1) In Ansible we need to assign Elastic IP (every reboot and every shutdown public ip goes change so we are going to assign elastic IP)  
Action ->assosiate->particular address

2) Then we need to create user called test to avoid password authentication each and every time.

Sudo su –

Useradd test

Passwd test

And then we need to enable the “password authentication” and “permit root login “in

[root@ip-172-31-24-150 ~]# vi /etc/ssh/sshd\_config

Then needs to edit the above file to enable “password authentication” and “permit root login “

[root@ip-172-31-24-148 ~]# systemctl restart sshd

Then we can login by test user by using test user password

3) To connect internally to other server by using private ip’s its will ask password each and every time so we need to make keyless authentication by using ‘ssh-keygen’ command run this command under test what we created the user (we need to generate this key in all machine)   
share this key around all other machine like master to node1, node2, node3 by using “ssh-copy-id” command

Eg: [test@ip-172-31-24-150 ~]$ ssh-copy-id 172.31.24.148(private ips)

If we do this it will not ask password to connect next time by using ssh

Eg: [test@ip-172-31-24-150 ~]$ ssh test@172.31.24.147

Last login: Thu Nov 3 02:33:47 2016 from 223.227.229.28

[test@ip-172-31-24-147 ~]$

4. Configure EPEL Repo

[test@ip-172-31-24-149 yum.repos.d]$ sudo yum install wget

[test@ip-172-31-24-150 ~]$ ping dl.fedoraproject.org

//error//[test@ip-172-31-24-149 yum.repos.d]$ wget <http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-8.noa> rch.rpm

2016-11-03 03:39:18-- http://dl.fedoraproject.org/pub/epel/7/x86\_64/e/epel-release-7-8.noarch.rpm

Resolving dl.fedoraproject.org (dl.fedoraproject.org)... 209.132.181.26, 209.132.181.27, 209.132.181.23, .epel-release-7-8.noarch.rpm: Permission denied

Cannot write to ‘epel-release-7-8.noarch.rpm’ (Permission denied).(because we are in /etc/yum.repo its belongs to root user)

Done (path for rpm files:http://dl.fedoraproject.org/pub/epel/7/x86\_64/e/epel-release-7-8.noarch.rpm)

[test@ip-172-31-24-149 ~]$ wget http://dl.fedoraproject.org/pub/epel/7/x86\_64/e/epel-release-7-8.noarch.rpm

--2016-11-03 03:41:40-- http://dl.fedoraproject.org/pub/epel/7/x86\_64/e/epel-release-7-8.noarch.rpm

Resolving dl.fedoraproject.org (dl.fedoraproject.org)... 209.132.181.25, 209.132.181.26, 209.132.181.27, ...

Connecting to dl.fedoraproject.org (dl.fedoraproject.org)|209.132.181.25|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 14612 (14K) [application/x-rpm]

Saving to: ‘epel-release-7-8.noarch.rpm’

100%[=============================================================================================>] 14,612 51.1KB/s in 0.3s

2016-11-03 03:41:41 (51.1 KB/s) - ‘epel-release-7-8.noarch.rpm’ saved [14612/14612]

[test@ip-172-31-24-149 ~]$

total 1296

-rw-rw-r--. 1 test test 14612 Jul 24 14:22 epel-release-7-8.noarch.rpm

To install we need to below command

[test@ip-172-31-24-149 ~]$ sudo rpm -ivh epel-release-7-8.noarch.rpm

warning: epel-release-7-8.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 352c64e5: NOKEY

Preparing... ################################# [100%]

Updating / installing...

1:epel-release-7-8 ################################# [100%]

Sudo yum update to all nodes.

Then we can install ansible

[test@ip-172-31-24-147 ~]$ sudo yum install ansible -y

Ansible installation

>>  
**## RHEL/CentOS 7 64-Bit ##**

# wget http://dl.fedoraproject.org/pub/epel/7/x86\_64/e/epel-release-7-8.noarch.rpm

# rpm -ivh epel-release-7-8.noarch.rpm

To verify repo list

yum repolist

After configuring epel repository, you can install Ansible using following command.

sudo yum install ansible -y

[root@ip-172-31-24-204 ~]# ansible --version

ansible 2.2.0.0

Step 2: Preparing SSH Keys to Remote Hosts

4. To perform any deployment or management from the localhost to remote host first we need to create and copy the ssh keys to the remote host. In every remote host there will be a user account tecmint (in your case may be different user).

First let we create a SSH key using below command and copy the key to remote hosts.

[root@ip-172-31-24-204 ~]# ssh-keygen -t rsa -b 4096 -C "admin@prem.com"

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

/root/.ssh/id\_rsa already exists.

Overwrite (y/n)? y(for second time it will ask this)

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

The key fingerprint is:

cb:eb:17:75:d0:39:1c:33:36:56:6e:d2:21:98:36:fc admin@prem.com

The key's randomart image is:

+--[ RSA 4096]----+

After creating the ssh key successfully now copy the created key to all three remote server’s.

# ssh-copy-id tecmint@192.168.0.112

# ssh-copy-id tecmint@192.168.0.113

# ssh-copy-id tecmint@192.168.0.114