django-mellon - Support #50138

gérer le cas ou plusieurs comptes matchent les critères de LOOKUP_BY_ATTRIBUTES

14 Jan 2021 03:27 PM - Serghei Mihai

Status:	Information nécessaire	**Start date:**	14 Jan 2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Patch proposed:	No	**Planning:**	No

Description

Un agent qui a plusieurs comptes avec le même mail dans Publik et se fédére avec la l'IDP de la collectivité ou il a cette même adresse mail, arrive sur Publik avec un compte nouveau, alors qu'il s'attendrait d'être lié à un des comptes existants (et retrouver les rôles qui y ont été associés).

La critères définis dans LOOKUP_BY_ATTRIBUTES pourraient être plus explicites, mais s'ils ne le sont pas seul un warning est levé dans les logs:

```
            logger.warning('looking for user by attributes %r: too many users found(%d), failing',
                           lookup_by_attributes, len(users))
```

et un nouveau compte est créé.

On pourrait lier systématiquement à un des comptes locaux trouvés (le premier?) et avoir un setting qui désactive cela.

History

#2 - 14 Jan 2021 04:11 PM - Benjamin Dauvergne

- Status changed from Nouveau to Information nécessaire

On a éclaircir le problème du client d'abord avant de vouloir écrire du code, on a deux LDAP et un IdP SAML, a priori je ne connais pas les liens entre eux.

#4 - 18 Jan 2021 02:47 PM - Serghei Mihai

Constaté de nouveau sur l'instance de Villeurbanne, où 2 comptes (issus de l'annuaire, dans la même OU) ont le même mail.

#5 - 18 Jan 2021 02:49 PM - Nicolas Roche

(J'ai un peu peur d'embrouiller le ticket avec une problématique qui n'a rien à voir : 2 adfs. Dans #44499 on a conclu que finalement c'est plutôt bien qu'un agent puisse avoir 2 casquettes ; ici se serait : être connecté depuis la mairie ou depuis l'extérieur.)

#6 - 18 Jan 2021 03:07 PM - Benjamin Dauvergne

Le problèmes ce n'est pas n LDAP, ou n ADFS, c'est est-ce que l'annuaire derrière tout ça est le même et donc même compte, et donc on peut trouver un identifiant commun à mettre dans un attribut pour activer LOOKUP_BY_ATTRIBUTES ou bien non. Autre chose, dans le cas où on a provisionning via LDAP + ADFS, il faut désactiver la création dans la configuration Mellon, comme ça impossible de créer un compte différent de ceux dans le LDAP.

> Constaté de nouveau sur l'instance de Villeurbanne, où 2 comptes (issus de l'annuaire, dans la même OU) ont le même mail.

Donc 2 comptes du même annuaire ont le même mail ? Donc le mail n'est pas le bon attribut pour raccorder à l'ADFS, utilisons le sAMAccountName qui ne peut être commun, si on a une forêt au cul de l'ADFS (i.e. plusieurs annuaire et donc sAMAccountName commun possible) alors il utiliser

UserPrincipalName qui lui sera unique car incluant le domaine.

#7 - 18 Jan 2021 03:29 PM - Serghei Mihai

Benjamin Dauvergne a écrit :

> Donc 2 comptes du même annuaire ont le même mail ? Donc le mail n'est pas le bon attribut pour raccorder à l'ADFS, utilisons le sAMAccountName qui ne peut être commun, si on a une forêt au cul de l'ADFS (i.e. plusieurs annuaire et donc sAMAccountName commun possible) alors il utiliser UserPrincipalName qui lui sera unique car incluant le domaine.

Mille fois d'accord avec toi, mais lorsque malgré des critères de recherche poussés on tombe sur plusieurs comptes il ne faut pas en créer un nouveau, IMO, quitte à s'arrêter et lever une erreur (genre plusieurs comptes existent, blah blah. Contactez votre admin pour qu'il revoie les critères).