

ANSIBLE VAULT

In Ansible Vault, files are typically stored under the **group_vars/all** directory. The **all** folder allows every host to access shared passwords and keys defined within it.

Let's explore various **Ansible Vault commands** and understand how each one works.

There are 2 ways to create vault password:

A) `cd group_vars/all`

```
ansible-vault create aws_credential.yaml
```

It will ask to set up New Vault password.

B) Let's generate a strong Ansible Vault password using Base64 encoding and stored it inside a password file.

```
openssl rand -base64 2048 > vault.pass
```

→ Let create a file inside the Ansible vault using vault password:

```
ansible-vault create aws_credential.yaml --  
vault-password-file vault.pass
```

This will open the `aws_credential.yaml` file where we can store our aws credentials.

```
aws_access_key: hjshcuhfidjwsikdhwidj  
aws_secret_key: ksjnjxbsjdhguwdhwodjwikhu  
~  
~
```

If we now tried to cat the `aws_credential.yaml` file:

```
$ANSIBLE_VAULT;1.1;AES256  
626364396433373937393362316164663930333735613664  
35623262663833306564366438343837  
613061373830386334393032343461383163386261326531  
0a336165373235393264383764333837
```

The content inside the aws_credential.yaml file is encrypted by ansible vault.

→ Lets see the actual passwords inside the aws_credential.yaml:

```
ansible-vault view aws_credentials.yaml --vault-password-file vault.pass
```

```
3636346638613063650a3331623936343933361323739613135393735623633313635633130616565
61393639366266653133383664663739363830336538663730663939316162383132633334306235
343261333637663830633432366131666564336439373636363534616530373339633631383562
35373430353761373939366562643230646665383537636533666539653239373630333333303730
38663836393666306166373262633732656233343462363530646436373562393066323139333863
3831
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all# ansible-vault view aws_credentials.yaml --vault-password-file vault1.pass
aws_access_key: hjshcuhfidjwsikdhwidj
aws_secret_key: ksjnjxbsjdhguwdhwodjwikhu
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
```

→ If we want to add a new key to the aws_credentials.yaml file:

```
ansible-vault edit aws_credentials.yaml --vault-password-file vault.pass
```

```
aws_access_key: hjshcuhfidjwsikdhwidj
aws_secret_key: ksjnjxbsjdhguwdhwodjwikhu
api_token: alshjdsxdnswskwkswhjsdbwdjwend
~
```

→ Lets say there is already an existing credentials file
azure_credentials.yaml having sensitive data:

```
azure_access_key: wkdhwudwdwdhwdwkh
azure_secret_key: khsiqlhsusgwuishwuwiswusywis
api_token: akxsjgsuxdhskxnsxchvschsc
~
```

If we want to secure it using ansible vault:

```
ansible-vault encrypt azure_credentials.yaml --vault-password-file vault.pass
```

Now cat the azure_credentials.yaml and verify:

```
$ANSIBLE_VAULT;1.1;AES256
```

```
333065303031616435376132323530643239353163393038
38616430643365393263343161303464
663130626230666664316163393464353436303436613132
0a376365613434396338353763303661
```

Its encrypted!

→ We can even encrypt a variable separately instead of complete file:

```
ansible-vault encrypt_string rayees --vault-
password-file vault1.pass
```

```
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all# ansible-vault encrypt_string rayees --vault-password-file vault1.pass
Encryption successful
!vault |
$ANSIBLE_VAULT;1.1;AES256
65616663356431656362643339333634393463653735653637623637616263653539343163336265
3638623163306330636136306236653130656134353833340a306262353238356330373863623836
62333334663165616633343930663562333161666261383462636563663631356239666133623930
3336346634626534330a343030663565323035333431343562613466386131353237626237633563
6561
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
```

→ Lets decrypt the azure_credentials.yaml and cat it:

```
ansible-vault decrypt azure_credentials.yaml --
vault-password-file vault1.pass
```

```
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all# ansible-vault decrypt azure_credentials.yaml --vault-password-file vault1.pass
Decryption successful
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all# cat azure_credentials.yaml
azure_access_key: wkdhwudwdwdwdwdk
azure_secret_key: khshqhsugwuishwiswusywis
api_token: akxsjgsuxdhskxnsxchvschsc
root@DevOps:/home/mdrayeez/ansible-collections-2/group_vars/all#
```