Differences in GACL based authorization in gLite and EMI WMS

In gLite and EMI WMS releases (latest gLite version is 3.2.15, aka update 67, EMI versions are 3.3.0 - 3.3.4), access control is implemented through a library provided by Gridsite, which uses a XML based file to set permissions on DN/FQAN. This file is called the GACL file: http://www.gridsite.org/wiki/GACL . As documented in the WMS admin guide, 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 releases, that allowed to express not well formed FQANs, i.e. without the leading / and with wildcards. The EMI1 WMS, instead, always requires 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:

```
<entry><voms><fqan>cms/*</fqan></voms><allow><exec/></allow></entry>

<entry><voms><fqan>cms</fqan></voms><allow><exec/></allow></entry>
```

With EMI1 WMS each single group and role has to be specifed manually. For example, for VO CMS and its following roles:

/cms/Role=cmsprod

/cms/Role=cmssoft

/cms/Role=cmst1admin

the previous file would become (note the leading slash in the FQAN):

```
<entry><voms><fqan>/cms/Role=NULL</fqan></voms><allow><exec/></allow></entry>

<entry><voms><fqan>/cms/Role=cmsprod</fqan></voms><allow><exec/></allow></entry>

<entry><voms><fqan>/cms/Role=admin</fqan></voms><allow><exec/></allow></entry>

<entry><voms><fqan>/cms</fqan></voms><allow><exec/></allow></entry>
```

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 a significant number of VOs, as of Feb, 14th, 2012. Each time a new group is created, this file must be edited to include all the possibile combinations for this group and all the existing roles; then, yaim must be re-run so that it recreates the GACL file. As an example, if a new group 'team' is created in VO 'foo', here are the lines to be added to the group.conf file before re-running yaim, supposed that only three roles exist (pilot, production, lcgadmin):

"/foo/team"::::

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

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

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

If a new role is introduced (this should be even more rare), then 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"::::

For the record, the EMI2 releases (starting from WMS version 3.4.0, yet to be finalized), will support authorization 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.

-- MarcoCecchi - 2012-02-14

This topic: WMS > EMI_Gridsite_GACL
Topic revision: r2 - 2012-02-14 - MarcoCecchi

Copyright © 2008-2020 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? Send feedback