Security: How can I prevent users from seeing processes that do not belong to them?

Unix-like systems such as Solaris and FreeBSD provide kernel facilities that limit the information that a user can obtain about the processes run by other users. Linux does this too, as of kernel 3.2.20 [1]. With this, a system administrator is able to restrict users to view only their own processes. You can also permit specific groups access to view all processes, which can be handy for system administrators. The restriction feature has already been pushed back into the kernel for Red Hat Enterprise Linux 6.3 [2], and from there to CentOS 6.3 and Scientific Linux 6.3. Recently, this feature was also backported to RHEL 5.9 [3].

If you are using Bright Cluster Manager version 6.0 and above, and you run it on one of these distributions, then all you have to do to make this security feature available is to:

- change the mount options of the `/proc` filesystem
- remount proc on all the nodes.

The settings take effect right away on the node or node category.

Example: Assume that the head node is called `darkstar-head`. Assume we have a category `default`. This category has the processing nodes, ie the nodes on which you want to restrict the ability users to view others' processes

```
[root@darkstar-head ~]# cmsh
[darkstar-head]% category
[darkstar-head->category]% use default
[darkstar-head->category[default]]% fsmounts
[darkstar-head->category[default]->fsmounts]% use /proc
[darkstar-head->category[default]->fsmounts[/proc]]% set mountoptions
defaults,nosuid,hidepid=2
[darkstar-head->category*[default*]->fsmounts*[/proc*]]% commit
[darkstar-head->category[default]->fsmounts[/proc]]% quit
[root@darkstar-head ~]#
```

The *hidepid* option accepts three values:

- 0 (zero) sets the */proc* filesystem to the default configuration. This allows a user to view all processes on the system.
- 1 (one) allows a user to access only the */proc/[PID]* directories that the user owns. PID directories under /proc that do not belong to the user are restricted.
- 2 restricts the user from viewing all PIDs, including all under */proc*.

(c) 2019 Bright Computing <kb@brightcomputing.com> | 2019-12-12 14:44
URL: https://kb.brightcomputing.com/faq/index.php?action=artikel&cat=22&id=109&artlang=en

Security: How can I prevent users from seeing processes that do not belong to them?

After you enter the `commit` command, the changes go into the node fstab files. The changes will take effect during the next reboot. However, if you need the changes to take effect immediately, you will have to `ro` remount the `/proc` filesystem on all the nodes. You can do this by running the `pexec` command on the head node.

pexec "mount -o rw,hidepid=2,remount /proc"
Finding nodes that are alive...
Running pexec.

---
node001: Working directory: /root
---
node002: Working directory: /root

Finally, if you have multiple system administrators on the system and you want to permit them to see all processes on the system for troubleshooting, you can add the `gid` option, to specify a group ID that is permitted to view all process on the system regardless of the `hidepid` option.

...[darkstar-head->category[default]->fsmounts[/proc]]% set mountoptions defaults,nosuid,hidepid=2,gid=100...

Unique solution ID: #1108
Author: Panos Labropoulos
Last update: 2014-08-12 11:06

(c) 2019 Bright Computing <kb@brightcomputing.com> | 2019-12-12 14:44
URL: https://kb.brightcomputing.com/faq/index.php?action=artikel&cat=22&id=109&artlang=en