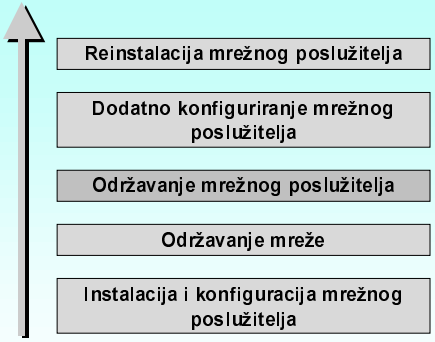
Održavanje mrežnog poslužitelja

priredio Damir Delija
veljače 2000.



Ciljevi

- upoznati se s dnevnom administracijom Solaris računala - naš najčešći mrežni poslužitelj
- osposobiti se za svakodnevni samostalni rad kao administrator

Potrebno predznanje

- Rad sa Solaris 2.x OS
- Poznavanje shell-a (sh, ksh)
- Poznavanje funkcioniranja UNIX-a
- Poznavanje grafičkih alata

Sadržaj

Dnevna administracija sustava	30 min
Politika nadzora sustava	30 min
Rutinsko praćenje sustava	15 min
Pregledavanje logova	30 min
Pauza	15 min
Sigurnost	30 min
Praćenje i rotacija logova na sustavu	20 min
Dnevna administracija korisnika	15 min
Automatsko izvođenje	20 min
Modificiranje rc skripti	20 min
Papirna dokumentacija	20 min
Backup sustava	20 min
Pauza	15 min
Vježbe	60 min

Što nećete naučiti na tečaju

- Puno toga!
- Nećete dobiti gotove ‘recepte’ za sve vaše probleme

Područja

- Solaris 2.x OS
- Administracija Solaris računala
- Tips & Tricks

Dnevna administracija sustava

Cilj:

STROJ radi za mene, a ne ja za njega!

- Administracija korisnika i grupa
- Komunikacija s korisnicima sustava
- Automatsko izvođenje programa: cron,at,batch
- Svakodnevno praćenje sustava
- Pomoćni alati i njihova integracija u sustav

Politika nadzora sustava

- Rutinsko praćenje sustava je dio politike nadzora sustava
- Idealno da administrator na konzoli prati stanje i prema potrebi reagira
- Granice pojedinih parametara su ovisne o sustavu
  - load ne više od 2
  - memorija do 90% RAM-a zauzeto
  - swap do 80% zauzeto
  - greške
    - `iostat -E`
    - `iostat -e`

Praćenje parametara sustava (baselining)

- Potrebno je povremeno pratiti stanje sustava da bi se znalo njegovo ponašanje "**fingerprint, footprint**"
- Load sustava
- Status diskova
- Mail koji dolazi za root
- Logovi sustava
- Korisnici na sustavu
- Obavezna papirna dokumentacija (papirologija)
- Komanda `script` ...
- `sar utility, se toolkit`

Pošta (mail) za root

- Povremeno pregledavanje pošte
- Povremeno pregledavanje kazala za prijem pošte */var/mail*
- Povremeno pregledavanje logova za mail
- Pošta od sendmaila programa
- Pošta od cron-a (greške u cron skriptama)

Rutinsko praćenje sustava

Što i kako gledati:

posao	komande
koliko je dugo sistem aktivan	`uptime`
poruke koje sistem sam šalje administratoru	`elm, mail`
opterećenje	`top,uptime`
mrežna komunikacija	`netstat`
broj korisnika na sistemu	`w,who,ps`
broj programa na sistemu	`ps,top`
zauzeće memorije	`top,vmstat`
zauzeće diskova	`df, du`

Praćenje stanja diskova

- Prati se zauzeće diskova (postotak slobodnog prostora za inodes i za podatke)
  - `df`
  - `du`
  - `fuser`
- Prati se opterećenje diskova tj. promet
  - `iostat -x`
  - `nfstsat` (za mrežne diskove)
- Greške - *posebno hard errors*
  - `/var/messages`
  - `iostat -e, iostat -E`

Pregledavanje logova

- Solaris sustav putem posebnog procesa piše poruke u datoteke ili ih šalje preko mreže
- To su obične ASCII datoteke
- `syslog deamon` i `/etc/syslog.conf` konfiguracijska datoteka
- Kazalo s logovima
  - `/var/adm/`
  - `/var/log/`

Log datoteke podsjetnik

- `/var/adm`
  - `messages` poruke bootanja sustava
  - `sulog` poruke su komande
  - `wtmp` tko je radio na sustavu
  - `lastlog` komande koje su izvedene
- `/var/log`
  - `authlog` auth poruke
  - `syslog` opće poruka sysloga
  - `xferlog` prenos ftp-om
- `/var/cron`
  - `log` poruke cron-a

Kako pronaći log datoteku

- Pogledati man page
- Pronaći konfiguracijske datoteke i tamo pogledati ima li što o logovima
- Pogledati *readme* datoteke od programa
- Napraviti `ps -ef` i pogledati argumente komandne linije programa (tu se može vidjeti i konfiguracija)
- Napraviti `lsof, truss` i sl.
- Napraviti `strings` komandu na `/proc/prog` datoteci i vidjeti kamo program piše
- Tražiti po listama, web u i sl.

Praćenje i rotacija logova na sustavu

- Logovi u
  - `/var/adm`
  - `/var/log`
  - `/var/cron`
  - i drugdje ako imate servise (ftp, http, baza i sl.)
- Povremeno ili u slučaju potrebe mora se uspoređivati sadržaj logova sa stanjem sustava
  - `iostat -E` (greške na diskovima)
  - `/var/adm/messages` (dodatne poruke za dijagnostiku)

Rotacija logova

- Najbolje skripta iz crona koja ih rotira periodički (onda kad je na sustavu najmanje opterećenje)
- Osnovna način rotacije logova:

```
gzip -c logX>logX.gz && cp /dev/null logX
```

Postoji opasnost od nereferenciranih datoteka!

- `fuser` komanda da se vidi da li netko drži datoteku!
- `lsof` komanda korisna

Rotacija logova postojeći alati

- `/etc/cron.d/logcheker`
- `/usr/lib/newsyslog`
- Može se napraviti vlastita skripta koja to sve objedinjuje!

Sigurnosne datoteke

- To su ujedno kritična mjesta sigurnosti sustava
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/group`
- **Potrebno je stalno gledati da ne postoje "neautorizirane promjene", što je znak provale na sustav!**

Osnovna dnevna administracija korisnika

- Dodavanje korisnika
  `useradd`
- Brisanje korisnika (ne zaboraviti find!)
  `userdel`
- Zaključavanje korisnika
  `passwd`
- Promjena korisnika i njegovih atributa
  `usermod, passwd`

```
passwd -x 40 pero
passwd -n 30 stef
```

Dodatna administracija korisnika i grupa

- Poslovi
  - Forsiranje politike lozinki i sigurnosti
  - Periodičko dodavanje ili uklanjanje korisnika
  - Periodičko dodavanje ili uklanjanje grupa
- Ovisi o politici sustava i strukturi korisnika i grupa na sustavu
- Osnovno:

  grupa služi za dijeljenje zajedničkih resursa

Specijalna administracija korisnika i grupa

- Dodavanje/mijenjanje podataka o korisnicima i grupama, te zaključavanje sumnjivih korisnika
- koriste se komande za administriranje korisnika i grupa i provjeru konzistentnosti
- potrebno je imati odgovarajuću popratnu dokumentaciju
  - obrazac za dodavanje korisnika/grupe
- potrebno je imati log aktivnosti na sustavu
  - datoteka u koji se pišu sve relevantne aktivnosti, obično skrivena datoteka, čisti ASCII

VAŽNO JE BITI UREDAN I SISTEMATIČAN

Komunikacija s korisnicima sustava

- Kada se nešto desi nastoji se komunicirati s korisnikom PRIJE nego što ga se ukloni sa sustava
- Koristimo komande `write,talk ...`
- Sve ovisi o procjeni administratora, ako se čini da korisnik ugrožava sustav treba ga odmah uloniti

  ! **kill -9** !
- U slučaju rušenja sustava upozoriti unaprijed korisnike (`wall, rwall`)
- Prekide rada sustava treba najaviti unaprijed

Pauza
15 minuta

Osvrt na sigurnost

Sigurnost sustava osniva se na korisničkim računima i grupama (user, groups model)!

- datoteke u kojima su podaci,
  - u njih može pisati samo root,
  - datoteke s lozinkama može čitati samo root
- Administriranje korisnika se preporuča kroz alate zbog konzistentnosti datoteka

Opaske o sigurnosti

- Dio dnevnog nadzora sustava!
- Dogovorena politika sigurnosti koju treba slijediti
- Ako postoji sumnja na provalu (sigurnosni incident) potrebo je kontaktirati cert

  `ccert@carnet.hr`
- Što je sumnjivo - sve ono što nije uobičajeno!
- Poruke u logovima, promjena performanse, mrežni scanovi I sl.!

Reakcija na sigurnosne incidente (1)

Ako postoji sumnja na sigurnosni incident treba kontaktirati CCERT: ccert@carnet.hr

Potrebno je spremiti logove sustava s tragovima provale

- Ustanoviti opseg provale ili problema,
  - da li su provaljeni samo korisnički računi
  - da li je ugrožen root
  - da li stroj služi kao uporište za daljnje provale
- Ustanoviti tko je počinio provalu te, ako je moguće, odakle je došao

Reakcija na sigurnosne incidente (2)

- Najvažnije je mirno postupati, ne paničariti, sve akcije dokumentirati
- Šteta je već počinjena treba je minimizirati, a ne povećati
- Koristiti `script` utility, ako je moguće napraviti dump sustava

Automatsko izvođenje programa

- Solaris dozvoljava automatsko izvođenje programa i pozadinsko izvođenje programa

Osnova automatiziranja administracije!

`cron`	izvođenje u pravilnim razmacima
`at`	izvođenje jednom, u zadano vrijeme
`batch`	izvođenje kada je opterećenje malo

cron

- cron izvodi komande periodički, rezolucija crona do na 1 minutu
- crontab komanda
  - `crontab -l` izlistava sadržaj cron datoteke
  - `crontab -e` editira sadržaj cron datoteke

  Napomena: *treba postaviti env. varijablu* `VISUAL` *na editor koji se želi koristiti, crontab inače poziva ed*
- Format cron komande

```
M H D m d command
5 3 * * * /usr/local/bin/my_rotate.sh > /dev/null 2>&1
```

Odličan za automatizaciju administracije (brisanje i rad s logovima, brisanje /tmp i sl.)

at

- Pokretanje komande u točno zadanom trenutku samo jednom

```
at [vrijeme]
   komada
   <CRTL d>
```

- Zahtjevi na komade isti kao i za cron

batch

- Jednostavno izvođenje komandi kada je opterećenje sustava malo
- Nije pravi batch u smislu velikih poslovnih sustava, prekid posla je stalan, nema checkpointa i sl.
- Neke funkcije mogu biti emulirane preko sustava za štampanje (rijetko se koristi)

Skripta za automatsko pokretanje

- Skripta mora biti dobro napisana i bez grešaka, pošto se odvija sama *i možda kao root*
- ne smije imati `suid` ili `sgid` (Solaris to neće ni dozvoliti)
- Koristiti `sh` ili `ksh`, ***`ne csh`!***
- Pravila:

  ukradi, shvati, prilagodi, testiraj

Modificiranje rc.d/skripti

- To su sh skripte (bourne shell tradicionalno)
- `/etc/rcA.d/BCDEime`
  - A je radni nivo (runlevel)
  - KCDEime kill (stop) skripta CDE je broj
  - SCDEime start skripta
  - simbolički linkovi linkovi na `/sbin/init.d/ime`
- Upravljanje servisima na sustavu preko njih
- `init` i `shutdown` ih koriste
- Argumenti skripte:

  start, stop, restart

Isključivanje rc skripte (isključivanje servisa)

- Dva načina!
- Obrisati linkove iz `/etc/rcX.d` kazala
- Preimenovati
  - SXXime u sXXime
  - KXXime u kXXime
- Dodatno osiguranje
  - staviti kao prvu izvršnu komandu

```
exit 0
```

Pomoćni alati

- Postoji niz alata za pomoć u nadzoru sustava neki dolaze sa sustavom a neki su free
- Solaris 2.x
  - `Solstice Symon`
  - `sar`
- Free alati
  - `cops` nadzor rupa na sustavu
  - `tripwire` nadzor promjena sustava, više nije free
  - `se toolkit` (virtual adrian)
  - `satan, gabriel`

Praćenje sustava getunix

- Naši alati - `getunix` sustav za udaljeno praćenje ponašanja sustava
- Dobija se osjećaj za stanje sustava
- deamon koji ispisuje rezultate u html-u
- Instalira se automaski sa CARNetovim paketima

Patchiranje sustava

- Patch je zakrpa tj. ispravljanje greške ili dodavanje nove funkcionalnosti sustavu!
- Postoje patchevi
  - sigurnosni (treba biti jako oprezan)
  - ostali
- Svaki patch ima svoj jednistveni broj
- Postoje single, te jumbo (skupni) patchevi
- `patchinstall`, osnovna komanda dolazi u patch datoteci

Postupci patchiranja sustava

- Prvo provjeriti koji patch je potreban

Mi nemamo support, pa sve treba detaljno provjeriti!

- Provjeriti veličinu patcha, te slobodan prostor na disku
- patchevi se nalaze na ftp.carnet.hr ili na nekom drugom "košer" izvoru, ftp://ftp.carnet.hr/mirrors/sunsolve.sun.com/pub/patches/
- patch dolazi tar.Z formatu - cca 40% kompresije
- Preba ga otpakirati u posebano kazalo!
- Obavezno backupirati sustav!
- Instalirati patch po uputama!
- Pratiti ponašanje sustava nakon patcha!

Papirna dokumentacija što i kako pisati

- Preporuča se imati
  - log datoteka u koji se piše
  - papirni log s najvažnijim podacima (brodski dnevnik)
- Kod rada na sustavu `script utility` za važne stvari, log naših aktivnosti
- Zgodno je imati kakav alat za praćenje stvari, može i mailom (1 folder - 1 događaj), web wreq i sl.!
- Treba planirati unaprijed i računati barem u grubo trajanje zahvata, potrebne resurse i sl.!

Dnevni backup sustava

Cilj:

- Što je backup-a sustava i zašto je obavezan
- Kako ga sam napraviti
- Zbog malog broja tape unita - improvizacija!

Značenje backup-a

- backup je u osnovi jedna ili više kopija sustava
- backup može biti potpun ili djelomičan
- backup može biti mrežni ili lokalni
- Kakav god da je backup cilj mu je da se omogući restauriranje stanja sustava

- Osnovno:

  Backup ne smije zakazati kada je potreban

Postupci backup-a

- Cilj je: ***sačuvati integritet sustava***
- Podaci se spremaju na
  - trake
  - diskete (?)
  - mrežne diskove
  - rezervne particije
- Backup se radi redovito i u skladu s politikom sustava
- Backup se radi na nivou sustava datoteka (file systema) ili za važne datoteke

Strategije backup-a

- Postoje dva osnovna tipa backupa
  - full kompletna kopija sustava
  - inkrementalni samo promjene na sustavu
- Nakon svake instalacije sustava ili personalizacije sustava obavezan je *full backup*
- backup se radi kada je sustav neopterećen i preporuča se u single user modu (osim ako alat ne dozvoljava multi user mode backup)

Full backup

- Kompletna slika sustava, zauzima isto prostora koliko i sustav
- Radi se jednom mjesečno ili jednom tjedno, može i rjeđe

Inkrementalni backup

- To su samo one izmjene na sustavu datoteka od zadnjeg backup-a
- sistemske datoteke se rijetko mijenjaju, one obično ne ulaze u inkrementalni backup
- Stvari koje se lako instaliraju isto ne ulaze u inkrementalni backup

Komande backup i restore

- `ufsdump`
- `ufsrestore`
- `rdump` i `rrestore` - remote dump i restore
- `tar` - Tape Archive Program
- `cpio` - Copy Input Output
- Mrežni backup
  - `amanda`
  - `legato`

ufsdump komanda

- ufsdump komanda radi backup
  - `ufsdump` (SunOS 5.X)
- Postoje nivoi 0-9
  - 0 najviši nivo **FULL DUMP**
  - 9 najniži nivo **inkrementalni**
  - nivo x+1 će uzeti sve promjene nakon zadnjeg nivoa x

ufsrestore komanda

- `ufsrestore` komanda radi restore
- `ufsrestore -i` u interaktivnom modu, vraća podatke u kazalo u kom se nalazimo

tar

- Odličan za brze arhive i prijenos koda i programa
- Obično kombinacija tar + gz => tar.gz, tgz

- `tar cvf` kreiraj arhivu
- `tar tvf` izlistaj arhivu
- `tar xvf` izvadi iz arhive

- Kombinacija find + tar za backup datoteka po nekom kriteriju

Rezime

- Adminstracija se radi svaki dan - treba planirati vrijeme za oko 30 minuta po stroju
- Mora se biti pedantan i sistematičan
- To je rutina koja se ne smije propustiti ili mijenjati
- Što više stvari automatizirati - skripte

- Važno:

Nitko je neće raditi umjesto vas!

Pauza
15 minuta

Vježba 1
Rutinsko praćenje sustava

Prijaviti se na sustav i provjeriti

- stanje quota — `quota -v`
- stanje diskova — `df`
- greške — `iostat`
- aktivne korisnike — `w,who`
- opterećenje sustava — `uptime`
- procese — `top, ps`

Što se može zaključiti uspoređivanjem rezultata top i w komandi ?

Vježba 2
Logovi na sustavu

Praćenje i rotacija logova na sustavu

Prijaviti se na sustav i provjeriti sustavske logove

- tražtiti moguće greške u `/var/adm/*` logovima
- tražiti nepravilnosti u `cron` logovima
- tražiti nepravilnosti u `/var/log/*` logovima

Nakon pregledavanja logova, treba rotirati datoteke i obrisati stare i nepotrebne logove

Vježba 3
Administracija korisnika

Dnevna administracija korisnika

Prijaviti se na sustav

- pronaći aktivne korisnike koji su idle više od dana i ubiti njihove procese
- kreirati korisnika pero
- postaviti inicijalni password za pero i provjeriti prijavu na sustav
- podesiti atribute za pero

Vježba 4
Automatsko izvođenje

Prijaviti se na sustav

- provjeriti stanje crontaba za root
- spremiti kopiju crontaba za root
- dodati u root crontab brisanje datoteka `/tmp` kazala svaki dan u ponoć i 5 minuta
- provjeriti dozvole za pristup cron servisu

Što se može dogoditi ako nismo napravili `su -` ?

Što se može dogoditi ako `EDITOR` varijabla nije postavljena ?

Vježba 5
Modificiranje rc skripti

Osnovni postupak:

- Prijaviti se na sustav
- dodati skriptu /etc/init.d/ime
- postaviti dozvole na 700
- kreirati S, K sripte iz potrebnih runlevela

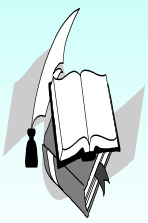
Vježba 5 (2)
Pokretanje ssh

- Prijaviti se na sustav
- dodati skriptu za pokretanje deamona
- postaviti dozvole na 700
- kreirati S, K sripte iz potrebnih runlevela

```
#!/bin/sh
vrag= /usr/local/sbin/sshd
if [ $1 - "start" ]; then
   test -x "$vrag" && $vrag
else
   if [ $1 - "stop" ]; then
      pid=`cat /etc/sshd.pid`
      test "${pid}" != "" && kill ${pid}
fi; fi
```


Literatura

- Ć leen Frisch: **Essential System Administration**, O'Reilly & Associates
- Solaris 2.7 dokumentacija
  http://bagan.srce.hr:8888/
- Frank G. Fiamingo: **Introduction to Unix System Administration**,
  http://wks.uts.ohio/state.edu/sysadm_course
- Mark Burgess: **Principles of system administration**,
  http://www.iu.hioslo.no/~mark/sysadmin/SystemAdmin.html
- "**System Administration**" priručnici



Što dalje?

- Samostalan rad
- Proučavanje dokumentacije
- *Učenje na greškama (svojim i tuđim)*
- Seminari