Správa a provoz serveru Knot DNS

IT13 Workshop 21. 5. 2013

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

Obsah workshopu

- Krátké představení projektu Knot DNS
- Instalace
- Popis konfigurace a ovládání
- Praktické ukázky (lokálně, mezi sebou)

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 1.2.0 (připravujeme 1.3.0)

Instalace – závislosti

- libtool
- autoconf >= 2.65
- flex >= 2.5.31
- bison >= 2.3
- libssl-dev >= 0.9.8
- liburcu-dev >= 0.5.4 (http://lttng.org/urcu)
- (texinfo)

Možnosti instalace

- Binární balík z příslušného repozitáře
- Balík zdrojového kódu:
  - http://www.knot-dns.cz
- Zdrojový kód z repozitáře git:
  - git clone git://git.nic.cz/knot-dns

Instalace ze zdrojového kódu

- autoreconf -fi
- ./configure --sysconfdir=/etc/knot/
- make
- make install
- (make html)

Hlavní části Knot DNS

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

1. příklad: Minimální konfigurace

- /etc/knot/knot.conf:

```
system {
  storage "/var/lib/knot";
}

interfaces {
  ipv4 { address 127.0.0.1@5353; }
}

zones {
  example.com. {
    file "example.com.zone";
  }
}

log {
  syslog { any all; }
}
```

1. příklad: Ověření funkčnosti

- Spuštění serveru:
  - knotc start
- Ověření chodu server:
  - netstat -lnptu
  - tail -n 20 /var/log/syslog
- Dotaz na server:
  - dig @127.0.0.1 -p 5353 example.com ANY

2. příklad: Možnosti logování

- Umístění logu:
  - stdout/stderr – pouze pokud neběží jako démon
  - jakýkoliv soubor
  - syslog
- Závažnost:
  - debug, info, notice, warning, error, fatal, all
- Kategorie:
  - server, zone, answering, any

2. příklad: Nastavení logování

- Upravit /etc/knot/knot.conf:

```
log {
  syslog { any all; }
  file “/tmp/knot-server.log” { server info; }
}
```

- Restart serveru:
  - knotc restart
- Ověření nastavení:
  - cat /tmp/knot-server.log

3. příklad: Vzdálená správa

- Do /etc/knot/knot.conf přidat:

```
remotes {
  local { address 127.0.0.1; }
}

control {
  listen-on { address 127.0.0.1@5553; }
  allow local;
}
```

- Restart serveru (zapnutí vzdálené správy):
  - knotc restart

3. příklad: Ověření vzdálené správy

- Ověření nastavení:
  - netstat -lnptu
- Použití vzdálené správy:
  - knotc -s 127.0.0.1 -p 5553 reload
- Ověření funkce:
  - cat /tmp/knot-server.log

4. příklad: Úprava zónového souboru

- Soubor /var/lib/knot/example.com.zone:
  - přidání TXT záznamu:

    example.com. TXT "Knot DNS workshop IT13"
  - navýšení SOA serial:

    2010111213 → 2010111214
- Reload serveru:
  - knotc reload
- Ověření aktualizace zóny:
  - dig @127.0.0.1 -p 5353 example.com TXT

5. příklad: Přidání další zóny

- Soubor /var/lib/knot/example2.com.zone
- Do sekce *zones* /etc/knot/knot.conf přidat:

```
example2.com. {
  file “example2.com.zone”;
}
```

- Načtení nové zóny:
  - knotc reload
- Ověření dostupnosti nové zóny:
  - dig @127.0.0.1 -p 5353 example2.com NS +dnssec

6. příklad: Slave server + TSIG

- Do /etc/knot/knot.conf přidat:

```
keys {
  master-key hmac-sha256
"FWdYWd4PVIFhN2g6TvK2eIccm8kxk7Sh658CIV8aGTc="
}
```

- Dále přidat do *remotes* a *zones:*

```
master {
  address x.x.x.x;
  port 5354;
  key master-key;
}

example3.com. {
  file “example3.com.zone”;
  xfr-in master;
  notify-in master;
}
```

6. příklad: Transfer zóny

- Stav před transferem:
  - dig @127.0.0.1 -p 5353 example3.com NS
- Aktualizace nastavení (transfer zóny):
  - knotc reload
- Ověření dostupnosti zóny:
  - cat /tmp/knot-server.log
  - dig @127.0.0.1 -p 5353 example3.com NS

7. příklad: Master server (1)

- Určete si role (master/slave)
- Master /etc/knot/knot.conf:

```
interfaces {
   ipv4 { 0.0.0.0@5353; }
}

remotes {
   soused { address soused_ip@5353; }
}

zones {
  example4.com. {
    file "example4.com.zone";
    xfr-out soused;
    notify-out soused;
  }
}
```

7. příklad: Master server (2)

- Slave /etc/knot/knot.conf:

```
remotes {
    soused { address soused_ip@5353; }
}

zones {
  example4.com. {
    file "example4.com.zone";
    xfr-in soused;
    notify-in soused;
  }
}
```

- Master restart, slave reload a ověřit funkčnost
- Prohoďte si role

8. příklad: Dynamický update zóny (1)

- Vyjdeme z nastvení pro master example4.com
- Soubor /etc/knot/knot.conf:

```
Remotes {
    all { address 0.0.0.0/0; }
}

zones {
  example4.com. {
     ...
     update-in all;
  }
}
```

- Reload serveru

8. příklad: Dynamický update zóny (2)

- Spustíme *knsupdate/(*nsupdate – bind9utils)

```
> server localhost 5353
> zone example4.com.
> update add ddns.example4.com. 3600 A 1.2.3.4
> update del mail.example4.com.
> show
> send
```

- Ověříme změny:
  - tail /var/log/syslog
  - dig @127.0.0.1 -p 5353 ddns.example4.com a
  - dig @127.0.0.1 -p 5353 mail.example4.com any

9. příklad: IXFR z lokálních změn (1)

- Do /etc/knot/knot.conf přidat:

```
zones {
  example4.com. {
    ...
    ixfr-from-differences on;
  }
}
```

- Reload serveru
- Udělat libovolnou změnu v zónovém souboru:
  - přidat/odebrat záznam, změnit data

9. příklad: IXFR z lokálních změn (2)

- Zvýšit serial v SOA záznamu!
- Reload serveru
- Ověření:
  - tail /var/log/syslog
  - slave:

    dig @127.0.0.1 -p 5353 example4.com soa
  - master (nutné nejprve povolit xfr pro localhost):

    dig @127.0.0.1 -p 5353 example4.com ixfr=2010111214

Děkujeme!

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