Metacat - Bug #6086

publish service call fails to authenticate properly

09/06/2013 04:45 PM - Matt Jones

Status:	Closed	**Start date:**	09/06/2013
Priority:	Normal	**Due date:**	
Assignee:	ben leinfelder	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	2.2.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

I was trying to issue a DOI for Sarah Olson's data set tonight via curl on the KNB using the KNB node certificate as my identity. Doing this pointed out two issues, the second of which is definitely a bug.

First error

I ran this:

```
# curl -X PUT -E /var/metacat/certs/urn_node_KNB.pem http://knb.ecoinformatics.org/knb/d1/mn/v1/publish/solson.11.5
<?xml version="1.0" encoding="UTF-8"?>
<error detailCode="1210" errorCode="401" name="InvalidToken">
    <description>No session has been provided</description>
</error>
```

That error is traced back to the beginning of MNodeService.update() where sessions are checked. Looking at ezid, I can see that the DOI was reserved successfully, but then the publish fails doing the update() on the object. I had thought that passing in the client cert was sufficient to identify myself and set up a session, but apparently not. Any thoughts on why this didn't work, and what is needed to successfully log in via curl? There may not be a bug here, but rather me using curl incorrectly. Or maybe it should work.

Second error

Also, it seems that the EZID mint() call worked even though I wasn't authenticated on metacat, so I tried the same call again without a certificate at all:

```
# curl -X PUT http://knb.ecoinformatics.org/knb/d1/mn/v1/publish/solson.11.5
```

and I got the same error. The new DOI is still reserved on the EZID system despite not being authenticated in Metacat, so there seems to be a bug here in not checking the session before contacting EZID to mint() the identifier.

History

#1 - 09/06/2013 04:46 PM - Matt Jones

- Description updated

#2 - 09/09/2013 08:22 AM - ben leinfelder

- Status changed from New to In Progress

Well, for the first issue, you cannot expect a client certificate to work if you aren't using https. If the URL in the curl command is accurate, then that'd be your "no session" error.

For generating an identifier, we are not requiring that the person be logged in. You'll see in our implementation the following note:

```
// TODO: reserve the identifier with the CN. We can only do this when
// 1) the MN is part of a CN cluster
// 2) the request is from an authenticated user
```

I think it is not unusual for someone to be doing work locally (say in Morpho) and requesting identifiers from the MN when they are not logged in yet (packaging up stuff before saving to the network) or when their MN is not actually a MN in a CN cluster yet.
And since we don't do any MN-side identifier reservations, I don't see a compelling reason to force them to authenticate before generating an identifier. EZID will give us a unique DOI each time it is called -- essentially a reservation -- so I've been assuming we can rely on that. If we'd like to

clear out old minted IDs that are not fully registered after X days, I think we could do that as well.

#3 - 09/09/2013 03:11 PM - ben leinfelder

I should also mention that you should not call publish() on the KNB until Metacat 2.1.1 is installed since there is a somewhat severe bug fixed by that patch release. See. https://projects.ecoinformatics.org/ecoinfo/issues/6057

#4 - 09/16/2013 02:34 PM - Matt Jones

Part of the issue was not running under SSL. Fixing that, the correct update() command would be:

```
# curl -X PUT -E /var/metacat/certs/urn_node_KNB.pem -F "pid=solson.11.5" -F "object=@eml.xml" -F "newPid=doi:
10.5063/F1WD3XHP" -F "sysmeta=@sysmeta-fo.xml" https://knb.ecoinformatics.org/knb/d1/mn/v1/object
<?xml version="1.0" encoding="UTF-8"?>
<error detailCode="1310" errorCode="500" name="ServiceFailure">
    <description>Error inserting or updating document: &lt;?xml version="1.0"?&gt;&lt;error&gt;User CN=urn:nod
e:KNB,DC=dataone,DC=org does not have permission to update XML Document #solson.11.5&lt;/error&gt;</descriptio
n>
</error>
```

which generates a permission error from Metacat, showing that the node cert is not being allowed to undertake the requested function. Need to fix this for update() to work as the node administrator. In general, we need the DataONE API and the Metacat API to allow the same ops by the same users, and they should include the administrators defined through both the node cert and the administrators list.

Regarding the mint() operation, I do not think it should be possible to mint() without authenticating.

#5 - 09/16/2013 03:49 PM - ben leinfelder

Added the dataone.subject to the list of metacat admins. This identity will enjoy the perks of being an admin when accessing the system via the DataONE API using the Node's client certificate.

#6 - 09/16/2013 04:34 PM - ben leinfelder

- Status changed from In Progress to Feedback

Now requiring authentication (session) to generate an identifier. Not reserving it with the CN at this point.

#7 - 10/02/2013 09:46 AM - ben leinfelder

- Status changed from Feedback to Closed