

# Déployer un contrôleur de domaine avec Windows Server 2012 R2



## Introduction

Ce tutoriel a pour but de vous montrer comment déployer un contrôleur de domaine avec Windows Server 2012 R2. Le déploiement d'un contrôleur de domaine doit se faire en plusieurs étapes. Il s'agit d'ajouter les fonctionnalités une à une sur le serveur et de les configurer au fur et à mesure. Ce que nous cherchons au final, c'est un serveur ayant les rôles suivants :

- DNS
  - Active Directory DS de la forêt nommée : mondomaine.fr
- Notre serveur "amelia" va supporter tous ces rôles.

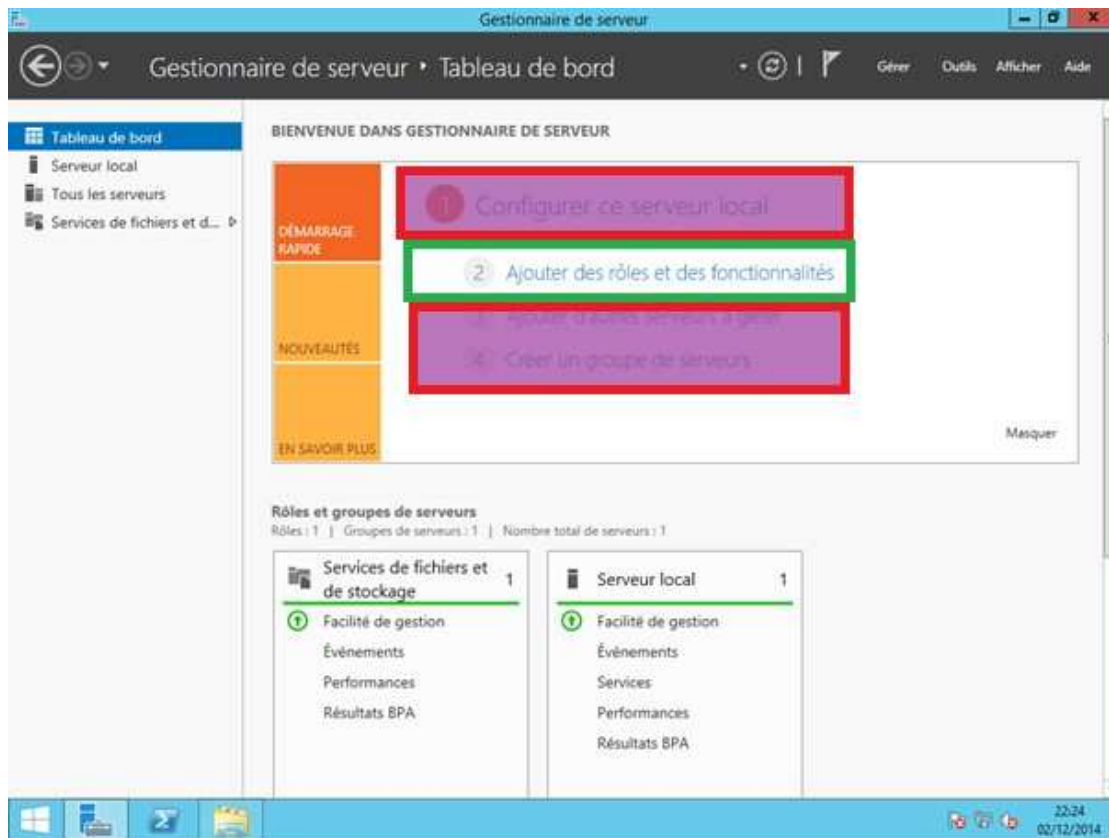
## 1. Définition du DNS

Le système DNS est un système d'appellation d'ordinateurs et de services réseau organisé selon une hiérarchie de domaines. Les réseaux TCP/IP tels qu'Internet utilisent DNS pour localiser des ordinateurs et des services à l'aide de noms conviviaux. Si un utilisateur entre le nom DNS d'un ordinateur dans une application, les clients et les serveurs DNS collaborent pour rechercher ce nom et fournir d'autres informations associées à l'ordinateur, telles que son adresse IP ou les services qu'il fournit au réseau. Ce processus s'appelle la résolution de noms.

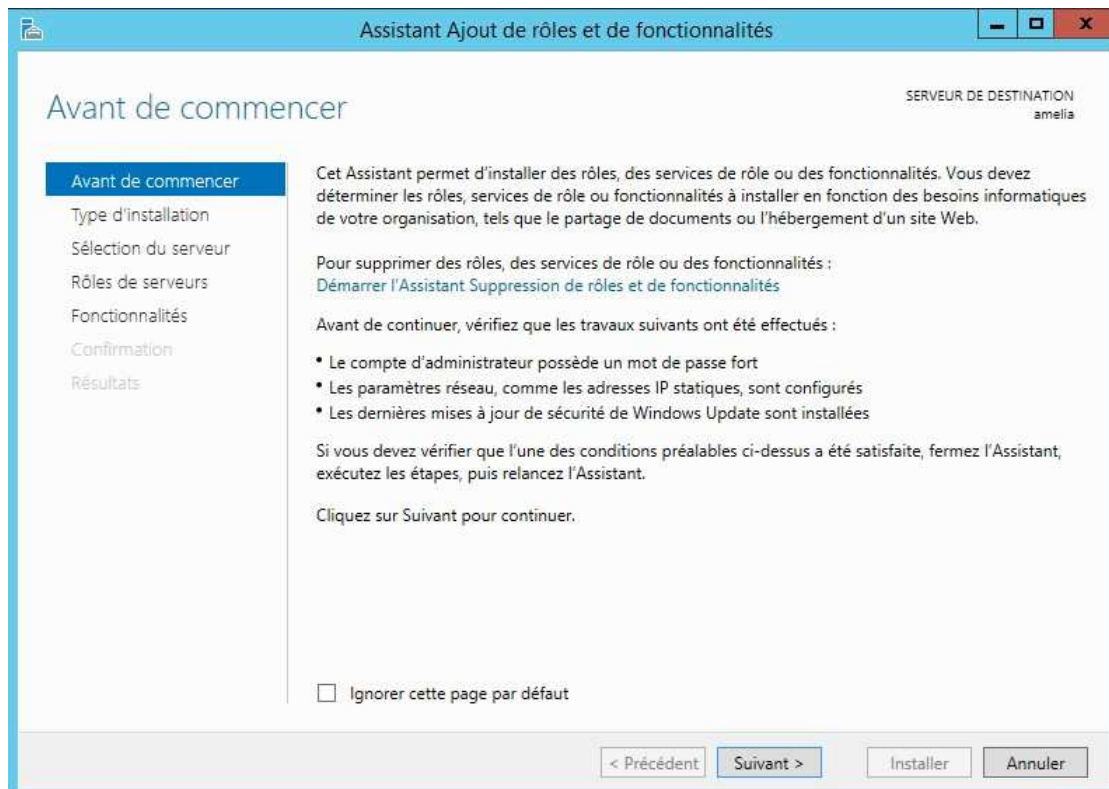
Le rôle de serveur DNS permet à un serveur qui exécute Windows Server 2012 R2 de servir de serveur de résolution de noms pour un réseau TCP/IP. Le réseau peut contenir des ordinateurs qui exécutent Windows et des ordinateurs qui fonctionnent sous d'autres systèmes d'exploitation. Le service DNS dans Windows Server 2012 R2 est étroitement intégré au protocole DHCP (Dynamic Host Configuration Protocol) pour permettre aux clients et aux serveurs DHCP Windows d'inscrire automatiquement les noms d'hôte et les adresses IP sur le serveur DNS du domaine approprié.

Tous les contrôleurs de domaine exécutent le service DNS serveur et sont autoritaires pour le domaine.

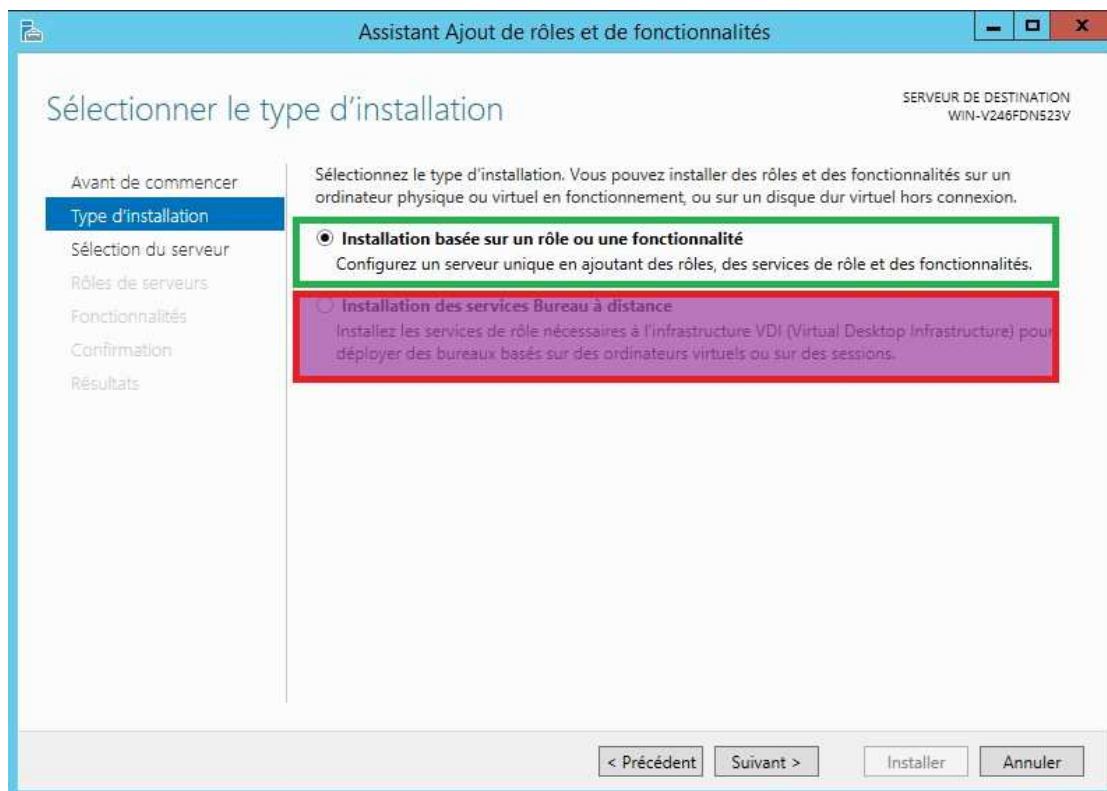
## 2.1 Installation du DNS



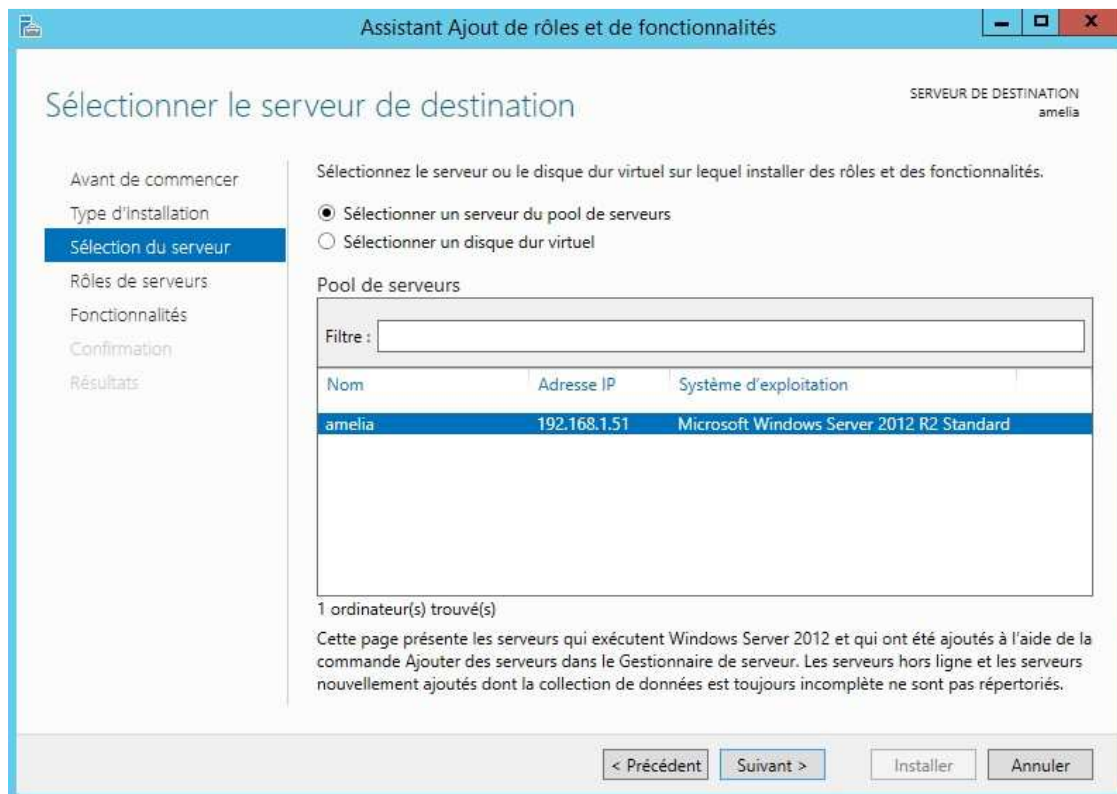
Dans la page du « Gestionnaire de serveur », cliquez sur « Ajouter des rôles et des fonctionnalités ».



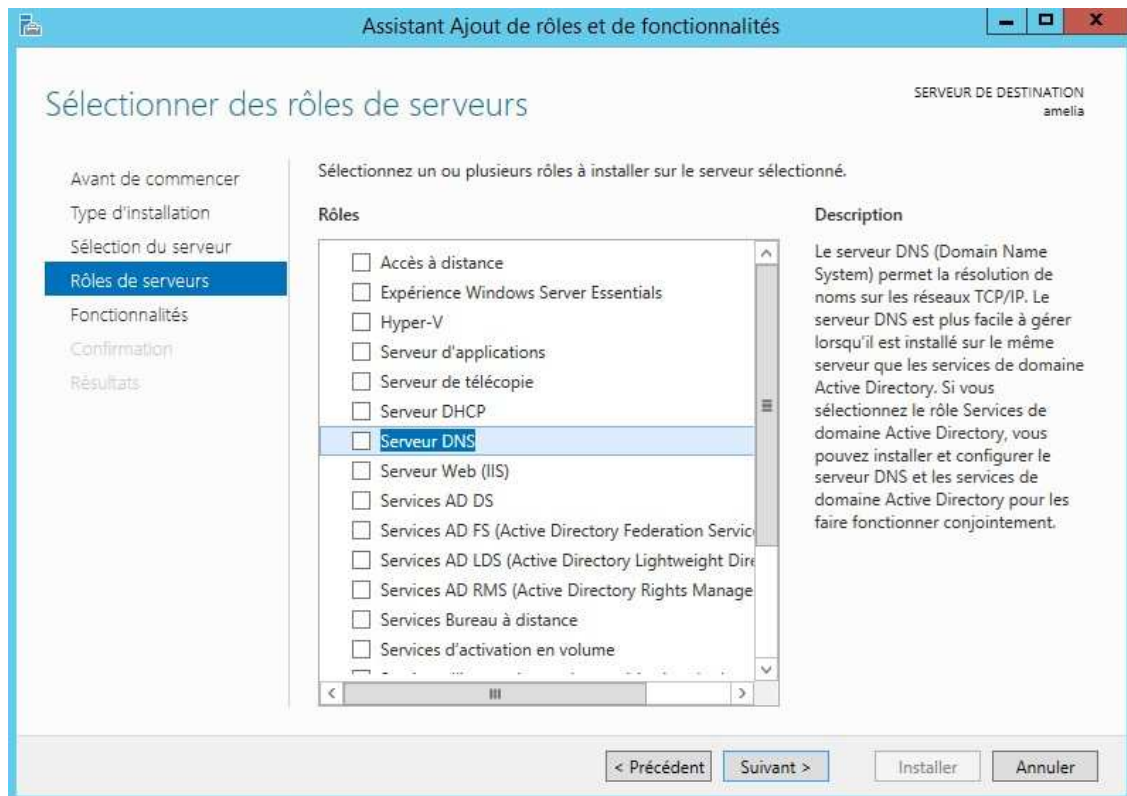
Cliquez sur « Suivant ».



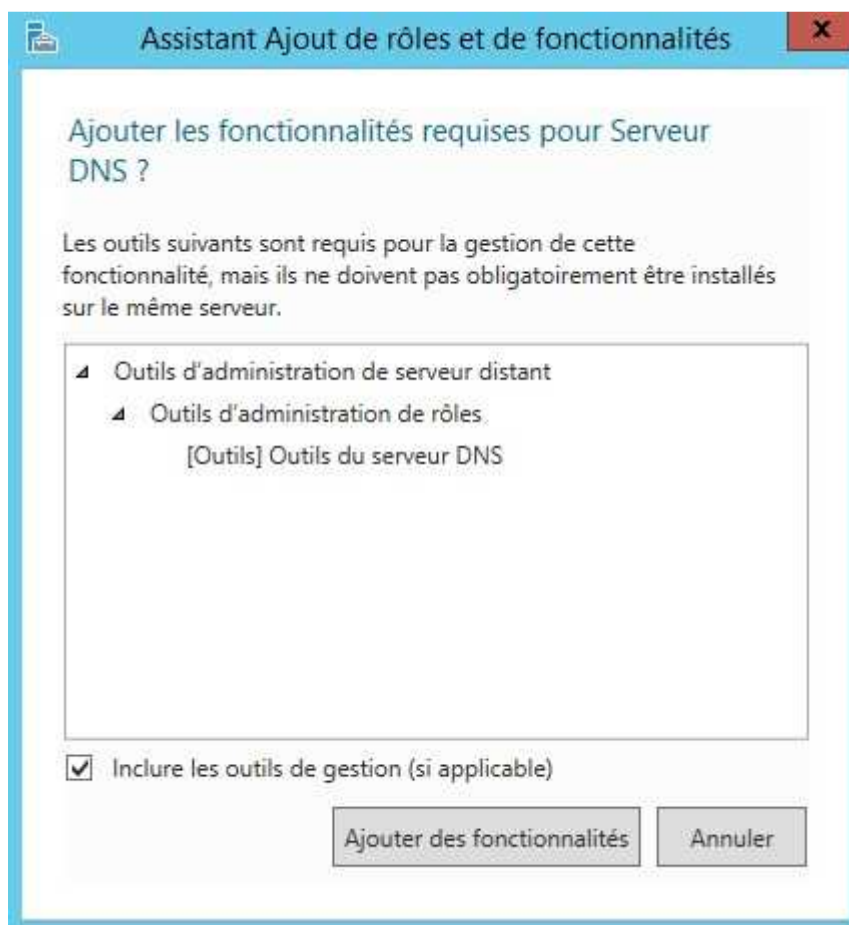
Choisissez l'option « Installation basée sur un rôle ou une fonctionnalité »



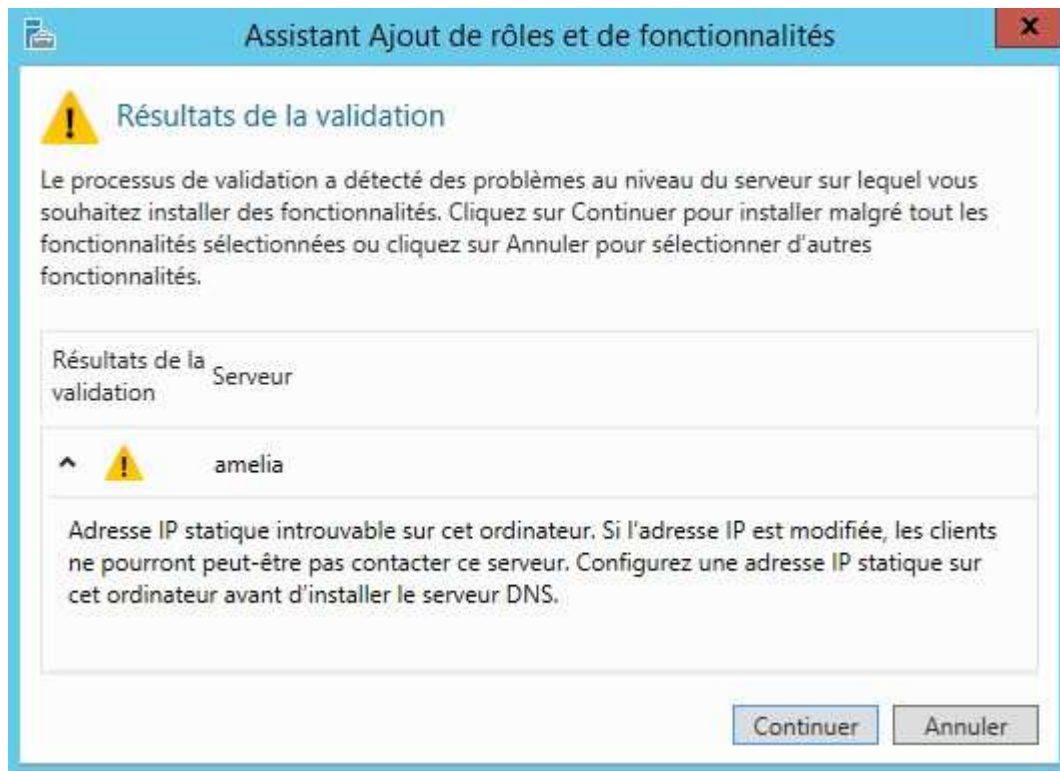
Sélectionnez votre serveur dans la liste.



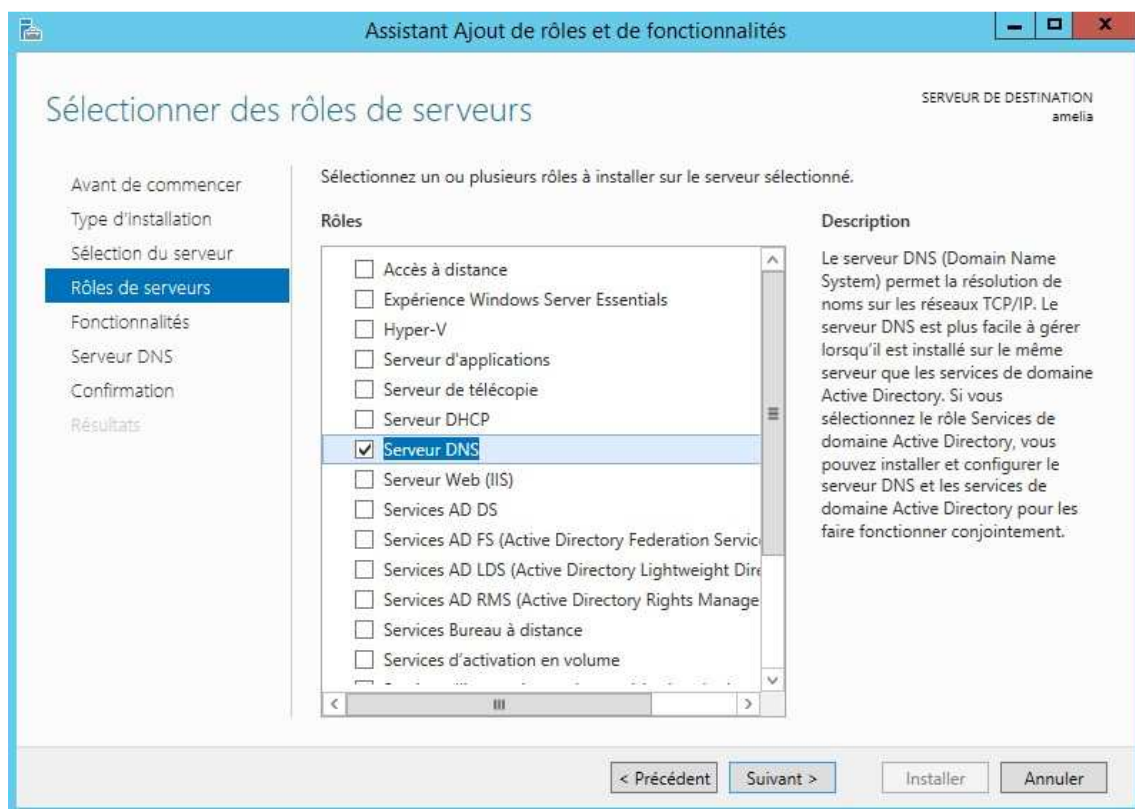
Cochez la case « Serveur DNS »



Cliquez sur « Ajouter des fonctionnalités »

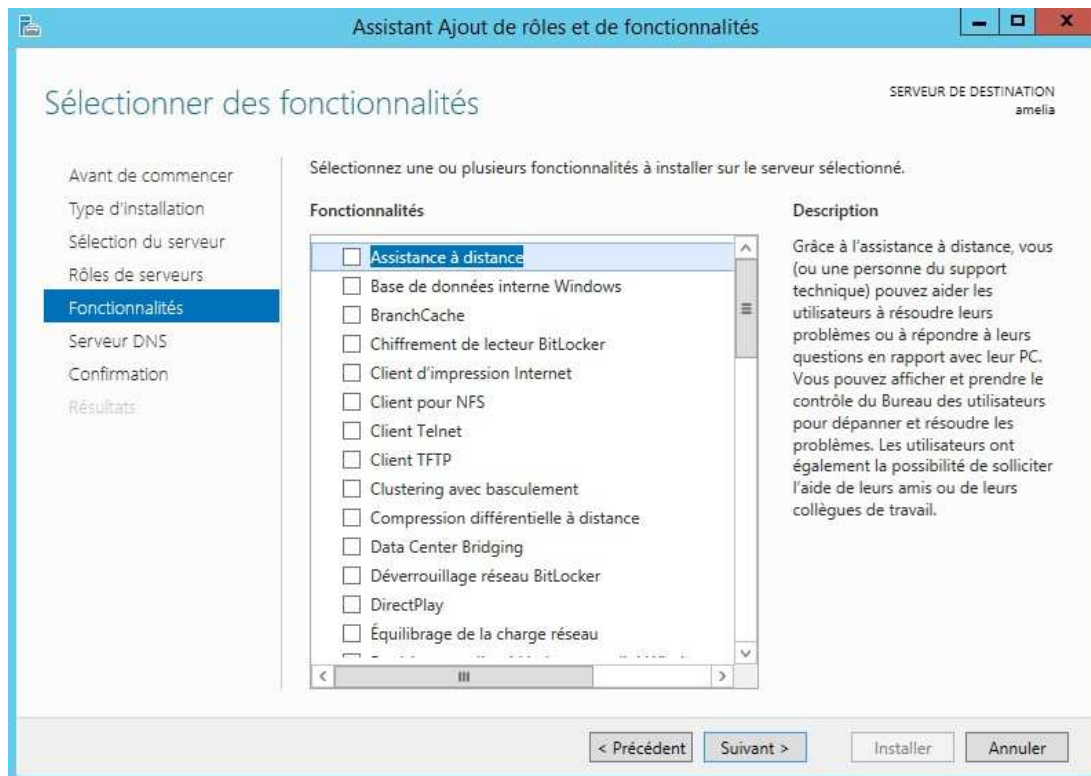


J'ai décidé d'ignorer cet avertissement car j'ai déjà configuré une adresse statique dans les paramètres de mon routeur.

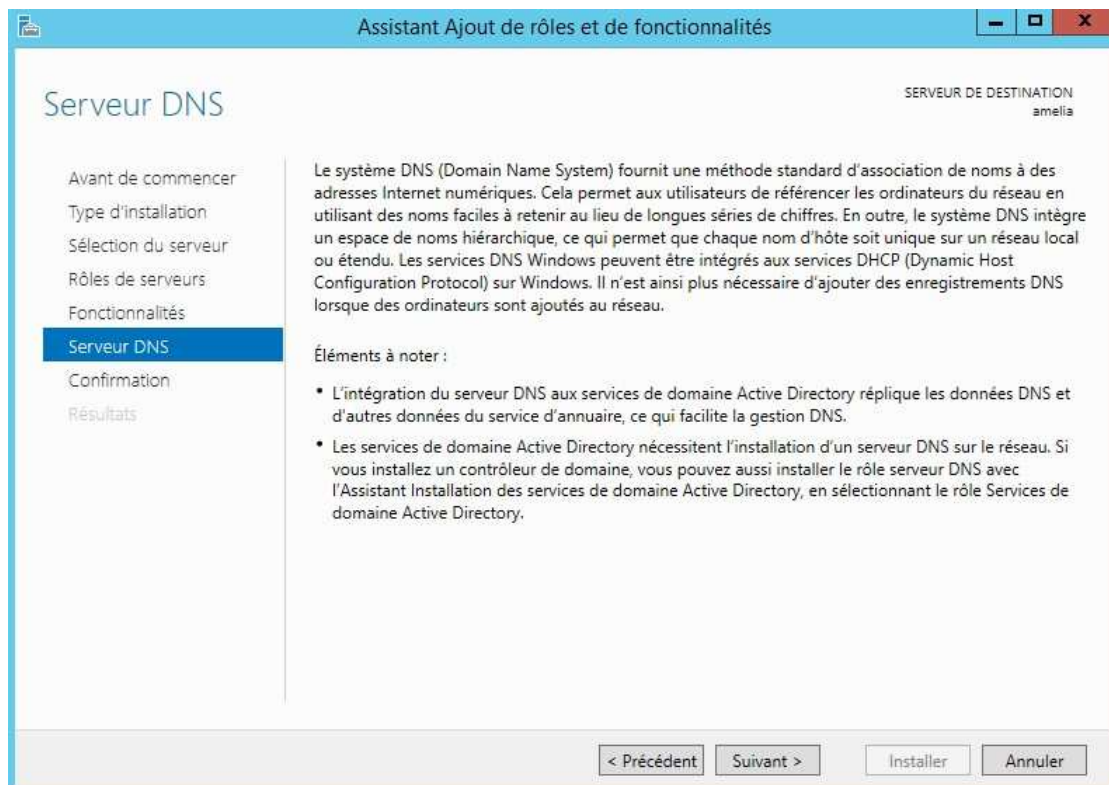




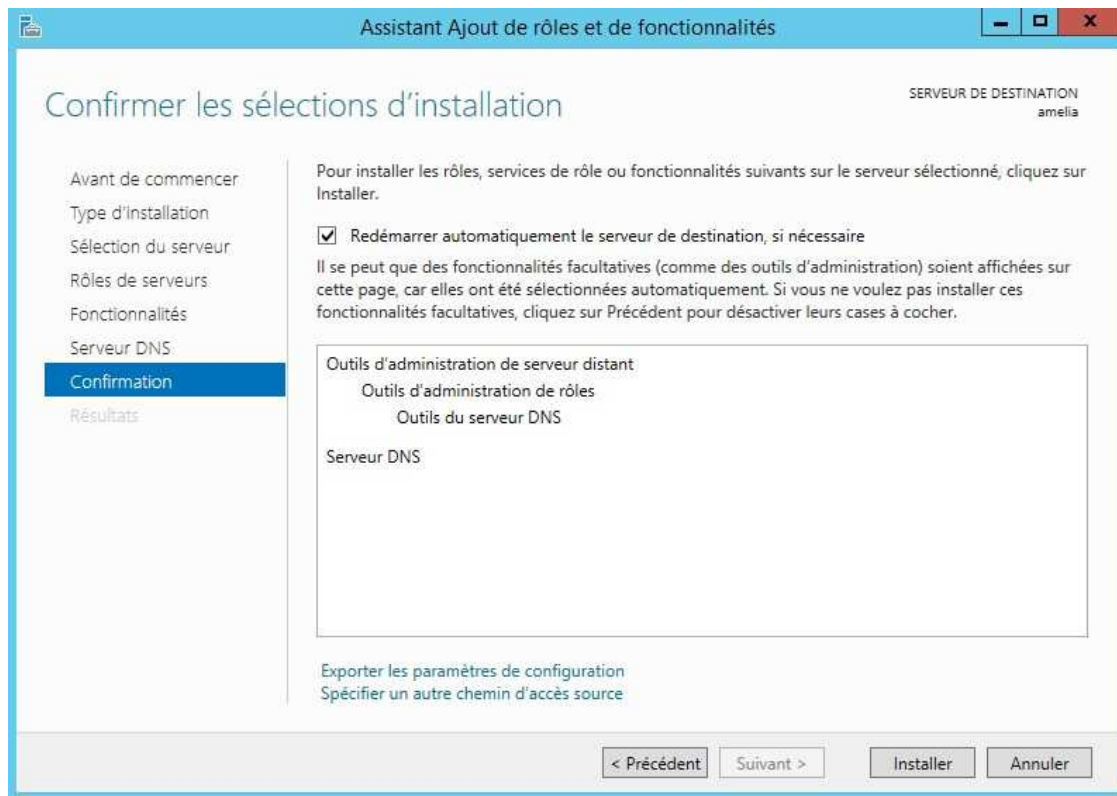
Cliquez sur « Suivant »



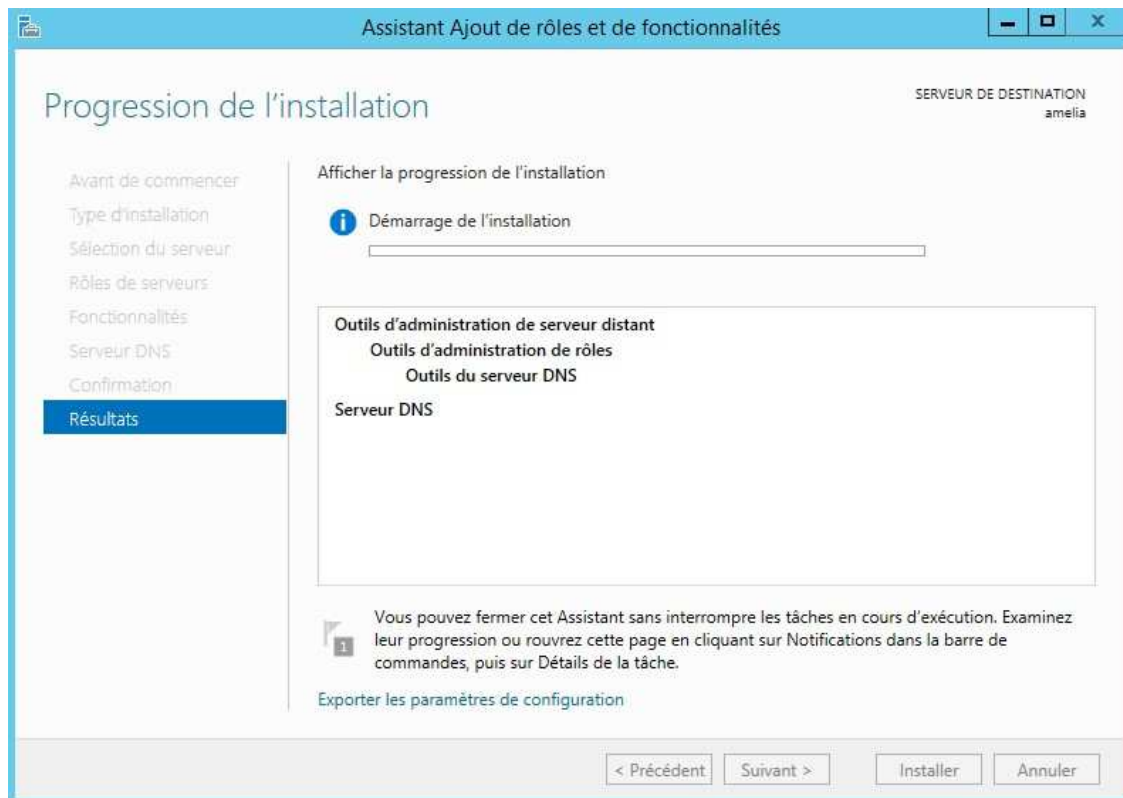
De nouveau cliquez sur « Suivant »



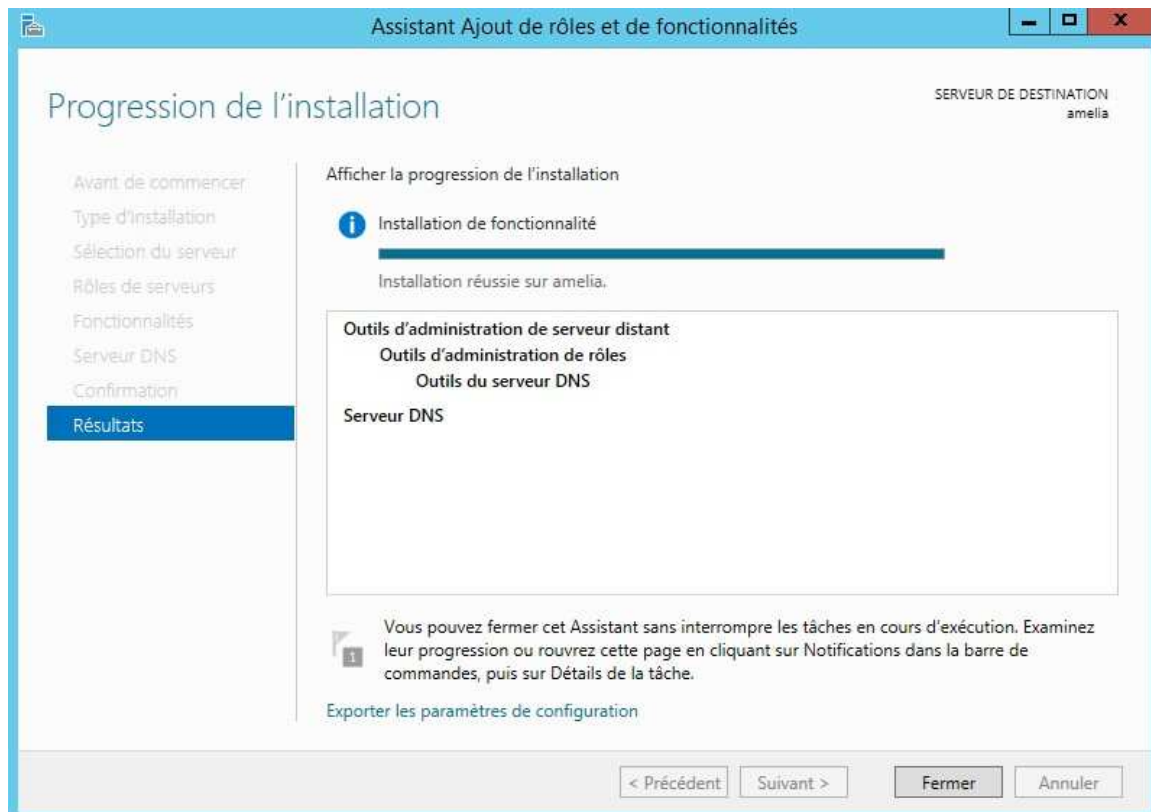
Cliquez sur « Suivant »



Cochez la case « Redémarrer automatiquement le serveur de destination si nécessaire ».  
Cliquez sur « Installer »

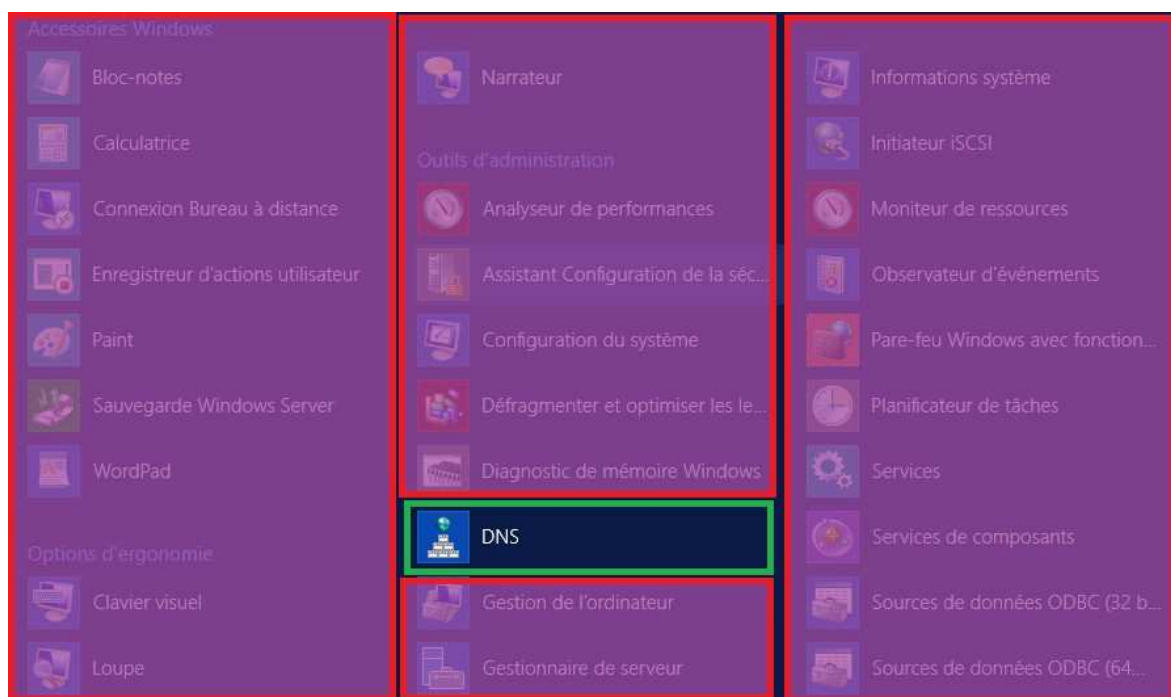


L'installation se lance.



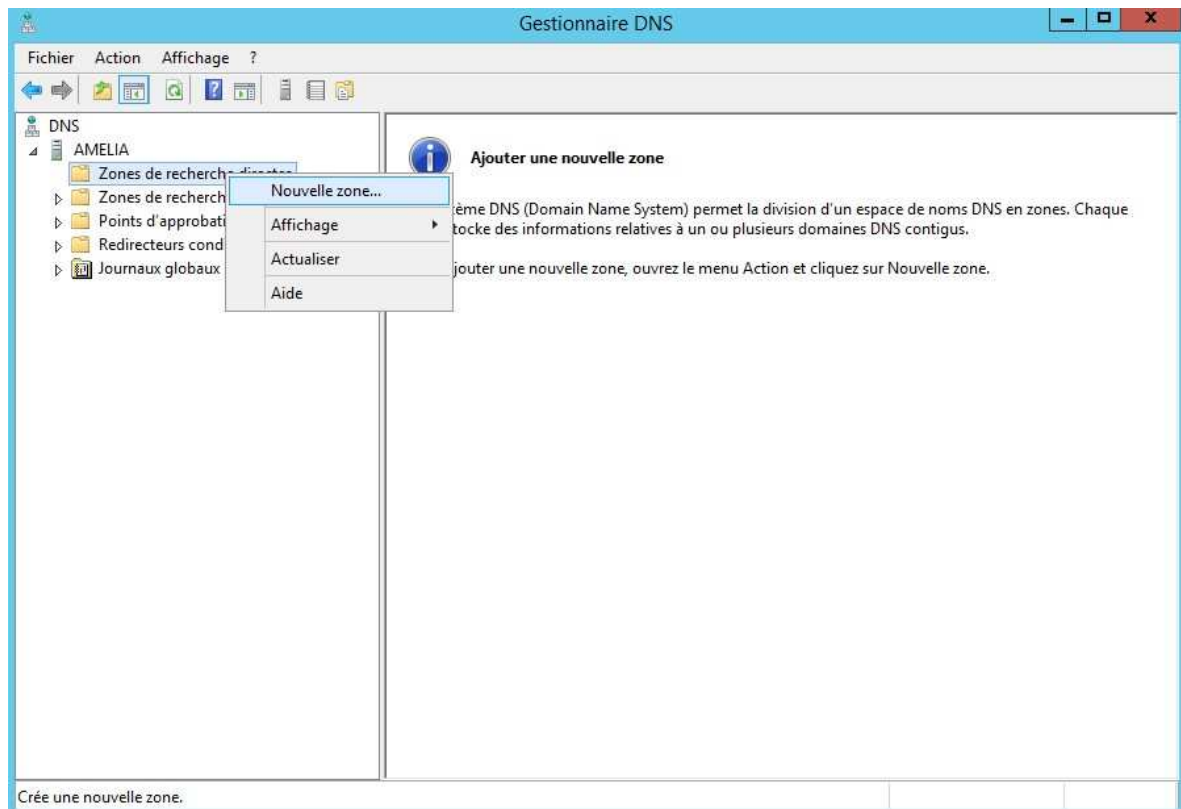
L'installation est terminée. Il faut maintenant configurer le service DNS du serveur.

## 2.2 Configuration du DNS

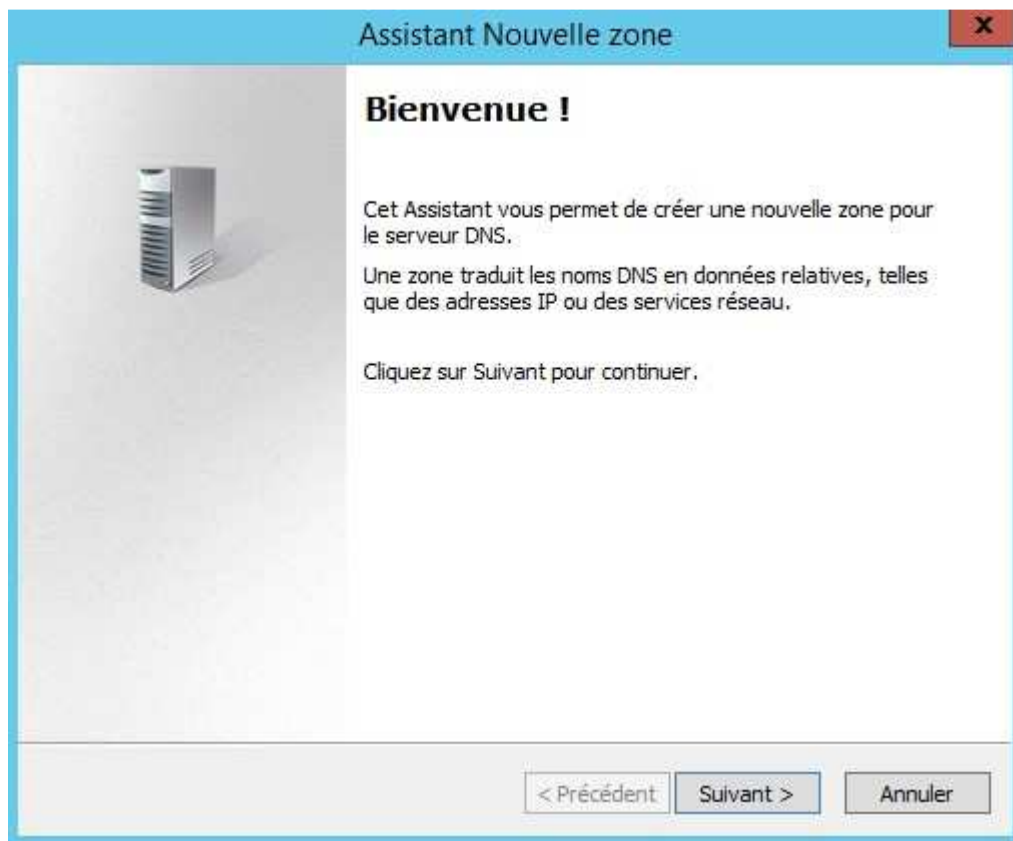


Dans le menu démarrer de Windows Server 2012 R2, cliquez sur l'outil d'administration « DNS ».





Dans la fenêtre MMC, faites un clic droit sur « Zones de recherche directe » et cliquez sur « Nouvelle zone... »



Cliquez sur « Suivant ».

**Assistant Nouvelle zone**

**Type de zone**  
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- ☒ **Zone principale**  
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- ☐ **Zone secondaire**  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- ☐ **Zone de stub**  
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☐ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent   Suivant >   Annuler

Choisissez la première option « Zone principale » et cliquez sur « Suivant ».

**Assistant Nouvelle zone**

**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

< Précédent   Suivant >   Annuler

Renseignez le nom de votre domaine et cliquez sur « Suivant ».

**Assistant Nouvelle zone**

**Fichier zone**  
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

☒ Créer un nouveau fichier nommé :

☐ Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent   Suivant >   Annuler

Laissez le nom du fichier qui va être créé et cliquez sur « Suivant ».

**Assistant Nouvelle zone**


---

**Mise à niveau dynamique**

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)  
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées**  
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.  
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☐ Ne pas autoriser les mises à jour dynamiques  
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

Choisissez la première option non grisée « Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées ».

**Assistant Nouvelle zone**

---

**Fin de l'Assistant Nouvelle zone**

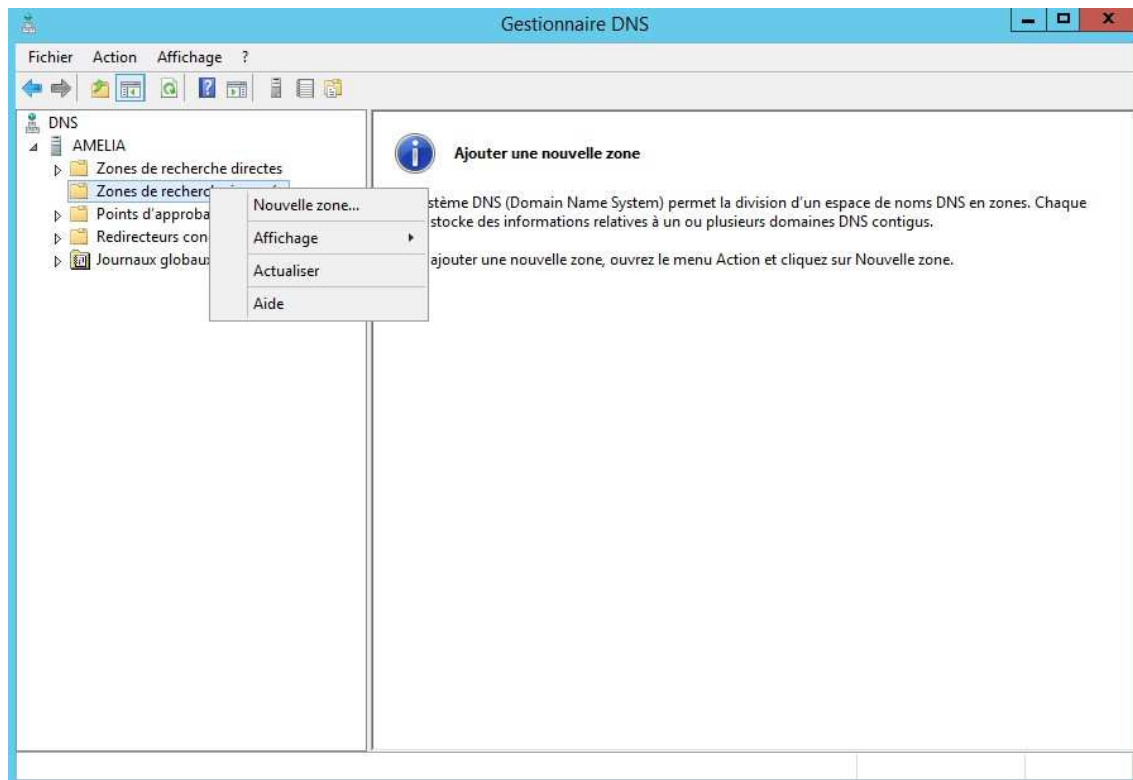
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom :	mondomaine.fr
Type :	Zone principale standard
Type de recherche :	Directe
Nom de fichier :	mondomaine.fr.dns

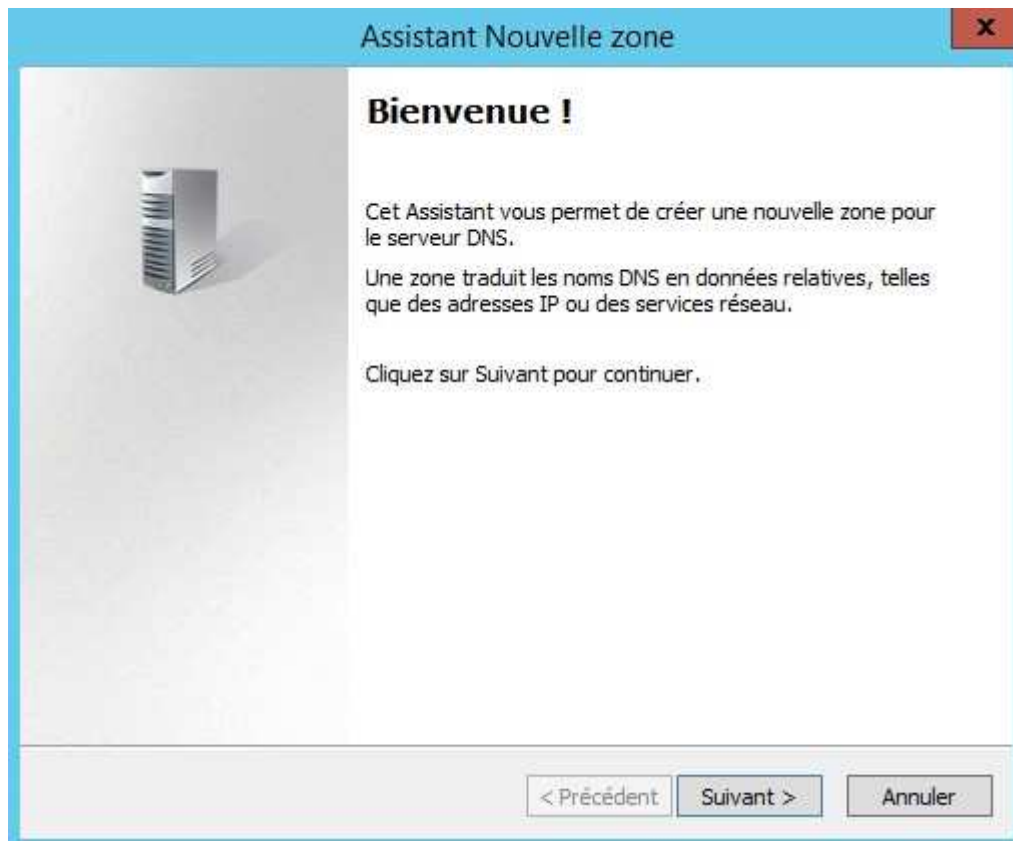
Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

Cliquez sur « Terminer ». Il reste à créer la zone de recherche inversée et son pointeur.



Faites un clic droit sur « Zones de recherche inversée » et cliquez sur « Nouvelle zone... »





Cliquez sur « Suivant »

Choisissez la première option « Zone principale » et cliquez sur « Suivant ».

**Assistant Nouvelle zone** ✕

---

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

☒ Zone de recherche inversée IPv4  
☐ Zone de recherche inversée IPv6

< Précédent Suivant > Annuler

Sélectionnez la première option « Zone de recherche inversée IPv4 ». Cliquez sur « Suivant ».

**Assistant Nouvelle zone** ✕

---

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

☒ ID réseau :

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

☐ Nom de la zone de recherche inversée :

< Précédent Suivant > Annuler

Entrez l'identifiant réseau qui est « 192.168.1 » et faites « Suivant ».

### Assistant Nouvelle zone

**Fichier zone**

Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

☒ Créer un nouveau fichier nommé :

1.168.192.in-addr.arpa.dns

☐ Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent
Suivant >
Annuler

Laissez le nom enregistré et cliquez sur « Suivant ».

### Assistant Nouvelle zone

**Mise à niveau dynamique**

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.


Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)

Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées

Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

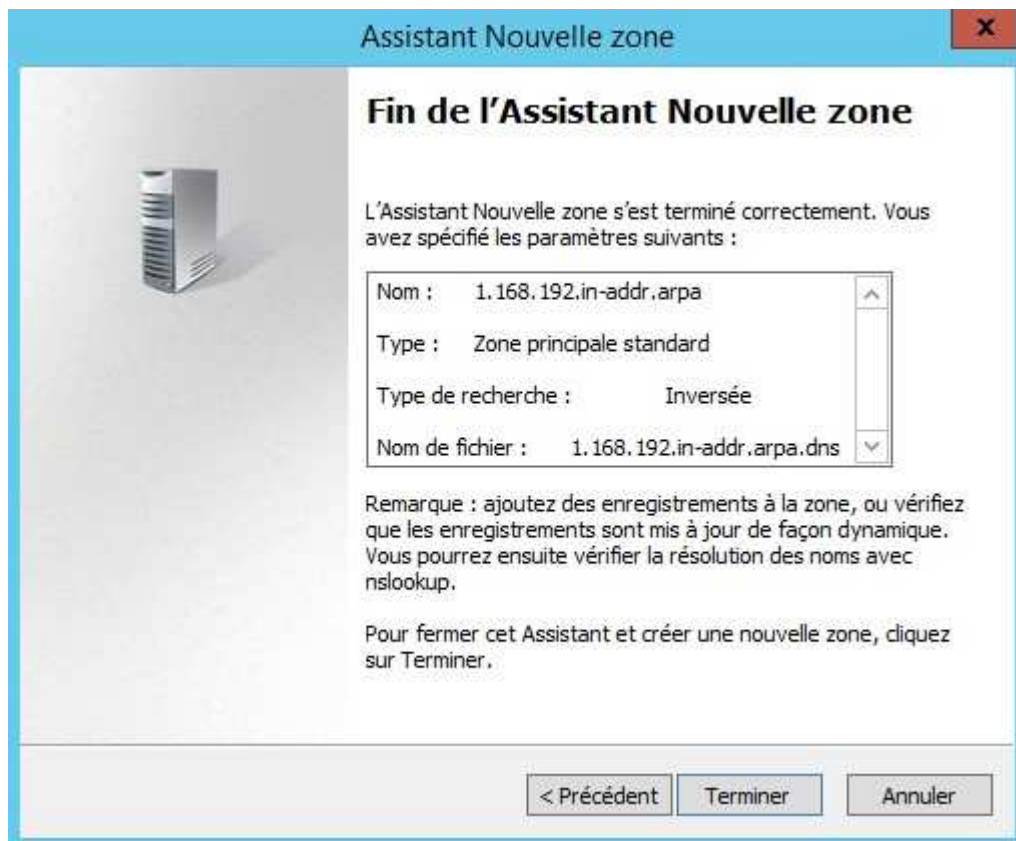
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☐ Ne pas autoriser les mises à jour dynamiques

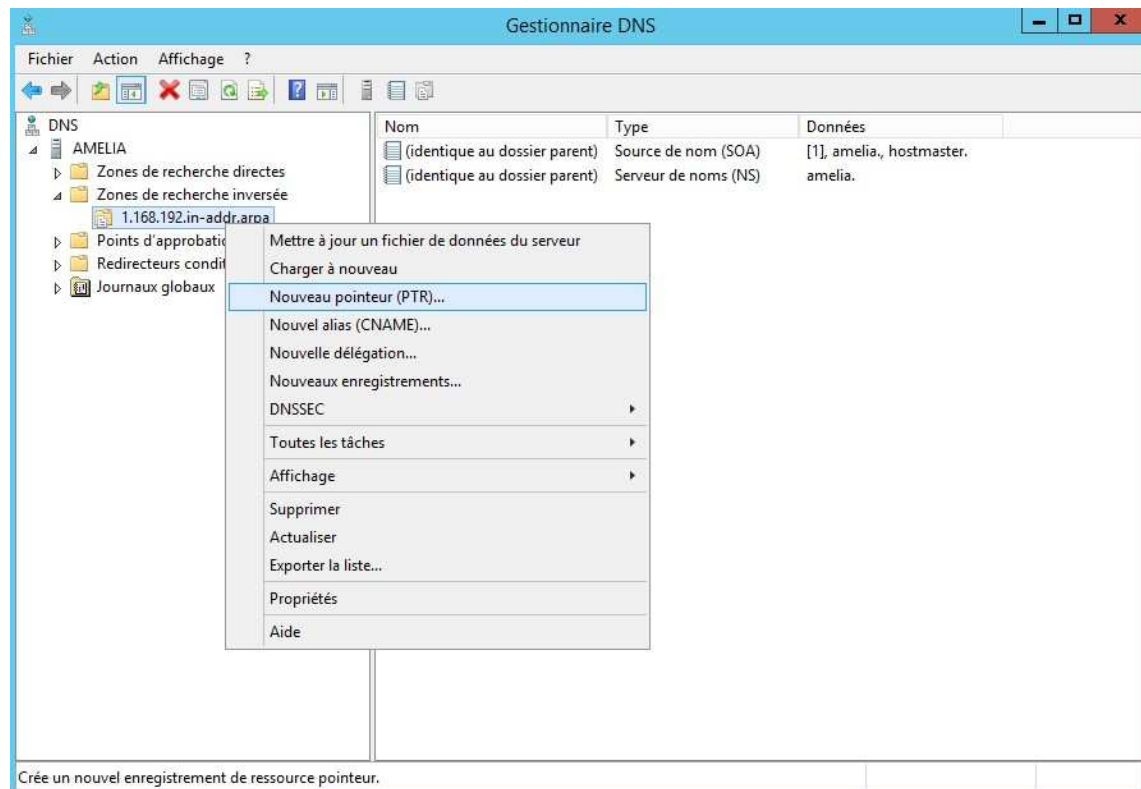
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent
Suivant >
Annuler

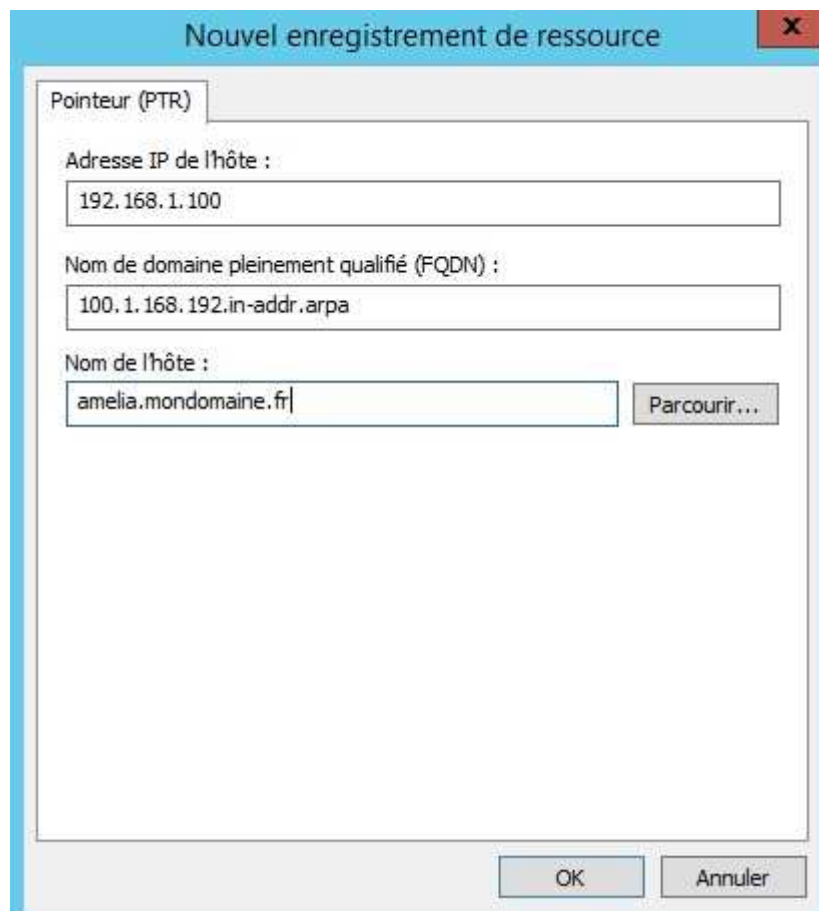
Choisissez la première option non grisée « Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées ».



Cliquez sur « Terminer ». La zone de recherche inversée est créée, il ne reste que le pointeur à mettre.



Dans l'arborescence du DNS, faites un clic droit sur votre zone de recherche inversée, ici "1.168.192.in-addr.arpa" et cliquez sur « Nouveau pointeur ».

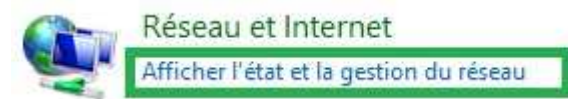




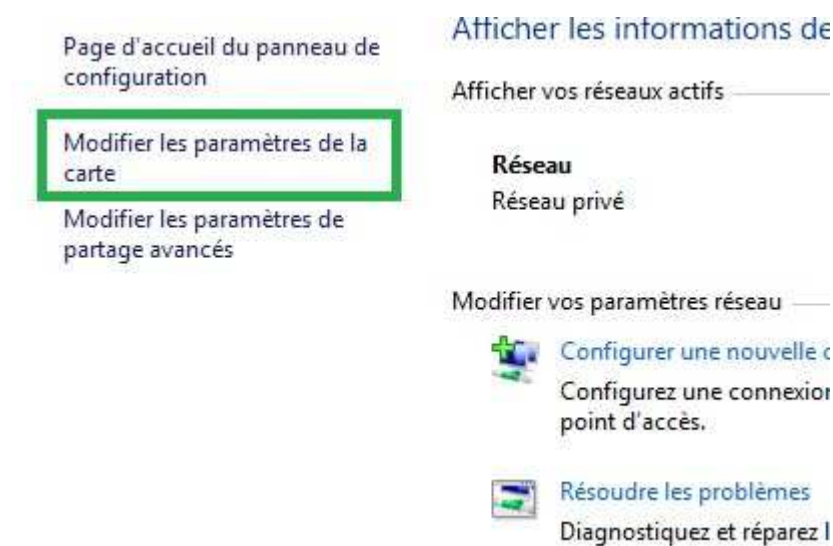
On y renseigne l'adresse IP de notre serveur et le nom d'hôte complet (nomdelamachine.nomdudomaine). Cliquez ensuite sur « OK ».

## 2.3 Vérification du DNS par NSLOOKUP

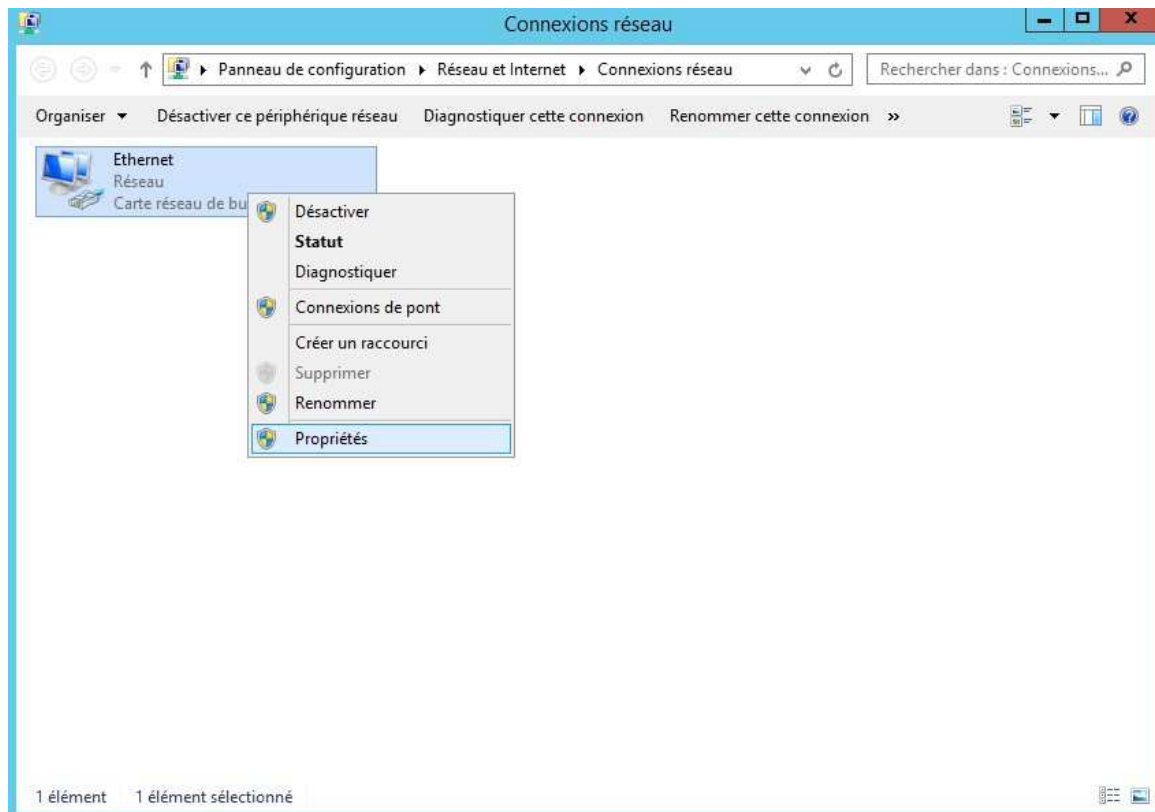
Pour vérifier que notre DNS fonctionne, définissez votre serveur comme DNS principal dans les paramètres de sa carte réseau. Pour cela, allez dans les paramètres TCP/IP de votre carte. Pour ce faire, allez dans le « Panneau de configuration ».



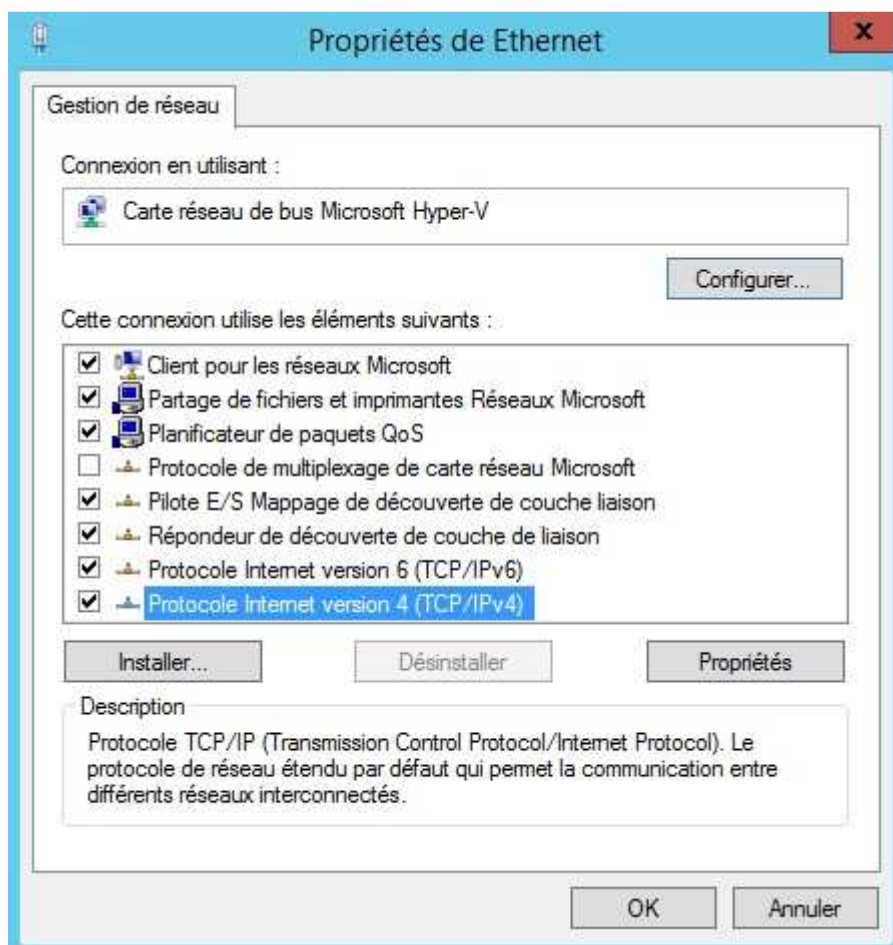
Cliquez sur « Afficher l'état et la gestion du réseau » en dessous de « Réseau et Internet ».



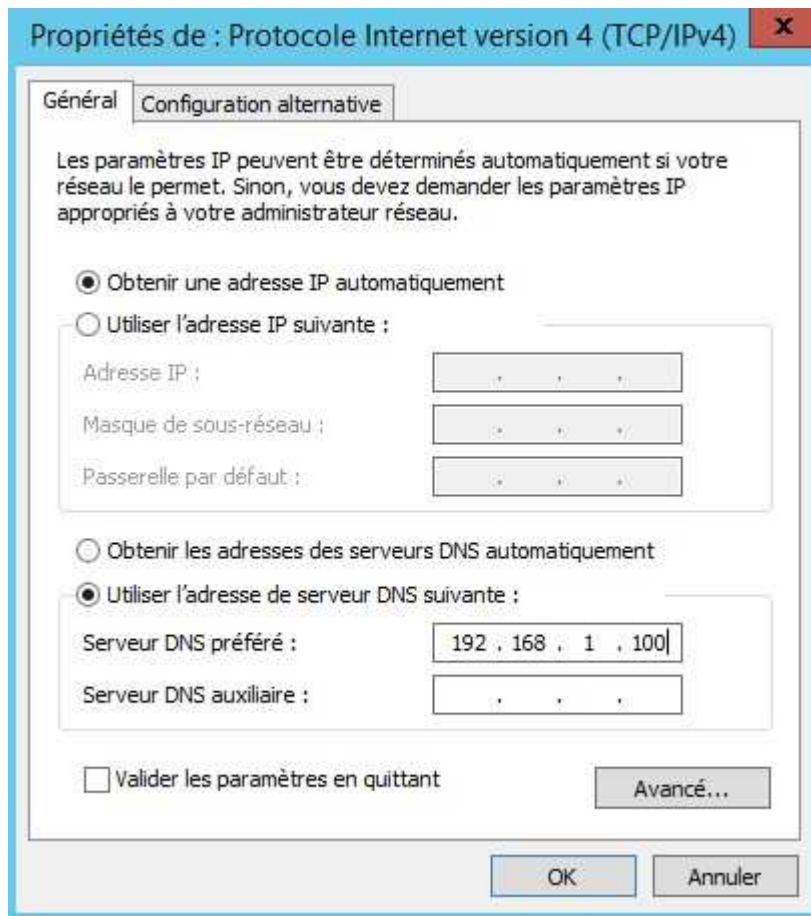
En haut à gauche, cliquez sur « Modifier les paramètres de la carte ».



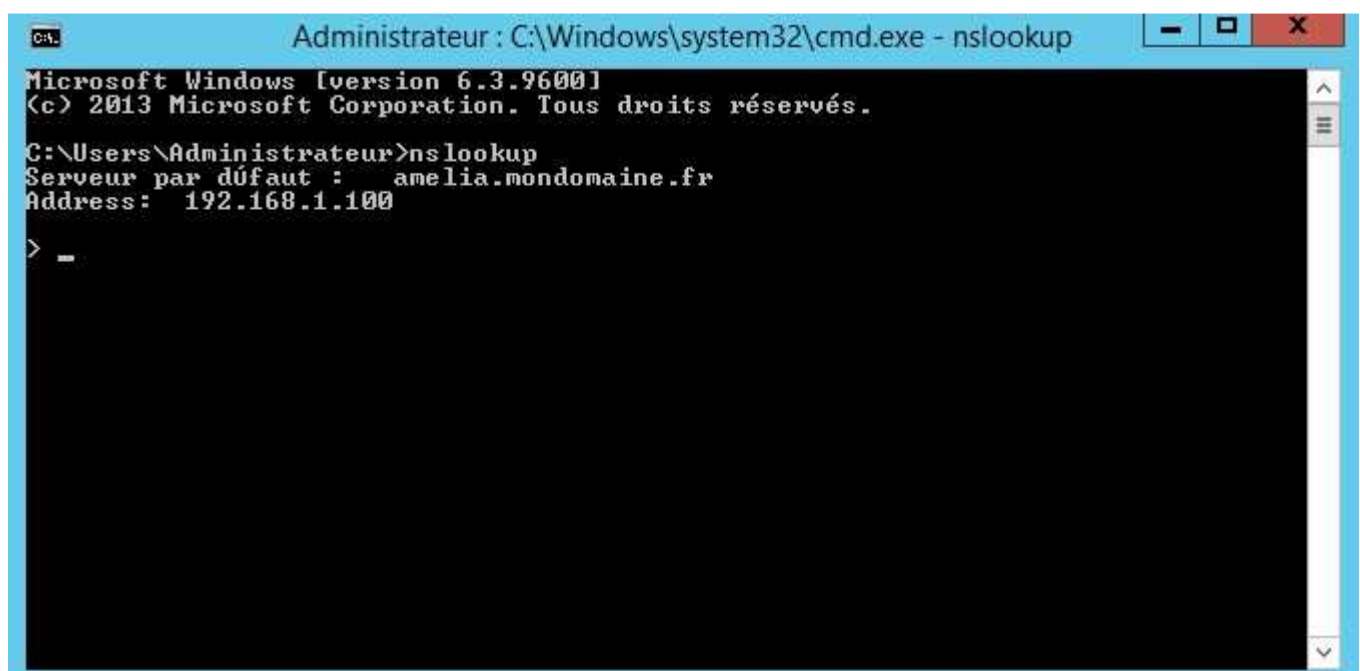
Faites un clic droit sur votre carte réseau et cliquez sur « Propriétés ».



Double-cliquez sur « Protocole Internet version 4 ».



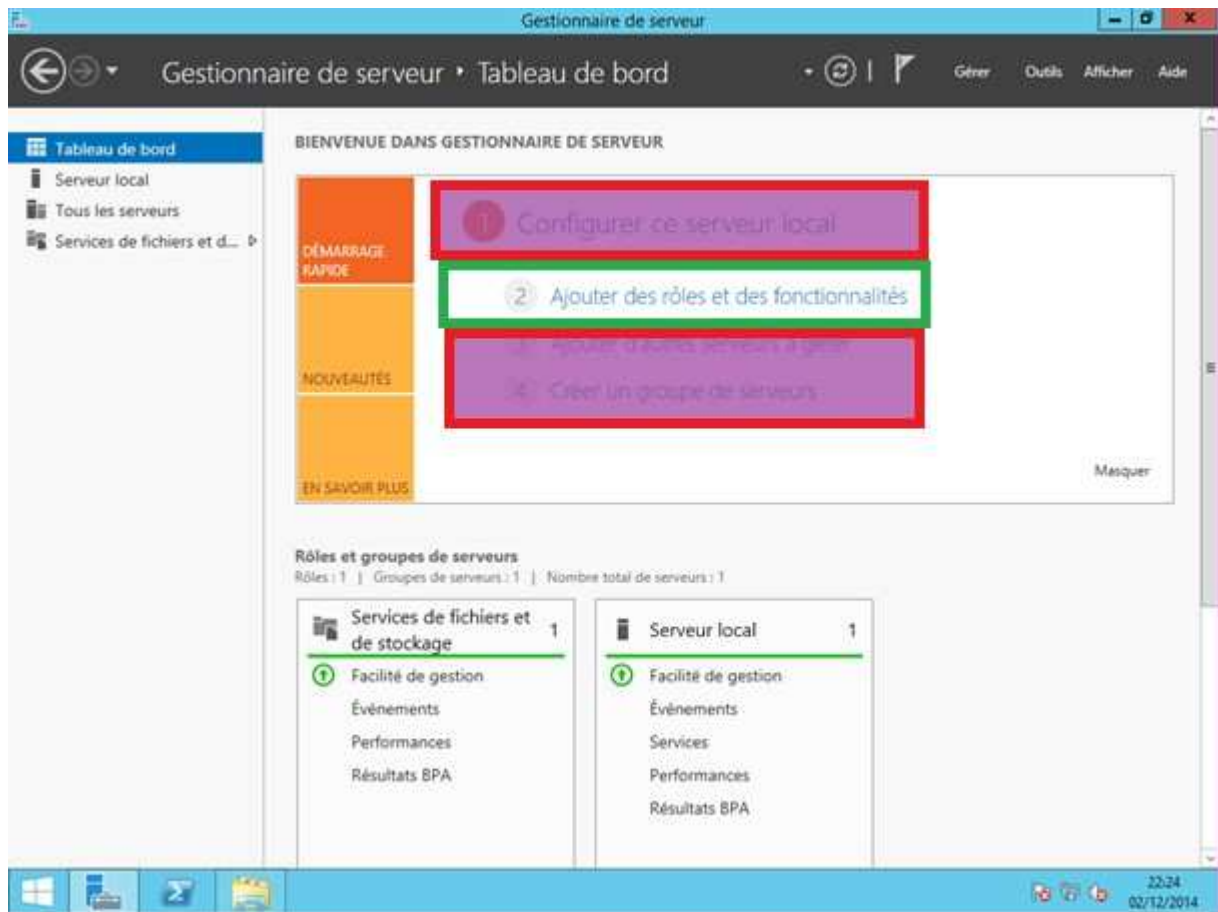
Dans les propriétés du protocole, renseignez le serveur DNS préféré avec l'adresse IP de notre serveur. Ensuite faite « OK » et fermez toutes les fenêtres. Lancez une invite de commande et la tapez la commande suivante « nslookup ».



Le résultat de la commande nous indique que nous avons correctement configuré le DNS. Nous pouvons désormais promouvoir notre serveur amelia en contrôleur de domaine. Pour ce faire, nous allons lui installer le rôle « Active Directory DS ».

## 2.4 Installation de l'Active Directory Domain Service

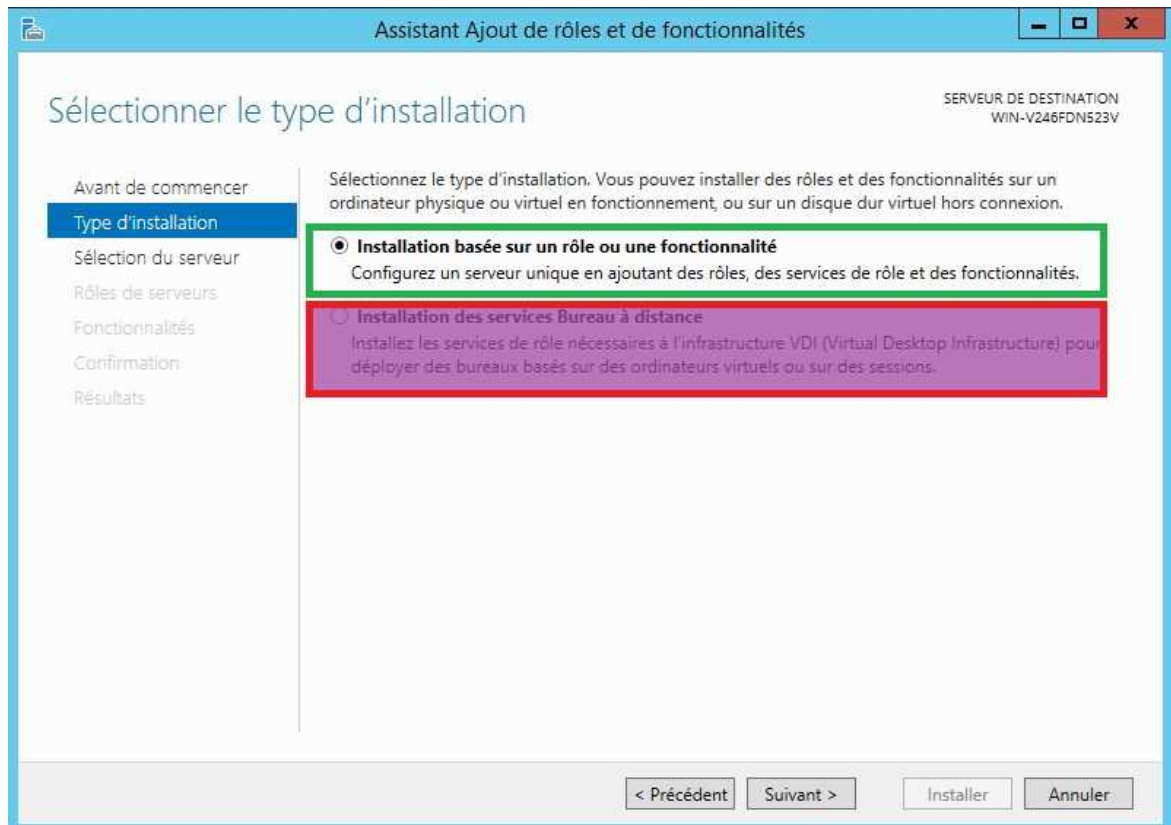
Les services de domaine Active Directory (AD DS, Active Directory Domain Services) stockent les données d'annuaire et gèrent les communications entre les utilisateurs et les domaines, y compris les processus d'ouverture de session utilisateur, l'authentification et les recherches dans l'annuaire.



Dans la page du « Gestionnaire de serveur », cliquez sur « Ajouter des rôles et des fonctionnalités ».

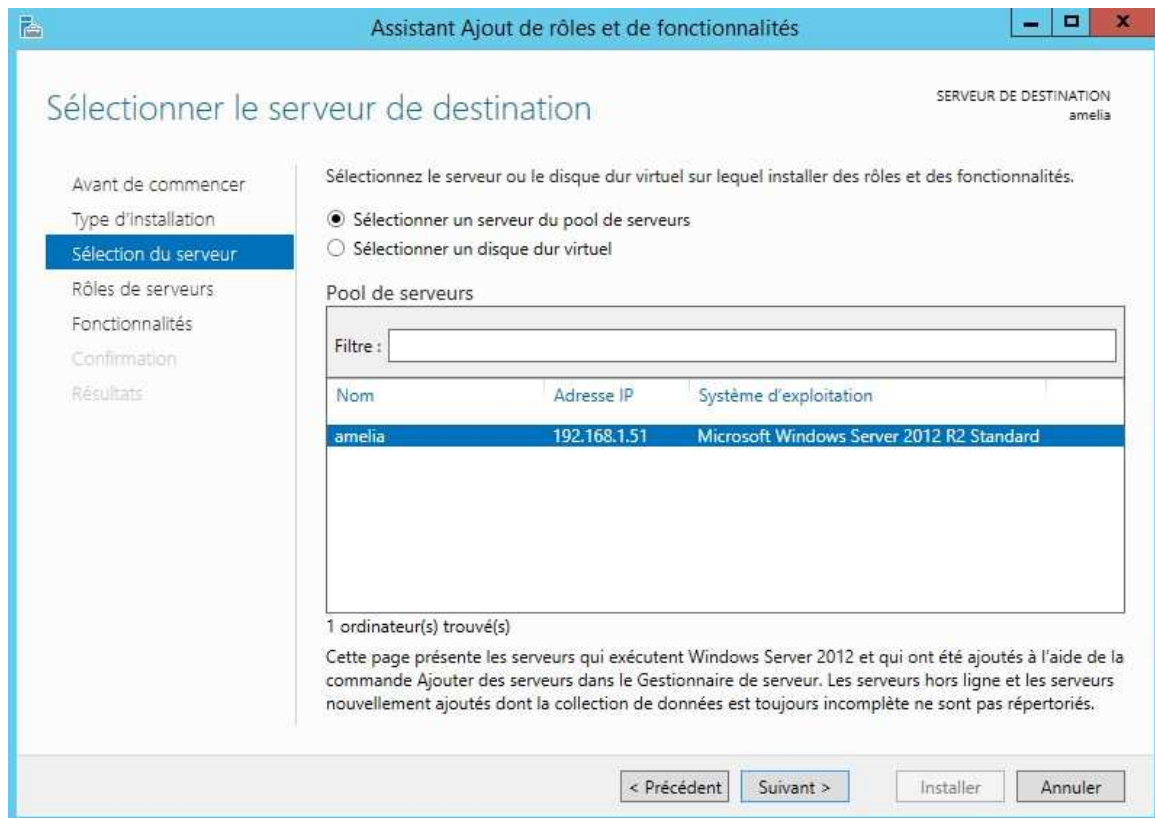


Cliquez sur « Suivant ».

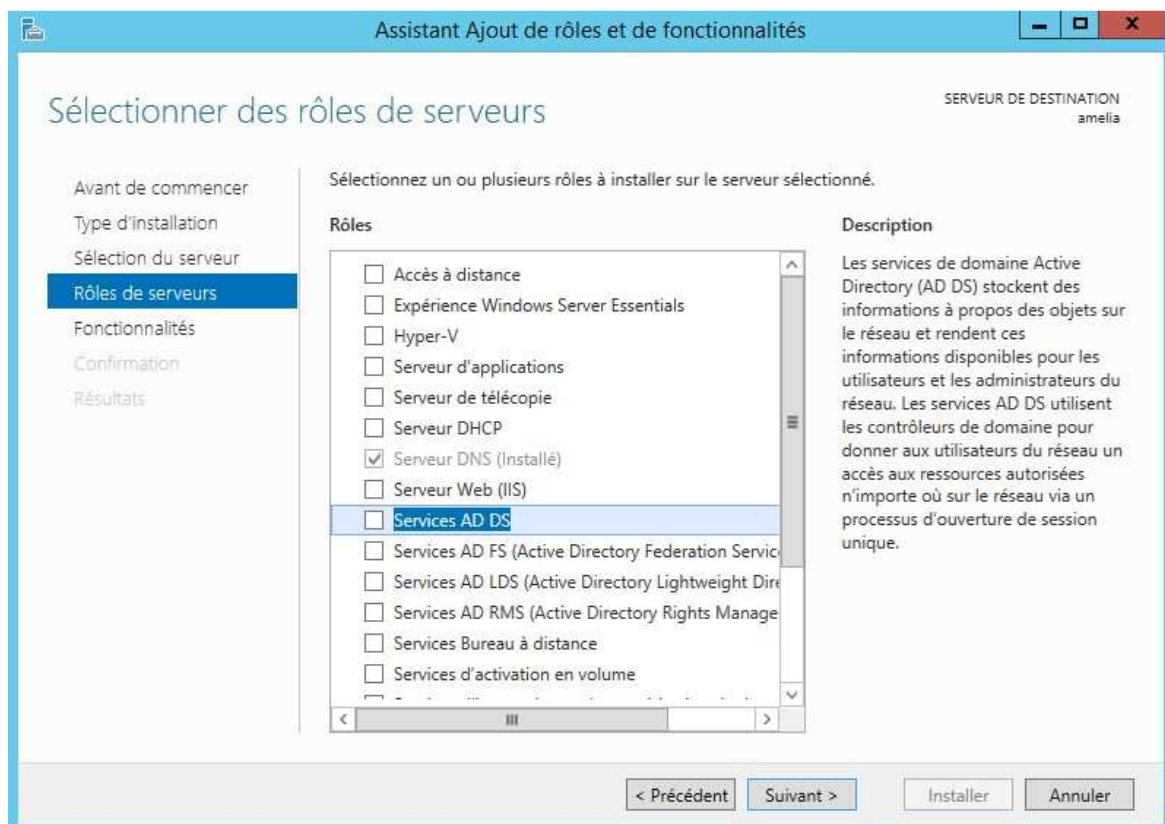


Choisissez l'option « Installation basée sur un rôle ou une fonctionnalité »

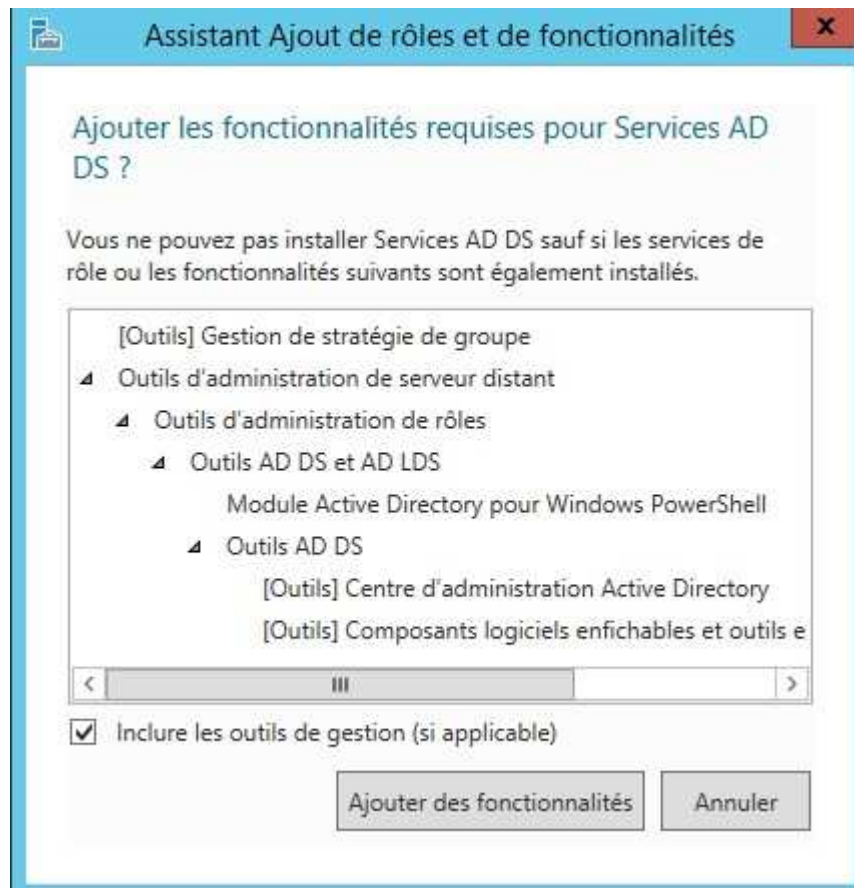




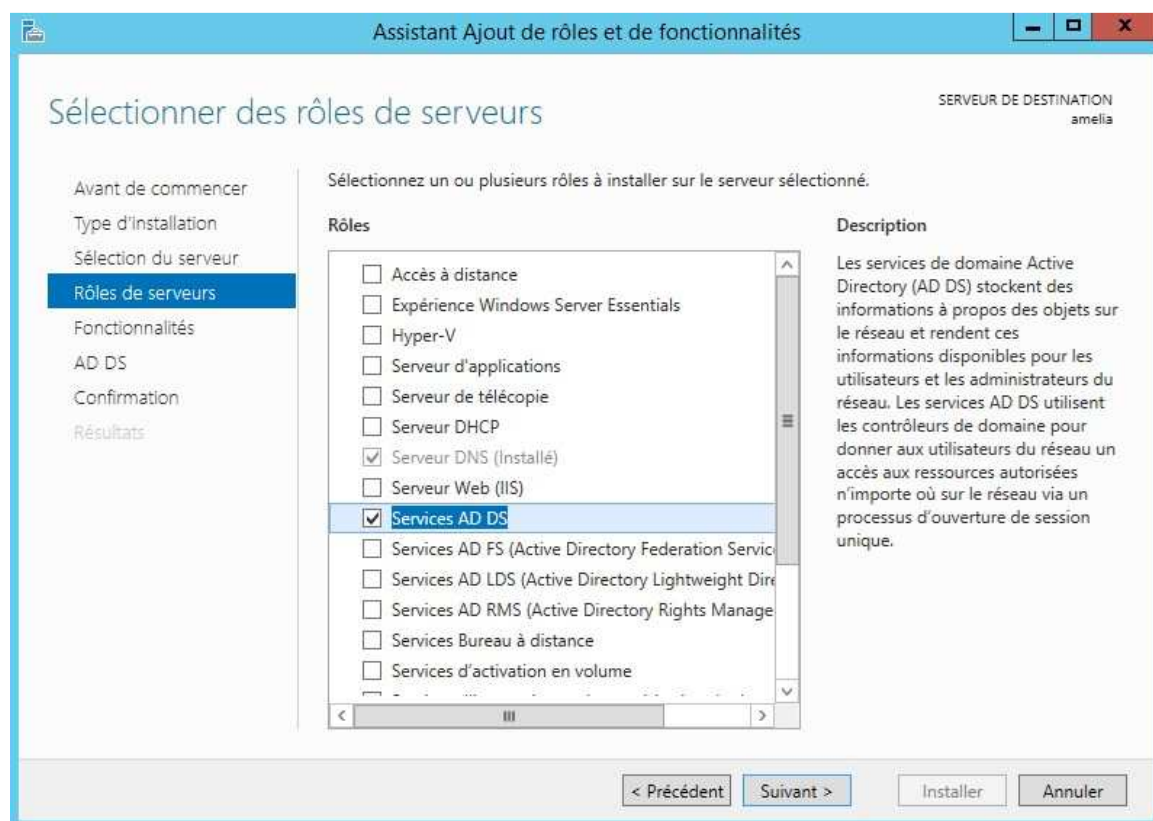
Sélectionnez votre serveur dans la liste et faites « Suivant ».



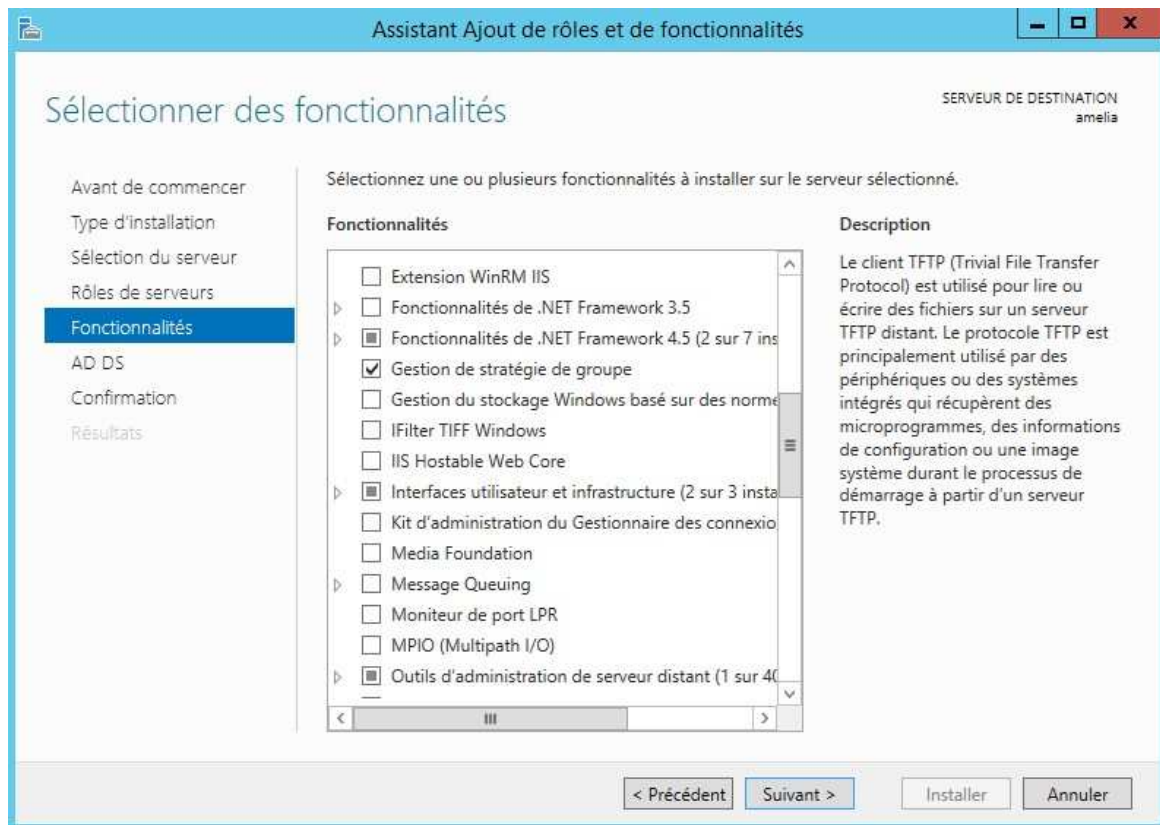
Sélectionnez le rôle « Services AD DS ».



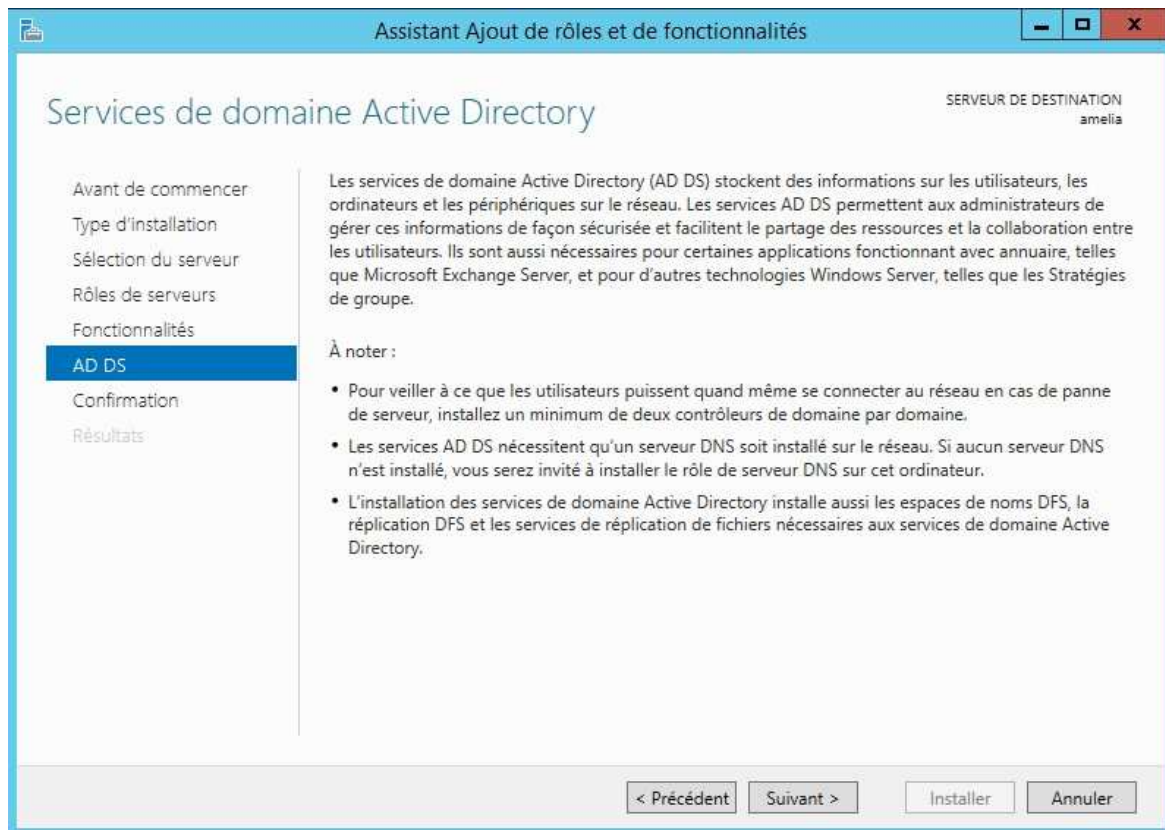
Cliquez sur « Ajoutez les fonctionnalités »



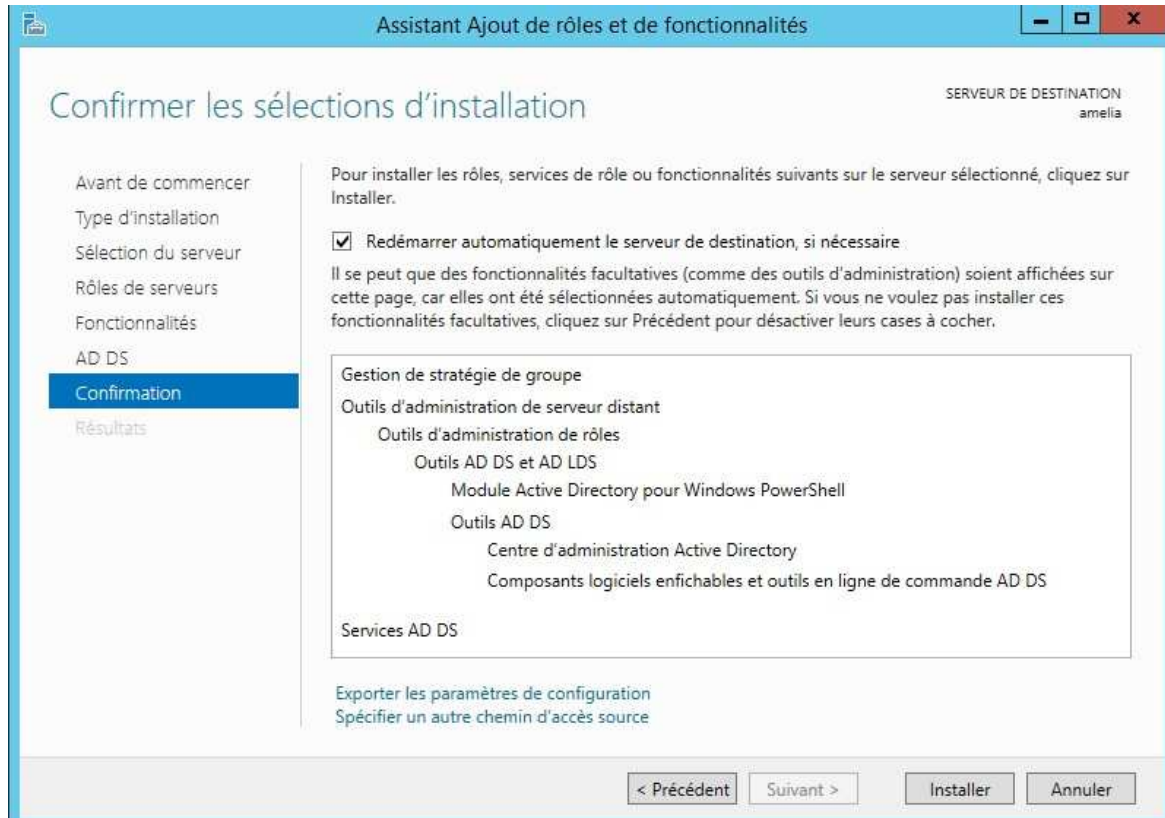
Faites « Suivant ».



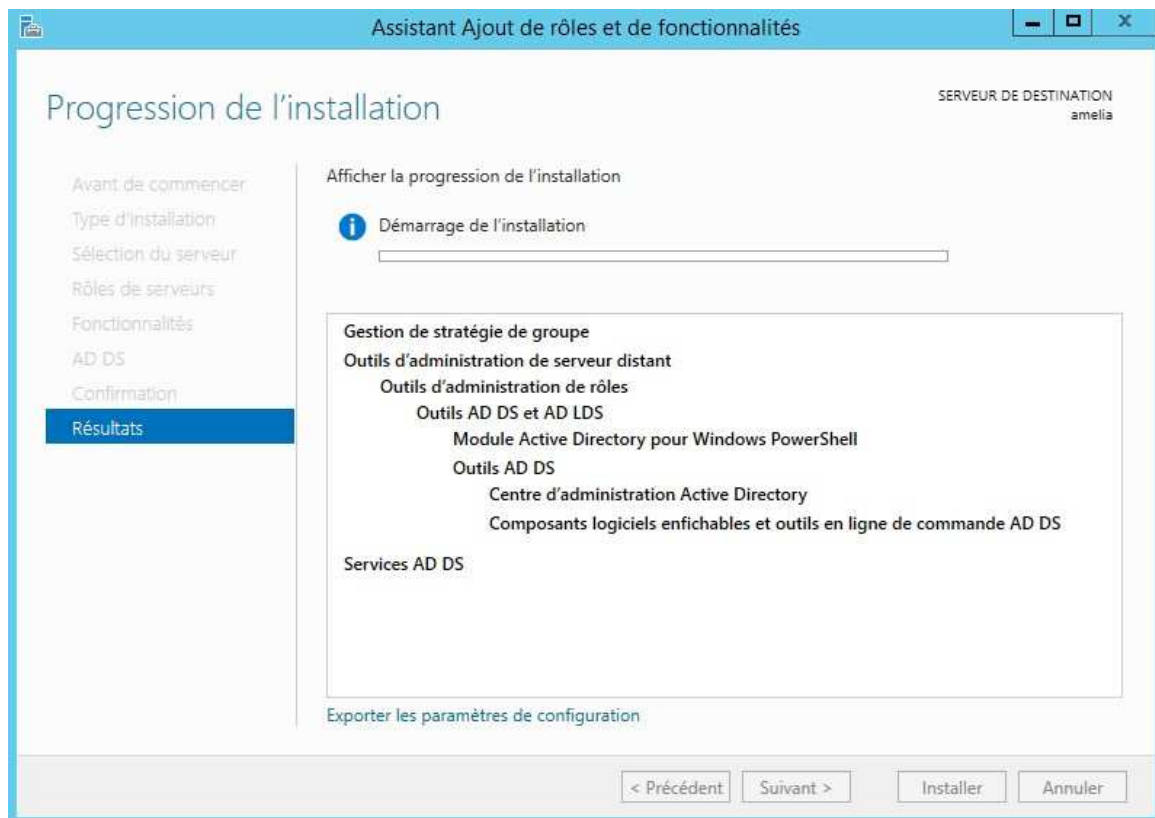
Vous pouvez jeter un œil aux fonctionnalités qui vont être installées et qui sont nécessaires au rôle AD DS. Après faites « Suivant ».



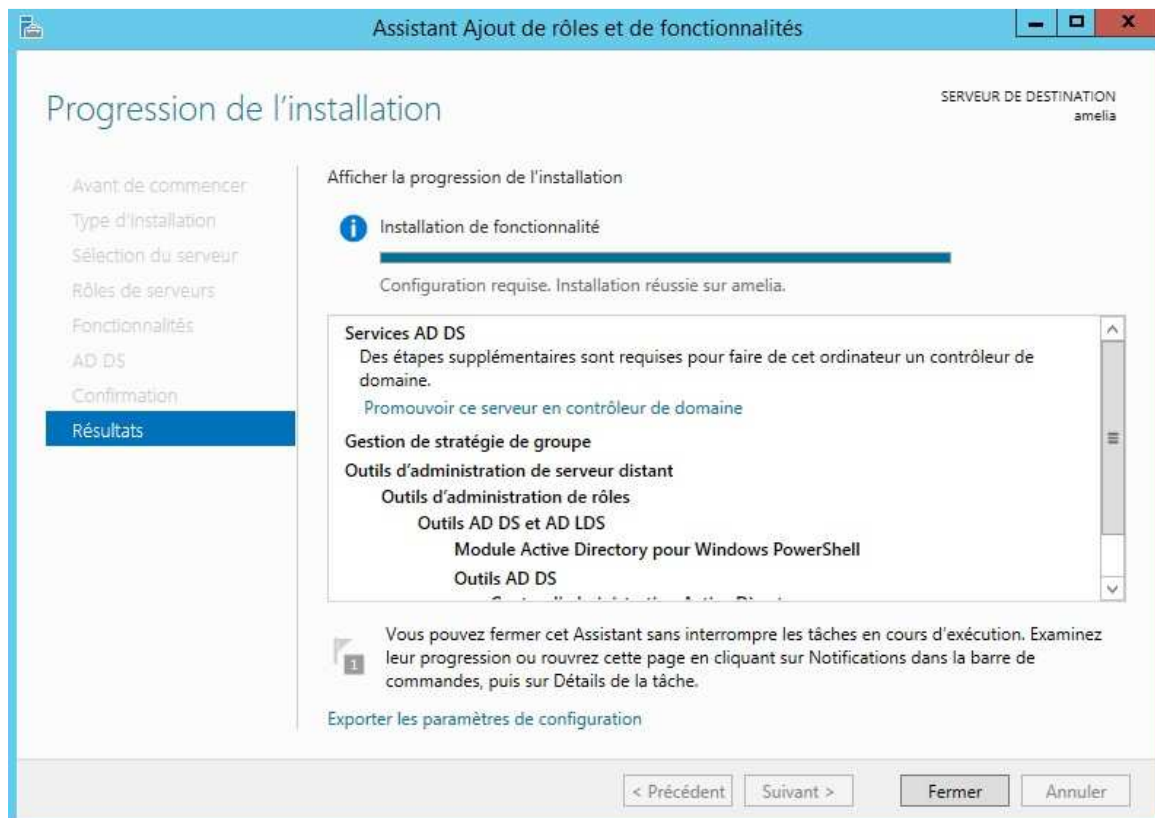
Faites « Suivant ».



Cochez la case « Redémarrer automatiquement le serveur de destination si nécessaire » et cliquez sur « Installer ».



L'installation va débiter.





A la fin de l'installation, nous pouvons désormais promouvoir notre serveur en contrôleur de domaine.

## 2.5 Promotion en contrôleur de domaine

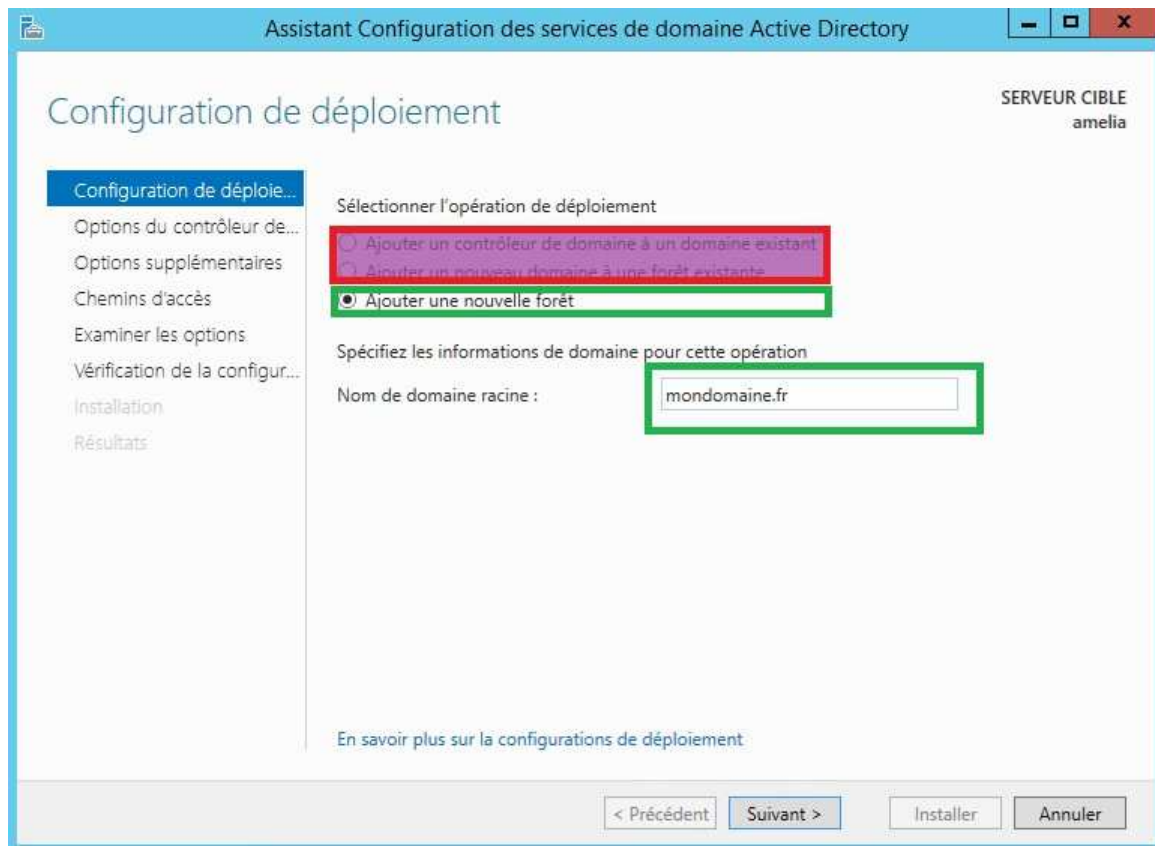
### Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

Promouvoir ce serveur en contrôleur de domaine

Gestion de stratégie de groupe

Toujours dans la même fenêtre Cliquez sur « Promouvoir ce serveur en contrôleur de domaine ». L'assistant nous propose ici l'équivalent du très connu « DCPROMO ».



Choisissez la troisième option « Ajouter une nouvelle forêt » et spécifiez un nom pour votre domaine racine, ici ce sera « mondomaine.fr ». Faites « Suivant ».

Assistant Configuration des services de domaine Active Directory

## Options du contrôleur de domaine

SERVEUR CIBLE  
amelia

- Configuration de déploiement
- Options du contrôleur de domaine**
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration
- Installation
- Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2012 R2

Niveau fonctionnel du domaine : Windows Server 2012 R2

Spécifier les fonctionnalités de contrôleur de domaine

- ☒ Serveur DNS (Domain Name System)
- ☒ Catalogue global (GC)
- ☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

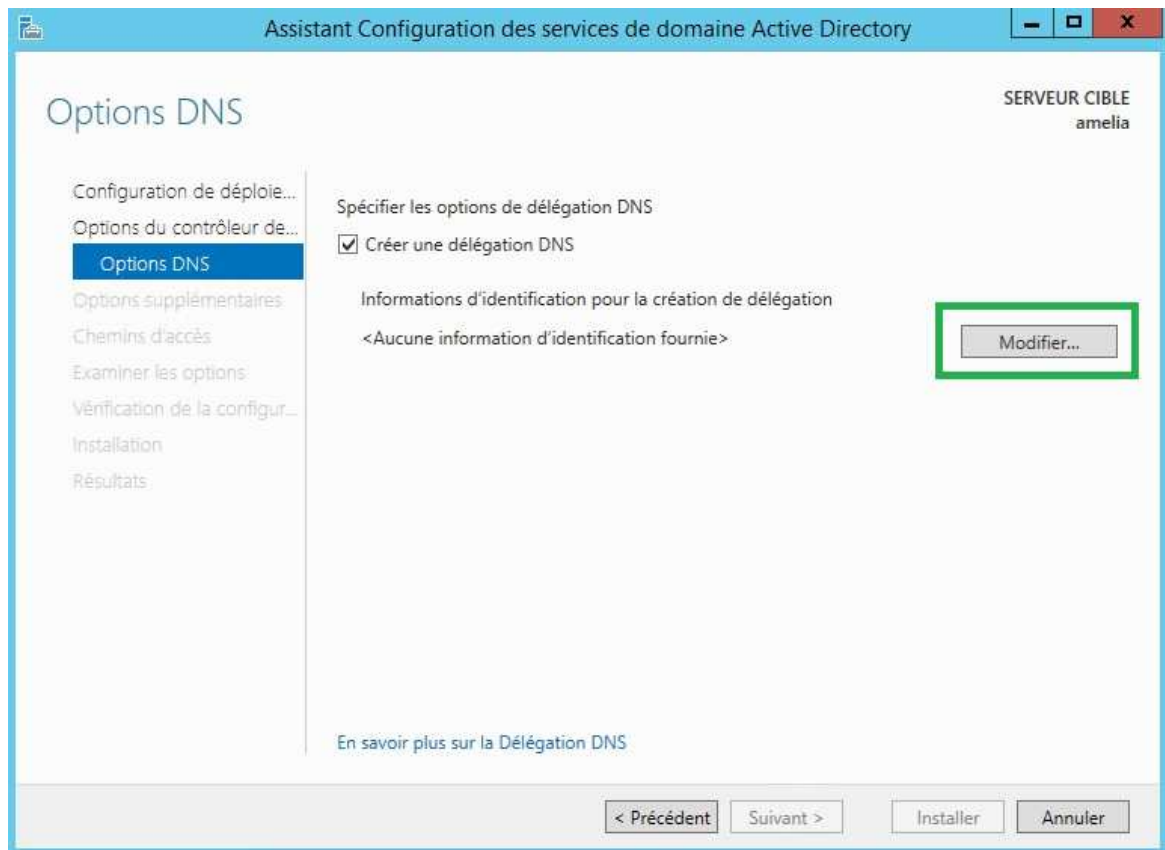
Mot de passe : .....

Confirmer le mot de passe : .....

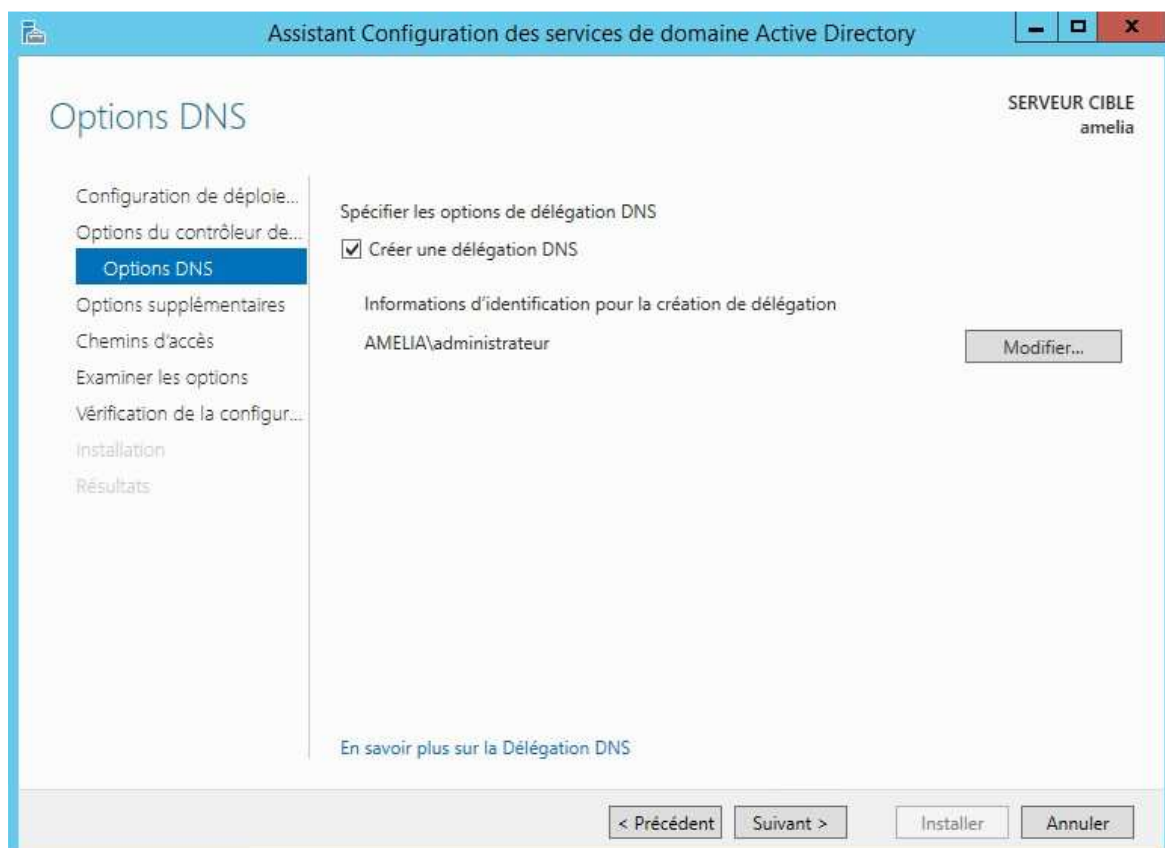
[En savoir plus sur la options du contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

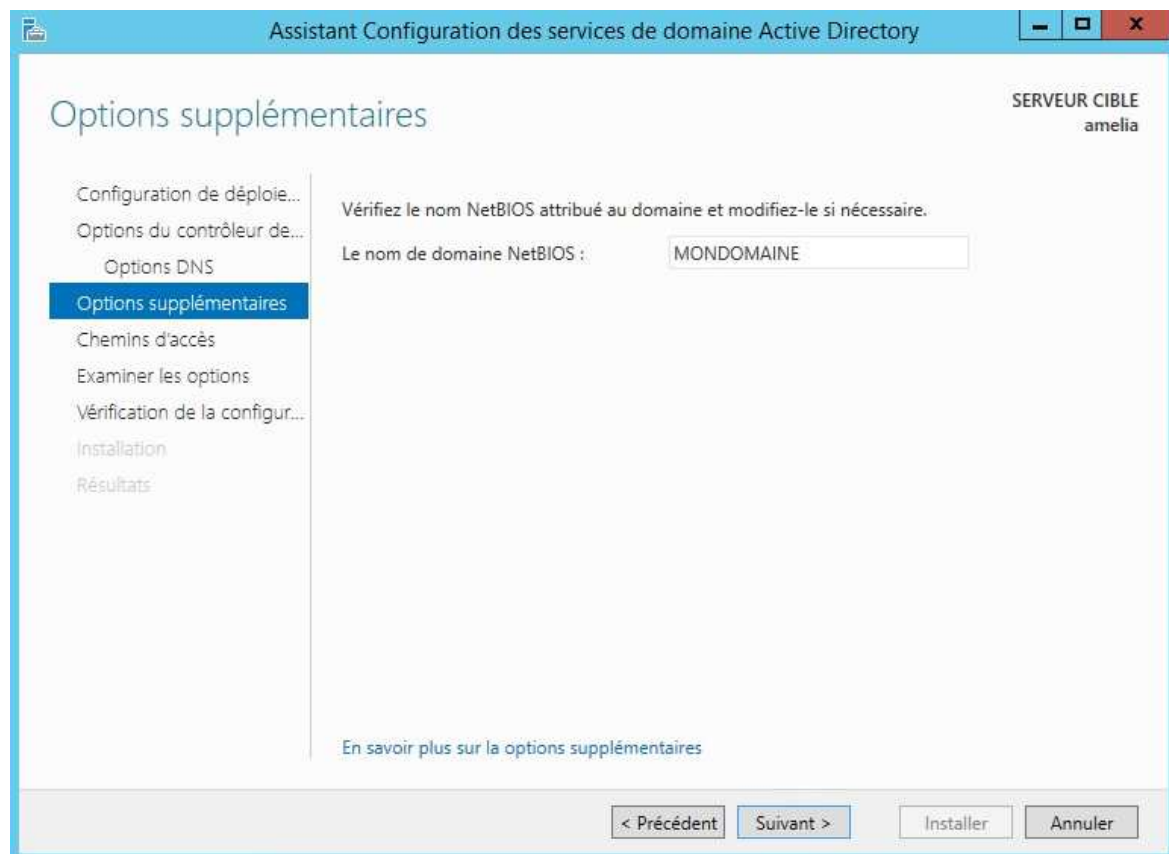
Nous comptons n'installer que des serveurs exécutant Windows Server 2012 R2 donc nous pouvons laisser le niveau fonctionnel tel quel. Spécifiez un mot de passe de restauration des services d'annuaire. Ce mot de passe va vous permettre de vous connecter sur d'autres contrôleurs de domaine de la forêt qui n'ont pas encore AD DS d'installé. Cliquez sur « Suivant ».



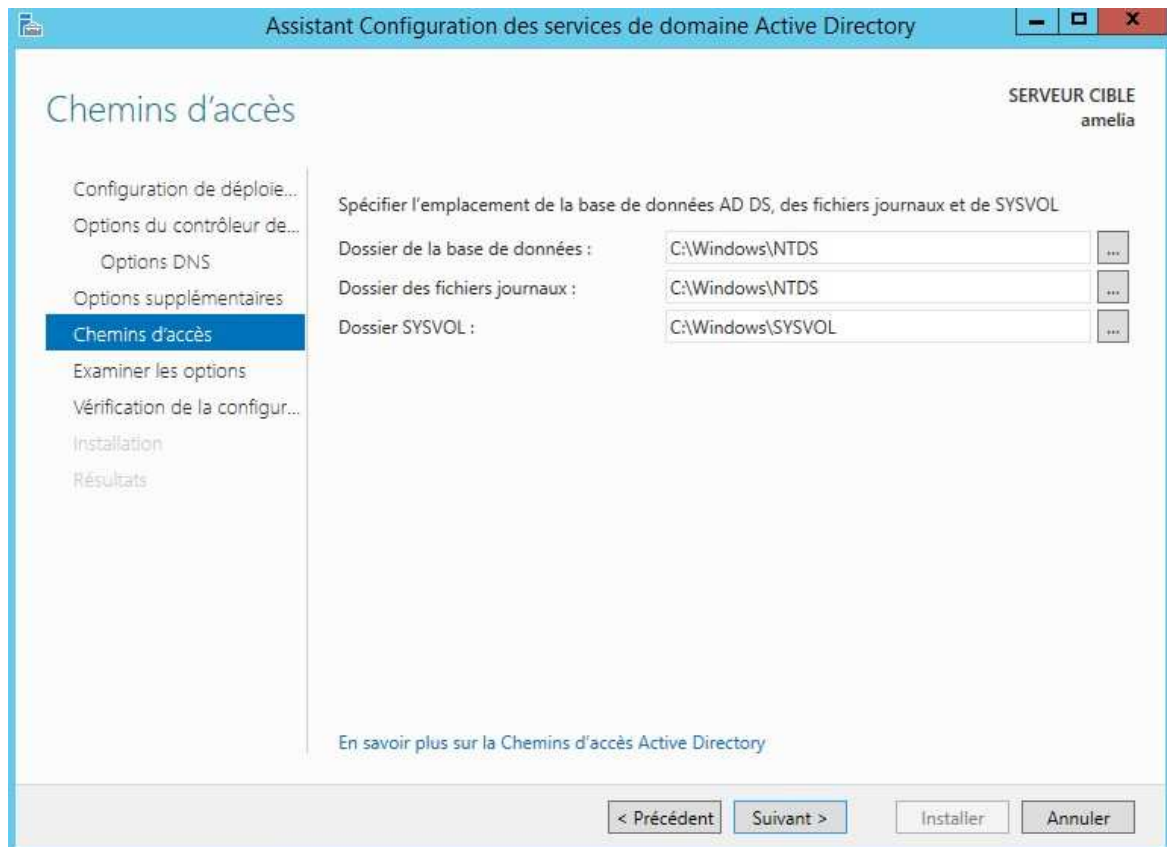
Cliquez sur le bouton « Modifier » pour y entrer ensuite les informations d'identification. Ici le nom d'utilisateur « administrateur » et son mot de passe.



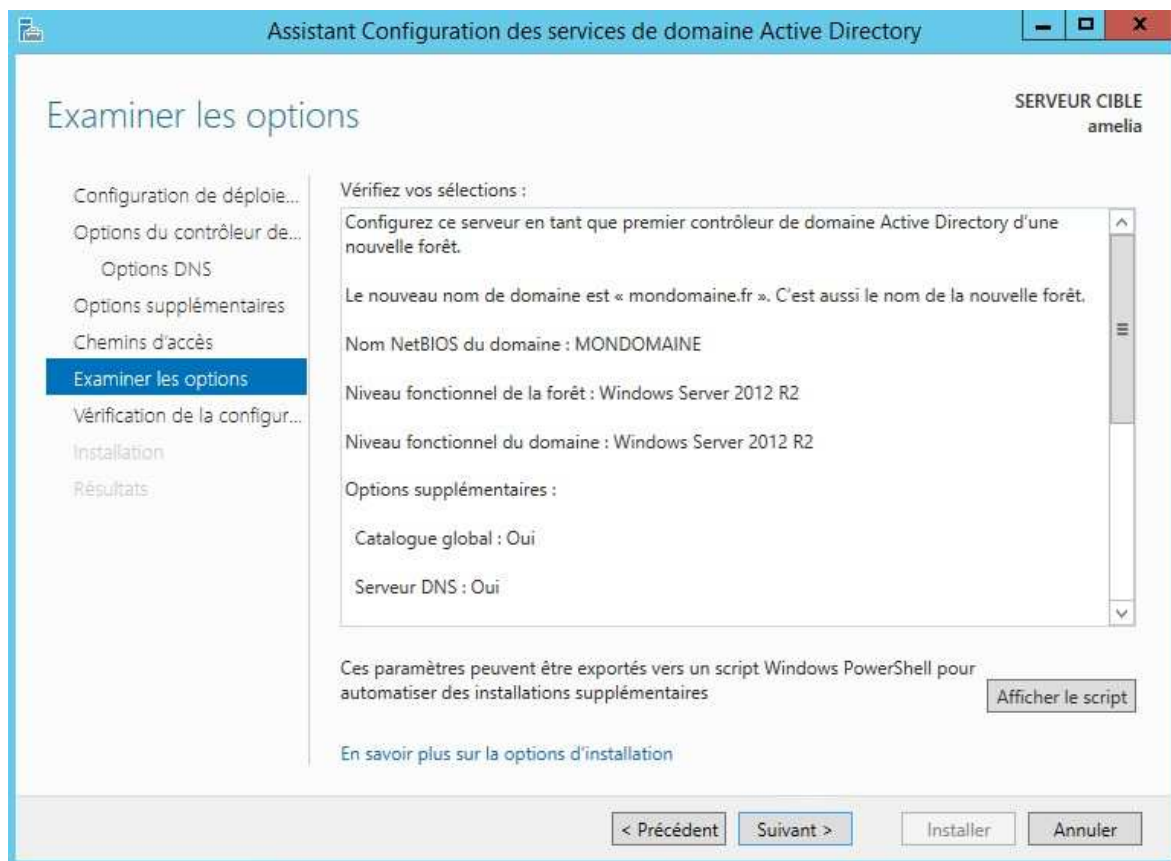
Cliquez sur « Suivant ».



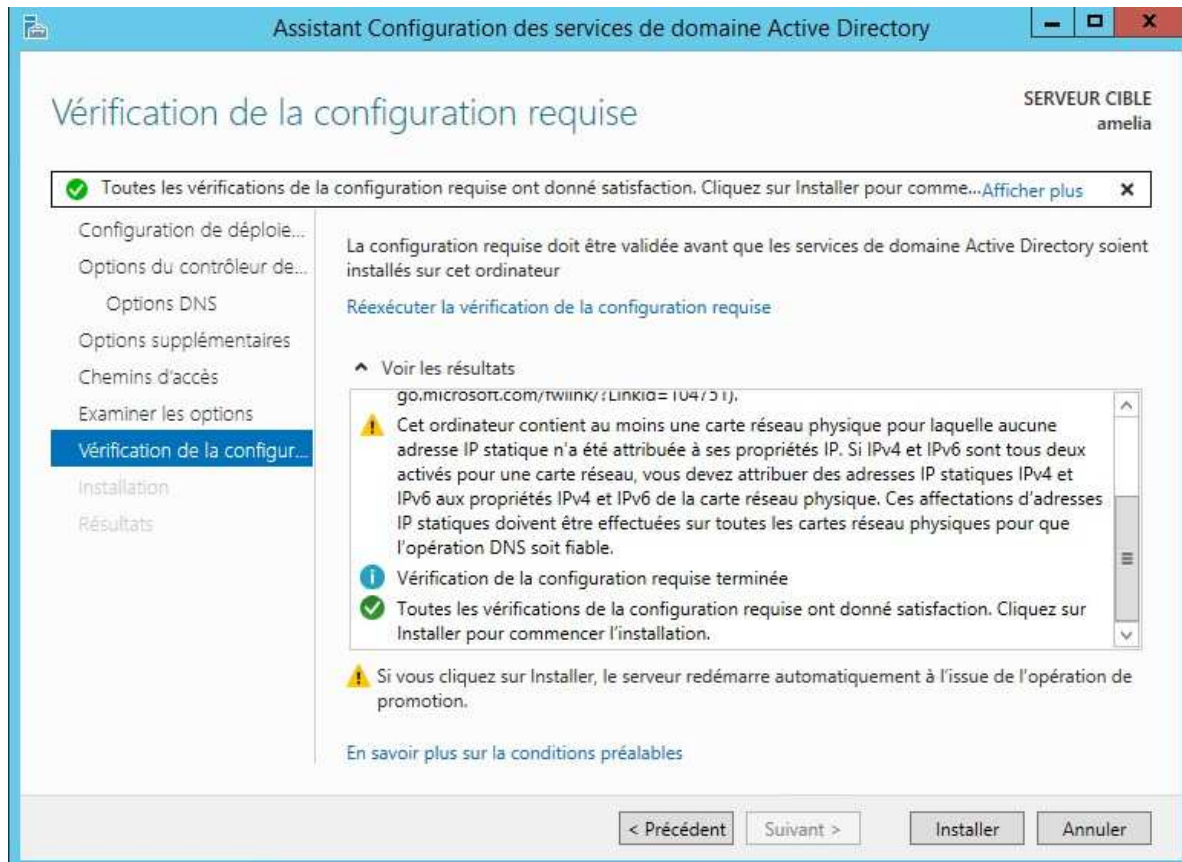
Vérifiez le nom et cliquez sur « Suivant ».



Laissez les valeurs par défaut et faite « Suivant »

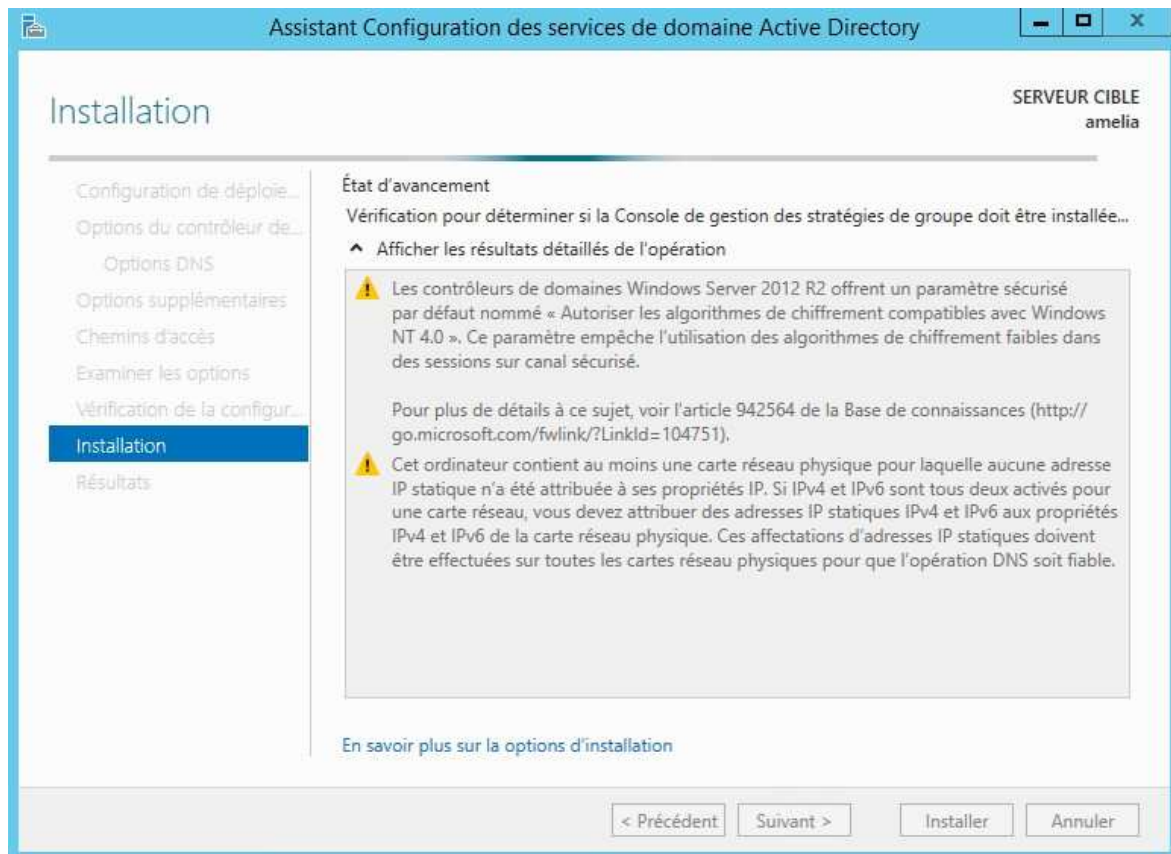


Vous pouvez vérifier ici les informations que vous avez entrées dans l'assistant. Faites « Suivant »

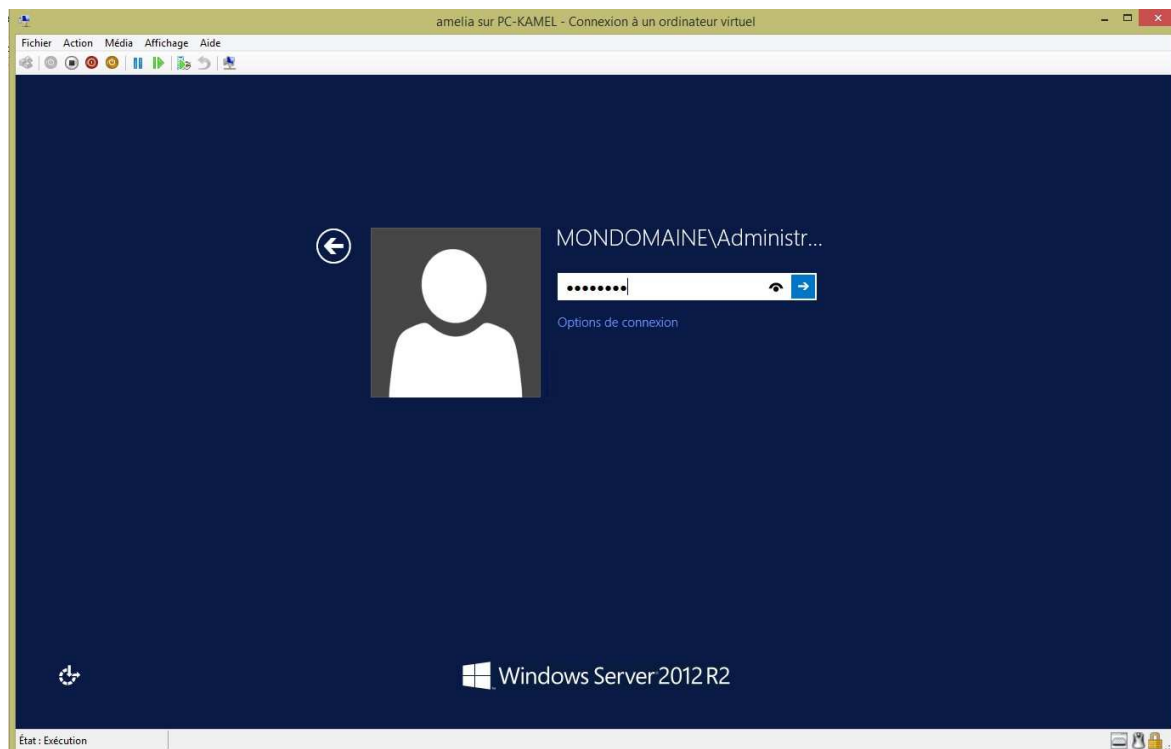


Windows m'informe de deux avertissements (chiffrement NT 4.0 et adresse IP automatique) qui n'ont cependant pas d'importance. Cliquez sur « Installer ».



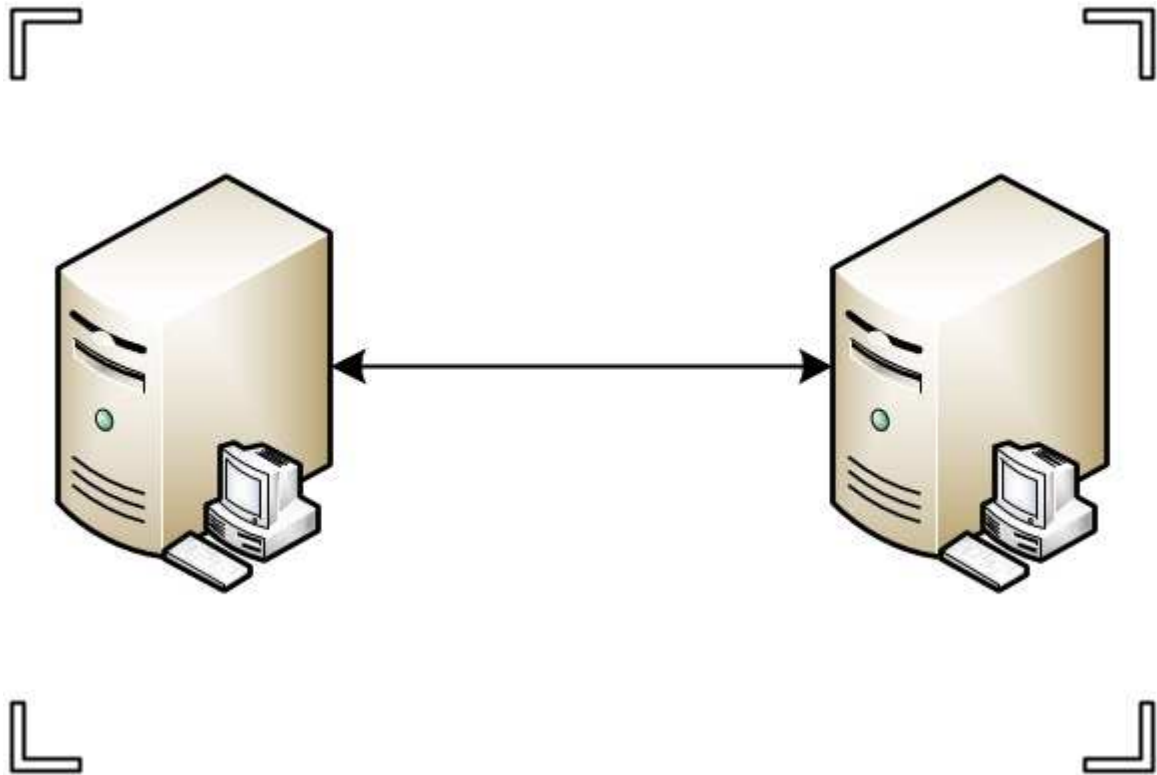


L'installation démarre. A la fin de celle-ci, votre serveur va redémarrer automatiquement.



A la fin du redémarrage, vous remarquerez que vous pouvez vous loguer désormais sur le domaine.

**Déployer un contrôleur de domaine  
secondaire**



Après avoir installé votre premier contrôleur de domaine, il est primordial de se lancer dans l'installation du serveur qui servira de contrôleur secondaire. Le système d'exploitation expliqué ici est le même que le précédent. Il s'agit ni plus ni moins d'installer les rôles similaires et de faire la jonction entre les deux.

Une fois votre serveur opérationnel (système d'exploitation Windows Server 2012 R2 installé, nom de la machine et jonction au domaine configurés), il vous faudra maintenant lui installer les rôles qui lui permettront de devenir le contrôleur de domaine secondaire et le premier rôle à installer est celui de DNS. Suite à l'installation du rôle DNS sur le serveur (si nécessaire, se référer à l'article " [Déployer un contrôleur de domaine](#) "), nous passons directement au rôle Active Directory DS. Pour l'installation de ce rôle, référez-vous à l'article précédemment cité. Une fois arrivé à l'étape "Promouvoir ce serveur en contrôleur de domaine", suivez la suite de ce tutoriel :

Assistant Configuration des services de domaine Active Directory

## Configuration de déploiement

SERVEUR CIBLE  
gargantua.mondomaine.fr

- Configuration de déploie...
- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configur...
- Installation
- Résultats

Sélectionner l'opération de déploiement

- ☒ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine :

Fournir les informations d'identification pour effectuer cette opération

MONDOMAINE\KAMSAOUBI (Utilisateur actuel)

[En savoir plus sur la configurations de déploiement](#)

< Précédent   Suivant >   Installer   Annuler

Dans l'assistant de création du nouveau contrôleur de domaine, sélectionnez la première option « Ajouter un contrôleur de domaine à un domaine existant ». Renseignez ensuite le nom de votre domaine, ici « mon domaine ». Et faites « Suivant »

Assistant Configuration des services de domaine Active Directory

## Options du contrôleur de domaine

SERVEUR CIBLE  
gargantua.mondomaine.fr

- Configuration de déploiement...
- Options du contrôleur de...**
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration...
- Installation
- Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site : Default-First-Site-Name

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

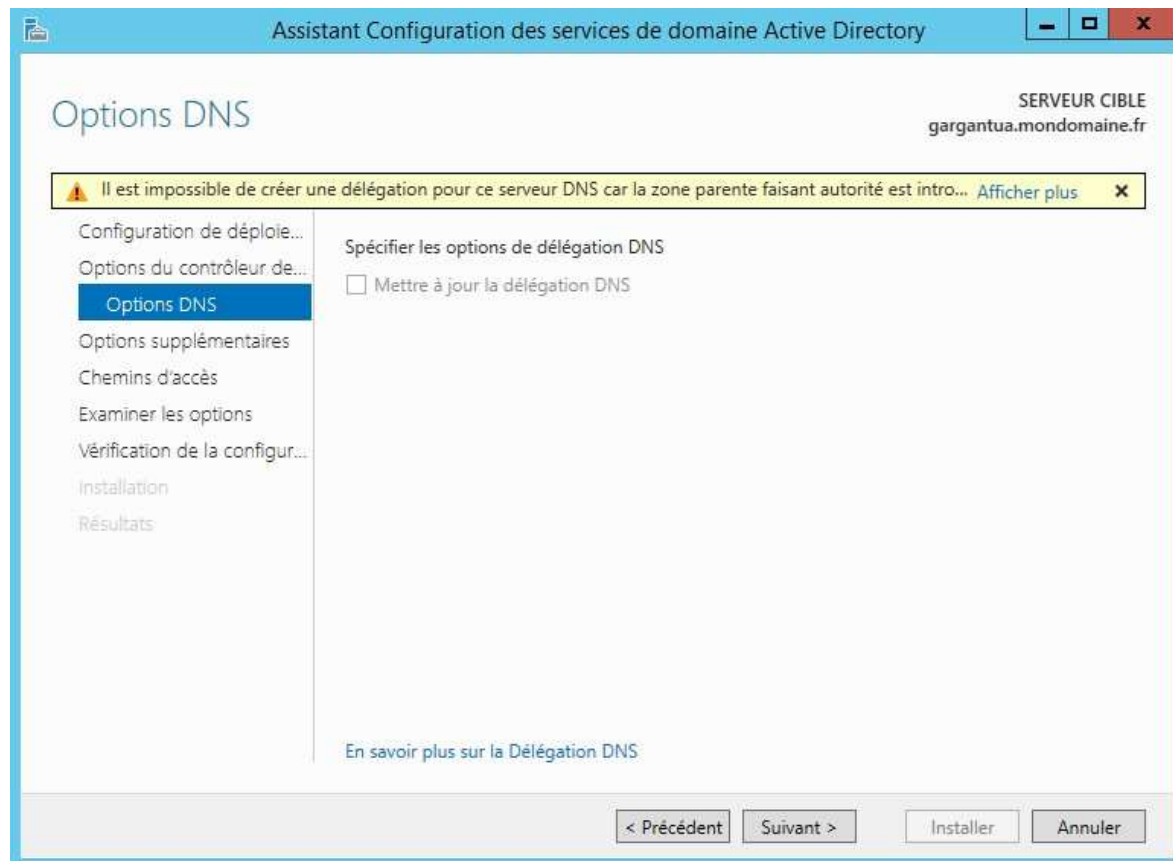
Mot de passe : .....

Confirmer le mot de passe : .....

[En savoir plus sur la options du contrôleur de domaine](#)

< Précédent   Suivant >   Installer   Annuler

Renseignez le mot de passe du mode de restauration des services d'annuaire (vous l'avez rentré lors du déploiement de votre contrôleur de domaine principal) et laissez les cases cochées par défaut.

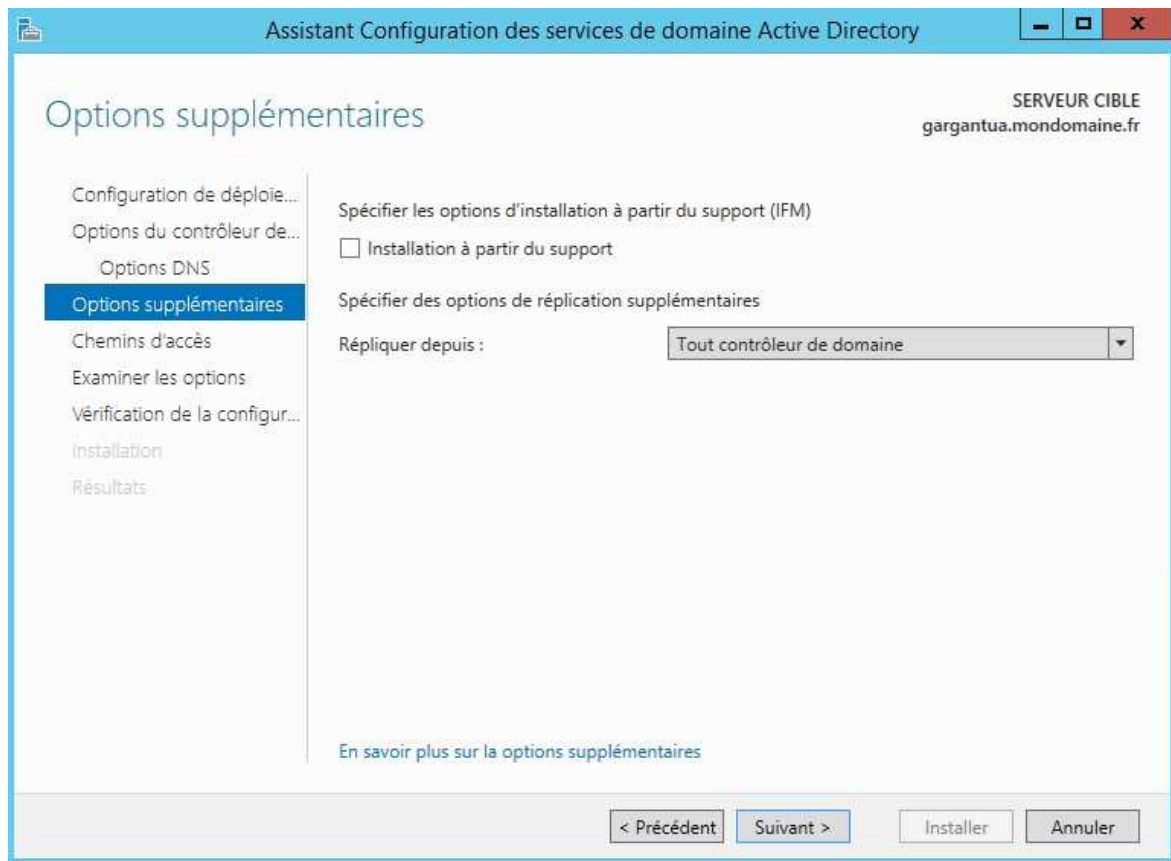


Un message d'erreur apparaît nous indiquant qu'il est impossible de créer une délégation pour notre serveur DNS.

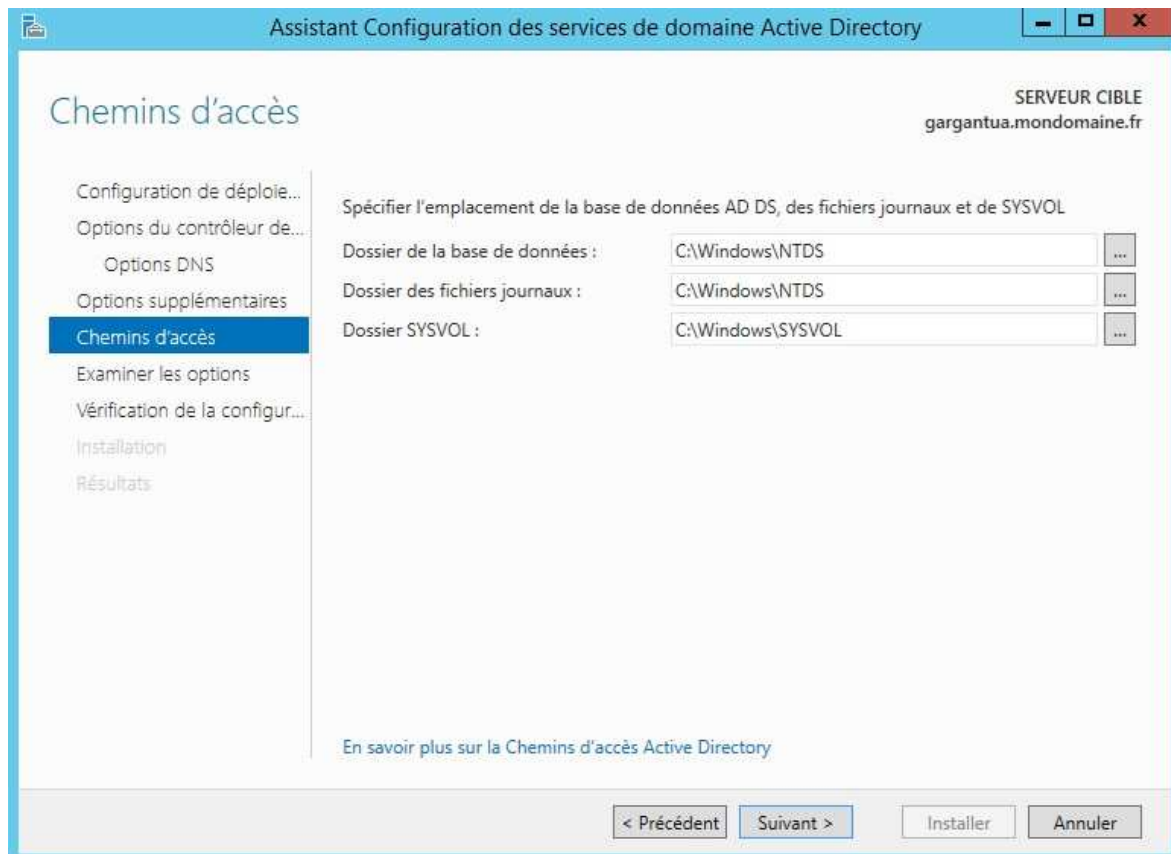
Étant donné que de nombreux domaines Active Directory ne sont pas enregistrés avec un organisme d'enregistrement Internet, ce message d'erreur peut être ignoré sans risque afin de poursuivre la promotion. [source : technet]

Ce qu'il faut comprendre, c'est que si votre domaine n'est pas renseigné sur Internet alors on peut ignorer cette délégation. Dans ce cas, les éléments de votre domaine ne seront pas joignables depuis l'Internet. Dans mes exemples, mon domaine n'est pas renseigné sur Internet. Je décide donc d'ignorer la délégation DNS.

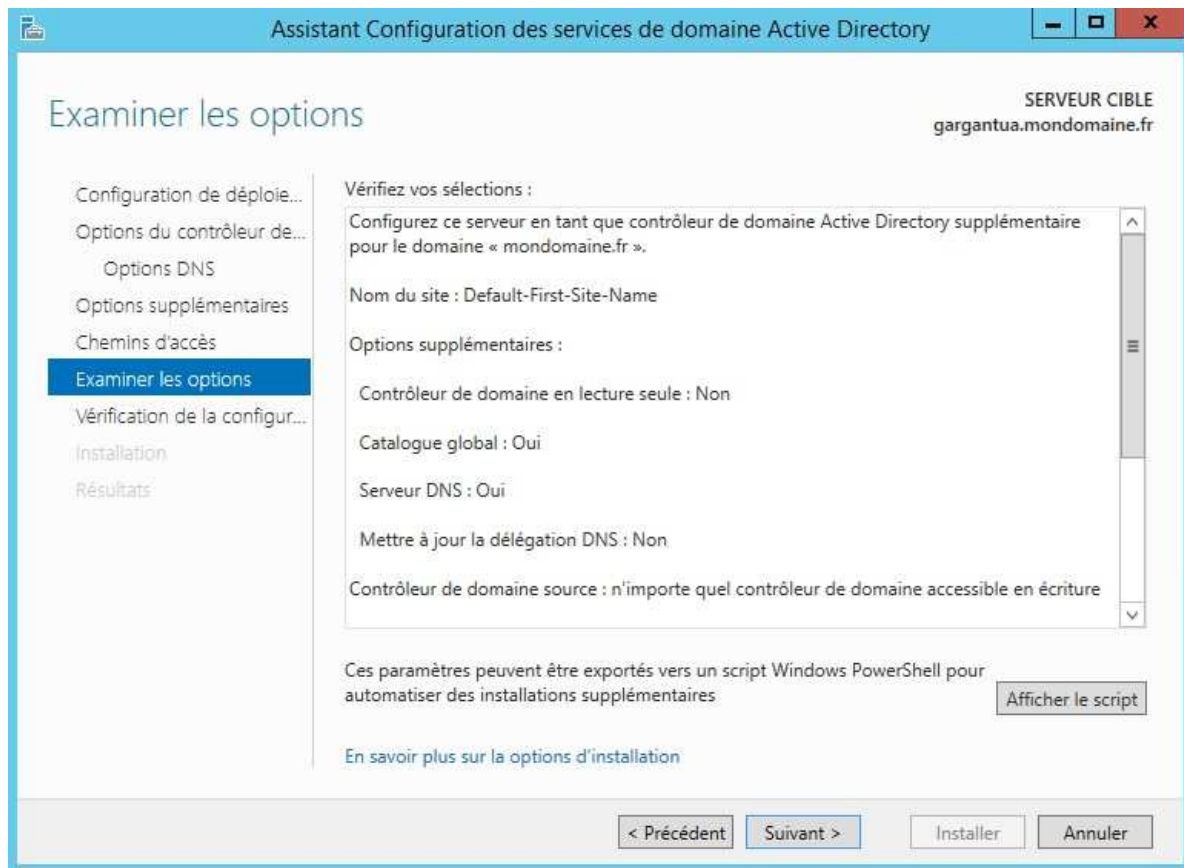




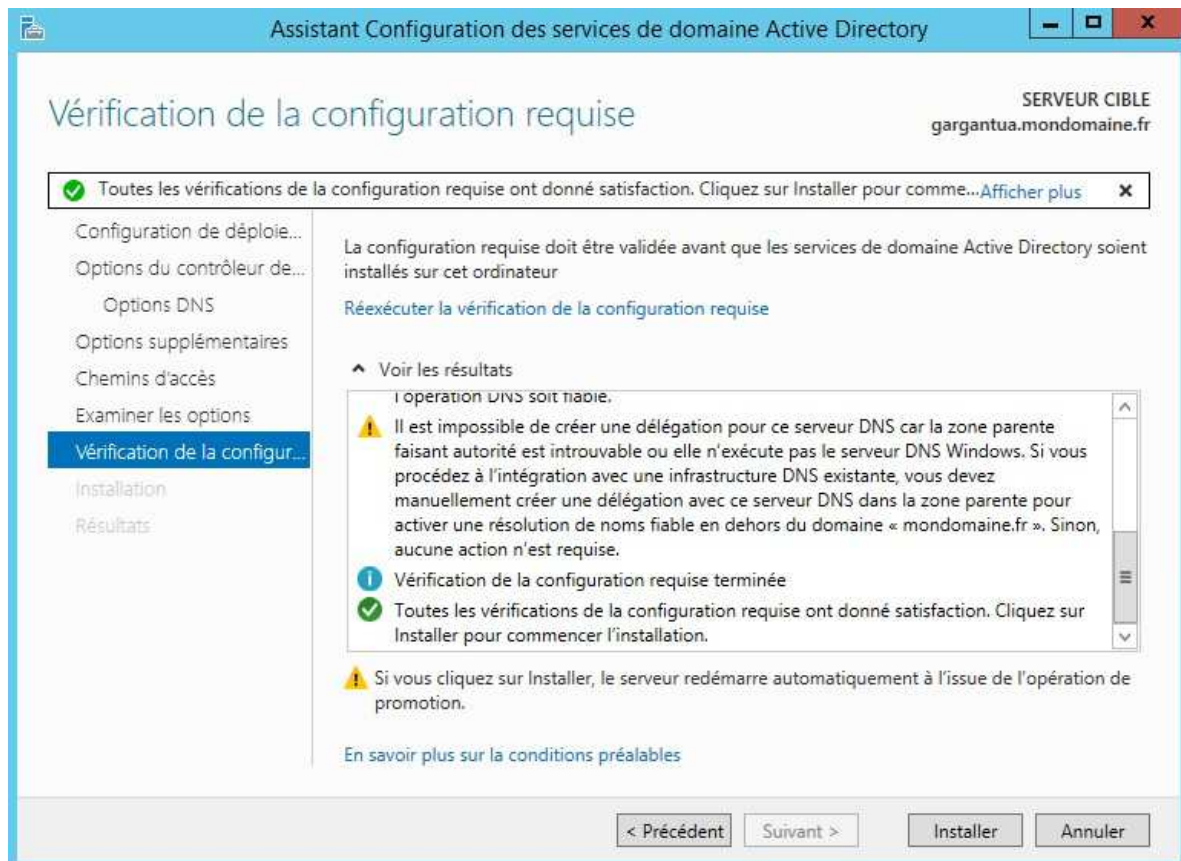
Faites « Suivant »



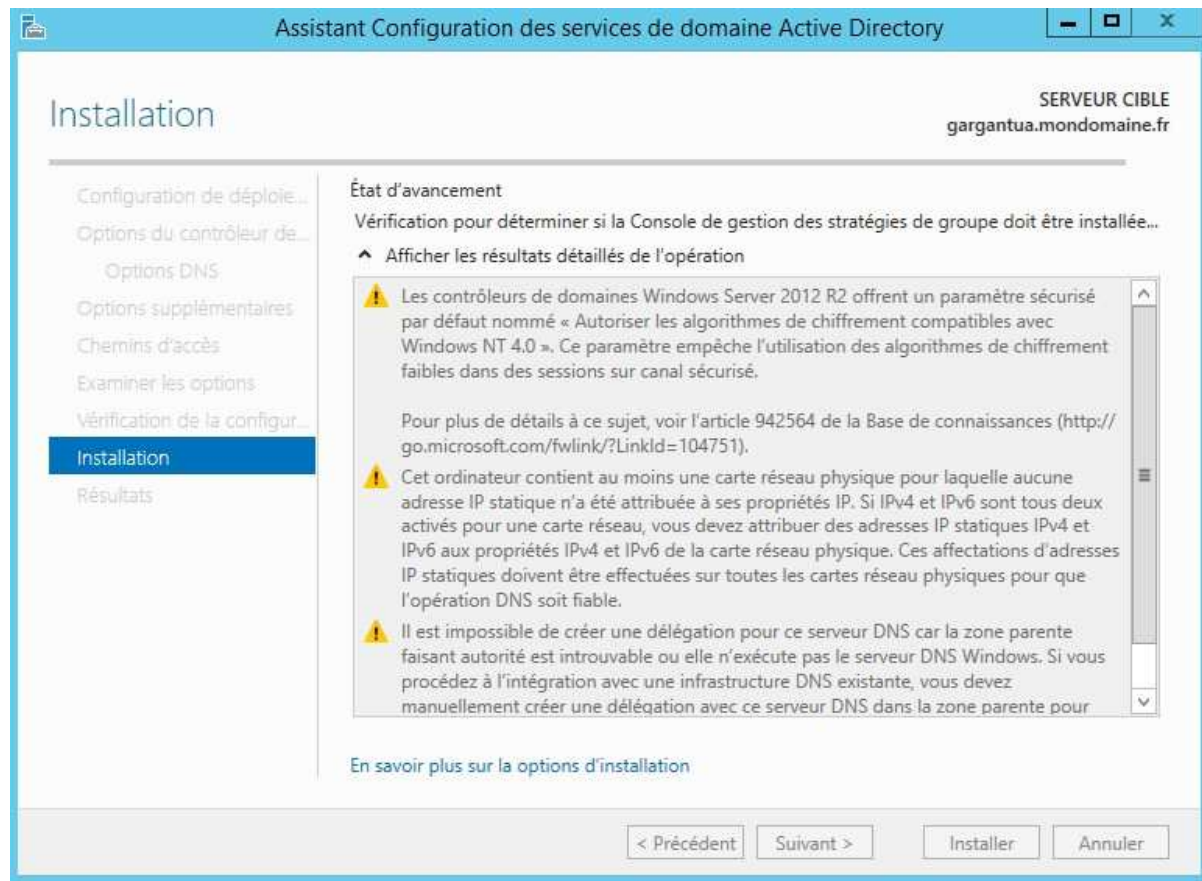
Laissez les valeurs par défaut et faites « Suivant »



L'assistant vous génère un résumé de la création du rôle. Vous pouvez à tout moment revenir en arrière pour corriger. Si tout vous semble correct, faites « Suivant ».



L'assistant vérifie que toutes les options sont réalisables. Dans mon cas j'ai deux avertissements liés à l'adressage IP et la délégation que je décide d'ignorer.



L'installation se lance et l'ordinateur redémarre automatiquement.

Suite au redémarrage du poste, vous pourrez aller dans l'outil « Utilisateurs et ordinateurs Active Directory » et vous apercevoir que vous retrouvez correctement les informations que vous avez entrées sur le premier contrôleur de domaine.