Authentic 2 - Development #45531

ldap : disposer d'un système de masques permettant d'exclure certains annuaires de la tentative d'authn, en fonction de la forme du CN

28 juillet 2020 15:55 - Paul Marillonnet

Statut:	Information nécessaire	**Début:**	28 juillet 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Exemple : notre (branche) LDAP où, si le CN de l'usager a une forme autre que <un-login> ou <un-login>@entrouvert.{org,com}, alors ce n'est pas la peine de tenter l'authn.

Demandes liées:

Lié à Authentic 2 - Bug #43737: backend ldap : un annuaire down suffisamment ...	**Nouveau**	**08 juin 2020**

Historique

#1 - 28 juillet 2020 15:55 - Paul Marillonnet

- Lié à Bug #43737: backend ldap : un annuaire down suffisamment longtemps, puis up de nouveau, plante l'authentification ajouté

#2 - 28 juillet 2020 16:08 - Paul Marillonnet

- Statut changé de Nouveau à En cours

L'intitulé et la description sont inexacts. Je vais relire cette partie du code et je reformulerai le problème dès que j'y vois plus clair.

#3 - 29 juillet 2020 12:40 - Paul Marillonnet

- Statut changé de En cours à Information nécessaire

En fait, la déclaration des annuaires dans le backend ldap dispose déjà d'une option de configuration limit_to_realm :

```
class LDAPBackend(object):
    def authenticate(self, request=None, username=None, password=None, realm=None, ou=None):
        # …
        for block in config:
            uid = username
            # …
            if block['limit_to_realm']:
                if realm is None and '@' in username:
                    uid, realm = username.rsplit('@', 1)
                if realm and block.get('realm') != realm:
                    continue
```

Est-ce qu'on a intérêt à fournir quelque chose de plus souple que ce qui est déjà là i.e. un test en égalité stricte avec une seule valeur possible ?

#4 - 29 juillet 2020 12:51 - Frédéric Péters

Je propose une direction toute différente : la plupart du temps il y aura eu synchro LDAP et donc on doit pouvoir savoir à quel annuaire est associé un compte local. Dans cette situation, tester (en premier) le mot de passe vers cet annuaire. (en supposant que ça ne se soit pas déjà le cas).

Le reste du temps, fonctionner comme maintenant.

Parce que, le ticket dit juste "pas la peine de tenter l'authn" mais quel est le problème si elle est tentée ? ça charge trop l'annuaire ? ça remplit de logs inutiles ? y a-t-il vraiment un problème, en fait ?

#5 - 29 juillet 2020 15:51 - Thomas Noël

Frédéric Péters a écrit :

> Parce que, le ticket dit juste "pas la peine de tenter l'authn" mais quel est le problème si elle est tentée ? ça charge trop l'annuaire ? ça remplit de logs inutiles ? y a-t-il vraiment un problème, en fait ?

Si l'annuaire n'est pas dispo, Authentic attend le timeout pour tenter les auth suivantes. C'est juste ça.

#6 - 29 juillet 2020 16:04 - Paul Marillonnet

Thomas Noël a écrit :

> Frédéric Péters a écrit :
>
> > Parce que, le ticket dit juste "pas la peine de tenter l'authn" mais quel est le problème si elle est tentée ? ça charge trop l'annuaire ? ça remplit de logs inutiles ? y a-t-il vraiment un problème, en fait ?
>
> Si l'annuaire n'est pas dispo, Authentic attend le timeout pour tenter les auth suivantes. C'est juste ça.

Et systématiser l'usage des config realm et limit_to_realm lors de la déclaration des annuaires connus du backend ldap, est-ce que ça suffirait ?

#7 - 29 juillet 2020 17:33 - Frédéric Péters

> Si l'annuaire n'est pas dispo, Authentic attend le timeout pour tenter les auth suivantes. C'est juste ça.

Mais c'est quelque chose qui arrive uniquement pour les utilisateurs inconnus, ou pour tout le monde ? Parce que si c'est juste les comptes inconnus, je dirais qu'on peut vivre avec, et si c'est pour tous les comptes, cf ma suggestion plus haut pour viser correctement le bon annuaire.