Ansible Vault – Secure Your Secrets

Ansible Vault is a feature that allows you to **encrypt sensitive data** such as passwords, API tokens, and private keys. This is crucial when storing credentials in version control systems like Git.

🧩 Why Use Ansible Vault?

- ✅ **Protect secrets** in your playbooks and variable files
- 🔒 Store **API keys, SSH passwords, database credentials** securely
- 🛡️ Helps in compliance & security best practices

🔐 Basic Vault Commands

1️⃣ Create a New Encrypted File

ansible-vault create secret.yml

This opens a text editor for you to add secrets (YAML format). The file is saved encrypted.

2️⃣ Edit an Encrypted File

ansible-vault edit secret.yml

3️⃣ View an Encrypted File

ansible-vault view secret.yml

4️⃣ Encrypt an Existing File

ansible-vault encrypt vars.yml

5️⃣ Decrypt a File

ansible-vault decrypt secret.yml

6️⃣ Change Vault Password

ansible-vault rekey secret.yml

🔧 Using Vault in a Playbook

Suppose you have an encrypted file `secret.yml`:

db_password: my-secret-password

In your playbook:

```
- name: Example playbook using vault
  hosts: db
  vars_files:
    - secret.yml

  tasks:
    - name: Print secret
      debug:
        msg: "The password is {{ db_password }}"
```

Run with vault password prompt:

ansible-playbook playbook.yml --ask-vault-pass

🔁 Using Vault with Password File (Not recommended for production)

ansible-playbook playbook.yml --vault-password-file vault_pass.txt

---

💡 Best Practices

- 🛑 Never hardcode secrets in playbooks or templates
- 🗂️ Use separate encrypted variable files for environment-specific secrets
- 🔐 Use **Ansible Vault IDs** for multiple vaults with different keys

---

🧪 Bonus: Encrypt Single Variables

Ansible Vault can encrypt **individual variables** inline:

ansible-vault encrypt_string 'supersecret' --name 'db_pass'

Output:

```
db_pass: !vault |
        $ANSIBLE_VAULT;1.1;AES256
        656165386264663735346...
```

🚨 Tips

Task	Command
Encrypt all vars in file	`ansible-vault encrypt <file>`
Inline encryption	`ansible-vault encrypt_string`
Prompt for password	`--ask-vault-pass`
Automate password entry	`--vault-password-file vault.txt`