Distribution EOLE - Scénario #34660

EOLE 2.9 : utiliser au minimum TLS1.3

30/09/2022 13:55 - Gilles Grandgérard

Statut:	Terminé (Sprint)	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	01/01/2024
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Livraison Cadoles 30/11/2022	**Temps passé:**	0.00 heure

Description

Il reste des applications en TLS 1.2.

SSLPort 127.0.0.1:4200 192.168.0.5 EAD2
Verification: OK
subject=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = dc1.domseth.ac-test.fr
issuer=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = CA-dc1.domseth.ac-test.fr
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384

SSLPort 192.168.0.5:4200 192.168.0.5 EAD2
Verification: OK
subject=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = dc1.domseth.ac-test.fr
issuer=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043 015, OU = ac-test, CN = CA-dc1.domseth.ac-test.fr
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384

Sous-tâches:

Tâche # 34754: Étude	**Fermé**
Tâche # 34764: utiliser TLS 1.3	**Fermé**
Tâche # 34771: Tester	**Fermé**

Demandes liées:

Lié à Distribution EOLE - Tâche #29741: Backport en 2.6 du TLS 1.2 EAD2 et Zé...	**Fermé**	**09/04/2019**
Lié à Distribution EOLE - Tâche #35232: ZEPHIR 2.9 : problème communication a...	**Fermé**	**13/02/2023**

Historique

#1 - 30/09/2022 17:04 - Joël Cuissinat

- Lié à Tâche #29741: Backport en 2.6 du TLS 1.2 EAD2 et Zéphir_Web ajouté

#2 - 30/09/2022 17:23 - Joël Cuissinat

Visiblement, pour l'EAD2 (et Zéphir), il faut utiliser **SSL.TLS_METHOD** à la place de l'actuel **SSL.TLSv1_2_METHOD**.

- Fichier EAD2 : /usr/share/ead2/lib/libsecure.py
- Fichier Zéphir : certificats.py

La désactivation des anciens protocoles peut être forcée en ajoutant cette ligne :

```
tx.set_options(SSL.OP_NO_TLSv1_2 | SSL.OP_NO_TLSv1_1 | SSL.OP_NO_TLSv1)
```

Vérifier si le TLS 1.3 est disponible sur la version de python OpenSSL utilisée sur EOLE 2.8.

#3 - 30/09/2022 17:24 - Joël Cuissinat

- Release mis à EOLE 2.9.0

#4 - 20/10/2022 10:34 - Gilles Grandgérard

- Release changé de EOLE 2.9.0 à Carnet de produit (Cadoles)

#5 - 20/10/2022 10:41 - Laurent Gourvenec

- Echéance mis à 01/01/2024

- Assigné à mis à Philippe Caseiro

- Version cible mis à Carnet Cadoles

- Début mis à 01/10/2022

#6 - 20/10/2022 12:37 - Laurent Gourvenec

- Assigné à changé de Philippe Caseiro à Benjamin Bohard

#7 - 07/11/2022 10:59 - Ludwig Seys

- Statut changé de Nouveau à Résolu

#8 - 15/11/2022 17:47 - Joël Cuissinat

- Release changé de Carnet de produit (Cadoles) à EOLE 2.9.0

#9 - 15/11/2022 17:55 - Joël Cuissinat

- Statut changé de Résolu à Terminé (Sprint)

#10 - 17/11/2022 15:40 - Joël Cuissinat

- Version cible changé de Carnet Cadoles à Livraison Cadoles 30/11/2022

#11 - 14/02/2023 10:32 - Joël Cuissinat

- Lié à Tâche #35232: ZEPHIR 2.9 : problème communication avec les Horus 2.6 (suite à la désactivation du TLS 1.2) ajouté