

Microsoft Windows 2000

Administration de Microsoft Windows 2000

Memento

Par :

TATEFO WAMBA Fidèle



23, rue Château Landon
75010 – PARIS
www.supinfo.com

Table des Matières :

Module 1 Présentation de la MMC	5
1 Fenêtres MMC	5
2 Consoles MMC	5
3 Fenêtre de console	5
a) Description des menus de la fenêtre de console	5
4 Types de consoles MMC	5
a) Consoles MMC Pré configurées	5
b) Consoles MMC personnalisées	6
5 Composants Logiciels enfichables	6
a) Composants logiciels enfichables autonomes	6
b) Composants logiciels enfichables d'extension	6
6 Option de console	6
a) Mode auteur	6
b) Mode utilisateur	7
Module 2 Principe des services d'annuaires	8
1 Présentation de Active directory	8
2 Description sommaire de la structure logique	8
3 Description sommaire de la structure physique	8
4 Les objets active directory	8
5 Identification d'objets dans l'Annuaire	8
Module 3 Groupes Locaux	10
1 Présentation	10
2 Groupes locaux créés	10
3 Groupes locaux intégrés	10
4 Groupes locaux prédéfinis	10
5 Groupes spéciaux prédéfinis	11
Module 4 Groupes de domaines	12
1 Rôle des groupes sous Windows 2000	12
a) Groupe sécurité	12
b) Groupe de distribution	12
c) Conversion d'un type de groupe en un autre	12
d) Etendue de groupe	12
Module 5 Partages et permissions	14
1 Les partages	14
2 Créations	14
3 Partages administratifs (partages cachés)	14
4 Autorisations sur les partages	14
5 Fichiers hors connexion	14
a) Configuration du client pour les fichiers hors connexion	15
b) Présentation du gestionnaire de synchronisation	15
6 Autorisations NTFS	15
a) L'héritage des autorisations NTFS	16
b) Les autorisations spéciales	16

7	L'appropriation	16
8	Un peu de technique sur le contrôle d'accès aux ressources de Windows 2000.	16
9	Combinaison des autorisations de partage et des autorisations NTFS	17
10	Copie et déplacement des fichiers et des dossiers	17
Module 6 Administration des comptes utilisateurs		18
1	Comptes utilisateurs	18
2	Profils de l'utilisateur	18
a)	Les profils d'utilisateurs locaux	18
b)	Les profils d'utilisateurs errants	18
c)	Les profils utilisateurs obligatoires	19
3	Le dossier Mes documents	19
4	Répertoire de base	19
5	Gestion des scripts	20
6	Les propriétés des comptes d'utilisateurs	21
7	Les Suffixes UPN	22
Module 7 Organisation des objets de l'annuaire		23
1	Les unités organisationnelles	23
a)	Conception et structuration de la hiérarchie d'unités d'organisation	23
2	Les clients Active directory	23
3	La délégation du contrôle d'administration	24
4	La publication des ressources dans Active directory	24
a)	Publication d'imprimantes	24
b)	Recherche d'imprimantes	24
c)	Publication d'un dossier partagé	24
d)	Recherche d'un dossier publié	25
Module 8 Présentation et administration de la stratégie de groupe		26
1	Présentation des stratégies de groupes	26
2	Outils de gestion et gestion d'un GPO	26
a)	Création d'un GPO	26
b)	Modification d'un GPO	26
c)	Suppression d'un GPO	26
d)	Gestion de la liaison d'un GPO	27
e)	Configuration des paramètres de GPO	27
f)	Surveillance des stratégies de groupe	27
g)	Outils de support des stratégies de groupe	27
3	Structure des stratégies de groupes	27
4	Application des stratégies de groupes	28
a)	Cas spécifique des clients Windows NT 4, Windows 95, Windows 98	29
b)	Héritage d'une stratégie de groupe	29
c)	Conflit entre deux stratégies de groupe	29
5	Administration des stratégies de groupes	29
a)	Contrôleur de domaine dédié à la gestion des stratégies de groupe	29
b)	Délégation du contrôle d'administration des stratégies de groupes	30
c)	Activation et désactivation d'un GPO	30
d)	Traitement de bouclage de rappel	30
6	Gestion des environnements à l'aide des stratégies de groupes	31
a)	Paramètres de modèle d'administration	31
b)	Paramètres de script	31

c)	Redirection des dossiers	31
d)	Paramètres de sécurité	31
7	Présentation du déploiement de logiciels	32
a)	Service et package Windows Installer	32
b)	Déploiement de logiciel	32
c)	Catégories de logiciels	32
d)	Association d'extensions de noms de fichiers	32
e)	Mise à jour et services pack	33
f)	Suppression de logiciels déployés	33
Module 9 Présentation et administration de l'audit		34
1	Présentation de la stratégie d'audit	34
2	Planification de la stratégie d'audit	34
3	Implémentation de l'audit	34
4	Utilisation de l'observateur d'événement	34
Module 10 Etude de cas		36
1	Scénario	36
2	Planification	36
3	Mode opératoire	37
a)	Création des différents dossiers : Les ressources	37

Module 1

Présentation de la MMC

La MMC (Microsoft Management Console) est l'un des principaux outils d'administrations permettant la gestion de Windows 2000. Elle permet de créer, sauvegarder et ouvrir les outils administratifs. C'est un programme qui héberge des applications de gestion appelées composants logiciels enfichables auxquelles il fournit un environnement commun. Se sont les composants logiciels enfichables qui prennent en charge la gestion proprement dite du système.

Elle permet d'effectuer les tâches suivantes :

- Effectuer les différentes tâches d'administration au moyen d'une seule console
- Centraliser l'administration
- Effectuer l'administration à distance à l'aide des composants logiciels qui le permettent
- Créer une console personnalisée

1 Fenêtres MMC


L'interface utilisateur MMC ressemble à l'explorateur Windows. Elle présente plusieurs Menus appelés Menus Standards ainsi qu'une barre d'outils appelée barre d'outils standard, une barre d'état (le bas de la fenêtre) et une barre de description. La barre d'outil standard fournit les commandes d'ouverture, de création et d'enregistrement de console MMC. La fenêtre parent contient des fenêtres enfants qui sont les consoles proprement dites.

2 Consoles MMC

Les consoles MMC possèdent plusieurs composants logiciels enfichables. Elles sont enregistrées sous la forme de fichiers possédant l'extension **.msc**. Tout les paramètres des différents composants logiciels enfichables sont enregistrés puis restaurés lors de l'ouverture du fichier de la console les hébergeant, quand bien même ce fichier est ouvert sur un ordinateur ou sur un réseau différent.

3 Fenêtre de console

Elle assure le rôle d'interface avec le fichier de console. Elle propose de nombreux affichages possibles. Elle comprend une barre de commande, une arborescence de console (volet gauche) et un volet de détails.

 Lorsqu'on ouvre une nouvelle console, une fenêtre de console apparaît dans l'espace de travail de la fenêtre MMC.

a) Description des menus de la fenêtre de console

Menu	Description
Action	Permet de créer, supprimer et de modifier les éléments gérés par le composant logiciel enfichable.
Affichage	Configure l'affichage du composant logiciel enfichable
Favoris	Permet d'organiser les composants logiciels enfichables ou les nœuds qui les intègre. Permet aussi de gérer les dossiers contenant des objets MMC.

4 Types de consoles MMC

2 types : pré configurée et personnalisée

a) Consoles MMC Pré configurées

Elles sont installées par défaut lors d'une installation de Windows 2000 ou lors de l'ajout de composants supplémentaires tels que le service DNS. Elles contiennent les composants logiciels enfichables utilisés pour les tâches d'administration les plus répandus. Fonctionnant en mode auteur, elles ne peuvent ni être modifiées, ni être

enregistrées, ni se voir être ajouter de nouveaux composants. Elles diffèrent en fonction de la version de Windows 2000 installée.

✎ L'exécution de la commande **Adminpak.msi** permet d'ajouter les consoles MMC pré configurées de Windows 2000 Server à une station Windows 2000 Professionnel pour l'administration à distance des fonctions des serveurs sur le réseau.

b) Consoles MMC personnalisées

Créées par un utilisateur qui en possède l'autorisation, elles permettent notamment d'utiliser un composant logiciel enfichable unique ou d'en combiner plusieurs partiellement ou en totalité. L'environnement MMC personnalisé permet aux administrateurs de :

- Combiner, unifier et centraliser les tâches administratives ;
- Enregistrer la console MMC pour un usage ultérieur ;
- Distribuer et partager la console avec d'autres utilisateurs ;
- Fournir une console MMC sur mesure lors de la délégation des tâches d'administration ;

Les fichiers de consoles personnalisées sont enregistrés dans le dossier outils d'administration de Windows 2000 avec l'extension .MSC. Le contenu de ce dossier est enregistré de façon séparée pour chaque utilisateur.

5 Composants Logiciels enfichables

Conçus pour fonctionner dans un environnement de MMC, chacun d'eux correspond à une seule unité de fonctionnalité de gestion. Il existe des composants logiciels enfichables autonomes et d'extension. Ils peuvent être ajoutés à une console MMC personnalisée.

a) Composants logiciels enfichables autonomes

Appelés généralement composants logiciels enfichables, ils sont utilisés pour effectuer les tâches administrative de Windows 2000. Windows 2000 intègre un jeu de composants standards tels sorte que ceux intégrés dans Windows 2000 PRO sont plus restreints que ceux de Windows 2000 Server.

b) Composants logiciels enfichables d'extension

Appelés généralement extensions, ils fournissent une fonctionnalité supplémentaire à un composant logiciel enfichable autonome donné. ils ne sont conçues pour ne fonctionner qu'avec les composants logiciels enfichables. Lors de l'ajout d'une extension, Windows 2000 n'affiche que les extensions compatibles au composant logiciel enfichable donné.

✎ Certains composants logiciels enfichables peuvent fonctionner en mode autonome ou en mode extension.

6 Option de console

Les options de console déterminent la manière de fonctionner d'une console MMC. Le mode de console détermine la fonctionnalité d'une console MMC enregistrée lors de son exploitation avec d'autres utilisateurs. On parlera d'option de console uniquement pour les consoles MMC personnalisées.

Les options MMC peuvent être configurées dans la boîte de dialogue **options** de la console MMC.

a) Mode auteur

Une console MMC enregistrée en mode auteur fournit l'**accès totale** à toutes les fonctionnalités de la MMC. Les utilisateurs ont le droit d'effectuer les tâches suivantes sur ce type de console MMC :

- Créer et ajouter des composants logiciels enfichables ;

- Créer de nouvelles fenêtres ;
- Afficher l'arborescence de la fenêtre en totalité ;
- Enregistrer les consoles MMC ;

b) Mode utilisateur

Ce mode permet de restreindre les actions que peuvent faire les utilisateurs sur les consoles MMC. Ainsi, les utilisateurs ne peuvent ni ajouter, ni supprimer des composants logiciels enfichables. Ils ne peuvent pas non plus enregistrer les consoles MMC. Ce mode est idéale pour la délégation du contrôle d'administration ou l'utilisation d'une console MMC avec d'autres administrateurs.

Il existe 3 types de modes administrateurs :

Type de mode utilisateur	Description
Accès total	Les utilisateurs peuvent naviguer au sein des différents composants logiciels enfichables, ouvrir de nouvelles fenêtres et accéder à la totalité de l'arborescence de console.
Accès limité, fenêtres multiples	Les utilisateurs peuvent afficher plusieurs fenêtres. Les utilisateurs ne peuvent pas ouvrir de nouvelles fenêtres. Les utilisateurs accèdent seulement à une partie de l'arborescence de la console.
Accès limité, fenêtres uniques	Les utilisateurs ne peuvent afficher qu'une partie de la fenêtre. Les utilisateurs ne peuvent ouvrir de nouvelles fenêtres. Les utilisateurs ne peuvent accéder à une partie de la l'arborescence de la console.

Module 2

Principe des services d'annuaires

1 Présentation de Active directory

Active directory est une base de donnée distribuée dite base d'annuaire dont le rôle est de fournir des services, et la gestion des objets de l'annuaire. AD stocke, organise, gère et contrôle des objets. Dans un réseau, AD fournis aux Administrateurs et aux utilisateurs les avantages suivants :

- L'administration centralisé ;
- La disponibilité et la tolérance aux pannes de l'annuaire grâce à la réplication à maitres multiples ;
- La simplification de la recherche et de la localisation des ressources grâce aux protocoles tels que LDAP ;
- La garantis de la sécurité et la confidentialité des informations et des données grâce à l'authentification et à l'infrastructure à clé publique ;
- L'interopérabilité avec d'autres systèmes et services d'annuaires grâce à l'intégration de protocoles standards et du système de nommage Internet ;

AD est composé d'une structure physique et d'une structure logique. La structure logique organise et stocke les objets et la structure physique sert à configurer et gérer le trafic réseau.

2 Description sommaire de la structure logique

Domaine : C'est une structure logique de AD qui a pour rôle de stocker des objets. Il regroupe des ordinateurs et partage la même base d'annuaire. C'est une unité de réplication (tout les Contrôleurs de domaine participent à la réplication), de ce fait il sert à réguler le trafic de réplication. C'est une limite de sécurité (stratégies de comptes, mots de passe), et une unité d'administration (droits, autorisation, délégation d'approbation).

Forêt : Ensemble d'arborescences de domaine partageant un espace de nom non contiguë.

Arbre : Arborescence de domaine regroupant plusieurs domaines Windows 2000 sous le même espace de nom.

Unité d'organisation : C'est un objet conteneur utilisé pour regrouper et organiser les objets du domaine.

3 Description sommaire de la structure physique

Site : C'est un ensemble de un ou plusieurs sous réseaux IP reliés entre eux par des connexions fiables et rapides. Il sert à l'optimisation du trafic de réplication de AD entre les contrôleurs de domaines à travers le réseau.

Contrôleur de domaine : c'est un serveur LDAP qui stocke la base d'annuaire AD et possède le service KDC (centre de distribution des clés) intervenant pour sécuriser l'authentification des ressources sur le réseau.

✍ Afin de garantir la disponibilité de AD, il est conseillé de disposer de plusieurs contrôleurs de domaines sur le réseau.

4 Les objets active directory

Dans Active directory, un objet peut être un compte d'utilisateur, une imprimante, un dossier partagé public, un groupe. Certains objets peuvent contenir d'autres objets, on parle alors d'objets conteneurs ou tout simplement conteneurs **Exemple : les unités d'organisation**.

Les objets sont en fait des instances d'une classe définis dans le schéma de Active directory. Une classe est un ensemble d'attributs représentatifs d'un type d'éléments ou de fonction.

5 Identification d'objets dans l'Annuaire

GUID (Globally Unique Identifier): C'est une valeur codée sur 128 bits unique dans l'entreprise, mais aussi dans le monde entier. Il est attribué par l'agent système de l'annuaire Active directory lorsqu'un nouvel objet est créé et il est stocké dans l'attribut **ObjectGuid** de cet objet. Il est utilisé en interne par Active directory pour identifier les objets. C'est l'une des propriétés qui est publiée dans le catalogue globale et qui est utilisée lors de la réplication. Il est non renommable et non supprimable.

SID : C'est une valeur codée sur 128 bits composée d'un **RID** (identificateur relatif) et d'un identificateur de domaine. Il est stocké dans la propriété **Object-SID** du compte ou du groupe nouvellement créé. Il est modifié lorsque par exemple l'utilisateur est déplacé dans un autre domaine (l'identificateur de domaine est modifié, le RID reste identique). Il fait partie du jeton d'accès créé lors de l'ouverture de session et identifie l'utilisateur et le groupe dans les ACL des ressources. Les SIDs ne sont fournis qu'aux comptes d'utilisateur et aux groupes. Il est non renommable et non supprimable

Plus de renseignements

Ce document étant dédié à l'administration de Windows 2000, pour plus d'informations sur la structure logique, la structure physique, les forêts, les arbres, les sites OU, et les rôles FSMO consulter l'essentiel de formation à **l'Implémentation et l'administration des services d'annuaires Microsoft Windows 2000** sur le site www.laboratoire-microsoft.org.

Module 3

Groupes Locaux

1 Présentation

Ils servent à contrôler l'accès à une ressource de l'ordinateur locale et à réaliser des tâches dites systèmes. Ils existent sur les contrôleurs de domaine, sur les ordinateurs membres d'un domaine ou sur des serveurs membres. On les retrouve donc sur toutes les machines qui tournent sous Windows 2000 pro et serveur.

L'appartenance à un groupe donne à l'utilisateur certains droits et la possibilité de réaliser certaines tâches sur l'ordinateur.

Tous les groupes locaux sont affichés dans le dossier **Groupes** du gestionnaire de l'ordinateur locale sauf sur un contrôleur de domaine (cette option est désactivée). Un groupe peut contenir des utilisateurs, des ordinateurs, des contacts.

✍ Sous 2000, il existe 2 types de groupes locaux : les groupes locaux créés et les groupes locaux intégrés (build in).

2 Groupes locaux créés

Ce sont ceux qui sont créés manuellement, par un administrateur par exemple.

3 Groupes locaux intégrés

Ils sont automatiquement créés lors de l'installation de Windows 2000. Vous ne pouvez pas les supprimer. Ils se composent des **groupes locaux prédéfinis** et des **groupes spéciaux prédéfinis** ou groupes à identités spéciales. Les groupes à identités spéciales (groupes spéciaux) permettent d'organiser automatiquement les utilisateurs pour l'utilisation du système.

✍ Les groupes spéciaux prédéfinis ne sont pas listés dans le dossier groupe du dossier utilisateurs et groupes des outils systèmes dans la MMC gestion de l'ordinateur en locale. Par contre, ils sont listés lorsque l'on essaye d'ajouter un nouvel utilisateur à un groupe.

✍ Il y a des groupes locaux prédéfinis qui sont ajoutés en fonction des services installés sur la machine.

Les modifications portant sur les utilisateurs et les groupes se font à l'aide du **gestionnaire de l'ordinateur locale** sauf sur un contrôleur de domaine (ou le gestionnaire de l'ordinateur locale est désactivée).

4 Groupes locaux prédéfinis

Groupe Local	Description
Administrateurs	Peuvent effectuer toutes les tâches administratives sur le système local. Le compte prédéfini administrateur est par défaut membre de ce groupe par défaut.
Opérateurs de sauvegarde	Peuvent sauvegarder et restaurer des données.
Invités	Accès temporaire et limité aux ressources
Utilisateurs avec pouvoirs	Peuvent créer et modifier des comptes locaux sur l'ordinateur, partager des ressources ou installer des pilotes de périphériques.
Duplicateurs	Gèrent la réplication sur un domaine
Utilisateurs	Les utilisateurs peuvent effectuer des tâches pour lesquelles des permissions leur ont été assignées. Tous nouveaux comptes créés sur une machine Windows 2000 sont ajoutés à ce groupe. Quand un ordinateur ou un serveur membre qui fait tourner un client réseau Microsoft rejoint le domaine, alors, Windows 2000 ajoute les utilisateurs du domaine au groupe local Utilisateur.

5 Groupes spéciaux prédéfinis

Groupe Local	Description
Tout le monde	Inclus tout les utilisateurs qui accèdent à l'ordinateur
Utilisateurs authentifiés	Inclus tout les utilisateurs avec un compte utilisateur sur l'ordinateur et sur le domaine utilisé pour éviter le accès anonymes à des ressources.
Créateur propriétaire	Inclus le compte utilisateur qui a crée ou pris possession d'une ressource
Réseau	Inclus tout utilisateur avec une connexion courante depuis un autre ordinateur du réseau vers une ressource partagée de l'ordinateur
Interactif	Inclus le compte utilisateur pour l'utilisateur qui est loggé sur l'ordinateur. Les membres de ce groupe ont un accès aux ressources de l'ordinateur local sur lequel ils se trouvent physiquement
Utilisateur anonyme	Tout utilisateur Windows qui n'est pas authentifié
Accès distant	Tout utilisateur qui a une connexion d'accès distante

Les stratégies de gestion des ressources dans un groupe de travail est **ALP** : **A**ccount **L**ocal Group **P**ermissions. Elle indique la procédure de création des comptes et des groupes dans un groupe de travail : L'on crée un compte, on l'ajoute dans un groupe local puis l'on positionne les permissions.

Module 4

Groupes de domaines

Sous 2000, il existe deux types de groupes dans un domaine : les groupes sécurité et distribution

1 Rôle des groupes sous Windows 2000

a) Groupe sécurité

Les groupes sécurités sont répertoriés dans les DACL (Discretionary Access Control List), les listes de contrôle d'accès discrétionnaire qui sont utilisées pour définir des autorisations sur les objets. S'ils permettent de gérer les autorisations d'accès à une ressource, ils permettent aussi de gérer les listes de distribution de messagerie puisqu'ils peuvent être utilisés en tant qu'entités de courrier électronique. De ce fait, lorsque vous envoyez un message électronique à un groupe d'utilisateurs, ce message est envoyé à tout les membres du groupe. On peut imaginer une application comme MS Exchange 2000 Server qui va utiliser les groupes de sécurité de Windows 2000 en tant que liste de distribution.

b) Groupe de distribution

La sécurité n'étant pas activé sur ces groupes, ils ne sont donc pas répertoriés dans les DACL, et ne servent pas à des fonctions liés à la sécurité. Ils sont utilisés uniquement avec des applications de courrier électronique (***par exemple Microsoft Exchange***) pour envoyer du courrier à un ensemble d'utilisateurs. Il est impossible de gérer les autorisations avec ce groupe.

c) Conversion d'un type de groupe en un autre

Il est possible de convertir un groupe de sécurité en un groupe de distribution et vice versa. Ceci n'est possible que si les domaines sont en mode natif.

d) Etendue de groupe

Chaque groupe a une étendue qui délimite son application dans l'arborescence du domaine ou dans la forêt. L'étendue d'un groupe est sa portée et son champ d'utilisation. Il existe trois étendues différentes : Universelle, globale et de domaine locale.

Etendue universelle	Etendue globale	Etendue locale
Uniquement dans les domaines en mode natif	C'est l'équivalent des groupes globaux sous Windows NT 4.0 ;	C'est l'équivalent des groupes locaux sous Windows NT 4.0
Les groupes universels en mode natif peuvent avoir comme membres des comptes, des groupes globaux et des groupes universels de n'importe quel domaine ;	Ils Organisent les comptes utilisateur par domaine ; Ils peuvent être ajoutés à d'autres groupes globaux à partir du domaine dans lequel ils sont créés ;	Ils permettent d'accorder des autorisations d'accès à des ressources du domaine sur lesquelles ils sont créés.
Les groupes peuvent être placés dans d'autres groupes (lorsque le domaine est en mode natif) et peuvent recevoir des autorisations dans n'importe quel domaine.	Ils peuvent être ajoutés à un groupe de domaine locale ou un groupe universel ;	Ils peuvent contenir des comptes utilisateurs, des groupes universels et des groupes globaux de n'importe quel domaine ;
Les groupes de sécurité avec une étendue universelle peuvent être créés dans les domaines en mode natif.	Peut être converti en étendue universelle à condition qu'il ne soit pas membre d'un groupe avec une étendue globale (en mode natif) ;	Les groupes peuvent être placés dans d'autres groupes de domaine local et peuvent recevoir des autorisations dans le même domaine ;

Ne peut être converti en aucune autre étendue de groupe	Ils sont créés sur le DC du domaine du compte et sont stockés dans l'annuaire d'Active Directory ;	Ils sont stockés dans l'annuaire d'Active Directory ;
Ils sont stockés dans l'annuaire d'Active Directory		Ils peuvent être converti en étendue universelle à condition qu'ils n'aient pas comme membre un groupe avec une étendue de domaine local.

La stratégie de gestion des ressources dans un domaine en mode mixte est **A G DL P** : **A**ccount **G**roup **G**lobal **D**omain **L**ocal **P**ermission indique :

- Création du compte ;
- Ajout de ce dernier dans un groupe global de domaine ;
- Ajout du groupe global dans un groupe de domaine local ;
- Positionnement des autorisations ;

On peut modifier les étendus de groupes. Cette modification n'est possible qu'en mode natif :

Groupe global vers universel : Si et seulement si le groupe n'est pas membre d'un groupe à étendu globale.

Domaine local vers universel : Attention, le groupe qui va être converti ne peut pas avoir comme membre un autre groupe ayant une étendue de domaine local.

La stratégie de gestion des ressources dans un domaine en mode natif est **A G U DL P** : **A**ccount **G**roup **G**lobal **U**niversal **D**omain **L**ocal **P**ermission indique :

- Création du compte ;
- Ajout de ce dernier dans le groupe global du domaine d'appartenance du compte ;
- Ajout du groupe global dans le groupe universel ;
- Ajout du groupe universel dans le groupe de domaine local de la ressource ;
- Positionnement des autorisations ;

Par défaut, un domaine Windows 2000 nouvellement créé est en **mode mixte**, ce qu'il signifie qu'il peut exister sur le domaine des contrôleurs secondaire de domaine fonctionnant sous Windows NT4 et il n'est pas question que dans un domaine en mode mixte, il puisse exister un contrôleur principale de domaine NT4.

Le passage au **mode natif** impose qu'il n'existe plus sur le domaine des contrôleurs secondaire de domaine NT4.

Module 5

Partages et permissions

1 Les partages

Un dossier peut être partagé avec d'autres utilisateurs sur le réseau. Les utilisateurs qui ouvrent une session sur un ordinateur sur le réseau peuvent accéder aux partages (dossiers partagés) se trouvant sur un autre ordinateur du réseau s'ils possèdent les autorisations adéquates.

A l'aide des partages réseau, un utilisateur va pouvoir depuis sa machine locale accéder aux ressources réseaux d'une autre machine.

2 Créations

Sous Windows 2000 Pro, uniquement par les administrateurs et les utilisateurs avec pouvoir.

Sous 2000 Serveur, seuls les administrateurs et les opérateurs de serveurs peuvent effectuer cette tâche.

Le composant logiciel enfichable **Dossiers partagés** permet d'afficher un récapitulatif des partages utilisés sur l'ordinateur locale et des ordinateurs distants. Il permet aussi de créer, afficher et définir les autorisations associés au partages de la machine locale et des machines distantes (y compris des stations Windows NT 4.0).

3 Partages administratifs (partages cachés)

Ces partages sont terminés avec le caractère \$, ce qui les cachent lors de l'exploration du réseau.

4 Autorisations sur les partages

- Contrôle Total
- Modifier
- Lire
- Aucun accès
- (Mnémotechnique : **CLAM**)

Les autorisations de partages s'appliquent lorsque l'utilisateur accède à un dossier depuis le réseau.


Par défaut, le groupe tout le monde possède l'autorisation Contrôle Total.

Lorsqu'un utilisateur est membre d'un groupe, l'autorisation effective est la moins restrictive (si l'on exclut la présence de l'autorisation **Aucun Accès**). Les autorisations sont cumulatives, aucune n'est donc prioritaire...A l'exception de **Aucun Accès** qui outre passe toutes les autres.

Les autorisations au niveau des partages peuvent être accordés à des utilisateurs de groupes approuvés. Les autorisations de partages ne s'appliquent qu'aux dossiers partagés.

5 Fichiers hors connexion

Ils permettent aux utilisateurs d'accéder aux fichiers enregistrés sur un partage réseau lorsqu'ils sont déconnectés de celui-ci. Cette opération est possible parce que les fichiers hors connexions sont mis en cache sur les disques durs locaux. Lorsque l'utilisateur se reconnecte au réseau, la copie en cache locale est synchronisée avec la version réseau. Le gestionnaire de synchronisation du menu **Accessoires** dans le menu **Démarré** permet de configurer et gérer les fichiers hors connexions.

 Tous les fichiers contenus dans un dossier partagé configuré pour prendre en charge les fichiers hors connexions sont susceptibles d'être configurés comme fichiers hors connexions.

Si deux versions d'un fichier marqué pour la prise en charge de fichiers hors connexion ont été modifiées différemment, Windows 2000 propose à l'utilisateur soit de choisir la version à conserver, soit de renommer l'une des 2 versions afin de conserver les deux.

Il existe 3 méthodes de mise en cache que l'on peut configurer sur Windows 2000 Server et Advanced Server :

Méthode	Description
Mise en cache manuelle des documents	C'est la configuration par défaut des dossiers partagés. Les utilisateurs doivent spécifier manuellement les documents qu'ils souhaitent mettre en cache. Seuls les fichiers marqués ainsi seront disponibles hors connexion.
Mise en cache automatique des documents	Tous les fichiers ouverts par l'utilisateur sont automatiquement mis en cache. Toutes les anciennes copies des fichiers sont automatiquement supprimées. Recommandée pour les dossiers contenant les documents créés par les utilisateurs.
Mise en cache automatique des programmes	Active la mise en cache unidirectionnelle des fichiers en lecture seule et des applications exécutées via le réseau. Le fichier d'origine n'est pas écrasé par une copie plus récente mise en cache sur l'ordinateur de l'utilisateur.

a) Configuration du client pour les fichiers hors connexion

La boîte de dialogue **Fichiers hors connexion** des **Options de dossiers** accessible depuis le menu **Outils** de l'explorateur de Windows permet de configurer les fichiers hors connexion sur les ordinateurs clients (Windows 2000 Professionnel).

Il est aussi possible de rendre une page Web disponible hors connexion à l'aide du menu **Favoris** en cliquant sur **Ajouter aux favoris** et en activant la case à cocher **Rendre disponible hors connexion**. Il est possible d'utiliser un objet stratégie de groupe pour empêcher l'utilisation des fichiers hors connexion.

b) Présentation du gestionnaire de synchronisation

Il permet de spécifier la manière avec laquelle les fichiers hors connexions seront synchronisés. Il permet notamment de :

Synchroniser à partir d'un seul point des fichiers et d'autres ressources réseaux déconnectés (dossiers, messages électroniques, bases de données...).

Choisir les périodes au cours desquelles les éléments déconnectés sont synchronisés (pour la synchronisation de fichiers volumineux ou l'économie de la bande passante).

6 Autorisations NTFS

Fixent le niveau d'accès que possèdent les utilisateurs aux ressources. Elles sécurisent les ressources locales et les accès via réseau. Ces autorisations peuvent être cumulées, sauf **Aucun Accès** qui outre passe toutes les autres. Les autorisations peuvent s'appliquer aux fichiers et aux dossiers.

Les autorisations sur les fichiers sont prioritaires sur celles appliquées aux dossiers.

L'autorisation **Refuser** est prioritaire sur les autres autorisations. Elle s'applique au cas par cas pour les utilisateurs.

Autorisation NTFS sur les dossiers : Lecture, Ecriture, Afficher le contenu du dossier, Lecture et Exécution, Contrôle total.

Autorisation NTFS sur les fichiers : Lecture, Ecriture, Lecture et Exécution, Modifier, Contrôle Totale.

☞ L'autorisation **Contrôle Totale** est accordée par défaut au groupe **Tout le monde** sur une partition NTFS. **Cacls.exe** est utilisé pour modifier les permissions des volumes NTFS en ligne de commande. L'autorisation **Refusé** n'est utilisée que pour interdire explicitement à un groupe ou à un compte l'accès à une ressource.

a) L'héritage des autorisations NTFS

Permet aux sous-dossiers et aux fichiers (objets d'un conteneur) d'hériter des autorisations accordées au dossier parent (le conteneur). Toutes les autorisations d'un dossier créé seront héritées par les dossiers et fichiers qu'il contiendra.

Il est possible de bloquer cet héritage pour éviter la propagation des permissions du dossier conteneur.

b) Les autorisations spéciales

Permettent de créer des autorisations NTFS sur mesure lorsque les autorisations NTFS standard ne suffisent pas.

☞ Les autorisations ne peuvent être définies que sur des lecteurs de type NTFS.
Pour modifier les autorisations NTFS, vous devez être le propriétaire de la ressource concernée ou avoir reçu de ce dernier l'autorisation correspondante.

7 L'appropriation

Peut s'effectuer sur un fichier ou un dossier. Pour prendre possession, il faut soit être : le **Créateur propriétaire**, l'**Administrateur**, avoir l'autorisation **Contrôle totale**, soit avoir l'autorisation d'accès spéciale Approbation pour un utilisateur normal ou un membre d'un groupe.

Seuls les membres du groupe **Administrateurs** ou le propriétaire d'une ressource peuvent accorder l'autorisation d'appropriation à la ressource concernée.

8 Un peu de technique sur le contrôle d'accès aux ressources de Windows 2000.

Comment est-ce que Windows 2000 prend-il la décision d'accorder l'accès à une ressource NTFS ?

L'accès à une ressource NTFS se fait de la même manière que sous Windows NT 4. Lorsque l'utilisateur ouvre une session sur un ordinateur Windows 2000, le gestionnaire des comptes de sécurité génère un jeton d'accès pour la session courante, qui contient, entre autre : l'identifiant d'utilisateur et les identifiants de groupes de cet utilisateur (que nous appellerons les SIDs ; System Identifier).

Une ressource NTFS (ex : une dossier) possède une liste d'autorisations que l'on appelle ACL (Access Control List), chaque entrée dans cette liste s'appelle une ACE (Access Control Entry).

Lorsqu'un utilisateur demande un accès à une ressource NTFS (*par exemple lecture sur un fichier*), un composant du système de sécurité Windows 2000 appelé le Moniteur de référence de sécurité (SRM : Security Reference Monitor) analyse l'ACL en recherchant tout les SID contenus dans le jeton d'accès de l'utilisateur. Cette recherche se fait jusqu'à ce que l'une des conditions suivantes soit remplie :

?? Le moniteur de référence de la sécurité rencontre une interdiction (représentation interne d'Aucun Accès) pour un SID du jeton d'accès de l'utilisateur. La recherche s'arrête à ce point et l'accès est refusé.

?? Le moniteur de référence de la sécurité rencontre une autorisation pour le SID du jeton. La recherche s'arrête et l'accès est autorisé. Si l'autorisation spécifie certaines et non toutes les autorisations demandées, la recherche continue jusqu'à ce qu'on ait accumulé toutes les autorisations, auquel cas, l'accès est accordé. Si l'autorisation ne spécifie aucune autorisation demandée, la recherche continue.

?? Lorsque le moniteur de référence de la sécurité atteint la fin de l'ACL sans avoir accumulé toutes les autorisations requises, l'accès est refusé. Aucun accès partiel ne peut être accordé

Il est important de noter que ce procédé ne fonctionne que si les interdictions sont placées en tête d'ACL. Si une autorisation précède une interdiction, un utilisateur peut obtenir l'accès même si Aucun Accès a été accordé à l'un des SID de son jeton d'accès. La recherche s'arrête dès que les autorisations requises ont été accumulées et avant qu'on ait rencontré Aucun Accès. Windows 2000 comme NT place toutes les interdictions avant les autorisations.

9 Combinaison des autorisations de partage et des autorisations NTFS

Lorsqu'un utilisateur possède aussi bien des autorisations NTFS que des permissions de partages (à l'exception de Aucun Accès), la permission effective est la permission la plus restrictive résultant de la combinaison des niveaux maximums de ses différents types de sécurité.

10 Copie et déplacement des fichiers et des dossiers

Toutes les opérations de copies entraînent l'héritage des autorisations du dossier cible. Seul le déplacement vers la même partition permet le maintien des autorisations.

Un dossier ou fichier copier au sein d'une partition NTFS ou vers une autre partition NTFS hérite des autorisations du dossier cible.

Un dossier ou fichier déplacé au sein d'une même partition NTFS conserve ses mêmes autorisations.

Les fichiers déplacés depuis une partition NTFS vers une partition FAT ne gardent pas leurs attributs et leurs descripteurs de sécurité, mais ils conservent leurs longs noms de fichier.

Copier à l'intérieur d'une partition	Crée un nouveau fichier identique au fichier original. Il hérite des autorisations du dossier de destination.
Déplacer à l'intérieur d'une partition	Ne crée pas de nouveau fichier. Met seulement à jour les pointeurs du dossier. Cela conserve les autorisations appliquées à l'origine au fichier.
Déplacer vers une autre partition	Crée un nouveau fichier identique à l'original et détruit le fichier original. Le nouveau fichier hérite des autorisations du répertoire de destination.

✍ Il peut être intéressant d'utiliser la gestion des quotas de disque pour limiter l'espace disque utilisé par les utilisateurs. Elle ne fonctionne que sur les partitions NTFS. Pour plus d'informations, consulter l'article correspondant sur le site : www.laboratoire-microsoft.org.

✍ Afin de garantir la sécurité et la confidentialité des données sur une partition NTFS, il est possible d'utiliser EFS, le système de cryptage de fichier, très facile à mettre en œuvre. Voir essentiel 70-210/70-215.

Module 6

Administration des comptes utilisateurs

1 Comptes utilisateurs

	Les comptes d'utilisateurs locaux	Les comptes d'utilisateurs du domaine
Lieu de Résidence	Dans la base SAM de la machine locale	Dans Active directory sur les DC (Domains Controllers)
Portée d'accès	Accèdent uniquement aux ressources de la machine locale	Accède aux ressources du domaine à condition d'avoir les privilèges nécessaires.
Les noms d'utilisateurs	Sont uniques dans Active Directory et sur l'ordinateur local Ne peuvent pas dépasser 20 caractères. Ne peuvent contenir les caractères suivants : « / \ : ; = , + * ? < > », ils ne sont pas sensibles à la casse.	
Les mots de passes	Sont sensibles à la casse	
Gestion des comptes	Gérés à travers : Gestion de l'ordinateur	Gérés à partir du composant Utilisateurs et ordinateurs Active Directory. (Gestion de l'ordinateur est désactivé sur un contrôleur de domaine.)
Option 'compte désactiver'	Désactive le compte sans le supprimer. Méthode conseillée : Utiliser cette méthode dans le cadre de départs non définitifs des utilisateurs ; Toujours créer des comptes utilisateurs étant désactivés.	
Connexion des utilisateurs	Depuis la machine locale qui possède le compte correspondant dans sa base SAM	Depuis n'importe qu'elle station appartenant au domaine si aucunes restrictions de connexion n'est imposée.

Il est conseillé d'utiliser un compte d'utilisateur type pour créer les utilisateurs en copiant le compte type; tout les éléments sont copiés sauf : Nom Utilisateur, Nom Complet, Compte Désactivé.

Chaque utilisateur possède un SID unique, la suppression d'un utilisateur est irrémédiable.

2 Profils de l'utilisateur

Profil d'utilisateur par défaut : Il est à la base des autres profils utilisateurs. Ils sont copiés à partir de ce dernier.

a) Les profils d'utilisateurs locaux

Ils sont créés la première fois qu'un utilisateur ouvre une session sur un ordinateur. Ils sont stockés dans l'ordinateur locale, ils se trouvent dans **%Systemroot%\Documents and settings** (*exemple : c:\Documents and settings\xxxx.*)

b) Les profils d'utilisateurs errants

Ce sont des profils utilisateurs centralisés, ils sont créés par l'administrateur et sont stockés sur un serveur sur le réseau. Ce type de profil est disponible quelque soit la machine à partir de laquelle l'utilisateur ouvre une session.

Lorsque l'utilisateur se connecte, le processus d'ouverture de session vérifie si la base des comptes contient un chemin de **profil errant** pour le compte. Si c'est le cas, Windows 2000 vérifie si l'utilisateur a changé le type de profil pour qu'il devienne local. Si le type de profil est défini comme étant locale, le système utilise la version du profil stocké localement plutôt que de télécharger une nouvelle version spécifiée dans la base de donnée des comptes. Si l'utilisateur n'a pas défini le type du profil comme étant locale, Windows 2000 compare la version locale de son profil avec la version errant spécifié dans la base des comptes.

Si la version du profil locale est plus récente, Windows 2000 demande à l'utilisateur quelle version de profil utiliser. Sinon, il télécharge le profil errant.

Au moment de la fermeture de session, si l'utilisateur est un invité ou si le profil est obligatoire, (suffixe .MAN au lieu de .DAT pour le fichier NTUSER.DAT), Win2000 n'enregistre pas le profil utilisateur courant.

Nous savons que Windows 2000 crée automatiquement le profil. Dans le cas du profil errant, cela implique qu'il existe un partage adéquat.

Exemple: \\SERVEUR\PROFILS\$.

c) Les profils utilisateurs obligatoires

Ils sont aussi créés par l'administrateur, ils peuvent être locaux ou itinérants. Ils ne permettent pas à l'utilisateur d'enregistrer leurs paramètres.

Pour rendre un profil obligatoire, il suffit de renommer le fichier Ntuser.dat en Ntuser.man (man = mandatory= obligatoire). Ainsi, les modifications ne seront pas prises en compte, le fichier devenant en quelque sorte en Lecture seule.

Le fichier NTUSER.DAT contient des informations de registre qui initialiseront le sous-arbre HTKEY_CURRENT_USER. Le fichier NTUSER.DAT.LOG quand à lui est un fichier d'enregistrement transactionnel. Ces deux fichiers se trouvent à la racine de chaque profil utilisateur. Lorsque l'utilisateur se déconnecte, NTUSER.DAT est mis à jour à partir de HTKEY_CURRENT_USER de la base de registre. En deux mots, NTUSER.DAT contient les informations de registres spécifiques à l'utilisateur (ex : les couleurs). Pour améliorer les performances d'ouverture de sessions, il est préférable de placer les dossiers de profil d'utilisateurs itinérants sur un serveur membre plutôt que sur un contrôleur de domaine.

3 Le dossier Mes documents

Il sert d'emplacement pour l'enregistrement des fichiers personnels. C'est l'emplacement par défaut sur lequel pointe les commandes d'application **Ouvrir** et **Enregistrer sous**. L'icône Mes documents facilite la localisation des documents personnels.

Il est possible de modifier le dossier de destination de Mes Documents à partir de l'icône Mes Documents. Il est préférable que les utilisateurs stockent leurs documents dans le dossier Mes documents plutôt que dans les dossiers de base. De ce fait, il serait judicieux de configurer la redirection de dossiers et les dossiers hors connexion pour stocker Mes documents sur un emplacement réseau.

4 Répertoire de base

Les informations de la section Répertoire de base servent chaque fois qu'un utilisateur ouvre ou enregistre un fichier dans une application, ou lorsqu'un utilisateur invoque une fenêtre d'invite de commande. Le répertoire de base par défaut est **USER\DEFAULT**.

Il s'agit simplement de l'espace de travail par défaut qui leur est affecté au départ.

Le bouton **Chemin local** permet de spécifier un chemin local pour le répertoire de base. Si ce chemin est un chemin réseau, il faudra cliquer sur le bouton **Connecter un lecteur réseau**, puis choisir la lettre du lecteur dans la liste déroutante et entrer le chemin réseau.

Il faut penser à partager le dossier pour que le gestionnaire **Utilisateurs et Ordinateurs Active Directory** crée automatiquement le répertoire de base. (L'administrateur doit avoir au moins la permission Modifier sur le partage).

Lors de la création automatique sur une partition NTFS, l'utilisateur reçoit Contrôle Totale comme autorisation par défaut sur ce dossier, et l'accès est interdit à tout les autres utilisateurs, y compris l'administrateur. (Pour modifier le contenu par la suite, il faudra en prendre possession.)

Il est possible d'améliorer la fonction de dossier de base en dirigeant le pointeur de l'utilisateur sur Mes Documents.

5 Gestion des scripts

Il est possible de spécifier un script d'ouverture ou de fermeture de session pour les utilisateurs et/ou un script de démarrage et d'arrêt pour les machines. Ces fichiers de Script peuvent posséder une extension de type **CMD** ou **BAT**. Ils s'exécutent automatiquement lorsque l'utilisateur ouvre ou ferme une session, ou lorsque la machine démarre ou s'arrête. Ils sont généralement utilisés pour établir des connexions réseaux.

Dans l'onglet **Profil** de la boîte de dialogue des propriétés du compte utilisateur, on peut indiquer un fichier de script d'ouverture de session. Dans ce cas, les Scripts se trouvent dans un sous-répertoire du chemin du script d'ouverture de session du contrôleur de domaine (**sysvol\nomdomaine\scripts**).

Exemples de commandes dans un script :

NET USE Z:\SERVEUR\PARTAGE /PERSISTENT : NO

Explication de l'argument **PERSISTENT** : cet argument gère l'emploi des connexions réseau permanentes.

?? **Yes** : Enregistre toutes les connexions à mesure qu'elles sont établies et les rétablit à l'ouverture de la session suivante.

?? **No** : N'enregistre pas les connexions établies ni les connexions ultérieures ; les connexions existantes sont rétablies à l'ouverture de sessions suivante.

Le paramètre **/delete** peut être utilisé pour supprimer les connexions existantes.

NET USE*\SERVEUR\PARTAGE

Alloue la prochaine lettre de lecteur

NET TIME\SERVEUR /SET /Y


Permet de synchroniser l'heure (le **/Y** évite la confirmation du changement par l'utilisateur)

Voici des paramètres pouvant être utilisés dans les scripts d'ouverture de session.

Paramètre	Description
%HOMEDRIVE%	Lettre de lecteur de la station de travail locale de l'utilisateur, connectée au répertoire de base de l'utilisateur
%HOMEPATH%	Chemin complet du répertoire de base de l'utilisateur
%OS%	Système d'exploitation de la station de travail de l'utilisateur
%PROCESSOR_ARCHITECTURE%	Type de processeur (<i>par exemple, 80386</i>) de la station de travail de l'utilisateur
%PROCESSOR_LEVEL%	Niveau de processeur de la station de travail de l'utilisateur
%USERDOMAIN%	Domaine contenant le compte de l'utilisateur
%USERNAME%	Nom de l'utilisateur

Les scripts peuvent aussi comprendre des fichiers VBScripts(.vbs) ou Jscripts créés dans un environnement d'exécution de scripts Windows 2000.

La gestion de l'attribution des scripts dans Active directory se fait aussi à l'aide des stratégies de groupe.

 Dans Active Directory, Windows 2000 enregistre les scripts dans le dossier Scripts du GPT. La valeur de délai d'expiration de traitement des scripts est de 2 minutes. Cette valeur peut être modifiée en utilisant une stratégie logicielle.

6 Les propriétés des comptes d'utilisateurs

Dans **Gestion de l'ordinateur** (pour un ordinateur locale) ou **Utilisateurs et ordinateurs Active directory, Utilisateurs et groupes, Nouvel utilisateur** :

La boîte de dialogue contient de nombreuses informations, mais toutes les options sont centrées autour des mots de passe.

- L'utilisateur doit changer de mot de passe à la prochaine ouverture de session
- L'utilisateur ne peut pas changer de mot de passe
- Le compte est désactivé
- Le mot de passe n'expire jamais
- Enregistrer le mot de passe en utilisant le cryptage réversible (Uniquement pour les comptes d'utilisateurs Active directory)

Toutes ses options s'expliquent d'elles mêmes à l'exception de « enregistrer le mot de passe en utilisant le système de cryptage réversible » qui sera utilisé lorsque des utilisateurs se connectent au réseau Windows 2000 à partir de systèmes Apple.

La boîte de dialogue **Propriétés** d'un compte utilisateur préalablement créé présente un certain nombre d'onglets qui permettent la configuration de différentes propriétés relatives à l'utilisateur associé au compte. Ce sont :

Onglet	Description
Onglet de propriétés personnelles	Se sont : Générale, Adresse, Téléphones et Organisation. Leurs attributs permettent de localiser les utilisateurs correspondants par le biais des services d'annuaire Active Directory.
Onglet Compte	Pour définir un nom d'utilisateur pour l'ouverture de session et les autres options du compte. Certaines de ses options sont paramétrables lors de la création d'un objet utilisateur dans Active Directory. Se sont ceux cités plus haut.
Onglet profil	Pour permettre aux utilisateurs de créer et de préserver automatiquement les paramètres de leur environnement de travail.
Onglet certificats publiés ou distribués	Permet de créer une liste de certificats X.509 pour le compte d'utilisateur sélectionné.
Onglet membre de	Permet d'indiquer le groupe d'appartenance du compte utilisateur sélectionné.
Onglet appel entrant	Permet de contrôler l'accès d'un utilisateur par le biais d'une connexion par numérotation à partir d'un emplacement distant.
Onglet Objet	Il fournit le nom de domaine de l'objet et des informations complémentaires tels que la classe de l'objet, les dates de créations et de modification et les numéros de séquences uniques d'origine (destinés au suivi des modifications apportés aux objets active directory) et actuels.
Onglet sécurité	Permet de définir les autorisations sur l'objet dans Active Directory.
Onglets relatifs aux services Terminal Server	Contiennent des informations relatives à l'utilisateur et au service Terminal Server.
Onglet environnement	On peut y indiquer une application qui sera automatiquement lancée lors de l'ouverture d'une session Terminal Server, mais aussi configurer Terminal Server pour qu'il puisse connecter des lecteurs et imprimantes locaux du client.
Onglet sessions	Permet de configurer les paramètres des sessions Terminal Server.
Onglet Contrôle distant	Permet de configurer les paramètres de contrôle distant des services Terminal Server.
Onglet Profil de services Terminal	Permet d'attribuer à l'utilisateur un profil appliqué aux sessions

Server	Terminal Server.
--------	------------------

7 Les Suffixes UPN

Se sont des alias de compte permettant de créer un suffixe de nom principal d'utilisateur. Ils ont pour but de simplifier l'administration et l'ouverture de session des utilisateurs. Pour ouvrir une session sur le domaine, un utilisateur doit utiliser son **nomdecompet@FQDN** (nom de domaine pleinement qualifié). Seulement, si FQDN est du genre : **sousdomainenfant.domainenfant.domaine.lan**, il est possible de créer un suffixe UPN tels que l'utilisateur puisse se connecter avec un nom de domaine semblable a : **nomdecompte@domaine.lan**. Les propriétés de **Domaine et approbation Active directory** permettent de créer un suffixe UPN aux comptes utilisateurs.

Module 7

Organisation des objets de l'annuaire

1 Les unités organisationnelles

Elles permettent d'organiser les objets active directory dans l'objectif de simplifier les tâches d'administration. Il est conseillé de d'abord créer des unités organisationnelles avant de créer les objets Active directory. Il est possible de créer une OU (organisationnal units) sous un domaine, sous l'objet contrôleur de domaine, dans une autre unité organisationnelle. La création d'une OU (mais aussi de tout objet active directory) dans une autre OU donne aux OUs la propriété de conteneur active directory.

Les unités d'organisations héritent des stratégies de sécurité qui sont définies à leur niveau ou au niveau du domaine parent sauf si elles ont été spécifiquement désactivées.

a) Conception et structuration de la hiérarchie d'unités d'organisation

Lors de la création d'unités d'organisations, il faut tenir compte des indications ci-dessous :

- Créer des unités d'organisation pour déléguer des tâches d'administration ;
- Créer une structure d'OU permettant aux administrateurs d'effectuer leurs tâches ;
- Créer des OUs pour appliquer des stratégies de sécurité (à travers les objets stratégie de groupe) ;
- Créer des OUs pour limiter l'accès des utilisateurs à certaines ressources ;
- Créer des structures d'OU relativement statiques (bien qu'elles assurent une certaine souplesse à l'espace) ;
- Eviter d'allouer trop d'objets enfants à une même OU ;
- Songer à la création d'une convention de nommage pour les OUs et les objets d'Active directory ;

En générale, les entreprises fondent leur structure de domaine sur les activités de leur entreprise, il est possible d'organiser les OUs selon les méthodes suivantes :

OU fondées sur l'administration des objets : dans ce cas, il est possible de créer des OUs basées sur les objets tels que les utilisateurs, les ordinateurs, les applications, les groupes, les imprimantes, les stratégies de sécurité. Il s'agit généralement de la meilleure méthode et facilite le travail des administrateurs.

OU géographiques : Pour l'organisation des objets en fonction de la structure géographique de l'entreprise (répartition des « surcursales », étages d'un immeuble). Cette méthode n'est pas préférable dans cas où la structure physique de l'entreprise sera profondément remaniée. Elle est intéressante pour les structures stables.

OU par rapport aux activités de l'entreprise : elles sont basées sur les fonctions existantes dans l'entreprise (marketing, services informatique, fonctions opérationnelles).

OU par rapport aux services de l'entreprise : elle représente l'organisation de l'entreprise.

OU par rapport aux projets : convient à certaines firmes tels que les entreprises informatiques ou les celles d'aéronautiques qui sont organisées autour de projets. Ce modèle n'est pas recommandé car il est considéré comme instable.

La création d'unité d'organisation se fait à l'aide du composant logiciel enfichable **utilisateurs et ordinateurs Active directory**.

2 Les clients Active directory

Ils permettent à un ordinateur de se connecter à un réseau Active directory. Ainsi, ce dernier peut ouvrir une session sur le réseau en recherchant un contrôleur de domaine ou rechercher des objets de Active directory.

Les ordinateurs avec le client Active directory sont :

- Des ordinateurs sous Windows 2000 Pro et Server.
- Des ordinateurs sous Windows 95 et 98 qui possède le **module complémentaire logiciel client Active directory**.

3 La délégation du contrôle d'administration

La délégation du contrôle d'administration permet de répartir les tâches d'administration entre les administrateurs d'un domaine. L'intérêt est de garantir qu'un administrateur ne possède pas plus de droits dans Active directory qu'il ne lui en faut en définissant précisément l'ensemble des tâches qu'il peut effectuer sur les objets de l'annuaire. La délégation des tâches permet d'accorder des droits sur les objets de l'annuaire et d'autoriser la modification de certaines de leurs propriétés.

La console **utilisateurs et ordinateurs Active directory** permet de déléguer le contrôle d'administration des objets. Il suffit de sélectionner l'unité d'organisation sur laquelle le contrôle d'administration sera délégué, de choisir l'option **Déléguer le contrôle** du menu contextuel pour lancer l'assistant **Délégation du contrôle d'administration**. Cet assistant permet de choisir le groupe ou l'utilisateur à qui la délégation de contrôle sera accordée, de déléguer des tâches courantes ou de créer des tâches personnalisées à déléguer. Par la suite, il permet d'indiquer les types d'objets définis pour la délégation. Enfin, il permet de définir des autorisations à déléguer.

Il est possible de créer des consoles d'administration dites personnalisées pour fournir aux administrateurs disposants de tâches déléguées des MMC qui correspondent à leurs tâches. Ainsi, si un utilisateur s'occupe des serveurs DNS, il aura une console qui lui permettra de gérer uniquement les serveurs DNS. On s'assure donc que ce dernier n'aura pas à rechercher dans les outils d'administration la console dont il se servira certainement le plus, mais on garantit qu'il ne pourra utiliser que cette console et non une autre. Un article et une vidéo express sont disponibles sur le site www.laboratoire-microsoft.org pour illustrer la délégation du contrôle d'administration.

Il est possible d'activer l'audit des événements liés à la délégation de contrôle d'administration. Cela permet dans un cadre précis d'évaluer les actions réalisées par des administrateurs débutants.

4 La publication des ressources dans Active directory

La publication va permettre aux utilisateurs de localiser un partage ou une imprimante sans se soucier de connaître la machine qui possède la ressource partagée. Les utilisateurs peuvent effectuer des recherches dans Active directory en utilisant les informations d'identification de la ressource qu'ils souhaitent atteindre si elle a été au préalable publiée.

Attention, la publication d'un objet dans l'annuaire va créer un objet active directory différent de la ressource physique. De ce fait, les autorisation d'accès ACL accordent ou refusent l'accès à la ressource physique et les permissions DACL influent sur l'accès à l'objet Active directory.

a) Publication d'imprimantes

Il est possible de publier une imprimante à partir de la console **Utilisateurs et ordinateurs Active Directory** ou directement à partir du serveur d'impression. Par défaut, tous les serveurs d'impressions Windows 2000 publient les imprimantes partagées dont ils disposent. Pour les autres types de serveurs Windows, la publication doit être manuelle. La MMC **utilisateurs et ordinateurs Active directory** permet aux administrateurs de localiser les imprimantes publiées à condition que l'option **Utilisateurs groupes et ordinateurs en tant que conteneurs** soit activée dans le menu affichage.

Un objet imprimante publiée peut être déplacée, ouverte, supprimée et renommée au même titre que n'importe quel objet Active Directory. Enfin, on peut agir sur les documents en cours d'impression d'une imprimante publiée ou modifier ses propriétés à partir du conteneur dans lequel elle se trouve.

b) Recherche d'imprimantes

Lors de la recherche d'imprimantes, Active Directory recherche d'abord cette dernière dans le sous-réseau qui fait référence à l'objet sous-réseau dans lequel se trouve la machine de l'utilisateur. Il ne faut pas oublier de compléter l'attribut **Emplacement** des propriétés de l'imprimante pour faciliter sa recherche.

La commande **Rechercher** dans le menu **Démarrer** permet de rechercher une imprimante publiée.

c) Publication d'un dossier partagé

La console **Utilisateurs et ordinateurs Active Directory** sert à la publication des dossiers partagés. Il suffit à l'aide du bouton droit à partir du conteneur du dossier partagé de cliquer sur **Nouveau** puis sur **Dossier partagé** pour renseigner les informations du partage à publier. C'est aussi à partir de cette console que l'on peut indiquer les mots clés qui faciliteront la recherche de la ressource dans Active directory (à partir des propriétés du partage).

d) Recherche d'un dossier publié

A partir du menu **recherche** ou du **domaine** dans le conteneur **Active Directory** des **favoris réseau**.

Module 8

Présentation et administration de la stratégie de groupe

1 Présentation des stratégies de groupes

Elles Permettent de configurer et de gérer la configuration du bureau pour les groupes d'ordinateurs et d'utilisateurs. La console **Stratégie de groupe** inclut les paramètres pour la stratégie de groupe de registre, de sécurité, d'installation logiciels, de scripts de démarrage et arrêt de l'ordinateur, d'ouverture et fermeture de session par l'utilisateur, et de la redirection de dossier. Les configurations de l'utilisateur sont enregistrées dans le registre dans HKEY_CURRENT_USER et celle de l'utilisateur dans HKEY_LOCAL_MACHINE. L'ordre de l'application des GPOs est la suivante : Site, domaine, OU, locale. Les GPOs sont des objets Active Directory qui possèdent des listes de contrôle d'accès discrétionnaires ou DACL.

Il existe 2 types de stratégies de groupes, la stratégie de groupe locale et la stratégie de groupe non locale.

Un GPO locale existe sur tous les ordinateurs Windows 2000 et est enregistré dans le dossier %systemroot%\System32\Grouppolicy et dispose d'une liste d'autorisation ACL.

Un GPO non locale est stocké sur les contrôleurs de domaines Windows 2000. Lorsqu'un GPO est crée, la structure du dossier GPT correspondant est crée et le nom de dossier attribué au GPT est le GUID du GPO correspondant. Un GPT (Group Policy Template) ou modèle de stratégie de groupe est un dossier contenant la disposition des paramètres applicables dans un GPO. Les GPCs sont des conteneurs Active directory qui contiennent les informations de version du GPO, les attributs des composants de la stratégie de groupe, et les extensions des composants logiciels enfichables. Les GPCs sont utilisés lors de la réplication de Active Directory pour déterminer l'objet le plus récent.

2 Outils de gestion et gestion d'un GPO

a) Création d'un GPO

GPO lié à :	Outil à utiliser pour la configurer
Un ordinateur local	Stratégie de sécurité locale obtenue en créant une MMC
Un ordinateur distant	Idem que ci-dessus en choisissant parcourir et l'ordinateur cible
Un site	La MMC Site et Service Active directory
Un domaine	La MMC Utilisateur et ordinateur Active directory
Une Unité d'organisation	
Une GPO non lié	Le composant Stratégie de groupe dans une nouvelle console.

b) Modification d'un GPO

Il est possible de modifier un GPO à l'aide d'une console en fonction du type de liaison implémentée par la stratégie de groupe. De manière générale, les consoles **Utilisateurs et ordinateurs Active Directory** et **Sites et services Active directory** seront utilisées pour modifier des stratégies de groupe. Les modifications apportées aux stratégies de groupes réécrivent les paramètres du registre. Les stratégies de groupes locales sont modifiées à l'aide de la MMC **Stratégie de sécurité** ou d'une MMC stratégie de groupe préalablement créée.

c) Suppression d'un GPO

La suppression d'un GPO va remettre les paramètres de registre concernés dans leur état initial, il est donc inutile de créer un GPO inverse pour revenir à l'état précédent. Les consoles utilisées pour la création et la manipulation des GPOs permettent la suppression de ses dernières.

d) Gestion de la liaison d'un GPO

Autant il est possible de lier plusieurs GPOs à un seul site, une OU, ou un domaine, autant il est possible de lier un GPO à plusieurs sites, plusieurs OUs, ou plusieurs domaines. Les console **Utilisateurs et Ordinateurs Active Directory** et **Sites et Services Active Directory** servent à lier ou à délier des GPOs.

☞ Bien qu'il soit possible de lier à un conteneur un GPO non lié auparavant, il est conseillé de créer l'objet stratégie de groupe directement sur le conteneur concerné.

e) Configuration des paramètres de GPO

Pour ce faire, il faut en générale afficher la stratégie de groupe qui contient la configuration que l'on veut effecteur, cliquer dans la **partie droite** de la fenêtre sur le paramètre à spécifier et choisir l'une des trois options présentes dans la boîte de dialogue. Ses options sont : **Non configurée** qui indique que aucunes modifications ne sera apportée au registre, **Activée** qui signifie que l'option choisis sera activée, et **Désactivé** qui signifie que l'option est explicitement refusée.

f) Surveillance des stratégies de groupe

Pour utiliser le journal d'application afin observer les évènements détaillés liés aux stratégies de groupe, il faut en tant qu'administrateur locale dans la clé : **HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Winlogon** ajouter **RunDiagnosticLogginGlobal** de type **DWORD** en lui affectant la valeur **1**.

Toutes les modifications et configurations affectés à l'ordinateur local et aux utilisateurs dotés d'une stratégie de groupe peuvent être consignés dans un journal (**%systemroot%\ Debug\UserMode\UserEnv.Log**). Pour ce faire, il faut effectuer la modification suivante dans le registre : Clé : **HKLM\Software\Microsoft\WindowsNT\CurrentVersion: UserEnvDebugLevel** de type **DWORD** qui va recevoir la valeur **3002** (activation de l'inscription commentée).

☞ La valeur **3000** n'enregistre aucuns suivit, la valeur **3001** active uniquement l'enregistrement des erreurs et avertissements d'applications des GPOs.

g) Outils de support des stratégies de groupe

Nom de l'outil	Localisation	Rôle
NetDiag.exe	Outils de support Windows 2000 dans le CD-Rom (\Support\tools)	Teste et liste les problèmes de connectivité du réseau client
Replmon.exe	Outils de support Windows 2000 dans le CD-Rom (\Support\tools)	Permet d'identifier les problèmes de réplication des stratégies de groupe. Son véritable rôle est de surveiller la réplication entre contrôleurs de domaine de façon graphique.
GpoTool.exe	Kit de ressource Technique Windows 2000	Vérifie l'état des GPOs sur les contrôleurs de domaine.
Gpresult.exe	Kit de ressource Technique Windows 2000	Affiche les informations sur l'impact des stratégies de groupe sur le compte d'un utilisateur qui se connecte à un ordinateur local.

3 Structure des stratégies de groupes

La fenêtre stratégie de groupe possède dans sa partie gauche deux nœuds : **Configuration utilisateur** et **Configuration ordinateur**.

Configuration Ordinateur sert à paramétrer l'ordinateur tandis que configuration utilisateur sert à paramétrer l'environnement utilisateur. Voici une description rapide des composants de la stratégie de groupe :

Modèles d'administration	Paramètrent la configuration d'ordinateur et utilisateur concernant les applications et les environnements de bureau. On peut ainsi g�rer de fa�on centraliser des �l�ments tels que les fichiers hors connexion, les quotas de disques, la restriction des commandes du menu d�marrer, l'affichage de certains �l�ments du bureau.
S�curit�	Permet de g�rer la s�curit� du r�seau. Il est ainsi possible de configurer les strat�gies de comptes, les strat�gies Kerberos, la s�curit� IPSec, les droits des utilisateurs, l'audit, les strat�gies de cl�s publiques, les journaux d'�v�nements, les cl�s de registres locales, l'administration de l'appartenance aux groupe locaux.
Installation de logiciels	Sert � administrer le d�ploiement de logiciel pour les ordinateurs et les utilisateurs. Windows Installer est le service c�t� client qui permettra de centraliser et d'automatiser l'installation, la modification et la suppression des logiciels.
Scripts	Permet d'ajouter des scripts au d�marrage et/ou arr�t des machines ou � l'ouverture et/ou la fermeture des sessions utilisateurs
Services d'installation � distance	Permet de configurer les options de l'installation des syst�mes Windows 2000 Professionnels via le service RIS
Maintenance d'Internet explorer	Permet de configurer les options d'Internet explorer.
Redirection de dossiers	Permet de rediriger des dossiers sp�cifiques vers un emplacement r�seau.

4 Application des strat gies de groupes

Les strat gies de groupe modifiant la configuration des ordinateurs s'appliquent et se r initialisent au d marrage de ses derniers. Les strat gies de groupes concernant la configuration des utilisateurs s'appliquent et se r initialisent lors de l'ouverture de session des utilisateurs sur le domaine. Les strat gies ordinateurs et utilisateurs sont actualis es par l'**intervalle de rafra chissement** des GPOs. Dans le cas d'un conflit entre les  l ments de strat gies qui s'appliquent autant   la configuration ordinateur et   la configuration utilisateur, la strat gie ordinateur s'appliquant en dernier  crase les param tres de la strat gie utilisateur.

Par d faut, le traitement des strat gies de groupes est **synchrone**, le syst me les traite les unes apr s les autres. Bien que d conseill , il est possible de rendre ce traitement **asynchrone** et d' viter que le syst me attende la fin du traitement d'un GPO avant de lancer le traitement du suivant.

Les clients disposent d'une biblioth que de liaison dynamique correspondant   une strat gie d'ordinateur, ce sont les **extensions clients**. Elles sont charg es de traiter des parties sp cifiques des GPOs. Quand le client obtient la liste des strat gies, chaque extension c t  client consulte la liste, extrait et applique les param tres de strat gie qui la concerne.

Les GPOs sont dupliqu es toute les **5 min** entre les contr leurs de domaine. Elles sont rafra chies toute les **90 min** avec un temps al atoire de **30 min** sur les postes clients Windows 2000 Professionnels. Il est possible de modifier ses param tres.

Bien que les strat gies de groupes ne soient pas mises   jour par d faut sur les clients si aucune modification n'a  t  effectu e, il est possible d'imposer une intervalle d'actualisation m me si les GPOs n'ont pas chang s. Cela peut servir afin de garantir qu'aucun utilisateur ne modifie certains param tres de l'ordinateur.

Il est possible de forcer l'actualisation des strat gies de groupe. La commande **SECEDIT /REFRESHPOLICY** permet de r actualiser les param tres de strat gies de groupes.

Dans le cas de la d tection des liaisons lentes, il est possible de d finir le comportement des GPOs. IL peut par exemple  tre int ressant pour des raisons de performance d'autoriser le traitement d'un GPO   travers une liaison lente sauf pour l'installation de logiciel car, Windows Installer transporte un volume important de donn es. Par ailleurs, il est possible d'indiquer quelle est la valeur en dessous de laquelle une connexion est consid r e comme liaison lente, elle est de **500 Kilobits** par d faut.

a) Cas spécifique des clients Windows NT 4, Windows 95, Windows 98

Les objets stratégies de groupe créées dans un domaine Windows 2000 ne s'appliquent pas aux ordinateurs clients Windows NT4, Windows 98 et Windows 95. Pour gérer l'environnement utilisateur pour ses ordinateurs, il faut utiliser l'utilitaire **POLEDIT.EXE**. Les fichiers stratégies utilisateurs et ordinateurs doivent être sauvegardés sous le nom unique et obligatoire **NTCONFIG.POL** pour les clients NT4 et **CONFIG.POL** pour les clients Windows 95 et 98 dans le partage NetLogon du contrôleur de domaine.

☞ Sous Windows 2000, le partage NetLogon correspond au dossier **%Systemroot%\Sysvol\sysvol\nom_de_domaine\Scripts**. L'outil **Reg View** du Kit de ressources technique Windows 2000 permet de visualiser les fichiers de configuration .pol sans les appliquer au registre.

b) Héritage d'une stratégie de groupe

Les stratégies de groupes sont appliquées et héritées dans l'ordre suivant : Site, Domaine, puis unité d'organisation

Les utilisateurs et les ordinateurs héritent des GPOs situés sur des conteneurs parents (par défaut).

Lorsque plusieurs GPOs s'appliquent, il y a cumul des paramètres. Ainsi, les objets utilisateurs et ordinateurs situés dans des conteneurs héritent de tous les GPOs qui sont liés à ses conteneurs (même si elles s'appliquent sur chaque conteneur parent séparément).

Il est possible de filtrer, forcer ou bloquer l'héritage des stratégies de groupes.

L'option **forcer** oblige tout les conteneurs enfants à hériter d'un objet stratégie de groupe lié au conteneur parent, même si l'option bloquer est explicitement indiquée.

L'option **filtrer** permet d'indiquer quels sont les comptes ou groupes qui ne seront pas affectés par un GPO. Cela se configure au niveau des paramètres de sécurité de l'objet stratégie de groupe en utilisant les DACLs du GPO.

c) Conflit entre deux stratégies de groupe

En cas de conflit entre des GPOs appliqués sur différents conteneurs parents, le GPO effectif est celle qui est le plus proche du client. Si les GPOs en conflits sont définis sur un même conteneur, Windows 2000 applique la stratégie qui est situé le plus haut dans la liste des GPOs. En effet, pour Active directory, plus un GPO est situé en haut de la liste plus il est prioritaire.

☞ Sous Windows 2000, le partage NetLogon correspond au dossier **%Systemroot%\Sysvol\sysvol\nom_de_domaine\Scripts**. L'outil **Reg View** du Kit de ressources technique Windows 2000 permet de visualiser les fichiers de configuration .pol sans les appliquer au registre.

☞ Les paramètres ordinateurs prennent toujours le dessus sur les paramètres utilisateurs en cas de conflit.

5 Administration des stratégies de groupes

a) Contrôleur de domaine dédié à la gestion des stratégies de groupe

Par défaut, c'est sur le contrôleur de domaine qui possède le rôle d'**émulateur PDC** que sont créées les stratégies de groupe. Il est possible de désigner un autre contrôleur de domaine pour gérer les stratégies de groupe. Pour cela, il faut créer une console avec le composant logiciel enfichable **Stratégie de groupe**, sélectionner le GPO concerné et utiliser la commande Options du contrôleur de domaine dans le **menu affichage**. A partir de la boîte de dialogue qui s'affiche, il est possible de choisir le contrôleur de domaine sur lequel l'administrateur est connecté ou un autre contrôleur de domaine du domaine concerné (fortement déconseillé).

b) Délégation du contrôle d'administration des stratégies de groupes

Permet de donner à un utilisateur la possibilité de créer des GPOs, de les modifier et de modifier leurs liaisons. L'objectif est d'accorder l'accès en lecture et écriture aux attributs **gPlink** et **gPoptions** de la stratégie à déléguer. Les autorisations par défaut sont les suivantes :

Compte ou groupes	Lire	Ecrire	Créer	Appliquer	Supprimer
Administrateurs de l'entreprise	Oui	Oui	Oui	Non	Oui
Administrateurs du domaine	Oui	Oui	Oui	Non	Oui
Créateurs propriétaires	Oui	Oui	Oui	Non	Oui
Groupe Système	Oui	Oui	Oui	Non	Oui
Utilisateurs authentifiés	Oui	Non	Non	Oui	Non

Deux choix sont disponibles pour autoriser la gestion des stratégies de groupes à un utilisateur : déléguer une tâche d'administration ou positionner les autorisations DACL sur les objets concernés.

Au cours de la délégation des tâches d'administration, il faut choisir l'option **Créer les liens des stratégies de groupes**. Après quoi, il faut soit ajouter l'utilisateur possédant la tâche déléguée au **groupe propriétaires créateurs de la stratégie de groupe**, soit modifier directement les droits de l'utilisateur directement sur l'objet GPO.

La modification des DACLs des attributs des liens **gPlink** et **gPoptions** se fait à partir de l'onglet **Sécurité** du conteneur. Pour cela, utiliser le bouton **Avancé** pour accéder à la boîte de dialogue **Paramètres de contrôle** de l'objet concerné à partir de laquelle, la modification des attributs des liens est possible.

Il est possible de créer une console **MMC personnalisée** dédiée à l'administrateur concerné par la délégation des tâches. Ainsi, ce dernier peut gérer les objets du conteneur concerné. Il faut songer à configurer les paramètres pour la gestion de la MMC dans une GPO. Il est ainsi possible de contrôler les composants logiciels enfichables utilisés par l'administrateur auquel la gestion d'un GPO a été attribuée.

c) Activation et désactivation d'un GPO

Il est possible de désactiver un GPO pour que ce dernier ne s'applique pas à un conteneur. Il est aussi possible de désactiver les paramètres ordinateur ou utilisateur pour un objet GPO. Cela est intéressant dans la mesure où il est possible de décider si les paramètres de configuration de l'ordinateur ou de l'utilisateur inscrits dans la stratégie doit s'appliquer.

d) Traitement de bouclage de rappel

Par défaut, si un utilisateur se connecte sur un ordinateur appartenant à une OU sur laquelle est définie un GPO (l'utilisateur n'appartenant pas à cette OU), la configuration ordinateur de cette stratégie s'applique cumulée à la configuration utilisateur du GPO définie sur l'OU à laquelle appartient l'utilisateur. Il est possible de ne pas prendre en compte la stratégie de l'utilisateur en activant le **Traitement par boucle de rappel**. Deux modes sont disponibles :

Le mode **fusion** (par défaut) : qui va appliquer la configuration de l'utilisateur et celle du poste sur lequel l'utilisateur se connecte

Le mode **remplacement** : qui va permettre de ne prendre en compte que les paramètres de configuration ordinateur du poste sur lequel l'utilisateur se connecte et empêcher l'exécution de la stratégie de l'utilisateur.

6 Gestion des environnements à l'aide des stratégies de groupes

a) Paramètres de modèle d'administration

Il sont configurés à partir du dossier modèle d'administration à partir des nœuds **Configuration utilisateur** et **Configuration ordinateur**. Ils sont enregistrés dans les fichiers **Registry.pol** contenus dans le GPT du GPO correspondant. Les fichiers **Registry.pol** sont au nombre de 2 : un pour les paramètres utilisateur et un pour les paramètres ordinateur. Ses fichiers sont situés dans les dossiers suivants : Sysvol\Sysvol\Nom_de_domaine\Policies\GUID_GPO : \machine\Registry.Pol et User\Registry.Pol. Ils vont directement influencer sur les paramètres HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER du registre. Ses fichiers sont recherchés par le système lorsqu'un ordinateur démarre ou lorsqu'un utilisateur ouvre une session. Le système inscrit ensuite les paramètres du registre et les paramètres personnalisés des fichiers **Registry.Pol**.

Les paramètres du modèle d'administration permettent de définir l'environnement de l'utilisateur. On pourra donc les utiliser pour personnaliser le bureau des utilisateurs, par exemple, ajouter un suffixe DNS principal, interdire la suppression des imprimantes, interdire l'affichage du voisinage réseau, supprimer des éléments du menu démarrer, interdire à Windows d'exécuter des programmes précis. Les types de paramètres disponibles sont : **Composants Windows**, **Système**, **Réseau**, **Imprimantes**, **Menu Démarrer** et **barres des tâches**, **Bureau**, **Panneau de configuration**.

b) Paramètres de script

Vont permettre d'affecter les scripts aux ordinateurs et aux utilisateurs pour personnaliser le démarrage/arrêt ou l'ouverture/fermeture de session. Les paramètres de **Configuration ordinateur** définissent les scripts de démarrage et d'arrêt des ordinateurs sur le domaine. Les paramètres de configuration utilisateur définissent les scripts d'ouverture et de fermeture de session. Par défaut, Windows 2000 recherche les scripts dans le dossier : %Systemroot%\System32\Rep\Import\Scripts.

Les scripts d'ouverture et de fermeture de sessions sont exécutés de haut en bas conformément à leur position dans la boîte de dialogue propriétés (dans le cas où l'attribution de ce script s'est faite via un GPO (Group policy object)). Lorsqu'un ordinateur Windows 2000 s'arrête, les scripts de fermeture de sessions sont exécutés en premier, puis les scripts d'arrêt sont exécutés.

L'exécution des scripts d'ouverture de session est masquée et asynchrone tandis que celle des scripts de démarrage et d'arrêt est masquée et synchrone. Il est bien entendu possible de modifier ses paramètres.

c) Redirection des dossiers

Il est possible de rediriger certains dossiers appartenant au profil des utilisateurs afin de les centraliser sur un serveur. Ceci facilite les tâches de gestion de la sécurité et de sauvegarde des fichiers personnels de chaque utilisateur. Les dossiers pouvant être redirigés sont les suivants : **Mes Documents**, **Menu Démarrer**, **Bureau**, **Application Data**. Lorsqu'on choisit de rediriger ses dossiers, il est possible de les paramétrer. On peut donc s'assurer que seul l'utilisateur aura le droit d'accéder à ses documents personnels ou conserver la redirection des dossiers sélectionnés même si la stratégie de groupe est supprimée. Pour cela, il faut consulter les propriétés du document redirigé.

d) Paramètres de sécurité

Permet de paramétrer et d'uniformiser la sécurité. Les paramètres de sécurité sont inscrits dans le registre et sont conservés même si la stratégie de groupe est supprimée. Le paramétrage de la sécurité permet de configurer la sécurité des comptes et des mots de passe (uniquement au niveau du domaine), l'audit des objets et de Active directory, les droits des utilisateurs, l'appartenance aux groupes restreints, le type de démarrage des services systèmes, l'accès, la sécurité et l'audit du registre, la sécurité du trafic IP et la gestion des modèles de sécurité.

7 Présentation du déploiement de logiciels

a) Service et package Windows Installer

Le déploiement de logiciel est basé sur la technologie **IntelliMirror** et utilise le service **Windows Installer** disponible sur Windows 2000 et installable sur Windows 95, 98 et NT. Il permet de centraliser et de faciliter le déploiement et la maintenance des logiciels sur plusieurs postes sur le réseau. Pour déployer un logiciel, il faut posséder toutes les informations d'installation de ce logiciel dans un fichier appelé **package Windows Installer**, **Lots Windows Installer** ou simplement **lots Installer**. Certains sont fournis avec les fichiers d'installation des applications (*office 2000 par exemple*). On distingue les packages Windows Installer suivant :

.MSI : Accompagne les fichiers d'installation d'application. Il est utilisé pour déployer les applications sur le réseau et est fournis par les éditeurs de ses applications.

.MST : Associé au package MSI préalablement déployé, il permet de déployer une application avec des modifications. Il est possible d'indiquer l'ordre de priorité de l'application des transformations.

.MSP : Permet d'appliquer des correctifs ou des mise à jour aux applications déployées.

.AAS : Fichiers de script d'attribution de logiciel.

.ZAP : Fichier texte dans lequel sont indiqués les informations pour l'installation de logiciel avec setup.exe ou install.exe

b) Déploiement de logiciel

Les packages Windows Installer doivent être placés dans un **point de distribution** (dossier partagé) sur le réseau. Dans une stratégie de groupe, utiliser le dossier **paramètre logiciel** de l'un des nœuds **configuration utilisateur** ou **configuration ordinateur** pour indiquer le package à déployer. Il est question par la suite d'indiquer la méthode de déploiement entre **Attribution**, **Publication**, ou **Publication ou Attribution avancée**.

Attribution : Pour la configuration utilisateur et ordinateur. Lorsque l'application est attribuée à des utilisateurs, elle est inscrite dans le registre local et une icône est ajoutée dans le menu démarré. Lorsque l'utilisateur clique sur cette icône ou lorsqu'il ouvre un fichier possédant une extension associée à l'application déployée, celle-ci s'installe. Lorsque l'application est attribuée à des ordinateurs, elle est automatiquement installée au démarrage de celles-ci. Aucune participation de la part des utilisateurs n'est de ce fait nécessaire pour ce type de déploiement.

Publication : Uniquement pour la configuration utilisateur. Les utilisateurs doivent utiliser le programme **Ajout/suppression de programmes** pour pouvoir installer l'application. Cette méthode est conseillée lorsque les utilisateurs ont une certaine pratique de Windows 2000 et qu'ils ont la possibilité de choisir les applications qui les intéressent. Par ailleurs, il faut veiller à ce que des paramètres des stratégies de groupe n'empêchent pas l'accès au programme ajout/suppression de programme ou au panneau de configuration.


Publication ou attribution avancée : Permet de personnaliser l'installation des applications : configurer des options ou modifier des packages.

c) Catégories de logiciels

Permet de classer les applications publiées par catégories. L'un des intérêts de cette méthode est qu'elle va faciliter la recherche de l'application dans une longue liste.

d) Association d'extensions de noms de fichiers

Il est possible d'organiser le classement des extensions en modifiant la priorité des applications pour chaque extension. Les boutons **Monter** et **Descendre** des propriétés de **Installation logiciel** permettent d'indiquer l'application à prendre en compte en premier (début de la liste).

 Il n'est possible d'associer une extension que si le package correspondant a été déployé.

e) Mise à jour et services pack

Pour mettre à jour une application, il est possible d'utiliser un nouveau package MSI fournis par l'éditeur du logiciel ou un correctif Windows Installer **.MSP** . Il faut ensuite placer le package Windows Installer dans le même dossier de distribution que les lots Installer à mettre à jour. Dans la stratégie de groupe de l'application à mettre à niveau, il faut ajouter le fichier de mise à niveau comme nouveau package, et dans les propriétés de ce nouveau package, indiquer le package à mettre à niveau. Il faudra alors choisir le type de mise à jour : **obligatoire** (désinstalle le package existant et installe le nouveau) ou **facultative** (met à jour le package existant). Il est possible de forcer la mise à niveau lorsque l'utilisateur utilise l'application. Pour cela, utiliser l'option **Mise à jour nécessaire pour les packages existants**.

Windows 2000 propose l'outil **Veritas WinINSTALL LE** qui permet de modifier et de repackager des packages Windows Installer. Il se trouve dans le dossier \valueadd\3rdparty\mgmt\winstle du CD Rom Windows 2000 Server.

f) Suppression de logiciels déployés

Il existe deux méthodes pour désinstaller des applications déployées.

Suppression forcée : Le logiciel est désinstallé au prochain redémarrage de la machine (publication aux machines) ou désinstallé à la prochaine ouverture de session (attribution ou publication aux utilisateurs).

Suppression optionnelle : L'application n'est pas automatiquement désinstallée sur les ordinateurs. Les utilisateurs peuvent continuer à l'utiliser et devront la désinstaller manuellement.

Module 9

Présentation et administration de l'audit

1 Présentation de la stratégie d'audit

L'audit permet de conserver les traces d'une activité système (ouverture de session réussie ou avortée, création, ouverture ou suppression de fichiers ou d'autres objets). La **stratégie d'audit** est utilisée pour assurer les fonctions d'audit sous Windows 2000 et stocke les informations d'audits sous forme d'entrées dans le journal de sécurité de l'**Observateur d'événements**. Une entrée d'audit indique la nature de l'action exécutée, le nom de l'utilisateur l'ayant effectuée et la réussite ou l'échec de l'événement audité.

Les événements sont en générale consignés sur les ordinateurs où ils ont lieu. Par contre certains événements comme l'ouverture de session sur le domaine sont consignés sur les contrôleurs de domaine.

2 Planification de la stratégie d'audit

L'audit n'est pas activé par défaut sous Windows 2000. Il faut donc choisir les ordinateurs à auditer au moment de l'activer. Puis, il faut choisir le type d'événement susceptible d'être audité, exemple :

Accès aux fichiers et aux dossiers ;

- Ouverture et fermeture de sessions par les utilisateurs ;
- Arrêt et redémarrage d'ordinateurs Windows 2000 ;
- Tentatives de modification des objets Active Directory ;

Il faut ensuite choisir d'auditer la **réussite** ou l'**échec** des événements. Le premier peut permettre de déterminer la fréquence d'accès des utilisateurs, le second peut permettre d'identifier des tentatives d'accès frauduleuses aux réseaux ou à ses services.

Voici quelques recommandations pour définir la stratégie d'audit :

- Déterminer s'il faut suivre les tendances générales du système. Prévoir d'archiver les enregistrements d'événements.
- Examiner régulièrement les journaux de sécurité ;
- Auditer systématiquement et intelligemment les données sensibles afin de récolter les informations importantes et d'assurer la bonne charge des serveurs ;
- Auditer l'accès aux ressources du groupe **Tout le monde** au lieu du groupe **Users** pour auditer tout utilisateurs se connectant au réseau.

3 Implémentation de l'audit

L'audit des Serveurs membres ou autonomes ou des ordinateurs Windows 2000 est configuré sur les ordinateurs locaux.

L'audit des contrôleurs de domaine est configuré à partir des stratégies de groupes du domaine. Pour auditer les modifications sur des objets Active Directory, il faut créer un GPO qui s'appliquera à tous les contrôleurs de domaine du domaine.

L'audit des fichiers et des dossiers ne fonctionne que si ceux-ci sont sur des partitions NTFS.

Il faut disposer de l'autorisation permettant de gérer l'audit et le journal des événements pour créer des stratégies d'audit. Cette autorisation est accordée par défaut aux membres du groupe **Administrateurs**.

Pour configurer l'audit, il faut dans un premier temps définir l'**audit d'objet** et ensuite activer l'**audit des ressources** sur les ressources spécifiques.

4 Utilisation de l'observateur d'événement

L'observateur d'événement permet entre autre de visualiser différents types de journaux :

- Le **journal des applications** : contient les erreurs, les avertissements et les informations renvoyés par les applications ;

- Le **journal de sécurité** : contient les informations de réussite ou d'échec des éléments audités en fonction de la configuration de la stratégie d'audit ;
- Le **journal système** : contient les erreurs, les avertissements et les informations émises par Windows 2000.

Les évènements peuvent être consultés à partir de n'importe quel ordinateur à condition de posséder les privilèges administratifs sur l'ordinateur source de l'événement.

Il est possible de rechercher dans le journal des événements spécifiques en utilisant la commande **filtrer**.

Il est aussi possible d'archiver les journaux générés par la stratégie d'audit pour des comparaisons futur avec d'autres journaux, de définir la taille des fichiers journaux et le comportement de Windows 2000 lorsque les fichiers journaux sont pleins. Il est possible de sauvegarder le fichier journal à partir de la console de l'observateur d'événements en sélectionnant le journal et en utilisant la commande **action**.

Module 10

Etude de cas

1 Scénario

Vous venez d'intégrer la structure de l'entreprise CHOCHOTESOFTWARE. Vous voici désormais responsable du réseau interne. A vous de faire les bons choix afin d'administrer correctement le parc informatique de notre entreprise. Notre entreprise est équipée du matériel suivant : 200 postes de travail sous Windows 2000 Professionnel et XP, 4 serveurs, sous Windows 2000 Serveur dont un serveur d'impression. Notre entreprise comporte plusieurs directions : Une direction générale avec son secrétariat, une direction financière, une direction technique.

Chaque directions souhaite avoir un espace disque commun à toutes les personnes de la direction.

Voici l'ensemble des requêtes de chaque direction :

La direction générale souhaite :

Etre capable de se connecter à partir de n'importe qu'elle machine appartenant à l'entreprise. De plus, ils voient tous les espaces disques ;
Mettre à disposition office 2000 à tous les utilisateurs de l'entreprise ;
Que le bureau du secrétariat soit restreint au strict minimum leur permettant d'effectuer leur travail ; de plus, leurs dossiers Mes Documents doit être sauvegardé continuellement ;
Que tout le monde puisse facilement localiser l'imprimante ;

La direction financière :

Voici les requêtes du responsable de cette direction :

Les membres de cette directions doivent accéder aux espaces suivants : clients, achats, ventes, paye. Ils doivent pouvoir localiser facilement l'espace disque « **Clients** ». Ils veulent s'assurer qu'ils peuvent consulter les fichiers de l'espace « **Client s** » même en cas de coupure du réseau. Ils veulent s'assurer que les membres de cette direction possèdent un bureau qui sera restreint aux icônes dont ils ont besoin pour empêcher toute confusions. Il souhaite savoir qui essaye d'accéder à l'espace « **Paye** » et surtout est-ce qu'il y a des tentatives d'accès frauduleux.

La direction technique :

Des stagiaires sont engagés à la direction technique pour vous aider dans l'administration des ressources du domaine. Vous leur confiez la gestion de l'OU du secrétariat. Vous devez vous assurer qu'ils ne font que ça.

Chacun de membres des autres groupes ne se connecte que sur les machines appartenant à leur groupe.

La répartition des machines se veut uniforme.

Voici quelques noms afin que vous puissiez créer les utilisateurs correspondants. Les autres personnes de l'entreprise calquant leurs droits sur les comptes indiqués ci-après (les modèles). Ainsi, nous avons dans la direction générale, Mr Alex Furax, dans la direction Financière, Mme Alexis Furax et enfin dans la direction technique, Mr Vlade Tepes.

Proposez une démarche de planification afin de gérer au mieux le réseau et ses utilisateurs. Vous disposez d'un domaine Windows 2000 et d'un poste de travail sous Windows XP.

2 Planification

Comptes :

- ?? Définir la nomenclature pour les comptes : 8 caractères, 1 caractère pour le prénom + 1 séparateur (.) + 6 caractères du nom. Dans notre cas, il faudra ajouter un caractère de différentiation. (ex : A.FURAX1)
- ??Durée de vie maximale des mots de passe : 365 jours
- ?? Durée de vie minimale des mots de passe : 121 jours
- ?? Les mots de passes doivent être complexes pour ralentir les attaques de type **brute de force**.
- ?? Longueur minimale des mots de passe : 8 caractères.

Groupes :

- ?? Groupes à étendue globale à créer : Direction général, Direction Financière, Direction Technique, Secrétariat, Admin Juniors ;
- ?? Groupes à étendue locale à créer : AccèsGénérale, AccèsTechnique, AccèsFinancier, Accès Secrétariat, AccèsJunior ...

Profils :

- ?? Les profils sont stockés sur le serveur.
- ??Mes documents du secrétariat seront redirigés sur le serveur.

Espaces de travail :

- ?? Il y a un dossier commun pour chaque service.
- ?? Chaque utilisateur possède un dossier personnel.
- ??Le dossier des clients doit être mis en cache sur les machines de la direction financière. Il doit être publié dans Active Directory pour faciliter sa localisation.
- ??il y a un audit sur le dossier des payes.
- ??On voudrait que vous puissiez plus tard limiter l'espace utilisé dans le volume commun pour certains utilisateurs.

Application :

- ??L'application Office 2000 sera attribuée aux ordinateurs directement sur le conteneur NomDeDomaine pour que l'application soit disponible directement à tous les utilisateurs.

Imprimantes :

- ??Elles doivent facilement être localisées grâce à Active directory.

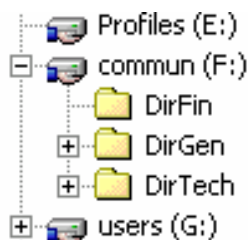
3 Mode opératoire

Avant toute chose, pour pouvoir effectuer les tâches d'administration depuis une station de travail Windows XP à votre disposition, il faut installer les outils d'administration de Windows XP (la commande AdminPack.MSI). Ne pas oublier la commande **RUNAS** ou **exécuter en tant que** (Shift + bouton droit sur une MMC) pour se connecter à un serveur distant à l'aide d'une console MMC pour indiquer le compte Administrateur du domaine afin de pouvoir effectuer les tâches d'administration. L'intérêt est de pouvoir se loguer sur sa station de travail à partir de n'importe quel compte utilisateur et d'effectuer les tâches d'administration sur n'importe quel serveur appartenant au domaine.

a) Création des différents dossiers : Les ressources

Votre serveur disposant de plusieurs disques, vous avez la possibilité d'utiliser des volumes différents comme espaces de travail et de les partager.

Le volume **Commun** stocke les informations de chaque direction ;
Le volume **Profils** contiendra le profil des utilisateurs ;
Le volume **Users** contiendra les dossiers personnels des utilisateurs ;
Le volume **documents** sert à sauvegarder le dossier Mes Documents du secrétariat ;
Les volumes **clients**, **achats**, **ventes**, **paye** stockes les informations de financières de l'entreprise ;



1. A Le volume Commun :

Partager **DirFi** en tant que **DirFi\$**, **DirGen** en tant que **DiGen\$** et **DirTech** en tant que **DirTech\$**
Utiliser les autorisations suivantes :

NTFS	PARTAGE
Administrateur : Contrôle Total	Administrateur : Contrôle Totale

?? Utiliser le groupe de sécurité d'étendue locale **Administrateurs** au lieu du groupe **Administrateur du domaine** qui est un groupe d'étendue globale. Le groupe d'étendue locale **Administrateur** contient **Administrateur du Domaine** (G d'étendue globale) qui lui même contient le compte Administrateur.

?? Eviter de mettre plus de 8 caractères pour ce dossier si des clients MS-DOS doivent y accéder.

1. B Le volume Profils :

Partager le volume en tant que **Profils\$**.
Utiliser les Autorisations suivantes :

NTFS	PARTAGE
Administrateur : Contrôle Totale	Administrateur : Contrôle Totale
Utilisateurs: Modifier	Utilisateurs : Modifier

Users (G d'étendue locale) contient le groupe d'étendue globale **Users**. Chaque utilisateur ajouté fait automatiquement partie de ces groupes.

Attention : La racine du Volume reste accessible à tous les utilisateurs, mais cela permet au système de créer automatiquement les dossiers des profils pour tous les utilisateurs. Par contre, les dossiers de profils sont convenablement protégés.

1. C Le Volume Users :

Partager le en tant que **Users\$**.

Les dossiers des utilisateurs y seront créés par le système.

Partage **Users\$** purement administratif (notamment pour que les dossiers de base des utilisateurs puissent être automatiquement créés par le système et se voir attribuer les autorisations adéquates).

NFTS	PARTAGE
Administrateurs : Contrôle Totale	Administrateurs : Contrôle Totale

1. D Les Volumes Clients, Chats, Ventres, Payes :

Partager les respectivement en tant que **Clients\$, Achats\$, Vente\$, Payes\$**. Ils sont en administratifs car confidentiels.

2. CREATION DES OUS ET DES GROUPES :





REMARQUE : Penser à l'acronyme **AGDLP** : **A**ccount – **G**roup **G**lobal – **D**omain Local – **P**ermission (Autorisation)
Il s'agit de la stratégie de gestion des ressources dans un groupe de travail sous Windows 2000 tels que conseillé par Microsoft.



2. A Création des unités d'organisation :


























Tous les groupes vont appartenir à des unités d'organisation afin de mieux les organiser. Il est conseillée de créer des ressources directement dans les OU qui doivent les regrouper. Pour cela, il faut au préalable créer ses OU.

Dans le tableau suivant :

 : indique une OU ;

 : indique les comptes de machines ;

 +  : indiquent groupes et comptes ;






Conteneur et contenu				
Domaine	 : D GENERAL	Contient les ressources de la direction générale	 : MAT DG	
			 : PERS DG	 +  de la DG
				 PERS SECT  +  secrétariat
	 : D FINANCE	Contient les ressources de la direction financière	 : MAT DF	 de la DF
			 : PERS DF	 +  la DG
	 : D TECHNIQUE	Contient les ressources de la direction technique	 : MAT DT	 de la DT
			 : PERS DT	 +  DT
				 AdminJr  +  l'admin jr
	 : SERVEUR	Contient les serveurs du domaine		

2.B Création des groupes :

Créer les groupes d'étendue locale : AccèsGénérale, Accéstechnique, AccèsFinancier, AccèsSecrétariat, AccèsJunior.

Créer les groupes d'étendue globale : Direction Financière, Secrétariat, Direction Générale, Direction Technique, AdminJunior.

Mettre les groupes d'étendue globale dans les groupes d'étendue locale :

Groupe Etendue Local	Groupe Etendue Globale	Conteneur
AccèsGénérale	Direction Générale	 : PERS DG
AccèsSecrétariat	Direction Générale Secrétariat	 : PERS SECT
AccèsFinancier	Direction Générale Direction Financière	 : PERS DF
AccèsJunior	Direction Générale AdminJunior	 : AdminJr
Accéstechnique	Direction Générale Direction Technique	 : PERS DT

Les Directeurs généraux ont accès à tous les dossiers, ce qui explique leur présence au sein de tous les groupes d'étendue locale.

3. CREATION DES MODELES DE COMPTES

??Permet la création simplifiée et sûre des comptes utilisateurs, les modèles ainsi que les comptes plus tard seront créés dans chacune des OUs précédemment créés.

?? Utiliser une nomenclature pour différencier les comptes valides (une pratique courante consiste à utiliser un _ comme préfixe), ces comptes doivent être désactivés : **_Directeur**, **_Financier**, **_Technicien**, **_Secrétaire**, **_Admjnr**.

?? Dans les profils du modèle, spécifier les informations suivantes :

CHAMP	CONTIENT
Chemin de profil	\\SERVEUR\PROFILS\$\%USERNAME%
Script d'ouverture de session	Init_DG.cmd(pour Direction Générale), Init_DT.cmd (pour Direction Technique), Init_DF.cmd (pour Direction Financière), Init_SC.cmd (pour le secrétariat), Init_AJ (pour les Administrateurs débutants)
Dossier de Base	\\SERVEUR\USERS\$\%USERNAME%\

?? Mettre les appartenances aux groupes d'étendue globale (le modèle **_Directeur** appartient au groupe **Direction Générale**).

??Penser à supprimer le dossier du compte modèle que le composant logiciel enfichable le utilisateurs et ordinateurs Active Directory crée systématiquement.

4. RESTRICTION DES ORDINATEURS POUR L'ACCES

Se fait à partir du composant logiciel enfichable utilisateurs et ordinateurs Active Directory ; il faut sélectionner l'utilisateur concerné (le compte de modèle pour chaque groupe d'utilisateurs), afficher les propriétés du compte et à partir de l'onglet **Compte**, cliquer sur le bouton « **Se connecter à** » pour sélectionner l'ordinateur à partir duquel seront positionnés les restrictions d'ouverture de session.

A l'aide du bouton **Ajouter**, on peut introduire le nom de l'ordinateur sur lequel l'utilisateur (créé à partir de ce compte de modèle) ne pourra pas se connecter.

Par exemple, le compte de modèle **_technique** ne doit pas se connecter aux machines du groupe de la direction financière.

5. MISE À JOUR DES AUTORISATIONS

5.1 Partage Commun

Revenons sur les autorisations des dossiers communs et modifions les afin de prendre en compte les groupes d'étendue locale.

NTFS	PARTAGE
Administrateur : Contrôle Totale	Administrateur : Contrôle Totale
AccèsGénérale : Modifier	AccèsGénérale : Modifier

Avec les autorisations **Modifier** au lieu de **Contrôle total**, les utilisateurs ne peuvent pas prendre possession ou changer les autorisations des fichiers contenus dans les dossiers communs. Positionner l'autorisation modifier pour ce partage à tout les autres groupes pour que ces derniers puissent y accéder.

5.2 Partage Documents\$:

NTFS	PARTAGE
Administrateur : Contrôle Totale	Administrateur : Contrôle Totale
AccèsSécretariat : Modifier	AccèsSécretariat: Modifier

Les membres de la direction générale pourront eux aussi y accéder du fait qu'ils appartiennent au groupe de domaine locale AccèsSécretariat.

5.3 Partage Clients, Achat, Ventes, Paye :

Pour permettre à la direction financière de modifier le contenu de chacun de ses partages, voici les autorisations qu'il faut y placer :

NTFS	PARTAGE
Administrateur : Contrôle Totale	Administrateur : Contrôle Totale
AccèsFinancier : Modifier	AccèsFinancier: Modifier

Les raisons du choix de ses permissions sont les mêmes que celles du choix du partage Commun.

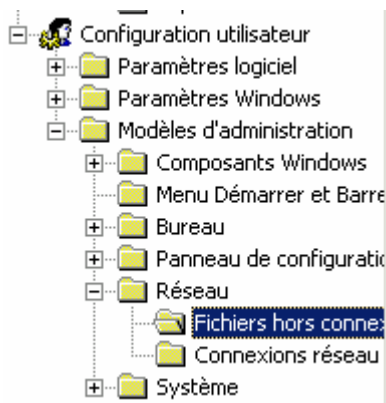
6. FICHIERS HORS CONNEXIONS

6.1 Autorisation de la mise en cache des fichiers

Dans les propriétés du volume partagé Clients\$, le bouton **Mise en cache** donne accès aux propriétés de la mise en cache des dossier et des fichier de ce partage. Activer la mise en cache automatique des documents pour s'assurer que les membres de la direction technique auront toujours ses documents à leur disposition même en cas de coupure du réseau. Attention, il en sera de même pour le membre de la direction.

6.2 Interdiction des modifications des options de Mise en Cache

A l'aide d'un GPO lié à l'OU D TECHNIQUE, dans le dossier **configuration utilisateur\Modèle d'administration\Réseau\Fichiers hors connexions**, activer la stratégie **désactiver la configuration utilisateur des fichiers hors connexions**.



7. SAUVEGARDE DES DOCUMENTS DU SECRETARIAT

7.1 Redirection du dossier Mes Documents

Créer un GPO ou ouvrir un GPO existant pour activer la redirection du dossier Mes Documents. Vérifier la liaison de cette stratégie de groupe, elle doit être liée à l'Unité organisationnelle **PERS SECT**.

7.2 Sauvegarde

Utiliser le gestionnaire de sauvegarde des outils système pour planifier la sauvegarde du volume documents.

Vous pouvez aussi utiliser des outils de sauvegarde d'éditeurs tiers.

8. CONTROLE DE L'ESPACE DISQUE DU VOLUME COMMUN

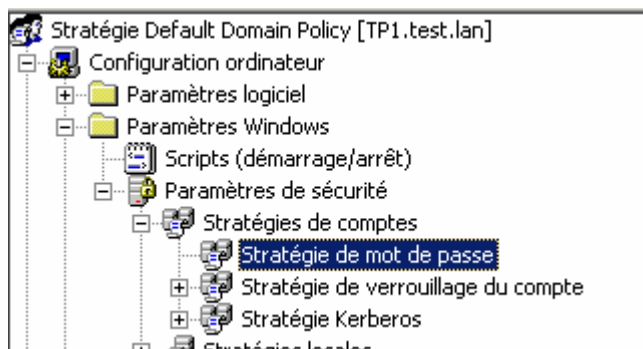
Activer les quotas de disque sur le volume Commun et indiquer les entrées de quotas pour chaque utilisateurs ou groupes d'utilisateurs. Consulter l'article sur la gestion des quotas de disque sur le site [du laboratoire SUPINFO des technologies Microsoft](http://www.laboratoire-supinfo.com). Il est possible via une stratégie de groupe d'activer les quotas de disque. Attention tout de même au conteneur concerné par la gestion des quotas.

9. STRATEGIES DE COMPTES

Ouvrir la stratégie de Groupe par défaut du domaine ou créer une nouvelle stratégie de groupe liée au domaine. A partir de **Configuration de l'ordinateur\Paramètres Windows**, indiquer les éléments de stratégies suivants :

Stratégies de mot de passe	Durée de vie maximale des mots de passe	365 jours
	Durée de vie minimale des mots de passe	121 jours

Verrouillage de compte	Les mots de passes doivent respecter les contraintes de complexité	Activé
	Longueur minimale des mots de passe	8
	Durée de verrouillage des comptes	10 heures
	Réinitialiser le compteur de verrouillage.....	10 Heures
	Seuil de verrouillage des comptes	3 tentatives
	Stocker les mots de passes en utilisant le....	Non configuré



Bien entendu, cela dépend de la politique de sécurité de l'entreprise. Attention, cette stratégie outre passe toute stratégie l'annulant qui serait créée au niveau des conteneurs enfants.

10. DEPLOIEMENT DE LOGICIELS

10.1 Déploiement de office 2000 dans domaine :

Créer un GPO ou ouvrir un GPO (*exemple : la stratégie de groupe par défaut du domaine*). Dans les paramètres logiciels de la configuration matérielle, créer un nouveau package à déployer. Ainsi, au démarrage des machines du domaine, l'application Office 2000 sera installée.

10.3 Cas particulier de la direction technique :

Il est possible de bloquer la stratégie ci-dessus et d'en créer une autre au niveau de l'OU **PERS DT** dans le but de laisser à ses derniers le choix d'installer eux même Office 2000. Dans ce cas, la méthode de déploiement sera différente. Pour cela choisissez entre l'attribution aux utilisateurs ou aux machines. Vérifiez aussi que la stratégie permettant de déployer Office 2000 configurée au niveau du domaine ne possède pas l'option **Aucun remplacement**.





11. RESTRICTION DE L'ENVIRONNEMENT UTILISATEUR

Les restrictions du bureau du secrétariat et de la direction des finances vont se faire à partir des **modèles d'administration** dans la console **Utilisateurs et ordinateurs Active directory**. Dans le cas ou les configurations de restriction de bureau sont les mêmes pour le bureau du secrétariat et le bureau de la direction des finances, utiliser le même GPO lié aux unités d'organisation **PERS SECT** et **PERS DF**.

A partir d'un GPO nouvellement crée ou d'un GPO existant, dans **Configuration utilisateur** ou dans **Configuration ordinateur, Modèles d'administration**, appliquer les modifications qui s'imposent.

Exemple de l'icône favoris réseau du bureau du secrétariat :

Dans configuration utilisateur\bureau\ activer la stratégie cacher l'icône des favoris réseau.

	Supprimer l'icône Mes documents du Bureau	Non configuré
	Supprimer l'icône Mes documents du menu Démarrer	Non configuré
	Cacher l'icône Favoris réseau sur le Bureau	Non configuré
	Cacher l'icône Internet Explorer sur le Bureau	Non configuré

12. DELEGATION DE CONTROLE D'ADMINISTRATION

12.1 Délégation de l'administration à AdmJr :

A partir de la MMC utilisateurs et ordinateurs active directory, faire bouton droit, sur l'OU PERS SECT et choisir **délégation de contrôle**. Ajouter l'utilisateur AdmJr, faire suivant et choisir de créer une tâche personnalisée à déléguer, cliquer ensuite sur suivant. Utiliser les indications suivantes :

Objets spécifiques	Autorisation
Objet Unité d'organisation	Contrôle Totale
Objet Utilisateurs	

Sélectionner les tâches **Création/suppression d'objets enfants spécifiques** puis cliquer sur **Contrôle Totale**.

Assistant Délégation de contrôle

Tâches à déléguer
 Vous pouvez sélectionner des tâches communes ou personnaliser tâches.

☒ Déléguer les tâches courantes suivantes :

- ☐ Crée, supprime et gère les comptes d'utilisateurs
- ☐ Réinitialiser les mots de passe des comptes d'utilisateurs
- ☐ Lire toute l'information sur l'utilisateur
- ☐ Créer, supprimer et gérer les groupes
- ☐ Modifier l'appartenance à un groupe
- ☐ Gérer les liens de stratégies de groupe

☐ Créer une tâche personnalisée à déléguer

12.2 Création de console MMC personnalisée pour l'administration :

Créer une console MMC qui va respecter tous les critères suivants :



Libellé	Choix
Style de liste pour le volet information	Infos-Bulle
Type de description pour la liste des tâches	Verticale
Cible de la liste des tâches	Eléments d'arborescence sélectionnée
Nom de la MMC	Gestion du secrétariat

Type de commandes	commande de menu
-------------------	------------------

Choix des commandes du menu contextuel :

Source des commandes du menu contextuel	Commandes
Tâches des éléments de l'arborescence	Ajouter des membres, Nouveau->groupe, Nouveau->utilisateur, Nouveau ->Unité d'organisation
Liste du volet d'information	: Désactiver le compte, Réinitialiser le mot de passe, Supprimer, Renommer, Propriétés

Modifier les droits d'écritures sur le groupe existant pour permettre au groupe AdminJr d'y ajouter des comptes. Dans les propriétés du groupe, donner les autorisation **Lire** et **Ecrire** au groupe AdminJr.

Limiter l'affichage de la console :

. Activer et fermer la fenêtre racine utilisateur et ordinateur Active directory, personnaliser les paramètres de l'affichage de la présente fenêtre en décochant toutes les options qui se trouvent dans la boîte de dialogue correspondante. Dans les options de la console, passer en mode **utilisateur, accès limité-fenêtre unique**. Enfin, choisir l'icône correspondante à la console et l'enregistrer dans le partage de la direction technique ou l'envoyer par mail aux administrateurs stagiaires.



13. PUBLICATION DE RESSOURCES

La publication se fait à partir de la console Utilisateurs et ordinateurs Active Directory

13.1 Publication de l'imprimante :

Sur le conteneur **NomDeDomaine**, faire **bouton droit**, et sélectionner la commande **Nouveau** puis **Imprimantes**, et indiquer le **nom UNC** de l'imprimante. Ou directement à partir des propriétés de l'imprimante (à partir du serveur d'impression, dans l'onglet **partage**, cocher la case **Liste dans Active Directory**. Cette opération va faciliter la recherche de l'imprimante dans Active directory.

13.2 Publication du partage des clients

Pour faciliter la recherche du partage **Clients\$** à la direction Financière à l'aide de Active directory, bouton droit sur l'unité d'organisation **D FINANCE** et choisir la commande **Nouveau** puis **Dossier partager**. Saisir le nom de l'objet dossier Active Directory ainsi que le chemin UNC **\\SERVEUR\Clients\$**. Ajouter les mots clés Clientèles, fiches clients....

Modifier ensuite les autorisations des DACLs de l'objet Active directory créée pour que seuls les utilisateurs de l'OU de la direction Financière et la direction générale puisse voir ce partage. Pour cela, s'assurer que **l'option Fonctionnalités avancées** dans le menu Affichage de la MMC Utilisateurs et ordinateurs Active directory est **activée**. Faire bouton droit sur l'objet du dossier publier **NomduPartagePublié**, puis propriétés et utiliser l'onglet sécurité. Supprimer le groupe **Utilisateurs authentifiés**, ajouter le groupe **AccèsFinanciers**, et donner lui l'autorisation **Lire**.

14. SCRIPTS D'OUVERTURE DE SESSION

Pour affecter les scripts de connexion, deux possibilités : soit à partir des propriétés des comptes utilisateurs, soit à partir d'un GPO. Pour le second cas, veiller à ce que les scripts soient indiqués à partir des OUs correspondantes aux utilisateurs qui seront affectés par ses scripts. *Par exemple, pour la direction financière* (📁 : **D FINANCE** ou

PERS DF), le GPO crée sera soit un GPO existant modifié pour prendre en compte les scripts d'ouverture de session, soit une nouvelle stratégie de groupe configuré pour les mêmes objectifs.

Voici la liste des scripts à créer :

Init_DG.cmd, init_DF.cmd, init_DT.cmd, Init_SC.cmd, Init_AJ.cmd

Le script doit connecter le lecteur partagé pour le département :

NET USE W:\\SERVEUR\\DIRGEN\$ /PERSISTENT : NO

Le script doit synchroniser l'heure de la station avec celle du serveur :

NET TIME \\SERVEUR /SET /Y

Ainsi le script iniDG.cmd contiendra par exemple :

@echo off

@rem Script de connexion Direction GENERALE 10/07/2002

@echo Connexion au lecteur commun Direction Générale

NET USE W:\\SEVEUR\\DIRGEN\$ /PERSITENT: NO

@echo Connexion au lecteur commun DirectionFinancière

NET USE X:\\SERVEUR\\DIRFIN\$ /PERSISTENT : NO

@echo Connexion au lecteur commun DirectionTechnique

NET USE Y : \\SERVEUR\\DIRTECH\$ /PERSISTENT : NO

NET TIME \\SERVEUR /SET /Y

@echo Connexion au lecteur Clients\$ DirectionFinancière

NET USE Y : \\SERVEUR\\CLIENTS\$ /PERSISTENT : NO

NET TIME \\SERVEUR /SET /Y

@echo Connexion au lecteur Achats\$ DirectionFinancière

NET USE Y : \\SERVEUR\\ACHATS\$ /PERSISTENT : NO

NET TIME \\SERVEUR /SET /Y

@echo Connexion au lecteur Ventes\$ DirectionFinancière

NET USE Y : \\SERVEUR\\VENTES\$ /PERSISTENT : NO

NET TIME \\SERVEUR /SET /Y

@echo Connexion au lecteur Paye\$ DirectionFinancière

NET USE Y : \\SERVEUR\\PAYE \$ /PERSISTENT : NO

NET TIME \\SERVEUR /SET /Y

15. CREATION DES COMPTES

Elle va se faire dans les OUs précédemment créés.

Copier le modèle concerné, mettre le nouveau nom d'utilisateur ainsi que son mot de passe dans les champs correspondants.

Si nous souhaitons que chaque utilisateur possède une unité connectée sur son répertoire personnel, nous devons partager ce dossier manuellement et mettre les Autorisations adéquates :

Partager le dossier de l'utilisateur (partage caché avec \$), **exemple** : AFURAX1

Mettre les autorisations suivantes (dans le cas de l'utilisateur AFURAX1)

NTFS	PARTAGE
Administrateur : Contrôle Total	Administrateur : Contrôle Total
AFURAX1 : Modifier	AFURAX1 : Modifier

Modifier ensuite le chemin du dossier de base en spécifiant le partage caché
(Par **exemple**: \\SERVEUR\USER\$\%USERNAME% devient \\SERVEUR\ AFURAX1)

16. AUDIT

Avant tout, il faut via un GPO activer l'audit sur l'OU contenant le serveur à auditer. Dans le cas présent, il s'agit de l'OU SERVEURS. Dans le dossier **Configuration Ordinateur\Paramètres Windows\Paramètres de sécurité\stratégies locale\stratégie d'audit** de l'objet stratégie de groupe, choisir auditer l'accès aux objets. Sélectionner les options **Essais ayants réussis** et/ou **Essais ayant échoués**.

Il est aussi possible de d'activer l'audit directement sur le serveur concerné. Pour cela, il faut utiliser la console Stratégies de sécurité locale sur le serveur.

16.1 Audit de l'accès au partage de Paye\$:

Après l'activation de l'audit sur l'OU SERVEURS, dans les propriétés du partage **Paye\$**, utiliser l'onglet **Sécurité** et le bouton **Avancé** pour obtenir l'onglet **Audit**. Indiquer les paramètres suivants :

Groupe	Evènements audités
Tout le monde	Modifier les autorisations : Echec, Supprimer : Echec et réussite, Appropriation : Echec.

