w.c.s. - Development #9210

Quand l'idp contrôle les rôles les actions de workflow pour ajouter/soustraire un rôle doivent utiliser le web-service de l'IdP

04 décembre 2015 17:14 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	04 décembre 2015
Priorité:	Normal	**Echéance:**	30 décembre 2015
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	v1.35		
Patch proposed:	Oui	**Planning:**	

Description

Pour ajouter un rôle:

```
POST /api/user/<user.names_identifiers[0]>/<role.slug>/
```

renvoie toujours 201;

pour supprimer un rôle

```
DELETE /api/user/<user.names_identifiers[0]>/<role.slug>/
```

renvoie toujours 200

Demandes liées:

Lié à Publik - Project management #8006: Supprimer la création de rôles dans ...	**Fermé**	**03 août 2015**	**05 janvier 2016**

Révisions associées

Révision 790023bd - 19 février 2016 10:18 - Benjamin Dauvergne

add helper method to test if user attributes are IdP managed (#9210)

Révision 9d13b21b - 19 février 2016 10:18 - Benjamin Dauvergne

misc: add an http_delete_request helper function (#9210)

Révision 6772ebef - 19 février 2016 10:18 - Benjamin Dauvergne

wf/roles: handle case when user attributes are managed by the idp (#9210)

If the user's attributes are managed by an idp, we add/remove roles by calling
the idp role management web-services. It only works with authentic2.

Historique

#1 - 04 décembre 2015 17:14 - Benjamin Dauvergne

- Lié à Project management #8006: Supprimer la création de rôles dans w.c.s. ajouté

#2 - 05 décembre 2015 23:52 - Benjamin Dauvergne

- Fichier 0001-add-helper-method-to-test-if-user-attributes-are-IdP.patch ajouté

- Fichier 0002-misc-add-an-http_delete_request-helper-function-9210.patch ajouté

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

- Patch proposed changé de Non à Oui

Pas testé un brin, je ferai un test en déployant manuellement sur montpellier-dev avant de pousser.

#3 - 14 décembre 2015 14:12 - Benjamin Dauvergne

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

Testé à l'aide du workflow https://eservices-montpellier.dev.entrouvert.org/backoffice/workflows/27/status/2/, de la classe d'authentification du ticket

#8896 et de la configuration suivante dans /etc/authentic2-multitenant/config.py:

```
# Test REST Authentication

try:
    import hobo.rest_authentication
    REST_FRAMEWORK['DEFAULT_AUTHENTICATION_CLASSES'] += ('hobo.rest_authentication.PublikAuthentication',)
except ImportError:
    print 'Unable to install PublikAuthentication'
```

J'ai aussi mis en dur dans la classe PublikAuthentication la clé secrète employée par w.c.s. pour signer.

L'ajout/retrait du rôle "Alex Jany" au soumissionnaire du formulaire fonctionne, avec propagation jusqu'à w.c.s. dans les secondes qui suivent.

Le patch numéro 3 a été mis à jour avec la signature des URLs qui manquait.

#4 - 24 décembre 2015 15:56 - Frédéric Péters

s/is_idp_manage_user_attributes/is_idp_managing_user_attributes/ (ou does_idp_manage_user_attributes mais j'aime moins).

Même quand c'est le cas, on ne perdrait rien à quand même exécuter le code local.

#5 - 24 décembre 2015 15:58 - Frédéric Péters

Et peut-être même alors taper les appels HTTP en afterjob, pour ne pas perdre de temps.

#6 - 24 décembre 2015 15:59 - Thomas Noël

Frédéric Péters a écrit :

> Même quand c'est le cas, on ne perdrait rien à quand même exécuter le code local.

On gagnerait beaucoup (c'est instantané, si la présence du rôle est nécessaire aussitôt). En fait, il faut absolument le faire.

#7 - 24 décembre 2015 18:06 - Thomas Noël

- Echéance mis à 30 décembre 2015

- Statut changé de Nouveau à Information nécessaire

- Priorité changé de Normal à Haut

J'augmente la priorité parce que c'est une fonctionnalité nécessaire dans les workflows d'Alfortville.

(Je laisse non assigné cependant)

#8 - 24 décembre 2015 18:36 - Thomas Noël

- Statut changé de Information nécessaire à En cours

#9 - 27 décembre 2015 12:19 - Benjamin Dauvergne

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

J'ai pris en compte la remarque de Thomas concernant l'inconditionnalité de l'action locale.

Le diff entre l'ancien patch numéro 3 et le nouveau:

```
diff --git a/wcs/wf/roles.py b/wcs/wf/roles.py
index 4834fb9..0a5e200 100644
--- a/wcs/wf/roles.py
+++ b/wcs/wf/roles.py
@@ -76,10 +76,9 @@ class AddRoleWorkflowStatusItem(WorkflowStatusItem):
             # we can't work on anonymous or user_hash'ed forms
             return
         user = get_publisher().user_class.get(formdata.user_id)
+        self.perform_local(user, formdata)
         if user.name_identifiers and is_idp_manage_user_attributes():
             self.perform_idp(user, formdata)
-        else:
-            self.perform_local(user, formdata)
```

```
    def perform_local(self, user, formdata):
        if not user.roles:
```

#10 - 03 janvier 2016 15:00 - Thomas Noël

A priori tu as posté l'ancien patch. Sur le nouveau, il faut penser à laisser l'action locale sur le Remove aussi. Avec ça, c'est ack pour moi. (je laisse la main à Fred pour insister sur le s/is_idp_manage_user_attributes/is_idp_managing_user_attributes/ le cas échéant)

#11 - 04 janvier 2016 10:33 - Benjamin Dauvergne

- Fichier 0001-add-helper-method-to-test-if-user-attributes-are-IdP.patch ajouté

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

J'ai pris en compte la remarque de Fred sur le renommage et le after_job et aussi l'action locale (et oui j'avais posté le mauvais patch).

#12 - 04 janvier 2016 10:40 - Frédéric Péters

Dans 0003, c'est resté is_idp_manage_user_attributes.

#13 - 04 janvier 2016 10:43 - Benjamin Dauvergne

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

C'est dur la rentrée.

#14 - 04 janvier 2016 10:52 - Thomas Noël

Fallait pas prendre de congés.

Et donc, Ack pour moi.

#15 - 04 janvier 2016 10:59 - Frédéric Péters

```
Exception:
  type = '<type 'exceptions.AttributeError'>', value = ''module' object has no attribute 'urlquote''

Stack trace (most recent call first):
  File "/home/fred/src/eo/wcs/wcs/wf/roles.py", line 33, in roles_ws_url
    31     entity_id = idps.values()[0]['metadata']
    32     base_url = entity_id.split('idp/saml2/metadata')[0]
>   33     return urlparse.urljoin(base_url, '/api/roles/%s/members/%s/' % (urllib.urlquote(role_uuid),
    34                                                                      urllib.urlquote(user_uuid)))
    35
```

Et après ça il yaura le fait que "idps.values()[0]['metadata']" donne le nom du fichier avec les métadata, et pas les métadata.

Peut-être dès lors, pour ne pas creuser trop dans le SAML, simplement avoir un "Role Webservice URL", à l'instar du Registration URL (dans /settings/identification/idp/identities). (?)

#16 - 04 janvier 2016 14:31 - Benjamin Dauvergne

Frédéric Péters a écrit :

> [...]

C'est corrigé depuis le patch du 14 décembre.

> Et après ça il yaura le fait que "idps.values()[0]['metadata']" donne le nom du fichier avec les métadata, et pas les métadata.

Idem.

Je pense que tu as testé un vieux patch, le code actuel ressemble à cela:

```
    entity_id = idps.values()[0]['metadata_url']
    base_url = entity_id.split('idp/saml2/metadata')[0]
    url = urlparse.urljoin(base_url, '/api/roles/%s/members/%s/' % (urllib.quote(role_uuid),
                                                                    urllib.quote(user_uuid)))
```

#17 - 04 janvier 2016 16:33 - Frédéric Péters

En effet j'avais appliqué par mégarde un vieux patch.

Cela étant :

```
Exception:
  type = '<type 'exceptions.AttributeError'>', value = ''NoneType' object has no attribute 'get_server''

Stack trace (most recent call first):
  File "/home/fred/src/eo/wcs/wcs/wf/roles.py", line 43, in roles_ws_url
    41                                                                urllib.quote(user_uuid)))
    42     secret = get_secret(url)
>   43     orig = get_request().get_server().split(':')[0]
    44     url += '?orig=%s' % orig
    45     return sign_url(url, secret)
```

Et je n'aime guère le entity_id.split('idp/saml2/metadata')[0] (le "Registration URL" avait été créé pour ne pas dépendre des URL d'Authentic 2); mais je laisserai passer.

#18 - 04 janvier 2016 16:57 - Benjamin Dauvergne

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

J'ai sorti la construction de l'URL du after_job. Ne pas dépendre des URLs d'authentic2 ? Dans l'hypothèse ou quelqu'un serait ok pour implémenter le même web-service avec le même protocole de signature dans un autre logiciel qu'authentic2... si ça arrive on changera le code.

#19 - 04 janvier 2016 18:54 - Frédéric Péters

J'imagine maintenant une dépendance à #8896, non ?

```
[04/Jan/2016 18:48:06] "POST /api/roles/d100b3f981ef409f8a56d410e8573aeb/members/fred/?orig=auquo&algo=sha256&
timestamp=2016-01-04T17%3A48%3A06Z&nonce=3e2603f2cc9e4cd44fe765b722ff438c&signature=6UNsPjsJtOrkKvLm/TyT1kOTcx
gCxlyAeVK3UTqgfqU%3D HTTP/1.1" 401 58
```

#20 - 04 janvier 2016 20:30 - Benjamin Dauvergne

Oui, j'avais le secret espoir que #8896 soit intégré bien avant celui-ci :)

#21 - 04 février 2016 15:34 - Thomas Noël

- Version cible mis à v1.32

#22 - 04 février 2016 15:43 - Frédéric Péters

Pour le moment ça signe la requête vers authentic avec une clé tirée de [api-secrets]; afin que les choses soient claires, [api-secrets] devrait uniquement être utilisé pour la vérification des requêtes s'adressant à l'API de w.c.s.

Pour ça je propose d'intégrer le patch suivant dans le 0003; et puis derrière il faudra adapter le hobo_deploy pour créer et remplir la section [wscall-secrets].

#23 - 04 février 2016 16:01 - Benjamin Dauvergne

Manque le patch.

#24 - 04 février 2016 16:05 - Frédéric Péters

- Fichier 0001-fixup-9210.patch ajouté

#25 - 04 février 2016 16:12 - Benjamin Dauvergne

- Fichier 0003-wf-roles-handle-case-when-user-attributes-are-manage.patch ajouté

- Fichier 0004-populate-wscall-secrets-in-check_hobos-9210.patch ajouté

J'ai mis à jour le 0003 et j'ai crée un patch pour check_hobos pour remplir la section wscall-secrets.

#26 - 04 février 2016 16:52 - Frédéric Péters

Ça marche pour moi.

#27 - 04 février 2016 16:52 - Frédéric Péters

(cela étant je préfère qu'on attende que l'authentic avec l'authent rest framework publik se trouve en prod)

#28 - 04 février 2016 17:01 - Thomas Noël

- Version cible v1.32 supprimé

#30 - 12 février 2016 15:18 - Thomas Noël

- Version cible mis à v1.33

#31 - 16 février 2016 14:24 - Thomas Noël

- Version cible changé de v1.33 à v1.34

#32 - 19 février 2016 00:29 - Thomas Noël

- Version cible changé de v1.34 à v1.35

#33 - 19 février 2016 10:07 - Benjamin Dauvergne

Voilà l'authentification REST_FRAMEWORK est en prod:

```
In [1]: from django.conf import settings

In [2]: settings.REST_FRAMEWORK
Out[2]:
{'DEFAULT_AUTHENTICATION_CLASSES': ('rest_framework.authentication.BasicAuthentication',
  'rest_framework.authentication.SessionAuthentication',
  'hobo.rest_authentication.PublikAuthentication'),
 'DEFAULT_FILTER_BACKENDS': ('rest_framework.filters.DjangoFilterBackend',
  'rest_framework.filters.OrderingFilter'),
 'DEFAULT_PAGINATION_CLASS': 'rest_framework.pagination.LimitOffsetPagination',
 'DEFAULT_PERMISSION_CLASSES': ('rest_framework.permissions.IsAuthenticated',),
 'NON_FIELD_ERRORS_KEY': '__all__',
 'PAGE_SIZE': 10}
```

Je pousse ?

#34 - 19 février 2016 10:13 - Frédéric Péters

Yep, c'est ok pour moi.

#35 - 22 février 2016 09:25 - Thomas Noël

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

- Assigné à mis à Benjamin Dauvergne

- Priorité changé de Haut à Normal

```
commit 6772ebef00c10b135111188b14a38b53b2cbe075
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Dec 5 23:47:17 2015 +0100

    wf/roles: handle case when user attributes are managed by the idp (#9210)

    If the user's attributes are managed by an idp, we add/remove roles by calling
    the idp role management web-services. It only works with authentic2.

commit 9d13b21b69b7b515125e7494baefb22c8fe031d1
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Dec 5 23:33:53 2015 +0100

    misc: add an http_delete_request helper function (#9210)

commit 790023bd1190aa3478e748ff70917743d1e4677c
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Dec 4 17:35:47 2015 +0100

    add helper method to test if user attributes are IdP managed (#9210)
```

#36 - 04 avril 2016 10:10 - Thomas Noël

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0002-misc-add-an-http_delete_request-helper-function-9210.patch	898 octets	05 décembre 2015	Benjamin Dauvergne
0001-add-helper-method-to-test-if-user-attributes-are-IdP.patch	3,59 ko	05 décembre 2015	Benjamin Dauvergne
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,01 ko	05 décembre 2015	Benjamin Dauvergne

0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,35 ko	14 décembre 2015	Benjamin Dauvergne
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,35 ko	27 décembre 2015	Benjamin Dauvergne
0001-add-helper-method-to-test-if-user-attributes-are-IdP.patch	3,61 ko	04 janvier 2016	Benjamin Dauvergne
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,67 ko	04 janvier 2016	Benjamin Dauvergne
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,68 ko	04 janvier 2016	Benjamin Dauvergne
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	4,68 ko	04 janvier 2016	Benjamin Dauvergne
0001-fixup-9210.patch	2,15 ko	04 février 2016	Frédéric Péters
0003-wf-roles-handle-case-when-user-attributes-are-manage.patch	5,09 ko	04 février 2016	Benjamin Dauvergne
0004-populate-wscall-secrets-in-check_hobos-9210.patch	963 octets	04 février 2016	Benjamin Dauvergne