Morpho - Bug #88

need ability to manipulate access control lists

08/20/2000 08:56 PM - Matt Jones

Status:	Resolved	**Start date:**	08/20/2000
Priority:	Normal	**Due date:**	
Assignee:	Saurabh Garg	**% Done:**	0%
Category:	morpho - general	**Estimated time:**	0.00 hour
Target version:	1.5	**Spent time:**	0.00 hour
Bugzilla-Id:	88		

Description

The client will be saving metadata and data to the server. It needs to be able to send owner and ACL information when saving to the network, and there needs to be an easy-to-use user interface for assigning access permissions (probably a dialog with checkboxs for assigning permissions that is reachable from the query resultset records and the mde).

Related issues:

Blocks Morpho - Bug #548: consolidate metadata editing systems in morpho	**In Progress**	**07/09/2002**
Blocks Metacat - Bug #92: need access control tracking for metadata documents	**Resolved**	**08/20/2000**
Blocks Morpho - Bug #553: support eml 2.0.0 and later revisions	**Resolved**	**07/09/2002**

History

#1 - 08/24/2000 12:21 PM - Matt Jones

increased priority on this because it is essential that it be available for testing the server ACL features (see bug #92).

#2 - 09/22/2000 03:08 PM - Matt Jones

changed target milestone to Beta2 as we discussed

#3 - 07/12/2001 05:11 PM - Matt Jones

Changed milestone for a number of morpho features that will not be able to be completed by Beta 1 (ESA). Delaying these features to Beta 2.

#4 - 02/12/2002 04:46 PM - Matt Jones

Need a better GUI for editing eml-access documents. At a minimum, need a dialog with 3 checkboxes for read/write/all permission for the "public" user.
Secondarily, need to be able to type in a user's DN and have 3 checkboxes for read/write/all for that user. Please discuss this UI with me before implementing.

#5 - 12/16/2003 08:51 AM - Dan Higgins

Still need a better interface for access control with eml2.0.0

#6 - 01/07/2004 04:28 PM - Saurabh Garg

Right now it does the minimum requirement of asking for public read access.

Next step could be to ask for DNs and giving permissions. Can DNs be asked as username and organizations Names?
The user can enter the username, pick an organization from a drop down list and select read/write/all permissions. CustomList class can be used so that a user can add as many DNs as he wants.

#7 - 01/07/2004 05:28 PM - Matt Jones

In general we don't want to have the user have to type in a DN. Unfortuately, that's hard to do generically because we have several trees that have different root suffixes, so just appending dc=ecoinformatics,dc=org on the end will not work (that's how we do it now in the profile, and its too simplistic to support NRS DNs and others later as we grow).

Unfortunately, ldap authentication doesn't work for trees that aren't rooted at dc=ecoinformatics,dc=org if the DN provided is actually a referral. This is true of several LDAP trees, notably PISCO (ou=People,dc=piscoweb,dc=org) and UCNRS (ou=People,o=ucnrs.org). So...in its next incarnation Morpho needs to deal more flexibly with both profile DNs and DNs for access control lists.

One potential solution is this: User provides uid and org for both profile and ACLs, and morpho looks this up in LDAP to get a true DN back, and that is what is entered in the profile or acl field. So, for example, if a user provides this:
1) uid=mjones,o=UCNRS
Morpho would do a search like this:
2) (&(uid=mjones)(o=UCNRS)) with search base: dc=ecoinformatics,dc=org
which would return this DN:
3) uid=mjones,ou=People,o=ucnrs.org

It is this thrid (3) DN that would be used in ACLs and other places. This works because of the cross-tree referrals in place on the root server. Morpho should probably cache these DN lookups, as they'll be expensive to perform, users will largely work with a limited set of DNs repeatedly, the mappings will not change (almost never), and they'll be SOL offline if they don't have the mapping cached.

Morpho currently only talks to Metacat for this info, so we may want to add a new metacat action to support this type of lookup request.

As far as the interface goes, it would be best if the user could either type in the username/org, or browse an existing list. Browsing the list is a matter of making a tree organized by organization and maybe organizational unit. Morpho would first query for all organizations in the LDAP and display this as a collapsed tree (e.g., NCEAS, PISCO, LTER, UCNRS, SDSC, KU,...). When the user clicks on a tree, we do a search for all ou's in that subtree and display them (e.g., LTER sites). If there are no ou's, or if the user clicks on an ou, we do a query for all uids for that ou/o combination, and display the list. This allows us to present a very large list of users in a compact space and makes it so we don't have to query the whole LDAP tree at once. Again, this should probably be cached locally each time a query is run so the user can work offline. It'll change relatively slowly, but steadily, so refreshing the cache once a session, maybe in a background thread after Morpho startup, would be a good idea, and it would be good to have a UI button that says "Refresh list" so a user can trigger a new query if the user they are looking for doesn't show up.

These are just some of my background thoughts on this UI component. We need to discuss it and mock it up before we get to implementation details.

#8 - 01/30/2004 10:54 AM - Saurabh Garg

Based on the morpho discussion (Jan 29th), I will do a mookup and then go ahead with the screen.

#9 - 03/03/2004 04:36 PM - Saurabh Garg

The LDAP tree can be retrieved from metacat using getprincipal. So this url would give back a list of users entered in LDAP:
http://indus.nceas.ucsb.edu/knb-test/metacat?action=getprincipals

But there are a few things that didn't fall into place.
First is that UCNRS is not in the results that are returned from this URL. This is strange because, the web registry uses NRS as an organization name for identifying users and logging in the users using LDAP.
Second this that is strange is the NRS LDAP tree. In the previous comment, Matt mentioned that UCNRS follows following convention: ou=People,o=ucnrs.org
But when we login from registry we use dollowing DN:
o=NRS,dc=ecoinformatics,dc=org. So is there a mapping between the two trees?

Besides the above, I think result from getprincipal can be used to generate a tree. Though getting origanization name wouldn't be easy as not all trees mentioned use o=OrganizationName convention. e.g. PISCO
For that we could have the convention that first look for o=OrganizationName.
If that doesn't exsist then use first dc= to find the organization name. But I am not sure if that will be true for all.

#10 - 03/04/2004 08:25 AM - Matt Jones

Right now the UCNRS suffix in ldap is o=ucnrs.org,and there is a referral that points across the trees like this:
o=UCNRS,dc=ecoinformatics,dc=org ==> ou=People,o=ucnrs.org

So, if someone searches for a DN under the ecoinfo.org tree, they will find uids under the ucnrs.org tree. I explained how this worked in Comment #7.

The metacat operation getprincipals must be using a hardcoded root suffix set to dc=ecoinformatics,dc=org when it does its search to return the user list. It should traverse the ucnrs referral and see those entries -- I'm not sure why it doesn't. This will need to be explored. Is getprincipals returning all of the LTER and PISCO entries?

All organizations use the o=organizationName in the ecoinformatics.org tree. For example, PISCO's referral looks like this:

```
o=PISCO,dc=ecoinformatics,dc=org  ==> ou=People,dc=piscoweb,dc=org
```

So, if you stick to the ecoinfo.org tree, you'll get all of the organizations.

#11 - 03/04/2004 10:51 AM - Saurabh Garg

The entries returned were:
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=SDSC,dc=ecoinformatics,dc=org">
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=OBFS,dc=ecoinformatics,dc=org">
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=NCEAS,dc=ecoinformatics,dc=org">
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=KU,dc=ecoinformatics,dc=org">
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=LTER,dc=ecoinformatics,dc=org">
<authSystem
URI="ldap://ldap.ecoinformatics.org:389/o=unaffiliated,dc=ecoinformatics,dc=org"

So LTER entries are retunred but PISCO is not returned.

In build.properties for Metacat, the entry for ldapUrl is
ldap://ldap.ecoinformatics.org/dc=ecoinformatics,dc=org
So I guess, Metacat is using a hardcoded root suffix set to
dc=ecoinformatics,dc=org

Though I couldn't find a function in Metacat which will take uid & o as parameters and return back DN after doing a search. I guess, this is LDAP functionality which is not yet replicated in Metacat.

Finally, if o=OrganizationName will always be the case (once PISCO and NRS cases are figured out), then I guess a two level JTree can be made based on results from getprincipal. First level can contain organization name. Second level can contain username.

#12 - 04/13/2004 10:31 AM - Saurabh Garg

Morpho now has an Access screen through which you can select the ACL. It uses JTreeTable and seems to be efficient and easy to use at this point. It can be further improved in future by making it able to select multiple enteries. Assumig the present functionality is good enough for v1.5, I am changing target milestone to version 1.6 for including multiple enteries.

#13 - 04/13/2004 10:55 AM - Matt Jones

Changing milestone back to 1.5 and closing this bug to record that access control interface was developed for 1.5. Have opened new bug 1481 regarding the mutliple selections in the tree and targeted that at 1.6.

#14 - 03/27/2013 02:13 PM - Redmine Admin

Original Bugzilla ID was 88