**DNS (systém správy doménových jmen)**

* systém DNS slouží pro překlad doménových názvů na IP adresy a obráceně
* systém DNS má stromovou strukturu
* doménová jména se skládají z domén jednotlivých úrovní, nejvyšší (nejobecnější je vpravo), směrem doleva se větví a konkretizují (strom)
* vyhledání příslušného záznamu probíhá rekurzivně
* hledání probíhá v databázích DNS serverů, kdy každý obsluhuje určitou část DNS stromu, tzv. zónu

**DNS servery můžeme rozdělit na:**

* kořenové
* autoritativní
* rekurzivní (cachovací)

**Kořenové servery**

Obsluhují kořenovou doménu, která je označena znakem "." úplně vpravo, kořenová doména obsahuje záznamy o doménách 1. úrovně, neboli TLD - top level domain (.cz, .com, .net, .org). Kořenových serverů je 13, aby se vešly do jednoho UDP paketu s dotazem, jsou značeny písmeny abecedy A až M. Ve skutečnosti je jich fyzicky více než 13, dotaz je směrován pomocí anycastu na nejbližší servery, vyrovnává se tím zátěž.

**Autoritativní servery**

Obsluhují záznamy konkrétní části DNS stromu (např. všechny pro doménu .cz, spsmb.cz atd.). Informace jsou uloženy v tzv. zónových souborech.

**Rekurzivní servery**

Slouží klientům k provedení rekurzivních dotazů v DNS stromu, výsledky dotazů ukládají do cache na určitou dobu, snižují tak zátěž především kořenových serverů)

**DNS zóny**

* **dopředné (forward) zóny** - obsahují jednotlivé záznamy (A, AAAA, CNAME, MX, NS), překlad doménových jmen na IP adresy
* **reverse zóny** - obsahují záznamy PTR pro překlad IP adres na doménová jména, nejvyšší doména je v tomto případě pro IPv4 **in-addr.arpa**. a pro IPv6 **ip6.arpa.**

**DNS záznamy**

* **A** - mapuje IP adresu k doménovému jménu

např. název IN A 95.85.193.130

* **AAAA** - totéž jako A, ale v IPv6
* **CNAME** - alias (jiný název) pro zavedený A záznam

např. alias IN CNAME název

* **MX** - server pro elektronickou poštu (mail exchange)

např. doména IN MX 10 poštovní\_server

* **NS** - záznam o autoritativním jmenném serveru pro zónu

např. zóna IN NS jmenný\_server

* **SOA** - začátek zóny (start of authority), obsahuje jméno primárního serveru, e-amil správce, údaje serial, refresh, retry, expire a ttl

**serial** - sériové číslo zóny (datum + pořadí)

**refresh** - jak často se mají obnovovat data na podřízených serverech

**retry** - pokus o opětovné načtení zóny z primárního serveru v případě selhání

**expire** - čas po kterém je server prohlášen jako nedostupný, po tuto dobu budou sekundární servery poskytovat informace o zóně klientů, pak je označí za zastaralé

**ttl** - časová platnost údajů negativní TTL cache (údaje o neexistujících záznamech)

* **PTR** - převádí IP adresu na jméno
* např. 10 IN PTR host.doména

**Získávání informací z DNS stromu**

nástroje:

* nslookup
* host
* dig

Pomocí nástroje **dig** můžeme získat poměrně jednoduše přehledné údaje.

Syntaxe:

dig @dns-server doménový\_název typ dotazu

např. příkazem dig @a.root-servers.net spsmb.cz se dotážeme na nejbližší DNS server obsahující přesnější údaje o doméně spsmb.cz.

Pomocí rekurzivních dotazů v jednotlivých částech DNS stromu získáme podrobné informace o konkrétním doménovém jménu.

**DNS server v Linuxu**

Velmi rozšířený je balík bind9 z konsorcia ISC, aktuálně dostupný ve verzi 9.10. Na balíku bind jsou založeny i DNS servery a klienty v operačních systémech Microsoft Windows.

**Instalace**

apt-get install bind9 bind9utils bind9-doc

Instalovanou verzi zjistíme příkazem:

bind9-config --version

**Konfigurace**

Pro zvýšení bezpečnosti je doporučeno provozovat bind v prostředí **chroot**.

**Základní nastavení**

/etc/default/bind9

RESOLVCONF=(yes|no) - určuje, jestli se má bind po startu zapsat jako DNS resolver do /etc/resolv.conf

OPTIONS="-u bind"

**Můžeme změnit na:**

OPTIONS="-4 -u bind" pro podporu pouze IPv4

Pro Debian 8 a vyšší používající systemd je konfigurace v:

/etc/systemd/system/multi-user.target.wants/bind9.service

**Konfigurace klíčů**

/etc/bind/rndc.key

Zde najdeme klíč TSIG pro provádění transakcí. Budeme ho potřebovat pro nastavení aktualizace pomocí DHCP. Klíč můžeme vygenerovat nový.

**Konfigurace základních vlastností DNS serveru**

/etc/bind/named.conf.options

acl "trusted" {   
 127.0.0.0/8; #konfigurace povolených adres pro komunikaci  
 jiná-ip/maska;  
};

options {  
 directory "/var/cache/bind"; #pracovní adresář  
 forwarders {  
 8.8.8.8; #nastavení forwarderů  
 8.8.4.4;   
 };  
 dnssec-validation auto; #pokus o kontrolu odpovědí ze zón s nastaveným DNSSEC  
 auth-nxdomain no; #autoritativní odpověď NXDOMAIN (neexistuje)  
 listen-on-v6 { none; }; #naslouchání pro IPv6  
 allow-recursion { trusted; }; #komu povolit rekurzivní dotazy  
 listen-on { 127.0.0.1; jiná-ip; }; #naslouchat na adrese  
 allow-transfer { none; }; #seznam adres strojů, které mohou žádat transfer zóny  
};

**Konfigurace zón**

zone "dopředná-zóna (doména.local)" {  
 type master; #typ zóny  
 file "/etc/bind/adresář/db.dopředná-zóna"; #umístění zónového souboru  
 allow-transfer { adresa-počítače; }; #povolení transferu zóny  
};

zone "reverzní-zóna" {  
 type master;  
 file "/etc/bind/adresář/db.reverzní-zóna";  
 allow-transfer { adresa-počítače; };  
};

**Hlavní konfigurační soubor**

/etc/bind/named.conf

sem vložíme odkazy na předešlé soubory

include /etc/bind/named.conf.options;  
include /etc/bind/named.conf.local;  
include /etc/bind/named.conf.default-zones; #výchozí zóny

**Zónové soubory**

Výchozí zóny:

* **db.0** - broadcast
* **db.127** - reverzní zóna localhost
* **db.255** - broadcast
* **db.empty** - prázdná zóna pro lokální sítě (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
* **db.local** - dopředná zóna localhost
* **db.root** - zóna s root servery

**Soubor dopředné zóny**

$TTL 604800

@ IN SOA doména. mail. (  
serial  
refresh  
retry  
expire  
negative cache TTL )

;nameservery

@ IN NS jmenná-sdresa-nameserveru.  
adresa-ns IN A ip-adresa

;zónové záznamy  
něco IN A ip-adresa atd.

**Soubor reverzní zóny**

$TTL 604800

@ IN SOA doména. mail. (  
serial  
refresh  
retry  
expire  
negative cache TTL )

;nameservery

@ IN NS jmenná-sdresa-nameserveru.

;zónové záznamy  
adresa IN PTR FQDN.

**Nástroje pro správu**

**rndc reload** - opětovné nahrání konfiguračních a zónových souborů  
**named-checkconf** - kontrola konfiguračních souborů  
**named-checkzone** *doména zónový soubor* - kontrola zónového souboru

**Dynamická aktualizace z DHCP**

**Vygenerujeme nový TSIG klíč**:

rndc-confgen –a

soubor si zkopírujeme a pojmenujeme dle potřeby např. na ddns.key

cp /etc/bind/rndc.key /etc/bind/ddns.key

**nastavíme vlastníka a oprávnění:**

chown root:bind /etc/bind/ddns.key  
chmod 640 /etc/bind/ddns.key

**a upravíme název klíče v tomto souboru:**

key "ddns-key" { …….

Zónové soubory zkopírujeme do **/var/cache/bind**, abychom mohli do souborů dynamicky zapisovat. Přístup do **/etc/bind** pro zápis jiným uživatelem, než je **root**, nepovolujeme.  
Zkontrolujeme nastavení oprávnění na zkopírovaných souborech (**644**) a vlastníka, skupinového vlastníka (oba by měly být **bind**).

**upravíme soubor /etc/bind/named.conf.local:**

include /etc/bind/ddns.key

zone "dopředná-zóna (doména.local)" {  
 type master; #typ zóny  
 file "/var/cache/bind/db.dopředná-zóna"; #umístění zónového souboru  
 allow-transfer { key ddns-key; }; #TSIG klíč  
}

zone "reverzní-zóna" {  
 type master;  
 file "/var/cache/bind/db.reverzní-zóna";  
 allow-transfer { key ddns-key; };  
};

**TSIG klíč zkopírujeme do adresáře /etc/dhcp:**

chown root:bind /etc/dhcp/ddns.key  
chmod 640 /etc/dhcp/ddns.key

**upravíme konfigurační soubor /etc/dhcp/dhcpd.conf:**

vzorový soubor:

ddns-updates on; #zapnutí automatických aktualizací  
ddns-update-style standard; #způsob aktualizace  
update-static-leases on; #aktualizovat DHCP statické zápůjčky  
ignore vlient-updates; #ignorovat pokusy o update ze strany klienta

default-lease-time 600;  
max-lease-time 7200;

authoritative;

include "/etc/dhcp/ddns.key"; #načtení TSIG klíče

zone domena.llocal. { #dopředná zóna  
 primary 127.0.0.1;  
 key ddns-key;  
}

zone 0.0.10.in-addr.arpa. { #reverzní zóna  
 primary 127.0.0.1;  
 key ddns-key;  
}

subnet 10.0.0.0 netmask 255.255.255.0 {  
 range 10.0.0.50 10.0.0.150;  
 option domain-name-servers 10.0.0.1;  
 option domain-name "doména.local";  
 option routers 10.0.0.1;  
 ddns-domainname "doména.local"; #ddns dopředná zóna  
 ddns-rev-domainname "0.0.10.in-addr.arpa"; #ddns reverzní zóna  
}

Po úpravě provedeme restart služeb (pc) a spustíme klienta i server. V zónových souborech zkontrolujeme, zda-li automatická aktualizace pracuje. V případě potřeby příkazem **rndc sync –clean** provedeme synchronizaci žurnálového souboru a zónových souborů.