Authentic 2 - Development #66416

Ajout du support de ppolicy lors de la modification du mot de passe

20 juin 2022 14:59 - Benjamin Renard

Statut:	Fermé	**Début:**	20 juin 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Nous avions par le passé ajouté le support de ppolicy lors de la connexion et autre client nous demande aujourd'hui de l'ajouter lors du changement de mot de passe (changement & réinitialisation). Aujourd'hui, en cas de mot de passe refusé par l'annuaire LDAP (du fait de ppolicy ou non d'ailleurs), Authentic renvoi une erreur 500 sans précision. L'idée serait ici d'ajouter ici le contrôle *PasswordPolicyControl* lors de la modification du mot de passe d'un utilisateur (*LDAPUser.set_password*) comme cela avait été fait lors de la connexion (*LDAPBackend.authenticate_block*) de manière paramétrable via le paramètre *use_controls* existant.

Demandes liées:

Lié à Authentic 2 - Development #82521: ppolicy : désactiver l'exécution des ...	**Nouveau**	**18 octobre 2023**

Révisions associées

Révision a27ef68c - 17 octobre 2023 10:10 - Benjamin Renard

test_ldap: use USERNAME & PASS instead of hard-coded values (#66416)

Licence: MIT

Révision 42961dad - 17 octobre 2023 10:10 - Benjamin Renard

password_policy_control_messages: fix handling passwordExpired (#66416)

Licence: MIT

Révision c309d20a - 17 octobre 2023 10:10 - Benjamin Renard

ldap: fix encoding password on modify_password (#66416)

Licence: MIT

Révision fddbade0 - 17 octobre 2023 10:10 - Benjamin Renard

ldap: rename process_controls method to process_bind_controls (#66416)

Licence: MIT

Révision 3d10be82 - 17 octobre 2023 10:10 - Benjamin Renard

ldap: handle ppolicy controls at password-reset time (#66416)

Licence: MIT

Révision c4289cda - 17 octobre 2023 10:10 - Benjamin Renard

ppolicy: handle reset redirect after a changeAfterReset error (#66416)

Licence: MIT

Révision 284d1851 - 17 octobre 2023 10:10 - Benjamin Renard

ldap: set sharper ppolicy_control error messages when relevant (#66416)

License: MIT

Révision 20f98dd9 - 17 octobre 2023 10:10 - Benjamin Renard

ldap: improve password expiration date formatting (#66416)

License: MIT

Révision 7c7c631f - 17 octobre 2023 10:10 - Benjamin Renard

password_change: stay on form page when ldap ppolicy errors happen (#66416)

License: MIT

Révision ad06d282 - 17 octobre 2023 10:10 - Benjamin Renard

password_reset_confirm: handle ldap ppolicy errors (#66416)

License: MIT

Révision 554491b1 - 17 octobre 2023 10:10 - Benjamin Renard

tests/ldap: fix conflicting access rights with slapd>2.4 (#66416)

License: MIT

Révision 376c66a9 - 17 octobre 2023 10:10 - Paul Marillonnet

ldap: use a separate backend config flag for ppolicy controls (#66416)

Révision 38d52ede - 17 octobre 2023 10:30 - Paul Marillonnet

translation update (#66416)

Historique

#1 - 20 juin 2022 15:15 - Benjamin Renard

J'ai commencé à regarder le sujet et cela ne semble pas très compliqué. La seule problématique qui me pose problème c'est de savoir remonter l'erreur correctement à l'utilisateur. En effet, la méthode *set_password* étant appelée par la méthode *save* des formulaires Django et il ne suffit donc pas de déclencher simplement une exception *ValidationError*. J'ai fait quelques recherches sur le sujet et je n'ai pas trouvé de solution simple et propre documentée pour cela. Avez-vous une idée de comment faire ?

PS : dans l'idéal, on aurait pu tenter d'utiliser la fonctionnalité LDAPv3 *Grouping of Related Operations* pour implémenter une validation via *form.clean* avant *form.save*, mais cela n'est pas encore supporté par python ldap3 (et j'ai pas trouvé si c'était le cas par OpenLDAP).

#2 - 27 juin 2022 15:05 - Benjamin Renard

Benjamin Renard a écrit :

> J'ai commencé à regarder le sujet et cela ne semble pas très compliqué. La seule problématique qui me pose problème c'est de savoir remonter l'erreur correctement à l'utilisateur. En effet, la méthode *set_password* étant appelée par la méthode *save* des formulaires Django et il ne suffit donc pas de déclencher simplement une exception *ValidationError*. J'ai fait quelques recherches sur le sujet et je n'ai pas trouvé de solution simple et propre documentée pour cela. Avez-vous une idée de comment faire ?

Je me permets une petite relance sur le sujet : une idée pour ma problématique exposée ci-dessus ?

#3 - 22 septembre 2022 18:28 - Benjamin Renard

- Fichier 0005-ldap-handle-ppolicy-control-changing-reseting-passwo.patch ajouté

Le patch ci-joint implémente la gestion de *PasswordPolicyControl* en cas de modification ou de réinitialisation du mot de passe. Comme proposé, cela reste conditionné à l'activation du paramètre de configuration *use_controls* (au niveau du block), comme c'est le cas pour le support de l'authentification.

#4 - 19 octobre 2022 14:35 - Benjamin Dauvergne

- j'ai l'impression qu'il y a la correction d'un bug dans le tas :

```
                modlist = [(ldap.MOD_REPLACE, key, [new_password.encode('utf-8')])]
```

  si cet encodage est nécessaire il faut le séparer dans un autre patch
- il faudrait découper ça en 3 patchs:
  - renommage process_controls -> process_bind_controls
    - à relire je n'ai pas l'impression qu'il y ait de différence entre les deux méthode à part le message de log, je me trompe ? Dans ce cas autant rendre le message variable et ne garder qu'une méthode,
  - correction citée plus haut
  - enfin l'ajout des contrôles, il faudrait factoriser ces lignes entre les différentes méthodes de modification

Il faudrait des tests.

#5 - 10 novembre 2022 23:38 - Benjamin Renard

- Fichier 0006-Add-tests-on-LDAP-password-change-reset-with-ppolicy.patch ajouté

- Fichier 0005-ldap-handle-ppolicy-control-changing-reseting-passwo.patch ajouté

- Fichier 0004-ldap-rename-process_controls-method-to-process_bind_.patch ajouté

- Fichier 0003-ldap-fix-encoding-password-on-modify_password.patch ajouté

- Fichier 0002-password_policy_control_messages-fix-handling-passwo.patch ajouté

- Fichier 0001-test_ldap-use-USERNAME-PASS-instead-of-duplicated-ha.patch ajouté

Benjamin Dauvergne a écrit :

> - j'ai l'impression qu'il y a la correction d'un bug dans le tas :
> [...]
> si cet encodage est nécessaire il faut le séparer dans un autre patch

Effectivement, contrairement au cas avec un AD, le mot de passe n'était pas encodé, python-ldap requiert un bytes-string. J'ai fait un patch dédié pour ça.

> - il faudrait découper ça en 3 patchs:
>   - renommage process_controls -> process_bind_controls
>   - à relire je n'ai pas l'impression qu'il y ait de différence entre les deux méthodes à part le message de log, je me trompe ? Dans ce cas autant rendre le message variable et ne garder qu'une méthode,

Pas exactement, mais c'est pas loin effectivement : dans le cas du login, on gère la *request* et on affiche le message d'erreur via *messages.add_message()* en plus d'activer *request.needs_password_change* dans certains cas. Dans le cas d'une modification de mot de passe, on affiche l'erreur simplement en levant une exception *PasswordChangeError*.

J'ai mis le renommage dans un commit dédié.

> - correction citée plus haut
> - enfin l'ajout des contrôles, il faudrait factoriser ces lignes entre les différentes méthodes de modification

C'est fait également et dans un commit dédié.

> Il faudrait des tests.

J'ai ajouté des tests via un commit dédié pour chacun des messages d'erreurs gérés sauf *changeAfterReset* que je ne vois pas trop comment provoquer.

Au passage, j'ai également ajouté des patchs pour :

- utiliser les variables *USERNAME* & *PASS* un peu partout dans les tests LDAP au lieu de dupliquer des valeurs hard-codées
- corriger la gestion des erreurs *passwordExpired* (son code vaut zéro et il fallait un donc faire un test à coup de *is not None*)

Note : je précise que les tests sont prévus pour fonctionner une fois l'ensemble des autres patchs intégrés, y compris ceux de #69468, #69466 et #69464.

#6 - 14 novembre 2022 15:37 - Benjamin Renard

- Fichier 0007-ppolicy-handle-reset-password-redirection-after-a-ch.patch ajouté

Benjamin Renard a écrit :

> J'ai ajouté des tests via un commit dédié pour chacun des messages d'erreurs gérés sauf *changeAfterReset* que je ne vois pas trop comment provoquer.

Après réflexion, j'ai trouvé un moyen de tester cette erreur : il faut bloquer le compte à force de connexion avec un mauvais mot de passe, débloquer le compte comme un admin le ferait en spécifiant *pwdReset* à *TRUE* et retenter une connexion avec le bon mot de passe cette fois-ci.

En implémentant ce test, je me suis par ailleurs rendu compte que dans cette situation, on devrait provoquer une redirection vers le formulaire de réinitialisation du mot de passe et non laisser l'utilisateur sur le formulaire de connexion. J'ai donc implémenté cela et ajuster mon test en conséquence.

Note : À ce sujet, je suis pas sûre que j'utilise la bonne manière pour détecter la next URL lors de la redirection vers le formulaire de réinitialisation du

mot de passe.

#7 - 06 décembre 2022 22:12 - Benjamin Dauvergne

- Statut changé de Nouveau à Solution proposée

- Assigné à mis à Benjamin Renard

#8 - 14 décembre 2022 17:10 - Benjamin Renard

Je me permets une petite relance sur le sujet. Notre client nous relance sur le sujet.

#9 - 12 mai 2023 10:24 - Robot Gitea

- Statut changé de Solution proposée à En cours

- Assigné à changé de Benjamin Renard à Paul Marillonnet

Paul Marillonnet (pmarillonnet) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/56
- Titre : WIP: wip/66416-ldap-add-ppolicy-support
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/56/files

#10 - 12 mai 2023 10:28 - Paul Marillonnet

- Assigné à changé de Paul Marillonnet à Benjamin Renard

J'ai rebasé et poussé le tout dans une branche à jour, mais des tests explosent :

```
FAILED tests/test_ldap.py::test_user_change_password_too_short - assert 'The password is too short (minimun le
ngth: 15)' in '<!DOCTYPE html>\n<html>\n  <head>\n    <meta charset="utf-8"/>\n    <title>Authentic2 - testser
ver - \n  Password cha...\n  Co...
FAILED tests/test_ldap.py::test_user_change_password_too_soon - assert 'It is too soon to change the password.
' in '<!DOCTYPE html>\n<html>\n  <head>\n    <meta charset="utf-8"/>\n    <title>Authentic2 - testserver - \n
 Password cha...\n  Copyright ...
FAILED tests/test_ldap.py::test_reset_password_must_supply_old_password - AssertionError: assert 'The old pass
word must be supplied.' in <302 Found text/html location: / no body>
FAILED tests/test_ldap.py::test_login_ppolicy_must_change_password_after_locked - assert 'after 2 failures' in
 '<ul class="messages">\n                  \n                    <li class="warning">The account is locked sin
ce 202305...   \n                </ul>\n        ...
FAILED tests/test_ldap.py::test_user_change_password_not_allowed - assert 'It is not possible to modify the pa
ssword.' in '<!DOCTYPE html>\n<html>\n  <head>\n    <meta charset="utf-8"/>\n    <title>Authentic2 - testserve
r - \n  Password cha...\n  Copyri...
FAILED tests/test_ldap.py::test_login_ppolicy_pwdMaxFailure - assert 'after 2 failures' in '<ul class="message
s">\n                  \n                    <li class="warning">The account is locked since 202305...   \n
            </ul>\n        ...
FAILED tests/test_ldap.py::test_login_ppolicy_password_expired - IndexError: list index out of range
FAILED tests/test_ldap.py::test_user_change_password_in_history - assert 'This password has already been used
and can no longer be used.' in '<!DOCTYPE html>\n<html>\n  <head>\n    <meta charset="utf-8"/>\n    <title>Aut
hentic2 - testserver - \n  Passw...
```

#11 - 05 juillet 2023 20:36 - Benjamin Renard

- Fichier complete.patch ajouté

Paul Marillonnet (retour le 10/07) a écrit :

> J'ai rebasé et poussé le tout dans une branche à jour, mais des tests explosent :
> [...]

J'ai enfin trouvé le temps de regarder cela. Le problème vient principalement du fait que tu n'as pas repris mes patchs des tickets #69468, #69466 et #69464 (cf. la note en fin de #note-5). Je viens de m'occuper de rebaser tous les commits concernés sur votre branche main (b450d83546d60a620baebf09fd5e156714afe931 / v4.88) et je te joins un patch les incluant tous. Chez moi, tous les tests ldap passent bien à l'exception de deux, mais pour le coup, il ne passe pas non plus sans mes patchs, donc je penche pour un problème d'environnement. Et d'ailleurs j'en ai cinq autres du même genre lorsque je lance tous les tests.

#12 - 05 juillet 2023 20:57 - Frédéric Péters

(je viens de pousser cette série dans la branche.)

#13 - 05 juillet 2023 21:17 - Frédéric Péters

> (je viens de pousser cette série dans la branche.)

et le build réussit.

#14 - 06 juillet 2023 12:40 - Benjamin Renard

Frédéric Péters a écrit :

> > (je viens de pousser cette série dans la branche.)
>
> et le build réussit.

Top, tu penses que ce serait intégrable upstream du coup ?

#15 - 06 juillet 2023 12:54 - Frédéric Péters

Paul revient lundi de congés, il reprendra la main.

#16 - 06 juillet 2023 16:16 - Benjamin Renard

Frédéric Péters a écrit :

> Paul revient lundi de congés, il reprendra la main.

Ça marche, merci !

#17 - 10 juillet 2023 14:09 - Paul Marillonnet

- Assigné à changé de Benjamin Renard à Paul Marillonnet

Je commence à relire en détails.

#18 - 11 juillet 2023 10:26 - Paul Marillonnet

Paul Marillonnet a écrit :

> Je commence à relire en détails.

J'ai posé des remarques suite à ma première relecture, directement dans la PR : https://git.entrouvert.org/entrouvert/authentic/pulls/56
Je m'occupe des modifications induites, et poursuis ma relecture entamée hier.

#19 - 13 juillet 2023 18:47 - Benjamin Renard

Paul Marillonnet a écrit :

> Paul Marillonnet a écrit :
>
> > Je commence à relire en détails.
>
> J'ai posé des remarques suite à ma première relecture, directement dans la PR : https://git.entrouvert.org/entrouvert/authentic/pulls/56

Bonne idée, mais n'ayant pas de compte sur votre gitea, je ne peux réagir à tes commentaires. Il y a un moyen d'avoir un compte sur votre gitea ou c'est uniquement à usage interne ?

> Je m'occupe des modifications induites, et poursuis ma relecture entamée hier.

À lire certains de tes commentaires, il faudra que je m'occupe de certains points. N'hésite pas à me nommer si c'est le cas !

#20 - 13 juillet 2023 18:57 - Frédéric Péters

> Bonne idée, mais n'ayant pas de compte sur votre gitea, je ne peux réagir à tes commentaires. Il y a un moyen d'avoir un compte sur votre gitea ou c'est uniquement à usage interne ?

Je viens de te créer un compte (il y manquera encore ensuite peut-être des permissions, j'ajusterai).

#21 - 27 septembre 2023 17:03 - Benjamin Renard

- Fichier 0003-ppolicy-improve-timeBeforeExpiration-date-formating.patch ajouté

- Fichier 0002-ppolicy-clean-computing-passwordTooShort-error-messa.patch ajouté

- Fichier 0001-ppolicy-clean-computing-accountLocked-error-message.patch ajouté

Comme vu avec Paul, quelques patchs qu'il m'a demandé dans gitea.

PS : j'avais développé la solution proposée à propos de formatage de la date d'expiration future du mot de passe, alors je met le patch ici, mais je vous laisse voir si vous préférez rester comme précédemment.

#22 - 28 septembre 2023 09:39 - Paul Marillonnet

Merci Benjamin, je regarde comment intégrer cela.

#23 - 17 octobre 2023 10:17 - Robot Gitea

- Statut changé de En cours à Solution proposée

#24 - 17 octobre 2023 10:24 - Robot Gitea

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

Paul Marillonnet (pmarillonnet) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/56
- Titre : Ajout du support de ppolicy lors de la modification du mot de passe (#66416)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/56/files

#25 - 17 octobre 2023 14:14 - Transition automatique

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

#26 - 18 octobre 2023 08:44 - Paul Marillonnet

- Lié à Development #82521: ppolicy : désactiver l'exécution des tests ppolicy sur un environnement bullseye (?) ajouté

#27 - 17 décembre 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0005-ldap-handle-ppolicy-control-changing-reseting-passwo.patch	6,12 ko	22 septembre 2022	Benjamin Renard
0005-ldap-handle-ppolicy-control-changing-reseting-passwo.patch	4,1 ko	10 novembre 2022	Benjamin Renard
0006-Add-tests-on-LDAP-password-change-reset-with-ppolicy.patch	13,3 ko	10 novembre 2022	Benjamin Renard
0004-ldap-rename-process_controls-method-to-process_bind_.patch	3,02 ko	10 novembre 2022	Benjamin Renard
0003-ldap-fix-encoding-password-on-modify_password.patch	983 octets	10 novembre 2022	Benjamin Renard
0002-password_policy_control_messages-fix-handling-passwo.patch	928 octets	10 novembre 2022	Benjamin Renard
0001-test_ldap-use-USERNAME-PASS-instead-of-duplicated-ha.patch	6,01 ko	10 novembre 2022	Benjamin Renard
0007-ppolicy-handle-reset-password-redirection-after-a-ch.patch	5,07 ko	14 novembre 2022	Benjamin Renard
complete.patch	44,8 ko	05 juillet 2023	Benjamin Renard
0003-ppolicy-improve-timeBeforeExpiration-date-formating.patch	1,69 ko	27 septembre 2023	Benjamin Renard
0002-ppolicy-clean-computing-passwordTooShort-error-messa.patch	2,04 ko	27 septembre 2023	Benjamin Renard
0001-ppolicy-clean-computing-accountLocked-error-message.patch	3,92 ko	27 septembre 2023	Benjamin Renard