Metacat - Bug #7195

LDAP-based group authorization is failing

05/26/2017 10:44 AM - Chris Jones

Status:	Resolved	**Start date:**	05/26/2017
Priority:	Normal	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	2.8.4	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

In calls to MNRead.getSystemMetadata() where the user logged in is a member of a group, and the group is listed in the SystemMetadata.AccessPolicy with read, write, and changePermission permissions, authorization to read the private object is not allowed. In D1NodeService.getSystemMetadata(), we call isAuthorized(), which in turn calls userHasPermission(). Recent changes to this code allows for DataONE group authorization to work. However, group DNs defined in the dc=ecoinformatics,dc=org LDAP tree that are listed in the AccessPolicy and stored Metacat look to not be expanded to their individual group members when comparing DNs. On lines 1229 to 1255 of D1NodeService, we call:

```
if (accessRule.getSubjectList().contains(s)) {
    logMetacat.debug("Access rule contains subject: " + s.getValue());
    for (Permission p: accessRule.getPermissionList()) {
        logMetacat.debug("Checking permission: " + p.xmlValue());
        expandedPermissions = expandPermissions(p);
        allowed = expandedPermissions.contains(permission);
        if (allowed) {
            logMetacat.info("Permission granted: " + p.xmlValue() + " to " + s.getValue());
            break search; //label break
        }
    }
}
```

It looks like the call to accessRule.getSubjectList() is not expanding the the list of subjects if the subject DN is a group from the locally configured Metacat auth store (LDAP or file store).

An example is in the KNB: kengmiller.14.15. This object has an access rule allowing cn=snapp,o=NCEAS,dc=ecoinformatics,dc=org to r/w/chP. Members of the group can not read the object, much less modify it. Jing, I've added you to the SNAPP group for troubleshooting this.

Change userHasPermission() to correctly expand all groups, and write a unit test to exercise group-based authorization from auth file, LDAP, or DataONE group definitions.

History

#1 - 06/05/2017 01:34 PM - Jing Tao

- Status changed from New to Resolved

It turned out that the authen token doesn't include any group information. So the access rules about the group permission didn't work. In d1_libclient_java, we have the code to add the dataone groups information for the token during the the authorization, so the dataone group access control still works and I tested it.

I added code to append ldap group information during the authentication in Metacat. Then the issue has gone.