# Promotion d'un contrôleur de domaine

Un contrôleur de domaine est un serveur dont la fonction principale est l'authentification des utilisateurs et ordinateurs. Il a également la charge de permettre l'accès aux ressources partagées (boîtes aux lettres, dossiers partagés, imprimantes…).

## 1. Prérequis nécessaires à la promotion d'un serveur

La promotion d'un serveur en contrôleur de domaine nécessite certains prérequis. Si ces derniers ne sont pas respectés, l'opération est stoppée.

- **Système de fichiers NTFS** : les volumes et les partitions doivent être formatés avec un système de fichiers NTFS.
- **Nom du poste** : un nom de 15 caractères maximum est recommandé de plus il est préférable de ne pas utiliser de caractères spéciaux (#, é, è...), les chiffres et les caractères minuscules et majuscules peuvent eux être utilisés sans risques.
- **L'interface réseau** : elle doit être configurée avec une configuration IPv4/IPv6 correcte. L'adressage statique est recommandé pour tous les serveurs et si besoin, une exclusion doit être effectuée dans le DHCP.
- **Nom de domaine** : le nom de domaine utilisé doit être sous la forme d'un nom DNS (domaine.extension). Il est souhaitable d'utiliser des extensions qui ne soient pas utilisées sur Internet (.msft, …).
- **Serveur DNS** : un serveur DNS est nécessaire pour le fonctionnement de l'Active Directory. Néanmoins, si aucun serveur DNS n'est présent, l'installation de ce dernier peut s'effectuer pendant la promotion du serveur. Dans le cas contraire, vérifier la configuration IP afin d'utiliser le serveur DNS de production.

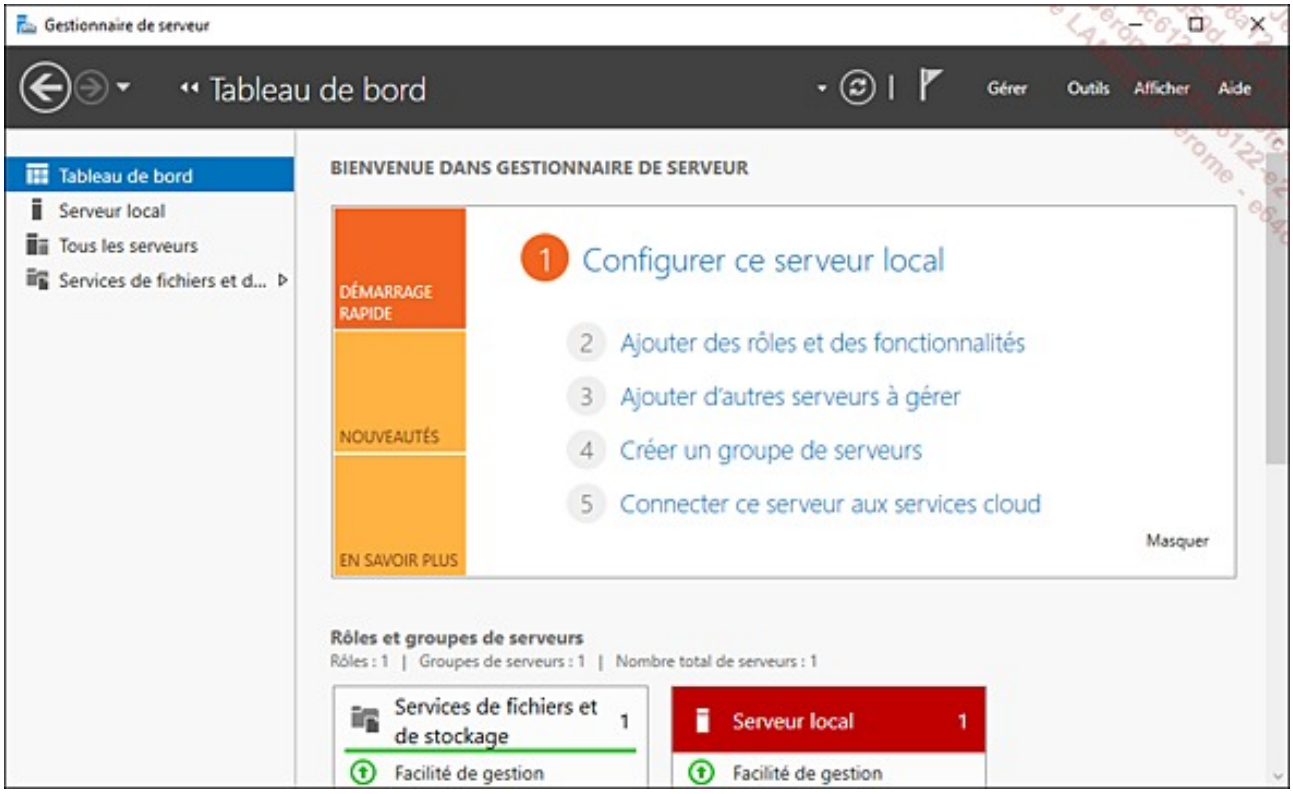
## 2. Installation d'un nouveau domaine dans une nouvelle forêt

Les services AD sont considérés comme des rôles et sont présents dans la liste des rôles.

Démarrez la machine virtuelle **AD1**.

La configuration ayant déjà été faite, il suffit maintenant d'installer Active Directory.

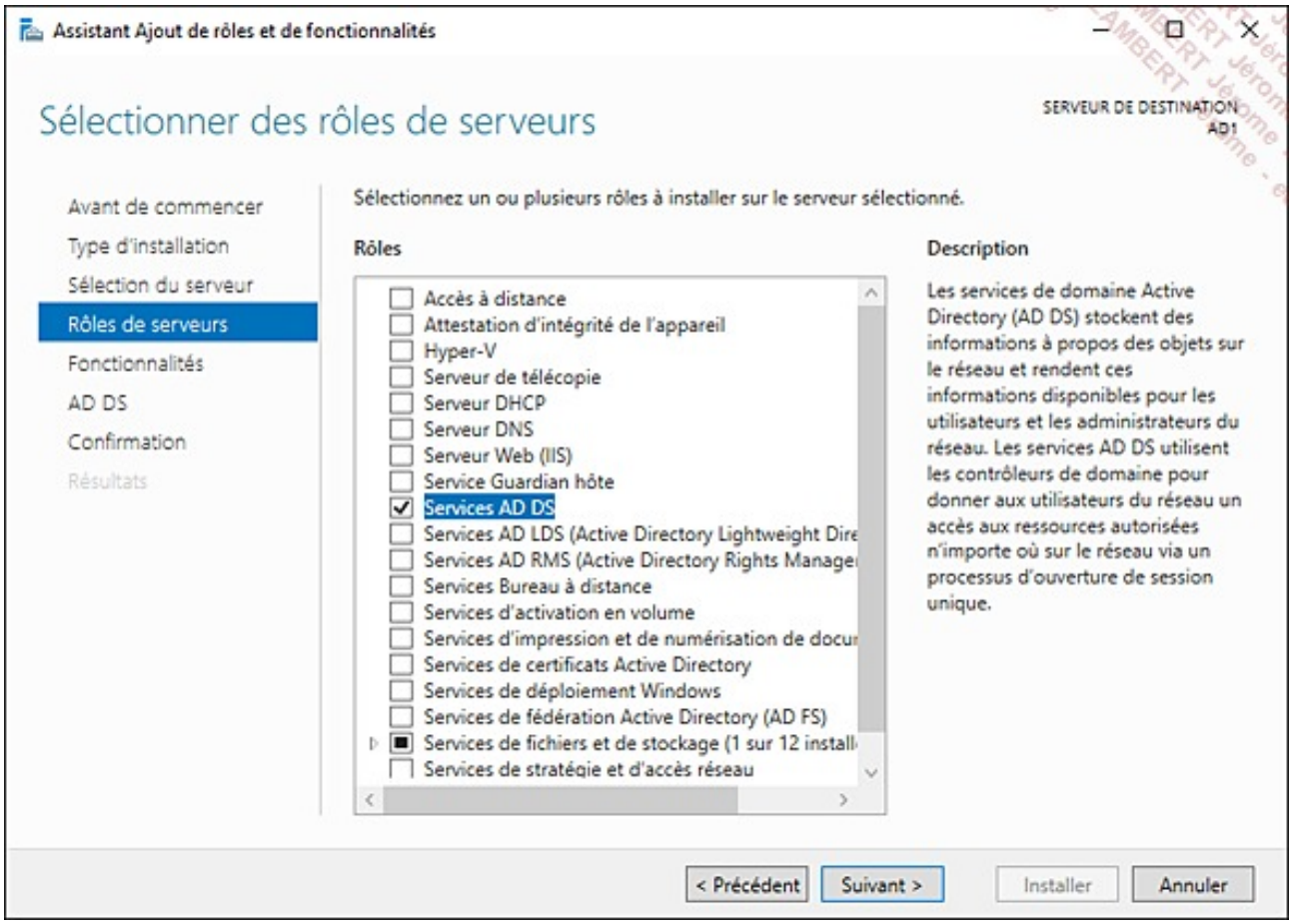
Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et fonctionnalités**.



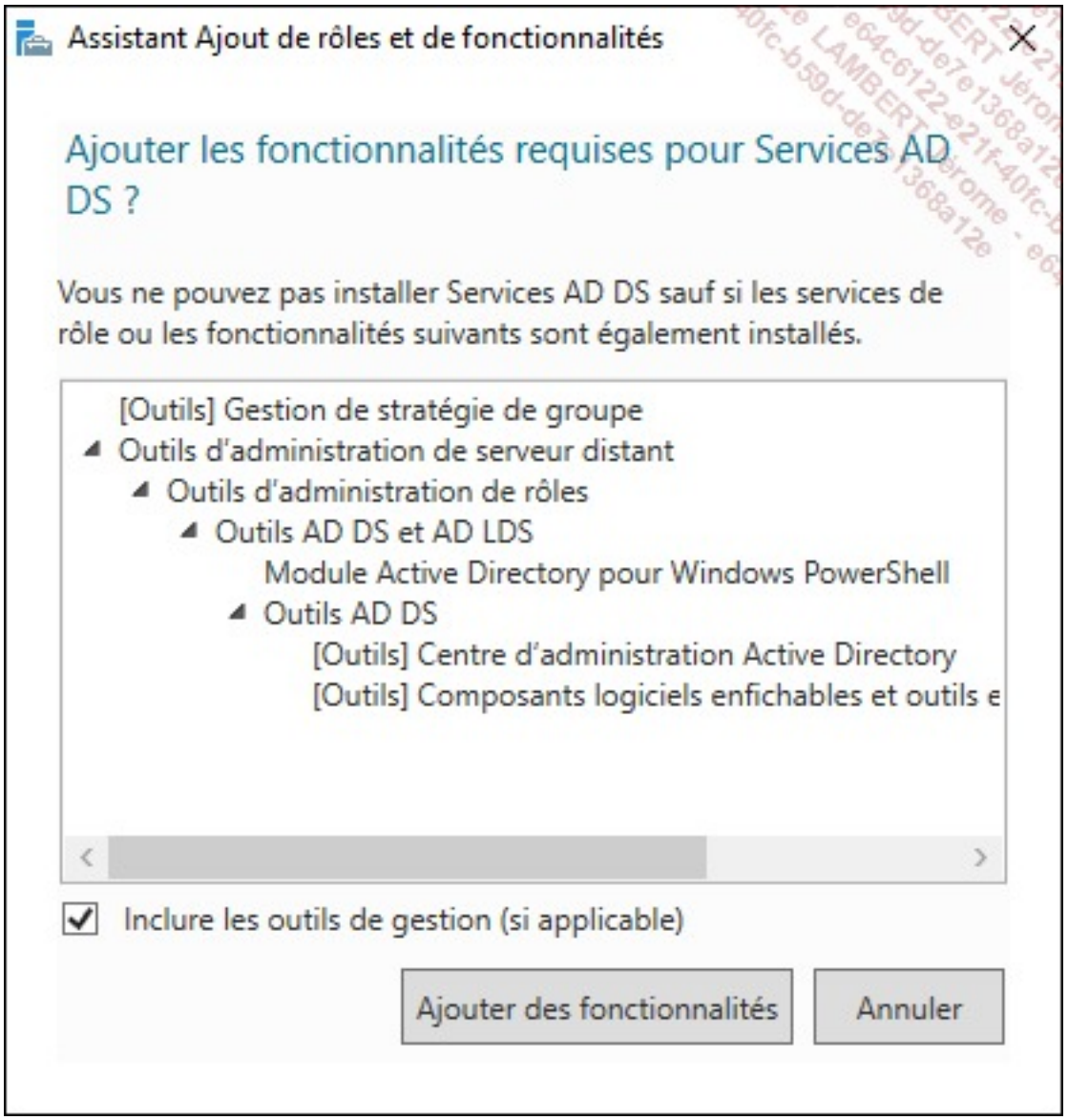

L'assistant se lance. Cliquez sur **Suivant**.

Dans les fenêtres **Type d'installation** et **Sélection du serveur**, laissez le paramètre par défaut puis cliquez sur **Suivant**.

Activez la case à cocher **Services AD DS** pour effectuer l'installation.

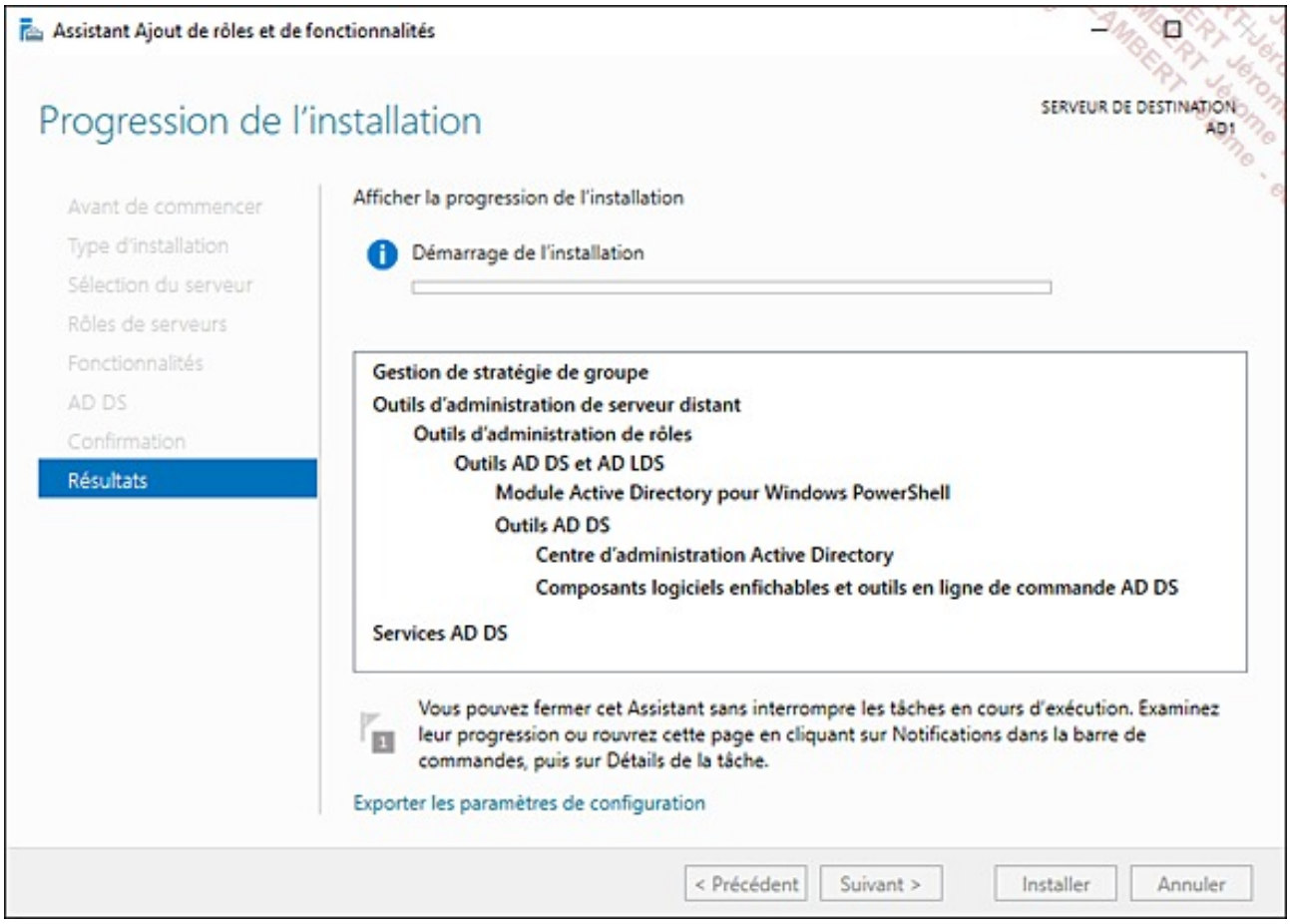



Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche, afin d'installer les fonctionnalités nécessaires à Active Directory.

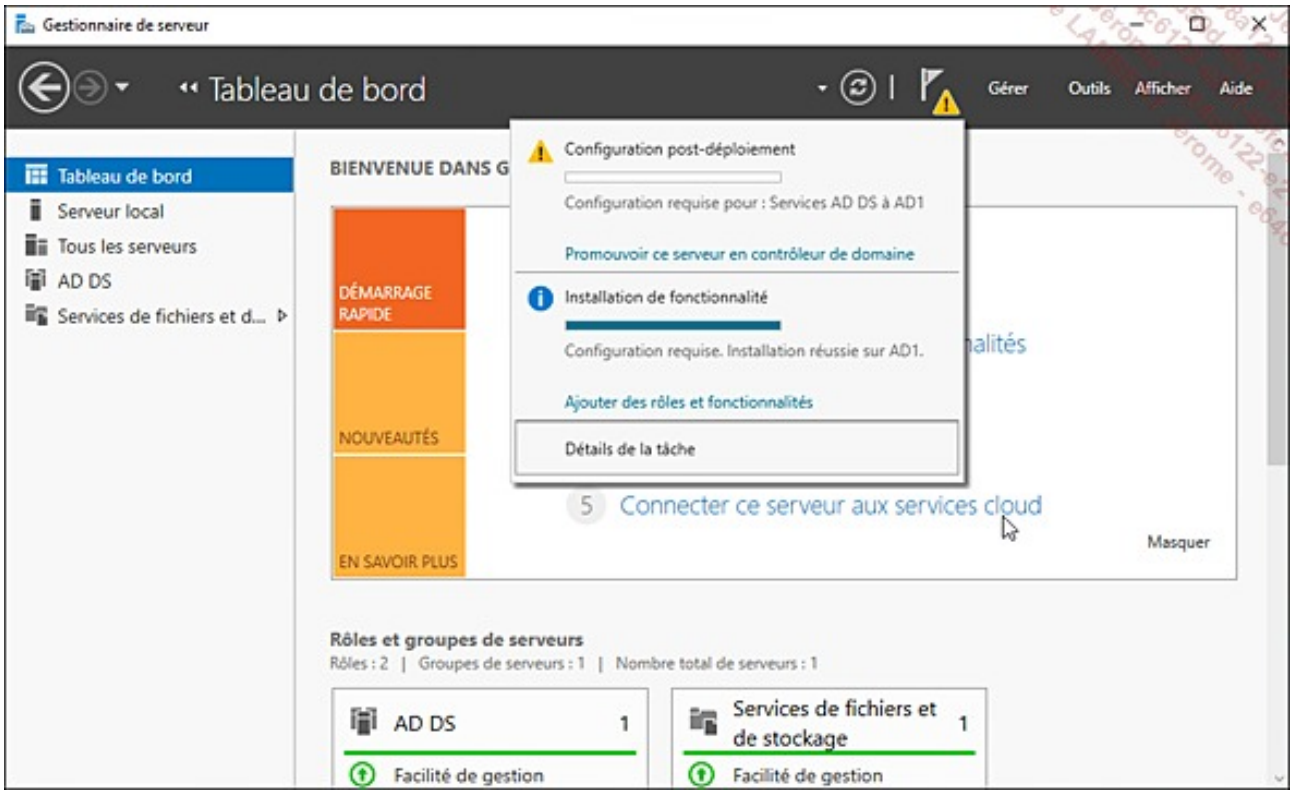



- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités** et dans les autres fenêtres.
- Cliquez sur **Installer** pour lancer l'installation.

L'installation est en cours…



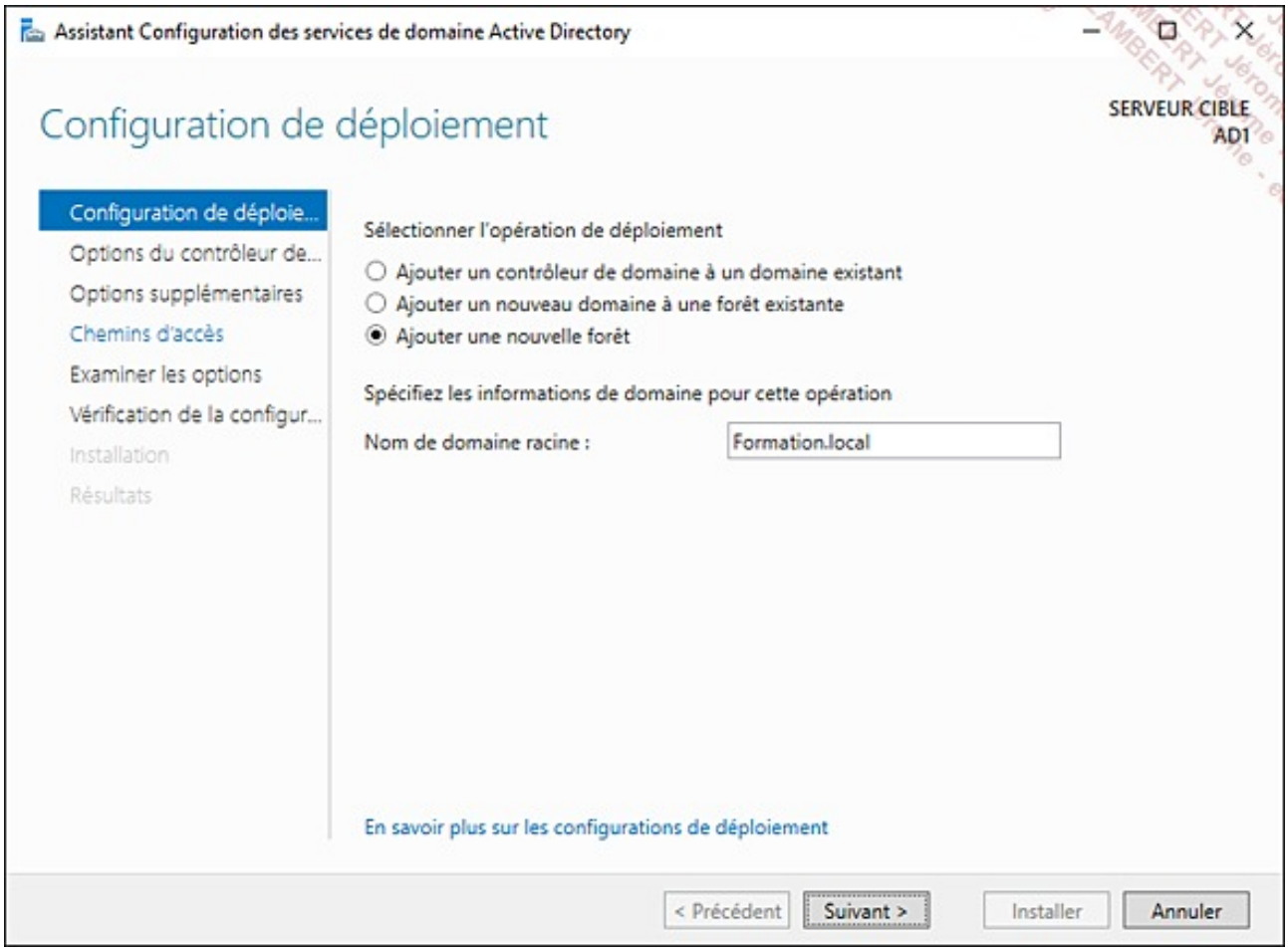

- Une fois l'installation terminée, cliquez sur **Fermer**.
- Dans la console **Gestionnaire de serveur**, cliquez sur le drapeau contenant le point d'exclamation.
- Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



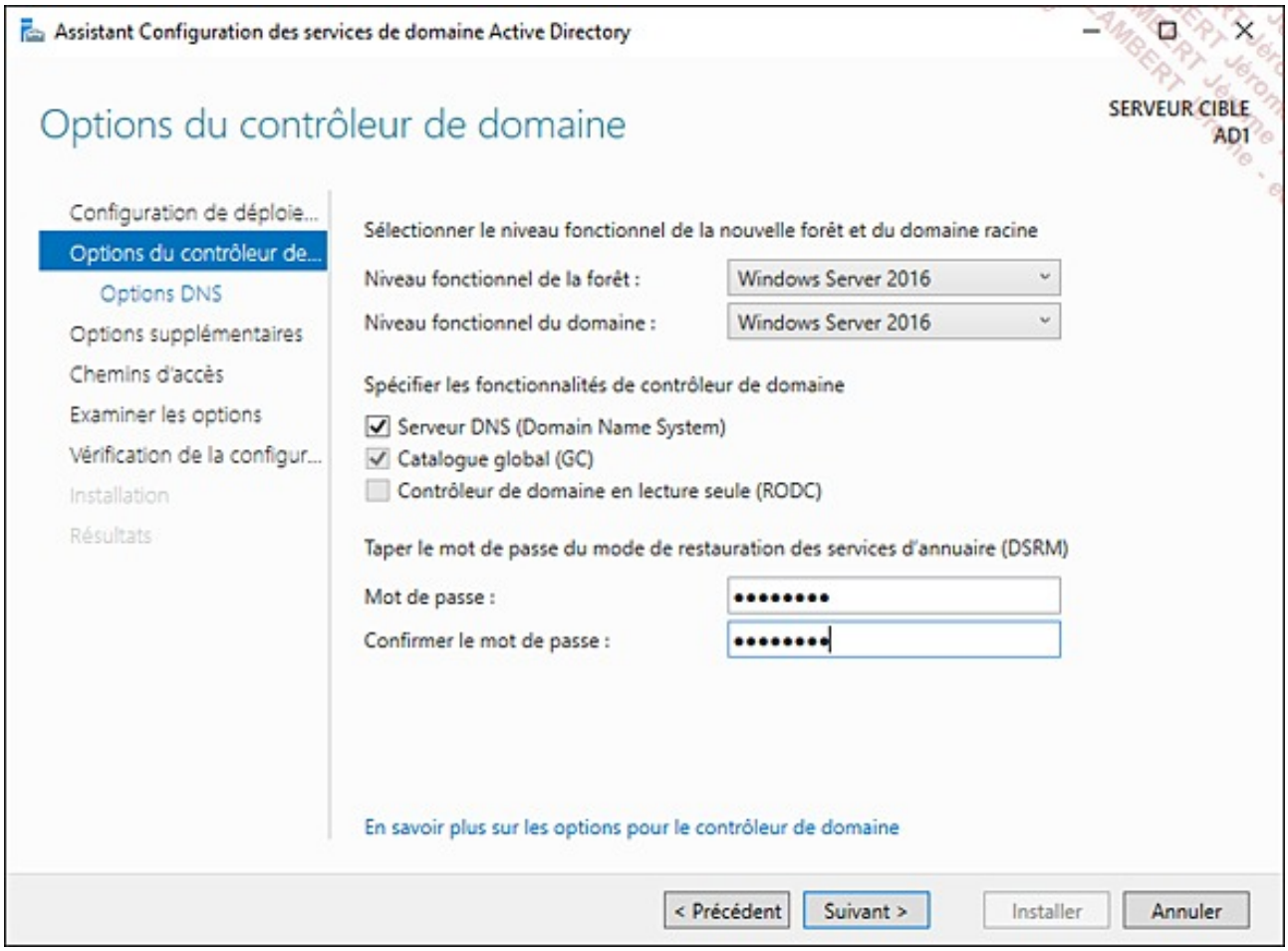

Trois options sont possibles :

- **Ajouter un contrôleur de domaine à un domaine existant** : un contrôleur de domaine est ajouté au domaine Active Directory afin d'assurer une tolérance de panne. Le deuxième serveur ajouté peut également assurer l'authentification des utilisateurs et postes de travail. Il est recommandé d'avoir deux contrôleurs de domaine dans un domaine dont un physique.
- **Ajouter un nouveau domaine à une forêt existante** : cette option permet d'effectuer la création d'une nouvelle arborescence ou l'ajout d'un domaine enfant.
- **Ajouter une nouvelle forêt** : une nouvelle forêt est créée et le domaine racine donne son nom à la forêt.

Cliquez sur **Ajouter une nouvelle forêt** et saisissez **Formation.local** dans le champ **Ajouter une nouvelle forêt**.




- Cliquez sur **Suivant** pour valider votre choix.
- Laissez la valeur par défaut dans les listes déroulantes **Niveau fonctionnel de la forêt** et **Niveau fonctionnel du domaine**. Laissez cochée la case **Serveur DNS** afin que le rôle soit installé et configuré.
- Saisissez **Pa$$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**.




- Dans la fenêtre **Options DNS**, cliquez sur **Suivant**.
- Après quelques secondes, le nom de domaine NetBIOS apparaît. Vérifiez que le nom est FORMATION.
- Cliquez sur **Suivant** pour valider la fenêtre.
- Laissez les **Chemins d'accès** par défaut et cliquez sur **Suivant**.
- Cliquez sur **Suivant** après avoir vérifié les paramètres dans la fenêtre **Examiner les options**.
- Cliquez sur **Installer** pour lancer l'installation de l'Active Directory et la promotion du serveur. À la fin de l'installation, le serveur redémarre.
- Ouvrez la session en tant qu'administrateur.

Le mot de passe du compte administrateur du domaine est l'ancien mot de passe du compte administrateur local. Un contrôleur de domaine n'a pas de base SAM (*Security Account Manager*), donc pas de compte ou groupe locaux.

Affichez le menu **Démarrer**, puis accédez aux **Outils d'administration**.

Suite à l'installation, de nouvelles consoles ont été ajoutées. Elles permettent l'administration de l'annuaire.

- **Utilisateurs et Ordinateurs Active Directory** : administration des différents objets de l'annuaire (OU, groupe, utilisateur…).
- **Sites et Services Active Directory** : administration des sites AD et de la réplication.
- **Domaine et approbation Active Directory** : création de relations d'approbation entre domaines ou entre forêts.
- **Gestion des stratégies de groupe** : création, administration et maintenance des différentes stratégies de groupe.
- **Modification ADSI** : modification des attributs LDAP.

Le serveur qui vient d'être installé peut effectuer des modifications sur la base de données AD et donc répliquer ces modifications. Cette réplication peut poser des problèmes en cas d'altération de la base de données ou en cas de mauvaise modification. De plus, en cas de vol du contrôleur de domaine, l'ensemble des comptes présent dans l'annuaire Active Directory est compromis.

Pour ces raisons, il est utile dans certains cas d'installer un **contrôleur de domaine en lecture seule (RODC)**.

## 3. Installation d'un serveur en mode RODC

Apparue avec Windows Server 2008, la fonctionnalité de contrôleur de domaine en lecture

seule consiste à installer un contrôleur de domaine qui possède uniquement des droits de lecture sur la base de données AD. Il sera impossible d'effectuer des modifications : les différentes opérations (ajout/modification/suppression) sont apportées sur un contrôleur de domaine en lecture/écriture et par réplication au RODC.

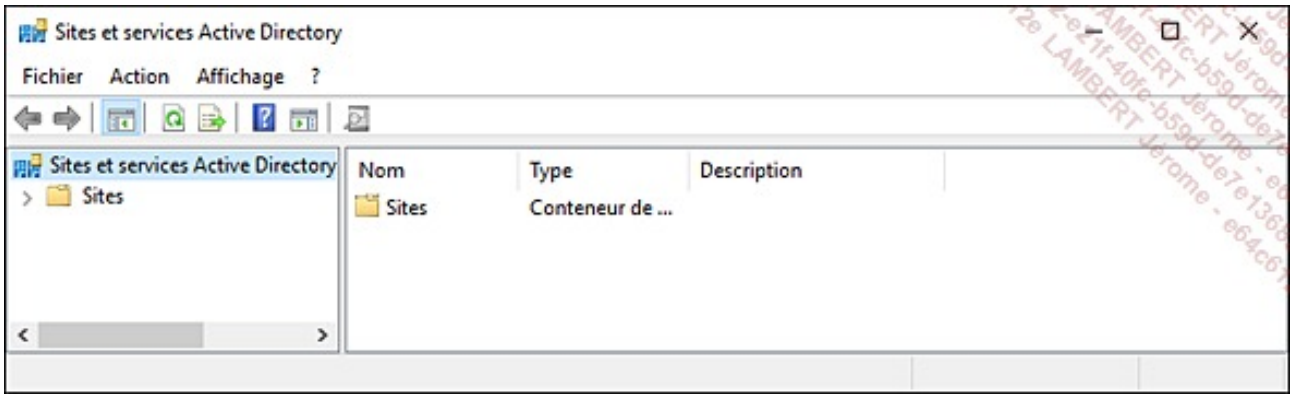
Contrairement à un contrôleur de domaine en lecture/écriture, un utilisateur peut se connecter en local à un RODC. Une délégation peut donc être donnée à un autre utilisateur pour l'administration du serveur (mise à jour Windows Update…) sans que celui-ci ne soit **administrateur du domaine**.

Néanmoins, certains prérequis sont à respecter :

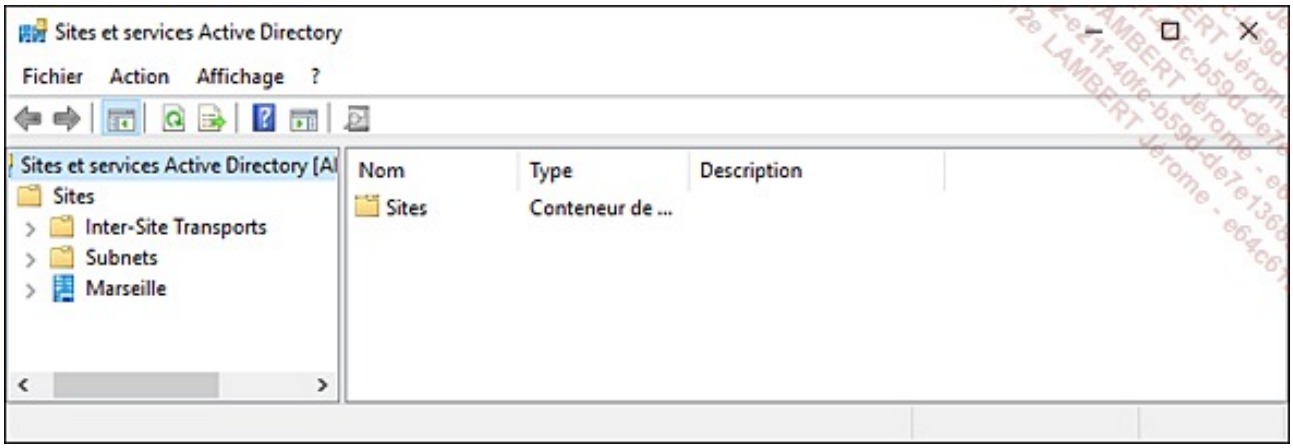
- **Niveau fonctionnel** : Windows Server 2003 ou supérieur pour la forêt et le domaine.
- **Schéma** : l'extension du schéma doit être effectuée afin d'accueillir la fonctionnalité RODC (adprep/rodcprep).
- **Contrôleur de domaine** : un contrôleur de domaine en lecture/écriture sous Windows Server 2008 ou supérieur doit être présent sur le domaine.

L'installation d'un RODC (*Read Only Domain Controller*, contrôleur de domaine en lecture seule) s'effectue souvent sur des sites distants. Nous allons donc dans un premier temps effectuer la création d'un deuxième site AD. Ce dernier contiendra uniquement le serveur RODC. Par la suite, la promotion du serveur pourra être effectuée.

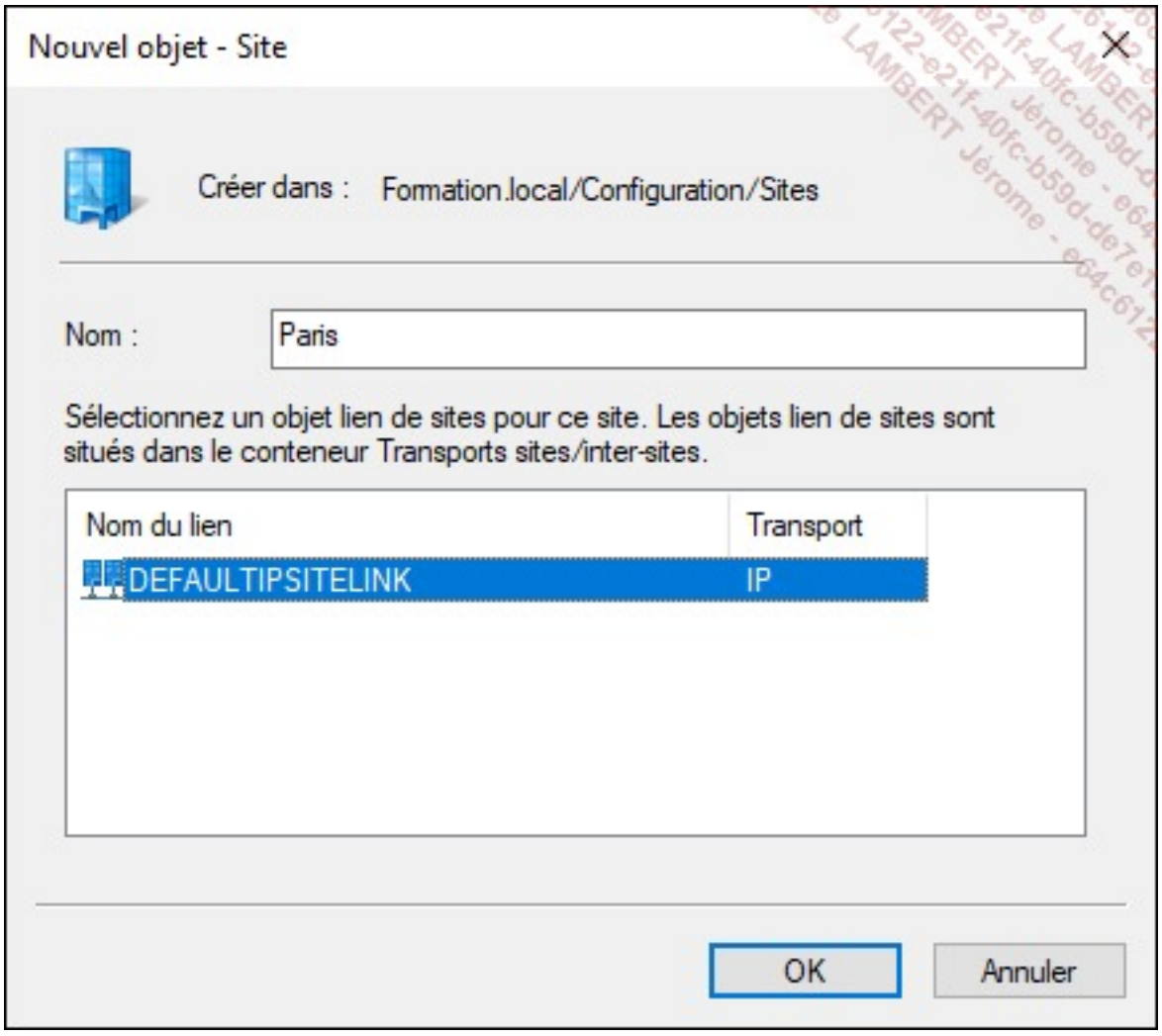
Sur **AD1**, accédez à la console Sites et services Active Directory.




- Déroulez le dossier **Sites** afin d'afficher les sites présents dans AD.
- Effectuez un clic droit sur **Default-First-Site-Name** puis sélectionnez l'option **Renommer**.
- Remplacez le nom par défaut par **Marseille**.



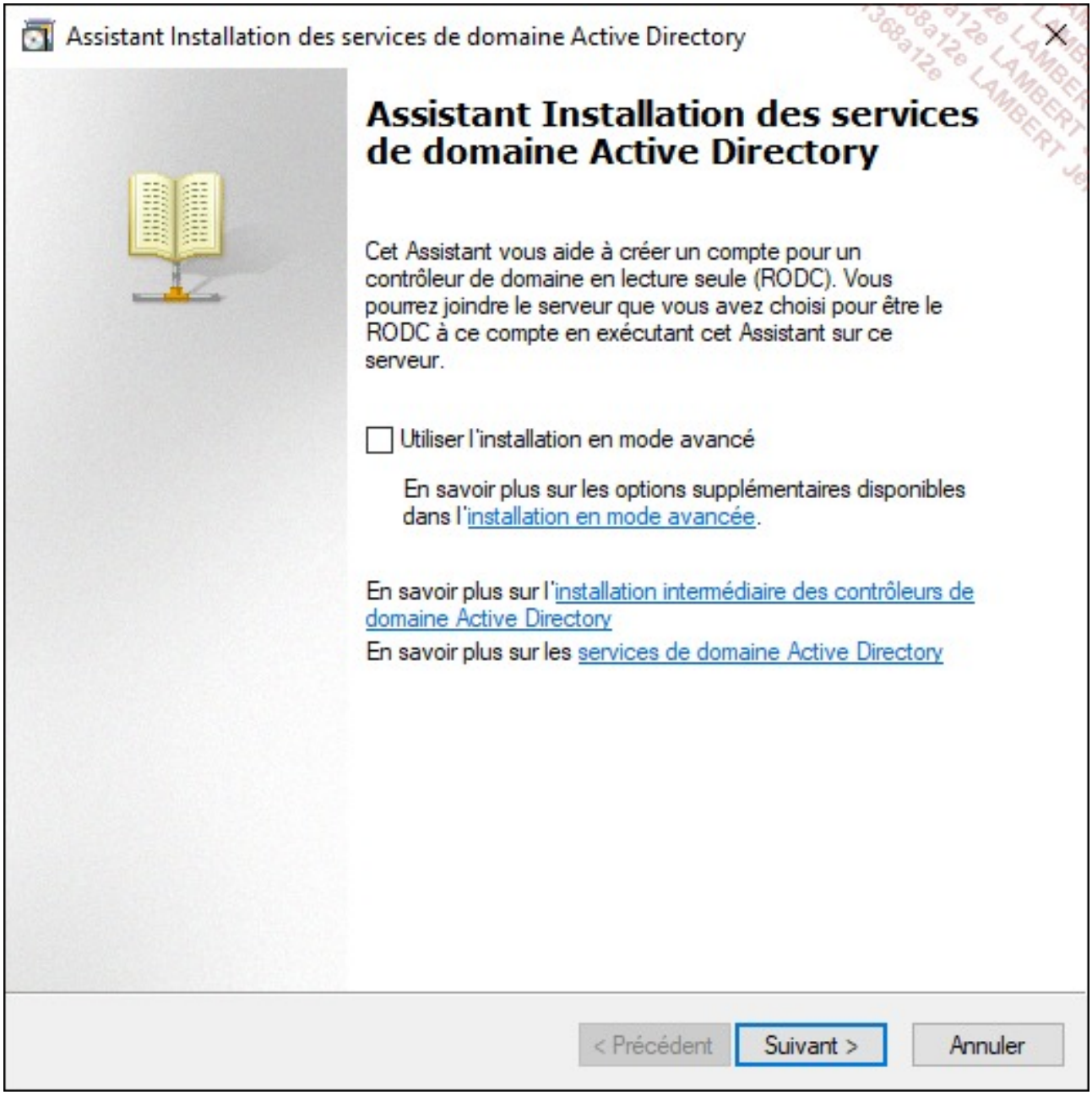

- Effectuez un clic droit sur le dossier **Sites** et sélectionnez **Nouveau Site**.
- Dans le champ **Nom**, saisissez **Paris** et sélectionnez **DEFAULTIPSITELINK**.




Le RODC va être placé sur le site de Paris. Ce dernier va être créé en amont de la promotion.

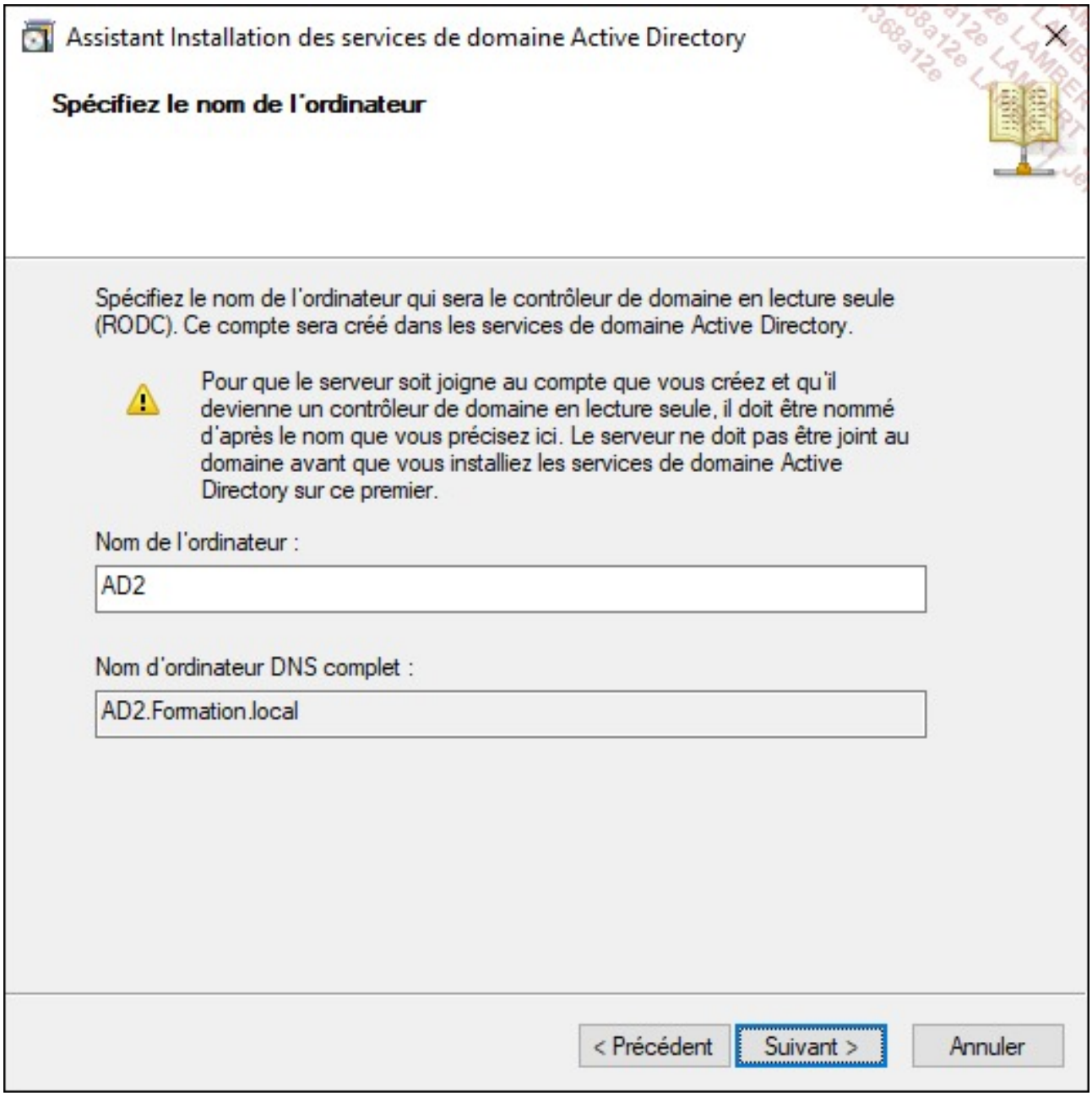
- Cliquez sur **OK** au message d'information.
- Depuis les outils d'administration, ouvrez la console **Utilisateurs et Ordinateurs Active Directory**.
- Effectuez un clic droit sur l'OU **Contrôleur de domaine** puis sélectionnez l'option **Créer au préalable un compte de contrôleur de domaine en lecture seule…**.

Cliquez sur **Suivant** dans la fenêtre d'accueil de l'assistant.



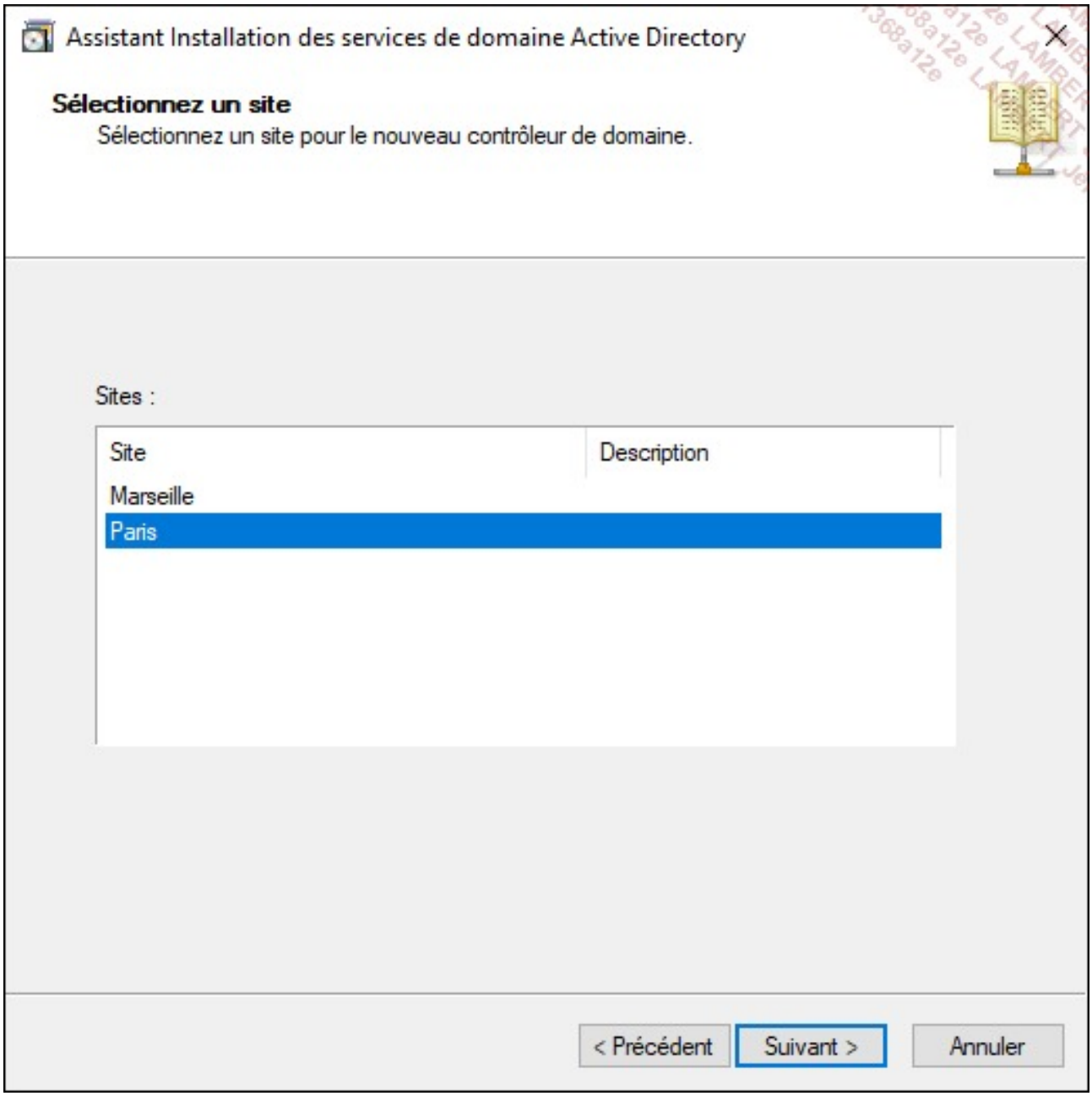

Dans la fenêtre **Informations d'identification réseau**, laissez le choix par défaut. Le compte **Administrateur** est utilisé pour l'installation.

Saisissez le nom du serveur (AD2) dans le champ **Nom de l'ordinateur** puis cliquez sur **Suivant**. AD2 ne doit pas être membre du domaine, et si le compte ordinateur existe, ce dernier doit être supprimé. Dans le cas contraire, un message vous avertit qu'un compte existe déjà.



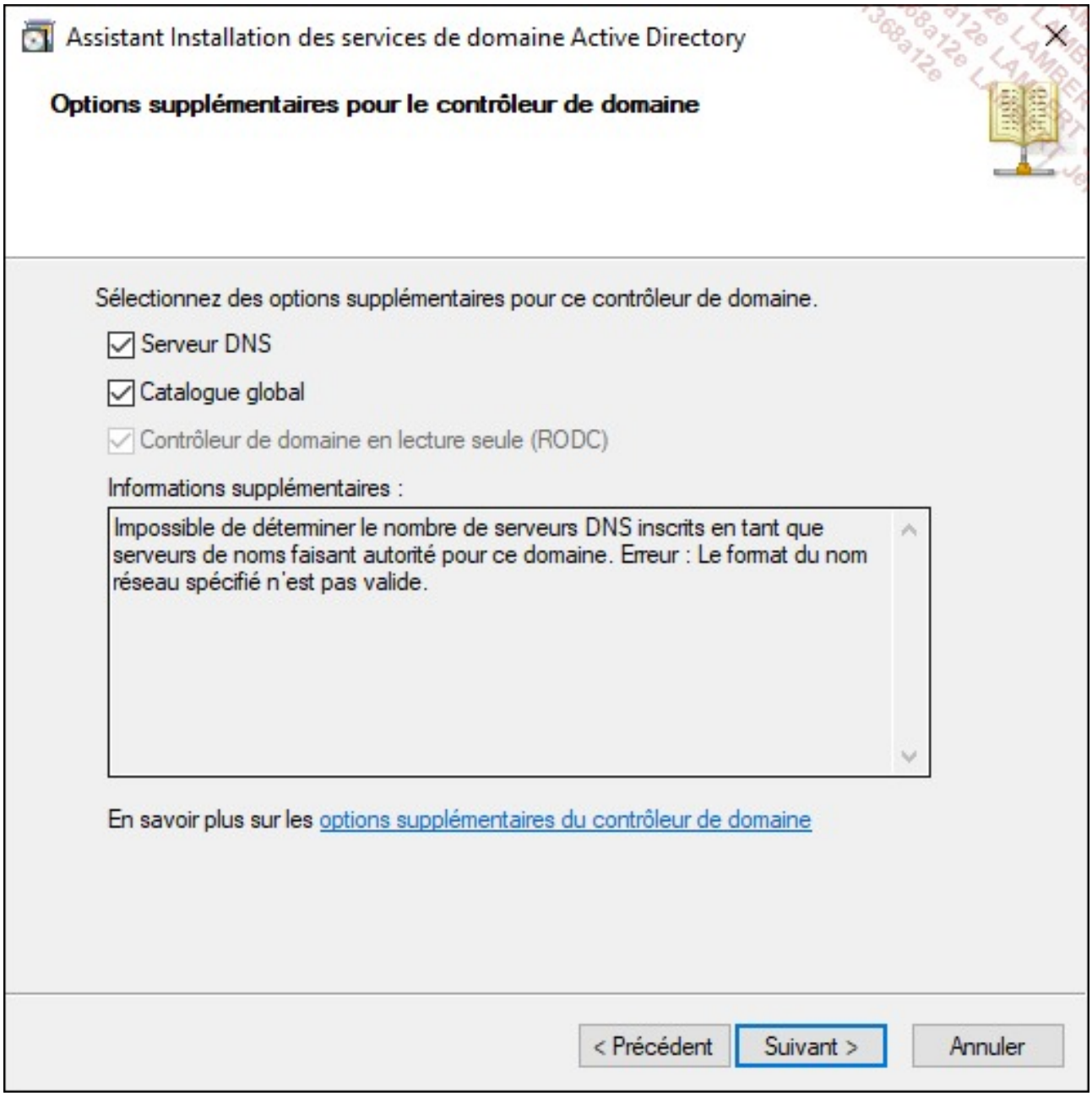

Il est très important de mettre le nom exact du futur RODC.

Le choix du site doit être fait, sélectionnez **Paris** et cliquez sur **Suivant**.

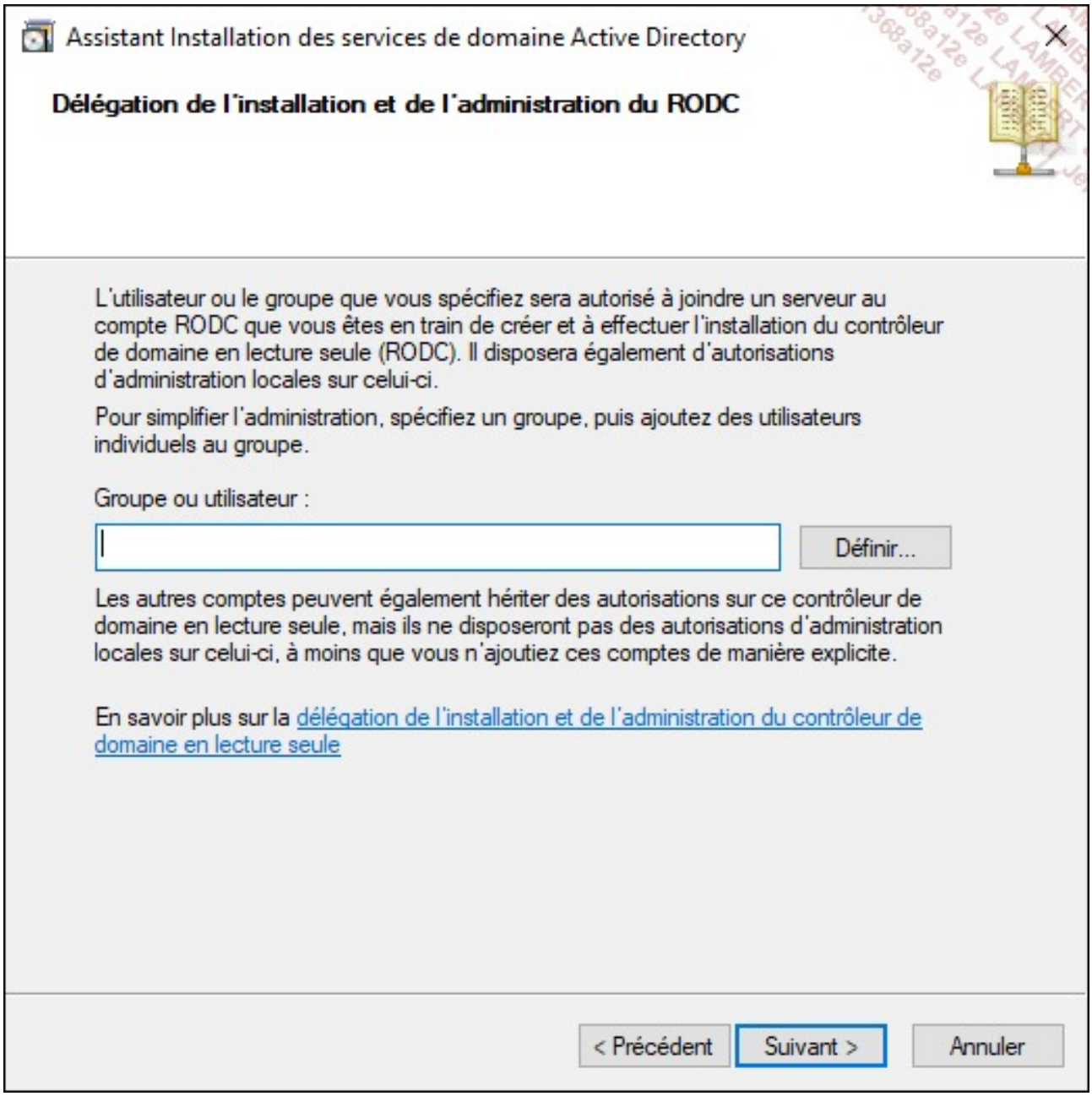



Attendez la fin de l'analyse de la configuration DNS. À l'aide de la fenêtre suivante, il est possible d'effectuer plusieurs choix :

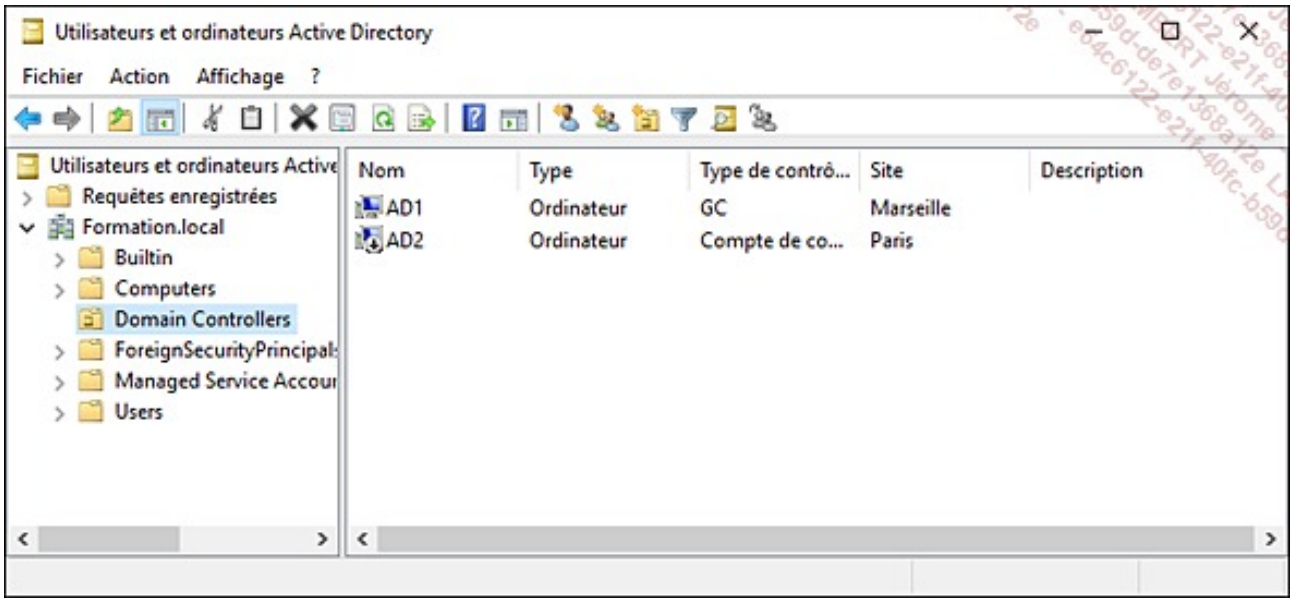
- **Serveur DNS** : installation d'un serveur DNS en mode lecture seule.
- **Catalogue global** : le serveur installé aura le rôle de catalogue global.
- **Contrôleur de domaine en lecture seule (RODC)** : le contrôleur de domaine installé est un RODC et non un serveur avec des droits de lecture/écriture dans Active Directory.




Il n'est pas envisagé de déléguer l'administration du serveur sur le site de Paris, l'installation est donc faite avec le compte **administrateur du domaine**. Cliquez sur **Suivant** dans la fenêtre **Délégation de l'installation et de l'administration du RODC**.

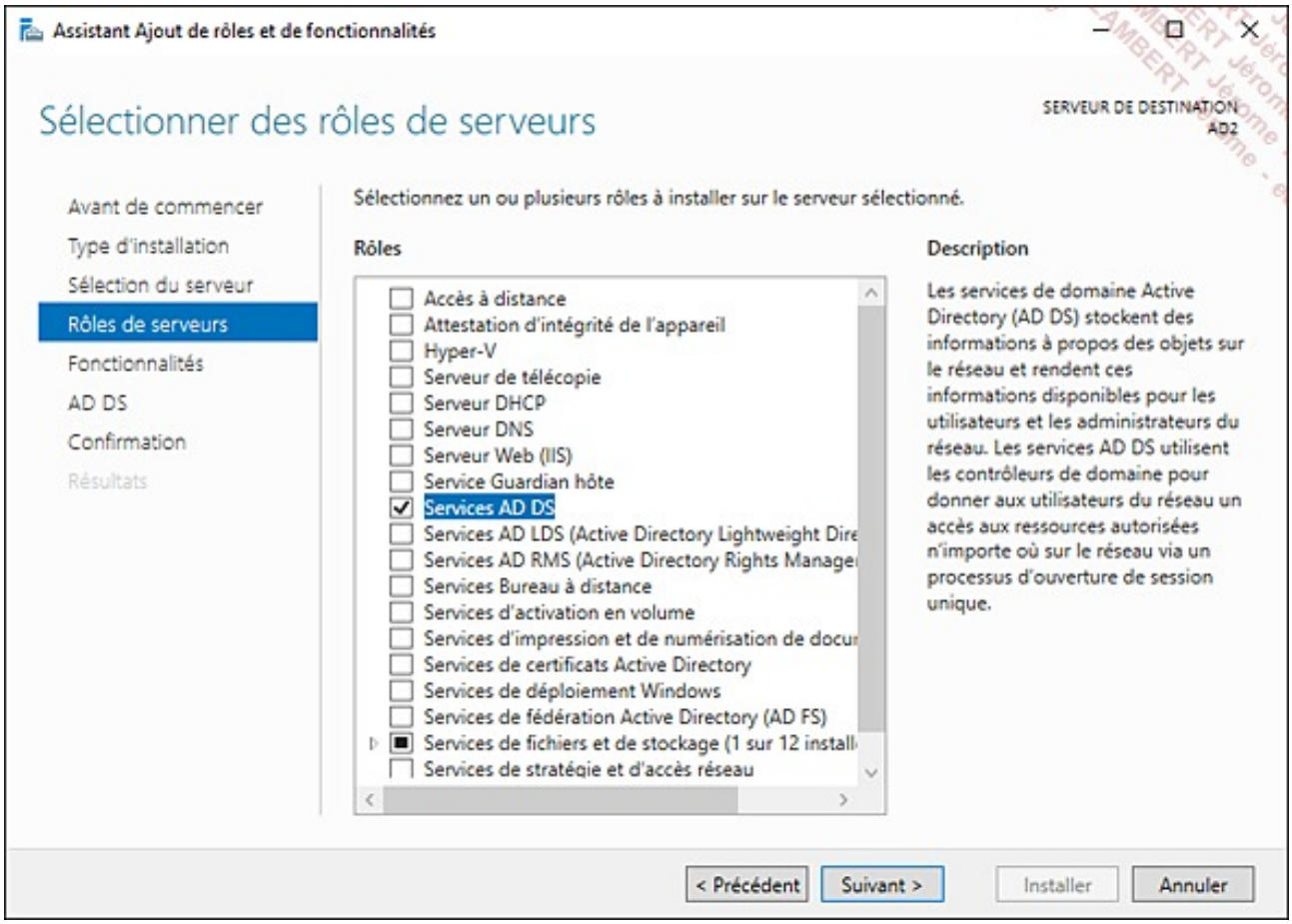



Dans la fenêtre de résumé, cliquez sur **Suivant** puis sur **Terminer**. Le compte de la machine apparaît avec l'état désactivé.

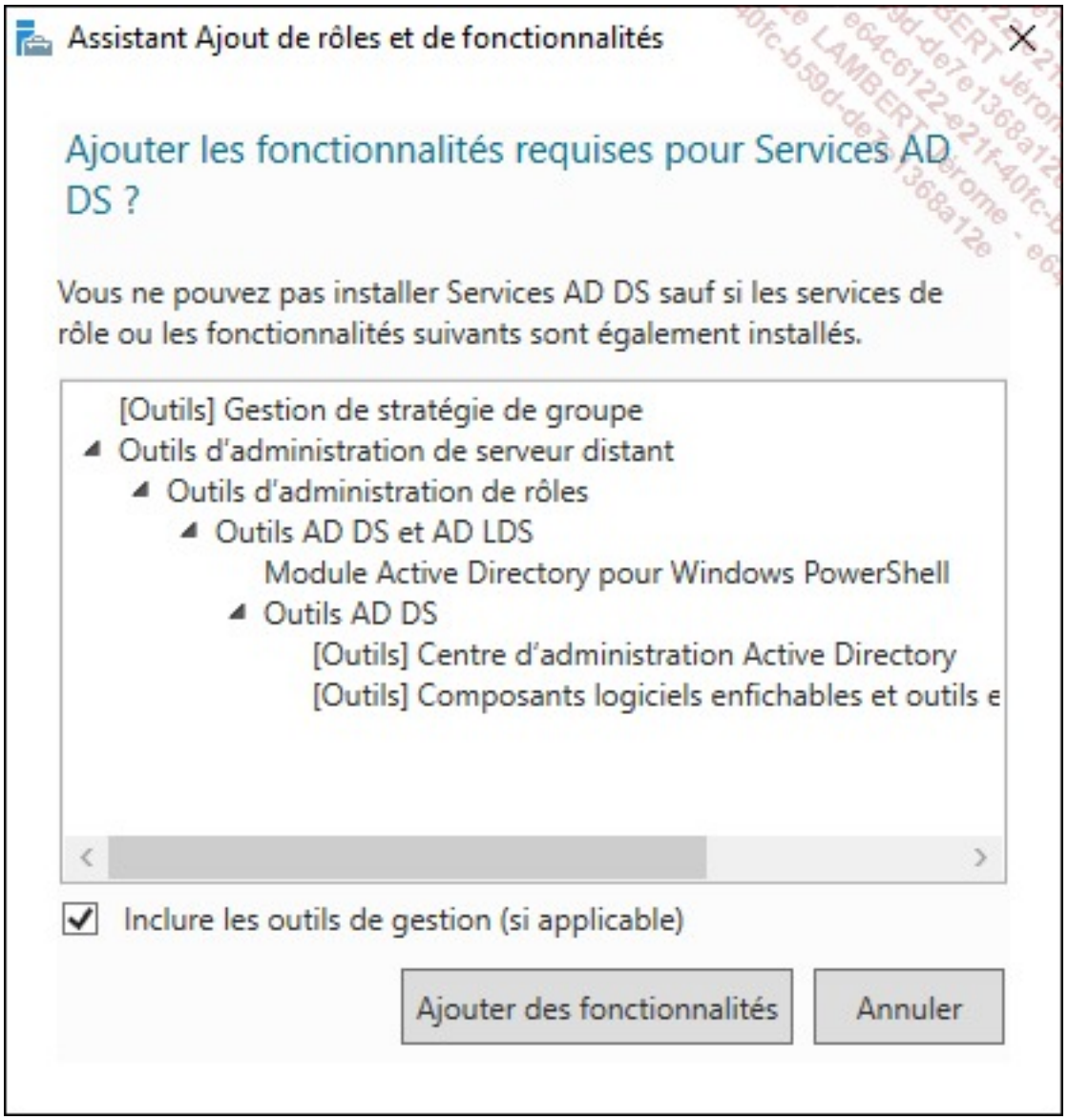



Le compte ayant été créé au préalable, la promotion peut maintenant être effectuée. Cette étape peut évidemment être évitée, dans ce cas le compte ordinateur du RODC est créé lors de la promotion. Néanmoins, dans ce cas précis, la mise en place d'une délégation est impossible, il sera nécessaire de le faire à la suite de la promotion, un compte administrateur devrai ainsi être utilisé pour la promotion. La création du compte ordinateur permet de déléguer l'opération de promotion à un support de proximité.

- Connectez-vous à la machine virtuelle **AD2** puis ouvrez une session en tant qu'administrateur.
- Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des Rôles et des fonctionnalités**.
- L'assistant se lance, cliquez sur **Suivant**.
- Cliquez sur **Installation basée sur un rôle ou une fonctionnalité** dans la fenêtre **Sélectionner le type d'installation**.
- Dans la fenêtre du choix de serveur de destination, laissez le paramètre par défaut.
- Cochez la case **Services AD DS**.



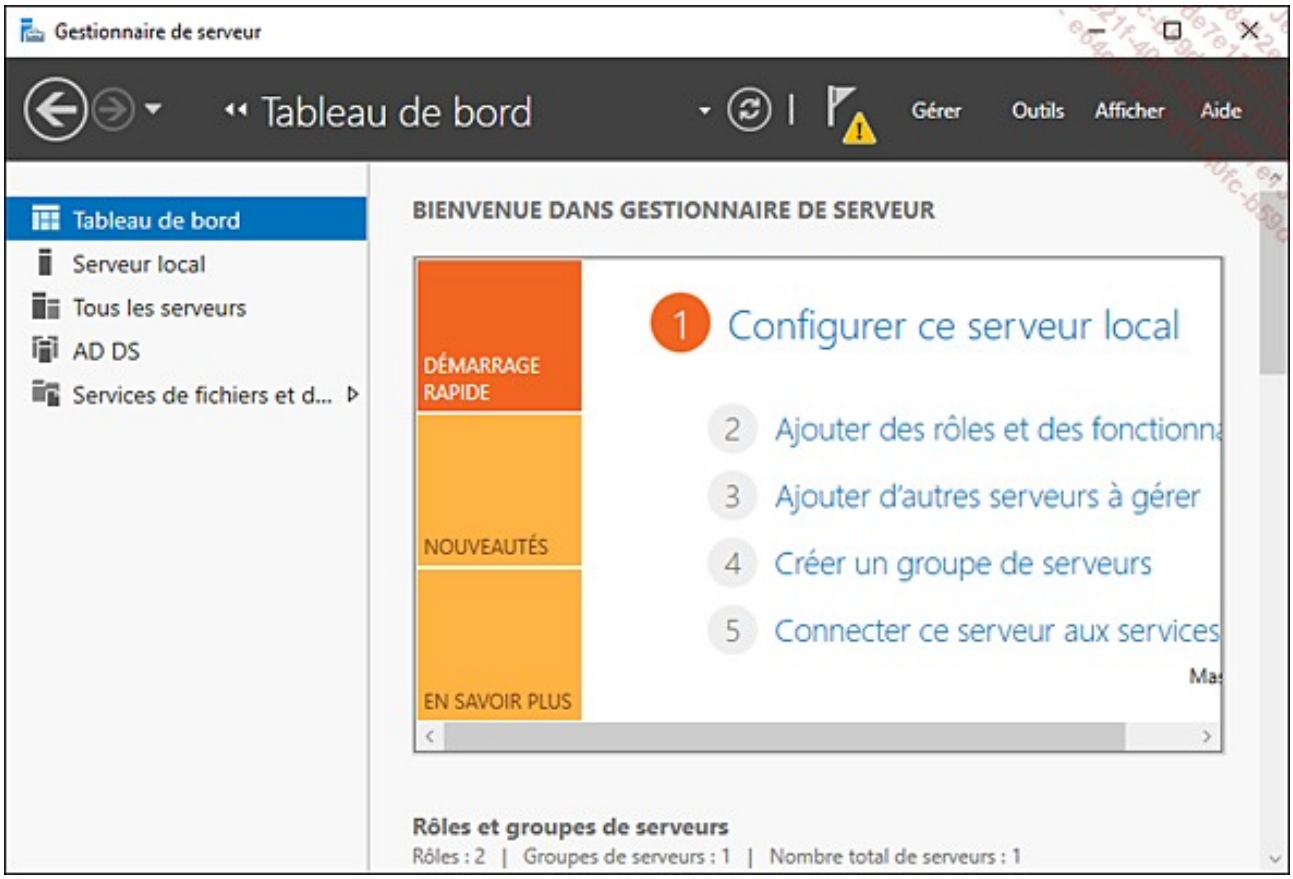

Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche afin d'installer les fonctionnalités nécessaires à Active Directory.



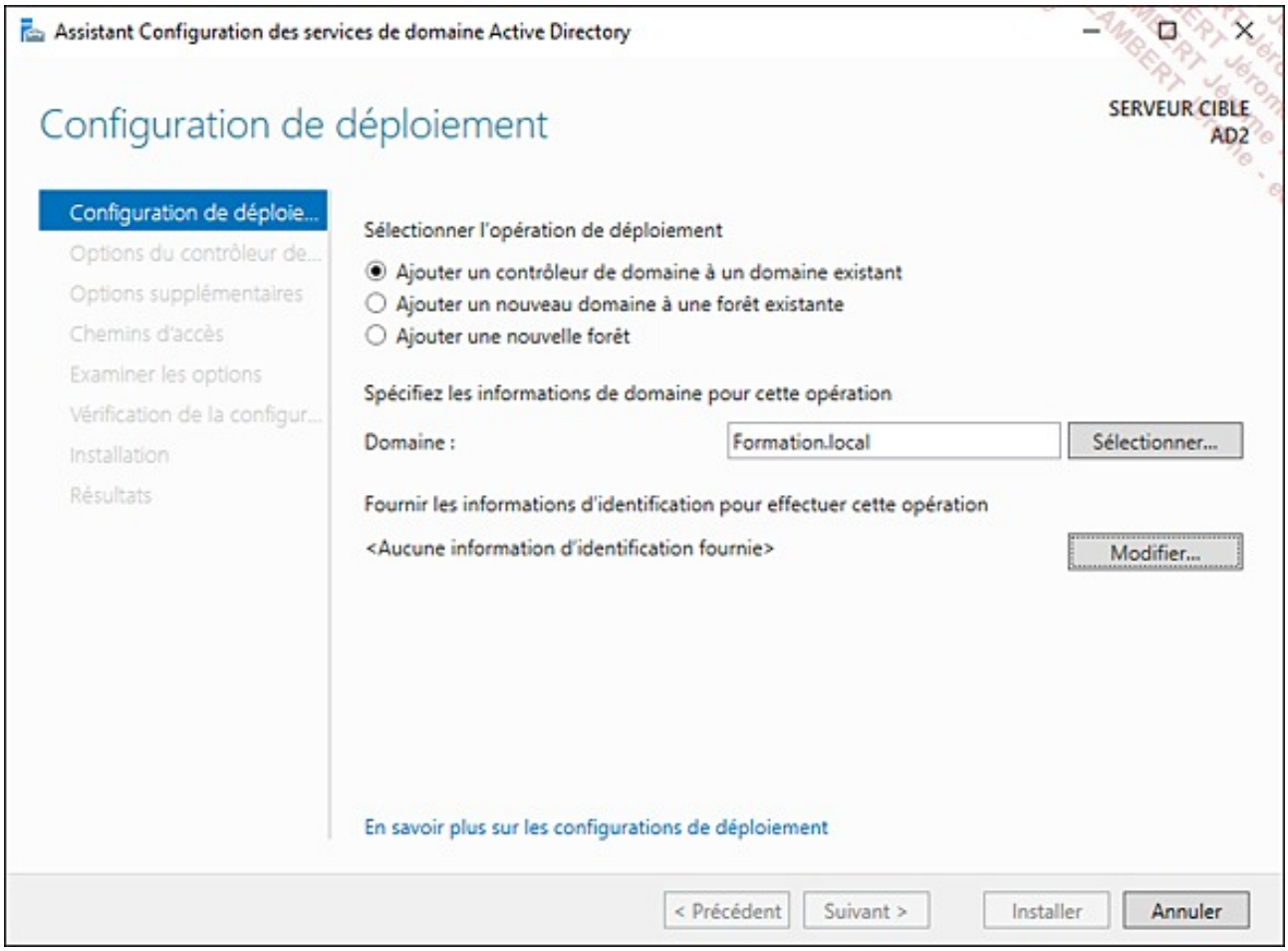

- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités**.
- Cliquez sur **Installer** pour lancer l'installation.

L'installation est en cours…

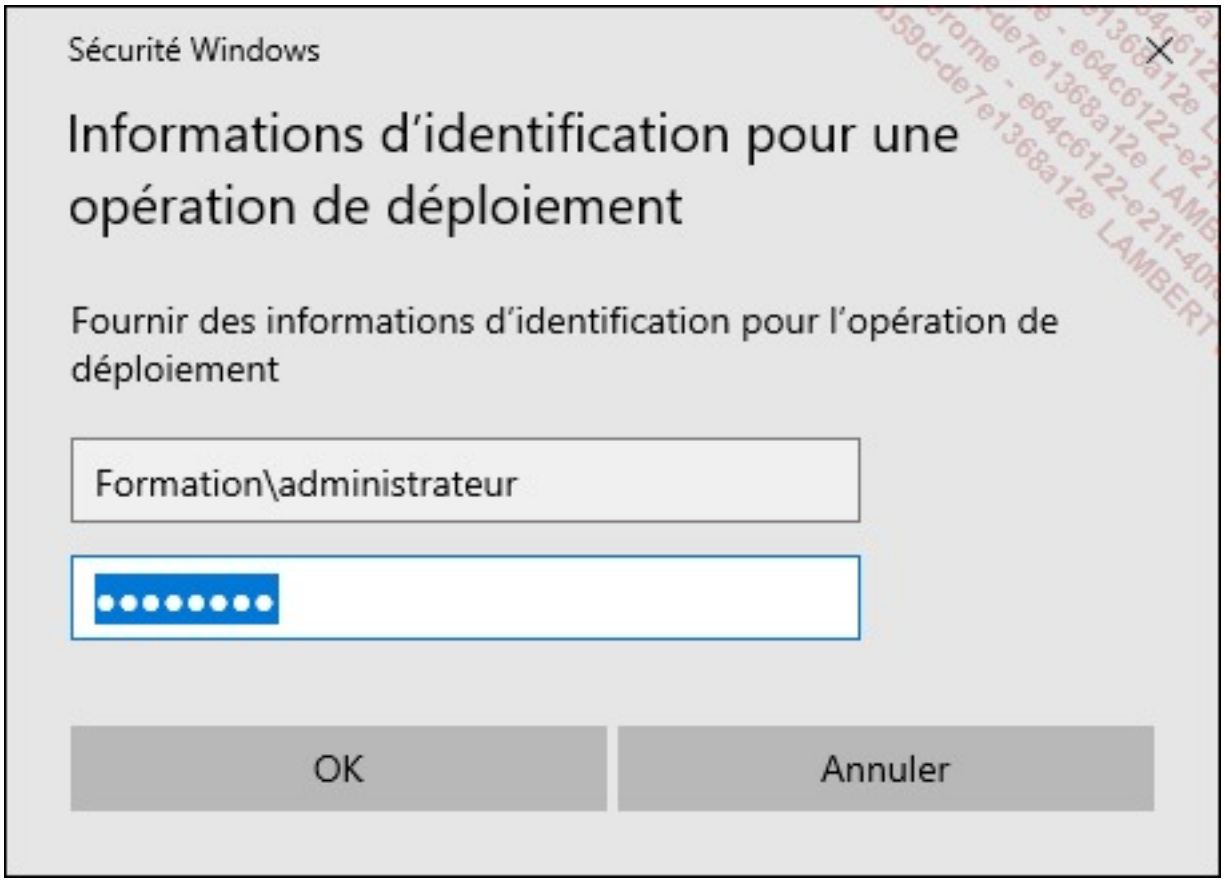
- Une fois l'installation terminée, cliquez sur **Fermer**.
- Dans la console **Gestionnaire de serveur**, cliquez sur le drapeau présent dans la zone de notification.
- Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



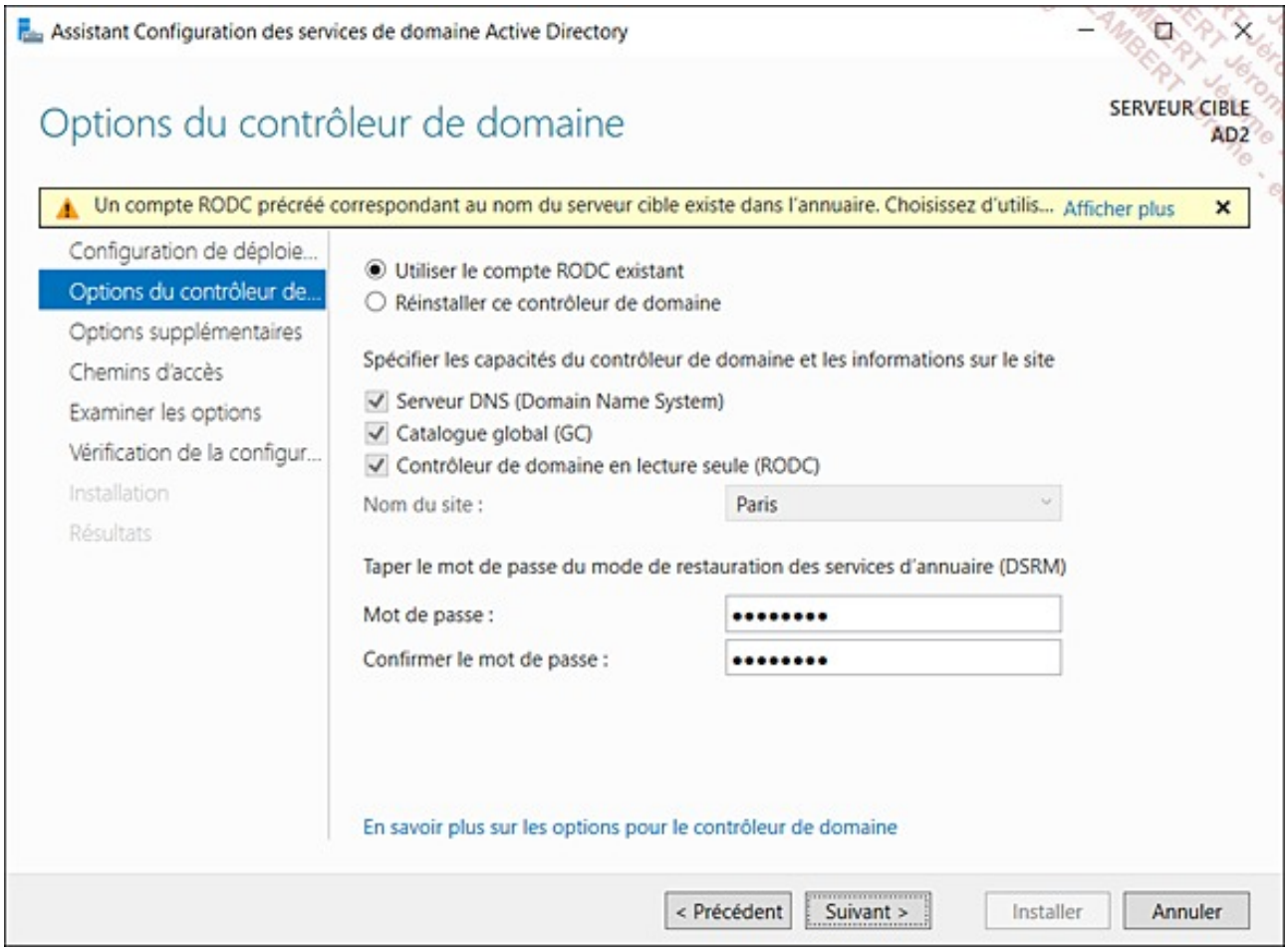

Cliquez sur **Ajouter un contrôleur de domaine à un domaine existant** et saisis-sez dans le champ **Domaine** le nom du domaine **Formation.local**.



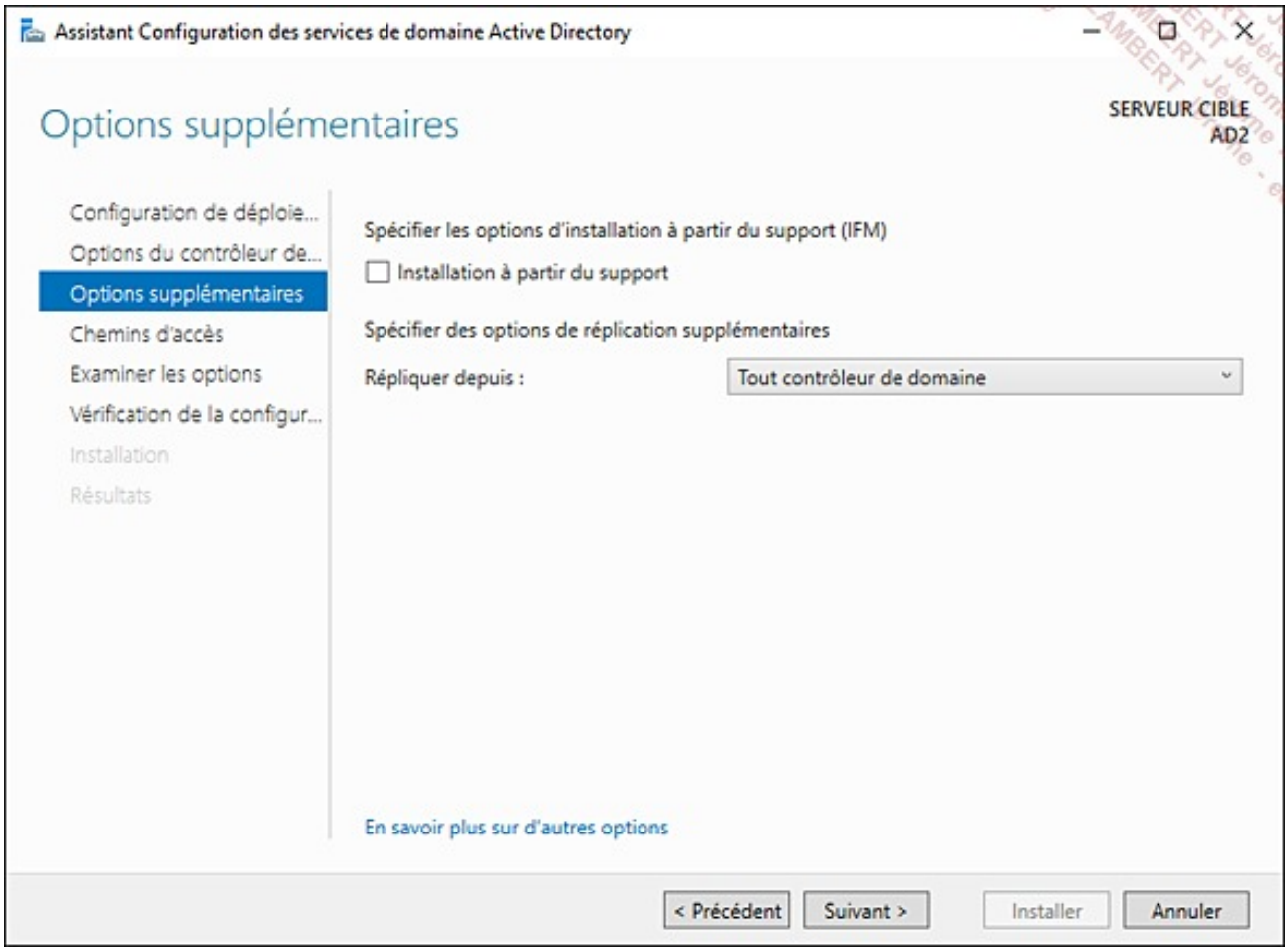

- Cliquez sur le bouton **Modifier** afin de saisir les informations d'identification.
- Saisissez **Formation\administrateur** dans le champ du nom d'utilisateur ainsi que le mot de passe dans le champ adéquat.




Saisissez **Pa$$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)** puis cliquez sur **Suivant**.



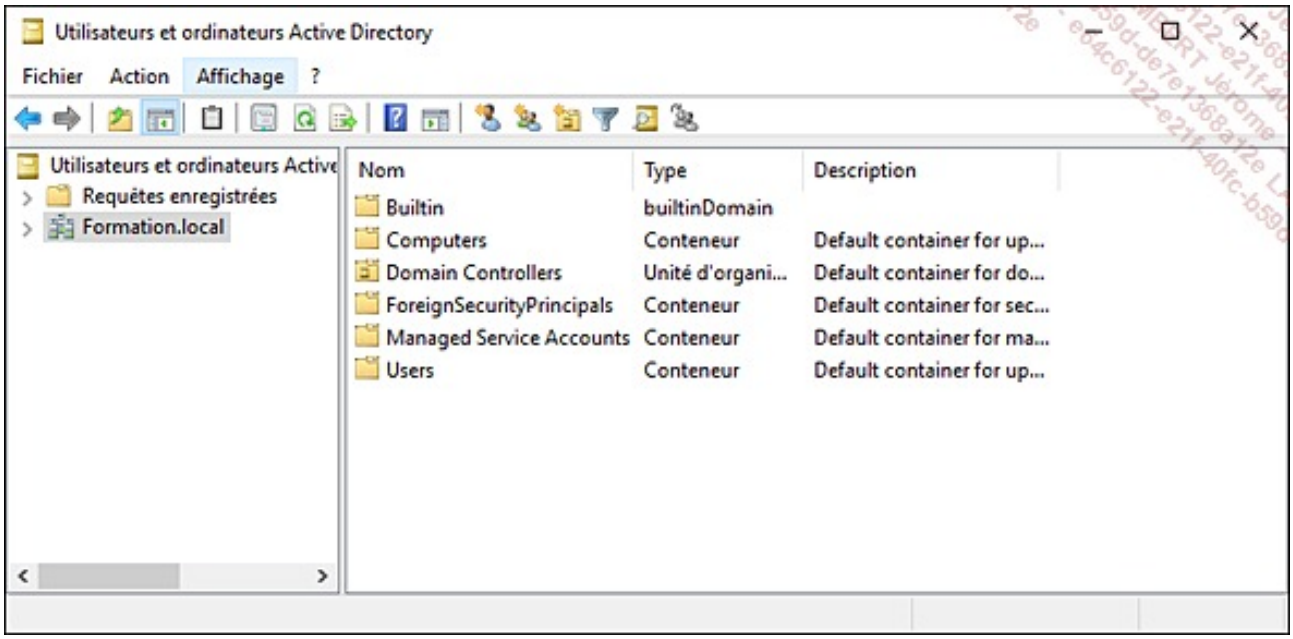

Un seul contrôleur de domaine est présent, laissez les choix par défaut dans la fenêtre **Options supplémentaires** et cliquez sur **Suivant**.



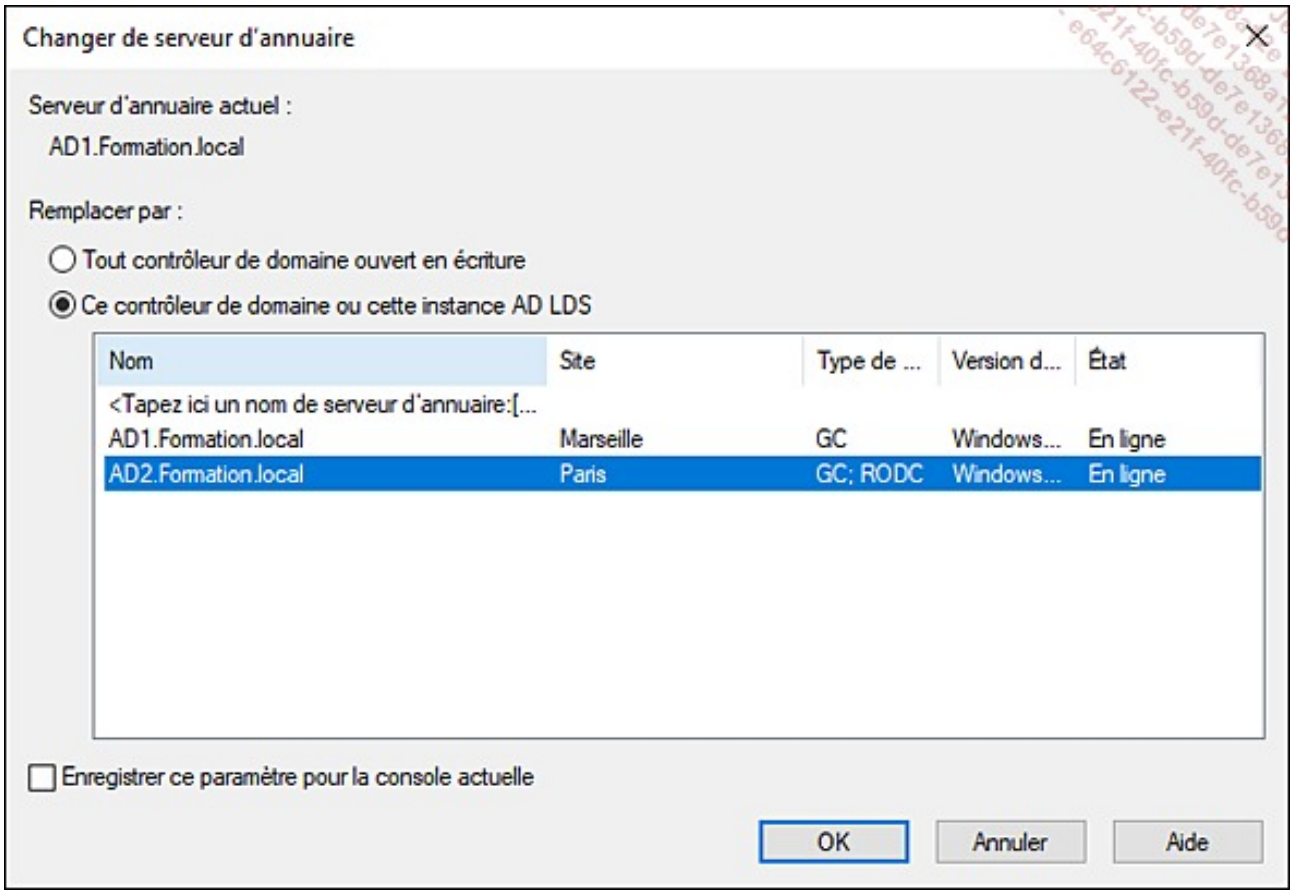

- Dans la fenêtre des chemins d'accès, cliquez sur **Suivant**.
- Dans la fenêtre du résumé, cliquez sur **Suivant**.
- Cliquez sur **Installer** dans la fenêtre de vérification de la configuration.

À la fin de l'installation, le serveur redémarre afin de finaliser l'installation. Le RODC est maintenant installé correctement.

- Démarrez une session en tant qu'**administrateur du domaine**.
- Ouvrez la console **Utilisateurs et ordinateurs Active Directory**.

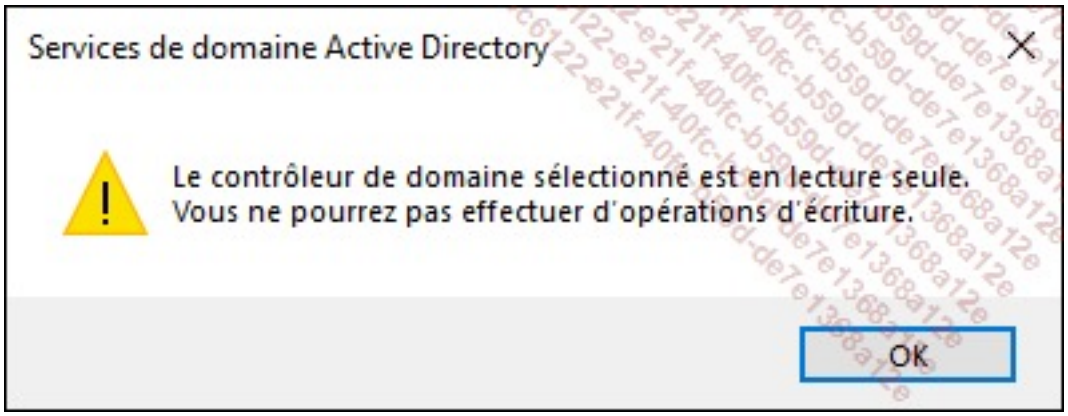



- Effectuez un clic droit sur le domaine puis un clic gauche sur **Changer de contrôleur de domaine**.
- Sélectionnez **AD2.Formation.local** puis cliquez sur **OK**.




Un message vous avertit que la connexion a été faite sur un RODC.

→ Cliquez sur **OK**.

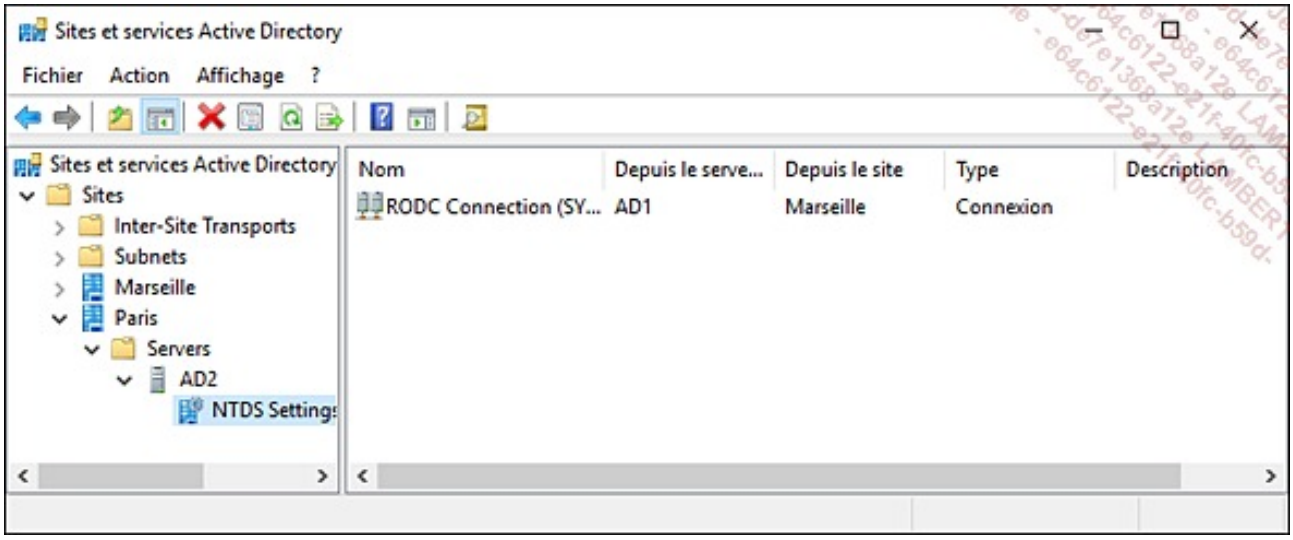



Il est impossible de créer un nouvel objet sur **AD2**.

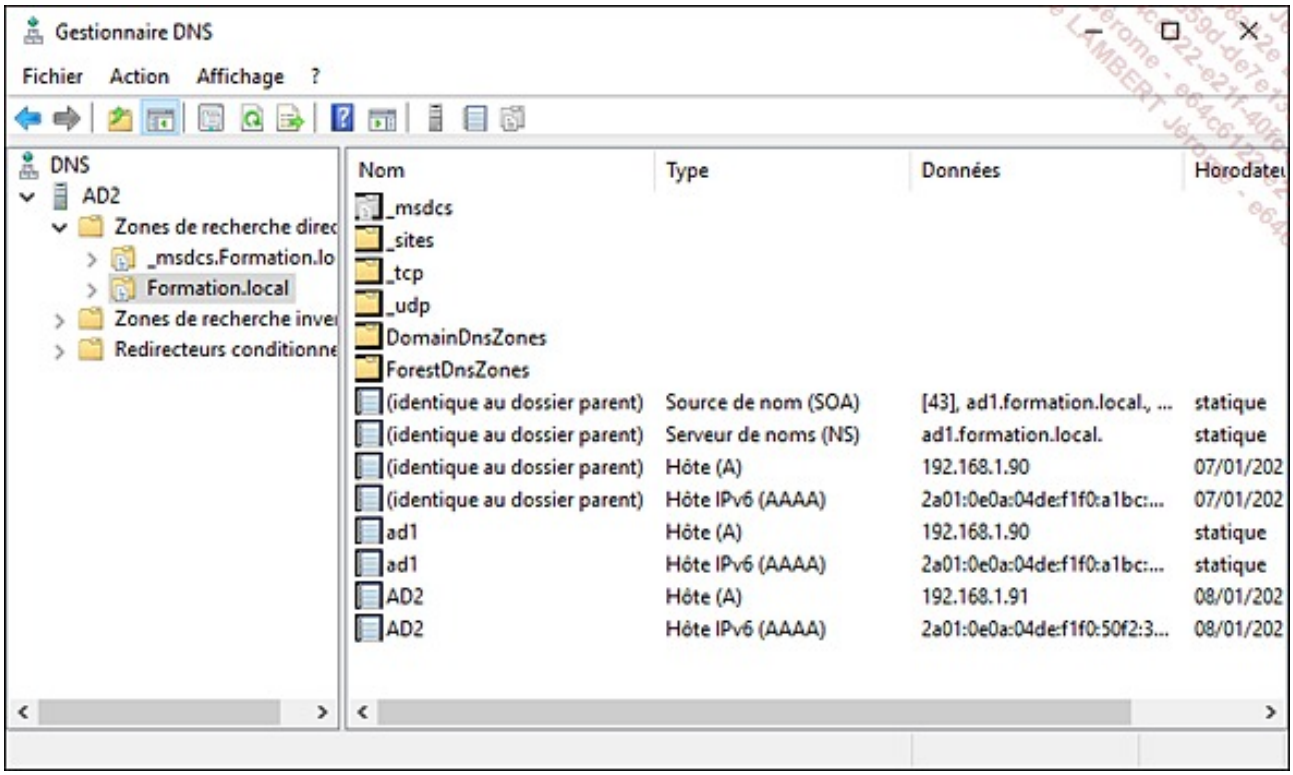
# 4. Vérifications à réaliser après l'installation d'un contrôleur de domaine

L'installation d'un contrôleur de domaine terminée, il peut être utile de vérifier les points suivants :

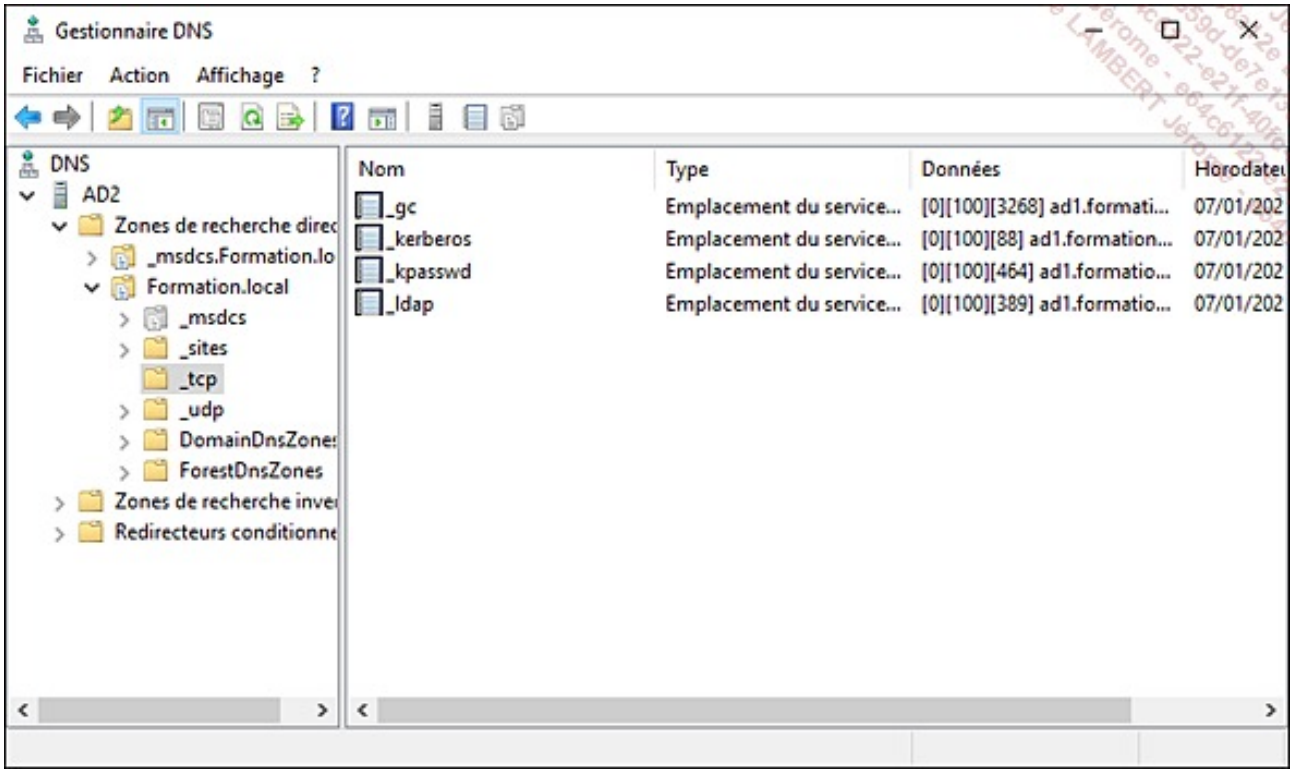
- La bonne configuration des sites AD.
- La configuration de la réplication intersites.
- L'association des sous-réseaux IP avec les bons sites.




- La bonne configuration de la zone DNS. Cette vérification peut être effectuée par l'intermédiaire de la console DNS.




- La présence des enregistrements de type SRV dans le DNS doit également être vérifiée.



- Exécutez la commande `dcdiag /test:replications` qui permet de s'assurer d'une bonne réplication entre AD1 et AD2.

Il est possible d'effectuer d'autres vérifications en fonction de l'architecture de votre réseau (plusieurs forêts avec des relations d'approbation entre elles, plusieurs domaines dans la forêt…).