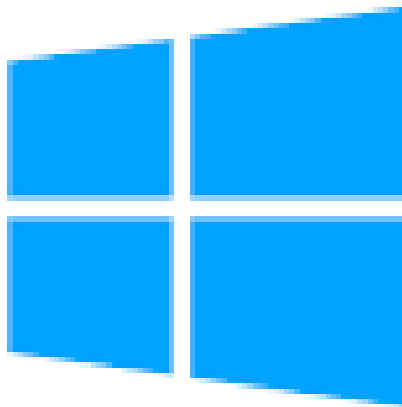


# **MISE EN PLACE D'UNE INFRASTRUCTURE ACTIVE DIRECTORY REDONDANTE**



Active Directory

## **SOMMAIRE :**

<b>I-</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>II-</b>	<b>ARCHITECTURE RESEAU DU PROJET .....</b>	<b>3</b>
<b>III-</b>	<b>DEPLOIEMENT DU CONTROLEUR DE DOMAINE PRINCIPAL (PDC) .....</b>	<b>4</b>
	<b>III.1- Installation des rôles .....</b>	<b>4</b>
	<b>III.2- Promotion du serveur en contrôleur de domaine.....</b>	<b>7</b>
<b>IV-</b>	<b>DEPLOIEMENT DU CONTROLEUR DE DOMAINE SECONDAIRE (BDC) .....</b>	<b>11</b>
	<b>IV.1- Préparation et Jonction .....</b>	<b>11</b>
	<b>IV.2- Réplication de la foret .....</b>	<b>13</b>
<b>V-</b>	<b>INTEGRATION DES POSTES CLIENTS WINDOWS AU DOMAINE .....</b>	<b>15</b>
	<b>V.1- Jonction au domaine.....</b>	<b>15</b>
	<b>V.2- Vérification de l'inventaire .....</b>	<b>16</b>
<b>VI-</b>	<b>Compétences validées .....</b>	<b>17</b>

**Franck Tchinkou**

**Version 1.0**

**Février 2026**

## I- INTRODUCTION

L'objectif de ce projet est de déployer le pilier central de l'identité numérique de l'entreprise.

En tant que futur Analyste SOC, je considère l'Active Directory non seulement comme un outils d'administration, mais comme une cible critique à sécuriser. La mise en place d'une redondance (Primary DC/Backup DC) est ici une réponse directe au besoin de continuité d'Activité (PCA).

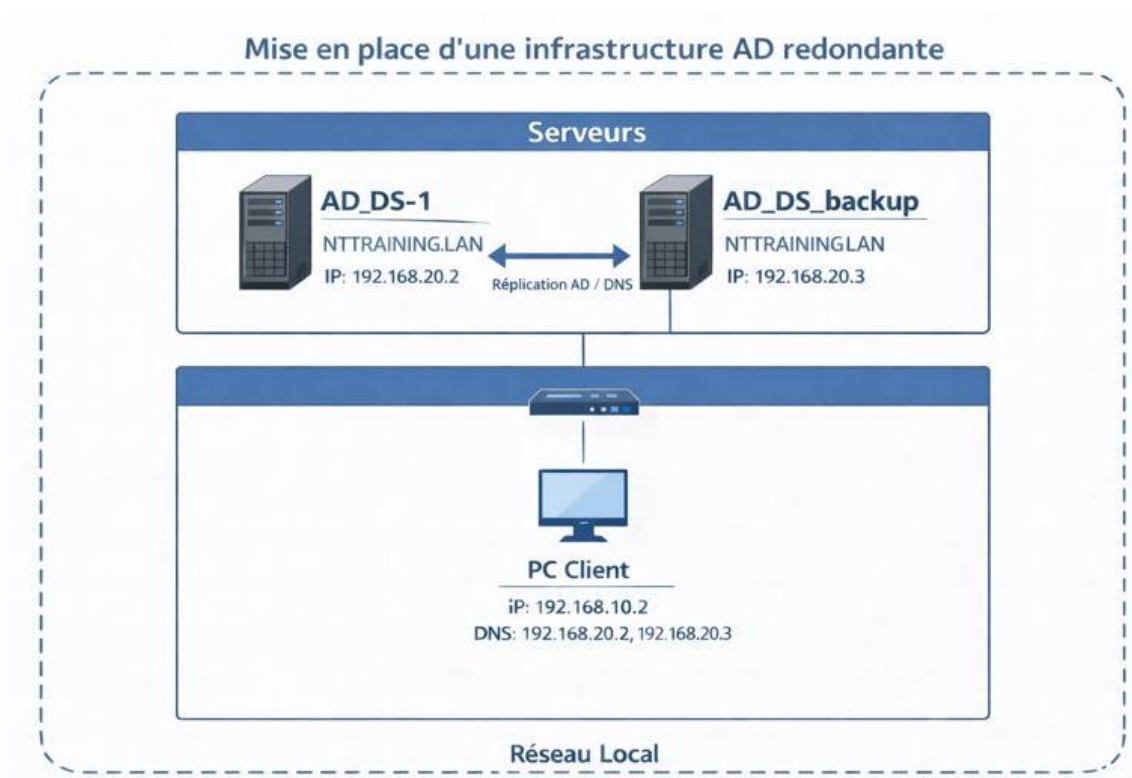
Objectifs Cibles :

- Centralisation de l'authentification et de la gestion des privilèges.
- Haute disponibilité des services d'annuaires et DNS.
- Sécurisation des accès au parc informatique.

## II- ARCHITECTURE RESEAU DU PROJET

Pour ce laboratoire, l'adressage est statique pour les serveurs afin de garantir la stabilité de la résolution DNS.

- Nom de domaine (FQDN) : NTTRAINING.LAN
- AD\_DS-1 (Principal) : 192.168.20.2
- AD\_DS\_backup (Secondaire): 192.168.20.3 / DNS: 192.168.20.2
- DESKTOP-01: 192.168.10.02 / DNS: 192.168.20.2 & 192.168.20.3

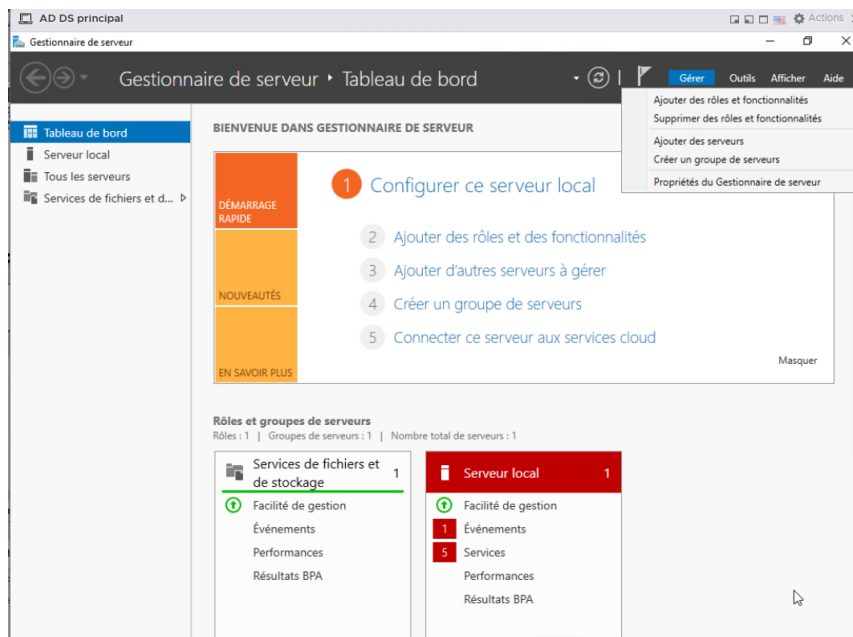


### III- DEPLOIEMENT DU CONTROLEUR DE DOMAINE PRINCIPAL (PDC)

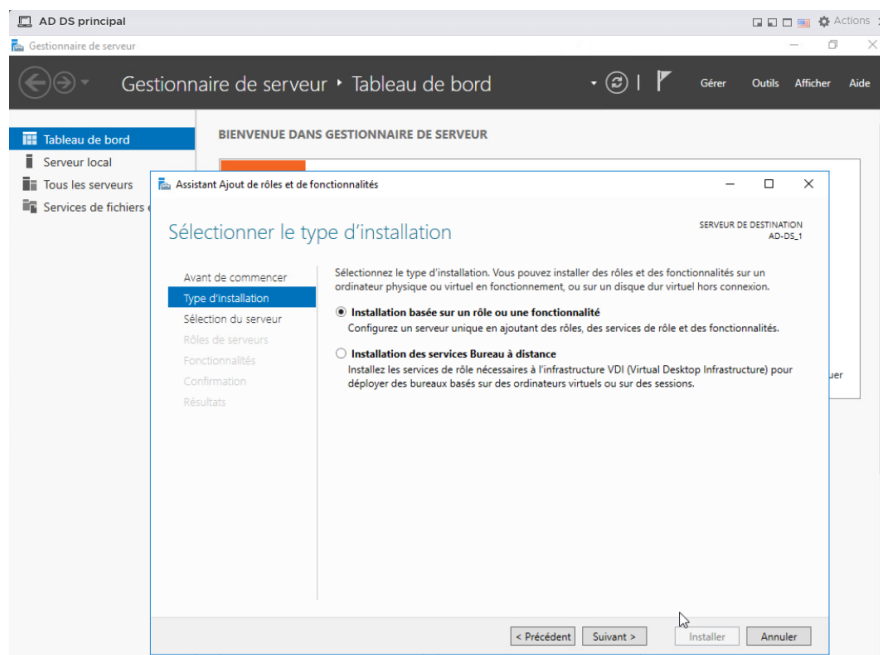
#### III.1- Installation des rôles

L'installation commence par l'ajout des rôles **AD DS (Active Directory Domain Services)** et **DNS** via le gestionnaire de Serveur.

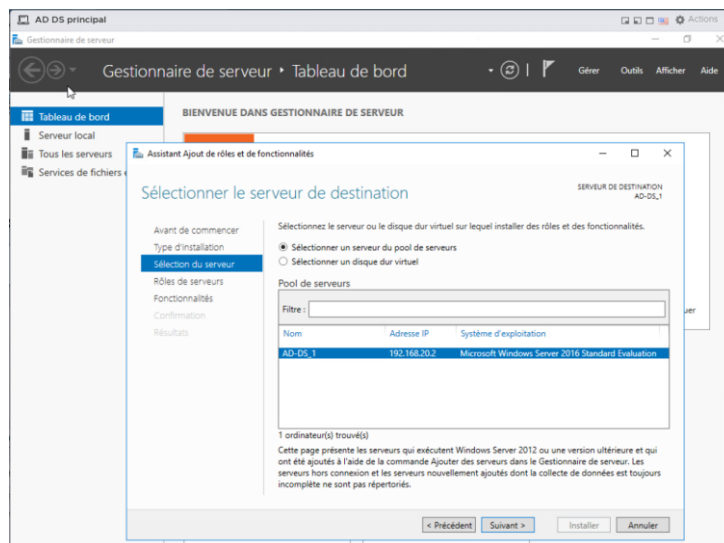
Une fois sur le **Gestionnaire de serveur** aller **Gérer** puis **Ajout des rôles et fonctionnalités**.



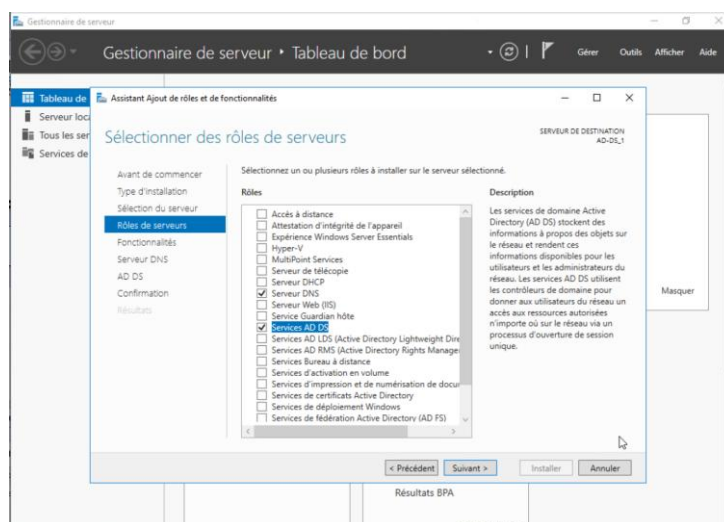
Puis choisir le type d'installation.



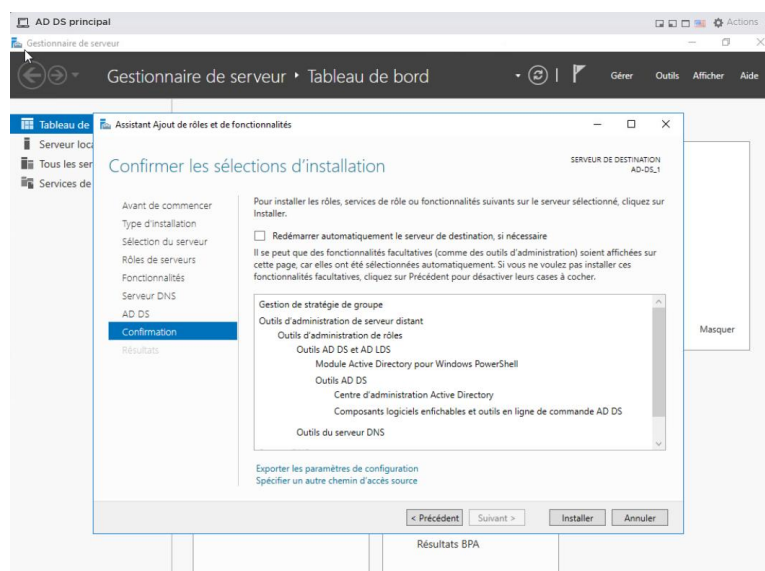
En suite sélectionner le serveur sur lequel l'installation sera faite.



Il faut maintenant choisir les rôles à installer.



Après cliquer sur « suivant » « suivant » jusqu'à installer.



**Rôle d'Active Directory Domain Services (AD DS) :** Active Directory Domain Services, abrégé AD DS est le service principal de gestion des identités et des ressources dans un environnement Windows. Il permet de centraliser l'administration du réseau et d'assurer la sécurité des accès. Grâce à AD DS, l'administrateur peut gérer l'ensemble des utilisateurs, des ordinateurs, des groupes et des ressources depuis un point unique.

AD DS est un annuaire informatique qui regroupe toutes les informations importantes du domaine. Ces données sont stockées dans une base appelée NTDS.dit, présente sur chaque contrôleur de domaine. Elle contient les comptes du réseau et les paramètres de sécurité, permettant ainsi aux machines du domaine de fonctionner correctement.

Lorsqu'un utilisateur se connecte à un poste de travail, AD DS intervient pour vérifier son identité. Le contrôleur de domaine compare les informations saisies avec celle stockées dans l'annuaire. Si elles sont correctes, l'accès est autorisé grâce au protocole kerberos, qui délivre un ticket d'authentification. Ce mécanisme garantit que seuls les utilisateurs autorisés peuvent accéder au réseau.

AD DS permet également de gérer les droits d'accès aux ressources. L'administrateur peut attribuer des permissions aux utilisateurs en utilisant des groupes. Par exemple, un groupe peut avoir accès à un dossier spécifique tandis qu'un autre en est exclu. Cette organisation facilite l'administration et renforce la sécurité.

Un autre rôle important d'AD DS est la gestion des stratégies de groupe, appelées GPO. Ces stratégies permettent d'imposer des règles sur les ordinateurs et utilisateurs du domaine, comme la complexité des mots de passe, le blocage de certains logiciels, la configuration du pare-feu ou encore l'installation automatique d'applications. Les GPO sont appliquées automatiquement lors du démarrage des ordinateurs ou à la connexion des utilisateurs.

### **Importance du rôle DNS pour un contrôleur de domaine**

Dans un environnement Active Directory, le service DNS est indispensable au bon fonctionnement du domaine. Active Directory repose entièrement sur le DNS pour localiser les serveurs et permettre aux clients de communiquer avec eux. Sans DNS correctement configuré, un domaine Windows ne peut pas fonctionner normalement.

Le DNS permet avant tout aux ordinateurs clients de trouver les contrôleurs de domaine. Lorsqu'un poste démarre ou lorsqu'un utilisateur tente de se connecter, l'ordinateur interroge le serveur DNS pour savoir où se trouve un contrôleur de domaine disponible. Cette recherche

se fait à l'aide d'enregistrements spécifiques appelés enregistrements SRV, qui indiquent les services fournis par chaque serveur. Grâce à ces informations, le client sait vers quel contrôleur se diriger.

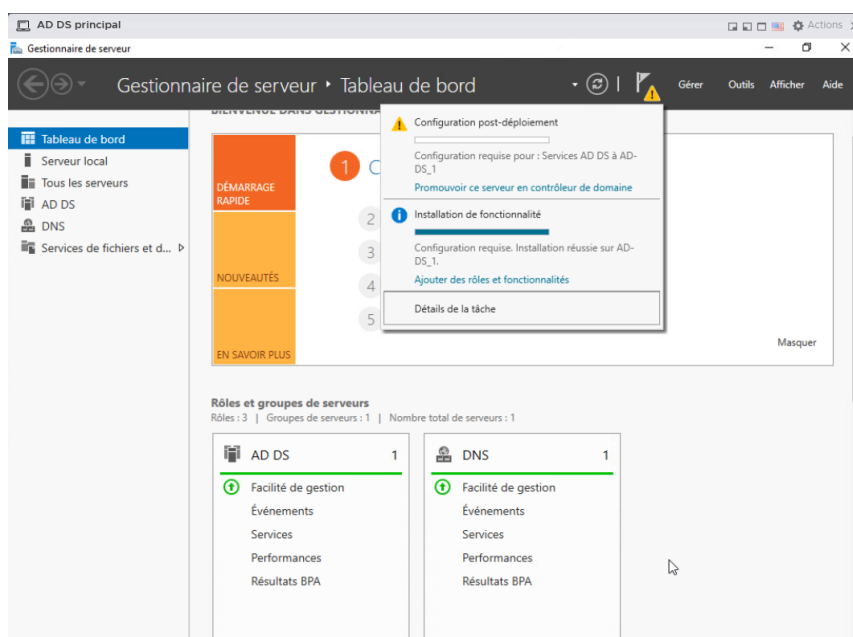
Le processus d'authentification dépend directement du DNS. Pour vérifier un mot de passe, utiliser Kerberos ou accéder aux services LDAP, le poste doit d'abord localiser un contrôleur de domaine. Si le DNS ne répond pas ou est mal configuré, l'ordinateur ne peut pas trouver le serveur AD, ce qui empêche la connexion de l'utilisateur. Cela peut provoquer des erreurs, des profils temporaires ou des échecs d'ouverture de session.

Le DNS est également utilisé pour accéder aux services internes du domaine, comme les partages de fichiers, les imprimantes réseau, les serveurs de messagerie ou les applications métier. Chaque service est identifié par un nom dans le DNS, ce qui permet aux utilisateurs de s'y connecter facilement sans connaître les adresses IP.

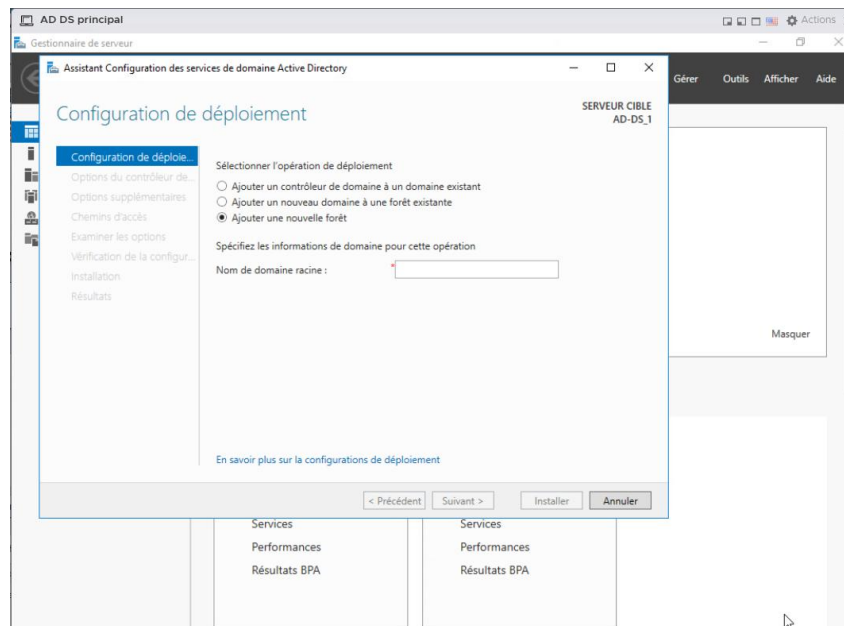
### III.2- Promotion du serveur en contrôleur de domaine

Une fois les rôles installés le serveur est promu au rang de contrôleur de domaine. Cette étape définit la racine de confiance de toute l'infrastructure.

Nous devons maintenant configurer le contrôleur de domaine. Nous allons cliquer sur le message d'erreur puis sur « promouvoir ce serveur en contrôleur de domaine ».

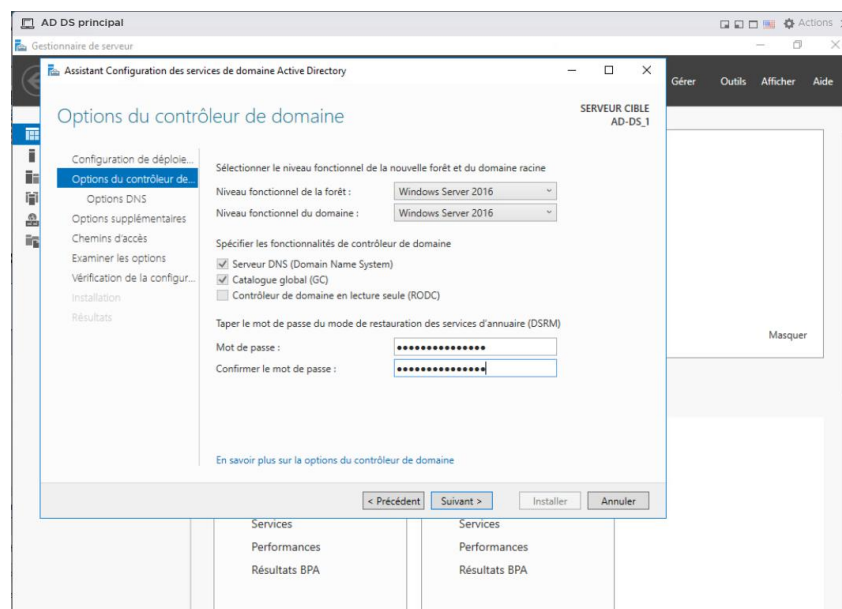


Nous allons sélectionner le type de déploiement et définir le nom de domaine racine  
«NTTRAINING.LAN »

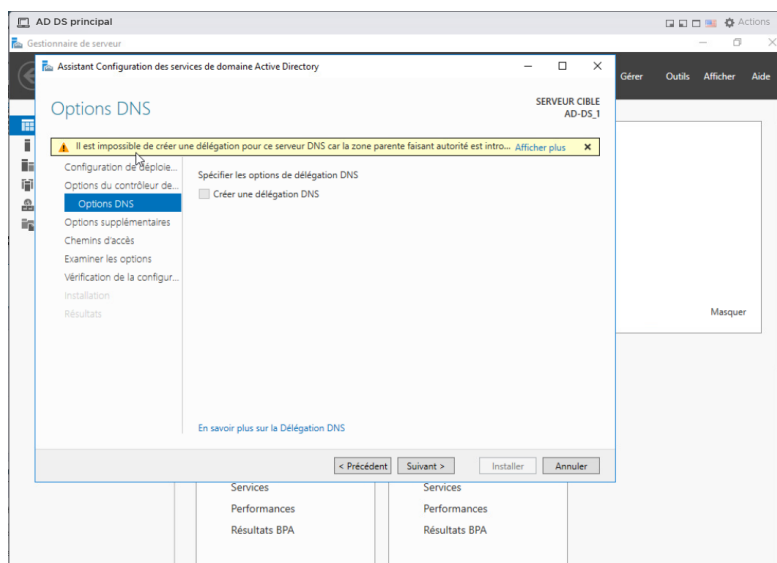


- Ajout un contrôleur de domaine a un domaine existant : A utiliser si on a déjà un domaine et qu'on veut ajouter un autre serveur pour la redondance.
- Ajouter un nouveau domaine a une foret existante : A utiliser si on a déjà une foret AD et qu'on veut créer un sous domaine.
- Ajouter une nouvelle foret : A utiliser si on veut créer un tout nouvel Active Directory à partir de zéro.

Ensuite nous allons définir le mot de passe DSRM utilise pour la restauration des services de l'annuaire généralement utilise si (AD est corrompu, La base AD est endommagé, on veut restaurer une sauvegarde...)



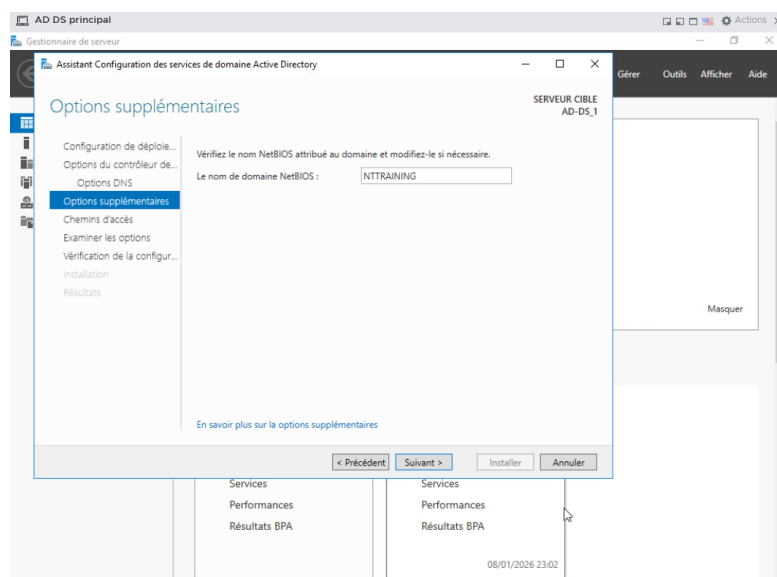
Nous allons poursuivre notre installation en choisissant « suivant ».



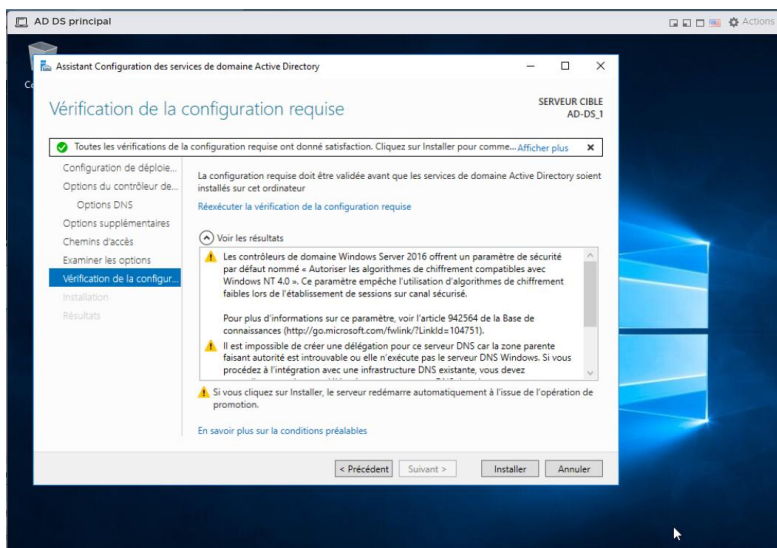
Dans notre cas on ne coche pas la case. Nous sommes en train de créer le premier contrôleur de domaine donc il n'existe aucun DNS parent au-dessus de notre domaine. Une délégation DNS sert lorsqu'on a déjà une infrastructure DNS et on ajoute un sous domaine.

Exemple : pour le domaine nttraining.lan on crée un entreprise.nttraining.lan (pour le domaine entreprise.nttraining.lan aller demander à nttraining.lan).

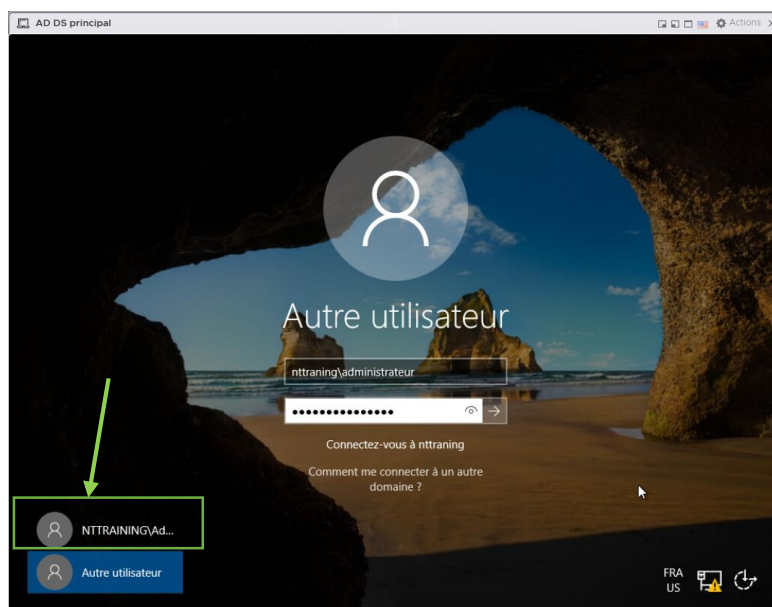
Le nom NetBios est défini automatiquement et est déduit du nom du domaine racine.



Ici on valide l'installation, après l'installation le serveur va redémarrer.



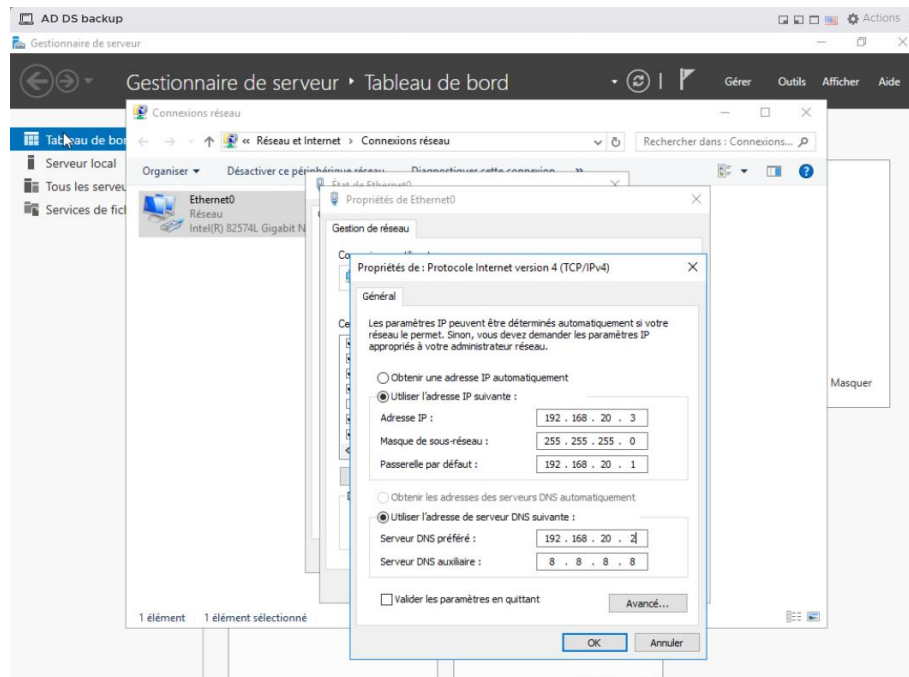
Notre contrôleur de domaine a été installé et configuré avec succès.



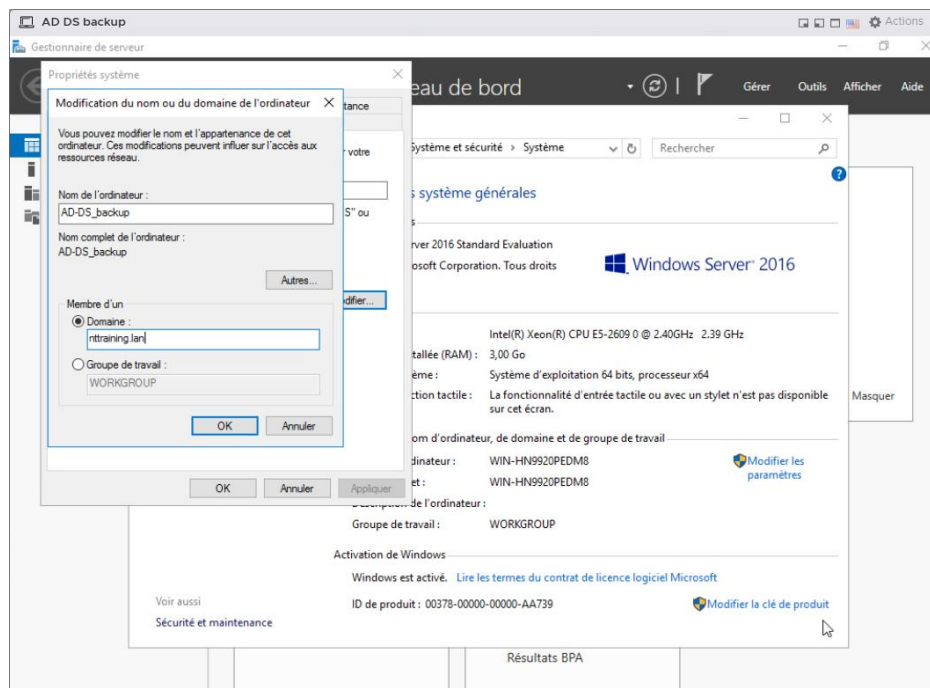
## IV- DEPLOIEMENT DU CONTROLEUR DE DOMAINE SECONDAIRE (BDC)

### IV.1- Préparation et Jonction

Avant sa promotion en contrôleur de domaine, le DC secondaire doit être capable de résoudre le nom de domaine du PDC. Son DNS primaire est configuré sur l'IP du PDC.

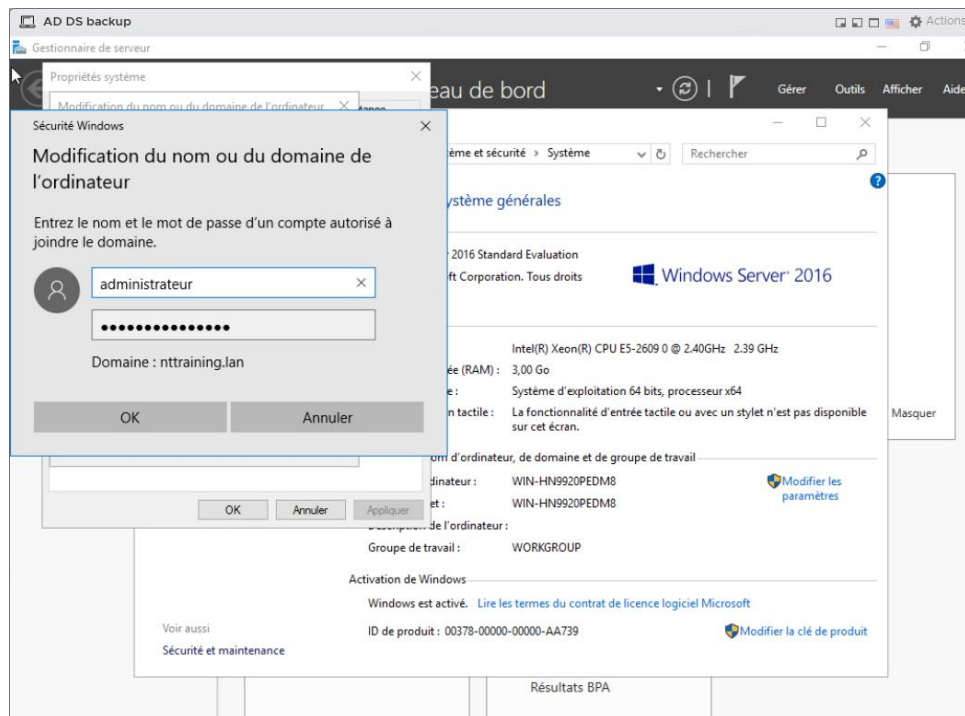


Après la configuration réseau nous devons joindre le DC secondaire au DC primaire.

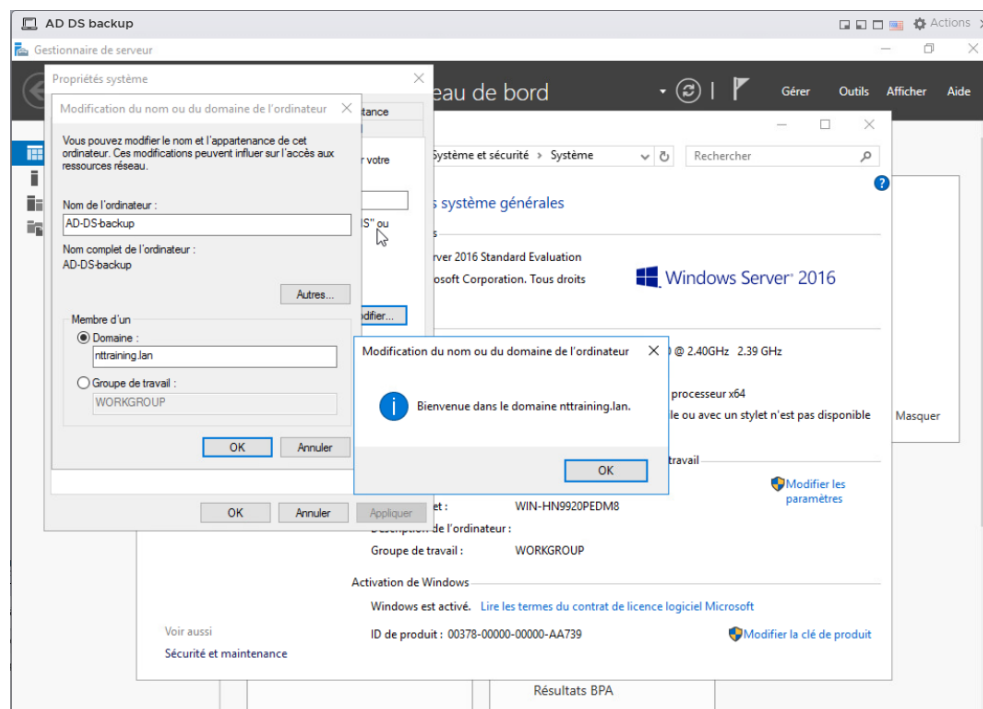


On entre le nom du domaine racine puis valider sur « ok ».

Si la configuration réseau est correcte, on va devoir entrer les informations de connexion du compte administrateur du domaine principale.

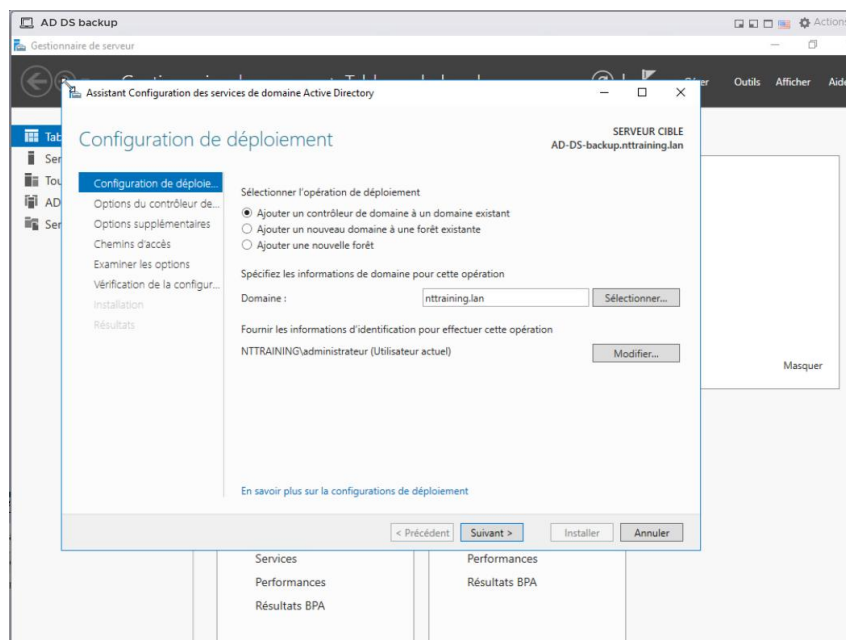


Nous venons de joindre notre DC secondaire au DC principale.

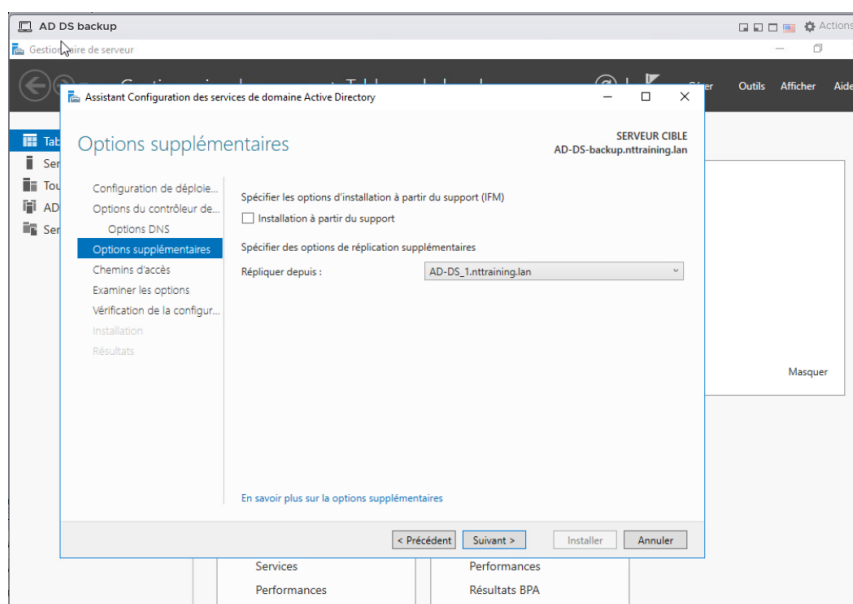


## IV.2- Réplication de la forêt

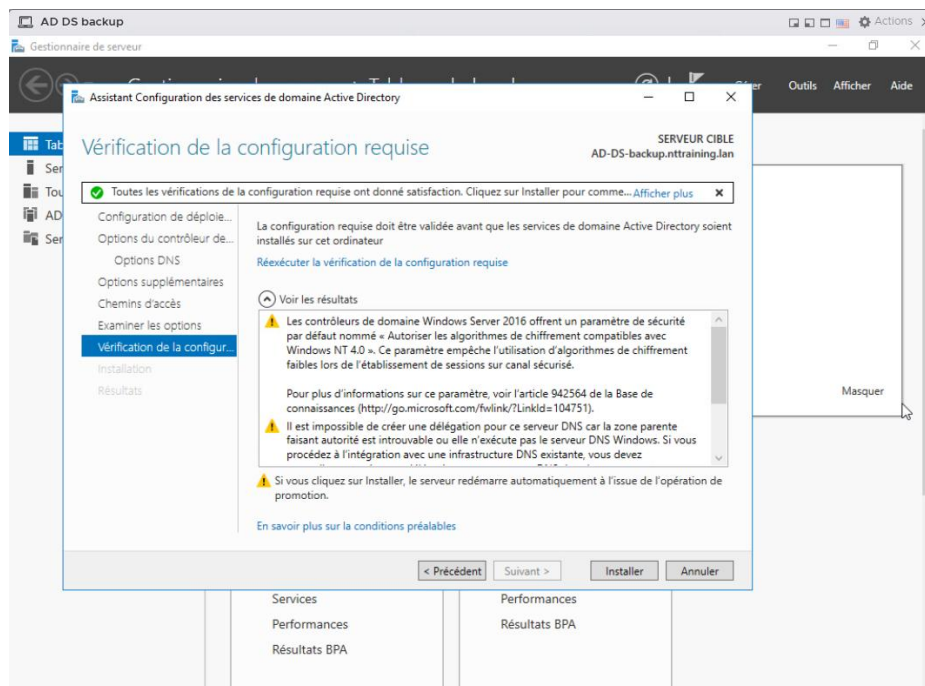
Une fois le rôle AD DS installé, le serveur est promu en contrôleur de domaine en choisissant l'option « Ajouter un contrôleur de domaine à un domaine existant ». Cela déclenche la réplication de la base de données NTDS et du dossier SYSVOL (ce répertoire contient des dossiers qui stockent les objets de stratégie de groupe et les scripts d'ouverture de session nécessaires aux clients pour accéder aux DC).



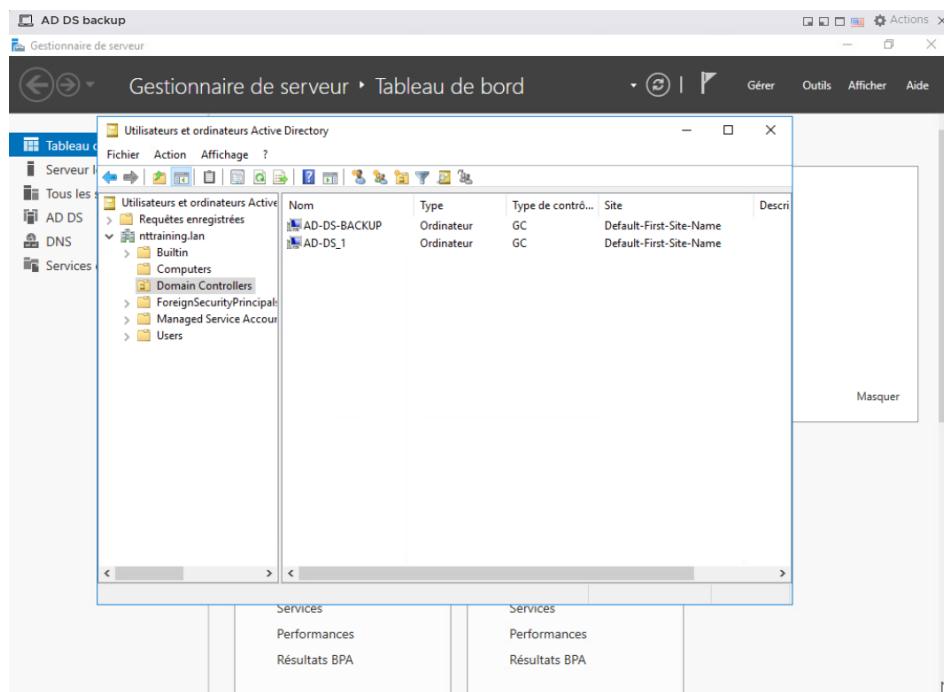
On choisit en suite le serveur depuis lequel on souhaite faire la réplication dans notre cas AD-DS\_1.



Puis on installe.



Notre contrôleur de domaine a bien été installé.

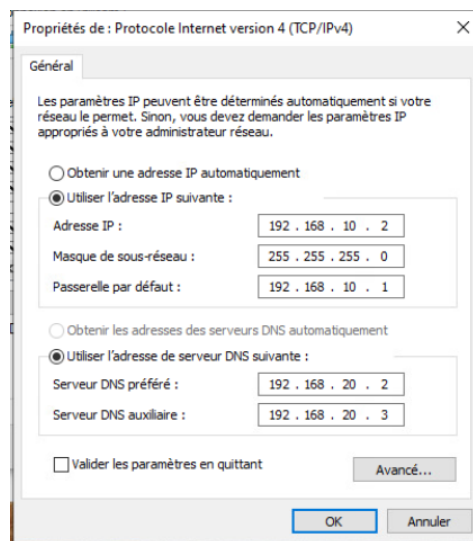


## V- INTEGRATION DES POSTES CLIENTS WINDOWS AU DOMAINE

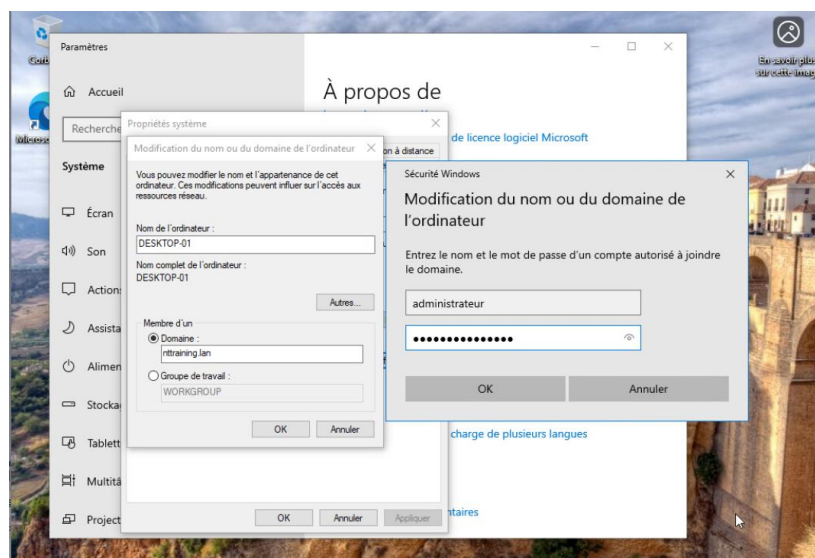
### V.1- Jonction au domaine

Le poste client Windows est configuré pour utiliser les deux DC comme serveurs DNS. La jonction s'effectue via les propriétés systèmes en saisissant les identifiants de l'administrateur du domaine.

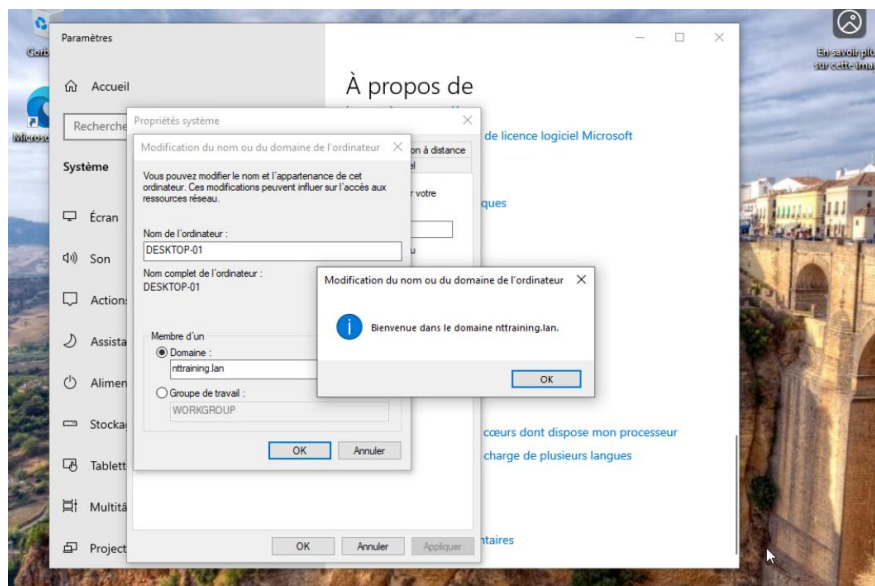
Une fois les paramètres réseau renseignés (Les DNS sont respectivement les IP du PDC et du BDC).



Nous ajoutons le pc dans le domaine en renseignant le domaine racine. Si la configuration réseau est correcte on nous demande d'entrer les identifiants du compte administrateur du domaine.

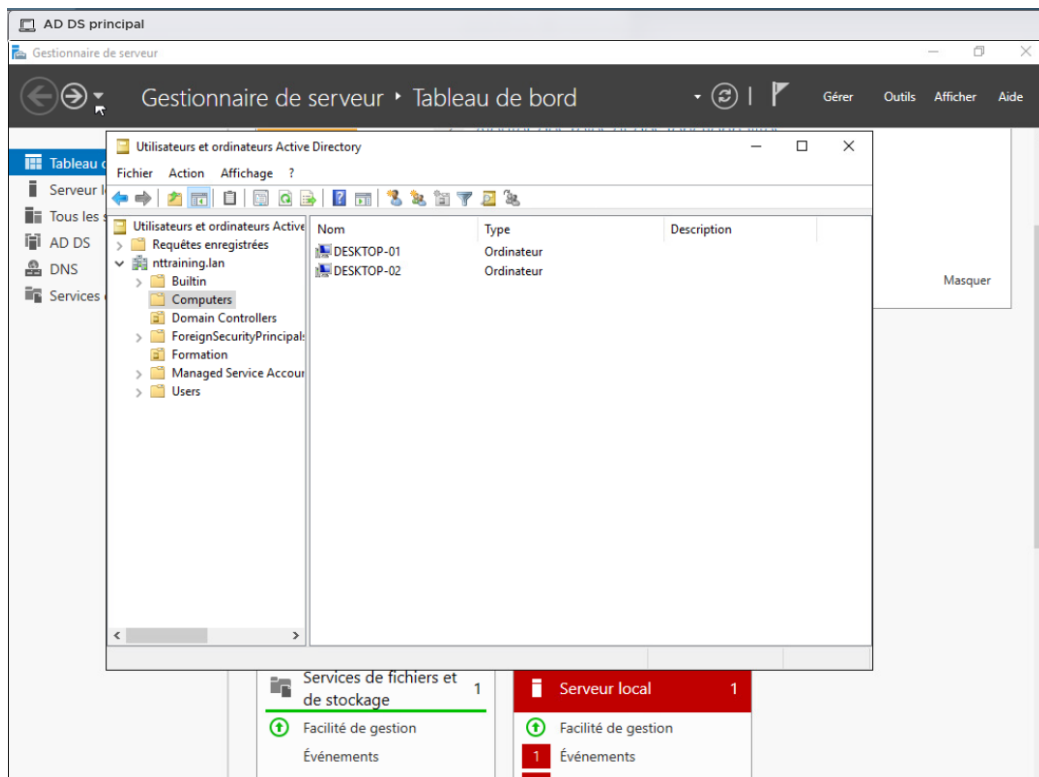


Le PC client a bien été ajouté dans le domaine.



## V.2- Vérification de l'inventaire

Cote serveur, on valide que l'objet ordinateur a bien été créé dans l'unité D'organisation par défaut.



## **VI- Compétences validées**

- **Système** : Installation et promotion de serveurs Windows server en contrôleur de domaine.
- **Sécurité des SI** : Compréhension des mécanismes de réplication et de la gestion centralisée des identités.
- **Haute disponibilité** : Mise en œuvre d'une architecture résiliente.