DETROZ Sébastien Version 1 10/11/2016

Sommaire :

Sommaire : 1
Introduction 1
Installation : 2
Ajout d'un rôle : 8
Installation d'Active Directory : 14
DNS : 23
AD : 29
Création d'UO : 29
Création de Groupes : 30
Création d'Utilisateurs (et de modèles) : 30
Créer un script de connexion : 30
TD Active Directory : 30

Introduction

Objectif : L'objectif de ce TP est d'installer et de configurer un contrôleur de domaine Windows Server 2008, d'utiliser les services qu'il propose afin de créer une infrastructure : un annuaire Active Directory avec des utilisateurs, un DHCP et un DNS.

Pré-requis : Il faut des connaissances en Windows Server.

Norme : Toutes les commandes issues d'une machine avec un système d'exploitation Debian ou Windows sont écrites ***en gras et en italique***.

Nous allons installer une machine virtuelle de Windows Server 2012. Pour pouvoir correctement fonctionner, elle aura besoin de 4 Go de mémoire RAM et de 32 Go d'espace disque.

Choses à savoir faire :

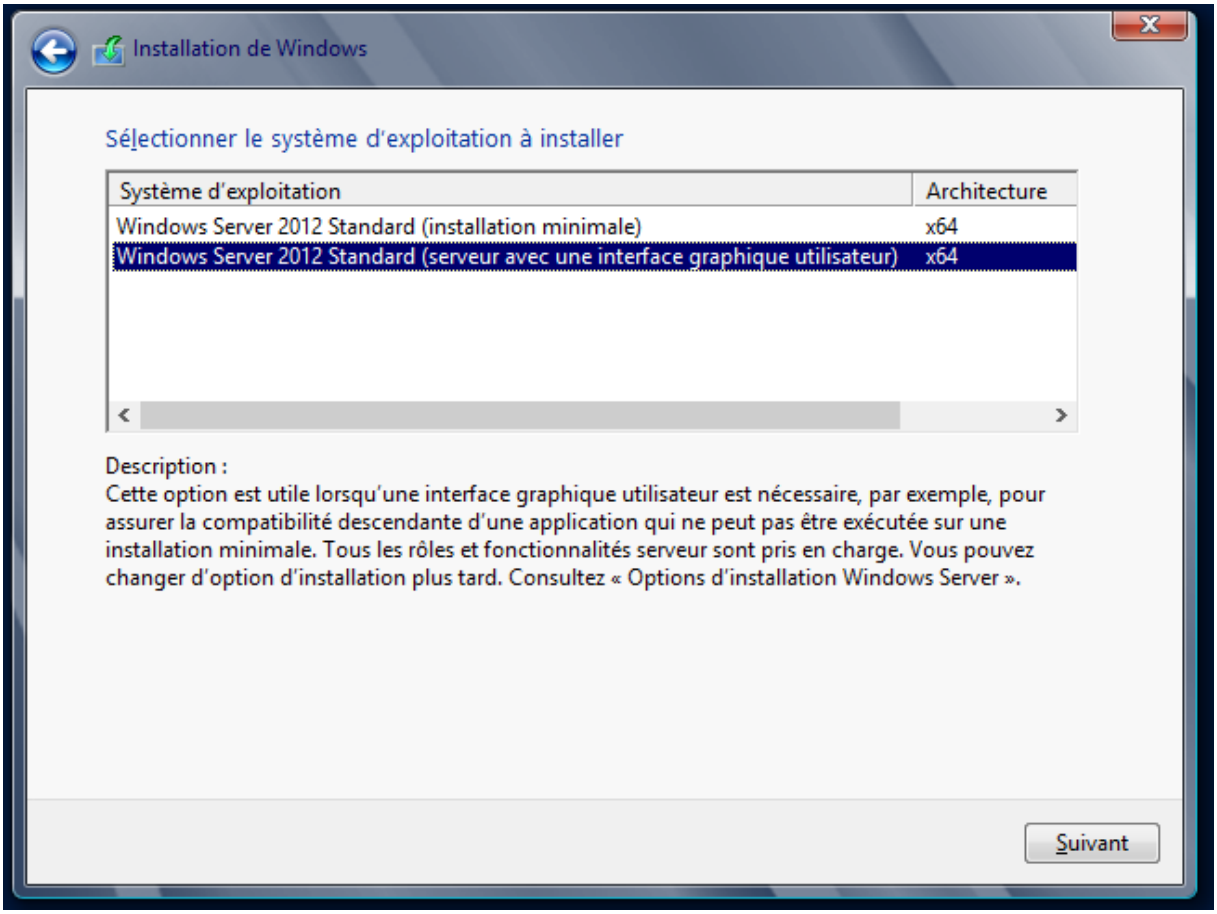
- Création des différents objets dans la base Active Directory (UO, groupes, comptes utilisateurs, les partages, etc…).
- Pour les comptes utilisateurs : Compte, Profil, Membre de, etc.
- Créer et utiliser un modèle de compte utilisateur (Utilisation de la variable %username%).
- Application et gestion des droits de partage et des droits de sécurité NTFS.
- Gestion des quotas. Grâce à l'apparition du NTFS (car le FAT est dépendant de chaque bloc pour accéder au suivant, le NTFS connaît toutes les adresses par blocs).
- Gestion des stratégies de groupe (GPO). GPT et GPC et une seule GPO peut avoir un numéro identique. Deux stratégies de groupe par défaut : Default-Domain-Policy est celle qui est sur le domaine et contrôle tout ce qui est sécurité des comptes (mots de passe).

Installation :

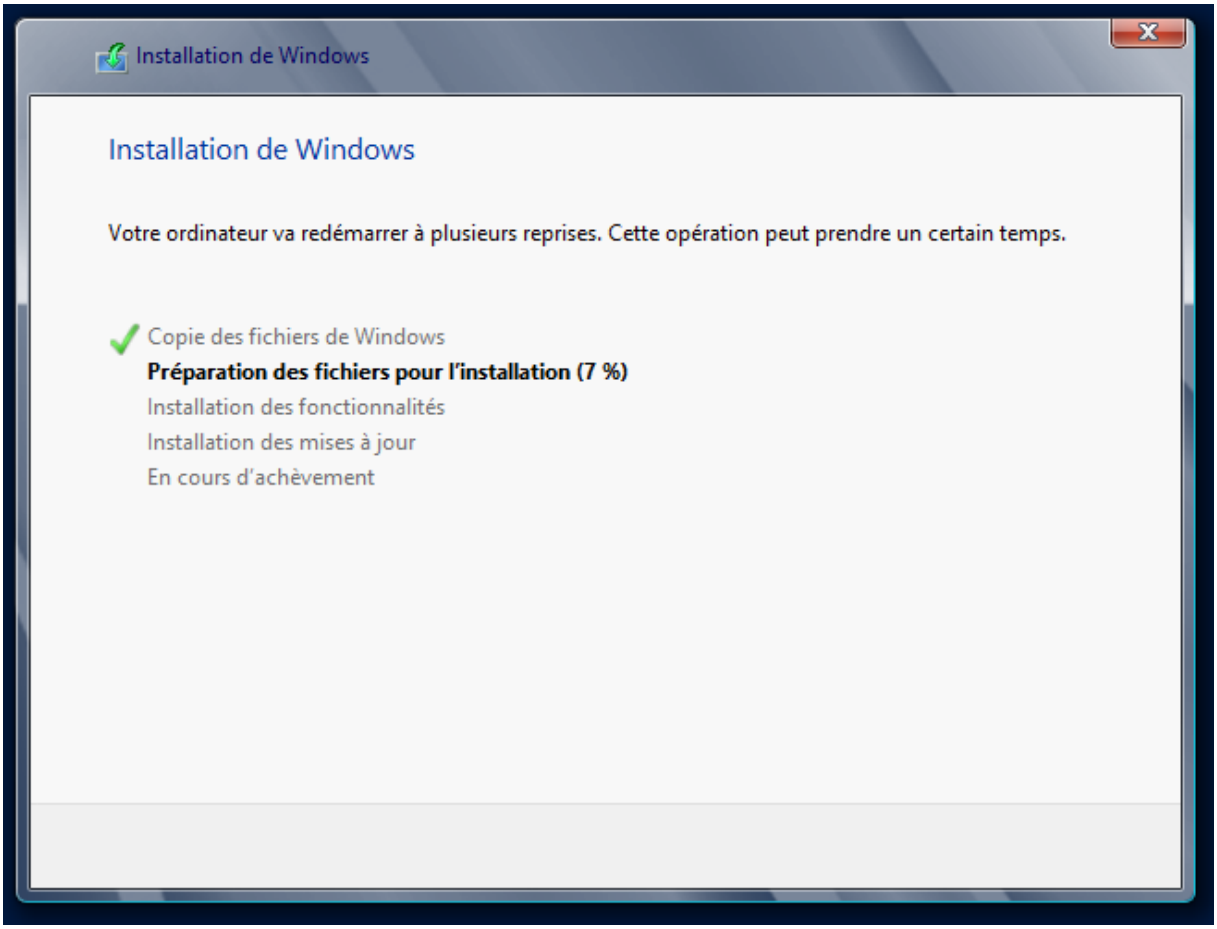
L'installation débute par l'insertion de clé valide. Nous allons donc utiliser une clé KMS, qui est une clé de test à des fins pédagogiques, que nous trouvons sur le site : https://msdn.microsoft.com/fr-fr/library/jj612867%28v=ws.11%29.aspx

Windows Server 2012 Server Standard	XC9B7-NBPP2-83J2H-RHMBY-92BT4

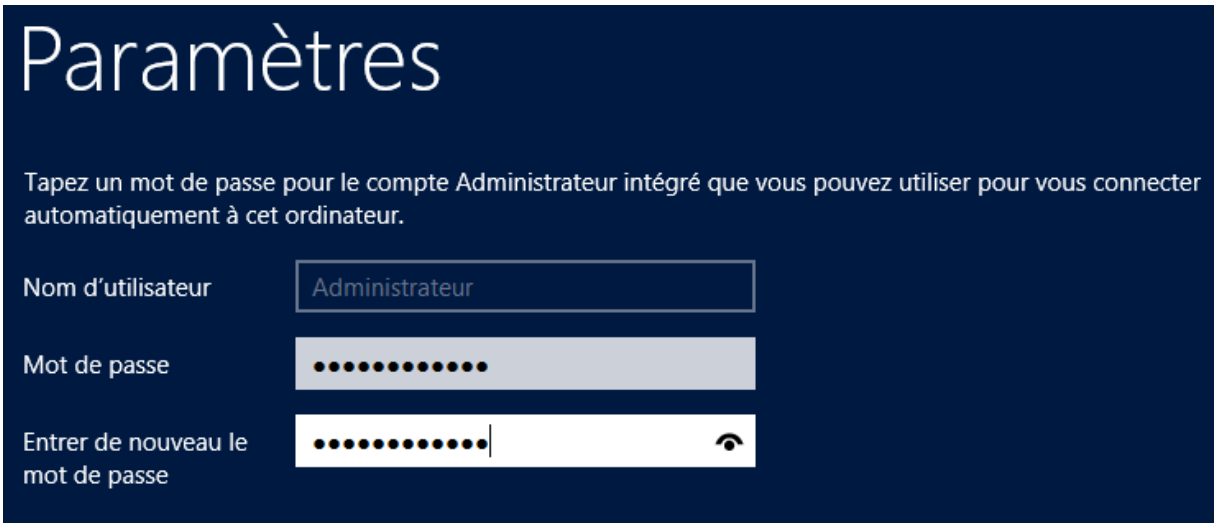
Après avoir entré la clé, il faut maintenant choisir la version à installer : une interface graphique sera nécessaire.



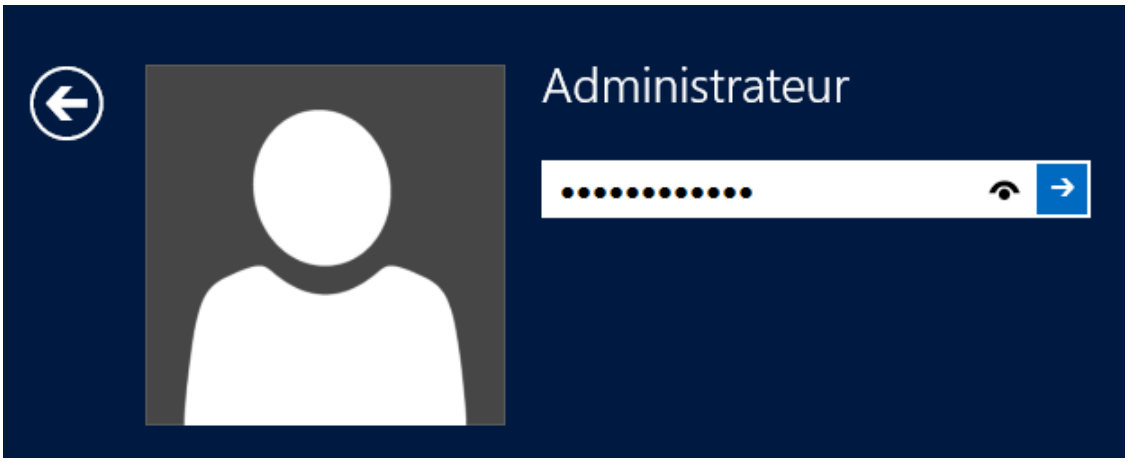
Il faut ensuite sélectionner l'installation personnalisée, et non la mise à niveau, car c'est notre première installation. L'installation s'effectue ensuite :

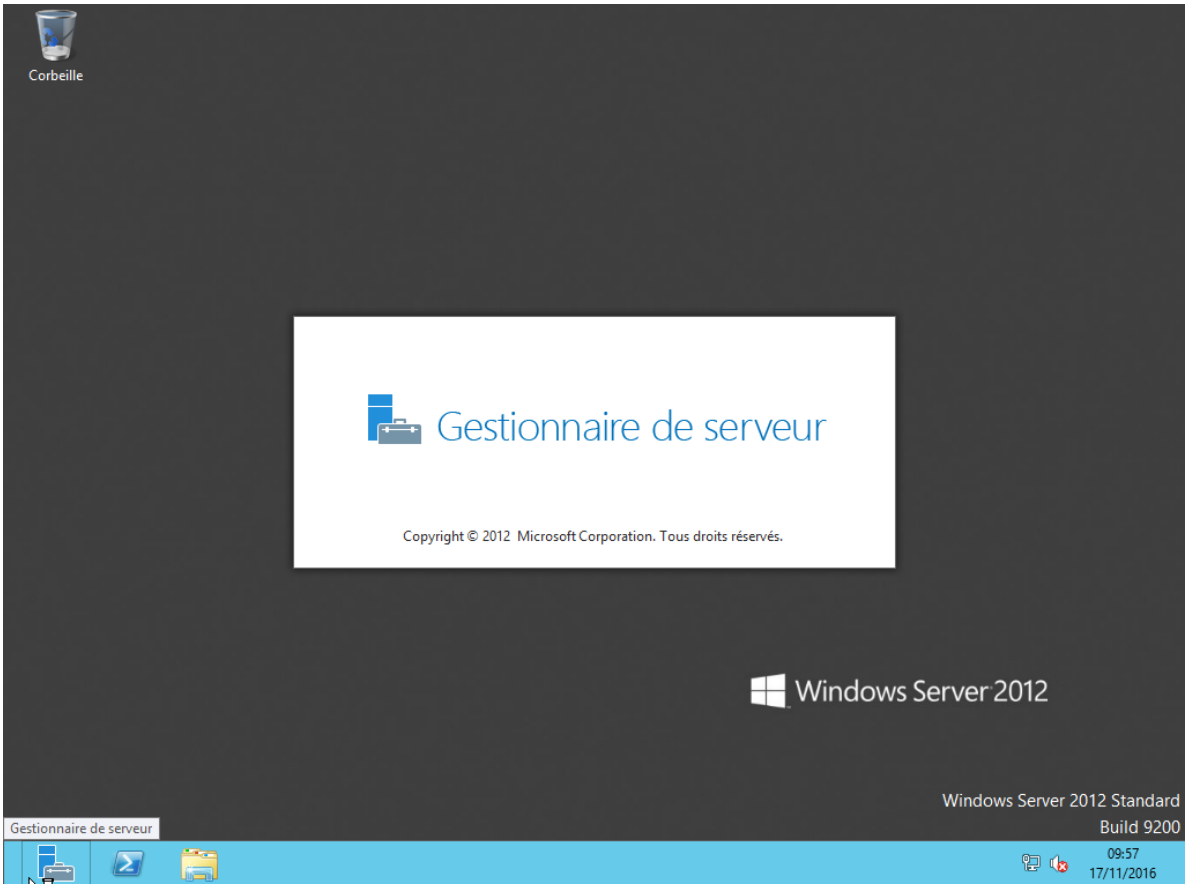


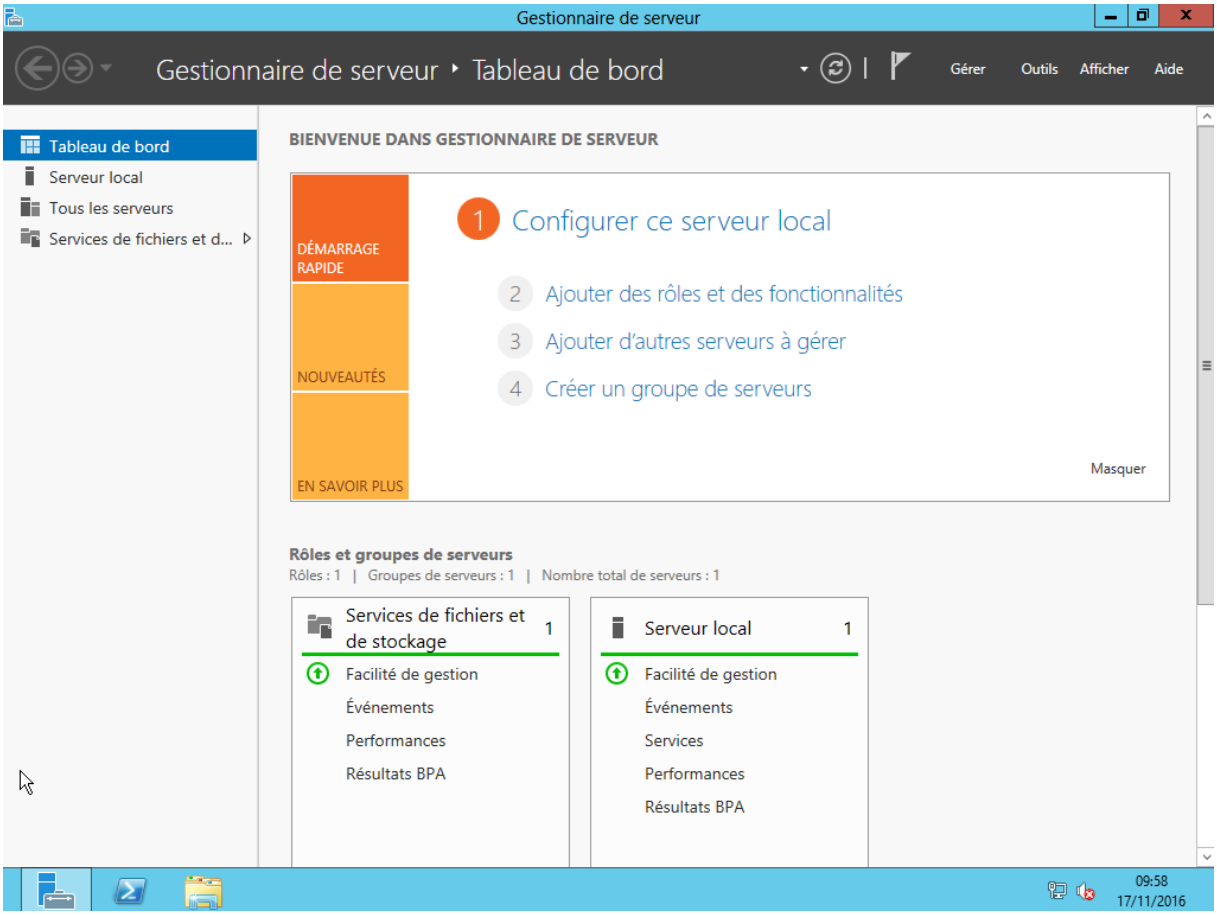
Après redémarrage automatique de la machine, il faut attribuer un mot de passe au compte Administrateur. Nous choisirons Password1234.

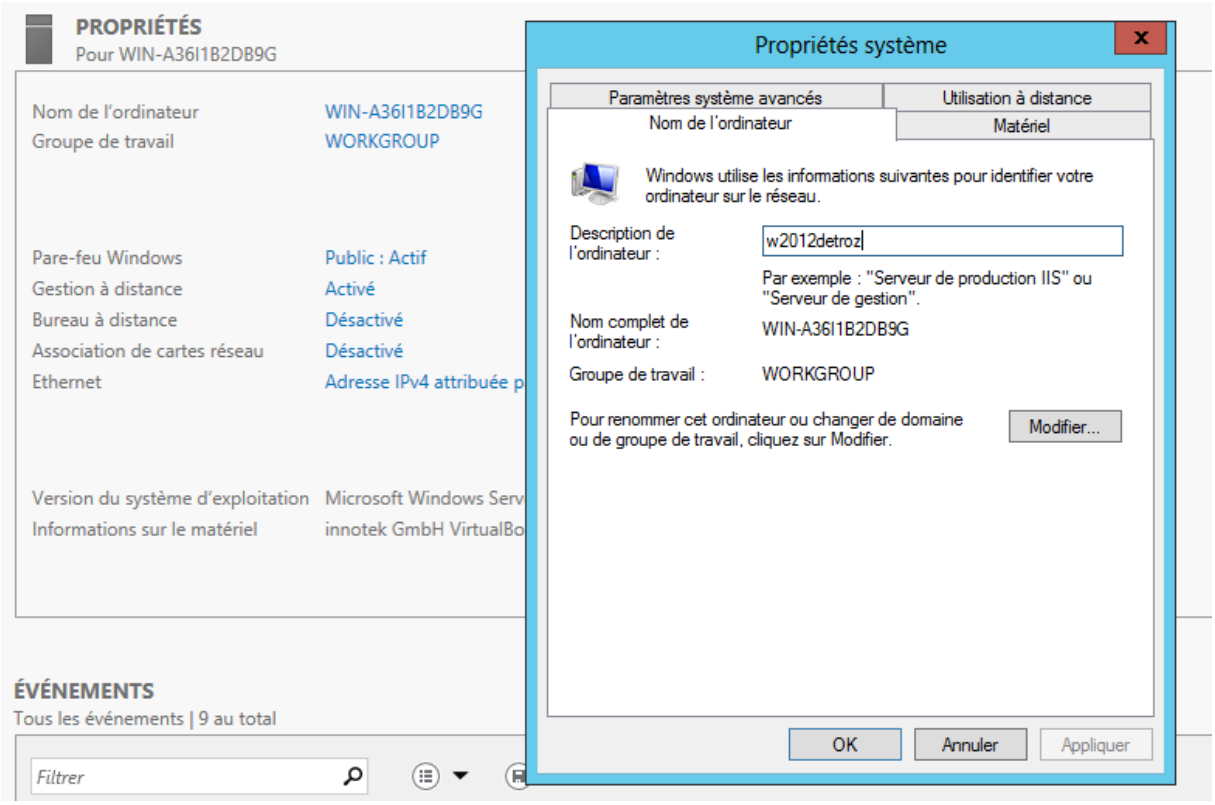


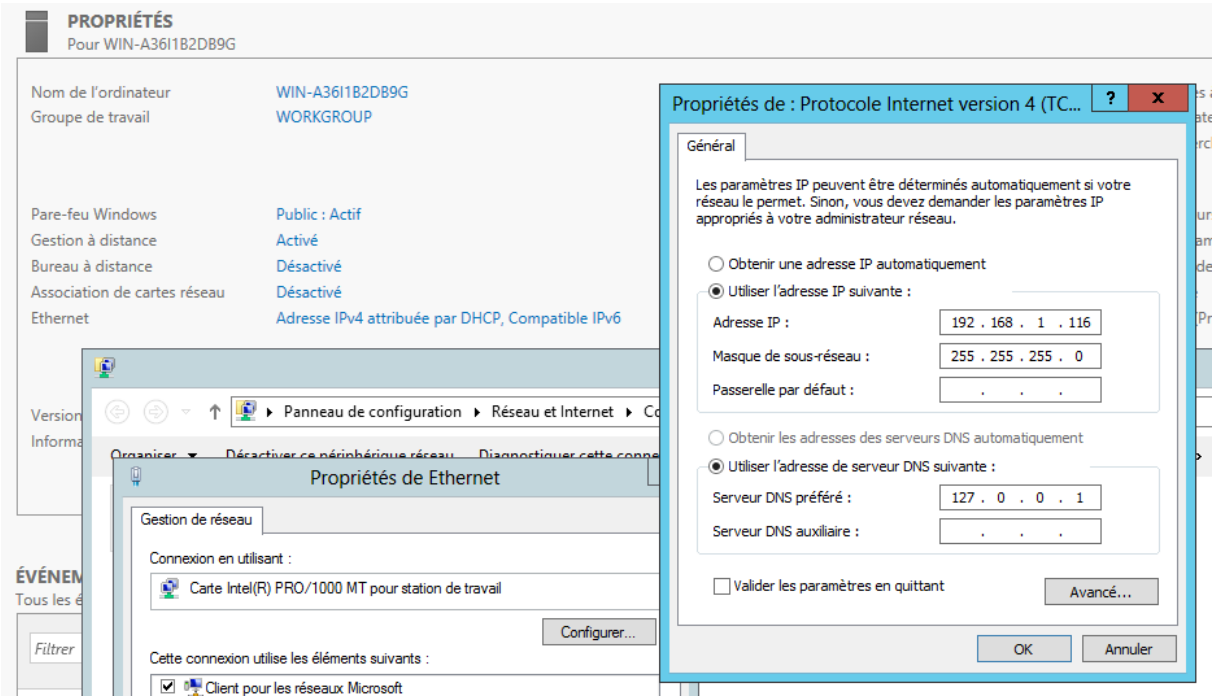

Appuyez sur Ctrl+Alt+Suppr pour vous connecter.
09:55
jeudi 17 novembre


Administrateur

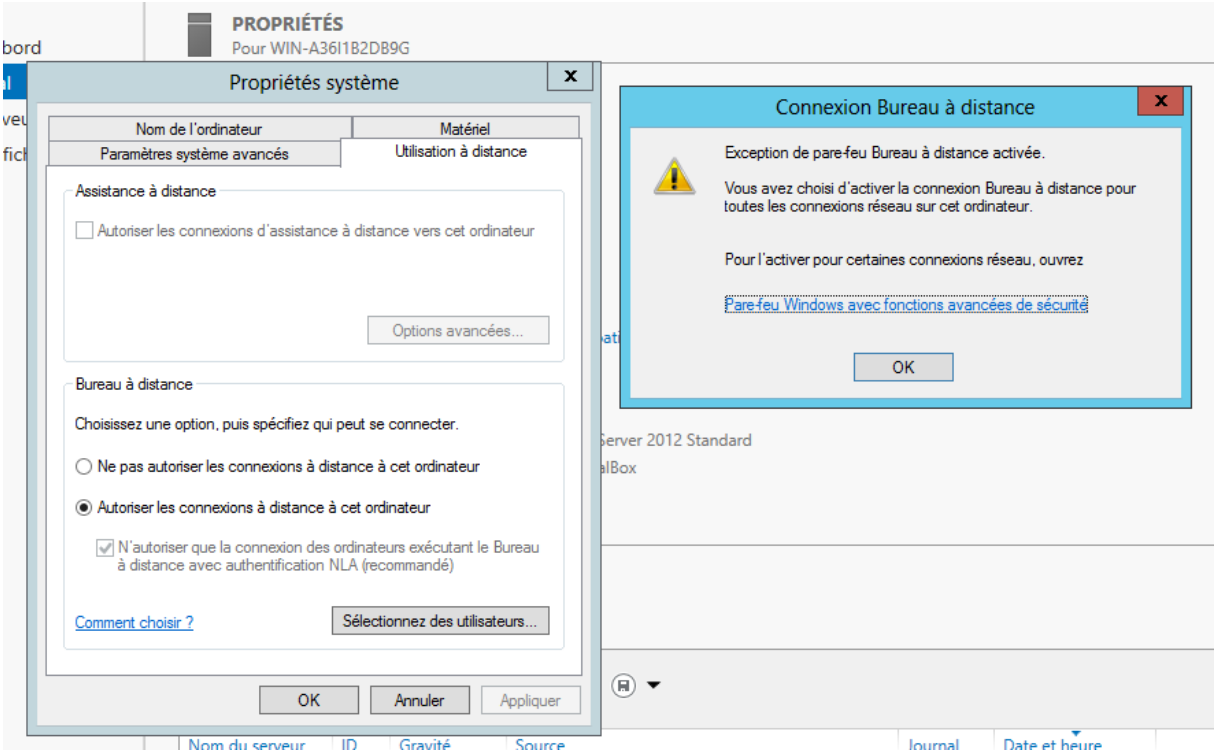

Corbeille
Gestionnaire de serveur
Copyright © 2012 Microsoft Corporation. Tous droits réservés.
Windows Server 2012
Windows Server 2012 Standard
Build 9200
Gestionnaire de serveur
09:57
17/11/2016


Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers et d...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce serveur local
2 Ajouter des rôles et des fonctionnalités
3 Ajouter d'autres serveurs à gérer
4 Créer un groupe de serveurs
Masquer
Rôles et groupes de serveurs
Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
Services de fichiers et de stockage 1
Facilité de gestion
Événements
Performances
Résultats BPA
Serveur local 1
Facilité de gestion
Événements
Services
Performances
Résultats BPA
09:58
17/11/2016

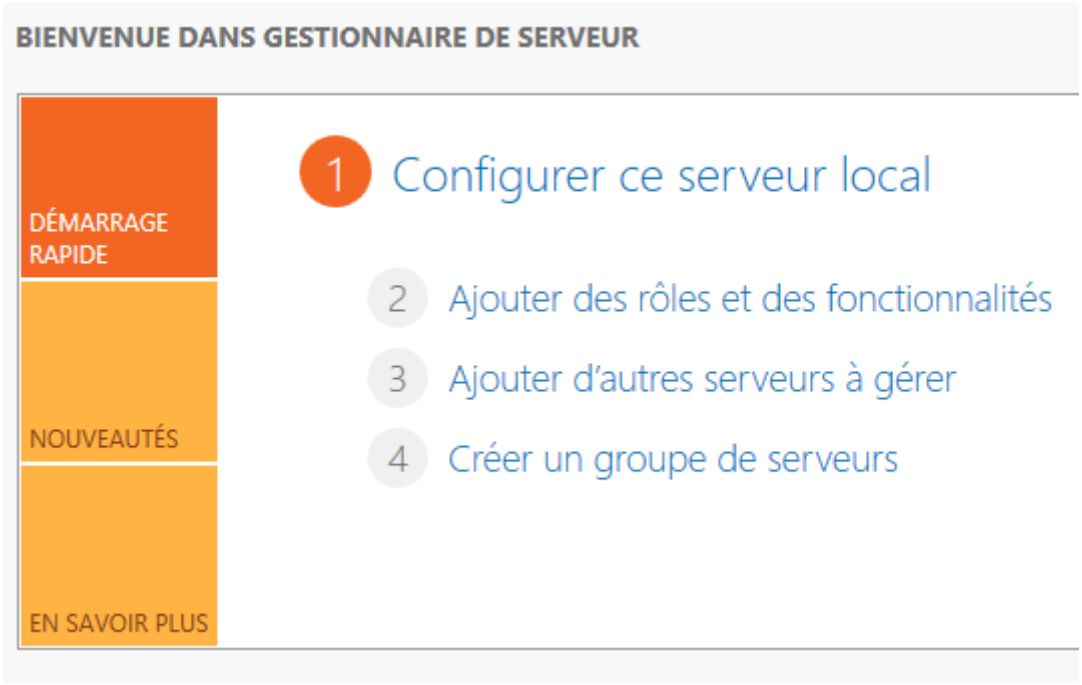


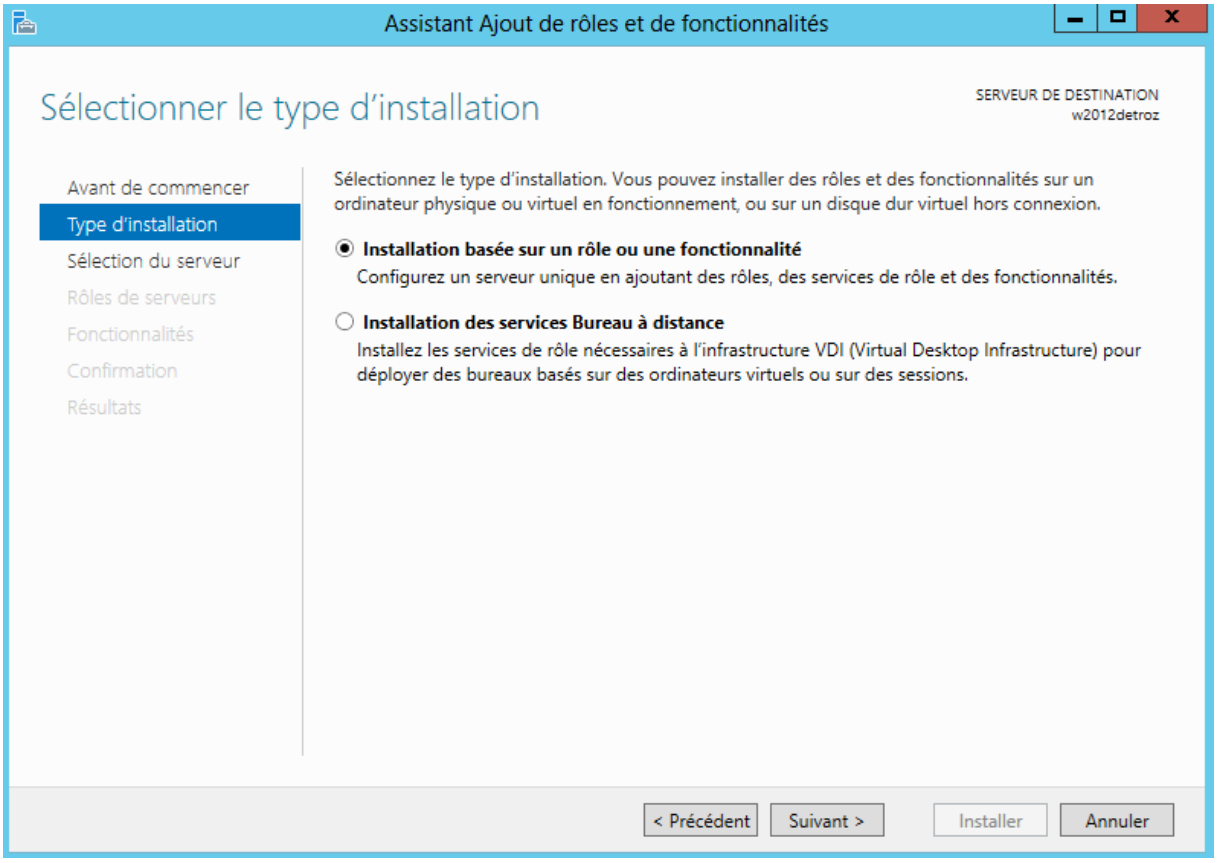


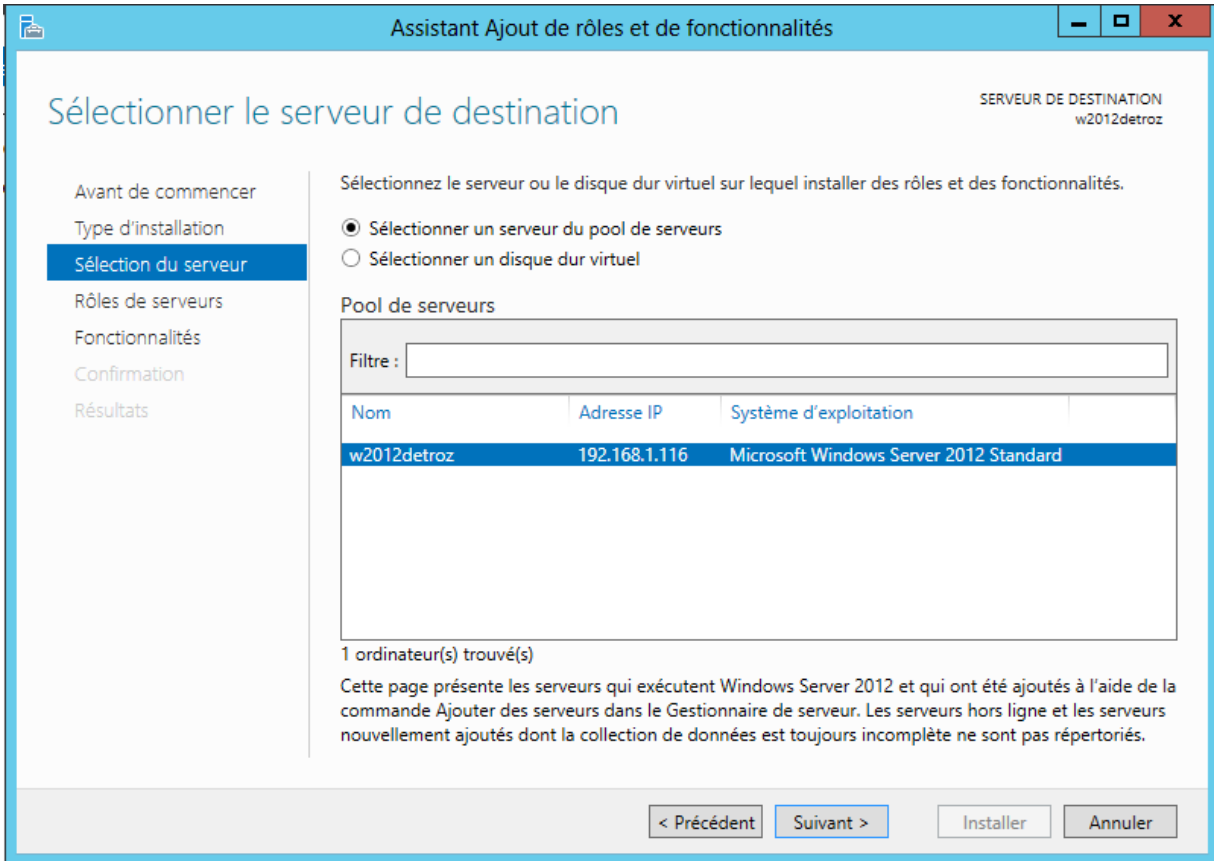
On redémarre ensuite le serveur pour appliquer les modifications.

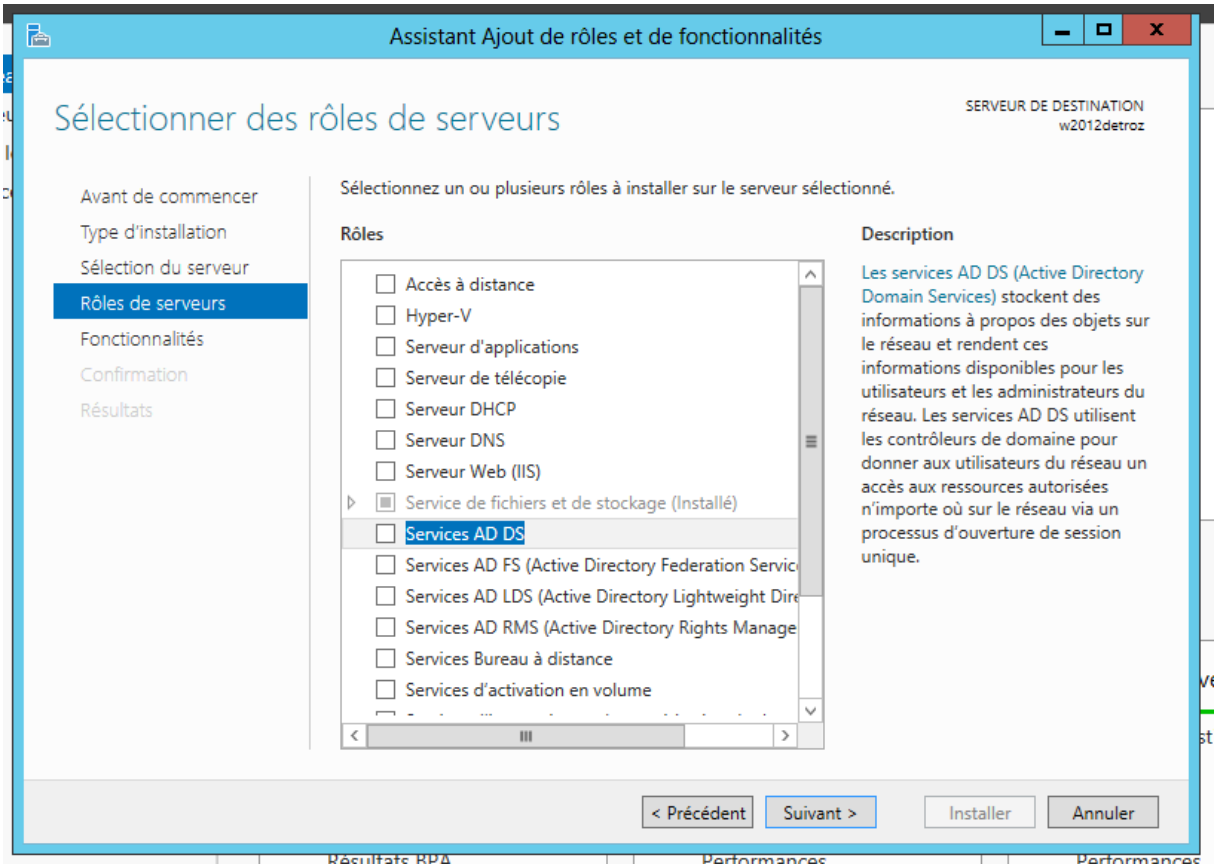


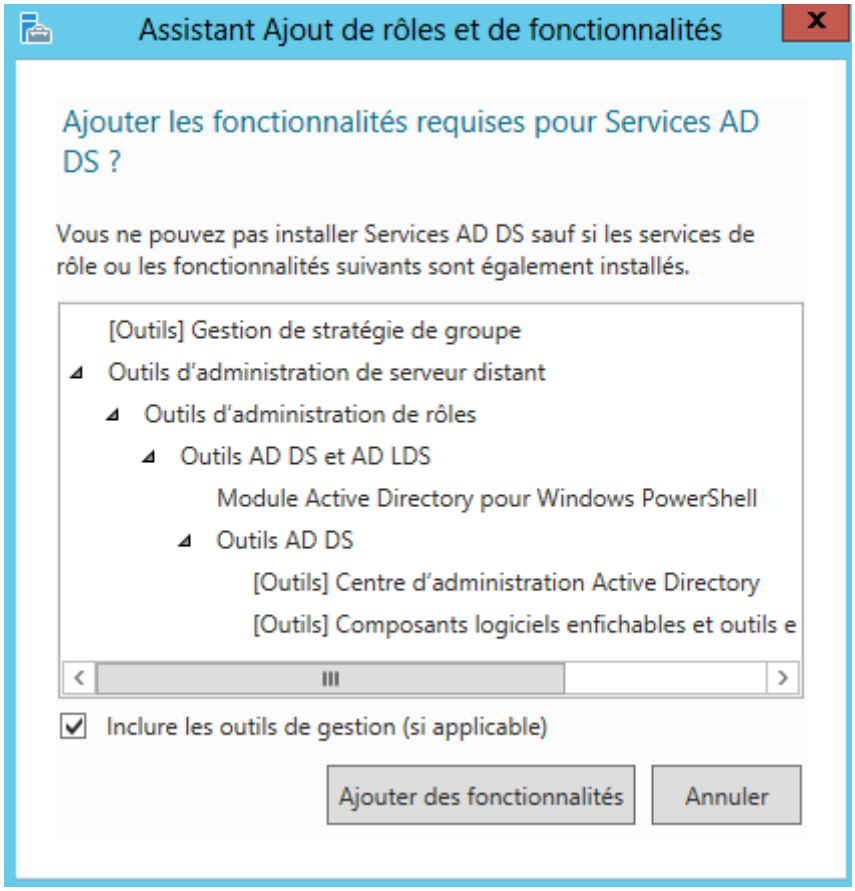
Ajout d'un rôle :

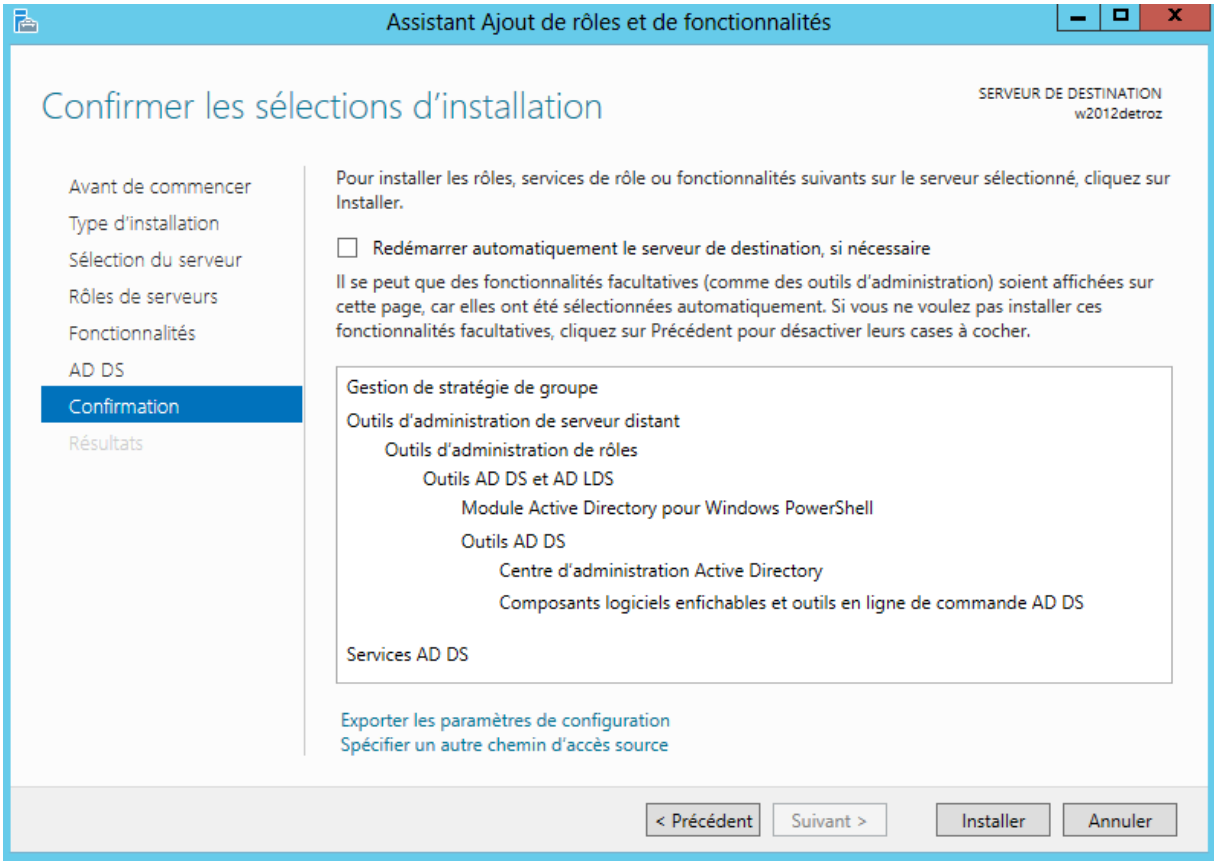


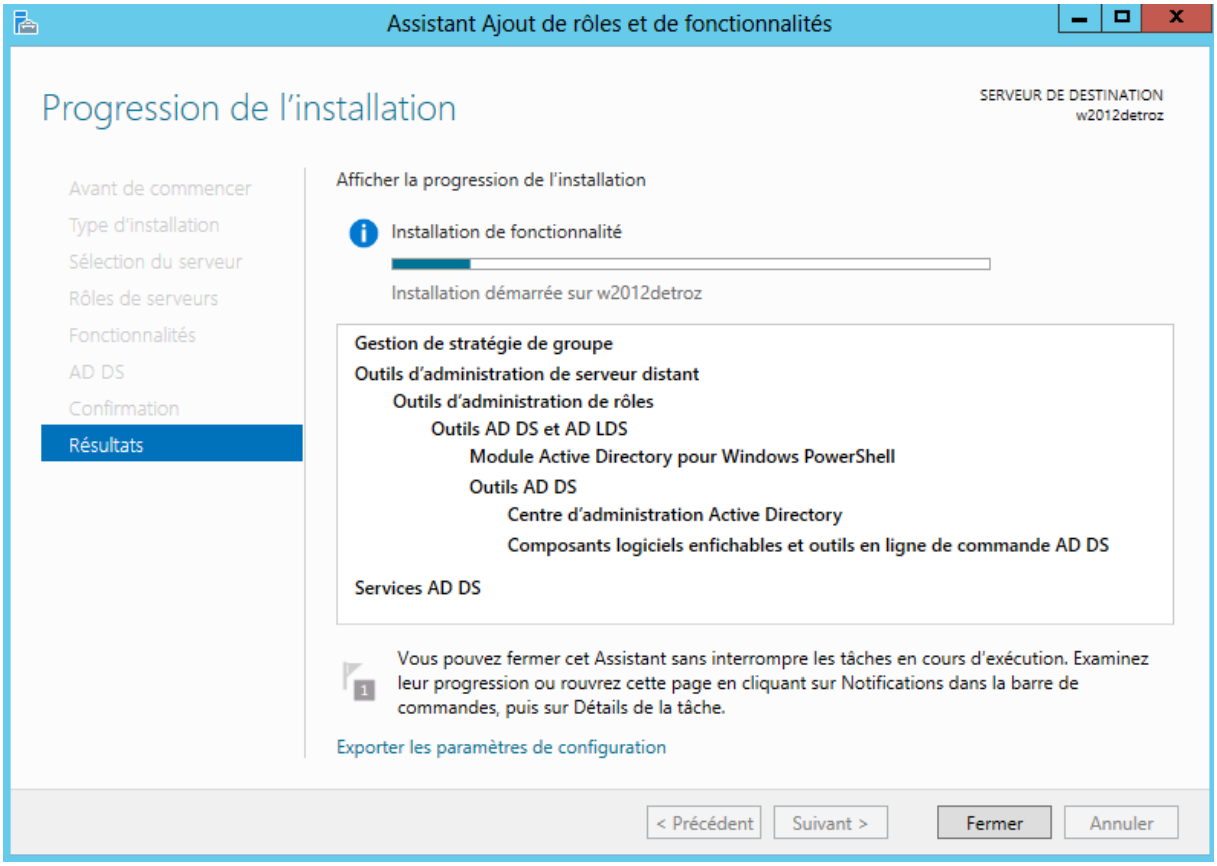

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le type d'installation
SERVEUR DE DESTINATION
w2012detroz
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
w2012detroz
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
w2012detroz
192.168.1.116
Microsoft Windows Server 2012 Standard
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

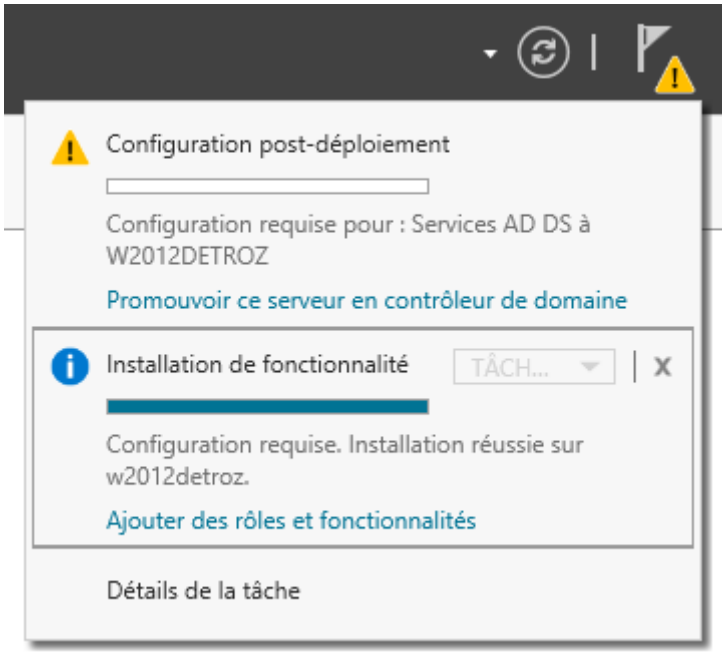

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
w2012detroz
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Hyper-V
Serveur d'applications
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service de fichiers et de stockage (Installé)
Services AD DS
Services AD FS (Active Directory Federation Servic
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Description
Les services AD DS (Active Directory Domain Services) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
< Précédent
Suivant >
Installer
Annuler

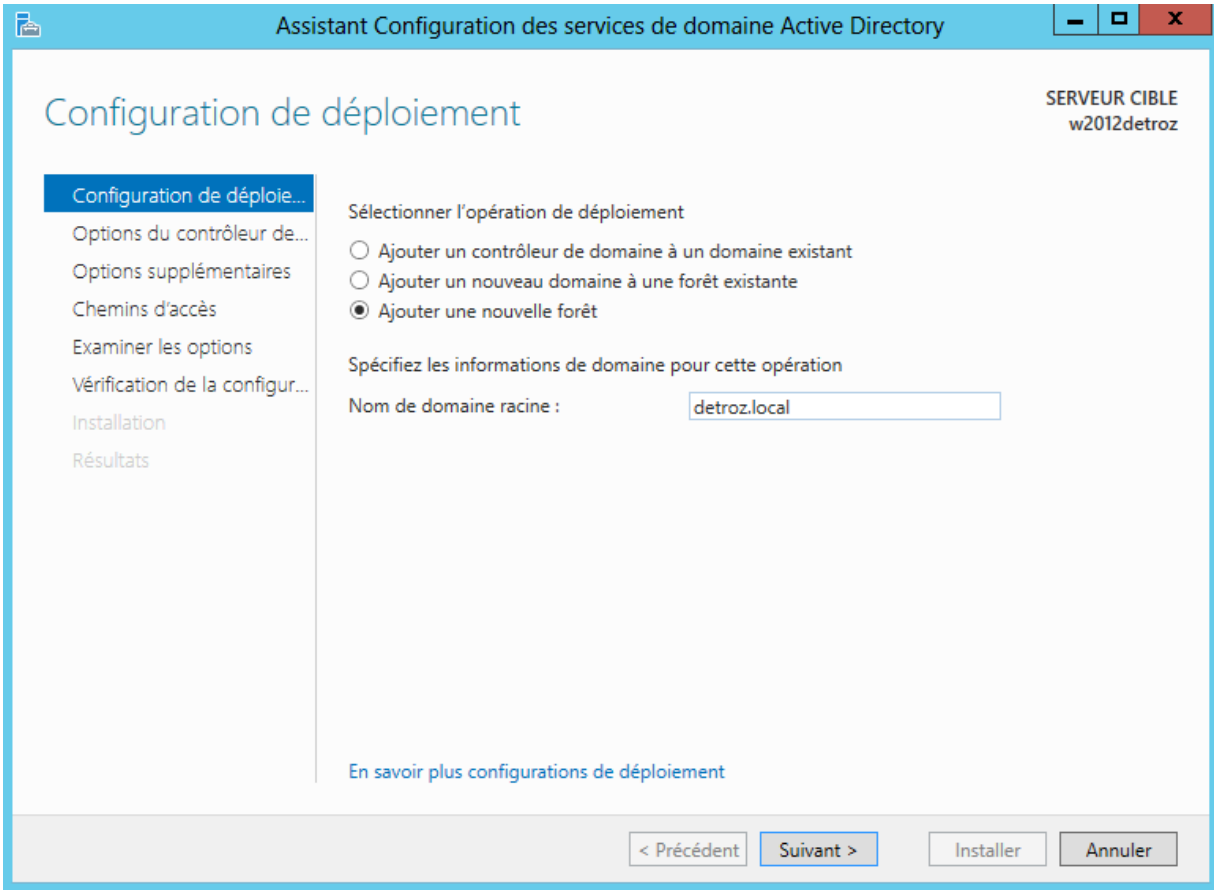

Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Services AD DS ?
Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.
[Outils] Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
[Outils] Centre d'administration Active Directory
[Outils] Composants logiciels enfichables et outils e
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler

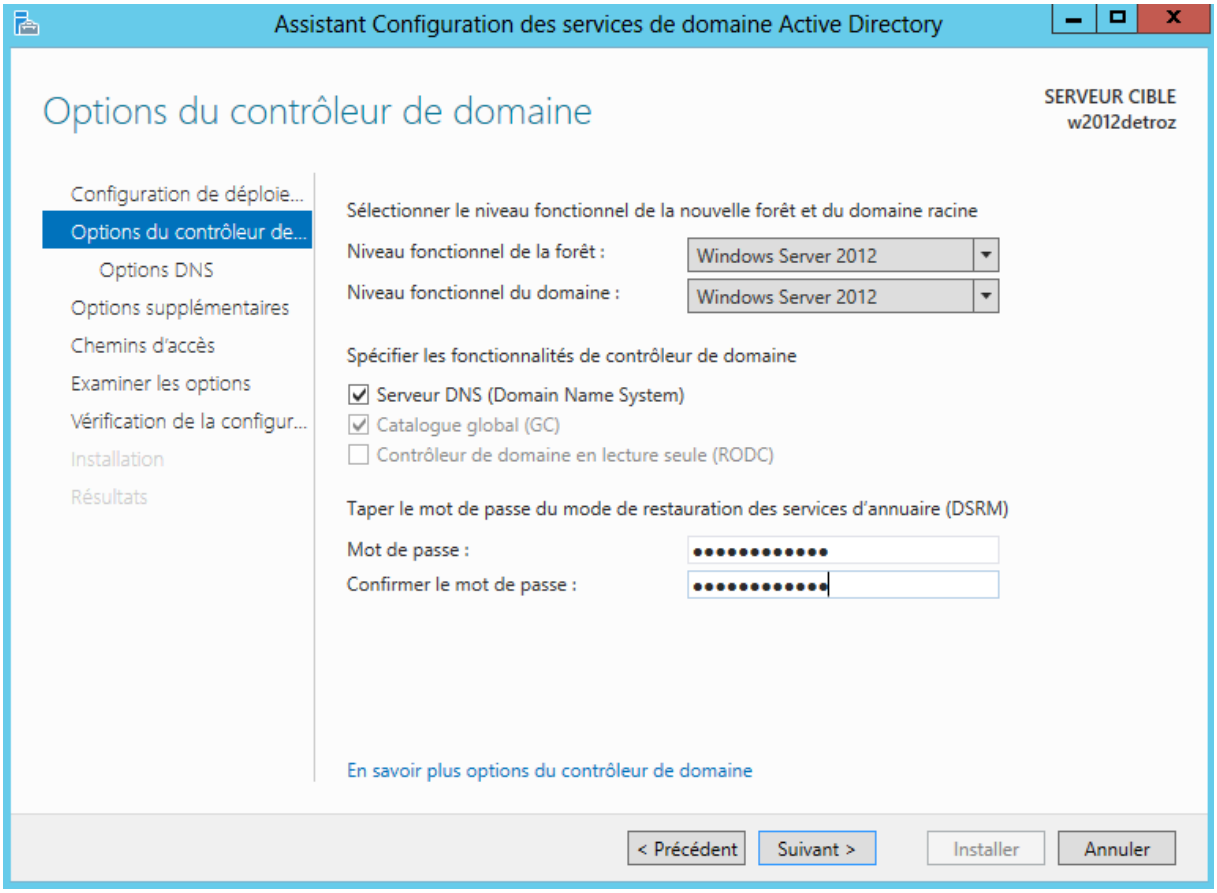

Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
w2012detroz
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Centre d'administration Active Directory
Composants logiciels enfichables et outils en ligne de commande AD DS
Services AD DS
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler



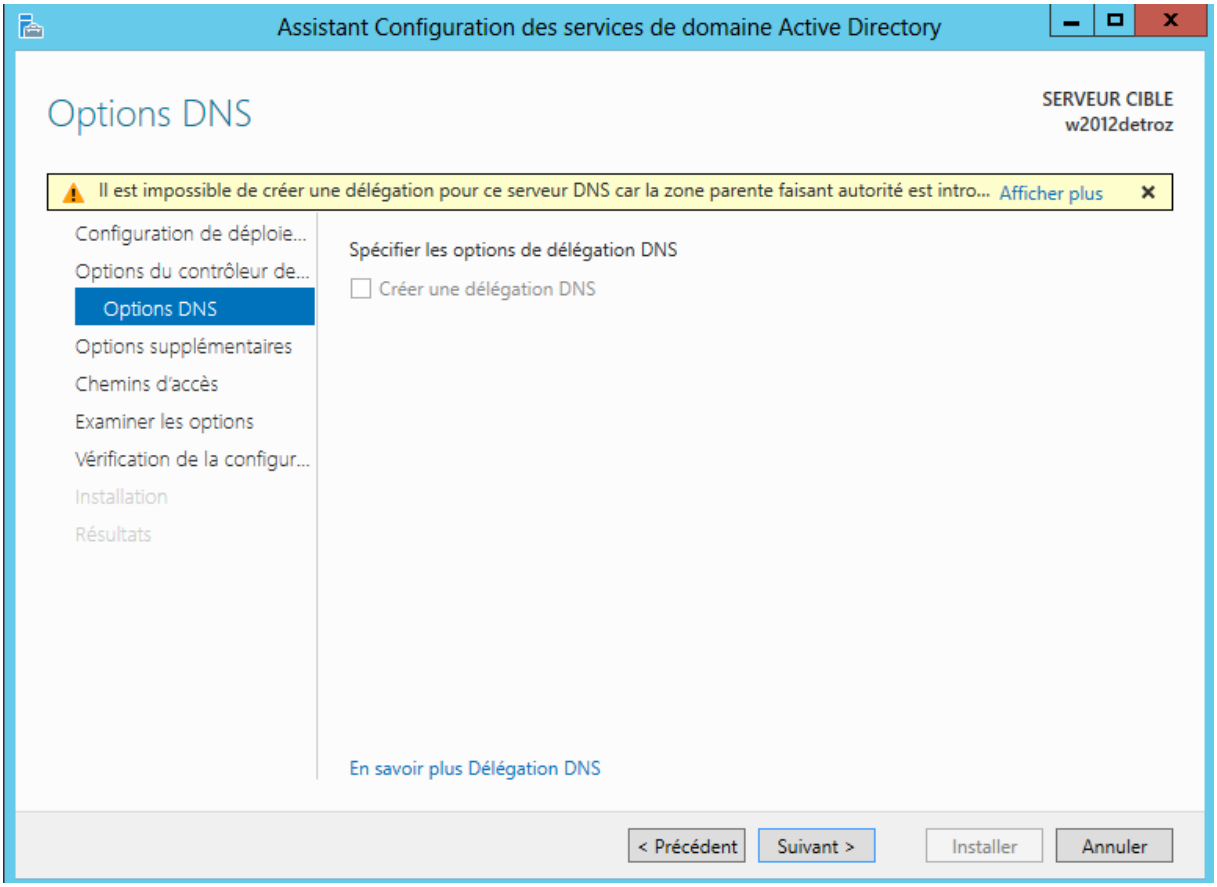
Installation d'Active Directory :


Configuration post-déploiement
Configuration requise pour : Services AD DS à W2012DETROZ
Promouvoir ce serveur en contrôleur de domaine
Installation de fonctionnalité
TÂCH...
Configuration requise. Installation réussie sur w2012detroz.
Ajouter des rôles et fonctionnalités
Détails de la tâche

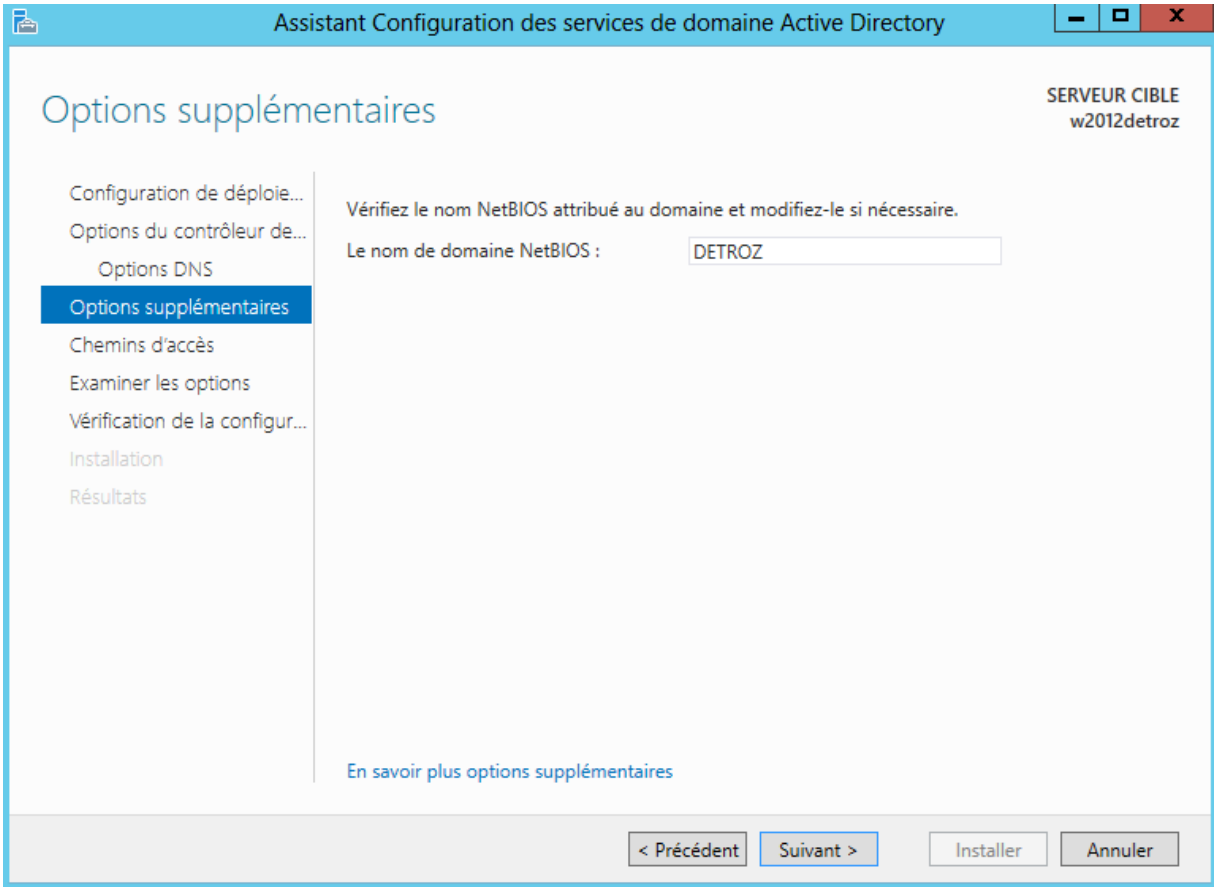

Assistant Configuration des services de domaine Active Directory
Configuration de déploiement
SERVEUR CIBLE
w2012detroz
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner 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
Nom de domaine racine :
detroz.local
En savoir plus configurations de déploiement
< Précédent
Suivant >
Installer
Annuler



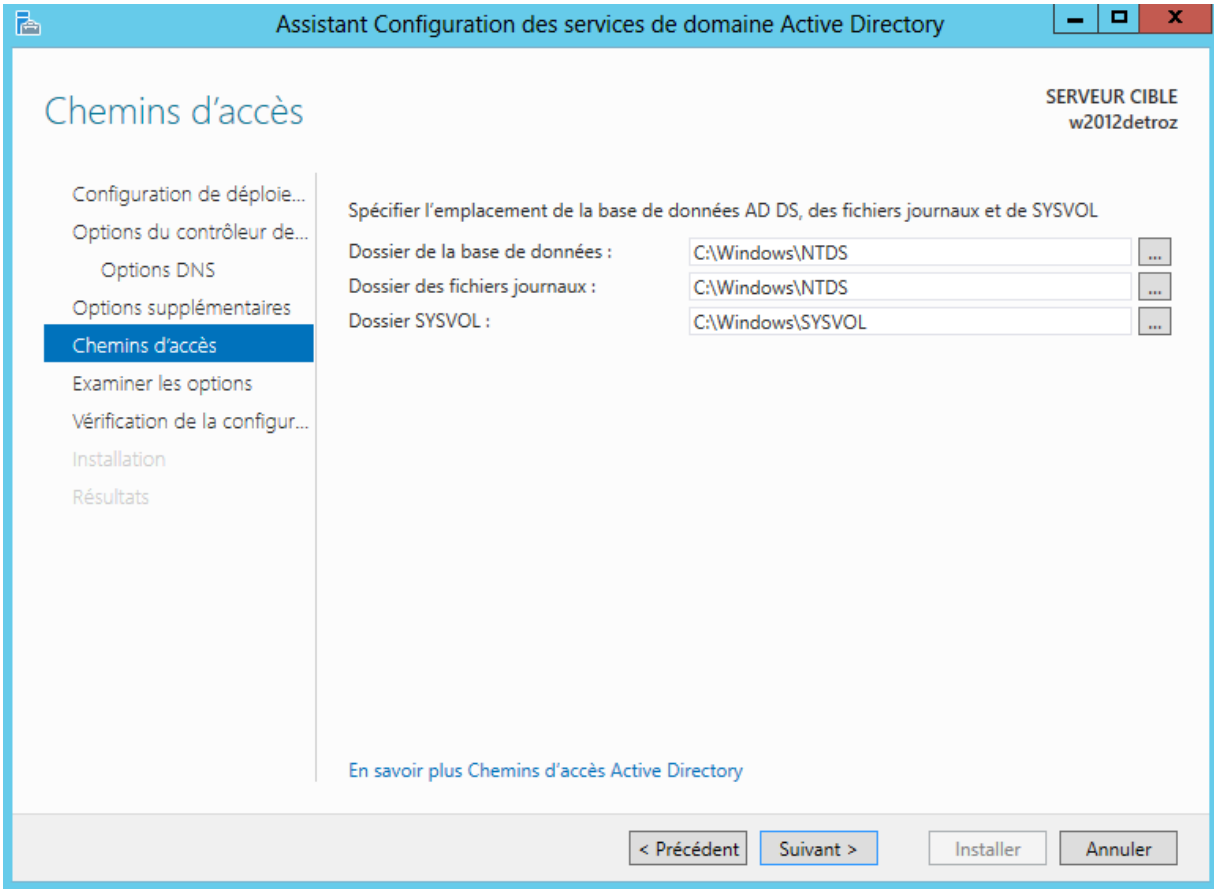
Le serveur DNS est nécessaire. Le catalogue global stock toutes les infos de l'AD, car premier serveur.

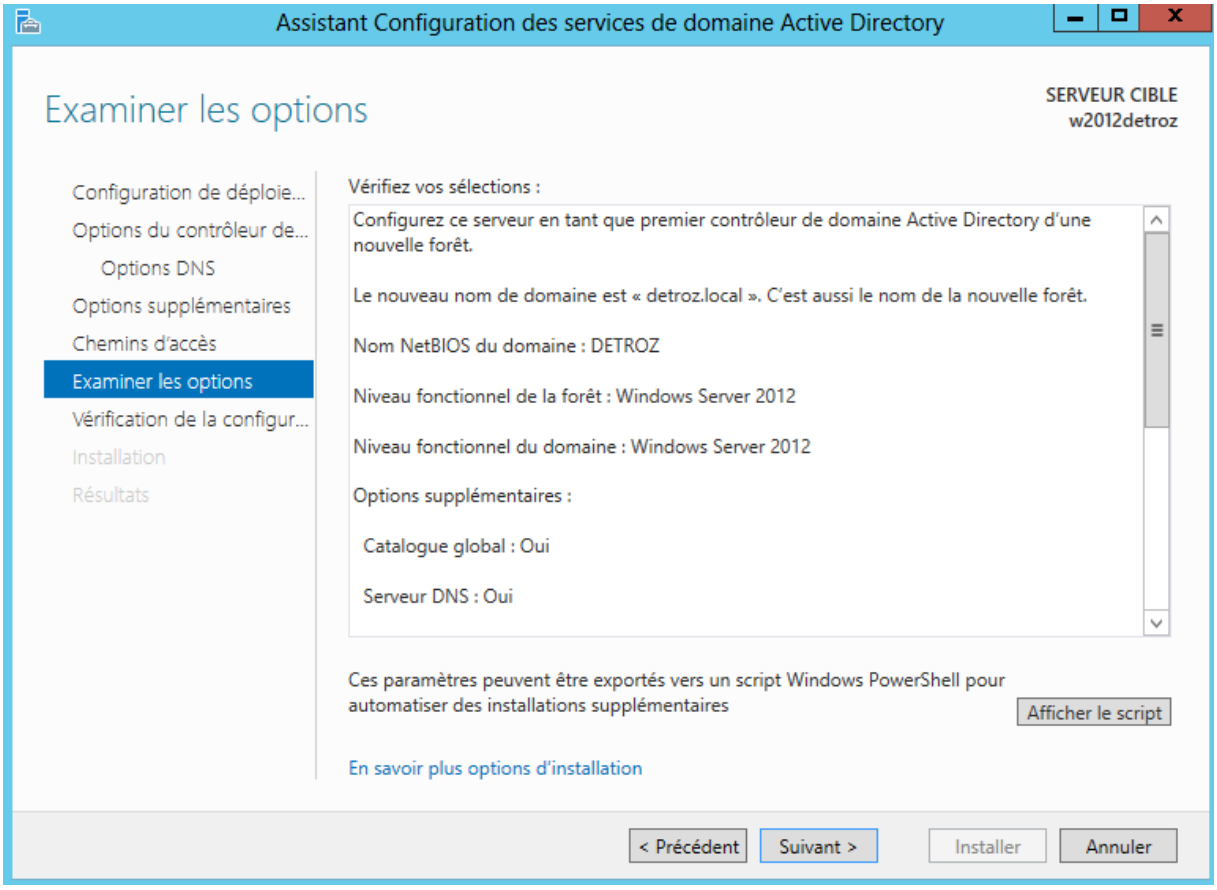


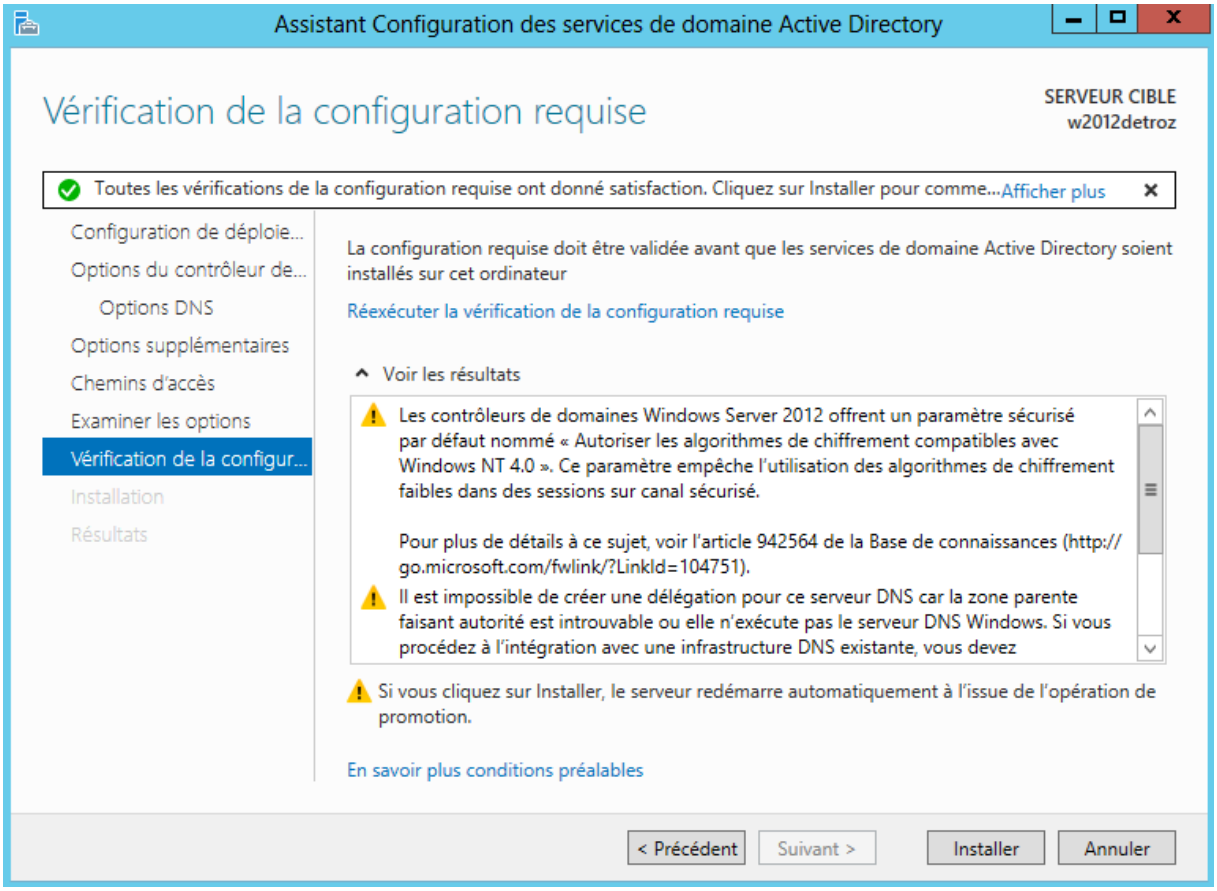
Le service DNS n'est pas encore installé, il se fera automatiquement plus tard.



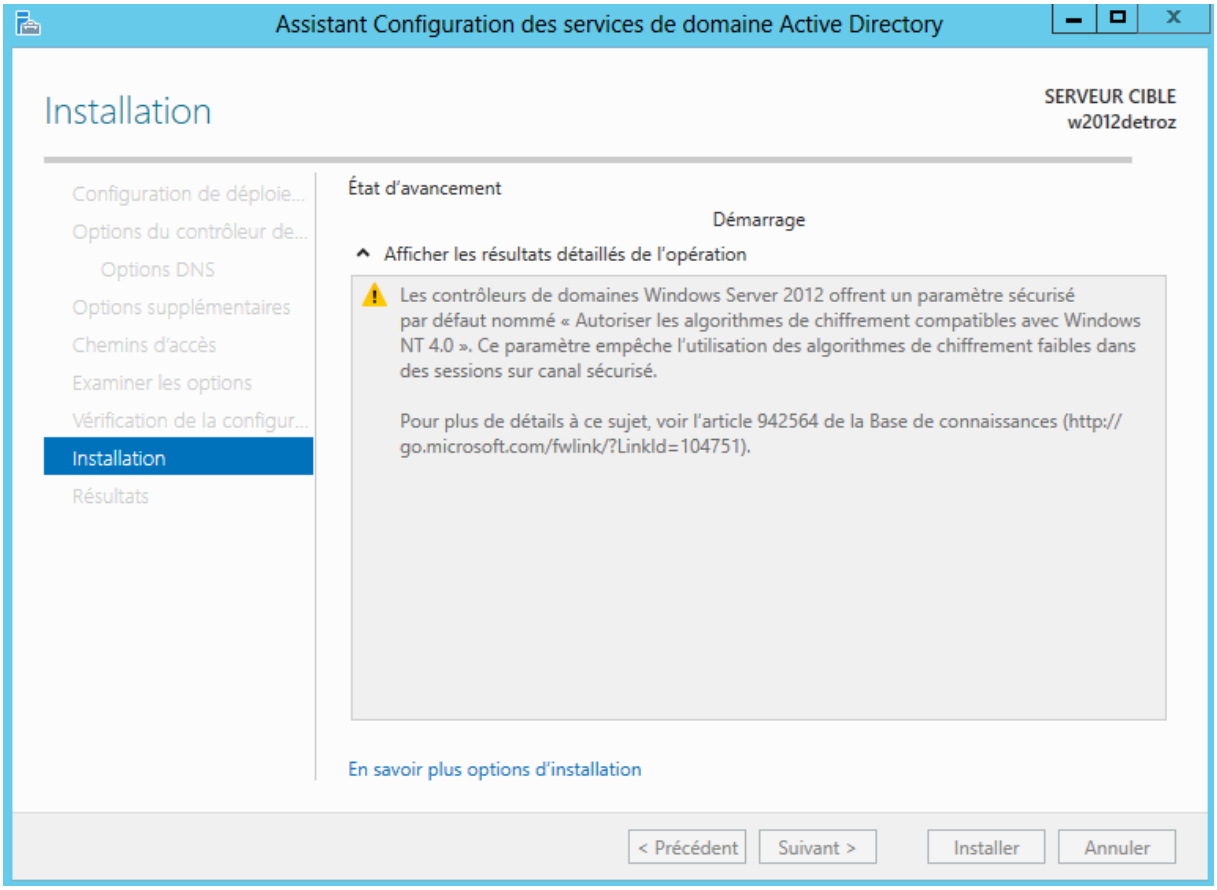
Il ne doit pas dépasser 15 caractères.


Assistant Configuration des services de domaine Active Directory
Chemins d'accès
SERVEUR CIBLE
w2012detroz
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL
Dossier de la base de données :
C:\Windows\NTDS
Dossier des fichiers journaux :
C:\Windows\NTDS
Dossier SYSVOL :
C:\Windows\SYSVOL
En savoir plus Chemins d'accès Active Directory
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Examiner les options
SERVEUR CIBLE
w2012detroz
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez vos sélections :
Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.
Le nouveau nom de domaine est « detroz.local ». C'est aussi le nom de la nouvelle forêt.
Nom NetBIOS du domaine : DETROZ
Niveau fonctionnel de la forêt : Windows Server 2012
Niveau fonctionnel du domaine : Windows Server 2012
Options supplémentaires :
Catalogue global : Oui
Serveur DNS : Oui
Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires
Afficher le script
En savoir plus options d'installation
< Précédent
Suivant >
Installer
Annuler



La croix vert signifie qu'on respecte les pré-requis : une IP fixe, pas d'IPv6, une loopback en serveur DNS.

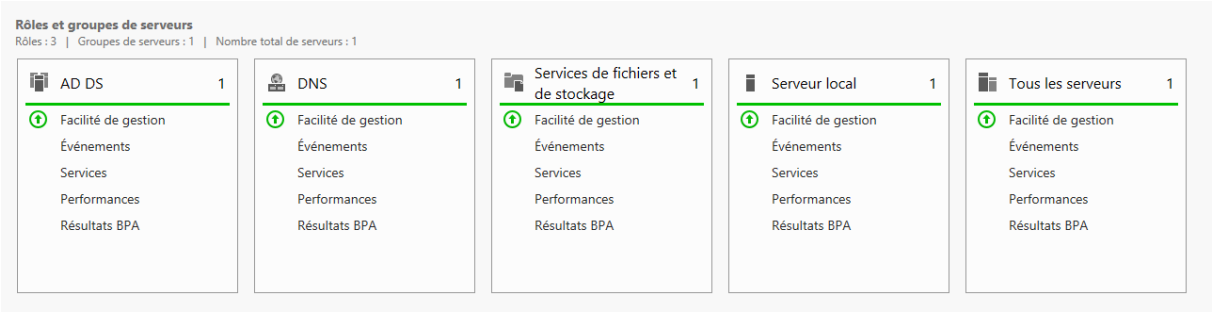


L'installation est longue car il doit installer tous les outils pour gérer la base d'annuaire, et créer un domaine, puis redémarrer le serveur.

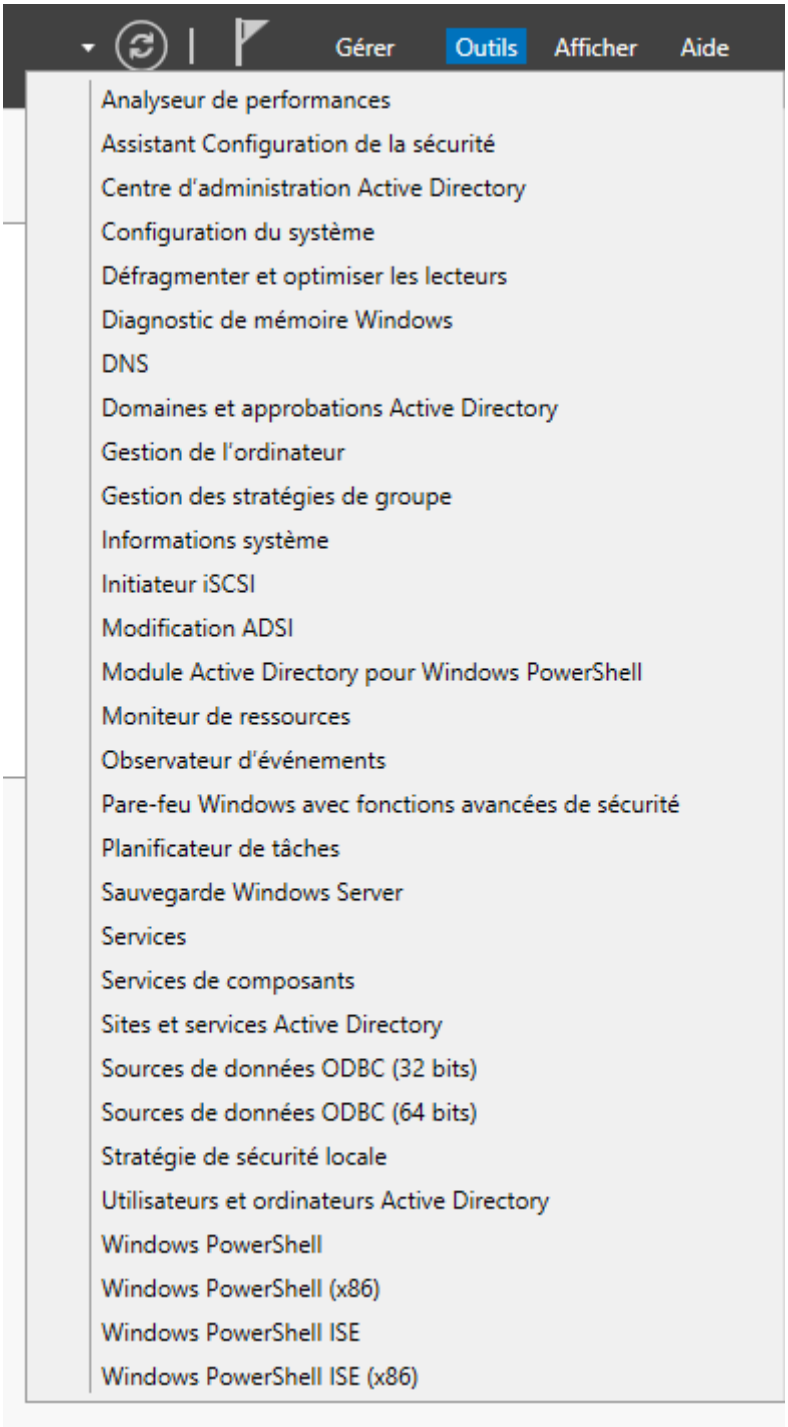
Il faut ensuite se connecter en Administrateur de domaine, et non en Administrateur local.

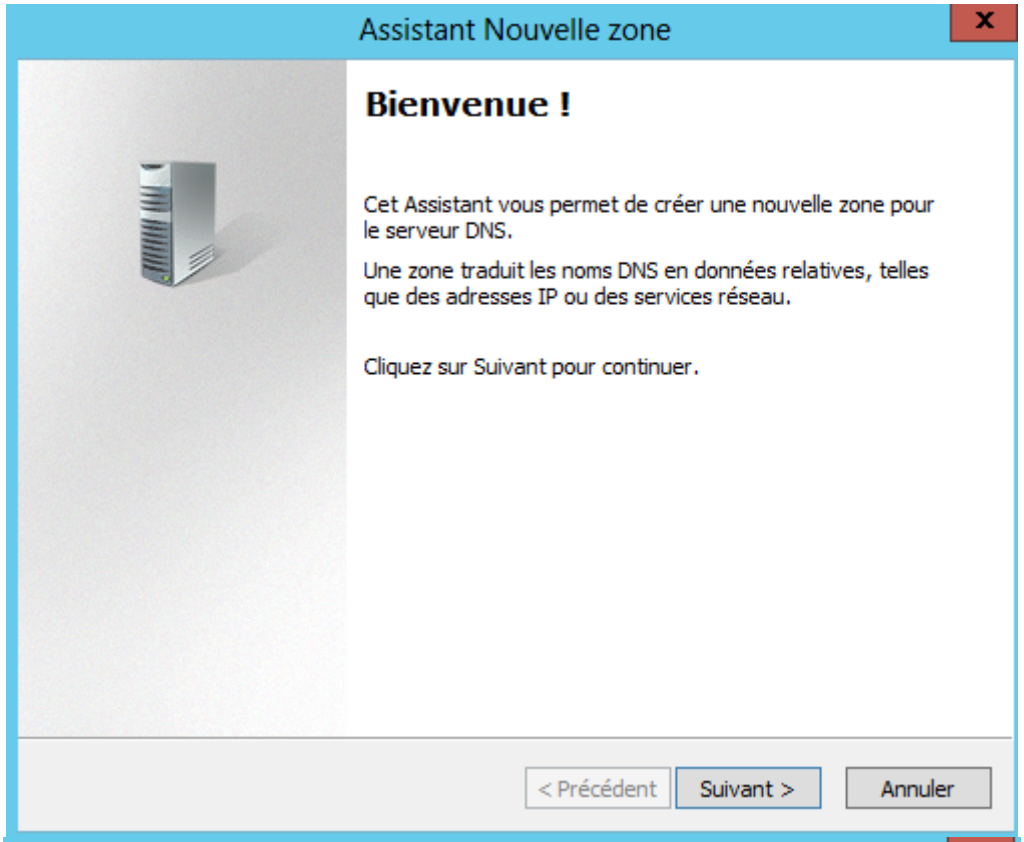
On est automatiquement placé dans le domaine :

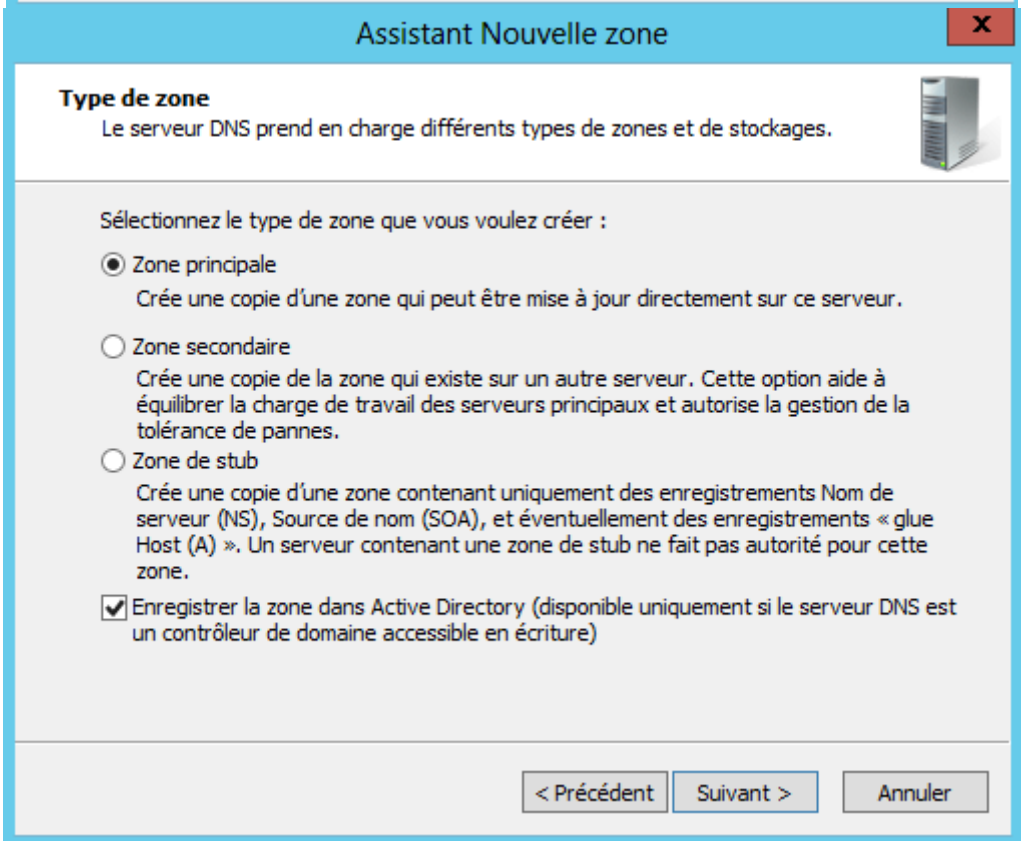
Et tous les rôles sont là :

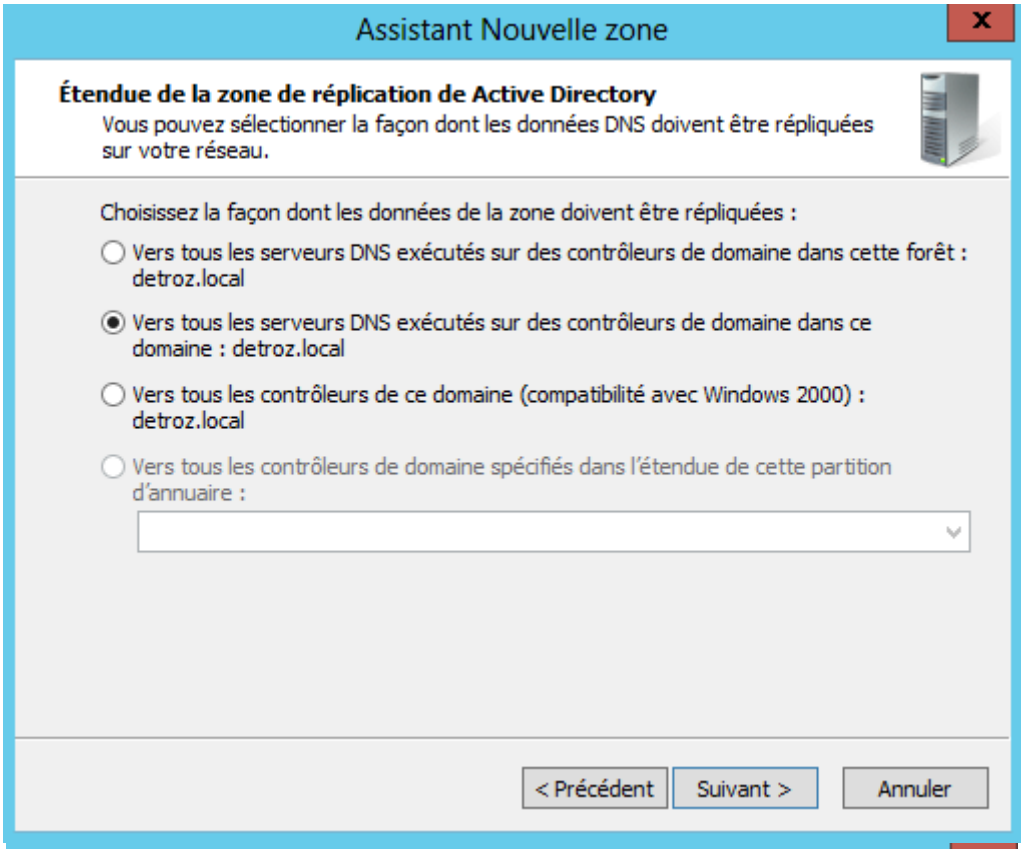


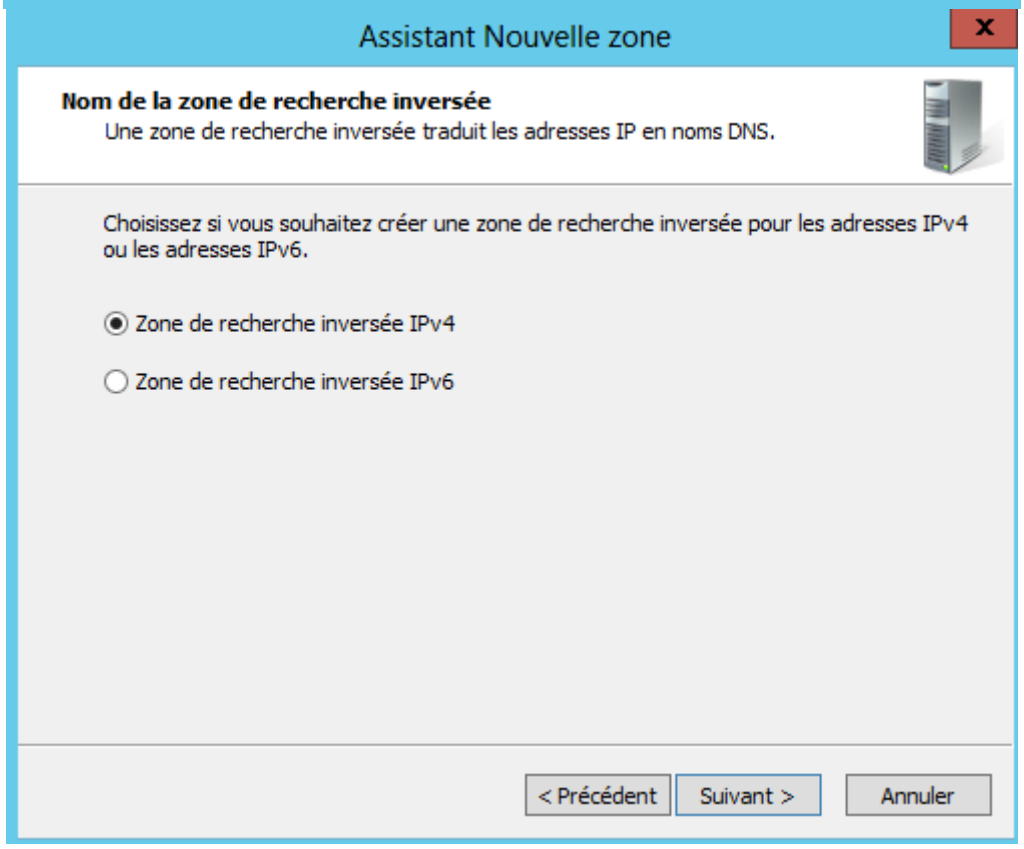
DNS :

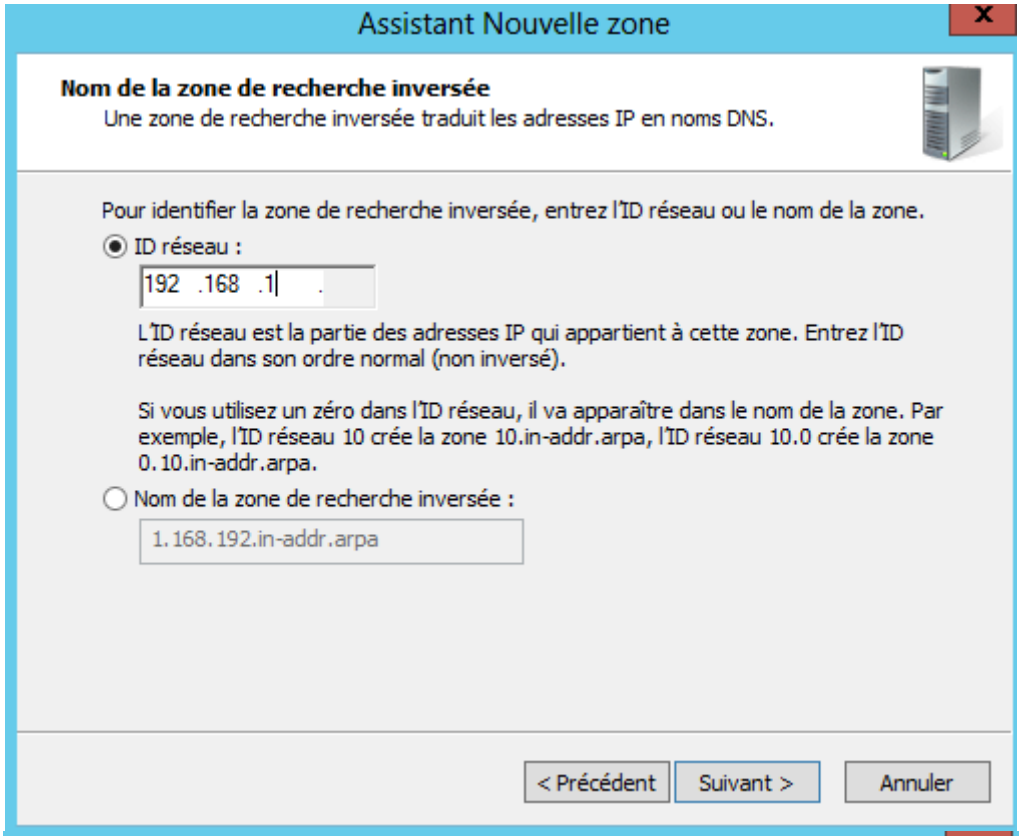

Gérer
Outils
Afficher
Aide
Analyseur de performances
Assistant Configuration de la sécurité
Centre d'administration Active Directory
Configuration du système
Défragmenter et optimiser les lecteurs
Diagnostic de mémoire Windows
DNS
Domaines et approbations Active Directory
Gestion de l'ordinateur
Gestion des stratégies de groupe
Informations système
Initiateur iSCSI
Modification ADSI
Module Active Directory pour Windows PowerShell
Moniteur de ressources
Observateur d'événements
Pare-feu Windows avec fonctions avancées de sécurité
Planificateur de tâches
Sauvegarde Windows Server
Services
Services de composants
Sites et services Active Directory
Sources de données ODBC (32 bits)
Sources de données ODBC (64 bits)
Stratégie de sécurité locale
Utilisateurs et ordinateurs Active Directory
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)

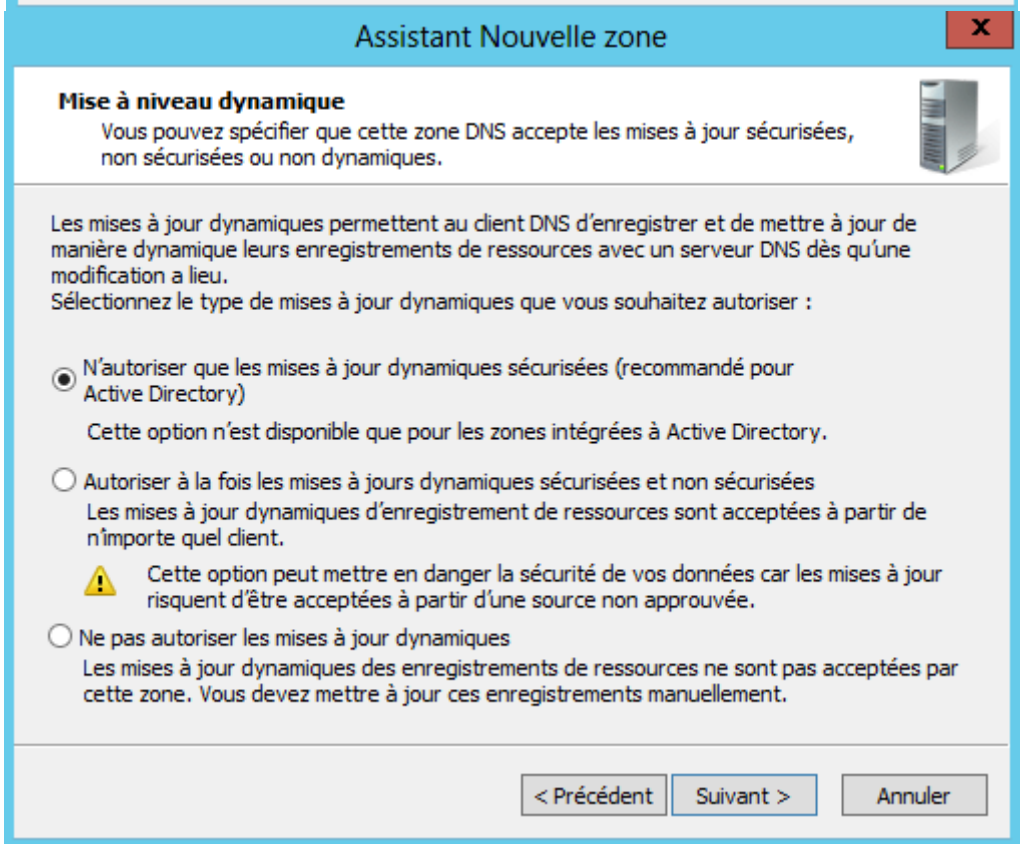

Assistant Nouvelle zone
Bienvenue !
Cet Assistant vous permet de créer une nouvelle zone pour le serveur DNS.
Une zone traduit les noms DNS en données relatives, telles que des adresses IP ou des services réseau.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

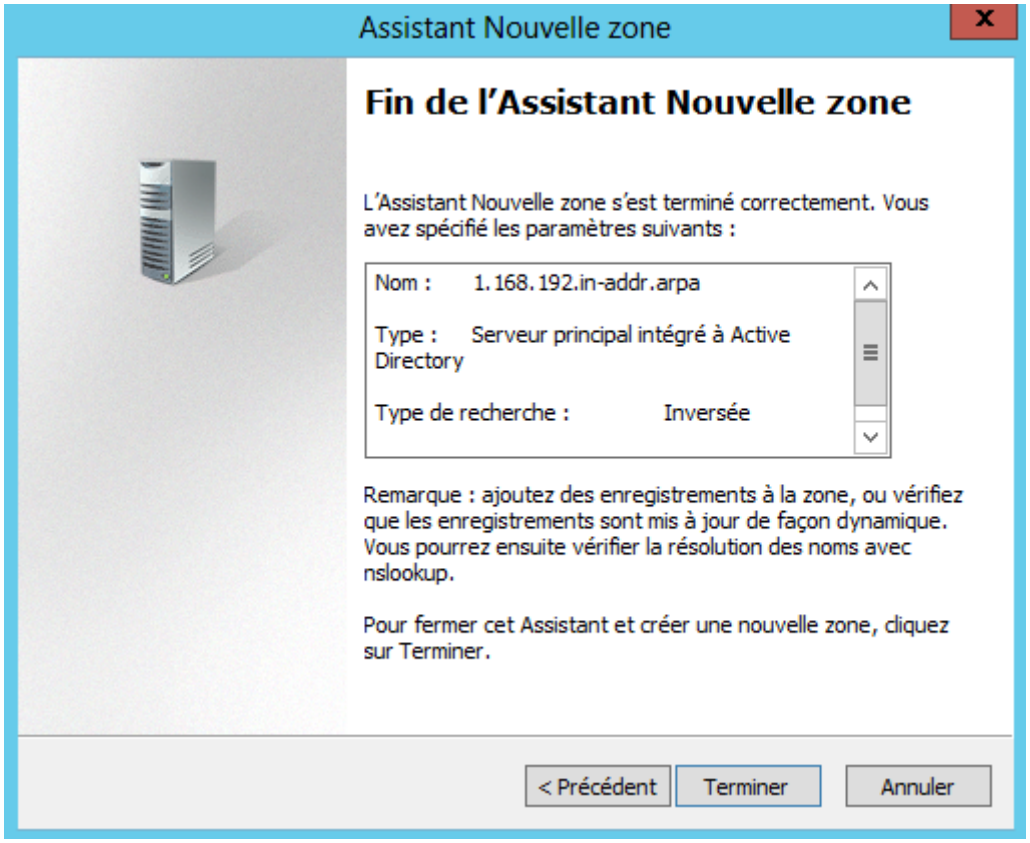

Assistant Nouvelle zone
Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.
Sélectionnez le type de zone que vous voulez créer :
Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
Zone secondaire
Crée une copie de la zone 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

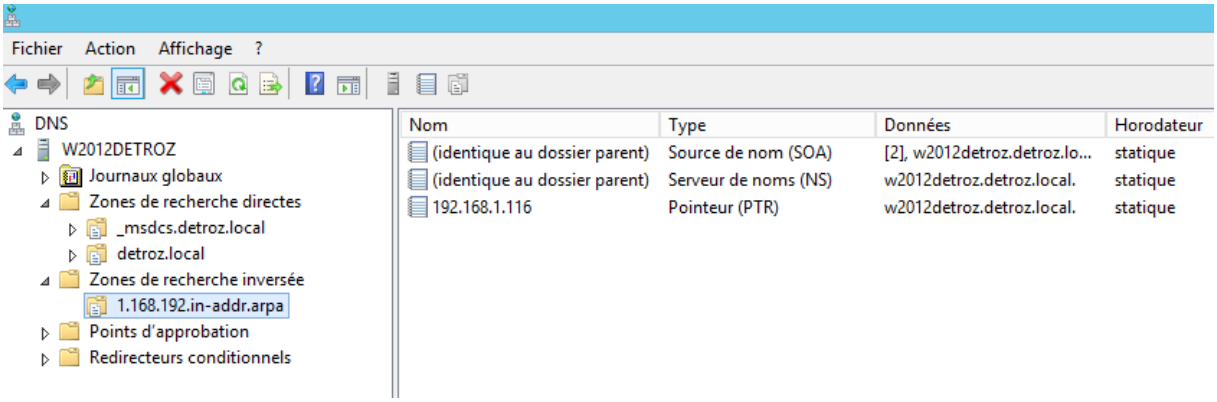

Assistant Nouvelle zone
Étendue de la zone de réplication de Active Directory
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.
Choisissez la façon dont les données de la zone doivent être répliquées :
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : detroz.local
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : detroz.local
Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : detroz.local
Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :
< Précédent
Suivant >
Annuler

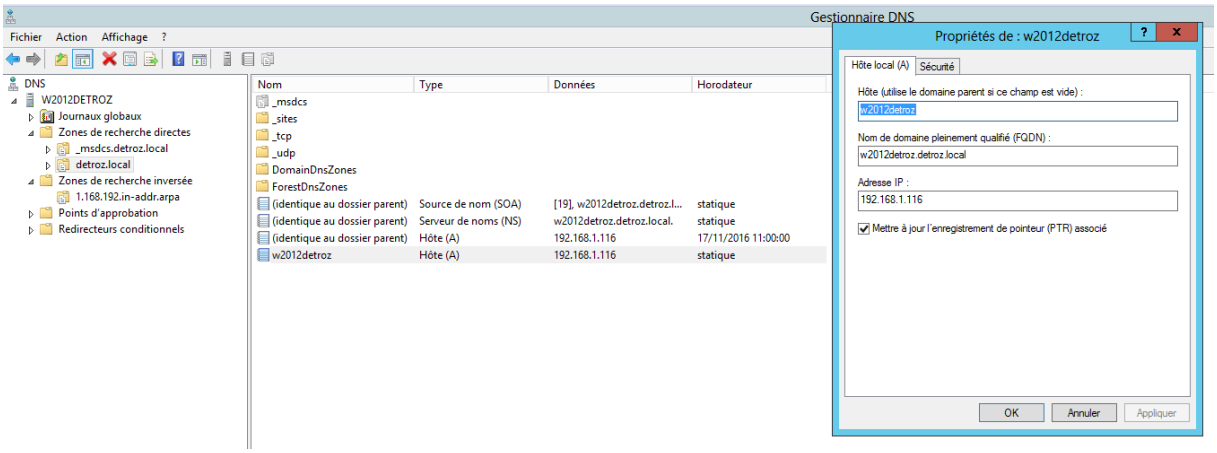

Assistant Nouvelle zone
Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.
Zone de recherche inversée IPv4
Zone de recherche inversée IPv6
< Précédent
Suivant >
Annuler


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 :
192 .168 .1
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 :
1.168.192.in-addr.arpa
< Précédent
Suivant >
Annuler


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


Assistant Nouvelle zone
Fin de l'Assistant Nouvelle zone
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :
Nom : 1.168.192.in-addr.arpa
Type : Serveur principal intégré à Active Directory
Type de recherche : Inversée
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.
< Précédent
Terminer
Annuler

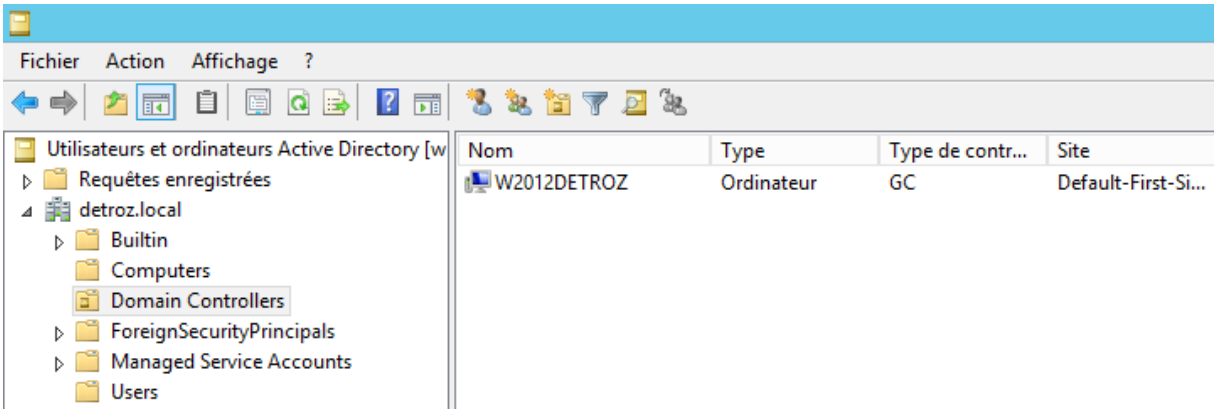

Fichier Action Affichage ?
DNS
W2012DETROZ
Journaux globaux
Zones de recherche directes
_msdcs.detroz.local
detroz.local
Zones de recherche inversée
1.168.192.in-addr.arpa
Points d'approbation
Redirecteurs conditionnels
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [2], w2012detroz.detroz.lo... statique
(identique au dossier parent) Serveur de noms (NS) w2012detroz.detroz.local. statique
192.168.1.116 Pointeur (PTR) w2012detroz.detroz.local. statique



Lorsque l'on ajoutera un nouvel hôte dans la zone de recherche directe, elle sera automatiquement insérée dans la zone inverse.

AD :

Créer les UO, puis les Groupes, et les Utilisateurs.



Le Serveur est dans Domain Controller, qui est une UO, parce que l'on doit pouvoir y attribuer une stratégie de groupe (GPO).

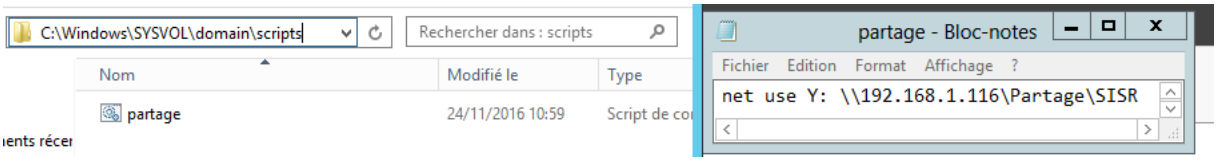
Avec 2012, on peut utiliser la commande redircmp pour rediriger un nouveau poste vers l'UO choisie. Il faut relancer la commande pour remettre la redirection par défaut.

Création d'UO :

Création de Groupes :

Création d'Utilisateurs (et de modèles) :

Créer un script de connexion :



TD Active Directory :

Déploiement et Gestion de Windows Server 2012 :

1) **Quel est l'avantage du tableau de bord de la console Gestionnaire de serveur ?**

   L'avantage du tableau de bord est que l'on peut visualiser l'ensemble des informations, des fonctionnalités, des rôles de notre serveur. De nombreux liens permettent d'accéder à toutes les configurations (AD, DNS, IP, Bureau à distance, etc…).

2) **Quels sont les types d'installation que l'on peut trouver sur Windows Server 2012 ?**

   On peut trouver l'installation minimale sans interface graphique, dite « core », et l'installation complète avec interface graphique.

3) **Quel est l'avantage d'installer un serveur en mode Core ?**

   L'avantage d'un serveur en mode core est qu'il est moins volumineux et peut être installé sur des serveurs peu puissants, moins de mise à jour, plus de sécurité car moins soumis aux attaques, pas de grosse carte graphique, pas d'interface. Et la version nano-serveur est encore plus légère et est administrable en PowerShell.

4) **Citez quelques rôles et fonctionnalités présents sur Windows Server 2012.**

   Windows Server 2012 peut être un contrôleur de domaine, un serveur DNS, DHCP.

5) **Quel est le rôle à installer si vous souhaitez distribuer des certificats numériques ?**

   Il faut installer un rôle de certification SSL.

6) **Quel est le rôle d'un serveur AD DS ?**

   Un serveur AD DS est un annuaire qui répertorie tous les utilisateurs et leurs informations d'authentification pour leur permettre de rejoindre un domaine.

Services Active Directory :

7) **Qu'est-ce qu'un domaine Active Directory ?**

   Un domaine Active Directory est un annuaire d'utilisateurs, d'ordinateurs et de groupes, réunissant des informations et des droits sur ces différents objets.

8) **Qu'est-ce qu'une forêt Active Directory ?**

Une forêt est constituée d'un ou plusieurs domaines Active Directory. Une forêt Active Directory est donc composée d'une suite de domaines appelées également une arborescence de domaines.

9) Citez les partitions dans Active Directory.

Partition de domaine : Elle contient les informations des différents objets qui ont été créés sur le domaine (attributs de compte utilisateur et ordinateur…).
Partition de configuration : La topologie de l'annuaire (liste complète des domaines, arborescences) est décrite dans cette partition.
Partition de schéma : Elle contient tous les attributs et classes de tous les objets qui peuvent être créés.
Partition DNS : L'ensemble des zones et donc des enregistrements est stocké dans cette partition.

10) Quelle est l'utilité d'un serveur catalogue global ?

Administration des objets AD :

11) Citez les attributs d'un compte utilisateur qui sont obligatoires lors de la création.

12) Que peut-on voir avec l'onglet Éditeurs d'attributs ? Les valeurs qu'il contient sont-elles modifiables ?

13) Comment fonctionne un profil itinérant ?

14) Citez les types d'étendues de groupe que l'on peut trouver.

15) Quelle est l'utilité de la commande redircmp ?

La commande **redircmp** permet de rediriger un ordinateur vers une UO. Cette commande défini le « chemin par défaut » des ordinateurs nouvellement créés vers l'UO choisie. Il faut donc relancer la commande pour remettre le chemin d'origine.

Stratégies de groupe :

16) Où sont stockés les différents composants de la GPO et comment se répliquent-ils ?

17) Quel est le but d'une GPO Starter ?

18) Quel est l'ordre d'application d'une GPO ?

Les GPO sont appliquées dans l'ordre de l'arborescence, c'est-à-dire que la plus haute est d'abord appliquée sur tout le domaine, puis viennent les GPO des UO. La dernière GPO (la plus profonde dans la racine) est celle qui a le dernier mot. Par exemple, si on interdit au domaine de changer de fond d'écran, et qu'on autorise une UO spécifique à le changer, c'est l'autorisation qui l'emporte, car elle est appliquée en dernier.

19) À quel moment est appliquée une stratégie de groupe ?

Une stratégie de groupe est appliquée lors de l'authentification de l'utilisateur sur le domaine.

20) Est-il possible de forcer la mise à jour depuis la console GPMC ?

Oui, avec la commande **gpupdate /force** sur la console de l'utilisateur.

21) Quelles sont les stratégies de groupe par défaut ?

Les stratégies de groupe par défaut sont :

- Default Domain Policy : Qui gère les stratégies de groupe pour tout le domaine.
- Default Domain Controllers Policy : Qui gère les stratégies de groupe pour les contrôleurs de domaine du domaine, soit ici, notre serveur.