Distribution EOLE - Scénario #27453

diagnose des certificats doit prendre en compte les CA natives si on ne spécifie pas de CAFILE ($4)

03/28/2019 05:26 PM - Emmanuel GARETTE

Status:	Terminé (Sprint)	**Start date:**	09/23/2019
Priority:	Normal	**Due date:**	10/11/2019
Assigned To:	Philippe Caseiro	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Prestation Cadoles 39-41	**Spent time:**	6.00 hours

Description

Dans /usr/share/eole/diagnose/05-common il y a "TestCerts $server_cert 10 "certificat expiré"".

Dans la fonction TestCerts il y a :

```
    if [ -z "$4" ]; then
        echo "$CERTFILE" | grep -q '^/etc/ipsec.d/'
        [ $? = 0 ] && CAFILE=/etc/ipsec.d/cacerts/CertifCa.pem || CAFILE=/etc/ssl/certs/ca.crt
```

On est bien dans ce cas puisque $4 n'est pas défini. Donc CAFILE est /etc/ssl/certs/ca.crt.

On a ensuite :

```
    if [[ -d ${CAFILE}  ]]
    then
        cat ${CAFILE}/* > ${TMPFILE}
        CAFILE=${TMPFILE}
    fi
```

Je vois pas bien pourquoi un fichier CAFILE deviendrait tout d'un coup un répertoire mais admettons.

Après nous avons :

```
ssl_cmd="/usr/bin/openssl verify -CAfile $CAFILE -CApath $FAKE_CAPATH -purpose any $CERTFILE"
```

Donc le certificat n'est validé que sur la CA généré localement pour les certificats auto signés :

. cadoles.crt => Erreur : self signed certificate

Si je lis la documentation :

```
Après génération de la CA locale, un fichier /etc/ssl/certs/ca.crt est créé qui regroupe les certi
ficats suivants :

    ca_local.crt ;
    ACInfraEducation.pem ;
    tout certificat présent dans le répertoire /etc/ssl/local_ca/
```

Le problème c'est que mon certificat est signé pour une CA nativement reconnu sur Ubuntu (donc n'est pas dans local_ca).

Solutions à mettre en œuvre

- prendre en compte les CA local lors du test du certificat (ca me semble mieux).
- Corriger le test diagnose pour qu'il soit fonctionnel dans tous les cas

Critères d'acceptation

- diagnose correct

Subtasks:

Tâche # 29020: Etude et analyse du problème	**Fermé**
Tâche # 29021: Création d'un test diagnose pour les certificats manuels et LE	**Fermé**

Related issues:

Related to Distribution EOLE - Tâche #23543: Let's Encrypt et diagnose	**Fermé**	**01/20/2021**
Related to Distribution EOLE - Tâche #29041: Validation du scénario : diagnos...	**Fermé**	**09/23/2019**

History

#1 - 04/01/2019 11:30 AM - Fabrice Barconnière

- Tracker changed from Demande to Scénario

- Subject changed from diagnose des certificats étrange to diagnose des certificats doit prendre en compte les CA natives si on ne spécifie pas de CAFILE ($4)

- Start date deleted (03/28/2019)

- Release set to EOLE 2.6.2.2

- Story points set to 1.0

#2 - 08/20/2019 03:04 PM - Gilles Grandgérard

- Due date set to 09/20/2019

- Target version set to sprint 2019 36-38 Equipe MENSR

- Start date set to 08/20/2019

#3 - 09/03/2019 10:15 AM - Joël Cuissinat

- Due date deleted (09/20/2019)

- Target version deleted (sprint 2019 36-38 Equipe MENSR)

- Start date deleted (08/20/2019)

- Release changed from EOLE 2.6.2.2 to Carnet de produit (Cadoles)

#4 - 09/11/2019 05:31 PM - Joël Cuissinat

- Description updated

#5 - 09/12/2019 04:49 PM - Gilles Grandgérard

- Description updated

#6 - 09/16/2019 03:09 PM - Joël Cuissinat

- Related to Tâche #23543: Let's Encrypt et diagnose added

#7 - 09/16/2019 03:10 PM - Joël Cuissinat

- Description updated

#8 - 09/17/2019 10:58 AM - Joël Cuissinat

- Due date set to 10/11/2019

- Target version set to Prestation Cadoles 39-41

- Start date set to 09/23/2019

#9 - 09/24/2019 10:16 AM - Philippe Caseiro

- Assigned To set to Philippe Caseiro

#10 - 09/24/2019 02:22 PM - Philippe Caseiro

Bonjour

Je viens de passer la matinée à analyser la situation, et pour y voir plus clair, voici un résumé.

Lorsqu'on utilise un certificat "acheté" ou "fournis" par une autorité, on passe le serveur en mode "Manuel" actuellement dans ce mode nous sommes incapables de vérifier la validité du certificat car notre méthode de vérification se base sur des CA locales. Problème supplémentaire si on utilise un certificat signé par une autorité intermédiaire (TERENA par exemple) nous ne sommes pas en mesure de vérifier le certificat car nous n'avons pas cet intermédiaire.

Dans le cas évoqué par Emmanuel, nous avons un certificat TERENA et nous avons placé l'autorité intermédiaire dans le fichier indiqué dans la variable server_pem donc si j'utilise ce fichier, je peut vérifier le certificat mais c'est valable pour notre cas et pas forcément dans le cas général.

Donc pour avancer sur le sujet, je propose qu'en mode manuel dans diagnose nous indiquions l'autorité de certification ainsi que la date limite du certificat et une alerte quand elle se rapproche, et uniquement en mode manuel. Cette proposition change légèrement la demande, pouvez-vous me valider cette proposition ?

Merci.

#11 - 09/25/2019 08:01 AM - Fabrice Barconnière

```
<Puppet_Master> Bonjour
<Puppet_Master> jojo2024: https://dev-eole.ac-dijon.fr/issues/27453
<Puppet_Master> pour avis et validation
<Puppet_Master> merci
<Puppet_Master> je suis dispo au téléphone si besoin
<jojo2024> Puppet_Master: on regarde
<Puppet_Master> merci jojo2024
<barco>
 Puppet_Master: il me semble qu'un service ne peut pas fonctionner s'il n'a pas toutes les CA intermédiaires
<barco> donc la variable server_pem doit faire référence à la chaîne dans tous les cas, non ?
<Puppet_Master>
 barco: pas forcément par contre on peut avoir des services ou du coup le certificat n'est pas considéré comme
 valide
<Puppet_Master> si t'as pas toute la chaine
<barco>
 Puppet_Master: en tout cas, openssl en a besoin pour vérifier le certificat. Je n'ai pas de service en tête q
ui n'aurai pas besoin des CA intermédiaires.
<Puppet_Master>
 barco: tu peux mettre à jour la demande, je bosse déjà sur une version spécifique du diagnose pour le mode "m
anuel" je vais ajouter la vérfication avec le chain.pem
<Puppet_Master> enfin avec la chaine quoi
<Puppet_Master> merci barco
```

#12 - 10/01/2019 08:59 AM - Fabrice Barconnière

- Related to Tâche #29041: Validation du scénario : diagnose des certificats doit prendre en compte les CA natives si on ne spécifie pas de CAFILE ($4) added

#13 - 10/02/2019 09:34 AM - Fabrice Barconnière

- Status changed from Nouveau to Terminé (Sprint)

#14 - 10/31/2019 02:08 PM - Joël Cuissinat

- Release changed from Carnet de produit (Cadoles) to EOLE 2.7.1.2