Authentic 2 - Bug #45650

idp_oidc : la page de gestion des consentements par service fait apparaître les consentements donnés à l'échelle de l'OU

31 juillet 2020 11:24 - Paul Marillonnet

Statut:	Fermé	**Début:**	31 juillet 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

(Et sans doute que l'affichage va mal se passer car l'objet d'autorisation lié ne renseigne pas de service)

Historique

#1 - 31 juillet 2020 11:24 - Paul Marillonnet

- Priorité changé de Normal à Bas

D'abord évaluer l'état du support des consentements par OU avant de s'avancer sur la criticité de ce bug.

#2 - 01 août 2020 09:21 - Paul Marillonnet

- Fichier 0001-idp_oidc-ban-any-ou-based-authz-from-service-authz-p.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Voilà qui est mieux, par rapport à ce que j'essayais, à tort, de faire dans #45635-2.
En fait, la clé étrangère OIDCAuthorization.client est générique car on y place, au choix, des clients ou des OU…

#3 - 01 août 2020 09:37 - Paul Marillonnet

- Fichier 0001-idp_oidc-ban-any-ou-based-authz-from-service-authz-p.patch ajouté

- Priorité changé de Bas à Normal

Hmm, sans les typos et avec les imports, c'est mieux :)
Je remets en priorité normale parce qu'après lecture des implications ça me paraît quand même non-négligeable.

#4 - 01 août 2020 09:48 - Frédéric Péters

> Je remets en priorité normale parce qu'après lecture des implications ça me paraît quand même non-négligeable.

Il y a des endroits avec cette configuration d'autorisation par OU ? En pratique, ça fait quoi ?

#5 - 01 août 2020 10:01 - Paul Marillonnet

Frédéric Péters a écrit :

> > Je remets en priorité normale parce qu'après lecture des implications ça me paraît quand même non-négligeable.
>
> Il y a des endroits avec cette configuration d'autorisation par OU ?

J'imagine que dans des projets où plusieurs clients partagent le même "service intelligible" offert à l'usager ça doit faire sens, mais je ne suis pas au courant des déploiements.

> En pratique, ça fait quoi ?

Lors de la phase d'autorisation du client, si celui-ci est en mode d'autorisation géré par l'OU (AUTHORIZATION_MODE_BY_OU), alors c'est les autorisations attachée à l'OU qui sont prises pour la décision d'accorder ou non l'autorisation pour les portées demandées.

#6 - 01 août 2020 10:08 - Paul Marillonnet

Paul Marillonnet a écrit :

> J'imagine que dans des projets où plusieurs clients partagent le même "service intelligible" offert à l'usager ça doit faire sens, mais je ne suis pas au courant des déploiements.

Et, ça rejoint l'idée de sectorisation OAuth, où des clients dans un même secteur (métier) offrent à eux tous un service à l'usager, et se voient donc délivrés le même sub. À partir de là il est légitime de sectoriser la gestion des autorisations (l'usager veut autoriser un service, même si techniquement il y a plusieurs clients pour mener à bien la fourniture du service).

#7 - 01 août 2020 10:42 - Frédéric Péters

Je ne pige toujours pas trop, à balancer le long de la lecture entre deux compréhensions des relations :

- les OU c'est ce qui existe aujourd'hui c'est genre Usagers / Collectivité1 / etc., et du coup prendre l'autorisation attachée à l'OU ça voudrait dire qu'un utilisateur de l'OU en premier se connecte et accorde l'autorisation et que ça vaut pour tout le monde.
- les OU c'est ici autre chose une utilisation parallèle pour grouper des services personne dedans et un utilisateur se connecte et accorde l'autorisation et ça vaut aussi pour les autres services de l'OU en question.

La première compréhension n'a pas tellement de sens, surtout amène trop de nouvelles questions, et donc ça serait l'autre mais ça me semble totalement quelque chose jamais fait et un détournement de l'usage courant des OU et bien bizarre aussi, au final.

Reste que si on est dans le cas 2, avec une autorisation accordée par l'usager connecté (et pas un "premier usager qui a accordé et ça vaut pour tout le monde" du cas 1), je dirais que ça appelle plutôt à gérer l'existence de telles autorisations sur la page en question, ce qui veut sans doute juste dire trouver un terme englobant pour "service/organisation", plutôt que faire ce patch que je ne comprends de toute façon pas mais qui retire la possibilité de contrôler ces autorisations.

Option "retirer la possibilité de contrôler ces autorisations" qui lance vers le cas 1, parce que si les autorisations sont accordées par quelqu'un d'autre, c'est alors compréhensible de ne pas pouvoir les retirer.

#8 - 01 août 2020 10:43 - Frédéric Péters

Mon souhait de réponse étant qu'on me pointe un endroit où c'est concrètement utilisé, et si ce n'est utilisé nulle part, j'aurai une tendance à vouloir alors dégager/ignorer ces options théoriques qui empêchent d'avancer sur les considérations réelles.

#9 - 01 août 2020 11:13 - Paul Marillonnet

Frédéric Péters a écrit :

> Je ne pige toujours pas trop, à balancer le long de la lecture entre deux compréhensions des relations :
>
> - les OU c'est ce qui existe aujourd'hui c'est genre Usagers / Collectivité1 / etc., et du coup prendre l'autorisation attachée à l'OU ça voudrait dire qu'un utilisateur de l'OU en premier se connecte et accorde l'autorisation et que ça vaut pour tout le monde.

Non, ce n'est pas un utilisateur nécessairement de l'OU qui autorise, quand tu dis pour tout le monde, il faut comprendre non pas tous les usagers mais bien tous les clients de cette OU.

Exemple, sur la métropole de Lille, un usager dans l'OU Tourcoing qui achète une place assise au vélodrome de Roubaix pour voir l'arrivée du Paris-Roubaix donnerait l'autorisation "J'autorise la ville de Roubaix a accéder à l'adresse email liée à mon compte Lille métropole."
Derrière, les clients "Organisateurs événementiels" et "Service communication" de l'OU Roubaix, s'il sont configurés pour l'autorisation par OU, bénéficient du consentement.

> - les OU c'est ici autre chose une utilisation parallèle pour grouper des services personne dedans et un utilisateur se connecte et accorde l'autorisation et ça vaut aussi pour les autres services de l'OU en question.

C'est une vision non strictement GRC qui n'est qu'une généralisation dc ce que j'écris deux lignes plus haut, mais qui je crois ne remet pas en cause notre usage des OUs.

> La première compréhension n'a pas tellement de sens, surtout amène trop de nouvelles questions, et donc ça serait l'autre mais ça me semble totalement quelque chose jamais fait et un détournement de l'usage courant des OU et bien bizarre aussi, au final.

(Oui, ce n'est pas de ça dont il est question.)

> Reste que si on est dans le cas 2, avec une autorisation accordée par l'usager connecté (et pas un "premier usager qui a accordé et ça vaut pour tout le monde" du cas 1), je dirais que ça appelle plutôt à gérer l'existence de telles autorisations sur la page en question, ce qui veut sans doute juste dire trouver un terme englobant pour "service/organisation", plutôt que faire ce patch que je ne comprends de toute façon pas mais

> qui retire la possibilité de contrôler ces autorisations.

Ok je comprends l'argument mais il faut trouver les termes pour mettre clients et OU dans la même page sans que l'usager soit perdu.

> Option "retirer la possibilité de contrôler ces autorisations" qui lance vers le cas 1, parce que si les autorisations sont accordées par quelqu'un d'autre, c'est alors compréhensible de ne pas pouvoir les retirer.

(Pas compris. Ce que tu dis ici n'est pas lié au fait que les consentements portent sur un service ou une OU, non ? (En plus de l'idée de "consentement donné par quelqu'un d'autre" que je ne vois pas être autre chose qu'un dangereux oxymore))

#10 - 01 août 2020 11:32 - Paul Marillonnet

Frédéric Péters a écrit :

> Mon souhait de réponse étant qu'on me pointe un endroit où c'est concrètement utilisé, et si ce n'est utilisé nulle part, j'aurai une tendance à vouloir alors dégager/ignorer ces options théoriques qui empêchent d'avancer sur les considérations réelles.

Je ne sais pas, mais je vois des endroits où c'est concrètement utilisable. J'ai posé le patch qui va logiquement avec, dans #45651, parce que ça m'a littéralement pris 10 min pour plagier Nico :)
À voir si on va vers ça ou pas.

#11 - 01 août 2020 11:51 - Frédéric Péters

Ok je vois mieux et mon propos est donc que ça doit être une unique page, parce que c'est justement taper ça dans des pages différentes qui va perdre l'usager.

Alors, ce que je disais :

> ce qui veut sans doute juste dire trouver un terme englobant pour "service/organisation",

et que tu reprends

> mais il faut trouver les termes pour mettre clients et OU.

Je ne pense pas ça compliqué, la question se contourne, aujourd'hui on a la phrase "Vous avez autorisé un service à accéder à vos données de profil.", ça peut juste devenir "Vous avez accordé des autorisations d'accès à vos données de profil" ou "Vous avez autorisé certains accès à vos données de profil", genre.

#12 - 05 août 2020 11:06 - Paul Marillonnet

Frédéric Péters a écrit :

> Ok je vois mieux et mon propos est donc que ça doit être une unique page, parce que c'est justement taper ça dans des pages différentes qui va perdre l'usager.

Ok, c'est proposé dans #45651-3.

> Je ne pense pas ça compliqué, la question se contourne, aujourd'hui on a la phrase "Vous avez autorisé un service à accéder à vos données de profil.", ça peut juste devenir "Vous avez accordé des autorisations d'accès à vos données de profil" ou "Vous avez autorisé certains accès à vos données de profil", genre.

Sans chercher à trouver un intitulé qui conviendrait pour les deux, j'ai mis dans deux div différentes, donc avec deux intitulés différents. L'usager voit d'abord les autorisations données à l'échelle des OUs puis à l'échelle des services.

#13 - 05 août 2020 11:07 - Paul Marillonnet

- Statut changé de Solution proposée à Fermé

Et donc ce ticket n'est plus un bug mais un comportement qui sera cadré par #45651. Je pense qu'on peut fermer ici.

Fichiers

0001-idp_oidc-ban-any-ou-based-authz-from-service-authz-p.patch	2,78 ko	01 août 2020	Paul Marillonnet
0001-idp_oidc-ban-any-ou-based-authz-from-service-authz-p.patch	3,12 ko	01 août 2020	Paul Marillonnet