Authentic 2 - Development #39383

idp_oidc: lors de la cession resource owner password credentials (ROPC) pouvoir discriminer sur l'OU supposée de l'usager

29 janvier 2020 15:10 - Paul Marillonnet

Statut:	Fermé	**Début:**	29 janvier 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans l'état actuel du code introduit par #35205, le client ne peux pas indiquer que le propriétaire de la ressource, dont il détient les crédentiels, est rangé dans une OU donnée – ce qui pose problème notamment dans le cas où authentic est configuré pour la non-unicité globale du doublet login/motdepasse.

On pourrait envisager de (i) pouvoir restreindre un client ROPC à une OU donnée, et donc logiquement de (ii) lors de l'authentification de l'usager, restreindre l'ensemble d'usagers candidats pour l'authn à cette OU, et enfin de gérer cette restriction lors de l'émission (iii) du jeton d'accès et la consommation (iv) de celui-ci.

(iii) et (iv) pourraient s'inscrire dans une démarche plus globale (non spécifique à la cession ROPC) de gestion des OU à travers les portées du jeton d'accès dans le fournisseur OIDC – mais je reste mitigé sur ce point, ne sachant pas s'il est recommandé voire même possible d'étendre la gestion des portées à quelque chose de compatible OAuth2 mais qui sortirait du cas d'usage OIDC — cas d'usage dans lequel les portées sont uniquement utilisées pour la déclaration des revendications (claims).

Révisions associées

Révision 2c3d0e58 - 03 février 2020 15:48 - Paul Marillonnet

idp_oidc: add ou selection on ropc grant (#39383)

Historique

#1 - 29 janvier 2020 15:14 - Paul Marillonnet

- Description mis à jour

#2 - 29 janvier 2020 15:14 - Benjamin Dauvergne

Tu peux permettre un paramètre supplémentaire à la vue token pour ce besoin, ce n'est pas un souci, sinon tu testes tous les comptes concernés et tu prends le premier qui valide (ce que fait le backend je pense, à voir).

#3 - 29 janvier 2020 15:16 - Paul Marillonnet

- Description mis à jour

#4 - 29 janvier 2020 15:17 - Frédéric Péters

> pouvoir restreindre d'un client ROPC à une OU donnée, et donc logiquement de (ii) lors de l'authentification de l'usager, restreindre l'ensemble d'usagers candidats pour l'authn à cette OU

Oui mais on n'a pas envie de devoir créer autant de client oidc qu'il y a d'OU d'utilisateurs.

La situation est vraiment la même que concernant l'écran de connexion où un <select> a été ajouté pour choisir une collectivité, mais dans l'API.

Sans sortir du cadre oidc, si jamais ajouter une clé au dictionnaire n'est pas autorié, ça peut aussi s'imaginer comme étant un realm ajouté à l'username.

#5 - 29 janvier 2020 15:18 - Frédéric Péters

> (ce que fait le backend je pense, à voir).

oui ça prend le premier qui valide, le cas limite imaginé étant celui de la même personne dans deux OU, avec même email même mot de passe, et donc la demande de collectivité comme critère différenciant.

#6 - 29 janvier 2020 16:11 - Benjamin Dauvergne

Frédéric Péters a écrit :

> (ce que fait le backend je pense, à voir).

> oui ça prend le premier qui valide, le cas limite imaginé étant celui de la même personne dans deux OU, avec même email même mot de passe, et donc la demande de collectivité comme critère différenciant.

On peut déprécier le support des realm[1] au niveau du username ou en tout cas pour le cas commun gérer en plus de ça comme un slug d'ou. Du code actuel le dernier usage des realm est dans le backend LDAP pour la construction du username par défaut mais ça peut très bien disparaître.

Dans ce cas la modification serait à faire les backends d'authentification par login et mot de passe : modèle et LDAP; coté LDAP ça veut dire matcher le '@<realm>' contre le slug de l'OU associé à la connexion LDAP (et pas contre le champ realm prévu).

PS: avant l'existence des OUs on avait la possibilité d'ajouter @{nimportekoi} à un username pour permettre à plusieurs personne d'avoir le même username, c'était les OUs du pauvre.

#7 - 29 janvier 2020 18:33 - Paul Marillonnet

- Assigné à mis à Paul Marillonnet

#8 - 30 janvier 2020 16:58 - Paul Marillonnet

Frédéric Péters a écrit :

> Oui mais on n'a pas envie de devoir créer autant de client oidc qu'il y a d'OU d'utilisateurs.

L'idée était bien sûr que les clients qui peuvent taper dans plusieurs OU ne soient pas liés à une OU en particulier (lien 0…* <-> 0…* voire 0…* <-> 0…1 entre respectivement clients et OU).

Mais l'idée de Benj de rajouter simplement un paramètre à la vue token me va très bien, je vais partir là-dessus.

#9 - 30 janvier 2020 17:44 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Mais l'idée de Benj de rajouter simplement un paramètre à la vue token me va très bien, je vais partir là-dessus.

J'ai proposé deux pistes :

- ajouter un paramètre ou* à la vue token
- gérer le suffix @<ou_slug> dans les backends d'authent

Choisis celui que tu veux (je trouve le suffixe pas si mal, ça permet aussi d'avoir ça en front quand on oublie d'activer le sélecteur d'OU, mais il y a peut-être des inconvénients que je n'imagine pas).

#10 - 03 février 2020 14:50 - Paul Marillonnet

- Fichier 0001-idp_oidc-add-ou-selection-on-ropc-grant-39383.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

J'ai opté pour quelque chose qui se rapproche de l'option 1 parmi les deux que tu mentionnes ici.

#11 - 03 février 2020 14:58 - Benjamin Dauvergne

Tu peux virer le warning, personne ne s'attendra à ce que ça marche en flow SSO classique (à vrai dire credential grant ne semble pas vraiment faire partie d'OIDC, ils l'ont gardé parce que c'était dans OAUTH2 mais le rapport est faible).

#12 - 03 février 2020 15:03 - Paul Marillonnet

- Fichier 0001-idp_oidc-add-ou-selection-on-ropc-grant-39383.patch ajouté

Benjamin Dauvergne a écrit :

> Tu peux virer le warning, personne ne s'attendra à ce que ça marche en flow SSO classique (à vrai dire credential grant ne semble pas vraiment faire partie d'OIDC, ils l'ont gardé parce que c'était dans OAUTH2 mais le rapport est faible).

Oui ok, avertissement retiré de la vue token dans ce nouveau patch.

#13 - 03 février 2020 15:29 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#14 - 03 février 2020 15:50 - Paul Marillonnet

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

```
commit 2c3d0e5898a7ae27d76372507c9e472c423337df
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Jan 30 17:50:50 2020 +0100

    idp_oidc: add ou selection on ropc grant (#39383)
```

#15 - 07 février 2020 09:14 - Frédéric Péters

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

Fichiers

0001-idp_oidc-add-ou-selection-on-ropc-grant-39383.patch	6,46 ko	03 février 2020	Paul Marillonnet
0001-idp_oidc-add-ou-selection-on-ropc-grant-39383.patch	5,61 ko	03 février 2020	Paul Marillonnet