Authentic 2 - Development #20513

Ajouter une permission explicite pour gérer les membres d'un rôle

08 décembre 2017 00:54 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	08 décembre 2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Valentin Deniaud	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Les rôles d'administration des rôles ne devraient pas avoir comme permission admin sur le rôle administré, mais une permission plus fine nommée manager-members.

En plus d'ajouter cette permission et de modifier le code de création des rôles d'administration, il faudra une migration lancée par le signal post_migrate pour corriger tous les rôles d'administration des rôles existants.

Demandes liées:

Lié à Authentic 2 - Bug #20512: BO: le lien de création des rôles s'affiche a...	**Fermé**	**08 décembre 2017**
Lié à Authentic 2 - Development #42086: L'opération d'auto-administration des...	**Fermé**	**24 avril 2020**
Bloque Authentic 2 - Development #37187: manager, affichage/lecture seule pou...	**Fermé**	**24 octobre 2019**

Révisions associées

Révision 599555f3 - 24 avril 2020 11:08 - Valentin Deniaud

a2_rbac: add manage members permission for role admins (#20513)

Révision 3827154e - 24 avril 2020 11:08 - Valentin Deniaud

a2_rbac: update role admins using post_migrate signal (#20513)

Révision adaf0a7d - 24 avril 2020 11:08 - Valentin Deniaud

manager: use new manage_members permission (#20513)

Historique

#1 - 08 décembre 2017 00:55 - Benjamin Dauvergne

- Lié à Bug #20512: BO: le lien de création des rôles s'affiche aux utilisateurs qui ne peuvent administrer qu'un rôle et certainement pas en ajouter ajouté

#2 - 04 octobre 2019 15:37 - Valentin Deniaud

- Assigné à changé de Benjamin Dauvergne à Valentin Deniaud

Je vais essayer de regarder, ça m'avait gêné sur l'auth multi-facteurs et le fix temporaire n'est pas terrible (il se contente de masquer un bouton ie l'admin d'un rôle peut toujours s'amuser à en ajouter en allant direct sur /manage/roles/add).

#3 - 07 octobre 2019 11:11 - Valentin Deniaud

- Fichier 0001-manager-add-manage-members-permission-for-role-admin.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

Déjà la partie qui ajoute la permission, reste la migration.
Le ticket sous-entend un peu qu'elle doit permettre seulement de toucher à la liste des membres, or actuellement être admin d'un rôle permet aussi de le supprimer. C'est désormais trivial de faire autrement, mais je suppose qu'on laisse comme c'est ?

#4 - 07 octobre 2019 12:40 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> Déjà la partie qui ajoute la permission, reste la migration.

> Le ticket sous-entend un peu qu'elle doit permettre seulement de toucher à la liste des membres, or actuellement être admin d'un rôle permet aussi de le supprimer. C'est désormais trivial de faire autrement, mais je suppose qu'on laisse comme c'est ?

Non justement on voudrait que les admins de rôles n'aient plus que le droit de modifier la liste des membres, il faudrait faire en sorte que ça évolue tout seul (je n'ai pas encore lu le patch c'est peut-être déjà le cas) via une migration.

#5 - 07 octobre 2019 15:54 - Valentin Deniaud

- Fichier 0001-manager-add-manage-members-permission-for-role-admin.patch ajouté

- Fichier 0002-a2_rbac-update-role-admins-using-post_migrate-signal.patch ajouté

- Statut changé de En cours à Solution proposée

Modif de settings.py dans le patch 1 pour enlever la permission de supprimer, et ajout du patch 2 avec la migration.

#6 - 14 octobre 2019 11:03 - Lauréline Guérin

Pourquoi faire une migration "à la main" sur un post_migrate, au lieu d'une data migration ?

#7 - 14 octobre 2019 12:00 - Benjamin Dauvergne

Lauréline Guerin a écrit :

> Pourquoi faire une migration "à la main" sur un post_migrate, au lieu d'une data migration ?

J'ai oublié, faisons une data migration.

#8 - 15 octobre 2019 11:24 - Valentin Deniaud

Benjamin Dauvergne a écrit :

> J'ai oublié

Pourrait-ce être parce que les rôles d'administration sont créés par des méthodes custom qui totalisent au final plus d'une centaine de lignes, avec en bonus des branchements conditionnels sur des settings, méthodes auxquelles on a pas accès avec les modèles historiques dans une data migration ? Donc data migration => réécrire plein de code bizarre pour un résultat pas garanti, post_migrate => 20 fois moins de code, 20 fois moins de risque d'erreur.

#9 - 15 octobre 2019 11:41 - Valentin Deniaud

- Fichier 0002-a2_rbac-update-role-admins-using-post_migrate-signal.patch ajouté

- Fichier 0001-manager-add-manage-members-permission-for-role-admin.patch ajouté

En attendant j'ai fixé mon test, ça devrait être bon (merci Lauréline c'était bien le flush le coupable).

#10 - 15 octobre 2019 13:20 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> Benjamin Dauvergne a écrit :
>
> > J'ai oublié
>
> Pourrait-ce être parce que les rôles d'administration sont créés par des méthodes custom qui totalisent au final plus d'une centaine de lignes, avec en bonus des branchements conditionnels sur des settings, méthodes auxquelles on a pas accès avec les modèles historiques dans une data migration ? Donc data migration => réécrire plein de code bizarre pour un résultat pas garanti, post_migrate => 20 fois moins de code, 20 fois moins de risque d'erreur.

Ah oui effectivement sans les Manager customisé ça doit être un peu chiant.

#11 - 20 octobre 2019 00:11 - Benjamin Dauvergne

Un souci dans l'héritage des permissions, quelqu'un qui a manage_members ne devrait pas avoir change; c'est justement l'objectif ici, ne pouvoir changer que les membres et pas le nom du rôle.

Aussi il faudrait vérifier dans le manager :

- que les boutons permissions et éditer sur la page d'un rôle ne sont plus disponible quand on est juste administrateur d'un rôle

- qu'on peut toujours :
  - faire hériter des membres d'un autre rôle X un rôle Y quand on est administrateur du rôle Y
  - faire hériter des permissions d'un rôle X un rôle Y quand on est administrateur du rôle X

#12 - 21 octobre 2019 18:15 - Valentin Deniaud

Je fais ça. Comme tu ne les as pas incluses dans ta liste je suppose que les deux autres options sous « paramètres avancés », c'est à dire ajouter un administrateur au rôle et ajouter un rôle administrateur, doivent elles aussi être inaccessibles, dis moi si j'ai pas bon.

#13 - 21 octobre 2019 19:49 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> Je fais ça. Comme tu ne les as pas incluses dans ta liste je suppose que les deux autres options sous « paramètres avancés », c'est à dire ajouter un administrateur au rôle et ajouter un rôle administrateur, doivent elles aussi être inaccessibles, dis moi si j'ai pas bon.

Yep, ça aussi c'est réservé à la permission change.

#14 - 22 octobre 2019 11:21 - Valentin Deniaud

> - qu'on peut toujours :
>   - faire hériter des membres d'un autre rôle X un rôle Y quand on est administrateur du rôle Y
>   - faire hériter des permissions d'un rôle X un rôle Y quand on est administrateur du rôle X

Plot twist, ça n'a jamais marché, en tout cas dans l'interface (la permission admin d'un rôle telle qu'elle existe actuellement ne donnant pas le droit de lister les rôles).

Donc ajouter un view_role_perm de manière analogue à view_user_perm dans a2_rbac.models.Role.get_admin_role ?

#15 - 22 octobre 2019 12:33 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> > - qu'on peut toujours :
> >   - faire hériter des membres d'un autre rôle X un rôle Y quand on est administrateur du rôle Y
> >   - faire hériter des permissions d'un rôle X un rôle Y quand on est administrateur du rôle X
>
> Plot twist, ça n'a jamais marché, en tout cas dans l'interface (la permission admin d'un rôle telle qu'elle existe actuellement ne donnant pas le droit de lister les rôles).
> Donc ajouter un view_role_perm de manière analogue à view_user_perm dans a2_rbac.models.Role.get_admin_role ?

Ce n'est pas gênant pour ce ticket, dans les faits soit on est administrateur de tous les rôles d'un OU ou d'un a2 complet, soit on est juste administrateurs des membres d'un rôle. Le cas administrateur de tout sur un seul rôle n'a pas de sens.

Mais donc juste pour savoir que c'est couvert pour plus tard il y aurait à tester :

- j'ai la permission role_admin sur tout une OU U1
  - je peux tout faire
- j'ai la permission role_manage_members sur un rôle R1 de l'OU U1:
  - je vois bien ce rôle dans le listing des rôles
  - je vois les utilisateurs de U1 et je peux les affecter/retirer de R1
  - si j'ai la visibilité sur un rôle R2 (donnée fortuitement sur le test):
    - je peux hériter de ses membres sur la page d'administration de R1
    - je peux hériter de ses permissions sur la page d'administration de R2

On pourra réfléchir à view_role_perm sur un autre ticket je pense.

#16 - 22 octobre 2019 18:04 - Valentin Deniaud

- Fichier 0004-manager-use-new-manage_members-permission-20513.patch ajouté

- Fichier 0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch ajouté

- Fichier 0002-a2_rbac-add-manage-members-permission-for-role-admin.patch ajouté

- Fichier 0001-Revert-manager-do-not-use-has_any_perm-to-get-add-pe.patch ajouté

OK je comprends pourquoi ça marche comme ça. Voici donc un nouveau patch avec le boulot dans le manager et les tests. Pas de changement autre part si ce n'est faire hériter les permissions change et admin de manage_members. J'ai aussi réorganisé les commits parce que je commençais à m'y perdre.

En passant, je suis pas fan de la sécurité « par l'affichage » (en l'état ça permet pas exemple d'hériter des membres d'un rôle x qu'on a pas le droit de voir si on en connaît l'id, ou plus grave d'hériter de ses permissions), mais je ne vais pas y toucher dans ce ticket sauf indication contraire.

- j'ai la permission role_admin sur tout une OU U1
  - je peux tout faire

Pas compris ce que ça avait à voir là dedans ?

#17 - 22 octobre 2019 19:58 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> OK je comprends pourquoi ça marche comme ça. Voici donc un nouveau patch avec le boulot dans le manager et les tests. Pas de changement autre part si ce n'est faire hériter les permissions change et admin de manage_members. J'ai aussi réorganisé les commits parce que je commençais à m'y perdre.

Ok je vais relire ça.

> En passant, je suis pas fan de la sécurité « par l'affichage » (en l'état ça permet pas exemple d'hériter des membres d'un rôle x qu'on a pas le droit de voir si on en connaît l'id, ou plus grave d'hériter de ses permissions), mais je ne vais pas y toucher dans ce ticket sauf indication contraire.

Normalement non mais je veux bien que tu montres que c'est possible, il y a revalidation de l'id soumi par rapport au queryset qui le restreint.

> - j'ai la permission role_admin sur tout une OU U1
>   - je peux tout faire
>
> Pas compris ce que ça avait à voir là dedans ?

Rien, juste si le test n'existe pas encore c'était l'occasion de l'avoir parce que c'est dans le même style.

#18 - 24 octobre 2019 17:55 - Valentin Deniaud

Pendant que j'y pense, le dernier patch qui modifie le manager est incomplet, je n'ai pas fait le tour des vues qui permettent de modifier les membres d'un rôle (typiquement celles dans /manage/users/). Les ajouts seront mineurs, je laisse en Solution Proposée.

#19 - 29 octobre 2019 11:20 - Valentin Deniaud

- Fichier 0004-manager-use-new-manage_members-permission-20513.patch ajouté

Complété.

#20 - 30 octobre 2019 10:56 - Benjamin Dauvergne

Il y a un truc que je ne comprends pas dans ce code :

```
        old_perm = role.permissions.get(operation__slug=ADMIN_OP.slug)
        administered_role = old_perm.target
        admin_role = administered_role.get_admin_role()
        new_perm = admin_role.permissions.get(operation__slug=MANAGE_MEMBERS_OP.slug)
        role.permissions.remove(old_perm)
        role.permissions.add(new_perm)
```

en tout logique on devrait avoir admin_role == role, sinon .get_admin_role() a un souci non ?
Je trouverai utile d'avoir des assert ici pour en être sûr.

Ok pour le reste.

#21 - 30 octobre 2019 17:13 - Valentin Deniaud

- Fichier 0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch ajouté

Ah oui, gros bug. get_admin_role récupère ou crée le rôle à partir de la permission (admin_role = get_mirror_role(perm, ...)) donc nouvelle permission ==> nouveau rôle. Et moi je me contente d'affecter la nouvelle permission à l'ancien rôle, donc ça marche sauf que les administrateurs passés et futurs n'auront pas le même rôle (mais les mêmes permissions, ça aurait pas été drôle à débugger).

Le fix, pas compliqué :

```
          admin_role = administered_role.get_admin_role()
          new_perm = admin_role.permissions.get(operation__slug=MANAGE_MEMBERS_OP.slug)
+         admin_role.delete()
+         role.admin_scope_id = new_perm.pk
+         role.save()
          role.permissions.remove(old_perm)
          role.permissions.add(new_perm)
+         assert role.pk == administered_role.get_admin_role().pk
```

#22 - 18 novembre 2019 16:57 - Valentin Deniaud

- Bloque Development #37187: manager, affichage/lecture seule pour les rôles pilotés depuis un annuaire LDAP ajouté

#23 - 20 avril 2020 17:33 - Valentin Deniaud

- Fichier 0004-manager-use-new-manage_members-permission-20513.patch ajouté

- Fichier 0002-a2_rbac-add-manage-members-permission-for-role-admin.patch ajouté

- Fichier 0001-Revert-manager-do-not-use-has_any_perm-to-get-add-pe.patch ajouté

- Fichier 0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch ajouté

- Tracker changé de Bug à Development

#24 - 20 avril 2020 17:34 - Valentin Deniaud

(rebasé)

#25 - 20 avril 2020 17:59 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Je rajouterai un atomic autour de @update_user_admin_roles_permission par sécurité, sinon c'est tout bon. À pousser vendredi.

#26 - 22 avril 2020 15:31 - Valentin Deniaud

Yep, branche à jour.

#27 - 24 avril 2020 11:11 - Valentin Deniaud

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

```
commit adaf0a7d7be4a873c4665e0c9ebd609e1d1b4766
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Oct 22 17:30:57 2019 +0200

    manager: use new manage_members permission (#20513)

commit 3827154e76c8a37225324008bb0755c9d24bd177
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Mon Oct 7 15:50:21 2019 +0200

    a2_rbac: update role admins using post_migrate signal (#20513)

commit 599555f3cb1363eb6fafb0c24f67bd723565c98b
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Oct 22 17:31:37 2019 +0200

    a2_rbac: add manage members permission for role admins (#20513)

commit d9f387a115db9b3bc96a6e1d60606ee55a11e625
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Oct 22 17:30:37 2019 +0200

    Revert "manager: do not use has_any_perm() to get add permission on roles (fixes #20512)"

    This reverts commit 1972076bfd4f69cf1bb277ce59b19a802b0a7a40.
```

#28 - 24 avril 2020 16:43 - Benjamin Dauvergne

- Lié à Development #42086: L'opération d'auto-administration des rôles devrait être MANAGE_MEMBERS_OP pas CHANGE_OP ajouté

#29 - 28 avril 2020 00:16 - Frédéric Péters

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

Fichiers

0001-manager-add-manage-members-permission-for-role-admin.patch	5,82 ko	07 octobre 2019	Valentin Deniaud
0002-a2_rbac-update-role-admins-using-post_migrate-signal.patch	4,8 ko	07 octobre 2019	Valentin Deniaud
0001-manager-add-manage-members-permission-for-role-admin.patch	5,81 ko	07 octobre 2019	Valentin Deniaud
0002-a2_rbac-update-role-admins-using-post_migrate-signal.patch	4,67 ko	15 octobre 2019	Valentin Deniaud
0001-manager-add-manage-members-permission-for-role-admin.patch	5,87 ko	15 octobre 2019	Valentin Deniaud
0004-manager-use-new-manage_members-permission-20513.patch	9,94 ko	22 octobre 2019	Valentin Deniaud
0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch	4,64 ko	22 octobre 2019	Valentin Deniaud
0002-a2_rbac-add-manage-members-permission-for-role-admin.patch	3,73 ko	22 octobre 2019	Valentin Deniaud
0001-Revert-manager-do-not-use-has_any_perm-to-get-add-pe.patch	1,02 ko	22 octobre 2019	Valentin Deniaud
0004-manager-use-new-manage_members-permission-20513.patch	11,8 ko	29 octobre 2019	Valentin Deniaud
0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch	4,8 ko	30 octobre 2019	Valentin Deniaud
0004-manager-use-new-manage_members-permission-20513.patch	11,9 ko	20 avril 2020	Valentin Deniaud
0002-a2_rbac-add-manage-members-permission-for-role-admin.patch	3,73 ko	20 avril 2020	Valentin Deniaud
0001-Revert-manager-do-not-use-has_any_perm-to-get-add-pe.patch	1,02 ko	20 avril 2020	Valentin Deniaud
0003-a2_rbac-update-role-admins-using-post_migrate-signal.patch	4,84 ko	20 avril 2020	Valentin Deniaud