Authentic 2 - Bug #69468

ldap.password_policy_control_messages : corriger la génération des messages d'erreurs même si les attributs ne sont pas disponibles

22 septembre 2022 18:23 - Benjamin Renard

Statut:	Fermé	**Début:**	22 septembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Renard	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans la fonction *ldap.password_policy_control_messages*, tous les messages d'erreurs sont générés quel que soit l'erreur remontée par l'annuaire. Par ailleurs, certaines erreurs utilisent des informations issues des attributs de la politique ou de l'utilisateur pour rendre les messages plus précis.

Cela provoque dans certaines situations des exceptions : par exemple si le compte n'est pas bloqué, la génération du message pour *accountLocked* provoquera une erreur du fait que l'attribut *pwdaccountlockedtime* ne sera pas renseigné.

Le patch ci-joint fait en sorte que les messages d'erreurs générés ne soient pas sensibles à l'absence des attributs qu'ils utilisent. Au passage, certaines utilisations *hasardeuses* des informations des attributs ont été supprimés.

Historique

#1 - 19 octobre 2022 14:37 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 19 octobre 2022 14:54 - Benjamin Dauvergne

- Statut changé de Nouveau à Information nécessaire

- Assigné à changé de Benjamin Dauvergne à Benjamin Renard

Pour passwordTooShort tu as fait l'effort de garder la chaîne actuelle en la rendant insensible à l'absence des attributs, pourquoi ne pas avoir de même avec les autres ?

Le patch passe l'intégration continue, il faudrait des tests.

#3 - 10 novembre 2022 16:17 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Pour passwordTooShort tu as fait l'effort de garder la chaîne actuelle en la rendant insensible à l'absence des attributs, pourquoi ne pas avoir de même avec les autres ?

Pour passwordExpired, le message ne voulait pas dire grand-chose (ex: "The password expired after 7776000", pwdMaxAge stockant un nombre de seconde) et le fait d'afficher une durée propre me semblait sans grand intérêt, mais si tu préfères, je peux le faire.

Pour accountLocked, le message précédent était hyper optimiste sur la présence des attributs utilisés, j'ai fait en sorte qu'il reste compréhensible dans tous les cas, quel que soit la présence ou non des attributs utilisés.

Pour passwordTooYoung, là encore, le message ne voulait pas dire grand-chose (ex: "It is too soon to change the password 2592000.", pwdMinAge stockant également des secondes) et le fait d'afficher une durée propre me semblait pas non plus avoir un grand intérêt. Si tu préfères, je peux le faire.

Enfin, pour passwordInHistory, le message précédent intégrait pwdHistory ce qui est complètement inutile voire dangereux : cet attribut stocke une liste des derniers mots de passe utilisés (normalement hashés, mais pas forcément) avec quelques metadata (date, longueur, syntaxe, ...). Je ne vois pas ce que l'on pourrait tirer de pertinent de cet attribut pour rendre l'erreur plus explicite sans divulguer des infos sensibles. Mon message va donc à l'essentiel : This password has already been used and can no longer be used.

> Le patch passe l'intégration continue, il faudrait des tests.

Je vais voir à ajouter quelques tests pour les cas de refus que je peux tester dans le ticket 69964 si ça te va.

#4 - 14 décembre 2022 17:09 - Benjamin Renard

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

#5 - 17 mars 2023 10:41 - Benjamin Renard

- Fichier 0001-ldap-improve-formating-password-expiration-date.patch ajouté

Benjamin Renard a écrit :

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

J'ai eu a réutilisé ce patch (et quelques autres proposés sur le sujet ppolicy) chez un autre client et à cette occasion, je me suis rendu compte que le formatage de la date d'expiration du mot de passe (en cas d'expiration prochaine) était vraiment pas terrible (on utilisait un simple *time.asctime()*).
Ci-joint, un nouveau patch passant à une utilisation de *django.utils.dateformat.format()* pour un meilleur résultat (et s'adaptant à la locale de la requête).

PS : cela ne casse pas à priori les tests sur le sujet.
PPS : je n'ai pas mergé avec le premier patch, car le sujet me semblait pas vraiment le même.

#6 - 17 octobre 2023 12:01 - Paul Marillonnet

- Statut changé de Information nécessaire à Fermé

Géré directement dans #66416.

Fichiers

0004-ldap-fix-messages-generation-in-password_policy_cont.patch	2,9 ko	22 septembre 2022	Benjamin Renard
0001-ldap-improve-formating-password-expiration-date.patch	1,64 ko	17 mars 2023	Benjamin Renard