EOLE AD DC - Tâche #21000

Scénario # 21111 (Terminé (Sprint)): Intégrer la version samba 4.6.5 (ou plus)

Remplacer le vfs_object acl_xattr par acl_tdb ?

04/07/2017 09:18 - Benjamin Bohard

Statut:	Fermé	**Début:**	04/07/2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	sprint 2017 37-39 Equipe PNE-SR	**Temps estimé:**	2.00 heures
		Temps passé:	0.25 heure

Description

Dans la version 4.6.x, le support de acl_xattrs n'est pas compilé par défaut.

Actuellement, on charge le module vfs acl_xattr pour la gestion des acl étendues des systèmes de fichiers NTFS.
Il existe le module acl_tdb permettant de stocker ces acl dans une base tdb.

https://www.samba.org/samba/docs/man/manpages/vfs_acl_tdb.8.html

Historique

#1 - 04/07/2017 09:20 - Benjamin Bohard

- Description mis à jour

#2 - 04/08/2017 09:37 - Emmanuel IHRY

- Tâche parente mis à #21111

#3 - 05/09/2017 11:35 - Emmanuel IHRY

si acl_tdb : il faut prévoir la sauvegarde du fichier + impact procédure install preservation de données

#4 - 11/09/2017 13:09 - christophe guerinot

- Assigné à mis à christophe guerinot

#5 - 11/09/2017 13:09 - christophe guerinot

- Temps estimé mis à 2.00 h

- Restant à faire (heures) mis à 2.0

#6 - 11/09/2017 13:12 - christophe guerinot

- Assigné à christophe guerinot supprimé

#7 - 11/09/2017 13:17 - Emmanuel IHRY

réponse de l'expertise Samba :

Sur l'AD samba, historiquement les ACLs étaient gérées à travers le module NTVFS qui stockait les ACLs du SYSVOL dans une base TDB. Maintenant que Samba AD supporte à peu près correctement les ACLs directement sur le filesystem à travers une combinaison de droits UGO, ACLs et d'attribut étendues xattr, le mode par défaut est use-xattr.

Pour info, le mode par défaut basé sur les attributs étendus pose quand même quelques soucis, notamment par rapport à la gestion IDMAP_BOTH: c'est à dire que dans le monde Microsoft, un groupe peut être propriétaire d'un fichier, alors que dans le monde linux, la propriété est lié à l'utilisateur (le U de UGO). Pour palier à ce problème, winbindd sur AD peut utiliser un gidnumber pour définir le uid d'un fichier, d'ailleurs dans les fichiers idmap.tdb, Samba parle de xidnumber, et non de uidnumber et gidnumber (cf. le thread récent [1], qui met en garde contre les problèmes de mapping induit par le mapping gid du groupe "domain admins").

D'ailleurs, nous avons tendance en interne à désactiver de plus en plus souvent le mapping rfc2307 sur les contrôleurs de domaine, et rester sur du mapping TDB pour éviter les problèmes mentionnés ci-dessus (on remarque le problème lors de samba-tool ntacl sysvolcheck/sysvolreset)

Donc pas de soucis vis à vis du --use-xattr qui disparait, mais il faudrait aussi faire attention au paramètre idmap_ldb:use rfc2307 = yes dans les

smb.conf des contrôleurs de domaine pour éviter les problèmes d'ACL sur le SYSVOL.

--> En conclusion :

Ne pas utiliser acl_tdb, il suffit de supprimer l'option --use-xattrs=yes dans instance :

```
samba-tool domain provision --use-rfc2307 \
      --use-xattrs=yes \
      --dns-backend=SAMBA_INTERNAL \
      --realm="${AD_REALM^^}" \
      --domain="${AD_DOMAIN^^}" \
```

et par ailleurs rien à faire coté idmap_ldb:use rfc2307 = yes qui n'est pas utilisé sur le SETH

#8 - 11/09/2017 13:18 - Emmanuel IHRY

- Assigné à mis à Benjamin Bohard

#9 - 14/09/2017 15:35 - Benjamin Bohard

- Statut changé de Nouveau à Fermé

- % réalisé changé de 0 à 100

- Restant à faire (heures) changé de 2.0 à 0.0

En 2.6.2, l'option acl_xattr a déjà été supprimée de la commande de provisionnement.