Akademie

Zone Transfer + TSIG

Zbyněk Michl
<*zbynek.michl@nic.cz*>

Ondřej Surý
<*ondrej.sury@nic.cz*>

10. února 2011

cz nic

Zone Transfer

- Master → Slave, Slave → Slave
- AXFR
  - Přenáší se vždy celá zóna
  - Transportní vrstva TCP
- IXFR
  - Inkrementální transfer
  - Přenáší se pouze změny
  - Transportní vrstva TCP

Konfigurace AXFR

- Bind9

```
options { allow-transfer { acl; <ip_addr>; }; };
zone "udp53.cz" { allow-transfer { acl; ip; };};
view { … };
```

- NSD3

```
provide-xfr: <ip_addr> NOKEY|<tsig_keyname>
request-xfr: <ip_addr> NOKEY|<tsig_keyname>
```

Konfigurace IXFR

- Bind9

```
provide-ixfr yes/no;
request-ixfr yes/no;
zone "udp53.cz" {
  journal "/var/lib/bind/udp53.cz.jnl";
  ixfr-from-differences yes/no;
};
```

- NSD3
  - master neumí IXFR, slave standardně

TSIG

- RFC2845 (r. 2000)
  - Secret Key Transaction Authentication for DNS (TSIG)
  - Obecný podpis DNS zpráv
- Více použití
  - Autorizace transferů zón
  - Autorizace notify zpráv
  - Autorizace dotazů
    - Cisco má ohavný bug

TSIG

- Symetrická kryptografie
  - ~~HMAC-MD5 [1..512]~~
    - Raději už nepoužívat
  - HMAC-SHA1 [1..160]
  - HMAC-SHA(224|256|384|512)

Vygenerování klíče

- Balík bind9utils

```
$ dnssec-keygen -a HMAC-SHA1 -b 160\
   -n HOST server.
```

- Generujeme
  - Algoritmem HMAC-SHA1 (-a)
  - Počet bitů 160 (-b)
  - Pro HOST (-n)
  - Název klíče: server.

Úkol

- Vygenerujte TSIG klíč
  - Algoritmus HMAC-SHA1
  - Počet bitů: 1

```
# dnssec-keygen -a HMAC-SHA1 -b 1 -n HOST
pc<NN>.lab.nic.cz.
```

- Podívejte se do vygenerovaného souboru

```
# cat Kpc<NN>.lab.nic.cz.+<yyy>+<xxxxx>.key
```

Vygenerovaný klíč

```
$ dnssec-keygen -a HMAC-SHA1 -b 160
  -n HOST server
Kserver.+161+41482
$ cat Kserver.+161+41482.key
server. IN KEY 512 3 163
EwByWMi+r7AyQDkxUGaf25eUNmVnVzGObeAcztjqeHM=
```

- Veřejná i soukromá část je stejná

Konfigurace master Bind9

```
key "server." {
  algorithm hmac-sha1;
  secret
"EwByWMi+r7AyQDkxUGaf25eUNmVnVzGObeAcztjqeHM=";
};

acl stahovaci { key server.; };

zone "udp53.cz" {
  type master;
  file "/etc/bind/udp53.cz";
  allow-transfer { stahovaci; };
  notify explicit; also-notify { <ip_addr>; };
};
```

Konfigurace slave Bind9

```
key "server." {
  algorithm hmac-sha1;
  secret
"EwByWMi+r7AyQDkxUGaf25eUNmVnVzGObeAcztjqeHM=";
};

server <ip_addr> { keys { server.; }; };

zone "udp53.cz" {
  type slave;
  file "/var/cache/bind/udp53.cz“;
  masters { <ip_addr>; };
  notify no; allow-notify { <ip_addr>; };
};
```

Úkol

- Povolte transfer přes TSIG pro souseda

```
key "pc<SS>.lab.nic.cz." {
  algorithm hmac-sha1; secret "<klic_souseda>";
};

acl soused { key pc<SS>.lab.nic.cz; };

zone "z<NN>.lab.nic.cz." {
  type master;
  file "/etc/bind/z<NN>.lab.nic.cz";
  allow-transfer { soused; };
  notify explicit;
  also-notify { 10.0.0.1<SS>; };
};
```

Úkol

- Nakonfigurujte transfer slave zóny pomocí TSIG

```
key "pc<NN>.lab.nic.cz." {
  algorithm hmac-sha1; secret "<vas_klic>";
};

server 10.0.0.1<SS> {keys{pc<NN>.lab.nic.cz;};};

zone "z<SS>.lab.nic.cz." {
  type slave;
  file "/var/cache/bind/z<SS>.lab.nic.cz";
  masters { 10.0.0.1<SS>; };
  notify no; allow-notify { 10.0.0.1<SS>; };
};
```

Konfigurace NSD3

```
key:
  name: "<nazev_klice>"
  algorithm: hmac-sha1
  secret: "0Q="
zone:
  name: "udp53.cz."
  zonefile: "/etc/nsd3/udp53.cz"
  provide-xfr: 0.0.0.0/0 nazev_klice   # master
  request-xfr: ip_adresa nazev_klice   # slave
```

Úkol

- Povolte transfer přes TSIG pro souseda

```
key:
  name: "pc<SS>.lab.nic.cz."
  algorithm: hmac-sha1
  secret: "<klic_souseda>"
zone:
  name: "z<NN>.lab.nic.cz."
  zonefile: "/etc/bind/z<NN>.lab.nic.cz"
  provide-xfr: 10.0.0.1<SS> pc<SS>.lab.nic.cz.
  notify: 10.0.0.1<SS> pc<SS>.lab.nic.cz.
```

Úkol

- Nakonfigurujte transfer slave zóny pomocí TSIG

```
key:
  name: "pc<NN>.lab.nic.cz."
  algorithm: hmac-sha1
  secret: "<vas_klic>"
zone:
  name: "z<SS>.lab.nic.cz."
  zonefile: "/var/lib/nsd3/z<SS>.lab.nic.cz"
  request-xfr: 10.0.0.1<SS> pc<NN>.lab.nic.cz.
  allow-notify: 10.0.0.1<SS> pc<NN>.lab.nic.cz.
```

Úkol

- Spusťte wireshark nad rozhraním eth0
- Nastavte filter na TCP port 53

```
tcp.port == 53
```

- Stáhněte ručně zónu souseda

```
# dig -k Kpc<NN>.lab.nic.cz.+161+xxxx.key IN
AXFR z<SS>.lab.nic.cz. @10.0.0.1<SS>
```

- Podívejte se na obsah podepsaného paketu