3 SERVEUR DE FICHIERS

3.1 PARTAGE D'UN RÉPERTOIRE

Cette section décrit comment partager un répertoire sur une poste de travail Windows 2000.

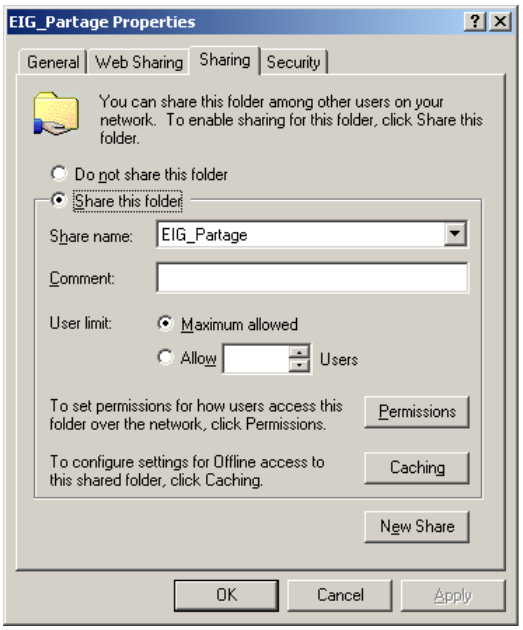
1. Vérifier dans ***My Computer – Control Panel – Network and Dial-up Connections – Local Area Connection – Properties*** que l'option ***File and Printer Sharing for Microsoft Networks*** est bien activée. Sinon, on ne peut pas partager des ressources.

2. Cliquer sur le répertoire qu'on désire partager. Afficher ***Properties* – Onglet *Sharing* – *Share this folder*** (figure 3.1). Entrer un nom (*Share Name*) pour le partage et une petit description (*Comment*).

3. Sur *Permissions*, configurer les différentes autorisations voulues (autorisations de partage → § 2.3) au **niveau réseau**.

4. Dans l'onglet ***Security***, configurer les autorisations **locales** (→ § 2.2).

FIGURE 3.1 : PARTAGE D'UN RÉPERTOIRE



3.2 AUDIT

3.2.1 Définition de la stratégie d'audit

La stratégie d'audit peut être appliquée de deux manières :

- localement : pour cela il faut exécuter ***My Computer – Control Panel – Administrative Tools – Local Security Policy*** sur l'ordinateur où on désire auditer.

- pour le domaine : la configuration s'effectue sur le contrôleur de domaine en utilisant la console de gestion (MMC – *Microsoft Management Console*) : ***Run… – mmc – Console – Add/Remove Snap-in… – Add… – Group Policy*** et sélectionner ***Default Domain Policy*** à la place de *Local Computer*.

Dans notre cas, la stratégie d'audit est appliquée localement sur les deux serveurs de fichiers (→ § 5.5).

Cliquez sur ***Local Policies*** – ***Audit Policy*** – ***Audit object access*** et activer la réussite (*Success*) et l'échec (*Failure*).
Il existe neuf stratégies d'audit différentes :

- *Audit account logon events* : Un contrôleur de domaine a reçu une demande de validation d'un compte d'utilisateur.
- *Audit account management* : Un administrateur a crée, modifié ou supprimé un compte d'utilisateur ou un groupe. Un compte d'utilisateur a été renommé, désactivé ou activé, ou un mot de passe a été défini ou modifié.
- *Audit directory service access* : Un utilisateur a accédé à un objet d'Active Directory. Pour que cela fonctionne, il faut configurer des objets d'Active Directory à auditer.
- *Audit logon events* : Un utilisateur a ouvert ou fermé un session, ou a établi ou annulé une connexion réseau à l'ordinateur.
- *Audit object access* : Un utilisateur accède à un fichier, un dossier ou une imprimante. Pour que cela fonctionne, il faut configurer les fichiers, dossiers ou imprimantes à auditer.
- *Audit policy change* : Une modification a été apportée aux options de sécurité, aux droits des utilisateurs ou aux stratégies d'audit.
- *Audit privilege use* : Un utilisateur a exercé un droit, tel que la modification de l'heure système.
- *Audit process tracking* : Un programme a exécuté une action. Ces informations s'adressent principalement aux développeurs désireux de connaître les détails de l'exécution d'un programme.
- *Audit system events* : Un utilisateur a redémarré ou arrêté l'ordinateur, ou encore un événement affectant la sécurité de Windows 2000.

3.2.2 Activation de l'audit pour des ressources spécifiques

Certaines stratégies d'audit fonctionne dès qu'elles sont activées. Pour les autres, il faut définir quels objets doit être audité.

La configuration suivante explique les différentes étapes pour la stratégie *Audit object access*.

1. Choissiez un répertoire ou un fichier qui doit être audité. Dans notre cas, le répertoire partagé est audité.

2. Affichez ses *Properties* et cliquez sur l'onglet ***Security – Advanced… – Auditing***.

3. Il faut définir le type (***Success*** ou ***Fail***), à quel utilisateur ou groupe cet audit s'applique et quel(s) accès est (sont) audité(s) (***Read Data***, ***Write Data***, ***Delete***, etc.).
   Pour cela cliquez sur ***Add…***, sélectionnez l'utilisateur ou le groupe d'utilisateur et parmi les différents types d'accès, cochez ceux qui doivent être audité (figure 3.2).

FIGURE 3.2: AUDIT D'UN RÉPERTOIRE