

Algebra visoka škola za

visoka škola za primijenjeno računarstvo

Sustavi za e-mail - postfix, IMAP, antispam, antivirus

www.racunarstvo.hr

E-mail

- e-mail sustavi postali su tijekom zadnjih desetak godina osnovno sredstvo poslovne i privatne komunikacije
- za slanje privatnih poruka, poslovnih dokumenata, može se koristiti i sa certifikatima, metodama enkripcije i sve, od jednostavnog dogovaranja sastanaka i korištenja imenika i kalendara do planiranja online sastanaka danas konvergira e-mailu kao osnovnom komunikacijskom sredstvu





- postfix
- sendmail (obsolete)
- integracija SSL-a
- IMAP
- antivirusna zaštita
- antispam zaštita





- najviše korišteni mail poslužitelj od izlaska RedHat Enterprise Linuxa 6 (kraj 2010.godine)
- ulogu primarnog mail servera za Linux preuzeo je ulogu od servisa sendmail, koji se preko 15 godina prije toga koristio na svim UNIX/Linux sustavima kao uobičajeni servis za slanje elektroničke pošte
- razlozi većinom sigurnosne i konfiguracijske prirode - sendmail je doista bio "švicarski sir" po pitanju sigurnosti (pun sigurnosnih rupa, propusta), a konfiguracija mu je kompleksna i nerazumljiva
- po pitanju ova dva parametra, postfix je kvantni pomak u pravom smjeru





- kao standalone poslužitelj po spajanju odmah može primati e-mail
- kao null-client samo za slanje e-maila
- lokalni postfix na lokalnoj, NAT mreži, za lokalne potrebe, tipična organizacija je sa jednim glavnim i više dodatnih mail servera koji mogu i slati i primati mail
- kao e-mail firewall/gateway npr.radi forwarding e-mail poruka za example.com domenu, ali ne i za nesto.example.com poddomenu.



Primjer

 instalacija postfixa kao standalone poslužitelja





- editiranje /etc/postfix/main.cf ili kroz postconf komandu
- myorigin konfiguracija imena domene sa koje će izgledati da je e-mail poruka primljena;
- myhostname podešavanje punog mrežnog imena našeg servera, za slučaj da to nije napravljeno na razini sustava;
- relayhost preko kojeg mail poslužitelja šaljemo sav odlazni mail;
- inet_interfaces podešavanje sučelja preko kojih postfix radi (all, \$myhostname, localhost, ...)
- mydestination lista odredišnih domena za koje će se poslužitelj smatrati autoritativnim;
- relay_domains za restrikciju destinacija za koje ćemo raditi mail relaying,
- mynetworks lista trusted SMTP klijenata kojima je dopušten mail relaying,
- mynetworks_style (class, subnet, host, ...) da li mynetworks parametar koristimo radi jednog poslužitelja, klase adresa ili podmreže;





- prije su se koristili POP2/POP3 protokoli (portovi 109 i 110), da bi se kasnije (upravo zbog slanja korisničkih imena i lozinki tekstualno) razvili drugi, sigurniji protokoli koji koriste enkripciju (*IMAP over* SSL na portu 993, POP3 over SSL/TLS na portu 995)
- u većini Linux distribucija za podršku oba protokola koristi se paket dovecot

[root@OOS2 ~]# yum -y install dovecot*

 otkomentirati jednu liniju u u konfiguracijskoj datoteci /etc/dovecot/dovecot.conf

protocols = imap pop3 lmtp

[root@OOS2 ~]# service dovecot start; chkconfig dovecot on; telnet localhost 993





- spamassasin alat za eliminaciju spam mailova
- jednostavna konfiguracija:

[root@OOS2 ~]# yum -y install spamass*
[root@OOS2 ~]# groupadd spamfilter; useradd -g spamfilter -s /bin/false -d /usr/local/spamfilter spamfilter; chown spamfilter:spamfilter /usr/local/spamassassin

 potrebno je napraviti izmjenu konfiguracijske datoteke /etc/mail/spamassassin/local.cf, u koju treba dodati jednu konfiguracijsku liniju:

required_score 5.0

izmjena datoteke /etc/sysconfig/spamassassin.



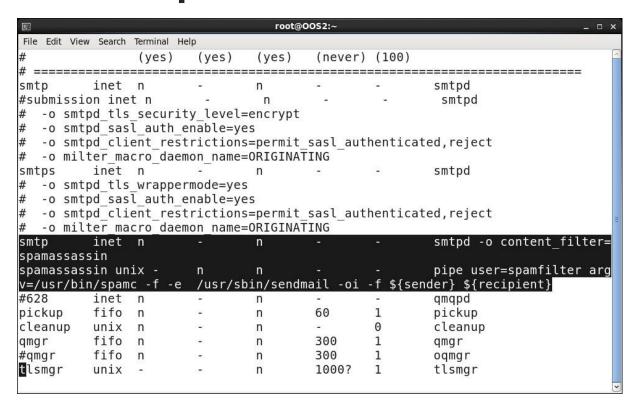
Spamassasin, II

 nakon toga je potrebno pokrenuti servis:

[root@OOS2 ~]# service spamassassin start; chkconfig spamassassin on



Spamassasin, III



 zadnji korak - konfiguracija spamassasina kao filter za postfix, potrebno je modificirati konfiguracijsku datoteku /etc/postfix/master.cf kao u navedenom primjeru i restartati postfix:

[root@OOS2 ~]# service postfix restart



Slijedeći koraci...

- konfiguracija spam filtera korištenjem regularnih izraza
- odabir blacklist servera za update spamassasin filtera
- instalacija ClamAV-a za antivirusnu provjeru maila (procedura opisana u priručniku)

