Authentic 2 - Development #58151

préciser sur un échec d'authentification dans le journal que ça vient d'un annuaire LDAP down

25 octobre 2021 09:47 - Frédéric Péters

Statut:	Fermé	**Début:**	25 octobre 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

On a juste :

> échec d'authentification pour l'identifiant « xxx »

et il faut se connecter sur le serveur et chercher dans les logs ou lancer sync-ldap-users pour voir que c'est un compte LDAP et qu'on n'a pas pu obtenir de réponse du serveur.

Demandes liées:

Lié à Authentic 2 - Development #12516: display a different error message whe...	**Nouveau**	**11 juillet 2016**
Lié à Authentic 2 - Development #58340: backend ldap : encore du code de comp...	**Fermé**	**03 novembre 2021**
Lié à Authentic 2 - Development #58358: backend ldap : découper plus finement...	**Nouveau**	**03 novembre 2021**

Révisions associées

Révision 342be77c - 18 novembre 2021 08:47 - Paul Marillonnet

journal: add ldap down info on failed user login (#58151)

Historique

#1 - 26 octobre 2021 10:40 - Paul Marillonnet

- Statut changé de Nouveau à En cours

- Assigné à mis à Paul Marillonnet

Je pense qu'on peut, sans toucher aux logs génériques dans la vue de login principale, rajouter un ligne de log à ce sujet dans le backend ldap.

#2 - 26 octobre 2021 11:59 - Paul Marillonnet

Un commit qui gère ça dans la branche. C'est sur du code pas testé, je regarde comment tester ça correctement.

#3 - 26 octobre 2021 12:10 - Benjamin Dauvergne

Il faut que ce soit assez sioux parce qu'on ne souhaite pas annoncer d'erreur LDAP sur n'importe quel échec du backend d'authent LDAP. Quand on reçoit un login/mdp on ne sait pas s'il vient du LDAP ou pas actuellement, on le ne sait que si on recherche dans l'annuaire et que ça ne renvoie rien; et quand le LDAP ne répond pas, on n'en sait donc pas plus.

PS: je faisais la même remarque dans #12516.

#4 - 26 octobre 2021 12:11 - Benjamin Dauvergne

- Duplique Development #12516: display a different error message when trying to authenticate against a down ldap server ajouté

#5 - 26 octobre 2021 12:17 - Frédéric Péters

- Duplique Development #12516: display a different error message when trying to authenticate against a down ldap server supprimé

#6 - 26 octobre 2021 12:18 - Frédéric Péters

- Lié à Development #12516: display a different error message when trying to authenticate against a down ldap server ajouté

#7 - 26 octobre 2021 12:20 - Valentin Deniaud

On peut peut-être étendre le mécanisme introduit par #51626, ce qui rejoindrait l'idée de #12516 qui parle aussi d'attacher l'info à la requête.

On ajouterait alors pas de type d'évènement supplémentaire, on pourrait logger l'info en même temps que l'évènement 'user.login.failure', et dans le manager ça s'afficherait entre parenthèses : échec d'authentification pour l'identifiant « xxx » (ldap down).

#8 - 27 octobre 2021 11:42 - Paul Marillonnet

Valentin Deniaud a écrit :

> On peut peut-être étendre le mécanisme introduit par #51626, ce qui rejoindrait l'idée de #12516 qui parle aussi d'attacher l'info à la requête. On ajouterait alors pas de type d'évènement supplémentaire, on pourrait logger l'info en même temps que l'évènement 'user.login.failure', et dans le manager ça s'afficherait entre parenthèses : échec d'authentification pour l'identifiant « xxx » (ldap down).

Oui ok l'idée me va, j'ai poussé un truc dans la branche qui reprend cette idée. Bien sûr ça ne résout toujours la question des tests, je regarde comment ajouter de la couverture de tests à ces bouts d'erreur ldap (actuellement pas testés — et il faut aussi une adaptation des tests existants pour tenir compte du changement de structure de request.failed_logins).

#9 - 27 octobre 2021 11:54 - Benjamin Dauvergne

J'ai fait une remarque que vous ne prenez pas en compte, on n'a pas moyen de faire la différence entre un vrai échec d'authentification parce que LDAP down et un qui n'a aucun rapport; quand le LDAP est down, le code va logger "échec parce que LDAP down" pour chaque usager qui tape mal son login ou son mot de passe mais qui n'est pas dans l'annuaire LDAP.

Et ce sera pareil si un message en front est remonté, on ne veut pas ça, il faut d'abord avoir un moyen depuis un login de déterminer si oui ou non cet utilisateur est dans le LDAP. Alors on a divers moyens imparfaits de singer ça, si un login correspond à un user.username et que ce user est lié à un UserExternalId pour le LDAP en question, ou idem si le login est une adresse de courriel, et que ça matche le user.email d'un utilisateur lié au LDAP aussi.

Disgression:

Dans d'autres tickets j'ai préconisé l'abandon du provisionning au login pour les LDAPs pour un mode avec provisionning purement en cron et recherche des utilisateurs purement localement (sur la base .username ou .email commes les autres). Je pense que provisionner au login était une mauvaise idée que j'ai prise mais à l'époque on ne faisait pas des crons et je m'étais inspiré bêtement du code utilisé auparavant django-auth-ldap). À ce titre je ressors une petite analyse des configurations LDAP que j'avais faite (le code est là https://git.entrouvert.org/misc-bdauvergne.git/tree/a2-analyze-ldap-auth-settings) :

```
realm                           53 values
                                           dordogne.fr
                                           villejuif.fr
                                           cinor.org
                                           ldap-calvados
                                           metropole-toulouse
                                           ldap-senonais
                                           dreux.fr
                                           villedupre.fr
                                           lahague.com
                                           ldap-mairie-slv
                                           ldap-cap-atlantique
                                           mairie.toulouse.intra
                                           thononagglo.fr
                                           agglo-haguenau.fr
                                           cca.bzh
                                           ldap-mincult
                                           mutualisation.fr
                                           mairie-lille.adsi
                                           mairie-nanterre.fr
                                           atd24.fr
                                           ldap-cd55
                                           pfwb.be
                                           cr-reunion.fr
                                           ldap.culture.fr
                                           ville-venissieux.fr
                                           rouen.fr
                                           ldap-bethune-bruay
                                           cch
url                             53 values, not shown
basedn                          53 values, not shown
binddn                          53 values, not shown
bindpw                          53 values, not shown
user_filter                     53 values
                                           (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=GS-Publik
-Users,OU=Groupes,DC=senonais,DC=local)(mail=*)(samaccountname=%s))
                                           (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=THA - Pub
lik,OU=Groupes,OU=Thonon Agglomeration,DC=ta,DC=local)(samaccountname=%s))
                                           (&(objectClass=user)(userPrincipalName=%s))
                                           (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s)))
```

```
                                        (&(|(mail=%s)(uid=%s))(cg14IndicCptActif=TRUE)(|(cg14Type=assfam)(cg
14Type=interne)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(|(mail=%s)(samaccount
name=%s))(|(memberOf=CN=.LD_Agents_BO_RSU,OU=NANTERRE,DC=vnan,DC=intra)(memberOf=CN=.LD_Agents_Publik,OU=NANTE
RRE,DC=vnan,DC=intra)))
                                        (&(objectClass=MCCPerson)(uid=%s)(!(|(MCCOuBis=AC/SG/Service/QUATRE)
(MCCOuBis=AC/SG/Service/UN))))
                                        (&(objectclass=user)(givenName=*)(|(samaccountname=%s)(mail=%s))(!(u
serAccountControl:1.2.840.113556.1.4.803:=2)))
                                        (&(objectClass=user)(memberOf=CN=PUBLIK,OU=- Applications,OU=Mairie,
OU=Venissieux,DC=veni,DC=local)(|(sAMAccountName=%s)(mail=%s)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(mail=*)(|(samaccountn
ame=%s)(mail=%s)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(|(mail=%s)(sAMAccount
Name=%s))(memberOf=CN=GTT-PUBLIK,OU=PUBLIK,OU=Groupes Transverses Techniques,DC=mairie,DC=toulouse,DC=intra))
                                        (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s))(objectCategory=C
N=Person,CN=Schema,CN=Configuration,DC=psg,DC=local)(memberOf=CN=publik,OU=ENTROUVERT,DC=psg,DC=local))
                                        (&(objectClass=user)(mail=*)(cn=*)(sn=*)(givenName=*)(|(sAMAccountNa
me=%s)(mail=%s))(memberOf:1.2.840.113556.1.4.1941:=CN=GR_MUT_APP_Publik,OU=Groupes,OU=Infrastructure,OU=Cap At
lantique,DC=cap-atlantique,DC=fr))
                                        (&(objectClass=user)(sAMAccountType=805306368)(|(samaccountname=%s)(
mail=%s)(userPrincipalName=%s)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=App_GRU,O
U=Applications,OU=Groupes,OU=Mairie,DC=mairie-slv,DC=priv)(|(samaccountname=%s)(mail=%s)))
                                        (&(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=CN=GG_PUBLIK,
OU=Applications,OU=Groupes,DC=ad-mairie,DC=rouen,DC=fr)(sAMAccountName=%s))
                                        (&(objectClass=user)(sAMAccountType=805306368)(mail=*)(samaccountnam
e=%s))
                                        (&(objectClass=MCCPerson)(uid=%s))
                                        (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=GRP_PUBLI
K,OU=Applicatifs,OU=Groupes,DC=mairiedreux,DC=local)(samaccountname=%s))
                                        (&(objectClass=user)(sAMAccountType=805306368)(samaccountname=%s))
                                        (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=apppublik
,OU=Groupes,OU=Utilisateurs,DC=esc1dom,DC=mairie-lille,DC=adsi)(|(sAMAccountName=%s)(mail=%s)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(samaccountname=%s)(|(
memberOf=CN=THA - Publik,OU=Groupes,OU=Thonon Agglomeration,DC=ta,DC=local)(memberOf=CN=THA - Publik - Commune
s,OU=Groupes,OU=Thonon Agglomeration,DC=ta,DC=local)))
                                        (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s))(|(memberof=CN=gg
sadFormBadge,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormInternet,OU=ou
Formulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormSG,OU=ouFormulaire,OU=ouPortail,
OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormExpedition,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=do
m,DC=pfwb,DC=be)(memberof=CN=ggsadFormDGFRA,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memb
erof=CN=ggsadFormInfo,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormSante
,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormSalaire,OU=ouFormulaire,OU
=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormEconomat,OU=ouFormulaire,OU=ouPortail,OU=OuUs
ers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormTabellio,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb
,DC=be)(memberof=CN=ggsadFormDGRE,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=gg
sadFormCompta,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormDGTL,OU=ouFor
mulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormJuridique,OU=ouFormulaire,OU=ouPort
ail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormJuridiqueMandat,OU=ouFormulaire,OU=ouPortail,OU=OuUs
ers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadFormPresse,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,D
C=be)(memberof=CN=ggsadFormDIV,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsad
FormCRI,OU=ouFormulaire,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadAgendaAgent,OU=ouAgenda
,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadAgendaStreaming,OU=ouAgenda,OU=ouPortail,OU=Ou
Users,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggsadAgendaEdition,OU=ouAgenda,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,
DC=be)(memberof=CN=ggsadDocbowAgents,OU=ouDocbow,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)(memberof=CN=ggs
adLoginSSO,OU=ouPortail,OU=OuUsers,DC=dom,DC=pfwb,DC=be)))
                                        (&(objectClass=user)(sAMAccountType=805306368)(memberOf=CN=GRP-ACCES
-GRC,OU=Groupes,OU=CCA,DC=CCCC-siege,DC=4c,DC=local)(samaccountname=%s))
                                        (&(objectClass=MCCPerson)(uid=%s)(|(MCCOuBis=AC/SG/Service/QUATRE)(M
CCOuBis=AC/SG/Service/UN)))
                                        (&(objectClass=user)(memberOf=CN=XenApp-Publik,OU=GroupesApplicatifs
,OU=Xenapp,DC=cr-reunion,DC=fr)(mail=%s))
username_template               53 values
                                        {mail[0]}
                                        {uid[0]}@{realm}
                                        {userprincipalname[0]}
                                        {samaccountname[0]}@mairie.toulouse.intra
                                        {samaccountname[0]}@thononagglo.fr
                                        {samaccountname[0]}@{realm}
                                        {samaccountname[0]}
                                        {uid[0]}@ldap-mincult
attributes                      53 values, not shown
external_id_tuples              48 values
                                        (('samaccountname',), ('dn:noquote',))
```

```
                                        (('samaccountname',),)
active_directory                44 values
                                        True
set_mandatory_roles             39 values, not shown
update_username                 38 values
                                        True
shuffle_replicas                31 values
                                        False
                                        True
require_cert                    25 values
                                        never
                                        allow
use_tls                         22 values
                                        False
                                        True
ou_slug                         10 values
                                        hobo-tm
                                        default
                                        hobo-atd24
                                        agents
certfile                        9 values
                                        /var/lib/authentic2-multitenant/tenants/connexion.demarches.dordogne
.fr/dordogne.crt
                                        /var/lib/authentic2-multitenant/tenants/connexion.nestor.culture.fr/
client-ldap.crt
                                        /var/lib/authentic2-multitenant/tenants/connexion-mincult.test.entro
uvert.org/publik-culture-recette.crt
                                        /var/lib/authentic2-multitenant/tenants/connexion-dordogne.test.entr
ouvert.org/dordogne.crt
keyfile                         9 values
                                        /var/lib/authentic2-multitenant/tenants/connexion-mincult.test.entro
uvert.org/publik-culture-recette.key
                                        /var/lib/authentic2-multitenant/tenants/connexion.demarches.dordogne
.fr/dordogne.key
                                        /var/lib/authentic2-multitenant/tenants/connexion.nestor.culture.fr/
client-ldap.key
                                        /var/lib/authentic2-multitenant/tenants/connexion-dordogne.test.entr
ouvert.org/dordogne.key
user_attributes                 7 values, not shown
group_to_role_mapping           7 values, not shown
group_filter                    4 values
                                        (&(objectClass=group)(member:1.2.840.113556.1.4.1941:={user_dn})(sAM
AccountName=*))
group_basedn                    4 values
                                        OU=GRU,OU=Groupes,OU=VILLEJUIF,DC=villejuif,DC=fr
                                        OU=Groupes,OU=Thonon Agglomeration,DC=ta,DC=local
user_can_change_password        3 values
                                        False
member_of_attribute             3 values
                                        memberof
sync_ldap_users_filter          2 values
                                        (&(objectclass=user)(givenName=*)(mail=*@*)(!(userAccountControl:1.2
.840.113556.1.4.803:=2)))
set_mandatory_groups            2 values, not shown
timeout                         1 values
                                        2
```

Dans tous les cas on cherche soit dans sAMAccountName, uid ou mail, soit une combinaison mais par contre le template pour générer username n'est pas uniforme ce qui pourrait poser un souci.

#10 - 27 octobre 2021 11:58 - Frédéric Péters

Dans le cas à l'origine, l'identifiant de l'usager est correct et dans mon idée ça fournissait toute l'info nécessaire pour voir qu'il venait du LDAP parce qu'info visible via UserExternalId(source='ldap').

#11 - 27 octobre 2021 12:03 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> J'ai fait une remarque que vous ne prenez pas en compte, on n'a pas moyen de faire la différence entre un vrai échec d'authentification parce que LDAP down et un qui n'a aucun rapport; quand le LDAP est down, le code va logger "échec parce que LDAP down" pour chaque usager qui tape mal son login ou son mot de passe mais qui n'est pas dans l'annuaire LDAP.

J'ai pas relevé parce que pas compris en quoi c'était problématique ici. Ça ne me choque pas qu'une erreur relativement bas niveau (i.e. l'annuaire

est par terre l'usager n'a pas pu se logguer) masque des erreurs de plus haut niveau (i.e. on ne retrouve pas l'usager dans l'annuaire). Bien sûr cette première erreur survient quand bien même l'usager ne se trouverait pas dans l'annuaire si celui-ci était up. C'est grave ?

#12 - 27 octobre 2021 12:29 - Paul Marillonnet

Frédéric Péters a écrit :

> Dans le cas à l'origine, l'identifiant de l'usager est correct et dans mon idée ça fournissait toute l'info nécessaire pour voir qu'il venait du LDAP parce qu'info visible via UserExternalId(source='ldap').

(Et donc petite remarque quand même ça exclurait toute première connexion sans synchro préalable, cas dans lequel cet identifiant externe n'a pas encore été créé.)

#13 - 27 octobre 2021 13:09 - Frédéric Péters

Oui, mais (perso) ça n'est pas important (pour moi).

Le cas commun c'est le ticket pour dire que la personne de la collectivité n'arrive pas à se connecter, une tentative de connexion chez nous où ça passe, et à ce moment on peut juste regarder le journal et voir qu'il y a de fait eu échec de connexion, mon souhait à ce ticket c'était de pouvoir à ce moment répondre dans le ticket : en effet on voit que la connexion à votre annuaire LDAP échoue. (sans avoir à aller chercher l'info dans des logs sur le serveur, ce qui limite le support aux devs).

(ajout : et #12516 est le ticket pour que la personne de la collectivité soit elle-même informée du problème, sans avoir à créer de ticket chez nous).

#14 - 27 octobre 2021 14:51 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> J'ai pas relevé parce que pas compris en quoi c'était problématique ici. Ça ne me choque pas qu'une erreur relativement bas niveau (i.e. l'annuaire est par terre l'usager n'a pas pu se logguer) masque des erreurs de plus haut niveau (i.e. on ne retrouve pas l'usager dans l'annuaire). Bien sûr cette première erreur survient quand bien même l'usager ne se trouverait pas dans l'annuaire si celui-ci était up. C'est grave ?

Parce que tu n'as pas compris le problème je pense.

Frédéric Péters a écrit :

> Dans le cas à l'origine, l'identifiant de l'usager est correct et dans mon idée ça fournissait toute l'info nécessaire pour voir qu'il venait du LDAP parce qu'info visible via UserExternalId(source='ldap').

On utilise pas cette information actuellement, je le dis dans mon deuxième commentaire, donc oui si on se met à utiliser cette information ça irait. Là le code n'attache pas d'utilisateur à l'erreur :

```
+                    request.failed_logins.update({None: {'username': authz_id, 'reason': 'ldap timeout'}})
```

donc le problème ne sera pas visible dans le journal de l'utilisateur concerné, on aura un "échec d'authentification pour l'identifiant « toto » (serveur LDAP ijoignable)" perdu au milieu du journal global.

#15 - 27 octobre 2021 14:52 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> (Et donc petite remarque quand même ça exclurait toute première connexion sans synchro préalable, cas dans lequel cet identifiant externe n'a pas encore été créé.)

Même après ça ne marchera pas avec le code que je vois sur la branche.

#16 - 27 octobre 2021 14:56 - Paul Marillonnet

Frédéric Péters a écrit :

> Le cas commun c'est le ticket pour dire que la personne de la collectivité n'arrive pas à se connecter, une tentative de connexion chez nous où ça passe, et à ce moment on peut juste regarder le journal et voir qu'il y a de fait eu échec de connexion, mon souhait à ce ticket c'était de pouvoir à ce moment répondre dans le ticket : en effet on voit que la connexion à votre annuaire LDAP échoue. (sans avoir à aller chercher l'info dans des logs sur le serveur, ce qui limite le support aux devs).

Ok, je comprends mieux. Cette recherche sur les identifiants externes est l'un des "moyens imparfaits" listés par Benjamin dans son précédent message (édité). On peut considérer ici que bien qu'imparfait c'est suffisant pour ce cas de la personne de la collectivité cherchant à se connecter. Je vais revoir le code pour introduire cette recherche sur l'identifiant externe au moment où une erreur technique ldap survient.

Benjamin Dauvergne a écrit :

> On utilise pas cette information actuellement, je le dis dans mon deuxième commentaire, donc oui si on se met à utiliser cette information ça irait. Là le code n'attache pas d'utilisateur à l'erreur
> donc le problème ne sera pas visible dans le journal de l'utilisateur concerné, on aura un "échec d'authentification pour l'identifiant « toto » (serveur LDAP ijoignable)" perdu au milieu du journal global.

Ok oui, je comprends pourquoi dans ce cas c'est important que ce soit dans le journal de l'usager concerné. Comme dit plus haut dans ce message, je vais revoir le code pour inclure cette information.

Benjamin Dauvergne a écrit :

> Même après ça ne marchera pas avec le code que je vois sur la branche.

Et donc oui, ça ne marchera pas comme ça. Code à revoir donc, je m'en occupe.

#17 - 27 octobre 2021 16:16 - Paul Marillonnet

Paul Marillonnet a écrit :

> Et donc oui, ça ne marchera pas comme ça. Code à revoir donc, je m'en occupe.

Voilà, à redécouper logiquement mais l'idée est là : on reprend la logique de lookup_existing_user (sans la partie de récupération des attributs, parce qu'on part du principe que le LDAP est down) et si on trouve un usager on le lie à l'entrée de journal relative à l'échec d'authentification pour motif d'erreur technique de l'annuaire. Je regarde pour tester.

#18 - 03 novembre 2021 11:17 - Paul Marillonnet

- Lié à Development #58340: backend ldap : encore du code de compat python 2 à virer ajouté

#19 - 03 novembre 2021 15:32 - Paul Marillonnet

- Fichier 0001-journal-add-ldap-down-info-on-failed-user-login-5815.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Paul Marillonnet a écrit :

> Voilà, à redécouper logiquement mais l'idée est là : on reprend la logique de lookup_existing_user (sans la partie de récupération des attributs, parce qu'on part du principe que le LDAP est down) et si on trouve un usager on le lie à l'entrée de journal relative à l'échec d'authentification pour motif d'erreur technique de l'annuaire. Je regarde pour tester.

Et en fait le lookup par identifiant externe a besoin des attributs, on ne peut pas faire sans. Le nouveau patch présume qu'il y a un intérêt à tenter de chercher, après erreur de connexion, les attributs, et ceci pour retrouver l'usager en local dont le journal va être alimenté. Le code se rapproche davantage de ce que fait lookup_existing_user, et est testé.

#20 - 03 novembre 2021 15:55 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Arf, j'avais oublié pylint, les tests sont rouges. Je regarde.

#21 - 03 novembre 2021 16:16 - Paul Marillonnet

- Fichier 0001-journal-add-ldap-down-info-on-failed-user-login-5815.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, une variable était inutilisée dans les tests, lesquels sont d'ailleurs maintenant plus clairs avec un parametrize.

#22 - 03 novembre 2021 16:41 - Valentin Deniaud

Paul Marillonnet a écrit :

> Et en fait le lookup par identifiant externe a besoin des attributs, on ne peut pas faire sans. Le nouveau patch présume qu'il y a un intérêt à tenter de chercher, après erreur de connexion, les attributs, et ceci pour retrouver l'usager en local dont le journal va être alimenté.

Perso je suis perdu par ces histoires, je me demande si on ne pourrait pas faire plus simple :

- Noter que le ldap est down dans ldap_backend.py, ça serait genre request.ldap_down = True à la place des self._record_failure_for_user(request, 'ldap server down'
  - Ne rien modifier d'autre dans ce fichier parce que du code dans ce fichier = du code compliqué (d'ailleurs avec le lookup des attributs tu retombes peut-être sur #53685)
- Dans authenticators.py, quand on s'apprête à enregistrer un évènement login.failure :
  - Regarder si l'utilisateur vient du ldap (user.userexternalid_set.exists() ?)
  - Si oui, regarder si le ldap est down grâce au flag posé sur la requête, le noter s'il l'est

À Benjamin de confirmer que ça pourrait marcher avant de se lancer, bien sûr.

#23 - 03 novembre 2021 17:01 - Paul Marillonnet

Valentin Deniaud a écrit :

> Paul Marillonnet a écrit :
>
> > Et en fait le lookup par identifiant externe a besoin des attributs, on ne peut pas faire sans. Le nouveau patch présume qu'il y a un intérêt à tenter de chercher, après erreur de connexion, les attributs, et ceci pour retrouver l'usager en local dont le journal va être alimenté.
>
> Perso je suis perdu par ces histoires, je me demande si on ne pourrait pas faire plus simple :
> […]

À mon avis la partie complexe est celle qui consiste à retrouver l'usager pour lequel on veut l'entrée de journal. Je crois qu'on ne peut cependant pas en faire l'économie : si la connexion a échoué, il faut retrouver l'utilisateur par un autre moyen qui tient compte de la façon dont sont gérés les identifiants dans notre backend ldap (et donc en particulier on ne peut pas taper directement un user.userexternalid_set dans authentic2.authenticators).

Sans ça on aura juste ce qui se passe déjà dans le code, à savoir une entrée

```
request.journal.record('user.login.failure', username=username)
```

non rattachée à l'usager.
Je loupe un truc évident ?

Après c'est vrai que cette méthode authenticate_block du backend commence à être massive, on pourrait faire un ticket à part pour découper et gagner ainsi en lisibilité.

#24 - 03 novembre 2021 17:23 - Paul Marillonnet

- Lié à Development #58358: backend ldap : découper plus finement la méthode @authenticate_block@ ajouté

#25 - 03 novembre 2021 17:23 - Valentin Deniaud

Paul Marillonnet a écrit :

> Sans ça on aura juste ce qui se passe déjà dans le code, à savoir une entrée non rattachée à l'usager.

Oui dac c'est moi qui ait rêvé l'entrée déjà rattachée à l'usager, et donc qu'il suffisait d'ajouter le mention ldap down. Du coup je comprends le code compliqué pour retrouver le compte.

#26 - 03 novembre 2021 17:24 - Paul Marillonnet

Paul Marillonnet a écrit :

> Après c'est vrai que cette méthode authenticate_block du backend commence à être massive, on pourrait faire un ticket à part pour découper et gagner ainsi en lisibilité.

(#58358)

#27 - 03 novembre 2021 17:29 - Paul Marillonnet

Et, rebondissement, je ne sais pas où j'ai rêvé que les éléments additionnels passés dans le **data à l'écriture de l'entrée de journal apparaissaient dans la ligne dans l'UI, mais ce n'est de toute évidence pas le cas. Je regarde s'il faut corriger ce patch ou ajouter la présence de ces éléments additionnels dans l'entrée de journal.

#28 - 03 novembre 2021 17:34 - Paul Marillonnet

Paul Marillonnet a écrit :

> Et, rebondissement, je ne sais pas où j'ai rêvé que les éléments additionnels passés dans le **data à l'écriture de l'entrée de journal

> apparaissaient dans la ligne dans l'UI, mais ce n'est de toute évidence pas le cas. Je regarde s'il faut corriger ce patch ou ajouter la présence de ces éléments additionnels dans l'entrée de journal.

(C'est déjà dans le patch, my bad, fatigue de fin de journée…)

#29 - 08 novembre 2021 11:07 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ok. Remarque annexe : on peut faire avec mock.patch/mock.patch.object la même chose qu'avec monkeypatch mais en plus localement vu que ça fournit un contextmanager, c'est souvent plus joli.

```
def mafonction():
    ....

with mock.patch('package.module.Class.method', mafonction):
    .....
```

#30 - 08 novembre 2021 14:38 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Remarque annexe : on peut faire avec mock.patch/mock.patch.object la même chose qu'avec monkeypatch mais en plus localement vu que ça fournit un contextmanager, c'est souvent plus joli.
>
> [...]

D'ac c'est noté, je laisse le patch en l'état mais pour les prochains je verrai si c'est mieux avec mock plutôt qu'avec monkeypatch.

#31 - 18 novembre 2021 08:49 - Paul Marillonnet

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

```
commit 342be77cccc74a0c656884acf045673659043e43
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Tue Oct 26 10:48:06 2021 +0200

    journal: add ldap down info on failed user login (#58151)
```

#33 - 18 novembre 2021 11:16 - Frédéric Péters

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

Fichiers

0001-journal-add-ldap-down-info-on-failed-user-login-5815.patch	8,59 ko	03 novembre 2021	Paul Marillonnet
0001-journal-add-ldap-down-info-on-failed-user-login-5815.patch	8,57 ko	03 novembre 2021	Paul Marillonnet