Authentic 2 - Development #48889

idp_oidc : le setting utilisé pour la durée des access token n'est pas le bon

26 novembre 2020 17:59 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	26 novembre 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

C'est IDTOKEN_DURATION qui est utilisé au lieu d'ACCESS_TOKEN_DURATION, ça fait que par défaut ils ont une durée de vie de 30 secondes, c'est un poil court. Je pense que le mieux c'est de ne pas en mettre que ce soit lié à la session utilisateur par défaut.

Révisions associées

Révision 1687d1a7 - 04 décembre 2020 11:56 - Benjamin Dauvergne

idp_oidc: make access_token validity depends on expiration or session existence (#48889)

Historique

#2 - 26 novembre 2020 18:00 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 27 novembre 2020 08:12 - Benjamin Dauvergne

- Fichier 0001-idp_oidc-make-access_token-validity-depends-on-expir.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Le code de calcul de la validité d'un access_token était mauvais pour la session, j'ai factorisé avec celui d'OIDCCode (absence de session.load() pour valider que la session_key existe).

L'attribut OIDCAccessToken.expired peut désormais être NULL rendant l'access_token uniquement dépendant de la session utilisateur, c'est désormais le fonctionnement par défaut pour un token généré avec l'authorization code flow; ça reste débrayable si on pose une valeur de durée de jeton d'accès dans OIDCClient.access_token_duration.

Pour les jetons obtenus via credentials grant c'est soit la valeur par défaut, 8h soit la valeur posée au niveau de OIDCClient.access_token_duration.

#5 - 03 décembre 2020 23:13 - Benjamin Dauvergne

- Fichier 0001-idp_oidc-make-access_token-validity-depends-on-expir.patch ajouté

Rebasé sur #47900.

#6 - 03 décembre 2020 23:25 - Benjamin Dauvergne

En fait j'avais déjà fait cette correction sur le chargement des sessions dans #47900, donc j'ai rebasé dessus.

#7 - 04 décembre 2020 09:55 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Quitte à faire une modif sur le modèle, j'en aurais peut-être profité pour renommer les attributs created et expired en respectivement created_on et expires_on, pour qu'on arrête de croire que c'est des booléens, je ne sais pas, je te laisse décider.
À part ça, c'est ok.

#8 - 04 décembre 2020 10:18 - Benjamin Dauvergne

Paul Marillonnet a écrit :

Quitte à faire une modif sur le modèle, j'en aurais peut-être profité pour renommer les attributs created et expired en respectivement created_on et expires_on, pour qu'on arrête de croire que c'est des booléens, je ne sais pas, je te laisse décider.
À part ça, c'est ok.

C'est une convention dans a2 maintenant, j'ai des created/modified partout.

#9 - 04 décembre 2020 10:20 - Paul Marillonnet

Ah oui ok je vois ça, tant pis, pas grave.

#10 - 04 décembre 2020 11:58 - Benjamin Dauvergne

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

```
commit 1687d1a7a460598e49eafaf16469b5596504133b
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Nov 27 08:07:49 2020 +0100

    idp_oidc: make access_token validity depends on expiration or session existence (#48889)
```

#11 - 15 décembre 2020 17:16 - Frédéric Péters

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

Fichiers

0001-idp_oidc-make-access_token-validity-depends-on-expir.patch	9,61 ko	27 novembre 2020	Benjamin Dauvergne
0001-idp_oidc-make-access_token-validity-depends-on-expir.patch	8,28 ko	03 décembre 2020	Benjamin Dauvergne