Create and Deploy A static application infrastructure with ansible-IAC (infrastructure as a code).

* Ansible Vault is an Ansible feature that helps you encrypt confidential information without compromising security.

Or

* Ansible Vault is an Ansible feature that helps you encrypt confidential information without compromising security.
* Ansible is a configuration management tool.While working with Ansible ,you can create various playbooks,inventory files,variable files,etc.Some of the files contain sensitive and important data like usernames and paawords.Ansible provides a feature named Ansible Vault that prevents this data from being exposed.It keeps passwords and other sensitive data in an encrypted file rather than in plain text files.It provides paaword-based authentication.
* Editor Note: Ansible Vault is one tool that one might use.but not necessarly what most sysadmins run in production.Red Hat Ansible Automation platform is enterprise=grade and it can also work with existing tools that most enterorises have.You might also enjoy :Handling secretes in your Ansible Playbooks.
* ANsible Vault performs various operations. Specificaally,it can

1. Encrypte an existing file
2. Decrypt the file
3. View an encrypted file without breaking encryption
4. Edit an encrypted file
5. Create an encrypted file.
6. Generate or reset the encrypted key

* Encrypt an existing file:

1. The ansible-vault encrypt command is used to encrypt od existing file.

#ansible-vault encrypt file.yaml

1. After typing this command,it will ask for a password and than ask where to put your content.to check use cat command.

* Create an encrypted file:

1.the ansicle-vault create command is used to create the encrypted file.

#ansible-vault create file.yaml

* The following command is used to create encrypted files with –vault id.

#ansible-vault create –vault-id password@prompt vault.yml

* Editing the encrypted file:

1. If the file is encrypted and changes are required , use the edit command.

#ansible-vault edit secure.yml

* Decrypting the file:

1. The ansible-vault devcrypt command is used to decrypt the encrypted file.

#ansible-vault decrypt f.yml

* Decrypt a running playbook:

1. To decrypt the playbook while it is running, you usually ask for its password.
2. # ansible-playbook –ask-vault-pass file.yml

* Reset the file password:

1. Use the ansible-vault rekey cpmmand to reset the encrypted file password.
2. # ansible-vault rekey secure.yml

* Process steps:

1. Prepare AWS account
2. Install required software on local computer
3. Setup non Ansible local files – project Directory,SSH keys
4. Steup Ansible vault
5. Setup Ansivle playbook
6. Run Ansible to generate EC@ instances
7. Connect to EC2 instance via SSH.

* Create an Iam account user.

1. Give ec2 full permissions.

* Python,pip,boto,boto3 or botocore and ansible are required to install.
* Install botocore or boto3 after switching to the path /usr/bin/

<sudo pip3 install boto3 or botocore>

* Next copy the pemfile securily from windows downloads path by using any one of the terminal with the help of following command

<scp-I pemfile pemfile ec2-user@public ip of the destination ec2 instance(ansible running server):~>

And changes the pemfile permissions by following command as <sudo chmod 600 pemfile>

* [localhost]

ansible ansible\_host=10.0.49.164 ansible\_python\_interpreter=/usr/bin/python3 ansible\_user=ec2-user ansible\_ssh\_private\_key\_file=/home/ec2-user/new.pem

* Next check the syntax for scripts.

<ansible-playbook vpc.yaml –syntax-check>

<ansible-playbook vpc.yaml –vvvv>

### VPC Creation ####

­---

* hosts: localhost

become: yes

tasks:

-