

Essentiel Windows 2003

ADMINISTRER ET GERER UN ENVIRONNEMENT MICROSOFT WINDOWS SERVER 2003

Auteurs : Yann ALET, Brahim NEDJIMI et Loïc THOBOIS
Revu par LHOME L Guillaume, TALMANT Grégory
Version 0.95 - 16-11-2004

Table des matières

| | | |
|-----------|--|-----------|
| 1. | INTRODUCTION A L'ADMINISTRATION DES COMPTES ET DES RESSOURCES..... | 7 |
| 1.1. | L'ENVIRONNEMENT DE WINDOWS 2003 SERVER | 7 |
| 1.1.1. | Rôles des serveurs..... | 7 |
| 1.1.2. | La Famille Serveur Windows 2003..... | 7 |
| 1.1.3. | Présentation du service d'annuaire (Active Directory) | 8 |
| 1.1.4. | Structure d'Active Directory | 8 |
| 1.2. | INSTALLATION ET CONFIGURATION DES OUTILS D'ADMINISTRATION | 9 |
| 1.2.1. | Installation des outils d'administration | 9 |
| 1.2.2. | Présentation et configuration d'une MMC | 9 |
| 1.2.3. | Résolution des problèmes lors de l'installation des outils d'administration..... | 10 |
| 1.3. | PRESENTATION ET CONFIGURATION DES UNITES D'ORGANISATIONS | 10 |
| 1.3.1. | Présentation des unités d'organisations | 10 |
| 1.3.2. | Modèle hiérarchique des unités d'organisation..... | 10 |
| 1.3.3. | Dénomination des unités d'organisation | 10 |
| 1.3.4. | Création d'une unité d'organisation..... | 11 |
| 1.4. | DEPLACEMENT DES OBJETS DU DOMAINE..... | 11 |
| 2. | GESTION DES COMPTES D'UTILISATEUR ET D'ORDINATEUR..... | 12 |
| 2.1. | CREATION DES COMPTES UTILISATEUR | 12 |
| 2.1.1. | Présentation des comptes d'utilisateurs..... | 12 |
| 2.1.2. | Convention de nom des comptes utilisateurs..... | 12 |
| 2.1.3. | Nomenclature de création de compte utilisateur..... | 12 |
| 2.1.4. | Mot de passe utilisateur | 13 |
| 2.1.5. | Création de compte d'utilisateur..... | 13 |
| 2.2. | CREATION DE COMPTES D'ORDINATEUR..... | 13 |
| 2.2.1. | Présentation des comptes d'ordinateurs | 13 |
| 2.2.2. | Création de compte d'ordinateur | 13 |
| 2.3. | MODIFICATION DES PROPRIETES DES COMPTES D'UTILISATEUR ET D'ORDINATEUR | 13 |
| 2.4. | CREATION DE MODELES DE COMPTES UTILISATEUR | 14 |
| 2.4.1. | Présentation d'un modèle de compte utilisateur..... | 14 |
| 2.4.2. | Propriétés maintenues lors de la copie du modèle de compte..... | 14 |
| 2.5. | ACTIVATION ET DESACTIVATION D'UN COMPTE UTILISATEUR | 15 |
| 2.6. | RECHERCHE DANS ACTIVE DIRECTORY | 15 |
| 2.6.1. | Recherche standard..... | 15 |
| 2.6.2. | Recherche personnalisée..... | 15 |
| 2.6.3. | Sauvegarde des requêtes | 15 |
| 3. | GESTION DES GROUPES | 17 |
| 3.1. | PRESENTATION DES GROUPES..... | 17 |
| 3.1.1. | Groupes sur un ordinateur local..... | 17 |
| 3.1.2. | Groupes sur un contrôleur de domaine..... | 17 |
| 3.2. | CONVENTION DE NOMMAGE DES GROUPES..... | 18 |
| 3.3. | GESTION DES GROUPES | 18 |
| 3.3.1. | Stratégie d'utilisation des groupes dans un domaine unique..... | 18 |
| 3.3.2. | Stratégie d'utilisation des groupes dans un environnement à domaines multiples | 19 |
| 3.3.3. | Modification de l'étendue d'un groupe | 19 |
| 3.4. | GROUPES PAR DEFAUT | 19 |
| 3.4.1. | Groupes par défaut sur un serveur membre..... | 19 |
| 3.4.2. | Groupes par défaut dans Active Directory..... | 20 |
| 3.5. | GROUPES SYSTEME | 20 |
| 4. | GESTION D'ACCES AUX RESSOURCES | 21 |
| 4.1. | CONTROLE D'ACCES..... | 21 |
| 4.1.1. | Les entités de sécurité | 21 |
| 4.1.2. | Le SID | 21 |
| 4.1.3. | DACL - Discretionary Access Control List..... | 21 |

| | | |
|-----------|--|-----------|
| 4.2. | AUTORISATIONS..... | 21 |
| 4.2.1. | Autorisations standards | 21 |
| 4.2.2. | Autorisations spéciales..... | 22 |
| 4.3. | ADMINISTRATION DES ACCES AUX DOSSIERS PARTAGES | 22 |
| 4.3.1. | Description des dossiers partagés..... | 22 |
| 4.3.2. | Partages administratifs..... | 22 |
| 4.3.3. | Création de dossiers partagés..... | 22 |
| 4.3.4. | Publication des dossiers partagés..... | 22 |
| 4.3.5. | Autorisations sur les dossiers partagés..... | 23 |
| 4.3.6. | Connexion à un dossier partagé..... | 23 |
| 4.4. | ADMINISTRATION DES ACCES AUX FICHIERS ET DOSSIERS NTFS | 23 |
| 4.4.1. | Présentation de NTFS..... | 23 |
| 4.4.2. | Autorisations sur les fichiers et dossiers NTFS..... | 24 |
| 4.4.3. | Impact de la copie et du déplacement sur les autorisations NTFS..... | 24 |
| 4.4.4. | Présentation de l'héritage NTFS..... | 25 |
| 4.4.5. | Identification des autorisations effectives | 25 |
| 4.4.6. | Cumul des autorisations NTFS et des autorisations de partage | 26 |
| 4.5. | MISE EN PLACE DES FICHIERS HORS CONNEXION | 26 |
| 4.5.1. | Présentation des fichiers hors connexion..... | 26 |
| 5. | IMPLEMENTATION DE L'IMPRESSION..... | 28 |
| 5.1. | PRESENTATION DE L'IMPRESSION DANS LA FAMILLE WINDOWS SERVER 2003 | 28 |
| 5.1.1. | Terminologie de l'impression..... | 28 |
| 5.1.2. | Types de clients d'impression supportés par Windows 2003..... | 28 |
| 5.1.3. | Fonctionnement de l'impression | 29 |
| 5.2. | INSTALLATION ET PARTAGE D'IMPRIMANTES | 29 |
| 5.2.1. | Imprimantes locales et imprimantes réseau..... | 29 |
| 5.2.2. | Installation et partage d'une imprimante..... | 29 |
| 5.3. | AUTORISATIONS D'IMPRIMANTES PARTAGEES | 30 |
| 5.4. | GESTION DES PILOTES D'IMPRIMANTES | 30 |
| 6. | ADMINISTRATION DE L'IMPRESSION | 31 |
| 6.1. | CHANGEMENT DE L'EMPLACEMENT DU SPOULEUR D'IMPRESSION | 31 |
| 6.2. | DEFINITION DES PRIORITES D'IMPRIMANTES | 31 |
| 6.3. | PLANIFICATION DE LA DISPONIBILITE DES L'IMPRIMANTES | 32 |
| 6.4. | CONFIGURATION D'UN POOL D'IMPRESSION..... | 32 |
| 7. | GESTION D'ACCES AUX OBJETS DANS LES UNITES D'ORGANISATION..... | 33 |
| 7.1. | STRUCTURE DES UNITES D'ORGANISATION | 33 |
| 7.2. | MODIFICATION DES AUTORISATIONS SUR LES OBJETS ACTIVE DIRECTORY | 33 |
| 7.2.1. | Autorisations sur les objets Active Directory..... | 33 |
| 7.2.2. | Définitions des autorisations effectives..... | 33 |
| 7.3. | DELEGATION DU CONTROLE DES UNITES D'ORGANISATION | 34 |
| 8. | IMPLEMENTATION DES STRATEGIES DE GROUPES | 35 |
| 8.1. | DESCRIPTION DES STRATEGIES DE GROUPES..... | 35 |
| 8.1.1. | Présentation des stratégies de groupes..... | 35 |
| 8.1.2. | Description des paramètres de configuration des utilisateurs et des ordinateurs | 35 |
| 8.2. | IMPLEMENTATION D'OBJETS DE STRATEGIE DE GROUPE..... | 35 |
| 8.2.1. | Les outils permettant d'implémenter les GPO | 35 |
| 8.2.2. | Les modèles d'administration | 36 |
| 8.2.3. | Description d'un lien d'objet de stratégie de groupe..... | 36 |
| 8.2.4. | Héritage de l'autorisation de stratégie de groupe dans Active Directory | 36 |
| 8.3. | ADMINISTRATION DU DEPLOIEMENT D'UNE STRATEGIE DE GROUPE..... | 36 |
| 8.3.1. | Impact de l'existence d'objets de stratégie de groupe conflictuels | 36 |
| 8.3.2. | Attributs d'un lien d'objet de stratégie de groupe..... | 37 |
| 8.3.3. | Filtrage du déploiement d'une stratégie de groupe | 37 |
| 9. | GESTION DE L'ENVIRONNEMENT UTILISATEUR A L'AIDE DES STRATEGIES DE GROUPES | 38 |

| | |
|--|-----------|
| 9.1. CONFIGURATION DE PARAMETRES DE STRATEGIE DE GROUPE..... | 38 |
| 9.1.1. Présentation des stratégies de groupes..... | 38 |
| 9.1.2. Paramètres « Non configuré », « Activé » et « Désactivé »..... | 38 |
| 9.2. ATTRIBUTION DES SCRIPTS AVEC LA STRATEGIE DE GROUPE..... | 38 |
| 9.3. CONFIGURATION DE LA REDIRECTION DE DOSSIERS | 39 |
| 9.4. DETERMINATION DES OBJETS DE STRATEGIE DE GROUPE | 39 |
| 9.4.1. GPOupdate..... | 39 |
| 9.4.2. GPOresult | 40 |
| 9.4.3. Rapport de stratégie de groupe..... | 40 |
| 9.4.4. Simulation de déploiement de GPO | 40 |
| 9.4.5. Résultat de déploiement de GPO..... | 40 |
| 10. IMPLEMENTATION DES MODELES D'ADMINISTRATION ET DES STRATEGIES D'AUDIT | 41 |
| 10.1. VUE D'ENSEMBLE DE LA SECURITE DANS WINDOWS 2003 | 41 |
| 10.2. UTILISATION DE MODELES DE SECURITE POUR PROTEGER LES ORDINATEURS | 41 |
| 10.2.1. Présentation des stratégies de sécurité | 41 |
| 10.2.2. Description des modèles de sécurité | 41 |
| 10.2.3. Description des paramètres de modèles de stratégies..... | 42 |
| 10.2.4. Outils de création et d'importation des modèles de sécurité personnalisés..... | 42 |
| 10.3. CONFIGURATION DE L'AUDIT | 42 |
| 10.3.1. Présentation de l'audit..... | 42 |
| 10.3.2. Description d'une stratégie d'audit | 43 |
| 10.4. GESTION DES JOURNAUX DE SECURITE..... | 43 |
| 11. PREPARATION DE L'ADMINISTRATION D'UN SERVEUR..... | 45 |
| 11.1. PREPARATION DE L'ADMINISTRATION D'UN SERVEUR..... | 45 |
| 11.1.1. Utilisation des appartenances de groupe pour administrer un serveur..... | 45 |
| 11.1.2. Qu'est-ce que la commande Exécuter en tant que ?..... | 45 |
| 11.1.3. Qu'est-ce que l'outil Gestion de l'ordinateur ?..... | 46 |
| 11.1.4. Rôle de la console MMC dans le cadre d'une administration à distance..... | 46 |
| 11.1.5. Comment créer une MMC pour gérer un serveur ? | 47 |
| 11.2. CONFIGURATION DE LA FONCTION BUREAU A DISTANCE POUR ADMINISTRER UN SERVEUR..... | 47 |
| 11.2.1. Qu'est-ce que l'outil Bureau à distance pour administration ?..... | 47 |
| 11.2.2. Que sont les préférences des ordinateurs clients dans le cadre d'une connexion Bureau à distance ? | 48 |
| 11.2.3. Bureaux à distance..... | 48 |
| 11.3. GESTION DES CONNEXIONS AU BUREAU A DISTANCE | 49 |
| 11.3.1. Que sont les paramètres de délai des connexions de Bureau à distance ? | 49 |
| 11.3.2. Qu'est-ce que le Gestionnaire des services Terminal Server ? | 50 |
| 12. PREPARATION DE L'ANALYSE DES PERFORMANCES DU SERVEUR..... | 51 |
| 12.1. PRESENTATION DE L'ANALYSE DES PERFORMANCES DU SERVEUR | 51 |
| 12.1.1. Pourquoi analyser les performances ?..... | 51 |
| 12.2. ANALYSE EN TEMPS REEL ET PROGRAMMEE..... | 51 |
| 12.2.1. Qu'est-ce que l'analyse en temps réel et programmée ?..... | 51 |
| 12.2.2. Qu'est-ce que le Gestionnaire des tâches ?..... | 51 |
| 12.2.3. Qu'est-ce que la console Performances ? | 52 |
| 12.2.4. Pourquoi analyser les serveurs à distance ?..... | 52 |
| 12.3. CONFIGURATION ET GESTION DES JOURNAUX DE COMPTEUR | 53 |
| 12.3.1. Qu'est-ce qu'un journal de compteur ? | 53 |
| 12.3.2. Comment planifier un journal de compteur ? | 53 |
| 12.4. CONFIGURATION DES ALERTES..... | 53 |
| 12.4.1. Qu'est-ce qu'une alerte ?..... | 53 |
| 12.4.2. Comment créer une alerte ?..... | 54 |
| 12.5. CONSEIL D'OPTIMISATION D'UN SERVEUR | 54 |
| 13. MAINTENANCE DES PILOTES DE PERIPHERIQUES | 56 |
| 13.1. CONFIGURATION DES OPTIONS DE SIGNATURE DES PILOTES DE PERIPHERIQUES | 56 |
| 13.1.1. Qu'est-ce qu'un périphérique ? | 56 |

| | | |
|------------|--|-----------|
| 13.1.2. | <i>Qu'est-ce qu'un pilote de périphérique ?</i> | 56 |
| 13.1.3. | <i>Qu'est-ce qu'un pilote de périphérique signé ?</i> | 56 |
| 13.1.4. | <i>Qu'est-ce que la console Gestion des stratégies de groupe ?</i> | 57 |
| 13.2. | UTILISATION DE LA VERSION PRECEDENTE D'UN PILOTE DE PERIPHERIQUE | 57 |
| 14. | GESTION DES DISQUES | 58 |
| 14.1. | PREPARATION DES DISQUES | 58 |
| 14.1.1. | <i>Qu'est-ce que l'outil Gestion des disques ?</i> | 58 |
| 14.1.2. | <i>Qu'est-ce que l'outil DiskPart ?</i> | 58 |
| 14.1.3. | <i>Qu'est-ce qu'une partition ?</i> | 58 |
| 14.1.4. | <i>Comment convertir les systèmes de fichiers ?</i> | 59 |
| 14.2. | GESTION DES PROPRIETES D'UN DISQUE | 59 |
| 14.2.1. | <i>Comment effectuer une nouvelle analyse des propriétés d'un disque ?</i> | 59 |
| 14.3. | GESTION DES LECTEURS MONTES | 59 |
| 14.3.1. | <i>Qu'est-ce qu'un lecteur monté ?</i> | 59 |
| 14.3.2. | <i>Quel est l'intérêt du lecteur monté ?</i> | 59 |
| 14.3.3. | <i>Comment gérer un lecteur monté ?</i> | 60 |
| 14.4. | TYPE DE DISQUES | 60 |
| 14.4.1. | <i>Utilisation des disques de base</i> | 60 |
| 14.4.2. | <i>Utilisation des disques dynamiques</i> | 60 |
| 14.5. | CREATION DE VOLUMES..... | 62 |
| 15. | GESTION DU STOCKAGE DES DONNEES | 63 |
| 15.1. | GESTION DE LA COMPRESSION DES FICHIERS..... | 63 |
| 15.1.1. | <i>Qu'est-ce que la compression des fichiers ?</i> | 63 |
| 15.1.2. | <i>Qu'est-ce que la commande compact ?</i> | 63 |
| 15.2. | CONFIGURATION DU CRYPTAGE DES FICHIERS | 64 |
| 15.2.1. | <i>Qu'est-ce que le cryptage EFS ?</i> | 64 |
| 15.2.2. | <i>Comment crypter un fichier ou un dossier ?</i> | 65 |
| 15.2.3. | <i>Quels sont les effets produits par le déplacement ou la copie de fichiers ou de dossiers cryptés ?</i> | 65 |
| 15.3. | IMPLEMENTATION DES QUOTAS DE DISQUE | 65 |
| 15.3.1. | <i>Qu'est-ce qu'un paramètre de quota de disque ?</i> | 65 |
| 15.3.2. | <i>Comment activer et désactiver des quotas de disque ?</i> | 65 |
| 15.3.3. | <i>Comment ajouter et supprimer des entrées de quota de disque ?</i> | 66 |
| 16. | GESTION DE LA RECUPERATION EN CAS D'URGENCE | 67 |
| 16.1. | SAUVEGARDE DES DONNEES | 67 |
| 16.1.1. | <i>Vue d'ensemble de la sauvegarde des données</i> | 67 |
| 16.1.2. | <i>Qui peut sauvegarder les données ?</i> | 67 |
| 16.1.3. | <i>Qu'est-ce que les données sur l'état du système ?</i> | 67 |
| 16.1.4. | <i>Types de sauvegardes</i> | 67 |
| 16.1.5. | <i>Qu'est-ce que nbackup ?</i> | 68 |
| 16.1.6. | <i>Qu'est-ce qu'un jeu de récupération automatique du système ?</i> | 68 |
| 16.2. | PLANIFICATION DES OPERATIONS DE SAUVEGARDE | 68 |
| 16.2.1. | <i>Qu'est-ce qu'une opération de sauvegarde planifiée ?</i> | 68 |
| 16.2.2. | <i>Comment planifier une opération de sauvegarde ?</i> | 69 |
| 16.3. | RESTAURATION DES DONNEES | 69 |
| 16.3.1. | <i>Qu'est-ce que la restauration des données ?</i> | 69 |
| 16.4. | CONFIGURATION DES CLICHES INSTANTANES..... | 69 |
| 16.4.1. | <i>Qu'est-ce que les clichés instantanés ?</i> | 69 |
| 16.4.2. | <i>Comment configurer des clichés instantanés sur le serveur ?</i> | 70 |
| 16.4.3. | <i>Logiciel client pour les versions précédentes des clichés instantanés</i> | 70 |
| 16.5. | RECUPERATION SUITE A UNE DEFAILLANCE DU SERVEUR | 71 |
| 16.5.1. | <i>Contrôle des paramètres système au cours du processus d'amorçage</i> | 71 |
| 16.5.2. | <i>Modification du comportement au démarrage à l'aide du fichier Boot.ini</i> | 72 |
| 16.5.3. | <i>Utilisation des options d'amorçage avancées pour résoudre les problèmes de démarrage</i> | 72 |
| 16.5.4. | <i>Utilisation de la console de récupération pour démarrer l'ordinateur</i> | 72 |
| 16.6. | CHOIX D'UNE METHODE DE RECUPERATION EN CAS D'URGENCE..... | 73 |
| 16.6.1. | <i>Quels sont les outils de récupération en cas d'urgence ?</i> | 73 |
| 17. | MAINTENANCE DES LOGICIELS A L'AIDE DES SERVICES SUS | 74 |

| | |
|--|----|
| 17.1. PRESENTATION DES SERVICES SUS..... | 74 |
| 17.1.1. <i>Qu'est-ce que Windows Update ?</i> | 74 |
| 17.1.2. <i>Qu'est-ce que la fonctionnalité Mises à jour automatiques ?</i> | 74 |
| 17.1.3. <i>Comparaison entre Windows Update et la fonctionnalité Mises à jour automatiques</i> | 74 |
| 17.1.4. <i>Qu'est-ce que les services SUS ?</i> | 74 |
| 17.2. INSTALLATION ET CONFIGURATION DES SERVICES SUS | 75 |
| 17.2.1. <i>Qu'est-ce qu'un point de distribution du serveur de service SUS ?</i> | 75 |
| 17.2.2. <i>Configurations de serveur requises pour les services SUS</i> | 75 |
| 17.2.3. <i>Comment installer et configurer les services SUS ?</i> | 75 |
| 17.2.4. <i>Configuration de la fonctionnalité Mises à jour automatiques</i> | 75 |

1. Introduction à l'administration des comptes et des ressources

1.1. L'environnement de Windows 2003 Server

1.1.1. Rôles des serveurs

De plus en plus d'entreprises implémentent de multiples technologies afin d'améliorer l'environnement de travail de leurs employés.

Ainsi il n'est pas rare de voir une seule machine configurée avec Active Directory, le serveur DNS, le serveur DHCP, le partage de connexion Internet, un serveur VPN et exécutant aussi les services de partages de fichiers et d'impression.

On distingue ainsi un certain nombre de rôles :

- **Les contrôleurs de domaines** : Ce sont des serveurs sur lesquels on a installé Active Directory et qui s'occupent de l'authentification des utilisateurs dans un domaine.
- **Les serveurs de fichiers** : Ce sont des serveurs qui permettent de créer un espace de stockage partagé sur le réseau. Ils mettent ainsi une partie de leur espace disque disponible sur le réseau.
- **Les serveurs d'impression** : Ils permettent de partager une imprimante sur un réseau et de gérer la file d'attente d'impression de celle-ci.
- **Les serveurs d'applications** : Ils permettent à une application d'utiliser le système d'exploitation comme support afin d'en utiliser les composants de gestion (ex : serveur de messagerie, de base de données, ...).

L'ensemble de ces rôles peuvent être gérés à l'aide de l'outil **Assistant Configurer votre serveur** sous Windows 2003 Server.

1.1.2. La Famille Serveur Windows 2003

Parmi les produits de la famille Windows 2003, il existe quatre systèmes d'exploitation : Windows 2003 Web, Windows 2003 Standard, Windows 2003 Enterprise et Windows 2003 Datacenter. Mis à part pour l'édition Web, peu de choses les différencient.

Le tableau suivant indique la configuration minimale requise pour l'installation de chacun de ces quatre systèmes.

| | Windows 2003 Web Edition | Windows 2003 Standard Edition | Windows 2003 Enterprise Edition | Windows 2003 Datacenter Edition |
|--|---|---|---|--|
|  Processeurs | 133 MHz ou plus (supporte 2 processeurs au plus) | 133 MHz ou plus (supporte 4 processeurs au plus) | 133 MHz ou plus (supporte 8 processeurs au plus) 733 MHz ou plus pour les processeurs de type Itanium | 400 MHz ou plus (supporte 64 processeurs au plus) 733 MHz ou plus pour les processeurs de type Itanium |

| | | | | |
|---|--|--|--|---|
|  Mémoire vive | 128Mo minimum 256Mo recommandés 2Go maximum | 128Mo minimum 256Mo recommandés 4Go maximum | 128Mo minimum 256Mo recommandés 32Go maximum pour les X86 et 64Go pour les processeurs de type Itanium | 512Mo minimum 1Go recommandés 32Go maximum pour les X86 et 512Go pour les processeurs de type Itanium |
|  Disque dur | Disque avec 1,5Go d'espace libre pour l'installation | Disque avec 1,5Go d'espace libre pour l'installation | Disque avec 1,5Go d'espace libre pour l'installation et 2Go pour les Itanium | Disque avec 1,5Go d'espace libre pour l'installation et 2Go pour les Itanium |

1.1.3. Présentation du service d'annuaire (Active Directory)

Le service Active Directory (Active Directory) permet une gestion centralisée. Cela vous donne la possibilité d'ajouter, de retirer et de localiser les ressources facilement.

Ainsi, nous avons :

- **Une administration simplifiée** : Active Directory offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- **Une mise à l'échelle** : Active Directory permet de gérer des millions d'objets répartis sur plusieurs sites si cela est nécessaire.
- **Un support standard ouvert** : Active Directory utilise DNS pour nommer et localiser des ressources, ainsi les noms de domaine Windows 2003 sont aussi des noms de domaine DNS. Active Directory fonctionne avec des services de clients différents tels que NDS de Novell. Cela signifie qu'il peut chercher les ressources au travers d'une fenêtre d'un navigateur web. De plus, le support de Kerberos 5 apporte la compatibilité avec les autres produits qui utilisent le même mécanisme d'authentification.

1.1.4. Structure d'Active Directory

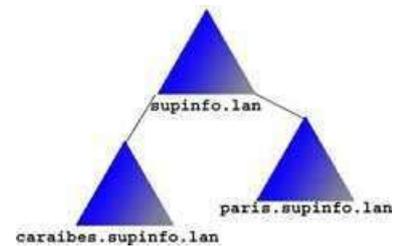
La structure d'Active Directory est hiérarchique, elle se décompose comme suit :

- **Objet** : représente une ressource du réseau qui peut-être par exemple un ordinateur ou un compte utilisateur.
- **Classe** : description structurelle d'objets tels les comptes d'utilisateurs, ordinateurs, domaines, ou unités organisationnelles.
- **Unité organisationnelle (OU)** : conteneur utilisé pour organiser les objets d'un domaine à l'intérieur de groupes administratifs logiques tels les ordinateurs, les imprimantes, les comptes d'utilisateurs, les fichiers partagés, les applications et même d'autres unités organisationnelles.
- **Domaine** : chacun des objets d'un réseau existe dans un domaine et chaque domaine contient les informations des objets qu'il contient. Un domaine est sécurisé, c'est à dire que l'accès aux objets est limité par des ACL (Access Control List). Les ACL contiennent les permissions, associées aux objets, qui déterminent quels utilisateurs ou quels types d'utilisateurs peuvent y accéder. Dans Windows 2003, toutes les stratégies de sécurité et les configurations (telles

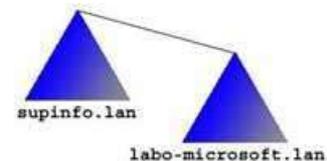


les droits administratifs) ne se transmettent pas d'un domaine à l'autre. L'administrateur de domaine peut déterminer les stratégies uniquement à l'intérieur de son propre domaine.

- **Arbre** : c'est un groupement ou un arrangement hiérarchique d'un ou plusieurs domaines Windows 2003 qui partagent des espaces de noms contigus (par exemple : administration.supinfo.com, comptabilité.supinfo.com, et training.supinfo.com). Tous les domaines d'un même arbre partagent le même schéma commun (la définition formelle de tous les objets qui peuvent être enregistrés dans une architecture d'Active Directory) et partagent un catalogue commun.



- **Forêt** : c'est un groupement ou un arrangement hiérarchique d'un ou plusieurs arbres qui ont des noms disjoints (par exemple : laboratoire-microsoft.org et supinfo.com). Tous les arbres d'une forêt partagent le même schéma commun et le même catalogue, mais ont des structures de noms différentes. Les domaines d'une forêt fonctionnent indépendamment les uns des autres, mais les forêts permettent la communication d'un domaine à l'autre.



- **Sites** : combinaison d'une ou plusieurs IP de sous-réseaux connectés par des liens à hauts débits. Ils ne font pas partie d'un espace de nommage d'Active Directory, et ils contiennent seulement les ordinateurs, les objets et les connexions nécessaires pour configurer la réplication entre sites. Ils permettent d'intégrer la topologie physique du réseau dans Active Directory.

1.2. Installation et configuration des outils d'administration

1.2.1. Installation des outils d'administration

Les outils d'administration permettent la gestion des serveurs à distance. Ils peuvent être installés sur n'importe quelle machine sous Windows 2003 par l'intermédiaire de **adminpak.msi** qui se trouve dans le dossier i386 du CD ROM d'installation du système.

Les outils d'administration sont installés par défaut sur le contrôleur de domaine.

Il peut être utile, pour des raisons de sécurité, d'utiliser les outils d'administration en ayant ouvert une session avec votre compte de domaine basique et en utilisant la commande **Exécuter en tant que** pour lancer les outils d'administration.

1.2.2. Présentation et configuration d'une MMC

Windows 2003 (toutes versions) intègre un modèle d'outils d'administration nommé MMC (Microsoft Management Console) qui donne la possibilité aux administrateurs de créer eux-mêmes leur propre console d'administration.

Il suffit pour cela d'intégrer les composants logiciels enfichables (snap-in) couramment utilisés.

Cela permet aussi de mettre à disposition des administrateurs subalternes des outils d'administration personnalisés. Ainsi un administrateur ayant pour unique fonction la maintenance des comptes du domaine ne pourra supprimer un utilisateur ou un groupe par erreur puisque l'option de suppression n'apparaîtra pas dans sa console.

Afin de pouvoir créer une MMC personnalisée, il vous suffit de suivre la procédure suivante :

Allez dans le menu **Démarrer / Exécuter** (☰-R).

Tapez **MMC**, puis **Entrer**.

Dans le menu console, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.

Cliquez ensuite sur **Ajouter** et sélectionnez le composant que vous souhaitez ajouter à votre console (Notez que l'interface de cette fenêtre est trompeuse: si vous double-cliquez sur un composant ou si vous cliquez sur Ajouter, le composant est ajouté à la liste sans aucune confirmation).

1.2.3. Résolution des problèmes lors de l'installation des outils d'administration

Si des problèmes surviennent lors de l'installation des outils d'administration, deux raisons principales peuvent en être la cause :

- **Permissions insuffisantes** : Seul les utilisateurs membres du groupe Administrateurs ont les privilèges suffisants pour pouvoir installer les outils d'administration.
- **Système d'exploitation non supporté** : Seul Windows XP et Windows 2003 supportent l'installation des outils d'administration.

Si des problèmes de liens morts dans l'aide surgissent :

Lors de l'installation des outils d'administration sur Windows XP, l'aide peut faire référence aux fichiers d'aide de Windows 2003 Server et ainsi générer des erreurs. Pour résoudre ce problème, il suffit de copier le fichier d'aide de Windows 2003 Server sur la station Windows XP.

1.3. Présentation et configuration des unités d'organisations

1.3.1. Présentation des unités d'organisations

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.



Les unités d'organisation permettent d'organiser de façon logique les objets de l'annuaire (ex : représentation physique des objets ou représentation logique).

Les unités d'organisation permettent aussi de faciliter la délégation de pouvoir selon l'organisation des objets.

1.3.2. Modèle hiérarchique des unités d'organisation

Afin de pouvoir utiliser les propriétés de gestion associées aux unités d'organisation, il est nécessaire de construire un modèle hiérarchique d'imbrication des unités d'organisation.

1.3.3. Dénomination des unités d'organisation

Plusieurs méthodes de dénomination permettent de pointer sur une unité d'organisation :

- **Les noms uniques** : le nom unique identifie le domaine dans lequel est situé l'objet, ainsi que son chemin d'accès complet (ex : OU=Recherche, DC=labo-microsoft, DC=lan)
- **Les noms uniques relatifs** : partie du nom unique qui permet d'identifier l'objet dans son conteneur (ex : Recherche).
- **Le nom canonique** : apportant autant d'informations que les noms uniques, il est utilisé dans certains outils d'administration (ex : labo-microsoft.lan/Recherche).

1.3.4. Création d'une unité d'organisation

Deux possibilités s'offrent à vous pour créer une unité d'organisation :

- **Interface graphique** : dans l'outil d'administration **Utilisateurs et ordinateurs Active Directory**.
- **Ligne de commande** : avec l'outil **dsadd** ou `OrganizationalUnitDomainName [-desc Description] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]`

1.4. Déplacement des objets du domaine

Dans certaines conditions, il est utile de modifier l'emplacement d'un objet (utilisateur, ordinateur, ...) d'une unité d'organisation à une autre dans le cadre d'un changement de poste par exemple.

Cette manipulation se fait dans l'outil d'administration **Utilisateurs et ordinateurs Active Directory**.

2. Gestion des comptes d'utilisateur et d'ordinateur

2.1. Création des comptes utilisateur

2.1.1. Présentation des comptes d'utilisateurs

Les Comptes d'utilisateurs permettent aux utilisateurs d'accéder aux ressources du réseau. Ils sont associés à un mot de passe et fonctionnent dans un environnement défini (machine locale ou domaine).

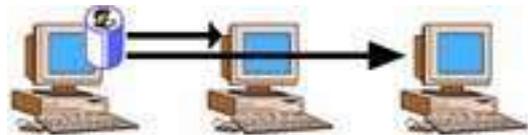
Un utilisateur disposant d'un compte de domaine pourra s'authentifier sur toutes les machines du domaine (sauf restriction explicite de l'administrateur).

Un utilisateur disposant d'un compte local ne pourra s'authentifier que sur la machine où est déclaré le compte.

Compte local : Les informations de Comptes d'utilisateurs sont stockées localement sur les machines hébergeant les ressources réseau. Si une modification doit être apportée à un compte, celle-ci devra être répercutée manuellement sur toutes les machines où le compte existe.



Compte de domaine : Les informations de comptes sont centralisées sur un serveur, dans l'annuaire des objets du réseau. Si une modification doit être apportée à un compte, elle doit être effectuée uniquement sur le serveur qui la diffusera à l'ensemble du domaine.



2.1.2. Convention de nom des comptes utilisateurs

On distingue quatre méthodes pour nommer un compte utilisateur :

- Le nom d'ouverture de session (login) : **thoboi_1**
- Le nom d'ouverture de session pré-windows : **ESI\thoboi_1**
- Le nom d'utilisateur principal : **thoboi_1@esi-supinfo.lan**
- Le nom unique LDAP : **CN=thoboi_1, CN=users, DC=esi-supinfo, DC=lan**

Un login ne peut dépasser les 20 caractères, il est sensible à la casse et ne peut pas contenir de caractères spéciaux comme : " / \ [] : ; | = , + * ? < > .

2.1.3. Nomenclature de création de compte utilisateur

Un login doit obligatoirement être unique dans son domaine. Ainsi il est nécessaire dans une grosse entreprise de créer une nomenclature de création de login prenant en compte des particularités de noms comme les membres d'une même famille travaillant dans l'entreprise par exemple.

Il peut être intéressant aussi d'identifier rapidement le login des employés temporaires (ex : T_thoboi_1).

Une fois le compte créé, il suffit de le placer dans l'unité d'organisation correspondant au département de l'utilisateur.

2.1.4. Mot de passe utilisateur

A la création d'un utilisateur, il est possible de spécifier un certain nombre de propriétés concernant la gestion des mots de passe :

- **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session** : cette option permet de définir un mot de passe temporaire lors de la création d'un compte ou de la réinitialisation du mot de passe et d'obliger ensuite l'utilisateur à le modifier.
- **L'utilisateur ne peut pas changer de mot de passe** : cette option permet de bloquer la fonctionnalité de modification de mot de passe.
- **Le mot de passe n'expire jamais** : particulièrement utile pour les comptes de service, cette option permet de s'assurer que le compte en question ne soit pas assujéti aux règles de stratégie de compte.
- **Le compte est désactivé** : Permet de désactiver un compte sans le supprimer.

2.1.5. Création de compte d'utilisateur

La création d'un utilisateur se fait via l'outil graphique d'administration **Utilisateurs et ordinateurs Active Directory** ou à l'aide de l'outil en ligne de commande **dsadd user** (**dsadd user** UserDomainName [-samid SAMName] [-upn UPN] [-fn FirstName] [-ln LastName] [-display DisplayName] [-pwd {Password*}]).

2.2. Création de comptes d'ordinateur

2.2.1. Présentation des comptes d'ordinateurs

Un compte d'ordinateur n'existe que dans un environnement de domaine, il permet d'identifier chaque ordinateur qui a accès à la base de comptes Active Directory notamment pour l'authentification des utilisateurs.

Les comptes d'ordinateur sont particulièrement utiles pour la sécurité et la gestion centralisée : ainsi on va pouvoir utiliser ces comptes pour configurer des audits, IPSec, le déploiement de logiciels, les stratégies de sécurité,....

2.2.2. Création de compte d'ordinateur

La création d'un compte d'ordinateur se fait via l'outil graphique d'administration **Utilisateurs et ordinateurs Active Directory** ou à l'aide de l'outil en ligne de commande **dsadd computer** (**dsadd computer** ComputerDomainName [-samid SAMName] [-desc Description] [-loc Location] [-memberof GroupDomainName ..] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]).

Une autre possibilité s'offre à vous pour créer un compte d'ordinateur est de le créer à partir du client lorsque celui-ci se joint au domaine. Dans ce cas, le compte d'ordinateur est créé dans le conteneur Computer.

2.3. Modification des propriétés des comptes d'utilisateur et d'ordinateur

Une fois le compte créé, il est possible d'en modifier les propriétés. La première utilité est d'en mettre à jour les informations, la seconde est d'accéder à des propriétés qui ne sont pas disponibles lors de la procédure de création de compte.

Les différentes modifications qui vont être apportées aux comptes peuvent avoir plusieurs utilités :

- **Faciliter la recherche** : le département, le bureau, ...
- **Permettre de centraliser des informations liées au compte** : le téléphone, l'email, ...

Afin de modifier ces propriétés, il vous suffit d'utiliser l'outil graphique d'administration **Utilisateurs et ordinateurs Active Directory** et d'afficher les propriétés de l'objet en double-cliquant dessus. Il est à noter que dans ce mode graphique il est possible de sélectionner plusieurs utilisateurs afin de réaliser des modifications en "masse".

Une autre solution consiste à utiliser l'outil en ligne de commande **dsmod [user | computer]** :

```
dsmod user UserDN ... [-upn UPN] [-fn FirstName] [-mi Initial] [-ln LastName] [-display DisplayName] [-empid EmployeeID] [-pwd (Password | *)] [-desc Description] [-office Office] [-tel PhoneNumber] [-email E-mailAddress] [-hometel HomePhoneNumber] [-pager PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel IPPhoneNumber] [-webpg WebPage] [-title Title] [-dept Department] [-company Company] [-mgr Manager] [-hmdir HomeDirectory] [-hmdrv DriveLetter:] [-profile ProfilePath] [-loscr ScriptPath] [-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires NumberOfDays] [-disabled {yes | no}] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

```
dsmod computer ComputerDN ... [-desc Description] [-loc Location] [-disabled {yes | no}] [-reset] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

2.4. Création de modèles de comptes utilisateur

2.4.1. Présentation d'un modèle de compte utilisateur

Un modèle de compte est un compte utilisateur générique contenant les informations communes à tous les comptes ayant le même rôle dans l'entreprise. Une fois ce modèle de compte créé (en utilisant la même procédure que n'importe quel compte utilisateur), il suffira de le dupliquer à chaque création d'un nouveau compte correspondant au rôle. Ainsi le nouveau compte créé, héritera des propriétés du modèle.

Pour des raisons de sécurité il est nécessaire de désactiver l'ensemble des modèles de compte afin qu'ils ne soient pas utilisés pour entrer dans le système. De plus il est conseillé d'identifier les modèles de compte par une lettre significative en début de nom (ex : M_<nom_du_modele>).

2.4.2. Propriétés maintenues lors de la copie du modèle de compte

Lorsqu'un modèle de compte est dupliqué, toutes les propriétés ne sont pas copiées. La liste qui suit vous informe des propriétés qui le sont :

- **Onglet Adresse** : Les informations sont copiées, à l'exception de la propriété **Adresse**.
- **Onglet Compte** : Les informations sont copiées, à l'exception de la propriété **Nom d'ouverture de session de l'utilisateur** qui est récupéré de l'assistant de duplication de compte.
- **Onglet Profil** : Les informations sont copiées, à l'exception des propriétés **Chemin du profil** et **Dossier de base** qui sont modifiées pour refléter le changement de nom d'ouverture de session.
- **Onglet Organisation** : Les informations sont copiées, à l'exception de la propriété **Titre**.

- **Membre de :** Les informations sont copiées.

2.5. Activation et désactivation d'un compte utilisateur

Chaque compte utilisateur bénéficie d'un identifiant unique interne, à Active Directory ou à la base SAM, qui permet de l'identifier. Cet identifiant appelé SID est utilisé notamment par le système de sécurité de Windows 2003.

Lorsque l'on supprime un compte et que l'on recrée ce compte, même avec des informations strictement identiques, celui-ci se voit affecter un nouveau SID. Il perd ainsi l'ensemble de son contexte de sécurité.

Afin d'éviter d'avoir à reconfigurer l'ensemble des droits et autorisations du compte utilisateur, il est conseillé de toujours désactiver les comptes utilisateur (l'utilisateur ne pourra plus l'utiliser) dans un premier temps. Après vérification, si la suppression peut se faire dans de bonnes conditions, vous pouvez la réaliser.

L'activation et la désactivation se fait via l'outil graphique d'administration **Utilisateurs et ordinateurs Active Directory** ou à l'aide de l'outil en ligne de commande **dsmod user** *UserDN* -disabled {yes|no}.

2.6. Recherche dans Active Directory

2.6.1. Recherche standard

Une fois les comptes d'utilisateurs et d'ordinateurs créés, des outils sont mis à votre disposition pour pouvoir effectuer des recherches dans l'annuaire.

Ces recherches peuvent être définies selon divers critères comme le type d'objet, les valeurs des propriétés de ces objets.

Pour lancer l'outil de recherche, il suffit de lancer l'outil de recherche graphique **Utilisateurs et Ordinateurs Active Directory**.

Vous pouvez aussi utiliser l'outil en ligne de commande **dsquery user** ou **dsquery computer** :

```
dsquery user [{StartNode | forestroot | domainroot}] [-o {dn | rdn | upn | samid}] [-scope {subtree | onelevel | base}] [-name Name] [-desc Description] [-upn UPN] [-samid SAMName] [-inactive NumberOfWeeks] [-stalepwd NumberOfDays] [-disabled] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

```
dsquery computer [{StartNode | forestroot | domainroot}] [-o {dn | rdn | samid}] [-scope {subtree | onelevel | base}] [-name Name] [-desc Description] [-samid SAMName] [-inactive NumberOfWeeks] [-stalepwd NumberOfDays] [-disabled] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

2.6.2. Recherche personnalisée

Il vous est possible aussi de réaliser des requêtes personnalisées directement en LDAP.

Pour cela, il vous suffit de sélectionner l'option **Recherche personnalisée** dans l'option **Recherche** :

2.6.3. Sauvegarde des requêtes

Un nouveau répertoire fait son apparition dans l'outil Utilisateurs et ordinateurs Active Directory. Il permet de créer, organiser et sauvegarder des requêtes LDAP. Cela permet d'effectuer les recherches courantes plus rapidement.

Une fonctionnalité d'export au format XML est aussi disponible pour chacune des requêtes sauvegardées.

3. Gestion des groupes

3.1. Présentation des groupes

Les groupes permettent de simplifier la gestion de l'accès des utilisateurs aux ressources du réseau. Les groupes permettent d'affecter en une seule action une ressource à un ensemble d'utilisateurs au lieu de répéter l'action pour chaque utilisateur. Un utilisateur peut être membre de plusieurs groupes.

Il y a deux emplacements où l'on peut trouver les groupes :

3.1.1. Groupes sur un ordinateur local

Ils permettent d'accorder des permissions uniquement au niveau de la machine. Dans le cas d'une machine non-reliée à un domaine, il est possible d'inclure uniquement les comptes locaux.

Les groupes locaux sont créés à l'aide de l'outil **Gestion de l'ordinateur**, puis dans le composant enfichable **Utilisateurs et groupes locaux**.

3.1.2. Groupes sur un contrôleur de domaine

Ils sont utilisables sur l'ensemble des machines du domaine et permettent d'avoir une gestion centralisée de la hiérarchie des groupes. Ils peuvent contenir des utilisateurs du domaine et même d'autres domaines.

Les groupes de domaine sont créés à l'aide de l'outil d'administration **Utilisateurs et ordinateurs Active Directory** et cela dans n'importe quelle unité d'organisation présente ou à l'aide de l'outil en ligne de commande **dsadd group** GroupDN -samid SAMName -secgrp yes | no -scope l | g | u.

3.1.2.1. Type de groupe

Il existe deux types de groupes dans Active Directory :

Les groupes de sécurité : permettent d'affecter des utilisateurs et des ordinateurs à des ressources. Peuvent aussi être utilisés comme groupes de distribution.

Les groupes de distribution : exploitables entre autres via un logiciel de messagerie. Ils ne permettent pas d'affecter des permissions sur des ressources aux utilisateurs.

3.1.2.2. Etendue des groupes

Les deux types de groupes dans Active Directory gèrent chacun 3 niveaux d'étendue. Leur fonctionnement va dépendre du niveau fonctionnel du domaine qui peut varier entre mixte, natif 2000 et natif 2003. Selon le mode fonctionnel, les fonctionnalités des groupes changent :

3.1.2.2.1. Les groupes globaux:

| | Mode mixte | Mode natif |
|---------------------------|--|---|
| Membres | Comptes d'utilisateurs du même domaine | Comptes d'utilisateurs et groupes globaux du même domaine |
| Membres de | Groupes locaux du même domaine | Groupes locaux de domaines |
| Etendue | Visibles dans leur domaine et dans tous les domaines approuvés | |
| Autorisations pour | Tous les domaines de la forêt | |

3.1.2.2.2. Les groupes de domaine local :

| | Mode mixte | Mode natif |
|---------------------------|---|--|
| Membres | Comptes d'utilisateurs et groupes globaux de tout domaine | Comptes d'utilisateurs, groupes globaux et groupes universels d'un domaine quelconque de la forêt, et groupes de domaine local du même domaine |
| Membres de | Membres d'aucun groupe | Groupes de domaine local du même domaine |
| Etendue | Visibles dans leur propre domaine | |
| Autorisations pour | Le domaine dans lequel le groupe de domaine local existe | |

3.1.2.2.3. Les groupes universels :

| | Mode mixte | Mode natif |
|---------------------------|---|---|
| Membres | Non utilisables | Comptes d'utilisateurs, groupes globaux et autres groupes universels d'un domaine quelconque de la forêt. |
| Membres de | Non utilisables | Groupes de domaine local et universels de tout domaine. |
| Etendue | Visibles dans tous les domaines de la forêt | |
| Autorisations pour | Tous les domaines de la forêt | |

3.1.2.3. Propriétés Géré par

La propriété gestionnaire des groupes utilisateurs permet de connaître le responsable d'un groupe. Cela permet aussi via l'option « Le gestionnaire peut mettre à jour la liste des membres » d'en modifier les membres.

3.2. Convention de nommage des groupes

Il est conseillé de toujours identifier l'étendue voir le type de groupe en ajoutant une lettre au début du nom du groupe.

Exemple :

G_ *nom* : Groupe global
 U_ *nom* : Groupe Universel
 DL_ *nom* : Groupe de domaine local

3.3. Gestion des groupes

3.3.1. Stratégie d'utilisation des groupes dans un domaine unique

La stratégie recommandée pour les groupes globaux et locaux dans un domaine unique est la suivante :

- Ajoutez les comptes d'utilisateur aux groupes globaux.
- Ajoutez les groupes globaux à un autre groupe global (dans le cas d'un environnement natif).
- Ajoutez les groupes globaux à un groupe de domaine local.
- Affectez les autorisations sur les ressources au groupe de domaine local.

 Cette stratégie est aussi appelée A G DL P.

3.3.2. Stratégie d'utilisation des groupes dans un environnement à domaines multiples

- Dans chaque domaine, ajoutez aux groupes globaux des comptes d'utilisateurs ayant la même fonction.
- Imbriguez des groupes globaux dans un seul groupe global pour intégrer les utilisateurs. Cette étape n'est utile que si vous gérez un grand nombre d'utilisateurs.
- Imbriguez des groupes globaux dans un groupe universel.
- Ajoutez les groupes universels aux groupes de domaine local pour gérer l'accès aux ressources.
- Affectez aux groupes de domaine local des autorisations appropriés sur les ressources.

 . Cette stratégie est aussi appelée A G U DL P.

3.3.3. Modification de l'étendue d'un groupe

Dans certains cas, il peut être utile de modifier l'étendue d'un groupe dans Active Directory.

Groupe global vers universel : Ceci n'est possible que si le groupe n'est pas lui-même membre d'un groupe global.

Groupe global vers domaine local : Il n'est pas possible de modifier directement un groupe global vers un groupe de domaine local. Pour réaliser cette modification, il est obligatoire de modifier le groupe global en groupe universel, puis en groupe de domaine local.

Groupe de domaine local vers universel : Ceci n'est possible que si le groupe n'est pas lui-même membre d'un groupe de domaine local.

Groupe universel vers global : Ceci n'est possible que si le groupe n'est pas lui-même membre d'un groupe universel.

Groupe universel vers domaine local : Aucune limitation n'existe dans ce cas.

3.4. Groupes par défaut

Les groupes par défaut possèdent des droits et des autorisations prédéfinis qui permettent de faciliter la mise en place d'un environnement sécurisé. Ainsi un certain nombre de rôles courants sont directement applicables en rendant membre du groupe par défaut adéquat l'utilisateur à qui l'on souhaite donner des droits ou autorisations.

Ces groupes et les droits qui leurs sont associés sont créés automatiquement.

3.4.1. Groupes par défaut sur un serveur membre

Les groupes par défaut sur un serveur membre sont stockés dans la base de compte locale de la machine et sont visibles via le composant enfichable **Utilisateurs et groupes locaux** de la console d'administration Gestion de l'ordinateur. Ils sont créés automatiquement lors de l'installation de Windows 2003.

Voici les rôles et les propriétés de certains d'entre eux :

| | |
|------------------------|--|
| Administrateurs | Pleins pouvoirs sur le serveur. Lorsqu'un serveur est ajouté au domaine, le groupe Admins. du domaine est ajouté à ce groupe. |
| Invités | Un profil temporaire est créé pour l'utilisateur que l'on place dans ce groupe. |

| | |
|----------------------------------|--|
| Utilisateurs avec pouvoir | Peut créer des comptes utilisateurs et les gérer. Peut créer des groupes locaux et les gérer. Peut créer des ressources partagées. |
| Utilisateurs | Peut lancer des applications, utiliser les imprimantes. |
| Opérateurs d'impression | Peut gérer les imprimantes et les files d'attente |

Certains groupes par défaut ne sont disponibles que lorsqu'un service précis est installé comme les services DHCP et WINS qui installent les groupes par défaut **Administrateurs DHCP**, **Utilisateurs DHCP**, **Utilisateurs WINS**.

3.4.2. Groupes par défaut dans Active Directory

Les groupes par défaut dans Active Directory sont stockés dans la base Active Directory et sont visibles via la console d'administration Utilisateurs et ordinateurs Active Directory dans les conteneurs **Builtin** et **Users**. Ils sont créés automatiquement lors de l'installation d'Active Directory.

Voici les rôles et les propriétés de certains d'entre eux :

| | |
|--|--|
| Opérateurs de compte | Les membres de ce groupe peuvent gérer les comptes utilisateurs. |
| Opérateurs de serveur | Les membres de ce groupe peuvent administrer les serveurs du domaine. |
| Contrôleurs de domaine | Ce groupe contient tous les comptes d'ordinateurs des contrôleurs de domaine. |
| Invités du domaine | Les membres de ce groupe vont bénéficier d'un profil temporaire. |
| Utilisateurs du domaine | Contient tout les utilisateurs du domaine. Tous les utilisateurs créés du domaine sont membre de ce groupe |
| Ordinateurs du domaine | Ce groupe contient tous les ordinateurs du domaine |
| Administrateurs du domaine | Ce groupe contient les utilisateurs administrateurs du domaine. |
| Administrateurs de l'entreprise | Ce groupe contient les administrateurs de l'entreprise. Permet de créer les relations d'approbations entre domaines. |
| Administrateurs du schéma | Ce groupe contient les utilisateurs capables de faire des modifications sur le schéma Active Directory. |

3.5. Groupes système

Les groupes systèmes sont des groupes dont les membres sont auto-gérés par le système. Ces groupes sont particulièrement utiles dans le cas d'affectations d'autorisations.

| | |
|----------------------------------|---|
| Anonymous Logon | Représente les utilisateurs qui ne se sont pas authentifiés. |
| Tout le monde | Tous les utilisateurs se retrouvent automatiquement dans ce groupe. |
| Réseau | Regroupe les utilisateurs connectés via le réseau. |
| Utilisateurs authentifiés | Regroupe les utilisateurs authentifiés. |
| Créateur propriétaire | Représente l'utilisateur qui est propriétaire de l'objet. |

4. Gestion d'accès aux ressources

4.1. Contrôle d'accès

Le système de contrôle d'accès dans Windows 2003 est basé sur trois composants qui permettent la définition du contexte de sécurité des éléments du système.

Ces trois éléments sont :

- **Les entités de sécurité**
- **Le SID**
- **DACL – Discretionary Access Control List**

4.1.1. Les entités de sécurité

Les entités de sécurité peuvent être un compte utilisateur, d'ordinateur ou un groupe. Ils permettent d'affecter l'accès à un objet en le représentant dans le système informatique.

4.1.2. Le SID

Toutes les entités de sécurité sont identifiées dans le système par un numéro unique appelé SID.

Ce SID est lié à la vie de l'objet, ainsi si l'on supprime un groupe et qu'on le recrée ce même groupe juste après (même nom, mêmes propriétés), celui-ci se verra attribuer un nouveau SID.

L'ensemble des définitions de sécurité étant basé sur ce SID, les accès donnés au groupe supprimé ne seront pas transférés au nouveau groupe.

4.1.3. DACL - Discretionary Access Control List

Les DACL sont associées à chaque objet sur lequel on va définir un contrôle d'accès.

Les DACL sont composées d'ACE (Access Control Entry) qui définissent les accès à l'objet.

Les ACE se composent de la façon suivante :

- Le SID de l'entité à qui l'on va donner ou refuser un accès.
- Les informations sur l'accès (ex : Lecture, Ecriture, ...)
- Les informations d'héritage.
- L'indicateur de type d'ACE (Autoriser ou refuser).

A chaque tentative d'accès à une ressource, cette liste sera parcourue afin de déterminer si l'action voulue peut être réalisée.

4.2. Autorisations

4.2.1. Autorisations standards

Les autorisations permettent de fixer le niveau d'accès qu'ont les entités de sécurité (pour un compte utilisateur, groupe d'utilisateurs ou ordinateur) sur une ressource.

Les ressources utilisant ce système d'autorisations pour réguler leurs accès sont multiples (Registre, Fichiers, Imprimantes, Active Directory, ...)

4.2.2. Autorisations spéciales

Les autorisations standards sont limitées aux actions de base sur un objet (ex : Lecture, Modifier, Contrôle Total, ...). Aussi pour pouvoir granuler de façon plus précise les autorisations, vous avez accès via le bouton « Avancé » à une liste étendue d'autorisations.

4.3. Administration des accès aux dossiers partagés

4.3.1. Description des dossiers partagés

Le partage d'un dossier permet de rendre disponible l'ensemble de son contenu via le réseau.

Par défaut, lors de la création d'un partage, le groupe « Tout le monde » bénéficie de l'autorisation « Lecture ».

Il est possible de cacher le partage d'un dossier en ajoutant le caractère « \$ » à la fin du nom. Pour pouvoir y accéder, il sera obligatoire de spécifier le chemin UNC complet ([\\nom du serveur\nom du partage\\$](#)).

4.3.2. Partages administratifs

Windows 2003 crée automatiquement des partages administratifs. Les noms de ces partages se terminent avec un caractère \$ qui permet de cacher le partage lors de l'exploration par le réseau. Le dossier système (Admin\$), la localisation des pilotes d'impression (Print\$) ainsi que la racine de chaque volume (c\$, d\$, ...) constituent autant de partages administratifs.

Seuls les membres du groupe « Administrateurs » peuvent accéder à ces partages en accès Contrôle Total.

Le partage IPC\$ permet l'affichage des ressources partagées (dossiers partagés, imprimantes partagées).

4.3.3. Création de dossiers partagés

Sur des machines Windows 2003 Server en mode autonome ou serveur membre, seuls les membres des groupes « Administrateurs » et « Utilisateurs avec pouvoirs » peuvent créer des dossiers partagés.

Sur des machines contrôleurs de domaine Windows 2003 Server, seuls les membres des groupes « Administrateurs » et « Opérateurs de serveurs » peuvent créer des dossiers partagés.

Pour pouvoir créer un partage vous avez trois possibilités :

- L'outil d'administration Gestion de l'ordinateur à l'aide du composant logiciel enfichable « Dossiers partagés ».
- L'explorateur par le biais du menu contextuel de tous les dossiers de l'arborescence.
- La commande NET SHARE (net share NomDossierPartagé=Unité:Chemin).

4.3.4. Publication des dossiers partagés

Grâce à Active Directory, il est possible aux utilisateurs de retrouver un partage du domaine en faisant une recherche sur des mots clés.

Pour mettre en place cette fonctionnalité, il suffit de créer un objet « Dossier partagé » à l'aide de la console « Utilisateurs et ordinateurs Active Directory » et de spécifier lors de sa création, le chemin UNC

permettant d'accéder physiquement à ce partage (l'objet Active Directory n'étant qu'un raccourci vers la ressource physique).

Il est aussi possible d'automatiser cette tâche en cochant l'option « Publier ce partage dans Active Directory » à l'aide de l'outil d'administration « Gestion de l'ordinateur » et du composant enfichable « Dossiers Partagés » directement sur le serveur qui héberge la ressource.

Suite à la publication, rien ne vous empêche si le serveur hébergeant le partage de fichier tombe en panne de modifier le raccourci de l'objet Active Directory pour le faire pointer vers un nouveau serveur accueillant le partage temporairement. Les utilisateurs ne perdent donc pas la trace de leurs ressources.

4.3.5. Autorisations sur les dossiers partagés

Chaque dossier partagé peut être protégé par une ACL qui va restreindre son accès spécifiquement aux utilisateurs, groupes ou ordinateurs qui y accèdent via le réseau.

Il existe trois niveaux d'autorisations affectables :

- Lecture : Permet d'afficher les données et d'exécuter les logiciels.
- Modifier : Comprend toutes les propriétés de l'autorisation lecture avec la possibilité de créer des fichiers et dossiers, modifier leurs contenus et supprimer leurs contenus.
- Contrôle total : Comprend toutes les propriétés de l'autorisation Modifier avec la possibilité de modifier aux travers le réseau les autorisations NTFS des fichiers et dossiers.

Les trois niveaux d'autorisations sont disponibles en « Autoriser » ou en « Refuser » en sachant que les autorisations de refus sont prioritaires.

Pour affecter des autorisations de partage, vous avez deux solutions :

- A l'aide de l'outil d'administration « Gestion de l'ordinateur » et du composant enfichable « Dossiers Partagés ».
- A l'aide de l'explorateur dans les propriétés du dossier partagé.

4.3.6. Connexion à un dossier partagé

Afin qu'un client puisse accéder à un dossier partagé, plusieurs moyens sont disponibles :

- Favoris réseau : Permet de créer des raccourcis vers les partages désirés.
- Lecteur réseau : Permet d'ajouter le dossier partagé directement dans le poste de travail en lui attribuant une lettre.
- Exécuter : Permet d'accéder ponctuellement à la ressource en spécifiant simplement le chemin UNC d'accès à la ressource.

4.4. Administration des accès aux fichiers et dossiers NTFS

4.4.1. Présentation de NTFS

NTFS est un système de fichiers qui offre les avantages suivants :

- Fiabilité : NTFS est un système de fichiers journalisé. En cas de problème, ce journal sera utilisé pour analyser les parties du disque qui ont posé problème (cela évite le scandisk de l'intégralité du disque que l'on avait sous Windows 98).

- **Sécurité** : Le système NTFS prend en charge le cryptage de fichiers avec EFS. EFS permet d'éviter des problèmes comme l'espionnage industriel en empêchant l'exploitation des données même si le disque dur est volé. NTFS permet aussi l'utilisation d'autorisations NTFS qui permettent de restreindre l'accès aux données de la partition.
- **Gestion du stockage** : NTFS permet la compression de données transparente pour tous les fichiers stockés sur la partition. Il permet aussi l'implémentation de la gestion de quotas pour restreindre de façon logique l'espace dont peut bénéficier un utilisateur sur une partition.

L'utilisation de systèmes de fichiers comme FAT et FAT32 est recommandée uniquement pour faire du dual boot entre des systèmes Windows 2003 et d'autres systèmes d'exploitation tels que DOS 6.22, Win 3.1 ou Win 95/98.

Utilisez *convert.exe* pour convertir les partitions FAT ou FAT32 vers NTFS. Les partitions NTFS ne peuvent pas être converties vers FAT ou FAT32, la partition doit alors être effacée et recréée en tant que FAT ou FAT32.

4.4.2. Autorisations sur les fichiers et dossiers NTFS

Les autorisations NTFS permettent de définir les actions que vont pouvoir effectuer les utilisateurs, groupes ou ordinateurs sur les fichiers.

4.4.2.1. Autorisations sur les fichiers

- **Contrôle total** : Dispose de toutes les autorisations de Modification avec la prise de possession et la possibilité de modifier les autorisations du fichier.
- **Modification** : Permet de modifier, supprimer, lire et écrire les fichiers.
- **Lecture et exécutions** : Permet de lire les fichiers et d'exécuter les applications.
- **Ecriture** : Permet d'écraser le fichier, de changer ses attributs et d'afficher le propriétaire.
- **Lecture** : Permet de lire le fichier, d'afficher ses attributs, son propriétaire et ses autorisations.

4.4.2.2. Autorisations sur les dossiers

- **Contrôle total** : Dispose de toutes les autorisations de « Modification » avec la prise de possession et la possibilité de modifier les autorisations du dossier.
- **Modification** : Dispose de toutes les autorisations de « Ecriture » avec la possibilité de supprimer le dossier.
- **Lecture et exécutions** : Permet d'afficher le contenu du dossier et d'exécuter les applications.
- **Ecriture** : Permet de créer des fichiers et sous-dossiers, de modifier ses attributs et d'afficher le propriétaire.
- **Lecture** : Affiche les fichiers, sous-dossiers, attributs de dossier, propriétaire et autorisations du dossier.
- **Affichage du contenu des dossiers** : Affichage seul du contenu direct du dossier.

4.4.3. Impact de la copie et du déplacement sur les autorisations NTFS

Toutes les opérations de copie héritent des autorisations du dossier cible. Seul le déplacement vers la même partition permet le maintien des autorisations.

Les fichiers déplacés depuis une partition NTFS vers une partition FAT perdent leurs attributs et leurs descripteurs de sécurité.

Les attributs de fichiers pendant la copie/déplacement d'un fichier à l'intérieur d'une partition ou entre deux partitions sont gérés ainsi:

- Copier à l'intérieur d'une partition : Crée un nouveau fichier identique au fichier original. Il hérite des permissions du répertoire de destination.
- Déplacer à l'intérieur d'une partition : Ne crée pas un nouveau fichier. Il y a seulement une mise à jour des pointeurs du dossier. Garde les permissions 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 permissions du répertoire de destination.

4.4.4. Présentation de l'héritage NTFS

Sur le système de fichiers NTFS de Windows 2003, les autorisations que vous accordez à un dossier parent sont héritées et propagées à tous les sous-dossiers, et les fichiers qu'il contient. Tous les nouveaux fichiers et dossiers créés dans ce dossier hériteront aussi de ces permissions.

Par défaut, toutes les autorisations NTFS d'un dossier créé seront héritées par les dossiers et fichiers qu'il contiendra.

Il est possible de bloquer cet héritage (pour des raisons de sécurité) afin que les permissions ne soient pas propagées aux dossiers et aux fichiers contenus dans le dossier parent.

Pour bloquer l'héritage des permissions, afficher les propriétés du dossier, allez dans l'onglet Sécurité, puis cliquez sur le bouton « Paramètres avancés » désactiver la case à cocher « Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants. Cela inclut les objets dont les entrées sont spécifiquement définies ici. ».

Dans la nouvelle fenêtre, cliquez sur *Copier* si vous souhaitez garder les autorisations précédemment héritées sur cet objet, ou alors cliquez sur *Supprimer* afin de supprimer les autorisations héritées et ne conserver que les autorisations explicitement spécifiées.

4.4.5. Identification des autorisations effectives

Lorsque vous accordez des autorisations à un utilisateur, à un groupe ou à un utilisateur, il est parfois difficile de s'y retrouver avec par exemple les groupes auxquels un utilisateur peut appartenir et les autorisations héritées.

Lorsque l'on définit des autorisations, il est possible qu'un même utilisateur obtienne plusieurs autorisations différentes car il est membre de différents groupes.

Dans ce cas, les autorisations se cumulent et il en résulte l'autorisation la plus forte (ex : lecture + contrôle total → contrôle total).

Lorsqu'un utilisateur ne se trouve pas dans la DACL de l'objet, il n'a aucune autorisation dessus. C'est une autorisation « Refuser » implicite.

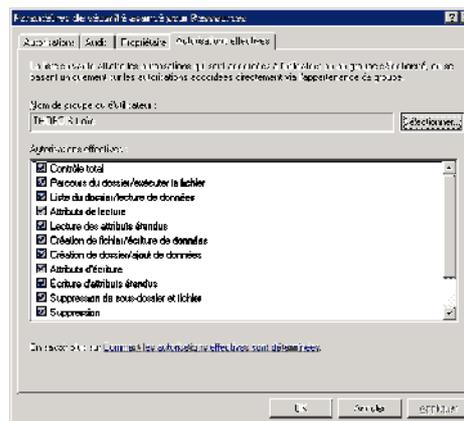
Les autorisations sur les fichiers sont prioritaires aux autorisations sur les dossiers.

Les autorisations « Refuser » sont prioritaires sur les autres autorisations et ceci dans TOUS les cas (ex : contrôle total + refuser lecture → La lecture sera bien refusée).

Le propriétaire a la possibilité d'affecter les autorisations qu'il désire sur tous les fichiers dont il est le propriétaire même si il n'a pas d'autorisations contrôle total dessus.

☞ Un administrateur qui doit modifier les autorisations sur un fichier NTFS doit tout d'abord se l'approprier.

Il est possible de vérifier les permissions effectives d'un utilisateur à l'aide de l'onglet Autorisations effectives de la fenêtre de paramètres de sécurité avancé.



4.4.6. Cumul des autorisations NTFS et des autorisations de partage

Lorsqu'un utilisateur est sujet aussi bien aux autorisations NTFS qu'aux autorisations de partage, ses permissions effectives s'obtiennent en combinant le niveau maximum d'autorisations indépendamment pour les autorisations NTFS et pour les autorisations de partage (ex : Lecture pour les autorisations de partage et modification pour les autorisations NTFS).

Une fois les deux autorisations définies, il suffit de prendre la plus restrictive des deux.

Exemple :

Partage – lecture + NTFS – contrôle total → lecture
et inversement

Partage – contrôle total + NTFS – lecture → lecture

4.5. Mise en place des fichiers hors connexion

4.5.1. Présentation des fichiers hors connexion

Les fichiers Hors Connexion remplacent le Porte-Documents et fonctionnent de manière similaire à l'option « Visualiser Hors-Connexion » d'Internet Explorer. Ainsi il est possible pour les utilisateurs itinérants de continuer à accéder à leurs ressources réseau alors qu'ils sont déconnectés de celui-ci.

Pour activer la fonction de mise hors-connexion côté serveur, il suffit de partager un dossier et d'activer son cache afin de le rendre disponible hors connexion. Trois modes de mise en cache sont alors disponibles :

- **Cache manuel pour les documents** : réglage par défaut. Les utilisateurs doivent spécifier quels documents ils souhaitent rendre disponibles hors connexion.

- **Cache automatique pour les documents** : tous les fichiers ouverts par un utilisateur sont mis en cache sur son disque dur pour une utilisation hors connexion – les versions anciennes du document sur le disque sont automatiquement remplacées par des versions plus récentes du partage quand elles existent.

- **Cache automatique pour les programmes** : cette mise en cache est unidirectionnelle et ne concerne que les fichiers dont les modifications des utilisateurs doivent être ignorées (ex : tarifs, applications, ...). Elle permet notamment un gain de performance car les fichiers sont alors consultés en local et non pas sur le réseau. Elle est activée via l'option « Optimisé pour les performances ».

☞ La mise en cache peut être aussi activée par la commande NET SHARE et le commutateur /cache.

L'utilitaire de Synchronisation, vous permet de spécifier les fichiers qui seront synchronisés, le type de connexion employée pour cette synchronisation (pour empêcher par exemple une synchronisation lorsque l'on est connecté au réseau à distance via un modem) et le moment où cette synchronisation est effectuée (lors d'une connexion, d'une déconnexion, lorsque l'ordinateur est en veille,...).

Lorsque vous synchronisez, si vous avez édité un fichier hors connexion et qu'un autre utilisateur a fait de même, alors, il vous sera demandé si vous souhaitez :

Garder et renommer votre exemplaire

Écraser votre exemplaire avec la version disponible sur le réseau

Écraser la version disponible sur le réseau et perdre les modifications de l'autre utilisateur

5. Implémentation de l'impression

5.1. Présentation de l'impression dans la famille Windows Server 2003

5.1.1. Terminologie de l'impression

- Pilote d'impression : Logiciel permettant d'implémenter sur l'ordinateur le langage de communication de l'imprimante.
- Tâche d'impression : Tout document qui est envoyé pour être imprimé.
- Serveur d'impression : Ordinateur centralisant les tâches d'impression et gérant la file d'attente d'impression. Il contient le pilote d'imprimante propre à chacun des périphériques d'impression connectés. Ce pilote est disponible dans la version de chacun des clients qui vont utiliser le serveur pour demander des travaux d'impression (Windows 95, 98, NT, 2000, 2003, ...).
- Imprimante : C'est l'interface logicielle qu'il y a entre le périphérique d'impression et Windows. Concrètement, le file d'attente du périphérique d'impression (à ne pas confondre avec votre Epson ou votre Canon).
- Spouleur d'impression : Le spouleur d'impression est chargé de recevoir, stocker et d'envoyer vers le bon périphérique d'impression, les tâches d'impression.
- File d'attente d'impression : C'est l'ensemble des tâches d'impression dans leurs ordre d'arrivée.
- Port Imprimante : Interface logique de communication avec le périphérique d'impression.
- Périphérique d'impression : C'est le périphérique physique réalisant les tâches d'impression (c'est votre Epson, votre Canon, ...).

5.1.2. Types de clients d'impression supportés par Windows 2003

5.1.2.1. Clients Microsoft

Les clients 32 bits & 64 bits Microsoft (à partir de Windows 95), sont capables de télécharger les pilotes d'impressions directement à partir du serveur d'impression. Ceci se fait à l'aide du partage administratif print\$.

Pour les clients 16 bits Microsoft (famille MS-DOS), l'installation des pilotes est manuelle sur chaque poste client en ayant pris soin de télécharger les bonnes versions de pilotes.

5.1.2.2. Clients NetWare

Pour supporter les clients NetWare, il est obligatoire d'avoir installé les services de fichiers et d'impression pour NetWare. Le protocole IPX/SPX peut lui aussi être nécessaire sur les clients et le serveur si les clients n'implémentent pas TCP/IP (protocole réseau utilisé par Microsoft).

5.1.2.3. Clients Macintosh

Les clients Macintosh nécessitent l'installation des services d'impression Microsoft pour Macintosh. Le protocole Appletalk est lui aussi nécessaire pour la communication avec les clients Macintosh.

5.1.2.4. Clients UNIX

Les clients UNIX nécessitent l'installation des services d'impression Microsoft pour UNIX. Les clients se connectent au serveur LPD en suivant les spécifications LPR.

5.1.2.5. Clients IPP (Internet Printing Protocol)

Le support des clients IPP est assuré sous Windows 2003 à la suite de l'installation de IIS (Internet Information Services) ou de PWS (Personal Web Server).

5.1.3. Fonctionnement de l'impression

Il existe deux méthodes dans un environnement Windows 2003 d'imprimer :

5.1.3.1. Impression sans serveur d'impression

Dans ce cas, les différents clients se connectent directement à l'imprimante réseau (cette imprimante doit être équipée d'une carte réseau intégrée).

Inconvénients de cette méthode:

- Chacun des clients hébergent sa propre file d'attente, impossible de connaître sa position par rapport aux autres clients.
- Les messages d'erreur sont retournés uniquement vers le client dont la tâche d'impression est en cours.
- Le spouling est réalisé sur le client et non pas sur le serveur ce qui engendre une charge de travail supplémentaire sur le client.

5.1.3.2. Impression avec serveur d'impression

Dans ce cas, les différents clients se connectent via un serveur d'impression qui peut être lui-même connecté à une imprimante réseau ou directement relié au périphérique d'impression.

Avantages de cette méthode:

- Le serveur gère la distribution des pilotes aux clients.
- La file d'attente est unique pour tous les clients qui peuvent donc voir de façon effective leur position dans la file d'attente.
- Les messages d'erreur sont retournés sur tous les clients dont la tâche d'impression est en cours.
- Certains traitements sont transmis et réalisés directement par le serveur d'impression.

5.2. Installation et partage d'imprimantes

5.2.1. Imprimantes locales et imprimantes réseau

Une imprimante locale est une imprimante qui va être directement reliée au serveur d'impression par un câble de type USB, parallèle (LPT) ou Infrarouge (IR).

Une imprimante réseau est une imprimante qui va être reliée au serveur d'impression via l'infrastructure réseau et la mise en place d'un protocole réseau comme TCP/IP, IPX/SPX ou AppleTalk.

5.2.2. Installation et partage d'une imprimante

Vous devez avoir les privilèges d'Administrateur afin d'ajouter une imprimante à votre serveur. L'assistant d'Ajout d'imprimante vous guide pendant tout le processus qui vous permettra de définir quel périphérique d'impression est disponible, sur quel port physique le périphérique d'impression est branché, quel pilote utiliser, ainsi que le nom du périphérique d'impression sous lequel il sera connu sur le réseau.

Dans le cas d'une imprimante réseau, il est nécessaire de créer un port TCP/IP avec l'adresse IP de l'imprimante réseau.

Le partage d'une imprimante se fait dans les mêmes conditions que l'ajout d'une imprimante, c'est à dire qu'il faut être Administrateur. Un clic droit sur l'imprimante, puis Propriétés, là il faut choisir l'onglet Partage. Choisir le nom de partage de l'imprimante sur le réseau, et ensuite ajouter tous les pilotes nécessaires aux clients qui vont utiliser cette imprimante (en cliquant sur 'Pilotes supplémentaires').

Le partage d'une imprimante sur un serveur membre publie l'imprimante automatiquement dans Active Directory. Pour annuler cette publication, décocher l'option « Lister dans l'annuaire ».

5.3. Autorisations d'imprimantes partagées

Il existe trois niveaux d'autorisations pour définir les accès d'une imprimante partagée :

- Impression : L'utilisateur peut imprimer des documents.
- Gestion des documents : L'utilisateur ne peut pas imprimer mais il peut gérer complètement la file d'attente de l'impression.
- Gestion d'imprimantes : Permet de modifier les autorisations de l'imprimante, de gérer la file d'attente et d'imprimer.

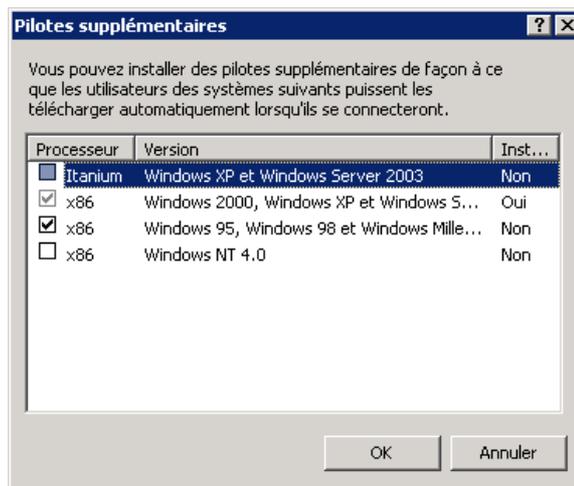
Le principe de gestion de cette ACL est identique à la gestion des ACL du système de fichiers NTFS.

5.4. Gestion des pilotes d'imprimantes

Windows 2003 Server offre le téléchargement automatique des pilotes pour les clients qui tournent sous Windows 2003, Windows XP, Windows 2000, Windows NT 4, Windows NT 3.51 et Windows 95/98.

La plate-forme Itanium est même supportée avec Windows XP et Windows 2003.

Cela est transmis au client via le partage administratif admin\$ sur le serveur d'impression.



6. Administration de l'impression

6.1. Changement de l'emplacement du spouleur d'impression

Le spouleur d'impression est un exécutable prenant en charge la gestion de l'impression.

Il effectue notamment les tâches suivantes :

- Gestion de l'emplacement des pilotes imprimantes.
- Récupération des documents, stockage et envoi à l'imprimante.
- Planification du travail d'impression.

Par défaut, le spouleur d'impression se trouve dans le répertoire système à l'emplacement %SystemRoot%\System32\Spool\Printers.

Il peut être nécessaire de changer son emplacement pour des questions de performances ou d'espace disque.

En effet, l'accès aux fichiers système et au répertoire du spouleur simultanément réduit les performances du serveur car la tête de lecture du disque va faire des allers-retours incessants.

De plus, des problèmes de fragmentation de fichiers pourraient apparaître sur le disque au vu des écritures multiples.

Le déplacement du fichier du spouleur est aussi utile dans le simple cas de la saturation du disque dur qui le contient.

Il est aussi intéressant de pouvoir définir des quotas (en terme de taille de fichier et non en terme de nombre d'impressions) en utilisant la fonctionnalité de quotas du système de fichiers NTFS. Pour cela il est indispensable d'isoler les fichiers du spouleur sur un volume dédié.

Pour finir, une simple implémentation d'un système de disques durs à tolérance de pannes incite à déplacer les fichiers du spouleur.

En prenant en compte l'ensemble de ces considérations, il est conseillé de déplacer les fichiers du spouleur sur un disque dédié possédant son propre contrôleur de disques.

Une fois la décision prise, il suffit d'aller dans le panneau de configuration « Imprimantes et télécopieurs », puis dans le menu fichier et de cliquer sur « Propriétés de Serveur d'impression ».

Ensuite dans « Avancé », de modifier le champ « Dossier du spouleur ».

Une fois la modification effectuée, il vous suffit de redémarrer le spouleur (NET STOP SPOOLER et NET START SPOOLER).

 Il est recommandé que les travaux d'impression en cours soient finis avant de déplacer les fichiers du spouleur.

6.2. Définition des priorités d'imprimantes

Les priorités d'impression sont fixées en créant plusieurs imprimantes logiques qui pointent vers le même périphérique d'impression et en leur assignant individuellement des priorités.

L'échelle des priorités va de 1 (la plus faible, par défaut) à 99, la plus forte. Il faut ensuite limiter via l'onglet sécurité l'utilisation de chacune des imprimantes aux bons utilisateurs.

Pour mettre en place les priorités d'une imprimante, il suffit de se rendre dans l'onglet Avancé, puis de remplir la zone 'Priorité' avec la valeur voulue.

☞ Les priorités ne sont prises en compte qu'au niveau de la file d'attente, donc si un long travail d'impression est en cours, même l'arrivée d'un travail prioritaire n'arrêtera pas le travail en cours.

6.3. Planification de la disponibilité des imprimantes

Afin de pouvoir relayer un certain nombre d'impressions à des plages horaires précises (des gros travaux d'impression que l'on souhaite réaliser la nuit), il est possible de spécifier dans les propriétés de l'imprimante une plage horaire de disponibilité qui permettra à tous les documents envoyés à cette imprimante (et ce, quelque soit le moment de la journée) de pouvoir être réalisés uniquement pendant la plage horaire de disponibilité de l'imprimante.

Il est conseillé lors de la mise en place de la planification de la disponibilité de l'imprimante de créer deux imprimantes pointant vers le même périphérique d'impression et de restreindre l'accès de cette imprimante à l'aide de l'onglet sécurité.

6.4. Configuration d'un pool d'impression

Si vous avez de grosses charges d'impression, vous pouvez utiliser un ou plusieurs périphériques d'impression identiques pour ne faire qu'une imprimante logique. C'est le Print Pooling (Pool d'impression). Le pool d'impression ne comporte pas nécessairement que des périphériques d'impression locaux, il peut aussi comporter des périphériques d'impression munis de carte (interface) réseau.

Quand un travail d'impression sera réceptionné par le serveur, alors, il sera envoyé au premier périphérique d'impression qui sera disponible.

Pour créer un pool d'impression, il faut se rendre dans l'onglet « Port », puis cliquer sur la case « Activer le pool d'imprimante » et il ne reste plus qu'à choisir sur quels ports sont connectés les périphériques d'impression.

7. Gestion d'accès aux objets dans les unités d'organisation

7.1. Structure des unités d'organisation

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine.

Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.



Les unités d'organisation permettent d'organiser de façon logique les objets de l'annuaire Active Directory. Elles permettent, un peu à la manière des dossiers de disques durs, d'ordonner les objets sous une représentation physique (emplacements des utilisateurs ou des ordinateurs) des objets ou représentation logique (départements d'appartenance des utilisateurs ou des ordinateurs).

 Il est fortement déconseillé de dépasser les 5 niveaux d'imbrication d'unités d'organisation.

Les unités d'organisation facilitent la délégation d'administration selon l'organisation des objets.

Les unités d'organisation permettent aussi de déployer les stratégies de groupes efficacement et de manière ciblée. De plus, la hiérarchie créée à l'aide des unités d'organisation va permettre un système d'héritage pour les stratégies de groupes.

7.2. Modification des autorisations sur les objets Active Directory

7.2.1. Autorisations sur les objets Active Directory

Les autorisations Active Directory permettent de restreindre l'accès des utilisateurs au contenu de l'annuaire à savoir les objets ou leurs propriétés.

Tout comme les autorisations NTFS, des autorisations standards et spéciales sont disponibles aussi bien en « Accepter » qu'en « Refuser ».

Lorsqu'un utilisateur ne se trouve pas dans la DACL de l'objet, il n'a aucune autorisation dessus. C'est une autorisation « Refuser » implicite.

Les autorisations peuvent être définies sur les objets ou sur les unités d'organisation qui bénéficient de la propriété d'héritage pour transmettre ces autorisations aux objets enfants. Cette fonctionnalité peut être bloquée si nécessaire.

Dans tous les cas, les objets déplacés héritent des autorisations de l'unité d'organisation de destination.

Pour pouvoir visualiser les fonctions de modification des autorisations sur les objets Active Directory, dans l'outil « Utilisateurs et ordinateurs Active Directory », cochez l'option « Fonctionnalités avancées » dans le menu « Affichage ». Il suffit ensuite d'afficher les propriétés de l'objet ou de l'unité d'organisation.

7.2.2. Définitions des autorisations effectives

Lorsque vous accordez des autorisations à un utilisateur, ou à un groupe, il est parfois difficile de s'y retrouver au milieu des autorisations de groupe et des héritages.

Lorsque l'on définit des autorisations, il est possible qu'un même utilisateur obtienne plusieurs autorisations différentes car il est membre de différents groupes.

Dans ce cas, les autorisations se cumulent et il en résulte l'autorisation la plus forte (ex : lecture + contrôle total → contrôle total).

Les autorisations « Refuser » sont prioritaires sur les autres autorisations et ceci dans TOUS les cas (ex : contrôle total + refuser lecture → La lecture sera bien refusée).

Lorsqu'un utilisateur ne se trouve pas dans la DACL de l'objet, il n'a aucune autorisation dessus. C'est une autorisation « Refuser » implicite.

Le propriétaire a la possibilité d'affecter les autorisations qu'il désire sur tous les fichiers dont il est le propriétaire même si il n'a pas d'autorisation contrôle total dessus.

7.3. Délégation du contrôle des unités d'organisation

Il est possible de déléguer un certain niveau d'administration d'objets Active Directory à n'importe quel utilisateur, groupe ou unité organisationnelle.

Ainsi, vous pourrez par exemple déléguer certains droits administratifs d'une unité organisationnelle Ventes à un utilisateur de cette UO.

L'un des principaux avantages qu'offre cette fonctionnalité de délégation de contrôle est qu'il n'est plus nécessaire d'attribuer des droits d'administration étendus à un utilisateur lorsqu'il celui-ci doit effectuer un certain nombre de tâches d'administration.

Ainsi, sous NT4, si l'on souhaitait qu'un utilisateur dans un domaine gère les comptes d'utilisateurs pour son groupe, il fallait le mettre dans le groupe des Opérateurs de comptes, ce qui lui permettait de gérer tous les comptes du domaine.

Avec Active Directory, il suffira de faire un clic-droit sur l'UO pour laquelle on souhaite lui déléguer cette tâche et de sélectionner « Déléguer le contrôle ». On pourra définir quelques paramètres comme les comptes concernés par cette délégation et le type de délégation, dans notre cas, « Créer, supprimer et gérer des comptes d'utilisateur » (On peut affiner en déléguant des tâches personnalisées comme par exemple uniquement le droit de réinitialiser les mots de passe sur l'UO ou un objet spécifique de l'UO, ...).

8. Implémentation des stratégies de groupes

8.1. Description des stratégies de groupes

8.1.1. Présentation des stratégies de groupes

Une Stratégie de Groupe est une collection de variables de configuration d'environnement de l'utilisateur et de l'ordinateur qui est imposée par le système d'exploitation et non modifiable par l'utilisateur.

Une stratégie de groupe peut s'appliquer à un **site**, un **domaine** ou à une **unité d'organisation** et peut être assignée plusieurs fois simultanément sur différents conteneurs.

Les stratégies de groupes sont aussi appelées GPO pour Group Policy Object.

8.1.2. Description des paramètres de configuration des utilisateurs et des ordinateurs

La console de gestion des stratégies de groupes se divise en deux arborescences : Ordinateur et Utilisateur :

- Les paramètres de stratégies de groupes pour les **ordinateurs** définissent le comportement du système d'exploitation, d'une partie du bureau et la configuration de la sécurité.
- Les paramètres de stratégies de groupes pour les **utilisateurs** définissent les options d'applications affectées et publiées, la configuration des applications et les paramètres du bureau.

8.2. Implémentation d'objets de stratégie de groupe

8.2.1. Les outils permettant d'implémenter les GPO

Les différents outils permettant d'éditer les stratégies de groupes sont les suivants :

- Utilisateurs et ordinateurs Active Directory : Permet d'éditer les stratégies associées au domaine et aux unités d'organisation.
- Sites et services Active Directory : Permet d'éditer les stratégies associées aux sites.
- Stratégie de sécurité locale : Permet d'éditer les stratégies locales des machines.

L'outil *Gestion des stratégies de groupes* est disponible pour faciliter la gestion des GPO, celui-ci reprend les interfaces et fonctionnalités des outils suivants :

- Utilisateurs et ordinateurs Active Directory.
- Sites et services Active Directory.

Ainsi que des modules d'administration des stratégies :

- Module de vérification des stratégies résultantes (RSoP, Resultant Set of Policy).
- Module de sauvegarde et de restauration des objets de stratégie de groupe.
- Module de copie et d'import des objets de stratégies de groupes.
- Intégration du filtrage par le langage WMI (Windows Management Instrumentation).
- Module de génération de rapport.

- Module de recherche d'objets de stratégies de groupes.

 L'outil Gestion des stratégies de groupes n'est pas fourni avec Windows Server 2003. Il est nécessaire de le télécharger sur le site de microsoft à l'adresse <http://www.microsoft.com>

8.2.2. Les modèles d'administration

L'ensemble de la description des GPO se trouve dans des fichiers dont l'extension est « .adm ».

Ceux-ci contiennent une description hiérarchique des modifications à effectuer sur les clients pour mettre en place la stratégie sur le client.

Ils contiennent aussi, les options de restrictions pour les valeurs, la valeur par défaut, l'explication de chaque paramètre et les versions de Windows qui prennent en charge le paramètre.

Rien ne vous empêche de créer vos propres modèles d'administration pour gérer des éléments qui ne le sont pas nativement.

8.2.3. Description d'un lien d'objet de stratégie de groupe.

Une stratégie de groupe est composée d'un objet Active Directory et d'un dossier dont le nom est le SID de la GPO et qui se trouve dans le répertoire SYSVOL celui-ci étant répliqué sur tous les contrôleurs de domaine.

Cet objet une fois créé et paramétré peut être lié à un ou plusieurs conteneurs (Sites, Domaines, Unités d'organisation).

De même, plusieurs GPO peuvent être liées à un même conteneur.

8.2.4. Héritage de l'autorisation de stratégie de groupe dans Active Directory

L'ordre dans lequel les objets GPO (Group Policy Object – Objet de Stratégie de Groupe) sont appliqués dépend des conteneurs Active Directory auxquels les objets GPO sont liés.

Ils sont hérités et sont appliqués dans l'ordre suivant : au site, au domaine, puis aux unités d'organisations.

8.3. Administration du déploiement d'une stratégie de groupe

8.3.1. Impact de l'existence d'objets de stratégie de groupe conflictuels

Les stratégies sont cumulatives, ce qui signifie que plusieurs stratégies peuvent entrer en conflit sur un même paramètre.

Lorsqu'il y a un conflit entre deux GPO appliquées, la GPO conflictuelle la plus proche du client est appliquée. Lorsque les deux GPO sont définies à un même niveau (par exemple sur la même OU), la GPO appliquée est celle qui se trouve en haut de la liste des stratégies de groupe appliquées au conteneur.

Toutefois, les paramètres de sécurité IP et les droits utilisateurs font exceptions. Le dernier objet GPO (le plus proche du client) remplace totalement tout autre objet GPO.

Dans certains cas, il peut être intéressant de changer ce mode de résolution de conflits comme par exemple lorsque l'on a délégué l'administration d'une UO à une personne et que l'on souhaite empêcher cette personne d'avoir le dernier mot sur l'application d'un paramètre précis.

Pour cela vous pouvez utiliser l'option « Ne pas passer outre » qui va empêcher qu'une GPO plus proche de l'objet utilisateur ou ordinateur ne prime sur une GPO plus éloignée.

Vous avez aussi « Bloquer l'héritage des stratégies », ce qui va stopper les fonctions d'héritage.

8.3.2. Attributs d'un lien d'objet de stratégie de groupe

8.3.2.1. Option « Appliqué »

Cette option n'est disponible qu'après l'installation de la console « Gestion des stratégies de groupe ».

L'option « Appliqué » est un attribut du lien qui lie l'objet GPO aux conteneurs (sites, domaines, UO).

Cette option propre à chaque liaison d'une GPO permet de forcer l'application de son contenu.

Elle est aussi appelée Ne pas passer outre lorsque la console « Gestion des stratégies de groupe » n'est pas installée.

8.3.2.2. Activation et désactivation d'un lien

Cette option permet de ne plus appliquer une GPO à un conteneur sans pour autant supprimer le lien qui les lie.

8.3.3. Filtrage du déploiement d'une stratégie de groupe

Vous pouvez décider d'appliquer les GPO seulement à des groupes et pas à d'autres à l'aide de cette option.

En effet, chaque objet GPO va être lié à une ACL qui va définir quels sont les utilisateurs, ordinateurs ou groupes qui vont pouvoir accéder à l'objet GPO donc pouvoir appliquer ces paramètres.

Ainsi si vous désirez appliquer une GPO seulement sur le groupe Administrateurs, il vous suffit d'afficher les paramètres de sécurité de l'objet GPO et de retirer l'autorisation Appliquer la stratégie de groupe à tous les utilisateurs à l'exception du groupe « Administrateurs ».

9. Gestion de l'environnement utilisateur à l'aide des stratégies de groupes

9.1. Configuration de paramètres de stratégie de groupe

9.1.1. Présentation des stratégies de groupes

L'implémentation des stratégies de groupes va permettre de centraliser la gestion de l'environnement des utilisateurs. Ainsi les GPO vont permettre de définir les droits nécessaires aux utilisateurs.

Lorsque vous administrez l'environnement d'un utilisateur de façon centralisée, vous pouvez intervenir sur les éléments suivants :

- Administration des utilisateurs et des ordinateurs : Modification des propriétés du bureau à l'aide de modifications distantes de la base de registre.
- Déploiement de logiciels : Automatisation complète de l'installation des programmes sur les postes clients en fonction du profil de l'utilisateur.
- Application des paramètres de sécurité : Permet de modifier le contexte de sécurité de l'environnement utilisateur.
- Définition d'un environnement adapté : Possibilité de rediriger certains répertoires sensibles ou de bloquer la modification de leurs contenus.

9.1.2. Paramètres « Non configuré », « Activé » et « Désactivé »

Avant même la définition des propriétés d'un paramètre de stratégie de groupe, il est nécessaire de choisir si vous allez configurer ce paramètre et si oui, si vous allez l'activer ou le désactiver.

En effet tout paramètre a une valeur par défaut. Si vous souhaitez laisser cette valeur par défaut, il vous suffit de ne pas configurer le paramètre. Si vous souhaitez modifier ce paramètre, vous avez le choix dans la plupart des cas entre « Activer » ou « Désactiver » ce paramètre.

Exemple : *Supprimer le menu Exécuter du menu Démarrer.*

- Non configuré : Le menu Exécuter va s'afficher sauf si **n'importe quelle** autre GPO spécifie le contraire.
- Activé : Le menu Exécuter va être supprimé sauf si une GPO ayant une **priorité plus importante** spécifie le contraire.
- Désactivé : Le menu Exécuter va s'afficher sauf si une GPO ayant une **priorité plus importante** spécifie le contraire.

Certains paramètres demandent une configuration plus importante qu'un simple choix booléen. Si dans ce cas, une GPO ayant une priorité plus importante spécifie des propriétés différentes pour le paramètre, l'ensemble des propriétés sera remplacé.

9.2. Attribution des scripts avec la stratégie de groupe

Grâce à une stratégie de groupe, vous pouvez affecter des scripts aux machines ou aux utilisateurs.

Les scripts affectés aux ordinateurs seront exécutés au démarrage et/ou à l'arrêt de l'ordinateur et les scripts affectés aux utilisateurs seront exécutés à l'ouverture et à la fermeture de la session.

Plusieurs langages sont supportés avec les scripts batch (NET USE ...), les scripts WSH (Windows Script Host) ou des exécutables.

☞ Via les propriétés d'un compte utilisateur, il est possible de spécifier un script d'ouverture de session, mais cette méthode est moins souple au niveau administratif.

9.3. Configuration de la redirection de dossiers

Ce paramètre de stratégie de groupe permet de rediriger les dossiers sensibles de l'utilisateur afin de centraliser sur un serveur les données et ainsi en faciliter la sécurité et la sauvegarde.

Les dossiers pouvant être redirigés sont les suivants :

- Mes documents : Permet de centraliser les données utilisateur sur un serveur de fichiers pour que son contenu soit disponible quelque soit l'ordinateur sur lequel se connecte l'utilisateur (ex : redirection vers le dossier de base de l'utilisateur).
- Menu Démarrer : Permet de faire pointer le contenu du menu Démarrer de tous les utilisateurs vers un contenu unique.
- Bureau : Permet de faire pointer le contenu du Bureau de tous les utilisateurs vers un contenu unique.
- Application Data : Contient les préférences applicatives de certaines applications qui peuvent être sauvegardées sur un serveur avec la réplication.

Il est possible via la redirection avancée, de rediriger les répertoires vers des dossiers différents selon l'appartenance de l'utilisateur à un groupe.

☞ La fonction de redirection de dossiers crée elle-même automatiquement des dossiers avec les autorisations adéquates.

9.4. Détermination des objets de stratégie de groupe

9.4.1. GPUpdate

GPUpdate est un outil en ligne de commande qui permet de rafraîchir instantanément l'application des stratégies de groupes sur une machine cliente.

En effet, les ordinateurs clients depuis Windows 2000 actualisent les GPO à des intervalles définis.

L'actualisation assure que les paramètres qui ont pu être modifiés par un administrateur sont appliqués le plus tôt possible. (Eventualité d'une personne qui ne redémarre jamais son ordinateur ou ne ferme jamais sa session).

Par défaut, les ordinateurs effectuent cette réactualisation toutes les 90 minutes + un temps aléatoire entre 0 et 30 minutes et ce, afin d'éviter que tous les ordinateurs fassent des requêtes au contrôleur de domaine (DC) en même temps.

En ce qui concerne les contrôleurs de domaine, ils sont réactualisés toutes les 5 minutes.

 Vous pouvez modifier ces valeurs à l'aide d'une stratégie de groupe.

GPUpdate [/Target:{ Ordinateur | Utilisateur}] [/Force] [/Wait:<valeur>] [/Logoff] [/Boot] [/Sync]

9.4.2. GPResult

GPResult est un outil en ligne de commande qui permet de visualiser les stratégies résultantes pour l'ordinateur et un utilisateur spécifié.

Comme de nombreuses stratégies peuvent entrer en conflit, cet outil permet de visualiser les stratégies effectives.

GPResult [/S système [/U utilisateur [/P mot_de_passe]]] [/SCOPE étendue] [/USER utilisateur_cible] [/V | /Z]

9.4.3. Rapport de stratégie de groupe

Grâce à la console Gestion de stratégie de groupe, il est possible d'afficher un rapport par GPO permettant de visualiser uniquement les paramètres qui ont été modifiés.

Ce rapport sera créé au format HTML et sera enregistrable aussi au format XML.

9.4.4. Simulation de déploiement de GPO

Dans la console Gestion de stratégies de groupes, il est possible de lancer une simulation de déploiement de stratégies de groupes. Ce qui va générer un rapport.

9.4.5. Résultat de déploiement de GPO

Dans la console Gestion de stratégies de groupes, il est possible de récupérer les informations de déploiement de stratégies de groupes et d'en générer un rapport.

10. Implémentation des modèles d'administration et des stratégies d'audit

10.1. Vue d'ensemble de la sécurité dans Windows 2003

Un droit sous Windows 2003 est la possibilité d'agir sur la configuration du système. Ainsi pour qu'un utilisateur modifie l'heure, ouvre une session, ou éteigne l'ordinateur, il est nécessaire qu'il ait le droit associé.

La différence avec une autorisation est que l'autorisation constitue la possibilité d'accéder ou d'utiliser une ressource (ex : fichier, dossier, imprimante, ...).

Par défaut, un certain nombre de droits sont associés à des groupes prédéfinis (ex : les membres du groupe « Opérateurs de sauvegarde » peuvent sauvegarder et restaurer des fichiers et des répertoires.).

10.2. Utilisation de modèles de sécurité pour protéger les ordinateurs

10.2.1. Présentation des stratégies de sécurité

Une stratégie de sécurité est un ensemble de paramètres de sécurité permettant de définir le contexte de sécurité d'un ordinateur.

Les stratégies de sécurité vont permettre de définir ces paramètres sur l'ordinateur local ou à partir d'Active Directory. L'avantage de l'implémentation dans Active Directory est la possibilité d'appliquer ces paramètres sur un nombre défini de machines via une GPO.

10.2.2. Description des modèles de sécurité

Vu la multitude de paramètres qui sont personnalisables dans une stratégie de sécurité, il fournit directement avec Windows 2003 un certain nombre de modèles correspondant chacun à un contexte de sécurité précis.

| Modèle | Fichier | Description |
|---------------------|---------------------------------------|---|
| Sécurité par défaut | setup security.inf dc security.inf | Configure la machine avec un niveau de sécurité basique |
| Compatible | compatws.inf | Offre un contexte de sécurité très proche de celui de Windows NT 4 ce qui permet d'assurer une compatibilité accrue pour les applications conçues pour l'ancien système. |
| Sécurisé | securews.inf securedc.inf | Il améliore les variables de sécurité pour les Stratégies de Compte et d'Audit. Enlève tous les membres du groupe Utilisateur avec Pouvoir. Les ACL ne sont pas modifiées. Il ne peut garantir le bon fonctionnement de toutes les applications (et leurs fonctionnalités). |
| Hautement sécurisé | hisecws.inf hisecdc.inf | Modèle le plus sûr mis à disposition des machines qui utilisent Windows 2000 en mode natif seulement. Il demande à ce que toutes les connexions réseau soient signées et cryptées de manière digitale (implémentation de IPSec). Il ne permet pas la communication avec |

| | | |
|--------------------------------|-------------|---|
| | | des machines employant des modèles plus anciens de clients Windows. Il ne se soucie pas du bon fonctionnement des applications. |
| Sécurité racine système | Rootsec.inf | Spécifie les autorisations pour la racine du disque système. |

10.2.3. Description des paramètres de modèles de stratégies

| | |
|-----------------------------------|--|
| Stratégies de comptes | Configurent des stratégies pour les mots de passe et les comptes. |
| Stratégies locales | Configurent l'audit, les droits d'utilisateur et les options de sécurité. |
| Journal des événements | Configure les paramètres des journaux des applications, des journaux système et des journaux de sécurité |
| Groupes restreints | Configurent l'adhésion aux groupes prédéfinis comme « Administrateurs », « Utilisateurs avec pouvoir », Admins du domaine, ... |
| Services système | Configurent les paramètres de sécurité et de démarrage des services exécutés sur un ordinateur |
| Registre | Configure la sécurité d'accès (DACL) au niveau des clés du registre. |
| Système de fichiers | Configure la sécurité d'accès (DACL) au niveau des chemins d'accès de fichiers spécifiques |
| Stratégies de clé publique | Configurent les agents de récupération de données cryptées, les racines de domaines, les autorités de certification approuvées, etc. |

10.2.4. Outils de création et d'importation des modèles de sécurité personnalisés

Dans le cas où les modèles ne correspondent pas à vos besoins, il est possible de personnaliser l'un des modèles existants ou d'en créer un nouveau.

Pour cela il suffit d'utiliser les deux composants logiciels enfichables :

- **Modèles de sécurité** : Permet de visualiser et de gérer les modèles existant sur le système (par défaut dans le répertoire %systemroot%\security\templates).
- **Configuration et analyse de la sécurité** : Permet de tester et d'appliquer à la machine en cours les modèles de stratégies que l'on a créés.

Une fois votre modèle créé et testé, vous pouvez l'importer dans Active Directory pour le déployer via une GPO. Pour cela, il vous suffit dans votre GPO de développer le conteneur **Configuration de l'ordinateur**, puis **Paramètres Windows** et enfin faire un clic droit sur **Paramètres de sécurité** pour sélectionner **Importer une stratégie**.

10.3. Configuration de l'audit

10.3.1. Présentation de l'audit

L'audit permet la création d'un journal recensant l'ensemble des actions effectuées sur un objet ou un élément de configuration par une population précise.

Cela peut permettre par exemple de surveiller l'accès à certains fichiers ou la modification des paramètres de configuration des comptes utilisateur par des administrateurs subalternes.

10.3.2. Description d'une stratégie d'audit

Une stratégie d'audit détermine les types d'actions que Windows 2003 va enregistrer dans le journal sécurité.

Pour implémenter une stratégie d'audit, plusieurs méthodes sont mises à votre disposition :

- Utiliser un modèle de stratégie de sécurité au niveau de l'ordinateur ou au niveau d'une GPO. En effet, les stratégies de sécurité contiennent des stratégies d'audit pré configurées.
- Configurer la stratégie d'audit directement dans le composant logiciel enfichable **Stratégie de sécurité local** de votre ordinateur.
- Configurer la stratégie d'audit dans une GPO pour l'appliquer à un ensemble d'ordinateurs.

La stratégie de sécurité va vous permettre de vérifier la réussite ou l'échec des évènements suivants :

| | |
|------------------------------------|---|
| Connexions aux comptes | Un évènement est enregistré à chaque authentification d'un compte sur la machine qui authentifie l'utilisateur. |
| Gestion des comptes | Un évènement est créé à chaque création, modification ou suppression d'un compte ou d'une propriété d'un utilisateur ou d'un groupe. |
| Accès au service d'annuaire | Un évènement est enregistré à chaque accès à un objet Active Directory. Pour cela vous devez spécifier les objets dans les propriétés d'AD. |
| Ouverture de session | Un évènement est enregistré à chaque ouverture de session réseau ou local sur l'ordinateur qui accepte la connexion. |
| Accès aux objets | Un évènement est enregistré à chaque accès à un fichier, dossier NTFS ou imprimante. Pour cela vous devez spécifier les objets dans les propriétés NTFS ou de l'imprimante. |
| Modification de stratégie | Un évènement est enregistré à chaque modification des options de stratégies de sécurité. |
| Utilisation de privilèges | Un évènement est enregistré à chaque utilisation d'un droit. |
| Suivi des processus | Un évènement est enregistré lorsqu'une application exécute une action. |
| Système | Un évènement est enregistré lorsqu'un utilisateur redémarre ou arrête Windows Server 2003. |

☞ Lorsque vous mettez en place un audit sur des fichiers, dossiers, imprimantes ou objets Active Directory, assurez vous d'avoir activé les audits correspondant au niveau de la stratégie de sécurité de la machine.

10.4. Gestion des journaux de sécurité

Les journaux de sécurité sont visibles dans l'**Observateur d'évènements**, ils permettent de visualiser toutes les informations concernant votre système.

Vous pouvez trouver les trois journaux principaux suivants sur tous les serveurs :

| | |
|--------------------|---|
| Application | Contient les évènements générés par des applications installées sur l'ordinateur (ex : SQL Serveur, Exchange, ...). |
| Sécurité | Contient les évènements générés par le système d'audit. |
| Système | Contient les évènements générés par les services et les applications intégrés à Windows 2003. |

Les deux journaux suivants ne sont présents que sur les contrôleurs de domaine :

| | |
|---|---|
| Service d'annuaire | Contient les évènements générés par le service d'annuaire Active Directory. |
| Service de réplication de fichiers | Contient les évènements générés par le service de réplication de fichiers. |

Pour chaque journal, vous pouvez spécifier la taille de celui-ci et le type de remplacement des données d'un fichier journal :

| | |
|---|--|
| Remplacer les événements si nécessaire | Chaque nouvel enregistrement remplace l'enregistrement le plus ancien dans le journal. |
| Remplacer les événements datant de plus de [x] jours | Les enregistrements sont conservés dans le journal pendant la durée spécifiée avant d'être écrasés. Par défaut, cette durée est de sept jours. |
| Ne pas remplacer les événements | Les nouveaux enregistrements ne sont pas enregistrés et le journal doit être nettoyé à la main. |

Vous avez la possibilité de sauvegarder le contenu de vos journaux dans les formats suivants :

- Fichiers journaux d'événements (.evt) (par défaut)
- Fichiers délimités par des virgules (.csv)
- Fichiers texte (.txt)

 Par défaut seul l'administrateur ou les membres du groupe Administrateurs peuvent agir sur le contenu des journaux.

11. Préparation de l'administration d'un serveur

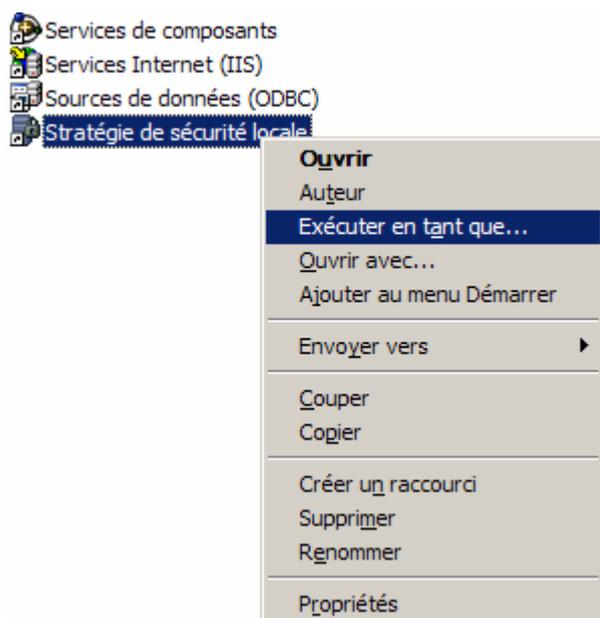
11.1. Préparation de l'administration d'un serveur

11.1.1. Utilisation des appartenances de groupe pour administrer un serveur

Nous pouvons distinguer 5 groupes locaux de domaines intégrés sous Windows 2003, ces groupes vont permettre de définir automatiquement des droits administratifs aux utilisateurs qui vont en devenir membres.

| | |
|---------------------------------|---|
| Administrateurs | Possède tous les droits nécessaires pour exécuter l'ensemble des tâches administratives. |
| Opérateurs de sauvegarde | Possède tous les droits nécessaires pour effectuer des sauvegardes et restauration sur le serveur. |
| Opérateurs de comptes | Possède tous les droits nécessaires pour créer, modifier, supprimer les comptes utilisateurs ou les groupes, à l'exception des groupes Administrateurs et Opérateurs de sauvegarde. |
| Opérateurs de serveur | Possède tous les droits nécessaires pour assurer la sauvegarde et la restauration des fichiers. |
| Opérateurs d'impression | Possède les permissions requises pour gérer et configurer les imprimantes réseau. |

11.1.2. Qu'est-ce que la commande Exécuter en tant que ?



Cette commande permet de lancer un programme en utilisant un autre compte utilisateur que celui utilisé pour la session en cours. Par exemple, si l'administrateur veut effectuer une tâche administrative sur un serveur Windows 2003, et qu'une session **Invité** est déjà ouverte sur ce serveur, il n'a pas besoin de fermer la session en cours pour le faire. Pour effectuer cette tâche il peut utiliser la commande **Exécuter en tant que** disponible en faisant un clic droit avec la touche « Shift » appuyée sur l'exécutable que l'on veut lancer et de sélectionner l'option **Exécuter en tant que...**

On peut également utiliser la commande **runas** en ligne de commande :

```
runas /user:nom_domaine\utilisateur nom_programme
```

Il est également possible de créer des raccourcis qui utilisent directement la commande **runas**.

☞ Il sera peut être nécessaire d'utiliser la touche MAJ+Click droit pour accéder à l'option exécuter en tant que dans le menu contextuel.

11.1.3. Qu'est-ce que l'outil Gestion de l'ordinateur ?

Il s'agit d'un ensemble d'outil permettant l'administration d'un ordinateur local ou distant.

Cette console MMC est disponible via le **Panneau de configuration**, dans les **Outils d'administrations** ou en faisant un clic droit sur le **Poste de travail** et en choisissant l'option **Gérer**.

Voila ci-dessous un descriptif des outils disponible :

| Catégorie | Outil | Description |
|---------------------------------|-------------------------------------|---|
| Outils système | | |
| | Observateur d'événements | Permet de visualiser le contenu des journaux Applications, Sécurité et Systèmes. Ces journaux sont d'une grande aide pour identifier une erreur sur le système. |
| | Dossiers partagés | Permet de visualiser l'ensemble des partages en cours sur le serveur, les sessions ouverte (utilisateurs authentifié sur la machine) ainsi que les fichiers ouverts sur le serveur. |
| | Utilisateurs et groupes locaux | Permet de créer et gérer les utilisateurs et les groupes de la base de compte local (base SAM). |
| | Journaux et alertes de performances | Permet d'analyser et de collecter les données relatives aux performances de l'ordinateur. |
| | Gestionnaire de périphériques | Permet de gérer les périphériques et les pilotes installés sur le serveur. |
| Stockage | | |
| | Stockage amovible | Permet de gérer les supports de stockage amovibles. |
| | Défragmenteur de disque | Permet de défragmenter le contenu d'un disque afin d'en augmenter les performances d'accès aux données. |
| | Gestion des disques | Permet de gérer les disques durs en créant des partitions ou volume, leurs affectant des lettres dans le poste de travail et en les formatant si nécessaires. |
| Services et applications | | |
| | Services | Permet de définir les options de démarrage des services du serveur. |
| | Contrôles WMI | Permet de configurer et gérer le service de gestion Windows. |
| | Service d'indexation | Permet de gérer, créer et configurer l'indexation des catalogues supplémentaires pour stocker les informations d'index. |

☞ Pour administrer un serveur à distance, il suffit de lancer la console Gestion de l'ordinateur sur un ordinateur quelconque, faire un clic droit sur Gestion de l'ordinateur (local), et de cliquer sur « Se connecter à ». Ensuite il suffit d'entrer le nom ou l'adresse IP de l'ordinateur que l'on veut administrer à distance.

11.1.4. Rôle de la console MMC dans le cadre d'une administration à distance

Vous pouvez utiliser Microsoft Management Console (MMC) pour créer, enregistrer et ouvrir des outils d'administration (appelés consoles MMC) qui gèrent les composants matériels, logiciels et réseau de votre système Windows.

MMC n'exécute pas de fonctions administratives alors que les outils hôtes les exécutent. Les outils que vous pouvez ajouter à une console sont principalement des composants logiciels enfichables. Vous pouvez

également ajouter des contrôles ActiveX, des liens vers des pages Web, des dossiers, des affichages de listes des tâches et des tâches.

Il existe deux façons générales d'utiliser MMC : en mode utilisateur, en utilisant des consoles MMC existantes pour administrer un système, ou en mode auteur, en créant des consoles ou en modifiant des consoles MMC existantes.

11.1.5. Comment créer une MMC pour gérer un serveur ?

Il suffit pour cela d'ouvrir une nouvelle console MMC (Démarrer \ Executer puis taper **mmc**).

Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**, puis cliquez sur **Ajouter**.

Dans la liste des composants logiciels enfichables, cliquez sur un composant logiciel enfichable, puis sur **Ajouter**.

À l'invite, sélectionnez l'ordinateur local ou distant que vous souhaitez gérer à l'aide de ce composant logiciel enfichable, puis cliquez sur **Terminer**.

Cliquez sur **Fermer**, puis sur **OK**.

11.2. Configuration de la fonction Bureau à distance pour administrer un serveur

11.2.1. Qu'est-ce que l'outil Bureau à distance pour administration ?

Le bureau à distance permet à l'utilisateur de se connecter à distance à un ordinateur et de contrôler ce dernier à distance. L'utilisateur se retrouve donc dans l'environnement de la machine à laquelle il se connecte (fond d'écran, apparences, fichiers locaux, etc...).

L'outil Bureau à distance pour administration fournit un accès au serveur à partir d'un ordinateur situé sur un autre site, à l'aide du protocole RDP (Remote Desktop Protocol). Ce protocole transmet l'interface utilisateur à la session cliente. De même, il transmet les manipulations sur le clavier et la souris du client vers le serveur.

Vous pouvez créer jusqu'à deux connexions distantes simultanées. Chaque session que vous ouvrez est indépendante des autres sessions clientes et de celle de la console du serveur. Lorsque vous utilisez l'outil Bureau à distance pour administrer un serveur distant, la connexion est établie comme s'il s'agissait de l'ouverture d'une session sur le serveur local.

Les paramètres relatifs à l'utilisation du bureau à distance sont configurables via les propriétés du **Poste de travail**, dans l'onglet **Utilisations à distance**.

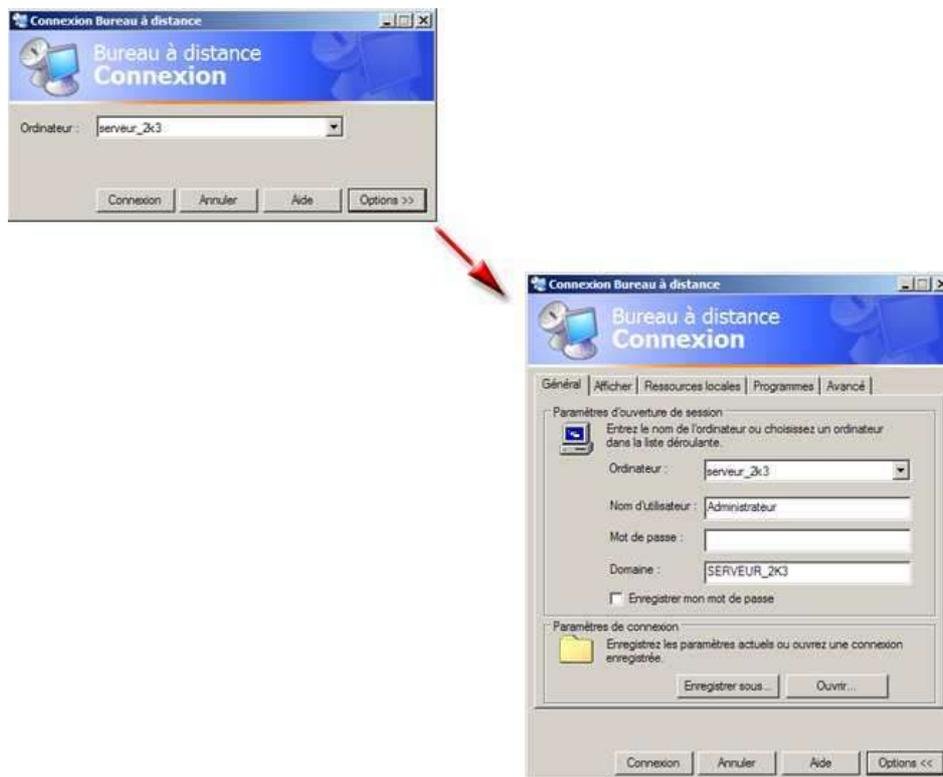
La connexion à distance peut s'effectuer grâce à l'outil **mstsc.exe** présent dans **%SystemRoot%\System32**.

 Le compte utilisé pour ouvrir une session en utilisant le bureau à distance doit obligatoirement avoir un mot de passe, et être également membre du groupe **Utilisateurs du Bureau à distance**.

Vous devez également vous assurer que l'option bureau à distance est activée, ce qui n'est pas le cas par défaut sous Windows 2003.

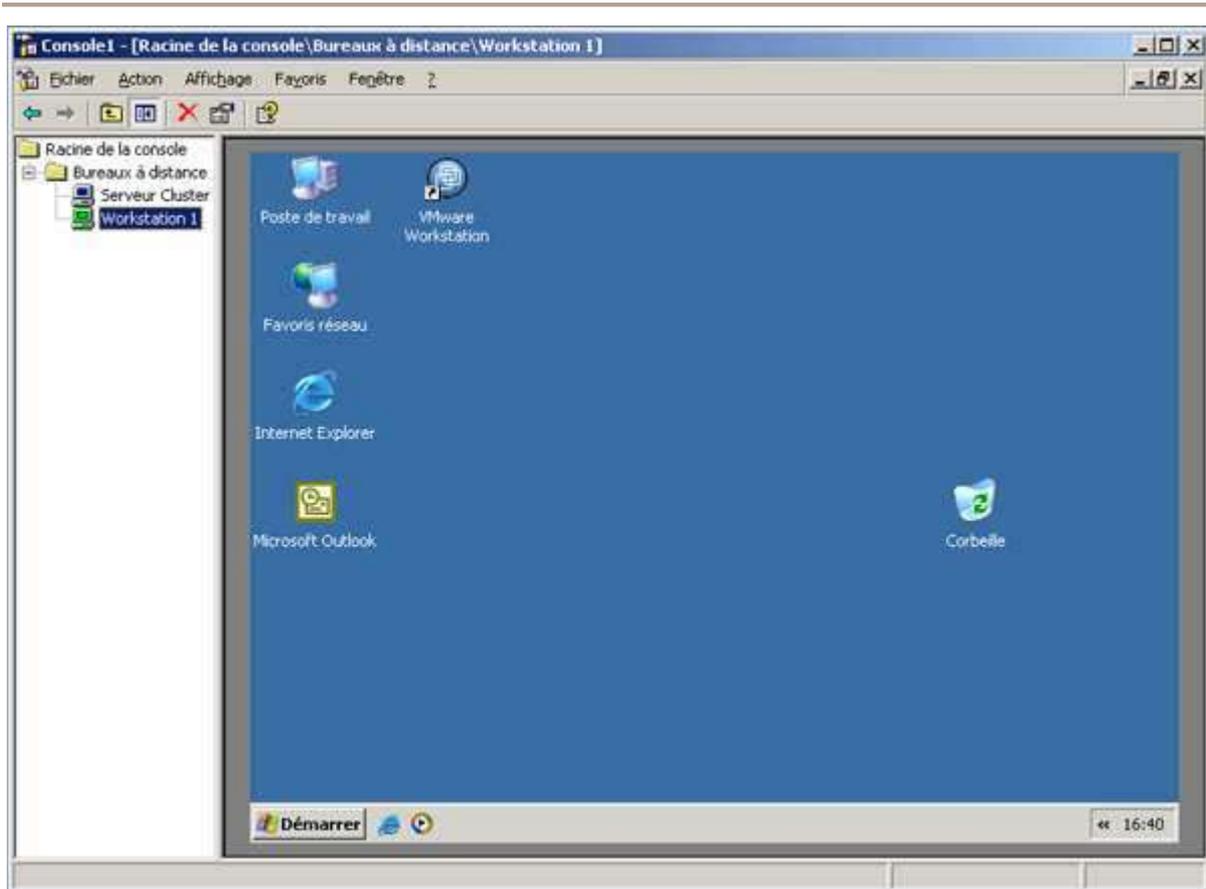
11.2.2. Que sont les préférences des ordinateurs clients dans le cadre d'une connexion Bureau à distance ?

Il est possible de créer des profils de connexions Bureau à distance qui lanceront chaque connexion avec des paramètres bien précis. Par exemple, Il est possible de créer et sauvegarder une connexion Bureau à distance qui lancera automatiquement une application à l'ouverture de sessions, et changera la résolution. Pour définir ce genre de comportement à l'ouverture d'une session bureau à distance, il faut cliquer sur le bouton **Option >>**



11.2.3. Bureaux à distance

Il existe également un composant logiciel enfichable MMC qui permet de gérer plusieurs sessions Bureau à distance simultanément. Il s'agit du composant **Bureau à distance**.



11.3. Gestion des connexions au Bureau à distance

11.3.1. Que sont les paramètres de délai des connexions de Bureau à distance ?

Il faut savoir que chaque session Bureau à distance ouverte sur un Serveur Windows 2003 consomme des ressources. Afin de limiter cette consommation, l'administrateur a la possibilité de définir des délais au bout desquelles les sessions seront automatiquement fermées.

Il est possible de définir un délai suivant 3 cas de figures :

- Fin de session déconnecté : Délai au bout duquel une session déconnectée sera fermée.
- Limite de session active : Durée maximale d'une session.
- Limite de session inactive : Durée maximale d'une session inactive, c'est-à-dire que l'utilisateur n'utilise ni la souris, ni le clavier ou tout autre périphérique d'entrée.

Ces paramètres peuvent être définis via les outils d'administration dans la console **Configuration des services terminal serveur**.

☞ **Une session déconnectée** est une session Bureau à distance qui n'a pas été fermée. Cela signifie que l'utilisateur a lancé la session, puis a fermé la fenêtre Bureau à distance directement. Dans ce cas de figure les processus lancés dans cette session tournent toujours jusqu'à fermeture de la session.

L'utilisateur pourra récupérer cette session si il se reconnecte.

11.3.2. Qu'est-ce que le Gestionnaire des services Terminal Server ?

Ce gestionnaire permet de surveiller les sessions en cours via un listing complet des processus s'exécutant sur chaque session. L'administrateur aura ainsi la possibilité de terminer un processus tournant sur une session inactive consommant trop de ressources par exemple.

Il aura également la possibilité de fermer la session d'un utilisateur.

12. Préparation de l'analyse des performances du serveur

12.1. Présentation de l'analyse des performances du serveur

12.1.1. Pourquoi analyser les performances ?

L'analyse des performances est indispensable à la maintenance du serveur. Effectuée de façon quotidienne, hebdomadaire ou mensuelle, elle permet de définir les performances de base du serveur. Grâce à cette analyse, vous obtenez des données sur les performances qui facilitent le diagnostic des problèmes du serveur.

Les données sur les performances permettent :

- De comprendre les caractéristiques de la charge de travail et les effets correspondants sur les ressources du système.
- D'observer les modifications et les tendances de ces caractéristiques et de l'utilisation des ressources afin de planifier les mises à niveau ultérieures.
- De tester les changements de configuration ou tout autre effort de réglage des performances en analysant les résultats.
- De diagnostiquer les problèmes et d'identifier les composants ou les processus pour optimiser les performances.

12.2. Analyse en temps réel et programmée

12.2.1. Qu'est-ce que l'analyse en temps réel et programmée ?

L'analyseur de performance permet d'effectuer deux types d'analyse :

| | |
|----------------------|--|
| En temps réel | Les compteurs sont affichés en temps réel. On peut utiliser ce type d'analyse pour un problème de performance ponctuel, non périodique. |
| Programmé | Ce type d'analyse se déclenche à une date et heure précise (en cas de réplique entre 1h et 2h du matin par exemple), puis sauvegarde l'activité des compteurs dans un journal qui pourra être consulté ultérieurement. |

12.2.2. Qu'est-ce que le Gestionnaire des tâches ?

Le Gestionnaire des tâches, accessible en pressant en même temps les touches **CTRL+ALT+SUPPR**, puis en cliquant sur **Gestionnaire des tâches** ou en pressant **CTRL+SHIFT+ECHAP**, permet d'obtenir la liste des processus en cours d'exécution ainsi que les ressources systèmes sollicitées pour chacun de ces processus.

Cela permet de détecter des anomalies comme par exemple un petit processus prenant la quasi-totalité de la mémoire système et ralentissant ainsi ce dernier de façons importantes.

Il est possible via l'onglet processus de stopper ou de définir la priorité de certains processus.

L'onglet **Performance** renseigne l'utilisateur sur l'intensité d'utilisation du microprocesseur et du fichier d'échange via un graphique.

Enfin l'onglet **Mise en réseau** renseigne l'utilisateur sur l'intensité du trafic réseau sur chacune des connexion via un graphique.



12.2.3. Qu'est-ce que la console Performances ?

La console performances est l'outil permettant d'effectuer des analyses de performances en temps réel ou programmé.

Pour sélectionner les données à récupérer, indiquez les objets, les compteurs et les instances d'objets de performances.

- **Un objet** de performance est un ensemble logique de compteurs associés à une ressource ou à un service pouvant être analysés (ex : le processeur).
- **Un compteur** de performance est un élément de données associé à un objet de performance. Pour chaque compteur sélectionné, le Moniteur système affiche une valeur qui correspond à un aspect spécifique des performances définit pour l'objet de performance (ex : % d'utilisation du processeur).
- **Les instances** d'objets de performance sont des ensembles d'un même type d'objet. Par exemple, si un système comporte plusieurs processeurs, le type d'objet Processeur dispose de plusieurs instances (ex : chaque processeur correspond à une instance).

12.2.4. Pourquoi analyser les serveurs à distance ?



Ceci permet de ne pas fausser les résultats des performances. En effet, l'analyseur de performance consomme également des ressources. Il convient donc de lancer cette console MMC sur un autre serveur et de créer des compteurs pointant sur le serveur qu'on veut analyser.

12.3. Configuration et gestion des journaux de compteur

12.3.1. Qu'est-ce qu'un journal de compteur ?

Les journaux de compteur permettent d'effectuer des analyses programmées. Dans le processus de création d'un journal de compteurs, les informations suivantes sont requises :

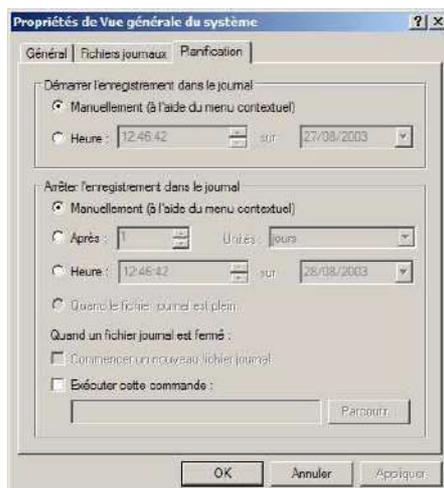
- Nom du journal
- Type de fichier, format binaire, SQL, texte, etc...
- Compteurs utilisés pendant l'analyse
- Type de lancement : planifié ou manuel.

Il est également possible de créer un journal en utilisant la commande **logman**.

12.3.2. Comment planifier un journal de compteur ?

Il est possible de lancer un journal de compteur manuellement ou via une planification.

La planification se définit dans les propriétés du journal, ou pendant le processus de création du journal.



12.4. Configuration des alertes

12.4.1. Qu'est-ce qu'une alerte ?

Une alerte est une fonction qui détecte à quel moment la valeur d'un compteur atteint une valeur appelée **seuil d'alerte**.

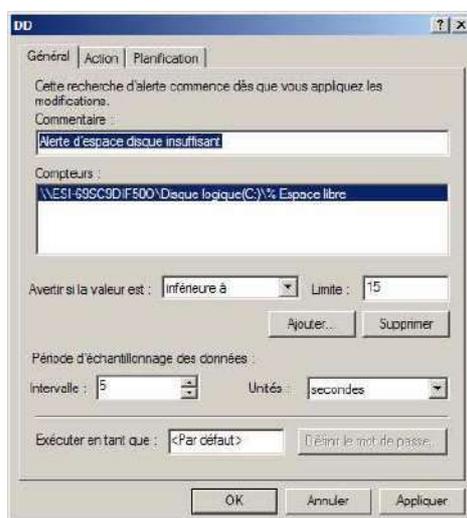
Si le seuil d'alerte est atteint, l'administrateur peut planifier une action à effectuer.

Par exemple, il pourrait être intéressant de définir une alerte sur un serveur de fichier si l'espace disque libre (objet : disque logique, compteur : espace libre) devient inférieur à 10% de l'espace total, et de planifier le lancement d'un programme qui se chargera de supprimer les fichiers temporaires se trouvant sur ce serveur de fichier.

12.4.2. Comment créer une alerte ?

Suivez la procédure ci-après pour créer une alerte. :

- Pour créer une alerte :
- Pour ouvrir la console Performances, cliquez sur Démarrer, Outils d'administration, puis sur Performances.
- Double-cliquez sur Journaux et alertes de performance, puis cliquez sur Alertes.
- Toutes les alertes existantes apparaissent dans le volet des informations.
- L'icône verte indique que l'alerte est en cours et l'icône rouge signale l'arrêt de l'alerte.
- Cliquez avec le bouton droit sur une zone vierge du volet des informations, puis cliquez sur Nouveaux paramètres d'alerte.
- Dans la zone de texte Nom, tapez le nom de l'alerte, puis cliquez sur OK.
- Sous l'onglet Général, vous pouvez ajouter un commentaire pour votre alerte, ainsi que des compteurs, des seuils d'alerte et des intervalles d'échantillonnage.
- L'onglet Action permet de définir les actions à réaliser lorsque des données de compteur génèrent une alerte.



12.5. Conseil d'optimisation d'un serveur

Voilà ci-dessous un tableau reflétant les valeurs des compteurs d'un serveur Windows 2003 performant :

| Objet | Compteur | Place moyenne acceptable | Valeur désirée |
|-------------------|---|-----------------------------------|----------------|
| Mémoire | Page/s | 0 à 20 | Basse |
| | Octets disponibles | Au moins 5% de la mémoire totale | Haute |
| | Octets validés | Moins que la mémoire RAM physique | Basse |
| | Octets de réserve non paginés | Reste constante, n'augmente pas. | Sans objet |
| | Défauts de page/s | Inférieure à 5 | Basse |
| Processeur | % Temps processeur | Inférieure à 85 % | Basse |
| | Système : Longueur de la file du processeur | Inférieure à 10 | Basse |
| | Files de travail du | Inférieure à 4 | Basse |

| | | | |
|-------------------------|--|--|------------|
| | serveur : Longueur de la file | | |
| | Interruptions/s | Dépend du processeur | Basse |
| Disque dur | | | |
| | % Temps du disque | Inférieure à 50 % | Basse |
| | Taille de file d'attente du disque actuelle | 0 à 2 | Basse |
| | Disque, octets/transfert moy. | Ligne de base ou supérieure | Haute |
| | Octets disque/s | Ligne de base ou supérieure | Haute |
| Interface Réseau | | | |
| | Utilisation du réseau (dans Gestionnaire des tâches) | Inf. à 30 %, en général | Basse |
| | Interface réseau : Octets envoyés/s | Ligne de base ou supérieure | Haute |
| | Interface réseau : Total des octets/s | Ligne de base ou supérieure | Haute |
| | Serveur : Octets reçus/s | Moins de 50 % de la capacité de la bande passante de la carte réseau | Sans objet |

13. Maintenance des pilotes de périphériques

13.1. Configuration des options de signature des pilotes de périphériques

13.1.1. Qu'est-ce qu'un périphérique ?

Un périphérique est un équipement matériel qui se branche sur un ordinateur. Il peut s'agir d'une carte vidéo, une webcam, une souris, un disque dur, etc...

Nous pouvons distinguer deux types de périphérique :

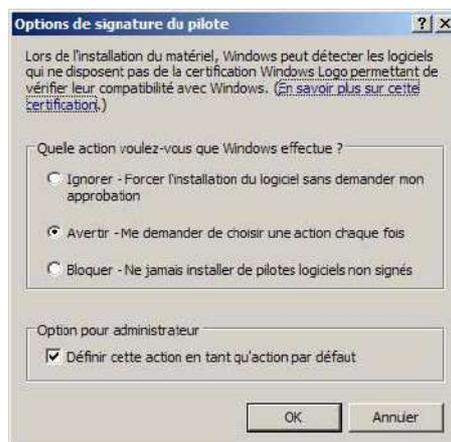
- **Plug-and-Play** : Le périphérique est automatiquement reconnu par la famille Windows 2003.
- **Non Plug-and-Play** : L'utilisation d'un pilote est indispensable pour pouvoir utiliser le périphérique sur la famille Windows 2003.

13.1.2. Qu'est-ce qu'un pilote de périphérique ?

Un pilote de périphérique est un logiciel fournis par le constructeur du périphérique permettant à un OS de détecter, configurer, et utiliser le périphérique correspondant à ce pilote. C'est un peu comme un manuel d'instruction numérique (donc non exploitable par l'utilisateur) pour OS.

 Les périphériques figurant dans la HCL ont leurs pilotes directement intégrés à Windows.

13.1.3. Qu'est-ce qu'un pilote de périphérique signé ?



Un pilote de périphérique signé est un pilote qui a été testé et approuvé par Microsoft dans le WHQL (Windows Hardware Quality Lab).

L'utilisation d'un pilote signé garanti donc les performances et la stabilité du système. Leurs utilisation est donc fortement recommandée sur les serveurs jouant un rôle important dans votre infrastructure réseau.

Vous pouvez définir le comportement qu'adoptera Windows 2003 en cas d'installation de pilote non signé :

- Les pilotes de périphériques non signés numériquement ne sont pas pris en compte

- Un message d'avertissement s'affiche lorsqu'un pilote de périphérique non signé est détecté
- Les utilisateurs ne sont pas autorisés à installer des pilotes de périphériques non signés

Ces paramètres sont définissables via les propriétés systèmes, dans l'onglet **matériel**, puis cliquez sur **Signature du pilote**.

Le vérificateur des fichiers système, **sfc**, est un outil de ligne de commande qui analyse et vérifie les versions de tous les fichiers système protégés à chaque redémarrage de votre ordinateur. Il remplace les fichiers effacés par des fichiers systèmes valides et fournis par Microsoft. Cela fait partie de la fonctionnalité de protection des fichiers Windows de Windows Server 2003.

13.1.4. Qu'est-ce que la console Gestion des stratégies de groupe ?

La console de gestion des stratégies de groupes est un composant d'administration librement téléchargeable sur le site de Microsoft permettant de mieux gérer les stratégies de groupes.

13.2. Utilisation de la version précédente d'un pilote de périphérique

A chaque mise à jour d'un pilote de périphérique, Windows 2003 sauvegarde les fichiers du pilote en cours d'utilisation. En cas de mise à jour infructueuse (dysfonctionnement du périphérique), l'option **Retour à la version précédente** permet d'utiliser la sauvegarde du précédent pilote qui fonctionnait correctement.



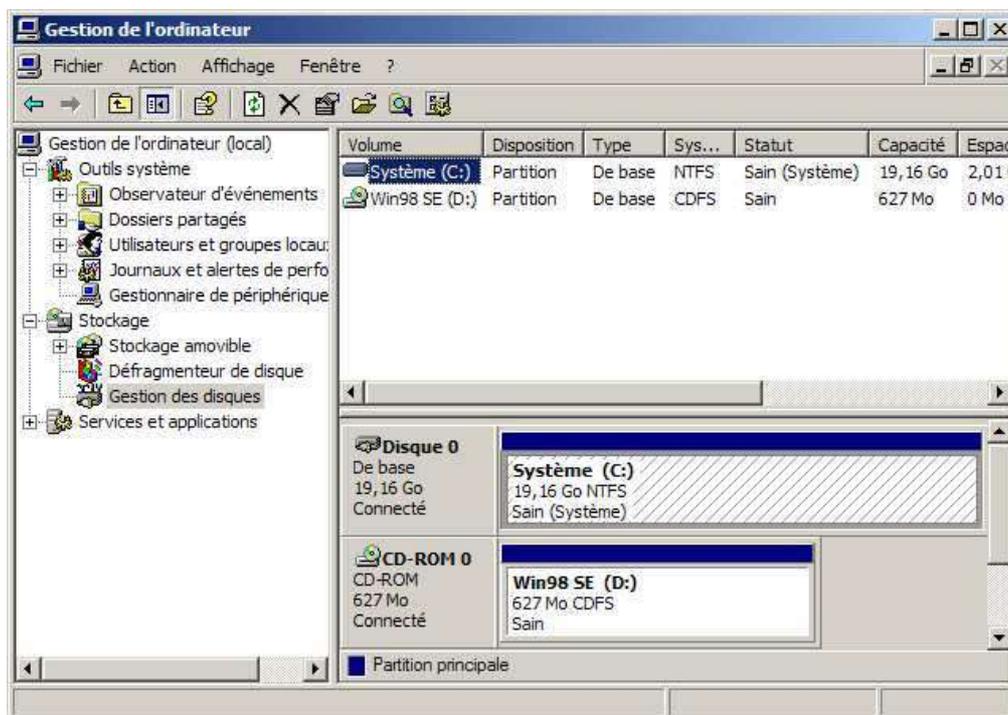
14. Gestion des disques

14.1. Préparation des disques

14.1.1. Qu'est-ce que l'outil Gestion des disques ?

Cet outil permet de gérer les disques connectés à l'ordinateur. Il permet aux utilisateurs ayant les permissions adéquates de créer, modifier, supprimer des partitions ou volumes sur les disques connectés.

Il est également possible via le composant MMC de transformer des disques de base en disques dynamiques.



14.1.2. Qu'est-ce que l'outil DiskPart ?

Diskpart est un outil ayant exactement les mêmes fonctions que le gestionnaire de disque. La seule différence vient du fait qu'il s'utilise sous l'invite de commande, ou dans la console de récupération si cette dernière a été installée.

14.1.3. Qu'est-ce qu'une partition ?

Avant de pouvoir écrire des informations sur un disque, l'utilisateur devra au préalable créer une ou plusieurs partition(s). Il s'agit d'un espace réservé sur un disque dur, cet espace devra par la suite être formaté dans un système de fichiers reconnu par Windows 2003 (FAT, FAT32, NTFS) avant de pouvoir y stocker la moindre information. Il ne peut y avoir que 4 partitions par disque, une partition va permettre d'héberger un système d'exploitation qui sera directement démarrable par le bios de l'ordinateur.

Nous pouvons distinguer 2 types de partition :

- **Partition principale** : Réserve un espace disque défini par l'utilisateur directement exploitable.

- **Partition étendue** : La partition étendue ne peut pas, à la différence de la partition principale, être formatée avec un système de fichiers. Ce sont les lecteurs logiques que vous créez dans cette partition qui sont formatés selon un système de fichiers donné.

Les **lecteurs logiques** sont similaires aux partitions principales, à l'exception près que vous pouvez créer jusqu'à 24 lecteurs logiques par disque. Vous pouvez formater un lecteur logique et lui affecter une lettre de lecteur.

Une fois la partition principale ou le lecteur logique créé, ils sont accessibles via une lettre de l'alphabet, **C** : par exemple pour la partition hébergeant le plus souvent le système.

14.1.4. Comment convertir les systèmes de fichiers ?

Le système de fichier NTFS est apparu sous Windows NT. Ce système de fichier permet contrairement au FAT, ou FAT32 de bénéficier des avantages suivants :

- Sécurité d'accès : Possibilité de définir grâce aux ACL (Access Control List) la liste des utilisateurs autorisés à accéder, à une ressource stockée sur la partition formatée en NTFS.
- EFS : Possibilité de cryptage.
- Quota : Restriction d'espace utilisable pour un utilisateur donné.
- Compression des données à la volée.

Son principal inconvénient est qu'il n'est pas supporté sous les systèmes de la famille Windows 9x.

Pour convertir sous Windows 2003 une partition formatée FAT en NTFS, l'administrateur peut utiliser la commande **convert** (convert [lecteur :] /fs:ntfs).

14.2. Gestion des propriétés d'un disque

14.2.1. Comment effectuer une nouvelle analyse des propriétés d'un disque ?

Il peut arriver que Windows ne détecte pas un disque qui vient d'être connecté à l'ordinateur, dans ce cas, il est nécessaire d'utiliser la commande **Analyser les disques de nouveau**.

Windows effectuera ainsi une nouvelle analyse des disques connectés, et mettra à jour les propriétés de ce dernier.

14.3. Gestion des lecteurs montés

14.3.1. Qu'est-ce qu'un lecteur monté ?

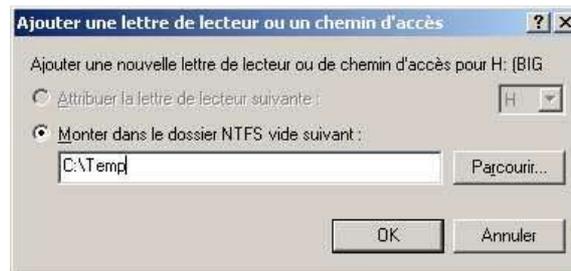
Un lecteur monté est une partition formatée à laquelle on accède via un dossier plutôt qu'une lettre d'accès. Ce dossier servant de point d'accès à la partition doit obligatoirement se trouver sur une partition NTFS et être vide au moment du montage du lecteur.

14.3.2. Quel est l'intérêt du lecteur monté ?

Les lecteurs montés NTFS se révèlent pratiques pour ajouter des volumes à un ordinateur alors que toutes les lettres de lecteur ont déjà été affectées. Vous pouvez également ajouter de l'espace à un volume en y montant d'autres disques en tant que dossiers au lieu d'avoir à recréer le volume sur un disque de plus grande capacité.

14.3.3. Comment gérer un lecteur monté ?

Pour créer un lecteur monter on peut passer par le gestionnaire de disque en faisant un click droit sur la partition ou le volume que l'on désire monter, puis en sélectionnant l'option : **Modifier la lettre de lecteur et les chemins**



On peut également utiliser **diskpart** avec l'option **assign**.

14.4. Type de disques

14.4.1. Utilisation des disques de base

L'appellation disque de base représente le mode gestion par défaut des disques. Il permet la création de deux types de partition : **Principale** et **Étendue**.

Les partitions principales (qui peuvent être au nombre maximal de 4 sur un même disque) sont celles qui sont amorçables. Les OS doivent impérativement se trouver sur ce type de partition, faute de quoi ils ne pourront démarrer.

Une partition étendue constitue un espace non alloué du disque. Afin de pouvoir exploiter cet espace, il faut au préalable y créer un ou plusieurs lecteur(s) logique(s). Cette partition permet d'outrepasser la limite des 4 « conteneurs » que l'on peut créer.

14.4.2. Utilisation des disques dynamiques

Les disques dynamiques offrent de nombreux avantages par rapport aux disques de base. Il va être par exemple possible d'étendre un volume sur plusieurs disques à condition qu'ils soient dynamiques afin de créer un volume réunissant l'espace disponible de ces disques.

Tout ceci est de plus réalisé de façon entièrement logiciel il n'y a donc pas à ajouter de carte particulière.

Il est également possible de redimensionner les tailles des volumes créés à l'origine sur un disque dynamique et cela à la volée sans avoir à redémarrer l'ordinateur, ni même avoir à déconnecter les clients travaillant sur le volume.

Mais les disques dynamiques présentent toutefois des contraintes. Il n'est pas possible de réaliser un double amorçage sur des disques dynamiques, et ce, même si les deux systèmes d'exploitation reconnaissent ce type de disque.

De plus, les disques amovibles, connectés en USB ou par interface IEEE ne peuvent être transformés en disques dynamiques. C'est également le cas des disques d'ordinateurs portables.

Il faut également noter qu'un espace minimum de 1Mo pour la base de données des disques dynamiques est requis. Cet espace est automatiquement réservé lorsque l'on utilise les outils de Windows 2003 pour partitionner un disque.

Enfin, il faut savoir que les disques dynamiques ne sont pas reconnus par les versions antérieures à Windows 2000, ni par les systèmes Linux ou UNIX.

La conversion d'un disque de base en disque dynamique est extrêmement simple : cela se fait via la console Gestion des disques, ou via l'utilitaire diskpart.exe. Il s'agit de sélectionner le disque à convertir, de faire un clic droit dessus, et de choisir l'option **Convertir en disque dynamique**. L'opération inverse requiert que tous les volumes présents sur le disque dynamique soient supprimés avant de procéder à la conversion.

Il est possible de créer 5 types de volumes avec des disques dynamiques sous Windows 2003 Server :

- Volume simple
- Volume agrégé par bande
- Volume fractionné
- Volume en miroir
- Volume RAID5

14.4.2.1. Volume simple

Un volume simple est l'équivalent d'une partition principale ou d'un volume logique sur un disque dynamique. L'unique différence est qu'il n'est pas soumis aux mêmes limites que ces derniers notamment par le fait que l'on peut en créer autant que l'on souhaite.

Il est possible d'étendre un volume simple en volume fractionné. Cependant, vous ne pouvez étendre que les volumes natifs, c'est-à-dire, tous les volumes non issus d'une mise à niveau de disque de base vers disque dynamique.

14.4.2.2. Volume agrégé par bande

Avec des volumes agrégés par bandes, le volume est créé sur plusieurs disques dynamiques en utilisant un espace de taille égal sur l'ensemble de ces disques.

Exemple : Si l'on possède 2 disques de 20Go et 1 disques de 30 Go, la taille de notre volume composé des trois disques sera au final de 60Go au lieu de 70Go). Les 10Go restant pourront être utilisés pour un autre volume.

Les données sont réparties de manière équitable sur chacun des volumes, ce qui a pour avantage d'améliorer les performances de lecture et d'écriture.

Cependant, étant donné que les données sont réparties sur tous les disques, si l'un d'eux est défaillant, l'intégralité des données est perdue.

De plus, si l'on souhaite ajouter un disque à un volume agrégé existant, il est nécessaire de sauvegarder le contenu du volume, puis de supprimer le volume, de le recréer avec le disque supplémentaire et de restaurer la sauvegarde sur le volume. Ce qui signifie que l'on ne peut pas directement ajouter un disque dur à un volume agrégé existant.

14.4.2.3. Volume fractionné

Le système de volume fractionné, sollicite lui aussi plusieurs disques dynamiques, cependant la méthode de remplissage est différente. En effet, les données sont dans un premier temps écrites sur le premier disque, puis une fois ce dernier rempli, les données vont continuer à être stockées sur le suivant et ainsi de suite. Comme le système de volume agrégé par bandes, si l'un des disques connaît une défaillance, l'intégralité des données est perdue.

L'avantage de ce type de volume est de pouvoir être étendu tant que de l'espace est disponible sur l'un des disques de la machine.

14.4.2.4. Disques étrangers

Quand vous déplacez un disque dynamique vers un nouvel ordinateur, ce dernier le traite comme un disque étranger. En effet, la base de données du disque déplacé ne correspond pas encore à la base de données des disques dynamiques de l'ordinateur.

Afin de la faire correspondre, il est nécessaire de sélectionner l'option **Importer des disques étrangers**. Cette option met à jour la base de données du disque déplacé avec la base de données des disques existant et permet de vérifier si l'ensemble des disques composant un volume ont bien été déplacés.

14.4.2.5. Réactivation d'un disque

Si un disque est déconnecté à cause d'un endommagement, d'une coupure de courant ou d'une déconnexion, le disque n'est pas accessible. Le cas échéant, vous devez réparer les partitions ou les volumes. Pour ce faire, ouvrez l'outil Gestion des disques, cliquez avec le bouton droit sur la partition ou le volume affichant l'état Manquant ou Déconnecté, puis cliquez sur Réactiver le volume. Une fois le disque réactivé, il doit afficher l'état Connecté.

Il faut toujours essayer de réactiver le disque si celui-ci est marqué comme manquant, ou déconnecté

14.5. Création de volumes

La création d'un volume simple, comme tout autre type de volume se fait toujours de la même façon. Il suffit de faire un click droit sur un **Espace non alloué** dans le gestionnaire de disque, de cliquer sur **Nouveau nom**, et de suivre les instructions de l'assistant de création de volume.

Dans le cas de la création d'autre type de volume, un assistant va vous permettre de faciliter vos choix dans le cadre de la création de volume fractionné et de volume agrégé en réalisant tous les calculs pour vous.

15. Gestion du stockage des données

15.1. Gestion de la compression des fichiers

15.1.1. Qu'est-ce que la compression des fichiers ?

La compression des données est une option qui permet de compresser les données de façon transparente pour l'utilisateur. Cela va utiliser un algorithme (comme on le fait pour des fichiers zip, rar ou ace) qui va permettre d'utiliser moins d'espace sur un volume au format NTFS.

L'utilisation de la compression des données affecte tout de même les performances lors de l'accès à ces données. Il vaut donc mieux envisager cette option que si aucune autre alternative n'est possible.

Il faut également noter que les dossiers et les fichiers se compressent indépendamment. Cela signifie qu'un dossier peut être compressé sans que les fichiers qu'il contient le soient pour autant, et vice versa (l'attribut de compression au niveau des dossiers permettant uniquement de spécifier l'attribut dont vont hériter les fichiers qui vont y être copiés).

Pour que la compression des dossiers affecte également les fichiers qu'il contient, le dossier doit être compressé avant d'y placer les fichiers.

Enfin, notez qu'en cas de copie d'un fichier compressé, ce dernier est dans un premier temps décompressé, puis copié dans le dossier de destination, et enfin compressé à nouveau. Il faut donc s'assurer que le volume de destination possède suffisamment d'espace libre pour accueillir le fichier décompressé.

Ci-dessous, le tableau récapitulant le traitement de l'état de compression d'un fichier ou d'un dossier :

| | Même lecteur | Lecteur d'origine et de destination différents |
|-------------|---|---|
| Copie | Les fichiers et dossiers héritent de leur état de compression | Les fichiers et dossiers héritent de leur état de compression |
| Déplacement | Les fichiers et dossiers conservent leur état de compression | Les fichiers et dossiers héritent de leur état de compression |

 Il n'est pas possible de compresser un fichier ou un dossier crypté.

15.1.2. Qu'est-ce que la commande compact ?

La commande **compact** affiche et modifie la compression des fichiers ou des répertoires dans les partitions NTFS. Utilisée sans paramètre, la commande compact affiche l'état de la compression du répertoire en cours.

Syntaxe

compact [{/c|/u}] [/s[:rép]] [/a] [/i] [/f] [/q] [NomFichier[...]]

| Paramètres | Description |
|------------|---|
| /c | Comprime le répertoire ou le fichier indiqué. |
| /u | Décompresse le répertoire ou le fichier indiqué. |
| /s:rép | Indique que l'action demandée (compression ou décompression) doit s'appliquer à tous les sous répertoires du répertoire indiqué ou du répertoire en cours si aucun répertoire n'est spécifié. |
| /a | Affiche les fichiers cachés ou les fichiers système. |
| /i | Ne tient pas compte des erreurs. |

| | |
|------------|--|
| /f | Force la compression ou la décompression du répertoire ou du fichier indiqué. Ce paramètre est utilisé lorsque la compression d'un fichier est interrompue par une panne du système. Pour forcer la compression du fichier dans sa totalité, utilisez les paramètres /c et /f et spécifiez le fichier compressé partiellement. |
| /q | Signale uniquement les informations les plus importantes. |
| NomFichier | Indique le nom du fichier ou du répertoire. Vous pouvez utiliser plusieurs noms de fichier ainsi que des caractères génériques (* et ?). |
| /? | Affiche de l'aide à l'invite de commandes. |

15.2. Configuration du cryptage des fichiers

15.2.1. Qu'est-ce que le cryptage EFS ?

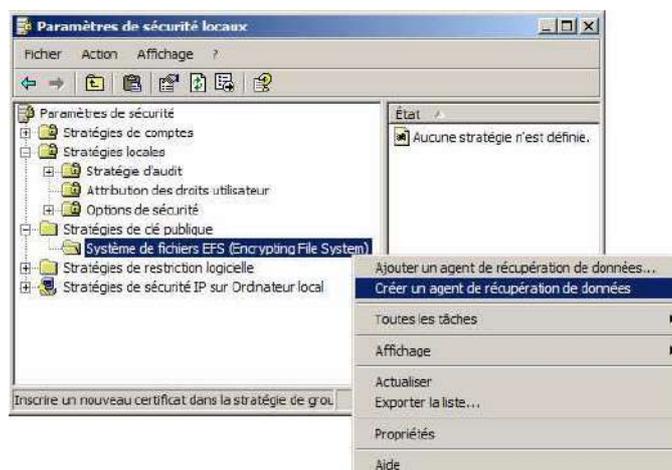
Le cryptage des fichiers est une opération très utile dans le cadre d'une organisation devant être sécurisée. En effet, la gestion des autorisations ne permet pas une sécurité maximum ; si un utilisateur malveillant réussit à récupérer le média sur lequel se trouvent les données auxquelles il n'a normalement pas accès sur le réseau, il peut cependant brancher ce disque dur sur un autre OS où il est administrateur et ensuite avoir accès à l'intégralité des informations.

Le cryptage des données évite que ce genre de situation puisse se produire.

Quand un utilisateur crypte un fichier ou un dossier, le système stocke le fichier en question sous une forme cryptée en utilisant la clé publique de cet utilisateur, et le décrypte quand l'utilisateur veut y accéder à nouveau en utilisant sa clé privée. Seule la clé privée de l'utilisateur ayant crypté le fichier peut décrypter le fichier. Ceci se fait de façon totalement transparente pour l'utilisateur, alors que l'utilisateur non autorisé se verra l'accès refusé.

Il faut cependant noter que les données ne sont pas cryptées quand elles circulent sur le réseau. Il faut donc penser à activer IPSec et WebDAV pour permettre un cryptage des données lors de leurs transports sur le réseau.

Un agent de récupération doit être configuré afin de pouvoir récupérer les fichiers cryptés dans le cas, par exemple, du départ d'un employé ou de la perte de sa clé de décryptage. Cet agent de récupération doit être défini avant le cryptage des fichiers



Par défaut le compte administrateur est utilisé comme Agent de récupération

15.2.2. Comment crypter un fichier ou un dossier ?

Pour crypter un dossier : dans la boîte de dialogue Propriétés pour le dossier, cliquer sur l'onglet Général, ensuite, cliquer sur le bouton Avancé et sélectionner la case à cocher « Crypter le contenu pour sécuriser les données ». Le dossier n'est pas crypté, mais les fichiers qui y seront placés seront cryptés. Décocher la case si vous souhaitez que les fichiers ne soient plus cryptés.

15.2.3. Quels sont les effets produits par le déplacement ou la copie de fichiers ou de dossiers cryptés ?

Ci-dessous, le tableau récapitulant le traitement de l'état de cryptage d'un fichier ou d'un dossier :

| Action\Destination | Destination : Dossier crypté | Destination : Dossier non crypté |
|--------------------|---|---|
| Copie | Les fichiers et dossiers deviennent cryptés | Les fichiers et dossiers conservent leur état de cryptage |
| Déplacement | Les fichiers et dossiers deviennent cryptés | Les fichiers et dossiers conservent leur état de cryptage |

☞ Si vous copiez le fichier crypté d'un volume NTFS dans un volume FAT ou FAT32, le fichier devient non crypté. Si vous copiez le fichier d'un volume FAT dans un dossier crypté sur un volume NTFS, le fichier est crypté.

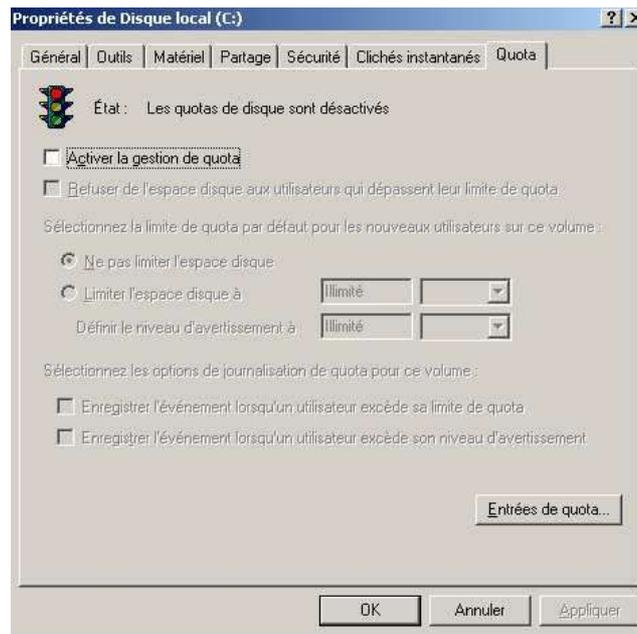
15.3. Implémentation des quotas de disque

15.3.1. Qu'est-ce qu'un paramètre de quota de disque ?

Un quota est une limite d'espace disque virtuel pour un utilisateur. En activant un Quota, l'administrateur va pouvoir définir l'espace maximum que pourront exploiter les utilisateurs locaux, ou du domaine sur le disque sur lequel il a activé le quota et ceci même si le disque détient encore de l'espace libre.

15.3.2. Comment activer et désactiver des quotas de disque ?

Il suffit d'aller dans les propriétés du disque sur lequel on désire activer le quota, cliquer sur l'onglet **Quota**, puis cocher la case **Activer la gestion de quota**.



15.3.3. Comment ajouter et supprimer des entrées de quota de disque ?

En activant la gestion de quota, les limites d'espace exploitable seront par défaut appliquées pour tous les utilisateurs (sauf l'administrateur). Cependant, il peut arriver que pour une raison particulière, l'administrateur veuille autoriser un utilisateur particulier à utiliser une plus grande ou plus petite portion d'espace disque que les autres utilisateurs. Dans ce cas, il faudra créer une entrée de quota. Une entrée de quota permet de définir un quota pour un utilisateur. Cependant il n'est pas possible de créer une entrée de quota pour un groupe d'utilisateur.

Il faut également savoir qu'une entrée de quota est prioritaire sur le quota par défaut.

☞ En cas de stockage de fichiers compressés sur un disque sur lequel est activé la gestion de quota, c'est la taille du fichier sans compression qui est comptabilisé.
La gestion de quota est une option accessible que sur les partitions ou volumes formatés en NTFS.

Ce screenshot montre 2 entrées de quota :

- Une entrée illimitée pour l'administrateur créée automatiquement en cas d'activation de la gestion de quota
- Une entrée définie manuellement qui limite à 100 Mo l'espace disque exploitable pour l'utilisateur **invité**.

| État | Nom | Nom d'ouverture de session | Quantité utilisée | Limite de quota | Niveau d'avertissement |
|------|-----|----------------------------|-------------------|-----------------|------------------------|
| OK | | SERVER_2K3\Invité | 0 octets | 100 Mo | 80 Mo |
| OK | | BUILTIN\Administrateurs | 0 octets | Illimité | Illimité |

Total de 2 élément(s), dont 0 sélectionnés.

Il est également possible d'importer et d'exporter des entrées de quota vers d'autre volume afin d'alléger les tâches administratives.

16. Gestion de la récupération en cas d'urgence

16.1. Sauvegarde des données

16.1.1. Vue d'ensemble de la sauvegarde des données

La sauvegarde est un processus simple qui consiste à dupliquer des informations d'un emplacement à un autre. Ceci permet de faire face aux situations d'urgences où les données ont été perdues. On peut alors utiliser une sauvegarde afin de restituer un environnement de travail pour reprendre la production de l'entreprise.

Reste à savoir quelles sont les informations à sauvegarder, sur quelle fréquence se feront les sauvegardes, et quel type de sauvegarde seront effectué.

16.1.2. Qui peut sauvegarder les données ?

Par défaut, seuls les membres des groupes suivant peuvent effectuer une sauvegarde :

- Administrateur
- Opérateurs de sauvegardes
- Opérateurs de serveurs

Sinon l'utilisateur doit soit être propriétaire du fichier qu'il souhaite sauvegarder, ou soit au moins avoir l'autorisation NTFS **lecture** sur le fichier en question.

16.1.3. Qu'est-ce que les données sur l'état du système ?

Dans le processus de sauvegarde, l'utilisateur a la possibilité (si il possède les autorisations requises) d'effectuer une sauvegarde de l'état du système. Il s'agit d'une sauvegarde de toutes les informations requises par le système d'exploitation pour son bon fonctionnement. Voici la liste des composants de l'état du système :

- Registre
- Fichiers de démarrage, inscriptions de classe Com+, y compris les fichiers système
- Base de données Services de certificats
- Service d'annuaire Active Directory
- Répertoire SYSVOL
- Information de service de cluster
- Métarépertoire IIS
- Fichiers système sous protection de fichiers Windows

16.1.4. Types de sauvegardes

L'utilisateur a la possibilité d'effectuer plusieurs types de sauvegardes en fonctions de la stratégie adoptée.

| Type de sauvegarde | Description | Désactivation de l'attribut archive |
|--------------------|---|-------------------------------------|
| Normal / Complète | Sauvegarde les fichiers et dossiers sélectionnés. | Oui |

| | | |
|--------------|--|-----|
| Copie | Sauvegarde les fichiers et dossiers sélectionnés | Non |
| Incrémentiel | Sauvegarde les fichiers et dossiers sélectionnés qui ont été modifiés depuis la sauvegarde normale ou incrémentielle | Oui |
| Différentiel | Sauvegarde les fichiers et dossiers sélectionnés qui ont été modifiés depuis la dernière sauvegarde | Non |
| Journalière | Sauvegarde les fichiers et dossiers sélectionnés qui ont été modifiés au cours de la journée | Non |

☞ Le logiciel de sauvegarde considère qu'un fichier a été sauvegardé si son attribut prêt à être archivé est désactivé.

16.1.5. Qu'est-ce que ntbacup ?

L'utilitaire de sauvegarde est aussi disponible en ligne de commande avec la syntaxe suivante :

```
ntbackup backup [systemstate] "nom de fichier bks" /J {"nom tâche"} [/P {"nom pool"}] [/G {"nom GUID"}] [/T {"nom bande"}] [/N {"nom média"}] [/F {"nom fichier"}] [/D {"description jeu"}] [/DS {"nom serveur"}] [/IS {"nom serveur"}] [/A] [/V:{yesno}] [/R:{yesno}] [/L:{flsln}] [/M {type sauvegarde}] [/RS:{yesno}] [/HC:{onloff}]
```

Cela permet de créer des scripts de sauvegarde, par contre il existe des limites à ce mode d'exécution :

- Avec l'outil en ligne de commande il n'est pas possible de sauvegarder des fichiers. On ne peut sauvegarder que des dossiers complets. Vous pouvez par contre pointer sur une sélection de sauvegarde (.bks) qui contient cette liste de fichier.
- La commande ne supporte pas les caractères joker comme * ou ? ce qui signifie que *.jpg n'enregistrera pas les fichiers .jpg dans la sauvegarde.

16.1.6. Qu'est-ce qu'un jeu de récupération automatique du système ?

L'utilitaire de sauvegarde propose l'utilisation de la **Récupération du système automatique** (ASR).

Cet outil permet d'effectuer une sauvegarde complète du système (sans les données personnels), sur disquette.

Ceci permettrait de restaurer le système si ce dernier de démarrer plus tel qu'il l'était au moment de la sauvegarde.

Bien que cet outil soit spécialisé dans la sauvegarde de l'état du système, il dispose d'une option, **Toute les informations sur cet ordinateur**, qui permet de sauvegarder non seulement l'état du système, mais également toutes les données stockées sur l'ordinateur.

16.2. Planification des opérations de sauvegarde

16.2.1. Qu'est-ce qu'une opération de sauvegarde planifiée ?

Il s'agit d'une opération de sauvegarde qui se déclenchera à une date et heure précise. Ceci permet d'éviter d'oublier une sauvegarde qui devrait être effectuée périodiquement, ou d'être physiquement présent pour lancer une sauvegarde en dehors des horaires de travail.

Plusieurs options de planification de sauvegarde sont disponibles :

| | |
|---------------------------------|--|
| Une fois | Une seule fois à une date et une heure spécifiques |
| Tous les jours | À l'heure spécifiée chaque jour |
| Toutes les semaines | À l'heure spécifiée chacun des jours spécifiés de la semaine |
| Tous les mois | À l'heure spécifiée une fois par mois |
| Au démarrage du système | Au prochain démarrage du système |
| A l'ouverture de session | À la prochaine ouverture de session par le propriétaire de l'opération de sauvegarde |
| Si inactif | Quand le système est resté inactif pendant un nombre de minutes donné |

16.2.2. Comment planifier une opération de sauvegarde ?

Vous pouvez planifier des sauvegardes régulières à l'aide de l'Assistant Sauvegarde ou Restauration pour que vos données archivées soient toujours à jour.

Vous devez avoir ouvert une session en tant qu'administrateur ou opérateur de sauvegarde pour planifier une opération de sauvegarde.



16.3. Restauration des données

16.3.1. Qu'est-ce que la restauration des données ?

La restauration des données est le processus de restitution des informations provenant d'une sauvegarde. On a souvent recours aux restaurations en cas d'urgence (sinistre).

16.4. Configuration des clichés instantanés

16.4.1. Qu'est-ce que les clichés instantanés ?

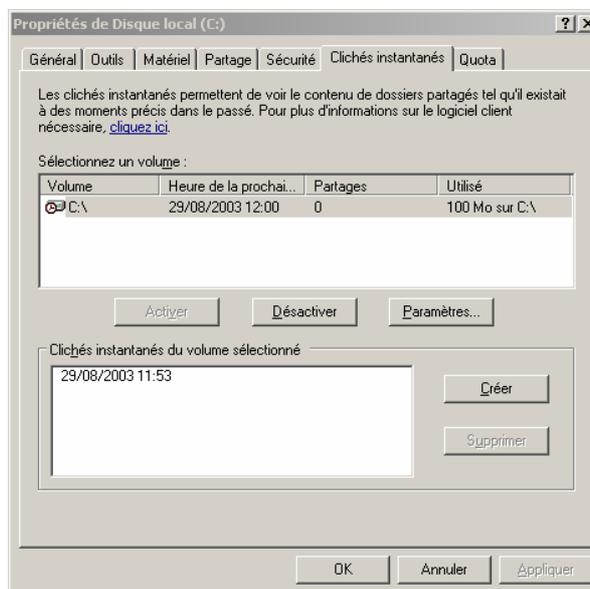
Un cliché instantané (shadow copy) est un système de récupération de donnée(s) partagée(s). Ainsi, à la suite d'une mauvaise manipulation d'un fichier présent sur un volume sur lequel on a activé les clichés instantanés, il va être possible d'accéder (en lecture seule) à une version précédente du document.

Les clichés instantanés sont désactivés par défaut.

16.4.2. Comment configurer des clichés instantanés sur le serveur ?

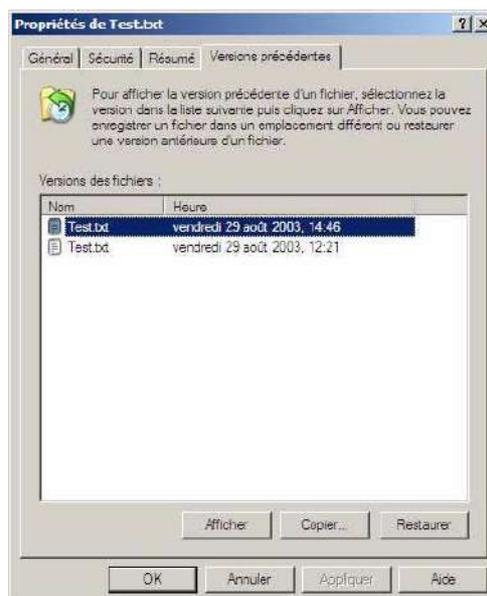
Il y a deux façons de d'activer les clichés instantanés sur un volume. Soit en utilisant la console **gestion de l'ordinateur**, soit en affichant les propriétés du volume et en sélectionnant l'onglet **Clichés instantanés**. Ensuite, il s'agit d'activer, ou désactiver la gestion de clichés instantanés.

Il est possible également de définir la quantité d'espace maximale exploitable pour la sauvegarde des clichés instantanés. Par défaut cette taille est fixée à 100 Mo.



16.4.3. Logiciel client pour les versions précédentes des clichés instantanés

Pour que les clients puissent accéder à une version précédente d'une ressource partagée, ils doivent au préalable installer le logiciel **Client pour version précédente**.



Ce logiciel est disponible sur le serveur Windows 2003 dans le dossier suivant :

`%systemroot%\WINDOWS\system32\clients\twclient\x86\twcli32.msi`

Ensuite pour pouvoir obtenir un listing des différentes versions d'une ressource partagée, il suffit d'afficher les **propriétés** du fichier, et d'aller dans l'onglet **Versions précédentes**.

16.5. Récupération suite à une défaillance du serveur

16.5.1. Contrôle des paramètres système au cours du processus d'amorçage

Windows 2003 Server fournit deux types de configuration pour démarrer un ordinateur : la configuration par défaut, et la dernière bonne configuration connue.

Les informations relatives à ces deux configurations sont stockées dans la base de Registre dans `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet` et `HKEY_LOCAL_MACHINE\SYSTEM\LastKnownGood`.

Lors de l'ouverture de session réussie, la configuration en cours de Windows est systématiquement sauvegardée en tant que dernière bonne configuration connue.

Ces options de démarrage sont accessibles en tapant sur la touche F8 au démarrage de l'ordinateur au menu de sélection du système d'exploitation.

Voici un tableau indiquant les cas où il faut ou non utiliser la dernière bonne configuration connue :

| Cas | Dernière bonne configuration connue |
|---|-------------------------------------|
| Après installation d'un nouveau pilote, Windows 2003 Server ne répond plus. | Oui |
| Désactivation accidentelle d'un pilote de périphérique essentiel. | Oui |
| Problème non lié à des changements de configuration de Windows 2003 Server. | Non |
| Après une ouverture de session | Non |
| Pannes matérielles, fichiers manquants ou endommagés. | Non |

16.5.2. Modification du comportement au démarrage à l'aide du fichier Boot.ini

Le fichier Boot.ini se compose de deux sections :

- [boot loader] qui contient le timeout et l'emplacement de l'OS à lancer par défaut.
- [operating systems] qui contient l'emplacement de l'ensemble des OS installés sur l'ordinateur.

Les emplacements des OS sont indiqués grâce à des chemins ARC (Advanced RISC Computing). Cette notation permet d'indiquer la ou les partitions sur lesquelles le(s) système(s) résident. Le tableau suivant contient une description de chaque élément du chemin de nom.

| Convention | Description |
|--------------|--|
| scsi(x) | Spécifie un contrôleur SCSI sur lequel le BIOS SCSI n'est pas actif. La variable x représente un chiffre qui indique l'ordre de chargement du contrôleur. La numérotation du contrôleur commence à 0. |
| multi(x) | Spécifie n'importe quel contrôleur qui n'utilise pas la convention SCSI(x), en l'occurrence, les contrôleurs IDE et les contrôleurs SCSI avec BIOS actif. La variable x représente un chiffre qui indique l'ordre de chargement du contrôleur. La numérotation du contrôleur commence à 0. |
| disk(y) | L'identificateur SCSI du disque lorsque le BIOS du contrôleur SCSI n'est pas actif. La numérotation commence à 0. |
| rdisk(z) | Le numéro qui identifie le disque sur lequel le système d'exploitation réside lorsque multi identifie le contrôleur. La numérotation commence à 0. |
| partition(a) | Spécifie la partition sur laquelle le système d'exploitation réside. La numérotation commence à 1. |

Voici un exemple de fichier boot.ini:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows 2003 Server"
```

Ce fichier décrit un ordinateur qui utilise Windows 2003 Server comme OS par défaut. Cet OS se trouve sur un contrôleur IDE ou SCSI avec BIOS actif, sur le premier disque, sur la partition 1.

16.5.3. Utilisation des options d'amorçage avancées pour résoudre les problèmes de démarrage

Le **mode sans échec** est le mode de diagnostic le plus souvent utilisé pour résoudre des problèmes de démarrage du système. Il permet de lancer Windows avec un nombre minimum de pilotes. Ainsi, si l'installation d'un nouveau logiciel empêche Windows de démarrer normalement, il est toujours possible de lancer ce dernier en mode sans échec, et à partir de là, modifier le paramètre du logiciel qui pose problème, ou tout simplement le supprimer.

Ce mode, est accessible en tapant sur la touche F8 au démarrage de l'ordinateur, au niveau de la sélection de l'OS à lancer.

16.5.4. Utilisation de la console de récupération pour démarrer l'ordinateur

La console de récupération peut être utilisée dans le cas où les deux solutions proposées précédemment ne fonctionnent pas. Il faut cependant avoir le mot de passe administrateur de la machine pour pouvoir l'utiliser.

Cette console permet d'effectuer les tâches suivantes :

- Démarrer et arrêter de services
- Reconfigurer les services qui empêchent l'ordinateur de démarrer correctement
- Formater les lecteurs sur un disque dur
- Lire et écrire des données sur un disque formaté en FAT ou NTFS
- Réparer le système en copiant un fichier à partir d'une disquette ou d'un CD-ROM
- Autres tâches d'administration

L'installation de la console de récupération se fait à partir du CD-ROM d'installation de Windows 2003 Server. Tapez la commande ci-dessous à partir de l'invite de commande en basculant sur le lecteur CD-ROM (d : par exemple):

D:\i386\winnt32.exe /cmdcons

Il est également possible de lancer la console de récupération en bootant avec le CD-ROM d'installation de Windows 2003 Server, et en tapant r au menu « Bienvenue ! » du CD.

Ensuite pour lancer la console de récupération à partir du menu, choisissez l'OS à démarrer, puis sélectionnez l'installation à récupérer, et enfin entrez le mot de passe administrateur. Utilisez ensuite la commande **help** pour obtenir la liste des commandes accessibles.

16.6. Choix d'une méthode de récupération en cas d'urgence

16.6.1. Quels sont les outils de récupération en cas d'urgence ?

Ce tableau résume les outils à utiliser en cas d'urgence :

| | |
|---|---|
| Mode sans échec | À utiliser quand un problème empêche le démarrage normal de Windows Server 2003 |
| Dernière bonne configuration connue | À n'utiliser que si la configuration est incorrecte et que l'utilisateur n'a pas déjà ouvert de session depuis la modification qui pose problème. |
| Sauvegarde | À utiliser pour créer une copie des données sur le disque dur et l'archiver sur un autre périphérique de stockage |
| Console de récupération | À utiliser si vous ne pouvez pas corriger les problèmes avec une des méthodes de démarrage |
| Récupération système automatique (ASR) | À utiliser lors de la restauration des données d'une sauvegarde |

17. Maintenance des logiciels à l'aide des services SUS

17.1. Présentation des services SUS

17.1.1. Qu'est-ce que Windows Update ?

Windows Update est l'extension en ligne de Windows qui vous permet de maintenir votre ordinateur parfaitement à jour. Utilisez Windows Update pour choisir les mises à jour que vous souhaitez appliquer au système d'exploitation, aux logiciels et au matériel de votre ordinateur. Le contenu du site Web de Windows Update est amélioré régulièrement, de sorte à toujours vous proposer les mises à jour et les solutions les plus récentes pour protéger votre ordinateur et en assurer le fonctionnement optimal. Windows Update analyse votre ordinateur et vous propose ensuite une sélection de mises à jour entièrement personnalisée, qui s'applique uniquement aux logiciels et au matériel dont vous disposez.

17.1.2. Qu'est-ce que la fonctionnalité Mises à jour automatiques ?

La fonctionnalité de mise à jour automatique permet de configurer et de planifier une installation automatisée des mises à jour de Windows.

Plusieurs options vous sont proposées :

- Vous êtes prévenus avant de télécharger une nouvelle mise à jour et juste avant de l'installer.
- Les nouvelles mises à jour sont téléchargées, et vous êtes prévenus juste avant de les installer.
- Les nouvelles mises à jour sont téléchargées et installées selon la planification de votre choix.

17.1.3. Comparaison entre Windows Update et la fonctionnalité Mises à jour automatiques

Windows Update et la fonctionnalité Mises à jour automatiques sont deux composants distincts conçus pour fonctionner ensemble et assurer la sécurité des systèmes d'exploitation Windows.

- **Windows Update** est un site Web Microsoft sur lequel les utilisateurs de Windows peuvent télécharger des logiciels cruciaux et non cruciaux.
- La fonctionnalité **Mises à jour automatiques** vous permet d'interagir automatiquement avec le site Web Windows Update pour obtenir les mises à jour critiques des logiciels. En tant qu'administrateur système, vous contrôlez totalement le niveau de cette interaction avec la fonctionnalité Mises à jour automatiques, à l'aide des services SUS.

17.1.4. Qu'est-ce que les services SUS ?

Le service SUS, qui est disponible depuis Windows 2000, a pour rôle de consulter Windows Update régulièrement (via des planifications), et de télécharger des mises à jour.

Ces Mises à jour sont ensuite stockées en interne, et sont disponibles pour tous les serveurs et clients Windows du réseau. Il s'agit en quelque sorte d'un Proxy pour mises à jour.

L'administrateur devra ensuite configurer les clients pour planifier leurs connections vers le(s) serveur(s) SUS afin d'effectuer les mises à jour. Cette configuration peut être effectuée en utilisant une GPO.

L'intérêt principal des services SUS est de pouvoir tester une mise à jour sur un nombre restreint de machine, puis de publier ces mises à jour si celles-ci se sont déroulées correctement sur les machines de test.

17.2. Installation et configuration des services SUS

17.2.1. Qu'est-ce qu'un point de distribution du serveur de service SUS ?

Le service SUS permet l'utilisation de point de distribution. Il s'agit de serveurs présents sur le réseau qui hébergeront les fichiers de mise à jours téléchargés. Cependant, par défaut, le serveur exécutant le service SUS est le point de distribution.

17.2.2. Configurations de serveur requises pour les services SUS

La configuration minimale pour exécuter le service SUS est la suivante.

Matériel :

- Pentium III 700 Mhz ou supérieur
- 512 Mo de mémoire vive
- 6 Go d'espace disponible

Logiciel :

- Windows 2000 SP2 ou supérieur, ou Windows 2003 Server
- IIS 5.0 ou version ultérieur
- IE 6.0 ou supérieur

17.2.3. Comment installer et configurer les services SUS ?

Le service SUS n'est pas directement disponible sur Windows 2003, l'administrateur réseau doit se connecter à l'adresse suivante pour télécharger cet outil :

<http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>.

17.2.4. Configuration de la fonctionnalité Mises à jour automatiques



La fonctionnalité **Mises à jour automatiques** représente la partie cliente de SUS. Ce client (présent sur tous les systèmes depuis Windows 2000) permet de maintenir à jour les différents patch du système en choisissant un mode opératoire parmi les 3 suivantes :

- Le système avertit l'administrateur avant le téléchargement des mises à jour et avant l'installation des mises à jour téléchargées.
- Le téléchargement des mises à jour s'effectue automatiquement, et le système avertit un administrateur avant l'installation des mises à jour.
- Le téléchargement et l'installation des mises à jour s'effectuent suivant une planification spécifiée.

Pour définir la source ou se connecte **Mises à jour automatiques** il vous suffit de modifier dans une stratégie de groupe (GPO) la configuration (Configuration de l'ordinateur\Modèles d'administration\Composants Windows\Windows Update).