w.c.s. - Bug #60665

Perte du jeton data_source_query_info entre formulaire et API autocomplete

14 janvier 2022 11:17 - Benjamin Dauvergne

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

Description

Cf. ticket client #60659

À l'arrivée sur un formulaire de soumission backoffice, un champ liste à choix en autocomplétion vers une vue personnalisée sur des fiches répond "Les résultats ne peuvent pas être chargés" résultant d'une 403 de l'API autocomplete.

Le seule cas de 403 dans le code c'est ça :

```
class AutocompleteDirectory(Directory):
    def _q_lookup(self, component):
        info = get_session().get_data_source_query_info_from_token(component)
        if not info:
            raise AccessForbiddenError()
```

Ça ressemble furieusement aux soucis d'écrasement de session (perte du user_id #58168 par exemple, m'enfin on peut perdre un peu n'importe quoi qui a été écrit en session lors d'écritures concurrentes), vu que la communication du jeton entre l'ouverture de la page du formulaire et l'API autocomplete passe par celle-ci (la session). Comme pour les autres cas je suggérerai de ne pas stocker ça en session mais dans une table à part session_tokens avec une ligne par jeton, sauf à trouver une solution magique.

Révisions associées

Révision 65eb70f4 - 28 janvier 2022 09:22 - Frédéric Péters

misc: move password token info into a context dictionary (#60665)

(this is to match email action token, before going sql)

Révision fc0b120b - 28 janvier 2022 09:22 - Frédéric Péters

misc: move tokens to an SQL table (#60665)

Révision 49bdcd2e - 28 janvier 2022 09:22 - Frédéric Péters

tokens: add job to clean expired tokens (#60665)

Révision b05cb6ed - 28 janvier 2022 09:22 - Frédéric Péters

misc: remove explicit handling of account-confirmation token expiration (#60665)

Révision 940c4066 - 28 janvier 2022 09:22 - Frédéric Péters

misc: use tokens to store autocompletion context (#60665)

Historique

#2 - 14 janvier 2022 12:08 - Frédéric Péters

- Assigné à mis à Frédéric Péters

> dans une table à part session_tokens

Plutôt migrer le jeton vers wcs/qommon/tokens.py qui est déjà prévu pour être "jeton générique". Peut-être après un autre ticket qui en ferait la

migration SQL; je regarderai ça.

#3 - 14 janvier 2022 21:40 - Benjamin Dauvergne

- Tracker changé de Development à Bug

#4 - 14 janvier 2022 21:45 - Benjamin Dauvergne

- Lié à Development #60693: Déplacer le stockage de wcs.qommon.tokens.Token en base SQL ajouté

#5 - 14 janvier 2022 21:47 - Frédéric Péters

- Lié à Development #60693: Déplacer le stockage de wcs.qommon.tokens.Token en base SQL supprimé

#6 - 14 janvier 2022 21:51 - Benjamin Dauvergne

À regarder Token je ne vois rien d'intéressant à reprendre autant partir sur une table et une classe spécifique et ne pas s'embêter à trouver quelque chose de commun.

#7 - 15 janvier 2022 09:48 - Frédéric Péters

(je me suis assigné le ticket)

#8 - 17 janvier 2022 14:37 - Frédéric Péters

- % réalisé changé de 100 à 0

#9 - 18 janvier 2022 18:00 - Frédéric Péters

- Fichier 0005-misc-use-tokens-to-store-autocompletion-context-6066.patch ajouté

- Fichier 0004-misc-remove-explicit-handling-of-account-confirmatio.patch ajouté

- Fichier 0003-tokens-add-job-to-clean-expired-tokens-60665.patch ajouté

- Fichier 0002-misc-move-tokens-to-an-SQL-table-60665.patch ajouté

- Fichier 0001-misc-move-password-token-info-into-a-context-diction.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

0001 pour modifier la manière dont le jeton est utilisé pour diverses actions dans la gestion native des utilisateurs de w.c.s.; ça déplace les infos dans un dictionnaire "context" pour correspondre à ce qui est fait côté "actions emails". Il n'y a pas de migration des données parce qu'on n'utilise pas cette gestion dans Publik.

0002 pour déplacer le stockage dans la db; pour avoir quelque chose de vraiment propre ça modifie aussi l'expiration pour être un datetime avec timezone. (plutôt qu'un timestamp).

0003 pour ajouter un job pour supprimer les vieux jetons, ça n'existe actuellement pas et j'ai vu un répertoire avec 200000+ fichiers. Il y a migration des données parce que des liens d'action dans les emails doivent continuer à fonctionner.

0004 pour retirer la gestion de l'expiration sur les jetons utilisés pour la confirmation de la création de compte dans la gestion native des utilisateurs.

0005 pour arriver à ce ticket et utiliser ces jetons plutôt que des entrées dans la session. Le patch est en partie chargé par des modifications d'indentation dans data_sources.py

#10 - 18 janvier 2022 21:24 - Benjamin Dauvergne

Dans le système actuel les jetons pour l'autocomplete ont pour durée de vie celle de la session, dans celui-ci c'est fixé à une heure indépendamment de la session, c'est un changement de comportement inutile je pense, autant fixer une durée qui dépasse celle des sessions par défaut pour éviter cela, ces jetons ne coûtent rien.

PS: la durée de vie max des sessions par défaut c'est 30j ou 3j sans accès; mais c'est bloqué par la partie SAML qui récupère le sessionNotOnOrAfter par défaut à 8h coté authentic; on peut mettre 3j pour tenir compte des formulaires soumis anonymement.

#11 - 21 janvier 2022 18:34 - Frédéric Péters

Poussé dans la branche avec pas d'expiration explicite et donc l'expiration par défaut à un jour des jetons, supérieure à SESSION_COOKIE_AGE = 36000 qu'on a par défaut.

#12 - 22 janvier 2022 10:01 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#13 - 28 janvier 2022 09:22 - Frédéric Péters

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

```
commit 940c4066d6818369c546b8e7dd7ede96a201d521
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Mon Jan 17 17:50:11 2022 +0100

    misc: use tokens to store autocompletion context (#60665)

commit b05cb6ed2aaab40bf6bb68e5b88df66d8b2c260d
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Tue Jan 18 10:00:06 2022 +0100

    misc: remove explicit handling of account-confirmation token expiration (#60665)

commit 49bdcd2eba94f8898f9cf3c73454286787849ccd
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Mon Jan 17 18:09:23 2022 +0100

    tokens: add job to clean expired tokens (#60665)

commit fc0b120b2fe533351b270a635d9986342553570c
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Mon Jan 17 16:00:27 2022 +0100

    misc: move tokens to an SQL table (#60665)

commit 65eb70f47a3e96c0757e70aed973d1e31d27b73b
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Mon Jan 17 14:46:38 2022 +0100

    misc: move password token info into a context dictionary (#60665)

    (this is to match email action token, before going sql)
```

#14 - 28 janvier 2022 16:16 - Frédéric Péters

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

#15 - 03 avril 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0005-misc-use-tokens-to-store-autocompletion-context-6066.patch	11,2 ko	18 janvier 2022	Frédéric Péters
0004-misc-remove-explicit-handling-of-account-confirmatio.patch	1,95 ko	18 janvier 2022	Frédéric Péters
0003-tokens-add-job-to-clean-expired-tokens-60665.patch	4,89 ko	18 janvier 2022	Frédéric Péters
0002-misc-move-tokens-to-an-SQL-table-60665.patch	13,6 ko	18 janvier 2022	Frédéric Péters
0001-misc-move-password-token-info-into-a-context-diction.patch	3,3 ko	18 janvier 2022	Frédéric Péters