

Distribution EOLE - Tâche #35935

Scénario # 35830 (Terminé (Sprint)): Le certificat Let's Encrypt ne sont pas reconnu à l'enregistrement_zephir

Suite à la dernière mise à jour certificat non valide

10/05/2024 10:27 - moncef ziani

Statut:	Fermé	Début:	10/05/2024
Priorité:	Normal	Echéance:	
Assigné à:	Joël Cuissinat	% réalisé:	100%
Version cible:	Livraison Cadoles 31/03/2024 (90)	Temps estimé:	0.00 heure
		Temps passé:	0.00 heure
Description			
Bonjour, Suite à la dernière mise à jour du zephir, notre serveur zephir, en version 2.9.0 n'est plus fonctionnel, cela n'est pas confortable car nous sommes en pleine migration de nos serveurs scribe en version 2.8. Le problème est la conséquence du certificat qui est déclaré comme non valide nous empêchant d'accéder à l'interface de gestion par le Web et empêchant par la même occasion le gestion de nos serveurs à distance. Dans le gencibfig apparaît un nouveau champ où l'on doit intégré le fichier contenant la chaîne et le certificat Si j'ai bien compris, la mise à jour ne devait concernait que les certificat Let's encrypt. Serait-il possible d'activer ce changement seulement pour Let's encrypt et par pour les autres types de certificats ? C'est une demande urgente car le serveur zephir qui est en production ne fonctionne plus et nous sommes bloqué dans nos migrations de serveur.			

Révisions associées

Révision c28970d8 - 13/05/2024 16:21 - Joël Cuissinat

Correction pb de certificat "manuel"

Ref: #35935

Révision f4d3cd9d - 06/06/2024 11:20 - Joël Cuissinat

Correction pb de certificat "manuel"

Ref: #35935

Historique

#1 - 13/05/2024 09:36 - Emmanuel GARETTE

Bonjour,

Je viens d'avoir le problème également avec un certificat "manuel".

Avec le dictionnaire suivant (a mettre par exemple dans /usr/share/eole/creole/dicos/local/02_certif.xml) je n'ai plus de problème :

```
<?xml version="1.0" encoding="utf-8"?>

<creole>
  <variables>
    <family name='général'>
      <variable name='server_full_chain_pem' redefine="True"/>
    </family>
  </variables>
  <constraints>
    <fill name='calc_multi_condition' target='server_full_chain_pem'>
      <param>letsencrypt</param>
      <param type='eole' name='condition_1'>cert_type</param>
      <param name='default_match'>/etc/ssl/certs/eole_fullchain.pem</param>
      <param name='mismatch' type="eole">server_cert</param>
    </fill>
  </constraints>
</creole>
```

```
</constraints>  
</creole>
```

#2 - 13/05/2024 10:49 - moncef ziani

Bonjour,

Merci pour votre réponse rapide.

Je viens de rajouter ce dico **02_certif.xml** dans **/usr/share/eole/creole/dicos/local/**

Suite au reconfigure cela plant le service **creole**

ci-dessous le log correspondant:

```
2024-05-13T10:40:37.640269+02:00 zephir.toutatice.fr creoled[466082]: creoled - Impossible de charger la configuration Creole.XML declaration allowed only at the start of the document, line 3, column 6 (02_certif.xml, line 3)
```

#3 - 13/05/2024 10:54 - Joël Cuissinat

- Assigné à mis à Joël Cuissinat

- Tâche parente mis à #35830

#4 - 13/05/2024 10:59 - Joël Cuissinat

Bonjour Moncef,

Ça ressemble à un pb de copier/coller du XML...

Il ne faut pas la ligne vide en début de fichier !

+ vérifier les éventuels caractères spéciaux qui auraient pu se glisser...

Dès que tu valides la correction, je prépare une diffusion rapide ;)

#5 - 13/05/2024 11:00 - Joël Cuissinat

- Statut changé de Nouveau à En cours

#6 - 13/05/2024 12:16 - moncef ziani

- Fichier Diagnose.png ajouté

- Fichier 00_certif.xml.png ajouté

- Fichier Gen_Config.png ajouté

Merci, j'ai été trop vite dans le copier/coller pour cette précision.

Le reconfigure va jusqu'à son terme.

Par contre pas d'évolution, toujours non opérationnel.

Ci joint trois captures:

-> résultat du diagnose

-> contenu du 00_certif.xml

-> Gen_config section certificats

#7 - 13/05/2024 12:56 - Laurent Gourvenec

Bonjour Moncef,

Le dico supplémentaire est là pour donner une valeur par défaut correcte à la nouvelle variable ("Chemin du fichier contenant le certificat SSL et la chaîne")

De ce que je lis de la capture d'écran de genconfig, vous avez dû modifier cette nouvelle variable à la main.

Pourriez-vous réinitialiser cette variable à sa valeur par défaut via genconfig ? Avec le dictionnaire en plus, cette valeur par défaut devrait être la valeur de la variable "Chemin du fichier contenant le certificat SSL" (/etc/ssl/certs/zephir_toutatice_fr.crt je suppose)

#8 - 13/05/2024 13:35 - moncef ziani

- Fichier Certif-ok-Diagnose-NOK.png ajouté

Bonjour Joël et Laurent,

C'est réglé pour l'accès au zephir et la prise en compte du certificat.

Un grand merci pour votre réactivité.

Par contre il est toujours vu comme invalide suite au diagnose.

Il reste des chose à ajuster au niveau du diagnose.

#9 - 13/05/2024 16:24 - Joël Cuissinat

=> eole-common 2.9.0-66

#10 - 14/05/2024 09:14 - Yoni Baude

Bonjour,

Suite à l'ajout du dico /usr/share/eole/creole/dicos/local/02_certif.xml et la modification de la variable server_full_chain_pem, notre zéphir 2.9 est de nouveau accessible en web.

```
*** Validité des certificats
Validité du certificat zephirpublic.crt
.          Certificat => OK
.          Chaîne => OK
.          Expiration => Fin de validité dans plus de 30 jours
.          DNS reconnus => zephirpublic.ac-caen.fr
.          Date de fin => dim. 16 févr. 2025 00:59:59 CET
.          CA => Sectigo RSA Organization Validation Secure Server CA
```

Seulement, nos Horus 2.6 ne peuvent plus récupérer leurs configurations :

```
-----
Préparation pour reconfigure
-----
```

```
Restart Systemd service creoled [ OK ]
```

Impossible de vérifier sur Zéphir les interdictions pour RECONFIGURE.

Message d'erreur : [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590)

Utilisation des paramètres en cache

Merci de votre aide,

Cordialement,

Yoni

#11 - 14/05/2024 13:42 - Yoni Baude

Problème de communication entre le zéphir et les horus résolu, il manquait la chaîne de certification sur le zéphir.
Merci
Yoni

#12 - 14/05/2024 14:59 - Joël Cuissinat

- Statut changé de En cours à À valider
- % réalisé changé de 0 à 100

#13 - 15/05/2024 14:48 - Joël Cuissinat

Publication maj corrective : <https://dev-eole.ac-dijon.fr/news/681>

#14 - 04/06/2024 16:11 - Laurent Gourvenec

- Projet changé de Zéphir à Distribution EOLE
- Statut changé de À valider à Résolu

#15 - 05/06/2024 10:28 - Joël Cuissinat

- Statut changé de Résolu à Fermé
- Restant à faire (heures) mis à 0.0

Fichiers

Diagnose.png	128 ko	13/05/2024	moncef ziani
00_certif.xml.png	53,2 ko	13/05/2024	moncef ziani
Gen_Config.png	139 ko	13/05/2024	moncef ziani
Certif-ok-Diagnose-NOK.png	109 ko	13/05/2024	moncef ziani