Authentic 2 - Development #56865

idp_saml: définir sessionNotOnOrAfter à la moitié de la durée de la session A2

10 Sep 2021 04:08 PM - Benjamin Dauvergne

Status:	Solution déployée	**Start date:**	10 Sep 2021
Priority:	Normal	**Due date:**	
Assignee:	Benjamin Dauvergne	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Patch proposed:	Yes	**Planning:**	No

Description

Si l'objectif est de prolonger la session quand le service est utilisé, il est important que celle-ci soit plus courte que celle sur l'IdP pour permettre à un SSO de prolonger celle-ci (et l'authentification qui a lieu revalide que c'est la bonne personne).

L'alternative c'est d'avoir un appel keepalive; dans feu MSP tous les TS devaient ajouter un pixel invisible chargé depuis l'IdP pour y maintenir la session, je préfère qu'on évite cette solution un peu sale.

L'effet visible avec notre configuration actuelle de 8h, c'est qu'au bout de 4h sur un service, on sera redirigé pour authentification sur l'IdP, c'est déjà ce qui se passe au bout de 8h, sauf qu'on a plus de session ouverte. Avec une session courte d'1h, si on accède au service dans la dernière demi-heure, on est réauthentifié de manière transparente et la session IdP est prolongée d'1h. Ça a surtout un impact pour les gens travaillant dans un BO (front portail-agent ou BO w.c.s.) longtemps.

Associated revisions

Revision 12fe40c0 - 30 Sep 2021 05:57 PM - Benjamin Dauvergne

idp_saml2: set sessionNotOnOrAfter to half the current session duration (#56865)

History

#2 - 10 Sep 2021 04:55 PM - Benjamin Dauvergne

- Patch proposed changed from No to Yes

- File 0001-idp_saml2-set-sessionNotOnOrAfter-to-half-the-curren.patch added

#3 - 13 Sep 2021 02:32 PM - Paul Marillonnet

Ok dans l'idée mais

- l'un des deux datetime a une info de fuseau horaire, l'autre non, la soustraction de l'un à l'autre plante.
- le commentaire juste au dessus doit être mis à jour (en l'état c'est "Set SessionNotOnOrAfter to expiry date of the current session […]" (avec peut-être une petite explication de pourquoi le facteur ½ entre la session IdP et la valeur dans l'assertion ?)).
- peut-être un test à coup de freezer pour vérifier le comportement souhaité, i.e. celui qui faciliterait les parcours usagers "pro" tel que décrit dans #56857 ?

#4 - 14 Sep 2021 06:30 PM - Benjamin Dauvergne

- Status changed from Nouveau to Solution proposée

- File 0001-idp_saml2-set-sessionNotOnOrAfter-to-half-the-curren.patch added

Voilà, je pense que j'ai répondu à tout (pas besoin de freezer, juste mesurer la différence entre durée de session locale et ce qui est donné au SP).

#5 - 30 Sep 2021 05:15 PM - Paul Marillonnet

- Status changed from Solution proposée to Solution validée

Yes.

#6 - 30 Sep 2021 05:58 PM - Benjamin Dauvergne

- Status changed from Solution validée to Résolu (à déployer)

```
commit 12fe40c0ae962c8822efdd2f5297a1c4b712d7fe
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Sep 10 16:55:04 2021 +0200

    idp_saml2: set sessionNotOnOrAfter to half the current session duration (#56865)
```

#7 - 07 Oct 2021 10:16 PM - Frédéric Péters

- Status changed from Résolu (à déployer) to Solution déployée

Files

0001-idp_saml2-set-sessionNotOnOrAfter-to-half-the-curren.patch	1.35 KB	10 Sep 2021	Benjamin Dauvergne
0001-idp_saml2-set-sessionNotOnOrAfter-to-half-the-curren.patch	3.71 KB	14 Sep 2021	Benjamin Dauvergne