ANSIBLE

Table des matières

Installation & Configuration ANSIBLE :

Apt install ansible

Le fichier inventory est crucial car il permet à Ansible de connaître les serveurs sur lesquels exécuter les tâches définies dans les playbooks.

Nano inventory

```
[webservers]
192.168.1.206 ansible_user=theo ansible_ssh_private_key_file=~/.ssh/id_rsa
```

192.168.1.206 :

- C'est l'adresse IP du serveur cible que vous souhaitez gérer avec Ansible.
- Ansible se connectera à ce serveur pour exécuter les commandes et les playbooks.

ansible_user=theo :

- Spécifie le nom d'utilisateur SSH (theo) que Ansible utilisera pour se connecter au serveur distant.
- Cela signifie que toutes les commandes seront exécutées avec l'utilisateur theo.

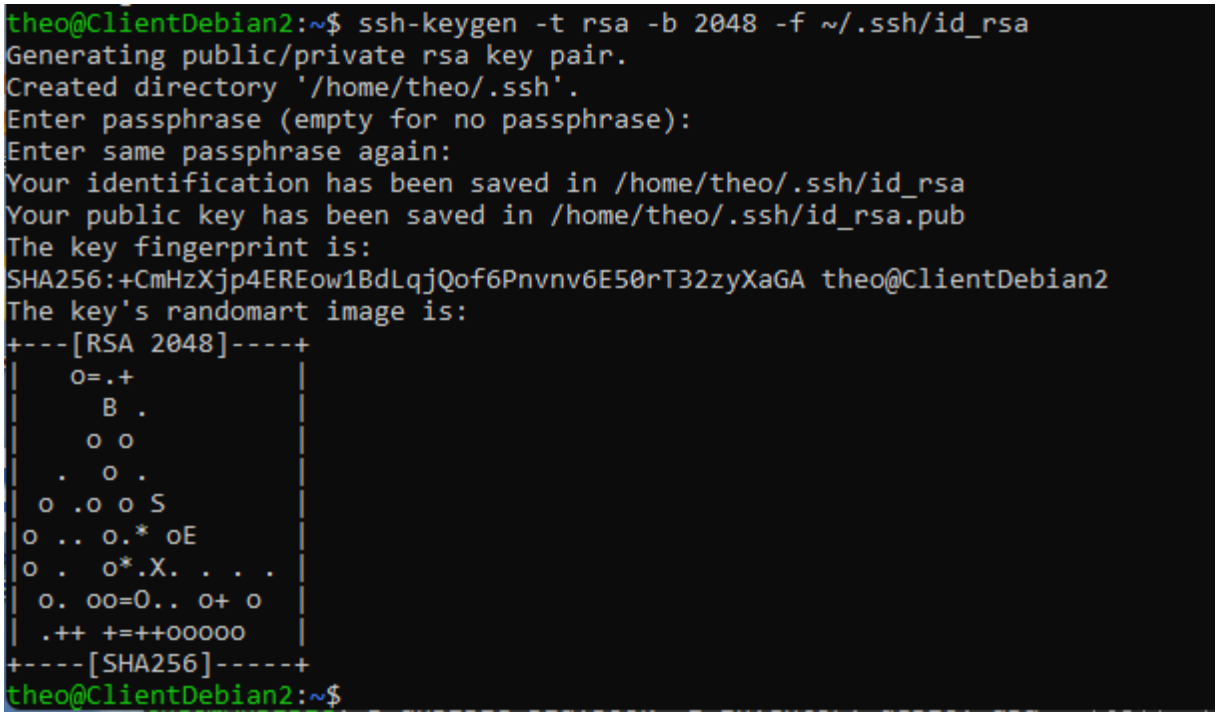
ansible_ssh_private_key_file=~/.ssh/id_rsa :

- Indique à Ansible d'utiliser une clé privée spécifique pour s'authentifier auprès du serveur via SSH.
- Ici, ~/.ssh/id_rsa est le chemin vers la clé privée sur votre machine locale.
- Cette clé doit correspondre à la clé publique qui a été copiée sur le serveur distant .
- En utilisant une clé SSH, vous évitez d'avoir à entrer un mot de passe pour chaque connexion, ce qui est crucial pour l'automatisation.

Configuration de l'accès SSH pour Ansible :

Vous devez vous assurer que la connexion SSH sans mot de passe est configurée pour chaque serveur cible afin d'automatiser les tâches sans interruption.

Générer une clé SSH sur le serveur avec ansible et le serveur cible :



```
theo@Ansible:~$ ssh-keygen -t rsa -b 2048 -f ~/.ssh/id_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/theo/.ssh/id_rsa
Your public key has been saved in /home/theo/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:5bFCXTYuhZzXQ+75ATgQyMYzrm8Mrq1kdo29xqUilyQ theo@Ansible
The key's randomart image is:
+---[RSA 2048]----+
|      o .+.o=o.  |
|       B .==ooo  |
|      o + =+.... |
|       o o +.... |
|      . S o   o. |
|   E ++  o     ..|
|   ++o*oo       .|
|  +.o= B.        |
|   o=.+.         |
+----[SHA256]-----+
theo@Ansible:~$ ansible-playbook -i inventory deploy_apache.yml
```

Copier la clé publique sur le serveur distant :

```
theo@Ansible:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub theo@192.168.1.206
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/theo/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
theo@192.168.1.206's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'theo@192.168.1.206'"
and check to make sure that only the key(s) you wanted were added.
```

Ceci permet d'exécuter des commandes root sans demander le mdp cela est utile pour quand on fait une connexion ssh avec un compte autre que root.

```
theo ALL=(ALL) NOPASSWD: ALL
```

Création et exécution d'un Playbook :

Le playbook Ansible (deploy_apache.yml) est un script YAML contenant une liste de tâches à exécuter sur les serveurs cibles.

Nano deploy_apache.yml

```
  GNU nano 7.2
---
- name: Déployer Apache
  hosts: webservers
  become: yes
  tasks:
    - name: Installer Apache
      apt:
        name: apache2
        state: present
        update_cache: yes
```

hosts : webservers : Indique que ce playbook s'applique aux hôtes du groupe webservers.

become: true : Permet d'exécuter les commandes avec des privilèges sudo.

tasks : Liste des actions à exécuter. Ici, on installe Apache

Et ensuite on déploie :

ansible-playbook deploy_apache.yml -i inventory

```
theo@Ansible:~$ ansible-playbook -i inventory deploy_apache.yml

PLAY [Déployer Apache] *********************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [192.168.1.206]

TASK [Installer Apache] ********************************************************************************************
ok: [192.168.1.206]

PLAY RECAP *********************************************************************************************************
192.168.1.206              : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=

theo@Ansible:~$
```

Résultat :

Déployé un site apache2 en HTTPS :

Tout d'abord il faut créer sa clé privée comme ceci a l'aide d'openssl :

sudo openssl genpkey -algorithm RSA -out /etc/ssl/private/selfsigned.key -aes256

Une fois ceci fait il faut rentrer comme indiquer un mot de passe qui permet de déchiffrer cette clé. Une fois ceci fait on peut créer le certificat qui utilisera cette clé il faudra rentrer le mdp défini juste avant :

Il ne reste plus qu'à rentrer toutes les informations relative au certificat le pays, la ville une adresse mail etc...

Une fois ceci fait on peux passer a la configuration du playbook :

```yaml
---
- name: Déployer Apache avec certificat SSL
  hosts: webservers
  become: true
  tasks:
    - name: Générer un certificat auto-signé pour Apache
      openssl_certificate:
        path: /etc/ssl/certs/selfsigned.crt
        privatekey_path: /etc/ssl/private/selfsigned.key
        provider: selfsigned
        selfsigned_not_after: "+365d"
        selfsigned_not_before: "+0d"
        selfsigned_digest: "sha256"

    - name: Activer SSL sur Apache
      command: a2enmod ssl

    - name: Configurer Apache pour utiliser le certificat SSL
      lineinfile:
        path: /etc/apache2/sites-available/default-ssl.conf
        regexp: 'SSLCertificateFile'
        line: 'SSLCertificateFile /etc/ssl/certs/selfsigned.crt'

    - name: Configurer la clé SSL dans Apache
      lineinfile:
        path: /etc/apache2/sites-available/default-ssl.conf
        regexp: 'SSLCertificateKeyFile'
        line: 'SSLCertificateKeyFile /etc/ssl/private/selfsigned.key'
    # 5. Activer le VirtualHost SSL par défaut
    - name: Activer le site SSL par défaut
      command: a2ensite default-ssl
      notify: Restart Apache

  handlers:
    - name: Restart Apache
      systemd:
        name: apache2
        state: restarted
```

On voit que l'on utilise bien les clés créer précédemment pour configurer la clé SSL dans apache2 et pour le certificats. On définit aussi le hachage qui est en sha256 et la période de validité du certificat.

On peut commencer le déploiement :

```
theo@Ansible:~$ ansible-playbook -i inventory deploy_apache.yml

PLAY [Déployer Apache avec certificat SSL] ************************************************************************************************************

TASK [Gathering Facts] ********************************************************************************************************************************
ok: [192.168.1.6]

TASK [Générer un certificat auto-signé pour Apache] ***************************************************************************************************
ok: [192.168.1.6]

TASK [Activer SSL sur Apache] *************************************************************************************************************************
changed: [192.168.1.6]

TASK [Configurer Apache pour utiliser le certificat SSL] **********************************************************************************************
ok: [192.168.1.6]

TASK [Configurer la clé SSL dans Apache] **************************************************************************************************************
ok: [192.168.1.6]

TASK [Activer le site SSL par défaut] *****************************************************************************************************************
changed: [192.168.1.6]

RUNNING HANDLER [Restart Apache] **********************************************************************************************************************
changed: [192.168.1.6]

PLAY RECAP ********************************************************************************************************************************************
192.168.1.6                : ok=7    changed=3    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

theo@Ansible:~$
```

REMARQUE :

DANS CERTAIN CAS IL APACHE2 NE POURRA PAS REDEMARRER CAR IL Y A UN PROBLEME AVEC LE FICHIER DE CONFIG IL SUFFIT DE COMMENTER CETTE LIGNE :

```
#   SSLCertificateFile directive is needed.
#SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
```

CAR SINON DEUX CERTIFICATS SONT PRESENT DANS LE FICHIER DE CONFIG ET CELA PROVOQUE UN CONFLIT

Résultat :

(inconnu)

Validité

Pas avant	Mon, 11 Nov 2024 16:25:45 GMT
Pas après	Sat, 06 Sep 2025 16:25:45 GMT

Informations sur la clé publique

Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	A5:F3:7D:84:D9:96:E5:47:E4:46:9B:5F:AE:ED:6C:2D:53:FE:3D:12:D4:06:29:20:3B:02...

Divers

Numéro de série	1A:69:E6:B5:BD:26:3E:F6:F3:B4:47:60:6F:86:24:AF:C4:15:69:04
Algorithme de signature	SHA-256 with RSA Encryption
Version	3
Télécharger	

Empreintes numériques

SHA-256	CD:1A:00:DE:BD:0E:F6:E2:A1:8A:0A:39:4A:0F:4F:2B:DE:CC:AF:1A:CB:89:0D:E8:52:...
SHA-1	20:40:79:E6:9C:C8:4D:93:74:AC:52:23:52:24:B5:84:3F:7E:FA:47

Identifiant de clé du sujet

ID de clé	8D:A5:AC:EA:94:8E:7F:80:29:1B:6F:78:0B:A6:8D:C1:69:CE:03:28