Distribution EOLE - Scénario #31635

L'autorité de certificat locale n'est pas connue du système ca-certificates sur Seth (et peut-être d'autres)

02/04/2021 10:03 AM - Daniel Dehennin

Status:	Terminé (Sprint)	**Start date:**	02/22/2021
Priority:	Normal	**Due date:**	03/12/2021
Assigned To:	Benjamin Bohard	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Prestation Cadoles MEN 08-10	**Spent time:**	0.00 hour

Description

Problèmes

Seth

Sur un **aca.dc1-2.8.0-instance-avecImport**, exécuter la commande suivante :

```
ldapsearch -H ldaps://localhost -b dc=domseth,dc=ac-test,dc=fr -DCN=admin,CN=Users,DC=domseth,DC=ac-test,DC=fr -W
```

Après avoir saisi le mot de passe, cela renvoie les messages suivants :

```
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
root@dc1:~# ldapsearch -d1 -H ldaps://localhost -b dc=domseth,dc=ac-test,dc=fr -DCN=admin,CN=Users,DC=domseth,DC=ac-test,DC=fr -W
ldap_url_parse_ext(ldaps://localhost)
ldap_create
ldap_url_parse_ext(ldaps://localhost:636/??base)
Enter LDAP Password:
ldap_sasl_bind
ldap_send_initial_request
ldap_new_connection 1 1 0
ldap_int_open_connection
ldap_connect_to_host: TCP localhost:636
ldap_new_socket: 3
ldap_prepare_socket: 3
ldap_connect_to_host: Trying 127.0.0.1:636
ldap_pvt_connect: fd: 3 tm: -1 async: 0
attempting to connect:
connect success
TLS: peer cert untrusted or revoked (0x42)
TLS: can't connect: (unknown error code).
ldap_err2string
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
```

La configuration LDAP est vierge :

```
root@dc1:~# cat /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.
```

```
#BASE    dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
```

Scribe

Nous avons un problème équivalent sur Scribe :

```
root@scribe:~# ldapsearch -d1 -x -H ldaps://addc.domscribe.ac-test.fr
ldap_url_parse_ext(ldaps://addc.domscribe.ac-test.fr)
ldap_create
ldap_url_parse_ext(ldaps://addc.domscribe.ac-test.fr:636/??base)
ldap_sasl_bind
ldap_send_initial_request
ldap_new_connection 1 1 0
ldap_int_open_connection
ldap_connect_to_host: TCP addc.domscribe.ac-test.fr:636
ldap_new_socket: 3
ldap_prepare_socket: 3
ldap_connect_to_host: Trying 192.0.2.2:636
ldap_pvt_connect: fd: 3 tm: -1 async: 0
attempting to connect:
connect success
TLS: peer cert untrusted or revoked (0x42)
TLS: can't connect: (unknown error code).
ldap_err2string
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
```

Avec une configuration LDAP non adaptée :

```
root@scribe:~# cat /etc/ldap/ldap.conf

# cas Amon sans AmonEcole

host 127.0.0.1
base o=gouv,c=fr
port 389
timelimit 10
bind_time_limit 10
bind_policy soft
ldap_version 3
scope sub
pam_login_attribute uid
pam_password md5
nss_map_attribute gecos displayName
nss_base_passwd o=gouv,c=fr?sub
nss_base_group o=gouv,c=fr?sub
#fixe #1809
nss_initgroups_ignoreusers root
ssl off
```

Proposition

- À faire pour **EOLE >= 2.8.0**
- Lorsque les certificats sont en mode **autosigné**, il faut intégrer l'autorité de certification locale à **ca-certificates**
- La configuration LDAP devrait toujours inclure **TLS_CACERT /etc/ssl/certs/ca-certificates.crt**

Critères d'acceptations

Scribe

Sur **aca.scribe-2.8.0-instance-AvecImport**:

- La commande **ldapsearch -LLL -o ldif-wrap=no -x cn=professeurs dn** doit affichier le résultat suivant, sans poser de question :

```
dn: cn=professeurs,ou=local,ou=groupes,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
```

- La commande **ldapsearch -LLL -o ldif-wrap=no -b dc=domscribe,dc=ac-test,dc=fr -x -H ldaps://addc.domscribe.ac-test.fr -Dcn=admin,cn=Users,dc=domscribe,dc=ac-test,dc=fr -W cn=professeurs dn** doit affichier le résultat suivant, en ne demandant que le mot de passe de l'utilisateur **admin** :

```
dn: CN=professeurs,CN=Users,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/CN=Configuration,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/DC=DomainDnsZones,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/DC=ForestDnsZones,DC=domscribe,DC=ac-test,DC=fr
```

Seth

Sur **aca.dc1-2.8.0-instanceAvecImport**

- La commande **ldapsearch -LLL -o ldif-wrap=no -b dc=domseth,dc=ac-test,dc=fr -x -H ldaps://dc1.domseth.ac-test.fr -Dcn=admin,cn=Users,dc=domseth,dc=ac-test,dc=fr -W cn=professeurs dn** doit affichier le résultat suivant, en ne demandant que le mot de passe de l'utilisateur **admin** :

```
dn: CN=professeurs,CN=Users,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/CN=Configuration,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/DC=DomainDnsZones,DC=domscribe,DC=ac-test,DC=fr

# refldaps://domscribe.ac-test.fr/DC=ForestDnsZones,DC=domscribe,DC=ac-test,DC=fr
```

Subtasks:

Tâche # 31781: Ajouter une étape d'intégration du certificat autosigné à la procédure d...	**Fermé**
Tâche # 31850: Étude du problème sur Scribe	**Fermé**

Related issues:

Related to Distribution EOLE - Tâche #31739: Valider le scénario L'autorité d...	**Fermé**	**02/24/2021**

History

#1 - 02/17/2021 10:54 AM - Daniel Dehennin

- Description updated

#2 - 02/17/2021 10:55 AM - Daniel Dehennin

Cela est très problématique pour la mise en place de LemonLDAP::NG qui se connecte sur le service LDAPS du Samba.

#3 - 02/17/2021 11:20 AM - Daniel Dehennin

- Description updated

#4 - 02/17/2021 11:21 AM - Joël Cuissinat

- Subject changed from L'autorité de certificat locale n'est pas connu du système ca-certificates sur Seth (et peut-être d'autres) to L'autorité de certificat locale n'est pas connue du système ca-certificates sur Seth (et peut-être d'autres)

#5 - 02/17/2021 11:42 AM - Joël Cuissinat

- Start date deleted (02/04/2021)

- Parent task deleted (#31587)

#6 - 02/17/2021 11:43 AM - Joël Cuissinat

- Tracker changed from Tâche to Scénario

- Description updated

- Due date set to 03/12/2021

- Target version changed from sprint 2021 05-07 Equipe MENSR to Prestation Cadoles MEN 08-10

- Start date set to 02/22/2021

- Release set to EOLE 2.8.0.1

- Story points set to 3.0

#7 - 02/22/2021 02:40 PM - Benjamin Bohard

- Assigned To set to Benjamin Bohard

#8 - 02/24/2021 10:06 AM - Joël Cuissinat

- Related to Tâche #31739: Valider le scénario L'autorité de certificat locale n'est pas connue du système ca-certificates sur Seth (et peut-être d'autres) added

#9 - 03/08/2021 03:46 PM - Benjamin Bohard

- Status changed from Nouveau to Résolu

#10 - 03/09/2021 09:26 AM - Daniel Dehennin

- Status changed from Résolu to Terminé (Sprint)

Je confirme le bon fonctionnement des critères d'acceptation.

J'ai intégré la branche **2.8.0/master** de creole à la branche **master** et refait un paquet **eole-2.8-unstable**.