Authentic 2 - Development #65475

idp_oidc: ajouter les paramètres iss et sid permettant éventuellement un logout sans cookie de session

19 mai 2022 21:46 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	19 mai 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Ce n'est pas garanti mais ça le rend possible.

Révisions associées

Révision 8f1ea08a - 20 mai 2022 09:58 - Benjamin Dauvergne

idp_oidc: add iss and sid parameter to frontchannel_logout_uri (#65475)

Historique

#1 - 19 mai 2022 22:04 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 19 mai 2022 22:05 - Benjamin Dauvergne

- Fichier 0001-idp_oidc-add-iss-and-sid-parameter-to-frontchannel_l.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 20 mai 2022 01:50 - Thomas Noël

Pour référence, la spec de ces paramètres c'est semble-t-il https://openid.net/specs/openid-connect-frontchannel-1_0.html#RPLogout

Si je comprends, c'est quelque chose qui permettrait de parfois lutter contre les pépins de cookies tiers (qui sont bien difficiles à passer dans un iframe en 2022, sinon impossibles) ?

Ma relecture :

- Dans le test, tu pourrais aller un poil plus loin et tester ce qui est envoyé dans iss (au lieu de juste tester la présence « assert '&iss=' in iframes.attr('src') »)
- Je n'ai pas trop compris pourquoi tu supprimes iss et sid dans les enregistrements des oidc_sessions : parce que tu es sûr que ça sert à rien ?

En fait, comme ces deux iss et sid étaient déjà dans oidc_session, pourquoi ne pas avoir juste construit l'URL dans apps.py Plugin::logout_list ? (y'a peut-être une raison que j'ai pas vue)

#4 - 20 mai 2022 08:48 - Benjamin Dauvergne

Thomas Noël a écrit :

> Pour référence, la spec de ces paramètres c'est semble-t-il https://openid.net/specs/openid-connect-frontchannel-1_0.html#RPLogout
>
> Si je comprends, c'est quelque chose qui permettrait de parfois lutter contre les pépins de cookies tiers (qui sont bien difficiles à passer dans un iframe en 2022, sinon impossibles) ?
>
> Ma relecture :
>
> - Dans le test, tu pourrais aller un poil plus loin et tester ce qui est envoyé dans iss (au lieu de juste tester la présence « assert '&iss=' in iframes.attr('src') »)

Ok.

- Je n'ai pas trop compris pourquoi tu supprimes iss et sid dans les enregistrements des oidc_sessions : parce que tu es sûr que ça sert à rien ?

Parce que ça ne sert à rien de les stocker, clairement je n'avais pas fini ce code quand je l'ai poussé, ils sont présent dans l'URL qui est stockée à coté et régénérable à la volée de toute façon car dépendant uniquement du domaine et du numéro de la session. Je pense me souvenir vaguement que c'était pour Strasbourg qui n'avait pas besoin du sid juste qu'on ouvre une URL dans une iframe (mais qui doit avoir le même souci maintenant).

> En fait, comme ces deux iss et sid étaient déjà dans oidc_session, pourquoi ne pas avoir juste construit l'URL dans apps.py Plugin::logout_list ? (y'a peut-être une raison que j'ai pas vue)

Je ne sais plus, on pourrait vraisemblablement tout faire à la volée sans rien stocker en session en se basant sur les objets OIDCAccessToken qui référencent les OIDCService pour lesquels ont a eu une interaction dans la session en cours. Là mon objectif c'était juste d'avoir des données suffisantes pour dire aux gens "il y a une solution sans cookie de session, vous pouvez la gérer ou arrêter de vous plaindre'. Ici le sid est servi au login dans l'id_token, ils n'ont qu'à le stocker avec l'issuer dans une table à trois colonne "session_id,iss,sid" et sur réception d'un appel fermer la session correspondante, sans même regarder le cookie en cours.

#5 - 20 mai 2022 09:59 - Benjamin Dauvergne

- Fichier 0001-idp_oidc-add-iss-and-sid-parameter-to-frontchannel_l.patch ajouté

Voilà, tests plus précis.

#6 - 20 mai 2022 11:43 - Thomas Noël

- Statut changé de Solution proposée à Solution validée

En tout cas c'est cool, parce que les cookies, on peut pas toujours les envoyer (cf #53387)

#7 - 20 mai 2022 13:48 - Benjamin Dauvergne

Thomas Noël a écrit :

> En tout cas c'est cool, parce que les cookies, on peut pas toujours les envoyer (cf #53387)

Oui c'est bien en voyant ce ticket que je me suis dit que je pouvais faire ce petit ajustement.

#8 - 20 mai 2022 13:48 - Benjamin Dauvergne

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

```
commit 8f1ea08a6274659f1777326cc7deb32efb5b4daa
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu May 19 22:04:25 2022 +0200

    idp_oidc: add iss and sid parameter to frontchannel_logout_uri (#65475)
```

#9 - 23 mai 2022 13:14 - Transition automatique

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

#10 - 24 juillet 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-idp_oidc-add-iss-and-sid-parameter-to-frontchannel_l.patch	2,44 ko	19 mai 2022	Benjamin Dauvergne
0001-idp_oidc-add-iss-and-sid-parameter-to-frontchannel_l.patch	4,02 ko	20 mai 2022	Benjamin Dauvergne