Authentic 2 - Development #71275

contrôle d'accès : gérer l'appartenance à des collectivités pour les clients d'API

14 novembre 2022 13:18 - Paul Marillonnet

Statut:	Fermé	**Début:**	14 novembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

C'est à mon avis typiquement le genre de chose qu'on voudrait pouvoir classer par collectivité (au sens OU) pour pouvoir restreindre les accès à l'API.
Un exemple parmi d'autres, un déploiement multi-collectivités où on veut ouvrir l'API sur l'une des collectivités et pas les autres.

Demandes liées:

Lié à Authentic 2 - Development #71267: a2_rbac : avoir un rôle interne d'adm...	**Fermé**	**14 novembre 2022**
Lié à Hobo - Development #71288: gérer les accès en fonction de la collectivi...	**En cours**	**14 novembre 2022**
Lié à Authentic 2 - Development #71463: api/rbac : au lieu d'une vérification...	**Nouveau**	**18 novembre 2022**
Lié à Authentic 2 - Development #72151: /manage/ : gérer dans les écrans de c...	**Nouveau**	**07 décembre 2022**
Lié à Hobo - Bug #72355: tests cassés suite à l'introduction des rôles de ges...	**Rejeté**	**13 décembre 2022**
Lié à Hobo - Development #72354: Buid hobo en erreur suite à changement dans ...	**Fermé**	**13 décembre 2022**
Lié à Authentic 2 - Development #72688: /manage/ : l'écran de gestion des cli...	**Fermé**	**21 décembre 2022**
Lié à Authentic 2 - Development #72703: /manage/ : l'écran de gestion des cli...	**Fermé**	**22 décembre 2022**

Révisions associées

Révision 5a821a88 - 28 novembre 2022 09:12 - Paul Marillonnet

a2_rbac: add global management role for api clients (#71267)

`ou-wise api-client management roles will be added in #71275.`

Révision a7ffb583 - 13 décembre 2022 14:39 - Paul Marillonnet

models: add ou field to api clients (#71275)

Révision 4240f989 - 13 décembre 2022 14:39 - Paul Marillonnet

api_views: handle ou-wise api-client checks (#71275)

Historique

#1 - 14 novembre 2022 13:18 - Paul Marillonnet

- Lié à Development #71267: a2_rbac : avoir un rôle interne d'administration des clients d'API ajouté

#3 - 14 novembre 2022 16:46 - Paul Marillonnet

- Assigné à mis à Paul Marillonnet

Il y aurait aussi une partie hobo à gérer, je vais créer un ticket.

#4 - 14 novembre 2022 16:48 - Paul Marillonnet

- Lié à Development #71288: gérer les accès en fonction de la collectivité d'appartenance du client d'API ajouté

#5 - 17 novembre 2022 11:31 - Paul Marillonnet

Paul Marillonnet a écrit :

> C'est à mon avis typiquement le genre de chose qu'on voudrait pouvoir classer par collectivité (au sens OU) pour pouvoir restreindre les accès à l'API.
> Un exemple parmi d'autres, un déploiement multi-collectivités où on veut ouvrir l'API sur l'une des collectivités et pas les autres.

Et en fait ça passe déjà nécessairement par des rôles de gestion dans les collectivités. Pas sûr qu'on gagne à ajouter quoi que ce soit ici, je vérifie et rejette le ticket ensuite.

#6 - 18 novembre 2022 08:43 - Paul Marillonnet

Si, c'est sans doute quand même intéressant d'avoir des rôles de gestion des clients d'API cloisonnés à une collectivité. Ce serait purement a2, rien dans hobo ; lorsque la personne qui détient le rôle édite un client d'API, il faut vérifier que les rôles ajoutés ne sont pas en dehors de l'OU d'appartenance du rôle de gestion.

#7 - 18 novembre 2022 11:33 - Paul Marillonnet

Paul Marillonnet a écrit :

> Si, c'est sans doute quand même intéressant d'avoir des rôles de gestion des clients d'API cloisonnés à une collectivité. Ce serait purement a2, rien dans hobo ; lorsque la personne qui détient le rôle édite un client d'API, il faut vérifier que les rôles ajoutés ne sont pas en dehors de l'OU d'appartenance du rôle de gestion.

Et avec ça un autre bout intéressant : en finir avec les permissions globales dans l'API a2, et au lieu de ça filtrer automatiquement les querysets en fonction des permissions équivalentes par OU détenues par l'appelant.

#8 - 18 novembre 2022 11:46 - Paul Marillonnet

- Lié à Development #71463: api/rbac : au lieu d'une vérification booléenne sur une permission globale, filtrer automatiquement les querysets en fonction des permissions équivalentes par OU détenues par l'appelant ajouté

#9 - 07 décembre 2022 16:28 - Paul Marillonnet

- Fichier 0002-api_views-handle-ou-wise-api-client-checks-71275.patch ajouté

- Fichier 0001-models-add-ou-field-to-api-clients-71275.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Voici ce qu'on pourrait passer pour la partie modèle et adaptation de l'endpoint /check-api-client/, je vais faire un ticket pour la partie /manage/, qu'on discute de ce qu'on peut y faire.

#10 - 07 décembre 2022 16:36 - Paul Marillonnet

- Lié à Development #72151: /manage/ : gérer dans les écrans de clients d'API l'appartenance à une collectivité ajouté

#11 - 09 décembre 2022 11:37 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Je mettrai directement ou comme non-null et valeur par défaut get_default_ou(), aucune raison d'avoir des API client sans OU (on a déjà le souci sur les utilisateurs ne le reproduisons pas ici).

#12 - 09 décembre 2022 12:11 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Je mettrai directement ou comme non-null et valeur par défaut get_default_ou(), aucune raison d'avoir des API client sans OU (on a déjà le souci sur les utilisateurs ne le reproduisons pas ici).

Mais justement je pensais que ces utilisateurs qui n'appartiennent à aucune OU ne vont être atteignables par aucun client d'API réduit à une OU, et que c'est justement la raison pour laquelle il faut tolérer que ces clients puissent ne pas avoir d'OU. Je loupe un truc ? Comment on ferait pour atteindre les utilisateurs sans OU sans cette possibilité APIClient.ou := null ?

#13 - 09 décembre 2022 12:21 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Benjamin Dauvergne a écrit :
>
> > Je mettrai directement ou comme non-null et valeur par défaut get_default_ou(), aucune raison d'avoir des API client sans OU (on a déjà le souci sur les utilisateurs ne le reproduisons pas ici).
>
> Mais justement je pensais que ces utilisateurs qui n'appartiennent à aucune OU ne vont être atteignables par aucun client d'API réduit à une OU, et que c'est justement la raison pour laquelle il faut tolérer que ces clients puissent ne pas avoir d'OU. Je loupe un truc ? Comment on ferait

> pour atteindre les utilisateurs sans OU sans cette possibilité APIClient.ou := null ?

Y a pas de lien entre APIClient.ou et les utilisateurs visibles ou alors je n'ai pas bien lu le patch. Si un APIClient veut voir tous les utilisateurs il faut lui filer la permission globale custom_user.search_user. Pour moi APIClient.ou c'est juste pour compartimenté l'administration des APIClient en BO.

#14 - 13 décembre 2022 13:59 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Y a pas de lien entre APIClient.ou et les utilisateurs visibles ou alors je n'ai pas bien lu le patch. Si un APIClient veut voir tous les utilisateurs il faut lui filer la permission globale custom_user.search_user. Pour moi APIClient.ou c'est juste pour compartimenté l'administration des APIClient en BO.

Ok, cette compartimentation peut être une première étape en effet.
À terme je pense qu'il faudrait tendre vers :

> Il y aurait avec ça un autre patche (dans un futur cycle toujours) pour s'assurer dans le /manage/ qu'un gestionnaire des clients d'API d'une collectivité Lambda ne peut pas aller accorder des rôles avec des permissions globales ni des permissions d'une autre collectivité Gamma, seulement les permissions pour la collectivité Lambda (car c'est la collectivité d'appartenance du rôle de gestion de clients d'API qu'il détient).

(Dans le fil de discussion de la release du 8 décembre).

#15 - 13 décembre 2022 14:49 - Paul Marillonnet

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

```
commit 4240f989ae5f3d7be2773bf8eed3fdb05fe42d17
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Nov 17 10:56:30 2022 +0100

    api_views: handle ou-wise api-client checks (#71275)

commit a7ffb583f830a2649f5703ba0d27435e1d9fe19c
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Nov 17 10:13:53 2022 +0100

    models: add ou field to api clients (#71275)
```

#16 - 13 décembre 2022 16:01 - Paul Marillonnet

- Lié à Bug #72355: tests cassés suite à l'introduction des rôles de gestion des clients d'API par OU dans authentic ajouté

#17 - 13 décembre 2022 16:03 - Paul Marillonnet

- Lié à Development #72354: Buid hobo en erreur suite à changement dans authentic ajouté

#19 - 21 décembre 2022 14:40 - Paul Marillonnet

- Lié à Development #72688: /manage/ : l'écran de gestion des clients d'API doit filtrer en fonction de l'OU du/des rôles de gestion détenus par l'usager ajouté

#20 - 22 décembre 2022 09:49 - Paul Marillonnet

- Lié à Development #72703: /manage/ : l'écran de gestion des clients d'API doit filtrer les rôles ajoutables au client en fonction de l'OU du client d'API ajouté

#21 - 23 décembre 2022 08:44 - Frédéric Péters

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

#22 - 26 février 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0002-api_views-handle-ou-wise-api-client-checks-71275.patch	3,53 ko	07 décembre 2022	Paul Marillonnet
0001-models-add-ou-field-to-api-clients-71275.patch	8,41 ko	07 décembre 2022	Paul Marillonnet