

Authentic 2 - Bug #32001

CAS : erreur "unable to compute an identifier for user" lors d'un accès post-réinitialisation du mot de passe

04 avril 2019 15:34 - Benjamin Renard

Statut:	Nouveau	Début:	04 avril 2019
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:	authentic2-idp-cas	Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Non		

Description

Bonjour,

Il semble y avoir un souci suite à la réinitialisation du mot de passe. Celui-ci semble se produire uniquement lors de la suite évènements suivant :

- on tente d'accéder à un service utilisant l'authentification SSO via CAS
- celle-ci nous renvoi vers la page d'authentification du SSO
- on clique sur le lien "mot de passe perdu" et on suit la procédure pour le changer
- une fois le mot de passe changé, Authentic tente de nous rediriger vers l'application ayant demandée initialement l'authentification

A ce moment précis, Authentic ne semble pas avoir accès aux informations issues des attributs LDAP de l'utilisateur : si dans la configuration du service CAS, le choix de l'information utilisée comme login est un attribut LDAP (par exemple, `l_uid_`), on a l'erreur suivante :

```
DEBUG modified password for dn u'uid=renardb,ou=people,o=example'
INFO user renardb (094a09) resetted its password with token u'557-ed207'...
INFO logged in (email)
DEBUG validation service: u'https://idp.domain.tld/myapp' ticket: u'ST-MlhaEE0TRIeg3dqzaC1YxUwwQ5'
  renew: False
DEBUG got config [{"binddn": u'uid=authentic,ou=sysaccounts,o=example', 'groupsu': (u'cn=ssosupera
dmins,ou=groups,o=example'), 'set_mandatory_groups': (), 'email_field': u'mail', 'sync_ldap_users
_filter': u'', 'multimatch': False, 'cacertdir': u'', 'group_filter': u'(&(uniqueMember={user_dn})
(objectClass=exampleGroup))', 'groupstaff': (u'cn=ssoadmins,ou=groups,o=example'), 'is_staff': No
ne, 'update_username': False, 'external_id_tuples': [[u'uid'], [u'dn:noquote']]], 'attribute_mappin
gs': [], 'set_mandatory_roles': (), 'clean_external_id_on_update': True, 'user_can_change_password
': True, 'realm': u'ldap_example_people', 'certfile': u'', 'username_template': u'{uid[0]}', 'can_
reset_password': True, 'replicas': True, 'group_dn_template': u'', 'use_tls': False, 'is_superuser
': None, 'keep_password_in_session': False, 'limit_to_realm': False, 'user_attributes': [], 'group
_mapping': (), 'lname_field': u'sn', 'mandatory_attributes_values': {}, 'create_group': False, 'ti
meout': -1, 'use_password_modify': True, 'connect_with_user_credentials': True, 'ldap_options': {}
, 'bind_with_username': False, 'basedn': u'o=example', 'lookups': (u'external_id', u'username'), 'u
se_first_url_for_external_id': True, 'bindpw': u'myBigSecret', 'attributes': (u'uid', u'mail', u'
displayname', u'sn', u'givenname', u'title', u'exampleIdentifier', u'o', u'ou', u'memberof'), 'gro
up_to_role_mapping': (), 'member_of_attribute': u'', 'user_basedn': u'ou=people,o=example', 'globa
l_ldap_options': {}, 'ou_slug': u'', 'cacertfile': u'/etc/ssl/certs/ca-certificates.crt', 'user_dn
_template': u'', 'keep_password': False, 'shuffle_replicas': True, 'require_cert': u'demand', 'ref
errals': False, 'url': ['ldaps://ldap.domain.tld:636'], 'bindsasl': (), 'active_directory': False,
  'groupactive': (), 'disable_update': False, 'fname_field': u'givenname', 'user_filter': u'(&(obje
ctClass=examplePeople)(|(uid=%s)(mail=%s)))', 'keyfile': u''}, {'groupsu': (), 'email_field': u'mai
l', 'sync_ldap_users_filter': u'', 'global_ldap_options': {}, 'attribute_mappings': [], 'set_mand
atory_roles': (), 'clean_external_id_on_update': True, 'member_of_attribute': u'', 'username templ
ate': u'{uid[0]}', 'group_dn_template': u'', 'is_superuser': None, 'user_attributes': [], 'ldap_op
tions': {}, 'bind_with_username': False, 'use_first_url_for_external_id': True, 'bindpw': u'myBigS
ecret', 'user_basedn': u'ou=sysaccounts,o=example', 'user_can_change_password': False, 'ou_slug': u
'', 'cacertfile': u'/etc/ssl/certs/ca-certificates.crt', 'user_dn_template': u'', 'keep_password
': False, 'require_cert': u'demand', 'referrals': False, 'bindsasl': (), 'active_directory': False,
  'disable_update': False, 'binddn': u'uid=authentic,ou=sysaccounts,o=example', 'cacertdir': u'', 'i
set_mandatory_groups': (), 'multimatch': False, 'group_filter': u'(&(member={user_dn})(objectClass
=groupOfNames))', 'groupstaff': (), 'is_staff': None, 'update_username': False, 'external_id_tuple
```

```
s': [[u'uid'], [u'dn:noquote']], 'can_reset_password': False, 'realm': u'ldap_example_sysaccounts', 'fname_field': u'givenname', 'replicas': True, 'use_tls': False, 'keep_password_in_session': False, 'limit_to_realm': False, 'group_mapping': (), 'lname_field': u'sn', 'mandatory_attributes_values': {}, 'create_group': False, 'timeout': -1, 'connect_with_user_credentials': True, 'basedn': u'o=example', 'user_filter': u'(&(objectClass=exampleSysaccount)(uid=%s))', 'group_to_role_mapping': (), 'certfile': u'', 'use_password_modify': True, 'shuffle_replicas': True, 'lookups': (u'external_id', u'username'), 'url': ['ldaps://ldap.domain.tld:636'], 'groupactive': (), 'attributes': (u'uid',), 'keyfile': u''}]  
ERROR unable to compute an identifier for user u'renardb (094a09)' and service https://idp.domain.tld/myapp  
WARNING validation failed service: u'https://idp.domain.tld/myapp' code: INTERNAL_ERROR
```

Si en outre, dans la configuration du service CAS, le choix de l'information utilisée comme login est une information propre à Authentic (par exemple, `django_user_username`), on a pas d'erreur.

Historique

#1 - 04 avril 2019 17:55 - Benjamin Dauvergne

Oui l'utilisation d'attributs LDAP est incompatible avec l'IdP CAS, puisqu'elle se fait hors session principale et donc on a plus l'accès au LDAP (et surtout l'objet User n'a pas la bonne classe) il faut utiliser un attribut stocké dans Authentic (ou au moins recopié à l'authentification).

#2 - 18 janvier 2022 15:50 - Mikaël Ates

- Assigné à *Gestion d'identité supprimé*
- *Planning mis à Non*