Authentic 2 - Bug #62900

gestion des personnes morales : par défaut ne pas renvoyer les claims relatives aux informations de compte standard si un profil PM est choisi par l'usager

17 mars 2022 14:33 - Paul Marillonnet

Statut:	Information nécessaire	**Début:**	17 mars 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Notamment dans le cas spécifique glcpro où les informations "couronne" (portée "crown") ne sont pas pertinentes pour une démarche PM et ne doivent donc pas être renvoyées.

Historique

#1 - 17 mars 2022 15:04 - Paul Marillonnet

Et les adaptations en front pour que l'usager comprenne que lorsqu'il sélectionne un profil PM ses informations personnelles ne sont pas transmises. Ces adaptations pourraient consister en du JS qui met à jour en live la liste des claims transmises, ou bien simplement une seconde page dans le process d'autorisation, ou bien encore un texte explicatif sur la même page accompagné de la liste des claims qui ne seront pas transmises si l'usager sélectionne un profil PM.

#2 - 21 mars 2022 11:27 - Paul Marillonnet

- Fichier 0001-idp_oidc-discard-any-extra-scopes-at-profile-selecti.patch ajouté

- Tracker changé de Support à Bug

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Basé sur #62889.

#3 - 28 mars 2022 10:37 - Paul Marillonnet

- Tags mis à personnes morales

#4 - 05 avril 2022 14:55 - Benjamin Dauvergne

- Assigné à mis à Paul Marillonnet

#5 - 05 avril 2022 15:24 - Benjamin Dauvergne

Que je comprenne bien, le besoin ici en fait c'est que le code qui surcharge la création des user_info/id_token dans authentic2-glc ne renvoie pas les données couronnes lorsqu'un profil est sélectionné ? Ce ne sera pas plus simple de faire ça dans dans le hook correspondant que de déporter de la logique ici qui manipule les scopes ? À terme l'idéal serait de pouvoir se passer complètement du hook en ayant une configuration des claims/scopes plus complexe, en attendant je me dis qu'on préférera garder du code simple ici plutôt que d'avoir du code dans authentic écrit spécifiquement pour un usage externe.

PS: sachant qu'effectivement le système de profil interagit très mal avec les scopes, voir l'ignore complètement en fait.

#6 - 12 avril 2022 11:34 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Benjamin Dauvergne a écrit :

> Que je comprenne bien, le besoin ici en fait c'est que le code qui surcharge la création des user_info/id_token dans authentic2-glc ne renvoie pas les données couronnes lorsqu'un profil est sélectionné ?

Oui c'est bien ça.

> Ce ne sera pas plus simple de faire ça dans dans le hook correspondant que de déporter de la logique ici qui manipule les scopes ?

Peut-être oui, je regarde.

> À terme l'idéal serait de pouvoir se passer complètement du hook en ayant une configuration des claims/scopes plus complexe, en attendant je me dis qu'on préférera garder du code simple ici plutôt que d'avoir du code dans authentic écrit spécifiquement pour un usage externe.
>
> PS: sachant qu'effectivement le système de profil interagit très mal avec les scopes, voir l'ignore complètement en fait.

Okay.

#7 - 13 avril 2022 15:17 - Paul Marillonnet

- Fichier 0001-idp_oidc-discard-any-extra-scopes-at-profile-selecti.patch ajouté

- Statut changé de En cours à Solution proposée

Une implémentation a2 mainline du hook, car il ne me semble pas que cette approche soit spécifique GL.

#8 - 25 octobre 2022 11:25 - Benjamin Dauvergne

- Statut changé de Solution proposée à Information nécessaire

Je ne comprends pas ce que fait ce code, si c'est le fonctionnement normal de l'idp oidc pas besoin d'un hook, autant mettre ça dans le code de génération des user_info/id_token. Et cette ligne particulièrement :

```
set(claim.get_scopes()) & extra_scopes and not set(claim.get_scopes()) & scope_set
```

Ça a l'air bien compliqué, le but semble être de retirer tout claim qui n'a pas été autorisé par un des claims "classiques/autorisés", openid, email et profile, dans ce cas autant faire cela:

```
# when profile is used, only keep generic claims linked to openid, email and profile scope (WHY???)
if profile:
   claim_removed = []
   for claim in OIDCClaim.objects.filter(client=client, name__in=user_info.keys()):
       if not (set(claim.get_scopes()) & {'openid', 'email', 'profile'} and claim.name in user_info:
           user_info.pop(claim.name)
           claim_removed.append(claim.name)
   if claim_removed:
       logger.info(....)
```

Fichiers

0001-idp_oidc-discard-any-extra-scopes-at-profile-selecti.patch	5,97 ko	21 mars 2022	Paul Marillonnet
0001-idp_oidc-discard-any-extra-scopes-at-profile-selecti.patch	7,93 ko	13 avril 2022	Paul Marillonnet