

- [简介](#)
- [Ansible-vault常用操作](#)
- [Ansible-vault配置示例](#)

简介

在使用ansible的过程中，不可避免的会存储一些敏感信息，比如在变量文件中存储帐号密码信息等。

ansible通过ansible-vault命令行工具来提供对敏感文件的加密和解密。

ansible-vault可以创建、加密、解密和查看文件。其可以加密任何ansible使用的文件，包括inventory文件，playbook中调用的变量文件等。

Ansible-vault常用操作

1. 创建加密文件

```
ansible-vault create file
```

2. 编辑加密文件

```
ansible-vault edit file
```

3. 重置密码

```
ansible-vault rekey file
```

4. 加密已有文件

```
ansible-vault encrypt file
```

5. 解密文件

```
ansible-vault decrypt file
```

6. 查看文件

```
ansible-vault view file
```

Ansible-vault配置示例

1. 创建一个user.yml的变量文件，内容如下:

```
username: "user1"  
pwhash: "$1$GkTPu7we$ZZtdsLPIHkS.fmoVcn3v51"
```

2. 加密上面创建的变量文件:

```
# ansible-vault encrypt user.yml  
New Vault password:  
Confirm New Vault password:  
Encryption successful
```

3. 编写playbook文件如下:

```
- name: create user accounts for all our servers  
  hosts: test  
  become: True  
  remote_user: ansible  
  vars_files:  
    - user.yml  
  tasks:  
    - name: Creating user from user.yml  
      user:  
        name: "{{ username }}"  
        password: "{{ pwhash }}"
```

4. 执行playbook

```
# ansible-playbook create_user.yml --ask-vault-pass  
Vault password:
```

也可以通过如下操作执行playbook:

```
echo redhat > vault-pass  
chmod 600 vault-pass  
  
ansible-playbook create_user.yml --vault-password-file=vault-pass
```