TP DNS

Olivier AUBERT

2001

1 Présentation du TP

On va s'intéresser aujourd'hui à la résolution de noms dans le réseau Internet. Ce TP comporte trois grandes parties :

- interrogation d'un serveur DNS.
- configuration de la résolution de noms sur une machine.
- installation d'un serveur pouvant gérer un sous-domaine.

2 Interrogation de DNS

Plusieurs outils sont disponibles pour interroger les serveurs DNS. Le plus ancien, et encore le plus courant, est `nslookup`. `host` propose une interface en ligne de commande.

L'outil le plus performant, qui tend à remplacer `nslookup` actuellement, est `dig`. Nous l'utiliserons notamment pour tester le bon fonctionnement des serveurs que nous installerons.

Pour afficher la totalité des informations disponibles sur une zone, il faut spécifier une requête du type `axfr` (Zone Transfer).

3 Configuration de la résolution de noms

Consulter les pages de manuel pour découvrir la syntaxe des fichiers de configuration suivants :

- `/etc/nsswitch.conf`
- `/etc/resolv.conf`
- `/etc/host.conf`

Le premier fichier indique quelles sont les différentes méthodes d'accès aux services de nommage (au sens large, i.e. comprenant également les utilisateurs, les groupes, etc). Les deux derniers concernent plus spécifiquement le nommage de machines, et la manière d'interroger les serveurs DNS.

Pour ce TP, nous configurerons les machines de manière à aller interroger le serveur DNS installé en local. Vérifiez que le fichier `resolv.conf` notamment contient les informations correctes.

4 Configuration d'un serveur

Supprimez et réinstallez le paquetage `bind` à partir du serveur `134.214.90.7`. Le répertoire des fichiers de configuration est `/etc/bind`. Le (re)démarrage et l'arrêt du serveur s'effectuent par le biais du script `/etc/init.d/bind`.

Le format du fichier de configuration `named.conf` est documenté dans sa page de manuel. Celui des fichiers de zones est documenté dans la page de manuel de `named`. Il est conseillé de s'inspirer de la syntaxe des fichiers déjà existants.

Les messages d'erreur de named se trouvent dans le fichier `/var/log/daemon.log`. Il est utile d'en vérifier périodiquement le contenu, afin de s'assurer que tout fonctionne correctement.

4.1 Informations d'administration

Vous avez à votre charge un parc (virtuel) de machines. Si vous êtes situé sur la machine `134.214.89.xx`, vous disposez des adresses IP du réseau `192.168.xx.0`. Si vous êtes situé sur la machine `134.214.90.xx`, vous disposez des adresses IP du réseau `192.168.1xx.0`.

Les deux TLD pour ce TP seront `tp11` et `td4`. Un serveur racine maître pour chacun de ces deux domaines sera déterminé au début de la séance. Chaque binôme devra alors aller informer l'administrateur du serveur racine des caractéristiques de son server DNS (adresse IP et nom de réseau).

Chaque binôme créera un domaine portant le nom d'un des binômes (ou bien deux domaines, avec le nom de chaque binôme, s'il y a des jaloux), et y référencera un certain nombre de machines. Ainsi, on obtiendra un nommage complet du type `prenom1.nom.tp11`, `prenom2.nom.tp11`, etc. Votre propre serveur DNS (i.e. l'adresse IP du type `134.214.xx.xx`) aura pour nom `dns.nom.tp11`.

4.2 Installation d'un serveur primaire

Créez le fichier de zone correspondant au domaine que vous administrez. Vous préciserez votre propre adresse mail comme adresse de l'administrateur. Déclarez cette zone dans le fichier `named.conf` et redémarrez le serveur.

Modifiez également le fichier `/etc/bind/db.root`, en déclarant l'adresse IP du serveur primaire de votre salle comme unique serveur racine (`A.ROOT-SERVERS.NET.`), et en supprimant toutes les autres adresses.

Vous devriez alors pouvoir tester votre configuration par la commande

```
dig @localhost nom.tp11. a
```

pour afficher l'ensemble des adresses déclarées sur votre domaine.

Testez également que vous pouvez accéder aux données des autres binômes, en demandant également la liste de leurs adresses. Il peut être intéressant dans cette phase d'utiliser l'analyseur de réseau `ethereal` afin de voir les interactions intervenant entre le serveur DNS local et le serveur primaire.

Vous pouvez à ce niveau déclarer votre propre nom de domaine comme domaine par défaut dans `resolv.conf`.

4.3 Installation d'un serveur secondaire

Nous allons installer un serveur secondaire redondant, permettant d'améliorer la tolérance au pannes du système. Pour cela, passez un accord avec le binôme voisin pour devenir serveur secondaire de son domaine (et inversement). Il ne faut pas oublier d'indiquer cette information dans le fichier de zone. Vérifiez que la mise à jour des informations s'effectue correctement.

Coupez ensuite un des serveurs primaires, et vérifiez que l'information concernant le domaine qu'il maintenait est toujours disponible via le serveur secondaire (attention aux problèmes de cache).

4.4 Mise en place de la résolution inverse

Pour assurer la résolution de noms inverse (traduction d'adresses IP en nom symbolique), il est nécessaire de créer un pseudo-domaine `xx.168.192.in-addr.arpa` qui contiendra des enregistrements de type PTR. Pour cela, inspirez-vous de l'exemple déjà mis en place pour le réseau `127.0.0.1`.

L'interrogation de la résolution de noms inverse s'effectue via la commande `dig -x 192.168.xx.yy`.