2. Ansible Playbook to do the following tasks on a newly created server running CentOS 7:

*---  
 - hosts: all  
   vars:  
     - provision\_password: ‘random password’   
  gather\_facts: no  
   remote\_user: root  
   
   tasks:  
   
   - name: Add a new user named provision  
     user:  
          name=provision  
          password={{ provision\_password }}  
   
   - name: Add provision user to the sudoers  
     copy:  
          dest: "/etc/sudoers.d/provision"  
          content: "provision  ALL=(ALL)  NOPASSWD: ALL"  
   
   - name: Deploy SSH Key  
     authorized\_key: user=provision  
                     key="{{ lookup('file', '/home/provision/.ssh/id\_rsa.pub') }}"  
                     state=present  
   
   - name: Disable Password Authentication  
     lineinfile:  
           dest=/etc/ssh/sshd\_config  
           regexp='^PasswordAuthentication'  
           line="PasswordAuthentication no"  
           state=present  
           backup=yes  
     notify:  
       - restart ssh  
   
   - name: Disable Root Login  
     lineinfile:  
           dest=/etc/ssh/sshd\_config  
           regexp='^PermitRootLogin'  
           line="PermitRootLogin no"  
           state=present  
           backup=yes  
     notify:  
       - restart ssh  
   
   handlers:  
   - name: restart ssh  
     service:  
       name=sshd  
       state=restarted*

- lineinfile:

path: /etc/ssh/sshd\_config

regexp: '^Port 22 '

insertafter: '^#Port 22 '

line: 'Port 10022'

name**:** example using security group rule descriptions

ec2\_group**:**

name**:** "{{ **name** }}"

description**:** sg with rule descriptions

vpc\_id**:** vpc-xxxxxxxx

profile**:** "{{ **aws\_profile** }}"

region**:** us-east-1

rules**:**

**-** proto**:** tcp

ports**:**

**-** 80

cidr\_ip**:** your.ip/0

rule\_desc**:** allow all on port 80