eole-courier - Tâche #11345

Désactiver le SSLv3 sur courier (pops/imaps)

04/20/2015 03:36 PM - Joël Cuissinat

Status:	Fermé	**Start date:**	04/20/2015
Priority:	Normal	**Due date:**	
Assigned To:	Laurent Flori	**% Done:**	100%
Target version:	Sprint 2015 49-51 - Équipe MENESR	**Estimated time:**	2.00 hours
		Spent time:	2.33 hours

Description

Associated revisions

Revision 5293ad0c - 12/01/2015 03:34 PM - lolo

Désactivation des chaines de chriffrement faibles
LEs chaines faibles sont désactivées.
Il ne reste que le TLS1 (impossible d'activer 1_1 et 1_2 avec)
cf: http://sourceforge.net/p/courier/mailman/message/32939849/

fixes: #11345 @2h

History

#1 - 11/30/2015 09:35 AM - Laurent Flori

- Assigned To set to Laurent Flori

#2 - 12/01/2015 10:14 AM - Scrum Master

- Status changed from Nouveau to En cours

#3 - 12/01/2015 03:53 PM - Anonymous

- Status changed from En cours to Résolu

- % Done changed from 0 to 100

Appliqué par commit 5293ad0c4258d5a08d5851c7914c27319b5a874a.

#4 - 12/04/2015 04:38 PM - Joël Cuissinat

- Remaining (hours) changed from 2.0 to 0.5

- Avant (2.5.1) :

```
root@scribe:~# openssl s_client -connect localhost:993 -ssl3
   [ ... ]
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : AES256-SHA
    Session-ID: 597892FD0732B6FE08774E14E26A91766794AF05455D63AB9AF3F8FF448E842C
```

```
    Session-ID-ctx:
    Master-Key: 01A08D3A6920B51CEC15A2C835C37A732FBCF797B360050D8F4F0C8CF9660DD3772B4BD8DC4355686619BDC307
49E462
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1449242261
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)


root@scribe:~# openssl s_client -connect localhost:995 -ssl3
   [ ... ]
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : AES256-SHA
    Session-ID: 24A2E762848ACE4D98C4EEEAD1AE9B5EC849590D4769B517AB12758EE88709E2
    Session-ID-ctx:
    Master-Key: 8E6F1129D05117115A0AAE9EFC9156B0DB17985C95327398C2AD965ED301F95AEBA9C1236BD352B10FC071882D
10D720
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1449242402
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
```

- Après (2.5.2) :

```
root@scribe:~# openssl s_client -connect localhost:993 -ssl3 >/dev/null
140184385988256:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1262:SS
L alert number 40
140184385988256:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:598:


root@scribe:~# openssl s_client -connect localhost:995 -ssl3 >/dev/null
140439805875872:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1262:SS
L alert number 40
140439805875872:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:598:
```

#5 - 12/04/2015 05:04 PM - Joël Cuissinat

- Status changed from Résolu to Fermé

- Remaining (hours) changed from 0.5 to 0.0