Knot DNS pour un meilleur DNS ?

Matthieu Herrb

Capitoul - 26 juin 2018

Les services DNS

- Serveurs faisant autorité,
- Serveurs récursifs
- Résolveurs

Sécurité

- Non je ne vais pas refaire la liste de tous les problèmes...

DNSSEC : un élément de solution.
(authentification via chaîne de confiance).

Un coupable : Bind

- Logiciel vieillissant (Bind 9 - 2000 $\rightarrow$ version stable 9.11)
- Bind 10 arrêté en 2015, bundy pas très vivant
- Confusion entre les rôles
- Support DNSSEC minimal
- CVEs réguliers

$\longrightarrow$ Merci, il a bien mérité la retraite !

Les nouveaux venus

- séparation entre rôles
- serveurs faisant autorité : nsd, powerdns, knot,...
- serveurs cache récursifs : unbound, knot resolver,...
- forwarders indépendants : dnsmasq, rebound,...

Knot DNS

`https://www.knot-dns.cz/`

- développé par le cz.nic
- hautes performances
- gestion DNSSEC automatique (depuis 2.6)
- configuration YAML
- mise à jour des fichiers de zone par transaction (`kdnsupdate`)
- fonctions de monitoring
- limitation de charge

Planifier une transition

Séparer les 2 rôles :

- résolveur : `/etc/resolv.conf` :
  `nameserver resolver.foo.bar`
- serveur faisant autorité : `master.zone` :
  `@ IN NS ns.foo.bar.`

Soit :

- 2 IP différentes (machines virtuelles, aliases,...)
- via redirections IPTables/pf

Facile dans le cas d'architecture type « Archimbauld » :

- les serveurs faisant autorité sur IP publiques (en DMZ)
- les serveurs récursifs sur IP privées (réseau interne)

DNSSEC avec Knot DNS

`https://www.swordarmor.fr/gestion-automatique-de-dnssec-avec-knot.html`

Knot gère automatiquement le renouvellement des clés DNSSEC et la signature des zones après modification.

C'est (presque) transparent pour les administrat·rices·eurs.

Reste à superviser le serveur pour vérifier que tout va bien.

Questions ?