M3102 - TP 1

Configuration interface réseau - Utilisation de SSH

Bruno BEAUFILS

16 novembre 2020

1 Introduction

Au cours de ce module, vous allez devoir installer et surtout gérer des serveurs. Pour ce faire, vous allez travailler à l'aide d'outils de virtualisation.

Le virtualisateur que nous allons utiliser est VirtualBox. Il permet d'exécuter un système invité au sein d'un système hôte.

Le but de cette première séance sera de manipuler la configuration réseau d'une machine Debian dans une machine virtuelle et de se familiariser avec l'outil de connexion à distance `ssh` qui implémente le protocole de même nom et qui vous a été présenté en cours.

2 Préparation de l'environnement

Étant donné les conditions sanitaires du moment, vous allez travailler à distance (chez vous depuis votre ordinateur personnel) sur les machines de l'IUT.

Pour préparer l'environnement de travail :

1. activez votre connection au VPN de l'Université ;
2. connectez-vous via SSH à la machine physique de TP qui vous a été attribuée en pensant de bien activer le transport des connections X11 (option `-X` de la commande `ssh`) ;
3. activez l'environnement de travail via la commande suivante exécutée dans le shell de votre machine à l'IUT

```
source /home/public/m3102/tp1.env
```

Une fois l'environnement de TP activé dans votre shell vous aurez accès à plusieurs nouvelles commandes :

- **`creer_machine_virtuelle`**
- **`demarrer_machine_virtuelle`**
- **`redemarrer_machine_virtuelle`**
- **`arreter_machine_virtuelle`**
- **`information_machine_virtuelle`**
- **`supprimer_machine_virtuelle`**
- **`monter_disque_virtuel`**
- **`demonter_disque_virtuel`**

Le nom de votre machine virtuelle sera `login-tp1` (avec `login` remplacé par votre login de TP). La machine sera stockée dans le repértoire `/usr/local/virtual_machine/infoetu/m3102/login-tp1` (avec `login` remplacé par votre login de TP).

Dans l'énoncé on distinguera 3 machines différentes.

- Votre **ordinateur personnel** : celle depuis laquelle vous travaillez chez vous. Il est probable que ce soit une machine virtuelle Debian GNU/Linux, hébergée sur votre micro-ordinateur, contenant un environnement de travail similaire aux machines de TP de l'IUT.
- La **machine physique de TP** : celle qui vous a été attribuée et sur laquelle le TP est effectué à l'IUT.
- Le **serveur virtuel du TP** : celle que vous allez créer et administrer pendant le TP.

3 Création du serveur virtuel de TP

Créez votre serveur virtuel de TP en exécutant la commande `creer_machine_virtuelle` dans votre shell.

Vous devriez obtenir une sortie de ce genre là :

```
$ creer_machine_virtuelle
Virtual machine 'beaufils-tp1' is created and registered.
UUID: 912c1dbb-3d36-49fd-8455-c79634bc45cc
Settings file: '/usr/local/virtual_machine/infoetu/m3102/beaufils-tp1/beaufils-tp1.vbox'
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VDI'. UUID: b4759f53-6956-4c30-bb2a-4a5379c36553
$
```

Cela vous crée une machine virtuelle ayant 1 Mo de mémoire, un disque dur virtuel de 5 Go sur lequel un version de Debian Buster (10.5) est préinstallée avec 2 utilisateurs :

- `root` avec comme mot de passe `root`
- `user` avec comme mot de passe `user`

Cette machine, qui est votre serveur virtuel de TP, est par ailleurs connectée à un réseau virtuel sur lequel se trouve également votre machine physique de TP (via son interface `vmnet8`).

Démarrez votre machine en exécutant la commande `demarrer_machine_virtuelle` dans votre shell.

Vous devriez obtenir une sortie de ce genre là :

```
$ demarrer_machine_virtuelle
Waiting for VM "beaufils-tp1" to power on...
VM "beaufils-tp1" has been successfully started.
$
```

Attendez quelques instants puis vérifiez votre serveur virtuel de TP

Pour cela vous allez devoir :

1. exécutez la commande **`information_machine_virtuelle`**
   Vous devriez avoir une sortie de ce genre là :

   ```
   $ information_machine_virtuelle
   etat=running
   mac=08:00:27:98:d9:df
   ips-probables=192.168.194.29
   etat-disque-virtuel=libre
   $
   ```

2. accédez à la console de votre machine virtuelle
   Pour cela vous devrez utiliser, depuis votre ordinateur personnel, un client RDP dirigé vers la machine physique de TP. Sous Linux la commande suivante, en remplaçant `arbre` par le nom de la machine physique de TP qui vous a été attribuée, fait l'affaire :

   ```
   rdesktop -k fr arbre.iutinfo.fr &
   ```

4 Modification de la configuration réseau

Actuellement, votre machine virtuelle obtient son adresse IP de façon automatique via le protocole DHCP. Nous allons changer cette configuration pour la fixer à une adresse appartenant au réseau virtuel.

Lisez la page `ip(8)` et utilisez cette commande pour connaître l'adresse IPv4 :

- de l'interface `vmnet8` de la machine physique de TP,

– de l'interface `enp0s3` du serveur virtuel de TP.

De même, déterminez la route par défaut (aussi appelée passerelle) de votre machine virtuelle.

Lisez la page `resolv.conf(5)` et déterminez la configuration DNS de votre machine virtuelle.

Après avoir lue les pages de manuel `interfaces(5)`, `ifup(8)`, rédigez une procédure permettant de changer l'adresse IP de votre machine.

N'oubliez pas d'y inclure la configuration de la passerelle ainsi que du serveur DNS aux valeurs que vous aurez obtenues dans les questions précédentes.

Faites valider votre procédure par votre enseignant, puis appliquez la pour configurer votre serveur virtuel de TP de façon à ce que son adresse soit fixée à :

`192.168.194.10`

Redémarrez la machine virtuelle.

À l'aide de la commande `ping`, vérifiez que :

– les deux machines puissent communiquer entre elles
  – de la machine physique de TP vers le serveur virtuel de TP,
  – du serveur virtuel de TP vers la machine physique de TP ;
– le serveur virtuel peut joindre la machine `www.univ-lille.fr`. On s'assure ici que le serveur virtuel de TP est non seulement capable peut communiquer vers le réseau du campus mais aussi qu'il peut le faire en utilisant des noms plutôt que des adresses IP.

5 Connexion distante

L'utilisation de la console du serveur virtuel de TP n'est pas des plus pratiques (pas de copier/coller, limitation à 80x25 caractères, etc.). Par ailleurs, si vous êtes amenés à administrer des machines, vous souhaiterez éviter le plus possible leur administration directement dans la salle qui les héberge (surtout si ce sont des machines physiques ou virtuelles louées chez un hébergeur).

Nous allons donc utiliser un logiciel de connexion à distance pour administrer le serveur virtuel de TP. Cet outil est `ssh`. Comme vu en cours, il permet la connexion à distance à travers une connexion chiffrée et sécurisée.

Sur votre votre machine physique de TP, supprimez la ligne `StrictHostKeyChecking no`, si elle est présente, du fichier `~/.ssh/config`. Si vous n'avez jamais modifié ce fichier, vous pouvez tout simplement le supprimer.

Première connexion

Lisez la page de manuel `ssh(1)` et trouvez la ligne de commande nécessaire pour vous connecter **de la machine physique de TP vers le serveur virtuel de TP** en tant que l'utilisateur `user`.

En exécutant cette commande, un message similaire au message suivant devrait apparaître :

```
The authenticity of host '192.168.194.10 (192.168.194.10)' can't be established.
ECDSA key fingerprint is SHA256:SQd8rO9+kH/WsLj2A4O1KkBj5FKw9dVYEqmiH42YDUQ.
Are you sure you want to continue connecting (yes/no)?
```

Ne répondez pas `yes` !

Ce message indique que votre client `ssh` ne s'est jamais connecté à la machine virtuelle. Il vous demande alors de vérifier si l'empreinte (*fingerprint* en anglais) du certificat de la machine correspond bien à la machine à laquelle vous voulez vous connecter.

Le but de cette vérification est de vous assurer que vous vous connectez bien à une machine de confiance. En effet, si la machine à laquelle vous tentez de vous connecter n'est pas la votre, mais une machine contrôlée par un tiers malveillant, il pourrait récupérer votre mot de passe.

Lisez la page `ssh-keygen(1)` et trouvez comment afficher, **sur votre serveur virtuel de TP**, l'empreinte de la clé de type ECDSA du, stockée dans le fichier `/etc/ssh/ssh_host_ecdsa_key.pub`.

Vérifiez que cette empreinte correspond à celle que vous avez obtenue, sur votre machine physique de TP, en tentant de vous connecter à la machine virtuelle.

Si c'est le cas, vous pouvez saisir `yes` et établir la connexion.

Déconnectez vous du serveur virtuel de TP et effectuez à nouveau la connexion. Devez-vous à nouveau vérifier l'empreinte ? Pourquoi ?

Simulation d'une attaque

Vous allez simuler ce qui se passerait si un tiers malveillant avait modifié le réseau pour que votre connexion n'aboutisse pas sur votre serveur mais sur un autre (en truquant les réponses du serveur DNS par exemple) ?

Pour cela vous allez modifier les clés du serveur virtuel de TP.

À l'aide de la commande `ssh-keygen`, générez, sur le serveur virtuel de TP, un nouvel ensemble de clés, de type ECDSA, puis redémarrez ensuite son serveur `ssh` à l'aide de la commande `service ssh restart` (ou `systemctl restart ssh`).

Refaites une tentative de connexion. Que se passe-t-il ? Pourquoi ?

Sur votre machine physique de TP, utilisez la commande `ssh-keygen` pour supprimer l'empreinte de l'ancienne clé.

Authentification par échange de clés

Comme vous avez pu le voir dans les exercices précédents, il est possible de se connecter à une machine distante avec `ssh` en fournissant son login et son mot de passe.

Il existe une autre solution pour prouver votre identité au serveur. Cette solution est de vous authentifier à l'aide d'une paire de clés. C'est le même principe que celui utilisé pour la vérification de l'identité du serveur.

Dans cet exercice, vous allez donc vous fabriquer une paire de clés (publique et privée) que vous utiliserez ensuite pour vous connecter à votre serveur, sans avoir à donner votre mot de passe.

Sur votre machine physique de TP et **seulement si vous n'avez pas déjà des clés SSH**, fabriquez une paire de clés en utilisant la commande `ssh-keygen` pour fabriquer des clés de type RSA. Cette clé devra être générée dans le fichier par défaut : `~/.ssh/id_rsa`.

Quand la commande vous le demande, saisissez une *passphrase* pour cette clé. Ce sera le mot de passe de la clé. En **effet, pour plus de sécurité, cette clé sera stockée dans un fichier chiffré**. La passphrase sert alors de clé de chiffrement.

La commande que vous avez utilisée a produit deux fichiers :

- `id_rsa` : c'est votre clé **privée**. Comme son nom l'indique, elle est privée et ne doit **jamais** être communiquée à quiconque ;
- `id_rsa.pub` : c'est votre clé **publique**. Vous pouvez communiquer cette clé. Elle permettra de vérifier, par des moyens cryptographiques, que vous possédez bien la clé **privée** associée.

Pour utiliser cette paire de clés, vous devez fournir **à la machine sur laquelle vous voulez vous connecter** votre clé **publique**. Dans le cas de ssh, un utilisateur peut autoriser une connexion en ajoutant une clé publique au fichier `~/.ssh/authorized_keys` de la machine sur laquelle il veut se connecter.

Lisez la page de `ssh-copy-id(1)` et trouvez comment ajouter la clé publique que vous venez de créer au compte `user` de votre serveur virtuel de TP.

Connectez-vous à votre serveur virtuel de TP en tant que `user` depuis votre machine physique de TP.

Connexion `root`

Sous Debian et par défaut on peut se connecter en tant que l'utilisateur `root` via ssh uniquement si l'authentification n'est pas faite par l'échange de mot de passe. Cette politique de sécurité est fixée par une valeur fixée à la clé `PermitRootLogin` dans le fichier `/etc/ssh/sshd_config`. Elle est justifiée par le choix d'éviter les authentifications interactives (via la saisie d'un mot de passe au clavier par exemple).

Après avoir lu la page `sshd_config(5)` rédigez une procédure vous permettant d'ajouter votre clé publique comme clé autorisée pour l'utilisateur `root` de votre serveur virtuel de TP. La politique de sécurité de Debian doit être la même avant et après l'application de votre procédure.

Faites valider votre procédure par votre enseignant puis appliquez votre procédure et vérifiez que vous pouvez vous connecter depuis votre machine physique de TP vers votre serveur virtuel de TP en tant que `root`.