

## ENHANCED USER SECURITY WITH SUDO

SUDO:

- > Sudo stands for either "substitute user do" or "super user do" (depending upon how you want to look at it).
- Users can login using their username and password and can issue administrative commands placing sudo in front of the commands, e.g. `sudo rpm -Uvh *.rpm`, to run the command which installs and updates programs in Linux (rpm).
- ➔ The file `/etc/sudoers` file has the rules that users have to follow when using sudo command. That means that whatever commands access is provided to any user in `/etc/sudoers` file, that user can only run those commands.
- ➔ Do not edit the `/etc/sudoers` directly; instead use "visudo" command to edit the sudoers file. There are two reasons for that- it prevents two users from editing the file at the same time, and it also provides limited syntax checking. Even if you are the only root user, you need the syntax checking, so use "visudo".
- ➔ All commands executed by sudo users will be stored in `/var/log/secure` file, but still if you want you can make your own log file by passing an entry in `/etc/sudoers` file at the bottom as "Defaults logfile=/var/log/sudo.log" or whatever name you want, to save the logs of what commands is executed by which sudo user.
- ➔ `root ALL=(ALL) ALL`
- ➔ This line means that the user root can execute from ALL terminals, acting as ALL (any) users, and run ALL (any) command.
- ➔ So the first part is the user, the second is the terminal from where the user can use sudo, the third is as which user he may act, and the last one, is which commands he may run.
- ➔ The advantage of visudo command, while editing if there are any syntax error it will be reflected as follows

```
[root@master-server tmp]# visudo
>>> /etc/sudoers: syntax error near line 117 <<<
>>> /etc/sudoers: syntax error near line 118 <<<
>>> /etc/sudoers: syntax error near line 119 <<<
>>> /etc/sudoers: syntax error near line 120 <<<
>>> /etc/sudoers: syntax error near line 121 <<<
>>> /etc/sudoers: syntax error near line 122 <<<
>>> /etc/sudoers: syntax error near line 123 <<<
>>> /etc/sudoers: syntax error near line 124 <<<
>>> /etc/sudoers: syntax error near line 125 <<<
>>> /etc/sudoers: syntax error near line 126 <<<
>>> /etc/sudoers: syntax error near line 127 <<<
>>> /etc/sudoers: syntax error near line 128 <<<
```

- ➔ What now?
- ➔ **Note:** Always take backup before doing any changes in sudoers file

root@master-server:/tmp

```
[root@master-server tmp]# tail -1 /etc/sudoers
yallareddy ALL=(ALL)      ALL
[root@master-server tmp]#
```

- 
- Note: If you don't want to give password every time then you can give entry like
- Yallareddy ALL=(ALL) NOPASSWD:ALL
- Allow a user "yallareddy" all privileges like root
- Now logged in as "yallareddy" and run admin commands like fdisk -l etc

yallareddy@master-server:~

```
[yallareddy@master-server ~]$ fdisk /dev/sda
```

```
Unable to open /dev/sda
```

```
[yallareddy@master-server ~]$ sudo fdisk /dev/sda
```

```
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
```

```
Command (m for help):
```

=====End sudo