Knot DNS workshop

CZ.NIC Labs
Daniel Salzman / daniel.salzman@nic.cz
Jan Kadlec / *jan.kadlec@nic.cz*
24. 11. 2012

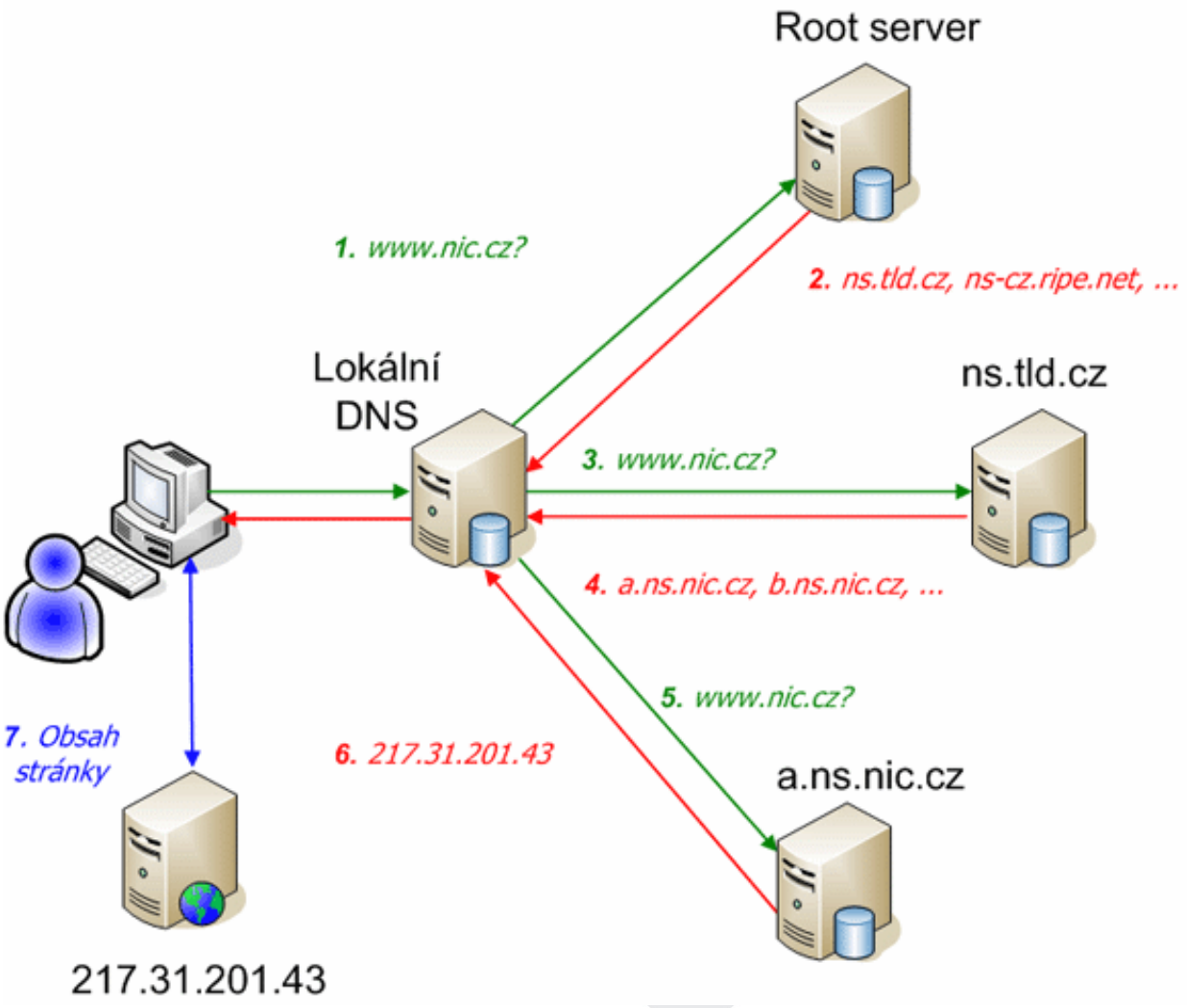
cz.nic | SPRÁVCE DOMÉNY CZ

Obsah workshopu

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

- Rozsah ~ 2 x 2 hodiny

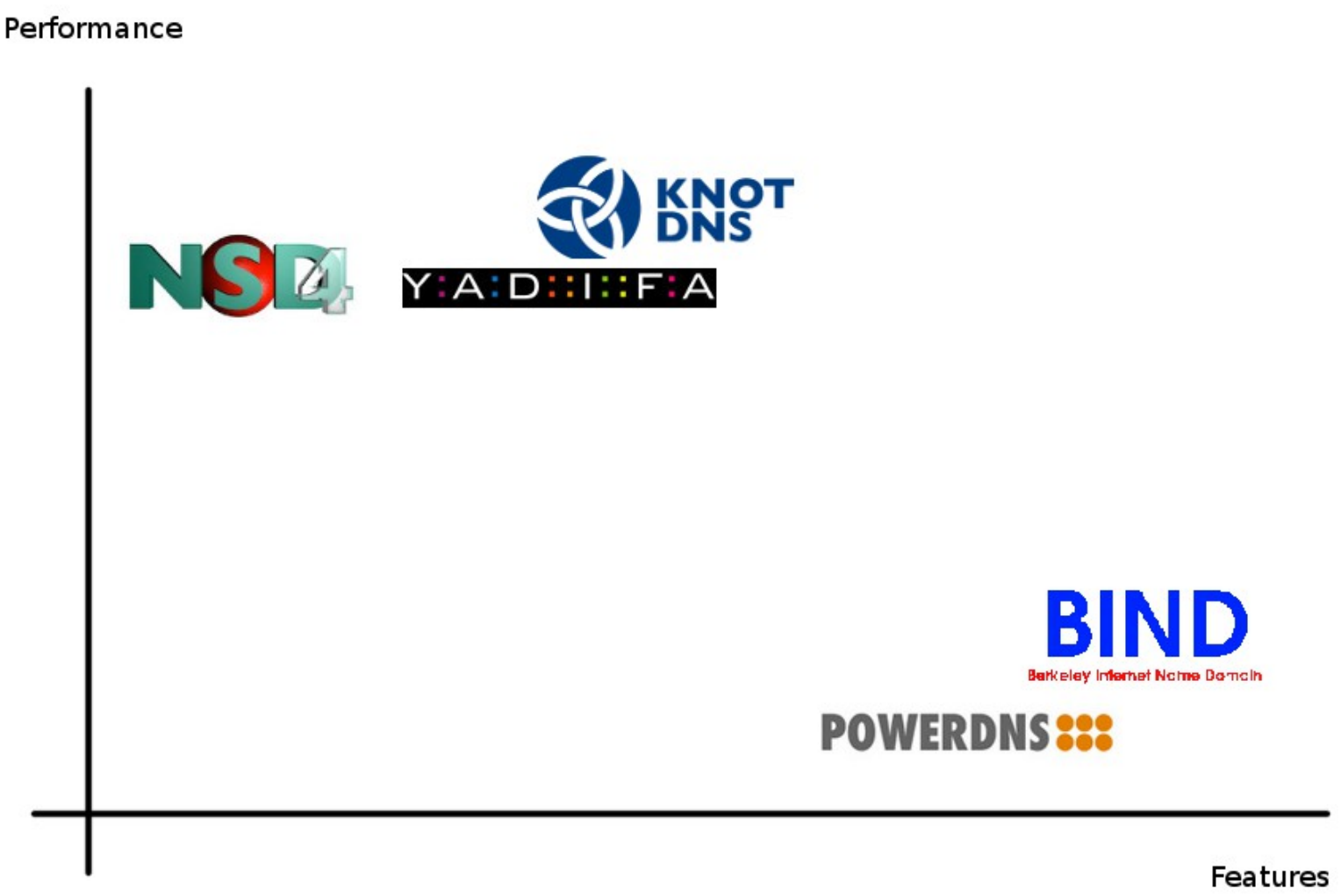
DNS


Root server
1. www.nic.cz?
2. ns.tld.cz, ns-cz.ripe.net, ...
Lokální
DNS
ns.tld.cz
3. www.nic.cz?
4. a.ns.nic.cz, b.ns.nic.cz, ...
5. www.nic.cz?
7. Obsah
stránky
6. 217.31.201.43
a.ns.nic.cz
217.31.201.43

Knot DNS

- Autoritativní DNS server
- Open source – vývoj v CZ.NIC Labs
- Výkonný, stále odpovídá – bez zámků
- Master / slave – velké zóny, mnoho zón
- Transfery – AXFR, IXFR
- EDNS0, TSIG, DDNS
- Možnost vzdálené správy

Srovnání s konkurencí



Významná nasazení Knot DNS

- L-root – experimentální provoz
- .cz, .dk, .ru – slave server
- CZ.NIC – slave server
- igloonet.cz
- hosting90.cz

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)

Instalace

- Binární balík z repozitáře – Debian backports, Ubuntu, Fedora, FreeBSD, NetBSD, ...
- Balík zdrojového kódu:

  http://www.knot-dns.cz
- Zdrojový kód z repozitáře git:

  git clone git://git.nic.cz/knot-dns -b release1.2

Instalace ze zdrojového kódu

- autoreconf -fi
- ./configure
- make
- make install
- (make html)

Hlavní části Knot DNS

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

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: Základní funkčnost

- Spuštění serveru:

  knotc start

- Ověření chodu serveru:

  netstat -lnptu

- Dotaz na server:

  dig @127.0.0.1 -p 5353 example.com. NS

Možnosti logování

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

2. příklad: Nastavení logování

- Upravit /etc/knot/knot.conf:

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

- Restart serveru:

  knotc restart

- Ověření nastavení:

  cat /tmp/knot-server.log

3. příklad: Vzálená 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:

  knotc restart

- Ověření komunikace:

  knotc -s localhost reload

4. příklad: Úprava zóny

- Soubor /var/lib/knot/example.com.zone:
  - přidat TXT záznam do vrcholu zóny:

    example.com. TXT “Knot Workshop IT12”
  - zvýšit SOA serial o 1:

    2012112401 → 2012112402
- Překlad zóny a její aktualizace:

  knotc compile

  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 /etc/knot/knot.conf přidat:

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

- Překlad zóny a její načtení:

  knotc compile

  knotc reload

- Ověření dostupnosti zóny example2.com:

  dig +dnssec @127.0.0.1 -p 5353 example2.com. NS

6. příklad: Slave server + TSIG

- Do /etc/knot/knot.conf přidat:

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

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

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

6. příklad: Zprovoznění

- Sledování logu:

  tail -f /var/log/syslog

- Načtení zóny:

  knotc reload

- Ověření dostupnosti zóny:

  dig @127.0.0.1 -p 5353 example3.com. NS

7. příklad: Knot jako master

- Určete si role a pak se v nich vystřídejte
- Master: do /etc/knot/knot.conf přidat:

```
interfaces {
   outer { 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: Knot jako master

- Slave: do /etc/knot/knot.conf přidat:

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

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

- Prohoďte si role a zkuste to naopak
- Ukončete cvičení s zónou example4.com nakonfigurovanou jako master – budeme potřebovat dále.

8. příklad: Změna zóny s DDNS (1)

- Budeme používat tool **nsupdate**

  balíček bind9utils

- Do /etc/knot/knot.conf přidejte:

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

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

8. příklad: Změna zóny s DDNS (2)

- Spustit **nsupdate -v** (bez zabezpečení)

```
> server localhost 53533
> zone example.com.
> update add ddns.example.com. 3600 A 1.2.3.5
> show
> send
```

- Ověřit, že se update zdařil
  - Digem

    dig ddns.example.com. A @127.0.0.1 -p 53533

    dig example.com. SOA @127.0.0.1 -p 53533
  - Kontrola logu

8. příklad: Změna zóny s DDNS (3)

- Spustit **nsupdate -v** (bez zabezpečení)

```
> server localhost 53533
> zone example.com.
> update delete ddns.example.com. A
> show
> send
```

- Oveřit, že se update zdařil
  - Digem

    dig ddns.example.com. A @127.0.0.1 -p 53533

    dig example.com. SOA @127.0.0.1 -p 53533
  - Kontrola logu

Generování diferencí pro IXFR

- Direktiva **ixfr-from-differences**
  - Lze zapnout pro všechny zóny nebo jednotlivě

- Workflow:
  - Ručně editovat zónový soubor
  - Změnit serial v SOA
  - knotc compile, knotc reload [jméno zóny]
  - Transfer na slave

9. příklad: IXFR-out z lokálních změn

- Zapnout **ixfr-from-differences** v konfigu:

```
zones {
  example4.com. {
    file "example.com.zone";
    xfr-out soused;
    ixfr-from-differences on;
    ...
  }
}
```

- Udělat libovolnou změnu do zónového souboru
  - Přidat/odebrat RR, změnit RDATA, změna RRSIG
- **Zvýšit SOA serial** – jinak se nestane nic

9. příklad: IXFR-out z lokálních změn

- Překompilovat zónu a reload serveru

  knotc compile

  knotc reload

- Kontrola aktuálního serialu
  - V logu, digem
- Oveření, že slave má aktuální zónu
- Nebo ještě lépe:

  dig example.com. IXFR=201211240X @127.0.0.1 -p 5353

Jak přeložit s ladícími výpisy

- Na výběr jsou tyto oblasti:
  - server, zones, xfr, packet, dname, rr, ns, hash, compiler, stash
- A tyto úrovně podrobnosti:
  - brief, verbose, details
- Napište a my vám poradíme, co zapnout :)
- Jako parametr configure skriptu:

./configure --enable-debuglevel=details –enable-debug=ddns,rr

Jak nás kontaktovat

- Věřejný mailing list:

  knot-dns-users@lists.nic.cz
- Bug reporty:

  knot-dns@labs.nic.cz
- Vývojářský systém:

  https://git.nic.cz/redmine/projects/knot-dns/

Děkujeme!

knot-dns.cz

jan.kadlec@nic.cz

daniel.salzman@nic.cz