Authentic 2 - Development #53442

possibilité d'attribuer des rôles à un utilisateur se connectant via un IdP OIDC

26 avril 2021 19:17 - Frédéric Péters

Statut:	Fermé	**Début:**	26 avril 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Valentin Deniaud	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Côté LDAP on a une possibilité de correspondance de groupes vers rôles (group_to_role_mapping), côté SAML des instructions d'affectation (A2_ATTRIBUTE_MAPPING avec dedans des "action": "toggle-role"), mais côté OIDC il me semble qu'on n'a rien.

Révisions associées

Révision fc093735 - 27 septembre 2022 14:48 - Valentin Deniaud

authenticators: remove obsolete manager_form_class (#53442)

Révision c12438b5 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: move model form parameters to class (#53442)

Révision 2bd79c0b - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: genericize related object code (#53442)

Révision 700a5bb1 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: switch related object foreign key to base model (#53442)

Révision b24fad1b - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: move related object code to authenticators app (#53442)

Révision ad2d35fe - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: move add role action to authenticators app (#53442)

Révision b524ae20 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_saml: move role choice field outside of module (#53442)

Révision cf5132d7 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_oidc: configure claims widget through subclass (#53442)

Révision 5e156b61 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_oidc: use generic related object code (#53442)

Révision d7212589 - 27 septembre 2022 14:48 - Valentin Deniaud

auth_oidc: allow adding roles on login (#53442)

Historique

#5 - 08 avril 2022 08:12 - Benjamin Dauvergne

Ce ticket serait agréablement remplacé par le fait de finir #20690 qui concerne le fait d'affecter automatiquement des rôles aux utilisateurs membre d'une collectivité. Ici il suffirait de créer une OU Agent et d'y accrocher l'authentification OIDC et le mécanisme serait uniforme pour tous les moyens d'authentification. Et surtout ça vous obligera à créer des OUs Agent et ne plus mélanger les agents et les usagers ce qui est bien pour votre karma RGPD.

#8 - 20 septembre 2022 11:02 - Valentin Deniaud

- Assigné à mis à Valentin Deniaud

#9 - 21 septembre 2022 12:47 - Valentin Deniaud

- Fichier 0008-auth_oidc-configure-claims-widget-through-subclass-5.patch ajouté

- Fichier 0001-authenticators-remove-obsolete-manager_form_class-53.patch ajouté

- Fichier 0004-auth_saml-switch-related-object-foreign-key-to-base-.patch ajouté

- Fichier 0006-auth_saml-move-add-role-action-to-authenticators-app.patch ajouté

- Fichier 0007-auth_saml-move-role-choice-field-outside-of-module-5.patch ajouté

- Fichier 0005-auth_saml-move-related-object-code-to-authenticators.patch ajouté

- Fichier 0010-auth_oidc-allow-adding-roles-on-login-53442.patch ajouté

- Fichier 0002-auth_saml-move-model-form-parameters-to-class-53442.patch ajouté

- Fichier 0009-auth_oidc-use-generic-related-object-code-53442.patch ajouté

- Fichier 0003-auth_saml-genericize-related-object-code-53442.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

On a côté SAML 3 objets liés à l'authenticator (affecter un attribut, rechercher par attribut et ajouter un rôle), manipulés par les mêmes vues génériques locales au module auth_saml.

On a côté OIDC un objet lié, les claims, manipulés par des vues spécialisées locales au module auth_oidc.

Ici bêtement ajouter un deuxième objet lié OIDC pour l'ajout de rôle aurait conduit à dupliquer les vues spécialisées déjà présentes.

Plutôt que de faire ça, gros effort de factorisation, avec notamment :

- 0003, rendre les vues génériques SAML encore plus génériques (enlever toute mention de SAML)
- 0004, dernier bout du travail, splitté pour la clarté parce qu'il y a une migration
- 0005, déplacement du code générique obtenu dans le module principal
- 0006, tant qu'on y est, mutualisation du modèle d'ajout de rôle
- 0009, utilisation des vues génériques côté OIDC pour la manipulation des claims
- 0010, enfin le patch, tout bête.

#11 - 22 septembre 2022 16:06 - Benjamin Dauvergne

Je relis.

#12 - 22 septembre 2022 16:25 - Benjamin Dauvergne

- Statut changé de Solution proposée à Information nécessaire

Fonctionnellement ça m'a l'air tout ok, par contre tu supprimes/renommes des types d'évènement mais je ne vois pas de migration pour corriger les évènements existants. Ne faudrait-il pas renommer les instances de EventType voir migrer les Event liés si leur contenu a changé (je n'ai trop vérifié, le renommage suffira peut-être) ?

#13 - 22 septembre 2022 16:39 - Valentin Deniaud

Ça fait un mois que les vues SAML existent, deux semaines pour OIDC, à mon avis il existe sur tout le SaaS 10 évènements concernés côté SAML et 0 pour OIDC.

Pour ces évènements le journal affiche « authenticator.saml.related_object.edit » au lieu du libellé attendu (pas de crash ni de donnée manquante, donc).

Les solutions par ordre de préférence :

- Considérer que ce n'est pas grave (solution actuelle)
- Laisser les fichier journal_event_types.py que j'ai viré
- Coder un truc générique dans apps/journal/ pour pouvoir indiquer legacy_names = authenticator.saml.related_object.edit aux nouveaux EventType et que les anciens évènements soient rattachés à la volée aux nouveaux types dans la vue (dans l'idée que ça resservira un jour, aucune idée de la complexité)
- Écrire une migration (soupir)

#14 - 22 septembre 2022 16:41 - Benjamin Dauvergne

- Statut changé de Information nécessaire à Solution proposée

Valentin Deniaud a écrit :

> Ça fait un mois que les vues SAML existent, deux semaines pour OIDC, à mon avis il existe sur tout le SaaS 10 évènements concernés côté SAML et 0 pour OIDC.

Pour ces évènements le journal affiche « authenticator.saml.related_object.edit » au lieu du libellé attendu (pas de crash ni de donnée manquante, donc).

Les solutions par ordre de préférence :

- Considérer que ce n'est pas grave (solution actuelle)

Ok ta réponse me va, je fais deux/trois tests en live et je valide.

#15 - 27 septembre 2022 12:31 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#16 - 27 septembre 2022 15:31 - Valentin Deniaud

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

```
commit d7212589c26a898a57f1bd9a42c20a687fa0e586
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 15:38:41 2022 +0200

    auth_oidc: allow adding roles on login (#53442)

commit 5e156b616827aa9254796bcdfccf0d8ea95386c7
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 14:17:19 2022 +0200

    auth_oidc: use generic related object code (#53442)

commit cf5132d72f9a164ae4d8052d2341e9411358e2f7
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 14:00:42 2022 +0200

    auth_oidc: configure claims widget through subclass (#53442)

commit b524ae206f6d138db73cd76950f2aa038695ec53
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 14:10:08 2022 +0200

    auth_saml: move role choice field outside of module (#53442)

commit ad2d35fed53f8d207610e6aa1eb54930024f3271
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 16:38:46 2022 +0200

    auth_saml: move add role action to authenticators app (#53442)

commit b24fad1bd2922b2ae4eb904d75f3191c1b2aea18
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 12:08:19 2022 +0200

    auth_saml: move related object code to authenticators app (#53442)

commit 700a5bb196770a1dd132e26d4eb773e8f9be3555
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Wed Sep 21 11:40:27 2022 +0200

    auth_saml: switch related object foreign key to base model (#53442)

commit 2bd79c0b810bb1a2ec20c07bf8e958286561d46f
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Wed Sep 21 11:09:25 2022 +0200

    auth_saml: genericize related object code (#53442)

commit c12438b5ee630f13a72f3517b0825597e8d325c1
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 11:51:05 2022 +0200

    auth_saml: move model form parameters to class (#53442)

commit fc093735ba6d57d986ef2a7be6a14137839e626a
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Tue Sep 20 11:33:06 2022 +0200
```

```
    authenticators: remove obsolete manager_form_class (#53442)
```

#17 - 29 septembre 2022 11:14 - Transition automatique

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

#18 - 04 décembre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0008-auth_oidc-configure-claims-widget-through-subclass-5.patch	1,97 ko	21 septembre 2022	Valentin Deniaud
0001-authenticators-remove-obsolete-manager_form_class-53.patch	865 octets	21 septembre 2022	Valentin Deniaud
0004-auth_saml-switch-related-object-foreign-key-to-base-.patch	2,69 ko	21 septembre 2022	Valentin Deniaud
0006-auth_saml-move-add-role-action-to-authenticators-app.patch	7,8 ko	21 septembre 2022	Valentin Deniaud
0007-auth_saml-move-role-choice-field-outside-of-module-5.patch	2,8 ko	21 septembre 2022	Valentin Deniaud
0005-auth_saml-move-related-object-code-to-authenticators.patch	23,8 ko	21 septembre 2022	Valentin Deniaud
0010-auth_oidc-allow-adding-roles-on-login-53442.patch	4,12 ko	21 septembre 2022	Valentin Deniaud
0002-auth_saml-move-model-form-parameters-to-class-53442.patch	2,39 ko	21 septembre 2022	Valentin Deniaud
0009-auth_oidc-use-generic-related-object-code-53442.patch	24,9 ko	21 septembre 2022	Valentin Deniaud
0003-auth_saml-genericize-related-object-code-53442.patch	24,5 ko	21 septembre 2022	Valentin Deniaud