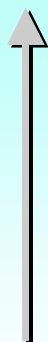


Dodatno konfiguriranje mrežnog poslužitelja

priređio Dražen Kačar
svibnja 2000.

(c) 1999-2000 CARNET & SRCE. Sva prava pridržana.
<http://sistemac.carnet.hr/ots/copyright.html>



- Reinstalacija mrežnog poslužitelja
- Dodatno konfiguriranje mrežnog poslužitelja
- Održavanje mrežnog poslužitelja
- Održavanje mreže
- Instalacija i konfiguracija mrežnog poslužitelja

Ciljevi tečaja

- Osposobiti se za dodatno konfiguriranje operativnog sustava
- Osposobiti se za temeljno administriranje osnovnih servisa



Potrebno predznanje

- Unix s korisničke točke gledišta
- Osnove konfiguriranja OS-a
- Instalacija poslužitelja
- Održavanje poslužitelja



Što nećete naučiti na tečaju

- Raditi s korisničkim aplikacijama
- Programirati
- Sigurnosne implikacije
- Zašto je Unix bolji od konkurencije



Sadržaj

- | | |
|--|--------|
| 1. Konfiguriranje korisničkih parametara | 35 min |
| 1.1. Korisnička okolina | |
| 1.2. Konfiguriranje quota | |
| 2. Konfiguriranje parametara sustava | 35 min |
| 2.1. Podizanje sustava | |
| 2.2. Konfiguriranje dozvola pristupa | |



Sadržaj (2)

3. Konfiguriranje programske potpore	170 min
3.1. Logovi sustava	
3.2. Konfiguriranje informacijskih servisa	
3.2.1. Mail poslužitelj	
Pauza	15 min
3.2.2. Web poslužitelj	
3.2.3. Anonimni FTP poslužitelj	
3.2.4. Ostali servisi	
Pauza	15 min
Vježbe	90 min

Inicijalizacija servisa

- Većina servisa na računalu mora imati konfiguracijske datoteke iz kojih će pročitati početne postavke za rad
- Kompleksne datoteke tog tipa se obično nalaze u direktoriju `/etc/` i imaju nazive izvedene iz imena programa, npr. `inetd.conf`, `nscd.conf` itd.
- Jednostavne konfiguracijske datoteke su obično smještene u datoteke koje se nalaze u direktoriju `/etc/default`. To ne znači da su manje važne.

`/etc/default`

- Bitne su nam: `login`, `passwd` i `su`.
- `/etc/default/login` definira osnovne parametre prilikom prijavljivanja na sistem preko tekstualnog sučelja.
- `/etc/default/passwd` definira minimalnu duljinu zaporke i vrijeme njenog trajanja
- `/etc/default/su` definira osnovne parametre korisničke okoline nakon izvođenja naredbe `su`.

/etc/default/login

- `CONSOLE=/dev/console` — root se može prijaviti samo s konzole
- `PASSREQ=YES` — svaki korisnik mora imati zaporku
- `PATH` — definira stazu za nalaženje izvršnih programa za obične korisnike

```
PATH=/usr/bin:/usr/sbin:/usr/ccs/bin:  
/usr/proc/bin:/usr/dt/bin:/usr/openwi  
n/bin:/usr/openwin/demo:/opt/SUNWspro  
/bin:/usr/local/bin:/usr/local/sbin
```

/etc/default/login (2)

- `UMASK=022` — maska dozvola za kreiranje datoteka
- `SYSLOG=YES` — sistem bilježi podatke o pokušaju prijavljivanja administratora
- `SUPATH` — definira stazu za nalaženje programa za administratora sustava

```
SUPATH=/sbin:/usr/sbin:/usr/bin:/usr/c  
cs/bin:/usr/proc/bin:/usr/dt/bin:/usr/  
openwin/bin:/usr/openwin/demo:/opt/SUN  
Wspro/bin:/usr/local/sbin:/usr/local/b  
in
```

/etc/default/passwd

- `MAXWEEKS` — najdulji period valjanosti zaporke.
- `MINWEEKS` — najkraći period koji mora proći da bi se zaporka mogla promijeniti.
- `WARNWEEKS` — period u kojem će biti ispisivana upozorenja o istjecanju zaporke.
- `PASSLENGTH` — najmanja duljina zaporke.

/etc/default/su

- SLOG=/var/adm/sulog — bilježenje su naredbe
- PATH — definira stazu za nalaženje izvršnih programa za obične korisnike
- SUPATH — definira stazu za nalaženje izvršnih programa za administratora
- SYSLOG=YES — bilježimo i preko sysloga

Ulaz u sistem preko X sučelja

- Ulazimo preko dtlogin servisa
- Ne koristi se /etc/default/login
- dtlogin ima svoje konfiguracijske datoteke — najprije se traže u /etc/dt/config direktoriju, a zatim u /usr/dt/config
- Nikad ne mijenjamo datoteke u /usr/dt stablu direktorija
- Datoteku koju želimo promijeniti najprije kopiramo na ekvivalentno mjesto u /etc/dt stablu i zatim mijenjamo tu kopiju

Xconfig

- mkdir -p /etc/dt/config
- cp /usr/dt/config/Xconfig /etc/dt/config/Xconfig
- Unesemo stazu pod Dtlogin*userPath resurs

```
Dtlogin*userPath: /usr/bin:/usr/sbin:  
/usr/ccs/bin:/usr/proc/bin:/usr/dt/bin:  
/usr/openwin/bin:/usr/openwin/demo:/opt  
/SUNWspro/bin:/usr/local/bin
```

Terminfo

- Ponekad je potrebno dodati opis novog tipa terminala
- Baza poznatih terminala se nalazi u `/usr/share/lib/terminfo` stablu direktorija
- Binarni format zbog brzine rada
- Dekompajliranje, ispisivanje razlika i slične funkcije radi naredba `infocmp`
- Kompajliranje u binarni format radi naredba `tic`

Quota

- Prostor na disku je resurs koji dijele svi korisnici
- Za pojedinog korisnika možemo ograničiti prostor koji zauzimaju njegove datoteke na pojedinoj particiji, kao i broj inode-ova (što je približno jednako broju datoteka)
- Postoje `soft` i `hard` limiti
- Ako imamo dovoljno diskovnog prostora i "pristojne korisnike", nema potrebe za uvođenjem quota

Postavljanje quote

- Svaka particija na kojoj ćemo uvesti `quotu` mora imati opciju `rq` u `/etc/vfstab` datoteci
- Na svakoj particiji mora postojati datoteka `quotas` u koju će se `quote` zapisivati
- Primjer retka iz `/etc/vfstab`:

```
/dev/dsk/c0t0d0s7 /dev/rdisk/c0t0d0s7  
/home ufs 2 yes logging,rq
```

Postavljanje quote (2)

- `touch /home/quotas` — kreira potrebnu datoteku
- `chmod 600 /home/quotas`
- `edquota` — postavlja quotu za jednog korisnika

```
edquota quotuser
```

```
fs /home blocks (soft = 3000, hard =  
5000) inodes (soft = 0, hard = 0)
```



Postavljanje quote (3)

- Za druge korisnike quotu postavljamo tako da kopiramo postavke od *proto-korisnika*
- `edquota -p quotuser dobrisa pero`
- Posao možemo automatizirati pomoću skripti
- Prije uključivanja quota moramo provjeriti konzistentnost datotečnog sustava (eng. file system)
- `quotacheck filesystem`
- `quotaon filesystem` — uključuje quotu na zadanim datotečnim sustavima

Provjeravanje i isključivanje quote

- `quota [-v] username` — ispisuje podatke o korisniku
- `repquota [-v] filesystem` — ispisuje podatke o datotečnom sustavu
- `quotaoff filesystem` — isključuje quote na zadanim datotečnim sustavima
- `edquota -t username` — promjena vremenskog ograničenja

Podizanje sustava

- Sustav prolazi kroz nekoliko faza (run level) prije nego što postane upotrebljiv za korisnike
- Ponekad ga je namjerno potrebno dovesti u određeno stanje zbog administrativnih razloga
- Koristimo naredbu `init`

Run levels

Run Level	Opis
0	power down (isključen)
1 s S	single user (jednokorisnički)
2	multiuser (višekorisnički)
3	multiuser (NFS export)
4	ne koristi se
5	power down
6	reboot

rc skripte

- Svaka faza ima svoje skripte za inicijalizaciju
- `rc` dolazi od `run control`
- Nalaze se u direktorijima `/etc/rc1.d`, `/etc/rc2.d`, `/etc/rc3.d` itd.
- Imena koja počinju sa `S` (start) označavaju skripte koje pokreću servise
- Imena koja počinju sa `K` (kill) označavaju skripte koje zaustavljaju servise
- Sistem sortira imena skripti (po ASCII rasporedu) i izvršava ih tim redoslijedom

rc skripte (2)

- Skripte iz `rc` direktorija pokreću odgovarajuće skripte koje se nalaze u `/sbin` direktoriju (`/sbin/rc0`, `/sbin/rc1`, `/sbin/rc2`, itd.)
- `/etc/init.d` direktorij sadrži linkove na skripte u `/etc/rc?.d` direktorijima s imenima koja je lakše zapamtiti
- Ista skripta se nalazi u nekoliko direktorija, pa bi editiranje bilo teško kad bi se radilo o nezavisnim datotekama

/etc/system

- Shared memory
`set shmsys:shminfo_shmmax = 0x2000000`
`set shmsys:shminfo_shmmni = 0x1000`
`set shmsys:shminfo_shmseg = 0x100`
- Noexec stack (samo SPARC)
`set noexec_user_stack = 1`
`set noexec_user_stack_log = 1`
- Dozvola pristupa NFS poslužitelju
`set nfssrv_nfs_portmon = 1`

/etc/system (2)

- Maksimalni broj procesa po korisniku
`set maxuprc = 64`
- Priority paging
`set priority_paging = 1`
- Broj pseudoterminala (podrazumijeva se 64)
`set pt_cnt = 1024`
- DNLC i inode cache ($\text{maxuser} * 17 + 90$)
`set ncsiz = 32000`
`set ufs_ninode = 32000`

identd

- RFC 1413
- Pruža podatak vanjskom poslužitelju o lokalnom korisniku koji se spaja na servis na vanjskom poslužitelju
- Vanjski poslužitelj ne može računati na apsolutnu pouzdanost podataka
- Dovoljno dobro za bilježenje i kasniju obradu

TCP wrapper

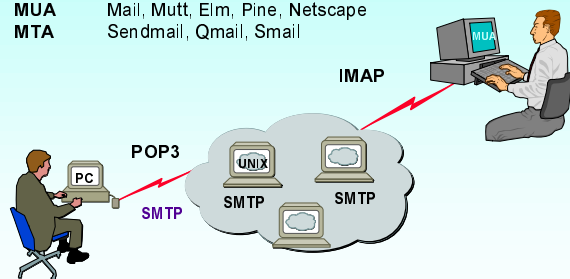
- Samo za TCP servise
- Omogućava bilježenje korisnika s vanjskih poslužitelja preko ident protokola
- Omogućava konfiguriranje dozvola pristupa prema IP adresi klijenata
- Uključuje se u `/etc/inetd.conf` za servise koje opslužuje `inetd` poslužitelj.
- Konfiguracijske datoteke:
`/etc/hosts.allow`
`/etc/hosts.deny`

syslogd

- Bilježi logove za razne servise
- Konfiguracijska datoteka: `/etc/syslog.conf`
- Svaka linija ima oblik:
`facility.level [; facility.level] action`
- Facility može biti: `user, kern, mail, daemon, auth, lpr, news, uucp, cron, local0-7` ili `*`
- Nivo može biti: `emerg, alert, crit, err, warning, info, debug` ili `none`
- Rotacija logova preko `crona`
(`/usr/lib/newsyslog`)

Model sustava el. pošte

MUA Mail, Mutt, Elm, Pine, Netscape
MTA Sendmail, Qmail, Smail



E-mail

Sastoji se od tri dijela:

- Omotnica (eng. envelope)
- Zaglavlja (eng. headers)
- Tijelo (eng. body)

```
svarozic> mailx -tnv
From: dave@svarozic.srce.hr
To: dave@srce.hr
Subject: test
```

burek sa sirom

Osnovne SMTP naredbe

- HELO (EHLO za prošireni protokol) — identificira klijenta
- MAIL — identificira pošiljaoca
- RCPT — identificira primaoca (može ih biti više)
- DATA — slijedi tijelo poruke
- QUIT — završava razmjenu pošte
- RSET — prekida transakciju; oba kraja odbacuju podatke
- VRFY — klijent zahtijeva ovjeru primatelja

sendmail

- MTA — Mail Transfer Agent, prenosi poštu između poslužitelja
- Za dostavljanje u korisničke pretince koristi eksterni program, podrazumijeva se `/usr/lib/mail.local`
- SMTP — Simple Mail Transfer Protocol (RFC 821)
- Postoje razne ekstenzije
- Dodijeljeni SMTP port je 25
- Konfiguracijske datoteke su u direktoriju `/etc/mail`

sendmail.cf

- Gradi se pomoću `m4` pretprocesora
 - Predlošci (eng. templates) su u `/usr/lib/sendmail.cf` direktoriju
 - Predlošci se spajaju pomoću `.mc` datoteke
- ```
m4 ${CFDIR}/m4/cf.m4 config.mc >sendmail.cf
```
- CARNet paket donosi dvije `.mc` datoteke: `sendmail.mc` i `sendmail-nomx.mc`
  - Manje promjene možemo raditi direktno u `sendmail.cf` datoteci

---

---

---

---

---

---

---

---

## sendmail.cf – direktive

- Maksimalna veličina poruke
  - `MaxMessageSize=1000000`
- Maksimalni broj aktivnih poslužitelja
  - `MaxDaemonChildren=15`
- Relaying
  - `FR-o /etc/mail/relay-domains`
- Alias datoteka
  - `AliasFile=/etc/mail/aliases`
- Spool direktorij za poštu
  - `QueueDirectory=/var/spool/mqueue`

---

---

---

---

---

---

---

---

## sendmail opcije

- `-q` zadaje frekvenciju čišćenja queue direktorija  
`/usr/lib/sendmail -q1h — svaki sat`
- `-bi` inicijalizira bazu aliasa (isto što i `newaliases`)
- `-bd` pokreni se kao daemon i čekaj na dolaznu poštu
- Skripta za automatsko pokretanje je  
`/etc/rc2.d/S88sendmail`
- Za ručno zaustavljanje i pokretanje koristiti  
`/etc/init.d/sendmail [stop | start]`

---

---

---

---

---

---

---

---

## Mail aliasi

- Alias je alternativno ime za jednog ili više korisnika  
planeri: `dobrisa`, `miro`, [tvujec@carnet.hr](mailto:tvujec@carnet.hr)
- Upisuju se u datoteku `/etc/mail/aliases`, a u oblik koji je potreban sendmailu se dovode naredbom `newaliases`
- Alias oblika `Ime.Prezime@host` su podrazumno podržani (eng. default)
- Opcija se ukida direktivom  
`MatchGECOS=false`

---

---

---

---

---

---

---

---

## ...@domena

- Ako MUA (Mail User Agent) sendmailu ne dostavi adresu korisnika koji šalje poštu, sendmail će ju sam dopisati
- Oblik je: [korisnik@host.domena](mailto:korisnik@host.domena)
- Da bi oblik bio samo [korisnik@domena](mailto:korisnik@domena), potrebna je direktiva:  
`DA$w`

---

---

---

---

---

---

---

---

## Pauza 15 min.



---

---

---

---

---

---

---

---

## HTTP

- HyperText Transfer Protokol — služi za razmjenu podataka preko World Wide Web-a
- Inicijalno vrlo jednostavan, kasnije više puta proširivan
- Poslužitelj sluša na portu (obično 80)
- Klijent se spoji i pošalje zahtjev
- Poslužitelj pošalje odgovor (ili traženi objekt ili poruku o grešci)
- Veza se prekida

---

---

---

---

---

---

---

---

## HTTP zahtjev

```
> telnet sistemac.carnet.hr 80
GET / HTTP/1.0
Accept: */*
Accept-Language: hr, en; q=0.5
User-Agent: telnet

<- prazna linija
```

---

---

---

---

---

---

---

---

## HTTP odgovor

```
HTTP/1.1 200 OK
Date: Tue, 22 Feb 2000 14:42:41 GMT
Server: Apache/1.3.9 (Unix) PHP/4.0B2
Last-Modified: Tue, 16 Nov 1999 12:24:17 GMT
ETag: "68591-1af1-38314cf1"
Accept-Ranges: bytes
Content-Length: 6897
Connection: close
Content-Type: text/html;charset=iso-8859-2
```

<HTML>

---

---

---

---

---

---

---

---

---

---

## HTTP metode

| Metoda | Klijent          | Poslužitelj                                                         |
|--------|------------------|---------------------------------------------------------------------|
| GET    | zahtjev          | šalje zaglavlje i podatke                                           |
| HEAD   | zahtjev          | šalje samo zaglavlje                                                |
| POST   | zahtjev i podaci | obrađuje podatke i šalje odgovor (zaglavlje i podaci)               |
| PUT    | zahtjev i podaci | kreira novi dokument i šalje odgovor (zaglavlje, podaci nisu nužni) |

---

---

---

---

---

---

---

---

---

---

## Apache

- Instalira se u `/usr/local/apache`
- Stablo direktorija:
  - `bin` sam poslužitelj i pomoćni programi
  - `libexec` poslužiteljski moduli
  - `conf` konfiguracijske datoteke
  - `man` man stranice
  - `logs` logovi
  - `icons` ikone
  - `proxy` proxy cache
  - `include` headeri za dodavanje modula

---

---

---

---

---

---

---

---

---

---

## Konfiguracija

- U prijašnjim verzijama su konfiguracijske direktive bile raspoređene u tri datoteke: `httpd.conf`, `access.conf` (dozvole pristupa) i `srm.conf` (name space, servisiranje zahtjeva i formatiranje odgovora)
- Sada su sve u `httpd.conf`
- I dalje se može koristiti stari raspored – konfiguracijske direktive mogu biti u bilo kojoj datoteci
- Linije koje počinju znakom `#` su komentari, a sve ostale su konfiguracijske direktive

---

---

---

---

---

---

---

---

## MIME tipovi

- Konfiguracijska datoteka koja opisuje koja ekstenzija odgovara pojedinom tipu dokumenta
- Obično se zove `mime.types`
- Ne sadrži direktive za konfiguraciju poslužitelja
- Primjer:

```
text/html html htm
image/gif gif
image/jpeg jpeg jpg
application/msword doc
```

---

---

---

---

---

---

---

---

## Sintaksa konfiguracijskih datoteka

- Osnovni oblik:  
Direktiva `arg1 arg2 ...`
- Kontekst:  
`poslužitelj` — `httpd.conf`, `srm.conf`,  
`access.conf`  
`virtualni poslužitelj` — unutar `<VirtualHost>` grupe  
`direktorij` — unutar `<Directory>`, `<Location>` ili  
`<Files>` grupe  
`.htaccess` — unutar `.htaccess` datoteke u pojedinom  
direktoriju

---

---

---

---

---

---

---

---



## Osnovne direktive

- Bazično stablo direktorija s datotekama poslužitelja  
ServerRoot "/usr/local/apache"
- Vrijeme nakon kojeg poslužitelj prekida neaktivnu vezu

Timeout 300

- Broj aktivnih procesa

MinSpareServers 5

MaxSpareServers 10

StartServers 5

MaxClients 150



---

---

---

---

---

---

---

---

---

---

## Osnovne direktive (2)

- Port na kojem poslužitelj prima zahtjeve

Port 80

- Korisnik i grupa poslužitelja

User nobody

Group nobody

- Adresa administratora (automatska instalacija ju ne može pogoditi)

ServerAdmin dobrisa@srce.hr



---

---

---

---

---

---

---

---

---

---

## Osnovne direktive (3)

- Tip poslužitelja (samostalan ili pod nadzorom inetd-a)

ServerType standalone

- Vrh stabla direktorija u kojem se nalaze konfiguracijske datoteke i logovi

ServerRoot /usr/local/apache

- PID glavnog Apache procesa

PidFile var/run/httpd.pid



---

---

---

---

---

---

---

---

---

---

## Osnovne direktive (4)

- Vrh stabla direktorija s dokumentima  
`DocumentRoot "/home/httpd/htdocs"`
- Vrh stabla dokumenata kod korisnika  
`UserDir public_html`
- Imena dokumenata koji se pokušavaju pronaći kad klijent zatraži direktorij  
`DirectoryIndex index.asis index.html  
index.htm index.shtml index.cgi`
- Ime datoteke s konfiguracijom za pojedini direktorij  
`AccessFileName .htaccess`

## Osnovne direktive (5)

- Datoteka s opisom MIME tipova  
`TypesConfig conf/mime.types`
- Tip dokumenta za koji nema MIME tipa u gornjoj datoteci  
`DefaultType text/plain`
- Logovi  
`ErrorLog logs/error_log  
LogFormat "%h %l %u %t \"%r\" %>s %b"  
common  
CustomLog logs/access_log common`

## Aliasing

- Kod statičkih dokumenata URL-ovi pokazuju na direktorije i datoteke u datotečnom sustavu
- Ako želimo, to možemo promijeniti
- Alias direktiva mapira URL na proizvoljni direktorij  
`Alias /icons/ "/usr/local/apache/icons"`
- ScriptAlias radi isto što i Alias. Uz to sve datoteke u direktoriju postaju CGI programi  
`ScriptAlias /cgi-bin/ /home/httpd/cgi-bin`

## Upravljanje konfiguracijom

- Za stablo direktorija  
`<Directory> ... </Directory>`
- Za grupe direktorija  
`<DirectoryMatch regex> ...  
</DirectoryMatch>`
- Za pojedine datoteke  
`<Files file1 file2 ...> ... </Files>`
- Za grupe datoteka  
`<FilesMatch regex> ... </FilesMatch>`



---

---

---

---

---

---

---

---

## Upravljanje konfiguracijom (2)

- Za URL-ove  
`<Location URL> ... </Location>`  
`<LocationMatch regex> ...  
</LocationMatch>`
- Prema HTTP metodi  
`<Limit method method ...> ... </Limit>`  
`<LimitExcept method method ...> ...  
</LimitExcept>`

---

---

---

---

---

---

---

---

## Koncept zaštite

- Na nivou poslužitelja, direktorija, URL-a ili datoteke
- Dva načina: putem lozinki (username/password) ili provjerom domene, odnosno IP adrese
- Za lozinke u teoriji možemo birati enkripcijski algoritam. U praksi je nužno da i klijent i poslužitelj podržavaju isti algoritam, što bitno smanjuje skup mogućnosti
- Jedini koji svi podržavaju je `AuthType Basic`, koji uopće ne kriptira lozinke

---

---

---

---

---

---

---

---

## Upravljanje pristupom

```
<Directory />
 Options FollowSymlinks
 AllowOverride None
</Directory>
<Directory "/home/httpd/htdocs">
 Options Indexes FollowSymlinks
 AllowOverride None
 Order allow,deny
 Allow from all
</Directory>
```

---

---

---

---

---

---

---

---

## Zaštita pristupa (host-based)

```
<Directory protected>
 order deny, allow
 deny from all
 allow from .srce.hr
</Directory>
```

---

---

---

---

---

---

---

---

## Zaštita pristupa (lozinke)

- Za pojedine korisnike  
htpasswd -c /home/httpd/admin/pass mujo
- Izgleda kao /etc/passwd
- Za grupe korisnika: kreirati sve korisnike i njihove lozinke, a zatim konfigurirati grupe u posebnoj datoteci, npr. /home/httpd/admin/grupa  
admini: mujo haso dobrisa
- Sve potrebne grupe se mogu konfigurirati u jednoj datoteci



---

---

---

---

---

---

---

---

## Lozinke (2)

Kontrolna datoteka sadrži:

```
<Directory protected>
 AuthUserFile /home/httpd/admin/pass
 AuthUserGroup /home/httpd/admin/group
 AuthName Nema bureka bez passworda
 AuthType Basic
 <Limit GET>
 require user dobrisa
 ili
 require group admini
 </Limit>
</Directory>
```

---

---

---

---

---

---

---

---

---

---

## Virtualni poslužitelji

- Osnovna ideja: jedan poslužitelj na jednoj IP adresi "glumi" nekoliko poslužitelja s različitim imenima u DNS-u
- U suprotnom bismo vrlo brzo ostali bez raspoloživih IP adresa
- Nije moguće preko HTTP/1.0 protokola
- HTTP/1.1 donosi proširenje koje se može koristiti i u HTTP/1.0 protokolu — Host header
- Danas svi klijenti i poslužitelji znaju raditi s njim



---

---

---

---

---

---

---

---

---

---

## Virtualni poslužitelji (2)

```
Port 80
ServerName mujo.srce.hr
NameVirtualHost 161.53.2.138
<VirtualHost 161.53.2.138>
 ServerName mujo.srce.hr
 DocumentRoot /home/httpd/mujo
 ...
</VirtualHost>
<VirtualHost 161.53.2.138>
 ServerName haso.srce.hr
 DocumentRoot /home/httpd/haso
 ...
</VirtualHost>
```

---

---

---

---

---

---

---

---

---

---

## Anonimni FTP poslužitelj

- Poseban datotečni sustav
- Poseban korisnik `ftp`
- Ispravno konfigurirana datoteka `/etc/shells`
- Poslužitelj radi `chroot()` u osnovni direktorij
- Datoteke `/etc/passwd` i `/etc/group` ne smiju biti iste kao i sistemske
- Trebaju sadržavati dovoljno podataka za ispravan rad naredbe `ls`, ali nimalo više

---

---

---

---

---

---

---

---

## Konfiguracijske datoteke

- `ftphosts` — dozvoljava ili zabranjuje pristup određenim korisnicima s raznih strojeva
- `ftpconversions` — omogućava automatsko prepakiranje formata (npr. kompresiju)
- `ftpaccess` — glavna konfiguracijska datoteka, njeno procesiranje se uključuje navođenjem opcije `-a` kod pokretanja poslužitelja

---

---

---

---

---

---

---

---

## FTP logovi

- Osnovni podaci se zapisuju preko `syslogd-a`
- Podrobni podaci o prenosu datoteka se zapisuju u `xferlog` (ako je to zapisivanje omogućeno u datoteci `ftpaccess`)
- Tabelirana statistika pristupa se iz `xferlog-a` može dobiti programom `xferstats`

---

---

---

---

---

---

---

---

## Ostali servisi

- Instalacija OS-a donosi još neke servise koji su nam manje zanimljivi (ne treba ih dodatno konfigurirati ili tipičan poslužitelj ne treba tu funkcionalnost)
- U `inetd.conf`-u možemo naći: `tftpd`, `finger`, `rusersd`, `rwalld`, `rstatd`, `rpc.cmsd`, `dtspcd`, `lpd` i `kerbd`.
- Sve osim `finger`a je poželjno isključiti iz sigurnosnih razloga
- Samostalni servisi: `automountd`, `cron`, `nscd`, `nfsd`, `statd`, `lockd`, `mountd`, `powerd`, `speckeyd` itd.

---

---

---

---

---

---

---

---

## Posebni servisi

- Ako imamo posebne želje, možemo instalirati i dodatne servise (neki ne dolaze sa samim OS-om)
- Imenički servisi: NIS, NIS+, **whois++**, **LDAP**
- Mailing list poslužitelji: **majordomo**, **listproc**, **pejdomo** itd.
- Usenet poslužitelj: **inn**
- Web proxy: Apache modul ili **Squid**

---

---

---

---

---

---

---

---

## Pauza 15 min.



---

---

---

---

---

---

---

---

## Vježba 1: quota

- Kreirati tri grupe i deset korisnika raspoređenih u te grupe. Korisnički direktoriji trebaju biti na `/home` particiji.
- Za svaku grupu odabrati quote (u rasponu od 2 MB do 20 MB) i postaviti jednake quote korisnicima koji su u istoj grupi
- Svim korisnicima postaviti `soft` time limit na šest dana, a `hard` na sedam (samo za prostorno zauzeće diska, ne i za broj datoteka).

---

---

---

---

---

---

---

---

## Vježba 2: logovi

- Identificirati sve CARNetove pakete koji donose poslužitelje čiji se logovi bilježe izvan `syslog` sustava.
- Konfigurirati `syslogd` tako da bilježi sve poruke, s tim da svaki `facility` ide u posebnu datoteku u `/var/log` direktoriju.

---

---

---

---

---

---

---

---

## Logovi (2)

- Napraviti `cron` skriptu koja jednom tjedno sve logove iz `/var/log` prebacuje u `/var/oldlogs`. Želimo čuvati logove za barem mjesec dana.
- Ukoliko neki od poslužitelja koji ne bilježe logove preko `syslog` radi rotaciju logova s drukčijim periodom, postaviti njihovu rotaciju na jednotjedni period. Stari logovi trebaju biti u posebnom direktoriju.
- Sve stare logove nakon rotacije komprimirati.
- Automatizirati brisanje logova starijih od mjesec dana.

---

---

---

---

---

---

---

---



### Vježba 3: mail

- Kreirati jednog korisnika i napraviti mail aliase za adrese `www`, `webmaster` i `ftpadmin` tako da pošta upućena na te adrese dolazi njemu.
- CARNetov `sendmail` paket se nakon instalacije konfigurira tako da prima poštu upućenu na adresu `korisnik@domena`. Takvu konfiguraciju obično imamo samo na jednom stroju u domeni. Kojem?
- Isključiti lokalni DNS poslužitelj i konfigurirati `sendmail` tako da poštu upućenu na `user@domena` ne pokušava isporučiti lokalnim korisnicima.

---

---

---

---

---

---

---

---

---

---

### Vježba 4: virtualni web

- Napraviti dvije različite HTML stranice i staviti ih u dva različita direktorija.
- Izabrati imena za dva virtualna web poslužitelja
- Konfigurirati dva virtualna web poslužitelja tako da im osnovne stranice budu one koje su prethodno napravljene, da imaju odvojene error i access logove, te različite mail adrese administratora poslužitelja (kreirati dva korisnike za ovu namjenu).

---

---

---

---

---

---

---

---

---

---

### Vježba 5: zaštita web stranica

- U stablu dokumenata WWW poslužitelja kreirati dva direktorija s barem jednom HTML stranicom.
- Za prvi direktorij zabraniti pristup svima osim lokalnim korisnicima.
- Za drugi direktorij kreirati dva korisnika, izabrati im zaporke i dozvoliti pristup klijentima koji znaju ispravnu username/password kombinaciju.

---

---

---

---

---

---

---

---

---

---

## Literatura

- System Administration Guide, Volume I
- System Administration Guide, Volume II

<http://docs.sun.com>  
<http://bagan.srce.hr:8888>

- Man stranice
- Apache dokumentacija  
<http://localhost/manual/>



---

---

---

---

---

---

---

---

## Što dalje?

- Proučiti dokumentaciju
- Proučiti dokumentaciju
- Proučiti dokumentaciju
- Bez panike



---

---

---

---

---

---

---

---