Fonctionnement et Administration d'un serveur de noms

McInfo4 - Réseaux

Département d'informatique
IUT Bordeaux 1

Janvier 07

Rôle d'un serveur de noms

DNS : Domain Name Server (Paul Mokapetris, 1983)

- Rôle : établir une correspondance entre
  - adresses IP, par exemple `147.210.94.197`
  - noms de *domaines*, `www.info.iut.u-bordeaux1.fr`
- Résolution, résolution inverse
- et plus généralement, trouver des informations à partir d'un *nom de domaine* (par exemple liste des échangeurs de courrier).

Système réparti sur des centaines de milliers de serveurs DNS

Organisation générale

Organisation hiérarchique, délégation

- quelques “serveurs racine” connaissent les serveurs des “top-level domains” (fr, org, com, net, etc)
- le serveur de “.fr” connait le serveur pour “u-bordeaux.fr”, qui connait celui de “iut.u-bordeaux.fr” etc.
- pour chaque domaine, il y a un serveur primaire et un ou plusieurs serveurs secondaires, qui font autorité (authoritative answer)
- les informations peuvent être conservées par d’autres serveurs intermédiaires (caches)

Fonctionnement

- Un client interroge un serveur qu'il connait (par exemple le DNS indiqué par le FAI)
- Deux type de serveurs
  - récursif : s'occupe de trouver une réponse et la transmet au client
  - itératif : renvoie le client sur un autre serveur.

Exemple de résolution

Un poste du département veut connaitre l'adresse de `www.labri.fr`

- le poste client interroge un DNS local (172.16.95.6)
- celui-ci interroge un serveur racine, qui lui donne l'adresse d'un serveur pour ".fr".
- il demande à ce serveur l'adresse du DNS pour "labri.fr"
- il demande au DNS du Labri l'adresse de "www.labri.fr"
- il fournit la réponse au client.

Remarques

- En réalité, certaines étapes ont pu être évitées (données mémorisées en cache, comme l'adresse du serveur de ".fr")
- le serveur DNS local agit comme *mandataire* (proxy) pour le client.
- Ici il fonctionne en mode récursif : il se charge de la résolution pour le compte du client.

La résolution inverse

A partir d'un numéro IP, trouver un nom de domaine.

- Même principe, mais à l'envers :
  - le nom le plus générique est à droite,
  - la partie générale d'un numéro IP est à gauche.
- On retourne donc les adresses : 147.210.94.203 devient donc 203.94.210.147.in-addr.arpa.
- délégation pour les zones ".in-add.arpa", ".147.in-addr.arpa", ".210.147.in-addr.arpa", etc.

Remarque

Remarque : cette astuce

- permet de traiter de façon homogène la résolution directe et la résolution inverse
- repose sur le découpage des adresses IP calé sur des frontières d'octets (classes A, B et C)

Or le routage "sans classe" (CIDR - Classless Inter-Domain Routing) est une technique standard depuis les années 90.
Comment faire la délégation de DNS pour le sous-réseau 147.210.94.192/28 ?

Protocoles

Echanges par

- UDP quand c'est possible, (requêtes courtes) pour des raisons d'efficacité
- par TCP sinon (transfert de zones).
- Port serveur $= 53$, port client > 1023
- serveur à serveur UDP : port 53 à 53.
- serveur à serveur tcp : > 1023 à 53

Au département

Au département,

- les postes clients sont non-routables (adresses privées)
- donc pas de communication UDP directe avec l'extérieur
- a priori, les postes clients doivent passer par un proxy interne
- d'où nécessité d'un DNS local.

Utilisation de caches

- souci d'efficacité : on réutilise les informations connues
- stockage dans des "caches"
- Mais les informations peuvent changer. Techniques :
  - durée de vie déclarée
  - numéros de version

Redondance

Objectif : résistance très forte aux pannes

- disponibilité : plusieurs serveurs “autoritatifs” pour un même domaine
- serveur primaire, serveurs secondaires.
- Le serveur primaire notifie les changements aux serveurs secondaires
- les serveurs secondaires interrogent le serveur primaire

En pratique

- Implantation de serveurs secondaires sur des réseaux éloignés (petits arrangements entre administrateurs).
- réglage des durées de vies, et délais d’interrogation.

Sous Unix

- L'adresse des DNS peut être fournie par DHCP
- Sinon, on la met dans /etc/resolv.conf

Exemple :

```
search maison.net
nameserver 10.1.1.3
```

Serveur : déclaration de zone “maison.net”

```
@   IN   SOA wallace.maison.net. admin.maison.net. (
                        2       ; Serial
                   604800       ; Refresh
                    86400       ; Retry
                  2419200       ; Expire
                   604800 )     ; Negative Cache TTL
          IN NS       wallace.maison.net.
          IN MX       10 wallace

wallace IN       A          10.1.1.254
          IN       MX         10 wallace

mcgraw    IN       A          10.1.1.253

www       IN       CNAME      wallace
```

Principales déclarations

- IN SOA (start of auhority) indique
  - Le serveur primaire
  - Le responsable (adresse avec . au lieu de @)
  - Durée de vie des infos
- IN NS : déclaration de serveur(s) de nom
- IN A : déclaration d'adresse
- IN MX : déclaration d'échangeur de courrier

Fichier de configuration général

Dans le fichier de configuration**?** “/etc/bind/named.conf”

```
...
zone "maison.net" {
        type master;
        file "/etc/bind/db.maison";
};
...
```

Déclaration de zone inverse

Dans /etc/bind/named.conf**?** :

```
zone "1.1.10.in-addr.arpa" {
  type master;
  file "/etc/bind/db.maison-rev";
};
```

Contenu de zone inverse

Dans /etc/bind/bd.maison.rev**?** :

```
@       IN      SOA     wallace.maison.net. admin.maison.net. (
                              4         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
          IN        NS      wallace.maison.net.

254       IN PTR    wallace.maison.net.
253       IN PTR    mcgraw.maison.net.
```

DNS et courrier

- Les DNS est indispensable au système de transmission du courrier
- envoi d'un mail à "xyz@site.fr" : le courrier est transmis au serveur de courrier de site.fr.
- information donnée par le champ MX (mail exchanger) de site.fr.
- il peut y avoir plusieurs MX (MX de secours), priorités.

Sous-domaines

Un sous-domaine peut être géré par le même serveur, ou par un autre, ou par plusieurs.
Déclaration par la directive NS

```
niche IN NS wallace.maison.net.
      IN NS dns2.maison.net.
```

Travaux pratiques

- Configurer un serveur avec un domaine et quelques (=3) machines. Logiciel bind, fichiers de config. dans /etc/bind
- Vérifier son fonctionnement (nslookup, dig), configurer un client, observer le trafic (tcpdump)
- Ajouter un sous-domaine avec quelques (=2) noms, géré par un autre serveur. Observer le trafic lors des interrogations.