

Authentic 2 - Bug #23900

idp oidc: restaurer la fourniture de preferred_username

17 mai 2018 17:05 - Josué Kouka

Statut:	Fermé	Début:	17 mai 2018
Priorité:	Normal	Echéance:	
Assigné à:	Josué Kouka	% réalisé:	100%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	
Patch proposé:	Oui		
Description			
Depuis #21870 , preferred_username n'est plus fourni par défaut.			
Demandes liées:			
Lié à Authentic 2 - Bug #23643: Crash connexion oidc		Fermé	07 mai 2018

Révisions associées

Révision d4d4aa65 - 16 août 2018 09:41 - Josué Kouka

idp oidc: set user identifier as preferred username claim (#23900)

Historique

#1 - 17 mai 2018 17:06 - Josué Kouka

- Lié à Bug #23643: Crash connexion oidc ajouté

#2 - 17 mai 2018 17:46 - Benjamin Dauvergne

Non, non, non le username n'est pas un email, à la base c'est un système qui permettait d'avoir 10 fois le même username en créant des realm, donc on pouvait se connecter avec too ou toto@entrouvert.org si on voulait être certain de ne pas avoir de collision avec too@easter-eggs.com (mais ce ne sont pas des email).

#3 - 17 mai 2018 17:54 - Josué Kouka

Benjamin Dauvergne a écrit :

Non, non, non le username n'est pas un email, à la base c'est un système qui permettait d'avoir 10 fois le même username en créant des realm, donc on pouvait se connecter avec too ou toto@entrouvert.org si on voulait être certain de ne pas avoir de collision avec too@easter-eggs.com (mais ce ne sont pas des email).

Ok, peut être que j'ai mal exposé le problème remonté par Fred dans [#23643](#). Comment l'on fait pour revenir à ça

```
user_info['preferred_username'] = user.username.split('@', 1)[0]
```

#4 - 17 mai 2018 18:03 - Benjamin Dauvergne

On utiliser django_user_identifieur voir http://git.entrouvert.org/authentic.git/tree/src/authentic2/attributes_ng/sources/django_user.py#n79

#5 - 17 mai 2018 18:28 - Josué Kouka

- Statut changé de Nouveau à Rejeté

Benjamin Dauvergne a écrit :

On utiliser django_user_identifieur voir http://git.entrouvert.org/authentic.git/tree/src/authentic2/attributes_ng/sources/django_user.py#n79

Ok neat !!

#6 - 30 mai 2018 09:47 - Frédéric Péters

- Statut changé de Rejeté à En cours

Euh ?

Ce ticket rejeté mais ne pas avoir preferred_username positionné, alors que c'était le cas avant, c'est un vrai problème, ça fait crasher l'alfresco lors du SSO à Tournai.

#7 - 30 mai 2018 09:50 - Frédéric Péters

À noter l'intitulé à côté de la plaque du ticket; le soucis c'est qu'on avait avant preferred_username et qu'on ne l'a plus.

#8 - 30 mai 2018 09:54 - Benjamin Dauvergne

- *Sujet changé de idp oidc: retourner juste le local-part lorsque le username est de type email. à idp oidc: restaurer la fourniture de preferred_username*

- *Description mis à jour*

Je modifie l'intitulé et la description, si c'est urgent pour Tournai la solution et de passer par la configuration manuelle et de remettre preferred_username avec comme source django_user_identifier.

#9 - 30 mai 2018 09:58 - Frédéric Péters

C'est (c'était) urgent pour Tournai (ça bloquait tout SSO vers Alfresco). (mais une fois trouvée l'origine du problème, j'ai contourné)

#10 - 30 mai 2018 10:35 - Benjamin Dauvergne

Josué tu vois un moyen de restaurer la règle par défaut avec la configuration que je donne ? On les ajoute (les règles par défaut) à la création mais ici il faudrait une migration qui vérifie si les règles sont celles par défaut et si oui ajoute la règle manquante.

#11 - 30 mai 2018 16:00 - Josué Kouka

Benjamin Dauvergne a écrit :

Josué tu vois un moyen de restaurer la règle par défaut avec la configuration que je donne ? On les ajoute (les règles par défaut) à la création mais ici il faudrait une migration qui vérifie si les règles sont celles par défaut et si oui ajoute la règle manquante.

Non, je ne pense pas. J'ai du mal à saisir ce que c'est qu'une règle. Est ce la configuration d'un claim ?

#12 - 31 mai 2018 09:26 - Benjamin Dauvergne

Oui la configuration des claims OIDC, désolé de changer de terme. J'ai tendance à tout appeler règle du moment que ça parle d'attributs.

#13 - 31 mai 2018 15:23 - Josué Kouka

Benjamin Dauvergne a écrit :

Oui la configuration des claims OIDC, désolé de changer de terme. J'ai tendance à tout appeler règle du moment que ça parle d'attributs.

Ok.

Josué tu vois un moyen de restaurer la règle par défaut avec la configuration que je donne ? On les ajoute (les règles par défaut) à la création mais ici il faudrait une migration qui vérifie si les règles sont celles par défaut et si oui ajoute la règle manquante.

Oui je vois.

#14 - 08 août 2018 17:27 - Josué Kouka

- *Fichier 0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch ajouté*

- *Statut changé de En cours à Solution proposée*

- *Patch proposed changé de Non à Oui*

#15 - 08 août 2018 18:11 - Benjamin Dauvergne

Je testerai les claim.name ainsi que les claim.value.

#16 - 09 août 2018 11:21 - Josué Kouka

- *Fichier 0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch ajouté*

#17 - 09 août 2018 13:46 - Benjamin Dauvergne

Je vois aucune changement dans la migrations:

```
if DEFAULT_CLAIM_VALUES.symmetric_difference(claim_values):
```

C'est ça qu'il faut changer.

#18 - 09 août 2018 14:40 - Josué Kouka

- Fichier 0001-idp-oidc-set-user-identifier-as-preferred-username-c.patch ajouté

Ye t'as raison. C'est fait

#19 - 09 août 2018 15:07 - Benjamin Dauvergne

Presque...

```
OLD_DEFAULT_CLAIM_MAPPING = {
    'email': 'default_user_email',
    'email_verified': 'django_user_email_verified',
    'family_name': 'django_user_last_name',
    'given_name': 'django_user_first_name',
    'preferred_username': 'django_user_username',
}
...
claim_mapping = set(oidcclient.oidcclaim_set.values_list('name', 'value'))
if set(OLD_DEFAULT_CLAIM_MAPPING.items()).symmetric_difference(claim_mapping):
...
```

Aussi tu as oublié de corriger la valeur par défaut dans l'admin (src/authentic2_idp_oidc/admin.py).

#20 - 09 août 2018 17:22 - Josué Kouka

- Fichier 0001-idp-oidc-set-user-identifier-as-preferred-username-c.patch ajouté

Aussi tu as oublié de corriger la valeur par défaut dans l'admin (src/authentic2_idp_oidc/admin.py).

Ajouté.

#21 - 09 août 2018 22:51 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Je trouve ça indélicatement formaté, ce n'est pas la première fois, c'est plus joli quand tout est aligné non ? En plus comme j'avais fait le boulot dans mon exemple...

```
OLD_DEFAULT_CLAIMS_MAPPING = {
    'email': 'django_user_email', 'email_verified': 'django_user_email_verified',
    'family_name': 'django_user_last_name', 'given_name': 'django_user_first_name',
    'preferred_username': 'django_user_username'
}
```

Je n'avais pas remarqué mais ça change quand même la sémantique par rapport à avant:

```
@@ -235,7 +238,7 @@ def test_authorization_code_sso(login_first, oidc_settings, oidc_client, simple_
    else:
        assert claims['acr'] == '1'
        assert claims['sub'] == make_sub(oidc_client, simple_user)
- assert claims['preferred_username'] == simple_user.username
+ assert claims['preferred_username'] == ''
        assert claims['given_name'] == simple_user.first_name
        assert claims['family_name'] == simple_user.last_name
        assert claims['email'] == simple_user.email
@@ -244,7 +247,7 @@ def test_authorization_code_sso(login_first, oidc_settings, oidc_client, simple_
    user_info_url = make_url('oidc-user-info')
    response = app.get(user_info_url, headers=bearer_authentication_headers(access_token))
    assert response.json['sub'] == make_sub(oidc_client, simple_user)
- assert response.json['preferred_username'] == simple_user.username
+ assert response.json['preferred_username'] == ''
    assert response.json['given_name'] == simple_user.first_name
    assert response.json['family_name'] == simple_user.last_name
    assert response.json['email'] == simple_user.email
```

Il y a un souci.

Il faut modifier la définition de django_user_identifier pour que ça colle avec la définition précédente de preferred_username:

```
+         if user.username:  
+             user_info['preferred_username'] = user.username.split('@', 1)[0]
```

voir src/authentic2/attributes_ng/sources/django_user.py :

```
77         splitted = user.username.rsplit('@', 1)  
78         ctx['django_user_domain'] = splitted[1] if '@' in user.username else ''  
79         ctx['django_user_identifier'] = splitted[0] if '@' in user.username else ''
```

#22 - 10 août 2018 15:30 - Josué Kouka

- Statut changé de Solution validée à Solution proposée

Il y a un souci.

Il faut modifier la définition de django_user_identifier pour que ça colle avec la définition précédente de preferred_username

J'y ai pensé, mais puis je me suis dit que vu que preferred_username n'est en aucun cas un identifiant unique (doc oidc) j'ai pas fait la modification. C'est fait dans ce patch.

#23 - 10 août 2018 17:14 - Benjamin Dauvergne

Manque le patch.

#24 - 10 août 2018 17:20 - Josué Kouka

- Fichier 0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch ajouté

#25 - 10 août 2018 17:25 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#26 - 16 août 2018 09:42 - Josué Kouka

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

- % réalisé changé de 0 à 100

```
commit d4d4aa65c58d74c8832c57e0144d6766ab1044a2 (HEAD -> master, origin/master, origin/HEAD)  
Author: Josue Kouka <jkouka@entrouvert.com>  
Date: Wed Aug 8 17:17:26 2018 +0200
```

```
idp oidc: set user identifier as preferred username claim (#23900)
```

#27 - 04 décembre 2018 20:08 - Frédéric Péters

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch	5,56 ko	08 août 2018	Josué Kouka
0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch	5,97 ko	09 août 2018	Josué Kouka
0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch	6,93 ko	09 août 2018	Josué Kouka
0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch	8,78 ko	09 août 2018	Josué Kouka
0001-idp-oidc-set-user-identifiant-as-preferred-username-c.patch	8,46 ko	10 août 2018	Josué Kouka