ANSIBLE

Ansible Installation:

<u>For Ansible Control Server:</u>

Step 1: Add Ansible PPA to our system

```
$ sudo apt-add-repository ppa:ansible/ansible
```

Step 2: Update the packages and Installing Ansible

```
$ sudo apt-get update && sudo apt-get install ansible
```

Step 3: Check whether ansible installed or not

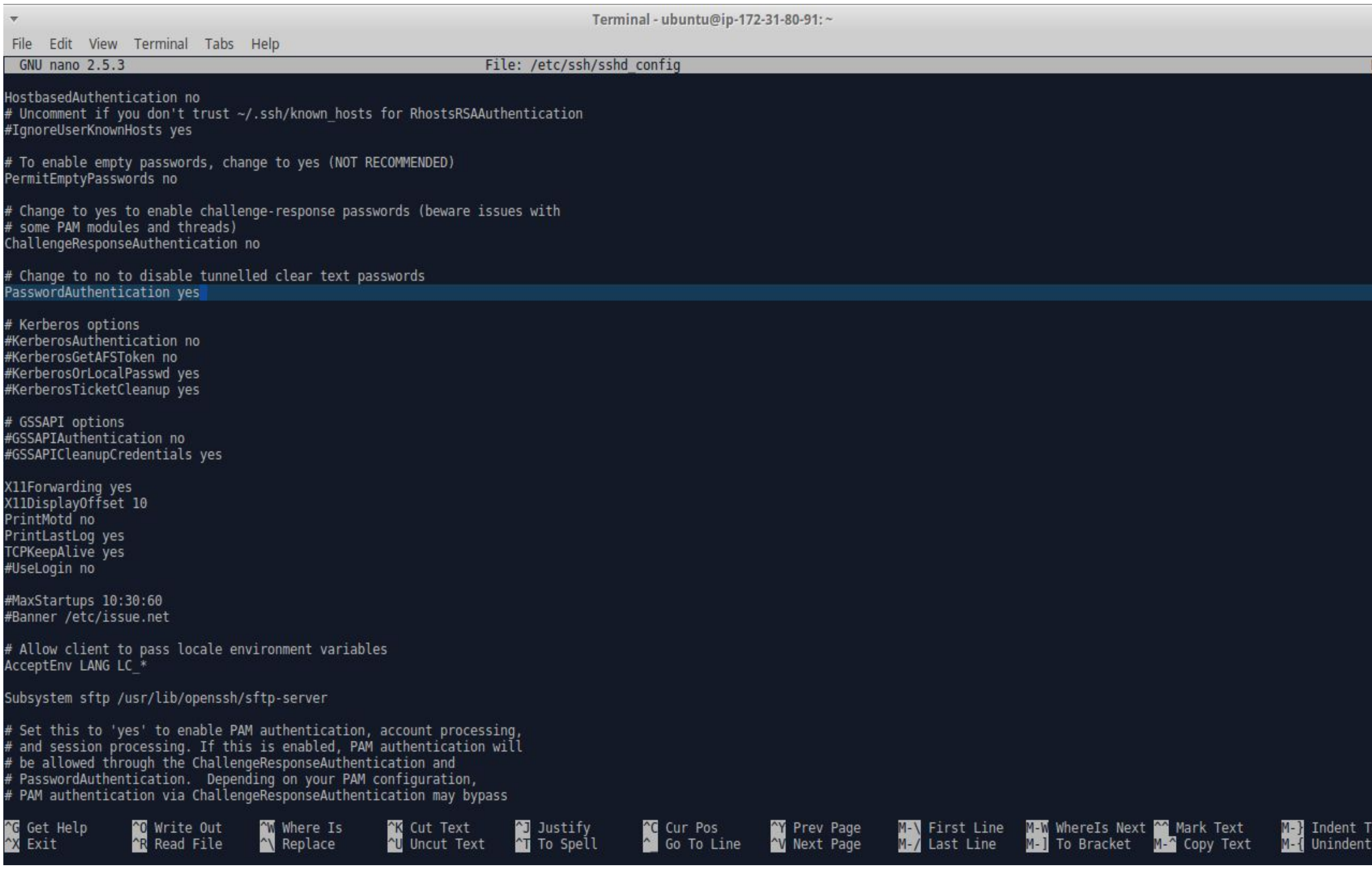
```
ansible --version
```

Step 4: Make password authentication as ‘yes’

```
$ sudo nano /etc/ssh/sshd_config
```

Find the below line,

Change password authentication ‘yes’, by default it is ‘no’


Terminal - ubuntu@ip-172-31-80-91: ~
File Edit View Terminal Tabs Help
GNU nano 2.5.3
File: /etc/ssh/sshd_config

```
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes

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

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
```

Step 5: Make sure to restart sshd service

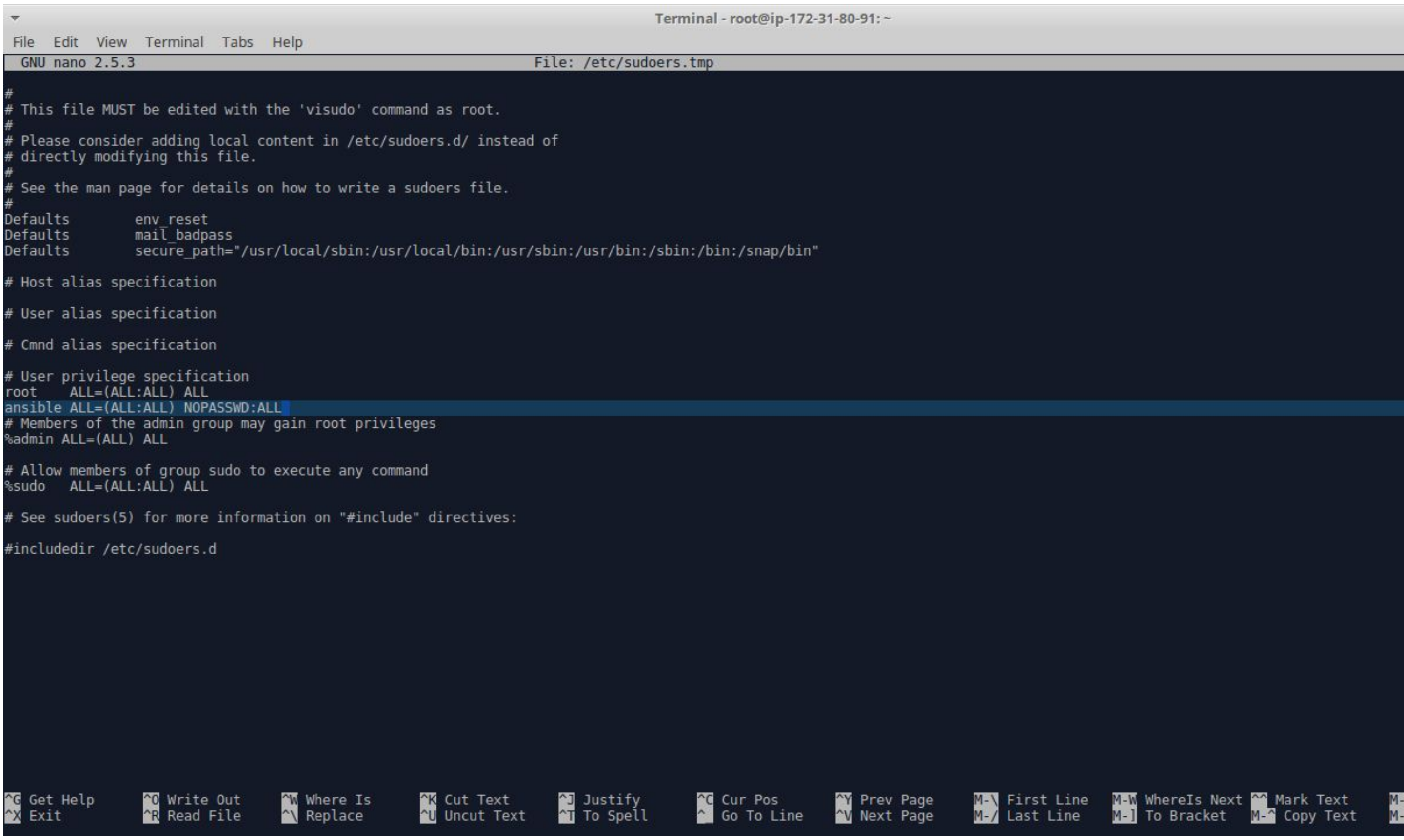
```
$ sudo service sshd restart
```

Step 6: create a user and give sudo privileges to that user

```
$ sudo -i
$ adduser ansible
$ visudo
```

Add below line at user privilege specification.

```
ansible ALL=(ALL:ALL) NOPASSWD: ALL
```



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
ansible ALL=(ALL:ALL) NOPASSWD:ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Step 7: Generate the key for ssh authentication for nodes

```
$ su ansible
$ ssh-keygen
```

Generated key will be available at ‘/home/ansible/.ssh/id_rsa.pub’ location

Step 8: Copy the key into node which you want to configure with control server.

$ ssh-copy-id <user>@<node’s IP>

Step 9: Check whether the node is properly configured or not

ssh <user>@<node’s IP>

If it is not asking password, then your configuration with node is succeeded

For Ansible Node:

Step 1: Update packages and Installing Python

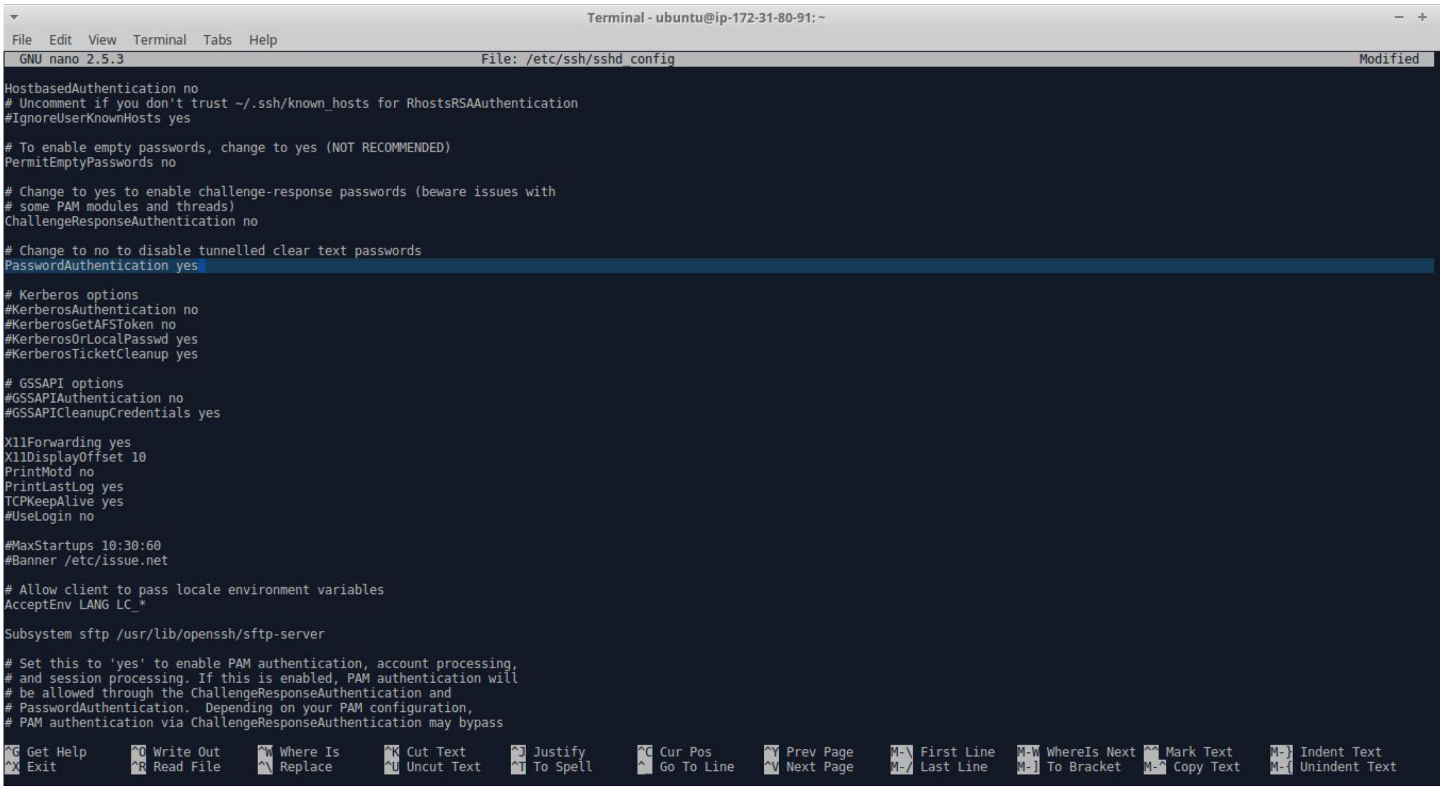
```
sudo apt-get update && sudo apt-get install python
```

Step 2: Make password authentication as ‘yes’

```
$ sudo nano /etc/ssh/sshd_config
```

Find the below line,

Change password authentication ‘yes’, by default it is ‘no’


Terminal - ubuntu@ip-172-31-80-91: ~
File Edit View Terminal Tabs Help

```
  GNU nano 2.5.3                        File: /etc/ssh/sshd_config                                              Modified

HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes

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

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page   M-\ First Line  M-W WhereIs Next ^^ Mark Text   M-} Indent Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page   M-/ Last Line   M-] To Bracket   M-^ Copy Text   M-{ Unindent Text
```

Step 5: Make sure to restart sshd service

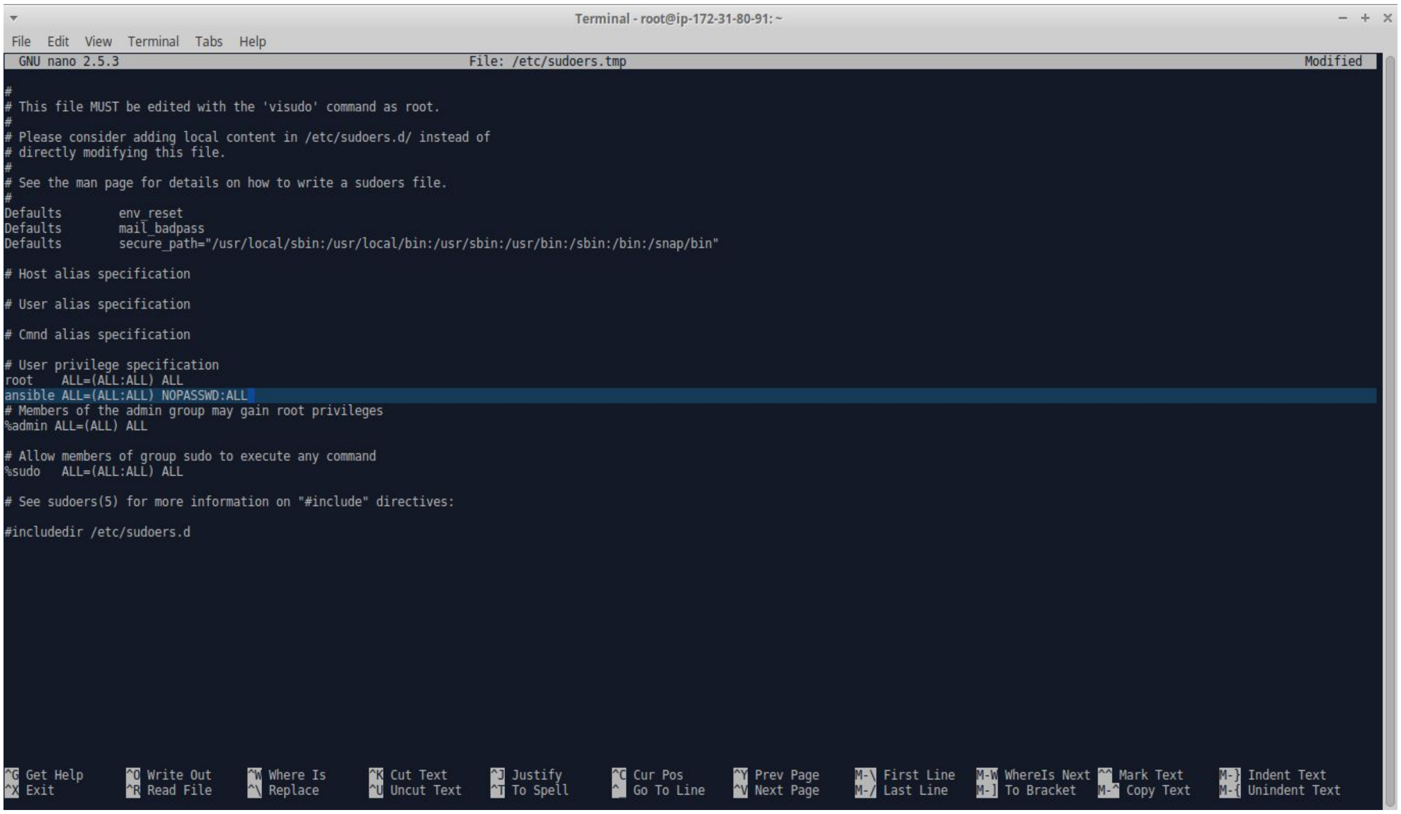
```
$ sudo service sshd restart
```

Step 6: create a user and give sudo privileges to that user

```
$ sudo -i
$ adduser ansible
$ visudo
```

Add below line at user privilege specification.

```
ansible ALL=(ALL:ALL) NOPASSWD: ALL
```



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
ansible ALL=(ALL:ALL) NOPASSWD:ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```