

Authentic 2 - Bug #70439

Idap: crash sur une erreur de mot de passe

18 octobre 2022 16:45 - Benjamin Dauvergne

Statut:	Solution déployée	Début:	18 octobre 2022
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposé:	Non		
Description			
https://sentry.entrouvert.org/entrouvert/publik/issues/96073/			
<pre>INVALID_CREDENTIALS: {'desc': 'Invalid credentials'} File "authentic2/backends/ldap_backend.py", line 726, in authenticate_block results = conn.simple_bind_s(authz_id, password, serverctrls=serverctrls) File "ldap/ldapobject.py", line 1222, in simple_bind_s res = self._apply_method_s(SimpleLDAPObject.simple_bind_s,*args,**kwargs) File "ldap/ldapobject.py", line 1204, in _apply_method_s return func(self,*args,**kwargs) File "ldap/ldapobject.py", line 446, in simple_bind_s resp_type, resp_data, resp_msgid, resp_ctrls = self.result3(msgid,all=1,timeout=self.timeout) File "ldap/ldapobject.py", line 748, in result3 resp_type, resp_data, resp_msgid, decoded_resp_ctrls, retoid, retval = self.result4(File "authentic2/backends/ldap_backend.py", line 184, in result4) = NativeLDAPObject.result4(File "ldap/ldapobject.py", line 758, in result4 ldap_result = self._ldap_call(self._l.result4,msgid,all,timeout,add_ctrls,add_intermediates,ad d_extop) File "ldap/ldapobject.py", line 331, in _ldap_call reraise(exc_type, exc_value, exc_traceback) File "ldap/compat.py", line 44, in reraise raise exc_value File "ldap/ldapobject.py", line 315, in _ldap_call result = func(*args,**kwargs) TransactionManagementError: select_for_update cannot be used outside of a transaction. File "django/core/handlers/exception.py", line 34, in inner response = get_response(request) File "django/core/handlers/base.py", line 115, in _get_response response = self.process_exception_by_middleware(e, request) File "django/core/handlers/base.py", line 113, in _get_response response = wrapped_callback(request, *callback_args, **callback_kwargs) File "django/views/decorators/clickjacking.py", line 15, in wrapped_view resp = view_func(*args, **kwargs) File "django/views/decorators/csrf.py", line 54, in wrapped_view return view_func(*args, **kwargs) File "django/urls/decorators.py", line 142, in _wrapped_view response = view_func(request, *args, **kwargs) File "django/views/decorators/cache.py", line 44, in _wrapped_view_func response = view_func(request, *args, **kwargs) File "authentic2/views.py", line 400, in login auth_blocks.append(utils_misc.get_authenticator_method(authenticator, 'login', parameters)) File "authentic2/urls/misc.py", line 196, in get_authenticator_method content = response = getattr(authenticator, method)(**parameters) File "authentic2/apps/authenticators/models.py", line 206, in login return views.login_password_login(request, self, *args, **kwargs) File "authentic2/views.py", line 719, in login_password_login csrf_token_check(request, form) File "authentic2/urls/views.py", line 48, in csrf_token_check if form.is_valid() and not getattr(request, 'csrf_processing_done', False): File "django/forms/forms.py", line 185, in is_valid</pre>			

```

return self.is_bound and not self.errors
File "django/forms/forms.py", line 180, in errors
    self.full_clean()
File "django/forms/forms.py", line 382, in full_clean
    self._clean_form()
File "django/forms/forms.py", line 409, in _clean_form
    cleaned_data = self.clean()
File "authentic2/forms/authentication.py", line 105, in clean
    self.clean_authenticate()
File "authentic2/forms/authentication.py", line 122, in clean_authenticate
    self.user_cache = utils_misc.authenticate(
File "authentic2/utils/misc.py", line 1310, in authenticate
    return dj_authenticate(request=request, **kwargs)
File "django/contrib/auth/__init__.py", line 73, in authenticate
    user = backend.authenticate(request, **credentials)
File "authentic2/backends/ldap_backend.py", line 652, in authenticate
    user = self.authenticate_block(request, block, uid, password)
File "authentic2/backends/ldap_backend.py", line 744, in authenticate_block
    user = self._lookup_existing_user(authz_id, block, attributes)
File "authentic2/backends/ldap_backend.py", line 1485, in _lookup_existing_user
    user = self._lookup_by_email(ou=ou, block=block, attributes=attributes)
File "authentic2/backends/ldap_backend.py", line 1396, in _lookup_by_email
    Lock.lock_email(email)
File "authentic2/models.py", line 626, in lock_email
    cls.lock('email:%s' % email, nowait=nowait)
File "authentic2/models.py", line 615, in lock
    cls.objects.select_for_update(nowait=nowait).get(name=name)
File "django/db/models/query.py", line 402, in get
    num = len(clone)
File "django/db/models/query.py", line 256, in __len__
    self._fetch_all()
File "django/db/models/query.py", line 1242, in _fetch_all
    self._result_cache = list(self._iterable_class(self))
File "django/db/models/query.py", line 55, in __iter__
    results = compiler.execute_sql(chunked_fetch=self.chunked_fetch, chunk_size=self.chunk_size)
File "django/db/models/sql/compiler.py", line 1129, in execute_sql
    sql, params = self.as_sql()
File "django/db/models/sql/compiler.py", line 518, in as_sql
    raise TransactionManagementError('select_for_update cannot be used outside of a transaction.')

```

`_lookup_existing_user()` fait en dehors d'une transaction, mais dans ce cas précis aucun lock ne devrait être pris, le fix le plus simple reste de faire ça dans un scope atomic().

Demandes liées:

Lié à Authentic 2 - Bug #70437: sur un login, avec du LDAP, TransactionManage...

Fermé

18 octobre 2022

Révisions associées

Révision 0c77d676 - 23 février 2024 20:18 - Benjamin Dauvergne

ldap: prevent use of lock_email outside of a transaction (#70439)

Historique

#1 - 18 octobre 2022 16:48 - Frédéric Péters

- Lié à Bug #70437: sur un login, avec du LDAP, TransactionManagementError: select_for_update cannot be used outside of a transaction. ajouté

#3 - 29 novembre 2023 10:14 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 29 novembre 2023 14:00 - Robot Gitea

- Statut changé de Nouveau à Solution proposée

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : <https://git.entrouvert.org/entrouvert/authentic/pulls/192>
- Titre : Ne pas utiliser Lock.lock_email si on est pas dans la création d'un nouvel utilisateur et donc dans une transaction ([#70439](#))

- Modifications : <https://git.entrouvert.org/entrouvert/authentic/pulls/192/files>

#5 - 23 février 2024 12:07 - Robot Gitea

- Statut changé de *Solution proposée* à *Solution validée*

Nicolas Roche (nroche) a approuvé une pull request sur Gitea concernant cette demande :

- URL : <https://git.entrouvert.org/entrouvert/authentic/pulls/192>

#6 - 23 février 2024 20:18 - Robot Gitea

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

Benjamin Dauvergne (bdauvergne) a mergé une pull request sur Gitea concernant cette demande :

- URL : <https://git.entrouvert.org/entrouvert/authentic/pulls/192>
- Titre : Ne pas utiliser Lock.lock_email si on est pas dans la création d'un nouvel utilisateur et donc dans une transaction ([#70439](#))
- Modifications : <https://git.entrouvert.org/entrouvert/authentic/pulls/192/files>

#7 - 23 février 2024 21:23 - Transition automatique

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