EOLE AD DC - Tâche #30090

Scénario # 29927 (Terminé (Sprint)): Ajouter la variable "ad_utiliser_xattr" sur Seth membre

Ajouter la variable ad_utiliser_xattr

05/12/2020 09:27 AM - Benjamin Bohard

Status:	Fermé	**Start date:**	04/16/2020
Priority:	Normal	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	100%
Target version:	Prestation Cadoles MEN 19-21	**Estimated time:**	0.00 hour
		Spent time:	0.00 hour

Description

Related issues:

Related to EOLE AD DC - Tâche #28369: Vérifier l'option "vfs objects"	**Fermé**	**04/29/2019**

Associated revisions

Revision 0087e662 - 05/14/2020 11:05 AM - Benjamin Bohard

Allow to disable acl_xattr vfs_object

Ref #30090

Revision 31b917ae - 05/20/2020 10:17 AM - Benjamin Bohard

Allow shares without acl_xattr

Ref #30090

Revision daa0509e - 05/20/2020 10:27 AM - Benjamin Bohard

Allow not loading acl_xattr vfs object.

Ref #30090

Revision a84515eb - 06/09/2020 04:22 PM - Benjamin Bohard

Insert xattr variable in share section of config

Ref #30090

Revision d4138b17 - 06/09/2020 05:09 PM - Benjamin Bohard

Insert xattr variable in share section of config

Ref #30090

Revision 76b3e0bd - 06/09/2020 05:10 PM - Benjamin Bohard

Insert xattr variable in share section of config

Ref #30090

History

#1 - 05/12/2020 09:27 AM - Benjamin Bohard

- Status changed from Nouveau to En cours

#2 - 05/14/2020 09:28 AM - Benjamin Bohard

Les valeurs par défaut, forcées par samba pendant le chargement de la configuration implique que les options appliquées aux partages dans le cas d'un DC servant ces partages ne respectent pas les consignes de samba telles qu'on les met en place actuellement :

```
You should be aware that if wish to use a vfs object on a DC share e.g. recycle, you must not just set vfs obj
ects = recycle in the share. Doing this will turn off the default vfs objects dfs_samba4 and acl_xattr. You mu
st set vfs objects = dfs_samba4 acl_xattr recyle.
```

Cela semble opportun de rétablir le fonctionnement correct mais comme ce problème existe dès la 2.7.0, cela impliquerait un changement de comportement.

Ce problème n'affecte que le DC et pas le membre qui est la cible de ce scénario.

#3 - 05/14/2020 10:04 AM - Gilles Grandgérard

voir https://dev-eole.ac-dijon.fr/issues/28369

#4 - 05/14/2020 10:04 AM - Gilles Grandgérard

- Related to Tâche #28369: Vérifier l'option "vfs objects" added

#5 - 05/14/2020 10:49 AM - Gilles Grandgérard

<icephale> actuellement, quand on active les partages sur un DC, si on ajoute le vfs recycle, on est typiquement dans le cas décrit par samba
<icephale> on écrase les options dfs_samba4 et acl_xattr
<icephale> l'activation des partages sur un DC n'est pas l'architecture privilégiée mais comme elle est possible, je suppose qu'il faudrait corriger ce comportement
<icephale> le problème existe dès la 2.7.0,
<icephale> ggrandgerard_asu, ma question est donc : à partir de quelle version change-t-on ce comportement ? Si c'est à partir de la 2.7.0, il faut prévoir un qualification partielle pour les 2.7.0 et 2.7.1 je suppose parce que ça entraîne un changement dans la configuration
<ggrandgerard_asu> icephale, je suis d'accord. il manque un test "if %%ad_server_role == 'membre'" autour des ces options
<icephale> tu veux dire que recycle ne doit pas pouvoir être ajouter sur les partages hébergés sur le DC ?
<ggrandgerard_asu> icephale, les DC ne doivent pas porter de partages (sauf sysvol, netlogon). Les variables activant les partages sont une scorie de la 1er version en 2.6.0. cela n'aurait pas du être fait.
<ggrandgerard_asu> icephale, exactement
<ggrandgerard_asu> icephale, ce sont les préco de samba...
<icephale> du coup, qu'est-ce qu'on fait pour les versions déjà publiées ?
<icephale> et pour la 2.7.2 ?
<jojo2024> icephale, si personne (MTES, ...) n'a signalé de dysfonctionnement pouvant être lié à ces options, on ne touche pas aux 2.7 en prod
<jojo2024> icephale, en 2.7.2, il faut faire "propre" par contre
<icephale> ok
<ggrandgerard_asu> icephale, et 2.8.0 ....

#6 - 05/15/2020 10:58 AM - Benjamin Bohard

- Status changed from En cours to Résolu

#7 - 05/15/2020 11:02 AM - Benjamin Bohard

Les modifications proposées sont dans les trois branches :

- 2.7.0/30090-xattr
- 2.7.1/30090-xattr
- 2.7.2/30090-xattr

Pour la 2.7.0 et la 2.7.1, le comportement actuel est conservé.
Pour la 2.7.2, lorsque des partages sont configurés sur le DC, les options dfs_samba4 et acl_xattr sont ajoutées si on active la corbeille.

#8 - 05/19/2020 10:33 AM - Joël Cuissinat

- en **2.7.0**, dans le template existant, l'option est :
  - en dur dans la section [global] (vfs objects = acl_xattr)
  - si la corbeille est activée, cumulée avec l'option recycle pour les [homes] et/ou les partages additionnels (non (re)défini sinon)

- Avec la modification proposée :
  - section [global] soit :

    ```
    vfs objects = acl_xattr
    ```

    soit :

    ```
    vfs objects
    ```

  - [homes] et/ou les partages additionnels : toutes les combinaisons possibles avec : acl_xattr/recycle (4 possibilités)

- en **2.7.1**, dans le template existant, l'option est :
  - absente de la section [global]
  - en dur dans la section [sysvol] uniquement si ad_server_role 'membre'
  - si la corbeille est activée, cumulée avec l'option recycle pour les [homes] et/ou les partages additionnels (non (re)défini sinon)

- Avec la modification proposée :
  - absente de la section [global]
  - si option activée : en dur dans la section [sysvol] +toujours uniquement si ad_server_role 'membre'
  - [homes] et/ou les partages additionnels : toutes les combinaisons possibles avec : acl_xattr/recycle (4 possibilités)

- en **2.7.2**, dans le template existant, le fonctionnement est le même qu'en 2.7.1

- Avec la modification proposée :
  - absente de la section [global]
  - dans la section [sysvol] : si membre : vfs objects = acl_xattr si option activée
  - [homes] et/ou les partages additionnels : toutes les combinaisons possibles avec : acl_xattr/recycle mais en forçant **dfs_samba4** et **acl_xattr** sur un controleur de domaine

#9 - 05/20/2020 09:45 AM - Benjamin Bohard

Avec le dictionnaire proposé dans la branche 2.7.0/30090-xattr et le fichier de configuration patché avec les modifications proposées également dans la branche 2.7.0/30090-xattr :

- sur un aca.dc1-2.7.0 avec ad_utiliser_xattr = oui

```
# Global parameters
[global]
  realm = DOMSETH.AC-TEST.FR
  workgroup = DOMSETH
  netbios name = DC1

  # disable netbios legacy protocol, only port 445 !
  disable netbios = yes
  smb ports = 445

  vfs objects = acl_xattr
  map acl inherit = Yes
  store dos attributes = Yes
  winbind separator = /

  # protection contre 'rpcclient -U "" -c enumdomusers <ip>'
  restrict anonymous = 2

  server role = active directory domain controller
  dns forwarder = 192.168.0.1

  # active TLS (pour LDAPS et la maj des mot de passe !
  tls enabled = yes
  tls keyfile = /var/lib/samba/private/tls/key.pem
  tls certfile = /var/lib/samba/private/tls/cert.pem
  tls cafile = /var/lib/samba/private/tls/ca.pem

[netlogon]
  comment = Network Logon Service
  path = /home/sysvol/domseth.ac-test.fr/scripts
  read only = No
  guest ok = yes

[sysvol]
  comment = Sysvol Service
  path = /home/sysvol
  read only = No
  guest ok = yes
```

- sur un aca.dc1-2.7.0 avec ad_utiliser_xattr = non

```
# Global parameters
[global]
  realm = DOMSETH.AC-TEST.FR
  workgroup = DOMSETH
  netbios name = DC1

  # disable netbios legacy protocol, only port 445 !
  disable netbios = yes
  smb ports = 445

  map acl inherit = Yes
  store dos attributes = Yes
  winbind separator = /

  # protection contre 'rpcclient -U "" -c enumdomusers <ip>'
  restrict anonymous = 2

  server role = active directory domain controller
  dns forwarder = 192.168.0.1

  # active TLS (pour LDAPS et la maj des mot de passe !
  tls enabled = yes
  tls keyfile = /var/lib/samba/private/tls/key.pem
  tls certfile = /var/lib/samba/private/tls/cert.pem
```

```
  tls cafile = /var/lib/samba/private/tls/ca.pem

[netlogon]
  comment = Network Logon Service
  path = /home/sysvol/domseth.ac-test.fr/scripts
  read only = No
  guest ok = yes

[sysvol]
  comment = Sysvol Service
  path = /home/sysvol
  read only = No
  guest ok = yes
```

- sur un aca.file-2.7.0 avec ad_utiliser_xattr = oui

```
# Global parameters
[global]
  realm = DOMSETH.AC-TEST.FR
  workgroup = DOMSETH
  netbios name = FILE

  # disable netbios legacy protocol, only port 445 !
  disable netbios = yes
  smb ports = 445

  vfs objects = acl_xattr
  map acl inherit = Yes
  store dos attributes = Yes
  winbind separator = /

  # protection contre 'rpcclient -U "" -c enumdomusers <ip>'
  restrict anonymous = 2

  # serveur membre, pas de server role !
  security = ADS
  #dedicated keytab file = /etc/krb5.keytab
  #kerberos method = secrets and keytab

  idmap config *:backend = autorid
  idmap config *:range = 1000000-19999999

  winbind enum users  = yes
  winbind enum groups = yes
  winbind refresh tickets = Yes

[homes]
  vfs objects = acl_xattr
  path = "/home/adhomes/%u"
  root preexec = /usr/share/eole/sbin/create_adhome.sh "%u" "/home/adhomes"
  comment = Home Directories
  browseable = no
  read only = no
  invalid users = nobody guest

[profiles]
  comment = Profiles
  path = "/home/adprofiles"
  read only = No
  invalid users = nobody guest
```

- sur un aca.file-2.7.0 avec ad_utiliser_xattr = non

```
# Global parameters
[global]
  realm = DOMSETH.AC-TEST.FR
  workgroup = DOMSETH
  netbios name = FILE

  # disable netbios legacy protocol, only port 445 !
  disable netbios = yes
```

```
  smb ports = 445

  map acl inherit = Yes
  store dos attributes = Yes
  winbind separator = /

  # protection contre 'rpcclient -U "" -c enumdomusers <ip>'
  restrict anonymous = 2

  # serveur membre, pas de server role !
  security = ADS
  #dedicated keytab file = /etc/krb5.keytab
  #kerberos method = secrets and keytab

  idmap config *:backend = autorid
  idmap config *:range = 1000000-19999999

  winbind enum users  = yes
  winbind enum groups = yes
  winbind refresh tickets = Yes

[homes]
  path = "/home/adhomes/%u"
  root preexec = /usr/share/eole/sbin/create_adhome.sh "%u" "/home/adhomes"
  comment = Home Directories
  browseable = no
  read only = no
  invalid users = nobody guest

[profiles]
  comment = Profiles
  path = "/home/adprofiles"
  read only = No
  invalid users = nobody guest
```

#10 - 06/09/2020 04:02 PM - Gilles Grandgérard

- Status changed from Résolu to Fermé

- Remaining (hours) set to 0.0

ok

#11 - 06/09/2020 04:02 PM - Joël Cuissinat

- Assigned To set to Benjamin Bohard

- Estimated time set to 0.00 h

#12 - 06/10/2020 10:23 AM - Joël Cuissinat

- % Done changed from 0 to 100