Gestion centralisée des attributs de sécurité du Système de Fichiers, du Registre et des groupes de sécurité d'un parc de machines XP en réseau Windows Server 2003

Mise à jour: 05/05/2007

Microsoft facilite de plus en plus la tâche des administrateurs-réseaux en leur permettant de configurer de manière centralisée les attributs de sécurité pour tous les fichiers et dossiers existants dans le système de fichiers local, pour les clés de Registre et pour les services système existants sur l'ordinateur local.

Les utilisateurs du Domaine ont, par défaut, des droits restreints sur certains dossiers et sur le Registre. Nous allons décrire, pas à pas, une méthode, exploitant Active Directory, qui va permettre de modifier les droits qui s'appliquent à l'un quelconque des dossiers X d'une partie ou de la totalité des machines XP du parc, en agissant sur le serveur et sur *une seule* machine du Parc.
Ce qui suit pourra aisément être transposé à tout dossier X résidant sur des machines XP rattachées au Domaine.

Par exemple, les Utilisateurs du Domaine ne possèdent pas le droit de modification et d'écriture dans *%systemroot%\temp* et cela peut constituer un problème pour certains logiciels qui y créent des fichiers temporaires. Il faut donc, dans ce cas, et pour avant hier, attribuer, à la connexion de ces utilisateurs, les droits requis, sur l'ensemble des machines.

Le lecteur adaptera les notations à sa situation ; dans ce document :

Dossier X: *%systemroot%\temp*

Nom machine XP « modèle »: *C7WXP*

Unité Organisationnelle S contenant C7WXP : *Salle001*

Domaine du serveur: *pai.di*

Nom du serveur 2003: *Dell2k*

Login conseillé: *tout membre du groupe global « Admins du domaine »*

ETAPE 0: Pré-requis

• SERVEUR : Windows 2000 (minimum SP3) ou Windows 2003
• CLIENT : Windows XP (minimum SP1)

Quelque soient les sytèmes d'exploitations, des Hotfixes doivent être appliqués, car la gestion sur les différentes machines des stratégies et de leurs fichiers adm peut générer des messages Pop-up indésirables :

Mise à jour pour Windows 2000 : KB842933
http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=ba478b46-3af7-4eaf-9ce6-e34ea2c74faf

Mise à jour pour Windows XP : KB842933
http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=3c599574-0f8d-4c2c-b3be-ebf3fb041214

Mise à jour pour Windows Server 2003 : KB842933
http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=532a4cd0-f2ce-4fa7-92ab-ac336ad18409

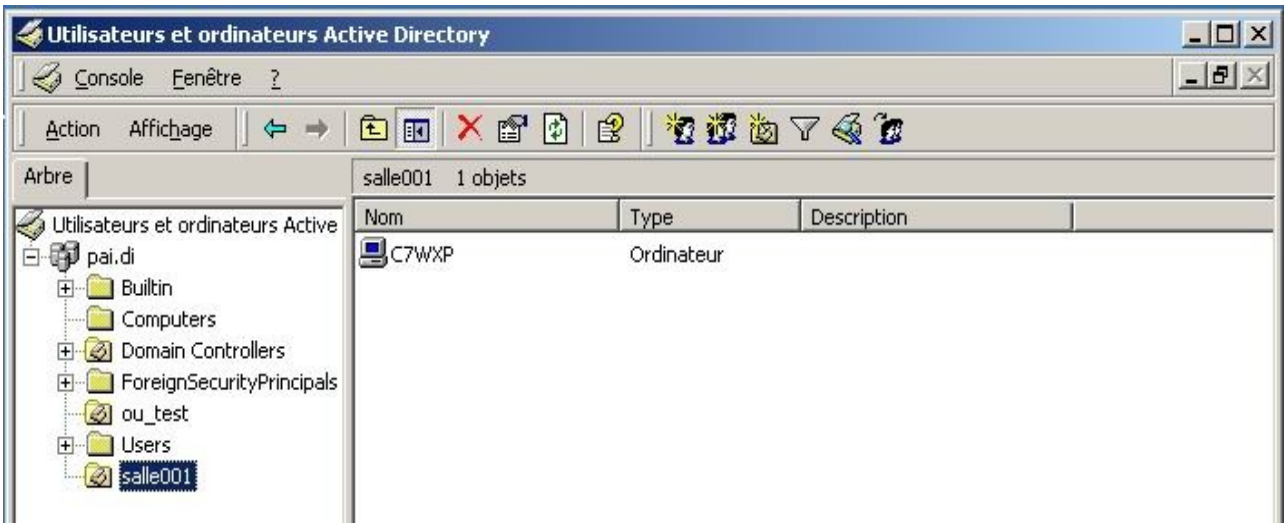
ETAPE 1: Préparation d'Active Directory

On peut opérer directement sur le serveur ou de manière distante selon la configuration existante ; prendre un café avant de cocher au moins une case:

- L'onglet « Bureau à distance » de l'utilitaire système du panneau de configuration du serveur est-il activé ?
- Les outils d'administration-serveur (Adminpak.msi) ont-ils été installés sur le poste XP?
- Je suis conquis par l'usage des consoles mmc (Menu démarrer / Exécuter / mmc)
- Je préfère me déplacer physiquement dans le local-serveur

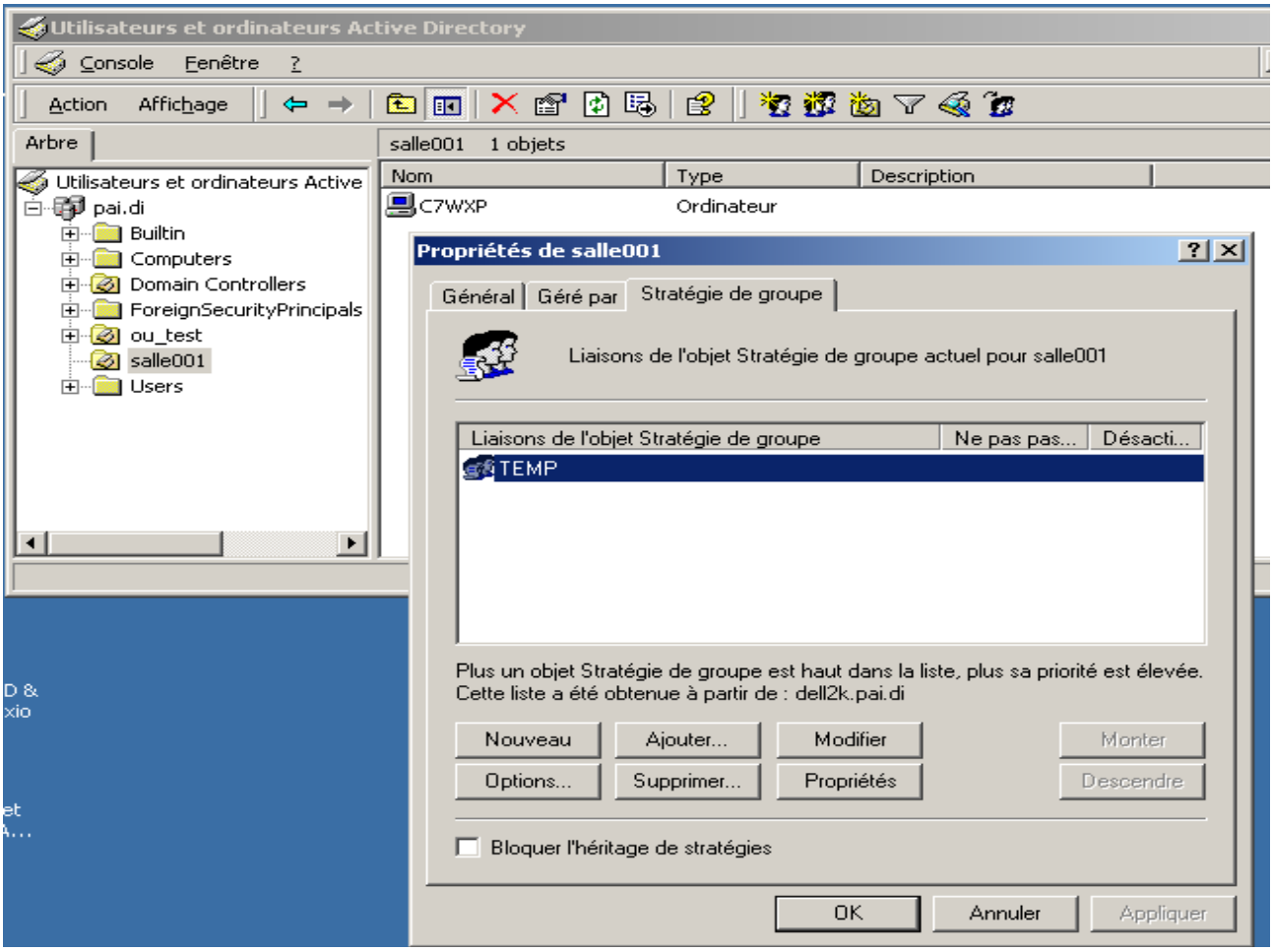
Lancer alors une console « Utilisateurs et Ordinateurs Active Directory ».

Les machines d'une même salle, initialement enregistrées dans l'Unité Organisationnelle « Computers » peuvent facilement être déplacées dans la nouvelle Unité Organisationnelle Salle001 ; par exemple, pour C7WXP :



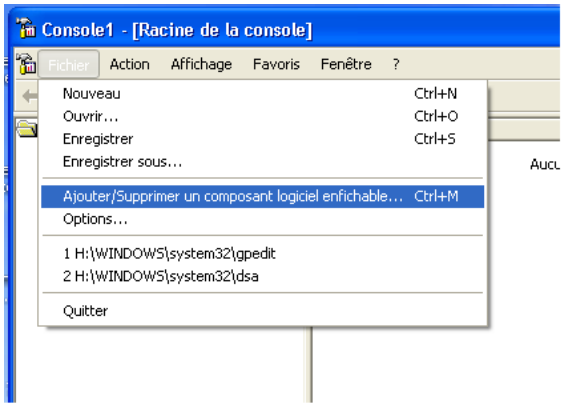
Dans les propriétés de l' Unité Organisationnelle Salle001, demander une nouvelle stratégie au nom explicite TEMP (pour s'y retrouver aisément par la suite). Valider.

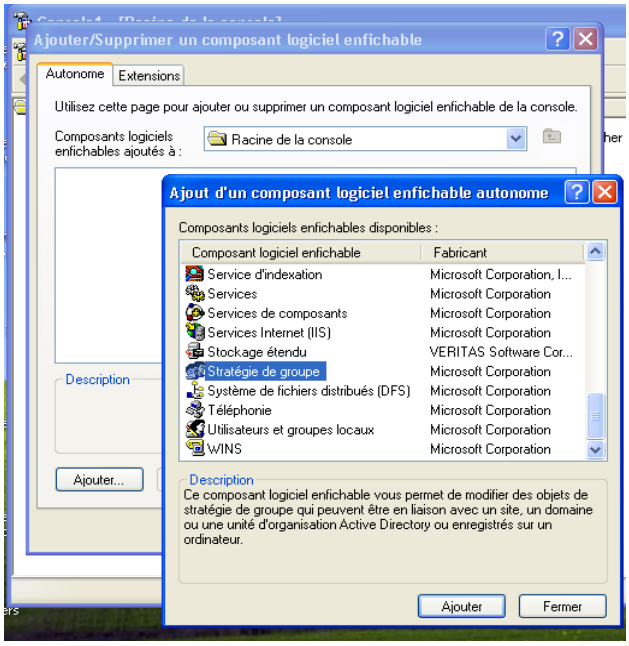
Il y a désormais dans Active Directory une stratégie qui s'appliquera à toutes les machines déplacées dans l' Unité Organisationnelle Salle001 ; il reste à la peaufiner ...



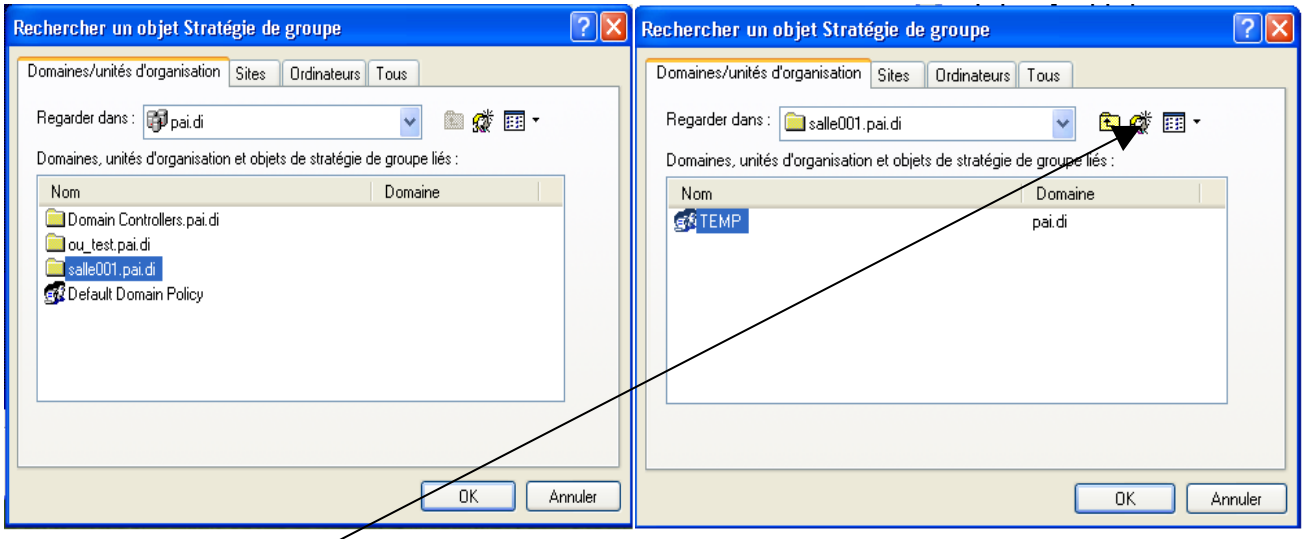
ETAPE 2: *Gestion des attributs de sécurité*

Ouvrir, sur la machine-modèle, une console mmc. Menu Fichier: Ajouter Composant logiciel enfichable, Sélectionner l'objet « Stratégie de groupe »:





L'ajouter, puis, à l'aide du bouton « parcourir », pointer l' Unité Organisationnelle Salle001, double-cliquer afin qu'apparaisse la stratégie de groupe TEMP précédemment créée:

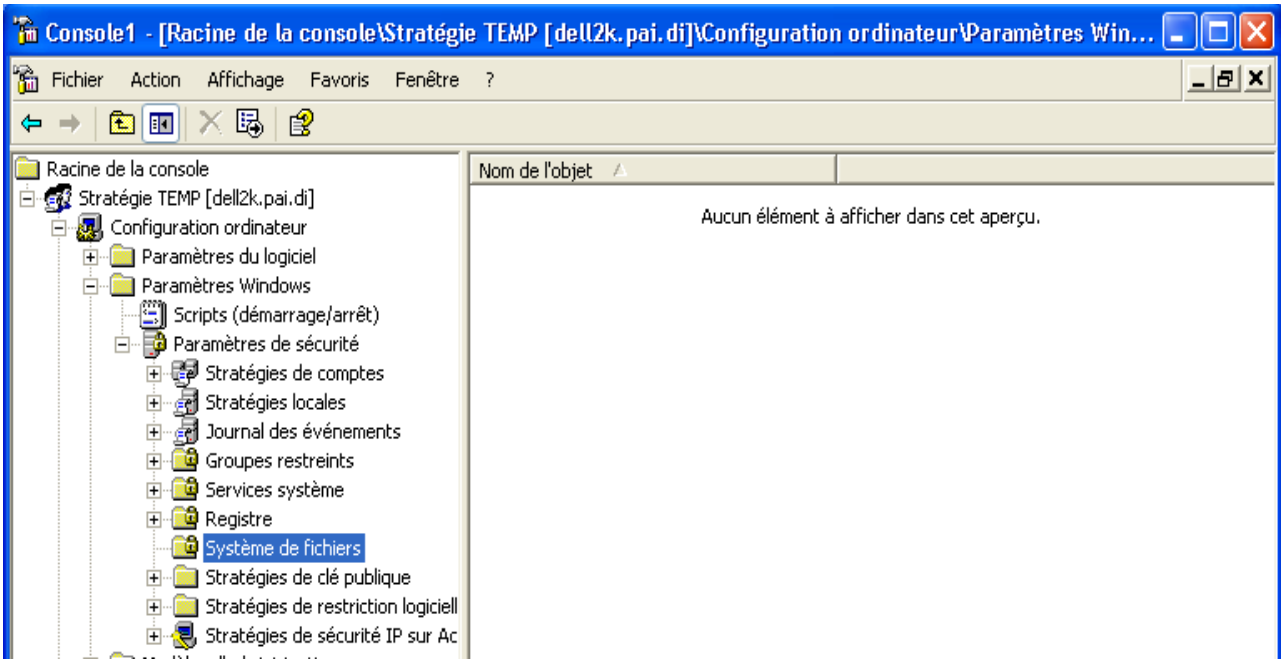


Remarquer, à ce stade, que la console permet de créer à distance une nouvelle stratégie par le bouton

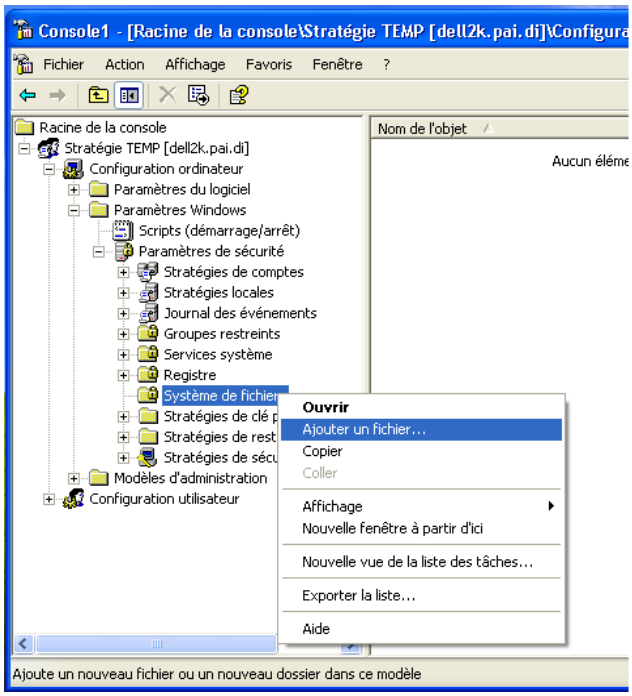
Tout valider. La console est prête. L'enregistrer, par exemple sur le bureau, car il y a tout de même une bonne série de clics pour la créer!

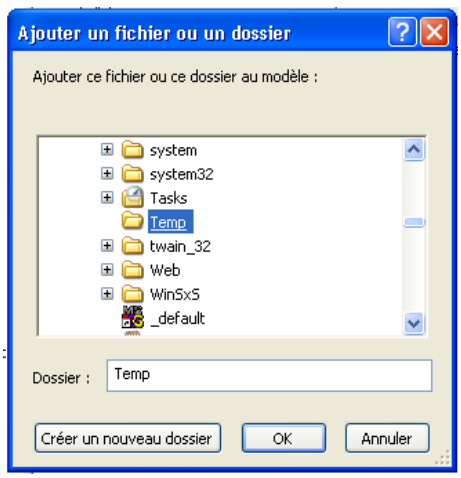
Dans l'arborescence de la console, rechercher:

Nom de l'objet Stratégie
Configuration de l'ordinateur
Paramètres de Windows
Paramètres de sécurité
Système de fichiers



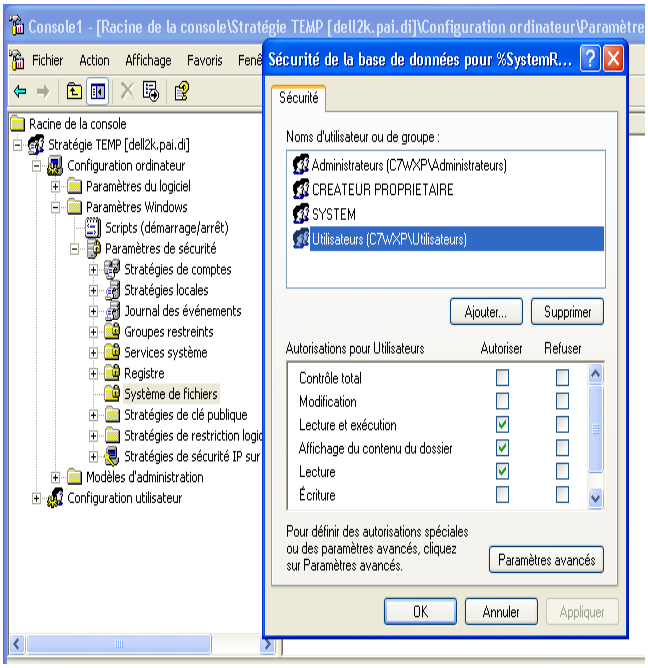
Faire un clic droit sur « Système de fichiers », ajouter le fichier ou le dossier convoité (ici, pour l'exemple %systemroot%\temp) :

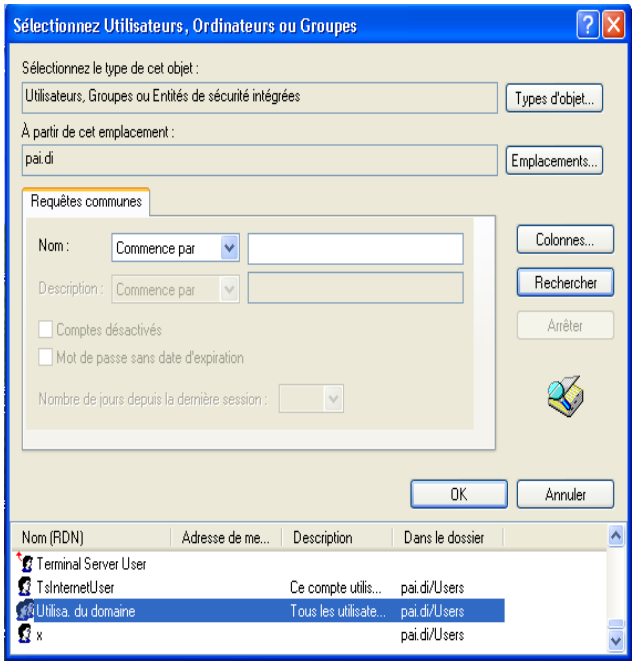




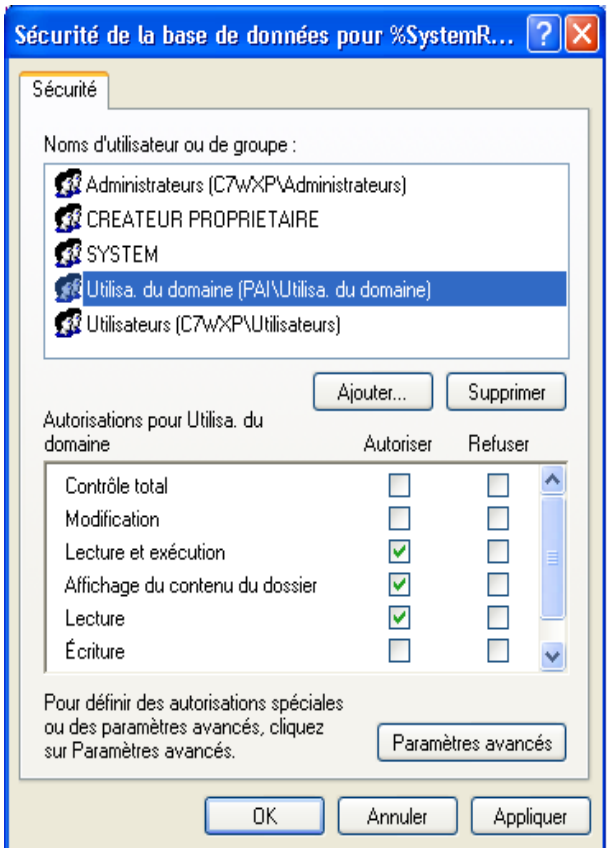
V / X

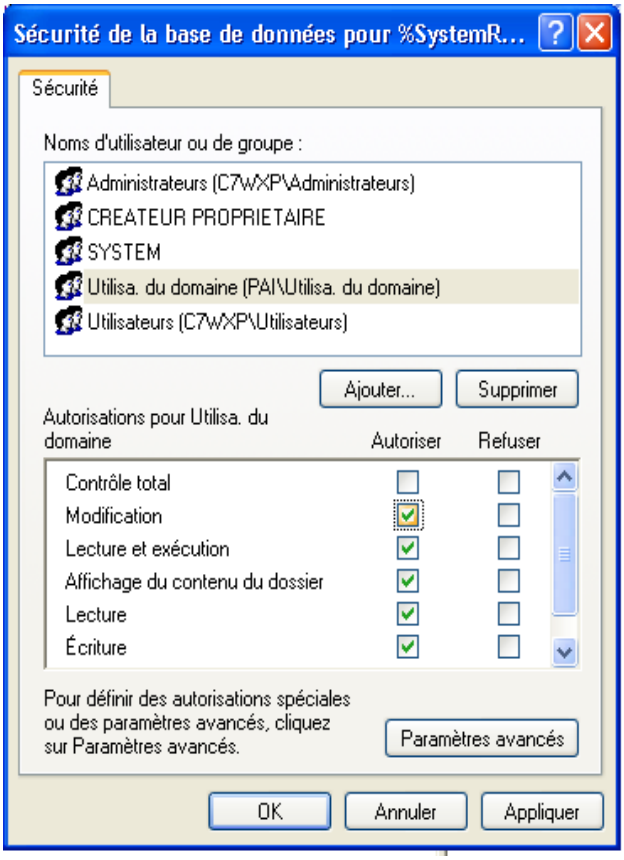
Valider. Aussitôt, la fenêtre de sécurité s'affiche ; faire ajouter, Avancé, Rechercher, afin de sélectionner les utilisateurs concernés :





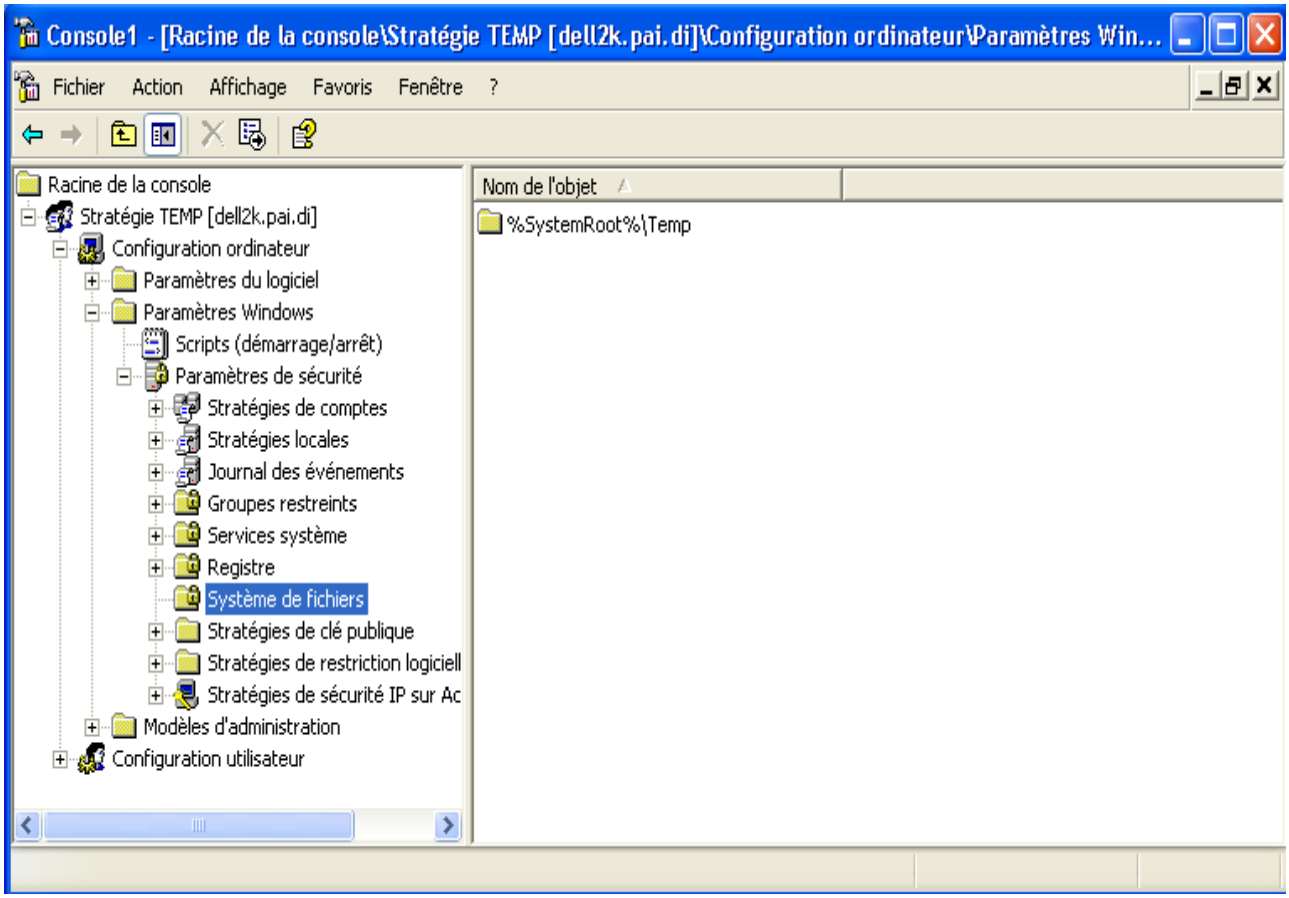
Valider deux fois et attribuer les droits souhaités aux utilisateurs concernés. Valider encore.





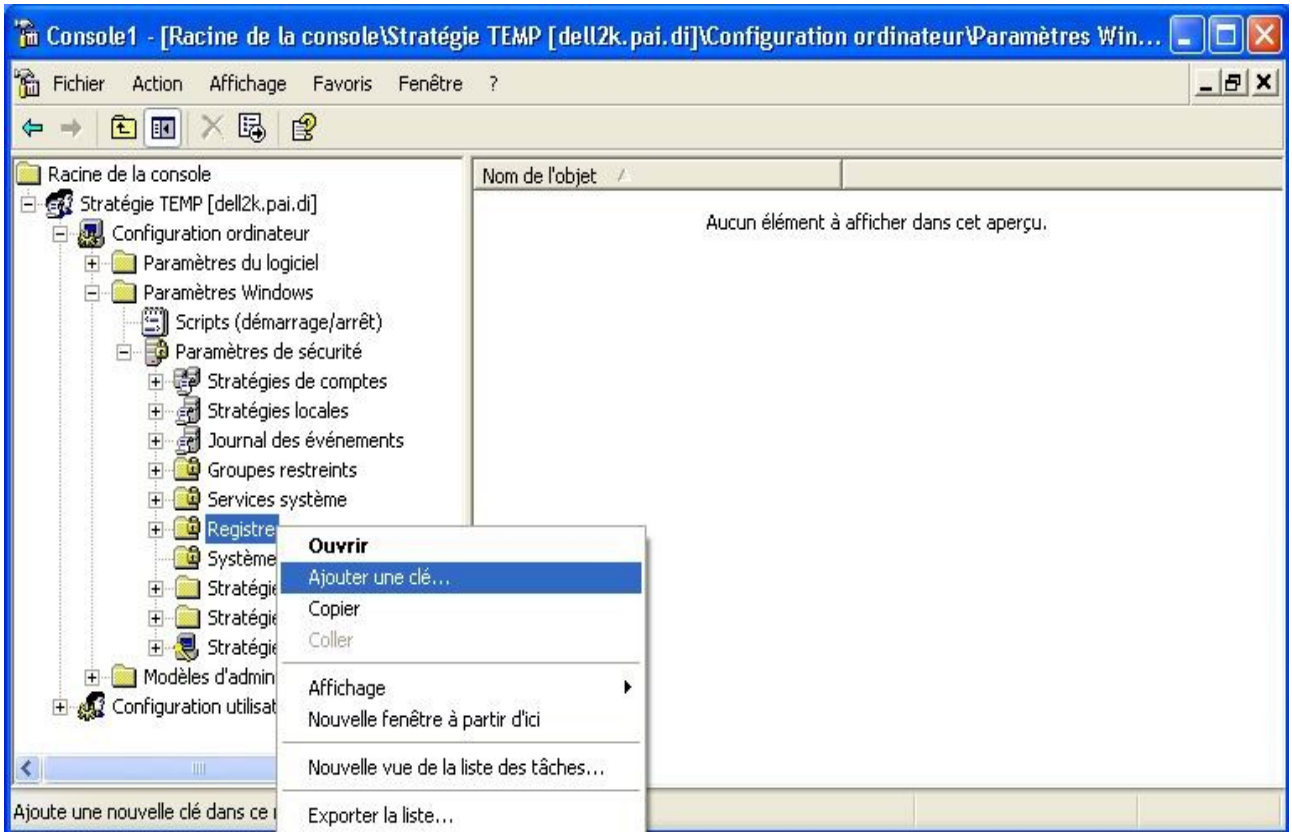
Demander le remplacement des autorisations existantes puis valider :

Après actualisation d'Active Directory (faire gpupdate), la stratégie TEMP sera appliquée sur toutes les machines contenues dans l'Unité Organisationnelle Salle001.



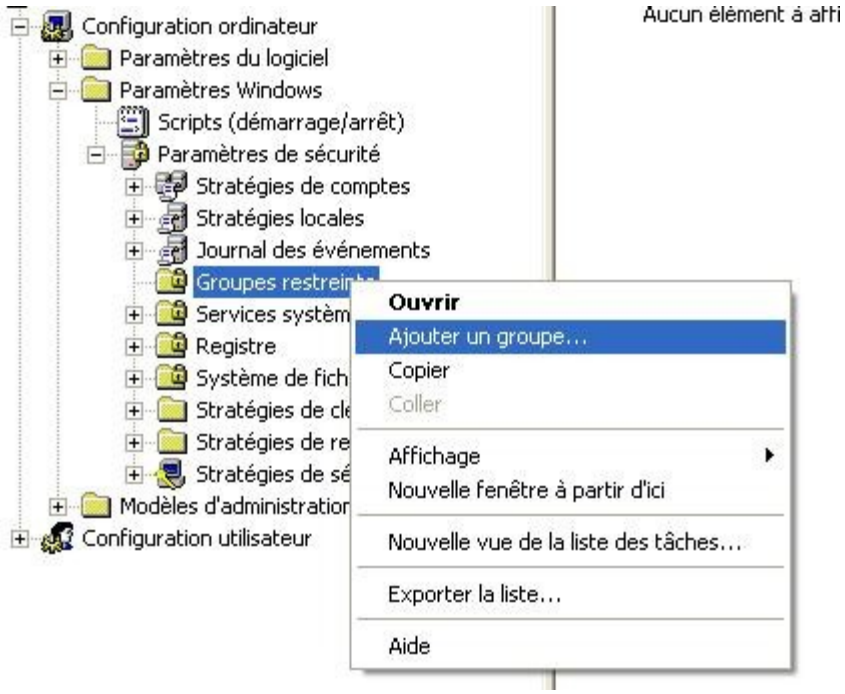
ETAPE 3: Au tour de la BDR ?

Une manipulation similaire permettrait de modifier les autorisations s'appliquant aux clés du Registre.....

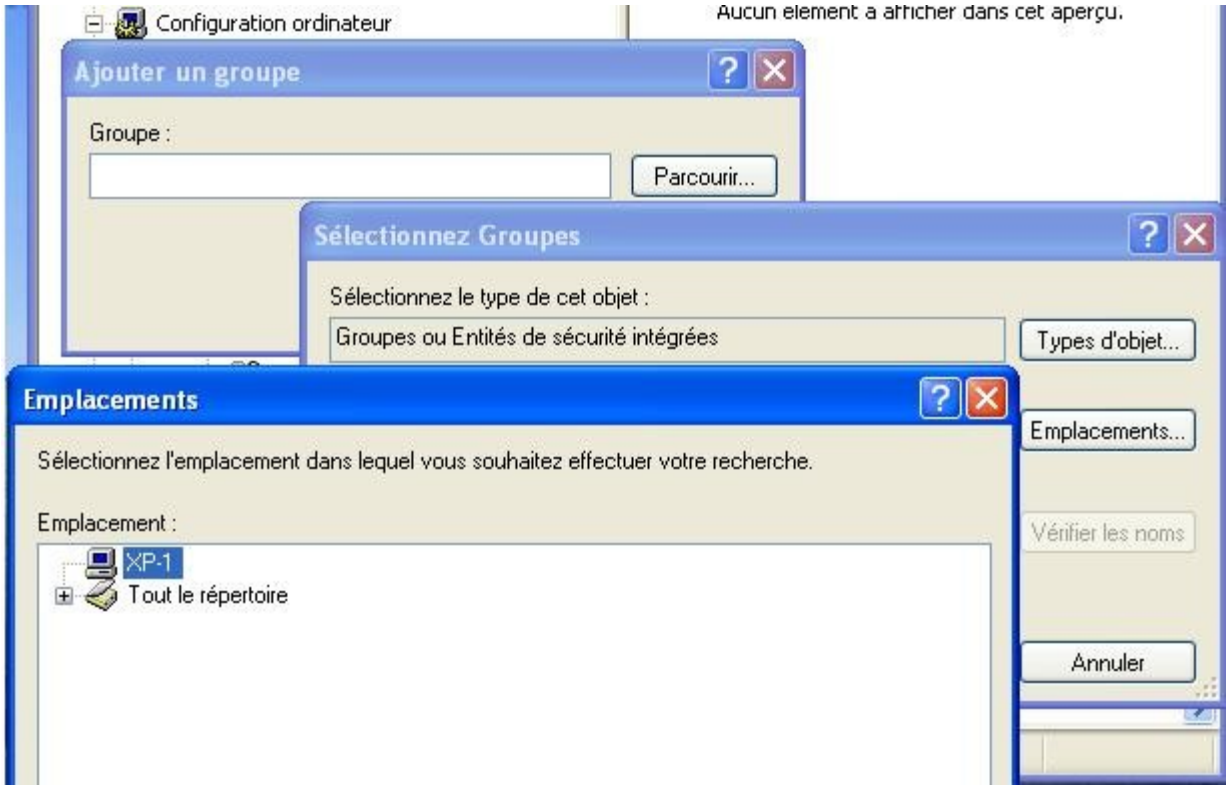


ETAPE 4: et des groupes restreints ?

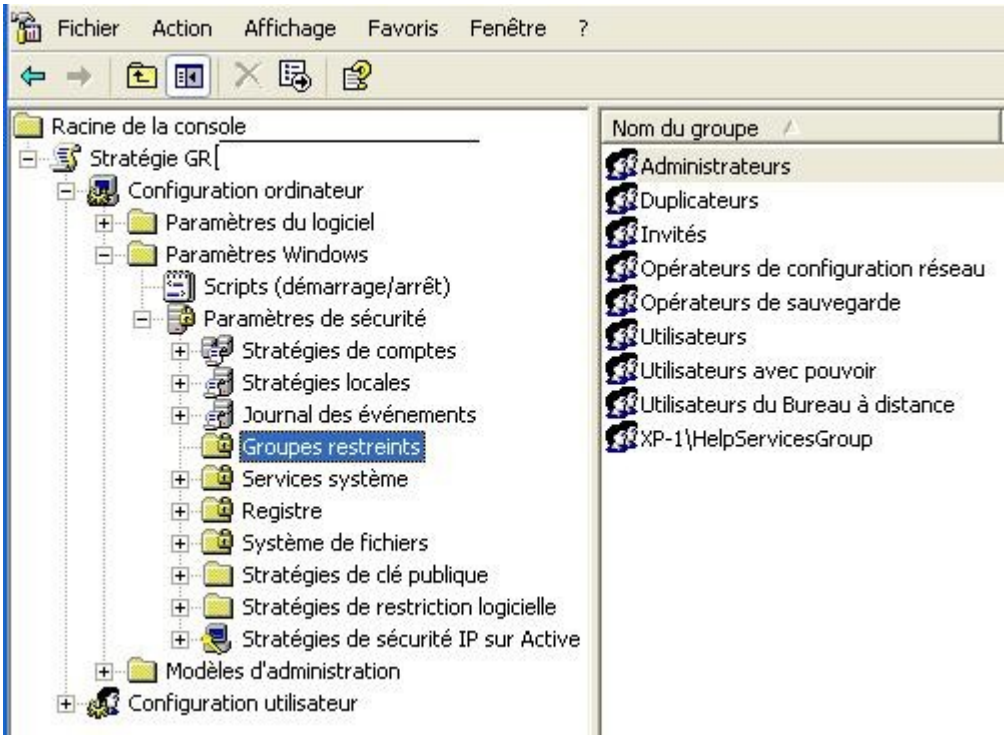
Des logiciels mal écrits pour XP peuvent réclamer des droits inattendus sur certains fichiers résidents parfois dans le dossier d'installation du système. Bien qu'un audit des échecs sur les entrées d'un dossier puisse renseigner, et parce que le temps peut manquer, il peut être plus simple de jouer sur l'imbrication des groupes globaux du domaine dans les groupes restreints prédéfinis sur les stations XP (groupe local des Administrateurs, Utilisateurs avec pouvoir, etc...).
Par exemple, comment faire, en quelques clics et sans passer sur tous les postes, pour que tous les Utilisateurs du Domaine soient Administrateur local de chaque machine de la salle 001 ? En agissant sur le paramètre « Groupes restreints » de la sécurité appliquée à l'O.U contenant ces machines :



Impératif : les groupes restreints doivent être recherchés sur le poste-modèle (ici XP-1) par le bouton « Emplacements »:



Conseillé : pour les avoir tous sous la main, importer, une bonne fois, par sélection multiple, la totalité des groupes locaux existants sur le poste-modèle :



Il reste, maintenant, à affecter les groupes globaux aux groupes restreints: attention, cette étape, très fine, peut se révéler très violente en cas d'oubli !
Dans notre cas, les groupes « Admin du Domaine » et Utilisateurs du Domaine » seront ajoutés au groupe local des Administrateurs :

1. Double-cliquer sur le groupe restreint visé, faire « ajouter ».

2. Sélectionner l'objet « groupes » non coché par défaut et décocher la liste encombrante des nombreux « utilisateurs ».

3. Ajouter les groupes globaux souhaités. Valider.

Gérard LESUEUR
DI 7
Division Informatique
Rectorat de Créteil