Département Informatique

TP n°1
Installation d'un serveur
Utilisation de SSH

2016/2017
M3102
DUT info – semestre 3

Au cours de ce module, vous allez devoir installer et gérer une machine serveur. Pour ce faire, vous allez travailler à l'aide d'un outil de virtualisation. Cet outil, VMWare Player, permet d'exécuter un système invité au sein d'un système hôte.

Le but de cette première séance sera d'installer une distribution Debian dans une machine virtuelle et de se familiariser avec l'outil de connexion à distance `ssh` qui implémente le protocole de même nom.

Exercice 1 : Récupération du media d'installation Debian

Sur le site `http://www.debian.org` récupérez une image d'installation en choisissant dans l'ordre

> *Installation par le réseau*
> > *Très petits CD, clefs USB personnalisées, etc.*
> > > *amd64*
> > > > *netboot*
> > > > > `mini.iso`

Exercice 2 : Création de la machine virtuelle

Q 1. Lancez l'outil de virtualisation VMWare Player (`vmplayer`).

Q 2. Créeez une nouvelle machine virtuelle avec les paramètres suivants :

- installation du système depuis une image ISO (vous indiquerez le fichier téléchargé dans l'exercice précédent) ;
- système invité **Linux**, version **Debian 8 64-bits** ;
- nom de la machine virtuelle : **serveur** ;
- emplacement : `/usr/local/virtual_machine/infoetu/votrelogin`.
  Attention : vérifiez bien le chemin, ne créez pas la machine virtuelle sur votre compte, elle va épuiser votre quota ;
- taille de disque : 20 GB ;
- disque séparé en plusieurs fichiers ;
- le reste peut être conservé avec les valeurs par défaut.

Exercice 3 : Installation Debian

Démarrez la machine virtuelle. Si tout va bien, vous devez obtenir l'écran d'installation Debian :

Suivez la procédure d'installation en faisant attention aux points suivants :

- Nom de machine : `serveur`
- Domaine : `local.domain`
- Miroir : **France > debian.polytech-lille.fr**
- Proxy (serveur mandataire) : `http://cache.univ-lille1.fr:3128`

- Méthode de partitionnement : **Assisté - utiliser un disque entier**
- Schéma de partitionnement : **Partition /home séparée**
- **Important!** Dans sélection des logiciels, laissez uniquement **Utilitaires usuels du système**. Pour décocher une case, il faut utiliser la barre espace.
- Installer GRUB sur le secteur d'amorçage

Exercice 4 : Configuration du réseau

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

Q 1. Lisez la page `ip(8)` et utilisez cette commande pour connaître l'adresse IPv4 de l'interface `vmnet8` de la machine physique.

Q 2. De même, déterminez la route par défaut (aussi appelée passerelle) de votre machine virtuelle.

Q 3. Lisez la page `resolv.conf(5)` et déterminez la configuration DNS de votre machine virtuelle.

Q 4. Lisez la page de manuel `interfaces(5)` et configurez votre machine de façon à ce que son adresse soit fixée à :

`aaa.bbb.ccc.128`

Le choix des valeurs `aaa`, `bbb` et `ccc` dépend de la configuration de votre machine physique. Machine virtuelle et machine physique doivent se trouver dans le même réseau.

N'oubliez pas de configurer également la passerelle ainsi que le serveur DNS aux valeurs que vous aurez obtenues dans les questions précédentes.

Q 5. Redémarrez la machine virtuelle et vérifiez qu'elle peut communiquer avec la machine physique (à l'aide de la commande `ping`).

Q 6. Vérifiez que la machine virtuelle peut joindre la machine `www.univ-lille1.fr` (toujours avec la commande `ping`).

Exercice 5 : Premier contact avec le gestionnaire de paquets

Une distribution linux est définie, entre autres, par une sélection de logiciels disponibles. Ces logiciels peuvent être installés à l'aide d'un système de paquets. Dans le cas de Debian, ce système est `apt`.

Q 1. Lisez la page de manuel `apt(8)` et trouvez la commande qui permet de mettre à jour la liste des paquets disponibles.

Q 2. Quelle commande doit on utiliser pour installer l'outil `tree` ?

Exercice 6 : Connexion à distance

L'utilisation de la machine virtuelle dans `vmplayer` n'est pas des plus pratiques (pas de copier/coller, limitation à 80x25 caractères, etc.), en plus, si vous êtes amenés à administrer des serveurs, vous souhaiterez éviter le plus possible leur administration directement dans la salle serveur.

Nous allons donc utiliser un logiciel de connexion à distance pour administrer le serveur. Cet outil est `ssh`. Il permet la connexion à distance à travers une connexion chiffrée et sécurisée.

Pour cela, nous allons devoir installer le service `ssh` sur la machine virtuelle.

Q 1. Recherchez le nom du paquet qui contient le serveur `openssh` et installez le.

Q 2. Recherchez le nom du paquet qui contient le client `openssh` et installez le.

Q 3. Sur votre compte étudiant (et donc sur la machine physique), supprimez la ligne `StrictHostKeyChecking no` du fichier `~/.ssh/config`. Si vous n'avez jamais modifié ce fichier, vous pouvez tout simplement le supprimer.

Q 4. Lisez la page de manuel `ssh(1)` et trouvez la ligne de commande nécessaire pour vous connecter **de la machine physique à la machine virtuelle** en tant qu'administrateur.

En exécutant cette commande, un message similaire au message suivant apparaît :

```
The authenticity of host '[192.168.194.128] (192.168.194.128)' can't be established.
ECDSA key fingerprint is 71:fc:dd:f2:c2:08:d2:f0:a8:24:2c:1c:1b:de:9c:d8.
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.

Q 5. Lisez la page `ssh-keygen(1)` et trouvez comment afficher l'empreinte du fichier `/etc/ssh/ssh_host_ecdsa_key.pub` de la machine **virtuelle**

Q 6. Vérifiez que cette empreinte correspond à celle que vous avez obtenue en tentant de vous connecter à la machine virtuelle.

Q 7. Si c'est le cas, vous pouvez saisir `yes` et établir la connexion.

Q 8. Déconnectez vous de la machine virtuelle et effectuez à nouveau la connexion. Devez-vous à nouveau vérifier l'empreinte ? Pourquoi ?

Q 9. Que se passerait-il si un tiers malveillant avait modifié le réseau pour que votre connexion n'aboutisse pas sur votre machine mais sur une autre [1] ?

Nous allons simuler ce comportement en modifiant les certificats du serveur.

Q 10. Toujours à l'aide de la commande `ssh-keygen`, générez un nouvel ensemble de clés pour le serveur de la machine virtuelle. Redémarrez ensuite le serveur `ssh` à l'aide de la commande `service ssh restart`.

Q 11. Refaites une tentative de connexion. Que se passe-t-il ? Pourquoi ?

Q 12. Utilisez la commande `ssh-keygen` pour supprimer l'empreinte de l'ancienne clé.

Exercice 7 : Authentification `ssh` par clé

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.

Q 1. Utilisez la commande `ssh-keygen` pour fabriquer une paire de clés en utilisant l'algorithme RSA. Cette clé devra être générée dans le fichier par défaut : `~/.ssh/id_rsa`.

Fabriquez cette clé sur votre machine **physique**. 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 son nom sur une machine en ajoutant une clé publique au fichier `~/.ssh/authorized_keys`

Q 2. Lisez la page de `ssh-copy-id(1)` et trouvez comment ajouter la clé publique que vous venez de créer au compte `root` de votre machine virtuelle.

Q 3. Essayez de vous connecter à votre machine virtuelle (en root) depuis votre machine physique.

1. Par exemple, en truquant les réponses du serveur DNS