Administration d'un serveur de noms

McInfo4 - Réseaux

Département d'informatique
IUT Bordeaux 1

Janvier 2008

Configuration des clients

Les clients interrogent des serveurs de noms.

Lesquels ?

- liste de DNS fournie par DHCP
- liste indiquée dans `/etc/resolv.conf`

Exemple `/etc/resolv.conf`

```
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
```

Start Of Authority

L'enregistrement Start Of Authority (SOA) indique

- Le serveur primaire de la zone
- Le responsable (adresse avec . au lieu de @)
- la durée de vie des infos

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

Important : augmenter le serial number après chaque modification du fichier.

Déclarations

- A : adresse IP
- MX : échangeur de courrier
- CNAME : synonyme (canonical name)

```
wallace IN      A       10.1.1.254
       IN      MX      10 wallace
; ------------------------------
mcgraw  IN      A       10.1.1.253
; ------------------------------
www     IN      CNAME   wallace
```

Fichier de configuration général

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.
```

PTR (pointeur) : nom associé à une adresse.

Protocoles

Échanges 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,

- postes clients non-routables (adresses privées)
- les postes clients transmettent leurs requêtes à un serveur mandataire (proxy) interne

Utilisation de caches

- réutilisation des informations déjà connues (efficacité)
- stockage dans des "caches"
- Mais les informations peuvent changer. Techniques :
  - durée de vie déclarée
  - numéros de version

Redondance

Objectif : résistance aux pannes

- disponibilité : plusieurs serveurs "autoritatifs" pour un même domaine
- serveurs primaire et secondaires.

Mise à jour : quand

- le serveur primaire notifie un changement
- les serveurs secondaires interrogent le serveur primaire

En pratique

- serveurs secondaires sur des réseaux éloignés (arrangements entre administrateurs).
- réglage des durées de vies, et fréquences d'interrogation.

DNS et courrier

Les DNS sont indispensables au système de transmission du courrier

Exemple

envoi d'un mail à `dupont@sav.site.fr` :

- le DNS de `site.fr` fournit l'adresse d'un échangeur de courrier pour `sav.site.fr`
- l'émetteur rentre en contact avec cet échangeur
- l'échangeur dépose le courrier dans la boîte de `dupont`

Remarques

- Les échangeurs sont indiqués par les enregistrements "MX"
- il peut y avoir plusieurs MX, avec un ordre de préférence

Savoir-faire

- Configurer un serveur avec un domaine et quelques (3 ?) machines. Logiciel bind9, fichiers de configuration 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.