

Présentation des services de l'Active Directory

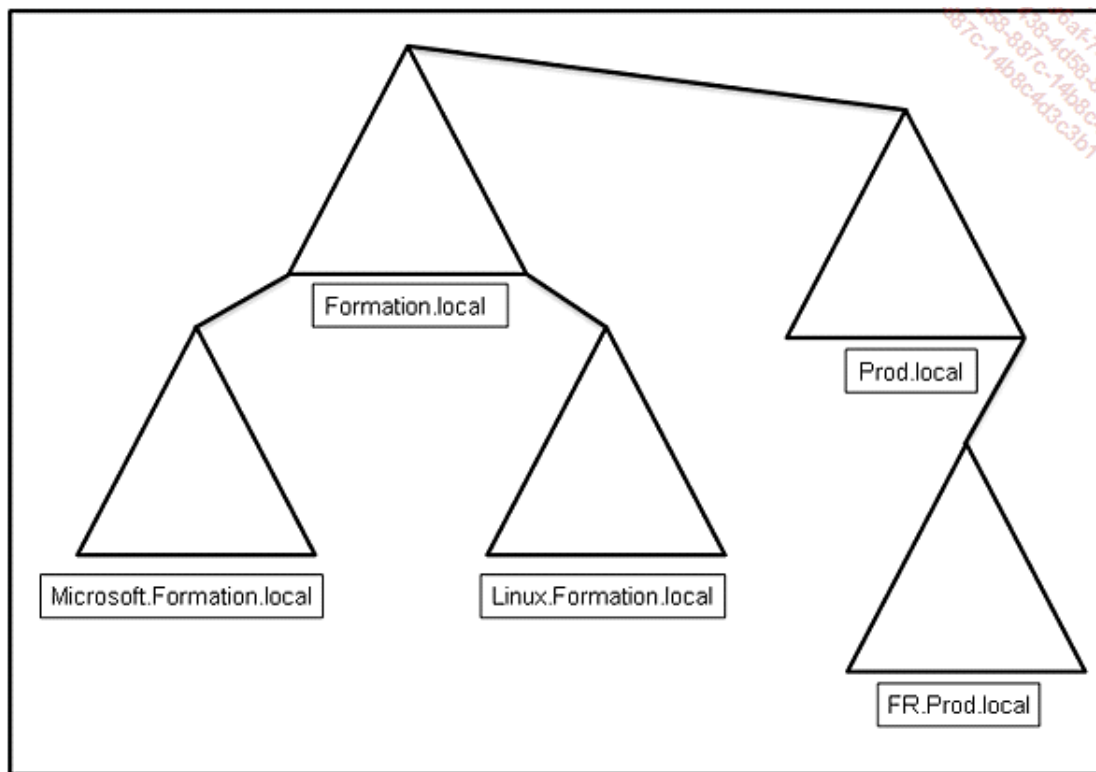
Active Directory est un annuaire implémenté sur les systèmes d'exploitation depuis Windows 2000 Server. Beaucoup d'améliorations ont été apportées depuis.

1. La forêt

Une forêt est une collection d'un ou plusieurs domaines Active Directory. Le premier domaine installé dans une forêt est appelé domaine racine, son nom DNS est le nom de la forêt. Une forêt contient une seule définition de la configuration du réseau et une seule instance du schéma de l'annuaire. Aucune donnée n'est répliquée en dehors de la forêt ; cette dernière sert de frontière de sécurité.

2. Le domaine et l'arborescence de domaine

Une arborescence de domaine est une suite de domaines qui partagent un espace de noms contigu. La relation entre les domaines d'une même arborescence est de type parent/enfant. Si l'espace de noms est différent, nous parlerons dans ce cas d'une nouvelle arborescence.



Le domaine représente une limite de sécurité et les utilisateurs sont définis par domaine. Ce dernier contient au moins un contrôleur de domaine, néanmoins il est recommandé d'en avoir deux. Un serveur ayant le rôle de contrôleur de domaine a la responsabilité de l'authentification dans un domaine AD.

3. L'unité d'organisation

Une **unité d'organisation (OU, Organizational Unit)** est un objet conteneur qui donne la possibilité de hiérarchiser Active Directory. Les objets sont ainsi regroupés pour l'application d'une GPO ou pour faciliter l'administration. Il est possible également de déléguer l'administration des objets contenus dans ce conteneur.

Depuis Windows Server 2008, il est possible de protéger la suppression accidentelle d'une OU. Par défaut lors de la création, la protection est activée, il faudra décocher la case **Protéger l'objet des suppressions accidentelles** dans l'onglet **Objet** des propriétés pour pouvoir supprimer une OU.

4. Les objets

Il est possible de trouver différents types d'objets Active Directory :

- **Utilisateur** : permet d'authentifier les utilisateurs physiques qui ouvrent une session sur le domaine. Des droits et permissions sont associés à ce compte afin de permettre l'accès à une ressource.
- **Groupe** : permet de rassembler différents objets qui ont le même accès sur une ressource. L'administration des permissions est plus aisée en utilisant des groupes.
- **Ordinateur** : permet d'authentifier les postes physiques connectés au domaine. Des droits et permissions lui sont associés afin de permettre l'accès à une ressource.
- **Unité d'organisation** : conteneur qui permet l'organisation des objets de façon hiérarchique. Il est possible de lui appliquer une ou plusieurs stratégies de groupe.
- **Imprimante** : une imprimante partagée peut être publiée dans Active Directory. Cette action simplifie la recherche et l'installation pour un utilisateur.
- **Dossier partagé** : comme pour les imprimantes, il est possible de publier des dossiers partagés dans AD.

5. Les partitions d'Active Directory

Active Directory utilise quatre types de partitions d'annuaire, ces dernières sont partagées par les contrôleurs de domaine :

- **Partition de domaine** : contient les informations sur les objets d'un domaine (attributs de compte utilisateur et attributs d'ordinateur...).
- **Partition de configuration** : permet de décrire la topologie de l'annuaire (liste complète des domaines, arborescences et forêt).
- **Partition de schéma** : contient tous les attributs et classes de tous les objets qui peuvent être créés.
- **Partition DNS** : contient la ou les bases de données DNS.

Ces partitions sont stockées dans la base de données et cette dernière est stockée dans le répertoire **%systemroot%\NTDS**.

6. Les maîtres d'opération FSMO

Cinq rôles **FSMO** (*Flexible Single Master Operation*) existent dans une forêt Active Directory. Deux rôles sont présents uniquement sur un des contrôleurs de domaine de la forêt, les trois autres sont attribués à un contrôleur de domaine par domaine.

- **Rôle maître de schéma** : seul un contrôleur de domaine dans la forêt dispose de ce rôle. L'administrateur a la possibilité de mettre à jour le schéma uniquement sur ce serveur. Les autres contrôleurs de domaine ont uniquement un accès en lecture sur le schéma.
- **Maître de dénomination de domaine** : lors de l'ajout ou de la suppression d'un domaine dans la forêt, ce serveur est contacté afin d'assurer la cohérence des noms de domaines. Seul un DC a ce rôle dans la forêt.

- **Maître RID** : un serveur par domaine possède ce rôle. Il a pour fonction d'allouer des **blocs d'identificateur relatifs (RID)** aux différents contrôleurs de domaine de son domaine. Le RID est utilisé lors de la création d'un objet pour créer le **SID (identifiant de sécurité)**. Ce dernier est construit en associant le RID à l'identificateur de domaine.
- **Maître infrastructure** : il a pour responsabilité de surveiller les objets des autres domaines de la forêt qui sont membres d'objet de son domaine.
- **Maître émulateur PDC** : ce rôle a été créé pour des raisons de compatibilité applicative. Il permet l'**émulation d'un serveur PDC**. Il a ainsi permis la migration entre Windows 2000 (utilisation de contrôleurs de domaine Active Directory) et Windows NT4 (utilisation de serveurs PDC et BDC). Son second rôle est la synchronisation de l'horloge pour l'ensemble du domaine.

7. Le catalogue global

Un serveur catalogue global est un contrôleur de domaine qui contient une copie des attributs de tous les objets Active Directory d'une forêt. Seuls certains attributs sont répliqués, ce choix s'effectuant au niveau de l'attribut et non de la classe.

La console Schéma Active Directory permet de sélectionner les attributs à répliquer.

Lors de l'authentification de l'utilisateur, le serveur catalogue global est interrogé, ceci afin de récupérer la liste des groupes universels dont l'utilisateur est membre. Le type de groupe est stocké dans le catalogue global et un nombre excessif alourdit la réplication.

8. Les sites AD

Les domaines sont découpés en sites AD, ces derniers représentant la topologie physique de l'entreprise. La connectivité réseau dans ce site est considérée comme très bonne, on parlera donc de réplication intrasite.

En créant ce découpage, une frontière de réplication est créée afin d'économiser la bande passante entre deux sites distants.

Lors de l'ouverture de session, le contrôleur de domaine du site AD sur lequel l'utilisateur est présent sera préféré mais si aucun serveur permettant l'authentification n'est présent, on tentera de réaliser cette dernière sur un autre site.

9. La réplication intrasite et la réplication intersite

La réplication permet de s'assurer qu'une modification effectuée sur un contrôleur de domaine est transmise aux autres serveurs responsables de l'authentification. Ces réplifications se font à l'aide d'objets de type « connexion » qui sont unidirectionnels (réplication entrante uniquement).

Par l'intermédiaire de ces chemins de réplication, la topologie va être automatiquement créée. Cette dernière assure la vérification de la cohérence des données (**KCC**, *Knowledge Consistency Checker*).

Ainsi, la topologie permet d'avoir une continuité au niveau de la réplication même en cas de défaillance d'un contrôleur de domaine. Elle permet aussi de s'assurer qu'il est impossible d'effectuer plus de trois sauts entre deux contrôleurs de domaine.

Il existe donc deux types de réplifications, l'intrasite et l'intersite.

La réplication intrasite permet une réplication des modifications pour les contrôleurs de domaine d'un même site.

À la suite d'une modification d'une des partitions Active Directory, le serveur notifie son premier partenaire du changement au bout de 15 secondes. Les autres partenaires sont ensuite avertis trois secondes plus tard. Ces délais de notifications initiales et ultérieures permettent la réduction du trafic réseau. Lors de la réception d'une notification, la modification est demandée et l'agent de réplication d'annuaire (**DRA**, *Directory Replication Agent*) effectue le transfert. Si aucune modification n'est effectuée, la méthode de scrutation est exécutée.

Cette méthode consiste à contacter un serveur afin de l'interroger si des changements ont été opérés sur une de ses partitions d'applications. Par défaut, l'intervalle de scrutation pour la réplication intrasite est d'une heure.

Entre les sites, les chemins sont créés à l'aide des liens de sites, ces derniers relient deux ou plusieurs sites.

L'**ISTG** (*Intersite Topology Generator*, générateur de topologie intersite) effectue la création d'objets de connexion entre les serveurs de chaque site, ceci afin de permettre la réplication intersite.

Les liens de sites peuvent être créés manuellement et un coût est donné afin de gérer les chemins prioritaires.

Dans chaque site, un contrôleur de domaine est sélectionné afin d'obtenir le rôle de tête de pont. Il permet d'effectuer la réplication vers un autre site Active Directory.

Pour effectuer la réplication intersite, deux protocoles sont utilisés :

- **IP** : utilisé pour toutes les réplifications intrasites et intersites, ce protocole est très souvent utilisé.
- **SMTP** : très utile en cas de connexions entre réseaux non fiables. Une CA (autorité de certification) est nécessaire, ce qui alourdit l'administration. Ce protocole est très peu utilisé pour la réplication.

10. Niveau fonctionnel du domaine et de la forêt

Un niveau fonctionnel active une ou plusieurs fonctionnalités à l'échelle d'un domaine ou d'une forêt. Il existe plusieurs niveaux fonctionnels mais l'opération qui consiste à faire monter le niveau fonctionnel est irréversible. Il est par la suite impossible de le faire redescendre.

Ceci a un impact sur le domaine ou la forêt, car il est nécessaire d'avoir au minimum tous les contrôleurs de domaine qui exécutent le système d'exploitation correspondant à celui du niveau fonctionnel choisi (si le niveau choisi est **Windows Server 2008**, les contrôleurs de domaine doivent au minimum exécuter **Windows Server 2008**).

Niveaux fonctionnels Windows Server 2003

Les contrôleurs de domaine doivent exécuter les systèmes d'exploitation Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2.

Le niveau fonctionnel de domaine Windows Server 2003 apporte :

- La disponibilité de l'outil en ligne de commande **Netdom**.
- La mise à jour de l'attribut **lastLogonTimestamp** (horodateur d'ouverture de session) avec l'heure de la dernière heure d'ouverture de session de l'utilisateur ou de l'ordinateur.
- La définition de l'attribut userPassword pour les objets Active Directory **inetOrgPerson** et **utilisateurs**.
- La redirection des dossiers systèmes Utilisateurs et ordinateurs dans un autre conteneur.
- L'utilisation de l'authentification sélective lors de la mise en place d'approbations.

Le niveau fonctionnel de forêt Windows Server 2003 permet lui :

- La mise en place d'approbations de forêts.
- La possibilité de changer le nom d'un domaine.
- Le déploiement d'un contrôleur de domaine en lecture seule Windows Server 2008 (**RODC**).

Niveaux fonctionnels Windows Server 2008

En augmentant le niveau fonctionnel du domaine, les fonctionnalités suivantes sont activées :

- Activation de la réplication du système de fichiers **DFS** (*Distributed File System*) pour le dossier **SYSVOL**.
- Protocole AES (*Advanced Encryption Services*) 128 et 256 bits pour l'authentification Kerberos.
- Mise en place de la stratégie de mot de passe affinée.

Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

Niveaux fonctionnels Windows Server 2008 R2

Le niveau fonctionnel permet l'utilisation de la **corbeille AD**. Cette dernière assure la restauration d'un objet Active Directory (unité d'organisation, compte utilisateur...). L'ensemble des propriétés est restauré.

Niveaux fonctionnel Windows Server 2012 R2

Ce niveau fonctionnel n'apporte pas de nouveautés à l'exception de l'ajout de la stratégie de modèles d'administration du centre de distribution de clés.

Promotion d'un contrôleur de domaine

Un contrôleur de domaine est un serveur chargé d'authentifier et de permettre l'accès aux ressources pour les utilisateurs.

1. Pré-requis nécessaire à la promotion d'un serveur

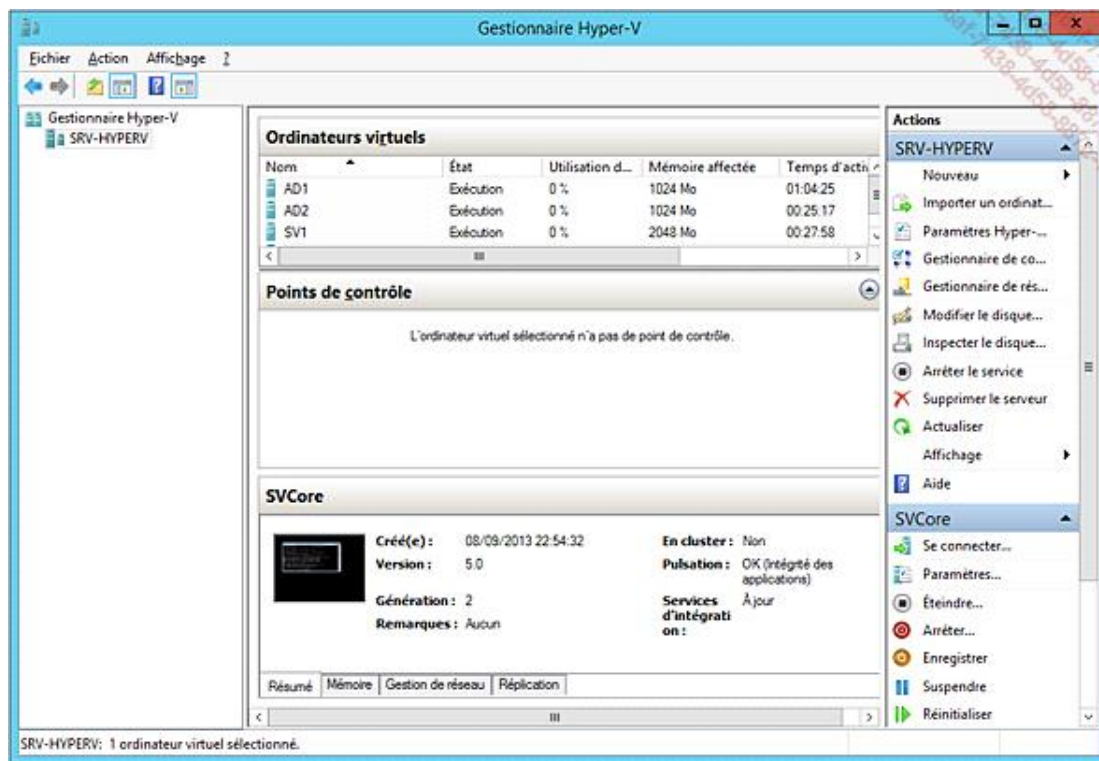
La promotion d'un serveur en contrôleur de domaine nécessite certains pré-requis. L'assistant d'installation s'arrête s'ils ne sont pas respectés.

- **Système de fichiers NTFS** : les volumes et partitions doivent être formatés avec un système de fichiers NTFS.
- **Nom du poste** : les spécifications DNS doivent être respectées pour le nom du poste. Néanmoins un nom de 15 caractères maximum est recommandé. Il est préférable de ne pas utiliser de caractères spéciaux (#, é, è...) dans le nom du poste, les chiffres et 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, .local...). L'enregistrement du domaine public est toutefois important et doit être fait chez les organismes gérant ce genre de noms.
- **Serveur DNS** : un serveur DNS est nécessaire pour l'installation 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 du serveur afin qu'il puisse contacter son serveur DNS.

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.

- Ouvrez la console **Gestionnaire Hyper-V**.
- Effectuez un clic droit sur la machine **AD1** et sélectionnez **Démarrer**.

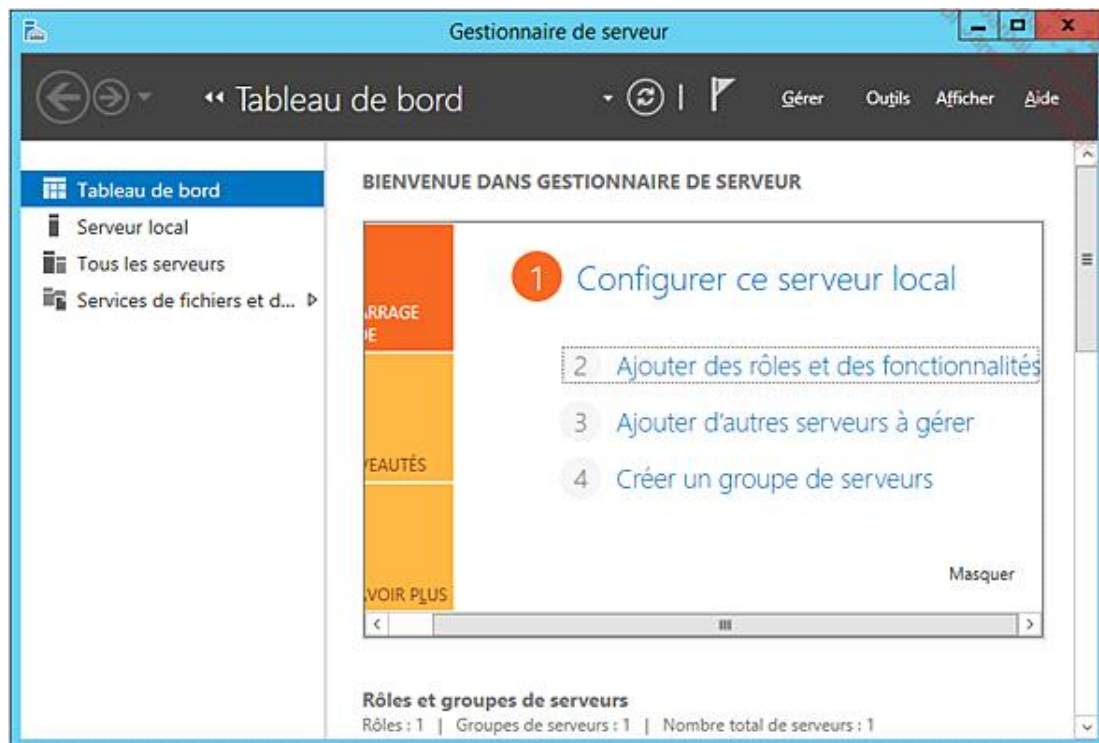


- Double cliquez sur la machine afin de vous y connecter.
- Cliquez sur la première icône afin d'envoyer à la VM la séquence de touches [Ctrl][Alt][Suppr].

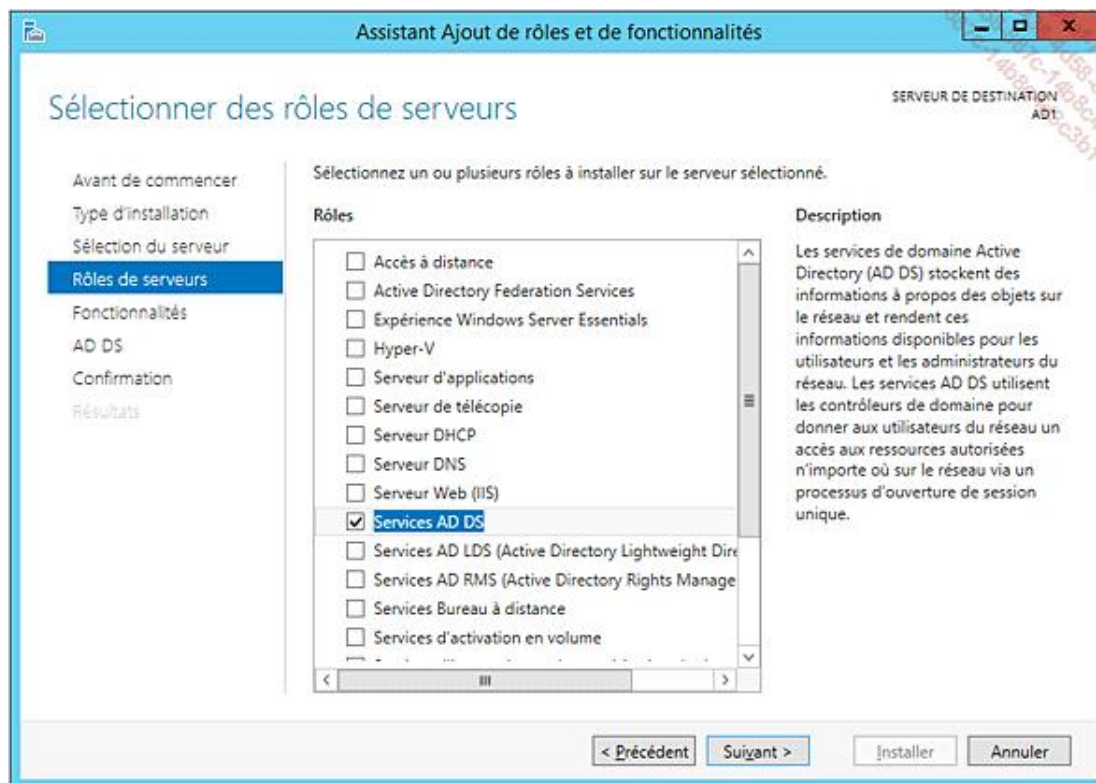


La configuration ayant déjà été faite, il suffit maintenant d'installer Active Directory.

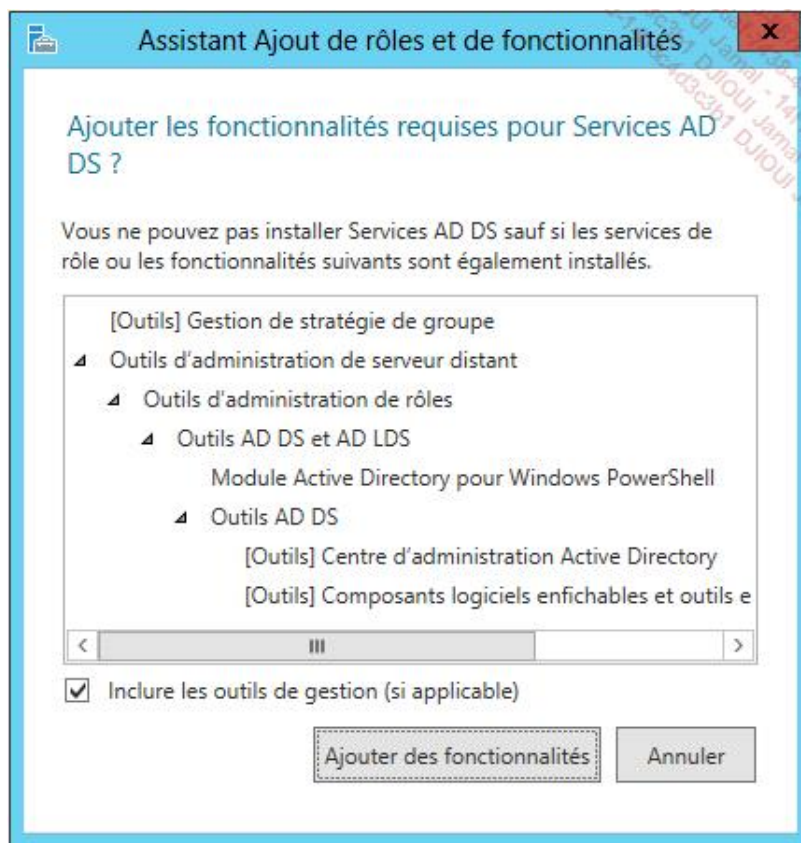
- Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.



- L'assistant se lance. Cliquez sur **Suivant**.
- Cliquez sur **Installation basée sur un rôle ou une fonctionnalité**.
- Dans la fenêtre **Sélectionner le serveur de destination**, laissez le paramètre par défaut puis cliquez sur **Suivant**.
- Activez la case à cocher **Services AD DS** pour effectuer l'installation.



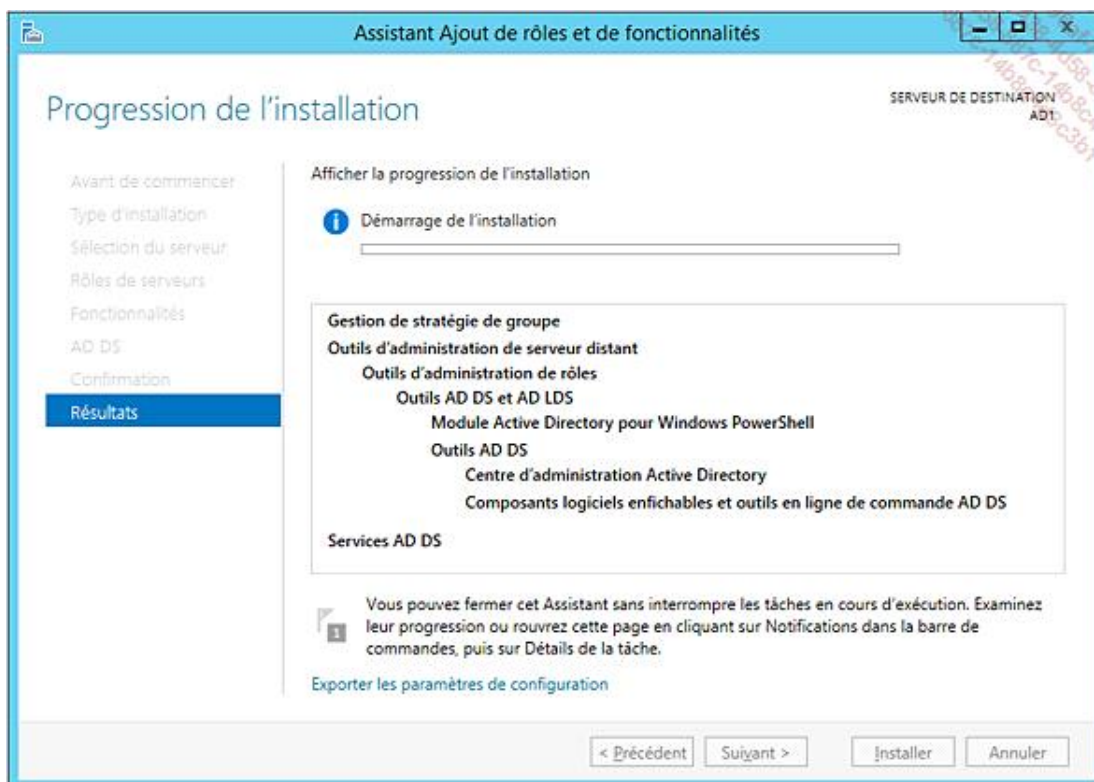
- Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche, afin d'installer les fonctionnalités nécessaires à Active Directory.



→ Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités** puis cliquez sur **Suivant**.

→ Cliquez sur **Installer** pour lancer l'installation.

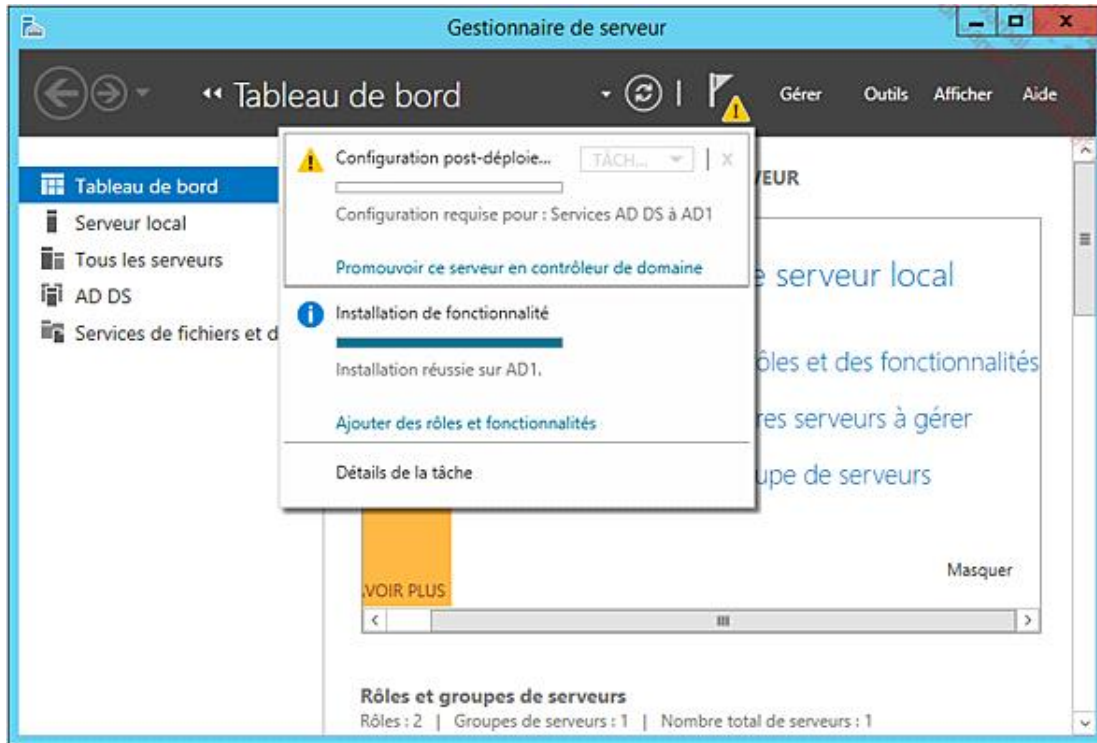
L'installation est en cours...



→ Une fois l'installation terminée, cliquez sur **Fermer**.

→ Dans le **Gestionnaire de serveur**, cliquez sur le drapeau contenant le point d'exclamation.

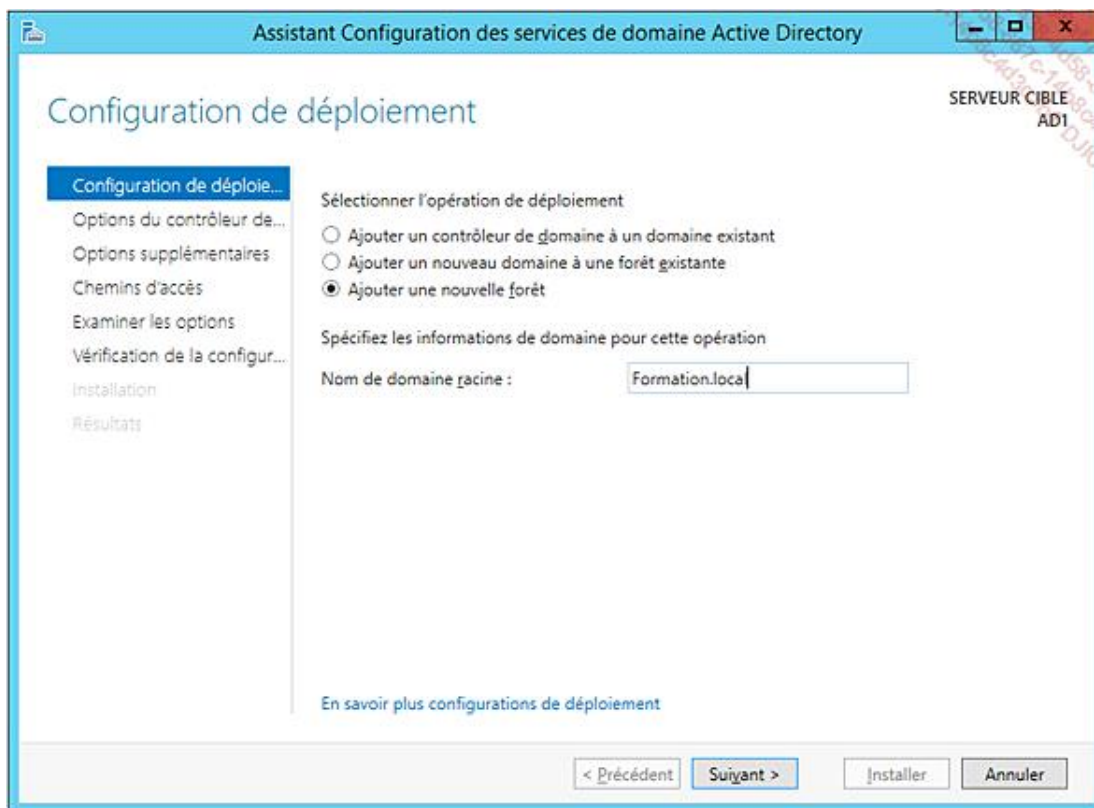
→ Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



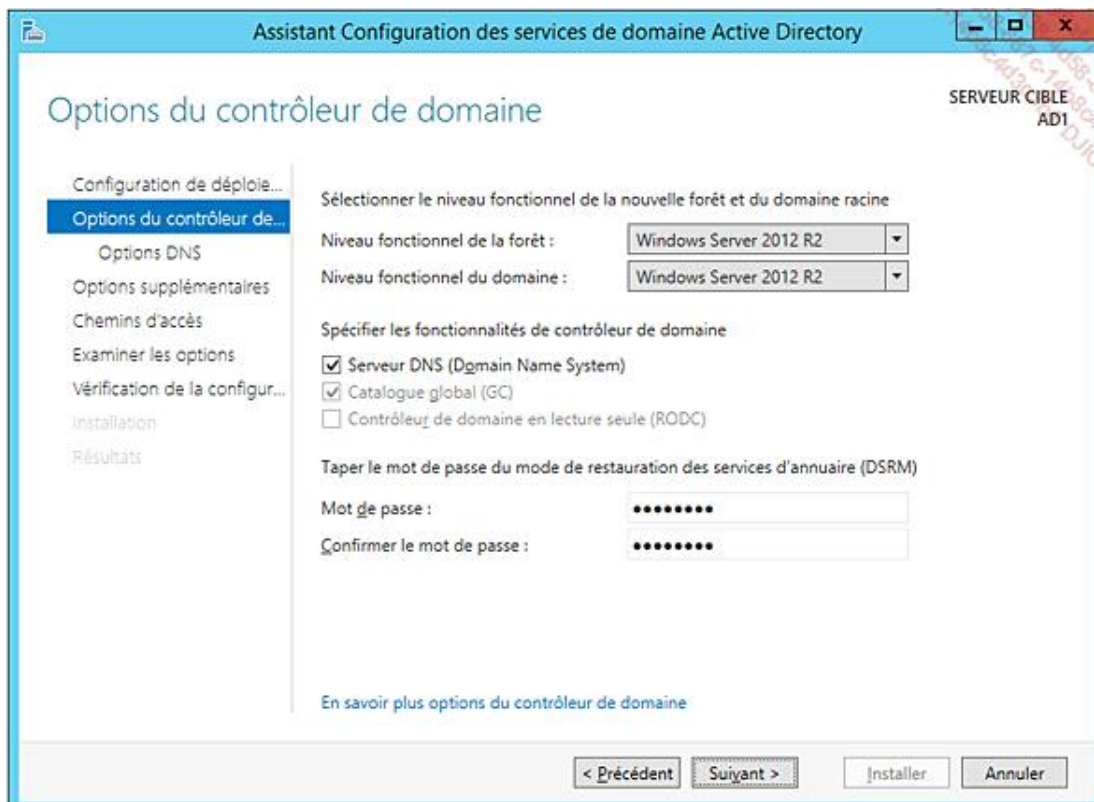
Trois options sont possibles :

- **Ajouter un contrôleur de domaine à un domaine existant** : un contrôleur de domaine est ajouté au domaine 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.
- **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 **Nom de domaine racine**.



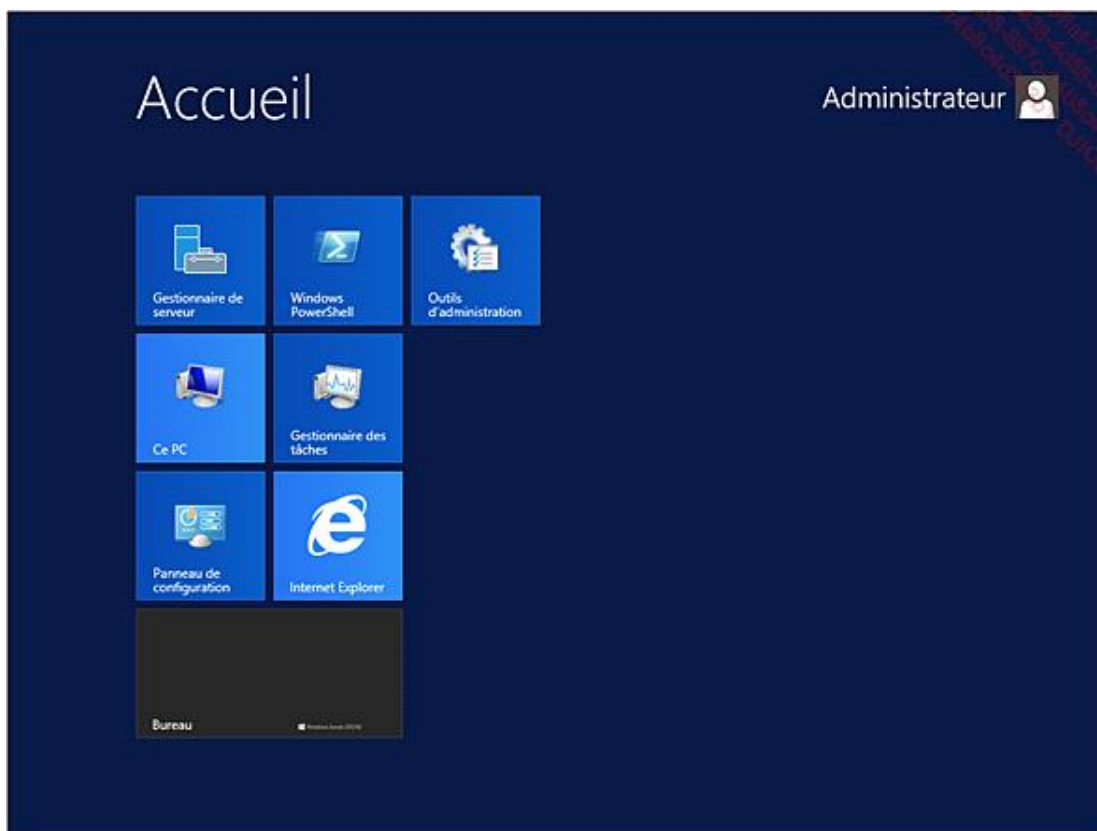
- Cliquez sur **Suivant** pour valider votre choix.
- Sélectionnez le niveau fonctionnel **Windows Server 2012 R2** et laissez cochée la case **Serveur DNS** afin que le rôle soit installé et configuré.
- Saisissez **Pa\$\$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**.



- Dans la fenêtre **Options DNS**, cliquez sur **Suivant**.
- Après quelques recherches, 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 l'interface Windows 8, puis cliquez sur **Outils d'administration**.



De nouvelles consoles sont disponibles dans **Outils d'administration**. 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.
- **Domaines et approbations AD** : création de relation 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 problème en cas d'altération de la base de données ou en cas de mauvaise modification.

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 donne la possibilité à un administrateur d'installer un contrôleur de domaine en lecture seule. Il sera impossible d'effectuer des modifications sur ce dernier : les modifications sont apportées à un contrôleur de domaine en lecture/écriture et par réplication au **RODC**.

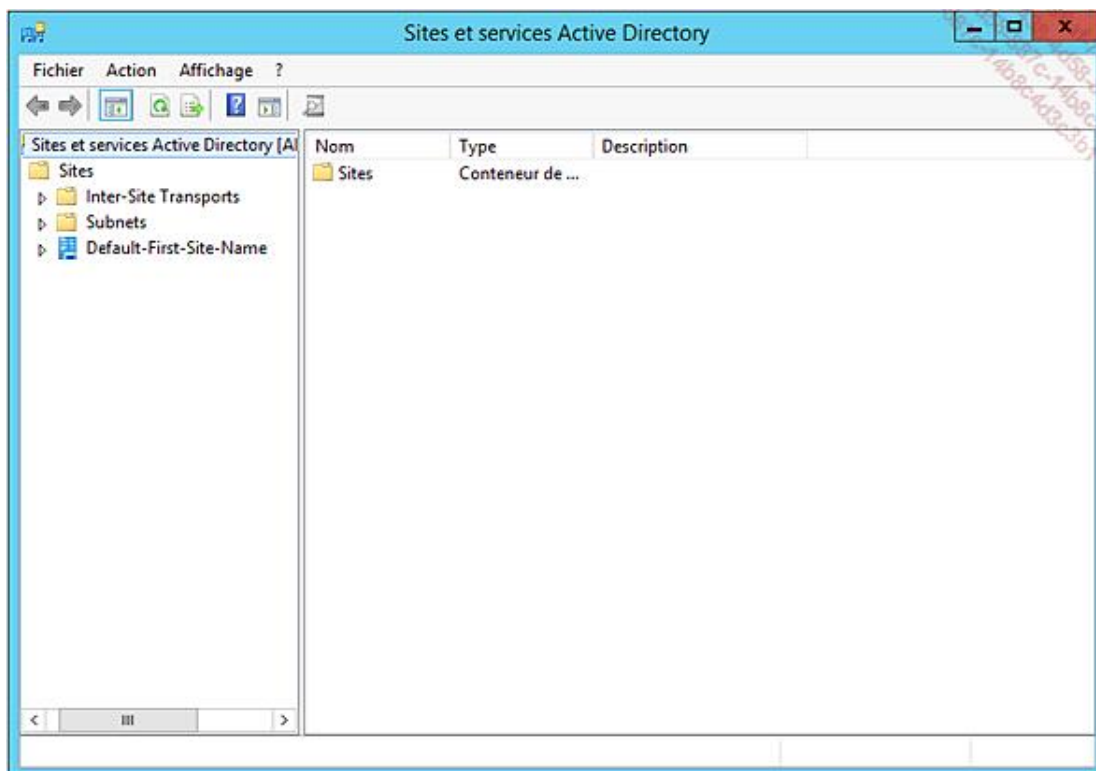
Il est également possible de se connecter en local à un **RODC**. Une délégation peut donc être donnée à un autre utilisateur pour l'administration du serveur (mise à jour Windows Update...) sans que celui-ci ne soit **administrateur du domaine**.

Néanmoins, certains pré-requis sont à respecter :

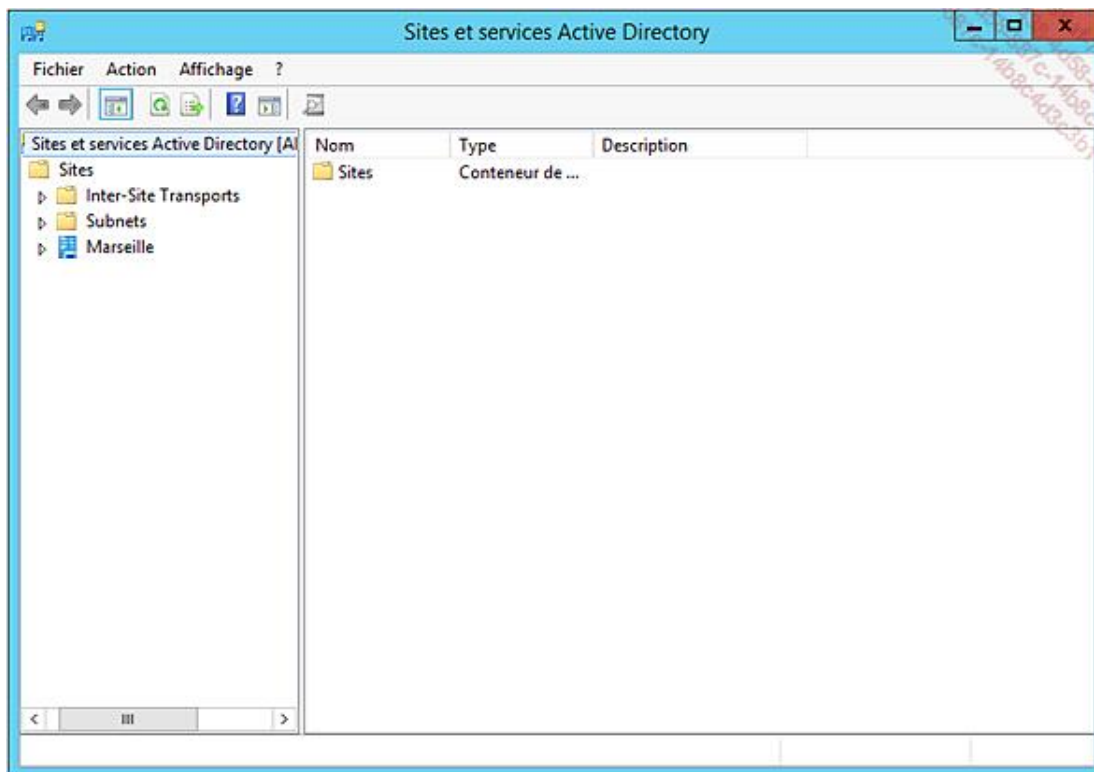
- **Niveau fonctionnel** : Windows Server 2003 ou supérieur pour la forêt et le domaine.
- **Schéma** : l'extension du schéma doit être effectuée afin d'accueillir la fonctionnalité **RODC**.
- **Contrôleur de domaine** : un contrôleur de domaine en lecture/écriture sous Windows Server 2008 ou supérieur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

➤ L'installation d'un **RODC** (*Read Only Domain Controller*, contrôleur de domaine en lecture seule) s'effectue souvent sur des sites distants. Ainsi, nous allons en premier lieu 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.

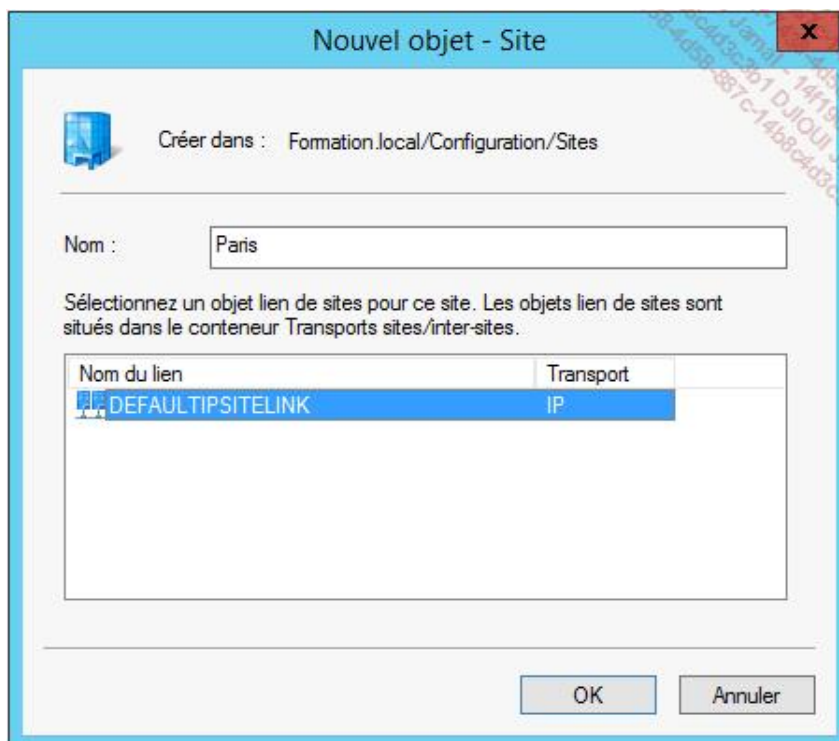
➔ Ouvrez **AD1**, puis lancez via l'interface Windows la console **Sites et services Active Directory**.



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

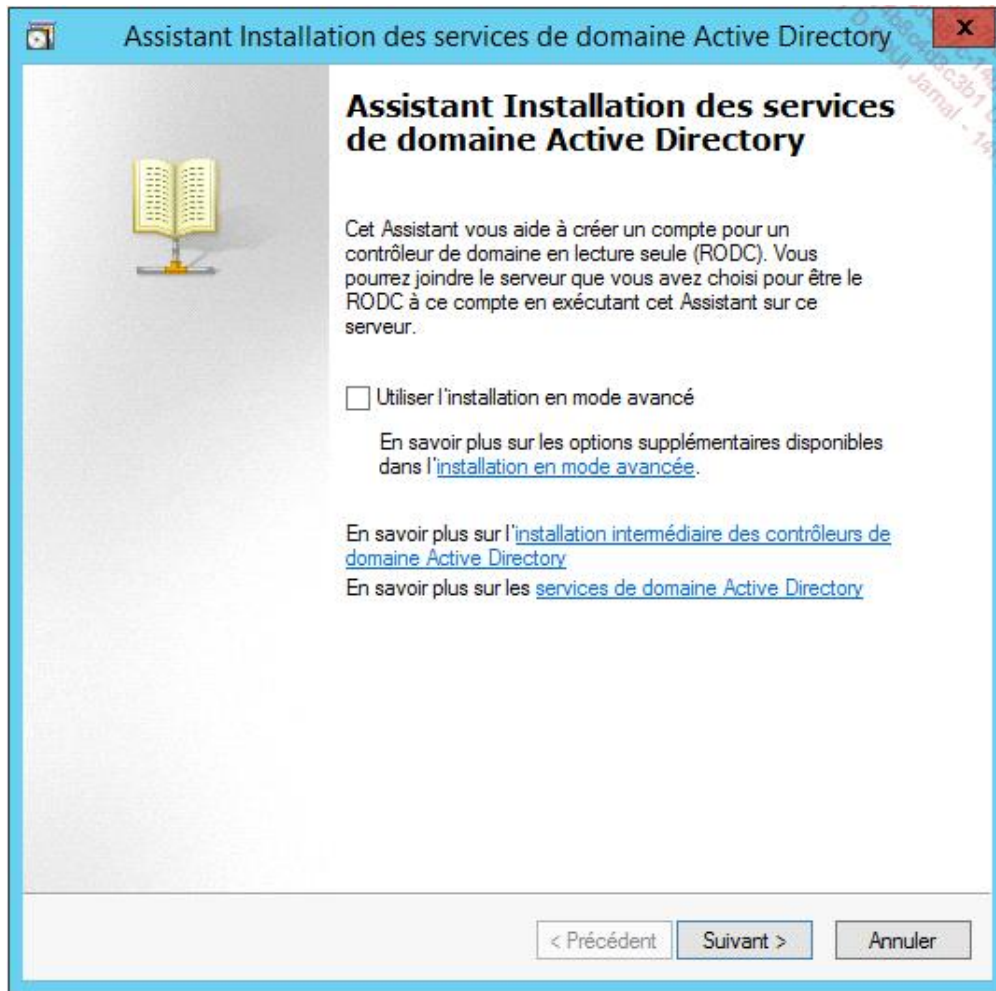


- Effectuez un clic droit sur le dossier **Sites** et sélectionnez **Nouveau Site**.
- Dans le champ **Nom**, saisissez **Paris** et sélectionnez **DEFAULTIPSITELINK**.






➔ Le RODC est placé sur le site de Paris. Il est donc nécessaire de le créer en amont.

- ➔ Cliquez sur **OK** au message d'information.
- ➔ Depuis l'interface Windows 8, ouvrez **Utilisateurs et ordinateurs Active Directory**.
- ➔ Effectuez un clic droit sur l'OU **Domain Controllers** 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 doit être sorti du domaine et son compte supprimé, sinon un message vous avertit qu'un compte existe déjà.

 Assistant Installation des services de domaine Active Directory 

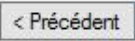
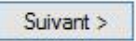
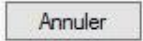
Spécifiez le nom de l'ordinateur 

Spécifiez le nom de l'ordinateur qui sera le contrôleur de domaine en lecture seule (RODC). Ce compte sera créé dans les services de domaine Active Directory.

 Pour que le serveur soit joint au compte que vous créez et qu'il devienne un contrôleur de domaine en lecture seule, il doit être nommé d'après le nom que vous précisez ici. Le serveur ne doit pas être joint au domaine avant que vous installiez les services de domaine Active Directory sur ce premier.

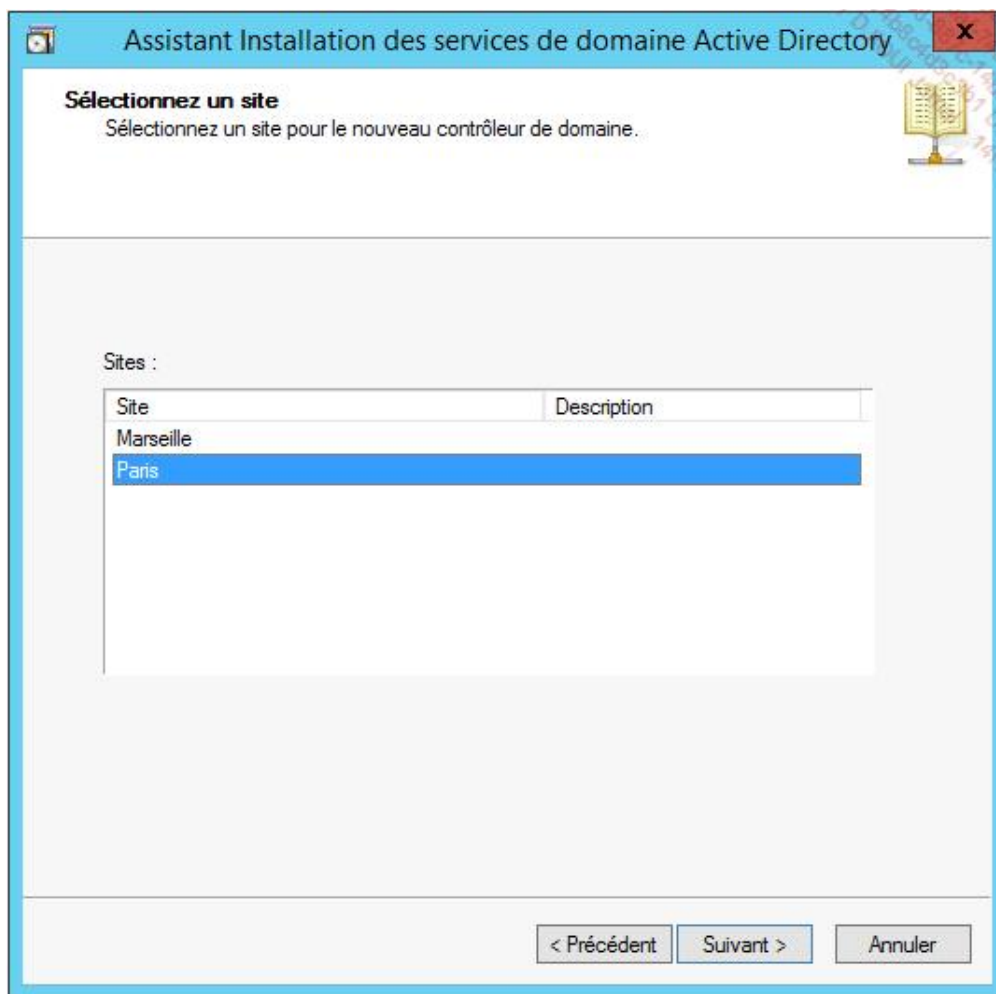
Nom de l'ordinateur :

Nom d'ordinateur DNS complet :

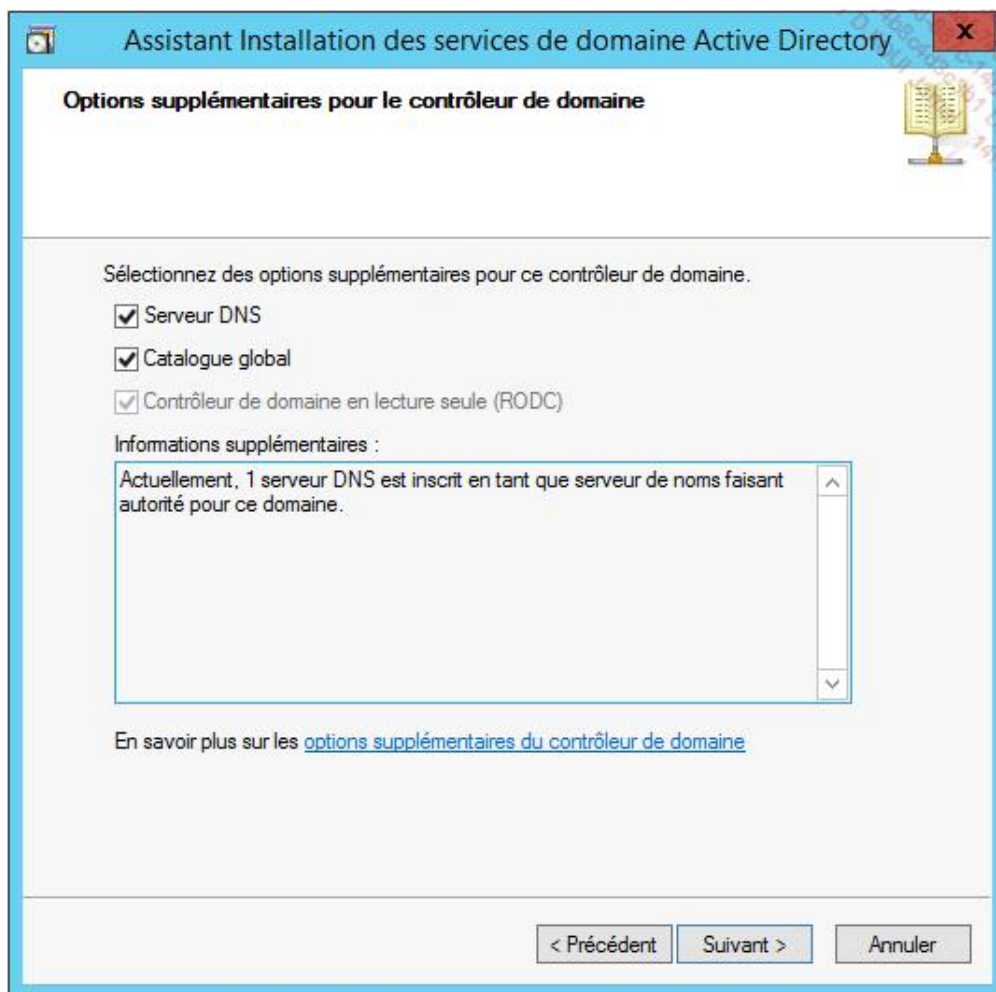
 Il est très important de mettre le nom exact du futur RODC.

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

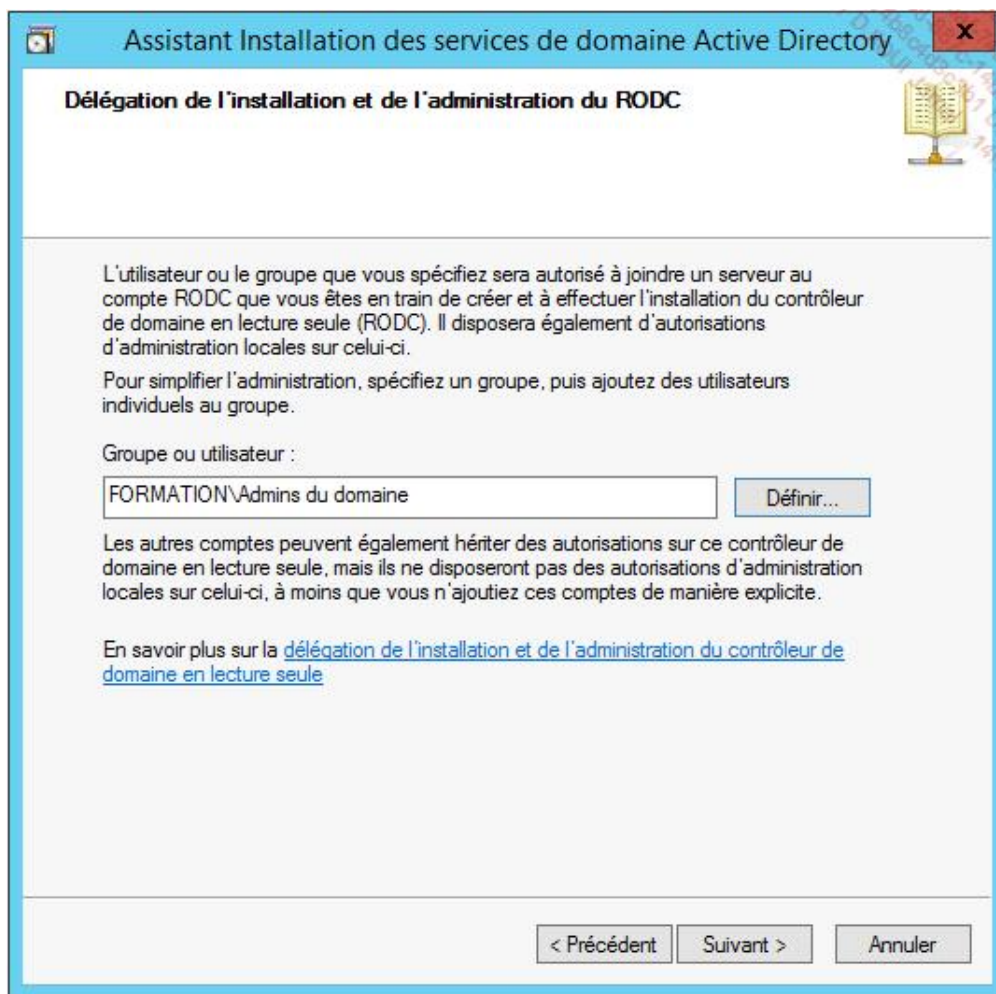


→ Attendez la fin de l'analyse de la configuration DNS. À l'aide de la fenêtre suivante, il est possible d'effectuer plusieurs choix :

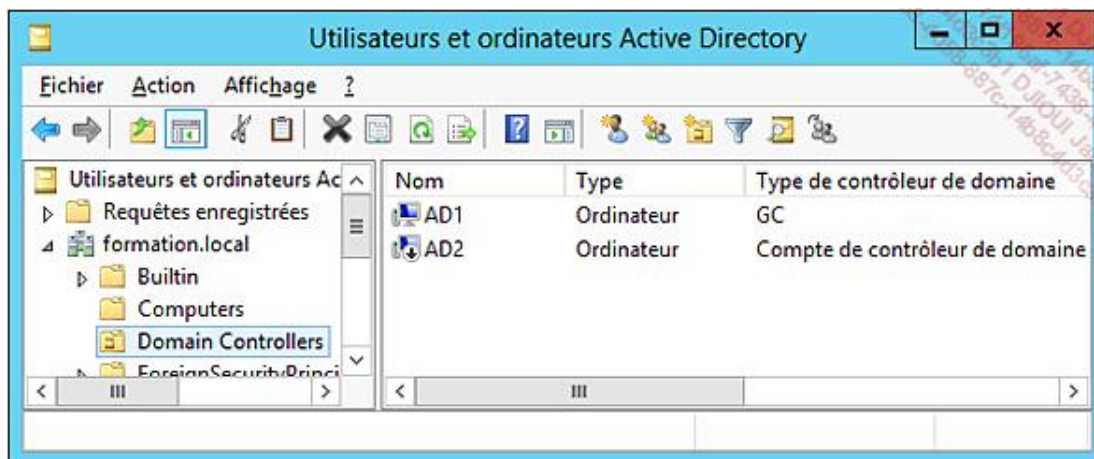
- **Serveur DNS** : installation d'un serveur DNS en mode lecture seule.
- **Catalogue global** : le serveur installé aura le rôle de catalogue global.
- **Serveur RODC** : le contrôleur de domaine installé est un **RODC** et non un serveur avec des droits de lecture/écriture dans Active Directory.



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**.



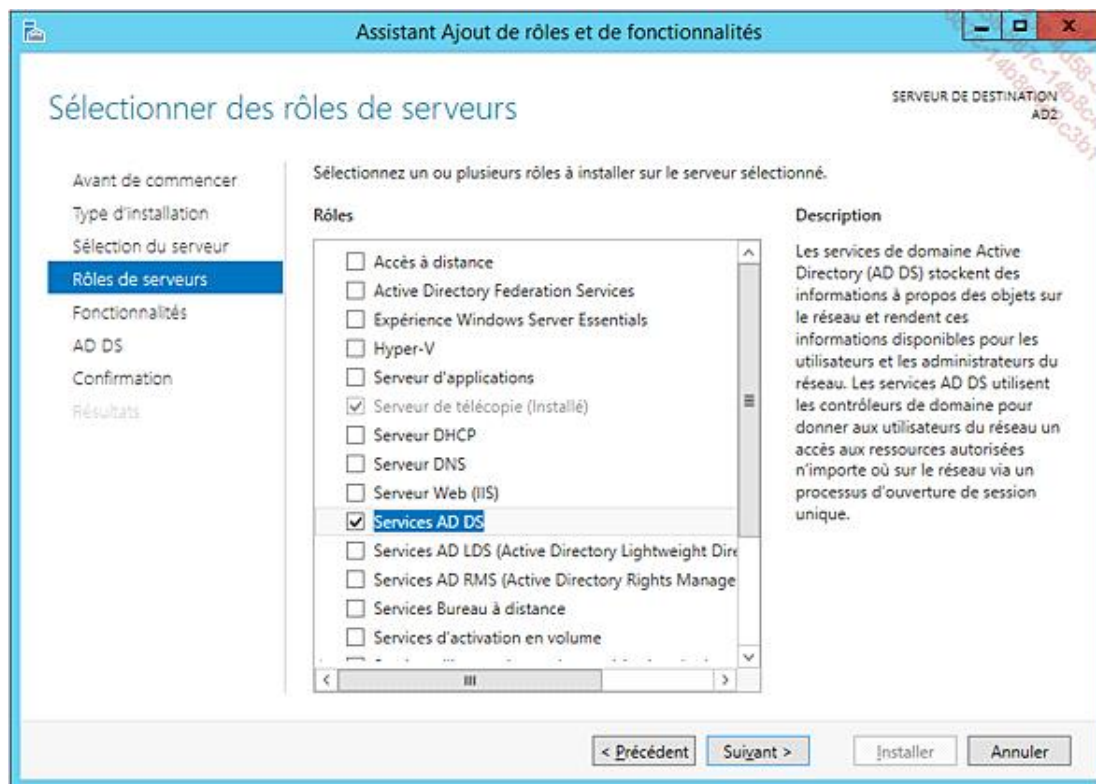
→ Dans la fenêtre de résumé, cliquez sur **Suivant** puis sur **Terminer**. Le compte de la machine apparaît avec l'état désactivé.



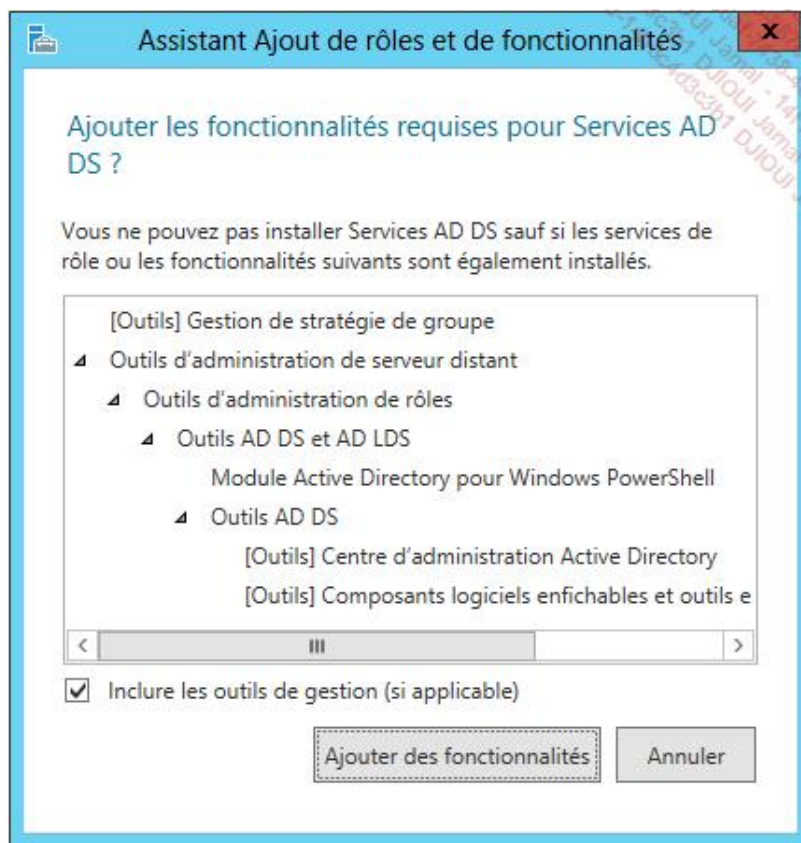
Le compte ayant été créé, la promotion peut maintenant être effectuée. La précréation peut évidemment ne pas être effectuée, dans ce cas le compte est créé lors de la promotion. Néanmoins, dans ce cas précis, la mise en place d'une délégation est impossible, il sera nécessaire de le faire à la suite de la promotion.

- 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**.



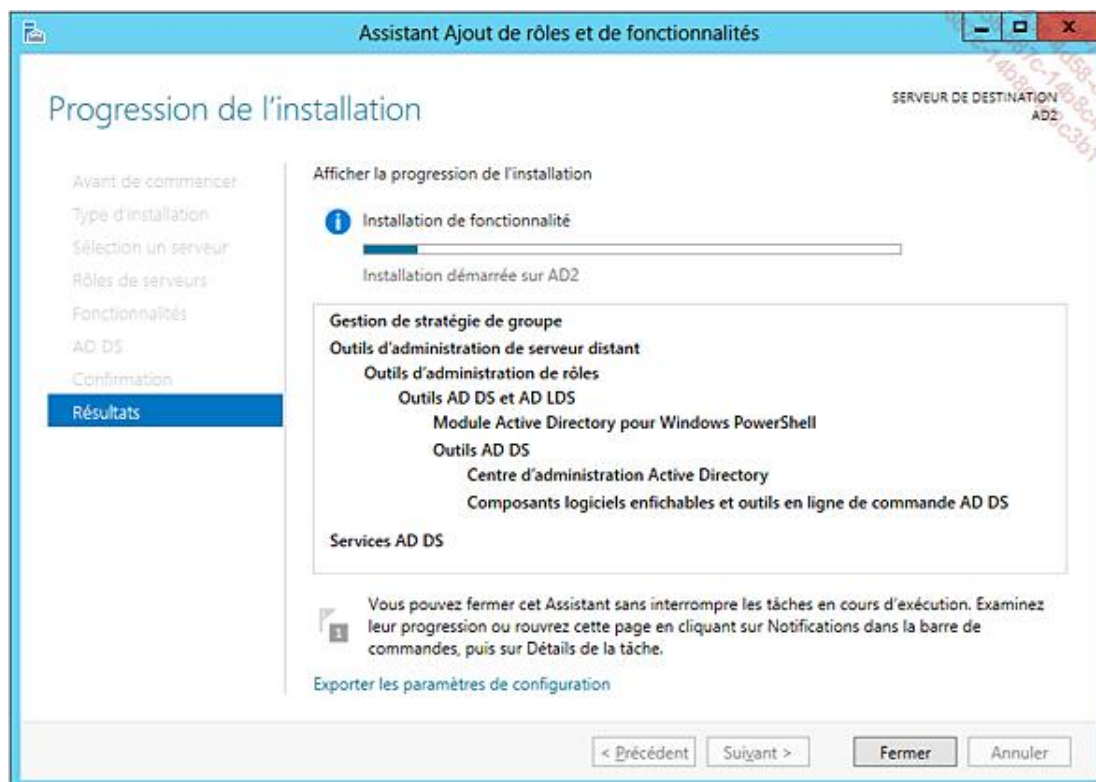
- Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche afin d'installer les fonctionnalités nécessaires à Active Directory.



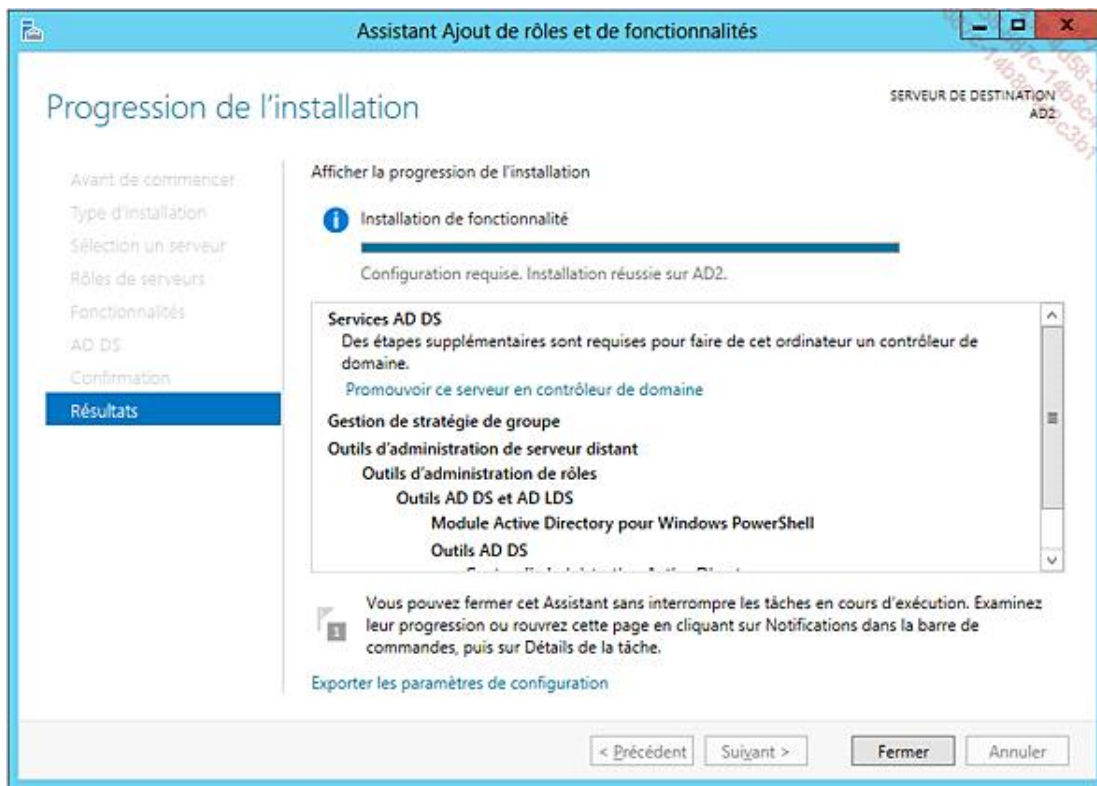
→ Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités**.

→ Cliquez sur **Installer** pour lancer l'installation.

L'installation est en cours...

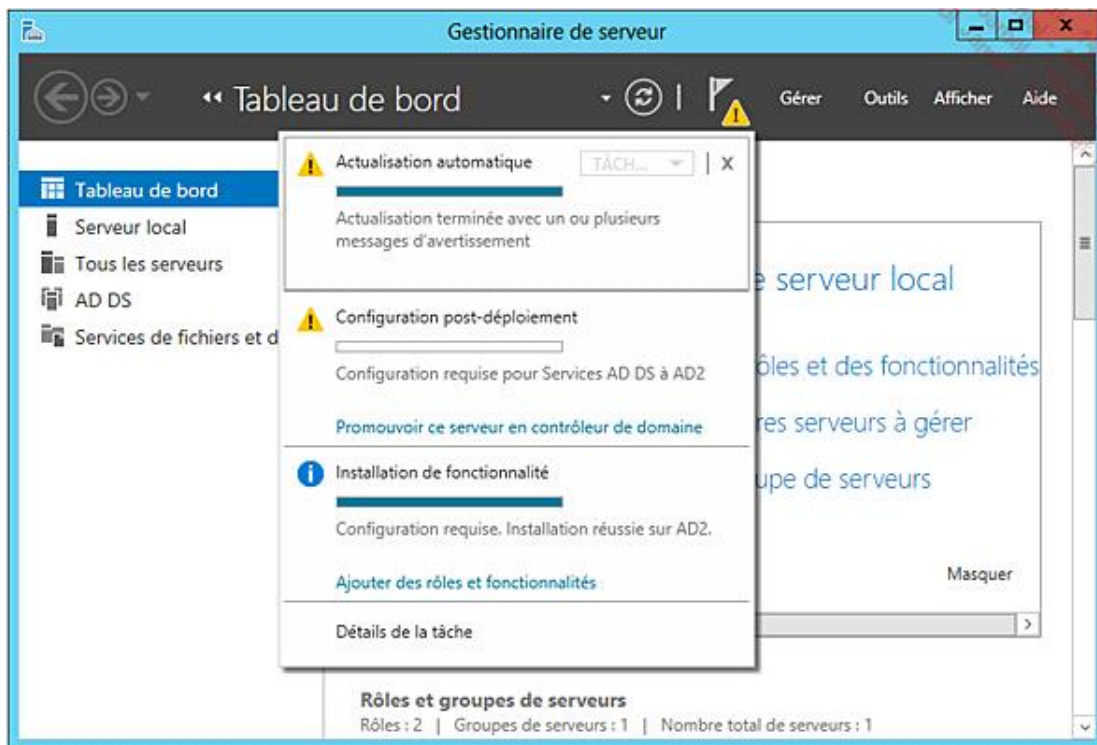


→ Une fois l'installation terminée, cliquez sur **Fermer**.

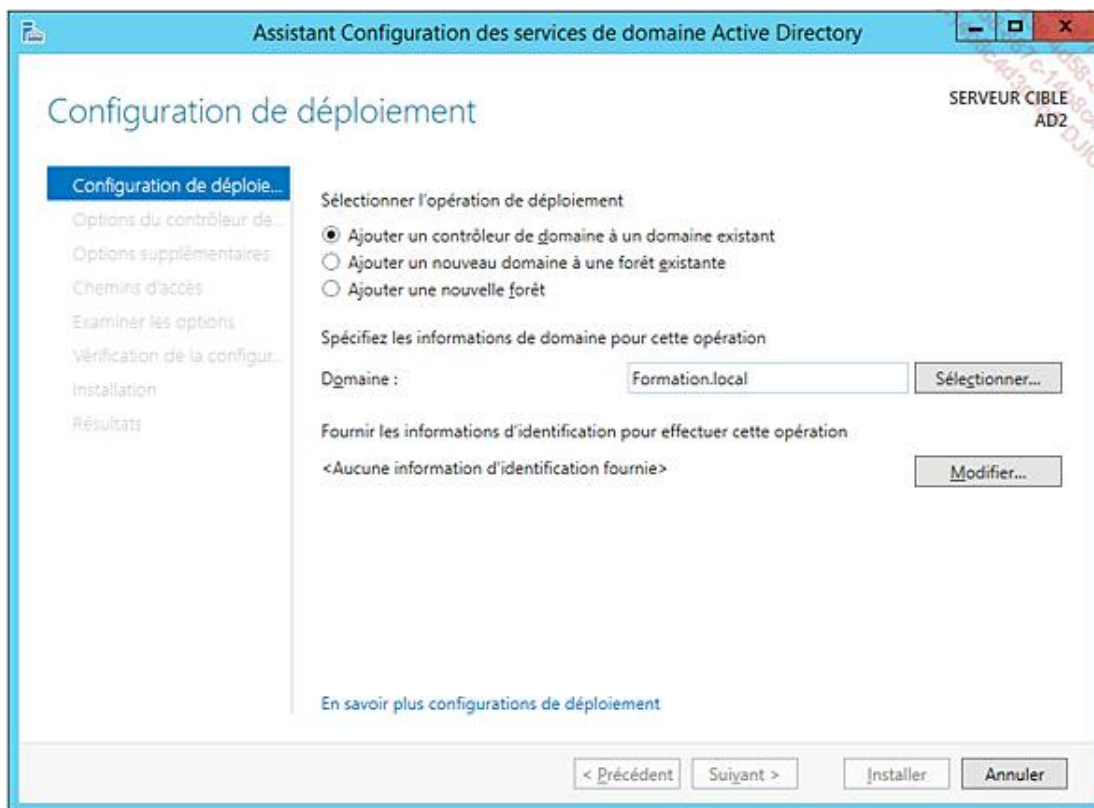


→ Dans le **Gestionnaire de serveur**, cliquez sur le drapeau contenant le point d'exclamation.

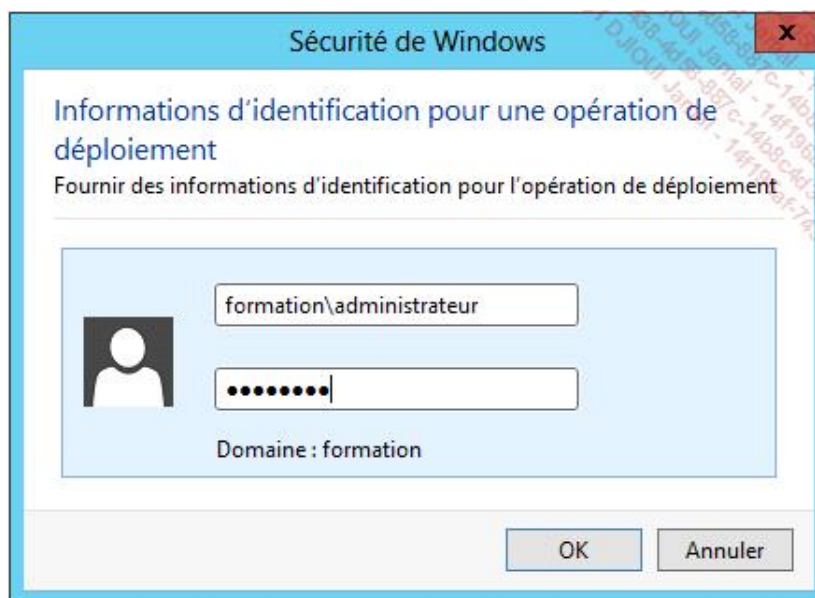
→ Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



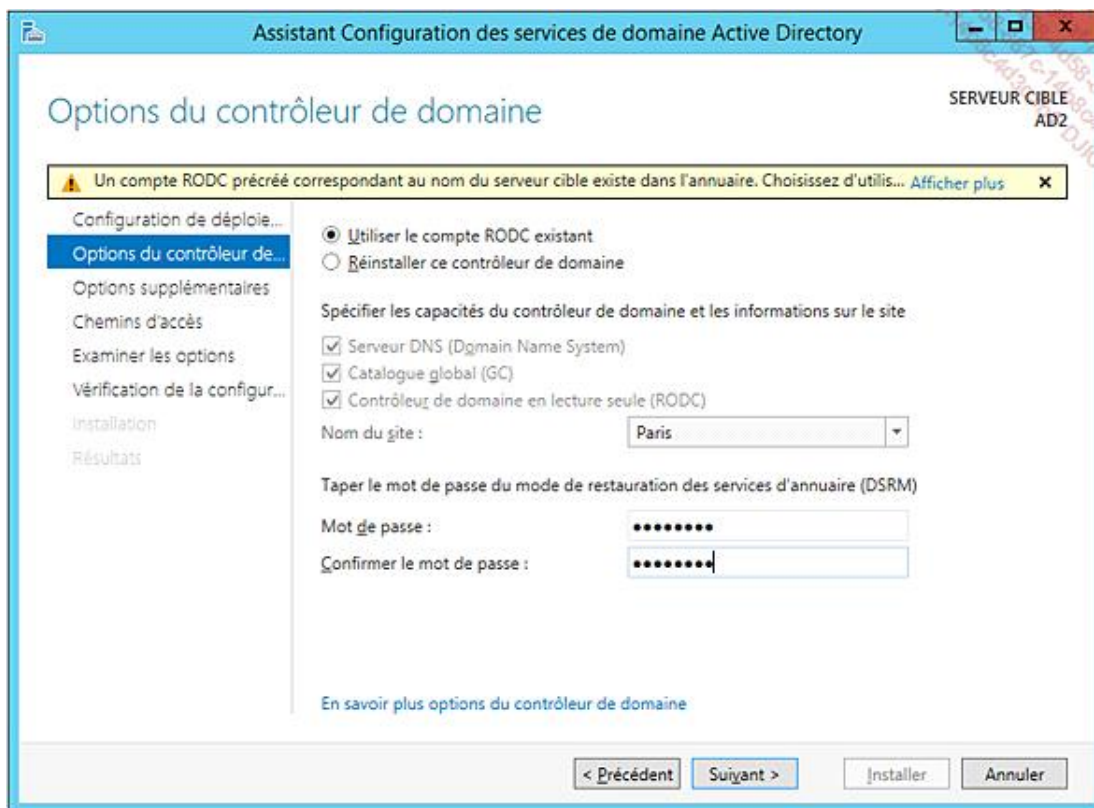
→ Cliquez sur **Ajouter un contrôleur de domaine à un domaine existant** et saisissez dans le champ **Domaine** le nom du domaine **formation.local**.



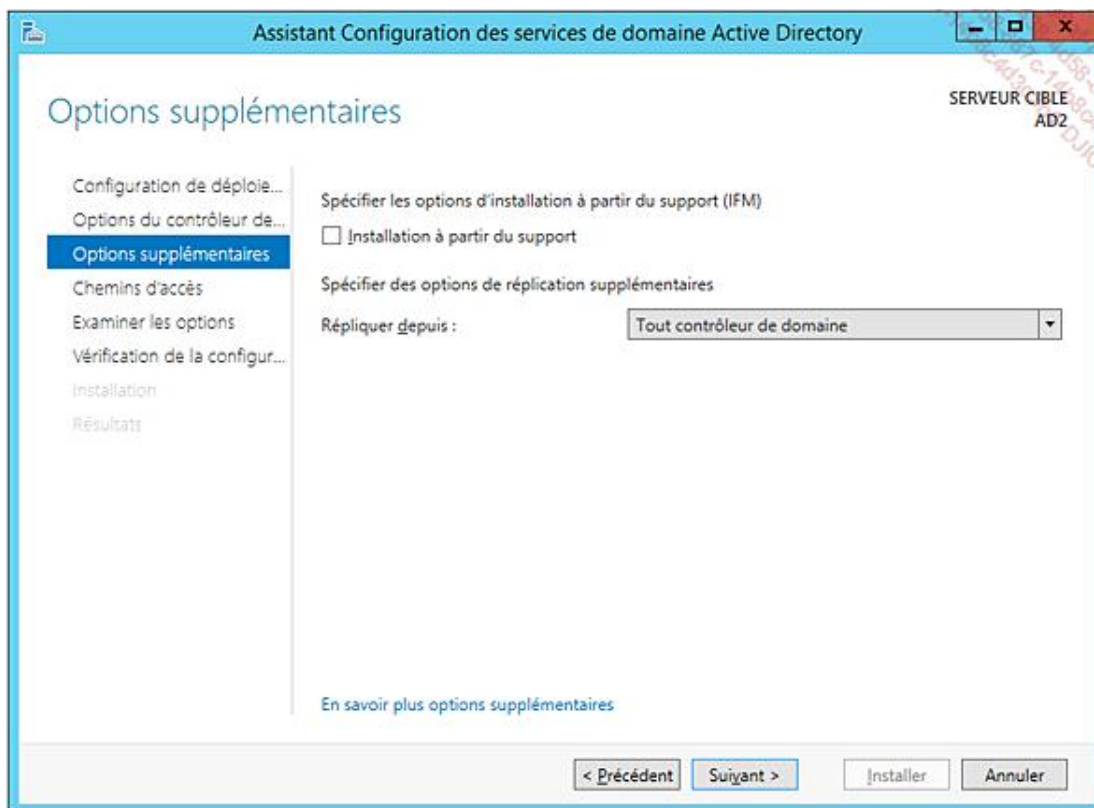
- Cliquez sur le bouton **Modifier** afin de saisir les informations d'identification.
- Saisissez **formation\administrateur** dans le champ du nom d'utilisateur ainsi que le mot de passe dans le champ adéquat.



- Cochez le bouton radio **Utiliser le compte RODC existant**.
- Saisissez **Pa\$\$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)** puis cliquez sur **Suivant**.



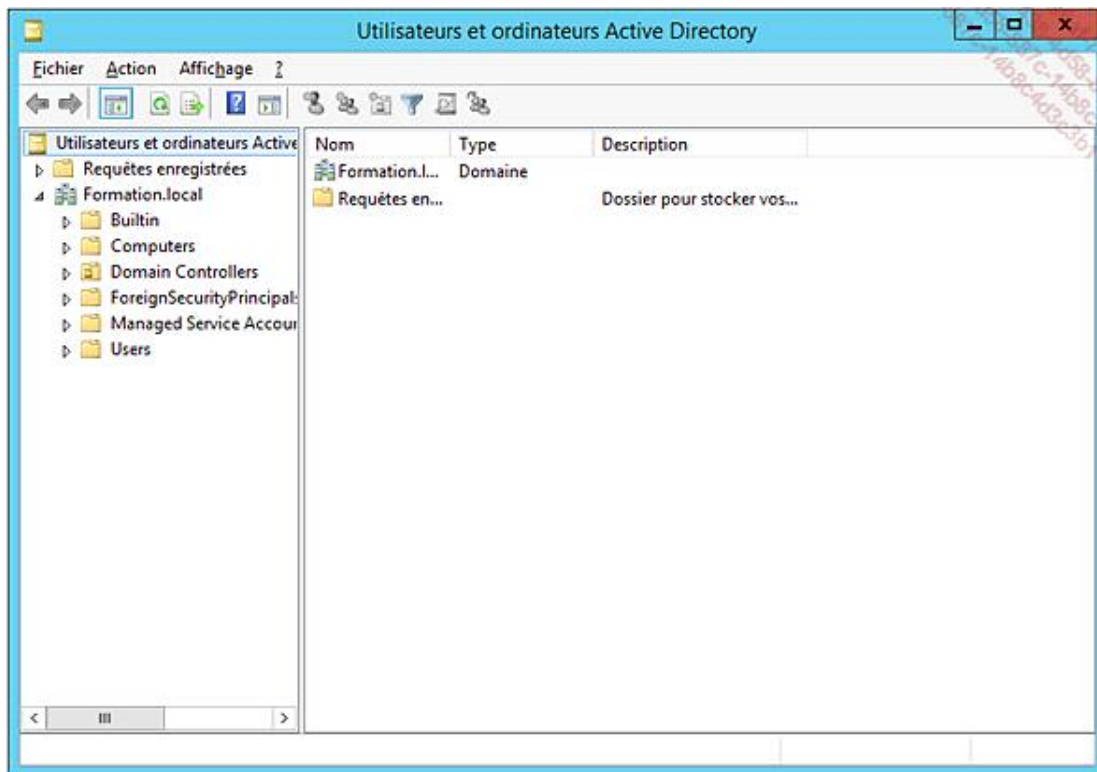
- Un seul contrôleur de domaine est présent, laissez les choix par défaut dans la fenêtre **Options supplémentaires** et cliquez sur **Suivant**.



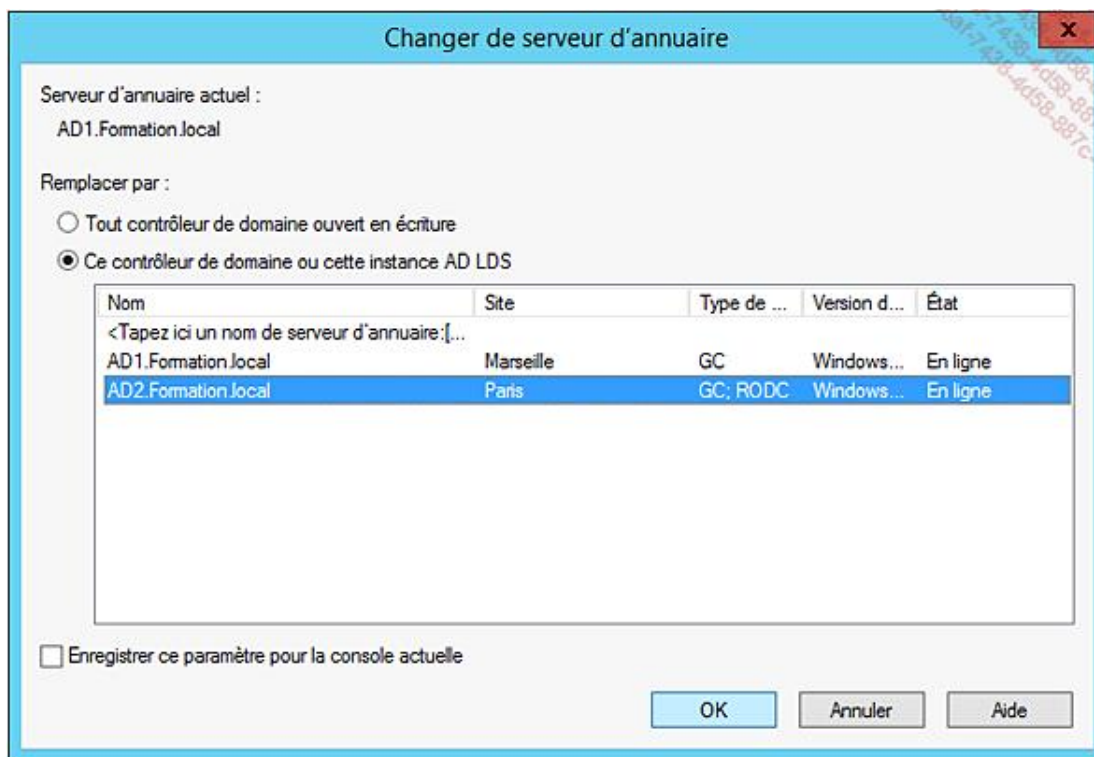
- Dans la fenêtre des chemins d'accès, cliquez sur **Suivant**.
- Dans la fenêtre du résumé, cliquez sur **Suivant**.
- Cliquez sur **Installer** dans la fenêtre de vérification de la configuration.

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**.

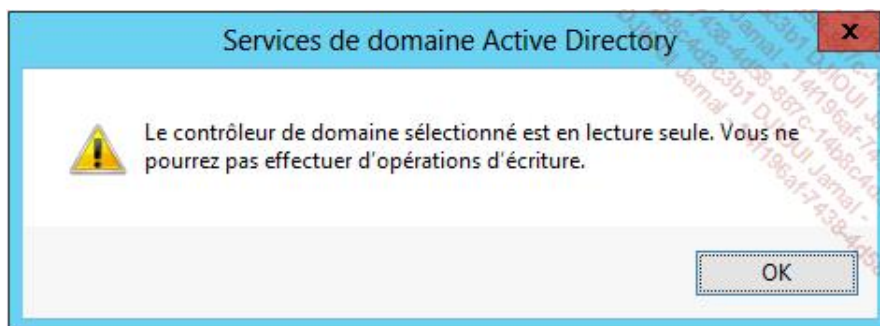


- Effectuez un clic droit sur le domaine puis un clic gauche sur **Changer de contrôleur de domaine**.
- Sélectionnez **AD2** puis cliquez sur **OK**.



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

→ Cliquez sur **OK**.

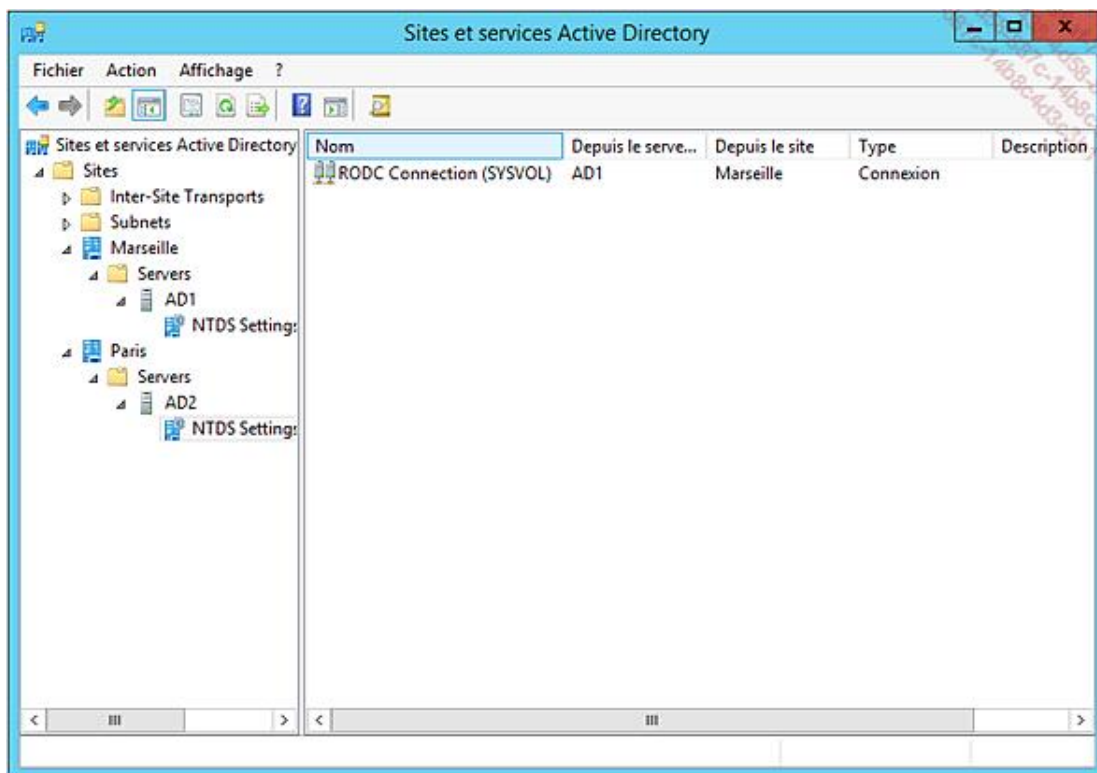


Il est impossible de créer un nouvel objet sur **AD2**.

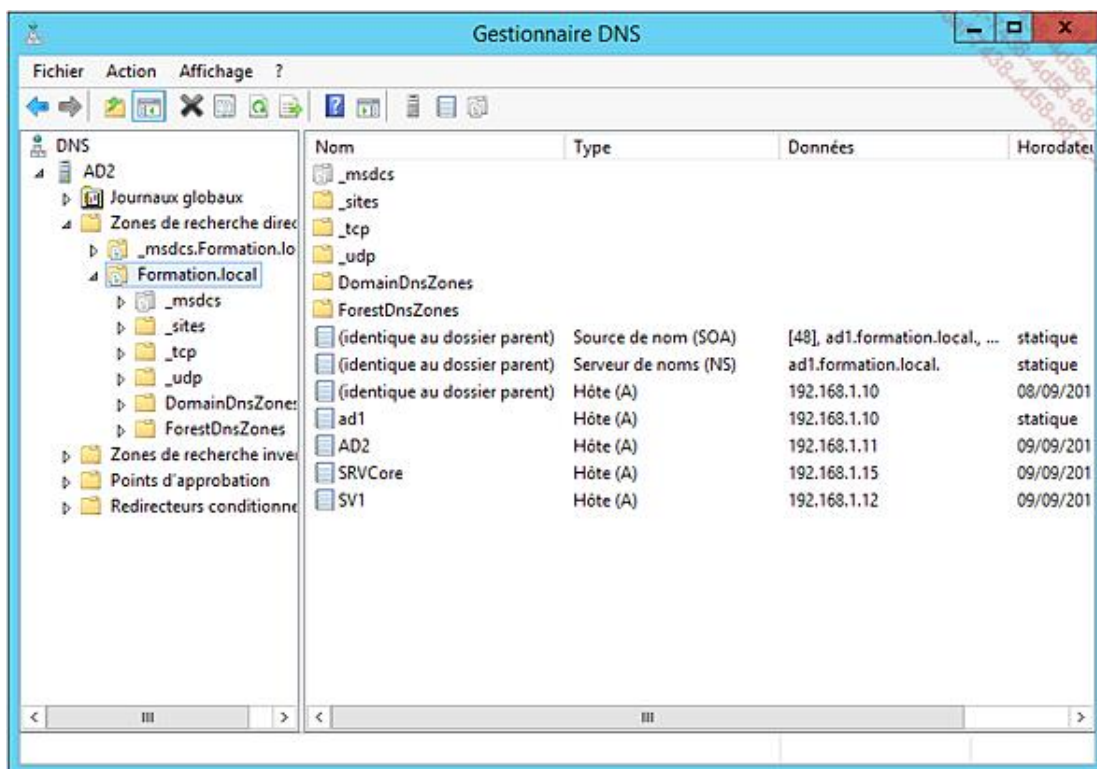
4. Vérification à réaliser après l'installation d'un contrôleur de domaine

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

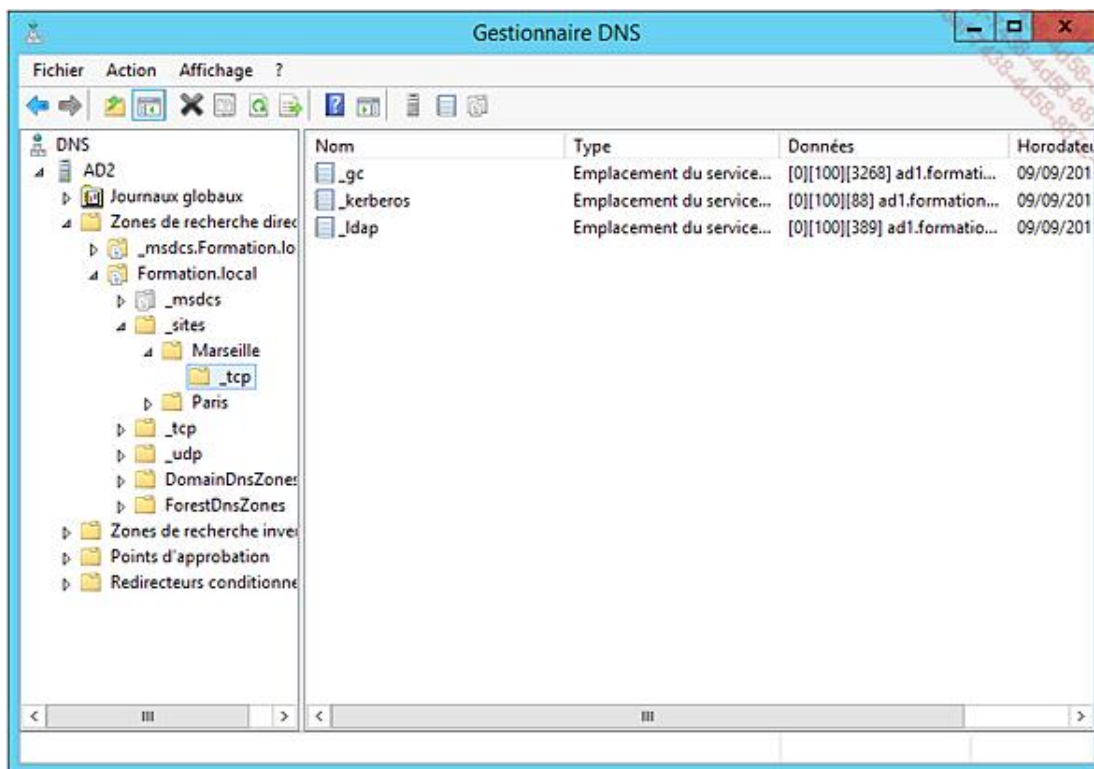
- La bonne configuration des sites AD.
- La configuration de la réplication intersite.
- L'association des sous-réseaux IP avec les bons sites.



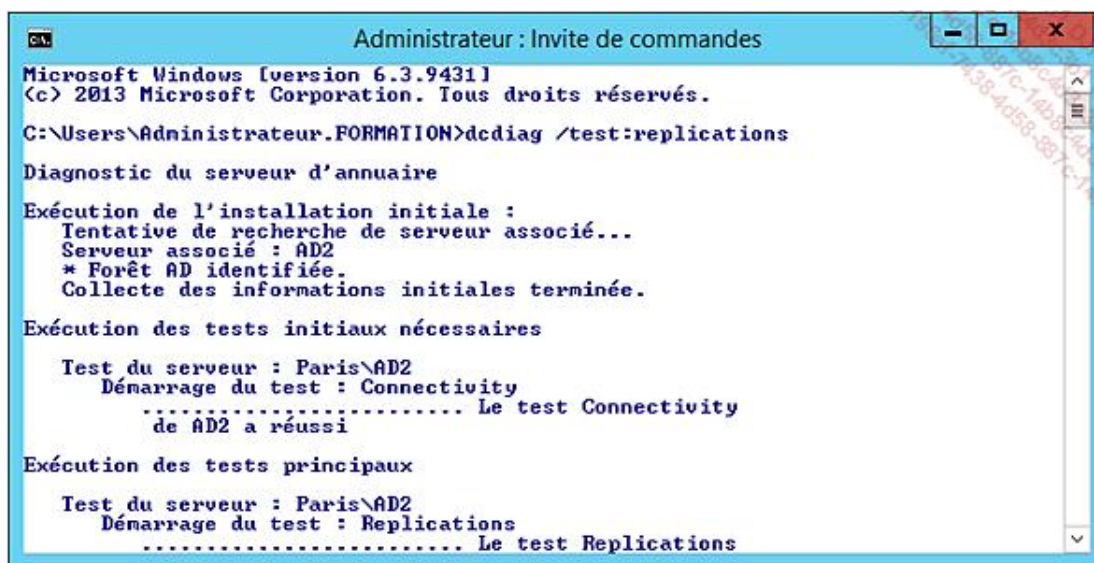
- La bonne configuration de la zone DNS qui a autorité sur le domaine. Cette vérification peut être effectuée par l'intermédiaire de la console DNS.



- 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.



- Distribuez les rôles FSMO aux serveurs adéquats afin d'éviter la perte de tous les rôles en cas de crash d'un serveur.

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

Redémarrage de l'AD

Active Directory s'appuie sur une base de données. Il est donc dans certains cas nécessaire de défragmenter la base, d'effectuer une restauration à la suite d'un crash, ou toute autre opération de maintenance.

Pour effectuer toutes ces manipulations, il faut un accès complet à la base de données. Lors de l'utilisation quotidienne de l'Active Directory, l'accès est limité aux fonctionnalités offertes par les différents outils (Sites et services AD, Utilisateurs et ordinateurs AD...).

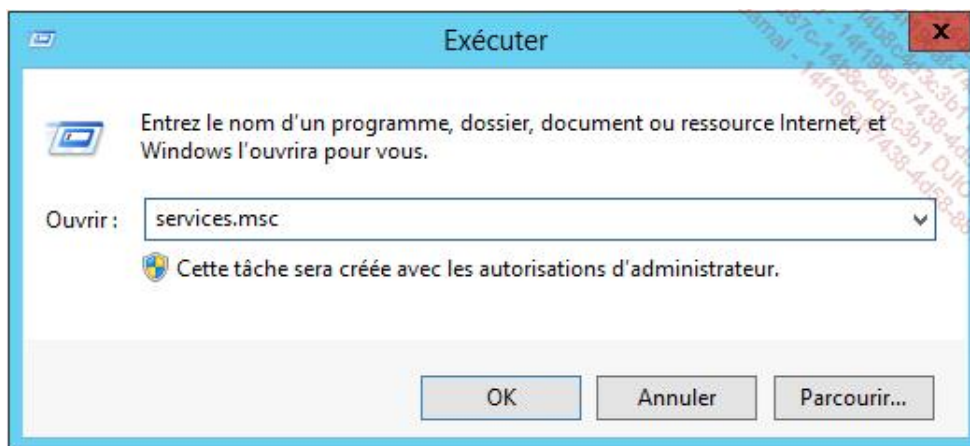
Depuis Windows Server 2008, un nouveau service Windows permet d'arrêter l'annuaire AD afin d'avoir un accès complet à la base de données.

1. Démarrage/arrêt des services Active Directory avec la console MMC Services

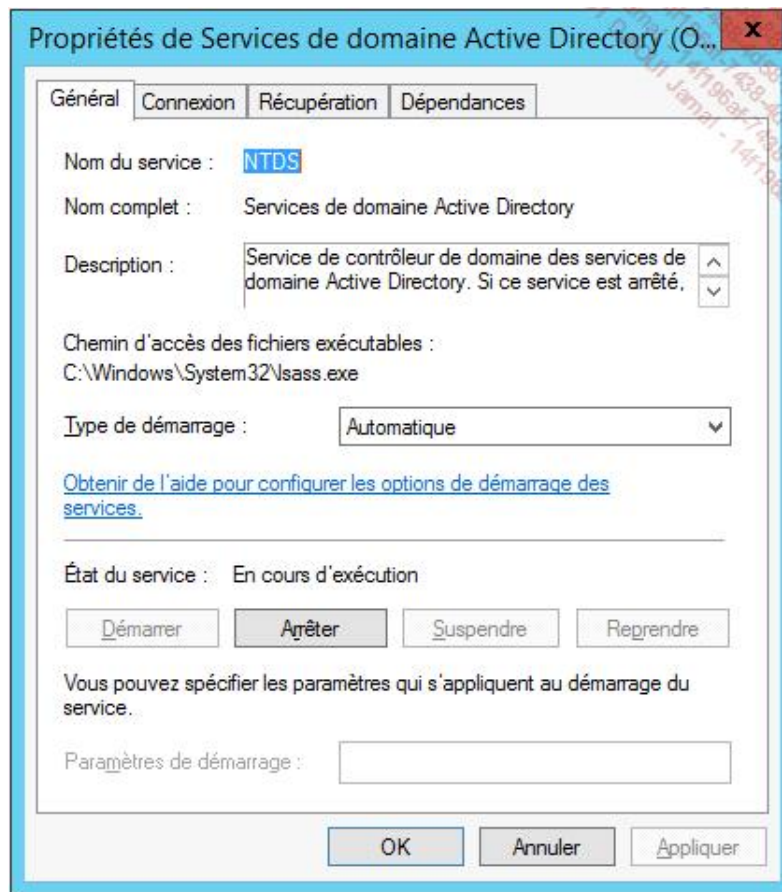
Il existe deux manières d'arrêter ou de démarrer le service Active Directory, la première, vue dans le présent point, est la gestion du service depuis la console MMC Services. La deuxième est vue dans le point suivant.

L'arrêt de ce service permet d'effectuer une maintenance (défragmentation...) sur la base de données du rôle AD DS.

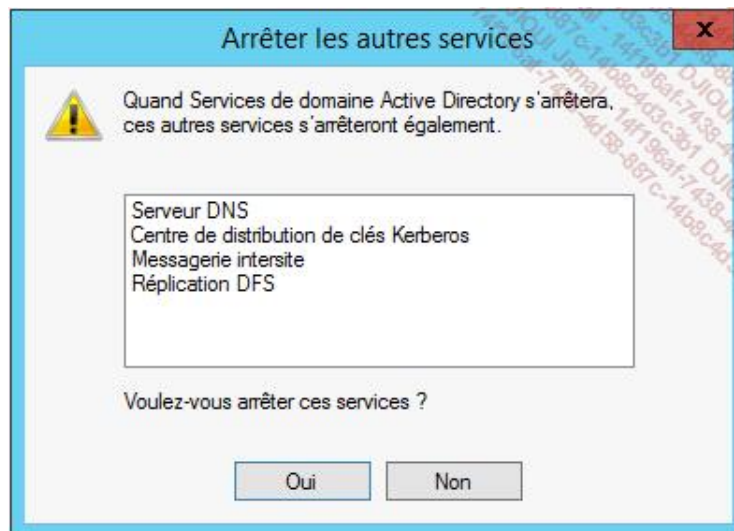
- Effectuez un clic droit sur le bouton **Démarrer** puis un clic gauche sur **Exécuter**.
- Saisissez dans le champ **services.msc**.



- Double cliquez sur **Services de domaine AD** puis sur **Arrêter**.



→ D'autres services doivent être également arrêtés. Cliquez sur **Oui**.



Après l'arrêt des services, il est impossible d'afficher les comptes **Utilisateurs et ordinateurs AD**.



→ Redémarrez le service de **domaine Active Directory**.

2. Démarrage/arrêt des services Active Directory avec l'invite de commandes

Comme pour tous les services, il est possible d'arrêter ou de redémarrer les services Active Directory en ligne de commande. L'instruction à utiliser est **net stop** pour l'arrêt du service et **net start** pour le démarrage.

→ Ouvrez une invite de commandes DOS.

→ Saisissez dans la fenêtre **net stop ntds**. Validez l'arrêt des autres services par un **O**.

```
Administrateur : C:\Windows\system32\cmd.exe
C:\Users\Administrateur>net stop ntds
Les services suivants dépendent du service Services de domaine Active Directory.
L'arrêt du service Services de domaine Active Directory arrête aussi ces service
s.
    Centre de distribution de clés Kerberos
    Messagerie intersite
    Réplication DFS
Voulez-vous continuer cette opération ? <O/N> [N] : O
Le service Centre de distribution de clés Kerberos s'arrête.
Le service Centre de distribution de clés Kerberos a été arrêté.
Le service Messagerie intersite s'arrête.
Le service Messagerie intersite a été arrêté.
Le service Réplication DFS a été arrêté.
Le service Services de domaine Active Directory s'arrête.
Le service Services de domaine Active Directory a été arrêté.
C:\Users\Administrateur>
```

→ Tentez d'ouvrir la console **Utilisateurs et ordinateurs AD**. Un message d'erreur apparaît.

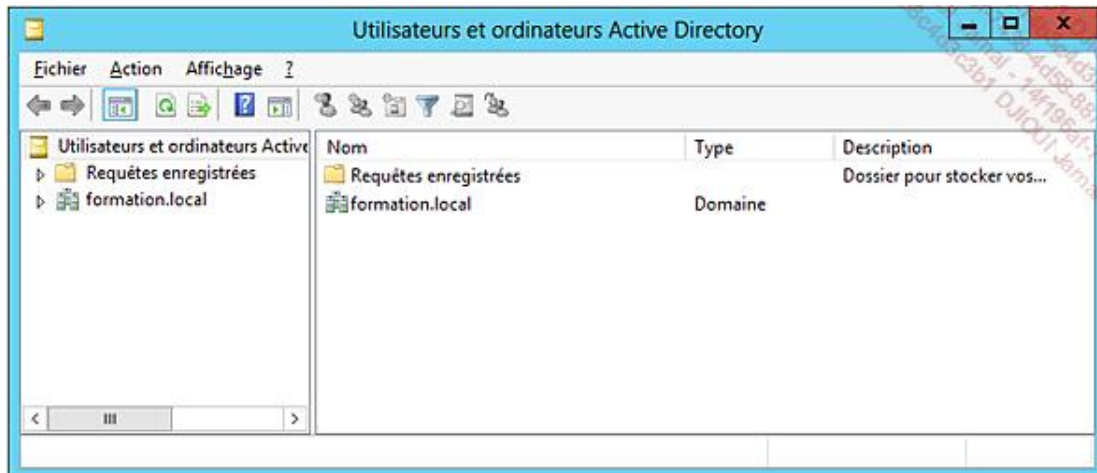
→ Saisissez dans la fenêtre **net start ntds**.

```
Administrateur : C:\Windows\system32\cmd.exe

C:\Users\Administrateur>net start ntds
Le service Services de domaine Active Directory démarre...
Le service Services de domaine Active Directory a démarré.

C:\Users\Administrateur>_
```

Il est désormais possible d'accéder à la console.



Suppression d'un contrôleur de domaine

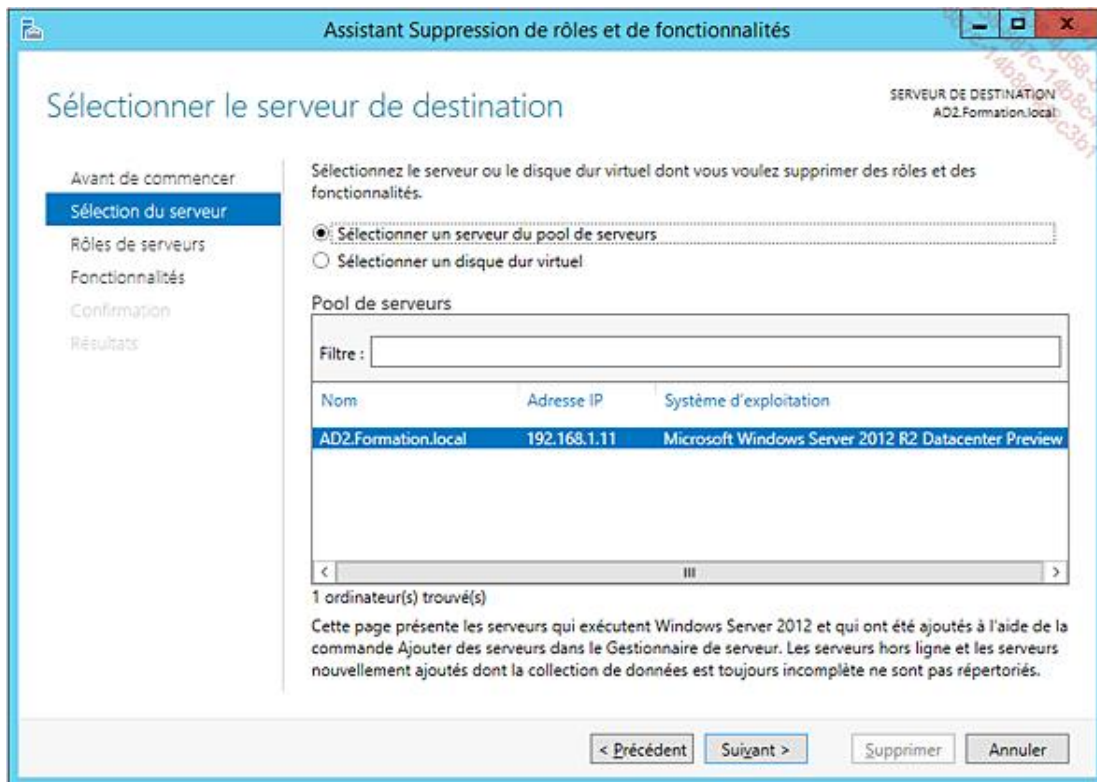
Un contrôleur de domaine peut être amené à être rétrogradé en simple serveur membre pour des raisons de changement de serveur ou autres.

La manipulation après avoir effectué la migration des comptes est donc d'enlever le rôle de contrôleur de domaine au serveur.

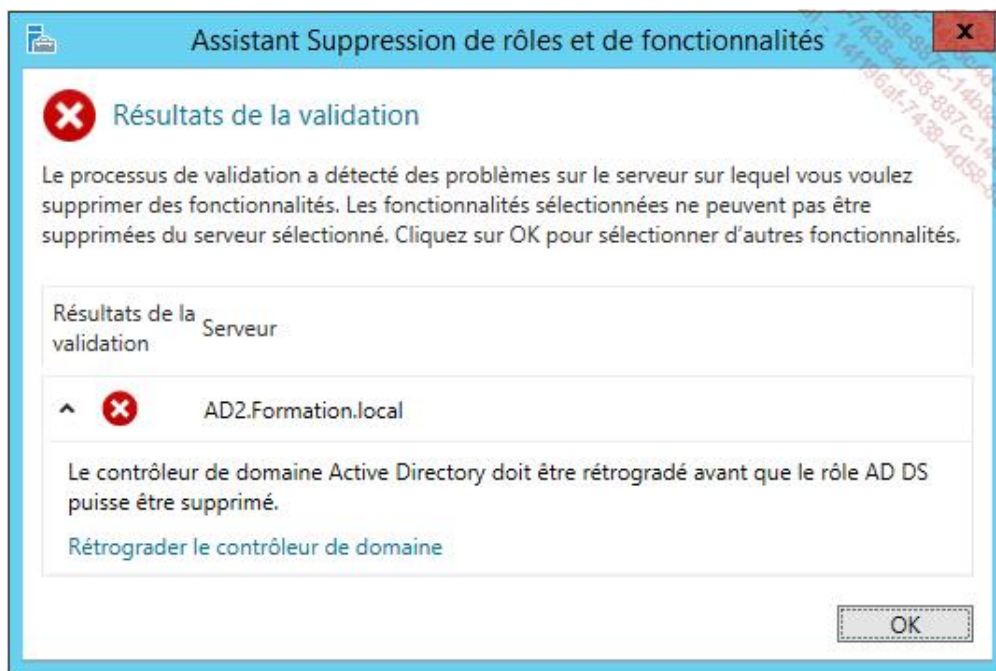
1. Supprimer un contrôleur de domaine d'un domaine

Le domaine **formation.local** est constitué d'un contrôleur de domaine en lecture/écriture et d'un contrôleur de domaine uniquement en lecture. L'opération consiste à supprimer le rôle **AD DS** sur le **RODC**. On parlera donc de rétrogradation du serveur.

- Ouvrez une session sur **AD2** en tant qu'administrateur du domaine.
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Gérer** puis sur **Supprimer des rôles et fonctionnalités**.
- Cliquez sur **Suivant** dans la page d'accueil de l'assistant.
- Dans la fenêtre **Sélectionner le serveur de destination**, cliquez sur **Suivant**.

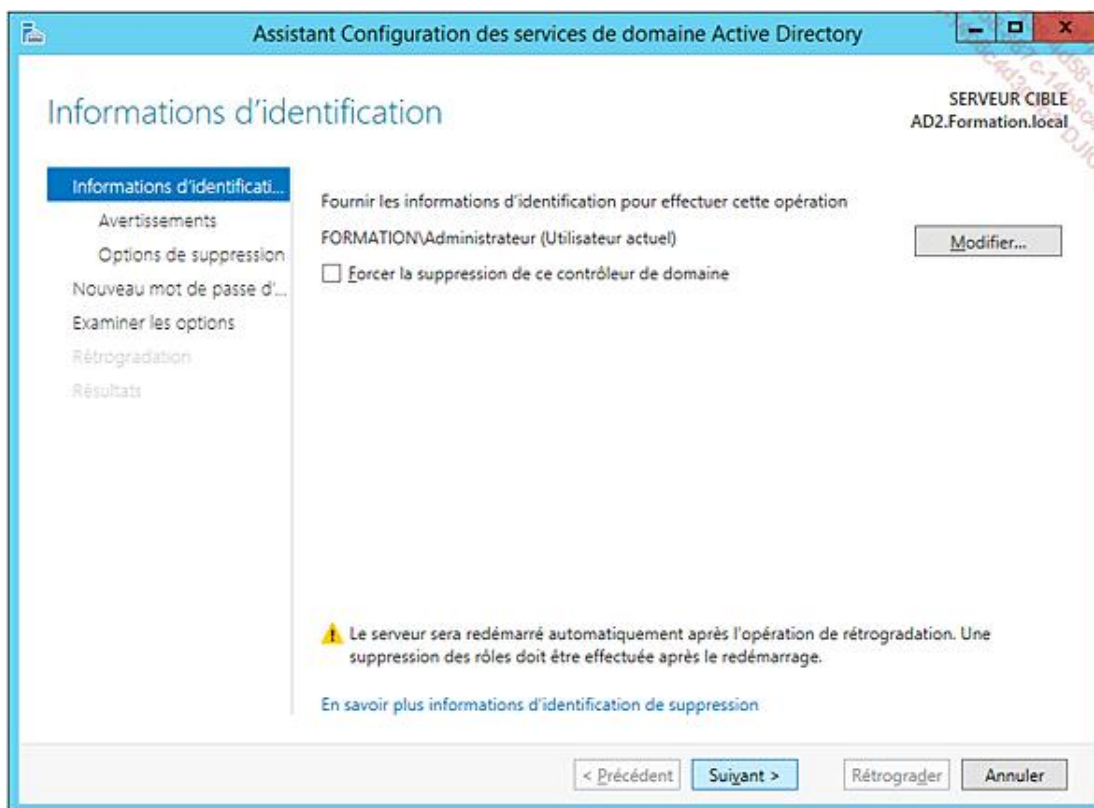


- Décochez le rôle **Services AD DS**. Les fonctionnalités sont également à supprimer. Un message d'erreur apparaît. Cliquez sur **Rétrograder le contrôleur de domaine**.

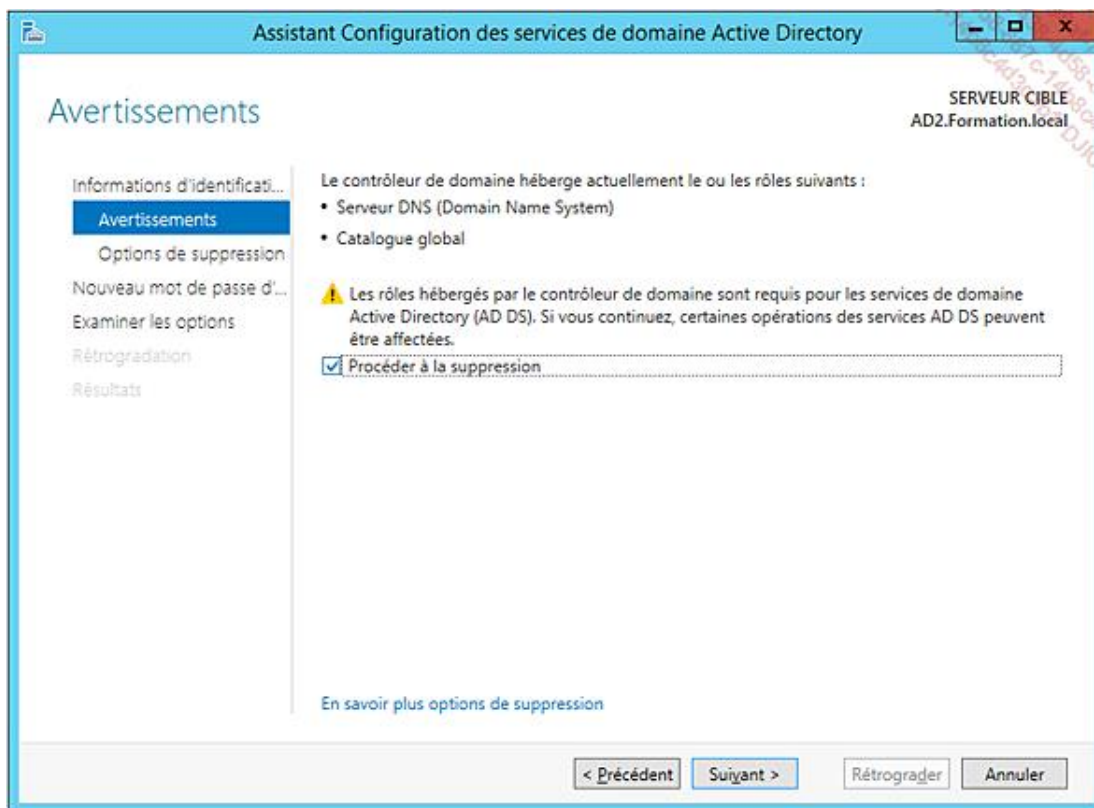


→ Dans la fenêtre d'identification, cliquez sur **Suivant**.

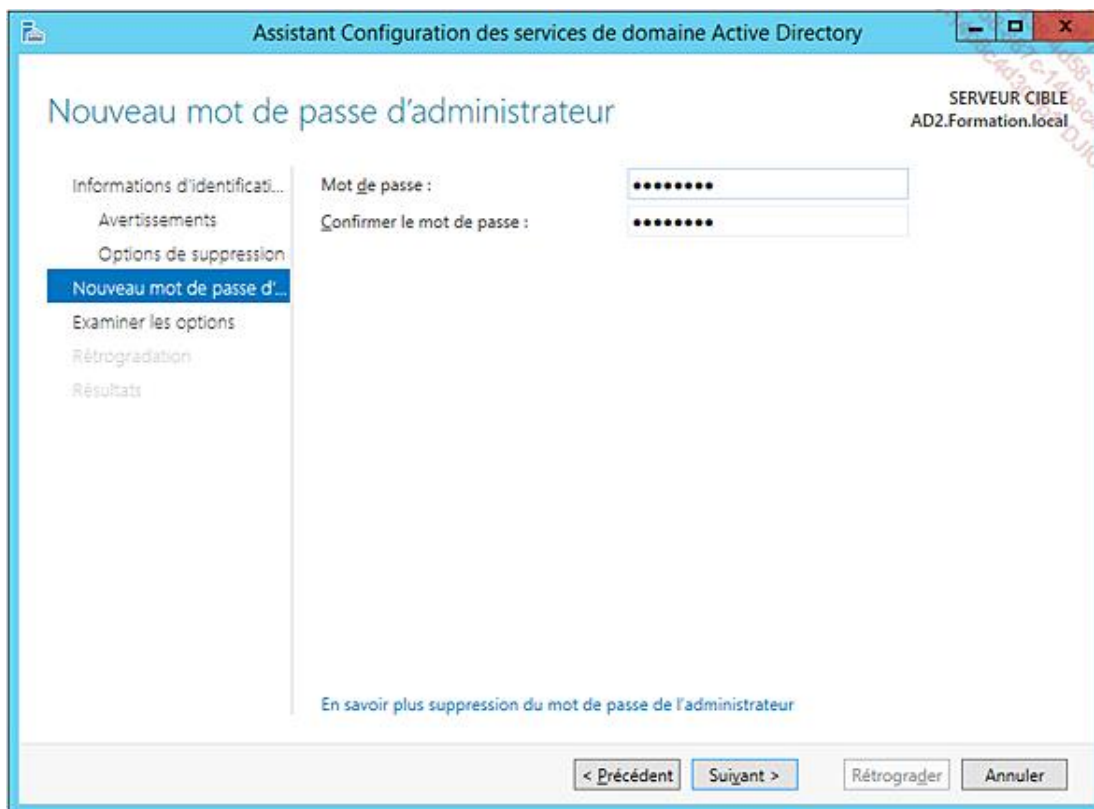
- Le compte à utiliser pour la rétrogradation du serveur peut être changé à l'aide du bouton **Modifier**. En cas de contrôleur de domaine isolé, il est utile de cocher la case **Forcer la suppression de ce contrôleur de domaine**.



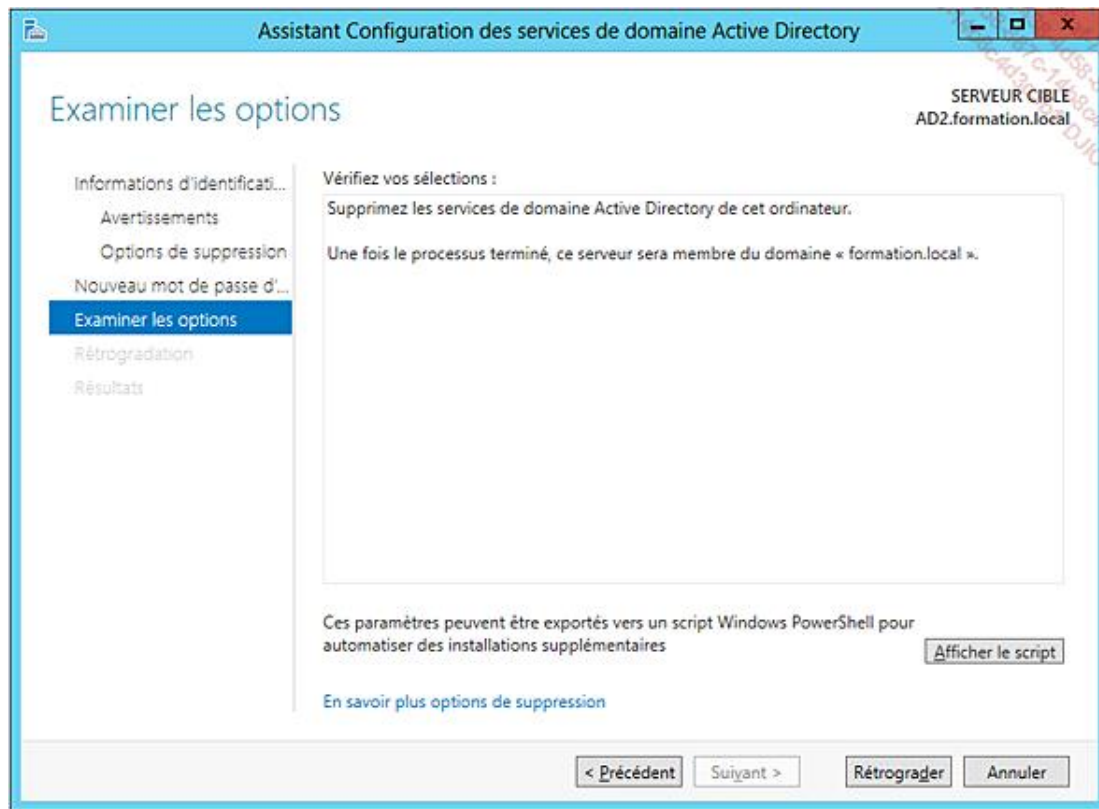
→ Cochez la case **Procéder à la suppression** puis cliquez sur **Suivant**.



- Cochez la case **Conserver les métadonnées de contrôleur de domaine** puis cliquez sur **Suivant**.
- Dans la fenêtre des **Options de suppression**, cliquez sur **Suivant**.
- Saisissez, à la fin de la rétrogradation, le mot de passe qui sera utilisé pour le compte administrateur local du serveur (mot de passe : **Pa\$\$w0rd**).

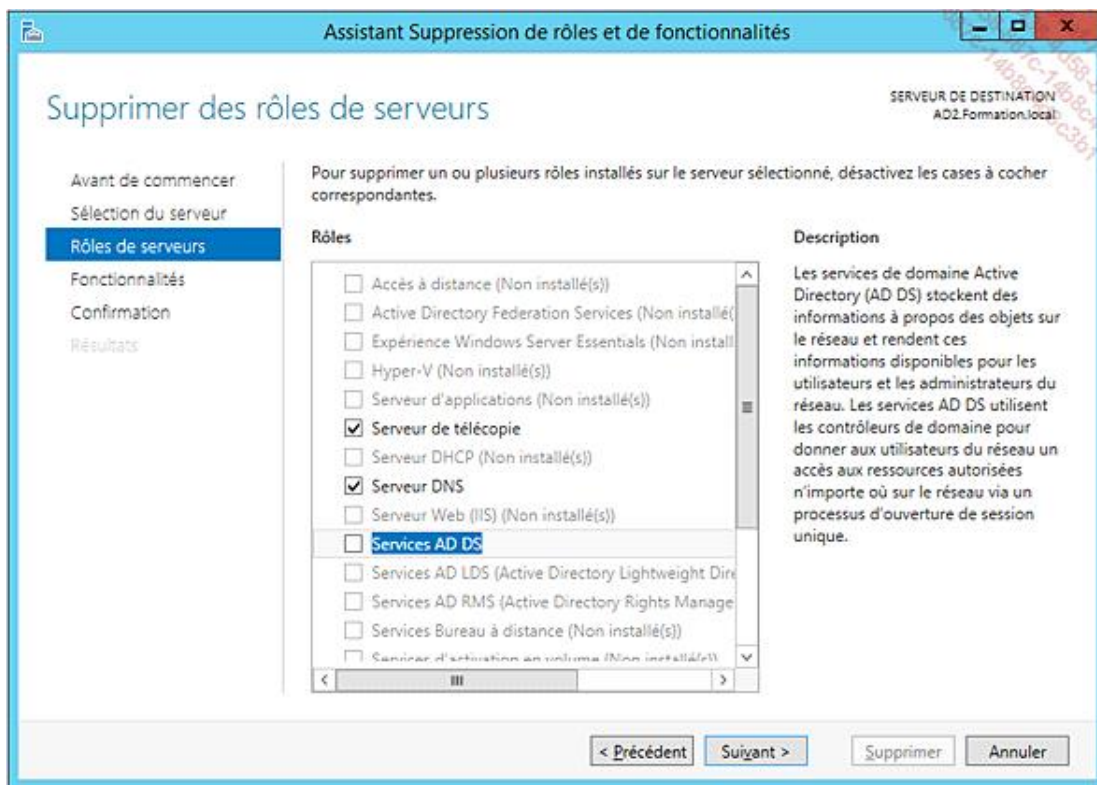


- Dans la page du résumé, cliquez sur **Rétrograder**.



À la fin de la rétrogradation, le serveur redémarre.

- Ouvrez une session sur **AD2** en tant qu'administrateur local.
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Gérer** puis sur **Supprimer des rôles et fonctionnalités**.
- Cliquez sur **Suivant** dans la page d'accueil de l'assistant.
- Dans la fenêtre de sélection du serveur de destination, cliquez sur **Suivant**.
- Décochez le rôle **Services AD DS**. Les fonctionnalités sont également à supprimer.



→ Dans la fenêtre **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

→ Confirmez la suppression en cliquant sur **Supprimer**.

Le rôle **Services AD DS** est maintenant supprimé. Le rôle DNS n'a pas été supprimé car ce rôle sera utilisé dans les chapitres suivants.

→ Supprimez le compte ordinateur présent dans l'unité d'organisation **Domain Controllers** (console **Utilisateurs et ordinateurs Active Directory**).