eole-saslauthd - Scénario #30667

Annuaire non fonctionnel après la 1er instance en 2.8

09/18/2020 08:42 AM - Emmanuel GARETTE

Status:	Terminé (Sprint)	**Start date:**	12/03/2020
Priority:	Normal	**Due date:**	12/18/2020
Assigned To:	Daniel Dehennin	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	sprint 2020 49-51 Equipe MENSR	**Spent time:**	0.00 hour

Description

Problème

Si je démarre un aca.scribe daily avec :

```
root@scribe:~# /root/mount.eole-ci-tests
root@scribe:~# /mnt/eole-ci-tests/scripts/configure-vm.sh -M instance -C default
Monte CDROM de CONTEXT dans /mnt/cdrom (Ubuntu)
Inject /usr/share/eole dans PATH
Inject /mnt/eole-ci-tests/scripts/monitor3 dans PYTHONPATH
[..]
```

Après l'instance :

```
root@scribe:~# ldapsearch -D uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr -w Eole12345!
ldap_bind: Invalid credentials (49)
root@scribe:~# systemctl restart slapd.service
root@scribe:~# ldapsearch -D uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr -w Eole12345!
# extended LDIF
#
# LDAPv3
# base <o=gouv,c=fr> (default) with scope subtree
[..]
```

Pas de problème observer après un reconfigure ou un redémarrage.

Proposition

Il faut renommer le script **posttemplate/30-ldap-sasl** pour qu'il s'exécute avant **posttemplate/02-annuaire**.

Critère d'acceptation

1. Démarrer une machine virtuelle **aca.scribe-2.8.0-daily**
2. Exécuter la commande

   ```
   /root/mount.eole-ci-tests
   ```

3. Exécuter la commande

   ```
   /mnt/eole-ci-tests/scripts/configure-vm.sh -M instance -C default
   ```

4. Exécuter la commande

```
ldapsearch -o ldif-wrap=no -LLL -D uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr -w Eole12345! uid=admin dn
```

Vous devez obtenir le résultat suivant :

```
dn: uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
```

Subtasks:

Tâche # 31284: Exécuter le posttemplate 30-ldap-sasl avant 02-annuaire qui démarre le s...	**Fermé**

History

#1 - 12/03/2020 03:01 PM - Daniel Dehennin

- Assigned To set to Daniel Dehennin

- Je reproduis bien le problème avec un **aca.scribe-2.8.0-daily**
- **testsaslauthd** fonctionne

```
root@scribe:~# testsaslauthd -u admin@domscribe.ac-test.fr -p Eole12345!
0: OK "Success."
```

- J'ai défini **ldap_loglevel** à **-1** avant l'instance, du coup j'obtiens les messages suivants dans les logs lorsque j'essaye la commande LDAP **ldapsearch -D uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr -w Eole12345!**

```
déc. 03 14:05:32 scribe slapd[37234]: <<< dnPrettyNormal: <uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr>, <uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000a,ou=ac-test,ou=education,o=gouv,c=fr>
déc. 03 14:05:32 scribe slapd[37234]: conn=1174 op=0 BIND dn="uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" method=128
déc. 03 14:05:32 scribe slapd[37234]: do_bind: version=3 dn="uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" method=128
déc. 03 14:05:32 scribe slapd[37234]: ==> bdb_bind: dn: uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
déc. 03 14:05:32 scribe slapd[37234]: bdb_dn2entry("uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000a,ou=ac-test,ou=education,o=gouv,c=fr")
déc. 03 14:05:32 scribe slapd[37234]: => access_allowed: result not in cache (userPassword)
déc. 03 14:05:32 scribe slapd[37234]: => access_allowed: auth access to "uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" "userPassword" requested
déc. 03 14:05:32 scribe slapd[37234]: => acl_get: [1] attr userPassword
déc. 03 14:05:32 scribe slapd[37234]: => acl_mask: access to entry "uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr", attr "userPassword" requested
déc. 03 14:05:32 scribe slapd[37234]: => acl_mask: to value by "", (=0)
déc. 03 14:05:32 scribe slapd[37234]: <= check a_dn_pat: self
déc. 03 14:05:32 scribe slapd[37234]: <= check a_dn_pat: anonymous
déc. 03 14:05:32 scribe slapd[37234]: <= acl_mask: [2] applying auth(=xd) (stop)
déc. 03 14:05:32 scribe slapd[37234]: <= acl_mask: [2] mask: auth(=xd)
déc. 03 14:05:32 scribe slapd[37234]: => slap_access_allowed: auth access granted by auth(=xd)
déc. 03 14:05:32 scribe slapd[37234]: => access_allowed: auth access granted by auth(=xd)
déc. 03 14:05:32 scribe slapd[37234]: SASL Canonicalize [conn=1174]: authcid="admin@domscribe.ac-test.fr"
déc. 03 14:05:32 scribe slapd[37234]: SASL [conn=1174] Failure: cannot connect to saslauthd server: Permission denied
```

- La configuration LDAP tente de se connecter sur la socket :

```
root@scribe:~# cat /etc/ldap/sasl2/slapd.conf
pwcheck_method: saslauthd
saslauthd_path: /var/run/saslauthd/mux
```

- Le répertoire est restreint à l'utilisateur **root** et le groupe **sasl** peut traverser le répertoire

```
root@scribe:~# ls -ld /var/run/saslauthd/
drwx--x--- 2 root sasl 140 déc.   3 11:59 /var/run/saslauthd/
```

- La socket est accessible par tout le monde

```
root@scribe:~# ls -l /var/run/saslauthd/mux
srwxrwxrwx 1 root root 0 déc.   3 11:59 /var/run/saslauthd/mux
```

- L'utilisateur **openldap** est bien ajouté au groupe **sasl** pendant le **posttemplate** :

```
run-parts: executing /usr/share/eole/posttemplate/30-ldap-sasl instance
Adding openldap in group sasl
Ajout de l'utilisateur « openldap » au groupe « sasl »...
Ajout de l'utilisateur openldap au groupe sasl
Fait.
```

- Une fois **slapd** redémarré

```
déc. 03 14:22:40 scribe slapd[56798]: <<< dnPrettyNormal: <uid=admin,ou=local,ou=personnels,ou=utilisateur
s,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr>, <uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0
000000a,ou=ac-test,ou=education,o=gouv,c=fr>
déc. 03 14:22:40 scribe slapd[56798]: conn=1005 op=0 BIND dn="uid=admin,ou=local,ou=personnels,ou=utilisat
eurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" method=128
déc. 03 14:22:40 scribe slapd[56798]: do_bind: version=3 dn="uid=admin,ou=local,ou=personnels,ou=utilisate
urs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" method=128
déc. 03 14:22:40 scribe slapd[56798]: ==> bdb_bind: dn: uid=admin,ou=local,ou=personnels,ou=utilisateurs,o
u=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
déc. 03 14:22:40 scribe slapd[56798]: bdb_dn2entry("uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=00
00000a,ou=ac-test,ou=education,o=gouv,c=fr")
déc. 03 14:22:40 scribe slapd[56798]: => access_allowed: result not in cache (userPassword)
déc. 03 14:22:40 scribe slapd[56798]: => access_allowed: auth access to "uid=admin,ou=local,ou=personnels,
ou=utilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" "userPassword" requested
déc. 03 14:22:40 scribe slapd[56798]: => acl_get: [1] attr userPassword
déc. 03 14:22:40 scribe slapd[56798]: => acl_mask: access to entry "uid=admin,ou=local,ou=personnels,ou=ut
ilisateurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr", attr "userPassword" requested
déc. 03 14:22:40 scribe slapd[56798]: => acl_mask: to value by "", (=0)
déc. 03 14:22:40 scribe slapd[56798]: <= check a_dn_pat: self
déc. 03 14:22:40 scribe slapd[56798]: <= check a_dn_pat: anonymous
déc. 03 14:22:40 scribe slapd[56798]: <= acl_mask: [2] applying auth(=xd) (stop)
déc. 03 14:22:40 scribe slapd[56798]: <= acl_mask: [2] mask: auth(=xd)
déc. 03 14:22:40 scribe slapd[56798]: => slap_access_allowed: auth access granted by auth(=xd)
déc. 03 14:22:40 scribe slapd[56798]: => access_allowed: auth access granted by auth(=xd)
déc. 03 14:22:40 scribe slapd[56798]: SASL Canonicalize [conn=1005]: authcid="admin@domscribe.ac-test.fr"
déc. 03 14:22:40 scribe slapd[56798]: conn=1005 op=0 BIND dn="uid=admin,ou=local,ou=personnels,ou=utilisat
eurs,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" mech=SIMPLE ssf=0
déc. 03 14:22:40 scribe slapd[56798]: do_bind: v3 bind: "uid=admin,ou=local,ou=personnels,ou=utilisateurs,
ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr" to "uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=0
000000A,ou=ac-test,ou=education,o=gouv,c=fr"
```

- Aucun message d'erreur **apparmor** lié à **slapd** et **saslauthd**

```
root@scribe:~# dmesg | grep slapd
[    2.910231] audit: type=1400 audit(1606992512.588:6): apparmor="STATUS" operation="profile_load" profil
e="unconfined" name="/usr/sbin/slapd" pid=497 comm="apparmor_parser"
[  589.590422] audit: type=1400 audit(1606993100.095:70): apparmor="DENIED" operation="connect" profile="/
usr/sbin/slapd" name="/run/samba/winbindd/pipe" pid=37233 comm="slapd" requested_mask="wr" denied_mask="wr
" fsuid=0 ouid=0
[ 9215.652874] audit: type=1400 audit(1607001726.453:81): apparmor="DENIED" operation="connect" profile="/
usr/sbin/slapd" name="/run/samba/winbindd/pipe" pid=56797 comm="slapd" requested_mask="wr" denied_mask="wr
" fsuid=0 ouid=0
```

C'est comme-ci le service **slapd**, démarré avec l'utilisateur **openldap**, n'est pas associé au groupe **sasl**. Chose qui est corrigé par un redémarrage

du service.

En fait, cela vient du fait que le service **slapd** est démarré par /**usr**/**share**/**eole**/**posttemplate**/**02-annuaire**, ainsi :

- Le service n'est pas associé au groupe **sasl**
- Le service n'est pas redémarré au démarrage des service car il est déjà fonctionnel

#2 - 12/03/2020 03:14 PM - Daniel Dehennin

- Tracker changed from Demande to Scénario

- Description updated

- Due date set to 12/18/2020

- Target version set to sprint 2020 49-51 Equipe MENSR

- Release set to EOLE 2.8.0

#3 - 12/03/2020 03:14 PM - Daniel Dehennin

- Project changed from Distribution EOLE to eole-saslauthd

- Story points set to 1.0

#4 - 12/10/2020 04:46 PM - Joël Cuissinat

- Status changed from Nouveau to Terminé (Sprint)