HESTIM
ENGINEERING & BUSINESS SCHOOL

Rapport technique – Mise en place d'une solution NAC avec PacketFence et authentification 802.1X

PROJET DE GROUPE

Sécurité des réseaux

Encadrant : Pr. Azeddine Khiat

Nom(s) des étudiants :

Aya Fadel
Hiba Zbari
Fatime ezzahra Montassif
Najoua Mouaddab

Date de remise : Février 2026

RÉSUMÉ

Ce rapport présente la mise en œuvre complète d'une solution de **Contrôle d'Accès au Réseau (NAC)** utilisant **PacketFence** et l'authentification **802.1X**, intégrée à un **Active Directory** sous Windows Server 2019.

Le projet vise à sécuriser l'accès au réseau d'entreprise en authentifiant les utilisateurs avant de leur accorder l'accès aux ressources. L'architecture mise en place comprend trois machines virtuelles : un serveur PacketFence jouant le rôle de NAC et de serveur RADIUS, un contrôleur de domaine Active Directory avec les rôles DNS et NPS, et un poste client Windows soumis à l'authentification 802.1X.

Les étapes clés du projet incluent l'installation et la configuration de PacketFence, la mise en place du domaine nac.local, la création des utilisateurs de test (user1 et user2), la configuration du NPS en tant que serveur RADIUS, l'intégration LDAP entre PacketFence et l'Active Directory, et enfin les tests d'authentification.

Les résultats obtenus confirment le bon fonctionnement de la solution : l'utilisateur autorisé (user1) obtient un accès réseau tandis que l'utilisateur non autorisé (user2) se voit refuser l'accès, conformément aux politiques définies.

Mots-clés : NAC, 802.1X, PacketFence, RADIUS, Active Directory, NPS, PEAP, Sécurité réseau, Authentification.

Lien Github : https://github.com/fatihokent/Projet_NAC

Contents

1.1 Introduction

1.1. CONTEXTE DU PROJET

Avec la multiplication des équipements connectés (postes utilisateurs, smartphones, objets connectés), la gestion et la sécurisation des accès au réseau sont devenues des enjeux majeurs pour les entreprises. Les réseaux modernes doivent non seulement assurer la connectivité, mais aussi contrôler qui peut accéder au réseau, depuis quel équipement et sous quelles conditions de sécurité.

Dans ce contexte, le **Contrôle d'Accès au Réseau (NAC)** constitue une solution essentielle pour renforcer la sécurité des infrastructures réseau. Le protocole **IEEE 802.1X**, associé à une solution NAC comme **PacketFence**, permet de contrôler dynamiquement l'accès au réseau en fonction de l'identité de l'utilisateur ou de l'équipement.

1.2. OBJECTIFS DU PROJET

Ce projet vise à mettre en place une solution de **Contrôle d'Accès au Réseau (NAC)** basée sur **PacketFence** et l'authentification **802.1X**, afin de sécuriser l'accès au réseau et de maîtriser les connexions des utilisateurs et des équipements. Les objectifs spécifiques sont :

- Comprendre le fonctionnement des réseaux d'entreprise et des mécanismes de contrôle d'accès.
- Maîtriser les principes du **RADIUS** et du protocole **802.1X** (EAP, authentification, autorisation).
- Installer et configurer **PacketFence** comme solution NAC.
- Intégrer PacketFence à un **Active Directory** pour l'authentification des utilisateurs.
- Mettre en œuvre une authentification **802.1X** pour un poste client filaire.
- Analyser les échanges de protocoles liés à l'authentification et à la sécurisation des accès.

1.3ARCHITECTURE DU PROJET

L'architecture mise en place repose sur trois machines virtuelles interconnectées sur un même réseau interne, conformément aux spécifications du projet.

Machine Virtuelle	Rôle	OS	Interfaces
VM1 : PacketFence	Serveur NAC + RADIUS	PacketFence ZEN v15.0.0	eth0 : LAN Client / eth1 : Management
VM2 : Active Directory	AD DS + DNS + NPS	Windows Server 2019	1 interface (LAN)
VM3 : Client Windows	Poste utilisateur	Windows 10	1 interface (LAN)

2. CONCEPTS THÉORIQUES

2.1 LE CONTROLE D'ACCES AU RESEAU (NAC)

Définition

Le **Network Access Control (NAC)** est une approche de sécurité réseau qui vise à contrôler l'accès des équipements et des utilisateurs au réseau d'entreprise. Il permet de définir et d'appliquer des politiques d'accès basées sur l'identité, le type d'équipement, sa configuration de sécurité, et sa conformité aux exigences de l'organisation.

Objectifs du NAC

- **Authentification** : Vérifier l'identité des utilisateurs et des équipements avant de leur accorder l'accès.
- **Autorisation** : Déterminer les ressources réseau auxquelles un utilisateur ou un équipement peut accéder.
- **Évaluation de conformité** : Vérifier que les équipements respectent les politiques de sécurité (antivirus à jour, pare-feu actif, etc.).
- **Remédiation** : Isoler les équipements non conformes pour leur permettre de se mettre à jour avant d'accéder au réseau.
- **Traçabilité** : Journaliser toutes les tentatives d'accès pour faciliter les audits et les investigations.

Mécanismes du NAC

Le NAC peut être mis en œuvre selon différentes approches :

- **802.1X** : Authentification au niveau du port du commutateur (filaire ou sans fil).
- **Portail captif** : Redirection des utilisateurs non authentifiés vers une page web d'authentification.
- **DHCP** : Contrôle basé sur l'attribution d'adresses IP (restriction ou isolation).
- **ARP/NDP** : Contrôle au niveau de la couche liaison.

2.2 LE PROTOCOLE 802.1X

Présentation

IEEE 802.1X est un standard de la famille IEEE 802 qui définit un mécanisme de contrôle d'accès au réseau basé sur les ports. Il permet d'authentifier un équipement avant de lui autoriser l'accès au réseau, au niveau de la couche liaison de données (couche 2 du modèle OSI).

Architecture 802.1X

L'architecture 802.1X repose sur trois entités :

1. **Le suppliant (Supplicant)** : Le client qui souhaite accéder au réseau (poste de travail, smartphone, etc.). Il implémente un logiciel client 802.1X (natif dans Windows, macOS, Linux).
2. **L'authentificateur (Authenticator)** : L'équipement réseau (commutateur, point d'accès WiFi) qui contrôle l'accès au réseau. Il agit comme un intermédiaire entre le suppliant et le serveur d'authentification.
3. **Le serveur d'authentification (Authentication Server)** : Généralement un serveur RADIUS, il valide les identifiants du suppliant et indique à l'authentificateur si l'accès doit être autorisé ou non.

Fonctionnement

1. **Initialisation** : Le port de l'authentificateur est en état "non autorisé" (bloqué). Seuls les trames EAPOL (EAP over LAN) sont autorisées.
2. **Déclenchement** : L'authentificateur peut initier l'authentification ou attendre que le suppliant se manifeste.
3. **Échange EAP** : Le suppliant et le serveur d'authentification échangent des messages EAP (Extensible Authentication Protocol) encapsulés dans RADIUS entre l'authentificateur et le serveur.
4. **Décision** : Le serveur d'authentification renvoie une réponse "Accept" ou "Reject". L'authentificateur place alors le port dans l'état correspondant.

5. **Comptabilité (Accounting)** : Des informations de session peuvent être envoyées au serveur RADIUS à des fins de traçabilité.

Méthodes EAP

Plusieurs méthodes EAP existent, offrant différents niveaux de sécurité :

- **EAP-MD5** : Authentification par mot de passe (peu sécurisé, obsolète).
- **EAP-TLS** : Authentification basée sur des certificats (très sécurisé mais complexe).
- **EAP-TTLS** : Tunnel TLS protégeant une authentification interne (mot de passe ou certificat).
- **PEAP (Protected EAP)** : Tunnel TLS similaire à TTLS, largement supporté.

2.3 LE PROTOCOLE RADIUS

RADIUS (Remote Authentication Dial-In User Service) est un protocole AAA (Authentication, Authorization, Accounting) qui centralise la gestion des accès réseau. Il fonctionne en mode client-serveur et utilise généralement les ports UDP 1812 (authentification) et 1813 (comptabilité).

Rôle dans l'architecture NAC

Dans une architecture 802.1X, RADIUS joue le rôle de serveur d'authentification :

- **Authentification** : Le client RADIUS (authentificateur) envoie les identifiants du suppliant au serveur RADIUS, qui les vérifie auprès d'une base d'utilisateurs (Active Directory, LDAP, base locale).
- **Autorisation** : Le serveur RADIUS peut renvoyer des attributs spécifiques (VLAN, liste de contrôle d'accès) qui définissent les droits de l'utilisateur.
- **Comptabilité** : Le serveur RADIUS enregistre les sessions (début, fin, volume de données) pour la traçabilité et la facturation

Attributs RADIUS

RADIUS utilise des attributs (AVP - Attribute Value Pairs) pour transporter les informations :

- **User-Name** : Nom de l'utilisateur.
- **User-Password** / **CHAP-Password** : Mot de passe (chiffré selon la méthode).
- **NAS-IP-Address** : Adresse IP du client RADIUS (authentificateur).
- **NAS-Port** : Port physique ou logique sur lequel la connexion est établie.
- **Framed-IP-Address** : Adresse IP attribuée à l'utilisateur.
- **Session-Timeout** : Durée maximale de la session.
- **Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-ID** : Utilisés pour l'attribution dynamique de VLAN.

2.4 PacketFence

PacketFence est une solution NAC open-source développée par Inverse Inc. Elle offre un ensemble complet de fonctionnalités pour le contrôle d'accès réseau :

- Serveur RADIUS intégré (FreeRADIUS)
- Portail captif personnalisable
- Gestion des invités
- Intégration avec les annuaires (LDAP, Active Directory)
- Détection et isolation des équipements non conformes
- Interface d'administration web
- API REST pour l'automatisation

Architecture de PacketFence

PacketFence s'articule autour de plusieurs composants :

- **pfdetect** : Détection des équipements sur le réseau.
- **pfdhcp** : Serveur DHCP pour l'attribution d'adresses IP.
- **pfmon** : Surveillance et traitement des événements.
- **pfsetvlan** : Modification dynamique des VLAN sur les commutateurs.
- **iptables** : Règles de filtrage pour l'isolation.
- **httpd.portal** : Serveur web pour le portail captif.

Éditions

PacketFence est disponible en deux éditions :

- **Community Edition** : Version open-source complète.
- **ZEN** : Appliance prête à l'emploi (machine virtuelle ou physique) avec configuration simplifiée.

2.5 ACTIVE DIRECTORY ET NPS

Active Directory (AD DS)

Active Directory Domain Services est le service d'annuaire de Microsoft. Il stocke les informations sur les utilisateurs, les ordinateurs, les groupes et les ressources du réseau, et les rend disponibles aux utilisateurs et applications autorisés.

Composants clés :

- **Domaine** : Unité administrative et de sécurité.

- **Forêt** : Ensemble de domaines partageant un schéma commun.
- **Unité d'organisation (OU)** : Conteneur permettant d'organiser les objets.
- **Groupe** : Ensemble d'utilisateurs ou d'ordinateurs partageant des droits.

Network Policy Server (NPS)

NPS est l'implémentation Microsoft d'un serveur RADIUS. Il permet de :

- Centraliser la gestion des politiques d'accès réseau.
- Authentifier les utilisateurs via Active Directory.
- Définir des stratégies basées sur le temps, le groupe, le type de connexion, etc.
- Journaliser les tentatives d'authentification.

Composants du NPS :

- **Clients RADIUS** : Équipements (commutateurs, points d'accès, serveurs NAC) qui envoient des requêtes d'authentification.
- **Stratégies de demande de connexion** : Déterminent quelles requêtes sont traitées localement ou transmises à un autre serveur RADIUS.
- **Stratégies réseau** : Définissent les conditions d'autorisation (groupes AD, heures, etc.) et les paramètres à appliquer (VLAN, filtres, etc.).
- **Comptabilité** : Enregistrement des sessions.

3.Installation et Configuration de l'environnement

3.1 PREMIER DEMARRAGE DE PACKETFENCE ZEN

L'appliance PacketFence ZEN v15.0.0 a été téléchargée depuis le site officiel et importée dans notre environnement de virtualisation.

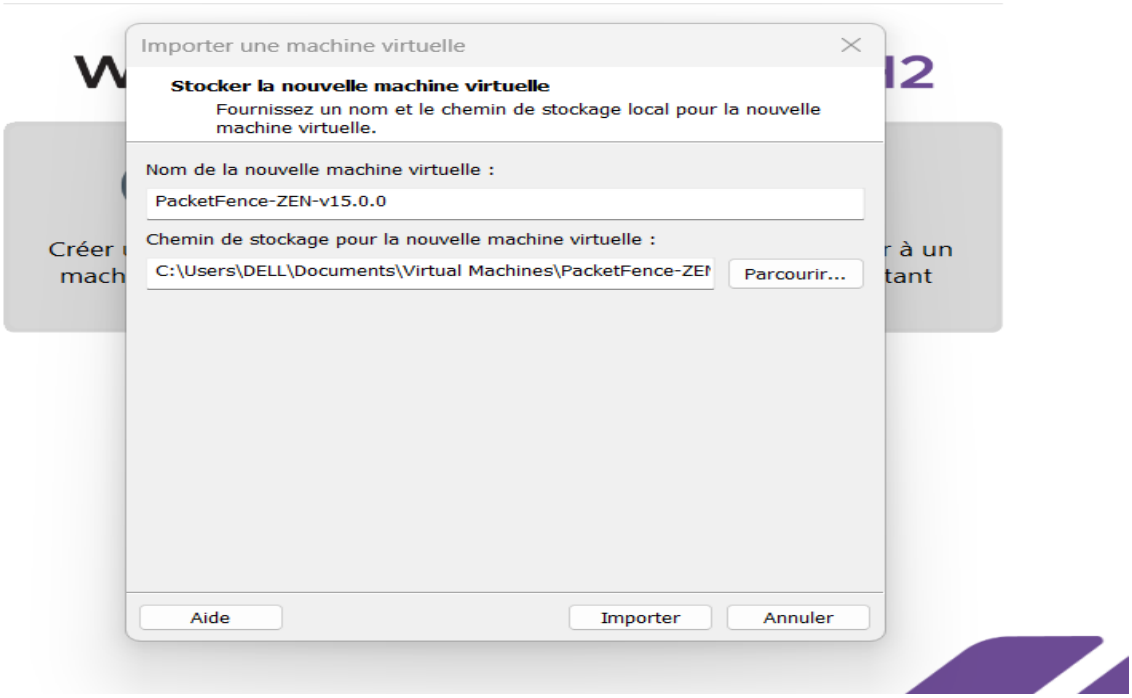


Figure 1 :Environnement de travail et contexte du laboratoire NAC

Figure 2:Interface de démarrage de PacketFence ZEN - Identification des interfaces réseau et des services disponibles

Au premier démarrage de l'appliance, nous accédons à l'interface en ligne de commande pour vérifier la configuration initiale et identifier les interfaces réseau disponibles.

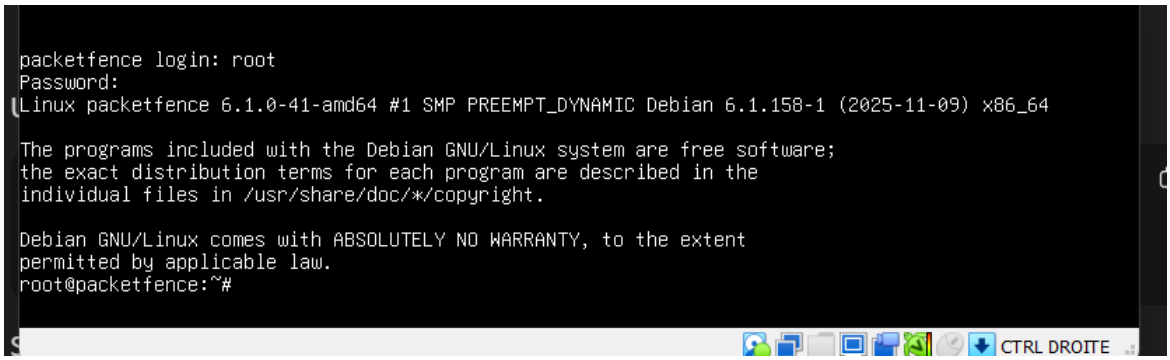


Figure 1: Interface d'administration en ligne de commande de PacketFence

L'écran d'accueil de PacketFence nous présente les informations de base sur le système, notamment les adresses IP configurées et l'état des services.

3.2 IDENTIFICATION DES INTERFACES RESEAU

Après connexion sur PacketFence, nous avons procédé à la configuration des interfaces réseau.

Figure 2: Écran de connexion PacketFence

Écran de connexion PacketFence montrant l'identification des interfaces - On peut voir que l'interface eth0 est connectée à la carte réseau VMnet1, ce qui correspond au LAN Client

L'analyse de la configuration nous permet de déterminer le rôle de chaque interface :

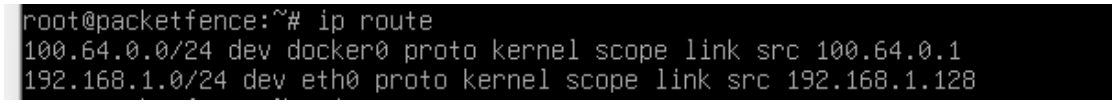


Figure 3:Confirmation que l'interface etho est celle connectée au réseau LAN Client (VMnet1)

Donc l'interface eth1 est celle qui dirigera vers Internet avec une adresse IP : 192.168.244.129

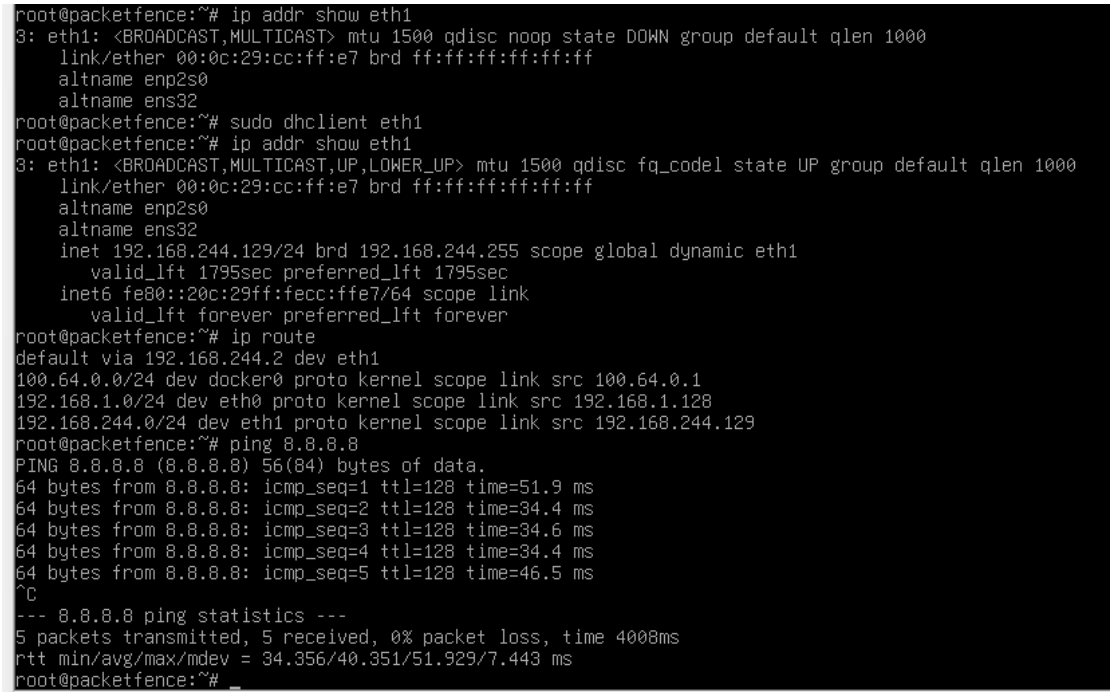


Figure 4: Identification de l'interface eth1 comme celle qui dirigera vers Internet avec l'adresse IP 192.168.244.129

L'interface **eth1** est identifiée comme l'interface de management, avec l'adresse IP 192.168.244.129. Elle permettra l'accès à l'interface web d'administration et éventuellement à Internet pour les mises à jour.

3.3 VERIFICATION DES SERVICES SYSTEME

Avant de poursuivre, nous vérifions l'état des services système pour s'assurer de leur bon fonctionnement.

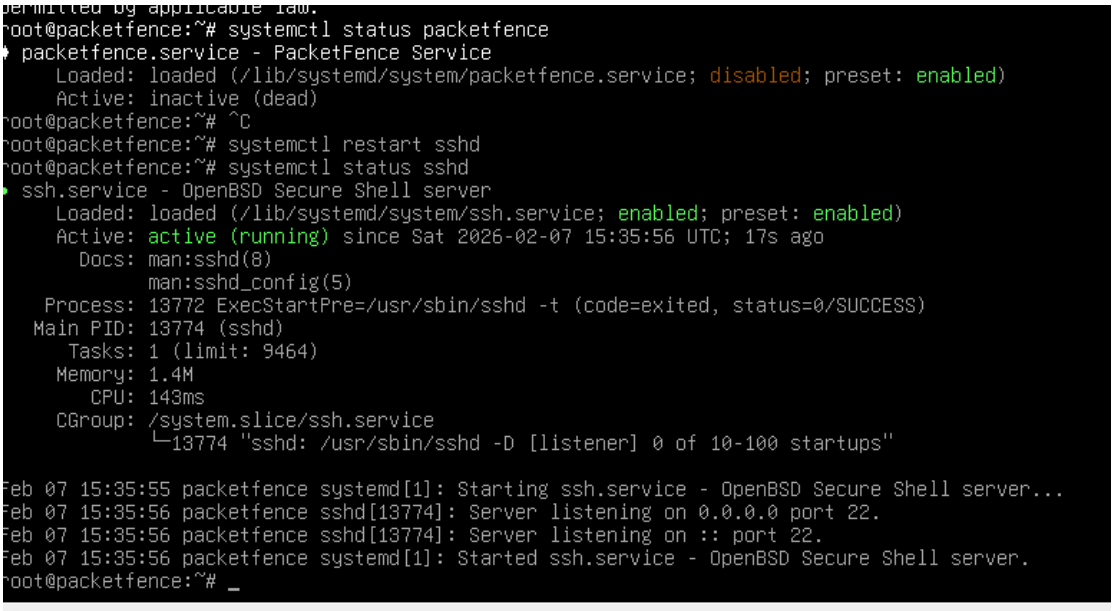


Figure 5: Vérification de l'état des services PacketFence et SSH

La commande systemctl status packetfence montre que le service PacketFence est inactif (inactive dead), tandis que systemctl status sshd confirme que le service SSH est actif et fonctionnel après redémarrage

Avant de poursuivre, nous vérifions l'état des services critiques. Le service SSH est actif, garantissant un accès à distance sécurisé. Le service PacketFence est inactif initialement, ce qui est normal avant la configuration complète via l'assistant.

3.5 ACCES A L'INTERFACE D'ADMINISTRATION WEB

L'interface web d'administration est accessible sur le port 1443 en HTTPS. Les identifiants par défaut sont **admin/admin**.

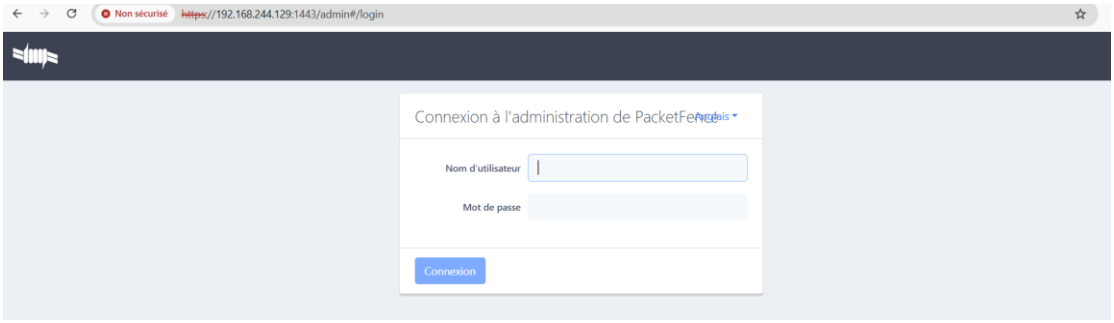


Figure 6: Interface de connexion à l'administration web de PacketFenc

C'est à partir de cette interface que nous allons configurer l'ensemble des paramètres de PacketFence.)

4. Configuration finale des interfaces PacketFence

4.1CONFIGURATION DE L'INTERFACE ETH0 (LAN) :

Nous procédons à la configuration détaillée de l'interface réseau etho qui servira pour le LAN client.

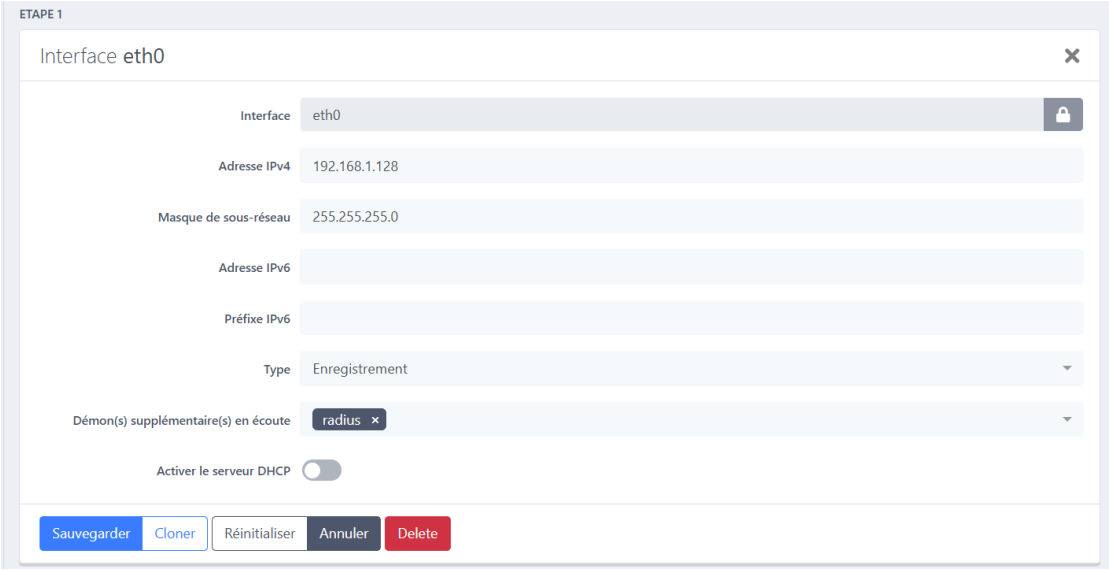


Figure 7: Configuration de l'interface etho dans PacketFence

L'interface etho est configurée avec l'adresse IP **192.168.1.128/24**. Le service RADIUS est activé sur cette interface car elle recevra les requêtes d'authentification des clients. Le type d'interface est défini sur "Enregistrement" (registration), ce qui correspond au rôle LAN client.

4.2 CONFIGURATION DE L'INTERFACE ETH1 (MANAGEMENT) :

L'interface eth1 est configurée pour la gestion et l'accès à Internet.

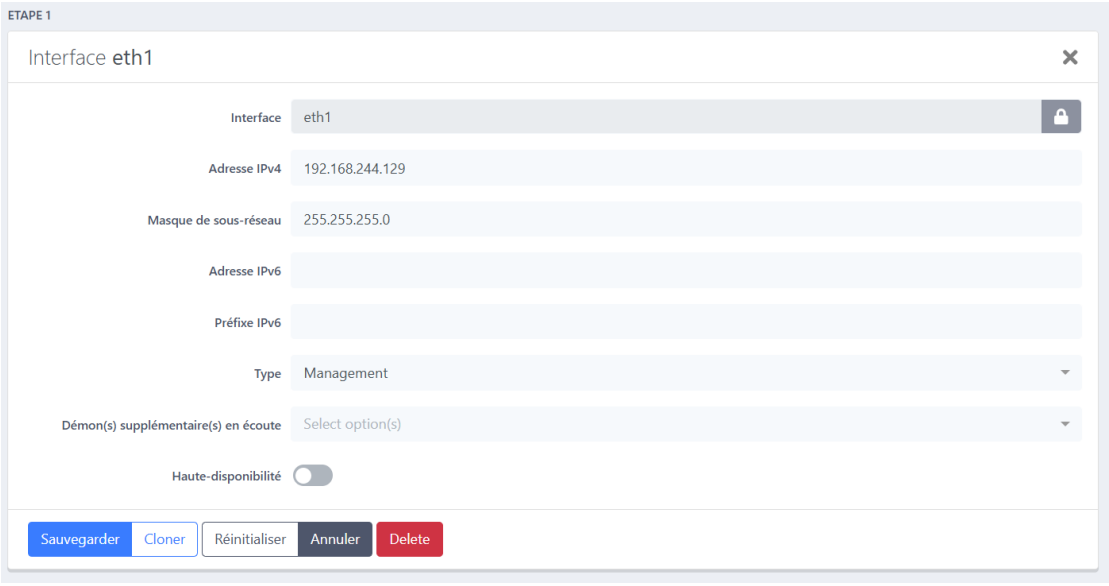


Figure 8: Configuration de l'interface eth1 dans PacketFence

L'interface eth1 est configurée avec l'adresse IP **192.168.244.129/24** en mode "Management". Cette interface sera utilisée pour l'administration du serveur et l'accès

à l'interface web. Le service RADIUS n'est pas activé sur cette interface car elle n'est pas destinée à recevoir des requêtes d'authentification.

4.3. ASSISTANT DE CONFIGURATION - ÉTAPE 1 : INTERFACES & RESEAUX

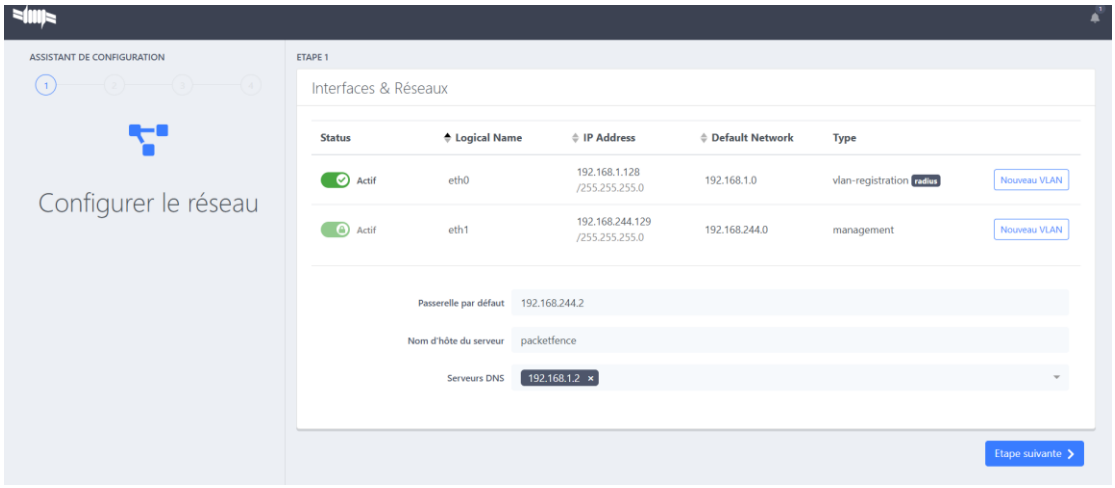


Figure 9: Assistant de configuration PacketFence

L'assistant de configuration récapitule les paramètres des interfaces. On note :

- **eth0** : 192.168.1.128/24, mode vlan-registration (pour l'enregistrement des clients)
- **eth1** : 192.168.244.129/24, mode management
- Passerelle par défaut : 192.168.244.2 (pour l'accès Internet)
- Serveur DNS : 192.168.1.2 (le futur serveur Active Directory)

4.4 ASSISTANT DE CONFIGURATION - ÉTAPE 2 : BASE DE DONNEES ET PARAMETRES GENERAUX

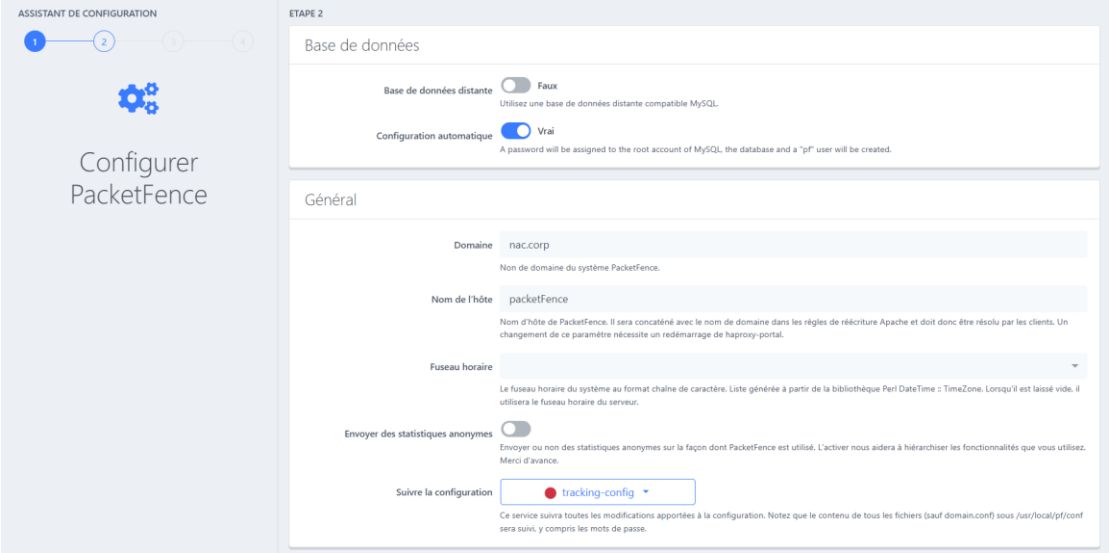


Figure 10: Assistant de configuration PacketFence

À cette étape, nous configurons :

- **Base de données** : Nous choisissons la configuration automatique (mot de passe généré pour MySQL).
- **Domaine** : "nacorp" (qui correspondra à notre domaine Active Directory).
- **Nom d'hôte** : "packetfence"
- **Fuseau horaire** : Laissé vide pour utiliser celui du serveur.

4.5 ASSISTANT DE CONFIGURATION - CONFIGURATION DES ALERTES& COMPTE ADMINISTRATEUR

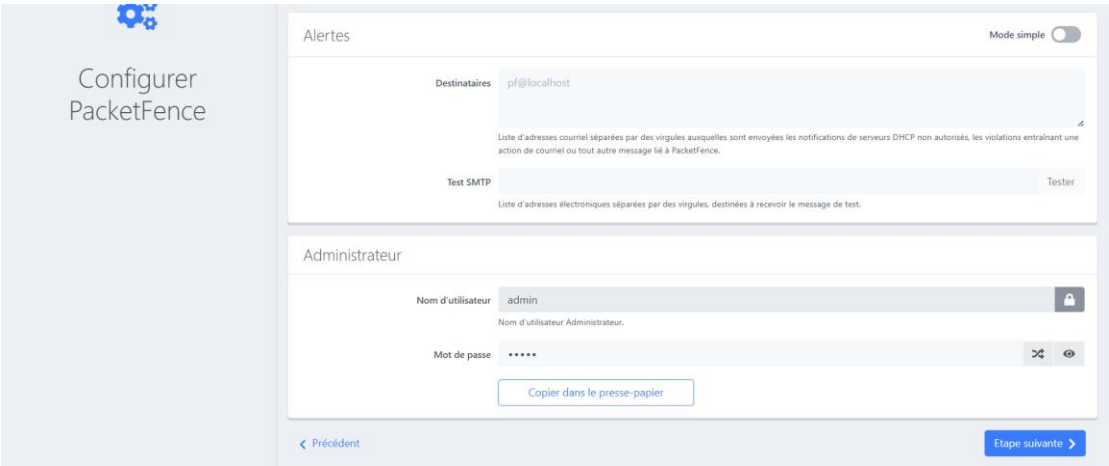


Figure 11: Assistant de configuration PacketFence

Les alertes permettent de recevoir des notifications par email en cas d'événements importants (serveurs DHCP non autorisés, violations, etc.). Nous configurons l'adresse locale par défaut pour les tests.

Le compte administrateur pour l'interface web est créé avec le nom d'utilisateur "admin" et le mot de passe "admin" (à modifier en production). Ce compte permettra d'accéder à toutes les fonctionnalités de configuration.

4.6 ASSISTANT DE CONFIGURATION - ÉTAPE 3 : FINGERBANK

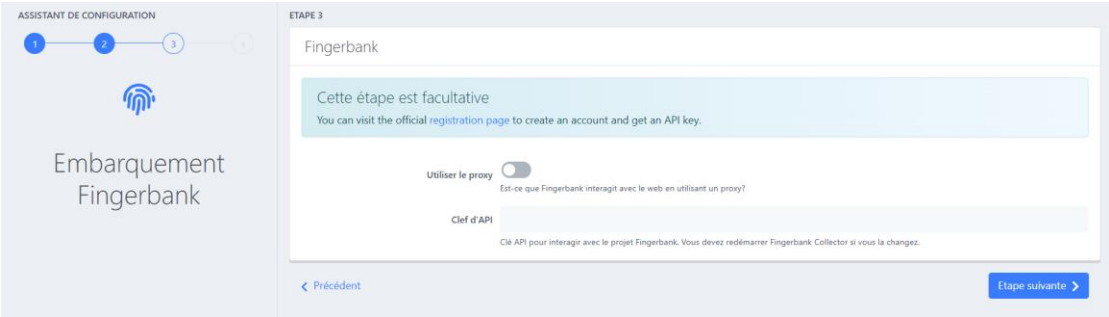


Figure 12: Assistant de configuration PacketFence

Fingerbank est un service optionnel qui permet d'identifier les équipements connectés (type d'OS, fabricant, etc.) à partir de leurs empreintes réseau. Cette étape peut être ignorée ou configurée ultérieurement avec une clé API obtenue sur le site officiel.

4.7 ASSISTANT DE CONFIGURATION - ÉTAPE 4 : CONFIRMATION DES MOTS DE PASSE

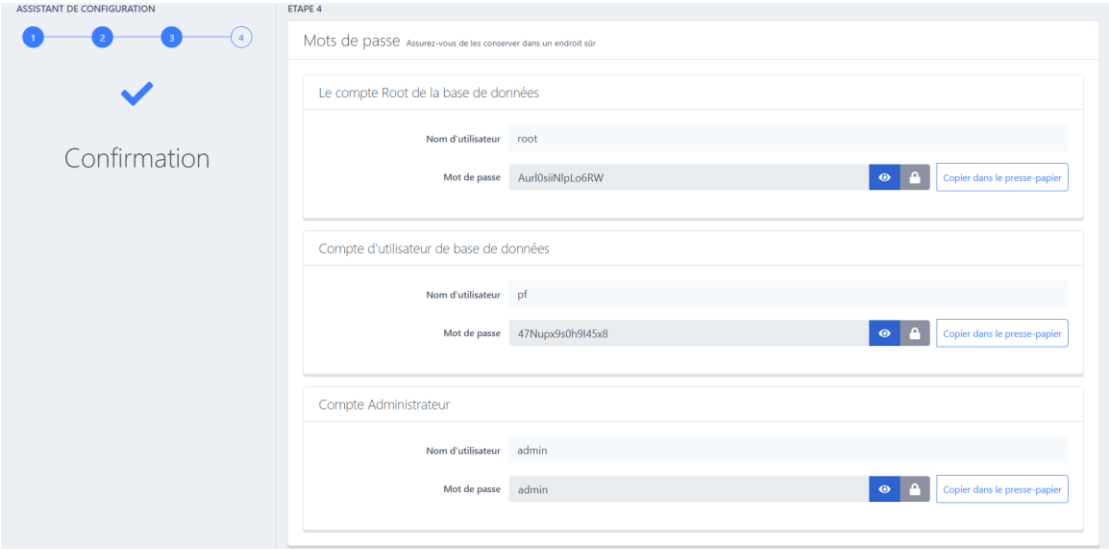


Figure 13: Assistant de configuration PacketFence

L'assistant génère automatiquement des mots de passe pour les comptes système :

Compte root de la base de données : AurIOsiNpLo6RW

Compte utilisateur pf : 47Nuq9soh9i45x8

Compte administrateur : admin (défini précédemment)

Il est **impératif de conserver ces informations** dans un endroit sûr, car elles seront nécessaires pour toute opération de maintenance ultérieure.

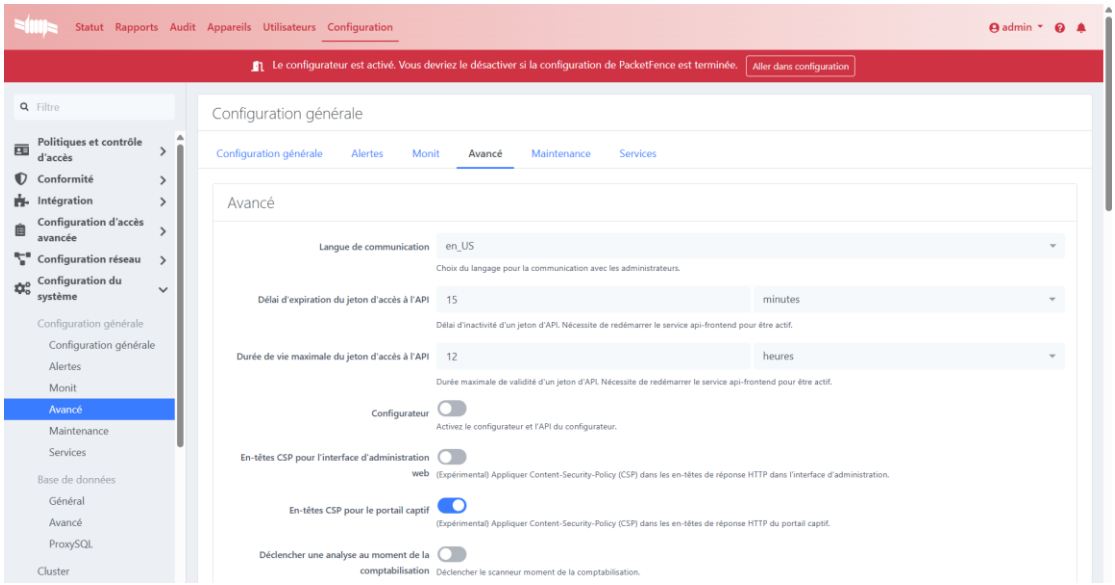


Figure 14:Assistant de configuration PacketFence

Menu Configuration générale / Avancé - Paramètres de langue (en_US), délais d'expiration des jetons API (15 minutes, 12 heures), et options expérimentales CSP pour l'interface d'administration et le portail captif

5. CONFIGURATION DE LA SOURCE D'AUTHENTIFICATION LDAP

5.1 ACCES AUX SOURCES D'AUTHENTIFICATION

Pour intégrer PacketFence avec l'Active Directory, nous devons configurer une source d'authentification LDAP.

Figure 15: Menu "Sources d'authentification"

Dans l'interface d'administration de PacketFence, nous accédons au menu Configuration > Authentication Sources. C'est ici que nous allons définir la source LDAP qui permettra à PacketFence d'interroger l'Active Directory pour valider les identifiants des utilisateurs.

5.2 CREATION DE LA SOURCE LDAP

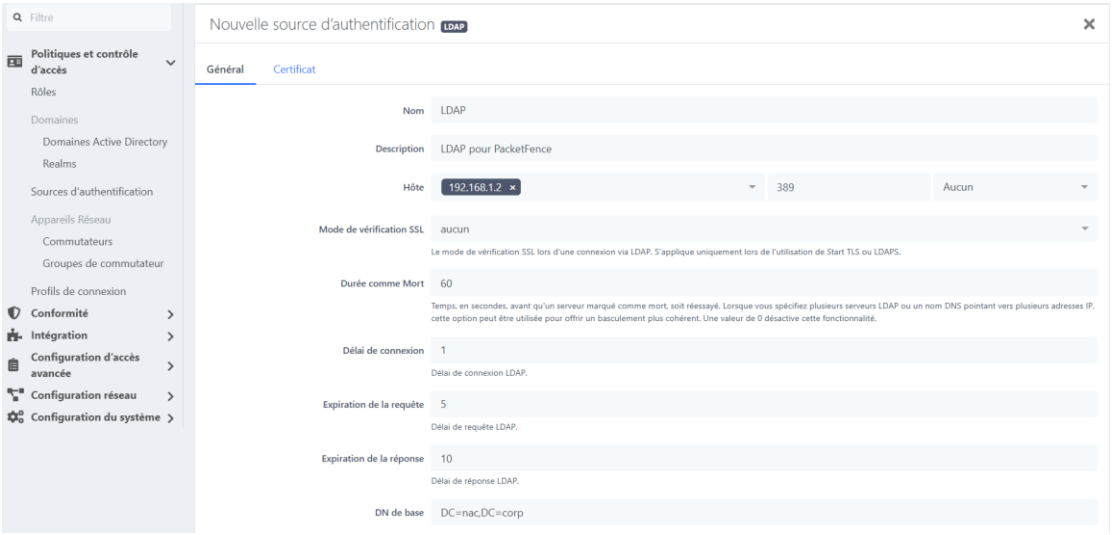


Figure 16:Configuration de la nouvelle source d'authentification LDAP

Nous créons une nouvelle source de type LDAP avec les paramètres suivants :

- **Nom** : LDAP
- **Description** : LDAP pour PacketFence
- **Hôte** : 192.168.1.2 (adresse IP du serveur Active Directory)
- **Mode de vérification SSL** : aucun (en environnement de laboratoire)
- **DN de base** : DC=rac,DC=corp (correspondant au domaine "nacorp")

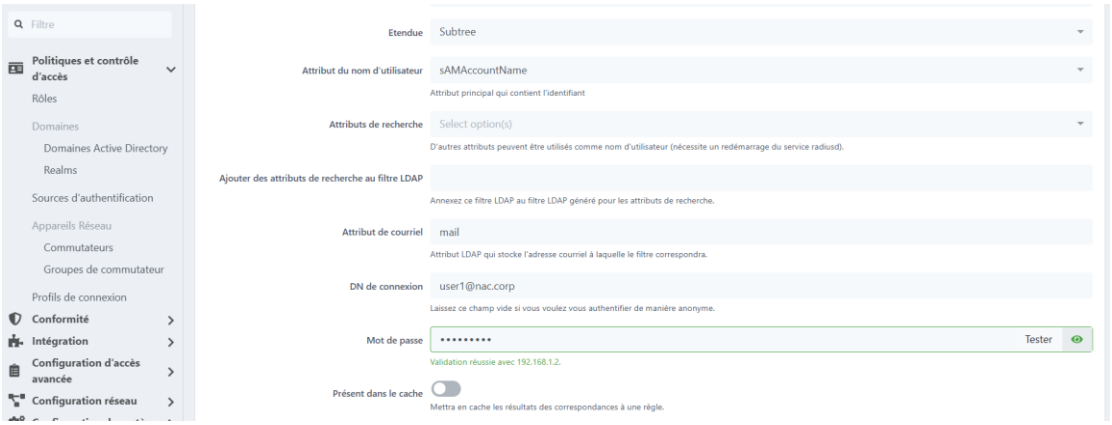


Figure 17: Configuration avancée de la source LDAP

5.3 PARAMETRAGE AVANCE ET TEST DE CONNEXION

Les paramètres avancés précisent :

Attribut du nom d'utilisateur : sAMAcountName (attribut Active Directory contenant le nom de connexion)

Attribut de courriel : mail

DN de connexion : user1@nacorp (compte de test pour la validation)

Le test de connexion est **réussi** (message "Validation réussie avec: 192.168.1.2"), confirmant que PacketFence peut communiquer avec l'Active Directory.

5.4 CONFIRMATION DE LA CREATION

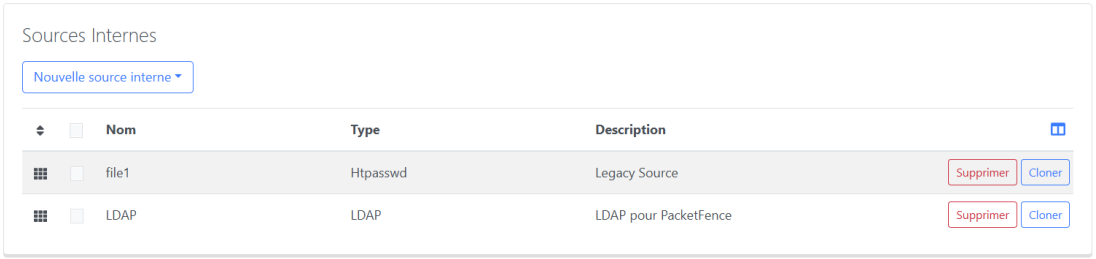


Figure 18:Confirmation de la création de la source LDAP

La nouvelle source LDAP apparaît dans la liste aux côtés de la source locale par défaut ("file1" de type Htpasswd). L'intégration entre PacketFence et l'Active Directory est désormais opérationnelle.

6.CONFIGURATION DE LA MACHINE VIRTUELLE WINDOWS SERVER2019

6.1 PARAMETRES VMWARE DE LA MACHINE VIRTUELLE

Avant d'installer Windows Server 2019, nous configurons les paramètres de la machine virtuelle dans VMware.

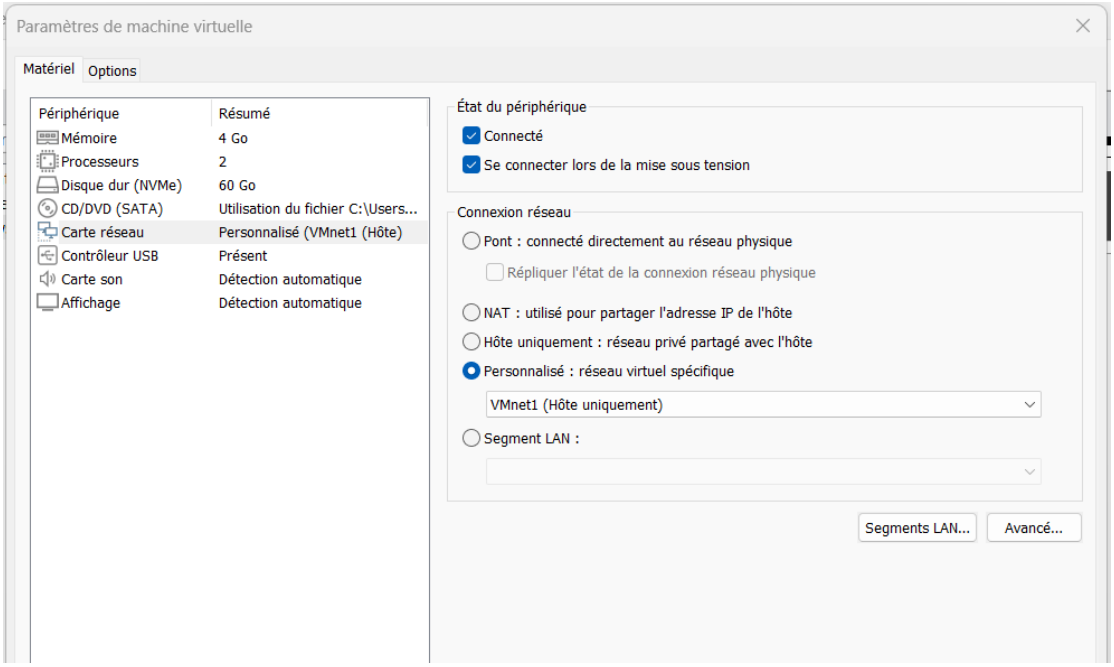


Figure 19: Configuration de la machine virtuelle Windows Server 2019 dans VMware

La machine virtuelle pour Windows Server 2019 est configurée avec :

- **Mémoire** : 4 Go (suffisant pour AD DS et NPS)
- **Processeurs** : 2
- **Disque dur** : 60 Go
- **Carte réseau** : Mode personnalisé VMnet1 (Hôte uniquement) - pour être sur le même réseau que PacketFence

6.2 INTERFACE VMWARE AVEC WINDOWS SERVER 2019

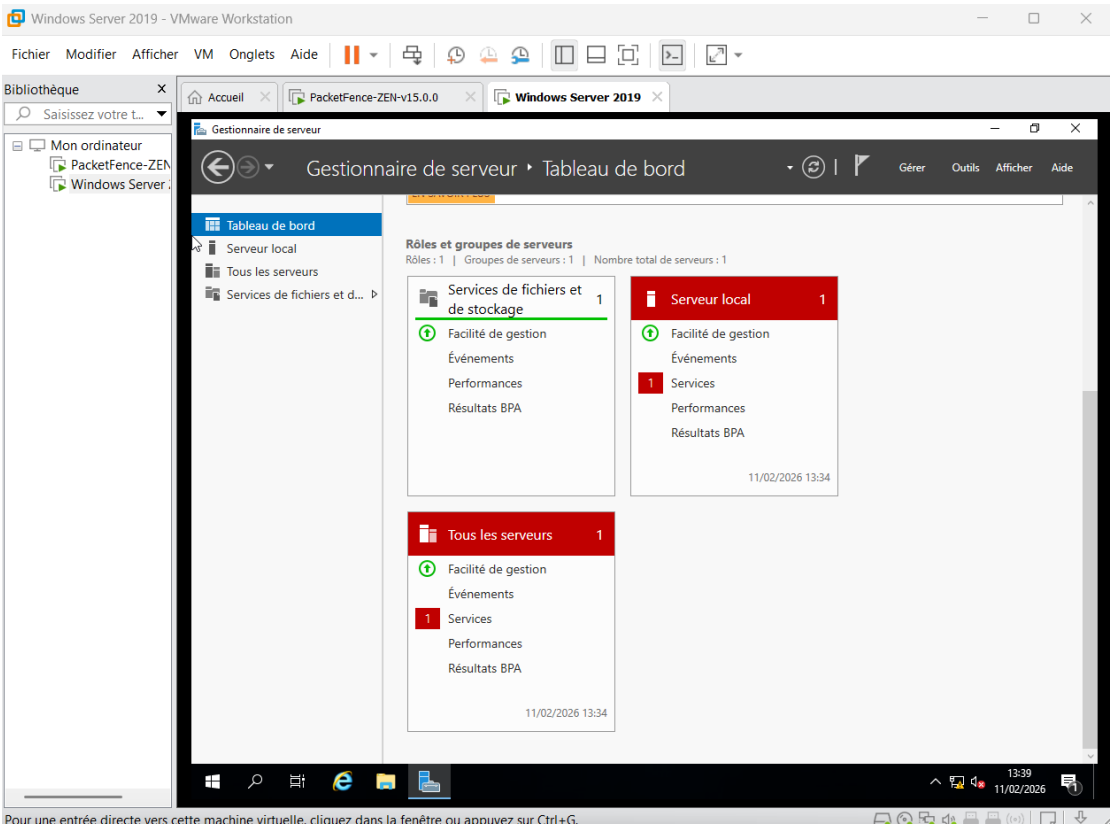


Figure 20: Interface VMware avec Windows Server 2019- Tableau de bord

Après l'installation de Windows Server 2019, le gestionnaire de serveur s'affiche. Le tableau de bord indique qu'aucun rôle n'est encore installé, ce qui est normal à ce stade.

6.3 CENTRE RESEAU ET PARTAGE - ÉTAT INITIAL

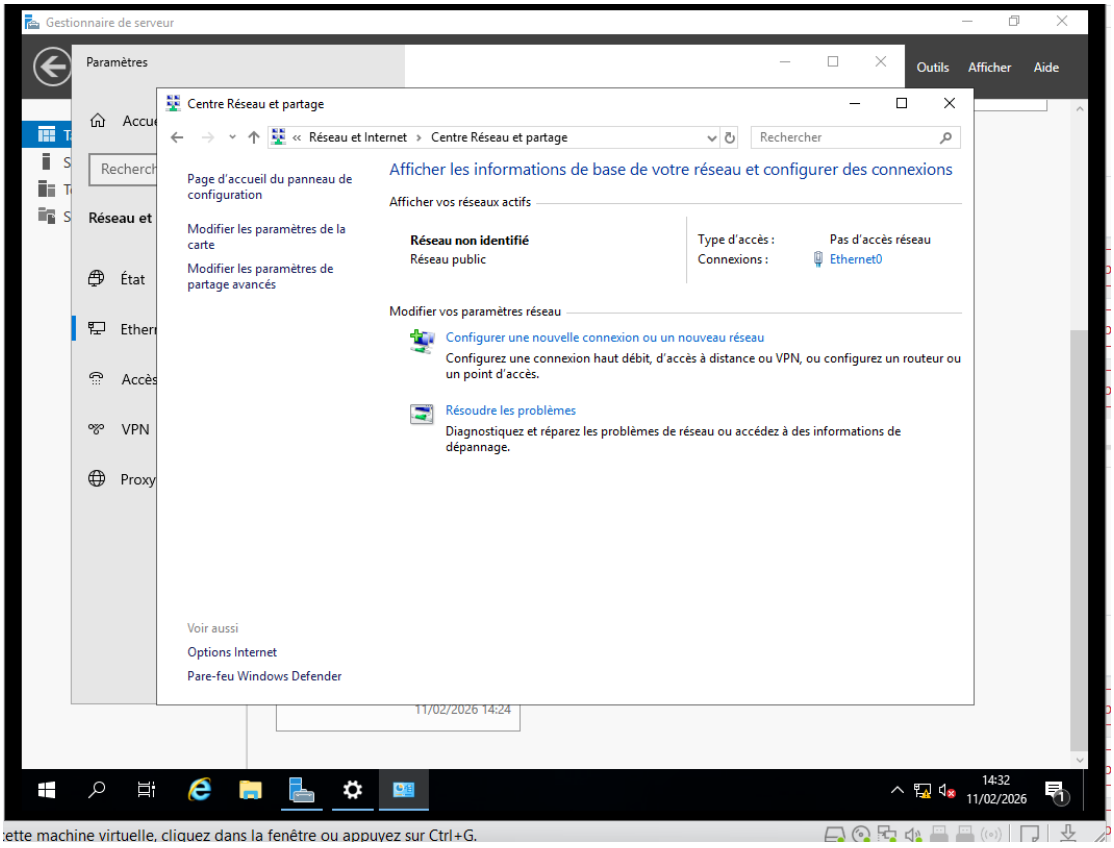


Figure 21:Centre Réseau et partage

Avant configuration, la carte réseau est en état "Réseau non identifié" avec "Pas d'accès réseau". Cela confirme que la machine est isolée du réseau physique, conformément à la configuration "Hôte uniquement" de VMware.

6.4 PROPRIETES DE LA CARTE RESEAU ETHERNET0

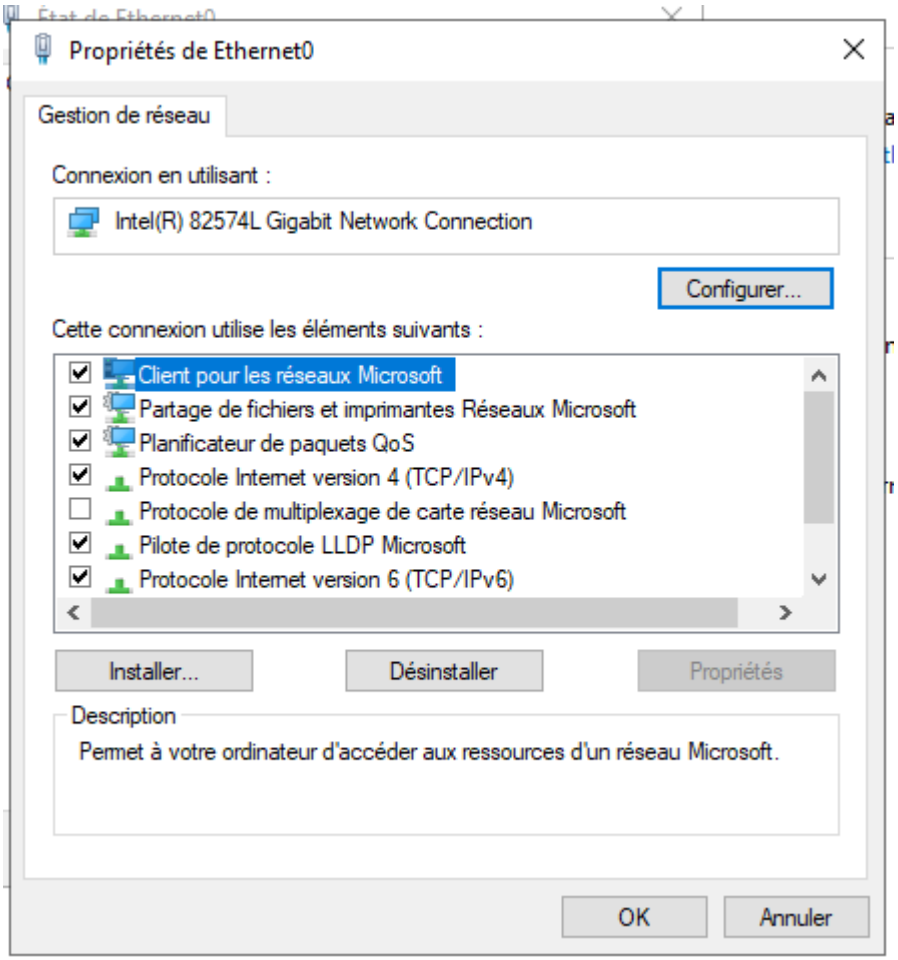


Figure 22:Propriétés de la carte réseau Etherneto

Les propriétés de la carte réseau montrent les composants installés. Nous allons configurer manuellement le protocole TCP/IPv4 pour attribuer une adresse IP fixe au serveur.

6.5 CONFIGURATION DU PROTOCOLE TCP/IPV4

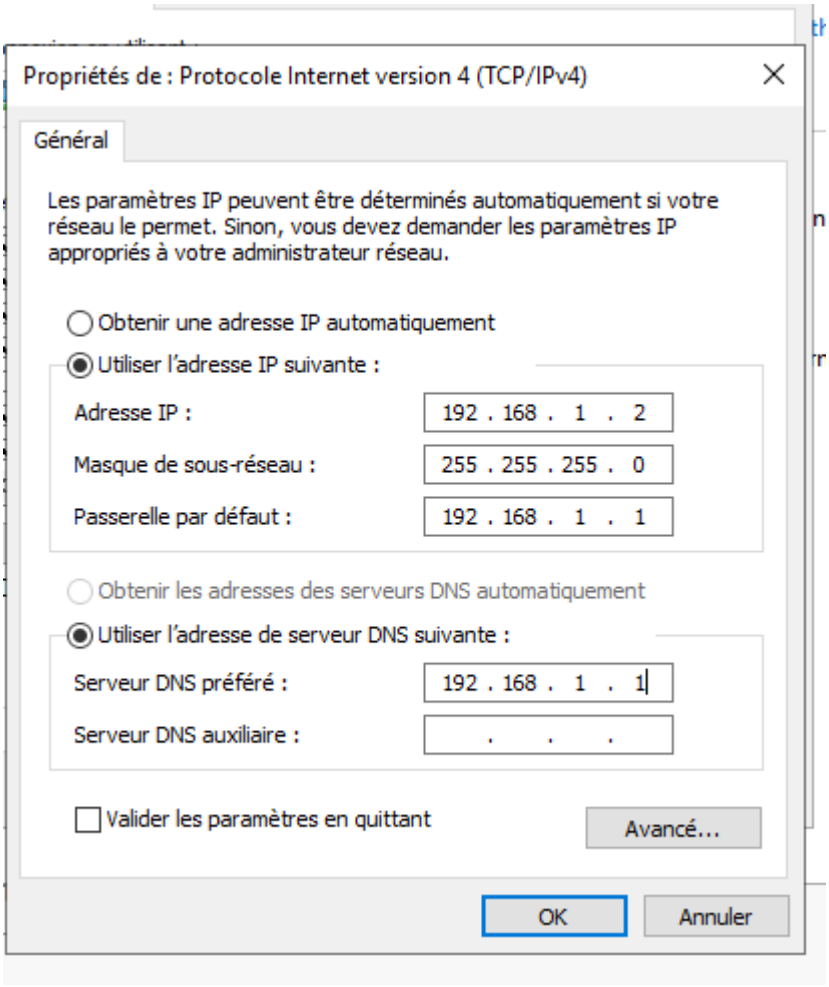


Figure 23:Propriétés du Protocole Internet version 4 (TCP/IPv4)

Nous configurons une adresse IP statique pour le serveur Active Directory :

- **Adresse IP** : 192.168.1.2
- **Masque** : 255.255.255.0
- **Passerelle par défaut** : 192.168.1.1 (passerelle du réseau interne)
- **Serveur DNS préféré** : 192.168.1.1 (lui-même, car il hébergera le rôle DNS)

6.6 VERIFICATION AVEC LA COMMANDE IPCONFIG

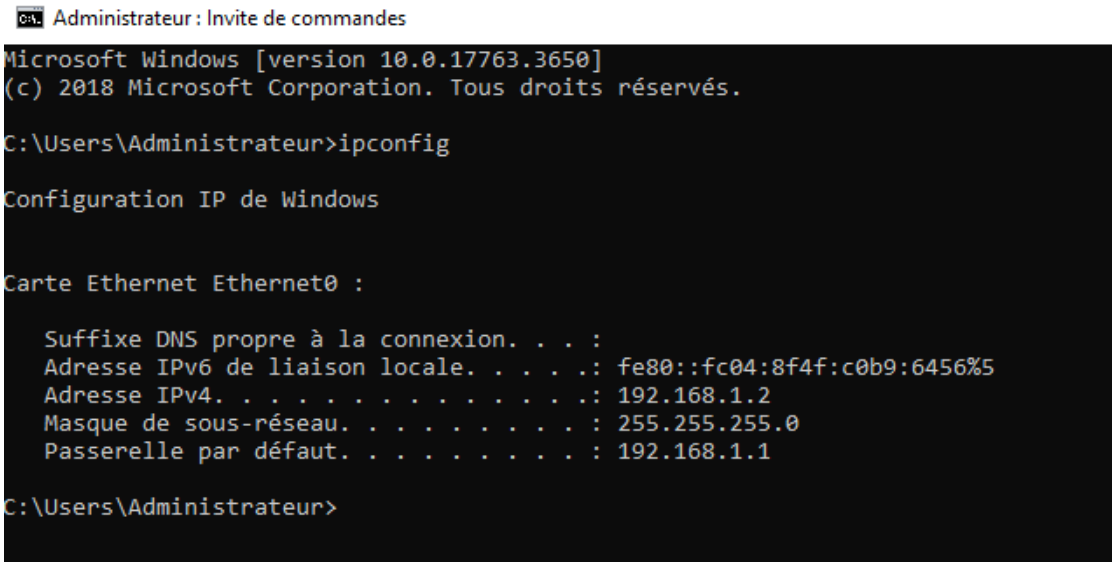


Figure 24:Affichage des paramètres IP de la carte Etherneto

La commande ipconfig confirme la bonne application des paramètres réseau. Le serveur est maintenant prêt pour l'installation des rôles Active Directory.

7. INSTALLATION DES RÔLES AD DS ET DNS

7.1 GESTIONNAIRE DE SERVEUR - TABLEAU DE BORD

Figure 25:Gestionnaire de serveur - Tableau de bord après configuration IP

Le gestionnaire de serveur affiche désormais les informations de base. Nous allons procéder à l'ajout des rôles nécessaires.

7.2 AJOUT DES ROLES ET FONCTIONNALITES

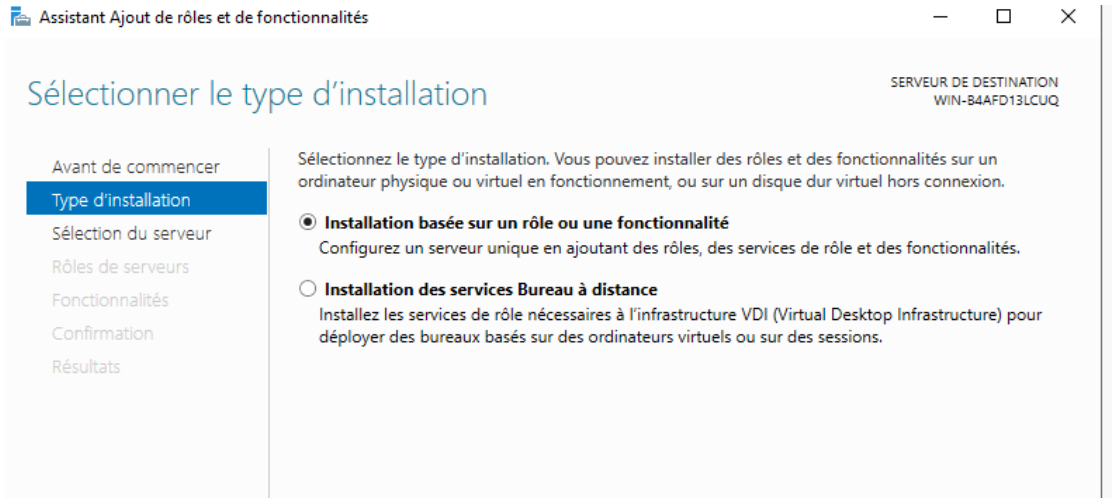


Figure 26:Ajout des rôles et fonctionnalités - Assistant de configuration

L'assistant d'ajout de rôles et fonctionnalités est lancé depuis le menu "Gérer" du gestionnaire de serveur.

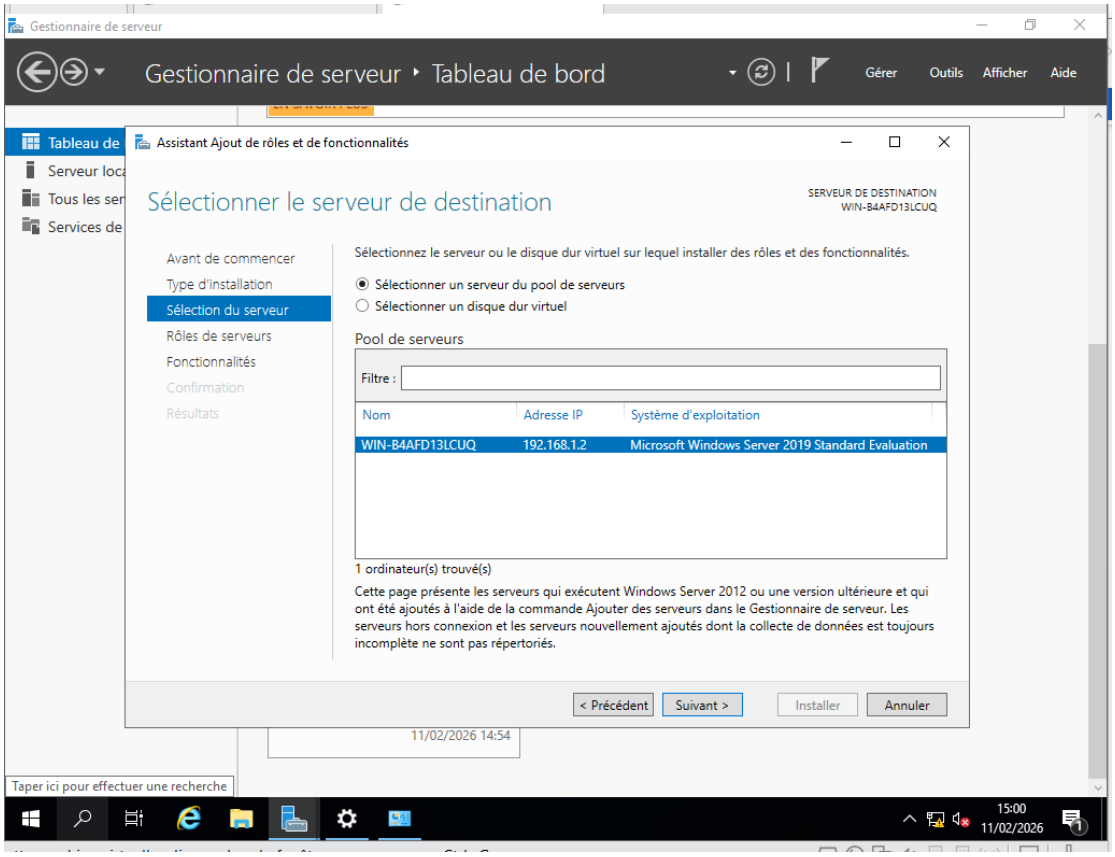


Figure 27:Sélection des rôles - Active Directory Domain Services (AD DS

Nous sélectionnons le rôle **Active Directory Domain Services**, qui inclut également les outils nécessaires à la gestion du domaine.

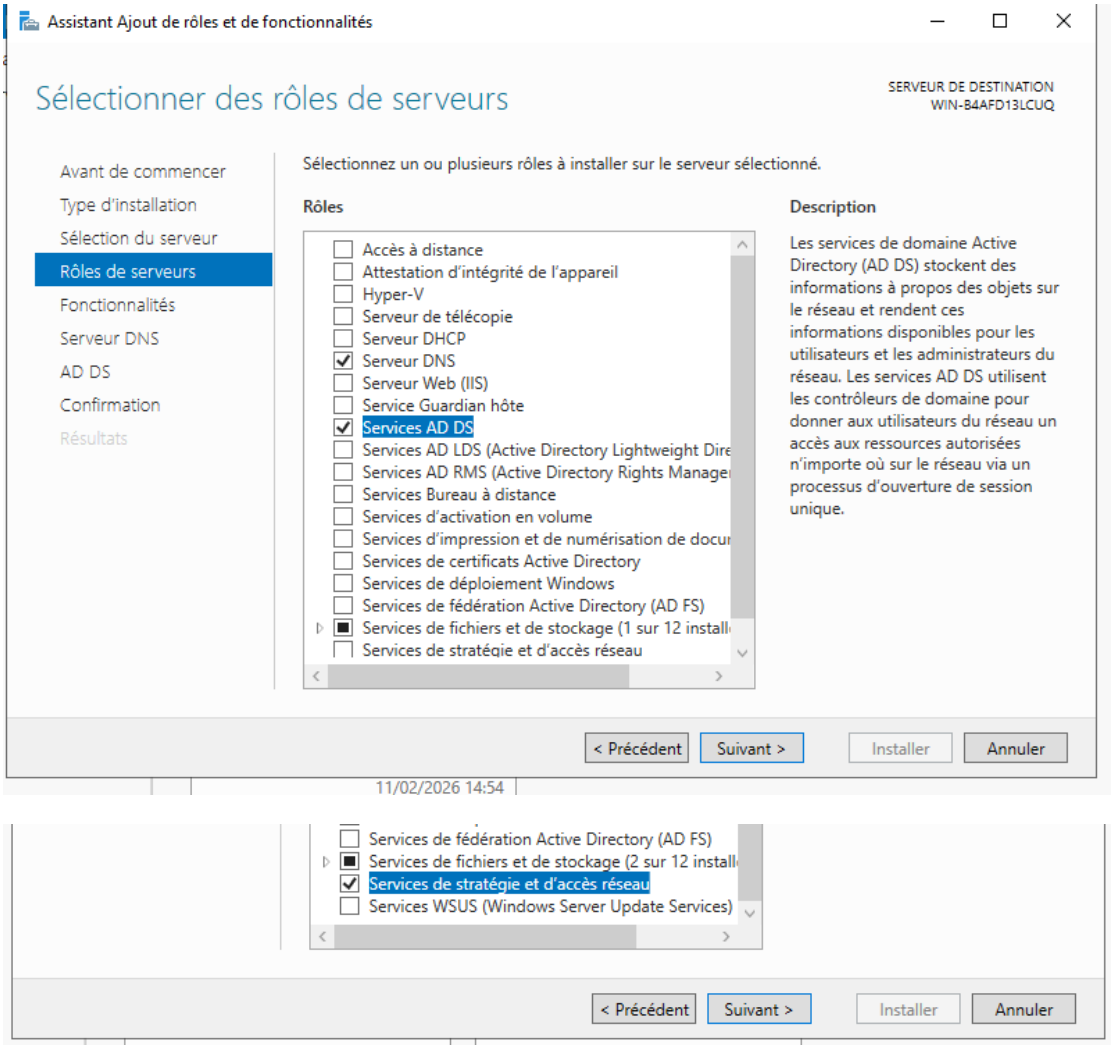


Figure 28: Sélection des fonctionnalités additionnelles - Outils d'administration de rôle AD DS

L'assistant propose d'ajouter les fonctionnalités requises pour AD DS, notamment les outils d'administration. Nous acceptons ces ajouts.

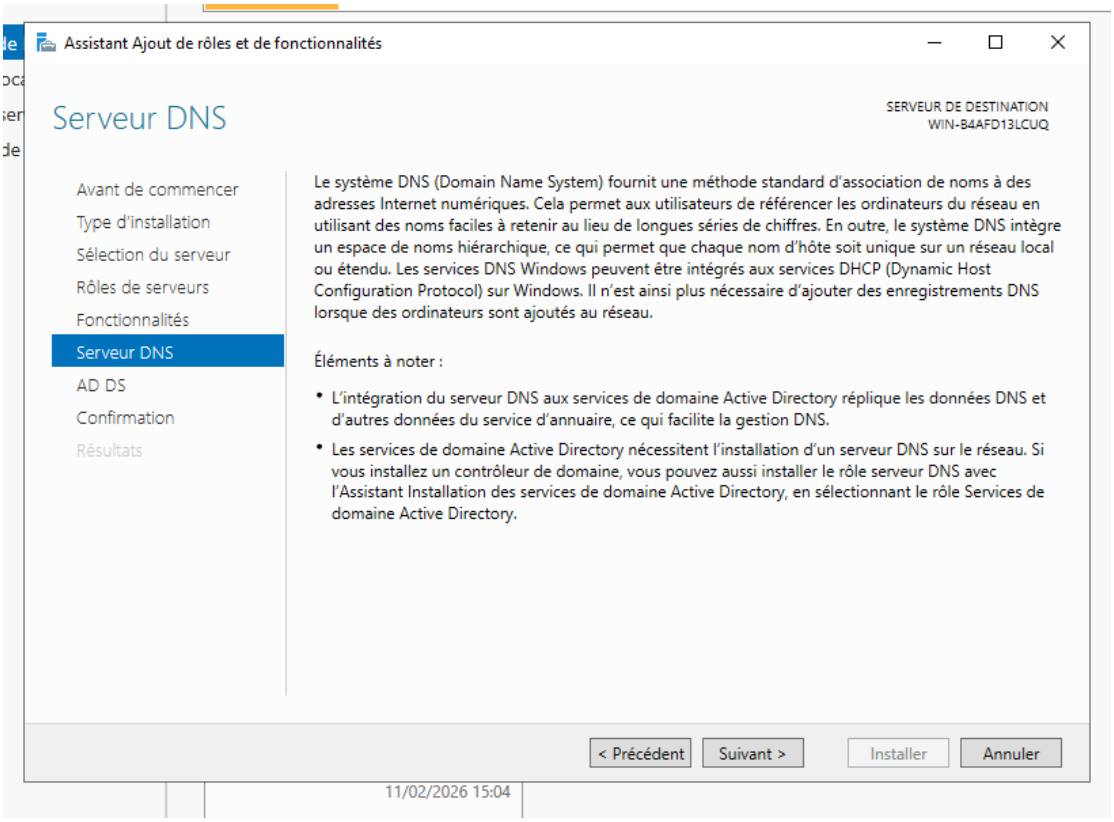


Figure 29: Installation des rôles AD DS et DNS en cours - On configure l'AD et le DNS

L'installation des rôles se déroule. Une fois terminée, le serveur doit être promu en contrôleur de domaine.

8. CONFIGURATION DU DOMAINE ACTIVE DIRECTORY

8.1 PROMOTION EN CONTROLEUR DE DOMAINE

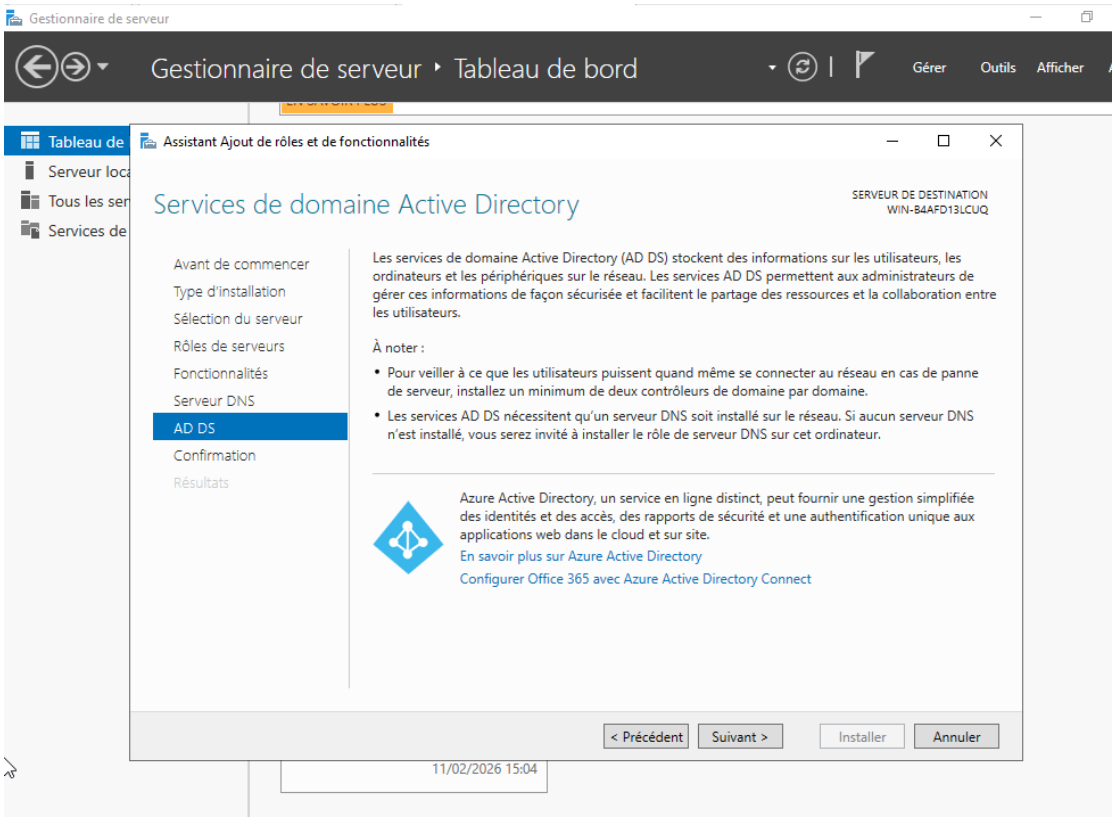


Figure 30: Promotion du serveur en contrôleur de domaine

Après l'installation des rôles, un drapeau jaune apparaît dans le gestionnaire de serveur, indiquant qu'il faut procéder à la promotion du serveur en contrôleur de domaine.

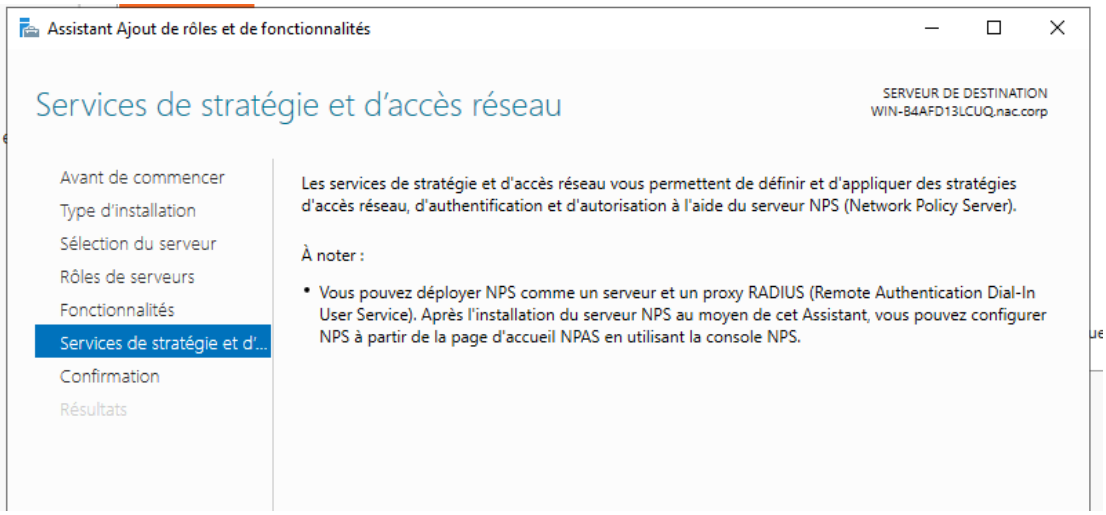


Figure 31:Assistant de configuration des services de domaine Active Directory

L'assistant de configuration des services de domaine permet de créer une nouvelle forêt, un nouveau domaine, ou d'ajouter un contrôleur à un domaine existant.

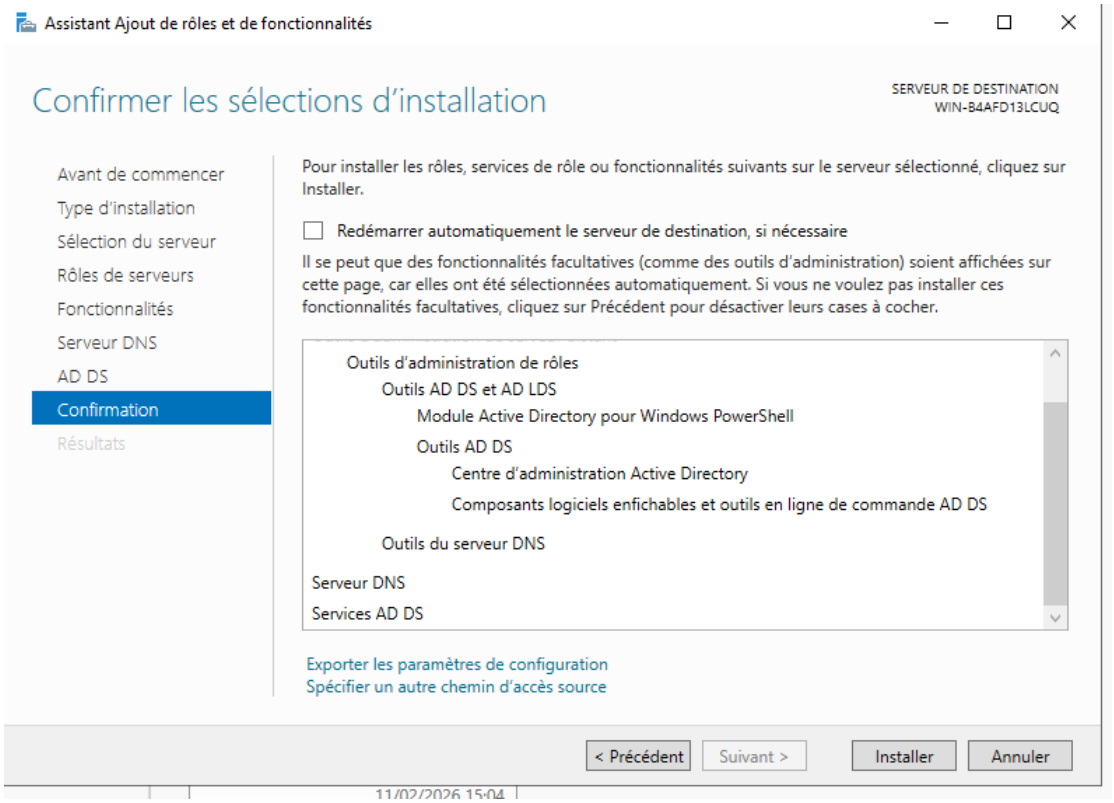


Figure 32:Confirmation et installation

Nous vérifions que tous les composants nécessaires sont bien sélectionnés :

- Services AD DS (Active Directory Domain Services)
- Serveur DNS

- Outils d'administration : Module Active Directory pour PowerShell, Centre d'administration Active Directory, composants logiciels enfichables

Nous cliquons sur "Installer" pour lancer l'installation.

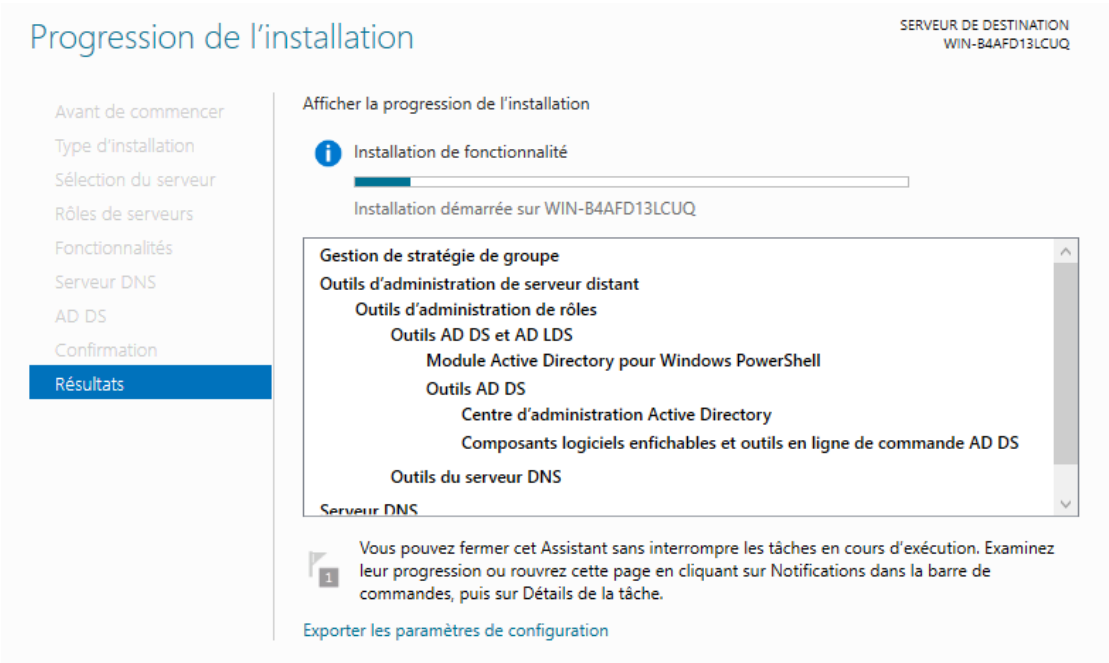


Figure 33: Progression de l'installation

L'installation des rôles et fonctionnalités est en cours. Nous pouvons suivre la progression directement dans l'assistant. Cette étape peut prendre quelques minutes.

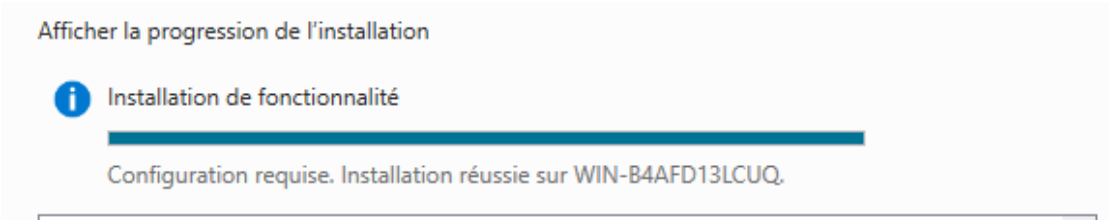


Figure 34: Installation terminée

L'installation s'est terminée avec succès. Tous les composants nécessaires sont maintenant installés. Le serveur est prêt à être promu en contrôleur de domaine.

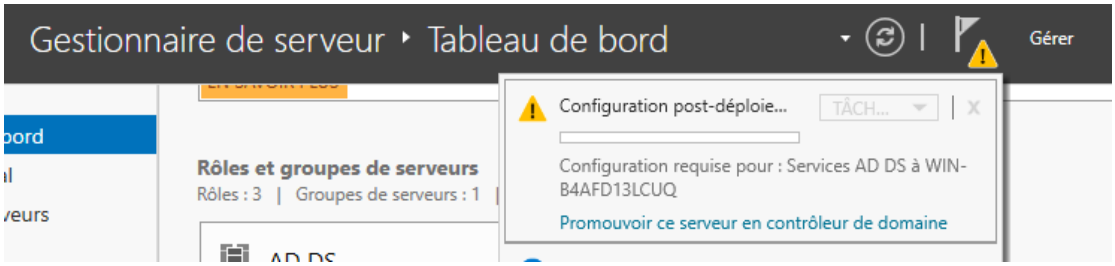


Figure 35:Gestionnaire de serveur

Après l'installation réussie des rôles AD DS et DNS, le gestionnaire de serveur affiche une notification avec un drapeau jaune. Cette notification nous invite à "Promouvoir ce serveur en contrôleur de domaine". C'est l'étape suivante pour créer notre domaine nac.local.

8.2 CREATION DU DOMAINE NAC.LOCAL

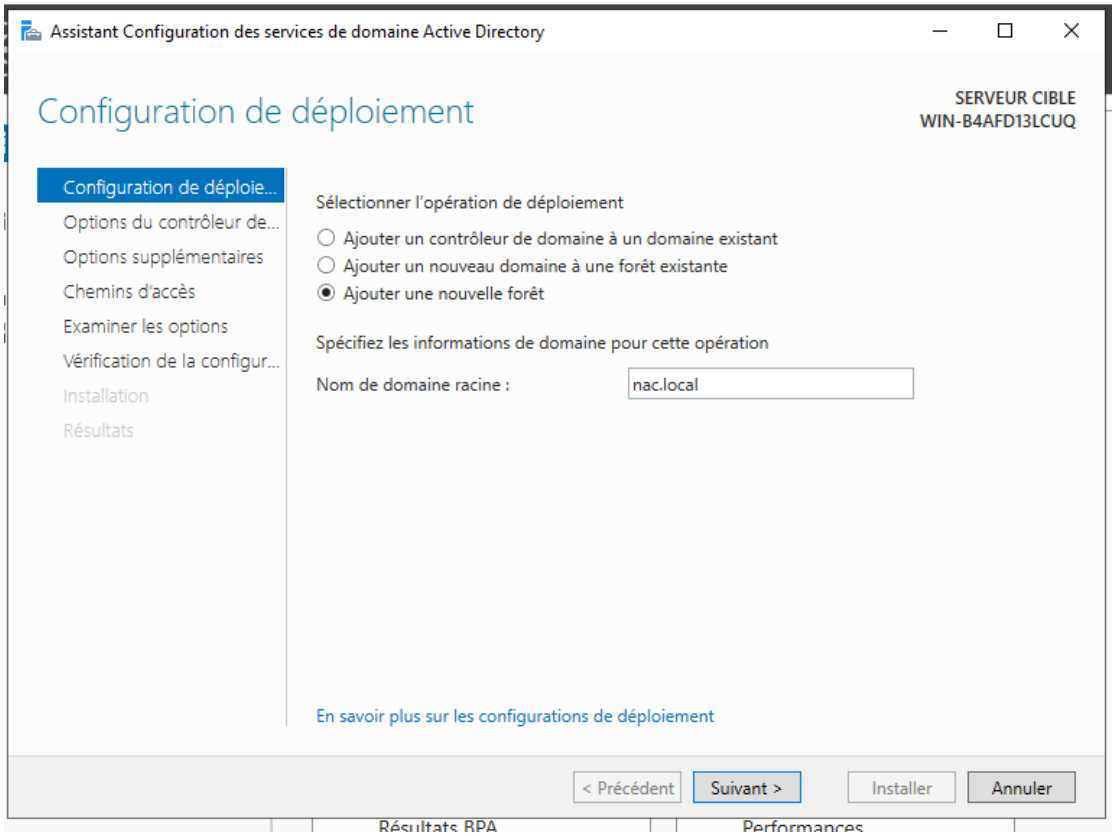


Figure 36: Création d'une nouvelle forêt - Configuration du nom de domaine "nac.local

Nous choisissons l'option **Ajouter une nouvelle forêt** avec le nom de domaine **nac.local** (conformément aux spécifications du projet).

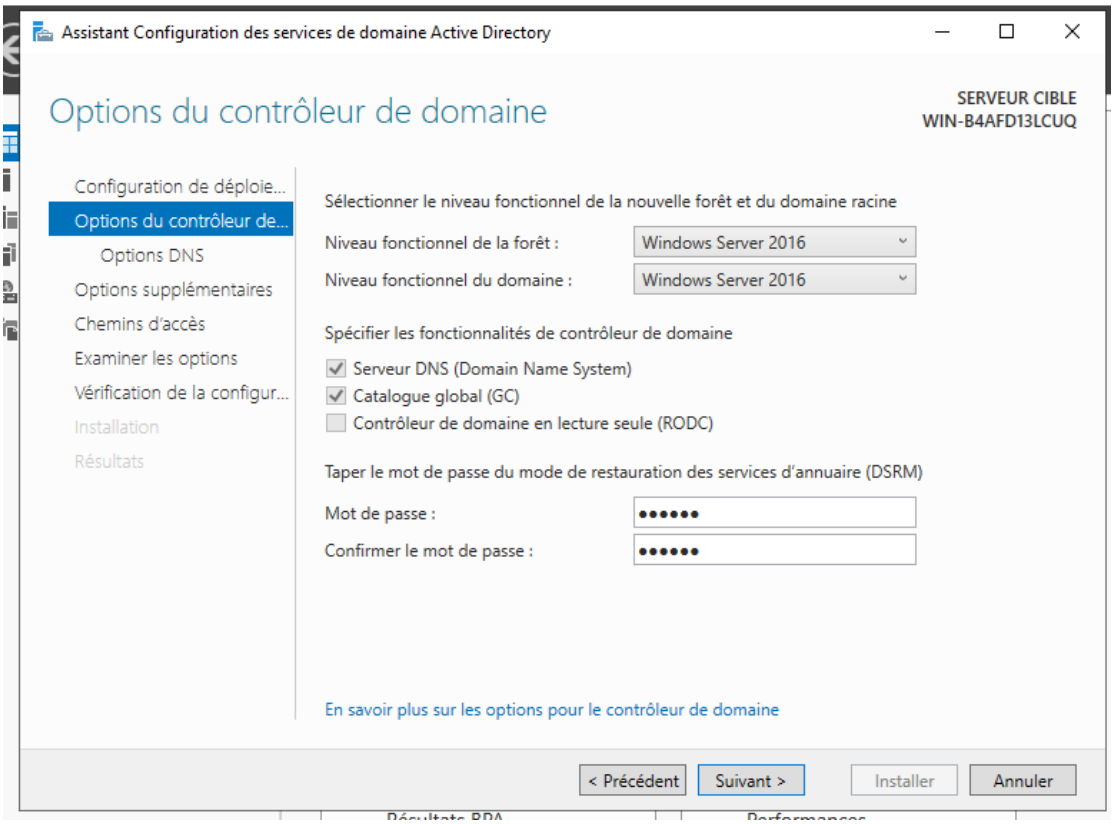


Figure 37 : Options du contrôleur de domaine - Niveau fonctionnel

Les niveaux fonctionnels sont laissés aux valeurs par défaut (Windows Server 2016). L'option "Serveur DNS" est cochée car nous avons installé ce rôle. Le mot de passe DSRM (Directory Services Restore Mode) est défini.

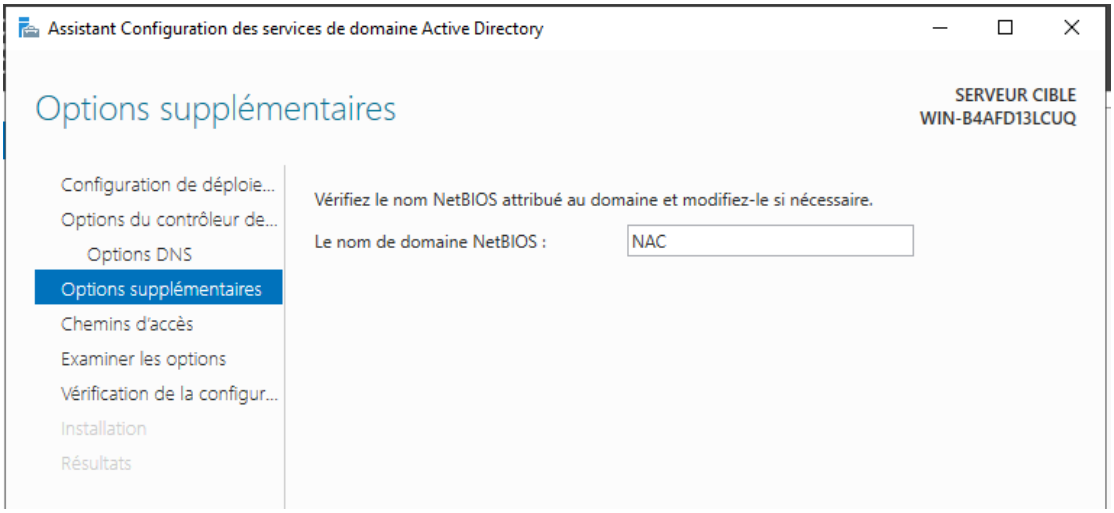


Figure 38:Vérification du nom NetBIOS du domaine

Nous vérifions que le nom NetBIOS attribué automatiquement est bien "NAC". Ce nom sera utilisé pour l'identification du domaine sur le réseau. Nous conservons cette valeur par défaut et poursuivons la configuration.

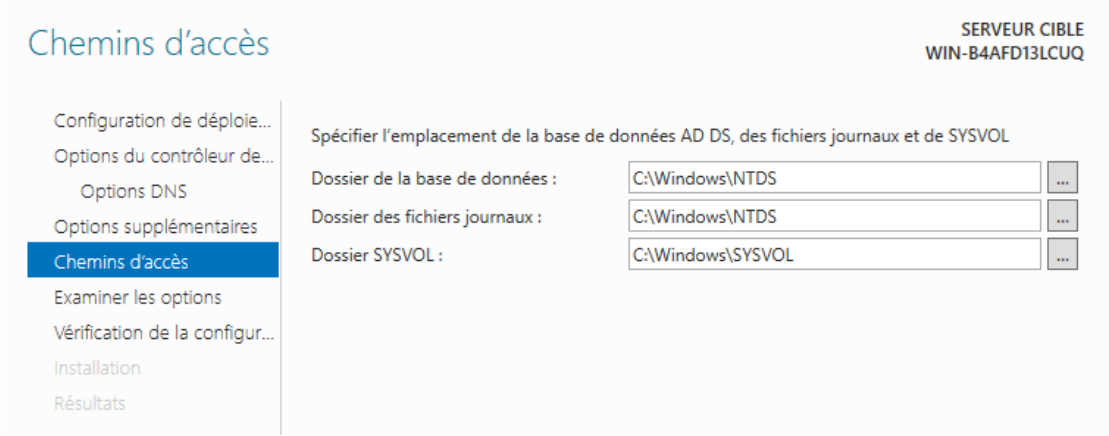


Figure 39:Emplacement des fichiers de base de données AD

Nous conservons les emplacements par défaut pour la base de données AD, les fichiers journaux et le dossier SYSVOL.

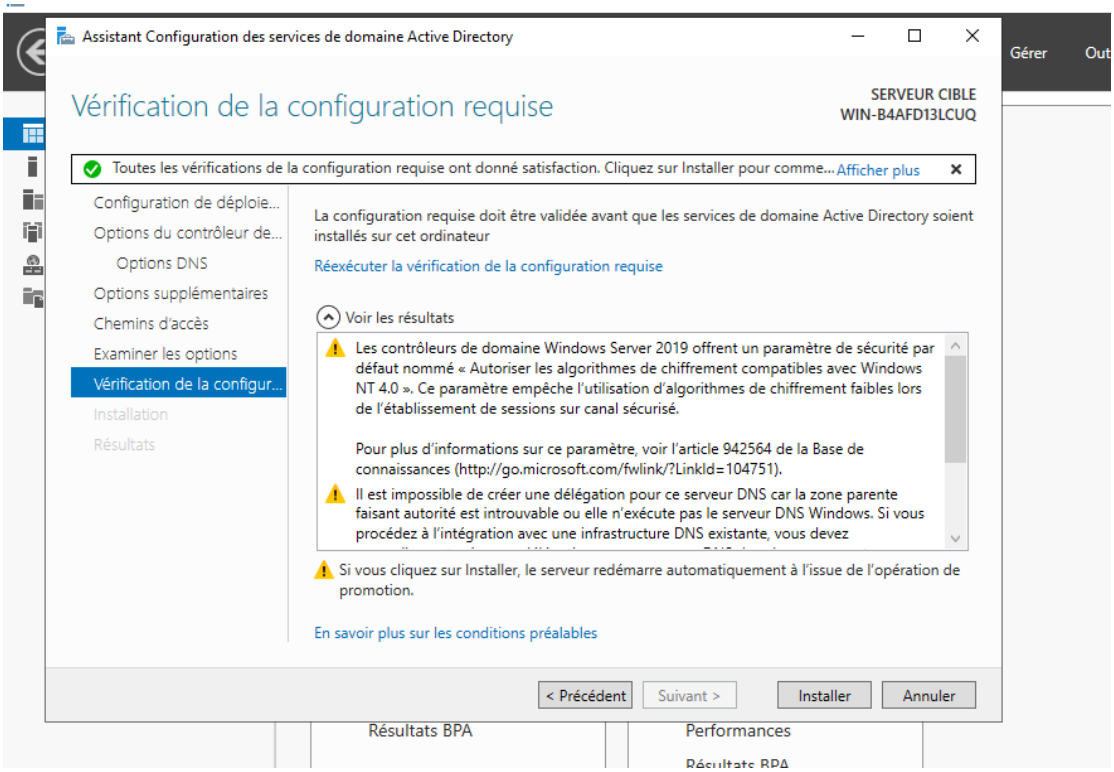


Figure 40: Vérification des prérequis avant installation

L'assistant effectue une vérification des prérequis. Tous les tests sont réussis, nous pouvons procéder à l'installation.

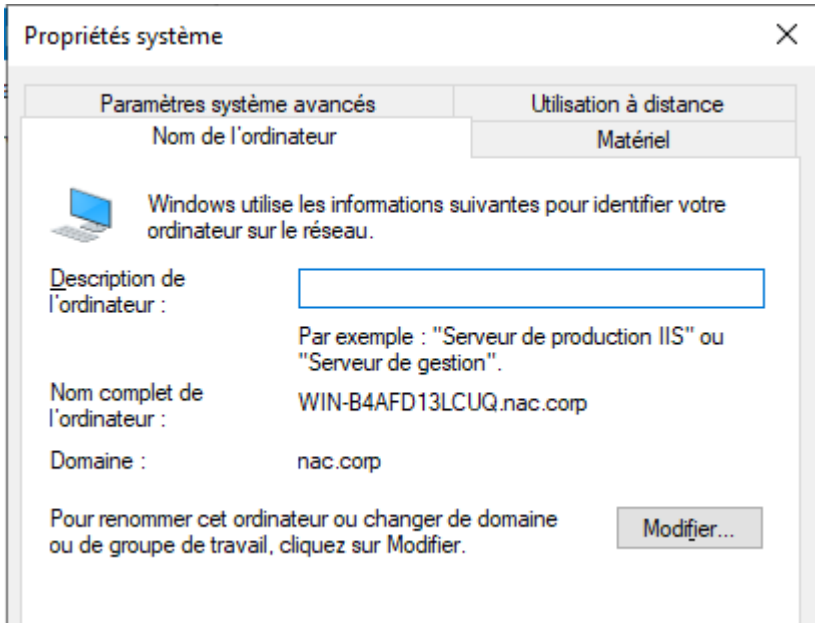


Figure 41: Installation et configuration du DNS - Création de la zone

L'installation configure automatiquement le DNS avec la zone correspondant au domaine nac.local

Figure 42: Finalisation de la promotion du serveur - Redémarrage nécessaire

Une fois la configuration terminée, le serveur redémarre pour appliquer les changements.

10. CONFIGURATION AVANCÉE DU DNS

10.1 ACCES AU GESTIONNAIRE DNS

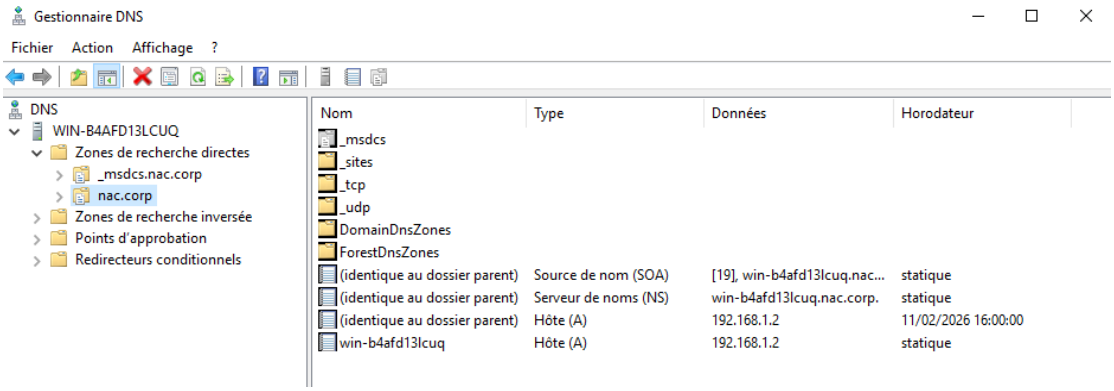


Figure 43:Configuration du DNS

Depuis le gestionnaire de serveur, nous accédons au gestionnaire DNS via le menu **Outils**.

10.2 CREATION DE LA ZONE DE RECHERCHE INVERSEE

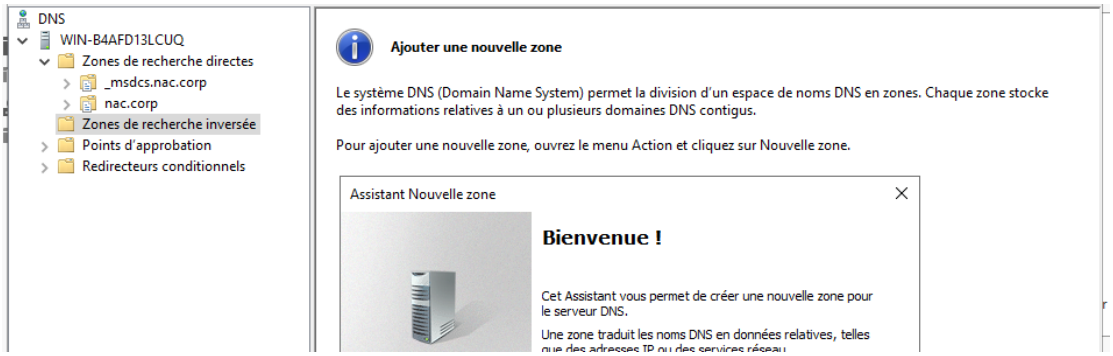


Figure 44: Création d'une nouvelle zone - Assistant

Nous créons une nouvelle zone de recherche inversée pour permettre la résolution des adresses IP en noms d'hôtes.

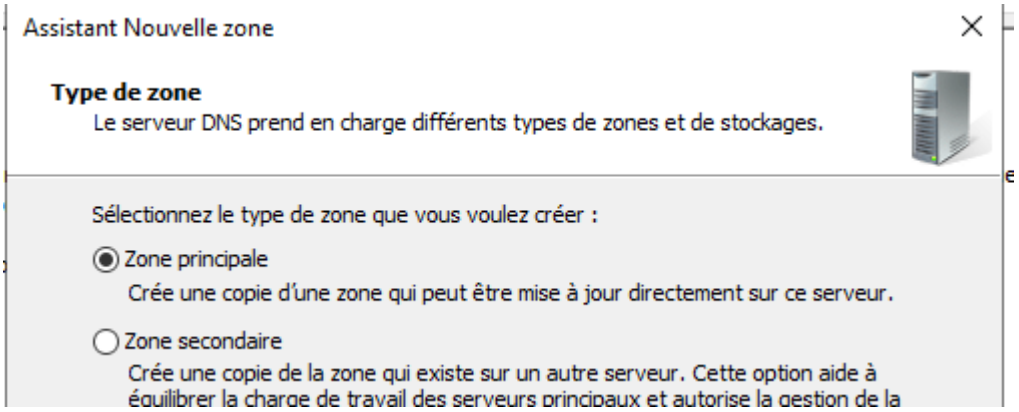


Figure 45:Type de zone - Zone principale

Nous choisissons une zone principale, stockée sur ce contrôleur de domaine.

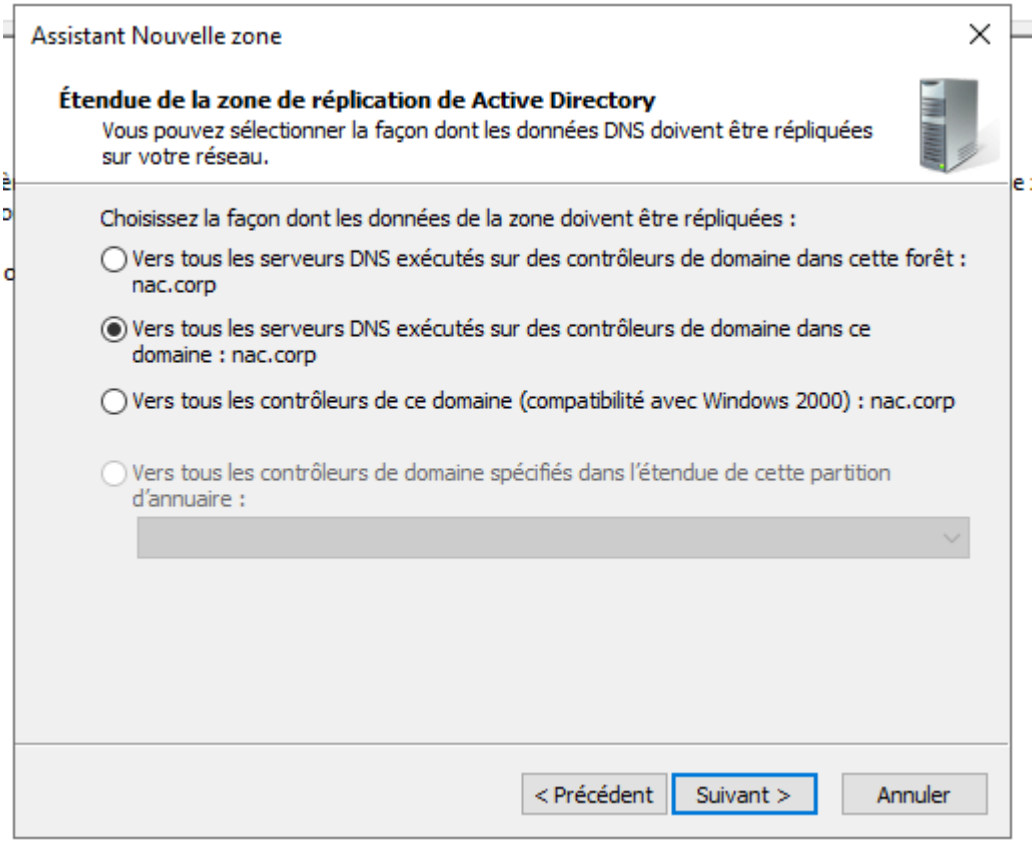


Figure 46:Assistant Nouvelle zone

Nous choisissons l'option de réplication "Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine". Cette option garantit que les enregistrements DNS seront répliqués sur tous les contrôleurs de domaine du domaine nac.corp, assurant ainsi la redondance et la disponibilité du service DNS.

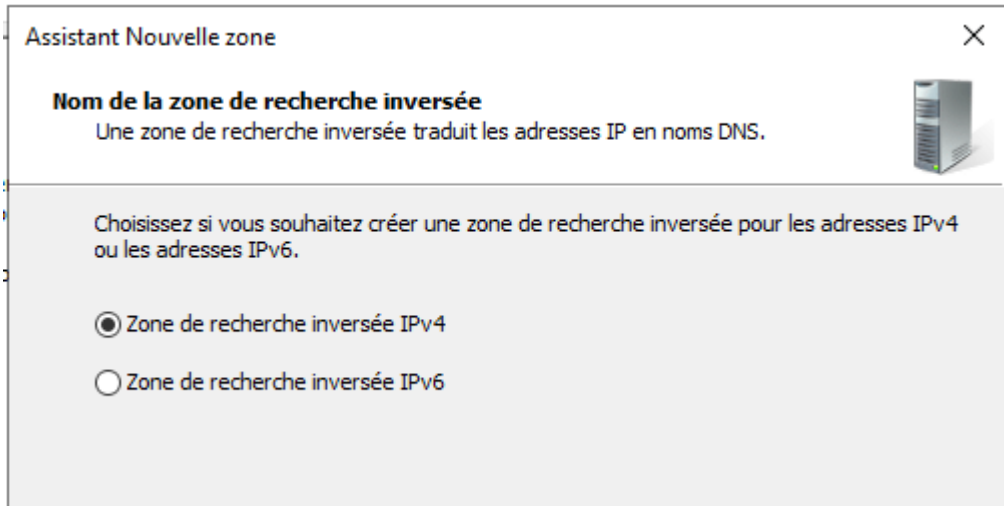


Figure 47:Configuration de la zone de recherche inversée

Nous sélectionnons une zone de recherche inversée IPv4.

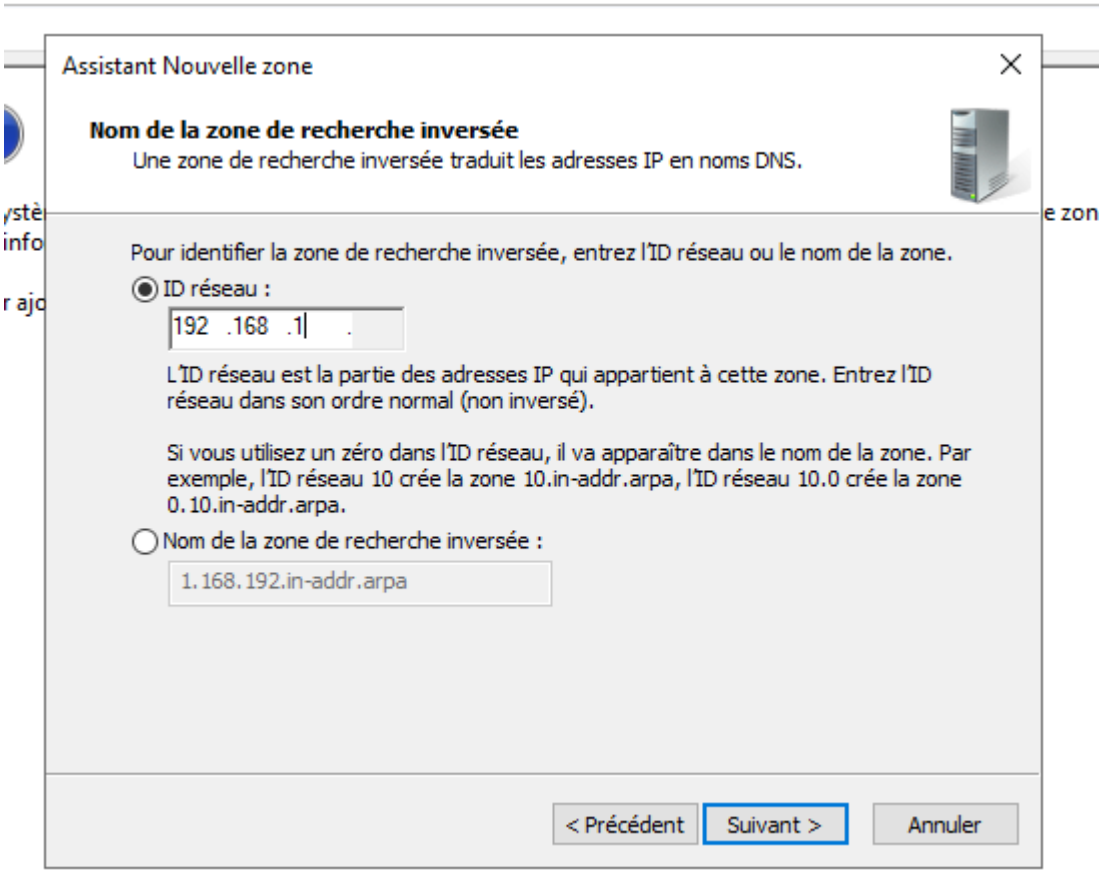


Figure 48:Définition de l'ID réseau pour la zone inversée

Nous spécifions l'ID réseau **192.168.1.0/24**. La zone inversée correspondante (1.168.192.in-addr.arpa) sera créée automatiquement.

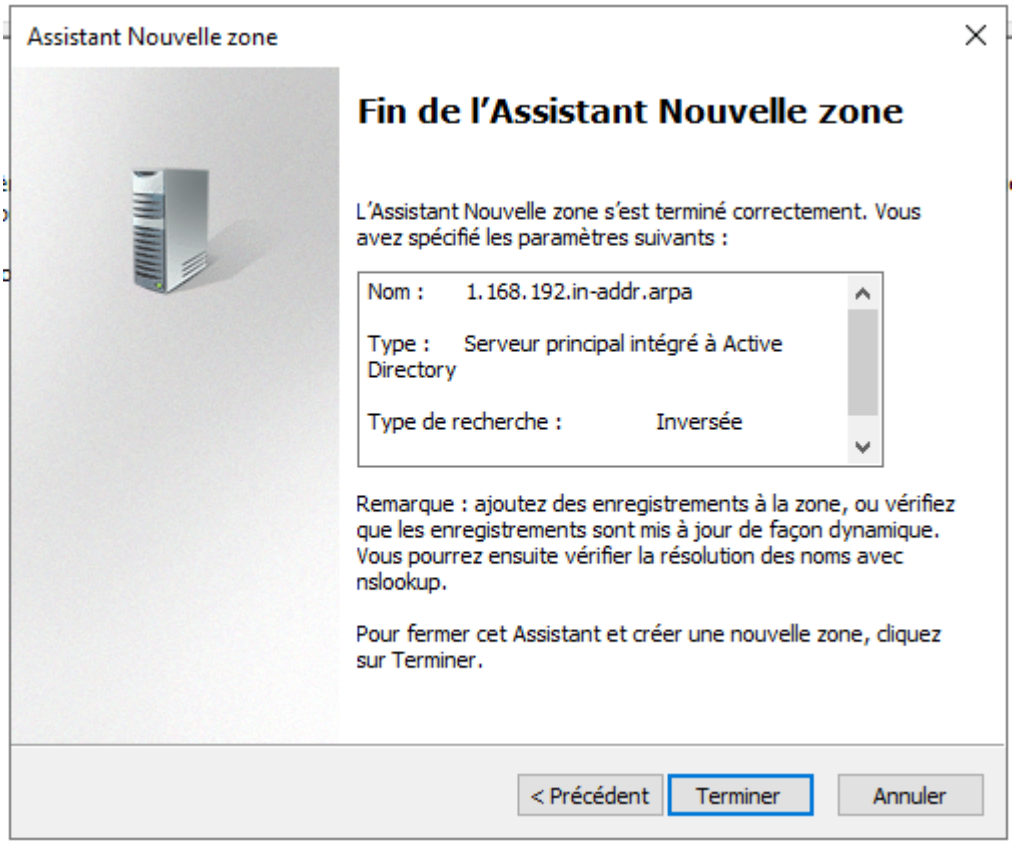


Figure 49:Nom du fichier de zone

Le nom du fichier de zone est généré automatiquement. Nous conservons la valeur par défaut.

La zone inverse a été créée

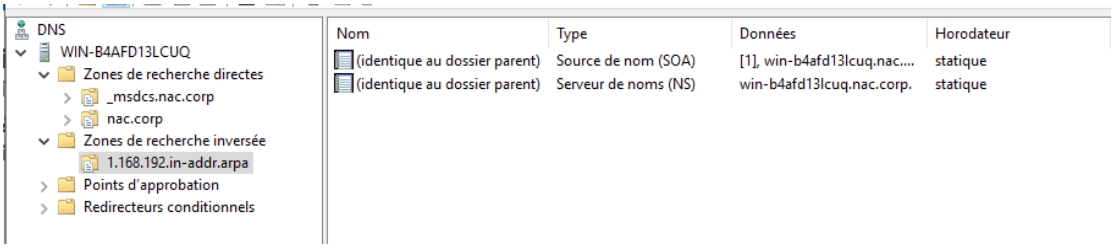


Figure 50:Finalisation de la création de la zone

L'assistant confirme la création de la zone. La zone de recherche inversée apparaît maintenant dans la console DNS, prête à recevoir des enregistrements PTR.

10.3 CREATION DES ENREGISTREMENTS PTR

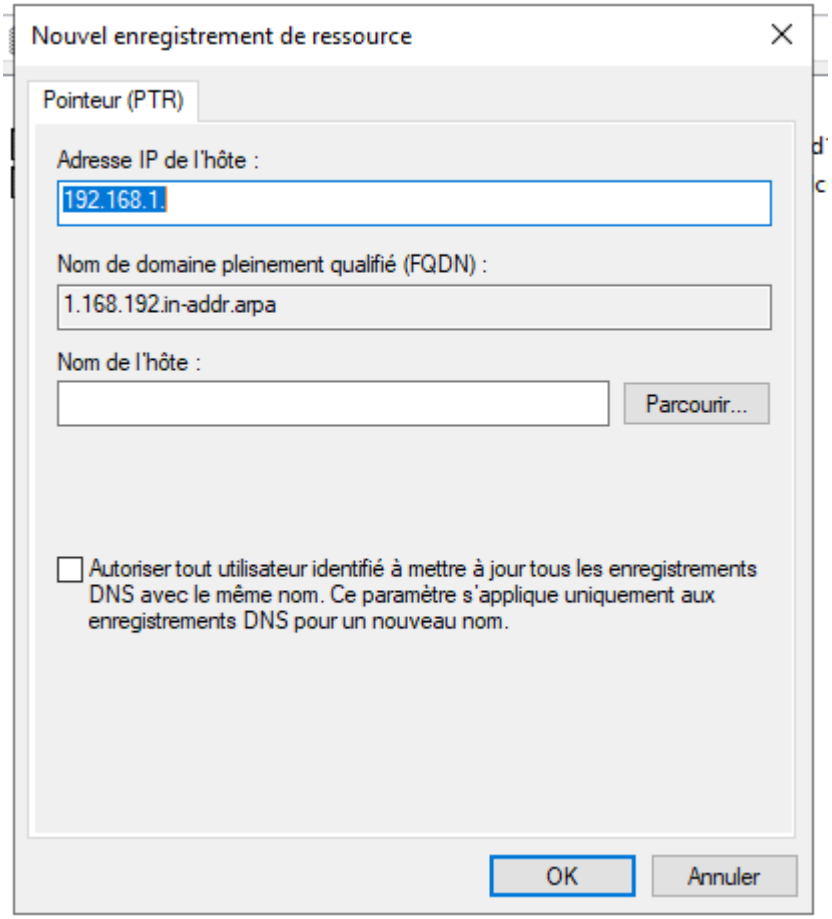


Figure 51: Création d'un nouveau pointeur

Dans la zone inversée, nous créons un nouvel enregistrement PTR (pointeur) pour associer l'adresse IP 192.168.1.2 au nom d'hôte du serveur.

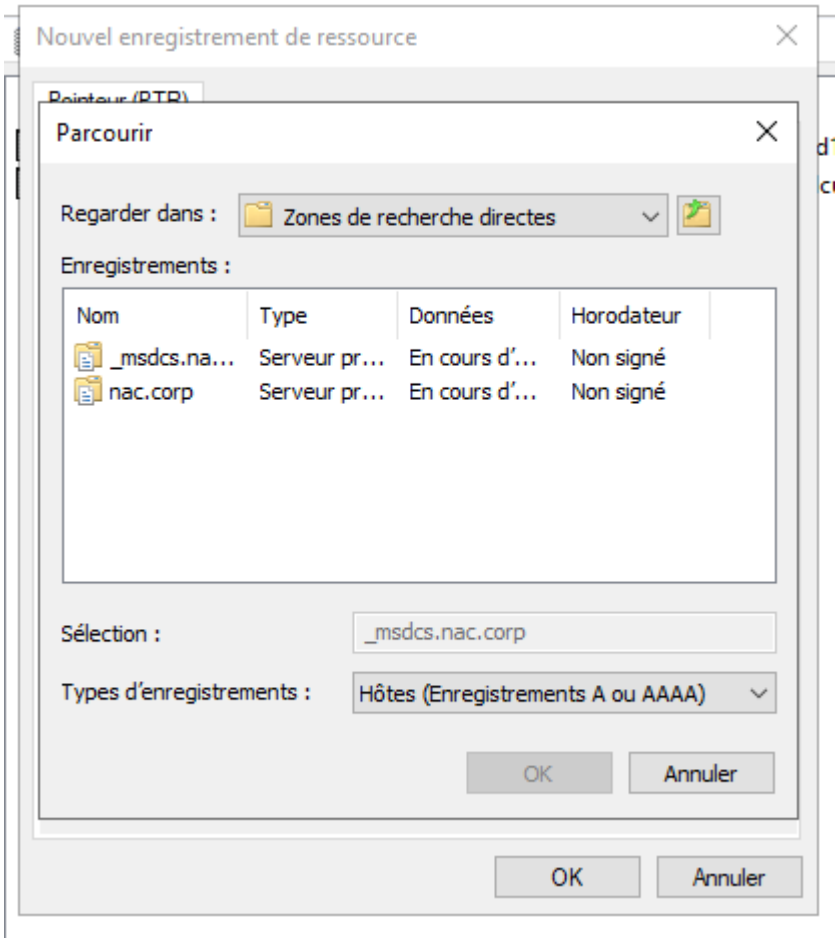


Figure 52: Assistant de création du pointeur

L'assistant de création de pointeur s'ouvre.

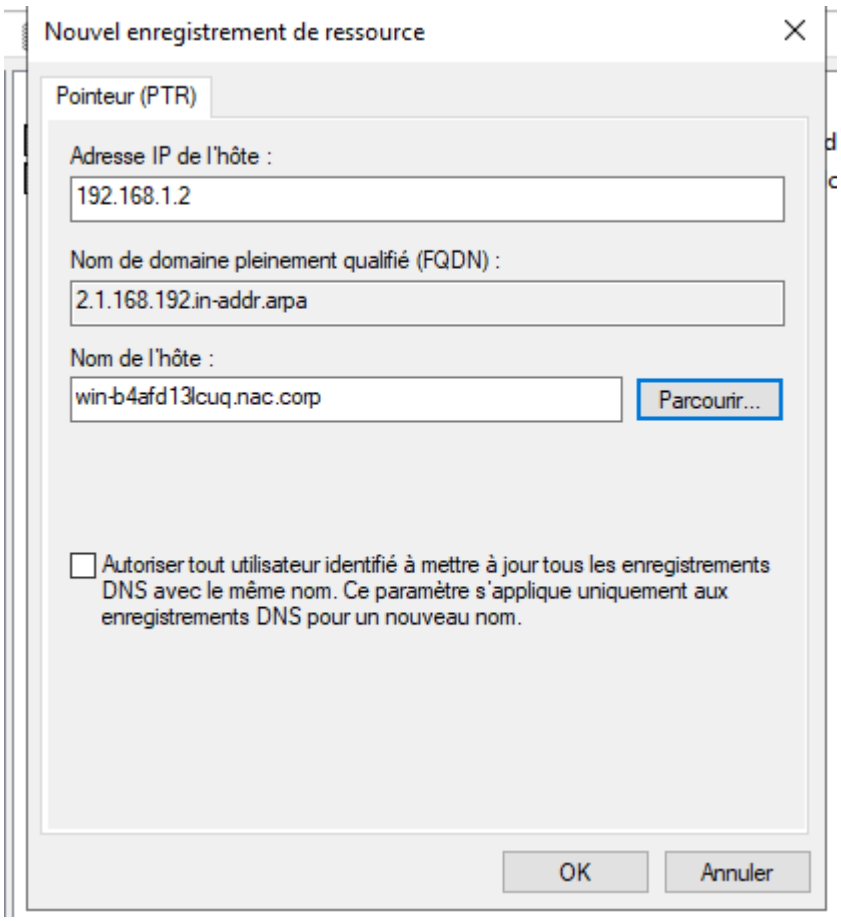


Figure 53:Configuration de l'enregistrement PTR

Nous spécifions l'adresse IP (192.168.1.2) et le nom d'hôte pleinement qualifié (FQDN) du serveur : **WIN-...nac.local**.

L'enregistrement PTR est créé et apparaît dans la zone inversée.

Une fois le pointeur créé, on actualise puis on exécute un nslookup

10.4 TEST DE RESOLUTION AVEC NSLOOKUP

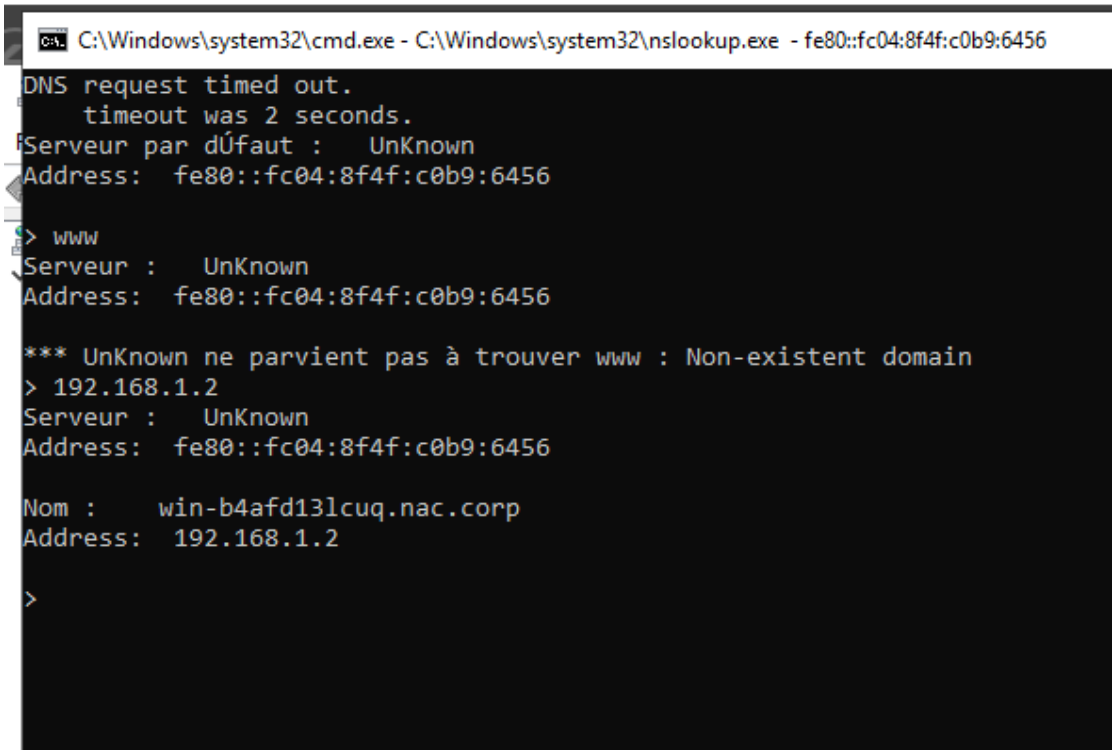


Figure 54:Test de résolution DNS avec nslookup

La commande nslookup permet de vérifier la résolution de noms. Nous testons la résolution directe et inverse pour confirmer le bon fonctionnement du DNS.

Maintenant, on configure le CNAME pour pouvoir accéder au domaine.

10.5 CONFIGURATION DE L'ENREGISTREMENT CNAME

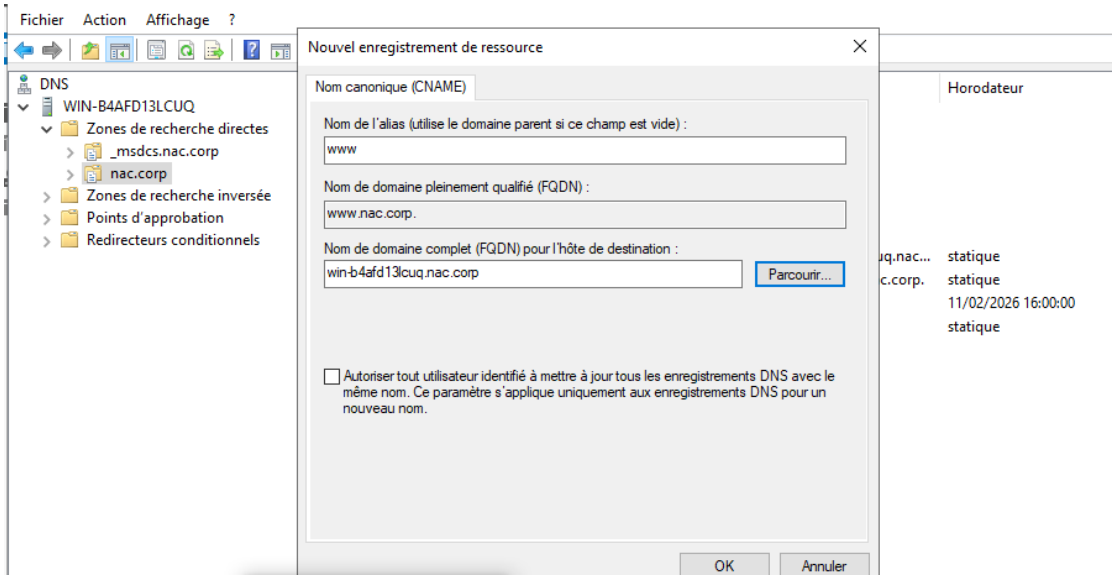


Figure 55:Configuration d'un enregistrement CNAME

Un enregistrement CNAME (alias) est créé pour faciliter l'accès au serveur. Par exemple, "ad.nac.local" peut pointer vers le nom réel du serveur.

10.6 DESACTIVATION D'IPV6

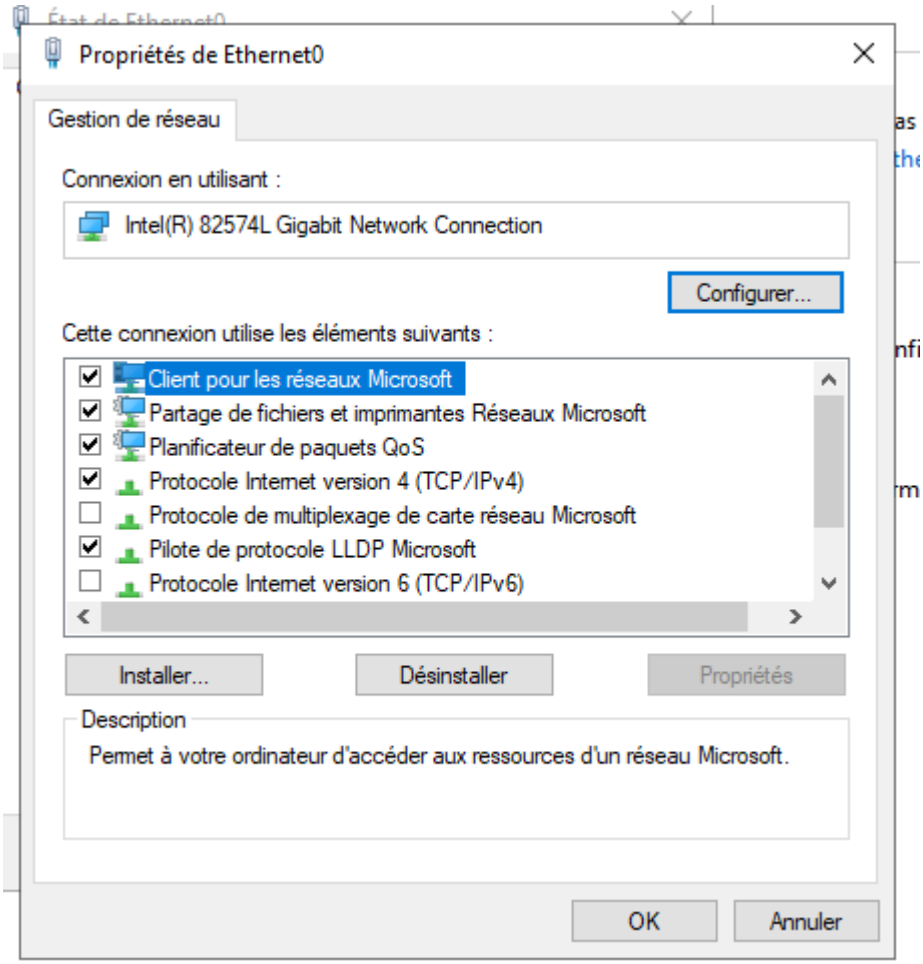


Figure 56:Désactivation du protocole IPv6 - Il faut pas oublier de désactiver le IPv6

Pour éviter les conflits potentiels entre IPv4 et IPv6, nous désactivons le protocole IPv6 sur la carte réseau du serveur.

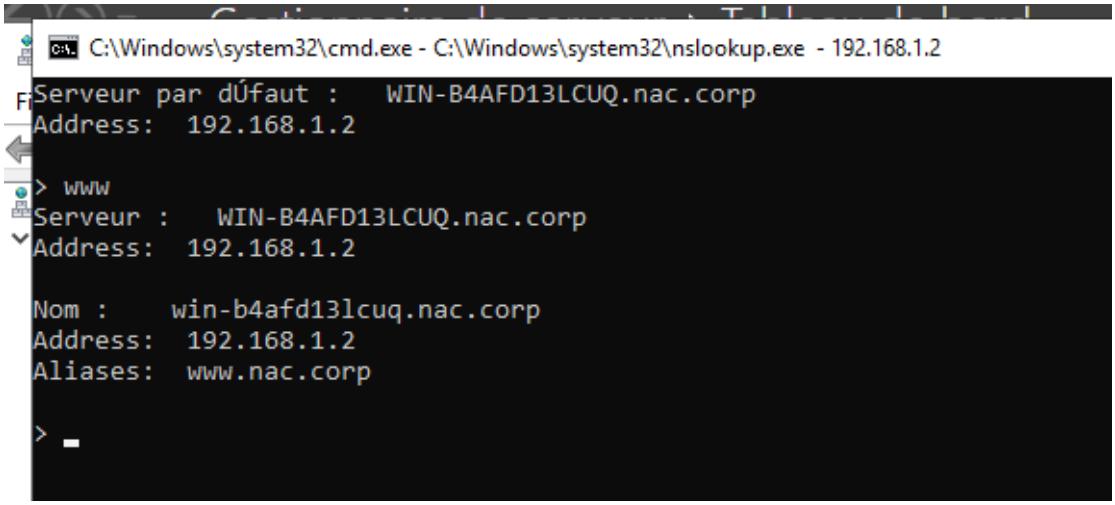


Figure 57:Vérification de la configuration réseau après désactivation IPv6

Après désactivation, la commande ipconfig ne montre plus que l'adresse IPv4, confirmant que IPv6 est bien désactivé.

11. CRÉATION DES UTILISATEURS ET GROUPES

11.1 ACCES A "UTILISATEURS ET ORDINATEURS ACTIVE DIRECTORY"

Pour ceci, se diriger vers le gestionnaire de serveur -> outils -> Utilisateurs et ordinateurs Active Directory

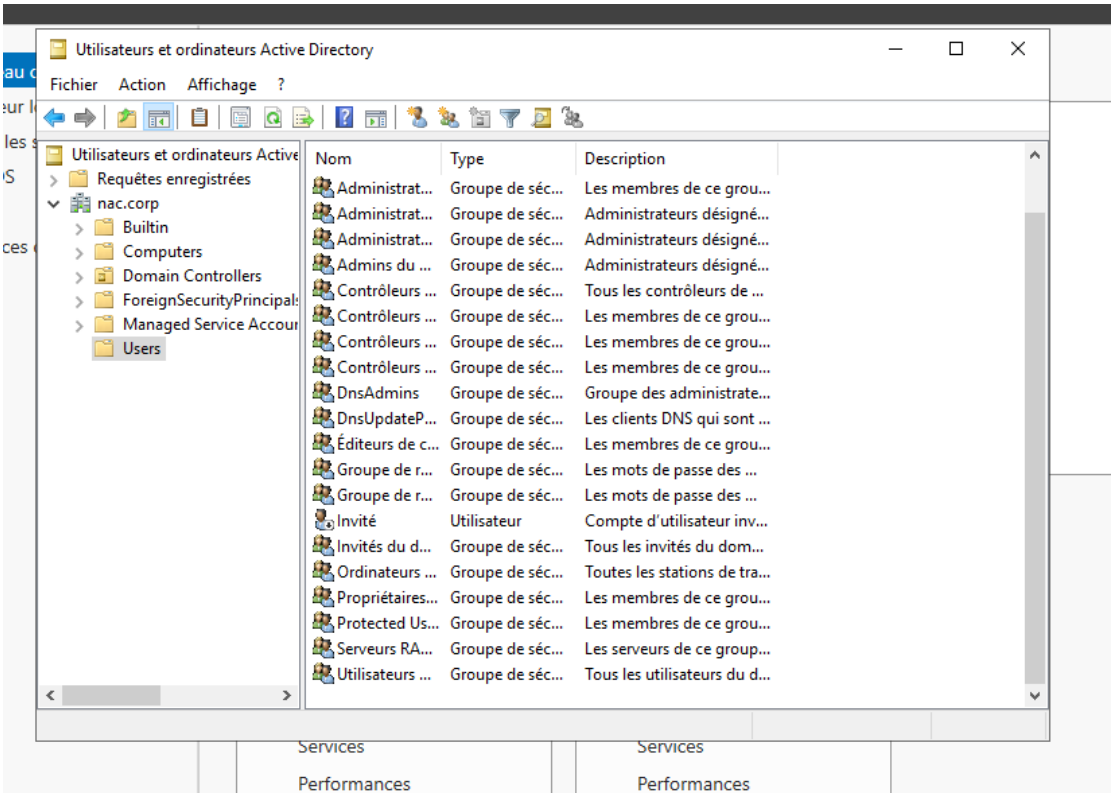


Figure 58:Accès à "Utilisateurs et ordinateurs Active Directory"

Depuis le gestionnaire de serveur, nous accédons à la console **Utilisateurs et ordinateurs Active Directory** pour créer les objets nécessaires.

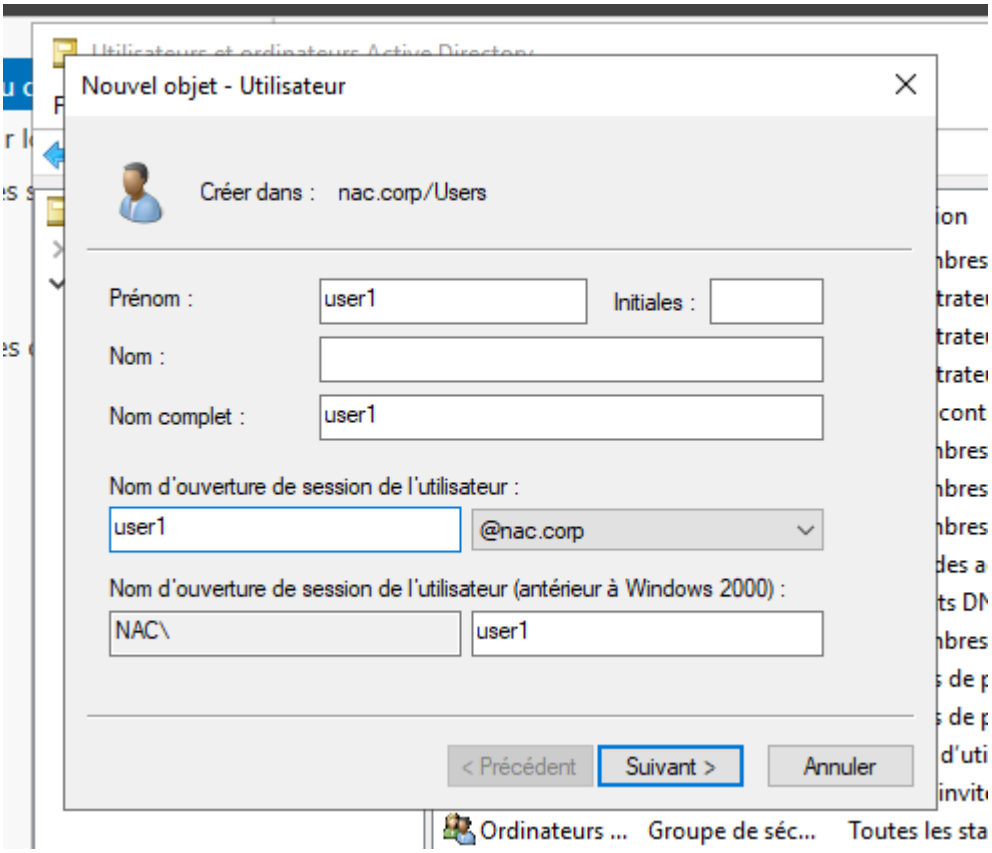


Figure 59:Console Active Directory

La console affiche la structure du domaine avec les conteneurs par défaut : Builtin, Computers, Domain Controllers, Users, etc.

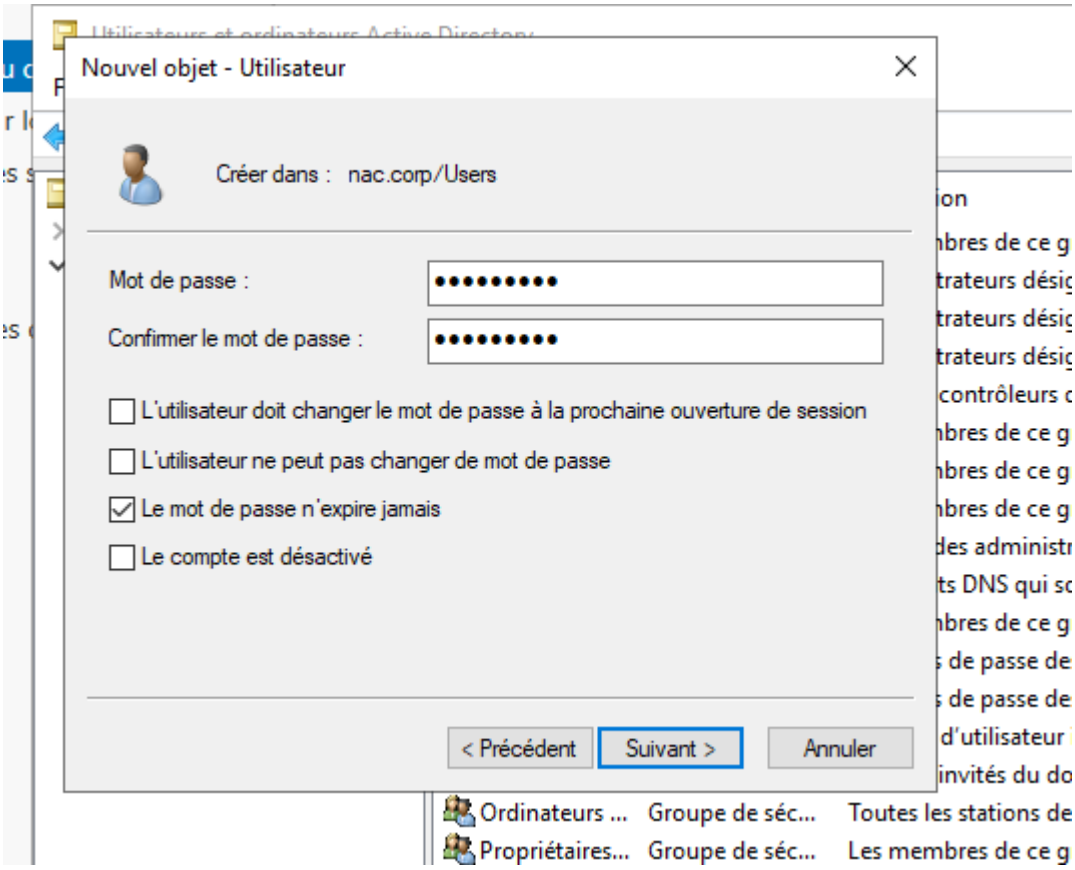


Figure 60:Assistant de création d'utilisateur

Nous configurons le mot de passe pour l'utilisateur en cours de création. Pour les utilisateurs de test dans ce projet, nous cochons l'option "Le mot de passe n'expire jamais" afin d'éviter les problèmes d'expiration de mot de passe pendant la durée du projet.

11.3 CREATION DES UTILISATEURS USER1 ET USER2

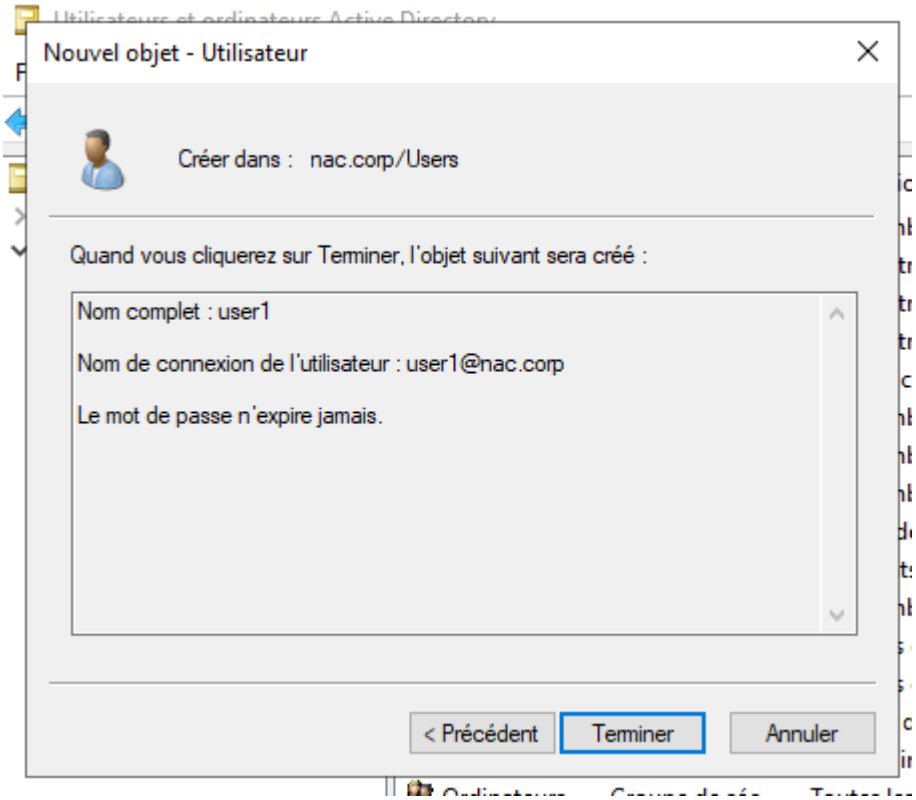


Figure 61: Création de l'utilisateur user1

Nous créons le premier utilisateur de test **user1** avec un mot de passe.

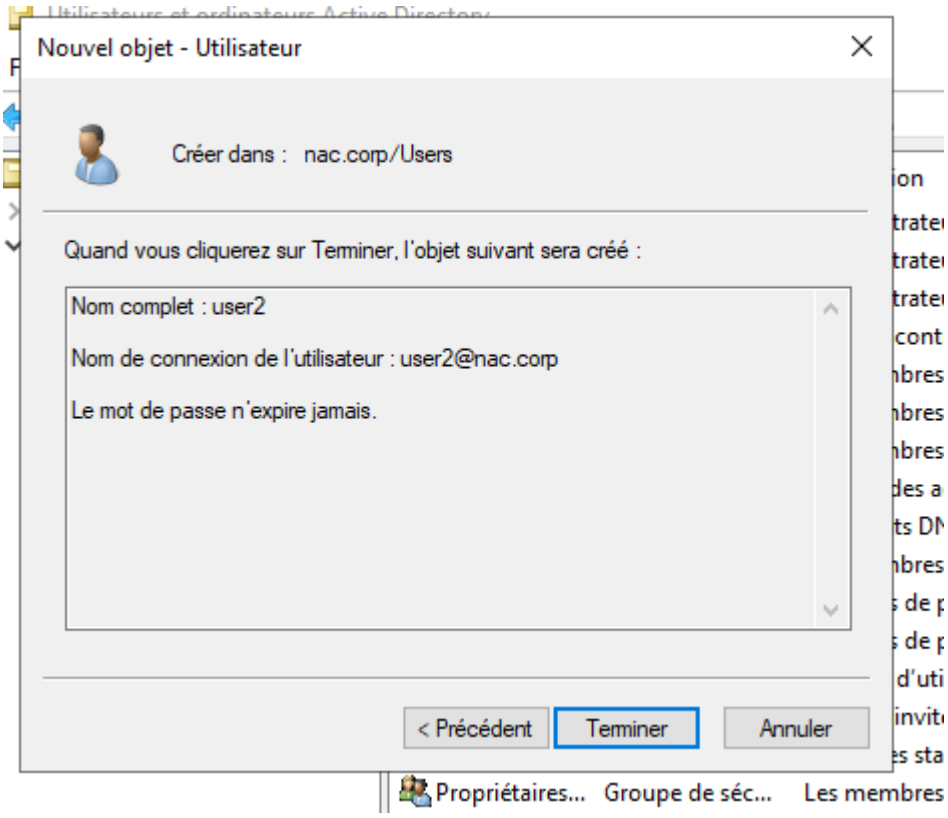


Figure 62: Création de l'utilisateur user2

Le second utilisateur **user2** est créé de la même manière.

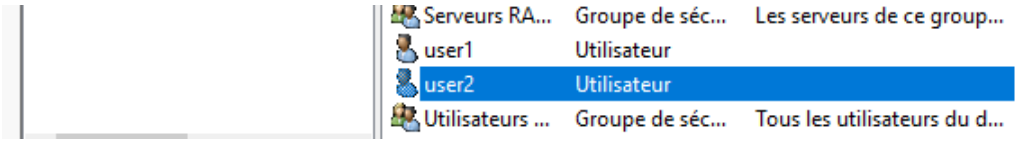


Figure 63:Console Active Directory

Les deux utilisateurs de test, user1 et user2, sont maintenant visibles dans la console Active Directory. Ils sont prêts à être utilisés pour les tests d'authentification. La prochaine étape consiste à ajouter user1 au groupe NAC_users conformément au cahier des charges.

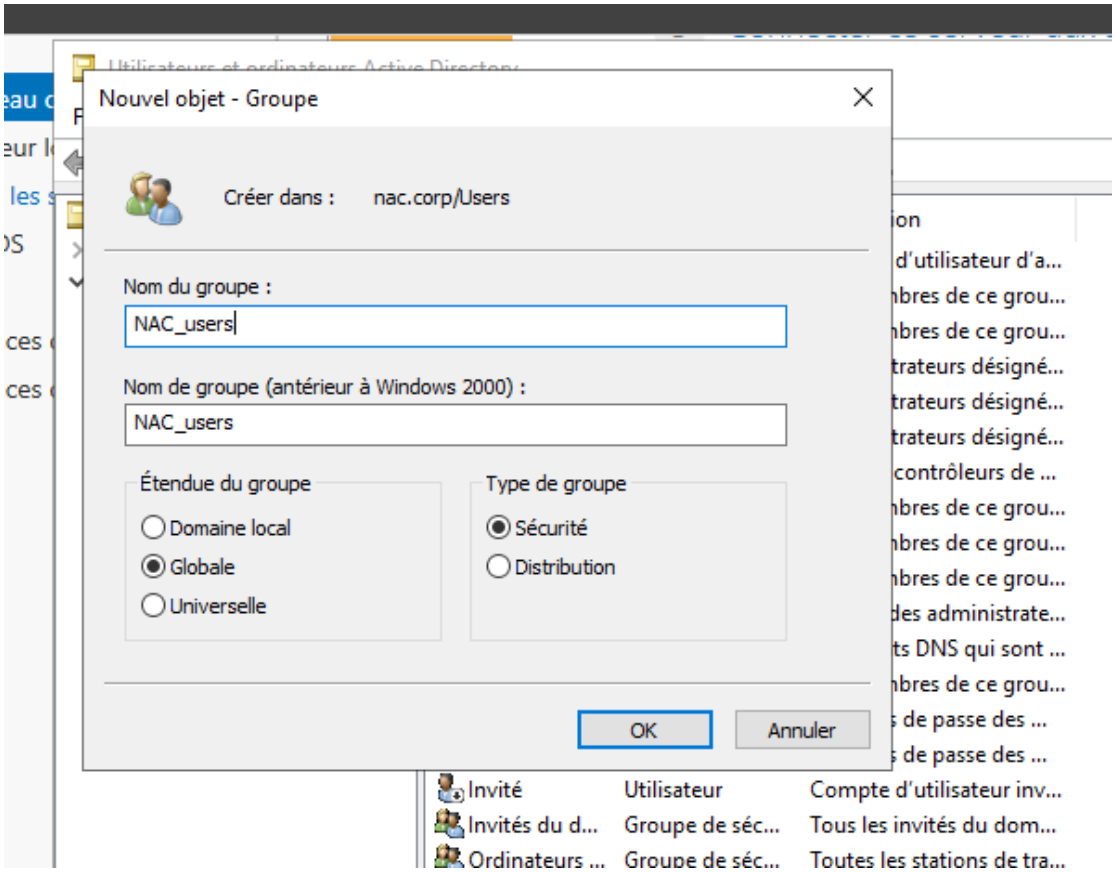


Figure 64: Assistant de création d'un nouveau groupe

Nous créons le groupe de sécurité NAC_users qui contiendra les utilisateurs autorisés à accéder au réseau via 802.1X. Les paramètres choisis sont :

- **Nom** : NAC_users
- **Étendue** : Globale (permet d'utiliser le groupe dans le domaine et les forêts)
- **Type** : Sécurité (pour attribuer des permissions)

11.4 AJOUT DE USER1 AU GROUPE NAC_USERS

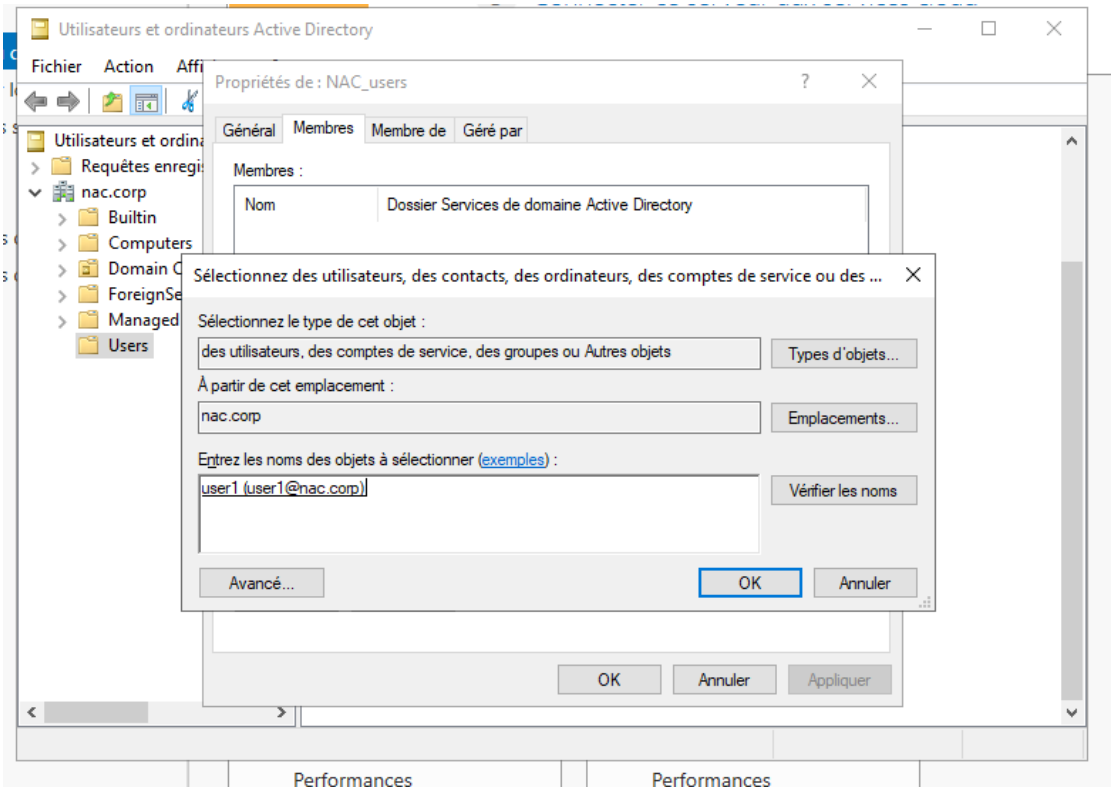


Figure 65:Ajout de user1 dans le groupe NAC_users

Dans les propriétés de user1, nous ajoutons l'utilisateur au groupe NAC_users via l'onglet "Membre de". Conformément au cahier des charges, seul user1 est membre du groupe ; user2 ne l'est pas.

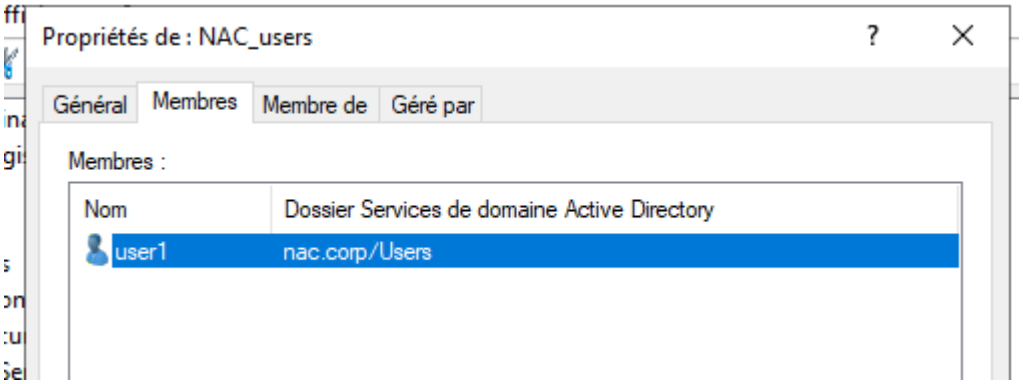


Figure 66: Confirmation de l'ajout de user1 au groupe NAC_users

La confirmation montre que user1 est maintenant membre du groupe NAC_users.

12. CONFIGURATION FINALE DU NPS (RADIUS)

12.1 ENREGISTREMENT DU NPS DANS ACTIVE DIRECTORY

Figure 67: Enregistrement du NPS dans Active Directory

Dans la console NPS, nous enregistrons le serveur dans Active Directory pour lui permettre de lire les propriétés des utilisateurs et des groupes.

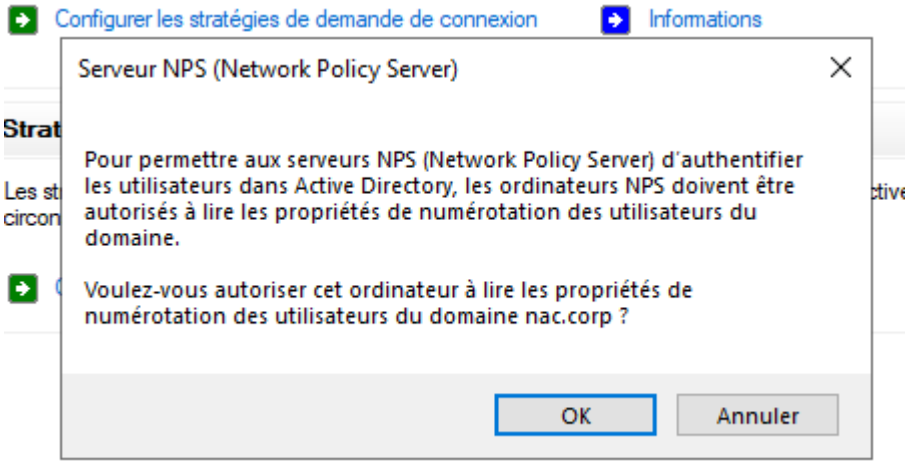


Figure 68:Confirmation de l'enregistrement du NPS

L'enregistrement est confirmé. Le NPS peut maintenant interroger Active Directory.

12.2 AJOUT DE PACKETFENCE COMME CLIENT RADIUS

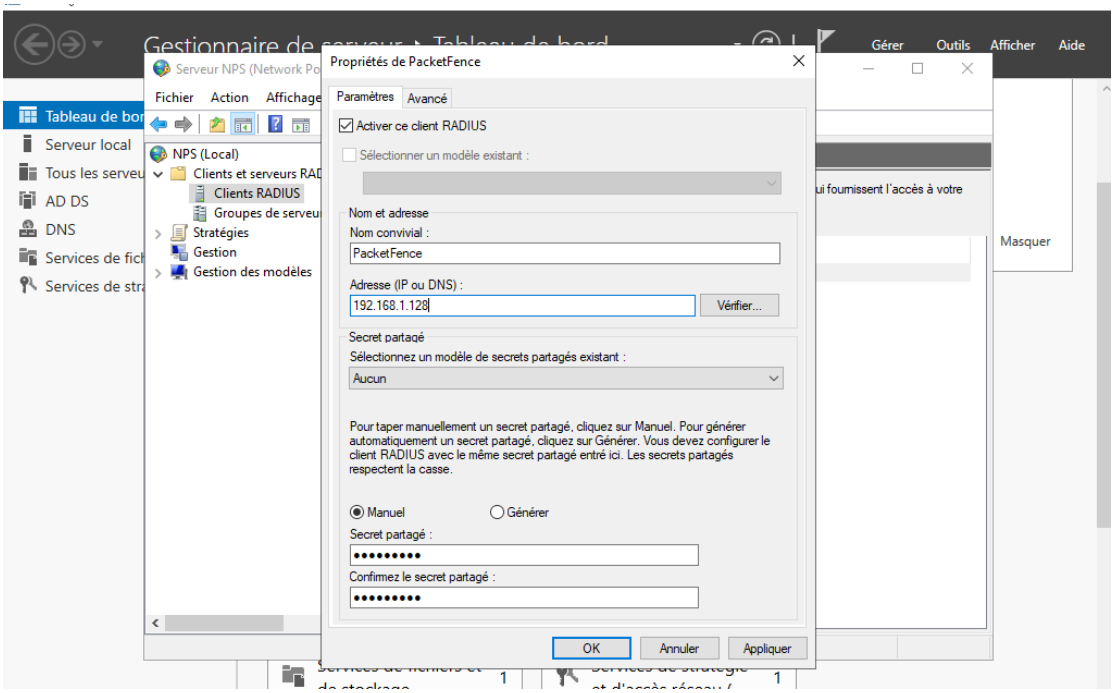


Figure 69:Ajout de PacketFence comme client RADIUS dans le NPS

Nous ajoutons un nouveau client RADIUS correspondant à PacketFence :

- **Nom** : PacketFence
- **Adresse IP** : 192.168.1.128
- **Secret partagé** : Un mot de passe partagé (à configurer identiquement dans PacketFence)

12.3 CREATION DE LA STRATEGIE RESEAU PEAP

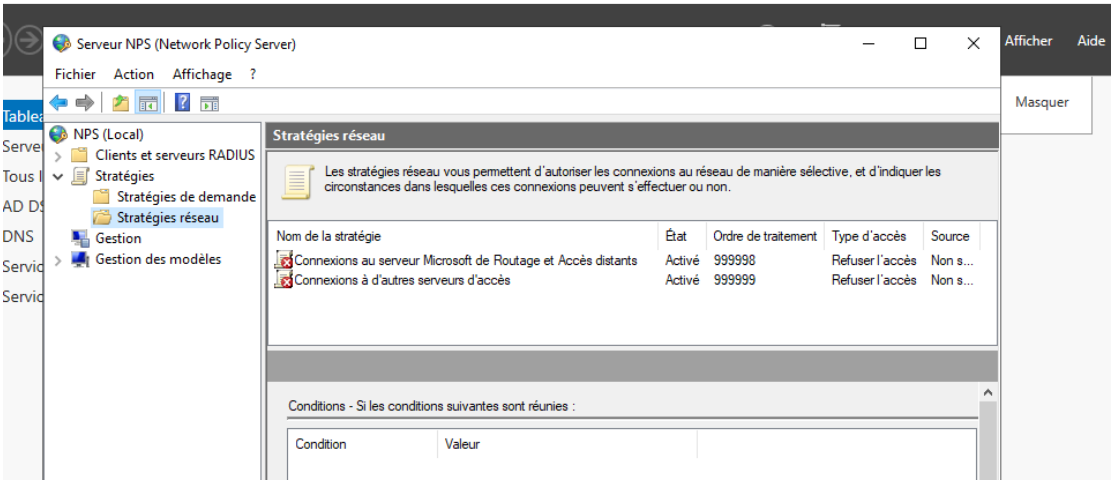


Figure 70:Création d'une nouvelle stratégie réseau pour PEAP

Nous créons une stratégie réseau qui définira les conditions d'autorisation pour les connexions 802.1X.

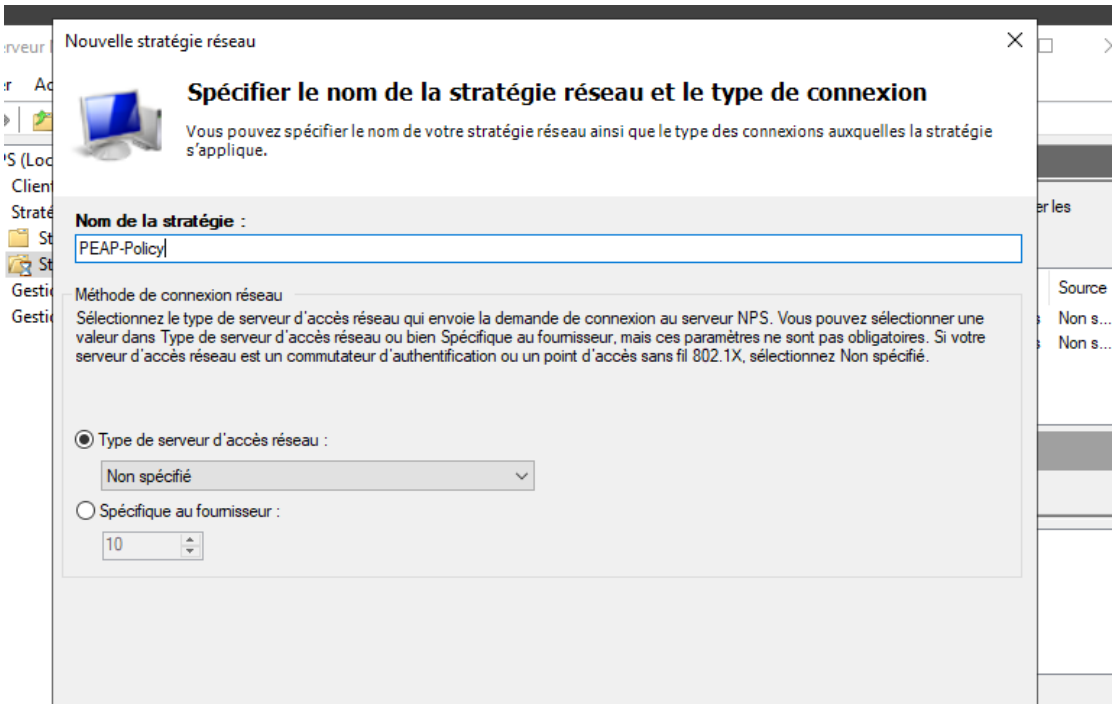


Figure 71: Assistant de création de stratégie réseau

L'assistant de création de stratégie réseau s'ouvre et nous nommons la stratégie " PEAP-Policy".

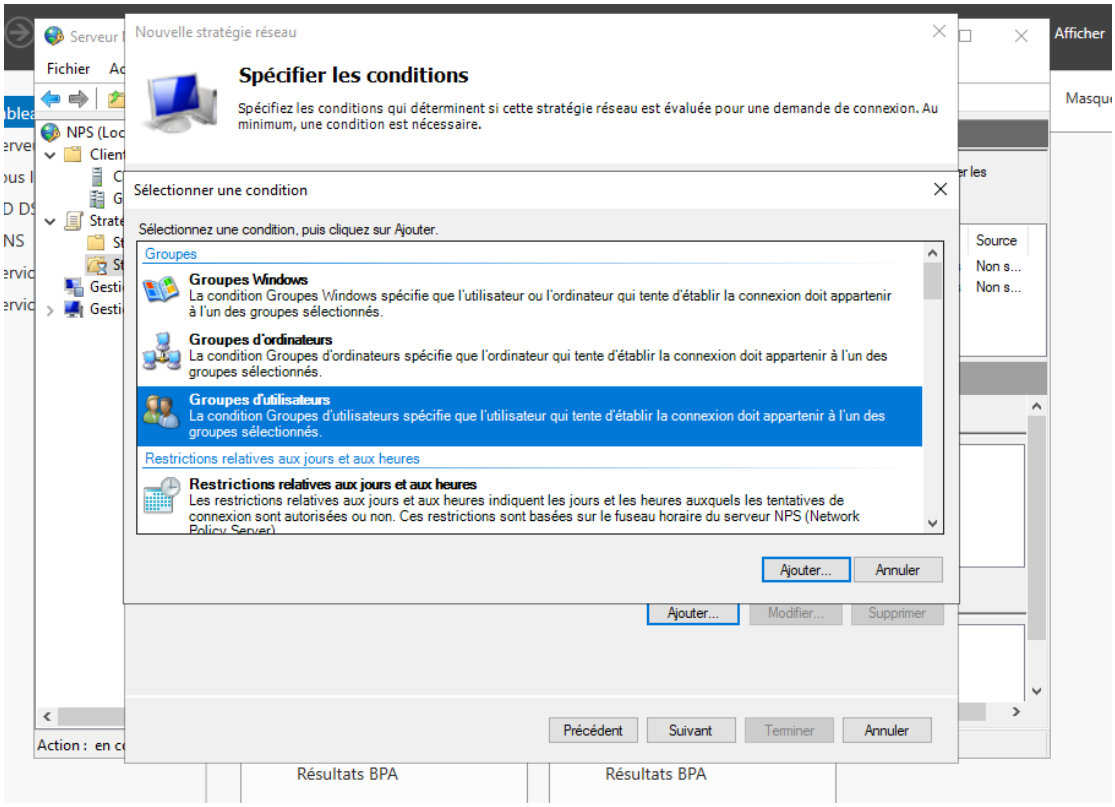


Figure 72:Configuration des conditions de la stratégie

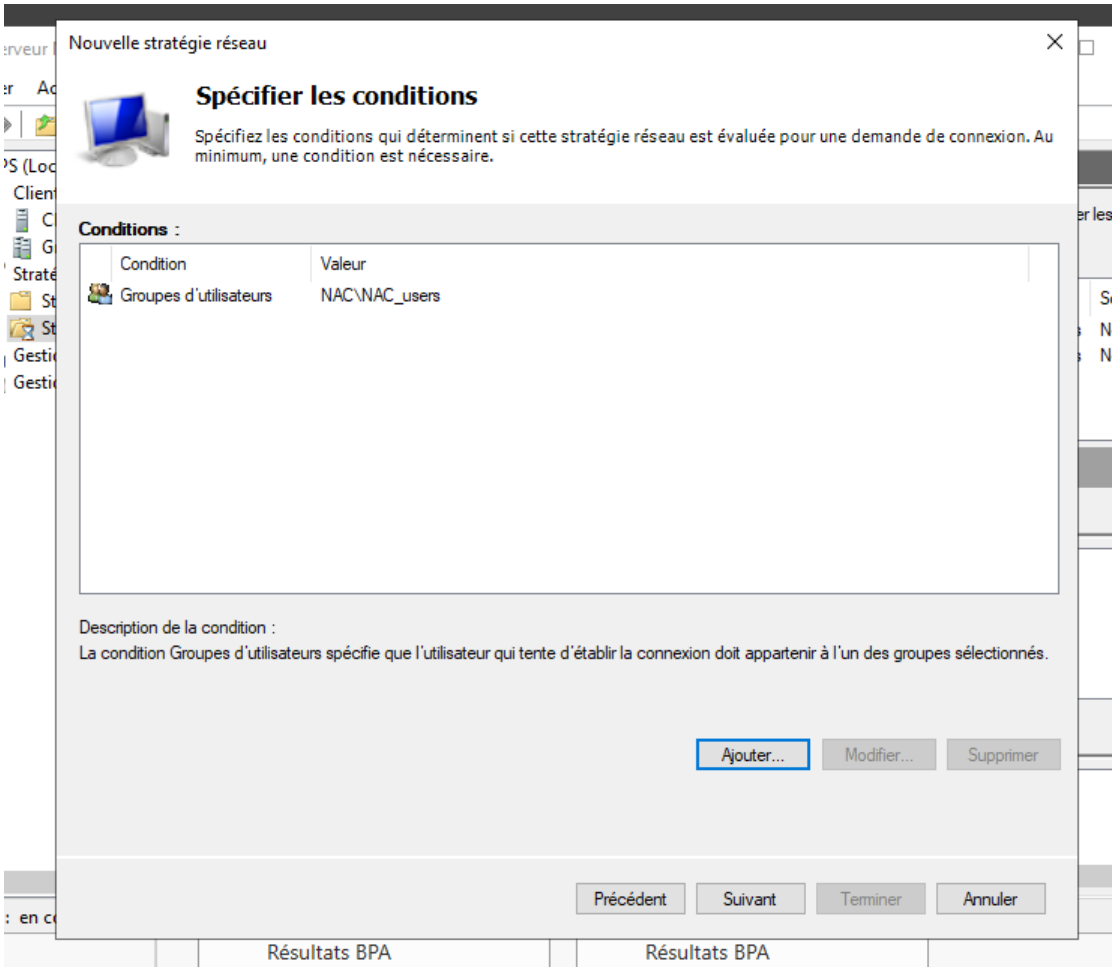


Figure 73: Configuration des conditions de la stratégie

Nous ajoutons une condition : l'utilisateur doit être membre du groupe **NAC_users**.

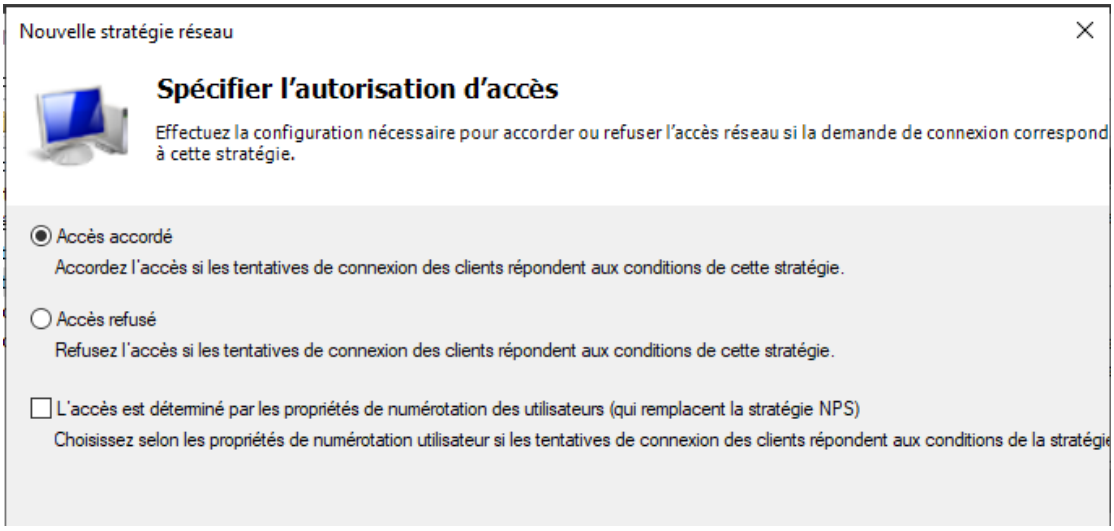


Figure 74:Définition des conditions d'accès

D'autres conditions peuvent être ajoutées (type de connexion, heure, etc.). Nous nous limitons au groupe pour ce projet.

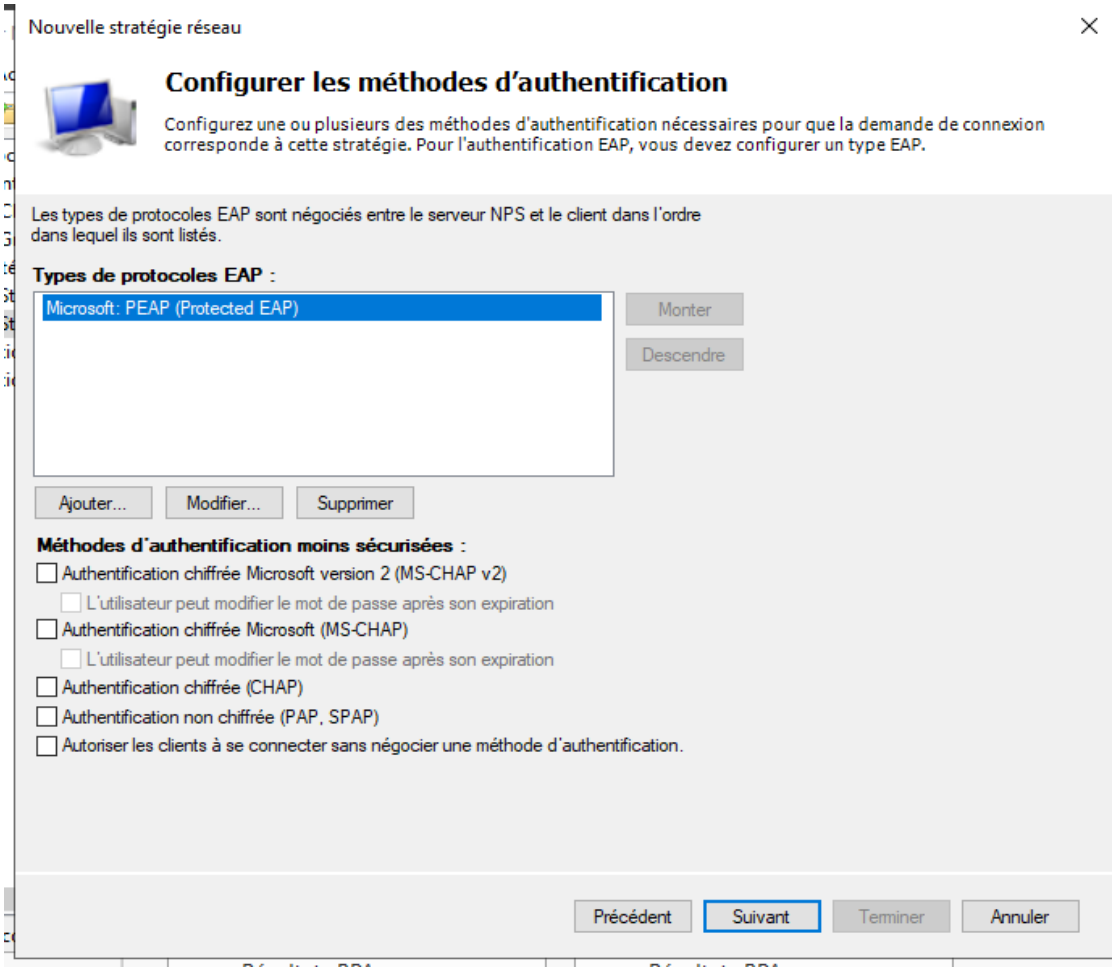


Figure 75:Configuration de l'authentification

Nous configurons les méthodes d'authentification : **PEAP** (Protected EAP) avec EAP-MS-CHAP v2 pour l'authentification par mot de passe.

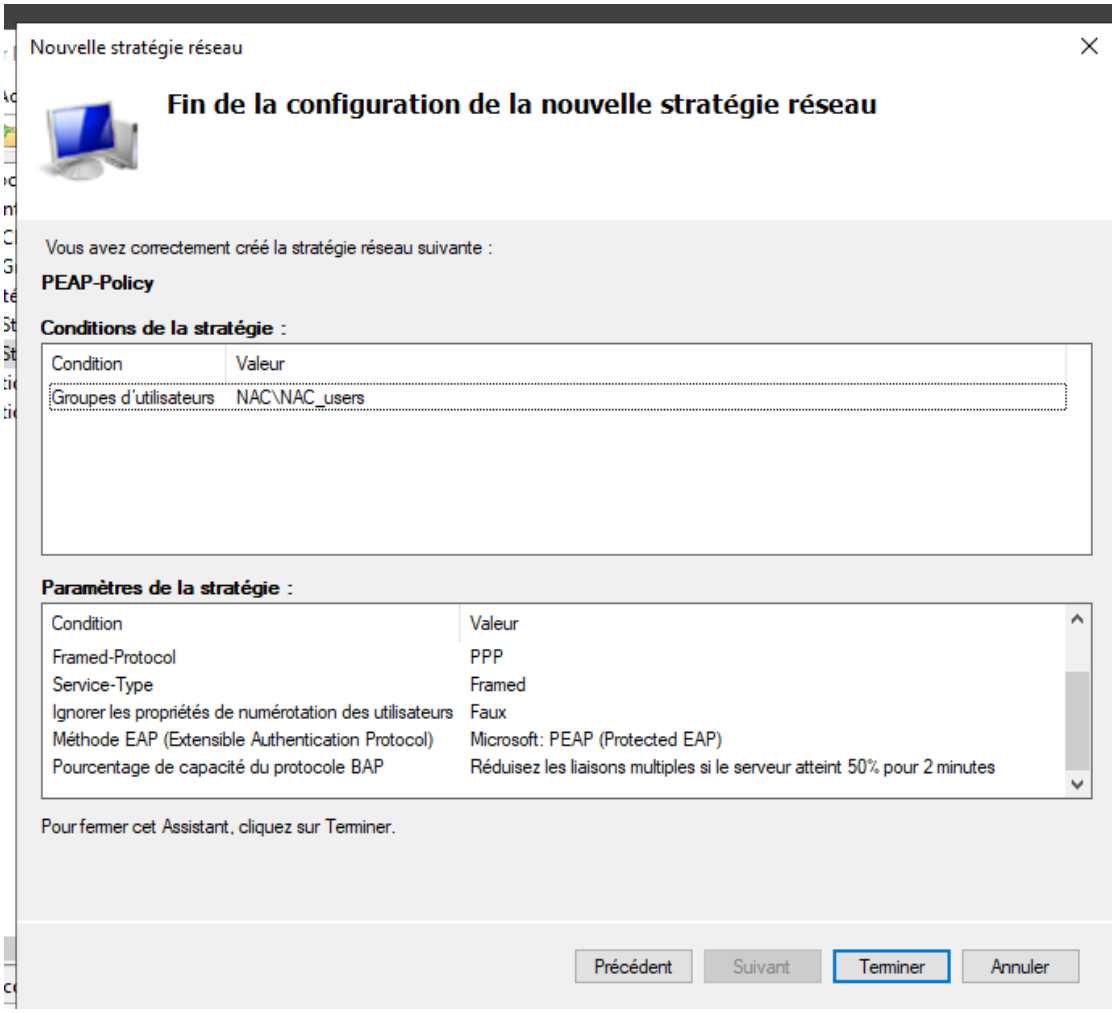


Figure 76:Finalisation de la stratégie réseau PEAP

L'assistant confirme la création de la stratégie, qui apparaît maintenant dans la liste des stratégies réseau.

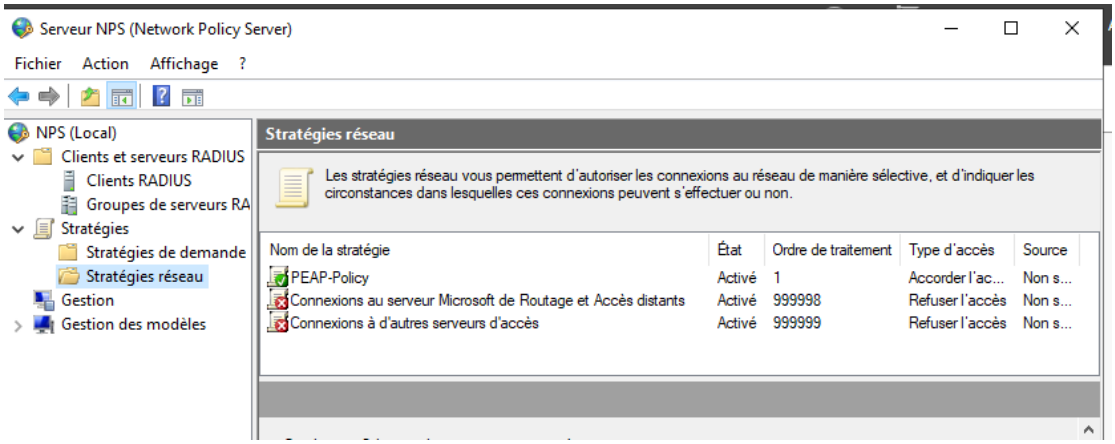


Figure 77:Console NPS (Network Policy Server)

La stratégie réseau "PEAP-Policy" apparaît maintenant dans la liste des stratégies avec :

- **État** : Activé
- **Ordre de traitement** : 1 (prioritaire)
- **Type d'accès** : Accorder l'accès

Les stratégies par défaut de refus sont conservées avec un ordre de traitement plus élevé (999998, 999999). Cela garantit que seule notre stratégie PEAP est appliquée pour les connexions 802.1X.

13. CONFIGURATION DU CLIENT WINDOWS ET TESTS D'AUTHENTIFICATION

13.1 CREATION DE LA MACHINE VIRTUELLE CLIENTE

Conformément aux spécifications du projet, nous créons une machine virtuelle Windows 10/11 qui jouera le rôle de poste utilisateur. Cette VM est connectée au même réseau interne (LAN) que le serveur PacketFence et le contrôleur de domaine Active Directory.

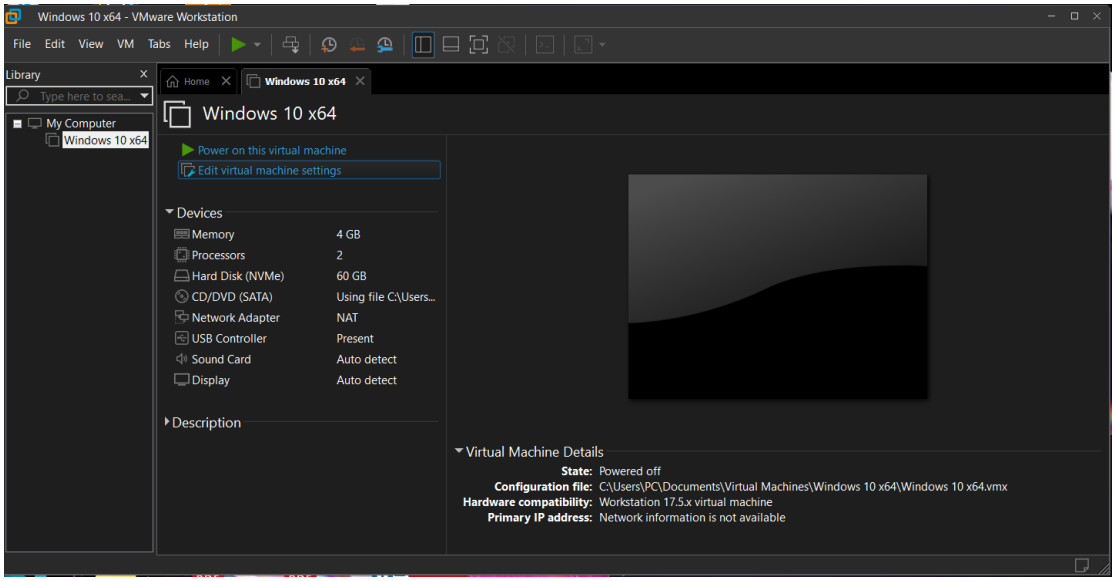


Figure 78:Création de la machine virtuelle Windows 10/11

13.2 ACTIVATION DU SERVICE D'AUTHENTIFICATION

Par défaut, Windows n'affiche pas les options d'authentification réseau pour les connexions Ethernet. Il est nécessaire d'activer manuellement le service **Service d'authentification** (EAPHost) pour rendre visible l'onglet Authentification dans les propriétés de la carte réseau.

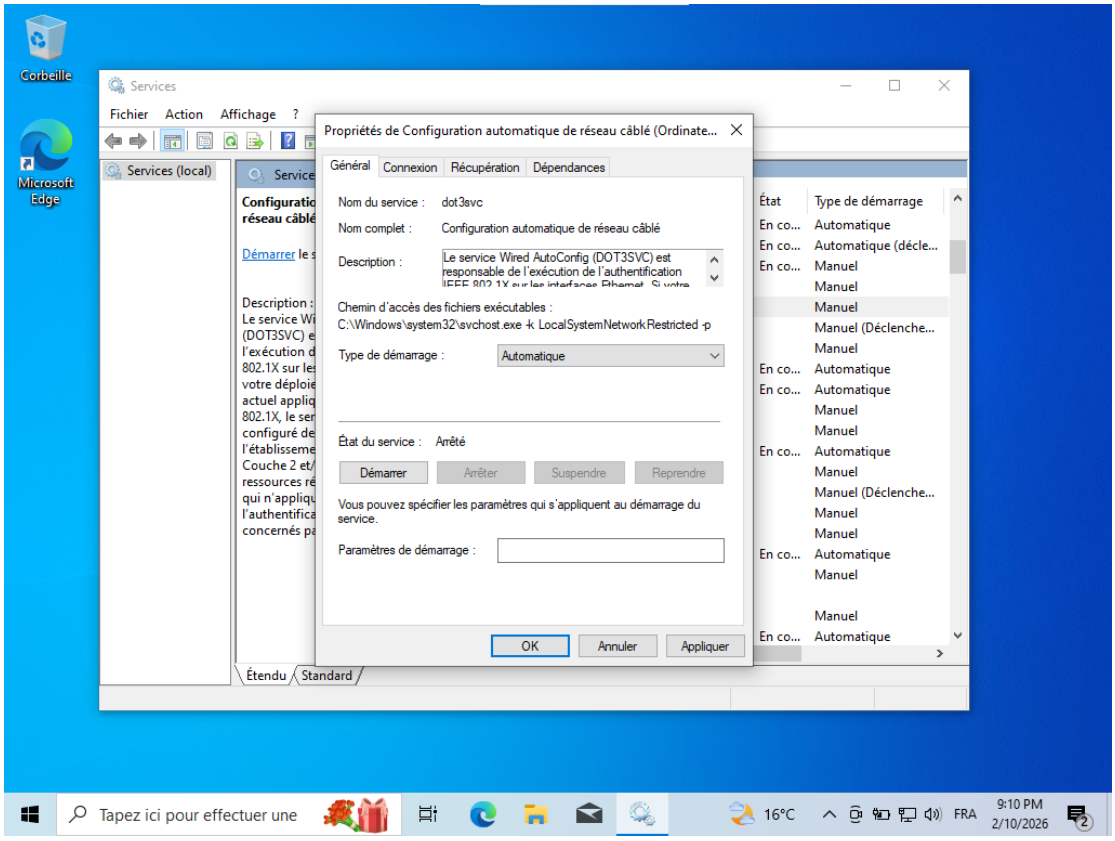


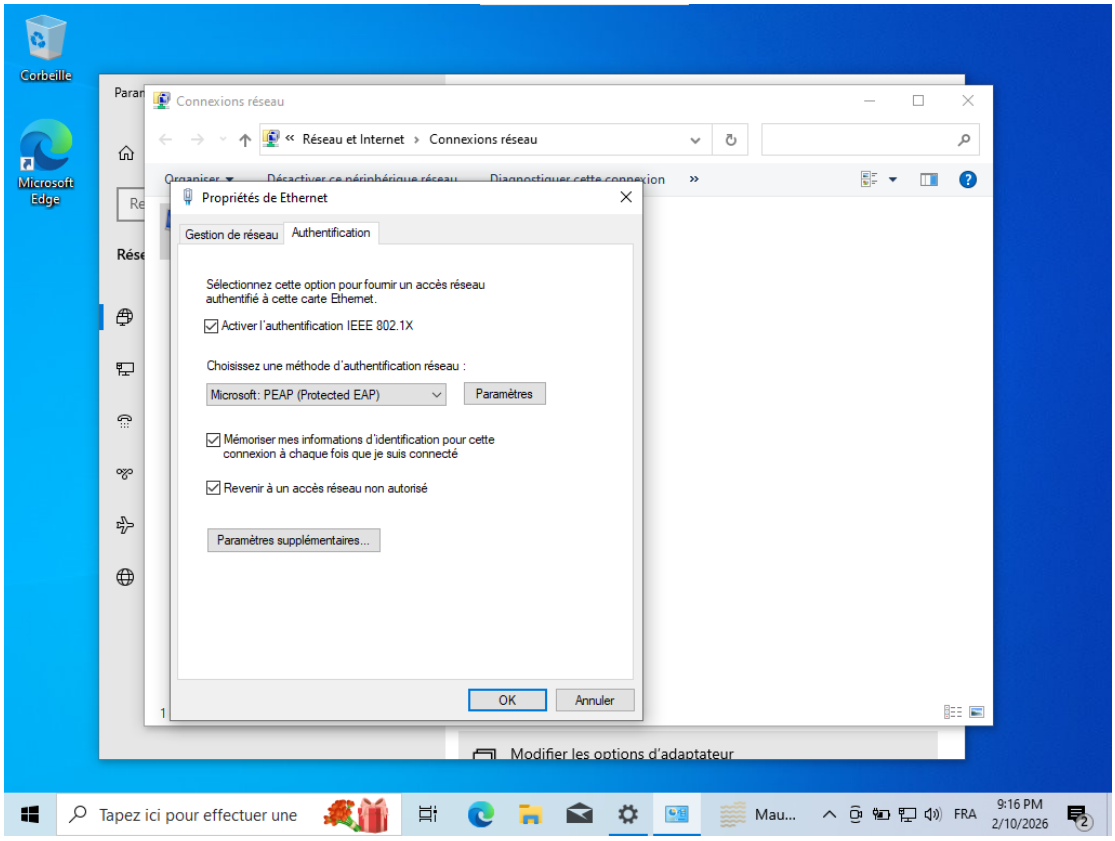
Figure 79:Démarrage du service et configuration en démarrage automatique

Procédure :

1. **Ouvrir le Gestionnaire de services (services.msc)**
2. **Rechercher le service Service d'authentification (EAPHost)**
3. **Démarrer le service et configurer son démarrage en automatique**

13.3 CONFIGURATION DU SUPPLICANT 802.1X

Une fois le service d'authentification activé, l'onglet **Authentification** apparaît dans les propriétés de la carte réseau. C'est ici que nous configurons le client (appelé "supplicant" dans la terminologie 802.1X) pour qu'il demande l'authentification au réseau.

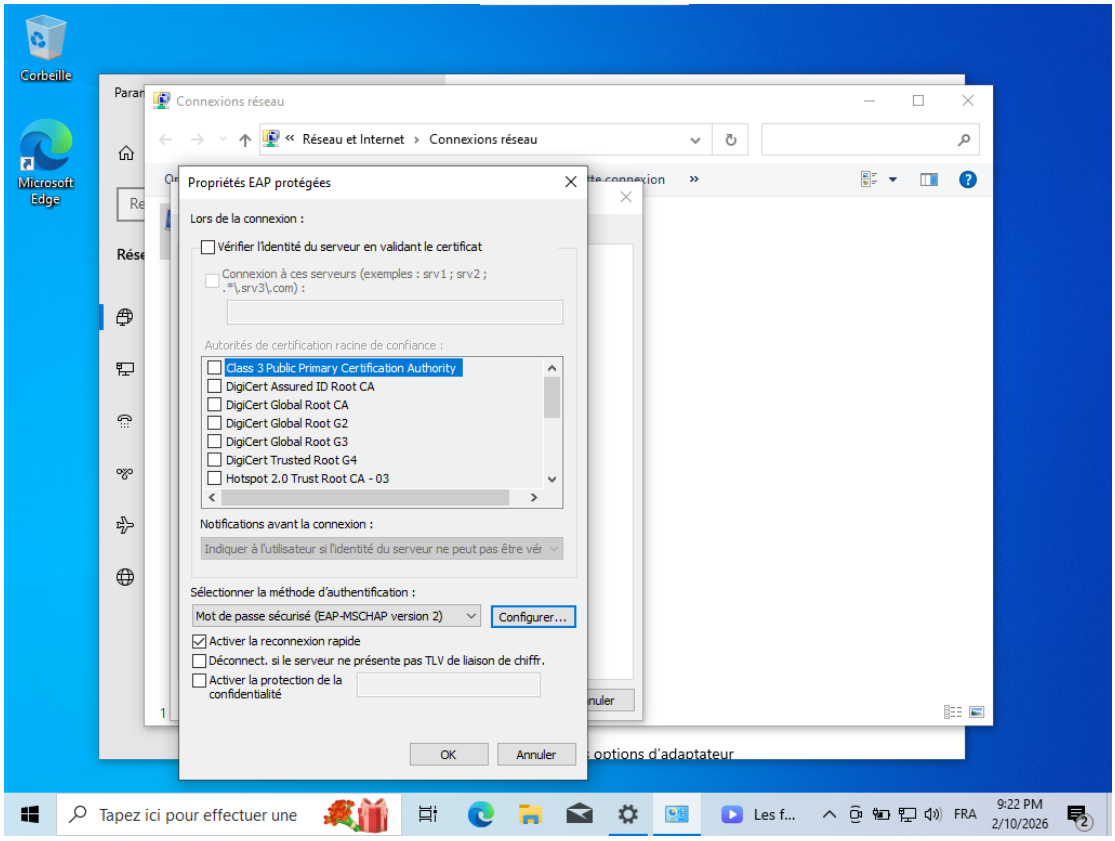


Paramètres configurés :

- **Activer l'authentification IEEE 802.1X**
- **Méthode d'authentification : Protected EAP (PEAP)**
- **Mode d'authentification : Authentification utilisateur**

13.4 CONFIGURATION AVANCEE DE PEAP

La méthode PEAP (Protected EAP) crée un tunnel TLS sécurisé entre le client et le serveur RADIUS avant de transmettre les identifiants. Nous configurons les paramètres avancés de PEAP :



Options configurées :

- Validation du certificat serveur : désactivée (en environnement de laboratoire)
- Sélection de la méthode d'authentification : **EAP-MSCHAP v2** (authentification par mot de passe)

13.5 TESTS D'AUTHENTIFICATION

Scénario 1 : Authentification avec user1 (utilisateur autorisé)

1. L'utilisateur **user1** (membre du groupe NAC_users) tente d'accéder au réseau
2. Windows affiche une invite de connexion demandant les identifiants
3. L'utilisateur saisit : user1@nac.local et son mot de passe
4. **Résultat** : Authentification réussie, accès réseau accordé

Scénario 2 : Authentification avec user2 (utilisateur non autorisé)

1. L'utilisateur **user2** (non membre du groupe NAC_users) tente d'accéder au réseau
2. Windows affiche une invite de connexion demandant les identifiants
3. L'utilisateur saisit : user2@nac.local et son mot de passe

4. **Résultat** : Authentification refusée, accès réseau bloqué

14. TESTS DE VALIDATION

13.1 TESTS DE CONNECTIVITE

```
C:\Users\Administrateur.WIN-B4AFD13LCUQ>ping 192.168.1.128

Envoi d'une requête 'Ping'  192.168.1.128 avec 32 octets de données :
Réponse de 192.168.1.128 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.128 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.1.128:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Administrateur.WIN-B4AFD13LCUQ>
```

Figure 80:Test de ping entre PacketFence et le serveur AD

Avant de tester l'authentification, nous vérifions la connectivité réseau de base. La commande ping 192.168.1.2 depuis PacketFence (ou inversement) doit réussir.

```
root@packetfence:~# ping -c5 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=1.19 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=1.38 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=1.25 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.753 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=128 time=0.990 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.753/1.113/1.382/0.220 ms
root@packetfence:~#
```

Figure 81:Test de ping entre le client et le serveur AD

Lors du premier démarrage de PacketFence ZEN, des messages d'erreur relatifs au service SSH et à la génération des certificats SSL ont été observés. Ce comportement est connu et n'empêche pas le fonctionnement du serveur NAC. Les services PacketFence et RADIUS ont démarré correctement et l'interface web est accessible.

14. CONCLUSION

14.1 SYNTHESE DES TRAVAUX

1. **Installation et configuration de PacketFence ZEN** avec deux interfaces réseau (LAN et Management) et paramétrage via l'assistant.
2. **Configuration de l'intégration LDAP** entre PacketFence et l'Active Directory.
3. **Mise en place d'un serveur Windows Server 2019** avec les rôles AD DS, DNS et NPS.
4. **Création du domaine** nac.local et configuration DNS (zones directes, zones inversées, enregistrements PTR et CNAME).
5. **Création des utilisateurs de test** (user1 et user2) et du groupe de sécurité NAC_users.
6. **Configuration du NPS** comme serveur RADIUS, avec PacketFence comme client et une stratégie réseau basée sur l'appartenance au groupe.
7. **Tests d'authentification** validant le comportement attendu :
    - user1 (membre du groupe) → Accès autorisé
    - user2 (non membre) → Accès refusé

14.2 DIFFICULTES RENCONTREES

Difficulté	Cause	Solution
Instabilité sous VirtualBox	Incompatibilité de virtualisation	Migration vers VMware Workstation
Service PacketFence inactif	Configuration initiale non finalisée	Lancement de l'assistant de configuration
Conflits de résolution de noms	IPv6 activé	Désactivation d'IPv6
Échec de la connexion LDAP	Base DN incorrecte	Correction en "DC=rac,DC=corp"

14.3 PERSPECTIVES D'AMELIORATION

Ce projet pourrait être enrichi par les évolutions suivantes :

1. **Mise en place de certificats** pour sécuriser les échanges (PEAP avec certificat serveur, EAP-TLS).
2. **Intégration de la conformité des postes** (vérification antivirus, pare-feu, mises à jour).
3. **Gestion des invités** avec portail captif et comptes temporaires.
4. **Segmentation VLAN dynamique** : Attribution de VLAN différents selon le rôle de l'utilisateur.
5. **Haute disponibilité** : Mise en place d'un second serveur PacketFence en cluster.
6. **Surveillance et alerting** : Configuration d'un système de supervision (Nagios, Zabbix) pour surveiller les services NAC.

15. BIBLIOGRAPHIE

1. **PacketFence Documentation officielle**
   https://www.packetfence.org/documentation.html

2. **IEEE 802.1X Standard**
   https://standards.ieee.org/standard/802_1X-2020.html

3. **Microsoft Docs - Network Policy Server**
   https://docs.microsoft.com/fr-fr/windows-server/networking/technologies/nps/nps-top

4. **Microsoft Docs - Active Directory Domain Services**
   https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/ad-ds-getting-started

5. **RADIUS Protocol (RFC 2865, 2866)**
   https://tools.ietf.org/html/rfc2865

6. **EAP Protocol (RFC 3748)**
   https://tools.ietf.org/html/rfc3748

7. **Inverse Inc. - PacketFence ZEN**
   https://www.packetfence.org/download.html#/zen

16. ANNEXES

16.1 GLOSSAIRE

Terme	Définition
NAC	Network Access Control - Contrôle d'accès au réseau
802.1X	Protocole standard IEEE pour l'authentification réseau
RADIUS	Remote Authentication Dial-In User Service - Protocole AAA
AD	Active Directory - Service d'annuaire Microsoft
AD DS	Active Directory Domain Services - Service de domaine
NPS	Network Policy Server - Serveur de stratégie réseau Microsoft
PEAP	Protected Extensible Authentication Protocol - Protocole d'authentification sécurisé
EAP	Extensible Authentication Protocol - Protocole d'authentification extensible
LDAP	Lightweight Directory Access Protocol - Protocole d'accès aux annuaires
DNS	Domain Name System - Système de résolution de noms
DHCP	Dynamic Host Configuration Protocol - Configuration automatique des adresses IP
PTR	Pointeur - Enregistrement DNS pour la résolution inverse