EoleSSO - Anomalie #4845

utiliser le compte de lecture défini pour chaque annuaire lors de la recherche des homonymes.

02/06/2013 12:14 PM - Bruno Boiget

Status:	Fermé	**Start date:**	02/06/2013
Priority:	Normal	**Due date:**	02/07/2014
Assigned To:	Bruno Boiget	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Mises à jour 2.3.12	**Spent time:**	0.42 hour
Distribution:	EOLE 2.3		

Description

problème remonté par plusieurs académies pour le branchement de Seshat sur un annuaire académique :

La recherche sur les 'DN' pour détecter les différents annuaires dans lesquels un utilisateur est présent se fait en anonyme.
Cela n'étant pas autorisée sur l'annuaire académique, EoleSSO ne détecte pas les utilisateurs dans celui-ci.

Pour éviter d'ajouter des autorisations, il faudrait également effectuer cette recherche avec l'utilisateur configuré le cas échéant.

Related issues:

Related to EoleSSO - Evolution #6734: permettre la configuration de l'attribu...	**Fermé**	**02/07/2014**
Related to EoleSSO - Anomalie #7300: applique la correction publiée en 2.3.12...	**Fermé**	**02/20/2014**

Associated revisions

Revision 0c5cd6e3 - 02/06/2013 12:16 PM - Bruno Boiget

détection des branches d'un utilisateur avec l'utilisateur en lecture de chaque annuaire (fixes #4845)

Revision e19438ea - 12/02/2013 03:52 PM - Bruno Boiget

Utilisation de l'utilisateur reader dans toutes les recherches ldap si possible

- recherche des dn d'utilisateurs (homonymes)
- lecture des informations sur les groupes
- l'attribut correpondant au login est désormais configurable en mode expert

Fixes #4845
Fixes #6734

Revision d355624c - 12/04/2013 05:32 PM - Bruno Boiget

eoleldaptor: ajout d'un fallback en mode anonyme si mauvais mot de passe reader (+log)

`Ref #4845`

Revision 0bc529e3 - 12/04/2013 05:42 PM - Bruno Boiget

Report des modifications de la version 2.3

- utilisation de l'utilisateur en lecture si possible (ref #4845)
- configuration de l'attribut de recherche des utilisateurs (ref #6743)

Revision cefc5832 - 12/04/2013 05:42 PM - Bruno Boiget

eoleldaptor: ajout d'un fallback en mode anonyme si mauvais mot de passe reader (+log)

`ref #4845`

Revision 7e17f458 - 12/11/2013 04:47 PM - Bruno Boiget

modif oubliée sur eoleldaptor (ref #4845)

Revision db74f254 - 12/11/2013 05:20 PM - Bruno Boiget

modif oubliée sur eoleldaptor (ref #4845)

Revision ad2c95e5 - 02/04/2014 02:20 PM - Bruno Boiget

correction de la recherche d'utilisateur en cas de fédération (FS)

Fixes #4845 @25m

History

#1 - 02/06/2013 12:16 PM - Bruno Boiget

- Status changed from Accepté to Résolu

- % Done changed from 0 to 100

Appliqué par commit 0c5cd6e3b96f99efd7c2f1089b48bf4a7193f3e1.

#2 - 02/08/2013 11:30 AM - Bruno Boiget

- Status changed from Résolu to Réouvert

- % Done changed from 100 to 80

fonctionne pour la recherche des annuaires où l'utilisateur est présent, mais pas au moment de l'authentification (il reste une recherche de DN anonyme dans ce cas).

Faire un bind sur l'utilisateur reader aussi dans ce cas

#3 - 02/11/2013 10:13 AM - Luc Bourdot

- Due date changed from 02/08/2013 to 02/15/2013

#4 - 02/13/2013 05:02 PM - Bruno Boiget

- Due date changed from 02/15/2013 to 02/22/2013

- Target version changed from Mises à jour 2.3.8 to Mises à jour 2.3.9

vu avec mathieu (poitiers), la demande peut être reportée à la candidate suivante.

#5 - 03/27/2013 11:36 AM - Fabrice Barconnière

- Due date deleted (02/22/2013)

#6 - 03/29/2013 10:32 AM - Redmine Admin

- Target version changed from Mises à jour 2.3.9 to Mises à jour 2.3.10

#7 - 07/04/2013 10:48 AM - Joël Cuissinat

- Target version changed from Mises à jour 2.3.10 to Mises à jour 2.3.11

#8 - 11/07/2013 09:26 AM - Fabrice Barconnière

- Due date set to 11/08/2013

#9 - 11/07/2013 10:41 AM - Bruno Boiget

- Due date deleted (11/08/2013)

- Target version changed from Mises à jour 2.3.11 to Mises à jour 2.3.12

problème contourné temporairement en jouant sur les règles des annuaires académiques

#10 - 12/02/2013 03:54 PM - Bruno Boiget

- Status changed from Réouvert to Résolu

- % Done changed from 80 to 100

Appliqué par commit e19438ea06dc6869894214a0479357323c4c563e.

#11 - 02/04/2014 02:19 PM - Bruno Boiget

- Status changed from Résolu to Réouvert

- % Done changed from 100 to 90

Les modifications sur eolesso/dataproxy.py empêchent la recherche d'utilisateur de fonctionner lors d'un fédération (fournisseur de service)

pb détecté dans le cas d'une fédération de seshat vers scribe (annuaire de scribe répliqué sur seshat avec uid comme attribut de fédération) :

test de fédération avec l'url : https://<adresse_seshat>:8443/saml?sp_ident=scribe

- scribe indique qu'il n'a pas retrouvé l'utilisateur
- dans les logs de scribe (/var/log/rsyslog/local/eoleosso/eolesso.alert.log)

```
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32] Traceback (most recent call last
):
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32]   File "./authserver.py", line 6
94, in authenticate_federated_user
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32]     defer_fed_data = self._data_
proxy.get_user_data(search_attrs, search_branch)
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32]   File "/usr/lib/pymodules/pytho
n2.6/eolesso/dataproxy.py", line 264, in get_user_data
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32]     return defer_auth.addCallbac
ks(self.callb_get_data, self.errb_auth, callbackArgs=[user_id, passwd, filter_attrs, search_branch, servers[1:
]])
Feb  4 12:18:11 scribe23-yo-91 eolesso: [TLSProtocolWrapper,5,192.168.230.32] NameError: global name 'user_id'
 is not defined
```

#12 - 02/04/2014 02:22 PM - Bruno Boiget

- Status changed from Réouvert to Résolu

- % Done changed from 90 to 100

Appliqué par commit ad2c95e58abc41226713f67a72876719cd9048a8.

#13 - 02/04/2014 03:29 PM - Lionel Morin

- Status changed from Résolu to Fermé

Testé sur un scribe avec accès à un zéphir dont le dn n'est pas accessible en mode anonyme (avec configuration de l'utilisateur reader).

```
access to dn=*
        by self read
        by dn="cn=reader,o=gouv,c=fr" read
        by * none

# ACL par défaut
access to *
        by * read
```

Si un utilisateur est présent dans les 2 annuaires, les 2 entrées sont bien détectées et apparaissent dans une liste déroulante.

#14 - 02/06/2014 04:21 PM - Fabrice Barconnière

- Due date set to 02/07/2014