Windows Server 2003

0. Installation / mise à niveau / configuration de Windows Server 2003

0.1. Installation ou mise à niveau

① Pour connaître la configuration système minimum requise pour l'installation de WS2003, il faut consulter le fichier RELNOTES.HTML qui se trouve sur le CD d'installation ou vérifier à l'URL http://www.microsoft.com/hwtest/hcl

En tout cas, il faut minimum :
- Pentium 133
- 128 Mo de mémoire vive
- 1 Go d'espace libre sur le disque dur

② Mise à jour et installation

③ Choix d'un mode de licence
- par serveur
- par client/siège

Serveur → siège
Exemple : 1) 30 licences client et 1 serveur
=> par serveur, il faut 30 licences

2) ajout d'un 2ème serveur
=> par serveur → 30 licences (donc 60 licences en tout pour les 2 serveurs
=> meilleure solution : passer le serveur 1 en mode par siège et installer l'autre en mode par siège => 30 licences au total

④ Choix d'une partition de disque

⑤ Choix d'un système de fichiers
NTFS FAT32
Ntfs : sécurité fichier et dossier, compression, quotas et cryptage
Fat/FAT32 : prise en charge double amrocage mais pas de sécurité

Convert.exe convertit partition FAT32 en NTFS
Exemple : **convert c:/fs :ntfs**

0.2. Installation

Soit en local : installation normale à partir du cd-rom
Soit par le réseau :
- on copie le dossier i386 du cd-rom sur le disque dur d'un serveur de distribution et on partage le répertoire
- sur chaque machine, un mini système d'exploitation avec une gestion réseau se charge.
Ces machines nécessitent un espace libre de 120 à 200 Mo pour les fichiers temporaires.

- A partir du serveur de distribution, on exécute :
  - **winnt.exe** pour les versions antérieures à Windows 95
  - **winnt32.exe** pour les autres versions

Remarque :

Pour une installation sans interaction de l'utilisateur, il faut rajouter **/u** à **winnt32.exe**

⇨ **winnt32.exe /u**
- on retrouve alors le fichier unattended.txt
  - Pour chaque machine différente, on retrouve un fichier UDF en plus

Mise à niveau

On peut faire une mise à niveau des versions de Windows suivantes :

- Windows NT Server 4.0 et Service Pack 5
  - Standard
  - Entreprise

- Windows 2000 Server
  Advanced Server

Conformité du matériel :
A partir du cd-rom, on a un lien « check system compatibility » pour vérifier si on peut mettre à niveau le Windows avec lequel on travaille
On peut aussi vérifier la configuration de l'ordinateur actuel grâce à la ligne de commande suivante : **winnt.exe/checkupgradeonly**

Si le système contient un Active Directory avec domaines et forêts, il faut préparer le domaine et la forêt avant la mise à niveau.
Pour cela on exécute les lignes de commande suivantes :
a**dprep /forestprep**
adprep /domainprep

0.3. Présentation de Windows Server 2003

0.3.1. Différentes versions

- Web Edition
  - Fournisseur d'accès à internet
  - Messagerie électronique
  - 1 à 2 processeurs
  - 32 bits
  - 2 Go maximum de mémoire vive
  - Version allégée de Active Directory
  - Firewall intégré
  - Répartition des charges en réseau

- Standard Edition
  - Orientée PME
  - 32 bits
  - 1 à 4 processeurs
  - 4 Go maximum de mémoire vive
  - Réseau virtuel intégré (applications centralisés)
  - Active Directory
  - Pont, réseau virtuel
  - Remplace Windows 2000 Server

- Entreprise Edition
  - Moyennes et grandes entreprises
  - 32 et 64 bits
  - 1 à 8 processeurs
  - Active Directory complète
  - 32 Go maximum de mémoire vive
    32 bits ➔ 4Go et 64bits ➔ 32 Go
  - Remplace Windows 2000 Advanced Server
  - Possibilité de clusters (jusque 8 nœuds)
  - Prends toute les possibilités précédentes

- Datacenter Edition
  - Applications complexes (grosse base de données, gestion temps réel,…)
  - 1 à 32 processeurs
  - Possibilités de clusters
  - Pas de firewall intégré au départ
  - Remplace Windows 2000 Datacenter Server
  - Prends toutes les caractéristiques précédentes

0.3.2. Nouveautés de Windows Server 2003

0.3.2.1. Active Directory

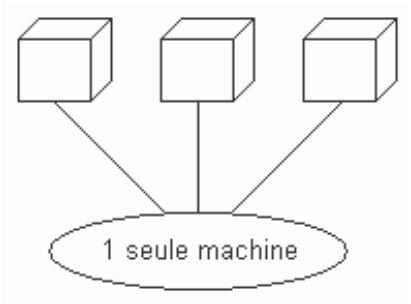
- amélioration au point de vue synchronisation, réplication des domaines
- renommer les noms de domaines
- approbation inter-forêt
- amélioration des consoles MMC

0.3.2.2. Services d'applications

- intégration de Framework.net (comprend les bibliothèques de classes pour ADO.net*, Windows Forms, ASP.net) *ADO = Active Data Objects
- intégration de la prise en charge de XML pour les applications Web

0.3.2.3. Technologies de mise en clusters

Un cluster est une association de plusieurs serveurs reliés ensemble pour n'en faire voir qu'un seul par l'utilisateur.
Si un serveur est hors service, les autres continuent leurs applications et prennent en charge les applications qui tournaient sur le serveur hors service.



Serveur source : basculement
Cluster service : gère la grappe et le basculement
Network Lood Balancing : équilibrage de la charge réseau

0.3.2.4. Serveur de fichiers et d'impression

- choisir un rôle pour le serveur
  - administrative tools
    - Manage your server

- EFS : cryptage de fichier
- DFS : système de fichiers distribués
  - Organisation logique des fichiers

- transformer le serveur de fichier en un serveur de collaboration
  => utilisation de Microsoft Sharepoint Services
  ↳ travail de collaboration par le web

0.3.2.5. Internet Information Server (IIS 6.0)

Sécurité supplémentaire
↳ par défaut, la sécurité est maximale (pas chargé de Control Active X, scripts,…)

http://www.microsoft.com
↳ domaine Microsoft est ajouté à la liste de confiance

0.3.2.6. Terminal Server

- Diminution de l'utilisation de la bande passante
- Seules les informations à écrire à l'écran et passées au clavier ou à la souris sont transmises

0.3.2.7. Réseau

- sécurité pour les réseaux sans fils
- utilisation du protocole IPv6

0.3.2.8. Services de gestion

- site du catalogue des services Microsoft (Windows Catalog)
- site de Windows Update

0.3.3. Architecture de Windows Server 2003

- Mode utilisateur :
  - ne peut accéder directement au hardware
  - possède un niveau de priorité inférieur au mode noyau

- mode noyau :
  - comprend des privilèges spéciaux
    - accéder au matériel
    - allouer la mémoire aux applications
    - choix du processus à exécuter
  - modification de win32 (pour gérer le cas du travail en terminal server)
  - ajout de gestionnaires de clusters
  - ajout de gestionnaires de http

0.3.3.1. Stockage de base.

- Partition système : partition sur laquelle on boot
- Partition d'amorçage : contient le répertoire winnt
- Partition principales/étendues : 4 max (3+1) ➔ diviser en lecteurs logiques
- Partition active ➔ partition système

0.3.3.2. Stockage dynamique.

- Volume : portion de disque vue comme partie distincte

- Volume simple : créer à partir d'un espace non alloué sur HD
- Spanned volume : volume fractionné ➔ regroupement de différents espace non alloués sur différents HD en une seule partie.
- Striped volume : agrégat de bande ➔ remplis les différents espace par 64Ko

0.3.3.3. Conversion de base en dynamique.

Onglet Computeur management\disk management
Cliquer sur le disque et le convertir en disque dynamique.
Rebooter **2x** la machine.

0.3.3.4. Gestion de tolérance de panne.

- Uniquement en dynamique
- Intégrée de façon logicielle : RAIDI et RAIDS

0.3.3.5. Assignation de quotas.

Permet de limiter l'espace disque disponible aux utilisateurs sur le serveur.

Créer un quota : Sur propriété du HD ➔ onglet quota\enable quota management

Console de gestion microsoft (MMC).

Elle contient les « snop in » (composants enfichable) qui sont intégré dans le s.e

Module 1 : Introduction à l'infrastructure Active Directory ®

1. Introduction.

Ce module présente la structure physique et logique du service d'annuaire Active Directory et sa fonction en tant qu'annuaire. Le module présente également les composant logiciels enfichables, les outils de ligne de commande et l'environnement d'exécution de scripts Windows vous permettant de gérer les composants Active Directory ainsi que ses processus de conception, de planification et d'implémentation.

2. Architecture d'Active Directory ®.

a) Introduction

Active Directory inclut des composants qui constituent sa structure logique et physique. Vous devez planifier les structures logique et physique d'Active Directory pour répondre à vos impératifs organisationnels. Pour gérer Active Directory, vous devez comprendre le rôle de ces composants et comment les utiliser.

b) Rôle d'Active Directory

- Centralisation du contrôle des ressources du réseau
- Centralisation et décentralisation de la gestion des ressources
- Stockage des objets de manière sécurisée dans une structure logique
- Optimisation du trafic réseau

Active Directory stocke des informations sur les utilisateurs, les ordinateurs et les ressources du réseau, afin de permettre aux utilisateurs et aux applications d'accéder à ces ressources. Il constitue un moyen cohérent de nommer, de décrire, de localiser, d'accéder, de gérer et de sécuriser les informations concernant ces ressources.

Active Directory fournit les fonctions suivantes :

- *Centralisation du contrôle des ressources du réseau.* La centralisation du contrôle des ressources, comme les serveurs, les fichiers partagé et les imprimantes, permet aux seuls utilisateurs autorisés d'accéder aux ressources dans Active Directory.
- *Centralisation et décentralisation de la gestion des ressources.* Les administrateurs peuvent gérer des ordinateurs clients distribués, des services réseau et des applications à partir d'un emplacement centralisé à l'aide d'une interface de gestion cohérente, ou distribuer des tâches d'administration en déléguant le contrôle des ressources à d'autres administrateurs.
- *Stockage des objets de manière sécurisée dans une structure logique.* Active Directory stocke toutes les ressources sous forme d'objets dans une structure logique hiérarchique sécurisée.
- *Optimisation du trafic réseau.* La structure physique d'Active Directory vous permet d'utiliser plus efficacement la bande passante du réseau. Il vous garantit que lorsque des utilisateurs se connectent au réseau, ils sont authentifiés par l'autorité d'authentification la plus proche de l'utilisateur, réduisant d'autant la quantité de trafic réseau.

c) Structure logique d'Active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans une structure logique hiérarchique. Les *objets* Active Directory représentent des utilisateurs et des ressources. Certains objets en contiennent d'autres.

La structure logique d'Active Directory inclut les composants suivants :

- *Les objets.* Il s'agit des composants les plus élémentaires de la structure logique. *Les classes objets* sont des modèles pour les types d'objets que vous pouvez créer dans Active Directory. Chaque classe d'objet est définie par une liste d'*attributs*, qui définit les valeurs possibles que vous pouvez associer à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.
- *Le unités d'organisation (OU, Organizational Unit).* Vous utiliser ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte vos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. Vous pouvez également déléguer l'autorité de gestion d'une unité d'organisation. Les unités d'organisation peuvent être *imbriquées* les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.
- *Les domaines.* Unités fonctionnelles centrales dans la structure logique d'Active Directory, les domaines sont un ensemble d'objets définis administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et de relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :
  - Une limite d'administration pour objets.
  - Une méthode de gestion de la sécurité pour les ressources partagées.
  - Une unité de réplication pour les objets.
- *Les arborescences de domaines.* Les domaines regroupés en structures hiérarchiques sont appelés arborescence de domaines. Lorsque vous ajoutez un second domaine à une arborescence, il devient *enfant* du domaineracine de l'arborescence. Le domaine auquel un domaine enfant est attaché est appelé *domaine* parent. Un domaine enfant peut à son tour avoir son propre domaine enfant.
  Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique. De cette manière, une arborescence a un *espace de noms contigu.*
- *Les forêts.* Une forêt est une instance complète d'Active Directory. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë.
  Le premier domaine de la forêt est appelé le *domaine racine de la forêt.* Le nom de ce domaine fait référence à la forêt. Par défaut, les informations dans Active Directory ne sont partagées qu'à l'intérieur de la forêt. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.

d) Structure physique d'Active Directory

La structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications.

Les éléments de la structure physique d'Active Directory sont :

- *Les contrôleurs de domaine.* (exécute Win Server 2003 ou Win 2000 et Active Directory). Chaque contrôleur de domaine exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleur de domaine.
- *Les sites Active Directory.* Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsque vous créez des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de *latence de réplication* à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. Vous pouvez donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaine situés à des emplacements différents. (Pour plus d'infos sur les sites voir module 7).
- *Partitions Active Directory.* Chaque contrôleur de domaine contient les partitions Active Directory suivantes :
  - *La partition de domaine* contient les réplicas de tous les objets de ce domaine. La partition de domaine n'est répliquée que dans d'autres contrôleurs appartenant au même domaine.
  - *La partition de configuration* contient la topologie de la forêt. La *topologie* est un enregistrement de tous les contrôleurs de domaine et des connexions entre eux dans une forêt.
  - *La partition de schéma* contient le schéma étendu au niveau de la forêt. Chaque forêt comporte un schéma de sorte que la définition de chaque classe d'objet est cohérente. Les partitions de configurations et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.
  - *Les partitions d'applications facultatives* contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications. Les partitions d'applications sont répliquées dans des contrôleurs de domaine spécifiés dans la forêt.

  (Pour plus d'infos sur les partitions voir module 7)

e) Définitions des maîtres d'opérations

Lorsqu'un domaine est modifié, la modification est répliquée sur tous les contrôleurs du domaine. Certaines modifications, telles que celles apportées au schéma, sont répliquées dans tous les domaines de la forêt. Cette réplication est appelée *réplication multimaître.*

Opérations de maître unique.

Lors d'une réplication multimaître, un conflit de réplication peut se produire si des mises à jour d'origine sont effectuées simultanément sur le même attribut d'un objet sur deux contrôleurs de domaine. Pour éviter des conflits de réplication, vous utiliserez une *réplication à maître unique*, qui désigne un contrôleur de domaine comme étant le seul sur lequel certaines modifications de l'annuaire peuvent être effectuées. Ainsi, des modifications ne peuvent intervenir simultanément sur différents endroits du réseau. Active Directory utilise une réplication à maître unique pour des modifications importantes, comme l'ajout d'un nouveau domaine ou une modification dans le schéma au niveau de la forêt.

Rôles de maître d'opérations.

Les opérations utilisant une réplication à maître unique sont regroupées dans des rôles spécifiques dans une forêt ou un domaine. Ces rôles sont appelés *rôles de maître d'opérations.* Pour chaque rôle de maître d'opérations, seul le contrôleur de domaine possédant ce rôle peut effectuer les modifications dans l'annuaire correspondant. Le contrôleur de domaine responsable d'un rôle particulier est appelé *maître d'opérations* pour ce rôle. Active directory stocke les informations concernant le contrôleur de domaine qui joue un rôle spécifique.
Active Directory définit cinq rôles de maître d'opérations, chacun possédant un emplacement par défaut. Les rôles de maître d'opérations s'étendent au niveau d'une forêt ou d'un domaine.

- *Rôles étendus au niveau d'une forêt :*
  - *Le contrôleur de schéma.* Il contrôle toutes les mises à jour du schéma. Le schéma contient la liste principale des classes et des attributs d'objets utilisés pour créer tous les objets Active Directory, comme les utilisateurs, les ordinateurs et les imprimantes.
  - *Le maître d'attribution des noms de domaine.* Il contrôle l'ajout ou la suppression de domaine dans une forêt. Lorsque vous ajoutez un domaine à la forêt, seul le contrôleur de domaine possédant le rôle de maître d'attribution des noms de domaine peut ajouter le nouveau domaine.

  L'ensemble de la forêt ne contient qu'un seul contrôleur de schéma et qu'un seul maître d'attribution des noms de domaine.

- *Rôles étendus au niveau d'un domaine :*
  - *L'émulateur de contrôleur principal de domaine (PDC, Primary Domain Controller).* Il se comporte comme un contrôleur principal de domaine Win NT pour la prise en charge de tout contrôleur secondaire de domaine *(BDC, Backup Domain Controller)* exécutant Win NT au sein d'un *domaine en mode mixte*. Ce type de domaine possède des contrôleurs de domaine exécutant Win NT 4.0. L'émulateur PDC est le premier contrôleur de domaine que vous créez dans un nouveau domaine.

- *Le maître des identificateurs relatifs (maître RID).* Lorsqu'un nouvel objet est créé, le contrôleur de domaine crée une nouvelle entité de sécurité qui représente l'objet et auquel un identificateur de sécurité (SID, Security IDentifier) unique. Cet identificateur consiste en un identificateur de sécurité de domaine, qui est le même pour toutes les entités de sécurité créées dans le domaine, et en un identificateur relatif (RID, Relative IDentifier) qui est unique pour chaque unités de sécurité créées dans le domaine. Le maître RID alloue des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Le contrôleur de domaine affecte ensuite un maître RID aux objets créés à partir de son bloc de maîtres RID alloués.

- *Le maître d'infrastructure.* Lorsque des objets sont déplacés d'un domaine vers un autre, le maître d'infrastructure met à jour dans son domaine les références d'objets qui pointent sur l'objet dans l'autre domaine. La référence d'objet contient l'identificateur global unique (GUID, Globally Unique IDentifier) de l'objet, son nom unique, et un identificateur de sécurité. Active Directory met régulièrement à jour le nom unique et l'identificateur de sécurité sur la référence d'objet afin de refléter les modifications apportées à l'objet réel.

Dans une forêt, chaque domaine possède ses propres émulateur PDC, maître RID et maître d'infrastructure.
(Pour plus d'infos sur les rôles de maître d'opérations voir module 9)

3. Fonctionnement d'Active Directory

a) Introduction.

Cette partie présente la fonction d'Active Directory en tant que service d'annuaire. Comprendre le fonctionnement d'Active Directory vous aidera à gérer les ressources et à résoudre les problèmes d'accès à ces ressources.

b) Définition d'un service d'annuaire.

Dans de grands réseaux, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre aux utilisateurs et aux applications d'accéder à ces ressources et aux informations les concernant, une méthode cohérente est nécessaire pour nommer, décrire, localiser, accéder, gérer et sécuriser les informations concernant ces ressources. Un service d'annuaire remplit cette fonction.

Définition d'un service d'annuaire.
Un service d'annuaire est un référentiel d'informations structuré concernant les personnes et les ressources d'une organisation. Dans un réseau Windows Server 2003, le service d'annuaire s'appelle Active Directory.

Fonctionnalités d'Active Directory.

- *Accès pour les utilisateurs et les applications aux informations concernant des objets.* Ces informations sont stockées sous forme de valeurs d'attributs. Vous pouvez rechercher des objets selon leur classe d'objet, leurs attributs, leurs valeurs d'attributs et leur emplacement au sein de la structure Active Directory ou selon toutes combinaison de ces valeurs.
- *Transparence des protocoles et de la topologie physique du réseau.* Un utilisateur sur un réseau peut accéder à toutes ressources sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.
- *Possibilité de stockage d'un très grand nombre d'objets.* Comme il est organisé en partitions, Active Directory peut répondre aux besoins issus de la croissance d'une organisation.
- *Possibilité d'exécution en tant que service indépendant du système d'exploitation.* AD/AM (Active Directory in Application Mode) est une nouvelle fonctionnalité de l'Active Directory permettant de résoudre certains scénarios de déploiement liés à des applications utilisant un annuaire. AD/AM s'exécute comme un service indépendant du système d'exploitation qui ne nécessite pas de déploiement sur un contrôleur de domaine.

c) Définition d'un schéma

Le schéma Active Directory définit les genres d'objet, les types d'informations concernant ces objets, et la configuration de sécurité par défaut pour les objets pouvant être stockés dans Active Directory.

Définition du schéma.

Le *schéma* contient les définitions de tous les objets comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Les contrôleurs de domaine ne comportent qu'un seul schéma pour toute une forêt. Ainsi, tous les objets créés dans Active Directory se conforme aux mêmes règles.

Le schéma possède deux types de définitions : Les classes d'objets et les attributs. *Les classes d'objets* décrivent les objets d'annuaires possibles que vous pouvez créer. Chaque classe d'objet est un ensemble d'attributs.

Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets.

Schéma Active Directory et extensibilité.

Vous pouvez créer de nouveaux types d'objets dans Active Directory en développant le schéma.

Modifications et désactivation de schéma.

Sur le contrôleur de domaine, vous pouvez annuler des modifications apportées à un schéma en les désactivant, permettant ainsi aux organisations de mieux exploiter les fonctionnalités d'Active Directory. Vous pouvez également redéfinir une classe ou un attribut de schéma. Vous pourriez, par exemple, modifier la syntaxe de la chaîne Unicode d'un attribut appelé SalesManager pour en faire un nom unique.

d) définition d'un catalogue global.

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparentes pour l'utilisateur. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Définition du catalogue global.

Le *catalogue global* est un référentiel d'informations qui contient un sous-ensemble des attributs de tous les objets d'Active Directory. Les membres du groupe Administrateurs du schéma peuvent modifier les attributs stockés dans le catalogue global, en fonction des impératifs d'une organisation. Le catalogue global contient :

- Les attributs les plus fréquemment utilisés dans les requêtes, comme les nom et prénom d'un utilisateur, et son nom d'ouverture de session ;
- Les informations requises pour déterminer l'emplacement de tout objet dans l'annuaire ;
- Un sous-ensemble d'attributs par défaut pour chaque type d'objet ;
- Les autorisations d'accès pour chaque objet et attribut stocké dans le catalogue global. Si vous recherchez un objet pour lequel vous ne possédez pas les autorisations de visualisation requises, cet objet n'apparaîtra pas dans les résultats de la recherche. Les autorisations d'accès garantissent que les utilisateurs ne puissent trouver que les objets pour lesquels ils possèdent un droit d'accès.

Définition d'un serveur de catalogue global.

Un *serveur de catalogue global* est un contrôleur de domaine qui traite efficacement les requêtes intraforêts dans le catalogue global. Le premier contrôleur de domaine que vous créez dans Active Directory devient automatiquement un serveur de catalogue global. Vous pouvez configurer des serveurs de catalogue global supplémentaires pour équilibrer le trafic lié aux authentifications de connexion et aux requêtes.

Fonctions du catalogue global.

Le catalogue global permet aux utilisateurs d'exécuter deux fonctions importantes :

- Trouver les informations Active Directory en tout point de la forêt, indépendamment de l'emplacement des données ;
- Utiliser les informations d'appartenance au groupe universel pour se connecter au réseau.

(Pour plus d'infos sur le catalogue, voir module 8)

e) Définition d'un nom unique et d'un nom unique relatif.

Les ordinateurs clients utilisent le protocole LDAP pour rechercher et modifier des objets dans une base de données Active Directory. Le protocole LDAP est un sous-ensemble de la norme ISO X.500 relative aux services d'annuaire. Il utilise les informations portant sur la structure d'un annuaire pour trouver des objets individuels possédant chacun un nom unique.

Définition.

Le protocole LDAP utilise un nom représentant un objet Active Directory par une série de composants concernant la structure logique. Cette représentation, appelée *nom unique* de l'objet, identifie le domaine dans lequel se trouve l'objet ainsi que le chemin complet permettant d'accéder à celui-ci. Un nom de ce type ne peut être qu'unique dans une forêt Active Directory.

Le *nom unique relatif* d'un objet identifie l'objet de manière unique dans son conteneur. Deux objets situés dans un même conteneur ne peuvent porter le même nom. Le nom unique relatif est toujours le premier composant du nom unique, mais il n'est pas toujours un nom usuel.

Exemple de nom unique

Chaque élément de la structure logique de l'utilisatrice Laura Bertoli de l'unité d'organisation Sales (ventes) du domaine Contoso.msft est représenté dans le nom unique suivant :

CN = Laura Bartoli, OU = Sales, DC = contoso, DC = msft

- CN (Common Name) est le nom usuel de l'objet dans son conteneur.
- OU (Organizatioal Unit) est l'unité d'organisation qui contient l'objet. Plusieurs valeurs d'OU peuvent exister si l'objet se trouve dans une unité d'organisation imbriquée.
- DC (Domain Component) est un composant de domaine, tel que « com » ou « msft ». Il existe toujours au moins deux composants de domaine, voire davantage si le domaine est un domaine enfant.

Les composants de domaine du nom unique sont basés sur le DNS (Domain Name System).

Exemple de nom unique relatif.

Dans l'exemple suivant, Sales est le nom unique relatif d'une unité d'organisation représentée par le chemin LDAP suivant :

OU = Sales, DC = contoso, DC = msft

f) Ouverture de session unique avec Active Directory.

L'activation d'une ouverture de session unique permet à Active Directory de rendre transparents pour l'utilisateur les processus complexes d'authentification et d'autorisation. Les utilisateurs n'ont pas besoin de gérer plusieurs ensembles d'autorisations.
Une ouverture de session unique consiste en :

- une *authentification*, qui vérifie les autorisations de la tentative de connexion ;
- une *autorisation*, qui vérifie que la demande de connexion est autorisée.

En tant qu'ingénieur système, vous devez comprendre le fonctionnement de ces processus afin d'optimiser et de dépanner votre structure Active Directory.

4. Analyse d'Active Directory

a) Introduction

Sous Windows Server 2003, les administrateurs disposent de composants logiciels enfichables et d'outils de ligne de commande pour gérer Active Directory. Ce chapitre présente ces composants et outils, et explique comment les utiliser pour analyser la structure logique et physique d'Active Directory.

b) Gestion d'Active Directory

L'utilisation d'Active Directory vous permet de gérer un grand nombre d'utilisateur, d'ordinateurs et de ressources réseau à partir d'un emplacement centralisé, à l'aide des outils et des composants logiciels enfichables d'administration de Windows Server 2003. Active Directory prend également en charge l'administration décentralisée. Un administrateur possédant l'autorité requise peut déléguer un ensemble sélectionnés de privilèges administratifs à d'autres utilisateurs ou groupes dans une organisation.

Prise en charge par Active Directory de la gestion centralisée.
Active Directory inclut plusieurs fonctionnalités de prise en charge de la gestion centralisée :

- *Informations concernant tous les objets et leurs attributs.* Les attributs contiennent des données qui décrivent la ressource que l'objet identifie ; comme les informations concernant toutes les ressources du réseau sont stockées dans Active Directory, un administrateur peut gérer et administrer ces ressources de façon centralisée.
- *Vous pouvez interroger Active Directory à l'aide de protocoles tels que LDAP*. Vous pouvez aisément localiser des informations concernant des objets en recherchant des attributs sélectionnés de l'objet, à l'aide d'outils prenant en charge le protocole LDAP.
- *Vous pouvez grouper en unités d'organisation des objets possédant des exigences similaires en termes d'administration et de sécurité.* Les unités d'organisations offrent plusieurs niveaux d'autorités administratives, de sorte que vous pouvez appliquer des paramètres de stratégie de groupe et déléguer le contrôle administratif. Cette délégation simplifie le travail de gestion de ces objets et vous permet de structurer Active Directory en fonction des impératifs de votre organisation.

- *Vous pouvez spécifier des paramètres de stratégie de groupe pour un site, un domaine, ou une unité d'organisation.* Active Directory applique ensuite ces paramètres de stratégie de groupe à tous les utilisateurs et ordinateurs à l'intérieur du conteneur.

Prise en charge par Active Directory de la gestion décentralisée.

Active Directory prend également en charge la gestion décentralisée. Vous pouvez affecter des autorisations et accorder des droits aux utilisateurs de manière très spécifique.

Vous pouvez déléguer l'affectation des autorisations :

- pour des unités d'organisation spécifiques à différents groupes de Domaine local ; par exemple, délégation de l'autorisation Contrôle total pour l'unité d'organisation Sales.
- pour modifier des attributs spécifiques d'un objet dans une unité d'organisation ; par exemple, affecter l'autorisation permettant de modifier les nom, adresse et numéro de téléphone d'un utilisateur et de réinitialiser les mots de passe sur l'objet compte d'utilisateur.
- pour exécuter la même tâche ; par exemple, réinitialiser les mots de passe, dans toutes les unités d'organisation d'un domaine

.

c) Outils et composants logiciels enfichables d'administration d'Active Directory.

Windows Server 2003 comporte plusieurs composants logiciels enfichables et outils de ligne de commande permettant de gérer Active Directory. Vous pouvez également gérer Active Directory à l'aide d'objets ADSI (Active Directory Service Interfaces) à partir de l'environnement d'exécution de scripts Windows. ADSI est une interface simple mais néanmoins puissante d'Active Directory permettant de créer des scripts réutilisables pour la gestion d'Active Directory.

Composants logiciels enfichables d'administration

Composant logiciel enfichable.	**Description**
Utilisateurs et ordinateurs Active Directory.	Cette console MMC est utilisée pour la gestion et la publication d'information dans Active Directory. Vous pouvez gérer des comptes d'utilisateur, des groupes et des comptes d'ordinateurs, ajoutez des ordinateurs à un domaine, gérer des stratégies de compte ainsi que des droits d'utilisateur, et procéder à l'audit des stratégie.
Domaines et approbations Active Directory.	Cette console MMC est utilisée pour gérer des approbations de domaines et de forêts, ajouter des suffixes au nom d'utilisateur principal, et modifier les niveaux fonctionnels de domaines et de forêts.
Sites et services Active Directory	Cette console MMC vous permet de gérer la réplication de données d'annuaire.
Schéma Active Directory	Cette console MMC vous permet de gérer le schéma. Il n'est pas disponible par défaut dans le menu Outils d'administration. Vous devez l'ajouter manuellement.

Vous pouvez personnaliser les consoles d'administration afin qu'elles correspondent aux tâches d'administration que vous déléguez à d'autres administrateurs. Vous pouvez également regrouper dans une même console toutes les consoles requises pour chaque fonction d'administration.

Outils de ligne de commande d'administration.

Outil	Description
Dsadd	Ajoute dans Active Directory des objets, comme des ordinateurs, des utilisateurs, des groupes, des unités d'organisation et des contacts.
Dsmod	Modifie dans Active Directory des objets, comme des ordinateurs, des utilisateurs, des groupes, des unités d'organisation et des contacts.
Dsquery	Exécute des requêtes dans Active Directory en fonction de critères spécifiés. Vous pouvez exécuter des requêtes portant sur des serveurs, des ordinateurs, des groupes, des utilisateurs, des sites, des unités d'organisation et des partitions.
Dsmove	Déplace un objet unique, à l'intérieur d'un domaine, vers un nouvel emplacement dans Active Directory ou renomme un objet unique sans le déplacer.
Dsrm	Supprime un objet dans Active Directory
Dsget	Affiche des attributs sélectionnés d'un ordinateur, d'un contact, d'un groupe, d'une unité d'organisation, d'un serveur ou d'un utilisateur dans Active directory
Csvde	Importe et exporte des données Active Directory à l'aide d'un format de séparation par virgule
Ldifde	Crée, modifie et supprime des objets Active Directory. Peut également prolonger le schéma Active Directory, exporter des informations utilisateur et de groupe vers d'autres applications ou service, et charger dans Active Directory des données d'autres services d'annuaire.

Environnement d'exécution de scripts Windows.

Bien que Windows Server 2003 fournisse plusieurs composants logiciels enfichables et outils de ligne de commande pour gérer Active Directory, ceux-ci ne sont pas adaptés pour des opérations de commandes destinées à effectuer des modifications dans Active Directory impliquant des conditions complexes. En pareils cas, vous pouvez procéder plus rapidement à des modifications à l'aide de scripts

Vous pouvez créer des scripts à partir de l'environnement d'exécution de scripts Windows utilisant ADSI pour exécuter les tâches suivantes :

- Extraire les informations concernant les objets Active Directory ;
- Ajouter des objets dans Active Directory ;
- Modifier les valeurs d'attributs pour les objets Active Directory ;
- Supprimer des objets dans Active directory ;
- Etendre le schéma Active Directory.

ADSI utilise le protocole LDAP pour communiquer avec Active Directory.

5. Processus de conception, de planification et d'implémentation d'Active Directory.

a) Vue d'ensemble de la conception, de la planification et de l'implémentation d'Active Directory

Conception d'active Directory

Un ou plusieurs architectes de systèmes créent la conception d'Active Directory, en se basant sur les besoins d'une entreprise. Ces besoins déterminent les spécifications fonctionnelles pour la conception.

Plan d'implémentation d'Active Directory

Le plan d'implémentation d'Active Directory détermine la mise en œuvre de la conception d'Active Directory en fonction de l'infrastructure matérielle de l'organisation. La conception d'Active Directory peut spécifier le nombre de contrôleur de domaine pour chaque domaine sur la base de la configuration d'un serveur spécifique. Cependant, si cette configuration n'est pas disponible, lors de la phase de planification vous pouvez décider de modifier le nombre de serveurs afin de répondre aux besoins de l'entreprise.

Après avoir implémenté Active Directory, vous devez gérer et assurer la maintenance d'Active Directory afin de garantir disponibilité, fiabilité et sécurité du réseau.

Implémentation d'Active Directory

Durant le déploiement d'Active Directory, les ingénieurs système :

- Créent la structure du domaine et de la forêt, et déploient les serveurs ;
- Créent la structure de l'unité d'organisation ;
- Créent les comptes d'utilisateur et d'ordinateur ;
- Créent des groupes de sécurité et de distribution ;
- Créent les objets Stratégies de groupe (GPO, *Groupe Policy Object*) qu'ils appliquent aux domaines, aux sites et aux unités d'organisation ;
- Créent les stratégies de distribution de logiciels.

b) Processus de conception d'Active Directory

Une conception d'Active Directory inclut plusieurs tâches. Chacune définit les besoins fonctionnels pour un composant de l'implémentation d'Active Directory.

Tâches incluses dans le processus de conception d'Active Directory.

- *Collecte d'informations sur l'organisation.* Cette première tâche définit les besoins en service d'annuaire et les besoins de l'entreprise concernant le projet. Les informations sur l'organisation incluent notamment un profil organisationnel de haut niveau, les implantations géographiques de l'organisation, l'infrastructure technique et du réseau, et les plans liés aux modifications à apporter dans l'organisation.

- *Analyse des informations sur l'organisation.* Vous devez analyser les informations collectées pour évaluer leur pertinence et leur valeur par rapport au processus de conception. Vous devez ensuite déterminer quelles sont les informations les plus importantes et quels composants de la conception d'Active Directory ces informations affecteront. Soyez prêt à appliquer ces informations dans l'ensemble du processus de conception.
- *Analyse des options de conception.* Lorsque vous analyser des besoins d'une entreprise spécifiques, plusieurs options de conception peuvent y répondre. Comme chaque choix que vous faites affecte les autres composants de la conception, restez flexible dans votre approche de la conception durant tout le processus.
- *Sélection d'une conception.* Développez plusieurs conceptions d'Active Directory, puis comparez leurs points forts et leurs points faibles. Lorsque vous sélectionnez un conception, analyser les besoins d'une entreprise qui entre en conflit et tenez compte de leurs effets sur les choix de vos conceptions. Il se peut qu'aucune des conceptions soumises ne fasse l'unanimité. Choisissez la conception qui répond le mieux à vos besoins d'entreprise et qui représente globalement le meilleur choix.
- *Affinage de la conception.* La première version de votre plan de conception est susceptible d'être modifiée avant la phase pilote de l'implémentation. Le processus de conception est itératif parce que vous devez tenir compte de nombreuses variables lorsque vous concevez une infrastructure Active Directory. Révisez et affinez plusieurs fois chacun des concepts de votre conception pour prendre en compte tous les besoins d'entreprise.

Résultat du processus de conception d'Active Directory

- *La conception du domaine et de la forêt.* La conception de la forêt inclut des informations comme le nombre de forêts requis, les consignes de création des approbations et le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name)* pour le domaine racine de chaque forêt. La conception inclut également la stratégie de contrôle des modifications de la forêt, qui identifie les processus de propriété et d'approbation pour les modifications de la configuration présentant un impact sur toute la forêt. Identifiez la personne chargée de déterminer la stratégie de contrôle des modifications de chaque forêt dans l'organisation. Si votre plan de conception comporte plusieurs forêts, vous pouvez évaluer si des approbations de forêts sont requises pour répartir les ressources du réseau parmi les forêts.

  La conception du domaine indique le nombre de domaines requis dans chaque forêt, le domaine qui sera le domaine racine pour chaque forêt et la hiérarchie des domaines si la conception comporte plusieurs domaines. La conception du domaine inclut également le nom DNS pour chaque domaine et les relations d'approbation entre domaines.

- *La conception de l'unité d'organisation.* Elle indique comment vous créerez les unités d'organisation pour chaque domaine dans la forêt. Incluez une description de l'autorité d'administration qui sera appliquée à chaque unité d'organisation, et à qui cette même autorité sera déléguée. Pour finir, incluez la stratégie utilisée pour appliquer la stratégie de groupe à la structure de l'unité d'organisation.
- *La conception du site.* Elle spécifie le nombre et l'emplacement des sites dans l'organisation, les liens requis pour relier les sites et le coût de ces liens.

c) Processus de planification d'Active Directory

Composant d'un plan Active Directory

- *Stratégie de compte.* Elle inclut des informations comme les consignes d'attribution de nom aux comptes et la stratégie de verrouillage, la stratégie en matière de mots de passe et les consignes portant sur la sécurité des objets.
- *Stratégie d'audit.* Elle détermine comment suivre les modifications apportées aux objets Active Directory.
- *Plan d'implémentation d'unité d'organisation.* Il définit quelles unités d'organisation créer et comment. Si la conception d'unité d'organisation spécifie que ces unités seront créées géographiquement et organisées par division à l'intérieur de chaque zone géographique, le plan d'implémentation des unités d'organisation définit les unités à implémenter. Le plan fournit également des consignes portant sur la délégation d'autorité.
- *Plan de stratégie de groupe.* Il détermine qui crée, relie et gère les objets de stratégie de groupe, et comment cette stratégie sera implémentée.
- *Plan d'implémentation du site.* Il spécifie les sites, les liens qui les relient, et les liaisons de sites planifiées. Il spécifie également la planification et l'intervalle de réplication ainsi que les consignes en matières de sécurisation et de configuration de la réplication entre sites.
- *Plan de déploiement de logiciels.* Il spécifie comment vous utiliserez la stratégie de groupe pour déployer de nouveaux logiciels et des mises à niveaux logiciels. Il peut spécifier si les mises a niveau de logiciels sont obligatoires ou facultatives.
- *Plan de placement des serveurs.* Il spécifie le placement des contrôleurs de domaine, des serveurs de catalogue global, des serveurs DNS intégrés à Active Directory et des maitre d'opérations. Il spécifie également si vous activerez la mise en cache des appartenances à un groupe universel pour les sites ne possédant pas de serveur de catalogue global.

Lorsque tous les plans de composants sont terminés, vous devez les combiner pour former le plan complet d'implémentation d'Active Directory.

d) Processus d'implémentation d'Active Directory

Processus d'implémentation.

Vous devez exécuter les tâches suivantes pour implémenter Active Directory.

- *Implémentation de la forêt, du domaine et de la structure DNS.* Créez le domaine racine de la forêt, les arborescences de domaines et tout autre domaine enfant constituant la forêt et la hiérarchie des domaines.
- *Création des unités d'organisation et des groupes de sécurité.* Créez la structure d'unité d'organisation pour chaque domaine dans chaque forêt, créez des groupes de sécurité et déléguez l'autorité administrative à des groupes administratifs dans chaque unité d'organisation.
- *Création des comptes d'utilisateur et d'ordinateur.* Importez les comptes d'utilisateurs dans Active Directory.
- *Création des objets de stratégies de groupe.* Créez des objets Stratégies de groupe basés sur la stratégie de groupe, puis reliez-les à des sites, a des domaines ou à des unités d'organisation.
- *Implémentation des sites.* Créez des sites en fonction du plan des sites, créez des liens reliant ces sites, définissez les liaisons de sites planifiées et déployez sur les sites des contrôleurs de domaine, des serveurs de catalogue global, des serveurs DNS et des maîtres d'opérations.

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
```

Module 3 : Implémentation de la structure d'une unité d'organisation.

1. Introduction.

Ce module explique comment créer et gérer des unités d'organisation, déléguer des tâches d'administration courantes et planifier l'implémentation de la structure d'une unité d'organisation.

2. Création et gestion d'unités d'organisation.

a) Introduction

Cette leçon présente les outils de ligne de commande et les composants logiciels enfichables MMC permettant la création et la gestion d'unités d'organisation. Elle apporte également les compétences requises pour créer, modifier et supprimer des unités d'organisation.

b) Présentation de la gestion des unités d'organisation.

Les unités d'organisation sont les conteneurs du service d'annuaire Active Directory que vous utiliser pour placer des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation. L'utilisation d'unités d'organisation vous permet de créer des conteneurs dans un domaine représentant les structures hiérarchique et logique de votre organisation. Vous pouvez ensuite gérer la configuration et l'utilisation de comptes et de ressources en fonction de votre modèle d'organisation.

Cycle de vie d'unités d'organisation.
Le cycle de vie des unités d'organisation inclut quatre phases :

- *Planification.* Vous planifiez au cours de cette phase la structure des unités d'organisation. Vous déterminez quelles unités d'organisation vous allez créer et comment vous en déléguerez le contrôle administratif.
- *Déploiement.* Vous créez au cours de cette phase la structure des unités d'organisation en fonction de leur plan.
- *Maintenance.* Après avoir créé la structure des unités d'organisation dans Active Directory, vous pouvez renommer, déplacer ou modifier les unités créées en fonction des besoins permanents de l'organisation.
- *Suppression.* Dans Active Directory, tous les objets, y compris les unités d'organisation, occupent de l'espace dans le contrôleur de domaine qui héberge Active Directory. Lorsque des unités d'organisation ne sont plus requises, vous devez les supprimer.

c) Méthode de création et de gestion des unités d'organisation.

Microsoft Windows Server 2003 fournit plusieurs comosants logiciels enfichables et outils de ligne de commande vous permettant de créer des unités d'organisation et de gérer la configuration et l'utilisation de comptes et de ressources dans le modèle de votre organisation. Vous pouvez également utiliser l'environnement d'exécution de scripts pour les plates-formes Microsoft Windows, afin de gérer des unités d'organisation.

Méthodes de création et de gestion des unités d'organisation

La liste suivante décrit quelques composants logiciels enfichables et outils de ligne de commande vous permettant de créer et de gérer des unités d'organisation :

- *Utilisateurs et ordinateurs Active Directory.* Ce composant logiciel enfichable MMC permet de créer, modifier et supprimer des unités d'organisation. Utilisez ce composant logiciels enfichable lorsque vous n'avez que quelques unités d'organisation à gérer, ou lorsque vous souhaitez gérer des unités de manière interactive.

- *Outils de service d'annuaire.* Cet ensemble d'outils de ligne de commande permet de gérer des objets et d'effectuer des requêtes d'informations dans active Directory. Les outils de ligne de commande incluent Dsadd, Dsmod et Dsrm. L'utilisation de ces outils avec le paramètre « ou » vous permet d'ajouter, de modifier et de supprimer des unités d'organisation dans Active Directory. Vous pouvez également utiliser des scripts et des fichiers de commandes avec ces outils pour gérer des services d'annuaire.

- *Ldifde (lightweight Directory Access Protocol Data Interchange Format Directory Exchange).* Cet outils de ligne de commande permet de créer des unités d'organisation et d'autre objets Active Directory. Ldifde utilise un fichier d'entrée contenant des informations sur les objets à ajouter, modifier ou supprimer. Ces informations sont stockées sous la forme d'une série d'enregistrements, séparés par une ligne vide dans un fichier d'entrée.

- *Environnement d'exécution de scripts Windows.* Vous pouvez créer des unités d'organisation à l'aide d'applications Windows, ou à l'aide de scripts Windows avec les composants fournit par les interfaces ADSI (Active Directory Service Interfaces). L'utilisation de scripts vous permet de créer des unités d'organisation dans le cadre d'une configuration d'application, le cas échéant.

d) Comment créer et gérer des unités d'organisation à l'aide d'outils de service d'annuaire.

Les outils de ligne de commande Dsadd, Dsmod et Dsrm du service d'annuaire vous permettent de créer et de gérer des unités d'organisation à partir de l'invite de commande. Vous pouvez également utiliser ces commandes dans des scripts et des fichiers de commandes.

Procédure de création d'une unité d'organisation

Pour créer une unité d'organisation, exécuter la commande **Dsadd** suivante à partir de l'invite de commande :

Dsadd ou *NU_Unité_Organisation* **–desc** *Description* **–d** *Domaine* **–u** *Nom_Utilisateur* **–p** *Mot_de_passe*

Où :

- *NU_Unité_Organisation* spécifie le nom unique de l'unité d'organisation que vous désirez ajouter. Par exemple, pour ajouter l'unité d'organisation *SupportTechnique* au domaine nwtraders.msft, le nom unique serait *ou=supporttechnique,dc=nwtarders,dc=msft.*
- *Description* spécifie la description de l'unité d'organisation que vous désirez ajouter.
- *Domaine* spécifie le domaine auquel se connecter. Par défaut, l'ordinateur est connecté au contrôleur de domaine du domaine sur lequel il a ouvert une session.
- *Nom_Utilisateur* spécifie le nom permettant de se connecter à un serveur distant. Par défaut, le nom de l'utilisateur connecté est utilisé. Vous pouvez spécifier un nom d'utilisateur selon l'un des formats suivants :

  - Nom d'utilisateur (par exemple, Linda)
  - Domaine\nom d'utilisateur (par exemple, widgets\Linda)
  - Nom d'utilisateur principal (UPN, *User Principal Name)* (par exemple, Linda@widgets.microsoft.com)

- *Mot_de_passe* est le mot de passe à utiliser pour ouvrir une session sur un serveur distant.Si vous tapez *(astérisque), un mot de passe vous sera demandé.

Procédure de modification d'une unité d'organisation

Pour modifier la description d'une unité d'organisation, exécutez la commande suivante :

Dsmod ou *NU_Unité_Organisation* **–desc** *Description* **–d** *Domaine* **–u** *Nom_Utilisateur* **–p** *Mot_de_passe*

Les paramètres qui sont transmis à la commande **dsmod** sont les mêmes que ceux de la commande **dsadd**. La nouvelle description doit être transmise comme paramètre *desc*.

Procédure de suppression d'une unité d'organisation

Vous devez suprimer d'Active Directory les unités d'organisation qui ne sont plus utilisées. Pour supprimer une unité d'organisation, exécuter la commande suivante :

Dsrm ou *NU_Unité_Organisation* **–d** *Domaine* **–u** *Nom_Utilisateur* **–p** *Mot_de_passe*

Les paramètres qui sont transmis à la commande **dsrm** sont les mêmes que ceux de la commande **dsadd**. Vous pouvez utiliser les paramètres supplémentaires suivants avec **dsrl :**

- *Subtree.* Spécifie de supprimer l'objet ainsi que tous les objet contenus dans la sous-arborescence située sous cet objet.
- *Exclude.* Spécifie de ne pas supprimer l'objet de base fournit par *NU_Unité_Organisatio* lorsque vous supprimer la sous-arborescence située au dessous. Par défaut, seul l'objet de base spécifié est supprimé. Le paramètre Exclude ne peut être spécifié qu'avec le paramètre subtree.

e) Comment créer et gérer des unités d'organisation à l'aide de l'outils Ldifde.

L'outil de ligne de commande Ldifde vous permet de créer des unités d'organisation en mode batch et de définir des hiérarchies d'unités d'organisation. Vous pouvez également utiliser Ldifde pour modifier et supprimer des unités d'organisation.

Procédure

La première étape à exécuter pour utiliser cet outil consiste à créer le fichier d'entrée (*.ldf) à utiliser avec Ldifde. Après avoir créer ce fichier, vous exécuterez la commande **Ldifde.**

Procédez comme suit pour créer des unités d'organisation à l'aide de l'outil de ligne de commande Ldifde :

1. Créez un fichier d'entrée. L'exemple suivant montre le format du fichier :

   ```
   dn : OU=ExempleOU,DC=nwtraders,DC=msft
   changetype : add
   objectClass : organizationalUnit
   ```

   Changetype détermine le type d'opération effectuée sur l'objet Active Directory. **ObjectClass** spécifie la classe de l'objet Active Directory.

   Dans l'exemple précédent, Ldifde ajoute un objet d'unité d'organisation appelé *ExempleOU* au domaine nwtraders.msft. Vous pouvez ajouter plusieurs unités d'organisation en ajoutant d'autres entrées comme celle ci-dessus. Chaque entrée dn doit être précédée d'une ligne vide, sauf la première.

2. Exécutez Ldifde pour créer, modifier ou supprimer des unités d'organisation en entrant la commande suivante :

   C:\>ldifde –i –k –f OUList.ldf –b *Nom_Utilisateur Domaine Mot_de_passe*

   Où :
   - -i spécifie le mode d'importation. Si celui-ci n'est pas spécifié, le mode par défaut est exportation.
   - -k permet de ne pas tenir compte des erreurs durant une opération d'importation et de poursuivre le traitement.
   - -f spécifie le nom du fichier d'importation ou d'exportation.
   - OUList.ldf est le fichier d'entrée.
   - -b spécifie le nom d'utilisateur, le nom de domaine et le mot de passe associés au compte d'utilisateur qui sera utilisé pour exécuter l'opération d'importation ou d'exportation.

f) Comment créer des unités d'organisation à l'aide de l'environnement d'exécution de scripts Windows.

ADSI est une interface de programmation d'application (API, *Application Programming Interface)* que vous utilisez à partir de l'environnement d'exécution de scripts Windows pour automatiser l'administration d'Active Directory. ADSI utilise le protocole LDAP (Lightweight Directory Access Protocol) pour communiquer avec Active Directory. Toutes les opérations ADSI que vous effectuez sur Active Directory respectent la même procédure. Vous devez tout d'abord vous connecter à Active Directory. Vous pouvez ensuite effectuer des tâches, comme extraire des informations concernant des objets, et ajouter, modifier ou supprimer des objets. Si vousq apportez des modifications à Active Directory, vous devez les enregistrer dans la base de données Active Directory afin qu'elles soient conservées.

Procédure

Procédez comme suit pour créer une unité d'organisation à l'aide de l'environnement d'exécution de scripts Windows :

1. A l'aide du bloc-notes, créez un fichier texte portant l'extension *.vbs. Insérez dans ce fichier les commandes figurant ci-après sous les points a, b et c, puis enregistrez le fichier.
    a) Commencez par vous connecter au domaine dans lequel vous souhaitez créer l'unité d'organisation, comme indiqué dans l'exemple suivant :

    ```
    Set objDom = GetObject(« LDAP://dc=nwtraders,dc=msft »)
    ```

    b) Créez ensuite l'unité d'organisation en spécifiant OrganizationalUnit comme type d'objet Active Directory à créer et le nom de l'unité d'organisation, comme indiqué dans l'exemple suivant :

    ```
    Set objOU = objDom.Create
    (« OrganizationalUnit », « ou=NouvelleOU »)
    ```

    Dans cet exemple, NouvelleOU est le nom de l'unité d'organisation que vous créez.

    c) Pour terminer, enregistrez ces informations dans la base de données Active Directory, comme indiqué dans l'exemple suivant :

    ```
    objOU.SetInfo
    ```

2. Pour exécuter les commandes dans le fichier *.vbs, tapez le texte suivant à l'invite de comande :

    ```
    Wscript nom_fichier_script.vbs
    ```

3.

Délégation du contrôle administratif des unités d'organisation.

a) Introduction.

Ce chapitre explique le rôle de la délégation de privilèges administratifs, les tâches d'administration que vous pouvez déléguer, comment les déléguer et comment vérifier que vous avez délégué les privilèges requis pour effectuer ces tâches.

b) Qu'est-ce que la délégation de privilèges administratifs ?

La raison majeure motivant la création d'unité d'organisation est de distribuer les tâches d'administration dans toute l'organisation en déléguant le contrôle administratif à différents administrateurs. La délégation est particulièrement importante lorsque vous développez un modèle d'administration décentralisé.

Qu'est-ce que la délégation de l'administration ?

La délégation de l'administration est le processus de décentralisation de la responsabilité de la gestion d'unités d'organisation d'un administrateur central vers d'autres administrateurs. La capacité à établir l'accès à des unités d'organisation individuelles est une fonctionnalité de sécurité importante dans Active Directory ; vous pouvez contrôler l'accès jusqu'au niveau le plus bas d'une organisation sans devoir créer de nombreux domaines Active Directory.

L'autorité déléguée au niveau du site couvrira probablement plusieurs domaines ou, à l'inverse, peut ne pas inclure de cibles dans le domaine. L'autorité déléguée au niveau du domaine affectera tous les objets qui s'y trouvent. L'autorité déléguée au niveau de l'unité d'organisation peut affecter cet objet et tous ses objets enfants, ou uniquement l'objet lui-même.

Pourquoi déléguer l'administration ?

Vous déléguez le contrôle administratif afin de permettre l'autonomie administrative des organisations au niveau des services et des données ou, au contraire, pour isoler les services ou les données dans une organisation. Vous pouvez éliminer le besoin de disposer de plusieurs comptes administrateur ayant une autorité étendue, sur un domaine entier par exemple, mais néanmoins utiliser le groupe prédéfini Admins du domaine pour gérer tout le domaine.

L'autonomie correspond à la possibilité qu'on les administarteurs d'une organisation de prendre en charge de manière indépendante :

- Tout ou partie de la gestion des services (*autonomie de la gestion des services) ;*
- Tout ou partie de la gestion des données de la base de données Active Directory ou des ordinateurs membres rattachés à l'annuaire (*autonomie dela gestion des données).*

L'autonomie administrative :

- Minimise le nombre d'administrateurs devant posséder des droits d'accès de haut niveau ;
- Limite l'impact d'une erreur administrative à une zone d'administration plus réduite.

L'isolation correspond à la possibilité qu'ont les administrateurs d'une organisation d'empêcher les autres administrateurs de :

- Contrôler ou d'interférer avec la gestion des services (*isolation de la gestion des services) ;*
- Contrôler ou visualiser un sous-ensemble de données dans l'annuaire ou sur les ordinateurs membres rattachés à l'annuaire (*isolation de la gestion des données).*

Windows Server 2003 comporte des autorisations et des droits utilisateur spécifiques qui vous permettent de déléguer le contrôle administratif. En utilisant une combinaison d'unités d'organisation, de groupes et d'autorisations, vous pouvez conférer des droits d'administration à un utilisateur particulier de telle sorte que celui-ci dispose d'un niveau approprié d'administration sur tout un domaine, sur toutes les unités d'organisation dans un domaine ou sur une seule unité d'organisation.

c) Tâches d'administration pour unités d'organisation.

Utilisez des unités d'organisation pour regrouper des objets Active Directory par type (par exemple, par utilisateurs, groupes et ordinateurs) afin de pouvoir les gérer de manière efficace.

Tâches d'administration courantes.

Les administrateurs exécutent régulièrement les tâches suivantes dans Active Directory :

- *Modification des propriétés sur un conteneur particulier.* Par exemple, lorsqu'un nouvel ensemble de logiciels est disponible, les administrateurs peuvent créer une stratégie de groupe qui contrôle leur distribution.

- *Création et suppression d'objets d'un type particulier.* Dans une unité d'organisation, ces types spécifiques peuvent être les utilisateurs, les groupes et les imprimantes. Lorsqu'un nouvel employé rejoint l'organisation, par exemple, vous créez un compte d'utilisateur pour l'employé, puis vous ajoutez cet employé dans l'unité ou le groupe d'organisation approprié.

- *Mise à jour de propriétés spécifiques sur des objets d'un type donné* dans une unité d'organisation. Il se peut que la tâche d'administration la plus courante que vous effectuiez, concernant la mise à jour de propriétés, inclut des tâches comme la réinitialisation des mots de passe et la modification des informations personnelles d'un employé, telles que son adresse et son numéro de téléphone en cas de déménagement, par exemple.

d) Comment déléguer le contrôle administratif.

Vous pouvez utiliser l'Assistant Délégation de Contrôle pour déléguer le contrôle administratif des objets Active Directory, comme les unités d'organisation. L'utilisation de l'Assistant vous permet de déléguer des tâches d'administration courantes, telles que la création, la suppression et la gestion des comptes d'utilisateurs.

Procédure.

Exécutez la procédure ci-dessous pour déléguer des tâches d'administration courantes pour une unité d'organisation.

1. Procédez comme suit pour démarrer l'Assistant Délégation de contrôle :
    a. ouvrez la console Utilisateurs et ordinateurs Active Directory.
    b. Dans l'arborescence de la console, double-cliquez sur le nœud du domaine.
    c. Dans le volet de détails, cliquez avec le bouton droit sur l'unité d'organisation, cliquez ensuite sur **Déléguer le contrôle**, puis sur **Suivant.**

2. Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez déléguer des tâches d'administration courantes. Pour ce faire, procédez comme suit :
    a. Dans la page **Utilisateurs ou groupes** cliquez sur **Ajouter.**
    b. Dans la boite de dialogue **Sélectionner des utilisateurs, des ordinateurs ou des groupes**, tapez les noms des utilisateurs et des groupes auxquels vous souhaitez déléguer le contrôle de l'unité d'organisation, cliquez ensuite sur **OK**, puis sur **Suivant**.

3. Affectez des tâches courantes à déléguer. Pour ce faire, procédez comme suit :
    a. Dans la page **Tâches à déléguer**, cliquez sur **Déléguer les tâches courantes suivantes.**
    b. Dans la page **Tâches à déléguer,** sélectionner les tâches que vous souhaitez déléguer, puis cliquez sur **Suivant.**

4. Cliquez sur **Terminer**.

Lorsque vous déléguez le contrôle de la création d'objets dans Active Directory à un utilisateur ou à un groupe, ces derniers peuvent créer un nombre d'objets illimité. Dans Windows Server 2003, vous pouvez limiter le nombre d'objets qu'une entité de sécurité peut posséder dans une partition d'annuaire, en implémentant un quota pour cette entité.

e) Comment personnaliser le contrôle administratif délégué.

Outre l'utilisation de l'Assistant Délégation de contrôle pour déléguer un ensemble personnalisé de tâches d'administration, telles que le création, la suppression et la gestion des comptes d'utilisateurs, vous pouvez utiliser l'Assistant pour sélectionner un ensemble de tâches personnalisées et ne déléguer le contrôle que de ces tâches.

Vous pouvez, par exemple, déléguer le contrôle de tous les objets existant dans une unité d'organisation et de tous les objets qui ne sont ajoutés. Mais vous pouvez également sélectionner dans l'unité d'organisation les objets dont vous souhaitez déléguer le contrôle administratif, par exemple les objets utilisateur d'une unité d'organisation. Vous pouvez par ailleurs spécifier que vous ne souhaitez déléguer que la création de l'objet sélectionné, ou sa suppression, ou les deux.

Procédure.

Procédez comme suit pour déléguer des tâches d'administration personnalisées dans le cadre d'une unité d'organisation :

1. Démarrer l'Assistant Délégation de contrôle.
2. Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez déléguer des tâches d'administration.
3. Affectez les tâches personnalisées à déléguer. Pour ce faire, procédez comme suit :
    a) Dans la page **Tâches à déléguer**, cliquez sur **Créer une tache personnalisée à déléguer**, puis cliquez sur **Suivant.**
    b) Dans la page **Types d'objet Active Directory**, effectuez l'une des opérations suivantes :
        i. Cliquez sur **De ce dossier et des objets qui s'y trouvent. Déléguer aussi la création de nouveaux objets dans ce dossier**, puis cliquez sur **Suivant.**
        ii. Cliquez sur **Seulement des objets suivants dans le dossier,** sélectionner le type d'objet Active Directory dont vous souhaitez déléguer le contrôle, puis cliquez sur **Suivant.**
    c) Sélectionnez les autorisations que vous souhaitez déléguer, puis cliquez sur **Suivant.**
4. Cliquer sur **Terminer**

f) Comment vérifier la délégation du contrôle administratif.

Utilisez Utilisateur et Ordinateurs Active Directory pour vérifier que l'Assistant Délégation de contrôle a correctement délégué l'autorité d'effectuer les tâches.

Procédure
Procédez comme suit pour vérifier la délégation du contrôle :

1. Dans la console Utilisateurs et Ordinateurs Active Directory, cliquez dans le menu **Affichage** sur **Fonctionnalités avancées.**
2. Dans l'arborescence de la console, double-cliquez sur le nœud du domaine.
3. Dans le volet de détails, cliquez avec le bouton droit sur l'unité d'organisation, puis cliquez sur **Propriétés.**
4. Sous l'onglet **Sécurité**, cliquez sur **Paramètres avancés.**
5. Sous l'onglet **Autorisations**, sous **Entrées d'autorisations**, visualisez les autorisations affectées.

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

a) Introduction

Les unités d'organisation dont des conteneurs dans chaque domaine Active Directory représentant les structures hiérarchiques dans une organisation. Pour créer la structure d'une unité d'organisation représentant au mieux la structure de l'organisation, vous devez comprendre les facteurs qui affectent dans votre organisation la création d'unités d'organisation. Ce chapitre vous apporte les connaissances et les compétences nécessaires pour planifier une stratégie d'unité d'organisation.

b) Processus de planification d'unité d'organisation.

La structure des unités d'organisation dans Active Directory est basée sur la structure administrative de l'organisation. La première étape de planification d'une structure d'unité d'organisation consiste à documenter la structure de l'organisation.

Processus de planification d'unité d'organisation
Procédez comme suit pour planifier la stratégie d'unité d'organisation pour votre organisation :

- *Documentez la structure existante de l'organisation.* Lors de la documentation de la structure existante de l'organisation, une stratégie consiste à diviser les tâches d'administration en catégories, puis à documenter les administrateurs qui sont responsable de chacune d'elles.
- *Identifiez les domaines à améliorer.* Travaillez avec l'équipe de planification pour identifier les domaines à améliorer. Par exemple, il peut être plus rentable de combiner plusieurs équipes IT provenant de différentes divisions. Vous pouvez identifier le personnel non informatique susceptible de vous aider dans le processus d'administration et réduire la charge de travaille du personnel informatique. Les administrateurs peuvent ainsi se concentrer sur les domaines où leur expertise est requise.

Utilisez ensuite les points suivants comme consignes pour votre plan délégation :

- *Déterminez le niveau d'administration.* Décidez ce que chaque groupe contrôlera et à quel niveau vous déléguerez l'administration dans la hiérarchie administrative. Lorsque vous créez le plan, identifiez quels groupes :
    - Auront un contrôle intégral sur les objets d'une classe particulière ; ces groupes peuvent créer et supprimer des objets dans une classe spécifiée et modifier tous les attributs des objets dans la classe spécifiée.
    - Seront autorisés à créer des objets d'une classe particulières ;par défaut,les utilisateurs ont le contrôle intégral des objets qu'ils créent ;
    - Seront autorisés à ne modifier que des attributs spécifiques d'objets existants d'une classe particulière.

- *Identifiez chaque administrateur et compte d'utilisateur dans votre organisation ainsi que les ressources qu'ils administrent.* Ces informations vous aideront à déterminer la propriété et les autorisations affectées aux unités d'organisation que vous créez pour prendre en charge la plan de délégation.

c) Facteurs organisationnels déterminant la structure d'une unité d'organisation.

Les facteurs qui affectent la structure d'une unité d'organisation sont : le type et la structure du modèle d'administration informatique. La compréhension de ces facteurs vous aidera à créer la structure d'une unité d'organisation la mieux adaptée à vos impératifs organisationnels.

Types de modèles d'administration informatique.
Les organisations informatiques les plus courantes sont les suivantes :

- *Informatique centralisée.* Dans ce modèle, l'organisation informatique ne rend de comptes qu'à une seule personne et est généralement le groupe responsable pour tous les services d'information et de réseau, bien que certaines tâches de routine puissent être déléguées à certains groupes ou services.
- *Informatique centralisée avec gestion décentralisée.* Dans ce modèle, une équipe informatique principale centralisée est responsable des principaux services d'infrastructure, mais elle délègue la plupart des opérations quotidiennes aux groupes informatiques situés dans des succursales, lesquels assurent un support administratif local à leurs utilisateurs.
- *Informatique décentralisée.* Ce type d'organisation permet à diverses unités commerciales de sélectionner un modèle informatique approprié pour répondre à leurs besoins. Une organisation de ce type peut comporter plusieurs groupes informatiques avec des objectifs et des besoins divers. Pour chaque initiative technologique affectant toute l'organisation, comme la mise à niveau d'une application de messagerie, les groupes informatiques doivent travailler ensemble pour implémenter les modifications.

- *Informatique externalisée.* Certaines organisations sous-traitent la gestion de tout ou partie de leur organisation informatique. Lorsque seuls quelques éléments de l'organisation informatique sont externalisés, il devient impératif d'implémenter un modèle de délégation en bonne et due forme. Ainsi, le groupe informatique interne conserve le contrôle de l'organisation sans compromettre les accords de niveau de service que le sous-traitant s'est engagé à fournir.

Structure d'un modèle d'administration informatique.

La structure du modèle d'administration informatique reflète la façon dont une organisation gère ses ressources informatiques, comme les utilisateurs, les ordinateurs, les groupes, les imprimantes et les fichiers partagés.
Les différentes manières selon lesquelles les modèles d'administration sont structurés incluent :

- *Administration basée sur l'emplacement géographique.* L'organisation informatique est centralisée, par exemple au siège, mais l'administration du réseau est distribuée géographiquement (par exemple, chaque succursale possède son propre groupe d'administration qui gère les ressources sur place).
- *Administration basée sur l'organisation.* Dans cette structure, l'organisation informatique est divisée en services ou en unités commerciales, chacun possédant son propre groupe informatique.
- *Administration basée sur une fonction business.* Une organisation informatique décentralisée base souvent son modèle d'administration sur des fonctions business dans l'organisation.
- *Administration hybride.* Cette structure associe les points forts de plusieurs modèles pour répondre aux besoins d'administration de l'organisation.

d) Consignes de planification d'une structure d'unité d'organisation

La conception d'unités d'organisation est basée sur le modèle d'administration informatique d'une organisation.

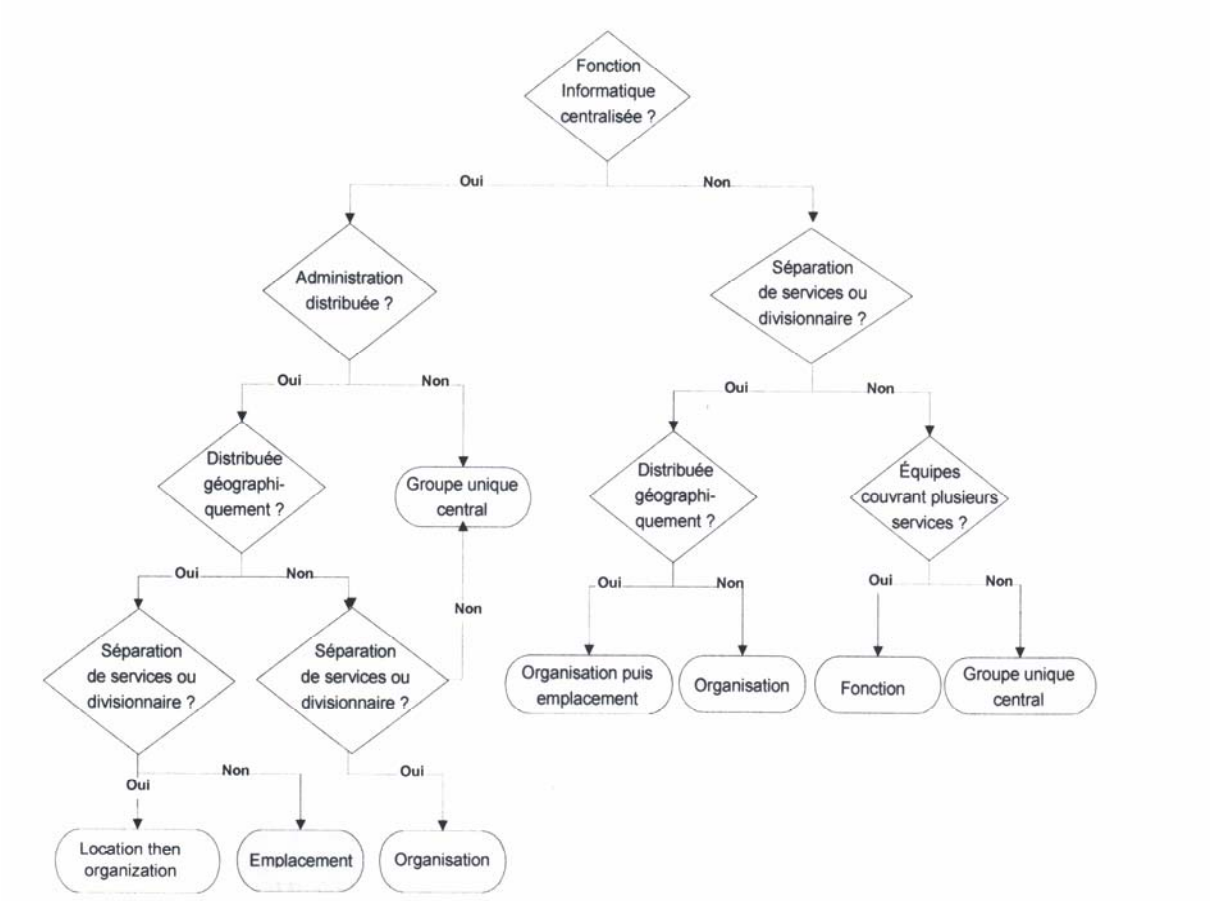
Instructions

Utilisez les consignes suivantes pour vous aider à planifier la structure d'unité d'organisation d'une organisation. La structure peut être basée sur :

- *L'emplacement géographique.* Si le modèle d'administration est distribué géographiquement et si des administrateurs sont présents dans chaque emplacement, organisez la structure d'Active Directory par emplacement.
- *L'organisation.* Si l'administration informatique est basée par service ou par division, concevez Active Directory en fonction de la structure de l'organisation. Vérifiez que vous respectez bien la structure d'administration, plutôt que l'organigramme, lorsque vous vous basez sur l'organisation. Il se peut que l'organigramme ne corresponde pas aux besoins d'administration d'une organisation.

- *Les fonctions business.* Si l'administration informatique est décentralisée, concevez la structure d'Active Directory en vous basant sur les fonctions de l'organisation. Ne choisissez cette approche que si la fonction informatique n'est pas basée sur l'emplacement ou l'organisation. Cette structure est idéale (c'est la mieux appropriée) pour de petites organisations avec des responsabilités professionnelles couvrant plusieurs services.
- *Le modèle hybride.* Dans le cas d'une organisation fortement distribuée avec une fonction informatique centralisée et une forte séparation de services ou divisionnaire, concevez les unités ou les domaines de niveau supérieure par emplacement et les niveaux inférieurs par organisation. Comme les niveaux les plus élevés sont basés sur l'emplacement, ce modèle est le moins susceptible d'être modifié et, par conséquent, moins susceptible d'exiger un effort important lors d'une réorganisation.

Utilisez le diagramme suivant comme arborescence de décision pour déterminer la structure d'unité d'organisation appropriée pour une organisation.



e) Consignes pour la délégation du contrôle administratif.

Déléguez autant que possible le droit d'octroyer des autorisations afin de limiter les coûts et les difficultés d'administration et, par conséquent, réduire le coût total de possession. Avant d'affecter des autorisations aux utilisateurs dans une organisation, vous devez déterminer qui peut et ne peut pas accéder à un objet et à son contenu, ainsi que le type d'accès dont une personne peut ou non disposer.

Instructions

Tenez compte des consignes suivantes lorsque vous planifiez la délégation du contrôle administratif dans votre organisation :

- *Affectez le contrôle au niveau le plus élevé possible d'unité d'organisation et utilisez la fonction d'héritage.* Vous pouvez ensuite gérer les autorisations de manière plus efficace. Cela crée un journal d'audit plus simple et réduit les risques d'incident si un administrateur commet une erreur alors qu'il a ouvert une session avec un compte administrateur.
- *Evitez d'affecter des autorisations au niveau propriétés ou tâche afin de simplifier l'administration.* Envisager de placer des objet dans les unités d'organisation séparées selon la manière dont ils seront gérés, plutôt que de gérer les propriétés à l'aide de listes de contrôle d'accès discrétionnaire (DACL, *Discretionary Access Control List)* distinctes pour objets dans une unité d'organisation unique.

  Lors de l'affectation d'autorisations, exécutez les tâches suivantes :
  - Déléguez à des utilisateurs ou à des groupes d'utilisateurs le droit d'affecter des autorisations de contrôle d'accès à des objets. En d'autres termes, déléguez le droit de déléguer.
  - Affectez des autorisations courantes ou spéciales sur des objets.
  - Utilisez la fonction d'héritage pour permettre le transfert des autorisations de contrôle d'accès aux objets enfants. Parfois, cependant, vous devrez bloquer l'héritage pour éviter qu'un objet enfant n'hérite des autorisations définies sur l'objet parent. Le blocage de l'héritage rend difficile la documentation et le dépannage des autorisations sur un objet. Par conséquent, évitez d'y avoir recours.

- *Affectez des autorisations d'accès à des groupes, plutôt qu'à des individus.* Les autorisations de groupe simplifient l'actualisation des DACL sur les réseaux comportant de nombreux utilisateurs et objets. Par ailleurs, l'affectation d'autorisations à des groupes est une puissante fonctionnalité car elle vous permet d'imbriquer des groupes, ce qui réduit le nombre total d'objets à gérer.
- *Minimisez le nombre d'administrateurs de domaine.* Le groupe Admins du domaine possède des droits spéciaux dans un domaine, comme celui de s'approprier tout objet et de définir des stratégies de sécurité pour tout le domaine. Lorsque vous souhaitez contrôler étroitement les privilèges de l'administrateur de domaine, accordez des droits d'administration aux utilisateurs pour les diverses unités d'organisation et limitez l'appartenance dans le groupe Admins du domaine.

Rmq : Pour plus d'informations sur la délégation du contrôle, consulter le Guide de planification et de déploiement Windows Srver 2003 à l'adresse http://www.microsoft.com/reskit

Module 4 : Implémentation de comptes d'utilisateurs, de groupes et d'ordinateurs

Types de comptes

On peut créer 3 types de comptes dans Active Directory :

- **Comptes d'utilisateurs**

C'est un objet stocké dans Active Directory qui permet une ouverture de session unique pour un utilisateur qui obtient donc l'accès aux ressources .Il y a 3 types de comptes d'utilisateurs, chacun ayant une fonction spécifique :

- *Un compte d'utilisateur local* permet à un utilisateur d'ouvrir une session sur un ordinateur spécifique pour accéder aux ressources sur cet ordinateur.

- *Un compte d'utilisateur de domaine* permet à un utilisateur de se connecter au domaine pour accéder aux ressources réseaux ou à un ordinateur individuel pour accéder aux ressources sur cet ordinateur.

- *Un compte d'utilisateur intégré* permet à un utilisateur d'effectuer des tâches d'administration ou d'accéder temporairement aux ressources réseau.

- **Comptes d'ordinateurs**

Chaque ordinateur éxecutant Win NT, 2000, XP ou 2003 Server qui rejoint un domaine possède un compte d'ordinateur. Celui ci permet d'authentifier et d'auditer l'accès d'un ordinateur au ressources réseau et du domaine. Chaque compte d'ordinateur doit être unique.

- **Comptes de groupes**

Un compte de groupe est un ensemble d'utilisateur, d'ordinateurs ou de groupes. Vous pouvez utiliser des groupes pour gérer efficacement l'accès aux ressources du domaine, et ainsi simplifier l'administration. Lorsque vous utilisez des groupes, vous affectez en une fois des autorisations pour des ressources partagées, telles que des dossiers et des imprimantes, à des utilisateurs individuels.

Types de groupes

Il existe 2 types de groupes : les groupes de distribution et les groupes de sécurité. Tous 2 possèdent un attribut d'étendue, qui détermine qui peut être membre du groupe et à quel endroit vous pouvez utiliser ce groupe dans un réseau. Vous pouvez convertir à tout moment un groupe de sécurité en un groupe de distribution et inversement, mais uniquement si le niveau fonctionnel de domaine est défini sur Windows 2000 ou ultérieur.

- **Groupes de distribution**

Utilisable uniquement avec des applications de messagerie telles que Microsoft Exchange, pour envoyer des messages à un ensemble d'utilisateurs.

La sécurité n'est pas activée sur les groupes de distribution, donc ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire(DACL).

- **Groupes de sécurité**

Vous pouvez utiliser des groupes de sécurité pour affecter des droits et des autorisations aux groupes d'utilisateurs et d'ordinateurs :

- Les droits déterminent les fonctions que les membres d'un groupe de sécurité peuvent effectuer dans un domaine ou une forêt.
- Les autorisations déterminent quelles ressources sont accessibles à un membre d'un groupe sur le réseau.

Une méthode d'utilisation efficace est l'imbrication, c'est à dire, ajouter un groupe à un autre groupe. Le groupe imbriqué hérite des autorisations du groupe dont il est membre, ce qui réduit le trafic que peut engendrer la réplication de l'appartenance à un groupe. Dans un domaine en mode mixte, vous ne pouvez pas imbriquer des groupes possédant la même étendue de groupe.

Les groupes de distribution et de sécurité prennent en charge l'une des trois étendues de groupe suivantes : locale de domaine, globale ou universelle. *Le niveau fonctionnel de domaine détermine le type de groupe que vous pouvez créer.*

Définition des groupes locaux de domaine

La structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications.

Les éléments de la structure physique d'Active Directory sont :

- *Les contrôleurs de domaine.* (exécute Win Server 2003 ou Win 2000 et Active Directory). Chaque contrôleur de domaine exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleur de domaine.
- *Les sites Active Directory.* Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsque vous créez des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de *latence de réplication* à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. Vous pouvez donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaine situés à des emplacements différents. (Pour plus d'infos sur les sites voir module 7).
- *Partitions Active Directory.* Chaque contrôleur de domaine contient les partitions Active Directory suivantes :
  - *La partition de domaine* contient les réplicas de tous les objets de ce domaine. La partition de domaine n'est répliquée que dans d'autres contrôleurs appartenant au même domaine.
  - *La partition de configuration* contient la topologie de la forêt. La *topologie* est un enregistrement de tous les contrôleurs de domaine et des connexions entre eux dans une forêt.
  - *La partition de schéma* contient le schéma étendu au niveau de la forêt. Chaque forêt comporte un schéma de sorte que la définition de chaque classe d'objet est cohérente. Les partitions de configurations et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.
  - *Les partitions d'applications facultatives* contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications. Les partitions d'applications sont répliquées dans des contrôleurs de domaine spécifiés dans la forêt.

b) Définitions des maîtres d'opérations

Lorsqu'un domaine est modifié, la modification est répliquée sur tous les contrôleurs du domaine. Certaines modifications, telles que celles apportées au schéma, sont répliquées dans tous les domaines de la forêt. Cette réplication est appelée *réplication multimaître.*

Opérations de maître unique

Lors d'une réplication multimaître, un conflit de réplication peut se produire si des mises à jour d'origine sont effectuées simultanément sur le même attribut d'un objet sur deux contrôleurs de domaine. Pour éviter des conflits de réplication, vous utiliserez une *réplication à maître unique*, qui désigne un contrôleur de domaine comme étant le seul sur lequel certaines modifications de l'annuaire peuvent être effectuées. Ainsi, des modifications ne peuvent intervenir simultanément sur différents endroits du réseau. Active Directory utilise une réplication à maître unique pour des modifications importantes, comme l'ajout d'un nouveau domaine ou une modification dans le schéma au niveau de la forêt.

Rôles de maître d'opérations

Les opérations utilisant une réplication à maître unique sont regroupées dans des rôles spécifiques dans une forêt ou un domaine. Ces rôles sont appelés *rôles de maître d'opérations.* Pour chaque rôle de maître d'opérations, seul le contrôleur de domaine possédant ce rôle peut effectuer les modifications dans l'annuaire correspondant. Le contrôleur de domaine responsable d'un rôle particulier est appelé *maître d'opérations* pour ce rôle. Active directory stocke les informations concernant le contrôleur de domaine qui joue un rôle spécifique.
Active Directory définit cinq rôles de maître d'opérations, chacun possédant un emplacement par défaut. Les rôles de maître d'opérations s'étendent au niveau d'une forêt ou d'un domaine.

- *Rôles étendus au niveau d'une forêt :*

    - *Le contrôleur de schéma.* Il contrôle toutes les mises à jour du schéma. Le schéma contient la liste principale des classes et des attributs d'objets utilisés pour créer tous les objets Active Directory, comme les utilisateurs, les ordinateurs et les imprimantes.
    - *Le maître d'attribution des noms de domaine.* Il contrôle l'ajout ou la suppression de domaine dans une forêt. Lorsque vous ajoutez un domaine à la forêt, seul le contrôleur de domaine possédant le rôle de maître d'attribution des noms de domaine peut ajouter le nouveau domaine.

  L'ensemble de la forêt ne contient qu'un seul contrôleur de schéma et qu'un seul maître d'attribution des noms de domaine.

- *Rôles étendus au niveau d'un domaine :*

    - *L'émulateur de contrôleur principal de domaine (PDC, Primary Domain Controller)*. Il se comporte comme un contrôleur principal de domaine Win NT pour la prise en charge de tout contrôleur secondaire de domaine *(BDC, Backup Domain Controller)* exécutant Win NT au sein d'un *domaine en mode mixte*. Ce type de domaine possède des contrôleurs de domaine exécutant Win NT 4.0. L'émulateur PDC est le premier contrôleur de domaine que vous créez dans un nouveau domaine.

    - *Le maître des identificateurs relatifs (maître RID).* Lorsqu'un nouvel objet est créé, le contrôleur de domaine crée une nouvelle entité de sécurité qui représente l'objet et auquel un identificateur de sécurité (SID, Security IDentifier) unique. Cet identificateur consiste en un identificateur de sécurité de domaine, qui est le même pour toutes les entités de sécurité créées dans le domaine, et en un identificateur relatif (RID, Relative IDentifier) qui est unique pour chaque unités de sécurité créées dans le domaine. Le maître RID alloue des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Le contrôleur de domaine affecte ensuite un maître RID aux objets créés à partir de son bloc de maîtres RID alloués.

- *Le maître d'infrastructure.* Lorsque des objets sont déplacés d'un domaine vers un autre, le maître d'infrastructure met à jour dans son domaine les références d'objets qui pointent sur l'objet dans l'autre domaine. La référence d'objet contient l'identificateur global unique (GUID, Globally Unique IDentifier) de l'objet, son nom unique, et un identificateur de sécurité. Active Directory met régulièrement à jour le nom unique et l'identificateur de sécurité sur la référence d'objet afin de refléter les modifications apportées à l'objet réel.

Dans une forêt, chaque domaine possède ses propres émulateur PDC, maître RID et maître d'infrastructure.
(Pour plus d'infos sur les rôles de maître d'opérations voir module 9)

Définition d'un catalogue global.

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparentes pour l'utilisateur. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Définition du catalogue global.

Le *catalogue global* est un référentiel d'informations qui contient un sous-ensemble des attributs de tous les objets d'Active Directory. Les membres du groupe Administrateurs du schéma peuvent modifier les attributs stockés dans le catalogue global, en fonction des impératifs d'une organisation. Le catalogue global contient :

- Les attributs les plus fréquemment utilisés dans les requêtes, comme les nom et prénom d'un utilisateur, et son nom d'ouverture de session ;
- Les informations requises pour déterminer l'emplacement de tout objet dans l'annuaire ;
- Un sous-ensemble d'attributs par défaut pour chaque type d'objet ;
- Les autorisations d'accès pour chaque objet et attribut stocké dans le catalogue global. Si vous recherchez un objet pour lequel vous ne possédez pas les autorisations de visualisation requises, cet objet n'apparaîtra pas dans les résultats de la recherche. Les autorisations d'accès garantissent que les utilisateurs ne puissent trouver que les objets pour lesquels ils possèdent un droit d'accès.

Définition d'un serveur de catalogue global.

Un *serveur de catalogue global* est un contrôleur de domaine qui traite efficacement les requêtes intraforêts dans le catalogue global. Le premier contrôleur de domaine que vous créez dans Active Directory devient automatiquement un serveur de catalogue global. Vous pouvez configurer des serveurs de catalogue global supplémentaires pour équilibrer le trafic lié aux authentifications de connexion et aux requêtes.

Fonctions du catalogue global.

Le catalogue global permet aux utilisateurs d'exécuter deux fonctions importantes :

- Trouver les informations Active Directory en tout point de la forêt, indépendamment de l'emplacement des données ;
- Utiliser les informations d'appartenance au groupe universel pour se connecter au réseau.

Définition de groupes locaux de domaines

- Introduction

Un groupe local de domaine est un groupe de sécurité ou de distribution qui peut contenir des groupes universels, des groupes globaux ou d'autres groupes locaux de domaines issus de ses propres domaines et comptes dans la forêt. Dans les groupes de sécurité locaux de domaine, vous pouvez accorder des droits et autorisations sur des ressources qui résident uniquement dans le même domaine que celui où se trouve le groupe local de domaine.

Par exemple, vous pouvez créer un groupe de sécurité local nommé Setup et accorder des autorisations de groupes à un partage nommé Setup sur l'un des serveurs membres du domaine. Vous pouvez ajouter des groupes globaux ou universels en tant que membres du groupe local de domaine Setup. Les membres auront alors l'autorisation d'accéder au dossier partagé Setup.

- Appartenance au groupe local de domaine, étendues et autorisation

Les règles suivantes s'appliquent à l'appartenance au groupe local de domaine, ainsi qu'à l'étendue et aux autorisations du groupe local de domaine :

- Appartenance. En mode Windows 2000 mixte, les groupes locaux de domaine peuvent contenir des comptes utilisateurs et des groupes globaux de n'importe quel domaine. En mode Windows 2000 natif, les groupes de domaine peuvent contenir des comptes utilisateur, des groupes globaux, des groupes universels de n'importe quel domaine approuvé et des groupes locaux issus du même domaine
- Peut être membre de. En mode Windows 2000 mixte, un groupe local de domaine ne peut pas être membre de n'importe quel groupe. En mode Windows 2000 natif, un groupe local de domaine peut être membre de groupes locaux de domaine issus du même domaine.
- Etendue. Un groupe local de domaine est visible uniquement dans son propre domaine.
- Autorisation. Vous pouvez affecter une autorisation qui s'applique au domaine dans lequel le groupe local de domaine existe.

- A quel moment utiliser des groupes locaux de domaine

Utiliser un groupe local de domaine lorsque vous souhaitez affecter des autorisations d'accès à des ressources qui se situent dans le même domaine que celui dans lequel vous créez le groupe local de domaine. Vous pouvez ajouter des groupes globaux partageant les mêmes ressources au groupe local de domaine approprié.

Définition de groupes globaux

- Introduction

Un groupe global est un groupe de sécurité ou de distribution qui peut contenir des utilisateurs, des groupes et des ordinateurs comme membres de son propre domaine. Vous pouvez accorder des droits et autorisations à des groupes de sécurité globaux pour des ressources situées dans n'importe quel domaine de la forêt.

Utilisez un groupe global pour organiser des utilisateurs qui partagent les mêmes tâches professionnelles et ont des conditions d'accès similaires, tels que tous les comptables du service comptabilité d'une organisation.

- Appartenance au groupe global, étendues et autorisation

Les règles suivantes s'appliquent à l'appartenance au groupe global , ainsi qu'à l'étendue et aux autorisations du groupe global :

- Appartenance. En mode Windows 2000 mixte, un groupe global peut contenir des comptes utilisateurs du même domaine. En mode Windows 2000 natif et en mode Windows Server 2003, les groupes globaux peuvent contenir des comptes utilisateur et des groupes globaux issus du même domaine

- Peut être membre de. En mode Windows 2000 mixte, un groupe global peut être membre des groupes locaux de domaine dans n'importe quel groupe approuvé. En mode Windows 2000 natif et en mode Windows Server 2003, un groupe global peut être membre de groupes universels et de groupes locaux de domaine dans n'importe quel domaine et être également membres de groupes globaux dans le même domaine même domaine.
- Etendue. Un groupe global est visible dans son domaine et tous les domaines approuvés, ce qui inclut tous les domaines de la forêt.
- Autorisation. Vous pouvez affecter une autorisation à un groupe global qui s'applique à tous les domaines approuvés.

- A quel moment utiliser des groupes globaux

Les groupes globaux étant visibles dans toute la forêt, ne les créez pas dans le but de permettre aux utilisateurs d'accéder à des ressources spécifiques à un domaine. Utilisez les groupes globaux pour organiser des utilisateurs ou des groupes d'utilisateurs. Un groupe local de domaine est plus approprié pour contrôler l'accès d'un utilisateur aux ressources situées dans un domaine unique.

Définition de groupes universels

- Introduction

Un groupe universel est un groupe de sécurité ou de distribution qui peut contenir des utilisateurs, des groupes et des ordinateurs comme menbres d'un domaine d'une forêt. Les groupes de sécurité universel peuvent bénéficier de droits et autorisations sur des ressources situées dans n'importe quel domaine de la forêt.

- Appartenance au groupe universel, étendue et autorisations

Les règles suivantes s'appliquent à l'appartenance au groupe universel, ainsi qu'à l'étendue et aux autorisations du groupe universel :

- Appartenance. Vous ne pouvez pas créer de groupes de sécurité universels en mode Windows 2000 mixte. En mode Windows 2000 natif et en mode Windows Server 2003, des groupes universels peuvent contenir des comptes utilisateur, des groupes globaux, et d'autres groupes universels de n'importe quel domaine de la forêt.

- Peut être membre de. Le groupe universel ne s'applique pas au mode Windows 2000 mixte. En mode Windows 2000 natif, un groupe universel peut être membre de groupes locaux de domaine et de groupes universels de n'importe quel domaine.
- Etendue. Les groupes universels sont visibles dans tous les domaines de la forêt.
- Autorisations. Vous pouvez affecter une autorisation à un groupe universel qui s'applique à tous les domaines de la forêt.

- A quel moment utiliser des groupes locaux de domaine

Utilisez les groupes universels lorsque vous souhaitez imbriquer des groupes globaux. De cette manière, vous pouvez affecter des autorisations aux ressources connexes dans plusieurs domaines. Un domaine Windows Server 2003 doit être en mode Windows 2000 natif ou en mode Windows 2003 Server pour utiliser des groupes de sécurité universels. Vous pouvez utiliser des groupes de distribution universels dans un domaine Windows 2003 Server en mode Windows 2000 mixte ou ultérieur.

Création et gestion de plusieurs comptes

- Introduction

Windows Server 2003 procure de nombreux outils et composants logiciels enfichables MMC (Microsoft Management Console) pour créer automatiquement plusieurs comptes d'utilisateurs dans AD. Certains de ces outils nécessitent l'utilisation d'un fichier texte qui contient des informations sur les comptes d'utilisateurs que vous souhaitez créer. Vous pouvez également gréer des scripts pour ajouter ou modifier des objets dans AD.

- Utilisateurs et ordinateurs AD

La console utilisateurs et ordinateurs Active Directory est un composant logiciel enfichable MMC que vous pouvez utiliser pour gérer des comptes d'utilisateurs, d'ordinateurs et de groupes. Il convient de l'utiliser lorsque vous gérez un petit nombre de comptes.

- Outils de service d'annuaire

Vous pouvez également utiliser les outils de lignes de commande Dsadd, Dsmod et Dsrm pour gérer des comptes d'utilisateurs, d'ordinateurs et de groupes dans AD. Vous devez spécifier le type d'objet que vous souhaitez créer, modifier ou supprimer. Par exemple, utilisez la commande dsadd user pour créer un compte utilisateur. Utilisez la commande dsrm group pour supprimer un compte de groupe. Bien que les outils Directory Service permettent de créer un seul objet AD à la fois, vous pouvez les utiliser dans des fichiers de commandes et des scripts.

- Outil Csvde

L'outil de ligne de commande Csvde utilise un fichier texte séparé par des virgules, également appelé format valeurs séparées par des virgules (format Csvde), comme entrée pour créer plusieurs comptes dans AD.

Vous devez utiliser le format Csvde pour ajouter des objets utilisateur et d'autres types d'objets à AD. Vous ne pouvez pas utiliser le format Csvde pour modifier ou supprimer des objets dans Active Directory. Avant d'importer un fichier Csvde, assurez vous que le fichier est correctement formaté. Le fichier d'entrée :

- doit inclure le chemin d'accès au compte utilisateur dans Active Directory, le type d'objet, qui est le compte utilisateur, et le nom d'ouverture de session de l'utilisateur (pour Win NT 4.0 et ultérieur) ;

- doit inclure le suffixe UPN (user principal name) et indiquer si le compte d'utilisateur est activé ou non. Si aucune valeur, compte supprimé.
- Peut inclure des infos personnelles (num tel, adresse) .Incluez autant d'info que possible pour faciliter les recherches dans AD.

Ne peut pas inclure de mots de passe. Une importation en bloc laisse le mot de passe vide donc n'importe qui peut se connecter avec juste le nom d'utilisateur. Activez les comptes juste avant la connexion des utilisateurs.

- Outil Ldifde

Outil utilisant un format à valeurs séparées par des lignes pour créer, modifier ou supprimer des objets. Facilement importable d'une application de base de données car format identique. Même fichier d'entrée que Csvde.

- Environnement de scripts Windows

On peut créer des scripts qui utilisent des interfaces ADSI pour créer, modifier, supprimer des objets. Utiliser de préférence pour changer les attributs de plusieurs objets.

Implémentation des suffixes UPN

Définition d'un nom d'utilisateur principal

C'est un nom d'ouverture de session utilisé uniquement pour la connexion sur un réseau Win server 2003. ex : Haludo@contoso.msft.

- Avantages : - Nom unique dans AD
  - Peut être identique à une adresse de messagerie
- Règles d'unicité des noms d'ouverture de session

  - Le nom complet doit être unique dans son conteneur et dans la forêt.
  - Le nom d'utilisateur doit être unique dans la forêt

Détection et résolution des conflits de suffixes de noms

- Un conflit de suffixes de noms se produit quand :

  - Un nom de DNS déjà utilisé
  - Un nom NetBios déjà utilisé
  - Un SID de domaine est en conflit avec un autre SID

Les conflits de suffixes de noms dans un domaine empêchent l'accès à ce domaine depuis l'extérieur de la forêt. L'accès inter-forêt est toujours possible.

Déplacement d'objets dans AD

Définition de l'historique SID

- Rôles de l'historique SID

    - Liste de tous les identificateurs SID affectés à un compte utilisateur
    - Fournit un compte d'utilisateur migré avec un accès continu aux ressources

Implications du déplacement d'objets

- Dans un domaine :

    - Pas de changement de SID ou de GUID

- Dans une forêt

    - Nouveau SID
    - Historique SID
    - GUID identique

- Entre les fotêts
    - Nouveaus SID
    - Historique SID
    - Nouvel identificateur GUID

- Implications sur la sécurité d'un historique SID

Un historique SID permet à des utilisateurs migrés d'accéder aux ressources situées dans leurs anciens domaines. Cependant, il permet aussi aux utilisateurs de tromper l'accès aux autres domaines, càd donner l'illusion qu'une transmission provient d'un utilisateur autorisé, en plaçant des SID d'autres domaines dans l'historique SID de leurs comptes d'utilisateurs. On peut se protéger de tels comportements en appliquant un filtrage des identificateurs SID aux relations approuvées.

- Autres applications de déplacement d'objets

    - Les comptes d'utilisateurs qui ont des privilèges administratifs pour l'OU vers laquelle le compte est déplacé
    - Les restrictions liées à la stratégie de groupe de l'OU, du domaine ou du site depuis lequel le compte d'utilisateur a été déplacé ne s'appliquent plus au compte d'utilisateur
    - Les paramètres de stratégie de groupe du nouvel emplacement s'appliquent au compte d'utilisateur

Planification d'une stratégie de compte d'utilisateur, de groupe et d'ordinateur

Instruction d'attribution des noms de comptes

- Définir des conventions d'attribution de nom pour :
    - Les noms de comptes utilisateur qui identifient l'utilisateur
    - Les noms d'ordinateur qui identifient le propriétaire, l'emplacement et le type d'ordinateurs
    - Les noms de groupe qui identifient le type de groupe, l'emplacement et la fonction du groupe

Instruction de définitions d'une stratégie de mots de passe

L e mot de passe constitue la première ligne de défense en cas d'accès non-autorisés à votre organisation. Stratégie :

- Paramétrez l'option *Conserver l'historique des mots de passe* sur un minimum de 24 mots de passes retenus.
- Définissez la durée de vie maximale du mot de passe sur 42 jours.
- Définissez la durée de vie minimale du mot de passe sur 2 jours.
- Définissez la longueur du mot de passe sur 8 caractères maximum.
- Activer l'option *Le mot de passe doit respecter des exigences de sécurité* .

Instruction d'authentification, d'autorisation et d'administration des comptes

Cette stratégie aidera à protéger le réseau de l'organisation.
On utilise les instructions suivantes pour authentifier, autoriser et administrer des comptes dans votre organisation :

- Attribuez une valeur élevée au paramètre de stratégie seuil de verrouillage de compte
- Eviter d'utiliser des comptes administrateurs pour répondre au besoin informatiques de routines.
- Utilisez une authentification multifactorielle
- Utilisez des groupes de sécurité basées sur la stratégie C-G-U-LD-A.
- Désactivez le compte administrateur et affectez aux utilisateurs et administrateurs le moindre privilège nécessaire pour affecter leurs tâches professionnelles.

Instruction de planification d'une stratégie de groupe

La planification d'une stratégie de groupe implique la planification de l'utilisation des groupes globaux, groupes locaux de domaine et groupes universels pour simplifier les tâches d'administration. On utilise les instructions suivantes pour planifier une stratégie de groupe :

- Affectez les utilisateurs aux responsabilités professionnelles commune aux groupes globaux
- Créez un groupe local de domaine pour partager les ressources.
- Ajoutez aux groupes locaux de domaine des groupes globaux qui exigent un accès aux ressources.
- Utilisez des groupes universels pour accorder l'accès aux ressources situées dans plusieurs domaines.
- Utilisez des groupes universels lorsque l'appartenance est statique.

Planification d'une stratégie d'audit AD

Pourquoi auditer l'accès à AD ?

- Pour enregistrer toutes les modification réussies dans AD.
- Pour assurer un suivi de l'accès à une ressource ou par un compte spécifique.
- Pour détecter et enregistrer les tentatives d'accès infructueuses

Instruction d'analyse des modifications apportées à AD

Des audits réussis génèrent une entrée d'audit lorsqu'un événement de gestion de comptes s'exécute avec succès. Même si les événements de gestion des comptes réussis sont généralement inoffensifs, ils fournissent un enregistrement inestimable d'activités pouvant compromettre la sécurité d'un réseau.

Utilisez ces instructions lors de la création d'une stratégie d'audit :

- Activez l'audit des événements de gestion de comptes.
- Activez l'audit des succès de modifications de stratégie
- Activez l'audit des échecs des événements système
- Activez l'audit des échecs des événements de modification de stratégie et des événements de gestion de comptes uniquement lorsque cela est nécéssaire.

MODULE 5 : Implémentation d'une stratégie de groupe

A) Introduction

L'utilisation de la stratégie de groupe dans le service d'annuaire Active Directory permet de gérer de façon centralisée les utilisateurs et les ordinateurs d'une entreprise. Vous pouvez centraliser les stratégies en définissant une stratégie de groupe pour toute une organisation au niveau du domaine du site ou au niveau d une unité d'organisation (OU) . Ou bien vous pouvez décentraliser les paramètres de stratégie de groupe en définissant une stratégie de groupe pour chaque service au niveau d'une unité d'organisation.

Ainsi vous pouvez vous assurer que chaque utilisateurs dispose de l'environnement utilisateur dont il a besoin , tout en appliquant les stratégies de l'organisation ,notamment en matière de sécurité . Par ailleurs vous pouvez abaissez le coût total de possession en contrôlant les environnements utilisateurs et les ordinateurs et en réduisant de ce fait le niveau de support technique nécessaire aux utilisateurs et la perte de productivité qui en découle .

B) Création et configuration d'objets stratégie de groupe

La stratégie de groupe vous donne le contrôle administratif sur les utilisateurs et les ordinateurs de votre réseau. L'utilisation d'une stratégie de groupe vous permet de définir une seule fois l'état de l'environnement de travail d'un utilisateur et d'appliquer ces paramètres à une organisation entière ou à des groupes spécifiques d'utilisateurs et d'ordinateurs.

- Introduction aux stratégie de groupe

1. Types de paramètres

Vous pouvez configurer différents paramètres de stratégie de groupe pour définir les stratégies affectant les utilisateurs et les ordinateurs :

Modèles d'administrations : Paramètres basés sur le Registre permettant de configurer les paramètres d'applications et les environnements de stations de travail utilisateur .
Scripts : Paramètres permettant de spécifier quand Serveur 2003 exécute des scripts spécifiques .
Services d'installation à distance : Paramètres qui contrôlent les options dont disposent les utilisateurs lorsqu'ils exécutent l'assistant installation client utilisé par les services d'installation à distance (RIS ,Remote Installation Service) .
Maintenance Internet Explorer : Paramètres permettant d'administrer et de personnaliser I.E. sur des ordinateurs exécutant 2003 Serveur.
Redirections des dossiers : Paramètres permettant de stocker des dossier de profils d'utilisateurs spécifiques sur un serveur réseau .
Sécurité : Paramètre permettant de configurer la sécurité des ordinateurs locaux, du domaine et du réseau.
Installation des logiciels : paramètre permettant de centraliser la gestion de installations, des mises à jour et des suppressions de logiciels.

2. Flux d'héritage

   Les GPO (Group Policy Object = Objet de stratégie de groupe) sont liés à des sites , des domaines ou des OU (Organisation Unit) . Un objets GPO associé à un domaine s'applique également aux utilisateurs et au ordinateurs qui se trouve dans les unité d'organisations figurant dans ce domaine. Une stratégie de groupe est transmise de l'unité d'organisation parent à l'unité d'organisation enfant dans un domaine mais elle ne se transmet pas d'un domaine parent à un domaine enfant. Il est possible que des paramètres de stratégie soient appliqués à un conteneur d'annuaire parents et que d'autres paramètres de stratégies soient appliqués à un une unité d'organisation enfant. Dans ce cas-là , si les paramètres « parent » et « enfant » sont compatibles , ils sont tous les deux appliqués . Si il ne sont pas compatible , l'unité d'organisation enfant n'hérite d'aucun paramètres et seuls ses paramètres sont appliqués.

3. Ordre de traitement des GPO

   Ces objet sont appliqués dans un ordre correspondant à la nature hiérarchique d'Active Directory . L'ordre de priorité par défaut est site , domaine et unité d'organisation.

4. Paramètres des GPO à valeurs multiples

   Certains paramètres sont à valeurs multiples . Ceux-ci sont traités comme des paramètres à valeurs simples c'est à dire que si le paramètre est défini dans plusieurs objets stratégie de groupe seuls les paramètres de l'un des objets stratégie de groupe observant les règles de l'héritage sont appliqués .

5. Fonctions avancées

   - *Blocage de l'héritage :* Vous pouvez empêcher un conteneur d'hériter de tous les objets stratégie de groupe de ses conteneurs parents en activant le blocage de l'héritage pour le conteneur enfant.
   - *Option Appliqué (ou ne pas passer outre) :* Cette option force tous les conteneurs enfant à hériter de la stratégie du parent même si celle-ci est en conflit avec la stratégie du conteneur enfant et que l'option « bloquer l'héritage » n'a pas été configurer pour l'enfant. Si un objet stratégie de groupe est lié à plusieurs conteneurs , vous pouvez configurer l'option « Appliqué » individuellement pour chaque conteneur car cette option est un attribut de liaison et non un attribut de l'objet stratégie de groupe .

6. Filtrer des objets GPO

   En définissant les autorisations appropriées pour les groupes de sécurité, vous pouvez filtrer la stratégie de groupe pou qu'elle s'applique uniquement aux ordinateurs et aux utilisateurs spécifiés .

- Composant d'un objet stratégie de groupe

1) Conteneur stratégie de groupe (GPC,Group Policy Container)

Le conteneur stratégie de groupe est un objet Active Directory qui contient l'état de l'objet stratégie de groupe , les informations de version, les informations de filtres WMI et une liste de composants dont les paramètres se trouvent dans l'objet stratégie de groupe . Les ordinateurs peuvent y accéder pour localiser des modèles Stratégie de groupe et les contrôleurs de domaines y accèdent pour obtenir des informations de version (qui est directement remplacé si la version n'est plus à jour) .

2) Modèle Stratégie de groupe (GPT,Group Policy Template)

C'est une arborescence de dossiers situé dans le dossier partagé SYSVOL d'un contrôleur de domaine. Lorsque qu'un objet Stratégie de groupe est créé , un modèle Stratégie de groupe correspondant est également créé .Il contient tous les paramètres et informations Stratégie de groupe correspondant (modèle d'administration, sécurité, installation de logiciels, scripts et redirection des dossiers) . Les ordinateurs se connecte au dossier SYSVOL pour obtenir ces paramètres.

- Gestion des objets Stratégie de groupe

Il est recommandé de spécifier un contrôleur de domaine pour la gestion des objets Stratégie de groupe pour éviter tout risque de conflit de réplication . En effet si deux administrateurs modifient simultanément un même objet Stratégie de groupe sur des contrôleurs de domaine différents , les modifications de l'un des administrateurs risquent de remplacer celles de l'autre . Il est d'autant plus conseillé de spécifier un contrôleur de domaine pour cette gestion quand on sait que les données concernant les objets Stratégie de groupe sont présente à la fois dans Active Directory et dans le dossier SYSVOL du contrôleur de domaine.

Emulateur PDC(Primary Domain Controler) :

Par défaut , la console de gestion de stratégie de groupe utilise l'émulateur PDC de chaque domaine pour garantir que tous les administrateurs utilisent le même contrôleur de domaine mais vous pouvez très bien cibler un autre contrôleur de domaine si vous en estimez l'utilité grâce à l'option « Modifier le contrôleur de domaine » .

- Définition des filtres WMI

On utilise des filtres WMI pour déterminer de façon dynamique l'étendue des objets Stratégie de groupe à partir des attributs de l'utilisateur ou de l'ordinateur .

Un filtre WMI est lié à un objet Stratégie de groupe . Lorsque vous appliquez un objet Stratégie de groupe à l'ordinateur de destination , Active Directory évalue le filtre sur l'ordinateur de destination . Un filtre WMI d'une ou de plusieurs requêtes évaluées par Active Directory en fonction de l'espace de stockage WMI de l'ordinateur de destination .Si la valeur totale des requêtes est FALSE , l'objet Stratégie de groupe n'est pas appliqué . Par contre si elle est TRUE, Active Directory applique l'objet Stratégie de groupe .Les requêtes sont exprimées en langage WQL(WMI Query Language) similaire au langage SQL. Chaque objet Stratégie de groupe ne peut comporter qu'un seul filtre . Par contre un filtre WMI peut être lié à plusieurs objets Stratégie de groupe.

Quelques exemples d'utilisations des filtres WMI :

*Services :*Ordinateurs sur lequel DHCP est installé et en cours d'exécution .
Inventaire matériel : Ordinateurs équipés q'un processeur PentiumIII et d'au moins 128 Mo de mémoire vive.
*Configuration logicielle :*Ordinateurs sur lesquels la multidiffusion est activée.

Pour les ordinateurs clients exécutant Windows 2000, Active Directory ignore les filtres WMI et applique toujours l'objet Stratégie de groupe .

- Définition du traitement par boucle de rappel

Par défaut , les objets Stratégie de groupe d'un utilisateur déterminent les paramètres à appliquer lors d'une ouverture de session de cet utilisateur . En revanche , le traitement par boucle de rappel permet d'appliquer l'ensemble des objets Stratégie de groupe de l'ordinateur à tout utilisateur qui ouvre une session sur l'ordinateur affecté par ce paramètre . Ce paramètre est bien utile dans le cas où l'ordinateur est ,par exemple, placé dans un endroit public.

Il y a deux modes de traitement des boucles de rappel :
Mode de remplacement : Ce mode remplace les paramètres utilisateur définis dans les objets Stratégie de groupe de l'ordinateur par les paramètres utilisateurs habituellement appliqués à l'utilisateur (? ,module 5 page 15 , ça me paraît bizarre ça devrait être l'inverse , à verifier).
Mode de fusion : Ce mode combine les paramètres utilisateurs définis dans les objets Stratégie de groupe de l'ordinateurs avec les paramètres utilisateur habituellement appliqué à l'utilisateur . En cas de conflits , Les paramètres utilisateurs des objets Stratégie de groupe de l'ordinateurs sont prioritaires.

C) Configuration des fréquences d'actualisation et des paramètres de stratégie de groupe

Windows 2003 Serveur exécute les paramètres et les stratégies d'ordinateur et d'utilisateur selon un ordre spécifique . Comprendre le traitement des stratégies de groupe et leur ordre de traitement vous permettra de créer les scripts approprié et de configurer les fréquences d'actualisation.

- A quel moment la stratégie de groupe est elle appliquée ?

Lorsqu'un utilisateur démarre un ordinateur et ouvre une session , 2003 Serveur traite d'abord les paramètres de l'ordinateur et ensuite les paramètres de l'utilisateur.

Voici les différentes action qui s'exécutent :

1) Démarrage du réseau ,du service RPCSS(Remote Procedure Call System Service) et du MUP (Multiple Universal Naming Convention Provider) .

2) 2003 Serveur obtient la liste classée des objets Stratégie de groupe pour l'ordinateur selon les facteurs suivant :
   - Est ce que l'ordinateur fait partie d'un domaine ? Si oui , il est sujet à la stratégie de groupe vie Active Directory.
   - L'emplacement de l'ordinateur dans Active Directory.
   - La liste des objets Stratégie de groupe a-t-elle été modifiée ?

3) Windows applique la stratégie de l'ordinateur c'est à dire les paramètres se trouvant sous Configuration de l'ordinateur dans le liste des objets Stratégie de groupe obtenue. Cette liste s'affiche dans l'ordre suivant :local, domaine, unité d'organisation, unité d'organisation enfant . Pendant ce traitement ,il n'y a aucune interface utilisateur.

4) Les scripts de démarrage s'exécutent les uns après les autres . On peut modifier les paramètre d'exécution de ces scripts dans les paramètres de stratégie de groupe (Par défaut ,ces scripts sont masqué et synchrone(?))

5) Ouverture de session de l'utilisateur (CTR-ALT-DELETE)

6) 2003 Serveur charge le profil de l'utilisateur , lequel est controlé par les paramètre de stratégie de groupe en vigueur

7) 2003 Serveur obtient la liste classée des objets Stratégie de groupe pour l'utilisateur selon les facteurs suivant :
   - Est ce que l'utilisateur fait partie d'un domaine ? Si oui , il est sujet à la stratégie de groupe vie Active Directory.
   - Le traitement par boucle de rappel est il activé ? Quel est l'état du paramètre de stratégie de bouclage ?
   - L'emplacement de l'utilisateur dans Active Directory.
   - La liste des objets Stratégie de groupe a-t-elle été modifiée ?

8) Windows applique la stratégie de l'utilisateur c'est à dire les paramètres se trouvant sous Configuration de l'ordinateur dans le liste des objets Stratégie de groupe obtenue. Cette liste s'affiche dans l'ordre suivant :local, domaine, unité d'organisation, unité d'organisation enfant . Pendant ce traitement ,il n'y a aucune interface utilisateur.

9) Les scripts d'ouverture de session s'exécutent (Par défaut ,ces scripts sont masqué et asynchrone(?))

10) L'interface utilisateur du SE prescrite par la stratégie de groupe s'affiche.

Les ordinateurs exécutant 2003 serveur actualisent et réappliquent les paramètres de stratégie de groupe à intervalles définis ce qui permet d'assurer que les paramètres sont toujours appliqués aux ordinateurs et aux utilisateurs même si ceux-ci ne redémarrent jamais ou ne ferment jamais leur session. (Pour la configuration des paramètres de scripts, de fréquence d'actualisation et pour l'utilisation de Gpupdate.exe : voir page 22 à 29 du module 5 (j'avoue j'ai pas envie de tout retaper et puis ça m'a pas l'air super important à étudier par cœur !))

D) Gestion des objets Stratégie de groupe .

Vous pouvez utiliser la console Gestion de stratégie de groupe pour gérer les objets Stratégie de groupe , à savoir pou copier un objet Stratégie de groupe à un autre emplacement, sauvegarder un objet Stratégie de groupe , restaurer un objet Stratégie de groupe à partir de la sauvegarde ou encore importer dans un objet Stratégie de groupe les paramètres d'un autre objet Stratégie de groupe.

- Opération de copie

La copie d'un objet Stratégie de groupe transfert uniquement les paramètres de l'objet Stratégie de groupe . Le nouvel objet possède un nouvel identificateur unique global (GUID, Globally Unique IDentifier) et de la liste de contrôle d'accès discrétionnaire (DACL , Discretionary Access Control List)de l'objet Stratégie de groupe copié . Le nouvel objet est créé mais pas lié car les liaisons sont une propriété de l'objet ayant défini l'objet Stratégie de groupe plutot qu'une propriété de l'objet Stratégie de groupe.

Le mappage des entités de sécurité désigne le fait de modifier les paramètre se rapportant aux entités de sécurité en convertissant les valeurs des entités de sécurité de l'objet copié en fonction du nouvel objet Stratégie de groupe (emplacement,…)

La console Gestion de stratégie de groupe offre deux techniques de mappage pour la copie des objets Stratégie de groupe :

- Copie identique de l'objet source
- Utilisation d'une table de migration pour mapper de nouvelles valeurs pour le nouvel objet .

Un table de migration est un fichier texte XML spécifiant le mappage personnalisé des entités de sécurité depuis le domaine source vers le domaine destination.

- Opération de sauvegarde

Lors de la sauvegarde d'objet Stratégie de groupe , la console de Gestion exporte les données dans le fichier de votre choix et enregistre tous les fichiers de modèle Stratégie de groupe. L'objet Stratégie de groupe sauvegardé pourra par la suite être restauré (c-à-d restauré dans le domaine où il a été créé) ou importé (c-à-d restauré dans un domaine différent).

Vous pouvez stockez plusieurs objets Stratégie de groupe sauvegardé (y compris plusieurs versions du même objet) dans un dossier de fichiers unique dans lequel vous pouvez identifié chaque objet par l'un des critères suivants :

- Nom complet de l'objet Stratégie de groupe
- Identificateur GUID de l'objet Stratégie de groupe
- Description de la sauvegarde
- Date et horodatage de la sauvegarde
- Nom de domaine

Remarque :Vérifiez que le répertoire des sauvegardes se trouve à un emplacement sécurisé du système de fichiers.

- Opération de restauration

Cette opération permet simplement de rétablir le contenu de l'objet Stratégie de groupe dans l'état dans lequel il était lors de la sauvegarde (possible uniquement dans le domaine où l'objet Stratégie de groupe sauvegardé a été créé). Vous pouvez restauré un objet Stratégie de groupe existant ou supprimé . Les autorisations de restauration varient selon l'existence ou non de l'objet Stratégie de groupe dans Active Directory lors de la restauration.

- Opération d'importation

Une opération d'importation copie l'ensemble des paramètres de stratégie de groupe depuis l'objet Stratégie de groupe source vers l'objet Stratégie de groupe de destination .

Il faut spécifier une table de migration afin d'être certain que le chemin UNC de l'objet Stratégie de groupe source est correctement mappé sur le chemin UNC de l'objet Stratégie de groupe de destination .

Remarque :Toutes les procédures correspondantes au opérations décrites ci-dessus sont présente dans la farde entre les pages 35 et 43 et vous expliquent comment accéder aux consoles de gestion des sauvegardes, etc…

E) Vérification et résolution des problèmes liés à la stratégie de groupe

Lors de l'implémentation d'une stratégie de groupe , il est possible que vous rencontriez quelques problèmes . Lors de la résolution de ces problèmes n'oubliez pas de prendre en compte les dépendance entre les différents composants (par exemple , la stratégie de groupe dépend de Active Directory qui lui même se base sur une configuration correcte des services réseaux .

2003 Serveur est doté de deux outils vous permettant de résoudre ces problèmes : L'Assistant Modélisation de stratégie de groupe et des Résultats des stratégie de groupe .

- Problème courant liés à l'implémentation de la stratégie de groupe

La première étapes de résolution des problèmes consiste bien sur à identifier les symptômes et les causes du problème . Dans la plupart des cas , le problème est lié à une valeur conflictuelle d'un paramètre entre deux objets Stratégie de groupe ce qui implique la stratégie de groupe ne nous donne pas l'effet escompté car dans ces cas-là c'est la stratégie prioritaire (en fonction du filtrage , du blocage de l'héritage,…) qui est appliquée .

Voici une liste de quelques symptômes et des méthodes de résolution possibles :

Symptôme	Résolution
Vous ne parvenez pas à ouvrir un objet stratégie de groupe, même avec l'autorisation en lecture	Devenez membre d'un groupe de sécurité avec les autorisations lier et écrire pour l'objet
Lorsque vous essayez de modifier un objet Stratégie de groupe, un message signalant qu'il est impossible de l'ouvrir s'affiche.	Assurez vous que le système DNS fonctionne correctement .
La stratégie de groupe n'est pas appliquée aux utilisateurs et ordinateurs d'un groupe de sécurité qui les contient, alors qu'un objet Stratégie de groupe est lié à une unité d'organisation contenant le groupe de sécurité.	Liez les objets Stratégie de groupe uniquement à de sites, domaines et unités d'organisation.
La stratégie de groupe n'affecte pas les utilisateurs et ordinateurs d'un conteneur Active Directory.	Liez un objet Stratégie de groupe à une unité d'organisation qui est parente du conteneur Active Directory . Ces paramètres sont alors appliqués par défaut aux utilisateurs et ordinateurs du conteneurs via l'héritage.
La stratégie de groupe n'est pas appliquée sur l'ordinateur client.	Déterminez quels objets Stratégie de groupe sont appliqués via Active Directory et si ces objets possèdent des paramètres en conflit avec les paramètres locaux

L'assistant Modélisation de stratégie de groupe : Cet assistant permet de simuler un déploiement de stratégie pour les utilisateurs et ordinateurs avant de réellement appliquer les stratégies. Cette fonctionnalité de la console de gestion de stratégie de groupe est appelé Jeu de stratégies résultant (RsoP, Resultant Set of Policies)-mode de planification et elle requiert un contrôleur de domaine exécutant 2003 Serveur dans la forêt.

Résultats de stratégie de groupe : On utilise les Résultats de stratégie de groupe pour déterminer les paramètres de stratégie qui sont appliqués à un ordinateurs, ainsi qu'à l'utilisateurs qui a ouvert une session sur cet ordinateur .Ces données sont directement obtenue de l'ordinateur client contrairement à la modélisation de stratégie de groupe qui les simulent. Les Résultats de stratégie de groupe sont accessible par la console Gestion de stratégie de groupe.

F) Délégation du contrôle administratif de la stratégie de groupe

Vous pouvez utiliser la stratégie de groupe pour déléguer certaines tâches à d'autres administrateurs . La console Gestion de stratégie de groupe simplifie la gestion des autorisations en combinant les autorisations de bas niveau sur un objet et en les gérant comme une seule unité. Celle-ci permet de déléguer le contrôle administratif des objets Stratégie de groupe, la stratégie de groupe pour un site, un domaine ou une unité d'organisation, les filtres WMI.

- Délégation des objets Stratégie de groupe.

Par défaut, la capacité de créer des objets Stratégie de groupe appartient au groupe Propriétaires créateurs de la stratégie de groupe mais vous pouvez déléguer ce pouvoir à tout groupe ou utilisateurs de 2 façons différentes :

- *Ajouter le groupe ou l'utilisateur au groupe Propriétaires créateurs de la stratégie de groupe* accessible avant la console Gestion de stratégie de groupe.
- *Attribuer explicitement au groupe ou à l'utilisateur l'autorisation de créer des objets Stratégie de groupe* disponible via la console Gestion de stratégie de groupe.

Les deux autorisations sont identique et confère les mêmes droits . Les utilisateurs peuvent créer des objets Stratégie de groupe dans le domaine et disposer d'un contrôle total sur ces objets mais ils n'ont aucunes autorisations sur des objets Stratégie de groupe créés par d'autres utilisateurs et cela ne signifie aucunement qu'il puissent lier les objets créés à un site ,un domaine ou une unité d'organisation.

Vous pouvez également gérer les autorisations sur l'objet Stratégie de groupe au niveau des taches. Les cinq catégories suivantes sont des autorisations sur un objet Stratégie de groupe : « Lecture »,« Modifier les paramètres », « Modifier les paramètres, supprimer, modifier la sécurité », « Lire (à partir du filtrage sécurisé) », « Paramètres personnalisés ».

- Délégation de la stratégie de groupe pour un site, un domaine ou une unité d'organisation.

Cette délégation inclut la capacité à lier des objets Stratégie de groupe et les autorisations pour la Modélisation de stratégie de groupe et les Résultats de stratégie de groupe.

Pour la liaison des objets Stratégie de groupe, la console Gestion de stratégie de groupe utilise une autorisation unique, appelée « Lier les objets GPO », qui permet de modifier les attributs gPLink et gPOption du site, du domaine ou de l'unité d'organisation. Cette autorisation est spécifique à un site, un domaine ou une unité d'organisation .

Le fait de déléguer les autorisations pour la Modélisation de stratégie de groupe à un utilisateurs ou à un groupe affecte à cet utilisateur ou à ce groupe l'autorisation « Générer jeu de stratégie résultant (planification)» ce qui leur permet d'utiliser la Modélisation de stratégie de groupe. La console Gestion de stratégie de groupe s'occupe de la gestion de cet autorisation .

Comme pour la Modélisation de stratégie de groupe, il est possible de déléguer les autorisations pour les Résultats de stratégie de groupe. Ces autorisations sont déléguées sur un domaine ou une unité d'organisation. Les utilisateurs disposant de ces autorisations peuvent lire les données des Résultats de stratégie de groupe pour tout objet de ce conteneur. Cette délégation affecte également à l'utilisateur ou au groupe l'autorisation « Générer jeu de stratégie résultant (enregistrement) ». La console Gestion de stratégie de groupe s'occupe de la gestion de cet autorisation .

- Délégation des filtres WMI

Vous pouvez déléguer la capacité de créer des filtres WMI dans un domaine et affecter des autorisations sur ces filtres.

Vous créez des filtres WMI dans le conteneur Filtres WMI de la console Gestion de stratégie de groupe. Lorsque vous créez un nouveau filtre WMI, Active Directory stocke celui-ci dans le conteneur WMIPolicy du conteneur system du domaine. Les autorisations sur le conteneur WMIPolicy déterminent les autorisations d'un utilisateurs pour créer, modifier et supprimer des filtres WMI.

Il existe deux autorisations de création de filtre WMI :

- *Propriétaire créateur* : autorise à créer de nouveaux filtres mais n'affecte pas d'autorisation sur les filtres créé par d'autres utilisateurs.
- *Contrôle total* : autorise à créer des filtres et affecte un contrôle total sur tous les filtres WMI du domaine.

Il existe deux autres autorisation sur les filtres WMI :

- *Modifier :* autorise à modifier le filtre WMI
- *Contrôle total :* autorise à modifier, supprimer et modifier la sécurité sur le filtre WMI.
-

Remarque :Toutes les procédures correspondantes au opérations décrites ci-dessus sont présente dans la farde entre aux pages 62 et 63 .

G) Planification d'une stratégie de groupe pour l'entreprise

- Instruction de planification des objets Stratégie de groupe

Créez des objets Stratégie de groupe de façon à offrir le plus de simplicité d'utilisation et de gestion optimale, notamment via l'utilisation de l'héritage et des liaisons multiples.

- *Appliquez les paramètres de stratégie de groupe au plus haut niveau :* pour bénéficier de l'héritage de stratégie de groupe. Déterminez le plus de paramètres communs.
- *Diminuez le nombre des objets Stratégie de groupe :* en utilisant plusieurs liaisons au lieu de créer plusieurs objets Stratégie de groupe identique et toujours de lier l'objet au plus grand conteneur possible.
- *Créez des objets Stratégie de groupe spécialisés :* pour appliquer des paramètres unique si nécessaire . Les objets Stratégie de groupe à un niveau supérieur n'appliqueront pas les paramètres des ces objets spécialisés.

- *Désactivez les paramètres de configuration de l'utilisateur ou de l'ordinateur :* Lorsque vous créez un objets Stratégie de groupe destiné à un utilisateur ou un ordinateur ,désactiver l'autre zone . Cela permet d'améliorer les performances d'application des objets Stratégie de groupe lors de la connexion de l'utilisateurs et empêche l'application accidentelle de paramètres dans l'autre zone.

- Instruction pou déterminer l'héritage des objets Stratégie de groupe

L'héritage des objets Stratégie de groupe tient une place importante dans l'implémentation de la stratégie de groupe et il vaut mieux décider à l'avance d'appliquer la stratégie à tout ou à une partie des utilisateurs.

- *Utilisez l'option Appliqué (Ne pas passer outre) uniquement lorsque c'est nécessaire :* par exemple pour les paramètres de sécurité exigés par l'entreprise et assurez vous que ces objets Stratégie de groupe contiendront uniquement ces paramètres importants.
- *Utilisez l'option blocage de l'héritage avec modération :* car cela complique la résolution des problèmes et l'administration des objets Stratégie de groupe.
- *Utilisez le filtrage de sécurité en cas de besoin uniquement :* lorsque des paramètres s'appliquent uniquement à un groupe de sécurité particulier dans un conteneur. Limitez le nombre de filtres en créant et liant les objets Stratégie de groupe au niveau approprié .

- Instruction pour déterminer une stratégie de groupe pour les sites

Vous pouvez lier des objets Stratégie de groupe à un site, de façon à appliquer des paramètres à l'ensemble des ordinateurs et utilisateurs se trouvant physiquement sur le site . Lorsque la stratégie de groupe est définie au niveau du site, elle n'affecte pas les utilisateurs itinérants sur ce site s'ils ont accès au réseau depuis un autre site.

- *Appliquez un objet Stratégie de groupe à un site uniquement si les paramètres sont spécifiques au site et no au domaine :* sinon la résolution des problèmes de paramètres de stratégie de groupe liés au site peut s'avérer compliquée.
- *Créez des objets Stratégie de groupe dans le domaine qui comporte le plus grand nombre de contrôleur de domaine sur ce site :* car un contrôleur de domaine du domaine contenant l'objet Stratégie de groupe lié au site est contacté avant l'application de l'objet, quel que soit le domaine auquel appartient l'utilisateur ou l'ordinateur.

- Instructions de planification de l'administration des objets Stratégie de groupe

- *Identifiez votre stratégie d'administration pour la gestion des objets stratégie de groupe :* Déterminez qui pourra créé des objet et les lié et qui ne pourra pas et qui va gérer les objets Stratégie de groupe.
- *Organisez les objets Stratégie de groupe en fonction de la maintenance administrative :* De cette façon vous pourrez déléguer le contrôle des objets Stratégie de groupe approprié et réduire le risque potentiel qu'un administrateur remplace les modifications apportées par un autre administrateur à un objet Stratégie de groupe donné.

- *Planifiez l'audit des objets Stratégie de groupe :* Votre organisation peut vous demander d'enregistrer les modifications apportée aux objets Stratégie de groupe ainsi que leur utilisation, afin que vous puissiez vérifier que Active Directory applique correctement les paramètres.

- Instructions de déploiement des objets Stratégie de groupe

  - *Testez les paramètres de stratégie de groupe :* dans différentes situations soit sur une version « miniature » de l'environnement de production d'une entreprise si il en existe une (beaucoup de grande entreprise le font) soit en dehors des heures de pointes et mettez en place une stratégie de régression afin de corriger tout problème qui surviendrait. Les stratégie de test incluent :
    - L'ouverture de session en tant qu'utilisateur représentatif sur des stations de travail représentative afin de vérifier que tout les paramètres sont appliqués et qu'il n'existe aucun conflit. Vous pouvez vous aidez de la Modélisation de stratégie de groupe et des Résultats de stratégie de groupe afin de voir quel paramètres sont appliqués et à partir de quel objet.
    - L'ouverture de session dans toutes les conditions envisageable
    - Le test des ordinateurs portables en les connectant au reseau depuis les différents sites sur lesquels les utilisateurs sont susceptibles d'ouvrir une session.
  - *Documentez le plan de stratégie de groupe :* Conservez toujours la liste détaillée de tous les objets Stratégie de groupe afin de facilement résoudre les problèmes et gérer la stratégie de groupe. Pensez à y rajouter les informations suivantes :
    - Le nom et la fonction de chaque objet de Stratégie de groupe
    - Les paramètres de stratégie de groupe à un site, un domaine, ou une unité d'organisation
    - Les liaisons d'objet Stratégie de groupe à un site, un domaine ou une unité d'organisation
    - Tout paramètre spécial appliqué à l'objet Stratégie de groupe.

Pour ce résumé, je n'ai pas trouvé l'utilité de reprendre les procédures d'accès aux différentes consoles parce qu'on ne peut déjà pas les résumer et parce que je ne vois pas l'utilité d'apprendre ça par cœur . Mais si vous en avez besoin sachez qu'elle sont toutes présentes dans la farde. Ensuite je ne prétend pas être très balèze en OS alors si vous repérez une erreur , n'hésitez pas à la signaler à tous. Travaillez bien.

Roadie

Module 6 : déploiement et gestion des logiciels à l'aide d'une stratégie de groupe.

1. Introduction.

Ce module présente les concepts de base du déploiement de logiciels à l'aide de la stratégie de groupe (SDG). Il explique comment, déployer des logiciels à l'aide de la stratégie de groupe, configurer le déploiement de logiciels à l'aide de la SDG, d'assurer la maintenance des logiciels déployés à l'aide de la SDG, de résoudre quelque problème courants liés au déploiement des logiciels et de planifier une stratégie de déploiement de groupe.

2. Présentation de la gestion du déploiement de logiciels.

a) Processus d'installation et de maintenance de logiciels

La stratégie de groupe vous permet d'automatiser l'installation, la mise à niveau et la suppression de logiciel en appliquant des paramètres de stratégie de groupe à des utilisateur ou à des ordinateurs dans un site, un domaine ou une unité d'organisation.

4 phases du processus d'installation et de maintenance de logiciel :

1. **Préparation :**
   a. Déterminer si on peut déployer le logiciel à l'aide de la structure des objets SDG courant.
   b. Identifier les risques liés à l'utilisation de l'infrastructure courante qui empêcherait l'installation logicielle.
   c. Préparer les fichiers permettant le déploiement d'une application à l'aide de la SDG soit en copiant les fichiers package Windows Installer pour une application dans un pont de distribution de logiciel.
2. **Déploiement :**
   Crée un objet SDG qui installe le logiciel sur l'ordinateur et relié l'objet SDG à un conteneur Active directory. Le logiciel est installé au démarrage de l'ordinateur ou lorsqu'un utilisateur démarre l'application.
3. **Maintenance :**
   Si vous procéder a des mises à niveau ou redéploiement d'un logiciel, cela sera fait automatiquement au démarrage de l'ordinateur ou lorsqu'un utilisateur démarre l'application
4. **Suppression :**
   Supprimez les paramètres du package de logiciel dans l'objet SDG à l'origine de son déploiement. Cela sera fait automatiquement au démarrage de l'ordinateur ou lorsqu'un utilisateur ouvre une session

b) Définition de Windows installer.

Ce composant sert a automatisé l'installation et la suppression d'application.
Composant de Windows Installer :

1. Le service Windows Installer :
   Service côté client qui automatise le processus d'installation et de configuration logicielle à partir du CD-ROM ou à l'aide de la SDG.

2. Le package Windows Installer :

Fichier qui contient toute les infos dont Windows Installer a besoin pour dés/installer des logiciels ce fichier contient :

- Un fichier Windows Installer *.msi
- Tout fichier source externe requis pour dés/installer le logiciel.
- Un résumé des infos standard concernant le logiciel et le package.
- Les fichiers du produit ou une référence à un point d'installation où ces fichiers se trouvent.

Avantages :

- Installation personnalisée
- Application tolérantes aux pannes : si un fichier critique est endommagé, l'application le récupère à partir de la source d'installation automatique.
- Suppression propre : Windows Installer supprime tout sauf les fichier utile a d'autre application.

3. Déploiement de logiciels.

a) Introduction.

Le déploiement de logiciels garantis que les applications requises sont disponibles à partir de chaque ordinateur auxquels l'utilisateur se connecte.

b) Vue d'ensemble du processus de déploiement de logiciels

1. Créez un point de distribution de logiciels :

Dossier partagé sur le serveur qui contient les fichiers de package et de logiciels. Lors de l'installation de logiciel Windows installer ira chercher les fichiers dans ce dossier.

2. Utilisez un objet SDG pour le déploiement de logiciels.

Vous devez créer ou modifier un objet SDG pour le conteneur dans lequel vous souhaitez déployer l'application.

3. Modifiez les propriétés de déploiement des logiciels en fonction des besoins.

c) Affectation de logiciels et publication de logiciels.

Affecter un logiciel : L'affectation de logiciels vous permet de vous assurer que l'utilisateur peut en disposer en permanence. Des raccourcis dans le menu démarrer et des icônes sur le bureau correspondant aux logiciels apparaissant

1. Affecter un logiciel : L'affectation de logiciels vous permet de vous assurer que l'utilisateur peut en disposer en permanence. Des raccourcis dans le menu démarrer et des icônes sur le bureau correspondant aux logiciels apparaissant. Le logiciel est installé automatiquement en cas de besoin.

Méthodes :

- Durant la configuration de l'utilisateur : le logiciel s'installe quand l'utilisateur ouvre le logiciel ou un fichier s'y rapportant.
- Le logiciel s'installe lors du démarrage de l'ordinateur.

2. Publier un logiciel : s'assurer que le logiciel soit disponible pour su l'utilisateur puissent l'installer.

Méthodes :

- Installation a l'aide de **Ajouter ou supprimer des programmes**
- 0 l'aide de l'activation de documents : Lorsque vous publier une application dans active directory, les extension de noms de fichier des documents qu'elle prend en charge sont enregistrées dans Active directory. Si un utilisateur double clique sur un type de fichier inconnu, l'ordinateur envoie une requête à Active directory pour déterminer si l'une des applications est associée à l'extension. Si Active directory contient l'application requise, l'ordinateur l'installe.

d) Création d'un point de distribution de logiciels.

1. Créez un dossier partagé en mode lecture.
2. Créez les dossiers d'applications appropriées dans le dossier partagé
3. Copiez dans les dossier approprier les package Windows installer ainsi que les fichier connexes.

e) Utilisation d'un objet SDG pour le déploiement de logiciels

Après avoir crée un pont de distribution de logiciels, créez un objet SDG qui déploie ces applications, puis reliez l'objet SDG au conteneur qui contient les utilisateurs et les ordinateurs auprès desquels vous souhaitez déployer des logiciels.

f) Options par défaut pour installation logicielle

- Emplacement des packages par défaut.
- Afficher la boite de dialogue de déploiement de logiciels : si il y a plusieurs fichier de package
- Publier : Pour publier automatiquement par défaut un nouveau fichier de package d'installation.
- Attribuer : pour affecter automatiquement un nouveau fichier de package
- Avancé : pour plus de contrôle
- Interface utilisateur : - De base : utilise les paramètre par défaut
  - Toute : l'utilisateur entre les valeurs.

g) Modification des options d'installation logicielle.

Après avoir déployé un package de logiciels, vous pouvez modifiez les propriété qui avant été définie durant le déploiement initial des logiciels.

4. Configuration du déploiement des logiciels

a) Définition des catégories de logiciels :

On utilise des catégories de logiciel pour organiser des logiciels affectés et publiés en groupes logiques, afin que les utilisateurs puissent trouver aisément les applications dans ajouter/supprimer. On peut créer des catégorie de logiciels pour regrouper différente applications sous une entête spécifique. Les catégories de logiciels recouvrent plusieurs

domaines. On les définit une seule fois pour toute une forêt. On peut utiliser la même liste de catégorie de logiciels dans toutes les stratégies dans la forêt.

b) Définition de l'association de logiciels.

Pour déterminer quels logiciels les utilisateur installent lorsqu'ils sélectionnent un fichier, on peut choisir un extension de nom de fichier et configurer un priorité d'installation des application associée à a l'extension.
Un ordinateur client gère une liste des extensions et des applications enregistrées qui utilisent ces extensions. Lorsqu'un utilisateur double clique sur un type de fichier inconnu, Windows installer utilise cette liste pour installer une application.

c) Définition de la modification de logiciels.

Des modifications sont associées au package W. I. au moment du déploiement plutôt que lorsque W.I. utilise le package pour installer ou modifier l'application.
Le déploiement de plusieurs configurations d'une application permet à différents groupes dans l'organisation d'utiliser un package de logiciels de manière différent.
UN fichier *.mst est un package de logiciels personnalisé qui modifie la manière dont W.I. installe le package *.msi associé.

5. Maintenance des logiciels déployés.

a) Types de mises à niveau de logiciels.

- Mise à niveau obligatoire : l'utilisateur final ne peut exploiter que la version mise à niveau.
- Mises à niveau facultatives : Les utilisateur ont le choix de l'installer ou de ne pas l'installer
- Mises à niveau sélectives : On peut choisir les utilisateur qui devront faire la mise à niveau.

b) Fonctionnement de redéploiement de logiciels

- Un redéploiement est l'application de service packs et de mises à niveau de logiciel à des logiciels déployés. On peut redéployer un package déployer pour forcer une réinstallation logiciel.
- Un redéploiement peut être nécessaire si le package de logiciels déployé précédemment est mis à jour mais conserve la même version, ou en cas de problème d'interopérabilité ou de virus qu'une installation peut résoudre.

c) Méthode de suppression de logiciels déployés.

- Suppression forcée : le logiciel est automatique supprimé d'un ordinateur sans avertissement
- Suppression facultative : le logiciel n'est pas supprimer d'un ordinateur et aucune mise à niveau ne peut être installer

6. Résolution de problèmes liés au déploiement de logiciels

a) Problème courant.

SYMPTOME	CAUSE POSSIBLE
Les applications n'apparaissent pas dans Ajouter/supprimer des programmes	• L'application a été affectée, et non publiée • Aucun objet SDG n'a été appliqué
Les applications n'apparaissent pas dans le menu Démarrer	• L'application a été publiée, et non affectée • Aucun objet SDG n'a été appliqué
L'application apparaît, mais ne peut être installée	• Le point de distribution logicielle n'est pas accessible • Les applications précédemment installées empêchent toute nouvelle installation.

b) Comment déterminer la cause du problème.

CAUSE	METHODE DE TEST
• L'application a été publiée, et non affectée. • L'application a été affectée et non publiée • Aucun objet SDG n'a été appliqué	Utiliser RSoP pour déterminer quel objet SDG est appliqué
• Le point de distribution logicielle n'est pas accessible	Installer manuellement Windows Installer
Les applications précédemment installées empêchent toute nouvelle installation.	Créer le fichier journal Windows Installer

.

c) Comment Résoudre les problèmes d'installation logiciels

CAUSE	METHODE DE RESOLUTION
• L'application a été publiée, et non affectée. • L'application a été affectée et non publiée • Aucun objet SDG n'a été appliqué	Modifier l'objet SDG
• Le point de distribution logicielle n'est pas accessible	Modifier les autorisations
Les applications précédemment installées empêchent toute nouvelle installation.	Supprimer les composants de registre

7. Planification d'un SDG de déploiement de logiciels

a) Instruction de planification des ponts de distribution de logiciels.

- Utilisez un système de fichier DFS basé sur un domaine pour les points de distribution de logiciels.
- Spécifiez un emplacement par défaut pour les packages
- Organisez les applications par fonction
- Configurer les autorisations NTFS
- Utilisez un dossier partager caché
- Procédez à l'audit d'accès aux objets pour les fichiers Windows Installer.

b) Instruction de planification d'un déploiement de logiciels à l'aide de la SDG

- Déployer les fichiers package en plusieurs phases.
- Classez les applications par catégorie
- Utilisez autant que possible des fichiers de transformation pour les package
- Déterminez les conflits potentiels dans les extensions de noms de fichiers
- Déployez les logiciels à un niveau élevé dans la hiérarchie Active directory

c) Instruction de planification de maintenance de logiciels

- Déterminez s'il est préférable de déployer la mise à jour graduellement ou rapidement vers tous les utilisateur et ordinateur.
- Déterminez si la mise à niveau sera obligatoire ou facultative.