SUDO - GRANULAR CONTROL

In a perfect world, each place where IT people work would have enough staff, but more importantly enough staff who are competent and are not malicious. Unfortunately, we do not live in a perfect world, we live in the world where we are short-staffed and under-trained. This means that very often we have to enlist the help of those who may not be entirely competent for the job, in order to do our jobs. Common examples are when we need to delegate backup duties to operator staff, or user administration of an email server to a supervisor, or many other possibilities. The problem here is that good administrators are paranoid, all of the above mentioned examples generally involve the delegated person having to run certain commands or operations with a high degree of access. Paranoid people try to only give people the rights they need, this is where the problem arises. *Sudo* is a program used to try to solve that problem. It can be used to allow certain people to run specific commands only. Therefore when you delegate tasks, all you do is delegate certain commands and nothing more. This article will cover the basics of getting this functionality working.

What do I need?
Obviously you need the *sudo* software, if it was not installed when you set your server up then you can get it from the software's homepage. The two main commands you will be using -which should now be available- are *visudo* and *sudo*. You will now also have your configuration file (generally */etc/sudoers*), this is where you setup your delegation using the *visudo* command. Remember that you can only use *visudo* to make changes to the sudo configuration file, nothing else will work.

Configuration
When you run visudo for the first time you will probably see something similar to (by the way never remove the line "*root   ALL=(ALL) ALL*" as it needs to be there);

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# Defaults specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
# Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
```

Lets go through some of the basic sections that used in most setups..

- *User Section*
  This where you can setup groups for the users you will specify commands for. Lets setup an Operations group;

User_Alias OPS = bob, jdoe

This creates the *OPS* group and puts the users named *bob* and *jdoe* into the group

- *Cmnd_Alias*
  Here we specify specific command sets. You must specify the full path and any command options you want used. Lets setup the Operations group commands;
  Cmnd_Alias OPSCMD = /admin/bin/srvbkup, /admin/bin/test
  This adds the three specified commands to the command group *OPSCMD*.

- *User Privilege Specification*
  This is where we will use the groups we have setup so far;
  OPS ALL=(root) OPSCMD
  First thing we specify are the users, here we use the *OPS* group we setup. Then the *ALL* means that it applies to all servers, this is useful only if you or running *sudo* over multiple servers each using the same configuration file. Next we specify the user that the *Operations* group will run the specified commands as, in this case we want them to run as *root*. Lastly we specify the commands that we want the *OPS* group to be able to run, specifically we are using *OPSCMD* group we setup. If you did not want them to enter their password each time they used *sudo*, then the command specification would rather be *NOPASSWD: OPSCMD*.

SUDO in Action

Now that we have setup what we need lets see it in action..

```
[bob@syplh bob]$ id
uid=530(bob) gid=5001(bob) groups=5001(bob)
[bob@syplh bob]$ ls -l /admin/bin/test
-rwx------    1 root     root           15 Feb 24 19:42 /admin/bin/test
[bob@syplh bob]$ /admin/bin/test
-bash: /admin/bin/test: Permission denied
[bob@syplh bob]$ sudo /admin/bin/test
Password:
test
uid=0(root) gid=0(root) groups=0(root)
[bob@syplh bob]$ id
uid=530(bob) gid=5001(bob) groups=5001(bob)
[bob@syplh bob]$
```

As you can see, bob could not run */admin/bin/test*, but using *sudo* he could. This is the benefit of using *sudo*.

Final Thoughts

Sudo is a great tool, and can be very useful. One warning note though, be very careful with how you use it, be very careful to not allow unrestricted access to potentially dangerous commands, like the *passwd* command. As long as you use it carefully, *sudo* can save you a lot of trouble, have fun and learn.