Distribution EOLE - Scénario #35264

Zephir 2.9 - Certificat => Invalide

01/03/2023 12:49 - Olivier FEBWIN

Statut:	Terminé (Sprint)	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	01/01/2024
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Livraison Cadoles 31/05/2023	**Temps passé:**	0.00 heure

Description

Erreur affichée par diagnose :

```
*** Validité des certificats
> Validité du certificat zephir2_ac-amiens_fr.pem
> .                  Certificat => Invalide
> .                      Chaîne => OK
> .                  Expiration => Fin de validité dans plus de 30 jours
> .                DNS reconnus => zephir2.ac-amiens.fr www.zephir2.ac-amiens.fr
> .               DNS superflus => www.zephir2.ac-amiens.fr
> .                  Date de fin => sam. 08 avril 2023 01:59:59 CEST
> .                           CA => GEANT OV RSA CA 4
>
```

Est-ce gênant ?

EOLE 2.9 :

- ~~ne pas considérer ce cas de figure comme une erreur~~
- ~~afficher les noms de domaine superflus en orange voir en blanc car il s'agit uniquement d'une information~~

Après discussion, il s'agit bien d'un cas d'erreur, il faudrait plutôt un message qui explique à l'utilisateur comment résoudre le problème.

Sous-tâches:

Tâche # 35379: Clarifier la démarche à suivre pour corriger le problème de validité du ...	**Fermé**
Tâche # 35385: Tester	**Fermé**

Historique

#1 - 01/03/2023 17:23 - Joël Cuissinat

C'est l'AC Sectigo (RENATER) qui ajoute un www en "Noms alternatifs du sujet"

#2 - 01/03/2023 18:05 - Joël Cuissinat

Dans notre infra, j'arrive à reproduire quelque chose qui s'en rapproche :

- [redacted]
  `www.zephir.ac-test.fr"`

- instance / re-génération du certificat (autosigné)
- diagnose OK

```
.                  Certificat => OK
.                      Chaîne => OK
.                   Expiration => Fin de validité dans plus de 30 jours
.                 DNS reconnus => zephir.ac-test.fr www.zephir.ac-test.fr
.                  Date de fin => dim. 01 mars 2026 17:37:04 CET
.                           CA => CA-zephir.ac-test.fr
```

- [redacted]

- diagnose KO

```
.                  Certificat => Invalide
.                      Chaîne => OK
.                   Expiration => Fin de validité dans plus de 30 jours
.                 DNS reconnus => zephir.ac-test.fr www.zephir.ac-test.fr
.                DNS superflus => www.zephir.ac-test.fr
.                  Date de fin => dim. 01 mars 2026 17:37:04 CET
.                           CA => CA-zephir.ac-test.fr
```

#3 - 02/03/2023 09:06 - Joël Cuissinat

Ajouter les domaines "superflus" dans "Nom DNS alternatif du serveur" (ssl_subjectaltname) permet bien de faire disparaître l'erreur, ceci dit, ce cas de figure ne devrait pas faire remonter une erreur mais juste une information...

→ ne pas considérer ce cas de figure comme une erreur
→ afficher les noms de domaine superflus en orange voir en blanc car il s'agit uniquement d'une information

#4 - 02/03/2023 09:13 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Début 01/03/2023 supprimé

- Release mis à EOLE 2.9.0

#5 - 14/03/2023 11:53 - Joël Cuissinat

- Points de scénarios mis à 1.0

#6 - 20/03/2023 11:30 - Joël Cuissinat

- Release changé de EOLE 2.9.0 à EOLE 2.8.0.1

#7 - 20/03/2023 11:30 - Joël Cuissinat

- Release changé de EOLE 2.8.0.1 à Carnet de produit (Cadoles)

#8 - 20/03/2023 11:34 - Joël Cuissinat

- Description mis à jour

#9 - 25/04/2023 08:52 - Benjamin Bohard

De mon point de vue, le certificat ne devrait être valide que pour des noms de domaines définis et le script ne devrait pas faire de déduction intelligente sur les exceptions à faire.

Dans le cas où la présence de noms de domaine superflus n'est pas remonté en erreur, l'utilisation du certificat pour un autre site que les sites déclarés rend ce site aussi légitime que les sites déclarés, sans que l'administrateur n'en soit clairement averti (par l'erreur).

Dans le cas présent où le nom superflu est accepté par l'administrateur, il me semble plus judicieux que l'administrateur ajoute ce nom dans la configuration.

Dans l'idéal, on devrait avoir un certificat par usage (identification machine, services), ce qui limiterait la nécessité d'avoir une multiplication des noms alternatifs dans un certificat.

#10 - 25/04/2023 08:53 - Benjamin Bohard

- Echéance mis à 01/01/2024

- Assigné à mis à Benjamin Bohard

- Version cible mis à Carnet Cadoles

- Début mis à 01/10/2022

#11 - 04/05/2023 14:43 - Joël Cuissinat

```
<febcrash> pour https://dev-eole.ac-dijon.fr/issues/35264#note-9 ce n'est pas gênant puisqu'on peut corriger c
ette erreur en ajoutant le nom alternatif
```

Proposition : dans le diagnose, ajouter une ligne suggérant de l'ajouter aux noms DNS alernatifs.

#12 - 05/05/2023 16:02 - Joël Cuissinat

- Description mis à jour

#13 - 05/05/2023 16:04 - Joël Cuissinat

- Description mis à jour

#14 - 11/05/2023 15:34 - Ludwig Seys

- Statut changé de Nouveau à Résolu

#15 - 12/05/2023 18:14 - Joël Cuissinat

- Statut changé de Résolu à Terminé (Sprint)

- Version cible changé de Carnet Cadoles à Livraison Cadoles 31/05/2023

- Release changé de Carnet de produit (Cadoles) à EOLE 2.8.1