Authentic 2 - Development #63729

auth_oidc : avoir une stratégie de fédération sur l'email, mais sans création

08 avril 2022 15:13 - Thomas Noël

Statut:	Fermé	**Début:**	08 avril 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

On a une STRATEGY_CREATE qui, si l'OU est configurer avec unicité de mail, va rechercher si un utilisateur avec le même mail existe, et sinon le créer.

Cette création peut ne pas être désirée, typiquement dans le cas d'un OIDC avec un annuaire qui est déjà pré-provisionné par LDAP

Il serait intéressant d'avoir une STRATEGY_FIND_EMAIL, qui fasse la réconciliation selon l'attribut email, mais n'aille pas plus loin (pas de création de compte).

Révisions associées

Révision e02bf69c - 01 juin 2022 10:22 - Paul Marillonnet

auth_oidc: add a STRATEGY_FIND_EMAIL user-matching provider option (#63729)

Historique

#1 - 27 avril 2022 17:29 - Paul Marillonnet

- Sujet changé de OIDC : avoir une stratégie de fédération sur l'email, mais sans création à auth_oidc : avoir une stratégie de fédération sur l'email, mais sans création

- Statut changé de Nouveau à En cours

- Assigné à mis à Paul Marillonnet

#2 - 28 avril 2022 12:08 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Avec un peu de churn car il faut inverser la logique du backend : résoudre les claims avant de tenter l'appairage, car on a besoin de l'email pour appairer.

#3 - 28 avril 2022 13:09 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Et en fait, à travailler sur #64626 je réalise que ce n'est pas la bonne façon d'aborder les différents cas d'unicité du courriel. Je revois ma copie.

#4 - 28 avril 2022 16:25 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch ajouté

- Statut changé de En cours à Solution proposée

#6 - 19 mai 2022 07:55 - Benjamin Dauvergne

Du coté FC j'ai viré toute considération concernant l'unicité du mail au niveau de l'OU considérant que c'est implicite avec FC, je ferai de même ici si la stratégie choisie est de rechercher par email (et globalement je pense que ça permettra de déprécier A2_EMAIL_IS_UNIQUE, ça n'a aucun usage à ma connaissance, c'était juste pour pallier à l'absence de ou.email_is_unique dans le passé). Coté FC ça a bien simplifié le code :

```
    def get_or_create_user_with_email(self, email):
        ou = get_default_ou()
```

```
        qs = User.objects.filter(email__iexact=email)
        if not a2_app_settings.A2_EMAIL_IS_UNIQUE:
            qs = qs.filter(ou=ou)
```

```
        Lock.lock_email(email)
        try:
            user = qs.get()
        except User.DoesNotExist:
            return User.objects.create(ou=ou, email=email), True
```

```
        if user.ou != ou:
            raise UserOutsideDefaultOu
        return user, False
```

#7 - 19 mai 2022 15:03 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Ok, très bien, ça me va, je vais proposer un nouveau patch qui emprunte cette direction.

#8 - 20 mai 2022 11:40 - Paul Marillonnet

- Fichier 0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch ajouté

Ok, c'est mieux ainsi, en effet.
Je peux couper en deux patches avec 0001 qui serait purement le churn, i.e. déplacer la résolution des claims **avant** la tentative d'appairage, si ça peut faire gagner en clarté.

#9 - 01 juin 2022 08:05 - Benjamin Dauvergne

- Statut changé de En cours à Solution validée

#10 - 01 juin 2022 10:22 - Benjamin Dauvergne

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

```
commit a6ab8a2624e1ec8d6a92a4c3dd1662ed76de7fd6
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Wed Apr 27 18:00:51 2022 +0200

    auth_oidc: add a STRATEGY_FIND_EMAIL user-matching provider option (#63729)
```

#11 - 02 juin 2022 16:14 - Transition automatique

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

#12 - 07 août 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch	15,1 ko	28 avril 2022	Paul Marillonnet
0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch	14,7 ko	28 avril 2022	Paul Marillonnet
0001-auth_oidc-add-a-STRATEGY_FIND_EMAIL-user-matching-pr.patch	13,5 ko	20 mai 2022	Paul Marillonnet