RHCE Practice Exam 3

To work through this exam, you need a total of five servers that are running RHEL 8 or Centos 8. One server needs to be configured as the control host; the other four servers need to be configured as managed servers, using the names ansible1.example.com through ansible4.example.com. The IP addresses used on the managed servers are not important; you can pick anything that matches your configuration. Make sure the servers meet the following requirements:

- 1 GB of RAM.
- 20 GB of disk space on the primary disk /dev/sda.
- 5 GB of disk space on the secondary disk /dev/sdb, which only exists on ansible1 and ansible2.
- The root user account configured with the password "password" on each of the servers.
- The control server with a user account "ansible". SSH public and private keys have been generated for this user. No further configuration has been done yet.

In the assignments in this exam, you'll need to create scripts and yaml files. Make sure that all these scripts are stored in the directory /home/ansible.

Common Tasks

1. Configure the control host with a static inventory, as well as the ansible.cfg configuration file. In the static inventory, configure the following host groups:
    a. Group test with ansible1.example.com as a member
    b. Group dev with ansible2.example.com as a member
    c. Group prod with ansible3 and ansible4 as members
    d. A group servers, with groups dev and prod as members

    Ensure that hosts can be reached through their FQDN, but also by using the short name (so ansible1.example.com as well as ansible1).
2. Create a playbook with the name setupreposerver.yml to set up the control host as a repository host. Make sure this host meets the following requirements, which must be done by the playbook:
    a. The RHEL 8 installation ISO is loop-mounted on the directory /var/ftp/repo.
    b. The firewalld service is disabled.
    c. The vsftpd service is started as well as enabled, and it allows anonymous user access to the /var/ftp/repo directory.
3. Create a script that configures the managed servers as repository clients to the repository server that you have set up in the previous task. This script must use ad hoc commands and perform the following tasks:
    a. Disable any currently existing repository.
    b. Enable access to the BaseOS repository on control.example.com.
    c. Enable access to the AppStream repository on control.example.com.
4. Create a script with the name setuphosts.sh that uses ad hoc commands to complete configuration on the managed servers. This includes:

a. Installing Python
b. Creating a user with the name ansible
c. Creating a sudo configuration that allows user ansible to run tasks with root privileges
d. Using an ad hoc command to call the appropriate module to test connectivity to the remote hosts

Exam 3 Specific Tasks

1. Write a playbook that installs software packages:
    a. Perl and php on servers in the groups dev, test, and prod
    b. All packages from the package group "Virtualization Host" on the group prod
    c. Servers in the group prod that are fully updated
2. Create a playbook that configures an LVM logical volume with the name lvdata in the volumegroup vgdata, according to the following requirements:
    a. Only on servers in the group prod, create a 2 GiB volume group with the name "vgdata".
    b. If the volume group vgdata does not exist, the playbook must return the message "vgprod does not exist".
    c. If the volume group exists but has less than 1 GiB storage available, the playbook must show the message "insufficient disk space available".
3. Create a playbook with the name sysreport.yml that generates a file on the ansible control server. The file should have the name hwtemplate.txt and the following contents:

    NAME=
    IPADDRESS=
    TOTAL_MEMORY=
    NIC_NAME=
    SECOND_NIC_NAME=

    Use this file to generate a report on the managed servers. To do so, copy the file to /root/report.txt, and have your playbook modify it, but do not overwrite current settings. Apply the following requirements:
    a. NAME= gets the FQDN of the managed host as argument.
    b. IPADDRESS= gets the IP address of the managed host.
    c. TOTAL_MEMORY= gets the total amount of memory on the managed host.
    d. NIC_NAME=gets the name of the network card on the host.
    e. If the host has a second network card, SECOND_NIC_NAME should get the name of that network card. If the managed host has no second network card, the playbook should set SECOND_NIC_NAME=NONE.
4. Create a vault-encrypted file with the name anspass.txt. This file should set the variable devpass to the value password and the variable prodpass to the value secret. Set the vault password required to access this file to vaultpass. Also create a vault password file with the name vaultpass.txt that can be used to automatically enter this password.
    After creating the vault-encrypted file, change the vault password to myvaultpass, and ensure it still can be used automatically.

5. Use the RHEL system role that manages time in a playbook with the name settime.yml. Ensure that control.example.com is used as the time server, and set the appropriate parameter that allows changing time even if a large difference exists between time on the managed machine and time on the time server. At the end of the playbook, verify that time is synchronized. If this is not the case, the playbook should print the text "Unfortunately time could not be synchronized".
6. Configure a playbook with the name runwebserver.yml that meets the following requirements. Ensure that the webserver contents are accessible from other machines:
    a. Create a file /webcontent/index.html that contains the text "welcome to this webserver. The server is managed by USERNAME."
    b. Use a variable to set USERNAME to anna. The variable should be set by using inclusion of a file that is created for servers in the group prod only.
    c. Create a symbolic link in /var/www/html/index.html that links to the file /webcontent/index.html, and ensure the contents of this file are visible from remote hosts.