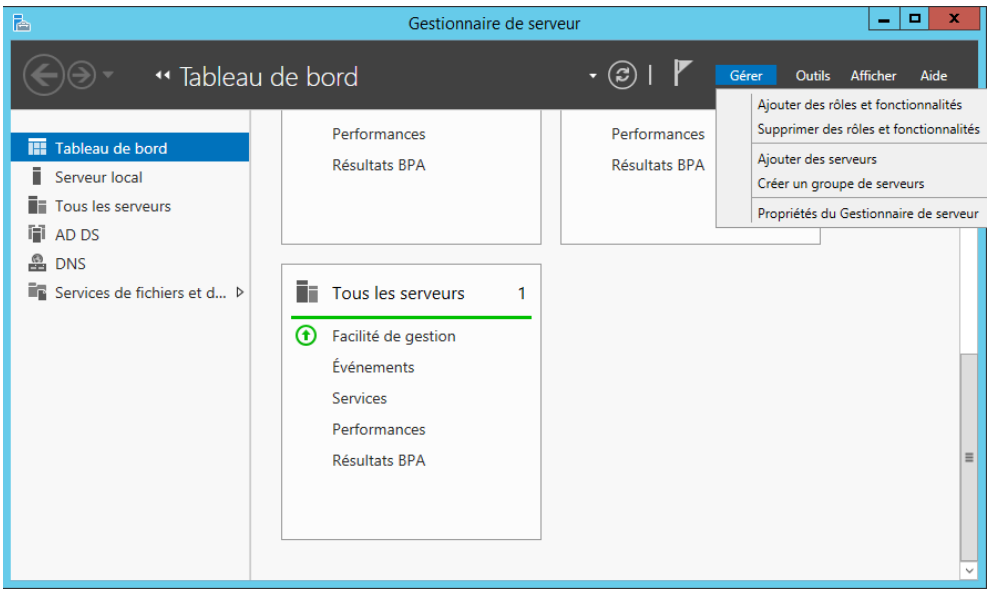
ACTIVE DIRECTORY : WINDOWS SERVER 2012 R2

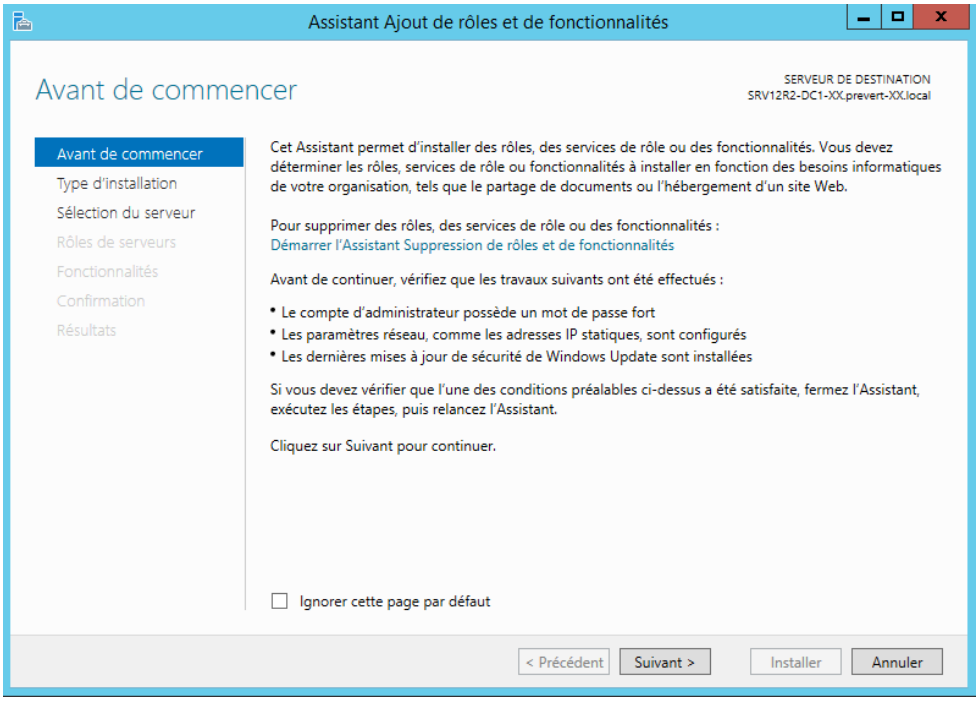
Source : http://www.it-connect.fr/creer-un-domaine-sous-windows-server-2012/

Installation du rôle ADDS

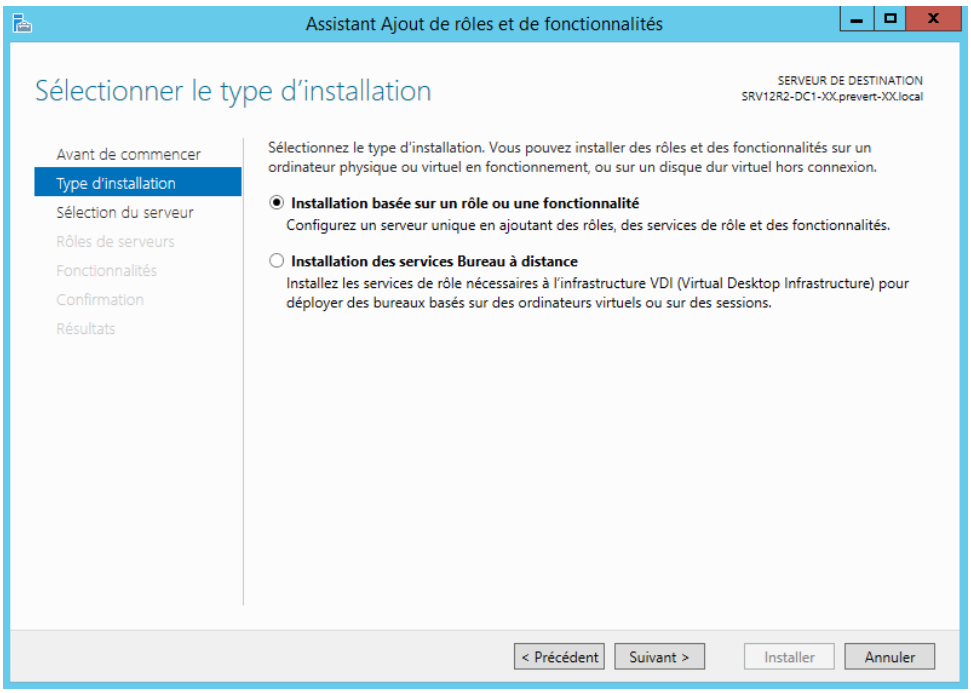
Avant de promouvoir le serveur en tant que contrôleur de domaine dans un nouveau domaine, il faut installer le rôle « Service de domaine Active Directory ».
Pour cela, dans la page d'accueil, cliquez sur « Gestionnaire de serveur ». Une fois que vous y êtes, cliquez sur « Ajouter des rôles et des fonctionnalités » présent dans la section « Démarrage rapide ».



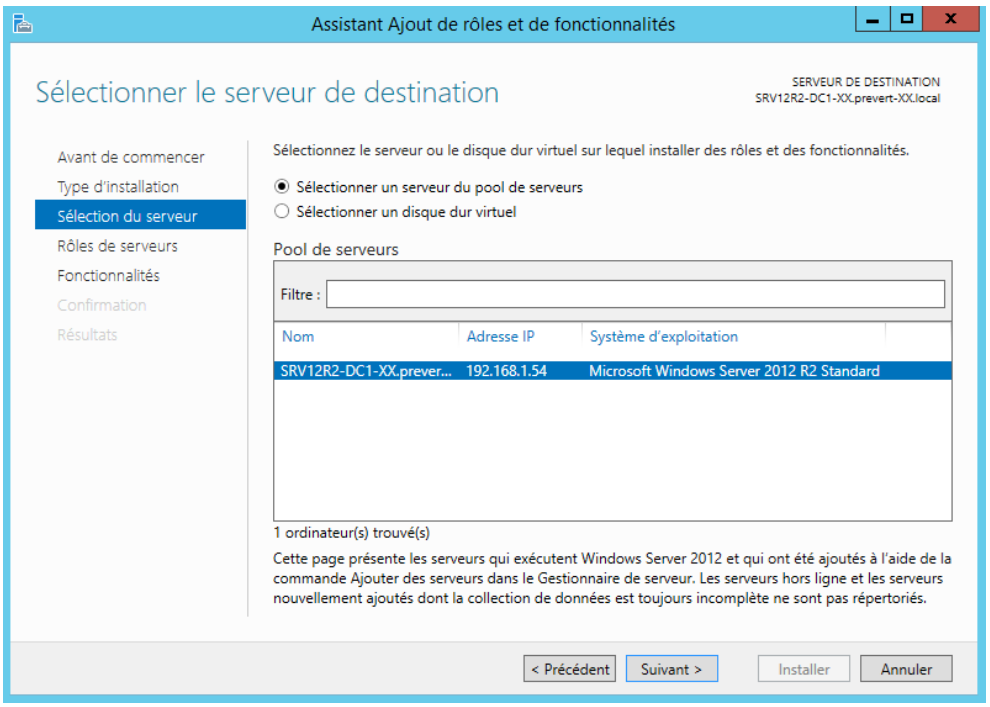
L'assistant s'exécute et vous demande de vous assurer que le compte Administrateur possède un mot de passe fort, que la configuration réseau est en adresse statique et que votre serveur est à jour au niveau des mises à jour de sécurité. Cliquez sur « Suivant ».



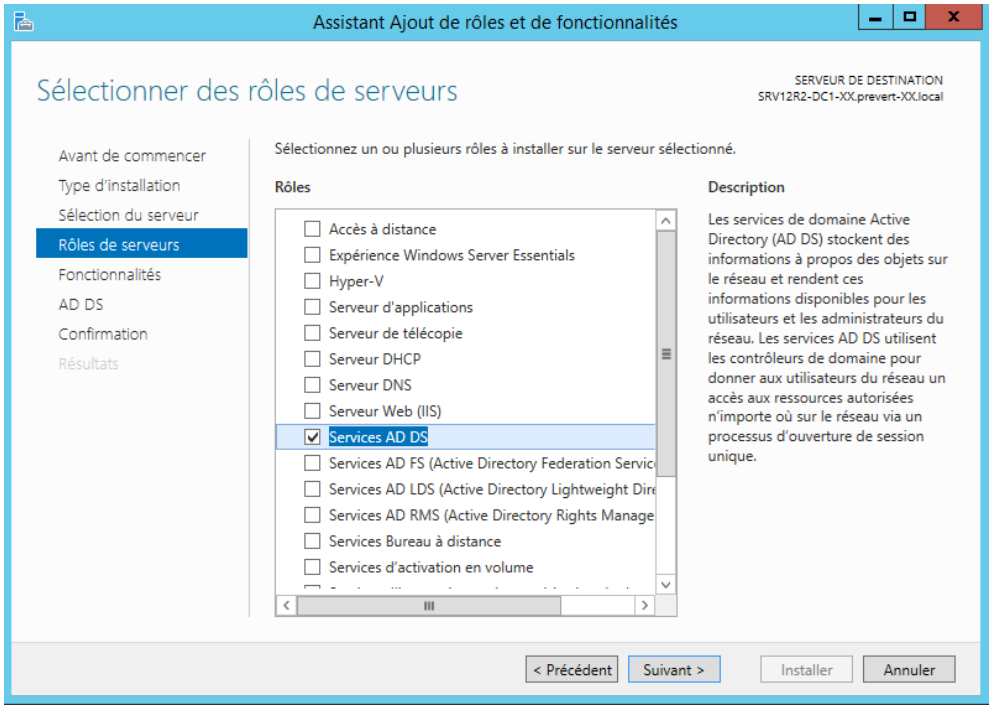
Laissez le choix par défaut puisque nous souhaitons ajouter un nouveau rôle à notre serveur et non installer des services de Bureau à distance comme le propose le second choix.



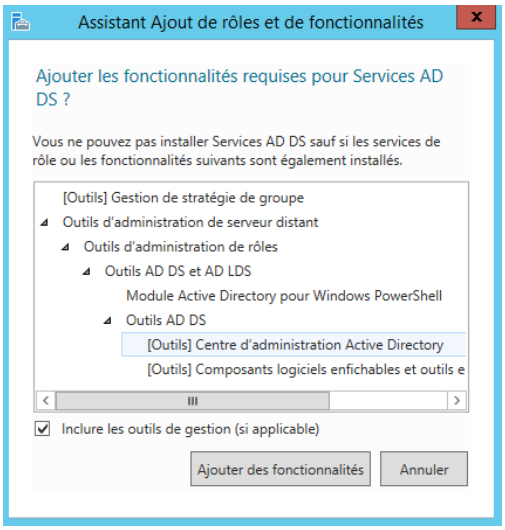
Sélectionner le serveur de destination dans la liste indiquée et cliquer sur « Suivant ». Ceci est une nouveauté de Windows Server 2012 qui permet à partir d'un serveur de gérer plusieurs autres serveurs qui sont configurés pour être gérés par un autre serveur. Dans notre cas, il n'y a qu'un seul serveur, le choix est donc restreint.

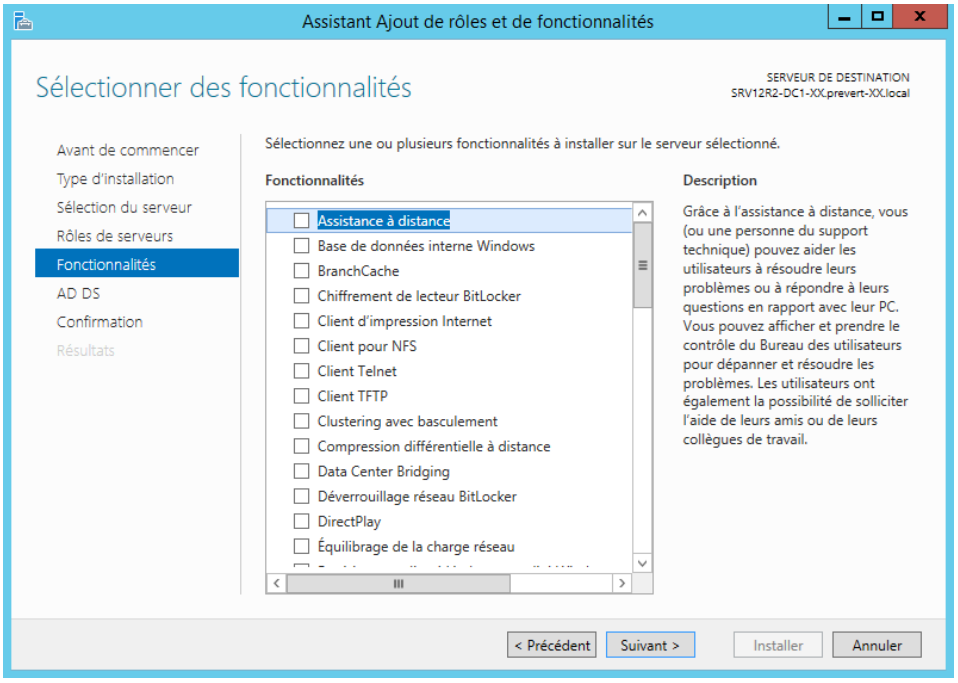


Au niveau des rôles, sélectionnez «Service AD DS» qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour vous indiquer que d'autres éléments requis par AD DS doivent être installés, cliquez sur « Ajouter des fonctionnalités ». Ensuite, cliquez sur « Suivant ».

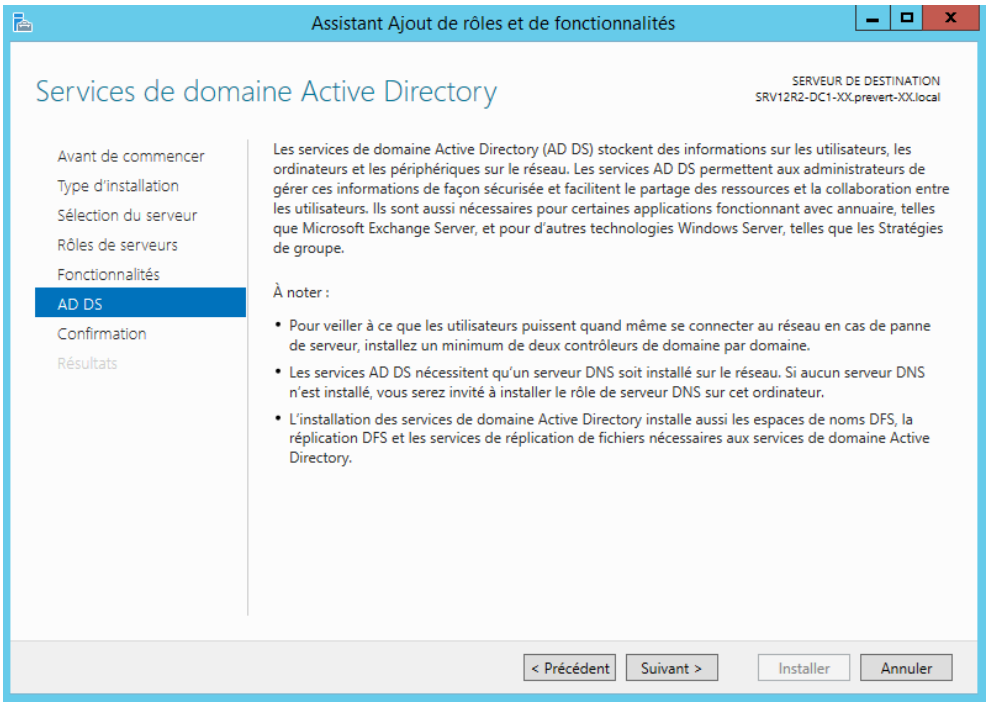


Au niveau des fonctionnalités, nous avons besoin de rien, cliquez sur « Ajouter des fonctionnalités » puis sur « Suivant » directement.

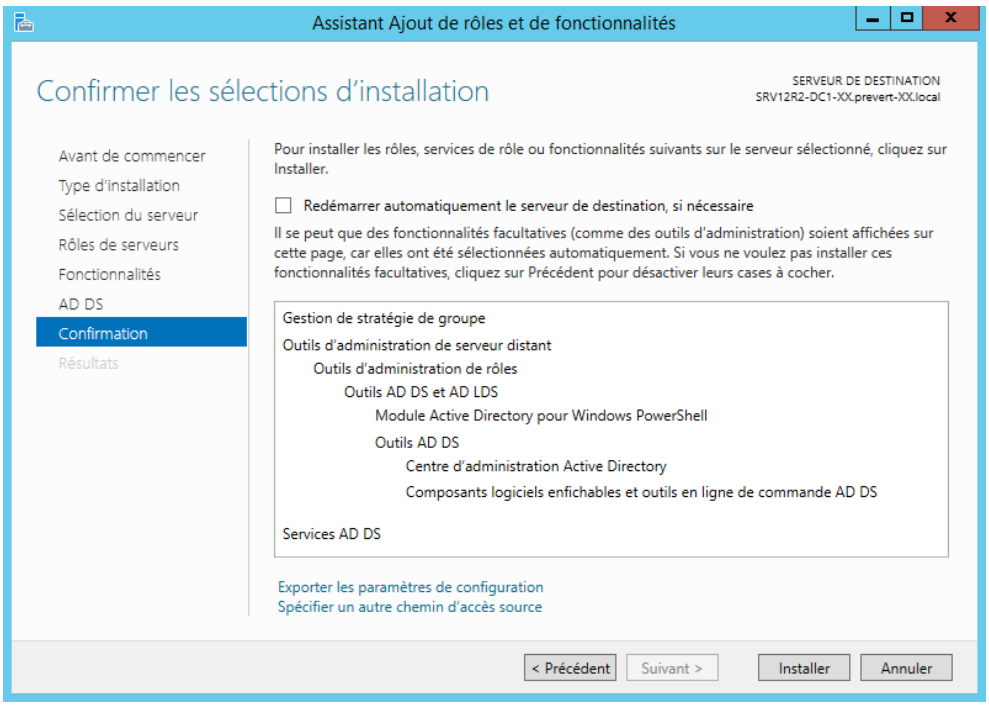




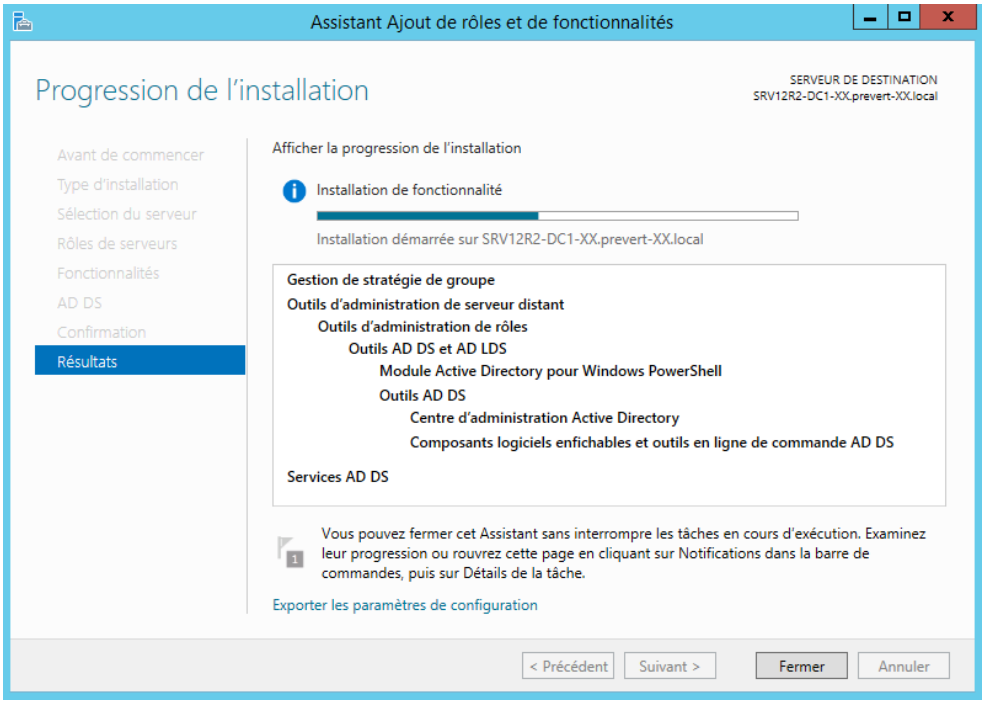
Lisez les explications concernant AD DS et cliquez sur « Suivant » à nouveau.



Un récapitulatif des éléments qui vont être installés et affichés, cliquez sur « Installer » pour exécuter l'installation des divers éléments.

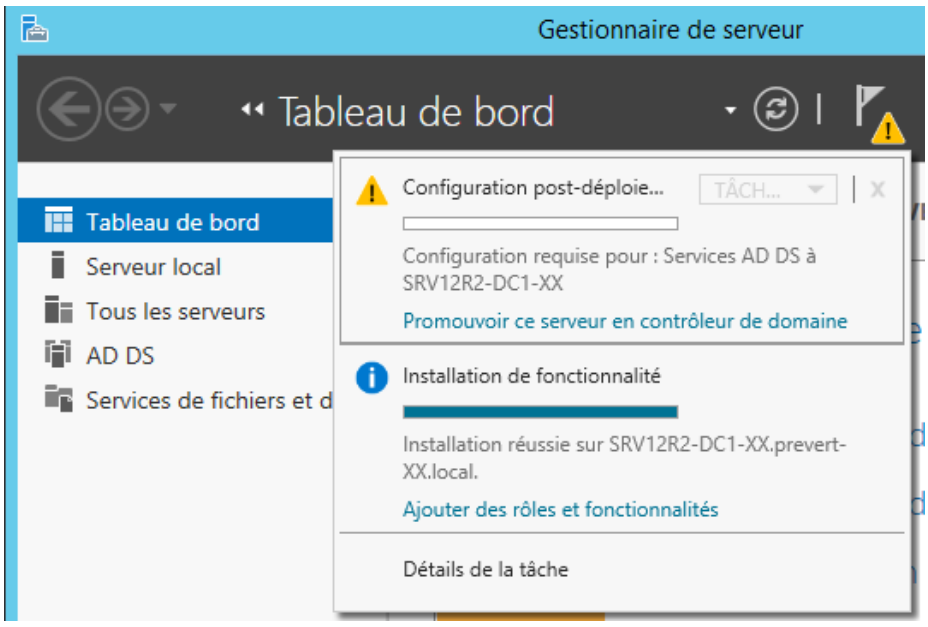


Une fois terminé c'est-à-dire que le message «Installation réussie sur SRV12R2-DC1-XX» apparaît, cliquez sur «Fermer».

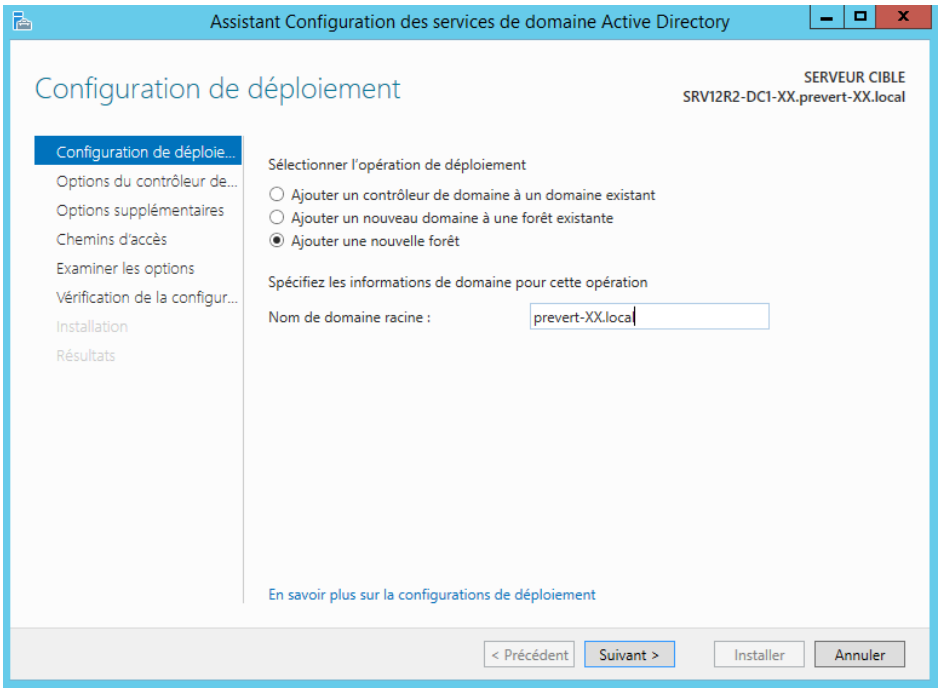


Promouvoir en tant que contrôleur de domaine

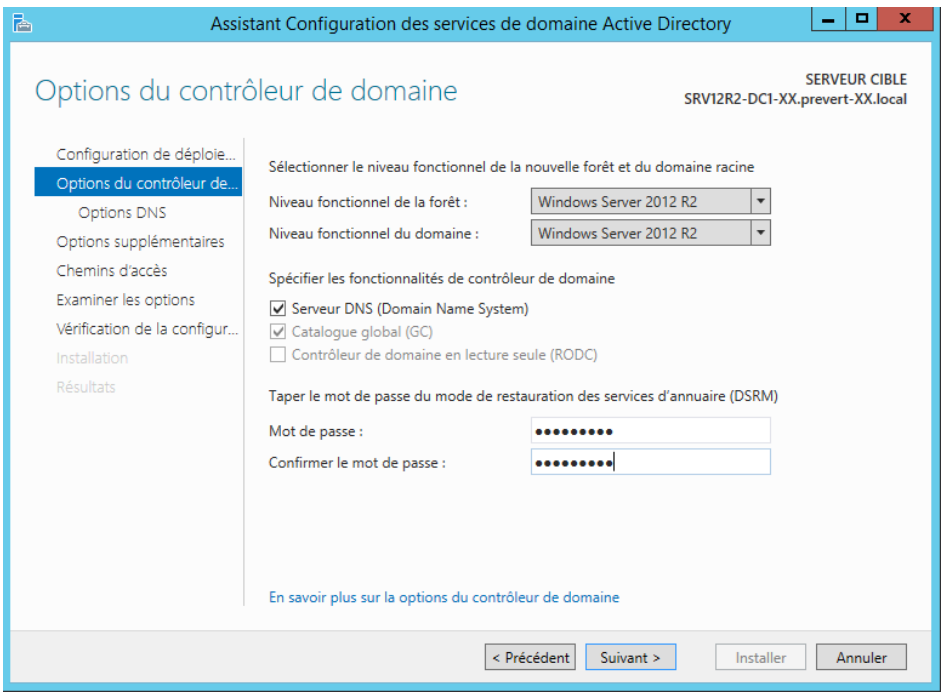
Afin de promouvoir notre serveur en tant que contrôleur de domaine, vous avez l'habitude d'effectuer la commande « dcpromo » qui permet d'exécuter l'assistant de promotion de serveur.
Avec Windows Server 2012, dans le Gestionnaire de serveur un symbole d'avertissement apparaît auprès du Centre de maintenance, cliquez dessus et vous verrez apparaître ceci :



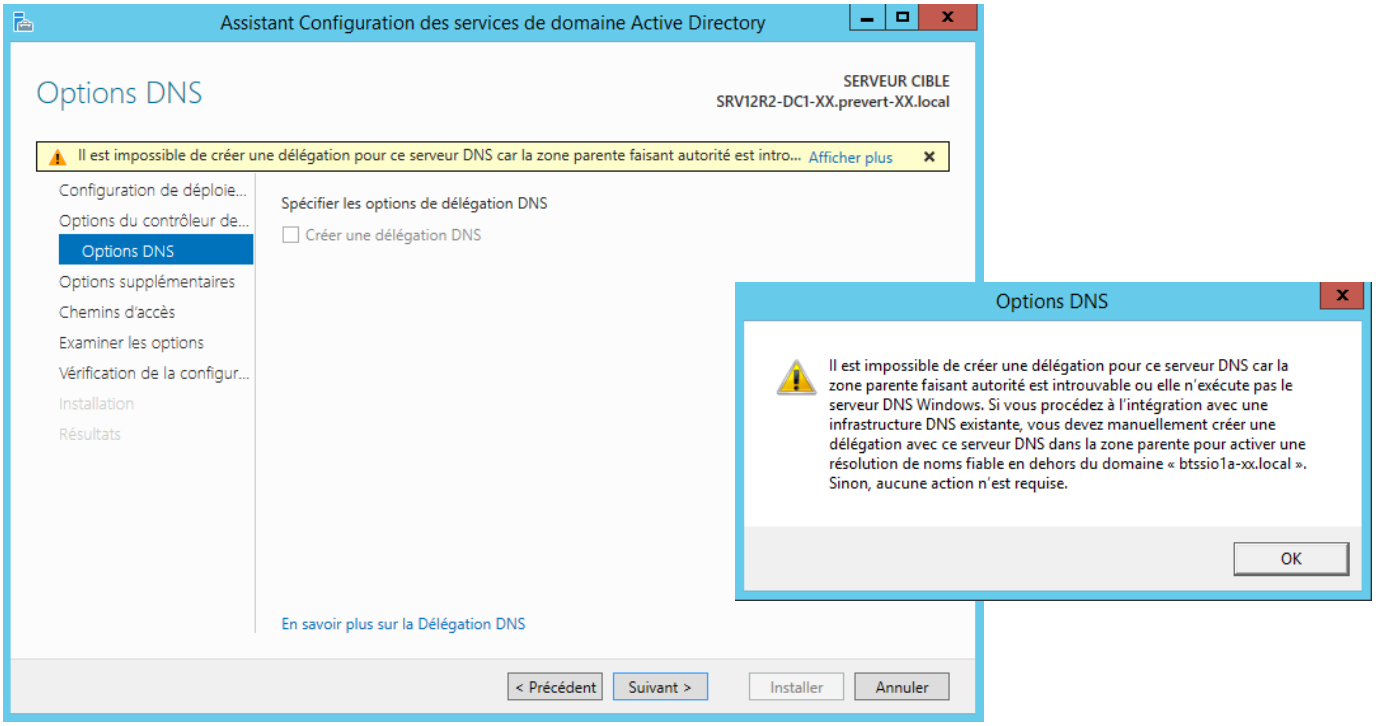
Il vous suffit de cliquer sur «Promouvoir ce serveur en contrôleur de domaine» pour exécuter l'équivalent d'un DCPROMO sous Windows Server 2012.
Vu que nous souhaitons créer un nouveau domaine appelé «**prevert-xx.local**», nous devons déployer une nouvelle forêt (une forêt étant un ensemble de domaines, ce qui permet d'ajouter d'autres domaines dans cette forêt par la suite). Cochez « Ajouter une nouvelle forêt » et indiquez «**prevert-xx.local**».

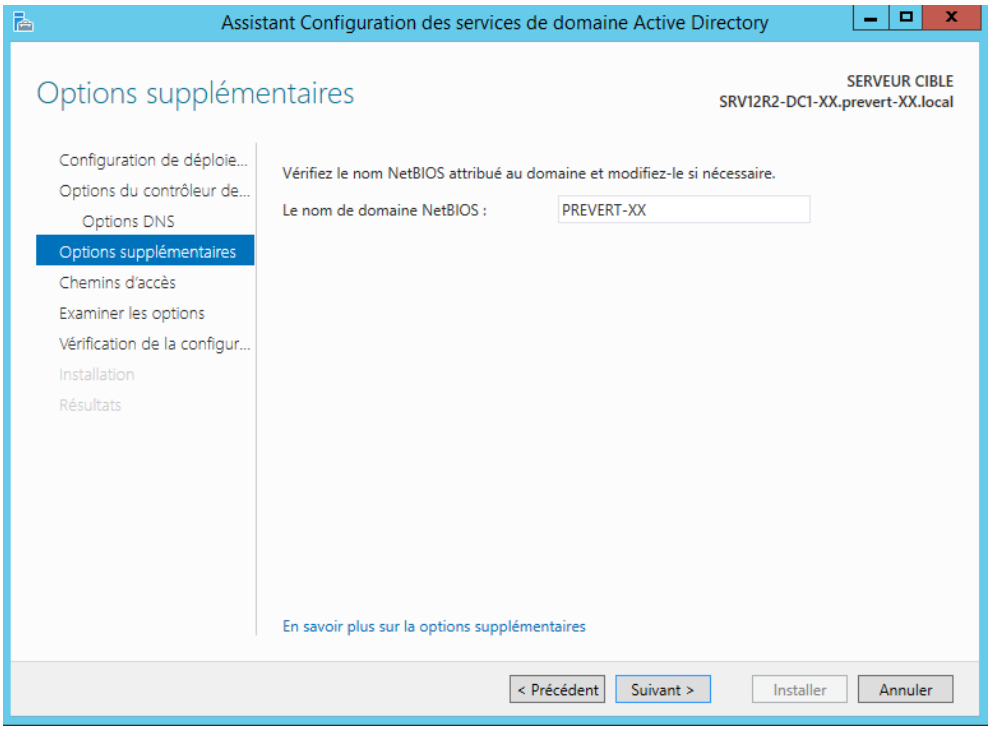


Note: Un domaine créé à partir d'un serveur Windows Server 2012R2 peut fonctionner uniquement sur un niveau fonctionnel «Windows Server 2012R2». Cependant, le niveau fonctionnel de la forêt quant à lui peut aller de « Windows Server 2003 » à «Windows Server 2012R2».
Choisissez le niveau fonctionnel qui vous convient le mieux pour la forêt. Cela dépend de ce que vous prévoyez à l'avenir, dans le cas où vous créez d'autres domaines dans cette forêt vous allez devoir adaptez le système d'exploitation embarqué par vos serveurs par rapport au niveau fonctionnel sélectionné.
Pour information, on peut augmenter le niveau fonctionnel, mais en aucun cas le diminuer.
Sélectionner «Windows Server 2012R2» pour les deux niveaux fonctionnels. Laissez coché «Serveur DNS» puisque ce serveur servira également de serveur DNS sur le domaine et indiquez un mot de passe de restauration des services d'annuaires. Une fois que tout est renseigné, cliquez sur «Suivant»

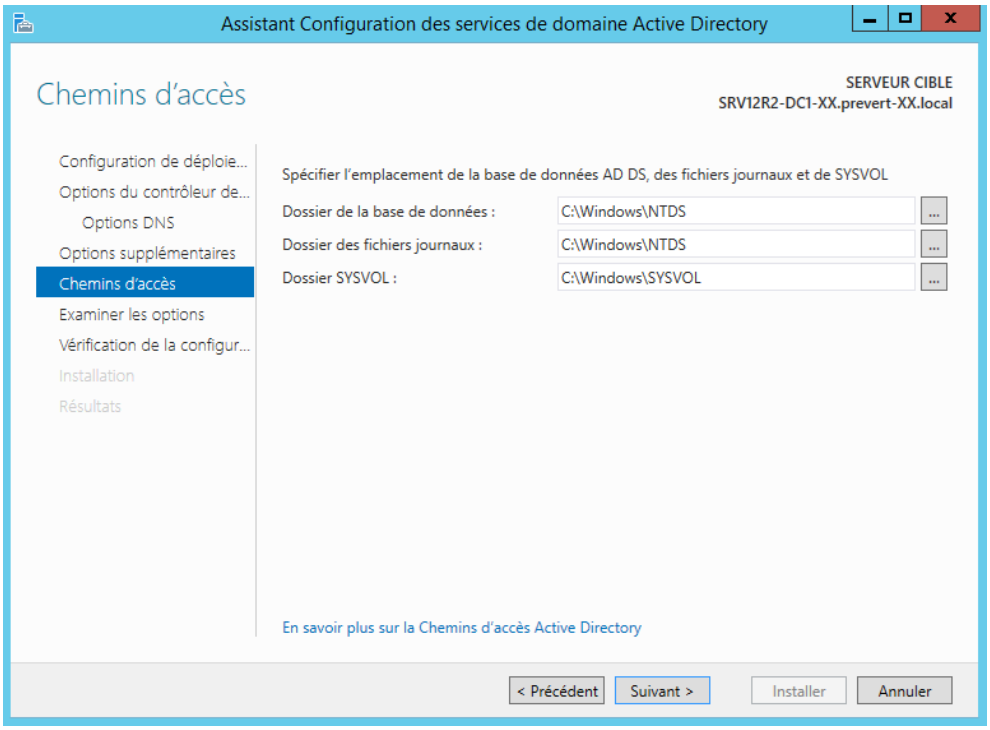


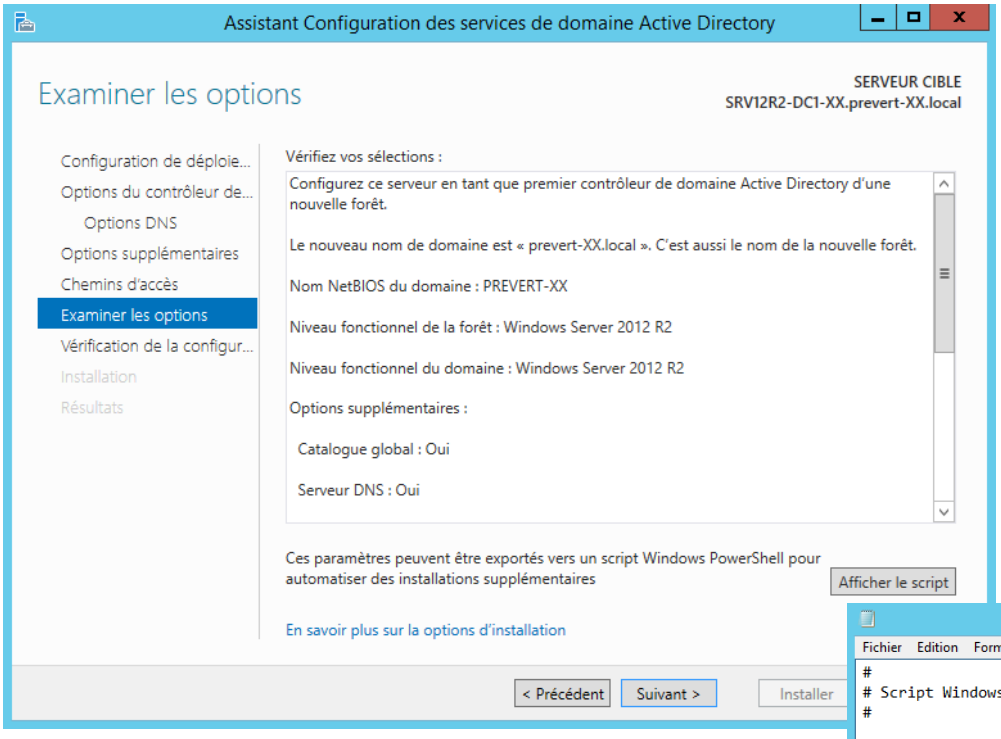
En ce qui concerne les options DNS, faites suivant puisqu'il n'y a aucune modification à effectuer. Ensuite, patientez pendant l'affichage du nom NETBIOS de votre domaine et modifiez le si nécessaire, le nom NETBIOS permet notamment d'ouvrir une session et de s'authentifier sur le domaine. Exemple, ouvrir une session «user1» sur le domaine «prevert-XX.local» ayant pour nom NETBIOS «PREVERT» : «PREVERT\user1».

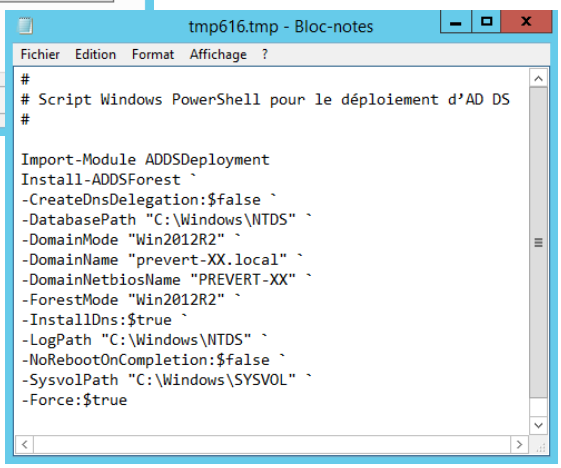




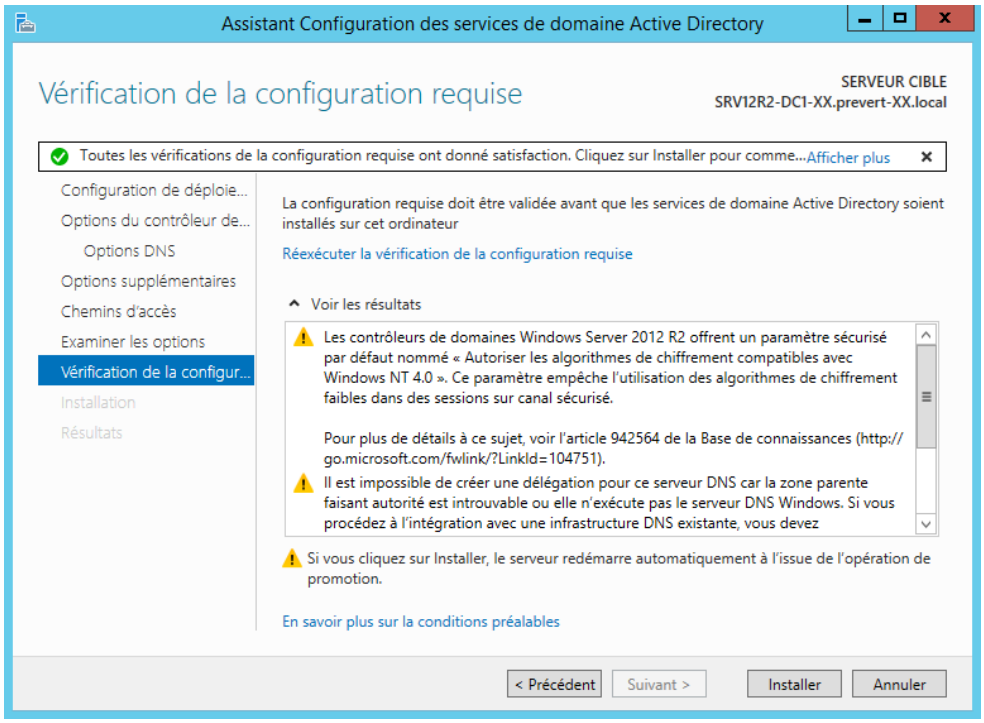
Lorsqu'on vous demande de choisir les différents chemins d'accès pour le dossier SYSVOL, la base de données et les fichiers journaux, laisser les paramètres par défaut afin de rester standard et d'être sûr de pouvoir les retrouver facilement.

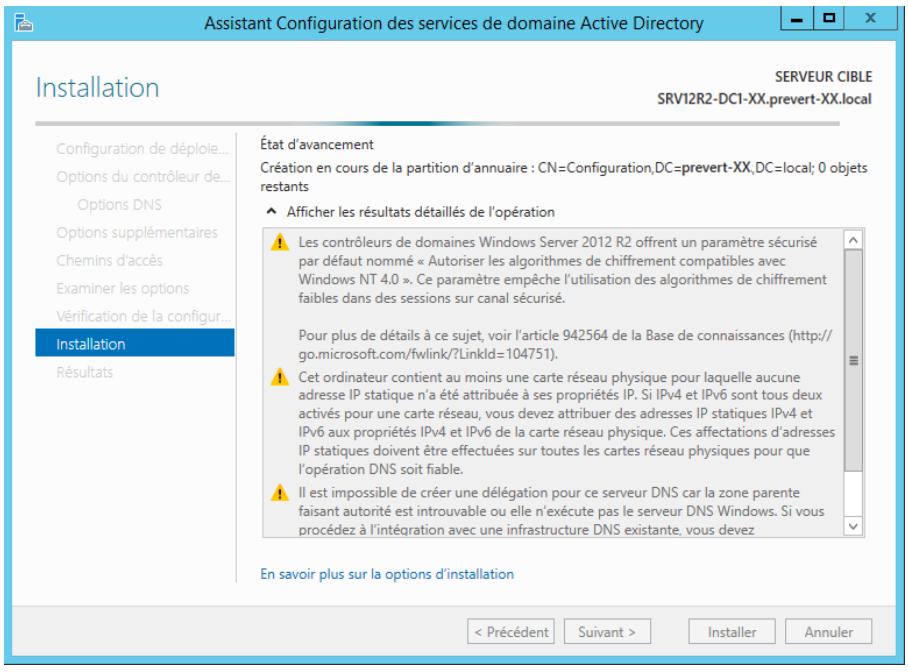




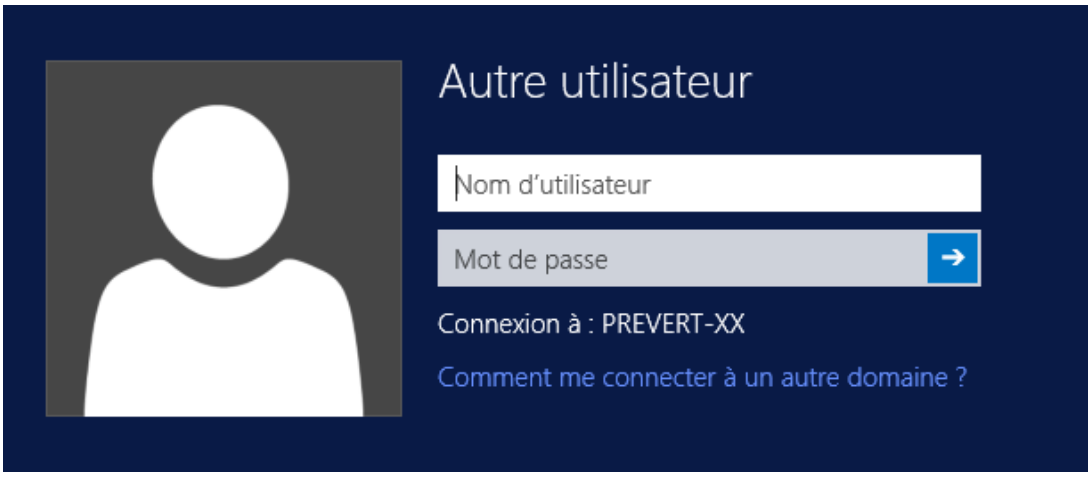


Cliquez sur « Suivant », puis examinez une dernière fois les options que vous avez définies dans la page récapitulative. Une fois que le tour est fait, cliquez une seconde fois sur « Suivant ».
Enfin, vérifiez qu'il n'y a pas d'erreur(s) critique(s) et cliquez sur « Installer ». Le serveur redémarrera automatiquement une fois le déploiement terminé.

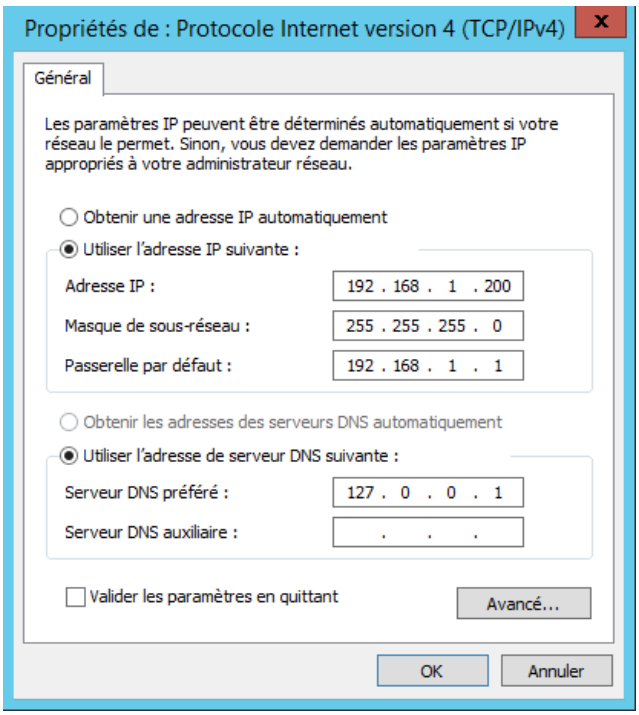




Une fois le serveur redémarré, connectez-vous avec le compte Administrateur présent désormais dans l'Active Directory et commencez à administrer votre domaine.

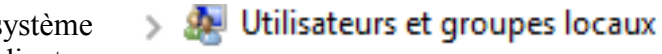


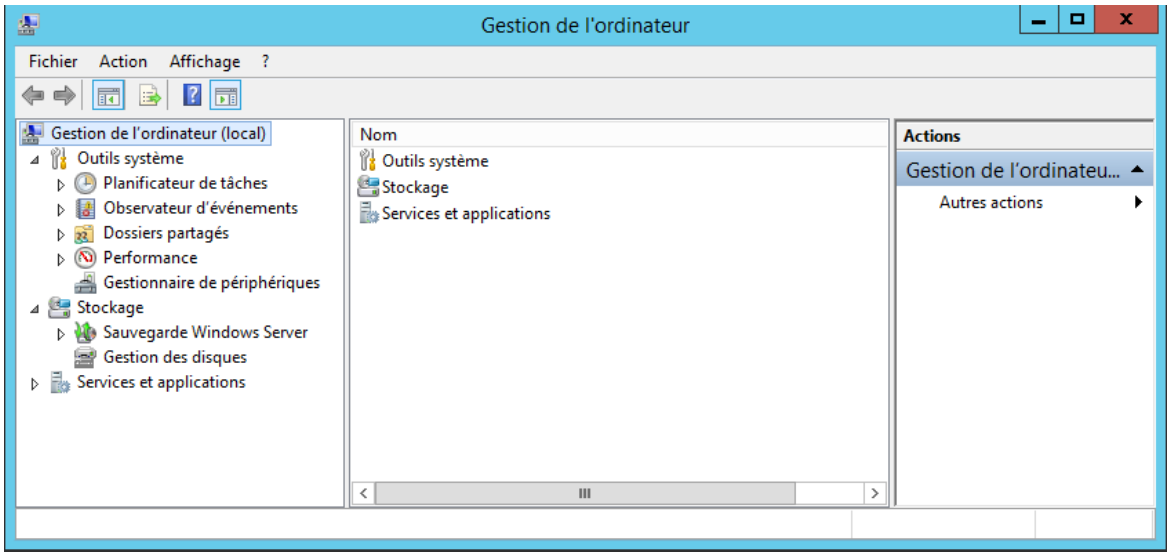
Vous devez vérifier une nouvelle fois le paramétrage du serveur DNS dans la connexion réseau. Le DNS préféré doit pointer sur le serveur A.D. :



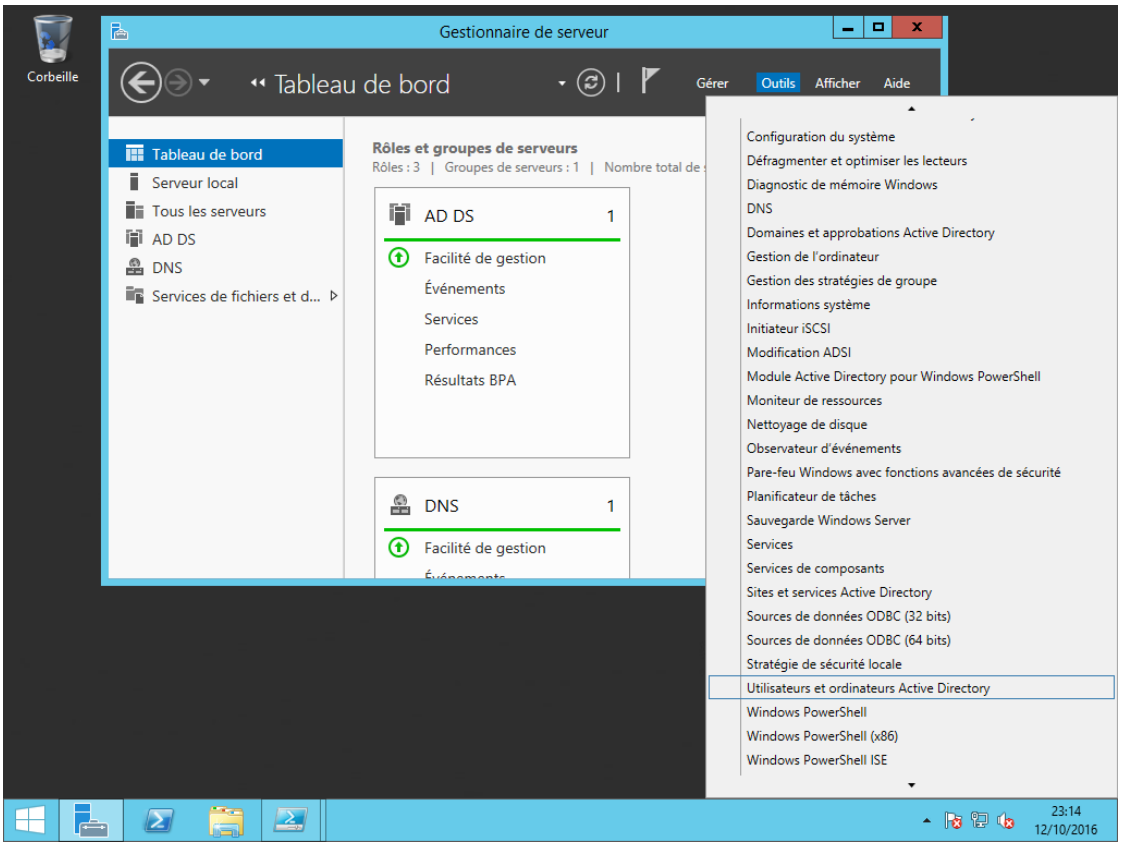
Sur l'image écran, le serveur DNS préféré est : 127.0.0.1. C'est l'IP de bouclage correspondant bien au serveur. On peut aussi utiliser l'IP : 192.168.1.200

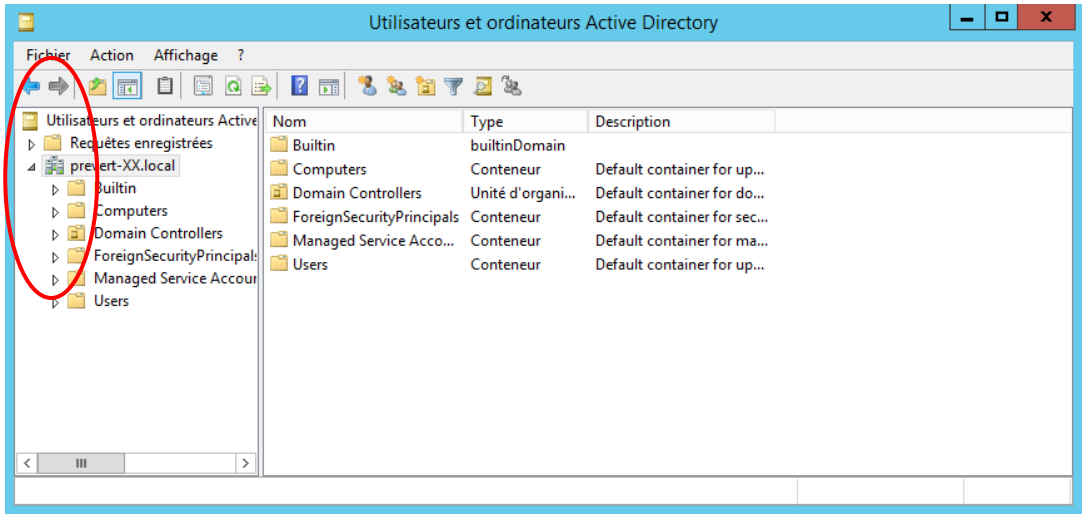
Vous pouvez constater que l'outils système N'existe plus dans la gestion de l'ordinateur





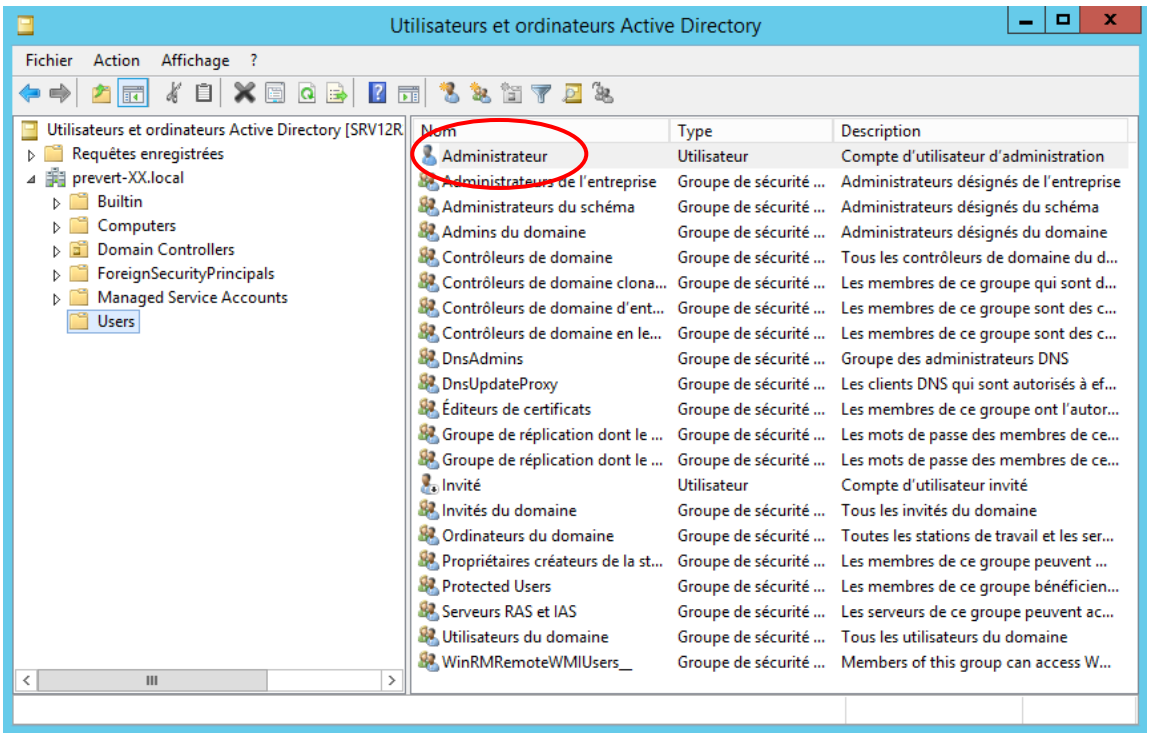
C'est maintenant Utilisateur et ordinateur Active Directory qui prend en charge les utilisateurs



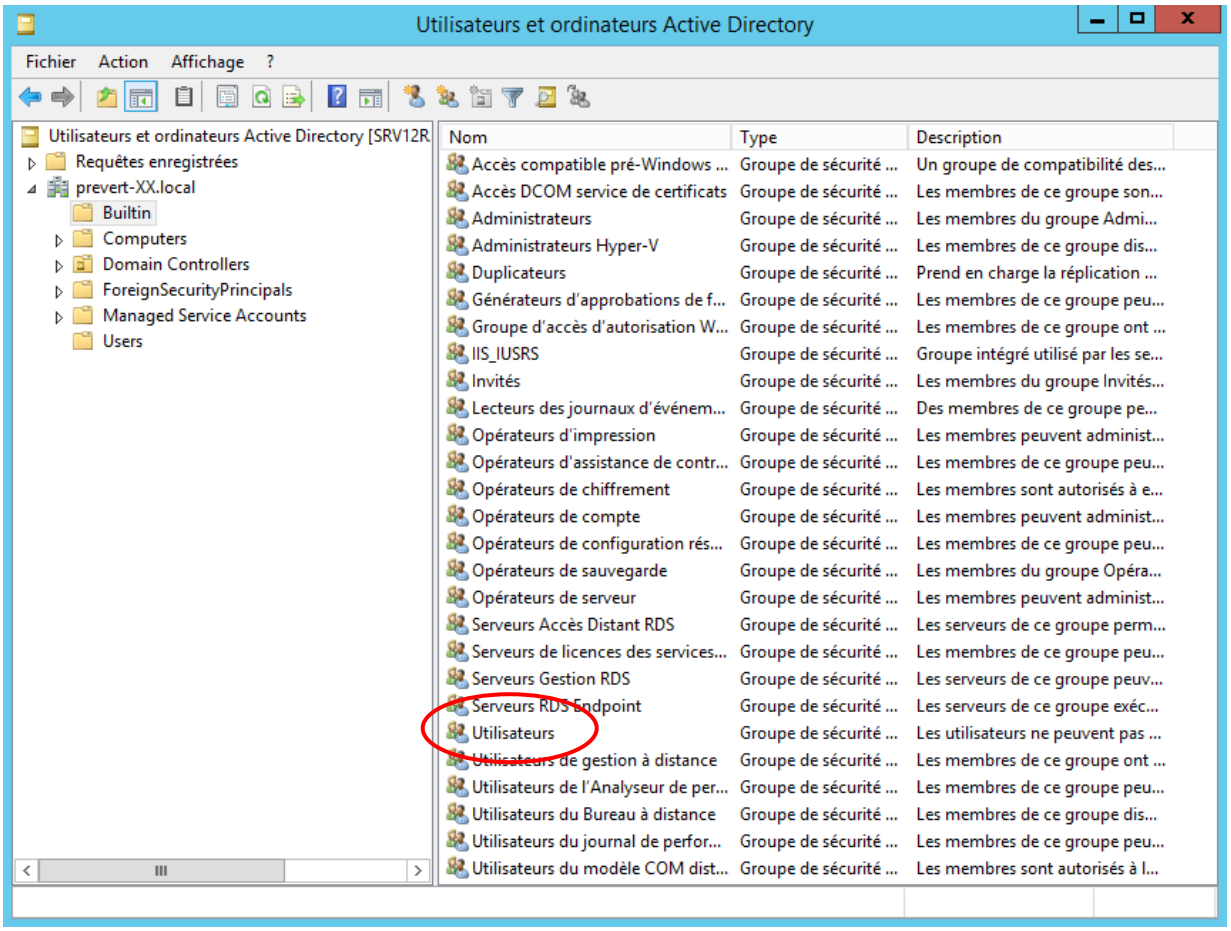


Les unités d'organisation peuvent contenir des utilisateurs, des groupes, des ordinateurs, des imprimantes, des dossiers partagés et une quantité illimitée d'autres unités d'organisation, mais elles ne peuvent pas contenir d'objets d'autres domaines.

Le compte administrateur se trouve dans l'OU **Users**



Le groupe Utilisateur se trouve dans l'OU **Builtin** ce sont des groupes intégrés



Sécurisation des comptes d'utilisateurs

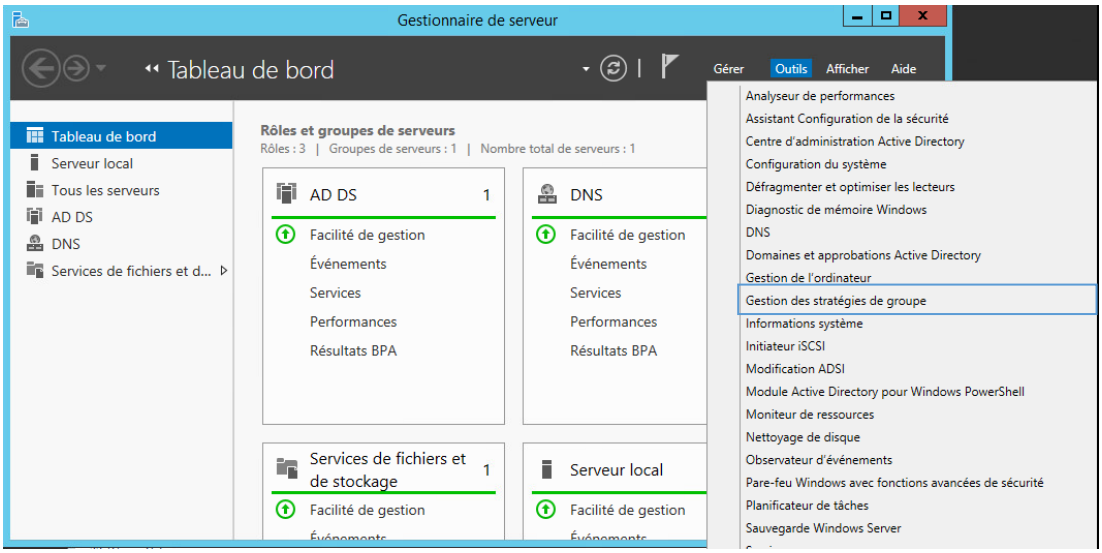
Si un administrateur réseau ne modifie pas les droits et autorisations des comptes intégrés, un utilisateur (ou service) malveillant peut les utiliser pour ouvrir illégalement une session sur un domaine à l'aide des comptes Administrateur ou Invité. Pour assurer la protection de ces comptes, il est recommandé de les renommer ou de les désactiver. Dans la mesure où un compte renommé conserve son identificateur de sécurité (SID, Security Identifier), il conserve également toutes ses autres propriétés, comme la description, le mot de passe, l'appartenance à des groupes, le profil utilisateur, les informations sur le compte ainsi que les autorisations et les droits qui lui ont été accordés.
Pour bénéficier de la sécurité de l'autorisation et de l'authentification de l'utilisateur, utilisez le Centre d'administration Active Directory pour créer un compte pour chaque utilisateur qui participe à votre réseau. Vous pouvez ensuite ajouter chaque compte d'utilisateur (y compris le compte Administrateur et le compte Invité) à un groupe pour contrôler les droits et les autorisations qui sont affectés au compte. Lorsque vous disposez des comptes et des groupes appropriés pour votre réseau, vous pouvez identifier les utilisateurs qui se connectent à votre réseau et leur donner accès uniquement aux ressources autorisées.

Vous pouvez contribuer à protéger votre domaine contre les pirates en exigeant des mots de passe forts et en mettant en œuvre une stratégie de verrouillage de compte. Les mots de passe forts réduisent le risque de leur décodage intelligent et des attaques par dictionnaire sur les mots de passe. Une stratégie de verrouillage de compte contribue à diminuer les risques d'attaques sous la forme de tentatives répétées d'ouverture de session, pouvant porter atteinte à votre domaine. Une telle stratégie détermine le nombre possible d'échecs de tentatives d'ouverture de session pour un compte d'utilisateur avant sa désactivation.

Malgré toutes ces recommandations nous allons désactiver les exigences de complexités de mot de passe afin de rendre la création des comptes utilisateurs plus simple.

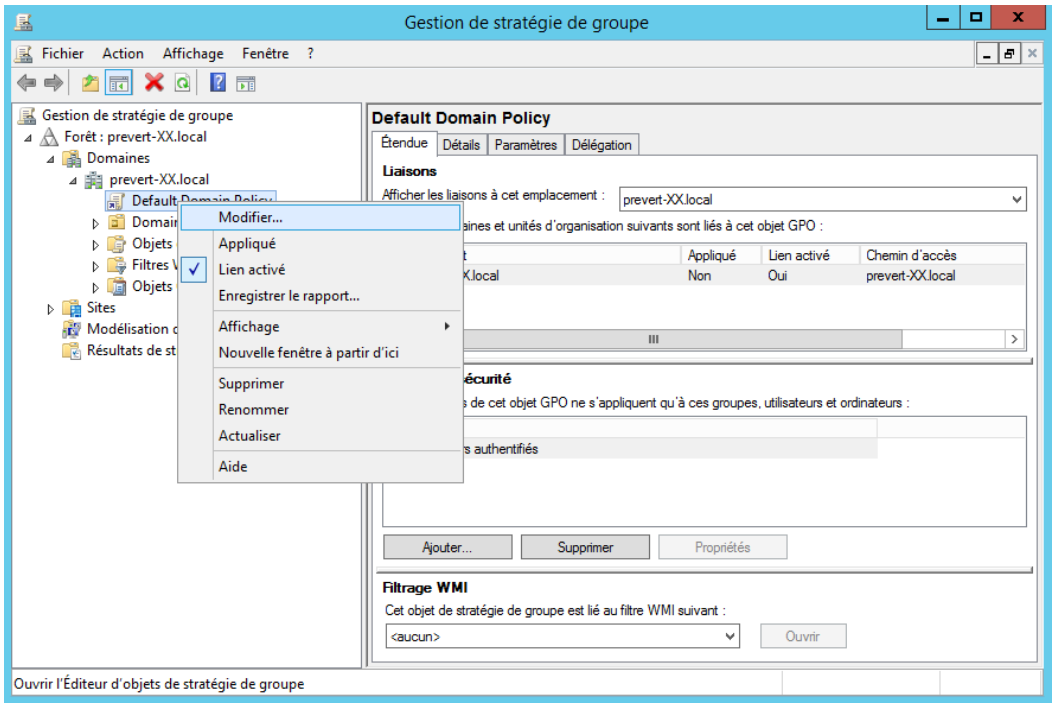
Désactiver les exigences de complexité du mot de passe

À l'installation du service AD DS, les paramètres de sécurité sont réinitialisés (Exigences de complexité du mot de passe, durée de vie minimale, ...). Si vous souhaitez modifier ces paramètres, procédez de la manière suivante :

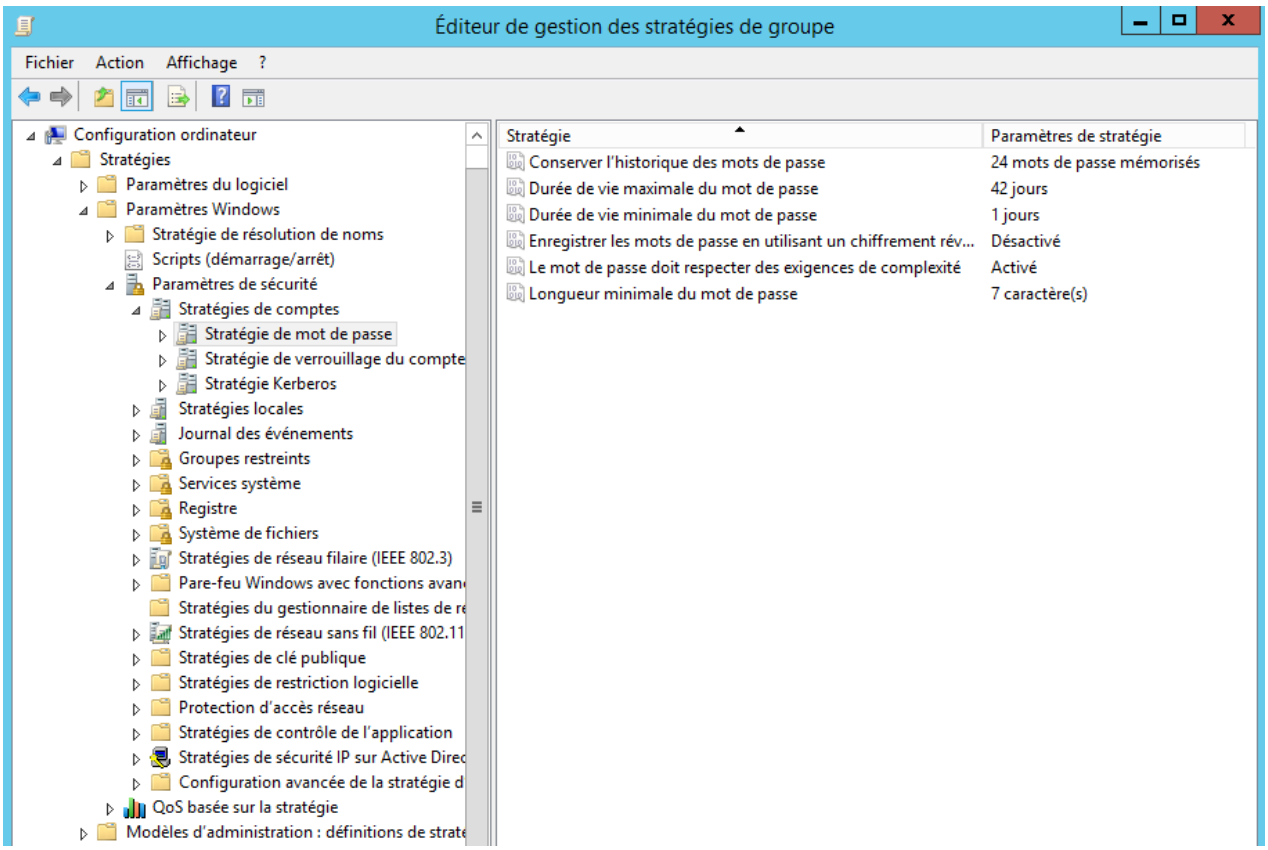


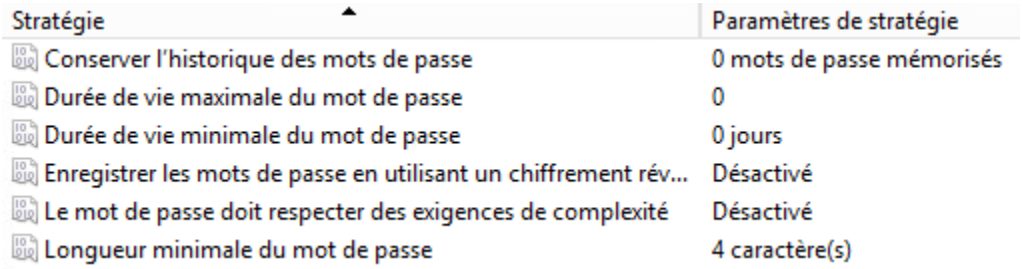
=> Lancer le gestionnaire de serveur / Outils /Gestion des stratégies de groupe

=> Développez la "Forêt".
=> Sélectionnez votre domaine.
=>Clique droit, sur "Default Domain Policy".
=> Sélectionnez l'option "Modifer".

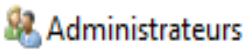


=> Développez la stratégie "Configuration ordinateur" => "Stratégies" =>"Paramètres Windows" => "Paramètres de sécurité" => "Stratégies de comptes".
=> Sélectionnez "Stratégie de mot de passe".

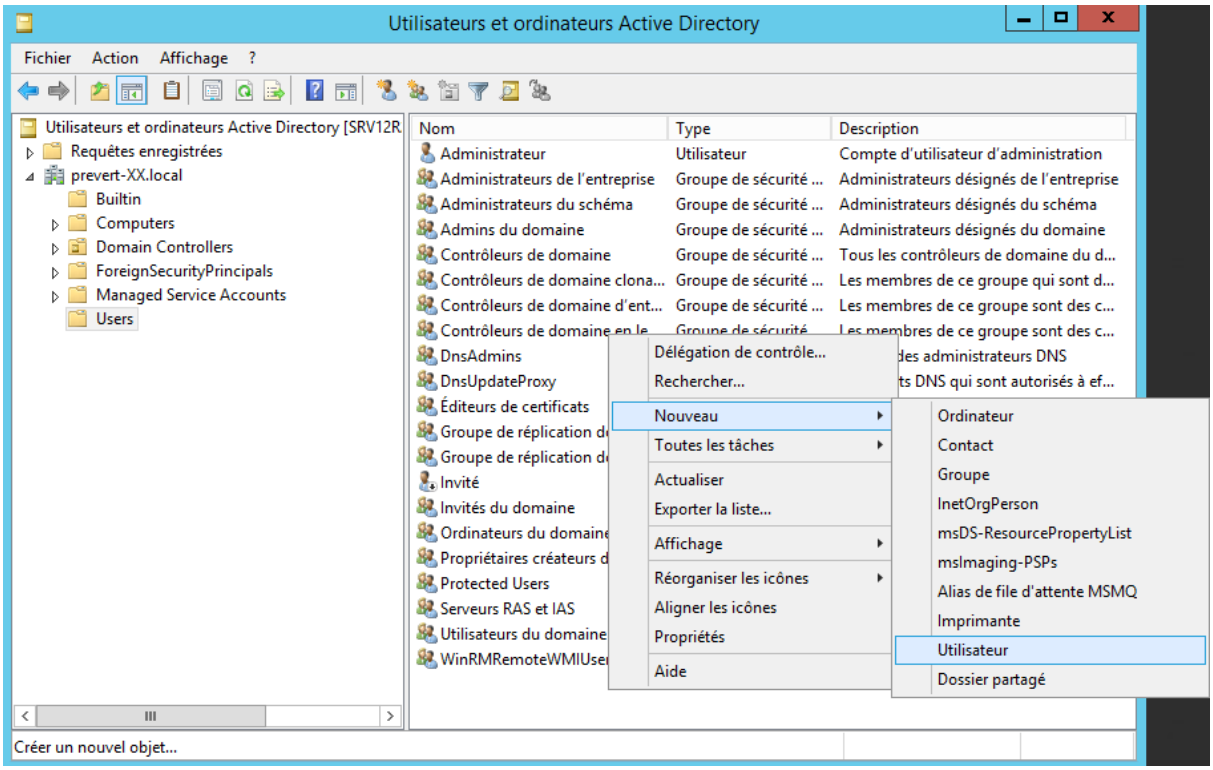


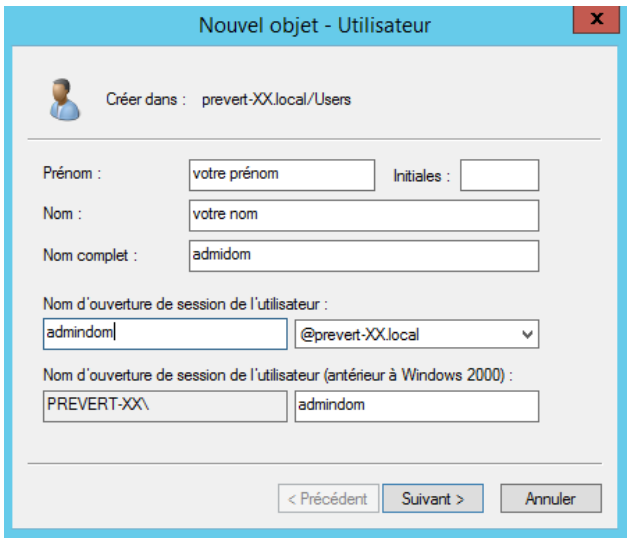


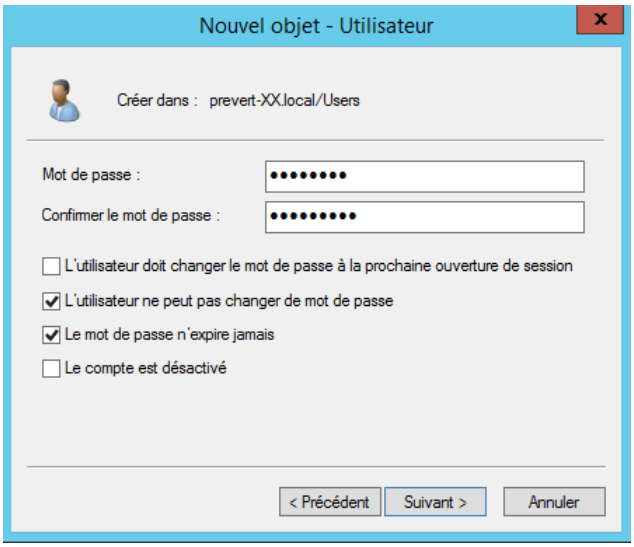
=> Modifiez les paramètres en tenant compte de l'image écran (Ci-dessus).
=> Validez vos choix.
=> Ouvrez l'invite de commandes puis tapez : gpupdate /force.
=> Lancez l'observateur d'événements pour corriger d'éventuelles erreurs.

Pour gérer votre Domaine vous devez créer un compte appartenant au groupe 

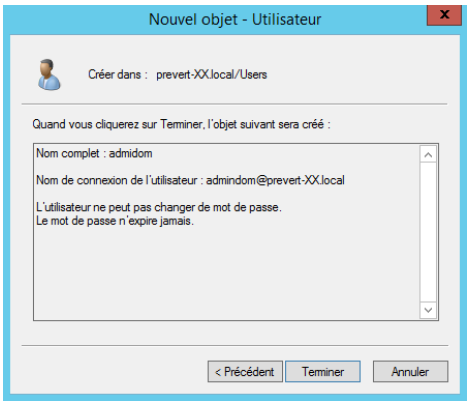
Dans l'unité d'organisation Users créer un nouvel utilisateur



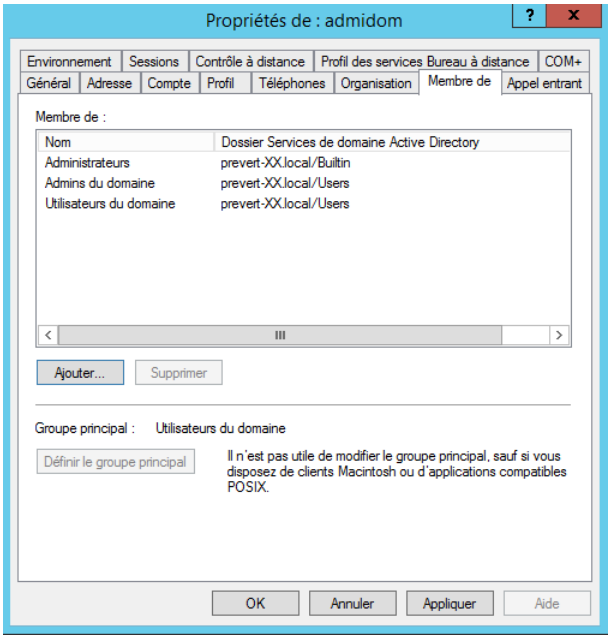




Nom d'ouverture de session: **admindom**
Mot de passe: **Prevert77**



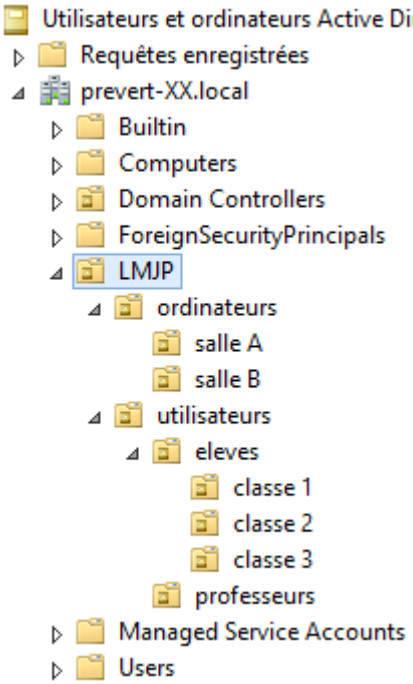
Ajouter **admindom** au groupe **Administrateurs** et **Admin du domaine**

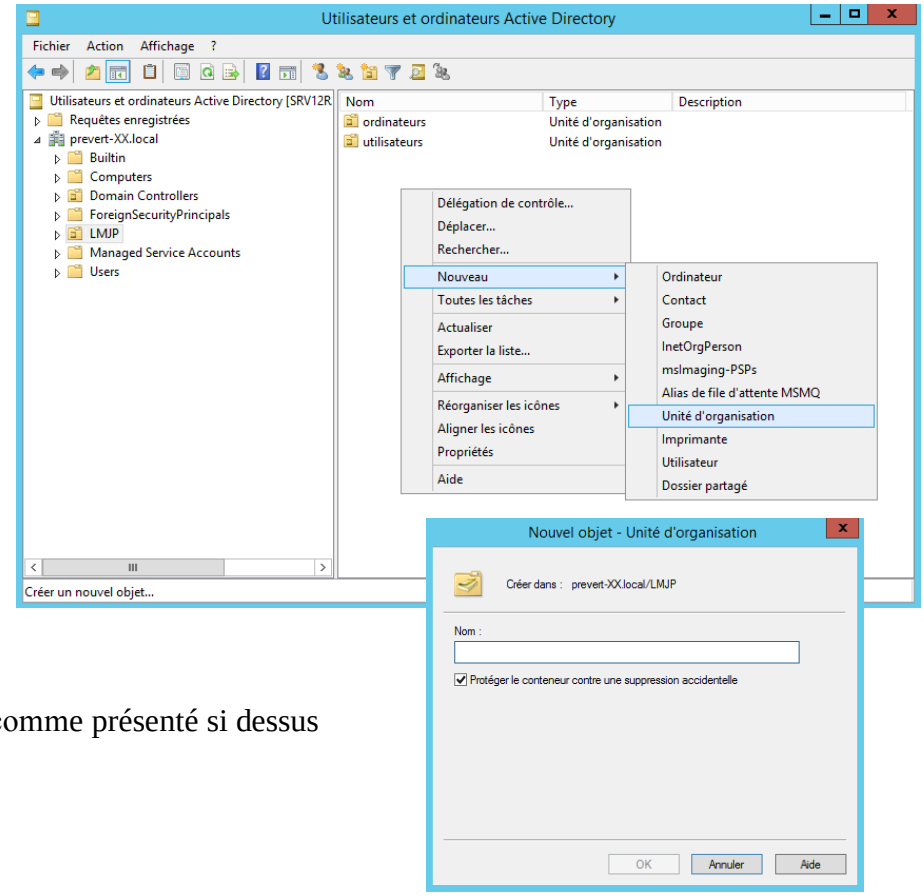


Connectez vous sur votre serveur avec ce nouveau compte

Construction des unités d'organisation

Nous allons maintenant intégrer tous les utilisateurs et tous les ordinateurs de notre domaine. Pour cela nous allons construire une achitecture d'Unités d'Organisations qui refléte la structure de notre entreprise.

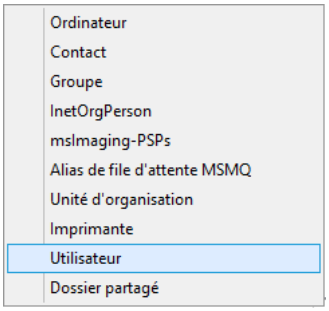




Construire les unités d'organisation comme présenté si dessus

Supprimer l'OU classe 3

Création des comptes utilisateurs



Créer dans l'unité d'organisation nommée **classe 1**
les comptes utilisateurs suivants :

Nom	prénom	Nom complet	Nom d'ouverture de session	Mot de passe
Eleve1	Eleve1	Eleve1 de classe 1	eleve1	111111
Eleve2	Eleve2	Eleve2 de classe 1	eleve2	222222

- ☑ L'utilisateur ne peut pas changer de mot de passe
- ☑ Le mot de passe n'expire jamais

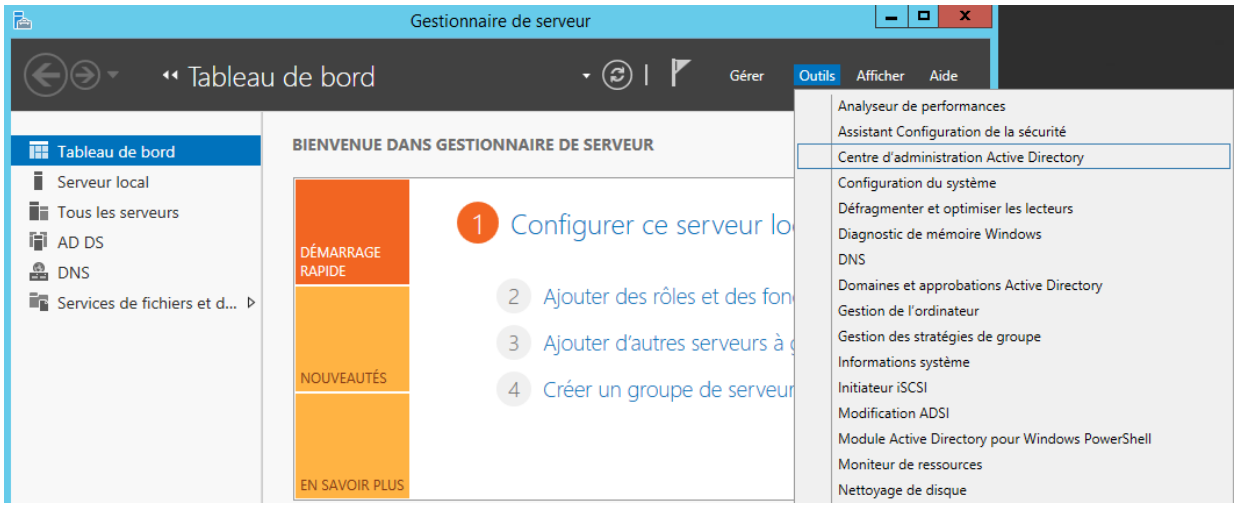
Créer dans l'unité d'organisation nommée **classe 2** les comptes utilisateurs suivants :

Nom	prénom	Nom complet	Nom d'ouverture de session	Mot de passe
Eleve3	Eleve3	Eleve3 de classe 2	eleve3	333333
Eleve4	Eleve4	Eleve4 de classe 2	eleve4	444444

- ☑ L'utilisateur ne peut pas changer de mot de passe
- ☑ Le mot de passe n'expire jamais

Centre d'administration Active Directory

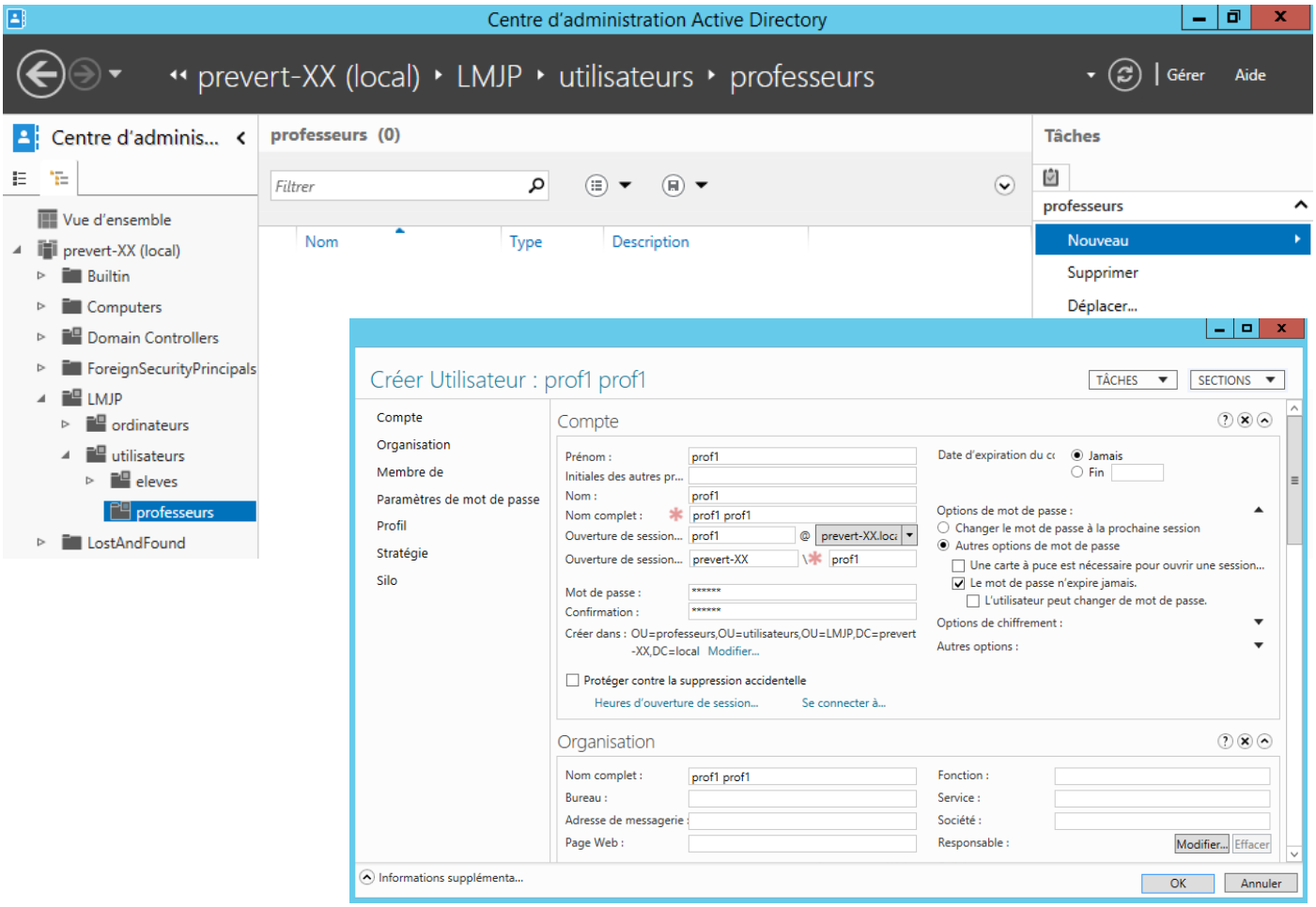
Windows server 2012R2 introduit un nouvel outil pour gérer active directory.



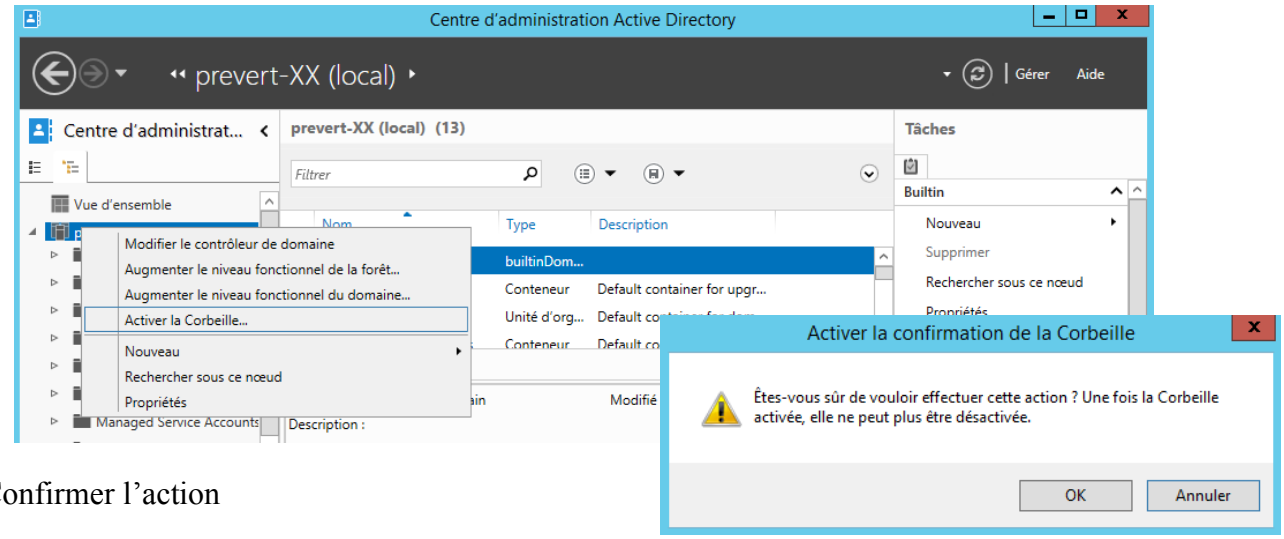
A l'aide du centre d'administration Active Directory, créer dans l'unité d'organisation nommée **professeurs** les comptes utilisateurs suivants :

Nom	prénom	Description	Nom d'ouverture de session	Mot de passe
Prof1	Prof1	Professeur1	prof1	ppp111
Prof2	Prof2	Professeur2	prof2	ppp222

☑ L'utilisateur ne peut pas changer de mot de passe
☑ Le mot de passe n'expire jamais

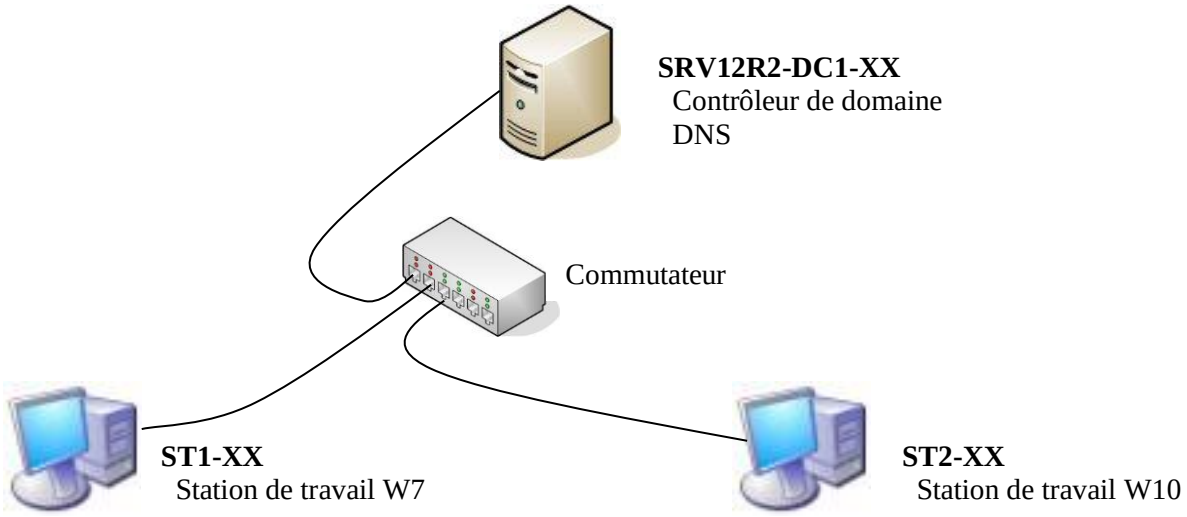


Bonne Pratiques : activer la corbeille afin de pouvoir récupérer facilement les utilisateurs supprimés ainsi que toutes les informations associées (adresse, groupe,…)



Confirmer l'action

Joindre les machines au domaine



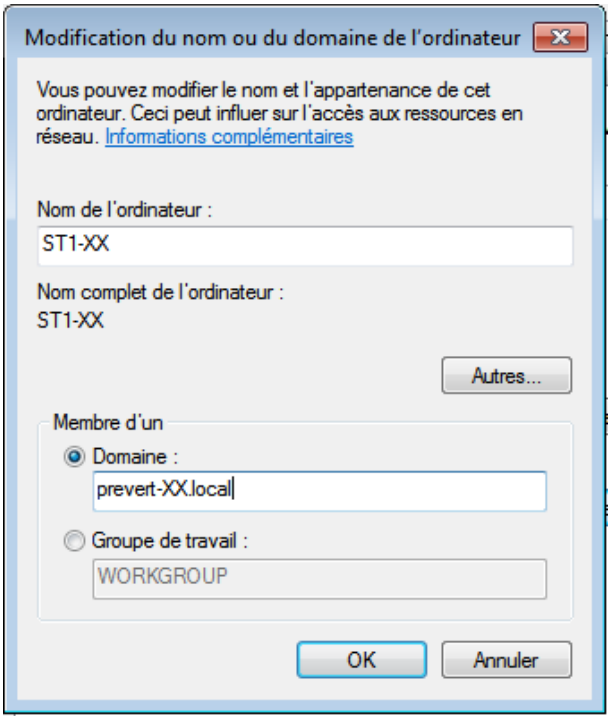
Faites en sorte que les stations ST1-XX et ST2-XX soient membre du domaine ***prevert-xx.local***

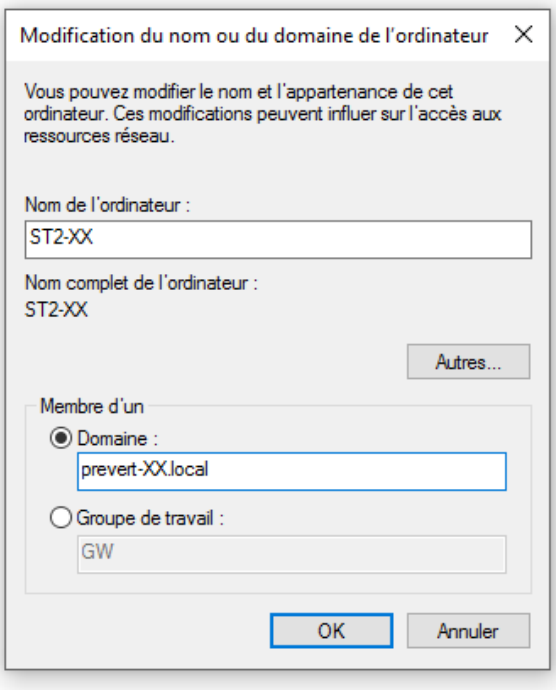
Sur les **STATIONS**

Paramétrer le serveur DNS des stations pour qu'elles interrogent notre serveur 2012

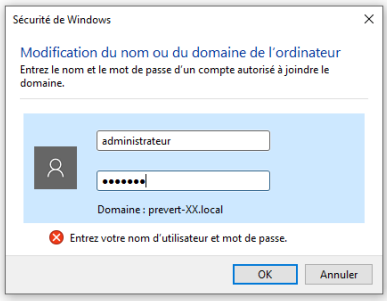
Mettre à jour le nom de l'ordinateur, ST1-XX et ST2-XX,

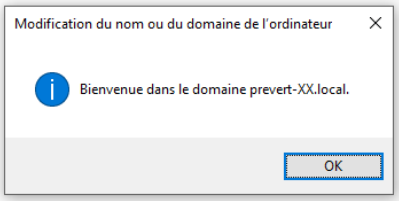
Intégrer les stations au Domaine prevert-xx.local.

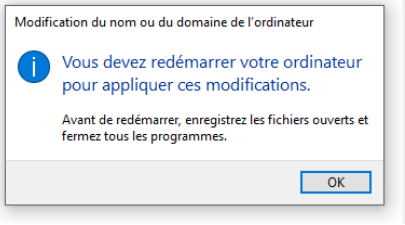




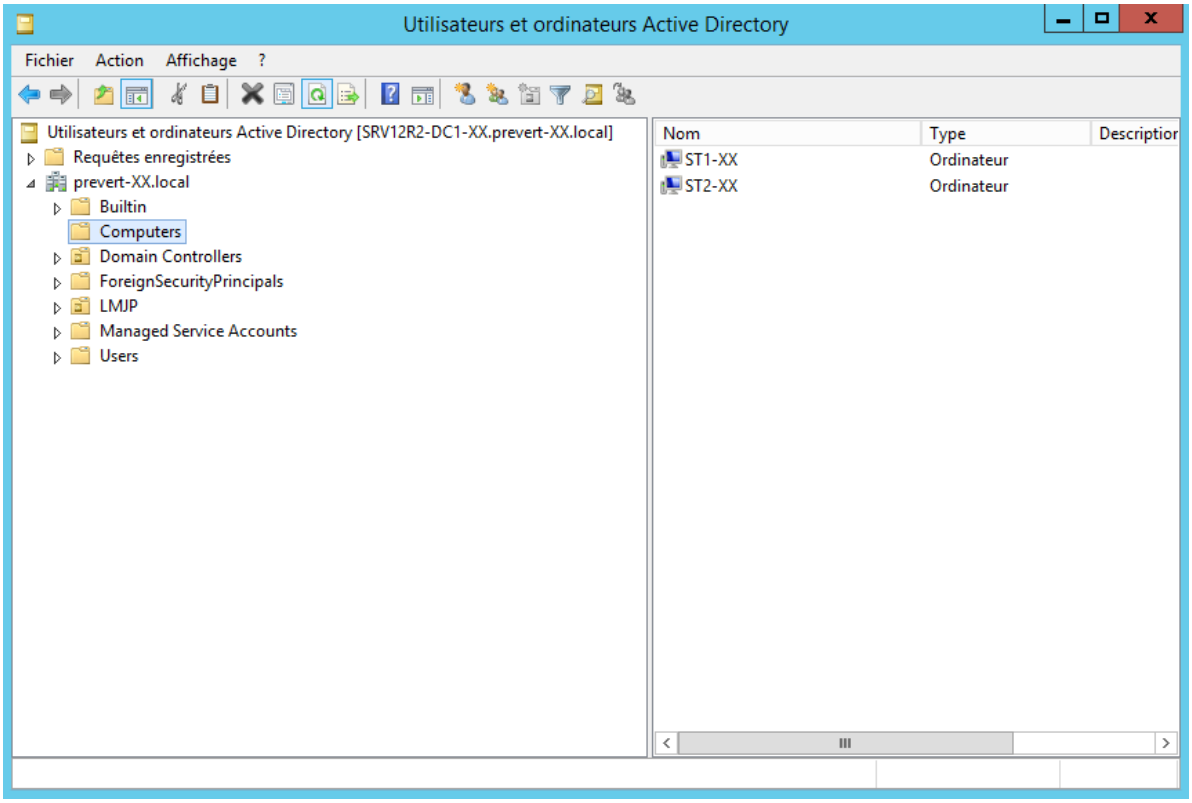
Identifiez vous avec un compte du domaine **administrateur / Prevert77**







Dans active directory vérifier la présence des stations ST1-XX et ST2-XX dans le conteneur **computers**



Déplacer les machines **ST1-XX** dans l'Unité d'Organisation **salle A** et **ST2-XX** dans l'OU **salle B**

Vérifier tous les comptes utilisateurs sur les deux machines**.**