Metacat - Bug #2646

allow eml to specify any valid user as access constraint

11/07/2006 09:15 AM - Matt Jones

Status:	Closed	**Start date:**	11/07/2006
Priority:	Immediate	**Due date:**	
Assignee:	Michael Daigle	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	Unspecified	**Spent time:**	0.00 hour
Bugzilla-Id:	2646		

Description

Currently EML defines a flexible access control language that targets setting access rights for particular users and groups, and the public. The convention in EML for specifying public access is to use the principal 'public'. When public access is utilized, systems like metacat can not log who downloaded the resources because the user is not logged in.

Sometimes, the data owner would like to specify that any valid user can download the data, which would allow systems like metacat to require users to be logged in but allow any person with a valid account to download data and metadata. This feature would allow systems like metacat to collect the same usage information as current self-registration systems in use at fields sites (basically, a valid email, which in our case is tied to a valid LDAP account).

Implementation of this feature involves two issues:
1) Defining a convention for specifying that any valid user can access the data. This can be easily accomplished by adopting a symbolic principal name (analogous to 'public' for anonymous access) that indicates that any authenticated user is sufficient. I suggest this symbolic name be 'valid-user', which matches the similar directive in apache access configurations.
2) Modifying the metacat access control modules to recognize the 'valid-user' symbolic principal name and handle that case specially by requiring that there be a valid session for any user, rather than a particular one. This should be a relatively strightforward modification of the existing access checks.

History

#1 - 03/27/2013 02:20 PM - Redmine Admin

Original Bugzilla ID was 2646

#2 - 09/10/2013 04:19 PM - ben leinfelder

- Status changed from New to Closed

This is supported in DataONE using the access rule conventions specified there, notably, "authenticatedUser"

http://mule1.dataone.org/ArchitectureDocs-current/design/Authentication.html