# Knot DNS a DNSSEC

## IT14 Workshop 23. 5. 2014

**Jan Kadlec • jan.kadlec@nic.cz**

**Daniel Salzman • daniel.salzman@nic.cz**

CZ.NIC | SPRÁVCE DOMÉNY CZ

# Co bude potřeba

- Vlastní notebook
- Operační systém Linux/*BSD/MAC OS
- Připojení k síti
  - https://secure.nic.cz/files/it14/knot/
- Nástroje dnssec-keygen, dnssec-settime, nsupdate
  - Ubuntu (bind9, bind9utils)...

# Obsah workshopu

- Instalace a základní zprovoznění Knot DNS
- Automatické podepisování DNSSEC
- Modifikace zóny
- Přechod z NSEC na NSEC3
- Výměna ZSK klíče
- Ochrana před zesilujícími útoky pomocí RRL
- Knot DNS 1.6 a DNSSEC

# Knot DNS

- Autoritativní DNS server
- Open source projekt CZ.NIC Labs
- Výkonný server bez přerušovaného odpovídání
- Transfery zón (AXFR, IXFR)
- DNSSEC, EDNS0, TSIG, DDNS, RRL
- Možnost vzdálené správy
- Aktuální verze 1.4.6 (připravujeme 1.5.0 a 1.6.0)

# Možnosti instalace

- Podporované platformy:
  - Linux, *BSD, MAC OS, OpenWRT
- http://www.knot-dns.cz
  - Pokud máte Debian nebo Ubuntu, naimportujte repositáře Labs CZ.NIC
  - Pro Fedoru: koji.fedoraproject.org → hledat knot
    stáhnout rpm pro knot-1.4.6-2
    nainstalovat rpm
- Zdrojový kód (release, git)
- Repozitář příslušného operačního systému
- Rozšířené repozitáře (EPEL, PPA)

# Hlavní části Knot DNS

- Serverová část – **knotd**
- Ovládací rozhraní – **knotc**
- Konfigurační soubor – **/etc/knot/knot.conf**
- Úložný adresář – **/var/lib/knot/**
  - zónové a pomocné soubory
- Manuálové stránky

# 1. příklad: Zprovoznění serveru

- Nahrát example.com.zone do /etc/knot
  - Nastavit vlastníka a skupinu na “knot“:

    chown knot:knot /etc/knot/example.com.zone
- do /etc/knot/knot.conf přidat:

```
remotes {
  slave0 { address 0.0.0.0/0; } #povolí všechny
}

zones {
  example.com. {  #musí být stejné jako v souboru
    file "/etc/knot/example.com.zone";
    xfr-out slave0;
  }
}

log { # loguj vše do souboru /tmp/knot.log
  file “/tmp/knot.log” { any all; }
  syslog { any all; }
}
```

# 1. příklad: Ověření funkčnosti

- Spuštění serveru:
  - knotc checkconf
  - service knot start
  - /etc/init.d/knot start
- Ověření chodu server:
  - netstat -lnptu
  - tail /tmp/knot.log
  - knotc zonestatus
- Dotaz na server:
  - dig @localhost it14.example.com TXT
  - dig @localhost CH TXT version.server

# 2. příklad: Automatický DNSSEC (1)

- Nejprve potřebujeme vytvořit klíče
- Použijeme algoritmus RSASHA256
  - Umí NSEC i NSEC3
- Potřebujeme dva klíče: KSK a ZSK
- KSK:
  - dnssec-keygen -f KSK -a RSASHA256 -b 4096 -r /dev/urandom example.com
- ZSK:
  - dnssec-keygen -a RSASHA256 -b 1024 -r /dev/urandom example.com

# 2. příklad: Automatický DNSSEC (2)

- Klíče (4 soubory) nahrát do /etc/knot/keys (složku vytvořte – mkdir /etc/knot/keys)
  - Nastavit vlastníka a skupinu na “knot“
- /etc/knot/knot.conf:

```
zones {
  example.com. {
    file "/etc/knot/example.com.zone";
    xfr-out slave0;
    dnssec-enable on;
    dnssec-keydir "/etc/knot/keys";
  }
}
```

- knotc reload
- Ověření:
  - dig @localhost it14.example.com TXT +dnssec
  - knotc zonestatus
  - Výpis logu

# 3. příklad: Modifikace zóny

- Ruční editace zónového souboru /etc/knot/example.com.zone
  - test.example.com. 3600 AAAA ::123
  - + zvýšit SOA serial
- knotc reload
- Ověření
  - dig @localhost test.example.com AAAA +dnssec
  - knotc zonestatus
  - Výpis logu

# 4. příklad: Přechod na NSEC3

- Otevřete soubor s zónou: /etc/knot/example.com.zone
- Do apexu zóny přidejte NSEC3PARAM záznam:
  - example.com. 0 NSEC3PARAM 1 0 10 BADCAFFE
- Zvyšte SOA serial
- knotc reload
- Dotaz na neexistující jméno by měl vrátit NSEC3:
  - dig bogus.example.com @127.0.0.1 +dnssec

# dnssec-settime

- Nástroj na nastavování metadat klíčů
  - použití: dnssec-settime -P/A/R/I/D cesta_ke_klici
- Možnost nastavit:
  - -P: Publish – kdy se klíč objeví v apexu
  - -A: Activate – kdy se klíčem začne podepisovat
  - -R: Revoke – použití jen na resolverech
  - -I:  Inactive – kdy se klíčem přestane podepisovat
  - -D: Delete – kdy klíč zmizí z apexu
- Výpis parametrů:
  - dnssec-settime -p all cesta_ke_klici

# Předčasné publikování (výměna ZSK)

| initial | new DNSKEY | new RRSIGs | DNSKEY removal |
|---|---|---|---|
| SOA0 | SOA1 | SOA2 | SOA3 |
| RRSIG10(SOA0) | RRSIG10(SOA1) | RRSIG11(SOA2) | RRSIG11(SOA3) |
| DNSKEY1 | DNSKEY1 | DNSKEY1 | DNSKEY1 |
| DNSKEY10 | DNSKEY10 | DNSKEY10 | DNSKEY11 |
| | DNSKEY11 | DNSKEY11 | |
| RRSIG1 (DNSKEY) | RRSIG1 (DNSKEY) | RRSIG1(DNSKEY) | RRSIG1 (DNSKEY) |
| RRSIG10(DNSKEY) | RRSIG10(DNSKEY) | RRSIG11(DNSKEY) | RRSIG11(DNSKEY) |

DNSKEY TTL MAX ZONE TTL

1 – KSK
10 – starý ZSK
11 – nový ZSK

# 5. příklad: Rotace ZSK (1)

- Vygenerujte nový **ZSK:**
  - dnssec-keygen -a RSASHA256 -b 1024 -r /dev/urandom example.com
  - změntě vlastníka a skupinu novému klíči
- Nastavte **starému** ZSK dobu deaktivace a zrušení a **novému** dobu aktivace:
  - Inaktivovat za 3 minuty a smazat za 5 (nereálné hodnoty):
    - dnssec-settime -I +3mi -D +4mi cesta_k_ZSK **&&**
      dnssec-settime -A +3mi cesta_k_novemu_ZSK
    - ověření: dnssec-settime -p all cesta_ke_staremu_ZSK
      dnssec-settime -p all cesta_k_novemu_ZSK

# 5. příklad: Rotace ZSK (2)

- Jakmile jsou klíče nastavené:
  - Reload serveru:
    - knotc reload
  - Sledujete log
    - kdy se plánuje další podepsání
    - public / not-public
    - active / inactive
  - Sledujte jaké RRSIG záznamy server posílá
    - watch dig example.com A +dnssec @localhost
    - V RRSIG záznamu je keytag klíče

# 6. příklad: Zapnutí RRL

- Omezení odpovídání na „podobné“ dotazy
- /etc/knot/knot.conf:

```
system {
  ...
  rate-limit 2;        # počet dotazů na tok za jednu sekundu
  rate-limit-slip 1;   # na kolikátý dotaz se odpoví s TC bitem
}
```

- knotc reload
- Ověření:
  - Počkejte na útok, nebo lokálně:
    - for i in $(seq 100); do dig example.com @127.0.0.1; done
  - Výpis logu
  - sudo tcpdump -i eth0 port 53

# Pohled do budoucna (Knot DNS 1.5)

- Radikální redukce množství kódu
- Podpora pro query moduly
  - zatím: reverzní záznamy a dnstap
- O 30 – 40% menší spotřeba paměti
- Jednodušší práce s událostmi
- Vydání 1. RC verze během následujících týdnů

# Pohled do budoucna (Knot DNS 1.6)

- Integrace knihovny libdnssec
  - Přechod od OpenSSL ke GnuTLS
  - Podpora pro hardwarová úložiště (HSM)
  - Politika klíčů a podepisování
- Možnost on-line podepisování generovaných záznamů
- Nástroje pro pro práci s klíči
  - Vytváření nových klíčů ...
  - Konverze z a do BIND formátu

# Pohled do budoucna (formát klíčů)

- YAML soubor s popisem veřejných klíčů pro zónu:

```
keys:
  - id: 22e78e67550d4d6ce9008630075638f3037c3648
    ksk: true
    algorithm: 7
    public_key: AwEAAekFD ...
    publish:  2014-04-06 10:30:00
    active: 2014-04-06 10:30:00
  - id: f98cf3fc013be37cfa4eba3a226733205ee7b928
    ksk: false
    algorithm: 7
    public_key: AwEAAeXIb ...
    publish: 2014-04-06 10:30:00
    active: 2014-04-06 10:30:00
```

- Privátní klíče uloženy v PEM souborech

# Děkujeme!

**CZ.NIC Labs • www.knot-dns.cz**
**Jan Kadlec • jan.kadlec@nic.cz**
**Daniel Salzman • daniel.salzman@nic.cz**