Distribution EOLE - Scénario #33470

[amonecole2.8.1]chaîne certificats incomplète avec Lets Encrypt

02/12/2021 09:38 - Christophe De Natale

Statut:	Terminé (Sprint)	**Début:**	05/01/2022
Priorité:	Normal	**Echéance:**	14/01/2022
Assigné à:	Emmanuel GARETTE	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Prestation Cadoles MEN 2021 50-02	**Temps passé:**	0.00 heure

Description

Bonjour,

En demandant des certificats LE la procédure s'achève correctement, ils sont obtenus et les accès aux adresses web du serveur sont ok depuis l'extérieur mais j'ai une erreur au diagnose dans le conteneur "addc" :

```
Certificat LDAPS :
    Certificat => Fichier tls/cert.pem manquant
                CA=>Fichier tls/ca.pem manquant
```

Dans le conteneur addc, il manque le chemin des certificats dans le smb.conf :

```
# active TLS (pour LDAPS et la maj des mot de passe !
  tls enabled = yes
```

Concernant le chemin des certificats, il n'y rien ici :

```
root@addc:~# ls -als /etc/samba/tls/
total 8
4 drwxr-xr-x 2 root root 4096 nov.  12 14:42 .
4 drwxr-xr-x 4 root root 4096 nov.  30 23:02 ..
```

Ils résident ici :

```
root@addc:~# ls -als /var/lib/samba/private/tls/
total 28
4 drwxr-xr-x 4 root root 4096 nov.  28 17:39 .
4 drwxr-xr-x 8 root root 4096 déc.   1 05:08 ..
4 -rw-r--r-- 1 root root 2037 nov.  28 15:57 ca.pem
4 -rw-r--r-- 1 root root 2041 nov.  28 15:57 cert.pem
4 drwxr-xr-x 2 root root 4096 nov.  28 17:39 certs
4 -rw------- 1 root root 3243 nov.  28 15:57 key.pem
4 drwx------ 2 root root 4096 nov.  28 17:39 private
```

A noter que de ce fait, dans le LAN la navigation vers Internet est ok mais "eoleapps" par exemple n'est pas fonctionnel à cause du ticket créé par SSO (url redirigée sur 3kms...)

En repassant en auto-signé, la conf smb est correcte mais l'accès aux applications ne fonctionne pas ou très difficilement (Firefox = page blanche lorsque l'on veut afficher le certificat, Edge l'accepte):

```
# active TLS (pour LDAPS et la maj des mot de passe !
 tls enabled = yes
 tls keyfile = /var/lib/samba/private/tls/private/addc.key
 tls certfile = /var/lib/samba/private/tls/certs/addc.crt
 tls cafile =
```

Peut-être une solution pour le conteneur addc, j'ai juste testé la requête du challenge DNS LE après avoir créé mon enregistrement TXT dans la zone dns du domaine : ça fonctionne, on obtient les certificats mais je n'ai pas su s'il fallait les concaténer ou les déposer directement dansle dossier tls du conteneur.
Un article ici explique comment ajouter un enregistrement txt dans la zone DNS autoritaire contenant "_acme-challenge.fqdn-du-serveurAD", puis effectuer un challenge "dns-01" afin de récupérer la valeur à inclure dans cet enregistrement : https://www.dvolve.net/blog/2019/12/using-lets-encrypt-for-active-directory-domain-controller-certificates/

Sous-tâches:

Tâche # 33627: Vérifier correctement le certificat SSL en mode auto généré	**Fermé**
Tâche # 33628: Tester	**Fermé**
Tâche # 33669: Voir le fonctionnement sur AmonEcole	**Fermé**

Demandes liées:

Lié à Distribution EOLE - Tâche #33585: Valider le scénario [amonecole2.8.1]...	**Fermé**	**22/12/2021**

Historique

#1 - 02/12/2021 09:43 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Début 02/12/2021 supprimé

- Release mis à Carnet de produit (Cadoles)

- Points de scénarios mis à 3.0

#2 - 14/12/2021 10:18 - Matthieu Lamalle

- Echéance mis à 14/01/2022

- Assigné à mis à Emmanuel GARETTE

- Version cible mis à Prestation Cadoles MEN 2021 50-02

- Début mis à 13/12/2021

- Release Carnet de produit (Cadoles) supprimé

#3 - 06/01/2022 15:28 - Ludwig Seys

- Statut changé de Nouveau à Résolu

#4 - 13/01/2022 15:13 - Joël Cuissinat

Rappel : En mode Let's Encrypt on n'est pas sûr des noms de domaine utilisés par Samba donc on utilise les certificats auto-générés par Samba.

#5 - 13/01/2022 15:14 - Joël Cuissinat

- Statut changé de Résolu à Terminé (Sprint)

- Release mis à EOLE 2.8.1

#6 - 17/01/2022 09:56 - Joël Cuissinat

- Lié à Tâche #33585: Valider le scénario [amonecole2.8.1]chaîne certificats incomplète avec Lets Encrypt ajouté