Hobo - Bug #26141

"race condition" sur la création d'un tenant puis la mise à dispo de la clé SAML

05 septembre 2018 15:52 - Thomas Noël

Statut:	Fermé	**Début:**	05 septembre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	

Description

Quand on déploie un site, via hobo_deploy :

- on créé le tenant
- puis on ajoute les clés SAML dessus

Entre ces deux moments, si hobo ou Authentic vient chercher les métadonnées, celle ci ne contiennent pas encore la clé publique. Et comme mellon fait un cache, les métadonnées ne contiennent plus jamais la clé publique.

Selon le code de hobo_deploy, difficile de changer l'ordre des choses. En revanche, peut-être qu'on pourrait faire en sorte que mellon réponde 404 sur les metadonnées tant que la clé publique n'est pas générée ? (et oui, ça serait donc un ticket pour mellon dans ce cas, mais je pose la question ici quand même)

Demandes liées:

Lié à django-mellon - Development #26143: ne pas faire de cache des métadonné...	**Fermé**	**05 septembre 2018**
Dupliqué par Publik - Bug #26142: Certificat manquant dans les métadonnés de ...	**Rejeté**	**05 septembre 2018**

Historique

#1 - 05 septembre 2018 15:53 - Thomas Noël

note: expérience vécue par Emmanuel sur des déploiements via devinst, particulièrement depuis le passage à Django 1.11 qui joue les migrations bien plus rapidement.

#2 - 05 septembre 2018 15:54 - Thomas Noël

- Tracker changé de Support à Bug

#3 - 05 septembre 2018 16:08 - Frédéric Péters

Mmm, et simplement modifier le check_operational d'authentic, pour vérifier la disponibilité de metadata, plutôt que la réponse à /manage/users/ ?

Différemment, ajouter un --disabled à la commande create_tenant, qui poserait un marqueur quelconque dans le répertoire, pour laisser le temps au reste de l'hobo_deploy de s'exécuter puis retirer ce marqueur.

#4 - 05 septembre 2018 16:40 - Emmanuel Cazenave

- Dupliqué par Bug #26142: Certificat manquant dans les métadonnés de mellon après un déploiement ajouté

#5 - 05 septembre 2018 16:42 - Frédéric Péters

> Mmm, et simplement modifier le check_operational d'authentic, pour vérifier la disponibilité de metadata, plutôt que la réponse à /manage/users/ ?

Je relis mieux (avec l'aide de l'autre ticket), et c'est dans l'autre sens, métadonnées exposées par les applications.

#6 - 05 septembre 2018 16:43 - Frédéric Péters

Du coup, à mon sens, c'est tout à fait inutile de faire un cache de cette info et ça pourrait être dégagé de mellon.

#7 - 05 septembre 2018 16:44 - Emmanuel Cazenave

Side note : pas réussi à confirmer l'hypothèse de Thomas (qui semble raisonnable), depuis qu'il m'a pointé cette possibilité, comme par hasard je n'arrive plus à reproduire, très pénible ce truc.

#8 - 05 septembre 2018 16:50 - Frédéric Péters

- Lié à Development #26143: ne pas faire de cache des métadonnées locales ajouté

#9 - 05 septembre 2018 16:51 - Thomas Noël

Emmanuel Cazenave a écrit :

> Side note : pas réussi à confirmer l'hypothèse de Thomas (qui semble raisonnable), depuis qu'il m'a pointé cette possibilité, comme par hasard je n'arrive plus à reproduire, très pénible ce truc.

Race condition, plutôt difficile à reproduire, c'est sûr... Surtout qu'on est sur du cache par workers, donc en "vraie" prod, c'est plutôt rare.

Pour ma part, le cache dans le settings._TRUC fait par mellon, je l'aime pas beaucoup non plus, je serais pour le supprimer. Cependant mellon diffusera encore pendant quelques instants des metadonnées erronnées (sans clés publiques) et c'est pas top. Je me demande dans quel cadre un SP SAML peut avoir des metadata sans clé publique ? (auquel cas je préférerais que mellon réponde 404, quitte à avoir un "METADATA_WITHOUT_PUBLIC_KEY = True" possible dans les settings -- qu'on utilisera jamais nous)

#10 - 07 septembre 2018 13:42 - Emmanuel Cazenave

- Statut changé de Nouveau à Fermé

Plus d'occurrence chez moi depuis #26143.

#11 - 07 septembre 2018 15:20 - Benjamin Dauvergne

A défaut de gérer ça au niveau de mellon on pourrait modifier le check de validation de hobo pour qu'il pointe sur /mellon/metadata (ou qu'on ajoute cette URL à celles qui sont vérifiés en plus de la première URL de backoffice déclarée) et vérifier que ça contient bien une clé publique. Si je me souviens bien dès qu'un service devient opérationnel un message de déploiement est relancé (ou alors j'ai rêvé).