Morpho - Bug #5864

ECP login causes new DN so user's can't see their data

02/12/2013 06:25 PM - Matt Jones

Status:	Resolved	**Start date:**	02/12/2013
Priority:	Immediate	**Due date:**	
Assignee:	ben leinfelder	**% Done:**	0%
Category:	morpho - general	**Estimated time:**	0.00 hour
Target version:	2.0.0	**Spent time:**	0.00 hour
Bugzilla-Id:	5864		

Description

Logging into the new version of Morpho using ECP has two negative side effects that need to be resolved.

1) The ECP login uses the ou=Account subtree, so my password changed and most users will not realize this, and thus will not be able to find their previously saved data packages

2) the DN for logged in users changes to the CILogon DN, which also causes their previously created data to not show up. Even once the user's old knb id is mapped to their new CILogon DN, its not clear if their data will be accessible in Morpho.

Related issues:

Blocks Metacat - Bug #5865: Ensure DataONE pathquery for owner uses mapped ac...	**Resolved**	**02/13/2013**

History

#1 - 02/12/2013 10:26 PM - ben leinfelder

On #1, yes, we are using a different account. I could have set up the test KNB IdP to use the o=NCEAS tree but I used the ou=Account tree to catch a more diverse set of users without committing to any one organizational affiliation. As far as I understand it, our IdP strategy is still in discussion even though we are running out of time to set up a production-ready IdP before a Morpho 2.0.0 release.

On #2, after a legacy "uid=X,o=Y" account has been mapped to its CILogon identity, the user will have the same level of access enjoyed previously. We should investigate the "owner" pathquery processing to make sure it honors this mapped access, but otherwise direct manipulations using a mapped identity should work without the user noticing any change.

In general I do feel as though there is still some uncertainty about how this will all be configured for our system (KNB) and for other similar systems that have been relying on our LDAP structure for many many years. The technical hurdles are less troublesome than the organizational/ID management decisions that need to be finalized at this point.

#2 - 02/13/2013 12:32 PM - ben leinfelder

I've now included the equivalent identities (listed in the CILogon certs that contain SubjectInfo) as additional <owner> elements in the pathquery used during the "Open..." command. In theory, this should show the documents owned by the user (assuming the access permissions also all this via the mapping).

#3 - 02/14/2013 10:41 PM - ben leinfelder

This is resolved in the sense that Morpho has been updated to search for packages that are owned by any of the equivalent identities. The other identity issues are being tracked in redmine: https://redmine.dataone.org/issues/3513

#4 - 03/27/2013 02:31 PM - Redmine Admin

Original Bugzilla ID was 5864