Authentic 2 - Development #56666

backend ldap : correction message d'erreur lorque le serveur n'est pas joignable

06 septembre 2021 10:26 - Paul Marillonnet

Statut:	Fermé	**Début:**	06 septembre 2021
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

actuellement c'est ldap is down, alors que ça peut dû à beaucoup d'autres choses, exemple #56661.

Révisions associées

Révision 1c7cc013 - 16 septembre 2021 15:15 - Paul Marillonnet

ldap: retrieve tls info on ldap errors (#56666)

Historique

#2 - 06 septembre 2021 11:14 - Paul Marillonnet

- Fichier 0001-ldap-fix-overly-confident-diagnosis-in-ldap-down-err.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 06 septembre 2021 12:48 - Benjamin Dauvergne

Je ne sais pas ce que contient exactement l'exception on peut tenter de la passer dans ligne de log aussi ("%s" % e) (il faudrait tester ça sur une erreur SSL voir ce que ça donne, suffit de faire un faux endpoint ssl avec openssl s_server le truc n'ira pas plus loin que le handshake SSL).

#4 - 06 septembre 2021 12:48 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

#5 - 08 septembre 2021 11:19 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Je ne sais pas ce que contient exactement l'exception on peut tenter de la passer dans ligne de log aussi ("%s" % e) (il faudrait tester ça sur une erreur SSL voir ce que ça donne, suffit de faire un faux endpoint ssl avec openssl s_server le truc n'ira pas plus loin que le handshake SSL).

Ok pour logguer l'exception, mais pour reproduire je pensais plutôt instancier un serveur ldap avec un mauvais certif. Slapd ne me laisse pas faire ça :)
L'idée du faux endpoint tls ne m'inspire pas trop : on voudrait un vrai échec de handshake, pas besoin de mocker au niveau tls dans ce cas.

Je vais creuser voir si on peut reproduire le cas du serveur ldap qui présente un mauvais certificat comme dans #56661.

#6 - 09 septembre 2021 15:31 - Paul Marillonnet

- Fichier 0001-ldap-broaden-overly-confident-diagnosis-in-error-mes.patch ajouté

- Statut changé de En cours à Solution proposée

Paul Marillonnet a écrit :

> Je vais creuser voir si on peut reproduire le cas du serveur ldap qui présente un mauvais certificat comme dans #56661.

Ce n'est pas exactement comme dans #56661 mais ça permet de tester qu'on a plus d'info lorsqu'on capture ldap.SERVER_DOWN.

#7 - 09 septembre 2021 15:45 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Benjamin Dauvergne a écrit :
>
> > Je ne sais pas ce que contient exactement l'exception on peut tenter de la passer dans ligne de log aussi ("%s" % e) (il faudrait tester ça sur une erreur SSL voir ce que ça donne, suffit de faire un faux endpoint ssl avec openssl s_server le truc n'ira pas plus loin que le handshake SSL).
>
> Ok pour logguer l'exception, mais pour reproduire je pensais plutôt instancier un serveur ldap avec un mauvais certif. Slapd ne me laisse pas faire ça :)
> L'idée du faux endpoint tls ne m'inspire pas trop : on voudrait un vrai échec de handshake, pas besoin de mocker au niveau tls dans ce cas.

Ben si justement, je ne comprends pas à quoi tu penses, pour avoir un handshake il faut une terminaison TLS; bon de fait j'ai vérifié avec s_server et python-ldap ça renvoie juste SERVER_IS_DOWN, pas moyen d'avoir mieux de la part de libldap (ou alors vaguement en activant le debug maximum avec ldapsearch mais va savoir comment faire ça en python et ou ça va partir). Si on veut faire mieux il faut tenter une connexion via socket sur le même port en cas d'erreur, il n'y a pas vraiment d'autre moyen, ou alors on en reste à server is down parce qu'on ne sait pas faire mieux et c'est tant pis.

> Je vais creuser voir si on peut reproduire le cas du serveur ldap qui présente un mauvais certificat comme dans #56661.

Je sais déjà que ça ne donnera rien de mieux qu'actuellement.

#8 - 09 septembre 2021 16:06 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Ben si justement, je ne comprends pas à quoi tu penses, pour avoir un handshake il faut une terminaison TLS; bon de fait j'ai vérifié avec s_server et python-ldap ça renvoie juste SERVER_IS_DOWN, pas moyen d'avoir mieux de la part de libldap (ou alors vaguement en activant le debug maximum avec ldapsearch mais va savoir comment faire ça en python et ou ça va partir). Si on veut faire mieux il faut tenter une connexion via socket sur le même port en cas d'erreur, il n'y a pas vraiment d'autre moyen, ou alors on en reste à server is down parce qu'on ne sait pas faire mieux et c'est tant pis.

Le ticket voulait simplement ne pas logguer “server is down” alors que ce n’est pas forcément le cas. Mais c’est ce que la bibliothèque ldap utilisée nous remonte.
Je vais voir ce que donne la piste de la connexion via socket sur le même port. Iirc on fait quelque comme ça dans ldaptools lorsque la connexion par url ne fonctionne pas.

#9 - 09 septembre 2021 16:51 - Thomas Noël

Comme je suis l'inspirateur du ticket je précise que mon idée est juste d'arrêter d'écrire "server is down" alors que c'est faux dans 99,99% des cas. C'est toujours un problème réseau (inclus les soucis TLS). C'est pour éviter de se voir répondre trop vite dans un ticket "votre serveur est-il en panne ?" (vu y'a quelque jour je ne sais plus où, alors que c'était un pépin tls).

#10 - 09 septembre 2021 17:37 - Benjamin Dauvergne

Thomas Noël a écrit :

> Comme je suis l'inspirateur du ticket je précise que mon idée est juste d'arrêter d'écrire "server is down" alors que c'est faux dans 99,99% des cas. C'est toujours un problème réseau (inclus les soucis TLS). C'est pour éviter de se voir répondre trop vite dans un ticket "votre serveur est-il en panne ?" (vu y'a quelque jour je ne sais plus où, alors que c'était un pépin tls).

Pour moi si t'as plus de réseau ou que ton certificat TLS est mauvais, ton serveur il est en panne vu d'ici. Alors si vous voulez dire "il y a un problème dans la liaison avec le serveur LDAP quelque part entre lui et nous" si vous voulez; mais quand je lis server is down, ça veut dire la même chose. Lister les 100 cas d'erreur possible ne changera pas le fait qu'il faut chercher le bon pour pouvoir réparer, et donc on va faire ldapsearch -H ldaps://trucmuche -d 255 -v -b '' * et espérer que le mode debug de libldap nous sorte quelque chose; ce qu'on faisait déjà.

Donc moi si ce n'est pas pour donner une indication plus précise du souci qui permet de débugger en 2s, je ne vois pas bien l'intérêt de changer quelque chose, parce que je ne vois pas à qui ça va vraiment faire gagner du temps. Le fait de retester la connection avec un coup de :

```
# https://docs.python.org/3/library/ssl.html \o/
with socket.create_connection((hostname, bind_port or 636), timeout=2) as sock:
    with context.wrap_socket(sock, server_hostname=hostname) as ssock:
        pass
```

apporterait ces informations.

#11 - 09 septembre 2021 17:48 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

#12 - 09 septembre 2021 18:27 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Donc moi si ce n'est pas pour donner une indication plus précise du souci qui permet de débugger en 2s, je ne vois pas bien l'intérêt de changer quelque chose, parce que je ne vois pas à qui ça va vraiment faire gagner du temps. Le fait de retester la connection avec un coup de :
> [...]
> apporterait ces informations.

Très bien, faisons comme ça. J'ai commencé à écrire quelque chose qui va en ce sens. Commit wip poussé dans la branche. Je vais regarder comment tester, avec les indications que tu m'as précédemment données.

#13 - 13 septembre 2021 15:35 - Paul Marillonnet

- Fichier 0001-ldap-attempt-to-retrieve-ssl-info-in-ldaps-error-mes.patch ajouté

- Statut changé de En cours à Solution proposée

Paul Marillonnet a écrit :

> Très bien, faisons comme ça. J'ai commencé à écrire quelque chose qui va en ce sens. Commit wip poussé dans la branche. Je vais regarder comment tester, avec les indications que tu m'as précédemment données.

Quelque chose comme ça, il me semble.

#14 - 13 septembre 2021 15:55 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

(C'est rouge et je ne reproduis pas en local. Je regarde.)

#15 - 13 septembre 2021 17:37 - Paul Marillonnet

- Fichier 0001-ldap-attempt-to-retrieve-ssl-info-in-ldaps-error-mes.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà qui est mieux.

N.B. : La gestion des erreurs dans du module ssl n'est super pas claire, j'ai préféré laisser un

```
+                except (OSError, ssl.SSLError) as e:
```

même si la seconde exception est censée hériter de la première, car un bout de code dans ce module lève une OSError au contraire de ce que la documentation indique.

#16 - 13 septembre 2021 18:23 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Paul Marillonnet a écrit :

> Voilà qui est mieux.
>
> N.B. : La gestion des erreurs dans du module ssl n'est super pas claire, j'ai préféré laisser un
> [...] même si la seconde exception est censée hériter de la première, car un bout de code dans ce module lève une OSError au contraire de ce que la documentation indique.

Il doit manquer un in caplog.text ou quelque chose comme ça, là tu testes juste que la chaîne existe :

```
    assert "ldap 'ldap://localhost.entrouvert.org:%s' is down" % wrong_port
```

J'aurai bien vu un test de timeout/port fermé et de résolution DNS pour aller avec celui là.

PS: aussi tu peux raccourcir ton test en tapant directement dans LDAPBackend.get_connections(), pas la peine de tester la vue de login ici.

#17 - 15 septembre 2021 10:52 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> J'aurai bien vu un test de résolution DNS.

C’est à dire ? Mocker une réponse DNS qui renvoie une mauvaise adresse ?

#18 - 15 septembre 2021 22:05 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Benjamin Dauvergne a écrit :
>
> > J'aurai bien vu un test de résolution DNS.
>
> C’est à dire ? Mocker une réponse DNS qui renvoie une mauvaise adresse ?

Non tu mets un hostname qui n'existe pas genre 'jenexistepas.example.com'.

#19 - 16 septembre 2021 14:46 - Paul Marillonnet

- Fichier 0001-ldap-retrieve-tls-info-on-ldap-errors-56666.patch ajouté

- Statut changé de En cours à Solution proposée

Ok, un second test de tentative de connexion sur un mauvais port et avec un mauvais hostname.

#20 - 16 septembre 2021 14:51 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#21 - 16 septembre 2021 15:16 - Paul Marillonnet

(J’attends que Jenkins voie vert avec la branche rebasée, et je pousse ensuite.)

#22 - 16 septembre 2021 15:31 - Paul Marillonnet

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

```
commit 1c7cc013ee42220052742bc54384d3e7eba4548b
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Mon Sep 6 10:28:36 2021 +0200

    ldap: retrieve tls info on ldap errors (#56666)
```

#23 - 17 septembre 2021 10:53 - Paul Marillonnet

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

Fichiers

0001-ldap-fix-overly-confident-diagnosis-in-ldap-down-err.patch	922 octets 06 septembre 2021	Paul Marillonnet
0001-ldap-broaden-overly-confident-diagnosis-in-error-mes.patch	4,33 ko 09 septembre 2021	Paul Marillonnet
0001-ldap-attempt-to-retrieve-ssl-info-in-ldaps-error-mes.patch	9,05 ko 13 septembre 2021	Paul Marillonnet
0001-ldap-attempt-to-retrieve-ssl-info-in-ldaps-error-mes.patch	9,03 ko 13 septembre 2021	Paul Marillonnet
0001-ldap-retrieve-tls-info-on-ldap-errors-56666.patch	10,2 ko 16 septembre 2021	Paul Marillonnet