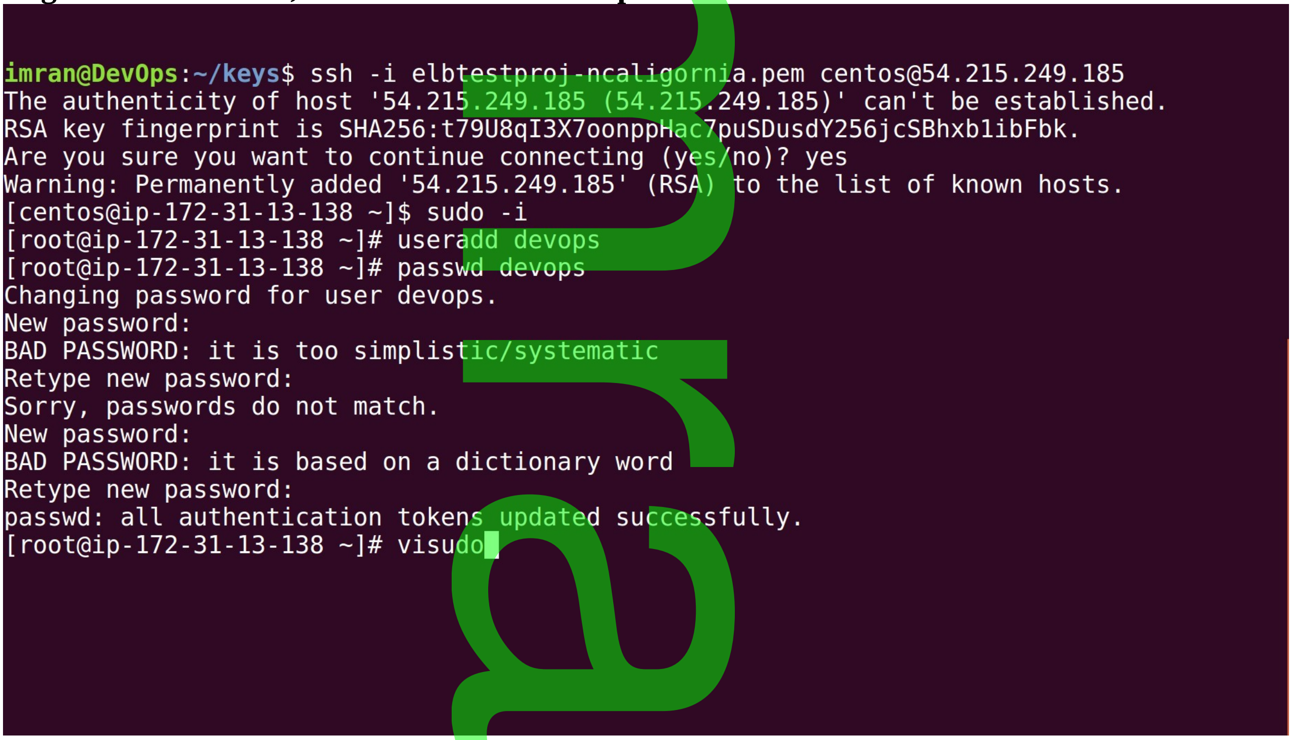
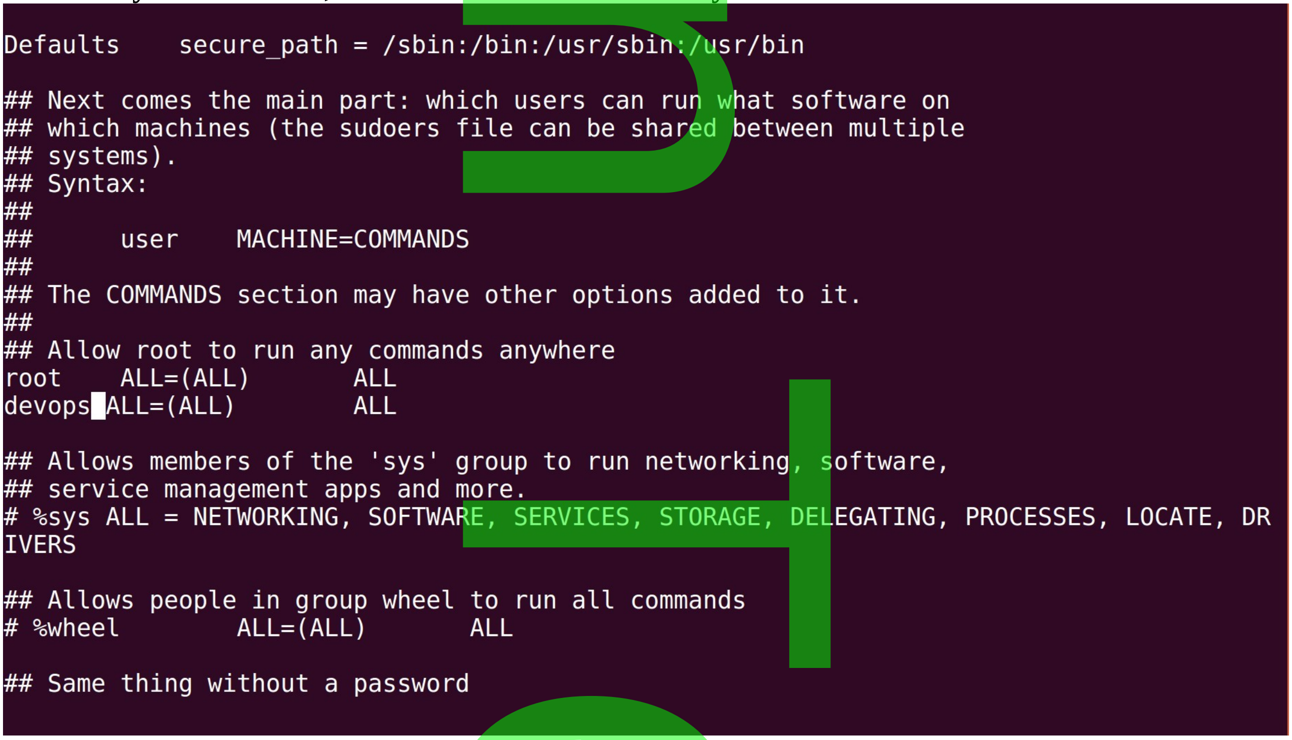
Adding user in centos ec2 instance with sudo priv.

Login to ec2 instance, switch to root user & open sudoers file



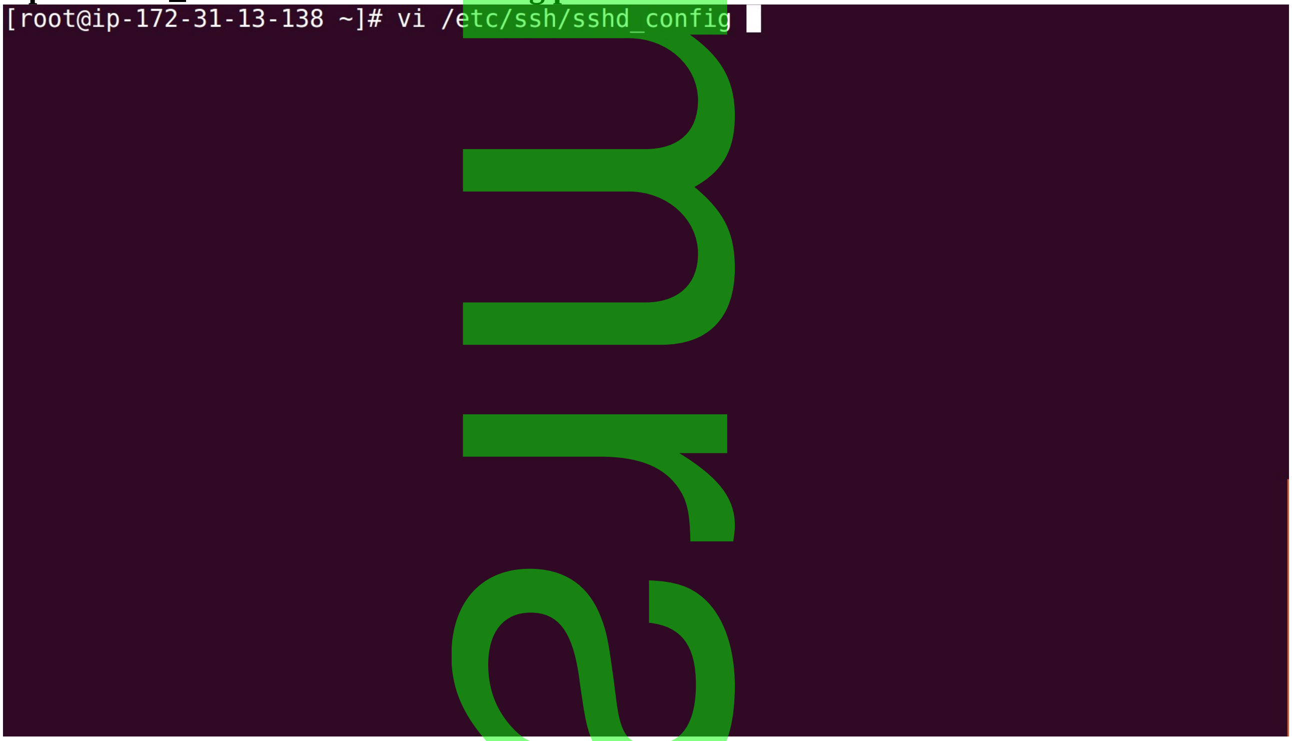
```
imran@DevOps:~/keys$ ssh -i elbtestproj-ncaligornia.pem centos@54.215.249.185
The authenticity of host '54.215.249.185 (54.215.249.185)' can't be established.
RSA key fingerprint is SHA256:t79U8qI3X7oonppHac7puSDusdY256jcSBhxb1ibFbk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '54.215.249.185' (RSA) to the list of known hosts.
[centos@ip-172-31-13-138 ~]$ sudo -i
[root@ip-172-31-13-138 ~]# useradd devops
[root@ip-172-31-13-138 ~]# passwd devops
Changing password for user devops.
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-13-138 ~]# visudo
```

Find entry for root user, below that add similar entry for our user.

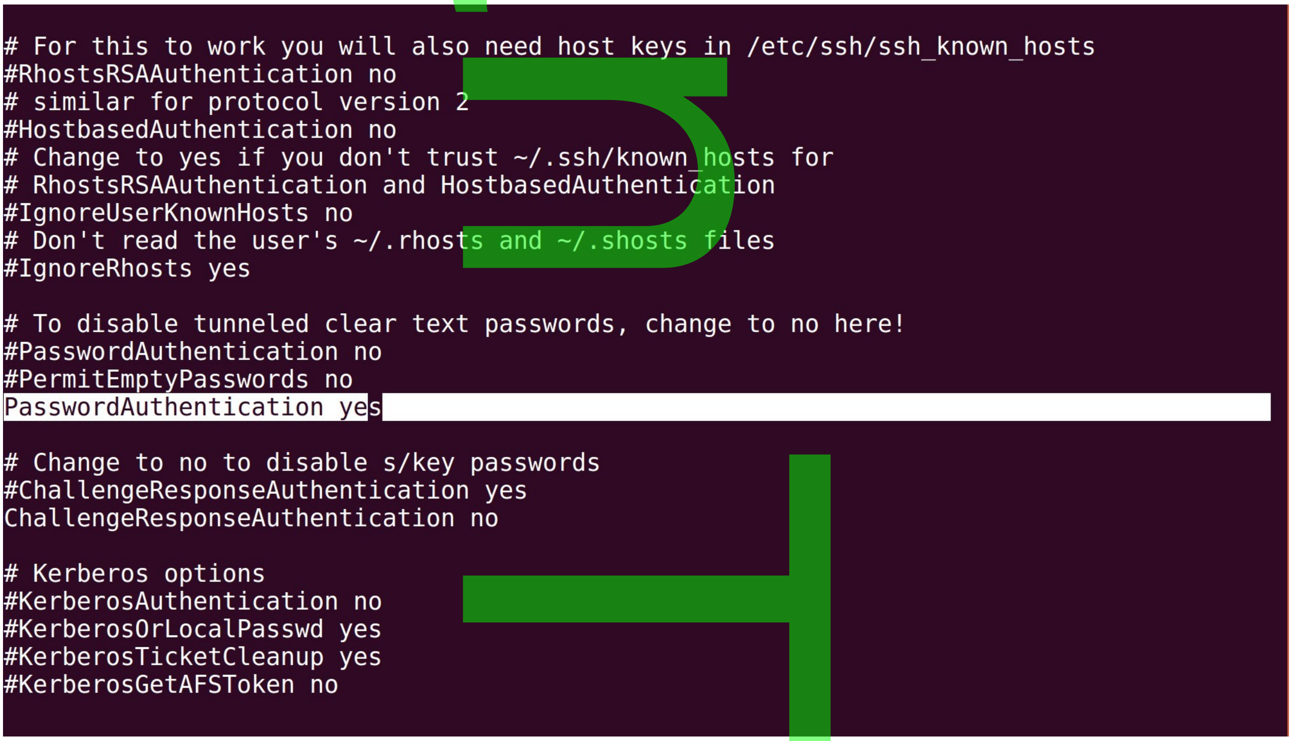


```
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
devops 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, LOCATE, DR
IVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
```

Open SSHD_CONFIG file for Enabling password authentication.

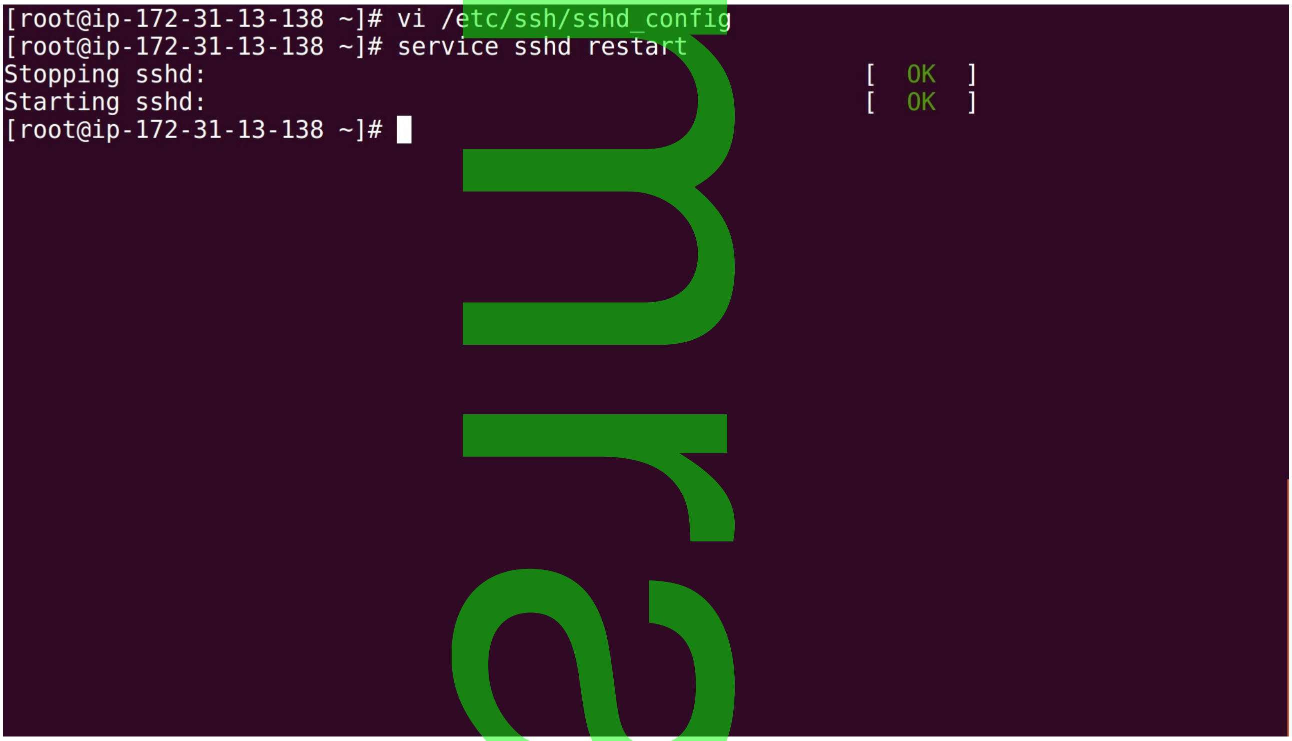


```
[root@ip-172-31-13-138 ~]# vi /etc/ssh/sshd_config
```



```
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

Restart SSHD service.



```
[root@ip-172-31-13-138 ~]# vi /etc/ssh/sshd_config
[root@ip-172-31-13-138 ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@ip-172-31-13-138 ~]# 
```