

Chrono - Development #48367

Faire une page de refus d'accès au lieu de retourner une 403

06 novembre 2020 15:00 - Mikaël Ates

Statut:	Fermé	Début:	06 novembre 2020
Priorité:	Normal	Echéance:	
Assigné à:	Nicolas Roche	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		
Description			
Il se peut que l'utilisateur arrive sur le backoffice chrono alors qu'il n'a pas de droit d'accès. Plutôt que de retourner une 403 moche, il faudrait afficher une page indiquant "Aucun agenda accessible" (et aucun bouton).			
Demandes liées:			
Lié à Gadjo - Development #48826: Ajout d'une classe big-msg-sorry		Fermé	25 novembre 2020

Révisions associées

Révision ef55e9de - 11 décembre 2020 15:55 - Nicolas Roche

manager: set a dedicated 403 response on home page (#48367)

Historique

#1 - 06 novembre 2020 15:00 - Mikaël Ates

- *Projet changé de Combo à Chrono*

#2 - 20 novembre 2020 17:58 - Nicolas Roche

- *Fichier 0001-manager-add-a-403-error-page-48367.patch ajouté*
- *Statut changé de Nouveau à Solution proposée*
- *Assigné à mis à Nicolas Roche*
- *Patch proposed changé de Non à Oui*

#3 - 20 novembre 2020 18:04 - Frédéric Péters

Je pense qu'il faudrait travailler le rendu et le texte de la page pour 1/ correspondre aux pages normales au niveau du titre notamment, 2/ pour exprimer de manière moins cash qu'il n'y a pas d'agenda disponible visible pour l'utilisateur.

#4 - 20 novembre 2020 18:39 - Nicolas Roche

- *Fichier 0001-manager-add-a-403-error-page-48367.patch ajouté*

(yep, merci Fred, je ne suis vraiment pas inspiré pour le message)

#5 - 20 novembre 2020 19:08 - Frédéric Péters

Bon, faut pas inventer un h4 ici; je serais plutôt pour <https://styleguide.entrouvert.com/motifs/etat-initial-vide/> (j'en verrais même peut-être une variation avec l'icône remplacée par un : () ; et côté message ne pas écrire "for current user", écrire un message qui s'adresse gentiment à lui, façon "Cet écran reprend les agendas que vous pouvez consulter. Malheureusement il n'y en a aucun configuré pour le moment.". (gentiment pousser ça comme non pas une erreur de navigation de l'utilisateur mais une erreur de configuration qui n'est pas sa faute).

#6 - 23 novembre 2020 15:47 - Nicolas Roche

- *Fichier 0001-manager-add-a-403-error-page-48367.patch ajouté*
- *Statut changé de Solution proposée à En cours*

Patch qui reprend <https://styleguide.entrouvert.com/motifs/etat-initial-vide/>

J'ai mis le texte en anglais mais je pensais à ça en français :
"Cet écran reprend les agendas que vous pouvez consulter.
Malheureusement, il n'y en a encore aucun de configuré pour qu'il vous soit accessible."

j'en verrais même peut-être une variation avec l'icône remplacée par un :(

Il s'agirait de faire un ticket lié dans gadjo,

- qui utilise le smiley fa-frown-o ("f119") de la fonte awesome,
- et de dériver le style "infonotice" (pour pas inventer un nouveau truc) ?

#7 - 23 novembre 2020 16:14 - Frédéric Péters

- Fichier Screenshot_2020-11-23 Chrono - dsd.png ajouté

qui utilise le smiley fa-frown-o ("f119") de la fonte awesome,

Pour l'icône d'info on a une vraie image, on peut pour moi faire pareil ici et ça pourra être plus élégant; genre dans l'idée rapidement fait la capture attachée. (et oui côté classe ça serait un big-msg-sorry comme on a big-msg-nfo).

#8 - 25 novembre 2020 12:05 - Nicolas Roche

- Lié à Development #48826: Ajout d'une classe big-msg-sorry ajouté

#9 - 25 novembre 2020 12:08 - Nicolas Roche

- Fichier 0001-manager-add-a-403-error-page-48367.patch ajouté

- Statut changé de En cours à Solution proposée

Est-ce qu'il faut que je revienne à la ligne entre les deux phrases ?
(je n'ai pas trouvé comment le faire proprement)

#10 - 29 novembre 2020 10:29 - Frédéric Péters

Le message est adapté à la page d'accueil, pas pour une erreur qui apparaîtrait ailleurs; je pense qu'il faut modifier le urls.py de la racine pour passer de manager_required à login_required et modifier le HomepageView pour faire le contrôle d'accès, et si aucun agenda disponible, que le big-msg-sorry soit affiché (idéalement avec un status_code 403 mais ça devient un détail).

(aussi, bien vérifier que les accès sur toutes les vues sont contrôlés mais ça doit déjà être le cas).

#11 - 02 décembre 2020 18:21 - Nicolas Roche

- Fichier 0003-manager-remove-manager_required-decorated-include-fo.patch ajouté

- Fichier 0002-manager-add-a-403-error-page-48367.patch ajouté

- Fichier 0001-tests-correct-role-assignation-on-a-test-48367.patch ajouté

0001: au passage j'ai corrigé un test

0002:

J'ai fait le tour des urls de /manage/. Mis à part '/manage/agendas/events.csv' qui fourni publiquement un exemple du format des événements à importer, je n'ai rien vu qui ne soit pas contrôlé.

Pour le template 403 de base j'ai mis ce message :

```
Forbidden access, sorry.  
Some configuration should be set if you need to access this page.
```

J'ai inclus le message discuté plus haut pour les utilisateurs qui arrivent sur la page d'accueil sans avoir accès à aucun calendrier, directement dans le template de la vue. Et pour renvoyer une 403, j'ai redéfini django/views/generic/list.py::BaseListView:get()

J'ai appliqué la même modification aux agendas d'indisponibilités.

J'ai du corriger 3 tests :

- test_agenda_day_view et test_virtual_agenda_day_view parce que l'on fait 2 requêtes SQL de moins (j'ai pas cherché à comprendre).
- test_unavailability_calendar_homepage_permission qui utilise le bouton d'action présent sur la page d'accueil, qui à présent est retournée (à l'identique) en 403.

0003: Je ne sais pas si je dois ou non supprimer le code de manager_required (qui n'est plus utilisé) car je me dis que ça pourrait resservir.

#12 - 02 décembre 2020 18:26 - Frédéric Péters

Pour le template 403 de base j'ai mis ce message :

Je me dis que celui-là pourrait être distribué par Gadjó, et suffisamment générique pour marcher partout.

J'ai appliqué la même modification aux agendas d'indisponibilités.

Pour moi là on est déjà sur une page à l'intérieur, on peut aller sur l'erreur générique.

0003: Je ne sais pas si je dois ou non supprimer le code de `manager_required` (qui n'est plus utilisé) car je me dis que ça pourrait resservir.

Oui supprimons le code mort; il continuera de toute façon à exister dans l'historique.

#13 - 03 décembre 2020 11:59 - Nicolas Roche

- Fichier `0004-manager-add-a-403-error-page-48367.patch` ajouté
- Fichier `0003-manager-keep-a-403-error-on-unavailability-calendars.patch` ajouté
- Fichier `0002-manager-set-a-didicated-403-response-on-home-page-48.patch` ajouté
- Statut changé de *Solution proposée* à *Information nécessaire*

0002 : message adapté sur la page d'accueil (remarques prises en compte)

Pour moi là on est déjà sur une page à l'intérieur, on peut aller sur l'erreur générique.

0003: corrige la régression sur `/manage/unavailability-calendars/` afin de continuer à retourner une 403 pour les utilisateurs qui n'ont pas de droits sur les agendas indisponibilité.

Je me dis que celui-là pourrait être distribué par Gadjó

~~0004 : template 403 qui inclut un message générique posé sur gadjo.~~

Parce qu'un template 403 chargé directement sur gadjo ne ferait pas apparaître le titre. (cf <https://dev.entrouvert.org/issues/48367#note-3>)

Le template gadjo ressemblerait à ça :

```
{% load i18n %}

<div class="big-msg-sorry">
  <p>{% trans 'Forbidden access, sorry.' %}</p>
  <p>{% trans 'Some configuration should be set if you need to access this page.' %}</p>
</div>
```

Dites-moi si ça conviendrait, que je crée le ticket lié dans gadjo, et éventuellement que je déplace 0004 dans un nouveau ticket (pour pouvoir faire tourner les tests ici).

#14 - 03 décembre 2020 12:13 - Frédéric Péters

Parce qu'un template 403 chargé directement sur gadjo ne ferait pas apparaître le titre

On s'en foutrait.

#15 - 03 décembre 2020 12:38 - Nicolas Roche

- Statut changé de *Information nécessaire* à *Solution proposée*

Yep. En fait j'ai l'impression qu'il faudra de toute façon poser un template 403 dans chrono pour pouvoir charger celui de gadjo. Quoi qu'il en soit, je réalise que 0004 n'a pas sa place ici, je le retire.

#16 - 11 décembre 2020 14:09 - Frédéric Péters

- Statut changé de *Solution proposée* à *Solution validée*

Je serais pour réunir tout ça en un seul patch, corriger "dicated" en "dedicated" dans l'intitulé, et ça sera ok.

#17 - 11 décembre 2020 15:56 - Nicolas Roche

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

```
commit ef55e9de5680beccb37a2f31650d3fd39e0eeda0
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date: Thu Dec 3 10:54:56 2020 +0100
```

```
manager: set a dedicated 403 response on home page (#48367)
```

#18 - 18 décembre 2020 17:17 - Frédéric Péters

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

Fichiers

0001-manager-add-a-403-error-page-48367.patch	1,79 ko	20 novembre 2020	Nicolas Roche
0001-manager-add-a-403-error-page-48367.patch	1,89 ko	20 novembre 2020	Nicolas Roche
0001-manager-add-a-403-error-page-48367.patch	1,99 ko	23 novembre 2020	Nicolas Roche
Screenshot_2020-11-23 Chrono - dsd.png	14,7 ko	23 novembre 2020	Frédéric Péters
0001-manager-add-a-403-error-page-48367.patch	1,99 ko	25 novembre 2020	Nicolas Roche
0003-manager-remove-manager_required-decorated-include-fo.patch	1,74 ko	02 décembre 2020	Nicolas Roche
0002-manager-add-a-403-error-page-48367.patch	12,3 ko	02 décembre 2020	Nicolas Roche
0001-tests-correct-role-assignation-on-a-test-48367.patch	1,06 ko	02 décembre 2020	Nicolas Roche
0004-manager-add-a-403-error-page-48367.patch	1,83 ko	03 décembre 2020	Nicolas Roche
0003-manager-keep-a-403-error-on-unavailability-calendars.patch	2,33 ko	03 décembre 2020	Nicolas Roche
0002-manager-set-a-dicated-403-response-on-home-page-48.patch	10,3 ko	03 décembre 2020	Nicolas Roche