Authentic 2 - Development #35302

auth_saml : avoir une action de mapping pour ajouter/retirer un rôle

08 août 2019 11:12 - Thomas Noël

Statut:	Fermé	**Début:**	08 août 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Lorsqu'Authentic est SP d'un IdP tiers, il serait bien qu'on ai la possibilité d'avoir un set_mandatory_roles comme ce qui existe pour la synchro LDAP.

Quelque chose qui permette une configuration de l'IdP du genre :

```
  "MELLON_IDENTITY_PROVIDERS": [
    {
      "METADATA": "/var/lib/authentic2-multitenant/tenants/whatever.test.entrouvert.org/idp.xml",
      "PROVISION": true,
      "SET_MANDATORY_ROLES": ["Agent"]     <-- et tous les comptes qui se logent par cet IdP gagnent ce rôle
      ...
    }
```

Révisions associées

Révision 0f17a562 - 19 août 2019 16:49 - Benjamin Dauvergne

log_filters: get user and ip from record if present (#35302)

Révision 5cb84716 - 19 août 2019 16:49 - Benjamin Dauvergne

create authentic2.utils package (#35302)

Révision 94486a72 - 19 août 2019 16:49 - Benjamin Dauvergne

utils: add module to evaluate condition expressions safely (#35302)

Révision 40307f51 - 19 août 2019 16:49 - Benjamin Dauvergne

auth_saml: add more mapping actions in A2_ATTRIBUTE_MAPPING (#35302)

Historique

#2 - 08 août 2019 17:20 - Benjamin Dauvergne

- Sujet changé de adapter mellon: avoir la possibilité d'imposer des rôles (set_mandatory_roles) à auth_saml : avoir la possibilité d'imposer des rôles (set_mandatory_roles)

- Assigné à mis à Benjamin Dauvergne

Ok mais ça doit s'appeler A2_SET_MANDATORY_ROLES pour faire propre.

#3 - 09 août 2019 12:20 - Benjamin Dauvergne

- Fichier 0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch ajouté

- Fichier 0001-log_filters-get-user-and-ip-from-record-if-present-3.patch ajouté

- Fichier 0003-utils-add-module-to-evaluate-condition-expressions-s.patch ajouté

- Fichier 0002-create-authentic2.utils-package-35302.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Bon plutôt que d'ajouter un nouveau setting j'ai ajouté de nouvelles actions.

#4 - 09 août 2019 12:26 - Benjamin Dauvergne

Le patch 0001 c'est pour que le filtre de log de base dans A2 soit plus proche de celui de hobo (notamment en pouvant poser directement un user dans logger.log().

Le 0002/0003 ça introduit un premier validateur d'expression pour des conditions simples qui ne peuvent pas créer de DOS ou de trou de sécu (normalement), pour l'instant je n'utiliser que dans de la config mais ça sera utiliser dans les modèles bientôt. Au passage je déplacer utils pour le découper dans le futur.

Le 0004 réorganise et introduit de nouvelles actions :

- par défaut set-attribute, l'action de base
- rename qui permet de renommer un attribut pour quelque chose d'utilisable plus simplement notamment dans des expressions
- toggle-role qui permet d'ajouter/retirer un rôle selon une condition ou pas (dans ce cas ça ne fait qu'ajouter)

#5 - 09 août 2019 12:26 - Benjamin Dauvergne

- Sujet changé de auth_saml : avoir la possibilité d'imposer des rôles (set_mandatory_roles) à auth_saml : avoir une action de mapping pour ajouter/retirer un rôle

#6 - 09 août 2019 14:39 - Benjamin Dauvergne

- Fichier 0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch ajouté

- Fichier 0001-log_filters-get-user-and-ip-from-record-if-present-3.patch ajouté

- Fichier 0003-utils-add-module-to-evaluate-condition-expressions-s.patch ajouté

- Fichier 0002-create-authentic2.utils-package-35302.patch ajouté

Corrections dans les imports de authentic2.utils.

#7 - 09 août 2019 14:43 - Thomas Noël

Je ne pige pas trop l'ajout de la gestion des conditions... quel besoin imagines-tu ? Perso j'en ai pas besoin, un "add-role" me suffirait très bien. Mais surtout si on a ici la gestion de condition, alors il la faudrait aussi dans la synchro LDAP (et autres systèmes de pré-provisioning).

#8 - 09 août 2019 15:45 - Benjamin Dauvergne

Thomas Noël a écrit :

> Je ne pige pas trop l'ajout de la gestion des conditions... quel besoin imagines-tu ? Perso j'en ai pas besoin, un "add-role" me suffirait très bien. Mais surtout si on a ici la gestion de condition, alors il la faudrait aussi dans la synchro LDAP (et autres systèmes de pré-provisioning).

Oui c'est un peu l'idée mais c'est un galop d'essai, l'idée c'est d'avoir ça partout sous la même forme, mais comme auth_saml ne sert pas beaucoup je préfère commencer ici.

Je vois assez bien dans une autre ville avec un ADFS :

```
{
    'action': 'toggle-role',
    'role': { 'name': 'Agent', 'ou': {'name': 'Ville'}},
    'condition': "'cn=Agent,ou=groups,dc=ville,dc=fr' in memberOf",
}
```

Et je vais avoir besoin des conditions pour le filtrage des modes d'authentification en front.

#9 - 13 août 2019 13:40 - Thomas Noël

- Statut changé de Solution proposée à Solution validée

Benjamin Dauvergne a écrit :

> Thomas Noël a écrit :
>
> > Je ne pige pas trop l'ajout de la gestion des conditions... quel besoin imagines-tu ? Perso j'en ai pas besoin, un "add-role" me suffirait très bien. Mais surtout si on a ici la gestion de condition, alors il la faudrait aussi dans la synchro LDAP (et autres systèmes de pré-provisioning).
>
> Oui c'est un peu l'idée mais c'est un galop d'essai, l'idée c'est d'avoir ça partout sous la même forme, mais comme auth_saml ne sert pas beaucoup je préfère commencer ici.

Okaye. Bon, ça ne sert tellement pas beaucoup que ça ne va en pratique service nulle part (je parle des conditions).

Aussi, je ne suis pas très fan du nom "toggle-role" (surtout quand il n'y a pas de condition), mais comme j'ai pas mieux à proposer, go.

#10 - 19 août 2019 16:49 - Benjamin Dauvergne

- Fichier 0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch ajouté

- Fichier 0001-log_filters-get-user-and-ip-from-record-if-present-3.patch ajouté

- Fichier 0003-utils-add-module-to-evaluate-condition-expressions-s.patch ajouté

- Fichier 0002-create-authentic2.utils-package-35302.patch ajouté

- Statut changé de Solution validée à Solution proposée

#11 - 19 août 2019 16:49 - Benjamin Dauvergne

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

```
commit 40307f519cb690bbdc22608f9431b2726bcdc5c0
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Aug 8 17:38:37 2019 +0200

    auth_saml: add more mapping actions in A2_ATTRIBUTE_MAPPING (#35302)

commit 94486a726bb0014f28840e9015cd4b75e2fa0cda
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Aug 9 10:33:52 2019 +0200

    utils: add module to evaluate condition expressions safely (#35302)

commit 5cb84716c8041492ecef18d21347efbf196ec47b
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Aug 8 17:53:28 2019 +0200

    create authentic2.utils package (#35302)

commit 0f17a5620249c68775a5a8bea2c3e27fda95b8db
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Aug 9 12:14:26 2019 +0200

    log_filters: get user and ip from record if present (#35302)
```

#12 - 04 septembre 2019 17:15 - Frédéric Péters

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

Fichiers

0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch	14,5 ko	09 août 2019	Benjamin Dauvergne
0001-log_filters-get-user-and-ip-from-record-if-present-3.patch	1,86 ko	09 août 2019	Benjamin Dauvergne
0003-utils-add-module-to-evaluate-condition-expressions-s.patch	9,33 ko	09 août 2019	Benjamin Dauvergne
0002-create-authentic2.utils-package-35302.patch	978 octets	09 août 2019	Benjamin Dauvergne
0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch	14,5 ko	09 août 2019	Benjamin Dauvergne
0001-log_filters-get-user-and-ip-from-record-if-present-3.patch	1,86 ko	09 août 2019	Benjamin Dauvergne
0003-utils-add-module-to-evaluate-condition-expressions-s.patch	9,33 ko	09 août 2019	Benjamin Dauvergne
0002-create-authentic2.utils-package-35302.patch	3,97 ko	09 août 2019	Benjamin Dauvergne
0004-auth_saml-add-more-mapping-actions-in-A2_ATTRIBUTE_M.patch	14,5 ko	19 août 2019	Benjamin Dauvergne
0001-log_filters-get-user-and-ip-from-record-if-present-3.patch	1,86 ko	19 août 2019	Benjamin Dauvergne
0003-utils-add-module-to-evaluate-condition-expressions-s.patch	9,34 ko	19 août 2019	Benjamin Dauvergne
0002-create-authentic2.utils-package-35302.patch	3,97 ko	19 août 2019	Benjamin Dauvergne