

Distribution EOLE - Scénario #33471

AmonEcole 2.8.1 - Integration clients Windows 10 - profil itinérant ne fonctionne pas

02/12/2021 10:40 - Christophe DESOUTTER

Statut:	Terminé (Sprint)	Début:	02/12/2021
Priorité:	Normal	Echéance:	10/12/2021
Assigné à:	Joël Cuissinat	% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	sprint 2021 50-02 Equipe MENSUR	Temps passé:	0.00 heure
Description Bonjour, A la connexion d'un utilisateur sur le domaine addc Windows 10 ne parvient pas à créer le profil itinérant. Il semble que le module scribe ne partage pas /home/netlogon/profil sur lequel est mappé le profile itinérant. Un contournement est d'utiliser un profil local. Est-il possible de connaître la marche à suivre pour permettre l'utilisation des profils itinérants à partir de clients Windows? Merci d'avance, Christophe			

Révisions associées

Révision 747f1a71 - 08/12/2021 14:05 - Joël Cuissinat

Profil obligatoire => obsolète

Ref: #33471

Historique

#1 - 02/12/2021 17:03 - Joël Cuissinat

Sur AmonEcole, l'option "profil itinérant" mappe le profil dans le homedir de l'utilisateur : profilePath=\\scribe\<login>\profil (comme c'était déjà le cas sur les versions précédentes de Scribe et AmonEcole).

Il faut juste vérifier que l'utilisateur est bien propriétaire de son répertoire racine (/home/adhomes/<login>).

Si vous obtenez un comportement différent c'est peut-être que vous utilisez des procédures différentes de celles fournies par le pôle ?

#2 - 02/12/2021 17:03 - Joël Cuissinat

- Assigné à mis à Joël Cuissinat

- Tâche parente mis à #33394

#3 - 02/12/2021 22:19 - Christophe DESOUTTER

Ci-dessous des informations complémentaire.

A la création d'un utilisateur se fait par l'interface web ead, dont le process est

```
"/usr/bin/python3 /usr/bin/twistd3 --nodaemon --no_save --pidfile  
/var/run/ead/ead-web.pid --python=/usr/share/ead2/frontend/frontend.tac"
```

A priori la génération du profil est faite par un script python:

```
/usr/lib/python3/dist-packages/scribe/eoleuser.py
```

On retrouve la fonction qui indique le chemin vers le profil:

```
def gen_profil(profil, login):
```

```
"""
```

Génération du sambaProfilePath selon le profil demandé

```
"""
```

```
profil = int(profil)
```

```
if profil 2:      # profil obligatoire #1
```

```
return "\\{0}\\netlogon\\profil".format(SMB_SERVEUR)
```

```

if profil 3:      # profil obligatoire #2
return "\\{0}\\netlogon\\profil2".format(SMB_SERVEUR)
if profil == 4:   # profil itinérant
return "\\{0}\\{1}\\profil".format(SMB_SERVEUR, login)  # profil local à la station
return ""

```

Note: sur AmonEcole, SMB_SERVEUR est le conteneur "partage" (scribe).
Donc si on choisit profil "obligatoire #1" pour l'utilisateur, cela est résolu en \\scribe\netlogon\profil, cependant ce partage n'est pas configuré par le module scribe (de AmonEcole) et l'ouverture d'une session depuis un poste Windows va échouer.

Si j'active manuellement ce partage (netlogon) et que je lui donne les bons droits cela fonctionne mais je m'attendais à ce que cela soit opérationnelle sans modification de la conf samba.

Si on choisit profil itinérant, le chemin (\\scribe\<login>\profil.V6) aboutit à un share configuré mais une erreur empêche la création du profil par windows: "L'utilisateur actuel ou le groupe Administrateurs doivent être propriétaire du dossier" (Event 1526).
Cependant en analysant le dossier on s'aperçoit que le propriétaire est le compte "Unix User\root".
Il y a donc une étape qui manque à la création de l'utilisateur au niveau des scripts du module AmonEcole.

#4 - 02/12/2021 23:12 - Christophe DESOUTTER

Information additionnelle:

Le owner des fichiers créés depuis Windows sous \\scribe\<login>\profile.Vx est aussi "Unix User\root".

#5 - 02/12/2021 23:59 - Christophe DESOUTTER

Selon ce wiki:

https://wiki.samba.org/index.php/Updating_Samba#Failure_To_Access_Shares_on_Domain_Controllers_If_idmap_config_Parameters_Set_in_the_smb.conf_File

__Failure To Access Shares on Domain Controllers If idmap config Parameters Set in the smb.conf File

4.4.6 or later

By default, the winbindd service on a Samba Active Directory (AD) domain controller (DC) generates ID's locally on the DC and stores them in the idmap.ldb database. You can override the generated ID's by setting uidNumber and gidNumber attributes in your user accounts and groups in Active Directory. Originally, if the idmap config parameters were set in the smb.conf file they were ignored, but due to a bug in Samba 4.4.6 and later, the parameters are no longer ignored and clients fail to connect to shares on the DC. To fix the problem:

```

Remove all idmap config parameters in the smb.conf file on DCs.
Restart the samba service.
Restart the clients.

```

As a result, the clients will now correctly connect to shares on the DC.

—

Il faut donc supprimer les lignes :

idmap config *:backend = tdb

idmap config *:range = 2000-999999

idmap config LF:backend = rid

idmap config LF:range = 1000000-1999999

Du fichier smb.conf sur le conteneur partage.

Le ownership des fichiers est maintenant correcte.

Bonne soirée

#6 - 03/12/2021 09:38 - Gilles Grandg  rard

- T  che parente #33394 supprim  

#7 - 03/12/2021 09:59 - Jo  l Cuissinat

Il y a donc deux probl  mes distincts :

- **profils itin  rants** : nous ne reproduisons pas le probl  me sur nos maquettes avec les configurations samba fournies par d  faut sur AmonEcole

```
root@amonecole:~# ll /home/adhomes/p* -d
drwxrwx---+ 5 prenom.eleve107    root 4096 d  c.  3 00:35 /home/adhomes/prenom.eleve107/
drwxrwx---+ 5 prenom.eleve112    root 4096 d  c.  3 00:35 /home/adhomes/prenom.eleve112/
drwxrwx---+ 5 prenom.prof21      root 4096 d  c.  3 00:36 /home/adhomes/prenom.prof21/
drwxrwx---+ 5 prenom.prof26      root 4096 d  c.  3 00:36 /home/adhomes/prenom.prof26/
drwxrwx---+ 5 prof1              root 4096 d  c.  3 00:39 /home/adhomes/prof1/
drwxrwx---+ 5 prof10             root 4096 d  c.  3 00:39 /home/adhomes/prof10/
```

La page wiki que vous signalez indique *Remove all idmap config parameters in the smb.conf file on DCs*. hors, le samba pr  sent dans le conteneur partage est en mode membre.

- **profils obligatoires** : son utilisation est d  sormais d  conseill  e par Microsoft. Vous pouvez faire des essais (vous pouvez d  clarer les partages manquants dans /etc/samba/conf.d/) mais aucun de nos utilisateurs n'a r  ussi    obtenir un r  sultat acceptable.

#8 - 03/12/2021 10:08 - Gilles Grandg  rard

- Tracker chang   de T  che    Sc  nario

- Ech  ance mis    10/12/2021

#9 - 03/12/2021 16:11 - Christophe DESOUTTER

Oui effectivement:

- 1/ Les profils obligatoires sont toujours propos  s dans l'interface d'administration EAD mais ne sont pas fonctionnels.
- 2/ La cr  ation depuis un poste Windows du profil itin  rant sur le share (   la premi  re connexion l'utilisateur)   choue car les r  pertoires et fichiers cr  s n'ont pas le bon propri  taire.

Dans votre exemple (et avec un poste Windows 10    jour):

```
drwxrwx---+ 5 prenom.eleve107    root 4096 d  c.  3 00:35 /home/adhomes/prenom.eleve107/
```

Windows va cr  er un r  pertoire Profil.V6 sous /home/adhomes/prenom.eleve107/ qui n'aura pas le bon propri  taire (root au lieu de prenom.eleve107) ce qui conduira Windows    cr  er un profil temporaire, perdu    la d  connexion.

Sur vos maquettes avez vous essay   de connecter un poste Windows 10 r  cent et de vous connecter avec un utilisateur ayant un profil itin  rant?

Merci

#10 - 08/12/2021 13:51 - Jo  l Cuissinat

Bonjour,

Je viens de tester sur ma maquette avec un Windows 10 **21H1**.

J'ai pris l'enseignant suivant :

```
root@amonecole:~# lxc-attach -n addc -- samba-tool user show prof.6a | grep ofileP
profilePath: \\scribe\prof.6a\profil
```

Ayant ces droits sur son "home" :

```
root@amonecole:~# getfacl /home/adhomes/prof.6a
getfacl : suppression du premier « / » des noms de chemins absolus
# file: home/adhomes/prof.6a
# owner: prof.6a
# group: root
user::rwx
user:prof.6a:rwx
group:---
mask::rwx
other:---
default:user::rwx
default:user:prof.6a:rwx
default:group:---
default:mask::rwx
default:other:---
```

Et j'obtiens :

```
root@amonecole:~# getfacl /home/adhomes/prof.6a/profil.V6/
getfacl : suppression du premier « / » des noms de chemins absolus
# file: home/adhomes/prof.6a/profil.V6/
# owner: prof.6a
# group: domain\040users
user::rwx
group:---
group:2007:rwx
group:domain\040users:---
group:prof.6a:rwx
mask::rwx
other:---
default:user::rwx
default:user:prof.6a:rwx
default:group:---
default:group:2007:rwx
default:group:domain\040users:---
default:group:prof.6a:rwx
default:mask::rwx
default:other:---
```

#11 - 08/12/2021 20:22 - Christophe DESOUTTER

Bonjour,
Merci pour ces informations, de mon côté j'ai eu le problème après une installation "from scratch" de AmonEcole 2.8.1.
Est-il possible de partager la conf samba du conteneur partage de votre maquette (smb.conf et conf.d/*)?
Merci

#12 - 10/12/2021 10:11 - Joël Cuissinat

- Fichier smb.zip ajouté

La configuration utilisée dans nos tests d'intégration continue est ici :
<https://dev-eole.ac-dijon.fr/projects/eole-ci-tests/repository/revisions/master/entry/configuration/etb3.amonecole/default-2.8.1/etc/eole/config.eol>
Nous évitons de trop nous écarter des valeurs par défaut.

Je joins les fichiers demandés (ils sont générés par le module et nous ne les modifions pas dans nos tests).

#13 - 13/12/2021 17:06 - Joël Cuissinat

- Version cible changé de sprint 2021 46-49 Equipe MENSUR à sprint 2021 50-02 Equipe MENSUR

#14 - 12/01/2022 09:35 - Joël Cuissinat

- Statut changé de Nouveau à Terminé (Sprint)
- Points de scénarios mis à 1.0

Fichiers

smb.zip	3,29 ko	10/12/2021	Joël Cuissinat
---------	---------	------------	----------------