Distribution EOLE - Tâche #34595

Scénario # 34549 (Terminé (Sprint)): Gestion du certificat LSC/ScribeAD

Tester

14/09/2022 09:12 - Benjamin Bohard

Statut:	Fermé	**Début:**	05/09/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	Prestation Cadoles MEN 2022 36-39	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 14/09/2022 09:20 - Benjamin Bohard

Plusieurs tests à effectuer.

En 2.7.2, il faut vérifier que le coffre le clés de java est mis à jour au reconfigure.

À partir de 2.8.1, il faut tester le diagnose dans différents cas :

- certificat autosigné :
  - sans sujet dns alternatif :
    - certificat concordant
    - certificat avec des noms alternatifs
  - avec sujet dns alternatif :
    - certificat concordant
    - certificat sans nom alternatif

- certificat letsencrypt :
  - sans sujet dns alternatif :
    - certificat concordant
    - certificat principal avec nom alternatif
  - avec sujet dns alternatif (deux variables : ssl_subjectaltname pour alimenter le certificat principal, le_extra_names) :
    - certificat concordant
    - certificat principal sans nom alternatif

Le test letsencrypt ne peut pas être effectué sur Scribe parce que le challenge du protocole acme necéssite un service web pouvant répondre à l'adresse résolue pour le nom DNS (addc.domscribe.ac-test.fr résout en 192.168.0.30, adresse du conteneur dans lequel aucun service n'écoute sur le port 80).

Pour tester sur Eolebase :

- cas autosigné :

1. diagnose (cas normal, un seul DNS, certificat autosigné valide)
2. CreoleSet ssl_subjectaltname pour ajouter un DNS
3. diagnose (avant regénération du certificat) => certificat invalide parce que tous les noms de la configuration ne sont pas pris en compte
4. regénération du certificat (reconfigure + /usr/share/creole/gen_certif.py -f + reconfigure)
5. diagnose => certificat de nouveau valide
6. CreoleSet ssl_subjectaltname pour enlever un DNS
7. diagnose (avant regénération du certificat) => certificat invalide parce qu'il y a un nom en trop dans le certificat
8. regénération du certificat
9. diagnose => certificat de nouveau valide

- cas letsencrypt :

1. s'assurer que les certificats autorité sont présents sur le serveur Eolebase [1]
2. s'assurer qu'on peut résoudre des noms de domaines supplémentaires vers l'IP du serveur Eolebase [2]
3. CreoleSet cert_type letsencrypt
4. diagnose => certificat valide
5. S'arranger pour que la demande de certificat soit de nouveau effectuée lors du prochain reconfigure (test l.130 du fichier /usr/share/eole/postservice/00-letsencrypt à tromper)
6. CreoleSet ssl_subjectaltname pour ajouter un DNS
7. diagnose (avant regénération du certificat) => certificat invalide parce que tous les noms de la configuration ne sont pas pris en compte

8. regénération du certificat (reconfigure + /usr/share/creole/gen_certif.py -f + reconfigure)
9. diagnose => certificat de nouveau valide
10. CreoleSet le_extra_names pour ajouter des demandes de certificat
11. diagnose => certificat local toujours valide, certificats supplémentaires non trouvés
12. reconfigure pour effectué les demandes de certificats supplémentaires
13. diagnose => tous les certificats sont valides

[1] Dans le cas de l'utilisation de step-ca, avec une installation basique, les certificats sont dans /root/.step/certs/

[2] Dans le cas de l'utilisation d'une pki interne se servant de la passerelle pour la résolution de noms, il est possible d'éditer la configuration de dnsmasq sur cette passerelle pour ajouter une entrée type "address=/.certtest.ac-test.fr/192.168.0.24/" dans un fichier /etc/dnsmasq.d/hosts.conf et de redémarrer le service dnsmasq pour avoir une résolution des noms *.certtest.ac-test.fr en 192.168.0.24.

#2 - 14/09/2022 12:21 - Benjamin Bohard

Mauvais test diagnose…

#3 - 14/09/2022 14:16 - Ludwig Seys

- Assigné à mis à Ludwig Seys

#4 - 15/09/2022 11:40 - Benjamin Bohard

Donc, pour le problème spécifique remonté dans le scénario sur le test du certificat pas assez pertinent, on peut vérifier le nouveau comportement avec la procédure suivante :

1. diagnose => le certificat samba est valide
2. CreoleSet ssl_subjectaltname pour enlever le nom de domaine addc.domscribe.ac-test.fr
3. regénération du certificat (reconfigure + /usr/share/creole/gen_certif.py -f + reconfigure) OU (pour valider également le fait qu'on évite de copier le fichier inexistant) en faisant la procédure rm -f /etc/ssl/certs/eole.crt;reconfigure
4. diagnose => le certificat samba est identifié comme invalide avec indication du nom de domaine manquant

#5 - 16/09/2022 09:34 - Ludwig Seys

- Statut changé de Nouveau à En cours

#6 - 26/09/2022 12:37 - Ludwig Seys

- Statut changé de En cours à Résolu

#7 - 29/09/2022 10:44 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- % réalisé changé de 0 à 100

- Restant à faire (heures) mis à 0.0