

Distribution EOLE - Tâche #23522

Scénario # 24251 (Terminé (Sprint)): Développement de script de migration de profil W7 et W10

Script migration profil Windows

04/03/2018 09:45 AM - Emmanuel IHRY

Status:	Fermé	Start date:	06/06/2017
Priority:	Normal	Due date:	
Assigned To:	Emmanuel GARETTE	% Done:	100%
Target version:	Sprint 2018 29-34 Equipe PNE-SR	Estimated time:	0.00 hour
		Spent time:	8.00 hours
Description			
Décrire ce qui manque pour le changement de domaine			

Associated revisions

Revision 9f11dc59 - 08/21/2018 12:17 PM - Emmanuel GARETTE

ajout du script de changement des droits d'un profil utilisateur (ref #23522)

Revision 70c82f80 - 08/21/2018 12:30 PM - Emmanuel GARETTE

ne changer les droits que si l'ancien SID est trouvé (ref #23522)

Revision 9dce7559 - 08/22/2018 12:30 PM - Emmanuel GARETTE

ne plus utiliser de fichier CSV intermédiaire (ref #23522)

Revision 22960737 - 08/23/2018 01:59 PM - Emmanuel GARETTE

correction erreur de syntaxe (ref #23522)

Revision 18042c0c - 08/23/2018 06:04 PM - Emmanuel GARETTE

changement de droit dans la ruche usrclass.DAT (ref #23522)

Revision e8a5d274 - 08/23/2018 06:20 PM - Emmanuel GARETTE

ne pas migrer si le SID est identique (ref #23522)

Revision c29bec84 - 08/24/2018 08:23 AM - Emmanuel GARETTE

remove set-owner (ref #23522)

Revision a24fb101 - 08/27/2018 10:02 AM - Emmanuel GARETTE

Guid peut etre vide (ref #23522)

History

#1 - 04/23/2018 12:32 PM - Emmanuel IHRY

- Parent task changed from #23460 to #23689

#2 - 05/14/2018 10:58 AM - Emmanuel IHRY

- Status changed from Nouveau to En cours

#3 - 05/14/2018 12:58 PM - Emmanuel IHRY

- Parent task changed from #23689 to #23498

Principe

Le script de migration doit permettre de migrer un poste client d'un domaine A vers un domaine B en conservant son profil initial (profil utilisateur du domaine A), ceci de façon automatique (pas d'intervention manuelle) et sans copie de profil.
Les postes clients sont des postes **Seven** ou **Windows 10**.

Remarque importante

Dans le cas éventuel où une(des) étape(s) ci-dessous ne fonctionne(nt) pas avec Windows 10 (les étapes fonctionnent avec les postes Seven), celle(s)-ci devra(ont) être adaptée(s) pour les postes Windows 10.

Préalable

Les comptes, dont les profils sur les postes clients doivent être récupérés lors de la migration, doivent exister dans le nouveau domaine.
Un fichier contenant tous les comptes et leur SID dans le nouveau domaine devra être établi.

Les différentes étapes du script

Étape 1

Récupérer le SID du compte prenom.nom dans le nouveau domaine : **Nouveau_SID**

Étape 2

Sortir la machine du domaine A et mettre le poste dans un workgroup (pas besoin de rebooter le poste).

Étape 3

Mettre le poste dans le nouveau domaine Active Directory B (script initial migration ldap vers AD)

Étape 4

Rebooter le poste et se loguer avec le compte "Administrateur local" (compte -smb du fichier de conf de migration actuel)

Étape 5

Modifier les droits du profil utilisateur prenom.nom (de l'ancien domaine)

Sur le répertoire **c:\Users\prenom.nom**, qui est le répertoire où se trouve le profil du compte prenom.nom de l'ancien domaine :

- ajouter l'autorisation "Contrôle total" pour le compte prenom.nom du nouveau domaine
- en "remplaçant toutes les autorisations des objets enfants par des autorisation pouvant être héritées de cet objet" (cad de "façon récursive")

=> voir pièce jointe **Migration-droits-prenom.nom.jpg**

PS: peut se faire avec l'utilitaire Windows SetACL (commande ci-dessous à vérifier/adapter)

voir aide <https://helgeklein.com/setacl/examples/managing-file-system-permissions-with-setacl-exe/>

```
SETACL -on "c:\Users\prenom.nom" -ot file -actn ace -ace "n:Nouveau_SID;p:full"
```

Étape 6

Modifier les droits du contenu du fichier " **c:\Users\prenom.nom\NTUSER.DAT** "

Dans la base de registre :

- charger dans une ruche le fichier
- donner les autorisations "Contrôle total" et "Lecture" au compte prenom.nom du nouveau domaine
- décharger la ruche

=> voir pièce jointe **Migration-droits-NTUSER.DAT.jpg**

PS: peut se faire avec l'utilitaire Windows SetACL (commande ci-dessous à vérifier/adapter)

voir aide <https://helgeklein.com/setacl/examples/managing-file-system-permissions-with-setacl-exe/>

```
REG LOAD HKEY_USERS\NtuserDat_compte "c:\Users\prenom.nom\NTUSER.DAT"  
SETACL -on "HKEY_USERS\NtuserDat_compte" -ot reg -actn ace -ace "n:Nouveau_SID;p:full"  
REG UNLOAD HKEY_USERS\NtuserDat_compte
```

Étape 7

Nettoyage du profil (obligatoire)

Supprimer les fichiers :

- "c:\Users\prenom.nom\NTUSER.DAT.L**"
- "c:\Users\prenom.nom\NTUSER.DAT{*"
- "C:\Users\prenom.nom\AppData\Local\Microsoft\Windows\usrclass**"

Étape 8

Création de la nouvelle clé du profil dans la base de registre

copier la clé

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ **Ancien_SID** "

dans la clé

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ **Nouveau_SID** "

Étape 9

Sauvegarde de l'ancienne clé du profil dans la base de registre

renommer la clé

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ **Ancien_SID** "

en

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ **Ancien_SID.old** "

Étape 10

Modifier le SID de la clé " **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileGuid** "

La clé ProfilGuid existe quand on est ou a été dans un domaine Active Directory.

Il faut modifier la donnée **SidString** avec le nouveau SID :

- dans la nouvelle clé du profil utilisateur, s'il existe une clé **GUID**, relever la valeur de cette clé soit "Valeur_Guid_relevée"

- dans la clé

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileGuid\Valeur_Guid_relevée"

modifier la donnée **SidString** avec **Nouveau_SID** .

=> voir pièce jointe **Migration-Profile.jpg**

Étape 11

Ajouter l'utilisateur prenom.nom dans le groupe local " **Utilisateurs** "

```
net localgroup /add Utilisateurs domaineB\prenom.nom
```

Étape 12

Connexion dans le nouveau domaine avec le compte prenom.nom après redémarrage du poste

#5 - 05/30/2018 06:08 PM - Alain Guichard

- % Done changed from 0 to 90

#6 - 05/31/2018 11:43 AM - Alain Guichard

- File Migration-droits-NTUSER.DAT.jpg added
- File Migration-droits-prenom.nom.jpg added
- File Migration-Profile.jpg added

#7 - 05/31/2018 03:13 PM - Alain Guichard

- Status changed from En cours to Fermé
- % Done changed from 90 to 100
- Remaining (hours) set to 0.0

#8 - 06/19/2018 03:49 PM - Emmanuel IHRY

- Subject changed from Spécifier les évolutions du script intégration PC to Script intégration PC
- Status changed from Fermé to Nouveau
- Estimated time set to 0.00 h
- Parent task changed from #23498 to #24251

#9 - 06/19/2018 03:51 PM - Emmanuel IHRY

A mon sens il faut deux scripts :
- script intégration au domaine--> déjà existant
- script de migration de profil W7 et W10

Donc dans la description faite par Alain, on ne devrait pas avoir besoin des étapes 2 et 3 dans le script de migration de profil W7 et W10

#10 - 06/21/2018 10:33 AM - Emmanuel IHRY

- Project changed from PNE-SR to Distribution EOLE
- Description updated
- Assigned To changed from Alain Guichard to force bleue

#11 - 06/21/2018 10:45 AM - Emmanuel IHRY

- Subject changed from Script intégration PC to Script migration profil Windows

#12 - 06/25/2018 05:33 PM - Emmanuel IHRY

Suite aux échanges avec cadoles
- le script <https://helgeklein.com/setacl/examples/managing-file-system-permissions-with-setacl-exe/> est juste une piste non testée. Il y a peut être une meilleure solution. d'autre part il nécessite une licence --> ce n'est donc pas la bonne piste
- Ok sur le principe de définir comme pré-requis une version powershell, le mieux serait la dernière, la version 6

#13 - 07/17/2018 10:28 AM - Emmanuel IHRY

- Assigned To changed from force bleue to Emmanuel GARETTE

#14 - 07/23/2018 10:49 AM - Emmanuel GARETTE

Voir ce qu'on peut faire avec powershell :
<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-6>

#15 - 07/24/2018 09:53 AM - Emmanuel IHRY

- Status changed from Nouveau to En cours

#16 - 08/01/2018 04:50 PM - Michel BALLY

Précisions

Pour l'étape 1, un fichier sera fourni contenant le nom des comptes ainsi que le SID du nouveau domaine sous la forme prenom.nom;Nouveau_SID

Sur chaque poste client traité, on recherchera tous les profils existants :

- si le compte correspondant au profil est dans le fichier ci-dessus, on exécute les étapes 5 à 11
- sinon le profil est non traité

Les étapes de modification de profil doivent être loguées dans un journal.

#17 - 08/21/2018 12:21 PM - Emmanuel GARETTE

Le script reprend les différentes étapes décrites.

Les étapes 5 et 6 ont été inversé, sinon je n'arrivais pas à me logger sur 7.

Par contre, la session ne s'ouvre pas sur 10. A priori la méthode n'a pas été complètement validé sur cette version.

Pour tester, faire un fichier CSV dans le même répertoire que le script, ayant le nom "changeright.csv" et le contenu ressemblant à :

```
username, domain, oldsid  
test30, CADOLLES, S-1-5-21-3651895017-3268876750-1920785127-1140
```

Un fichier changeright.txt sera créé avec le rapport.

#18 - 08/22/2018 11:25 AM - Michel BALLY

Après échanges et discussion, il s'avère qu'il n'y a pas besoin de fichier contenant les infos comptes ancien et nouveau SID

Le PC est considéré migré dans le nouveau domaine (avec le script de migration existant)

- on liste les répertoires dans c:\users
- on récupère le nouveau SID via l'API windows
 - si le compte existe dans le domaine "d'arrivée", on migre le profil et on récupère les anciens SID dans la base de registre pour ces répertoires pour faire les étapes décrites ci-dessus
 - si le compte n'existe pas dans le domaine "d'arrivée", on ne migre pas le profil
- on dispose donc : répertoire utilisateur + nom utilisateur + old_sid + new_sid, le nom du domaine dans lequel le PC est intégré est connu également

#19 - 08/27/2018 02:55 PM - Emmanuel IHRY

- Status changed from *En cours* to *Fermé*

A qualifier par le MTES dans le cadre de ce scénario [#24679](#)

Identification des étapes manquantes pour W10 à faire par le MTES

Files

Migration-droits-NTUSER.DAT.jpg	69.7 KB	05/31/2018	Alain Guichard
Migration-droits-prenom.nom.jpg	326 KB	05/31/2018	Alain Guichard
Migration-Profile.jpg	130 KB	05/31/2018	Alain Guichard