

Introduction

Le Vault Ansible est un outil de gestion de secrets et de protection des données sensibles telles que les clés d'API, les certificats et les mots de passe. Il permet de stocker ces informations de manière sécurisée et d'y accéder de manière centralisée.

Objectif du TP

L'objectif de ce TP est de créer un playbook Ansible pour déployer le SGBD MariaDB sur le nœud "host01" en utilisant des variables chiffrées avec Vault.

Étape 1 : Configuration de l'environnement

Nous allons créer un dossier de projet Ansible et configurer l'inventaire. Ouvrez un terminal et exécutez les commandes suivantes :

```
mkdir ansible-project
cd ansible-project
touch inventory.yml
```

Ensuite, ouvrez le fichier "inventory.yml" avec votre éditeur de texte préféré et ajoutez les nœuds suivants :

```
all:
  children:
    master:
      hosts:
        master01:
    hosts:
      host01:
      host02:
      host03:
```

Prérequis :

Avant de commencer, assurez-vous que les machines sont correctement configurées et que Ansible est installé sur le nœud de contrôle master01.

Étape 2 : Création du fichier Vault

Pour stocker les informations sensibles telles que le mot de passe de la base de données, nous allons créer un fichier Vault. Pour ce faire, ouvrez un terminal sur le nœud de contrôle et tapez la commande suivante :

```
ansible-vault create mariadb_vault.yml
```

Cette commande ouvre un éditeur de texte dans le terminal. Vous pouvez maintenant entrer les informations sensibles, telles que le mot de passe de la base de données :

```
mariadb_user: root
mariadb_password: MonMotDePasseSecret
```

Enregistrez le fichier en quittant l'éditeur de texte.

Étape 3 : Configuration du playbook

Maintenant que le fichier Vault est créé, nous allons configurer notre playbook Ansible pour déployer MariaDB sur le nœud host01. Créez un nouveau fichier playbook nommé "deploy_mariadb.yml" sur le nœud de contrôle master01 et ajoutez le contenu suivant :

```
---
- name: Deploy MariaDB on host01
  hosts: host01
  become: true

  vars_files:
    - mariadb_vault.yml

  tasks:
    - name: Install MariaDB
      yum:
        name: mariadb-server
        state: present

    - name: Start MariaDB service
      systemd:
        name: mariadb
        state: started

    - name: Secure MariaDB installation
      command: mysql_secure_installation
      args:
        stdin: "{{ mariadb_password }}"
```

Dans ce playbook, nous avons configuré une tâche pour installer MariaDB, démarré le service et sécuriser l'installation. Nous avons également spécifié le fichier Vault que nous avons créé précédemment.

Étape 4 : Exécution du playbook

Nous pouvons maintenant exécuter notre playbook pour déployer MariaDB sur le nœud host01. Pour ce faire, ouvrez un terminal sur le nœud de contrôle et tapez la commande suivante :

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

Cette commande exécute le playbook et demande le mot de passe du Vault pour accéder aux informations sensibles.

Conclusion :

Dans ce TP, nous avons appris à utiliser Ansible Vault pour stocker les informations sensibles de manière sécurisée et à les utiliser dans nos playbooks. Nous avons également déployé MariaDB sur le nœud host01 en utilisant les informations stockées dans le Vault.