

Installation de Windows 2003 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 2003 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 2003 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 2003 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 2003

Préparation

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

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 CD de Windows 2003 Serveur dans le lecteur de CDRom.

Choix des partitions : Je choisis habituellement 6 ou 8 Go pour installer Windows 2003 Serveur. Le reste du disque dur sera traité plus tard.

Choisissez un formatage NTFS.

Lorsque vous avez tapé le numéro de licence, le programme d'installation vous demande le mode de licences. Répondez "Par serveur" et indiquez le nombre de licences nécessaires. Une licence d'utilisation est une autorisation (un simple papier) vous donnant le droit d'utiliser le serveur à partir d'une station. Cinq licences sont déjà fournies avec Windows 2003 Serveur, donc si vous avez par exemple 50 stations, vous devez acheter 45 licences et mettre 50 comme nombre de licences.

Nom d'ordinateur : On pourra mettre SERVEUR si ce nom n'existe pas déjà dans votre réseau.

Mot de passe de l'administrateur : Il s'agit du mot de passe de l'administrateur local qui vous servira pour ouvrir une session (le même mot de passe sera utilisé après installation d'Active Directory mais vous pourrez bien sûr le changer).

Si vous choisissez un mot de passe trop simple, vous serez invité à en choisir un plus compliqué. Il est conseillé de choisir un mot de passe compliqué pour le compte administrateur. Il est toutefois possible d'utiliser un mot de passe simple.

Lorsque le programme d'installation vous demande le groupe de travail ou le domaine d'ordinateurs, laissez le choix "groupe de travail" et le nom du groupe de travail n'a pas d'importance.

Lorsque l'installation est terminée, votre ordinateur redémarre. Si vous avez oublié d'enlever le CD du lecteur, ce n'est pas gênant, ne touchez pas au clavier et au bout de quelques secondes, le démarrage se fera à partir du disque dur.

Vous êtes invité à taper le mot de passe de l'administrateur local.

A ce stade, votre ordinateur se comporte à peu près comme un Windows XP Pro.

Vous pouvez créer des utilisateurs, des groupes... Mais ce que vous faites maintenant sera oublié lors de l'installation d'Active Directory.

Vérifications

Vérifiez que tout est installé correctement à l'aide du "Gestionnaire de périphériques" que vous pouvez trouver en faisant "Démarrer", "Outils d'administration", "Gestion de l'ordinateur" et "Gestionnaire de périphériques". (On peut arriver également au même endroit en faisant "Démarrer", un clic droit sur "Poste de travail", "Propriétés", "Matériel" et "Gestionnaire de périphériques").

Paramétrage de la carte réseau.

"Démarrer", "Panneau de configuration" et "Connexions réseau". Faites un clic droit sur "Connexion au réseau local" et choisissez "Propriétés" (On peut arriver plus vite au même endroit en faisant un clic droit sur "Favoris réseau". Si vous ne trouvez pas facilement Favoris réseau, ouvrez le poste de travail et remontez d'un niveau ou encore ouvrez l'explorateur qui est dans les accessoires.).

Dans TCP/IP mettez l'adresse IP souhaitée pour ce serveur, mettez le masque de sous-réseau. Si vous avez un accès Internet, mettez comme passerelle l'adresse IP du routeur ou de l'ordinateur servant de passerelle.

Ne mettez pas de DNS, ils seront placés plus tard dans les redirecteurs.

Il n'est pas demandé de redémarrer l'ordinateur mais vous pouvez tout de même le faire.

Vérifiez que votre réseau fonctionne à l'aide de PING.

Pare-feu.

Pour la suite, si vous utilisez Windows 2003 SP1 ou plus récent, un pare-feu est disponible mais il est par défaut désactivé.

Vérifiez que vous n'avez pas activé le pare-feu. En effet si on activait le pare-feu il faudrait créer de nombreuses exceptions afin de permettre au serveur de jouer son rôle de contrôleur de domaine.

Installation d'Active Directory.

Si vous n'avez pas la fenêtre "Gérer votre serveur", vous pouvez la faire apparaître en faisant "Démarrer", "Outils d'administration" et "Gérer votre serveur".

Utilisez "Ajouter ou supprimer un rôle"



Fig. AD_Install_01

Placez la surbrillance sur "Contrôleur de domaine (Active Directory)"

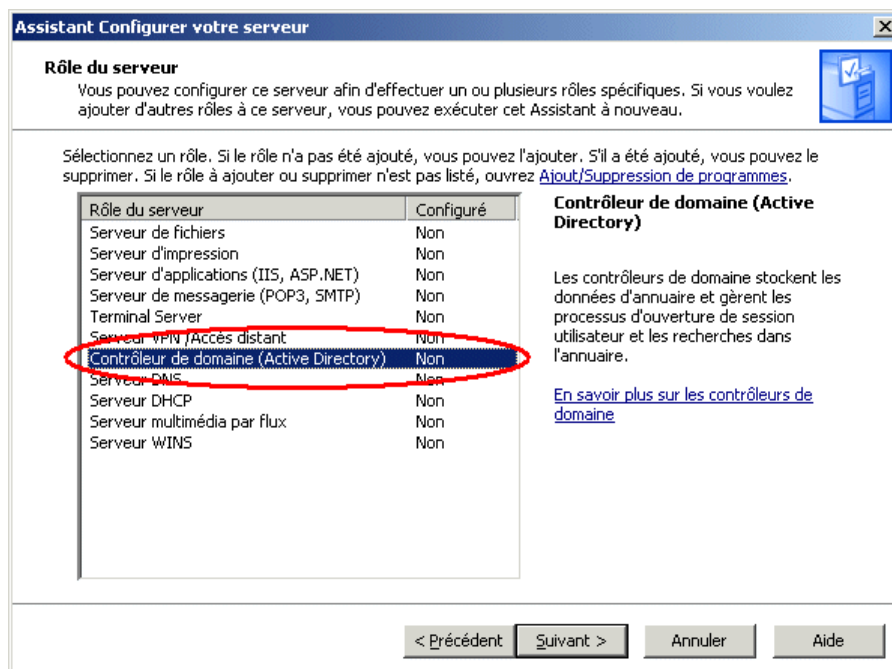


Fig. AD_Install_02

Remarque : L'installation du serveur DNS comme on le verra plus tard, se fera automatiquement en même temps que l'installation d'Active Directory.

Vous serez informé que les stations 95 ne fonctionneront pas avec votre serveur.

Les stations NT4 ayant un service pack inférieur au 4 devront être mises à jour pour être utilisées.

Si vous possédez des stations 95 il sera tout de même possible de les utiliser mais pour cela il faudra réduire la sécurité du serveur 2003 (décrit plus loin).

Choisissez "Contrôleur de domaine pour un nouveau domaine".

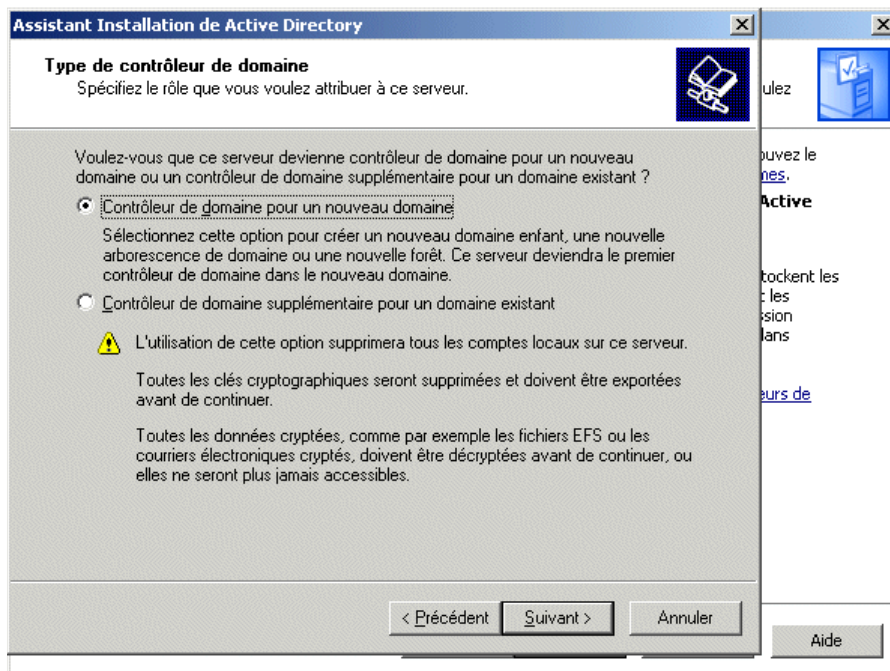


Fig. AD_Install_03

Domaine dans une nouvelle forêt

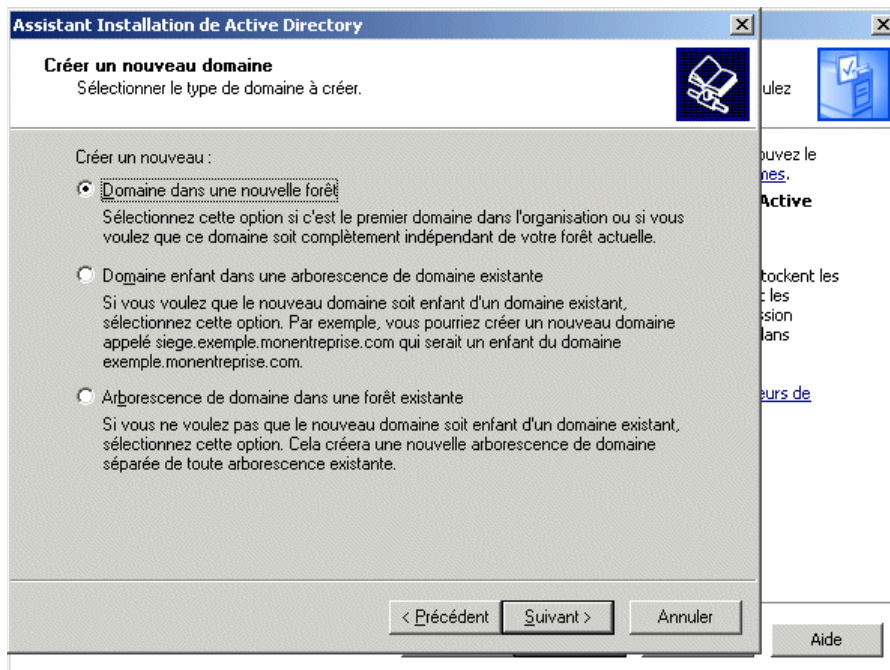


Fig. AD_Install_04

Vous devez maintenant choisir le nom que vous allez donner à votre domaine. Le nom **ac-reims.fr** est un exemple de nom de domaine, mais il ne serait pas souhaitable de reprendre ce nom puisqu'il existe déjà. Il n'est pas non plus souhaitable de choisir un nom se terminant par .com ou .fr ou .org ou .net... car ces noms existent déjà sur Internet.

Le nom de domaine doit être composé de deux parties séparées entre elles par un point. A droite du point il s'agit du "grand domaine" ou domaine de premier niveau. Vous choisirez l'un des deux mots **priv** ou **local** pour ce nom de grand domaine car ce sont les mots réservés pour un réseau local. Je suppose dans la suite que vous avez choisi priv. A gauche du point, vous pouvez choisir ce que vous voulez en respectant certaines règles :

Evitez de commencer par un chiffre.

N'utilisez pas de caractères spéciaux comme l'espace ou le point ou les accents...

Evitez de choisir un nom de plus de 15 caractères.

Le tiret - (signe moins) est à préférer au signe de soulignement _.

Ne prenez pas le même nom que le nom du serveur.

Exemple de mauvais choix :

domaine.lycee.priv (deux points)

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)

Si par exemple votre établissement s'appelle "Lycée Val des Champs fleuris" vous pourrez simplifier en choisissant comme nom de domaine lvdcf.priv. Dans la copie d'écran ci-après, le domaine que j'ai choisi est dom.priv.

On pourra remarquer que le nom a été tapé en minuscules (c'est ce qui est habituellement fait pour les noms de domaines sur Internet).

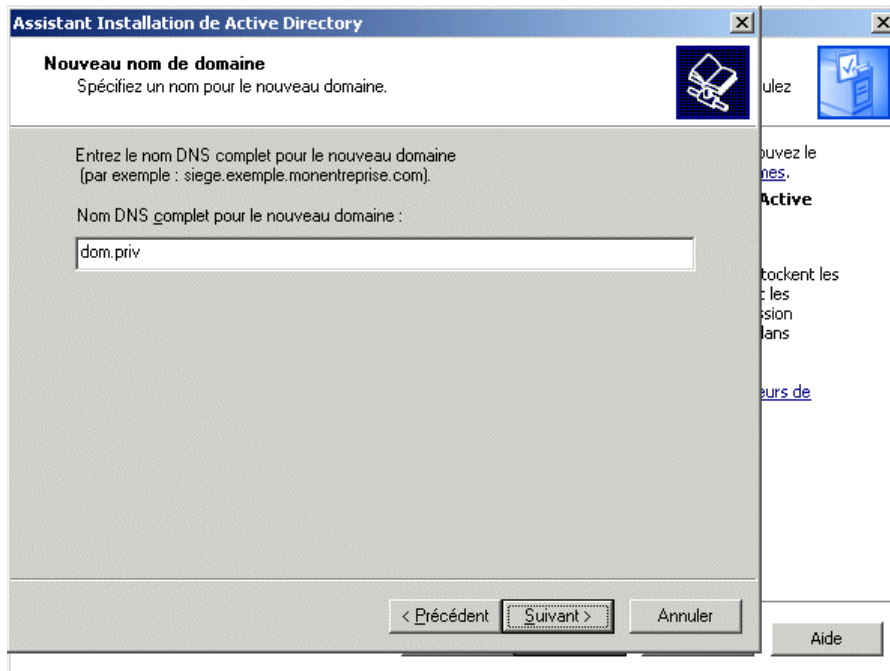


Fig. AD_Install_05

Le nom de domaine NetBIOS est fabriqué automatiquement à partir du nom du domaine complet. En général, il s'agit de la première partie convertie en majuscules. Dans certains cas, ce nom ne convient pas et un autre nom vous est proposé.

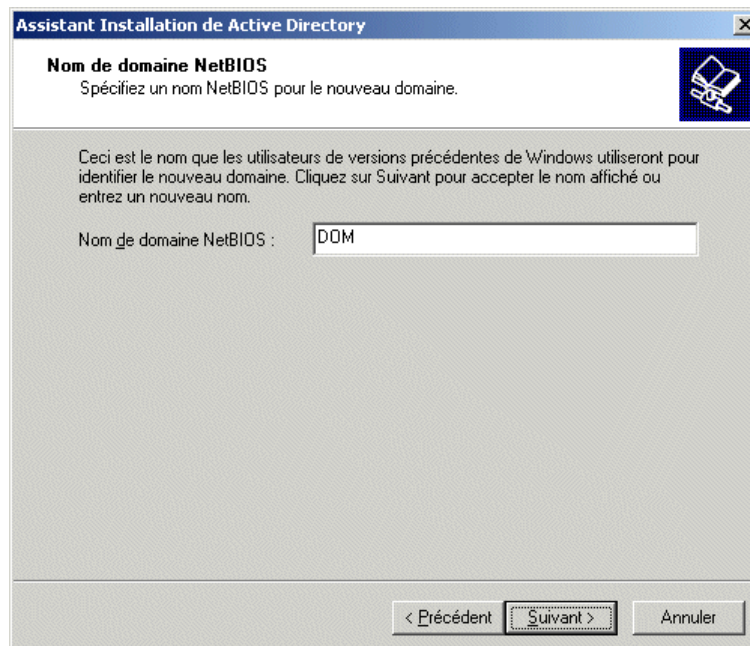


Fig. AD_Install_06

Laissez les dossiers proposés.

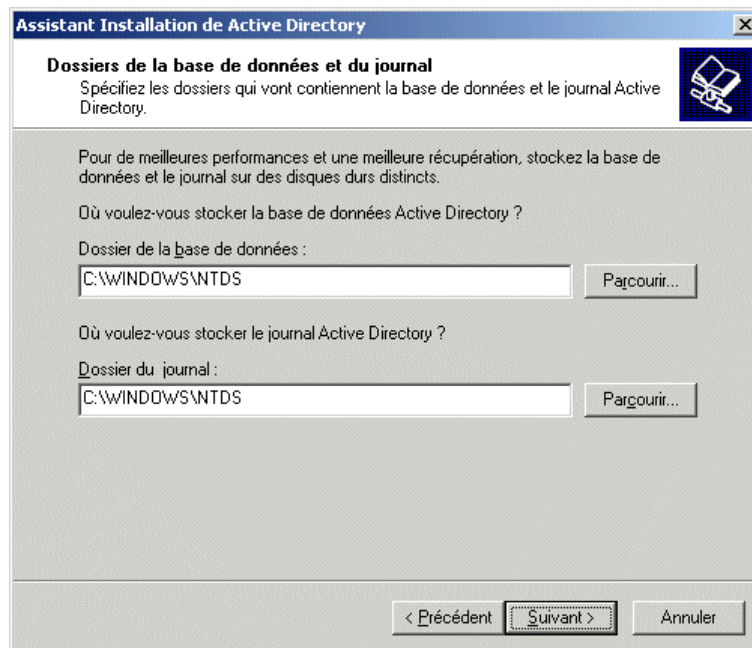


Fig. AD_Install_07

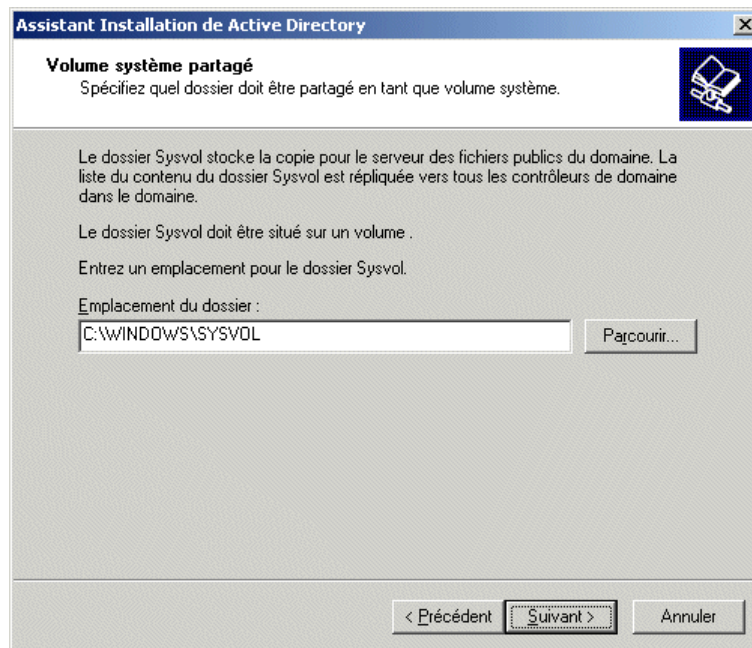


Fig. AD_Install_08

Vous êtes informé qu'un serveur DNS n'a pas été trouvé et que Windows 2003 s'apprête à en installer un. Laissez le choix "Installer et configurer le serveur DNS sur cet ordinateur...".

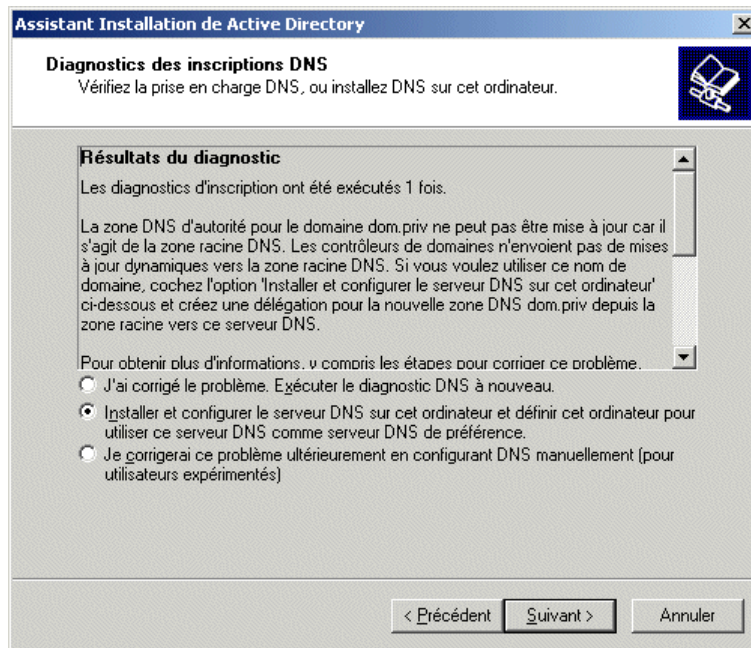


Fig. AD_Install_09

Comme j'ai supposé qu'il s'agit de l'unique serveur de votre réseau, le choix de la copie d'écran suivante convient. Si vous possédez un serveur NT4 pensez qu'il ne communiquera pas bien avec votre serveur 2003 (même si vous choisissez la première option).

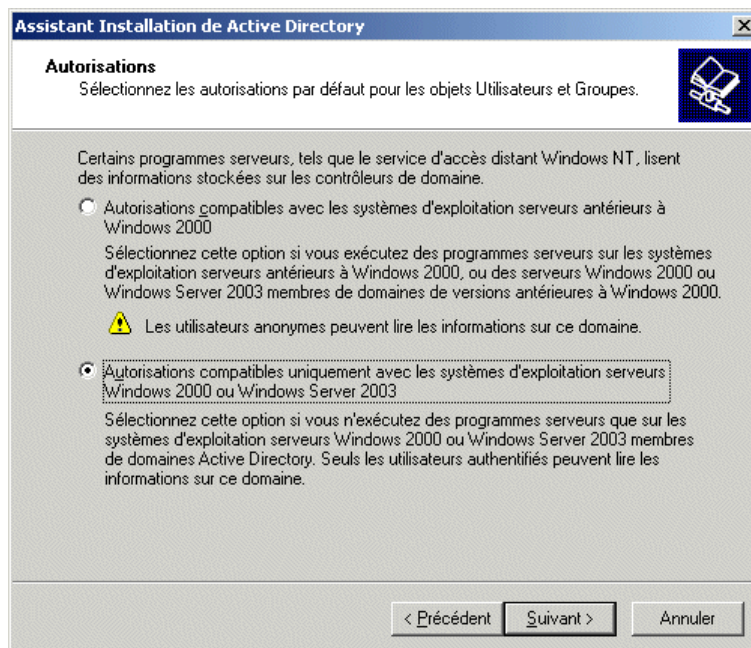


Fig. AD_Install_10

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.

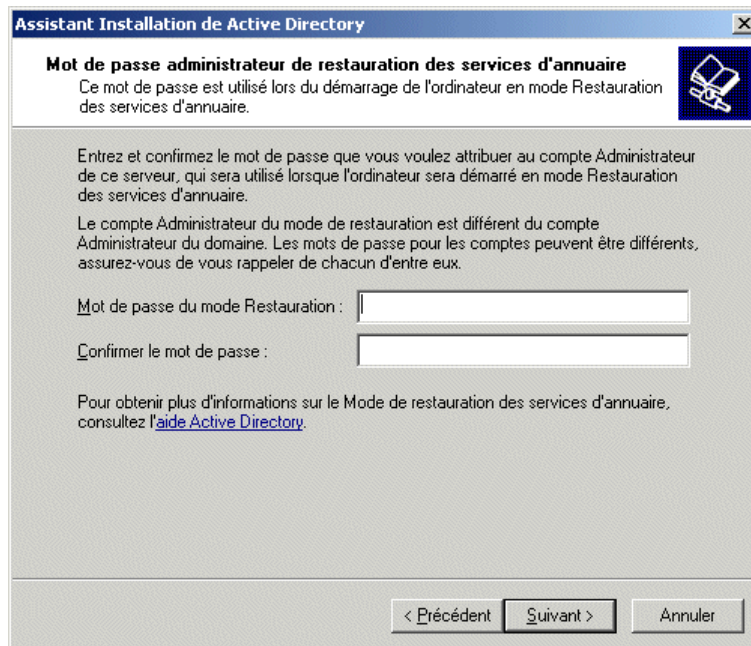


Fig. AD_Install_11

Voici le résumé de ce qui va être fait :

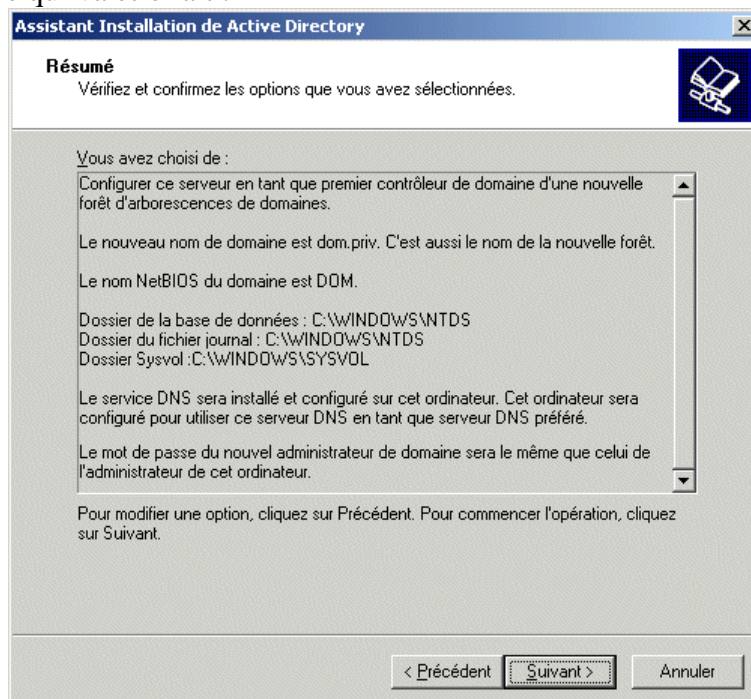


Fig. AD_Install_12

Remarquez qu'il est fait référence à deux mots de passe, celui de l'administrateur du domaine et celui de l'administrateur de la station. En effet lorsque Active Directory sera installé, les comptes locaux ne seront plus utilisables et en particulier le compte Administrateur de la station. Seuls les comptes du domaine pourront être utilisés.

Après installation d'Active directory, pour ouvrir une session sur votre serveur, ce sera le compte Administrateur du domaine qui sera utilisé.

Finalement, vous devriez obtenir ce résumé

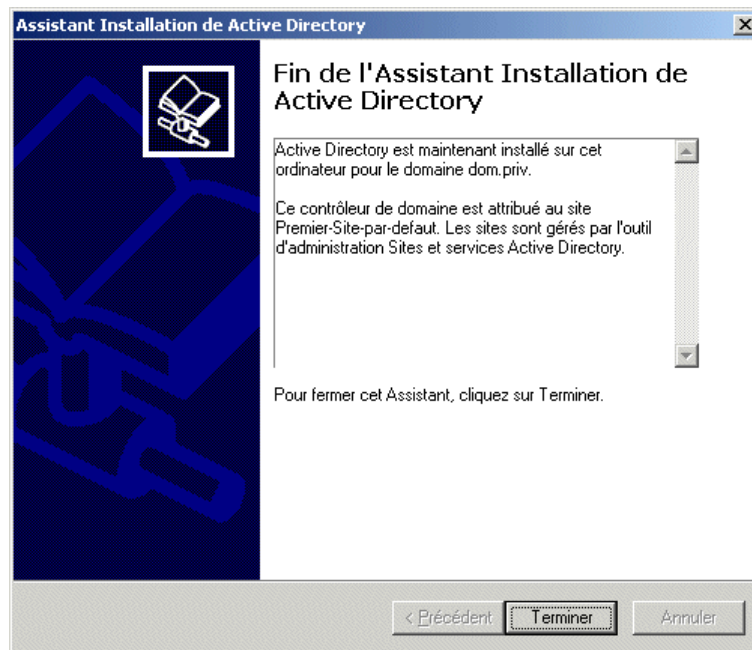


Fig. AD_Install_13

Votre ordinateur redémarre...

Configuration du service DNS

Introduction

Le serveur et les stations 2000 et XP ont besoin d'un serveur DNS dans le réseau local. Lorsqu'un ordinateur du réseau (Windows 2000, 2003 ou XP) 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 mettions 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 ou 2003), 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).

Les redirecteurs

Les stations 2000 et surtout XP ont besoin d'avoir l'adresse IP du serveur DNS dans leurs propriétés réseau. Les redirecteurs 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 redirecteurs. Dès qu'il reçoit la réponse, il la retient dans son cache et la donne à la station.

Quelle ou quelles adresses mettre comme redirecteurs ?

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 redirecteurs vers les DNS du fournisseur d'accès.

Donner au service DNS ses redirecteurs

Faites "Démarrer", "Outils d'administration" et "DNS".



Fig. DNS_Installer_01

Dans la copie d'écran, on peut voir que le serveur se nomme SERV2003.

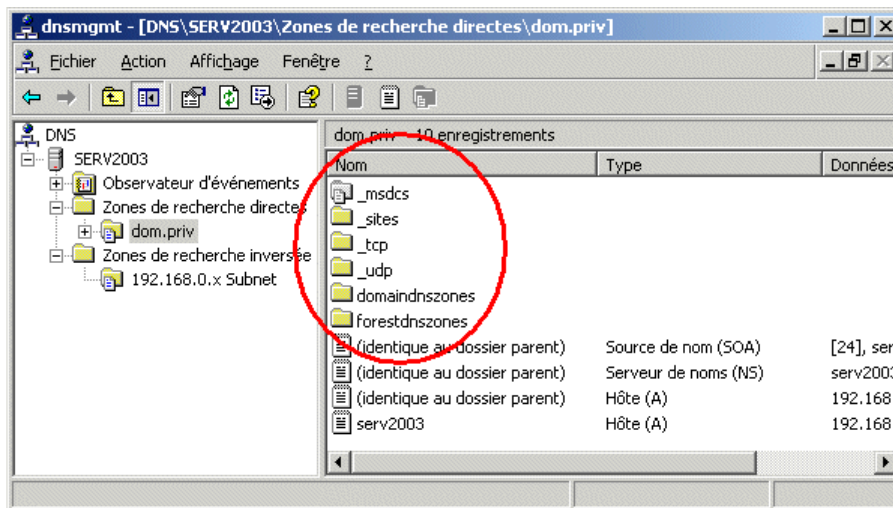


Fig. DNS_Installer_02

Remarquez que dans la partie droite, on trouve des dossiers qui sont indispensables au bon fonctionnement du serveur et des stations 2000 et XP ainsi qu'aux éventuelles autres serveurs 2000 ou 2003 du réseau.

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", arrêtez 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).

Clic droit sur le nom du serveur, "Propriétés" et "Redirecteurs"

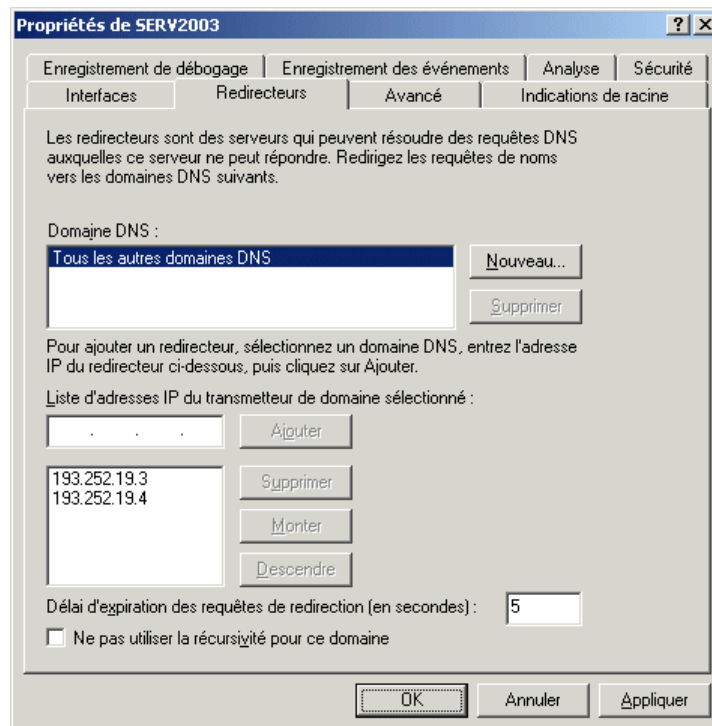


Fig. DNS_Installer_03

Dans la copie d'écran, ce sont les adresses des serveurs DNS de wanadoo qui ont été indiquées.

S'il est impossible d'indiquer des redirecteurs, c'est certainement que vous avez une zone de recherche directe composée d'un point seulement (votre serveur DNS se croit le "plus haut dans monde" et ne peut donc pas s'adresser au dessus de lui !). Supprimez cette zone composée d'un point seulement (il faudra peut-être actualiser ou attendre un peu avant de pouvoir ajouter les redirecteurs).

Recherche inversée (facultatif)

Si vous souhaitez activer la recherche inversée (possibilité de retrouver le nom de l'ordinateur à partir d'adresse IP), faites un clic droit sur "Zone de recherche inversée" (voir Fig. DNS_Install_01) et créez une nouvelle zone.

Cochez "Enregistrer la zone dans Active Directory..." (Fig. DNS_Installer_03).

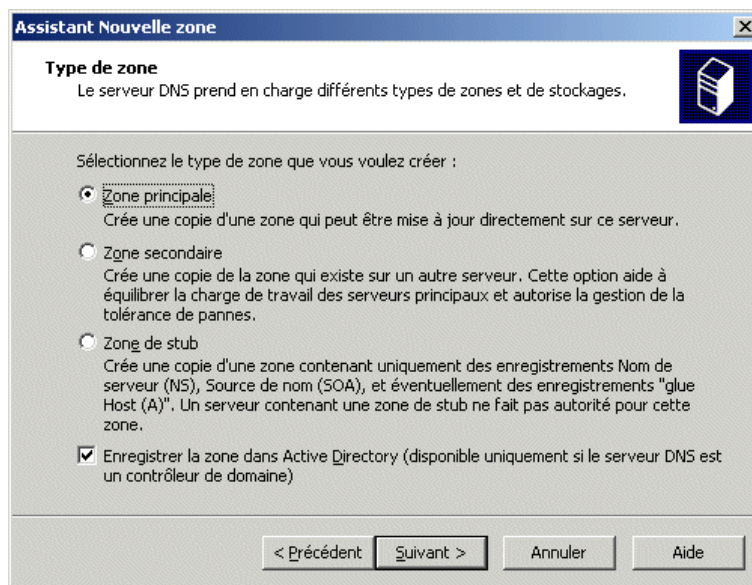


Fig. DNS_Installer_03

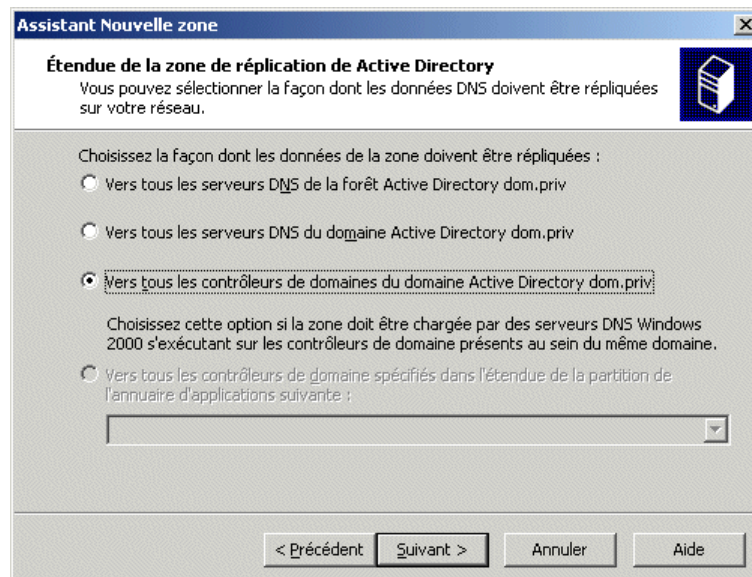


Fig. DNS_Installer_04

Indiquez votre sous-réseau (c'est à dire les premiers nombres de l'adresse IP de votre serveur).

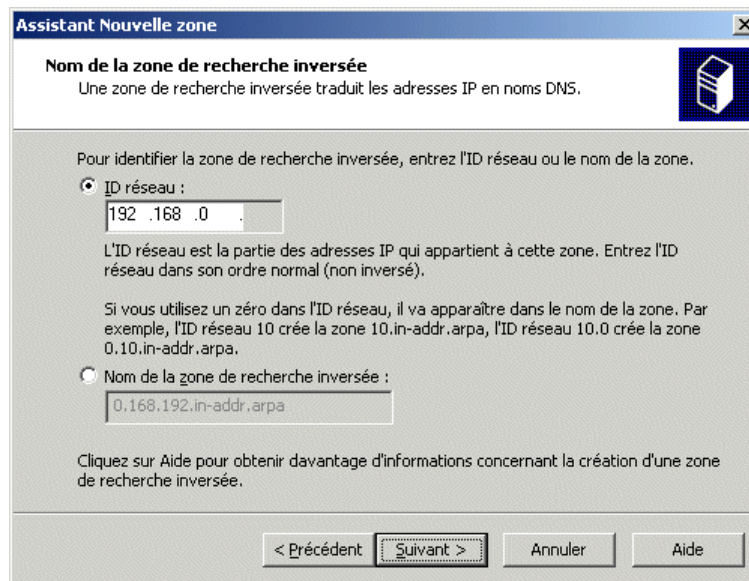


Fig. DNS_Installer_05

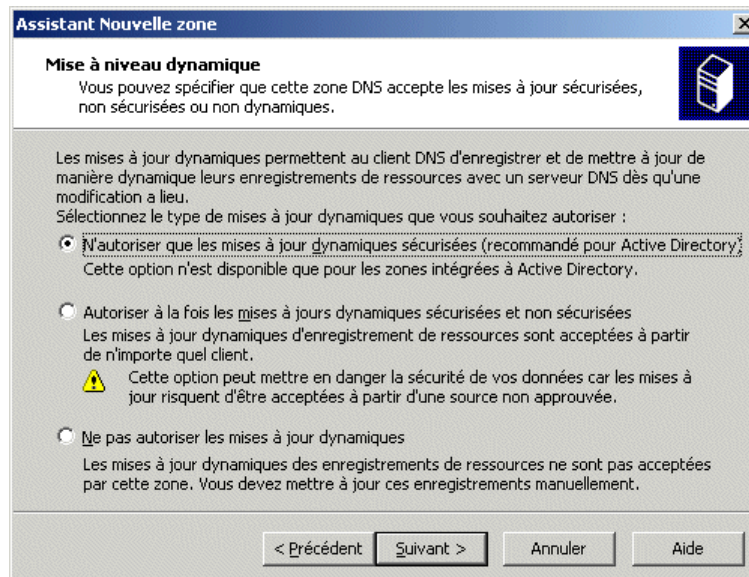


Fig. DNS_Installer_06

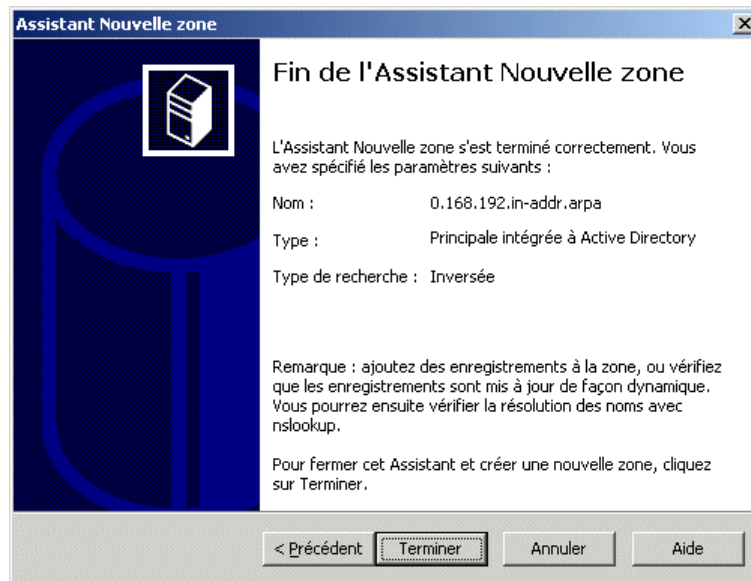


Fig. DNS_Installer_07

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 "Stratégie de sécurité du domaine"

Ne confondez pas avec "Stratégie de sécurité du contrôleur de domaine".

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.

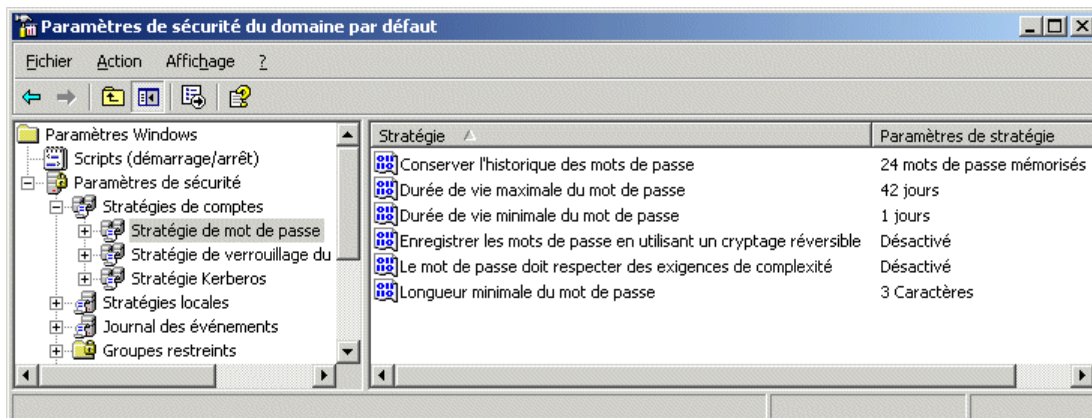


Fig. DNS_Installer_08

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 ne conviennent pas.
Si vous avez des stations NT4, vous devez au moins avoir le service pack 4 d'installé.
Si vous voulez démarrer une station en DOS et accéder au serveur, les exigences par défaut de Windows 2003 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

Dans les "Outils d'administration", ouvrez "Paramètres de sécurité du **contrôleur** de domaine".
Dans les "Paramètres de sécurité", "Stratégies locales" et "Options de sécurité", vous trouvez "Serveur réseau Microsoft : communications signées numériquement (toujours)" qu'il faut **désactiver**.

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.

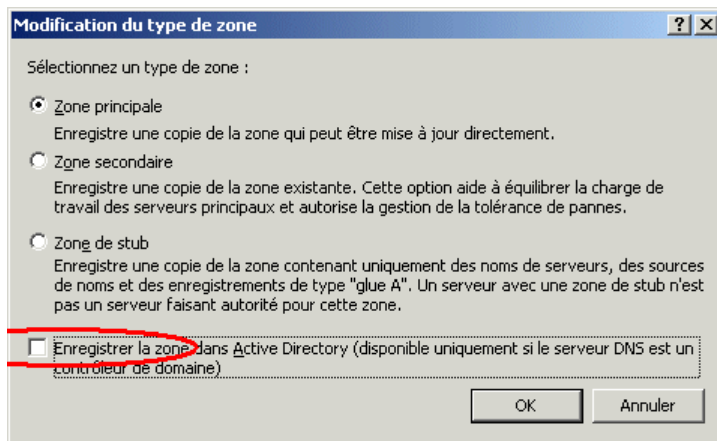
Désinstaller Active Directory

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 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 :

Comme le service DNS fait partie de Active Directory, il est souhaitable de commencer par sortir le service DNS d'Active Directory.

"Outils d'administration", "DNS". Allez dans "Zone de recherche directe", faites un clic droit sur votre domaine et choisissez "propriétés". Dans le volet "Général", utilisez le bouton "Modifier" correspondant au type "Intégré à Active Directory". Enlevez la coche devant "Enregistrer la zone dans..."



Si vous avez créé une zone inversée, faites de même avec pour cette zone de recherche inversée.

Dans "Gérer votre serveur", choisissez "Ajouter ou supprimer un rôle", placez-vous sur "Contrôleur de domaine (Active Directory)" et utilisez le bouton "Suivant". L'assistant d'installation d'active directory est alors appelé.

Vous pouvez arriver plus rapidement à cet assistant en exécutant DCPROMO

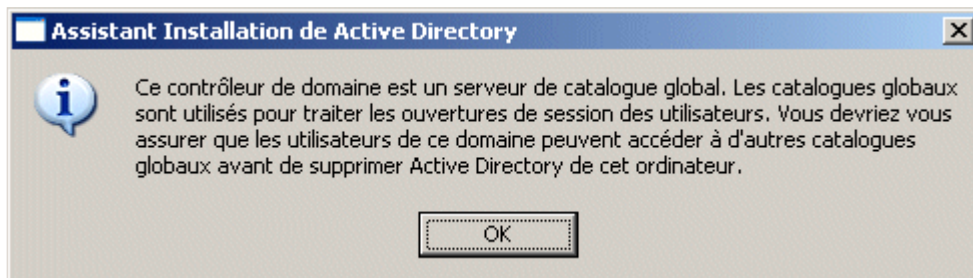


Fig. AD_Desinstaller_01

Cochez "Ce serveur est le dernier contrôleur de domaine"

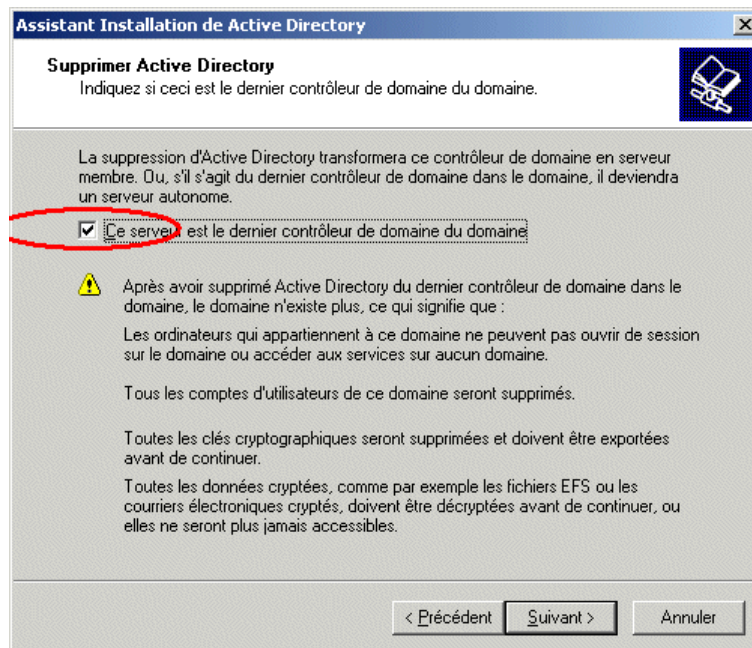


Fig. AD_Desinstaller_02

Il est possible que vous soyez informé que des données de DNS vont rester dans Active Directory.

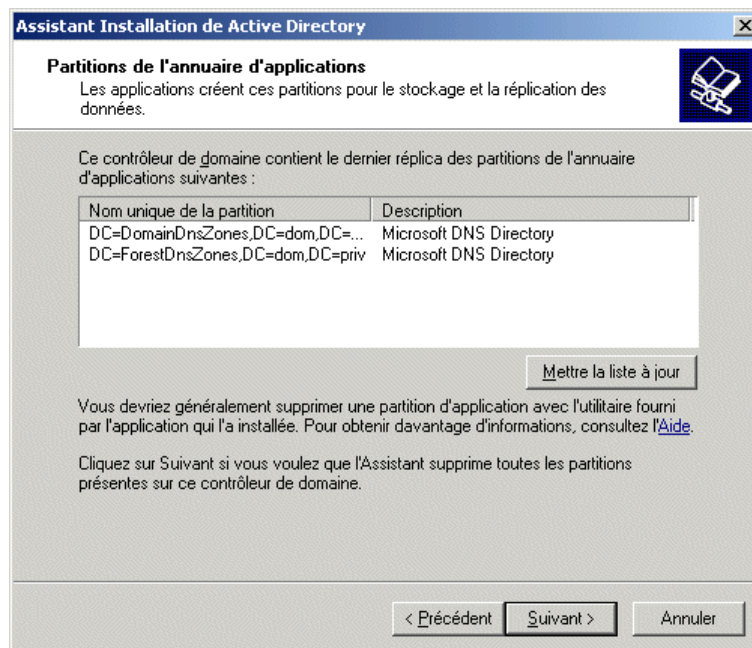


Fig. AD_Desinstaller_03

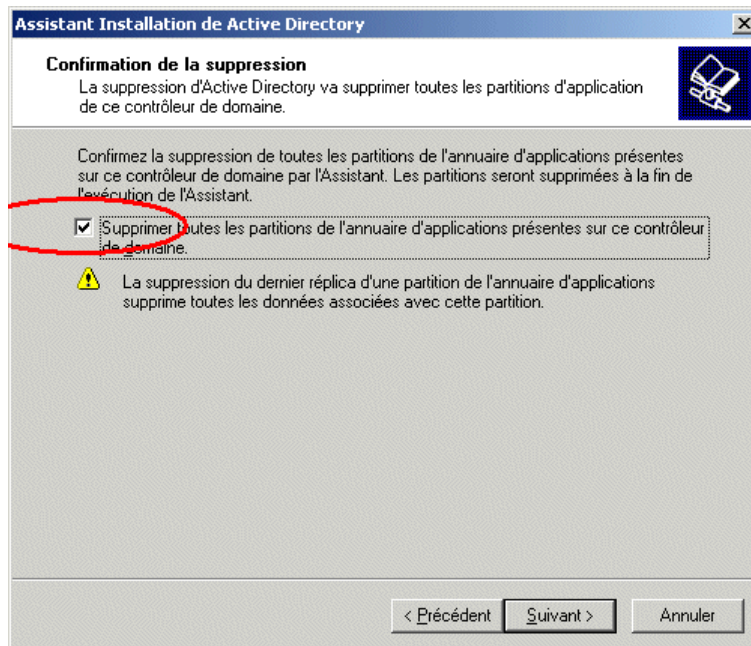


Fig. AD_Desinstaller_04

Le mot de passe qui vous est demandé est celui qui sera attribué au compte Administrateur local. C'est donc celui que vous devrez utiliser pour ouvrir une session lorsque Active Directory aura été supprimé. Ne le perdez pas !

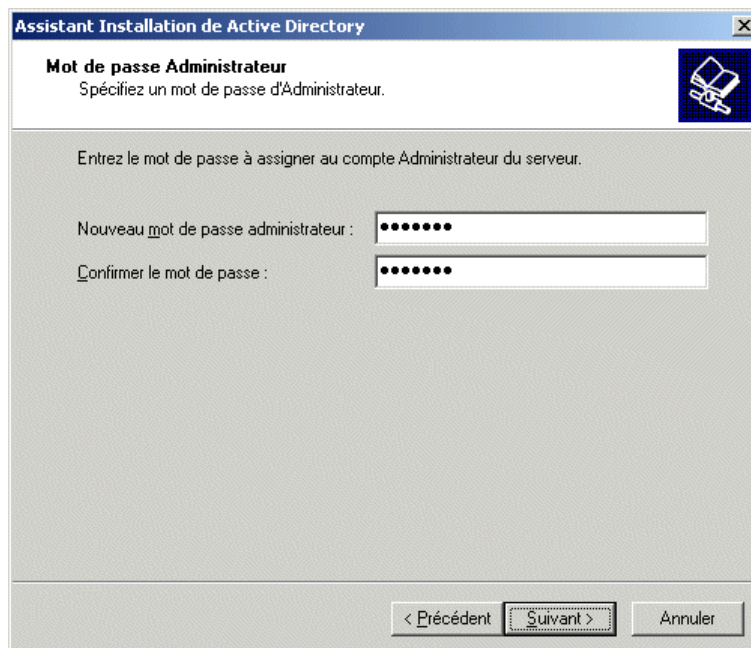


Fig. AD_Desinstaller_05

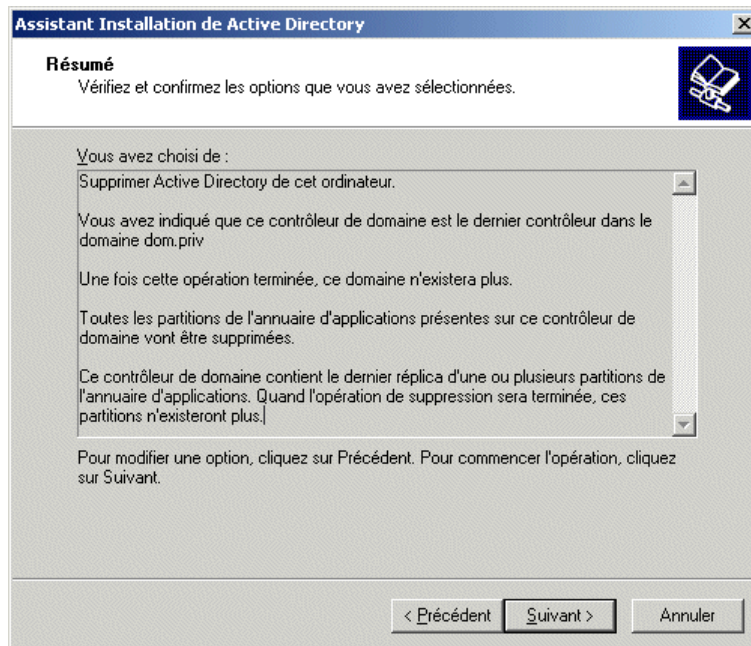


Fig. AD_Desinstaller_06

Vous obtenez le résumé.

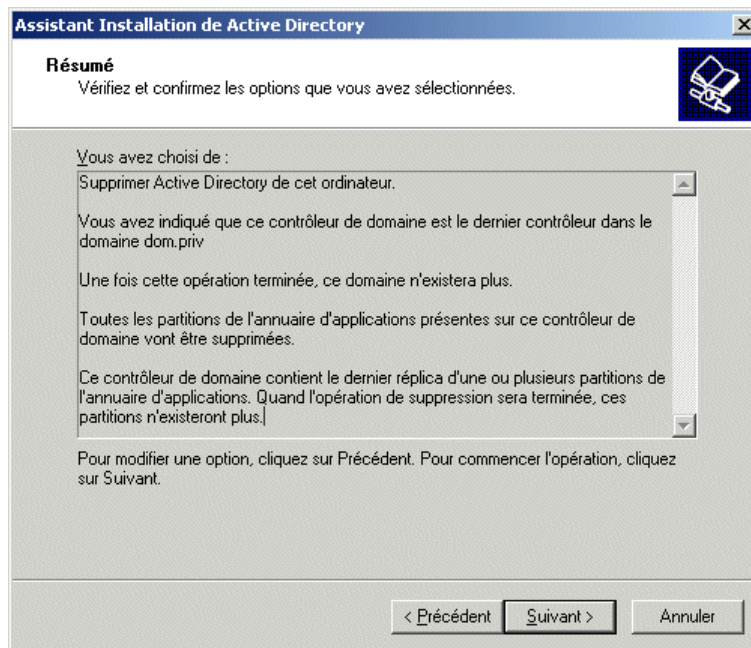


Fig. AD_Desinstaller_07

Choisissez "Suivant". La désinstallation prend un certain temps...
A la fin, vous devez redémarrer l'ordinateur.

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.

Si Active Directory a été désinstallé et si vous désinstallez DNS, votre ordinateur redeviendra dans l'état où il était à la fin de l'installation (donc juste avant l'installation d'Active Directory).

Dans "Gérer votre serveur", "Ajouter ou supprimer un rôle", placez la surbrillance sur "Serveur DNS". Comme il est actuellement à "Oui", en continuant, ce rôle sera supprimé.

Vous pouvez arriver au même résultat en passant par "Démarrer", "Panneau de configuration", "Ajout suppression de programmes" et "Ajouter/Supprimer des composants Windows".

Recherchez "Services de mise en réseau". Dans "Détails", enlevez la coche devant "Système DNS (Domain Name System)".

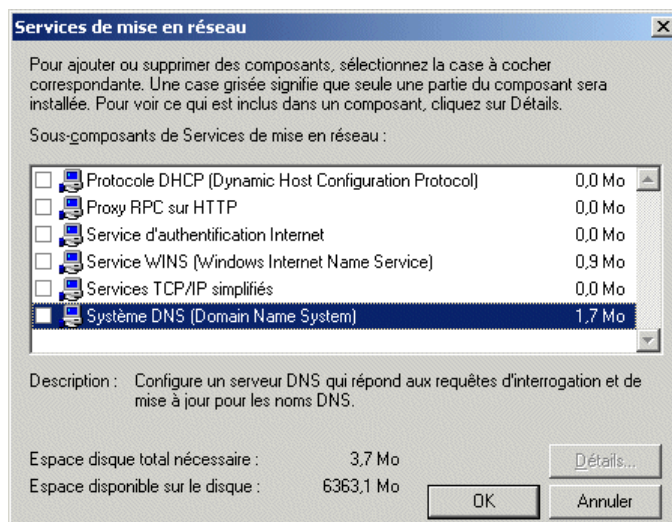


Fig. DNS_Desinstaller_01

Allez dans le répertoire WINDOWS\System32. Vous y trouvez un répertoire DNS qui conserve des traces de votre serveur DNS. Supprimez ce répertoire DNS.

Vous pouvez installer à nouveau Active Directory...

Installer le service DNS

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

Installer

Dans "Gérer votre serveur", "Ajouter ou supprimer un rôle", placez la surbrillance sur "Serveur DNS". Comme il est actuellement à "Non", en continuant, ce rôle sera ajouté.

Vous pouvez arriver au même résultat en passant par "Démarrer", "Panneau de configuration", "Ajout suppression de programmes" et "Ajouter/Supprimer des composants Windows". Recherchez "Services de mise en réseau". Dans "Détails", mettez la coche devant "Système DNS (Domain Name System)".

On obtient alors

DNS

SERVEUR

Zones de recherche directes

Zones de recherche inverses

Se mettre sur "Zones de recherche directes" et créer une nouvelle zone. Donner le nom du domaine géré par Active Directory soit par exemple dom.priv

Dans les propriétés de "dom.priv", dans "Activer les mises à jour automatiques" mettre au choix "Oui"

ou

"Uniquement les mises à jour sécurisées"

Faire "Actualiser".

"dom.priv" doit alors contenir un ensemble de dossiers et un certain nombre de lignes avec entre autre une ligne avec le nom de votre serveur comme hôte et son adresse IP.

Vérifier

Tout ordinateur du réseau qui a dans ses propriétés réseau, l'adresse IP du serveur comme serveur DNS doit être capable d'utiliser serv2003.dom.priv à la place de l'adresse IP du serveur.

On peut par exemple vérifier en tapant dans une fenêtre DOS

tracert serv2003.dom.priv

ou encore dans le navigateur

http://serv2003.dom.priv (à condition que le service Web soit installé et opérationnel sur le serveur).