EX294 Exam Paper Sample

Q1. Install and Configure Ansible on the control node as follows:

- Install the required packages.
- Create a static inventory file called /home/student/ansible/inventory as follows:

  - system1 is a member of the dev host group
  - system2 is member of the test host group
  - system3 and system4 are member of the prod host group
  - system5 is member of the balancers host group
  - The prod group is a member of the webservers host group

- Create a configuration file called /home/admin/ansible/ansible.cfg

  - The host inventory file is /home/admin/ansible/inventory
  - The location of role used in playbooks include /home/admin/ansible/roles
  - The Install Ansible Content Collection location /home/admin/ansible/mycollection

Q2. Create a playbook for yum configuration

As a system administrator you will need install software on the managed nodes.

Create a playbook called /home/admin/ansible/yum.yml , the user ansible create a yum repository oneach of the managed nodes as follows:

Repository 1:

- The name of the repository is EX294_BASE
- The description is EX294 base software
- The base URL is http://server.network.example.com/BaseOs
- GPG signature checking is enabled
- GPG Key is given as: http://server.network.example.com/RHEL/RPM-GPG-KEY-redhat-release
- The repository is enabled

Repository 2:

- The name of the repository is EX294_STREM
- The description is EX294 base software
- The base URL is http://server.network.example.com/AppStream
- GPG signature checking is enabled
- The GPG Key URL is http://server.network.example.com/RHEL/RPM-GPG-KEY-redhat-release
- The repository is enabled

Q3. Install Packages

- Create a playbook called /home/admin/ansible/packages.yml that:

- Installs the php & mariadb on hosts in the dev,test and prod host group
- Installs the RPM Development Tools package group on host in the dev host group
- Update all packages to the latest version on host in the dev host group

Q4. Install Ansible Content Collections

- Location of Collection inside http://utility.lab13.example.com/materails

1. install the redhat.rhel_system_roles-1.19.3.tar.gz collection
2. install the posix-1.20.2.tar.gz collection
3. install the community-general-5.5.0.tar.gz collection

Q5. Use a RHEL System Role

- Use a RHEL system role Install the RHEL System role package & create a playbookcalled /home/admin/ansible/timesync.yml that: -
- Runs on all managed nodes

- Uses the timesync role
- Configures the role to use the currently active NTP provider
- Configure the role to use the time server 172.24.1.254
- Configure the role to enable the iburst parameter

Q6. Install Roles using Ansible Galaxy

- Download and install role to /home/admin/ansible/roles from following URL:

- http://server.network.example.com/materials/haproxy.tar
  The Name of the role should be balancer
- http://server.network.example.com/materials/phpinfo.tar
  The name of this role should be phpinfo

Q7. Creating and Using a Role

- Create a role called apache in /home/admin/ansible/roles with the following requirement:

- The httpd package is install, enabled on boot and started
- The Firewall is enabled & running with a rule to allow access the web server
- A template file index.html.j2 exists and is used to create the file

/var/www/html/index.html with the content:

“Welcome to HOSTNAME ON IPADDRESS”

HOSTNAME is the fqdn of the managed nodes and

IPADDRESS is the ip address of managed nodes

- create a playbook called /home/admin/ansible/newrole.yml that uses this role as follow:
  The Playbook runs on host in the webservers host group

Q8. Use roles from Ansible Galaxy

- Create a playbook called /home/admin/ansible/roles.yml
- The playbook contains a play that runs on host in the balances host group and uses the balances role.

- This role configures a service to load balance web server request between hosts in the webserver host group.
- Browsing to host in the balances host group (for example http://system5.domain1.example.com) produces the following output:

  - Welcome to system3.domain1.example.com on 172.24.1.8

- Reloading the Browser produces output from the Alternate webserver:

  - Welcome to system4.domain1.example.com on 172.24.1.9

- The Playbook contains a play the runs on hosts in webserver host group and user the phpinfo role.
- Browsing to host in the webserver host group with the URL /hello.php produces the following output :

- Hello PHP World from FQDN - For example Browsing to http://system3.domain1.example.com/hello.php produces the following output:

  - Hello PHP World from system3.domain1.example.com along with various details of the PHP configuration include the version of PHP that is installed.

- Similarly, browsing to http://system4.doamin1.example.com/hello.php, produces the following output:

  - Hello PHP World from system4.domain1.example.com along with various details of the PHP configuration including the version of PHP that is installed.

Q9. Generate a Host File

- Download an initial template file from http://server.network.example.com/materials/host.j2 to /home/admin/ansible
    - Complete the template so that it can he used to generate a file with a line for each host in thesame format as /etc/hosts
- Download a certain playbook using the given link: http://server.network.example.com/materials/host.yml

This playbook will automatically save the info of all managed nodes as mentioned by you in the hosts.j2 in the dev hosts group.

- Do not make any changes to this playbook
- When the playbook is run, the file /etc/myhosts on host in the dev host group should have a line foreach managed hosts:

127.0.0.1 localhost localhost.localdoamin localhost4 localhost4.localdomain

::1 localhost localhost.localdoamin localhost6

localhost6.localdomain172.24.10.6

system1.domain1.example.com system1

172.24.10.7 system2.doamin1.example.com system2

172.24.10.8 system3.doamin1.example.com system3

172.24.10.9 system4.doamin1.example.com system4

172.24.10.10 system5.doamin1.example.com system5

Note: The order in which the inventory host names appear is not important.

Q10. Modify File Content

Create a playbook called /home/admin/ansible/issue.yml

- The playbook runs on all inventory hosts
- The playbook replaces the content of /etc/issue with a single line of text as follows:

- On host is the dev host group, the line reads: Development

- On hosts in the test host group, the line read: Test

- On hosts in the prod hosts group, the line read: Production

Q11. Create a Web Content Directory

- Create a playbook called /home/admin/ansible/webcontent.yml as follows:
  - The playbook runs managed node in the dev host group
- Create the directory /webdev with the following requirement:
  - it is owner by the webdev group
  - it has regular permissions: owner=read+write+execute,group=r+w+x,other=r+x
  - it has special permission: set group GID
- Symbolically link /webdev to /var/www/html/webdev
- Create the file /web/index.html with a single line of text that reads: Development
- Browsing this directory on host in the dev host group (for example: http://system1.domain1.example.com/webdev) gives the following output: Development

Q12. Generate a Hardware Report

- Create a playbook called /home/admin/ansible/hwreport.yml that produces an output file called /root/hwreport.txt on all managed nodes with the following information: -

- Hostname
- Total Memory
- BIOS version
- Size of disk device vda
- Size of disk device vdb

Each line of the output file contains a single key=value pair.

- your playbook should Download the file from http://server.network.example.com/materials/hwreport.empty and save it is at the given location: /root/hwreport.txt

- Modify /root/hwreport.txt with the correct values - if a hardware item does not exist, the associated value should be set to NONE

Q13. Create a Password Vault

Create an ansible vault to store user password as follows:

- The name of the vault is /home/admin/ansible/locker.yml
- The vault contains two variables with names:
  - **dev_pass** with value **wakennym**
  - **mgr_pass** with value **rocky**
- The Password to encrypt and decrypt the vault is **atenorth**
- The password is stored in the file /home/admin/ansible/secret.txt

Q14. Create User Accounts

- Download a list of users to be created from http://server.network.example.com/materials/user_list.yml
- Using the password vault /home/admin/ansible/locker.yml create elsewhere in this exam
- Your playbook should work using the vault password file /home/admin/ansible/secret.txt created elsewhere in this exam
- User with a job description of manager should be created in dev and test host groups with:

- assigned the password from mgr_pass variable

- a member of supplementary group opsmgr

- password should use the SHA512 hash format

- User with job description of developer should be created in prod host group with:

- create a member of supplementary group devops

- create on managed node in the dev and test host group

- assigned the password from the dev_pass variable

Q15. ReKey an Ansible Vault

Rekey an existing Ansible vault as follows:

- Download the Ansible vault from http://server.network.example.com/materials/salariries.yml to /home/admin/ansible/ and make the following amendments:

- The current vault password is jaishreeram

- The new vault password is jaimatadi

Q16. Storage LVM

- Create a playbook called /home/admin/ansible/ansible/lv.yml that runs on all managed nodes that does thefollowing:

- Creates a logical volume with these requirement:

- The logical Volume is Created in the research volume group

- The logical volume name is data

- The logical volume size is 1500 Mib

- Format the logical volume with the ext4 file system

- If the requested logical volume size cannot be created, the error message
  " Could not create logical volume of that size "
  should be displayed and size 800 MiB should be used instead.
- If the volume research does not exist, the error message
  " Volume group does not exist "
  should be displayed

- Do NOT mount the logical volume in any way.

Q. 17 Use a RHEL System Role

- Create a playbook name selinux.yml and use system roles to:
- Set selinux mode as enforcing in all manage node

Q.18 Setting a Cronjob

- Create a cronjob for user natasha in all nodes, the playbook name crontab.yml and the job details are that it in every 2 minutes the job will execute logger "EX294 in progress"