visudo

The visudo command allows you to make changes to the /etc/sudoers file by opening the file in a text editor and checking your changes for syntax. Run the command with “sudo visudo” and make sure that you understand the syntax. Privileges can be assigned by user or by group. On most Linux systems, the /etc/sudoers file will already be configured with groups like those shown below that allow the privileges to be assigned to groups set up in the /etc/group file. In those cases, you don’t need to use the visudo command at all – just be familiar with the groups that bestow root privileges in this way, and make your updates to the /etc/group file.

%admin ALL=(ALL) ALL

%sudo ALL=(ALL:ALL) ALL

%wheel ALL=(ALL:ALL) ALL

Note that group names are preceded by the % sign.

You can probably display the group providing sudo access in your /etc/group file like this since it is probably one of these:

$ egrep "admin|sudo|wheel" /etc/group

sudo:x:27:shs,jdoe

The easiest way to give someone sudo privilege is to add them to the empowered group in /etc/group. However, that means that they can run any command as root. If you want some users to have root authority for a limited set of commands (e.g., adding and removing accounts) you can define the commands you want them to be able to run through a command alias like this:

Cmnd_Alias ACCT_CMDS = /usr/sbin/adduser, /usr/sbin/deluser

Then give the user or group the ability to run these commands using sudo with a command like one of these:

nemo ALL=(ALL) ACCT_CMDS

%techs ALL=(ALL:ALL) ACCT_CMDS

The first line allows the user "nemo" to run the twp (adduser and deluser) commands with sudo while the second assigns the same privileges to anyone in the "tech" group in the /etc/group file.

To check & update the security patches in Centos run the below command but internet connection is required.

yum updateinfo list security all [To check the available all security updatesl]

#yum updateinfo list serurity installed [To check the installed security patches]

yum -y update --security [To installed all available security patches]

yum update-minimal --security -y [To only install the packages that have a security errata use]

man yum-security [For more commands consult the manual pages of yum-security with]

Note : you will be able to run these commands with yum "updateinfo" when you have installed "yum install yum-plugin-security" on centOS 6.

If it is already installed check with rpm command

#rpm -qa |grep 'yum-plugin-security'

if it is already there you can install & check the security updates.

Controlling and managing services

Previous versions of Red Hat Enterprise Linux, which were distributed with SysV init or Upstart, used *init scripts* located in the `/etc/rc.d/init.d/` directory. These init scripts were typically written in Bash, and allowed the system administrator to control the state of services and daemons in their system. In Red Hat Enterprise Linux 7, these init scripts have been replaced with *service units*.

Service units end with the `.service` file extension and serve a similar purpose as init scripts. To view, start, stop, restart, enable, or disable system services, use the `systemctl` command

Service	systemctl	Description
`service name start`	`systemctl start name.service`	Starts a service.
`service name stop`	`systemctl stop name.service`	Stops a service.
`service name restart`	`systemctl restart name.service`	Restarts a service.
`service name`condrestart	`systemctl try-restart name.service`	Restarts a service only if it is running.
`service name reload`	`systemctl reload name.service`	Reloads configuration.
`service name status`	`systemctl status name.service` `systemctl is-active name.service`	Checks if a service is running.
`service --status-all`	`systemctl list-units --type service --all`	Displays the status of all services.

User administration of user

Creating a user with a default setting: A user can be added by running the *useradd*command at the command prompt. After creating the user, set a password using the
passwd utility, as follows:

```
[root@localhost bhargab]# useradd user1
[root@localhost bhargab]# passwd user1
Changing password for user anirban.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

The system automatically assigns a UID, creates the home directory (*/home/<username>*) and sets the default shell to */bin/bash*.
The *useradd* command creates a user private group whenever a new user is added to the system and names the group after the user.