Authentic 2 - Development #65942

idp_oidc : un client ayant accès à l'/api/users/ ne doit avoir accès qu'aux usagers s'étant déjà connecté chez lui

02 juin 2022 16:49 - Paul Marillonnet

Statut:	Fermé	**Début:**	02 juin 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Suite de #65877 ; mais aussi assez indépendamment, dans la situation actuelle où OIDCClient.has_api_access == True signifie que c'est open-bar.

Demandes liées:

Lié à Authentic 2 - Development #65877: idp_oidc : les hooks de l'api /users/...	**En cours**	**01 juin 2022**
Lié à Authentic 2 - Development #65943: idp_oidc : pour un usager donné, un ...	**En cours**	**02 juin 2022**
Lié à Authentic 2 - Development #66114: idp_oidc : effectuer systématiquement...	**Nouveau**	**09 juin 2022**

Révisions associées

Révision 2bf67721 - 02 mars 2023 09:38 - Paul Marillonnet

idp_oidc: restrict client's returned qs to authorized users (#65942)

Historique

#1 - 02 juin 2022 16:49 - Paul Marillonnet

- Lié à Development #65877: idp_oidc : les hooks de l'api /users/ doivent tenir compte de la résolution des claims lorsque l'appelant est un client oidc connu ajouté

#2 - 02 juin 2022 16:52 - Paul Marillonnet

- Lié à Development #65943: idp_oidc : pour un usager donné, un client ayant accès à l'/api/users/ ne doit voir que les informations d'identité auxquelles il a accès dans la configuration oidc ajouté

#3 - 02 juin 2022 18:06 - Paul Marillonnet

- Fichier 0001-idp_oidc-restrict-client-s-returned-qs-to-authorized.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#4 - 02 juin 2022 18:12 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

- Assigné à mis à Paul Marillonnet

Si le mode d'autorisation est par ou, l'autorisation est accrochée à l'ou pas au client et sur OU et OIDCClient tu as une GenericRelation 'oidc_authorizations' pour simplifier ta requête.

#5 - 03 juin 2022 11:43 - Paul Marillonnet

- Fichier 0001-idp_oidc-restrict-client-s-returned-qs-to-authorized.patch ajouté

- Statut changé de En cours à Solution proposée

Benjamin Dauvergne a écrit :

> Si le mode d'autorisation est par ou, l'autorisation est accrochée à l'ou pas au client et sur OU et OIDCClient tu as une GenericRelation 'oidc_authorizations' pour simplifier ta requête.

Bien vu, en effet c'est mieux comme ça.

#6 - 03 juin 2022 14:08 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Il faudrait garder le fastpath avant aussi.

#7 - 07 juin 2022 10:42 - Paul Marillonnet

J'ai l'impression que dans le cas général, Client.authorized_roles n'est pas défini. On se retrouve donc pris dans ce fastpath et le queryset n'est pas réduit.
Je peux adapter les tests pour définir authorized_roles sur la fixture oidc_client, mais je ne sais pas si ce sera représentatif de la réalité.

#8 - 09 juin 2022 17:26 - Paul Marillonnet

- Lié à Development #66114: idp_oidc : effectuer systématiquement la réduction des informations retournées à un client en fonction des autorisations qu'il possède ajouté

#9 - 20 juin 2022 09:51 - Paul Marillonnet

- Statut changé de En cours à Solution proposée

Je laisse en solution proposée en attendant, car je ne vois pas comment le fastpath peut arriver avant.

#10 - 25 juillet 2022 11:34 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

C'est ça que j'aurai aimé garder avant, pour voir clairement les cas où on ne touche à rien, ensuite avoir tout le spécifique OIDC / User.

```
        # fast path
        if not issubclass(qs.model, User):
            return qs
        client = ....
        if client is None:
            return qs
```

#11 - 02 mars 2023 09:33 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> C'est ça que j'aurai aimé garder avant, pour voir clairement les cas où on ne touche à rien, ensuite avoir tout le spécifique OIDC / User.
> [...]

Ok, simplement il y a le if client.authorized_roles.exists(): qui doit rester en dessous de la modification du queryset propre à ce ticket. Je vais pousser cette version en remontant le fastpath qui ne contiendra alors plus que

```
+        # fast path
+        if not issubclass(qs.model, User) or client is None:
+            return qs
+
```

#12 - 02 mars 2023 09:39 - Paul Marillonnet

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

```
commit 2bf67721b7731a124512f0ff01d9e67457af5065
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Jun 2 17:28:32 2022 +0200

    idp_oidc: restrict client's returned qs to authorized users (#65942)
```

#13 - 02 mars 2023 17:14 - Transition automatique

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

#14 - 07 mai 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-idp_oidc-restrict-client-s-returned-qs-to-authorized.patch	4,34 ko	02 juin 2022	Paul Marillonnet
0001-idp_oidc-restrict-client-s-returned-qs-to-authorized.patch	10,3 ko	03 juin 2022	Paul Marillonnet