Construction d’un fichier de zone
Déboguage et dépannage

Atelier AfTLD, Yaoundé 2004

Construction d’un fichier de zone

Choisir un nom de domaine:

- **<tld>.ws.trstech.net**

Ecrire le nom et l’adresse IP de votre PC:

- **ns1.<tld>.ws.trstech.net**
- **216.252.236.x**

Créer les sous répertoires sous /etc/namedb:

- **"master" pour les zones primaires**
- **"slave" pour les zones secondaires**

Créer un fichier de zone pour votre nom de domaine:

vi /etc/namedb/master/<tld>.ws.trstech.net

```
$TTL 30m
@   SOA  ns1.<tld>.ws.trstech.net.  admin\@<tld>.ws.trstech.net. (
    2004121701 ; serial
    1h  ; refresh
    15m  ; retry
    4w  ; expire
    5m )  ; nttl

    NS ns1.<tld>.ws.trstech.net.

ns1 A 216.252.236.x
```

Rappel: ne pas oublier '.' après les noms, si ils sont absolus.
Rappel: tout ce qui suit un ';' est un commentaire

Vérification de la zone

Syntaxe:

- **named-checkzone nom_de_la_zone nom_du_fichier_zone**

```
named-checkzone <tld>.ws.trstech.net <tld>.ws.trstech.net
```

Chargemnet de la zone (1)

Modifier /etc/namedb/named.conf et y ajouter votre nouvelle zone:

```
zone "<tld>.ws.trstech.net" {
    type master;
    file "master/<tld>.ws.trstech.net";
};
```

Démarrer le serveur de nom

- **named -c /etc/namedb/named.conf**

Vérifier les erreurs éventuelles

- **tail /var/log/messages**

Chargemnet de la zone (2)

Vérifier que le serveur réponde avec autorité sur la zone:

- **dig @localhost <tld>.ws.trstech.net soa +norec**
- **dig @localhost <tld>.ws.trstech.net ns +norec**

Que remarquez-vous ?

Dépannage

Quels sont les erreurs communes ? RFC1912

- **Zone mal configurée**
  - (oubli de '.', délégation incorrecte/mal placée)
- **Serveur mal configuré**
  - Mauvais nom de zone / mauvais fichier
  - Pas le droit à l'écriture dans le répertoire slave
- **Machine mal configurée**
  - Mauvaise adresse IP
- **Réseau mal configuré**
  - Filtres réseau, route manquante, ...

Vérifiez les logs!!! /var/log/messages par défaut

Outils de déboguage

Les logs de BIND (voir le guide administrateur)

Options de débug intégrées à BIND

ping et traceroute (problèmes réseau)

tcpdump / ethereal (analyse de requête / réponse)

dig (outil de recherche DNS avancé)

La meilleure façon de prévenir les erreurs:

Savoir qu'on va de toute façon en faire

Se préparer en consultant les journaux (tail -f /var/log/messages dans une fenêtre séparée)

Journalisation de BIND

Dire à named quels TYPES de messages envoyer

- **Catégorie**

Dire à named OU envoyer ces messages

- **Canal (channel)**

Les catégories de BIND

BIND dispose de plusieurs catégories

Chacune d'entre elle est référencée dans le guide administrateur

Exemple:

```
category dnssec { dnssec_log; };
```

Les canaux de BIND

BIND sait utiliser syslog (standard UNIX)

BIND peut aussi écrire directement dans un fichier

Exemple:

```
channel dnssec_log {
    file "seclog" versions 3 size 10m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity debug 3;
};
```

Nous avons installé un serveur...

Quels tests devons nous effectuer ?

Le minimum

- **Le serveur tourne-t-il (indice: ps)**
- **La machine est-elle correctement configurée (indice: réseau)**

Les données retournées par le serveur

- **La zone a-t-elle été chargée (que disent les logs ?)**
- **Les transferts de zones, si secondaire, se sont-ils déroulés ?**

Vérification de la configuration

Pour voir named démarrer en détail, utiliser **-g**
named reste en tâche principale
affiche des diagnostics au fur et à mesure
ne logge rien

Quand vous êtes satisfait, tuer named + redémarrer sans '-g'

Autres outils

- **named-checkconf**
- **named-checkzone**

Le serveur tourne-t-il ?

Une fois que le serveur est lancé, s'assurer qu'il fonctionne:

```
dig @localhost version.bind chaos txt
```

named renvoie, si tout va bien, son numéro de version

Ceci confirme que le serveur a au moins demarré, et que c'est la bonne version.

Les données du serveur sont-elles correctes ?

Vérifier le SOA:

```
dig @127.0.0.1 <zone> soa
```

Vérifier le numéro de série, s'assurer que la bonne version est chargée

Rappel: Le numéro de série est vérifié par les secondaires, pour décider si un transfert de zone est nécessaire.

Le serveur est-il joignable ?

Si les tests avec dig échouent, il faut peut-être vérifier le ré seau:

```
ping ip.du.serveur
```

Ceci teste les fonctions de bases du réseau, et les erreurs communes

- **Interface mal configuée**
- **Route ou masque de réseau incorrect**

Le serveur écoute-t-il ?

Si le serveur ne répond pas, mais la machine répond au ping

- **Vérifier les fichiers de log**
- **telnet ip.du.serveur 53**

named peut tourner même s'il n'arrive pas à ouvrir de port!

- **Ceci est visible dans les journaux (logs)**
- **telnet sur le port 53 teste si le port est ouvert**

Le serveur journalise-t-il les bonnes informations ?

Certains logs n’apparaissent qu’au besoin

- **Example: journaux dnssec qui nécessitent que ’trusted-keys’ soit configuré.**
- **Il n’est pas toujours évident de comprendre ce qui constitue un évè nement suffisant à la création d’un log**

Utilisation des outils

named lui-même

dig/nslookup

outils système

analyseurs de réseau

Utilisation des outils

named -g

- **'named -g -c fichier_de_config'**
- **force named à rester en tâche interactive**

named -d <niveau>

- **règle le niveau de déboguage (le "volume")**
- **les niveaux ne sont pas clairement définis**
- **-d 3 est commun, -d 99 donne énormément de détail**

Outils non-BIND

Outils permettant de s'assurer que l'environnement est correct

- **Outils de contrôle de la machine serveur**
  - ifconfig, df, ...
- **Outil de test du réseau**
  - ping, traceroute
- **Outils de décodage des messages en transit**
  - tcpdump, ethereal
- **Autres outils**
  - dnstracer