

Installation de Windows 2008 Serveur

Introduction

Ce document n'explique pas les concepts, il se contente de décrire, avec copies d'écran, la méthode que j'utilise habituellement pour installer un Windows 2008 Serveur dans le cas simple d'un réseau avec un seul serveur.

Ce document ne convient pas si vous avez déjà un ou plusieurs serveurs et que vous voulez ajouter un serveur Windows 2008 à votre domaine.

Ce document convient cependant si vous avez déjà un ou plusieurs domaines dans votre réseau et que vous souhaitez créer un nouveau domaine.

L'installation peut être décomposée en deux grandes phases. L'installation de Windows 2008 puis l'installation d'Active Directory.

Ce document décrit également comment désinstaller Active Directory et le service DNS. Vous ne devriez normalement pas en avoir besoin.

Installation de Windows 2008

Préparation

Modifier le bios pour que l'ordre de démarrage permette de démarrer sur le DVD.

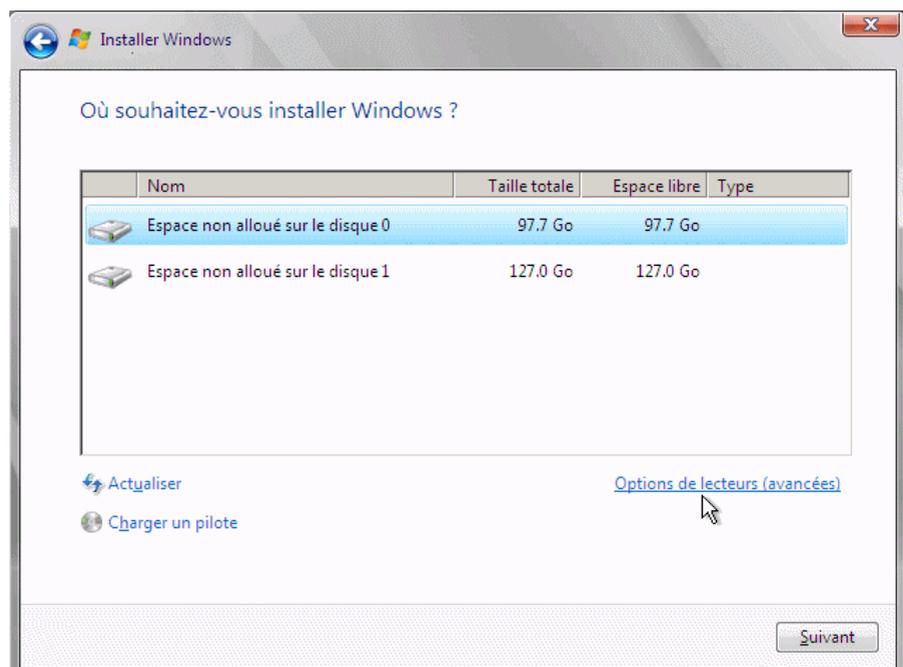
Le disque dur peut ne rien contenir (on peut supprimer toute trace d'anciennes partitions en remplissant le premier secteur du disque dur avec le caractère de code ascii 0).

Installation

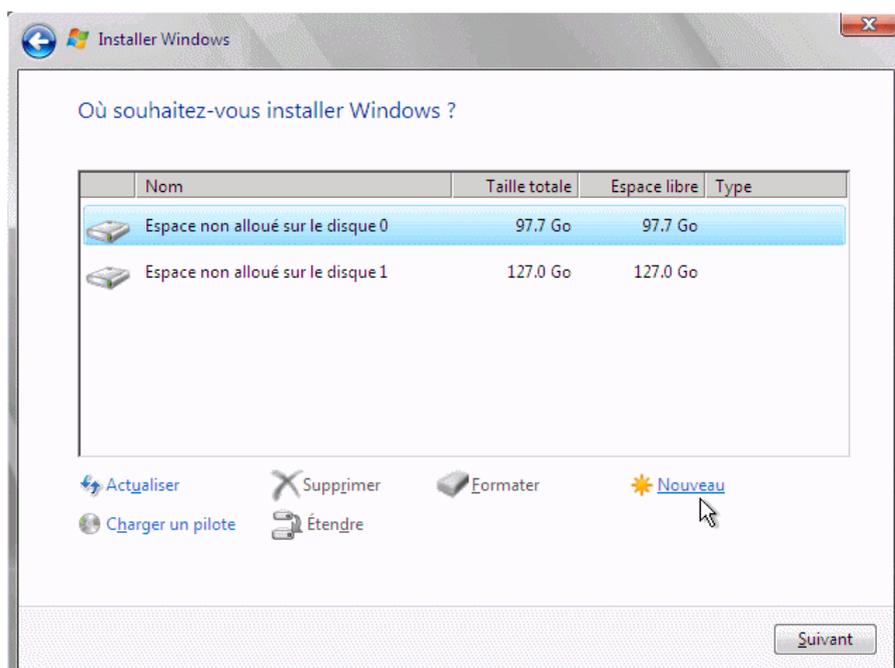
Démarrer l'ordinateur avec le DVD de Windows 2008 Serveur dans le lecteur.

Il est conseillé de ne pas utiliser la totalité de votre disque pour la partition système. Une partition de 30 ou 40 Go est en général une valeur correcte.

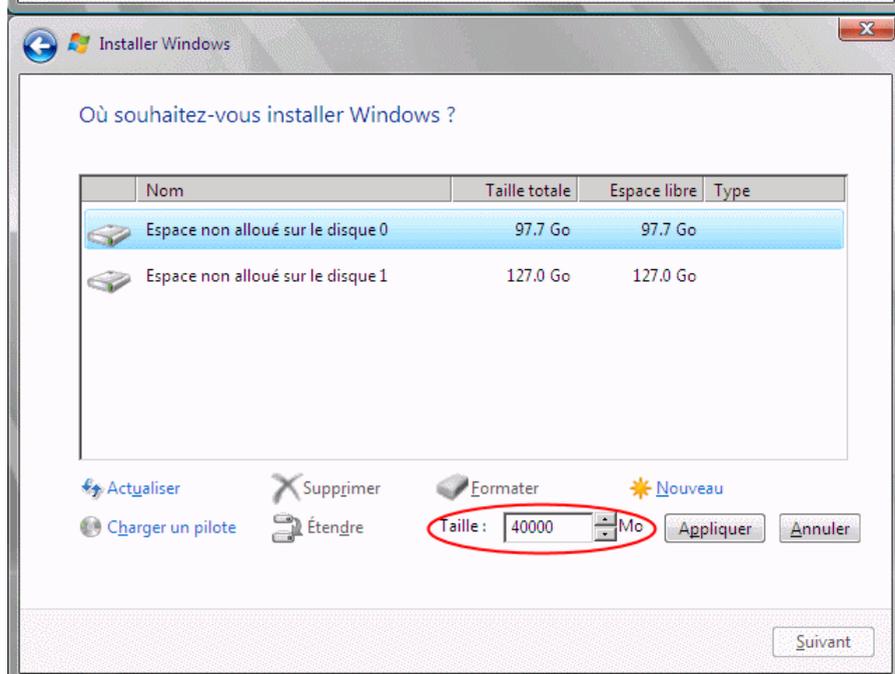
Utilisez "Options de lecteurs (avancées)" afin de pouvoir partitionner.



Puis choisissez "Nouveau".

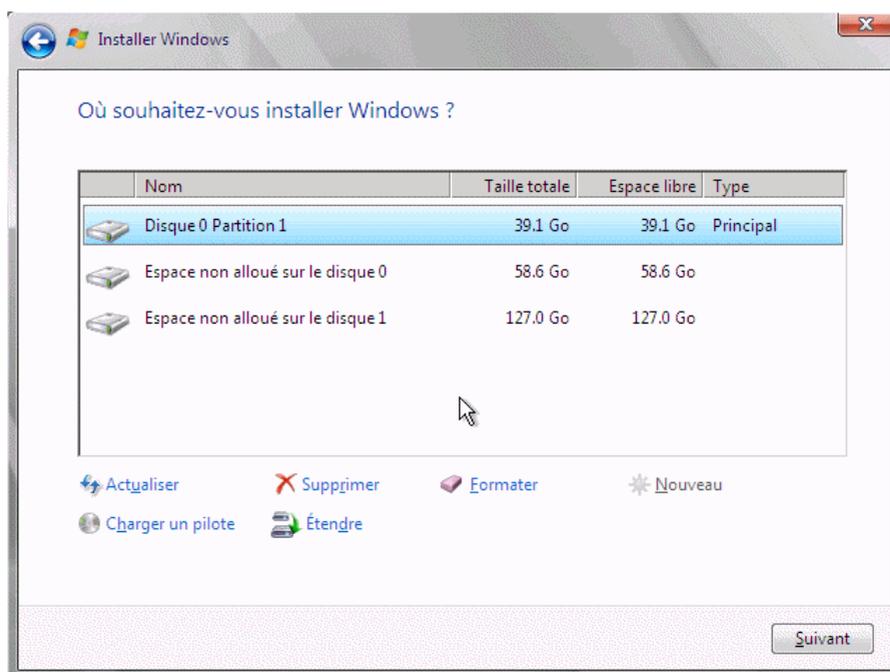


Indiquez la valeur souhaitée pour la partition système, faites "Appliquer".



Un peu après le bouton Suivant devient accessible. Faites maintenant "Suivant".

Les autres partitions seront définies plus tard lorsque Windows sera installé.



A la fin de l'installation l'ordinateur redémarre. Une fenêtre "Tâches de configuration initiales" permet d'accéder facilement au paramétrage de votre serveur. Si cette fenêtre a été fermée, vous pouvez la faire réapparaître en exécutant **oobe** (ce mot ne contient que des lettres et signifie "Out-of-box Experience").

Nom du serveur

Dans cette fenêtre, utilisez "Indiquez un nom d'ordinateur et un domaine" afin de remplacer le nom de votre serveur donné de façon aléatoire lors de l'installation par un nom qui convient mieux. Il aurait également été possible de faire "Démarrer", clic droit sur "Ordinateur" et "Propriétés". De même il était possible de choisir "Système" dans le panneau de configuration.

Un redémarrage est nécessaire après ce changement.

Paramétrage IP

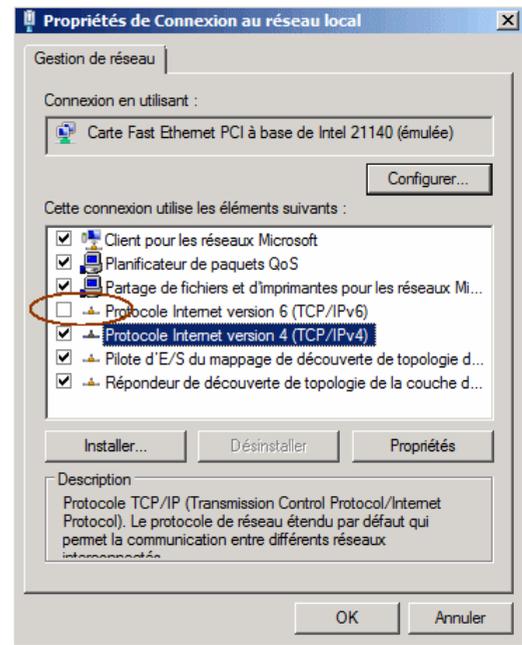
Le paramétrage IP ne doit pas rester en "Obtenir une adresse IP automatiquement". Dans la fenêtre "Tâches de configuration initiales", utilisez "Configurer le réseau". Il aurait également été possible de faire "Démarrer", clic droit sur "Réseau", "Propriétés" et "Gérer les connexions réseau".

Indiquez l'adresse IP version 4, et le masque.

Indiquez l'adresse IP de la passerelle.

Comme notre intension est d'installer DNS et Active Directory, vous pouvez dès maintenant mettre comme DNS l'adresse 127.0.0.1. Ne mettez pas d'autre adresse de DNS ici.

Décochez IPv6.



Partitions

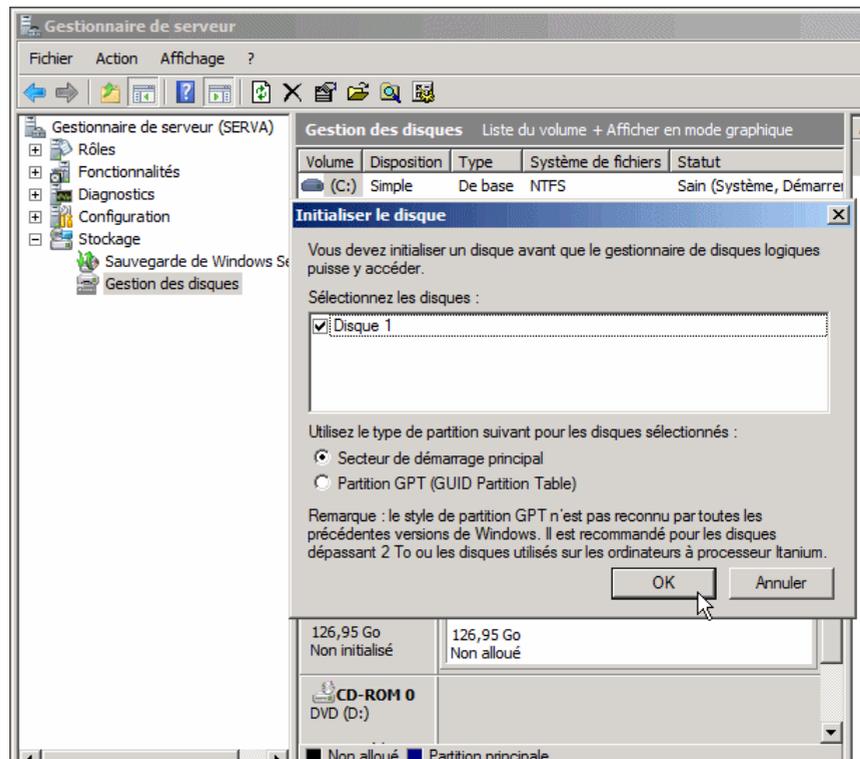
Actuellement, une partie du premier disque (disque 0) n'est pas encore utilisée. Le deuxième disque (disque 1) n'est pas du tout utilisé.

Faites "Démarrer", un clic droit sur "Ordinateur" et "Gérer".

La suite dépend de votre configuration matérielle.

Dans notre cas, le deuxième disque n'a pas encore été utilisé, il doit être initialisé.

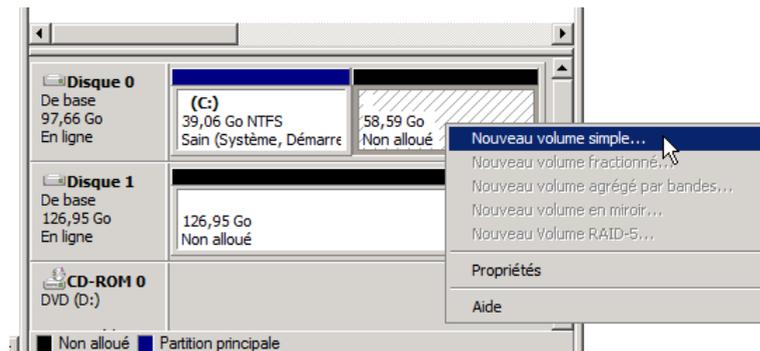
Faites simplement OK.



Faites un clic droit sur la deuxième partie du disque 0 et créez un "Nouveau volume simple".

Un assistant démarre. Faites simplement suivant afin de garder les choix par défaut.

Faites de même pour le disque 1.

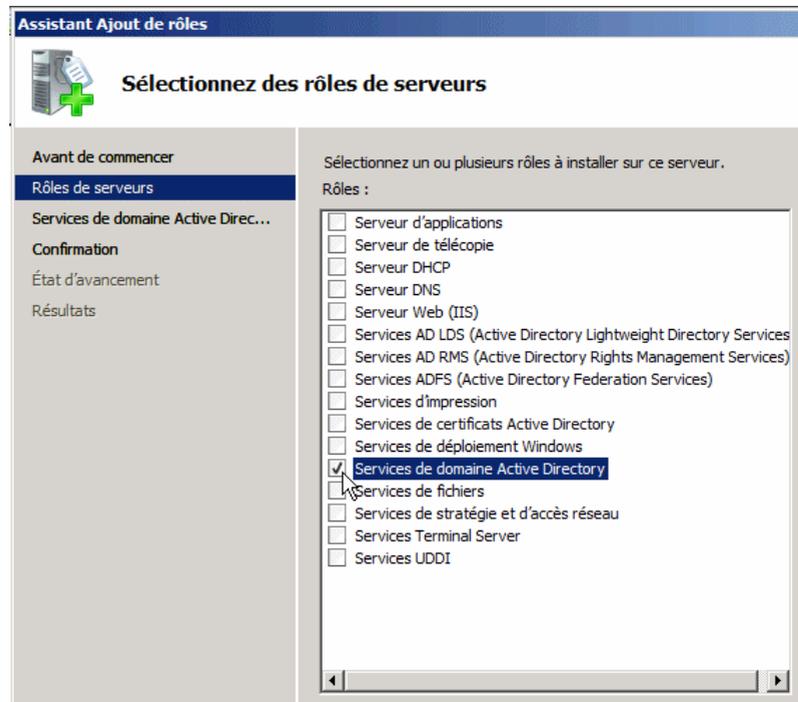


Installation d'Active Directory.

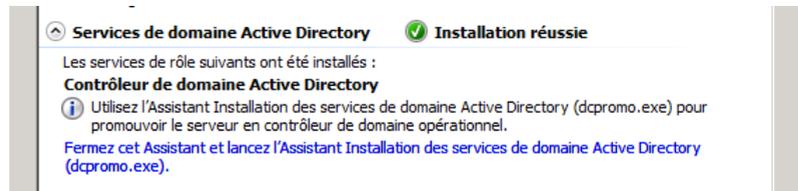
Dans la fenêtre "Tâches de configuration initiales" utilisez "Ajouter des rôles".

Il aurait également été possible de faire "Outils d'administration", "Gestionnaire de serveur", se placer sur "Rôles" et faire "Ajouter des rôles".

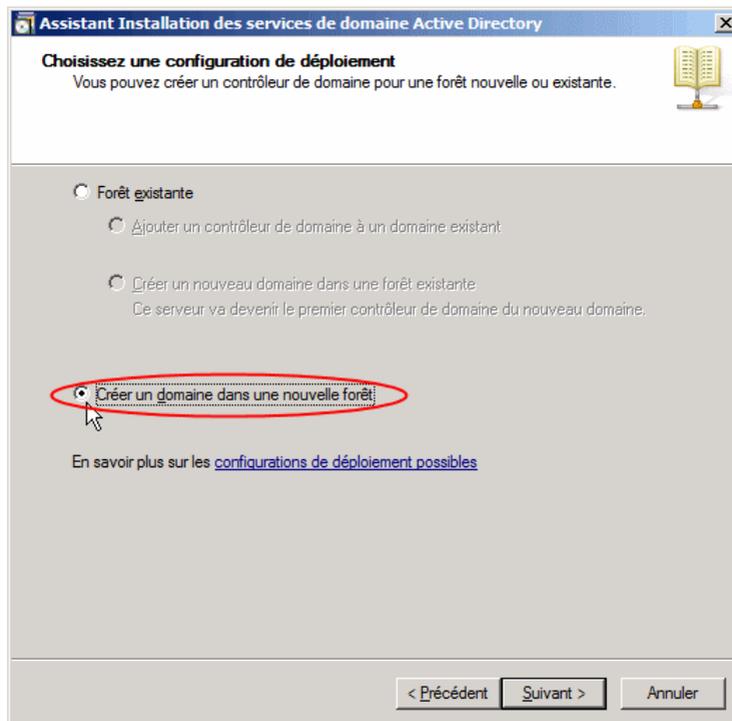
Cochez "Services de domaine Active Directory".



A la fin de l'installation, vous devez obtenir "Installation réussie".



Un assistant démarre. Dans notre cas, le mode avancé n'est pas nécessaire.



Sélectionner "créer un domaine dans une nouvelle forêt" et faites "Suivant".

Le nom de notre domaine est maintenant demandé. Comme le domaine est un domaine privé, on choisira un nom qui se termine par .priv ou .local. On utilisera de préférence des minuscules, éventuellement le signe moins (mais pas le signe _) éventuellement des chiffres. Tout autre caractère sera évité.

Exemples :

domaine.priv

lycee.priv

lycee-hugo.local

Exemple de mauvais choix :

serveur.priv (conviendrait mais prête à confusion car le mot serveur ne fait pas penser à un nom de domaine).

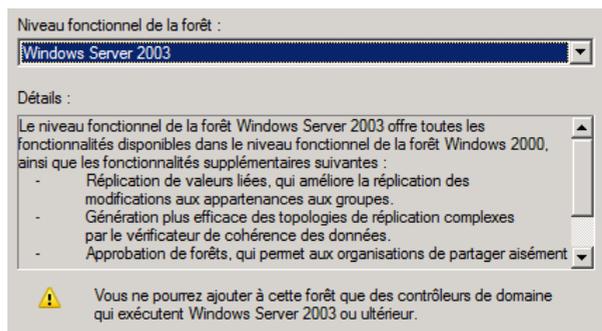
lycée.local (accent)

domaine-du-lycee-de-la-cote-d-argent.priv (nom trop long)

Le nom de domaine choisi ici est
domaine.priv

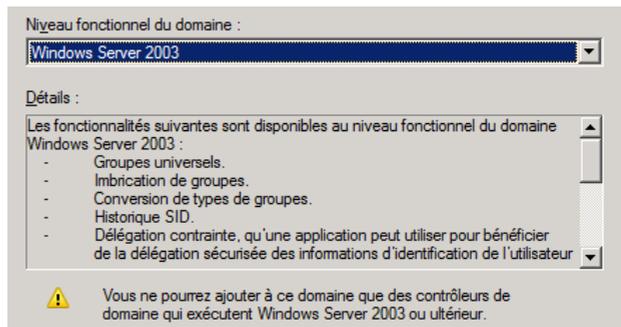


Le niveau fonctionnel de la forêt dépend des serveurs que vous voulez ajouter plus tard. On pourra par exemple choisir le niveau fonctionnel de Windows 2003.

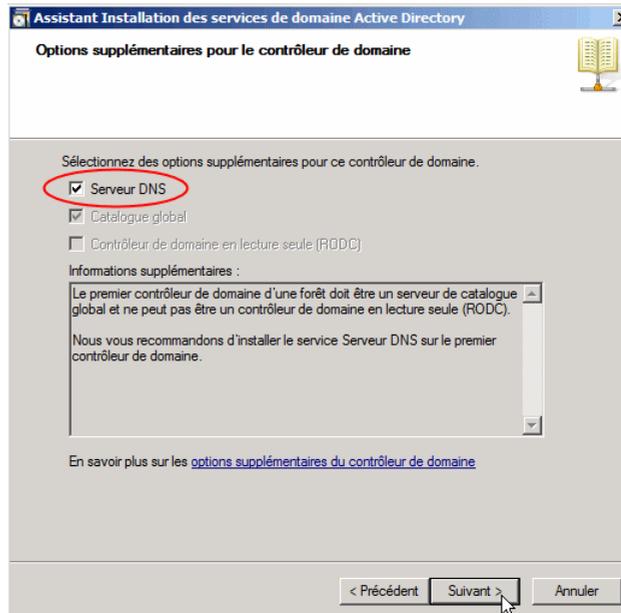


Si vous avez choisi Windows 2003 pour le niveau fonctionnel de la forêt, vous ne pouvez pas choisir plus que Windows 2003 pour le niveau fonctionnel du domaine.

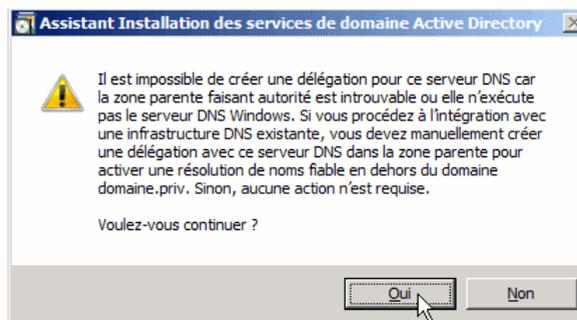
La copie d'écran montre que "Windows Serveur 2003" a été choisi pour le niveau fonctionnel du domaine.



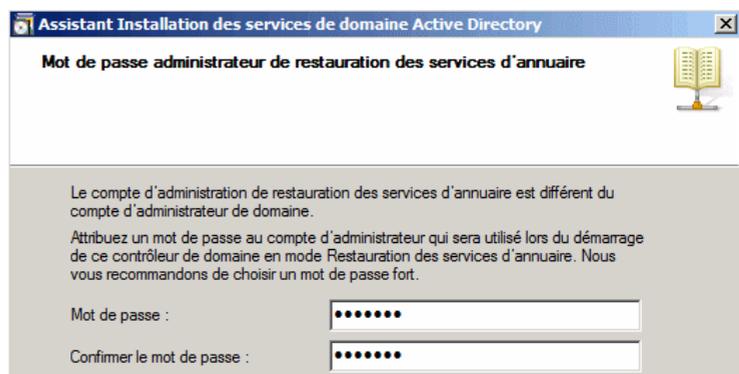
L'installation du service DNS va se faire en même temps que la création de notre domaine.



Un message d'information indique que vous ne pouvez pas créer une délégation... Indiquez que vous voulez continuer.



Le mot de passe qui vous est demandé maintenant est celui que vous devrez donner si vous avez besoin un jour de restaurer Active Directory (utilisation du programme NTBackup qui permet de sauvegarder et restaurer le système et Active Directory). Vous pouvez mettre le même mot de passe que celui de l'administrateur si vous le souhaitez.



Après un récapitulatif, l'installation commence.

Un redémarrage est demandé à la fin de l'installation d'Active Directory.

Vous devez maintenant trouver en plus dans les "Outils d'administration", "DNS" et "Utilisateurs et ordinateurs Active Directory".

Configuration du service DNS

Introduction

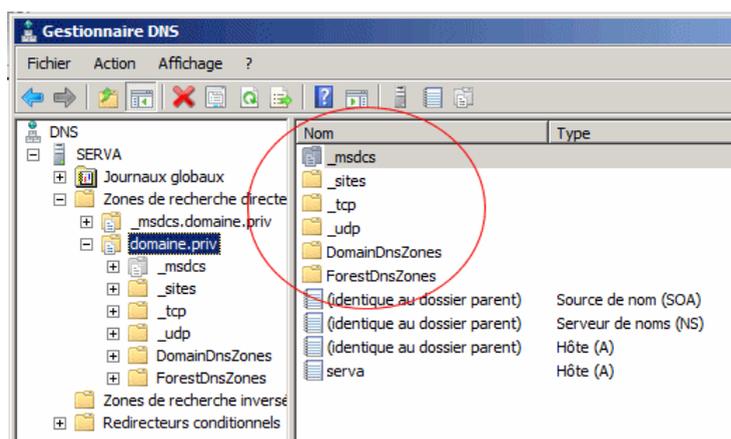
Le serveur et les stations 2000, XP et Vista ont besoin d'un serveur DNS dans le réseau local. Lorsqu'un ordinateur du réseau (à partir de Windows 2000) veut résoudre l'adresse du serveur ou d'un autre ordinateur du réseau, il s'adresse au serveur DNS déclaré dans ses propriétés réseau.

Mauvais : Imaginons que nous mettons dans le paramétrage TCP/IP des stations, l'adresse du ou des serveurs DNS du fournisseur d'accès. Les stations s'adresseraient aux DNS du fournisseur d'accès pour résoudre les adresses des ordinateurs du réseau local. Le fournisseur d'accès n'ayant pas ces informations, les stations vont mal fonctionner et des lenteurs seront inévitables.

Bon : En mettant dans le paramétrage TCP/IP des stations l'adresse du serveur DNS local (donc l'adresse IP du serveur 2000, 2003 ou 2008), les stations trouveront rapidement le serveur et les autres stations du réseau. Il reste le problème de la résolution des adresses Internet. C'est le serveur DNS qui, grâce à ses redirecteurs, va être capable de donner les réponses aux stations. Le serveur lui-même s'adresse à son propre service DNS pour résoudre les adresses. En effet dans ses propriétés réseau, c'est l'adresse 127.0.0.1 qui est indiquée comme DNS (il est également possible de mettre l'adresse IP réelle du serveur).

Vérification

Dans "Outils d'administration" cliquez sur "DNS".



Dans la copie d'écran, on peut voir que le serveur se nomme SERVA que le domaine est domaine.priv.

Remarquez que dans la partie droite, on trouve des dossiers (entourés en rouge sur la copie d'écran) qui sont indispensables au bon fonctionnement du serveur et des stations 2000, XP et Vista ainsi qu'aux éventuelles autres serveurs 2000, 2003 ou 2008 du réseau.

L'absence de ces dossiers indiquerait que le service DNS n'est pas installé correctement. Il peut être simplement nécessaire d'attendre un peu.

Si ces dossiers n'apparaissent pas :

- Vérifiez dans les propriétés réseau de votre serveur que le serveur DNS préféré contient 127.0.0.1 (ou l'adresse IP du serveur lui-même).
- Vérifiez dans votre serveur DNS que la zone de votre domaine accepte les mises à jour dynamiques (au moins les mises à jour dynamiques sécurisées).

Patientez quelques minutes, faites "Actualiser", arrêter le service DNS et redémarrez-le. Si après tout cela, les dossiers ne sont toujours pas là, essayez de désinstaller DNS puis de le réinstaller (voir plus loin dans le document pour la désinstallation et la réinstallation).

Les redirections

Les stations 2000 et surtout XP et Vista ont besoin d'avoir l'adresse IP du serveur DNS dans leurs propriétés réseau. Les redirections permettront au serveur et aux stations de résoudre les adresses extérieures.

Lorsque le service DNS connaît l'adresse demandée par une station, il donne la réponse immédiatement. C'est le cas pour toutes les adresses locales. C'est également le cas, lorsque le serveur a conservé l'information dans son cache.

Si la demande porte sur un domaine extérieur non connu, alors le service DNS s'adresse aux serveurs DNS indiqués dans ses redirections. Dès qu'il reçoit la réponse, il la retient dans son cache et la donne à la station.

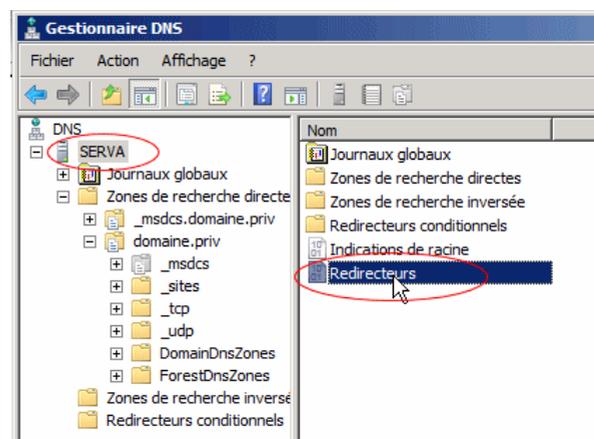
Quelle ou quelles adresses mettre comme redirections ?

Si vous accédez directement à Internet en passant par un routeur, mettez les adresses IP des serveurs DNS de votre fournisseur d'accès (ou mettez simplement l'adresse IP de votre routeur).

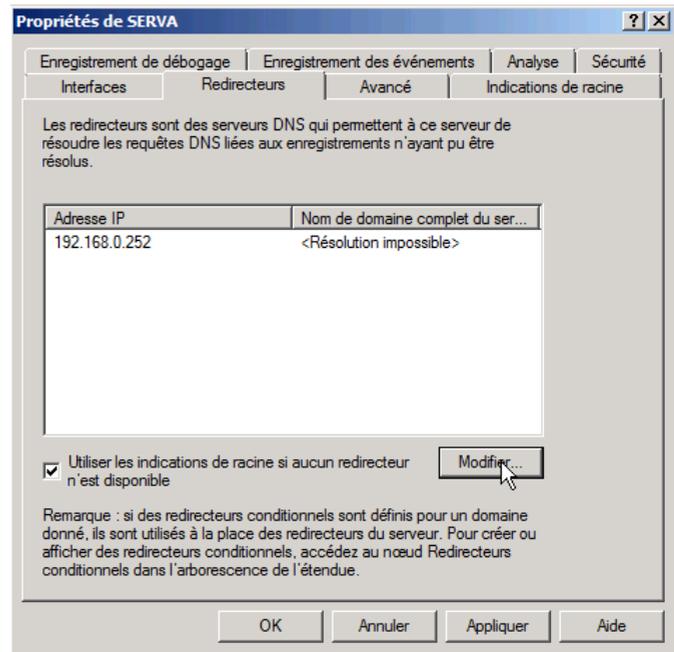
Si vous avez un serveur qui fait office de passerelle (Amon, SAI...) mettez l'adresse IP de la carte réseau côté réseau local de ce serveur. Ce serveur possède les redirections vers les DNS du fournisseur d'accès.

Donner au service DNS ses redirections

Sélectionnez le nom du serveur et cliquez sur "Redirections"



Dans la copie d'écran, l'adresse 192.168.0.252 a été indiquée. Mettez la ou les adresses qui correspondent à votre réseau.



Réduire les exigences de mots de passe

Par défaut, les mots de passe des utilisateurs doivent respecter des exigences qui ne sont peut-être pas nécessaires dans le cas d'un réseau d'établissement scolaire. En particulier, IACA fabrique des mots de passe trop simples qui ne respectent pas ces exigences.

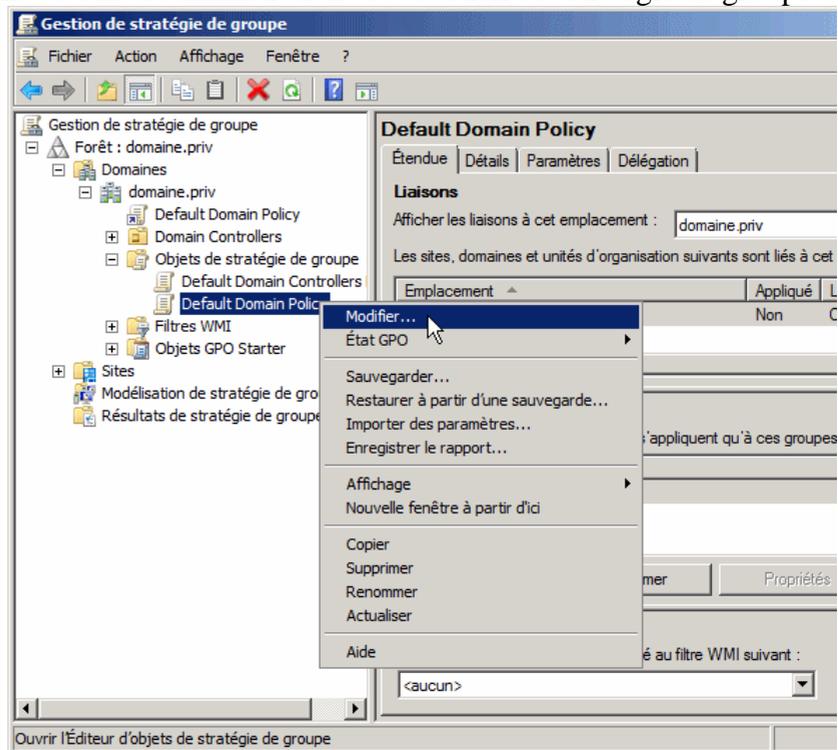
Règles par défaut pour les mots de passe :

- Les mots de passe doivent comporter au moins 7 caractères
- Chaque mot de passe doit utiliser au moins trois catégories de caractères parmi les 4 catégories suivantes.
 - Les lettres majuscules
 - Les lettres minuscules
 - Les chiffres
 - Les caractères spéciaux (@!\$*-&...)

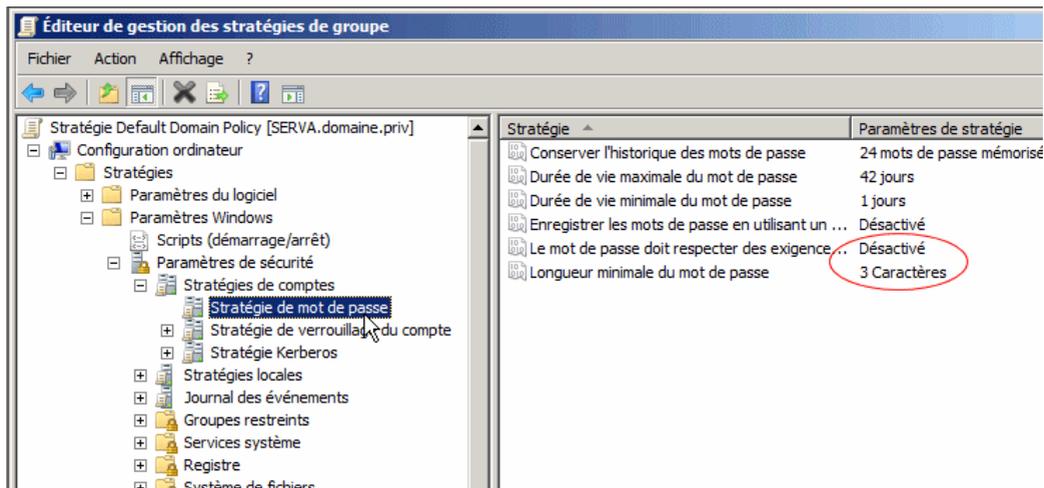
Pour réduire les exigences, allez dans "Outils d'administration" et "Gestion des stratégie de groupe".

Déployez comme indiqué sur la copie d'écran et faites un clic droit sur "**Default Domain Policy**" (ne confondez pas avec "Default Domain Controllers Policy"). Choisissez "Modifier".

Il aurait également été possible d'exécuter gpme.msc et de choisir "Default Domain Policy".



Dans la fenêtre de l'éditeur allez à "Stratégie de mot de passe" comme représenté sur la copie d'écran suivante.



Dans stratégie de mots de passe, désactivez "Le mot de passe doit respecter des exigences de complexité" et réduisez la longueur minimale du mot de passe.

Les mots de passe de IACA font par défaut 5 ou 6 caractères. Si vous avez laissé ce choix, vous pouvez mettre la longueur minimale du mot de passe à 5.

La modification de la stratégie n'est pas effective immédiatement. Il faut attendre quelques minutes. Si vous ne voulez pas attendre, vous pouvez exécuter GPUPDATE.

Réduire les exigences des communications réseau

Problème

Depuis Windows 2003, la nouvelle exigence des communications réseau fait que les stations ne peuvent communiquer avec le serveur que de façon signée numériquement.

Avec un serveur 2000, par défaut, cette communication signée ne se faisait que si la station en était capable.

Si vous avez des stations 95, les exigences par défaut de Windows 2003 et Windows 2008 ne conviennent pas.

Si vous avez des stations NT4, vous devez au moins avoir le service pack 4 installé.

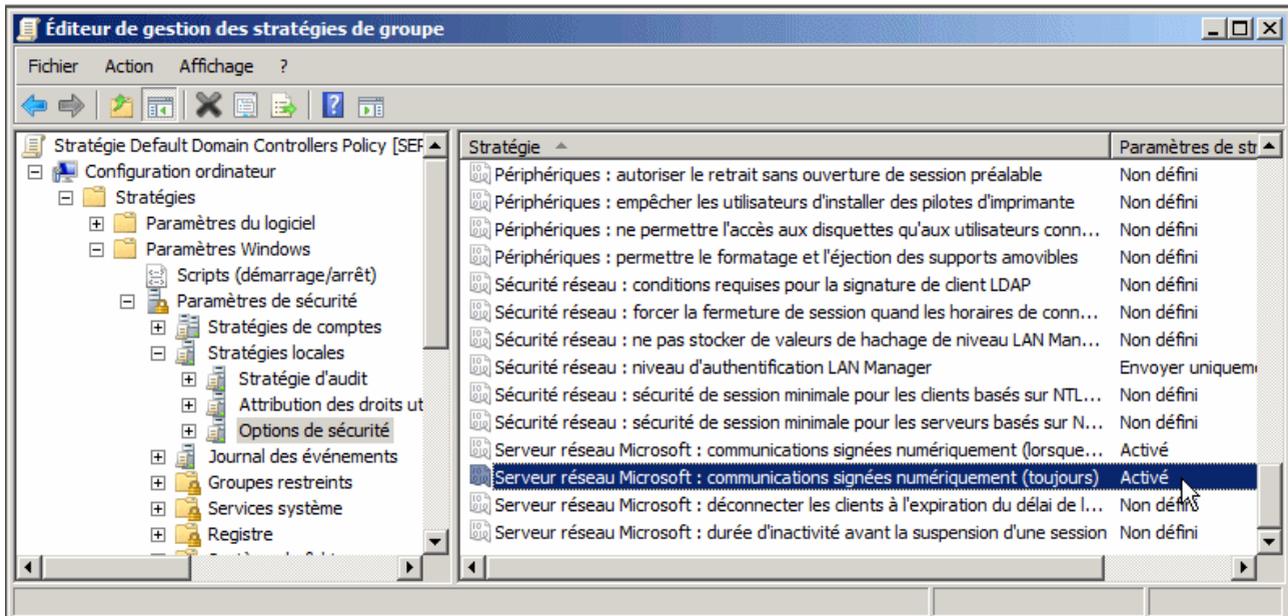
Si vous voulez démarrer une station en DOS et accéder au serveur, les exigences par défaut de Windows 2003 et Windows 2008 ne conviennent pas.

Il est possible également que des Windows 98 ne trouvent pas le voisinage réseau ou perde le voisinage réseau à cause de cette exigence.

Solution

Si toutes vos stations sont au moins en Windows 2000 pro ou si vous avez des Windows 98 qui accèdent correctement au serveur laissez le paramétrage par défaut.

Si ce n'est pas le cas, dans les "Outils d'administration", ouvrez " et "Gestion des stratégie de groupe". Faites un clic droit sur "Default Domaine Controllers Policy" et "Modifier".



Il est vivement conseillé de laisser le paramétrage par défaut (comme indiqué sur la copie d'écran). Ne désactivez "Serveur réseau Microsoft : communications signées numériquement (toujours)" que si vous avez des Windows 95 ou des NT4 qui n'ont pas au moins le service pack 3 installé.

Laissez "activé" pour les communications signées numériquement (lorsque le serveur l'accepte)

Exécutez GPUPDATE si vous voulez que cette modification soit prise en compte immédiatement.

Désinstaller Active Directory

ATTENTION cette opération supprime tous les comptes existants. Si votre serveur possède des comptes utilisateurs ou des groupes ou des comptes d'ordinateurs (des stations Windows NT Workstation ou Windows 2000 Pro ou XP Pro ou Vista Pro inscrites dans Active Directory), **tout disparaîtra si vous désinstallez Active Directory.**

Si, avec ces mises en garde, vous décidez tout de même de désinstaller Active Directory, voici comment procéder :

Exécutez **dcpromo**. Un assistant démarre...

Comme votre serveur est le seul serveur du domaine, vous pouvez cocher "Supprimer le domaine car le serveur est le dernier serveur du domaine".

Vous serez ensuite informé que "Microsoft DNS Directory" va également être supprimé. Cliquez sur Suivant.

Une confirmation est demandée. Cochez "Supprimer toutes partitions de l'annuaire..."

Lorsque Active Directory sera désinstallé, le compte Administrateur du domaine n'existera plus, mais le compte Administrateur local redeviendra accessible. Il vous est demandé le mot de passe de l'administrateur local. Ne l'oubliez pas.

Après redémarrage, vous pouvez ouvrir la session avec le compte Administrateur et le mot de passe que vous venez d'indiquer.

Vous pouvez éventuellement maintenant supprimer le rôle "Service de domaine Active Directory".

Si vous voulez réinstaller Active Directory, exécutez à nouveau **dcpromo**. Si vous avez supprimé le rôle il faudra au préalable réinstaller le rôle.

Désinstaller le service DNS

Si vous n'avez plus besoin du service DNS vous pouvez le supprimer.

Si votre service DNS ne fonctionne pas correctement, vous pouvez le désinstaller et le réinstaller même si Active Directory est installé.

Allez dans "Gestionnaire de serveur", placez-vous sur "Rôles". Faites "Supprimer des rôles" et enlevez la coche devant "Serveur DNS".

Le bouton "Supprimer" effectuera la première partie de la suppression, un redémarrage sera alors demandé et après redémarrage la suppression se poursuivra.

Active Directory a besoin d'un serveur DNS. Si vous n'avez pas l'intention de réinstaller le serveur DNS sur cet ordinateur, pensez à changer dans le paramétrage TCP/IP de la carte réseau l'adresse du serveur DNS afin de pointer vers un serveur DNS ayant toutes les données utiles et spécifiques à Microsoft.

Si votre intention est de réinstaller maintenant le serveur DNS laissez 127.0.0.1 dans le paramétrage DNS de la carte réseau et procédez à l'installation comme indiqué ci-après.

Installer le service DNS

Si le service DNS n'est pas installé, ou s'il a été désinstallé, vous pouvez procéder à son installation.

Faites "Ajouter des rôles" cochez "Serveur DNS".

Comme Active Directory est déjà installé vous êtes informé que les zones seront automatiquement ajoutées lors de l'installation. Tout est donc automatique.