DNS – Domain Name System

Tomáš Richter

Obsah

Motivace DNS

Jednotlivé uzly v internetu jsou identifikovány pomocí IP adres, které jsou celosvětově unikátní. Ty jsou ale těžce zapamatovatelé a neříkají nic o umístění uzlu v síti. Proto se spolu s IP adresami používají symbolická doménová jména. Je tedy potřeba umět přiřazovat doménovému jménu IP adresu a opačně. Původně tento překlad probíhal pomocí záznamů v `/etc/hosts`. Toto řešení se však společně s rozšiřováním internetu stalo napoužitelné a byl tedy navržen DNS.

Pojmy DNS

DNS
: zkratka může podle kontextu znamenat celkový systém, name server nebo protokol

Hierarchie domém
: . > cz > muni > fi > lab; stromová struktura; delegování autorit

FQDN
: Fully Qualified Domain Name; celosvětově jedinečné; lab.fi.muni.cz

Top-level domains
: domény národní a generické; nad nimi ještě doména "."

Národní domény
: vymezené územím státu; dvouznakový název – ISO3166

Generické domény
: Nadnárodní; .com, .edu, .net, .int, .org, .mil, .gov, .info, ...

Name server
: server překládající jména v doménovém tvaru na IP a naopak; každá doména musí mít (alespoň jeden) nameserver

Primary DNS
: name server nastavovaný správcem domény; právě jeden v doméně

Secondary DNS
: záložní name server (záloha dat, dostupnost); automaticky zrcadlí obsah primárního DNS

Cache-only DNS
: server se pouze táže dál a uchovává si záznamy; nemá doménu

Autoritativní a neautoritativní odpověď/server
: každý server je autoritativní pro vlastní doménu (pokud ji má – viz. cache-only servers); autoritativní odpověď pokud server odpovídá na dotaz o vlasní doméně; neautoritativní pokud odpovídá z cache

Kořenové DNS
: name servery pro doménu "."; v současnosti 13 kořenových name serverů označených písmeny A až M

Resolver

klient DNS – tazatel; v Linuxu standartní knihovna C; nastavení `/etc/resolv.conf`, `/etc/nsswitch.conf`

```
#/etc/resolv.conf
nameserver 192.168.1.254 #adresa name serveru, ktereho se resolver dotazuje
```

```
#/etc/nsswitch.conf
hosts: files dns #mrkni nejdriv do /etc/hosts a pak se teprv ptej DNS
```

Jak to funguje

Resolver se ptá nejbližšího name serveru. Pokud server zná odpověd, odpoví ihned. Pokud server nezná odpověď', může se zachovat dvěma způsoby:

- vrátí tazateli adresu (některého) kořenového DNS
- ptá se sám kořenového DNS a očekává odpověď' – tj. chová se jako resolver

Resolver takto zjistí (v nejhorším případě) adresy všech DNS pro jednotlivé domény v pořadí od nejvýznamější (cz, muni, fi, lab) a nakonec požadovanou IP. Aby se pokaždé nemusela celá procedura opakovat, DNS si určitou dobu pamatují odpovědi.

Konfigurace DNS v Linuxu

Nejpoužívanějšími implementacemi DNS v Linuxu jsou BIND a djbdns. BIND (Berkeley Internet Name Domain) je referenční implementací DNS.

[Djbdns je produkt profesora Daniela J. Bernsteina. Mezi jeho hlavní přednosti patři přehlednost kódu, bezpečnost, rychlost a implicitní chrootované prostředí. Tento server narozdíl od referenčního BINDu řeší spousty věcí jinak nebo je z důvodu bezpečnosti neřeší vůbec.]

Zde se budeme zabývat nastavení BINDU (verze 9).

Hlavní konfigurační soubor je `/etc/named.conf`, který může vypadat např. takto (převzato z DNS HOWTO):

```
options {
        directory "/var/named";
};

controls {
        inet 127.0.0.1 allow { localhost; };
};

zone "." {
        type hint;
        file "root.hints";
};

zone "localhost" {
```

```
  type master;
  file "pz/localhost";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "pz/127.0.0";
};

zone "linux.bogus" {
        type master;
        notify no;
        file "pz/linux.bogus";
};

zone "196.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "pz/192.168.196";
};
```

Tento konfigurační soubor definuje zóny localhost a linux.bogus a jejich reversní zóny. Konfigurace těchto zón se nachází v adresáři `/var/named/pz`. Pro tyto zóny je server *primární*.

Ukázka nastavení zóny *linux.bogus* v souboru `/var/named/pz/linux.bogus`

```
$TTL 3D
@       IN      SOA     ns.linux.bogus. hostmaster.linux.bogus. (
                        199802151       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        3H )            ; minimum, seconds
;
                TXT     "Linux.Bogus, your DNS consultants"
                NS      ns              ; Inet Address of name server
                NS      ns.friend.bogus.
                MX      10 mail         ; Pri mary Mail Exchanger
                MX      20 mail.friend.bogus. ; Secondary Mail Exchanger

gw              A       192.168.196.1
                TXT     "The router"

ns              A       192.168.196.2
                MX      10 mail
                MX      20 mail.friend.bogus.
www             CNAME   ns

donald          A       192.168.196.3
                MX      10 mail
                MX      20 mail.friend.bogus.
                TXT     "DEK"

mail            A       192.168.196.4
                MX      10 mail
                MX      20 mail.friend.bogus.

ftp             A       192.168.196.5
                MX      10 mail
                MX      20 mail.friend.bogus.
```

Nastavení reverzní zóny *196.168.192.in-addr.arpa* v souboru `/var/named/pz/192.168.196`:

```
$TTL 3D
@       IN      SOA     ns.linux.bogus. hostmaster.linux.bogus. (
                        199802151 ; Serial, todays date + todays serial
                        8H      ; Refresh
                        2H      ; Retry
                        4W      ; Expire
                        1D)     ; Minimum TTL
                NS      ns.linux.bogus.

1               PTR     gw.linux.bogus.
2               PTR     ns.linux.bogus.
3               PTR     donald.linux.bogus.
4               PTR     mail.linux.bogus.
5               PTR     ftp.linux.bogus.
```

Tabulka 1. Typy záznamů

Typ	Název	Funkce
SOA	Start Of Authority	Uvádí nastavení pro doménu
NS	Name Server	Označuje Name Server domény
A	host Adress	Konkrétní adresa IPv4
AAAA	host Adress	Konkrétní adresa IPv6
MX	Mail eXchange	Poštovní server, záznam obsahuje i prioritu
CNAME	Canonical NAME	Přezdívka; slouží k přiřazení více jmen jedné IP; omezení!
PTR	PoinTeR	Ukazuje na jméno u reverzního překladu
TXT	TeXT	Textová poznámka

Nastavení sekundárního DNS pro zónu linux.bogus v souboru `/etc/named.conf`:

```
zone "linux.bogus" {
        type slave;
        file "sz/linux.bogus";
        masters { 192.168.196.2; };
};
```

a v souboru `/var/named/sz/linux.bogus`:

```
@       IN      SOA     ns.linux.bogus. hostmaster.linux.bogus. (
                        199802151       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds
```

Zóna je přenesena pouze pokud je sériové číslo primárního serveru větší než sériové číslo sekundárního serveru. Pokud je primární server nedostupný delší dobu, než je doba expirace, sekundární server smaže tuto zónu a přestává být pro ni serverem.

Bezpečnost

Předchozí nastavení bylo jen základní, pro bezpečnější provoz je doporučeno nastavit několik omezení

Omezení přenosů zóny

Není třeba poskytovat všem kompletní informace o nastavení serveru. Stačí je poskytovat sekundárním serverům. Přidání nastavení **allow-transfer** do `/etc/named.conf`:

```
zone "linux.bogus" {
      allow-transfer { 192.168.1.4; localhost; };
};
```

Ochrana proti spoofování

Zakážeme dotazy na domény, které nevlastníme, kromě dotazů z vnitřních strojů. Změny v `/etc/named.conf`:

```
options {
      allow-query { 192.168.196.0/24; localhost; };
};

zone "linux.bogus" {
      allow-query { any; };
};

zone "196.168.192.in-addr.arpa" {
      allow-query { any; };
};
```

Ještě také povolíme rekursivní dotazy pouze pro vnitřní stroje:

```
options {
        allow-recursion { 192.168.196.0/24; localhost; };
};
```

Spuštění serveru bez rootovských práv

Nespouštějte server se superuživatelskými právy. Vytvořte uživatele a skupinu (např. named) a spouštějte server jako tento uživatel. Nekteré distribuce toto dělají automaticky.

Spuštění serveru v chrootovaném prostředí

Je silně doporučeno spouštět BIND v chrootovaném prostrědí. Případný útočník ovládnuvší proces tak nezíská přístup k jiným zdrojům na vašem počítači. Ke spouštění serveru v chrootovaném prostředí existuje několik vyčerpávajících HOWTO (např. pro BIND9[1]), tudíž jen v kostce.

Do adresáře, kam chceme chrootovat zkopírujeme potřebné soubory (i s adresářovou strukturou):

- *etc* – `/etc/named.conf`, `/etc/ld.so.conf`, `/etc/localtime`
- *lib* – soubory vybramé pomocí `ldd /usr/sbin/named`; poté je třeba spustit `ldconfig -r <chootovany adresar>`
- *dev* – je třeba vytvořit speciální soubory `null` a `random`
- *var* – vytvoříme adresář `var/run/named` s právem zápisu pro uživatele pod kterým budeme server spouštět
- Spustíme named pod s právy vytvořeného užibatele a v chrootovaném prostředí: `/usr/sbin/named -u <uzivatel pro server> -t <chrootovaci adresar>`

Nástroje

- **named-checkconf**, **named-checkzone** – kontrola konfiguracnich souboru named
- **dig** – výpis informací o serveru
- **host** – výpis informací o serveru, bez parametrů prostý překlad adres
- **nslookup** – interaktivní pokládání dotazů name serverům

Bližší informace viz. manové stránky :o)

Použité zdroje a odkazy

Informace k referátu jsem čerpal ze stránek DNS HOWTO[2], Chroot-BIND HOWTO[3] a některých předchozích referátů (citace o djbdns).

Další informace o DNS: RFCs[4], ISC BIND[5], článek o djbdns na root.cz[6] a mnoho dalšího[7].

Poznámky

1. http://www.linuxsecurity.com/docs/LDP/Chroot-BIND-HOWTO.html
2. http://www.faqs.org/docs/Linux-HOWTO/DNS-HOWTO.html
3. http://www.linuxsecurity.com/docs/LDP/Chroot-BIND-HOWTO-1.html
4. http://www.rfc-editor.org/

5. http://www.isc.org/index.pl?/sw/bind/
6. http://www.root.cz/clanky/djbdns-alternativni-dns-server/
7. http://www.google.com/search?q=dns