Python GMN - Bug #6868

GMN filters objects in list objects method from non-authenticated, non-rights-holder users

2015-02-24 22:17 - Mark Servilla

Status:	New	**Start date:**	2015-02-24
Priority:	Normal	**Due date:**	
Assignee:	Roger Dahl	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

The GMN filters objects when calling the listObjects REST end point (i.e., .../mn/v1/object) for users who are not rights-holders, including the PUBLIC user and those authenticated users who are not in the permitted access control list. This is true even when "PUBLIC_OBJECT_LIST = True" in GMN's settings_site.py config file; the PUBLIC_OBJECT_LIST documentation (below) clearly states the premise that only rights-holders may access the object. The only exception is the MN user and the CN of the working environment.

Discussion on dev-maintenance-standup on 24 Feb 2015 indicates that all objects should be listed regardless of ownership and access rights. It is not clear, however, that the current operation of GMN's listObjects method is incorrect since the MN API documentation (https://releases.dataone.org/online/api-documentation-v1.2.0/apis/MN_APIs.html#MNRead.listObjects) is vague on this point: "Access control for this method MUST be configured to allow calling by Coordinating Nodes and MAY be configured to allow more general access."

Enable MNRead.listObjects() for public and regular authenticated users.

#

False:

- MNRead.listObjects() can only be called by trusted infrastructure (CNs).

True:

- MNRead.listObjects() can be called by any level of user (trusted

infrastructure, authenticated and public), and results are filtered

to list only objects to which the user has access.

#

The primary means for a user to discover objects is to use the search

facilities exposed by CNs. By enabling this option, regular users can also

discover objects directly on the node by iterating over the object list. This

is disabled by default because the call can be expensive (as it must create a

filtered list of all objects on the node for each page that is returned).

These are also the reasons that DataONE specified implementation of access

control for public and regular users to be optional for this API.

History

#1 - 2016-04-14 14:19 - Mark Servilla

- Assignee changed from Mark Flynn to Roger Dahl