

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

Mise à jour: 04/03/2005

Microsoft a prévu de faciliter la tâche des administrateurs 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 (pour la salle du même nom)

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 puis cocher au moins une case:

L'onglet « Bureau à distance » de l'utilitaire système du panneau de configuration du serveur est-il activé ?

Les utilitaires d'administration du serveur (Adminpak.msi du CD-serveur)) ont-ils été installés sur le poste XP ?

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 :



🐗 Utilisateurs et ordinateurs Active Directory				
J & ⊆onsole Eenêtre ?				
Action Affichage   ← → 🗈 🖬 🗙 😭 😰 😫 🦉 छ 🗸 🍕 🍺				
Arbre	salle001 1 objets			
Jutilisateurs et ordinateurs Active	Nom	Туре	Description	
🖆 🗊 pai.di	EC7WXP	Ordinateur		
🔁 🖆 🛅 Builtin				
Computers				
Domain Controllers				
⊕ · iiii Users				
salle001				
A F				
	1			

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 ...

Subject of the second s			
Gonsole Eenêtre ?			
Action Affichage ← →	🗈 🔃 🗙 🖆 🗔 😫 🛛 🦉 💆 🗸 🏈 🍞		
Arbre	salle001 1 objets		
Utilisateurs et ordinateurs Active Definition Utilisateurs et ordinateurs Active Definition Utilisateurs Domain Controllers Domain Controllers Definition	Nom     Type     Description       C7WXP     Ordinateur       Propriétés de salle001       Général     Géré par	<u>?×</u>	
⊕ ∰ Users	Liaisons de l'objet Stratégie de groupe actuel pour salle	>001	
D & xio	Plus un objet Stratégie de groupe est haut dans la liste, plus sa prio Cette liste a été obtenue à partir de : dell2k.pai.di	rité est élevée.	
	Nouveau Ajouter Modifier	Monter	
Al	Options Supprimer Propriétés	Descendre	
er	Bloquer l'héritage de stratégies		
	OK Annuler	Appliquer	

## 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:

Rechercher un objet Stratégie de groupe	?×	Rechercher un objet Stratégie de groupe	? 🗙
Nechercher un objet Strategie de groupe         Domaines/unités d'organisation       Sites       Ordinateurs       Tous         Regarder dans :       Image: Comparisation       Image: Comparisation       Image: Comparisation         Domaines, unités d'organisation et objets de stratégie de groupe liés :       Image: Comparisation       Image: Comparisation       Image: Comparisation         Nom       Domaine       Image: Comparisation       Image: Comparisation       Image: Comparisation       Image: Comparisation         Nom       Domain       Domaine       Image: Comparisation       Image: Comparis		Rechercher un objet Stratégie de groupe         Domaines/unités d'organisation         Sites       Ordinateurs         Tous         Regarder dans :       Imaile alle001.pai.di         Domaines, unités d'organisation et objets de stratégie de groupe liés :         Nom       Domaine         Imaile       Imaile         Imai	
OK Ar	nnuler	OK Ar	nuler

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

🚡 Console1 - [Racine de la console\Stratégie TEMP [dell2k.pai.di]\Configuration ordinateur\Paramètres Win 🔳 🗖 🔀			
🚡 Fichier Action Affichage Favoris Fenêtre ?			
Racine de la console	Nom de l'objet 🛛 🗛		
<ul> <li>Gratégie TEMP [dell2k.pai.di]</li> <li>Gonfiguration ordinateur</li> <li>General Paramètres du logiciel</li> </ul>	Aucun élément à afficher dans cet aperçu.		
<ul> <li>Paramètres Windows</li> <li>Scripts (démarrage/arrêt)</li> </ul>			
<ul> <li>Paramètres de sécurité</li> <li>Elevent</li> <li>El</li></ul>			
⊡ gg Strategies locales ⊡ gg Journal des événements			
Tring Groupes restrents Tring Services système Tring Registre			
Système de fichiers			
<ul> <li>En attages de la patitique</li> <li>En attages de restriction logiciell</li> <li>En attages de sécurité IB sur às</li> </ul>			
Grategies de securite 1P sur Ac     Modèles d'administration			
⊞ ्यूयुर्ट Contiguration utilisateur			

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







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

🚡 Console1 - [Racine de la console\Strat	égie TEMP [dell2k.pai.di]\Configuration ordinateur\Paran	ètre Sélectionnez Utilisateurs , Ordinateurs ou Groupes 🛛 🤶 🗙
🚡 Fichier Action Affichage Favoris Fené	Sécurité de la base de données pour %SystemR ? 🛽	Sélectionnez le type de cet objet :
⇔ ⇒ 🗈 🖬 🗙 💀 😫	Sécurité	Utilisateurs, Groupes ou Entités de sécurité intégrées Types d'objet
<ul> <li>Racine de la console</li> <li>Stratégie TEMP (del/2k.pai.d)</li> <li>② Configuration ordinateur</li> <li>③ Paramètres du logiciel</li> <li>③ Paramètres du logiciel</li> <li>③ Paramètres du logiciel</li> <li>③ Paramètres du logiciel</li> <li>③ Paramètres de sécurité</li> <li>④ Paramètres de sécurité</li> <li>④ Stratégies locales</li> <li>④ Journal des événements</li> <li>④ ③ Services système</li> <li>④ Système de fichiers</li> <li>⑤ Stratégies de sécurité iP sur</li> <li>⑨ Stratégies de sécurité iP sur</li> <li>⑨ Modèles d'administration</li> <li>⑦ Modèles d'administration</li> </ul>	Noms d'utilisateur ou de groupe : Administrateurs (C7WXPVAdministrateurs) CREATEUR PROPRIETAIRE SYSTEM Utilisateurs (C7WXPVUblisateurs) Ajouter Supprimer Autorisations pour Utilisateurs Autorisations pour Utilisateurs Contrôle total Modification Lecture et exécution Affichage du contervu du dossier Lecture Écriture	A partir de cet emplacement : pai di Frequêtes communes Nom : Commence par Colonnes Description : Commence par Colonnes Description : Commence par Colonnes Pechercher Arrêter Mot de passe sans date d'expiration Nombre de jours depuis la dernière session : Colonnes DK Annuler
	Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés. Paramètres avancés	Nom (RDN) Adresse de me Description Dans le dossier
<	OK Annuler Appliquer	A remembrosen     Ce completituils     paid//disers       Image: Second completituils     paid//disers     Image: Second completituils       Image: Second completituils     paid//disers     Image: Second completituils

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

Sécurité de la base de données pour %SystemR ? 🔀	Sécurité de la base de données pour %SystemR ? 🔀		
Sécurité	Sécurité		
Noms d'utilisateur ou de groupe :	Noms d'utilisateur ou de groupe :		
Administrateurs (C7WXP\Administrateurs)     GEATEUR PROPRIETAIRE     GESYSTEM	Administrateurs (C7WXP\Administrateurs)     GREATEUR PROPRIETAIRE     GR SYSTEM		
Utilisa. du domaine (PAI\Utilisa. du domaine) Utilisateurs (C7wXP\Utilisateurs)	<ul> <li>Utilisa, du domaine (PAI\Utilisa, du domaine)</li> <li>Utilisateurs (C7WXP\Utilisateurs)</li> </ul>		
Ajouter Supprimer Autorisations pour Utilisa. du domaine Autoriser Refuser	Ajouter Supprimer Autorisations pour Utilisa. du domaine Autoriser Refuser		
Contrôle total       Image: Contrôle total         Modification       Image: Content of the cont	Contrôle total       Image: Contrôle total         Modification       Image: Content of the cont		
Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés.	Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés. OK Annuler Appliquer		



Demander le remplacement des autorisations existantes puis valider :

Ajouter un objet 🔹 💽
%SystemRoot%\Temp
O Configurer ce fichier ou ce dossier
Propager les autorisations pouvant être héritées à tous les sous-dossiers et les fichiers
Remplacer les autorisations existantes dans tous les sous-dossiers et les fichiers disposants d'autorisations pouvant être héritées
O Interdire le remplacement des autorisations de ce fichier
Modifier la sécurité
OK Annuler

Après actualisation d'Active Directory (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 le Registre.....

🚡 Console1 - [Racine de la	a console\Stratég	yie TEMP [dell2k.pai	.di]\Configuratio	n ordinateur Paramètres Win 🔳 🗖 🔀
🚡 Fichier Action Affichage	Favoris Fenêtre	9 7		_ B ×
⇐ ⇒ 🗈 🖬 🗡 🖳	2			
Racine de la console	100	Nom de l'objet 🗸		
Stratégie TEMP [dell2k.pai.di] Stratégie TEMP [dell2k.pai.di] Paramètres du logiciel Paramètres Windows Stripts (démarrage/arrêt) Paramètres de sécurité Stratégies de comptes Stratégies locales Stratégies locales Stratégies Stra		Aucun élément à afficher dans cet aperçu.		
<ul> <li>⊕ Modèles d'admin</li> <li>Affich</li> <li>⊕</li></ul>	Affichage Nouvelle fenêtre à	► partir d'ici		
< III	Nouvelle vue de la	liste des tâches		
Ajoute une nouvelle clé dans ce i	Exporter la liste			

Mais il conviendra, peut-être pour cette tâche, de définir préalablement une autre stratégie ...

Gérard LESUEUR PAI 77 Nord Division Informatique Rectorat de Créteil