Hobo - Development #6476

commande management hobo_deploy pour authentic (hobo.agent.authentic2)

11 février 2015 17:46 - Serghei Mihai

Statut:	Fermé	**Début:**	11 février 2015
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

ne contient que la commande de management hobo_deploy dédiée au déploiement d'un tenant authentic2 :

- create_tenant
- création de la bi-clé SAML dans le tenant (saml.crt, saml.key)
- copie du hobo.json reçu dans tenant/www.example.net/hobo.json
- ajout des policies par défaut
- download des metadonnées dans federation.xml
- sync-metadata de federation.xml
  Cette application est à ajouter dans le INSTALLED_APPS (ou SHARED_APPS) d'authentic2 pour lui donner cette commande hobo_deploy

Révisions associées

Révision 81b2e465 - 12 février 2015 10:19 - Serghei Mihai

agent: add authentic deployment agent (#6476)

Révision df501fe2 - 12 février 2015 19:56 - Serghei Mihai

agent: add authentic deployment agent (#6476)

Révision 32718e35 - 13 février 2015 11:49 - Serghei Mihai

agent: add authentic deployment agent (#6476)

Historique

#1 - 11 février 2015 17:49 - Serghei Mihai

- Fichier 0001-authentic-deployment-command.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

La commande ne fait pas l'ajout d'une policy par défaut.
Cette action nécessite la création d'une policy dans authentic et ensuite son utilisation dans la liste des SP

#2 - 11 février 2015 18:06 - Frédéric Péters

Toute la partie commune avec le code dans hobo/agent/common/... je ne la dupliquerais pas ici; plutôt, je ferais hériter cette commande de l'autre. Si on veut éviter que ne s'ajoute un idp-metadata-x.xml inutile dans le cas d'Authentic, la commande d'origine peut être subdivisée en méthodes.

C'est important, sans ça les commandes vont rapidement se trouver désynchronisées (pour tout dire, c'est déjà le cas).

```
        tenant = TenantMiddleware.get_tenant_by_hostname(hostname)
        with tenant_context(tenant):
```

Ça ne me semble servir à rien.

```
            for service in environment['services']:
                if service['service-id'] != ME:
                    meta_files_urls.append(service['saml-sp-metadata-url'])
```

Plutôt que cette condition, je ferais un if not service.get('saml-sp-metadata-url'): continue

```
            for meta_file_url in meta_files_urls:
```

On bouclait déjà juste au-dessus sur la liste des services, le boulot de cette boucle pourrait s'y trouver.

```
            if os.path.exists(federation_file):
                meta = file(federation_file).read()
                if meta != entities:
                    replace_file(federation_file, entities)
                    call_command('sync-metadata', federation_file, source='hobo')
            else:
                replace_file(federation_file, entities)
                call_command('sync-metadata', federation_file, source='hobo')
```

Je comprends la volonté de ne pas appeler sync-metadata si rien n'a changé mais ça ne vaut pas pour moi la multiplication par 4 du nombre de lignes.

#3 - 11 février 2015 18:09 - Frédéric Péters

> La commande ne fait pas l'ajout d'une policy par défaut.
> Cette action nécessite la création d'une policy dans authentic et ensuite son utilisation dans la liste des SP

L'idée importante c'est quand même de déployer un service et qu'il soit fonctionnel immédiatement, pas de demander à l'administrateur de se rappeler qu'il doit aller modifier des choses dans authentic, ce serait donc bien que tout le nécessaire soit fait.

#4 - 11 février 2015 21:10 - Serghei Mihai

- Fichier 0001-deploy-agents-refactoring-6476.patch ajouté

J'ai divisé la commande basique afin de permettre aux commandes l'heritant d'implementer leurs actions spécifiques.

Je rajoute également la politique par défaut pour les SP qui distribue les attributs nécessaires à MELLON

#5 - 11 février 2015 21:29 - Frédéric Péters

Il y a suppression non-justifée de :

```
       # add an attribute to current tenant for easier retrieval
       me['this'] = True
```

Et puis surtout je trouve que ça ne va pas du tout d'avoir des patchs qui font tout en un, l'ajout d'un agent authentic, l'ajout de générations de clés pour les SP (mais pas la modification au middleware de paramétrage de mellon pour les utiliser), du refactoring, etc.

Bref, je vais reprendre des éléments de ce patch, adapter le agent/common/management/commands/hobo_deploy.py, pousser ça dans la branche, et laisser ce ticket pour l'agent authentic.

#6 - 11 février 2015 22:05 - Frédéric Péters

Voilà, j'ai ajouté ça dans la branche sous forme de trois commits :

```
commit 6034ef27ca1651a6b357f0facd96b6d95f6644d2
Author: Serghei MIHAI <smihai@entrouvert.com>
Date:   Wed Feb 11 17:47:41 2015 +0100

    agent: add authentic deployment agent (#6476)

commit 6b3a3904b50fa7b9768427cc0eb98f131d40574b
Author: Serghei MIHAI <smihai@entrouvert.com>
Date:   Wed Feb 11 21:47:34 2015 +0100

    agent: move sso configuration to its own method

    The configuration code for SSO is common to all service providers but can be
    skipped in the authentic agent, making it its own method makes this possible.

commit c7f34452deba7442209c53c80bcea8133859cf9d
Author: Serghei MIHAI <smihai@entrouvert.com>
Date:   Wed Feb 11 21:39:46 2015 +0100

    move tenant directory layout knowledge into tenant model
```

Par rapport au contenu du patch, dans une première lecture j'avais cru que le code de génération de clé était dans le code commun parce qu'utilisé également pour les SP, ce n'était pas le cas, j'ai donc mis ce code du côté de l'authentic. Il sera temps de le déplacer quand il sera utile ailleurs.

J'ai renommé le "def deploy()" en "def deploy_specifics()", avec un commentaire, et la configuration des SP dans une autre méthode.

J'ai laissé le "me['this'] = True", n'ayant pas d'explication sur son retrait (et ayant expliqué dans le message de commit le pourquoi de son existence).

J'ai aussi laissé le "return" quand le timestamp n'a pas changé, ne comprenant pas là non plus son retrait.

Je n'ai pas testé le déploiement d'un authentic pour de vrai.

#7 - 11 février 2015 22:20 - Frédéric Péters

Élément qu'on a oublié dans le déploiement de l'authentic : la création d'un premier utilisateur avec les infos du json.

```
  "users": [
    {
      "username": "fred",
      "first_name": "",
      "password": "pbkdf2_sha256$12000$IMhPJgdW40BT$4WgLn4ZdZF8Jb0eEsHCOrwj3vBKOdvNZ5aTR6Yc59ZU=",
      "email": "fpeters@entrouvert.com",
      "last_name": ""
    }
```

#8 - 12 février 2015 11:16 - Thomas Noël

Frédéric Péters a écrit :

> J'ai laissé le "me['this'] = True", n'ayant pas d'explication sur son retrait (et ayant expliqué dans le message de commit le pourquoi de son existence).

Ça avait été retiré à ma demande, j'avais pas compris à quoi c'était destiné (utilisé nulle part ailleurs, ou alors j'ai raté un truc ?).

> J'ai aussi laissé le "return" quand le timestamp n'a pas changé, ne comprenant pas là non plus son retrait.

Idem, fait à ma demande aussi : ce n'est pas parce que les services ont toujours la même URL que leur metadonnées n'ont pas changé (clés publiques SAML). C'est la seule raison. Donc, ok pour le return, il faut juste se souvenir de forcer les mises à jour "à la main" quand une clé change dans la fédération.

#9 - 12 février 2015 11:35 - Frédéric Péters

> Ça avait été retiré à ma demande, j'avais pas compris à quoi c'était destiné (utilisé nulle part ailleurs, ou alors j'ai raté un truc ?).

C'est expliqué dans le commit qui l'ajoute, même si ce n'est pas utilisé par la suite (je voulais l'utiliser pour les template_vars puis je me suis dit que je n'allais y ajouter que les variables globales) :

```
    The tenants are using domain names but the native hobo json file has base_url
    (scheme + domain name + port); an attribute is added to mark the current
    tenant, to avoid having to run urlparse everytime.
```

#10 - 13 février 2015 11:52 - Frédéric Péters

- Statut changé de En cours à Résolu (à déployer)

Branche wip/hobo_deploy intégrée dans master.

#11 - 09 novembre 2015 12:19 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-authentic-deployment-command.patch	4,75 ko	11 février 2015	Serghei Mihai
0001-deploy-agents-refactoring-6476.patch	8,63 ko	11 février 2015	Serghei Mihai