**MANAGING SECRETS**

**ANSIBLE VALUT**

* Ansible may need access to sensitive data such as passwords or API keysin oder to configure managed hosts. Ansible vault can be used to encrypt and decrypt any structured data file used by Ansible.
* ANSIBLE-VALULT command used to create edit encrypt decrypt and view files.
* Files are protected with symmetric encryptionusing AES256 with a password as the secret key.

**Create Encrpted File**

* **#ansible-vault create secret.yml ---------------**create the password
* Instead of entering the vault password through standard input you can use a vault password file to store the vault password. You need to carefully protect this file using file permssions and other means.
* Create normal text file and store the vault password
* **#ansible-vault create secret.yml - -vault-password-file=<existed file name>**

**Viewing Encrpted File**

* + **#ansible-vault view secret.yml…….**it asks pwd to enter
  + **#ansible-vault view secret.yml - - vault-password-file=<filename>…….**it wil not ask pwd

**Edited Encrpted File**

* **#ansible-vault edit secret.yml…….**it asks pwd to enter
* **#ansible-vault edit secret.yml - - vault-password-file=<filename>…….**it wil not ask pwd

**Encripting existing file**

* **#ansible-vault encrypt secret.yml…….**it asks pwd to enter
* **#ansible-vault encrpt secret.yml - - vault-password-file=<filename>…….**it wil not ask pwd

**Changing the Password of an Encypted File**

* **#ansible-vault rekey secret.yml…….**it asks old and new pwd
* **#ansible-vault rekey secret.yml - -new-vault-password-file=<newfile\_with pwd>**

**Ansible Playbook && Vault**

* **#ansible-playbook play.yml - -ask-vault-pass**
* **#ansible-playbook play.yml - - vault-password-file=<filename>**

**Recommended Practive for Varaible File Mgmt**

**├── ansible.cfg**

**├── group\_vars ------------------------------directory**

**│   └── webservers ----------------------------directory**

**----vars ……………….file**

**├── host\_vars ---------------------------------directory**

**│   └── servera.example.com ---------------------------directory**

**Vars……………………file**

**Vault…………………file**

**├── inventory**

**├── play.yml**

**└── variable.yml**

**Instead of using files in group\_vars or host\_vars, you can also use dorectories for each host group or managed host. Those directories can then contain multiple variable files, all of the which are used by the host group or managed host.**

**Here sensitive varaibles can be kept secret by placing them in vault file.**