Metacat - Bug #7094

Metacat is not expanding groups in the rightsHolder field during authorization

08/26/2016 10:24 AM - Chris Jones

Status:	Closed	**Start date:**	08/26/2016
Priority:	Normal	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	2.8.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

With a SystemMetadata document like:

```
<?xml version="1.0" encoding="UTF-8"?>
<d1_v2.0:systemMetadata xmlns:d1_v2.0="http://ns.dataone.org/service/types/v2.0" xmlns:d1="http://
ns.dataone.org/service/types/v1">
  <serialVersion>0</serialVersion>
  <identifier>urn:uuid:a0f68bc4-1b67-4376-964f-70df0b58376c</identifier>
  <formatId>image/jpeg</formatId>
  <size>223220</size>
  <checksum algorithm="SHA256">60be2e67512b6f444be407a9cb87018b12e5bbf214deab3248c8d1834db8cb38</c
hecksum>
  <submitter>CN=Bryce Mecum A27576,O=Google,C=US,DC=cilogon,DC=org</submitter>
  <rightsHolder>CN=arctic-data-admins,DC=dataone,DC=org</rightsHolder>
  <accessPolicy>
    <allow>
      <subject>public</subject>
      <permission>read</permission>
    </allow>
    <allow>
      <subject>CN=Bryce Mecum A27576,O=Google,C=US,DC=cilogon,DC=org</subject>
      <permission>write</permission>
    </allow>
    <allow>
      <subject>CN=Bryce Mecum A27576,O=Google,C=US,DC=cilogon,DC=org</subject>
      <permission>read</permission>
      <permission>write</permission>
      <permission>changePermission</permission>
    </allow>
  </accessPolicy>
  <replicationPolicy replicationAllowed="true" numberReplicas="3"/>
  <archived>false</archived>
  <dateUploaded>2016-03-17T19:25:16.840+00:00</dateUploaded>
  <dateSysMetadataModified>2016-08-26T17:15:07.506+00:00</dateSysMetadataModified>
  <originMemberNode>urn:node:ARCTIC</originMemberNode>
  <authoritativeMemberNode>urn:node:ARCTIC</authoritativeMemberNode>
  <fileName>20090413_200904130059.noaa-18.4km_vis_ch1.jpeg</fileName>
</d1_v2.0:systemMetadata>
```

we would expect that anyone in the CN=arctic-data-admins,DC=dataone,DC=org group would have read/write/changePermission permissions. Updates to objects with access control like this by members of the group other than CN=Bryce Mecum A27576,O=Google,C=US,DC=cilogon,DC=org fail.

To get around this issue, I'm processing all 502K+ objects in the arcticdata.io Metacat to include:

```
    <allow>
      <subject>CN=arctic-data-admins,DC=dataone,DC=org</subject>
      <permission>read</permission>
      <permission>write</permission>
      <permission>changePermission</permission>
    </allow>
```

So, this isn't super critical, but it affects all Metacat systems, including the CNs.

History

#1 - 08/26/2016 11:19 AM - Chris Jones

- Target version set to 2.8.0

I'm targeting this for 2.8.0 since we have an immediate workaround on arcticdata.io.

#2 - 08/31/2016 03:29 PM - ben leinfelder

The docs aren't explicit about this, but I can see why you'd expect any Subject to work.
http://jenkins-1.dataone.org/jenkins/job/API%20Documentation%20-%20trunk/ws/api-documentation/build/html/apis/Types.html#Types.SystemMetadata.rightsHolder

#3 - 08/31/2016 05:48 PM - Matt Jones

I wrote those docs, which do explicitly say that RightsHolder is of Type.Subject, which is defined as "An identifier for a Person (user), Group, Organization, or System."

http://jenkins-1.dataone.org/jenkins/job/API%20Documentation%20-%20trunk/ws/api-documentation/build/html/apis/Types.html#Types.Subject

I think what happened is that our initial implementation got mixed messages from RightsHolder and Metacat's original "user_owner" field, which didn't allow groups. So, the implementation of RightsHolder as group would have been complicated, and I think it was overlooked. It would be good to fix, as the original intent in DataONE was to allow RightsHolder to be a group, and its useful to be able to do that.

#4 - 10/13/2016 02:13 PM - Jing Tao

- Status changed from New to Closed

Metacat now expands the rights holder if it is a group during the authorization check.