Operativni sistemi
- Administracija GNU/Linux sistema -

Veljko Stanković

Uvod

Osnovni zadaci administracije GNU/Linux sistema

- Upravljanje mrežom
- Administracija korisničkih naloga
- Upravljanje fajl sistemima
- Obezbeđivanje sistema I praćenje sigurnosnih propusta
- Bezbednost na mreži
- Upravljanje Internet uslugama, servereima i mrežnim fajl sistemom

Upravljanje mrežom

Podešavanje TCP/IP protokola kako bi sistem mogao da komucira reko mreže zahteva administraciju određenog broj konfiguracinih fajlova.

/etc/hosts

- ovaj fajl sadrži listu IP adresa i imena terminala na mreži
- U odsustvu DNS servera, svaki program proerava u ovom fajlu kom terminalu odgovara koja IP adresa.

/etc/networks

- sadrži listu mreža i IP adresa i služi pri rutiranju kada se umesto IP adresa za rutiranje koriste imena mreža.

/etc/hosts.conf

- sadržaj ovog fajla pomaže biblioteci za konverziju imena u IP adrese kako da izvrši tu konverziju.
  - order hosts, bind (kojim redosledom se pretražuju imena terminala)
  - multi on (da li terminal može imati više od joedne IP adrese)

Upravljanje mrežom

1010011
1110100
1100001
1010110

/etc/resolv.conf

sadrži listu imena DNS servera

search opcija određuje kako da traži ime terminala

nameserver 192.168.0.1 # dhcp: eth0

search nrockv01.md.comcast.net

/etc/hosts.allow

Identifikuje terminale kojima je dozvoljeno da koriste internet usluge na sistemu korisnika. Pre neego što se određena internet usluga pokrene, prvo se konsultuje ovaj fajl.

Zapis fajla je u obliku servicenam:IP address

- Ime ervera koji pruža određenu internet usugu
- IP adresa terminala koji sme da pristui datoj usluzi

in.telnetd:192.168.0. (svi računari na mreži 192.168.0.0 mogu da pristupe telnetu)

ALL:192.168.0. (svi hostovi na mreži sa datom IP adresom)

Upravljanje mrežom

/etc/hosts.deny

/etc/nsswitch.conf

name service switch – uređuje interakciju usluga (kao što su resolver, NIS) i lokalni konfiguracioni fajlovi.

Komandom /sbin/ifconfig se mogu videti trenutno konfigurisani mrežni interfejsi.

Komandom ping se lako može utvrditi veza sa ostalim hostovima na mreži.

Komandom netstat se može dobiti stanje mreže.

netstat -l -> aktivni mrežni interfejsi

netstat – t -> aktivne TCP konekcije

netstat – ta -> sve aktivne TCP konekcije i one koje nas sistem prati li preko kojih nije uspostavljena veza

Upravljanje mrežom

Snffing

Usluga koja omogućava praćenje sadržaja TCP/IP paketa.

tcpdump (kao root)

tcpdump -a -c 1000 > tdout

Osnove sistem administracije

1010011
1110100
1100001
1010110

Sistem administracija obuhvata sve one aktivnosti koje su potrbne kako bi sistem bio aktivan i funkcionalan.

Aktivnosti vezane za administraciju sistema

- Kreiranje i uklanjanje korisničkih naloga
- Upravljanje pristupa štampaču
- Instalacija, konfigurisanje i modernzacija OS-a i usluga
- Instalacija softvera
- Upravljanje hardverom
- Backup-ovanje sistema
- Upravljanje fajl sistemima
- Automatizacija zaataka
- Nadgledanje performansi sistema
- Podešavanje, upravllljanje i nadgledanje bezbednosti sistema

Osnove sistem administracije

Preuzimanje administratorskih prava (kako postati root)

- koanda su -
- komanda sudo

Oporavak od gubitka root lozike

- Sistem se pokreće sngle user modu (sistem startuje bez GUI)
- passwd – nakon čega možemo unet novu lozinku

Izvršavanje procesa

kojim redosledom se pokreću procesi na sistemu je bitno kako bi se kasnije pokretale i zaustavljale odeđene usluge.

Prvi proces koji se pokreće je init

Šta će init proces da pokrene zavissiće od tzv. runlevel

Obično ima 7 runlevela (0-6) koji identifikuju koji od grupe procesa mogu da se izvršavaju.

Tekst fajl /etc/inittatb definiše koji se procesi na kom runlevel-u mogu izvršavati.

Osnove sistem administracije

Komanda koja nam daje na kom smo treuntno runlevel

/sbin/runlevel

Promena runlevela

init br_runlevela

Table 1-7	Run Levels in Linux
Run Level	*Meaning*
0	Shuts down the system
1	Runs in single-user standalone mode (no one else can log in; you work at the text console)
2	Runs in multiuser mode (Debian, Ubuntu, and Xandros use run level 2 as the default run level)
3	Runs in full multiuser mode (used for text mode login in Fedora Core, MEPIS, and SUSE)
4	Runs in full multiuser mode (unused in Fedora Core, MEPIS, and SUSE)
5	Runs in full multiuser mode (used as the default run level with graphical login in Fedora Core, MEPIS, and SUSE)
6	Reboots the system

Pokretanje i zaustavljanje servera

- Skriptovi za pokretanje servera pri startovanju sistema se nalaze u dirketorijuu /etc/init.d
- Ovi skriptovi se mogu ručno okretati ili se pojedini procesi mogu zaustavljati
- /etc/init.d/vsftpd stop
- /etc/init.d/vsftpd restart

Osnove sistem administracije

Praćenje performansi sistema

- Iskorišćenost CPU
- Iskoršćenost radne memorije
- Iskorišćenost virtuelne memorije
- Iskorišćenost HDD

Lista procesa prema iskoršćenosti resursa

- top
  - Prva linija pokazuje trenutno vreme, vrme rada sistema, koliko je korisnika logovano i prosečan broj procesa koji su spremni za izvršavanje u poslednjih 1,5 i 15 minuta.
  - druga linija pokazuje koliko procesa aktivno i stanje tih procesa
  - treća lnija pokazuje iskorišćenost CPU od strane korisničkih i sistemskih procesa i koji procenat vremena je CPU neiskorišćen
  - Četvrta linija daje iskorišćenost fizičke memorije
  - peta linija daje iskorišćenost virtuelne memorije

Izlaz komande top

Tabela daje inforaciju o:

- iD procesa
- ime korisnika
- prioritet procesa
- NI – nice value ima vrednost od -20(najviši) do 19(najniži prioritet). Podrazumevana vrednost je 0. Definiše relativni prioritet procesa.
- Velčina virtuelne memorije koju koristi proces.
- Veličina fizičke memorije koju koristi proces
- Veličin zajedničke (shared) memorije koju koristi proces
- Stanje procesa (S)leeping, D-uninteruptable, (R)unning, (Z)ombie, (T)erminated
- Procenat iskorišćenosti CPU
- Iskorišćenost fizičke memorije
- Ukupno vreme izvršavanja na CPU od početka izvršavanja procesa
- Skraćeni obik komande koja je pokrenula dati proces

Generalna informacija o stanju sistema

- uptime

Informacija o ukupnoj iskorišćenosti sistema u nekom intervalu vremena

- Statistika sistema usrednjena na svakih 5 sekundi (+ max br iija koje ce prikazati)
- vmstat 5 8
  - Broj i tip procesa; r-running, b-uninteruptable sleep, w – swapped out but read to run
  - info o fizičkoj memoriji: swpd-iskorišćena virtuelna memorija, free-slbodna fizička memorija, buff-deo fizičke memorije kao bafer, cache-deo virtuelne memorije koji je kešran
  - broj svapovanja: si-swapped in , so-swapped out
  - io informacija: bi- učestanost upisa, bo-učestaanost čitanja sa diska
  - system: in-br intt u sec, cs- br promene konteksta u sec
  - procenat upotrebe CPU: us-korisnici, sy-sistem, id-CPU slobodan, wa-vreme provedeno u čekanju na I/O

Osnove sistem administracije

Da bi mogao da koristi bilo koji uređaj kernel mora da ima drajver za taj uređaj.

- Drajver može biti statički uključen u kernel
  - zahteva rekompilaciju kernela pri promeni
- može se dinamici učitavati kao modul

Komande za rad sa modulima:

- insmod. ubauje modul u kernel
- rmmod. uklanja modul
- depmod: utvrđuje međuzavisnost izeđu modula
- ksyms: lista simbola i ime modula koji definišu dati sibol
- lsmod: lista trenutno aktivnih modula
- modinfo: infomacija o mudulu
- modprobe:automatsko ubacivanje i uklanjanje modula sa međuzavisnim modulovima

Osnove sistem administracije

- Pri administaciji sistema se javlja potreba za periodičnim izvršavanjem određenih programa.
  - Zadatak se može izvšavati periodično ili samo jednom u nekom određenom trenutku.
    - Backup-ovanje fajlova
    - Preuzimanje fajlova kada sistm nije preiše zauzet
    - Slanje podsetnika
    - Periodična anaiza lof-fajlova i pretraživanje neuobičajenh aktivnosti.
- Komanda at za izvršavanje jedne i više komandi u nekom trenutku
  - /etc/at.aallow i /etc/at.deny
    - lista korisnika koji mogu ili ne da koriste at komandu

Planiranje izvšavanja zadatka u određenom trenutku

- Unese se vreme kada se žei izvršavanje
- na promt at> se unose komande koje želimo da izvršimo u tom trenutku
- Kraj unosa komandi se naznačava kombinacijom CTRL+D
- Pregled zadataka: atq
- Uklanjanje zadataka atrm

Table 1-14 Formats for the Time of Execution with the at Command

Command	*When the Job Will Run*
`at now`	Immediately
`at now + 15 minutes`	15 minutes from the current time
`at now + 4 hours`	4 hours from the current time
`at now + 7 days`	7 days from the current time
`at noon`	At noontime today (or tomorrow, if already past noon)
`at now next hour`	Exactly 60 minutes from now
`at now next day`	At the same time tomorrow
`at 17:00 tomorrow`	At 5 p.m. tomorrow
`at 4:45pm`	At 4:45 p.m. today (or tomorrow, if it's already past 4:45 p.m.)
`at 3:00 Dec 28, 2006`	At 3:00 a.m. on December 28, 2006

Planiranje periodičnih poslova

- Komanda crontab
- /etc/cron.allow i /etc/cron.deny
  - Imena korisnika koji mogu ili ne da zadaju peridične zaatke
- Po potrebi pripremiti shell skript koji će se izvršavati periodično(ako imamo neki program onda se ovaj korak preskače)
- Kreira se fajl (pr. jobinfo) sa informacijom kada želimo da se dati program/skript izvršava
  - Unos tipa:
  - 5 0 * * * $HOME/myjob
  - vreme se zadaje u formatu: minut sat dan mesec dan u nedelji
- Zadatak se izvršava pozivom: cron jobinfo
- Listanje periodičnih zadataka: crontab -l
- Uklanjanje periodičnih zadataka: crontab -r

Osnove sistem administracije

1010011
1110100
1100001
1010110

- Administracija korisničkih naloga
  - Potrebno je imati root privilegije
  - Dodavanje korisničkih naloga
    - ☑ useradd -c
  - Postavljanje lozinke
    - ☑ passwd ime_korisnika
  - Modifikacija korisničkih naloga
    - ☑ usermod -g root naba
      - Korisnik naba se pripaja grupi root
- Sadržaj passwd fajla:
  - /etc/passwd:
    - ☑ korisnik:x:500:10:Ime prezime:/home/korisnik:/bin/bash
    - ☑ korisnik:(lozinka šifrovana):UID:GID:Ime prezime:home folder:default shell