

## Principes d'administration Windows

### Administration Système et Réseaux, Sécurité

#### Administration Windows

Philippe Harrand

<sup>1</sup>Département Informatique  
Pôle Sciences et Technologies

<sup>2</sup>Direction Territoriale Sud Ouest  
France Télécom

25 novembre 2007

#### Les utilisateurs

Droits

Partages

Authentification distante

## Groupes

- ▶ Les groupes contrôlent les droits des utilisateurs
- ▶ Types de groupes
  - ▶ Groupes créés
  - ▶ Groupes intégrés
    - ▶ Créés automatiquement
    - ▶ Ne peuvent pas être supprimés
    - ▶ L'installation d'un service crée le groupe correspondant
  - ▶ Groupes prédéfinis
    - ▶ Administrateurs locaux
    - ▶ Administrateurs de domaine
    - ▶ Utilisateurs avec pouvoirs
    - ▶ Utilisateurs
    - ▶ Invités
    - ▶ ...
- ▶ Un utilisateur peut appartenir à plusieurs groupes

## Types d'utilisateurs

- ▶ Utilisateurs locaux
  - ▶ Authentifiés sur la machine locale
  - ▶ Utilisés sur une machine isolée
- ▶ Utilisateurs de domaine
  - ▶ Authentifiés sur un "Contrôleur de Domaine"
  - ▶ Gestion centralisée
- ▶ Utilisateurs prédéfinis
  - ▶ Administrateur (ou administrator)
  - ▶ Invité
  - ▶ IUSR\_<nom de machine> (accès à IIS)
  - ▶ IWAM\_<nom de machine> (lancement de services)

## Stratégies de groupes

- ▶ Stratégies
  - ▶ Sécurité
  - ▶ Installation logiciels
  - ▶ Scripts de démarrage et d'arrêt
  - ▶ Ouverture et fermeture de session
  - ▶ Redirection de dossiers
- ▶ Locale
  - ▶ %Systemroot%\system32\groupPolicy
  - ▶ Créer une MMC *Stratégie de sécurité locale*
- ▶ non locale
  - ▶ Stocké sur le Contrôleur de Domaine
  - ▶ Dans un dossier ou un conteneur **GPT**
  - ▶ Concerne un site, un domaine ou une Unité d'Organisation
  - ▶ Ecrase la stratégie locale

## Droits sur les fichiers

- ▶ FAT (16 / 32)
  - ▶ lecture seule
  - ▶ fichier caché
- ▶ NTFS
  - ▶ Droits FAT
  - ▶ contrôle total
  - ▶ modifier
  - ▶ lecture et exécution
  - ▶ afficher le contenu du dossier
  - ▶ lecture
  - ▶ écriture
  - ▶ Autorisations avancées
- ▶ Appliqués à des groupes et/ou à des utilisateurs
- ▶ + groupes virtuels
  - ▶ tout le monde
  - ▶ utilisateurs authentifiés
  - ▶ ANONYMOUS LOGON
  - ▶ TACHE
  - ▶ CREATEUR PROPRIETAIRE, GROUPE CREATEUR
  - ▶ RESEAU
  - ▶ SYSTEM
  - ▶ UTILISATEUR TERMINAL SERVEUR
- ▶ Héritage (Ce dossier, ses sous dossiers et les fichiers qu'ils contiennent)

## Partages

- ▶ Permettre l'accès distant à un répertoire
- ▶ SMB sur (NETBIOS sur TCP/IP) ou sur IPX/SPX
- ▶ Autorisations :
  - ▶ Aucun accès
  - ▶ Contrôle total
  - ▶ Modifier : correspond au droits d'écriture d'UNIX
  - ▶ Lire : correspond aux droits « lecture » ET « exécution » d'UNIX
- ▶ Imprimantes
  - ▶ Imprimer
  - ▶ Gestion des imprimantes
  - ▶ Gestion de documents
  - ▶ Ces autorisations s'appliquent aux groupes listés plus haut.

## Partages administratifs

- ▶ ADMIN\$ : répertoire d'installation du système
- ▶ LettreLecteur\$ (C\$, D\$, etc.)
- ▶ IPC\$ : communication entre programmes et administration à distance
- ▶ Print\$ : imprimantes
- ▶ REPL\$ : créé lorsqu'un serveur de réplication est configuré
- ▶ Les partages dont le nom se termine par un \$ ne sont pas affichés dans la fenêtre « connecter un lecteur réseau »

## Domaine

- ▶ Ensemble de machines gérées par un ou plusieurs **Contrôleurs de domaine** utilisant le même suffixe
- ▶ Serveur d'authentification
- ▶ Données stockées dans un serveur  $\cong$  LDAP nommé **Active Directory**
- ▶ Nécessite une licence Windows 2000 Server ou Windows 2003 Standard Edition, Enterprise Edition ou Datacenter Edition
- ▶ Attention, le service d'annuaire Active Directory ne peut pas être installé sur Windows 2003 Server Web Edition.
- ▶ Un serveur DNS spécial (il est préférable qu'il soit intégré à l'**AD**)

## Administration de l'AD

- ▶ Notion de *forêt*
  - ▶ Ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun
  - ▶ Dont tout les objets sont accessible par un quelconque **AD**
- ▶ Relation d'Approbation
  - ▶ Extension des droits des membres d'un domaine à un autre domaine
  - ▶ Par défaut bidirectionnelle transitive

## Consoles MMC

- ▶ Microsoft Management Console
- ▶ Méthode standard pour créer, enregistrer et ouvrir des outils d'administration appelés consoles
- ▶ Héberge des applications de gestion, les composants logiciels enfichables
  - ▶ Administrer des tâches et résoudre des problèmes
  - ▶ Centraliser l'administration
  - ▶ Administrer des tâches et résoudre des problèmes à distance
  - ▶ Contiennent un ou plusieurs composants logiciels enfichables (extension .msc)
- ▶ Vous pouvez créer vos propres consoles personnalisées en associant plusieurs composants logiciels enfichables préconfigurés à des composants logiciels enfichables tiers

## Créer une Console MMC

- ▶ Démarrer / Exécuter : Taper mmc
- ▶ Ajouter/Supprimer un composant logiciel enfichable
- ▶ Ajouter et sélectionner le composant
- ▶ Personnaliser le composant

## Outils d'administration de l'AD

### ▶ Consoles

- ▶ Utilisateurs et ordinateurs Active Directory
- ▶ Sites et Services Active Directory
- ▶ Domaines et approbations Active Directory
- ▶ Schéma Active Directory  
ouvrir une invite de commande et taper `regsvr32 schmmgmt.dll`
- ▶ Gestion des Stratégies de Groupe  
non disponible sur le CD-ROM de Windows 2003 Server, le télécharger sur le site de Microsoft
- ▶ ADSI Edit : Visualiser l'arborescence LDAP réelle du service d'annuaire

### ▶ commandes

- ▶ Lpc.exe : envoyer des requêtes LDAP vers Active Directory, NDS, Open LDAP, ...
- ▶ Dsadd, dsmod, dsrm, dsget, dsquery, dsmove : équivalent ldapadd, ldapmod, ...
- ▶ Ldifde : permet d'importer/exporter des données à partir d'un fichier texte vers Active Directory et réciproquement
- ▶ Csvde : importer des comptes d'utilisateurs à partir d'un fichier texte vers Active Directory
- ▶ WSH : exécuter des scripts en VBS ou en JScript sur une plateforme Windows 9x ou NT.

## Configuration des clients

### ▶ Chaque poste client doit être configuré par un Administrateur

- ▶ Click droit sur *Poste de travail*
- ▶ ⇒ propriétés
- ▶ ⇒ Identification Réseau
- ▶ ⇒ Propriétés
- ▶ ⇒ Domaine et indiquer le nom du domaine
- ▶ ⇒ Saisir les crédeniels de l'administrateur du Contrôleur de Domaine
- ▶ Redémarrer

## SAMBA

### ▶ SAMBA ⇒ serveur de domaine

- ▶ domain logons = yes
- ▶ domain master =yes
- ▶ name resolve order = wins host lmhosts bcast
- ▶ wins support = yes
- ▶ Créer les partages Netlogon et Profiles
- ▶ Netlogon ⇒ lecture pour tous
- ▶ Profiles ⇒ écriture par tous mais *sticky bit*

### ▶ SAMBA ne peut pas encore remplacer un **AD** (2007)

### ▶ SAMBA joint à openLDAP peut simuler un **AD** pour l'authentification

### ▶ SAMBA peut utiliser un **AD** existant