Configuration ESU4 lycée Jacques Cœur – Bourges

Version 2.2 - en date du 23/06/2008

Connexion sur le site du lycée Jacques Cœur de Bourges
http://lyc-jcoeur.ac-orleans-tours.fr

Authentification : ***esu***
Mot de passe : ***is-easy!***
Tice et Net >>>Configuration ESU pour Solaere

Merci à tous ceux qui directement ou indirectement par leurs contributions à la liste ESU ont participé à la rédaction de cette brochure.

1 Notre structure réseau

La nouvelle structure réseau du lycée Jacques Cœur de Bourges est une version très élaborée du système **Solaere Eole+** développé pour les lycées de l'académie d'Orléans-Tours par le Gip Récia.

Organisée en différents réseaux virtuels, cette structure inclus un nombre conséquent de serveurs pédagogiques ; tous sont des systèmes Linux, réels ou virtualisés, dont le plus important pour notre sujet est le **contrôleur de domaine PDC0180007K** qui est une machine Linux faisant tourner un **Samba 3 comme contrôleur de domaine**, authentifiant les utilisateurs sur une **base LDAP**.

Ce qui fait une différence majeure avec la première version de ce document, c'est que maintenant **cet annuaire d'authentification LDAP est celui des serveurs Scribe du projet Eole et que la version utilisée d'ESU est une version standard de production.**.

Vous pouvez avoir une vue complète de notre structure en vous connectant sur le serveur web du lycée : http://lyc-jcoeur.ac-orleans-tours.fr
L'authentification **esu** avec le mot de passe **is-easy!** vous permettant d'afficher la **structure de Solaere Eole+** accessible dans la rubrique **TICE et Net**, de télécharger cette brochure et d'autres utilitaires.

Préambule :

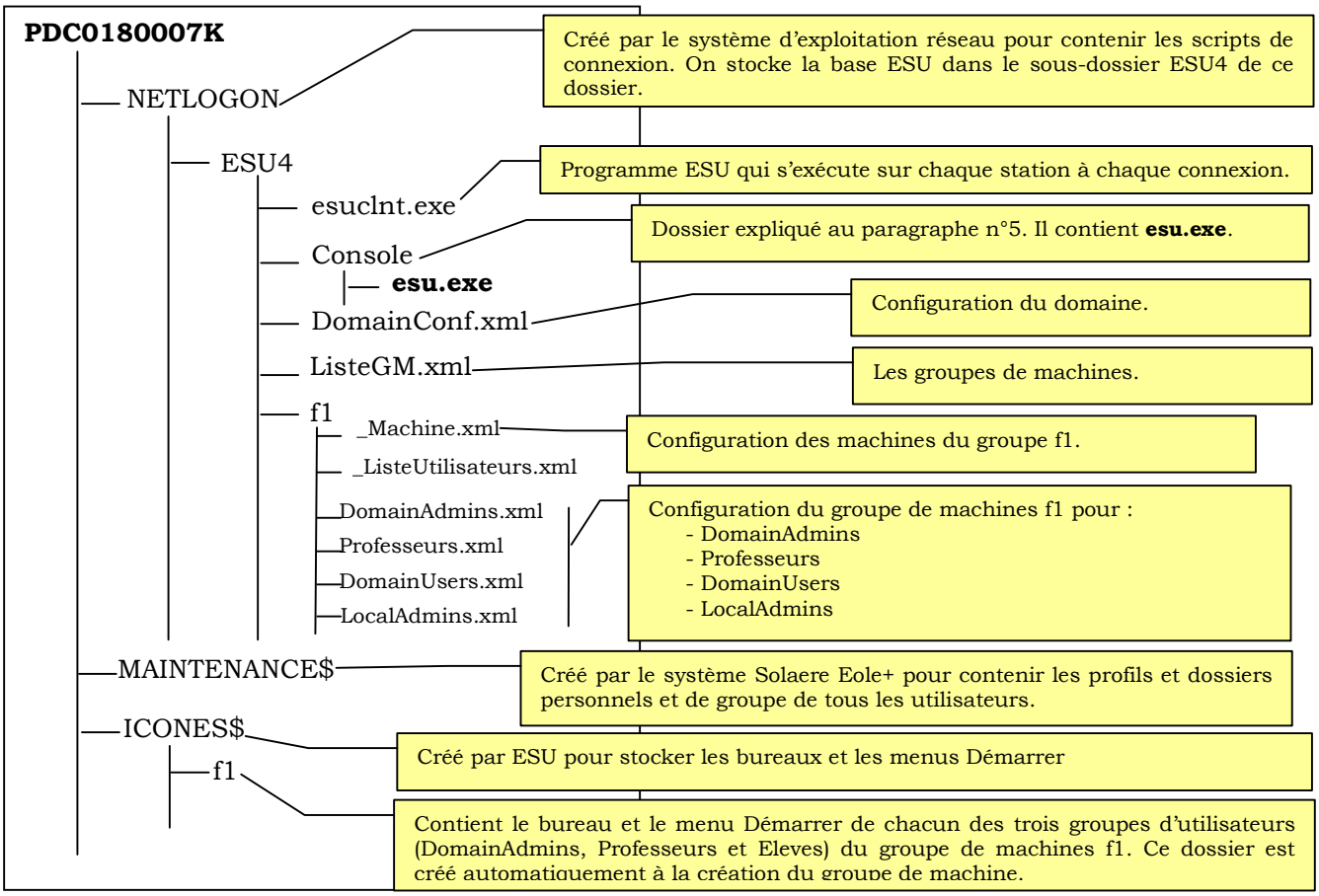
Première période

*Nous avons commencé l'installation d'ESU4 sur ce nouveau réseau au 15 Juin 2005 avec l'aide de deux collègues connaissant ESU dont l'un est un des pères de la solution Solaere**, Christophe Dubreuil** et l'autre un administrateur de collège, **Jérôme Perchet** ; qu'ils soient ici remerciés.*
Il nous a fallu un bon nombre d'heures avant d'être pleinement satisfaits et commencer de déployer les postes pour la rentrée de septembre 2005 (nous utilisons des images Ghost).
Nous avons utilisé une première version non officielle d'ESU4.

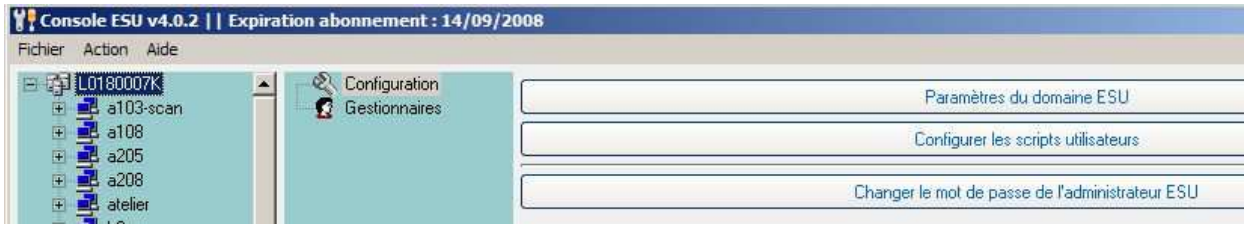
Seconde période

*Depuis septembre 2006, l'évolution de la solution Solaere vers « **Solaere Eole+** » fait que c'est un annuaire LDAP de type **Scribe** et la dernière version officielle d'ESU4 (**version 4.02 a** au moment de l'écriture de ce document) qui est utilisée, chacun devrait donc mieux retrouver les éléments standards habituels.*

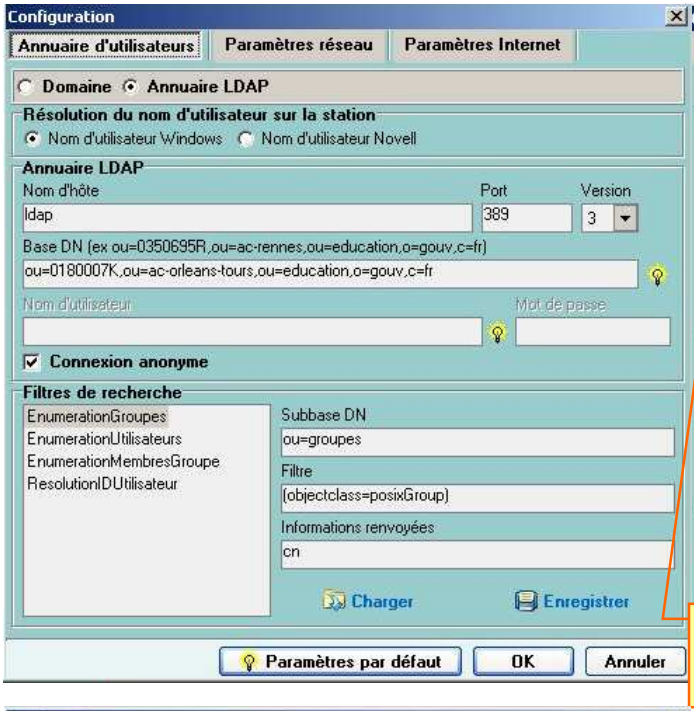
2 Structure d'ESU4 et installation sur le contrôleur de domaine

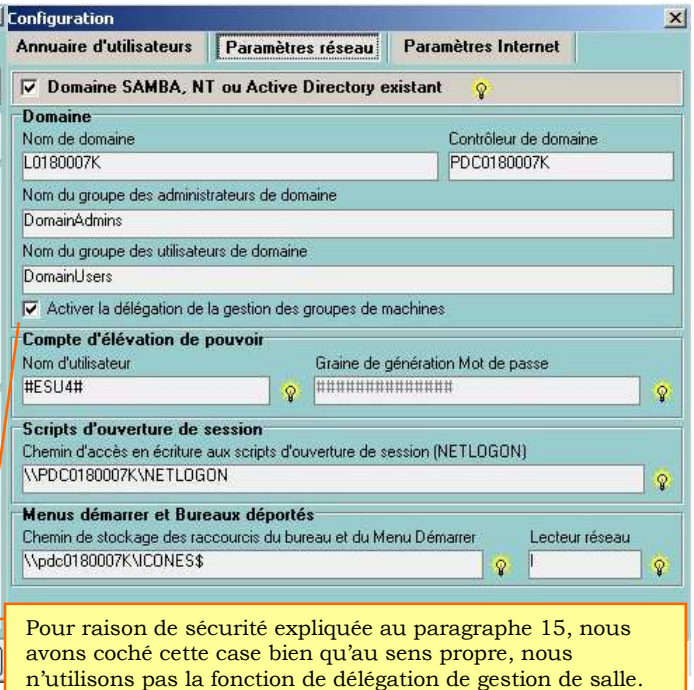


On lance **esu.exe** qui est la console de **configuration d'ESU4** :

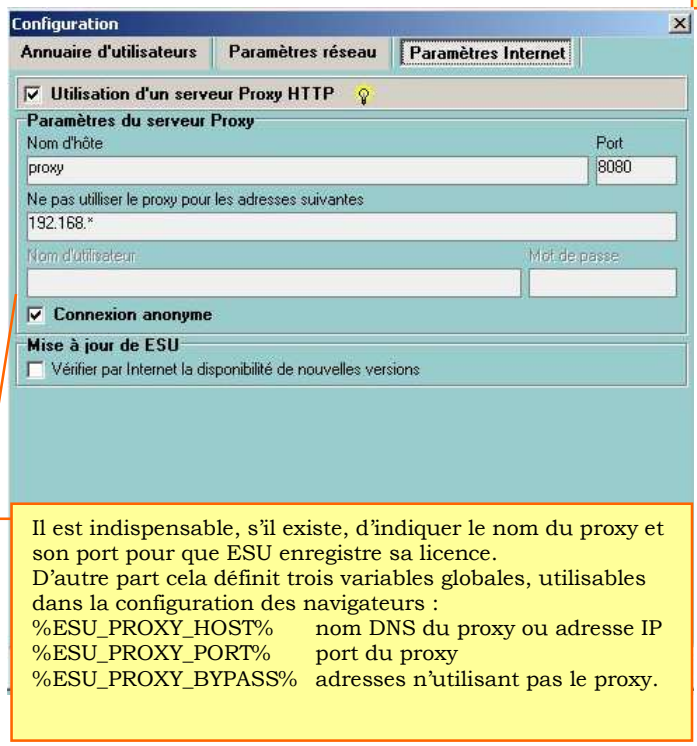


Un clic sur **Paramètres du domaine ESU :**





Pour raison de sécurité expliquée au paragraphe 15, nous avons coché cette case bien qu'au sens propre, nous n'utilisons pas la fonction de délégation de gestion de salle.



Il est indispensable, s'il existe, d'indiquer le nom du proxy et son port pour que ESU enregistre sa licence.
D'autre part cela définit trois variables globales, utilisables dans la configuration des navigateurs :

%ESU_PROXY_HOST%	nom DNS du proxy ou adresse IP
%ESU_PROXY_PORT%	port du proxy
%ESU_PROXY_BYPASS%	adresses n'utilisant pas le proxy.

On peut choisir d'associer ESU à un annuaire LDAP ou à un annuaire standard de domaine Samba, NT ou Active Directory.
Les chemins d'accès correspondent à la structure de l'arbre des répertoires ci-dessus.

Exemple de configuration pour le navigateur Internet Explorer utilisant les variables globales de configuration proxy (à mettre dans chaque groupe utilisateur de chaque groupe de machines) :

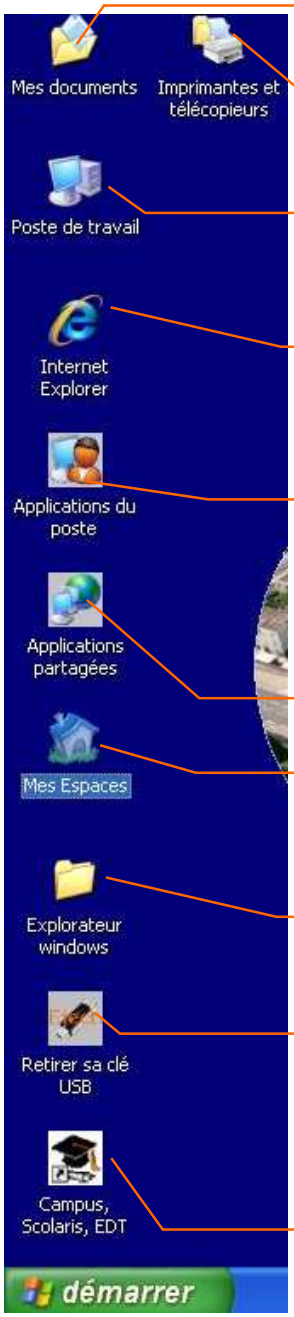
Le compte d'élévation de pouvoir a pour nom #ESU4#, il peut être modifié. Depuis la version 4.02a, la génération des mots de passe pour l'élévation de pouvoir est faite automatiquement sur chaque station et à chaque connexion, ce qui assure que le mot de passe généré par ce mécanisme ne donne accès qu'aux droits d'administrateur d'une seule station pendant la seule durée d'une session.

3 Le cahier des charges des fonctions attendues de ESU

Le système Solaere Eole+ fourni une base LDAP d'authentification des utilisateurs du domaine, des scripts de connexion et pour chaque utilisateur un espace contenant le « **Mes documents** » de l'utilisateur, d'autres dossiers personnels associés et les dossiers de groupe de l'utilisateur.
ESU4 devait donc avoir la tâche de :

- fournir à tout utilisateur un bureau unique, déporté sur le serveur, simple, dépendant de la machine et du groupe d'authentification et fournissant des accès commodes aux espaces construits par le système.
- fournir à tout utilisateur des accès uniformisés et simplifiés aux applications locales ou réseaux ainsi qu'aux seuls périphériques auxquels il a droit (imprimantes locales et réseau, scanners, graveurs, clé USB, …).
- configurer le poste de l'usager, notamment le mettre à l'heure à chaque début de session et assurer la protection de cette configuration
- autoriser éventuellement certaines tâches pour certaines authentifications ou certaines machines :
    - changer l'heure pour la durée d'une session
    - connecter une imprimante réseau en mode DOS à LPT1
    - avoir accès en lecture-écriture à certains dossiers de la machine locale pour certains produits logiciels.

Voici un bureau type pour un professeur avec les fonctionnalités implémentées :



Créé sur les bureaux Windows 2000-XP automatiquement par ESU4

Accès aux files d'impression (réservé aux professeurs)

Accès au poste de travail où ne sont visibles que les lecteurs pleinement nécessaires au travail de l'utilisateur.

L'icône Internet Explorer 6 ou 7 apparaît automatiquement selon la version qui est installée sur le poste. Cf. paragraphe 7.

Objet système qui apparaît automatiquement sur le bureau et qui cible automatiquement « Démarrer Tous les programmes » du poste, dossier déporté sur le serveur dans **icones$\groupe de la machine** qui est un dossier construit par ESU4 quand on crée un nouveau groupe de machines.

Objet système qui apparaît automatiquement sur le bureau .

Objet systèmes lié à notre réseau Solaere Eole+ qui apparaît automatiquement sur le bureau.

Explorateur est désormais un objet système comme expliqué au paragraphe 16.

Objet système qui permet le retrait facile des clés USB, avec vidage préalable du tampon et effacement de la connexion. Une contrainte : les lecteurs doivent être uniformisés pour que la clé arrive en F:

Objet système qui n'apparaît sur le bureau que pour une authentification d'un professeur sur un poste Windows 2000-XP

4 La mise en œuvre des règles de base

Dans ESU, les machines doivent être identifiées en groupe de machines : nous avons choisi de hiérarchiser ces groupes ainsi :

f0 est le groupe des machines du secteur f0 désigné avec le jocker * par **f0***
f010 est le groupe des machines de la classe f010 désigné avec le jocker * par **f010***
f010-03 est la machine n°3 de la classe f010.

Dans chaque groupe de machines, nous avons défini une stratégie pour quatre groupes d'utilisateurs :

DomainAdmins administrateurs du domaine pour lesquels tous les droits de modification de la machine locale sont accordés. Les profils errants sont traités à l'identique des autres utilisateurs.

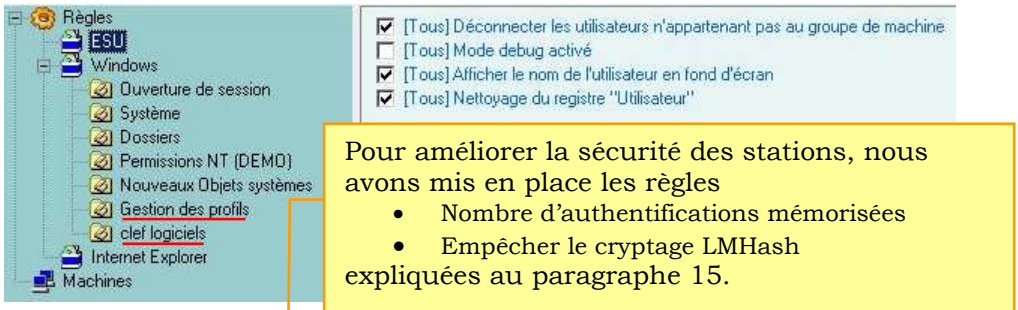
LocalAdmins groupe que nous avons créé et qui contient un (mais éventuellement plusieurs) utilisateurs qui seront élevés au rang d'administrateur de chaque station (cf. paragraphes 9 et 15).

Professeurs utilisateurs qui sont des membres du personnel du lycée pour lesquels tous les droits de modification de la machine locale sont restreints avec des profils errants traités à l'identique des autres utilisateurs.

DomainUsers utilisateurs qui sont les utilisateurs du domaine non membres des deux groupes précédents et pour lesquels tous les droits de modification de la machine locale sont très restreints avec des profils errants traités à l'identique des autres utilisateurs.

Les règles des groupes de machines

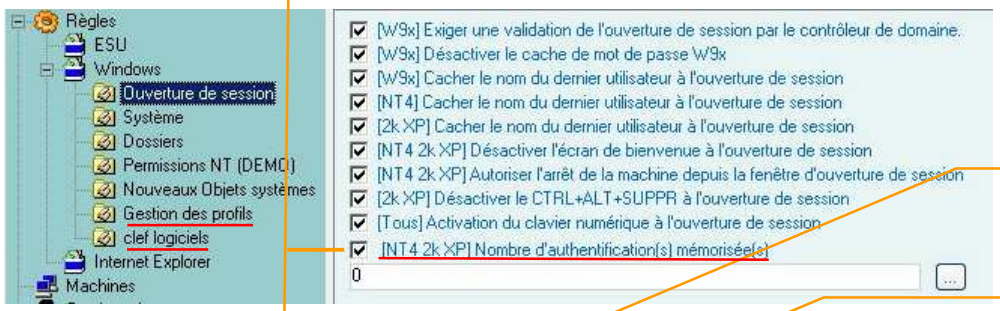
Ce sont les mêmes pour tous les groupes de machines, sont soulignées en rouge les règles que nous avons ajoutées et pour lesquelles vous trouverez des compléments explicatifs dans ce document.



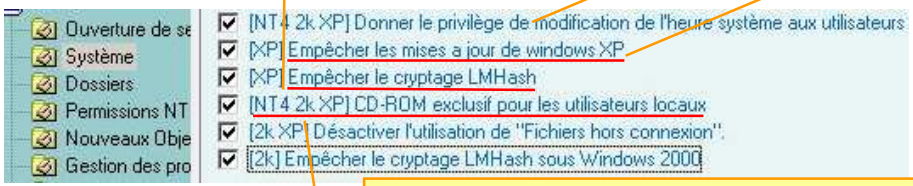
Pour améliorer la sécurité des stations, nous avons mis en place les règles

- Nombre d'authentifications mémorisées
- Empêcher le cryptage LMHash

expliquées au paragraphe 15.



Pour notre gestion de l'heure des stations, voir paragraphe 10.

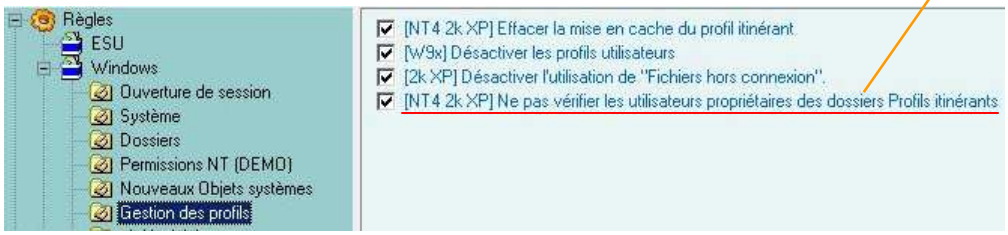


Pour diverses raisons, nous avons préféré désactiver complètement la mise à jour des systèmes Windows XP. Une règle simple a été mise en place et est expliquée au paragraphe 5.

Cette règle permet l'utilisation de logiciels d'extraction de pistes de CD Audio (Cdex par ex).

La règle « **Désactiver l'utilisation de fichiers hors connexion** » est une règle qui n'apparaissait pas dans notre brochure précédente, ni dans notre liste téléchargeable de règles (ListeRegles.xml). Il s'agit d'un bug historique de notre liste de règles construite sur une version de test du logiciel ESU4.

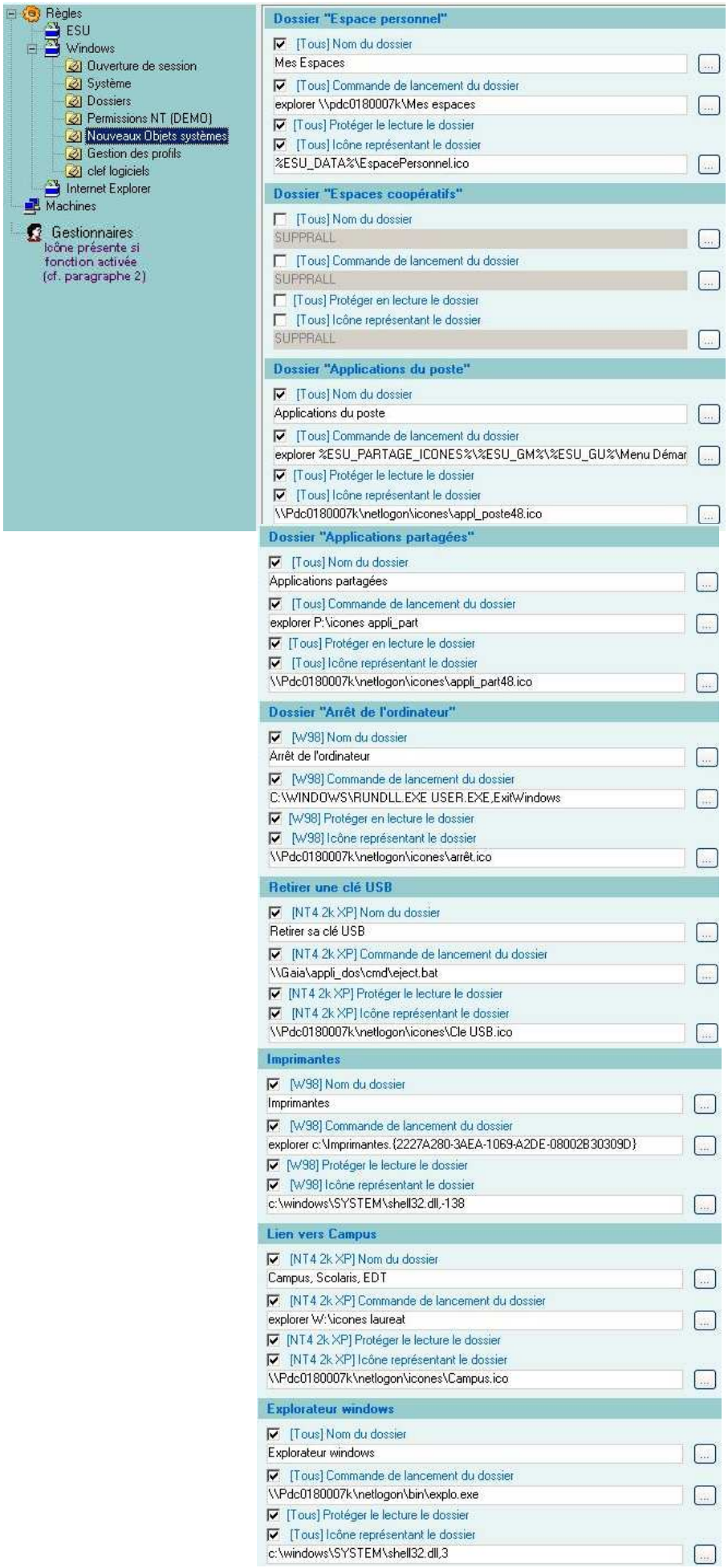
L'ensemble de ces règles sera expliqué au paragraphe 8.



Cette règle a été rajoutée à notre version d'ESU4 afin d'assurer le téléchargement des profils itinérants sans aucun problème sur notre réseau avec serveurs Linux et Samba. Communication de cette règle a été faite à Olivier Adam en octobre 2005. Voir les détails au paragraphe n°5.

L'ensemble de ces règles sera expliqué au paragraphe 6.

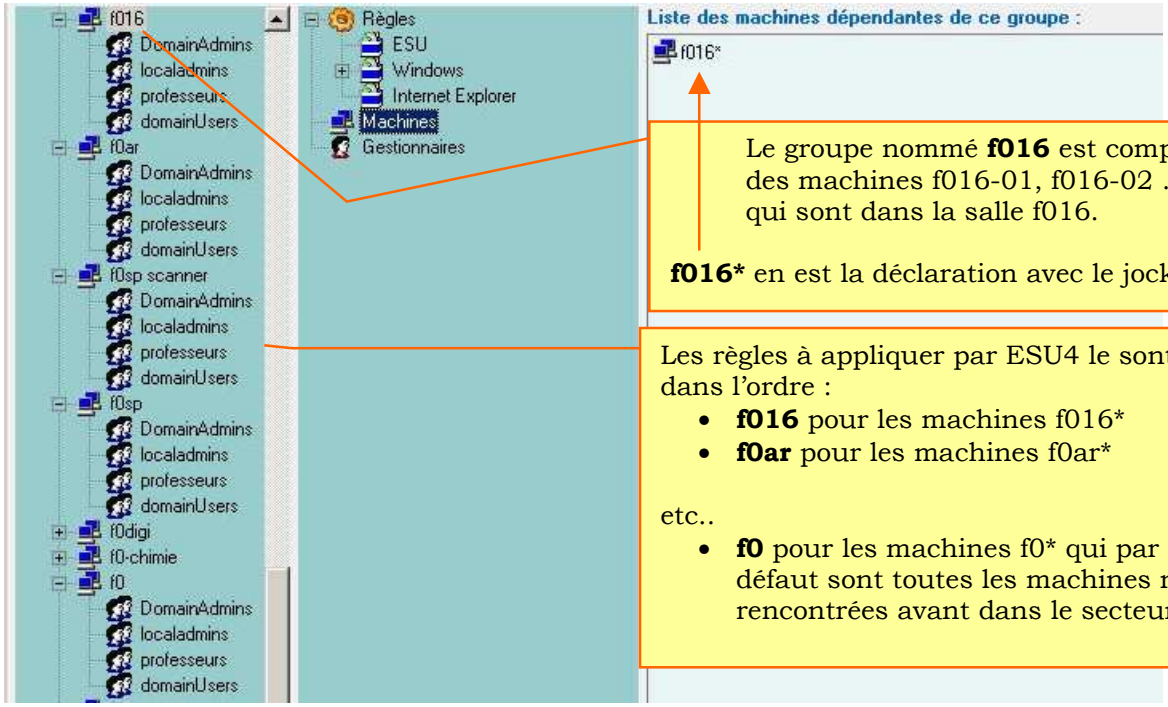
L'icône « **Gestionnaires** » n'est présente que si la case « **Activer la délégation de la gestion des groupes de machines** » est cochée. Cf. paragraphe 2.
Nous ne l'utilisons que pour un groupe du domaine de nom « **LocalAdmins** » qu'ESU élève automatiquement au rang d'administrateur local de chaque station : Cf. paragraphe 15.
Pour cela, **LocalAdmins** est un groupe qui est ajouté dans les Gestionnaires de chaque salle :



L'ensemble de ces règles sera expliqué au paragraphe 9.

Les règles des utilisateurs dans un groupe de machines

Dans un groupe de machine, les règles appliquées étant celles rencontrées en premier en coïncidence avec l'authentification de l'utilisateur, cela explique l'ordre impératif des trois groupes DomainAdmins, LocalAdmins, Professeurs et DomainUsers.



Le groupe nommé **f016** est composé des machines f016-01, f016-02 … qui sont dans la salle f016.

f016* en est la déclaration avec le jocker *

Les règles à appliquer par ESU4 le sont dans l'ordre :

- **f016** pour les machines f016*
- **f0ar** pour les machines f0ar*

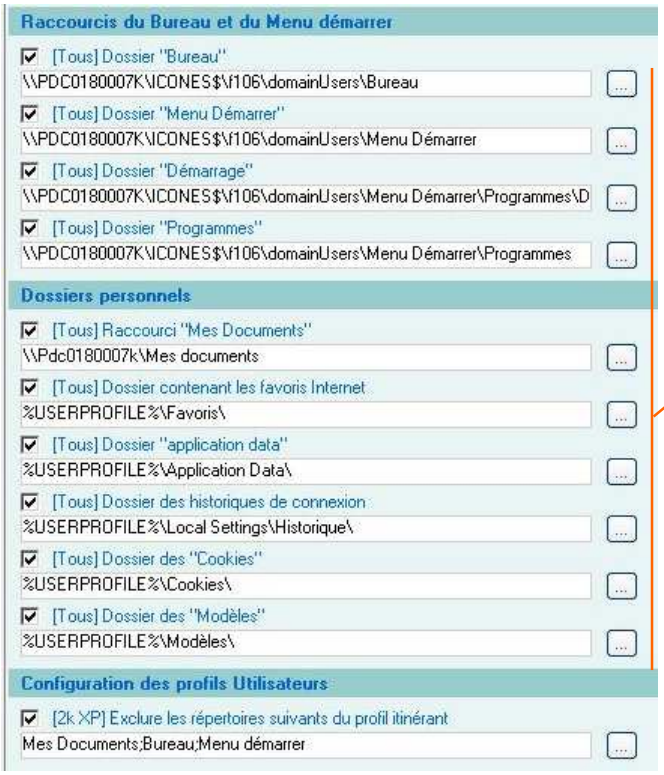
etc..

- **f0** pour les machines f0* qui par défaut sont toutes les machines non rencontrées avant dans le secteur f0

La fin de l'arbre des machines se termine par le groupe defaut_restreint qui porte sur les machines * c'est à dire toutes les machines qui n'ont pas accroché un groupe auparavant. D'où l'importance de l'ordre d'énumération de la liste des groupes de machines.

Pour chaque groupe de machines, les règles définies dans les quatre groupes d'utilisateurs sont sensiblement les mêmes (il n'y a que de rares exceptions). Elles sont recopiées depuis le modèle « defaut_restreint » qui, avec une astuce expliquée au paragraphe n°16, permet d'automatiser la création des règles pour un groupe.

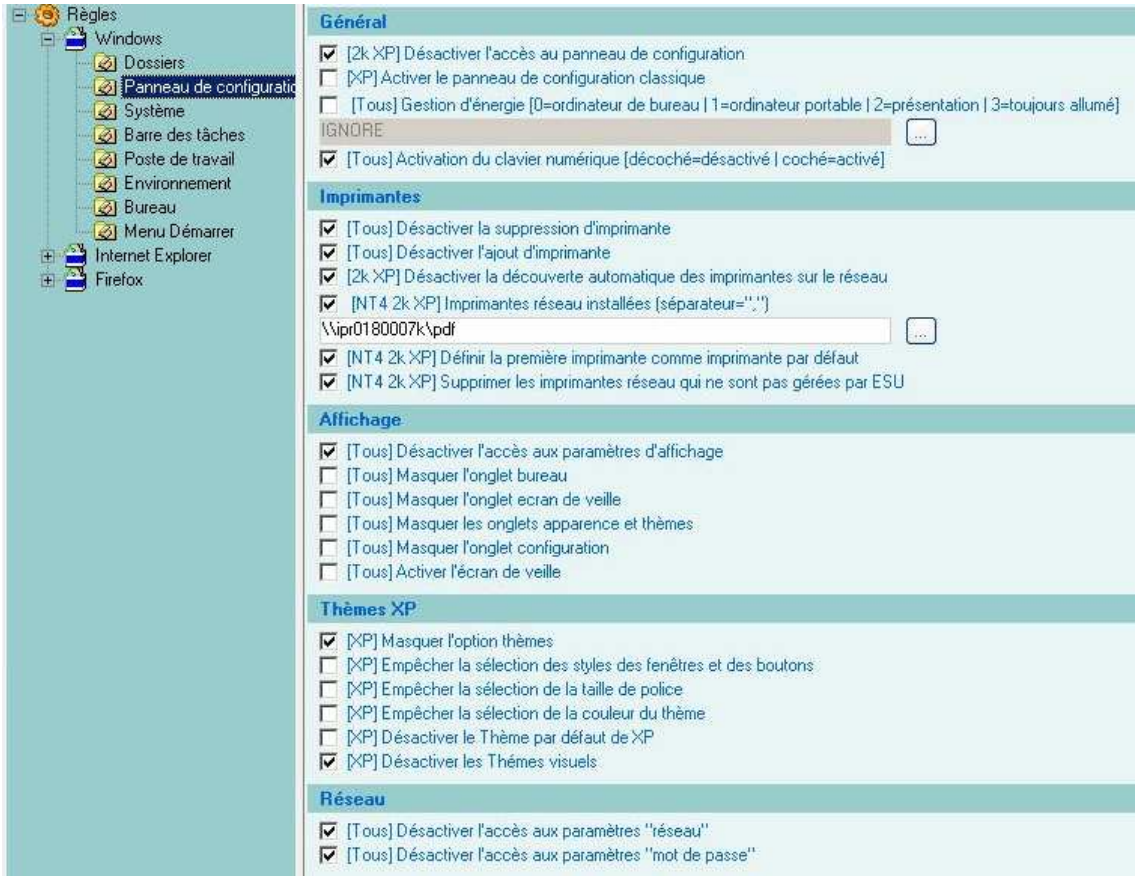
Les règles successives des utilisateurs du groupe DomainUsers pour le groupe machine « defaut_restreint » qui sert de modèle de base aux autres groupes standards.



Ces règles qui sont le modèle de base utilisent les variables :

- **%ESU_PARTAGE_ICONE%** qui désigne le dossier icones$
- **%ESU_GM%** qui désigne le dossier groupe machines
- **%ESU_GU%** qui désigne le dossier groupe utilisateur
- **%USERPROFILE%** qui désigne le dossier du profil utilisateur

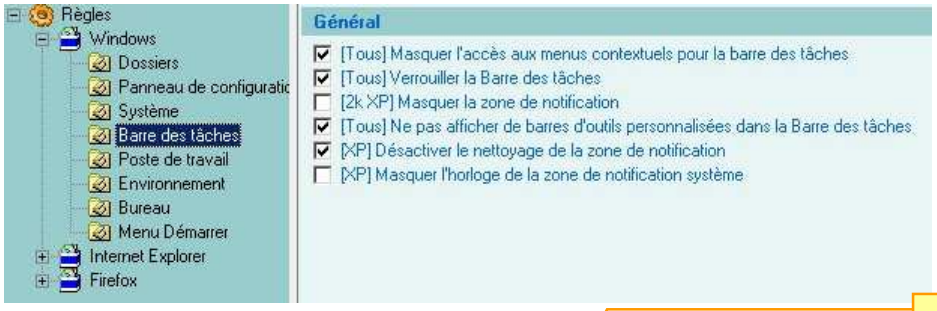
Avec une astuce expliquée au paragraphe n°16, cela permet la personnalisation automatique des modèles de groupes machines comme par exemple celui de la **salle f106** dont on voit ici les règles de DomainUsers obtenu **semi-automatiquement** par chargement du modèle précédent (cf. paragraphe n°16).

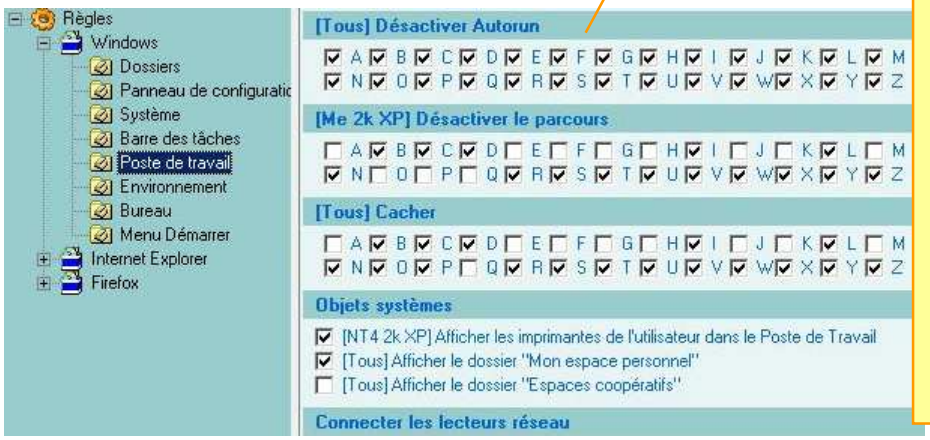


Cette règle fait l'objet d'une remarque :

Pour que les machines ne synchronisent pas le poste local avec le dossier réseau distant, c'est la règle, absente de notre précédente documentation, « **Désactiver l'utilisation de fichiers hors connexion** » et indiquée **page n°5** qu'il importe de cocher.

La règle qui figure ici mérite analyse qui figurera dans la prochaine version de notre brochure, mais il semble bien que son rôle soit modeste sinon inutile.



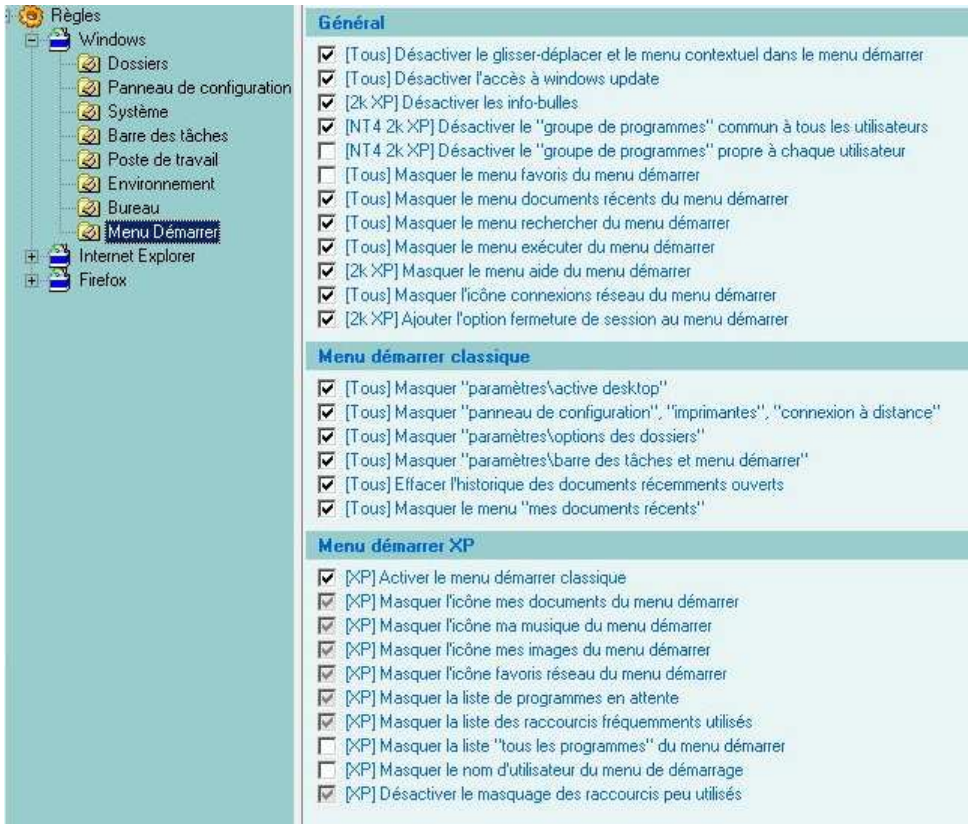


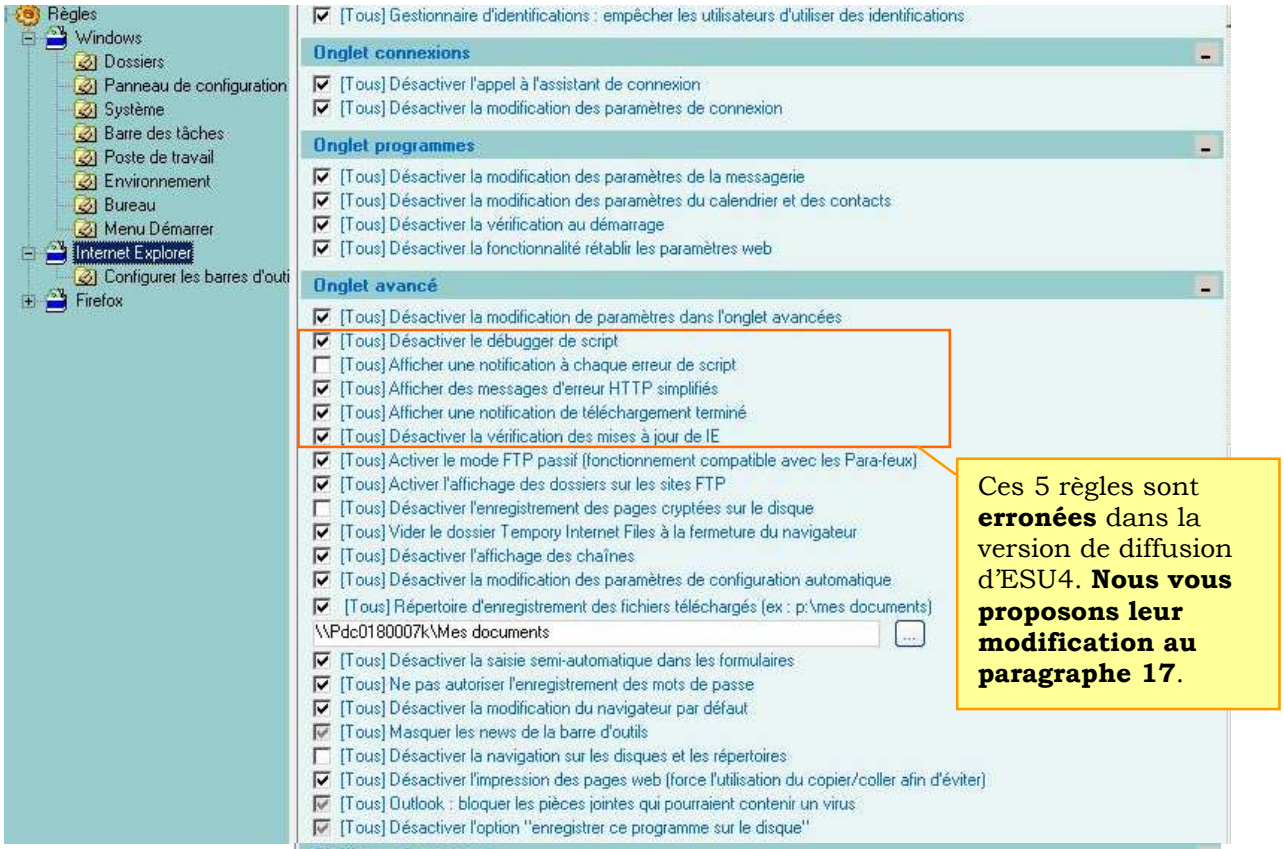
E, F, G et H sont les lettres gardées pour les lecteurs locaux en plus de la partition système C: et de la partition contenant l'image Ghost du poste qui est D:

A partir de I, les lettres désigne des lecteurs réseaux cachés ou non en fonction de notre organisation.

Les connexions des lecteurs réseaux sont uniquement gérés par les scripts de logon. Nous utilisons pour cela un exécutable construit avec AutoIt qui permet de faire un compte rendu de la connexion et notamment signaler un lecteur réseau indisponible.

Les objets systèmes ne sont pas standards. Ils ont été créés par les auteurs de Solaere Eole+ ou par nos soins. Voir paragraphes n°6 et n°8.



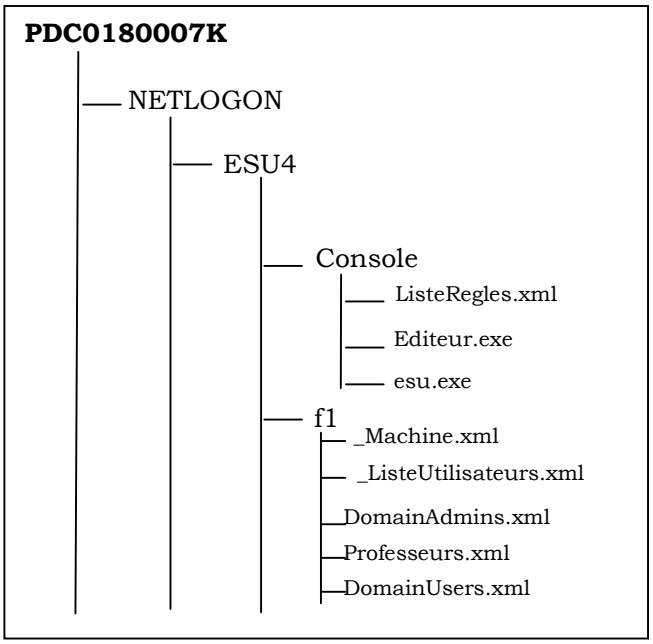


Ces 5 règles sont **erronées** dans la version de diffusion d'ESU4. **Nous vous proposons leur modification au paragraphe 17**.

La règle de configuration du serveur proxy est expliquée page 3 de ce document.

5 L'ajout d'une règle

Principe :



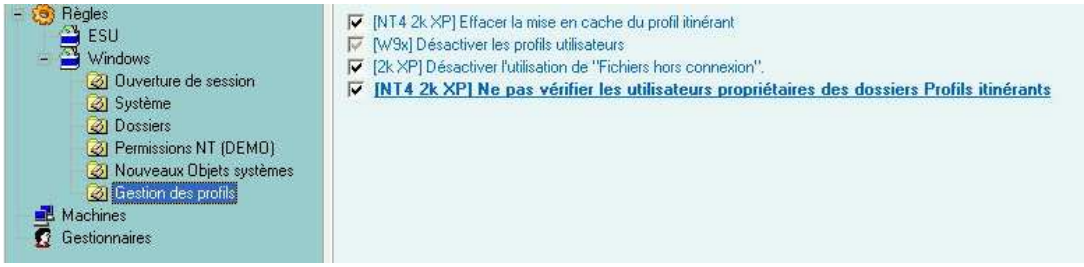
Quand on lance **editeur.exe**, ce programme relit la liste des règles présentes dans **ListeRegles.xml**.
Ceci permet de modifier des règles déjà existantes ou d'en créer de nouvelles qui seront stockées dans **ListeRegles.xml**.

Quand on lance la console ESU (**esu.exe**), les nouvelles règles sont lues dans **ListeRegles.xml** et systématiquement appliquées à tous les groupes de machines (exemple **f1**) pour les groupes d'utilisateurs (exemple **DomainAdmins**, **Professeurs**, **DomainUsers**) en mode grisé tant qu'une stratégie précise n'est pas appliquée aux groupes sus-désignés.

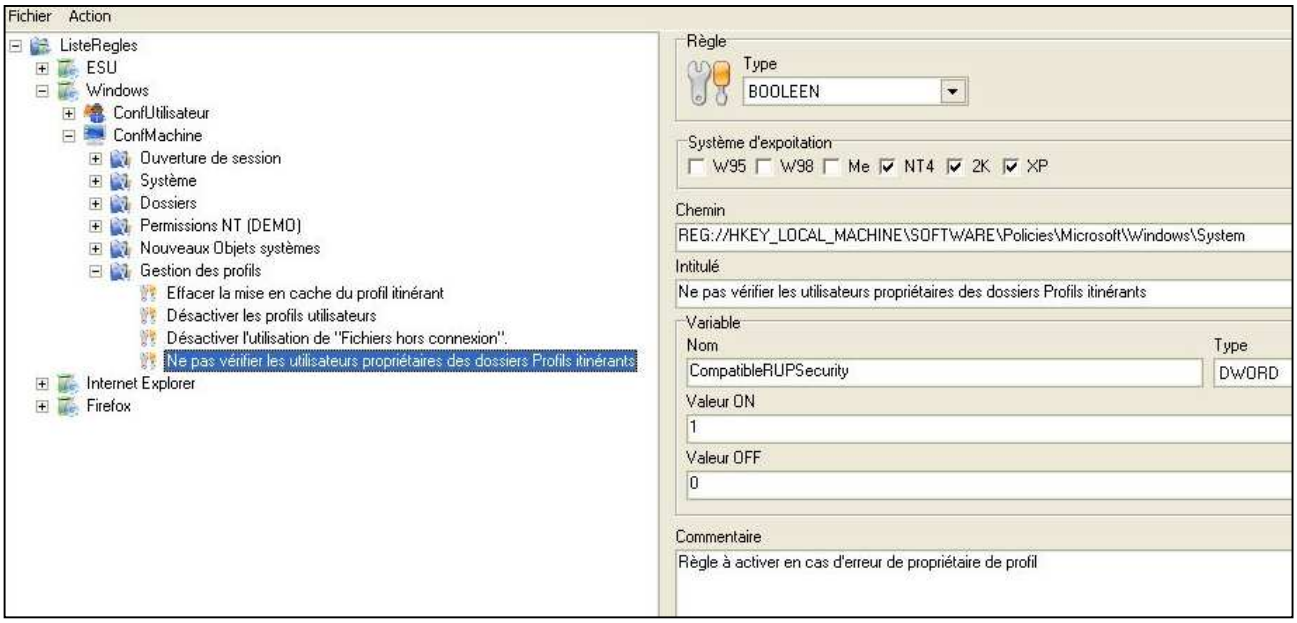
Lorsqu'une stratégie précise, différente du grisé, est appliquée pour un groupe (exemple **Professeurs dans f1**) alors le fichier **Professeurs.xml de f1** est actualisé avec ces règles.

Exemple n°1 : « **Ne pas vérifier les utilisateurs propriétaires des dossiers Profils itinérants** »

Afin d'obtenir une gestion correcte des profils itinérants sur notre réseau à base de serveurs Linux avec Samba 3, nous avons dû rajouter une règle qui **évite totalement les refus de chargements des profils itinérants** par Windows 2000-XP. Cet ajout a été communiqué à Olivier Adam en octobre 2005.



Pour construire cette règle, on utilise **« editeur.exe »** fourni avec ESU 4.



Règle utilisée :

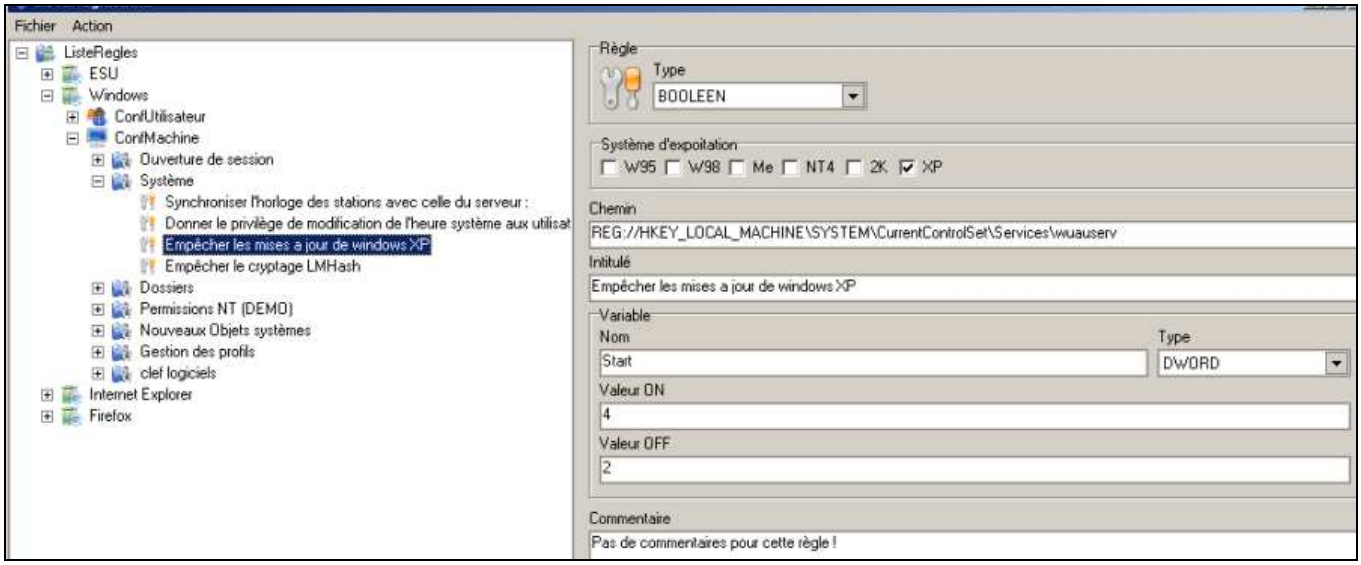
REG://HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System

Nom de la variable : **CompatibleRUPSecurity**

Valeur ON : **1**

Valeur OFF : **0**

Exemple n°2 : « **Empêcher les mises à jour de Windows XP** »
Pour diverses raisons nous préférons maîtriser pleinement les mises à jour d'un poste lorsque l'on se connecte en administrateur sur ce poste, c'est pourquoi nous avons introduit cette règle.



Règle utilisée :

REG://HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv

Nom de la variable : **Start**

Valeur ON : **4**
Valeur OFF : **2**

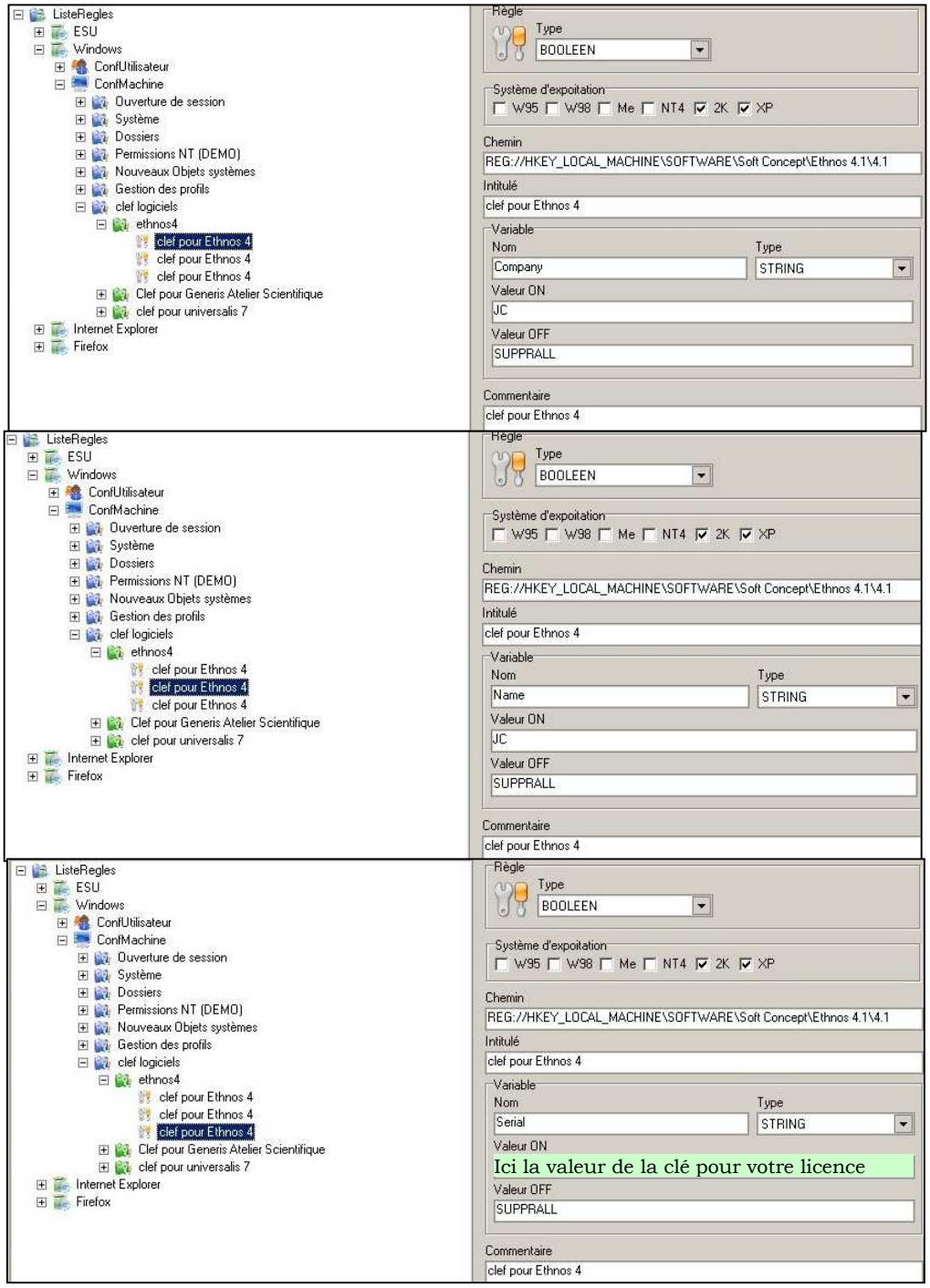
6 Des règles pour configurer automatiquement des applications.

Certaines des applications utilisées sont installées sur un **«serveur d'applications partagées» spécifique** ou sont installées sur certaines stations mais nécessitent une **configuration spécifique**.
Dans les deux cas, nous faisons en sorte **d'automatiser l'adaptation de l'application au poste de travail** de manière automatisée :

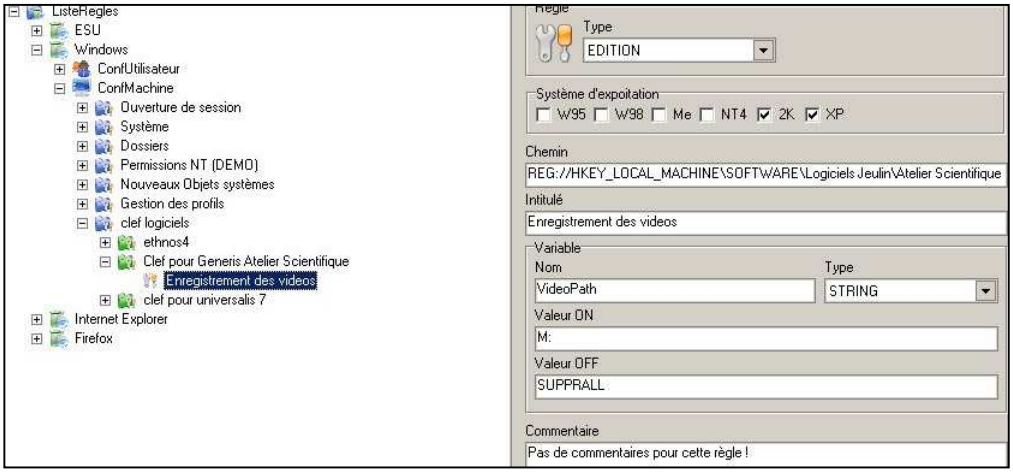
- soit par **modification de la branche « Hkey Current User »** de la base de registre **par le script de logon**.
  Par exemple :
  - pour les associations entre les extensions jpg, bmp, gif, png, … et **Photofiltre** qui est installé sur le «serveur d'applications partagées».
  - pour les menus contextuels de **7zip** qui est lui aussi installé sur un «serveur d'applications partagées».

- soit par application d'une **modification dans la base de registre par ESU4** en profitant des droits accordés par l 'élévation de pouvoir.

  Par exemple
  - Pour l'application **Ethnos4** qui est installée sur le «serveur d'applications partagées» mais nécessite une nouvelle clé dans ConfMachine>clef logiciels pour pouvoir fonctionner sans aucune installation sur les postes.



- Pour le client « **Atelier scientifique de Jeulin** » qui nécessite une configuration particulière pour que les vidéos soit enregistrées dans le dossier « Mes documents » (lecteur **M:**).

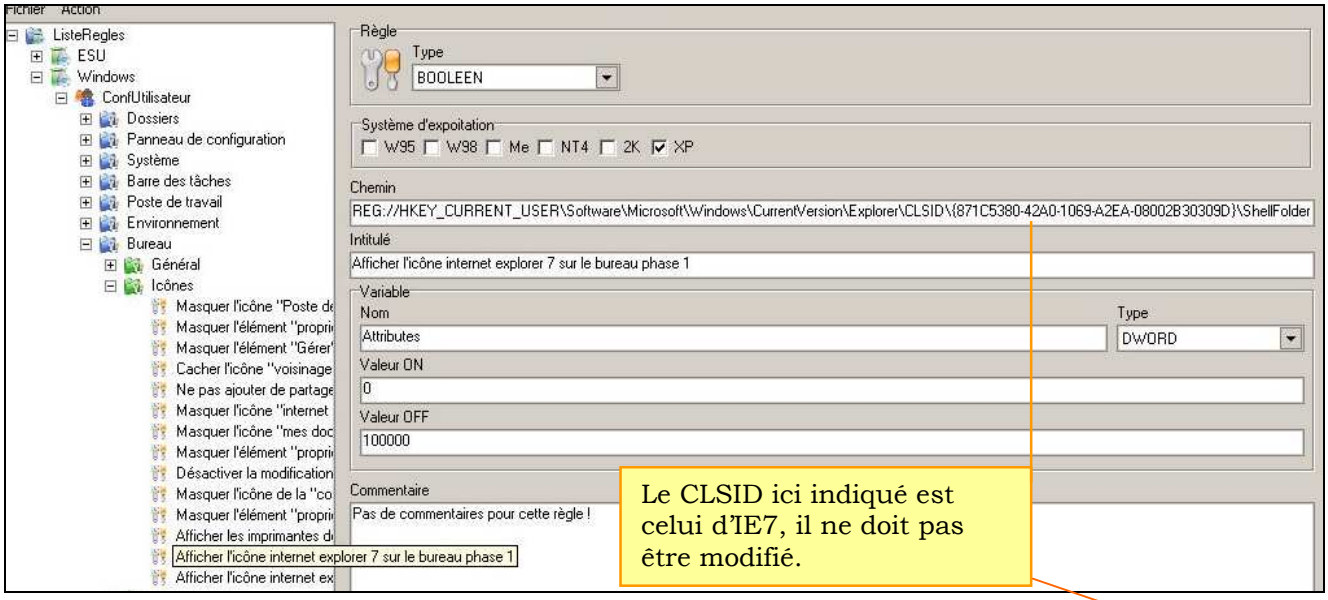


7 Des règles pour configurer automatiquement Internet Explorer 7.

Au moment de l'écriture de cette brochure, aucune prise en compte officielle d'IE7 n'était faite par ESU4, aussi nous avons créé l'ensemble des règles suivantes permettant une prise en compte de IE7 par ESU4 au même titre que la version IE6.

<u>Règle n°1 :</u> Règles permettant d'afficher l'icône d'Internet Explorer 7 sur le bureau

Cette première règle peut être activée en permanence, que l'on souhaite afficher l'icône sur le bureau ou non.



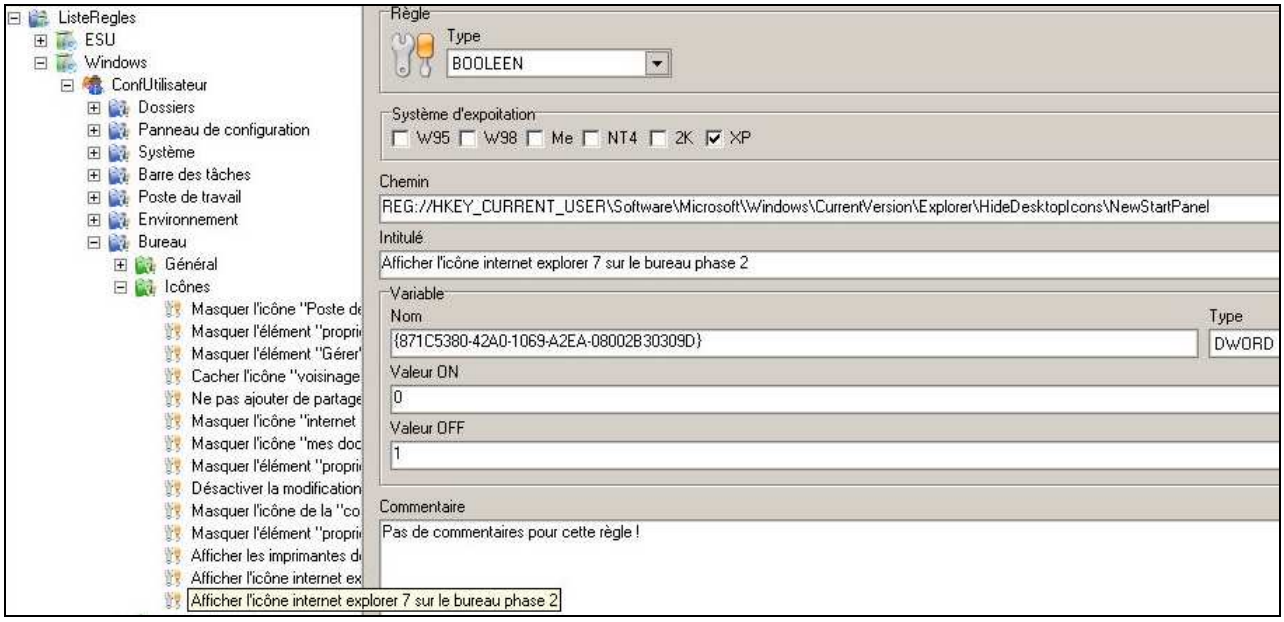
<u>Règle utilisée :</u>

REG://HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder

Nom de la variable : **Attributes**

Valeur ON : **0**
Valeur OFF : **100000** (attention à ne pas mettre une autre valeur, sinon la désactivation de cette règle n'aura aucun effet)

En laissant la première règle activée en permanence, l'affichage de l'icône d'ie7 sur le bureau ne dépend que de l'activation ou non de la règle suivante :



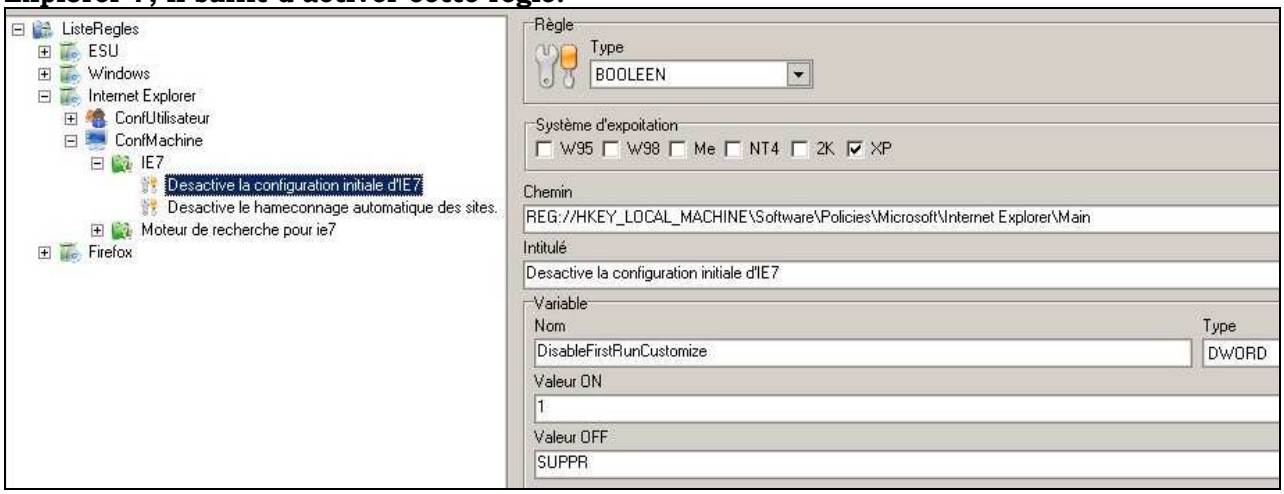
Règle utilisée :

REG://HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel

Nom de la variable : **{871C5380-42A0-1069-A2EA-08002B30309D}**

Valeur ON : **0**
Valeur OFF : **1**

Règle n°2 : Pour éviter les demandes de configuration lors du premier lancement d'Internet Explorer 7, il suffit d'activer cette règle.



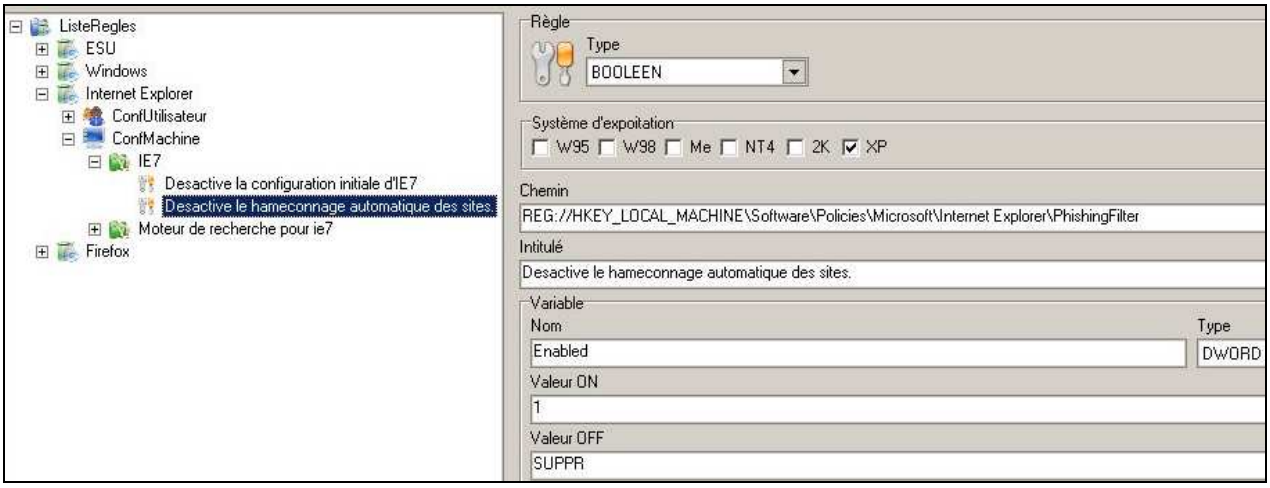
Règle utilisée :

REG://HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main

Nom de la variable : **DisableFirstRunCustomize**

Valeur ON : **1**
Valeur OFF : **SUPPR**

Règle n°3 : Activer cette règle empêche Internet Explorer 7 d'hameçonner automatiquement les sites (sans l'application de cette règle et en empêchant l'utilisateur de configurer tout ce qu'il veut dans Internet Explorer 7, on risque de ne pas pouvoir accéder à certains sites, hameçonnés automatiquement, sans possibilité pour l'utilisateur de l'empêcher).



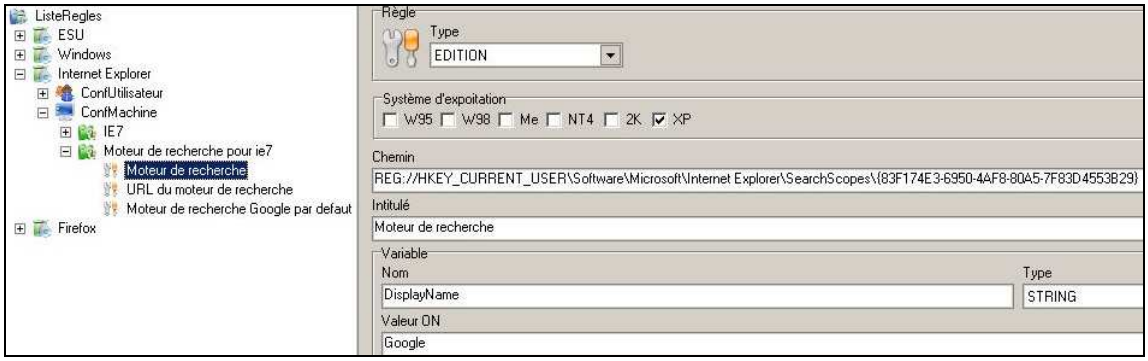
Règle utilisée :

REG://HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\PhishingFilter

Nom de la variable : **Enabled**

Valeur ON : **1**
Valeur OFF : **SUPPR**

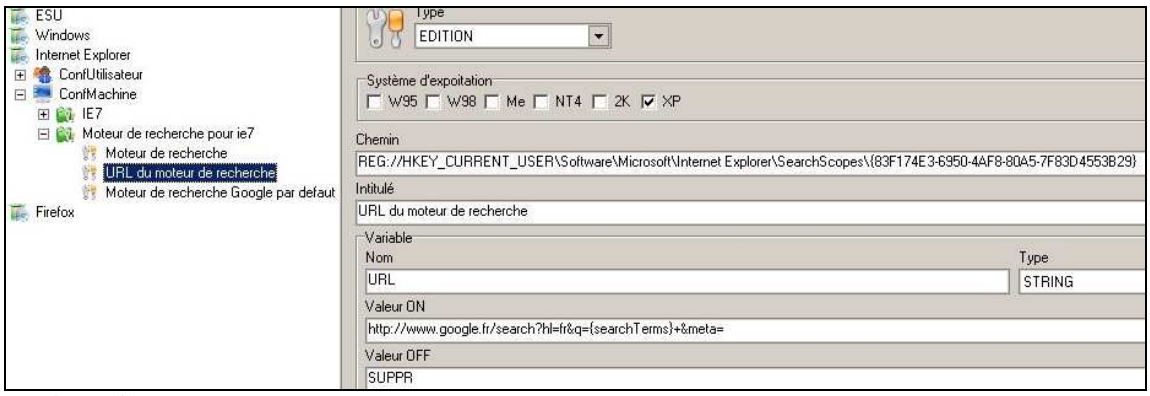
<u>Règles n°4 :</u> Activer ces règles affecte à Internet Explorer 7 le seul moteur de recherche Google dans la barre d'outils et désactive la possibilité d'en ajouter d'autres.



<u>Règle utilisée :</u>
REG://HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{83F174E3-6950-4AF8-80A5-7F83D4553B29}

Nom de la variable : **DisplayName**

Valeur ON : **Google**
Valeur OFF : **SUPPR**

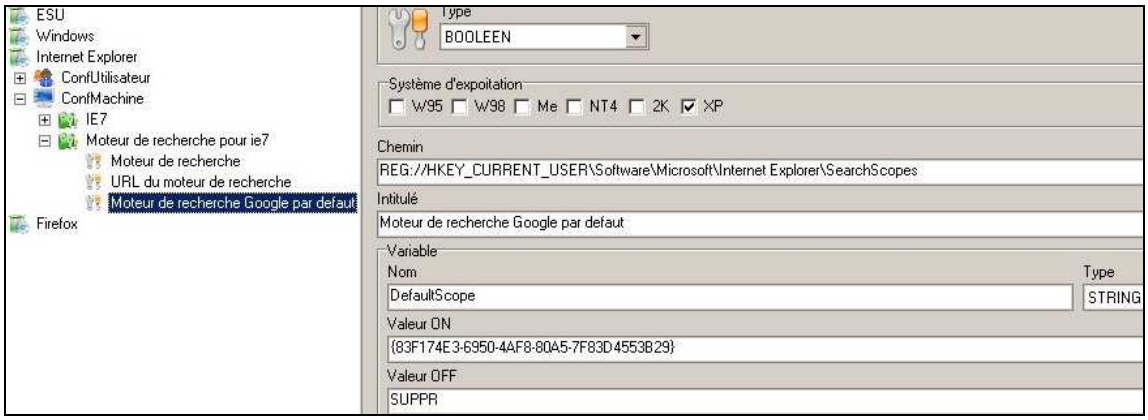


<u>Règle utilisée :</u>

REG://HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{83F174E3-6950-4AF8-80A5-7F83D4553B29}

Nom de la variable : **URL**

Valeur ON : **http://www.google.fr/search?hl=fr&q={searchTerms}+&meta=**
Valeur OFF : **SUPPR**



<u>Règle utilisée :</u>

REG://HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes

Nom de la variable : **DefaultScope**

Valeur ON : **{83F174E3-6950-4AF8-80A5-7F83D4553B29}**
Valeur OFF : **SUPPR**

Application de ces règles

<u>Attention</u> : il est important pour une machine où est installé IE7 qu'un premier lancement du navigateur soit fait par l'administrateur afin que l'icône apparaisse sur le bureau. Nous n'avons pas pour l'instant recherché de parade à ce petit problème.

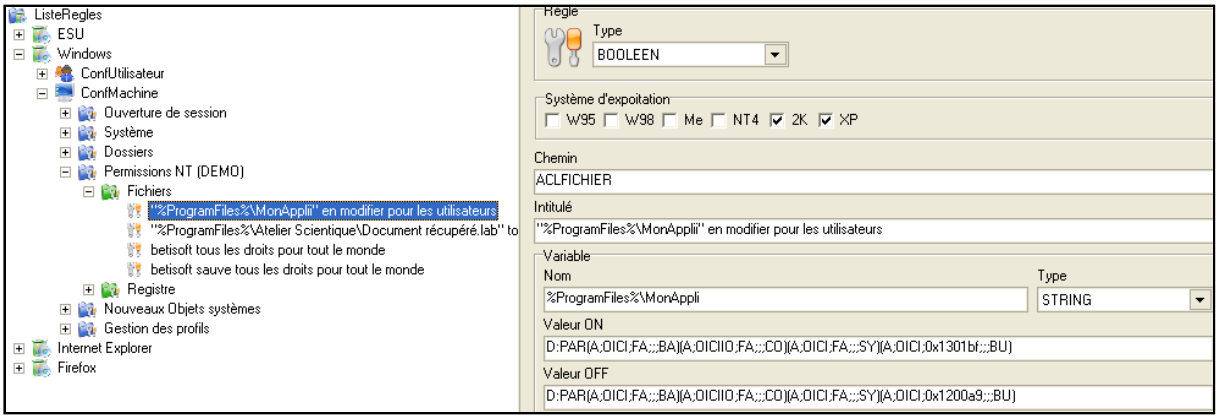
8 Ajout automatisé de permissions sur une machine locale (dossiers ou base de registre).

<u>a) Utilisation des règles pré-écrites</u>

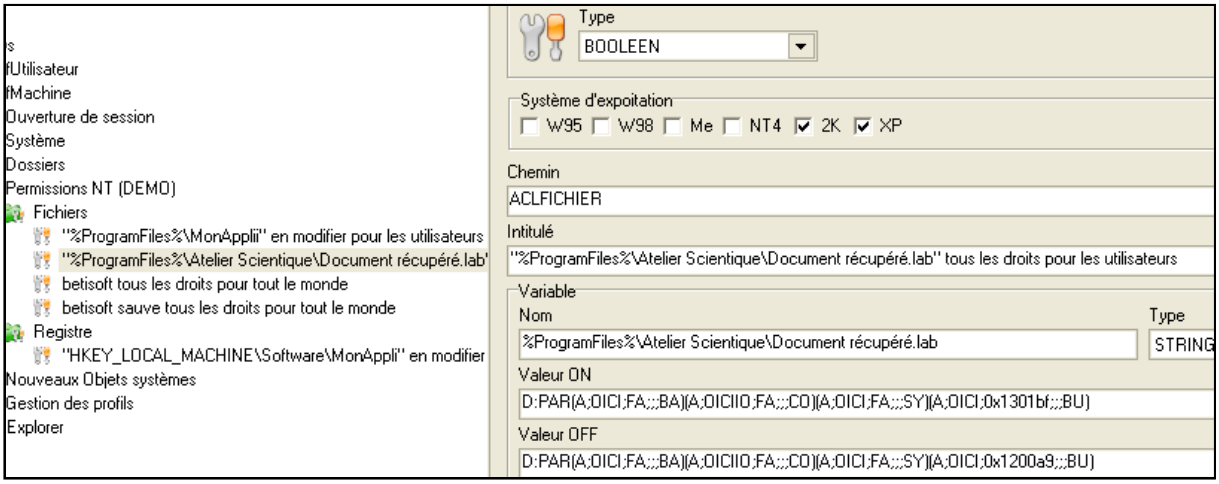
Dans ESU, deux exemples déjà intégrés permettent de voir ce qu'il est possible de faire.

- « **"%ProgramFiles%\MonAppli" en modifier pour les utilisateurs** » pour les modifications de droits sur des dossiers ou des fichiers
- « **"HKEY_LOCAL_MACHINE\Software\MonAppli" en modifier pour les utilisateurs** » pour les modifications de droits sur la base de registre.

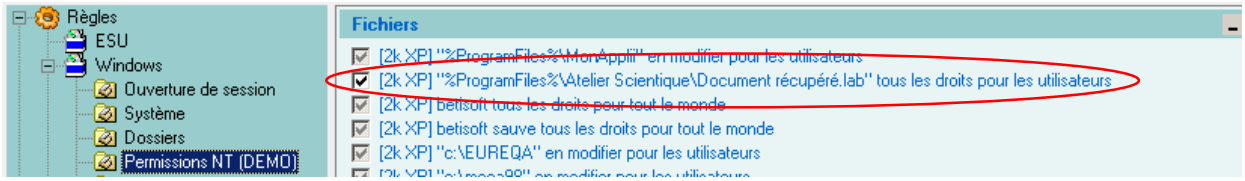
Pour donner à TOUS les utilisateurs les droits sur un dossier et ses sous dossiers ou bien sur un fichier, il faut ouvrir l'éditeur de règles et recopier la règle « **"%ProgramFiles%\MonAppli" en modifier pour les utilisateurs** ». Ensuite il faut simplement (et uniquement) remplacer le Nom de la variable (anciennement « %ProgramFiles%\MonAppli ») par le chemin menant au répertoire dont on souhaite modifier les droits.



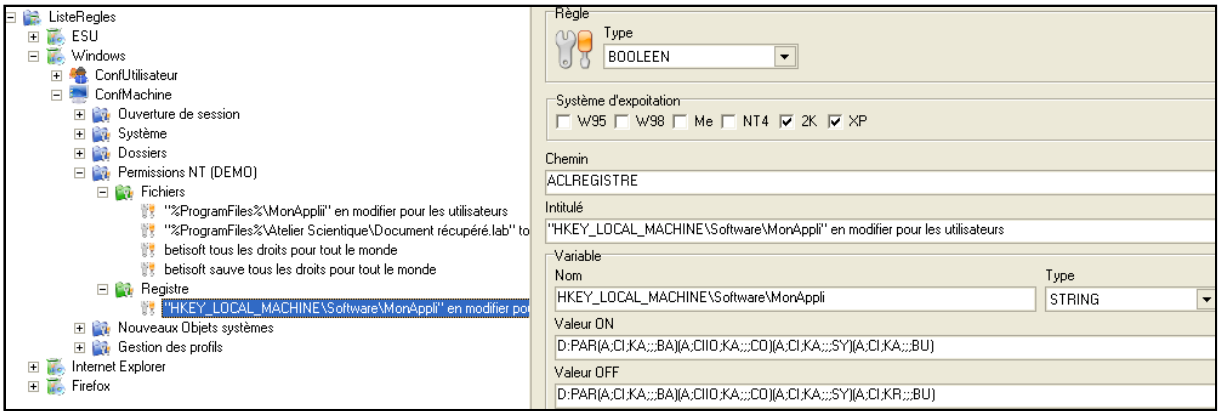
Dans l'exemple suivant, les droits ont été donnés à tous les utilisateurs sur le fichier « %ProgramFiles%\Atelier Scientique\Document récupéré.lab »



Ensuite, il ne faut pas oublier de **relancer la console ESU pour activer la règle** que l'on vient de créer.



Pour la base de registre, le principe est rigoureusement le même, sauf qu'il faut remplacer « **HKEY_LOCAL_MACHINE\Software\MonAppli** » par la clef sur laquelle on souhaite donner des droits.



b) Explications et construction avancée de règles

Dans le cas de pose de droits sur un dossier ou un fichier, la valeur ON entrée par défaut dans ESU est la suivante :
"**D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1301bf;;;BU)**"

En voici le décryptage complet fait par olivier Adam, ainsi que les liens vers les sites de Microsoft détaillant tout cela :
http://www.washington.edu/computing/support/windows/UWdomains/SDDL.html
http://msdn2.microsoft.com/en-us/library/aa379570.aspx

Cette chaîne de caractère correspond à un descripteur de sécurité pour un fichier.

D: → c'est une DACL
PAR → l'héritage depuis le conteneur (le dossier précédent) est rompu

Chaque "( )" contient une ACE (entrée d'accès)

A → ACE de type autorisé(allowed) en opposé avec D; : ACE de type refusée (denied))
OICI → héritage pour le contenu
OI → Les objets fils qui sont des conteneurs (les sous dossiers par ex) héritent de cette ACE
CI → Les objets fils qui ne sont pas des conteneurs (des fichiers par ex) héritent de cette ACE

FA → Full Access : Accès complet pour l'utilisateur ou le groupe associé à cette entrée
BA → Builtin Administrators, le groupe local des administrateurs de la machine (pas du domaine)
A → ACE de type autorisé(allowed) en opposé avec D; : ACE de type refusée (denied))
OICIIO
OI → Les objets fils qui sont des conteneurs (les sous dossiers par ex) héritent de cette ACE
CI → Les objets fils qui ne sont pas des conteneurs (des fichiers par ex) héritent de cette ACE
IO → L'objet courant n'est pas affecté par cette ACE, elle ne concerne que son contenu
FA → Full Access : Accès complet pour l'utilisateur ou le groupe associé à cette entrée
CO → Créateur propriétaire

A → ACE de type autorisé(allowed) en opposé avec D; : ACE de type refusée (denied))
OICI → cf. ci-dessus
FA → Full Access
SY → System : le système d'exploitation
A → ACE de type autorisé(allowed) en opposé avec D; : ACE de type refusée (denied))
OICI → cf. ci-dessus
0x1301bf → valeur de permission en hexadécimal : correspond à RWXD : lecture modification, exécution et suppression
BU → Bultin Users : le groupe local "utilisateurs" de la machine.

La valeur OFF est quant à elle la suivante :
« **D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)** »

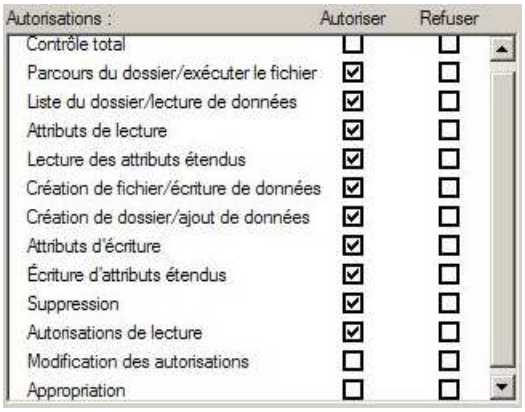
Pour résumer, les deux chaînes de caractères commencent par :

- D:PAR : une nouvelle série de droits est créée et cela ne dépend plus des dossiers contenant les fichiers suivants (on fait reset sur les droits en quelque sorte)
- (A;OICI;FA;;;BA) le groupe des administrateurs **locaux** a tous les droits sur l'objet et tous les objets fils
- (A;OICIIO;FA;;;CO) le créateur propriétaire a tous les droits sur tous les objets fils mais pas sur l'objet en question
- (A;OICI;FA;;;SY) le système a tous les droits sur l'objet et tous les objets fils

Viennent ensuite les deux chaînes donnant la pose des droits proprement dite :

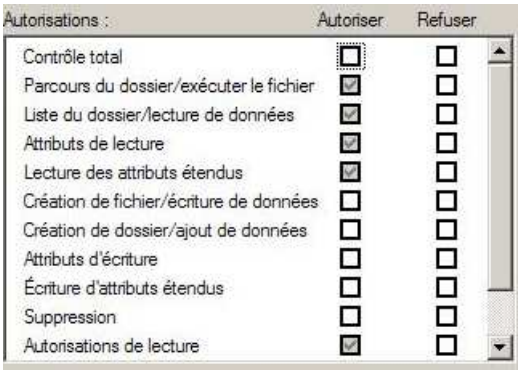
- (A;OICI; 0x1301bf;;;BU) qui correspond à donner lecture modification, exécution et suppression au groupe local "utilisateurs" de la machine sur l'objet et tous les objets fils

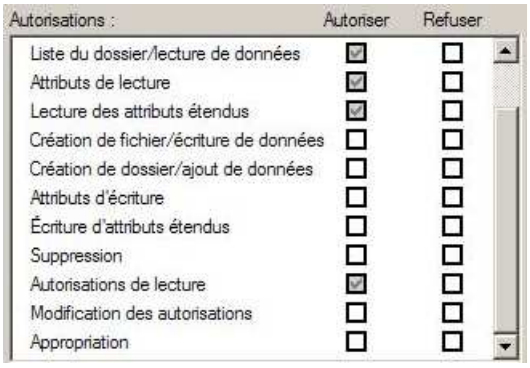
A l'aide de cette règle, on obtient les droits suivants :



- (A;OICI; 0x1200a9;;;BU) qui correspond à donner lecture, modification, exécution et suppression au groupe local "utilisateurs" de la machine sur l'objet et tous les objets fils

A l'aide de cette règle, on obtient les droits suivants :





Ces droits sont les valeurs par défaut pour un fichier même si dans le cas ou cela est créé par ESU, il n'y a plus l'hérédité.
Il est donc possible par exemple d'utiliser les syntaxes suivantes à la place de la dernière chaîne de caractères :

- (A;OICI;FA;;;BU) donner tous les droits au groupe local "utilisateurs" de la machine sur l'objet et tous les objets fils

De la même façon, on retrouve ces droits pour les clefs de la base de registre :

- D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KA;;;BU) en valeur ON, le principe est le même, seule nouveauté, l'ACE KA qui permet d'obtenir tous les droits
- D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU) en valeur OFF, ici KR ne donne que les droits de lecture.

Par exemple
Si vous installez sur des stations **le client BCDI**, alors pour fonctionner celui-ci a besoin de droits d'écriture pour « Tout le monde ». Vous pouvez par ESU :

- Donner ces droits à l'ensemble du dossier de client BCDI (**bcdicli** dans la version 2006).
- Plus finement donner ces droits seulement à **pos.ini** et **clientC.ini**.

Pour notre part, afin de permettre dans certains cas une installation automatique du client, celui-ci est recopié sur l'unité D : qui est une partition en FAT32 ; c'est la raison qui fait que vous ne trouverez pas trace de cette règle dans notre liste de règles.

9 Les gestionnaires de salle.

ESU4 permet de **déléguer l'administration de « salles »** à un ou plusieurs utilisateurs du domaine ou à un groupe d'utilisateurs du domaine.
Cette possibilité n'est opérationnelle que si la case « **Activer la délégation de la gestion des groupes de machines** » est cochée. Cf. paragraphe 2.

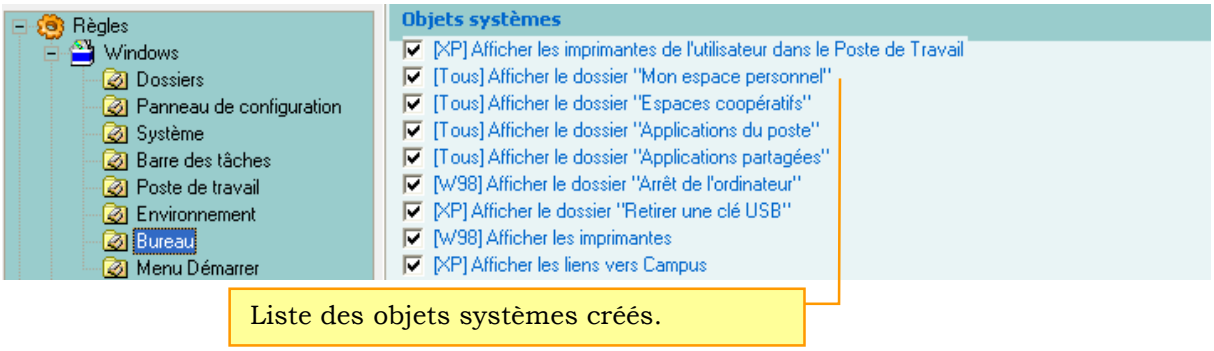
Les utilisateurs ou groupes d'utilisateurs sont automatiquement inclus dans le groupe d'administrateurs locaux des stations de la salle concernée.

Les machines de la salle C206 admettent comme administrateurs locaux les membres du groupe **LocalAdmins**.

L'opération consistant à inclure le gestionnaire dans le groupe des administrateurs locaux d'une station n'étant pas réversible, il est préférable de ne pas mettre des utilisateurs mais seulement des groupes du domaine puisque dans ceux-ci, on peux facilement mettre ou enlever des noms.

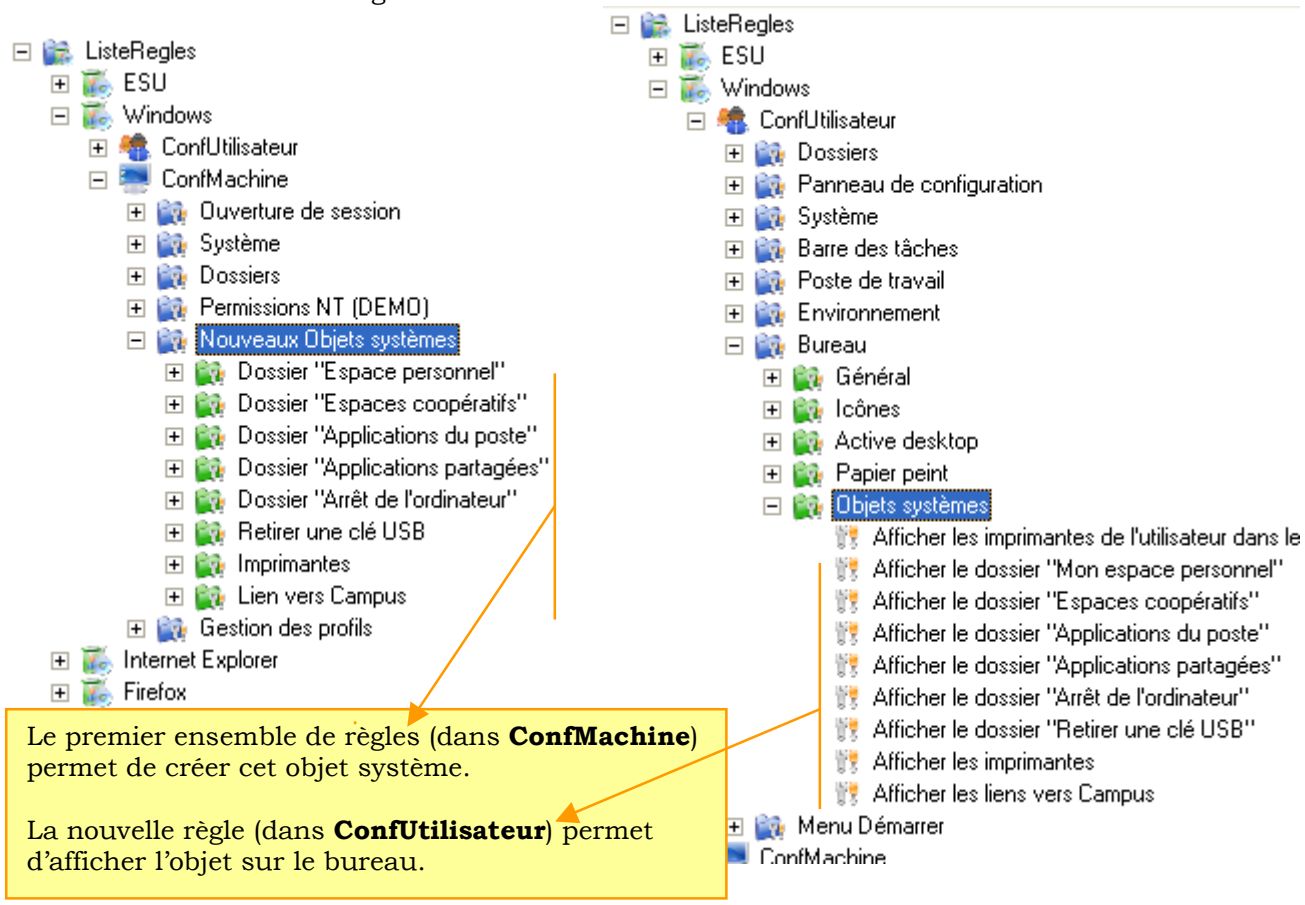
Nous n'utilisons qu'un seul groupe de gestionnaires de salle dont le rôle très spécifique que nous lui avons attribué est précisé au paragraphe 15.

10 Les objets systèmes ajoutés



Nous avons eu besoin de créer des « objets systèmes » apparaissant sur le bureau des utilisateurs. Pour cela, on utilise « **editeur.exe** » fourni avec ESU 4 (version 4.1).

Il faut créer des nouvelles règles dans deux endroits :



Cela permet donc de créer des « objets systèmes » sur le bureau qui peuvent dépendre du système d'exploitation , ce qui n'est pas le cas avec les bureaux que l'on trouve dans le répertoire icône$.

A Un exemple précis : le dossier « applications du poste »

Notre objectif était ici de créer un raccourci sur le bureau menant **vers le répertoire contenant tous les raccourcis vers les applications installées en local sur le poste**, sachant que ce répertoire est dans le partage **ICONES$** créé par ESU4 et **dépend de l'utilisateur et du groupe de machines**. Par exemple :

« ICONES$\B0SP\DomainUsers\Menu Démarrer\Programmes » pour tous les membres du groupe « DomainUsers » de la salle « B0SP ».

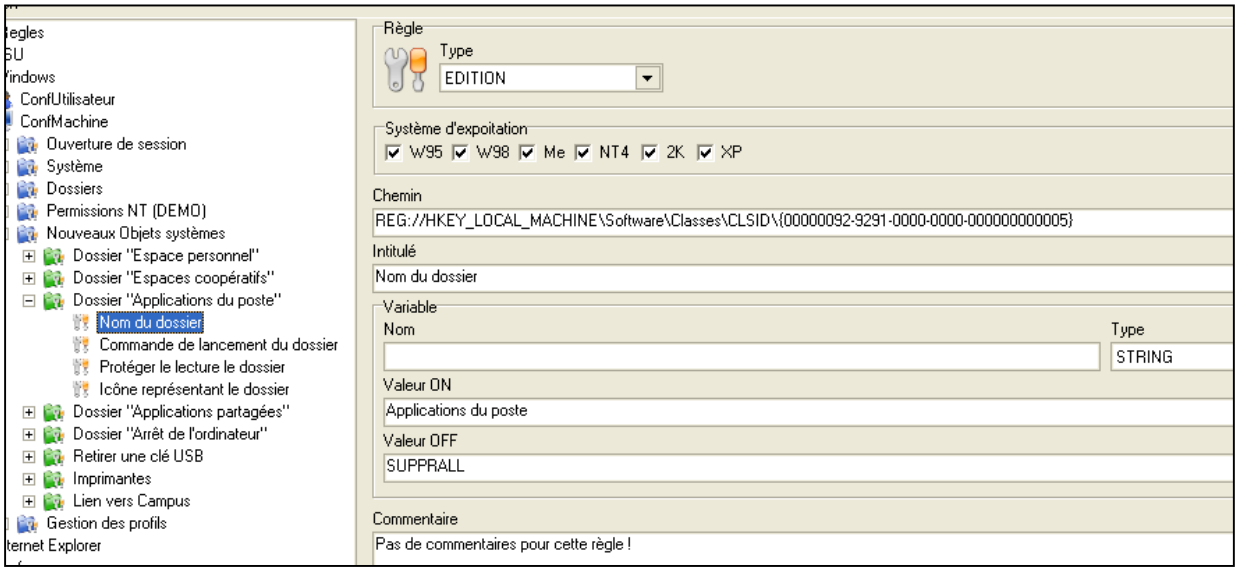
« ICONES$\C206\Professeurs\Menu Démarrer\Programmes » pour tous les membres du groupe « Professeurs » de la salle « C206 ».

C'est à dire en faisant en sorte que ce raccourci change pour chaque groupe de machines et chaque groupe d'utilisateurs.

a ConfMachine

Pour créer l'objet système, on fait un copier coller d'un bloc de règles existant ou on le créé directement à partir de cet exemple. Nous avons nommé ce dossier « applications du poste ». Il faut ensuite modifier les règles ainsi créées une par une :

α) nom du dossier



Il faut penser à cocher les cases pour tous les systèmes d'exploitation, notre règle étant compatible avec tous les systèmes, sachant que, de plus, nous voulons l'utiliser quelque soit le système d'exploitation.

Le chemin est ici :

REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9291**-0000-0000-000000000**05**}

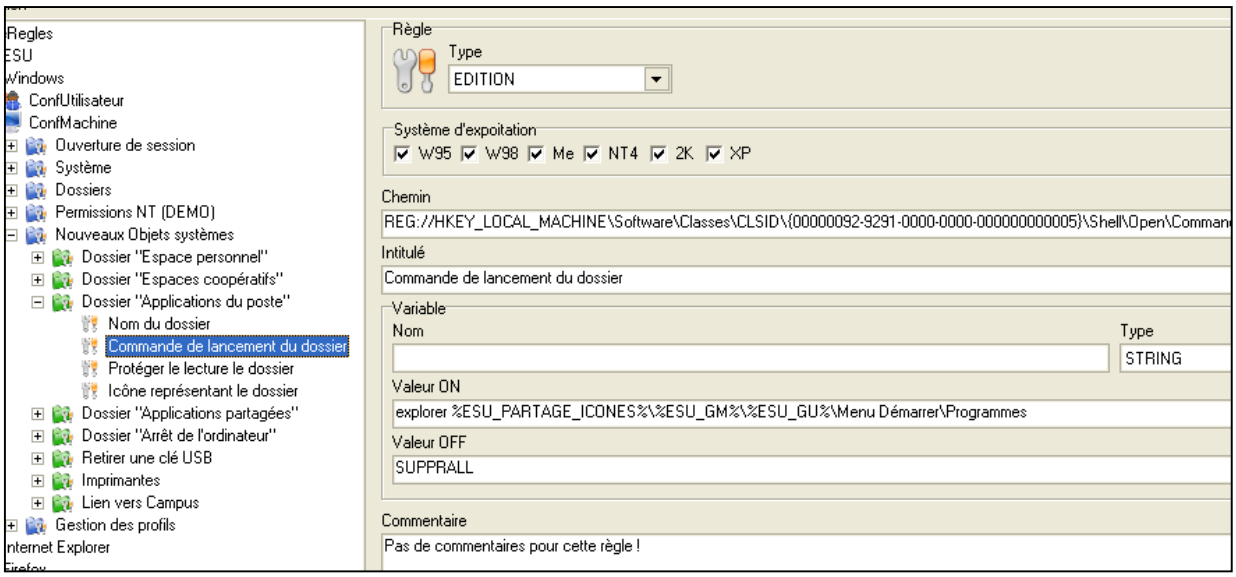
Nous avons fait en sorte que ceci ne soit pas un doublon avec les autres règles du dossier Nouveaux objets système en modifiant les valeurs notées en rouge (9291 et 05).

L'intitulé (le nom de la règle qui apparaîtra sous ESU) est « Nom du dossier », il n'est pas utile de le modifier ici.

La Valeur ON sera le nom qui va apparaître sur le bureau de chaque utilisateur du poste. Nous avons donc décidé de l'appeler ici « **Applications du poste** »

La valeur OFF restera toujours à SUPPRALL et nous n'avons pas jugé utile de mettre de commentaires.

β) Commande de lancement du dossier



Il faut penser à cocher les cases pour tous les systèmes d'exploitation, notre règle étant compatible avec tous les systèmes, sachant que, de plus, nous voulons l'utiliser quelque soit le système d'exploitation.

Le chemin est ici :

REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9291**-0000-0000-000000000**05**}\Shell\Open\Command

Nous avons fait en sorte que ceci ne soit pas un doublon avec les autres règles du dossier Nouveaux objets système en modifiant les valeurs notées en rouge (9291 et 05).

L'intitulé (le nom de la règle qui apparaîtra sous ESU) est « Commande de lancement du dossier» ; il n'est pas utile de le modifier ici.

La Valeur ON sera la commande exécutée lors de chaque utilisation de cet objet système par un utilisateur du poste. Nous avons donc décidé d'utiliser la commande suivante :

« explorer %ESU_PARTAGE_ICONES%\%ESU_GM%\%ESU_GU%\Menu Démarrer\Programmes»

explorer va permettre de parcourir le dossier
« %ESU_PARTAGE_ICONES%\%ESU_GM%\%ESU_GU%\Menu Démarrer\Programmes»

La variable « %ESU_PARTAGE_ICONES% » contient un lien vers Icones$.

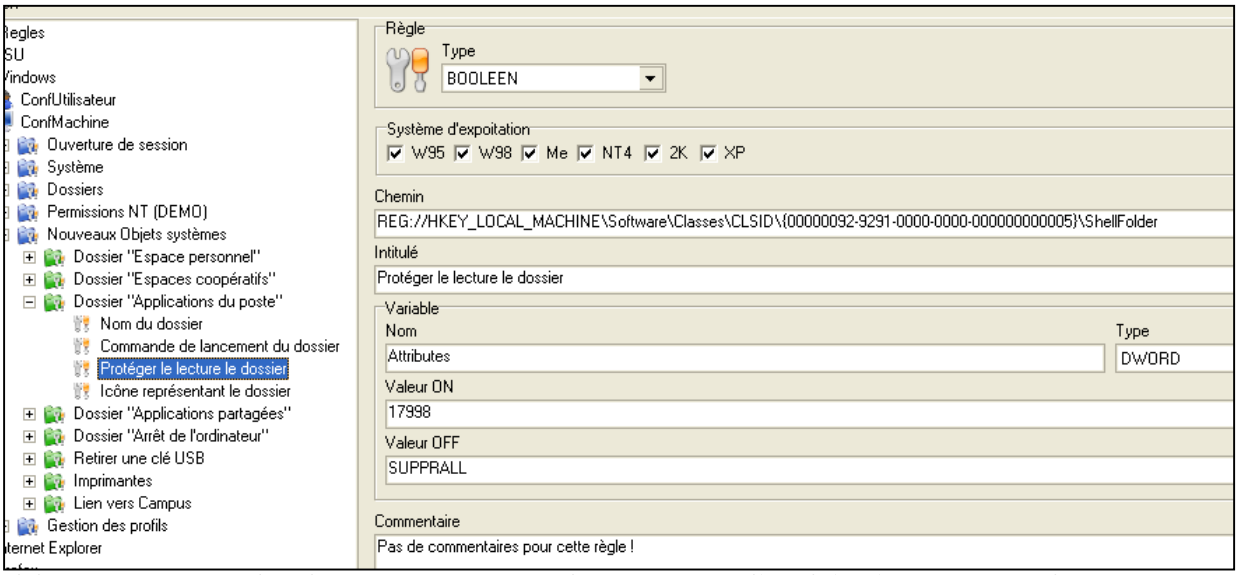
La variable « %ESU_GM% » sera remplacée par le nom du groupe de machine, suivant le groupe de machine dans lequel l'utilisateur sera connecté.

La variable « %ESU_GU% » sera remplacée par le nom du groupe auquel appartient l'utilisateur connecté.

Il est à noter que sous ESU, pour que cette règle fonctionne, il faut qu'elle soit toujours notée à l'aide des variables « %ESU_PARTAGE_ICONES% », « %ESU_GM% » et« %ESU_GU% » (voir paragraphe n°11).

La valeur OFF restera toujours à SUPPRALL et nous n'avons pas jugé utile de mettre de commentaires.

γ) Protéger le dossier



Il faut penser à cocher les cases pour tous les systèmes d'exploitation, notre règle étant compatible avec tous les systèmes, sachant que, de plus, nous voulons l'utiliser quelque soit le système d'exploitation.

Le chemin est ici :

REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9291**-0000-0000-000000000**05**}\ShellFolder

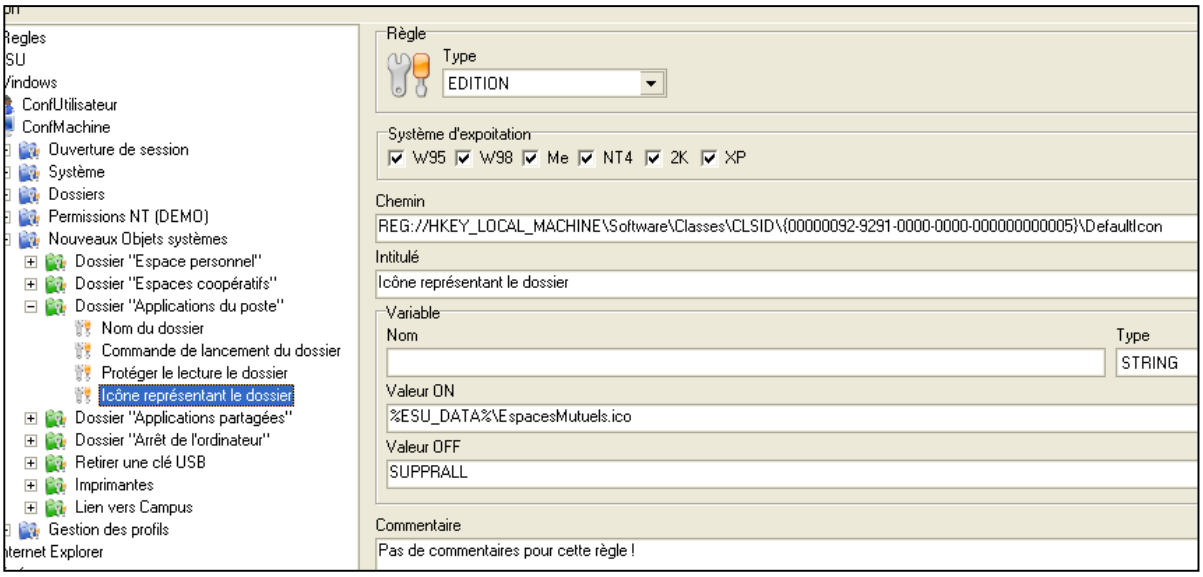
Nous avons fait en sorte que ceci ne soit pas un doublon avec les autres règles du dossier Nouveaux objets système en modifiant les valeurs notées en rouge (9291 et 05)..

L'intitulé (le nom de la règle qui apparaîtra sous ESU) est « Protéger le lecture le dossier», il n'est pas utile de le modifier ici, sauf si vous voulez enlever la faute de frappe…

La Valeur ON permet de protéger le dossier et vaut donc : « 17998 »

La valeur OFF restera toujours à SUPPRALL et nous n'avons pas jugé utile de mettre de commentaires

δ) icône représentant le dossier



Il faut penser à cocher les cases pour tous les systèmes d'exploitation, notre règle étant compatible avec tous les systèmes, sachant que, de plus, nous voulons l'utiliser quelque soit le système d'exploitation.

Le chemin est ici :

REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9291**-0000-0000-000000000**05**}\DefaultIcon

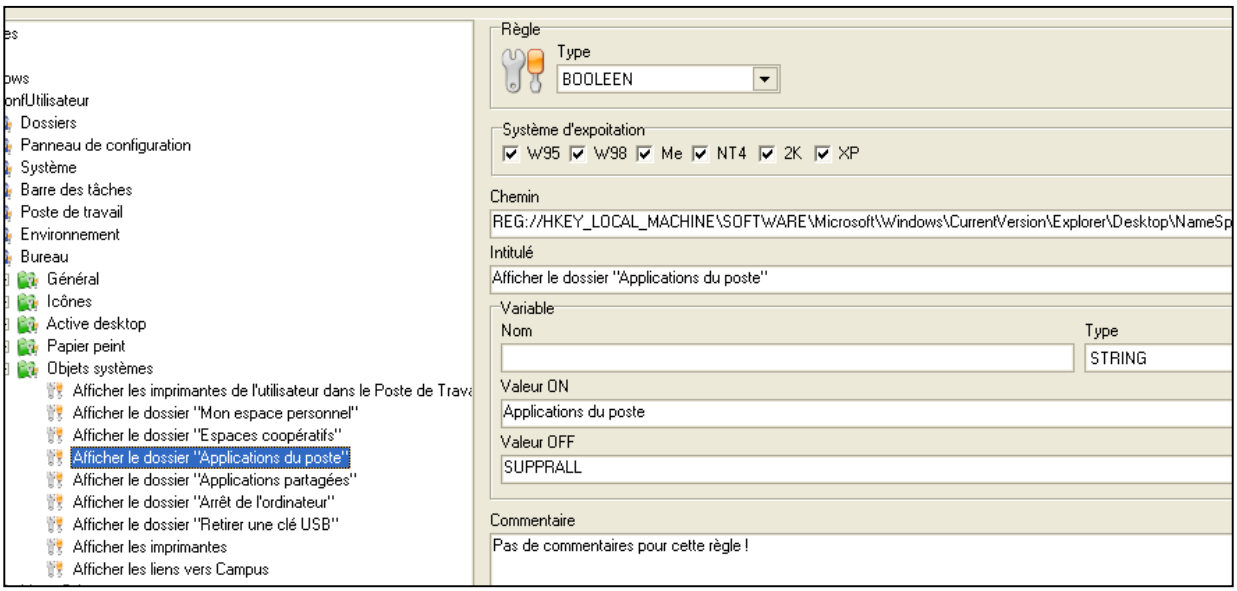
Nous avons fait en sorte que ceci ne soit pas un doublon avec les autres règles du dossier Nouveaux objets système en modifiant les valeurs notées en rouge (9291 et 05).

L'intitulé (le nom de la règle qui apparaîtra sous ESU) est « Icône représentant le dossier», il n'est pas utile de le modifier ici, sauf si vous voulez enlever la faute de frappe…

La Valeur ON est le lien vers l'icône et vaut donc : « %ESU_DATA%\EspacesMutuels.ico» mais il faut mettre ici le lien vers l'icône souhaitée.

La valeur OFF restera toujours à SUPPRALL et nous n'avons pas jugé utile de mettre de commentaires

b) ConfUtilisateur



Pour afficher l'objet système créé précédemment, il faut créer une nouvelle règle, le plus simple est copier coller une règle déjà existante, que l'on pourra ensuite modifier :

Il faut penser à cocher les cases pour tous les systèmes d'exploitation, notre règle étant compatible avec tous les systèmes, sachant que, de plus, nous voulons l'utiliser quelque soit le système d'exploitation.

Le chemin est ici :

REG://HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{00000092-**9291**-0000-0000-000000000**05**}

Nous avons fait attention de prendre les mêmes valeurs que dans le cas de ConfMachine.

L'intitulé (le nom de la règle qui apparaîtra sous ESU) est « Afficher le dossier "Applications du poste"»

La Valeur ON vaut : « Applications du poste» mais il faut mettre ici le lien vers l'icône souhaitée.

La valeur OFF restera toujours à SUPPRALL et nous n'avons pas jugé utile de mettre de commentaires

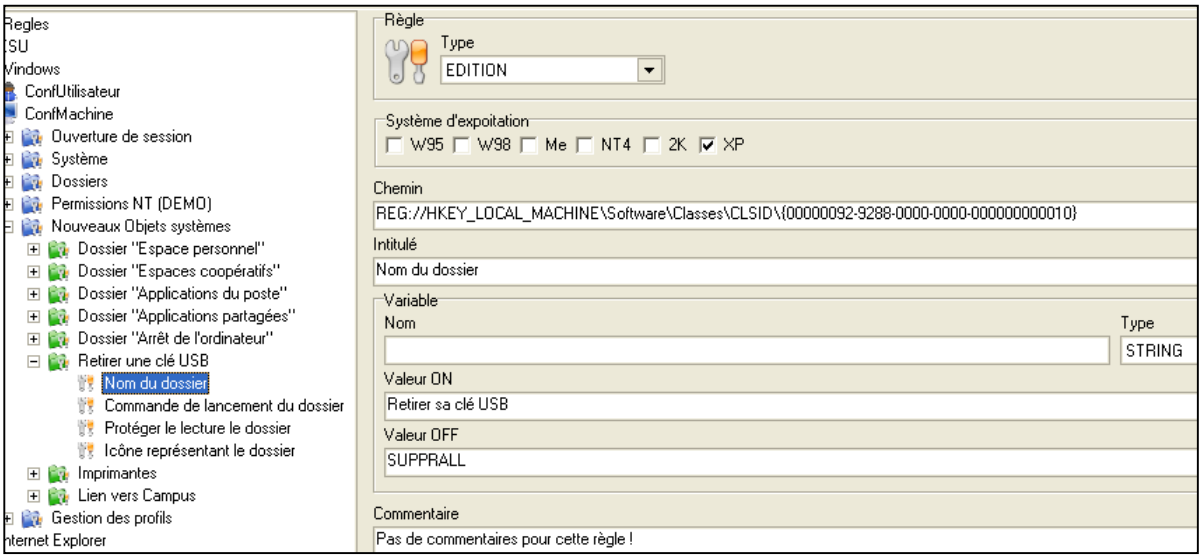
B Une méthode plus générale

a) ConfMachine

Pour créer l'objet système, on fait un copier-coller d'un bloc de règles existant pour le recopier dans le dossier nouveaux objets système ou on le crée à partir d'un modèle expliqué ici. Il faut ensuite modifier les règles ainsi créées une par une :

A chaque nouvelle règle, il est possible de choisir pour quel(s) système(s) d'exploitation les règles seront appliquées en cochant les cases appropriées.

α) nom du dossier



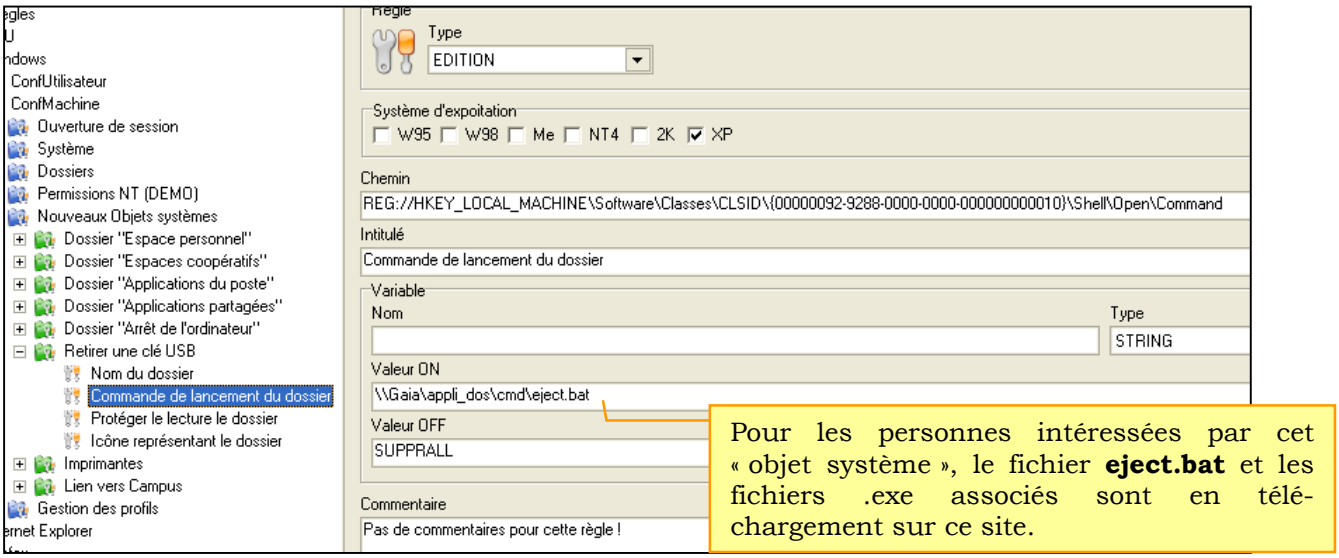
L'intitulé peut être modifié, mais cela n'est pas conseillé, c'est le nom qui apparaîtra sous ESU

Le chemin doit être modifié :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9288**-0000-0000-0000000000**10**}
En le remplaçant en diminuant 9288 de 1 et en augmentant 0000010 de 1, ce qui donne pour le nouvel objet :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9287**-0000-0000-0000000000**11**}
En faisant attention de ne pas avoir de doublons avec les objets déjà existants.

La valeur ON est celle qui apparaît par défaut dans la profils lorsqu'on sélectionne la règle. Autant mettre celle qui nous convient, on peut écrire ce que l'on veut à la place de « Retirer sa clé USB », ce sera ce qui apparaît sur le bureau. Il est possible de modifier cela à partir d'ESU, mais rentrer directement le nom souhaité ici permet d'éviter d'avoir à retaper sous ESU le nom que l'on veut donner à cet objet système pour chaque groupe de machine.

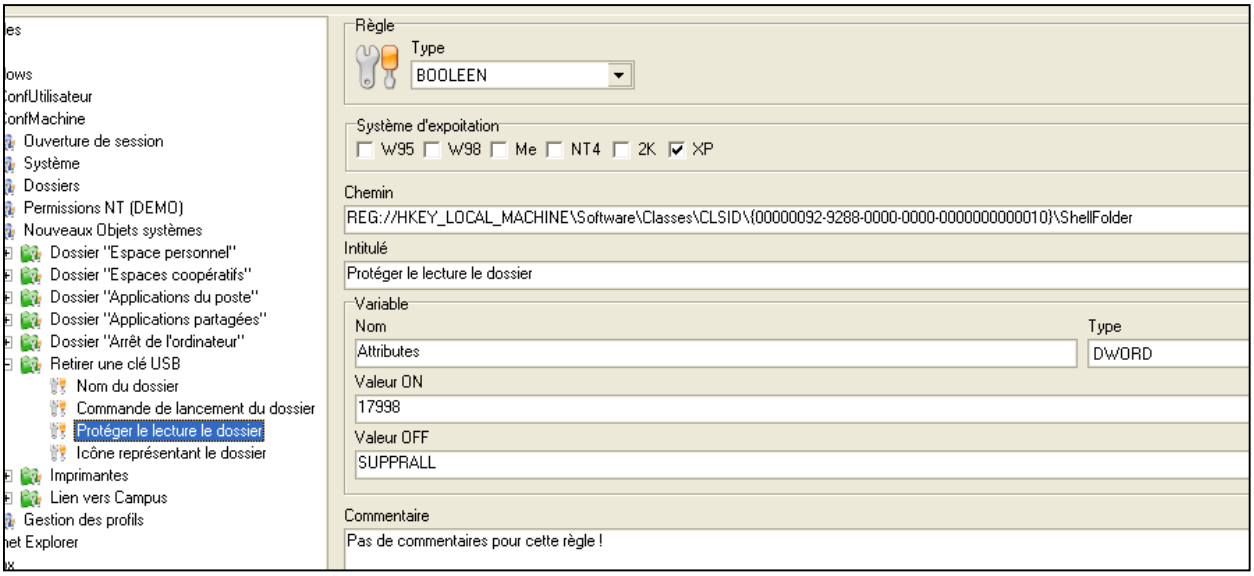
En rège générale, et même si cela n'est pas obligatoire, il est toujours préférable de mettre dans la valeur ON ce que l'on souhaite voir apparaître pour chaque application de cette règle, cela permet de gagner énormément de temps lors de la configuration d'ESU.

β) Commande de lancement du dossier



Ici aussi il faut changer le chemin **de la même manière** que précédemment :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9288**-0000-0000-000000000**10**}\Shell\Open\Command
Deviendra :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9287**-0000-0000-000000000**11**}\Shell\Open\Command
La valeur ON doit être la commande qui s'exécutera lors de l'utilisation (double–clic) de cet objet système.

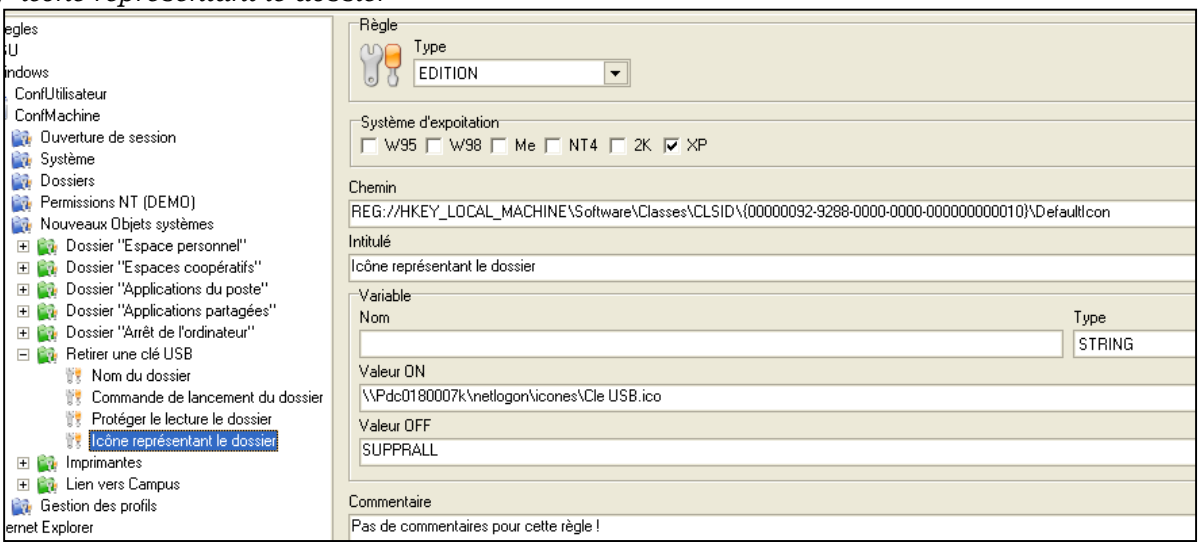
γ) Protéger le dossier



Cela empêche à tous les utilisateurs d'accéder aux propriétés du dossier et empêche toute modification ne passant pas par l'éditeur d'ESU.

La seule modification à effectuer est celle concernant le Chemin :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9288**-0000-0000-000000000**10**}\ShellFolder
Qui devient :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9287**-0000-0000-000000000**11**}\ShellFolder

δ) icône représentant le dossier

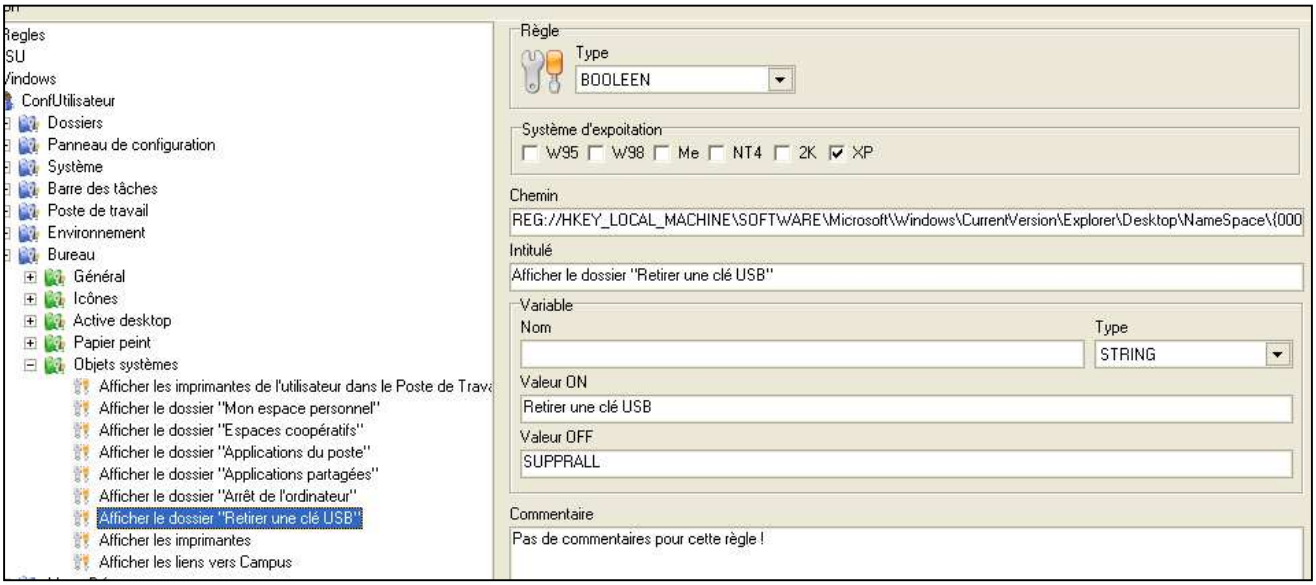


Ici encore il faut modifier le Chemin :
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9288**-0000-0000-000000000**10**}\DefaultIcon
Devient
REG://HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{00000092-**9287**-0000-0000-000000000**11**}\DefaultIcon

Et la valeur ON doit correspondre à l'endroit où se trouve l'icône représentant le dossier :

b) ConfUtilisateur

Pour afficher l'objet système créé précédemment, il faut créer une nouvelle règle, le plus simple est copier coller une règle déjà existante, que l'on pourra ensuite modifier :



Comme d'habitude, il faut modifier le chemin :
Ici :
REG://HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{00000092-**9288**-0000-0000-000000000**10**}
Devient
REG://HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{00000092-**9287**-0000-0000-000000000**11**}

En faisant attention de prendre les mêmes valeurs que dans le cas de ConfMachine.

Puis pour la valeur ON, il est possible de mettre ce que l'on veut, cela décrira ce que l'on veut faire.

11 Le service du temps

La problématique de la synchronisation horaire des machines repose sur trois contraintes :

- uniformiser la mise à l'heure des stations Windows XP, 2000 ou 98.
- autoriser les stations Windows 2000-XP à se mettrent à l'heure
- autoriser les élèves à changer la date sur certaines stations pour des enseignements de comptabilité dont les travaux sont datés et assurer la remise à date de ces stations automatiquement.

Pour résoudre ces trois points :

- Nous utilisons un serveur de temps Linux Samba (et non NTP) qui permet la synchronisation des stations à leur démarrage par **net time \\commr /set /yes** dans un des scripts de démarrage.
- Sur chaque station Windows 2000-XP, il est nécessaire d'autoriser la synchronisation horaire à « Tout le monde » comme ceci est expliqué dans le paragraphe 14.
- Afin de permettre aux élèves le changement de date sur les machines 2000-XP, et compte tenu de toutes les restrictions qui sont apportées sur les bureaux, un petit programme batch est déposé dans le dossier « Programmes » des machines concernées, il contient simplement la commande dos : **date**

12 Les imprimantes réseaux et locales

Objet informatique redoutable, l'imprimante peut se décliner en :

- imprimante locale sur un port LPT ou USB
- imprimante « locale » sur un port réseau IP que je qualifierai volontiers d'hybride.
- imprimante réseau partagée par le protocole standard de Windows.
- imprimante réseau partagée via un serveur d'impression selon divers protocoles.

Nous avons implémenté des imprimantes dans tous ces modes sauf le troisième qui est paradoxalement sans doute le plus courant.

Imprimantes réseaux partagées via un serveur d'impression CUPS

Dans l'implémentation faite, il assure une gestion centralisée des imprimantes avec automatisation des téléchargements de pilote pour chaque modèle d'imprimante.

Le serveur d'impression est un serveur **Cups** sous Samba-Linux de nom **Ipr0180007k** installé en serveur virtuel d'une machine hôte comme tous les serveurs de la solution Solaere Eole+.
Avec Christophe Dubreuil, nous avons particulièrement soigné la mise en place d'une nouvelle imprimante sur le serveur d'impression Cups :

- elle se déroule complètement par l'interface Windows XP d'ajout d'imprimantes sur le serveur **Ipr0180007k**
- elle permet le téléchargement des drivers adéquats directement sur le serveur Cups pour Windows XP, 2000 ou 98.
- elle automatise complètement l'installation d'une imprimante réseau sur un poste XP ou 2000 puisqu'à partir du moment où l'imprimante a été installée sur le serveur Cups (file d'impression + driver pour Windows 2000-XP) alors la simple déclaration de l'usage de l'imprimante dans la configuration ESU d'un poste pour un groupe d'utilisateurs provoque sa disponibilité pour ces utilisateurs avec téléchargement automatisé et silencieux du driver à la première requête d'impression.
- elle simplifie l'installation d'une imprimante réseau sur un poste Windows 98 puisqu'à partir du moment où l'imprimante a été installée sur le serveur Cups (file d'impression + driver pour Windows 98) alors l'ajout nécessaire de l'imprimante sur le poste pour tous les utilisateurs, télécharge automatiquement le driver associé.

Mais nous nous heurtons aux problèmes suivants :

- Le seul protocole que nous avons mis en service est le protocole **lpd** accepté par la majorité des imprimantes réseaux et par les postes sous tous les systèmes d'exploitation Windows.
- Les drivers fournis avec Windows XP pour les imprimantes réseaux sont parfaitement compatibles avec notre mode de fonctionnement mais les drivers fournis par certains

constructeurs d'imprimantes pour XP sont trop souvent inutilisables dans l'environnement choisi : nous utilisons alors des drivers d'origine XP, éventuellement d'un modèle équivalent antérieur.

Nous avons mis en place la politique suivante

- Afin d'éviter certains blocages de travaux en file d'impression ou déconnexions d'imprimantes, chaque heure une tâche automatisée reconnecte les imprimantes déconnectées au niveau du serveur Cups et chaque nuit, une tâche automatisée vide totalement les files d'impression où certains travaux seraient restés bloqués.
- Les « Professeurs » sont membres du groupe des administrateurs d'imprimantes réseaux (**PrinterAdmins**).

Imprimantes locales

Les imprimantes locales installées sur des postes Windows 98, Windows 2000 ou XP ne posent aucun problème spécifique.

Nettoyage des imprimantes résiduelles

Dans ESU, En cochant la case « **Supprimer les imprimantes réseaux qui ne sont pas gérées par ESU** », vous faites en sorte qu'à toute connexion sur un poste Windows 2000 ou XP, un utilisateur ne voit que les imprimantes locales ou réseaux disponibles pour ce poste.

Toutefois cette fonctionnalité n'est pas parfaitement effective chez-nous, les imprimantes ayant tendance à suivre l'utilisateur dans son profil. Aussi, nous avons doublé cette fonctionnalité d'ESU par un petit programme d'origine Microsoft, de nom **CON2PRT.EXE** qui par l'appel

\\pdc0180007k\netlogon\bin\Con2prt.exe /f

dans le script de logon **efface réellement toutes les imprimantes réseaux résiduelles**, ce qui permet à ESU d'attribuer proprement celles de l'utilisateur sur la station où il se connecte.

L'imprimante par défaut

ESU4 permet de **définir** la première imprimante réseau comme choix par défaut mais si vous ne cochez pas cette case et que vous laissiez les droits à vos utilisateurs de choisir une imprimante locale par défaut sur certains postes, alors, sous Windows 2000 et XP, ce choix est enregistré dans le profil de l'utilisateur qui retrouve sur chaque machine son choix d'imprimante par défaut.

Le problème posé par Windows 98.

Deux règles existantes sous ESU ne fonctionnent pas sous Windows 98 pour la gestion des imprimantes, à fortiori en interdisant le panneau de configuration à un utilisateur :

- Dans **Utilisateur/Poste de travail/Objets systèmes**, la règle intitulée : « **Afficher les imprimantes de l'utilisateur dans le Poste de Travail** » ne fonctionne pas sous Windows 98. Nous l'avons donc simplement cochée pour Windows 2000 et XP.
- De même pour **Utilisateur/Bureau/Objets systèmes** pour « **Afficher les imprimantes de l'utilisateur dans le Poste de Travail** » cochée uniquement pour Windows 2000 et XP.

Une solution à ce problème

Il est possible d'utiliser une règle permettant d'ouvrir un lien vers un dossier local de la machine jouant le rôle du dossier imprimantes de Windows tout en restreignant pleinement l'accès au panneau de configuration de Windows 98.

Il faut pour cela créer un dossier intitulé

Imprimantes.{2227A280-3AEA-1069-A2DE-08002B30309D}

Cela peut être fait automatiquement par l'exécutable : **creer_win98imp.exe** qui crée le dossier **C:\Imprimantes.{2227A280-3AEA-1069-A2DE-08002B30309D}**. Cet exécutable est téléchargeable sur le serveur du lycée Jacques Cœur de Bourges dont l'adresse est donnée en tête de ce document.

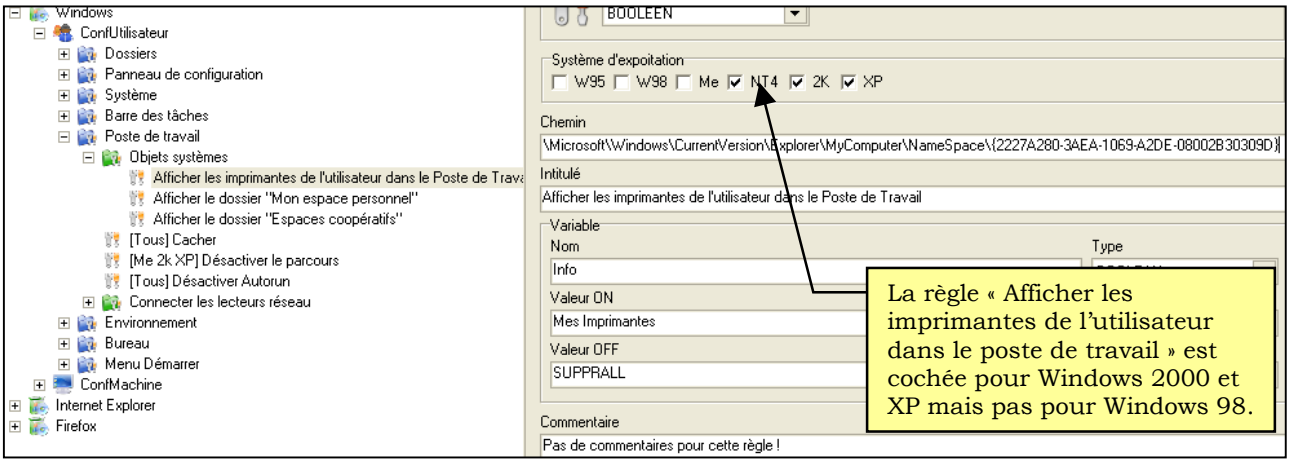
Ensuite il faut créer un objet système permettant d'ouvrir ce dossier (voir paragraphe 10). La commande permettant d'ouvrir ce dossier est :

« **explorer C:\Imprimantes.{2227A280-3AEA-1069-A2DE-08002B30309D}** ».

L'icône représentant les imprimantes peut être obtenue par :

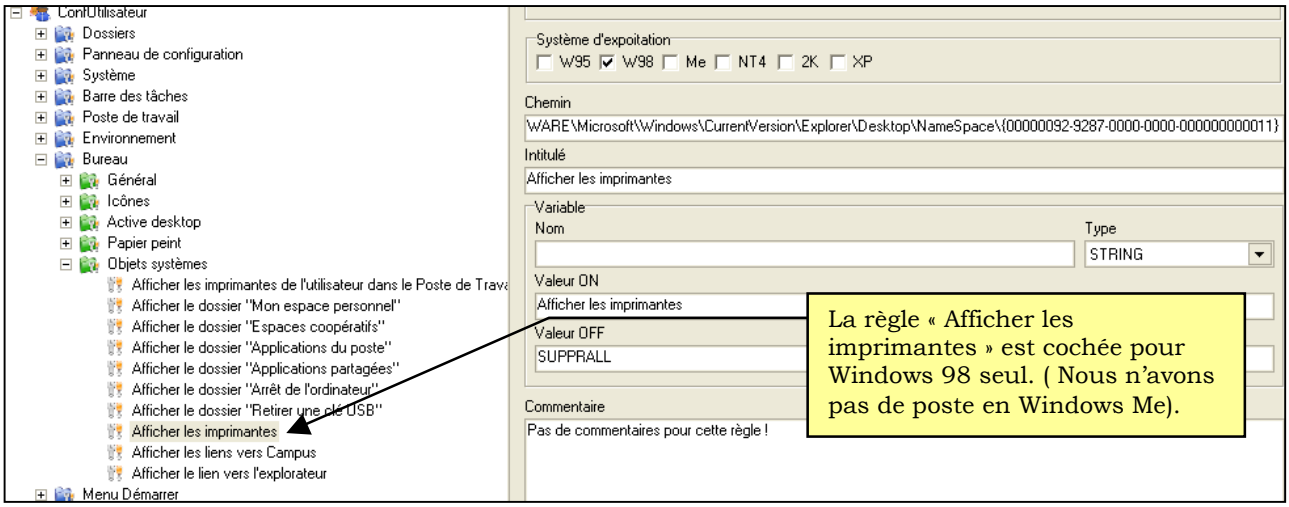
« **C:\windows\SYSTEM\shell32.dll,-138** » .

Modification de la règle « Afficher les imprimantes de l'utilisateur dans le Poste de travail »

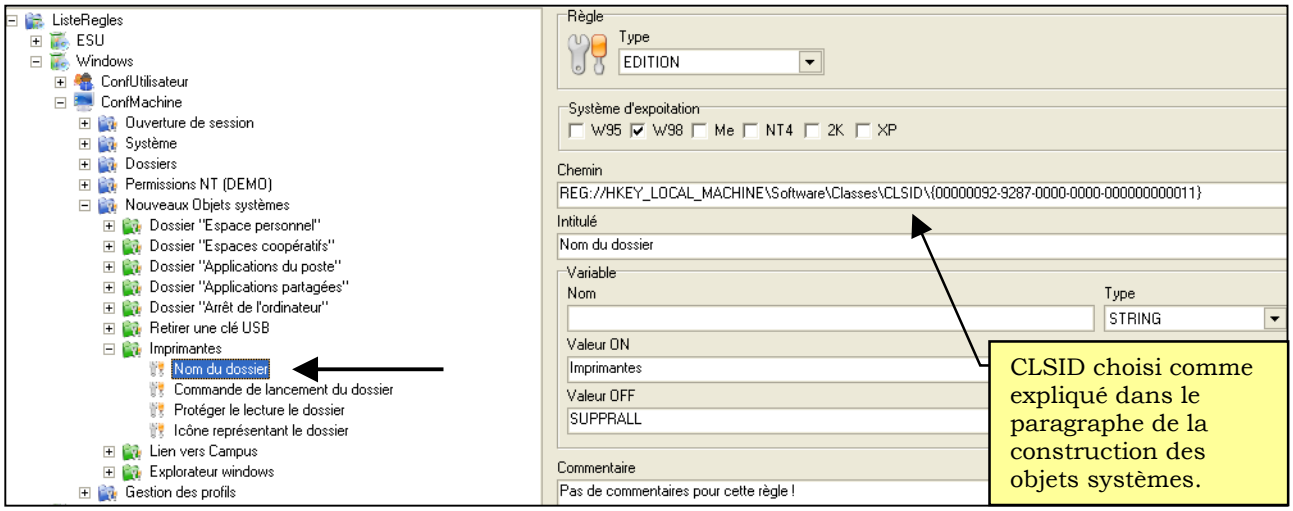


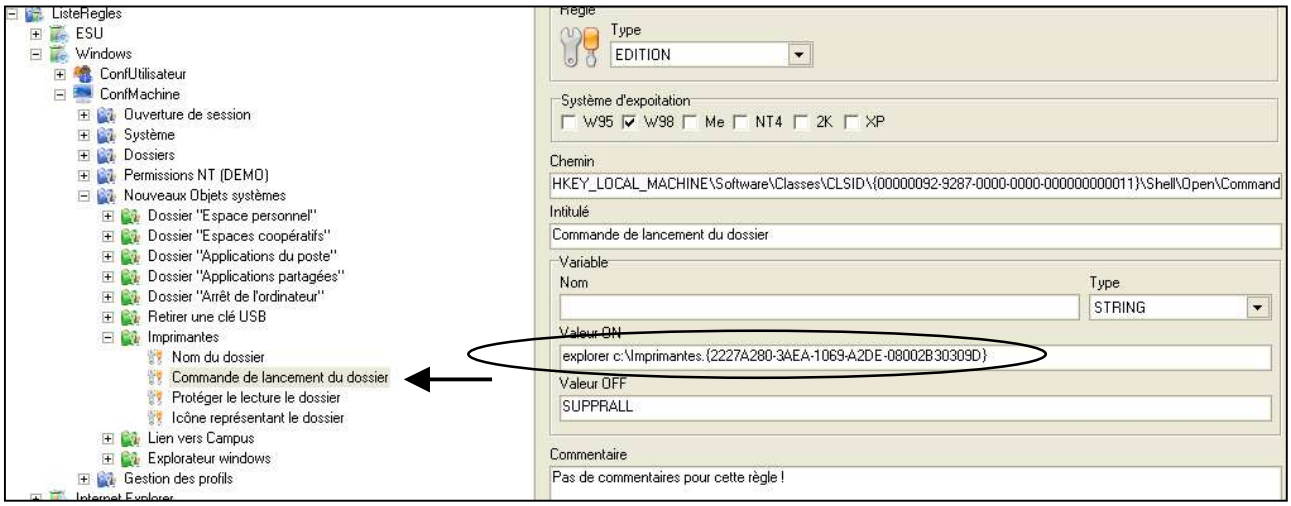
Création de l'objet système « Imprimantes »

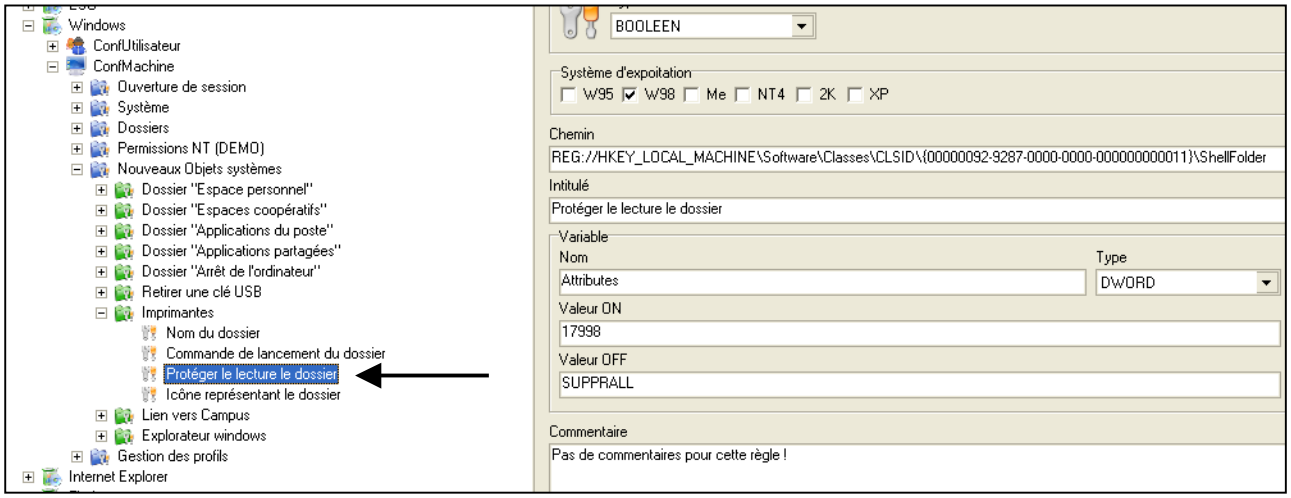
On consultera le paragraphe n°10 pour comprendre la construction de ce nouvel objet système.

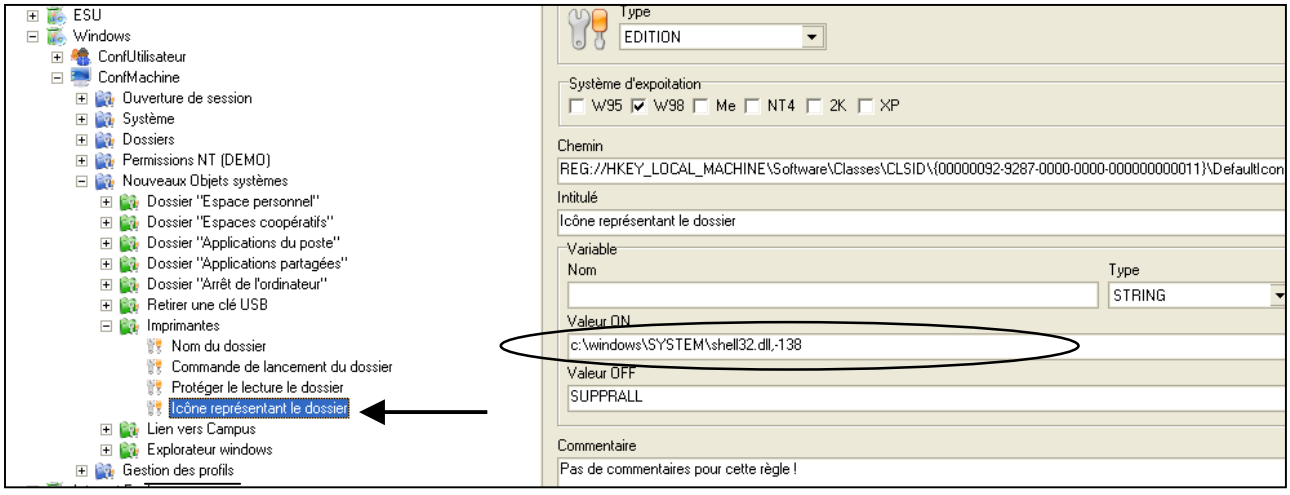


Les règles de création de cet objet système









13 Les postes Windows 98

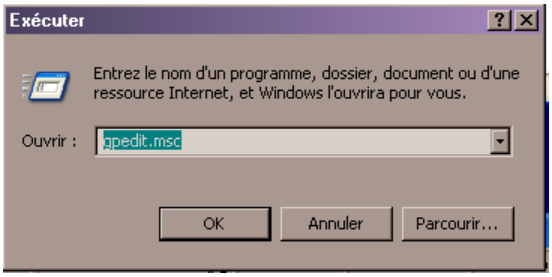
Deux connexions successives de l'administrateur permettent de configurer convenablement le poste. Nous n'avons mis en œuvre aucune configuration particulière, autre qu'**une mise à jour**, sur les postes Window 98 qui sont tous en version seconde édition. Nous n'avons pas de postes Windows Me.

Pour la rentrée 2007-2008, nous n'auront plus aucun poste sous Windows 98 qui posaient des problèmes de plus en plus redoutables dans notre système Solaere Eole+.

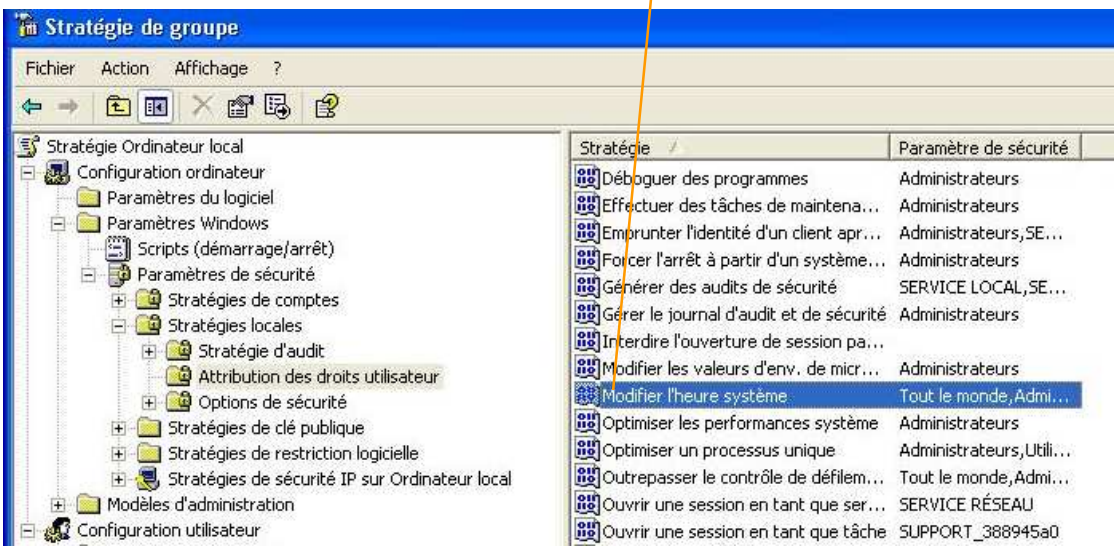
14 Les postes Windows 2000-XP

Deux connexions successives de l'administrateur permettent de configurer convenablement le poste, la première conduisant naturellement à plusieurs erreurs du système puisque l'utilisateur **#ESU4#** n'est pas encore créé. Ce n'est qu'à la deuxième ou troisième connexion que l'état de la machine est stable. Mais, il est important de configurer **préalablement** les points suivants :

a) Lancer sur le poste le programme **gpedit.msc**



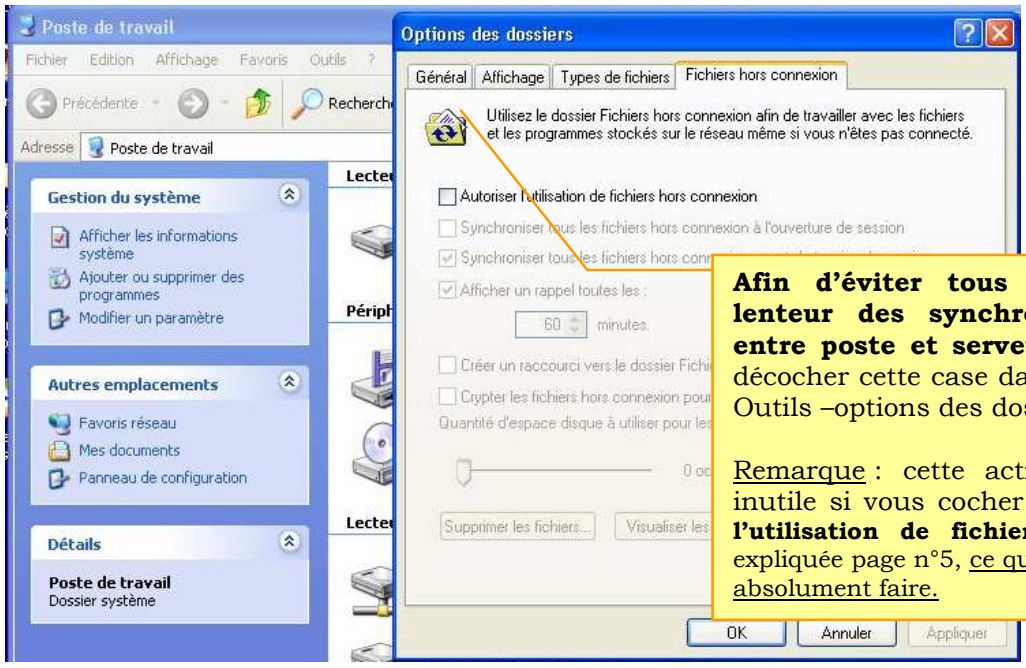
Accorder le droit de modifier l'heure système à Tout le Monde.



b) Mettre un **mot de passe à l'administrateur local** du poste.

c) Faire éventuellement un **changement des lecteurs** si vous voulez utiliser l'éjection automatisée de la clef USB par le raccourci conduisant à un script disponible sur le serveur web du lycée Jacques Cœur et uniformiser vos lecteurs sur toutes les machines du réseau que vous administrez.

d) Désactiver l'utilisation de fichiers hors connexion



Afin d'éviter tous les problèmes de lenteur des synchronisations inutiles entre poste et serveur, faire le choix de décocher cette case dans Poste de travail – Outils –options des dossiers.

Remarque : cette action est sans doute inutile si vous cocher la règle « **Désactiver l'utilisation de fichiers hors connexion** » expliquée page n°5, ce qu'il faut, de toute façon, absolument faire.

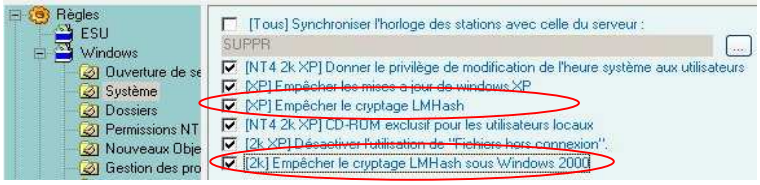
15 La sécurité et ESU4

Lors de la première connexion avec un compte du domaine, administrateur de la station, le client ESU crée un compte de nom standard #ESU4# qui fait partie du groupe des administrateurs de la station.
Lors d'une connexion avec un compte ordinaire du domaine, le client ESU utilise le pouvoir de ce compte #ESU4# pour configurer la station. Jusqu'à ESU4.01 ce compte avait un unique mot de passe sur l'ensemble des machines d'un domaine ; à partir de la version 4.02a, le mot de passe de ce compte change sur chacune des stations et à chaque connexion.
La faille qui existe inhérente au principe d'élévation de pouvoir utilisé par ESU4 est qu'il est possible en utilisant certains outils de découvrir le mot de passe associé au compte #ESU4# d'une station. Dorénavant, **connaître ce mot de passe ne donne que la possibilité de devenir administrateur de cette station pendant la durée de la session en cours**. Ce n'est pas forcément anodin mais ce n'est pas gravissime : une bonne politique qui s'impose, afin de prévenir toute tentative logicielle de capture de mot de passe est de ne jamais utiliser le compte administrateur de réseau sur les stations sensibles pour les interventions de maintenance courantes.

Ajout de la règle NoLMHash

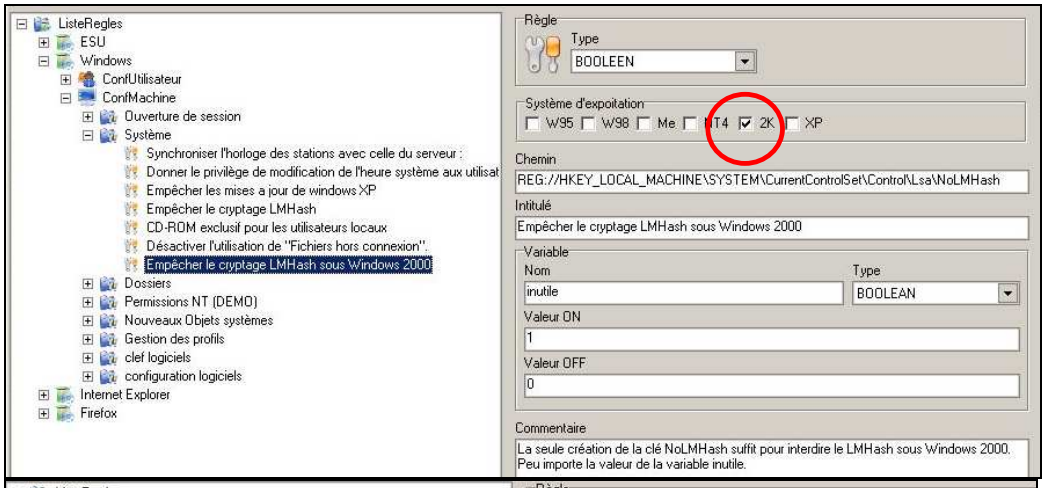
Toute station possède au moins un administrateur local et dans un réseau, souvent le mot de passe associé à l'administrateur local est identique sur l'ensemble de toutes les stations.

Sur les stations Windows 2000 ou XP, ce mot de passe est stocké en standard dans la base SAM selon deux cryptages, l'un est LM Hash et l'autre est NT Hash.



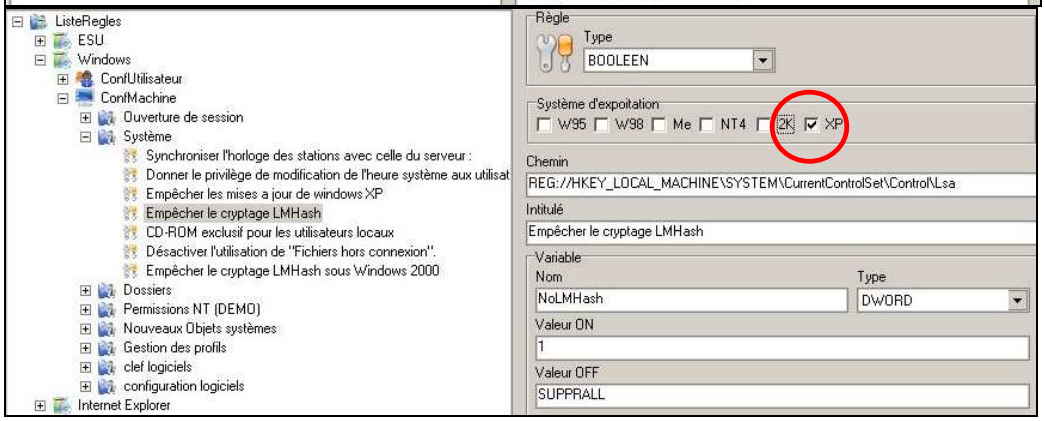
Un utilisateur qui se rendrait administrateur de la station, via le compte #ESU4# par exemple, ou qui utiliserait un outil démarrant sur un Live CD pourrait beaucoup plus facilement retrouver le mot de passe à partir de LM Hash que de NT Hash : c'est la raison qui nous a conduit à rajouter une règle faisant en sorte que les stations Windows 2000 ou XP ne stockent plus le mot de passe crypté en LM Hash mais seulement en NT Hash.

Deux règles différentes doivent être créées, l'une pour les stations 2000, l'autre pour les stations XP :



Pour Windows 2000, il suffit de créer la clé NoLMHash.

Ainsi fait, la création de la clé n'est pas réversible avec ESU et la station reste en codage NT Hash définitivement.



Pour Windows XP, il suffit de créer la valeur booléenne NoLMHash.

Le choix est alors réversible selon que la valeur est à 1 ou non.

Attention, pour les stations Windows 2000 et aussi Windows XP, même si Microsoft prétend le contraire, il faut redéfinir sur chacune des stations le mot de passe du ou des comptes concernés pour que la disparition du LM Hash soit effectif. (Cf. méthode automatisée page 39 paragraphe 16 e-)

Ce changement forcé du cryptage en cryptage fort est un élément accroissant beaucoup la sécurité pour un faible investissement mais il ne doit pas faire illusion d'absolu car il existe d'autres moyens de se rendre administrateur des stations et la bonne politique dans un réseau sera surtout celle qui fera qu'on ne puisse avoir connaissance de l'authentification complète d'un administrateur du réseau.

C'est pour cette raison que nous n'intervenons sur les machines en production pour la première maintenance qu'avec un compte du domaine membre du groupe **LocalAdmins** qui est inscrit comme gestionnaire des machines de chaque salle.
Un tel compte est donc administrateur des stations, mais non du domaine dans lequel il possède les stricts privilèges nécessaires. Il est modifiable à tout instant dans l'annuaire LDAP du serveur.

Ajout de la règle permettant d'interdire la mise en cache local des authentifications réseaux

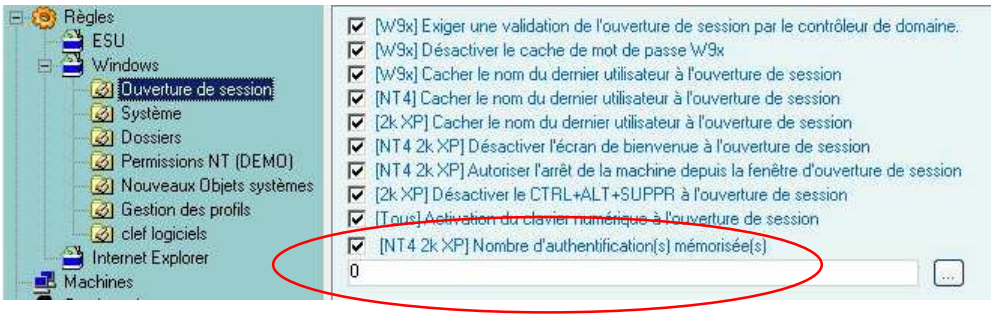
A l'ouverture d'une session réseau sur un poste Windows 2000 ou XP, **l'authentification faite sur le réseau est stockée dans un cache local sur le poste** où sont mémorisées en standard dix authentifications.

Ceci permet à tout utilisateur présent dans ces dix, de se connecter sans que la machine ne soit reliée physiquement au réseau (câble réseau débranché par exemple).

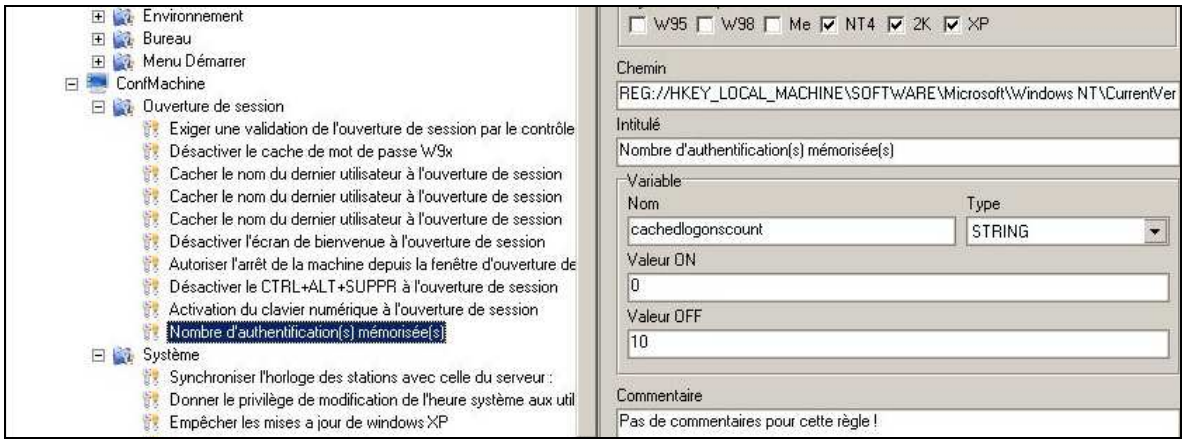
Il nous a semblé que cette possibilité nuisait à l'intégrité conceptuelle des stations et ouvrait la porte à une **brèche de sécurité importante**, aussi nous avons rajouté la règle nommée « **Nombre d'authentification(s) mémorisée(s)** » à ESU avec les deux possibilités suivantes :

- Le nombre d'authentifications mis en cache est 0 quand la case est cochée.
- Le nombre d'authentifications mis en cache est la valeur standard de 10 quand la case est décochée.

Nous vous recommandons de cocher cette case.



Ecriture de cette règle avec l'éditeur de règles.



Règle utilisée :

REG://HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Nom de la variable : **cachedlogonscount**

Valeur ON : **0**

Valeur OFF : **10**

Remarque importante : Cette règle ne devient active sur une station pour tous les comptes **qu'après un redémarrage de la station**.

16 Astuces, manques et souhaits divers

a) L'assurance de l'exécution du client ESU sur une station.

Afin de prévenir l'interruption volontaire du « **logon.bat** » par des utilisateurs mal intentionnés ou trop pressés, il est conseillé de débuter le fichier logon.bat par un appel à un **programme de blocage du clavier et de la souris**.

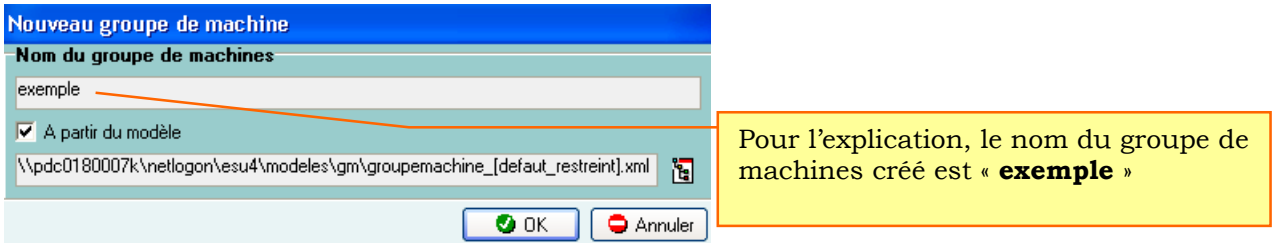
Nous vous proposons en téléchargement sur le site du lycée Jacques Cœur : l'utilitaire **blockinput** écrit par nos soins. Ses avantages sont la possibilité de cacher la fenêtre de connexion sous Windows 2000 ou XP, l'affichage éventuel d'un écran d'accueil pendant la connexion et la mise à disponibilité du code source permettant l'amélioration du produit (ce qui a été fait de la version 1 à la version 2 par collaboration avec un collègue d'une autre académie). Son inconvénient majeur dans la version actuelle reste sa taille : à peine 100 Ko dans sa version compilée la plus réduite, ce qui sur des réseaux modernes reste toutefois tout à fait raisonnable.

b) Les choix grisés

Le choix grisé dans les règles ESU est un non choix puisqu'il laisse la configuration du poste dans l'état précédent qui, à priori, n'est pas connu. Nous pensons donc que dans une bonne politique des gestion des machines d'un réseau, il ne devrait pas se trouver des règles grisées.

c) Astuce, problème et souhaits pour la création d'un nouveau groupe de machines

Lors de la création d'un nouveau groupe de machines, nous avons l'habitude d'utiliser le profil du groupe de machines **defaut_restreint**.



Un problème se pose, comme exposé au paragraphe n°4 : les variables **%ESU_GM%**, **%ESU_GU%**, … ont été remplacées par leurs valeurs, c'est pour cela que nous avons :

« **explorer \\PDC0180007K\ICONES$\exemple_Machine\Menu Démarrer\Programmes** » dans la commande de lancement du dossier « applications du poste ».

or nous voudrions obtenir :

« **explorer \\PDC0180007K\ICONES$\exemple\%ESU_GU%\Menu Démarrer\Programmes** » afin que cette commande dépende de l'utilisateur.

Le problème ici est que ESU remplace de toute façon les variables par leur valeur, or dans l'arborescence, lorsque sous ESU nous sommes dans le groupe de machines, le groupe d'utilisateur n'existe pas encore. ESU est donc obligé de le remplacer par le groupe « **_Machine** ».

Pour éviter ce problème, il suffirait que les variables ne soient jamais remplacées par leurs valeurs à l'intérieur de l'interface d'ESU, mais **uniquement lors de l'exécution du script de logon** (ce qui est d'ailleurs le cas en partie puisque notre solution consistant à laisser les variables %ESU_GM% et %ESU_GU% fonctionne.)

d) La logique des listes de règles.

Le fichier de référence des règles ESU est unique, il est nommé **ListeRegles.xml**.

Ce fichier contient tout aussi bien les règles standard d'ESU que les règles ajoutées par l'administrateur du réseau.

Afin de permettre la diffusion rapide de mise à jour des règles standard, il serait bien de doter ESU de trois fichiers de règles : **ListeReglesStandard.xml**, **ListeReglesDomain.xml** et **ListeRegles.xml**, ce dernier étant automatiquement construit par un utilitaire assurant la fusion des deux premiers, l'un diffusé officiellement par le site ESU, l'autre écrit localement par l'administrateur du réseau.

Une autre amélioration serait souhaitable, ceux qui ont cliqué des centaines de fois pour modifier une règle dans tous les groupes de machines me comprendront : on pourrait avoir une fonction permettant de modifier une règle dans tous les groupes de machines en un seul clic ! Il est possible de le faire actuellement uniquement en utilisant un éditeur de fichiers qui permet le « chercher remplacer » sur un ensemble de fichiers xml et à condition de faire une bonne analyse syntaxique préalable.

e) L'exécution de tâches par l'utilisateur #ESU4# - solution de substitution

Une amélioration fortement attendue d'ESU serait la possibilité de faire exécuter des tâches sous l'authentification de l'utilisateur **#ESU4#** qui possède des droits d'administrateur sur la machine locale quand elle est sous Windows 2000 ou XP.
Ces tâches pourraient être des scripts ou des programmes en code machine, exécutés au démarrage pour toutes les machines ou pour un groupe de machines seulement selon leur emplacement dans **\\Pdc0180007k\netlogon\esu\global** ou **\\Pdc0180007k\Icone$\%ESU_GM%_Machine\local** par exemple.

A défaut, on peut dans le script de logon faire appel à un script écrit dans un langage compilé comme **Autoit** (http://www.hiddensoft.com/autoit3/) qui a un **potentiel très intéressant** dans l'exploitation d'un réseau : il permet notamment l'élévation de pouvoir mais avec un risque potentiel équivalent à celui de l'élévation de pouvoir de ESU4 (voire supérieur car on n'a pas à priori le changement des mots de passe à chaque session mais par contre, on peut intervenir sur le code pour amoindrir le risque – je laisse ce point dans l'ombre de la sécurité).

Voici l'exemple d'un script permettant, s'il est appelé par le script de connexion logon.bat, de changer le mot de passe de l'administrateur standard de la station Windows XP ou 2000 à chaque connexion.

```
RunAsSet("compte", @LogonDomain, "passe")
Run("net user administrateur bon_mot_de_passe","",@SW_HIDE)
RunAsSet()
```

compte est un compte du domaine administrateur des stations et **passe** son mot de passe défini au niveau du contrôleur de domaine. Selon les conseils donnés, ce peut être un compte du groupe **LocalAdmins** tout simplement.

ATTENTION : cet exemple est donné en code AutoIt 3.2.10 et antérieur. Depuis mai 2008, les nouvelles versions 3.2.12 et postérieures ont substitué à **RunAsSet** la fonction **RunAs**.

Bien sûr la puissance du langage permet des variations importantes et intéressantes de ce script qui peut n'être qu'une partie d'un script plus ambitieux.
Voici par exemple un autre script qui installe silencieusement une police de caractères (math12) dans le cas où elle n'est pas présente sur le poste :

```
RunAsSet("compte", @LogonDomain, "passe")
        If not FileExists ( @WindowsDir&"\Fonts\math12.ttf" ) Then
          Run("xcopy \\serveur\chemin\fonts\*.ttf  %systemroot%\Fonts\ /y/c","",@SW_HIDE )
          Run("regedit /s \\serveur\chemin\fonts\math12.reg","",@SW_HIDE )
        EndIf
RunAsSet()
```

La partie indentée peut être incluse tout simplement dans le script précédent afin de s'exécuter sous l'élévation de pouvoir lors du script de connexion.

Le fichier math12.reg ayant pour contenu :

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts]
"math12 (TrueType)"="MATH12.TTF"
```

f) L'objet système Explorateur Windows

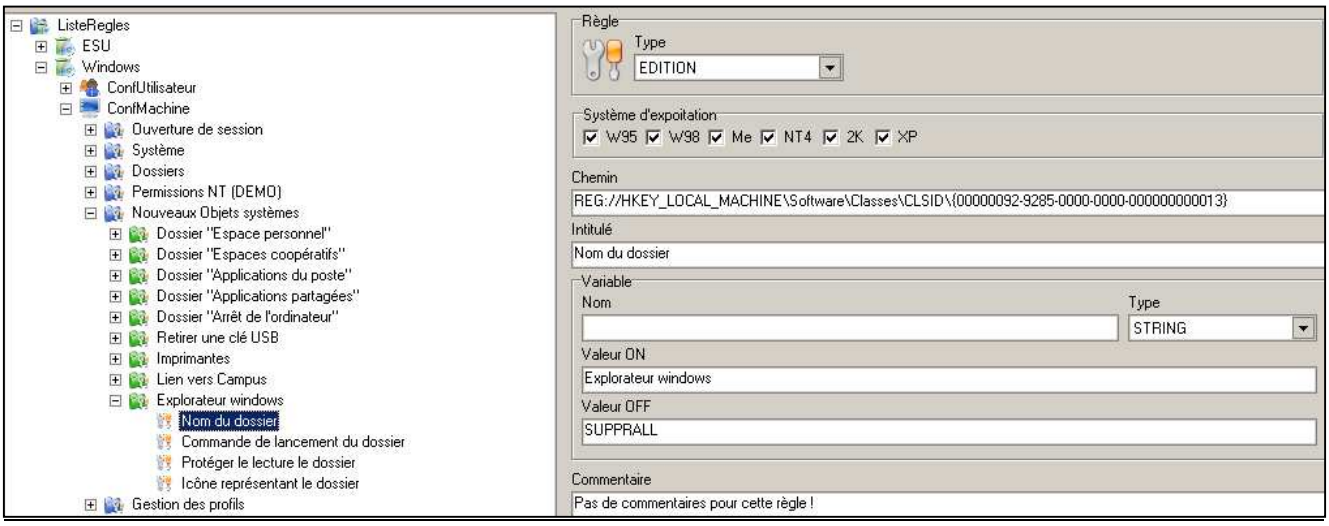
Autre exemple extrêmement simple de la création d'un script **AutoIt** : nous avons créé une commande **explo.exe** qui lance l'explorateur sur le dossier « Mes Documents » d'un utilisateur afin de contrer le bug rencontré sur Windows 98 qui, par l'icône Explorateur habituelle, lançait une exploration du disque C : alors que celui-ci était caché par ESU.

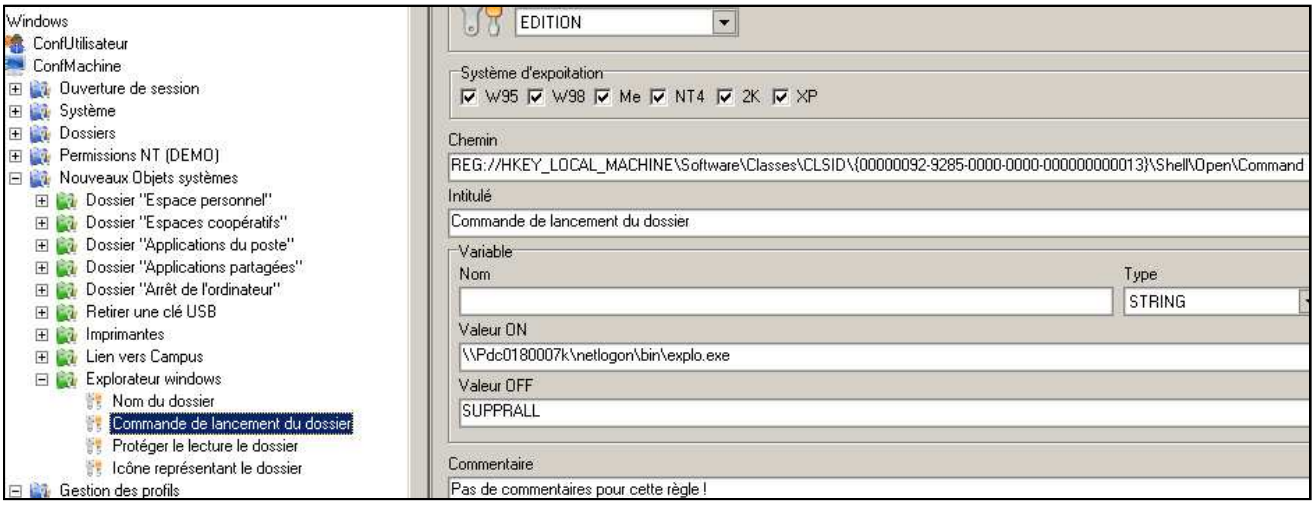
Un objet système a été associé à cette commande avec l'icône standard de l'explorateur Windows. Voici le script AutoIt qui utilise le SID de « Mes Documents » qui est une information fournie par AutoIt.

run("explorer.exe /e, ::{450D8FBA-AD25-11D0-98A8-0800361B1103}", "")

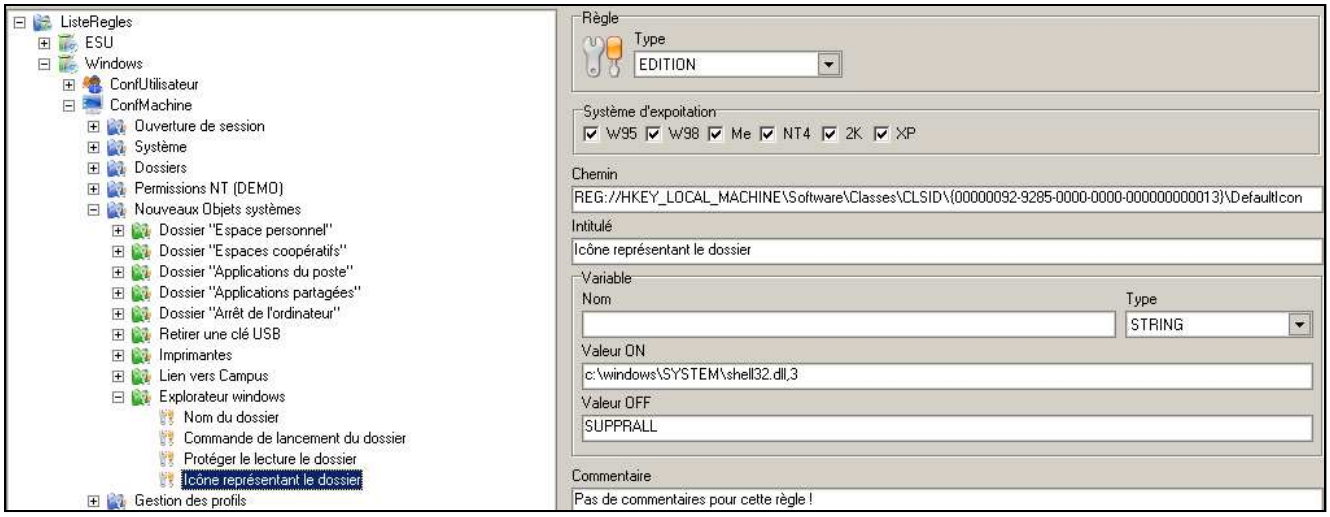
Sa compilation fournit la commande **explo.exe** que l'on associe à un objet système apparaissant automatiquement sur tous les bureaux Win98, Win2000 ou WinXP comme l'icône :

Construction de l'objet système associé à explo.exe :





Afin d'associer cet objet système à l'icône native de l'explorateur Windows, la règle a été complétée par une association à cette icône :



17 Reconfigurer rapidement une règle sur un site en production – exemple sur les règles erronées d'Internet Explorer.

Il arrive quelques fois que l'on désire changer la valeur d'une clé de la base de règles d'ESU4 sur tous les groupes de machines d'un site en production. C'est alors, souvent quelques centaines de clics répétitifs qu'il faut faire avec des risques d'erreur ou d'oubli.
Or il est possible d'automatiser de tels changements en utilisant un éditeur de texte permettant le rechercher/remplacer sur tous les fichiers d'un dossier : nous utilisons **PSPad** que vous trouverez en téléchargement sur le site du lycée Jacques Cœur, rubrique TICE et Net >> Logithèque ou directement à l'adresse http://www.pspad.com/fr/.

L'exemple qui va nous servir à expliquer la méthode est celui d'un bloc de règles dont les chemins dans la base de registre indiqués par la liste des règles d'ESU4 sont faux et les valeurs en partie inversées, ce qui fait de cet exemple un cas plus complexe que le simple changement de valeur.

Cette erreur touche les règles :

Désactiver le débugger de script
Afficher une notification à chaque erreur de script
Afficher des messages d'erreur HTTP simplifiés
Afficher une notification de téléchargement terminé
Désactiver la vérification des mises à jour de IE

Nous raisonnerons sur la règle « ***Afficher une notification à chaque erreur de script*** » qui est notre cible privilégiée mais le chemin erroné sera changé pour les 5 règles indiquées.

Extrait du fichier **ListeRegles.xml** :

Règle écrite dans ESU4 qui ne fonctionne pas sous IE6 ni IE7

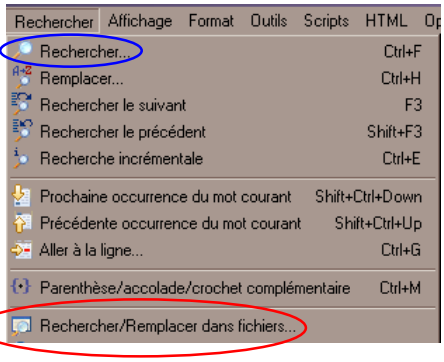
```
<Intitule>Afficher une notification à chaque erreur de script</Intitule>
<Chemin>REG://HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main</Chemin>
<Variable nom="Error Dlg Displayed On Every Error" type="STRING">
    <ValueOn>no</ValueOn>
    <ValueOff>yes</ValueOff>
</Variable>
```

Règle fonctionnant correctement pour IE6 et IE7

```
<Intitule>Afficher une notification à chaque erreur de script</Intitule>
<Chemin>REG://HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main</Chemin>
<Variable nom="Error Dlg Displayed On Every Error" type="STRING">
    <ValueOn>yes</ValueOn>
    <ValueOff>no</ValueOff>
</Variable>
```

1ère étape
Recopier le dossier ESU4 deux fois : une première pour faire une sauvegarde, une seconde pour faire un dossier de travail que nous conviendrons de nommer M:\ESU4.

2ème étape
Lancer PSPad et choisir **Rechercher/Remplacer dans fichiers.**



- Le texte recherché est le texte surligné bleu.
- Remplacer par est le texte surligné vert.
- Le répertoire sélectionné est M:\ESU4.
- Cocher la case inclure les sous-répertoires.

L'éditeur PSPad vous donne un compte rendu de tous les remplacements effectués, ce qui vous permet un contrôle. **Ont été ainsi effectués les remplacements sur ListeRegles.xml**

et sur tous les groupes de machines.

Il faut encore, dans **ListeRegles.xml**, échanger les valeurs yes et no pour la variable « **Error Dlg Displayed On Every Error** » ce qui peut être fait en ouvrant le fichier ListeRegles.xml avec PSPad et en recherchant cette variable.(Rechercher) ou directement avec l'éditeur de règles d'ESU4.

Il reste à mettre à « no » cette règle pour tous les groupes de machines et tous les groupes d'utilisateurs. Dans chacun des fichiers xml des utilisateurs, pour chaque groupe de machine, il y a les 5 lignes correspondant au 5 règles concernées par cette modification :

```
<Chemin nom="REG://HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main">
    <Variable nom="Disable Script Debugger" OS="252" type="STRING">yes</Variable>
    <Variable nom="Error Dlg Displayed On Every Error" OS="252" type="STRING">no</Variable>
    <Variable nom="Friendly http errors" OS="252" type="STRING">yes</Variable>
    <Variable nom="NotifyDownloadComplete" OS="252" type="STRING">yes</Variable>
    <Variable nom="NoUpdateCheck" OS="252" type="DWORD">1</Variable>
</Chemin>
```

Une recherche/remplacement effectuée sur tous le dossier ESU4 en incluant les sous-dossiers :

Texte recherché :

```
<Variable nom="Error Dlg Displayed On Every Error" OS="252" type="STRING">yes</Variable>
```

à remplacer par :

```
<Variable nom="Error Dlg Displayed On Every Error" OS="252" type="STRING">no</Variable>
```

permet de désactiver toutes les notifications d'erreurs de script sur toutes les machines et pour tous les groupes d'utilisateurs.

3ème étape

Recopier le dossier M:\ESU4 à la place du dossier opérationnel d'ESU4 sur le contrôleur de domaine et tester.

En cas de grosse bêtise, la sauvegarde faite du dossier ESU4 permet de revenir en l'état initial.

18 Errata et modifications par rapport à l'édition précédente

Correctifs et additifs par rapport à la version 2.1 :

page n°1 : nouveau sommaire.

page n°5 : image actualisée.

page 36 : La règle NoLMHash comportait une erreur dans la branche de la base de registre. Pour Windows XP, ce n'est pas la branche **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa** qui est concernée mais la branche **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa** et pour Windows 2000, une simple création de clé et non de valeur est nécessaire.

D'autre part le texte est repris avec une correction d'une information fausse donnée par Microsoft mais vérifiée comme inexacte.

page 39 : le paragraphe **« L'exécution de tâches par l'utilisateur #ESU4# »** est entièrement repris et porte le nom de « **L'exécution de tâches par l'utilisateur #ESU4# - solution de substitution »**
paragraphe **f) L'objet système Explorateur Windows**

page 43 : cette page.

Eric Pichon et Jacques Thomas,
responsables réseaux – lycée Jacques Cœur Bourges