de stratégie du service routage et accès à distance.



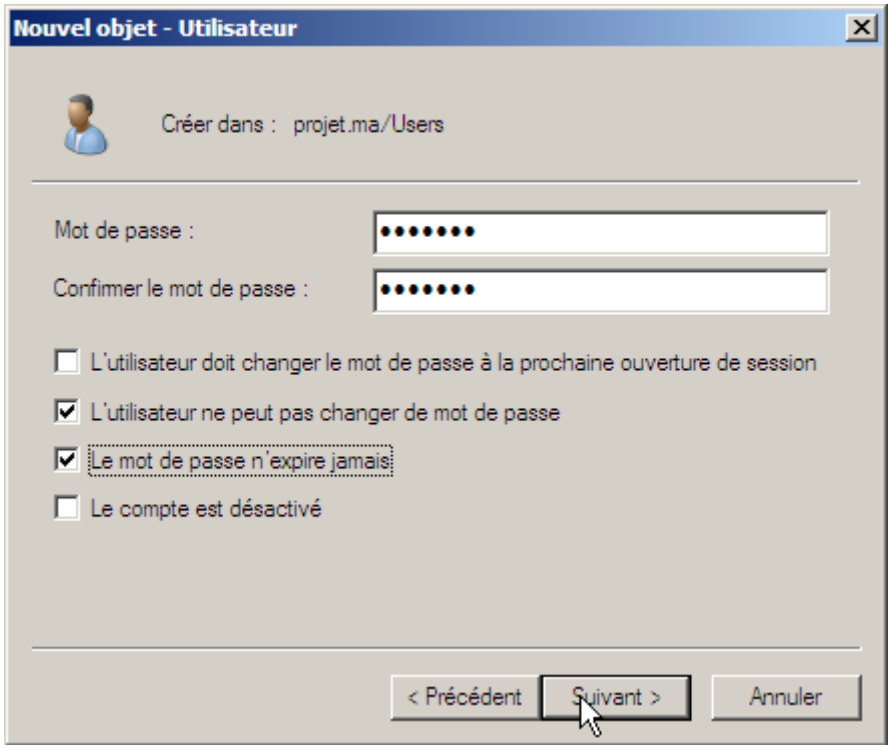
Création des utilisateurs et des groupes :

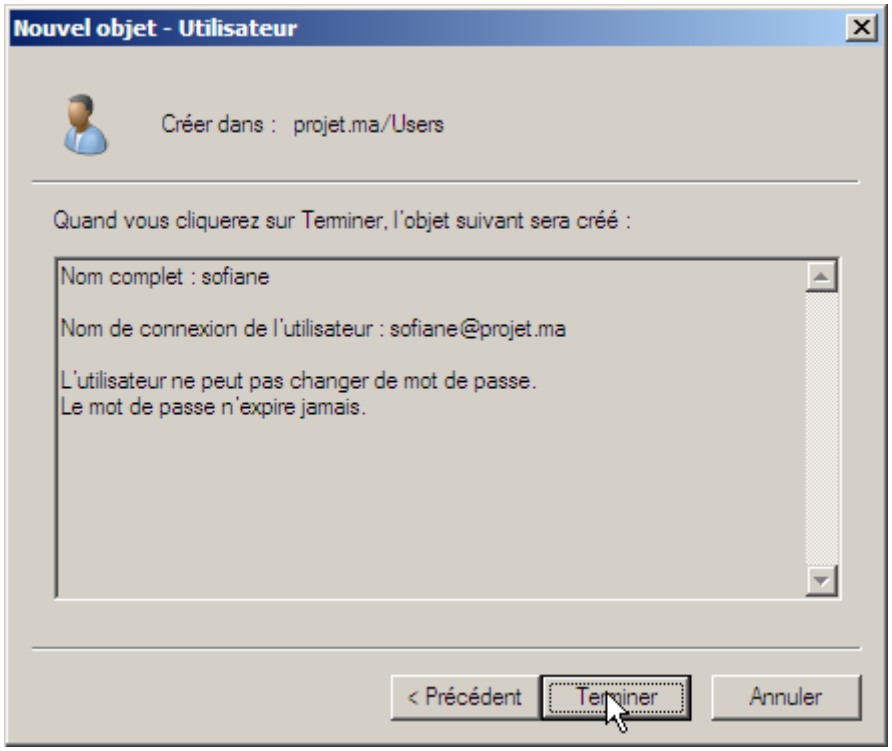
Dans le service de domaine Active Directory on ajoute l'utilisateur par clic droit sur user et on fait nouveau utilisateur.

Par exemple premier utilisateur : Sofiane

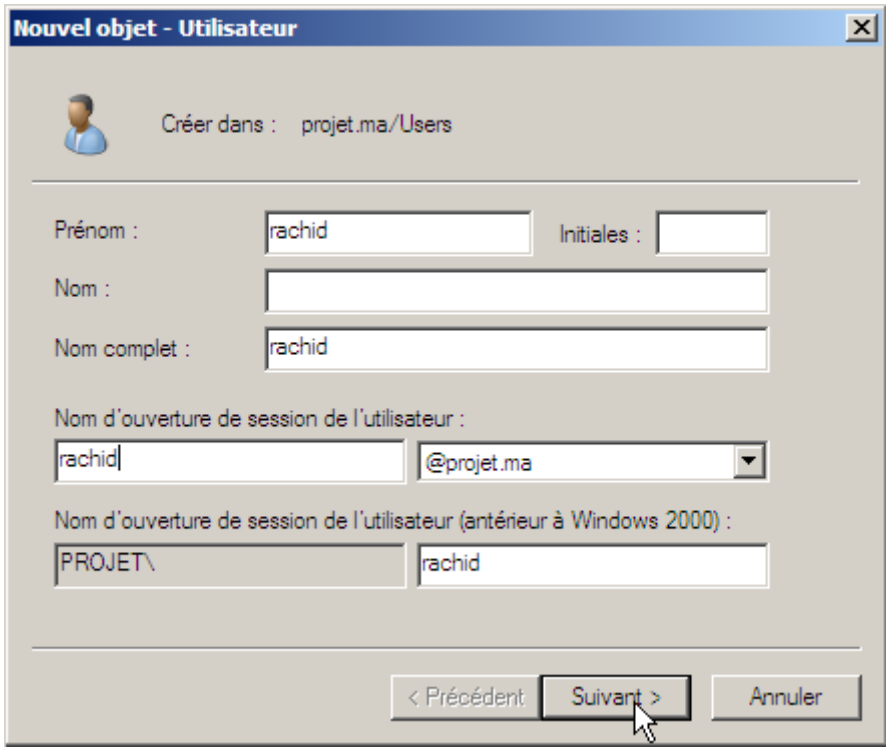


Puis en fait un mot de passe pour l'utilisateur.

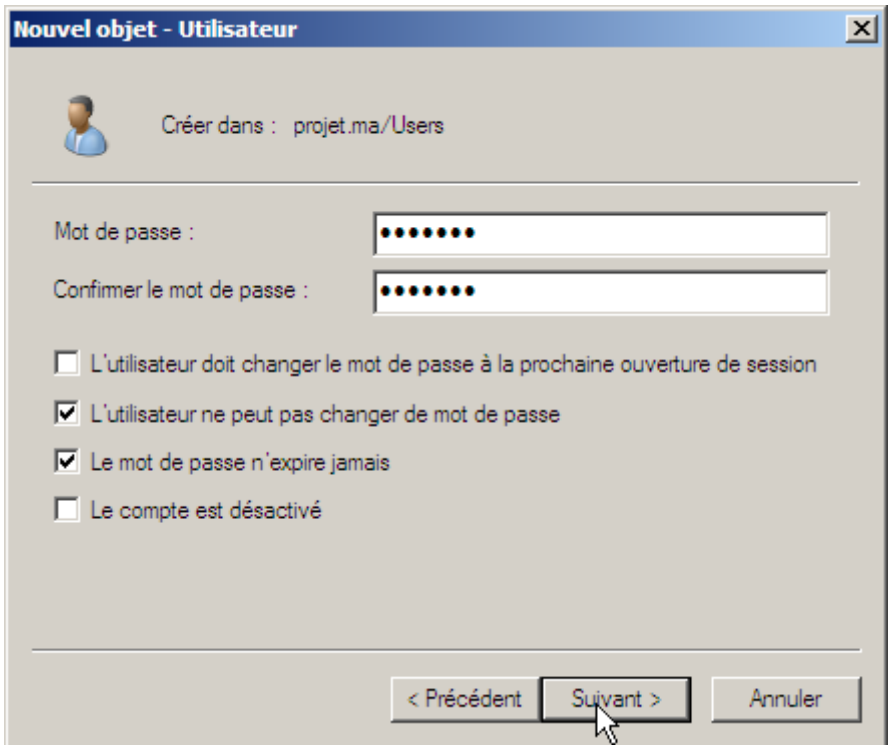


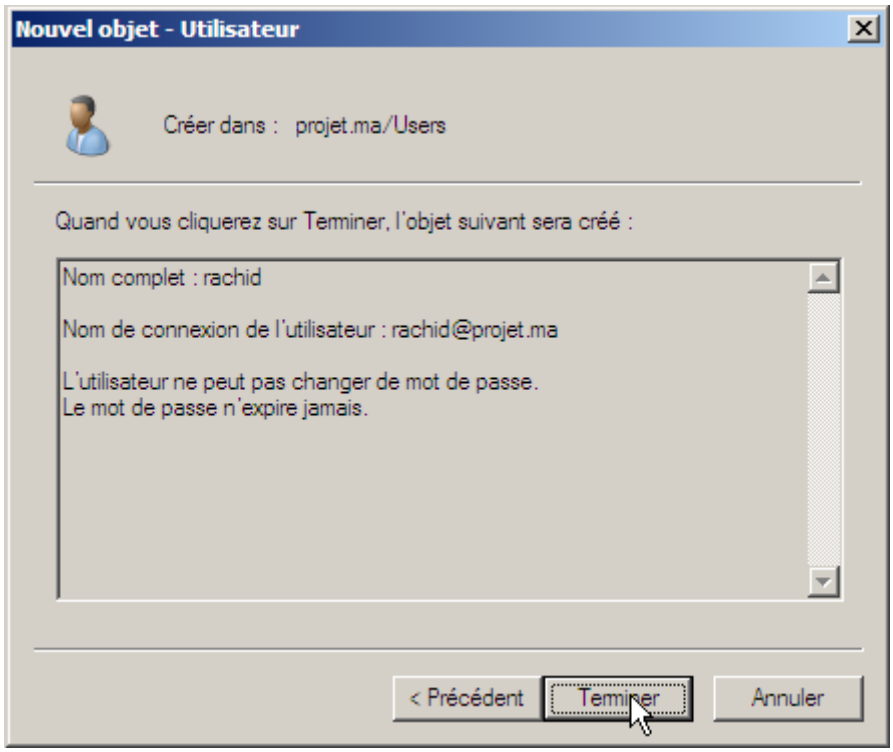


Deuxième utilisateur : Rachid



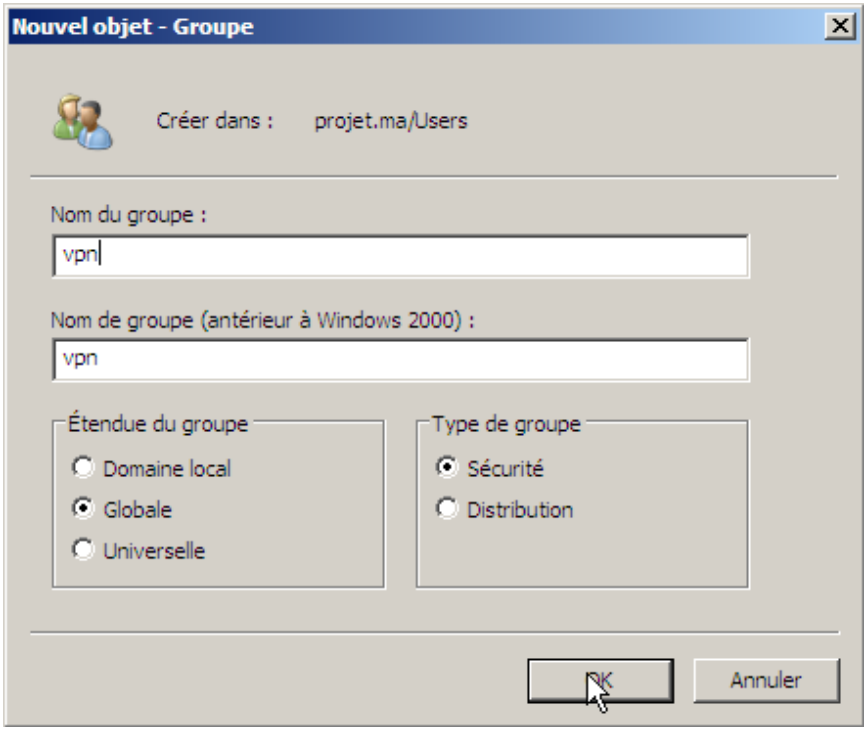
Puis en fait un mot de passe pour l'utilisateur.



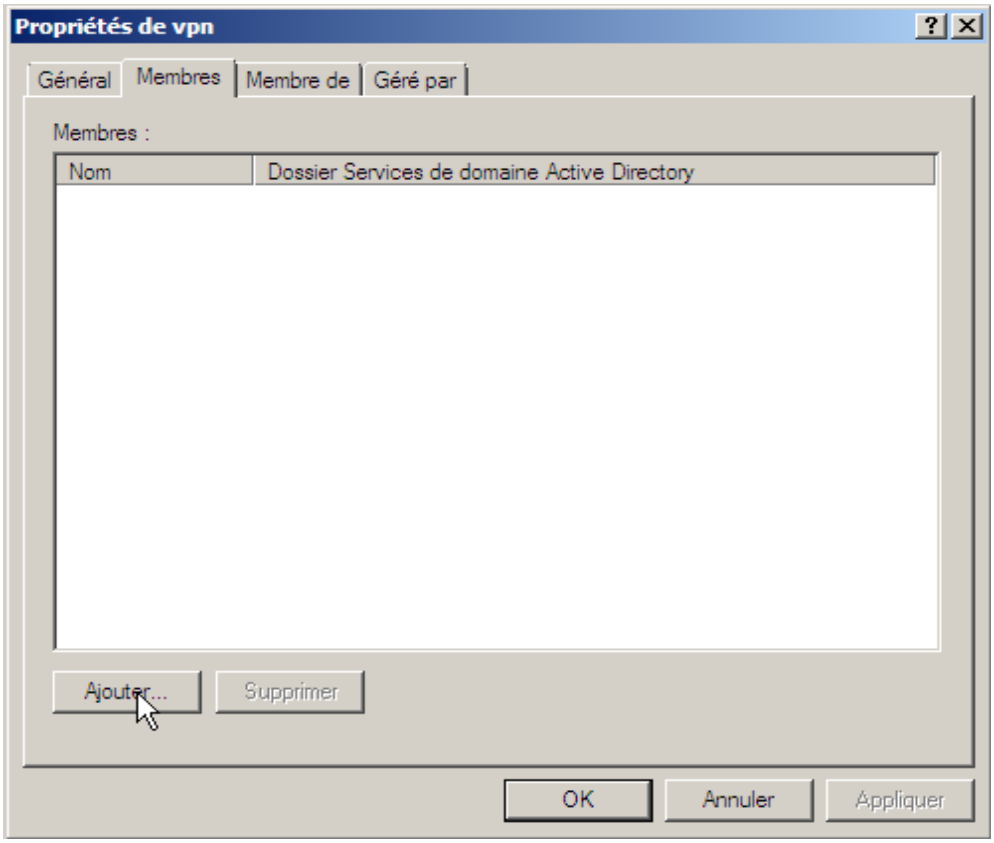


Dans le service de domaine Active Directory on ajoute l'utilisateur par clic droit sur user et on fait nouveau groupe.

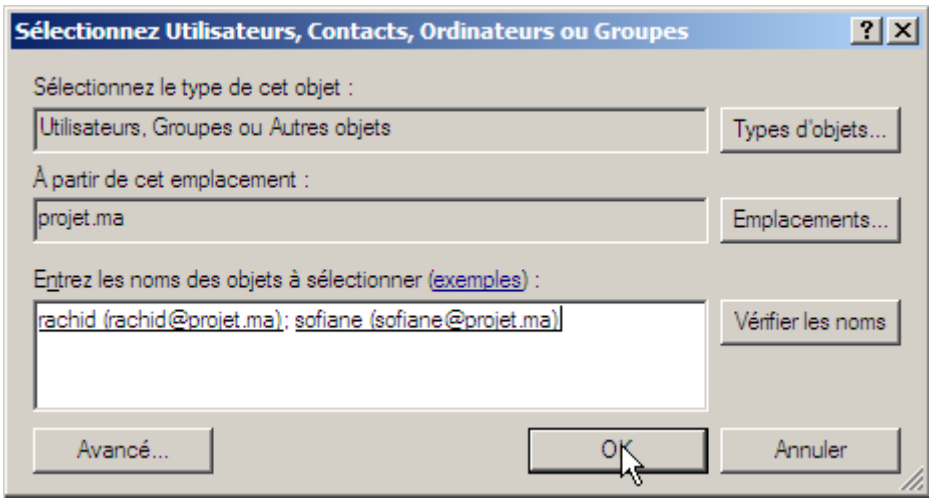
On crée un groupe globale de sécurité on donne par exemple le nom VPN.

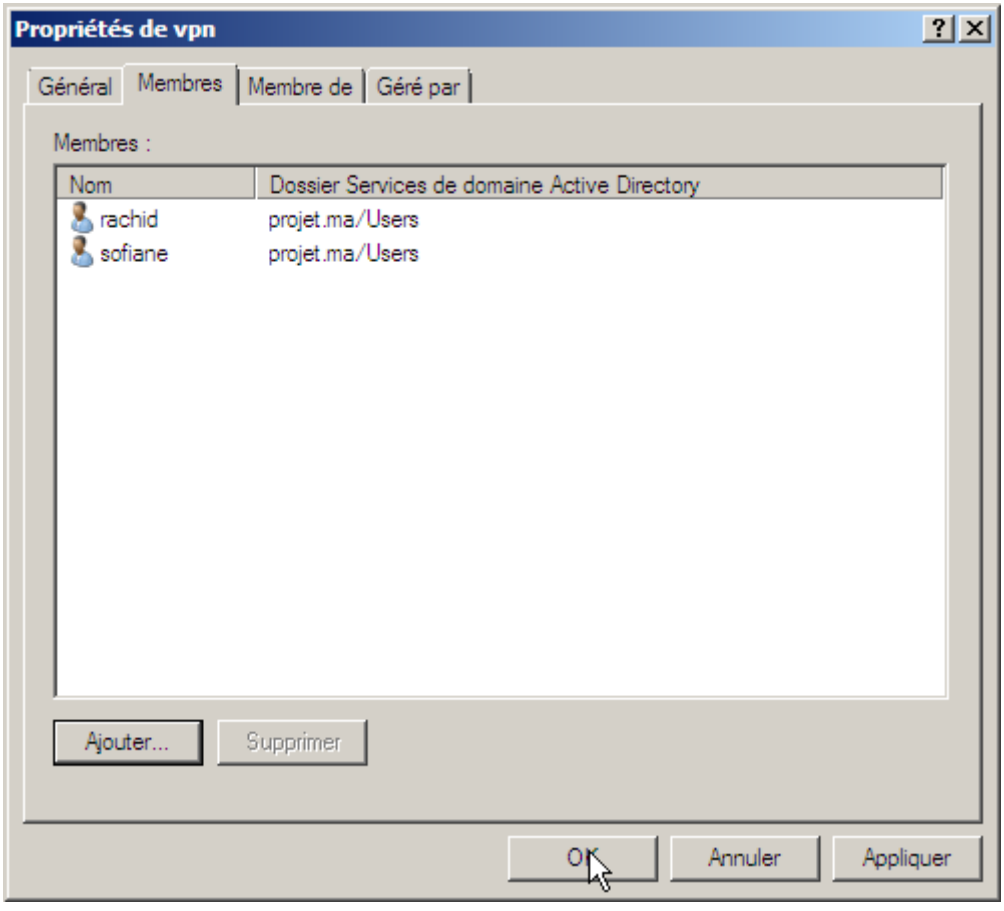


On clique sur ajouter pour ajouter les utilisateurs qu'on a créé.



On écrit les noms des utilisateurs puis on clique sur ok.

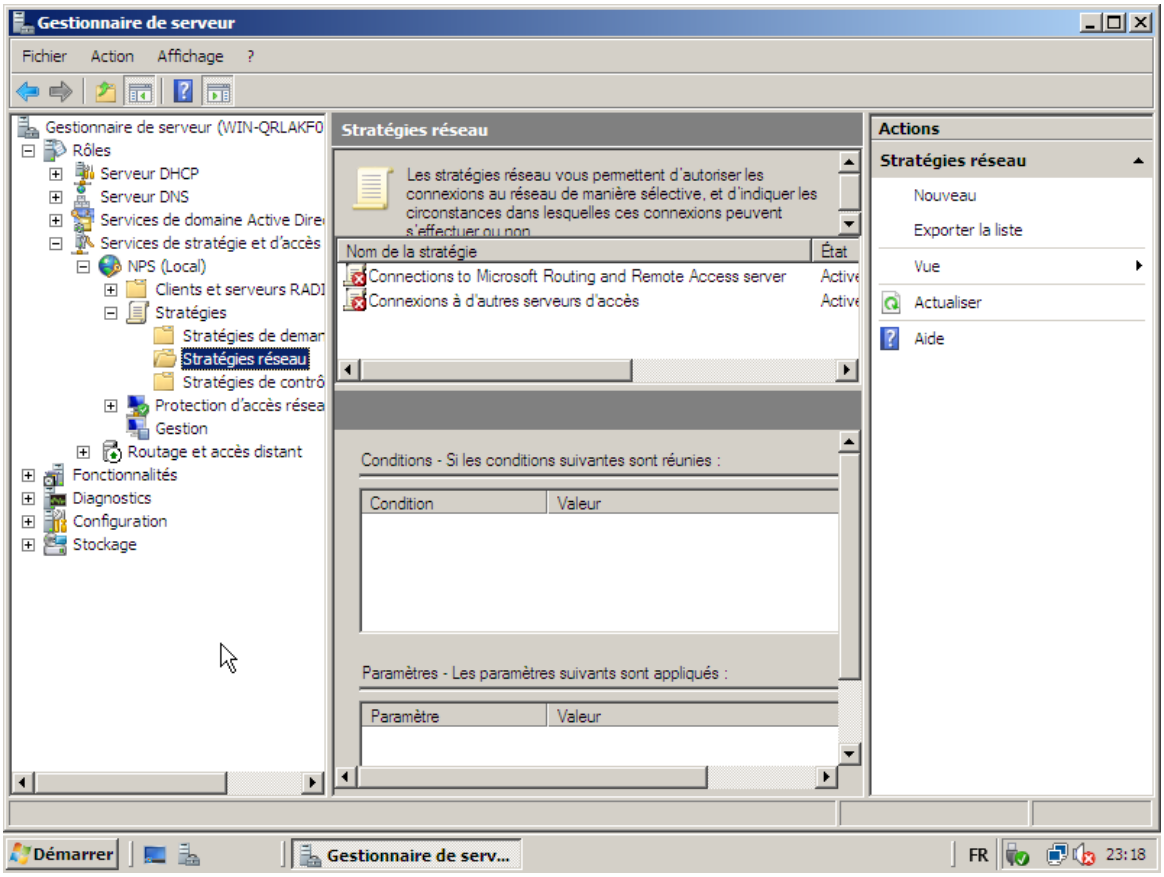




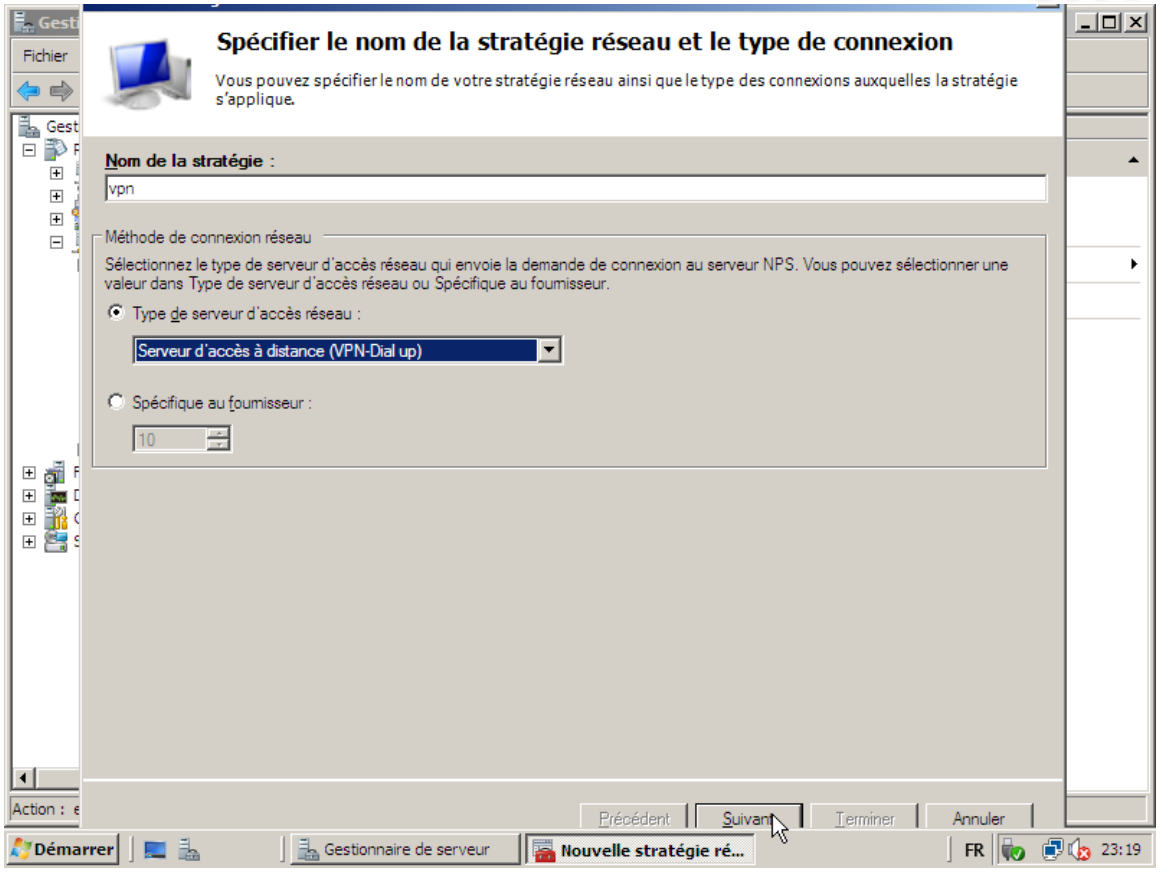
NPS (stratégies réseau) :

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

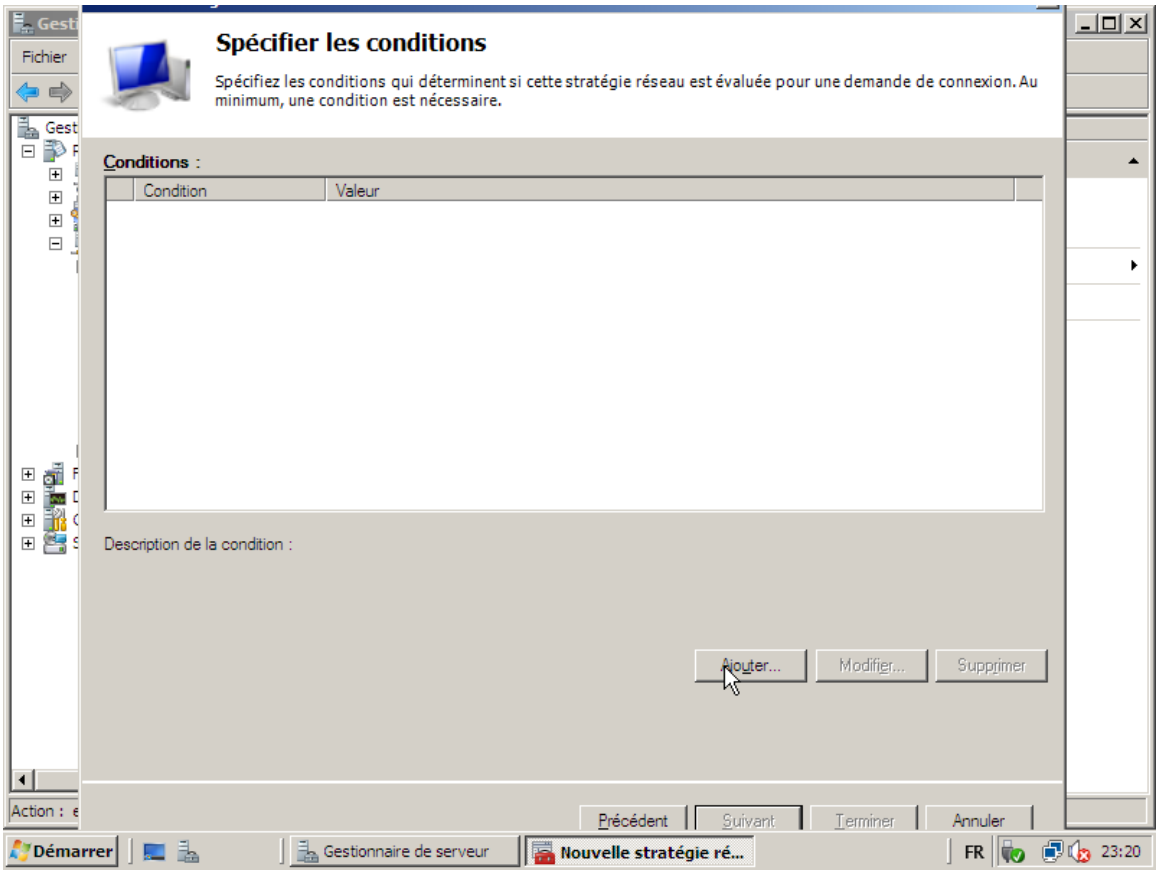
Dans NPS on ouvre le menue Stratégie puis on clic droit sur Stratégie réseau puis nouveau stratégie réseau.



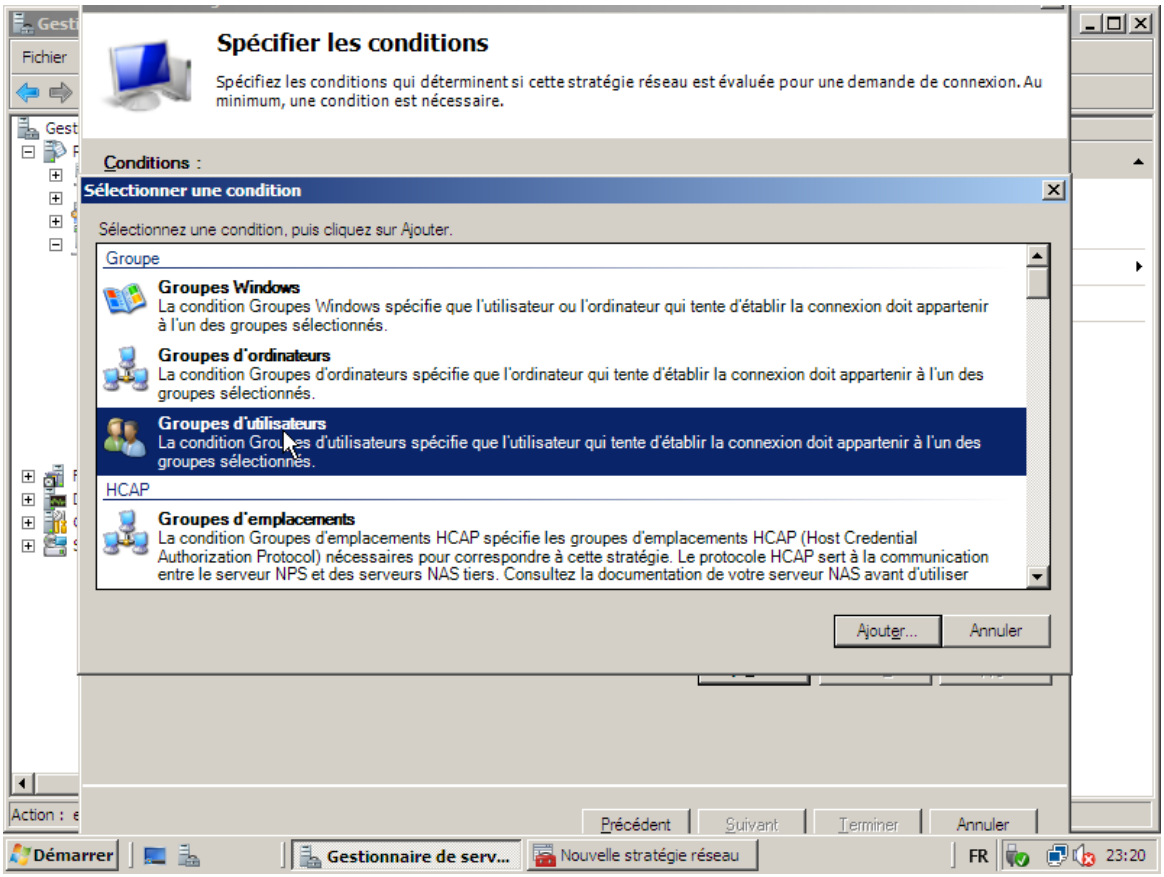
On donne un nom pour la stratégie et dans le type de serveur d'accès réseau on choisit Serveur d'accès à distance (VPN-Dial up) puis Suivant.



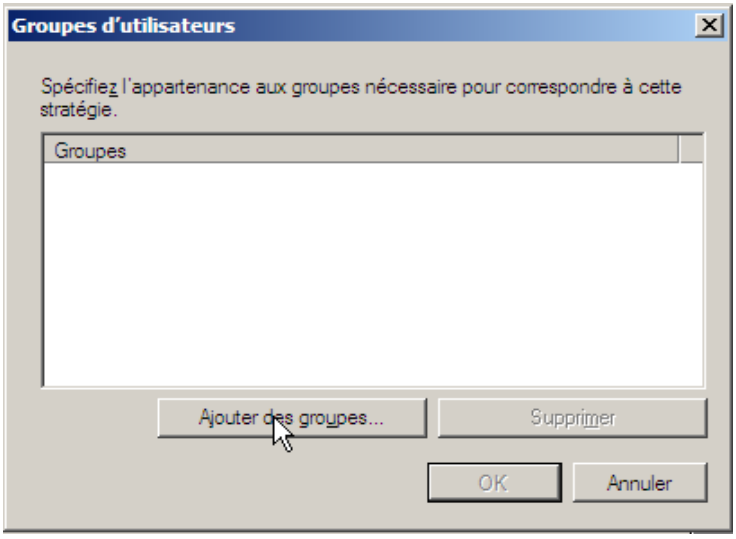
Pour spécifier les conditions de la stratégie on clique sur ajouter.



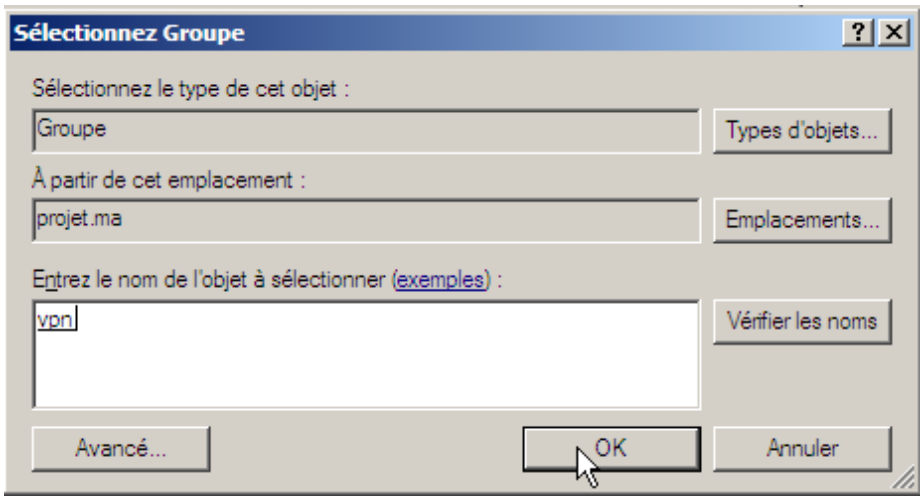
On sélectionne la condition groupe d'utilisateurs puis clique sur ajouter.

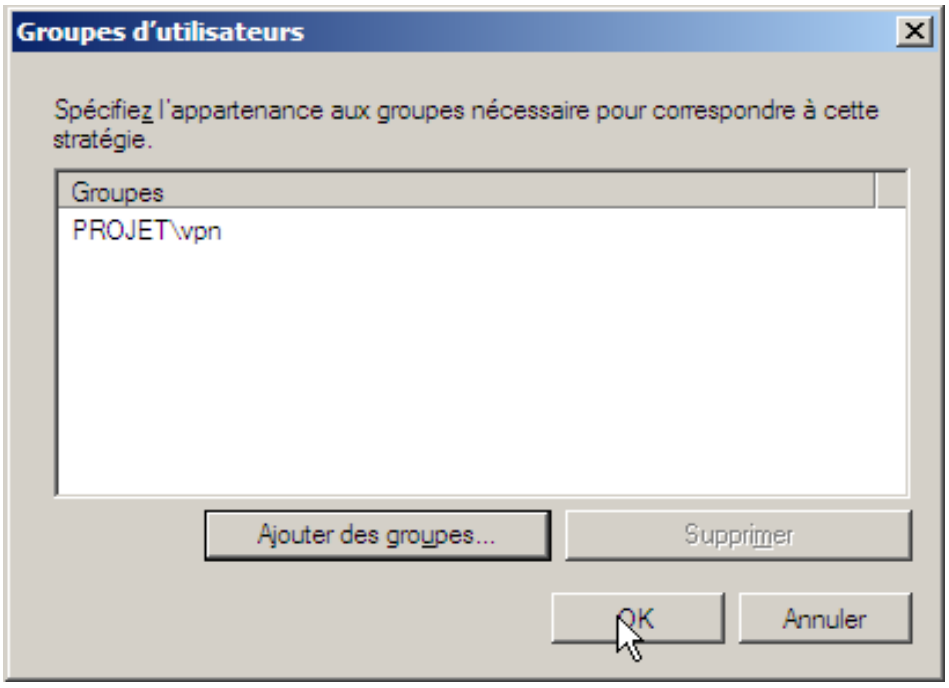


Cliquer sur ajouter des groupes pour ajouter le groupe dans la condition.

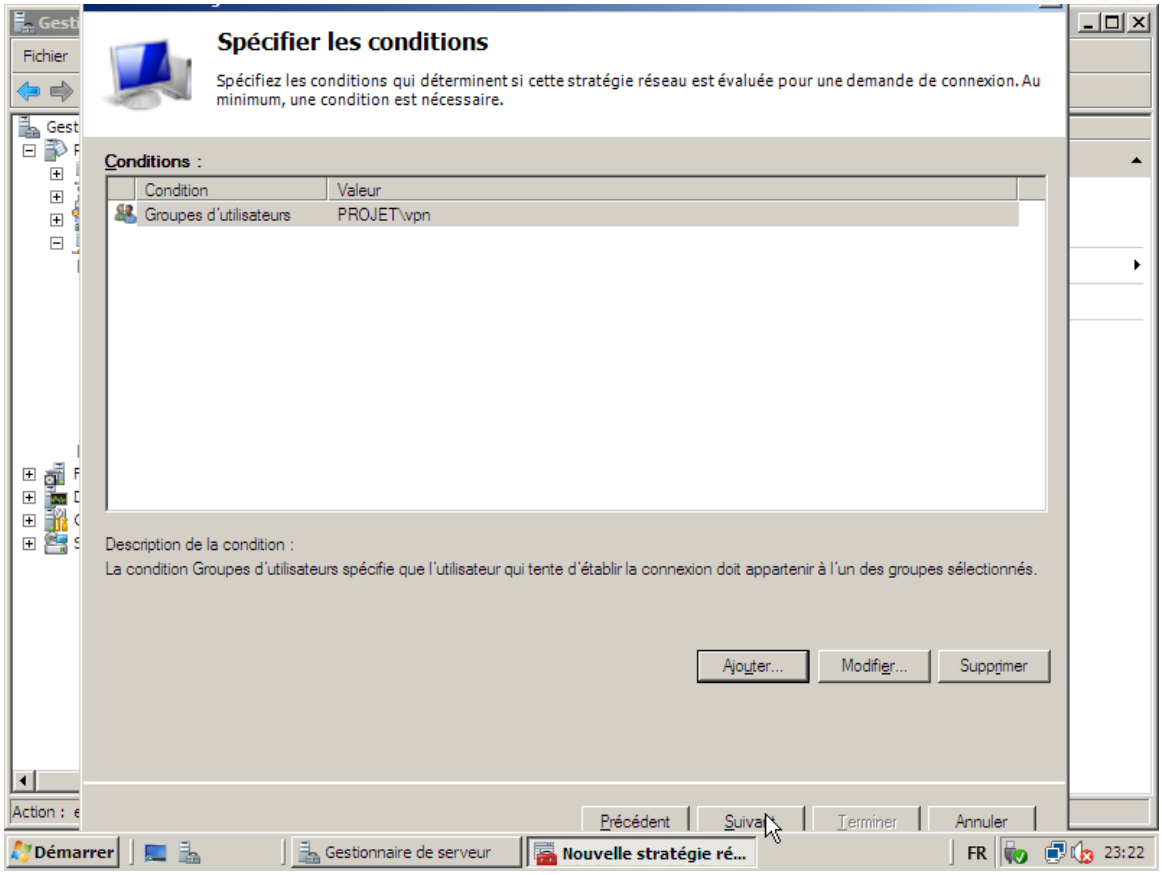


On écrit le nom de groupe qu'on a crèè.

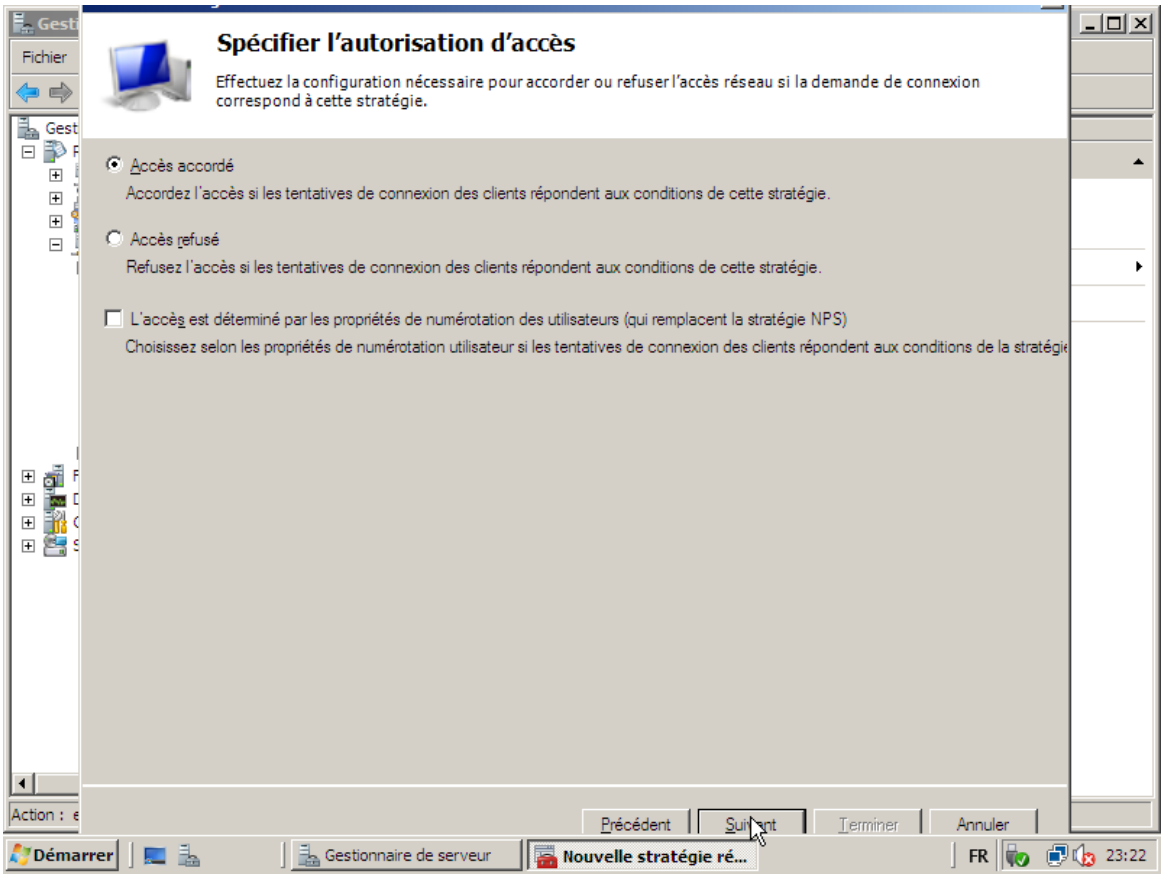




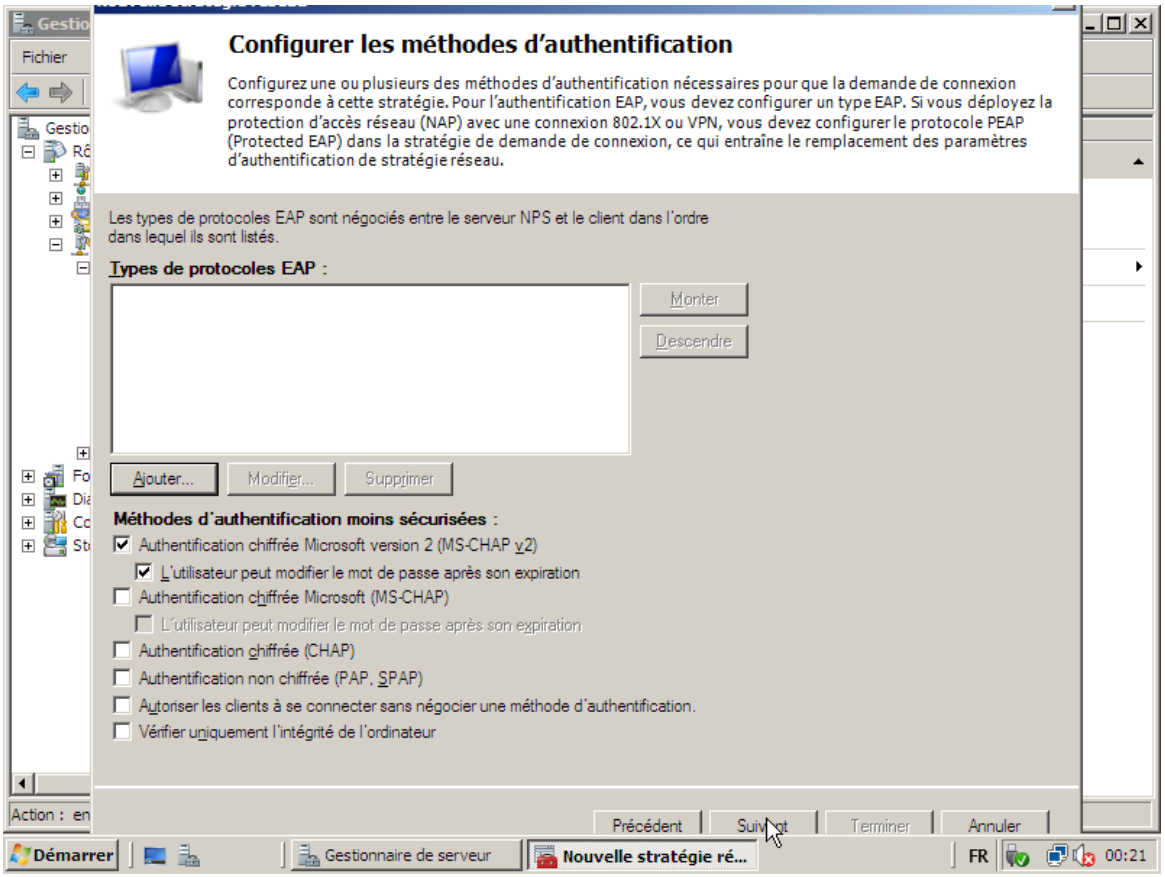
Puis on clique sur suivant

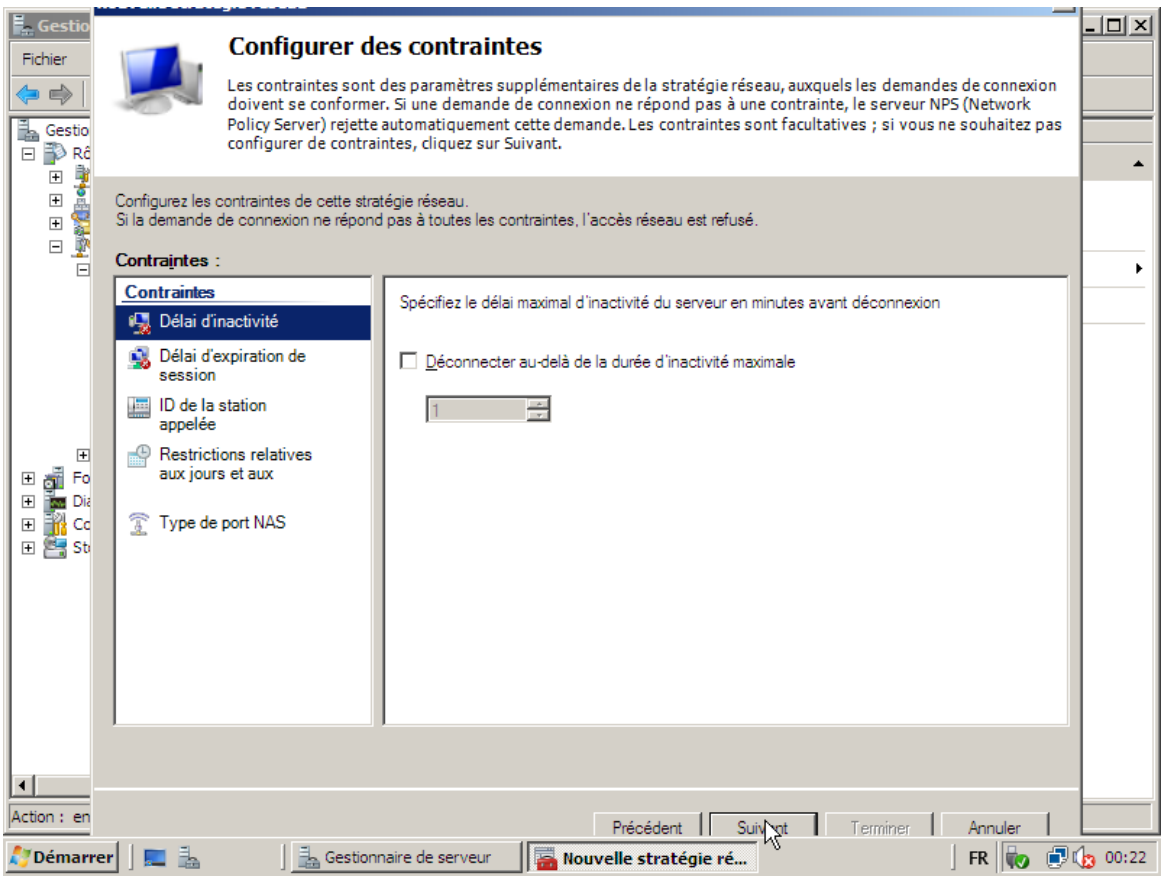


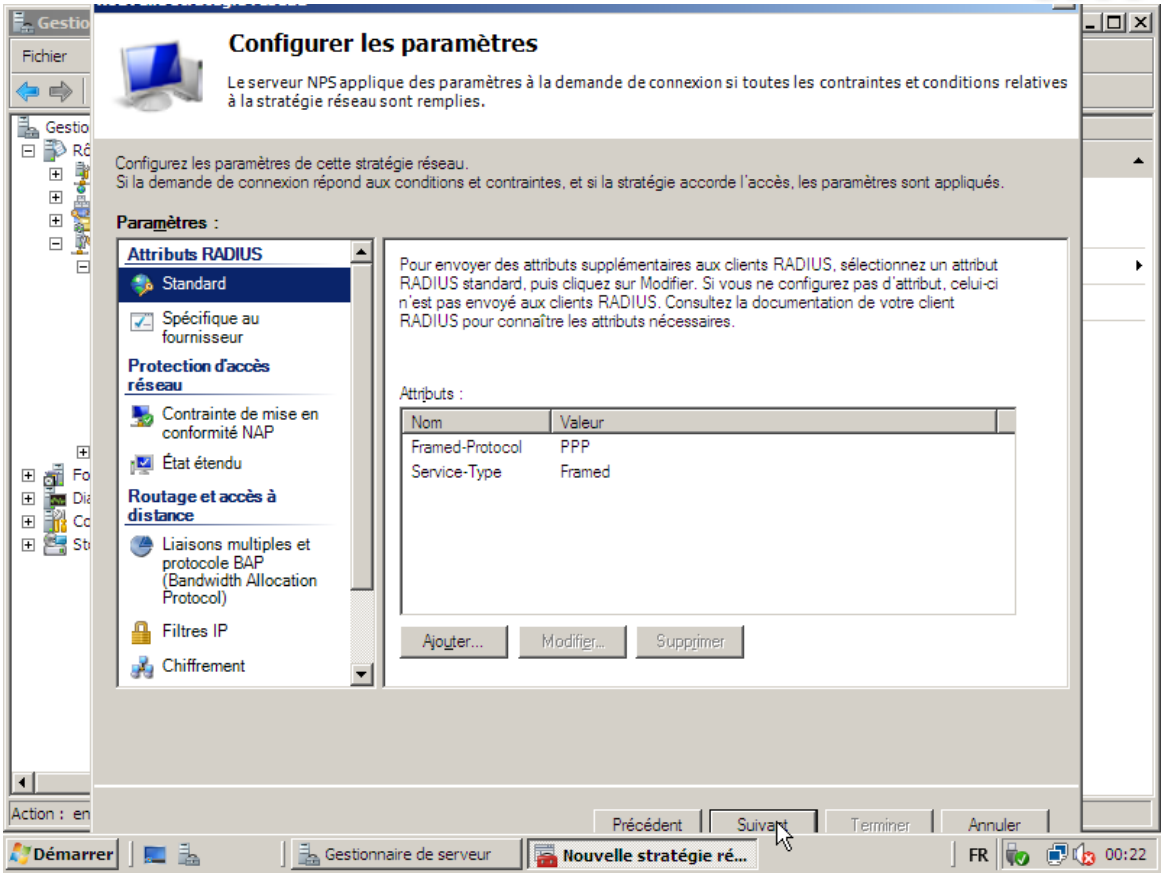
Autorisation d'accès aux réseau est accordé



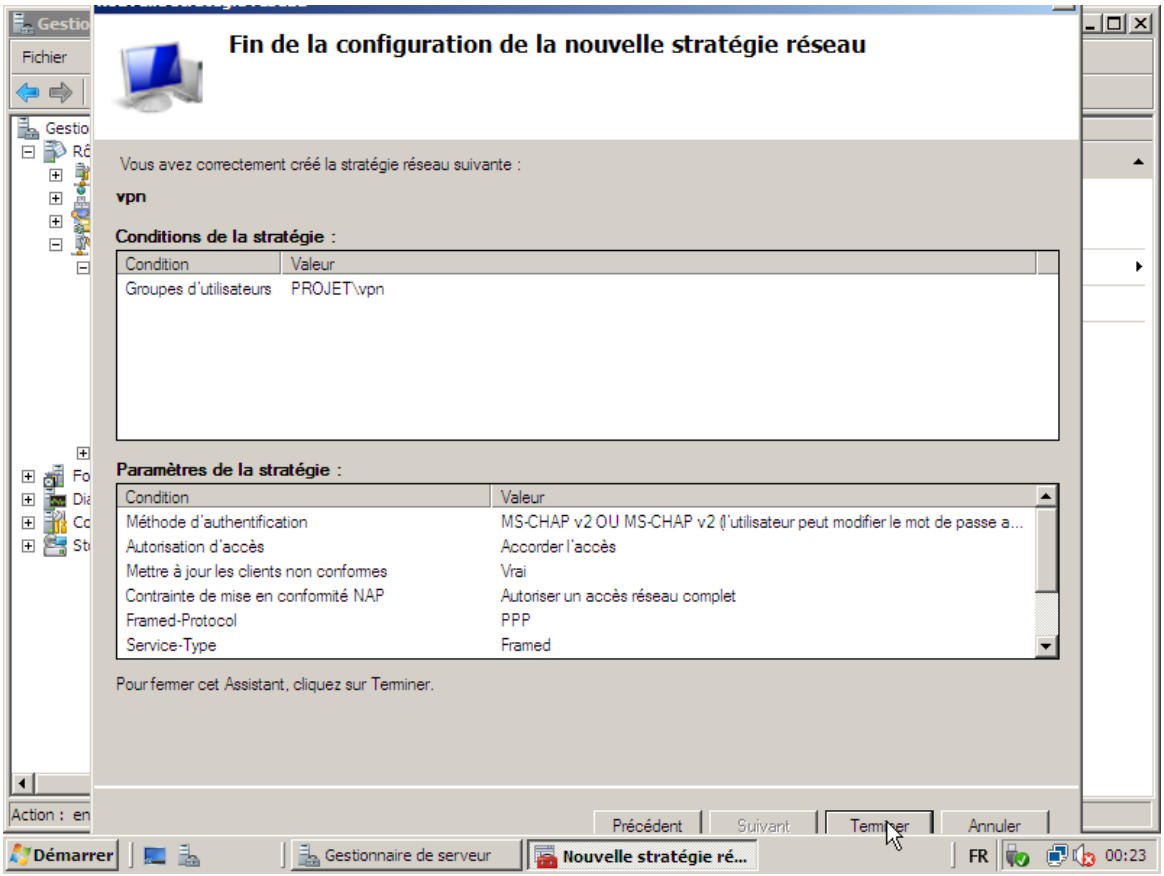
On choisi la methode d'authentification moins sécurisée MS-CHAP v2







A la fin de la configuration de la nouvelle stratégie réseau en clique sur terminer



Installation du client :

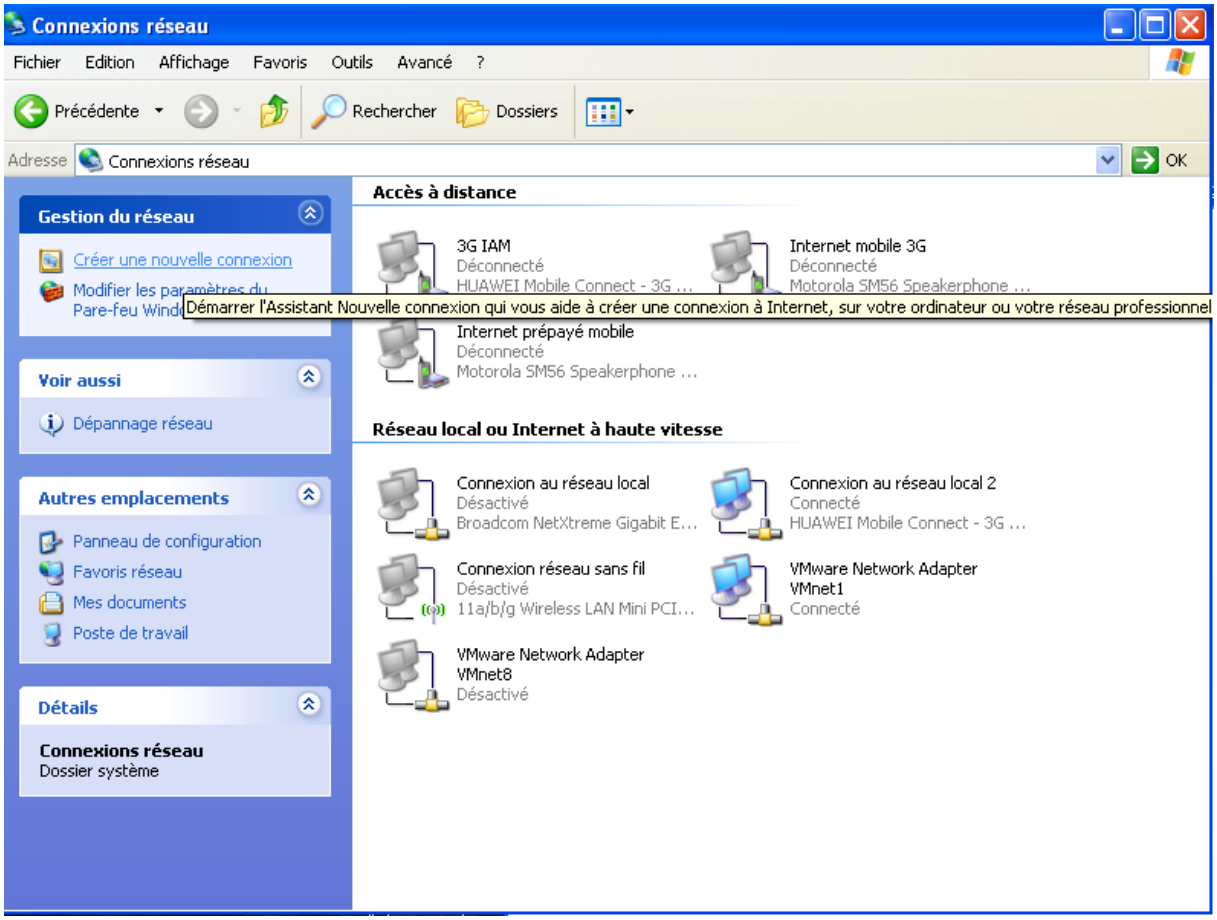
Client est un ordinateur Windows XP courante avec SP3 qui fonctionne comme un client d'accès distant pour le domaine projet.ma

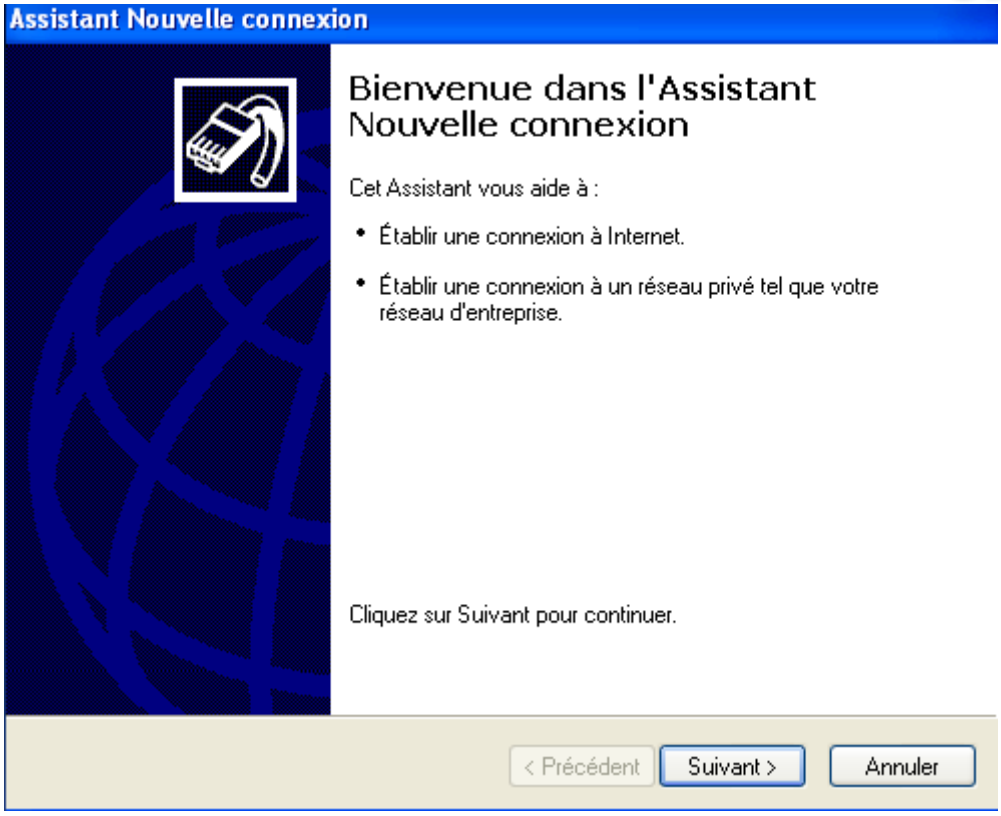
La configuration client consiste dans les étapes suivantes :

- Installez le système d'exploitation.
- Configuration TCP/IP.
- Création de la connexion VPN.

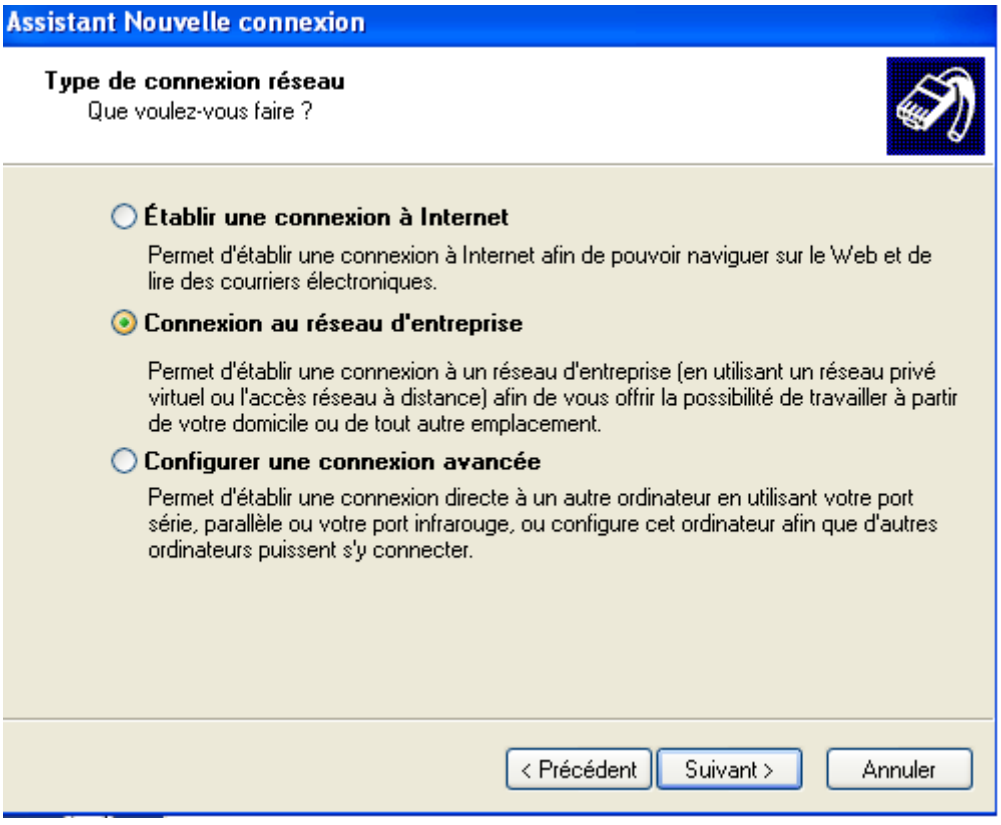
Installation de la connexion VPN cliente :

Dans favoris réseau en clic droit propriété puis on clique sur Créer une nouvelle connexion.

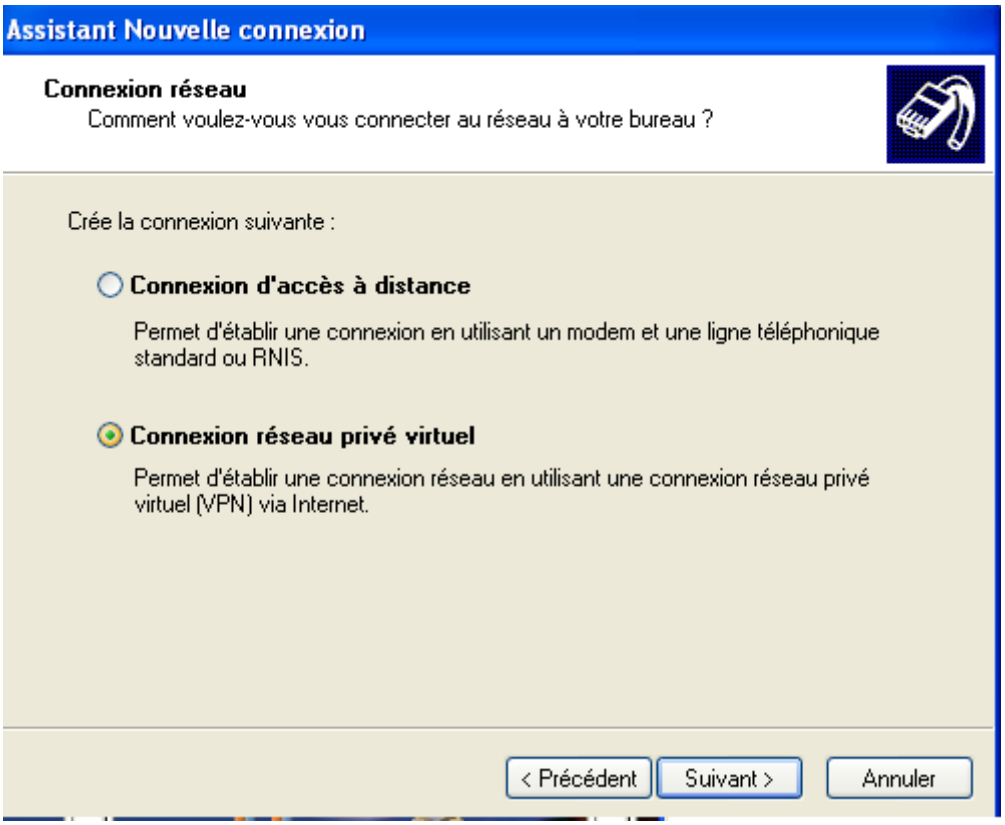




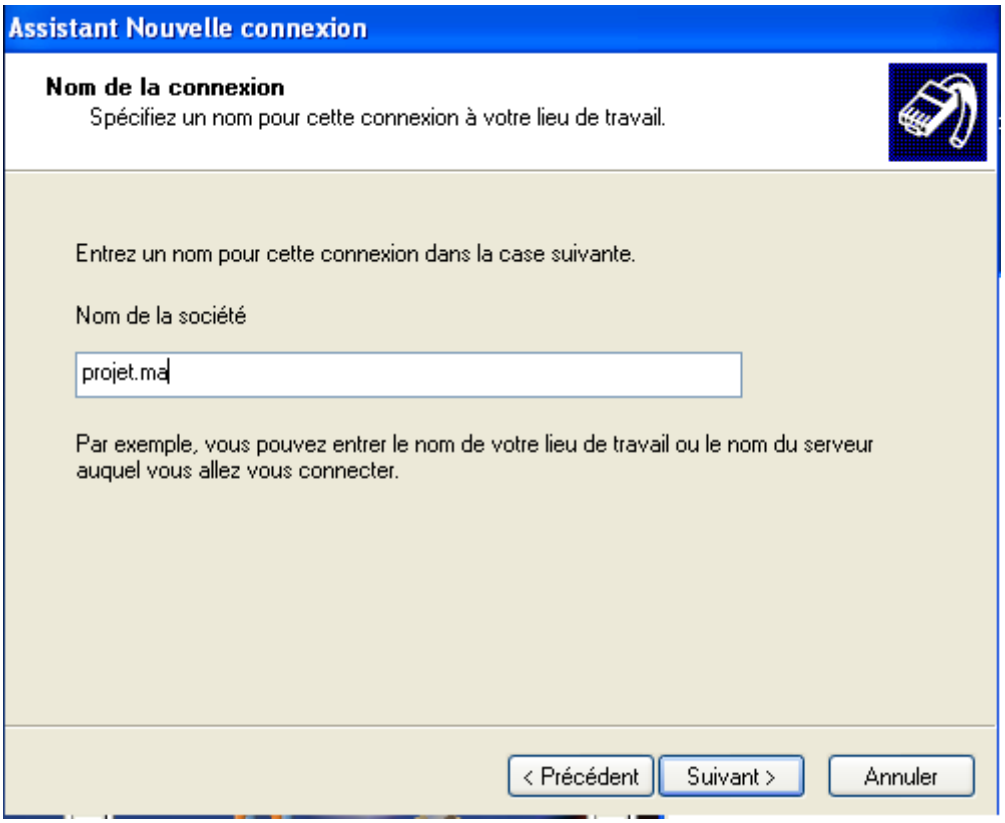
Dans le type connexion réseau on choisit connexion au réseau d'entreprise.



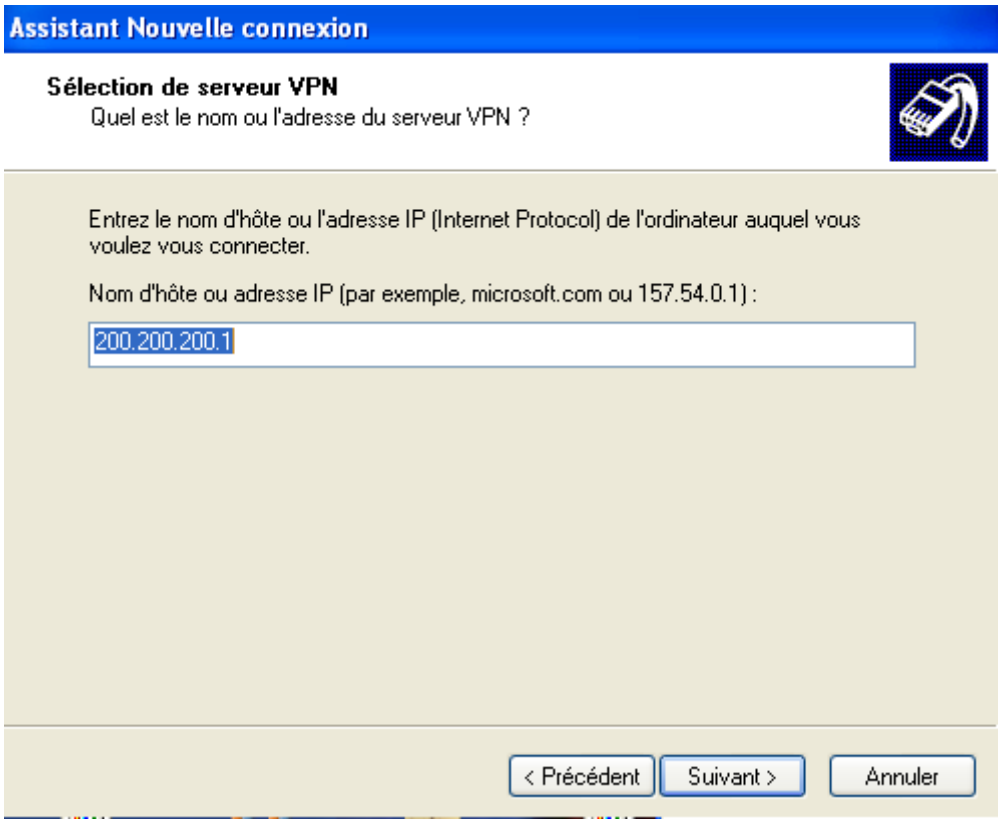
Puis on crée une connexion réseau privé virtuel.

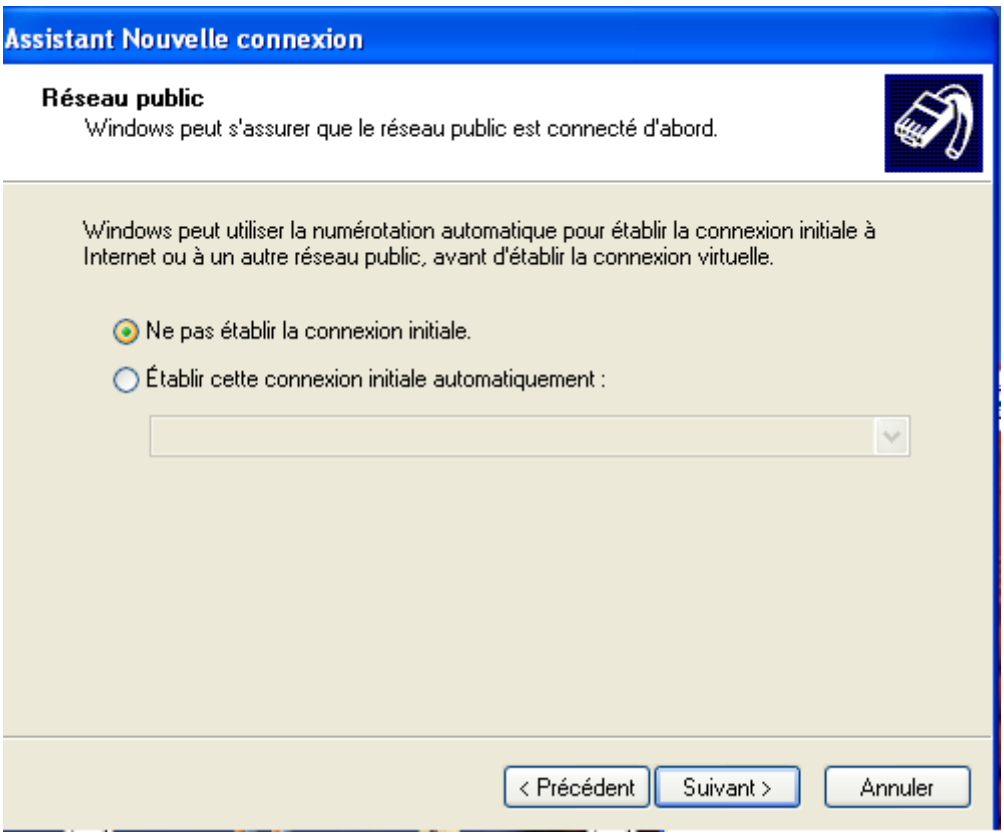


Puis on donne un nom pour cette connexion.

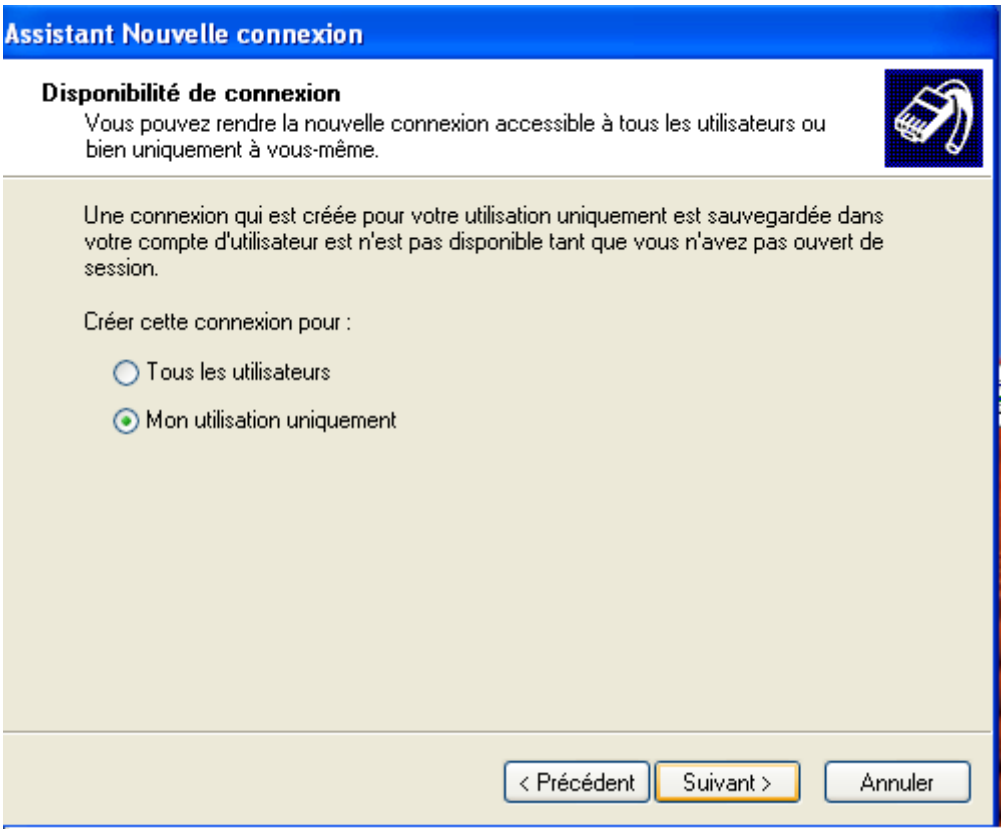


Puis on donne le nom du serveur ou lors adresse IP.

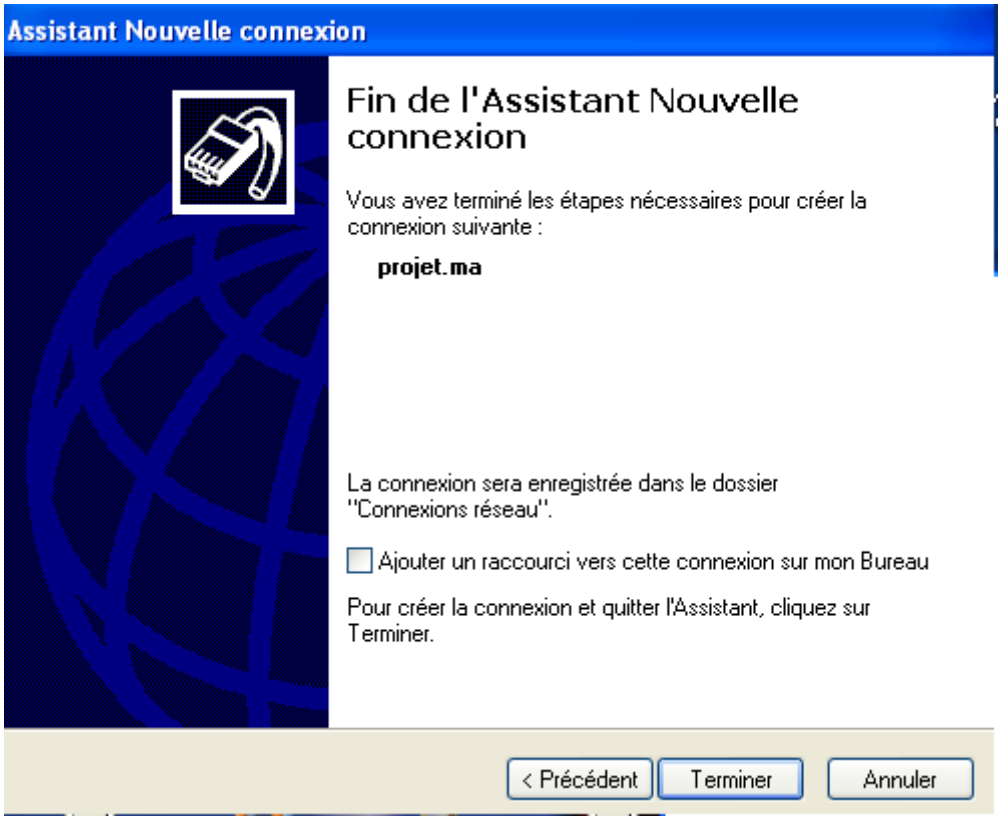




On créer cette connexion pour Mon utilisation uniquement.

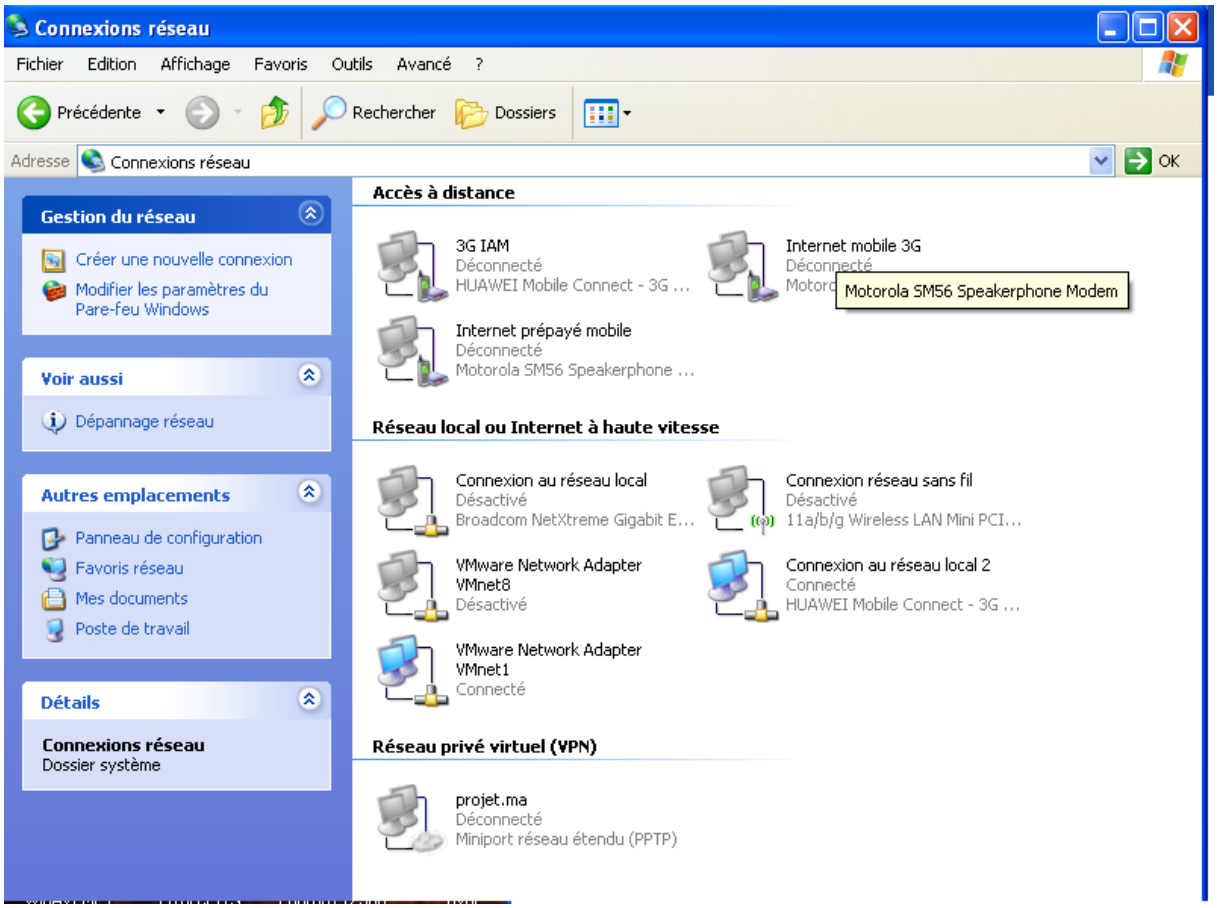


A la fin de l'assistant nouvelle connexion on clique sur terminer

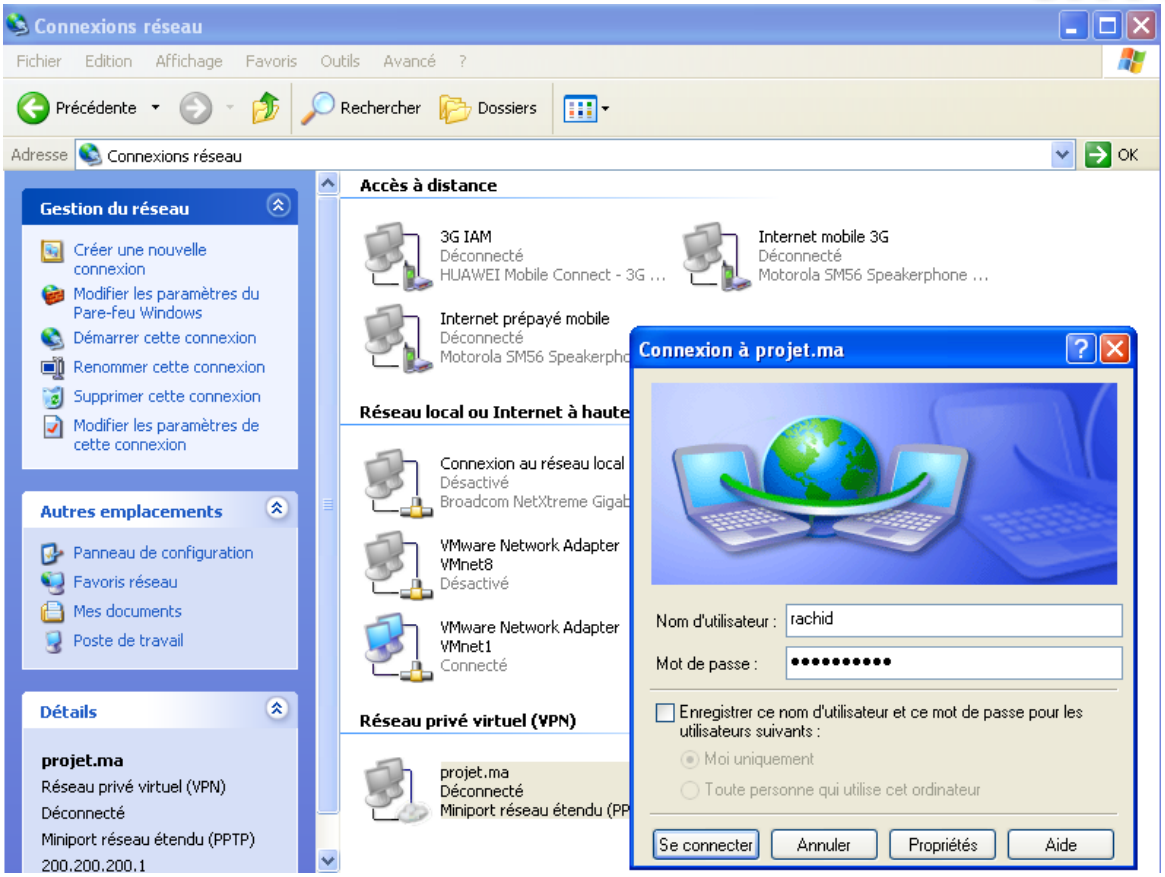


Phase de test du client

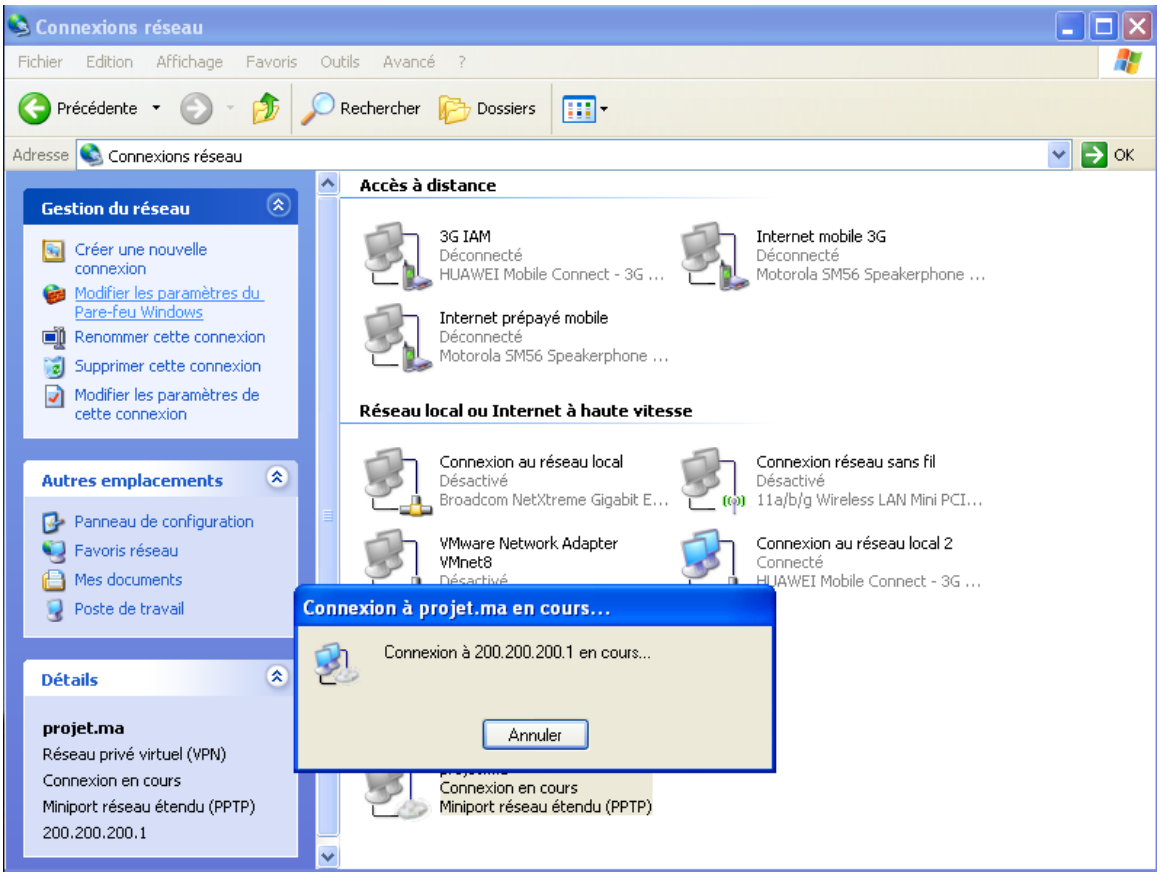
Pour connecter au connexion réseau privé virtuel qu'on a créé on fait double clic sur la connexion qu'on a créé.



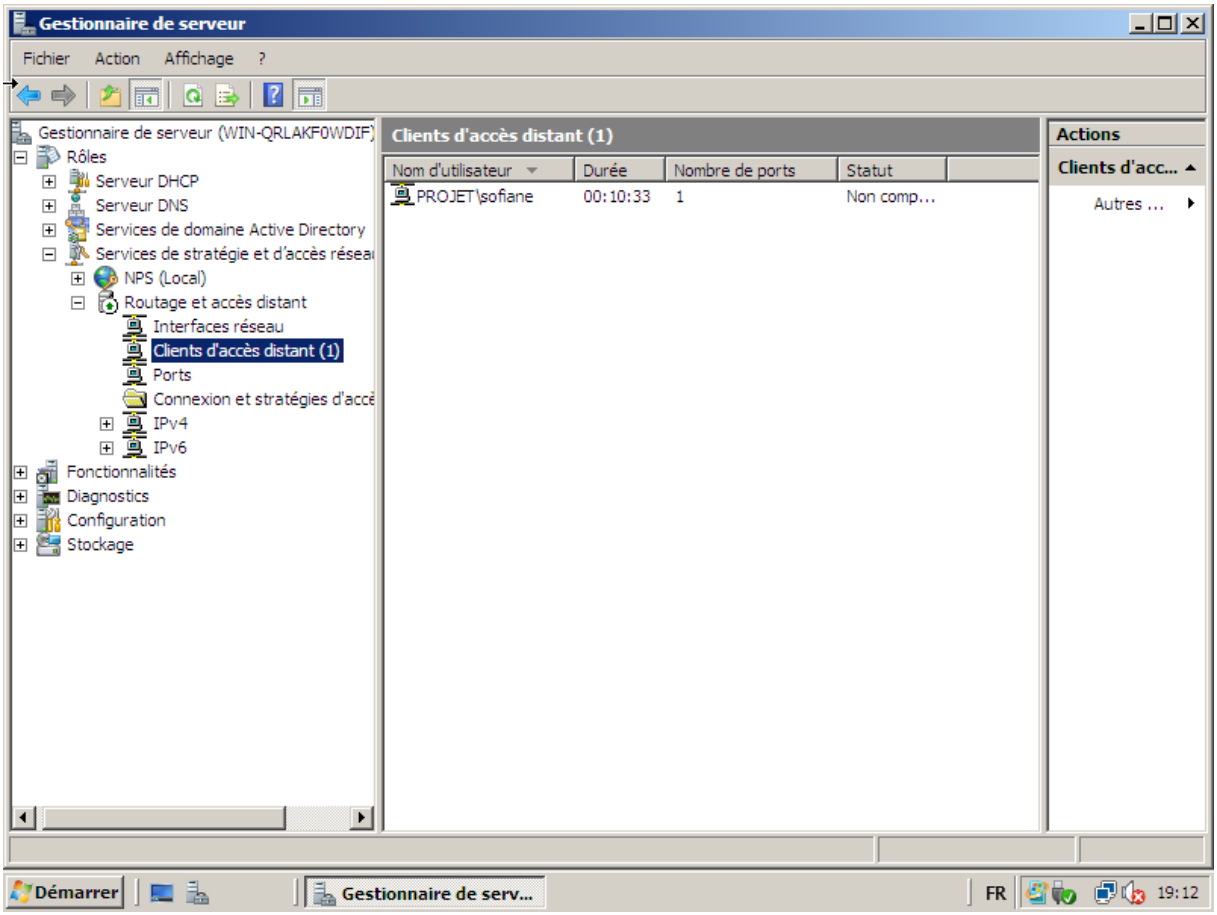
On donne le nom d'utilisateur et le mot de passe d'un utilisateur qu'on a créé puis on se connecte.



Puis il se connecte après un vérification de la stratégie et le groupe et l'utilisateur.



Dans le menu clients d'accès distant qui se trouve dans Routage et accès distant on voit l'utilisateur qui a accès distant au réseau de l'entreprise et on peut voir la durée de la connexion et le nombre de ports et le statut.



Conclusion :

A travers ce dossier, nous avons vu un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IP Sec. Nous avions en effet pour objectif de vous donner les concepts qui tournent autour de cette solution et de vous montrer un exemple de déploiement. Mais également que le terme de VPN ne se référençait pas qu'a la solution IP Sec. Certes cette solution est la plus utilisée et est une référence. Mais le VPN est avant tout un concept et ne précise rien concernant ses moyens.

Ainsi s'achève notre étude sur les VPNs. On se rend compte que derrière ce concept, une multitude de protocoles, techniques et architectures existent pour leur déploiement. Néanmoins, le choix d'une solution pour votre VPN dépendra évidement de l'utilisation que vous en ferez et de l'investissement financier que vous y mettrez.

Le VPN à pris une dimension proportionnelle au développement d'internet. A l'origine pour déployer les réseaux privés, une nouvelle utilisation voit le jour aujourd'hui avec l'arrivée des technologies sans file. En effet, dès les premières mises en place du 802.11 (WIFI), on nous à démontré ses failles en matière de confidentialité et de sécurité. Un risque parmi d'autres, est de voir ses données transitant dans le réseau être Lues par un « homme du milieu ». Ses problèmes de sécurité sont une grande problématique quand des données sensibles sont communiquées. Les solutions VPN offre une possibilité de garantir cette sécurité et on peut alors penser à la possibilité d'allier le confort d'utilisation d'un réseau sans file à la sécurité des données qu'on transmet.

Bibliothèque :

http://free.korben.info/index.php/VPN
http://www.frameip.com/vpn/
http://telecomix.ceops.eu/DeReynal-DeRorthais-Tan-VPN.pdf
http://www.commentcamarche.net/contents/initiation/vpn.php3
http://www.labo-microsoft.org/articles/win/ras2003/