Plugin FS FranceConnect - Bug #10015

We should fail a sso when userinfo are not resolved (including handling ressource call failure)

17 février 2016 17:05 - Mikaël Ates

Statut:	Fermé	**Début:**	17 février 2016
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Hors marché:	Non	**Planning:**	
Patch proposed:	Oui		

Description

From the spec (http://openid.net/specs/openid-connect-core-1_0.html#CodeFlowSteps), for a sso using the 'Authentication using the Authorization Code Flow', I do not see any requirement to successfully resolve the user info endpoint to have a successful sso. That makes sense, and we implement that, since the sub is taken from the id token received from the token endpoint and we authenticate the user only using the sub.

For now, it fails, e.g. a JSON error is raised if no user info is received, if the userinfo is not successfully resolved.

However, the FC documentation assumes at different place that a successful SSO includes the user info resolution (e.g. validation page, 3.1 Connexion via SSO : "je dois voir un lien avec mon prénom et mon nom").

In order to comply with FC, I propose to fail the sso if the userinfo ressource is not resolved.

Historique

#1 - 17 février 2016 17:06 - Mikaël Ates

- Description mis à jour

#2 - 17 février 2016 17:11 - Mikaël Ates

- Description mis à jour

#3 - 17 février 2016 17:16 - Benjamin Dauvergne

I would add data.raise_for_status(allow_redirects=False) after the line data = self.oauth_session.... to also handle such errors as HTTP (3xx, 4xx, 5xx). Also I don't know if catching SSLError after RequestException would work as SSLError is a child class of RequestException[1].

1

```
class RequestException(RuntimeError):
    """There was an ambiguous exception that occurred while handling your
    request."""

class HTTPError(RequestException):
    """An HTTP error occurred."""
    response = None

class ConnectionError(RequestException):
    """A Connection error occurred."""

class SSLError(ConnectionError):

    """An SSL error occurred."""
```

```
>>> class A(Exception):
...     pass
...
>>> try:
...     raise A
... except Exception:
...     print 'E'
... except A:
...     print 'A'
...
```

```
E
```

#4 - 17 février 2016 17:45 - Mikaël Ates

- Fichier 0001-Handle-ressource-resolution-failure-and-fail-sso-in-.patch ajouté

Ok for adding data.raise_for_status and I added to the get arguments allow_redirects=False, timeout=3.

For the exceptions, it is strange since I've tested for the access token request with the same error catching statements and I grab the SSL error :

```
    try:
        response = requests.post(app_settings.token_url, data=data,
                             verify=app_settings.verify_certificate, timeout=3)
    except requests.exceptions.RequestException as e:
        logger.error(u'unable to retrieve access token {}'.format(e))
    except requests.exceptions.SSLError as e:
        logger.error(u'ssl error : {}'.format(e))
    else:
        logger.info('resolve access token %r %r',
                                app_settings.token_url, response.content)
        return response.json()
```

```
ERROR authentic2_auth_fc.views.resolve_access_token: unable to retrieve access token [SSL: CERTIFICATE_VERIFY_
FAILED] certificate verify failed (_ssl.c:581)
```

#5 - 17 février 2016 17:45 - Mikaël Ates

- Fichier 0001-Handle-ressource-resolution-failure-and-fail-sso-in-.patch supprimé

#6 - 17 février 2016 17:51 - Benjamin Dauvergne

Mikaël Ates a écrit :

> Ok for adding data.raise_for_status and I added to the get arguments allow_redirects=False, timeout=3.
>
> For the exceptions, it is strange since I've tested for the access token request with the same error catching statements and I grab the SSL error :
>
> [...]
>
> [...]

"unable to retrieve access token" is the string returned by the first catch block, exactly like I said.

#7 - 17 février 2016 17:53 - Benjamin Dauvergne

I think the allow_redirects=False must be set on the raise_for_status() too but you can allow it on the get() (it's allowed by default I think).

#8 - 17 février 2016 18:25 - Mikaël Ates

- Fichier 0001-Handle-ressource-resolution-failure-and-fail-sso-in-.patch ajouté

Sorry for the exception I did not get your point. I removed that catch.

raise_for_status() does not seem to take any arguments.

#9 - 17 février 2016 18:25 - Mikaël Ates

- Fichier 0001-Handle-ressource-resolution-failure-and-fail-sso-in-.patch supprimé

#10 - 17 février 2016 18:30 - Benjamin Dauvergne

Ok for raise_for_status() I must have checked on an older version of raise_for_status() and the API has moved. Ack.

#11 - 23 février 2016 15:39 - Mikaël Ates

- Statut changé de Nouveau à Fermé

Fichiers

0001-Handle-ressource-resolution-failure-and-fail-sso-in-.patch	3,19 ko	17 février 2016	Mikaël Ates