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

1. Introduction.

Ce module présente la configuration requise de 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.

2. Création d'une structure de forêt et de domaine.

a) Introduction

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

b) Conditions requises pour installer Active Directory.

- Un ordinateur fonctionnant sous Windows Server 2003.
- Un espace disque minimum de 250Mo et une partition formatée NTFS.
  200Mo pour la base de données Active Directory et 50Mo pour les fichiers journaux de 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 sans 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.

- Des privilèges administratifs pour la création d'un domaine dans un réseau Windows Server 2003 existant.

- TCP/IP installé et configuré pour utiliser DNS

- Un serveur DNS faisant autorité pour le domaine DNS et prenant en charge les conditions requises répertoriées dans le tableau ci-dessous.

Condition requise	**Description**
Enregistrements de ressources SRV (obligatoires)	Les enregistrements de ressources SRV sont des enregistrements DNS qui identifie 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 mises 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 zones 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.

c) Processus d'installation d'Active Directory

Pour démarrer le processus d'installation d'Active Directory, lancez l'assistant d'installation d'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 version5.*

- *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 jours par l'intermédiaire de la réplication sur chaque contrôleur de domaine subséquent créé dans la forêt.

- *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.
- *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.

- *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 *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.

- *Activation de la sécurité sur les services 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 fournit par l'utilisateur au compte administrateur.* Vous utilisez ce compte pour lancer le contrôleur de domaine en mode Restauration des services d'annuaire.

d) Comment créer une structure de forêt et de domaine.

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.

Création d'un domaine racine de la forêt

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.
2. Dans la page **Assistant Installation de Active Directory**, cliquez sur **Suivant.**
3. Dans la page **Compatibilité du système d'exploitation**, cliquez sur **Suivant.**
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,** vérifier 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 l'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 serveur équipés de versions antérieures de Windows ou Windows NT, ou seulement équipés de serveurs 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 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.
13. Passez en revue la page **Résumé,** puis cliquez sur **Suivant** pour commencer l'installation.
14. A l'invite, redémarrer l'ordinateur.

Création d'un 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.

Page de l'assistant Installation de Active Directory	**Nouvelle étape à réaliser**
Créer un nouveau domaine	Cliquez sur **Domaine enfant dans une arborescence de domaine existante.**
Informations d'identification réseau	Tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte utilisateur que vous souhaitez utiliser pour cette opération. Le compte d'utilisateur doit être un membre du groupe Administrateurs de l'entreprise.
Installation d'un domaine enfant	Vérifier le domaine parent, puis tapez le nom du nouveau domaine enfant.

Lorsque vous utilisez l'Assistant Installation 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.

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.

Page de l'Assistant Installation de Active Directory	**Nouvelle étape à réaliser**
Créer un nouveau domaine	Cliquez sur **Arborescence de domaine dans une forêt existante.**
Informations d'identification réseau	Tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte d'utilisateur que vous souhaiter utiliser pour cette opération. Le compte d'utilisateur doit être un membre du groupe Administrateurs de l'entreprise.
Nouvelle arborescence de domaine	Tapez le nom DNS complet du nouveau domaine.

e) Comment ajouter un contrôleur de domaine répliqué

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 contrôleur 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 l'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 telles 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 répliquez 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 installer Active Directory.

Pour installer un contrôleur de domaine répliqué :

1. Exécuter **dcpromo**. Pour installer un contrôleur de domaine supplémentaire à partir des fichiers de sauvegarde, exécuter **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 lancer l'Assistant d'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.**
   - **A 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 installez les dossiers de la base de données et du journal, ou cliquez sur **Parcourir** pour choisir un emplacement.
6. Dans la page **Volume 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 restauration des services d'annuaire, puis cliquez sur **Suivant**.
8. Passer en revue la page **Résumé**, puis cliquez sur **Suivant** pour commencer l'installation.
9. Lorsque le système vous y invite, redémarrer l'ordinateur.

f) Comment renommer un contrôleur de domaine.

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

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**.

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. 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.

g) Comment supprimer un contrôleur de domaine Active Directory

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 sera supprimé de la forêt. 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

1. Ouvrez l'Assistant de Active Directory
2. Dans la page **Supprimer Active Directory**, s'il s'agit du dernier contrôleur de domaine, cochez la case **Ce serveur est le dernier contrôleur 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 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, puis exécutez la commande **ntdsutil** à l'aide de l'option de nettoyage des métadonnées. Pour ce faire, procédez comme suit :

1. A l'invite, tapez la commande suivante et appuyez sur ENTREE

   Ntdsutil.exe : metadata cleanup

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

   Metadata cleanup : connections

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

   Server connections : connect to serveur Nom_Seveur 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 commande suivante afin d'identifier et de sélectionner le contrôleur de domaine endommagé :

   Select operation target : list sites
   Select operation target : select site numero
   Select operation target : list servers in site
   Select operation target : select server numero
   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

h) Comment vérifier l'installation d'Active Directory

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 ses dossiers partagés nécessaires ont été créés. Si le dossier SYSVOL n'a pas été créé correctement, les données du dossier SYSVOL 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 :

- A l'invite de commande, tapez **net share** et appuyer sur ENTREE.

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

Nom de 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 données et les fichiers journaux d'Active Directory ont été créés, exécutez la procédure suivante :

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

  L'explorateur Windows affiche le contenu du dossier Ntds, sui 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 logiciels enfichable Utilisateurs et ordinateurs Active Directory. Le tableau suivant présente l'objectif de certains de ces objets par défaut :

Objet	**Description**
Builtin	Détient les groupes de sécurité intégrés par défaut
Computers	Emplacement par défaut des comptes d'ordinateurs
Domain COntrollers	Unité d'organisation et emplacements par défaut des comptes d'ordinateurs du contrôleur de domaine
ForeignSecurityPrincipals	Détient les identificateurs de sécurité (SID, Se*curity Identifier*) 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'applications
System	Enregistre les paramètres système intégrés.

Analyse des journaux d'événements pour voir les erreurs

Après avoir installé Active Directory, jetez un œil 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, services d'annuaire, Serveur DNS et Service de réplication de fichier.

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

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	Fermez la session, puis ouvrez-là de nouveau à l'aide d'un compte appartenant au groupe Administrateurs local. Fournissez les informations d'identification d'un compte d'utilisateur membre des groupe Admins du domaine et Administrateurs de l'entreprise.
Les noms de domaine DNS ou NetBIOS ne sont pas uniques	Modifiez le nom de sorte qu'il soit unique.
Le domaine ne peut pas être contacté	Assurez-vous que la connexion réseau est effective entre e 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 le contrôleur de domaine du domaine. Vérifiez que le système DNS fournit une résolution de noms à au moins un contrôleur en vous connectant à un contrôleur de domaine à l'aide de son nom DNS. Pour ce faire, à 'invite de commande, tapez le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name)* du contrôleur de domaine. Si le système DNS est configuré correctement, vous pourrez vous connecter au contrôleur de domaine. 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.
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.

3.

Analyse du système DNS intégré à Active Directory

a) 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.

Ce chapitre 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.

b) Espaces de noms DNS et Active Directory

Les domaines DNS et Active Directory utilisent des noms de domaine identiques pour différents espaces de noms. En utilisant des noms de domaines 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.

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 '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.

c) Définition des zones intégrées à Active Directory.

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 utilisés pour résoudre des noms d'hôte en adresse 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 zones dans une partition d'application Active Directory ou dans une partition de domaine Active Directory. Si les objets de zones sont stockés dans une partition d'application Active Directory, seuls les contrôleurs de domaine qui souscrivent à la partition d'application participent à se réplication. Toutefois, si les objets de zone sont stockés dans une partition de domaine, 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 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 ce 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 renseignements 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.

d) Définition des enregistrements de ressources SRV.

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 qui offre le service et le nom d'ordinateur DNS de l'ordinateur qui offre le service. 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

Tout 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.

Champ	**Description**
_Service	Spécifie le nom du service, (LDAP [Lightweight Directory Access Protocol] ou Kerberos, par exemple) fourni par le serveur qui enregistre cet enregistrement SRV.
_Protocole	Spécifie le type de protocole de transport, tel que TCP ou UDP (User Datagram Protocol)
Nom	Spécifie le nom du domaine auquel fait référence l'enregistrement de ressources.
Ttl	Spécifie la durée de vie (TTL, Time To Live) en secondes. C'est un champ standard des enregistrements de ressources DNS précisant la durée pendant laquelle l'enregistrement est considéré valide.
Classe	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.
Priorité	Spécifie la priorité du serveur. Les clients tentent de contacter l'hôte dont la priorité est la plus faible.
Poids	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.
Port	Spécifie le port sur lequel le serveur écoute ce service.
Cible	Spécifie le nom FQDN, également appelé nom de domaine complet, de l'ordinateur qui fournit le service.

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 de 600 secondes ou de 10 minutes.
- Possède un nom FQDN de london.contoso.msft.

e) Enregistrements SRV enregistrés par les contrôleurs de domaine.

Les enregistrements de ressources SRV sont enregistrés parles 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 démarrer, 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 de 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 ressource SRV en utilisant le format suivant :

*_Service._protocole.DcType.*__*msdcs.*__*Nom_domaine_Dns ouNom_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, spécifient 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.***_site.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**
_ldap._tcp.dc._msdcs.*Nom_Domaine_DNS*	Un serveur LDAP dans le domaine spécifié par *Nom _Domaine_Dns* Tous les contrôleurs de domaine enregistrent cet enregistrement
_ldap._tcp.*Nom_Site*.**_sites.dc._msdcs.***Nom_Domaine_Dns*	Un contrôleur de domaine spécifié par *Nom_Domaine_Dns* et dans le site appelé *Nom_Site*. Nom_Site est le nom unique relatif de l'objet Site qui est enregistré dans Active Directory. Tous les contrôleurs de domaine enregistrent cet enregistrement.
_ldap._tcp.gc._msdcs.*Nom_Forêt_DNS*	Un serveur de catalogue global dans la forêt appelée par *Nom_Forêt_Dns*. Nom_Forêt_Dns est le nom de domaine du domaine racine de la forêt. Seuls les contrôleurs de domaine configurés en tant que serveur de catalogue global enregistrent cet enregistrement.
_ldap._tcp.*Nom_Site*.**_sites.gc._msdcs.***Nom_Forêt_Dns*	Un serveur de catalogue global de la forêt appelée *Nom_forêt_Dns* et dans le site spécifié par *Nom_Site.* Seuls les contrôleurs de domaine configurés en tant que serveurs de catalogue global enregistre cet enregistrement.
_kerberos._tcp.dc._msdcs.*Nom_Domaine_Dns*	Un serveur KDC (Key Distribution Center) pour le domaine spécifié par *Nom_Domaine_Dns.* Tous les contrôleurs de domaine exécutant le protocole d'authentification Kerberos version 5 procèdent à cet enregistrement.
_kerberos._tcp.*Nom_Site*.**_site.dc._msdcs.***Nom_Domaine_Dns*	Un serveur KDC pour le domaine spécifié par *Nom_Domaine_Dns* dans le site spécifié par *Nom_Site.* Tous les contrôleurs de domaine exécutant le protocole Kerberos version 5 procèdent à cet enregistrement.

f) Comment analyser les enregistrements enregistrés par un contrôleur de domaine.

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 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**, exécuter 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 ENTREE.

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).

g) Utilisation de DNS par les ordinateurs clients pour trouver un contrôleur de domaine.

Processus d'utilisation du système DNS pour localiser un contrôleur de domaine

La procédure ci-dessous explique comment 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 en 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.

4. Augmentation des niveaux fonctionnels de la forêt et du domaine.

a) 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.

b) Définition des fonctionnalités des forêts et des domaines.

Sous Windows Server 2003, les fonctionnalités des forêts et des domaines offrent un moyen d'activer les fonctionnalités Active Directory étendue 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 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 Serveur 2003.* 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 réplication accrue

c) Conditions requises pour activer la nouvelle fonctionnalité de Windows Server 2003.

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 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 administrateur de l'entreprise.

d) Comment augmenter le niveau fonctionnel.

En augmentant les fonctionnalités de la forêt et du domaine vers Windows Server 2003, vous activez certaines fonctionnalités 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 A**ugmenter le niveau fonctionnel du domaine.**
3. Dans la boite 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 boite de dialogue **Sélectionner un niveau fonctionnel de la forêt disponible,** sélectionnez **Windows Server 2003**, puis cliquez sur **Augmenter.**

Rmq : 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.

5. Création de relations d'approbation

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

a) Types d'approbations.

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 ou 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 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 un 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'approbations 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.

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 quel a forêt 2 approuve la forêt 3, les domaine 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.

b) Définition des objets du domaine approuvé.

Lorsque vous configurez des approbations entre domaine 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 d'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.

c) Comment fonctionnent les approbations dans une forêt.

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 ressources 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'et pas établit avec un contrôleur de domaine du domaine dans lequel se trouve la ressource.

d) Comment fonctionnent les approbations entre les forêts.

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 les forêts.

Comment s'effectue l'accès à une ressource

Ci-dessous un description de la manière dont un ordinateur client Windows 2000 Professional ou Windows Xp Professional recherche et accède au ressources d'une autre forêt doté 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 de 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 *mwtraders.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.contoxo.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.

e) Comment créer des approbations.

Vous pouvez utiliser Domaines et approbations Active Directory pour créer des relations d'approbation entre des forêts ou 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 un 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 créer une approbation de forêt, tapez le nom DNS de la deuxième forêt, puis cliquez sur **Suivant.**
    - Si vous créer une approbation raccourcie, tapez le nom DNS du domaine, tapez et confirmez le mot de passe d'approbation, puis cliquez sur **Suivant.**
    - Si vous créer une approbation externe, tapez le nom DNS du domaine, puis cliquez sur **Suivant.**
    - Si vous créer 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 créer 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 un approbation unidirectionnelle entrante, cliquez sur **sens unique : en entrée,** puis suivez les instructions de l'Assistant.
    - Pour créer un approbation unidirectionnelle sortante, cliquez sur **sens unique : en sortie,** puis suivez les instructions de l'Assistant.

f) Comment vérifier et révoquer une approbation.

Lorsque vous créer des approbations non transitives, vous devez parfois vérifier et révoquer les chemins d'approbation que vous avez créés. Vous vérifier 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 Domaine et approbation 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 (approbation 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 appuyer sur ENTREE.

NETDOM TRUST nom_domaine_à_approuver /Domaine : 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 Domaine 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 **Domaines qui approuvent ce domaine (approbations entrantes)**, cliquez sur l'approbation que vous souhaitez refuser, puis cliquez 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 appuyer sur ENTREE.

NETDOM TRUST nom_domaine_à_approuver /Domaien : nom_domaine_approuvé /remove