Table Of Contents

Table Of Contents 1
Step # 1: Create and Maintain a Group For All Authorized Users 2
Step #2: Restrict Access 2
Disable the file permission for others 2
Step # 3: Test It 2
A Note About ACL and SELinux 3
Recommend readings: 3

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Linux / UNIX: Restrict Access To A Given Command

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

How do I restrict access to a given command for instance /opt/apps/start, to authorized users only under Linux / UNIX / BSD operating system?

You need to use traditional Unix groups concept to enhance security including restricted access to a given command.

Step # 1: Create and Maintain a Group For All Authorized Users

[2]

Create a group named appsonly:

```
# groupadd appsonly
```

Add all authorized users to appsonly:

```
# usermod -aG {groupName} {userName}
# usermod -aG appsonly tom
# usermod -aG appsonly jerry
# id jerry
```

Where,

1. -a : Add the user to the supplemental group(s) i.e. appends the user to the current supplementary group list.
2. -G : A list of supplementary groups which the user is also a member of.

Step #2: Restrict Access

Now a group of user had been created. Next, use the **chgrp command** to change the group of /opt/apps/start to appsonly group:

```
# chgrp {groupName} {/path/to/command}
# chgrp appsonly /opt/apps/start
```

Disable the file permission for others

Finally, use the **chmod command** to change file permission as follows:

```
# chmod 750 /path/to/command
# chmod 750 /opt/apps/start
```

You can also apply permissions to directory (this will disable ls command access to others) :

```
# chgrp appsonly /opt/apps
# chmod 0640 /opt/apps
```

Step # 3: Test It

su to tom, enter:

```
# su - tom
$ id
$ /opt/apps/start
$ exit
```

su to vivek (not a member of appsonly group), enter:

```
# su - vivek
$ id
$ /opt/apps/start
```

Sample outputs:

```
bash: /opt/apps/start: Permission denied
```

A Note About ACL and SELinux

The access control policies which can be enforced by chmod, chgrp, and usermod commands are limited, and configuring SELinux and fille system ACLs (access control list) is a better and recommend option for large deployments.

Recommend readings:

- man page chgrp, groupadd, useradd, usermod, passwd [3], and group [4] file.

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/linux/**
[2] Image: **http://www.cyberciti.biz/faq/category/unix/**
[3] passwd: **http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/**
[4] group: **http://www.cyberciti.biz/faq/understanding-etcgroup-file/**