Restrict SSH Access for User with LShell (Limited Shell)

LShell or Limited Shell is written in python for limiting user for specific set of commands and directories. You can create user environment with limited access, you can also enable disable commands over SSH access.

Install Limitet Shell:

- **Install Lshell on CentOS / RHEL 7:**

```
# yum update
# yum install lshell
```

- **Install Lshell on Debian / Ubuntu:**

```
# apt-get update
# apt-get install lshell
```

Switch User to LShell

Now set the LShell as default shell for users for which you are required. For example to change the shell of user sarah.

```
# chsh sarah
```

```
Changing the login shell for sarah
Enter the new value, or press ENTER for the default
    Login Shell [/bin/lshell]: /usr/bin/lshell
```

You may also set the lshell as default shell for user during creation of user account as following.

```
# adduser --shell /usr/bin/lshell raj
```

Configure LShell

Now start with the configuration of lshell. Edit lshell configuration file **/etc/lshell.conf**. There are 4 basic sections in configuration file.

- **[global] :** In this section we defines the settings which applied globally. For example logs.
- **[default] :** In this section we set default values which applied all users and groups. The settings of this section can be overridden with user and group specific settings.
- **[USERNAME] :** In this section we specify user specific settings. This section settings applied to user only
- **[grp:GROUPNAME] :** In this section we specify group specific settings. This section settings applied to all users of group

A **[default]** profile is applied for all users using lshell. You can create **[username]** section or a group **[grp:groupname]** section to customize users and group specific preferences.

The priority order is **User** » **Group** » **Default**. User section has highest priority and Default has lowest priority.

```
[global]
logpath         : /var/log/lshell/
loglevel        : 2

[default]
allowed         : ['ls','pwd','cd','cat','cp']
forbidden       : [';', '&', '|','`','>','<', '$(', '${']
sudo_commands   : ['ls', 'more']
warning_counter : 2
aliases         : {'ll':'ls -l', 'vim':'rvim'}
prompt          : "%u@%h"
timer           : 0
path            : ['/home', '/usr']
env_path        : ':/usr/bin/usr/local/bin'
env_vars        : {'foo':1, 'bar':'helloworld'}
scp             : 1 # or 0
sftp            : 1 # or 0
overssh         : ['rsync','ls']
strict          : 0
history_file    : "/home/%u/.lshell_history"

[grp:wheel]
warning_counter : 5
overssh         : - ['ls']

[raj]
allowed         : 'all' - ['su','rm','mv']
path            : ['/etc', '/usr'] - ['/usr/local']
home_path       : '/home/raj'

[sarah]
allowed         : + ['ping'] - ['ls']
path            : - ['/usr/local']
strict          : 1
scpforce        : '/home/sarah/uploads/'
```

For example User ‘rja’ and user ‘sarah’ both belong to the ‘wheel’ UNIX group:

Group wheel:

- Users of wheel group has a warning counter set to 5
- Users of wheel group is not allowed ‘ls’ command.

User raj:

- Can access /etc and /var but not /usr/local
- Can access all commands in his PATH execpt commands – su, rm, vm
- has a warning counter set to 5 [default]
- has his home path set to ‘/home/raj’

User sarah:

- Can access /home and /usr but not /usr/local
- is allowed default command ‘ping’ but not ‘ls’
- strictness is set to 1 (he is not allowed to type an unknown command)

Quelle: https://tecadmin.net/how-to-limit-user-access-with-lshell-limited-shell/#

Last update: **2019/03/07 14:01**