Passerelle - Development #38365

Ajouter un controle d'accès aux endpoints des connecteurs par rôle

10 décembre 2019 18:42 - Emmanuel Cazenave

Statut:	Fermé	**Début:**	10 décembre 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Valentin Deniaud	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Pour éviter le cas typique :

- besoin de tester un endpoint dans un navigateur
- j'ouvre le connecteur à tous vents
- j'oublie de rétablir le contrôle d'accès normal après mon test

Révisions associées

Révision d2d7aaf2 - 12 décembre 2019 10:38 - Valentin Deniaud

utils: authorize admin access to all endpoints (#38365)

Historique

#1 - 11 décembre 2019 15:46 - Valentin Deniaud

- Assigné à mis à Valentin Deniaud

#2 - 11 décembre 2019 17:06 - Valentin Deniaud

- Fichier 0001-base-grant-endpoint-permissions-using-roles-38365.patch ajouté

- Patch proposed changé de Non à Oui

#3 - 11 décembre 2019 17:09 - Frédéric Péters

Je ne sais pas si c'est ça qu'avait en tête Emmanuel; de mon côté j'imaginais simplement permettre l'accès aux endpoints à l'admin, inconditionnellement.

#4 - 11 décembre 2019 17:18 - Valentin Deniaud

Il va dire, mais ça me paraissait sans ambiguïté. Maintenant sûrement que ce que tu proposes est suffisant pour le cas d'usage évoqué, je laisse Manu trancher.

(j'étais en train d'écrire :)

C'est du wip qui wfm™, mais je veux bien un avis sur l'approche avant d'écrire les tests et de fignoler.

Notamment : un contrôle d'accès par rôles, c'est presque pareil qu'un contrôle d'accès par utilisateur d'api. Du coup, c'est un champ qui change dans le modèle, et par ruissellement un changement dans chaque formulaire, dans chaque vues, dans chaque template. Ça crie très fort duplication de code.
Pour la mitiger j'ai rajouté des classes abstraites là où c'était possible. Ma question c'est, est-ce qu'il faut aller plus loin et tout faire dans le modèle AccessRight, en remplaçant apiuser par une GenericForeignKey ? Ça limiterait au max la duplication, mais pas sûr qu'on économise beaucoup de lignes au final (dès qu'il faudra faire de l'affichage on aurait des disjonctions de cas chiantes à gérer, notamment pour le formulaire). Et aussi un code moins facile à lire.

#5 - 11 décembre 2019 17:24 - Frédéric Péters

Ce que je crains avec ce contrôle d'accès par rôle c'est qu'il laisse penser qu'il puisse y avoir vérification du rôle de l'"utilisateur" appelant, "utilisateur" qui serait l'agent dans une démarche dans w.c.s.

#6 - 11 décembre 2019 17:41 - Emmanuel Cazenave

Oups désolé si je t'ai lancé sur une fausse piste Valentin, j'ai mis "rôle" pour faire intelligent mais je pensais juste aux admins, j'aurais du m'abstenir avec ce mot.

L'accès inconditionnels aux admins me parait bien suffisant pour le cas d'usage.

#7 - 12 décembre 2019 01:24 - Thomas Noël

(Pour le coup il n'ose pas le dire, mais c'est moi qui a enduit Valentin d'erreur en causant de ce ticket ce matin)

(Enfin, non, je dis n'importe quoi : c'était hier matin)

#8 - 12 décembre 2019 10:31 - Valentin Deniaud

- Fichier 0001-utils-authorize-admin-access-to-all-endpoints-38365.patch ajouté

#9 - 12 décembre 2019 10:39 - Valentin Deniaud

- Fichier 0001-utils-authorize-admin-access-to-all-endpoints-38365.patch ajouté

#10 - 12 décembre 2019 10:44 - Valentin Deniaud

- Statut changé de Nouveau à Solution proposée

(git redmine a eu la flemme de changer le statut, on dirait)

#11 - 12 décembre 2019 11:08 - Emmanuel Cazenave

- Statut changé de Solution proposée à Solution validée

Yes (pour le prochain cycle).

#12 - 13 décembre 2019 15:56 - Thomas Noël

Un truc ça serait que ça ne marche pas pour les JSONP, mais bon, ça semble pas simple, là, comme ça. (Pour éviter que tout marche bien pour les admin, mais pas pour les agents ou usagers)

#13 - 17 décembre 2019 10:10 - Valentin Deniaud

```
commit d2d7aaf29472ff063f8b052877a2caa6e2b0f48e
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Thu Dec 12 10:20:34 2019 +0100

    utils: authorize admin access to all endpoints (#38365)
```

#14 - 17 décembre 2019 10:10 - Valentin Deniaud

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

#15 - 23 décembre 2019 18:15 - Frédéric Péters

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

Fichiers

0001-base-grant-endpoint-permissions-using-roles-38365.patch	13,3 ko	11 décembre 2019	Valentin Deniaud
0001-utils-authorize-admin-access-to-all-endpoints-38365.patch	1,88 ko	12 décembre 2019	Valentin Deniaud
0001-utils-authorize-admin-access-to-all-endpoints-38365.patch	2,04 ko	12 décembre 2019	Valentin Deniaud