eole-saslauthd - Scénario #28777

Étudier la délégation d'authentification OpenLDAP (Pass-Trough) avec SASL

07/22/2019 02:13 PM - Joël Cuissinat

Status:	Terminé (Sprint)	**Start date:**	10/10/2019
Priority:	Normal	**Due date:**	10/11/2019
Assigned To:	Daniel Dehennin	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	sprint 2019 39-41 Equipe MENSR	**Spent time:**	0.00 hour

Description

Cf. https://ltb-project.org/documentation/general/sasl_delegation

- utiliser une version d'OpenLDAP compilée avec l'option --enable-passwd (https://ltb-project.org/documentation/openldap-deb ?)
- configurer le service **saslauthd** (paquets sasl2-bin)
- modifier l'attribut userPassword d'un ou plusieurs utilisateurs

Subtasks:

Tâche # 29092: Reproduire les étapes décrites dans le scénario	**Fermé**

Related issues:

Related to eole-saslauthd - Scénario #29695: Scribe 2.8 devrait proposer nati...	**Terminé (Sprint)**	**04/14/2020**	**04/30/2020**

History

#1 - 08/20/2019 03:06 PM - Gilles Grandgérard

- Due date set to 09/20/2019

- Target version set to sprint 2019 36-38 Equipe MENSR

- Start date set to 08/20/2019

#2 - 09/03/2019 10:17 AM - Joël Cuissinat

- Story points set to 6.0

#3 - 09/03/2019 10:45 AM - Joël Cuissinat

- Target version changed from sprint 2019 36-38 Equipe MENSR to sprint 2019 39-41 Equipe MENSR

#4 - 09/23/2019 01:36 PM - Daniel Dehennin

Le paquet **openldap** utilisé sur Bionic utilise bien les options **--enable-spasswd** et **--with-cyrus-sasl**.

#5 - 10/10/2019 10:40 AM - Daniel Dehennin

Test réalisé

- **etb1.amon-2.7.1.1-instance-default**
- **etb1.scribe-2.7.1.1-instance-AvecImport**
- **etb1.pcprofs-10** intégré au domaine

Installation et paramétrage de saslauthd

- Installation du paquet

```
apt install sasl2-bin
```

- Configuration de la connexion LDAP sur ADDC

```
cat > /etc/saslauthd.conf <<EOF
ldap_servers: ldaps://addc.dompedago.etb1.lan
ldap_search_base: DC=dompedago,DC=etb1,DC=lan
```

```
ldap_auth_method: bind
ldap_bind_dn: CN=Administrator,CN=Users,DC=dompedago,DC=etb1,DC=lan
ldap_password: Eole12345!
ldap_filter: (userPrincipalName=%u)
ldap_deref: never
ldap_tls_cacert_file: /var/lib/lxc/addc/rootfs/var/lib/samba/private/tls/ca.pem
EOF
```

- Configuration du service

```
sed -i -e 's,^START=.*,START=yes,' \
       -e 's,^MECHANISMS=.*,MECHANISMS="ldap",' \
       -e 's,^OPTIONS=",OPTIONS="-r ,' /etc/default/saslauthd
```

- Démarrer le service

```
systemctl start saslauthd.service
```

- Test SASL avec le compte admin

```
testsaslauthd -u admin@dompedago.etb1.lan -p eole
0: OK "Success."
```

Adaptation de la configuration OpenLDAP

- Configuration SASL

```
cat > /etc/ldap/sasl2/slapd.conf <<EOF
pwcheck_method: saslauthd
saslauthd_path: /var/run/saslauthd/mux
EOF
```

- L'utilisateur **openldap** doit faire partie du groupe **sasl**

```
adduser openldap sasl
```

- Configurer apparmor pour l'accès **slapd** au socket **saslauthd**

```
cat > /etc/apparmor.d/local/usr.sbin.slapd <<EOF
/{,var/}run/saslauthd/mux rw,
EOF
```

- Redémarrer le service **apparmor**

```
systemctl restart apparmor.service
```

- Redémarrer le service **slapd**

```
systemctl restart slapd.service
```

Vérifier le fonctionnement

- Créer un LDIF pour modifier le mot de passe de l'utilisateur **admin**

```
cat > admin.ldif <<EOF
```

```
dn: uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=00000001,ou=ac-test,ou=education,o=gouv,c=fr
changetype: modify
replace: userPassword
userPassword: {SASL}admin@dompedago.etb1.lan
-
EOF
```

- Appliquer la modification

```
ldapmodify -Dcn=admin,o=gouv,c=fr -w $(awk -F'=' '/^masterPw/ {print $2}' /etc/smbldap-tools/smbldap_bind.conf | tr -d '"') -f admin.ldif
```

Vérifier que nous pouvons faire une recherche authentifié sur l'annuaire :

```
ldapsearch -LLL -x -D uid=admin,ou=local,ou=personnels,ou=utilisateurs,ou=00000001,ou=ac-test,ou=education,o=gouv,c=fr -w eole '(uid=admin)' userPassword | awk '/^userPassword/ {print $2}' | base64 -d; echo
```

ce qui doit renvoyer :

```
{SASL}admin@dompedago.etb1.lan
```

Nous pouvons mainenant modifier le mot de passe de l'utilisateur **admin** depuis un poste windows intégré au domaine et refaire la requête précédente en modifier le mot de passe (**-w eole**).

#6 - 10/10/2019 10:51 AM - Joël Cuissinat

- Status changed from Nouveau to En cours

- Assigned To set to Daniel Dehennin

#7 - 10/14/2019 10:46 AM - Joël Cuissinat

- Status changed from En cours to Terminé (Sprint)

#8 - 03/04/2020 03:38 PM - Joël Cuissinat

- Subject changed from Étudier la délégation d'autentification OpenLDAP (Pass-Trough) avec SASL to Étudier la délégation d'authentification OpenLDAP (Pass-Trough) avec SASL

#9 - 03/04/2020 03:44 PM - Joël Cuissinat

- Related to Scénario #29695: Scribe 2.8 devrait proposer nativement la délégation d'authentification OpenLDAP avec SASL added

#10 - 04/04/2020 02:20 PM - Joël Cuissinat

- Project changed from Distribution EOLE to eole-saslauthd