Hobo - Development #35168

provisioning des users: ne diffuser que les rôles liés à l'ou cible

31 juillet 2019 21:40 - Thomas Noël

Statut:	Fermé	**Début:**	31 juillet 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Actuellement lors du provisionning d'un utilisateur, on construit ainsi le JSON à envoyer en hobo_notify :

```
            def user_to_json(service, user, user_roles):
                from authentic2.api_views import BaseUserSerializer
                data = {}
                roles = user.roles_and_parents().prefetch_related('attributes')                dat
a.update({
                    'uuid': user.uuid,
                    'username': user.username,
                    'first_name': user.first_name,
                    'last_name': user.last_name,
                    'email': user.email,
                    'roles': [
                        {
                            'uuid': role.uuid,
                            'name': role.name,
                            'slug': role.slug,
                        } for role in roles],
                })
```

Autrement dit, on envoie absolument tous les rôles de l'utilisateur.

Mais en fait, le notify_agents qui utilise ces données est destiné à une certaine OU (depuis laquelle est calculée l'audience) :

```
                for ou, users in ous.iteritems():
                    ...
                    notify_agents({
                        '@type': 'provision',
                        'issuer': issuer,
                        'audience': audience,
                        'full': False,
                        'objects': {
                            '@type': 'user',
                            'data': [user_to_json(None, user, user_roles) for user in users],
                        }
                    })
```

On pourrait donc envoyer l'ou à user_to_json, et ainsi filtrer les rôles envoyés :

- ne prendre que les rôles de ou=None et l'ou concernée
- retirer ceux dont le slug commence par "_" (puisque de toute façon notify_roles ne les envoie jamais)

Ainsi, on ne risque pas d'envoyer un rôle de l'OU X vers des services de l'OU Y.

Demandes liées:

Lié à w.c.s. - Bug #35158: hobo_notify: le provisionning des rôles se base au...	**Fermé**	**31 juillet 2019**

Révisions associées

Révision 83ee68e2 - 06 août 2019 11:50 - Benjamin Dauvergne

provisioning: only send user's roles visible by the service (#35168)

Historique

#1 - 31 juillet 2019 21:41 - Thomas Noël

- Tracker changé de Support à Development

Je pose ça comme un dev, mais en fait c'est aussi un peu un bogue je pense. Les rôle d'une certaine OU ne doivent, je pense, jamais être connus dans une autre OU.

#2 - 31 juillet 2019 21:41 - Thomas Noël

- Lié à Bug #35158: hobo_notify: le provisionning des rôles se base aussi sur les noms, mais ne devrait pas ajouté

#3 - 05 août 2019 16:43 - Serghei Mihai

- Sujet changé de provisioning des uers: ne diffuser que les rôles liés à l'ou cible à provisioning des users: ne diffuser que les rôles liés à l'ou cible

#4 - 06 août 2019 11:22 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#5 - 06 août 2019 11:27 - Benjamin Dauvergne

- Fichier 0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#6 - 06 août 2019 11:41 - Thomas Noël

Mmh... service peut être None quelques lignes plus bas, user_to_json(None, ...), donc ça ne va pas marcher.

Je pense qu'il faut aussi éliminer les roles dont le slug commence par "_"

J'avais commencé un patch bête-et-méchant en ajoutant l'ou cible à l'appel de user_to_json, mais je m'étais arrêté en tentant de comprendre user_roles et en me disant que je ratais quelque chose (ce qui semble être le cas), ceci dit ça semblait fonctionner :

```
@@ -98,10 +98,12 @@ class Provisionning(threading.local):
         issuer = unicode(self.get_entity_id())
         if mode == 'provision':

-            def user_to_json(service, user, user_roles):
+            def user_to_json(service, user, user_roles, ou):
                 from authentic2.api_views import BaseUserSerializer
                 data = {}
                 roles = user.roles_and_parents().prefetch_related('attributes')
+                roles = set([role for role in roles
+                             if not role.slug.startswith('_') and (role.ou == ou or not role.ou)])
                 data.update({
                     'uuid': user.uuid,
                     'username': user.username,
@@ -166,7 +168,7 @@ class Provisionning(threading.local):
                                 'full': False,
                                 'objects': {
                                     '@type': 'user',
-                                    'data': [user_to_json(service, user, user_roles)],
+                                    'data': [user_to_json(service, user, user_roles, ou)],
                                 }
                             })
             else:
@@ -183,7 +185,7 @@ class Provisionning(threading.local):
                         'full': False,
                         'objects': {
                             '@type': 'user',
-                            'data': [user_to_json(None, user, user_roles) for user in users],
+                            'data': [user_to_json(None, user, user_roles, ou) for user in users],
                         }
                     })
         elif users:
```

#7 - 06 août 2019 11:47 - Benjamin Dauvergne

- Fichier 0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch ajouté

Je ne prenais pas en compte le cas où l'argument service était à None dans user_to_json, là je rajoute un argument ou en premier qui sera toujours défini, de plus au lieu de requêter la liste des rôles une fois par utilisateur je réutilise user_roles.

#8 - 06 août 2019 11:50 - Benjamin Dauvergne

- Fichier 0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch ajouté

Avec filtrage des préfixes '_'.

#9 - 06 août 2019 13:53 - Thomas Noël

- Statut changé de Solution proposée à Solution validée

#10 - 06 août 2019 13:55 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

```
commit 83ee68e26a9e251ae4217c0a5be3331f3e9c7ed4
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Aug 6 11:26:28 2019 +0200

    provisioning: only send user's roles visible by the service (#35168)
```

#11 - 06 août 2019 16:15 - Frédéric Péters

- Statut changé de Résolu (à déployer) à Solution déployée

Fichiers

0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch	1,46 ko	06 août 2019	Benjamin Dauvergne
0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch	2,5 ko	06 août 2019	Benjamin Dauvergne
0001-provisioning-only-send-user-s-roles-visible-by-the-s.patch	2,29 ko	06 août 2019	Benjamin Dauvergne