

TP1 – Préparation et configuration - correction

Brahim Hamdi

Préparation de l'environnement

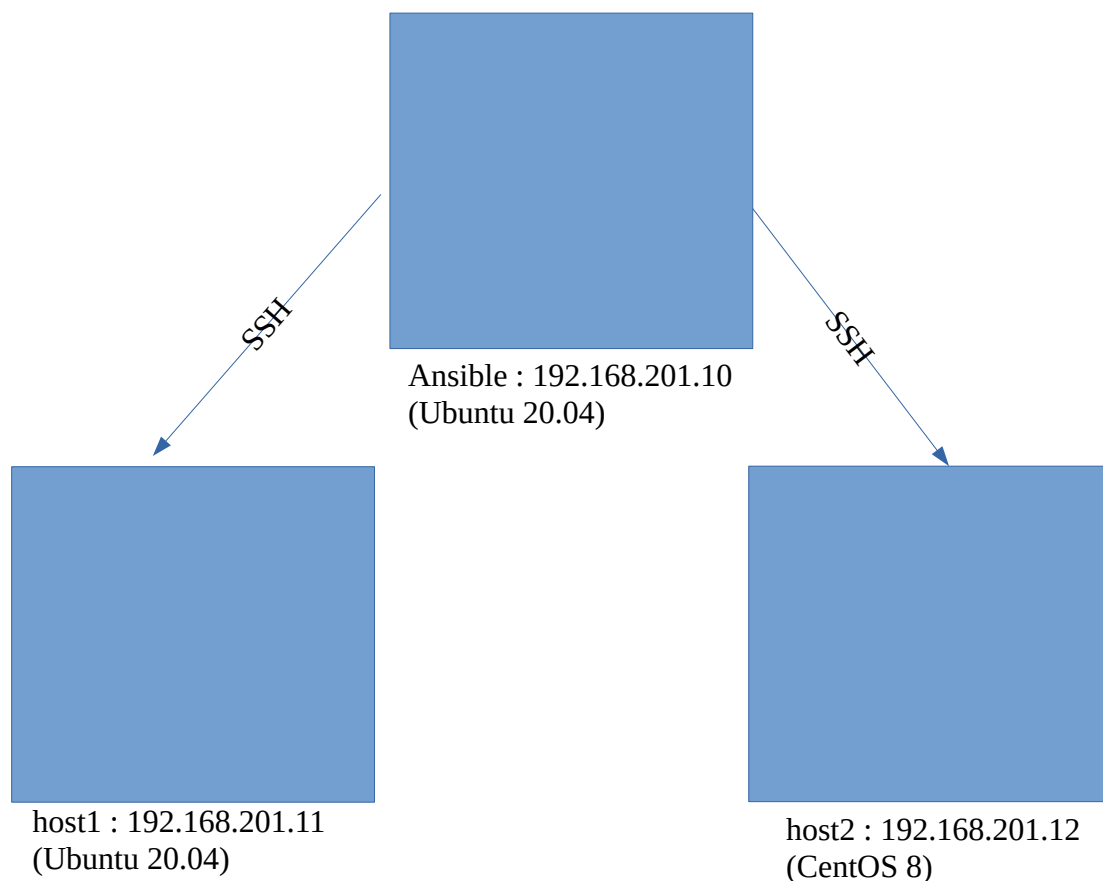
1. Installez les paquets suivants : Git, Virtualbox et Vagrant.

C'est fait.

2. Clonez le dépôt suivant : <https://github.com/brahimhamdi/ansible-lab>

git clone <https://github.com/brahimhamdi/ansible-lab>

3. Déplacez-vous dans le répertoire ansible-lab



- Affichez le contenu du fichier Vagrantfile, et donnez les informations suivantes sur chaque machine virtuelle :

<i>VM</i>	<i>ansible</i>	<i>host1</i>	<i>host2</i>
OS	Ubuntu 20.04	Ubuntu 20.04	CentOS 8
Nom	Ansible	host1	host2
Mémoire	1Go	1Go	1Go
CPU	1	1	1

- Démarrez toutes les VMs.

vagrant up

Installation d'ansible

4. Connectez-vous à la VM ansible.

Vagrant ssh ansible

- Installez la dernière version d'ansible

sudo apt install ansible

- Quelle est la version d'ansible ?

ansible --version

- Donnez le nom et le chemin du fichier de configuration

/etc/ansible/ansible.cfg

- Donnez le nom et le chemin par défaut du fichier inventory

/etc/ansible/hosts

Configuration et test d'accès par mot de passe

5. Depuis la machine ansible, accédez en ssh à hôte1 et hôte2.

Host1 (ubuntu 20.04) : ssh vagrant@192.168.201.11 → ok

Host2 (centos 8) : ssh vagrant@192.168.201.11 → ko (authentification par mot de passe n'est activé) ⇒ il faut l'activer sur le fichier /etc/ssh/sshd_config (directive PasswordAuthentication yes).

6. Ouvrez le fichier inventory.

cat /etc/ansible/hosts

- Que contient ce fichier ?

Toutes les lignes sont commentées et il y a 3 exemples.

- Ajoutez les hôtes cibles avec les paramètres d'accès (username et password)

192.168.201.11 ansible_user=vagrant ansible_password=vagrant

192.168.201.12 ansible_user=vagrant ansible_password=vagrant

7. Installez le paquet sshpass sur ansible

sudo apt install sshpass

- En utilisant le module « ping » d'ansible, testez la connexion aux 2 hôtes.

ansible all -m ping

Génération et accès par clés

8. Générez une paire de clés RSA (passphrase vide)

*Générer la paire de clés ssh sur ansible parce que c'est le client ssh.
ssh-keygen*

- Donnez le nom et le chemin de chaque clé RSA

clé privée : home/vagrant/.ssh/id_rsa

clé publique : home/vagrant/.ssh/id_rsa.pub

- Copiez la clé publique sur les machines cibles, dans le fichier ~/.ssh/authorized_keys.

ssh-copy-id -i .ssh/id_rsa.pub vagrant@192.168.201.11

ssh-copy-id -i .ssh/id_rsa.pub vagrant@192.168.201.12

- Testez l'accès ssh aux machines cibles (accès par clés).

ssh [vagrant@192.168.201.11](ssh://vagrant@192.168.201.11)

ssh [vagrant@192.168.201.12](ssh://vagrant@192.168.201.12)

Maintenant l'authentification ssh est par clés.

9. Faire les modifications nécessaires sur le fichier inventory.

192.168.201.11 ansible_user=vagrant ansible_ssh_private_key_file=~/.ssh/id_rsa

192.168.201.12 ansible_user=vagrant ansible_ssh_private_key_file=~/.ssh/id_rsa

- En utilisant le module ping d'ansible, testez la connexion aux 2 hôtes.

ansible all -m ping