Configurer le NPS, les contrôleurs de réseau local sans fil (WLC) et les réseaux sans fil

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Conventions
- Informations générales
- Présentation de PEAP
  - Première phase PEAP : Canal chiffré TLS
  - Deuxième phase PEAP : communication authentifiée d'EAP
- Configurer
  - Diagramme du réseau
  - Configurations
    - Configurez le serveur de Microsoft Windows 2008
    - Configurez le serveur de Microsoft Windows 2008 comme contrôleur de domaine
    - Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2008
    - Installation et configuration de Microsoft Windows 2008 Server en tant que serveur AC
    - Connectez les clients de routage au domaine de routage
    - Installer le serveur NPS sur Microsoft Windows 2008 Server
    - Installer un certificat
    - Configurer le service Serveur de stratégie réseau pour l'authentification PEAP-MS-CHAP v2
    - Ajoutez les utilisateurs à l'Active Directory
    - Configuration du contrôleur LAN sans fil et des LAP
    - Configurer le WLC pour l'authentification RADIUS
    - Configurez un WLAN pour les clients de routage
    - Configuration des clients sans fil pour l'authentification PEAP-MS-CHAP v2
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment configurer l’authentification PEAP avec MS-CHAP avec le serveur NPS de Microsoft comme serveur RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de l'installation de Windows 2008
- Connaissance de l'installation du contrôleur Cisco

Assurez-vous que ces conditions sont remplies avant de tenter cette configuration :

- Installez Microsoft Windows Server 2008 sur chacun des serveurs du TP de test.
- Mettez à jour tous les Service Packs.
- Installez les contrôleurs et les points d'accès légers (LAP).
- Configurez les dernières mises à jour logicielles.

Pour obtenir des informations sur l'installation initiale et la configuration des contrôleurs sans fil de la gamme Cisco 5508, reportez-vous au Guide d'installation des contrôleurs sans fil de la gamme Cisco 5500.



Remarque : Ce document est destiné à donner aux lecteurs un exemple sur la configuration requise sur un serveur Microsoft pour l'authentification PEAP-MS-CHAP. La configuration du serveur Microsoft Windows présentée dans ce document a été testée au cours des travaux pratiques et s'est révélée fonctionner comme prévu. Si vous rencontrez des problèmes avec la configuration, contactez Microsoft pour obtenir de l'aide. Le centre d'assistance technique Cisco (TAC) ne prend pas en charge la configuration du serveur Microsoft Windows.

Les guides d'installation et de configuration de Microsoft Windows 2008 sont disponibles sur Microsoft TechNet.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur sans fil Cisco 5508 exécutant la version 7.4 du microprogramme
- Point d'accès Cisco Aironet 3602 avec protocole LWAPP (Lightweight Access Point Protocol)
- Windows 2008 Enterprise Server avec NPS, autorité de certification (CA), protocole DHCP (Dynamic Host Control Protocol) et services DNS (Domain Name System) installés
- PC client Microsoft Windows 7
- Commutateur Cisco Catalyst 3560

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d’informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

Ce document fournit un exemple de configuration pour l'authentification PEAP (Protected Extensible Authentication Protocol) avec MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) version 2 dans un réseau sans fil unifié Cisco avec le serveur NPS (Microsoft Network Policy Server) comme serveur RADIUS.

Présentation de PEAP

Le protocole PEAP utilise le protocole TLS (Transport Level Security) pour créer un canal chiffré entre un client PEAP authentifié, tel qu'un ordinateur portable sans fil, et un authentificateur PEAP, tel que Microsoft NPS ou tout serveur RADIUS. PEAP ne spécifie pas de méthode d'authentification, mais fournit une sécurité supplémentaire pour les autres protocoles d'authentification extensible (EAP), tels que EAP-MS-CHAP v2, qui peuvent fonctionner via le canal chiffré TLS fourni par PEAP. Le processus d'authentification PEAP consiste en deux phases principales .

Première phase PEAP : Canal chiffré TLS

Le client sans fil s'associe avec l'AP. Une association basée sur la norme IEEE 802.11 fournit une authentification de système ouvert ou de clé partagée avant qu'une association sécurisée ne soit créée entre le client et le point d'accès. Après que l'association basée sur IEEE 802.11 est établie avec succès entre le client de routage et le point d'accès, la session de TLS est négociée avec l'AP. Une fois l'authentification terminée entre le client sans fil et NPS, la session TLS est négociée entre le client et NPS. La clé qui dérive de cette négociation est utilisée pour crypter toute la communication ultérieure.

Deuxième phase PEAP : communication authentifiée d'EAP

La communication d'EAP, qui inclut la négociation d'EAP, se produit à l'intérieur du canal de TLS créé par PEAP dans la première phase du processus d'authentification de PEAP. Le NPS authentifie le client sans fil avec EAP-MS-CHAP v2. Le LAP et le contrôleur transfèrent uniquement les messages entre le client sans fil et le serveur RADIUS. Le contrôleur LAN sans fil (WLC) et le LAP ne peuvent pas déchiffrer ces messages, car il ne s'agit pas du point d'extrémité TLS.

La séquence de messages RADIUS pour une tentative d'authentification réussie (où l'utilisateur a fourni des informations d'identification valides basées sur un mot de passe avec PEAP-MS-CHAP v2) est :

1. Le NPS envoie un message de demande d’identité au client : Requête EAP/Identité.
2. Le client répond avec un message de réponse d'identité : Réponse EAP/Identité.
3. Le NPS envoie un message de demande de confirmation MS-CHAP v2 : Requête-

EAP/Type-EAP=EAP MS-CHAP-V2 (défi).

4. Le client répond avec un défi et la réponse MS-CHAP v2 : Réponse-EAP/Type-EAP=EAP-MS-CHAP-V2 (réponse).
5. Le serveur NPS renvoie un paquet de réussite MS-CHAP v2 lorsque le serveur a authentifié le client : Requête-EAP/Type-EAP=EAP-MS-CHAP-V2 (réussite).
6. Le client de routage répond avec un paquet de réussite MS-CHAP v2 quand le client a authentifié le serveur avec succès : Réponse-EAP/Type-EAP=EAP-MS-CHAP-V2 (réussite).
7. Le NPS envoie une valeur TLV (EAP-type-length-value) qui indique une authentification réussie.
8. Le client répond avec un message de réussite d'état EAP-TLV.
9. Le serveur termine l'authentification et envoie un message EAP-Success en texte clair. Si des VLAN sont déployés pour l'isolation du client, les attributs VLAN sont inclus dans ce message.

Configurer

Dans cette section, vous trouverez les informations nécessaires à la configuration de PEAP-MS-CHAP v2.

Remarque : Utilisez l'outil Command Lookup Tool pour obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

Diagramme du réseau

Cette configuration utilise la configuration de réseau suivante :

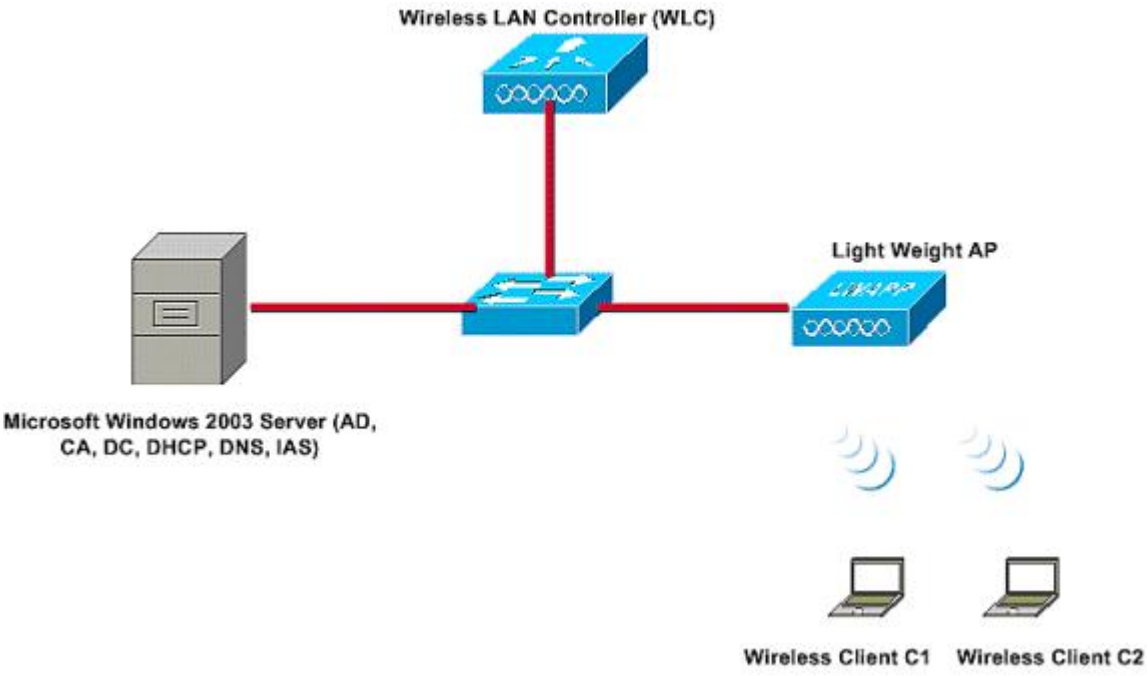


Diagramme du réseau

Dans cette configuration, un serveur de Microsoft Windows 2008 effectue ces rôles :

- Contrôleur de domaine pour le domaine
- Serveur DHCP/DNS
- serveur AC
- NPS : pour authentifier les utilisateurs sans fil
- Active Directory - pour mettre à jour la base de données utilisateur

Le serveur se connecte au réseau câblé via un commutateur de couche 2, comme illustré. Le WLC et le LAP enregistré se connectent également au réseau via le commutateur de couche 2.

Les clients sans fil utilisent l'authentification WPA2 (Wi-Fi Protected Access 2) - PEAP-MS-CHAP v2 pour se connecter au réseau sans fil.

Configurations

L'objectif de cet exemple est de configurer le serveur Microsoft 2008, le contrôleur de réseau local sans fil et le point d'accès léger pour authentifier les clients sans fil avec l'authentification PEAP-MS-CHAP v2. Ce processus comporte trois étapes principales :

1. Configurez Microsoft Windows 2008 Server.
2. Configurez le WLC et les points d'accès légers.
3. Configurer les clients sans fil

Configurez le serveur de Microsoft Windows 2008

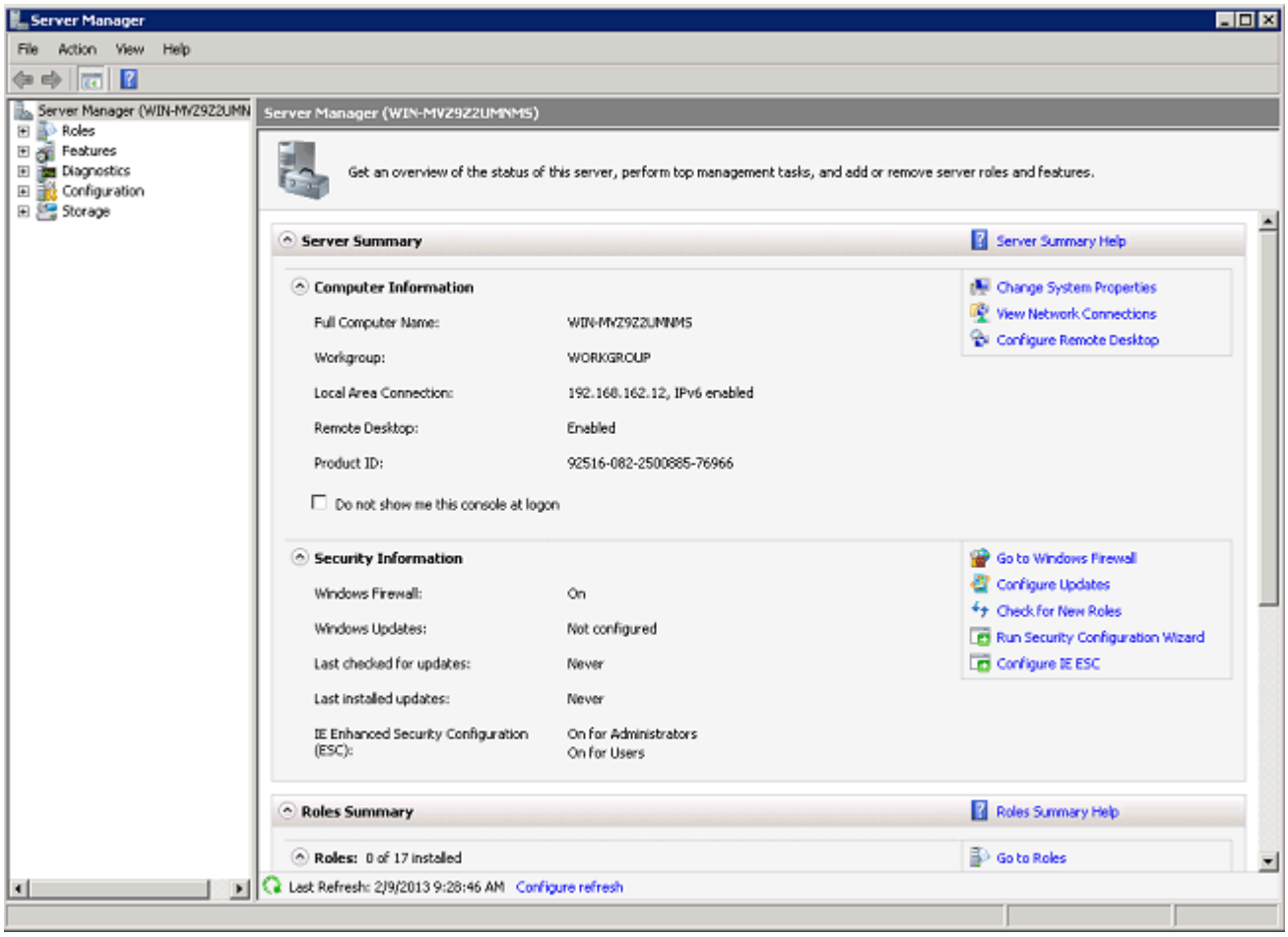
Dans cet exemple, la configuration complète du serveur Microsoft Windows 2008 comprend les étapes suivantes :

1. Configurez le serveur en tant que contrôleur de domaine.
2. Installer et configurer les services DHCP.
3. installer et configurer le serveur en tant que serveur AC.
4. Connectez les clients au domaine.
5. Installez le NPS.
6. Installer un certificat.
7. Configurez le NPS pour l'authentification PEAP.
8. Ajoutez des utilisateurs à Active Directory.

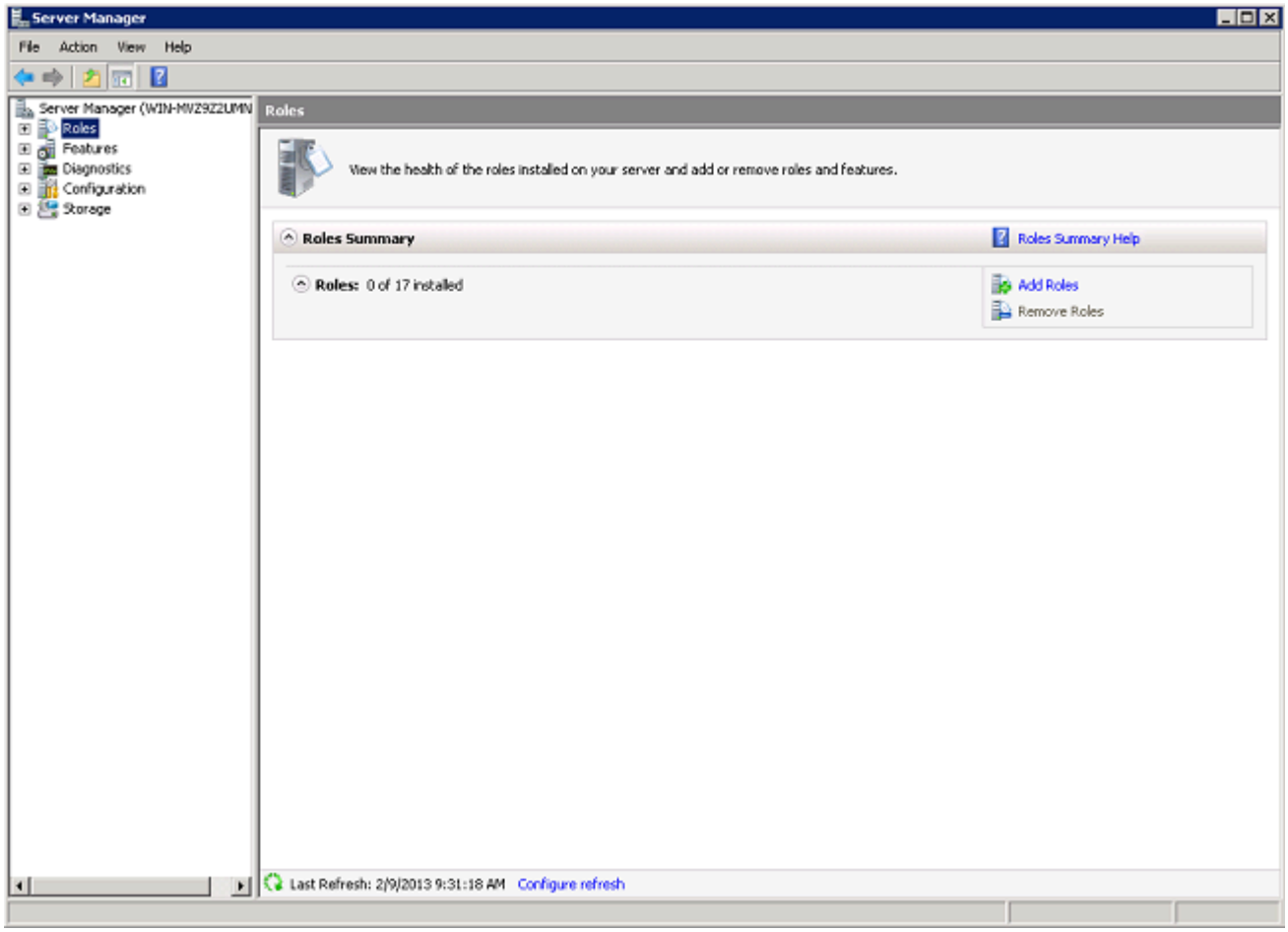
Configurez le serveur de Microsoft Windows 2008 comme contrôleur de domaine

Complétez ces étapes afin de configurer le serveur Microsoft Windows 2008 en tant que contrôleur de domaine :

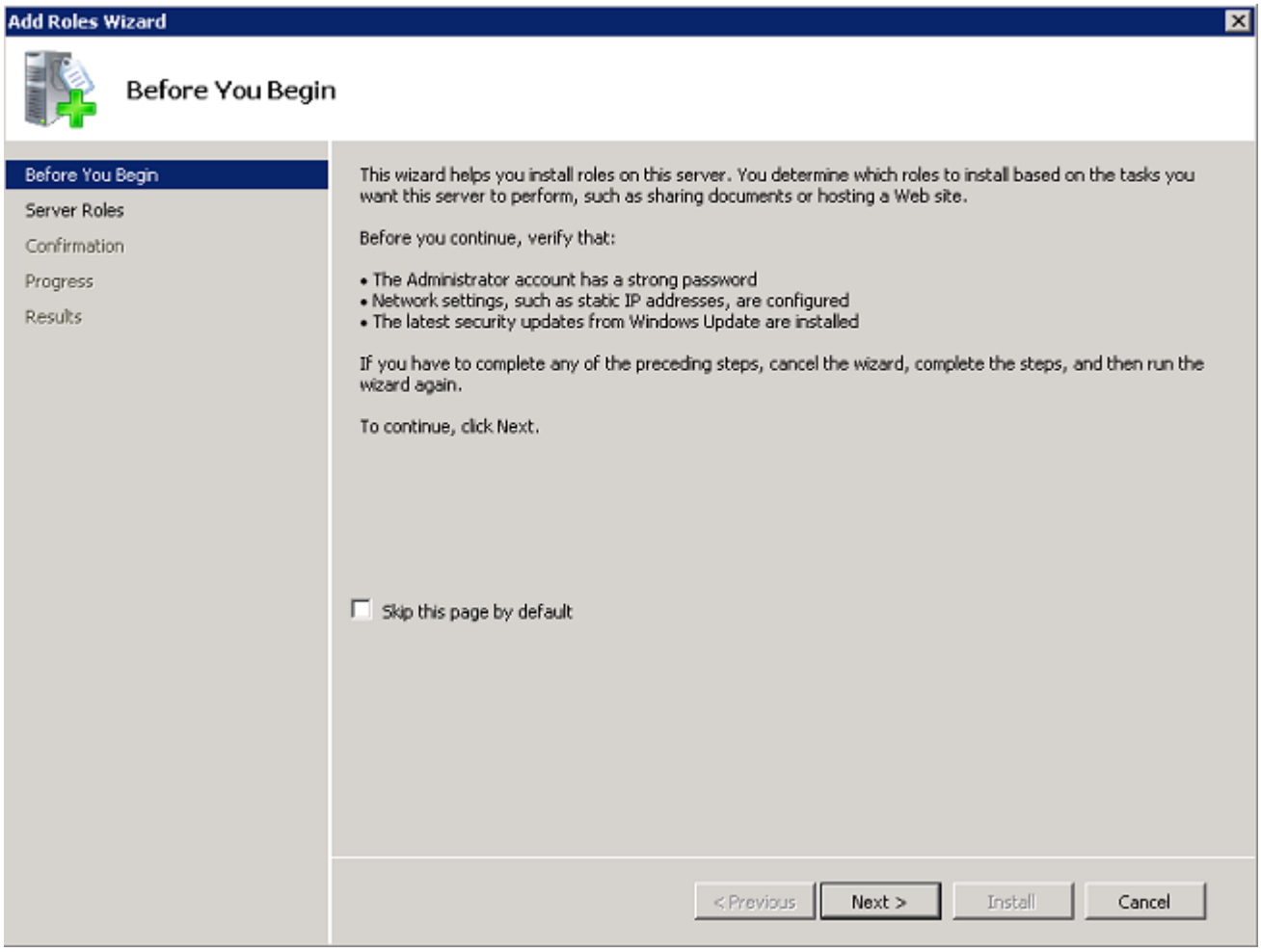
1. Cliquez sur Démarrer> Gestionnaire de serveur.



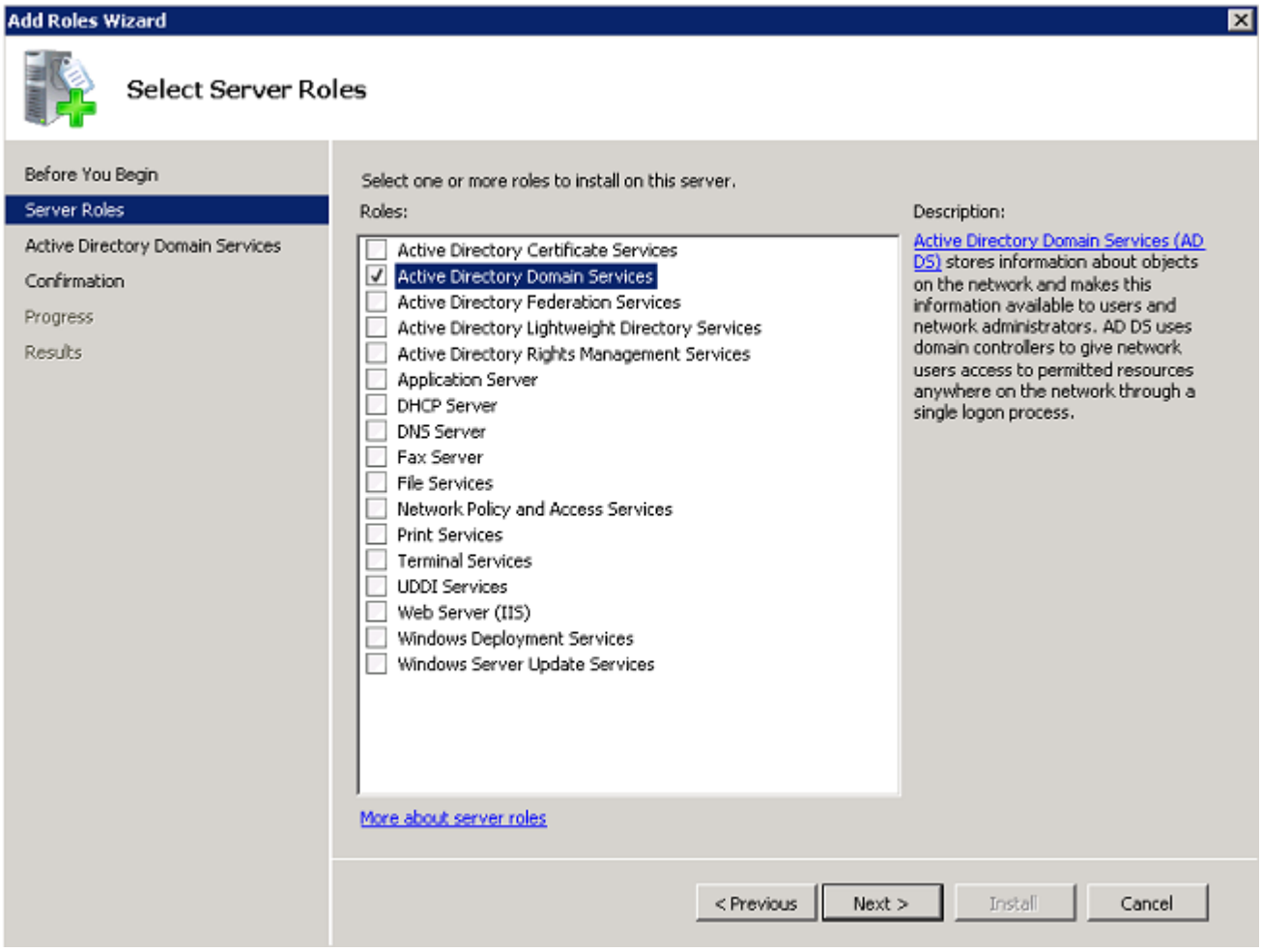
2. Cliquez sur Rôles> Ajouter des rôles.



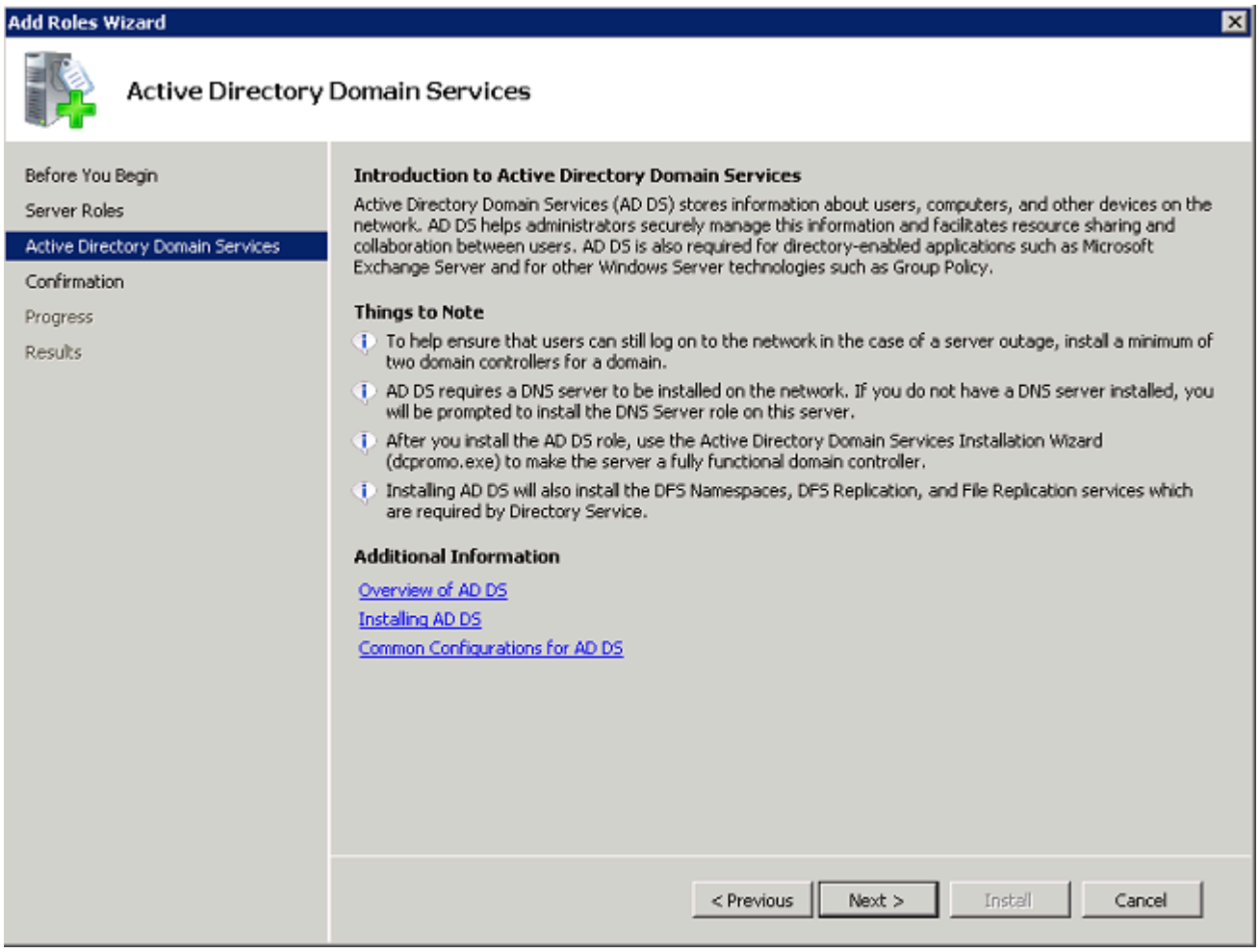
3. Cliquez sur Next (Suivant).



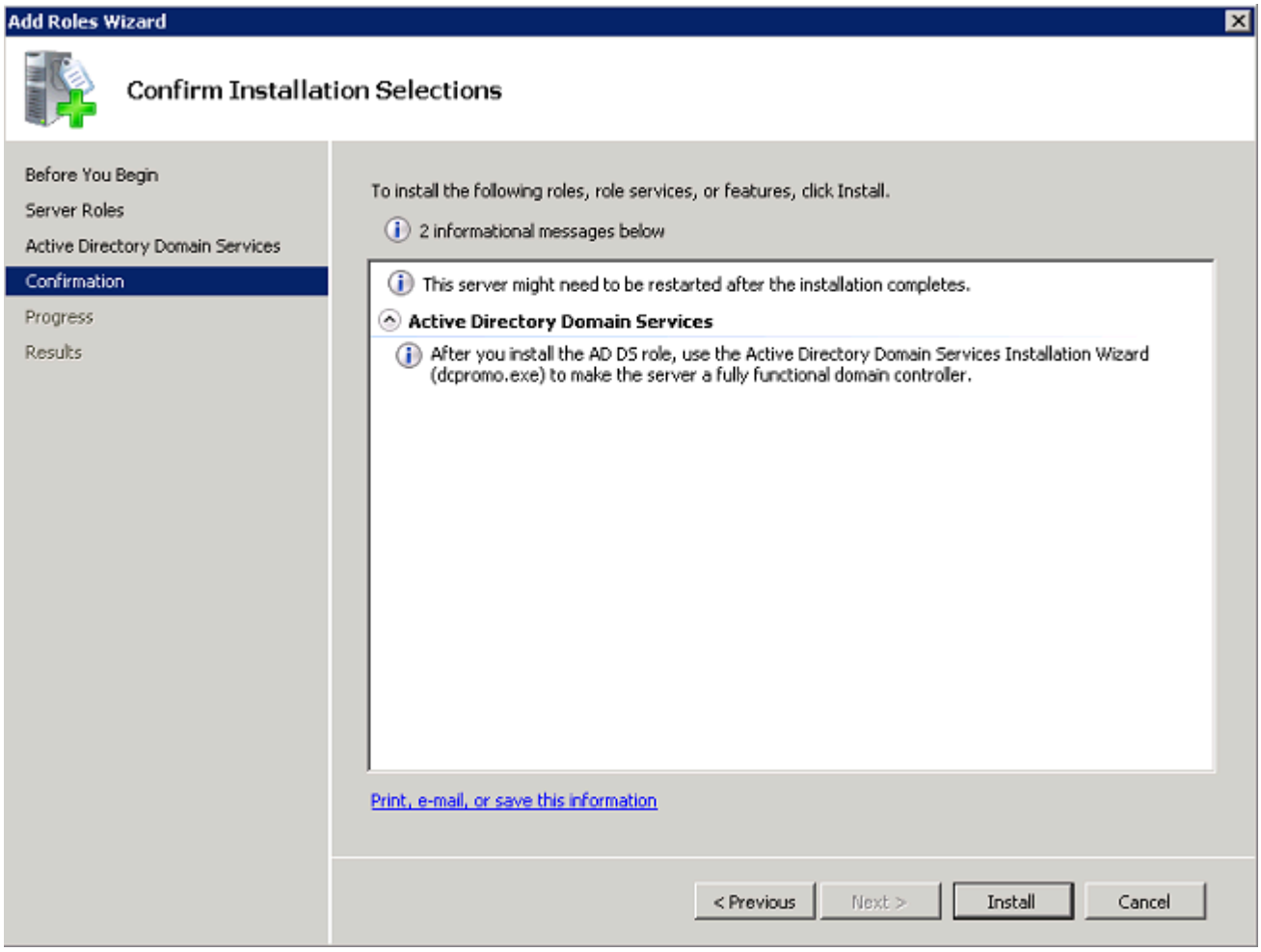
4. Sélectionnez le service Services de domaine Active Directory, puis cliquez sur Suivant.



5. Consultez la section Introduction aux services de domaine Active Directory, puis cliquez sur Suivant.

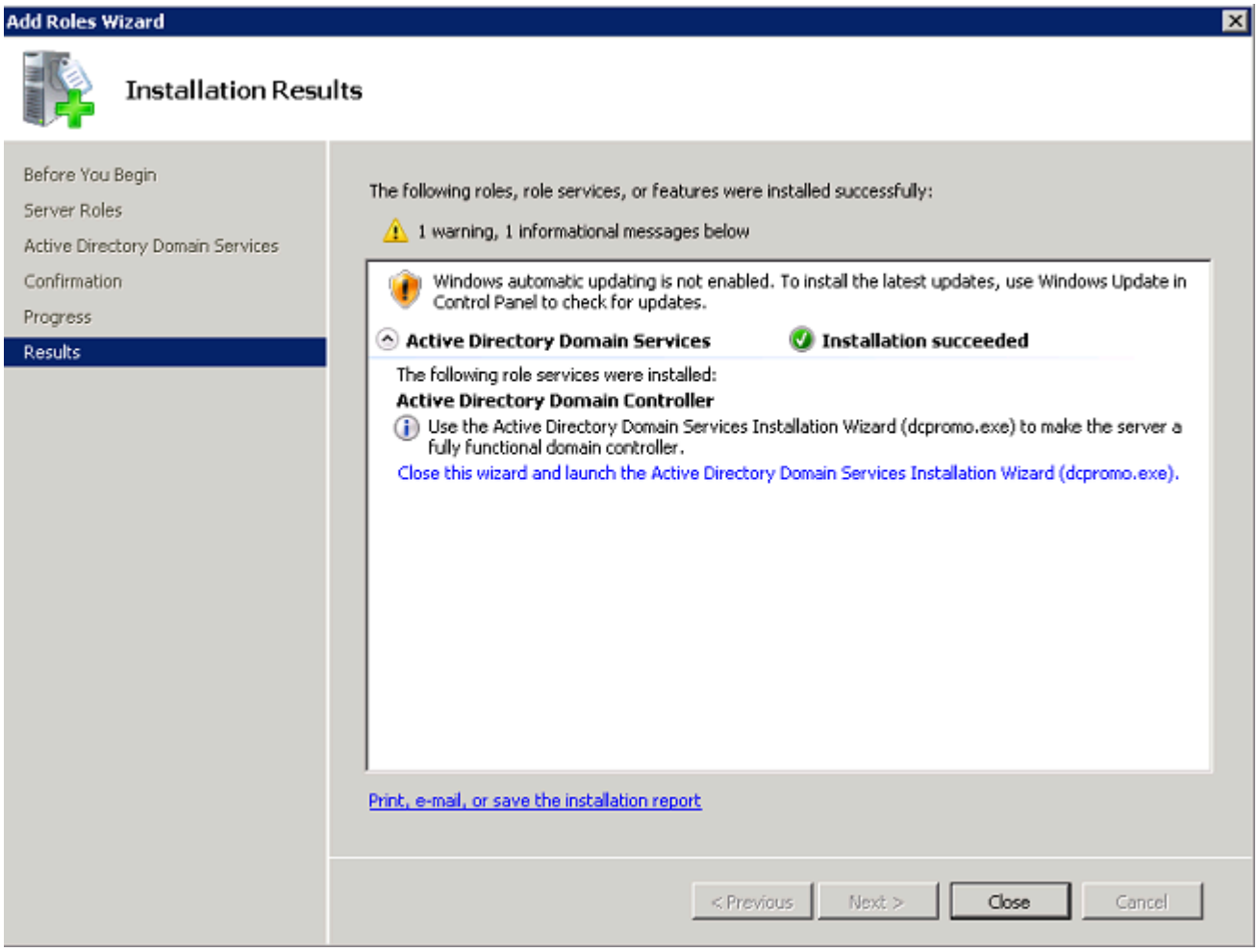


6. Cliquez sur Install pour lancer le processus d'installation.

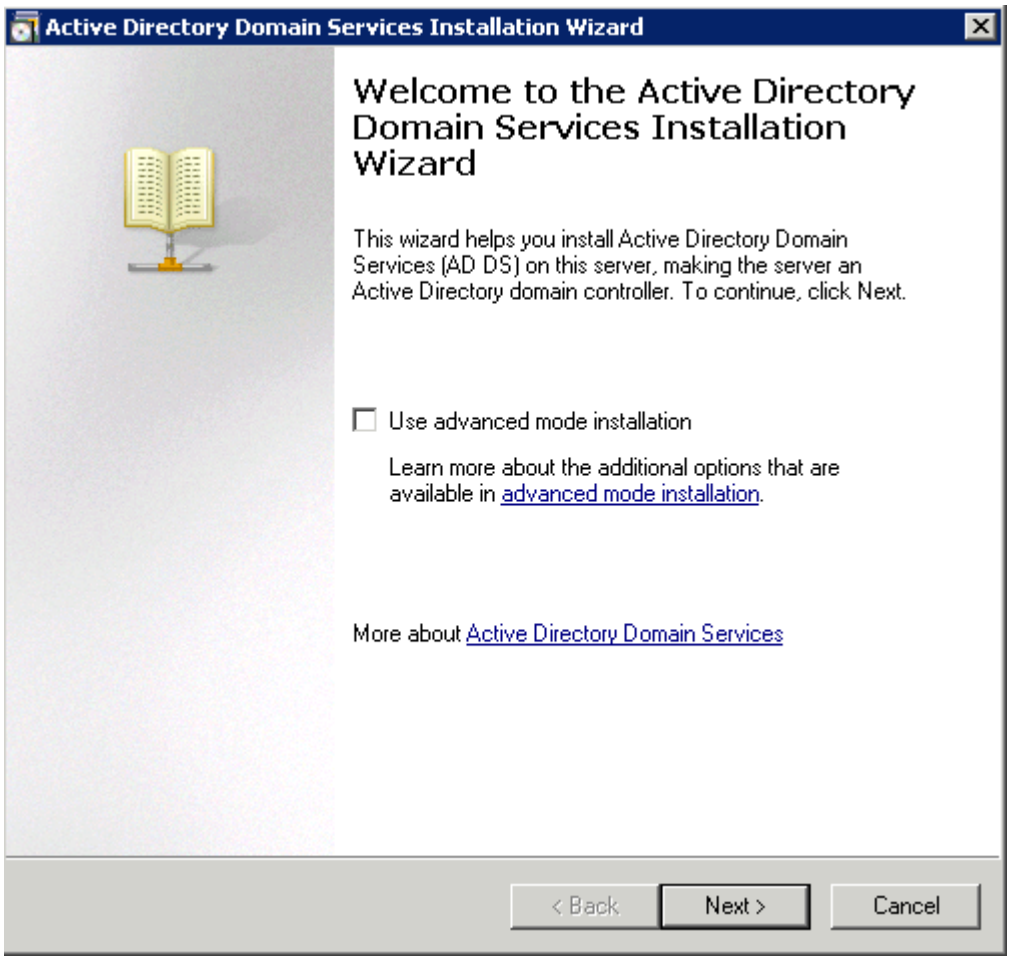


L'installation se poursuit et se termine.

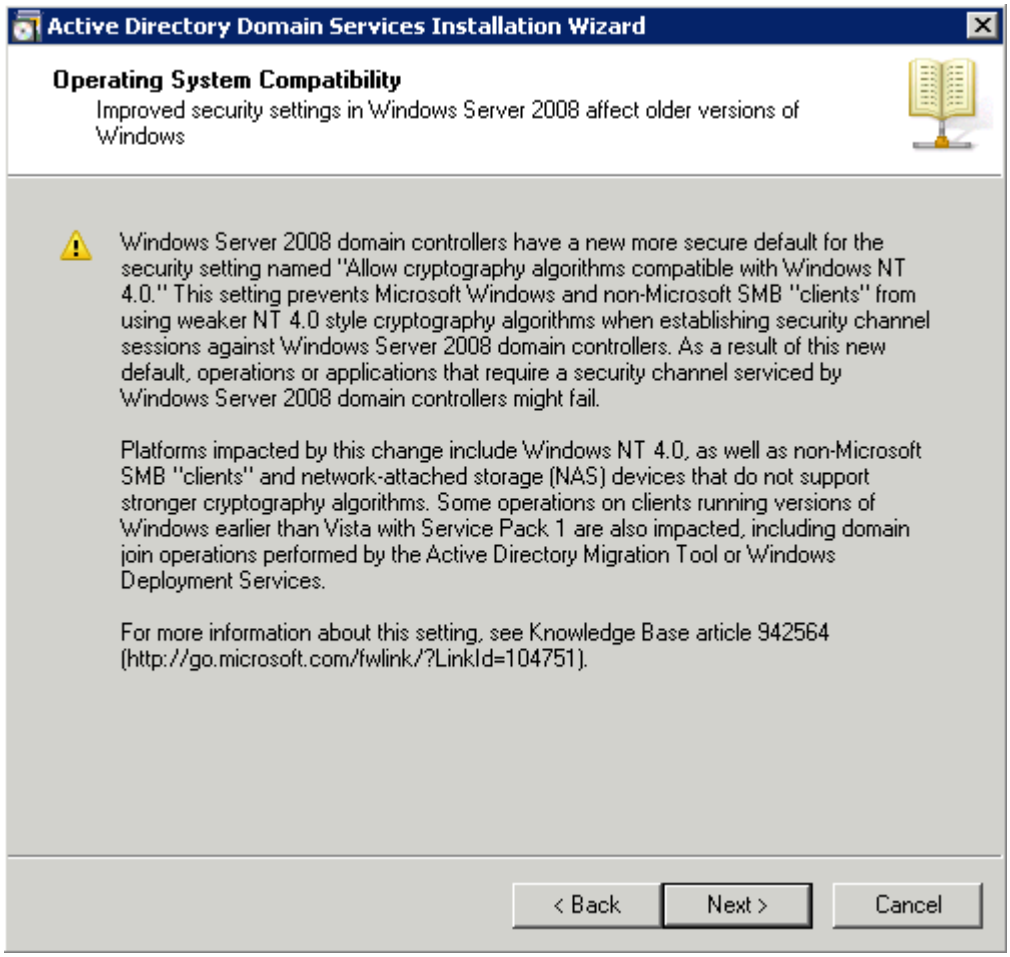
7. Cliquez sur Fermer cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour poursuivre l'installation et la configuration d'Active Directory.



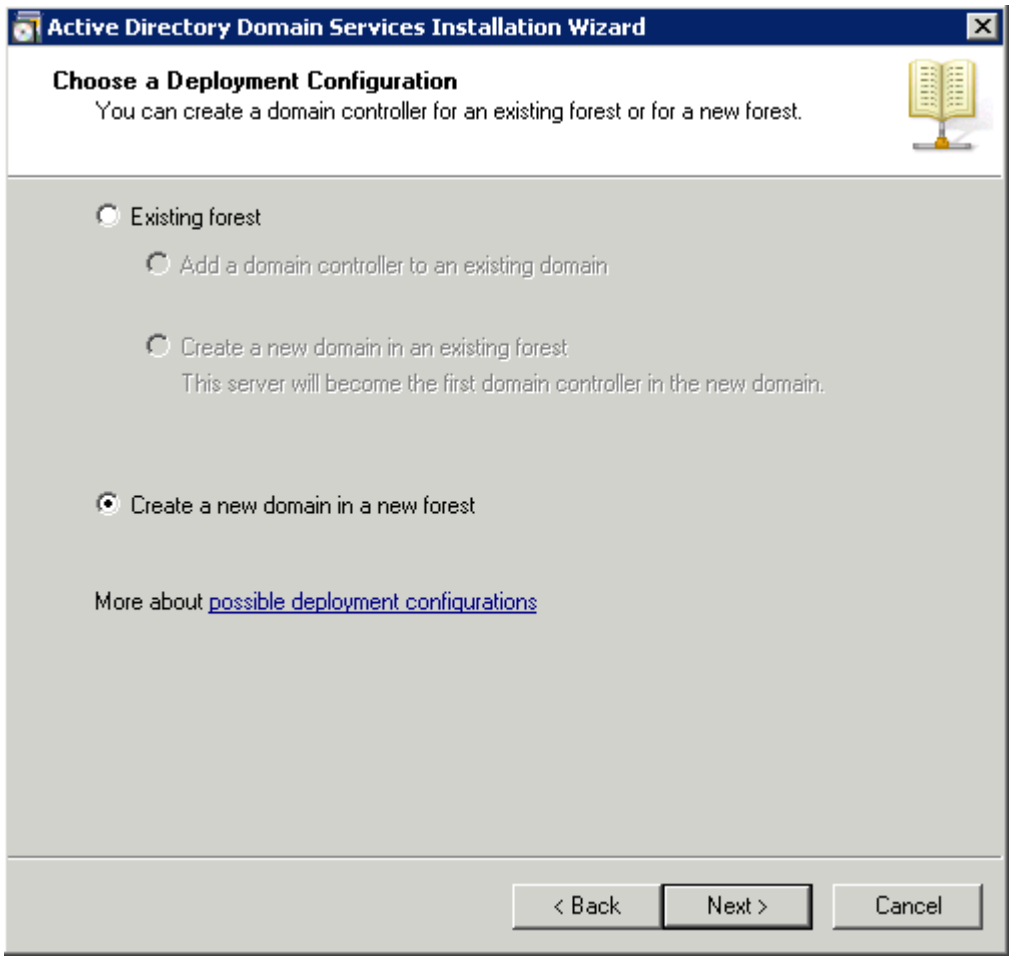
8. Cliquez sur Next pour exécuter l'Assistant Installation des services de domaine Active Directory.



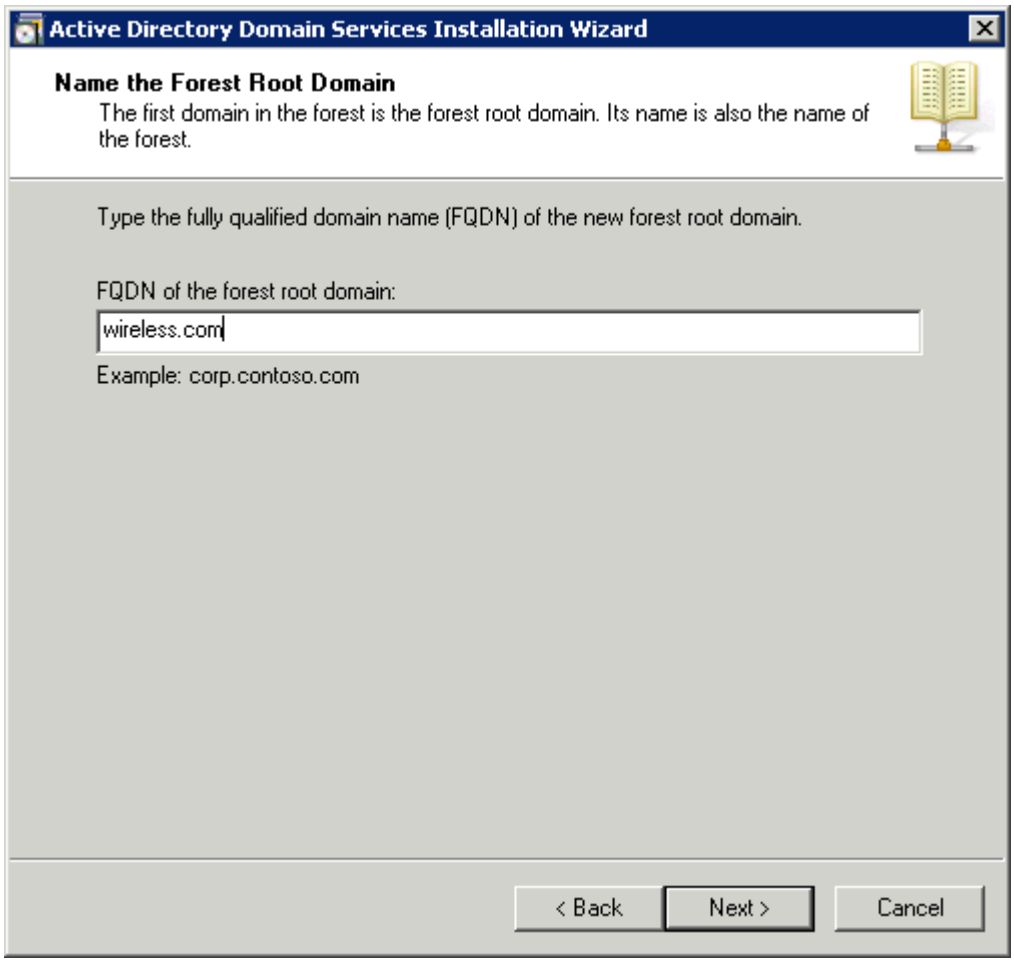
9. Vérifiez les informations sur la compatibilité du système d'exploitation, et cliquez sur Next.



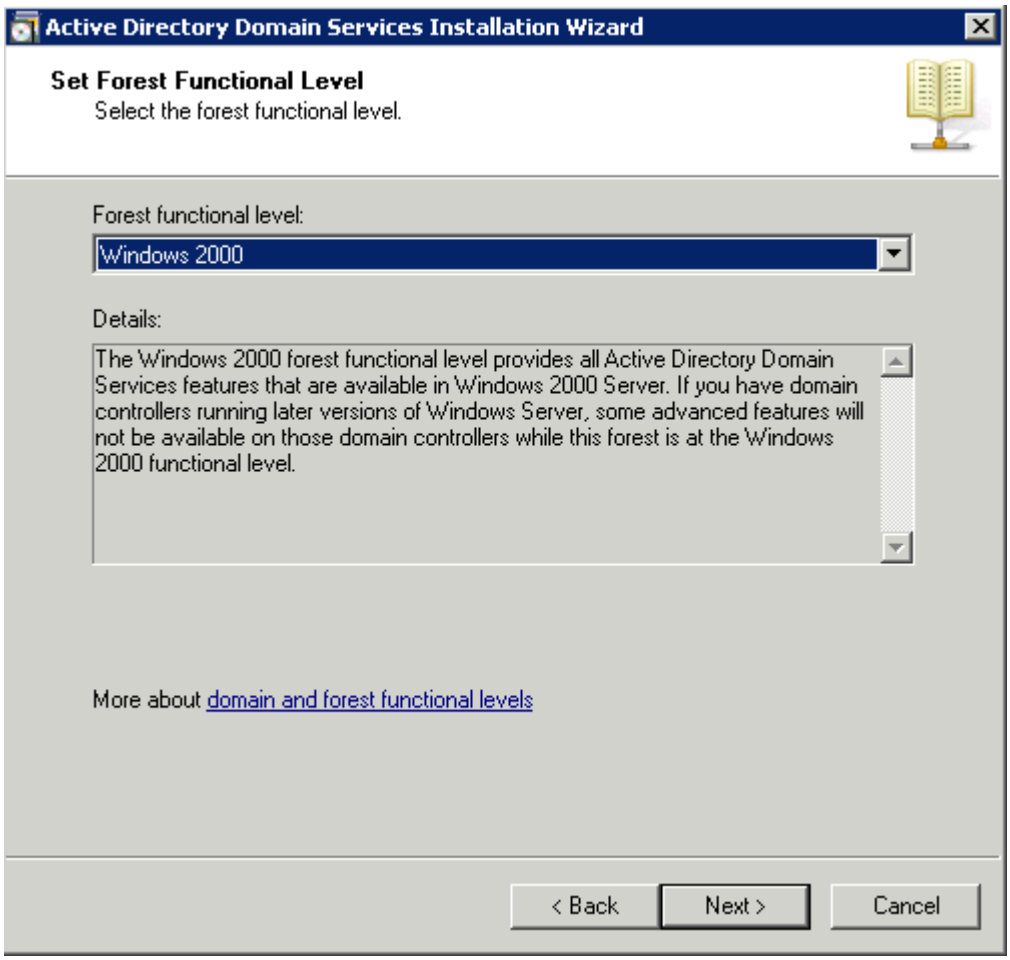
10. Cliquez sur Create a new domain in a new forest > Next afin de créer un nouveau domaine.



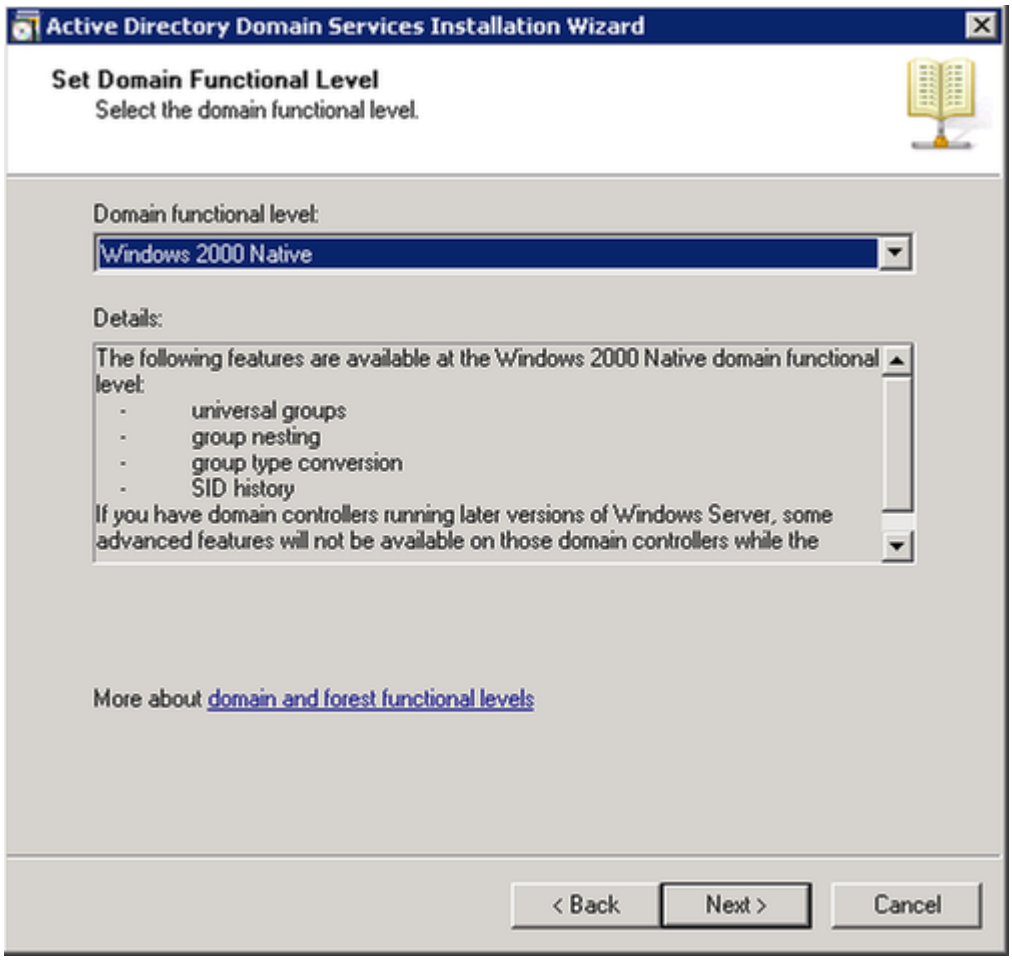
11. Entrez le nom DNS complet du nouveau domaine, puis cliquez sur Next.



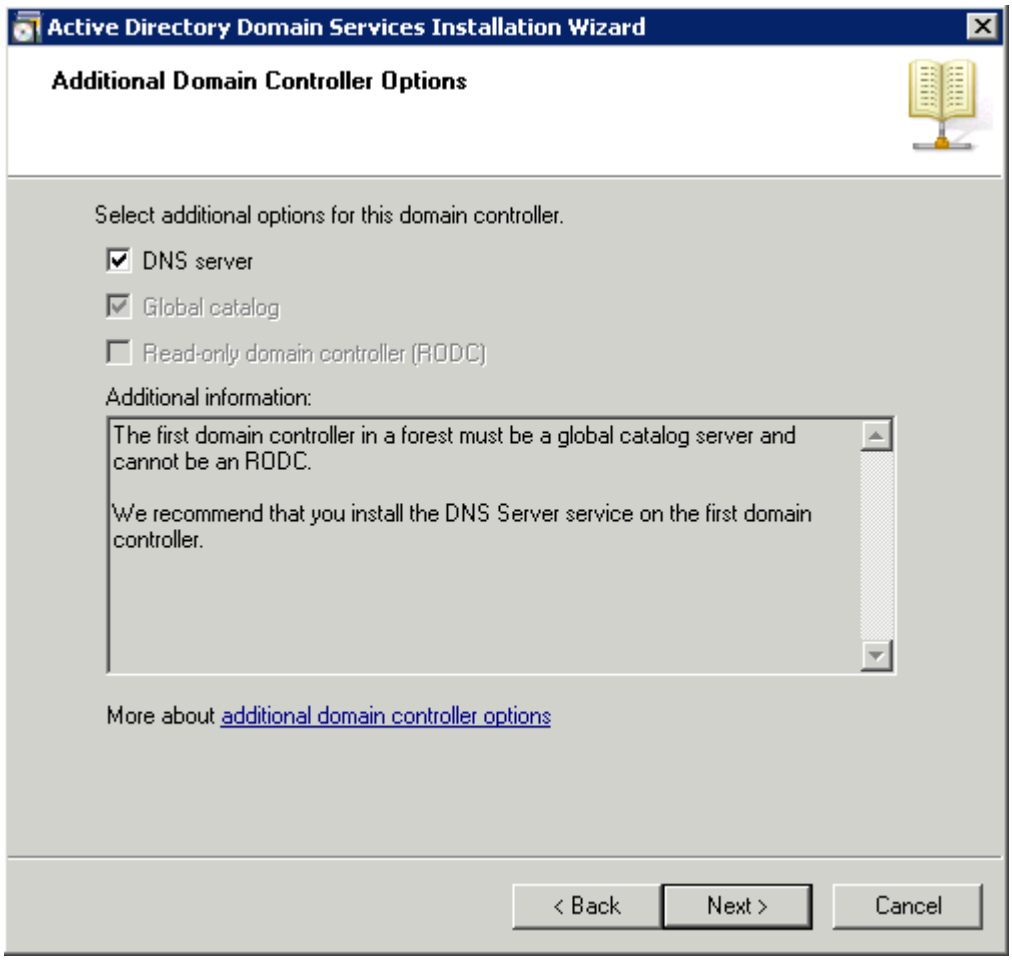
12. Sélectionnez le niveau fonctionnel de la forêt pour votre domaine, puis cliquez sur Suivant.



13. Sélectionnez le niveau fonctionnel de domaine pour votre domaine, puis cliquez sur Suivant.



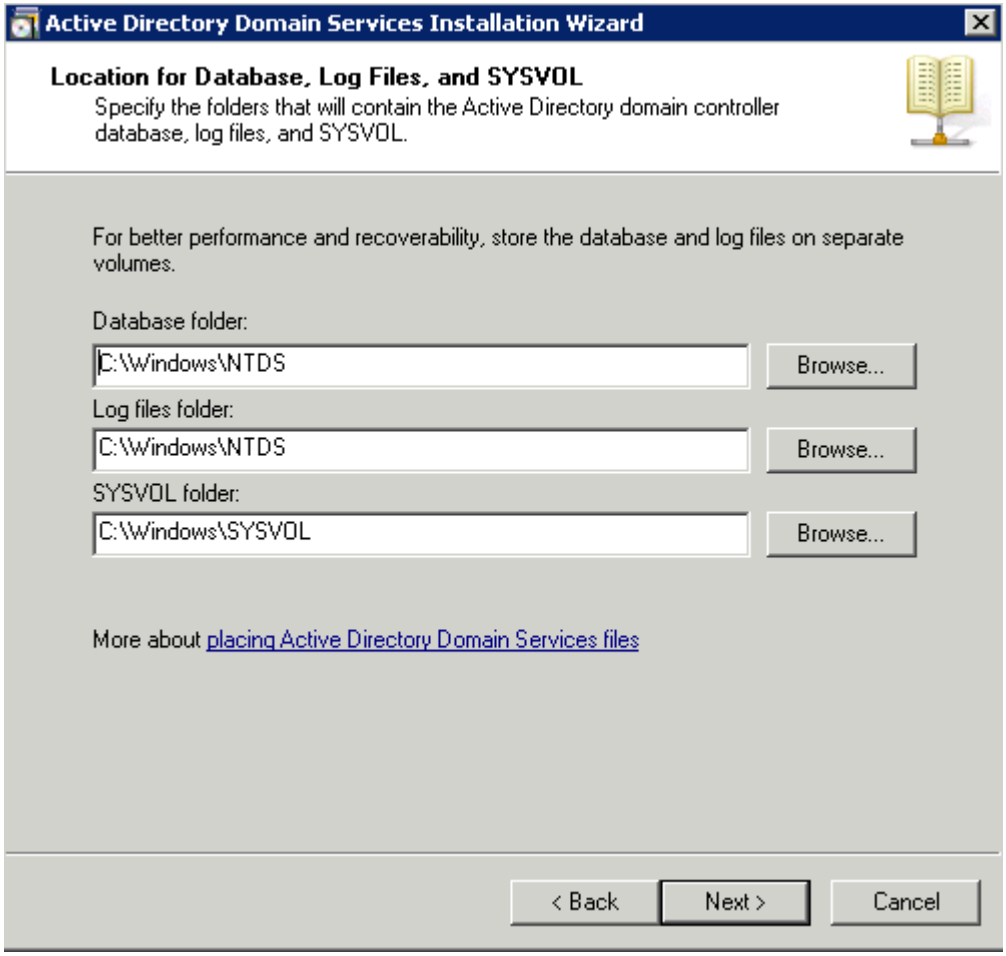
14. Assurez-vous que le serveur DNS est sélectionné, puis cliquez sur Next.



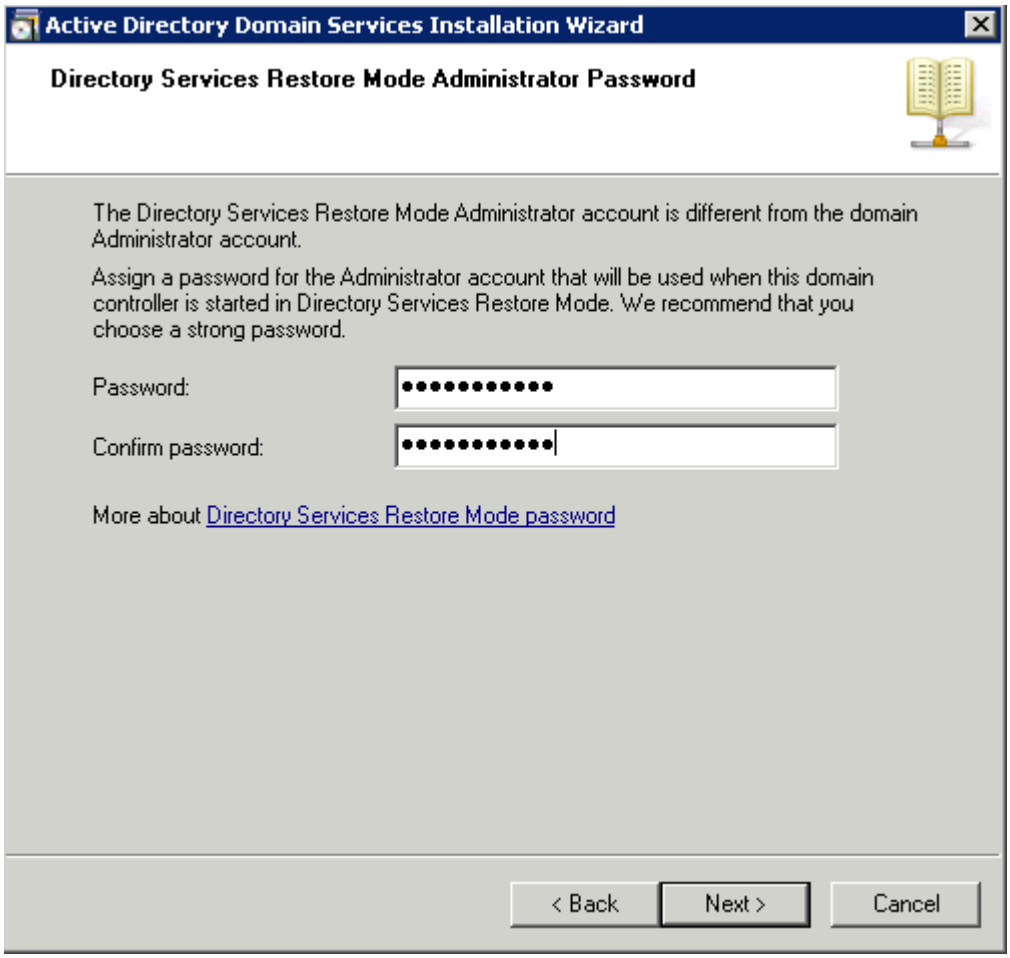
15. Cliquez sur Yes pour que l'assistant d'installation crée une nouvelle zone dans DNS pour le domaine.



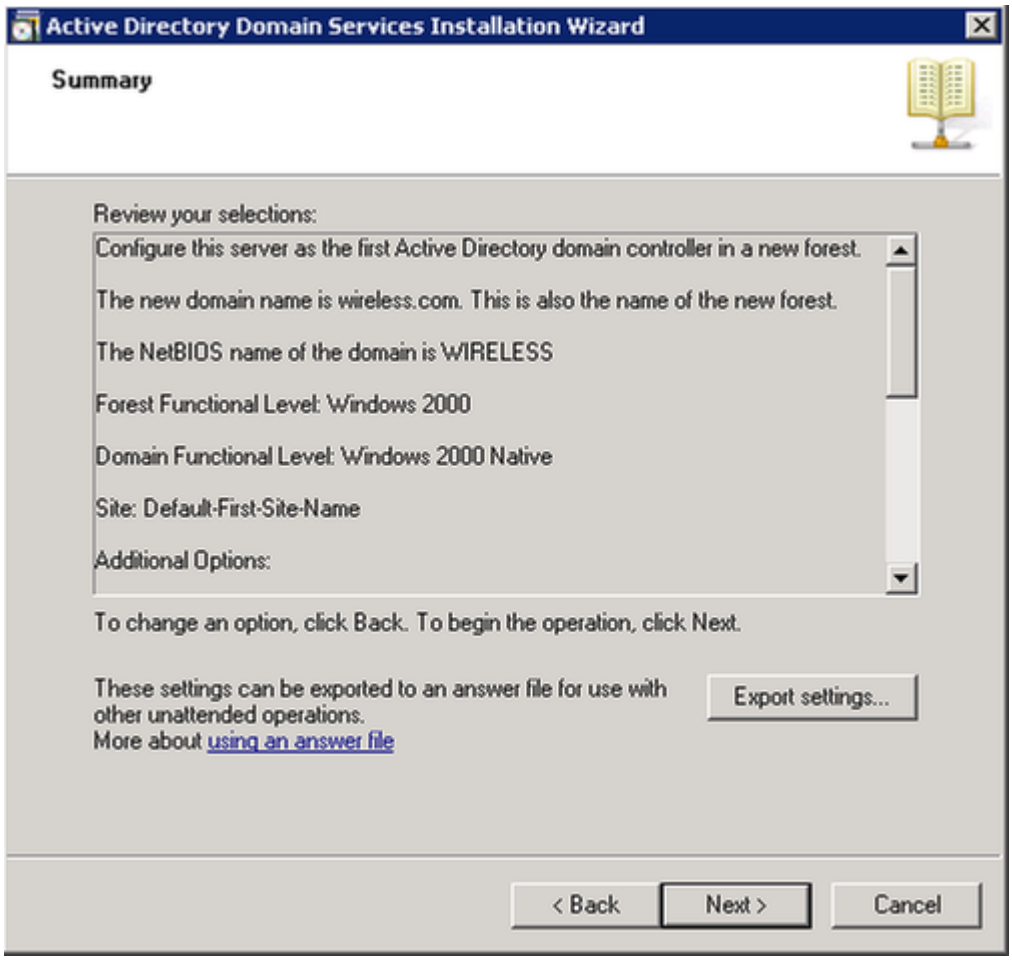
16. Sélectionnez les dossiers qu'Active Directory doit utiliser pour ses fichiers, puis cliquez sur Suivant.



17. Saisissez le mot de passe de l'administrateur, puis cliquez sur Next.

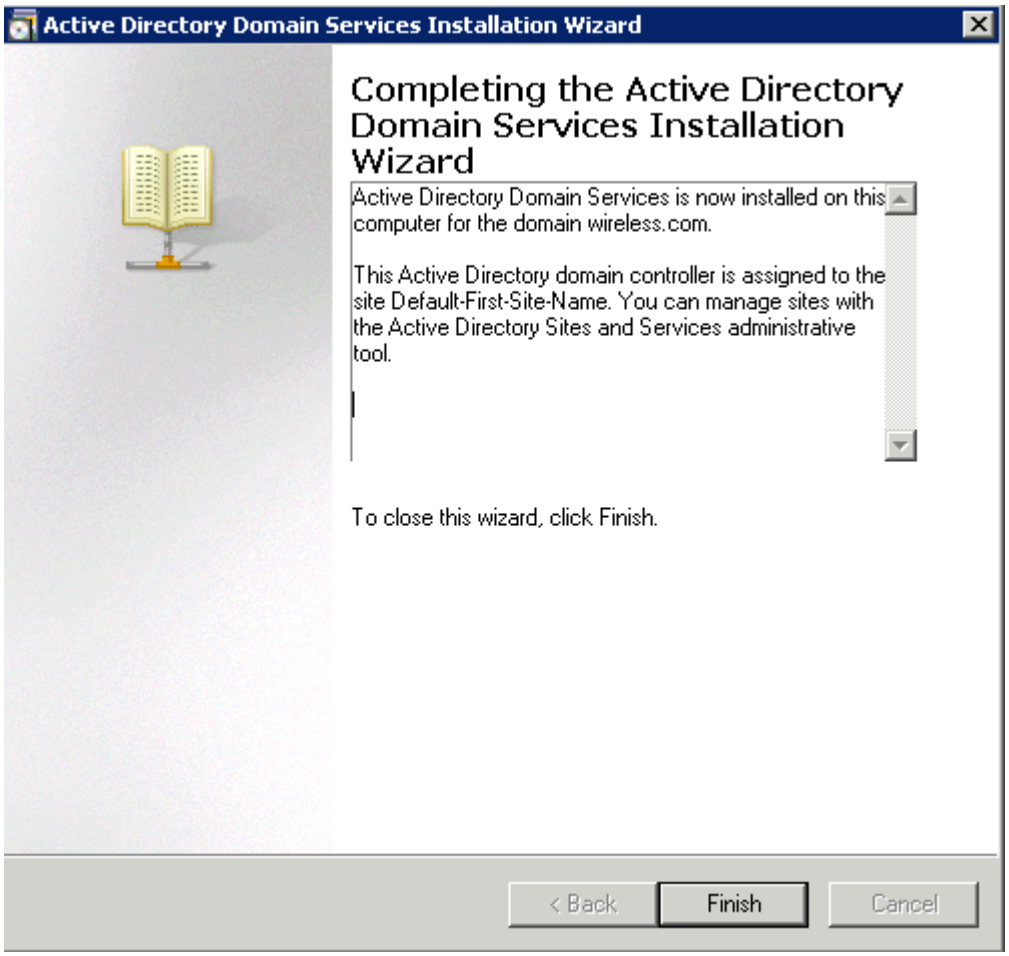


18. Vérifiez vos sélections, puis cliquez sur Next.

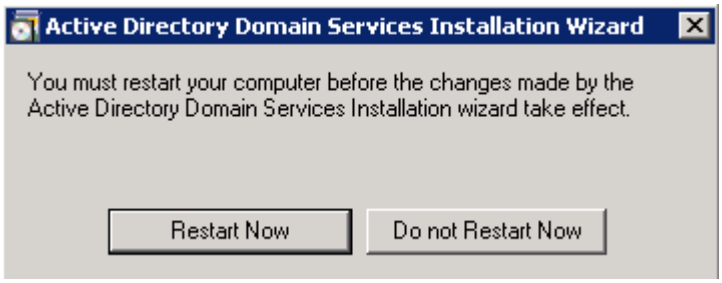


L'installation se poursuit.

19. Cliquez sur Terminer pour fermer l'Assistant.



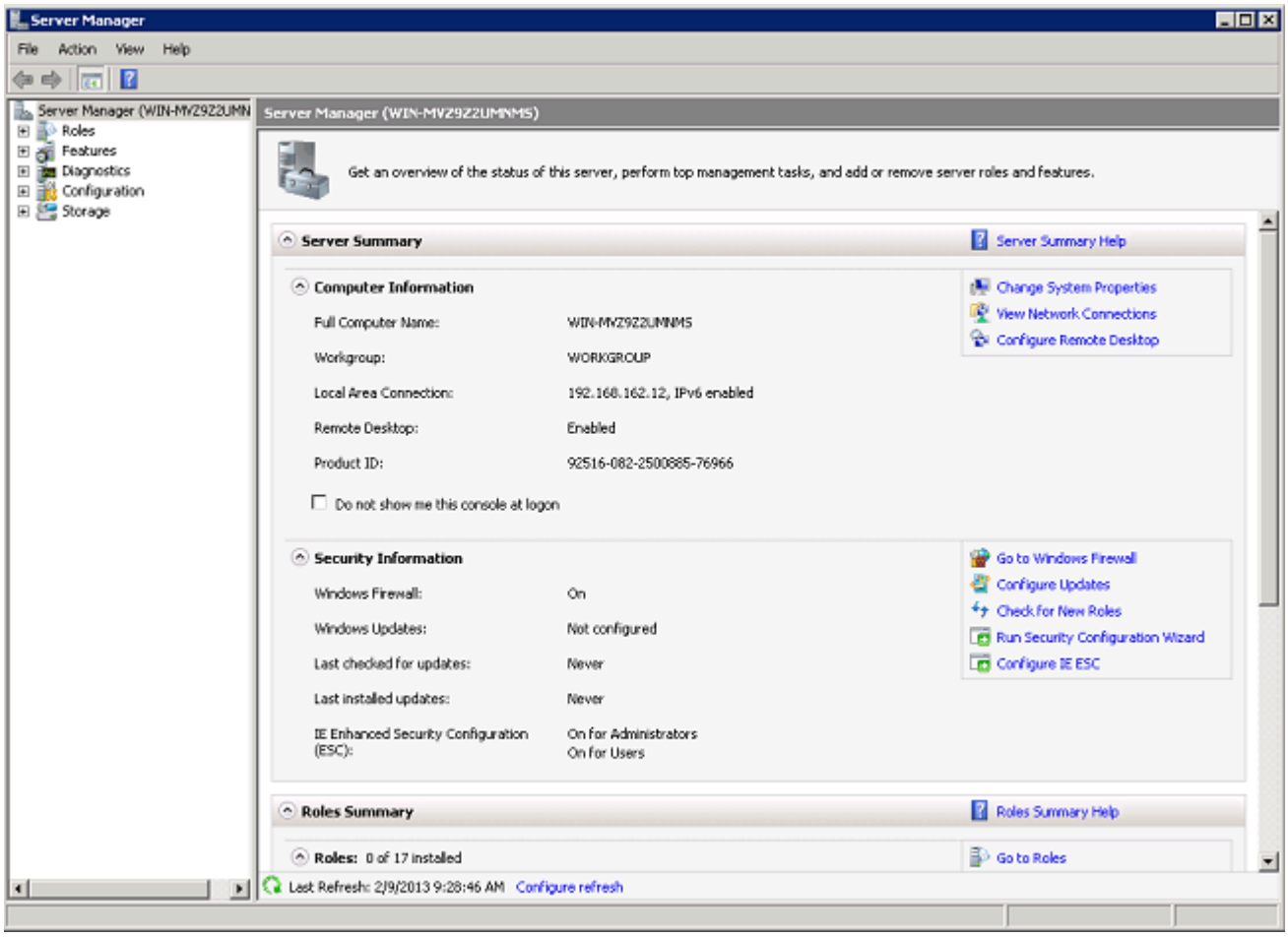
20. Redémarrez le serveur pour que les modifications prennent effet.



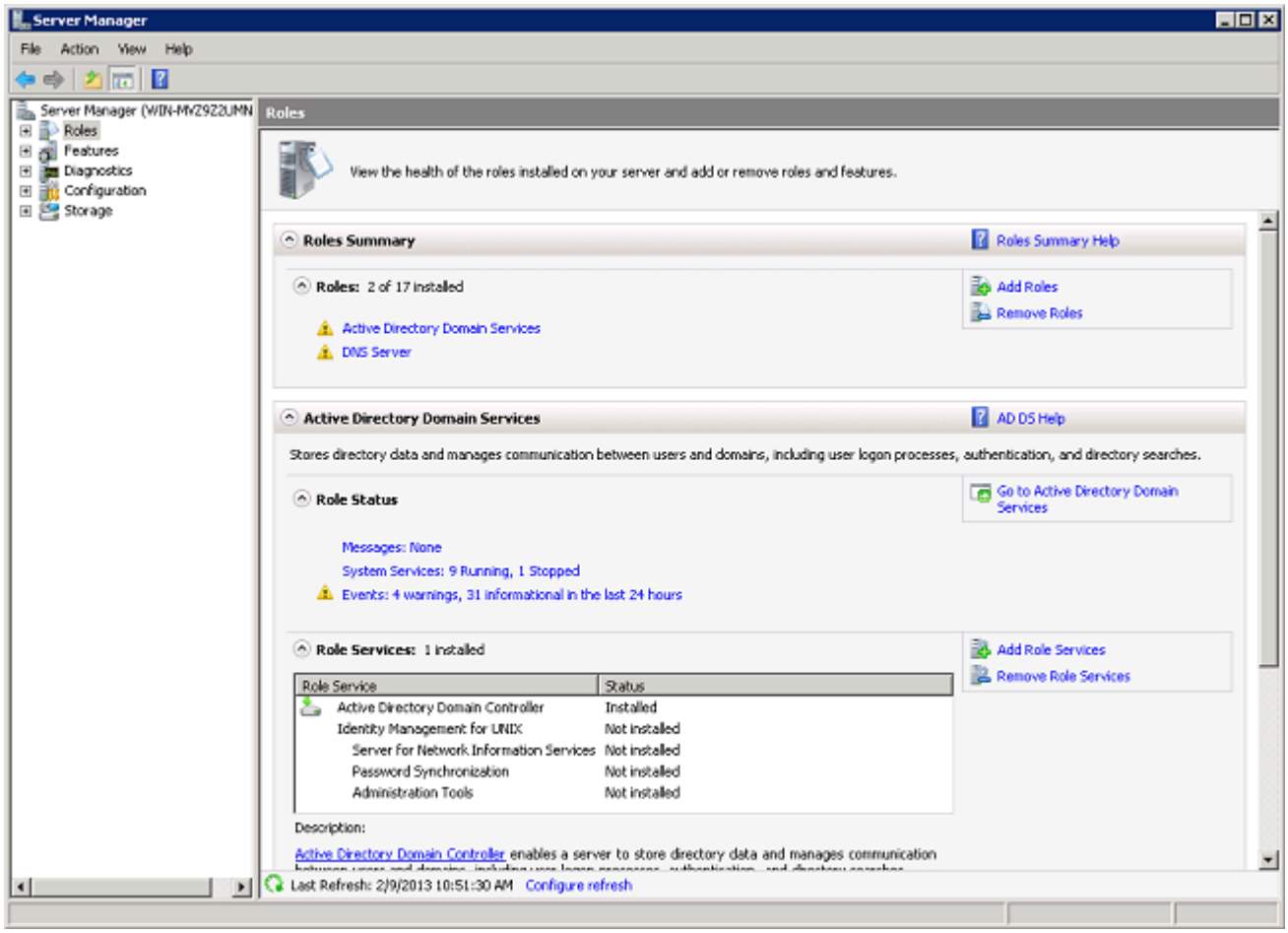
Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2008

Le service DHCP sur le serveur de Microsoft 2008 est utilisé pour fournir des adresses IP aux clients sans fil. Complétez ces étapes afin d'installer et de configurer les services DHCP :

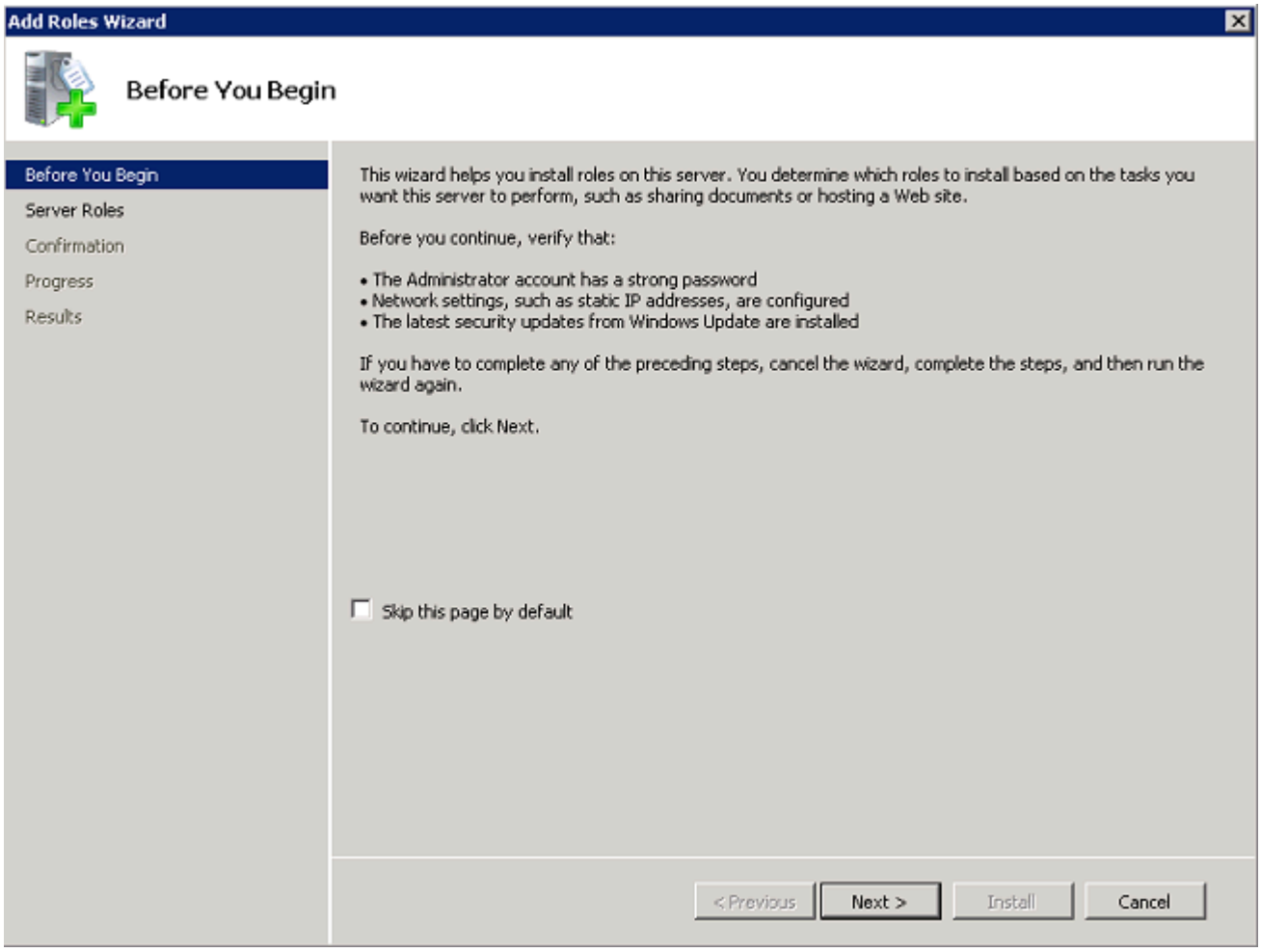
1. Cliquez sur Démarrer>Gestionnaire de serveur.



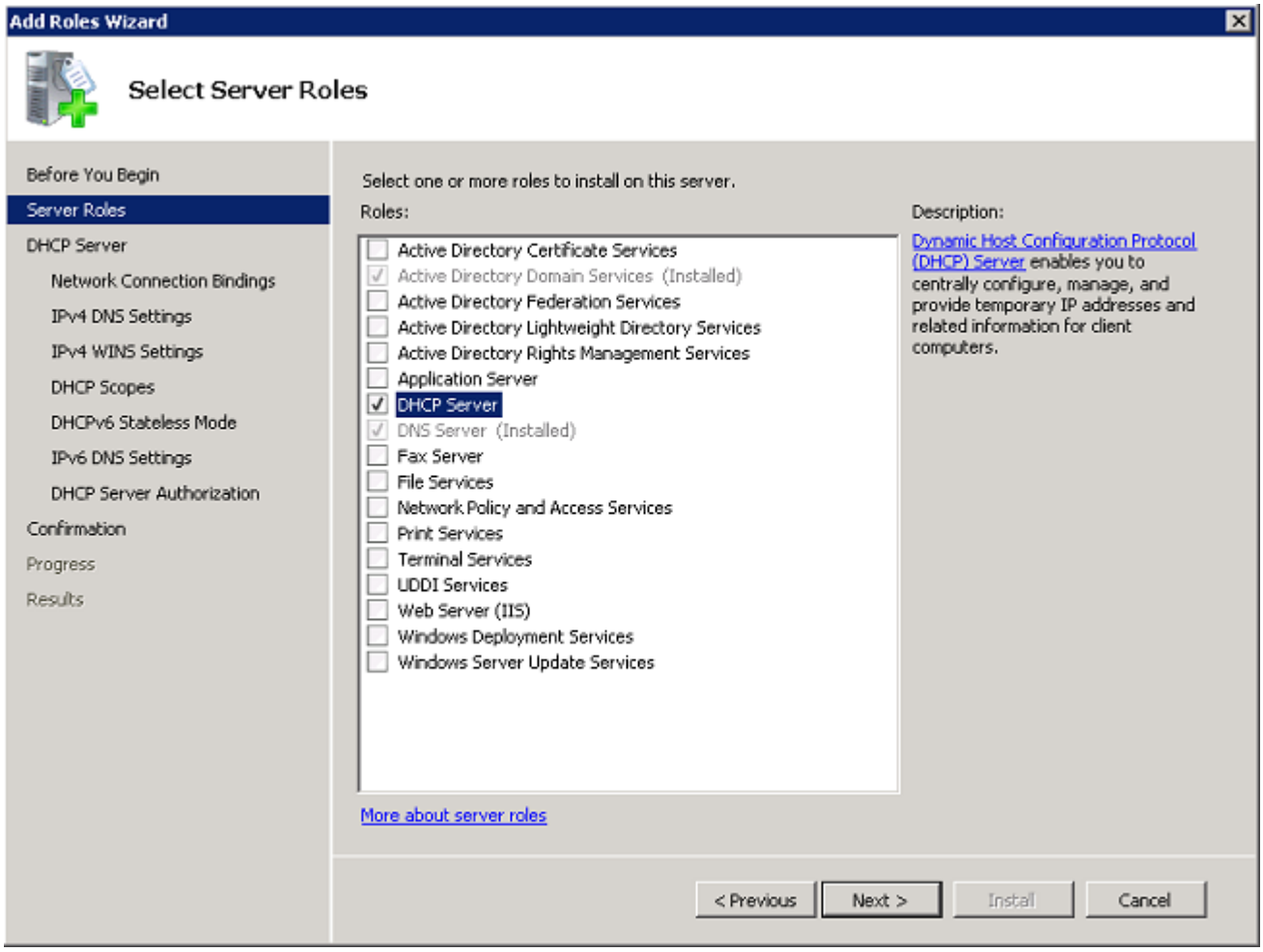
2. Cliquez sur Rôles> Ajouter des rôles.



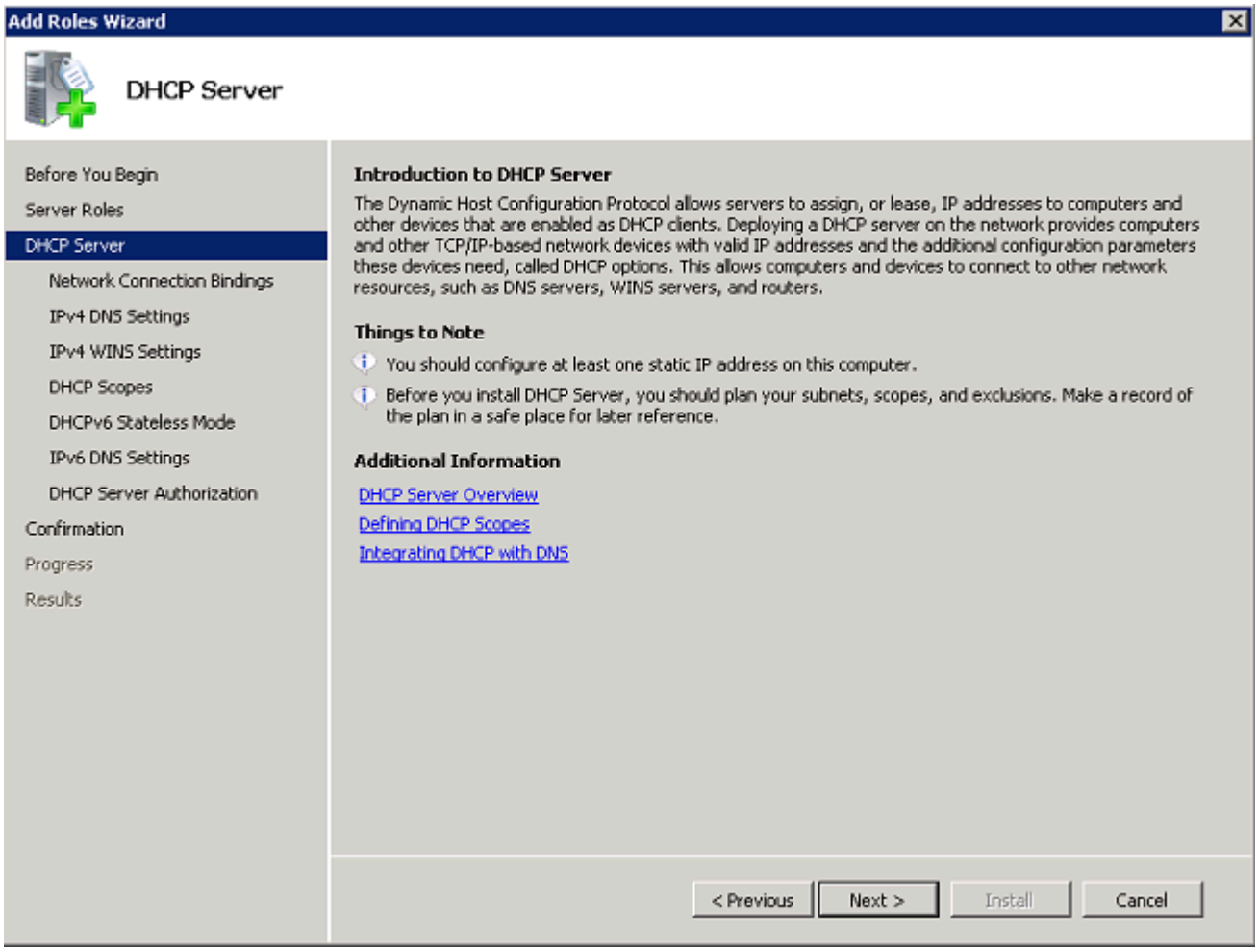
3. Cliquez sur Next (Suivant).



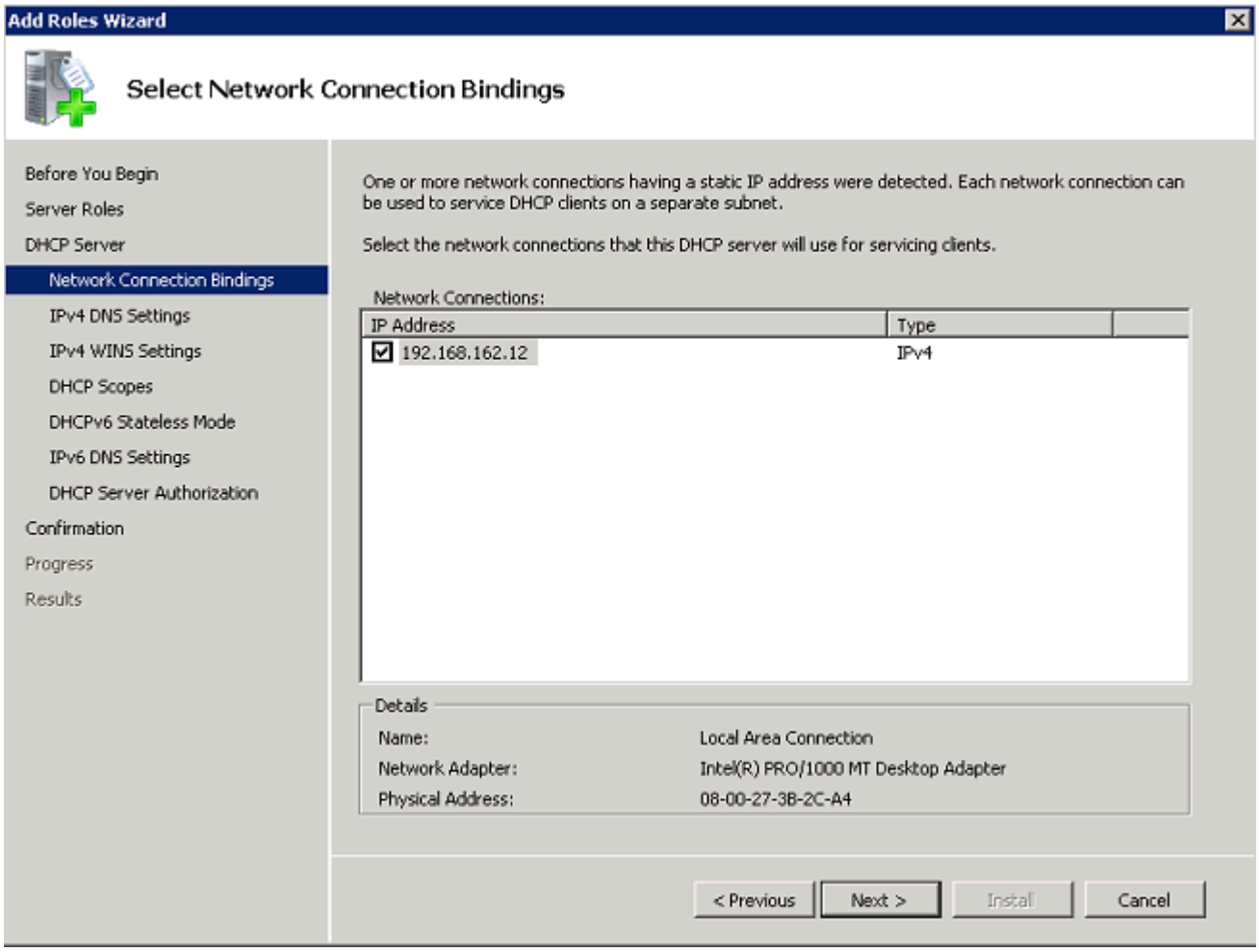
4. Sélectionnez le service DHCP Server, puis cliquez sur Next.



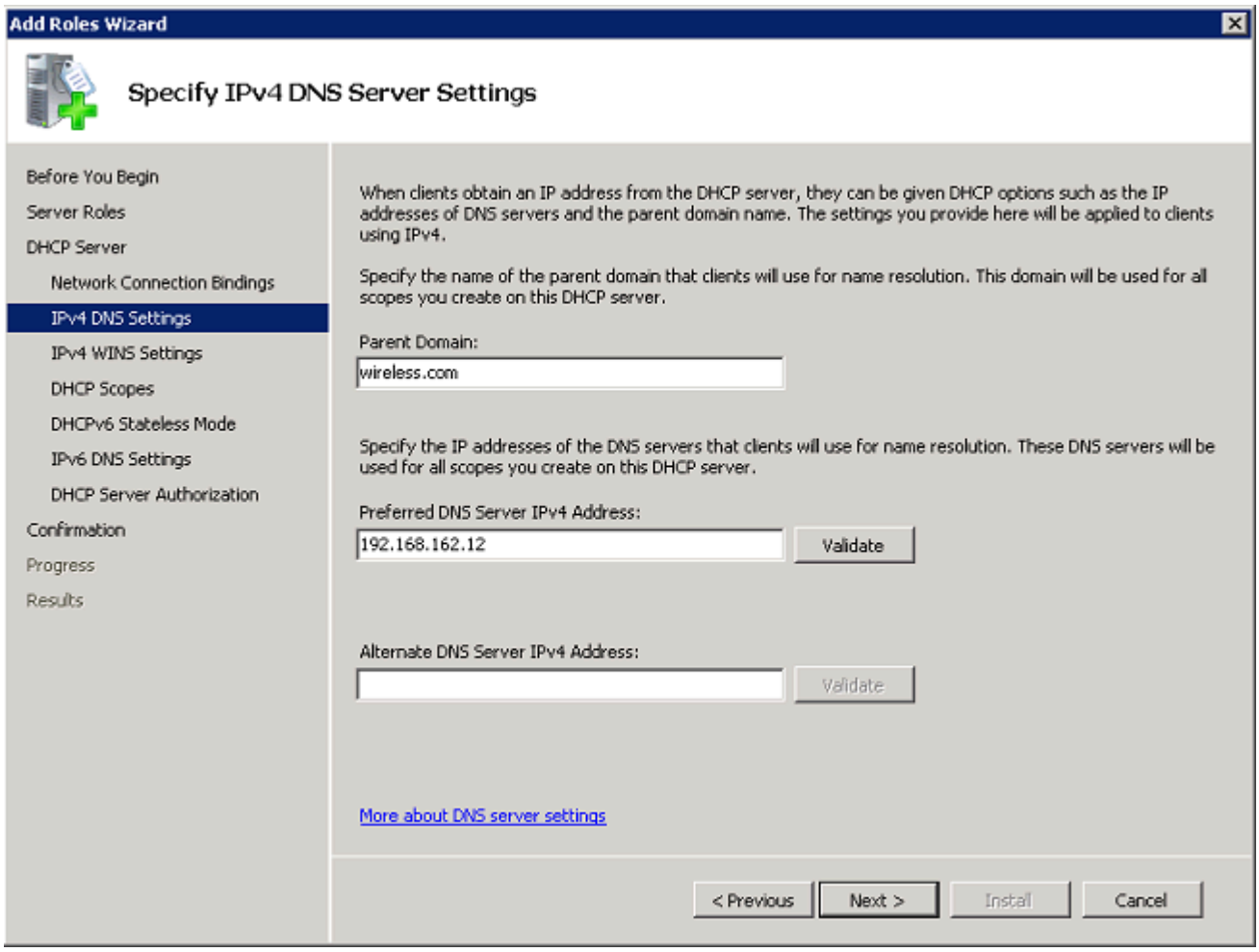
5. Reportez-vous à la section Introduction to DHCP Server, puis cliquez sur Next.



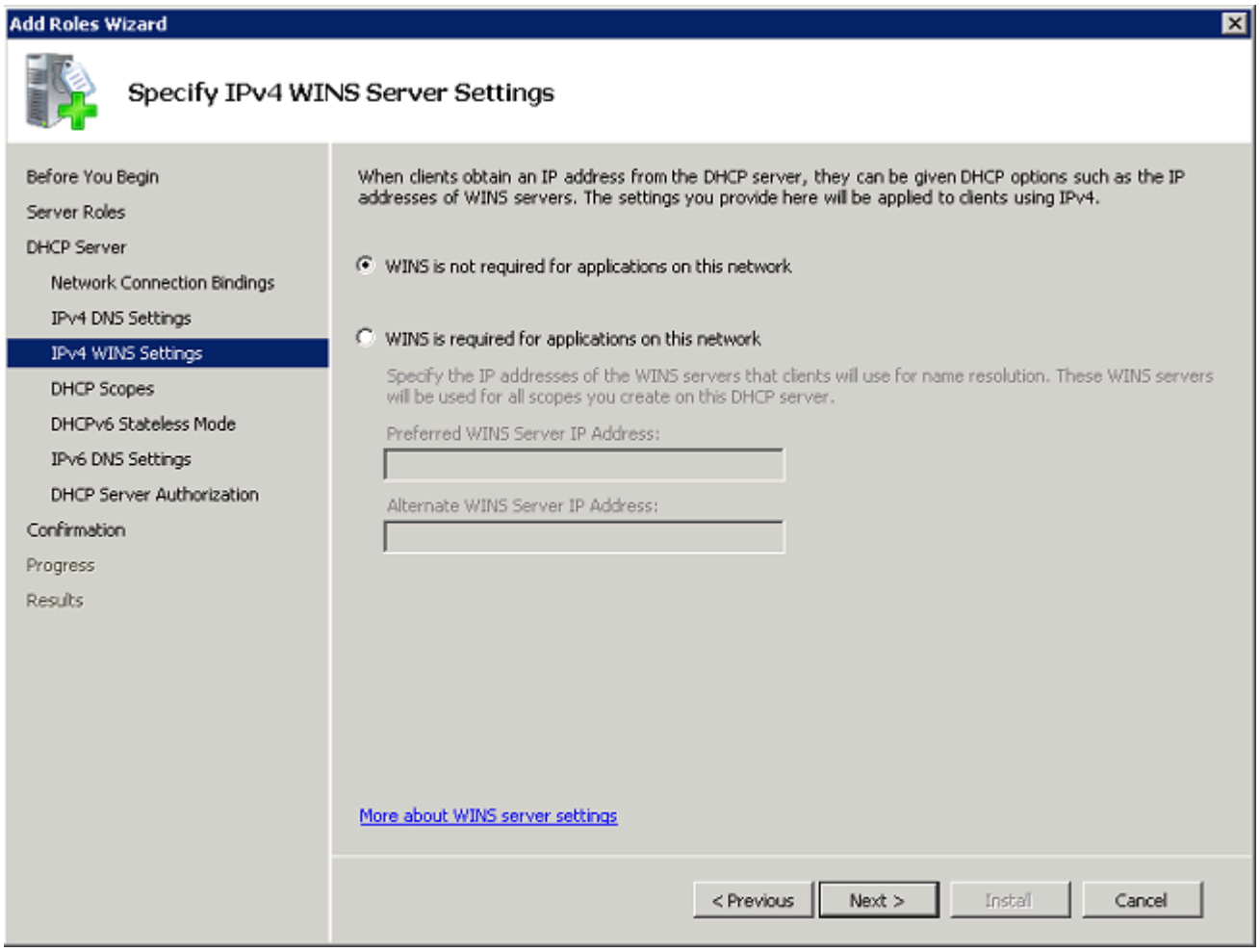
6. Sélectionnez l'interface que le serveur DHCP doit surveiller pour les demandes, et cliquez sur Next.



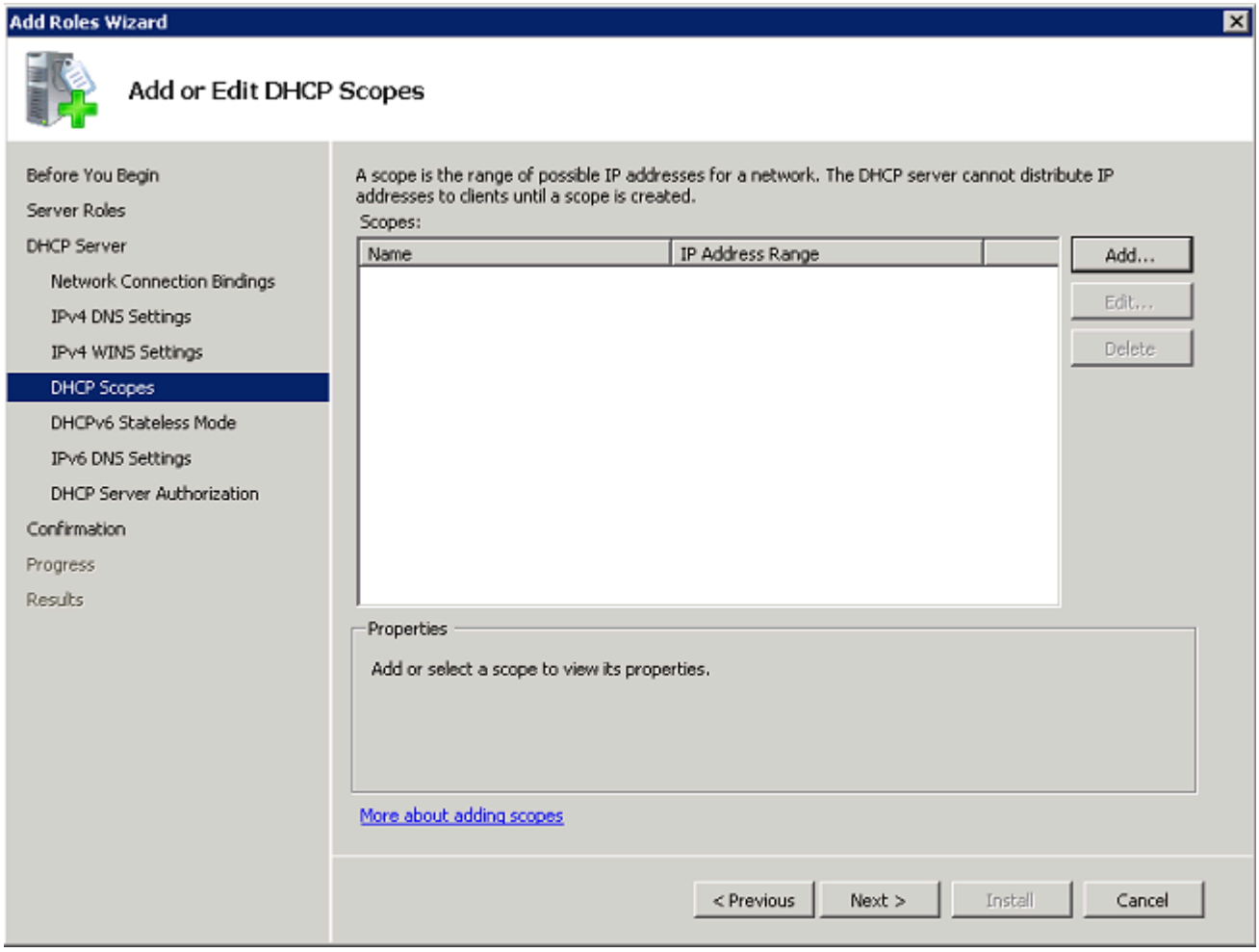
7. Configurez les paramètres DNS par défaut que le serveur DHCP doit fournir aux clients, puis cliquez sur Next.



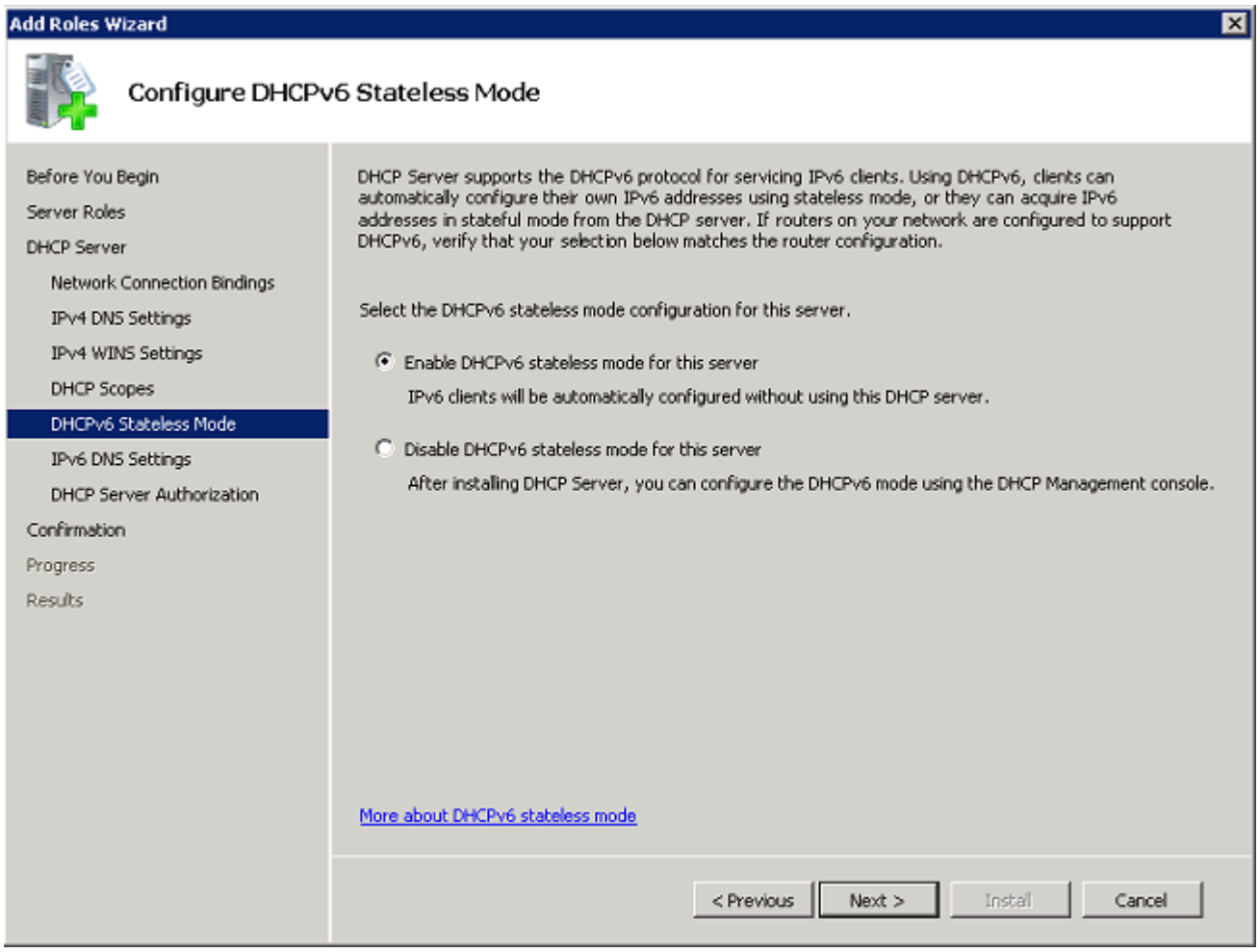
8. Configurez WINS si le réseau prend en charge WINS.



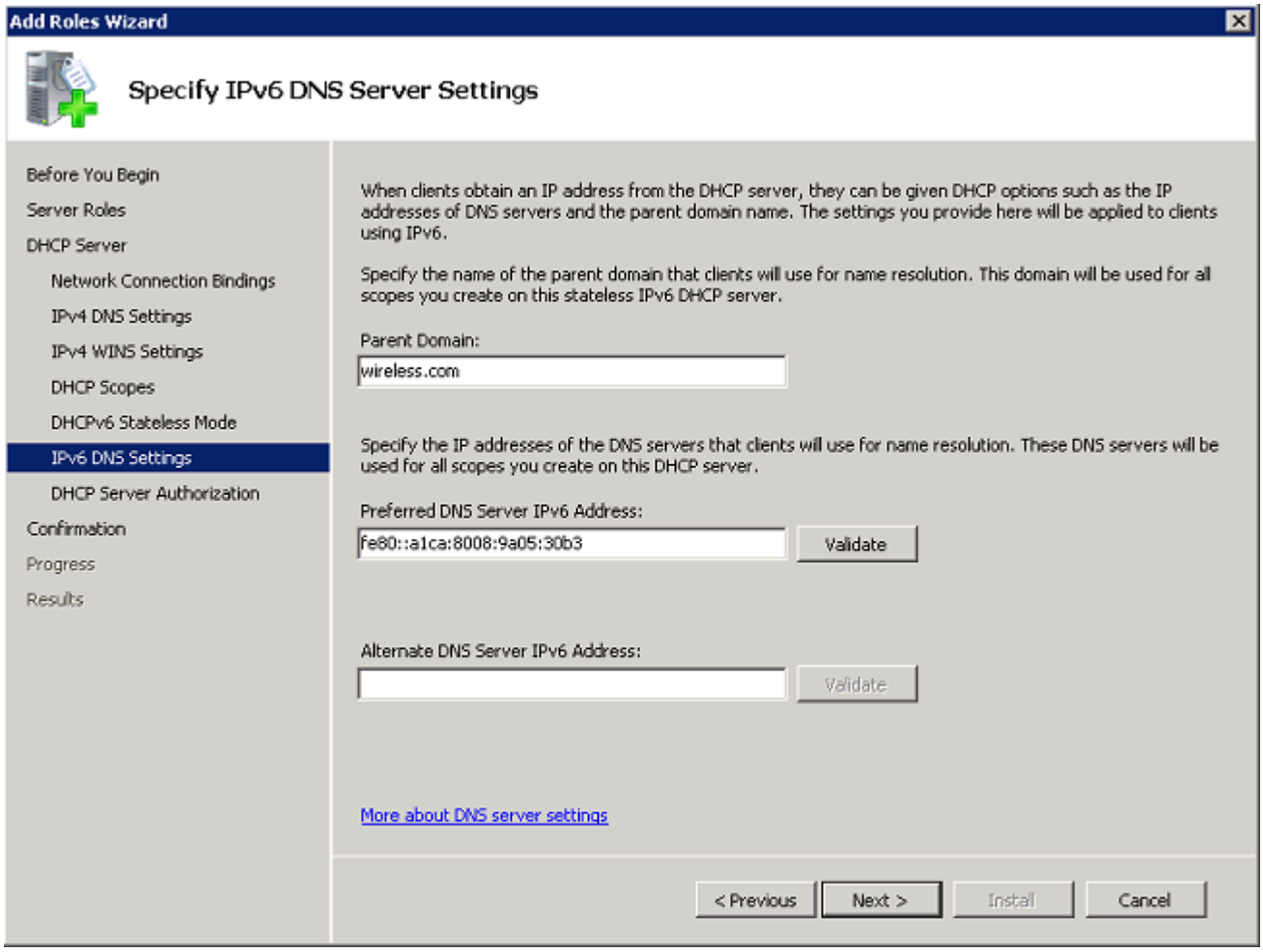
9. Cliquez sur Add pour utiliser l'assistant pour créer une étendue DHCP ou cliquez sur Next pour créer une étendue DHCP ultérieurement. Cliquez sur Next pour continuer.



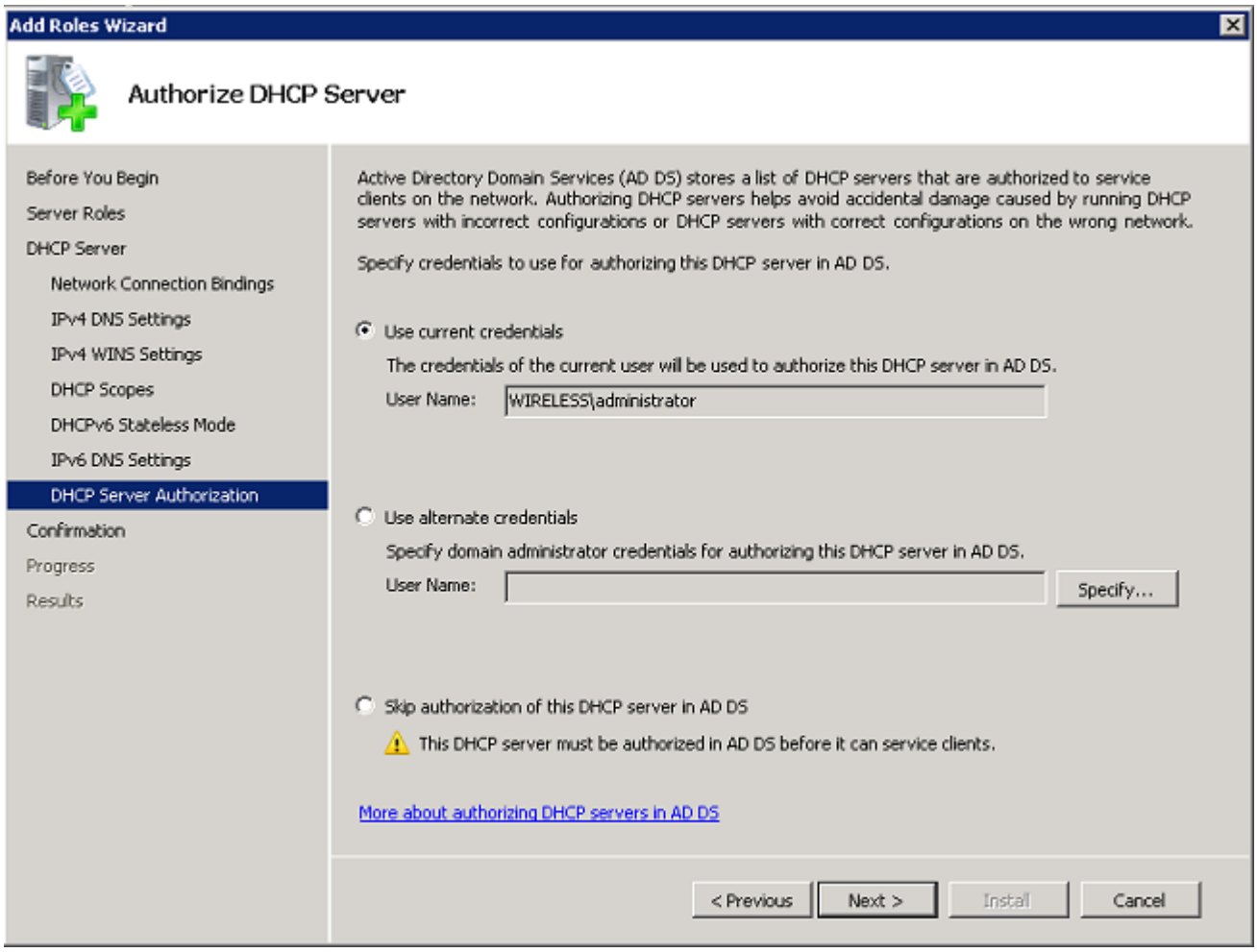
10. Activez ou désactivez la prise en charge DHCPv6 sur le serveur, puis cliquez sur Next.



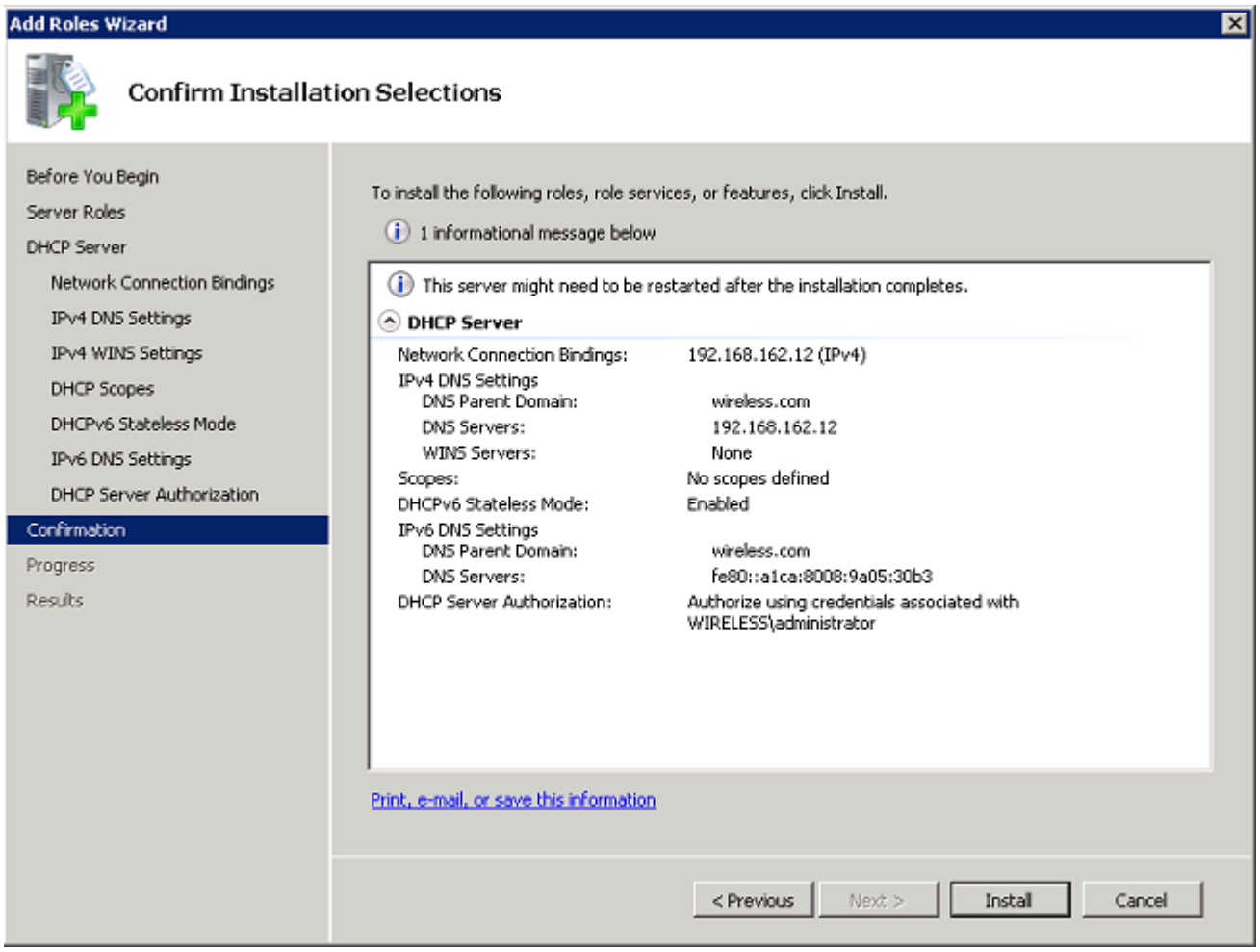
11. Configurez les paramètres DNS IPv6 si DHCPv6 a été activé à l'étape précédente. Cliquez sur Next pour continuer.



12. Fournissez des informations d'identification d'administrateur de domaine pour autoriser le serveur DHCP dans Active Directory, puis cliquez sur Next.

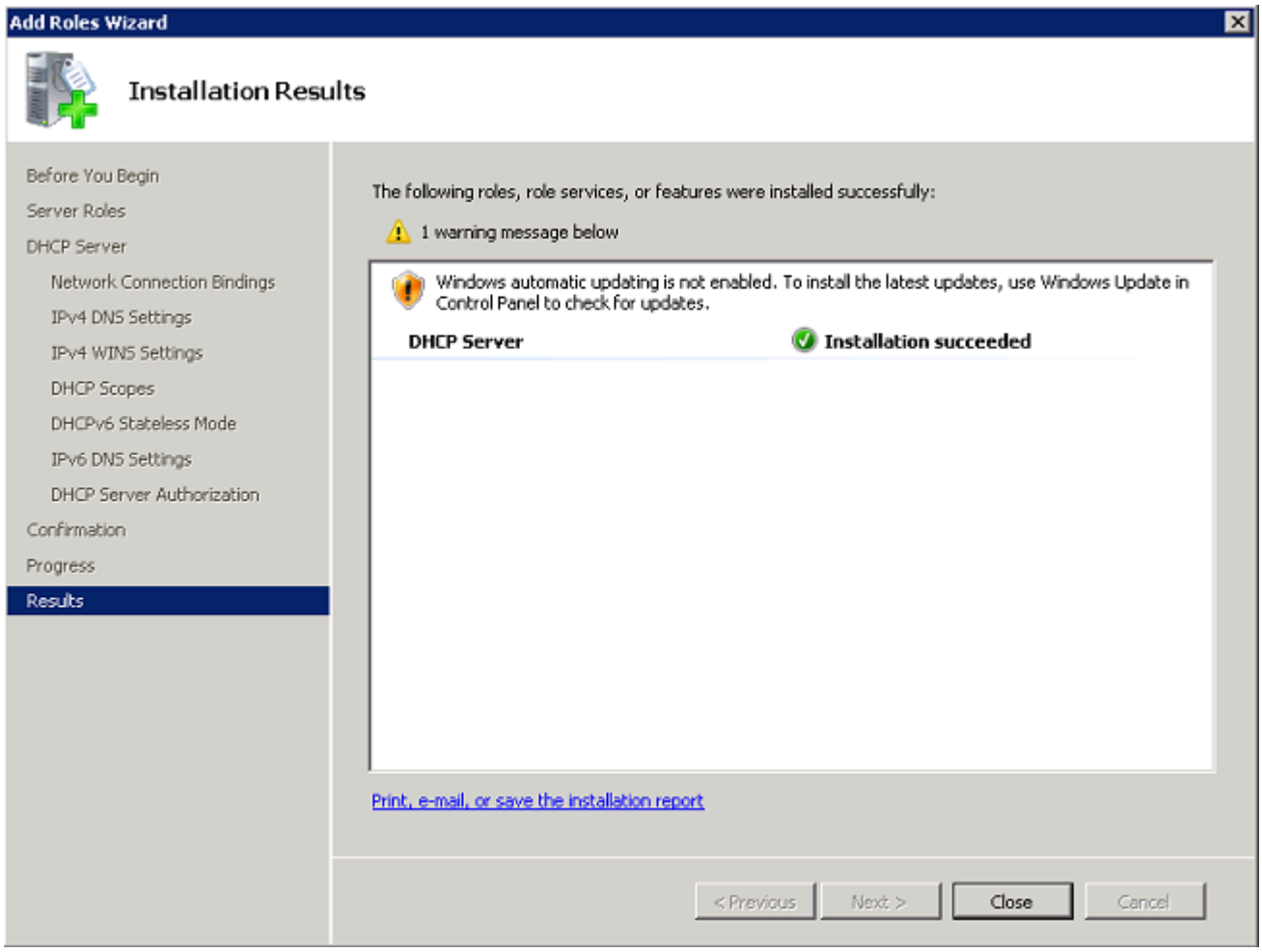


13. Vérifiez la configuration sur la page de confirmation, et cliquez sur Install pour terminer l'installation.



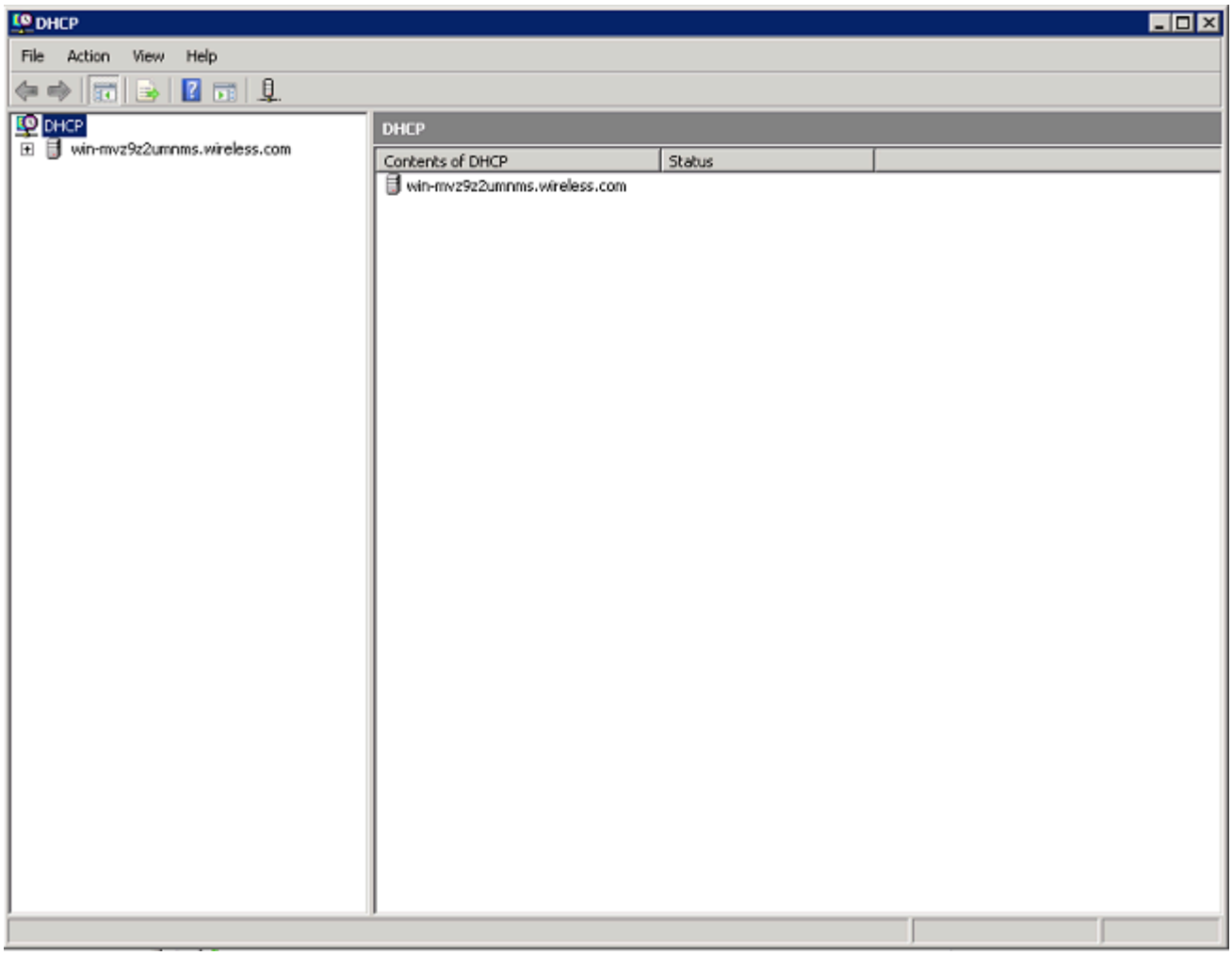
L'installation se poursuit.

14. Cliquez sur Fermer pour fermer l'Assistant.

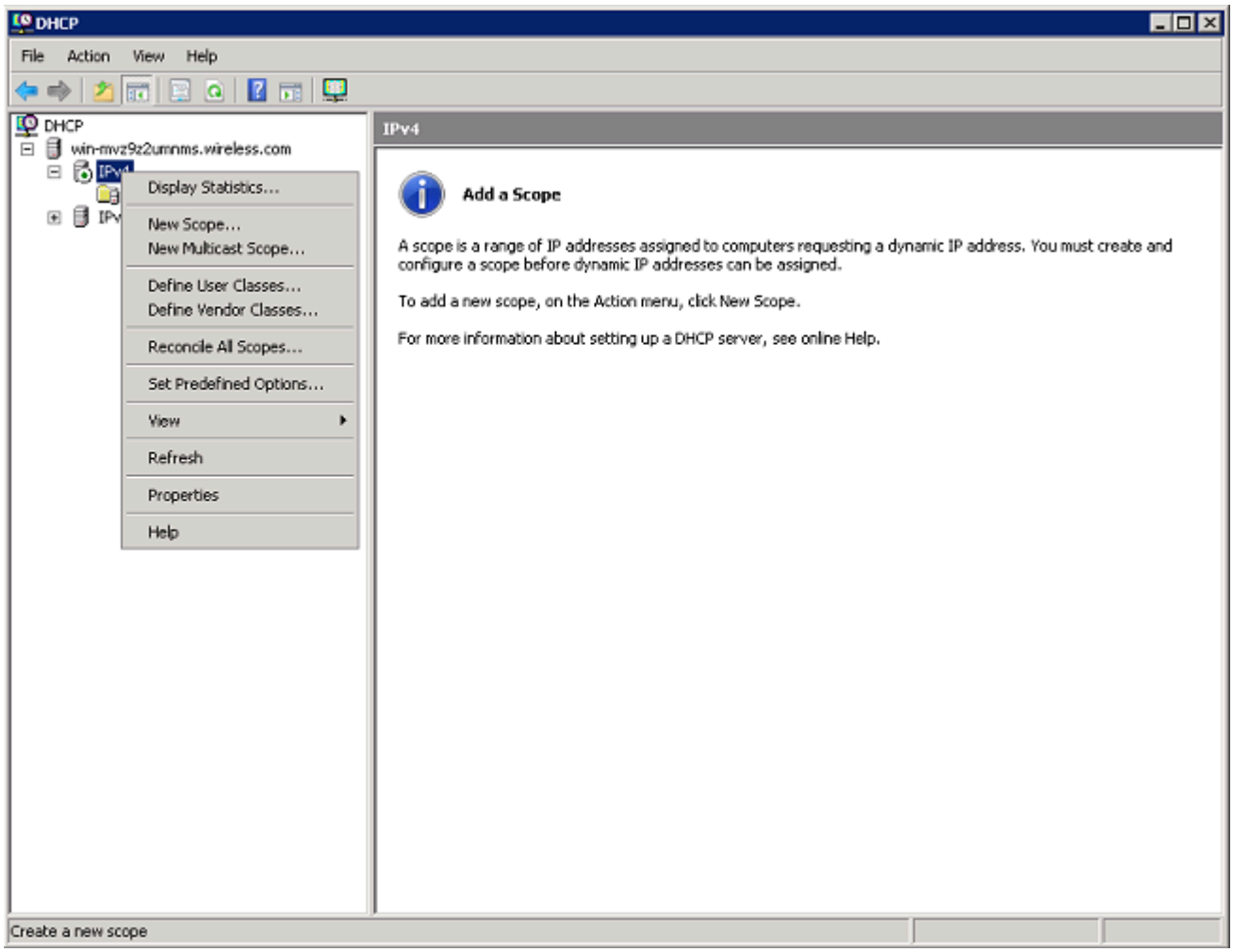


Le serveur DHCP est maintenant installé.

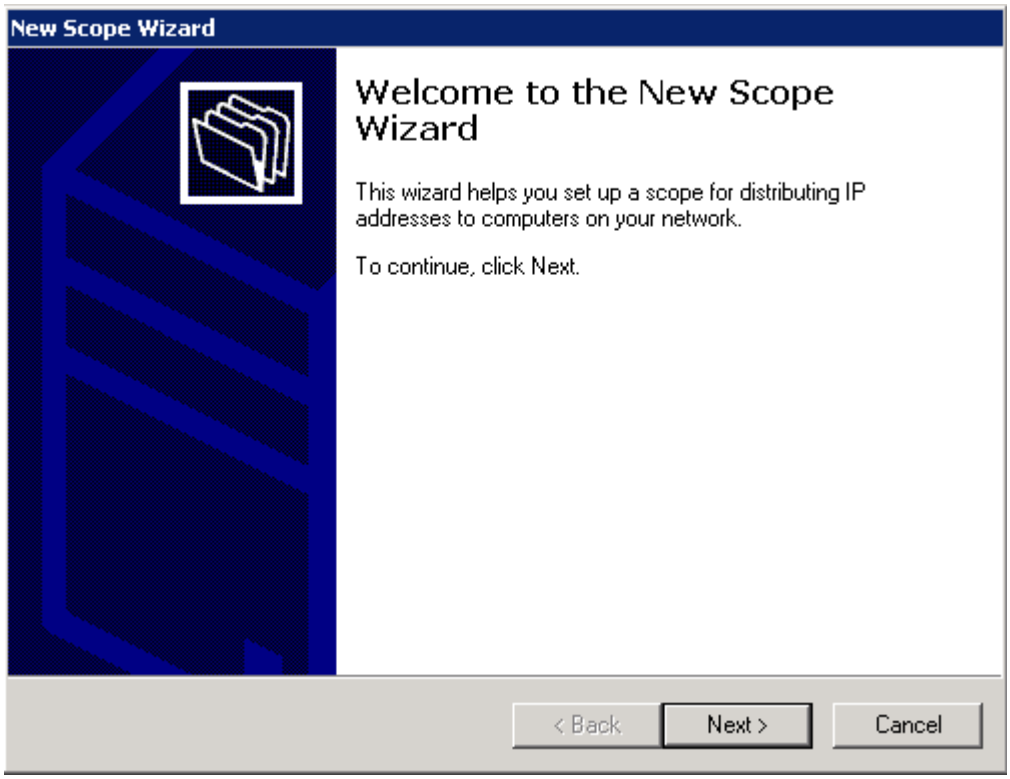
15. Cliquez sur Start > Administrative Tools > DHCP pour configurer le service DHCP.



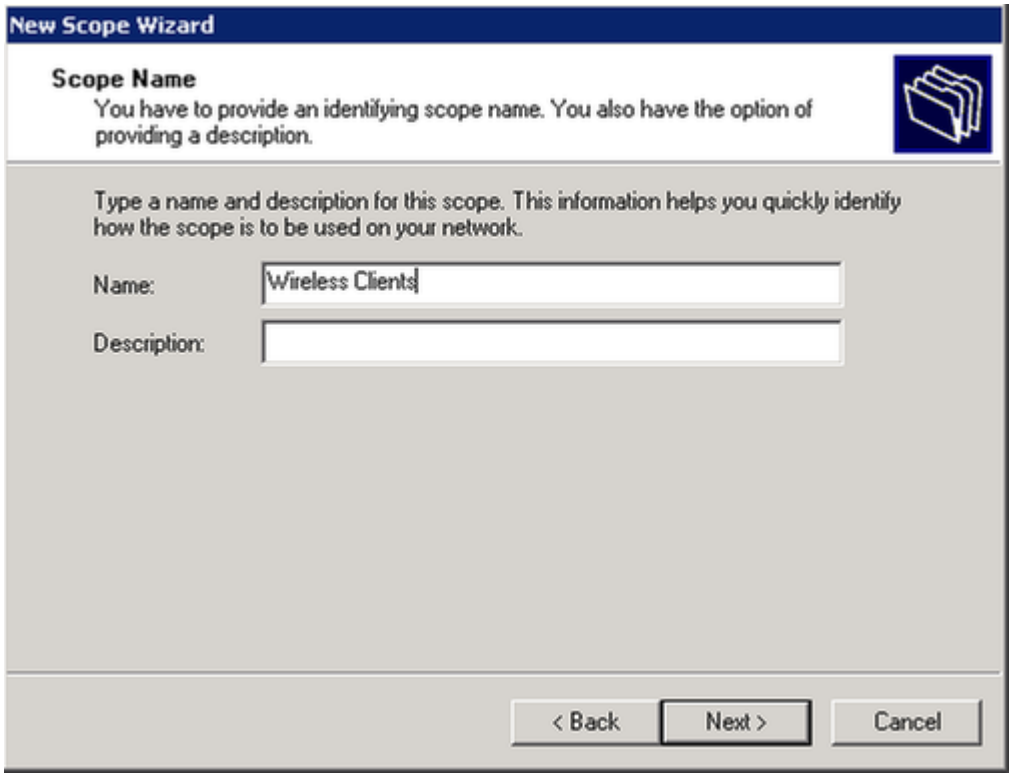
16. Développez le serveur DHCP (illustré dans l'image précédente pour cet exemple), cliquez avec le bouton droit sur IPv4 et choisissez New Scope pour créer une étendue DHCP.



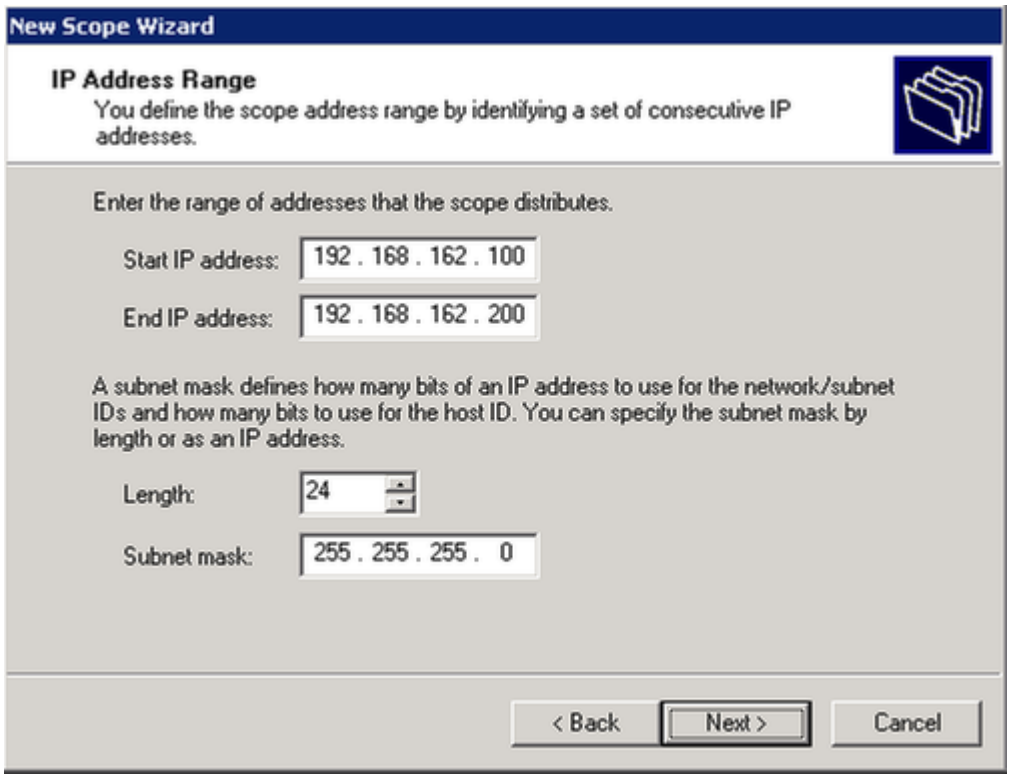
17. Cliquez sur Next pour configurer la nouvelle étendue via l'Assistant Nouvelle étendue.



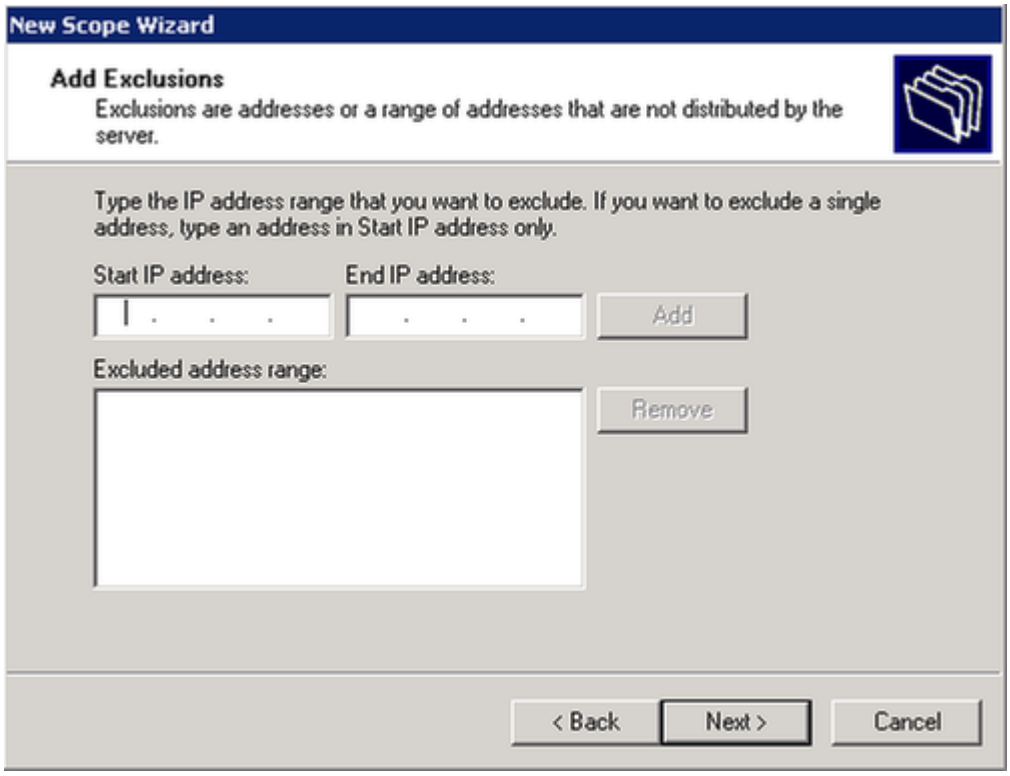
18. Entrez un nom pour la nouvelle étendue (Clients sans fil dans cet exemple), puis cliquez sur Next.



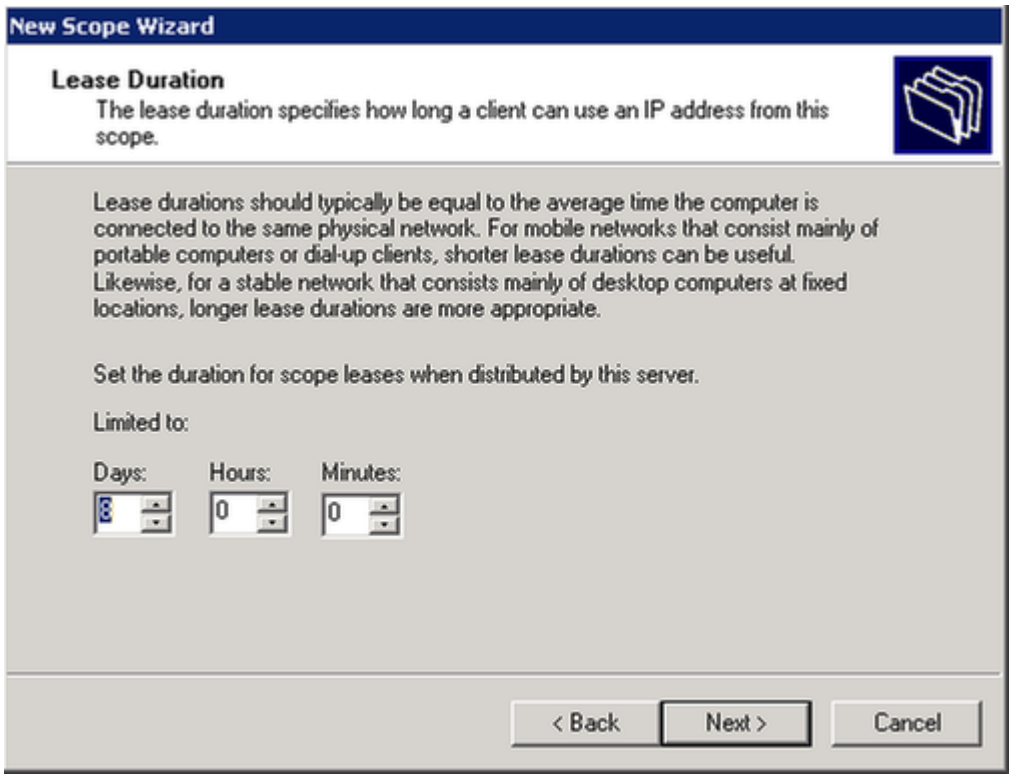
19. Saisissez la plage d'adresses IP disponibles pouvant être utilisée pour les baux DHCP. Cliquez sur Next pour continuer.



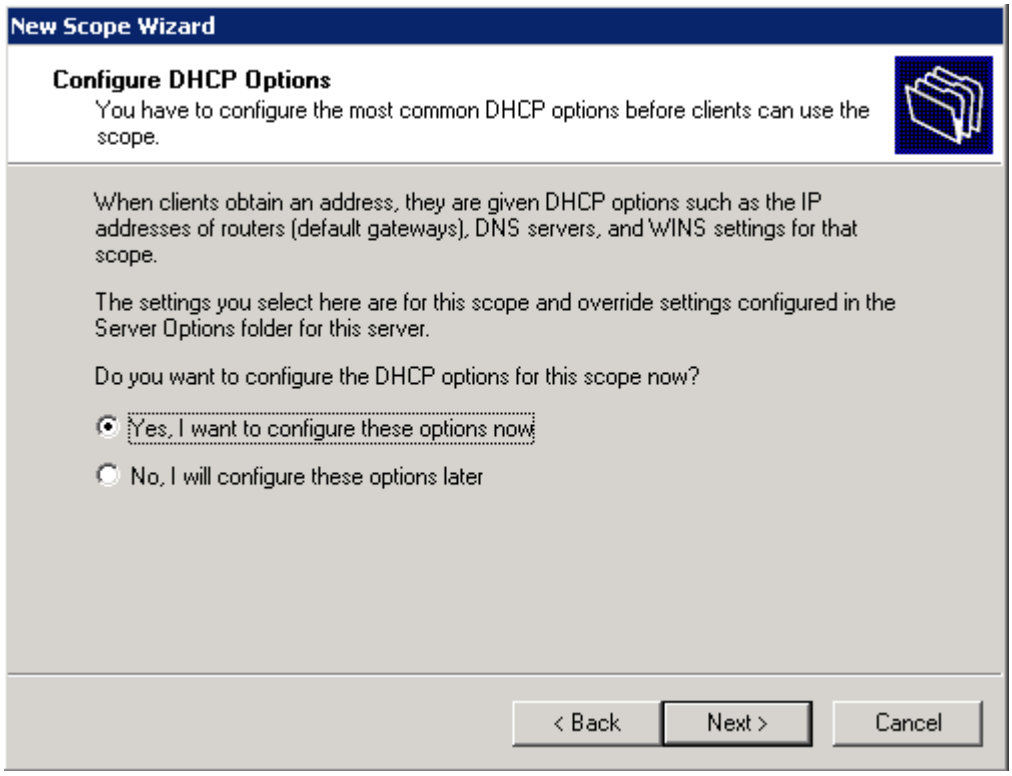
20. Créez une liste facultative d'adresses exclues. Cliquez sur Next pour continuer.



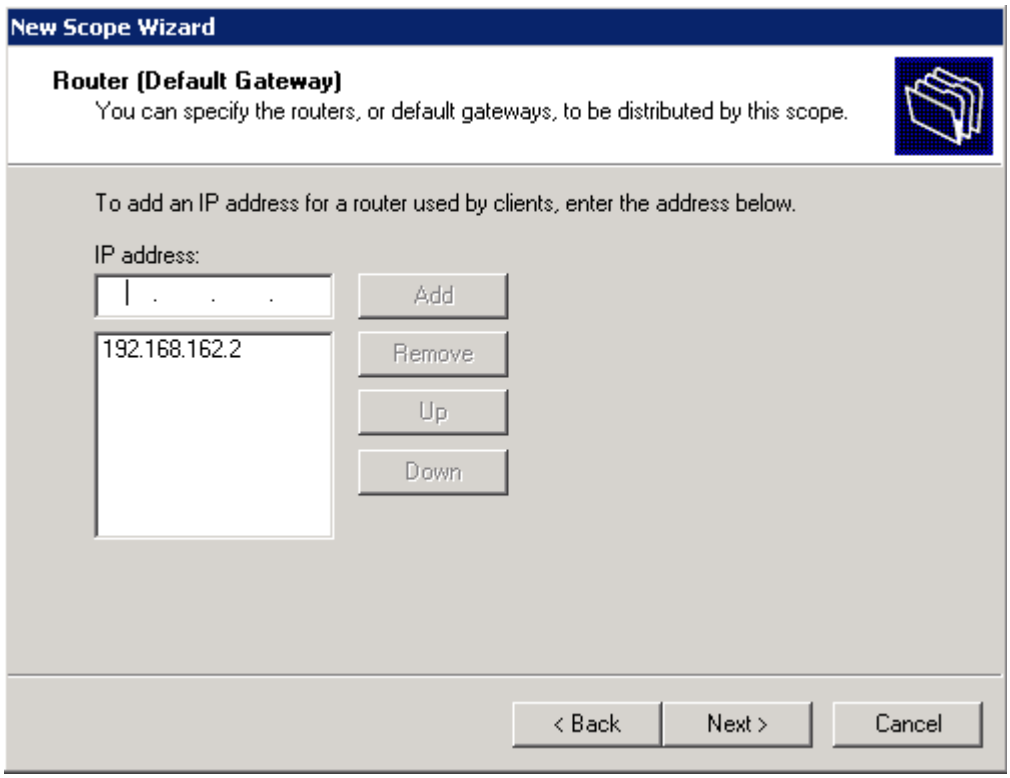
21. Configurez la durée du bail, puis cliquez sur Next.



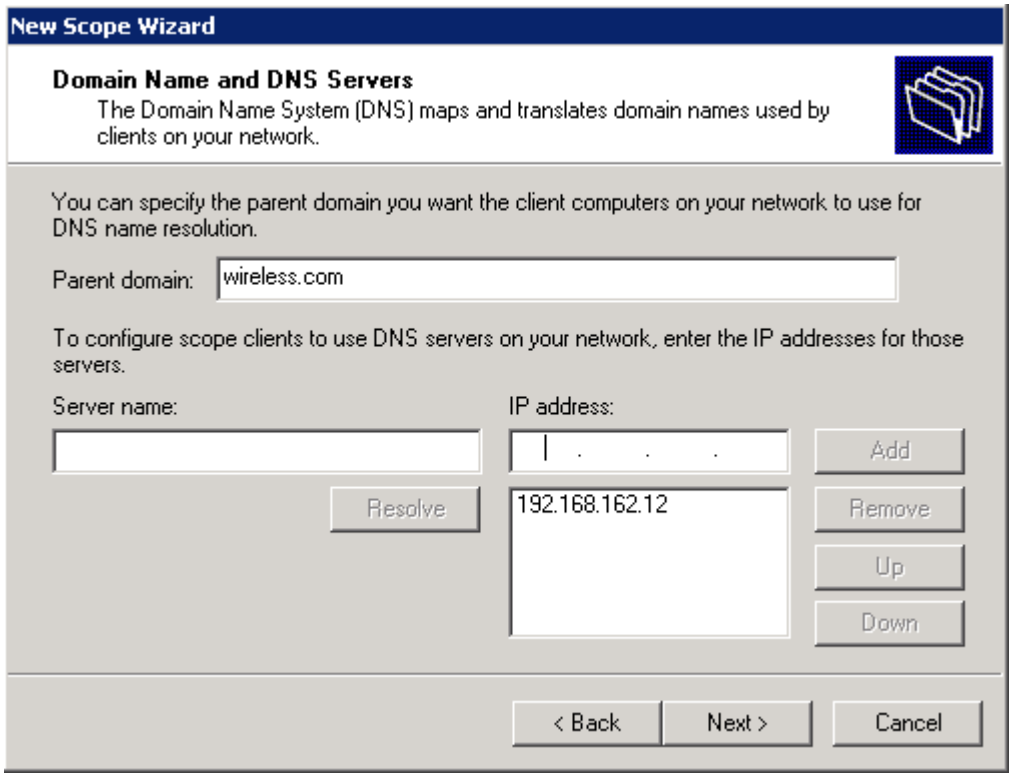
22. Cliquez sur Yes, I want to configure these options now, puis sur Next.



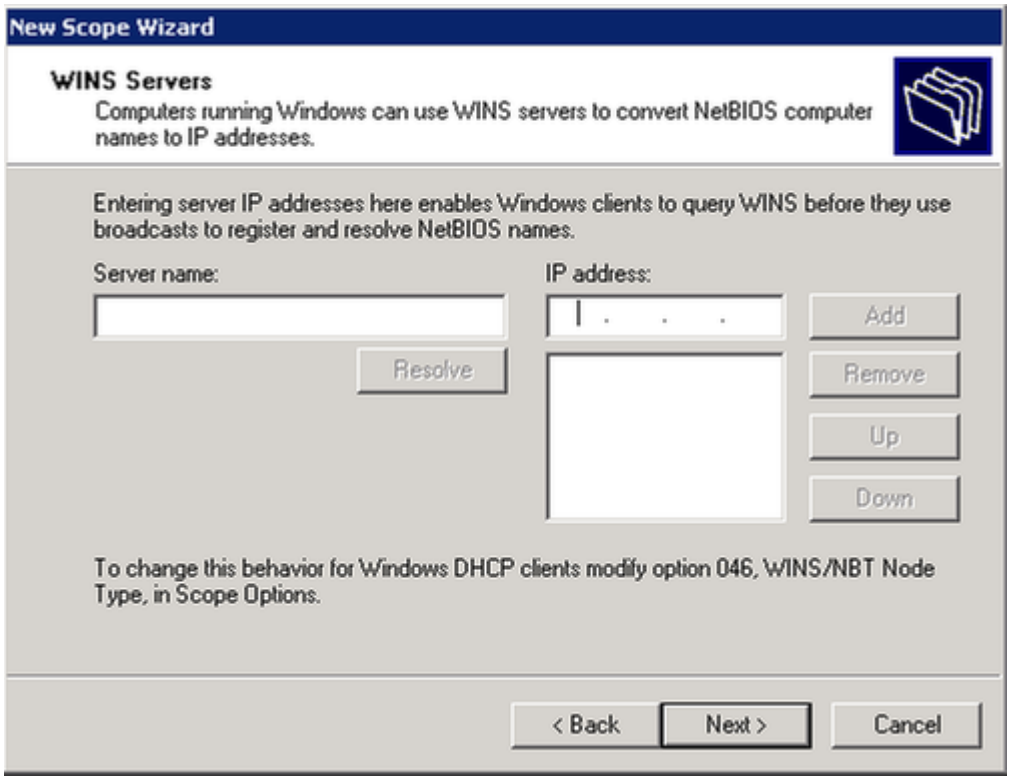
23. Entrez l'adresse IP de la passerelle par défaut pour cette étendue, cliquez sur Add > Next.



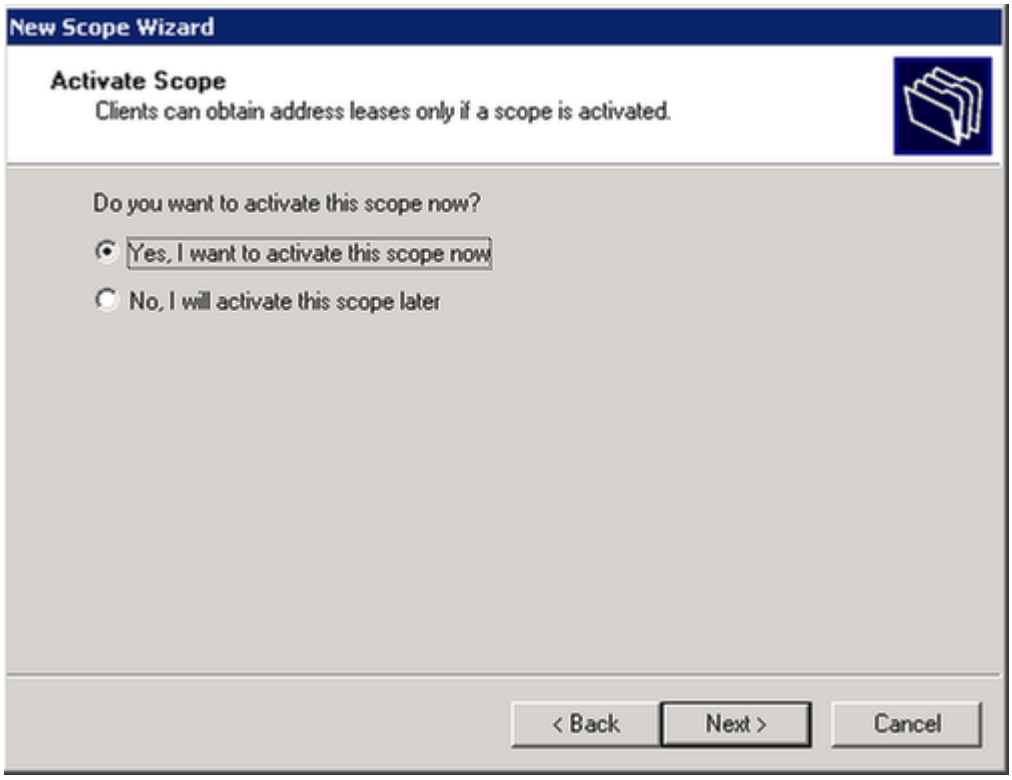
24. Configurez le nom de domaine DNS et le serveur DNS à utiliser par les clients. Cliquez sur Next pour continuer.



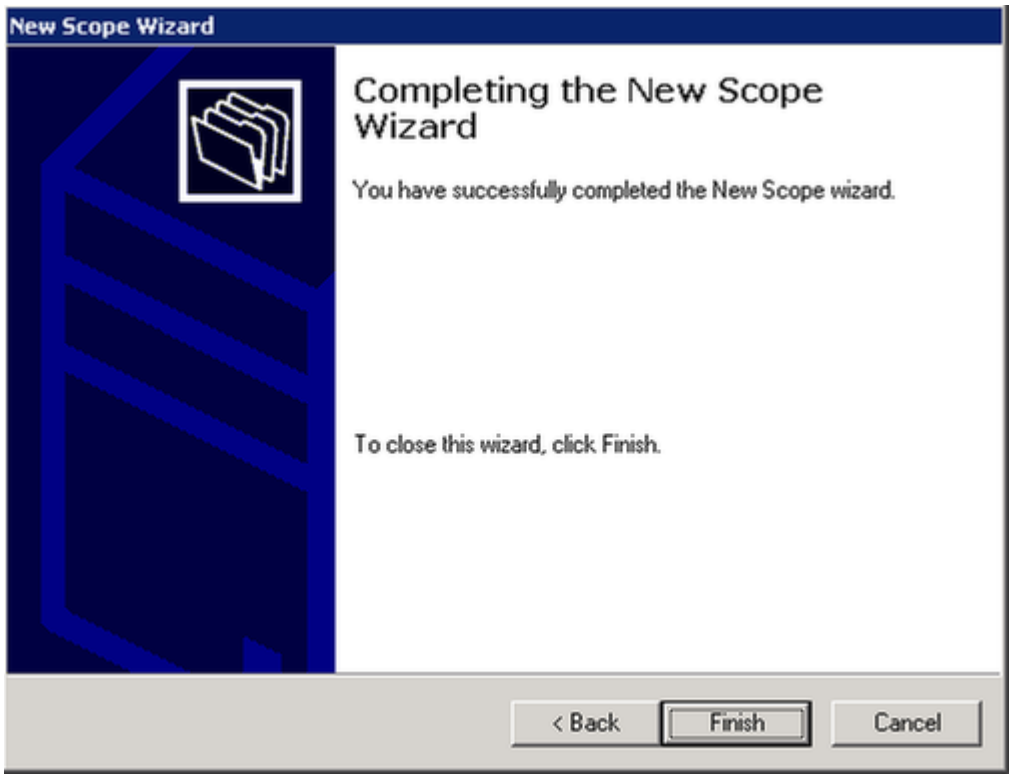
25. Entrez les informations WINS pour cette étendue si le réseau prend en charge WINS. Cliquez sur Next pour continuer.



26. Pour activer cette étendue, cliquez sur Oui, je veux activer cette étendue maintenant> Suivant.



27. Cliquez sur Terminer pour terminer et fermer l'Assistant.

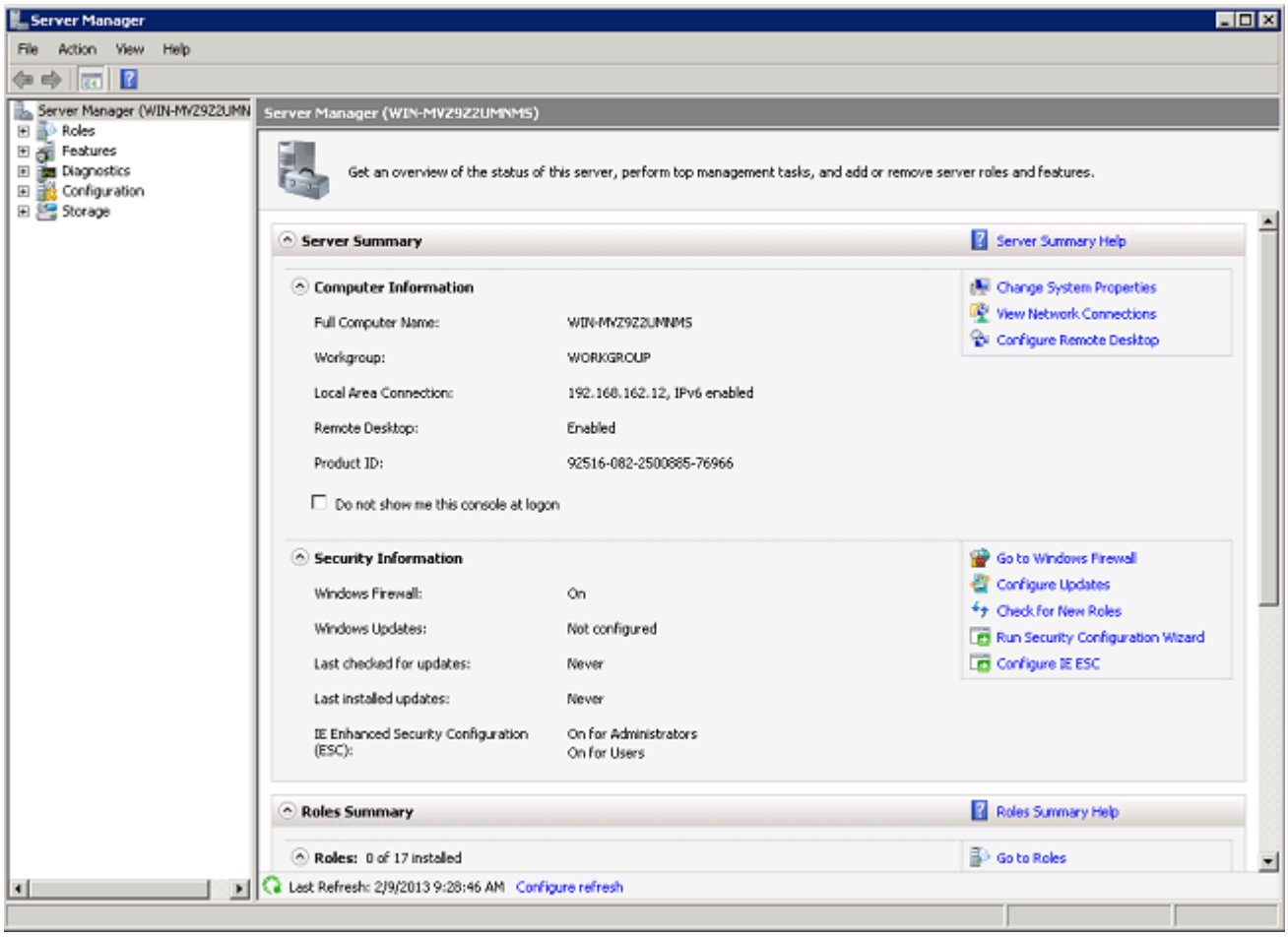


Installation et configuration de Microsoft Windows 2008 Server en tant que serveur AC

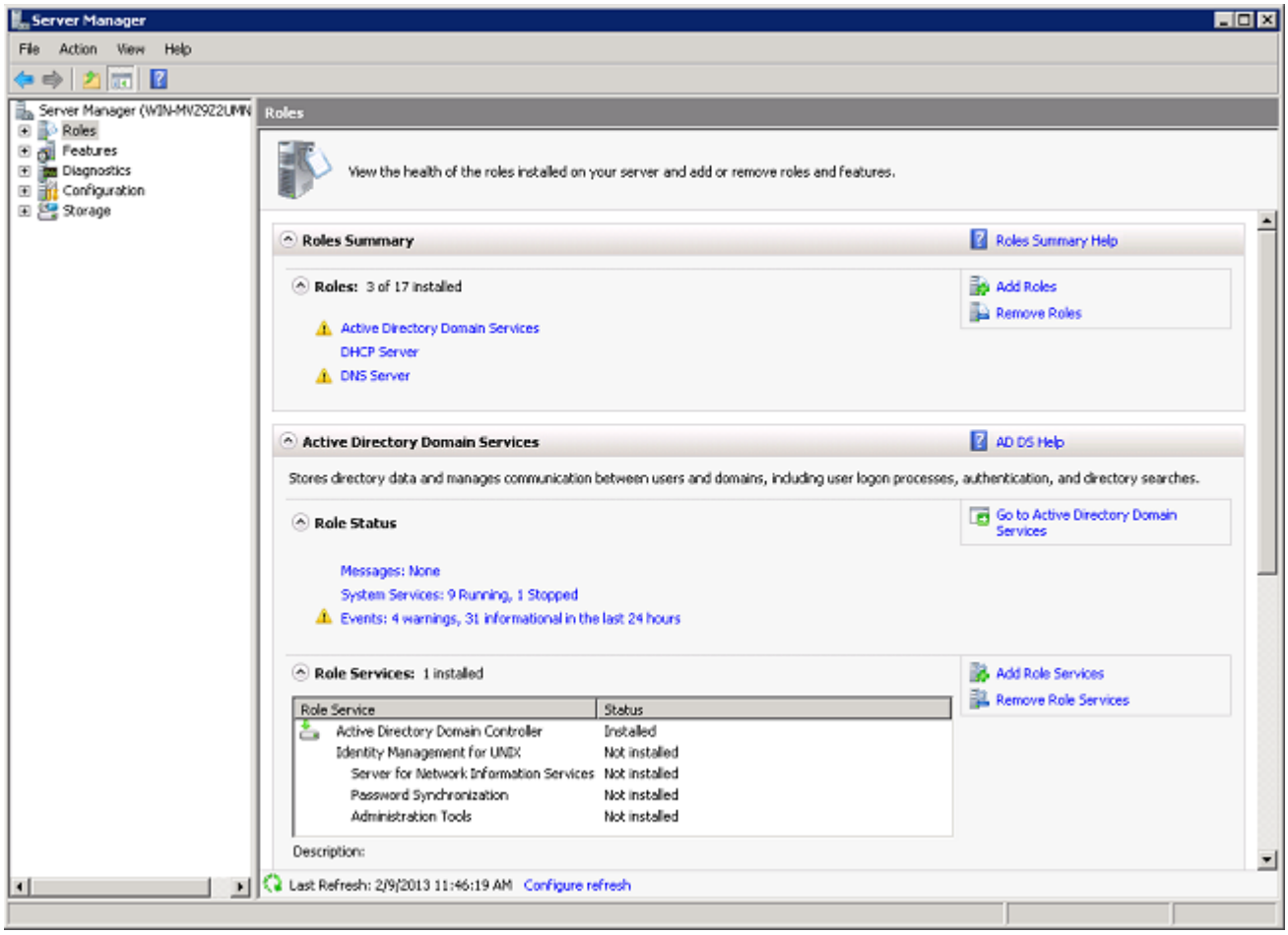
PEAP avec EAP-MS-CHAP v2 valide le serveur RADIUS en fonction du certificat présent sur le serveur. En outre, le certificat du serveur doit être émis par une autorité de certification publique approuvée par l'ordinateur client (c'est-à-dire que le certificat de l'autorité de certification publique existe déjà dans le dossier Trusted Root Certification Authority du magasin de certificats de l'ordinateur client).

Complétez ces étapes afin de configurer le serveur Microsoft Windows 2008 en tant que serveur AC qui émet le certificat vers le NPS :

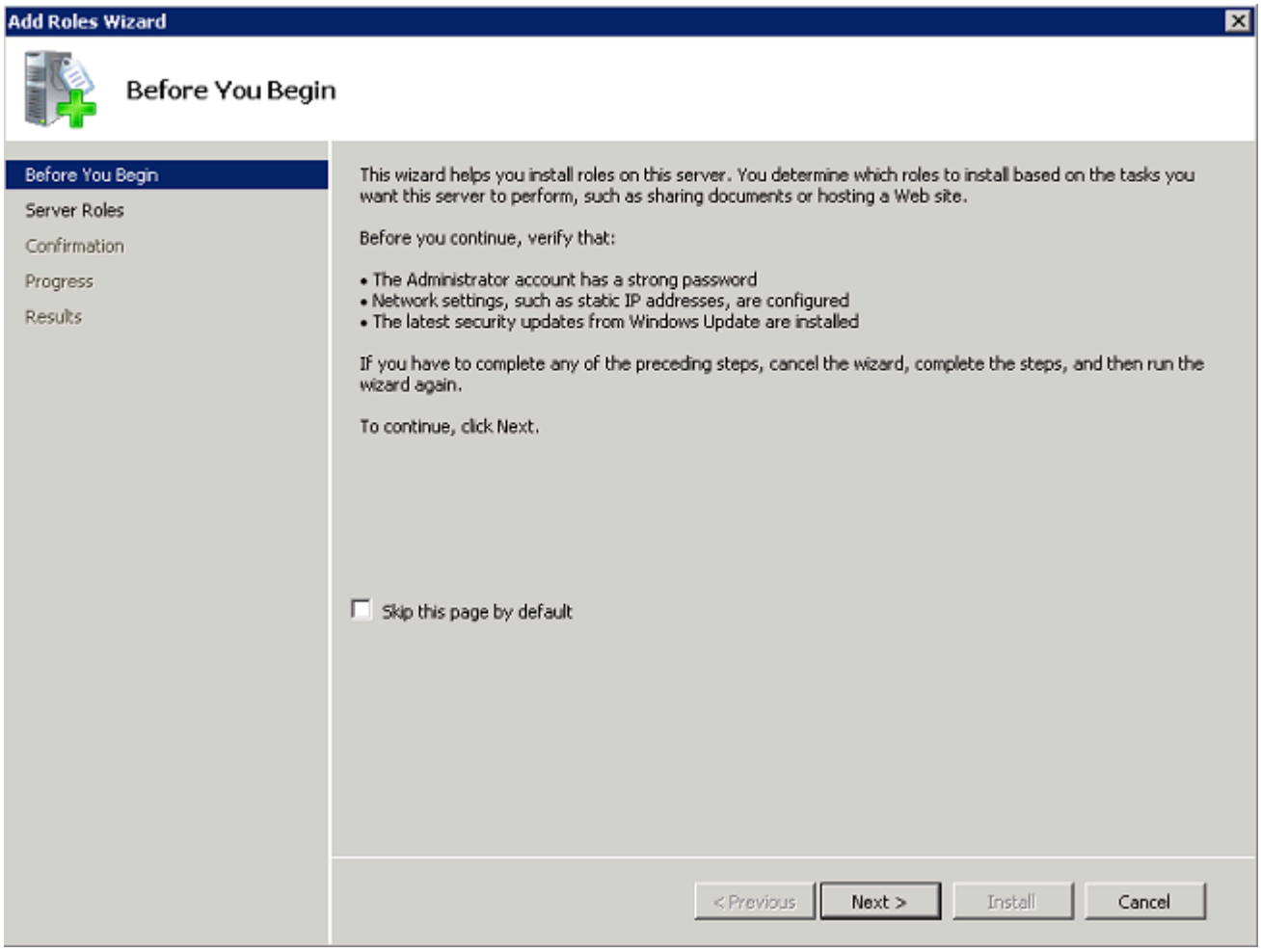
1. Cliquez sur Démarrer> Gestionnaire de serveur.



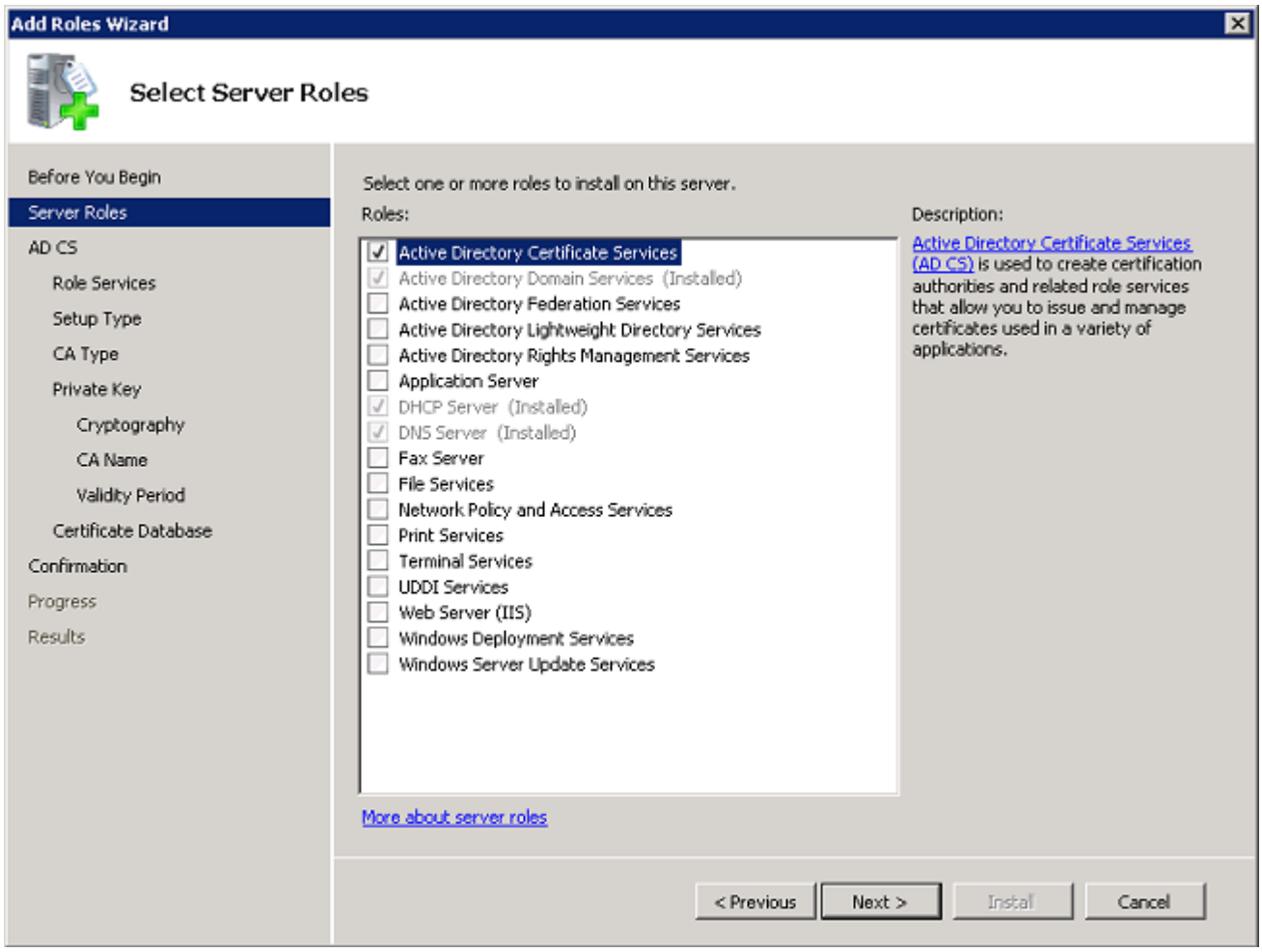
2. Cliquez sur Rôles> Ajouter des rôles.



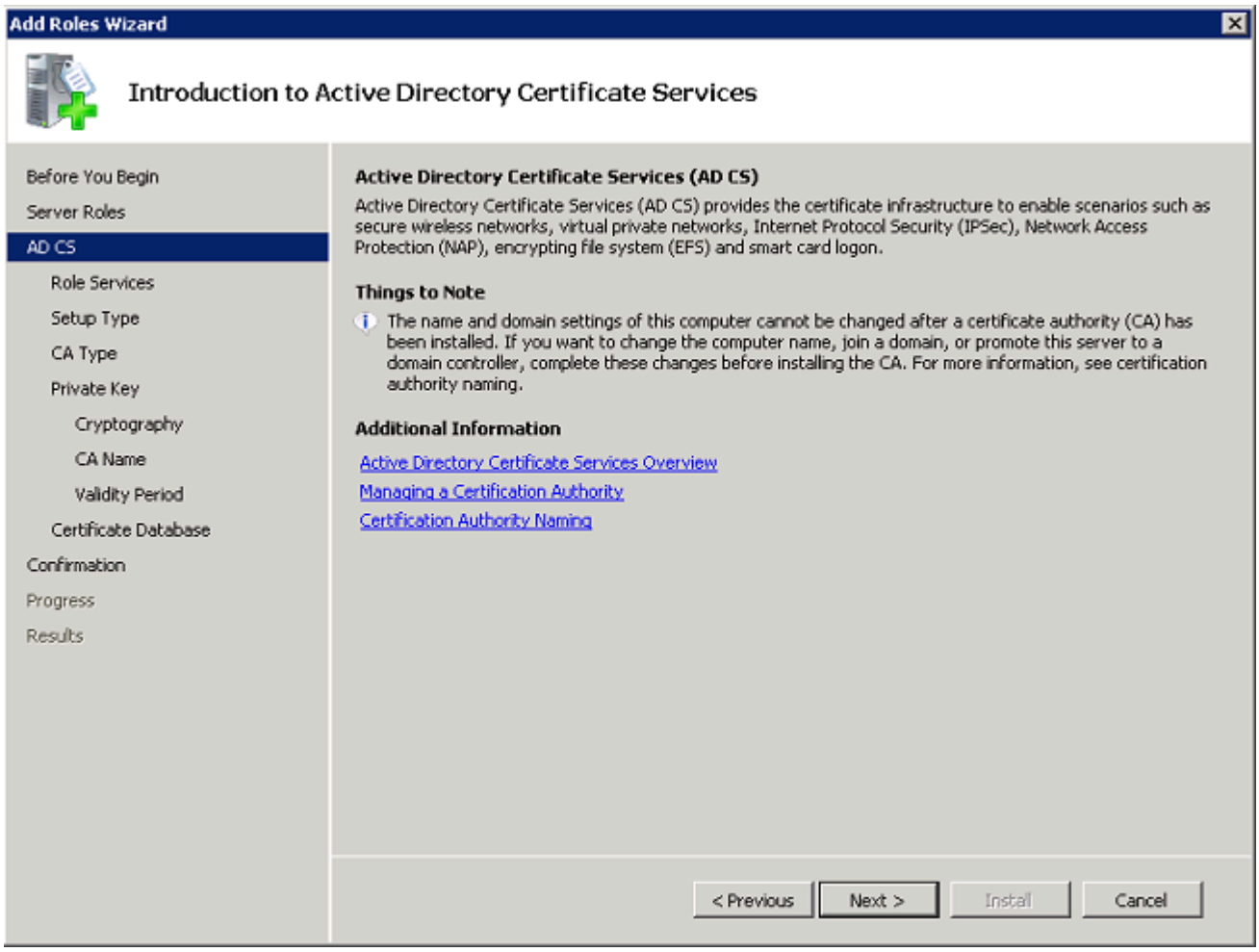
3. Cliquez sur Next (Suivant).



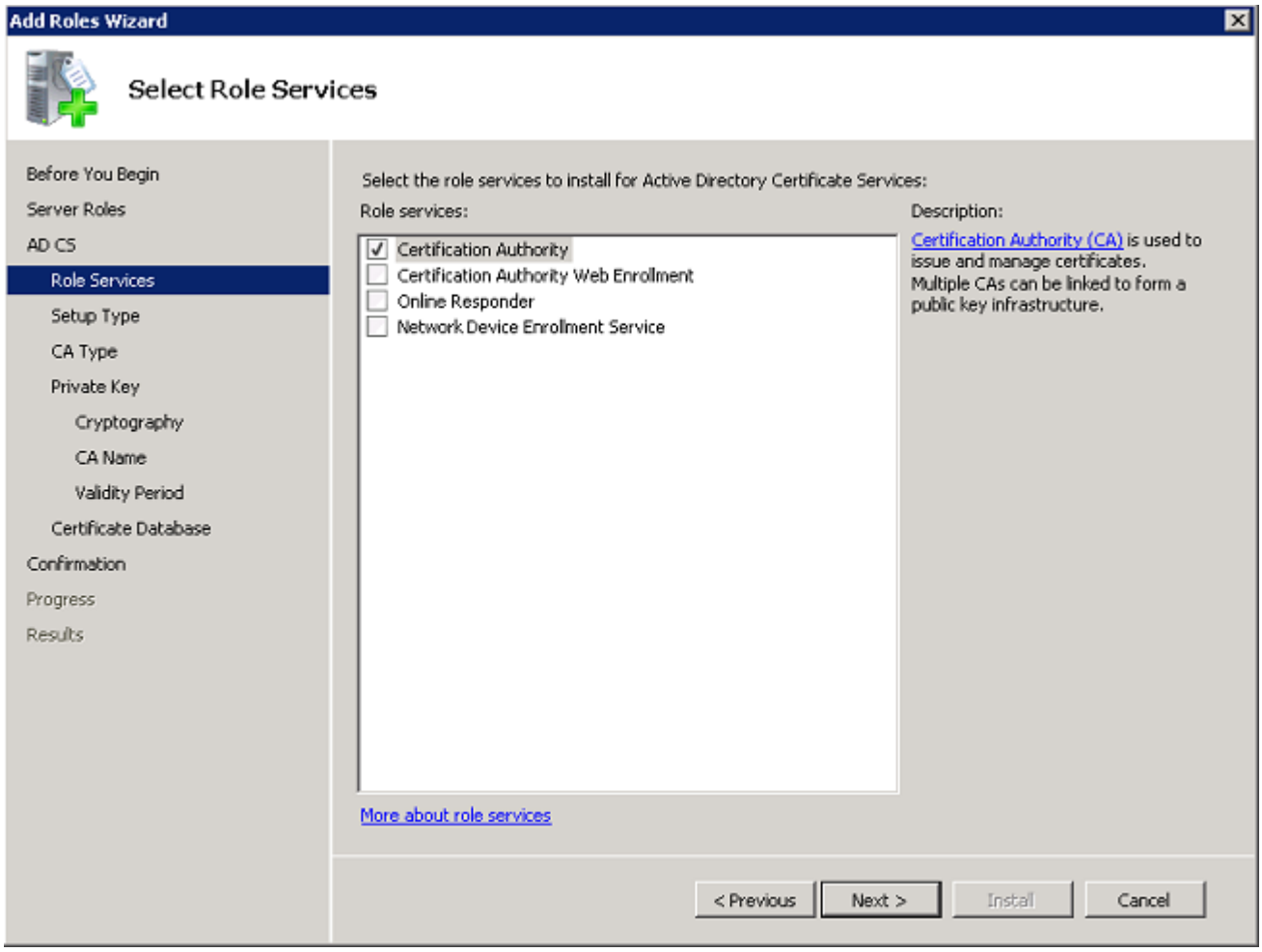
4. Sélectionnez le service Services de certificats Active Directory, puis cliquez sur Suivant.



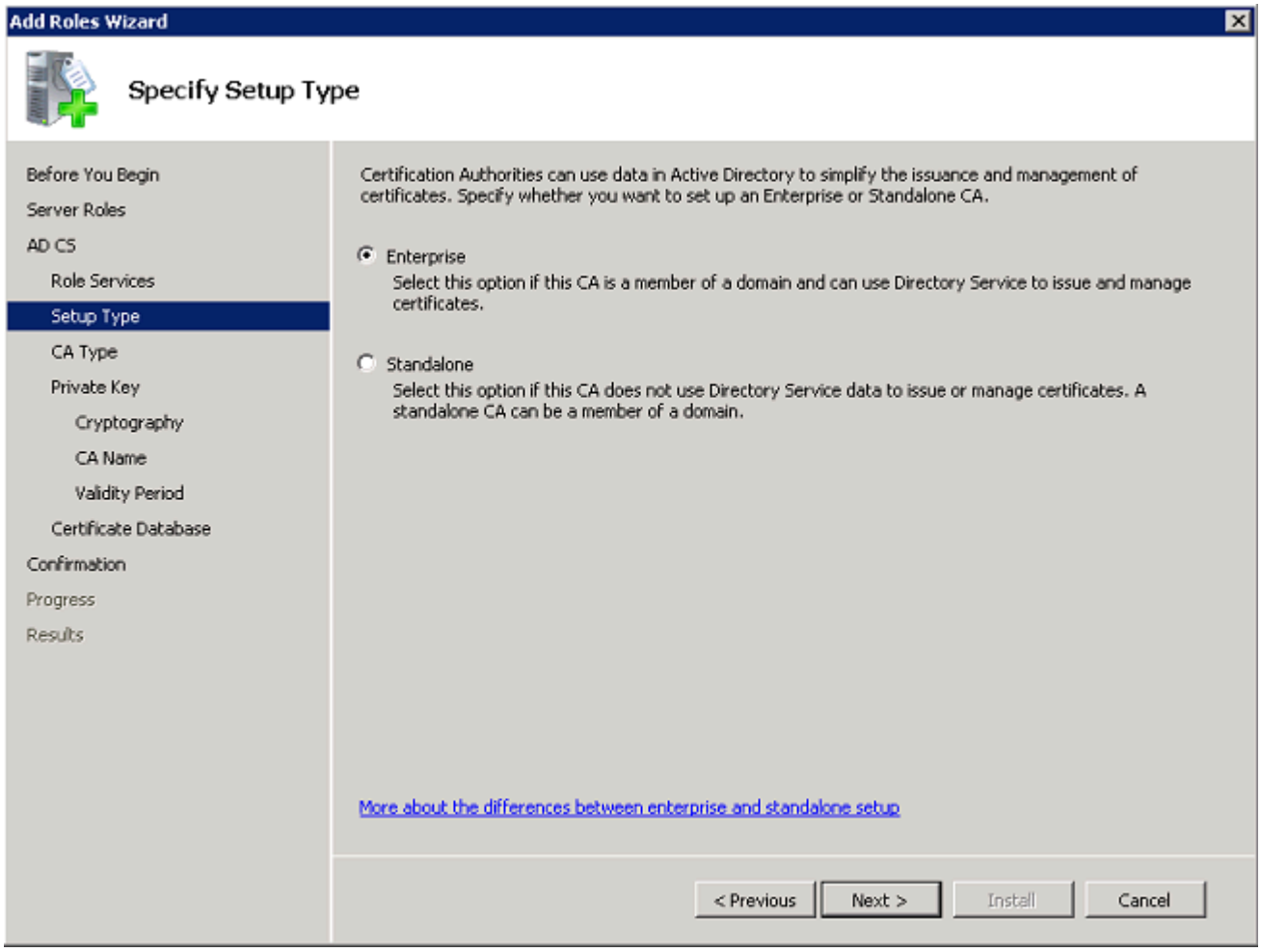
5. Consultez la section Introduction aux services de certificats Active Directory, puis cliquez sur Suivant.



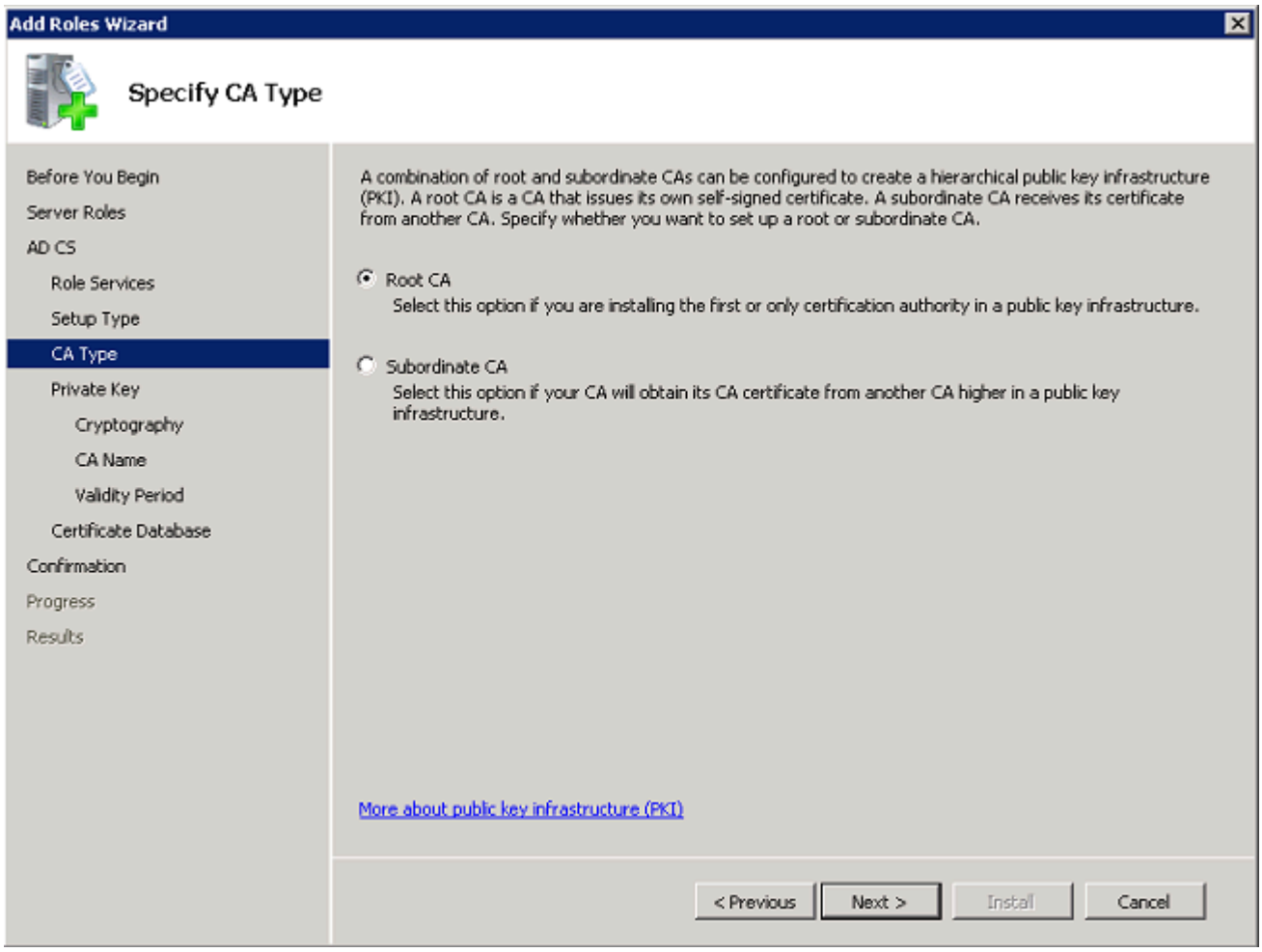
6. Sélectionnez l'autorité de certification, puis cliquez sur Next.



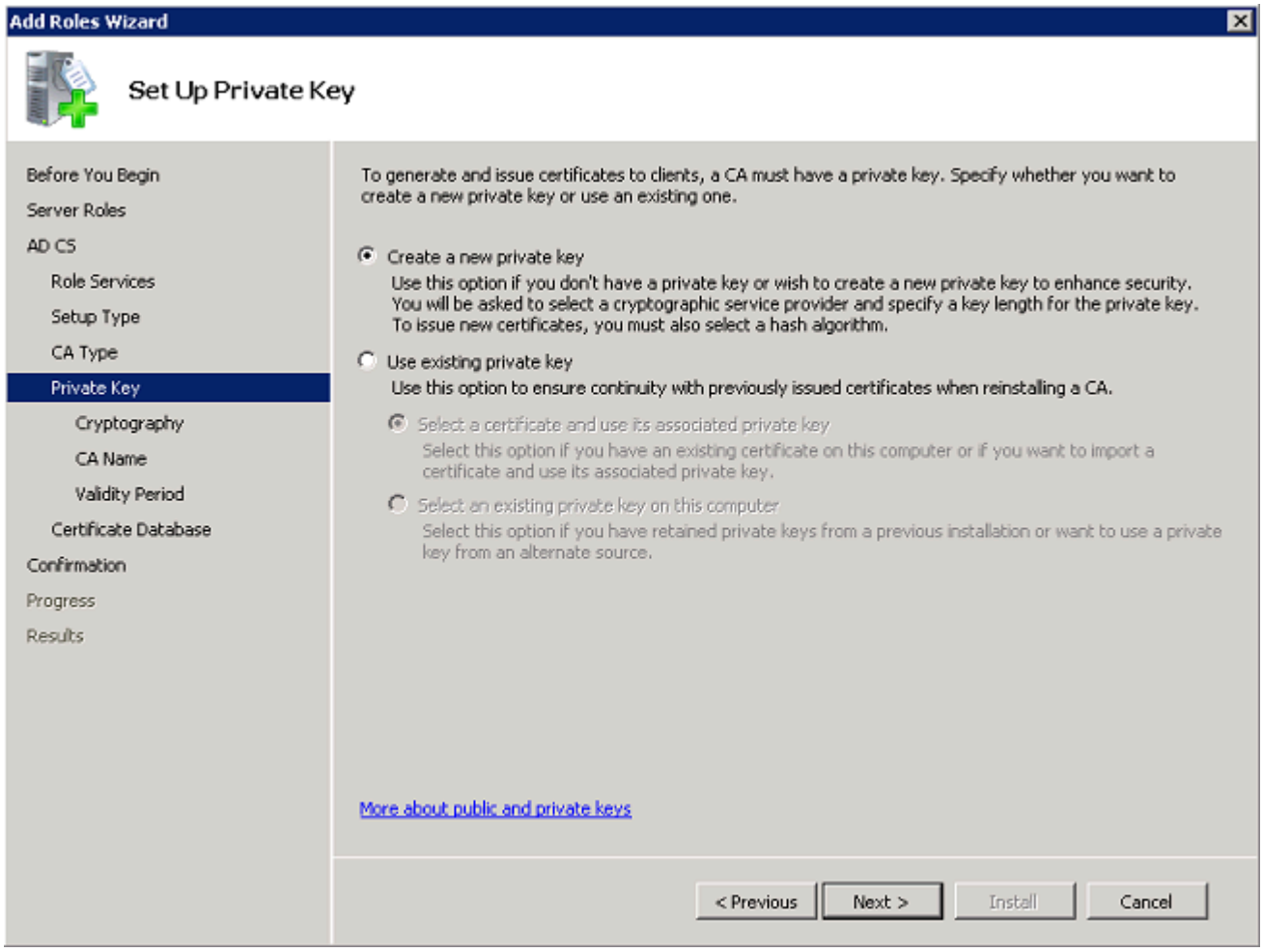
7. Sélectionnez Enterprise, puis cliquez sur Next.



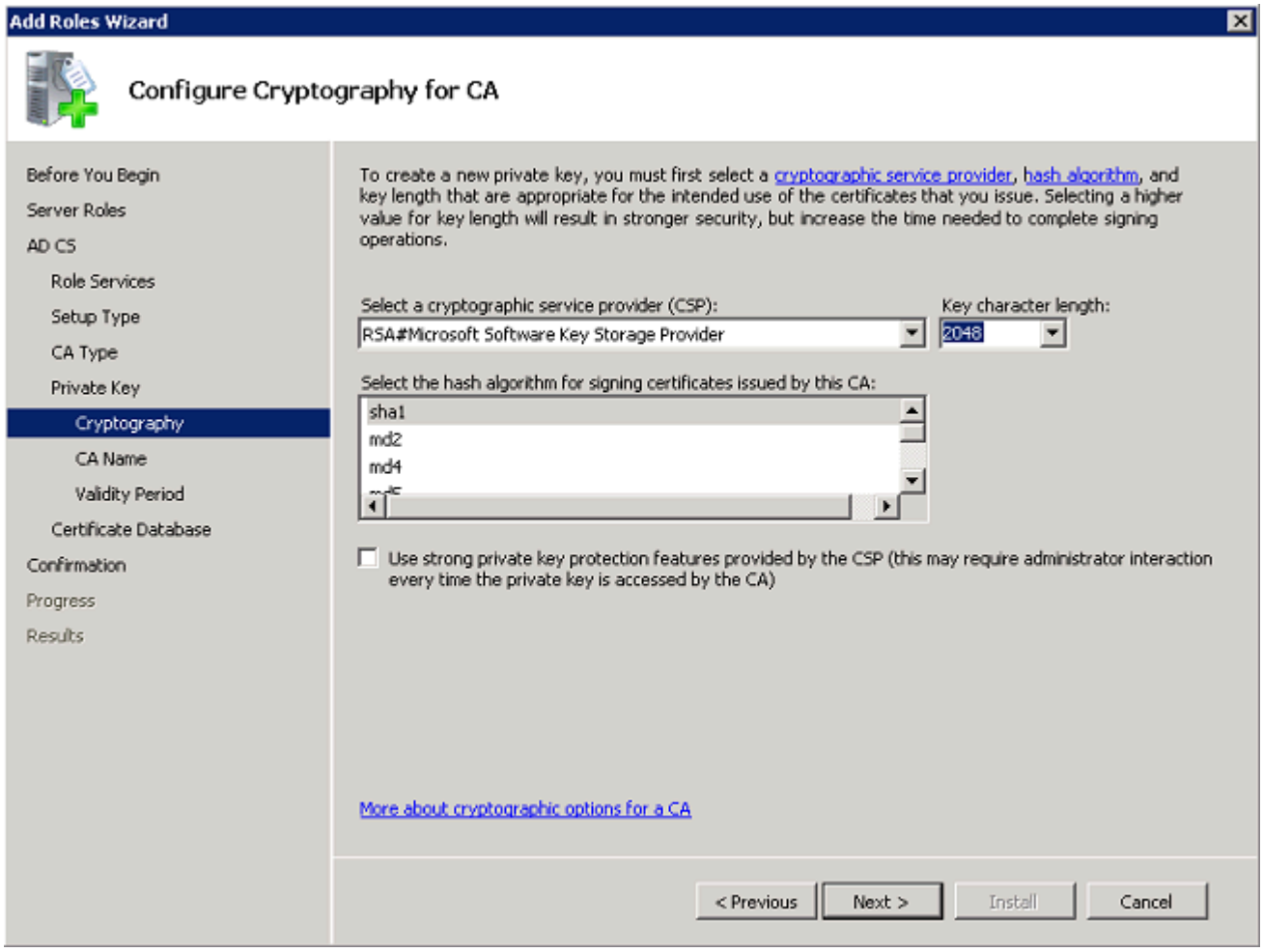
8. Sélectionnez Root CA, puis cliquez sur Next.



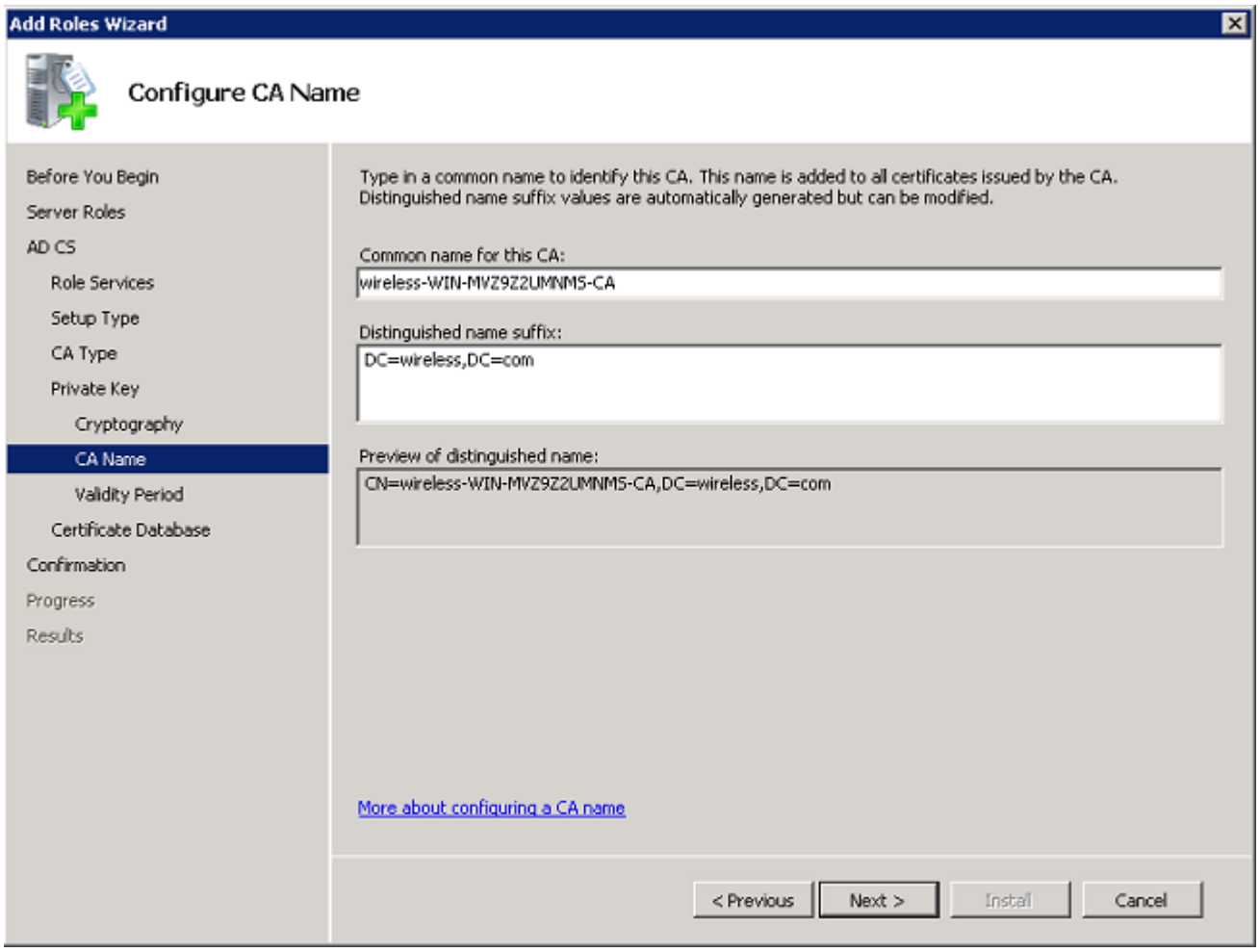
9. Sélectionnez Create a new private key, puis cliquez sur Next.



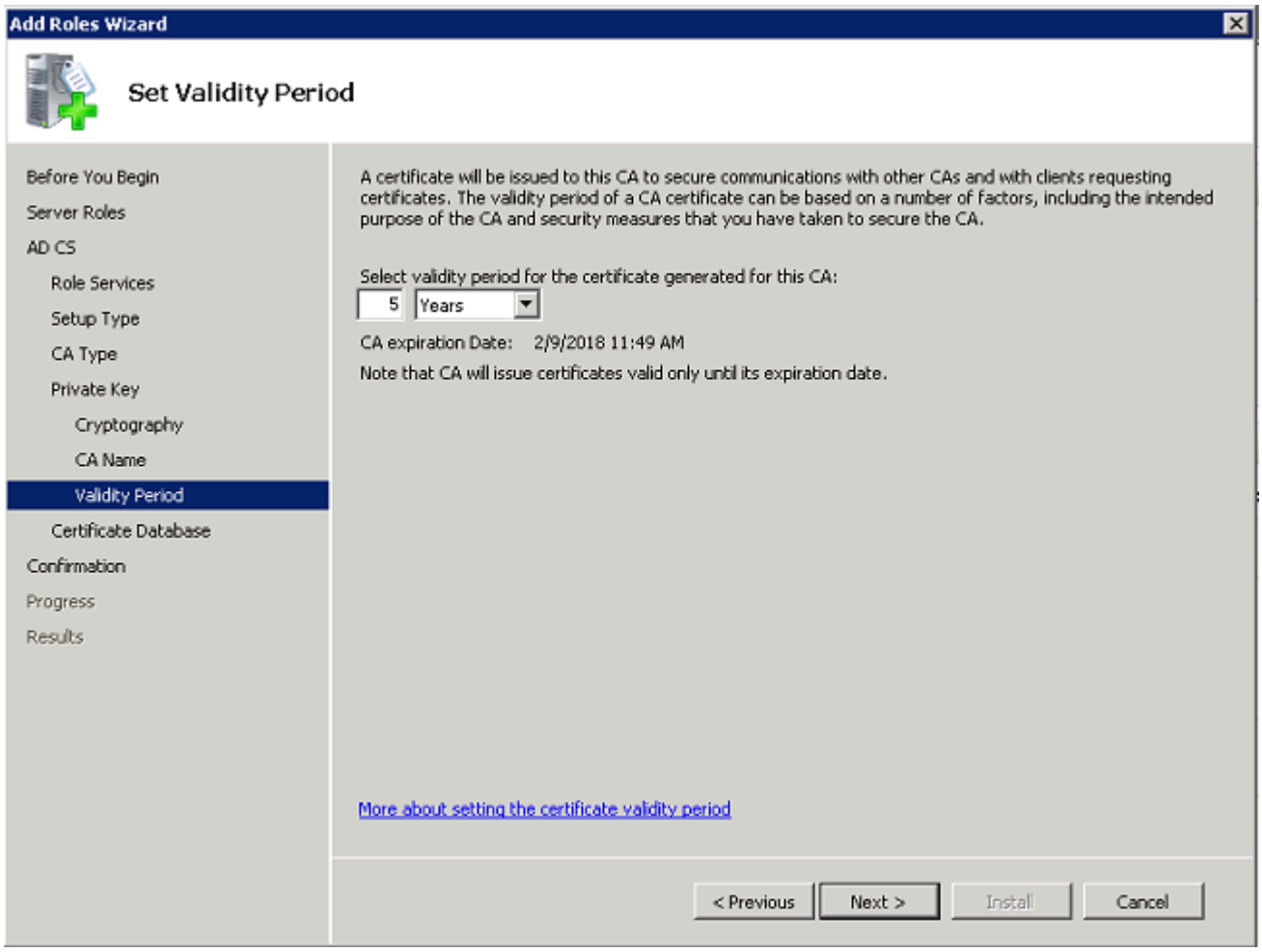
10. Cliquez sur Next sur Configure Cryptography for CA.



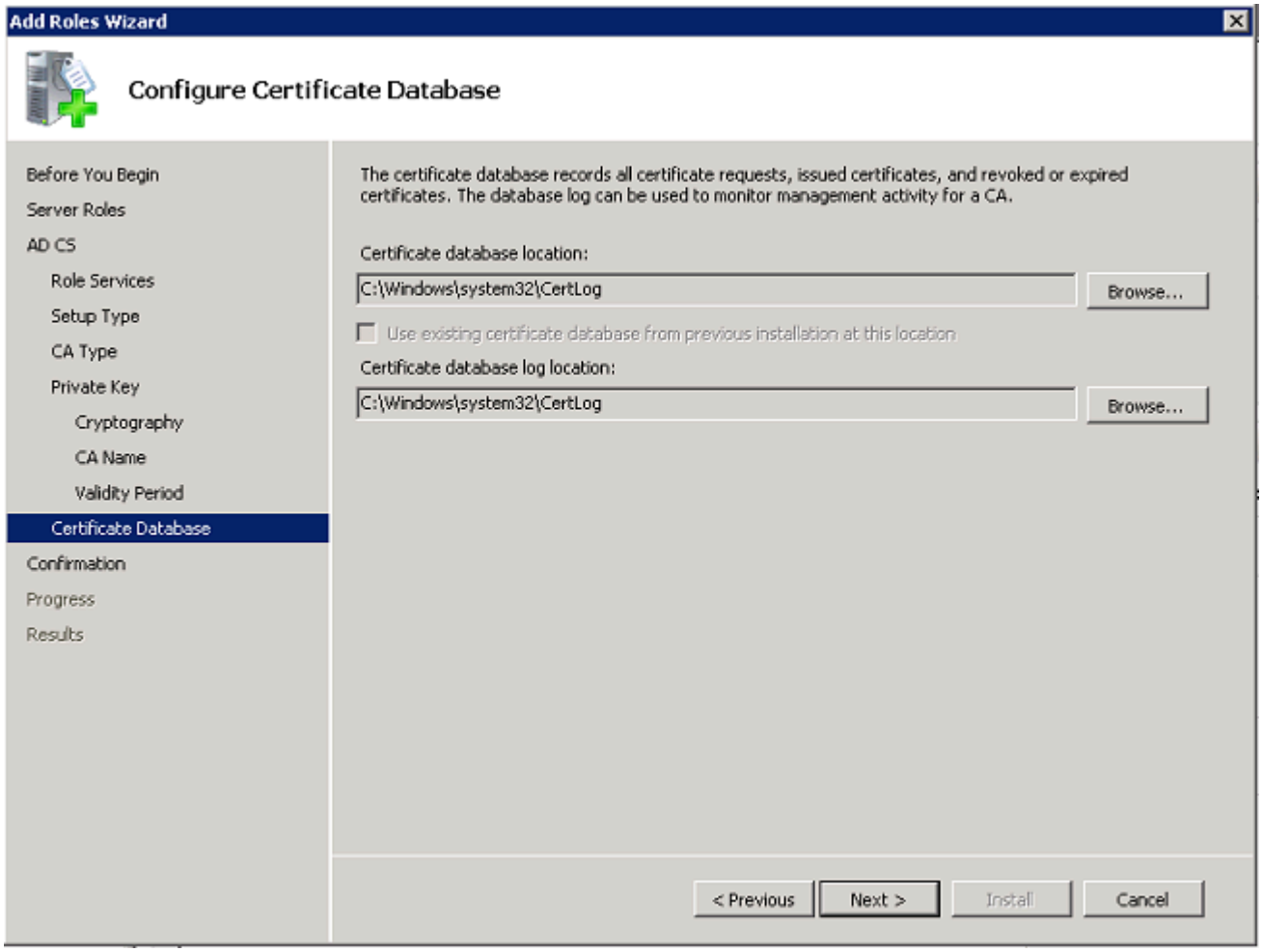
11. Cliquez sur Next pour accepter le nom commun par défaut pour cette autorité de certification.



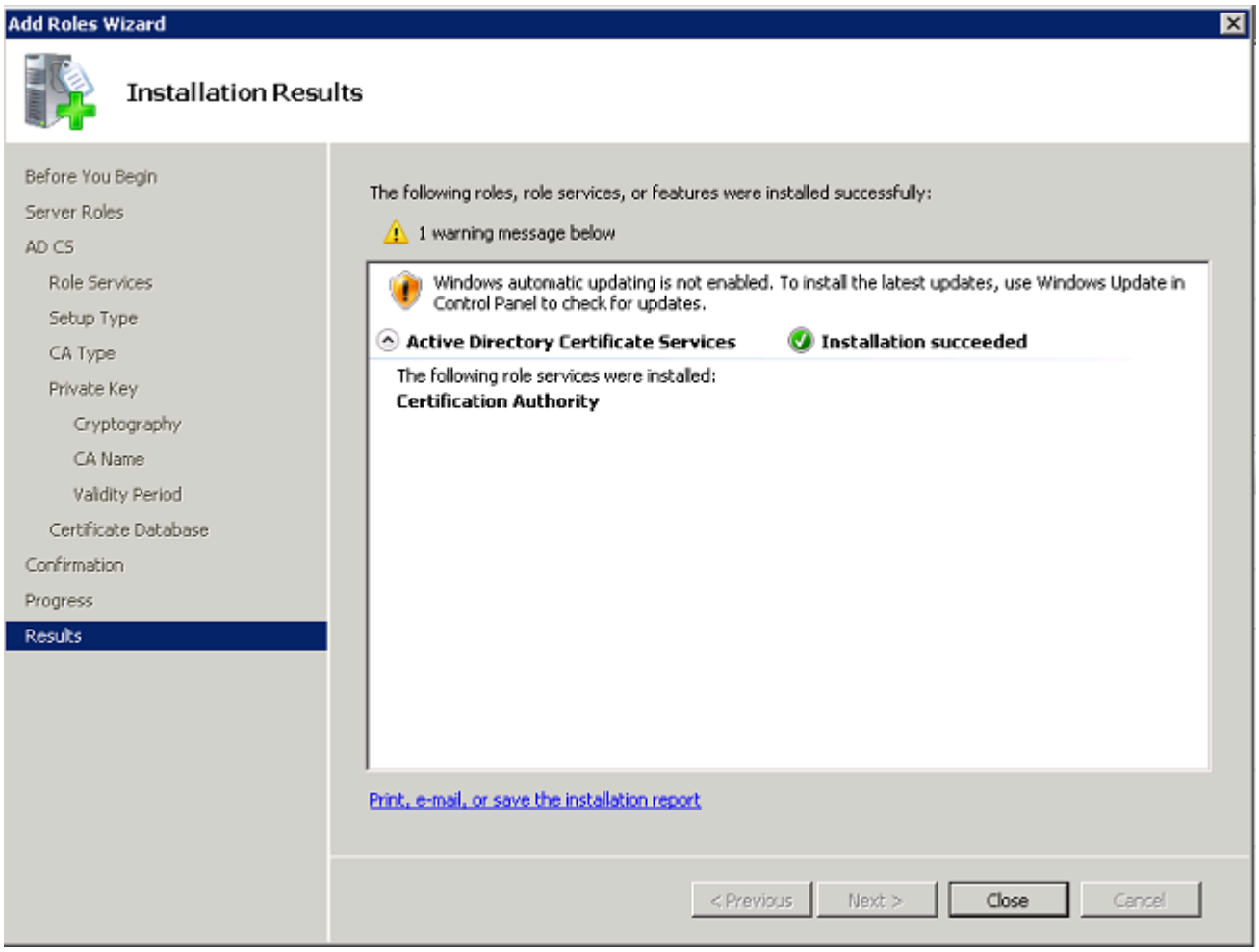
12. Sélectionnez la durée de validité de ce certificat d'autorité de certification, puis cliquez sur Suivant.



13. Cliquez sur Next pour accepter l'emplacement de la base de données de certificats par défaut.



14. Vérifiez la configuration et cliquez sur Installer pour démarrer les services de certificats Active Directory.

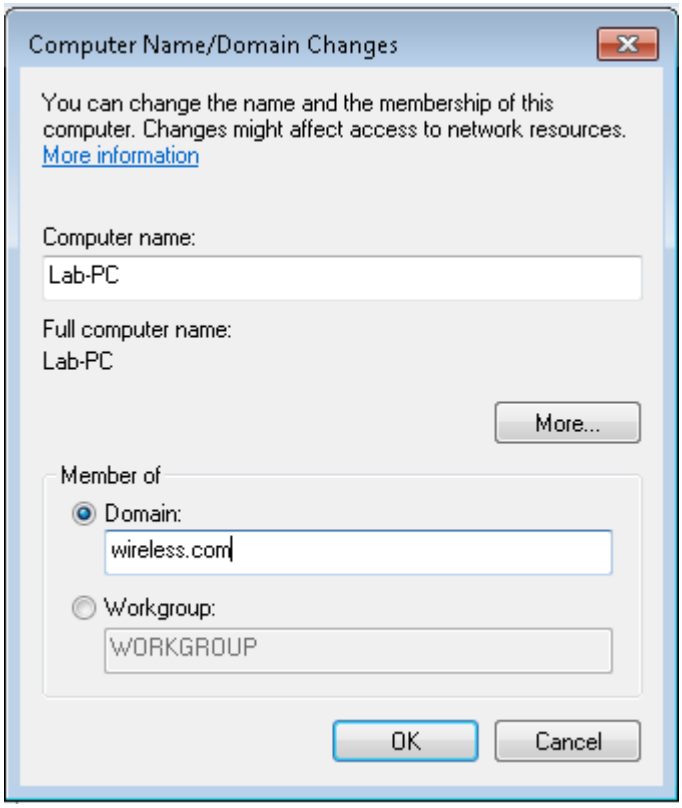


15. Une fois l'installation terminée, cliquez sur Close.

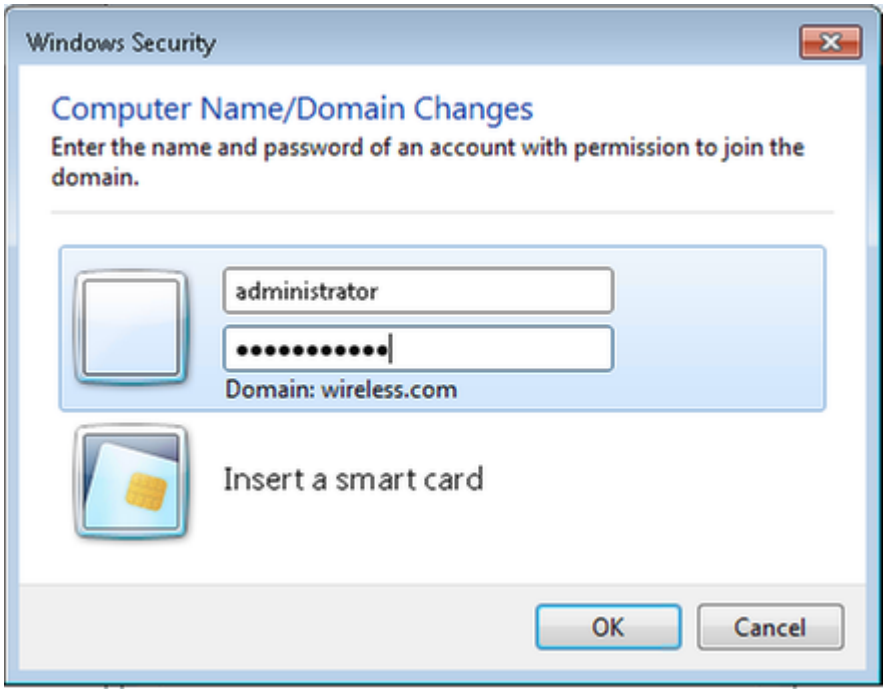
Connectez les clients de routage au domaine de routage

Complétez ces étapes afin de connecter les clients au réseau câblé et de télécharger les informations spécifiques au domaine à partir du nouveau domaine :

1. Connectez les clients au réseau câblé avec une droite par un câble Ethernet.
2. Démarrez le client et connectez-vous avec le nom d'utilisateur et le mot de passe du client.
3. Cliquez sur Démarrer>Exécuter, entrez cmd, puis cliquez sur OK.
4. À l'invite de commande, entrez ipconfig, puis cliquez sur Enter pour vérifier que DHCP fonctionne correctement et que le client a reçu une adresse IP du serveur DHCP.
5. Afin de joindre le client au domaine, cliquez sur Démarrer, cliquez avec le bouton droit sur Ordinateur, choisissez Propriétés, et choisissez Modifier les paramètres en bas à droite.
6. Cliquez sur Change.
7. Cliquez sur Domain, entrez le nom de domaine, wireless, pour cet exemple, et cliquez sur OK.



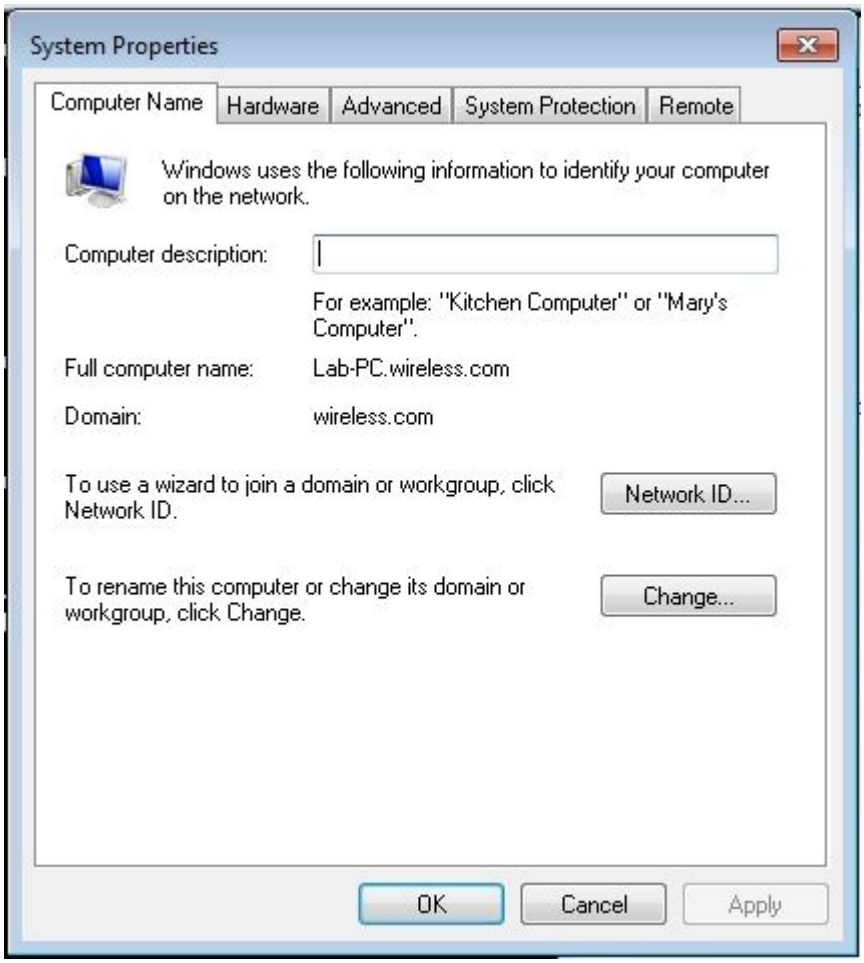
8. Entrez le nom d'utilisateur administrator et le mot de passe spécifique au domaine auquel le client se connecte. Il s'agit du compte administrateur dans Active Directory sur le serveur.



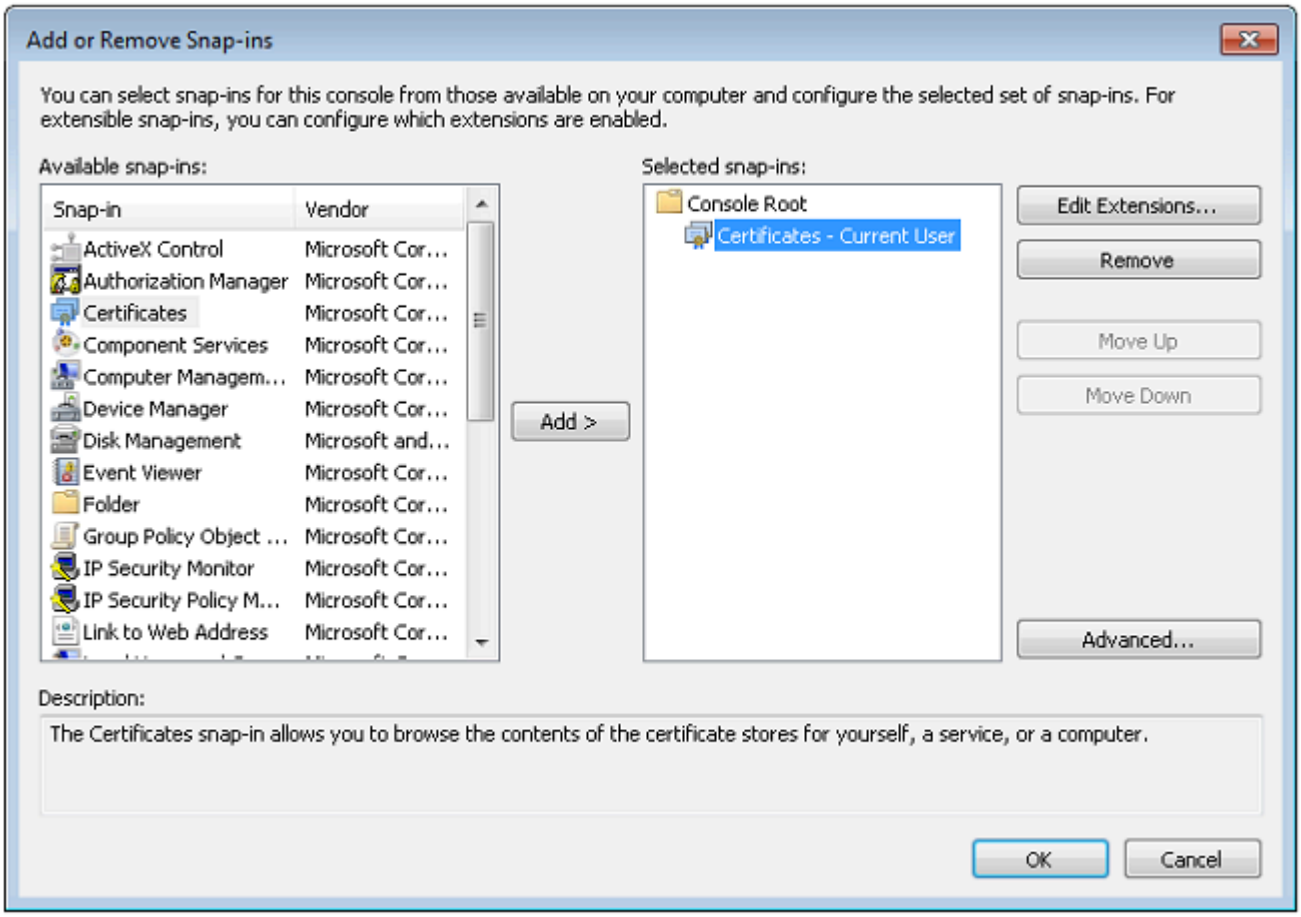
9. Cliquez sur OK, puis cliquez à nouveau sur OK.



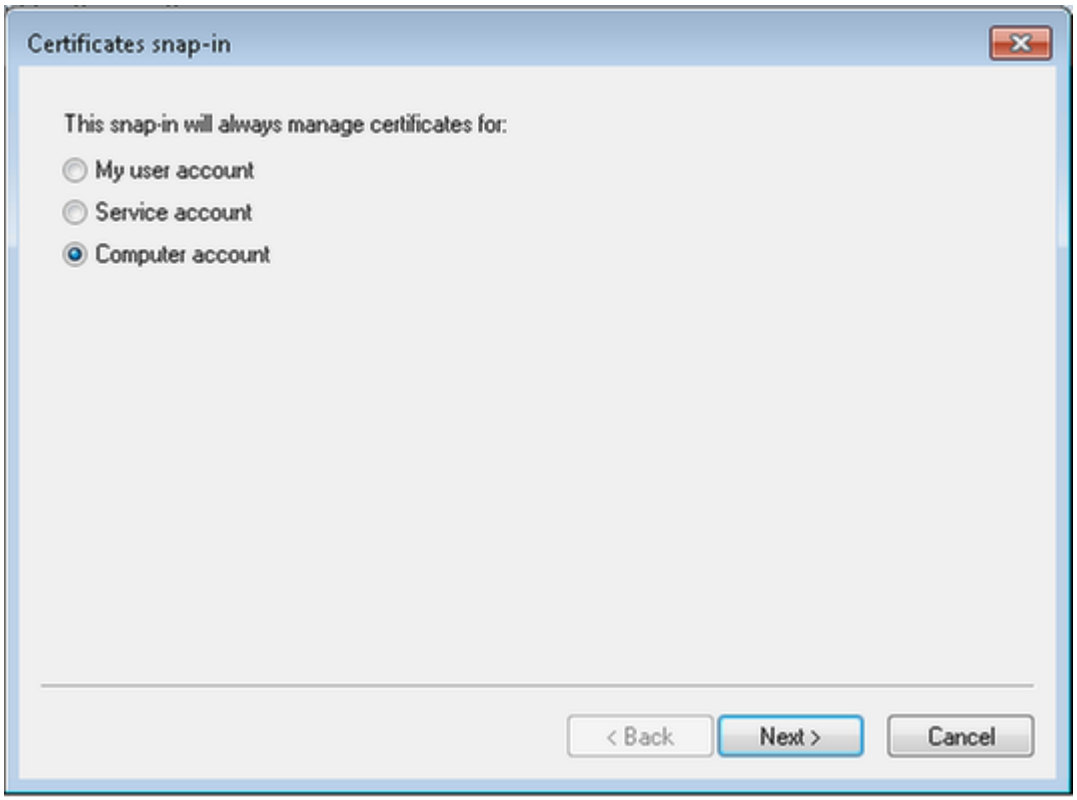
10. Cliquez sur Fermer>Redémarrer maintenant pour redémarrer l'ordinateur.
11. Une fois l'ordinateur redémarré, connectez-vous avec : Nom d'utilisateur = Administrateur ; Mot de passe = <mot de passedomaine>; Domaine = Sans fil.
12. Cliquez sur Démarrer, cliquez avec le bouton droit sur Ordinateur, choisissez Propriétés et choisissez Modifier les paramètres en bas à droite pour vérifier que vous êtes sur le domaine sans fil.
13. L'étape suivante consiste à vérifier que le client a reçu le certificat d'authentification (de confiance) du serveur.



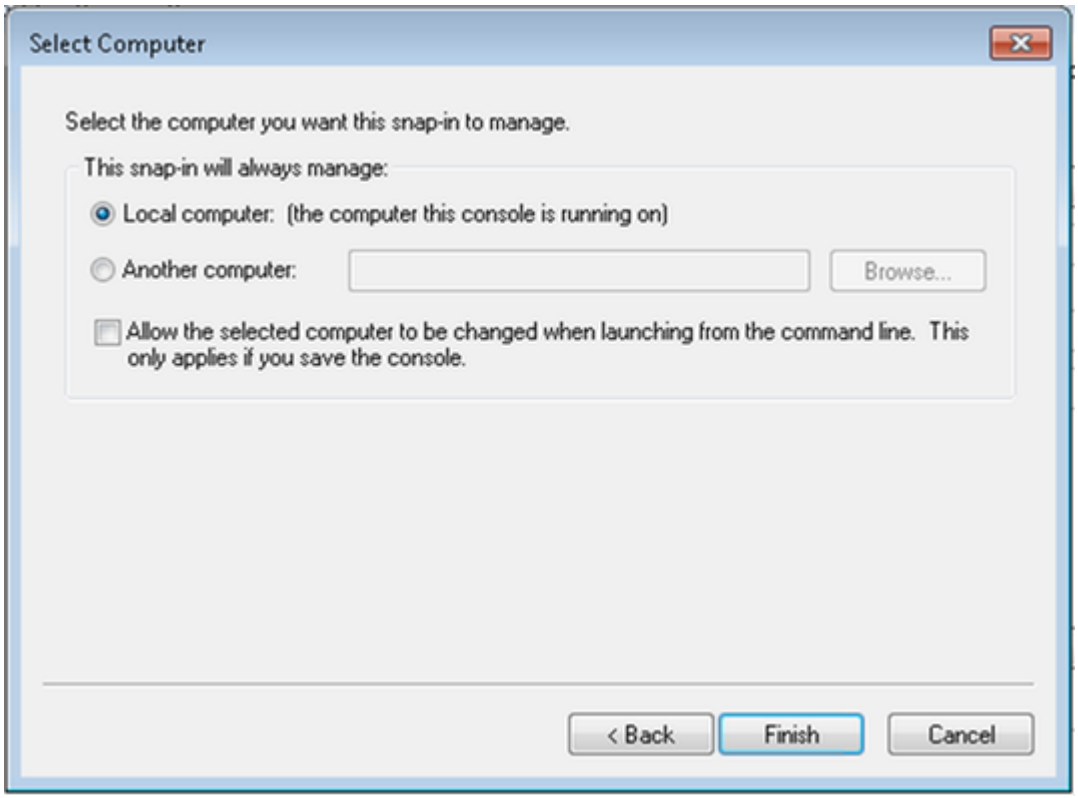
14. Cliquez sur Démarrer, entrez mmc, puis appuyez sur Entrée.
15. Cliquez sur File, puis cliquez sur le jeu d'outils Add/Remove.
16. Choisissez Certificates, puis cliquez sur Add.



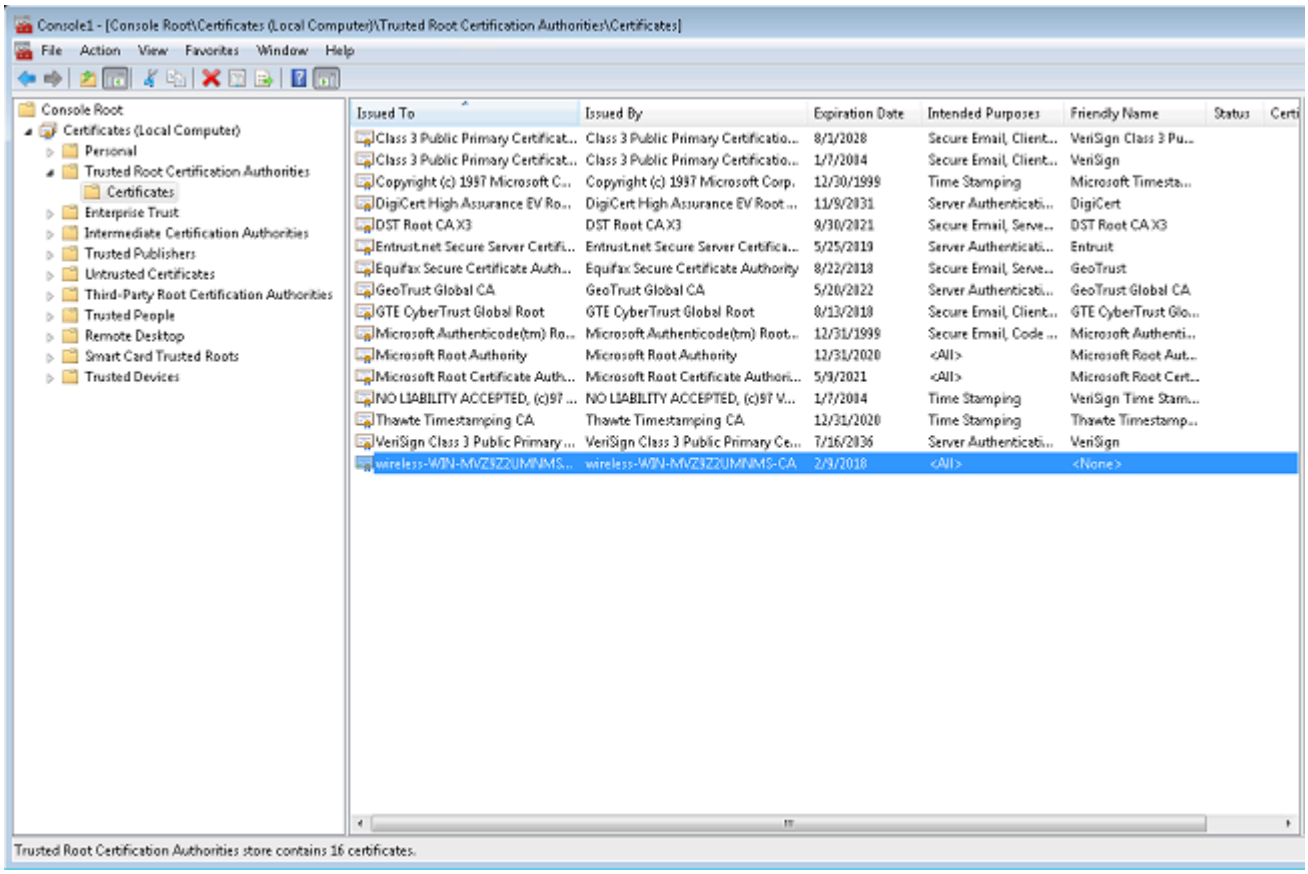
17. Cliquez sur Compte d'ordinateur, puis sur Suivant.



18. Cliquez sur Ordinateur local, puis sur Suivant.



19. Click OK.
20. Développez les dossiers Certificates (Local Computer) et Trusted Root Certification Authorities, puis cliquez sur Certificates. Recherchez le certificat CA de domaine sans fil dans la liste. Dans cet exemple, le certificat CA est appelé wireless-WIN-MVZ9Z2UMNMS-CA.

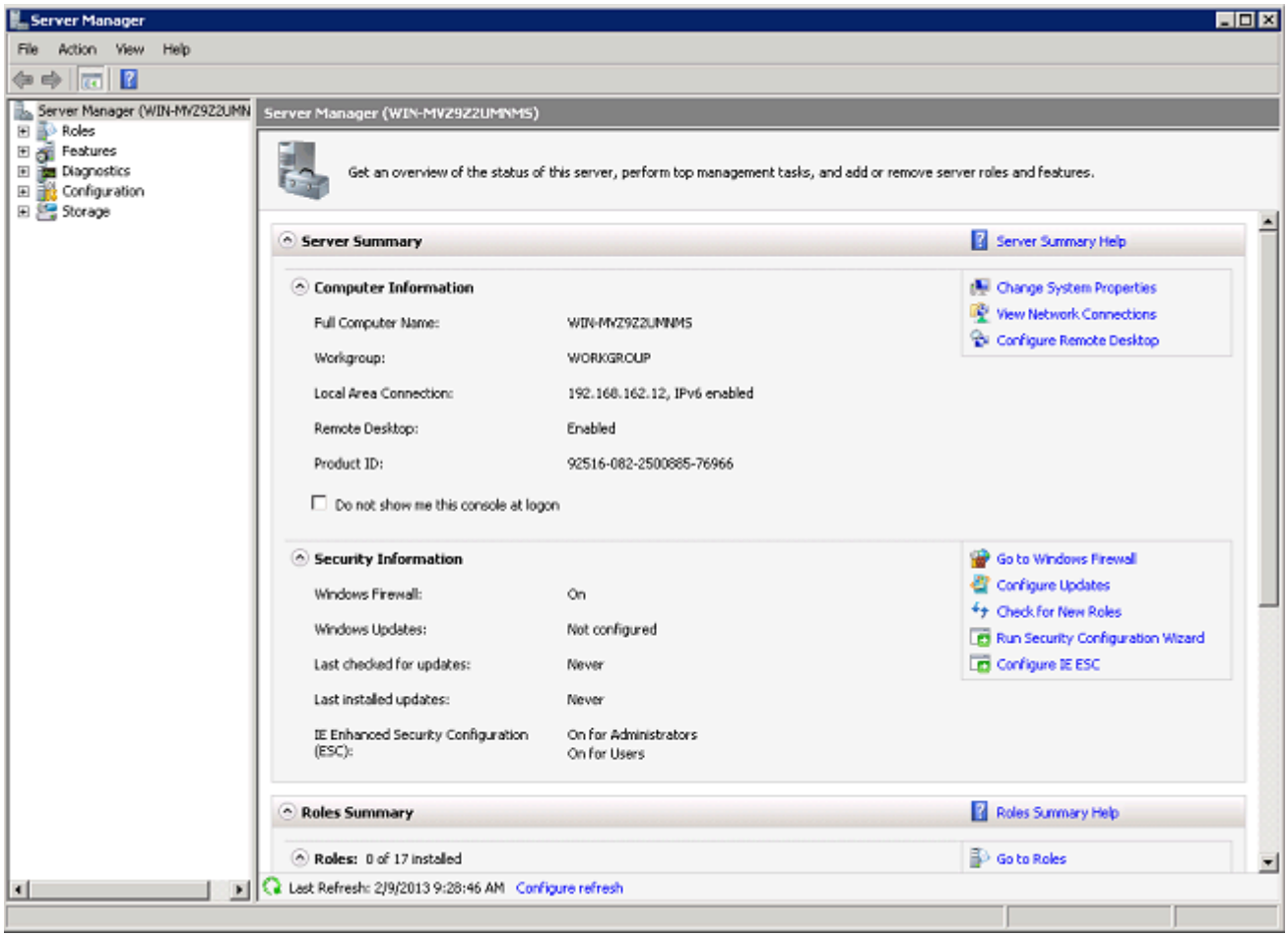


21. Répétez cette procédure pour ajouter plus de clients au domaine.

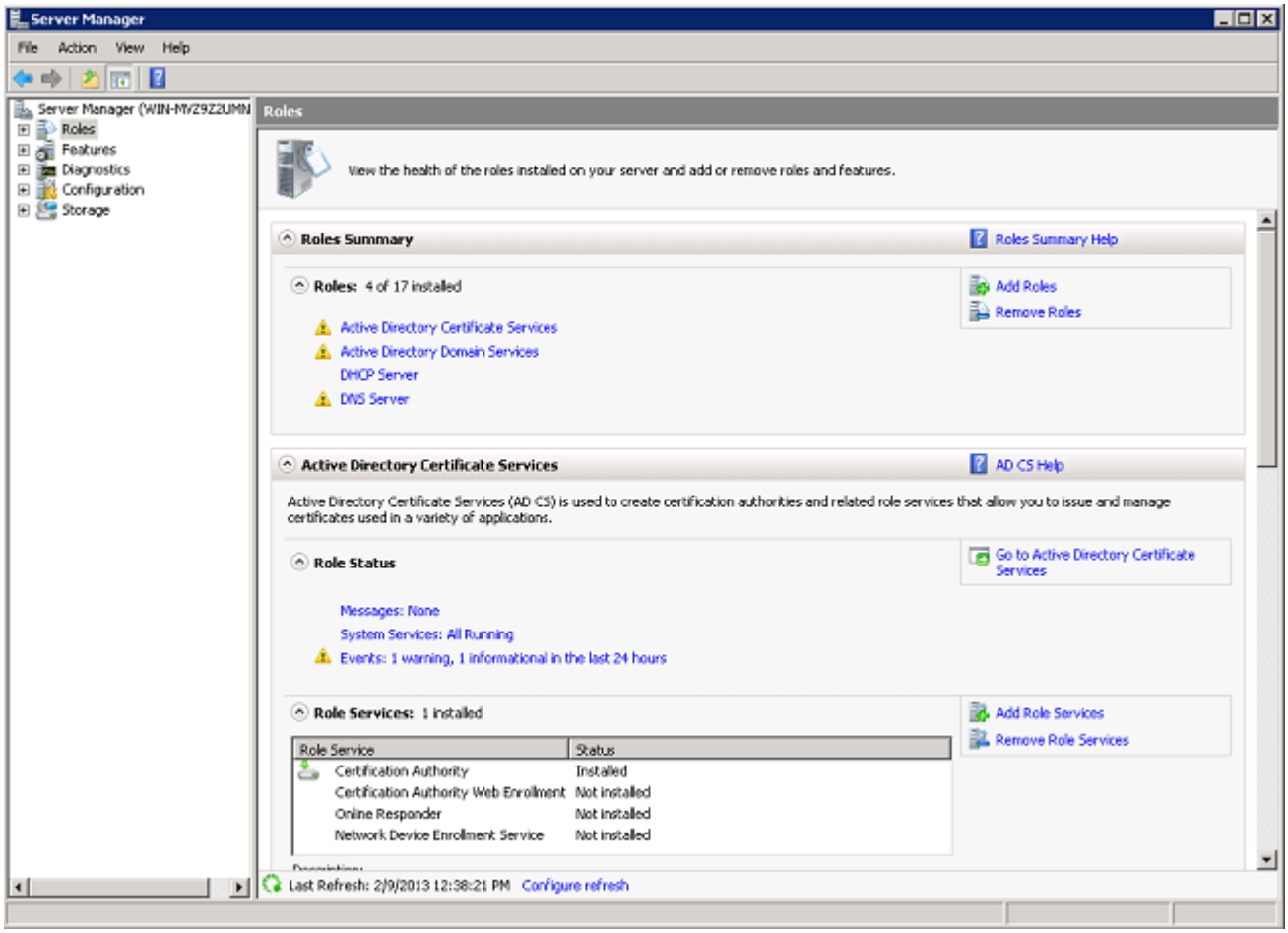
Installer le serveur NPS sur Microsoft Windows 2008 Server

Dans cette configuration, le serveur NPS est utilisé comme serveur RADIUS pour authentifier les clients sans fil avec l'authentification PEAP. Complétez ces étapes afin d'installer et de configurer le serveur NPS sur le serveur Microsoft Windows 2008 :

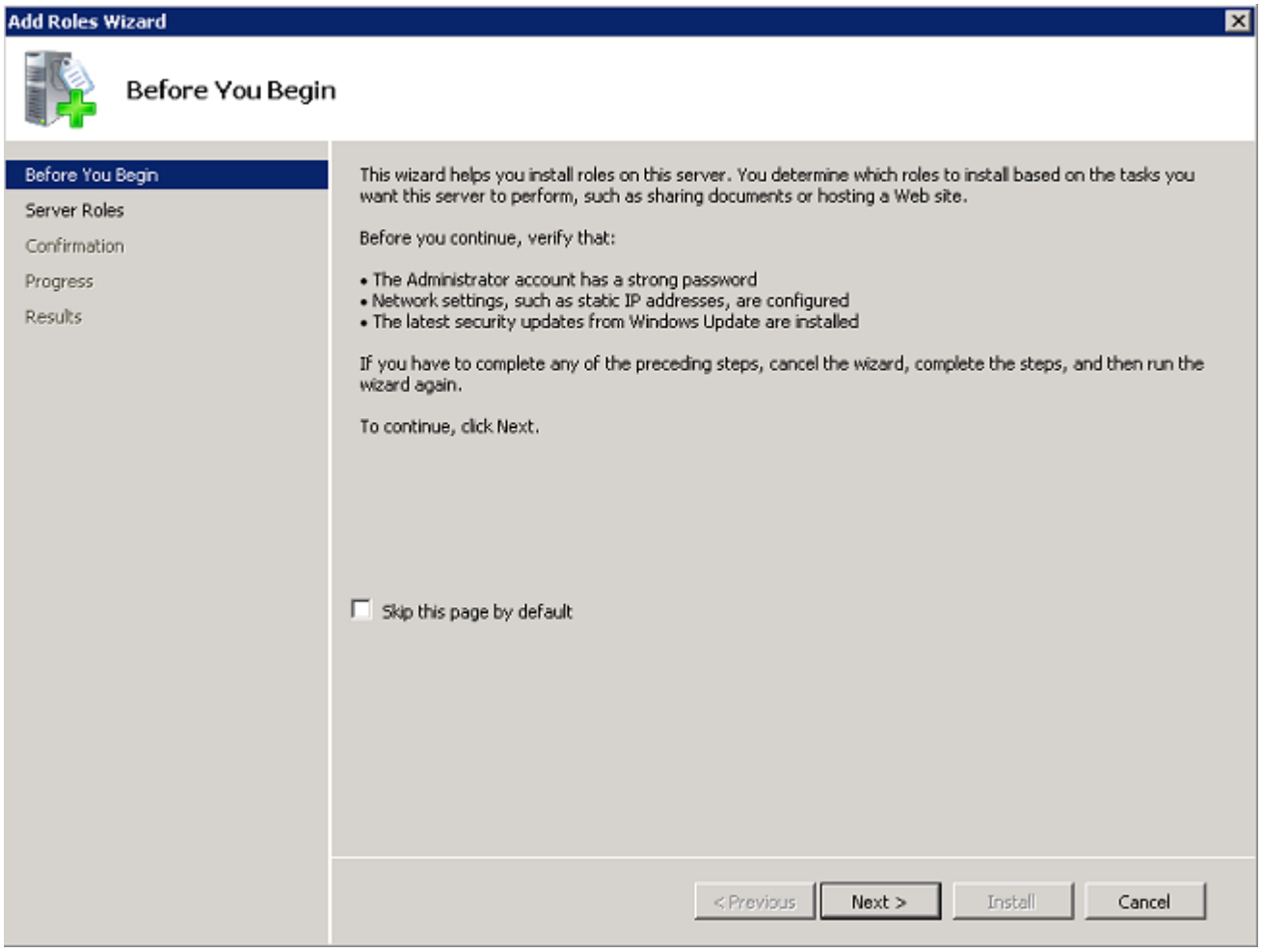
1. Cliquez sur Démarrer> Gestionnaire de serveur.



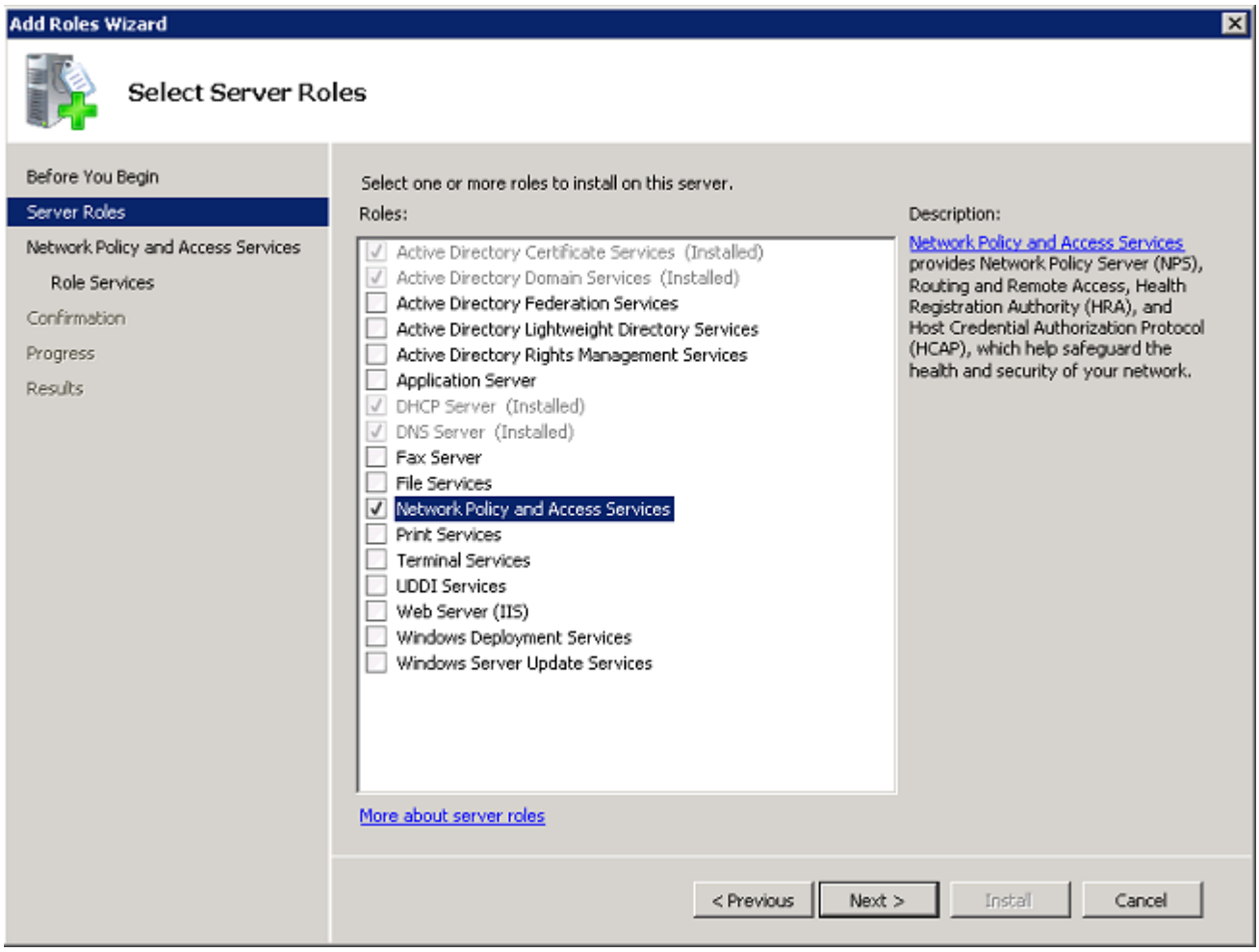
2. Cliquez sur Rôles> Ajouter des rôles.



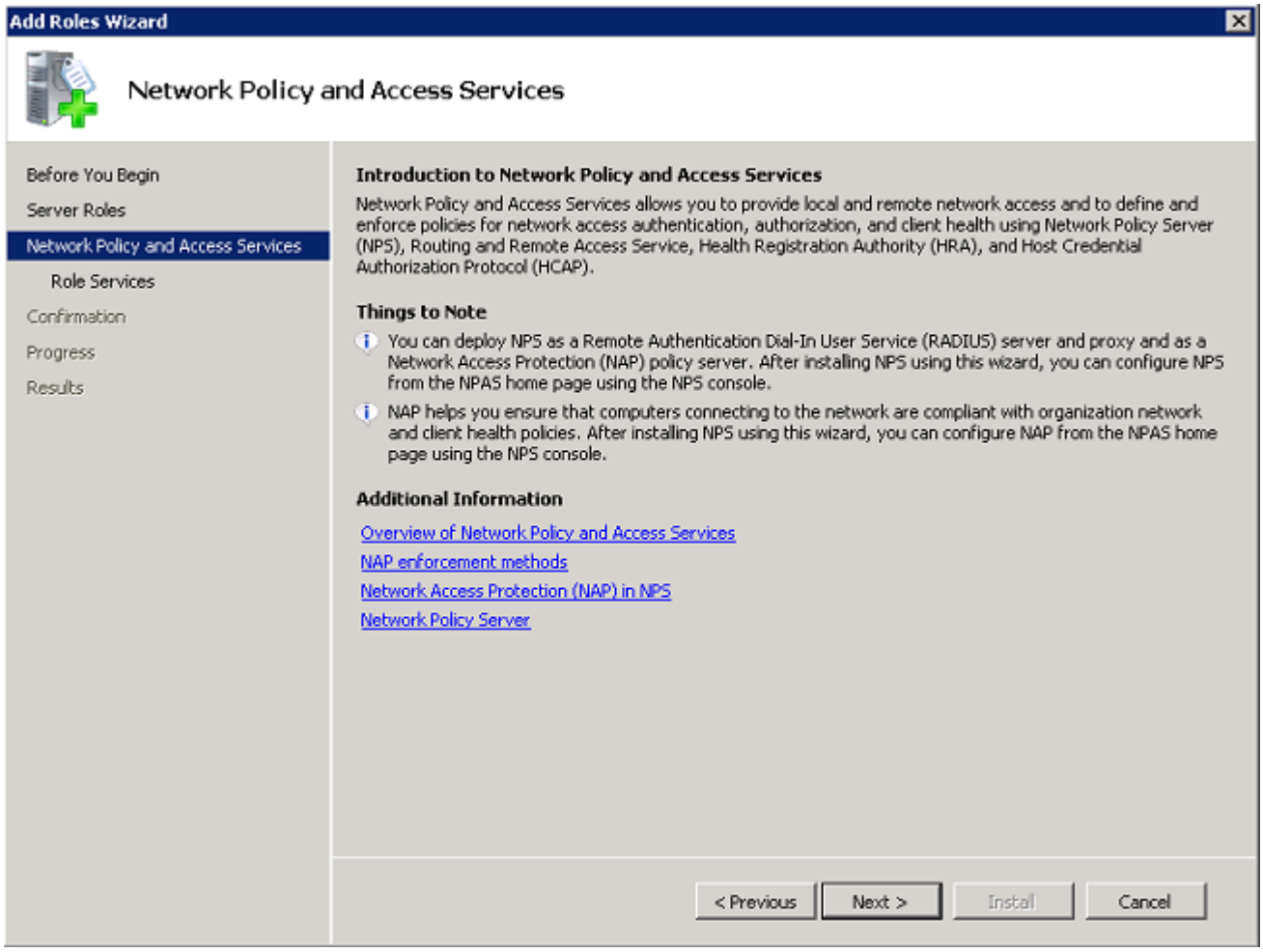
3. Cliquez sur Next (Suivant).



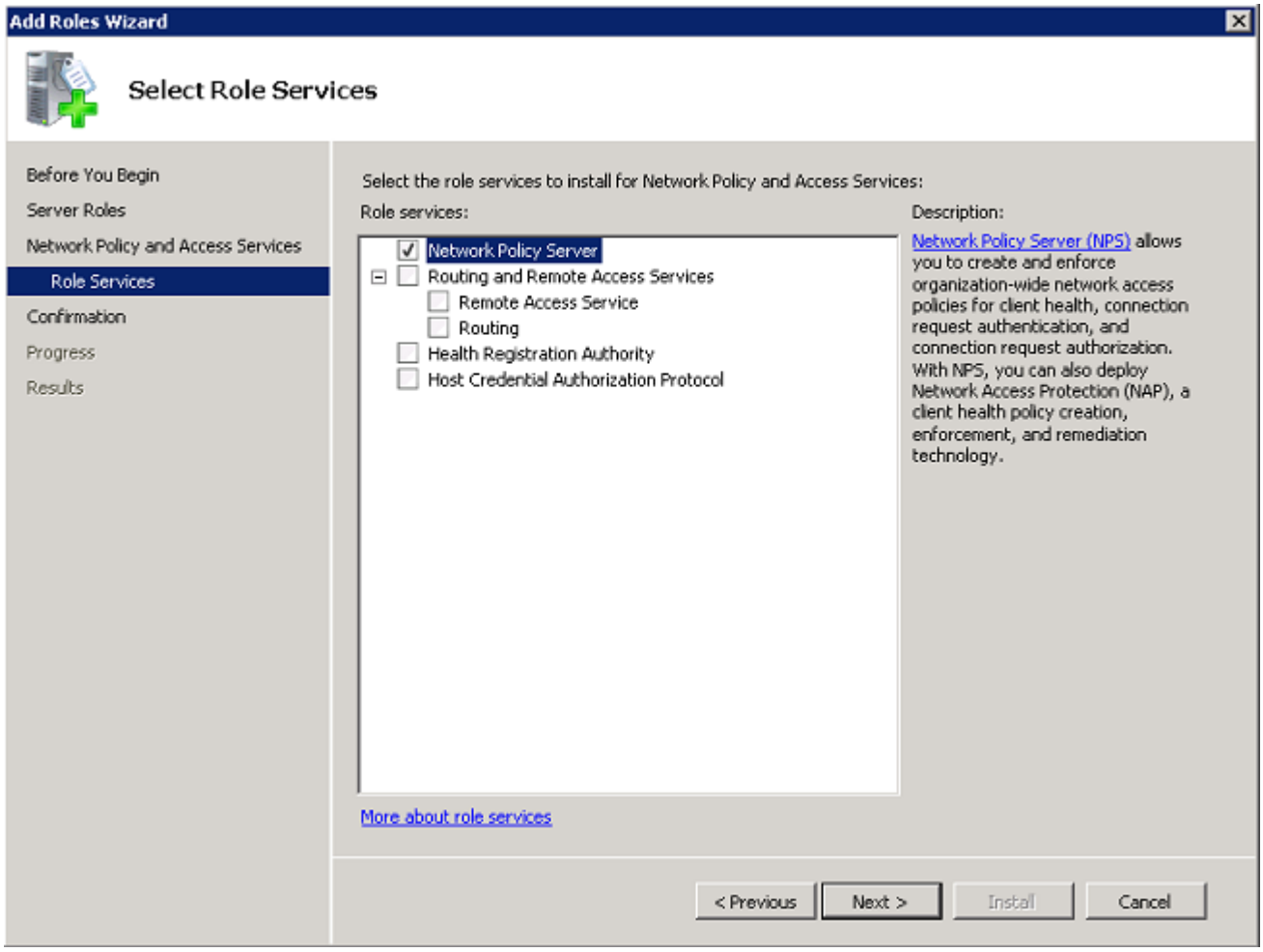
4. Sélectionnez le service Network Policy and Access Services, puis cliquez sur Next.



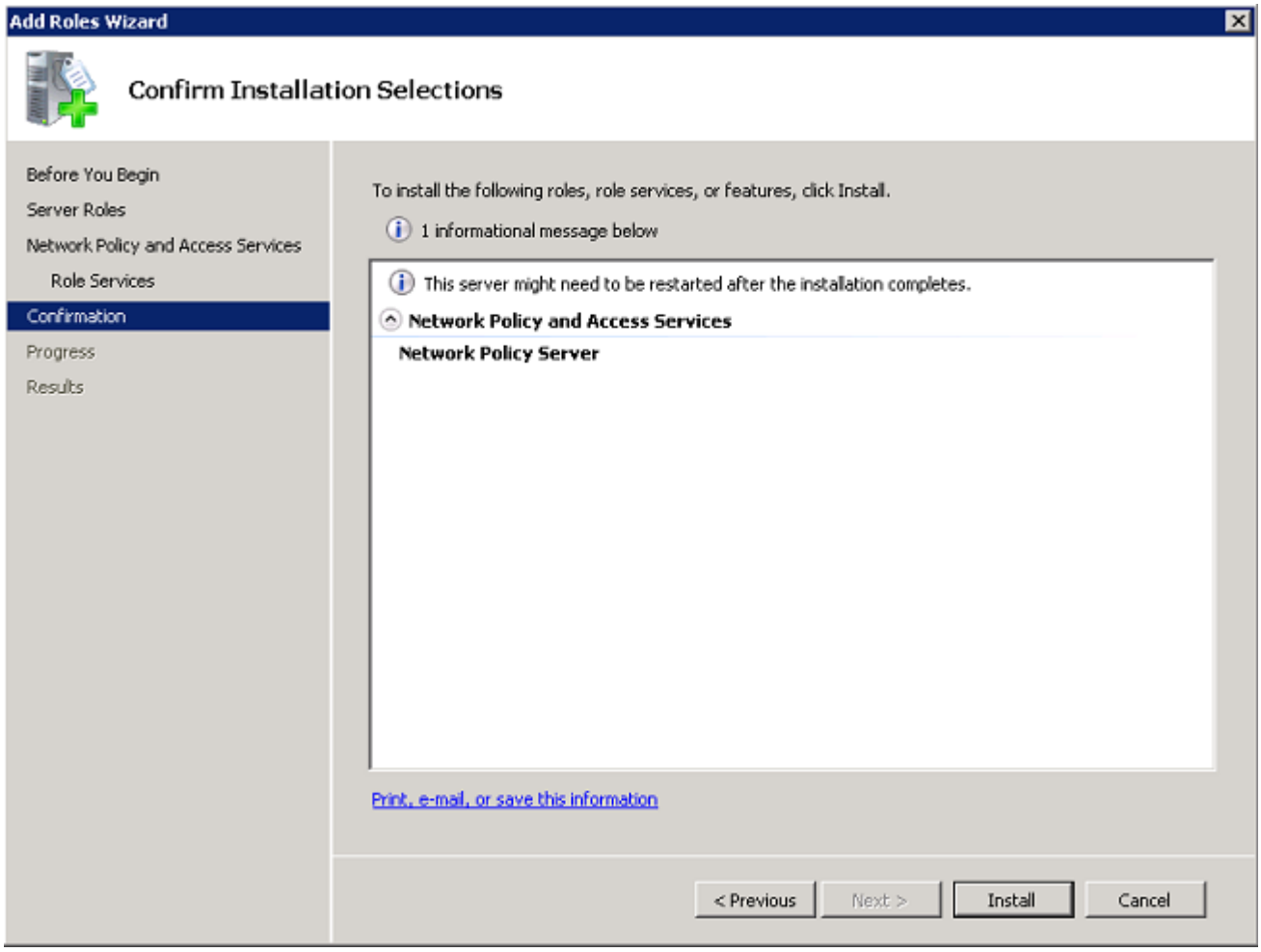
5. Reportez-vous à Introduction to Network Policy and Access Services, puis cliquez sur Next.



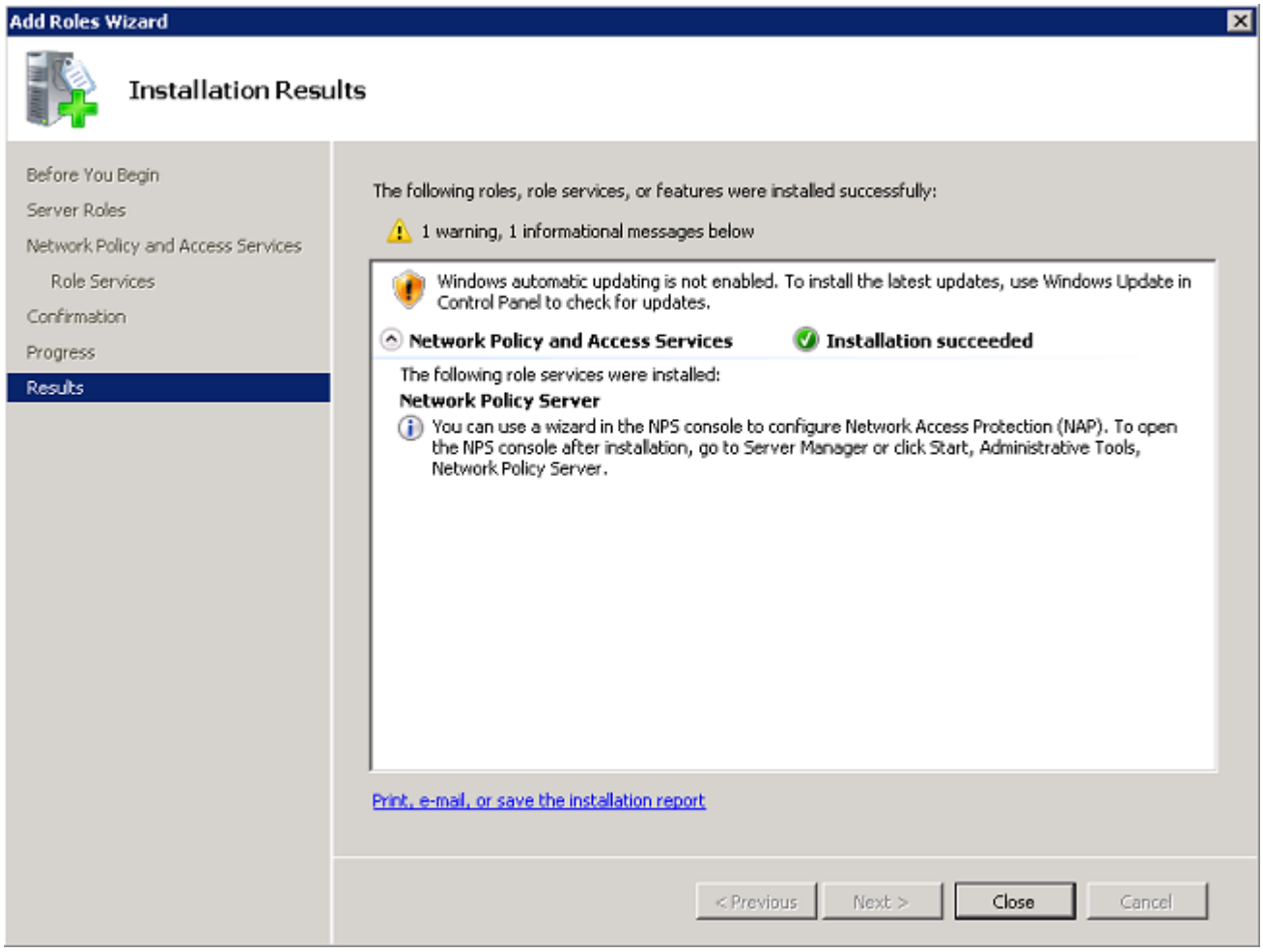
6. Sélectionnez Network Policy Server, puis cliquez sur Next.



7. Vérifiez la confirmation, puis cliquez sur Install.



Une fois l'installation terminée, un écran similaire à celui-ci s'affiche.

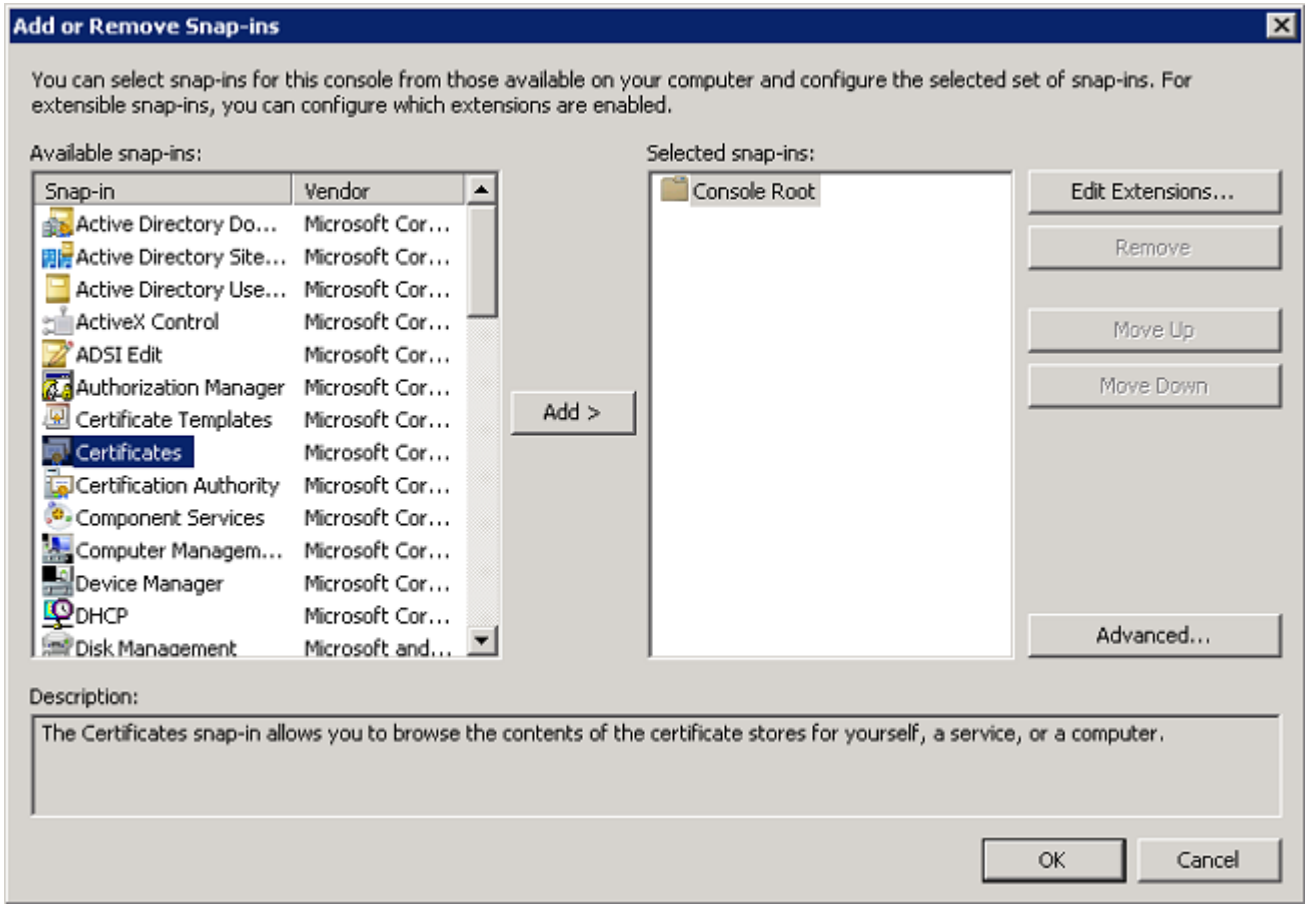


8. Cliquez sur Fermer.

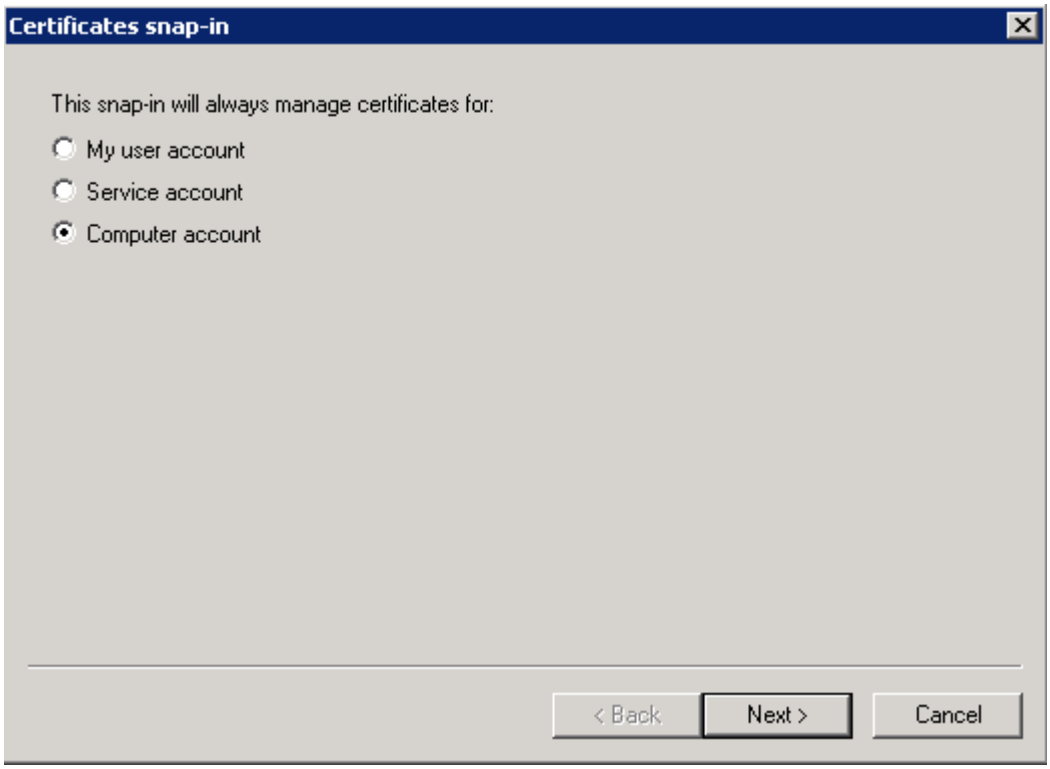
Installer un certificat

Complétez ces étapes afin d'installer le certificat d'ordinateur pour le NPS :

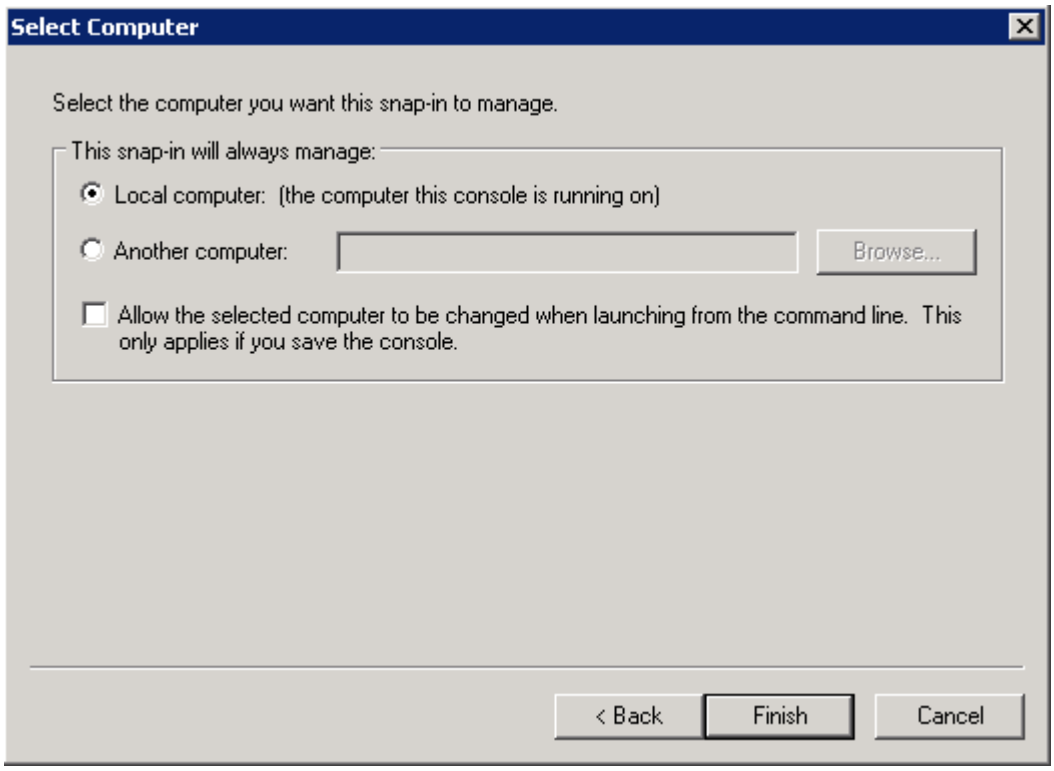
1. Cliquez sur Démarrer, entrez mmc, puis appuyez sur Entrée.
2. Cliquez sur Fichier > Ajouter/Supprimer un composant logiciel enfichable.
3. Choisissez Certificates, puis cliquez sur Add.



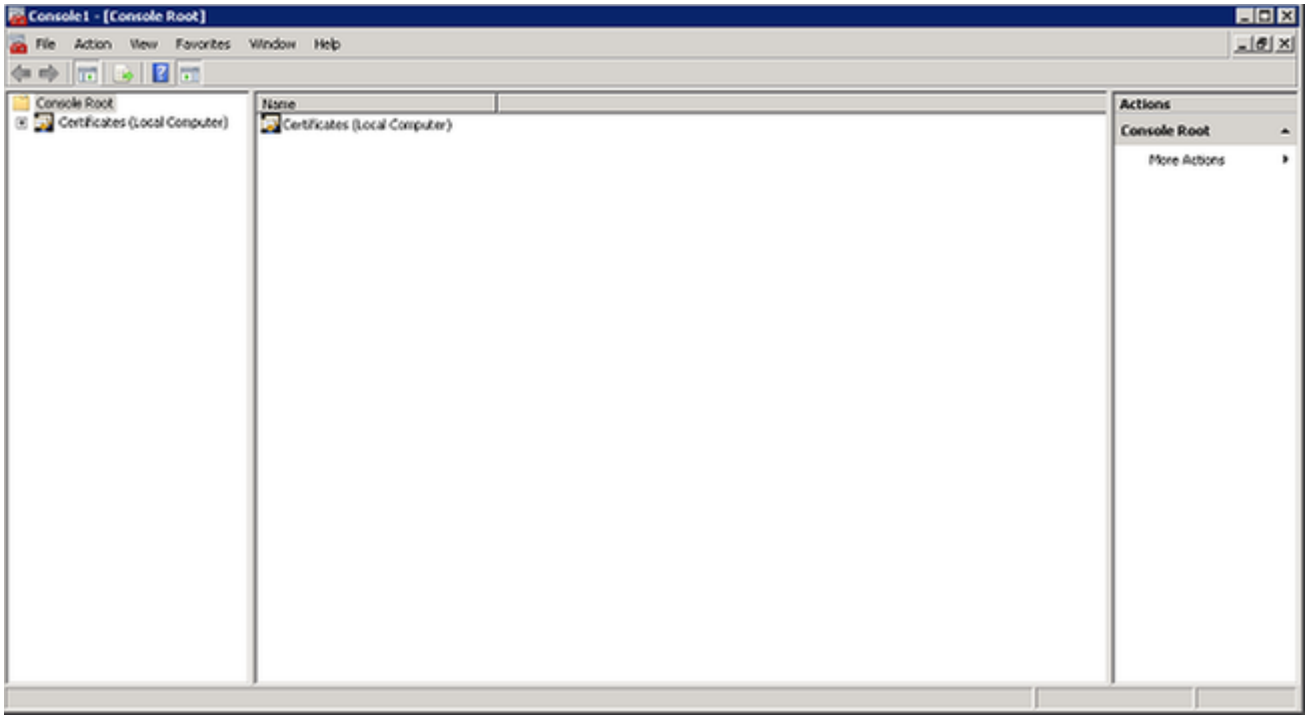
4. Choisissez Computer Account, puis cliquez sur Next.



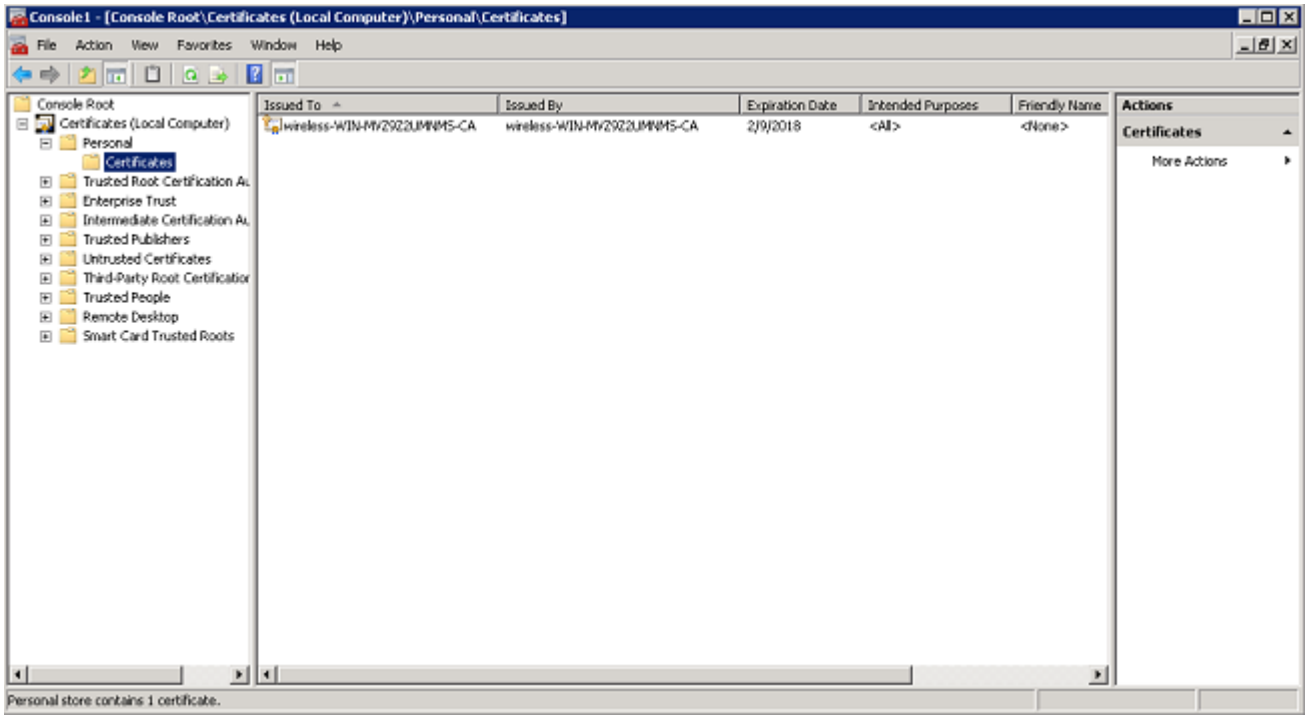
5. Sélectionnez Ordinateur local, puis cliquez sur Terminer.



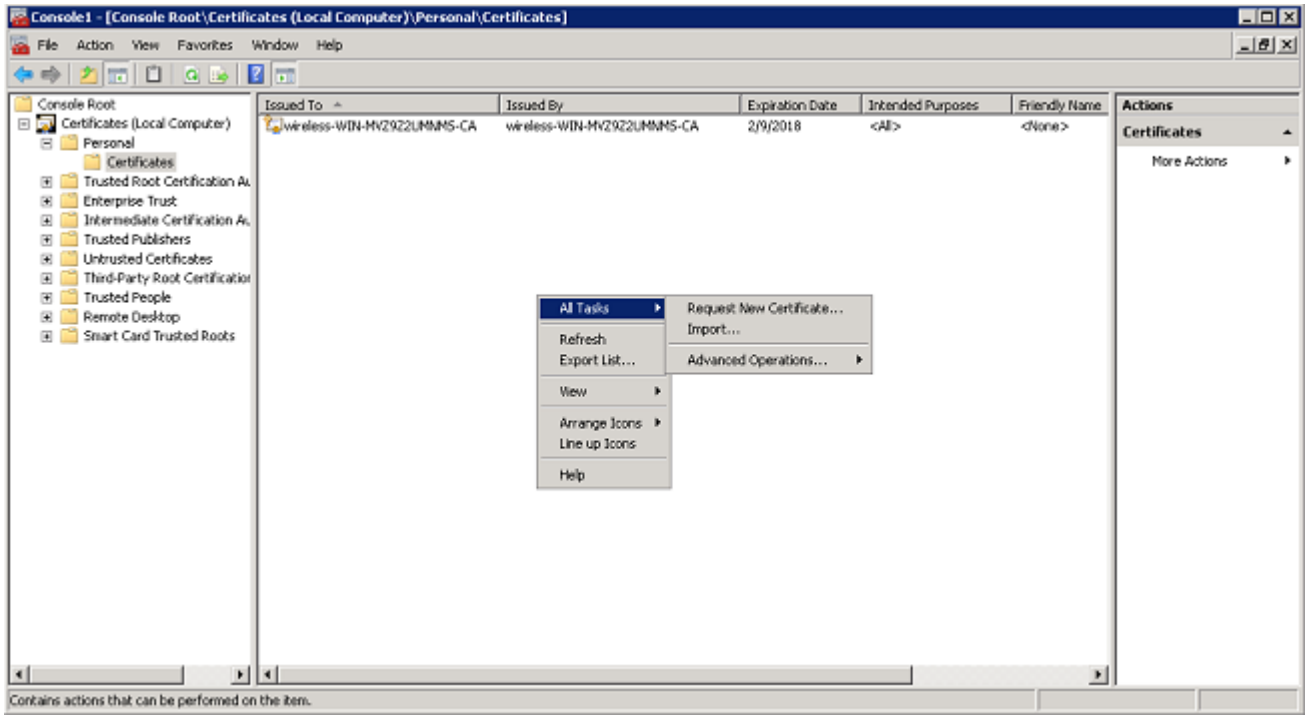
6. Cliquez sur OK pour revenir à la console MMC (Microsoft Management Console).



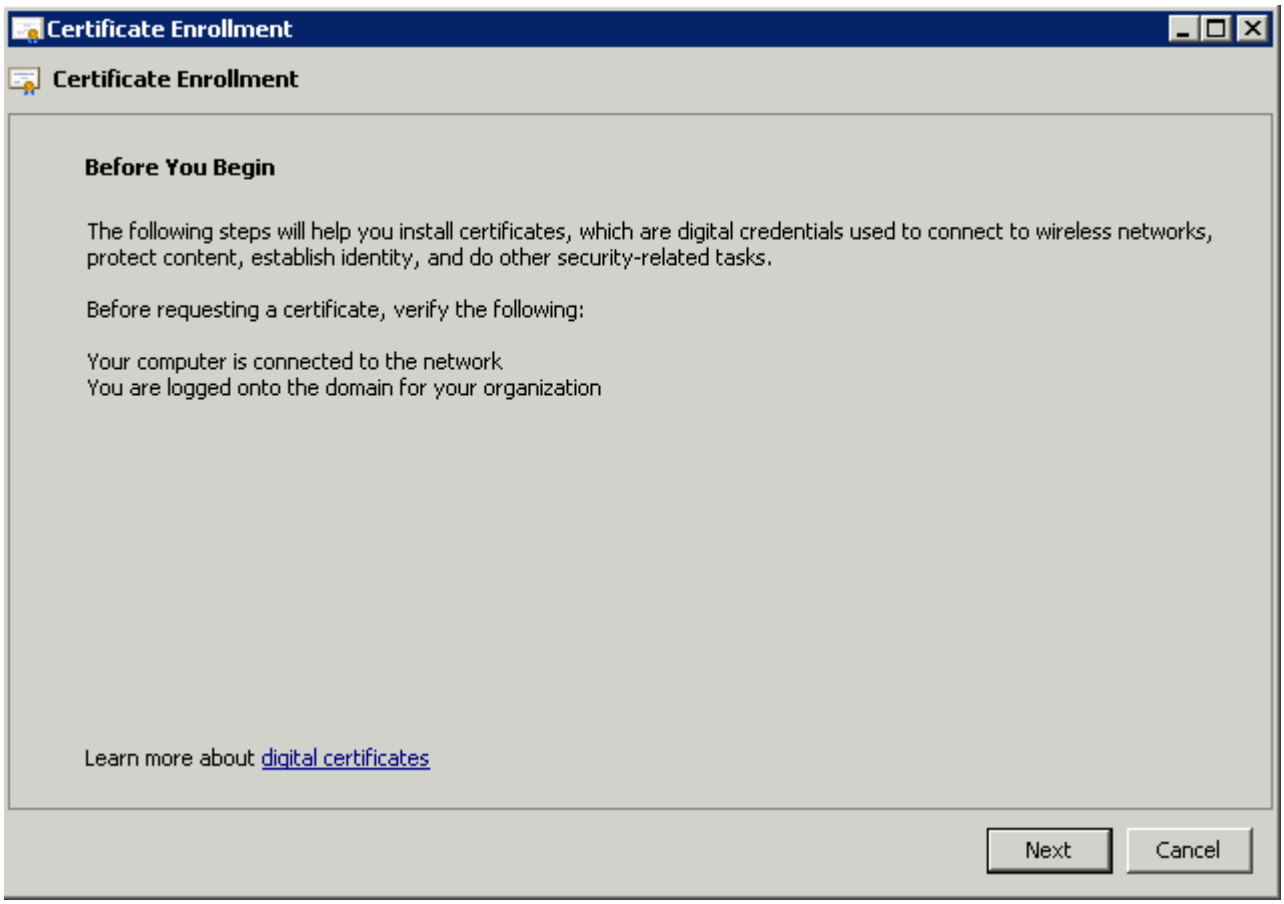
7. Développez les dossiers Certificates (Local Computer) et Personal, puis cliquez sur Certificates.



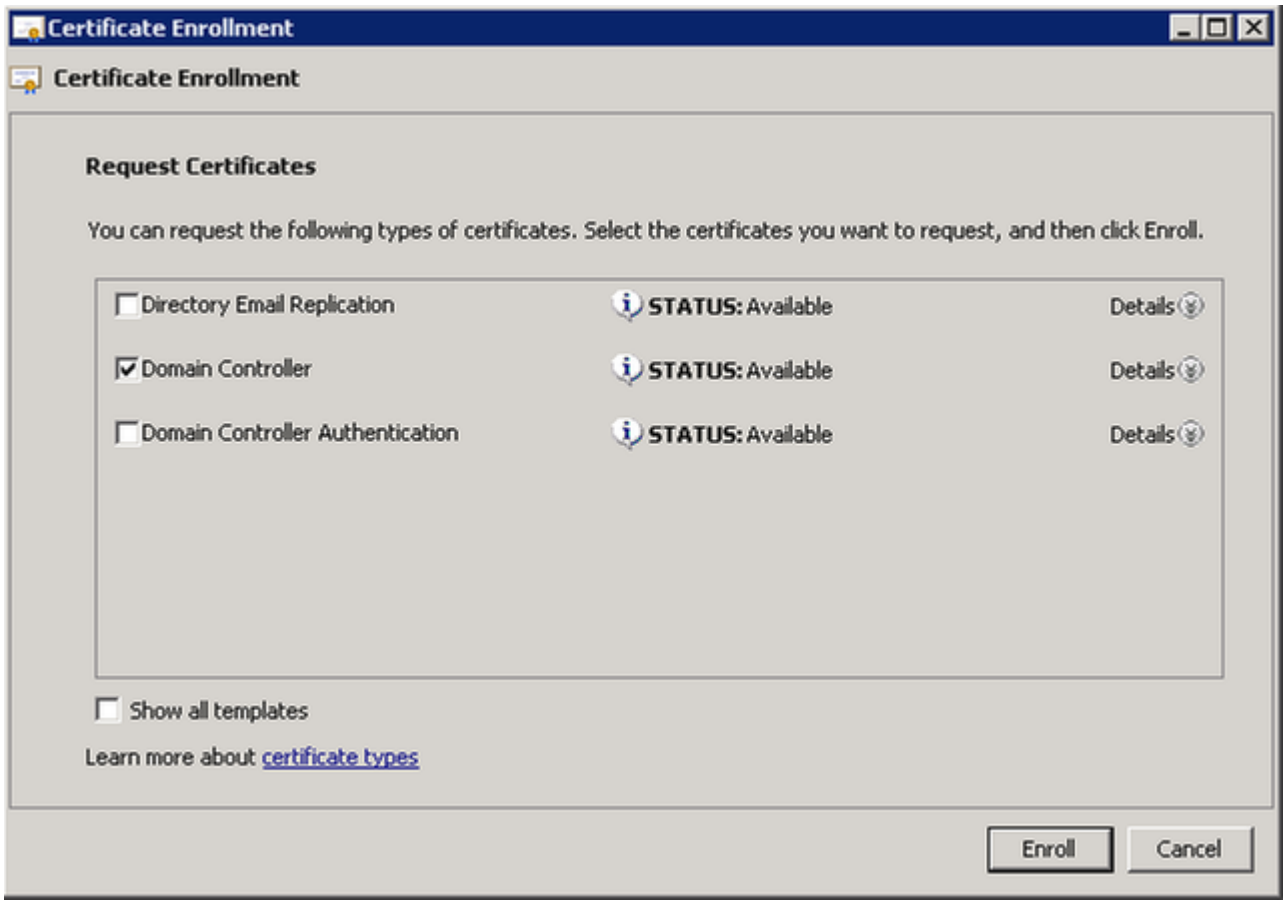
8. Cliquez avec le bouton droit dans l'espace blanc sous le certificat CA, et choisissez Toutes les tâches > Demander un nouveau certificat.



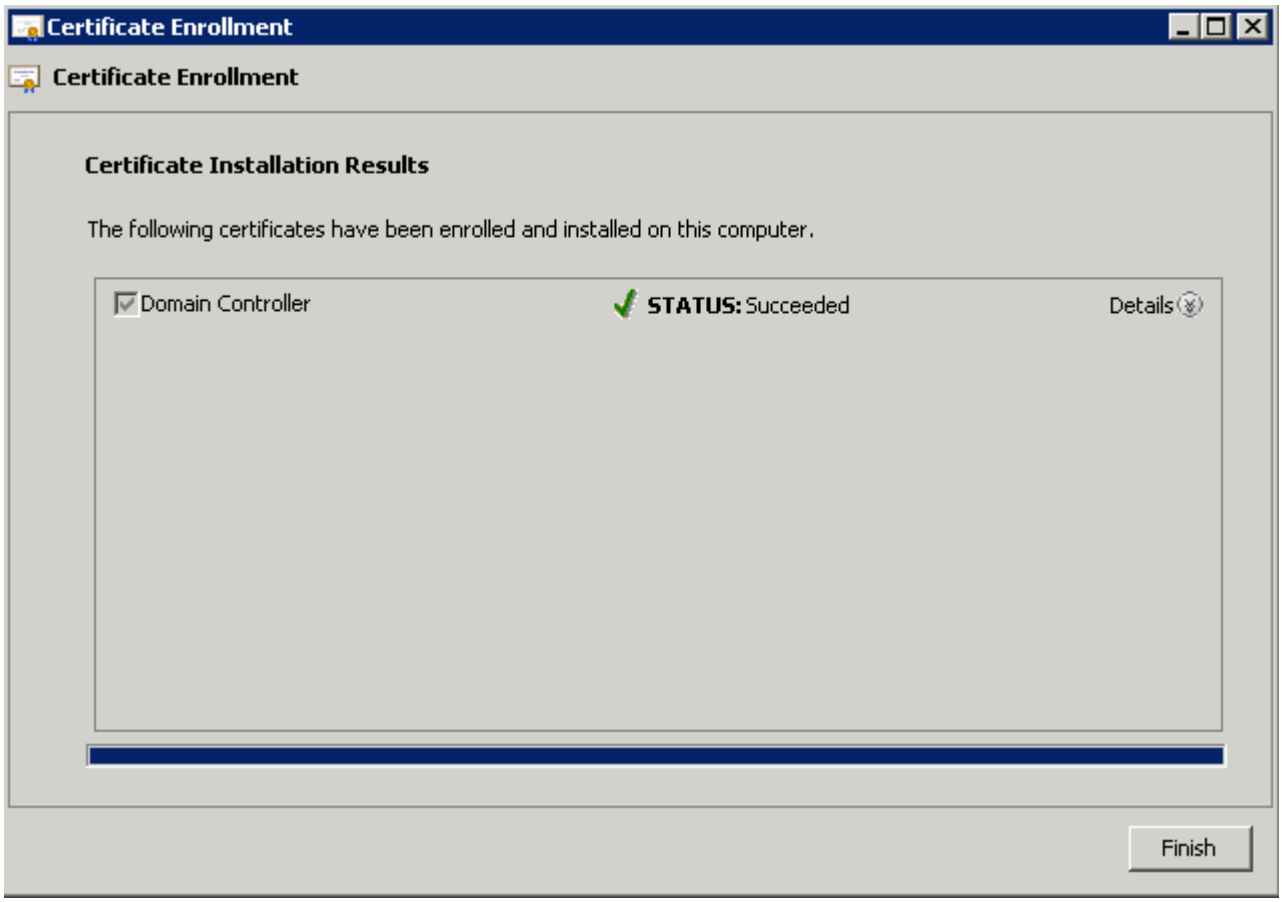
9. Cliquez sur Next (Suivant).



10. Sélectionnez Domain Controller, puis cliquez sur Enroll.

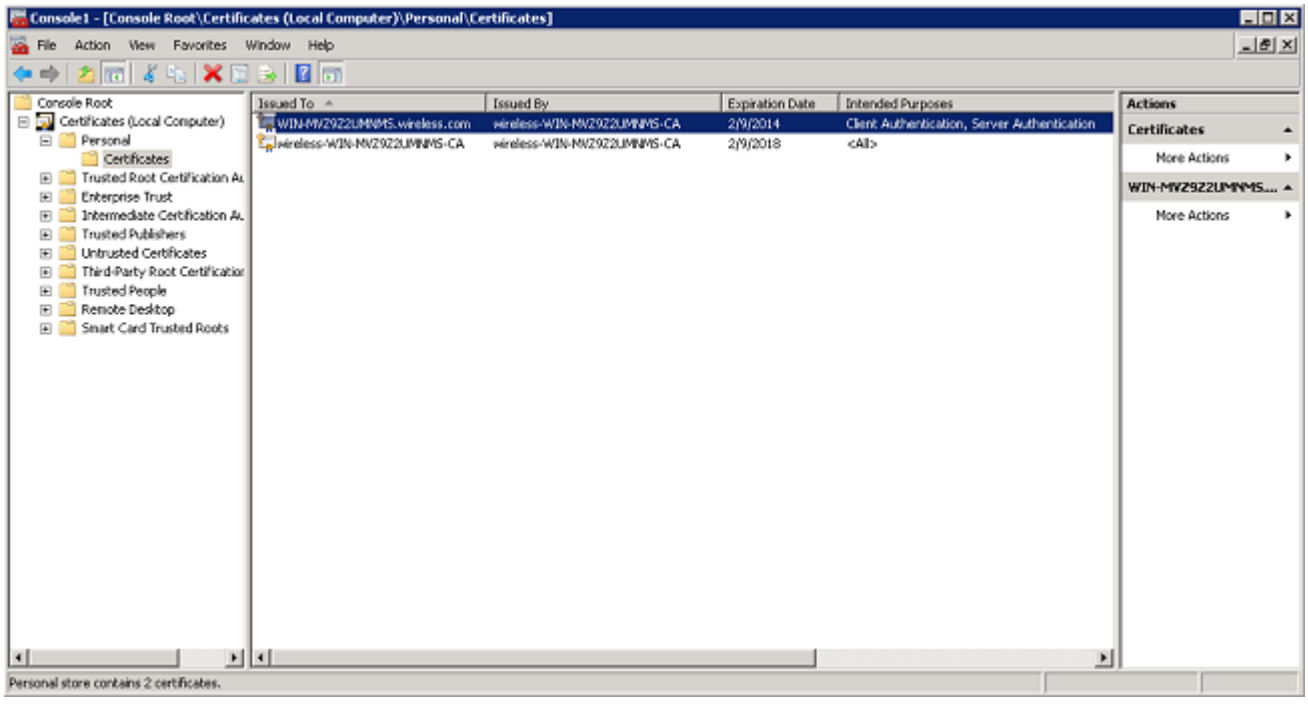


11. Cliquez sur Terminer une fois le certificat installé.



Le certificat NPS est maintenant installé.

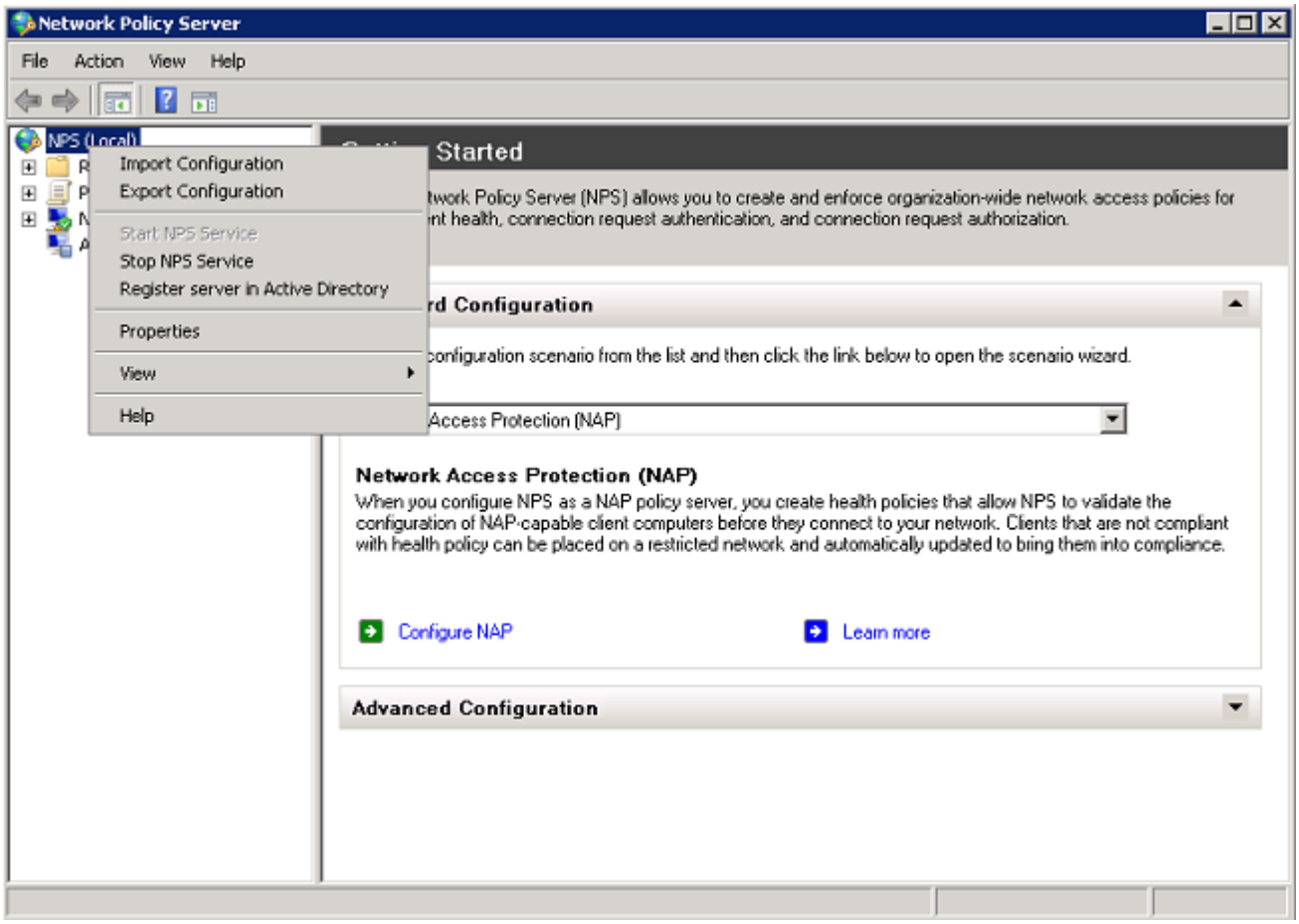
12. Assurez-vous que le champ Fonction prévue du certificat indique Authentification du client, Authentification du serveur.



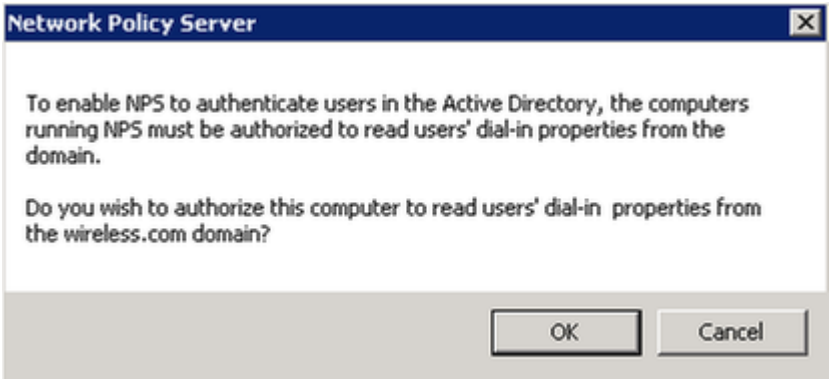
Configurer le service Serveur de stratégie réseau pour l'authentification PEAP-MS-CHAP v2

Complétez ces étapes afin de configurer le NPS pour l'authentification :

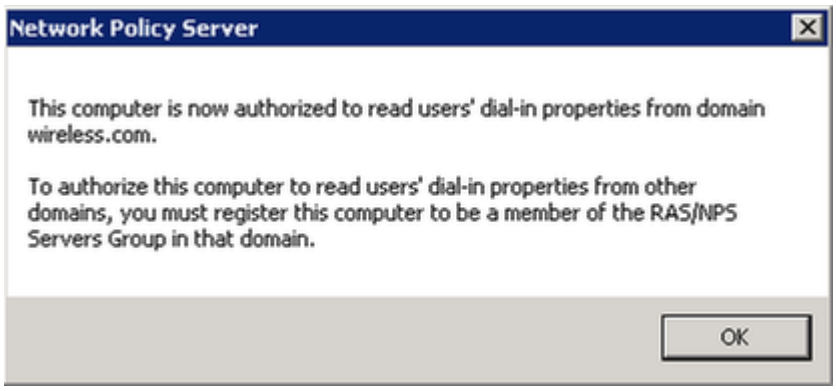
1. Cliquez sur Démarrer > Outils d'administration> Serveur de stratégie réseau.
2. Cliquez avec le bouton droit sur NPS (Local), puis choisissez Register server in Active Directory.



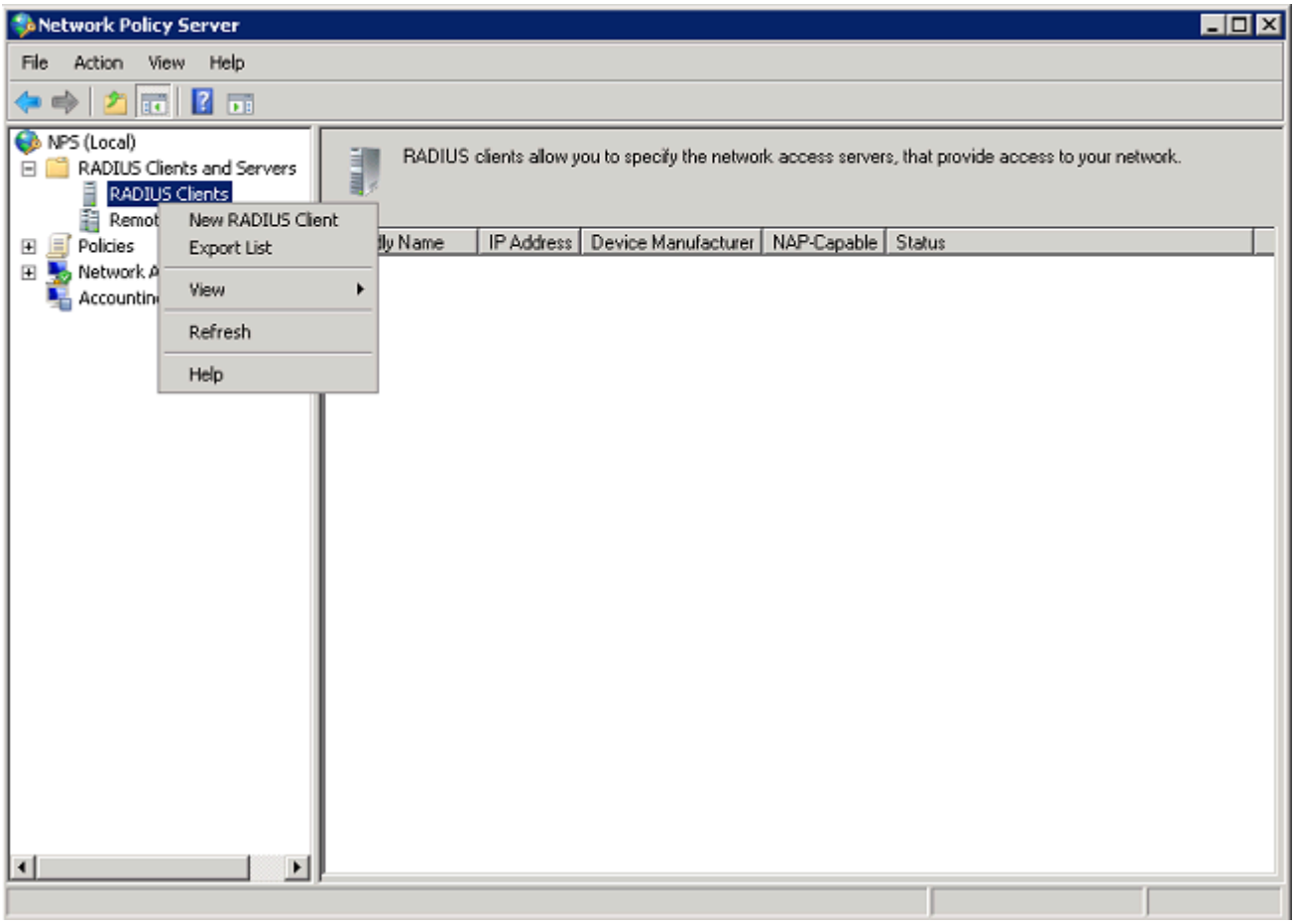
3. Click OK.



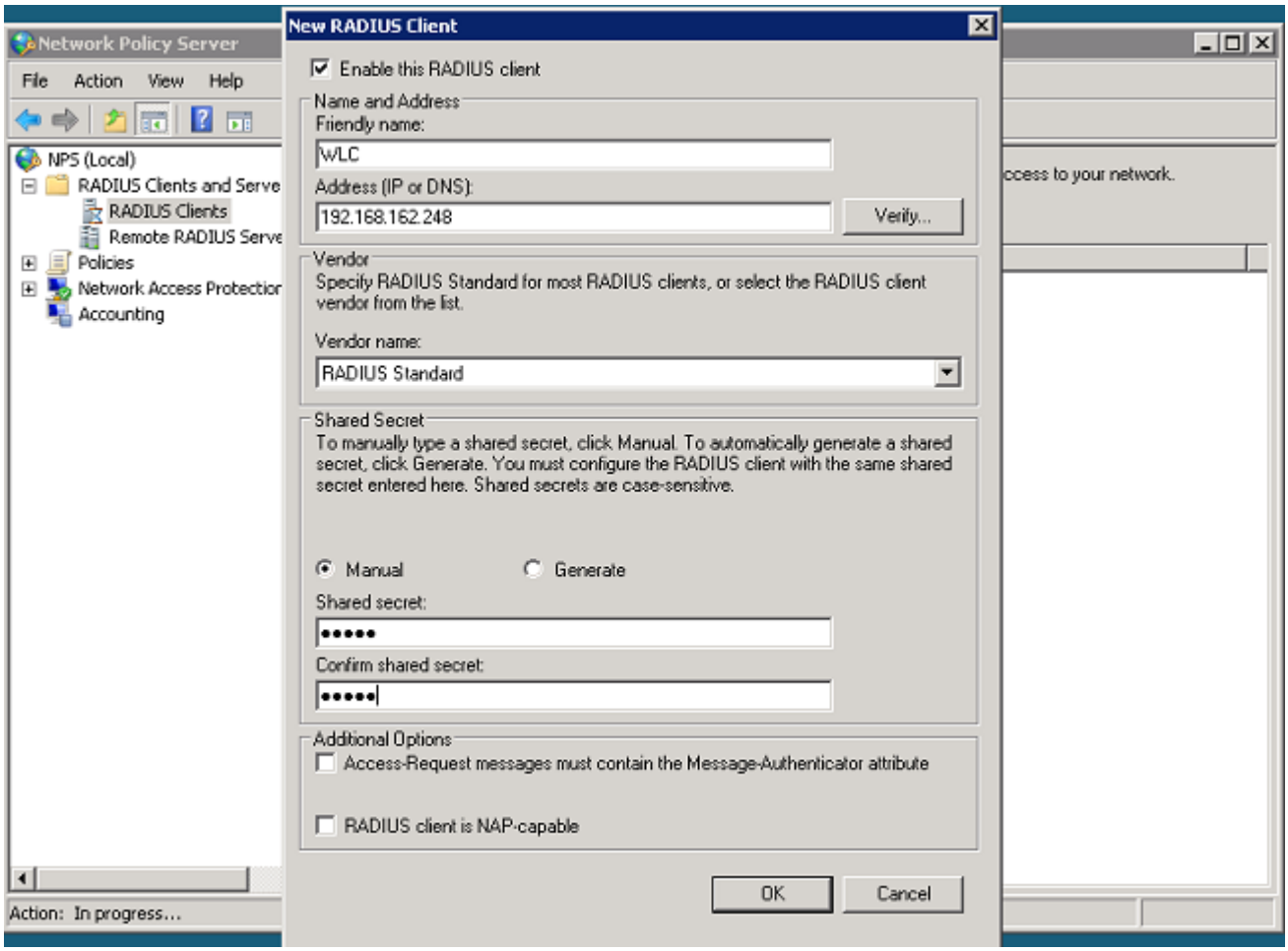
4. Click OK.



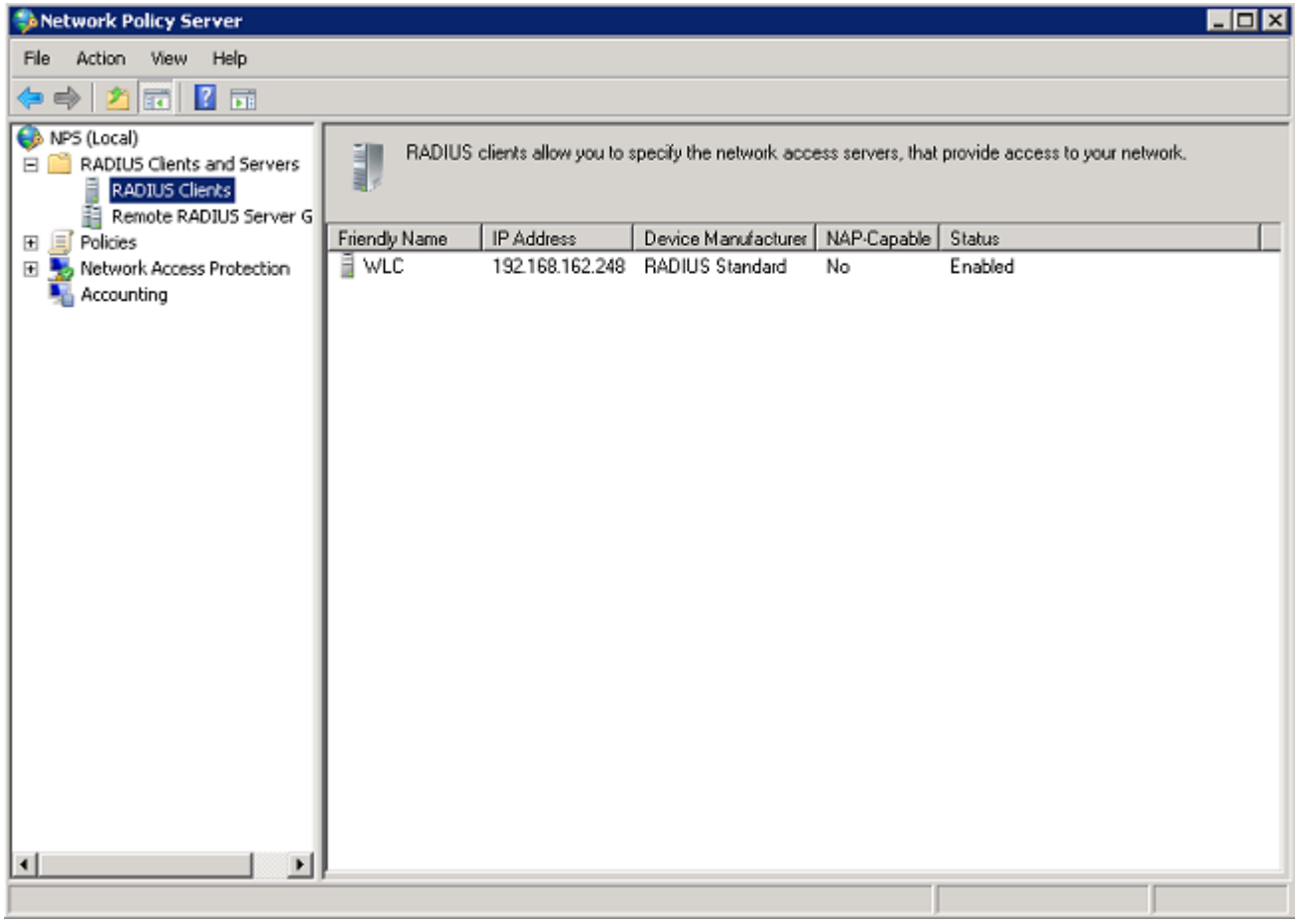
5. Ajoutez le contrôleur LAN sans fil en tant que client AAA (Authentication, Authorization, and Accounting) sur le NPS.
6. Développez Clients et serveurs RADIUS. Cliquez à droite sur RADIUS Clients, puis choisissez New RADIUS Client.



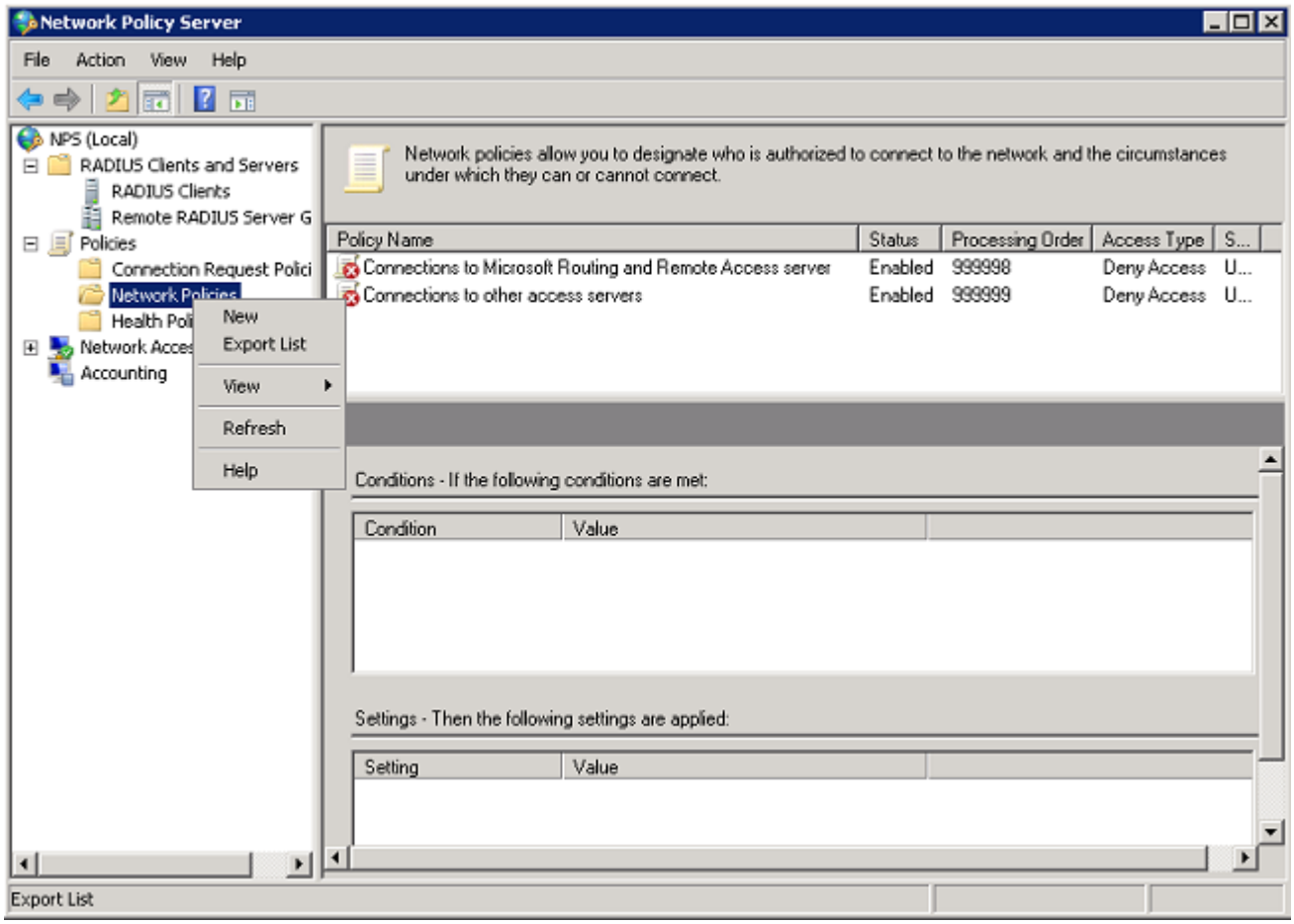
7. Entrez un nom convivial (WLC dans cet exemple), l'adresse IP de gestion du WLC (192.168.162.248 dans cet exemple) et un secret partagé. Le même secret partagé est utilisé pour configurer le WLC.



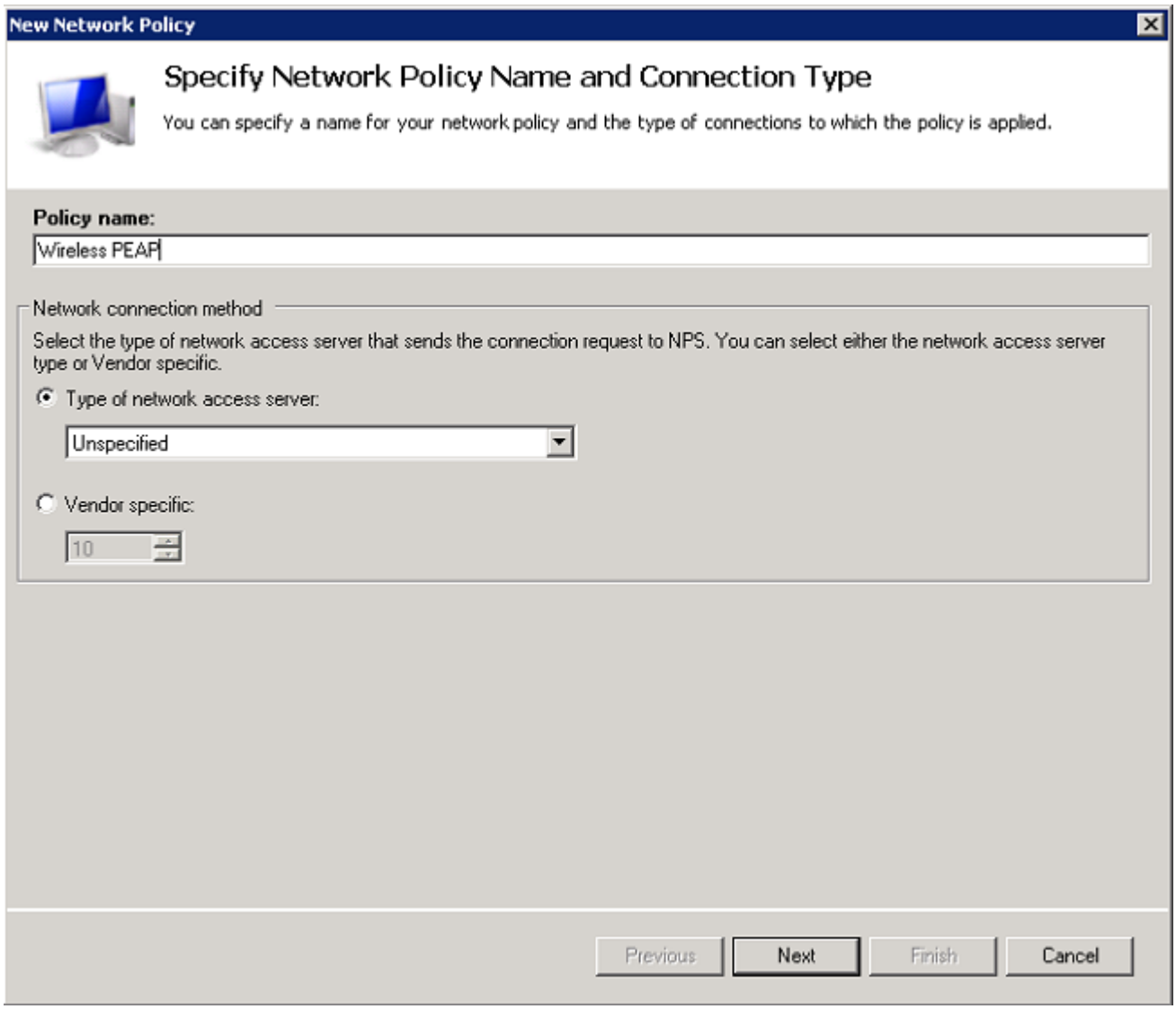
8. Cliquez sur OK pour revenir à l'écran précédent.



9. Créez une nouvelle stratégie réseau pour les utilisateurs sans fil. Développez Policies, cliquez avec le bouton droit sur Network Policies, puis choisissez New.

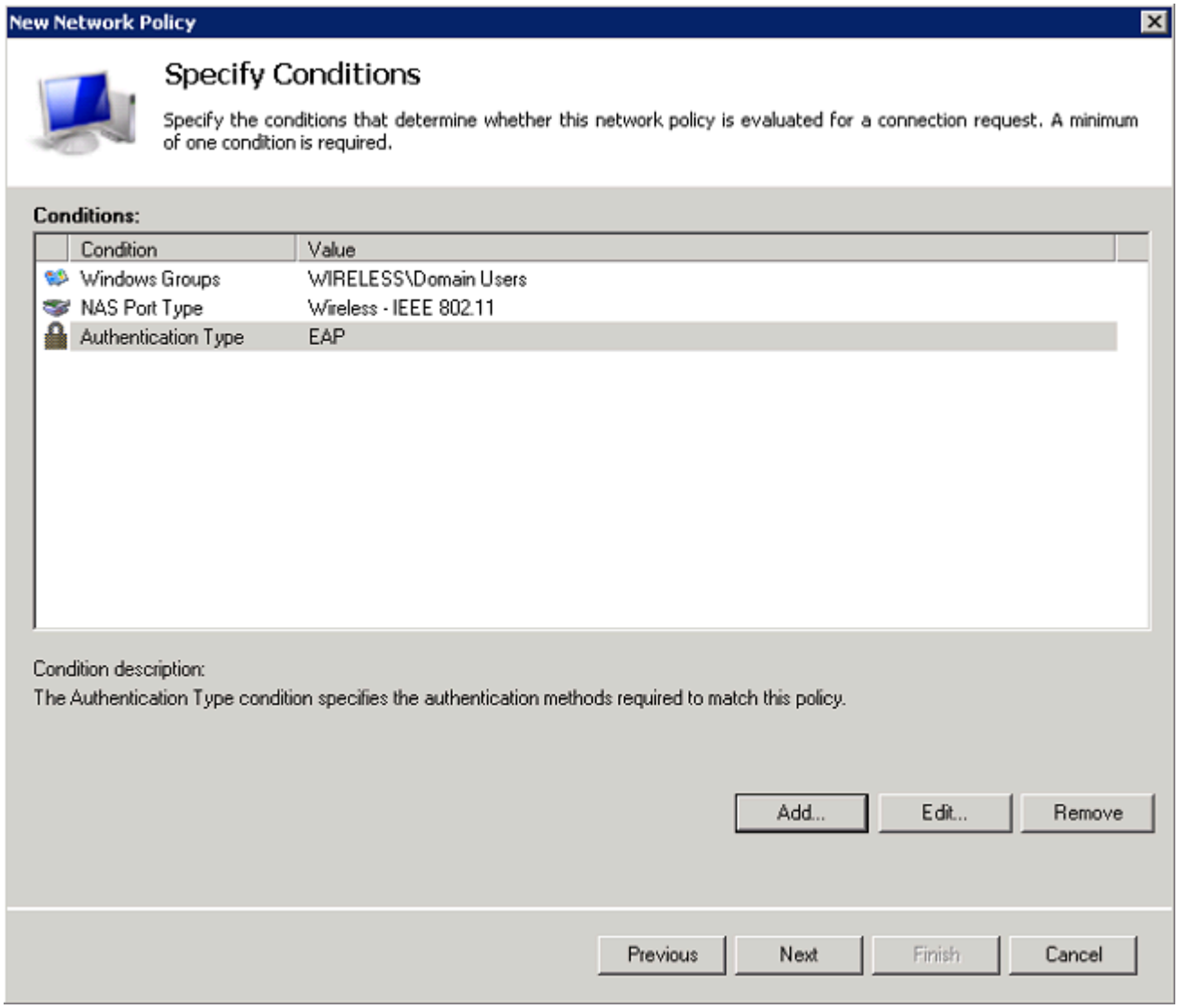


10. Entrez un nom de stratégie pour cette règle (PEAP sans fil, dans cet exemple), et cliquez sur Next.

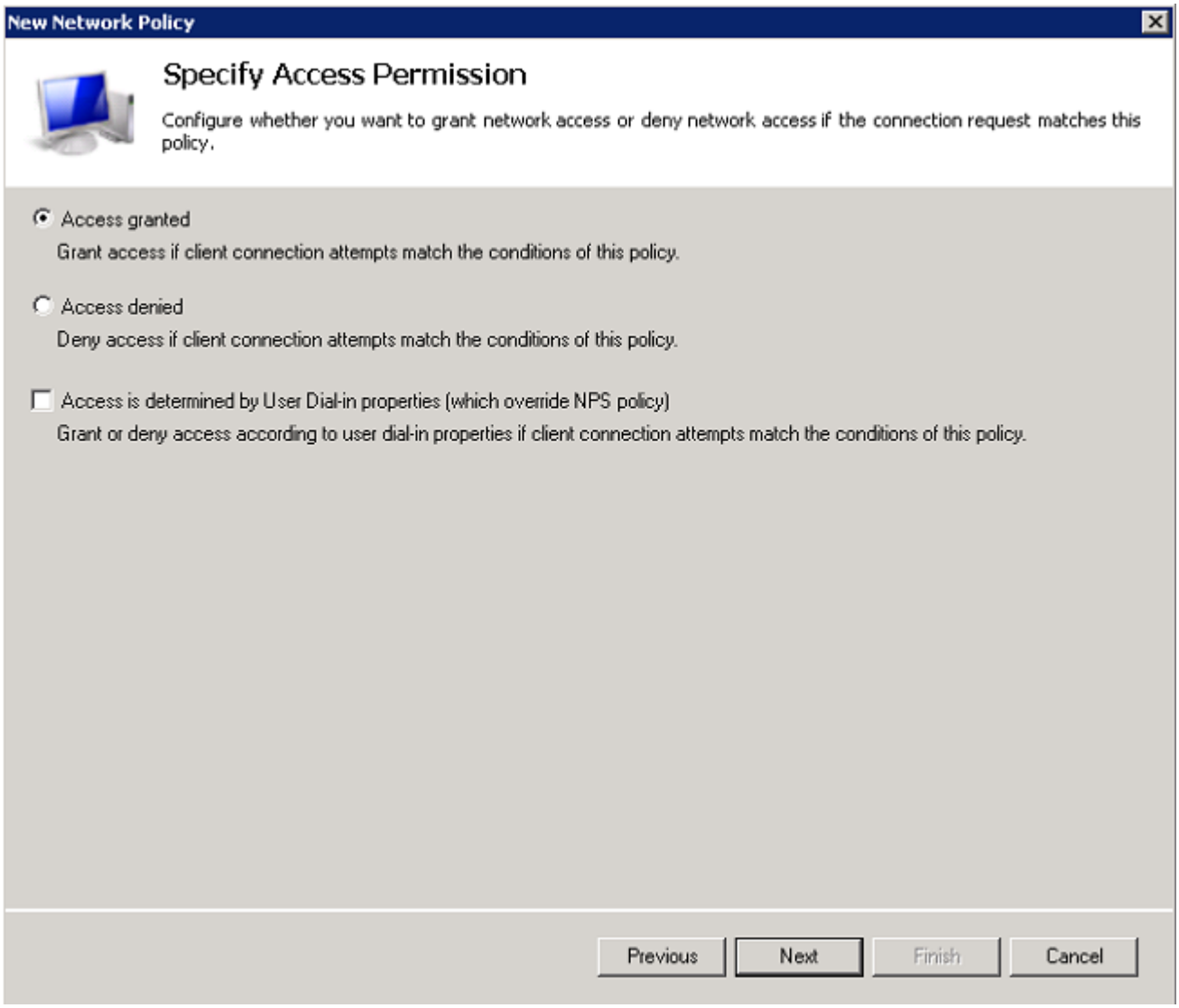


11. Pour que cette stratégie autorise uniquement les utilisateurs de domaine sans fil, ajoutez ces trois conditions, et cliquez sur Next :

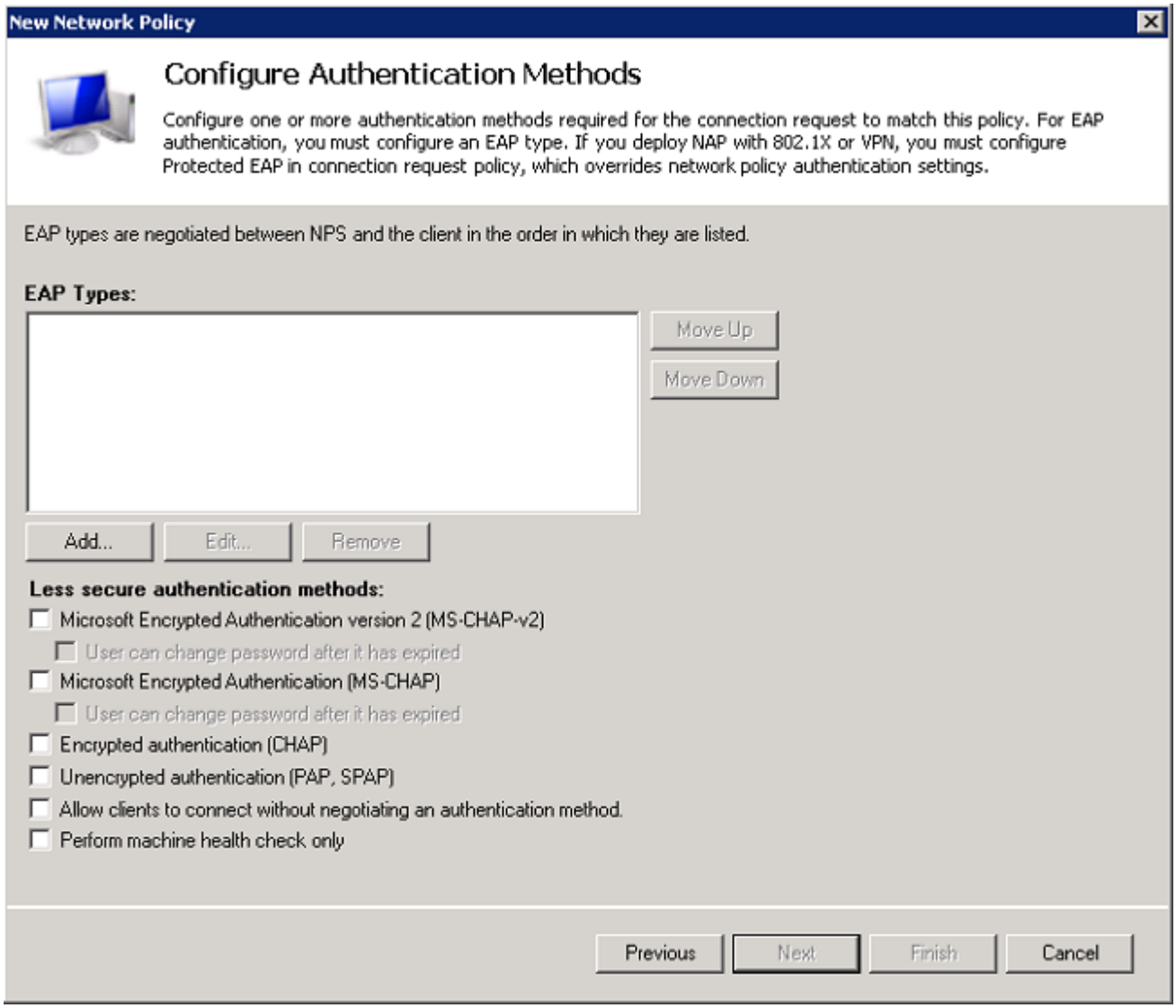
    - Groupes Windows - Utilisateurs du domaine
    - Type de port NAS - Sans fil - IEEE 802.11
    - Type d'authentification - EAP



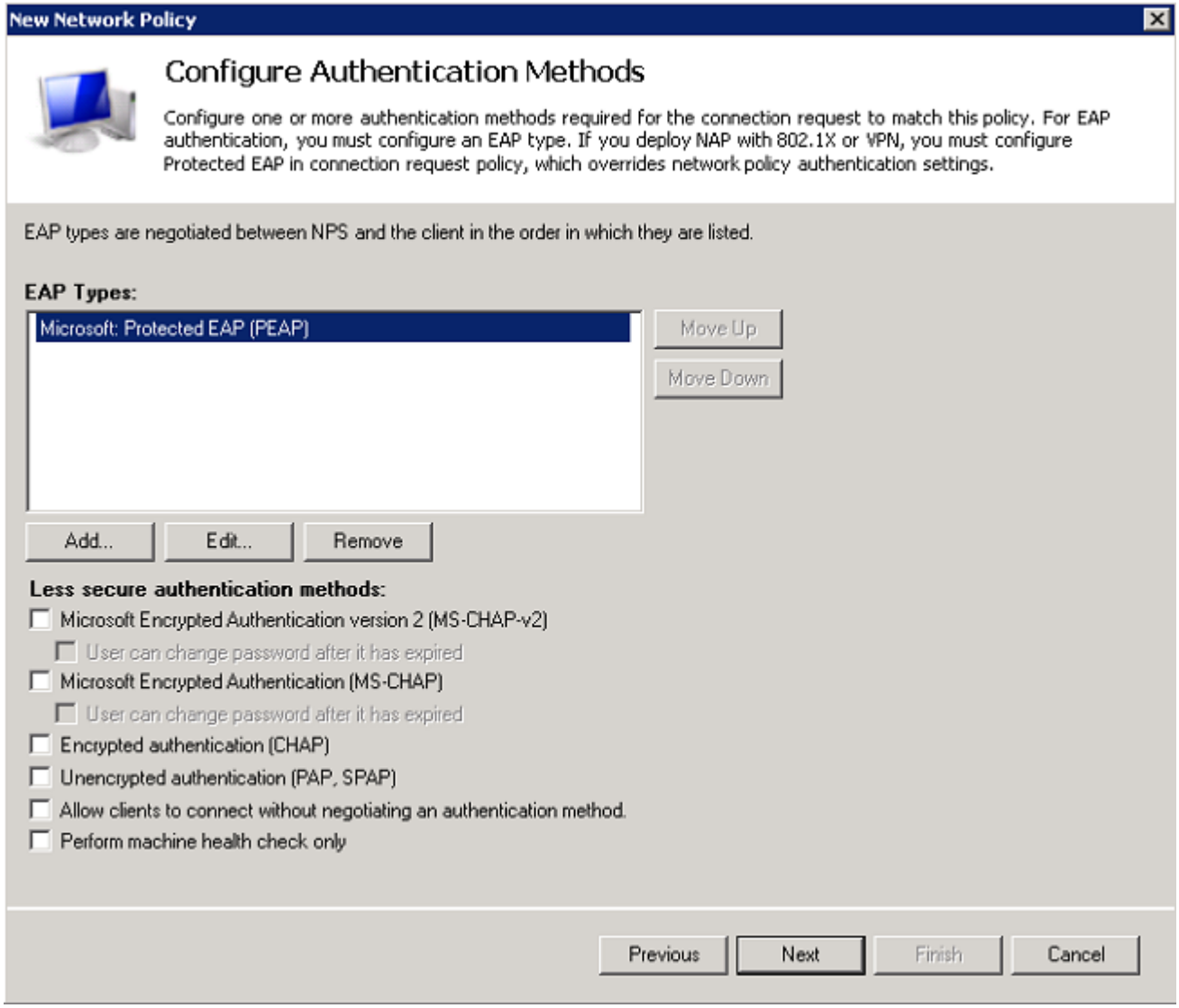
12. Cliquez sur Accès accordé pour accorder des tentatives de connexion qui correspondent à cette stratégie, puis cliquez sur Suivant.



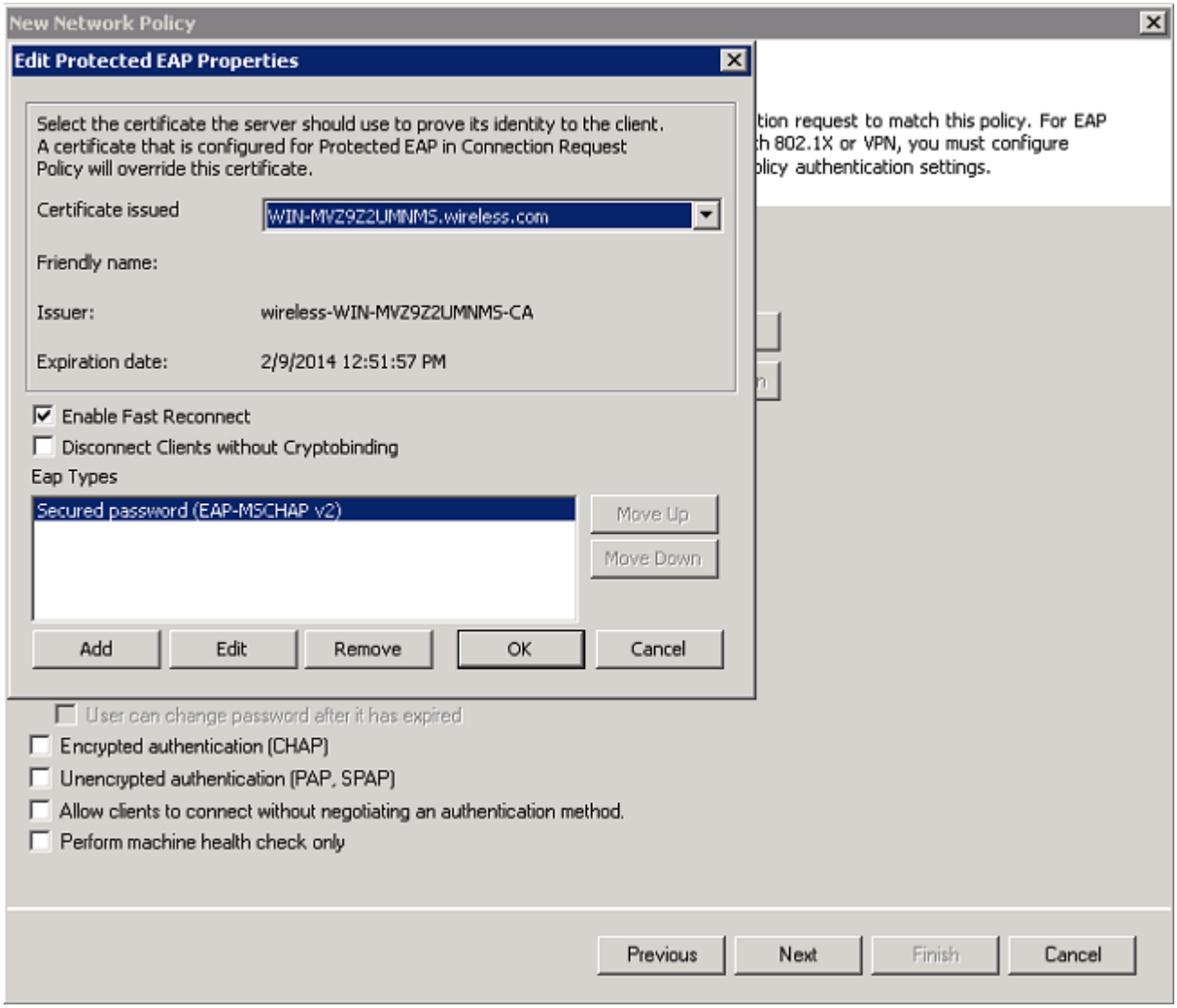
13. Désactivez toutes les méthodes d'authentification sous Méthodes d'authentification moins sécurisées.



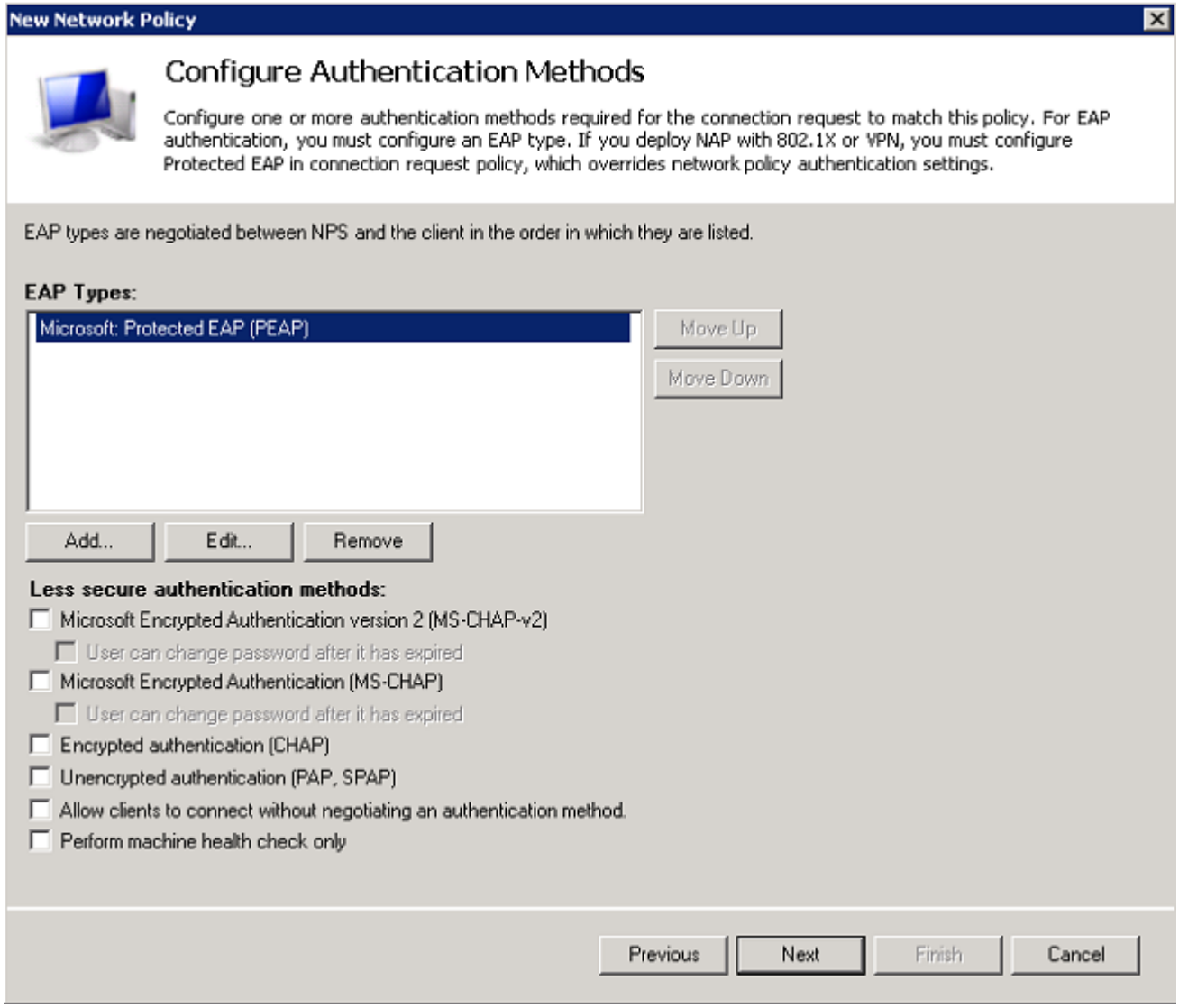
14. Cliquez sur Add, sélectionnez PEAP, puis cliquez sur OK pour activer PEAP.



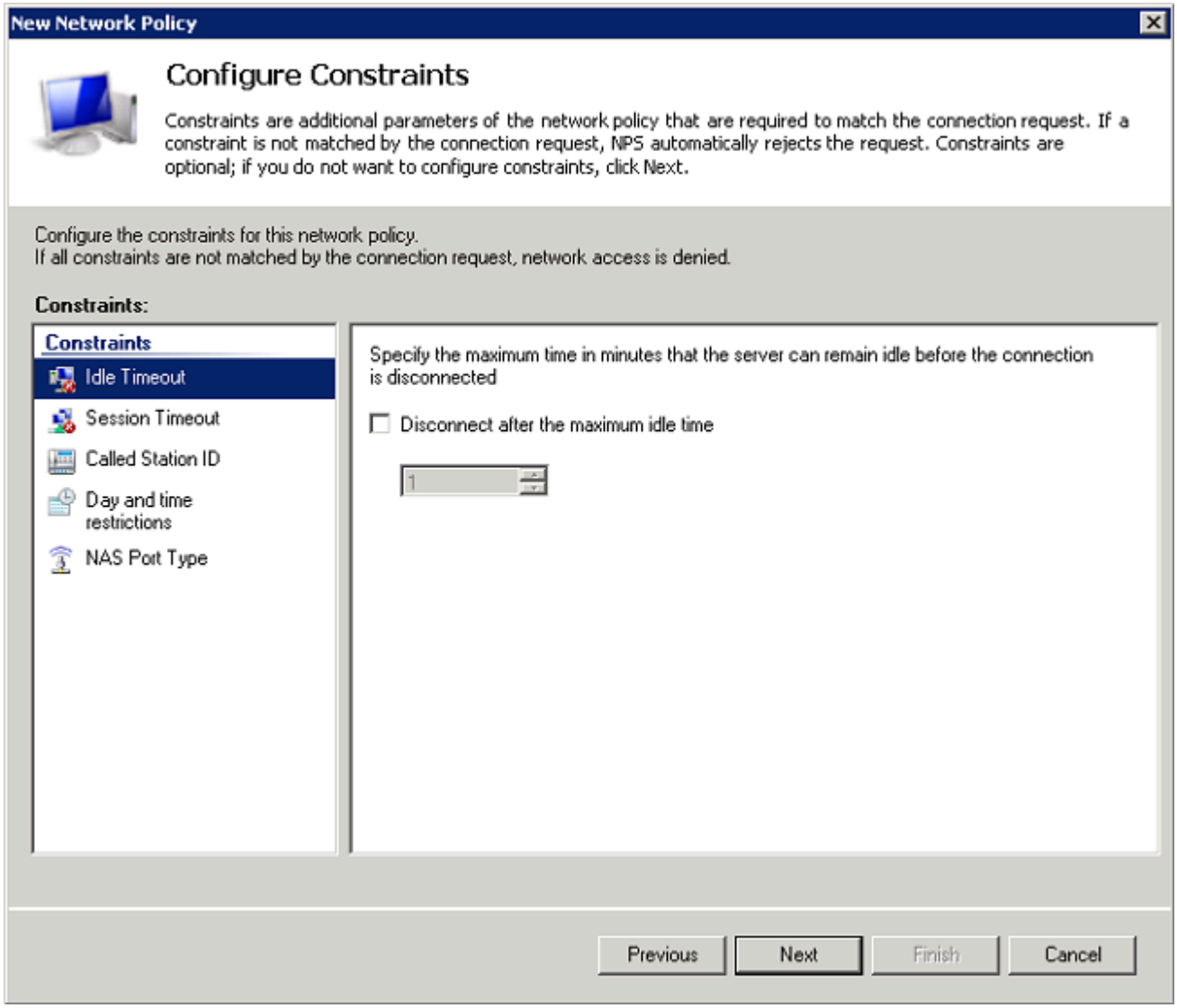
15. Sélectionnez Microsoft : Protected EAP (PEAP), puis cliquez sur Edit. Assurez-vous que le certificat de contrôleur de domaine précédemment créé est sélectionné dans la liste déroulante Certificate Issué, et cliquez sur OK.



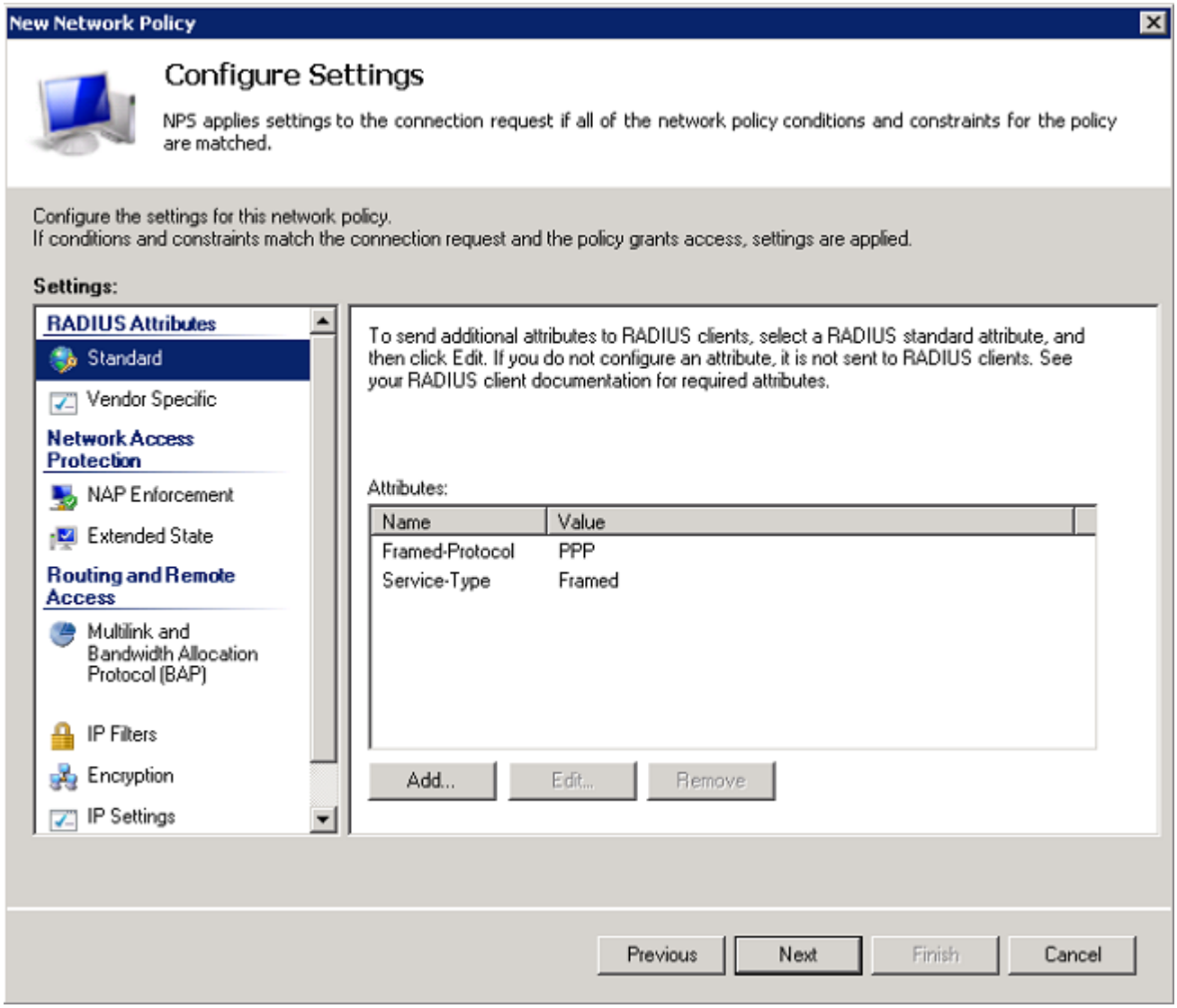
16. Cliquez sur Next (Suivant).



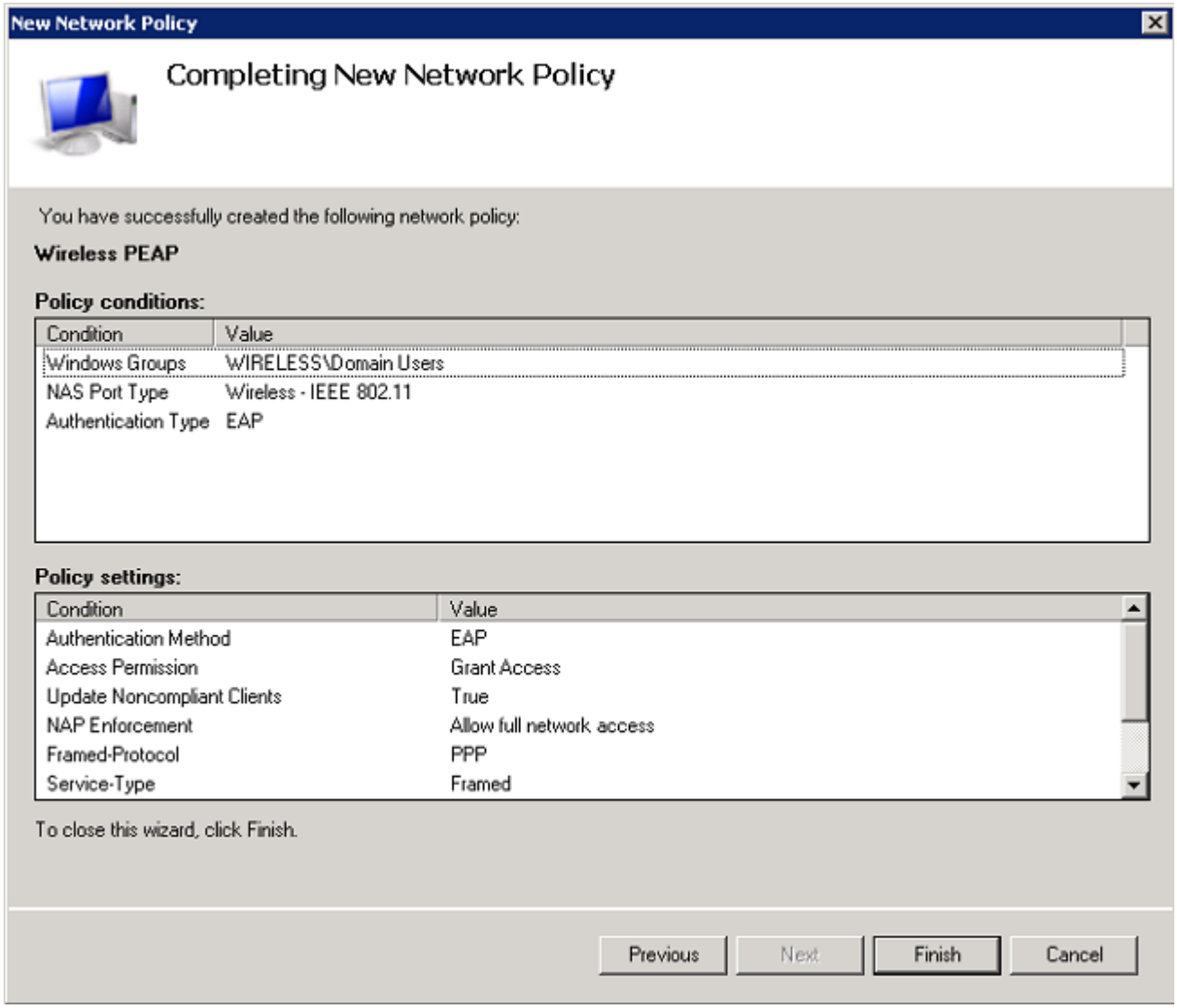
17. Cliquez sur Next (Suivant).



18. Cliquez sur Next (Suivant).



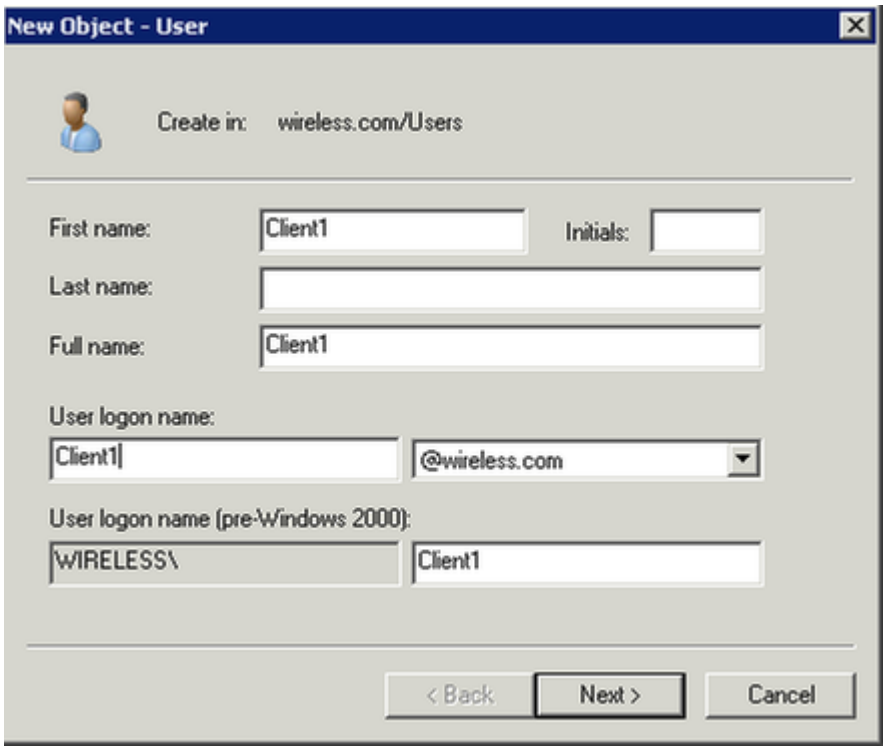
19. Cliquez sur Finish (Terminer).



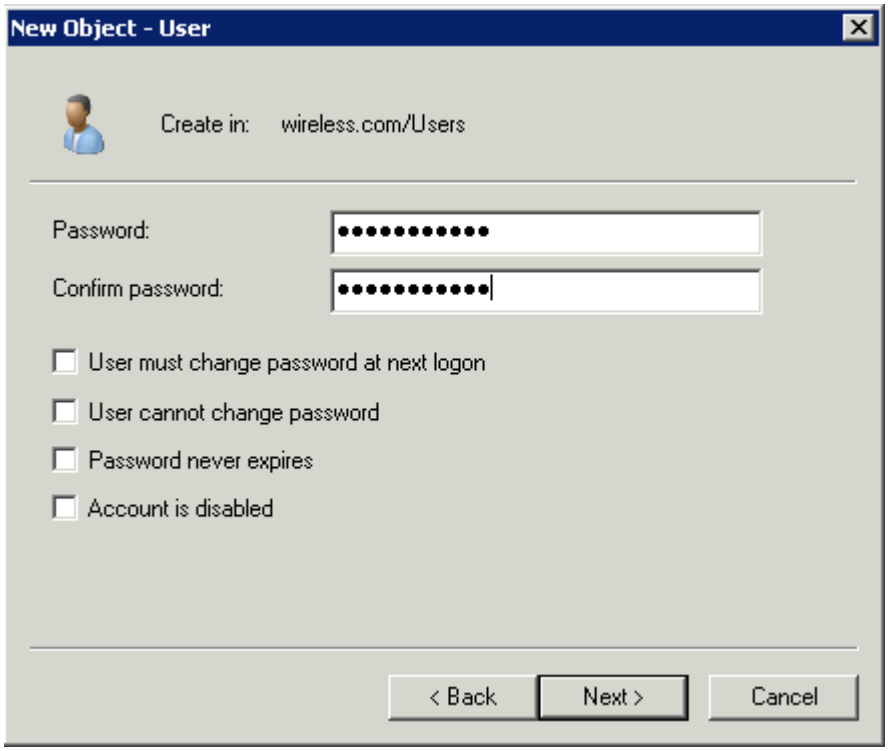
Ajoutez les utilisateurs à l'Active Directory

Dans cet exemple, la base de données utilisateur est gérée dans Active Directory. Effectuez ces étapes afin d'ajouter des utilisateurs à la base de données Active Directory :

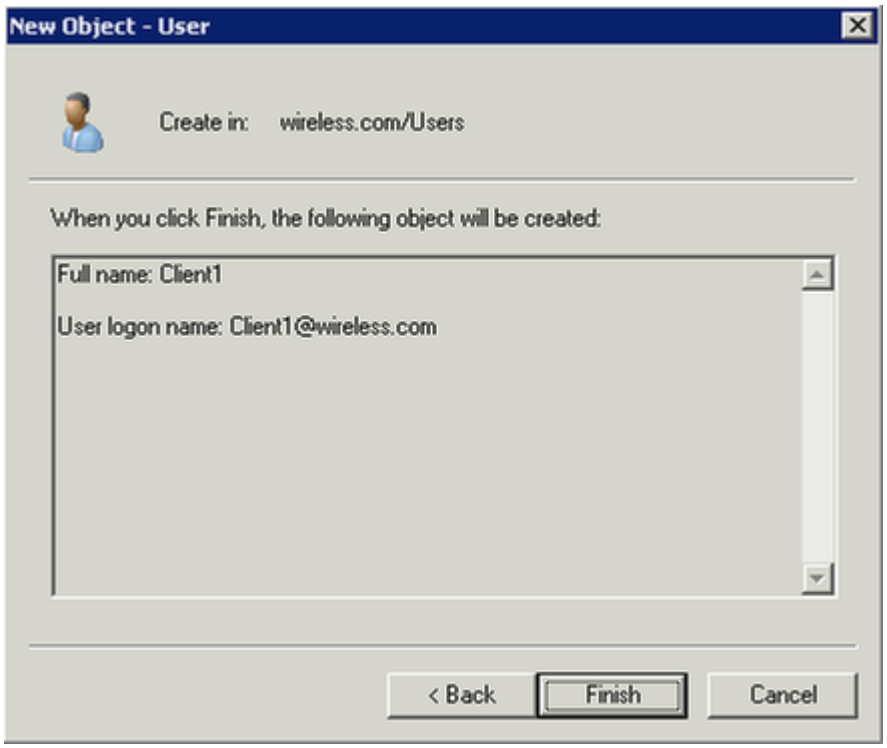
1. Ouvrez Utilisateurs et ordinateurs Active Directory. Cliquez sur Démarrer> Outils d'administration> Utilisateurs et ordinateurs Active Directory.
2. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, développez le domaine, cliquez avec le bouton droit sur Utilisateurs> Nouveau, puis choisissez Utilisateur.
3. Dans la boîte de dialogue Nouvel objet - Utilisateur, entrez le nom de l'utilisateur sans fil. Cet exemple utilise le nom Client1 dans le champ Prénom et Client1 dans le champ Nom d'ouverture de session utilisateur. Cliquez sur Next (Suivant).



4. Dans la boîte de dialogue Nouvel objet - Utilisateur, entrez un mot de passe de votre choix dans les champs Mot de passe et Confirmer le mot de passe. Assurez-vous que la case User must change password at next logon n'est pas cochée, puis cliquez sur Next.



5. Dans le nouvel objet - boîte de dialogue d'utilisateur, cliquez sur Finish.



6. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

Configuration du contrôleur LAN sans fil et des LAP

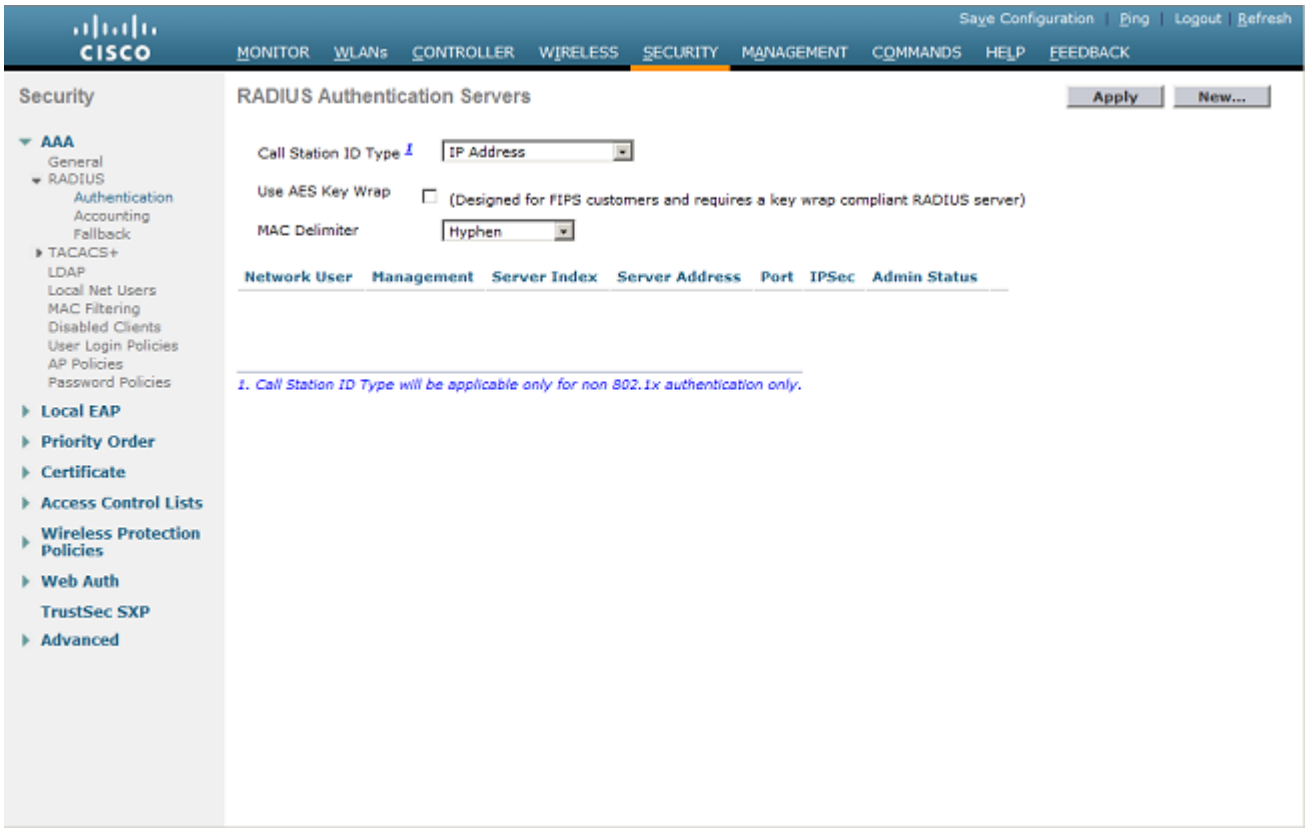
Configurez les périphériques sans fil (les contrôleurs LAN sans fil et les LAP) pour cette configuration.

Configurer le WLC pour l'authentification RADIUS

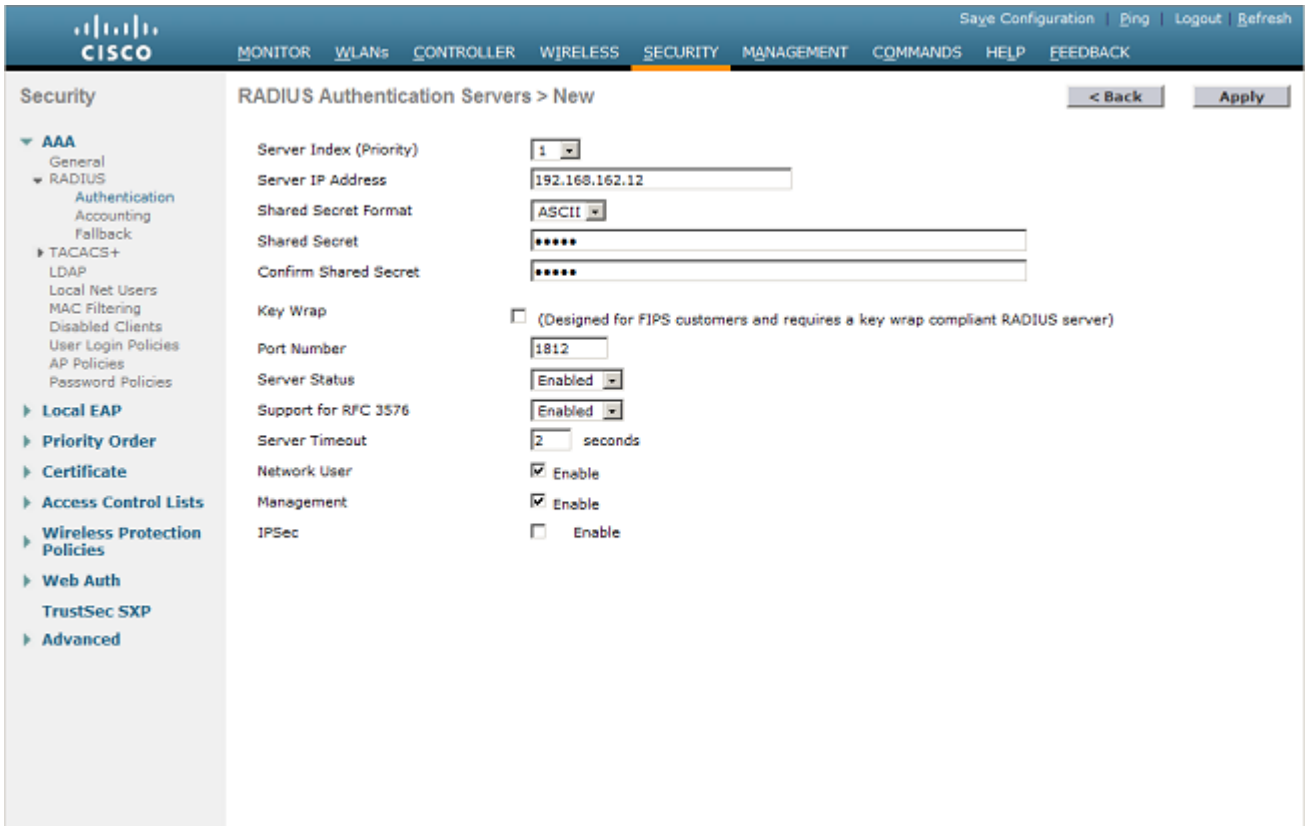
Configurez le WLC pour utiliser le NPS comme serveur d'authentification. Le WLC doit être configuré afin de transférer les informations d'identification de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide alors les identifiants de l'utilisateur et permet d'accéder aux clients sans fil.

Complétez ces étapes afin d'ajouter le NPS en tant que serveur RADIUS dans la page Security > RADIUS Authentication :

1. Choisissez Security> RADIUS > Authentication dans l'interface du contrôleur pour afficher la page RADIUS Authentication Servers. Cliquez sur New afin de définir un serveur RADIUS.



2. Définissez les paramètres du serveur RADIUS. Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher Network User et Management déterminent si l'authentification RADIUS s'applique à la gestion et aux utilisateurs réseau (sans fil). Cet exemple utilise le NPS comme serveur RADIUS avec une adresse IP de 192.168.162.12. Cliquez sur Apply.



Configurez un WLAN pour les clients de routage

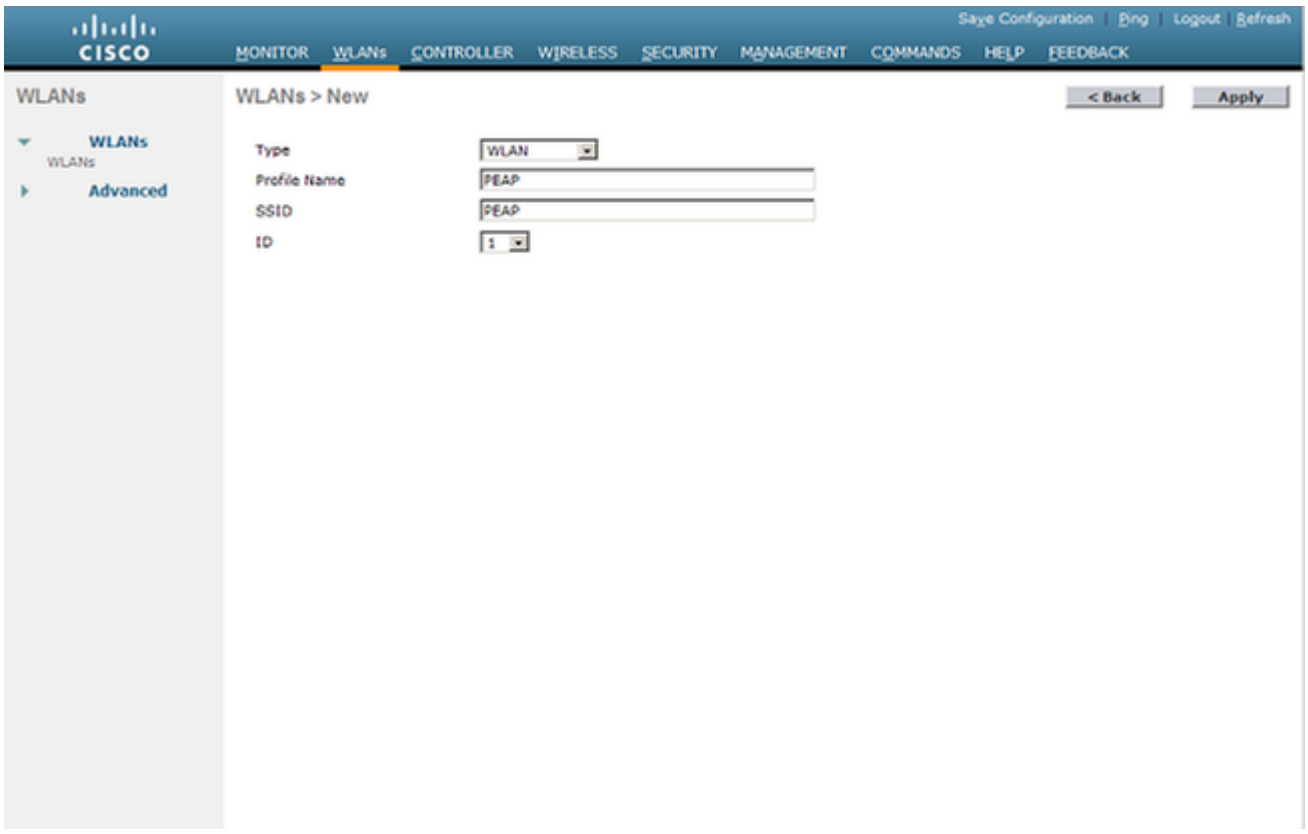
Configurez le SSID (Service Set Identifier) (WLAN) auquel les clients sans fil se connectent. Dans cet exemple, créez le SSID, puis nommez-le PEAP.

Définissez l'authentification de couche 2 en tant que WPA2 de sorte que les clients exécutent l'authentification basée sur EAP (PEAP-MS-CHAP v2 dans cet exemple) et utilisent la norme de chiffrement avancée (AES) comme mécanisme de chiffrement. Laissez toutes autres valeurs à leurs paramètres par défaut.

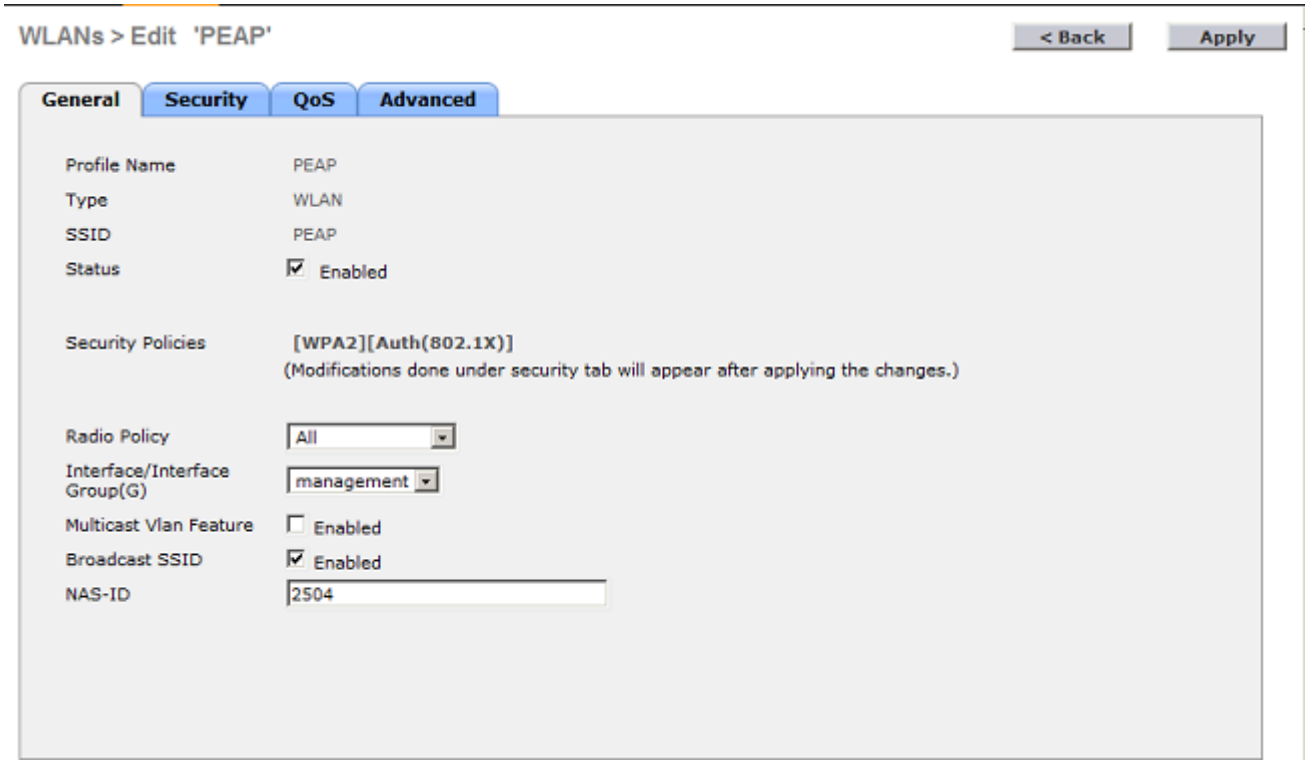
Remarque : Ce document relie le WLAN aux interfaces de gestion. Quand vous avez plusieurs VLAN dans votre réseau, vous pouvez créer un VLAN séparé et le relier au SSID. Pour les informations sur la façon de configurer des VLAN sur les WLC, reportez-vous aux VLAN sur l'exemple de configuration de contrôleurs LAN sans fil.

Complétez ces étapes afin de configurer un WLAN sur le WLC :

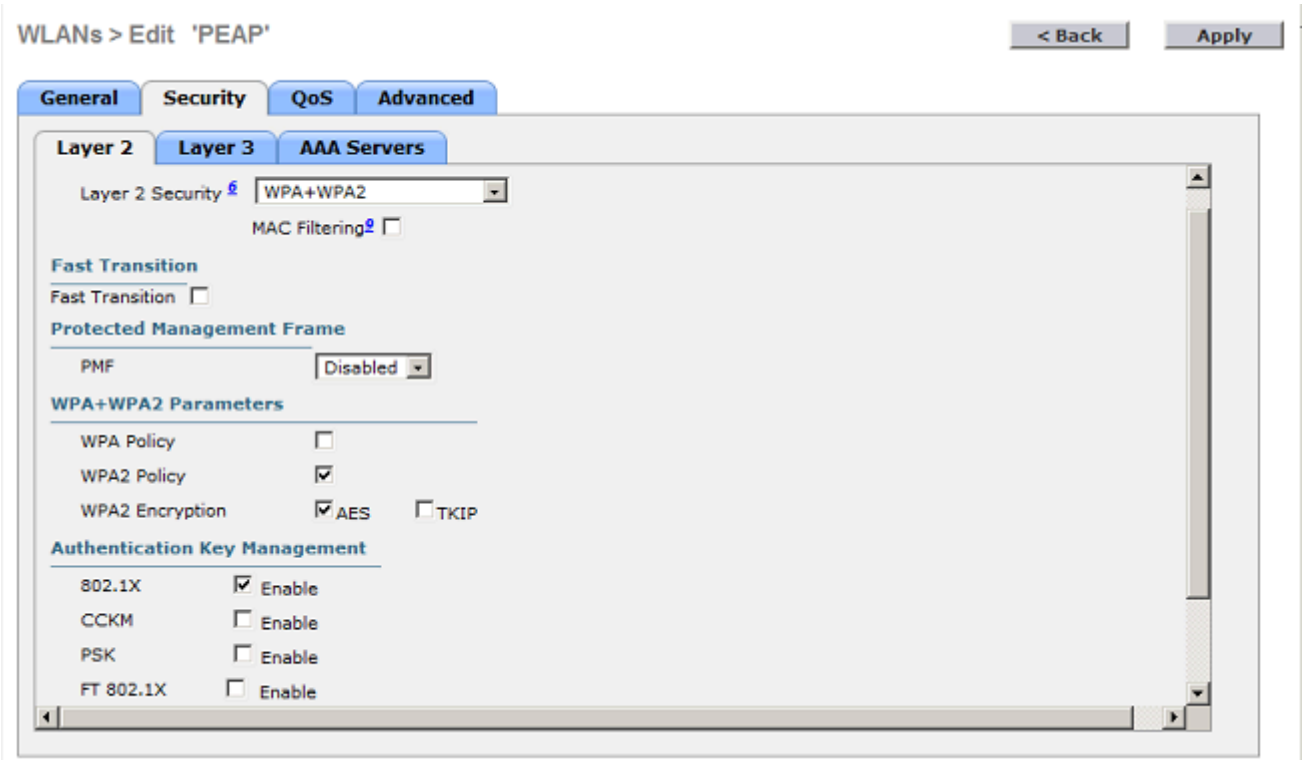
1. Cliquez sur WLANs à partir de l'interface du contrôleur afin d'afficher la page WLANs. Cette page énumère les WLAN qui existent sur le contrôleur.
2. Sélectionnez New afin de créer un nouveau WLAN. Saisissez l'ID WLAN et le SSID WLAN pour le WLAN, puis cliquez sur Apply.



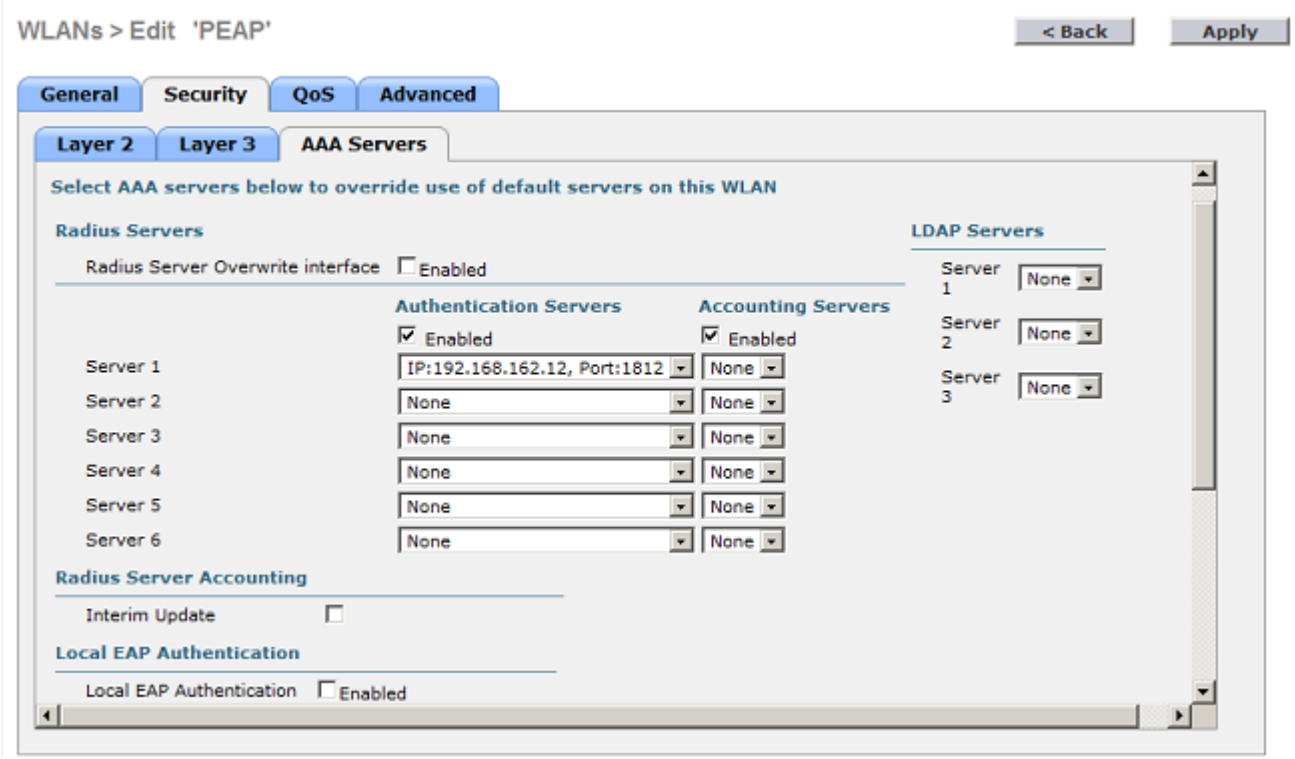
3. Pour configurer le SSID pour 802.1x, procédez comme suit :
    1. Cliquez sur l'onglet General et activez le WLAN.



2. Cliquez sur les onglets Security > Layer 2, définissez la sécurité de la couche 2 sur WPA + WPA2, cochez les cases WPA+WPA2 Parameters (par exemple, WPA2 AES) si nécessaire, et cliquez sur 802.1x comme Authentication Key Management.



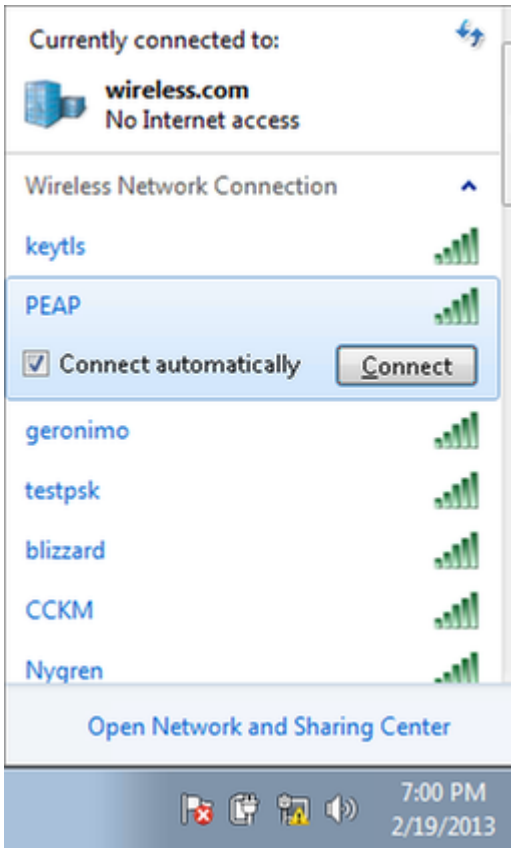
3. Cliquez sur les onglets Security > AAA Servers, choisissez l'adresse IP du NPS dans la liste déroulante Server 1, puis cliquez sur Apply.



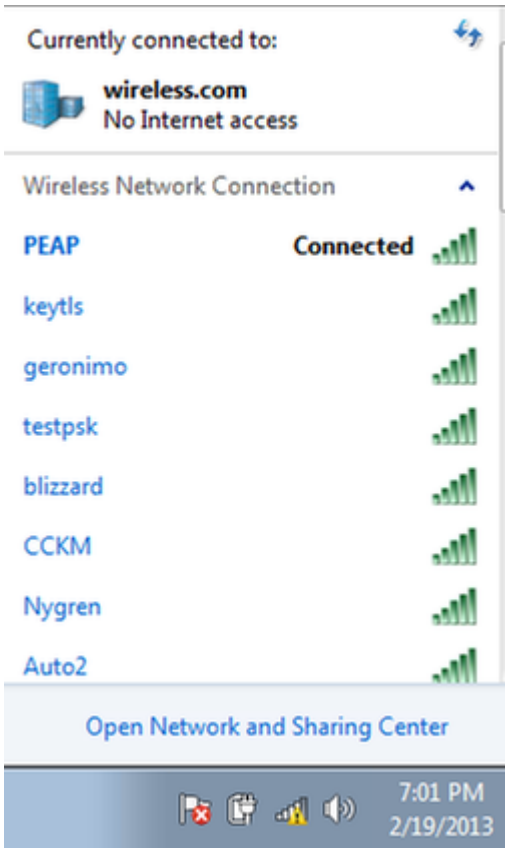
Configuration des clients sans fil pour l'authentification PEAP-MS-CHAP v2

Complétez ces étapes pour configurer le client sans fil avec l'outil Windows Zero Config Tool pour la connexion au WLAN PEAP.

1. Cliquez sur l'icône Réseau dans la barre des tâches. Cliquez sur le PEAP SSID, puis sur Connect.



2. Le client doit maintenant être connecté au réseau.



3. Si la connexion échoue, essayez de vous reconnecter au WLAN. Si le problème persiste, reportez-vous à la section Dépannage.

Vérifier

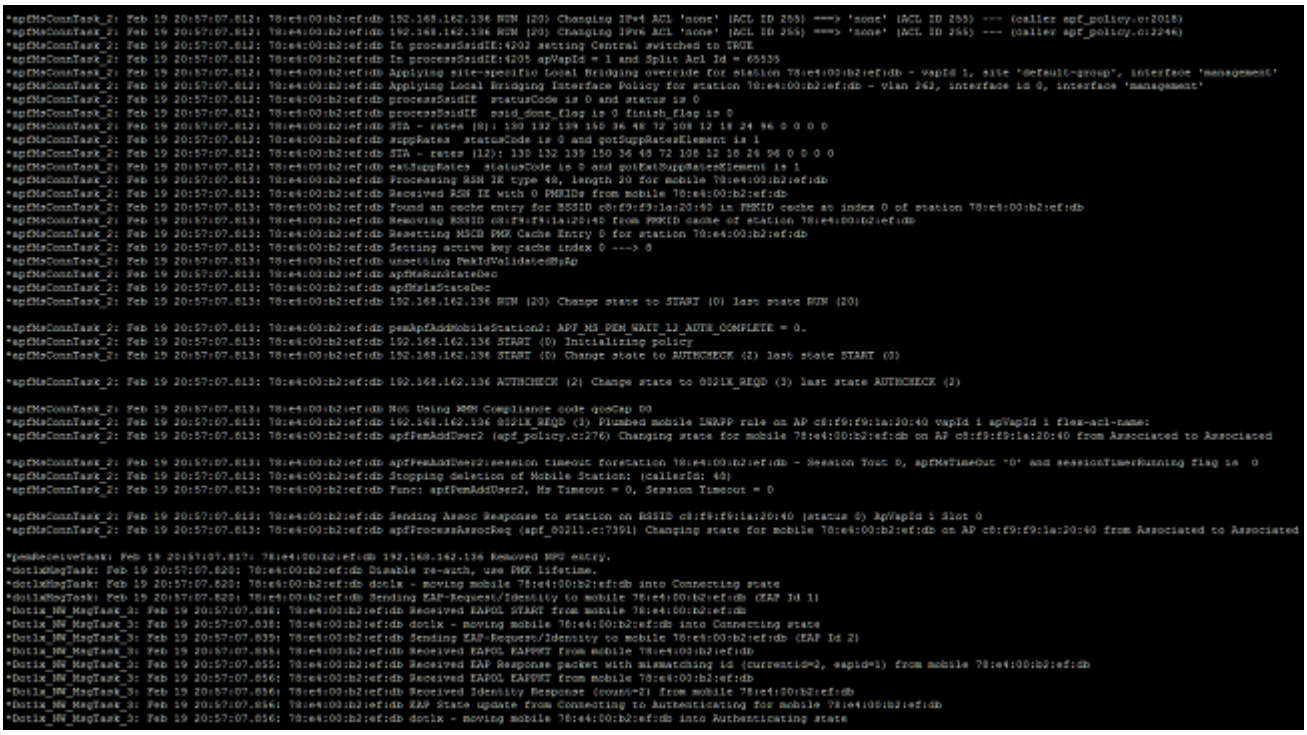
Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Si votre client ne s'est pas connecté au WLAN, cette section fournit des informations que vous pouvez utiliser pour dépanner la configuration.

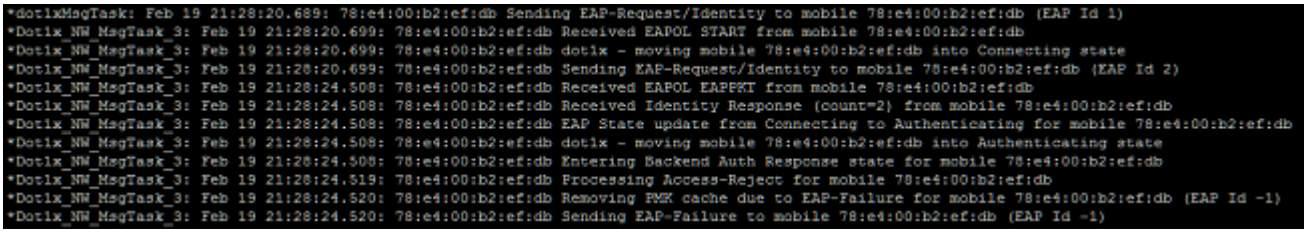
Deux outils peuvent être utilisés pour diagnostiquer les échecs d'authentification 802.1x : la commande debug client et l'Observateur d'événements dans Windows.

Si vous effectuez un débogage client à partir du WLC, il n'est pas gourmand en ressources et n'a pas d'impact sur le service. Pour démarrer une session de débogage, ouvrez l'interface de ligne de commande (CLI) du WLC, et entrez debug client mac address, où l'adresse mac est l'adresse mac sans fil du client sans fil qui ne peut pas se connecter. Pendant l'exécution de ce débogage, essayez de connecter le client ; il doit y avoir une sortie sur la CLI du WLC qui ressemble à cet exemple :



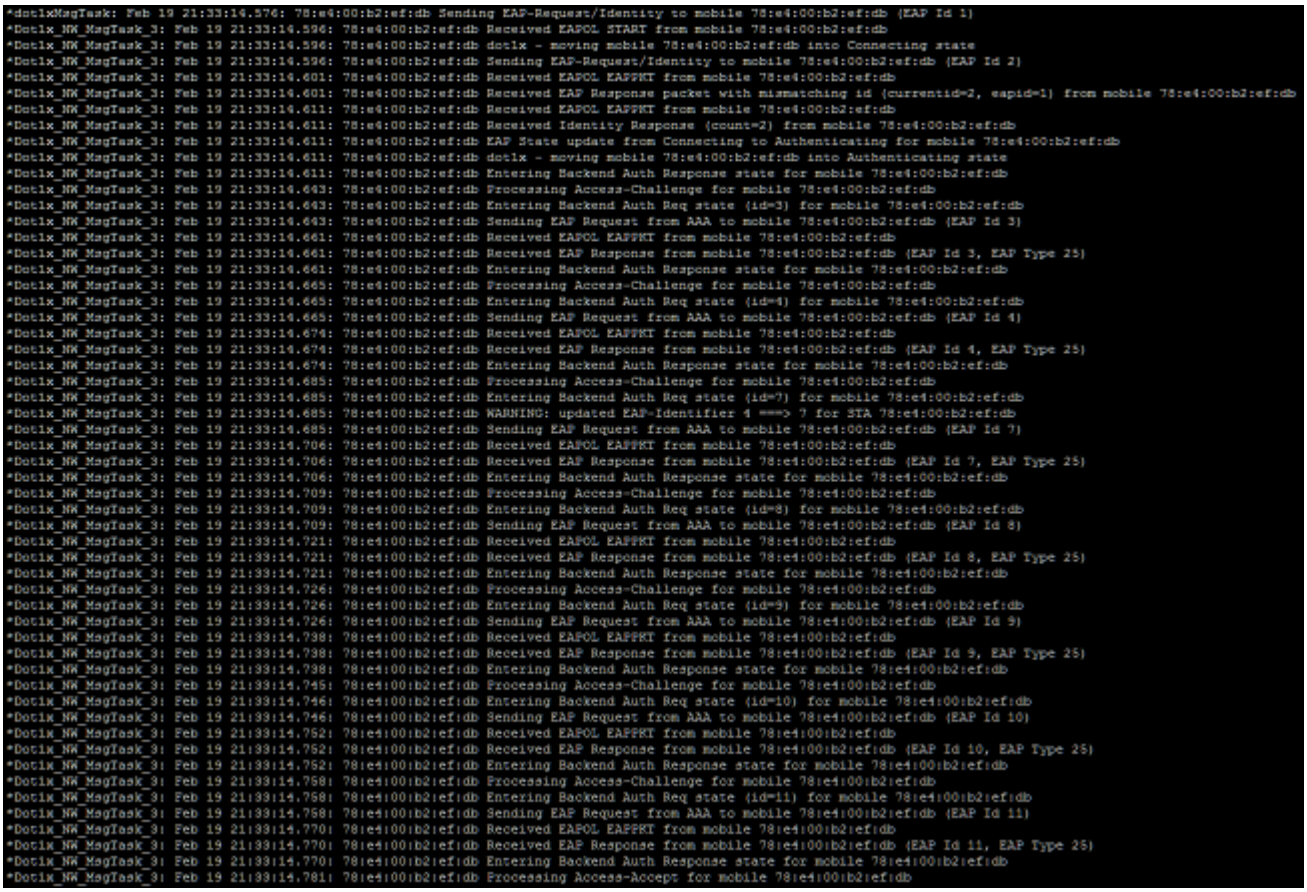
Il s'agit d'un exemple de problème qui peut se produire lors d'une mauvaise configuration. Ici, le débogage du WLC montre que le WLC est passé à l'état d'authentification, ce qui signifie que le WLC attend une réponse du NPS. Ceci est généralement dû à un secret partagé incorrect sur le WLC ou le NPS. Vous pouvez le confirmer via l'Observateur d'événements de Windows Server. Si vous ne trouvez pas de journal, la demande n'est jamais parvenue au SNP.

Un autre exemple trouvé dans le débogage du WLC est un refus d'accès. Un refus d'accès indique que le serveur NPS a reçu et rejeté les informations d'identification du client. Voici un exemple d'un client qui reçoit un refus d'accès :



Lorsque vous voyez un refus d'accès, vérifiez les journaux des événements Windows Server pour déterminer pourquoi le serveur NPS a répondu au client avec un refus d'accès.

Une authentification réussie a un access-accept dans le débogage du client, comme le montre cet exemple :

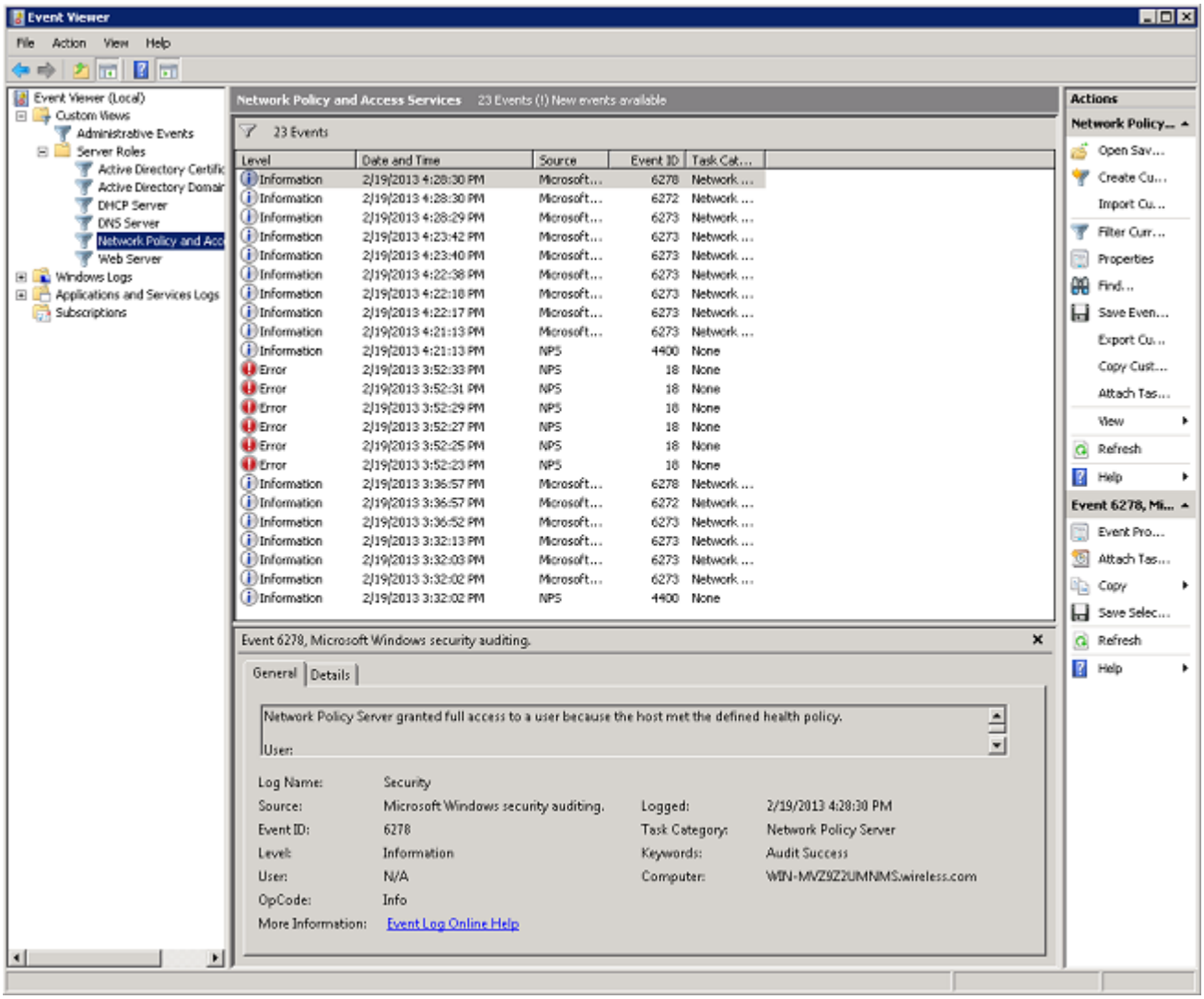


Si vous voulez dépanner les refus d'accès et les délais de réponse, il faut accéder au serveur RADIUS. Le WLC agit comme un authentificateur qui transmet des messages EAP entre le client et le serveur RADIUS. Un serveur RADIUS qui répond par un refus d'accès ou un délai de réponse doit être examiné et diagnostiqué par le fabricant du service RADIUS.

Remarque : Le TAC ne fournit pas d'assistance technique pour les serveurs RADIUS tiers ; cependant, les journaux sur le serveur RADIUS expliquent généralement pourquoi une requête client a été rejetée ou ignorée.

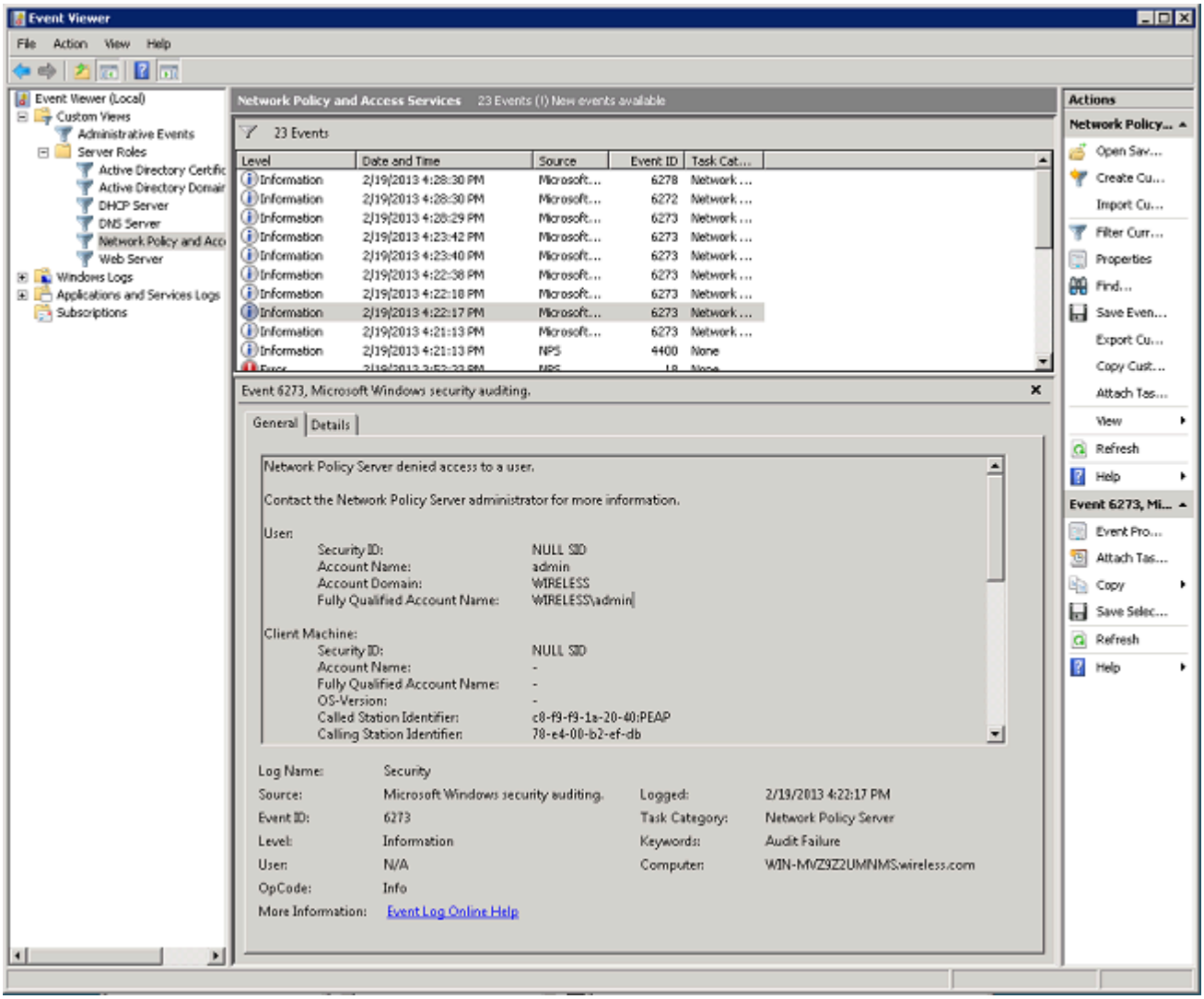
Afin de dépanner les refus d'accès et les délais de réponse du serveur NPS, examinez les journaux NPS dans l'Observateur d'événements Windows sur le serveur.

1. Cliquez sur Démarrer > Outils d'administration > Observateur d'événements pour démarrer l'Observateur d'événements et consulter les journaux NPS.
2. Développez Vues personnalisées > Rôles serveur > Stratégie et accès réseau.



Dans cette section de l'affichage des événements, il existe des journaux des authentifications passées et échouées. Examinez ces journaux pour déterminer pourquoi un client ne réussit pas l'authentification. Les authentifications réussies et échouées s'affichent en tant qu'informations. Faites défiler les journaux pour trouver le nom d'utilisateur dont l'authentification a échoué et qui a reçu un refus d'accès basé sur les débogages du WLC.

Voici un exemple de NPS lorsqu'il refuse l'accès à un utilisateur :

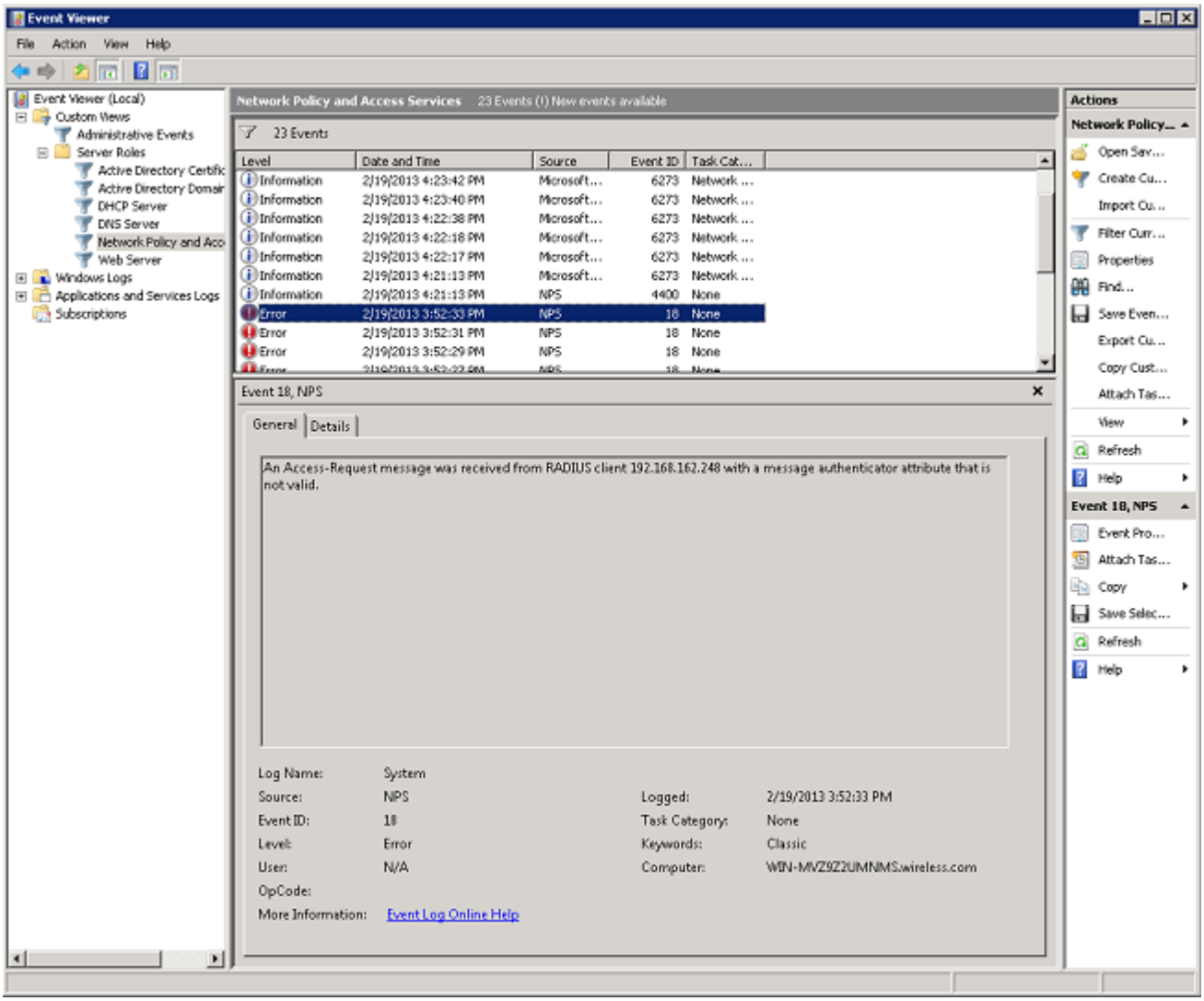


Lorsque vous consultez une instruction de refus dans l'Observateur d'événements, examinez la section Détails d'authentification. Dans cet exemple, vous pouvez voir que le serveur NPS a refusé l'accès utilisateur en raison d'un nom d'utilisateur incorrect :

```
Authentication Details:
        Proxy Policy Name:                Use Windows authentication for all users
        Network Policy Name:              -
        Authentication Provider:          Windows
        Authentication Server:            WIN-MVZ9Z2UMNMS.wireless.com
        Authentication Type:              EAP
        EAP Type:                         -
        Account Session Identifier:       -
        Reason Code:                      8
        Reason:                           The specified user account does not exist.
```

L'affichage des événements sur le NPS vous aide également lorsque vous avez besoin de dépanner si le WLC ne reçoit pas de réponse du NPS. Ceci est généralement causé par un secret partagé incorrect entre le NPS et le WLC.

Dans cet exemple, le NPS rejette la requête du WLC en raison d'un secret partagé incorrect :



Informations connexes

- [Assistance technique de Cisco et téléchargements]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.