Distribution EOLE - Tâche #33506

Scénario # 33424 (Terminé (Sprint)): évolutions Upgrade-Auto

Zéphir ne transmet pas les certificats intermédiaire

10/12/2021 17:06 - Emmanuel GARETTE

Statut:	Fermé	**Début:**	15/03/2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	MTES - prestation Cadoles - s46-52	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Si on édite le fichier :

zephir-parc/python/zephir/certificats.py

On voit la ligne suivante :

```
        ctx.use_certificate_chain_file(cert_file)
```

Contrairement à ctx.user_certificate_file, la fonction use_certificate_chain_file peut recevoir la chaine complète de certification (le certificat + les intermédiaires.

Dans posttemplate/10-conf-ssl-zephir on peut voir :

```
ret = run_bash_function("/usr/lib/eole/utils.sh", "InstallSSLFiles", "{0} {1} {2} {3}".format(cert
name, username, groupname, SSL_dir))
```

La commande InstallSSLFiles copie le fichier server_cert (sans la chaine) alors qu'il devrait copier server_pem (avec la chaine).

Demandes liées:

Lié à eole-ad - Tâche #34058: Documentation sur les certificats à relire et p...	**Fermé**	**09/05/2022**	**03/06/2022**

Historique

#1 - 10/12/2021 17:07 - Emmanuel GARETTE

- Description mis à jour

#2 - 16/12/2021 12:15 - Emmanuel GARETTE

- Statut changé de Nouveau à En cours

#3 - 16/12/2021 12:15 - Emmanuel GARETTE

- Assigné à mis à Emmanuel GARETTE

#4 - 10/01/2022 17:15 - Emmanuel GARETTE

La fonction utilisée pour charger le fichier est celle décrit dans la doc d'Openssl :

```
SSL_CTX_use_certificate_chain_file() loads a certificate chain from file into ctx. The certificates must be in
 PEM format and must be sorted starting with the subject's certificate (actual client or server certificate),
followed by intermediate CA certificates if applicable, and ending at the highest level (root) CA.
```

Le fichier doit donc contenir (et dans cette ordre) :

- le certificat local
- les éventuels intermédiaire
- le certificat de la CA

Aujourd'hui le fichier utiliser par cette fonction est le fichier %%creole_cert.
Ce fichier ne contient que le certificat local (qu'il soit généré par creole, obtenu par let's encrypt).

En cas de mise en place du certificat manuel ce n'est pas spécialement clair comment configurer le fichier :
http://eole.ac-dijon.fr/documentations/2.7/completes/HTML/ModuleZephir/co/07_certificats.html#vcNad :

creole_cert semble être le certificat appelé mon-serveur.crt. Il faudrait préciser qu'il s'agit bien de ce fichier.
De plus il manque la CA racine.

Au final c'est surement un problème de configuration.

#5 - 10/01/2022 17:36 - Emmanuel GARETTE

Je propose de réorganiser le paragraphe sur le certificat manuel comme suit :

La partie "Certificat de type manuel" ne bouge pas.

Suppression du titre : "Certificats intermédiaires"

Mettre le titre : "Chemin du fichier contenant le certificat SSL"

Le certificat SSL est contenu dans un fichier au format PEM. Ce certificat SSL commence par "-----BEGIN CERTIFICATE-----" et fini par "-----END CERTIFICATE-----".

Le chemin du fichier doit être le fichier contenant le certificat ainsi que les intermédiaires (reprendre le paragraphe "Certificats intermédiaires").

A la fin préciser que "Chemin du fichier contenant le certificat SSL" est bien /etc/ssl/cert/mon-serveur.crt dans notre exemple.

Ajouter le titre "Chemin du fichier contenant la clé privée du certificat SSL"

Mettre le chemin du fichier contenant la clé privée au format PEM (généralement fichier en .key).

La clé privé commence par "-----BEGIN RSA PRIVATE KEY-----" et fini par "-----END RSA PRIVATE KEY-----".

Ajouter le titre "Chemin du fichier contenant la chaîne de certification" (FIXME je trouve que la description de la variable n'est pas bonne).

Ce fichier est la concatenation du fichier du certificat (sans les intermédiaires) et de la clé privé.

Il y a une deuxième partie "Certificats intermédiaires" est-ce nécessaire ?

#6 - 10/01/2022 17:56 - Emmanuel GARETTE

Il y a un problème avec la phrase :

```
/etc/ssl/certs/eole.crt : certificat serveur généré par la CA locale, il est utilisé par les applications (apa
che, ead2, eole-sso, ...) ;
```

Le certificat n'est pas généré par la CA locale. Il est signé par la CA locale.

#7 - 13/01/2022 11:42 - Ludwig Seys

- Assigné à changé de Emmanuel GARETTE à Ludwig Seys

#8 - 13/01/2022 11:42 - Ludwig Seys

- % réalisé changé de 0 à 20

#9 - 13/01/2022 14:30 - Ludwig Seys

- % réalisé changé de 20 à 40

création :
/2_7/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/certificats-paramètre-letsEncrypt.unit
/2_7/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/certificat-letsencrypt-2.7.2-01.png
/2_7/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/certificats-paramètre-letsEncrypt.unit
modification :
/2_7/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats.scen

#10 - 13/01/2022 15:03 - Ludwig Seys

- % réalisé changé de 40 à 90

modification :
/2_8/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/07_certificats-letsEncrypt.unit
/2_7/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/07_certificats-letsEncrypt.unit
/2_8/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats.scen

création :
/2_8/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/certificat-letsencrypt-2.8.1-01.png
/2_8/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats/certificats-paramètre-letsEncrypt-2.8.unit

#11 - 14/02/2022 10:59 - Ludwig Seys

- Statut changé de En cours à À valider

- % réalisé changé de 90 à 100

correction apporté aux fichiers :
/2_8/commun/02_miseEnOeuvre/04_configuration/03_configurationExperte/07_certificats.scen

#12 - 11/04/2022 11:14 - Emmanuel GARETTE

- Statut changé de À valider à Résolu

#13 - 14/04/2022 10:18 - Joël Cuissinat

- Lié à Tâche #34058: Documentation sur les certificats à relire et porter en 2.9 ajouté

#14 - 17/05/2022 09:58 - Philippe Carre

- Statut changé de Résolu à Fermé

- Temps estimé mis à 0.00 h

- Restant à faire (heures) mis à 0.0