DNSSEC kuharica

U ovoj kuharici pokazat ćemo kako upravljati DNSSEC potpisanim zonama koristeći isključivo BIND server i njegove alate. Pokazat ćemo generiranje ključeva, ručno potpisivanje zona, periodički *resign* zona, automatsko potpisivanje zona koristeći BIND *inline-signing* i rotacije ključeva.

Inicijalni koraci

Prije svega potrebno je generirati ključeve. Generirat ćemo dva ključa, zone-signing ključ (ZSK) i key-signing ključ (KSK). Za to koristimo **dnssec-keygen**:

```
# mkdir -p /etc/bind/keys/carnet.tst.hr
# cd /etc/bind/keys/carnet.tst.hr
# dnssec-keygen -a RSASHA256 -b 1536 carnet.tst.hr
Generating key pair...
Kcarnet.tst.hr.+008+30234
# dnssec-keygen -a RSASHA256 -b 2048 -f KSK carnet.tst.hr
Generating key pair...
Kcarnet.tst.hr.+008+60151
```

Parametar **-a** specificira crypto algoritam, opcija **-b** definira duljinu ključa i opcija **-f** postavlja KSK flag na ključ.

Javni dio ključa nalazi se u datoteci s ekstenzijom **.key** te sadrži DNSKEY zapis i metapodatke ključa. Metapodaci su vremenski podaci koji govore BIND alatima kako koristiti ključ. Primjer datoteke:

```
# cat Kcarnet.tst.hr.+008+30234.key
; This is a zone-signing key, keyid 30234, for carnet.tst.hr.
; Created: 20151029103648 (Thu Oct 29 11:36:48 2015)
; Publish: 20151029103648 (Thu Oct 29 11:36:48 2015)
; Activate: 20151029103648 (Thu Oct 29 11:36:48 2015)
carnet.tst.hr. IN DNSKEY 256 3 8 AwEAAclahFcJxNbnjxwWsrBRS...
```

Publish definira kada se DNSKEY zapis ključa dodaje u zonu, dok *activate* definira kada se ključ počne koristiti za generiranje potpisa. Metapodacima ćemo manipulirati pri rotaciji ključeva, no više o tome kasnije.

Kreiramo zaseban direktorij zone i tamo postavimo nepotpisanu verziju zone (npr. /etc/bind/zone/carnet.tst.hr/carnet.tst.hr). Zatim generiramo potpisanu zonu **dnssec-signzone** alatom:

```
# cd /etc/bind/zone/carnet.tst.hr
# dnssec-signzone -S -K /etc/bind/keys/carnet.tst.hr carnet.tst.hr
Fetching KSK 60151/RSASHA256 from key repository.
```

```
Fetching ZSK 30234/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
carnet.tst.hr.signed
```

Parametar **-S** uključuje *smart signing* opciju koja automatizira dodavanje DNSKEY zapisa u zonu prema metapodacima koje se nalaze u datotekama ključeva. Opcija **-K** specificira direktorij u kojem će *signzone* pronaći ključeve zone. Na kraju zadamo ulaznu datoteku zone, tj. našu nepotpisanu datoteku zone.

Napomena: *smart signing* je u BIND-u od verzije 9.7 i znatno olakšava upravljanje ključevima.

Prema zadanim parametrima *bind* će generirati *NSEC chain* za autenticiranje negativnih odgovora (NXDOMAIN). NSEC chain je povezana lista (eng. *linked list*) svih imena u zoni koja se koriste za autenticiranje NXDOMAIN odgovora. Problem s NSEC chainom je u tome što omogućava čitanje svih imena u zoni (eng. *zone walk*) što možda i nije poželjno. Ako želimo otežati *zone walk* potrebno je uključiti generiranje *NSEC3 chaina* koji hashira imena prije dodavanja u chain.

Signzone naredba s generiranjem NSEC3 chaina:

```
# dnssec-signzone -S -K /etc/bind/keys/carnet.tst.hr -3 <salt> carnet.tst.hr
```

Opcija -3 specificira NSEC3 chain, dok je *salt* hexadecimalna vrijednost koja se nalijepi na kraj svih imena prije hashiranja. Preporuča se se redovna promjena salta, primjerice kod rotacije *zone-signing* ključeva ili čak kod svakog periodičkog resigna zone.

Definicija zone u BIND konfiguraciji referirat će na potpisanu verziju zone, primjer:

```
# edit /etc/bind/named.conf.local
zone "carnet.tst.hr" IN {
    type master;
    file "/etc/bind/zone/carnet.tst.hr/carnet.tst.hr.signed";
    allow-query { any; };
};
```

Na kraju učitamo promjene u BIND konfiguraciji:

```
# rndc reconfig
```

Spremni smo za dodavanje našeg *key-signing* ključa u *parent* zonu. *Signzone* će generirati datoteku *dsset-<ime_zone.>* u direktoriju zone koja sadrži DS zapise za naš KSK. DS zapisi se također mogu generirati naredbom **dnssec-dsfromkey**:

```
# cd /etc/bind/keys/carnet.tst.hr
# dnssec-dsfromkey Kcarnet.tst.hr.+008+60151
carnet.tst.hr. IN DS 60151 8 1 2559DFD85BF4BE6A38294AC1DF09F37EDA7B97B5
carnet.tst.hr. IN DS 60151 8 2 0E5675886BE12499ED3A7AEE0B78069CA2166719E880A45D3F9E3C
F24D7145F8
```

Prije dodavanja DS zapisa u parent zonu valja pričekati propagaciju potpisane zone na svim sekundarnim poslužiteljima zone.

Nakon editiranja datoteke nepotpisane zone treba obaviti potpisivanje (ulazna datoteka je nepotpisana zona kao i kod inicijalnog potpisivanja) i napravit *reload* zone - ako imate zonu u git repozitoriju jednostavni *post-commit* hook može to napraviti za vas. Ne zaboravite inkrementirati serial u nepotpisanoj zoni prije potpisivanja.

Periodički resign zona

Sljedeći korak je osigurati periodičko osvježavanje potpisa u zoni. RRSIG zapisi prema zadanim parametrima *signzone* naredbi ističu nakon 30 dana. Validirajući rekurzori će provjeravati vremenske podatke u zapisima i vratiti SERVFAIL ako je potpis istekao.

Periodički *resign* može se riješiti jednostavnom shell skriptom koju pozivamo iz cron-a. Primjer skripte:

```
#!/bin/sh -e
ZONE=$1
ZONEDIR=/etc/bind/zone/$1
KEYDIR=/etc/bind/keys/$1

cd $ZONEDIR
/usr/sbin/dnssec-signzone -S -K $KEYDIR \
  -N increment \
  -o $ZONE \
  -f ${ZONE}.signed \
  ${ZONE}.signed
/usr/sbin/rndc reload $ZONE
```

Pripadajući cronjob:

```
*/3 * * * * root /usr/local/sbin/resign carnet.tst.hr
```

Valja primijetiti da smo u skripti *signzone* naredbi kao ulaznu datoteku naveli potpisanu verziju zone. *Signzone* će provjeriti sve potpise u zoni i generirati nove potpise prema potrebi (ako su unutar tjedan dana do isteka). *Smart signing* će se pobrinuti i za eventualne rotacije ključeva čitanjem metapodataka u datotekama ključeva kod svakog poziva iz cron-a.

Parametrom **-N** možemo *signzone* alatu specificirati što treba napraviti sa serialom u potpisanoj verziji zone (izlazna datoteka). Ovdje nam je idealno inkrementiranje seriala jer je ulazna datoteka ista kao i izlazna datoteka (**-f** parametar). To znači da će se serial inkrementirati u potpisanoj zoni za svaki *resign* neovisno o serialu u nepotpisanoj verziji zone.

BIND inline-signing

Od verzije 9.9 *bind* podržava mogućnost *on-the-fly* potpisivanja promjena u zoni. Opcija *inline-signing* automatski generira potpisanu zonu i ažurira potpise kod promjena u nepotpisanoj verziji zone. Osim toga, opcija *auto-dnssec* kao i smart signing prati metapodatke ključeva što olakšava upravljanje ključevima. Ova konfiguracija eliminira potrebu za shell skriptama i *cron* jobovima kako bi se osigurala validnost zone.

Ako bi htjeli prekonfigurirati zonu iz primjera tako da koristi ove funkcionalnosti BIND servera prije

svega treba potvrditi da koristimo verziju BIND s podrškom za inline-signing:

```
# named -v
BIND 9.9.5-4~bpo70+1-Debian (Extended Support Version)
```

Zatim možemo podesiti konfiguraciju zone:

```
zone "carnet.tst.hr" IN {
    type master;
    //file "/etc/bind/zone/carnet.tst.hr/carnet.tst.hr.signed";
    file "/etc/bind/zone/carnet.tst.hr/carnet.tst.hr";
    key-directory "/etc/bind/keys/carnet.tst.hr";
    inline-signing yes;
    auto-dnssec maintain;
    allow-query { any; };
};
```

Uključili smo **inline-signing** i **auto-dnssec** opcije i preko **key-directory** direktive naveli BIND serveru gdje može pronaći ključeve zone. Umjesto potpisane zone sada referiramo na nepotpisanu datoteku zone u definiciji zone (bez obzira na to BIND će generirati i posluživati potpisanu verziju zone).

Napomena: bitno je osigurati korisniku pod kojim se pokreće BIND čitanje privatnih ključeva zone. BIND alati za rad s ključevima postavit će dozvole 600 tako da je ručno potrebno podesiti vlasništvo/dozvole na datotekama ključeva.

Zatim brišemo potpisanu zonu koju smo ranije ručno generirali i nakon toga ponovno učitamo BIND konfiguraciju:

```
# rm /etc/bind/zone/carnet.tst.hr/carnet.tst.hr.signed
# rndc reconfig
```

BIND će automatski generirati NSEC chain, ako želimo NSEC3 moramo specificirati BIND-u generiranje NSEC3 chaina:

```
# rndc signing -nsec3param 1 0 10 <salt> carnet.tst.hr
```

Ovom naredbom dodajemo NSEC3PARAM zapis u zonu koji specificira parametre NSEC lanca: hash algoritam, *opt-out flag* i broj iteracija. Zadane postavke su zadovoljavajuće za većinu potreba.

Bind će generirati potpisanu verziju zone u raw/binarnom formatu. Ako je potrebno, tekstualnu verziju potpisane zone možemo generirati naredbama:

```
# rndc sync carnet.tst.hr
# named-compilezone -f raw -F text -o carnet.tst.hr.signed.text carnet.tst.hr carnet.
tst.hr.signed
zone carnet.tst.hr/IN: loaded serial 2015102909 (DNSSEC signed)
dump zone to carnet.tst.hr.signed.text...done
OK
```

Zonu ažuriramo kao da se radi o standardnoj nepotpisanoj BIND zoni: izmijenimo zapise, inkrementiramo serial i reloadamo zonu. *Inline-signing* će se pobrinuti za generiranje i posluživanje potpisanih zapisa.

Rotacija ključeva

Ovime smo pokrili sve što je potrebno za nesmetan rad DNSSEC potpisanih zona u BIND okruženju. Preostala nam je samo tema periodičke zamjene ključeva. Rotacije ključeva nisu obavezne, tj. validiraćuji rekurzori ne provjeravaju starost ključeva tako da to ovisi samo o vašoj administrativnoj politici. Preporuča se barem rotacija zone-signing ključeva pošto je procedura relativno bezbolna i može se jednostavno automatizirati. Za ključ duljine 1024 i više bitova dovoljno je zamijeniti ključ jednom godišnje. Što se *key-signing* ključa tiče, za duljinu od 2048 bitova dovoljna je rotacija jednom u 5 godina.

U slučaju da administrator želi rotirati ZSK ključ potrebno je podesiti metapodatke aktivnog ZSK ključa i generirati ključ koji će ga naslijediti. Primjer:

```
# cd /etc/bind/keys/carnet.tst.hr
# dnssec-settime -I 20151129 -D 20151229 Kcarnet.tst.hr.+008+30234
./Kcarnet.tst.hr.+008+30234.key
./Kcarnet.tst.hr.+008+30234.private
# dnssec-keygen -S Kcarnet.tst.hr.+008+30234
Generating key pair...
Kcarnet.tst.hr.+008+03408
```

Koristimo **dnssec-settime** alat za postavljanje metapodataka za aktivni/stari ZSK ključ. Postavljamo **-I** parametar, tj. datum deaktivacije ključa (ostaje u zoni ali se ne koristi za potpisivanje). Također postavljamo **-D** parametar, tj. datum brisanja DNSKEY zapisa ključa iz zone.

Bitno je napomenuti da je potrebno ostaviti dovoljno vremena starim RRSIG zapisima da isteknu prije nego što obrišemo stari ZSK iz zone. Ako se koristi zadani *end-time* RRSIG-ova od 30 dana potreban je barem toliki razmak između deaktiviranja (**-I** parametar) i brisanja ključa (**-D** parametar).

Zatim generiramo *successor* ključ pozivanjem **dnssec-keygen** alata sa **-S** parametrom i kao drugi parametar dajemo ID našeg starog ZSK ključa. Keygen alat će pregledati metapodatke starog ZSK ključa i prema tome postaviti datum dodavanja novog ZSK ključa u zonu (**pre-publish** datum, default je 30 dana prije aktivacije) i datum aktivacije novog ključa (na dan kada se deaktivira stari ZSK ključ).

Metapodaci u datotekama ključeva nakon izvođenja gorenavedenih naredbi:

```
# cat Kcarnet.tst.hr.+008+30234.key
; This is a zone-signing key, keyid 30234, for carnet.tst.hr.
; Created: 20151029103648 (Thu Oct 29 11:36:48 2015)
; Publish: 20151029103648 (Thu Oct 29 11:36:48 2015)
; Activate: 20151029103648 (Thu Oct 29 11:36:48 2015)
; Inactive: 20151129000000 (Sun Nov 29 01:00:00 2015)
; Delete: 20151229000000 (Tue Dec 29 01:00:00 2015)
carnet.tst.hr. IN DNSKEY 256 3 8 AwEAAclahFcJxNbnjxwWsrBR...
# cat Kcarnet.tst.hr.+008+03408.key
; This is a zone-signing key, keyid 3408, for carnet.tst.hr.
; Created: 20151029122435 (Thu Oct 29 13:24:35 2015)
; Publish: 20151030000000 (Fri Oct 30 01:00:00 2015)
; Activate: 20151129000000 (Sun Nov 29 01:00:00 2015)
carnet.tst.hr. IN DNSKEY 256 3 8 AwEAAeJw/gsY66EwfQSpEXtF...
```

Za rotaciju KSK ključa možemo koristiti istu metodu kao i kod rotacije ZSK ključa (**pre-publish** metoda) ili možemo koristiti **double-signing** metodu. Za double-signing jednostavno generiramo novi KSK ključ koji će odmah postati aktivan u zoni uz naš stari KSK ključ. Novi ključ generiramo istom naredom kojom smo generirali naš inicijalni KSK ključ:

```
# cd /etc/bind/keys/carnet.tst.hr
# dnssec-keygen -a RSASHA256 -b 2048 -f KSK carnet.tst.hr
Generating key pair...
Kcarnet.tst.hr.+008+38770
# dnssec-dsfromkey Kcarnet.tst.hr.+008+38770
carnet.tst.hr. IN DS 38770 8 1 4A33CC9C14E2D86AAF8537195B9E0AB71E23DC03
carnet.tst.hr. IN DS 38770 8 2 07554D9348D1278742322C48AF92C5B2960E4D430C1374A50DEAC6
F0C78C16E4
```

Nakon propagacije novog KSK ključa dodajemo nove DS zpise u parent zonu. Stari ključ možemo obrisati nakon što smo sigurni da je novi DS zapis propagiran u *cache* rekurzora. Propagacija ovisi o TTL-u DS zapisa u parent zoni i TTL-u DNSKEY zapisa u našoj zoni. Brisanje starog KSK ključa iz zone:

```
# dnssec-settime -I now -D now Kcarnet.tst.hr.+008+60151
```

Ako se koristi *auto-dnssec* s **maintain** parametrom, nije potrebno ručno potpisivati i *reloadati* zonu nakon dodavanja novog ključa. BIND će kod svoje periodičke provjere zone (svakih sat vremena) primijetiti novi ključ i aktivirati ključ u zoni kako je definirano u metapodacima. Bitno je da nakon generiranja novog ključa ili postavljanja metapodataka **dnssec-settime** alatom osiguramo *bind* korisniku mogućnost čitanja privatnih ključeva zone.

Ako ručno potpisujemo zonu, *cron* iz ranijeg primjera pobrinut će se za rotaciju ključeva.

Korisni linkovi

BIND DNSSEC guide [1] - uvod u DNSSEC, upute za korištenje BIND inline potpisivanja, recepti za rotacije ključeva itd.

NSEC3 info [2] - usporedba NSEC i NSEC3 specifikacija uz detljna objašnjenja funkcionalnosti.

DNSSEC operational practices [3] - savjeti za administriranje DNSSEC potpisanih zona (ne nužno "Best Practices").

pet, 2015-10-30 12:21 - Alan Jurčić**Kuharice:** Za sistemce [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1576

Links
[1] http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html
[2] https://www.sidn.nl/fileadmin/docs/PDF-files_UK/wp-2011-0x01-v2.pdf
[3] https://tools.ietf.org/html/rfc6781
[4] https://sysportal.carnet.hr./taxonomy/term/22