1. Using AWS or another cloud provider, create and deploy a running instance of an LDAP serverusing Ansible.Ansible Tower is not allowed for this exercise.
2. Using Ansible, in the created instance, add a group named “techops\_dba”to /etc/security/access.conf and /etc/sudoers.
3. What is the NTP stratum of the created host? What is an acceptable load average threshold for the host (LDAP server)?
4. Instantiate a second host and implement security so that clients are only able to access the first host from the second host. Use SSH for connectivity. Access control must be implemented on the host itself and not via an external management tool such as AWS security groups.
5. Develop and apply automated tests to verify correctness of the LDAP server of step 1, the configuration of step 2, the results of the NTP findings of step 3, and the security restrictions of step 4.
6. Express everything in code and upload your code to GitHub. Submit the link to your code on GitHub to Beeline.

Be prepared to show your code, the hosts, the tests and their results, and your thought process.

1)

- name: LDAP Instance

hosts: localhost

gather\_facts: False

vars:

key\_name: my\_keypair

instance\_type: m1.small

security\_group: my\_securitygroup

image: my\_ami\_id

region: us-east-1

tasks:

- name: Launch instance

ec2:

key\_name: "{{ my\_keypair }}"

group: "{{ my\_securitygroup }{ LDAP\_group }}"}"

instance\_type: "{{ m1.small }}"

image: "{{ ami-5731123e }}"

wait: true

region: "{{ us-east-1}}"

vpc\_subnet\_id: subnet-29e63245

assign\_public\_ip: yes

register: ec2

- name: Add new instance to host group

add\_host: hostname={{ 192.168.0.25 }} groupname=LDAP\_group

with\_items: ec2.instances

- name: Wait for SSH to come up

wait\_for: host={{ 192.168.0.25 }} port=22 delay=60 timeout=320 state=started

with\_items: ec2.instances

- name: Configure instance(s)

hosts: launched

become: True

gather\_facts: True

2)

tasks:

- name: Add group remote

lineinfile: dest=/etc/security/access.conf line="group: name=techops\_dba state=present"

- name: Allow 'techops\_dba' group to have passwordless sudo

lineinfile:

dest: /etc/sudoers

state: present

regexp: '^%techops\_dba'

line: '%techops\_dba ALL=(ALL) NOPASSWD: ALL'

3) [ec2-user ~]$ ntpq -p

remote refid st t when poll reach delay offset jitter

==============================================================================

+dc1.dc 204.9.54.119 2 u 15 128 377 88.649 5.946 6.876

-dc2.dc 91.189.94.4 3 u 133 128 377 182.673 8.001 1.278

\*dc3.dc 216.218.254.202 2 u 68 128 377 29.377 4.726 11.887

+dc4.dc 149.20.64.28 2 u 31 128 377 28.586 -1.215 1.435

Cat /etc/ntp.conf

server 0.amazon.pool.ntp.org iburst

server 1.amazon.pool.ntp.org iburst

server 2.amazon.pool.ntp.org iburst

server 3.amazon.pool.ntp.org iburst

4)

below command will block all traffic except allowing the second host (only ssh ). only able to access the first host from the second host

First host IP : 192.168.0.25 second host IP : 192.168.0.26

#iptables -I INPUT -p tcp -s ! 192.168.0.26 --dport 22 -j DROP

5) run below on as root 192.168.0.26(bash script)

for i in 10.102.52.112 ; do sshadmin -q $i " sudo /usr/sbin/chkconfig --list ldap;sudo /usr/sbin/service ldap status;ntpq –p;cat etc/security/access.conf ;cat /etc/sudoers;Cat /etc/ntp.conf;nmap -p 22 192.168.0.25 “; done &> /tmp/out.txt