Metacat - Bug #199

changes in Access Control mechanism

04/09/2001 01:04 PM - Matt Jones

Status:	Resolved	**Start date:**	04/09/2001
Priority:	Immediate	**Due date:**	
Assignee:	Jivka Bojilova	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	Release1.0	**Spent time:**	0.00 hour
Bugzilla-Id:	199		

Description

The "public" attribute has been elimanted form eml-access. Need to accomodate this by searching for a special "public" user who can be granted permissions. This user can be considered a group that consists of all users on the system. Also need to change mechanism for associating access rights to docids because now we need to use the triples found in the new "resource" module. There will need to be parallel changes on Morpho.

History

#1 - 05/08/2001 11:45 AM - Jivka Bojilova

1. No changes are required for "public" access. Any LDAP auth server can hold a "public" entry as a user or a group. If it's a group, users on that server can be made members of it. As a user or a group it can be granted any permissions and Metacat Auth/AC System in its current implementation can handle that. Need only probably on Metacat and Morpho INSERT, UPDATE and DELETE actions for a "public" user to be allowed. They are now suppressed. public_access attr in xml_documents can be cleared any time later.

2. Associate user with LDAP context where user belongs to. On login add "authsystem" parameter to be sent by the client along with the username and password and store it in the Session object (read it from metacat.properties as a default, if such not provided). Add "auth_system" column in xml_access for that.(The "authsystem" for a "public" user can be read from metacat.properties).
username=bojilova
password=
authsystem=ldap://dev.nceas.ucsb.edu/o=NCEAS,dc=ecoinformatics,dc=org

3. Support multiple group membership for a user on Metacat. Currently I cut them to use groups[0]. It is easy change.

4. Apply the access rights using the triples from eml-resource module.

5. Access for the package to apply for its elements also.

6. Store multiple owners of a document: submitter + ResponsibleParties with a roleCode of "owner". Create new table as xml_document_owners(docid, owner, auth_system) for that.

7. Different format of duration in eml_access. Need slight change for that.

#2 - 05/08/2001 11:47 AM - Jivka Bojilova

.

#3 - 07/17/2001 03:09 PM - Matt Jones

Jivka: looks like a good plan. Here's a few notes about the points you make...

1. Using a real group for "public" has the disadvantage that we would have to keep it up to date with all current users. This would be an onerous task. Instead, I think that metacat should treat the "public" principal as a special, virtual group -- all LDAP user's would by default be a member of the "virtual" group public, no maintenance needed.

2. I don't understand the goal of your point #2. If it is simply to

distinguish between users from different LDAP servers, I think that is best accomplished by clients passing the entire distinguished name to metacat. Metcat can then use the DN to determine the subtree for that user, and therefore which LDAP server should be used for authentication (based on a redirect in the LDAP tree). We need to make this change (pass the whole DN) in Metacat and in Morpho.

3. Multiple group membership is needed.

4. The new EML 2.0 eml-access module depends on triples to do the association. Metacat will need to read the access rules by parsing the triples first.

5. I don't understand point 5 at all.

6. Although we need to enable multiple owners for a document, I'm not convinced it needs to be in a separate table. If the submitter and all responsible parties with a role code of 'owner' are granted 'all' permission (stored in the xml_access table), then they are effectively owners. I actually think this should be the job of the client to submit an appropriate access policy, rather than have the server enforce some arbitrary rule. So, I guess I would say to leave Metacat as is, and make any needed changes in Morpho.

7. There are several new format differences in the new eml-access that will need to be accomodated.

#4 - 07/23/2001 11:04 AM - Jivka Bojilova

Leave point 5. for Release1.0. Anything else is DONE.

#5 - 09/14/2001 01:12 PM - Jivka Bojilova

DONE

#6 - 03/27/2013 02:13 PM - Redmine Admin

Original Bugzilla ID was 199