

Table of Contents

How to switch to pool accounts for sgm/prd users.....	1
YAIM users.conf format.....	1
Caveats.....	1

How to switch to pool accounts for sgm/prd users

With `glite-yaim-3.0.1-22` and later it is possible to keep mapping `sgm` and/or `prd` users to *static* accounts, or to map either class of users to its own set of *pool* accounts. This can be decided per VO and per user class. There are 2 node types that still enforce static accounts by necessity: the `VOBOX` and the `SE_castor`. On those nodes one should keep the old static accounts instead of the new pool accounts.

Pool accounts are preferred for at least 2 reasons:

- Their audit trails are better defined.
- They allow batch systems to give fair shares to the individual users in a class.

On any service node the mappings should only be changed when the node is in scheduled maintenance and has been drained sufficiently. For example, a CE, RB or WMS should typically be given a week for its unfinished jobs to drain. The exact period depends on the number of unfinished jobs and the agreements with the relevant VOs: sometimes it is acceptable for a number of jobs to be lost.

YAIM users.conf format

Static `sgm/prd` accounts have lines like these:

```
33333:dteamprd:2688:dteam:dteam:prd:
18946:dteamsgm:2688:dteam:dteam:sgm:
```

`Sgm/prd` pool accounts have lines like these:

```
50501:prddtm01:2689,2688:dteamprd,dteam:dteam:prd
[...]
50519:prddtm19:2689,2688:dteamprd,dteam:dteam:prd
60501:sgmdtm01:2690,2688:dteamsgm,dteam:dteam:sgm
[...]
60559:sgmdtm59:2690,2688:dteamsgm,dteam:dteam:sgm
```

YAIM will detect the situation per VO and per user class.

NOTE: include *either* static *or* pool accounts (per VO, per user class), *not* both.

This is further explained in the YAIM documentation.

Caveats

- A site should only switch to *sgm pool accounts* for VOs which have confirmed that their software installation procedures have been adapted to such pool accounts. VOs should add the following logic to their software installation procedures: if the account running the installation happens to be an *sgm pool account*, then make all the newly installed files and directories group-writable. For example:

```
case `whoami` in
*[0-9])
    chmod -R g+w $new_stuff
esac
```

- Due to a bug in YAIM, `/opt/edg/var/info/$VO/$VO.list` on the CE will have the wrong mode, thereby preventing the `lcg-ManageVOTags` and `lcg-tags` commands from updating the list of VO

SgmPrdPoolAccounts < LCG < TWiki

software tags published in the information system. Work-around:

```
chmod 664 /opt/edg/var/info/*/*.list
```

This should only be done for VOs with *sgm pool accounts*.

- The `sgm` and `prd` pool account *prefixes* must **not** be extensions of the prefix for ordinary pool accounts, otherwise the LCG-CE will use the new accounts also for ordinary users. For example, if for a VO `test` the accounts for ordinary users are `test001 ... test199`, the `sgm` accounts must **not** be named `testsgm001` etc. because `testsgm` is an extension of `test`. Instead, they could be named `sgmst01 ... sgmst99` and the `prd` accounts `prdst01 ... prdst99`. It is advised to keep account names at most 8 characters long, otherwise utilities like `ps` will print UIDs instead of names, which may upset other tools or daemons.
- In principle the *number* of `sgm` and `prd` accounts should be much lower than the number of ordinary accounts for a VO, but for some VOs the current practice is different. The minimum number of `sgm` and `prd` accounts needed per VO can be determined like this:

```
awk '$NF ~ /(prd|sgm)$/ { print $NF }' /etc/grid-security/grid-mapfile |  
sort | uniq -c
```

This assumes the static `sgm` and `prd` accounts have names ending in `sgm` and `prd` respectively. For the LHC VOs the current numbers are:

```
3 aliceprd  
38 alicesgm  
44 atlasprd  
31 atlasgm  
56 cmsprd  
33 cmssgm  
16 dteamprd  
48 dteamsgm  
22 lhcbprd  
2 lhcbgm
```

Per mapping we suggest creating more accounts than the current value, to be on the safe side. Unused pool accounts will be recycled as needed, but ideally they should not. It is a good idea to check (via e.g. a cron job) periodically what fraction of the pool accounts are used, and send a mail when they are almost used up, e.g.:

```
Group(s) running out of available pool accounts:  
prlhcb : 23/ 25
```

The standard cron job `/etc/cron.d/lcg-expiregridmapdir` shows the current state of the pool accounts in `/var/log/lcg-expiregridmapdir.log`. For example:

```
VO alice: inuse / total = 9 / 199 = 0.05, thr = 0.8  
VO atlas: inuse / total = 153 / 199 = 0.77, thr = 0.8  
VO prdatl: inuse / total = 5 / 99 = 0.05, thr = 0.8  
VO cms: inuse / total = 153 / 199 = 0.77, thr = 0.8  
VO dteam: inuse / total = 73 / 99 = 0.74, thr = 0.8  
VO sgmdtm: inuse / total = 19 / 99 = 0.19, thr = 0.8  
VO lhcb: inuse / total = 110 / 199 = 0.55, thr = 0.8
```

SgmPrdPoolAccounts < LCG < TWiki

Ideally the usage stays far below the threshold at which the least recently used accounts start being recycled.

-- MaartenLitmaath - 12 Aug 2007

This topic: LCG > SgmPrdPoolAccounts

Topic revision: r4 - 2007-08-23 - MaartenLitmaath



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