Distribution EOLE - Tâche #37502

Scénario # 37405 (Terminé (Sprint)): Porter Zéphir en 2.11

Vérifier la configuration slapd

11/06/2026 17:04 - Joël Cuissinat

Statut:	Fermé	**Début:**	11/06/2026
Priorité:	Normal	**Echéance:**	
Assigné à:	Laurent Gourvenec	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 30/04/2026 (30)	**Temps estimé:**	0.00 heure

Description

Le service slapd ne voulait pas se lancer, j'ai commenté la variable **TLSCipherSuite** mais il faut peut-être la restaurer en actualisant sa valeur ?

```
6a2acc63.18999185 0x712714271e40 TLS: could not set cipher list SECURE256:+SIGN-ALL:-VERS-SSL3.0:!
AES-128-CBC:!3DES-CBC:!DES-CBC:!ARCFOUR-128:!ARCFOUR-40:!RC2-40:!CAMELLIA-128-CBC:!NULL.
6a2acc63.1899f801 0x712714271e40 TLS: error:0A0000B9:SSL routines::no cipher match ../ssl/ssl_ciph
.c:1299
   [ ... ]
6a2acc63.189aaad6 0x712714271e40 main: TLS init def ctx failed: -1 error:0A0000B9:SSL routines::no
 cipher match
6a2acc63.189f5501 0x712714271e40 slapd stopped.
```

Demandes liées:

Lié à Distribution EOLE - Tâche #15194: La réplication en ldaps n'est plus fo...	**Fermé**	**26/02/2016**

Révisions associées

Révision 12e7bff0 - 11/06/2026 17:07 - Joël Cuissinat

Mise en commentaire temporaire de TLSCipherSuite (ref #37502)

Révision 99a711ed - 22/07/2026 18:08 - Laurent Gourvenec

Changement de TLSCipherSuite pour openssl au lieu de gnu-tls

Ref #37502

Historique

#1 - 11/06/2026 17:05 - Joël Cuissinat

- Lié à Tâche #15194: La réplication en ldaps n'est plus fonctionnelle (SC-T13-002) ajouté

#2 - 11/06/2026 17:07 - Joël Cuissinat

- Description mis à jour

#3 - 20/07/2026 12:02 - Laurent Gourvenec

- Assigné à mis à Laurent Gourvenec

- Tâche parente changé de #37403 à #37405

#4 - 20/07/2026 17:38 - Laurent Gourvenec

En 2.11, slapd n'utilise plus la bibliothèque libgnutls.so mais la lib libssl.so :

```
zephir2.10 # ldd /usr/sbin/slapd
    libgnutls.so.30 => /lib/x86_64-linux-gnu/libgnutls.so.30 (0x0000763ab8e05000)
```

```
zephir2.11 # ldd /usr/sbin/slapd
    libssl.so.3 => /usr/lib/x86_64-linux-gnu/libssl.so.3 (0x000079b56cc7c000)
```

Ce ne sont donc plus les mêmes classes à utiliser. Par ailleurs, c'est précisé dans le fichier source slapd.README.debian, dans la section "Known issues for OpenLDAP 2.6.x upgrades". En revanche, difficile de retrouver la valeur par défaut ! La seule source que je trouve est ici : https://www.zytrax.com/books/ldap/ch6/ et dit que par défaut, ce serait "TLSCipherSuite ALL". Cela ne convient pas.

En 2.10, slapd est configuré pour accepter les connexions utilisant :

```
# gnutls-cli --list --priority 'SECURE256:+SIGN-ALL:-VERS-SSL3.0:!AES-128-CBC:!3DES-CBC:!DES-CBC:!ARCFOUR-128:
!ARCFOUR-40:!RC2-40:!CAMELLIA-128-CBC:!NULL'
Cipher suites for SECURE256:+SIGN-ALL:-VERS-SSL3.0:!AES-128-CBC:!3DES-CBC:!DES-CBC:!ARCFOUR-128:!ARCFOUR-40:!R
C2-40:!CAMELLIA-128-CBC:!NULL
TLS_AES_256_GCM_SHA384                          0x13, 0x02    TLS1.3
TLS_CHACHA20_POLY1305_SHA256                    0x13, 0x03    TLS1.3
TLS_ECDHE_ECDSA_AES_256_GCM_SHA384              0xc0, 0x2c    TLS1.2
TLS_ECDHE_ECDSA_CHACHA20_POLY1305               0xcc, 0xa9    TLS1.2
TLS_ECDHE_ECDSA_AES_256_CCM                     0xc0, 0xad    TLS1.2
TLS_ECDHE_RSA_AES_256_GCM_SHA384                0xc0, 0x30    TLS1.2
TLS_ECDHE_RSA_CHACHA20_POLY1305                 0xcc, 0xa8    TLS1.2
TLS_RSA_AES_256_GCM_SHA384                      0x00, 0x9d    TLS1.2
TLS_RSA_AES_256_CCM                             0xc0, 0x9d    TLS1.2
TLS_DHE_RSA_AES_256_GCM_SHA384                  0x00, 0x9f    TLS1.2
TLS_DHE_RSA_CHACHA20_POLY1305                   0xcc, 0xaa    TLS1.2
TLS_DHE_RSA_AES_256_CCM                         0xc0, 0x9f    TLS1.2

Protocols: VERS-TLS1.3, VERS-TLS1.2, VERS-DTLS1.2
Ciphers: AES-256-GCM, CHACHA20-POLY1305, AES-256-CBC, AES-256-CCM
MACs: AEAD
Key Exchange Algorithms: ECDHE-ECDSA, ECDHE-RSA, RSA, DHE-RSA
Groups: GROUP-SECP384R1, GROUP-SECP521R1, GROUP-FFDHE8192
PK-signatures: SIGN-RSA-SHA384, SIGN-RSA-PSS-SHA384, SIGN-RSA-PSS-RSAE-SHA384, SIGN-ECDSA-SHA384, SIGN-ECDSA-S
ECP384R1-SHA384, SIGN-EdDSA-Ed448, SIGN-RSA-SHA512, SIGN-RSA-PSS-SHA512, SIGN-RSA-PSS-RSAE-SHA512, SIGN-ECDSA-
SHA512, SIGN-ECDSA-SECP521R1-SHA512, SIGN-RSA-SHA256, SIGN-RSA-PSS-SHA256, SIGN-RSA-PSS-RSAE-SHA256, SIGN-ECDS
A-SHA256, SIGN-ECDSA-SECP256R1-SHA256, SIGN-EdDSA-Ed25519, SIGN-RSA-SHA1, SIGN-ECDSA-SHA1
```

Dans le man de openssl-ciphers, on peut lire "The default cipher suite list provides strong security and reasonable interoperability. A cipher suite can be not included in the default list for different reasons: because it is weak, or not "mature" enough, or not widely used, etc." -> je propose donc de mettre DEFAULT.

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES256-SHA
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-SHA
RSA-PSK-AES256-GCM-SHA384
DHE-PSK-AES256-GCM-SHA384
RSA-PSK-CHACHA20-POLY1305
```

```
DHE-PSK-CHACHA20-POLY1305
ECDHE-PSK-CHACHA20-POLY1305
AES256-GCM-SHA384
PSK-AES256-GCM-SHA384
PSK-CHACHA20-POLY1305
RSA-PSK-AES128-GCM-SHA256
DHE-PSK-AES128-GCM-SHA256
AES128-GCM-SHA256
PSK-AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256
ECDHE-PSK-AES256-CBC-SHA384
ECDHE-PSK-AES256-CBC-SHA
SRP-RSA-AES-256-CBC-SHA
SRP-AES-256-CBC-SHA
RSA-PSK-AES256-CBC-SHA384
DHE-PSK-AES256-CBC-SHA384
RSA-PSK-AES256-CBC-SHA
DHE-PSK-AES256-CBC-SHA
AES256-SHA
PSK-AES256-CBC-SHA384
PSK-AES256-CBC-SHA
ECDHE-PSK-AES128-CBC-SHA256
ECDHE-PSK-AES128-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
SRP-AES-128-CBC-SHA
RSA-PSK-AES128-CBC-SHA256
DHE-PSK-AES128-CBC-SHA256
RSA-PSK-AES128-CBC-SHA
DHE-PSK-AES128-CBC-SHA
AES128-SHA
PSK-AES128-CBC-SHA256
PSK-AES128-CBC-SHA
```

À noter : AES-128-CBC qui n'était pas dans la liste gnu-tls, est dans la liste DEFAULT de openssl.

On peut aussi retirer SSLv3 et TLSv1 comme pour la liste avec gnuTLS : openssl ciphers -v 'DEFAULT:!SSLv3:!TLSv1'

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
RSA-PSK-AES256-GCM-SHA384
DHE-PSK-AES256-GCM-SHA384
RSA-PSK-CHACHA20-POLY1305
DHE-PSK-CHACHA20-POLY1305
ECDHE-PSK-CHACHA20-POLY1305
AES256-GCM-SHA384
PSK-AES256-GCM-SHA384
PSK-CHACHA20-POLY1305
RSA-PSK-AES128-GCM-SHA256
DHE-PSK-AES128-GCM-SHA256
AES128-GCM-SHA256
PSK-AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256
```

Si quelqu'un a un avis, je suis preneur.

#5 - 22/07/2026 11:06 - Joël Cuissinat

OK pour :

```
DEFAULT:!SSLv3:!TLSv1
```

#6 - 22/07/2026 18:19 - Laurent Gourvenec

- Statut changé de Nouveau à À valider

- % réalisé changé de 0 à 100

#7 - 04/08/2026 15:46 - Ludwig Seys

- Statut changé de À valider à Résolu

#8 - 17/08/2026 12:03 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

```
eole-annuaire$ git branch -r --contains 99a711ed
  origin/HEAD -> origin/master
  origin/dist/eole/2.11.0/master
  origin/master
```