Service d'annuaire Active Directory

Sommaire

1. Description d'un service d'annuaire

Un service d'annuaire est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder.
Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur.

1.1. Rôle d'Active Directory

Active Directory est le service d'annuaire de la famille Windows Server 2003.
Il étend la fonctionnalité de base d'un service d'annuaire et fournit les avantages suivants :

- **Intégration DNS**

Active Directory utilise les conventions d'attribution de noms DNS pour créer une structure hiérarchique qui fournit une vue familière, ordonnée et évolutive des connexions réseau. DNS sert également à faire correspondre les noms d'hôtes, tels que microsoft.com, à des adresses numériques TCP/IP, telles que 192.168.19.2.

- **Évolutivité**

Active Directory est organisé en sections qui permettent de stocker un très grand nombre d'objets. Active Directory peut de ce fait évoluer en fonction des besoins de l'entreprise. Une organisation qui dispose d'un seul serveur avec quelques centaines d'objets peut évoluer vers des milliers de serveurs et des millions d'objets.

- **Administration centralisée**

Active Directory permet aux administrateurs d'administrer les ordinateurs distribués, les services réseau et les applications à partir d'un emplacement central tout en utilisant une interface d'administration cohérente.
Active Directory fournit également un contrôle centralisé de l'accès aux ressources réseau en permettant aux utilisateurs d'ouvrir une fois une session et d'obtenir un accès complet aux ressources d'Active Directory.

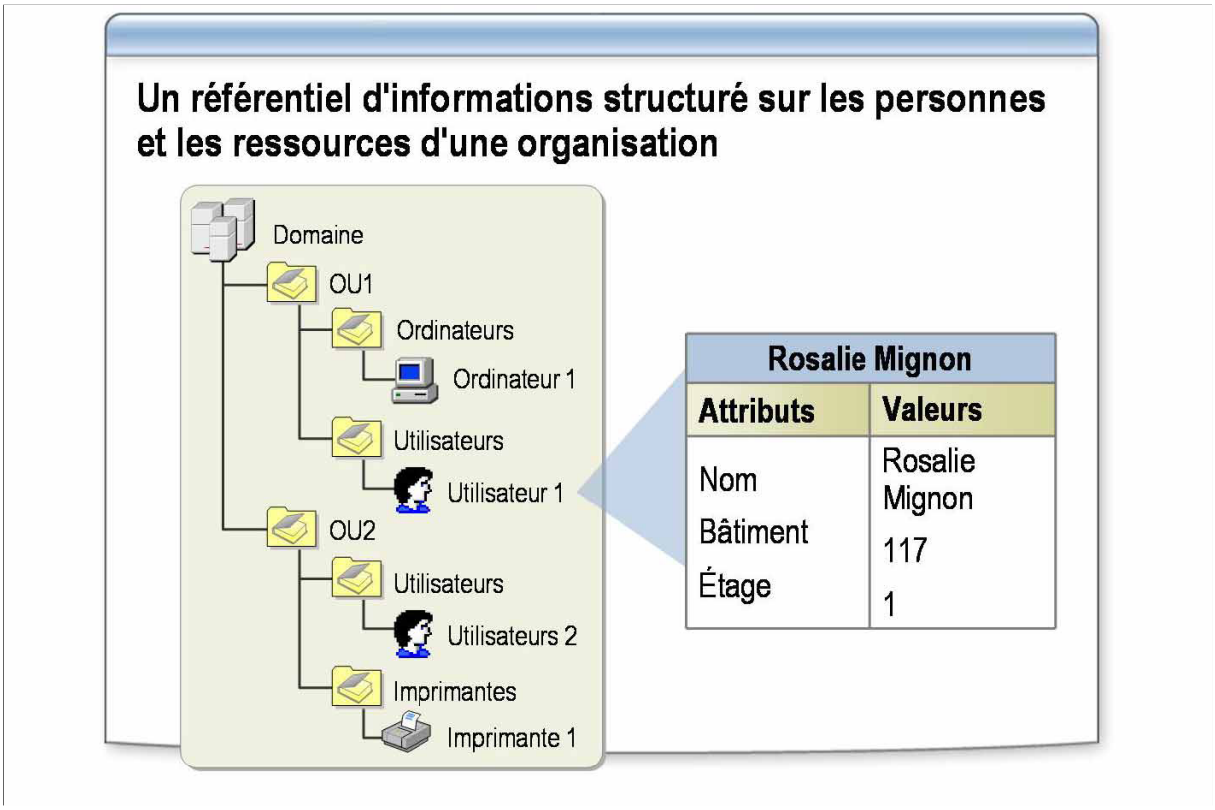
- **Administration déléguée**

La structure hiérarchique d'Active Directory permet de déléguer le contrôle d'administration sur des parties spécifiques de la hiérarchie. Un utilisateur

autorisé par une autorité administrative plus élevée peut effectuer des tâches d'administration dans la partie de la structure qui lui a été affectée.

1.2. Fonctionnement d'Active Directory

1.2.1. 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.

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.

Active Directory dispose des fonctionnalités suivantes :

- *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 toute combinaison de ces valeurs.

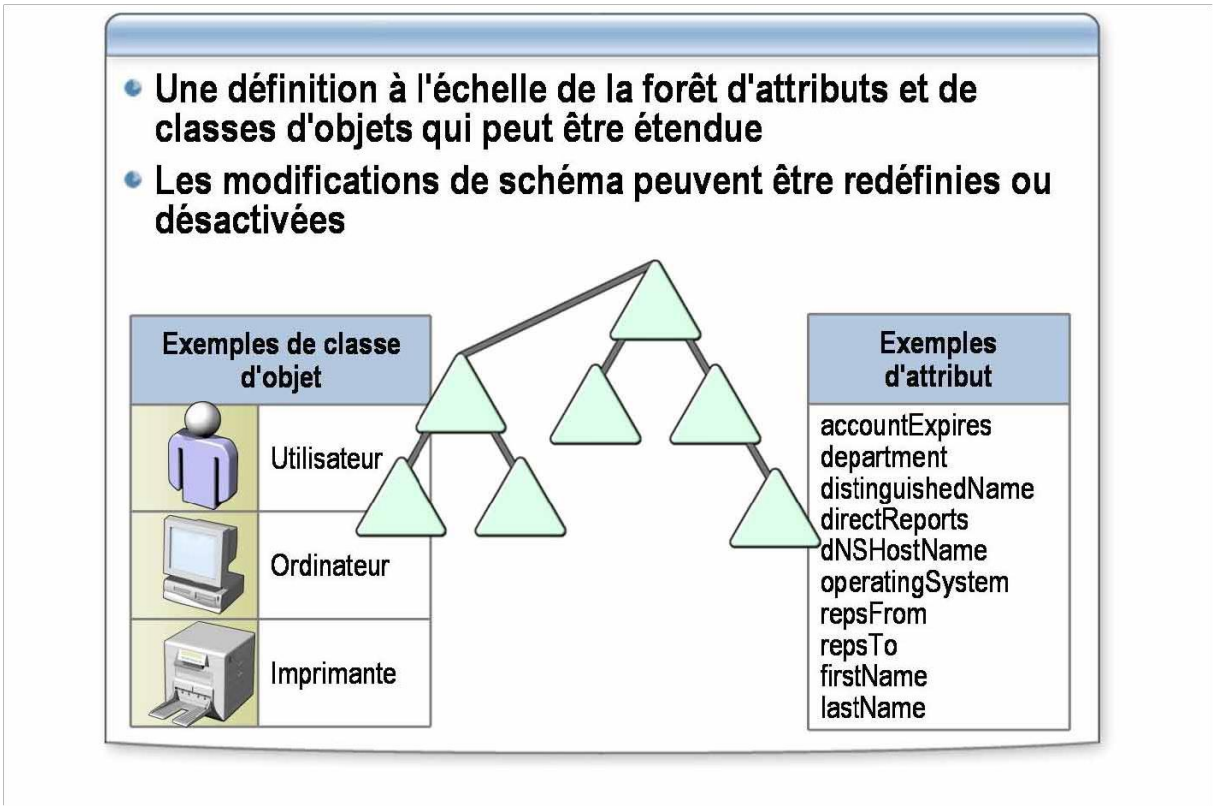
- *Transparence des protocoles et de la topologie physique du réseau*. Un utilisateur sur un réseau peut accéder à toute ressource, une imprimante par exemple, sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.

- *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. Par exemple, un annuaire peut ainsi passer d'un serveur unique contenant quelques centaines d'objets à des milliers de serveurs contenant des millions d'objets.
- *Possibilité d'exécution en tant que service indépendant du système d'exploitation.* AD/AM (Active Directory in Application Mode) est une nouvelle fonctionnalité de Microsoft 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, en tant que tel, ne nécessite pas de déploiement sur un contrôleur de domaine. L'exécution en tant que service indépendant du système d'exploitation signifie que plusieurs instances AD/AM peuvent s'exécuter simultanément sur un serveur unique, chaque instance étant configurable de manière indépendante.

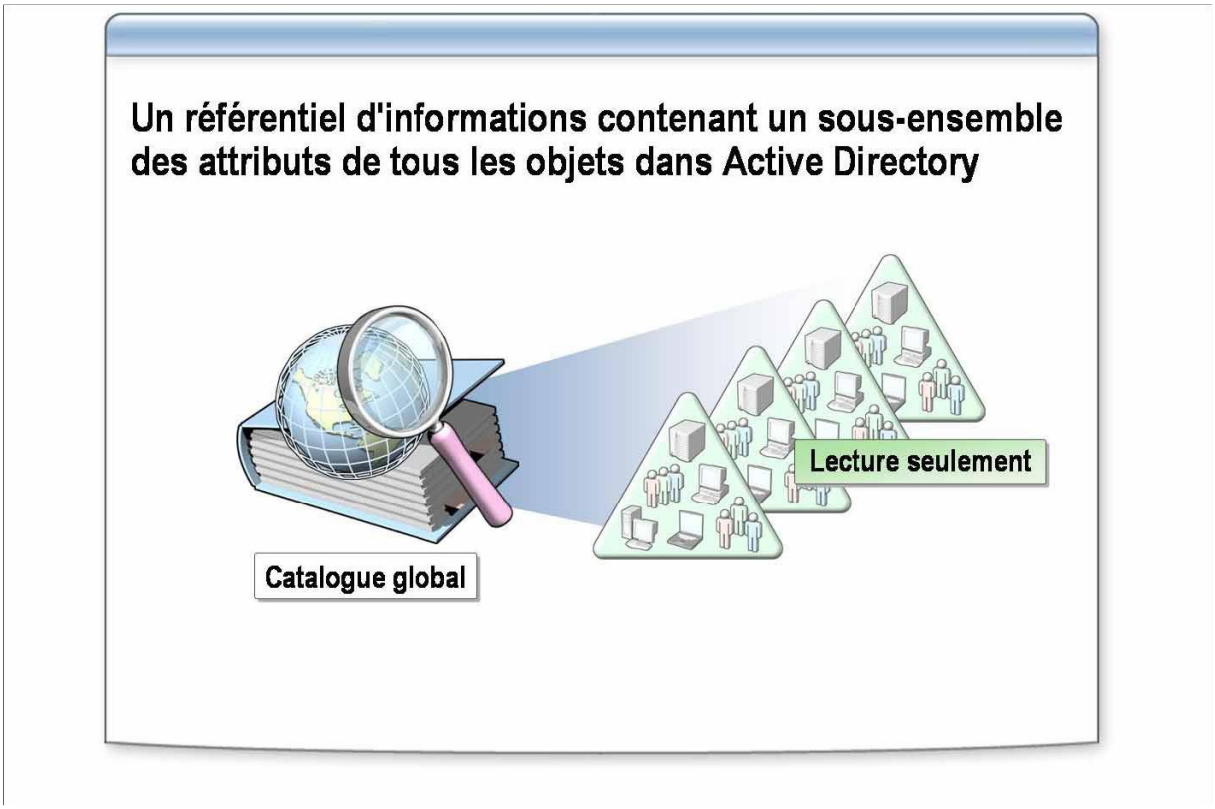
1.2.2. Définition d'un schéma

Le *schéma* Active Directory contient les définitions de tous les objets, comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Les contrôleurs de domaine exécutant Windows Server 2003 ne comportent qu'un seul schéma pour toute une forêt. Ainsi, tous les objets créés dans Active Directory se conforment aux mêmes règles.
Le schéma possède deux types de définitions : les classes d'objets et les attributs. Les *classes d'objets* comme utilisateur, ordinateur et imprimante décrivent les objets d'annuaire 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. Par exemple, l'attribut **Description** est utilisé dans de nombreuses classes d'objets,

mais il n'est défini qu'une seule fois dans le schéma afin de préserver la cohérence.



1.2.3. 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 transparente pour l'utilisateur. Par exemple, si vous recherchez toutes les imprimantes présentes dans une forêt, un serveur de catalogue global traite la requête dans le catalogue global, puis renvoie les résultats. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Le *catalogue global* est un référentiel d'informations qui contient un sousensemble 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.

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.

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.

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.

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.

CN=Benharraf Mohammed,OU=Formation,DC=Gsimaroc,DC=com

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

1.3.1. 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.

Le processus de conception d'Active Directory inclut les tâches suivantes :

- *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 analysez des besoins d'entreprise spécifiques, plusieurs options de conception peuvent y répondre. Par exemple, un besoin administratif peut être résolu par le biais d'une conception de domaine ou d'une structure d'unité d'organisation.
- 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 une conception, analysez les besoins d'entreprise qui entrent 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.

1.3.2. Résultat du processus de conception d'Active Directory

Le résultat de la phase de conception d'Active Directory inclut les éléments ci dessous.

- *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.

1.3.3. Processus de planification d'Active Directory

Le résultat du processus de planification est le plan d'implémentation d'Active Directory. Ce plan se compose lui-même de plusieurs plans qui définissent les besoins fonctionnels pour un composant spécifique de l'implémentation d'Active Directory.

Un plan Active Directory inclut les composants suivants :

- *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. Par exemple, 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, telles que celles des ventes, des ressources humaines et de production. 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 matière 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 niveau de logiciels. Il peut, par exemple, spécifier si les mises à 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 maîtres 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.

1.3.4. Processus d'implémentation d'Active Directory

Une fois le plan d'implémentation d'Active Directory en place, vous pouvez commencer à implémenter Active Directory conformément à votre plan de conception.

Vous devez exécuter les tâches ci-dessous 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'utilisateur dans Active Directory.
- *Création des objets Stratégie de groupe*. Créez des objets Stratégie de groupe basés sur la stratégie de groupe, puis reliez-les à des sites, à 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.

1.4. Structure logique d'Active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans sa structure logique hiérarchique. Les *objets* Active Directory représentent des utilisateurs et des ressources, tels que des ordinateurs et des imprimantes. Certains objets en contiennent d'autres. Lorsque vous aurez compris le rôle et la fonction de ces objets, vous pourrez effectuer des tâches diverses, comme l'installation, la configuration, la gestion et le dépannage d'Active Directory.
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 d'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.

- ***Les unités d'organisation (OU, Organizational Unit).***

Vous utilisez 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 des 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 arborescences de domaines. Lorsque vous ajoutez un second domaine à une arborescence, il devient *enfant* du domaine racine 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, par exemple corp.nwtraders.msft. 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 exemple nwtraders.msft.
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.

1.5. Structure physique d'Active Directory

Contrairement à la structure logique, qui modélise des exigencesadministratives, la structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications. Pour optimiser l'utilisation par Active Directory de la bande passante du réseau, vous devez en comprendre la structure physique. Les éléments de la structure physique d'Active Directory sont :

- ***Les contrôleurs de domaine***.

Ces ordinateurs exécutent Microsoft Windows Server. 2003 ou Windows® 2000 Server 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 contrôleurs 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 domaines situés à des emplacements différents.

- ***Partitions Active Directory.***

Chaque contrôleur de domaine contient les partitions Active Directory suivantes :

1. 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.

2. 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.

3. 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 configuration et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.

4. 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.

2. Implémentation d'une structure de forêt et de domaine Active Directory

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

2.1.1. Conditions requises pour installer Active Directory

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

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

partition NTFS est nécessaire pour le dossier SYSVOL.

- Les privilèges administratifs nécessaires pour la création, le cas échéant, d'un domaine dans un réseau Windows Server 2003 existant.
- Protocole TCP/IP installé et configuré pour utiliser le système DNS.
- Un serveur DNS qui fait autorité pour le domaine DNS et prend en charge les conditions requises répertoriées dans le tableau ci-dessous.

2.1.2. Processus d'installation d'Active Directory

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

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

• partition d'annuaire de schéma
• partition d'annuaire de configuration
• partition d'annuaire de domaine
• zone DNS de la forêt
• partition de la zone DNS du domaine

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

! *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.

Pour améliorer les performances, placez la base de données et les fichiers journaux sur des disques durs distincts. De cette manière, les opérations de lecture et d'écriture réalisées dans la base de données et dans les

fichiers journaux n'entrent pas en concurrence pour les ressources en entrée et en sortie.

- *Création du domaine racine de la forêt.* Si le serveur est le premier contrôleur de domaine du réseau, le processus d'installation crée le domaine racine de la forêt, puis attribue les rôles de maître d'opérations au contrôleur de domaine, notamment :

  • l'émulateur de contrôleur principal de domaine (PDC, *Primary Domain Controller*)
  • le maître d'opérations des identificateurs relatifs (RID, *Relative IDentifier*)
  • le maître de nommage de domaine
  • le contrôleur de schéma
  • le maître d'infrastructure

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

- *Création du dossier volume système partagé.* Cette structure de dossiers est hébergée sur tous les contrôleurs de domaine Windows Server 2003 et contient les dossiers suivants :

•le dossier partagé SYSVOL, qui contient des informations relatives à la stratégie de groupe ;
•le dossier partagé Net Logon, qui contient les scripts de connexion des ordinateurs qui ne sont pas équipés de Windows Server 2003.

- *Configuration de l'appartenance du contrôleur de domaine sur un site approprié*. Si l'adresse IP du serveur que vous souhaitez promouvoir contrôleur de domaine se trouve dans la plage d'adresses d'un sous-réseau donné défini dans Active Directory, l'Assistant configure l'appartenance du contrôleur de domaine dans le site associé au sous-réseau.

Si aucun objet de sous-réseau n'est défini ou si l'adresse IP du serveur ne se trouve pas dans la plage des objets de sous-réseau présents dans Active Directory, le serveur est placé sur le site *Premier-Site-par-Défaut* (premier site

configuré automatiquement lorsque vous créez le premier contrôleur de domaine dans une forêt).

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

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

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

2.1.3. Comment créer une structure de forêt et de domaine

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

Procédure de création du domaine racine de la forêt

Pour créer un domaine racine de la forêt, procédez comme suit :
1. Cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **dcpromo** en tant que nom du programme.
L'Assistant vérifie les points suivants :

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

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

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

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

4. Sur la page **Type de contrôleur de domaine**, cliquez sur **Contrôleur de domaine pour un nouveau domaine**, puis cliquez sur **Suivant**.

5. Dans la page **Créer un nouveau domaine**, cliquez sur **Domaine dans une nouvelle forêt,** puis sur **Suivant**.

6. Dans la page **Nouveau nom de domaine**, tapez le nom DNS complet du nouveau domaine, puis cliquez sur **Suivant**.

7. Dans la page **Nom de domaine NetBIOS**, vérifiez le nom NetBIOS, puis cliquez sur **Suivant**.

Le nom NetBIOS permet d'identifier le domaine sur les ordinateurs clients équipés de versions antérieures de Windows et Windows NT. L'Assistant identifie que le nom de domaine NetBIOS est unique. Si ce n'est pas le cas, il vous invite à modifier le nom.

8. Dans la page **Dossiers de la base de données et du journal**, indiquez l'emplacement dans lequel vous souhaitez installer les dossiers de la base de données et du journal, puis cliquez sur **Suivant**.

9. Dans la page **Volume système partagé**, tapez l'emplacement dans lequel vous souhaitez installer le dossier SYSVOL, ou cliquez sur **Parcourir** pour choisir un emplacement. Cliquez ensuite sur **Suivant**.

10. Dans la page **Diagnostics des inscriptions DNS**, assurez-vous qu'un serveur DNS existant va faire autorité pour cette forêt ou, le cas échéant, cliquez sur **Installer et configurer le serveur DNS sur cet ordinateur et définir cet ordinateur pour utiliser ce serveur DNS comme serveur DNS de préférence**. Cliquez ensuite sur **Suivant.**

11. Dans la page **Autorisations**, indiquez si vous souhaitez attribuer les autorisations par défaut à des objets utilisateur et groupe compatibles avec des serveurs équipés de versions antérieures de Windows ou Windows NT, ou

seulement avec des serveurs équipés de Windows Server 2003.
12. A l'invite, indiquez le mot de passe pour le mode Restauration des services d'annuaire.
Les contrôleurs de domaine Windows Server 2003 gèrent une petite version de la base de données des comptes de Microsoft Windows NT 4.0. Le seul compte de cette base de données est le compte Administrateur. Il est requis pour l'authentification au démarrage de l'ordinateur en mode Restauration des services d'annuaire, étant donné qu'Active Directory n'est pas démarré dans ce mode.
13. Passez en revue la page **Résumé**, puis cliquez sur **Suivant** pour commencer l'installation.
14. A l'invite, redémarrez l'ordinateur.

Procédure de création d'un domaine enfant

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

Page de l'Assistant Installation de Active Directory	**Nouvelle étape à réaliser**
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 d'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	Vérifiez le domaine parent, puis tapez le nom du nouveau domaine enfant.

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

2.1.4. 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 contrôleurs de domaine dans un seul domaine. Etant donné que tous les contrôleurs de domaine d'un domaine répliquent les données spécifiques au domaine de l'un vers un autre, l'installation de plusieurs contrôleurs de domaine dans le domaine active automatiquement la tolérance de pannes pour les données enregistrées dans Active Directory. Si un contrôleur de domaine tombe en panne, les contrôleurs de domaine restants fournissent les services d'authentification et assurent l'accès aux objets d'Active Directory, de telle sorte que le domaine, puisse continuer à fonctionner.

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

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

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

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

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

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

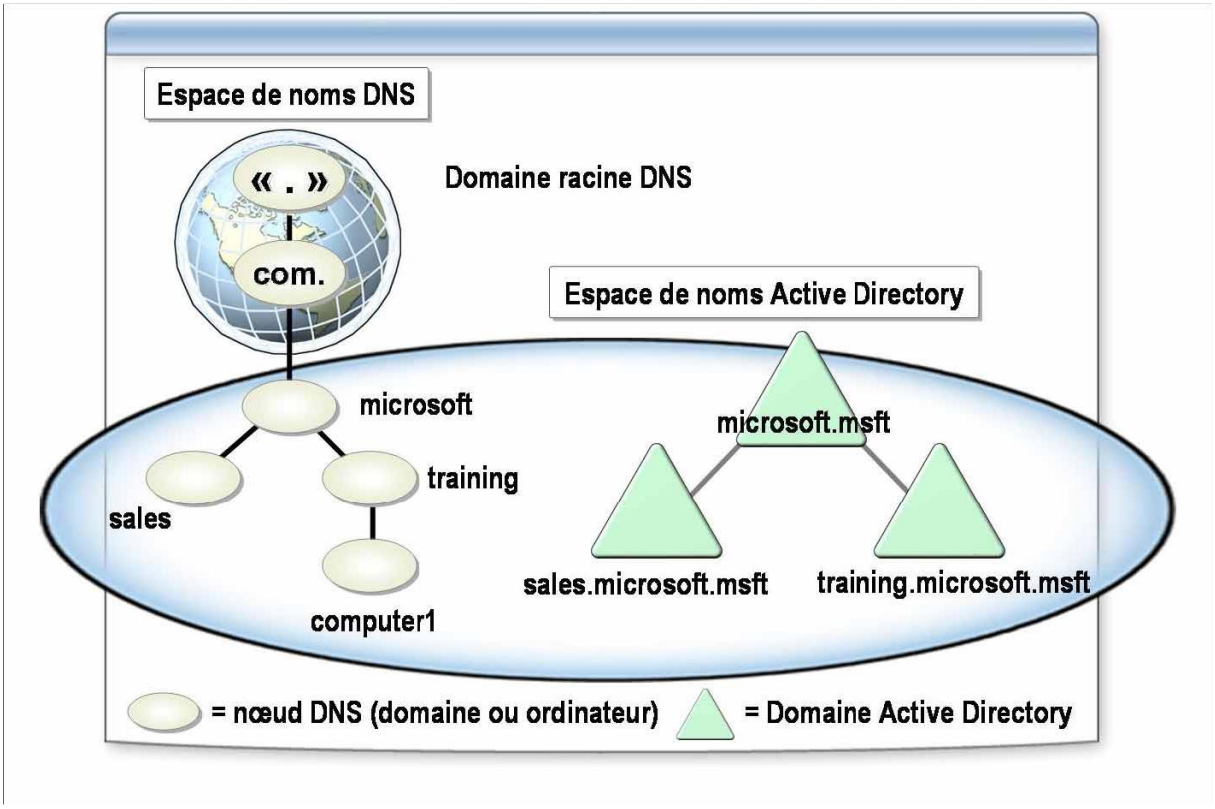
1. Exécutez **dcpromo**. Pour installer un contrôleur de domaine supplémentaire à partir des fichiers de sauvegarde, exécutez **dcpromo** avec l'option **/adv**.
2. Sur la page **Type de contrôleur de domaine**, cochez la case **Contrôleur de domaine supplémentaire pour un domaine existant**.
Sinon, si vous lancez l'Assistant Installation de Active Directory avec l'option **/adv**, choisissez l'une des options suivantes sur la page **Copie des informations du domaine en cours** :
• **Via le réseau**.
• **À partir des fichiers de restauration de cette sauvegarde**, puis indiquez l'emplacement des fichiers de sauvegarde restaurés.
3. Sur la page **Informations d'identification réseau**, tapez le nom d'utilisateur, le mot de passe et le domaine utilisateur du compte d'utilisateur que vous souhaitez utiliser pour cette opération.
Le compte d'utilisateur doit être un membre du groupe Admins du domaine pour le domaine cible.
4. Dans la page **Contrôleur de domaine supplémentaire**, spécifiez le nom de domaine pour lequel ce serveur deviendra un contrôleur de domaine supplémentaire.
5. Dans la page **Dossiers de la base de données et du journal**, indiquez l'emplacement dans lequel vous souhaitez installer les dossiers de la base de données et du journal, ou cliquez sur **Parcourir** pour choisir un emplacement.
6. Dans la page **Volume système partagé**, tapez l'emplacement dans lequel vous souhaitez installer le dossier SYSVOL, ou cliquez sur **Parcourir** pour choisir un emplacement.
7. Sur la page **Mot de passe administrateur de restauration des services d'annuaire**, tapez et confirmez le mot de passe du mode de restauration des services d'annuaire, puis cliquez sur **Suivant**.
8. Passez en revue la page **Résumé**, puis cliquez sur **Suivant** pour commencer l'installation.
9. Lorsque le système vous y invite, redémarrez l'ordinateur.

2.2. Analyse du système DNS intégré à Active Directory

2.2.1. 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 domaine identiques,

les ordinateurs d'un réseau Windows Server 2003 peuvent utiliser le système DNS pour rechercher des contrôleurs de domaine et d'autres ordinateurs qui fournissent des services Active Directory.
Les domaines et les ordinateurs sont représentés par des enregistrements de ressources dans l'espace de noms DNS et par des objets Active Directory dans l'espace de noms Active Directory.
Le nom d'hôte DNS d'un ordinateur est identique à celui du compte d'ordinateur stocké dans Active Directory. Le nom de domaine DNS (également appelé *suffixe DNS principal)* et le domaine Active Directory auquel appartient l'ordinateur ont le même nom. Par exemple, un ordinateur appelé Computer1 appartenant au domaine Active Directory appelé training.microsoft.msft ont le nom FQDN suivant : computer1.training.microsoft.msft



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

de ressources A contient le nom FQDN et l'adresse IP du contrôleur de domaine. L'enregistrement SRV contient le nom FQDN du contrôleur de domaine et le nom du service que fournit le contrôleur de domaine.

2.2.2. 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.
Les serveurs DNS Microsoft stockent des informations utilisées pour résoudre des noms d'hôte en adresses IP, et inversement, dans un fichier de base de données suivi de l'extension .dns pour chaque zone.
Les zones intégrées à Active Directory sont des zones DNS principales et de stub stockées en tant qu'objets dans la base de données Active Directory.
Vous pouvez stocker des objets de zone dans une partition d'application Active Directory ou dans une partition de domaine Active Directory. Si les objets de zone sont stockés dans une partition d'application Active Directory, seuls les contrôleurs de domaine qui souscrivent à la partition d'application participent à sa réplication. Toutefois, si les objets de zone sont stockés dans une partition de domaine Active Directory, ils sont répliqués sur tous les contrôleurs de domaine du domaine.

Les zones intégrées à Active Directory offrent les avantages suivants :

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

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

2.2.3. 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*.
Les enregistrements de ressources SRV établissent un lien entre un service et le nom d'ordinateur DNS de l'ordinateur qui offre le service. Par exemple, un enregistrement SRV peut contenir des informations permettant aux clients de localiser un contrôleur de domaine dans un domaine ou une forêt spécifique.
Lorsqu'un contrôleur de domaine démarre, il enregistre les enregistrements SRV et un enregistrement de ressources A, qui contiennent son nom d'ordinateur DNS et son adresse IP. Un ordinateur client DNS utilise ultérieurement ces informations combinées afin de localiser le service requis sur le contrôleur de domaine approprié.

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

_ Service._Protocole.Nom Ttl Classe SRV Priorité Poids Port Cible

Exemple:

_ldap._tcp.gsimaroc.com 600 IN SRV 0 100 389 Casablanca.gsimaroc.com

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 de 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.

2.3. Niveaux fonctionnels de la forêt et du domaine

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

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

- *Windows 2000 mixte.* Il s'agit du niveau fonctionnel par défaut. Vous pouvez augmenter le niveau fonctionnel du domaine vers Windows 2000 mode natif ou Windows Server 2003. Les domaines en mode mixte peuvent contenir des contrôleurs secondaires de domaine Windows NT 4.0 mais ne peuvent pas utiliser les fonctionnalités de groupes de sécurité universels, d'imbrication de groupes ni d'historique SID (Security IDentifier).
- *Windows 2000 natif.* Vous pouvez utiliser ce niveau fonctionnel si le

domaine contient uniquement des contrôleurs de domaine Windows 2000 et Windows Server 2003. Bien que les contrôleurs de domaine exécutant Windows 2000 Server ne connaissent pas la fonctionnalité de domaine, les fonctionnalités Active Directory (groupes de sécurité universels, imbrication des groupes et d'historique SID, par exemple) sont disponibles.

- *Windows 2003 Server*. Il s'agit du niveau fonctionnel le plus élevé pour un domaine. Vous pouvez l'utiliser uniquement si tous les contrôleurs de domaine du domaine exécutent Windows Server 2003. Toutes les fonctionnalités Active Directory pour le domaine sont disponibles.
- *Windows 2003 version préliminaire*. Il s'agit d'un niveau fonctionnel particulier qui prend en charge les contrôleurs de domaine Windows NT 4.0 et Windows 2003 Server.

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

2.3.1. Conditions requises pour activer les nouvelles fonctionnalités de Windows Server 2003

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

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

2.3.2. Procédure d'augmentation du niveau fonctionnel du domaine

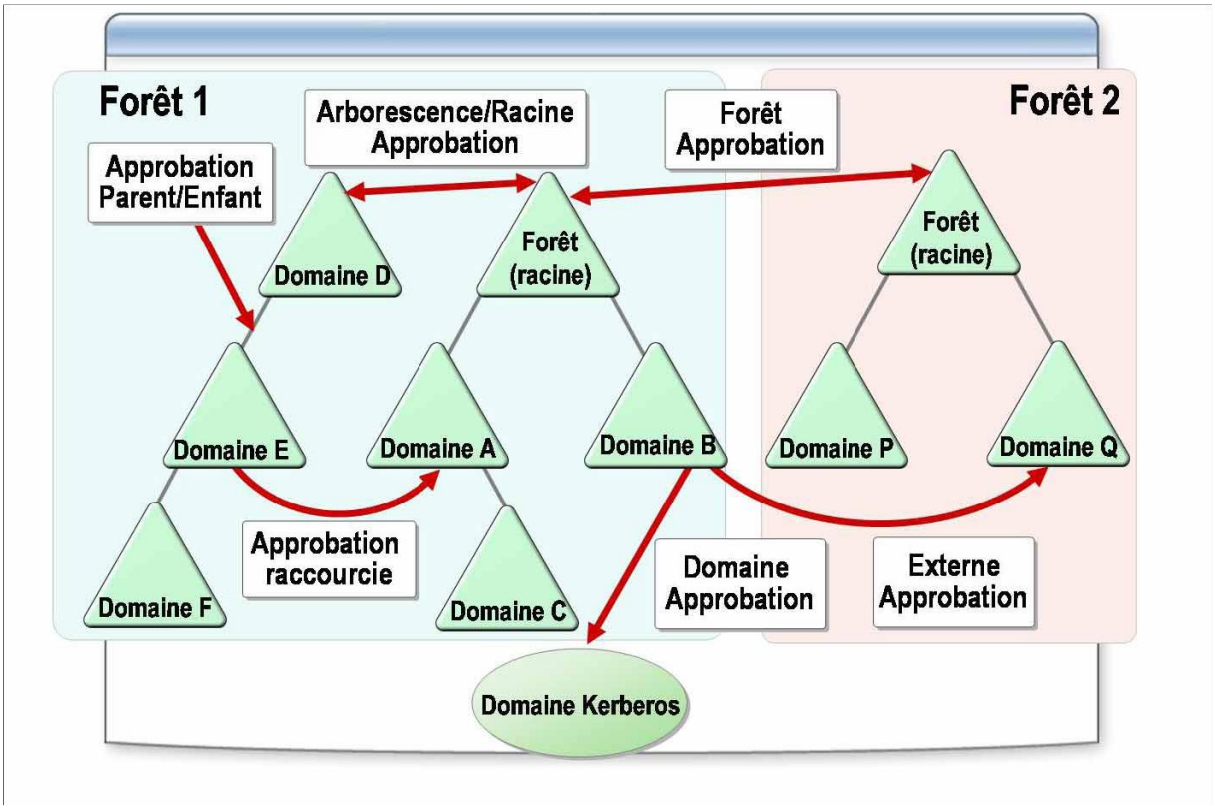
Pour augmenter le niveau fonctionnel du domaine, procédez comme suit :
1. Ouvrez Domaines et approbations Active Directory.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur le noeud du domaine dont vous souhaitez augmenter le niveau fonctionnel, puis cliquez sur **Augmenter le niveau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

2.3.3. Procédure d'augmentation du niveau fonctionnel de la forêt

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

2.4. Relations d'approbation

2.4.1. 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 et non transitives.

Dans une approbation transitive, la relation d'approbation étendue à un domaine est automatiquement étendue à tous les autres domaines qui approuvent ce domaine. Par exemple, le domaine D approuve directement le domaine E, qui approuve directement le domaine F. Etant donné que les deux approbations sont transitives, le domaine D approuve indirectement le domaine F et inversement.

Les approbations transitives sont automatiques. Une approbation parent/enfant est un bon exemple d'approbation. Les approbations non transitives ne sont pas automatiques et peuvent être configurées. Par exemple, une approbation non transitive peut être externe, comme l'approbation entre deux domaines de deux forêts distinctes.

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

bidirectionnelle, les deux domaines peuvent authentifier les utilisateurs de l'autre domaine.

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

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

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

3.1. Création et gestion d'unités d'organisation

3.1.1. Présentation de la gestion des unités d'organisation

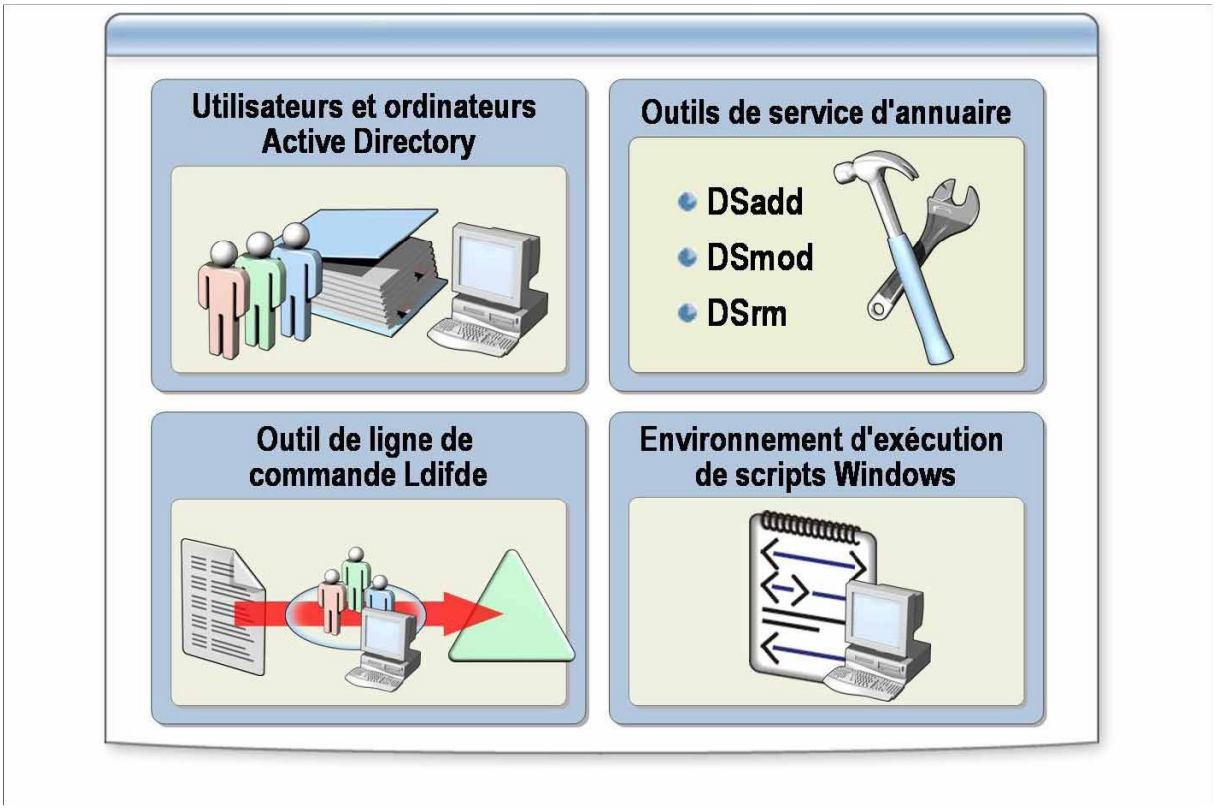
Les unités d'organisation sont les conteneurs du service d'annuaire Active Directory que vous utilisez pour placer des utilisateurs, des groupes, des

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. Vous pouvez, par exemple, utiliser les unités d'organisation pour appliquer automatiquement des stratégies de groupe définissant des paramètres par défaut pour les comptes d'ordinateurs et d'utilisateurs dans Active Directory.

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.

3.1.2. Méthodes de création et de gestion des unités d'organisation



Microsoft® Windows Server. 2003 fournit plusieurs composants 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.

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 logiciel 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 outil de ligne de commande permet de créer des unités d'organisation et d'autres 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 fournis 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.

3.1.3. Procédure de création d'une unité d'organisation à l'aide de la ligne de commande Dsadd

Pour créer une unité d'organisation, exécutez 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 ***poleformation*** au domaine **gsimaroc.com**, le nom unique serait *ou=poleformation,dc=gsimaroc,dc=com*.
- *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 d'utilisateur 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, Benharraf)
• domaine\nom d'utilisateur (par exemple, gsimaroc\Benharraf)
• nom d'utilisateur principal (UPN, *User Principal Name*) (par exemple, Benharraf@gsimaroc.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.

3.1.4. 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*.

3.1.5. Procédure de suppression d'une unité d'organisation

Vous devez supprimer d'Active Directory les unités d'organisation qui ne sont plus utilisées. Pour supprimer une unité d'organisation, exécutez 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 **dsrm** :

- *subtree*. Spécifie de supprimer l'objet ainsi que tous les objets contenus dans la sous-arborescence située sous cet objet.
- *Exclude.* Spécifie de ne pas supprimer l'objet de base fourni par *NU_Unité_Organisation* lorsque vous supprimez 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.

3.1.6. Comment créer et gérer des unités d'organisation à l'aide de l'outil 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.
La première étape à exécuter pour utiliser cet outil consiste à créer le fichier d'entrée à utiliser avec Ldifde. Après avoir créé 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=**formationOu**,DC=**gsimaroc**,DC=**com**
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.

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

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

1. À 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=gsimaroc,dc=com")

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=formationOu")

Dans cet exemple, FormationOu 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 commande : wscript nom_fichier_script.vbs

3.2. Délégation du contrôle administratif des unités d'organisation

3.2.1. Délégation de privilèges administratifs

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.
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'ont les administrateurs 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 de la 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.

3.2.2. 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.

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 n.ud 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 boîte 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**, sélectionnez 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.

3.3. Planification d'une stratégie d'unité d'organisation

3.3.1. 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.

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 responsables 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 travail 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 de 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 particulière ; par défaut, les utilisateurs ont le contrôle intégral des objets qu'ils créent ;

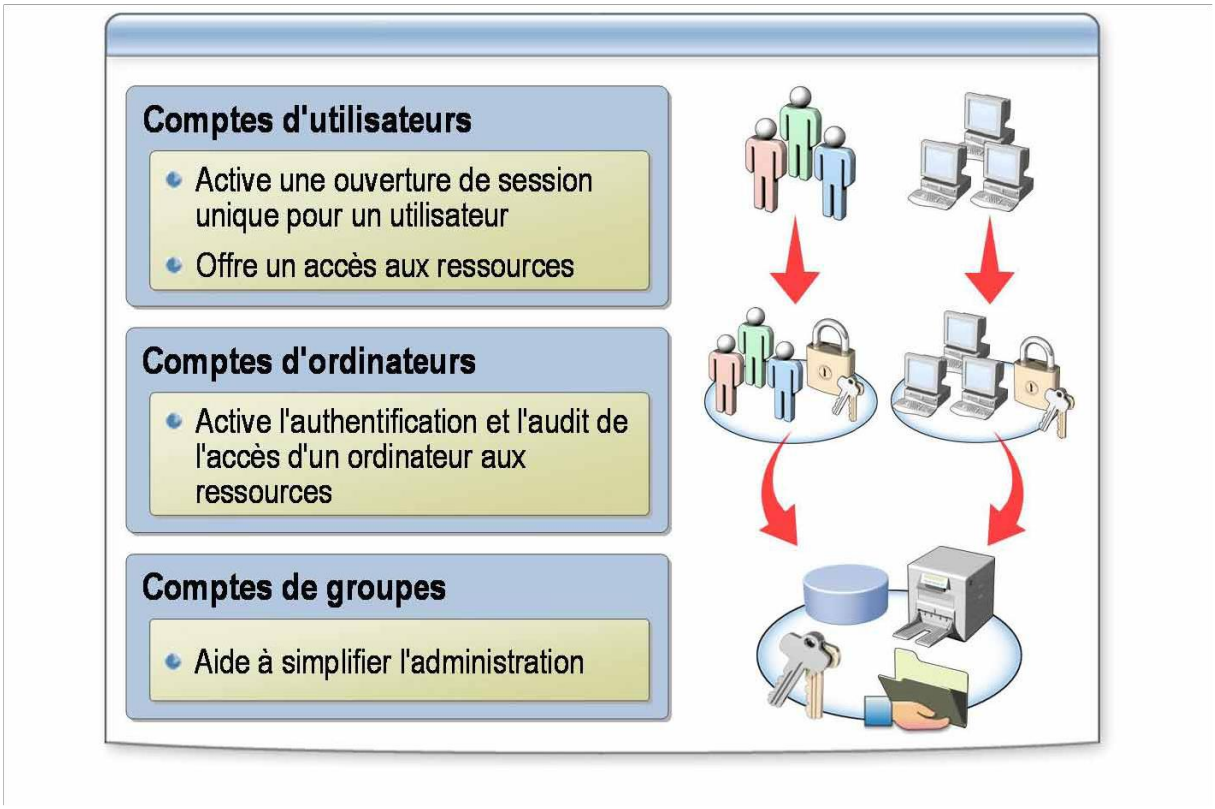
• seront autorisés à ne modifier que des attributs spécifiques d'objets existants d'une classe particulière.

- *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 le plan de délégation.

4. Implémentation de comptes d'utilisateurs, de groupes et d'ordinateurs

4.1. Présentation des comptes

4.1.1. Types de comptes



Vous pouvez créer trois types de comptes dans Active Directory : comptes d'utilisateurs, de groupes et d'ordinateurs. Les comptes d'utilisateurs et d'ordinateurs Active Directory représentent une entité physique, telle qu'un ordinateur ou une personne. Vous pouvez également utiliser les comptes d'utilisateurs comme comptes de services dédiés pour certaines applications.

Comptes d'utilisateurs

Un *compte d'utilisateur* est un objet stocké dans Active Directory qui permet une *ouverture de session unique*, autrement dit un utilisateur entre son mot de passe une seule fois lors de l'ouverture de session sur une station de travail pour obtenir un accès authentifié aux ressources réseau.
Il existe trois 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 réseau, 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 exécutant Microsoft Windows NT®, Windows 2000 ou Windows XP, ou un serveur exécutant Windows Server 2003 qui rejoint un domaine possède un compte d'ordinateur. À l'image des comptes d'utilisateurs, les comptes d'ordinateurs permettent d'authentifier et d'auditer l'accès d'un ordinateur aux ressources réseau et du domaine. Chaque compte d'ordinateur doit être unique.

Comptes de groupes

Un *compte de groupe* est un ensemble d'utilisateurs, 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.

4.1.2. Types de groupes

Il existe deux types de groupes dans Active Directory, les groupes de distribution et les groupes de sécurité. Tous deux 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 natif ou ultérieur.

Groupes de distribution

Vous pouvez utiliser des groupes de distribution 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, ce qui signifie qu'ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire (DACL, *Discretionary Access Control List*). Pour contrôler l'accès aux ressources partagées, créez un groupe de sécurité

Groupes de sécurité

Vous utilisez 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 des groupes de sécurité consiste à utiliser *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 simplifie l'affectation en une fois des autorisations à plusieurs groupes, et 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. En mode Windows 2000 mixte, vous ne pouvez pas créer de groupes de sécurité universels.

4.1.3. Etendue de groupes

Groupes locaux de domaine

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 domaine 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.

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 d'utilisateurs et des groupes globaux de n'importe quel domaine. En mode Windows 2000 natif, les groupes locaux de domaine

peuvent contenir des comptes d'utilisateurs, des groupes globaux, des groupes universels de n'importe quel domaine approuvé et des groupes locaux de domaine 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.
- *Étendue*. 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.

Groupes globaux

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.

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 d'utilisateurs du même domaine. En mode Windows 2000 natif et en mode Windows Server 2003, des groupes globaux peuvent contenir des comptes d'utilisateurs 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 mixte 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.
- *Étendue.* Un groupe global est visible dans son domaine et tous les domaines approuvés, ce qui inclut tous les domaines de la forêt.
- *Autorisations.* Vous pouvez affecter une autorisation à un groupe global qui s'applique à tous les domaines approuvés.

Groupes universels

Un groupe universel est un groupe de sécurité ou de distribution qui peut contenir des utilisateurs, des groupes et des ordinateurs comme membres d'un

domaine de sa forêt. Les groupes de sécurité universels peuvent bénéficier de droits et autorisations sur des ressources situées dans n'importe quel domaine de la forêt.
Les règles suivantes s'appliquent à l'appartenance au groupe universel, ainsi qu'à l'étendue et aux autorisations du groupe universel :

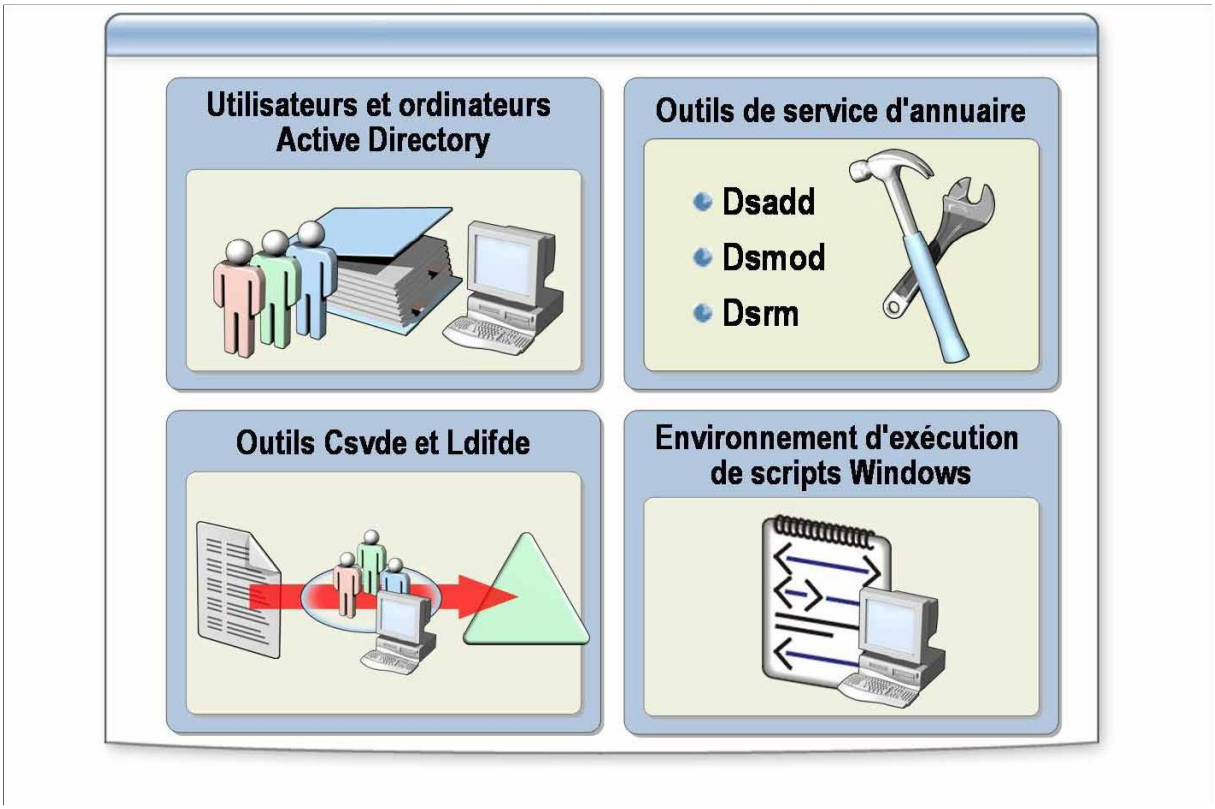
- *Appartenance*. Vous ne pouvez pas créer de groupes de sécurité universels en mode Windows 2000 mixte. En mode Windows 2000 natif et en mode Windows Server 2003, des groupes universels peuvent contenir des comptes d'utilisateurs, des groupes globaux et d'autres groupes universels de n'importe quel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

4.2. Création et gestion de comptes

4.2.1. Outils permettant de créer et gérer des comptes

Windows Server 2003 procure de nombreux outils et composants logiciels enfichables MMC (Microsoft Management Console) pour créer automatiquement plusieurs comptes d'utilisateurs dans Active Directory.
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 créer des scripts pour ajouter ou modifier des objets dans Active Directory.
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.
Vous pouvez également utiliser les outils de ligne de commande Dsadd, Dsmod et Dsrm pour gérer des comptes d'utilisateurs, d'ordinateurs et de groupes dans Active Directory. 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 d'utilisateur. Utilisez la commande **dsrm group** pour supprimer un compte de groupe. Bien que les outils Directory Service permettent de créer

un seul objet Active Directory à la fois, vous pouvez les utiliser dans des fichiers de commandes et des scripts.



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 Active Directory.
Vous devez utiliser le format Csvde pour ajouter des objets utilisateur et d'autres types d'objets à Active Directory. Vous ne pouvez pas utiliser le format Csvde pour supprimer ou modifier 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 d'utilisateur dans Active Directory, le type d'objet, qui est le compte d'utilisateur, et le nom d'ouverture de session de l'utilisateur (pour Microsoft Windows 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 vous ne spécifiez aucune valeur, le compte est désactivé ;
- peut inclure des informations personnelles, par exemple des numéros de téléphone ou des adresses personnelles. Incluez autant d'informations sur le compte d'utilisateur que possible afin que les utilisateurs puissent

effectuer des recherches dans Active Directory ;

- ne peut pas inclure de mots de passe. Une importation en bloc laisse le mot de passe vide pour les comptes d'utilisateur. Étant donné qu'un mot de passe vide permet à une personne non autorisée d'accéder au réseau grâce au seul nom d'ouverture de session de l'utilisateur, désactivez les comptes d'utilisateurs jusqu'à ce que les utilisateurs commencent à se connecter.

Pour modifier et formater le fichier texte d'entrée, utilisez une application qui possède de bonnes capacités d'édition, telle que Microsoft Excel ou Microsoft Word. Enregistrez ensuite le fichier en tant que fichier texte séparé par des virgules. Vous pouvez exporter des données d'Active Directory vers une feuille de calcul Excel ou importer des données d'une feuille de calcul vers Active Directory.
L'outil de ligne de commande Ldifde utilise un format *à valeurs séparées par des lignes* pour créer, modifier et supprimer des objets dans Active Directory.
Un fichier d'entrée Ldifde se compose d'une série d'enregistrements séparés par une ligne vierge. Un *enregistrement* décrit un objet annuaire unique ou un ensemble de modifications apportées aux attributs d'un objet existant, et se compose d'une ou plusieurs lignes dans le fichier. La plupart des applications de base de données peuvent créer des fichiers que vous pouvez importer dans l'un de ces formats. Les conditions requises pour le fichier d'entrée sont identiques à celles de l'outil de ligne de commande Csvde.
Vous pouvez créer des scripts d'environnement d'exécution de scripts Windows qui utilisent des interfaces ADSI (*Active Directory Service Interfaces*) pour créer, modifier et supprimer des objets Active Directory. Utilisez des scripts lorsque vous souhaitez modifier la valeur des attributs pour plusieurs objets Active Directory, ou lorsque les critères de sélection de ces objets sont complexes.

La ligne d'attribut.

Il s'agit de la première ligne du fichier. Elle précise le nom de chaque attribut que vous souhaitez définir pour les nouveaux comptes d'utilisateurs. Vous pouvez placer les attributs dans n'importe quel ordre, ils doivent être séparés par des virgules. Le code suivant est un exemple de ligne d'attribut

Lignes de comptes d'utilisateurs.

Pour chaque compte d'utilisateur que vous créez, le fichier d'importation contient une ligne qui précise la valeur de chaque attribut de la ligne d'attribut

Exemple
DN,objectClass,sAMAccountName,userPrincipalName,displayName,userAccountControl

"cn=Benharraf Mohammed,ou=formation, dc=gsimaroc,dc=com",user,benharraf, benharraf@gsimaroc.com, Benharraf mohammed,514

Exécutez la commande **csvde** en tapant la commande suivante à l'invite de commandes :

csvde -i -f *nom_fichier* -b *Nom_Utilisateur Domaine Mot_de_Passe*

Vous pouvez utiliser l'outil de ligne de commande Ldifde pour créer et modifier plusieurs comptes.

Pour créer des comptes à l'aide de l'outil de ligne de commande Ldifde, procédez comme suit :

1. Préparez le fichier Ldifde à importer.

Formatez le fichier Ldifde afin qu'il contienne un enregistrement qui se compose d'une suite de lignes qui décrivent une entrée pour un compte d'utilisateur ou un ensemble de modifications sur un compte d'utilisateur dans Active Directory. L'entrée du compte d'utilisateur précise le nom de chaque attribut que vous souhaitez définir pour le nouveau compte d'utilisateur. Le schéma Active Directory définit le nom des attributs. Pour chaque compte d'utilisateur que vous créez, le fichier contient une ligne qui précise la valeur de chaque attribut de la ligne d'attribut. Les règles suivantes s'appliquent aux valeurs de chaque attribut :

• toute ligne qui commence par un signe dièse (#) est une ligne de commentaire et est ignorée lorsque vous exécutez le fichier Ldifde ;

• s'il manque une valeur pour un attribut, elle doit être représentée comme *Description_Attribut* « : » .

Le code suivant est un exemple d'entrée dans un fichier d'importation Ldifde :

Créer Benharraf Mohammed

dn: cn=Benharraf Mohammed,ou= Formation, dc=gsimaroc,dc=com
Changetype: Add
objectClass: user
sAMAccountName: Benharraf
userPrincipalName: benharraf@gsimaroc.com
displayName: Benharraf Mohammed
userAccountControl: 514

Exécutez la commande **ldifde** pour importer le fichier et créer plusieurs comptes d'utilisateurs dans Active Directory.

À l'invite de commandes, tapez la commande suivante :

ldifde -i -k -f *nom_fichier* -b *Nom_Utilisateur Domaine Mot_de_Passe*

Créer et gérer des comptes à l'aide de l'environnement d'exécution de scripts Windows

Vous pouvez créer des objets Active Directory à partir de scripts d'environnement d'exécution de scripts Windows à l'aide d'une interface ADSI.

Le processus de création d'un objet Active Directory compte quatre étapes, comme l'indique la procédure suivante.

Pour créer un objet Active Directory, tel qu'un compte d'utilisateur dans un domaine, procédez comme suit :

1. Utilisez le Bloc-notes pour créer un fichier texte avec une extension .vbs.

Placez les commandes suivantes dans le fichier, puis enregistrez-le.

a. Connectez-vous au conteneur dans lequel vous souhaitez créer l'objet Active Directory en spécifiant la requête LDAP (Lightweight Directory Access Protocol).

Set objOU = GetObject("LDAP://ou=formation,dc=gsimaroc,dc=com")

Dans l'exemple précédent, LDAP doit être inscrit en lettres majuscules, sans quoi la commande échoue.

b. Créez l'objet Active Directory et spécifiez la classe et le nom de l'objet.

Set objUser = objOU.Create("User", "cn=Benharraf")

c. Définissez les propriétés de l'objet Active Directory.

objUser.Put "sAMAccountName", "Benharraf"

d. Inscrivez les informations dans la base de données Active Directory.

objUser.SetInfo

Les propriétés de certains objets Active Directory ne peuvent pas être définies lors de leur création. Par exemple, lorsque vous créez un compte d'utilisateur, vous ne pouvez pas activer le compte ni définir son mot de passe. Vous ne pouvez définir ces propriétés qu'après avoir créé l'objet, comme illustré dans l'exemple de code suivant :

objUser.AccountDisabled = FALSE
objUser.ChangePassword "", "jl3R86df"
objUser.SetInfo

e. Enregistrez le fichier avec l'extension .vbs.

2. Exécutez le script en tapant la commande suivante à l'invite de commandes :

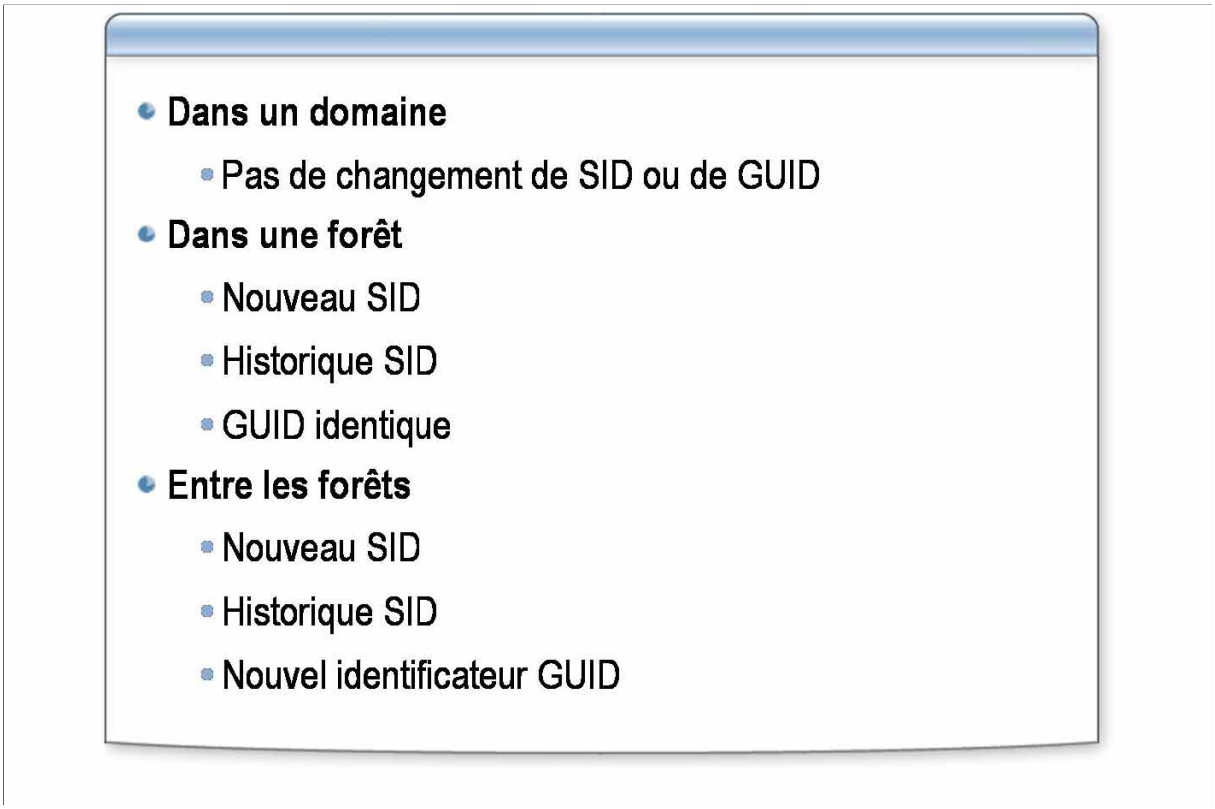
Wscript.exe *nom_fichier*

4.3. Déplacement d'objets dans Active Directory

4.3.1. Définition de l'historique SID

Lorsque vous déplacez un objet Active Directory, tel qu'un compte d'utilisateur, les principes de sécurité associés à cet objet sont également déplacés. Active Directory assure un suivi de ces principes de sécurité dans une liste intitulée Historique SID.
Un historique SID fournit à un utilisateur migré une continuité d'accès aux ressources. Lors de la migration d'un compte d'utilisateur vers un autre domaine, Active Directory lui affecte un nouveau SID. L'historique SID conserve le SID du précédent compte d'utilisateur migré. Lorsque vous migrez à plusieurs reprises un compte d'utilisateur, l'historique SID stocke une liste de tous les identificateurs SID affectés à l'utilisateur. Il met ensuite à jour les groupes et les listes de contrôle d'accès nécessaires avec le SID du nouveau compte. Les appartenances aux groupes basées sur le SID de l'ancien compte n'existent plus.

4.3.2. Déplacement d'objets



Pour que l'historique SID soit activé, le niveau fonctionnel du domaine doit être défini sur Windows 2000 natif ou Windows Server 2003. L'historique SID est désactivé si le niveau fonctionnel est défini sur Windows 2000 mixte. Lorsqu'un objet est déplacé au sein d'un domaine, le SID ou l'identificateur unique global (GUID, *Globally Unique IDentifier*) ne subissent aucune modification. Lorsque vous déplacez un objet sur plusieurs domaines d'une même forêt, Active Directory affecte un nouveau SID à l'objet mais conserve son GUID.

Vous devez utiliser la console Utilisateurs et ordinateurs Active Directory pour déplacer des objets dans un domaine.
Pour déplacer un objet dans un domaine, procédez comme suit :

- Dans le volet d'informations de la console Utilisateurs et ordinateurs Active Directory, faites glissez l'objet sur le nouveau conteneur.

Utilisez l'outil de migration Active Directory dans Windows Server 2003 pour déplacer des objets entre domaines d'une même forêt ou entre domaines situés dans des forêts différentes.
Pour migrer des utilisateurs ou des groupes d'un domaine vers un autre, procédez comme suit :
1. Exécutez l'outil de migration Active Directory.
2. Cliquez avec le bouton droit sur **Outil de migration Active Directory**, puis sélectionnez l'Assistant pour l'objet que vous souhaitez migrer.
Par exemple, pour déplacer un compte d'utilisateur, cliquez sur **Assistant Migration des comptes d'utilisateurs**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Effectuez une migration test en procédant comme suit :
a. Dans la page **Tester ou effectuer des changements**, cliquez sur **Tester les paramètres de migration et effectuer celle-ci ultérieurement**, puis cliquez sur **Suivant**.
b. Dans la page **Sélection du domaine**, sélectionnez les domaines source et cible, puis cliquez sur **Suivant**.
c. Dans la page **Sélection de l'utilisateur**, cliquez sur **Ajouter**, tapez le nom de l'objet, cliquez sur **OK**, puis sur **Suivant**.
d. Dans la page **Sélection de l'unité d'organisation**, cliquez sur **Parcourir**, sélectionnez le conteneur cible, cliquez sur **OK**, puis sur **Suivant**.
e. Dans la page **Options de l'utilisateur**, définissez les options de l'utilisateur, puis cliquez sur **Suivant**.
Ces options déterminent la migration de l'appartenance au groupe, des profils et des paramètres de sécurité.
f. Si une boîte de dialogue d'avertissement apparaît, cliquez sur **OK**.
g. Dans la page **Conflits de nommage**, sélectionnez les options appropriées pour spécifier les actions qui seront prises en cas de conflit de noms, puis cliquez sur **Suivant**.
h. Dans la page **Fin de l'Assistant Migration des comptes d'utilisateurs**, cliquez sur **Terminer**.
i. Dans la boîte de dialogue **Avancées de la Migration**, cliquez sur **Afficher le journal** pour afficher le journal des erreurs.
5. Effectuez une migration réelle en répétant les étapes 2 à 4.I. À l'étape 4.a, sélectionnez **Effectuer la migration maintenant** à la place de **Tester les paramètres de migration et effectuer celle-ci ultérieurement**.

5. Implémentation d'une stratégie de groupe

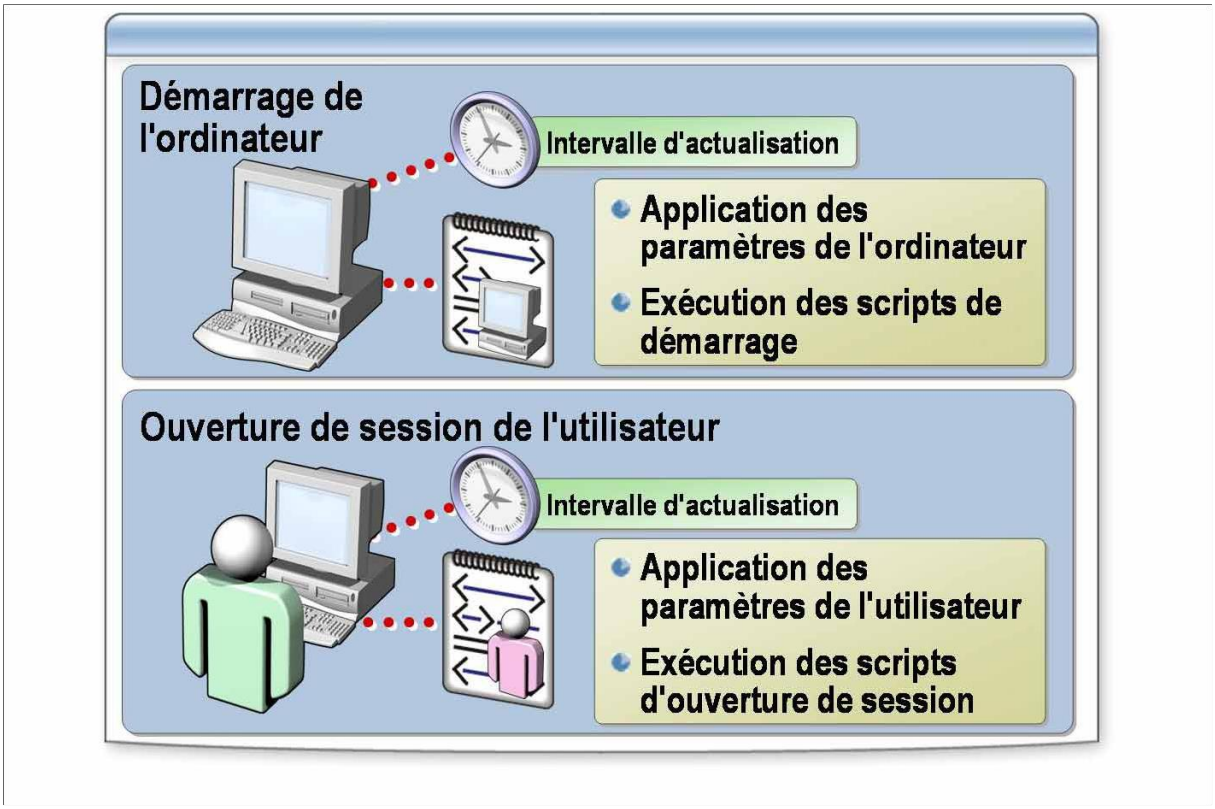
5.1. Composants d'un objet Stratégie de groupe

Windows Server 2003 applique les paramètres de stratégie de groupe contenus dans l'objet Stratégie de groupe aux objets utilisateur et ordinateur du site, du domaine ou de l'unité d'organisation associé à l'objet Stratégie de groupe. Le contenu d'un objet Stratégie de groupe est stocké à deux emplacements : dans le conteneur Stratégie de groupe (GPC, Group Policy Container) et dans le modèle Stratégie de groupe (GPT, Group Policy Template).
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

filtre WMI et une liste des composants dont les paramètres se trouvent dans ’objet Stratégie de groupe. Les ordinateurs peuvent accéder au conteneur Stratégie de groupe pour localiser des modèles Stratégie de groupe, et les contrôleurs de domaine peuvent y accéder pour obtenir des informations de version. Si le contrôleur de domaine ne possède pas la dernière version de l’objet Stratégie de groupe, la réplication a lieu.
Le modèle Stratégie de groupe est une arborescence de dossiers située dans le dossier SYSVOL d’un contrôleur de domaine. Lorsque vous créez un objet Stratégie de groupe, Windows Server 2003 crée le modèle Stratégie de groupe correspondant qui contient tous les paramètres et informations de stratégie de groupe, y compris les modèles d’administration, la sécurité, l’installation de logiciel, les scripts et les paramètres de redirection de dossiers. Les ordinateurs se connectent au dossier SYSVOL pour obtenir les paramètres.
Le nom du dossier du modèle Stratégie de groupe est l’identificateur unique global (GUID, Globally Unique IDentifier) de l’objet Stratégie de groupe que vous avez créé. Il est identique au GUID utilisé par Active Directory pour identifier l’objet Stratégie de groupe dans le conteneur Stratégie de groupe.
Le chemin d’accès au modèle Stratégie de groupe d’un contrôleur de domaine est racine_système\SYSVOL\sysvol.

5.2. Configuration des fréquences d’actualisation et des paramètres de stratégie de groupe

5.2.1. À quel moment la stratégie de groupe est-elle appliquée



Lorsqu’un utilisateur démarre un ordinateur et ouvre une session, Windows Server 2003 traite d’abord les paramètres de l’ordinateur, puis ceux de

l'utilisateur.
Windows Server 2003 applique la stratégie de l'ordinateur. Il s'agit des paramètres se trouvant sous Configuration de l'ordinateur dans la liste des objets Stratégie de groupe obtenue. Cette liste est synchrone par défaut, et s'affiche dans l'ordre suivant : local, domaine, unité d'organisation, unité d'organisation enfant. Aucune interface utilisateur n'apparaît lors du traitement des stratégies de l'ordinateur.
Les scripts de démarrage s'exécutent. Par défaut, les scripts sont masqués et synchrones. Chaque script doit se terminer ou son délai d'exécution doit être écoulé pour que le suivant puisse démarrer. Le délai d'attente par défaut est de 600 secondes. Vous pouvez utiliser les paramètres de stratégie de groupe pour modifier la valeur de ce paramètre.
Une fois que Windows Server 2003 a validé l'utilisateur, il charge le profil utilisateur, lequel est contrôlé par les paramètres de stratégie de groupe en vigueur.
Windows Server 2003 applique la stratégie de l'utilisateur, laquelle inclut les paramètres se trouvant sous Configuration utilisateur dans la liste obtenue.
Ces paramètres sont synchrones par défaut, et s'affichent dans l'ordre suivant : local, domaine, unité d'organisation, unité d'organisation enfant.
Aucune interface utilisateur n'apparaît lors du traitement des stratégies de l'utilisateur.
Les scripts d'ouverture de session s'exécutent. Par défaut, ces scripts basés sur la stratégie de groupe sont masqués et asynchrones.
Les ordinateurs exécutant Windows Server 2003 actualisent ou réappliquent les paramètres de stratégie de groupe à intervalles définis. L'actualisation des paramètres permet de s'assurer que les paramètres de stratégie de groupe sont appliqués aux ordinateurs et aux utilisateurs même si ces derniers ne redémarrent jamais leur ordinateur ou ne ferment jamais leur session.

Pour configurer les fréquences d'actualisation, procédez comme suit :
1. Ouvrez l'objet Stratégie de groupe approprié de la stratégie de groupe, développez successivement **Configuration utilisateur** ou **Configuration ordinateur** (selon l'objet Stratégie de groupe à modifier), **Modèles d'administration**, **Système**, cliquez sur **Stratégie de groupe**, puis double-cliquez sur l'un des paramètres suivants :
• **Intervalle d'actualisation de la stratégie de groupe pour les utilisateurs**
• **Intervalle d'actualisation de la stratégie de groupe pour les ordinateurs**
• **Intervalle d'actualisation de la stratégie de groupe pour les contrôleurs**

de domaine

2. Sélectionnez **Activé**.

3. Définissez l'intervalle d'actualisation en minutes.

4. Définissez le décalage aléatoire, puis cliquez sur **OK**.

Vous pouvez actualiser un objet Stratégie de groupe à l'aide de la commande **gpupdate**.

Pour actualiser les paramètres de stratégie de groupe sur l'ordinateur d'un utilisateur à l'aide de la commande **gpupdate**, procédez comme suit :

1. Dans la boîte de dialogue **Exécuter**, tapez **cmd** et appuyez sur ENTRÉE.

2. Tapez **gpupdate** [/**target**:{*ordinateur*|*utilisateur*}] [/**force**] [/wait:*valeur*] [/**logoff**] [/**boot**]

5.3. Gestion des objets Stratégie de groupe

5.3.1. Définition d'une opération de copie

La copie d'un objet Stratégie de groupe transfert uniquement les paramètres de l'objet Stratégie de groupe. L'objet Stratégie de groupe nouvellement créé est doté d'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. Le nouvel objet Stratégie de groupe créé est non lié, car les liaisons sont une propriété de l'objet ayant défini l'objet Stratégie de groupe plutôt qu'une propriété de l'objet Stratégie de groupe.

Pour copier un objet Stratégie de groupe, procédez comme suit :

1. Ouvrez la console Gestion de stratégie de groupe, développez **Objets de stratégie de groupe** dans la forêt et le domaine contenant l'objet Stratégie de groupe à copier, cliquez avec le bouton droit sur cet objet, puis cliquez sur **Copier**.

2. Effectuez l'une des opérations suivantes :

• Pour placer la copie de l'objet Stratégie de groupe dans le même domaine que l'objet source, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Coller**.

i. Dans la boîte de dialogue **Copier l'objet GPO**, sélectionnez **Utiliser les autorisations par défaut pour les nouveaux objets GPO** ou **Conserver les**

autorisations existantes, puis cliquez sur **OK**.

ii. Lorsque le processus de copie est terminé, cliquez sur **OK**.

• Pour placer la copie de l'objet dans un autre domaine, qu'il s'agisse de la même forêt ou d'une autre, développez le domaine de destination, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Coller**.

i. Dans la page **Assistant Copie entre domaines**, cliquez sur **Suivant**.

ii. Dans la page **Spécification des autorisations en cours**, sélectionnez **Utiliser les autorisations par défaut pour les nouveaux objets GPO** ou **Préserver ou effectuer la migration des autorisations à partir des objets GPO originaux**, puis cliquez sur **Suivant**.

iii. Dans la page **Analyse en cours de l'objet GPO original**, cliquez sur **Suivant**.

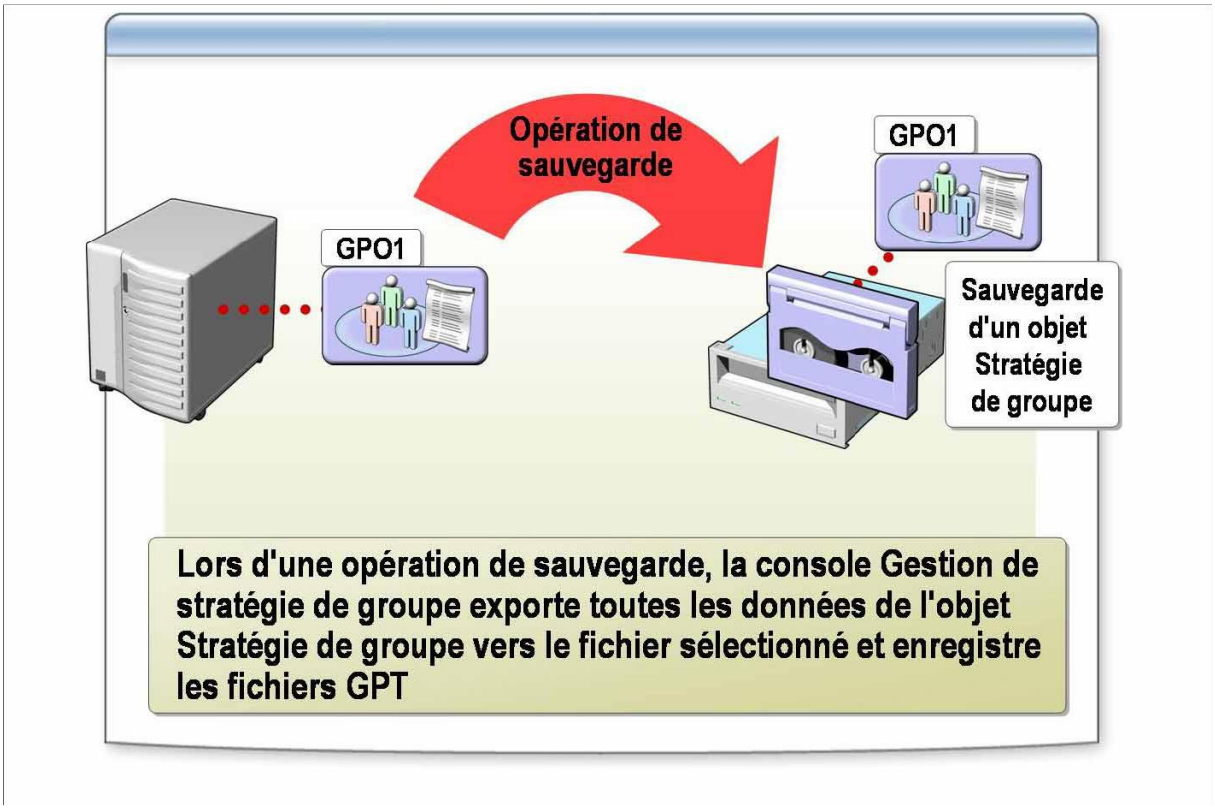
Si l'objet Stratégie de groupe source contient des références aux entités de sécurité et aux chemins UNC, vous verrez s'afficher la fenêtre mentionnée à l'étape suivante. Sinon, passez à l'étape v.

iv. Dans la page **Migration des références**, sélectionnez **Effectuant une copie identique à partir de la source** ou **Utilisant cette table de migration pour le mappage dans l'objet de stratégie de groupe cible**, sélectionnez la table de migration dans la liste, puis cliquez sur **Suivant**.

v. Dans la page **Fin de l'Assistant Copie entre domaines**, cliquez sur **Terminer**.

vi. Une fois l'opération de copie terminée, cliquez sur **OK**.

5.3.2. Définition d'une opération de sauvegarde



Lorsque la console Gestion de stratégie de groupe sauvegarde un objet Stratégie de groupe, elle exporte les données dans le fichier de votre choix et enregistre tous les fichiers de modèle Stratégie de groupe. Vous pouvez placer l'objet Stratégie de groupe sauvegardé dans un dossier par une opération de restauration ou d'importation. L'opération d'importation vous permet uniquement de restaurer un objet Stratégie de groupe sauvegardé dans un autre domaine.

Pour sauvegarder un objet Stratégie de groupe, procédez comme suit :

1. Ouvrez la console Gestion de stratégie de groupe, développez la forêt contenant l'objet Stratégie de groupe à sauvegarder, développez successivement **Domaines**, le domaine contenant l'objet Stratégie de groupe, **Objets de stratégie de groupe**, puis effectuez l'une des opérations suivantes :

• Pour sauvegarder un seul objet Stratégie de groupe, cliquez avec le bouton droit sur cet objet, puis cliquez sur **Sauvegarder**.

• Pour sauvegarder tous les objets Stratégie de groupe, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Sauvegarder tout**.

2. Dans la boîte de dialogue **Sauvegarde de l'objet GPO**, entrez le chemin d'accès à l'emplacement où vous souhaitez stocker l'objet Stratégie de groupe sauvegardé.

3. Entrez une description pour l'objet Stratégie de groupe à sauvegarder, puis

cliquez sur **Sauvegarder**.
4. Une fois l'opération de sauvegarde terminée, cliquez sur **OK**.

5.3.3. Définition d'une opération de restauration

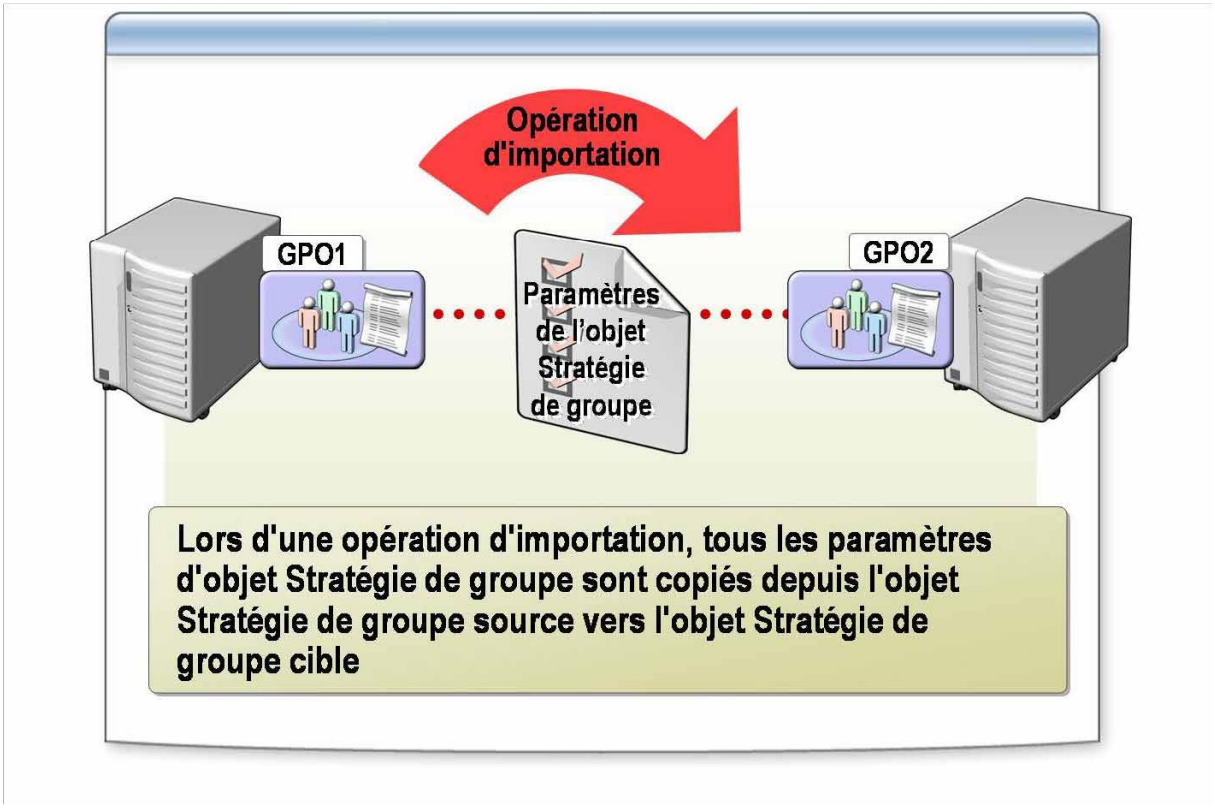
L'opération de restauration rétablit le contenu de l'objet Stratégie de groupe dans l'état dans lequel il était au moment de la sauvegarde. Cette opération est valide uniquement dans le domaine où l'objet Stratégie de groupe a été créé.
Vous pouvez restaurer un objet Stratégie de groupe existant ou un objet supprimé qui a été sauvegardé. Les autorisations requises pour restaurer un objet Stratégie de groupe varient selon que l'objet existe ou non dans Active Directory lorsque vous le restaurez.

Pour restaurer un objet Stratégie de groupe existant à l'aide de la console Gestion de stratégie de groupe, vous devez disposer des autorisations Modifier les paramètres, supprimer, modifier la sécurité sur cet objet. Vous devez également disposer de l'autorisation en lecture sur le dossier qui contient l'objet Stratégie de groupe sauvegardé.
Pour restaurer un objet Stratégie de groupe supprimé qui avait été sauvegardé, vous devez disposer d'autorisations pour créer des objets Stratégie de groupe dans le domaine, ainsi que de l'autorisation en lecture sur l'emplacement du système de fichiers de l'objet sauvegardé.
Pour restaurer une version antérieure d'un objet Stratégie de groupe existant, procédez comme suit :
1. Ouvrez la console Gestion de stratégie de groupe, développez la forêt contenant l'objet Stratégie de groupe à restaurer, développez successivement **Domaines**, le domaine contenant l'objet Stratégie de groupe, **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Objets de stratégie de groupe** puis cliquez sur **Gérer les sauvegardes**.
2. Dans la boîte de dialogue **Gestion des sauvegardes**, sélectionnez l'objet Stratégie de groupe sauvegardé à restaurer, puis cliquez sur **Restaurer**.
3. Lorsque vous êtes invité à restaurer la sauvegarde sélectionnée, cliquez sur **OK**.
4. Dans la boîte de dialogue **Restaurer**, cliquez sur **OK** une fois la restauration terminée.
5. Dans la boîte de dialogue **Gestion des sauvegardes**, sélectionnez un autre objet Stratégie de groupe à restaurer ou cliquez sur **Fermer** pour terminer l'opération de restauration.

Pour restaurer un objet Stratégie de groupe supprimé qui figure dans la liste des **Objets Stratégie de groupe**, effectuez l'une des opérations suivantes :

1. Ouvrez la console Gestion de stratégie de groupe, développez successivement la forêt contenant l'objet Stratégie de groupe à restaurer, **Domaines**, puis le domaine contenant l'objet Stratégie de groupe.
2. Cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Gérer les sauvegardes**.
3. Dans la boîte de dialogue **Gestion des sauvegardes**, cliquez sur **Parcourir**, recherchez le système de fichiers contenant l'objet Stratégie de groupe supprimé, sélectionnez l'objet, cliquez sur **Restaurer**, puis cliquez sur **OK** pour confirmer l'opération de restauration.

5.3.4. Définition d'une 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.

Spécifiez une table de migration afin d'être certain que le chemin UNC de l'objet Stratégie de groupe est correctement mappé sur le chemin UNC de l'objet Stratégie de groupe de destination. Indiquez le chemin d'accès à la table de migration appropriée lorsque vous importez des paramètres de stratégie de groupe d'un domaine dans un autre. Si vous spécifiez une table de migration,

vous devez spécifier le comportement de mappage du chemin UNC.
Si vous n'activez pas la case à cocher **Utiliser exclusivement la table de migration**, vous devez spécifier le comportement de mappage pour les entités de sécurité qui ne figurent pas dans la table de migration.
Si vous ne spécifiez pas de table de migration, toutes les entités de sécurité sont mappées en fonction du comportement que vous spécifiez.

Pour importer des paramètres dans un objet Stratégie de groupe, vous devez disposer des autorisations de modification de cet objet.
Pour importer des paramètres dans un objet Stratégie de groupe, procédez comme suit :
1. Ouvrez la console Gestion de stratégie de groupe, développez successivement la forêt contenant l'objet Stratégie de groupe dans lequel importer des paramètres, **Domaines**, le domaine contenant l'objet Stratégie de groupe, **Objets de stratégie de groupe**, cliquez avec le bouton droit sur l'objet Stratégie de groupe, puis cliquez sur **Importer des paramètres**.
2. Dans la page **Assistant Importation des paramètres**, cliquez sur **Suivant**.
3. Dans la page **Objet de stratégie de groupe de sauvegarde**, cliquez sur **Sauvegarder**.
4. Dans la boîte de dialogue **Sauvegarde de l'objet GPO**, entrez un emplacement et une description pour la sauvegarde de l'objet Stratégie de groupe, puis cliquez sur **Sauvegarder**.
5. Une fois l'opération de sauvegarde terminée, cliquez sur **OK** puis sur **Suivant**.
6. Dans la page **Emplacement de sauvegarde**, cliquez sur **Parcourir** pour rechercher le dossier de sauvegarde à partir duquel vous voulez importer des paramètres, puis cliquez sur **Suivant**.
7. Dans la page **Objet stratégie de groupe (GPO) source**, sélectionnez l'objet Stratégie de groupe à partir duquel vous voulez importer des paramètres, puis cliquez sur **Suivant**.
Si l'objet Stratégie de groupe source contient des références aux entités de sécurité et des chemins UNC, la boîte de dialogue **Migration des références** s'affiche. Choisissez le mode de migration des entités de sécurité et des chemins UNC en sélectionnant **Effectuant une copie identique à partir de la source** ou **Utilisant cette table de migration pour le mappage dans l'objet de stratégie de groupe cible**, puis sélectionnez une table de migration.
8. Cliquez sur **Suivant**.
9. Dans la page **Fin de l'Assistant Importation des paramètres**, cliquez sur **Terminer**.
10. Une fois l'opération d'importation terminée, cliquez sur **OK**.

5.4. Vérification et résolution des problèmes liés à la stratégie de groupe

5.4.1. Problèmes courants liés à l'implémentation de la stratégie de groupe

La première étape de la résolution des problèmes liés à la stratégie de groupe consiste à identifier les symptômes et les causes possibles.

Dans la plupart des cas, un paramètre de stratégie de groupe n'est pas appliqué comme prévu parce qu'un autre objet Stratégie de groupe contient une valeur conflictuelle pour le même paramètre. L'objet Stratégie de groupe est prioritaire en raison du filtrage, Blocage de l'héritage, Appliqué ou de l'ordre d'application.

Utilisez l'Assistant Modélisation de stratégie de groupe ou l'Assistant Résultats de stratégie de groupe pour déterminer l'objet Stratégie de groupe utilisé pour le paramètre.

Le tableau suivant répertorie certains des symptômes courants, ainsi que les méthodes de résolution possibles.

Symptôme	Cause
Impossible d'ouvrir un objet Stratégie de groupe	Aucune autorisation de lecture et d'écriture n'a été définie pour l'objet Stratégie de groupe
Impossible de modifier un objet Stratégie de groupe	Problème de réseau
Impossible d'appliquer une stratégie de groupe à un groupe de sécurité	Les objets Stratégie de groupe ne sont pas appliqués aux groupes de sécurité
La stratégie de groupe n'exerce aucun effet sur un site, un domaine ou une unité d'organisation	Les paramètres de la stratégie de groupe ne sont pas configurés correctement
Aucun effet d'une stratégie de groupe dans un conteneur Active Directory	Les objets Stratégie de groupe ne sont pas liés aux conteneurs Active Directory
La stratégie de groupe n'exerce aucun effet sur un ordinateur client	Un objet Stratégie de groupe non local peut écraser les stratégies locales

5.4.2. Comment vérifier les paramètres de stratégie de groupe à l'aide de l'Assistant Modélisation de stratégie de groupe

Vous avez la possibilité de simuler un déploiement de stratégie pour les utilisateurs et les ordinateurs avant de réellement appliquer les stratégies.
Cette fonctionnalité de la console Gestion de stratégie de groupe est appelée Jeu de stratégies résultant (RSoP, *Resultant Set of Policies*) . Mode de planification. Elle requiert un contrôleur de domaine exécutant Windows Server 2003 dans la forêt. Pour vérifier les paramètres de stratégie de groupe à l'aide de l'Assistant Modélisation de stratégie de groupe, vous devez d'abord créer une requête de modélisation de stratégie de groupe et afficher cette requête.
Pour créer une nouvelle requête de modélisation de stratégie de groupe, procédez comme suit :
1. Ouvrez la console Gestion de stratégie de groupe, naviguez jusqu'à la forêt dans laquelle vous souhaitez créer une requête de modélisation de stratégie de groupe, cliquez avec le bouton droit de la souris sur **Modélisation de stratégie de groupe**, puis sur Assistant Modélisation de stratégie de groupe.
2. Sur la page **Assistant Modélisation de stratégie de groupe**, cliquez sur **Suivant**, entrez les informations requises dans les pages de l'Assistant, puis cliquez sur **Terminer**.
Pour afficher la requête de modélisation de stratégie de groupe, procédez comme suit :
1. Ouvrez la console Gestion de stratégie de groupe.
2. Naviguez jusqu'à la forêt contenant la requête de modélisation de stratégie de groupe à afficher, développez **Modélisation de stratégie de groupe**, cliquez avec le bouton droit sur la requête, puis cliquez sur **Affichage avancé**.

5.4.3. Comment vérifier les paramètres de stratégie de groupe à l'aide des Résultats de stratégie de groupe

Utilisez les Résultats de stratégie de groupe pour déterminer les paramètres de stratégie qui sont appliqués à un ordinateur, ainsi que l'utilisateur qui a ouvert une session sur cet ordinateur. Bien que ces données soient similaires à celles de la modélisation de stratégie de groupe, elles sont obtenues à partir de l'ordinateur client au lieu d'être simulées sur le contrôleur de domaine. Pour obtenir des données à l'aide des Résultats de stratégie de groupe, l'ordinateur client doit exécuter Windows XP ou Windows Server 2003.

Pour créer une requête Résultats de stratégie de groupe, procédez comme suit :
1. Dans la console Gestion de stratégie de groupe, accédez à **Résultats de**

stratégie de groupe, cliquez avec le bouton droit sur **Résultats de stratégie de groupe**, puis cliquez sur **Assistant Résultats de stratégie de groupe**.
2. Dans la page **Assistant Résultats de stratégie de groupe**, cliquez sur **Suivant**.
3. Dans la page **Sélection des ordinateurs**, sélectionnez l'ordinateur actuel ou cliquez sur **Parcourir** pour sélectionner un autre ordinateur, puis cliquez sur **Suivant**.
4. Dans la page **Sélection de l'utilisateur**, sélectionnez l'utilisateur actuel ou spécifiez un utilisateur, puis cliquez sur **Suivant**.
5. Dans la page **Aperçu des sélections**, vérifiez les sélections effectuées, puis cliquez sur **Suivant**.
6. Dans la page **Fin de l'Assistant Résultats de stratégie de groupe**, cliquez sur **Terminer**.

Pour afficher la requête des Résultats de stratégie de groupe, procédez comme suit :
1. Ouvrez la console Gestion de stratégie de groupe.
2. Naviguez jusqu'à la forêt contenant la requête de modélisation de stratégie de groupe à afficher, développez **Résultats de stratégie de groupe**, cliquez avec le bouton droit sur la requête, puis cliquez sur **Affichage avancé**.

5.5. Délégation du contrôle administratif de la stratégie de groupe

5.5.1. Délégation des objets Stratégie de groupe

Vous pouvez déléguer la capacité de créer des objets Stratégie de groupe dans un domaine et d'affecter des autorisations sur un objet Stratégie de groupe individuel à l'aide de la console Gestion de stratégie de groupe.
Par défaut, la capacité de créer des objets Stratégie de groupe est attribuée au groupe Propriétaires créateurs de la stratégie de groupe. Vous pouvez cependant déléguer ce pouvoir à tout groupe ou utilisateur de deux façons différentes :

- *Ajouter le groupe ou l'utilisateur au groupe Propriétaires créateurs de la stratégie de groupe*. Il s'agit de la première méthode, disponible 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*. Cette méthode est disponible uniquement *via* la console Gestion de stratégie de groupe.

Dans le cas d'utilisateurs et de groupes du domaine, utilisez le groupe

Propriétaires créateurs de la stratégie de groupe pour affecter des autorisations de création d'un objet Stratégie de groupe. Ce groupe étant un groupe global du domaine, il ne peut pas contenir de membres extérieurs au domaine. Si des utilisateurs externes au domaine ont besoin de pouvoir créer des objets Stratégie de groupe, procédez comme suit :

1. Créez un nouveau groupe local du domaine dans le domaine.
2. Affectez à ce groupe l'autorisation de créer des objets Stratégie de groupe dans le domaine.
3. Ajoutez à ce groupe des utilisateurs de domaine externes.

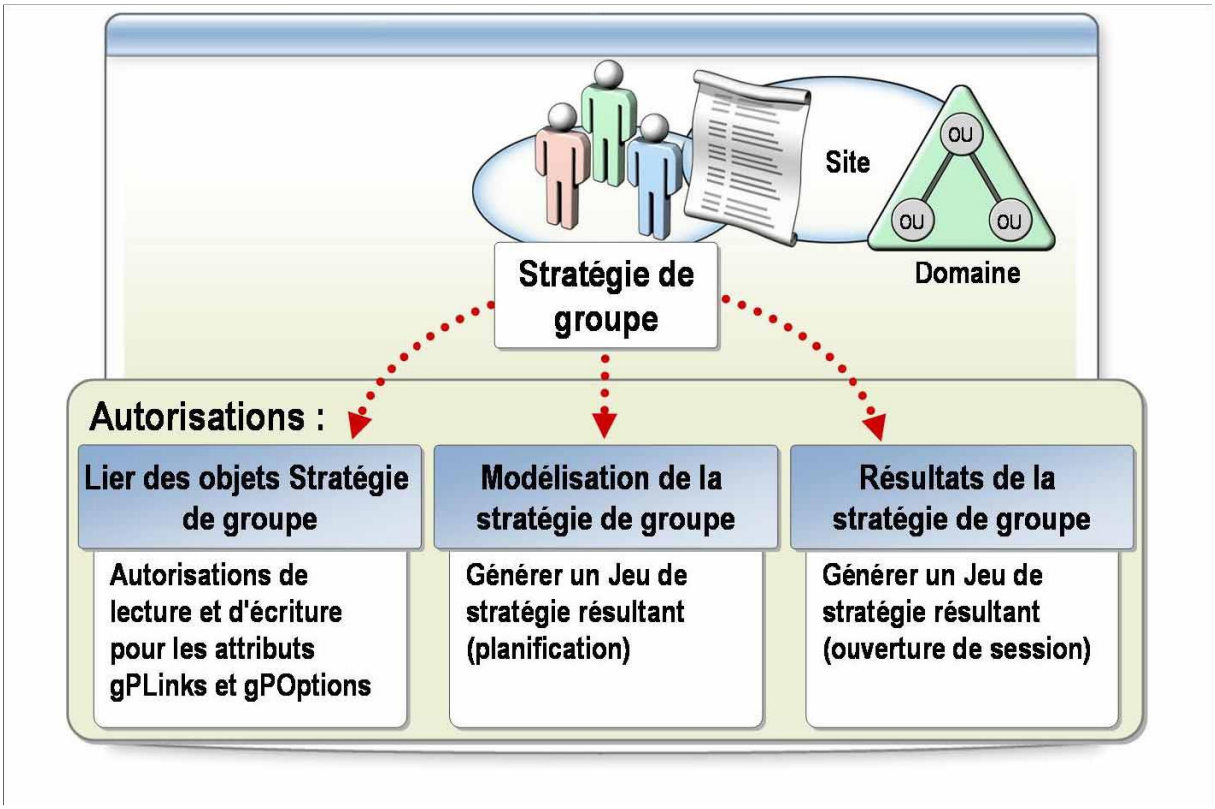
Les autorisations sont identiques, que vous ajoutiez un utilisateur au groupe Propriétaires créateurs de la stratégie de groupe ou que vous affectiez les autorisations utilisateur pour la création d'objets Stratégie de groupe directement à l'aide de la console Gestion de stratégie de groupe. Les utilisateurs peuvent créer des objets Stratégie de groupe dans le domaine et disposer d'un contrôle total sur ces objets, mais ils n'ont pas d'autorisation sur les objets Stratégie de groupe créés par d'autres utilisateurs.

Accorder à un utilisateur la possibilité de créer des objets Stratégie de groupe dans le domaine ne signifie pas qu'il peut lier ces objets 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 tâches. Les cinq catégories suivantes sont des autorisations Autoriser sur un objet Stratégie de groupe.

- Lecture
- Modifier les paramètres
- Modifier les paramètres, supprimer, modifier la sécurité
- Lire (à partir du filtrage de sécurité)
- Paramètres personnalisés

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



La délégation de la stratégie de groupe pour un site, un domaine ou une unité d'organisation inclut la délégation de la capacité à lier des objets Stratégie de groupe et la délégation des autorisations pour la Modélisation de stratégie de groupe et les Résultats de stratégie de groupe.

La console Gestion de stratégie de groupe utilise une autorisation unique, appelée Lier les objets GPO, pour gérer les attributs gPLink et gPOptions. Vous appliquez les paramètres d'un objet Stratégie de groupe à des utilisateurs et des ordinateurs en liant l'objet Stratégie de groupe (qu'il s'agisse d'un enfant direct ou indirectement par héritage) à un site, un domaine ou une unité d'organisation qui contient les objets utilisateur ou ordinateur.

L'autorisation Lier les objets GPO est spécifique à ce site, ce domaine ou à une unité d'organisation. L'autorisation équivaut à des autorisations Lire et Écrire sur les attributs gPLink et gPOptions du site, du domaine ou de l'unité d'organisation.

Vous pouvez utiliser la Modélisation de stratégie de groupe pour simuler un ensemble de stratégies pour des objets d'un domaine ou d'une unité d'organisation, ou bien vous pouvez la déléguer à d'autres utilisateurs ou groupes. Cette délégation affecte à l'utilisateur ou au groupe l'autorisation Générer Jeu de stratégie résultant (Planification), laquelle est disponible dans

toute forêt dotée du schéma Windows Server 2003.
La console Gestion de stratégie de groupe simplifie la gestion de cette autorisation en la faisant figurer sous l'onglet **Délégation** de tout domaine ou unité d'organisation. L'administrateur peut sélectionner **Lancer des analyses de modélisation de stratégie de groupe**, puis sélectionner les propriétés **Nom**, **S'applique à**, **Paramètre** et **Hérité** pour les délégations.

Vous pouvez utiliser les Résultats de stratégie de groupe pour lire les données d'enregistrement RSoP pour des objets du domaine ou de l'unité d'organisation.
Comme dans le cas de la Gestion de stratégie de groupe, vous pouvez déléguer cette autorisation à d'autres utilisateurs ou groupes. Les autorisations sont déléguées sur un domaine ou une unité d'organisation. Les utilisateurs disposant de cette autorisation 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), laquelle est disponible dans toute forêt dotée du schéma Windows Server 2003.
La console Gestion de stratégie de groupe simplifie la gestion de cette autorisation en la faisant figurer sous l'onglet **Délégation** du domaine ou de l'unité d'organisation. L'administrateur peut sélectionner **Lire les données du résultat de la stratégie**, puis sélectionner les utilisateurs et groupes auxquels accorder cette autorisation.

5.6. Planification d'une stratégie de groupe pour l'entreprise

5.6.1. Instructions de planification des objets Stratégie de groupe

Créez des objets Stratégie de groupe de façon à offrir une simplicité d'utilisation et de gestion optimale, notamment *via* l'utilisation de l'héritage et des liaisons multiples.
Appliquez les instructions suivantes pour planifier les objets Stratégie de groupe :

- *Appliquez les paramètres de stratégie de groupe au plus haut niveau*. De cette façon, vous bénéficiez de l'héritage de stratégie de groupe. Déterminez les paramètres communs des objets Stratégie de groupe pour le plus grand conteneur, en commençant par le domaine, puis en liant l'objet Stratégie de groupe de ce conteneur.
- *Diminuez le nombre des objets Stratégie de groupe*. Réduisez ce nombre

en utilisant plusieurs liaisons au lieu de créer plusieurs objets Stratégie de groupe identiques. Essayez de lier un objet Stratégie de groupe au plus grand conteneur possible, afin d'éviter de créer plusieurs liaisons du même objet à un niveau plus bas.

- *Créez des objets Stratégie de groupe spécialisés*. Utilisez ces objets Stratégie de groupe pour appliquer des paramètres uniques si nécessaire. Les objets Stratégie de groupe à un niveau supérieur n'appliqueront pas les paramètres de ces objets Stratégie de groupe spécialisés.
- *Désactivez les paramètres de configuration de l'ordinateur ou de l'utilisateur*. Lorsque vous créez un objet Stratégie de groupe destiné à contenir les paramètres de l'un de ces deux niveaux (utilisateur ou ordinateur), désactivez l'autre zone. Cela permet d'améliorer les performances d'application des objets Stratégie de groupe lors de la connexion de l'utilisateur et empêche l'application accidentelle des paramètres à l'autre zone.

5.6.2. Instructions pour 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 d'une entreprise. C'est pourquoi vous devez décider à l'avance d'appliquer la stratégie de groupe à tout ou partie des utilisateurs et ordinateurs.

Appliquez les instructions suivantes pour déterminer l'héritage des objets Stratégie de groupe.

- *Utilisez l'option Appliqué (Ne pas passer outre) uniquement lorsqu'elle est requise*. Utilisez cette option uniquement pour les objets Stratégie de groupe que vous voulez absolument appliquer, par exemple les paramètres de sécurité exigés par l'entreprise. Assurez-vous que ces objets Stratégie de groupe contiendront uniquement ces paramètres importants.
- *Utilisez l'option Blocage de l'héritage avec modération*. Ce paramètre complique la résolution des problèmes et l'administration des objets Stratégie de groupe.
- *Utilisez le filtrage de sécurité en cas de besoin uniquement*. Utilisez le filtrage de sécurité lorsque des paramètres s'appliquent uniquement à un groupe de sécurité particulier dans un conteneur. Limitez le nombre de filtres de sécurité en créant et en liant des objets Stratégie de groupe au niveau approprié.

5.6.3. Instructions 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 ce 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 à partir d'un autre site.

Appliquez les instructions suivantes pour déterminer une stratégie de groupe pour des sites :

- *Appliquez un objet Stratégie de groupe à un site uniquement si les paramètres sont spécifiques au site et non au domaine*. 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 contrôleurs de domaine sur ce site*. 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.

5.6.4. Instructions de planification de l'administration des objets Stratégie de groupe

Appliquez les instructions suivantes pour planifier l'administration des objets Stratégie de groupe :

- *Identifiez votre stratégie d'administration pour la gestion des objetsStratégie de groupe*. Déterminez quelles personnes vont créer et lier des objets Stratégie de groupe dans votre organisation, et quelles personnes vont mais ne pourront pas les créer. Déterminez également la personne 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 objetsStratégie de groupe au 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. Vous pouvez, par exemple, organiser la stratégie de groupe en fonction des catégories d'administration suivantes :

• Gestion de la configuration des utilisateurs
• Gestion des données
• Distribution des logiciels

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

5.6.5. Instructions de déploiement des objets Stratégie de groupe

Lorsque vous planifiez l'implémentation de la stratégie de groupe, veillez à tester et à documenter votre stratégie de groupe.
Appliquez les instructions suivantes pour déployer des objets Stratégie de groupe :

- *Testez les paramètres de stratégie de groupe*. Testez les résultats des objets Stratégie de groupe dans différentes situations. Bon nombre des organisations de moyenne et grande taille créent une version miniature de leur environnement de production pour l'utiliser comme « banc d'essai ».

Dans les petites entreprises, qui ne disposent pas des mêmes ressources, implémentez la stratégie de groupe dans l'environnement de production en dehors des heures de pointe, et mettez en place une stratégie de régression afin de corriger tout problème qui surviendrait. Les stratégies de test incluent :
• L'ouverture de session en tant qu'utilisateur représentatif sur des stations de travail représentatives, afin de vérifier que les paramètres de stratégie de groupe prévus ont bien été appliqués et qu'aucun conflit d'héritage ne se produit. Vous pouvez utiliser l'Assistant Modélisation de stratégie de groupe et l'Assistant Résultats de stratégie de groupe pour déterminer quels paramètres de stratégie de groupe ont été appliqués et à partir de quels objets Stratégie de groupe.
• L'ouverture de session dans toutes les conditions envisageables, afin de vous assurer que les paramètres de stratégie de groupe sont appliqués de façon homogène.
• Le test des ordinateurs portables en les connectant au réseau 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 inclure les informations suivantes dans votre liste :

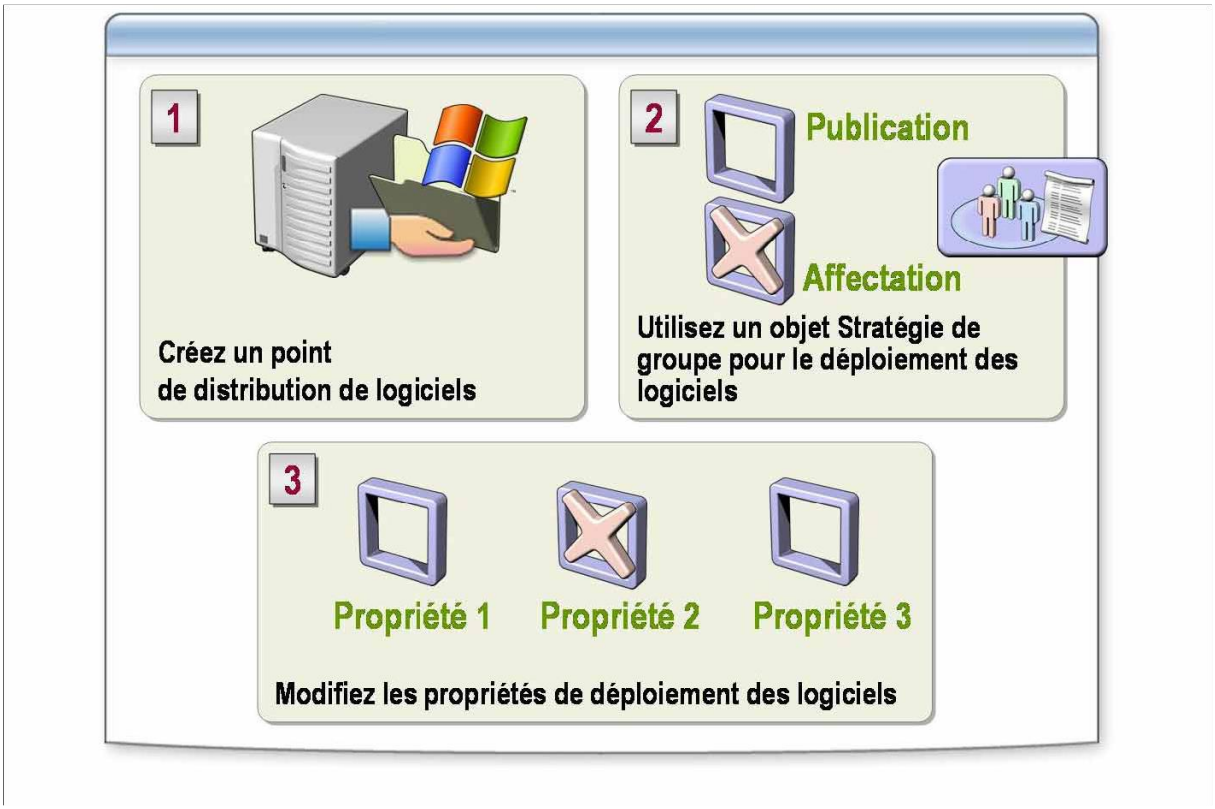
• Le nom et la fonction de chaque objet Stratégie de groupe.
• Les paramètres de stratégie de groupe de chaque objet Stratégie de groupe.
• Les liaisons d'objets Stratégie de groupe à un site, un domaine ou une unité d'organisation.

• Tout paramètre spécial appliqué à l'objet Stratégie de groupe (Appliqué, désactivation partielle ou totale, par exemple).

6. Déploiement et gestion des logiciels à l'aide d'une stratégie de groupe

6.1. Déploiement de logiciels

Le déploiement de logiciels garantit que les applications requises sont disponibles à partir de chaque ordinateur auquel l'utilisateur se connecte. Du point de vue de l'utilisateur, les logiciels sont toujours disponibles et fonctionnels. Les administrateurs peuvent installer à l'avance les logiciels pour les utilisateurs ou permettre à ceux-ci d'installer au coup par coup les logiciels dont ils ont besoin.



Lors du déploiement de logiciels, vous spécifiez comment les applications sont installées et gérées dans votre organisation.

Exécutez les tâches suivantes pour utiliser la stratégie de groupe pour le déploiement de nouveaux logiciels :

1. *Créez un point de distribution de logiciels*. Ce dossier partagé sur votre serveur contient les fichiers de package et de logiciels permettant le déploiement de logiciels. Lorsque des logiciels sont installés sur un ordinateur local, Windows

Installer copie des fichiers à partir de ce point de distribution. Le fait de rassembler les fichiers en un même endroit pour chaque application simplifie l'administration.
2. *Utilisez un objet Stratégie de groupe pour le déploiement des logiciels*. Vous devez créer ou modifier en conséquence un objet Stratégie de groupe pour le conteneur dans lequel vous souhaitez déployer l'application. Vous pouvez configurer l'objet Stratégie de groupe pour le déploiement de logiciels pour un compte d'utilisateur ou d'ordinateur. Cette tâche inclut la sélection du type de déploiement dont vous avez besoin.
3. *Modifiez les propriétés de déploiement des logiciels*. En fonction de vos besoins, vous pouvez modifier les propriétés qui avaient été définies durant le déploiement initial des logiciels.

6.1.1. Affectation de logiciels et publication de logiciels

L'affectation de logiciels et la publication de logiciels constituent les deux types de déploiement.
L'affectation des 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 lorsque l'utilisateur ouvre une session. Par exemple, si l'utilisateur ouvre un fichier qui utilise Microsoft Excel sur un ordinateur qui ne comporte pas Excel, mais que ce logiciel a été affecté à l'utilisateur, Windows Installer installe Excel sur cet ordinateur lorsque l'utilisateur ouvre le fichier concerné.
En outre, l'affectation de logiciels fait que ceux-ci sont tolérants aux pannes. Si, pour une raison quelconque, l'utilisateur supprime un logiciel, Windows Installer le réinstalle lorsque l'utilisateur se reconnecte et démarre l'application.

La publication des logiciels vous permet de vous assurer qu'ils sont disponibles aux utilisateurs pour que ceux-ci les installent sur leurs ordinateurs. Windows Installer n'ajoute pas de raccourcis sur le Bureau de l'utilisateur ou dans le menu **Démarrer**, et aucune entrée n'est enregistrée dans le registre local. Comme les utilisateurs doivent installer des logiciels publiés, vous ne pouvez publier des logiciels qu'auprès d'utilisateurs, pas auprès d'ordinateurs.

6.1.2. Création d'un point de distribution de logiciels

Pour déployer des logiciels pour des utilisateurs ou en assurer la disponibilité pour que ceux-ci les installent quand ils en ont besoin, créez un ou plusieurs points de distribution de logiciels dans lesquels vous copierez les logiciels concernés.

Pour créer un point de distribution de logiciels, procédez comme suit :
1. Créez un dossier partagé.
2. Créez les dossiers d'applications appropriés dans le dossier partagé.
3. Définissez l'autorisation appropriée pour le dossier partagé. Affectez aux utilisateurs l'autorisation en lecture (Read) sur le système de fichier NTFS afin qu'ils puissent accéder aux fichiers d'installation logicielle requis dans le point de distribution de logiciels.
4. Copiez dans les dossiers appropriés les packages Windows Installer ainsi que les fichiers connexes.

6.1.3. Utilisation d'un objet Stratégie de groupe pour le déploiement de logiciels

Après avoir créé un point de distribution de logiciels, créez un objet Stratégie de groupe qui déploie ces applications, puis reliez l'objet Stratégie de groupe au conteneur qui contient les utilisateurs ou les ordinateurs auprès desquels vous souhaitez déployer des logiciels.

Pour utiliser un objet Stratégie de groupe pour le déploiement de logiciels, procédez comme suit :
1. Créez ou éditez un objet Stratégie de groupe.
2. Sous **Configuration utilisateur** ou **Configuration ordinateur** (selon que vous affectez le logiciel à des utilisateurs ou des ordinateurs, ou que vous le publiez auprès d'utilisateurs), développez **Paramètres du logiciel**, cliquez avec le bouton droit sur **Installation logicielle**, pointez sur **Nouveau**, puis cliquez sur **Package**.
3. Dans la boîte de dialogue **Ouvrir un fichier**, naviguez jusqu'au point de distribution de logiciels à l'aide du nom UNC (Universal Naming Convention) . par exemple, *Nom_Serveur**Nom_Partage* .sélectionnez le fichier de package, puis cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue **Déploiement du logiciel**, sélectionnez une méthode de déploiement, puis cliquez sur **OK**.

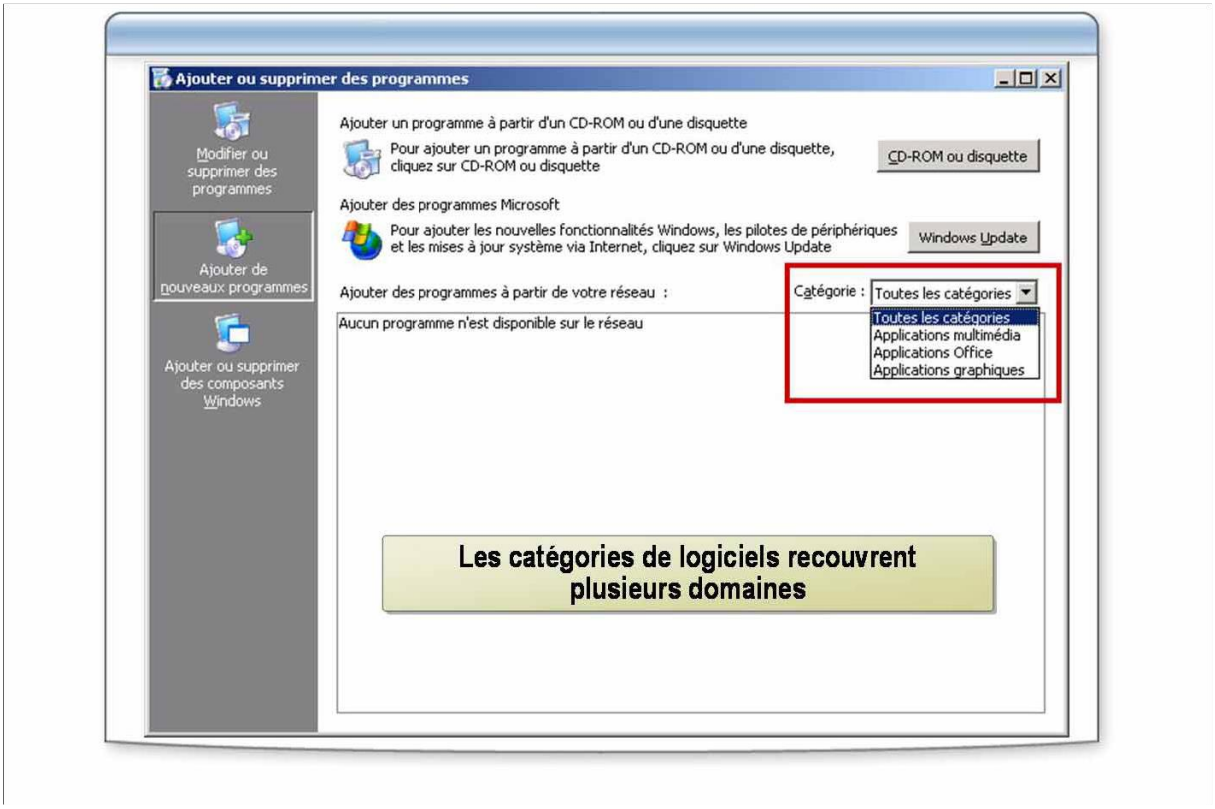
6.1.4. Options par défaut pour installation logicielle

Vous pouvez configurer les options par défaut d'installation logicielle pour l'objet Stratégie de groupe courant lorsque vous souhaitez ajouter simultanément plusieurs applications à un objet Stratégie de groupe ou utiliser les mêmes options pour elles par défaut.

6.2. Configuration du déploiement des logiciels

Installation de logiciel dans la stratégie de groupe inclut des options de configuration de logiciels déployés. Vous pouvez déployer plusieurs configurations différentes d'une application et contrôler comment cette application est affectée ou publiée chaque fois que les fonctions d'un utilisateur changent. Vous pouvez également simplifier la tâche de déploiement de logiciels en catégorisant les programmes répertoriés dans **Ajouter ou supprimer des programmes**, en associant des extensions de noms de fichiers avec des applications, et en ajoutant des modifications aux logiciels déployés.

6.2.1. Définition des catégories de logiciels



Vous utilisez des catégories de logiciels pour organiser des logiciels affectés et publiés en groupes logiques, afin que les utilisateurs puissent trouver aisément les applications dans **Ajouter ou supprimer des programmes** du Panneau de configuration. Windows Server 2003 est fourni sans catégories de logiciels prédéfinies.

Vous pouvez créer des catégories de logiciels pour regrouper différentes

Document	Page
4.Service d'annuaire Active Directory.doc	74 - 98

applications sous un en-tête spécifique. Au lieu de vous en remettre à une liste alphabétique des applications disponibles par défaut, vous pouvez organiser les logiciels en catégories, telles que Graphiques, Microsoft Office et Comptabilité.
Les utilisateurs peuvent alors choisir dans les catégories quelles applications installer dans **Ajouter ou supprimer des programmes**.
Les catégories de logiciels recouvrent plusieurs domaines. Vous les définissez une seule fois pour toute une forêt. Vous pouvez utiliser la même liste de catégories de logiciels dans toutes les stratégies dans la forêt.
La catégorisation des applications exige tout d'abord la création d'une catégorie, puis l'affectation des applications à la catégorie. Vous pouvez répertorier des packages sous plusieurs catégories.

6.2.2. Création de catégories de logiciels

La catégorisation des logiciels exige tout d'abord la création d'une catégorie de logiciels, puis l'affectation de logiciels à la catégorie.
Pour créer une catégorie, procédez comme suit :
1. Créez ou éditez un objet Stratégie de groupe.
2. Sous **Configuration utilisateur** ou **Configuration ordinateur** (selon que vous affectez le logiciel à des utilisateurs ou des ordinateurs, ou que vous le publiez auprès d'utilisateurs), développez **Paramètres du logiciel**, cliquez avec le bouton droit sur **Installation logicielle**, puis cliquez sur **Package**.
3. Dans l'onglet **Catégories**, cliquez sur **Ajouter** pour entrer une nouvelle catégorie.
4. Dans la zone **Catégorie**, tapez le nom de la catégorie puis cliquez deux fois sur **OK**.
Pour affecter un package de logiciels à une catégorie, procédez comme suit :
1. Créez ou éditez un objet Stratégie de groupe contenant le package de logiciels à catégoriser.
2. Dans l'arborescence de la console, développez **Paramètres du logiciel**, puis cliquez sur **Installation logicielle**.
3. Dans le volet de détails, cliquez avec le bouton droit sur le package de logiciels, puis cliquez sur **Propriétés**.
4. Dans l'onglet **Catégories**, affectez une ou plusieurs catégories au package de logiciels en cliquant sur la catégorie dans la liste **Catégories disponibles**, cliquez ensuite sur **Sélectionner**, puis sur **OK**.

7. Implémentation de sites pour gérer la réplication Active Directory

L'exécution d'une réplication dans le service d'annuaire Microsoft Windows Server. 2003 Active Directory® implique le transfert et la maintenance des données Active Directory entre les contrôleurs de domaine du réseau. Active Directory utilise un *modèle de réplication multimaître*.
Multimaître signifie qu'il y a plusieurs contrôleurs de domaine, également appelés principaux, qui ont l'autorisation de modifier ou de contrôler les mêmes données. Dans ce modèle de réplication, toute modification des données d'un contrôleur de domaine doit être répliquée sur tous les autres. En comprenant le fonctionnement du modèle de réplication Active Directory, vous pouvez gérer le trafic réseau de la réplication et assurer la cohérence des données Active Directory à travers votre réseau.

7.1. Présentation de la réplication Active Directory

Lorsqu'un utilisateur ou un administrateur exécute une action qui entraîne une mise à jour d'Active Directory, un contrôleur de domaine approprié est automatiquement désigné pour exécuter la mise à jour. Cette modification est effectuée de manière transparente sur l'un des contrôleurs de domaine.
Active Directory utilise la réplication multimaître avec cohérence relâchée pour s'assurer que tous les contrôleurs de domaine sont bien mis à jour. En connaissant le processus et la topologie de réplication, vous serez à même de gérer efficacement la réplication dans Active Directory.
La Réplication est le processus de mise à jour des données contenues dans Active Directory d'un contrôleur de domaine vers les autres contrôleurs de domaine du réseau. Ce processus synchronise le déplacement des données mises à jour entre les contrôleurs de domaine. La synchronisation garantit que toutes les données contenues dans Active Directory sont accessibles par tous les contrôleurs de domaine et les ordinateurs clients d'un réseau.

7.1.1. Réplication d'attributs à valeurs multiples liés

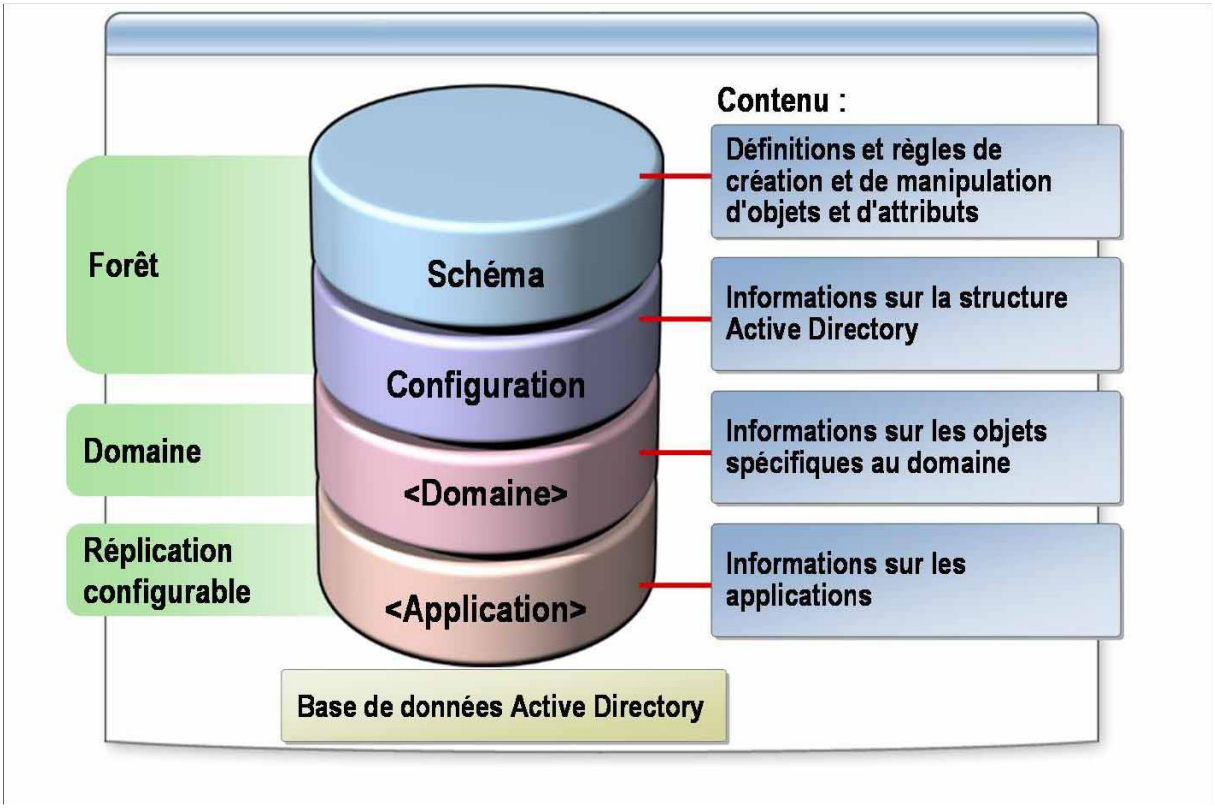
Le processus de réplication d'attributs à valeurs multiples liés est différent de celui de la réplication normale dans Active Directory.
Le processus qui réplique les attributs à valeurs multiples liés varie en fonction du niveau fonctionnel de la forêt :

- Lorsque le niveau fonctionnel de la forêt est antérieur à Windows Server

2003, toute modification apportée à l'appartenance de groupe déclenche la réplication de toute la liste des membres. Dans ce cas, l'attribut **member** à valeurs multiples est considéré comme un seul attribut dans le cadre de la réplication. Cette réplication augmente les risques d'écrasement d'une modification d'appartenance exécutée par un autre administrateur ou un autre contrôleur de domaine avant la réplication de la première modification.

- Lorsque le niveau fonctionnel de la forêt est défini sur Windows Server 2003, une valeur individuelle réplique les modifications aux attributs à valeurs multiples liés. Cette amélioration réplique les modifications uniquement aux informations d'appartenance et non à toute la liste des membres.

7.1.2. Définition des partitions d'annuaire



La base de données Active Directory est divisée de manière logique en plusieurs partitions : d'annuaire, du schéma, de la configuration, du domaine et d'application. Chaque partition est une unité de réplication et possède sa propre topologie de réplication. La réplication est exécutée entre les réplicas des partitions d'annuaire. Tous les contrôleurs de domaine de la même forêt ont au moins deux partitions d'annuaire en commun : celles du schéma et de la configuration. De plus, tous les contrôleurs de domaine partagent une partition

de domaine commune.

Partition de schéma

Chaque forêt possède une seule partition de schéma. Cette partition de schéma est stockée dans tous les contrôleurs de domaine de la même forêt. Elle contient les définitions de tous les objets et attributs créés dans l'annuaire, ainsi que les règles qui permettent de les créer et de les manipuler. Les données du schéma sont répliquées dans tous les contrôleurs de domaine de la forêt. C'est pourquoi les objets doivent être conformes aux définitions d'objet et d'attribut du schéma.

Partition de configuration

Chaque forêt possède une seule partition de configuration. Stockée dans tous les contrôleurs de domaine de la même forêt, la partition de configuration contient les données sur la structure Active Directory de l'ensemble de la forêt, dont les domaines et les sites existants, les contrôleurs de domaine existants dans chaque forêt et les services disponibles. Les données de la configuration sont répliquées dans tous les contrôleurs de domaine de la forêt.

Partition de domaine

Chaque forêt peut comporter plusieurs partitions de domaine. Les partitions de domaine sont stockées dans chaque contrôleur de domaine d'un domaine donné.
Une partition de domaine contient les données sur tous les objets propres au domaine et créés dans ce domaine, dont les utilisateurs, les groupes, les ordinateurs et les unités d'organisation. La partition de domaine est répliquée dans tous les contrôleurs de domaine de ce domaine. Tous les objets de chaque partition de domaine d'une forêt sont stockés dans le catalogue global avec un seul sous-ensemble de leurs valeurs d'attribut.

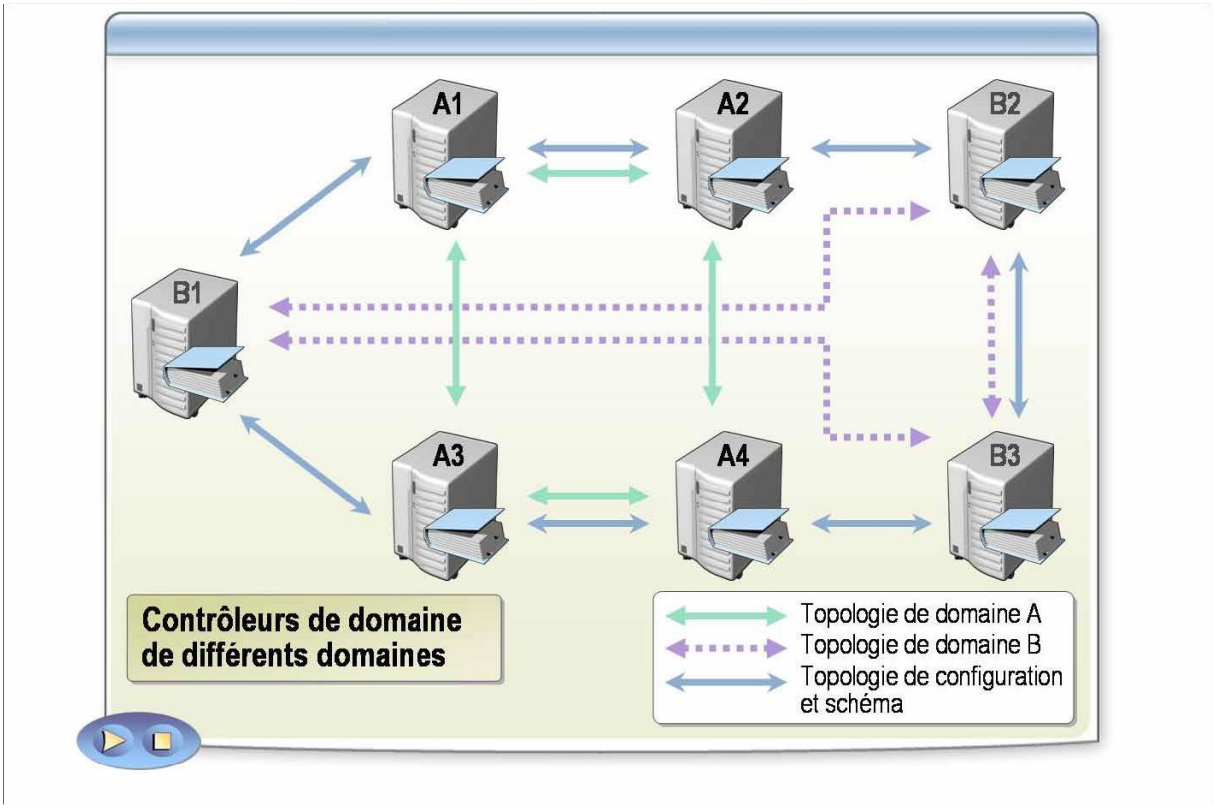
Partition d'applications

Les partitions d'applications stockent les données sur les applications dans Active Directory. Chaque application détermine comment elle stocke, classe et utilise ses propres données. Pour éviter toute réplication inutile des partitions d'applications, vous pouvez désigner les contrôleurs de domaine qui en hébergent dans une forêt. À la différence d'une partition de domaine, une partition d'applications ne peut pas stocker les principaux objets de sécurité, tels que les comptes d'utilisateurs. De plus, les données contenues dans une partition d'applications ne sont pas stockées dans le catalogue global.
Comme exemple de partition d'applications, si vous utilisez un système DNS qui est intégré à Active Directory, vous avez deux partitions d'applications pour les zones DNS : ForestDNSZones et DomainDNSZones.

- ForestDNSZones fait partie d'une forêt. Tous les contrôleurs de domaine et les serveurs DNS d'une forêt reçoivent un réplica de cette partition. Une partition d'applications d'une forêt entière stocke les données de la zone de la forêt.
- DomainDNSZones est unique pour chaque domaine. Tous les contrôleurs de domaine qui sont des serveurs DNS dans ce domaine reçoivent un réplica de cette partition. Les partitions d'applications stocke la zone DNS du domaine dans la DomainDNSZones <*nom_domaine*>.

7.1.3. Définition de la topologie de réplication

La topologie de réplication est l'itinéraire suivi par les données de la réplication à travers un réseau. La réplication se produit entre deux contrôleurs de domaine à la fois. Avec le temps, la réplication synchronise les données dans Active Directory pour toute une forêt de contrôleurs de domaine. Pour créer une topologie de réplication, Active Directory doit déterminer quels contrôleurs de domaine répliquent les données avec les autres contrôleurs de domaine.



Réplication de partitions

Active Directory crée une topologie de réplication basée sur les données stockées dans Active Directory. La topologie de réplication peut différer pour les partitions

de schéma, de configuration, de domaines et d'applications.
Tous les contrôleurs de domaine d'une même forêt partageant les partitions de schéma et de configuration, Active Directory réplique ces partitions de schéma et de configuration sur tous les contrôleurs de domaine. Les contrôleurs de domaine du même domaine répliquent également la partition du domaine.
De plus, les contrôleurs de domaine qui hébergent une partition d'applications répliquent la partition d'applications. Pour optimiser le trafic de la réplication, un contrôleur de domaine peut avoir plusieurs partenaires de réplication pour différentes partitions. Active Directory réplique les mises à jour d'annuaire dans tous les contrôleurs de domaine qui contiennent la partition mise à jour dans la forêt.

Objets de connexion

Les contrôleurs de domaine qui sont liés par des objets de connexion sont appelés *partenaires de réplication*. Les liens qui relient les partenaires de réplication sont appelés *objets de connexion*. Les objets de connexion sont créés dans chaque contrôleur de domaine et pointent vers un autre contrôleur de domaine pour une source de données de réplication. Les objets de connexion représentent un chemin de réplication à sens unique entre deux objets serveur.
La topologie de réplication par défaut d'un site est un anneau bidirectionnel, composé de deux objets de connexion unidirectionnels complémentaires entre deux contrôleurs de domaine adjacents. Cette topologie améliore la tolérance de pannes lorsque l'un des contrôleurs de domaine est déconnecté.
Si nécessaire, Active Directory crée des objets de connexion supplémentaires pour limiter statistiquement à un maximum de trois le nombre de tronçons empruntés pour répliquer une mise à jour provenant de tous les réplicas d'une partition donnée dans un anneau.

7.1.4. Génération automatique de la topologie de réplication

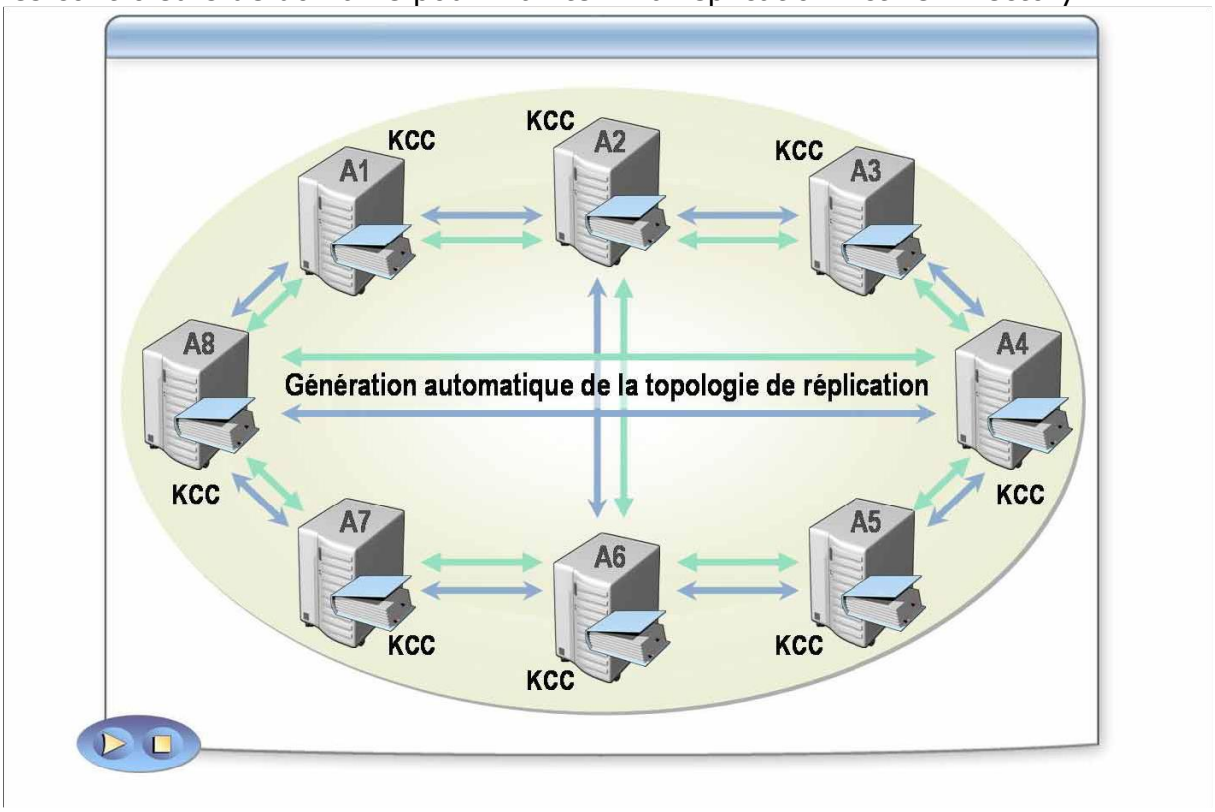
Lorsque vous ajoutez des contrôleurs de domaine à un site, Active Directory utilise le Vérificateur de cohérence de connaissances (KCC, *Knowledge Consistency Checker*) pour établir un chemin de réplication entre les contrôleurs de domaine.

Définition du KCC

KCC est un processus intégré qui s'exécute sur chaque contrôleur de domaine et génère la topologie de réplication pour toutes les partitions d'annuaire contenues dans ce contrôleur de domaine. Le vérificateur KCC s'exécute à intervalles définis

.par défaut toutes les 15 minutes . et désigne les itinéraires de réplication entre contrôleurs de domaine les plus judicieux disponibles à ce moment-là.

Pour générer automatiquement une topologie de réplication, le KCC évalue les données de la partition de configuration des sites, le coût de l'envoi des données entre ces sites (en fonction de la valeur relative des chemins de réplication), tout objet de connexion existant et les protocoles de réplication qu'il peut utiliser entre les sites. Ensuite, le KCC calcule les meilleures connexions pour envoyer les partitions d'annuaire d'un contrôleur de domaine vers les autres contrôleurs.
Si la réplication devient impossible dans un site ou à un point de défaillance unique, le KCC établit automatiquement de nouveaux objets de connexion entre les contrôleurs de domaine pour maintenir la réplication Active Directory.



7.1.5. Catalogue global et réplication de partitions

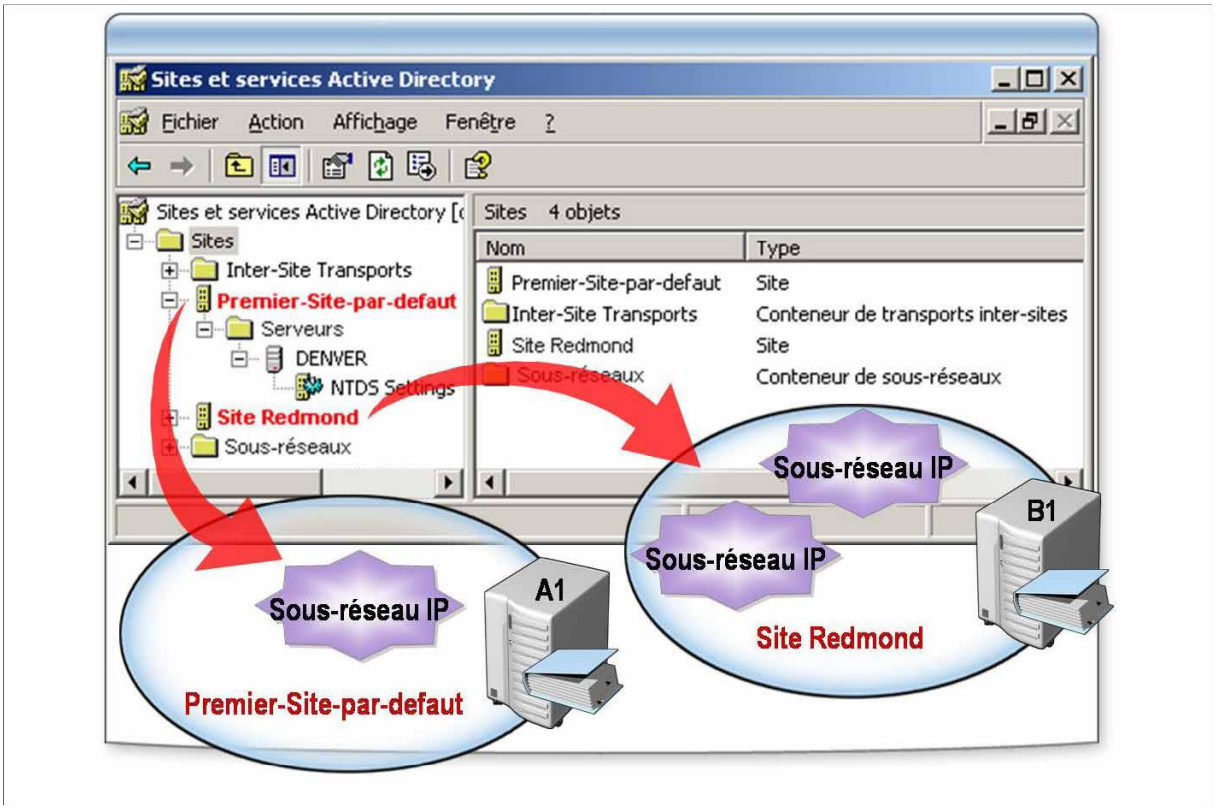
Un *serveur de catalogue global* est un contrôleur de domaine qui stocke deux partitions pour toute la forêt . les partitions de schéma et de configuration . plus une copie en lecture/écriture de la partition de son propre domaine et un réplica partiel de toutes les autres partitions de domaine dans la forêt. Ces réplicas partiels contiennent un sous-ensemble en lecture seule des données de chaque partition de domaine.
Lorsque vous ajoutez un nouveau domaine à une forêt, la partition de

configuration stocke les données sur ce nouveau domaine. Active Directory réplique la partition de configuration sur tous les contrôleurs de domaine, y compris les serveurs de catalogue global, lors d'une réplication normale dans toute la forêt. Chaque serveur de catalogue global devient un réplica partiel du nouveau domaine en contactant un contrôleur de domaine pour ce domaine et en obtenant les données du réplica partiel. La partition de configuration fournit également aux contrôleurs de domaine la liste de tous les serveurs de catalogue global de la forêt.
Les serveurs de catalogue global enregistrent les enregistrements DNS spéciaux dans la zone DNS qui correspond au domaine racine de forêt. Ces enregistrements, écrits uniquement dans la zone DNS racine de la forêt, aident les clients et les serveurs à localiser les serveurs de catalogue global à travers la forêt.

7.2. Création et configuration de sites

La réplication garantit que toutes les données contenues dans Active Directory sont à jour dans tous les contrôleurs de domaine et stations de travail d'un réseau. De nombreux réseaux sont composés de plusieurs réseaux plus petits, et les liens qui les connectent peuvent avoir des débits variés.
Vous utilisez des sites dans Active Directory pour contrôler la réplication et d'autres types de trafic Active Directory à travers les différentes liaisons du réseau. Lorsque vous configurez la réplication entre les sites, vous pouvez utiliser des objets sous-réseau, des liens de sites et des ponts entre les liens pour faciliter le contrôle de la topologie de réplication. La fiabilité et l'efficacité d'une topologie de réplication dépendent de la configuration des liens et des ponts entre les sites.

7.2.1. Définition des sites et des objets sous-réseau



Dans Active Directory, les sites facilitent la définition de la structure physique d'un réseau. Un ensemble de plages d'adresses de sous-réseaux TCP/IP définissent un site, qui à son tour définit un groupe de contrôleurs de domaine partageant les mêmes débits et coûts. Les sites sont composés d'objets serveurs, qui contiennent eux-mêmes les objets de connexion autorisant la réplication.
Les objets sous-réseau identifient les adresses réseau utilisées par mapper les ordinateurs avec les sites. Un sous-réseau est un segment d'un réseau TCP/IP auquel un ensemble d'adresses IP logiques est attribué. Les objets sous-réseau se mappant au réseau physique, les sites font de même. Par exemple, si trois sous-réseaux sont situés dans trois campus universitaires de la même ville et que ces campus sont reliés par des connexions à haut débit et à disponibilité élevée, vous pouvez associer chacun de ces sous-réseaux à un site.
Un site peut comporter un ou plusieurs sous-réseaux. Par exemple, pour un réseau composé de trois sous-réseaux à Redmond et deux à Paris, vous pouvez créer un site à Redmond, un à Paris et ajouter les sous-réseaux aux sites respectifs.

7.2.2. Liens de sites

Pour que deux sites échangent des données de réplication, ils doivent être connectés par un *lien de sites*, avec un chemin logique que le vérificateur

KCC utilise pour établir la réplication entre les sites.
Lorsque vous créez des sites supplémentaires, vous devez sélectionner au moins un lien de sites pour chaque site. Sans au moins un lien de sites, les connexions ne peuvent être établies entre les ordinateurs des différents sites, et la réplication entre sites ne peut donc pas avoir lieu. Les liens de sites supplémentaires ne se créent pas automatiquement. Pour ce faire, vous devez utiliser Sites et services Active Directory.
Lorsque vous créez le premier domaine d'une forêt, Active Directory crée un lien de sites par défaut appelé DEFAULTIPSITELINK. Il inclut le premier site et est situé dans le conteneur IP d'Active Directory. Vous pouvez le renommer.

Coût des liens de sites

Le coût des liens de sites est un nombre sans unité de mesure qui représente le débit relatif, la fiabilité et la préférabilité du réseau sous-jacent. Plus le coût d'un lien est bas, plus sa priorité est élevée, ce qui en fait un chemin privilégié. Par exemple, votre organisation a deux sites reliés entre eux, un dans le Casablanca et un à Rabat : une connexion haut débit et une connexion distante de secours.
Dans ce cas, vous configurez deux liens de sites : un pour chaque connexion.
La connexion à haut débit étant préférable à la connexion distante, configurez-la avec un coût inférieur à celui du lien de sites de la connexion distante. Lorsque le lien de sites avec la connexion à haut débit a un coût inférieur, sa priorité est plus élevée. Il est donc utilisé en priorité dès que possible.
En définissant le coût du lien de sites, vous pouvez déterminer la priorité relative de chaque lien de sites. La valeur par défaut du coût est de 100 et peut s'échelonner de 1 à 99999.

Planification de la réplication des liens de sites

La planification des horaires de réplication est un autre attribut des liens de sites que vous pouvez configurez. Lors de cette opération, vous spécifiez les horaires de disponibilité du lien pour la réplication. Souvent, la disponibilité de réplication est configurée à des heures où le trafic réseau est peu important : par exemple entre 2h00 et 5h00 du matin.
Plus le nombre d'heures pendant lesquelles un lien est disponible pour la réplication est restreint, plus le délai de latence entre les sites connectés par ce lien est grand. C'est pourquoi il faut trouver l'équilibre entre le besoin de réplication d'un lien pendant les heures à faible charge de travail et le besoin d'informations actualisées dans chaque site connecté par ce lien.

Fréquence de réplication des liens de sites

Lorsque vous configurez la fréquence de réplication, vous spécifiez le nombre de minutes que Active Directory doit attendre avant d'utiliser le lien pour vérifier si des mises à jour sont disponibles. La valeur par défaut de la fréquence de réplication est de 180 minutes. Vous devez choisir une valeur comprise entre 15 minutes et une semaine. La fréquence de réplication ne s'applique qu'aux heures pendant lesquelles le lien est programmé pour être disponible.
Des intervalles plus longs entre les cycles de réplication réduisent le trafic réseau et augmentent le délai de latence entre les sites. Des intervalles plus courts augmentent le trafic réseau et réduisent le délai de latence. C'est pourquoi il faut trouver l'équilibre entre le besoin de réduire le trafic réseau et le besoin d'informations actualisées dans chaque site connecté par ce lien.

Protocoles de transport des liens de sites

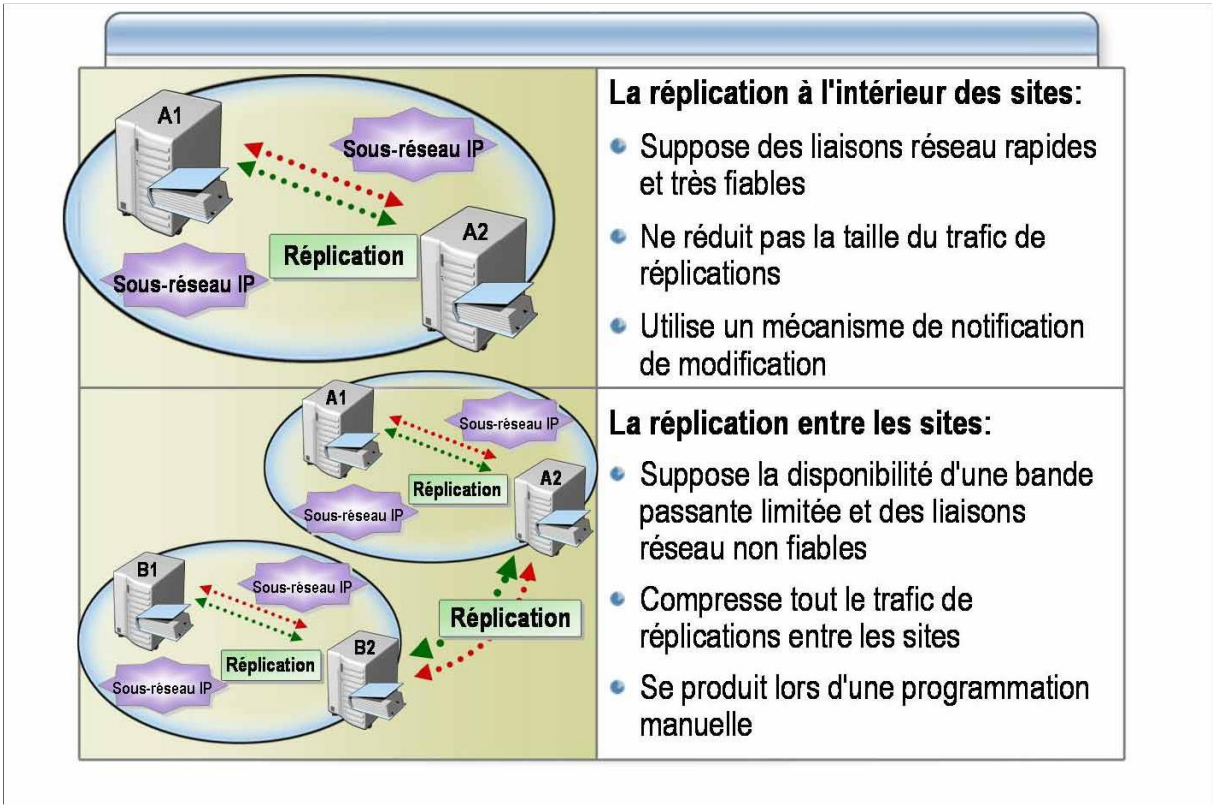
Un *protocole de transport* est un langage commun partagé par les ordinateurs pour communiquer entre eux pendant la réplication. Active Directory n'utilise qu'un seul protocole pour la réplication dans un site. Lorsque vous créez un lien de sites, vous devez en choisir un parmi les protocoles suivants :

- *RPC (Remote Procedure Call,* Appel de procédure distante*) sur IP*. RPC est le protocole par défaut. Protocole standard de l'industrie pour les communications clients/serveur, RPC sur IP fournit une connectivité fiable et à haut débit entre les sites. Entre les sites, RPC sur IP permet une réplication de toutes les partitions Active Directory. RPC sur IP est le meilleur protocole de transport pour la réplication entre sites.
- *SMTP (Simple Mail Transfer Protocol)*. Le protocole SMTP prend en charge la réplication du schéma, de la configuration et du catalogue global entre les sites et entre les domaines. Vous ne pouvez pas l'utiliser pour la réplication de la partition de domaine, car certaines opérations de domaine . par exemple, la Stratégie de groupe . requièrent la prise en charge du service de réplication de fichiers (FRS, *File Replication Service*), qui n'est pas compatible avec le transport asynchrone de la réplication. Si vous choisissez SMTP, vous devez installer et configurer une autorité de certificat pour signer les messages SMTP et garantir l'authenticité des mises à jour de l'annuaire. De plus, SMTP ne fournit pas le même niveau de compression des données que RPC sur IP.

7.2.3. Réplication à l'intérieur des sites et réplication entre les sites

Les principales caractéristiques ou hypothèses de la réplication à l'intérieur des sites sont les suivantes :

- Les connexions réseau d'un site sont fiables et ont suffisamment de bande passante disponible.
- Le trafic de réplications à l'intérieur d'un site n'est pas compressé car un site suppose la présence de liaisons réseau rapides et très fiables. Le fait de ne pas compresser le trafic de réplications réduit la charge de traitement des contrôleurs de domaine. Cependant, le trafic non compressé peut augmenter la bande passante réseau nécessaire aux messages de réplication.
- Un processus de notification de modification lance la réplication à l'intérieur d'un site.



Les principales caractéristiques ou hypothèses de la réplication entre sites sont les suivantes :

- La bande passante réservée aux liaisons réseau entre les sites est limitée et risque de ne pas être fiable.
- Le trafic de réplications entre les sites est conçu pour optimiser la bande passante en compressant tout le trafic de réplications entre les sites. Avant d'être transmis, ce trafic est compressé de 10 à 15 pour cent par rapport à sa taille originale. Bien que la compression optimise la bande passante du réseau, elle entraîne une charge de traitement supplémentaire des contrôleurs de domaine .lors de la compression et de

la décompression des données de la réplication.

- La réplication entre les sites se produit automatiquement dès que vous avez défini les valeurs configurables, telles que la planification et l'intervalle de réplication. Vous pouvez planifier la réplication aux heures creuses ou économiques. Par défaut, les modifications sont répliquées entre les sites selon une planification que vous définissez manuellement . et non pas en fonction du moment auquel se produisent les modifications. La planification détermine le moment de la réplication. L'intervalle spécifie la manière dont les contrôleurs de domaine vont vérifier la présence de modifications pendant la période de réplication planifiée.

Procédure de création d'un site

Pour créer un site, exécutez les opérations suivantes :

1. Ouvrez Sites et services Active Directory dans le menu **Outils d'administration**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau site**.
3. Dans la zone **Nom**, nommez le nouveau site.
4. Cliquez sur un objet lien de sites, puis cliquez deux fois sur **OK**.

Procédure de création d'un objet sous-réseau

Après avoir créé des sites, vous créez des sous-réseaux et les associez avec les sites.

Pour créer un objet sous-réseau, exécutez les opérations suivantes :

1. Dans Sites et Services Active Directory, dans l'arborescence de la console, double-cliquez sur **Sites**, cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
2. Dans la zone **Adresse**, entrez l'adresse IP du sous-réseau.
3. Dans la zone **Masque**, tapez le masque de sous-réseau qui décrit la plage d'adresses du sous-réseau.
4. Sélectionnez le site à associer à ce sous-réseau, puis cliquez sur **OK**.

Procédure de création de liens de sites

Pour créer un lien de sites, exécutez les opérations suivantes :

1. Dans Sites et Services Active Directory, développez **Sites**, puis **Inter-Site Transports**, cliquez avec le bouton droit sur **IP** ou **SMTP** en fonction du protocole qu'utilisera le lien, puis cliquez sur **Lien vers un nouveau site**.
2. Dans la zone **Nom**, nommez le lien.
3. Cliquez sur les sites à connecter, cliquez sur **Ajouter**, puis sur **OK**.

7.3. Gestion de la topologie de site

Pour satisfaire les besoins en réplication d'une organisation, vous pouvez être amené à exécuter manuellement certaines tâches de gestion de la topologie de site. Ces tâches comprennent l'identification des serveurs de tête de pont privilégiés, l'actualisation de la topologie de réplication et l'imposition de la réplication.

7.3.1. Serveur de tête de pont

Le *serveur de tête de pont* est un contrôleur de domaine que vous désignez pour envoyer et recevoir les données répliquées dans chaque site. Celui du site d'origine collecte toutes les modifications de la réplication et les envoie à celui du site destinataire, qui réplique les modifications dans tous les contrôleurs de domaine du site.

Vous devez désigner un serveur de tête de pont pour chaque partition du site.

Par exemple, un contrôleur de domaine peut être serveur de tête de pont pour les partitions de configuration et de schéma de l'ensemble de la forêt, ainsi que pour la partition de domaine du domaine qu'il représente. Si le site contient d'autres domaines, vous devez affecter un serveur de tête de pont à chacun d'eux.

Le serveur de tête de pont de chaque site est sélectionné automatiquement, ou vous pouvez désigner une liste de serveurs de tête de pont privilégiés. Pour garantir la fiabilité des mises à jour de l'annuaire, un serveur de tête de pont privilégié doit bénéficier d'une puissance de traitement et d'une largeur de bande suffisantes pour compresser, envoyer, recevoir et décompresser les données de la réplication avec efficacité. Active Directory utilise un seul serveur de tête de pont à la fois. Si le premier serveur privilégié devient indisponible, le prochain dans la liste des privilégiés est utilisé.

7.3.2. Générateur de topologie inter-sites

Le *générateur de topologie inter-sites* est un processus Active Directory qui définit la réplication entre les sites d'un réseau. Dans chaque site, un contrôleur de domaine est automatiquement désigné pour être le générateur de topologie inter-sites. Cette action étant effectuée par le générateur, vous n'avez pas à intervenir pour déterminer la topologie de la réplication et les rôles des serveurs de tête de pont.

Le contrôleur de domaine qui joue le rôle de générateur de topologie inter-sites exécute deux fonctions :

- Il sélectionne automatiquement un ou plusieurs contrôleurs de domaine pour devenir des serveurs de tête de pont. Ainsi, si l'un d'eux devient indisponible, il en sélectionne automatiquement un autre, si possible.
- Il exécute le vérificateur KCC pour déterminer la topologie de réplication et les objets de connexion résultants que le serveur de tête de pont peut utiliser pour communiquer avec les serveurs de tête de pont des autres sites.

Pour créer un serveur de tête de pont, exécutez les opérations suivantes :
1. Dans Sites et services Active Directory, développez **Sites**, puis le site contenant le serveur à configurer, développez **Servers**, et dans l'arborescence de la console, cliquez avec le bouton droit sur le contrôleur de domaine qui doit devenir un serveur de tête de pont privilégié, puis cliquez sur **Propriétés**.
2. Choisissez le ou les transports inter-sites pour lesquels ce serveur deviendra serveur de tête de pont privilégié, cliquez sur **Ajouter**, puis sur **OK**.

8. Implémentation du placement des contrôleurs de domaine

Un *contrôleur de domaine* est un ordinateur qui exécute Microsoft Windows Server. 2003 et qui stocke un réplica de l'annuaire du domaine. La possession de plusieurs contrôleurs de domaine dans un domaine permet de bénéficier de la tolérance de pannes. Si un contrôleur de domaine est hors connexion, un autre contrôleur peut assurer toutes les fonctions requises, comme l'enregistrement de modifications dans le service d'annuaire Active Directory. Les contrôleurs de domaine gèrent tous les aspects d'interaction dans le domaine des utilisateurs, comme la localisation d'objets Active Directory et la validation des tentatives d'ouverture de session par les utilisateurs.
Comme un domaine peut contenir un ou plusieurs contrôleurs de domaine, et que ceux-ci exécutent diverses fonctions clés, le placement de contrôleurs de domaine est une tâche importante dans l'implémentation d'Active Directory.

8.1. Implémentation du catalogue global dans Active Directory

Le catalogue global est le référentiel central des informations concernant les objets d'une forêt dans Active Directory. La mise en cache de l'appartenance au groupe universel dans Windows Server 2003 réduit le trafic et améliore le temps de connexion entre des liaisons lentes de réseau étendu (WAN, *Wide Area Network*). Vous devez comprendre les serveurs de catalogue global et la mise en cache de l'appartenance au groupe universel pour planifier le placement de contrôleurs de domaine dans votre réseau.

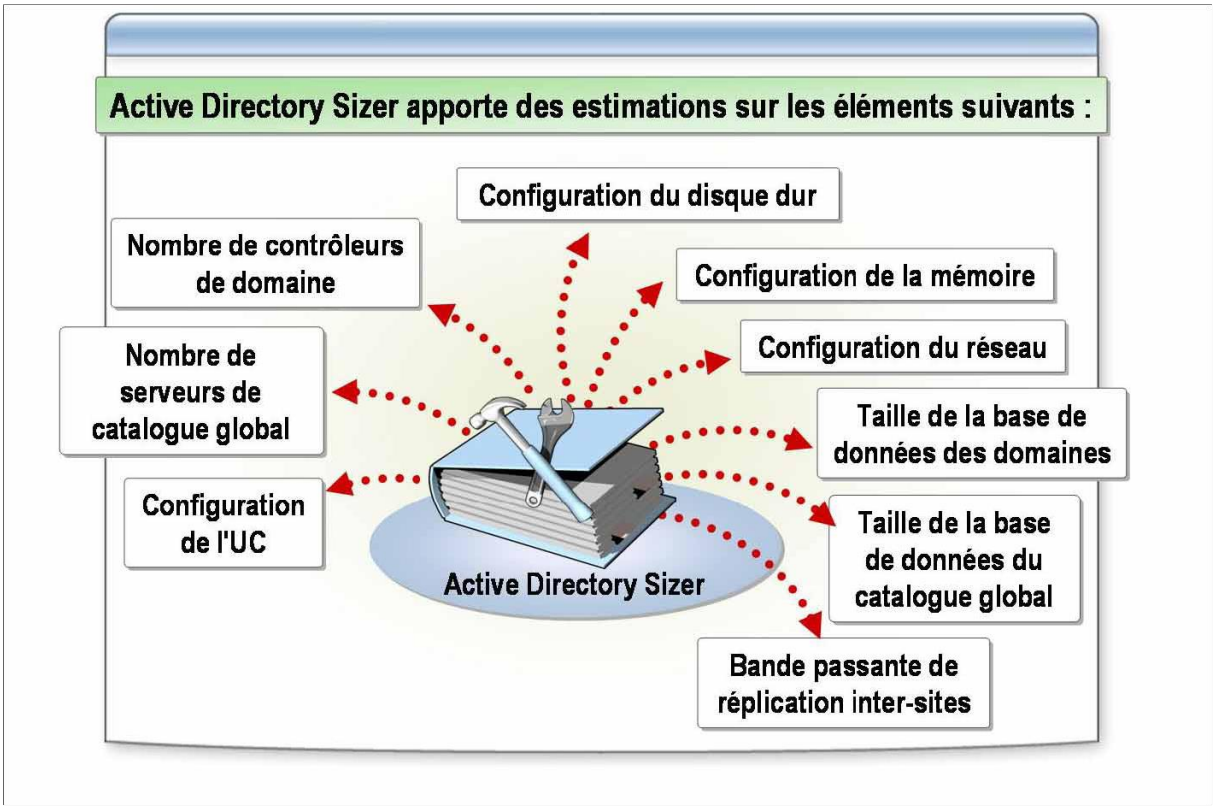
Un catalogue global résout les noms d'utilisateur principal lorsque le contrôleur de domaine procédant à l'authentification ne connaît pas le compte. Par exemple, si un compte d'utilisateur est situé dans exemple1.nwtraders.msft, et que l'utilisateur décide d'ouvrir une session sous le nom d'utilisateur principal user1@exemple1.nwtraders.msft à partir d'un ordinateur situé dans exemple2.nwtraders.msft, le contrôleur de domaine situé dans exemple2.nwtraders.msft ne pourra pas trouver le compte d'utilisateur ; il contactera alors un serveur de catalogue global pour terminer le processus de

connexion. Un catalogue global fournit des informations concernant l'appartenance au groupe universel dans un environnement à plusieurs domaines. Contrairement aux appartenances au groupe global, qu'Active Directory stocke dans chaque domaine, les appartenances au groupe universel ne sont stockées que dans un catalogue global. Par exemple, lorsqu'un utilisateur appartenant à un groupe universel se connecte à un domaine défini selon le niveau fonctionnel de domaine de Windows 2000 natif ou de Windows Server 2003, le catalogue global fournit des informations de l'appartenance au groupe universel concernant le compte d'utilisateur.

Si un catalogue global n'est pas disponible lorsqu'un utilisateur ouvre une session sur un domaine s'exécutant dans le niveau fonctionnel de domaine de Windows 2000 natif ou Windows Server 2003, le contrôleur de domaine qui traite la demande de connexion de l'utilisateur refuse la requête, et l'utilisateur ne peut pas ouvrir de session.

8.2. Détermination du placement de contrôleurs de domaine dans Active Directory

8.2.1. Active Directory Sizer



Active Directory Sizer (ADSizer.exe) vous aide à estimer la configuration matérielle requise pour déployer Active Directory en fonction du profil de l'organisation, des informations sur le domaine et de la topologie du site.
Vous utilisez Active Directory Sizer pour obtenir des estimations du nombre de :

- Contrôleurs de domaine par domaine par site.
- Serveurs de catalogue global par domaine par site.

Document	Page
4.Service d'annuaire Active Directory.doc	90 - 98

- Processeurs par ordinateur, ainsi que leur type.
- Disques requis pour stocker les données Active Directory.

Active Directory Sizer fournit également des estimations approximatives pour les besoins ou paramètres suivants :

- Quantité de mémoire
- Configuration réseau requise
- Taille de la base de données du domaine
- Taille de la base de données du catalogue global
- Bande passante requise pour la réplication inter-sites

Lorsque vous exécutez Active Directory Sizer, il collecte les informations suivantes sur chaque domaine afin de vous permettre de placer les contrôleurs de domaine avec précision :

- Nombre d'utilisateurs
- Attributs par utilisateur
- Groupes auxquels un utilisateur appartient
- Taux d'ouverture de sessions durant les heures de pointe
- Taux d'expiration des mots de passe
- Nombre d'ordinateurs
- Limite d'utilisation des processeurs
- Administration
- Informations concernant DNS (Domain Name System)

9. Planification du placement des contrôleurs de domaine

Avant de planifier le placement des contrôleurs de domaine, vous devez concevoir et déployer la topologie d'un site Active Directory. Pour Windows Server 2003, le service DNS a été soigneusement intégré dans la conception et l'implémentation d'Active Directory. Par conséquent, lorsque vous déployez ensemble Active Directory et Windows Server 2003, vous devez également planifier le placement des serveurs DNS intégrés à Active Directory.

Appliquez les instructions suivantes pour placer des contrôleurs de domaine :

- *Placez un contrôleur de domaine dans un site si* :

• *Le site comporte de nombreux utilisateurs*. Lorsque ces utilisateurs ouvrent une session, ils peuvent contacter un contrôleur de domaine local pour authentification au lieu de contacter un contrôleur de domaine distant par le biais d'une liaison WAN.
• *Des applications orientées site seront utilisées dans le site*. Ces applications peuvent ainsi accéder à un compte d'utilisateur et à d'autres informations à partir d'un contrôleur de domaine local.
• *Le site contient des ressources de serveur auxquelles les utilisateurs peuvent accéder lorsque la liaison avec le WAN n'est pas disponible*. Si la liaison avec le WAN n'est pas disponible et qu'aucun contrôleur de domaine local n'est disponible pour traiter les demandes de connexion, les utilisateurs ouvrent une session à l'aide d'informations de connexion en mémoire cache. Ils ne peuvent accéder à des ressources sur un autre ordinateur que celui sur lequel ils sont connectés. Si les utilisateurs doivent pouvoir accéder à des ressources sur

d'autres ordinateurs sur le réseau, configurez le contrôleur de domaine comme serveur de catalogue global. Ou bien activez au minimum la mise en cache de l'appartenance au groupe universel pour le site.

- *Ne placez pas un contrôleur de domaine dans un site dont la sécurité physique ou la maintenance est inadéquate*. Si un intrus peut accéde physiquement à un serveur, il lui est beaucoup plus facile de contourner les paramètres de sécurité et d'accéder aux données critiques de l'entreprise ou de les modifier. En l'absence de personnel assurant la maintenance des ordinateurs locaux, une panne matérielle ou logicielle sur un contrôleur de domaine peut interrompre le service pendant une durée prohibitive.
- *Déterminez le nombre de contrôleurs de domaine en fonction du nombre d'utilisateurs et des performances requises*. Utilisez Active Directory Sizer pour déterminer un processeur spécifique, la taille de la mémoire et les valeurs du réseau. Tenez compte également des besoins en termes de tolérance de pannes. Si Active Directory Sizer ne recommande qu'un seul contrôleur de domaine pour un site, mais que les utilisateurs doivent pouvoir ouvrir une session et accéder à des ressources locales basées sur un serveur en cas de rupture de liaison avec un WAN, envisagez de placer un second contrôleur de domaine dans le site afin de répondre à vos besoins en termes de tolérance de pannes.

10. Maintenance d'Active Directory

Les informations du service d'annuaire Active Directory® dans Microsoft Windows Server. 2003 sont stockées dans une base de données transactionnelle, laquelle facilite le maintien de l'intégrité des données en cas de défaillance. Le terme « défaillance » fait référence à toute panne matérielle, panne logicielle ou perte complète du système (par exemple, dans le cas d'un incendie).
La base de données Active Directory utilise des fichiers journaux de transactions pour récupérer les données corrompues dans une copie locale de la base de données. Après récupération des données, Active Directory utilise la réplication pour obtenir des données d'autres contrôleurs du domaine. Les interactions entre les composants Active Directory servent de base à Active Directory pour rassembler et sauvegarder des informations sur les données corrompues.
Lorsque les contrôleurs de domaine ne fonctionnent pas en raison de problèmes matériels ou logiciels, les utilisateurs risquent de ne pas pouvoir accéder aux ressources ou de ne pas pouvoir se connecter au réseau.

10.1. Base de données Active Directory et fichiers journaux

Le moteur de base de données d'Active Directory, ESE, stocke tous les objets d'Active Directory. Le moteur ESE utilise des transactions et des fichiers journaux pour garantir l'intégrité de la base de données Active Directory.

Active Directory inclut les fichiers suivants :

- *Ntds.dit*. La base de données Active Directory qui stocke tous les objets d'Active Directory au niveau du contrôleur de domaine. L'extension .dit fait référence à l'arborescence des informations de l'annuaire. Son

emplacement par défaut est le dossier %systemroot%\NTDS. Active Directory enregistre chaque transaction dans un ou plusieurs fichiers journaux associés au fichier Ntds.dit.

- *Edb*.log*. Le fichier journal des transactions dont le nom par défaut est Edb.log et d'une capacité de 10 mégaoctets (Mo). Lorsque le fichier Edb.log est saturé, Active Directory crée un autre fichier dénommé Edb*nnnnn*.log (où *nnnnn* correspond à l'ordre chronologique de création).

- *Edb.chk*. Un fichier de points de vérification que la base de données utilise pour garder une trace des données qui ne sont pas encore écrites dans le fichier de base de données Active Directory. Le fichier de points de vérification est un pointeur qui conserve des données de statut entre la mémoire et le fichier de la base de données sur le disque. Il indique le point de début à partir duquel les informations doivent être récupérées en cas de défaillance.

- *Res1.log et Res2.log*. Les fichiers journaux réservés de transactions. La quantité d'espace disque réservée sur un disque ou dans un dossier pour les journaux de transactions est de 20 Mo. Cet espace disque réservé offre aux fichiers journaux de transactions une marge suffisante de fermeture si le reste de l'espace disque est utilisé.

10.2. Déplacement et défragmentation de la base de données Active Directory

Au fil du temps, la fragmentation de la base de données se produit au fur et à mesure que des enregistrements sont ajoutés ou supprimés. Lorsque les enregistrements sont fragmentés, l'ordinateur doit parcourir la base de données Active Directory pour rechercher tous les enregistrements, et ce, à chaque fois que cette dernière est ouverte. Cette recherche ralentit le temps de réponse de la base de données. La fragmentation diminue également les performances générales des opérations de la base de données Active Directory.
Pour surmonter les problèmes liés à la fragmentation, vous devez défragmenter la base de données Active Directory. La *défragmentation* est le processus de réécriture des enregistrements dans la base de données Active Directory dans des secteurs contigus afin d'accroître la vitesse d'accès et d'extraction. Lorsque les enregistrements sont mis à jour, Active Directory enregistre ces mises à jour dans le plus large espace contigu de la base de données Active Directory.
Vous déplacez une base de données vers un nouvel emplacement lorsque vous défragmentez cette dernière. Déplacer la base de données ne supprimera pas la base de données originale. Vous pouvez donc utiliser la base de données originale si la base de données défragmentée ne fonctionne pas ou est corrompue. De même, si votre espace disque est limité, vous pouvez ajouter un autre disque dur pour y placer la base de données.
Enfin, vous pouvez déplacer les fichiers de la base de données en vue d'effectuer une opération de maintenance matérielle. Si le disque de stockage des fichiers doit être mis à niveau ou doit subir une opération de maintenance, vous pouvez déplacer les fichiers vers un autre emplacement de façon temporaire ou permanente.

Pour déplacer la base de données Active Directory, exécutez les étapes suivantes :

1. Par précaution, sauvegardez Active Directory.

Vous pouvez sauvegarder Active Directory en ligne si, dans l'Assistant de sauvegarde, vous choisissez de tout sauvegarder sur l'ordinateur ou de ne sauvegarder que les données d'état système.

2. Redémarrez le contrôleur de domaine, appuyez sur F8 pour afficher le menu **Menu d'options avancées de Windows**, sélectionnez **Mode restauration Active Directory**, puis appuyez sur ENTRÉE.
3. Ouvrez une session en utilisant le compte d'administrateur et le mot de passe défini pour le compte Administrateur local dans le Gestionnaire de comptes de sécurité (SAM, *Security Accounts Manager*).

4. À l'invite de commande, tapez **ntdsutil** et appuyez sur ENTRÉE.
5. Tapez **files** est appuyez sur ENTRÉE.
6. À l'invite **files**, et après avoir défini un emplacement offrant suffisamment d'espace pour y stocker la base de données, tapez **move DB to** <*drive*>:\<*directory*> (où <*drive*> et <*directory*> correspondent au chemin d'accès sur l'ordinateur local où vous voulez placer la base de données), puis appuyez sur ENTRÉE.
7. Tapez **quit** et appuyez sur ENTRÉE. Pour revenir à l'invite, tapez de nouveau **quit**.
8. Redémarrez le contrôleur de domaine.

Pour défragmenter une base de données Active Directory hors connexion, exécutez les étapes suivantes :

1. Sauvegardez les données d'état système.
2. Redémarrez le contrôleur de domaine, appuyez sur F8 pour afficher le menu **Menu d'options avancées de Windows**, sélectionnez **Mode restauration Active Directory**, puis appuyez sur ENTRÉE.
3. Ouvrez une session en utilisant le compte Administrateur et le mot de passe défini pour le compte Administrateur local dans le Gestionnaire des comptes de sécurité (SAM) hors connexion.
4. À l'invite de commande, tapez **ntdsutil** et appuyez sur ENTRÉE.
5. Tapez **files** est appuyez sur ENTRÉE.
6. À l'invite **files**, tapez **compact to <***drive***>:\<***directory***>** (où <*drive*> et <*directory*> définissent le chemin d'accès) et appuyez sur ENTRÉE.

Cette étape permet de définir un emplacement avec suffisamment d'espace disque libre pour y stocker la base de données compressée.

Si le chemin d'accès contient des espaces, il doit être mis entre guillemets (par exemple, « C:\Nouveau dossier »).

Une nouvelle base de données Ntds.dit est créée à l'emplacement spécifié.

7. Tapez **quit** et appuyez sur ENTRÉE. Pour revenir à l'invite, tapez de nouveau **quit**.
8. Remplacez l'ancien fichier Ntds.dit par le nouveau fichier dans le chemin d'accès de la base de données Active Directory.
9. Redémarrez le contrôleur de domaine.

10.3. Sauvegarde d'Active Directory

La sauvegarde d'Active Directory est essentielle pour la maintenance de la base de données Active Directory. Vous pouvez sauvegarder Active Directory en utilisant l'interface utilisateur graphique et les outils de ligne de commande de la famille Windows Server 2003.
Sauvegarder fréquemment les données d'état système des contrôleurs de domaine vous permet de restaurer des données toujours actualisées. En définissant un programme de sauvegarde régulière, vous avez plus de chance de pouvoir récupérer toutes les données en cas de nécessité.
Pour garantir une bonne sauvegarde, englobant au moins les données d'état système et le contenu du disque système, vous devez connaître la durée de vie des objets de désactivation. Par défaut, les objets de désactivation ont une durée de vie de 60 jours. Toute sauvegarde ultérieure à 60 jours n'est pas une sauvegarde correcte. Planifiez la sauvegarde d'au moins deux contrôleurs de domaine dans chaque domaine, dont l'un est détenteur du rôle de maître des opérations. Pour chaque domaine, vous devez conserver au moins une sauvegarde pour permettre une restauration forcée des données en cas de besoin.
Pour sauvegarder les données d'état système, exécutez les étapes suivantes :
1. Dans le menu **Démarrer**, pointez sur **Tous les programmes**, sur **Accessoires** et sur **Outils système**, puis cliquez sur **Utilitaire de sauvegarde**.
2. Dans la page **Assistant Sauvegarde ou Restauration**, cliquez sur **Suivant**.
3. Dans la page **Sauvegarder ou Restaurer**, cliquez sur **Sauvegarder des fichiers et des paramètres**, puis sur **Suivant**.
4. Dans la page **Que voulez-vous sauvegarder ?**, cliquez sur **Me laisser choisir les fichiers à sauvegarder**, puis sur **Suivant**.
5. Dans la page **Éléments à sauvegarder**, développez **Poste de travail**, activez la case à cocher **System State**, puis cliquez sur **Suivant**.
6. Dans la page **Type, nom et destination de la sauvegarde**, cliquez sur **Parcourir**. Sélectionnez ensuite un emplacement pour la sauvegarde et cliquez sur **Enregistrer**, puis sur **Suivant**.
7. Dans la page **Fin de l'Assistant Sauvegarde ou Restauration**, cliquez sur **Terminer**.
8. Dans la page **Sauvegarde en cours**, cliquez sur **Fermer**.

10.4. Restauration d'Active Directory

Dans Windows Server 2003, vous pouvez restaurer la base de données Active Directory si cette dernière a été corrompue ou détruite suite à une défaillance matérielle ou logicielle. Vous devez restaurer la base de données Active Directory lorsque des objets dans Active Directory ont été modifiés ou supprimés.
Vous pouvez restaurer des données répliquées dans un contrôleur de domaine de plusieurs façons. Vous pouvez réinstaller le contrôleur de domaine, puis laisser le processus de réplication normale alimenter le nouveau contrôleur de domaine avec les données de ses réplicas. Vous pouvez également utiliser l'Utilitaire de sauvegarde pour restaurer des données répliquées à partir d'un support de sauvegarde sans réinstaller le système d'exploitation ou reconfigurer le contrôleur de domaine.

Vous pouvez utiliser l'une des trois méthodes suivantes de restauration Active Directory à partir du support de sauvegarde : *restauration principale, normale ou forcée*.

! *Restauration principale*. Cette méthode de restauration reconstruit le premier contrôleur de domaine dans un domaine lorsqu'il n'est pas possible de reconstruire le domaine d'une autre façon. Effectuez une restauration principale uniquement lorsque tous les contrôleurs du domaine sont perdus et que vous souhaitez reconstruire le domaine à partir de la sauvegarde.
! *Restauration normale*. Cette méthode de restauration rétablit les données Active Directory dans l'état où elles étaient avant la sauvegarde, puis met à jour les données par le biais du processus de réplication normale. Effectuez une restauration normale uniquement lorsque vous souhaitez restaurer un seul contrôleur de domaine à son état précédent.
! *Restauration forcée*. Vous effectuez cette restauration en tandem avec la restauration normale. Une restauration forcée balise des données spécifiques comme données actuelles et empêche la réplication d'écraser ces données.
Les données forcées sont ensuite répliquées dans tout le domaine.
Effectuez une restauration forcée pour restaurer des objets individuels dans un domaine comportant plusieurs contrôleurs de domaine. Lorsque vous effectuez une restauration forcée, vous perdez tous les changements apportés après la sauvegarde aux objets de la restauration.

Pour effectuer une restauration principale d'Active Directory, exécutez les étapes suivantes :
1. Redémarrer votre contrôleur de domaine en Mode restauration
Active Directory.
2. Démarrez l'Utilitaire de sauvegarde.
3. Dans la page **Assistant Sauvegarde ou Restauration**, cliquez sur **mode avancé**.
4. Dans la page **Utilitaire Sauvegarde en mode avancé**, sous l'onglet **Restaurer et gérer le média**, sélectionnez les éléments à restaurer, puis cliquez sur **Démarrer**.
5. Dans la boîte de dialogue **Avertissement**, cliquez sur **OK**.
6. Dans la boîte de dialogue **Confirmation de restauration**, cliquez sur **Avancé**.
7. Dans la boîte de dialogue **Options de restauration avancées**, cliquez sur **Lors de la restauration de jeux de données répliqués, marquer les données restaurées en tant que données principales pour tous les réplicas**, puis cliquez deux fois sur **OK**.
8. Dans la boîte de dialogue **Restauration en cours**, cliquez sur **Fermer**.
9. Dans la boîte de dialogue **Utilitaire de sauvegarde**, cliquez sur **Oui**.

Pour effectuer une restauration normale d'Active Directory, exécutez les étapes suivantes :
1. Redémarrer votre contrôleur de domaine en Mode restauration Active Directory.
2. Démarrez l'Utilitaire de sauvegarde.
3. Dans la page **Assistant Sauvegarde ou Restauration**, cliquez sur **Suivant**.
4. Dans la page **Sauvegarder ou restaurer**, cliquez sur **Restaurer des fichiers et des paramètres**.
5. Dans la page **Que voulez-vous restaurer**, sous **Éléments à restaurer**, développez la liste, activez la case à cocher **System State**, puis cliquez sur **Suivant**.
6. Dans la page **Fin de l'Assistant Sauvegarde ou Restauration**, cliquez sur **Terminer**.

7. Dans la boîte de dialogue **Avertissement**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Restauration en cours**, cliquez sur **Fermer**.
9. Dans la boîte de dialogue **Utilitaire de sauvegarde**, cliquez sur **Oui**.

Pour effectuer une restauration forcée, exécutez les étapes suivantes :
1. Redémarrer votre contrôleur de domaine en Mode restauration
Active Directory.
2. Restaurez Active Directory dans son emplacement d'origine.
3. Si vous devez effectuer une restauration forcée au niveau du dossier SYSVOL, restaurez Active Directory dans un autre emplacement par l'intermédiaire de l'Utilitaire de sauvegarde. Surtout, ne redémarrez pas votre ordinateur après la restauration, même si un message vous y invite. Si vous n'effectuez pas une restauration forcée au niveau du dossier SYSVOL, passez à l'étape 4.
4. À l'invite, exécutez **Ntdsutil.exe**.
5. À l'invite **ntdsutil**, tapez **authoritative restore**.
6. À l'invite **authoritative restore**, tapez **restore subtree** *nom_unique_de_l'objet* (où *nom_unique_de_l'objet* correspond au nom unique, ou chemin d'accès, de l'objet). Par exemple, pour restaurer une unité d'organisation nommée formation, présente directement sous le domaine gsimaroc.com, tapez **restore subtree OU=formation,DC=gsimaroc,DC=com**
7. Tapez **quit** et appuyez sur ENTRÉE.
8. Tapez de nouveau **quit**, puis appuyez sur ENTRÉE pour quitter **ntdsutil**.
9. Redémarrez le contrôleur de domaine.
10. Après publication du dossier SYSVOL par le système FRS, copiez le dossier SYSVOL et uniquement les dossiers de la stratégie de groupe correspondant aux objets de la stratégie de groupe restaurés depuis le nouvel emplacement vers les emplacements existants.
11. Pour vérifier que l'opération de copie s'est bien déroulée, examinez le contenu du dossier SYSVOL*Domaine*, où *Domaine* correspond au nom de domaine.