

Configuration de serveur uniquement autoritaire

Alain Patrick AINA

aalain@trstech.net

Atelier DNS/CCTLD

Yaounde, 17-21 Decembre 2004



Différent types de serveurs

Plusieurs types de serveurs de noms

- ◆ Serveurs autoritaires
 - ◆ maitre (primaire)
 - ◆ esclave (secondaire)
- ◆ Serveurs (cache) récursifs
 - ◆ Aussi les caches forwarders
- ◆ Serveurs multi fonctions

Pourquoi séparer les fonctionnalités ?(2)

Les données autoritaires et non-autoritaires sont destinées à différents groupes de clients

- ◆ Afin de servir les données autoritaires à l'Internet, le serveur doit être hors firewall.
- ◆ Les serveurs cache sont généralement placés derrière les firewall pour les protéger contre les abus de l'extérieur.

Servir les données autoritaires est plus importante que servir les données d'un cache.

Pourquoi séparer les fonctionnalités ?(2)

Les serveurs cache sont exposés aux intoxications

- ◆ Si un intrus trompe votre serveur cache en lui faisant accepter des ER forgés avec un TTL élevé, des données invalides peuvent être utilisées dans les réponses autoritaires.
 - ◆ Facile à faire:RFC 3833

Certaines attaques de déni de service et de buffer overrun réussissent mieux contre les serveurs cache.

Pourquoi séparer les fonctionnalités ?(3)

Les serveurs autoritaires serviront les données autoritaires (constantes en taille) plus efficacement si les données du cache ne leur font pas compétition pour les ressources systèmes

- ◆ Les clients récursifs utilisent de la mémoire (jusqu'à 20kO)
- ◆ Les serveurs cache utilisent la mémoire pour garder les données en cache
- ◆ Les réponses récursives demandent du temps et des ressources systèmes

Comment configurer un serveur uniquement autoritaire

Arrêter la récursion

```
options {  
    recursion no;  
    .....  
};
```

Vérifier l'indicateur ‘r a’ dans les entêtes des réponses DNS du serveur

Rappel: Comment configurer un serveur uniquement récursif

// serveur récursifs pour les clients du bloc 192.168.0.0/24

```
acl clients { 192.168.0.0/24; };  
    options {  
        directory “/var/named”  
        allow-query { clients; };  
    };
```

// Bind9 a les “pointeurs” racine précompilés. Cette déclaration de zone est optionnelle

```
zone “.” {  
    type hint;  
    file “named.cache”;
```

```
// ftp://ftp.internic.net/domain/named.cache  
};
```