TD1

DNS d*omain name system*

Mise en pratique de la notion de serveur de noms. Installation d'un serveur DNS « à cache seul », d'un serveur DNS menteur et d'un serveur DNS maitre[1] *d'une zone dans le local.*

Le temps imparti pour cette manipulation (exposé oral compris) est de l'ordre de 4h.

***Conseil :** Au fur et à mesure de vos travaux complétez un document reprenant toutes vos manipulations. Insérez-y les contenus de vos fichiers de configuration et expliquez vos démarches et/ou les problèmes que vous avez rencontrés ainsi que les solutions et les moyens utilisés afin de les résoudre.*

Ce document vous sera bien utile pour vos révisions.

Lectures

Les lectures suivantes pourront vous être utiles.

- ✗ Le syllabus du cours
- ✗ Formation Linux "élémentaire" — sur base de Debian — voir la formation de Delattre (depuis 2002) *(lien mort à remplacer)*
- ✗ Voir Hunt, G. (Janvier 2000). TCP/IP Administration des réseaux. O'REILLY, 3e édition. ISBN : 2-84177-221-7 Épuisé. pp 175-179
- ✗ La documentation locale telle que les pages de manuel (*man named*, *man named.conf*, *man dig* par exemple) et le contenu du répertoire `/usr/share/doc/bind`

1 Ancienne orthographe « maître » http://www.renouvo.org/info.php?id=1356

Serveur DNS

Serveur DNS à cache seul

Implémenter sur chaque machine un serveur DNS à cache seul. Vous vous baserez sur :

- ✗ le syllabus, les *slides*, les références ;
- ✗ les *how-to* (bind9, dig…) ;
- ✗ (les pages de manuel `man named.conf` par exemple).

Il s'agit donc bien d'installer un programme qui se chargera de faire la résolution de noms — la traduction d'un nom internet *exemple.org* en une adresse IP — et vice versa.

Vous testerez un maximum de « notions ». Par exemple ;

- ✗ visualisation du cache de `named ;`
- ✗ (contrôle par `rndc`) ;
- ✗ la commande `digo`[2] en détail.

> Avant de commencer, renseignez-vous sur le gestionnaire de paquets — le programme permettant d'installer des programmes — debian. Il s'agit de **apt**.

Bref pas à pas

La démarche se résume en une série de vérifications (dépendantes de la version du logiciel installé) car *debian* fait (presque) tout le boulot lors de l'installation du paquet.

1. Installation[3] du paquet *bind<i>* (ou *named*).
2. Vérification de la localisation des divers fichiers de configuration. Ils se trouvent généralement dans un répertoire du type `/etc/bind/`.
   - `named.conf`, fichier de configuration de base,
     - Vous pourrez paramétrer `bind` afin qu'il soit plus loquace, pour ce faire ajouter une section *logging*[4] de la forme,

```
logging {
    category default { default_syslog; default_debug; };
    category security { default_syslog; default_debug;   };
    category database { default_syslog; default_debug;   };
    category resolver { default_syslog; default_debug;   };
    category queries { default_syslog; default_debug;    };
    category unmatched { null ; };
};
```

2 Il est probable qu'il faille intaller `dig`, la commande se trouve dans le paquet `dnsutils`.

3 Avant d'installer un paquet, renseignez vous bien sur le gestionnaire de paquet *debian.*

4 Sous `debian`, ça se passe dans le fichier *`etc/bind/named.conf.options`*

        - Attention avec ces options, vos log deviennent très verbeux… pensez à commenter ces options avant de quitter le laboratoire.
    - `db.root`, `db.local`, ...
3. Démarrage du dæmon, `systemctl`[5] `start bind9` et vérification éventuelle de son existence via un `ps aux | grep named`
4. Configuration du (d'un) résolveur. Édition du fichier `/etc/resolv.conf` signalant quel serveur DNS interroger[6]
5. Test du serveur via les commandes `ping`, `dig`, ...

Serveur DNS menteur

Un serveur DNS peut[7] mentir ou bloquer des résolutions de noms[8].

Arrangez-vous pour que votre serveur DNS bloque http://facebook.com et redirige http://google.com vers http://ddg.gg.

Serveur DNS maitre

Implémentez un serveur maitre pour la zone `my.esigoto.info` et la zone inverse. Mettez-y quelques champs A, AAAA et CNAME ainsi qu'un champ TXT.

Qu'écrire dans un champ TXT ?

Quelles seraient de « bonnes » valeurs pour les champs MX ?

5 Il existe plusieurs manières de faire, principalement : systemctl et service (vous pouvez choisir tout en sachant que la commande service n'est pas disponible « partout »).

6 Attention, dès lors que les paramètres réseaux sont reçus *via* dhcp, le fichier se met à jour automatiquement. Dans le cadre de la manipulation, le (re)modifier régulièrement peut suffire, sinon, ce référer à la remarque dans la section consacrée au fichier resolv.conf dans le syllabus (vers la p 57).

7 « pouvoir » prend ici le sens d'être capable de mentir pas qu'il en a l'autorisation. Posez-vous les questions des implications politiques d'un DNS menteur ou bloquant.

8 Lire à ce sujet http://namok.be/blog/?post/2016/10/18/quand-ton-serveur-dns-te-bloque-ou-te-ment et http://namok.be/blog/?post/2017/03/05/mise-en-place-dns-menteur