

# Module 2 : Implémentation d'une structure de forêt et de domaine Active Directory

## Table des matières

Vue d'ensemble	1
Leçon : Création d'une structure de forêt et de domaine	2
Leçon : Analyse du système DNS intégré à Active Directory	23
Leçon : Augmentation des niveaux fonctionnels de la forêt et du domaine	38
Leçon : Création de relations d'approbation	44
Atelier A : Implémentation d'Active Directory	57



Les informations contenues dans ce document, notamment les adresses URL et les références à des sites Web Internet, pourront faire l'objet de modifications sans préavis. Sauf mention contraire, les sociétés, les produits, les noms de domaines, les adresses de messagerie, les logos, les personnes, les lieux et les événements utilisés dans les exemples sont fictifs et toute ressemblance avec des sociétés, produits, noms de domaines, adresses de messagerie, logos, personnes, lieux et événements existants ou ayant existé serait purement fortuite. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Sans limitation des droits d'auteur, aucune partie de ce manuel ne peut être reproduite, stockée ou introduite dans un système d'extraction, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), sans la permission expresse et écrite de Microsoft Corporation.

Les produits mentionnés dans ce document peuvent faire l'objet de brevets, de dépôts de brevets en cours, de marques, de droits d'auteur ou d'autres droits de propriété intellectuelle et industrielle de Microsoft. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2003 Microsoft Corporation. Tous droits réservés.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Active X, MSDN, PowerPoint, Visio, Visual Basic, Visual C++ et Windows Media sont soit des marques de Microsoft Corporation, soit des marques déposées de Microsoft Corporation, aux États-Unis d'Amérique et/ou dans d'autres pays.

Les autres noms de produit et de société mentionnés dans ce document sont des marques de leurs propriétaires respectifs.

## Notes de l'instructeur

**Présentation :**  
120 minutes

**Atelier :**  
60 minutes

Ce module décrit la configuration requise du service d'annuaire Active Directory®, explique comment créer une structure de forêt et de domaine grâce à l'Assistant Installation de Active Directory et présente les tâches que vous devez effectuer après l'installation. Il explique également la manière d'analyser le système DNS (Domain Name System) dans un environnement Active Directory, d'augmenter les niveaux fonctionnels de la forêt et du domaine et de créer des relations d'approbation.

**Objectifs**

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- créer une structure de forêt et de domaine ;
- analyser le système DNS intégré à Active Directory ;
- augmenter le niveau fonctionnel d'une forêt et d'un domaine ;
- créer des relations d'approbation entre des domaines et des forêts.

**Documents de cours**

Pour animer ce module, vous devez disposer des éléments suivants :

- fichier Microsoft® PowerPoint® 2194A\_02.ppt
- fichier Macromedia Flash 2194A\_2279a\_02\_a\_dns.swf

---

**Important** Il est recommandé d'utiliser PowerPoint 2002 ou une version ultérieure pour afficher les diapositives de ce cours. Si vous utilisez la Visionneuse PowerPoint ou une version antérieure de PowerPoint, il se peut que toutes les fonctionnalités des diapositives ne s'affichent pas correctement.

---

**Préparation**

Pour préparer ce module, vous devez effectuer les tâches suivantes :

- lire tous les documents de cours relatifs à ce module, anticiper les questions que les stagiaires sont susceptibles de poser et préparer des réponses appropriées pour chacune de ces questions ;
- réaliser l'atelier ;
- étudier les applications pratiques et les questions d'évaluation ainsi que les suggestions de réponses fournies ; anticiper autant que possible les réponses que les stagiaires sont susceptibles de donner et préparer des réponses appropriées en conséquence ;
- lire le kit de déploiement Windows Server 2003 Deployment Kit (en anglais) et le kit de ressources techniques Windows Server 2003 pour vous familiariser avec les procédures d'installation d'Active Directory et les méthodes conseillées.

## Comment animer ce module

Cette section contient des informations qui ont pour but de vous aider à animer ce module.

---

**Important** Ce module inclut des éléments requis pour chaque leçon, situés sur le CD-ROM du stagiaire. Vous pouvez les présenter en introduction pour aider les stagiaires à identifier les difficultés ou en conclusion pour valider leurs connaissances.

Envisagez de les utiliser pour consolider leurs connaissances à la fin de la journée. Vous pouvez aussi les utiliser en début de journée pour passer en revue les éléments abordés la veille.

---

Laissez 10 minutes aux stagiaires pour préparer leurs réponses aux questions d'évaluation. Vous pouvez choisir de parcourir ensemble les questions et les réponses, ou demander aux stagiaires de préparer les réponses de leur côté.

---

**Remarque** Certaines rubriques font référence à des informations complémentaires situées dans les annexes. Les stagiaires n'ont pas besoin de ces informations pour exécuter les tâches présentées dans ce module. Avant d'animer la classe, passez en revue ces informations dans la page des annexes sur le CD-ROM du stagiaire. Durant la classe, indiquez ces annexes aux stagiaires pour obtenir des informations complémentaires.

---

### Procédures, applications pratiques et ateliers

Expliquez aux stagiaires de quelle manière les procédures, les applications pratiques et les ateliers ont été conçus pour ce cours. Un module comprend au minimum deux leçons. La plupart des leçons comprennent des procédures et une application pratique. Une fois que les stagiaires ont terminé les leçons, le module enchaîne sur un atelier.

#### Procédures

Les procédures vous permettent de montrer comment effectuer une tâche. Les stagiaires n'effectuent pas les tâches en même temps que vous. Ils se servent des étapes décrites pour effectuer l'application pratique à la fin de chaque leçon.

#### Applications pratiques

Après avoir présenté le contenu d'une rubrique et les procédures de la leçon, expliquez qu'une application pratique est une occasion pour les stagiaires d'effectuer les tâches décrites dans la leçon.

## Ateliers

À la fin de chaque module, l'atelier permet aux stagiaires de mettre en pratique toutes les tâches abordées dans l'ensemble du module.

En utilisant des scénarios correspondant à l'environnement professionnel du stagiaire, l'atelier propose des instructions présentées sous forme de deux colonnes. La colonne de gauche indique la tâche à effectuer (par exemple, créer un groupe). La colonne de droite contient des instructions spécifiques pour effectuer la tâche (par exemple : à partir du composant Utilisateurs et ordinateurs Active Directory, double-cliquez sur le nœud du domaine).

Si les stagiaires ont besoin d'instructions détaillées pour mener à bien l'atelier, ils disposent d'un corrigé de chacun des ateliers sur le CD-ROM du stagiaire. Ils peuvent également se reporter aux applications pratiques et aux procédures du module.

## Leçon : Création d'une structure de forêt et de domaine

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Cette leçon apporte aux stagiaires les compétences et connaissances nécessaires pour créer des structures de forêt et de domaine. Elle explique comment s'assurer qu'Active Directory a été installé correctement, et comment identifier et résoudre certains problèmes courants qui peuvent survenir lors d'une installation d'Active Directory.

Dans la rubrique Conditions requises pour installer Active Directory, n'expliquez pas la configuration DNS requise en détail. Les stagiaires ont simplement besoin de comprendre que seuls les serveurs DNS répondant à certaines conditions sont intégrés à Active Directory. L'intégration du système DNS à Active Directory est expliquée dans la leçon Analyse du système DNS intégré à Active Directory.

Utilisez la rubrique Processus d'installation d'Active Directory pour expliquer les modifications apportées à un serveur sur lequel est installé Microsoft Windows Server™ 2003 lorsqu'il est converti en contrôleur de domaine. Utilisez cette rubrique conjointement avec la rubrique suivante Comment créer une structure de forêt et de domaine. Lorsque vous expliquez la procédure à effectuer pour créer la structure de forêt et de domaine Active Directory, faites le point sur les modifications apportées suite à chaque étape, telles qu'elles sont répertoriées dans la rubrique Processus d'installation d'Active Directory.

Assurez-vous que les stagiaires ont bien compris que les contrôleurs de domaine répliqués sont indispensables dans un domaine pour assurer une tolérance de pannes avant de présenter la rubrique Comment ajouter un contrôleur de domaine répliqué.

Windows Server 2003 propose une nouvelle fonctionnalité permettant de renommer un contrôleur de domaine. Lors de la présentation de la rubrique Comment renommer un contrôleur de domaine, assurez-vous que les stagiaires ont bien compris que lorsque vous renommez un contrôleur de domaine et que vous modifiez son suffixe DNS principal, vous n'avez pas déplacé le contrôleur de domaine vers un nouveau domaine Active Directory.

---

**Remarque** Montrez la procédure permettant de renommer un contrôleur de domaine, mais n'effectuez pas la tâche. Si vous décidez toutefois d'effectuer cette tâche, assurez-vous de redonner à l'ordinateur son nom d'origine.

---

Lors de la présentation de la rubrique Comment supprimer un contrôleur de domaine d'Active Directory, commentez les opérations effectuées par l'Assistant Installation de Active Directory lors de la suppression d'Active Directory. Indiquez aux stagiaires que certaines opérations sont communes à tous les contrôleurs de domaine, tandis que d'autres dépendent du type de contrôleur de domaine supprimé. Insistez sur le fait que lorsque l'on supprime un contrôleur de domaine qui exécute un rôle spécialisé (un serveur de catalogue global ou un maître d'opérations, par exemple), vous devez préalablement prendre ou transférer le rôle vers un autre contrôleur de domaine avant de supprimer ce dernier.

---

**Important** Ne supprimez pas Active Directory du contrôleur de domaine London.

---

L'objectif de la rubrique Comment vérifier l'installation d'Active Directory est de présenter aux stagiaires la procédure permettant d'analyser les modifications apportées à un serveur Windows Server 2003 après avoir installé Active Directory. Soulignez que le processus d'installation d'Active Directory modifie également la base de données DNS, et que ces modifications sont décrites dans la leçon Analyse du système DNS intégré à Active Directory de ce module.

Présentez les options de dépannage permettant de résoudre les problèmes susceptibles de survenir lors de l'installation d'Active Directory grâce à la rubrique Comment résoudre les problèmes liés à l'installation d'Active Directory. Présentez les problèmes courants se produisant lors de l'installation d'Active Directory et proposez des stratégies permettant de les résoudre.

### Application pratique

A la fin de la leçon, demandez aux stagiaires de créer un domaine enfant à l'intérieur du domaine nwtraders.msft. Attribuez un nom de domaine enfant corpx à chaque stagiaire, où x est le dernier numéro de l'adresse IP de l'ordinateur du stagiaire. Lorsque les stagiaires ont renseigné la dernière page de l'Assistant Installation de Active Directory, commencez la leçon suivante pendant l'installation d'Active Directory.

## Leçon : Analyse du système DNS intégré à Active Directory

Cette leçon décrit le format des enregistrements de ressources SRV (Service Resource Record), qui sont les enregistrements DNS que les contrôleurs de domaine enregistrent. Elle explique également utiliser les enregistrements SRV pour trouver les fournisseurs de ressources. Lorsque les stagiaires ont bien compris comment le système DNS est intégré à Active Directory, ils sont en mesure de résoudre les problèmes liés au DNS (problèmes d'ouverture de session du client, par exemple).

Dans la rubrique Espaces de noms DNS et Active Directory, décrivez comment le système DNS est intégré à Active Directory. Présentez les fonctions principales que fournit le système DNS dans un réseau qui utilise Active Directory. Expliquez les relations entre l'espace de noms DNS et l'espace de noms Active Directory. Soulignez la manière dont vous pouvez utiliser le système DNS pour trouver les ordinateurs qui exécutent des rôles particuliers dans un domaine Active Directory en intégrant les espaces de noms DNS et Active Directory. Expliquez que le nom d'hôte DNS d'un ordinateur est identique à celui du compte d'ordinateur stocké dans Active Directory.

Avant de présenter la rubrique Définition des zones intégrées à Active Directory, passez brièvement en revue les zones DNS et le modèle de maître unique que fournit le système DNS. Bien que ces connaissances soient une condition préalable pour suivre ce cours, le fait de les réviser aidera les stagiaires à comprendre les avantages de l'utilisation d'un système DNS intégré à Active Directory. Demandez aux stagiaires de se reporter aux annexes pour obtenir des informations relatives à la réplication DNS et aux options de réplication de zone dont ils disposent.

Les rubriques Définition des enregistrements de ressources SRV et Enregistrements SRV enregistrés par les contrôleurs de domaine permettent de s'assurer que les stagiaires sont capables d'identifier les services fournis par un contrôleur de domaine à partir des enregistrements SRV enregistrés dans Active Directory. Ces rubriques apportent les connaissances fondamentales pour que les stagiaires comprennent comment les ordinateurs clients utilisent le système DNS pour trouver les contrôleurs et services de domaine. Ces informations sont présentées dans l'animation intitulée « Comment les ordinateurs clients utilisent le système DNS pour localiser des contrôleurs et services de domaine ». Après avoir visualisé la présentation multimédia, résumez les points clés. Demandez aux stagiaires de se reporter aux annexes pour obtenir des informations relatives au recouvrement de site et à la configuration des valeurs de priorité et de poids dans les enregistrements SRV.

### Application pratique

A la fin de la leçon, demandez aux stagiaires d'analyser les enregistrements SRV enregistrés dans leur contrôleur de domaine.

## Leçon : Augmentation des niveaux fonctionnels de la forêt et du domaine

Cette leçon présente les fonctionnalités activées selon la fonctionnalité de la forêt et du domaine, ainsi que la manière d'augmenter la fonctionnalité d'une forêt et d'un domaine.

Dans la rubrique Définition des fonctionnalités des forêts et des domaines, décrivez certaines fonctionnalités qui sont activées à chaque niveau fonctionnel des forêts et des domaines. Les fonctionnalités répertoriées dans les notes du stagiaire sont incomplètes. Une liste exhaustive de ces fonctionnalités est disponible dans Aide et Support de Windows Server 2003. Les fonctionnalités répertoriées dans le manuel de travail sont expliquées ultérieurement dans ce module ou dans des modules suivants. Ne passez pas trop de temps à expliquer le niveau fonctionnel de Windows Server 2003 version préliminaire. En effet, ce cours ne porte pas sur la migration à partir de Microsoft Windows® NT 4.0.

---

**Important** Assurez-vous que les stagiaires ont bien compris que le niveau fonctionnel d'un domaine ou d'une forêt ne peut plus être diminué après avoir été augmenté.

---

Dans la rubrique Conditions requises pour activer les nouvelles fonctionnalités de Windows Server 2003, assurez-vous que les stagiaires ont bien compris qu'ils doivent augmenter le niveau fonctionnel de chaque domaine avant d'augmenter celui de la forêt.

### Application pratique

A la fin de la leçon, demandez aux stagiaires d'augmenter le niveau fonctionnel du domaine au niveau de Windows Server 2003. Pendant qu'ils effectuent cette application pratique, augmentez les niveaux fonctionnels de nwtraders.msft et corp.nwtraders.msft au niveau de Windows Server 2003.

## Leçon : Création de relations d'approbation

Cette leçon présente les types d'approbations, leur fonctionnement et la méthode de création, de vérification et d'annulation des relations d'approbation.

Dans la rubrique Types d'approbations, expliquez en premier lieu la transitivité de l'approbation. Expliquez ensuite les approbations sortantes, entrantes et bidirectionnelles. Expliquez enfin les différents types d'approbations (raccourcies, de forêt, externes et de domaine [realm]).



Si une forêt n'utilise que les approbations transitives entre les domaines parents et enfants, expliquez qu'il peut être nécessaire de rechercher la ressource dans toute la hiérarchie, en fonction de son emplacement dans la hiérarchie de la forêt. Les approbations raccourcies aident à surmonter ce problème. Lorsque vous expliquez le fonctionnement des approbations au sein d'une forêt, assurez-vous que les stagiaires comprennent bien l'utilité des approbations raccourcies pour réduire le temps nécessaire à la recherche des ressources.

La rubrique Comment fonctionnent les approbations entre les forêts comporte une diapositive animée. Lorsque vous expliquerez le fonctionnement des approbations dans une forêt, soulignez qu'une forêt est une limite de sécurité dans Windows Server 2003. Insistez sur le rôle du protocole d'authentification Kerberos version 5 dans l'authentification de l'utilisateur. Indiquez aux stagiaires les annexes à consulter pour plus d'informations sur le filtrage des identificateurs de sécurité (SID, *Security IDentifier*).

#### **Application pratique**

A la fin de la leçon, demandez aux stagiaires de créer une approbation raccourcie entre leur domaine et un autre domaine dans leur forêt nwtraders.msft. Cette application pratique nécessite de créer des groupes d'au moins deux stagiaires chacun.

## **Atelier A : Implémentation d'Active Directory**

L'atelier de ce module va permettre aux stagiaires d'installer Active Directory et de créer une structure de forêt et de domaine. Ils vont préparer leurs contrôleurs de domaine pour l'installation en supprimant d'Active Directory un domaine enfant préalablement installé. Les stagiaires travailleront par deux. L'un installera le domaine racine de la forêt tandis que l'autre installera un domaine enfant. Les stagiaires vont ensuite augmenter les niveaux fonctionnels de la forêt et du domaine pour préparer la création d'une approbation de forêt. Puis, ils créeront une approbation de forêt.

La configuration de la classe requiert que vous utilisiez le tableau suivant pour attribuer des noms de domaine aux stagiaires.

<b>Nom de l'ordinateur</b>	<b>Domaine racine de la forêt</b>	<b>Domaine enfant</b>
Vancouver	Nwtraders1.msft	
Denver		Corp1.Nwtraders1.msft
Perth	Nwtraders2.msft	
Brisbane		Corp2.Nwtraders2.msft
Lisbon	Nwtraders3.msft	
Bonn		Corp3.Nwtraders3.msft
Lima	Nwtraders4.msft	
Santiago		Corp4.Nwtraders4.msft
Bangalore	Nwtraders5.msft	
Singapore		Corp5.Nwtraders5.msft
Casablanca	Nwtraders6.msft	
Tunis		Corp6.Nwtraders6.msft
Acapulco	Nwtraders7.msft	
Miami		Corp7.Nwtraders7.msft
Auckland	Nwtraders8.msft	
Suva		Corp8.Nwtraders8.msft
Stockholm	Nwtraders9.msft	
Moscow		Corp9.Nwtraders9.msft
Caracas	Nwtraders10.msft	
Montevideo		Corp10.Ntraders10.msft.
Manila	Nwtraders11.msft	
Tokyo		Corp11. Nwtraders11.msft
Khartoum	Nwtraders12.msft	
Nairobi		Corp12. Nwtraders12.msft

---

**Important** Si la réplication ne se produit pas entre un domaine racine de la forêt et un domaine enfant, utilisez Sites et services Active Directory pour vérifier la topologie de la réplication. La vérification de la topologie de la réplication va lancer le KCC, qui, d'une manière générale, résout les problèmes liés à la réplication.

---

## Informations sur la personnalisation

Cette section identifie la configuration requise pour l'atelier de ce module et les changements de configuration qui se produisent sur les ordinateurs des stagiaires lors de cet atelier. Ces informations sont données pour vous aider à dupliquer ou à personnaliser les cours MOC (Microsoft Official Curriculum).

Dans cet atelier, les stagiaires vont créer un contrôleur du domaine racine de la forêt pour un nouveau domaine répertorié dans le tableau ci-dessus. Ils vont installer le système DNS sur ce contrôleur lors de ce processus. Le cas échéant, assurez-vous que les ordinateurs des stagiaires qui sont les contrôleurs du domaine racine de la forêt pointent vers eux-mêmes pour la résolution de noms DNS. Si ce n'est pas le cas, les stagiaires risquent d'avoir des problèmes pour réaliser la répllication.

## Configuration de l'atelier

Les conditions de configuration ci-après s'appliquent à l'atelier de ce module.

**Configuration requise 1** Pour l'atelier de ce module, l'instructeur doit créer une délégation de domaine DNS conformément aux instructions du Guide de configuration manuelle de la classe pour configurer le service DNS sur l'ordinateur London. Si cette étape est omise, les stagiaires ne peuvent pas résoudre les noms hors de leur forêt.

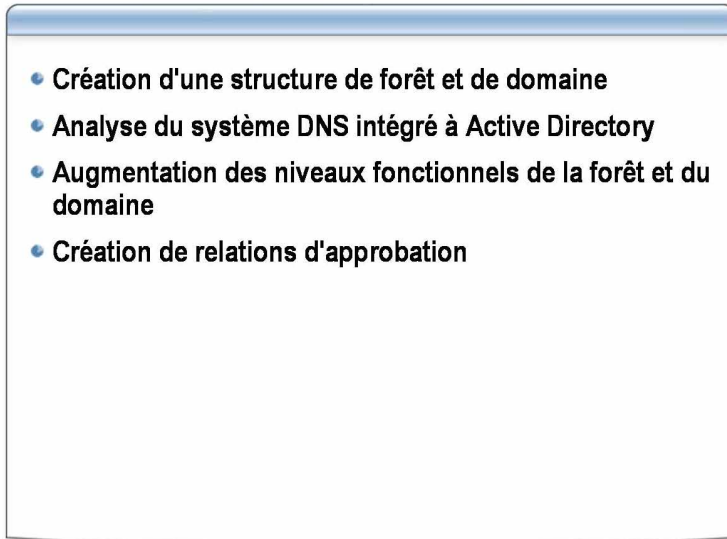
## Résultats de l'atelier

L'exécution de l'atelier de ce module induit les changements de configuration ci-dessous.

- Chaque paire d'ordinateurs stagiaire existera dans une forêt distincte.
- Chaque forêt du stagiaire disposera d'une approbation de forêt bidirectionnelle avec la forêt de la classe, nwtraders.msft.
- Chaque domaine et forêt sera élevé au niveau fonctionnel de Windows Server 2003.



## Vue d'ensemble



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Ce module présente la configuration requise du service d'annuaire Active Directory® et explique comment créer une structure de forêt et de domaine à l'aide de l'Assistant Installation de Active Directory. Il fournit également les connaissances et compétences nécessaires pour analyser le système DNS (Domain Name System) dans un environnement Active Directory, augmenter les niveaux fonctionnels de la forêt et du domaine et créer des relations d'approbation.

### Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- créer une structure de forêt et de domaine ;
- analyser le système DNS intégré à Active Directory ;
- augmenter le niveau fonctionnel d'une forêt et d'un domaine ;
- créer des relations d'approbation entre des domaines.

## Leçon : Création d'une structure de forêt et de domaine

- Conditions requises pour installer Active Directory
- Processus d'installation d'Active Directory
- Comment créer une structure de forêt et de domaine
- Comment ajouter un contrôleur de domaine répliqué
- Comment renommer un contrôleur de domaine
- Comment supprimer un contrôleur de domaine d'Active Directory
- Comment vérifier l'installation d'Active Directory
- Comment résoudre les problèmes liés à l'installation d'Active Directory

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Cette leçon fournit les compétences et connaissances nécessaires pour créer une structure de forêt et de domaine. Vous allez apprendre à vérifier qu'Active Directory a été installé correctement, à identifier et à résoudre les problèmes courants qui peuvent survenir lors de l'installation d'Active Directory.

### Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier les conditions requises pour installer Active Directory ;
- décrire le processus d'installation d'Active Directory ;
- créer une structure de forêt et de domaine ;
- ajouter un contrôleur de domaine répliqué à un domaine ;
- renommer un contrôleur de domaine ;
- supprimer un contrôleur de domaine d'Active Directory ;
- vérifier une installation d'Active Directory ;
- résoudre les problèmes liés à l'installation d'Active Directory ;

## Conditions requises pour installer Active Directory

- Un ordinateur fonctionnant sous Windows Server 2003
- Un espace disque minimum de 250 Mo et une partition formatée NTFS
- Des privilèges administratifs pour la création d'un domaine
- TCP/IP installé et configuré pour utiliser DNS
- Un serveur DNS faisant autorité pour gérer les ressources SRV

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Avant d'installer Active Directory, vous devez vous assurer que l'ordinateur devant être configuré comme contrôleur de domaine satisfait certaines conditions de configuration relatives au matériel et au système d'exploitation. De plus, le contrôleur de domaine doit être en mesure d'accéder à un serveur DNS satisfaisant certaines conditions de configuration pour prendre en charge l'intégration à Active Directory.

### Configuration requise pour les contrôleurs de domaine

La liste ci-dessous identifie la configuration requise pour une installation d'Active Directory.

- Un ordinateur équipé de Microsoft® Windows Server™ 2003 Standard Edition, Enterprise Edition ou Datacenter Edition. Windows Server 2003, Web Edition, ne prend pas en charge Active Directory.
- 250 mégaoctets (Mo) d'espace disque disponible au minimum — 200 Mo pour la base de données Active Directory et 50 Mo pour les fichiers journaux des transactions de la base de données Active Directory. La taille des fichiers journaux et des fichiers de la base de données Active Directory dépend du nombre d'objets dans le domaine et de leur type ; un espace disque supplémentaire est nécessaire si le contrôleur de domaine est également un serveur de catalogue global.
- Une partition ou un volume formaté avec le système de fichiers NTFS. La partition NTFS est nécessaire pour le dossier SYSVOL.
- Les privilèges administratifs nécessaires pour la création, le cas échéant, d'un domaine dans un réseau Windows Server 2003 existant.

- Protocole TCP/IP installé et configuré pour utiliser le système DNS.
- Un serveur DNS qui fait autorité pour le domaine DNS et prend en charge les conditions requises répertoriées dans le tableau ci-dessous.

<b>Condition requise</b>	<b>Description</b>
Enregistrements de ressources SRV (obligatoires)	Les enregistrements de ressources SRV sont des enregistrements DNS qui identifient les ordinateurs qui hébergent des services spécifiques dans un réseau Windows Server 2003. Le serveur DNS qui prend en charge le déploiement d'Active Directory doit également prendre en charge les enregistrements de ressources SRV. Si ce n'est pas le cas, vous devez configurer le système DNS localement lors du processus d'installation d'Active Directory ou le configurer manuellement après l'installation d'Active Directory.
Mises à jour dynamiques (facultatives)	Microsoft recommande vivement de faire en sorte que les serveurs DNS prennent en charge les mises à jour dynamiques. Le protocole de mise à jour dynamique permet aux serveurs et aux clients évoluant dans un environnement DNS d'ajouter et de modifier automatiquement des enregistrements dans la base de données DNS, ce qui permet de réduire les tâches administratives. Si vous utilisez un logiciel DNS qui prend en charge des enregistrements de ressources SRV mais pas le protocole de mise à jour dynamique, vous devez entrer les enregistrements de ressources SRV manuellement dans la base de données DNS.
Transferts de zone incrémentiels (facultatif)	Dans un transfert de zone incrémentiel, les modifications apportées à une zone d'un serveur DNS maître doivent être répliquées sur les serveurs DNS secondaires pour cette zone. Les transferts de zone incrémentiels sont facultatifs. Ils sont toutefois recommandés car ils permettent d'économiser de la bande passante réseau en permettant uniquement aux enregistrements de ressources nouveaux ou modifiés d'être répliqués entre des serveurs DNS, au lieu de répliquer le fichier de base de données de zone entier.

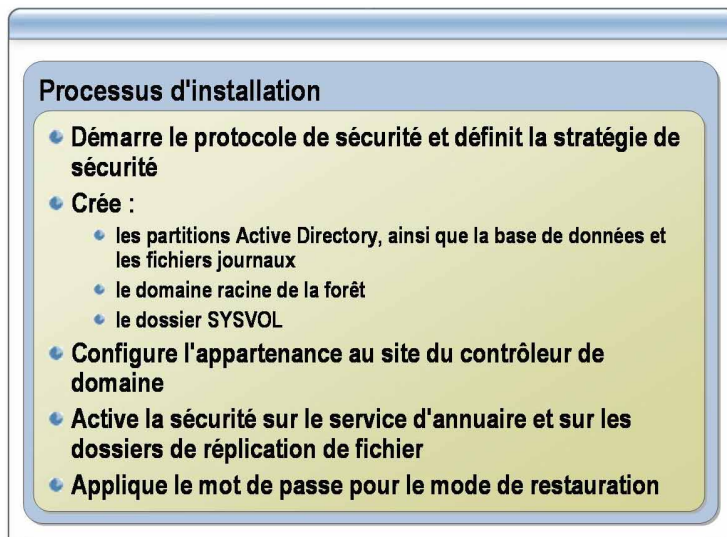
---

**Remarque** Pour plus d'informations sur les enregistrements de ressources SRV, sur les mises à jour dynamiques et les transferts de zone incrémentiels, reportez-vous à la section « Windows 2000 DNS » de la rubrique « Documentation supplémentaire » sur le CD-ROM du stagiaire.

---



## Processus d'installation d'Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Pour démarrer le processus d'installation d'Active Directory, lancez l'Assistant Installation de Active Directory. Lors de l'installation, un certain nombre de modifications sont apportées au serveur Windows Server 2003 sur lequel est installé Active Directory. La connaissance de ces modifications va vous permettre de résoudre les problèmes susceptibles de survenir après l'installation.

### Processus d'installation

Le processus d'installation exécute les tâches suivantes :

- *Démarrage du protocole d'authentification Kerberos version 5*
- *Définition de la stratégie de l'autorité de sécurité locale (LSA, Local Security Authority)*. Le paramètre indique que ce serveur est un contrôleur de domaine.
- *Création de partitions Active Directory*. Une partition de répertoire est une partie de l'espace de noms du répertoire. Chaque partition du répertoire contient une hiérarchie, ou une sous-arborescence, des objets d'annuaire de l'arborescence de répertoire. Lors de l'installation, les partitions ci-dessous sont créées sur le premier contrôleur de domaine d'une forêt :
  - partition d'annuaire de schéma
  - partition d'annuaire de configuration
  - partition d'annuaire de domaine
  - zone DNS de la forêt
  - partition de la zone DNS du domaine

Les partitions sont alors mises à jour par l'intermédiaire de la réplication sur chaque contrôleur de domaine subséquent créé dans la forêt.

---

**Remarque** Pour plus d'informations sur les partitions d'annuaire, reportez-vous au module 7, « Implémentation de sites pour gérer la réplication Active Directory », du cours 2194, *Planification, implémentation et maintenance d'une infrastructure Active Directory Microsoft Windows Server 2003*.

---

- *Création de la base de données Active Directory et des fichiers journaux.* L'emplacement par défaut de la base de données et des fichiers journaux est systemroot\Ntds.

---

**Remarque** Pour améliorer les performances, placez la base de données et les fichiers journaux sur des disques durs distincts. De cette manière, les opérations de lecture et d'écriture réalisées dans la base de données et dans les fichiers journaux n'entrent pas en concurrence pour les ressources en entrée et en sortie.

---

- *Création du domaine racine de la forêt.* Si le serveur est le premier contrôleur de domaine du réseau, le processus d'installation crée le domaine racine de la forêt, puis attribue les rôles de maître d'opérations au contrôleur de domaine, notamment :
  - l'émulateur de contrôleur principal de domaine (PDC, *Primary Domain Controller*)
  - le maître d'opérations des identificateurs relatifs (RID, *Relative Identifier*)
  - le maître de nommage de domaine
  - le contrôleur de schéma
  - le maître d'infrastructure

---

**Remarque** Vous pouvez attribuer les rôles de maître d'opérations à un autre contrôleur de domaine lorsque vous ajoutez des contrôleurs de domaine répliqués au domaine.

---

- *Création du dossier volume système partagé.* Cette structure de dossiers est hébergée sur tous les contrôleurs de domaine Windows Server 2003 et contient les dossiers suivants :
  - le dossier partagé SYSVOL, qui contient des informations relatives à la stratégie de groupe ;
  - le dossier partagé Net Logon, qui contient les scripts de connexion des ordinateurs qui ne sont pas équipés de Windows Server 2003.
- *Configuration de l'appartenance du contrôleur de domaine sur un site approprié.* Si l'adresse IP du serveur que vous souhaitez promouvoir contrôleur de domaine se trouve dans la plage d'adresses d'un sous-réseau donné défini dans Active Directory, l'Assistant configure l'appartenance du contrôleur de domaine dans le site associé au sous-réseau.

Si aucun objet de sous-réseau n'est défini ou si l'adresse IP du serveur ne se trouve pas dans la plage des objets de sous-réseau présents dans Active Directory, le serveur est placé sur le site *Premier-Site-par-Défaut* (premier site configuré automatiquement lorsque vous créez le premier contrôleur de domaine dans une forêt).

L'Assistant Installation de Active Directory crée un *objet serveur* pour le contrôleur de domaine dans le site approprié. L'objet serveur contient les informations nécessaires pour la réplication. Cet objet serveur contient une référence à l'objet ordinateur de l'unité d'organisation Domain Controllers qui représente le contrôleur de domaine en cours de création.

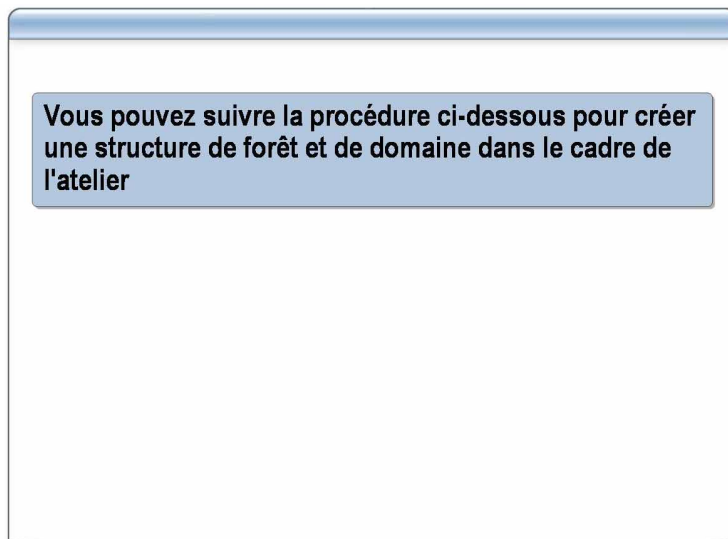
---

**Remarque** Si un objet serveur pour ce domaine existe déjà dans le conteneur Servers du site dans lequel vous ajoutez le contrôleur de domaine, l'Assistant le supprime, puis le crée à nouveau car il suppose que vous réinstallez Active Directory.

---

- *Activation de la sécurité sur le service d'annuaire et sur les dossiers de réplication de fichier.* Ceci vous permet de contrôler l'accès des utilisateurs aux objets Active Directory.
- *Application du mot de passe fourni par l'utilisateur au compte administrateur.* Vous utilisez ce compte pour lancer le contrôleur de domaine en mode Restauration des services d'annuaire.

## Comment créer une structure de forêt et de domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Vous utilisez l'Assistant Installation de Active Directory pour créer une structure de forêt et de domaine. Lorsque vous installez Active Directory dans un réseau pour la première fois, vous devez créer un domaine racine de la forêt. Après avoir créé le domaine racine de la forêt, utilisez l'Assistant pour créer une arborescence et des domaines enfants supplémentaires.

### Procédure de création du domaine racine de la forêt

L'Assistant Installation de Active Directory vous accompagne tout au long du processus d'installation et vous donne des informations, qui diffèrent en fonction des options que vous sélectionnez.

Pour créer un domaine racine de la forêt, procédez comme suit :

1. Cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **dcpromo** en tant que nom du programme.

L'Assistant vérifie les points suivants :

- l'utilisateur actuellement connecté est un membre du groupe local Administrateurs ;
- l'ordinateur est équipé d'un système d'exploitation prenant en charge Active Directory ;
- une installation précédente ou une suppression d'Active Directory n'a pas eu lieu sans un redémarrage de l'ordinateur ; une installation ou une suppression d'Active Directory n'est pas en cours.

Si l'un des ces quatre points ne se vérifie pas, un message d'erreur s'affiche et vous quittez l'Assistant.

2. Dans la page **Assistant Installation de Active Directory**, cliquez sur **Suivant**.

3. Dans la page **Compatibilité du système d'exploitation**, cliquez sur **Suivant**.

---

**Attention** La page Compatibilité du système d'exploitation contient des informations relatives à la compatibilité des systèmes d'exploitation Windows antérieurs. Windows Server 2003 implémente un niveau de sécurité plus élevé que celui de Windows® 2000. Vous devez installer le client Active Directory sous Windows 95 et Microsoft Windows NT® (avec Service Pack 3) afin d'activer l'authentification par un contrôleur de domaine Windows Server 2003.

---

4. Sur la page **Type de contrôleur de domaine**, cliquez sur **Contrôleur de domaine pour un nouveau domaine**, puis cliquez sur **Suivant**.
5. Dans la page **Créer un nouveau domaine**, cliquez sur **Domaine dans une nouvelle forêt**, puis sur **Suivant**.
6. Dans la page **Nouveau nom de domaine**, tapez le nom DNS complet du nouveau domaine, puis cliquez sur **Suivant**.
7. Dans la page **Nom de domaine NetBIOS**, vérifiez le nom NetBIOS, puis cliquez sur **Suivant**.

Le nom NetBIOS permet d'identifier le domaine sur les ordinateurs clients équipés de versions antérieures de Windows et Windows NT. L'Assistant identifie que le nom de domaine NetBIOS est unique. Si ce n'est pas le cas, il vous invite à modifier le nom.
8. Dans la page **Dossiers de la base de données et du journal**, indiquez l'emplacement dans lequel vous souhaitez installer les dossiers de la base de données et du journal, puis cliquez sur **Suivant**.
9. Dans la page **Volume système partagé**, tapez l'emplacement dans lequel vous souhaitez installer le dossier SYSVOL, ou cliquez sur **Parcourir** pour choisir un emplacement. Cliquez ensuite sur **Suivant**.
10. Dans la page **Diagnostics des inscriptions DNS**, assurez-vous qu'un serveur DNS existant va faire autorité pour cette forêt ou, le cas échéant, cliquez sur **Installer et configurer le serveur DNS sur cet ordinateur et définir cet ordinateur pour utiliser ce serveur DNS comme serveur DNS de préférence**. Cliquez ensuite sur **Suivant**.
11. Dans la page **Autorisations**, indiquez si vous souhaitez attribuer les autorisations par défaut à des objets utilisateur et groupe compatibles avec des serveurs équipés de versions antérieures de Windows ou Windows NT, ou seulement avec des serveurs équipés de Windows Server 2003.
12. A l'invite, indiquez le mot de passe pour le mode Restauration des services d'annuaire.

Les contrôleurs de domaine Windows Server 2003 gèrent une petite version de la base de données des comptes de Microsoft Windows NT 4.0. Le seul compte de cette base de données est le compte Administrateur. Il est requis pour l'authentification au démarrage de l'ordinateur en mode Restauration des services d'annuaire, étant donné qu'Active Directory n'est pas démarré dans ce mode.

---

**Remarque** Pour obtenir de plus amples informations relatives à la manière de modifier le mot de passe du mode Restauration des services d'annuaire, reportez-vous à « Ntdsutil : référence de la ligne de commande » dans Aide et Support de Windows Server 2003.

---

13. Passez en revue la page **Résumé**, puis cliquez sur **Suivant** pour commencer l'installation.

14. A l'invite, redémarrez l'ordinateur.

#### Procédure de création d'un domaine enfant

La procédure de création d'un domaine enfant à l'aide de l'Assistant Installation de Active Directory est similaire à celle permettant de créer un domaine racine de la forêt. Le tableau suivant répertorie les étapes que vous allez réaliser lors de l'installation.

#### Page de l'Assistant Installation de Active Directory

#### Nouvelle étape à réaliser

<b>Créer un nouveau domaine</b>	Cliquez sur <b>Domaine enfant dans une arborescence de domaine existante</b> .
<b>Informations d'identification réseau</b>	Tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte d'utilisateur que vous souhaitez utiliser pour cette opération. Le compte d'utilisateur doit être un membre du groupe Administrateurs de l'entreprise.
<b>Installation d'un domaine enfant</b>	Vérifiez le domaine parent, puis tapez le nom du nouveau domaine enfant.

Lorsque vous utilisez l'Assistant Installation de Active Directory pour créer ou supprimer un domaine enfant, il contacte le maître de nommage de domaine pour demander l'ajout ou la suppression. Le maître de nommage de domaine doit impérativement s'assurer que les noms de domaine sont uniques. Si le maître de nommage de domaine est indisponible, vous n'avez pas la possibilité d'ajouter ni de supprimer des domaines.

#### Procédure de création d'une arborescence

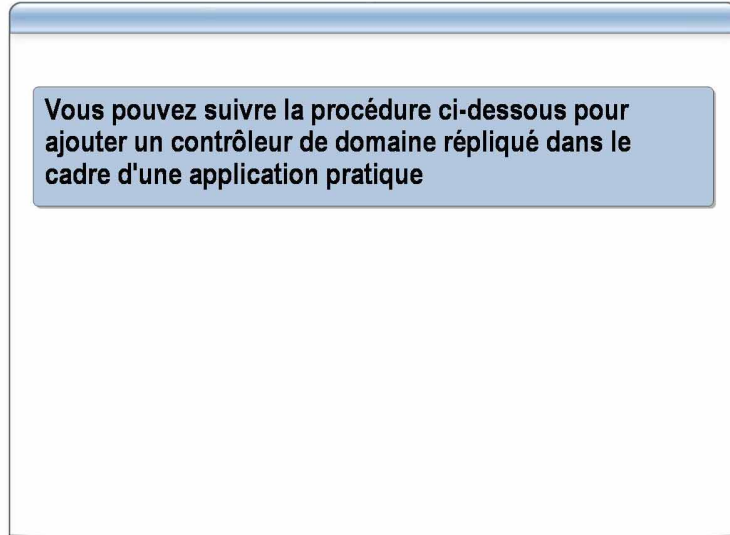
La procédure de création d'une arborescence à l'aide de l'Assistant Installation de Active Directory est similaire à celle permettant de créer un domaine racine de la forêt. Le tableau suivant répertorie les étapes que vous allez réaliser lors de l'installation.

#### Page de l'Assistant Installation de Active Directory

#### Nouvelle étape à réaliser

<b>Créer un nouveau domaine</b>	Cliquez sur <b>Arborescence de domaine dans une forêt existante</b> .
<b>Informations d'identification réseau</b>	Tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte d'utilisateur que vous souhaitez utiliser pour cette opération. Le compte d'utilisateur doit être un membre du groupe Administrateurs de l'entreprise.
<b>Nouvelle arborescence de domaine</b>	Tapez le nom DNS complet du nouveau domaine.

## Comment ajouter un contrôleur de domaine répliqué



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Pour activer la tolérance de pannes au cas où le contrôleur de domaine se déconnecte de manière inattendue, vous devez disposer d'au moins deux contrôleurs de domaine dans un seul domaine. Etant donné que tous les contrôleurs de domaine d'un domaine répliquent les données spécifiques au domaine de l'un vers un autre, l'installation de plusieurs contrôleurs de domaine dans le domaine active automatiquement la tolérance de pannes pour les données enregistrées dans Active Directory. Si un contrôleur de domaine tombe en panne, les contrôleurs de domaine restants fournissent les services d'authentification et assurent l'accès aux objets d'Active Directory, de telle sorte que le domaine, puisse continuer à fonctionner.

### Procédure

Avant de commencer l'installation, déterminez si vous allez effectuer la réplication initiale d'Active Directory par le biais du réseau à partir d'un contrôleur de domaine à proximité ou d'un support sauvegardé.

Choisissez de répliquer Active Directory par le biais du réseau si le contrôleur de domaine répliqué va être installé :

- sur un site sur lequel un autre contrôleur de domaine existe ;
- sur un nouveau site connecté à un site existant par un réseau à grande vitesse.

Choisissez de répliquer Active Directory à partir d'un support de sauvegarde si vous souhaitez installer le premier contrôleur de domaine sur un site distant pour un domaine existant.

Lorsque vous copiez des informations relatives au domaine à partir de fichiers de sauvegarde restaurés, vous devez préalablement sauvegarder les données sur l'état du système d'un contrôleur de domaine exécutant Windows Server 2003 à partir du domaine dans lequel ce serveur membre va devenir un contrôleur de domaine supplémentaire. Ensuite, vous devez restaurer la sauvegarde de l'état du système sur le serveur sur lequel vous installez Active Directory.

**Important** Si un contrôleur de domaine qui a été sauvegardé contient une partition d'annuaire de l'application, cette partition ne sera pas restaurée sur le nouveau contrôleur de domaine. Si le contrôleur de domaine à partir duquel vous avez restauré les données sur l'état du système était un serveur de catalogue global, vous aurez la possibilité de faire de ce nouveau contrôleur de domaine un serveur de catalogue global.

---

Pour installer un contrôleur de domaine répliqué, procédez comme suit :

1. Exécutez **dcpromo**. Pour installer un contrôleur de domaine supplémentaire à partir des fichiers de sauvegarde, exécutez **dcpromo** avec l'option **/adv**.
2. Sur la page **Type de contrôleur de domaine**, cochez la case **Contrôleur de domaine supplémentaire pour un domaine existant**.

Sinon, si vous lancez l'Assistant Installation de Active Directory avec l'option **/adv**, choisissez l'une des options suivantes sur la page **Copie des informations du domaine en cours** :

- **Via le réseau.**
  - **À partir des fichiers de restauration de cette sauvegarde**, puis indiquez l'emplacement des fichiers de sauvegarde restaurés.
3. Sur la page **Informations d'identification réseau**, tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte d'utilisateur que vous souhaitez utiliser pour cette opération.  
Le compte d'utilisateur doit être un membre du groupe Admins du domaine pour le domaine cible.
  4. Dans la page **Contrôleur de domaine supplémentaire**, spécifiez le nom de domaine pour lequel ce serveur deviendra un contrôleur de domaine supplémentaire.
  5. Dans la page **Dossiers de la base de données et du journal**, indiquez l'emplacement dans lequel vous souhaitez installer les dossiers de la base de données et du journal, ou cliquez sur **Parcourir** pour choisir un emplacement.
  6. Dans la page **Volume système partagé**, tapez l'emplacement dans lequel vous souhaitez installer le dossier SYSVOL, ou cliquez sur **Parcourir** pour choisir un emplacement.
  7. Sur la page **Mot de passe administrateur de restauration des services d'annuaire**, tapez et confirmez le mot de passe du mode de restauration des services d'annuaire, puis cliquez sur **Suivant**.
  8. Passez en revue la page **Résumé**, puis cliquez sur **Suivant** pour commencer l'installation.
  9. Lorsque le système vous y invite, redémarrez l'ordinateur.

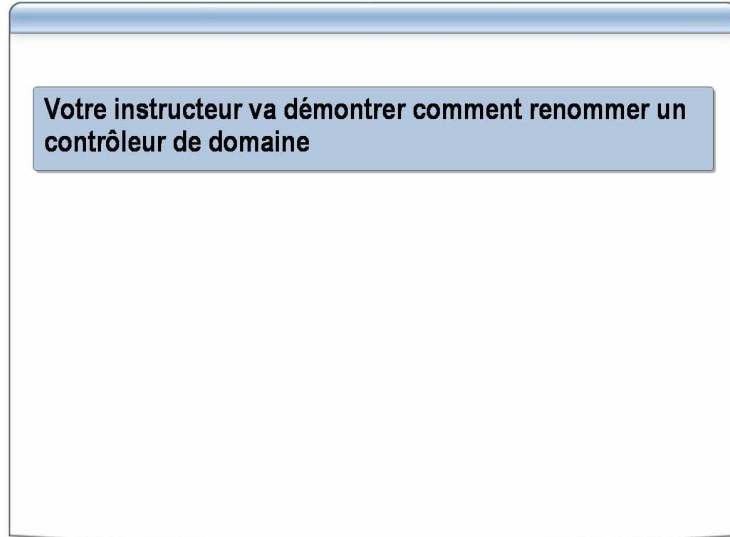
---

**Remarque** Pour plus d'informations sur la sauvegarde et la restauration d'Active Directory, consultez le Module 10, « Maintenance d'Active Directory », du cours 2194, *Planification, implémentation et maintenance d'une infrastructure Active Directory Microsoft Windows Server 2003*.

---



## Comment renommer un contrôleur de domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Dans Windows Server 2003, vous avez la possibilité de renommer un contrôleur de domaine après l'avoir installé. Pour ce faire, vous devez disposer des droits Administrateurs du domaine. Lorsque vous renommez un contrôleur de domaine, vous devez ajouter le nouveau nom du contrôleur de domaine et supprimer l'ancien des bases de données DNS et Active Directory. Vous pouvez renommer un contrôleur de domaine uniquement si le niveau fonctionnel du domaine est défini sur Windows Server 2003.

### Procédure

Pour renommer un contrôleur de domaine, procédez comme suit :

1. Dans le Panneau de configuration, double-cliquez sur l'icône **Système**.
2. Dans la boîte de dialogue **Propriétés Système**, sous l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**.
3. Lorsque vous y êtes invité, confirmez que vous souhaitez renommer le contrôleur de domaine.
4. Entrez le nom complet de l'ordinateur (notamment le suffixe DNS principal), puis cliquez sur **OK**.

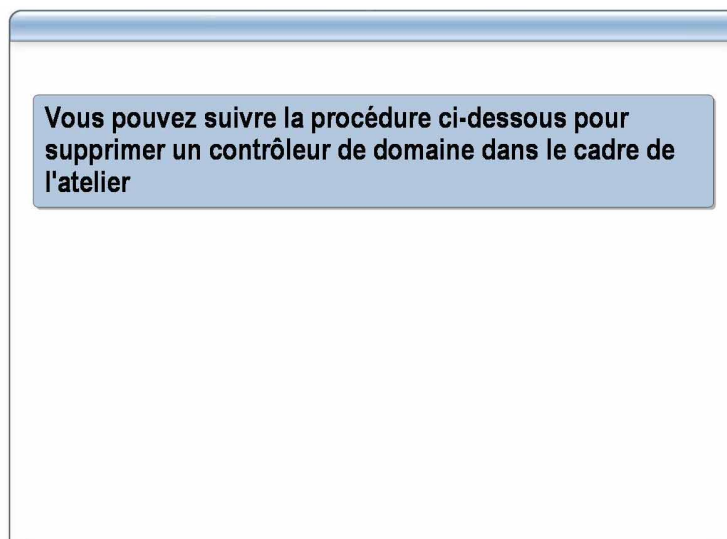
---

**Remarque** Le fait de renommer ce contrôleur de domaine risque de le rendre provisoirement indisponible aux utilisateurs et aux ordinateurs.

---

Lorsque vous renommez un contrôleur de domaine, vous pouvez modifier son suffixe DNS principal. Toutefois, cette modification ne permet pas de déplacer le contrôleur de domaine vers un nouveau domaine Active Directory. Par exemple, si vous renommez le serveur dc2.nwtraders.msft en dc1.contoso.msft, l'ordinateur reste un contrôleur de domaine pour le domaine nwtraders.msft, même si le suffixe DNS principal est contoso.msft. Pour déplacer un contrôleur de domaine vers un autre domaine, vous devez préalablement « rétrograder » le contrôleur de domaine, puis le promouvoir au titre de contrôleur de domaine dans le nouveau domaine.

## Comment supprimer un contrôleur de domaine d'Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Dans Windows Server 2003, vous avez la possibilité de supprimer un contrôleur de domaine qui n'est plus nécessaire ou qui a été endommagé par une catastrophe naturelle. S'il s'agit du dernier contrôleur de domaine, le domaine va être supprimé de la forêt lors du retrait du contrôleur de domaine. Si ce domaine est le dernier de la forêt, le retrait du contrôleur de domaine va supprimer la forêt.

### Procédure de suppression d'un contrôleur de domaine qui est en ligne

Pour supprimer un contrôleur de domaine qui est en ligne et qui n'est plus nécessaire, procédez comme suit :

1. Ouvrez l'Assistant Installation de Active Directory.
2. Dans la page **Supprimer Active Directory**, s'il s'agit du dernier contrôleur de domaine du domaine, cochez la case **Ce serveur est le dernier contrôleur de domaine du domaine**, puis cliquez sur **Suivant**.
3. Dans la page **Mot de passe administrateur**, tapez le nouveau mot de passe administrateur dans les boîtes de dialogue **Nouveau mot de passe administrateur** et **Confirmer le mot de passe**, puis cliquez sur **Suivant**.
4. Dans la page **Résumé**, passez en revue le résumé, puis cliquez sur **Suivant**.

**Procédure de suppression d'un contrôleur de domaine endommagé**

Pour supprimer un contrôleur de domaine endommagé et qui ne peut pas être démarré à partir d'Active Directory, redémarrez le contrôleur de domaine en Mode restauration Active Directory (contrôleurs de domaine Windows), puis exécutez la commande **ntdsutil** à l'aide de l'option de nettoyage des métadonnées. Pour ce faire, procédez comme suit :

1. À l'invite, tapez la commande suivante et appuyez sur ENTRÉE.

```
Ntdsutil.exe: metadata cleanup
```

2. A l'invite Metadata cleanup, tapez la commande suivante et appuyez sur ENTRÉE.

```
metadata cleanup: connections
```

3. A l'invite Server connections, tapez la séquence de commandes suivante pour vous connecter au contrôleur de domaine du domaine qui contient le contrôleur de domaine endommagé :

```
Server connections: Connect to server Nom_Serveur FQDN  
Server connections: quit
```

4. A l'invite Metadata cleanup, sélectionnez la cible des opérations en entrant la commande suivante :

```
metadata cleanup: select operation target
```

5. A l'invite Select operation target, tapez la séquence de commandes suivante afin d'identifier et de sélectionner le contrôleur de domaine endommagé :

```
select operation target: list sites  
select operation target: select site numéro  
select operation target: list servers in site  
select operation target: select server numéro  
select operation target: quit
```

6. A l'invite Metadata cleanup, tapez la commande suivante pour supprimer le contrôleur de domaine endommagé d'Active Directory :

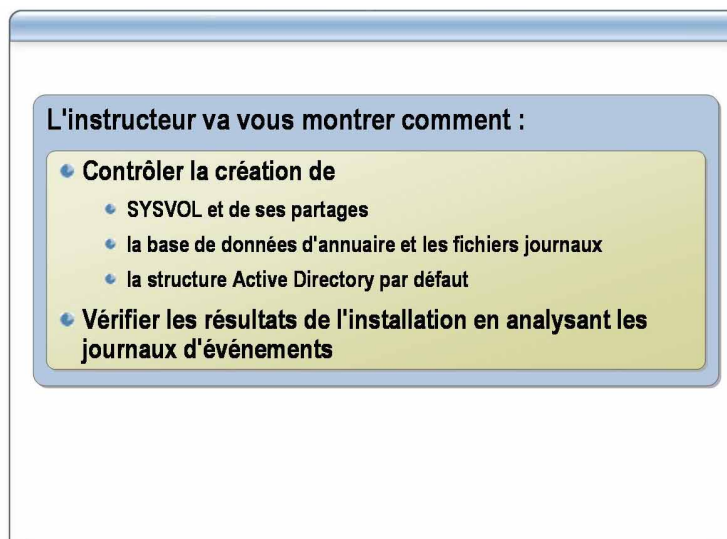
```
metadata cleanup: remove selected server  
metadata cleanup: quit
```

---

**Important** Lorsque vous supprimez un contrôleur de domaine qui est serveur de catalogue global, assurez-vous que les utilisateurs peuvent disposer d'un autre catalogue global avant de supprimer le contrôleur de domaine. De même, si le contrôleur de domaine détient un rôle de maître d'opérations, vous devez transférer ce rôle vers un autre contrôleur de domaine avant de le supprimer. Pour obtenir des informations relatives au transfert d'un rôle de maître d'opérations vers un autre contrôleur de domaine, reportez-vous au Module 9, « Gestion des maîtres d'opérations », du cours 2194, *Planification, implémentation et maintenance d'une infrastructure Active Directory Microsoft Windows Server 2003*.

---

## Comment vérifier l'installation d'Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Le processus d'installation d'Active Directory crée un certain nombre d'objets par défaut dans la base de données Active Directory. Il crée également le dossier système partagé ainsi que la base de données et les fichiers journaux. Vérifiez l'installation d'Active Directory lorsque l'Assistant a terminé l'installation et que le nouveau contrôleur de domaine redémarre.

---

**Remarque** Si vous avez modifié l'emplacement de la base de données et des fichiers journaux de l'annuaire lors de l'installation, remplacez **%systemroot%** par l'emplacement correct. Par exemple, pour la classe, l'emplacement est C:\WINNT.

---

### Vérification de la création de la structure de dossiers SYSVOL et de ses dossiers partagés

Vous devez vérifier que la structure de dossiers SYSVOL et que les dossiers partagés nécessaires ont été créés. Si le dossier SYSVOL n'a pas été créé correctement, les données du dossier SYSVOL (Stratégie de groupe et scripts, par exemple) ne seront pas répliquées entre les contrôleurs de domaine.

Pour vérifier que la structure de dossiers a été créée, exécutez la procédure suivante :

- Cliquez sur **Démarrer**, puis sur **Exécuter**, tapez **%systemroot%\sysvol** et cliquez sur **OK**.

L'Explorateur Windows affiche le contenu du dossier SYSVOL, qui doit contenir les sous dossiers domain, staging, staging areas et sysvol.

Pour vérifier que les dossiers partagés nécessaires ont été créés, exécutez la procédure suivante :

- À l'invite de commande, tapez **net share** et appuyez sur ENTRÉE.

La liste suivante des dossiers partagés doit s'afficher sur l'ordinateur.

Nom du partage	Enregistrements	Remarque
NETLOGON	%systemroot%\SYSVOL\sysvol\domaine\SCRIPTS	Partage de serveur d'accès
SYSVOL	%systemroot%\SYSVOL\sysvol	Partage de serveur d'accès

**Vérification de la création de la base de données et des fichiers journaux d'Active Directory**

Pour vérifier que la base de données et les fichiers journaux d'Active Directory ont été créés, exécutez la procédure suivante :

- Cliquez sur **Démarrer**, sur **Exécuter**, tapez **%systemroot%\ntds** et cliquez sur **OK**.

L'Explorateur Windows affiche le contenu du dossier Ntds, qui doit comporter les fichiers suivants :

- Ntds.dit. Il s'agit du fichier de la base de données de l'annuaire.
- Edb.\*. Il s'agit des fichiers journaux des transactions et de points de vérification.
- Res\*.log. Il s'agit des fichiers journaux réservés.

**Vérification de la création de la structure Active Directory par défaut**

Lors de l'installation d'Active Directory sur le premier contrôleur de domaine d'un nouveau domaine, plusieurs objets par défaut sont créés. Ces objets peuvent être des conteneurs, des utilisateurs, des ordinateurs, des groupes et des unités d'organisation.

Affichez ces objets par défaut à l'aide du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Le tableau suivant présente l'objectif de certains de ces objets par défaut.

<b>Objet</b>	<b>Description</b>
Builtin	Détient les groupes de sécurité intégrés par défaut.
Computers	Emplacement par défaut des comptes d'ordinateurs.
Domain Controllers	Unité d'organisation et emplacement par défaut des comptes d'ordinateurs du contrôleur de domaine.
ForeignSecurityPrincipals	Détient les identifiants de sécurité (SID, <i>Security Identifier</i> ) des domaines externes approuvés.
Users	Emplacement par défaut des comptes d'utilisateurs et de groupes.
LostAndFound	Conteneur par défaut des objets orphelins.
NTDS Quotas	Enregistre les spécifications relatives au quota. Les objets Quota déterminent le nombre d'objets d'annuaire qu'une entité de sécurité peut détenir dans Active Directory.
Program Data	Emplacement de stockage par défaut des données d'application.
System	Enregistre les paramètres système intégrés.

**Analyse des journaux des événements pour voir les erreurs**

Après avoir installé Active Directory, jetez un oeil dans les journaux des événements pour prendre connaissance des éventuelles erreurs qui se sont produites lors du processus d'installation. Les messages d'erreur générés lors de l'installation sont enregistrés dans les journaux Système, Service d'annuaire, Serveur DNS et Service de réplication de fichier.

## Comment résoudre les problèmes liés à l'installation d'Active Directory

Symptôme	Causes éventuelles
Accès refusé lors de la création ou de l'ajout d'un contrôleur de domaine	<ul style="list-style-type: none"> <li>Vous n'avez pas ouvert une session avec un compte du groupe Administrateurs locaux</li> <li>Vos informations d'identification n'appartiennent pas à un compte d'utilisateur membre du groupe Admins du domaine ou Administrateurs de l'entreprise</li> </ul>
Les noms de domaine DNS ou NetBIOS ne sont pas uniques	<ul style="list-style-type: none"> <li>Un autre domaine possède le même nom DNS ou NetBIOS</li> </ul>
Impossible d'accéder au domaine	<ul style="list-style-type: none"> <li>Erreur réseau</li> <li>Erreur DNS</li> </ul>
Espace disque insuffisant	<ul style="list-style-type: none"> <li>L'espace disque disponible est inférieur au minimum requis pour installer Active Directory</li> </ul>

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Lors de l'installation d'Active Directory, vous risquez de rencontrer certains problèmes. Ces problèmes peuvent être le résultat d'informations d'identification de sécurité invalides, de l'utilisation de noms qui ne sont pas uniques, d'un réseau qui n'est pas fiable ou de ressources insuffisantes.

### Problèmes courants liés à l'installation

Le tableau suivant décrit certains problèmes courants que vous êtes susceptible de rencontrer lors de l'installation d'Active Directory, ainsi que les stratégies permettant de les résoudre.

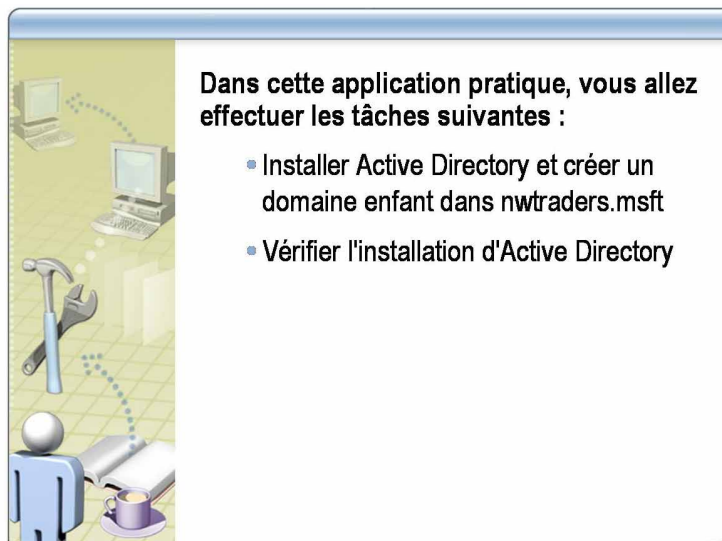
Problème	Solution
Accès refusé lors de l'installation ou de l'ajout de contrôleurs de domaine	<p>Fermez la session, puis ouvrez-la de nouveau à l'aide d'un compte appartenant au groupe Administrateurs local.</p> <p>Fournissez les informations d'identification d'un compte d'utilisateur membre des groupes Admins du domaine et Administrateurs de l'entreprise.</p>
Les noms de domaine DNS ou NetBIOS ne sont pas uniques	<p>Modifiez le nom de sorte qu'il soit unique.</p>

(suite)

Problème	Solution
Le domaine ne peut pas être contacté	<p>Assurez-vous que la connexion réseau est effective entre le serveur que vous souhaitez promouvoir au titre de contrôleur de domaine et au moins l'un des contrôleurs de domaine du domaine. Utilisez la commande ping à partir de l'invite de commande pour tester la connexion avec un contrôleur de domaine du domaine.</p> <p>Vérifiez que le système DNS fournit une résolution de noms à au moins un contrôleur de domaine en vous connectant à un contrôleur de domaine à l'aide de son nom DNS. Pour ce faire, à l'invite de commande, tapez le nom de domaine pleinement qualifié (FQDN, <i>Fully Qualified Domain Name</i>) du contrôleur de domaine. Si le système DNS est configuré correctement, vous pourrez vous connecter au contrôleur de domaine.</p> <p>Vous pouvez également vous assurer que le système DNS a été configuré correctement en vérifiant les enregistrements A que les contrôleurs de domaine enregistrent dans la base de données DNS.</p>
Espace disque insuffisant	Augmentez la taille de la partition ou installez la base de données et les fichiers journaux Active Directory sur des partitions distinctes.



## Application pratique : Création d'un domaine enfant



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

- Objectifs** Dans cette application pratique, vous allez installer Active Directory et créer un domaine enfant dans le domaine racine de la forêt nwtraders.msft. Après l'installation d'Active Directory, vous allez vérifier la création du dossier de volume de système partagé, ainsi que celle de la base de données et des fichiers journaux.
- Scénario** La société Northwind Traders ouvre des bureaux à de nouveaux emplacements. Vous devez créer de nouveaux domaines dans le domaine nwtraders.msft pour chaque nouveau bureau.
- Application pratique**
- **Installer Active Directory et créer le domaine enfant**
1. Connectez-vous en tant que **Nwtraders\Nom\_OrdinateurUser** avec le mot de passe **P@ssw0rd** (où *Nom\_Ordinateur* est le nom de l'ordinateur sur lequel vous travaillez).
  2. Cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Inviter de commandes**, puis cliquez sur **Exécuter en tant que**.
  3. Dans la boîte de dialogue **Exécuter en tant que**, cliquez sur **L'utilisateur suivant**, tapez un nom d'utilisateur **Nwtraders\Administrateur** et le mot de passe **P@ssw0rd**, puis cliquez sur **OK**.
  4. À l'invite de commandes, tapez **depromo** et appuyez sur ENTRÉE.
  5. Dans la page **Assistant Installation de Active Directory**, cliquez sur **Suivant**.
  6. Dans la page **Compatibilité du système d'exploitation**, cliquez sur **Suivant**.
  7. Sur la page **Type de contrôleur de domaine**, cliquez sur **Contrôleur de domaine pour un nouveau domaine**, puis cliquez sur **Suivant**.
  8. Dans la page **Créer un nouveau domaine**, cliquez sur **Domaine enfant dans une arborescence de domaine existante**, puis sur **Suivant**.

9. Dans la page **Informations d'identification réseau**, tapez **Administrateur** comme nom d'utilisateur, **P@ssw0rd** comme mot de passe, assurez-vous que **nwtraders.msft** est le domaine, puis cliquez sur **Suivant**.
10. Sur la page **Installation d'un domaine enfant**, assurez-vous que le domaine parent est nwtraders.msft, tapez le nom de domaine enfant **corp $x$**  où  $x$  est le dernier numéro de votre adresse IP, puis cliquez sur **Suivant**.
11. Dans la page **Nom de domaine NetBIOS**, vérifiez le nom NetBIOS corp $x$ , puis cliquez sur **Suivant**.
12. Dans la page **Dossier de la base de données et du journal**, acceptez la sélection par défaut, puis cliquez sur **Suivant**.
13. Dans la page **Volume système partagé**, acceptez l'emplacement par défaut d'installation du dossier SYSVOL, puis cliquez sur **Suivant**.
14. Dans la page **Diagnostics des inscriptions DNS**, assurez-vous que les paramètres de configuration DNS sont exacts, puis cliquez sur **Suivant**.
15. Dans la page **Autorisations**, cliquez sur **Autorisations compatibles uniquement avec les systèmes d'exploitation Windows 2000 ou Windows Server 2003**, puis cliquez sur **Suivant**.
16. Sur la page **Mot de passe administrateur de restauration des services d'annuaire**, tapez et confirmez le mot de passe **P@ssw0rd** et cliquez sur **Suivant**.
17. Passez en revue la page **Résumé**, cliquez sur **Suivant** pour commencer l'installation, puis sur **Terminer**.
18. Lorsque vous y êtes invité, redémarrez l'ordinateur.

# Leçon : Analyse du système DNS intégré à Active Directory

- Espaces de noms DNS et Active Directory
- Définition des zones intégrées à Active Directory
- Définition des enregistrements de ressources SRV
- Enregistrements SRV enregistrés par les contrôleurs de domaine
- Comment analyser les enregistrements enregistrés par un contrôleur de domaine
- Présentation multimédia : Utilisation de DNS par les ordinateurs clients pour trouver un contrôleur de domaine

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

## Introduction

Windows Server 2003 exige qu'une infrastructure DNS soit en place avant d'installer Active Directory. Il est important de comprendre comment DNS et Active Directory sont intégrés et comment les ordinateurs clients utilisent le système DNS lors de l'ouverture de session afin de résoudre les problèmes liés au système DNS (problèmes d'ouverture de session client, par exemple).

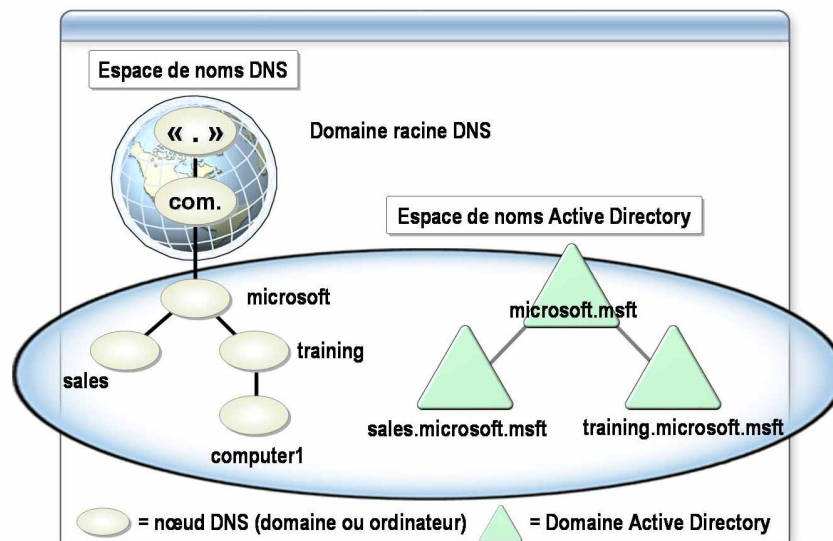
Cette leçon décrit le format des enregistrements de ressources SRV (enregistrements DNS que les contrôleurs de domaine enregistrent) et explique comment Active Directory utilise ces enregistrements pour rechercher les fournisseurs de ressources.

## Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les relations entre les espaces de noms du système DNS et d'Active Directory ;
- expliquer la finalité des zones intégrées à Active Directory ;
- décrire la finalité des enregistrements SRV ;
- décrire les enregistrements SRV enregistrés par les contrôleurs de domaine ;
- analyser les enregistrements DNS enregistrés par un contrôleur de domaine ;
- décrire comment les ordinateurs clients utilisent le système DNS pour rechercher des contrôleurs et des services de domaine.

## Espaces de noms DNS et Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Les domaines DNS et Active Directory utilisent des noms de domaine identiques pour différents espaces de noms. En utilisant des noms de domaine identiques, les ordinateurs d'un réseau Windows Server 2003 peuvent utiliser le système DNS pour rechercher des contrôleurs de domaine et d'autres ordinateurs qui fournissent des services Active Directory.

### Relations entre l'espace de noms DNS et l'espace de noms Active Directory

Les domaines et les ordinateurs sont représentés par des enregistrements de ressources dans l'espace de noms DNS et par des objets Active Directory dans l'espace de noms Active Directory.

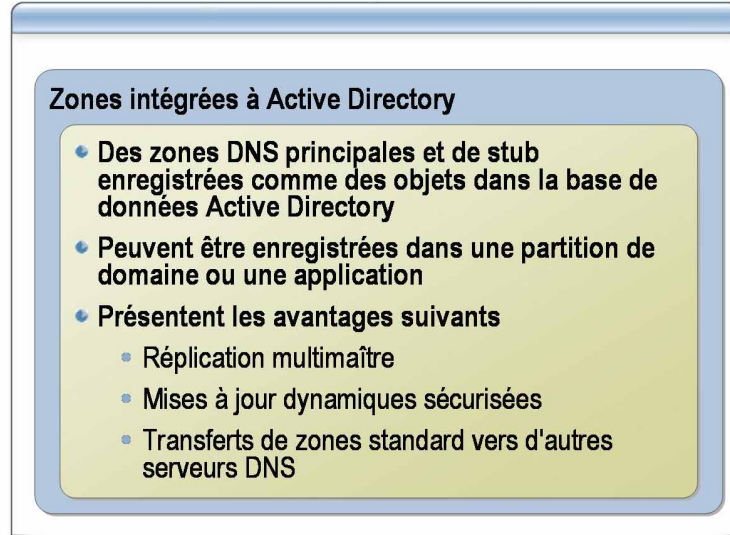
Le nom d'hôte DNS d'un ordinateur est identique à celui du compte d'ordinateur stocké dans Active Directory. Le nom de domaine DNS (également appelé *suffixe DNS principal*) et le domaine Active Directory auquel appartient l'ordinateur ont le même nom. Par exemple, un ordinateur appelé Computer1 appartenant au domaine Active Directory appelé training.microsoft.msft ont le nom FQDN suivant :

computer1.training.microsoft.msft

### Intégration du système DNS et d'Active Directory

L'intégration du système DNS et d'Active Directory est essentielle car un ordinateur client d'un réseau Windows Server 2003 doit pouvoir rechercher un contrôleur de domaine de sorte que les utilisateurs, puissent ouvrir une session sur un domaine ou utiliser les services proposés par Active Directory. Les clients recherchent les contrôleurs de domaine et les services grâce aux *enregistrements de ressources A* et aux *enregistrements SRV*. L'enregistrement de ressources A contient le nom FQDN et l'adresse IP du contrôleur de domaine. L'enregistrement SRV contient le nom FQDN du contrôleur de domaine et le nom du service que fournit le contrôleur de domaine.

## Définition des zones intégrées à Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

L'intégration DNS et Active Directory offre la possibilité d'intégrer des zones DNS dans une base de données Active Directory. Une zone est une partie de l'espace de noms de domaine possédant un groupement logique d'enregistrements de ressources, qui permet de transférer des zones de ces enregistrements pour fonctionner en tant qu'unité unique.

### Zones intégrées à Active Directory

Les serveurs DNS Microsoft stockent des informations utilisées pour résoudre des noms d'hôte en adresses IP, et inversement, dans un fichier de base de données suivi de l'extension .dns pour chaque zone.

*Les zones intégrées à Active Directory* sont des zones DNS principales et de stub stockées en tant qu'objets dans la base de données Active Directory. Vous pouvez stocker des objets de zone dans une partition d'application Active Directory ou dans une partition de domaine Active Directory. Si les objets de zone sont stockés dans une partition d'application Active Directory, seuls les contrôleurs de domaine qui souscrivent à la partition d'application participent à sa réplication. Toutefois, si les objets de zone sont stockés dans une partition de domaine Active Directory, ils sont répliqués sur tous les contrôleurs de domaine du domaine.

**Avantages des zones intégrées à Active Directory**

Les zones intégrées à Active Directory offrent les avantages suivants :

- *Réplication multimaître.* Lorsque vous configurez les zones intégrées à Active Directory, des mises à jour dynamiques du système sur le système DNS sont menées en fonction d'un modèle de mise à jour multimaître. Dans ce modèle, les serveurs DNS qui font autorité (un contrôleur de domaine exécutant un serveur DNS, par exemple) sont conçus en tant que source principale pour la zone. Etant donné que la copie principale de la zone est gérée dans la base de données Active Directory, qui est intégralement répliquée sur tous les contrôleurs de domaine, la zone peut être mise à jour par les serveurs DNS fonctionnant sur un contrôleur de domaine pour le domaine.

Dans le modèle de mise à jour multimaître d'Active Directory, tout serveur principal de la zone intégrée d'annuaire peut traiter des requêtes émises par les clients DNS pour mettre à jour la zone, aussi longtemps qu'un contrôleur de domaine est disponible sur le réseau.

- *Mises à jour dynamiques sécurisées.* Etant donné que les zones DNS sont des objets Active Directory des zones intégrées à Active Directory, vous pouvez définir des autorisations d'accès aux enregistrements au sein de ces zones afin de contrôler les ordinateurs qui peuvent mettre à jour leurs enregistrements. De cette manière, les mises à jour qui utilisent le protocole de mise à jour dynamique ne peuvent provenir que des ordinateurs autorisés.
- *Transferts de zone standard vers d'autres serveurs DNS.* Effectue des transferts de zone standard vers des serveurs DNS qui ne sont pas configurés en tant que contrôleur de domaine. Cela permet également d'effectuer des transferts de zone standard vers des serveurs DNS qui se trouvent dans d'autres domaines. Il s'agit de la méthode requise pour répliquer des zones vers des serveurs DNS dans d'autres domaines.

---

**Remarque** Pour plus d'informations sur les zones intégrées à Active Directory et à la réplication DNS, reportez-vous à la rubrique « Définition des zones intégrées à Active Directory » de la page des annexes du module 2 sur le CD-ROM du stagiaire.

---

## Définition des enregistrements de ressources SRV

- Les enregistrements de ressources SRV sont des enregistrements DNS qui mettent en correspondance un service et l'ordinateur fournissant ce service
- Format des enregistrements SRV  
`_Service._Protocole.Nom Ttl Classe SRV Priorité Poids Port Cible`
- Exemple  
`_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft`

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Pour qu'Active Directory fonctionne correctement, les ordinateurs clients doivent être en mesure de localiser les serveurs qui fournissent des services spécifiques tels que l'authentification des demandes d'ouverture de session et la recherche d'informations dans Active Directory. Active Directory stocke les informations relatives à l'emplacement des ordinateurs qui fournissent ces services dans des enregistrements DNS connus sous le nom d'*enregistrements de ressources SRV*.

### Finalité des enregistrements SRV

Les enregistrements de ressources SRV établissent un lien entre un service et le nom d'ordinateur DNS de l'ordinateur qui offre le service. Par exemple, un enregistrement SRV peut contenir des informations permettant aux clients de localiser un contrôleur de domaine dans un domaine ou une forêt spécifique.

Lorsqu'un contrôleur de domaine démarre, il enregistre les enregistrements SRV et un enregistrement de ressources A, qui contiennent son nom d'ordinateur DNS et son adresse IP. Un ordinateur client DNS utilise ultérieurement ces informations combinées afin de localiser le service requis sur le contrôleur de domaine approprié.

**Format des enregistrements SRV**

Tous les enregistrements SRV utilisent un format standard composé de champs contenant les informations qu'Active Directory utilise afin de mapper un service à l'ordinateur qui fournit le service. Les enregistrements SRV utilisent le format suivant :

*\_Service.\_Protocole.Nom Ttl Classe SRV Priorité Poids Port Cible*

Le tableau ci-dessous présente chaque champ d'un enregistrement SRV.

<b>Champ</b>	<b>Description</b>
<i>_Service</i>	Spécifie le nom du service, (LDAP [Lightweight Directory Access Protocol] ou Kerberos, par exemple) fourni par le serveur qui enregistre cet enregistrement SRV.
<i>_Protocole</i>	Spécifie le type de protocole de transport, tel que TCP ou UDP (User Datagram Protocol).
<i>Nom</i>	Spécifie le nom de domaine auquel fait référence l'enregistrement de ressources.
<i>Ttl</i>	Spécifie la durée de vie (TTL, <i>Time To Live</i> ) en secondes. C'est un champ standard des enregistrements de ressources DNS précisant la durée pendant laquelle l'enregistrement est considéré valide.
<i>Classe</i>	Spécifie la valeur de la classe de l'enregistrement de ressources DNS, qui est presque toujours « IN » pour le système Internet . Il s'agit de la seule classe prise en charge par le système DNS de Windows Server 2003.
<i>Priorité</i>	Spécifie la priorité du serveur. Les clients tentent de contacter l'hôte dont la priorité est la plus faible.
<i>Poids</i>	Indique un mécanisme d'équilibre de charge que les clients utilisent lors de la sélection d'un hôte cible. Lorsque le champ de priorité est identique pour deux ou trois enregistrements d'un même domaine, les clients choisissent de manière aléatoire des enregistrements SRV dont le poids est supérieur.
<i>Port</i>	Spécifie le port sur lequel le serveur écoute ce service.
<i>Cible</i>	Spécifie le nom FQDN, également appelé nom de domaine complet, de l'ordinateur qui fournit le service.

---

**Remarque** Pour plus d'informations sur la priorité et le poids (notamment sur la manière de les configurer), reportez-vous à la rubrique « Définition des enregistrements de ressources SRV » de la page d'annexe du module 2 sur le CD-ROM du stagiaire.

---



**Exemple**

L'exemple suivant illustre un enregistrement SRV d'un ordinateur :

```
_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft
```

L'enregistrement SRV indique que l'ordinateur possède les services ou les caractéristiques suivantes :

- Fournit le service LDAP
- Fournit le service LDAP grâce au protocole de transport TCP
- Enregistre l'enregistrement SRV dans le domaine DNS contoso.msft
- Dispose d'une durée de vie (TTL, *Time To Live*) de 600 secondes ou de 10 minutes
- Possède un nom FQDN de london.contoso.msft

## Enregistrements SRV enregistrés par les contrôleurs de domaine

- Les contrôleurs de domaine fonctionnant sous Windows Server 2003 enregistrent les ressources SRV dans le sous-domaine `_msdcs` au format suivant :  
`_Service._Protocol.DcType._msdcs.Nom_Domaine_Dns`
- Exemples
  - `_ldap.tcp.Nom_Domaine_Dns`
  - `_ldap.tcp.Nom_Site_sites.dc`
  - `_msdcs.Nom_Domaine_Dns`
  - `_gc.tcp.Nom_Forêt_Dns`
  - `_gc.tcp.Nom_Site_sites.Nom_Domaine_Dns`
  - `_kerberos.tcp.Nom_Domaine_Dns`
  - `_kerberos.tcp.Nom_Site`
  - `_sites.Nom_Domaine_Dns`

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Les enregistrements de ressources SRV sont enregistrés par les ordinateurs qui fournissent un service Active Directory. Dans Windows Server 2003, les contrôleurs de domaine et les serveurs de catalogue global enregistrent les services avec le système DNS.

### Comment les services sont enregistrés avec le système DNS

Lorsqu'un contrôleur de domaine démarre, le service Ouverture de session réseau installé sur le contrôleur de domaine utilise les mises à jour dynamiques pour enregistrer les enregistrements de ressources SRV dans la base de données DNS. Les enregistrements de ressources SRV mappent le nom du service que le contrôleur de domaine fournit sur le nom d'ordinateur DNS de ce contrôleur de domaine.

### Services enregistrés avec le système DNS

Pour permettre à un ordinateur de localiser un contrôleur de domaine, les contrôleurs de domaine exécutant Windows Server 2003 enregistrent les enregistrements de ressources SRV en utilisant le format suivant :

`_Service._Protocole.DcType._msdcs.Nom_Domaine_Dns` ou  
`Nom_Forêt_Dns`

Le composant `_msdcs` indique un sous-domaine dans l'espace de noms DNS spécifique à Microsoft, qui permet aux ordinateurs de localiser les contrôleurs de domaine ayant des fonctions dans le domaine ou la forêt de Windows Server 2003.

Les valeurs possibles pour le composant `DcType`, qui est un préfixe du sous-domaine `_msdcs`, spécifie les types de rôles du serveur suivants :

- **dc** pour le contrôleur de domaine
- **gc** pour le serveur de catalogue global

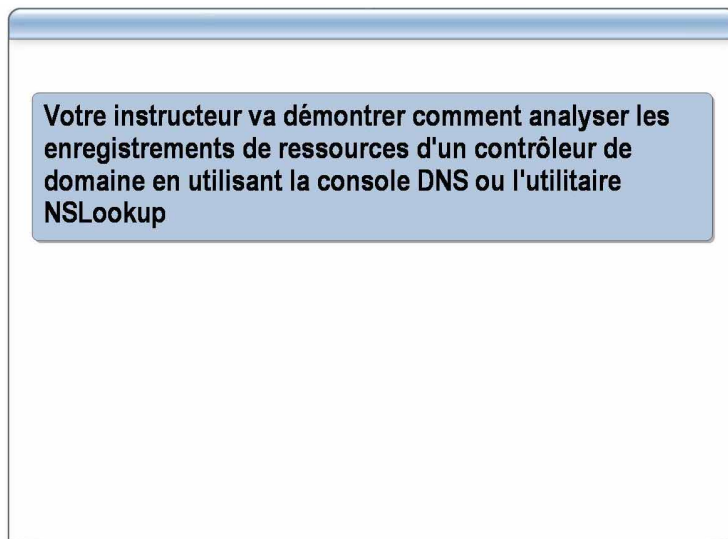
La présence du sous-domaine *\_msdcs* signifie que les contrôleurs de domaine exécutant Windows Server 2003 enregistrent également les enregistrements de ressources SRV suivants :

- \_ldap.\_tcp.dc.\_msdcs.Nom\_Domaine\_Dns*
- \_ldap.\_tcp.Nom\_Site.\_sites.dc.\_msdcs.Nom\_Domaine\_Dns*
- \_ldap.\_tcp.gc.\_msdcs.Nom\_Forêt\_Dns*
- \_ldap.\_tcp.Nom\_Site.\_sites.gc.\_msdcs.Nom\_Forêt\_Dns*
- \_kerberos.\_tcp.dc.\_msdcs.Nom\_Domaine\_Dns*
- \_kerberos.\_tcp.Nom\_Site.\_sites.dc.\_msdcs.Nom\_Domaine\_Dns*

Le tableau suivant répertorie certains enregistrements de ressources SRV enregistrés par les contrôleurs de domaine et définit les critères de recherche pris en charge par chaque enregistrement.

Enregistrement SRV	Permet à un ordinateur de rechercher
<i>_ldap._tcp.Nom_Domaine_Dns</i>	Un serveur LDAP dans le domaine spécifié par <i>Nom_Domaine_Dns</i> .  Tous les contrôleurs de domaine enregistrent cet enregistrement.
<i>_ldap._tcp.Nom_Site._sites.dc._msdcs.Nom_Domaine_Dns</i>	Un contrôleur de domaine dans le domaine spécifié par <i>Nom_Domaine_Dns</i> et dans le site appelé <i>Nom_Site</i> . <i>Nom_Site</i> est le nom unique relatif de l'objet Site qui est enregistré dans Active Directory.  Tous les contrôleurs de domaine enregistrent cet enregistrement.
<i>_gc._tcp.Nom_Forêt_Dns</i>	Un serveur de catalogue global dans la forêt appelée par <i>Nom_Forêt_Dns</i> . <i>Nom_Forêt_Dns</i> est le nom de domaine du domaine racine de la forêt.  Seuls les contrôleurs de domaine configurés en tant que serveurs de catalogue global enregistrent cet enregistrement.
<i>_gc._tcp.Nom_Site._sites.Nom_Forêt_Dns</i>	Un serveur de catalogue global de la forêt appelée <i>Nom_Forêt_Dns</i> et dans le site spécifié par <i>Nom_Site</i> .  Seuls les contrôleurs de domaine configurés en tant que serveurs de catalogue global enregistrent cet enregistrement.
<i>_kerberos._tcp.Nom_Domaine_Dns</i>	Un serveur KDC (Key Distribution Center) pour le domaine spécifié par <i>Nom_Domaine_Dns</i> .  Tous les contrôleurs de domaine exécutant le protocole d'authentification Kerberos version 5 procèdent à cet enregistrement.
<i>_kerberos._tcp.Nom_Site.sites.Nom_Domaine_Dns</i>	Un serveur KDC pour le domaine spécifié par <i>Nom_Domaine_Dns</i> dans le site spécifié par <i>Nom_Site</i> .  Tous les contrôleurs de domaine exécutant le protocole Kerberos version 5 procèdent à cet enregistrement.

## Comment analyser les enregistrements enregistrés par un contrôleur de domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Vous pouvez utiliser la console DNS ou l'utilitaire Nslookup pour afficher les enregistrements de ressources SRV que les contrôleurs de domaine enregistrent.

### Procédure d'affichage des enregistrements SRV grâce à la console DNS

Pour afficher les enregistrements de ressources SRV enregistrés à l'aide de la console DNS, suivez la procédure suivante :

1. Ouvrez DNS à partir du menu **Outils d'administration**.
2. Double cliquez sur *Serveur* (où *Serveur* est le nom de votre serveur DNS), sur **Zones de recherche directes**, puis sur *domaine* (où *domaine* est le nom de domaine).
3. Ouvrez les dossiers suivants dans le dossier *domaine* pour afficher les enregistrements de ressources enregistrés :
  - `_msdcs`
  - `_sites`
  - `_tcp`
  - `_udp`

**Procédure d'affichage des enregistrements SRV grâce à Nslookup**

Pour afficher les enregistrements de ressources SRV enregistrés à l'aide de la commande **Nslookup**, exécutez la procédure suivante :

1. Ouvrez une fenêtre d'invite de commande, puis exécutez l'utilitaire Nslookup.
2. Tapez **ls -t SRV domaine** (où *domaine* est le nom de domaine) et appuyez sur ENTRÉE.

Les enregistrements de ressources SRV enregistrés sont répertoriés.

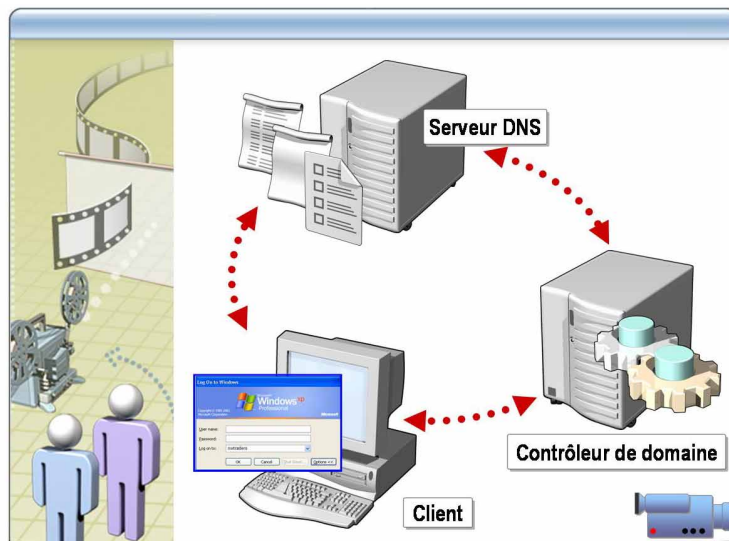
Pour enregistrer les résultats de cette liste dans un fichier, tapez **ls -t SRV domaine > nom\_fichier** (où *nom\_fichier* est le nom que vous attribuez au fichier).

---

**Remarque** Si aucune zone de recherche inversée n'est configurée, Nslookup affiche des erreurs de dépassement de délai lorsque vous exécutez l'utilitaire pour la première fois. En effet, Nslookup génère une recherche inversée afin de déterminer le nom d'hôte du serveur DNS en fonction de son adresse IP. La commande **ls -t** procède à un transfert de zone. Assurez-vous que les transferts de zone sont activés avant d'exécuter la commande.

---

## Présentation multimédia : Utilisation de DNS par les ordinateurs clients pour trouver un contrôleur de domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

**Emplacement de fichier** Pour commencer la présentation *Utilisation de DNS par les ordinateurs clients pour trouver un contrôleur de domaine*, ouvrez la page Web sur le CD-ROM des stagiaires, cliquez sur **Multimédia**, puis sur le titre de la présentation. N'ouvrez pas cette présentation avant d'y être invité par l'instructeur.

**Objectifs** A la fin de cette présentation, vous serez à même d'expliquer comment des ordinateurs clients utilisent le système DNS pour localiser des contrôleurs et des services de domaine.

**Processus d'utilisation du système DNS pour localiser un contrôleur de domaine** La procédure ci-dessous explique comme un client utilise le système DNS pour localiser un contrôleur de domaine :

1. Un service sur l'ordinateur client collecte les informations sur le client et le service requis.
2. Le service client envoie les informations collectées à un serveur DNS sous forme de requête DNS.
3. Le serveur DNS renvoie une liste d'enregistrements SRV pour les contrôleurs de domaine qui fournissent le service requis dans le domaine et le site spécifiés.
4. Le service client parcourt les enregistrements SRV et en sélectionne un en fonction de la priorité et du poids affectés dans l'enregistrement SRV.
5. Le service client envoie une seconde requête DNS pour demander l'adresse IP du contrôleur de domaine spécifique.
6. Le serveur DNS retourne l'enregistrement hôte pour ce contrôleur de domaine, qui contient l'adresse IP du contrôleur de domaine.

7. Le client utilise l'adresse IP pour contacter le contrôleur de domaine et lancer une communication avec le service requis.

Si le client ne parvient pas à contacter le contrôleur de domaine, il sélectionne un autre enregistrement parmi les enregistrements SRV retournés pour trouver un contrôleur de domaine alternatif.

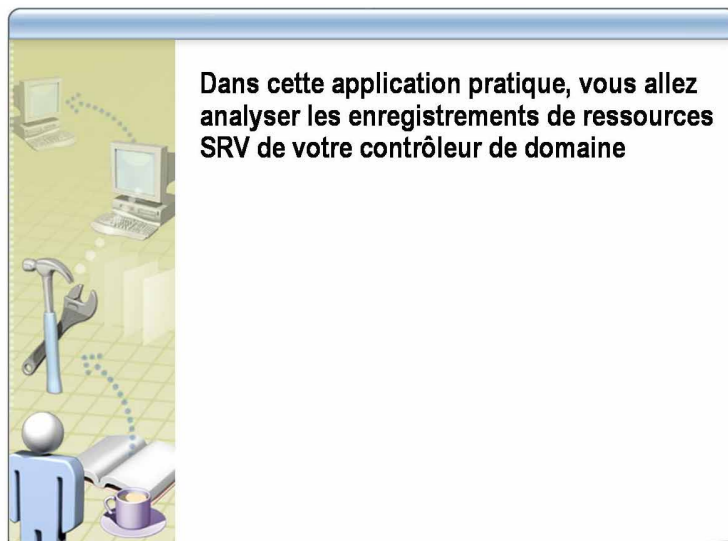
8. Le service client place ensuite en mémoire cache le nom du contrôleur de domaine et les informations relatives aux services qu'il offre. Les requêtes suivantes du client utilisent les informations placées dans la mémoire cache.

---

**Remarque** Pour plus d'informations sur le recouvrement de site, reportez-vous à la rubrique « Comment les ordinateurs clients utilisent le système DNS pour localiser des contrôleurs et services de domaine » de la page d'annexe du module 2 sur le CD-ROM du stagiaire.

---

## Application pratique : Vérification des enregistrements SRV



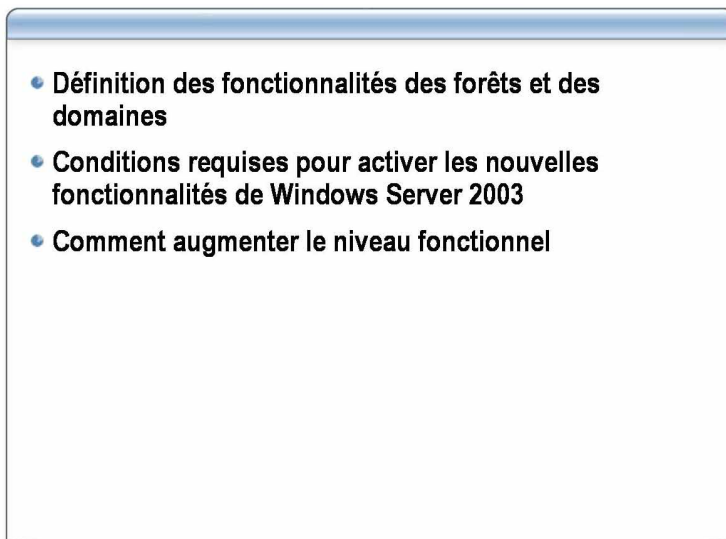
\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

- Objectifs** Dans cette application pratique, vous allez analyser les enregistrements SRV enregistrés par votre contrôleur de domaine à l'aide de la console DNS.
- Scénario** Vous venez de créer un domaine enfant sur votre réseau. Vous souhaitez vérifier que votre contrôleur de domaine a enregistré ses enregistrements de ressources SRV avec Active Directory.
- Application pratique**
- ▶ **Afficher les enregistrements de ressources SRV enregistrés par votre contrôleur de domaine**
1. Ouvrez une session en tant que **Corp\Administrateur** avec le mot de passe **P@ssw0rd**
  2. Cliquez sur **Ne pas afficher cette page lors de l'ouverture de la session**, puis fermez la page **Gérer votre serveur**.
  3. Cliquez sur **Démarrer**, sélectionnez **Outils d'administration**, puis cliquez sur **Stratégie de sécurité du contrôleur de domaine**.
  4. Dans l'arborescence de la console, développez **Stratégies locales**, puis cliquez sur **Attributions des droits utilisateurs**.
  5. Dans le volet de détails, double-cliquez sur **Permettre l'ouverture d'une session locale**.
  6. Dans la boîte de dialogue **Propriétés de Permettre l'ouverture d'une session locale**, cliquez sur **Ajouter un utilisateur ou un groupe**.
  7. Dans la boîte de dialogue **Ajouter un utilisateur ou un groupe**, tapez **Nwtraders\Nom\_OrdinateurUser** (où *Nom\_Ordinateur* est le nom de l'ordinateur sur lequel vous travaillez), puis cliquez sur **OK**.
  8. Dans la boîte de dialogue **Propriétés de Permettre l'ouverture d'une session locale**, cliquez sur **OK**.
  9. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **gpupdate** et cliquez sur **OK**.
  10. Fermez la session, puis ouvrez-la en tant que **Nwtraders\Nom\_OrdinateurUser** avec le mot de passe **P@ssw0rd**.



11. Dans le menu **Outil d'administration**, pointez sur **DNS**, appuyez sur la touche Maj et maintenez-la enfoncée, cliquez avec le bouton droit, puis cliquez sur **Exécuter en tant que**.
12. Dans la boîte de dialogue **Exécuter en tant que**, cliquez sur **L'utilisateur suivant**, tapez un nom d'utilisateur **Nwtraders\Administrateur** et le mot de passe **P@ssw0rd**, puis cliquez sur **OK**.
13. Dans la boîte de dialogue **Connexion au serveur DNS**, cliquez sur **L'ordinateur suivant**, tapez **LONDON** et cliquez sur **OK**.
14. Développez London, développez **Zones de recherche directes**, développez **nwtraders.msft**, puis ouvrez les dossiers suivants dans le dossier corpx pour afficher les enregistrements de ressources SRV qui ont été enregistrés :
  - **\_msdcs**
  - **\_sites**
  - **\_tcp**
  - **\_udp**
15. Fermez la console DNS.

## Leçon : Augmentation des niveaux fonctionnels de la forêt et du domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Les fonctionnalités des forêts et des domaines déterminent quelles sont les fonctionnalités actives d'Active Directory. Cette leçon présente ces fonctionnalités et explique comment augmenter les fonctionnalités des forêts ou des domaines.

### Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les fonctionnalités des forêts et des domaines ;
- décrire les conditions requises pour augmenter les niveaux fonctionnels des forêts et des domaines ;
- augmenter le niveau fonctionnel des forêts et des domaines.

## Définition des fonctionnalités des forêts et des domaines

Environnement réseau	Niveaux fonctionnels du domaine	Niveaux fonctionnels de la forêt
Domaine en mode mixte Windows 2000	✓	
Domaine en mode natif Windows 2000	✓	✓
Domaine Windows Server 2003	✓	✓
Windows Server 2003 version préliminaire	✓	

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Sous Windows Server 2003, les fonctionnalités des forêts et des domaines offrent un moyen d'activer les fonctionnalités Active Directory étendues à l'échelle de la forêt ou du domaine dans votre environnement réseau. Selon votre environnement, différents niveaux de fonctionnalité de forêt et de fonctionnalité de domaine sont disponibles.

### Définition de la fonctionnalité de domaine

La fonctionnalité de domaine active des fonctionnalités qui auront un impact sur le domaine entier, et sur ce domaine uniquement. Quatre niveaux fonctionnels de domaine sont disponibles :

- *Windows 2000 mixte.* Il s'agit du niveau fonctionnel par défaut. Vous pouvez augmenter le niveau fonctionnel du domaine vers Windows 2000 mode natif ou Windows Server 2003. Les domaines en mode mixte peuvent contenir des contrôleurs secondaires de domaine Windows NT 4.0 mais ne peuvent pas utiliser les fonctionnalités de groupes de sécurité universels, d'imbrication de groupes ni d'historique SID (Security Identifier).
- *Windows 2000 natif.* Vous pouvez utiliser ce niveau fonctionnel si le domaine contient uniquement des contrôleurs de domaine Windows 2000 et Windows Server 2003. Bien que les contrôleurs de domaine exécutant Windows 2000 Server ne connaissent pas la fonctionnalité de domaine, les fonctionnalités Active Directory (groupes de sécurité universels, imbrication des groupes et d'historique SID, par exemple) sont disponibles.
- *Windows 2003 Server.* Il s'agit du niveau fonctionnel le plus élevé pour un domaine. Vous pouvez l'utiliser uniquement si tous les contrôleurs de domaine du domaine exécutent Windows Server 2003. Toutes les fonctionnalités Active Directory pour le domaine sont disponibles.
- *Windows 2003 version préliminaire.* Il s'agit d'un niveau fonctionnel particulier qui prend en charge les contrôleurs de domaine Windows NT 4.0 et Windows 2003 Server.

**Définition de la fonctionnalité de forêt**

La fonctionnalité de forêt active les fonctionnalités à travers tous les domaines de votre forêt. Deux niveaux fonctionnels de forêt sont disponibles : Windows 2000 et Windows Server 2003. Par défaut, les forêts opèrent au niveau fonctionnel Windows 2000. Vous pouvez élever le niveau fonctionnel de la forêt vers Windows Server 2003 afin d'activer des fonctionnalités qui ne sont pas disponibles au niveau fonctionnel Windows 2000, notamment :

- Les approbations de forêt
- Une réplification accrue

---

**Remarque** Pour obtenir une liste exhaustive des fonctionnalités activées pour chaque niveau fonctionnel de la forêt ou du domaine, reportez-vous à la rubrique « Fonctionnalité des domaines et des forêts », en ligne, dans Aide et Support.

---

---

**Important** Vous ne pouvez pas réduire le niveau fonctionnel du domaine ou de la forêt après l'avoir augmenté.

---

## Conditions requises pour activer les nouvelles fonctionnalités de Windows Server 2003

Condition requise	Domaine	Forêt
Les contrôleurs de domaine doivent fonctionner sous :	Windows Server 2003	Windows Server 2003
Le niveau fonctionnel du domaine doit être :	Élevé au niveau Windows Server 2003	Capable de passer au niveau Windows Server 2003
Administrateur :	L'administrateur de domaine doit augmenter le niveau fonctionnel du domaine	L'administrateur de l'entreprise doit augmenter le niveau fonctionnel de la forêt

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Outre les fonctionnalités de base d'Active Directory sur les contrôleurs de domaine individuels, de nouvelles fonctionnalités Active Directory étendues à la forêt et au domaine sont disponibles lorsque certaines conditions sont satisfaites.

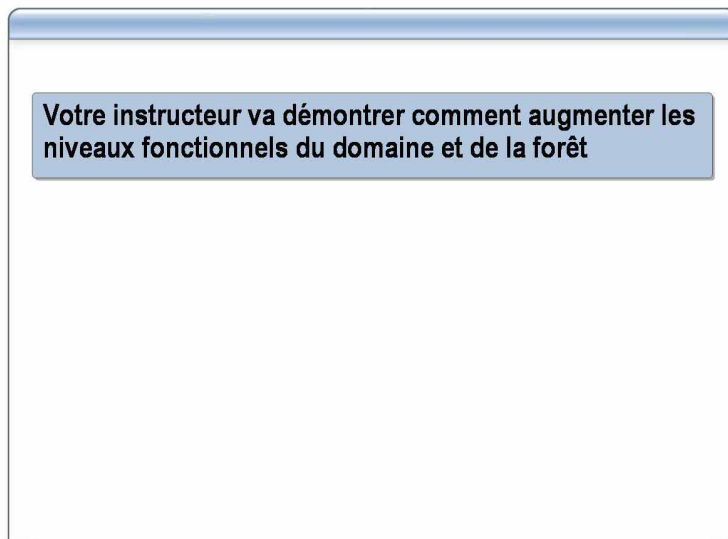
### Conditions requises pour activer de nouvelles fonctionnalités étendues au domaine

Pour activer les nouvelles fonctionnalités étendues au domaine, tous les contrôleurs de domaine du domaine doivent exécuter Windows Server 2003, et le niveau fonctionnel du domaine doit être élevé au niveau Windows Server 2003. Pour ce faire, vous devez être un administrateur de domaine.

### Conditions requises pour activer de nouvelles fonctionnalités étendues à la forêt

Pour activer les nouvelles fonctionnalités étendues à la forêt, tous les contrôleurs de domaine de la forêt doivent exécuter Windows Server 2003, et le niveau fonctionnel de la forêt doit être élevé au niveau Windows Server 2003. Pour ce faire, vous devez être un administrateur d'entreprise.

## Comment augmenter le niveau fonctionnel



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

En augmentant les fonctionnalités de la forêt et du domaine vers Windows Server 2003, vous activez certaines fonctionnalités (approbations de forêt, par exemple) qui ne sont pas disponibles à d'autres niveaux fonctionnels. Vous pouvez augmenter les fonctionnalités de la forêt ou du domaine en utilisant Domaines et approbations Active Directory.

### Procédure d'augmentation du niveau fonctionnel du domaine

Pour augmenter le niveau fonctionnel du domaine, procédez comme suit :

1. Ouvrez Domaines et approbations Active Directory.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur le nœud du domaine dont vous souhaitez augmenter le niveau fonctionnel, puis cliquez sur **Augmenter le niveau fonctionnel du domaine**.
3. Dans la boîte de dialogue **Sélectionner un niveau fonctionnel du domaine disponible**, sélectionnez le niveau fonctionnel, puis cliquez sur **Augmenter**.

### Procédure d'augmentation du niveau fonctionnel de la forêt

Pour augmenter le niveau fonctionnel de la forêt, procédez comme suit :

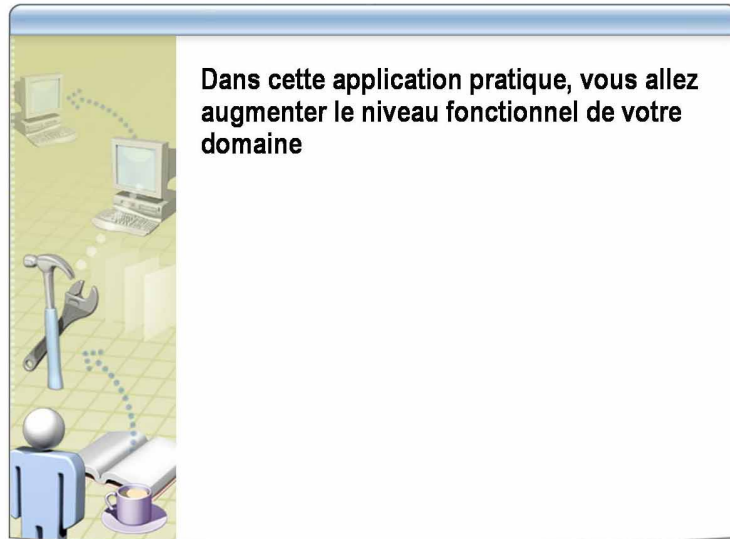
1. Dans Domaines et approbations Active Directory, dans l'arborescence de la console, cliquez avec le bouton droit sur **Domaine et approbations Active Directory**, puis cliquez sur **Augmenter le niveau fonctionnel de la forêt**.
2. Dans la boîte de dialogue **Sélectionner un niveau fonctionnel de la forêt disponible**, sélectionnez **Windows Server 2003**, puis cliquez sur **Augmenter**.

---

**Remarque** Vous devez augmenter le niveau fonctionnel de tous les domaines d'une forêt vers Windows 2000 natif ou supérieur avant de pouvoir augmenter celui de la forêt.

---

## Application pratique : Augmentation du niveau fonctionnel du domaine



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

- Objectifs** Dans cette application pratique, vous allez augmenter le niveau fonctionnel du domaine de Windows 2000 mixte vers Windows Server 2003.
- Scénario** Vous venez de créer un domaine enfant en installant Active Directory sur votre ordinateur Windows Server 2003. Vous allez préparer les approbations entre forêts en augmentant le niveau fonctionnel de votre domaine.
- Application pratique**
- ▶ **Augmenter le niveau fonctionnel de votre contrôleur de domaine de Windows 2000 mixte vers Windows Server 2003**
1. Ouvrez une session en tant que **Nwtraders\Nom\_OrdinateurUser** avec le mot de passe **P@ssw0rd**.
  2. Ouvrez Domaines et approbations Active Directory en tant que **Nwtraders\Administrateur** en utilisant **Exécuter en tant que**.
  3. Analysez le niveau fonctionnel de votre domaine, puis augmentez-le au niveau Windows Server 2003.
  4. Fermez Domaines et approbations Active Directory.

## Leçon : Création de relations d'approbation

- Types d'approbations
- Définition des objets du domaine approuvé
- Comment fonctionnent les approbations dans une forêt
- Comment fonctionnent les approbations entre les forêts
- Comment créer des approbations
- Comment vérifier et révoquer une approbation

\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Active Directory propose une sécurité à travers plusieurs domaines et forêts en utilisant des approbations de domaine et de forêt. Cette leçon explique les types d'approbations, leur fonctionnement et la méthode de création, de vérification et d'annulation des relations d'approbation.

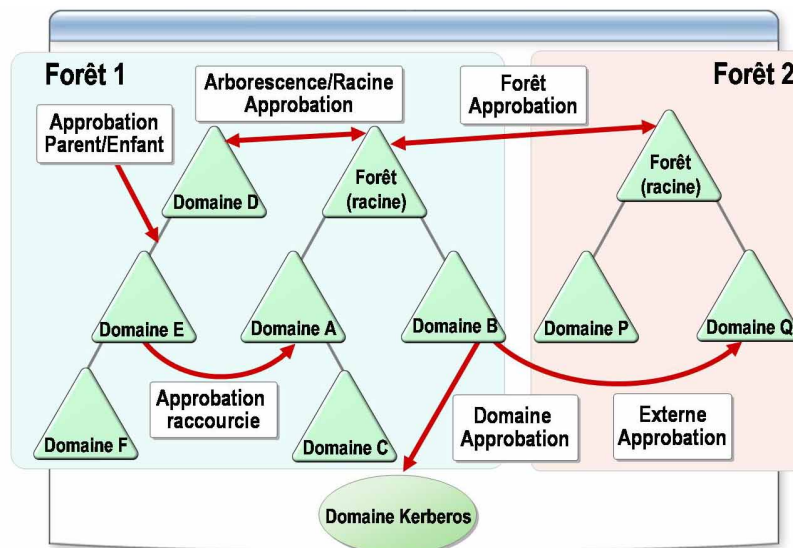
### Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les types d'approbations que vous pouvez établir entre les domaines ;
- expliquer la finalité des objets Domaine approuvé ;
- décrire le fonctionnement des approbations dans une forêt ;
- décrire le fonctionnement des approbations entre les forêts ;
- créer une approbation ;
- vérifier et refuser une approbation.



## Types d'approbations



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Les approbations sont des mécanismes qui permettent à un utilisateur authentifié dans son propre domaine d'accéder aux ressources de tous les domaines approuvés. Dans Windows Server 2003, il existe deux types d'approbations : transitives et non transitives.

### Approbations transitives/non transitives

Dans une approbation transitive, la relation d'approbation étendue à un domaine est automatiquement étendue à tous les autres domaines qui approuvent ce domaine. Par exemple, le domaine D approuve directement le domaine E, qui approuve directement le domaine F. Etant donné que les deux approbations sont transitives, le domaine D approuve indirectement le domaine F et inversement. Les approbations transitives sont automatiques. Une approbation parent/enfant est un bon exemple d'approbation. Les approbations non transitives ne sont pas automatiques et peuvent être configurées. Par exemple, une approbation non transitive peut être externe, comme l'approbation entre deux domaines de deux forêts distinctes.

### Direction de l'approbation

Dans Windows Server 2003, il existe trois directions d'approbation : unidirectionnel entrant, unidirectionnel sortant et bidirectionnelle. Si, dans un domaine B, vous avez configuré une approbation unidirectionnelle entrante entre le domaine B et le domaine Q, les utilisateurs du domaine B peuvent être authentifiés dans le domaine Q. Si vous avez configuré une approbation unidirectionnelle sortante entre le domaine B et le domaine Q, les utilisateurs du domaine Q peuvent être authentifiés dans le domaine B. Dans une approbation bidirectionnelle, les deux domaines peuvent authentifier les utilisateurs de l'autre domaine.

**Types d'approbations**

Windows Server 2003 prend en charge les types d'approbation suivants, dans les catégories transitives et non transitives.

Type	Transitivité	A utiliser si vous souhaitez
Raccourcie	Partiellement transitive	Réduire les sauts de l'authentification Kerberos.
Forêt	Partiellement transitive	Activer l'authentification entre les forêts.
Externe	Non transitive	Configurer une relation d'approbation entre un domaine d'une forêt et un domaine d'une autre forêt.
Domaine	Transitive ou non transitive, au choix de l'utilisateur	Approuver un domaine Kerberos externe.

Le type d'approbation *domaine* (« realm », en anglais) représente un ensemble de principes de sécurité dans un environnement non-Windows faisant l'objet d'une authentification Kerberos.

---

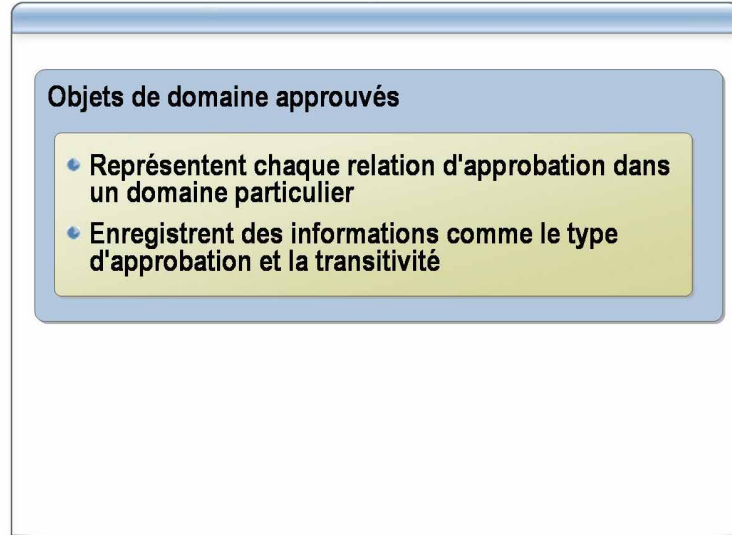
**Remarque** Pour plus d'informations sur les domaines Kerberos, reportez-vous à la rubrique « Interfonctionnement avec les implémentations RFC-1510 Kerberos » en ligne, dans Aide et Support.

---

Les approbations raccourcies sont partiellement transitives car la transitivité de l'approbation est uniquement étendue vers le bas de la hiérarchie à partir du domaine approuvé, et non vers le haut de la hiérarchie. Par exemple, s'il existe une approbation raccourcie entre le domaine E et le domaine A, Active Directory étend l'approbation vers le domaine enfant (le domaine C), mais pas vers le haut de la hiérarchie vers le domaine racine de la forêt. Les utilisateurs du domaine E ne peuvent accéder qu'aux ressources du domaine racine de la forêt par l'intermédiaire de l'approbation parent/enfant avec le domaine D et de l'approbation arborescence/racine que le domaine D entretient avec le domaine racine de la forêt.

Les approbations de forêt ne sont également que partiellement transitives car elles peuvent uniquement être créées entre deux forêts et ne peuvent pas être implicitement étendues à une troisième forêt. Par exemple, si la forêt 1 approuve la forêt 2, et que la forêt 2 approuve la forêt 3, les domaines des forêts 1 et 2 approuvent respectivement de manière transitive les domaines des forêts 2 et 3. Toutefois, la forêt 1 n'approuve pas de manière transitive la forêt 3.

## Définition des objets du domaine approuvé



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Lorsque vous configurez des approbations entre domaines de la même forêt, entre des forêts ou avec un domaine externe, les informations relatives à ces approbations sont stockées dans Active Directory de sorte qu'elles, puissent être extraites au moment voulu.

### Objets du domaine approuvé

Chaque relation d'approbation d'un domaine est représentée par un objet connu sous le nom d'objet Domaine approuvé (TDO, *Trusted Domain Object*). Le TDO stocke des informations relatives à l'approbation, comme sa transitivité ou son type. A chaque création d'une approbation, un TDO est créé et stocké dans le conteneur System du domaine de l'approbation.

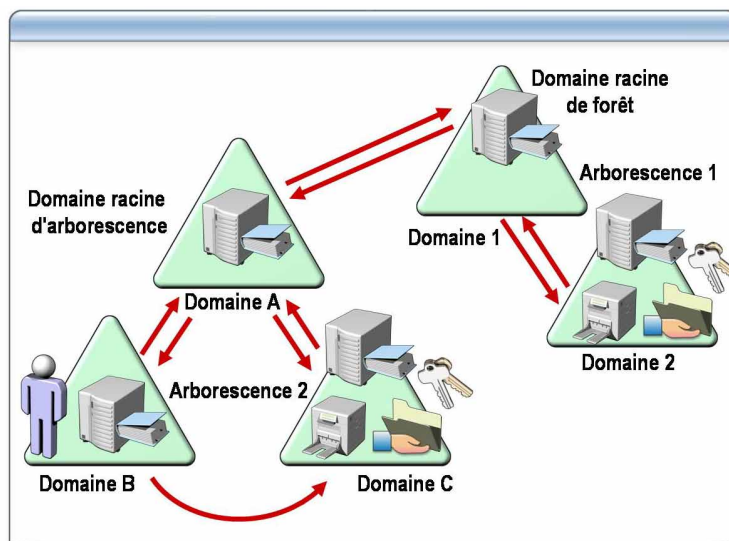
Les TDO d'approbation de forêt stockent des informations supplémentaires permettant d'identifier la totalité des espaces de noms approuvés à partir de la forêt de son partenaire. Lorsque vous créez une approbation de forêt, chaque forêt rassemble tous les espaces de noms approuvés dans la forêt de son partenaire et stocke les informations dans un TDO. Ces informations contiennent :

- les noms d'arborescence de domaine ;
- les suffixes du nom principal du service (SPN, *Service, Principal Name*) ;
- les espaces de noms de l'identificateur de sécurité (SID) ;

Les SPN sont des structures permettant d'identifier l'ordinateur sur lequel est exécuté un service.

Lorsqu'un poste de travail demande un service qui est introuvable dans le domaine ou dans la forêt dont il est membre, les TDO recherchent le service dans toutes les forêts approuvées.

## Comment fonctionnent les approbations dans une forêt



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Les approbations permettent aux utilisateurs d'un domaine d'accéder aux ressources d'un autre domaine. Les relations d'approbation peuvent être transitives ou non transitives.

### Comment les approbations permettent aux utilisateurs d'accéder aux ressources d'une forêt

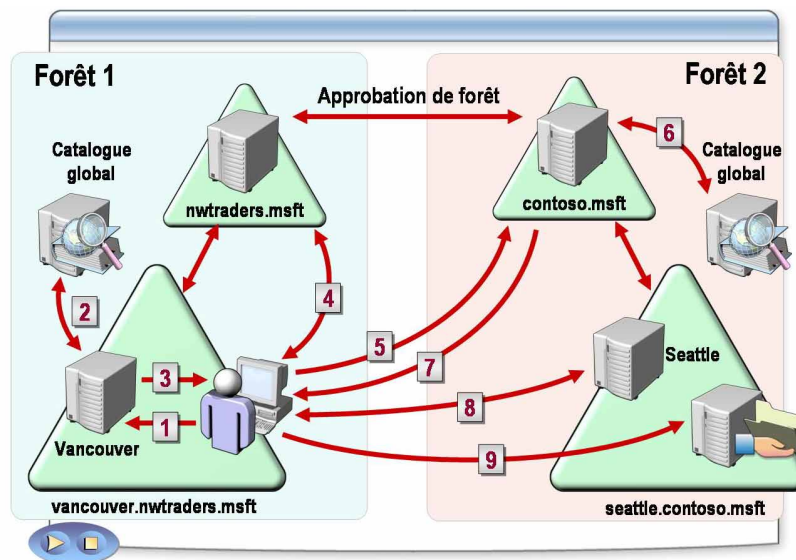
Lorsqu'un utilisateur tente d'accéder à une ressource d'un autre domaine, le protocole d'authentification Kerberos version 5 doit déterminer si le domaine *à approuver* (c'est-à-dire le domaine qui contient la ressource à laquelle tente d'accéder l'utilisateur) possède une relation d'approbation avec le domaine *approuvé* (c'est-à-dire le domaine dans lequel l'utilisateur tente d'ouvrir une session).

Pour déterminer cette relation, le protocole Kerberos version 5 suit le chemin d'approbation en utilisant le TDO afin d'obtenir une référence au contrôleur de domaine du domaine cible. Le contrôleur de domaine cible émet un ticket de service pour le service demandé. Le *chemin d'approbation* est le chemin d'accès le plus court dans la hiérarchie d'approbation.

Lorsqu'un utilisateur du domaine approuvé tente d'accéder aux ressources d'un autre domaine, son ordinateur contacte d'abord le contrôleur de domaine de son domaine afin d'obtenir l'authentification pour la ressource. Si la ressource ne se trouve pas dans le domaine de l'utilisateur, le contrôleur de domaine utilise la relation d'approbation avec son parent et renvoie l'ordinateur de l'utilisateur vers un contrôleur de domaine de son domaine parent.

Cette tentative de localisation de la ressource se poursuit jusqu'au sommet de la hiérarchie, si possible vers le domaine racine de la forêt, et vers le bas de la hiérarchie tant qu'un contact n'est pas établi avec un contrôleur de domaine du domaine dans lequel se trouve la ressource.

## Comment fonctionnent les approbations entre les forêts



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Windows Server 2003 prend en charge les approbations entre forêts, qui permettent aux utilisateurs d'accéder aux ressources d'une autre forêt. Lorsqu'un utilisateur tente d'accéder aux ressources d'une forêt approuvée, Active Directory doit préalablement rechercher les ressources. Une fois que les ressources ont été localisées, l'utilisateur peut être authentifié et autorisé à accéder aux ressources. Si vous comprenez bien le fonctionnement de ce processus, vous serez à même de résoudre les problèmes susceptibles de survenir avec les approbations entre forêts.

### Comment s'effectue l'accès à une ressource

Ci-dessous une description de la manière dont un ordinateur client Windows 2000 Professional ou Windows XP Professional recherche et accède aux ressources d'une autre forêt dotée de serveurs Windows 2000 Server ou Windows Server 2003.

1. Un utilisateur qui a ouvert une session sur le domaine vancouver.nwtraders.msft tente d'accéder à un dossier partagé de la forêt contoso.msft. L'ordinateur de l'utilisateur contacte le KDC d'un contrôleur de domaine de vancouver.nwtraders.msft et demande un ticket de service en utilisant le SPN de l'ordinateur sur lequel résident les ressources. Un SPN peut être le nom DNS d'un hôte ou d'un domaine, ou le nom unique d'un objet point de connexion de service.
2. Les ressources ne sont pas localisées dans vancouver.nwtraders.msft, le contrôleur de domaine de vancouver.nwtraders.msft demande donc au catalogue global de voir si elles se trouvent dans un autre domaine de la forêt.

Etant donné qu'un catalogue global ne contient que des informations relatives à sa propre forêt, il ne trouve pas le SPN. Il recherche alors dans sa base de données les informations relatives à des approbations de forêt qui ont été établies avec sa forêt. S'il en trouve une, il compare les suffixes de noms répertoriés dans le TDO de l'approbation de forêt par rapport au suffixe du SPN cible. S'il trouve une correspondance, le catalogue global fournit les informations de routage relatives à la manière de localiser les ressources au contrôleur de domaine de vancouver.nwtraders.msft.

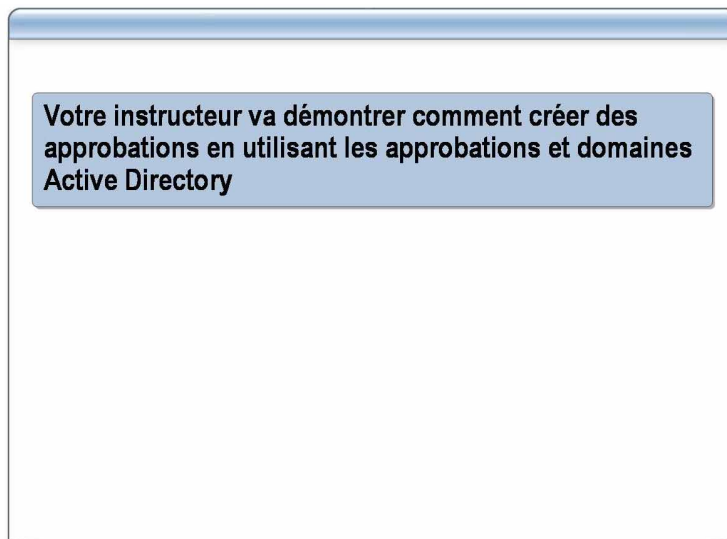
3. Le contrôleur de domaine de vancouver.nwtraders.msft envoie une référence à son domaine parent, nwtraders.msft, à l'ordinateur de l'utilisateur.
4. L'ordinateur de l'utilisateur contacte un contrôleur de domaine de nwtraders.msft pour obtenir une référence à un contrôleur de domaine du domaine racine de la forêt contoso.msft.
5. Grâce à la référence renvoyée par le contrôleur de domaine de nwtraders.msft, l'ordinateur de l'utilisateur contacte un contrôleur de domaine de la forêt contoso.msft pour obtenir un ticket de service pour le service demandé.
6. Les ressources ne se trouvent pas dans le domaine racine de la forêt contoso.msft, le contrôleur de domaine contacte donc son catalogue global pour trouver le SPN. Le catalogue global trouve une correspondance pour le SPN et l'envoie au contrôleur de domaine.
7. Le contrôleur de domaine envoie une référence à seattle.contoso.msft à l'ordinateur de l'utilisateur.
8. L'ordinateur de l'utilisateur contacte le KDC sur le contrôleur de domaine de seattle.contoso.msft et négocie un ticket pour l'utilisateur afin de pouvoir accéder aux ressources du domaine seattle.contoso.msft.
9. L'ordinateur de l'utilisateur envoie le ticket de service à l'ordinateur sur lequel se trouvent les ressources partagées, qui lit les informations d'identification de sécurité et crée un jeton d'accès permettant à l'utilisateur d'accéder aux ressources.

---

**Remarque** Les approbations entre forêts permettent aux utilisateurs d'une forêt d'accéder aux ressources d'une autre forêt. Active Directory protège les approbations entre forêts grâce au filtrage SID. Pour obtenir des informations relatives au filtrage SID, reportez-vous à la rubrique « Comment fonctionnent les approbations entre les forêts » de la page d'annexe du module 2 sur le CD-ROM du stagiaire.

---

## Comment créer des approbations



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Vous pouvez utiliser Domaines et approbations Active Directory pour créer des relations d'approbation entre des forêts ou entre des domaines de la même forêt. Vous pouvez également l'utiliser pour créer des approbations raccourcies.

Avant de créer une relation de forêt, vous devez créer une zone secondaire de recherche inversée sur le serveur DNS dans chaque forêt qui pointe vers le serveur DNS d'une autre forêt. La création de zones secondaires de recherche inversée garantit que le contrôleur de domaine de la forêt dans laquelle vous créez une approbation de forêt est à même de localiser un contrôleur de domaine de l'autre forêt et de définir une relation d'approbation.

### Procédure

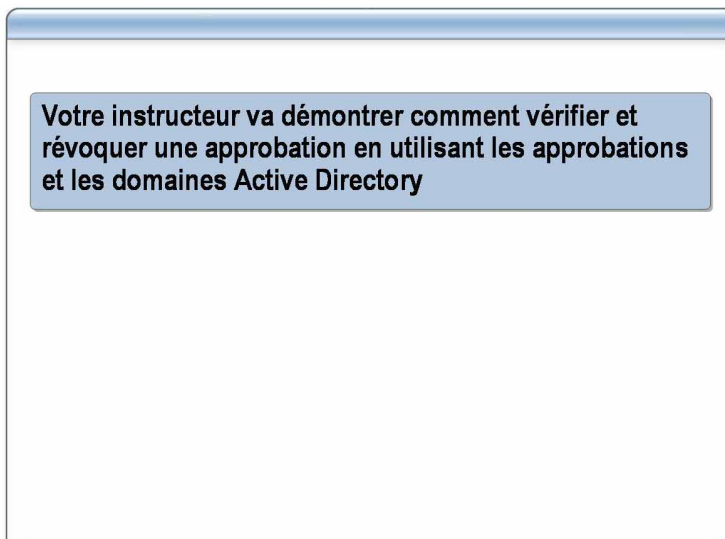
Pour créer une approbation, procédez comme suit :

1. Ouvrez Domaines et approbations Active Directory.
2. Dans l'arborescence de la console, suivez l'une des étapes ci-dessous.
  - Pour créer une approbation de forêt, cliquez avec le bouton droit sur le nœud de domaine du domaine racine de la forêt, puis cliquez sur **Propriétés**.
  - Pour créer une approbation raccourcie, cliquez avec le bouton droit sur le nœud de domaine du domaine avec lequel vous souhaitez établir une approbation raccourcie, puis cliquez sur **Propriétés**.
  - Pour créer une approbation externe, cliquez avec le bouton droit sur le nœud de domaine du domaine avec lequel vous souhaitez établir une approbation, puis cliquez sur **Propriétés**.
  - Pour créer une approbation de domaine, cliquez avec le bouton droit sur le nœud de domaine du domaine que vous souhaitez administrer, puis cliquez sur **Propriétés**.
3. Dans l'onglet **Approbation**, cliquez sur **Nouvelle approbation**, puis sur **Suivant**.
4. Dans la page **d'accueil** de l'Assistant Nouvelle approbation, cliquez sur **Suivant**.

5. Sur la page **Nom d'approbation**, suivez l'une des étapes ci-dessous.
  - Si vous créez une approbation de forêt, tapez le nom DNS de la deuxième forêt, puis cliquez sur **Suivant**.
  - Si vous créez une approbation raccourcie, tapez le nom DNS du domaine, tapez et confirmez le mot de passe de l'approbation, puis cliquez sur **Suivant**.
  - Si vous créez une approbation externe, tapez le nom DNS du domaine, puis cliquez sur **Suivant**.
  - Si vous créez une approbation de domaine, tapez le nom DNS du domaine cible, puis cliquez sur **Suivant**.
6. Sur la page **Type d'approbation**, suivez l'une des étapes suivantes :
  - Si vous créez une approbation de forêt, cliquez sur **Approbation de forêt**, puis sur **Suivant**.
  - Si vous créez une approbation raccourcie, passez à l'étape 7.
  - Si vous créez une approbation externe, cliquez sur **Approbation externe**, puis sur **Suivant**.
  - Si vous créez une approbation de domaine, cliquez sur **Approbation de domaine**, puis sur **Suivant**. Sur la page **Transitivité de l'approbation**, suivez l'une des étapes suivantes :
    - Pour créer une relation d'approbation avec le domaine et le domaine Kerberos spécifié, cliquez sur **Non transitif**, puis sur **Suivant**.
    - Pour créer une relation d'approbation avec le domaine et le domaine Kerberos spécifié, cliquez sur **Transitif**, puis sur **Suivant**.
7. Dans la page **Direction de l'approbation**, suivez l'une des étapes ci-dessous.
  - Pour créer une approbation bidirectionnelle, cliquez sur **Bidirectionnel**, puis suivez les instructions de l'Assistant.
  - Pour créer une approbation unidirectionnelle entrante, cliquez sur **Sens unique : en entrée**, puis suivez les instructions de l'Assistant.
  - Pour créer une approbation unidirectionnelle sortante, cliquez sur **Sens unique : en sortie**, puis suivez les instructions de l'Assistant.



## Comment vérifier et révoquer une approbation



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Introduction

Lorsque vous créez des approbations non transitives, vous devez parfois vérifier et révoquer les chemins d'approbation que vous avez créés. Vous vérifiez une approbation afin de vous assurer qu'elle peut valider les demandes d'authentification provenant d'autres domaines. Vous révoquez une approbation pour éviter que le chemin d'authentification ne soit utilisé lors d'une authentification. Vous pouvez utiliser Domaines et approbations Active Directory ou la commande **netdom** pour vérifier et révoquer les chemins d'approbation.

### Procédure de vérification des approbations

Pour vérifier une approbation à l'aide de Domaines et approbations Active Directory, exécutez la procédure suivante :

1. Dans Domaines et approbations Active Directory, dans l'arborescence de la console, cliquez avec le bouton droit sur l'un des domaines de l'approbation que vous souhaitez vérifier, puis cliquez sur **Propriétés**.
2. Dans l'onglet **Approbations**, sous **Domaines approuvés par ce domaine (approbations sortantes)** ou **Domaine qui approuvent ce domaine (approbations entrantes)**, cliquez sur l'approbation que vous souhaitez vérifier, puis sur **Propriétés**.
3. Cliquez sur **Valider**, puis sur **Non, ne pas valider l'approbation entrante**.
4. Reprenez les étapes 1 à 3 afin de vérifier l'approbation de l'autre domaine de la relation.

Pour vérifier une approbation à l'aide de la commande **netdom**, conformez-vous à l'étape ci-dessous :

- A l'invite, tapez la commande suivante et appuyez sur ENTRÉE.

```
NETDOM TRUST nom_domaine_à_approuver
/Domain:nom_domaine_approuvé /Verify
```

### Procédure de révocation des approbations

Pour révoquer une approbation à l'aide de Domaines et approbations Active Directory, exécutez la procédure suivante :

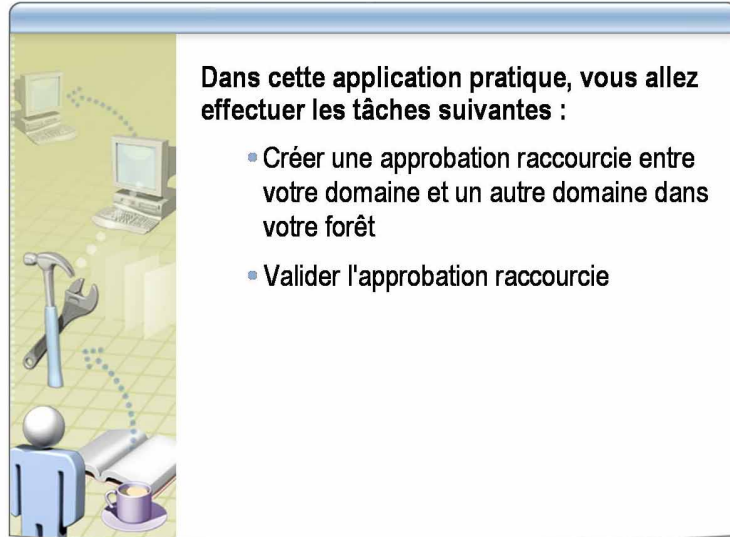
1. Dans Domaines et approbations Active Directory, dans l'arborescence de la console, cliquez avec le bouton droit sur l'un des domaines de l'approbation que vous souhaitez refuser, puis cliquez sur **Propriétés**.
2. Dans l'onglet **Approbations**, sous **Domaines approuvés par ce domaine (approbations sortantes)** ou **Domaine qui approuvent ce domaine (approbations entrantes)**, cliquez sur l'approbation que vous souhaitez refuser, puis sur **Supprimer**.
3. Reprenez les étapes 1 et 2 afin de révoquer l'approbation de l'autre domaine de la relation d'approbation.

Pour révoquer une approbation à l'aide de la commande **netdom**, conformez-vous à l'étape ci-dessous :

- A l'invite, tapez la commande suivante et appuyez sur ENTRÉE.

```
NETDOM TRUST nom_domaine_à_approuver  
/Domain:nom_domaine_approuvé /Remove
```

## Application pratique : Création d'une approbation raccourcie



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

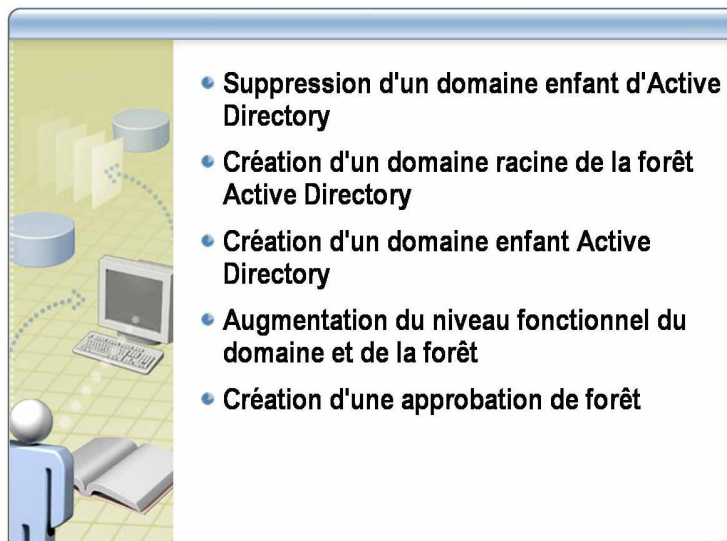
<b>Objectifs</b>	Dans cette application pratique, vous allez créer et valider une approbation raccourcie entre votre domaine et un autre domaine de votre forêt.
<b>Scénario</b>	Vous avez créé un domaine enfant dans la forêt nwtraders.msft. Les responsables des ventes d'un autre domaine doivent accéder aux ressources commerciales de votre domaine, et inversement. Vous devez définir une approbation raccourcie bidirectionnelle entre les domaines.
<b>Instructions</b>	Vous allez travailler avec un partenaire que va vous attribuer votre instructeur. Vous allez créer l'approbation raccourcie entre votre domaine et celui de votre partenaire.
<b>Application pratique : Création de l'approbation raccourcie</b>	<p>► <b>Créer l'approbation raccourcie</b></p> <ol style="list-style-type: none"> <li>1. Ouvrez une session en tant que <b>Nwtraders\Nom_OrdinateurUser</b> avec le mot de passe <b>P@ssw0rd</b></li> <li>2. Ouvrez Domaines et approbations Active Directory en tant que <b>Nwtraders\Administrateur</b> en utilisant <b>Exécuter en tant que</b>.</li> <li>3. Créez une approbation bidirectionnelle vers le domaine de votre partenaire. Utilisez le mot de passe <b>P@ssw0rd</b> de l'approbation et acceptez les sélections par défaut.</li> </ol>

**Application pratique :  
Validation de  
l'approbation raccourcie**

► **Valider l'approbation raccourcie**

1. Dans l'onglet **Approbation** de la page **Propriétés**, cliquez sur l'approbation que vous avez créée avec le domaine de votre partenaire, puis cliquez sur **Propriétés**.
2. Sur la page **Propriétés**, cliquez sur **Valider**.
3. Cliquez sur **Non, ne pas valider l'approbation entrante**, puis sur **OK**.  
Si l'approbation est valide, un message de validation s'affiche. Si vous procédez à un test de validation avant que votre partenaire ait défini une approbation raccourcie bidirectionnelle avec votre domaine, vous allez recevoir un message.
4. Fermez toutes les boîtes de dialogue, puis fermez Domaines et approbations Active Directory.

## Atelier A : Implémentation d'Active Directory



\*\*\*\*\*DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR\*\*\*\*\*

### Objectifs

À la fin de cet atelier, vous serez à même d'effectuer les tâches suivantes :

- supprimer un domaine enfant d'Active Directory ;
- créer un domaine racine de la forêt ;
- vérifier les niveaux fonctionnels de la forêt et du domaine ;
- augmenter le niveau fonctionnel d'un domaine et d'une forêt ;
- créer un domaine enfant dans une forêt existante ;
- créer et vérifier des approbations de forêt.

### Connaissances préalables

Avant de commencer cet atelier, vous devez avoir :

- des connaissances relatives aux composants qui constituent la structure logique et physique d'Active Directory ;
- des connaissances relatives au fonctionnement des zones intégrées à Active Directory et au système DNS ;
- des connaissances relatives aux niveaux fonctionnels de la forêt ;
- des connaissances relatives aux approbations de forêt.

### Scénario

Vous êtes un ingénieur système de la société Northwind Traders. Suite à une série de fusions avec plusieurs sociétés de plus petite taille, Northwind Traders a décidé de consolider son infrastructure Active Directory. Les organisations individuelles doivent gérer leur structure Active Directory, et être cependant en mesure de communiquer avec toutes les filiales. Vous allez fournir l'infrastructure nécessaire à la prise en charge de ces objectifs grâce à plusieurs forêts et approbations, le cas échéant, entre elles.

**Durée approximative de cet atelier :**  
60 minutes

## Exercice 1

### Suppression d'un domaine enfant d'Active Directory

Dans cet exercice, vous allez supprimer Active Directory de votre contrôleur de domaine afin de préparer la création d'une structure de forêt et de domaine Active Directory.

#### Scénario

Northwind Traders doit implémenter Active Directory à différents emplacements. L'équipe de gestion informatique (IT) a demandé aux ingénieurs d'implémenter Active Directory en utilisant des forêts séparées. Vous allez travailler de manière indépendante en tant qu'administrateur local du bureau auquel vous avez été affecté. Vous allez créer un domaine racine de la forêt et un domaine enfant Active Directory grâce aux serveurs présents sur votre site. Mais en premier lieu, vous devez rétrograder votre contrôleur de domaine.

Tâches	Instructions spécifiques
1. Supprimer Active Directory de votre contrôleur de domaine.	<ol style="list-style-type: none"><li>Ouvrez une session en tant que <b>Nwtraders\Nom_OrdinateurUser</b>.</li><li>Utilisez <b>Exécuter en tant que</b> pour lancer une invite de commande et exécutez <b>depromo</b> en tant que Nwtraders\Administrateur.</li></ol>
2. Vérifier qu'Active Directory a été supprimé de votre serveur.	<ol style="list-style-type: none"><li>Ouvrez une session en tant qu'<b>Administrateur</b> avec le mot de passe <b>P@ssw0rd</b>.</li><li>Vérifiez que les partages NETLOGON et SYSVOL n'existent plus.</li></ol>

## Exercice 2

### Création d'un domaine racine de la forêt Active Directory


Dans cet exercice, vous allez travailler avec un partenaire afin de créer votre forêt Active Directory. L'un de vous deux va créer le domaine racine de la forêt et l'autre un domaine enfant.

#### Scénario

Vous créez une forêt Active Directory qui va éventuellement être fusionnée dans un environnement administratif polyvalent. En tant que filiale régionale de Northwind Traders, vous devez coordonner vos efforts avec la filiale de votre pays. L'une des filiales va créer le domaine racine de la forêt et l'autre un domaine enfant dans la nouvelle forêt. Le domaine racine de la forêt doit être créé avant que le domaine enfant, puisse rejoindre la forêt. Vous devez coordonner vos efforts avec l'autre filiale pour être sûr que la procédure appropriée est réalisée au moment opportun.

Votre instructeur va vous attribuer l'un des noms de domaine de la liste ci-dessous.

Nom de l'ordinateur	Domaine racine de la forêt	Domaine enfant
Vancouver	Nwtraders1.msft	
Denver		Corp1.Nwtraders1.msft
Perth	Nwtraders2.msft	
Brisbane		Corp2.Nwtraders2.msft
Lisbon	Nwtraders3.msft	
Bonn		Corp3.Nwtraders3.msft
Lima	Nwtraders4.msft	
Santiago		Corp4.Nwtraders4.msft
Bangalore	Nwtraders5.msft	
Singapore		Corp5.Nwtraders5.msft
Casablanca	Nwtraders6.msft	
Tunis		Corp6.Nwtraders6.msft
Acapulco	Nwtraders7.msft	
Miami		Corp7.Nwtraders7.msft
Auckland	Nwtraders8.msft	
Suva		Corp8.Nwtraders8.msft
Stockholm	Nwtraders9.msft	
Moscow		Corp9.Nwtraders9.msft
Caracas	Nwtraders10.msft	
Montevideo		Corp10.Ntraders10.msft.
Manila	Nwtraders11.msft	
Tokyo		Corp11. Nwtraders11.msft
Khartoum	Nwtraders12.msft	
Nairobi		Corp12. Nwtraders12.msft

Tâches	Instructions spécifiques
1. Créer un domaine racine de la forêt.	<p>a. Reportez-vous au tableau pour vos attributions de domaine.</p> <p>b. Ouvrez une session sur votre serveur en tant qu'<b>Administrateur</b> avec le mot de passe <b>P@ssw0rd</b> si vous ne l'avez pas encore fait.</p> <p> Vous devez installer le système DNS en utilisant l'Assistant Installation de Active Directory. Le service de résolution DNS du contrôleur de domaine racine doit pointer sur London.</p>
2. Créer deux comptes d'utilisateurs à des fins de connexion.	<ul style="list-style-type: none"><li>▪ Créez <b>Nom_OrdinateurUser</b> pour chaque ordinateur de la forêt.</li></ul>
3. Vérifier la création de la nouvelle forêt.	




## Exercice 3

### Création d'un domaine enfant Active Directory

Dans cet exercice, vous allez terminer la création de la forêt Active Directory en créant un domaine enfant à l'intérieur de la racine de la forêt.

#### Scénario

En tant qu'entreprise sœur de la racine de la forêt nouvellement créée, vous allez terminer la forêt en créant le premier domaine enfant. Ne suivez pas cette procédure tant que vous n'avez pas vérifié, avec votre partenaire, que le domaine racine de la forêt a été configuré et qu'il fonctionne.

Tâches	Instructions spécifiques
1. Créer un domaine enfant.	<ul style="list-style-type: none"><li data-bbox="722 709 1503 772">▪ Ouvrez une session sur votre ordinateur local en tant qu'<b>Administrateur</b> avec le mot de passe <b>P@ssw0rd</b></li></ul> <p data-bbox="750 779 1503 842"> <i>Le service de résolution DNS du contrôleur du domaine enfant doit pointer sur le contrôleur du domaine racine de la forêt.</i></p>
2. Vérifier l'installation du nouveau domaine enfant.	

## Exercice 4

### Augmentation du niveau fonctionnel du domaine et de la forêt

Dans cet exercice, vous allez augmenter les niveaux fonctionnels du domaine et de la forêt vers Windows Server 2003.

#### Scénario

Northwind Traders prépare son environnement d'approbations entre forêts, que l'équipe informatique va implémenter ultérieurement. Avant d'implémenter des approbations entre forêts, le niveau fonctionnel des domaines et des forêts doit être augmenté afin de prendre en charge la fonctionnalité d'approbation de forêt.

Tâches	Instructions spécifiques
1. Augmenter le niveau fonctionnel du domaine.	<ul style="list-style-type: none"><li>▪ Ouvrez une session en tant que <b>Nwtradersx\Nom_OrdinateurUser</b> (où <i>x</i> est le numéro du domaine que votre instructeur vous a attribué) avec le mot de passe <b>P@ssw0rd</b>.</li></ul>
2. Augmenter le niveau fonctionnel de la forêt.	<ul style="list-style-type: none"><li>▪ Vous devez augmenter le niveau en utilisant uniquement un membre de la forêt.</li></ul>

## Exercice 5

### Création d'une approbation de forêt

Dans cette exercice, vous allez créer une approbation de forêt bidirectionnelle avec les forêts nwtraders.msft.

#### Scénario

Le conglomérat Northwind Traders se développe rapidement. Vous devez prendre en charge l'augmentation des conditions requises en matière de connectivité entre les différentes organisations. Pour satisfaire ces conditions, vous allez créer l'approbation requise avec laquelle activer les communications et l'accès aux ressources entre votre forêt et la forêt de la société.

Tâches	Instructions spécifiques
1. Configurer la redirection DNS.	▪ Effectuez cette tâche sur le contrôleur du domaine racine de la forêt.
2. Créer une approbation entre la forêt de la classe et la vôtre, puis vérifier que l'approbation a été créée.	▪ Effectuez cette tâche sur le contrôleur du domaine enfant.

