Authentic 2 - Bug #86089

CAS : plus accès aux attributs LDAP lors de la validation du ticket

24 janvier 2024 18:59 - Benjamin Renard

Statut:	Fermé	**Début:**	24 janvier 2024
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Renard	**% réalisé:**	0%
Catégorie:	authentic2-idp-cas	**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

La mise à jour d'une instance d'Authentic en version *4.82-1~eob110+1* vers *5.21-1~eob110+1* à casser les accès à une application utilisant l'IDP CAS : le ticket est bien généré, mais au moment de sa validation, j'ai l'erreur suivante :

```
Jan 24 17:25:13 sso-preprod-02 authentic2[1646195]: 192.168.3.67 - r:7FEEBBA37EB0 ERROR unable to
compute an identifier for user 'XXXX' and service XXXX
Jan 24 17:25:13 sso-preprod-02 authentic2[1646195]: 192.168.3.67 - r:7FEEBBA37EB0 WARNING validati
on failed service: 'XXXX' code: INTERNAL_ERROR
```

Ce service utilise l'attribut LDAP "mail" comme identifiant de l'utilisateur et en ajoutant un peu de debug dans le code (*/usr/lib/python3/dist-packages/authentic2_idp_cas/views.py*, ligne 267), je constate que l'attribut LDAP est effectivement manquant :

```
Jan 24 17:31:15 sso-preprod-02 authentic2[1658829]: 192.168.3.67 - r:7FB6055697F0 ERROR unable to
compute an identifier for user 'XXXX' and service XXXXXX (attribute = mail, attributes = {'request
': <WSGIRequest: GET '/idp/cas/serviceValidate?service=XXXXXX&ticket=ST-AieWsxHXYsjMDOCyawYkIKdINj
'>, 'user': <User: 5775 (95df72)>, 'service': <Service 'XXXXXX'>, '__wanted_attributes': ['mail'],
 'django_user_id': 6066, 'django_user_password': 'XXXX', 'django_user_last_login': datetime.dateti
me(2024, 1, 24, 16, 31, 8, 213521, tzinfo=<UTC>), 'django_user_uuid': '95df726dd34d48eb8bae9a57da2
d3258', 'django_user_username': '5775', 'django_user_first_name': 'XXXXXX', 'django_user_last_name
': 'XXXXX', 'django_user_email': 'support@easter-eggs.com', 'django_user_email_verified': True, 'd
jango_user_email_verified_date': datetime.datetime(2017, 8, 18, 17, 11, 50, 898526, tzinfo=<UTC>),
 'django_user_email_verified_sources': [], 'django_user_is_superuser': True, 'django_user_is_staff
': True, 'django_user_is_active': True, 'django_user_date_joined': datetime.datetime(2017, 8, 18,
17, 11, 50, 898526, tzinfo=<UTC>), 'django_user_modified': datetime.datetime(2019, 4, 2, 16, 44, 1
4, 328022, tzinfo=<UTC>), 'django_user_ou_uuid': '0430bd21fae5460fa7852d12f2bff24c', 'django_user_
ou_slug': 'default', 'django_user_ou_name': 'Collectivité par défaut', 'django_user_first_name:ver
ified': False, 'django_user_last_name:verified': False, 'django_user_groups': [], 'django_user_gro
up_names': [], 'django_user_domain': '', 'django_user_identifier': '5775', 'django_user_full_name'
: 'easter-eggs Support', 'a2_role_slugs': <RoleQuerySet []>, 'a2_role_names': <RoleQuerySet []>, '
a2_role_uuids': <RoleQuerySet []>, 'a2_service_ou_role_slugs': <RoleQuerySet []>, 'a2_service_ou_r
ole_names': <RoleQuerySet []>, 'a2_service_ou_role_uuids': <RoleQuerySet []>})
```

En grattant un peu le sujet, j'ai compris que le problème venait du fait qu'on tentait de récupérer les attributs de l'utilisateur à partir d'un objet User en non pas un objet *LDAPUser*. En remontant à la source de la récupération des attributs, j'ai pu constater que dans la méthode *ValidateBaseView.get_attributes* de la version *4.82-1~eob110+1*, l'objet user passer dans le contexte à la méthode *authentic2.attributes_ng.engine.get_attributes* était récupéré à l'aide de *authentic2.utils.misc.get_user_from_session_key* quand dans la version *5.21-1~eob110+1* on utilise directement l'utilisateur issu de la base et récupéré à partir du Ticket.

```
user = get_user_from_session_key(st.session_key)
assert user.pk  # not an annymous user
assert st.user_id == user.pk  # session user matches ticket user
st.attributes = get_attributes(
    {
        'request': request,
        'user': user,
[...]
```

VS:

```
st.attributes = get_attributes(
    {
        'request': request,
```

```
        'user': st.user,
[...]
```

En faisant un rollback à ce sujet, tout refonctionne comme avant.

Je ne sais pas ce qui a motivé ce changement, mais cela introduit une régression et cela me fait dire qu'il doit manquer un test unitaire à ce sujet.

Révisions associées

Révision d50622cb - 05 février 2024 10:51 - Benjamin Dauvergne

idp_cas: fix retrieval of LDAP user attributes (#86089)

Historique

#1 - 24 janvier 2024 19:05 - Benjamin Renard

Régression introduite par :

```
commit f1ec75622bcb94dfeb7bf9dc082623a493dbddbb
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Nov 30 07:23:47 2023 +0100

    idp_cas: does not revalidate the session key (#10688)

    Validation of the session_key is already done in Ticket.valid(), but we
    can move the test of the current session user in
    Ticket.session_exists().

[...]

@@ -280,13 +281,10 @@ class ValidateBaseView(CasMixin, View):
         '''Retrieve attribute for users of the session linked to the ticket'''
         if not hasattr(st, 'attributes'):
             wanted_attributes = st.service.get_wanted_attributes()
-            user = get_user_from_session_key(st.session_key)
-            assert user.pk  # not an annymous user
-            assert st.user_id == user.pk  # session user matches ticket user
             st.attributes = get_attributes(
                 {
                     'request': request,
-                    'user': user,
+                    'user': st.user,
                     'service': st.service,
                     '__wanted_attributes': wanted_attributes,
                 }
```

#2 - 24 janvier 2024 21:36 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#3 - 24 janvier 2024 21:37 - 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/242
- Titre : idp_cas: fix retrieval of LDAP user attributes (#86089)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/242/files

#4 - 25 janvier 2024 14:16 - Thomas Noël

- Assigné à changé de Benjamin Dauvergne à Benjamin Renard

Benjamin (R.), sur le papier, le patch proposé par Benjamin (D.)

- https://git.entrouvert.org/entrouvert/authentic/pulls/242/files

me parait cohérent et je m'apprêtai à le valider

Cependant je serais plus à l'aise si tu peux le tester de ton côté avant que je le "acke" et que ça soit mergé.

Je te remercie par avance.

#5 - 25 janvier 2024 15:09 - Benjamin Renard

Thomas Noël a écrit :

> Benjamin (R.), sur le papier, le patch proposé par Benjamin (D.)
>
> - https://git.entrouvert.org/entrouvert/authentic/pulls/242/files
>
> me parait cohérent et je m'apprêtai à le valider
>
> Cependant je serais plus à l'aise si tu peux le tester de ton côté avant que je le "acke" et que ça soit mergé.

Tu fais bien, car non, ça ne fonctionne pas. Mon test : j'ai appliqué ce patch (https://git.entrouvert.org/entrouvert/authentic/pulls/242/files) et testé une authentification sur un service CAS utilisant un attribut LDAP comment identifiant et le problème reste le même. Cela vient du fait que c'est toujours *st.user* (objet *User*) qui est passé à *authentic2.attributes_ng.engine.get_attributes* et non l'objet *user* (*LDAPUser*, récupéré via *authentic2.utils.misc.get_user_from_session_key*). Simplement en modifiant ce point, ça fonctionne comme attendu.

#6 - 25 janvier 2024 16:55 - Thomas Noël

Rebonjour Benjamin,

Benjamin (l'autre) a refait une version du patch qui envoie bien user et pas st.user : peux-tu voir si, cette fois, c'est mieux ?

(Désolé de ramer sur l'affaire, mais CAS+LDAP c'est «assez loin» de nos usages à Entr'ouvert)

C'est toujours sur https://git.entrouvert.org/entrouvert/authentic/pulls/242/files que tu verras la nouvelle version du patch.

#7 - 25 janvier 2024 18:47 - Benjamin Renard

Thomas Noël a écrit :

> Rebonjour Benjamin,
>
> Benjamin (l'autre) a refait une version du patch qui envoie bien user et pas st.user : peux-tu voir si, cette fois, c'est mieux ?
>
> (Désolé de ramer sur l'affaire, mais CAS+LDAP c'est «assez loin» de nos usages à Entr'ouvert)
>
> C'est toujours sur https://git.entrouvert.org/entrouvert/authentic/pulls/242/files que tu verras la nouvelle version du patch.

Pas de souci, cette fois on est bon ! :)

#8 - 26 janvier 2024 00:27 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Thomas NOËL (tnoel) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/242

#9 - 05 février 2024 10:03 - Benjamin Renard

Robot Gitea a écrit :

> Thomas NOËL (tnoel) a approuvé une pull request sur Gitea concernant cette demande :
>
> - URL : https://git.entrouvert.org/entrouvert/authentic/pulls/242

Seriez-vous me dire quand ce patch sera t-il mergé et inclus dans une release ? C'est histoire de planifier les upgrades bloqués chez nos clients en attendant.

Par avance, merci.

#10 - 05 février 2024 11:38 - 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/242

- Titre : idp_cas: fix retrieval of LDAP user attributes (#86089)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/242/files

#11 - 05 février 2024 13:18 - Transition automatique

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

#12 - 05 février 2024 14:09 - Benjamin Dauvergne

Benjamin Renard a écrit :

> Par avance, merci.

Ce sera dans le dépôt de prod ce vendredi.

#13 - 07 avril 2024 04:42 - Transition automatique

Automatic expiration