

## How to Use the “sudo” Command to Help Ensure Secure Linux System Administration

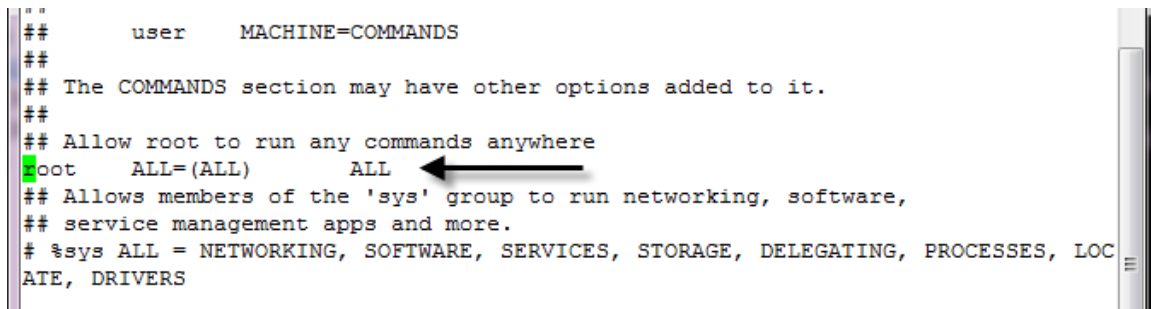
**By Don R. Crawley, author of “The Accidental Administrator: Linux Server Step-by-Step Configuration Guide”**

Seattle, WA. November 9, 2011--Most Linux and Unix system administrators know that best practice is to have two user accounts for the administrator. One account is used for daily use and the “root” (or superuser) account is used only when needed for administrative purposes. You can use the switch user command (su) to work as root, but doing so means that you have probably opened a terminal window and are executing all commands as root, whether needed or not. It can also be easy to forget to exit back to your regular user account, thus exposing your system to potential security issues.

An alternative to working as “root” is the use of “sudo” when administering a Linux or Unix system. Sudo is similar to “runas” in Windows. It allows you to execute specific commands under root context without leaving your regular user profile or context.

To use sudo, you preface the command you wish to run with the word “sudo”. For example, if you want to run the command “ifconfig”, you would enter it as “sudo ifconfig”. If your account is allowed to run that command, it would then execute. Otherwise, you would receive an error.

The use of sudo requires modifying /etc/sudoers, but you can’t just open the file in a text editor as you would normally. In order to modify /etc/sudoers, you must use the command “visudo” as root. When you execute visudo, an editor window appears similar to this:



```
##
##      user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)    ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS
```

Figure 1 Output from the “visudo” command

Notice the line: “root ALL=(ALL) ALL”. That statement gives root permission to run from any terminal (the first ALL), acting as any user (the second ALL), and execute any command (the third ALL).

Suppose you wanted to give the user `donc` the ability to run `ifconfig`. You would add the following line to /etc/sudoers (using visudo, of course):

```
donc ALL=/sbin/ifconfig
```

That gives user donc the ability to run ifconfig from any terminal, but in order to do so, he would enter the command as follows:

```
sudo ifconfig
```

You might want to give your personal user account the ability to run any command (similar to an Ubuntu system) by entering the following statement in /etc/sudoers (obviously, you would change “donc” to your name):

```
donc ALL=ALL
```

There are many other options available, including the ability to use aliases to group users. For more information, see man sudoers.

The above article is an excerpt from [The Accidental Administrator: Linux Server Step-by-Step Configuration Guide](http://amzn.com/1453689923) (http://amzn.com/1453689923) by Don R. Crawley, available in Kindle edition from Amazon and in paperback from Amazon and other channels.

A companion video is available at <http://youtu.be/imnEUvvDxc4>

Interviews and review copies available on request.

**The Accidental Administrator: Linux Server Step-by-Step Configuration Guide**

<http://amzn.com/1453689923>

List \$40.00

188 pages trade softcover

ISBN: 978-1453689929

Also available in Kindle edition.

### *About the author:*

Don R. Crawley is president/chief technologist at soundtraining.net (www.soundtraining.net), the Seattle-based I.T. training firm and an author and speaker for the I.T. industry. He is the author of numerous books and hundreds of articles on information systems and technology topics including Cisco, Linux, and customer service for I.T. professionals.

This article may be freely reprinted and distributed with a reference box including the name, website, phone and email of the author, please.

Accompanying graphic images are available upon request.

Contact: Don R. Crawley (206) 988-5858 or email [don@soundtraining.net](mailto:don@soundtraining.net)