Linux jako router, firewall, DHCP server, proxy a DNS cache, 2. část

Lukáš Zapletal
lukas.zapletal@liberix.cz

Poskytované služby

- DHCP, DNS
- HTTP
- e-mail (SMTP, POP3, IMAP)
- FTP, Samba
- ...
- ssh

SSH

- openssh - sshd (server),
  ssh / Putty a spol (klient)
- doporučuji používat RSA klíče (a vypnout autentizaci hesly - *ChallengeResponseAuthentication no; ChallengeResponseAuthentication no*)
- nebo alespoň vypnout možnost přihlášení roota pomocí hesla (*PermitRootLogin without-password*)
- zabrání se tak možnosti uhádnutí hesla, ssh je **zabezpečený** (nikoli **bezpečný**)

DHCP

- Dynamic Host Configuration Protocol
- nastavení IP, masky, routerů a DNS
- dhcpd (server), dhcpcd (klient)
- princip: klient vyšle do sítě broadcast zprávu „potřebuji adresu“, DHCP server odpoví „tady máš IP, masku, routery, DNS“
- dhclient provede nastavení sítě, upraví routovací tabulku a /etc/resolv.conf

DHCP server

 # cat /etc/dhcpd.conf

```
option domain-name "firma.cz";
option routers 192.168.1.254 192.168.1.253;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
default-lease-time 3600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.100 192.168.1.200;
}

host guru {
    hardware ethernet 08:00:4b:2c:22:23;
    fixed-address 192.168.1.100;
}
```

DNS

DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de facto jako distribuovaná databáze síťových informací. (wikipedia)

DNS

- příklad 1: webhosting firma.cz včetně DNS hostingu - platíte za www prostor, za doménu a za správu domény (balíček)
- příklad 2: webhosting firma.cz (server je ve vaší síti), u providera máte DNS server (správa obvykle webovým rozhraním) - platíte doménu a správu domény
- příklad 3: hosting i DNS server u sebe, platíte jen za doménu

DNS

- dva hlavní typy: autoritativní DNS (primární, sekundární) a caching DNS (neautoritativní)
- caching - pouze si na čas „pamatuje“ DNS záznamy
- typicky bývá v server distribucích nastaven v caching režimu (pro localhost)
- nejpoužívanější server pro DNS je asi ISC BIND (named) - umí oba typy

DNS - typy záznamů

- A (address record) obsahuje IPv4 adresu přiřazenou danému jménu, například když jménu cosi.kdesi.cz náleží IP adresa 1.2.3.4. Pokud je víc A záznamů, server vrací všechny ale v náhodném pořadí.
- CNAME (canonical name record) je alias - jiné jméno pro jméno již zavedené. Typicky se používá pro servery známých služeb, jako je například WWW.

DNS - typy záznamů

- MX (mail exchange record) oznamuje adresu a prioritu serveru pro příjem elektronické pošty pro danou doménu. Tentokrát jsou parametry dva - priorita (přirozené číslo, menší znamená vyšší prioritu) a doménové jméno serveru.
- NS (name server record) ohlašuje jméno autoritativního DNS serveru pro danou doménu.

DNS - typy záznamů

- PTR (pointer record) je speciální typ záznamu pro reverzní zóny.
- SOA (start of authority record) je zahajující záznam zónového souboru. Obsahuje jméno primárního serveru, adresu elektronické pošty jejího správce (zavináč je v ní ale nahrazen tečkou) a následující údaje: serial, refresh, retry, expire a TTL.

  (přebráno z wikipedie-cs)

DNS - zóna

```
$TTL 1w
@           IN    SOA    server.kdesi.cz.  franta.kdesi.cz. (
                         200605140
                         1h
                         5m
                         1w
                         1d
                         )
            IN    NS     server
            IN    NS     ns.jinde.cz.

            IN    MX     10 server
            IN    MX     20 mail.jinde.cz.

cosi        IN    A        1.2.3.4
            IN    AAAA     2001:718:1c01:1:02e0:7dff:fe96:daa8
server      IN    A        1.2.3.1
www         IN    CNAME    server
```

DNS

- BIND není jediným DNS serverem
- někteří provideři používají MyDNS (ten ukládá do SQL databáze MySQL, existuje také rozhraní v PHP pro administraci) - je to pouze autoritativní DNS (neumí vystupovat jako caching server)
- caching server je také dobrý djbdns (ten ale umí pouze cachovat)

Pošta

- MTA - mail transfer agent
- zajišťuje doručování e-mailů ven (odesílání, tzv. relay)
- a přijímání (ukládání do schránek)
- v Linuxu existuje spousty poštovních agentu (MTA): Postfix, qmail, exim, sendmail a jiné
- Postifx - snadný na konfiguraci, dostupná dobrá literatura v češtině, stabilní

Pošta - konfigurace

- doručování - tzv. relay: server přijímá z určitých sítí (vnitřní firemní síť například) poštu k doručení
- může být nastaven jako smart host (veškerou poštu pouze předá nadřazenému systému - např. provider)
- nebo může poštu doručovat přímo na cílový server příjemce (musí mít ale platný DNS záznam, pevnou IP...)

Pošta - konfigurace

- **nikdy** nesmíte povolit relay všem (např. z internetu) - začnou spamovat
- pokud nutně potřebujete umožnit zaměstnancům odesílat poštu vně sítě, pak aktivujte SMTP AUTH, POP before SMTP (ideálně přes SSL); ještě lepší je zprovoznit VPN do firemní sítě
- vždy tedy povolte jen lokální síť (např. síť 192.168.10.0/24)

Pošta - konfigurace

- pro příjem musíte mít platný MX záznam (například pro firma.cz bude v DNS záznam MX onyx.firma.cz)
- typické nastavení všech MTA - snaží se doručit do schránky uživatele na linuxovém systému, pokud uživatele nenajde, poštu odmítá
- uživatelé se mohou přes ssh přihlásit a poštu si číst

Pošta - konfigurace

- dnes je trend používat vzdálené MUA
- je třeba tedy nainstalovat POP3/IMAP server a schránky zpřístupnit přes síť
- opět doporučuji instalovat zabezpečené varianty (SSL, cram) a zakázat plain
- POP3 - jednoduchý, IMAP - ukládání na serveru, pomalejší, hodně klientů blbne
- servery: qpopper, dovecot, cyrrus, currier
- pozor na typ schránek: mbox, maildir

Pošta - konfigurace

- další „finty“ s e-mailovými servery:
- virtuální účty a hosté, konference, záložní servery, aliasy - zástupné názvy
- doménový koš - pro neexistující účty
- procmail - nástroj pro třídění a přeposílání pošty
- vacation - automatická odpověď
- antispam - SpamAssasin, DSPAM...
- antiviry

Apache 2 (httpd)

- ve většině distribucí je předkonfigurován (/etc/httpd nebo /etc/apache2)
- HTML soubory jsou obvykle umístěny ve /var/www/htdocs
- Apache 2 je velmi mocný HTTP server umožňující mnoho možných nasazení
- ukázka konfigurace jednoduchého webu
- ukázka virtuálních domén

Samba

- server pro sdílení složek ve Windows
- konfigurace jednoho sdíleného adresáře (public, anonymní přístup) je snadná a je uvedena ve většině tutoriálů
- Samba umí ale víc - domovské adresáře, profily, NT domény, antivirovou kontrolu
- ukázka anonymního sdíleného adresáře
- existuje kvalitní literatura v češtině