

Authentic 2 - Bug #20731

crash LDAP sur changement de mot de passe

15 décembre 2017 10:10 - Thomas Noël

Statut:	Fermé	Début:	15 décembre 2017
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	100%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	
Patch proposé:	Oui		
Description			
Il semble qu'en cas de backend LDAP Authentic cherche à modifier le mot de passe sur ce dernier, mais qu'en cas de problème on ait un crash, cf #20729 et trace visible sur la copie d'écran attachée			

Révisions associées

Révision 93b2cf18 - 17 juillet 2018 01:05 - Benjamin Dauvergne

disable password change for LDAP backend without user_can_change_password (fixes #20731)

Révision 26d39e05 - 17 juillet 2018 11:25 - Benjamin Dauvergne

tests: adapt test to new organization name (#20731)

Historique

#3 - 15 décembre 2017 11:28 - Thomas Noël

- Fichier FireShot Capture 1 - INSUFFICIENT_ACCESS at _accounts_passw_ - <https://connexion-preprod-moncompte.png> supprimé

#5 - 03 juillet 2018 09:42 - Frédéric Péters

Autre trace possible sur la même cause, non pas INSUFFICIENT_ACCESS mais UNWILLING_TO_PERFORM :

```
File "/usr/lib/python2.7/dist-packages/authentic2/backends/ldap_backend.py", line 177, in set_password
    self.ldap_backend.modify_password(conn, self.block, self.dn, old_password, new_password)
File "/usr/lib/python2.7/dist-packages/authentic2/backends/ldap_backend.py", line 975, in modify_password
    conn.modify_s(dn, modlist)
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 357, in modify_s
    return self.result(msgid,all=1,timeout=self.timeout)
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 458, in result
    resp_type, resp_data, resp_msgid = self.result2(msgid,all,timeout)
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 462, in result2
    resp_type, resp_data, resp_msgid, resp_ctrls = self.result3(msgid,all,timeout)
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 469, in result3
    resp_ctrl_classes=resp_ctrl_classes
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 476, in result4
    ldap_result = self._ldap_call(self._l.result4,msgid,all,timeout,add_ctrls,add_intermediates,add_extop)
File "/usr/lib/python2.7/dist-packages/ldap/ldapobject.py", line 99, in _ldap_call
    result = func(*args,**kwargs)
UNWILLING_TO_PERFORM: {'info': '00002077: SvcErr: DSID=03190E49, problem 5003 (WILL_NOT_PERFORM), data 0\n', '
desc': 'Server is unwilling to perform'}
```

#6 - 03 juillet 2018 10:10 - Benjamin Dauvergne

- Statut changé de Nouveau à Solution proposée

- Assigné à mis à Benjamin Dauvergne

Même réponse que #20729:

Il faut dire que les utilisateurs n'ont pas le droit de changer de mot de passe:

```
# Can users change their password ?
'user_can_change_password': True,
```

mettre False.

#7 - 03 juillet 2018 10:13 - Benjamin Dauvergne

Bon le unwilling to perform ça peut aussi venir de la politique de mot de passe coté AD¹, peut-être faudrait-il le récupérer mais malheureusement on a pas moyen de faire remonter l'erreur jusqu'au formulaire :/

[1]: <https://communities.ca.com/thread/241769648-password-reset-failed-code-53-unwillingtoperform>

Donc une autre solution possible c'est de voir comment catcher toute erreur sur .set_password() et la rapporter plus ou moins proprement sur le formulaire.

#8 - 03 juillet 2018 10:14 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

Bon le unwilling to perform ça peut aussi venir de la politique de mot de passe coté AD¹, peut-être faudrait-il le récupérer mais malheureusement on a pas moyen de faire remonter l'erreur jusqu'au formulaire :/

[1]: <https://communities.ca.com/thread/241769648-password-reset-failed-code-53-unwillingtoperform>

Donc une autre solution possible c'est de voir comment catcher toute erreur sur .set_password() et la rapporter plus ou moins proprement sur le formulaire.

En plus AD ne rapporte le détail de l'erreur (trop long, pas assez long, déjà utilisé, who knows...).

#9 - 03 juillet 2018 14:54 - Benjamin Dauvergne

- Statut changé de Solution proposée à Nouveau

Bon en fait le souci ici c'est que ça ne marche plus, à un moment [1] on a changé le comportement de la vue de changement de mot de passe qui si l'utilisateur n'avait pas un mot de passe "utilisable" refusait d'en définir un. Maintenant c'est possible. Sauf que le backend LDAP utilisait justement la méthode .has_usable_password() pour passer la valeur de 'user_can_change_password', surcharge sémantique malheureuse. Maintenant qu'on peut définir (et non plus juste redéfinir) un mot de passe over LDAP ça ne marche plus.

Bon ce que ça veut dire c'est qu'il faut une méthode .can_change_password() dont le sens sera évident.

[1]:

```
commit 2ba49444042e560ef1c943c1fb6f7af00946c0
Author: Mikaël Ates <mates@entrouvert.com>
Date: Wed Apr 20 22:13:51 2016 +0200
```

```
Adapt account management when the user has no password (fixes #10658).
```

#10 - 04 juillet 2018 10:39 - Benjamin Dauvergne

- Fichier 0001-disable-password-change-for-LDAP-backend-without-use.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#11 - 16 juillet 2018 07:52 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

Sujet de commit un peu trop long mais je ne propose pas de reformulation.

#12 - 17 juillet 2018 01:07 - Benjamin Dauvergne

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

- % réalisé changé de 0 à 100

Appliqué par commit [authentic293b2cf189dab8c925016a3eddf1e464069278a3e](https://communities.ca.com/thread/241769648-authentic293b2cf189dab8c925016a3eddf1e464069278a3e).

#13 - 13 décembre 2018 22:29 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-disable-password-change-for-LDAP-backend-without-use.patch	5,34 ko	04 juillet 2018	Benjamin Dauvergne
---	---------	-----------------	--------------------