Authentic 2 - Development #37187

manager, affichage/lecture seule pour les rôles pilotés depuis un annuaire LDAP

24 octobre 2019 11:42 - Frédéric Péters

Statut:	Fermé	**Début:**	24 octobre 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Valentin Deniaud	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	ticket facile		
Patch proposed:	Oui	**Planning:**	Non

Description

Pour un rôle qui se trouve mentionné dans LDAP_AUTH_SETTINGS/group_to_role_mapping on devrait afficher un message disant que le rôle est synchronisé depuis l'annuaire LDAP et ne pas permettre l'ajout/retrait de membres.

Demandes liées:

Bloqué par Authentic 2 - Development #20513: Ajouter une permission explicite...	**Fermé**	**08 décembre 2017**

Révisions associées

Révision 0d8ea42a - 02 juin 2020 12:04 - Valentin Deniaud

manager: forbid changing role members when synced from ldap (#37187)

Historique

#2 - 24 octobre 2019 14:40 - Benjamin Dauvergne

- Version cible mis à ticket facile

#3 - 29 octobre 2019 12:02 - Valentin Deniaud

Benjamin, tu imagines vérifier à la volée si un rôle est dans le mapping ? Ça se fait probablement de manière assez légère dans PermissionMixin, si on veut bien se contenter de planquer les boutons.
Un peu dommage par contre que le mapping soit de la forme [['dn', ['role1', 'role2']], ...] au lieu de {'dn': ('role1', 'role2'), ...}, ça fera pas un check très joli. Si c'est en prod à peu d'endroit et que le changer est envisageable...

#4 - 29 octobre 2019 16:47 - Benjamin Dauvergne

La plupart des déploiements n'ont pas de mapping et quand il y en a il n'y en a qu'un, donc oui un truc assez moche :

```
if any(role.name in mapping[1] for mapping in getattr(settings, 'LDAP_SETTINGS', {}).get('group_to_role_mappin
g', [])):
    show_warning()
```

qu'on enlèvera le jour où on saura faire plus propre.

#5 - 14 novembre 2019 18:03 - Valentin Deniaud

- Assigné à mis à Valentin Deniaud

#6 - 18 novembre 2019 16:56 - Valentin Deniaud

- Fichier 0001-manager-prevent-changing-ldap-sychronised-role-affec.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

Pas si droit devant au final, il y a deux vues impactées, /manage/roles/x/ et /manage/users/y/roles/, avec la dernière qui se subdivise en deux. Tout n'est pas gérable simplement à un endroit comme j'imaginais.

Pour traiter la première j'aimerais bien la permission manage-members de #20513 (à moins qu'on veuille aussi bloquer l'édition du rôle ?). Je joins quand même le patch incomplet, pour info.

#7 - 18 novembre 2019 16:57 - Valentin Deniaud

- Bloqué par Development #20513: Ajouter une permission explicite pour gérer les membres d'un rôle ajouté

#8 - 10 décembre 2019 16:14 - Valentin Deniaud

- Fichier 0002-manager-prevent-changing-ldap-sychronised-role-affec.patch ajouté

- Fichier 0001-manager-fix-typo-37187.patch ajouté

- Statut changé de En cours à Solution proposée

En utilisant manage_members ajouté dans #20513, donc.

#9 - 20 avril 2020 17:33 - Valentin Deniaud

- Fichier 0002-manager-prevent-changing-ldap-sychronised-role-affec.patch ajouté

- Fichier 0001-manager-fix-typo-37187.patch ajouté

Rebasé.

#10 - 20 avril 2020 18:21 - Benjamin Dauvergne

Tu n'y es pour rien mais au final c'est super moche et difficilement maintenable, je ne sais pas pourquoi j'ai mis ticket facile. On se retrouve déjà avec des histoires de 'manage_members' dans une vue sensée être générique et maintenant des histoires de LDAP.

Je propose une autre voie qui servira aussi à faire disparaître les slugs à la con genre _a2-bidule ou _hobo-machin: avoir différents flags sur les rôles pour restreindre les permissions ou leur visibilité[1].

Ici on aurait un flag can_manage_members=True par défaut, qui serait mis à False dès qu'un rôle devient synchronisé par LDAP (à terme on arrêtera de synchroniser un rôle existant, on synchronisera des requêtes LDAP vers des trucs liés au LDAP dont un rôle normal héritera).

Coté LDAP ça reviendrait à poser :

```
    if role.can_manage_members:
        logger.info('role %s is now only manageable tourgh LDAP', role)
        role.can_mamage_members = False
        role.save()
```

et coté vue des rôles, poser un accesseur sur les vues d'affichage et des gestion des membres et de l'héritage :

```
    @cached_
    def can_manage_members(self):
        return self.object.can_manage_members and self.request.user.has_perm(self.object, 'a2_rbac.role_manage_
members')
```

Et utiliser object.can_manage_members pour afficher le warning This role's members are managed elsewhere (LDAP). qu'on étendra ou améliorera où on aura un cas qui n'est pas LDAP.

[1] On pourrait avoir aussi visible pour les rôles purement techniques qui n'auraient même pas de slug ou de nom ou can_edit pour les rôles créer automatiquement mais dont on doit pas toucher aux nom et slug (genre "Administrateur du service <service>"; il faudrait rendre plus de chose explicites et ne plus jamais se baser sur la forme du slug.

#11 - 20 avril 2020 18:22 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

#12 - 27 mai 2020 16:13 - Valentin Deniaud

- Fichier 0001-manager-forbid-changing-role-members-when-synced-fro.patch ajouté

- Statut changé de En cours à Solution proposée

Plus propre, y a pas à dire.

#13 - 27 mai 2020 16:27 - Frédéric Péters

- Fichier Screenshot_2020-05-27 Authentic.png ajouté

(commentaire fait à partir d'une lecture du patch)

Ça peut être affiché plus visiblement que "caché" en tooltip ? (capture exemple attachée)

#14 - 27 mai 2020 16:40 - Valentin Deniaud

Frédéric Péters a écrit :

> Ça peut être affiché plus visiblement que "caché" en tooltip ? (capture exemple attachée)

Je fais ça (note quand même que les boutons pour ajouter/supprimer un utilisateur ne sont plus non plus affichés).

#15 - 28 mai 2020 12:04 - Valentin Deniaud

- Fichier 0001-manager-forbid-changing-role-members-when-synced-fro.patch ajouté

#16 - 29 mai 2020 14:47 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Tardif (désolé): tu pourrais renommer manage_members_allowed en can_manage_members ?

#17 - 02 juin 2020 12:05 - Valentin Deniaud

J'aime pas trop le nom mais OK, je pousse quand c'est vert.

#18 - 02 juin 2020 13:59 - Valentin Deniaud

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

```
commit 0d8ea42ad245d831ab11445502cb8a170f69d08b
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue May 26 17:53:35 2020 +0200

    manager: forbid changing role members when synced from ldap (#37187)
```

#19 - 02 juin 2020 18:56 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> J'aime pas trop le nom mais OK, je pousse quand c'est vert.

Je ne suis pas fan du nom non plus mais c'est pour rester cohérent avec les accesseurs sur les vues et ailleurs.

#20 - 05 juin 2020 09:16 - Frédéric Péters

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

Fichiers

0001-manager-prevent-changing-ldap-sychronised-role-affec.patch	6,96 ko	18 novembre 2019	Valentin Deniaud
0002-manager-prevent-changing-ldap-sychronised-role-affec.patch	8,29 ko	10 décembre 2019	Valentin Deniaud
0001-manager-fix-typo-37187.patch	1,23 ko	10 décembre 2019	Valentin Deniaud
0002-manager-prevent-changing-ldap-sychronised-role-affec.patch	8,29 ko	20 avril 2020	Valentin Deniaud
0001-manager-fix-typo-37187.patch	1,23 ko	20 avril 2020	Valentin Deniaud
0001-manager-forbid-changing-role-members-when-synced-fro.patch	8,82 ko	27 mai 2020	Valentin Deniaud
Screenshot_2020-05-27 Authentic.png	20,5 ko	27 mai 2020	Frédéric Péters
0001-manager-forbid-changing-role-members-when-synced-fro.patch	10,1 ko	28 mai 2020	Valentin Deniaud