Authentic 2 - Development #5530

Faciliter la migration des fédérations

17 septembre 2014 17:05 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	17 septembre 2014
Priorité:	Normal	**Echéance:**	13 mars 2015
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.2.0		
Patch proposed:	Oui	**Planning:**	

Description

Depuis le commit 21dfe1306 les identity dump sont de nouveaux générés à partir des champs name_id_qualifier et name_id_sp_name_qualifier de l'objet LibertyFederation ce qui fait que la migration de fédérations n'est pas évidente.

L'idée serait de stocker dans ses deux champs des sentinelles, par exemple la valeur http://authentic.entrouvert.org/same_id/, pour dire que la valeur à y mettre et la même que l'entity ID de l'IdP ou du SP.

Il faut pour cela une migration pour corriger les fédérations un peu partout et modifier le code de création de l'identity dump et le code de sauvegarde des fédérations.

Révisions associées

Révision 8d8edc9c - 31 mars 2015 16:52 - Benjamin Dauvergne

Modify federation storage so that we can store federation relative to the provider model (fixes #5530)

If the content of name_id_qualifier or name_id_sp_name_qualifier is
equals to the issuer or service provider entity ID then we store a
sentinel value instead, meaning 'same as provider entity ID'. If we
change the provider entity, all federations are still correct.

Historique

#1 - 02 octobre 2014 17:02 - Benjamin Dauvergne

- Fichier 0001-Modify-federation-storage-so-that-we-can-store-feder.patch ajouté

- Patch proposed changé de Non à Oui

#2 - 02 octobre 2014 17:02 - Benjamin Dauvergne

- Statut changé de Nouveau à En cours

#3 - 03 novembre 2014 10:17 - Frédéric Péters

Detail, could AUTHENTIC_SAME_ID_SENTINEL be urn:authentic:same-as-provider-entity-id, rather than an URL ? (I think it makes the usage clearer)

And would it be possible to use that AUTHENTIC_SAME_ID_SENTINEL constant in 0040_plug_sentinel_value_in_libertyfederation_qualifiers.py?

The migration calls raw_input(), I fear this won't fly with packages :/ there's no way to get the entity id from the database?

#4 - 03 novembre 2014 16:48 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Detail, could AUTHENTIC_SAME_ID_SENTINEL be urn:authentic:same-as-provider-entity-id, rather than an URL ? (I think it makes the usage clearer)

Ok. I'm not fan of using URNs as to do it really formally we should obtain the namespace from IANA but that's just pedantery.

> And would it be possible to use that AUTHENTIC_SAME_ID_SENTINEL constant in 0040_plug_sentinel_value_in_libertyfederation_qualifiers.py?

Of course.

> The migration calls raw_input(), I fear this won't fly with packages :/

It will block automatic updates, but it should work if the update is attended. What do you think ?

> there's no way to get the entity id from the database?

Not with 100% certainty; we do not use django.contrib.sites and it does not have the schema only the domain, it could be extracted from LibertyFederation if there are some but it does not make the update safe.

#5 - 05 novembre 2014 01:14 - Benjamin Dauvergne

- Fichier 0001-Modify-federation-storage-so-that-we-can-store-feder.patch ajouté

Updated patch. Sentinel changed to urn:authentic.entrouvert.org:same-as-provider-entity-id and SAME_ID constant re-used in migration.

#6 - 05 novembre 2014 08:43 - Frédéric Péters

> It will block automatic updates, but it should work if the update is attended. What do you think ?

I still don't like it :/ Here's kind of a proposal: look for the value in the environment (let's say AUTHENTIC_IDP_ENTITY_ID_MIGRATION), and fallback on raw_input() if it's missing (or even abort) if it's missing (and there are existing LibertyFederation and LibertyProvider objects); and add this info in the "How to upgrade to a new version of authentic" section of the README file, along as the recommended way to get the value from a running instance (is it looking in the saml metadata, or is there a better way?).

#7 - 05 novembre 2014 10:00 - Benjamin Dauvergne

Frédéric Péters a écrit :

> (is it looking in the saml metadata, or is there a better way?).

The URL is generated from each HTTP request, there is really no automatic way to get it from a script :/ You can deduct it from the virtual host configuration.

> > It will block automatic updates, but it should work if the update is attended. What do you think ?
>
> I still don't like it :/ Here's kind of a proposal: look for the value in the environment (let's say AUTHENTIC_IDP_ENTITY_ID_MIGRATION), and fallback on raw_input() if it's missing (or even abort) if it's missing (and there are existing LibertyFederation and LibertyProvider objects); and add this info in the "How to upgrade to a new version of authentic" section of the README file, along as the recommended way to get the value from a running instance

Ok.

#8 - 05 novembre 2014 10:03 - Frédéric Péters

Benjamin Dauvergne a écrit :

> Frédéric Péters a écrit :
>
> > (is it looking in the saml metadata, or is there a better way?).
>
> The URL is generated from each HTTP request, there is really no automatic way to get it from a script :/ You can deduct it from the virtual host configuration.

That's what I meant, so the instruction to get the value would be along the lines of "go to your site /idp/saml2/metadata, and take the entityId attribute", ok.

#9 - 06 mars 2015 16:35 - Benjamin Dauvergne

- Version cible mis à future

#10 - 09 mars 2015 10:57 - Benjamin Dauvergne

- Patch proposed changé de Oui à Non

#11 - 09 mars 2015 12:54 - Benjamin Dauvergne

- Echéance mis à 13 mars 2015

- Patch proposed changé de Non à Oui

#12 - 09 mars 2015 12:54 - Benjamin Dauvergne

- Patch proposed changé de Oui à Non

#13 - 18 mars 2015 15:45 - Benjamin Dauvergne

- Fichier 0001-Modify-federation-storage-so-that-we-can-store-feder.patch supprimé

#14 - 18 mars 2015 15:48 - Benjamin Dauvergne

- Fichier 0001-Modify-federation-storage-so-that-we-can-store-feder.patch ajouté

- Patch proposed changé de Non à Oui

This new version contains a Django 1.7 migration, it does not ask anymore for the current IdP entity ID; we just logically imply that if name_id_qualifier is not empty then it must contain the current IdP entity id; if it's empty then it should stay so.

Federations as a service provider are completely ignored as authsaml2 is deprecated and new SAML 2.0 support as a service provider will be remade with django-mellon and will not use current SAML framework.

#15 - 18 mars 2015 15:48 - Benjamin Dauvergne

- Version cible changé de future à 2.1.13

#16 - 23 mars 2015 16:40 - Benjamin Dauvergne

- Version cible changé de 2.1.13 à 2.2.0

#17 - 31 mars 2015 16:55 - Benjamin Dauvergne

- Statut changé de En cours à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit 8d8edc9c9261da33ae7c87774d3f55985a87543d.

#18 - 23 février 2016 12:58 - Benjamin Dauvergne

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

#19 - 06 décembre 2017 15:28 - Benjamin Dauvergne

- Statut changé de Solution déployée à Fermé

Fichiers

0001-Modify-federation-storage-so-that-we-can-store-feder.patch	31,4 ko	05 novembre 2014	Benjamin Dauvergne
0001-Modify-federation-storage-so-that-we-can-store-feder.patch	8,02 ko	18 mars 2015	Benjamin Dauvergne