Workspace and Submit Access Control Through Groups

When you get a new hub, by default everyone gets a workspace and can submit jobs to your attached cluster(s). This means that the user can run many different commands both on your hub and on your clusters, in addition to the software applications your hub provides.

For some sites, this causes security issues, so you may wish to limit access to the software the user can execute and the clusters he or she can submit jobs too. Usually only tool developers need workspace access.

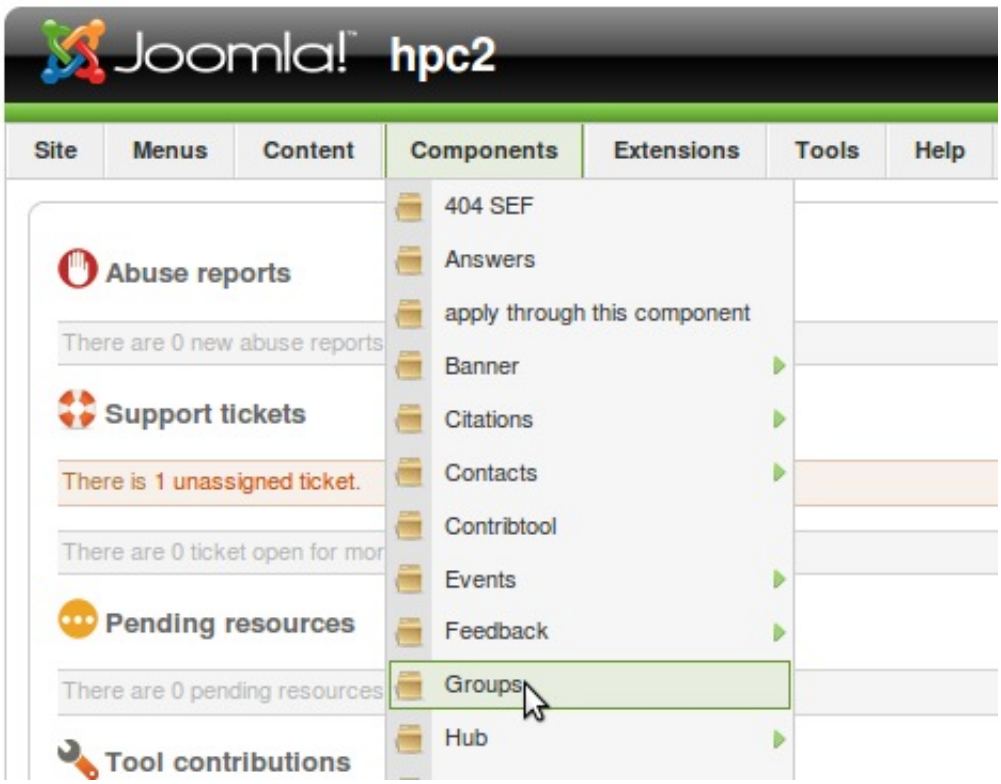
Limiting Workspace Access

The first thing to do is to ask HUBzero staff to **change the default to not provide workspace** access**.**

The user will still be able to run portal applications and pick up their output files by sftp or webdav.

Then, to give users a workspace:

- login to the Joomla interface
- select Components/Groups



- locate the app-workspace (Workspace Development) group, click Total Members
- add users as appropriate

Limiting Submit Access

There are several aspects to submit access control.

1. Allow a user run a HUB application that gets submitted as a job to a cluster.
2. Allow a user run standard unix and shell commands as jobs submitted to a cluster, even something as simple as **echo hello**
3. Allow a user stage his or her own executable to a cluster and run it.

Getting Started

To set access control, you will need to be a member of the group name *apps*. Membership will give you write permissions on the files */opt/submit/sites.dat* and */opt/submit/tools.dat* and on your HUB. You can add yourself through the Joomla interface as described above. It can take a day before the change propagates through the system.

It is a good default to limit the user to running HUB applications. To limit a user to only running HUB applications, ask the submit rules be tightened so that if a user is not in group submit they can **only run staged applications or executables from */apps/***. These executables are under control of group *apps* thus providing some oversight for the application code.

To limit the clusters a user can run on

Whether running submit from a workspace or HUB applications, you may want to limit the supercomputing sites that a user can run on. You first need to create a group for each cluster. For example, the hpc2.org HUB has three groups: *ccr* (Center for Computational Research), *ccni* (Computational Center for Nanotechnology Innovations) and *sbbnl* (Stony Brook/Brookhaven National Lab).

Next, edit sites.dat

For each cluster, add a line to restrict use of the application to the site group associated with the cluster with **restricted**ToGroups **= groupname**, e.g.

```
u2-grid
venues = u2-grid.ccr.buffalo.edu
remotePpn = 2
remoteBatchSystem = PBS
remoteUser = hpc2
remoteManager = mpi
venueMechanism = ssh
remoteScratchDirectory = /san/scratch/grid/grid-tmp/grid-
```

```
data/hpc2/hpc2jobs/
siteMonitorDesignator = u2-grid
arbitraryExecutableAllowed = False
checkProbeResult = False
restrictedToGroups = ccr
```

Then you can invite the user to join groups for clusters on which she'll be able to run applications.

To limit where the user can run a specific application

An application may be run at more than one site, but you wish to direct a user's run to one particular site.

You will need to edit */opt/submit/tools.dat* to set each execution to match one site. Below is an example. If the user is in group *ccni*, lammps will run on ccni's opteron cluster. If the user is in group *ccr*, lammps will run on ccr's cluster.

```
lammps
destinations = u2-grid
executablePath = lmp_linux
remoteManager = u2-grid_lammps
restrictedToGroups = ccr

lammps
destinations = rpi-opteron
executablePath = ${HOME}/apps/lammps/bin/lmp_opteron
remoteManager = rpi-opteron_lammps
restrictedToGroups = ccni
```

To prevent a user from running arbitrary shell commands on a cluster through submit

Users who have a workspace can submit jobs to clusters. Ask the HUB staff to tighten the range of submit jobs so restrictions by user or group can be specified for sites as well as tools. (The keywords and parameters will be specified in sites.dat in the same fashion as tools.dat.)

Open the file */opt/submit/sites.dat* on your HUB. For each cluster name, add or change the setting **arbitrary**ExecutableAllowed to **False**.

Then you can add users who have a workspace to the group *submit*.