Authentic 2 - Development #50959

ldap: log controls on authenticate and enable ppolicy

09 février 2021 08:54 - Loïc Dachary

Statut:	Fermé	**Début:**	09 février 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:	LDAP	**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Un baby step pour activer ppolicy dans les tests et dans le backend ldap sur la fonction authenticate. D'une valeur ajoutée assez faible en soit: n'hésitez pas à dire si ça n'est pas du tout comme ça qu'il faut aborder la question. Je me suis cultivé sur le sujet ces derniers jours mais je reste assez vert.

Demandes liées:

Dupliqué par Authentic 2 - Development #51003: ldap: enable custom messages f...	**Fermé**	**10 février 2021**
Dupliqué par Authentic 2 - Development #51035: affichage d'une page avant red...	**Fermé**	**11 février 2021**

Révisions associées

Révision 814e0192 - 16 février 2021 18:37 - Loïc Dachary

ldap: optionally collects messages from ppolicy

Enable PasswordPolicyControl[0] in authenticate() and log the
information it returns, on success or error. In the context of a
request, this information is also set as a message[1] to be displayed
to the user.

[0] https://github.com/python-ldap/python-ldap/blob/python-ldap-3.3.1/Lib/ldap/controls/ppolicy.py
[1] https://docs.djangoproject.com/en/3.1/ref/contrib/messages/

Fixes: #50959

License: MIT

Historique

#1 - 09 février 2021 08:57 - Loïc Dachary

- Fichier 0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch ajouté

Merci d'ignorer le patch précédente, voici celui que j'avais l'intention d'envoyer.

#2 - 09 février 2021 18:45 - Loïc Dachary

- Fichier 0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch ajouté

Nouvelle version qui corrige deux problèmes. D'abord que c'est pas très utile d'avoir une référence à un objet python dans les logs et c'est mieux d'avoir les attributs de l'objet et leur valeur. Et ensuite que ça marchait pas du tout parce que {1}mdb était utilisé dans le test alors que c'est {2}mdb qui a la ppolicy active. Un assert a été ajouté pour vérifier que la réponse est loggée au lieu de rien.

#3 - 11 février 2021 02:33 - Loïc Dachary

- Fichier 0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch ajouté

Nouvelle version qui ajoute des tests et produit des messages lisibles par un être humain, et i18n. Au passage je rencontre un mystérieux problème en testant **pwdGraceAuthnLimit** . La valeur décroît comme elle est supposé le faire. Mais quand elle arrive à 1 elle ne bouge plus et l'utilisateur peut toujours se loggé, ce qui n'est pas vraiment l'objectif. Le test qui montre le problème est **test_authenticate_ppolicy_pwdGraceAuthnLimit**.

#4 - 11 février 2021 11:06 - Loïc Dachary

- Fichier 0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch ajouté

L'objectif n'étant pas de vérifier le comportement du serveur LDAP mais d'assurer la couverture du code fourni, j'ai enlevé l'assert qui échoue (voir

https://dev.entrouvert.org/issues/50959#note-3).

Cette nouvelle version du patch inclus

- un test pour pwdExpireWarning
- une version human readable pour tout les messages d'erreur
- une traduction française pour tous les messages

#5 - 11 février 2021 14:14 - Loïc Dachary

- Fichier 0001-ldap-optionally-collects-messages-from-ppolicy.patch ajouté

Cette version du patch est prête pour un review et les tests qu'il contient passent. Je ne doute pas qu'il faille changer des choses mais comme je trouve que l'ensemble est cohérent et que je pense qu'il fait ce qu'on attend, je vais m'abstenir d'avancer plus pour l'instant. L'affichage des messages via MessageMiddleware étant trivial, je l'ai ajouté ici au lieu d'en faire un patch séparé (merci Benjamin :-)).

#6 - 11 février 2021 14:53 - Benjamin Dauvergne

- Statut changé de Nouveau à En cours

On a encore des machines en python 3.5, donc pas de f-string dans le code pour l'instant (f'The password will expire in {ctrl.timeBeforeExpiration} seconds.').

Les messages de log sont un peu succincts : log.info('%s: %s', authz_id, message) un suffixe (je sais il n'y en a pas ailleurs) style 'ldap: bind error with authz_id "%s" -> "%s"' serait plus lisible.

Expliciter le nom des variables retour plutôt que de créer un tuple ici :

```
                            results = conn.simple_bind_s(authz_id, password, serverctrls=[
                                ppolicy.PasswordPolicyControl()
                            ])
                            self.process_controls(request, authz_id, results[3])
```

On a des logs en base lisibles depuis le back-office, ex.:

```
src/authentic2/authenticators.py:139:                    request.journal.record('user.login.failure', username
=username)
```

ça n'enregistre pas le type d'erreur mais c'est extensible dans authentic2.journal_event_types; ça peut être un objectif pour un autre ticket, mais je le note ici quand même.

Pour ça m'a l'air bon j'ai juste une petite inquiétude sur le comportement des serveurs LDAP ne supportant pas cette extension. Par défaut les protocoles utilisant ASN/1 comme LDAP ou TLS utilisent un flag "criticalité" sur les extensions, qui la plupart du temps est à False, signifiant "si tu ne comprends pas cette extension, ce n'est pas grave ignore", c'est le cas sur PasswordPolicyControl par défaut avec python3-ldap :

```
$ grep criticality  /usr/lib/python3/dist-packages/ldap/controls/ppolicy.py
  def __init__(self,criticality=False):
    self.criticality = criticality
```

mais j'ai peur des serveurs qui ne feraient pas leur job correctement. Est-ce que tu pourrais entourer l'ajout du contrôle dans la requête de bind par un setting par défaut activé ? Si ça pose un souci j'aimerai pouvoir désactiver l'ajout du contrôle facilement.

#7 - 11 février 2021 15:08 - Loïc Dachary

Pour archive cross ref de mes notes de découverte dans ce contexte https://listes.entrouvert.com//arc/authentic/2021-02/msg00000.html

#8 - 11 février 2021 16:10 - Loïc Dachary

- Fichier 0001-ldap-optionally-collects-messages-from-ppolicy.patch ajouté

- Fichier 0002-ldap-do-not-use-f-for-python-3.5-compatibility.patch ajouté

- Fichier 0003-ldap-log-a-more-verbose-error-message.patch ajouté

- Fichier 0004-ldap-bind-serverctrls-is-not-used-when-use_controls-.patch ajouté

Merci pour la review détaillée. Je suis aussi très soulagé de ne pas m'être engagé dans une voie de garage, pfuiiii :-) Dans la série de patch tu trouveras le patch original histoire de tout avoir ensemble et un commit par modification pour que ce soit plus facile a relire.

#9 - 11 février 2021 17:43 - Benjamin Dauvergne

- Dupliqué par Development #51003: ldap: enable custom messages from backends when login fails ajouté

#10 - 11 février 2021 18:43 - Benjamin Dauvergne

La mise à jour des traductions est faite quand nous "taggons" une release, on préfère que ce ne soit pas mélanger aux commits sur le code (dsl j'aurai du faire la remarque avant, ça m'a échappé), ça nous permet une plus grande cohérence dans les termes usités et de se poser sur les traductions quand c'est nécessaire.

On préfère aussi les commits regroupés, on ne souhaite pas voir le cheminement pris au cours du développement (ici ajout puis retrait des f-strings) dans l'historique, un ticket = un commit si possible sauf si il y a plusieurs sujets disjoints traités en même temps. Donc il faudrait faire un fixup des 4 commits en un seul via git rebase.

```
        slapd.add_ldif(open('/etc/ldap/schema/ppolicy.ldif').read())
```

Utilise with open(...) as fd:...(fd.read) ça fait des warnings casse pieds sur les ressources non libérés quand on vérifie les warnings ensuite (pareil pas vu avant, j'ai pas jeté un gros coup d'oeuil aux tests).

Je vois dans les tests :

```
def test_authenticate_ppolicy_pwdAllowUserChange(slapd_ppolicy, settings, db, caplog):
...
    with pytest.raises(ldap.STRONG_AUTH_REQUIRED):
        user.set_password(u'ogutOmyetew4')
```

Plutôt que de faire d'une exception non interceptée un pré-requis des tests ce serai mieux de les cacher. Réutiliser User.set_password(...) pour modifier le mot de passe d'un annuaire casse de toute façon la sémantique espérée par Django[1] (normalement ça ne touche qu'à la base locale où ça ne peut "normalement" pas échouer). Ici il serait mieux de simplement logger l'erreur avec log.error(...) et cacher l'erreur à la vue de changement de mot de passe. Pour l'instant on ne peut pas faire beaucoup mieux. Le test peut vérifier cela par contre (via la fixture caplog).

Dans ce cas précis ça peut être dans un commit séparé, parce que je ne vois pas trop le rapport direct avec ppolicy ici (ça arrivera aussi dans le cas où les ACLs d'OpenLDAP ou AD ne permettent pas la modification du mot de passe pour des raisons diverses et variées, comme le faot que l'IP du client soit hors du LAN, et dans ce cas l'erreur n'est même pas STRONG_AUTH_REQUIRED je pense mais UNWILLING_TO_PERFORM ou un truc du genre obscure pour AD).

[1] https://github.com/django/django/blob/1.11.29/django/contrib/auth/forms.py#L353

#11 - 11 février 2021 18:52 - Benjamin Dauvergne

- Dupliqué par Development #51035: affichage d'une page avant redirection SSO ajouté

#12 - 12 février 2021 00:02 - Loïc Dachary

- Fichier 0001-ldap-optionally-collects-messages-from-ppolicy.patch ajouté

- Les traductions ont été enlevées
- Les commits sont squash en un seul
- open a été remplacé par with open
- Des modifications mineures de lisibilité ont été faites sur les messages
- L'exception ldap.STRONG_AUTH_REQUIRED est ignorée et loggée. Elle est levée lorsque **pwdAllowUserChange: FALSE** raison pour laquelle elle se trouve dans ce commit mais je peux la mettre dans un commit séparé si tu le souhaites.

Merci pour les reviews, ça fait plaisir de voir ça avancer :-)

#13 - 15 février 2021 09:30 - Benjamin Dauvergne

- Statut changé de En cours à Solution validée

#14 - 15 février 2021 09:41 - Loïc Dachary

\o/

#15 - 15 février 2021 09:42 - Loïc Dachary

Bon, j'imagine que pylint va crier très fort: ce serait très surprenant que le patch ne le froisse pas d'une façon ou d'une autre. Est-ce qu'il y a moyen d'avoir le fichier de configuration de pylint pour faire la vérification avant soumission ? Merci !

#16 - 15 février 2021 14:33 - Benjamin Dauvergne

Loïc Dachary a écrit :

> Bon, j'imagine que pylint va crier très fort: ce serait très surprenant que le patch ne le froisse pas d'une façon ou d'une autre. Est-ce qu'il y a moyen d'avoir le fichier de configuration de pylint pour faire la vérification avant soumission ? Merci !

Nous ne sommes pas très à cheval sur les résultats pylint, c'est juste informatif.

#17 - 16 février 2021 18:55 - Benjamin Dauvergne

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

```
commit 814e0192f33ce13b7cf6630b21c19a3dcddc8c86
Author: Loïc Dachary <ldachary@easter-eggs.com>
Date:   Tue Feb 9 08:46:22 2021 +0100

    ldap: optionally collects messages from ppolicy

    Enable PasswordPolicyControl[0] in authenticate() and log the
    information it returns, on success or error. In the context of a
    request, this information is also set as a message[1] to be displayed
    to the user.

    [0] https://github.com/python-ldap/python-ldap/blob/python-ldap-3.3.1/Lib/ldap/controls/ppolicy.py
    [1] https://docs.djangoproject.com/en/3.1/ref/contrib/messages/

    Fixes: #50959

    License: MIT
```

#18 - 16 février 2021 19:00 - Loïc Dachary

- % réalisé changé de 0 à 100

Appliqué par commit authentic2|814e0192f33ce13b7cf6630b21c19a3dcddc8c86.

#19 - 17 février 2021 08:23 - Loïc Dachary

Je m'attendais à voir un résultat de jenkins apparaitre ici, il y a une raison pour laquelle ce n'est pas le cas ? En tout cas content et pas peu fier de ce premier commit non trivial :-) Merci pour le suivi rapide et surtout pour les reviews tres détaillées et claires.

#20 - 18 février 2021 14:37 - Benjamin Dauvergne

- % réalisé changé de 100 à 0

Loïc Dachary a écrit :

> Je m'attendais à voir un résultat de jenkins apparaitre ici, il y a une raison pour laquelle ce n'est pas le cas ? En tout cas content et pas peu fier de ce premier commit non trivial :-) Merci pour le suivi rapide et surtout pour les reviews tres détaillées et claires.

L'intégration jenkins ne concerne que les branches wip/* sur notre dépôt, elle est faite de manière ad-hoc en javascript (appel ajax de redmine vers jenkins en cherchant une branche wip/<numéro-du-ticket>-.*.

#21 - 05 novembre 2021 13:11 - Frédéric Péters

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

(pas de ref ticket dans le commit)

Fichiers

0001-ldap-additional-tests-for-the-keep_password-function.patch	1,41 ko	09 février 2021	Loïc Dachary
0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch	4,4 ko	09 février 2021	Loïc Dachary
0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch	4,81 ko	09 février 2021	Loïc Dachary
0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch	9,26 ko	11 février 2021	Loïc Dachary
0001-ldap-log-controls-on-authenticate-and-enable-ppolicy.patch	13,5 ko	11 février 2021	Loïc Dachary
0001-ldap-optionally-collects-messages-from-ppolicy.patch	16,3 ko	11 février 2021	Loïc Dachary
0001-ldap-optionally-collects-messages-from-ppolicy.patch	16,3 ko	11 février 2021	Loïc Dachary
0002-ldap-do-not-use-f-for-python-3.5-compatibility.patch	6,67 ko	11 février 2021	Loïc Dachary

0003-ldap-log-a-more-verbose-error-message.patch	1,29 ko	11 février 2021	Loïc Dachary
0004-ldap-bind-serverctrls-is-not-used-when-use_controls-.patch	4,71 ko	11 février 2021	Loïc Dachary
0001-ldap-optionally-collects-messages-from-ppolicy.patch	16,5 ko	11 février 2021	Loïc Dachary