Distribution EOLE - Tâche #33725

Scénario # 33657 (Terminé (Sprint)): Traitement express MEN (03-05)

Impossible d'ajouter un certificat dans arv

26/01/2022 16:58 - Benoit Guinet

Statut:	Fermé	**Début:**	26/01/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Fabrice Barconnière	**% réalisé:**	100%
Version cible:	sprint 2022 03-05 Equipe MENSR	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Bonjour ,
Même problème que dans cette discussion sur un sphynx 2.7.2 à jour :
https://pcll.ac-dijon.fr/listes/arc/amon-sphynx/2021-10/msg00002.html

Historique

#1 - 27/01/2022 14:42 - Fabrice Barconnière

- Tâche parente mis à #33657

#2 - 27/01/2022 14:42 - Fabrice Barconnière

- Projet changé de Sphynx à Distribution EOLE

- Statut changé de Nouveau à En cours

#3 - 27/01/2022 14:43 - Fabrice Barconnière

- Sujet changé de Impossible d'ajouter un certificat dans arv à Impossible d'ajouter un certificat dans arv

- Assigné à mis à Fabrice Barconnière

#4 - 27/01/2022 15:05 - Fabrice Barconnière

Pour résumer

- La version openssl est passée de 1.0 à 1.1 entre EOLE 2.6 (Ubuntu 18.04) et EOLE 2.7 (Ubuntu 20.04).
  - Le format de sortie du subject avec la commande openssl a changé
- ARV a pris en compte ce changement depuis la version 2.7.2-3 (https://dev-eole.ac-dijon.fr/issues/28771). (sur EOLE 2.7.0 -> 2.7.0-7, sur EOLE 2.7.1 -> 2.7.1-3)
- L'image ISO 2.7.2 installe ARV en version 2.7.2-15 donc avec le correctif
- Les premiers certificats importés présentent une anomalie dans le "subject" comme si ARV était dans une version inférieure à 2.7.2-3

La seule chose que je vois, c'est qu'une ISO d'installation obsolète d'EOLE 2.7.2 embarque une version d'ARV inférieure à 2.7.2-3
Il faudrait voir avec l'ISO que vous utilisez quelle est la version d'ARV installée avant de faire une mise à jour.

Sinon, pour résoudre le problème, comme indiqué sur la liste amon-sphynx, voici ce qu'il convient de faire :

- Se connecter root en ssh sur le serveur Sphynx
- Exécuter ces commandes :
  - sqlite3 /var/lib/arv/db/sphynxdb.sqlite 'update arv_db_version_dbversion set version="1.0.0"'
  - /usr/share/eole/posttemplate/00-arv reconfigure

L'importation de certificat devrait être à nouveau opérationnelle.

Voici le suivi sur la liste amon-sphynx :

```
Pour ceux qui rencontreraient ce problème, voici comment le résoudre et ça ne devrait plus se reproduire :
- Se connecter root en ssh sur le serveur Sphynx
- Exécuter ces commandes :
  sqlite3 /var/lib/arv/db/sphynxdb.sqlite 'update arv_db_version_dbversion set version="1.0.0"'
  /usr/share/eole/posttemplate/00-arv reconfigure

L'importation de certificat devrait être à nouveau opérationnelle.
```

Le 27/01/2022 à 11:19, Fabrice Barconnière a écrit :
> Merci pour les renseignements.
> Effectivement, c'est du classique.
> Après l'exécution du script init_sphynx, j'ai bien les certificats sous le bon format :
> sqlite> select subject from arv_db_edge_credential;
> C = FR, L = Dijon, O = Education Nationale, OU = 0002 110043015, CN = sphynx
> C = FR, O = Education Nationale, L = Dijon, OU = 0002 110043015, CN = CA-sphynx-RVP
> C = FR, O = Education Nationale, OU = 0002 110043015, CN = AC EN Scolarite et Formation
> C = FR, O = Education Nationale, OU = 0002 110043015, CN = AC Education Nationale
> C = FR, O = Ministere Education Nationale Enseignement Superieur Recherche, CN = AC Racine Ministere ENESR
>
> Je n'arrive pas à comprendre comment les "subject" se retrouvent sous ce format (avec le "/CN=") :
> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=sphynx
> C = FR, O = Education Nationale, L = Lyon, OU = Academie de Lyon, OU = 0002 110043015/CN=CA-eole-sphynx-3-RVP
> C = FR, O = Education Nationale, OU = 0002 110043015/CN=AC EN Scolarite et Formation
> C = FR, O = Education Nationale, OU = 0002 110043015/CN=AC Education Nationale
> C = FR, O = Ministere Education Nationale Enseignement Superieur Recherche/CN=AC Racine Ministere ENESR
>
> Sauf si la version d'ARV au moment de l'importation de ces certificats est inférieure à 2.7.2-3 mais sur l'iso, ARV est déjà en 2.7.2-15.
>
> Le 27/01/2022 à 11:00, Dominique Jassin a écrit :
>> Bonjour,
>>
>> Du classique, en ce qui me concerne. Téléchargement de l'iso ici http://eole.ac-dijon.fr/pub/iso/EOLE-2.7/latest/ version eole2.7.2-alternate-amd.iso , ensuite enregistrement_zephir et instanciation puis lancement du script init_sphynx pour partir d'une base arv vierge. Je n'ai pas utilisé la procédure sauvegarde.sh et restauration.sh suite à mes ennuis lors de la première installation.
>> J'ai donc ensuite configuré ma base arv manuellement et pour les certificats, je les ai genèré via arv, ajouter générer une requête de certificat pour une AC et ensuite quand la PNCN m'a généré le certif je le rajoute via arv, ajouter , importer un certificat. Rien de particilier donc.
>> Je vous joindrai en privé, ma base sqlite. Mais de mon côté maintenant que mon infra tourne et que mes tunnels sont tous opérationnels, je ne pourrai pas faire des tests car tout est en production et fonctionnel.
>>
>> Cordialement,
>>
>> Le 27/01/2022 à 10:05, Fabrice Barconnière a écrit :
>>> Bonjour,
>>>
>>> Pouvez-vous m'indiquer les étapes d'installation et de configuration du serveur Sphynx et le mode d'importation des certificats pour que j'essaie de comprendre comment on arrive à cette situation ?
>>>
>>> - Image ISO utilisée
>>> - Enregistrement Zéphir ou non
>>> - Peut-être en privé, me fournir la base ARV (/var/lib/arv/db/sphynxdb.sqlite)
>>>
>>> Le 27/01/2022 à 08:01, Dominique Jassin a écrit :
>>>
>>>> Bonjour,
>>>>
>>>> Alors de mon côté j'étais revenu en arrière et j'avais décommenté les lignes 277 et 278 et juste fait une modif sur la ligne 275 de /usr/lib/python2.7/dist-packages/arv/db/node.py
>>>>
>>>> root@eole-sphynx-3:/usr/lib/python2.7/dist-packages/arv/db# diff node.py node.py.ori
>>>> 275c275
>>>> <   cred_subject = bin_encoding("%s/CN=%s"%(suffix_cred, name))
>>>> ---
>>>> >   cred_subject = bin_encoding("{0}, CN = {1}".format(suffix_cred, name))
>>>>
>>>> De mémoire car j'ai fait ça en octobre, çela m'a permis de rajouter les 285 certificats sous format pem ce qui ne me dérangeait pas puisque je migrais au fil de l'eau mes amons (changement zephir, sphynx, renouvellement certif, modif routage sur mes infras etc) mais je crois que cela ne fonctionnait pas en pkcs12. A tester mais cela n'explique pas pourquoi je ne pouvais pas intégrer mes certifs au départ sur une fresh install effectivement.
>>>>
>>>> Cordialement,
>>>>
>>>> Le 26/01/2022 à 17:00, Guinet Benoit a écrit :
>>>>> Bonjour
>>>>>
>>>>> Je relance à mon tour, on a le même souci, sur un sphynx 2.7.2 à jour, impossible d'ajouter un certificat
>>>>>

>>>>> Quelqu'un a t il réussi à résoudre le problème , à le contourner ?
>>>>>
>>>>> J'ai créé le ticket https://dev-eole.ac-dijon.fr/issues/33725 , le pole peut il prendre en charge notre problème?
>>>>>
>>>>>
>>>>>
>>>>> Cordialement
>>>>>
>>>>> Benoit Guinet
>>>>> Rectorat de Grenoble
>>>>> DSI - Infra Réseaux Sites et Etablissements
>>>>>
>>>>>
>>>>>
>>>>> Le 11/10/21 13:11, Dominique Jassin <dominique.jassin@ac-lyon.fr> a écrit :
>>>>>>
>>>>>> Re,
>>>>>>
>>>>>> En commentant les deux lignes 277 et 278 du fichier /usr/lib/python2.7/dist-packages/arv/db/node.py, je peux rajouter mon certificat mais celui ci n'est pas disponible pour monter les tunnels. Ce qui m'intrigue c'est que ce certificat semble être encore dans un autre format que le signalement de Laurent Haeffele avec la disparition du / entre le dernier OU et le CN
>>>>>> Voici ma sortie:
>>>>>> root@eole-sphynx-3:~# sqlite3 /var/lib/arv/db/sphynxdb.sqlite "select subject from arv_db_edge_credential ;"
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015, CN = 0010005A-01.ac-lyon.fr
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=0010002X-01.ac-lyon.fr
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=0690133V-01.ac-lyon.fr
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=0690133V-02.ac-lyon.fr
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=AGRIATES-LYON-27.ac-lyon.fr
>>>>>> C = FR, L = Lyon, O = Education Nationale, OU = Academie de Lyon, OU = 0002 110043015/CN=sphynx
>>>>>> C = FR, O = Education Nationale, L = Lyon, OU = Academie de Lyon, OU = 0002 110043015/CN=CA-eole-sphynx-3-RVP
>>>>>> C = FR, O = Education Nationale, OU = 0002 110043015/CN=AC EN Scolarite et Formation
>>>>>> C = FR, O = Education Nationale, OU = 0002 110043015/CN=AC Education Nationale
>>>>>> C = FR, O = Ministere Education Nationale Enseignement Superieur Recherche/CN=AC Racine Ministere ENESR
>>>>>>
>>>>>> On voit bien que le dernier certif que j'essaie de rentrer à savoir le 0010005A-01.ac-lyon.fr (j'ai pu en commentant le fichier node.py) est sous un format différent ce qui est certainement la cause de mes soucis.
>>>>>> Une idée pour corriger ce format svp ???
>>>>>>
>>>>>> Cordialement,
>>>>>>
>>>>>>
>>>>>> Le 11/10/2021 à 10:45, Dominique Jassin a écrit :
>>>>>>>> Bonjour,
>>>>>>>>
>>>>>>>> Rebelote, aujourd'hui je n'arrive plus à rajouter des certifs dans mon sphynx 2.7.2 alors que cela marchait vendredi. Toujours le même message L'ac n'existe pas dans la base, ne peut ajouter le certificat.
>>>>>>>> Une idée ??? Pourtant rien n'a changé depuis vendredi, aucune mise à jour et sphynx à jour.
>>>>>>>>
>>>>>>>> Cordialement,
>>>>>>>>
>>>>>>>> Le 20/09/2021 à 12:23, Dominique Jassin a écrit :
>>>>>>>>>>> Bonjour,
>>>>>>>>>>>
>>>>>>>>>>> Merci beaucoup pour ces précisions ;) Bon je suis reparti sur une base vierge et tout fonctionne parfaitement maintenant, j'ai pu monter mes tunnels sécurisés.
>>>>>>>>>>>
>>>>>>>>>>> Cordialement,
>>>>>>>>>>>
>>>>>>>>>>> Le 20/09/2021 à 11:55, Fabrice Barconnière a écrit :
>>>>>>>>>>>>> Bonjour,
>>>>>>>>>>>>>>
>>>>>>>>>>>>> Le problème est lié au changement de version openssl fournit par Ubuntu sur EOLE 2.7. La sortie de la commande est différente entre la v1.0 et la v1.1 actuellement installée sur EOLE 2.7.
>>>>>>>>>>>>> Ce problème est géré par les correctifs lié à ce scénario : https://dev-eole.ac-dijon.fr/issues/28771

>>>>>>>>> Il y a certainement un cas qui n'est pas géré mais je n'ai pas trouvé.
>>>>>>>>> La solution à l'époque a été de downgrader le numéro de version "arv_dbb_version" dans la base ARV et de relancer l'upgrade à l'aide du script "posttemplate/00-arv"
>>>>>>>>>
>>>>>>>>> Le 20/09/2021 à 10:30, Dominique Jassin a écrit :
>>>>>>>>>> Bonjour,
>>>>>>>>>>
>>>>>>>>>> Bon j'ai résolu le problème en refaisant une fresh install, je pense que le problème venait de la réutilisation d'un id sphynx existant dans zephir avec les archives arv correspondantes. En repartant de zéro ça fonctionne, il me reste juste à refaire ma conf arv :(
>>>>>>>>>>
>>>>>>>>>> Cordialement,
>>>>>>>>>>
>>>>>>>>>> Le 17/09/2021 à 14:59, Dominique Jassin a écrit :
>>>>>>>>>>> Bonjour,
>>>>>>>>>>>
>>>>>>>>>>> Je relance ce vieux message car je tente d'installer un nouveau sphynx en version 2.7.2 et je tombe sur le même message. Ce qui est incompréhensible, c'est que j'ai bien pu intégrer le certificat PNCN pour le sphynx lui même et quand je veux mettre mon certif de test sur un amon, j'ai ce message alors que l'AC est évidemment la même. Dans ARV j'ai bien AC EN Scolarite et formation. J'ai bien enregistré mon serveur Sphynx sur Zephir et fait un init_sphynx. Une piste ?? Merci d'avance.
>>>>>>>>>>>
>>>>>>>>>>> Voici ce que j'ai dans /var/log/arv/error.log:
>>>>>>>>>>>
>>>>>>>>>>> Traceback (most recent call last):
>>>>>>>>>>>   File "/usr/lib/python2.7/dist-packages/arv/web/page.py", line 87, in render
>>>>>>>>>>>   ret = self.render_page(request)
>>>>>>>>>>>   File "/usr/lib/python2.7/dist-packages/arv/web/childpage.py", line 163, in render_page
>>>>>>>>>>>   node.import_credential(private_key=private_key, credential=public_key, passwd=password)
>>>>>>>>>>>   File "/usr/lib/python2.7/dist-packages/arv/lib/util.py", line 53, in newFunc
>>>>>>>>>>>   return func(*args, **kwargs)
>>>>>>>>>>>   File "/usr/lib/python2.7/dist-packages/arv/db/node.py", line 280, in import_credential
>>>>>>>>>>>   raise ValueError(str(e))
>>>>>>>>>>> ValueError: CA does not exists in database, Can't add certificate
>>>>>>>>>>>
>>>>>>>>>>> Cordialement,
>>>>>>>>>>>
>>>>>>>>>>> Le 23/07/2019 à 16:00, Benjamin Randrianarivony a écrit :
>>>>>>>>>>>> d'après les log :
>>>>>>>>>>>>
>>>>>>>>>>>> ce serait la ligne : "ca = Credential.query.filter_by(subject=cred_subject).first()"
>>>>>>>>>>>> dans la fonction "import_credential(self, private_key, credential, passwd,old_credential=None, old_ca=None)"
>>>>>>>>>>>> du script "/usr/lib/python2.7/dist-packages/arv/db/node.py" qui poserait pb ...
>>>>>>>>>>>>
>>>>>>>>>>>> Cordialement,
>>>>>>>>>>>>
>>>>>>>>>>>> Le 23/07/2019 à 15:40, Benjamin Randrianarivony a écrit :
>>>>>>>>>>>>> Bonjour,
>>>>>>>>>>>>>
>>>>>>>>>>>>> Nous renouvelons le certificat PNCN du sphynx 2.5.2.
>>>>>>>>>>>>>
>>>>>>>>>>>>> Dans l'interface ARV, quand on veut rajouter le pkcs7 cela plante en indiquant que l'AC n'existe pas dans la base.
>>>>>>>>>>>>>
>>>>>>>>>>>>> Est-ce quelqu'un a déjà eu le souci et nous indiquer comment solutionner, svp.
>>>>>>>>>>>>>
>>>>>>>>>>>>> Merci d'avance pour vos retours

#5 - 07/02/2022 13:37 - Fabrice Barconnière

- Statut changé de En cours à À valider

- % réalisé changé de 0 à 100

#6 - 07/02/2022 13:37 - Fabrice Barconnière

- Statut changé de À valider à Résolu

#7 - 10/02/2022 11:28 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0