Utiliser OpenDNSSEC avec un serveur maître NSD

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 avril 2012

https://www.bortzmeyer.org/opendnssec-nsd.html

Gérer proprement DNSSEC n'est pas trivial : un certain nombre d'opérations de gestion des clés et de renouvellement des signatures doivent se faire dans un ordre précis, à certains moments. Si on le fait à la main, une erreur ou un oubli est vite arrivé et, comme illustré par mon article à SATIN 2011 <http://conferences.npl.co.uk/satin/papers/satin2011-Bortzmeyer.pdf>, de tels erreurs ou oublis sont fréquents. D'où l'intérêt d'utiliser une solution logicielle qui automatise tout cela, en l'occurrence OpenDNSSEC. Les exemples donnés dans la documentation sont pour un serveur DNS maître utilisant BIND. Et si on se sert de NSD ?

Ce dernier présente bien des avantages, notamment de rapidité, et aussi sans doute de sécurité, en raison d'un code bien plus court. Mais il n'a pas l'équivalent de la commande `rndc` de BIND, commande qui permet à OpenDNSSEC de signaler au serveur de noms qu'il a fini, et que la zone doit être rechargée. Il va donc falloir un peu plus de travail.

Les commandes à faire sur NSD, après la génération d'un nouveau fichier de zones par le signeur d'OpenDNSSEC, sont :

```
# Reconstruire la base de données de nsd
nsdc rebuild
# Charger la nouvelle base
nsdc reload
# Prévenir les esclaves
nsdc notify
```

Il faut en outre être root pour les lancer. Le signeur d'OpenDNSSEC tourne typiquement sous un autre nom (avec le paquetage Debian, il utilise le compte `opendnssec`). Il faut donc commencer par faire un programme setuid qui appelle les deux commandes ci-dessus. Pas besoin de programmer, Russell Harmon l'a fait et a publié le résultat <https://gist.github.com/1073357> (j'en garde une copie locale en (en ligne sur `https://www.bortzmeyer.org/files/opendnssec-nsd-reload.c`)).

Ce simple programme en C appelle les trois commandes ci-dessus. Il doit ensuite être installé setuid pour exécuter ces commandes sous root. Cela peut se faire avec un simple Makefile :

```
.PHONY: all clean

CHGRP := /bin/chgrp
CHMOD := /bin/chmod
CFLAGS := -Wall -Wextra -Werror
DEST := /usr/local/sbin
INSTALL := /usr/bin/install

all: opendnssec-nsd-reload

clean:
        $(RM) opendnssec-nsd-reload

opendnssec-nsd-reload: opendnssec-nsd-reload.c
        $(CC) $(CFLAGS) $(LDFLAGS) -o $@ $<

install: opendnssec-nsd-reload
        $(INSTALL) opendnssec-nsd-reload $(DEST)
        $(CHGRP) opendnssec $(DEST)/opendnssec-nsd-reload
        $(CHMOD) o=,g=x,u=rwxs $(DEST)/opendnssec-nsd-reload
```

Une fois ce programme installé avec `make install`, on peut le tester, vérifier qu'il recharge bien le serveur (`nsd[xxx]: signal received, reloading...` dans le journal).

Ensuite, il faut dire à OpenDNSSEC de l'appeler dès qu'il a fini de signer. Cela se fait dans le fichier de configuration `conf.xml` :

```
<NotifyCommand>/usr/local/sbin/opendnssec-nsd-reload</NotifyCommand>
```

Et voilà, lorsque OpenDNSSEC a fini de signer, il appelle la commande indiquée dans l'élement `NotifyCommand` et c'est tout.

Le programme est très simple et on peut facilement le modifier. Attention, toutefois, il est setuid et les bogues dans de tels programmes peuvent se payer cher. Pour des fonctions supplémentaires, comme de journaliser le rechargement, je préfère les faire dans un bête script shell qui appelera `opendnssec-nsd-reload` ensuite. Voici un exemple d'un tel script :

```
#!/bin/sh

logger -i -t OpenDNSSEC-signer -p daemon.info \
       "Reloading nsd, modification in zone $1 (file $2)"
/usr/local/sbin/opendnssec-nsd-reload
```

et on l'appelera (s'il se nomme `run-opendnssec-nsd-reload`) :

```
<NotifyCommand>/usr/local/sbin/run-opendnssec-nsd-reload %zone %zonefile</NotifyCommand>
```

(Notez les deux macros `%zone` et `%zonefile`, fournies par OpenDNSSEC.) Si tout marche bien, on verra dans le journal des choses comme :

```
 Apr 11 10:16:42 aetius OpenDNSSEC-signer[18571]: \
         Reloading nsd, modification in zone bortzmeyer.fr (file /var/lib/opendnssec/signed/bortzmeyer.fr)
```

Et voilà, désormais, tout est automatique, il n'y a plus qu'à surveiller.
