Distribution EOLE - Tâche #35223

Scénario # 35122 (Terminé (Sprint)): init_sphynx Sphynx 2.8.1

Impossible d'importer un certificat émis par la PNCN sur Sphynx 2.8.1

06/02/2023 16:33 - Olivier FEBWIN

Statut:	Fermé	**Début:**	06/02/2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	Livraison Cadoles 31/03/2023	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Je viens de tester après l'installation des paquets arv (2.8.1-11), eole-sphynx (2.8.1-2), eole-sphynx-all (2.8.1-2), eole-sphynx-module (2.8.1-2), python-arv (2.8.1-11) ça ne fonctionne toujours pas. J'obtiens cette fois l'erreur suivante en tentant d'importer le certificat via l'ARV :

(voir PJ)

et sensiblement la même chose en tentant d'importer le certificat via le script init_sphynx :

```
root@sphynx-agriates2:~# init_sphynx
Une base ARV existe déjà. Écraser la base actuelle ? [oui/non]
[non] : oui
* Génération du certificat de la CA
Entrez le login Zéphir : ofebwin
Entrez le mot de passe Zéphir :
1- 0800069R--Concentrateur VPN zone AGRIATES - Id Zéphir : 3 - Version : 2.8.1
2- 0800069R--Concentrateur VPN zone AGRIATES 2.7.2 - Id Zéphir : 5 - Version : 2.7.2
3- ajouter un serveur Sphynx non enregistré
Choisissez le serveur Sphynx à ajouter (1 par défaut) :
Serveur 0800069R--Concentrateur VPN zone AGRIATES - Id Zéphir : 3 - Version : 2.8.1 ajouté
* Certificat /var/lib/arv/CA/certs/sphynx.pem généré
Voulez-vous ajouter un certificat pour le serveur sphynx
    (les fichiers clé et certificat doivent être accessibles) ? [oui/non]
[non] : oui
Ajout du certificat du serveur sphynx...
Chemin complet du fichier pkcs7 : /tmp/nOK_agriates-amiens-14.ac-amiens.fr.p7b
Chemin complet de la clé privée : /tmp/priv-agriates-amiens-14.ac-amiens.fr.pem
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/arv/lib/util.py", line 420, in split_pkcs7
    chain = cert_chain.get_chain_by_subject(cert_chain.get_leaf_certificate())
  File "/usr/lib/python3/dist-packages/arv/lib/util.py", line 376, in get_chain_by_subject
    if self.certs[self.signed_by[subject]]:
KeyError: 'AC EN Scolarite et Formation'

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/share/eole/sbin/init_sphynx", line 262, in <module>
    populate_database()
  File "/usr/share/eole/sbin/init_sphynx", line 214, in populate_database
    ca_cred, cred = split_pkcs7(credential)
  File "/usr/lib/python3/dist-packages/arv/lib/util.py", line 53, in newFunc
    return func(*args, **kwargs)
  File "/usr/lib/python3/dist-packages/arv/lib/util.py", line 432, in split_pkcs7
    raise Exception('Cannot read pkcs7: {0}'.format(e))
Exception: Cannot read pkcs7: 'AC EN Scolarite et Formation'
```

Révisions associées

Révision dc09d27a - 14/02/2023 09:13 - Benjamin Bohard

Les PKCS7 ne contiennent pas obligatoirement des chaînes complètes.

Ref #35223

Révision e27a1337 - 14/02/2023 09:25 - Benjamin Bohard

Générer également des PKCS7 avec le certificat machine seulement.

Ref #35223

Historique

#1 - 07/02/2023 10:06 - Gilles Grandgérard

- Lié à Scénario #35122: init_sphynx Sphynx 2.8.1 ajouté

#2 - 07/02/2023 10:06 - Gilles Grandgérard

- Tracker changé de Demande à Tâche

#3 - 07/02/2023 10:35 - Joël Cuissinat

- Tâche parente mis à #35122

#4 - 07/02/2023 10:35 - Joël Cuissinat

- Description mis à jour

#5 - 13/02/2023 13:38 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#6 - 13/02/2023 13:38 - Benjamin Bohard

- Assigné à mis à Benjamin Bohard

#7 - 14/02/2023 09:19 - Benjamin Bohard

- Statut changé de En cours à À valider

#8 - 14/02/2023 09:19 - Benjamin Bohard

- % réalisé changé de 0 à 100

Ne pas considérer que les conteneurs PKCS#7 contiennent une chaîne de certificat complète.

#9 - 14/02/2023 09:40 - Benjamin Bohard

La procédure ne peux pas être testée de bout en bout dans le cas d'un PKCS #7 ne contenant pas la chaîne complète avec les données fournies.
Il existe encore un risque que l'importation ne soit pas fonctionnelle avec pour cause l'absence du certificat racine.
Si les certificats racines d'agriates ne sont pas dans la base d'arv avant le chargement du certificat machine, il faut les charger.

#10 - 14/02/2023 12:00 - Olivier FEBWIN

Je viens de tester l'importation du certificat, ça fonctionne parfaitement aussi bien via le script init_sphynx que via l'ARV.
Un grand merci à vous !

#11 - 23/02/2023 16:56 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#12 - 24/02/2023 14:43 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

```
arv$ git branch -r --contains dc09d27a
  origin/2.8.0/master
  origin/2.8.1/master
  origin/HEAD -> origin/master
  origin/dist/eole/2.8.0/master
  origin/dist/eole/2.8.1/master
  origin/dist/eole/2.9.0/master
  origin/master
```

Fichiers

91KTfvCMpfStX2sj.png	17,9 ko	06/02/2023	Olivier FEBWIN