

Linux prakticky ako server / 24.časť

V minulej časti sme si povedali, že na vyberanie pošty zo vzdialenej schránky pomocou protokolu POP3 a jej odovzdanie na ďalšie spracovanie slúži program *fetchmail*. Ukázali sme si, ako tento program nakonfigurovať a spúšťať pre klasickú poštovú schránku.

My však chceme vybrať nie obyčajnú poštovú schránku, ale doménový koš. A to sa dnes naučíme.

Doménový koš

Stručne si zopakujme, čo to doménový koš je a ako sa vytvára.

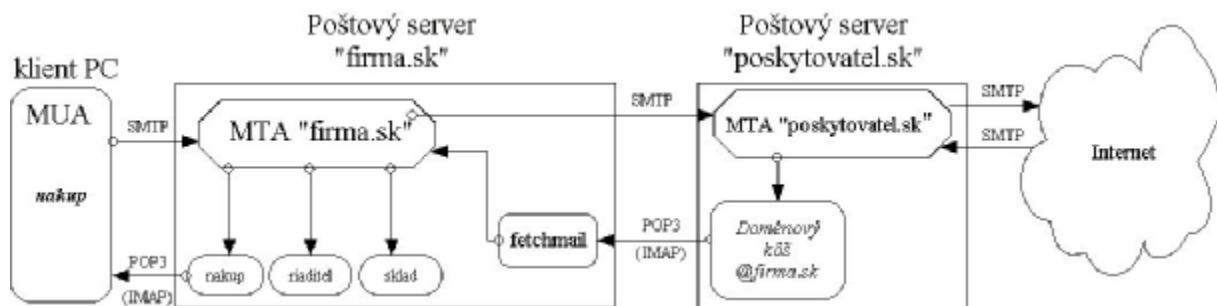
Predstavme si, že sme správcom počítačovej siete určitej firmy alebo školy, ktorá má väčší počet potencionálnych poštových používateľov - adresátov. A my chceme, aby každý používateľ mohol mať svoju vlastnú poštovú schránku.

Pre väčší počet poštových používateľov už nie je vhodné vytvárať sólo účty u poskytovateľa poštových služieb. Okrem toho, že to nie je ekonomické, vznikajú s tým určité problémy, keď pribudne alebo odbudne určitý zamestnanec či žiak, keď sa zmení organizačná štruktúra a podobne. To by sme museli zakaždým žiadať providera o zmenu, a to sú – bohužiaľ – peniažky naviac.

Vtedy je vhodnejšie požiadať o zriadenie doménového koša.

Doménový koš je zvláštna poštová schránka, ktorá sa nachádza u poskytovateľa poštových služieb, ale nesie meno našej poštovej domény. A všetka pošta, ktorá bude adresovaná na túto poštovú doménu, bude uložená do tejto schránky, nezávisle od skutočného adresáta.

Na obrázku č.1 máme vzorovú schému nepriameho doručovania pošty do doménového koša:



U vybraného poskytovateľa poštových služieb, nech je to POSKYTOVATEL(.SK) si necháme vytvoriť poštovú doménu pre našu firmu s názvom FIRMA(.SK). Spravidla každý poskytovateľ – provider je zároveň registrátorom domén, takže všetky potrebné papierovačky vybaví za nás a vytvorí nám poštový účet, ktorý bude mať názov @firma.sk (tento zápis sa v literatúre označuje RHS – *right hand side*).

Nech je na ľavej strane zápisu (označovanej ako LHS – *left hand side*) čokoľvek, bude to doručené do tejto schránky.

(Nech nás teraz netrápi, že ako je to možné, že doména firma.sk existuje na doméne poskytovatel.sk – to sa naučíme, keď sami budeme tvoriť doménové koše pre našich klientov – aj to bude, vydržme!)

Takže do tejto schránky môže prísť pošta pre pána riaditeľa, pre skladníka, šéfa nákupu, ale aj pre zamestnanca, ktorý vôbec neexistuje. Jednoducho všetka!

Pri vytváraní doménového koša nám provider prideli nielen jeho zápis vo formáte @firma.sk, ale tak ako u klasického účtu aj prihlasovacie meno, napr. *fixma* a heslo, nech je to *fi97m45*.

Keby sme sa k doménovému košu pripojili pomocou telnetu na port 110 (ako to urobíme, sme si už viackrát ukázali), listovaním by sme zistili, že sa skutočne v schránke nachádzajú mejly pre rôznych adresátov našej domény *firma.sk*.

Poviete si, že istotne by sa dalo ku košu pripojiť klasickým koncovým klientom MUA. Zadáme prihlasovacie meno a heslo a všetku poшту si stiahneme.

Lenže to by si museli všetci adresáti chodiť čítať poшту k nám a to práve nechceme.

Preto si zase postavíme poštový linuxový server, ktorý nazveme napríklad *rubin* a pridáme mu doménu *firma.sk*, takže plné meno bude *rubin.firma.sk* (ale nemusíme – jeho názov môže byť ľubovoľný, pretože sa nezobrazuje vo svete Internetu).

Skonfigurujeme postfix presne tak, ako sme si to ukázali v minulej časti, pretože skutočnosť, že pracujeme s doménovým košom a nie s klasickou stránkou je vec fetchmailu, nie postfixu!

Na strane nášho servera vytvoríme príslušných adresátov – linuxových používateľov. Nech to sú v našom prípade *nakup*, *riaditel* a *sklad*.

Poštových klientov MTA u jednotlivých používateľov nastavíme štandardným spôsobom.

Teraz už len stačí nastaviť program fetchmail tak, aby dokázal vybrať poštu z doménového koša a odovzdať ju postfixu na zatriedenie do schránok jednotlivých adresátov.

fetchmail a doménový kôš

Na výpise č.2 je vzor konfiguračného súboru *.fetchmailrc* pre spoluprácu s doménovým košom:

```
poll mail.poskytovatel.sk aka firma.sk no dns no envelope
protocol POP3
user fixma password fi97m45 to * here
smtp host localhost
```

Všimnime si, že zmena nastala v prvom riadku za slovom „aka“.

Kontaktujeme síce server *mail.poskytovatel.sk*, ale pre doménu *firma.sk*!

Ďalšia zmena nastala v riadku *user fixma password fi97m45 to * here*.

Znak * (hviezdica) za slovom „to“ symbolizuje, že poštu sťahujeme pre ľubovoľného používateľa linuxového servera.

Na poslednom riadku za parametrom „smtp host“ definujeme, ktorému serveru bude pošta po stiahnutí odovzdaná. „localhost“ značí, že sa jedná o náš server. Tu by mohlo byť uvedené aj plné meno, teda *rubin.firma.sk* alebo IP adresa servera, podľa toho, či je náš server podľa mena dosahateľný alebo nie.

Takže po stiahnutí pošty program fetchmail kontaktuje postfix na našom serveri a poštu mu odovzdá.

Ten poštu prevezme a roztriedi podľa mien, ktoré sa v obálke pošty nachádzajú pred zavináčom, teda podľa LHS.

Ak postfix nájde správneho adresáta, teda meno pred zavináčom sa zhoduje s menom používateľa, poštu uloží do jeho schránky.

Ak nenájde zhodu so žiadnym menom na Linuxe, poštu vráti ako nedoručiteľnú (ak v nastaveniach neurčíme inak – ako si ešte ukážeme).

Podobne ako v minulej časti, aj teraz zabezpečíme pravidelné spúšťanie programu fetchmail (*set daemon*) a jeho automatické štartovanie pri bootovaní systému (*rc.local*) a sťahovanie pošty z doménového koša máme zabezpečené.

Aby sme náš poštový systém zlepšovali, teraz sa budeme venovať určitým „pikoškám“ v nastavení postfixu. Sú to veci z praxe, ktoré nás môžu zaskočiť a my si nebudeme vedieť rady.

Autentifikácia

Na Internete sa čoraz viac rozmáha rozosielanie nevyžiadanej pošty. Tejto pošty sa hovorí aj *spam*. Spameri využívajú nezabezpečené SMTP servery, aby mohli cez nich v podstate nekontrolovateľne šíriť spamy.

Preto sa mnohé servery snažia chrániť pomocou *autentifikácie*. Jedná sa v podstate o to, že ak niekto posielajú poštu cez daný server, musí pred odoslaním pošty poslať serveru svoje meno a heslo. Ten overí, či odosielateľ je jeho klientom s právom odosielať poštu, teda či jeho meno a heslo existuje v jeho databáze. Ak áno, odosielanie mejlu povolí. Ak meno alebo heslo nesedí, alebo nebolo vôbec odoslané, server odmietne poštu prijať a odoslať. Ako sa to prejavuje?

Možno sa nám stalo, že keď sme sa skúšali telnetom pripojiť na niektorého poskytovateľa pomocou protokolu SMTP, nebolo možné s ním komunikovať, lebo vypisoval niečo o overení. Ako príklad si ukážme pripojenie na SMTP server *mail.stonline.sk*:

```
[root@rubin root]# telnet mail.stonline.sk 25
Trying 213.81.152.7...
Connected to mail.stonline.sk (213.81.152.7).
Escape character is '^\'.
```

```
220 smtp.stonline.sk – Server ESMTP (St Online)
mail from: leonka@doma.sk
250 ok
rcpt to: mior@firma.sk
530 5.7.1 Pri odosielaní pošty je nutné použiť meno a heslo. Prosíme nastavte váš e-mailový
program aby používal SMTP autentifikáciu. ....
Relaying not allowed – please use SASL: mior@firma.sk
Timeout while waiting for command.
Connection closed by foreign host.
```

Vidíme, že nie sme schopní odoslať poštu, pretože server je chránený proti neautorizovaným odosielateľom. (Vykonanie autentifikácie priamo pomocou telnetu vôbec nie je jednoduché, preto sa ním teraz nebudeme zaoberať).

Čo je však dôležité, je toto:

Ak nie sme schopní bez autentifikácie odoslať poštu my, tak takisto nebude schopný odoslať poštu postfix!

Čo teraz?

Poznámka:

Najprv si musíme uvedomiť, že na autentifikáciu môžeme nazerať z dvoch strán:

Z jednej strany je to autentifikácia, ktorú vyžaduje náš postfix voči našim klientom. To je prípad, ktorý nás však teraz nezaujíma (ale aj toto si neskôr ukážeme).

Čo nás zaujíma je druhá strana – autentifikáciu po našom postfixe vyžaduje jeho náprotivok na strane poskytovateľa poštových služieb, teda náš postfix je v tomto prípade klientom nadriadeného postfixu, ktorý je nadefinovaný v súbore `main.cf` ako hodnota parametru `relayhost`. A preto sa tomuto hovorí aj overovanie na strane klienta.

Takže musíme postfix nastaviť tak, aby dokázal overovanie na strane klienta.

Urobíme to takto:

- Ø pripravíme si súbor s menom a heslom pre nášho poskytovateľa. Nech sa tento súbor nazýva **`sasl_passwd`** a uložíme ho do adresára `/etc/postfix/`.
- Súbor **`sasl_passwd`** bude mať túto štruktúru:

poskytovateľ meno:heslo

Takže v našom prípade to bude takto:

mail.poskytovatel.sk fixma: fi97m45

- Ø súbor `/etc/postfix/sasl_passwd` uložíme
- Ø spustíme príkaz **`postmap`** na vytvorenie databáze z tohto textového súboru

[root@rubin postfix]# postmap /etc/postfix/sasl_passwd

- Ø v súbore `/etc/postfix/main.cf` musíme zapnúť overovanie klienta. Do tohto súboru dopíšeme tieto riadky:

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd

- Ø súbor `main.cf` uložíme
- Ø reštartujeme postfix, aby si načítal nové nastavenie konfiguračného súboru, napríklad pomocou služby `service`

[root@rubin postfix]# service postfix reload

Odteraz pri odosielaní pošty do sveta pomocou nadriadeného SMTP servera bude náš postfix odosielať meno a heslo na autentifikáciu sám!

Neexistujúci adresát

Povedali sme si, že ak príde do nášho doménového koša pošta pre konkrétného adresáta, bude uložená do jeho poštovej schránky. Ak je však adresát neznámy, bude táto pošta vrátená ako nedoručiteľná.

Občas sa však stáva, že by sme chceli, aby náš server poštu nevracal, ale ju predával niektorému zo skutočných adresátov – používateľov.

Načo je to dobré, to je vždy polemické. V praxi som sa však stretol, že firmy požadujú zachytávanie všetkej pošty, teda aj tej pre neexistujúcich používateľov a to z dôvodu, aby im neušla dôležitá informácia.

Môže sa stať, že sa niekto pri písaní mejlu pánovi riaditeľovi preklepne a namiesto adresy riaditel@firma.sk napíše riditel@firma.sk.

V klasickom prípade sa pošta vráti ako nedoručiteľná tak skúsený odosielateľ adresu opraví a správu pošle znova. Ale čo keď na druhej strane poštového kanála je niekto menej znalý poštových súvislostí a nedokáže posúdiť, či pošta bola doručená alebo nie?

A tak sa spolieha, že jeho správa dorazila na správne miesto....

(to nie je fikcia, to je prax!!!).

Zachytávanie pošty pre neznámych adresátov dosiahneme takto:

Najprv v linuxovom systéme vytvoríme používateľa, ktorému bude táto pošta doručovaná, napríklad s menom **zvysok**.

V konfiguračnom súbore postfixu *main.cf* nastavíme tieto parametre:

```
luser_relay = zvysok
local_recipient_map =
```

(Parameter *local_recipient_map* necháme prázdny, teda za znakom „rovná sa“ nič nevyplníme!)

Postfix reloadneme a odteraz bude pošta, ktorá nemá skutočného adresáta v našej poštovej doméne, ukladaná do poštovej schránky používateľa *zvysok*.

Treba poznamenať, že svetom Internetu sa šíri už vyššie spomínaný spam. Spameri vyzistia odniekiaľ poštové domény a potom slovníkovou metódou sa snažia šíriť spam do našej domény s predpokladom, že sa niekto predsa len na ich reklamy chytí. Potom bude všetok spam zachytený a doručený používateľovi *zvysok*. A preto treba zachytávanie nedoručiteľnej pošty dobre zvážiť.

O morálnosti spameroch a úspešnosti spamu tu nebudeme dnes hovoriť. Ale že sa dá spam značne redukovať, to si ukážeme neskôr.

Aliases

Aliases sú fiktívne mená adresátov, ktorí v skutočnosti na poštovom serveri neexistujú, ale sú zastúpení skutočnými používateľmi.

Predstavme si, že máme v našej firme expedičné oddelenie, kde pracujú pani Nováková, slečna Krásna a pán Radostný.

Všetci traja majú za povinnosť riešiť a vybavovať poštu, ktorá na toto oddelenie prichádza.

Preto vytvoríme fiktívnu poštovú adresu expedicia@firma.sk a nastavíme postfix tak, aby prijatú poštu doručil každému z tohto oddelenia – teda na skutočné poštové adresy novakova@firma.sk, krasna@firma.sk a radostny@firma.sk (používateľ *expedicia* nevytvárame, zato používatelia *novakova*, *krasna* a *radostny* musia v systéme existovať!!!)

Toho dosiahneme takto:

Ø v adresári */etc/postfix/* sa nachádza súbor *aliases*. Ak sa do neho pozrieme, vidíme, že v ňom už existujú určité aliasy, napríklad:

postmaster:	root
admin:	root
manager:	root
operator:	root
webmaster:	root
abuse:	postmaster
all:	postmaster
root:	postfix

Môžeme si overiť, že v linuxovom systéme používatelia *postmaster*, *admin*, *manager*, *operator*, *abuse* a *all* neexistujú. Z vyššie uvedených skutočne existuje iba *root* a *postfix* (vznikol pri inštalácii postfixu).

Ale keď niekto pošle poštu na *postmaster*, *admin*, *manager* alebo *operator*, mala by byť táto v zmysle tohto súboru preposlaná používateľovi *root*. Ale keďže existuje alias, že *root* je *postfix*, tak správy budú priamo doručené adresátovi *postfix*! Podobne keď niekto pošle poštu na adresu *abuse@firma.sk*, tak tá bude poslaná tiež používateľovi *postfix*, aj keď je smerovaná na príjemcu *postmaster* a cez neho na *roota*!

Isto nás zaujíma, prečo je to takto komplikovane urobené, veď by bolo jednoduchšie posilať to rovno rootovi, nie?

Musíme si uvedomiť, že vyberanie schránky heslom *roota* je proti všetkým bezpečnostným pravidlám. Preto bola všetka pošta pomocou súboru *aliases* presmerovaná na používateľa *postfix*.

Vráťme sa však k nášmu príkladu:

Na koniec súboru *aliases* dopíšeme riadok:

expedicia: novakova, krasna, radostny

- Ø súbor *aliases* uložíme
 - Ø z textového súboru */etc/postfix/aliases* musíme vytvoriť databázový súbor *aliases.db*
- Zadáme príkaz:

[root@rubin postfix]# newaliases

- Ø Postfix reloadneme

Odteraz každá pošta adresovaná na adresu *expedicia@firma.sk* bude automaticky doručená všetkým trom pracovníkom expedičného oddelenia.

Presmerovanie pošty (forward)

Stáva sa, že kolega Novák z našej firmy odišiel pracovať inam, a tak chceme, aby pošta adresovaná na jeho starú adresu *novak@firma.sk* bola premerovaná na jeho novú adresu *novak@inafirma.sk*.

Alebo druhý prípad:

Pán Letko odchádza na dovolenku, ale potrebuje poštu čítať aj na dovolenke. Keďže naše bezpečnostné opatrenia siete nedovoľujú čítanie pošty pomocou webmailu cez Internet, budeme po dobu jeho dovolenky preposielať jeho poštu na niektorý z verejných poštových serverov, ktorí webmail umožňujú, napríklad na VEREJNY.SK.

Paľkovi Letkovi založíme verejný poštový účet s adresou *pavel.letko@verejny.sk*.

Preposielanie (forwarding) pošty zabezpečíme takto:

- Ø v domovskom adresári používateľa *letko* vytvoríme súbor ***.forward*** (aj s tou bodkou)
- Ø do súboru */home/letko/.forward* zapíšeme adresu, kam sa má pošta preposielať, teda

pavel.letko@verejny.sk

- Ø súbor *.forward* uložíme

Hotovo, éto vsjo!

Odteraz bude pošta pre Paľka Letka (môjho dobrého bradatého kamaráta) bez nášho pričinenia presmerovaná na jeho dovolenkovú adresu.

Nesmieme zabudnúť na dve veci:

Po prvé - pošta sa presmerováva, teda sa na serveri neukladá, ani jej kópia!

Po druhé – keď sa Paľko z dovolenky vráti, súbor *.forward* zmažeme, aby mohol zase normálne prijímať poštu.

S poštou sa dajú robiť aj inakšie „psie kusy“. Môžeme ju kopírovať, filtrovať, testovať na vírusy, spam a podobne. Na to slúži ďalší program, ktorý dopĺňa poštový systém.

Nazýva sa ***procmail*** a o ňom si budeme rozprávať nabudúce.

Užívajme si zvyšok leta!

Miroslav Oravec