

Distribution EOLE - T che #15194

Sc nario # 15164 (Termin  (Sprint)): Corriger les probl mes de r plication LDAP Scribe & Horus

La r plication en ldaps n'est plus fonctionnelle (SC-T13-002)

26/02/2016 10:59 - Jo l Cuissinat

Statut:	Ferm�	D�but:	26/02/2016
Priorit�:	Normal	Ech�ance:	
Assign� �:	Jo�l Cuissinat	% r�alis�:	100%
Version cible:	sprint 2016 07-09 - Equipe MENESR	Temps estim�:	3.00 heures
		Temps pass�:	5.00 heures
<p>Description</p> <p>Apr�s mise en place de la configuration de r�plication ldaps :</p> <pre>root@seshat:~# slapd -f /etc/ldap/slapd.conf -u slapd -g slapd -d 16384 56d0217c @(#) \$OpenLDAP: slapd (Ubuntu) (Sep 15 2015 18:19:13) \$ build@lgw01-53:/build/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_bind_s failed (-1) 56d0217e do_sync_repl: rid=000 rc -1 retrying (9 retries left)</pre> <pre>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</pre>			

R visions associ es

R vision 286f40b6 - 01/03/2016 12:09 - Jo l Cuissinat

Modification de l'option tls_cipher_suite pour ldaps

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

Ref: #15194 @3h

Historique

#1 - 26/02/2016 11:02 - Jo l Cuissinat

- Description mis   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=2.12.23-1ubuntu2 libgnutls-openssl27=2.12.23-1ubuntu2
```

#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