Distribution EOLE - Tâche #15194

Scénario # 15164 (Terminé (Sprint)): Corriger les problèmes de réplication LDAP Scribe & Horus

La réplication en ldaps n'est plus fonctionnelle (SC-T13-002)

26/02/2016 10:59 - Joël Cuissinat

Statut:	Fermé	**Début:**	26/02/2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Joël Cuissinat	**% réalisé:**	100%
Version cible:	sprint 2016 07-09 - Equipe MENESR	**Temps estimé:**	3.00 heures
		Temps passé:	5.00 heures

Description

Après mise en place de la configuration de réplication ldaps :

```
root@seshat:~# slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 16384
56d0217c @(#) $OpenLDAP: slapd  (Ubuntu) (Sep 15 2015 18:19:13) $
    buildd@lgw01-53:/build/openldap-2QUgtL/openldap-2.4.31/debian/build/servers/slapd
56d0217c slapd starting
TLS: can't connect: The signature algorithm is not supported..
56d0217c slap_client_connect: URI=ldaps://192.168.0.31:636 DN="cn=reader,o=gouv,c=fr" ldap_sasl_bi
nd_s failed (-1)
56d0217e do_syncrepl: rid=000 rc -1 retrying (9 retries left)




root@seshat:~# openssl s_client -showcerts -connect 192.168.0.31:636 < /dev/null |  openssl x509 -
noout -text > cert.txt
depth=1 C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = C
A-scribe
verify error:num=19:self signed certificate in certificate chain
verify return:0
DONE
root@seshat:~# openssl s_client -showcerts -connect 192.168.0.31:636 < /dev/null |  openssl x509 -
noout -text | grep -i signature
depth=1 C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = C
A-scribe
verify error:num=19:self signed certificate in certificate chain
verify return:0
DONE
    Signature Algorithm: sha256WithRSAEncryption
                Digital Signature, Non Repudiation, Key Encipherment
    Signature Algorithm: sha256WithRSAEncryption
```

Révisions associées

Révision 286f40b6 - 01/03/2016 12:09 - Joël Cuissinat

Modification de l'option tls_cipher_suite pour ldaps

- tmpl/slapd.conf : ajout de "+SIGN-ALL" à l'option tls_cipher_suite

Ref: #15194 @3h

Historique

#1 - 26/02/2016 11:02 - Joël Cuissinat

- Description mis à jour

- Restant à faire (heures) changé de 3.0 à 2.0

#2 - 26/02/2016 13:47 - Joël Cuissinat

- Statut changé de Nouveau à En cours

#3 - 26/02/2016 13:48 - Joël Cuissinat

- Assigné à mis à Joël Cuissinat

#4 - 26/02/2016 13:51 - Joël Cuissinat

J'ai du mal à tout comprendre de https://bugs.launchpad.net/ubuntu/+source/gnutls26/+bug/1534230, cependant, si on utilise une version antérieure de la librairie **gnutls** sur le serveur Seshat, la réplication ldaps fonctionne !

```
apt-get install libgnutls26=2.12.23-12ubuntu2 libgnutls-openssl27=2.12.23-12ubuntu2
```

#5 - 26/02/2016 14:40 - Joël Cuissinat

Ajouter l'option suivante dans la configuration de réplication côté client (/etc/ldap/replication.conf sur Seshat) rend la réplication de nouveau fonctionnelle !

```
        tls_cipher_suite=NORMAL
```

#6 - 26/02/2016 14:41 - Joël Cuissinat

- % réalisé changé de 0 à 50

- Restant à faire (heures) changé de 2.0 à 1.0

#7 - 01/03/2016 12:13 - Joël Cuissinat

=> **eole-annuaire 2.5.2-6**

#8 - 01/03/2016 12:14 - Joël Cuissinat

- Statut changé de En cours à Résolu

- % réalisé changé de 50 à 100

- Restant à faire (heures) changé de 1.0 à 0.0

#9 - 01/03/2016 17:25 - Joël Cuissinat

- Statut changé de Résolu à Fermé