Authentic 2 - Development #46182

En BO, gestion des consentements de l'utilisateur donnés lors du SSO OIDC et les scopes de diffusion d'attributs

28 août 2020 12:36 - Mikaël Ates

Statut:	Fermé	**Début:**	28 août 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Nicolas Roche	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Gestion rendue possible en FO par l'usager dans #45200.

Permettre la même chose par un admin en BO sur un utilisateur. Ajouter pour cela une entrée sur la page de l'utilisateur via un bouton dans la barre latérale.

Demandes liées:

Lié à Authentic 2 - Bug #45200: Gestion par l'usager de ses consentements sur...	**Fermé**	**16 juillet 2020**
Lié à Authentic 2 - Development #45651: idp_oidc : disposer d'une page de ges...	**Fermé**	**31 juillet 2020**

Révisions associées

Révision c636b164 - 29 septembre 2020 11:55 - Nicolas Roche

a2_rbac: add manage_authorizations permission to custom_user (#46182)

Révision 14f37aee - 29 septembre 2020 11:55 - Nicolas Roche

manager: add a page to manage users authorized services (#46182)

Historique

#1 - 28 août 2020 12:37 - Mikaël Ates

- Lié à Bug #45200: Gestion par l'usager de ses consentements sur le SSO et et les scopes de diffusion d'attributs ajouté

#2 - 28 août 2020 12:37 - Mikaël Ates

- Lié à Development #45651: idp_oidc : disposer d'une page de gestion des consentements par OU ajouté

#6 - 31 août 2020 11:11 - Nadège Perez

Cette page est déjà disponible en PROD ?

#7 - 31 août 2020 11:40 - Mikaël Ates

Non, ce n'est pas encore développé.

#8 - 02 septembre 2020 10:54 - Nicolas Roche

- Assigné à mis à Nicolas Roche

#9 - 04 septembre 2020 17:42 - Nicolas Roche

- Fichier 0001-manager-add-a-page-to-manage-users-authorized-oauth-.patch ajouté

- Statut changé de Nouveau à Information nécessaire

- Patch proposed changé de Non à Oui

(help)

Voici un premier jet qui permet d'avoir un rendu avec la présentation de type table.

Ce patch ne gère pas encore les permissions.
D'instinct j'aurais choisi d'utiliser la permission : "Supprimer / oidc authorization".
Mais, les permissions sont attachées à un backend et le backend oidc ne les implémente pas.

(Est-ce que quelqu'un aurait une piste pour m'aiguiller ?)

#10 - 04 septembre 2020 18:21 - Nicolas Roche

- Fichier oauth-bo.ogv ajouté

(Le rendu, sans la gestion des permissions)

#11 - 07 septembre 2020 14:25 - Benjamin Dauvergne

Nicolas Roche a écrit :

> Ce patch ne gère pas encore les permissions.
> D'instinct j'aurais choisi d'utiliser la permission : "Supprimer / oidc authorization".
> Mais, les permissions sont attachées à un backend et le backend oidc ne les implémente pas.
> (Est-ce que quelqu'un aurait une piste pour m'aiguiller ?)

Je dirai que l'opération pourrait s'appeler 'manage-authorizations' comme on a 'manage-memebers' pour les rôles, opération associée au modèle custom_user.user.

#12 - 08 septembre 2020 17:51 - Nicolas Roche

Où/quand ajouter l'opération "manage-authorizations" en base (je n'arrive pas à trouver) ?

```
# select * from django_rbac_operation;
 id |                name                |      slug
----+------------------------------------+-----------------
  1 | Ajouter                            | add
  2 | Modifier                           | change
  3 | Supprimer                          | delete
  4 | Visualisation                      | view
  5 | Administration                     | admin
  6 | Rechercher                         | search
  7 | Modifier le mot de passe           | change_password
  8 | Réinitialiser le mot de passe      | reset_password
  9 | Activer                            | activate
 10 | Modifier votre adresse électronique | change_email
 11 | Manage role members                | manage_members
```

#13 - 08 septembre 2020 17:57 - Valentin Deniaud

Tu as vu ce commit 599555f3cb1363eb6fafb0c24f67bd723565c98b, qui ajoute manage_members ?

Me semble que l'opération est créée une fois dynamiquement via un get_or_create et puis voilà, mais à confirmer.

#14 - 08 septembre 2020 18:25 - Nicolas Roche

Oui, mais merci de m'avoir dit d'y regarder à 2 fois.
C'est fait dans a2_rbac/management.py et a2_rbac/managers.py via admin_role.add_self_administration(), à la création des nouveaux rôles.

#15 - 10 septembre 2020 14:50 - Nicolas Roche

- Fichier 0003-manager-add-a-page-to-manage-users-authorized-oauth-.patch ajouté

- Fichier 0002-manager-add-an-authorized-oauth-service-form-46182.patch ajouté

- Fichier 0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch ajouté

- Statut changé de Information nécessaire à Solution proposée

- 0001 ajouter la permission après une migration, comme c'est fait pour pour l'opération VIEW_OP associée au modèle a2_rbac.role.
- 0002 ajouter un formulaire de suppression des autorisations oidc qui vérifie la permission
- 0003 reprend le premier patch donnée plus haut, en ajoutant une popup de confirmation et (c'est peut-être superflus) qui grise l'icône de suppression si un utilisateur qui n'a pas la permission arrive quand même sur la page.

#16 - 10 septembre 2020 16:01 - Paul Marillonnet

Pas sûr de la phrase “No granted service access to this account profile data.” pour le texte vide dans 0002.
Je ne sais pas si c'est exactement ce que tu cherches à dire mais sans doute que “This user has not granted profile data access to any service yet.” pourrait faire l'affaire, qu'en dis-tu ?

#17 - 10 septembre 2020 17:45 - Nicolas Roche

- Fichier 0003-manager-add-a-page-to-manage-users-authorized-oauth-.patch ajouté

- Fichier 0002-manager-add-an-authorized-oauth-service-form-46182.patch ajouté

Merci. J'en ai profité pour déplacer le patch du fichier tables.py dans 0003.

#18 - 25 septembre 2020 10:58 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

La vue ne déclarer pas de permission (attribut de classe permissions) et donc est visible de tous, je penser qu'un permission adéquat serait "custom_user.view_user" (la vue est visible à ceux qui voient aussi la vue de détail d'un utilisateur).

Je ne vois rien d'autre qui me choque.

#19 - 25 septembre 2020 11:21 - Nicolas Roche

> une permission adéquat serait "custom_user.view_user"

Il a aura alors plusieurs accès possibles :

- Les utilisateurs qui ont la permissions "custom_user.view_user" ou "custom_user.manage_authorizations_user" :
  - Voient le bouton sur la fiche de l'utilisateur
  - Accèdent à la nouvelle vue, mais ne peuvent pas supprimer les autorisations (l'icône est grisée)
- Seuls les utilisateurs qui ont la permissions "custom_user.manage_authorizations_user" peuvent supprimer les autorisations.

#20 - 25 septembre 2020 18:29 - Nicolas Roche

- Fichier 0002-manager-add-a-page-to-manage-users-authorized-oauth-.patch ajouté

- Fichier 0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch ajouté

- Statut changé de En cours à Solution proposée

J'ai du mal avec les permissions (Perm = opération / destination) et j'ai dû revoir mes patchs pour corriger mes erreurs :
dans le second commit précédent je faisais pointer les permissions sur les autorisations OAuth, alors qu'elles doivent pointer sur l'utilisateur affiché.

Ici, j'ai fusionné ces 2 commits : j'ai retiré la vérification des permissions sur les champs du formulaire (ça n'a pas sens) et j'ai ajouté la vérification des permission sur l'utilisateur cible, lors de la validation du formulaire.

(Je note au passage que pour créer les nouvelles permissions, pour tester le patch à l'usage par exemple, il faut faire une migration : lancer la commande "migrate_schemas" ne suffit pas si elle ne migre rien)

#21 - 25 septembre 2020 18:37 - Benjamin Dauvergne

Nicolas Roche a écrit :

> > une permission adéquat serait "custom_user.view_user"
>
> Il a aura alors plusieurs accès possibles :
>
> - Les utilisateurs qui ont la permissions "custom_user.view_user" ou "custom_user.manage_authorizations_user" :
>   - Voient le bouton sur la fiche de l'utilisateur
>   - Accèdent à la nouvelle vue, mais ne peuvent pas supprimer les autorisations (l'icône est grisée)

Généralement on définit un héritage, ça évite de se poser cette question. Si on a manage_authorizations alors on a aussi view sur les mêmes objets. C'est défini là https://git.entrouvert.org/authentic.git/tree/src/authentic2/settings.py#n336 à modifier (je l'avais oublié, donc ça tombe bien qu'on en parle).

> - Seuls les utilisateurs qui ont la permissions "custom_user.manage_authorizations_user" peuvent supprimer les autorisations.

Yep.

#22 - 25 septembre 2020 18:57 - Benjamin Dauvergne

Nicolas Roche a écrit :

> *(Je note au passage que pour créer les nouvelles permissions, pour tester le patch à l'usage par exemple, il faut faire une migration : lancer la commande "migrate_schemas" ne suffit pas si elle ne migre rien)*

Oui les rôles techniques sont créés/mis-à-jour dans post_migrate.

#23 - 25 septembre 2020 19:07 - Benjamin Dauvergne

```
  {# avoid cycle for Django 1.2-1.6 compatibility #}
```

Je ne sais plus à quoi ça fait référence et je suppose que c'est du copier/coller mais si tu trouves on doit pouvoir s'en passer.

```
        yield Action('view_service_authorizations', _('View service authorizations'),
                     url_name='a2-manager-authorized-oauth-services',
                     permission='custom_user.view_user',
                     popup=False)
```

Est-ce qu'on ne mettrait pas plutôt ça en haut à coté d'Éditer/Supprimer (pour coller un peu plus aux autres briques) (et puis parce que c'est pas vraiment une action).

Ça m'inquiète que tes tests passent alors que manage_auth_role n'a que la permission d'administration des autorisations et que l'héritage avec view_user n'est pas en place (il n'a pas la permission view_user il ne devrait pas arriver à accéder à la page de détail).

#24 - 25 septembre 2020 19:07 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

#25 - 27 septembre 2020 19:07 - Nicolas Roche

- Fichier 0002-manager-add-a-page-to-manage-users-authorized-oauth-.patch ajouté

- Statut changé de En cours à Solution proposée

J'ai changé les noms des templates, classes, urls... en les préfixant par "user_oauth_services" (au lieu de "authorized_oauth_services")

> Bouton à côté d'éditer

J'ai réduit l'intitulé du bouton à "Services authorizations".
J'aurais bien mis 'Oauth services" pour coller avec le reste mais je pense que ce n'est pas assez compréhensible.

> virer {# avoid cycle for Django 1.2-1.6 compatibility #}

C'est du code copié/collé issu de src/authentic2/manager/templates/authentic2/manager/table.html que j'étends dans user_oauth_services_tables.html.
Je réalise que j'ai surchargé inutilement table.html pour retirer le lien sur la ligne, alors que je peux simplement l'invalider avec : '{% with row_link=0 %}'

Sinon, ce commentaire est introduit par le quatrième patch de #5180 qui met en place le fichier table.html. On retrouve le même code dans django_table2, sans le commentaire (que je n'arrive donc pas à élucider).
https://github.com/jieter/django-tables2/blob/master/django_tables2/templates/django_tables2/table.html#L27

> Ça m'inquiète que tes tests passent alors que manage_auth_role n'a que la permission d'administration des autorisations (Généralement on définit un héritage...)

C'est parce que l'héritage était déjà en place, je l'ai fait en m'alignant sur manage_members (dans 0001) :

```
DJANGO_RBAC_PERMISSIONS_HIERARCHY = {
    'admin': ['change', 'delete', 'add', 'view', 'change_password', 'reset_password', 'activate',
    'manage_members': ['view', 'search'],
    'manage_authorizations': ['view', 'search'],
}
```

Mais faut-il rajouter les permissions 'manage_*' à 'admin' ?

> il faut faire une migration : lancer la commande "migrate_schemas" ne suffit pas si elle ne migre rien

Je note ici qu'il faudra vérifier que ce patch passera en même temps qu'une migration, ou alors qu'il faudrait que j'en génère une factice.

#26 - 27 septembre 2020 19:32 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Nicolas Roche a écrit :

> J'ai changé les noms des templates, classes, urls... en les préfixant par "user_oauth_services" (au lieu de "authorized_oauth_services")

Ça n'a pas de rapport avec oauth, user_authorizations ça suffirait.

> Bouton à côté d'éditer

> J'ai réduit l'intitulé du bouton à "Services authorizations".

Juste "Authorizations" ?

> J'aurais bien mis 'Oauth services" pour coller avec le reste mais je pense que ce n'est pas assez compréhensible.

OAuth c'est un détail d'implémentation, n'en parlons nul part (on pourrait avoir des autorisations de SSO en SAML aussi).

> virer {# avoid cycle for Django 1.2-1.6 compatibility #}

> C'est du code copié/collé issu de src/authentic2/manager/templates/authentic2/manager/table.html que j'étends dans user_oauth_services_tables.html.
> Je réalise que j'ai surchargé inutilement table.html pour retirer le lien sur la ligne, alors que je peux simplement l'invalider avec : '{% with row_link=0 %}'
> Sinon, ce commentaire est introduit par le quatrième patch de #5180 qui met en place le fichier table.html. On retrouve le même code dans django_table2, sans le commentaire (que je n'arrive donc pas à élucider).
> https://github.com/jieter/django-tables2/blob/master/django_tables2/templates/django_tables2/table.html#L27

Oublions, vire le commentaire simplement.

> Ça m'inquiète que tes tests passent alors que manage_auth_role n'a que la permission d'administration des autorisations (Généralement on définit un héritage...)

> C'est parce que l'héritage était déjà en place, je l'ai fait en m'alignant sur manage_members (dans 0001) :
> [...]

Je suis rassuré :).

> Mais faut-il rajouter les permissions 'manage_*' à 'admin' ?

Oui, on ne l'a pas vu mais elles manquent.

> il faut faire une migration : lancer la commande "migrate_schemas" ne suffit pas si elle ne migre rien

> Je note ici qu'il faudra vérifier que ce patch passera en même temps qu'une migration, ou alors qu'il faudrait que j'en génère une factice.

Je comprends maintenant ce que tu voulais dire; en voulant accélérer les migrations on fait une passe sur la table des migrations de chaque tenant pour décider de lancer ou pas la commande migrate sur le tenant, en ne lançant pas cette commande on perd le lancement des actions post-migrate (qui après les checks Django et peut-être encore ce qui nous coûte cher). Un moyen d'obtenir quand même le post-migrate c'est de lancer migrate_schemas uniquement sur l'app authentic2, ça désactive « l'optimisation »[1].

[1] https://git.entrouvert.org/hobo.git/tree/hobo/multitenant/management/commands/migrate_schemas.py#n60

Rapidement relu, en dehors des OAuth/oauth partout c'est bon.

#27 - 28 septembre 2020 15:05 - Nicolas Roche

- Fichier 0002-manager-add-a-page-to-manage-users-authorized-servic.patch ajouté

- Fichier 0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch ajouté

#28 - 28 septembre 2020 15:09 - Benjamin Dauvergne

Je vois encore du oauth dans 0001.

#29 - 28 septembre 2020 16:57 - Nicolas Roche

- Fichier 0002-manager-add-a-page-to-manage-users-authorized-servic.patch ajouté

- Fichier 0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch ajouté

- Statut changé de Solution validée à Solution proposée

Oups, oui en effet.
J'ai corrigé le test de 0001 qui ne passait plus suite à l'ajout de la permission 'manage_authorizations' à 'admin'.

#30 - 28 septembre 2020 18:26 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Wunderbar.

#31 - 29 septembre 2020 11:57 - Nicolas Roche

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

```
commit 14f37aeedd6a349d3ae93616591be0337770b548
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date:   Thu Sep 10 12:31:53 2020 +0200

    manager: add a page to manage users authorized services (#46182)

commit c636b164242bd9e88f06bc8ae330ed73a16549ca
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date:   Thu Sep 10 12:24:42 2020 +0200

    a2_rbac: add manage_authorizations permission to custom_user (#46182)
```

#32 - 03 octobre 2020 11:16 - Frédéric Péters

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

Fichiers

0001-manager-add-a-page-to-manage-users-authorized-oauth-.patch	10,2 ko 04 septembre 2020	Nicolas Roche
oauth-bo.ogv	11,8 Mo 04 septembre 2020	Nicolas Roche
0003-manager-add-a-page-to-manage-users-authorized-oauth-.patch	12,2 ko 10 septembre 2020	Nicolas Roche
0002-manager-add-an-authorized-oauth-service-form-46182.patch	9,42 ko 10 septembre 2020	Nicolas Roche
0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch	10,4 ko 10 septembre 2020	Nicolas Roche
0003-manager-add-a-page-to-manage-users-authorized-oauth-.patch	13,9 ko 10 septembre 2020	Nicolas Roche
0002-manager-add-an-authorized-oauth-service-form-46182.patch	7,77 ko 10 septembre 2020	Nicolas Roche
0002-manager-add-a-page-to-manage-users-authorized-oauth-.patch	18,9 ko 25 septembre 2020	Nicolas Roche
0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch	10,4 ko 25 septembre 2020	Nicolas Roche
0002-manager-add-a-page-to-manage-users-authorized-oauth-.patch	18,2 ko 27 septembre 2020	Nicolas Roche
0002-manager-add-a-page-to-manage-users-authorized-servic.patch	18,2 ko 28 septembre 2020	Nicolas Roche
0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch	10,7 ko 28 septembre 2020	Nicolas Roche
0002-manager-add-a-page-to-manage-users-authorized-servic.patch	18,1 ko 28 septembre 2020	Nicolas Roche
0001-a2_rbac-add-manage_authorizations-permission-to-cust.patch	11,2 ko 28 septembre 2020	Nicolas Roche