Authentic 2 - Development #53685

ldap: traces de plus en plus fréquentes

03 mai 2021 15:18 - Serghei Mihai (congés, retour 15/05)

Statut:	Fermé	**Début:**	03 mai 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

On en reçoit de plus en plus souvent depuis les recettes et prods ces derniers temps:

```
Report
unable to retrieve attributes of dn 'cn=xxxxx,ou=users,ou=espc,ou=OU,dc=domaine,dc=DC': OPERATIONS
_ERROR({'desc': 'Operations error', 'info': '000004DC: LdapErr: DSID-0C0907E9, comment: In order t
o perform this operation a successful bind must be completed on the connection., data 0, v2580'})
```

Révisions associées

Révision c9b626d6 - 03 août 2021 11:52 - Benjamin Dauvergne

ldap: do not trace when SEARCH return no attributes (#53685)

Révision 7050db8b - 03 août 2021 11:52 - Benjamin Dauvergne

ldap: on INVALID_CREDENTIALS, try to rebind before looking up the user (#53685)

On a bind failure, the current bind context is lost, if we want to
lookup the user whose bind failed we must first rebind with the service
credentials.

Historique

#1 - 03 mai 2021 16:51 - Benjamin Dauvergne

Il me semble que ça viendrait de gens utilisant le reset de mot de passe pour un compte LDAP ou la modification du mot de passe n'est pas possible. On se retrouve alors avec un compte bancal qui ne peut pas lire ses propres informations. À vérifier.

#2 - 04 mai 2021 10:35 - Serghei Mihai (congés, retour 15/05)

A priori c'est ça: #53663#note-14

#3 - 04 mai 2021 11:21 - Benjamin Dauvergne

Ce qui est signalé là c'est autre chose que je n'avais pas identifié mais qui doit aussi arriver, le mot de passe étant conservé en session pour les prochaines connexions au LDAP et éviter d'utiliser le mot de passe admin (surtout pour un changement de mot de passe) ça va générer cette erreur, par contre ça ne peut pas bloquer la navigation de l'utilisateur comme dans le ticket pointé, l'erreur est gérée :

```
    @classmethod
    def get_ldap_attributes(cls, block, conn, dn):
        ...
        try:
            results = conn.search_s(dn, ldap.SCOPE_BASE, u'(objectclass=*)', attributes)
        except ldap.LDAPError as e:
            log.error('unable to retrieve attributes of dn %r: %r', dn, e)
            return None <- ici tout va bien
```

Le problème dans le ticket pointé me semble relatif aux soucis de désactivation des LDAPs orphelins; je ne vois pas comment un compte usager pourrait être désactivé sauf manuellement.

#4 - 04 mai 2021 11:25 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> Ce qui est signalé là c'est autre chose que je n'avais pas identifié mais qui doit aussi arriver, le mot de passe étant conservé en session pour les prochaines connexions au LDAP et éviter d'utiliser le mot de passe admin (surtout pour un changement de mot de passe) ça va générer cette

erreur, par contre ça ne peut pas bloquer la navigation de l'utilisateur comme dans le ticket pointé, l'erreur est gérée :

Non ce n'est pas ça, si le mot de passe change alors on aura une erreur de bind et la connection ne sera pas retournée, dans ce cas on aura une erreur de ce type :

```
            log.warning('ldap: get_attributes failed, could not get a connection')
```

(et là on peut se dire que si pose celle-ci en warning on pourrait poser l'autre)

#6 - 05 mai 2021 12:27 - Nicolas Roche

De mon côté j'ai l'impression que cette erreur correspond à Villejuif avec la mise en place de la synchronisation des membres des groupes présents dans l'OU (je dit ça parce que j'ai eu l'impression que ça coïncidait quand j'ai vu apparaître cette trace, mais ça daterait de 3 mois).
https://dev.entrouvert.org/issues/50881#note-33

#7 - 06 mai 2021 15:05 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

J'ai trouvé, ça vient de ce commit :

```
commit 57ded4fd8fe8fbd388390aaf845567ff636abab7
Author: Valentin Deniaud <vdeniaud@entrouvert.com>
Date:   Thu Mar 25 11:37:54 2021 +0100

    authenticators: attach login failure record to user (#51626)

diff --git a/src/authentic2/backends/ldap_backend.py b/src/authentic2/backends/ldap_backend.py
index c252b638..a967174e 100644
--- a/src/authentic2/backends/ldap_backend.py
+++ b/src/authentic2/backends/ldap_backend.py
@@ -720,6 +720,10 @@ class LDAPBackend(object):
                         except ldap.INVALID_CREDENTIALS as e:
                             if block.get('use_controls') and len(e.args) > 0 and 'ctrls' in e.args[0]:
                                 self.process_controls(request, authz_id, DecodeControlTuples(e.args[0]['ctrls
']))
+                            attributes = self.get_ldap_attributes(block, conn, authz_id)
+                            user = self.lookup_existing_user(authz_id, block, attributes)
+                            if user and hasattr(request, 'failed_logins'):
+                                request.failed_logins.add(user)
                             user_login_failure(authz_id)
                             pass
                     else:
@@ -1238,7 +1242,7 @@ class LDAPBackend(object):
         for lookup_type in block['lookups']:
             if lookup_type == 'username':
                 return self.lookup_by_username(username)
-            elif lookup_type == 'external_id':
+            elif lookup_type == 'external_id' and attributes:
                 return self.lookup_by_external_id(block, attributes)

     def update_user_identifiers(self, user, username, block, attributes):
```

Sur une erreur de mot de passe on essaie tout de même trouver l'utilisateur concerné via une récupération des attributs et une conversion de ceux-ci en external_id_tuple; soit ça ne marche pas avec le bind admin soit il y a un souci (genre les mauvais crédentiels sont conservés entre temps).

#8 - 06 mai 2021 15:05 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Nouveau

#10 - 03 août 2021 11:00 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#11 - 03 août 2021 11:53 - Benjamin Dauvergne

- Fichier 0001-ldap-do-not-trace-when-SEARCH-return-no-attributes-5.patch ajouté

- Fichier 0002-ldap-on-INVALID_CREDENTIALS-try-to-rebind-before-loo.patch ajouté

- Tracker changé de Support à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

J'ai ajouté un bind avec les credentials admin et ça passe (les tests sans code foire avec 'unable to retrive attributes').

#12 - 03 août 2021 12:15 - Serghei Mihai (congés, retour 15/05)

- Statut changé de Solution proposée à Solution validée

Go dès que jenkins est vert.

#13 - 03 août 2021 14:09 - Benjamin Dauvergne

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

```
commit 7050db8b4ec9ffef31a4e6a942dcb1b5449d74e7
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Aug 3 11:09:38 2021 +0200

    ldap: on INVALID_CREDENTIALS, try to rebind before looking up the user (#53685)

    On a bind failure, the current bind context is lost, if we want to
    lookup the user whose bind failed we must first rebind with the service
    credentials.

commit c9b626d614af23f4f0b043a12ae3fa5a60ac3f4c
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Aug 3 11:51:55 2021 +0200

    ldap: do not trace when SEARCH return no attributes (#53685)
```

#14 - 09 août 2021 10:16 - Frédéric Péters

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

Fichiers

0001-ldap-do-not-trace-when-SEARCH-return-no-attributes-5.patch	1,36 ko	03 août 2021	Benjamin Dauvergne
0002-ldap-on-INVALID_CREDENTIALS-try-to-rebind-before-loo.patch	3,9 ko	03 août 2021	Benjamin Dauvergne