

Plugin FS FranceConnect - Bug #45199

auth_fc: création d'un doublon même si un compte avec l'adresse mail envoyée par FC existe

16 juillet 2020 18:11 - Serghei Mihai

Statut:	Fermé	Début:	16 juillet 2020
Priorité:	Normal	Echéance:	
Assigné à:	Nicolas Roche	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Hors marché:	Non		
Patch proposed:	Oui		
Description			
Cas dans #45190.			
app_settings.A2_EMAIL_IS_UNIQUE et default_ou.email_is_unique sont toutes les deux à True. Pourtant un compte doublon a été créé.			
J'avais pensé que l'usager avait un autre mail sur FC, s'est fédéré avec Publik, ensuite mis dans FC la même adresse mail que celle de Publik, et s'est connecté de nouveau (et donc mail mis à jour). Mais la date de création et mäj de FcAccount sont les mêmes:			
In [16]: fac.created, fac.modified Out [16]: (datetime.datetime(2020, 6, 29, 13, 52, 11, 304922, tzinfo=<UTC>), datetime.datetime(2020, 6, 29, 13, 52, 11, 305033, tzinfo=<UTC>))			
donc j'exclue cette piste.			
Demandes liées:			
Lié à Authentic 2 - Bug #44301: Prendre en compte l'exception MultipleObjects...		Fermé	22 juin 2020

Révisions associées

Révision f1483997 - 19 mai 2021 10:15 - Nicolas Roche

test: auth_fc updates the user email with FC info (#45199)

Révision 019159d3 - 19 mai 2021 10:15 - Nicolas Roche

auth_fc: do not update user email with email returned by FC (#45199)

Historique

#2 - 28 juillet 2020 18:27 - Nicolas Roche

- Fichier 0001-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch ajouté
- Tracker changé de Support à Bug
- Statut changé de Nouveau à Solution proposée
- Assigné à mis à Nicolas Roche
- Patch proposed changé de Non à Oui

Ce scénario est bien possible (il est mis en évidence par le test inclus) :
une personne change son mail sur un FI, puis se re-connecte, alors son mail est mis à jour dans Authentic, même s'il introduit un doublon.

Ce patch accepte la connexion, puis si le mail existe déjà ailleurs, il ne prend pas en compte le nouveau mail et affiche un message compréhensible.

(Patch à prendre avec des pincettes car je n'ai pas réussi à déployer la bonne configuration pour le tester localement.)

#3 - 29 juillet 2020 22:36 - Nicolas Roche

- Fichier 0001-auth_fc-factorize-code-checking-email-unicity-45199.patch ajouté
- Fichier 0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch ajouté

Même proposition, mais en factorisant un peu de code (plutôt que de le copier/coller).

#4 - 29 juillet 2020 22:49 - Nicolas Roche

- Fichier 0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch ajouté

(et en complétant le test)

#5 - 30 juillet 2020 09:57 - Nicolas Roche

- Statut changé de Solution proposée à En cours

#6 - 30 juillet 2020 13:05 - Paul Marillonnet

- Lié à Bug #44301: Prendre en compte l'exception MultipleObjectsReturned dans l'implémentation get/update-or-create de l'API (était MultipleObjectsReturned: get() returned more than one User -- it returned 2!) ajouté

#7 - 30 juillet 2020 15:06 - Nicolas Roche

- Fichier 0001-auth_fc-factorize-code-checking-email-unicity-45199.patch ajouté

- Fichier 0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch ajouté

- Statut changé de En cours à Information nécessaire

Je réalise que l'on passe également dans "apply_user_info_mappings()" quand on s'authentifie via le backend FC, et donc que je dois directement intervenir dans cette fonction.

Rq: bien qu'il y ait 3 points d'entrés différents, je n'en teste que deux (pas encore/ou déjà authentifié), parce que dans le cas "pas encore authentifié" 2 appels se font à la suite :

```
/src/authentic2_auth_fc/views.py::LoginOrLinkView::get
if request.user.is_authenticated:
    ...
    self.update_user_info(request) # cas authentifié
    return self.redirect(request)

user = a2_utils.authenticate( ... # premier appel via le backend (en non authentifié)
...
if user:
    ...
    self.update_user_info(request)
    self.logger.info('logged in using fc sub %s', self.sub) # deuxième appel en non authentifié
    return self.redirect(request)
```

Le patch semble répondre au besoin, mais introduit une régression lorsque A2_FC_CREATE=True : le backend va préalablement créer le compte A2 sans mail, si A2_EMAIL_IS_UNIQUE=True et que le mail est déjà utilisé par un autre compte.

Ces 2 options semblent contradictoires : A2_EMAIL_IS_UNIQUE sous entend que l'email est une clé et qu'il existe forcément. Que faut-il prévoir si ces 2 options sont activées ?

(Je ne vois nul part l'option A2_FC_CREATE, qui est par défaut à False, d'activée en recette ou en production. Où puis-je trouver plus d'information à son sujet ? <https://dev.entrouvert.org/issues/10062>)

#8 - 10 août 2020 10:50 - Benjamin Dauvergne

- Projet changé de Authentic 2 à Plugin FS FranceConnect

- Hors marché mis à Non

#9 - 10 août 2020 10:52 - Benjamin Dauvergne

En fait c'est un problème déjà vu et résolu coté GLC, en passant la configuration existante par défaut :

```
return self._setting('USER_INFO_MAPPINGS', {
    'last_name': {
        'ref': 'family_name',
        'verified': True,
    },
    'first_name': {
        'ref': 'given_name',
        'verified': True,
    },
})
```

```
    'email': 'email',  
  })
```

à

```
'email': {  
  'ref': 'email',  
  'if-empty': True,  
  'tag': 'email',  
},  
'email_verified': {  
  'ref': 'email',  
  'translation': 'notempty',  
  'if-tag': 'email',  
},
```

Ici si le mail est déjà présent on y touche jamais, mais si le mail vient de FC on le coche vérifié, cette modification devrait suffire à faire passer ton test.

#10 - 10 août 2020 17:29 - Nicolas Roche

- Fichier 0001-test-auth-FC-using-user-info-mapping-45199.patch ajouté

Oui, tu as raison le test fonctionne juste avec cette configuration.
(je sais pas si je ferme ou si je propose juste le test)

#11 - 10 août 2020 17:30 - Nicolas Roche

- Fichier 0001-test-auth-FC-using-user-info-mapping-45199.patch supprimé

#12 - 10 août 2020 17:34 - Frédéric Péters

Si tu poses juste un test clairement le bug qui a amené ce ticket ne sera pas résolu. (i.e. ça ne peut pas juste être corrigé dans GLC, ça doit être corrigé partout).

#13 - 10 août 2020 17:41 - Benjamin Dauvergne

C'est moi qui n'ai pas été clair, le but pour moi était de changer la configuration par défaut plutôt que d'ajouter du code; maintenant on peut aussi passer ton code finalement parce qu'il y a des configuration modifiées en productions qui ne verront pas la nouvelle configuration par défaut (notamment quand des villes ont demandé à prendre en compte plus que nom, prénom et email depuis FC).

#14 - 10 août 2020 18:29 - Nicolas Roche

Alors ma question reste valable (dans l'éventualité où l'on changerait le code) :
comment faut-il interpréter le cumul des 2 options A2_FC_CREATE et A2_EMAIL_IS_UNIQUE ?

#15 - 10 août 2020 18:35 - Nicolas Roche

- Assigné à changé de Nicolas Roche à Benjamin Dauvergne

#17 - 11 août 2020 16:35 - Nicolas Roche

- Fichier 0001-test-auth-FC-using-user-info-mapping-45199.patch ajouté

- Patch proposed changé de Oui à Non

(au cas où, patch avec le changement de la configuration par défaut)

#19 - 17 mars 2021 00:09 - Benjamin Dauvergne

- Assigné à changé de Benjamin Dauvergne à Nicolas Roche

#20 - 17 mars 2021 10:17 - Nicolas Roche

- Statut changé de Information nécessaire à En cours

#22 - 19 mars 2021 18:40 - Nicolas Roche

- Fichier 0001-auth_fc-do-not-update-redondant-email-returned-by-FC.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Rebasé.

(il s'agit de la version du patch où la correction se fait en configuration)

La nouvelle fixture franceconnect m'a fait réaliser que je ne peux pas me reconnecter avec franceconnect alors que je le suis déjà (ce pourquoi j'ai simplifié le premier test).

J'ai ajouté un test pour exposer mon problème avec A2_EMAIL_IS_UNIQUE.
Comme #50964 prévoit de le supprimer, ce point se solutionnerait tout seul.
(j'ai testé au cas où, #50964 ne corrige pas le bug décrit par ce ticket)

#23 - 08 avril 2021 18:05 - Nicolas Roche

- Fichier 0001-auth_fc-add-tests-about-redondant-email-returned-by-.patch ajouté
- Statut changé de Solution proposée à Information nécessaire

À présent quand si un compte FC usurpe le mail d'un autre compte FC, alors on ne met plus à jour le compte Publik concerné mais le compte Publik qui possède le mail.

Je pense que ce ticket est obsolète et serais d'avis de le fermer : le backend FC ayant évolué, les patch proposés ici n'apportent plus rien.

Je fournis cependant 2 tests qui permettront éventuellement de repartir sur un nouvel intitulé de ticket.

#24 - 09 avril 2021 09:08 - Benjamin Dauvergne

Ah ben non il y a un bug, si on arrive avec le sub 1234 et qu'il existe une liaison pour ce sub on ne doit pas toucher à l'utilisateur avec le sub 4567.

#25 - 09 avril 2021 09:17 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

Ah ben non il y a un bug, si on arrive avec le sub 1234 et qu'il existe une liaison pour ce sub on ne doit pas toucher à l'utilisateur avec le sub 4567.

Je dirai même que c'est l'occasion de changer le mapping par défaut, une fois qu'on a un mail on ne le change pas, même s'il vient de FC donc ici le comportement devrait être : je suis loggé avec user1, son mail ne change pas.

#26 - 09 avril 2021 16:10 - Nicolas Roche

- Fichier 0002-auth_fc-do-not-update-redondant-email-returned-by-FC.patch ajouté
- Fichier 0001-auth_fc-update-info-on-the-FC-account-related-user-45.patch ajouté
- Statut changé de Information nécessaire à Solution proposée

Merci Benjamin pour la confirmation du bug.

0001 pour réparer le bug : si on arrive avec le sub 1234 et qu'il existe une liaison pour ce sub on ne doit pas toucher à l'utilisateur avec le sub 4567.
0002 qui reprend où on en était jusqu'à présent.

Note : j'ai délibérément zappé <https://dev.entrouvert.org/issues/45199#note-13> pour me concentrer en premier sur le test qui expose le problème.
(il y a des configurations modifiées en productions qui ne verront pas la nouvelle configuration par défaut)

Enfin,

c'est l'occasion de changer le mapping par défaut, une fois qu'on a un mail on ne le change pas, même s'il vient de FC

Je préférerais que ce soit l'objet d'un nouveau ticket (le sujet me dépasse), sinon je n'arriverai jamais à fermer proprement celui-là.
Après j'entends bien que ce nouveau paradigme est censé remplacer 0002.
(Pour moi il faudrait corriger 0001 dans un ticket dédié et en ouvrir un autre qui permette de partir sur cette nouvelle voie.)

#27 - 14 mai 2021 18:21 - Nicolas Roche

- Fichier 0002-auth_fc-do-not-update-user-email-with-email-returned.patch ajouté
- Fichier 0001-test-auth_fc-updates-the-user-email-with-FC-info-451.patch ajouté

0001: entre temps le bug mentionné ci-dessus a été corrigé, comme le montre le test.
0002: si le mail est déjà présent on y touche jamais (mais si le mail vient de FC on le coche vérifié).

0002 retire le second test qui devient redondant avec le premier.

#28 - 18 mai 2021 18:14 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ok.

#29 - 19 mai 2021 10:18 - Nicolas Roche

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

```
commit 019159d30e510f1a2579253beea75cedb7ac1ab3
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date: Fri May 14 18:09:19 2021 +0200
```

```
auth_fc: do not update user email with email returned by FC (#45199)
```

```
commit f148399793ccb163a536eb2ae7ae2e2315e57d99
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date: Fri May 14 17:34:48 2021 +0200
```

```
test: auth_fc updates the user email with FC info (#45199)
```

#30 - 21 mai 2021 09:32 - Frédéric Péters

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

Fichiers

0001-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch	9,33 ko	28 juillet 2020	Nicolas Roche
0001-auth_fc-factorize-code-checking-email-unicity-45199.patch	3,46 ko	29 juillet 2020	Nicolas Roche
0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch	8,98 ko	29 juillet 2020	Nicolas Roche
0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch	9,5 ko	29 juillet 2020	Nicolas Roche
0001-auth_fc-factorize-code-checking-email-unicity-45199.patch	5,55 ko	30 juillet 2020	Nicolas Roche
0002-auth_fc-do-not-update-non-uniq-email-returned-by-FC-.patch	11,1 ko	30 juillet 2020	Nicolas Roche
0001-test-auth-FC-using-user-info-mapping-45199.patch	7,04 ko	11 août 2020	Nicolas Roche
0001-auth_fc-do-not-update-redondant-email-returned-by-FC.patch	3,88 ko	19 mars 2021	Nicolas Roche
0001-auth_fc-add-tests-about-redondant-email-returned-by-.patch	2,92 ko	08 avril 2021	Nicolas Roche
0002-auth_fc-do-not-update-redondant-email-returned-by-FC.patch	3,16 ko	09 avril 2021	Nicolas Roche
0001-auth_fc-update-info-on-the-FC-accout-related-user-45.patch	4,86 ko	09 avril 2021	Nicolas Roche
0001-test-auth_fc-updates-the-user-email-with-FC-info-451.patch	2,62 ko	14 mai 2021	Nicolas Roche
0002-auth_fc-do-not-update-user-email-with-email-returned.patch	3,41 ko	14 mai 2021	Nicolas Roche