

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

### 1. Introduction.

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

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

#### a) Introduction

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

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

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

#### **Cycle de vie d'unités d'organisation.**

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

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

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

Microsoft Windows Server 2003 fournit plusieurs 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.

**Méthodes de création et de gestion des unités d'organisation**

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

- *Utilisateurs et ordinateurs Active Directory.* Ce composant logiciel enfichable MMC permet de créer, modifier et supprimer des unités d'organisation. Utilisez ce composant logiciels enfichable lorsque vous n'avez que quelques unités d'organisation à gérer, ou lorsque vous souhaitez gérer des unités de manière interactive.
- *Outils de service d'annuaire.* Cet ensemble d'outils de ligne de commande permet de gérer des objets et d'effectuer des requêtes d'informations dans active Directory. Les outils de ligne de commande incluent Dsadd, Dsmode et Dsrm. L'utilisation de ces outils avec le paramètre « ou » vous permet d'ajouter, de modifier et de supprimer des unités d'organisation dans Active Directory. Vous pouvez également utiliser des scripts et des fichiers de commandes avec ces outils pour gérer des services d'annuaire.
- *Ldifde (lightweight Directory Access Protocol Data Interchange Format Directory Exchange).* Cet outils de ligne de commande permet de créer des unités d'organisation et d'autre objets Active Directory. Ldifde utilise un fichier d'entrée contenant des informations sur les objets à ajouter, modifier ou supprimer. Ces informations sont stockées sous la forme d'une série d'enregistrements, séparés par une ligne vide dans un fichier d'entrée.
- *Environnement d'exécution de scripts Windows.* Vous pouvez créer des unités d'organisation à l'aide d'applications Windows, ou à l'aide de scripts Windows avec les composants 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.

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

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

### Procédure de création d'une unité d'organisation

Pour créer une unité d'organisation, 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 d'organisation *SupportTechnique* au domaine *nwtraders.msft*, le nom unique serait *ou=supporttechnique,dc=nwtarders,dc=msft*.
- *Description* spécifie la description de l'unité d'organisation que vous désirez ajouter.
- *Domaine* spécifie le domaine auquel se connecter. Par défaut, l'ordinateur est connecté au contrôleur de domaine du domaine sur lequel il a ouvert une session.
- *Nom\_Utilisateur* spécifie le nom permettant de se connecter à un serveur distant. Par défaut, le nom de l'utilisateur connecté est utilisé. Vous pouvez spécifier un nom d'utilisateur selon l'un des formats suivants :
  - Nom d'utilisateur (par exemple, Linda)
  - Domaine\nom d'utilisateur (par exemple, widgets\Linda)
  - Nom d'utilisateur principal (UPN, *User Principal Name*) (par exemple, [Linda@widgets.microsoft.com](mailto:Linda@widgets.microsoft.com))
- *Mot\_de\_passe* est le mot de passe à utiliser pour ouvrir une session sur un serveur distant. Si vous tapez \*(astérisque), un mot de passe vous sera demandé.

### Procédure de modification d'une unité d'organisation

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

```
Dsmmod ou NU_Unité_Organisation -desc Description -d Domaine -u  
Nom_Utilisateur -p Mot_de_passe
```

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

### **Procédure de suppression d'une unité d'organisation**

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

```
Dsrm ou NU_Unité_Organisation -d Domaine -u Nom_Utilisateur -p  
Mot_de_passe
```

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

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

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

### Procédure

La première étape à exécuter pour utiliser cet outil consiste à créer le fichier d'entrée (\*.ldf) 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=ExempleOU,DC=nwtraders,DC=msft
changetype : add
objectClass : organizationalUnit
```

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

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

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

```
C:\>ldifde -i -k -f OUList.ldf -b Nom_Utilisateur Domaine Mot_de_passe
```

Où :

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

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

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

### Procédure

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

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

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

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

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

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

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

```
objOU.SetInfo
```

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

```
Wscript nom_fichier_script.vbs
```

3.

## Délégation du contrôle administratif des unités d'organisation.

### a) Introduction.

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

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

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

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

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

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

#### **Pourquoi déléguer l'administration ?**

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

L'autonomie correspond à la possibilité qu'on les 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.

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

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

**Tâches d'administration courantes.**

Les administrateurs exécutent régulièrement les tâches suivantes dans Active Directory :

- *Modification des propriétés sur un conteneur particulier.* Par exemple, lorsqu'un nouvel ensemble de logiciels est disponible, les administrateurs peuvent créer une stratégie de groupe qui contrôle leur distribution.
- *Création et suppression d'objets d'un type particulier.* Dans une unité d'organisation, ces types spécifiques peuvent être les utilisateurs, les groupes et les imprimantes. Lorsqu'un nouvel employé rejoint l'organisation, par exemple, vous créez un compte d'utilisateur pour l'employé, puis vous ajoutez cet employé dans l'unité ou le groupe d'organisation approprié.
- *Mise à jour de propriétés spécifiques sur des objets d'un type donné* dans une unité d'organisation. Il se peut que la tâche d'administration la plus courante que vous effectuiez, concernant la mise à jour de propriétés, inclut des tâches comme la réinitialisation des mots de passe et la modification des informations personnelles d'un employé, telles que son adresse et son numéro de téléphone en cas de déménagement, par exemple.

d) Comment déléguer le contrôle administratif.

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

**Procédure.**

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

1. Procédez comme suit pour démarrer l'Assistant Délégation de contrôle :
  - a. ouvrez la console Utilisateurs et ordinateurs Active Directory.
  - b. Dans l'arborescence de la console, double-cliquez sur le nœud du domaine.
  - c. Dans le volet de détails, cliquez avec le bouton droit sur l'unité d'organisation, cliquez ensuite sur **Déléguer le contrôle**, puis sur **Suivant**.
2. Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez déléguer des tâches d'administration courantes. Pour ce faire, procédez comme suit :
  - a. Dans la page **Utilisateurs ou groupes** cliquez sur **Ajouter**.
  - b. Dans la 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**, sélectionner les tâches que vous souhaitez déléguer, puis cliquez sur **Suivant**.
4. Cliquez sur **Terminer**.

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

e) Comment personnaliser le contrôle administratif délégué.

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

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

**Procédure.**

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

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

f) Comment vérifier la délégation du contrôle administratif.

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

**Procédure**

Procédez comme suit pour vérifier la délégation du contrôle :

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

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

a) Introduction

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

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

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

**Processus de planification d'unité d'organisation**

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

- *Documentez la structure existante de l'organisation.* Lors de la documentation de la structure existante de l'organisation, une stratégie consiste à diviser les tâches d'administration en catégories, puis à documenter les administrateurs qui sont 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 délégation :

- *Déterminez le niveau d'administration.* Décidez ce que chaque groupe contrôlera et à quel niveau vous déléguerez l'administration dans la hiérarchie administrative. Lorsque vous créez le plan, identifiez quels groupes :
  - Auront un contrôle intégral sur les objets d'une classe particulière ; ces groupes peuvent créer et supprimer des objets dans une classe spécifiée et modifier tous les attributs des objets dans la classe spécifiée.
  - Seront autorisés à créer des objets d'une classe particulières ; par défaut, les utilisateurs ont le contrôle intégral des objets qu'ils créent ;
  - Seront autorisés à ne modifier que des attributs spécifiques d'objets existants d'une classe particulière.
- *Identifiez chaque administrateur et compte d'utilisateur dans votre organisation ainsi que les ressources qu'ils administrent.* Ces informations vous aideront à déterminer la propriété et les autorisations affectées aux unités d'organisation que vous créez pour prendre en charge la plan de délégation.

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

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

**Types de modèles d'administration informatique.**

Les organisations informatiques les plus courantes sont les suivantes :

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

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

### **Structure d'un modèle d'administration informatique.**

La structure du modèle d'administration informatique reflète la façon dont une organisation gère ses ressources informatiques, comme les utilisateurs, les ordinateurs, les groupes, les imprimantes et les fichiers partagés.

Les différentes manières selon lesquelles les modèles d'administration sont structurés incluent :

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

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

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

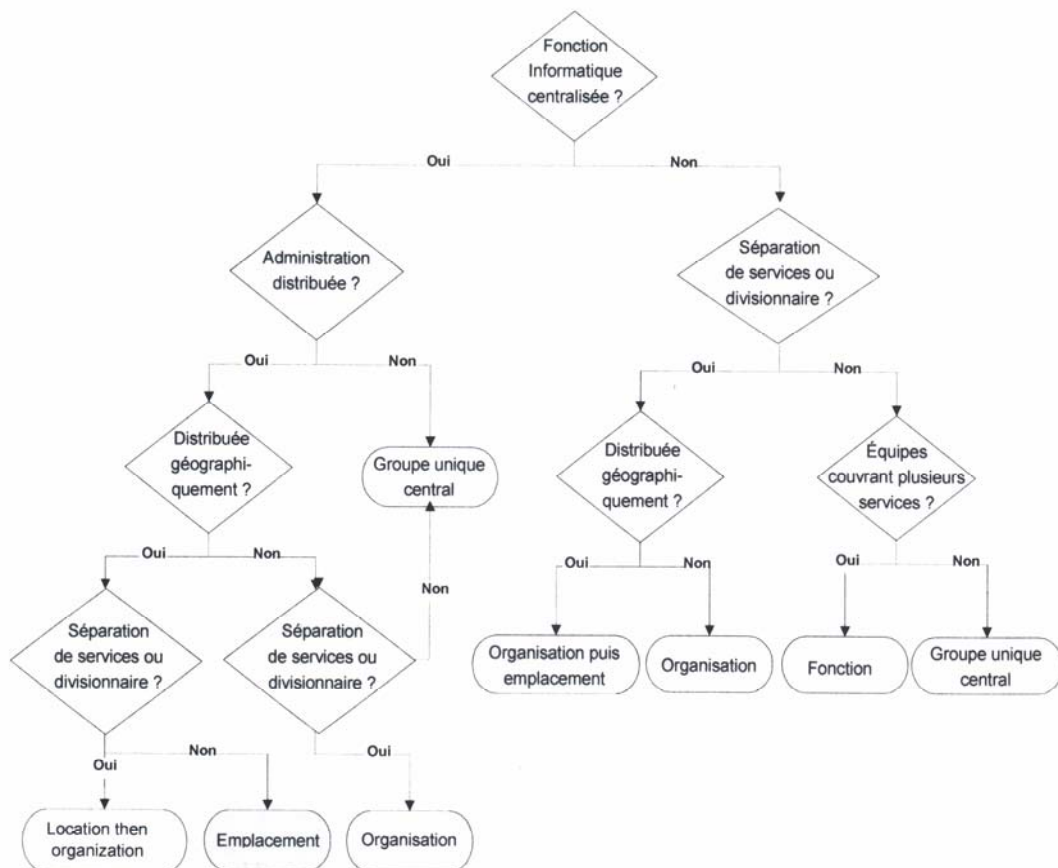
### **Instructions**

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

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

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

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



e) Consignes pour la délégation du contrôle administratif.

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

### **Instructions**

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

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

Lors de l'affectation d'autorisations, exécutez les tâches suivantes :

- Déléguez à des utilisateurs ou à des groupes d'utilisateurs le droit d'affecter des autorisations de contrôle d'accès à des objets. En d'autres termes, déléguez le droit de déléguer.
  - Affectez des autorisations courantes ou spéciales sur des objets.
  - Utilisez la fonction d'héritage pour permettre le transfert des autorisations de contrôle d'accès aux objets enfants. Parfois, cependant, vous devrez bloquer l'héritage pour éviter qu'un objet enfant n'hérite des autorisations définies sur l'objet parent. Le blocage de l'héritage rend difficile la documentation et le dépannage des autorisations sur un objet. Par conséquent, évitez d'y avoir recours.
- *Affectez des autorisations d'accès à des groupes, plutôt qu'à des individus.* Les autorisations de groupe simplifient l'actualisation des DACL sur les réseaux comportant de nombreux utilisateurs et objets. Par ailleurs, l'affectation d'autorisations à des groupes est une puissante fonctionnalité car elle vous permet d'imbriquer des groupes, ce qui réduit le nombre total d'objets à gérer.
  - *Minimisez le nombre d'administrateurs de domaine.* Le groupe Admins du domaine possède des droits spéciaux dans un domaine, comme celui de s'approprier tout objet et de définir des stratégies de sécurité pour tout le domaine. Lorsque vous souhaitez contrôler étroitement les privilèges de l'administrateur de domaine, accordez des droits d'administration aux utilisateurs pour les diverses unités d'organisation et limitez l'appartenance dans le groupe Admins du domaine.

**Rmq : Pour plus d'informations sur la délégation du contrôle, consulter le Guide de planification et de déploiement Windows Server 2003 à l'adresse**

**<http://www.microsoft.com/reskit>**