

Installation du rôle ActiveDirectory

Introduction

Votre client, la société CONTORSE crée et fabrique depuis une dizaine d'années, des piscines à coque plastique sur mesure.

Devant la forte croissance du marché, il est prévu d'embaucher une dizaine de salariés supplémentaires. Le Système d'Information que vous avez mis en place dans les cours précédents ne répond plus aux critères d'exigences demandés.

En effet, le responsable de la société veut un système qui lui permette de gérer simplement et efficacement les nouveaux employés entrants tout en assurant une sécurité des données. Il ne faut pas que certains employés puissent accéder à des informations confidentielles.

Vous lui proposez de mettre en place un serveur Active Directory qui est en mesure de répondre à ses besoins naissants et ceux à venir.

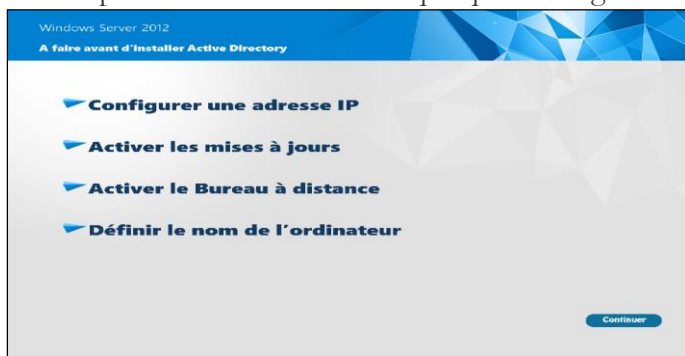
Pour le moment, dans ce cours, nous verrons comment installer un serveur Active Directory.

Les objectifs sont les suivants :

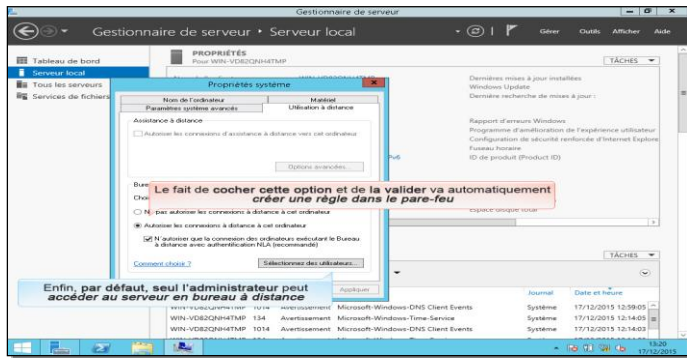
- Configurer le bureau à distance
- Identifier le rôle de la Forêt
- Installer et configurer le rôle AD DS

Nous allons générer un nouveau clone de la VM Serveur Windows afin d'y installer le rôle ActiveDirectory.

Mais auparavant il faut effectuer quelques configurations préalables :



Nous lui donnerons le nom SRVAD01.



Sélectionnez cette option afin d'autoriser les connexions Bureau à distance.

Le fait de cocher cette option et de la valider va automatiquement créer une règle dans le pare-feu qui va autoriser les connexions entrantes dont le port est 5900.

Cette option indique que les clients RDP (Remote Desktop Protocol) doivent gérer l'authentification NLA pour pouvoir se connecter.

Depuis Windows Vista, le client Bureau à distance gère le protocole NLA alors que certains clients RDP sous Linux ne le gèrent pas.

Nous n'utiliserons pas de clients Linux tout au long de ces différents cours.

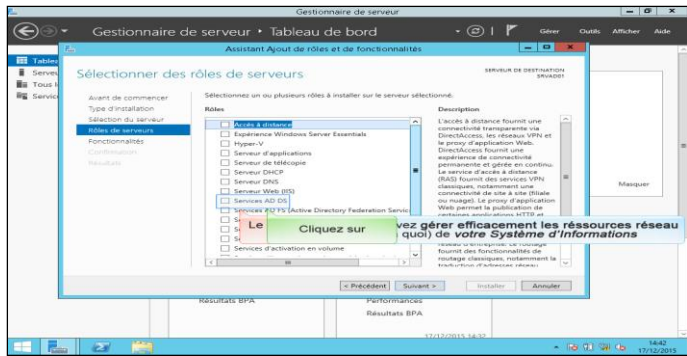
Enfin, par défaut, seul l'administrateur peut accéder au serveur en bureau à distance.

Il n'est pas nécessaire d'ajouter d'autres utilisateurs.

Bien que pour le moment cela ne soit pas utile, puisque notre machine virtuelle n'a pas encore accès à Internet, nous allons quand même configurer Windows Update.

Malgré les idées reçues, il ne faut surtout pas désactiver Windows Update au risque de rendre son serveur vulnérable.

Installation du rôle AD DS et DNS

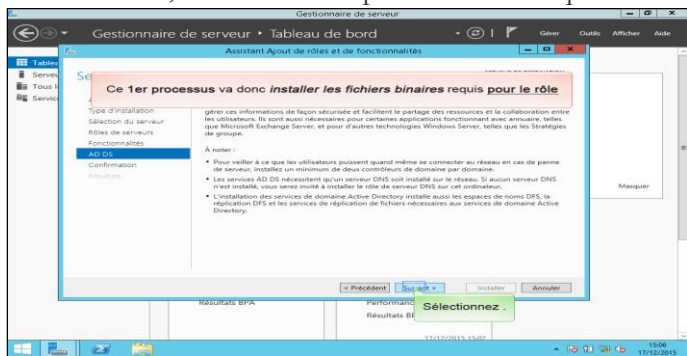


Le rôle Service AD DS (Active Directory Domain Services) est un service d'annuaire évolutif et extensible.

Grâce à lui vous pouvez gérer efficacement les ressources réseau (qui a accès à quoi) de votre Système d'Informations.

Depuis Windows 2008, le rôle Active Directory s'installe en 2 étapes.

Tout d'abord, on démarre le processus en cliquant sur Ajouter le rôle AD DS.



Avant de valider l'installation du rôle, il est important de voir que Windows nous fournit les commandes Powershell correspondant à l'installation de ce rôle.

Nous vous conseillons fortement de copier ces commandes car elles vous serviront dans les derniers chapitres du cours Windows 2012.

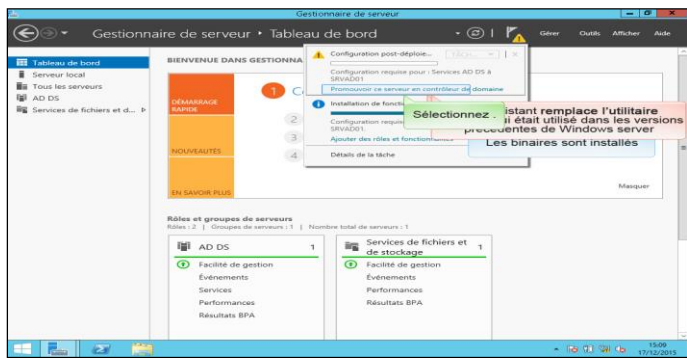
Nous le verrons plus tard, mais il est possible d'installer Windows sans interface graphique.

Les avantages sont intéressants puisque l'empreinte mémoire de Windows est optimisée et les risques de failles de sécurité sont moindres puisque seuls les composants de base sont installés.

Pour ce cours, nous utiliserons l'interface graphique de Windows.



En cliquant sur le drapeau, il est possible de consulter la progression de l'installation.



Les binaires sont installés.

Le 2nd Processus consiste à configurer le rôle AD DS.

Cet assistant remplace l'utilitaire dcpromo qui était utilisé dans les versions précédentes de Windows server.

Création du domaine

Avant de créer notre 1er serveur Active Directory, il faut d'abord comprendre quelques concepts. Par exemple, pour créer un serveur Active Directory, il faut lui donner un nom de domaine. En effet, chaque domaine Active Directory a un nom de domaine DNS qui lui est associé.

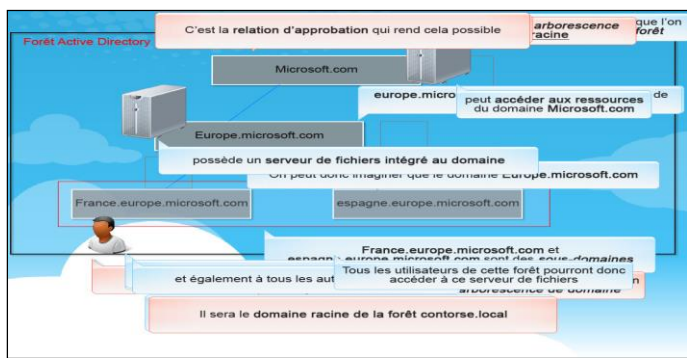
Par exemple, pour ce cours, notre serveur Active Directory aura comme nom contorse.local. Cela signifie que dans le serveur DNS il y a un enregistrement de type contorse.local = 192.168.0.1.

Ce nom de domaine étant géré par le serveur DNS.

Mais ce n'est pas tout car il existe une petite subtilité qui est fondamentale : il s'agit de la notion de forêt.

On appelle forêt un ou plusieurs domaines partageant les mêmes données d'annuaire.

Regardons cet exemple pour mieux comprendre.



Ce rectangle représente une Forêt Active Directory.

Une forêt contient un ou plusieurs domaines.

Le 1er serveur Active Directory que l'on crée correspond au domaine racine de la forêt.

Il est possible d'ajouter des domaines enfants.

europe.microsoft.com est un domaine enfant de microsoft.com.

France.europe.microsoft.com et Espagne.europe.microsoft.com sont des sous-domaines.

Tous ces domaines font partie de la même arborescence parce qu'ils ont le même domaine racine c'est-à-dire Microsoft.com.

Lorsque les domaines ont une structure de noms contigüe, on dit qu'ils sont dans la même arborescence de domaine.

Comme tous les domaines partagent la même arborescence, cela signifie qu'un utilisateur du domaine france.europe.microsoft.com peut accéder aux ressources du domaine Microsoft.comet également à tous les autres domaines.

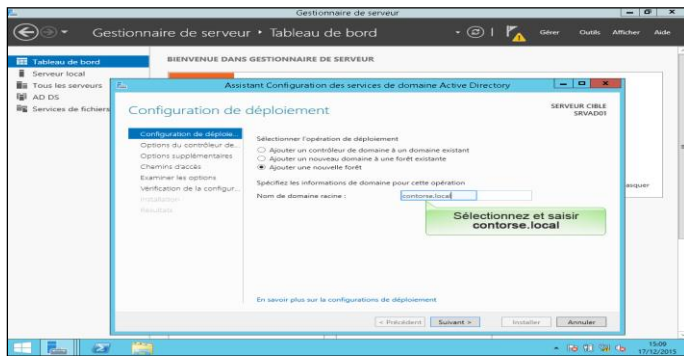
On peut donc imaginer que le domaine Europe.microsoft.com possède un serveur de fichiers intégré au domaine.

Tous les utilisateurs de cette forêt pourront donc accéder à ce serveur de fichiers.

C'est la relation d'approbation qui rend cela possible.

Pour ce cours nous installerons notre 1er serveur Active Directory.

Il sera le domaine racine de la forêt contorse.local.



Comme il s'agit du 1er serveur Active Directory, nous allons donc créer une nouvelle forêt.

Il existe 3 niveaux fonctionnels pour la forêt :

- Windows Server 2008 prend en charge les contrôleurs de domaine Windows 2008 et ultérieur
- Windows Server 2008R2 prend en charge les contrôleurs de domaine Windows 2008R2, 2012 et 2012R2
- Windows Server 2012 prend en charge les contrôleurs de domaine Windows 2012 et 2012R2

Cela signifie que s'il y a des serveurs AD 2008 dans votre Infrastructure, alors il faudra choisir le mode fonctionnel Windows 2008 pour la forêt.

Durant l'installation, le rôle Serveur DNS va être installé.

Nous aborderons la configuration du serveur DNS dans le prochain cours.

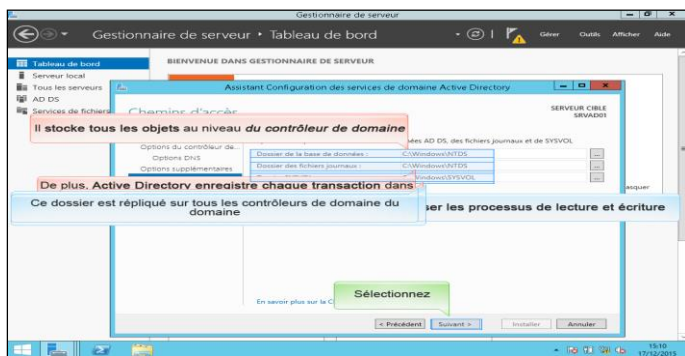
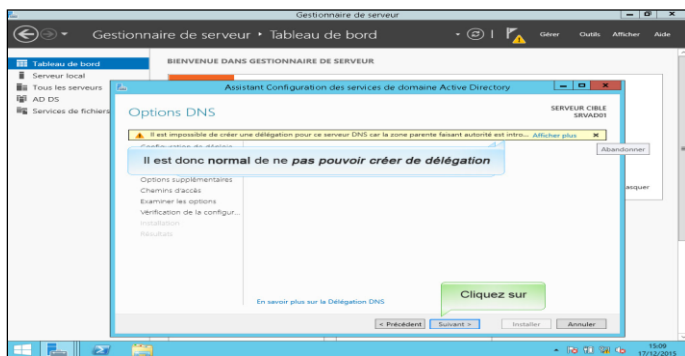
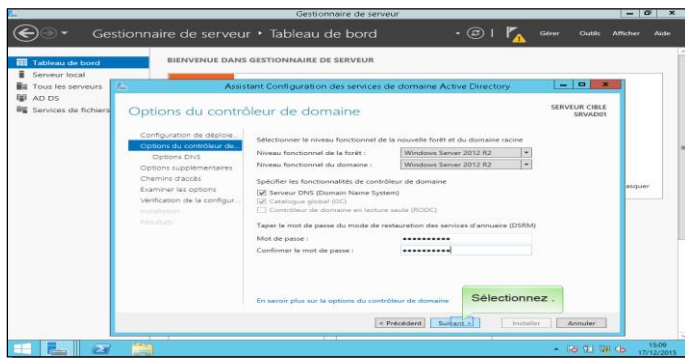
Mais pour le moment, retenez que DNS fait partie intégrante de la technologie Active Directory.

Par défaut, le 1er serveur Active Directory installé sur un domaine est désigné comme catalogue global.

Le catalogue global joue un rôle important dans un domaine puisque qu'il est utilisé pour l'ouverture de session et pour la recherche d'informations.

Si le catalogue global est indisponible, les utilisateurs du domaine ne pourront pas ouvrir de session sur le domaine.

Et enfin, il est demandé de renseigner un mot de passe pour le mode de restauration Active Directory.



Il est conseillé dans un environnement de production de stocker ces fichiers sur un disque dur secondaire afin d'optimiser les processus de lecture et écriture.

Le fichier NTDS est la base de données Active Directory.

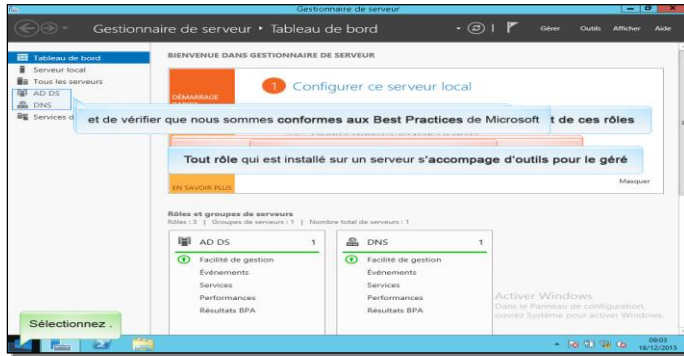
Il stocke tous les objets au niveau du contrôleur de domaine.

De plus, Active Directory enregistre chaque transaction dans un ou plusieurs fichiers journaux associés au fichier NTDS.

Le dossier partagé SYSVOL est présent uniquement sur les contrôleurs de domaine.

Il contient les modèles Stratégie de groupe, les stratégies de groupe par défaut (Default Domain Policy et Default domain Controllers Policy) ainsi que les scripts d'ouverture de session.

Ce dossier est répliqué sur tous les contrôleurs de domaine du domaine.



Après le redémarrage, les rôles AD DS et DNS ont été installés. Nous verrons plus tard, qu'il est possible de consulter le bon fonctionnement de ces rôles et de vérifier que nous sommes conformes aux Best Practices de Microsoft. Par ailleurs, retenez qu'un serveur Active Directory doit uniquement jouer le rôle AD DS et DNS. Pour des raisons de performance, de sécurité et d'évolution, tout rôle qui est installé sur un serveur s'accompagne d'outils pour le gérer.



Les outils qui ont été installés par le rôle DNS et AD DS sont listés ici. Nous utiliserons la plupart de ces outils tout au long de notre progression.

Conclusion

Ce cours sur l'installation d'un serveur Active Directory est à présent terminé.

Nous avons pu voir qu'il est préférable de modifier le Nom du serveur afin qu'il représente le rôle qu'il joue dans le Système d'Informations.

L'installation d'un serveur Active Directory est un processus simple, mais qui peut s'avérer complexe par les termes employés (DNS, Forêt, Domaine...).

C'est la raison pour laquelle nous aborderons le rôle du serveur DNS dans une Infrastructure Active Directory ultérieurement.