Member Nodes - Task #3815

MNDeployment # 3557 (Operational): LTER Network

Resolve access policy discrepancies between system metadata and science metadata

2013-06-19 16:09 - Chris Jones

Status:	Closed		**Start date:**	2013-06-19
Priority:	Normal		**Due date:**	
Assignee:	Roger Dahl		**% Done:**	100%
Category:			**Estimated time:**	0.00 hour
Target version:	Operational			
Story Points:				

Description

While working to synchronize all content on the LTER MN, I noticed an inexplicably high number (13,914) of documents that returned a NotAuthorized exception when trying to call getSystemMetadata() on the production CNs. This seemed odd since the vast majority of these documents are EML science metadata. I compared this with a select number of documents on the MN, and found that the MN, too, returns a NotAuthorized exception. However, in looking directly at some of the EML documents on disk on the CNs, there *are* public:read ACLs in the EML. For instance, for doi:10.6073/AA/knb-lter-bes.392.39, we get a NotAuthorized exception, but the EML states:

uid="BES",o=lter,dc=ecoinformatics,dc=org
all

public
read

On the CN, xml_access table includes the uid="BES",o=lter,dc=ecoinformatics,dc=org:all ACL, but not the public:read. My thought is that somewhere in Metacat's SystemMetadataFactory we've missed adding some ACLs to system metadata, but I haven't confirmed this. Nevertheless, for the documents in the file attached to this ticket, we need to iterate through them, confirm a public:read ACL in the EML, and call CNAuthorization.setAccessPolicy() to update the system metadata appropriately.

I will update this list with a complete count after re-running my query script because it encountered a number of ServiceFailure exceptions on certain pids, so I'll re-do that subset.

History

#1 - 2013-06-19 16:14 - Ben Leinfelder

It's entirely possible to change access control rules after EML has been inserted. Your example EML file is not readable by public as far as Metacat (and by extension, DataONE) is concerned:
https://tropical.lternet.edu/knb/metacat?action=read&docid=knb-lter-bes.392.39

#2 - 2013-06-19 16:25 - Chris Jones

- File deleted (lter-not-authorized.txt)

#3 - 2013-06-19 16:27 - Chris Jones

- File lter-not-authorized.txt added

- File lter-not-authorized.txt added

I've updated the NotAuthorized file, and have these pids remaining: They look to be accessible on the MN, but the CN is throwing a ServiceFailure:

knb-lter-bnz.359.13
knb-lter-bnz.360.9

knb-lter-bnz.414.9
knb-lter-bnz.453.9
knb-lter-bnz.455.5
knb-lter-cap.312.3
knb-lter-cap.334.5
knb-lter-cap.548.4

#4 - 2013-06-20 18:18 - Mark Servilla

Here is a list of the affected sites and the number of problem IDs based on the content of "lter-not-authorized.txt"; I only filtered on the canonical scope string for each site (e.g., knb-lter-lno) and ignored other odd names or those that contained "test":

and 1
arc 128
bes 13026
bnz 36
cap 0
cce 0
cdr 1
cwt 9
fce 10
gce 0
hbr 0
hfr 0
jrn 7
kbs 11
knz 0
lno 0
luq 2
mcm 23
mcr 21
ntl 2
nwt 1
pal 3
pie 0
sbc 24
sev 99
sgs 74
vcr 1

#5 - 2013-06-20 20:11 - Mark Servilla

I have shared a Google spreadsheet that contains the result of site IM queries regarding public read access:
https://docs.google.com/spreadsheet/ccc?key=0AvmNJnP7eHevdGMwcGpHRDR5RUMxNVlTc2FyZWQ4T1E&usp=sharing.

#6 - 2018-08-31 15:27 - Mark Servilla

- Status changed from New to Closed

- Assignee changed from Mark Servilla to Roger Dahl

- % Done changed from 0 to 100

The LTER MN requires a complete overhaul.

Files

lter-not-authorized.txt	468 KB	2013-06-19	Chris Jones