

Authentic 2 - Development #43585

Accès aux attributs LDAP suite à une reconnexion en tant qu'un autre utilisateur

03 juin 2020 15:52 - Benjamin Renard

Statut:	Fermé	Début:	03 juin 2020
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		

Description

Suite aux dernières évolutions de la fonctionnalité de reconnexion en tant qu'un autre utilisateur, les attributs issus de l'annuaire LDAP ne sont plus propagés aux services auxquels l'utilisateur tente d'accéder. Seuls les attributs stockés dans Authentic sont accessibles (identifiant & courriel par exemple).

Cette régression est assez gênante, car il est assez courant de mettre en place un filtrage d'accès par exemple sur une valeur issue d'un attribut LDAP et dans ce cas précis, l'utilisateur se voit interdire l'accès. La fonctionnalité de reconnexion en tant qu'un autre utilisateur perd donc beaucoup de son intérêt avec cette contrainte.

Serait-il envisageable de corriger cela ?

Exemple pour reproduire ce problème:

1. configurer un service (via SAML par exemple) avec un attribut issu de l'annuaire
2. se connecter avec un utilisateur admin
3. dans l'interface `/manages/users/XXX`, se reconnecter avec un autre utilisateur
4. tenter d'accéder au service configuré initialement

L'attribut SAML ne sera alors pas renseigné bien qu'existant dans l'annuaire LDAP.

Révisions associées

Révision c70f2059 - 09 avril 2021 14:47 - Benjamin Dauvergne

views: use LDAPBackendPasswordLost to switch to LDAP account (#43585)

Historique

#1 - 03 juin 2020 17:51 - Benjamin Dauvergne

Ça n'a jamais marché comme cela avant, les attributs LDAP ont toujours été indisponible; c'était un effet de bord qui faisait que si l'utilisateur précédent venait du backend LDAP le suivant aussi (mais a priori en sens inverse ça devait bugger) :

```
-def su(request, username, redirect_url='/'):  
-     '''To use this view add:  
-  
-     url(r'^su/(?P<username>.*)/$', 'authentic2.views.su', {'redirect_url': '/'}),  
-     '''  
-     if request.user.is_superuser or request.session.get('has_superuser_power'):  
-         su_user = shortcuts.get_object_or_404(User, username=username)  
-         if su_user.is_active:  
-             request.session[SESSION_KEY] = su_user.id  
-             request.session['has_superuser_power'] = True  
-             return http.HttpResponseRedirect(redirect_url)  
-     else:  
-         return http.HttpResponseRedirect('/')
```

Je faisais des manipulations limitées en session, mais je ne changeais pas le backend, il faudrait traiter cela de façon particulière, à la manière du backend LDAPBackendPasswordLost.

#2 - 01 avril 2021 16:53 - Loïc Dachary

Pour archive, bien que LDAPBackendPasswordLost fonctionne comme attendu les attributs ne sont pas disponibles, mais [pour une autre raison](#)

#3 - 01 avril 2021 17:34 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 01 avril 2021 17:37 - Benjamin Dauvergne

- Fichier 0001-views-use-LDAPBackendPasswordLost-to-switch-to-LDAP-.patch ajouté
- Tracker changé de Bug à Development
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

Au dessus de [#52638](#) pour avoir un simulate_authentication() qui respecte le user.backend déjà présent.

#5 - 08 avril 2021 14:37 - Loïc Dachary

- Fichier 0001-views-use-LDAPBackendPasswordLost-to-switch-to-LDAP-.patch ajouté

Après rebase sur main ([#52638](#) a été merge) j'ai pu vérifier que le test passe.

#6 - 09 avril 2021 15:10 - Benjamin Dauvergne

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

```
commit c70f205987e6660edeb4a6dbed06bf19b6905b9b
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Thu Apr 1 17:36:54 2021 +0200
```

```
views: use LDAPBackendPasswordLost to switch to LDAP account (#43585)
```

#7 - 30 avril 2021 11:17 - Frédéric Péters

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

Fichiers

0001-views-use-LDAPBackendPasswordLost-to-switch-to-LDAP-.patch2,28 ko	01 avril 2021	Benjamin Dauvergne
0001-views-use-LDAPBackendPasswordLost-to-switch-to-LDAP-.patch2,29 ko	08 avril 2021	Loïc Dachary