

Requirements - Requirement #777

(Requirement) Authorization rules should support common permission levels

2010-08-11 07:53 - Matthew Jones

Status:	New	Start date:	
Priority:	High	Due date:	
Assignee:	Dave Vieglais	% Done:	0%
Category:	Requirement	Estimated time:	0.00 hour
Target version:			
Description			
Several types of access directives are in common use in data packages in the environmental sciences, and the authorization system should support these. The most common authorization levels would include:			
** read: the ability to display or download an object			
** write: the ability to change the content of an object through an update operation (which does not mean it actually changes the object -- it may just create a new version that obsoletes the old)			
** changePermission: the ability to change access control rules on the object			
Often, the permission levels are nested, in that higher privilege levels encompass the lower levels as well (e.g., write access to an object implies read access).			
See the EML access control module for a detailed explanation of these levels (eml-access module).			
In addition to specifying levels of permissions on the individual data objects, the authorization system should allow node administrators to specify what services principals can utilize on their nodes, and any resource constraints that may apply. For example, a Member Node operator may want to specify for their node several rules, such as:			
** user joe can insert or update objects on node 32			
** user jack can not update objects on node 21			
** user joe has an aggregate storage limit of 1TB (may want to consider soft and hard resource limits)			
** user joe has a network bandwidth transfer limit of 10mb/s			
Note that these types of node-level resource limitations may not be implemented currently on most member nodes, but the authorization system should be expressive enough to allow node operators to build in these restrictions.			