TP 1 : Les noms et les adresses sous Debian

Jean-Yves COLIN et Bruno LEGRIX

03/01/2018

1 La gestion des noms de machines et du réseau

Le fichier `/etc/hostname` contient le nom de la machine.

La commande `hostname` permet de connaître le nom de la machine, c'est également ce nom qui apparaît au prompt lorsqu'on se connecte en mode console.
La commande `hostname` assortie du commutateur `-d` permet d'obtenir le nom de domaine DNS auquel cette machine est rattachée, assortie du commutateur `-f` elle permet d'obtenir le FQDN (Fully Qualified Domain Name) de cette même machine.

La commande `/etc/init.d/hostname.sh` permet de prendre en compte les modifications faites dans le fichier `/etc/hostname`. En effet, les modifications dans ce fichier ne seront prises en compte par défaut qu'au prochain reboot (de la VM). Exécuter directement `/etc/init.d/hostname.sh` permet de prendre en compte ces modifications sans avoir à rebooter (la VM).

La commande `ifconfig` permet de configurer et d'afficher les informations des interfaces réseau IP. Quand on redémarre la machine, la configuration, réalisée avec `ifconfig`, sera oubliée.

Un rebouclage (loopback) est une interface virtuelle d'un matériel réseau. Ainsi, quand une commande la contacte elle "boucle" en fait vers elle-même sans passer par le réseau extérieur. Ce qui est pratique pour faire des tests d'applications réseau quand il n'y pas de réseau disponible.

La commande `ping` permet de tester l'accessibilité d'une autre machine à travers un réseau IP. La commande mesure également le temps mis pour recevoir une réponse, appelé round-trip time (temps aller-retour).

Le fichier `/etc/hosts` contient une liste d'adresses IP connues d'office et les noms des machines correspondantes. En général, ça concerne la machine et les machines les plus importes du réseau. On met l'adresse IP, puis une tabulation, puis le FQDN, puis un espace et le nom de la machine.

Le fichier `/etc/host.conf` est destiné à spécifier la méthodologie de résolution des noms, c'est à dire comment la convertion noms - adresses IP sera effectuée.
Si on a `order hosts,bind` alors la résolution de noms s'effectuera en premier sur la base de la table `/etc/hosts` puis si le nom de la machine recherchée ne s'y trouve pas, alors la question sera posée au serveur DNS (`bind`).

Si on a `multi on` alors on autorise à associer plusieurs adresse IP à un même nom de machine.

Le fichier `/etc/network/interfaces` contient les paramètres de configuration des interfaces réseau. Il définit l'interface loopback `lo` **(on laisse ces deux lignes !)**. Ceci permet de rendre persistant la configuration des interfaces.

La commande `/etc/init.d/networking restart` permet de prendre en compte les modifications du fichier `/etc/network/interfaces`. Les options `start` et `stop` permettent de démarrer ou arrêter les adresses IP.

La commande `arp` affiche et modifie les entrées du cache ARP ("Address Resolution Protocol"), qui contient une ou plusieurs tables permettant de stocker les adresses logiques IP et leurs adresses physiques MAC. Le commutateur `-a` permet d'afficher les tables en cours du cache ARP de toutes les interfaces. Le commutateur `-d` permet de supprimer une entrée correspondant à une adresse IP spécifique ou une interface spécifique.

La commande `netstat` permet de dresser la liste des sessions TCP actives ou en attente ainsi que les ports UDP que les programmes actifs écoutent.
Invoquée sans arguments, `netstat` se contente de lister toutes les connexions ouvertes, mais cette liste est très verbeuse. On utilise les options suivantes :

- `-t` pour avoir les connexions TCP
- `-u` pour avoir les connexions UDP
- `-p` pour avoir les processus mis en jeu
- `-a` pour avoir les sockets en écoute
- `-n` pour avoir les adresses IP et non les noms des machines
- `-c` pour rafraîchir la liste des connexions en continu.

Les administrateurs système réseau devraient avoir comme réflexe de taper : `netstat -tupan`

La commande `nmap` identifiera les services Internet hébergés par une machine. Il est équivalent à `netstat` mais s'utilise à distance. Il permet de balayer un ensemble de ports classiques d'une ou plusieurs machines distantes, et de lister les ports auquels une application répond aux connexions entrantes. `nmap` est capable d'identifier certaines de ces applications, et parfois la version.
Le commutateur `-A` déclenche les tentatives d'identification des versions.
Il suffit d'installer le paquet `nmap` : `apt-get install nmap`
On l'utilise en tapant : `nmap nomMachine`

Pour voir ce qui se passe réellement sur un réseau, paquet par paquet, on utilise un analyseur de trame (sniffeur).
La commande `tcpdump`, du paquet homonyme, permet toutes sortes de capture de trafic réseau.
Exemple d'utilisation (écoute du `ping`) : `tcpdump -i eth0 icmp`
On installe le paquet `tcpdump`.

2 Travaux pratiques

1) On démarre `master`, nous n'utiliserons pas le fichier `/root/configuration`. Dans l'énoncé du TP, il faut remplacer `.nomDomaine` par votre nom de domaine, pour nous, ça serait `.jycbl.fr`.

2) a) Quel est le nom de la machine *(commande `hostname`)* ?
   Dans le fichier `/etc/hostname`, mettre `master.nomDomaine`.
   Est-ce que la modification a été prise en compte ?

   b) Utiliser la commande `/etc/init.d/hostname.sh`, que retourne `hostname` cette fois ?

   c) Que retournent `hostname -d` et `hostname -f` ?

   d) Dans le fichier `/etc/hosts`, il faut y remplacer `debian` par `master.nomDomaine master`. *Il faut bien respecter la structure de ce fichier !*
   Que retournent `hostname -d` et `hostname -f` ?

3) Dans le fichier `/etc/host.conf`, vérifier qu'on a bien les options

```
order hosts,bind
multi on
```

   Si une option manque, il faut la rajouter sur une ligne.

4) En utilisant la commande `ifconfig`, vérifier si eth0 est bien reconnue, quelles sont ses adresses MAC et IP ?
   Quelle est l'adresse de rebouclage de cette machine ?
   Quel est le nom de rebouclage de cette machine ?

5) Utiliser la commande `ping`, pour tester 127.0.0.1, 127.0.1.1 et `master`.
   Ces deux adresses IP correspondent à quoi ?
   La première ligne (retournée par `ping`) donne quelle information ?
   On teste aussi `ping6 ::1` et `ping6 adresse_link-local%eth0` où `adresse` désigne l'adresse IPv6 "link-local".

6) a) Analyser le fichier `/etc/network/interfaces`. L'adresse IP d'`eth0` est définit dans quel mode ? On met en commentaire les deux lignes contenant le mot `eth0`.
   On va utiliser une adresse IP statique pour la première interface ethernet (`eth0`), lancée au démarrage :

```
auto eth0
iface eth0 inet static
   address 192.168.1.10
   netmask 255.255.255.0
   gateway 192.168.1.1
```

   A quoi correspondent toutes ces options ? Est-ce que ces changements ont été pris en compte ?

   b) Tester la commande `/etc/init.d/networking restart`. Donner la suite de commandes.

   c) On teste `ping` sur `192.168.1.10` et sur `master`. Remarques ?

7) On rajoute dans le fichier `/etc/hosts` une ligne ayant la correspondance du nom de la machine et de l'adresse IP `192.168.1.10`. On refait les tests précédents, on change l'ordre des lignes contenant les deux adresses IP de notre machine, et on note les différences. Bien faire attention de respecter la structure du fichier de configuration, et rajouter bien une ligne avec l'adresse IP `192.168.1.10`.

   Une fois le test fait, il faut garder la ligne

   `192.168.1.10 master.nomDomaine master`

   Et effacer l'autre ligne, puis on peut passer à la suite.

8) a) Il faut arrêter `master` avec la commande `halt`. Pour cloner, il suffit d'aller dans le menu "Machine" de VirtualBox, en donnant un nouveau nom `client20` en n'oubliant pas de demander de réinitialiser l'adresse MAC. Le clone est intégral.

      On démarre `master` et `client20`.

   b) Sur `client20`, il faut changer le nom de la machine (elle est dans le même domaine), et son adresse IP (`192.168.1.20`). On vérifie.

   c) On teste `ping` sur `192.168.1.10`. Ca marche ? Pourquoi ?

   d) On teste `arp -a` sur les deux machines. Quelle information retrouve-t-on ? Quel problème a-t-on ? Pourquoi ?

   e) Sur `client20`, on teste `ping master`. Ca marche ? Pourquoi ? Quelle est le rajout qu'il faut faire ? Le faire et retester.

      Que donne maintenant `arp -a` ?

   f) Sur `master`, on teste `ping client20`. Remarques ?

9) Les commandes `netstat`, `nmap` et `tcpdump` :

   a) Quelles sont les connexions Internet actives avec serveurs sur `master` ? *(commande `netstat`)* A quoi correspondent les autres connexions (sans serveurs) ouvertes ?

      On lance la commande `nc -l -p 900`, puis réutiliser la commande `netstat -tupan`.

      > On peut ouvrir plusieurs sessions en même temps. Il suffit d'enfoncer en même temps les touches `Alt` et `F2` (on note `Alt+F2`). Pour revenir sur la première session : `Alt+F1`.

   b) A partir de `client20`, en utilisant `nmap`, qu'on aura préalablement installé, on identifie les services de `master`, avec et sans le commutateur `-A`.

      Remarques ?

   c) On installe le paquet `tcpdump` sur `client20`, puis on écoute le ping, et de `master` on fait un `ping` sur `client20`.

      Comment fonctionne le `ping` ?