Table of Contents

Authorization in the WMS with the GACL file

In gLite 3.1 and EMI1 WMS, access control is implemented through a library provided by Gridsite, which uses a XML based file to set permissions on DN/FQAN (http://www.gridsite.org/wiki/GACL). This file is called the GACL file. For the record, the EMI2 release will support authZ based on a service, called Argus, more than a library like Gridsite is. Authorization based on Gridsite will still be possible, by configuration, but strongly discouraged. As documented in the WMS admin guide for EMI1, WMPROXY GACL , with EMI1 an exact match is required between the DN/FQAN expressed in the gacl file and the one in the user proxy. This represents a change with respect to the previous gLite 3.1 release, that allowed to express not well formed FQANS, i.e. without the leading / and with wildcards. The EMI1 WMS, instead, always required a valid FQAN, that in turn does not foresee wildcards in its syntax. So, for example, while in gLite 3.1 WMS the following GACL file would have been enough to grant access to all CMS users, indistinctively:

cms/*

cms

With EMI1 WMS each single group and role has to be specifed manually. For example, the previous file would become:

/cms/Role=NULL /cms/Role=cmsprod /cms/Role=admin /cms

For VO CMS and its following roles:

/cms/Role=cmsprod

/cms/Role=cmssoft

/cms/Role=cmst1admin

The GACL file is rarely edited by the admins, as it gets generated by yaim starting from file groups.conf. The groups.conf attached in this twiki comprises all the possibile combinations of existing groups/roles for some VOs as of today. Each time a new group is created, this file must be edited to include all the combinations for this group and all the possibile existing roles; then, yaim must be re-run. If, for example, a new group 'team' is created in VO 'foo', here are the lines that should be added to the group.conf file:

"/foo/team"::::

"/foo/team/ROLE=pilot"::::

"/foo/team/ROLE=production"::::

"/foo/team/ROLE=lcgadmin"::::

before re-running yaim. If a new role is introduced (this should be even more rare) it must be added for each existing group. For example:

"/foo/oldteam"::::

"/foo/oldteam/ROLE=pilot"::::

"/foo/oldteam/ROLE=production"::::

"/foo/oldteam/ROLE=lcgadmin"::::

"/foo/oldteam/ROLE=newrole"::::

"/foo/newteam"::::

"/foo/newteam/ROLE=pilot"::::

"/foo/newteam/ROLE=production"::::

"/foo/newteam/ROLE=lcgadmin"::::

"/foo/newteam/ROLE=newrole"::::

-- MarcoCecchi - 2012-02-14

This topic: WMS > EMI1_GACL
Topic revision: r1 - 2012-02-14 - MarcoCecchi