Authentic 2 - Development #15456

Contrôle d'accès au SSO basé sur les rôles

16 mars 2017 16:34 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	16 mars 2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Josué Kouka	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

- ajouter une méthode authentic2.models.Service.authorize(self, request) qui renvoie True
- ajouter dans le SSO SAML, OIDC et CAS un appel à authorize, si cela renvoie False affiche une page avec le template authentic2/unauthorized.html contenant dans le contexte l'objet service (LibertyProvider, OIDCClient ou authentic2_idp_cas.models.Service selon le cas) et par défaut un message You are not authorized to access this service, please contact your administrator. avec un lien de retour vers {% url 'auth_homepage' %}
- ajouter un champ M2M authentic2.models.Service.authorized_roles vers django_rbac.utils.get_role_model_name().
- ajouter un champ URL authentic2.models.Service.unauthorized_url nullable
- réécrire authentic2.models.Service.authorize pour renvoyer False si authorized_roles n'est pas vide et si l'utilisateur ne possède aucun des rôles (si ! authorized_roles.exists() alors renvoyer True)
- réécrire unauthorized.html pour utiliser unauthorized_url comme URL de retour si celle-ci est définie

Demandes liées:

Lié à Authentic 2 - Development #5262: Manage authorizations to connect to a ...	**Rejeté**	**12 août 2014**

Révisions associées

Révision 5b50795b - 02 juin 2017 14:46 - Josué Kouka

add redirect to unauthorized page function (#15456)

Révision f5749cd1 - 02 juin 2017 14:46 - Josué Kouka

add ServiceAccessMiddleware (#15456)

Révision fceb69f8 - 02 juin 2017 14:46 - Josué Kouka

add authorized roles and unauthorized url field to Service (#15456)

Révision 6b24c60a - 02 juin 2017 15:39 - Josué Kouka

cas: check if user is authorized through the client (#15456)

Révision 7d6a94de - 02 juin 2017 15:39 - Josué Kouka

oidc: check if user is authorized through the client (#15456)

Révision 5820d403 - 02 juin 2017 15:41 - Josué Kouka

saml2: check if user is authorized through the client (#15456)

Révision 2f28bcec - 02 juin 2017 15:41 - Josué Kouka

add front office management interface (#15456)

Révision 143bbb9b - 02 juin 2017 15:41 - Josué Kouka

manage sp federation only when allowed (#15456)

Historique

#1 - 17 mars 2017 14:14 - Josué Kouka

- Statut changé de Nouveau à En cours

#2 - 21 avril 2017 11:28 - Josué Kouka

- Patch proposed changé de Non à Oui

- Fichier 0004-cas-role-access-control-test.patch ajouté

- Fichier 0003-cas-check-if-user-is-authorized-through-the-client.patch ajouté

- Fichier 0002-add-redirect-to-unauthorized-page-function.patch ajouté

- Fichier 0001-add-authorized-roles-and-unauthorized-url-field-to-S.patch ajouté

- Fichier 0006-saml2-check-if-user-is-authorized-through-the-client.patch ajouté

- Fichier 0005-oidc-check-if-user-is-authorized-through-the-client.patch ajouté

En attendant que je finisse le test SAML, je voulais déja avoir un retour

#3 - 21 avril 2017 13:30 - Benjamin Dauvergne

Patch 0001:

Plutôt que request, je ne passerai que user à l'appel authorize pour l'instant (on pourra passer d'autres choses en paramètres supplémentaires si un jour on ajoute des autorisations d'un autre type, par IP par exemple).

Ça c'est un poil lent et faux aussi (ça ne prend pas en compte l'héritage), si tu enlèves le '+' au paramètre related_name de la propriété authorized_roles et que tu le renommes en 'authorized_services', on pourra écrire au lieu de :

```
        for role in self.authorized_roles.all():
            if request.user.roles.filter(uuid=role.uuid).exists():
                return True
```

plutôt

```
        if request.user.roles_and_parents().filter(authorized_services=self).exists():
            return True
```

Patch 0002:

Comme unauthorized_url peut-être nulle (ce qui est bien) plutôt prévoir un retour vers la homepage d'authentic dans ce cas. Ne pas appeler ça 'redirect_to_unautorized' puisque ça ne redirige rien, plutôt unauthorized_view().

(Je le place ici pour idée mais ça aurait été sympa de plutôt utiliser une exception comme ceci dans Service.authorize() raise PermissionDenied(service=service) et de gérer dans un middleware la conversation vers l'affichage d'une vue, ça simplifierait le code à juste un appel à Service.authorize(user=user))

Patch 0003:

Virer les corrections PEP8 aux espaces et sauts de ligne.

Le test d'autorisation devrait être fait avance le validate_ticket() sinon on peut contourner l'autorisation en passant soi même le numéro de ticket au service.
Le test manque aussi ligne 117, cas passant du SSO CAS quand on est déjà connecté.
Le mettrai aussi un test ligne 364 dans la vue de proxy CAS (un fois qu'on a trouvé le target_service, on compare avec l'utilisateur dans pgt.user).

Patch 0004:

Ok, même tests pour OIDC et SAML à faire.

Patch 0005:

À ce stade je ne changerai pas de comportement pour OIDC, on ne renvoie pas d'erreur au service OIDC, on affiche la même page que pour tout le monde. Si jamais on nous demandait de retournait l'erreur au service, je préfèrerai qu'on ajoute ça comme un choix possible (unauthorized_behaviour=return_to_service/show_error_page), mais on fera ça plus tard si le besoin se présente.

Patch 0006:

#4 - 03 mai 2017 13:39 - Frédéric Péters

- Lié à Development #5262: Manage authorizations to connect to a service provider ajouté

#5 - 04 mai 2017 16:30 - Frédéric Péters

Vite fait,

- du texte d'explication pour dire que la gestion des rôles sur l'écran d'un service, c'est pour de la gestion d'accès, et qu'aucun rôle = service ouvert
- quand on ajoute un rôle à un service, il apparait dans le tableau, quand on clique dessus, 404.

- crash au premier essai,
  - service.authorize(request) vs def authorize(self, user)
  - → 'WSGIRequest' object has no attribute 'roles_and_parents'
  - → ajouter des tests pour les services saml et oidc, pas uniquement cas.

#6 - 05 mai 2017 11:08 - Frédéric Péters

(nouvelle branche poussée par Josué, prenant en compte les remarques, sauf)

> du texte d'explication pour dire que la gestion des rôles sur l'écran d'un service, c'est pour de la gestion d'accès, et qu'aucun rôle = service ouvert
>
> Besoin de suggestions là-dessus ?
>
> - → ajouter des tests pour les services saml et oidc, pas uniquement cas.
>
> **et oidc**.

#7 - 05 mai 2017 11:13 - Josué Kouka

Frédéric Péters a écrit :

> (nouvelle branche poussée par Josué, prenant en compte les remarques, sauf)
>
> > du texte d'explication pour dire que la gestion des rôles sur l'écran d'un service, c'est pour de la gestion d'accès, et qu'aucun rôle = service ouvert
> >
> > Besoin de suggestions là-dessus ?
>
> Volontier.
>
> > - → ajouter des tests pour les services saml et oidc, pas uniquement cas.
> >
> > **et oidc**.

Je suis en train de le faire et j'ai une AssetionError sur un response.form.submit().follow() et je cherche le pourquoi.
D'ou l'absence dans la branche.

#8 - 05 mai 2017 11:59 - Serghei Mihai

Un message qui accompagne le AssertionError ou une trace?

#9 - 05 mai 2017 12:31 - Frédéric Péters

Aussi, Authentic affiche sur sa page d'accueil la liste des services avec des boutons de connexion, il faudrait en exclure les services auxquels l'usager n'a pas accès. (cette page n'est pas affichée en mode hobo/publik).

#10 - 10 mai 2017 16:13 - Frédéric Péters

Sur la page d'un service actuellement il y a déjà un tableau de rôles (qui serait les administrateurs du service); ce tableau a disparu.

#11 - 10 mai 2017 19:17 - Frédéric Péters

> Sur la page d'un service actuellement il y a déjà un tableau de rôles (qui serait les administrateurs du service); ce tableau a disparu.

Disparu/remplacé, par :

```
     def get_table_queryset(self):
-        return self.object.roles.all()
+        return self.object.authorized_services.all()
```

C'est peut-être compliqué avec la structure actuelle d'authentic d'avoir deux tableaux sur la même page, l'idée serait alors du coup d'avoir deux pages différentes, une avec les tableaux des rôles du service (object.roles) et l'autre les rôles autorisés à s'y connecter (object.authorized_services).

Au passage, vu que dans .authorized_services on n'a pas des services mais des rôles, c'est plutôt mal nommé.

#12 - 15 mai 2017 15:02 - Frédéric Péters

> Au passage, vu que dans .authorized_services on n'a pas des services mais des rôles, c'est plutôt mal nommé.

Reste d'actualité.

Le tableau vide affiche "aucun" alors que pour les rôles autorisés à se connecter, le tableau vide signifie "tout le monde", non ?

Maintenant qu'il y a deux tableaux sur la même page, il faudrait également ajouter un titre au-dessus du premier pour expliciter son contenu.

Le fonctionnement à deux tableaux, avec la recherche/filtre qui s'applique uniquement à un seul, c'est étrange. Ma préférence déjà exprimée de manière plus générale dans un autre ticket (#14452) ce serait une uniformisation des page du /manage/, page de vue qui affiche les infos, puis sous-pages pour d'autres aspects. À voir si on veut caler ça dans ce ticket aussi. (si ça n'est pas le cas il faudrait malgré tout arranger ça rapidement après).

Le message de la popup "Do you really want to remove role "XXX" from service "YYY" ?", il devrait être adapté au contrôle d'accès.

#13 - 16 mai 2017 07:36 - Frédéric Péters

> Aussi, Authentic affiche sur sa page d'accueil la liste des services avec des boutons de connexion, il faudrait en exclure les services auxquels l'usager n'a pas accès. (cette page n'est pas affichée en mode hobo/publik).

Toujours d'application.

#14 - 16 mai 2017 09:26 - Josué Kouka

- Fichier a2_federation_management.png ajouté

Frédéric Péters a écrit :

> > Aussi, Authentic affiche sur sa page d'accueil la liste des services avec des boutons de connexion, il faudrait en exclure les services auxquels l'usager n'a pas accès. (cette page n'est pas affichée en mode hobo/publik).
>
> Toujours d'application.

Je pensais que c'était la page /account/ ? (cf pj)
Le commit lié est celui ci
http://git.entrouvert.org/authentic.git/commit/?h=wip/access-control-15456&id=ec9897df2a9a2ea56c0469a6c9fdc3b1acb7587b

Je n'avais pas trouvé d'autre page que celle la, j'ai sûrement omis quelque chose

#15 - 16 mai 2017 09:33 - Frédéric Péters

"page d'accueil" → "/". Hobo pose A2_HOMEPAGE_URL pour une redirection donc on ne voit pas la page d'accueil; faut taper None dans ce paramètre de config pour la voir.

#16 - 16 mai 2017 11:47 - Josué Kouka

Frédéric Péters a écrit :

> "page d'accueil" → "/". Hobo pose A2_HOMEPAGE_URL pour une redirection donc on ne voit pas la page d'accueil; faut taper None dans ce paramètre de config pour la voir.

Merci.
Avec ce commit http://git.entrouvert.org/authentic.git/commit/?h=wip/access-control-15456&id=54af7540c5e60776caa787234b4b2b7d92a0e53f ça devrait etre bon normalement.

#17 - 17 mai 2017 15:04 - Frédéric Péters

(commentaire numéro 12 toujours d'application)

Sur le fond, aussi, je préférerais que ça soit tourné avec une fonction qui fasse la vérification d'accès, et dans les situations de contrôle d'accès que l'exception soit levée, plutôt que l'inverse avec l'exception tout le temps levée et une fonction de vérification d'accès basée dessus :

```
+def is_user_authorized(service, request):
+    try:
```

```
+         service.authorize(request.user)
+         return True
+     except ServiceAccessDenied:
+         return False
```

Et sur le style, il continue à y avoir quantité de chunks inutiles, notamment :

```
-     LibertySession, LibertyFederation,
+     LibertySession, LibertyFederation,

      http_method_names = ['get']
-
+
      def get(self, request):

+
+
 def test_invalid_request(oidc_settings, oidc_client, simple_user, app):
```

#18 - 17 mai 2017 15:38 - Benjamin Dauvergne

Josué Kouka a écrit :

> Frédéric Péters a écrit :
>
> > "page d'accueil" → "/". Hobo pose A2_HOMEPAGE_URL pour une redirection donc on ne voit pas la page d'accueil; faut taper None dans ce paramètre de config pour la voir.
>
> Merci.
> Avec ce commit http://git.entrouvert.org/authentic.git/commit/?h=wip/access-control-15456&id=54af7540c5e60776caa787234b4b2b7d92a0e53f ça devrait etre bon normalement.

La homepage est déjà très lente pour le cas d'usage "Fédération Renater" (des centaines de SPs), ça ne va pas arranger les choses. Sachant que c'est 95% du cas d'usage de cette page actuellement (on la voit aussi chez Vinci, mais il n'y a que quelques dizaines de SPs).

#19 - 17 mai 2017 16:35 - Benjamin Dauvergne

Et donc aussi parce je ne dois pas uniquement faire mes remarques en Jabber: on va garder les deux tableaux pour l'instant et ne pas prolonger ce ticket trop longtemps, par contre je suis pour inverser leur order, celui des autorisation devenant bien plus important.

Le premier pourrait donc s'appeler 'Roles of users allowed on this service' (c'est long mais c'est explicite et ça se traduit donc assez bien) et le deuxième 'Roles solely visible from this service'.

#20 - 18 mai 2017 01:01 - Josué Kouka

Branche mise à jour.

- Les titres des tableaux ont été mis à jour
- Il n'y a plus de filtrage des SP

#21 - 18 mai 2017 06:14 - Frédéric Péters

> Branche mise à jour.

Sans prendre en compte mes commentaires (quick check sur .authorised_services).

> Il n'y a plus de filtrage des SP

Je note mon regret.

#22 - 18 mai 2017 08:19 - Benjamin Dauvergne

Frédéric Péters a écrit :

> > Branche mise à jour.
>
> Sans prendre en compte mes commentaires (quick check sur .authorised_services).

> Il n'y a plus de filtrage des SP

Je note mon regret.

Je me suis mal exprimé, c'est lent comme c'est ici mais ça peut être plus rapide, il suffit d'intégrer le filtrage à la requête

```
qs = qs.filter(Q(authorized_services__isnull=True)|Q(authorized_services__in=user.roles_and_parents()))
```

idéalement plutôt que d'écrire ce code ici il faudrait une méthode authorized_for_user() sur le Manager du modèle Service, qu'on puisse modifier le code si de nouvelles conditions apparaissaient dans le futur.

#23 - 18 mai 2017 08:20 - Benjamin Dauvergne

Et je suis d'accord avec le fait que authorized_services c'est mal nommé.

#24 - 22 mai 2017 11:15 - Josué Kouka

La branches est mise à jour.

#25 - 22 mai 2017 14:08 - Benjamin Dauvergne

1. Typo: callback url when unathorized

2. context = {'callback_url': service.unauthorized_url or '/'} On est jamais sûr que '/' existe, utilise reverse('a2-homepage') à la place.

3. Merge raise ServiceAccessDenied when user not authorized (#15456) dans add authorized roles and unauthorized url field to Service et déplace add ServiceAccessMiddleware et add redirect to unauthorized page function (#15456) avant

4. correction de blancs/sauts de ligne inutiles dans cas: check if user is authorized through the client (#15456) (relire les patchs, git log -p), y en a d'autres, si tu peux repasser sur chaque commit (git rebase -i master), faire un git gui pour séparer ces modifications PEP8 et ensuite les rebaser toutes ensembles

Remarques assez cosmétiques, ça m'a l'air tout bon sinon.

#26 - 02 juin 2017 13:14 - Frédéric Péters

Parce que Josué a perdu l'adresse du redmine, je note ici que la branche a été mise à jour pour suivre les remarques de Benjamin. (je n'ai pour ma part pas vériifé).

#27 - 02 juin 2017 13:24 - Frédéric Péters

```
+    authorized_roles = models.ManyToManyField(
+        get_role_model_name(), verbose_name=_('authorized services'),
```

verbose_name pas modifié.

> 4. correction de blancs/sauts de ligne inutiles

Écrivais Benjamin et c'est toujours le cas.

#28 - 02 juin 2017 13:39 - Frédéric Péters

> Le tableau vide affiche "aucun" alors que pour les rôles autorisés à se connecter, le tableau vide signifie "tout le monde", non ?

Toujours d'application. S'il faut une suggestion, on pourrait par exemple mettre "Aucune restriction d'accès, tous les utilisateurs peuvent se connecter à ce service" ("No access restriction. All users are allowed to connect to this service.").

#29 - 06 juin 2017 09:31 - Benjamin Dauvergne

J'ai dit à Josué de pousser mais ta dernière remarque n'était pas traité il va poser un patch supplémentaire aussi.

#30 - 09 juin 2017 16:20 - Frédéric Péters

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

Benjamin Dauvergne a écrit :

> J'ai dit à Josué de pousser mais ta dernière remarque n'était pas traité il va poser un patch supplémentaire aussi.

Isolé dans #16795.

#31 - 06 décembre 2017 15:26 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0006-saml2-check-if-user-is-authorized-through-the-client.patch	2,04 ko	21 avril 2017	Josué Kouka
0005-oidc-check-if-user-is-authorized-through-the-client.patch	1,58 ko	21 avril 2017	Josué Kouka
0004-cas-role-access-control-test.patch	3,88 ko	21 avril 2017	Josué Kouka
0003-cas-check-if-user-is-authorized-through-the-client.patch	2,17 ko	21 avril 2017	Josué Kouka
0002-add-redirect-to-unauthorized-page-function.patch	1,79 ko	21 avril 2017	Josué Kouka
0001-add-authorized-roles-and-unauthorized-url-field-to-S.patch	3,03 ko	21 avril 2017	Josué Kouka
a2_federation_management.png	139 ko	16 mai 2017	Josué Kouka