Distribution EOLE - Scénario #15927

Étudier la gestion des certificats sur 2.6

04/18/2016 03:53 PM - Joël Cuissinat

Status:	Terminé (Sprint)	**Start date:**	03/29/2016
Priority:	Normal	**Due date:**	05/26/2016
Assigned To:	force indigo	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	sprint 2016 19-21 - Equipe MENESR	**Spent time:**	13.33 hours

Description

Pistes de travail :

- droits appliqués sur les fichiers (600)
- contenu de la requête :
  - bannir les IP/nom
  - vérifier les CN et les altname
- maquette OCSP/CRL
- certificats auto-signés :
  - génération aléatoire su serial id
  - plus de certificat auto-signé à terme

Subtasks:

Tâche # 15676: Étudier les problèmes de communication entre ead-server et ead-web	**Fermé**
Tâche # 15948: Étudier la possibilité de ne plus générer de certificat auto signé	**Fermé**
Tâche # 15950: Bannir les IP des alterateName	**Fermé**
Tâche # 15951: Tester letsencrypt	**Fermé**
Tâche # 15949: Générer des serialId aléatoires	**Ne sera pas résolu**
Tâche # 16158: le numero de serie des ceritificats devrait etre unique	**Fermé**

History

#1 - 04/18/2016 04:03 PM - Joël Cuissinat

- Description updated

- Story points set to 8.0

#2 - 05/04/2016 03:30 PM - Joël Cuissinat

- Target version changed from sprint 2016 16-18 - Equipe MENESR to sprint 2016 19-21 - Equipe MENESR

#3 - 05/09/2016 02:20 PM - Joël Cuissinat

- Assigned To changed from force orange to force indigo

#4 - 05/23/2016 01:37 PM - Philippe Caseiro

La problématique des certificats est fortement liée au problème du nommage de la machine.

Aujourd'hui sur un serveur scribe il est possible que la machine ai jusqu'a 3 noms :

1. Nom de domaine local : scribe.etb1.lan
2. Nom de domaine public : scribe.ac-test.fr
3. Web url : etb1.ac-test.fr

Ce mode de fonctionnement est incompatible avec la gestion des certificats "modernes".

Le problème est qu'il n'est pas possible de produire un certificat "valide" pour tous les noms.
Les services comme l'EAD utilisent 127.0.0.1 ce qui deviens également impossible, du coup comment déterminer quel nom utiliser pour la communication entre le backend et le frontend, pareil pour zephir, ou tous les services EOLE qui utilisent le principe "frontend/backend".

Il y a deux approches pour "résoudre" ce problème :

1. Le nom unique ! la machine a un et un seul nom resolvable depuis n'importe ou

(interieur/extérieur).
2. Le domaine unique et un nom par service (imap, sso, ead, services web ...) et les noms en question doivent être résolvables depuis n'importe ou (intérieur/extérieur).

Les deux solutions sont très proches, et compatibles avec 'Let's Encrypt' si les domaines sont publics.

En l'état actuel des choses il est très difficile d'apporter une solution sans remettre en question nos méthodes dans la gestion des noms de machines et de génération de certificats.

#5 - 05/30/2016 02:10 PM - Fabrice Barconnière

- Status changed from Nouveau to Terminé (Sprint)