Nadzor rada Linux/Unix poslužitelja

v1.1

Zdenko Skiljan
zskiljan@srce.hr

CARNet

srce

Sadržaj (1/2)

- UVOD
- Alati za grafički prikaz podataka
- Nadzor sklopovlja
- SNMP

Sadržaj (2/2)

- Nadzor logova
- Nadzor integriteta sistemskih datoteka
- Nadzor servisa
- Nadzor operacijskog sustava

UVOD
Predmet nadzora (1)

- **Rad sklopovlja**
  - Temperatura sistema (procesora, ploče itd.),
  - Brzina okretaja ventilatora,
  - Greške u sklopovlju (diskovi, memorija, mreža).
- **Opterećenje podsustava**
  - **Potrošnja procesora** (besposlenost, korisnički procesi, sistemski procesi – funkcije jezgre, I/O itd., korisnički procesi niskog prioriteta - nice),
  - **Broj prekida** (broj zahtjeva I/O uređaja za procesorom),

UVOD
Predmet nadzora (2)

- **Opterećenje podsustava (nastavak)**
  - **Opterećenje sustava za upravljanje procesima** (Context Switching) **-** određivanje prioriteta i količine vremena koje procesi imaju za izvođenje je proces koji na nekim operacijskim sustavima može biti faktor opterećenja i stoga je faktor koji se može promatrati,
  - **Zauzeće memorije**.

UVOD
Predmet nadzora (3)

- **Opterećenje podsustava (nastavak)**
  - **Uporaba virtualne memorija –** paging i swaping**,**
  - **I/O diskova, I/O mreže**,
- Anomalije u logovima,
- Cjelovitost sistemskih datoteka
- Dostupnost, ispravnost i anomalije u radu servisa
- Aktivni napadi na sustav (IDS)

UVOD
Izvori podataka

- Naredbe za propitivanje sustava (df,du,iostat,netstat, top, htop, atop, lsof itd.)
- Logovi /var/log/*
- /proc file system

Alati za grafički prikaz podataka

- Tijekom prezentacije analizirati ćemo čitav niz alata za nadzor.
- Većina od njih za prikaz sakupljenih podataka rabi ili može rabiti popularne alate za grafički prikaz podataka.
- Stoga ćemo pobrojiti najvažnije takve alate i njihove značajke.

Alati za grafički prikaz podataka MRTG – Uvod (1)

- Alat za skupljanje podataka i prikaz jednostavnih grafova s najviše dvije vrijednosti
- Mrtg prikuplja podatke kroz skripte definirane u konfiguraciji.
- Te skripte izvraćaju jednu ili dvije vrijednosti koje se mjere, periodikom koja je određena u sistemskom kalendaru (cron).

Alati za grafički prikaz podataka
MRTG – Uvod (2)

- Obično se MRTG pokreće svakih 5 minuta kroz sistemski kalendar ili je stalno aktivan kao daemon (ako se u konfiguraciji navede direktiva **RunAsDaemon** i **Interval 5** – nakon kojeg se skupljaju podaci i kreiraju grafovi).
- Iz podataka koje je dobio izračunava prosjek, rezultate pohranjuje te izrađuje grafove i html stranicu.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (1)

- Kroz konfiguracijsku datoteku MRTG-a dade se definirati niz postavki kao np.: gdje se smještaju generirane html datoteke (HtmlDir), a gdje su slike (ImageDir) itd.
- Za svaki par nadziranih veličina definiraju se u konfiguraciji posebne postavke kroz direktivu **Target**.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (2)

- Kroz direktivu **Options** dade se definirati niz izbora od kojih su možda najvažniji oni koji određuju način izračunavanja vrijednosti koje se prikazuju na grafu:
  - **Bits, perminute, perhour** (množi dobivene vrijednosti s 8, 60 i 3600),
  - **Nopercent –** sprječava postotni ispisa vrijednosti u legendi.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (3)

- **Gauge -** dobivene vrijednosti se tretiraju kao 'trenutne' a ne apsolutne vrijednosti i **ne dijele** se s vremenom proteklim od zadnjeg ispitivanja kako bi se dobio prosjek. Takav način računanja prikladan je za prikaz stanja diskovnog prostora, opterećenja procesora, temperature itd. Np. Prikazuje se jednostavno temperatura procesora ili količina dostupne memorije svakih 5 minuta.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (4)

- **Absolute –** dobivena vrijednost je broj koji je počeo od nula na početku intervala i za razliku od 'Gauge mjerenja' dijele se s vremenom proteklim od zadnjeg ispitivanja (ne izračunava se razlika vrijednosti od zadnjeg ispitivanja).
  Na primjer koliko prosječno poruka prolazi kroz server u zadanom intervalu ispitivanja.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (5)

- **Inače**, ako se ne navedu opcije **Gauge** i **Absolute** - dobivene vrijednosti se tretiraju kao brojači. Računa se razlika između trenutno očitane i prethodno očitane vrijednosti te se dijeli s proteklim vremenom i tako se dobiva vrijednost koja će se prikazati na grafu.
  Np. prikaz koliko je prosječno poruka prošlo kroz mail server u 5 minuta ako je ulazna veličina apsolutan broj poruka prošlih do sada.

Alati za grafički prikaz podataka
MRTG – Konfiguracija (6)

- **Thresh*** direktive definiranju uvjete slanja obavijesti
- **Growright** - definiranje smjera grafova svih mjerenih veličina (Target)

```
options[_]: growright
```

Alati za grafički prikaz podataka
MRTG – Konfiguracija (7)

```
RunAsDaemon: Yes
Interval:    5
```

Podnožje stranice:

```
PageFoot[myrouter]: Contact <A
   HREF="mailto:admin@domena.hr">Admin
   </A>  if you have questions
   regarding this page
```

ili zaglavlje:

```
AddHead[myrouter]: <link rev="made"
   href="mailto:mrtg@domena.hr">
```

Alati za grafički prikaz podataka
MRTG – Konfiguracija (8)

Izostavljanje nekog od grafova koji se rade podrazumno (w]eekly, [m]onthly and [y]early):

```
Suppress[myrouter]: y
```

Specifičan direktorij za pojedini graf:

```
Directory[myrouter]: myrouter
```

Za prikaz realnih neskaliranih vrijednost pojednih grafova:

```
Unscaled[myrouter]: ym
```

Alati za grafički prikaz podataka
MRTG – Primjer (1)

Konfiguracija:

```
WorkDir: /var/mrtg
WriteExpires: Yes
Target[cputemp]:
   `/root/scripts/cpu_temperature.sh`
MaxBytes[cputemp]: 120
Options[cputemp]: gauge, nopercent
Unscaled[cputemp]: dwym
YLegend[cputemp]: CPU0 & CPU1 temp
ShortLegend[cputemp]: C
```

Alati za grafički prikaz podataka
MRTG – Primjer (2)

Konfiguracija (nastavak):

```
LegendO[cputemp]:  CPU0:
LegendI[cputemp]:  CPU1:
Title[cputemp]: CPU temperatures - jagor
PageTop[cputemp]: <H1>CPU temperatures jagor
   (115C - (!) shutdown temperature)
 </H1>
  <TABLE>
   <TR><TD>System:</TD><TD>jagor</TD></TR>
   </TABLE>
```

Alati za grafički prikaz podataka
MRTG – Primjer (3)

Skripta za prikup podataka:

```
/root/scripts/cpu_temperature.sh
#!/bin/sh
 /usr/platform/sun4u/sbin/prtdiag -v |egrep
   "CPU0|CPU2" |egrep -v "FAN"| awk '{print
   $2}'
```

Rezultat skripte za prikup podataka:

```
% /usr/platform/sun4u/sbin/prtdiag -v |egrep
   "CPU0|CPU2" |egrep -v "FAN"| awk '{print
   $2}'
49
47
```

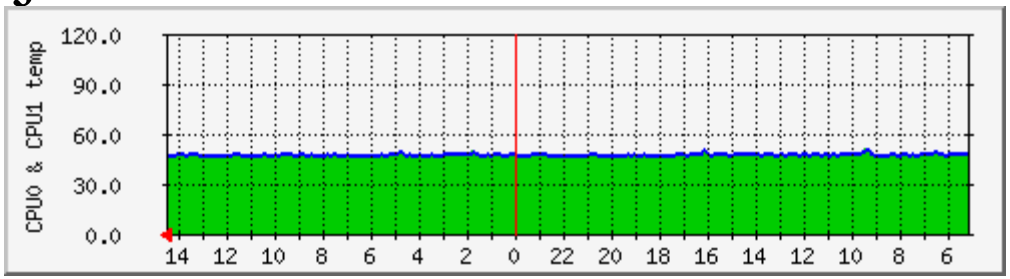
Alati za grafički prikaz podataka
MRTG – Primjer (4)

Cron posao (Solaris):

```
0,5,10,15,20,25,30,35,40,45,50,55 * \
   *  * * if [ -x /usr/local/bin/mrtg
   ]\ && [ -r /usr/local/etc/mrtg.cfg
   ]; then
   /usr/local/bin/mrtg \
   /usr/local/etc/mrtg.cfg >> \
   /var/log/mrtg/mrtg.log 2>&1;
   fi
```

Alati za grafički prikaz podataka
MRTG – Primjer (5)

- Opipljivi rezultati:



- Max CPU1:52.0 CAverage CPU1:49.0 CCurrent CPU1:49.0 CMax CPU0:51.0 CAverage CPU0:48.0 CCurrent CPU0:47.0 C
- **GREEN ###** Incoming Traffic in Bytes per Second
- **BLUE ###** Outgoing Traffic in Bytes per Second

Alati za grafički prikaz podataka
MRTG – Zaključak (1)

- MRTG je jednostavan (što se tiče konfiguracije),
- ograničen (na praćenje dvije unaprijed zadane vrijednosti), ali
- često vrlo upotrebljiv alat za prikupljanje i raznolik prikaz mjerenih veličina u nekom vremenskom razdoblju,
- s jednostavnim mehanizmom za slanje obavijesti.

Alati za grafički prikaz podataka
RRDtool - Uvod

- RRDTool je napravio autor MRTG-a.
- Napravljen je kako bi nadišao nedostatke MRTG-a.
- Konceptualno je drugačiji po tome što MRTG radi grafove svaki puta kada se pokreće dok RRDTool radi grafove tek po zahtjevu.

Alati za grafički prikaz podataka JRobin (1)

- JRobin je Java verzija RRDTool alata koja nam daje fleksibilnost i portabilnost Jave.
- JRobin rabi istu logiku, pojmove i definicije kao i RRDTool, a
- isto tako i omogućava potpuno isti izlaz za isti ulaz

Alati za grafički prikaz podataka JRobin (2)

- Prednost JRobina:
  - Portabilnost - baza podataka je skalabilna i neovisna o platformi
- Nedostaci JRobina:
  - Složen za uporabu kao i RRDTool

Alati za grafički prikaz podataka RRDtool & JRobin

- RRDTool/JRobin pružaju velik broj opcija za promjenu načina spremanja podataka i crtanja grafova.
- Slijedi kratak pregled upotrebljivosti RRDTool alata,
- Detaljnije opcije ćete morati proučiti sami.

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (1)

- Sakupljanje podataka i crtanja grafova kroz RRDTool ili JRobin
- Klasičan primjer je praćenje prosječnog broja kilobajta na mrežnom sučelju.
- Sustav počinje brojati od nule i povećava brojač za svaki (ulazni/izlazni) preneseni bajt.

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (2)

- Naredbom netstat dobijemo podatke:
  `% netstat -in`
  - skupljati ćemo vrijednost brojača u nekom vremenskom intervalu (5 minuta),
  - Oduzeti trenutnu vrijednost brojača od prošle zabilježene vrijednosti
  - Oduzeti trenutno vrijeme od prošlog zabilježenog vremena
  - Podijeliti razliku brojača s razlikom vremena.

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (3)

Ili matematički :

- B/sec= (brojač_trenutno - brojač_prethodno) / (vrijeme_trenutno - vrijeme_prethodno) / 8
- Time ćemo dobiti koliko je prosječno bajtova preneseno preko toga mrežnog sučelja u tom vremenskom intervalu.

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (4)

- Prvo kreiramo RRD bazu naziva **eth0.rrd** koja počinje **yyyyyyy**. Baza sadrži izvor podataka (Data Source - DS) **izlaz** u koji se svakih 5 minuta upisuje vrijednost brojača.
- U istu bazu se bilježe dvije **RR arhive** (**RRA**). U jednu arhivu se bilježi 24 uzorka od prosjeka vrijednosti svih ispitivanja (svaka dva sata), a u drugu se bilježi 10 vrijednosti od prosjeka vrijednosti 6 ispitivanja.
- rrdtool create eth0.rrd \
  DS:izlaz:COUNTER:600:U:U \
  RRA:AVERAGE:0.5:1:24 \
  RRA:AVERAGE:0.5:6:10

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (5)

- Nakon kreiranja baze podataka. Potrebno je napraviti mehanizam za punjenje baze.
- U cron np. postavimo mjerenje svakih 5 minuta i punjenje baze.

```
24/5 * * * * /root/scripts/izlazKb
```

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (6)

Skripta za prikupljanje podataka:

```
/root/scripts/IzlazKb
counter=`/bin/netstat -in | grep
  eth0 | awk '{print $7}'`
datum=`/bin/date '+%s' `
rrdtool update eth0.rrd
  $seconds:$counter
exit 0
```

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (7)

- Sadržaj baze lako možemo pregledati naredbom:

```
% rrdtool fetch test.rrd AVERAGE
  --start 920804400 --end
  920809200
```

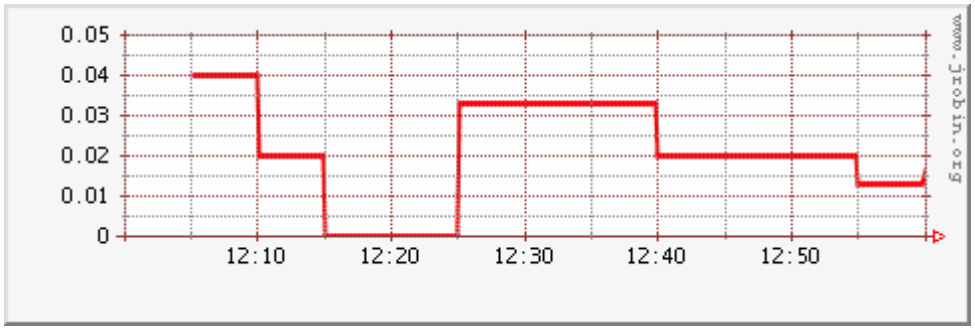
Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (8)

- Ali konačne rezultate najčešće želimo vidjeti u obliku grafa:

```
% rrdtool graph eth0.gif                    \
--start 920804400 --end 920808000   \
DEF:hostIzlaz=eth0.rrd:izlaz:AVERAGE\
LINE2:hostIzlaz#FF0000
```

Alati za grafički prikaz podataka RRDtool & JRobin - Primjer (9)

- Rezultat – GRAF



Alati za grafički prikaz podataka RRDtool & JRobin – Štivo za čitanje

- http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/rrdworld/index.html
- http://www.jrobin.org

Alati za grafički prikaz podataka RRDtool & JRobin – Zaključak

- Izuzetno moćni alati za izradu grafova
- Rabi ih jako velik broj programa za nadzor
- Postoji velik broj front-end programa za njih koji olakšavaju uporabu
- Složeni za uporabu, ali
- Nemaju premca i
- Trud uložen u učenje se isplati

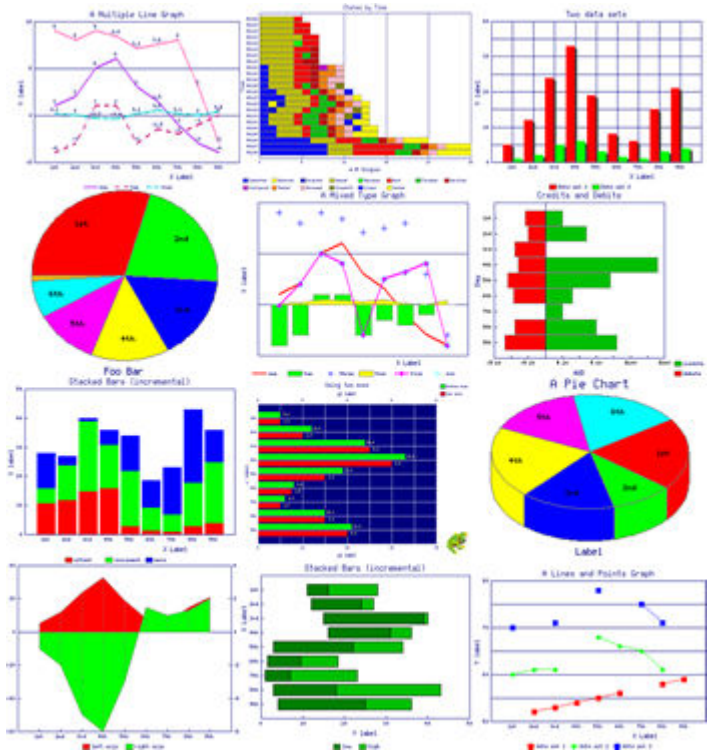
Alati za grafički prikaz podataka
Perl GD::Graph modul

- Glavni nedostatak prethodno prikazanih alata je da se vrijednosti koje se prikazuju u grafovima moraju unaprijed definirati.
- Ako želimo promatrati npr. promet mailova po korisnicima, koji korisnici su poslali velik broj mailova i sl., moramo unaprijed definirati korisnike u bazi.
- Ili ako želimo promatrati procese koji opterećuju poslužitelj, moramo unaprijed definirati procese, tako da ako neki novi proces iskoči po potrošnji on može biti samo definiran pod nepoznati proces.

Alati za grafički prikaz podataka
Perl GD::Graph modul

- Upravo za takve situacije idealan alat je GD::Graph modul za Perl.
- Nedostatak takvoga pristupa:
  - Potrebno znanje Perla
  - Treba uložiti više napora u programiranje
  - Grafovi koje nam pruža GD::Graph modul nisu tako moćni i složeni kao kod RRTool-a.

Alati za grafički prikaz podataka
Perl GD::Graph modul - Primjer



Alati za grafički prikaz podataka
Perl GD::Graph – Preporučeno štivo

http://search.cpan.org/~mverb/GDGraph-1.43/

http://www.devpapers.com/article/128

http://madpenguin.org/cms/?m=show&id=1197

Alati za grafički prikaz podataka
Perl GD::Graph modul - Zaključak

- Alat za ‘programatsku’ izradu grafova
- Nije pogodan za izradu ‘bogatih’ grafova,
- Ali je nezamjenjiv u slučaju potrebe iscrtavanja dinamičkih vrijednosti

Nadzor sklopovlja
Uvod (1)

- Pod nadzorom sklopovlja podrazumijeva se
  - nadzor temperature i napona pojedinih dijelova sklopovlja,
  - nadzor broja okretaja ventilatora,
  - nadzor ispravnosti diskovnih sustava
  - itd.

Nadzor sklopovlja
Uvod (2)

- Postoje niz alata prikladnih za nadzor sklopovlja.
- Među njima, obradit ćemo
  - standardne Linux/UNIX alate,
  - lm-sensors
  - alate za nadzor kroz sustave za udaljeno upravljanje poslužiteljima (Remote management console – RMC).

Nadzor sklopovlja
Standardni alati (1)

- U samom OS-u postoji čitav niz pomagala koji nam mogu pomoći u nadzoru sklopovlja
  - df, ifconfig, netstat, iostat, sar , /proc (/proc/cpu, /proc/partitions...), /var/log/kern.log
  - Paket smartmontools (control and monitor storage systems using S.M.A.R.T.)

Nadzor sklopovlja
Standardni alati (1)

- hwtools - collection of tools for low-level hardware management
- hwinfo - is used to probe for the hardware present in the system.
- hdparm
- prtdiag (Solaris)

- Mi smo ipak usmjereni na ozbiljne sustave za nadzor

Nadzor sklopovlja
Lm-sensors - Uvod (1)

- Standardan način nadzora rada sklopovlja na Linux sustavima je nadzor kroz lm-sensors programsku podršku.
- Od kraja 1997, većina matičnih ploča dolazi s čipom za nadzor sklopovlja koje su dostupni preko I2C, ISA ili SMBus sabirnica.
- ISA sabirnica postoji na poslužiteljima, iako nemate ISA utora :-). To nije nužno fizička sabirnica.

Nadzor sklopovlja
Lm-sensors - Uvod (2)

- SMBus (System Management Bus) je specifična implementacija I2C sabirnice. To je dvožična, serijska sabirnica koja služi za nadzor i upravljanje sklopovljem.
- I I2C i SMBus uređaji mogu biti spojeni na istu I2C sabirnicu.
- **Debianov Lm-sensors paket** uključuje skup modula za pristup nadzornim čipovima preko tih sabirnica.

Nadzor sklopovlja
Lm-sensors – Instalacija (1)

- Potrebna dva paketa:
  - **i2c-x.x.tar.gz** i
  - **lm_78-x.x.tar.gz**
- Kompiliraju se upravo tim redom. Prvi kreira /dev/i2c* uređaje, a drugi niz ‘drivera’ za čipove i neke 'user space' programe koji ih rabe.
- Konfiguracijska datoteka /etc/sensors.conf sadrži postavke za 'user space' programe koji sakupljaju podatke i prikazuju ih na definirani način.

Nadzor sklopovlja
Lm-sensors – Instalacija (2)

```
% wget
  http://www.lmsensors.nu/archive/lm_
  sensors-2.6.2.tar.gz
(% apt-get install lm-sensors-
  source;cd /usr/src)
% tar -xzvf lm-sensors.tar.gz
% cd modules/lm-sensors*
% make && make install
```

Nadzor sklopovlja
Lm-sensors – Instalacija (3)

```
% cd /usr/src
% wget
  http://www.lmsensors.nu/archiv
  e/i2c-2.9.1.tar.gz
(% apt-get install i2c-source)
% tar -xzvf  i2c*.tar.gz
% cd modules/ i2c*
% make && make install
```

Nadzor sklopovlja
Lm-sensors – Detekcija čipova

- Instalacijom gore navedenih paketa dobijemo naredbu sensors-detect koja će nam pomoći pri detekciji čipova prisutnih na sustavu
- Ti će nam podaci pomoći pri konfiguraciji senzora.

Nadzor sklopovlja
Lm-sensors – Konfiguracija (1)

- Sastoji se od konfiguracije datoteke /etc/sensors.conf u kojoj se definiraju čipovi koji se nadziru te željeni senzori.

Nadzor sklopovlja
Lm-sensors – Konfiguracija (2)

- /etc/sensors.conf:

```
bus "i2c-0" "SMBus ALI15X3 adapter at
   e800" "Non-I2C SMBus adapter"
chip "lm78-*" "lm78-j-*" "lm79-*"
   "w83781d-i2c-0-*" "sis5595-*"
label in0 "VCore 1"
label in1 "VCore 2"
label in2 "+3.3V"
```

Nadzor sklopovlja
Lm-sensors – Konfiguracija (3)

- /etc/sensors.conf: (nastavak)

```
label temp1 "MB-Temp"
label temp2 "CPU Temp"
compute in3 ((6.8/10)+1)*@ ,  @/((6.8/10)+1)
compute in4 ((28/10)+1)*@  ,  @/((28/10)+1)
# Lowered MIN Below!!!    set in0_min
   vid*0.60    set in0_max vid*1.05
# Lowered MIN Below!!!    set in1_min
   vid*0.60    set in1_max vid*1.05    set
   in2_min 3.3 * 0.95
```

Nadzor sklopovlja
Lm-sensors – rezultat

```
% sensors
w83781d-i2c-0-2d
Adapter: SMBus ALI15X3 adapter at e800
Algorithm: Non-I2C SMBus adapter
VCore 1:    +2.24 V  (min =  +2.09 V, max =  +3.66 V)
VCore 2:    +2.24 V  (min =  +2.09 V, max =  +3.66 V)
+3.3V:      +3.56 V  (min =  +3.13 V, max =  +3.63 V)
…
Fan1 N/A!:    0 RPM  (min = 3000 RPM, div = 2) ALARM
-Fan:  5273 RPM  (min = 3000 RPM, div = 2)
MB-Temp:  +27 C   (limit = +60 C, hysteresis = +50
   C)
CPU Temp: +28.5 C   (limit = +60.0 C, hysteresis =
   +50.0 C)  …
```

Nadzor sklopovlja
Lm-sensors – Preporučeno štivo

- http://howtos.linux.com/howtos/K7s5a-HOWTO-3.shtml
- http://paradoxical.nbtsc.org/~iguanacog/projects/lm_78/

Nadzor sklopovlja
Lm-sensors – Zaključak

- Izvrstan alat za nadzor sklopovlja
- Zahtijeva više truda za instalaciju i prave rezultate
- Za svaku preporuku

Nadzor sklopovlja
Remote management console (RMC)

- Sustave za udaljeno upravljanje poslužitelja najčešće ćemo pronaći kod poslužitelja s imenom (SUN, HP, Dell).
- Oni pored osnovnih funkcionalnosti (konzola za udaljeni rad koja omogućuje i paljenje i gašenje poslužitelja itd.) dozvoljavaju i osnovne funkcije nadzora sklopovlja.
- Tipično je riječ o posebnim karticama (PCI ili sl.) i koje posjeduju zasebno mrežno sučelje
- Ali mogu biti ugrađeni i na ploči.

Nadzor sklopovlja
Remote management console (RMC)

- Najpoznatiji su takvi sustavi iLO (HP), IPMI (Intel) i ALOM (SUN)
- Svaki od njih ima različite verzije, no općenito govoreći osnovne su značajke tih sustava da
  - iLO pruža raznolikije načine spajanja (Serial Port Telnet, Serial Port Web, Serial Port, sWebKV port (text), KVM port (graphics)), dok
  - ALOM i IPMI imaju snažniju podršku za nadzor sklopovlja i obavještavanje

Nadzor sklopovlja
RMC – IPMI (1)

- Nešto više ćemo govoriti o IPMI RMC sustavu
- IPMI je prije svega specifikacija za nadzor i upravljanje poslužiteljskim sklopovljem, koja standardizira nekoliko mehanizama za mjerenje i izvještavanje:
  - način nadzora temperature sklopovlja
  - udaljeno upravljanje gašenja/paljenja poslužitelja
  - upravljanje logovima sklopovlja
  - preusmjeravanje serijske konzole preko mreže

Nadzor sklopovlja
RMC – IPMI (2)

- IPMI se oslanja na BMC - Baseboard Management Controller, autonoman upravljačko nadzorni čip povezan na napajanje poslužitelja zahvaljujući čemu unatoč neaktivnosti ili padu sustava može upravljati paljenjem i gašenjem poslužitelja.
- Obično BMC sadrži i vlastito mrežno sučelje tako da je njime moguće upravljati i preko mreže, no moguće je i da BMC presreće promet s klasičnog mrežnog sučelja

Nadzor sklopovlja
RMC – IPMI (3)

- U principu ethernet sučelje se obično automatski pali kada se sustav uključi u struju tako da je teoretski uvijek moguće rabiti IPMI preko LAN-a.
- Pri tome naravno treba razmišljati o sigurnosti.

Nadzor sklopovlja
RMC – IPMI (4)

- Važno je napomenuti da je IPMI otvoreni standard i da na Debian sustavu postoji 'kernel space' programska podrška (Open IPMI – open source implementacija), a isto tako i 'user space' aplikacije (ipmitool, Intel DPC)
- Također postoji i GNU FreeIPMI (http://www.gnu.org/software/freeipmi/) 'user space' programska podrška.

Nadzor sklopovlja
RMC - OpenHPI

- Još jedan standard – obuhvatniji od IPMI standarda!
- OpenHPI - je open source implementacija HPI standarda (Hardware Platform Interface) koji razvija SA Forum i namjera mu je osigurati upravljanje i nadzor sklopovlja na višoj razini od IPMI standarda kako bi mogla omogućiti i upravljanje sustavim koji ne podržavaju IPMI.

Nadzor sklopovlja
RMC - Preporučeno štivo

http://www.cyclades.com/newsletter/articles/tech20040703

ILO:

http://www.columbia.edu/acis/sy/unixdev/projects/acis-linux/hp.html

IPMI:http://www.intel.com/platforms/applied/eiacomm/papers/25133701.pdf

IPMI: http://www.ami.com/support/doc/Mini-brochure_IPMI.pdf

HPI: http://openhpi.sourceforge.net/

Nadzor sklopovlja
RMC - Zaključak

- Zavisno od sklopovlja vašeg poslužitelja izabrat ćete prikladne programe za nadzor
- Ako i nemate RMC kartice, preporuka je da ih nabavite jer će vam uvelike olakšati administraciju i nadzor u slučaju ozbiljnijih problema na sustavu

SNMP – Uvod (1)

- “Standard” kada govorimo o alatima za nadzor, klasa za sebe
- Upravo zbog toga ga obrađujemo na početku
- Prikladan ne samo za nadzor poslužitelja
- Većina mrežnih uređaja podržava SNMP
- Simple Network Management Protocol

SNMP – Uvod (2)

- Simple Network Management Protocol (SNMP) je unatoč svome imenu složeni protokol za nadzor uređaja na mreži.
- SNMP pretpostavlja tri elementa,
  - mrežne uređaje koji se nadziru (usmjerivači, preklopnici, poslužitelji, pisači itd.),
  - SNMP agenta (server) koji na mrežnom uređaju sakuplja informacije i
  - SNMP upravljački program (klijent) koji traži informacije od agenta

SNMP - Razvoj

- Postoji 7 verzija SNMP protokola - SNMPv1, SNMPsec, SNMPv2p, SNMPv2c, SNMPv2u, SNMPv2* and SNMPv3.
- Preporučena je verzija SNMPv3.
- Debianov paket podržava sve verzije
- Razvoj protokola uglavnom motiviran sigurnosnim problemima

SNMP - Instalacija

- Na Debianovom Linuxu jednostavna.

```
% apt-get install snmp
```

- Inače:

```
% cd
% wget
http://kent.dl.sourceforge.net/sourceforg
e/net-snmp/net-snmp-5.2.1.tar.gz
% tar -xvzf net-snmp-5.0.2.tar.gz
% ln -s net-snmp-5.0.2 net-snmp
% cd ~/net-snmp
% ./configure  &&  make && make install
```

SNMP – Struktura podataka

- Informacije koje se sakupljaju, SNMP organizira u hijerarhijsku granaljkoliku strukturu poput datotečnog sustava koja se naziva Baza informacija za upravljanje (Management Information Base - MIB).
- Svaki čvor u toj granaljci ima oznaku (kratak tekst – label) i pripadajući broj koji označuje poziciju na određenoj razini granaljke

SNMP – Struktura podataka

- Za čuvanje podataka u tome sustavu SNMP rabi varijable koje mogu biti jedan od četiri tipa, integer, string, object identifier i null.
- Također imena varijabli slijede specifična ograničenja.

SNMP – Struktura podataka

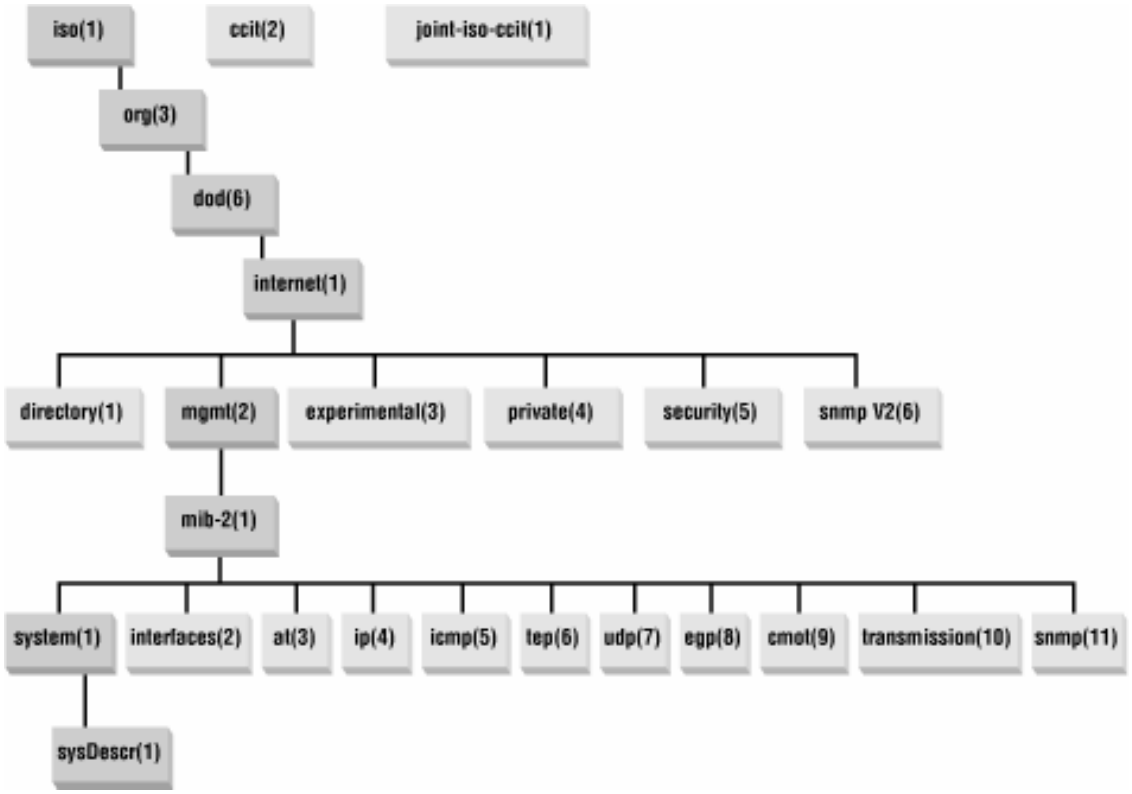
- Hijerarhijski najviši dio granaljke je unaprijed definiran i tek na 5. razini u granaljci čvora internet (1) nalaze se čvorovi koji su zanimljivi za nadzor mrežnih uređaja.
- Upravo u tim čvorovima ćemo pronaći podgranaljke (object groups) koje sadrže varijable koje želimo propitivati.

SNMP – Struktura podataka

- Varijable i objekte MIB granaljke možemo propitivati naredbom

```
snmpwalk: % snmpwalk -v 3 -c
  public localhost
  .iso.org.dod.internet.mgmt.mib
  -2.system
```

SNMP – Struktura podataka



SNMP – Sigurnost

- Svaki objekt u MIB granaljci je dostupan kao read-only, read-write ili je nedostupan.
- Kasnije verzije SNMP-a, dodale su bitno poboljšane sigurnosne mehanizme,
  - User Security Model – USM koji dodaje mogućnost enkriptiranu autentikaciju i enkriptirane poruke, i
  - View Based Access Control – VACM.

SNMP – Sigurnost

- Ako definiramo SNMP MIB pogled (view) i SNMP politiku pristupa (access mode) kažemo da smo definirali SNMP zajednicu (community), npr:

/etc/snmp/snmpd.conf

```
view all      included  \
   .iso.org.dod.internet.mgmt.mib-2.system
rwcommunity    private 10.0.15.0 \
   rocommunity   public
```

SNMP – Proširenje MIB granaljke

- Postojeće granaljke se dadu proširivati. Proširenja se dodaju kroz ascii datoteku MIB-XXX.txt koja se dodaje u direktorij definiran u datoteci /etc/default/snmpd:

```
export MIBDIRS=/usr/share/snmp/mibs
```

- Te datoteke definiraju objekte integrirane u pojedine dijelove MIB granaljke.

SNMP – Proširenje MIB granaljke

```
% ls -la /usr/share/snmp/mibs
-rw-r--r--  1 root root  17455 Mar 31 17:20
   AGENTX-MIB.txt
....
-rw-r--r--  1 root root  35242 Mar 31 17:20
   UCD-SNMP-MIB.txt
-rw-r--r--  1 root root   4076 Mar 31 17:20
   UDP-MIB.txt
```

SNMP – Proširenje MIB granaljke

Kada se dodaje nova MIB datoteka u popis MIBova, objekte se dade provjeriti kroz naredbu:

```
% snmptranslate 1.3.6.1.2.1.1.3.0
% snmptranslate -Tp -IR udp
```

Ili

```
% snmptranslate -Tp -IR \
  .iso.org.dod.internet.private.enter
  prises.ucdavis|less
```

SNMP – Proširenje MIB granaljke

- Također se može izlistati sve module koji su uključeni u SNMP agenta:

```
% snmpd -Dmib_init -H 2> moduli.snmp
```

- Uz popis modula dobije se i popis svih direktiva iz konfiguracijske datoteke (ekspliciranih i onih zadanih) koje su ispravne i koje su neispravne.

SNMP – Konfiguracija (1)

- Primjer Debianove zadane (Default) konfiguracije `/etc/snmpd/snmpd.conf`:

```
# sec.name  source          community
com2sec paranoid  default       public
group MyROSystem v1        paranoid
group MyROSystem v2c       paranoid
group MyROSystem usm       paranoid
group MyROGroup v1         readonly
group MyROGroup v2c        readonly
group MyROGroup usm        readonly
group MyRWGroup v1         readwrite
```

SNMP – Konfiguracija (2)

```
group MyRWGroup v2c        readwrite
group MyRWGroup usm        readwrite
view all    included  .1                              80
view system included  .iso.org.dod.internet.mgmt.mib-2.system
access MyROSystem ""      any       noauth    exact  system none
    none
access MyROGroup ""       any       noauth    exact  all    none
    none
access MyRWGroup ""       any       noauth    exact  all    all    none
syslocation Unknown (configure /etc/snmp/snmpd.local.conf)
syscontact Root <root@localhost> (configure
    /etc/snmp/snmpd.local.conf)
```

SNMP – Konfiguracija (3)

- Ona je vrlo restriktivna. Linijom:

```
com2sec paranoid  default          public
```

  Zadanom izvoru (bilo tko default public) pridružena je politika paranoid.

- Zatim je politika paranoid pridružena grupi MyROSystem.

```
group MyROSystem v1          paranoid
```

- I na kraju je grupi dopušten pristup samo na pogled (view) system.

```
access MyROSystem ""      any       noauth    exact
   system none   none
```

- Rezultat te konfiguracije je takav da netko tko pristupa s „default“ imenom zajednice (community string, password) public može vidjeti samo dio granaljke System.

SNMP – Konfiguracija (3)

- Primjer iščitavanja vrijednosti objekta naredbom snmpwalk i snmpget:

```
% snmpwalk -v 1 -c public localhost\
  .iso.org.dod.internet.mgmt.mib-\
  2.system.sysDescr.0
RFC1213-MIB::sysDescr.0 = STRING:
  "Linux pierre 2.4.29-grsec #1 SMP
  Tue Jan 25 00:15:20 CET 2005 i686"
```

SNMP – Konfiguracija (4)

```
% snmpwalk -m ALL -v 1 -c public \
  localhost system.sysDescr.0
RFC1213-MIB::sysDescr.0 = STRING:
  "Linux pierre 2.4.29-grsec #1 SMP
  Tue Jan 25 00:15:20 CET 2005 i686"
% snmpwalk -m ALL -v 1 -c public \
  localhost \
  .iso.org.dod.internet.private.enter
  prises.ucdavis.memory.memAvailReal.
  0
End of MIB
```

SNMP – Konfiguracija (5)

```
% snmpget -m ALL -v 1 -c public \ localhost
   .1.3.6.1.2.1.1.1.0
   RFC1213-MIB::sysDescr.0 = STRING: "Linux
   pierre 2.4.29-grsec #1 SMP Tue Jan 25
   00:15:20 CET 2005 i686"
% snmpget -m ALL -v 1 -c public localhost \
   .iso.org.dod.internet.mgmt.mib-\
   2.system.sysDescr.0
RFC1213-MIB::sysDescr.0 = STRING: "Linux
   pierre 2.4.29-grsec #1 SMP Tue Jan 25
   00:15:20 CET 2005 i686"
```

SNMP – Konfiguracija (6)

- Ako želimo malo slobodniju konfiguraciju možemo definirati konfiguracijsku datoteku **/etc/snmp/snmpd.local.conf** s novim dozvolama pristupa

SNMP – Konfiguracija (7)

/etc/snmp/snmpd.local.conf

```
#         sec.name     source          community
#  alias           host       password
com2sec localro      localhost localcomm
# grupa XXX          SNMPvalias
group MyROGroup      v1   localro
group MyROGroup      v2c  localro
group MyROGroup      usm  localro
```

- Umjesto da definiramo novu grupu, ovdje samo redefiniramo staru

SNMP – Konfiguracija (8)

- Primjer iščitavanja vrijednosti objekta naredbom snmpwalk:

```
% snmpwalk -m ALL -v 1 -c public localhost
   .iso.org.dod.internet.private.enterprises
   .ucdavis.memory.memAvailReal.0
End of MIB
% snmpwalk -m ALL -v 1 -c localcomm
   localhost
   .iso.org.dod.internet.private.enterprises
   .ucdavis.memory.memAvailReal.0UCD-SNMP-
   MIB::memAvailReal.0 = INTEGER: 18260
```

SNMP – Konfiguracija (9)

- Za pristup možemo definirati i korisnika: /etc/snmp/snmpd.local.conf:

....

```
createUser zskiljan MD5 malipero1
rwuser  zskiljan auth system
```

...

- Provjera pristupa:

```
% snmpwalk -v 3 -u zskiljan -l
  authNoPriv -a MD5 -A malipero1
  localhost
```

SNMP + MRTG – Primjer (1)

- U sljedećem primjeru pokazat ćemo kako možemo pomoću SNMPa i MRTGa uspostaviti nadzor opterećenja procesora
- Napravimo potrebne direktorije:

```
mkdir /etc/mrtg
mkdir /etc/cron.mrtg
mkdir /var/www/mrtg
```

SNMP + MRTG – Primjer (2)

- Zatim uredimo /etc/mrtg/cpu.cfg:

```
WorkDir: /var/www/mrtg
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[localhost.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:public@localhost + ssCpuRawSystem.0&ssCpuRawSystem.0:localcomm@localhost + ssCpuRawNice.0&ssCpuRawNice.0:localcomm@localhost
RouterUptime[localhost.cpu]: localcomm@localhost
```

SNMP + MRTG – Primjer (3)

- /etc/mrtg/cpu.cfg (nastavak)
  MaxBytes[localhost.cpu]: 100
  Title[localhost.cpu]: CPU
  LoadPageTop[localhost.cpu]: <H1>Active CPU Load %</H1>
  Unscaled[localhost.cpu]: ymwd
  ShortLegend[localhost.cpu]: %
  YLegend[localhost.cpu]: CPU Utilization
  Legend1[localhost.cpu]: Active CPU in % (Load)
  Legend2[localhost.cpu]:Legend3[localhost.cpu]:Legend4[localhost.cpu]:
  LegendI[localhost.cpu]: ActiveLegendO[localhost.cpu]:
  Options[localhost.cpu]: growright,nopercent

SNMP + MRTG – Primjer (4)

- Podesimo Cron posao **`/etc/cron.mrtg/cpu.sh`**

```
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/cpu.cfg
```

- Podesimo dozvole:

```
% /bin/chmod +x /etc/cron.mrtg/*.sh
```

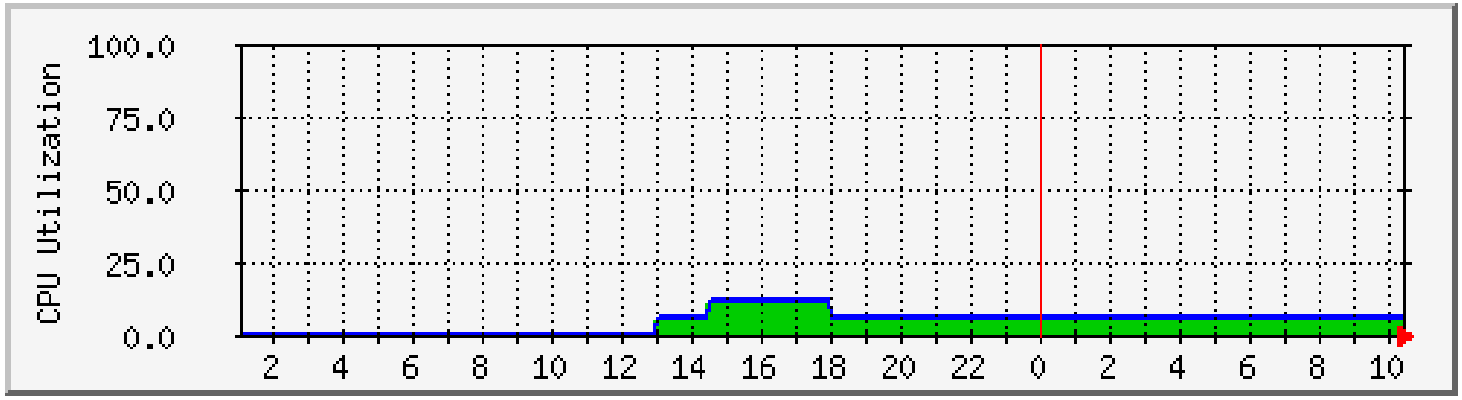
/etc/cron.mrtg/cpu.sh

- I na kraju: napravimo cron posao:

```
% /bin/cat >>
   /var/spool/cron/crontabs/root*/5 * * * *\
   /bin/run-parts /etc/cron.mrtg 1> \
   /dev/null^D
```

SNMP + MRTG – Primjer (5)

- I kroz neko vrijeme dobit ćemo pristojne grafove:



SNMP + MRTG – Preporučeno štivo

http://www.net-snmp.org

http://people.ee.ethz.ch/~oetiker/webtools/mrtg

SNMP - Zaključak

- Izuzetan alat za nadzor
- Često sastavnica drugih sustava
- Upotrebljiv na svim mogućim uređajima, od poslužitelja, usmjerivača, preklopnika do raznih drugih uređaja
- I zato se preporuča upoznavanje s njime i uporaba

Nadzor logova
Uvod

- Logovi su najvažniji izvor informacija za administratore sustava.
- Upravo zbog toga je razvijen čitav niz alata za nadzor logova sustava koji omogućuju reakciju (mail ili razne akcije) na neuobičajene logove kao:
  - logovima koji ukazuju na sigurnosne probleme,
  - logove koji ukazuju na probleme sa sistemom,
  - veliki broj pojavljivanja određenih logova i sl.

Nadzor logova
Logwatch - Uvod

- Logwatch je alat za nadzor i dnevno izvještavanje o zanimljivim događajima vezanim uz logove
- Koristan je za detekciju anomalija u logovima nastalim tijekom proteklog dana

Nadzor logova
Logwatch - Instalacija

Instalacija:

```
% wget
  ftp://ftp.kaybee.org/pub/linux/logwatch-
  6.0.1.tar.gz
% gunzip -c logwatch-6.0.1.tar.gz |tar xvf -
% cd logwatch-6.0.1; mkdir /etc/log.d
% cp -R scripts/ conf/ lib/ /etc/log.d/
% joe /etc/log.d/conf/logwatch.conf
```

Definiranje dinamike pokretanja:

```
% echo " 30 1 * * *
  /etc/log.d/scripts/logwatch.pl" >>
  /var/spool/cron/crontabs/root
```

Nadzor logova
Logwatch - Konfiguracija

- Logwatch dozvoljava nadzor svih ili pojedinih logova kroz konfiguracijsku direktivu `Service`.
- Šalje izvještaj mailom (`MailTo = root`) ili ih može snimiti na zadano mjesto (`Save = /arhiva/logwatch`).
- Razina detalja izvještaja može se podesiti kroz direktivu `Detail = 5  # (0,5,10),`
- Obavezno provjerite je li ispravna putanja do mailera (`mailer = /usr/bin/mail`).

Nadzor logova
Logwatch – Primjer izvještaja

```
##################### LogWatch 2.6 Begin
---------- Connections (secure-log) Begin --
   ------------
   **Unmatched Entries**
   userdel[12234]: delete user `rpcuser'
   userdel[12234]: remove group `rpcuser'
   userdel[12236]: delete user `nfsnobody'
   userdel[12236]: remove group `nfsnobody'
---------- Connections (secure-log) End ---
   -
######################### LogWatch End
```

Nadzor logova
Logwatch - Zaključak

- Odličan alat za utvrđivanje anomalija na dnevnoj razini
- Nema previše opcija za reguliranje detaljnosti izvještaja

Nadzor logova
Logcheck – Uvod (1)

- Logcheck je univerzalni alat za nadzor logova kroz bazu karakterističnih uzoraka te korisničku bazu uzoraka koji se trebaju zanemariti.

Nadzor logova
Logcheck – Uvod (2)

- Postoje dva odvjetka. Jedan se gotovo ne razvija. Logcheck-1.1.1 Drugi se razvija unutar Debian distribucije (Logcheck-1.2.35).
- Razlika je u strukturi baze uzoraka i nekoliko opcija.
- Debianov Logcheck uzorke dijeli po servisima. Uzorci za svaki servis se nalaze u posebnoj datoteci. Debianov Logcheck je ovisan o nizu drugih Debian paketa i nije ga jednostavno rabiti na drugim platformama.

Nadzor logova
Logcheck – Instalacija (1)

- Debian:

```
% apt-get install logcheck
```

- Instalirat će se paketi logcheck i logcheck-database.
- Logcheck-database sadrži bazu uzoraka za zanemarivanje za servise. Pojedini novi paketi za Debian nose sa sobom i baze uzoraka za zanemarivanje toga servisa koji se instalira.
- Također će se u administratorov cron dodati linija za periodično izvršavanje logcheck-a (tipično svakih sat vremena), no treba ga još i otkomentirati.

Nadzor logova
Logcheck – Instalacija (2)

- Ostale platforme:

```
% wget
  http://switch.dl.sourceforge.net/so
  urceforge/logcheck/logcheck-
  1.1.2.tar.gz
% gunzip -c logcheck-1.1.2.tar.gz |
  tar xvf -
```

...

- Instalacija nije zahtjevna.

Nadzor logova
Logcheck – Konfiguracija (1)

- /etc/logcheck/logcheck.conf
- Nakon instalacije valja podesiti tip računala koji se nadgleda,

REPORTLEVEL="server" # (workstation,paranoid)

- kome idu izvještaji,

SENDMAILTO="root"

- datum koji se pojavljuje u Naslovu izvještaja. Praktično kod izvještavanja s više računala, u liniju datuma se dade ubaciti i npr. ime računala s kojeg se obavijesti šalju.

DATE=`date +'%Y/%m/%d %H:%M';echo " igk"`

- Zanimljiva osobina Debianovog Logchecka je to da on omogućava i kreiranje korisničke baze uzoraka za obavijesti tipa „Active System Attack“.

SUPPORT_CRACKING_IGNORE=1

Nadzor logova
Logcheck – Konfiguracija (2)

- Osnova za pregledavanje logova je
  - baza uzoraka za traženje i
  - baza uzoraka za zanemarivanje
- Baza uzoraka se traženje sastoji od tri dijela,
  - uzorci koji znače aktivan napad na sustav,
  - sigurnosni uzorci i
  - sistemski uzorci (nepoznati događaji).
- Za svaku ot tih skupina uzoraka postoji u Debian-ovom Logcheck-u odgovarajuće korisničke datoteke s uzorcima koje treba zanemariti

Nadzor logova
Logcheck – Uzorci (1)

```
# ls -la /etc/logcheck/
drwxr-s---   2 root logcheck 1024 Feb 14 23:50 cracking.d
```

- **Uzorci koji upućuju na aktivni napad na sustav.**

```
drwxr-s---   2 root logcheck 1024 Jan 24 03:37 cracking.ignore.d
```

- **Korisnički uzorci koji upućuju na napad a treba ih zanemariti.**

```
-rw-r--r--   1 root logcheck  180 Apr 19  2004 header.txt
```

- **Tekst koji se pojavljuje na početku izvještaja.**

```
drwxr-s---   2 root logcheck 1024 Feb 18 00:58 ignore.d.paranoid
drwxr-s---   2 root logcheck 2048 Feb 18 09:13 ignore.d.server
drwxr-s---   2 root logcheck 1024 Feb 18 00:58 ignore.d.workstation
```

- **Uzorci koji upućuju na neobične incidente a treba ih zanemariti (zavisno od toga koji ste tip nadzora izabrali u datoteke u jednom od ova tri direktorija upisujete uzorke koji će se zanemarivati).**

Nadzor logova
Logcheck – Uzorci (2)

-rw-r----- 1 root logcheck 1970 Mar 7 11:33 logcheck.conf

- **Glavna konfiguracijska datoteka.**

-rw-r----- 1 root logcheck 131 Jan 24 03:37 logcheck.logfiles

- **Popis logova koji se nadziru.**

drwxr-s--- 2 root logcheck 1024 Feb 14 23:50 violations.d

- **Uzorci koji upućuju na sigurnosne incidente.**

drwxr-s--- 2 root logcheck 1024 Feb 18 00:58 violations.ignore.d

- **Uzorci koji upućuju na sigurnosne incidente, a treba ih zanemariti.**

Nadzor logova
Logcheck – Uzorci (3)

- Logcheck dolazi s povećom bazom predefiniranih uzoraka
- U načelu da bi se dnevno dobile zaista bitne informacije, potrebno je u bazu uzoraka za zanemarivanje ubaciti sve događaje koji su nebitni
- Pri tome je potrebno barem minimalno znanje regularnih izraza

Nadzor logova
Logcheck – Uzorci (4)

- Primjer ubacivanja uzorka za zanemarivanje logova sendmaila:
- Uzorak se ubacuje u datoteku:

/etc/logcheck/ignore.d.server/sendmail

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+
   (sendmail|sm-(mta|msp|que))\[[0-9]+\]:
   .*collect: premature EOM: Connection
   timed out
```

Ili (ako se ne želimo gnjaviti s finesama regularnih izraza)

```
sendmail.*collect: premature EOM: Connection
   timed out
```

Nadzor logova
Logcheck – Izvještaji (1)

- Logcheck se tipično izvršava svakih sat vremena
- Kada u logovima pronađe definirane uzorke koji su zabilježeni u bazi kao znak potencijalnog problema ili incidenta, on zadanom korisniku šalje mail s izvještajem

Nadzor logova
Logcheck – Izvještaji (2)

From: Super-User <root@xxx.xxx.hr>
Apparently-To: root@xxx.xxx.hr

Security Violations
=-=-=-=-=-=-=-=-=-=-=
Mar 10 15:42:06 xxx.xxx.hr identd[15163]: [ID 716877 daemon.error]
request_thread: read(0, ..., 1023) failed: Connection
+reset by peer

Unusual System Events
=-=-=-=-=-=-=-=-=-=-=
Mar 10 15:17:56 xxx.xxx.hr sendmail[14249]: [ID 801593 mail.crit]
j29Jl2tS027062: SYSERR(root): univ.oicp.net. config
+error: mail loops back to me (MX problem?)

Nadzor logova
Logcheck – Zaključak

- Izvrstan alat za kontrolu događaja na sustavu bez kojega ni jedan administrator ne može kvalitetno nadzirati logove
- Većih nedostataka nema
- Izvrsna nadopuna za logcheck je …

Nadzor logova
Swatch

- Alat koji je vrlo sličan Logcheck-u, no koji ipak funkcionira dosta drugačije.
- Za razliku od Logchecka koji može samo slati izvještaja putem mail-a, Swatch može izvršiti najrazličitije akcije pri pronalasku određenih uzoraka u logovima.
- Vrlo važna osobina Swatcha koja ga razlikuje od Logchecka je definiranje broja poruka u vremenu nakon koje se šalje poruka odnosno izvršava neka akcija.

Nadzor logova
Swatch – Konfiguracija (1)

- Općeniti obrazac za podešavanje konfiguracije programa swatch je:

```
Watch /REGEXP/
AKCIJE
```

Nadzor logova
Swatch – Konfiguracija (2)

- Akcije pak mogu biti vrlo raznolike:
  - Možete ispisati pronađenu linije na različite načine (`echo [modes]`)
  - Možete izvršiti neku naredbu (`exec command`)
    - (pri tome naredba može sadržavati varijable koje su zamijenjene dijelovima linije koja je zadovoljila uvijet zadan regularnim izrazom.. $N se zamjenjuje N-tim dijelom linije, a $0 ili $* se zamjenjuje cijelom linijom)

Nadzor logova
Swatch – Konfiguracija (3)

- Možete poslati mail s linijama koje su zadovoljile uvijet (`mail \ [addresses=address:address:...][, subject=your_text_here]`)
- Možete limitirati koliko puta se akcija može izvršiti na nekom uzorku (`throttle hours:minutes:seconds,[use=message|regex|<regex]>`)

Nadzor logova
Swatch – Konfiguracija (4)

- Možete zadati broj linija u zadanom vremenu koji treba zadovoljiti uvjete da bi se izvršila akcija (`threshold events:seconds,[repeat=no|yes]`)
- Možete i odrediti vremensko razdoblje kada naredba smije biti izvršena, npr. mail se izvršava u radno vrijeme, a sms iza radnog vremena radnim danom. (`when=day_of_week:hour_of_day`)

Primjer: `mail=sysad-pager@somehost.somedomain,when=1-6:8-17`

Nadzor logova
Swatch – Primjeri (1)

```
# System reboots
watchfor   /SunOS Release/
      echo
      bell
      mail
      exec "call_pager 3667615 0411“
# System crashes and halts
watchfor    /(panic|halt)/
          echo
          bell
          mail
          exec "call_pager 3667615 0911"
```

Nadzor logova
Swatch – Primjeri (2)

```
watchfor    /sm-mta.*from=/
mail=root@xxx.hr, subject=---- \
   PREVISE MAILOVA UNUTAR 1 SATA ----\
   throttle 10:00:00
watchfor    /disk full (.*)/
mail= root@xxx.hr, subject=----\
   ZAPUNJENA PARTICIJA $1----
watchfor    /user (.*) over quota/
mail=$1@xxx.hr, subject=----PREMASEN\
   DOZVOLJENI PROSTOR ---
```

Nadzor logova
Swatch - Pokretanje

Ako se pokreće bez argumenata zadane su vrijednosti argumenata:

```
% swatch --config-file=~/.swatchrc --tail-
   file=/var/log/syslog
```

ili ako postoji /var/log/messages

```
%  swatch --config-file=~/.swatchrc --tail-
   file=/var/log/messages
```

Umjesto zadanog (default) ponašanja možete zadati neke specifične logove, kao npr. logove IDS sustava Snort i specifičan tail program, kao npr. gtail s posebnim argumentima.

```
% swatch --tail-prog=/usr/local/bin/gtail \
              --tail-args '--follow=name --lines=1' \
              --tail-file="/var/log/messages
   /var/log/snort/alert"
```

Nadzor logova
Swatch – Zaključak

- Odličan alat za nadzor logova i djelovanje na pojavu određenog broja ili vrste logova
- Jako puno opcija za fino podešavanje
- Odlična nadopuna za logcheck
- Jedan od alata koji svaki administrator MORA rabiti

Nadzor integriteta datoteka
Uvod (1)

- Postoji niz alata za provjeru integrita datoteka, AIDE, Samhain, Tripwire, Integrit, Osiris, Fcheck, itd.
- Takvi programi provjeravaju, jesu li zadane datoteke mijenjane, brisane ili doživjele promjenu atributa te u slučaju promjene šalju izvještaje.

Nadzor integriteta datoteka
Uvod (2)

- Tripwire je najpoznatiji među tima alatima
- Izvrsni su AIDE i Samhain
- Usporedni prikaz dostupan na adresi:

http://la-samhna.de/library/scanners.html

Nadzor integriteta datoteka
AIDE - Konfiguracija (1)

- Konfiguracija datoteka je /etc/aide/aide.conf
- Definira datoteke ili direktorije koje se provjeravaju:

```
/usr/lib
```

- I izuzetke:

```
!/usr/lib/amavis
```

Definira atribute koji se provjeravaju:

```
Binlib = p+i+n+u+g+s+b+m+c+md5+sha1
/usr/lib Binlib
```

Nadzor integriteta datoteka
AIDE - Pokretanje i osvježavanje baze

- AIDE se pokreće kroz cron:

/etc/cron.daily/aide

- Nakon instalacije novih programa na sustav, valja napraviti update baze kako bi dobili što manje šuma u informacijama:

```
% /usr/bin/aide --init && cp \
  /var/lib/aide/aide.db.new \
  /var/lib/aide/aide.db&
```

Nadzor integriteta datoteka
AIDE – Izvještaj (1)

```
From: Super-User <root@jagor.srce.hr>
Subject: Daily AIDE report for jagor.srce.hr
To: root@jagor.srce.hr
This is an automated report generated by the
   Advanced Intrusion Detection
Environment on jagor.srce.hr at 04:00:00 on
   03/11/05.
Output of the daily AIDE run:
AIDE found differences between database and
   filesystem!!
Start timestamp: 2005-03-11 04:00:01
```

Nadzor integriteta datoteka
AIDE – Izvještaj (2)

```
Summary:
Total number of files=9392,added files=2,removed
   files=0,changed files=7
Added files:
added:/usr/sbin/logtail
added:/usr/sbin/logcheck
Changed files:
changed:/etc/pam.conf
Detailed information about changes:
File: /etc/pam.conf
  Mtime     : 2005-03-01 23:20:02                    ,
   2005-03-09 21:55:32
  Ctime     : 2005-03-01 23:20:02                    ,
   2005-03-09 21:55:32
```

Nadzor integriteta datoteka
AIDE - Zaključan

- Izuzetno moćan i upravljiv alat
- Apsolutno nužan za kontrolu integriteta sistema
- Jedina mana je to da se izvještaji šalju bez obzira na to je li stanje promijenjeno (ako je to mana)

Nadzor servisa
Uvod

- Postoji niz alata za nadzor servisa na sustavu.
- Općenito se takovi alati spajaju putem mreže i provjeravaju aktivnost/ispravan rad servisa, no neki od njih omogućuju instalaciju udaljenih agenata za nadzor
- Od brojnih alata istaknut ćemo MON monitoring daemon i Nagios

Nadzor servisa
MON – Uvod (1)

- MON je program koji rabi Srce za nadzor svoji poslužitelja.
- Vrlo je moćan, upravljiv i proširiv.
- Uglavnom je orijentiran na provjeru servisa putem mreže, te nema mehanizme za sakupljanje podataka o udaljenom sustavu.)

Nadzor servisa
MON – Uvod (2)

- Njegovi nedostaci su:
  - siromašno web sučelje koje dolazi s njim
  - spremanje podataka o nadzoru u 'plain text' formatu, što onemogućuje jednostavne upite na bazi.
  - Vrlo loše je riješeno propitivanje tekućeg stanja servisa na pojedinim hostovima (Može se pitati samo za sve hostove, ne i pojedinačno)

Nadzor servisa
MON – Monitori, alerti itd.

- S distribucijom MON-a, dolazi velik broj programa za propitivanje servisa i slanje obavijesti
- Većina je pisana u perlu i C-u, a svi su smješteni u direktorije:

`/usr/lib/mon/mon.d,  i`

`/usr/lib/mon/alert.d`

To su dns.monitor, http.monitor, mail.alert, sms.alert itd.

- Po potrebi se mogu nadopunjavati novima

Nadzor servisa
MON – Konfiguracija (1)

- Kofiguracija je jednostavna.
- Nakon instalacije (Debian: `% apt-get install mon`) treba urediti glavnu konfiguracijsku datoteku /etc/mon/mon.cf.
- Za svaki host, definiraju se servisi
- za svaki servis definira se
  - program koji propituje servis
  - ovisnost
  - Učestalost obavijesti i osobe koje se kontaktiraju, itd

Nadzor servisa
MON – Konfiguracija (2)

- /etc/mon/mon.cf određuje gotovo sve postavke:

```
# Direktorij s skriptama za slanje
  obavijesti
# (mail.alert, sms.alert itd.)
alertdir    = /usr/lib/mon/alert.d
# Direktorij s skriptama za nadzor
  servisa
# (ping.monitor, https.monitor,
  dns.monitor itd.)
mondir      = /usr/lib/mon/mon.d
```

Nadzor servisa
MON – Konfiguracija (3)

```
maxprocs    = 100
histlength = 100
randstart = 300s
logdir = /var/log/mon
# Log s informacijama o padovima servisa
dtlogfile = downlog
dtlogging = yes
histlength = 2000
historicfile = alerthistorylog
```

Kraj općih postavki

Nadzor servisa
MON – Konfiguracija (4)

Definiranje popis nadziranih hostova:

Alias Ime

Početak popisa hostova

```
hostgroup nepostojeci.izmisljena.hr \
   nepostojeci.izmisljena.hr
hostgroup zzz.zzz.hr  \
   zzz.zzzz.hr
hostgroup aaaa.yyy.hr  \
   aaa.yyy.hr
```

Kraj popisa hostova

Nadzor servisa
MON – Konfiguracija (5)

Definiranje servisa za svaki host:

```
watch nepostojeci.izmisljena.hr
        service dns
                description
   root@izumisljena.hr
                interval 10m
                monitor dns.monitor -master\
   nepostotjeci.izmisljena.hr -zone
   izmisljena.hr nepostojeci.izmisljena.hr
                …
```

Nadzor servisa
MON – Konfiguracija (6)

Definiranje servisa za svaki host: (nastavak)

```
depend  nepostojeci.izmisljena.hr:ping
                dep_behavior m
                period wd {Mon-Sun}
                        alertafter 2 40m
                        alert mail.alert \
   root@izmisljena.hr sef@izmisljena.hr
                        alertevery 24h
```

Nadzor servisa
MON – Propitivanje stanja (1)

Stanje hostova se može nadzirati na više načina:

- kroz web sučelje (s MONom dolazi rudimentarno web sučelje)
- kroz moncmd naredbu
- spajanjem na port 2583

Nadzor servisa
MON – Propitivanje stanja (2)

Održavane ustanove – NSA

01. + prvi.nemame.hr
02. + drugi. nemame.hr
03. + tretji. nemame.hr
04. + cetvrti. nemame.hr
05. + peti. nemame.hr
06. + sesti. nemame.hr
07. - sedmi. nemame.hr (! imap ! pop3)
08. + osmi. nemame.hr
09. + deveti. nemame.hr

Nadzor servisa
MON – Propitivanje stanja (3)

```
% moncmd -s monserver.domena.hr listopstatus
    | grep host.domena.hr | grep ntp
```

group=host.domena.hr service=ntp opstatus=1
last_opstatus=1 exitval=0 timer=1047
last_success=1113555707 last_trap=0
last_check=1113555706 ack=0 ackcomment=''
alerts_sent=0 depstatus=1
depend='host.domena.hr:ping'
monitor='ntp.monitor' last_summary='' last_detail=''
interval=3600

Nadzor servisa
MON – Propitivanje stanja (4)

- Spajanjem na port 2583, dobijemo iste informacije kao i kroz naredbu moncmd.

Nadzor servisa
MON – Preporučeno štivo

http://www.kernel.org/software/mon/

Nadzor servisa
MON – Zaključak

- MON je izuzetno kvalitetan sustav za nadzor servisa
- Lako se dade proširivati, no
- Ima vrlo nekvalitetno web sučelje
- I gotovo se ne razvija
- Preporučuje se zbog jednostavnosti

Nadzor servisa
Nagios – Uvod (1)

- Nagios je noviji alat za nadzor servisa, koji je nadmašio MON po brojnim mogućnostima
  - bogatom web sučelju,
  - SQL bazom podataka o nadziranim uređajima,
  - mogućnošću instaliranja lokalnih agenata,
  - administratorskim web sučeljima, od kojih je najbolji Nagmin, plugin za Webmin koji konfiguraciju također čuva u sql bazi podataka. Pored njega, tu je i Nagat.
  - mogućnošću definiranja akcija u slučaju problema

Nadzor servisa
Nagios – Uvod (2)

- To je vrlo moćan ali i za konfiguriranje izuzetno zahtjevan sustav
- Kao i MON, ima velik broj monitora koji se dadu dopuniti
- Za razliku od MONa u stalnom je razvoju
- Za Debian postoji čitav niz paketa oko Nagiosa
- Vidi: `% apt-cache search nagios`

Nadzor servisa
Nagios – Uvod (3)

- Nagios posjeduje veliki broj opcija koje premašuju opseg ovog pregleda
- Kroz konfiguraciju se dade definirati, skupine hostova, hostove, servise, kontakte, vremenska razdoblja, naredbe itd.
- Dodatni programi NRPE i NSCA omogućuju izvršavanje programa za nadzor na udaljenim računalima

Nadzor servisa
Nagios – Instalacija (1)

Na Debianu, instalacija je vrlo jednostavna:

```
% apt-get install nagios-mysql
    (nagios-text)
```

No konfiguracija i nije potpuno jednostavna.

Konfiguracijeske datoteke se nalaze u **/etc/nagios**.

Nadzor servisa
Nagios – Instalacija (2)

Na Debianu, instalacija je vrlo jednostavna:

```
% apt-get install nagios-mysql
    (nagios-text)
```

No konfiguracija i nije potpuno jednostavna.

Konfiguracijeske datoteke se nalaze u **/etc/nagios**.

- Vidi: `% ls -la /etc/nagios`

Nadzor servisa
Nagios – Instalacija (3)

- Da bismo aktivirali web sučelje, potrebno je u konfigueraciju apache servera nadodati konfiguraciju za nagios web:

```
% echo 'Include \
  /etc/nagios/apache.conf' >> \
  /etc/apache/httpd.conf
```

- Ako pri instalaciji nismo definirali lozinku za nagios admin korisnika, možemo to napraviti sada:

```
%  htpasswd -b \
  /etc/nagios/htpasswd.users \
  nagiosadmin 'LOZINKA'
```

Nadzor servisa
Nagios – Instalacija (4)

- Kada smo to sve napravili, možemo pogledati i web sučelje:

```
% lynx http://localhost/nagios
```

- U lynxu bas i nije impresivno, ali u Firefoxu ili Exploderu je lijepse:

Nadzor servisa
Nagios – Web sučelje

Nadzor servisa
Nagios – kreiranje Mysql baze (1)

- Nakon konfiguriranja nagiosa, potrebno je kreirati nagiosovu mysql bazu podataka
- Za to morate znati root password mysql daemona.
- Obično je on prazan string ukoliko niste, a poželjno je da jeste definirali drugi password.

```
% mysqladmin -u root -p create nagios
Enter password:
```

Nadzor servisa
Nagios – kreiranje Mysql baze (2)

- Kada je kreirana baza, treba je napuniti s tablicama itd.

```
% zcat /usr/share/doc/nagios-
   mysql/create_mysql.gz | mysql -u
   root -p nagios
Enter password:
```

- Još je potrebno podesiti dozvole na tablicama:

```
% mysql -u root -p nagios
Enter password:
```

Nadzor servisa
Nagios – kreiranje Mysql baze (3)

…

```
mysql> GRANT SELECT, INSERT,
   UPDATE, DELETE ON nagios.* TO
   nagios@localhost IDENTIFIED BY
   'password';
GRANT LOCK TABLES ON nagios.* TO
   nagios@localhost IDENTIFIED BY
   'password';
```

Nadzor servisa
Nagios – kreiranje Mysql baze (4)

- Završna operacija je postavljenje ispravnih vrijednosti u **/etc/nagios/resource.cfg** i **/etc/nagios/cgi.cfg:**

```
XXddb_database=nagios
XXddb_username=nagios
XXddb_password=password
```

- I još malo podešavanja dozvola na sistemu:

```
% chmod +x
   /etc/nagios/check_nagios_db
```

Nadzor servisa
Nagios – Konfiguracija - Uvod

- Konfiguracija je bazirana na templatama
- Kontrola pristupa definira se po korisnicima i grupama
- Na početku, zbog velikog broja opcija treba malo više truda za konfiguraciju
- Stvari uvelike olakšavaju web sučelja za konfiguriranje (Nagat, Webmin)

Nadzor servisa
Nagios – Konfiguracija (1)

- Za razliku od MONa, konfiguracija se definira kroz nekoliko datoteka

/etc/nagios/ hostgroups.cfg

```
define hostgroup{
        hostgroup_name  sredisnji_serveri
        alias           Sredisnji serveri
        contact_groups  jagor-chiefs,regoc-chiefs
        members         jagor.srce.hr,regoc.srce.hr
        }
```

Nadzor servisa
Nagios – Konfiguracija (2)

- **/etc/nagios/hosts.cfg**

```
define host{
        use                     generic-host
        host_name               jagor.srce.hr
        alias                   Javno racunalo
        address                 161.53.2.130
        check_command           check-host-alive
        max_check_attempts      10
        notification_interval   480
        notification_period     24x7
        notification_options    d,u,r
        }
```

Nadzor servisa
Nagios – Konfiguracija (3)

- /etc/nagios/Services.cfg

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               jagor.srce.hr
        service_description     PING
        is_volatile             0
        check_period            24x7
        max_check_attempts      3
        normal_check_interval   5
        retry_check_interval    1
        contact_groups          jagor-admins,jagor-chiefs
        notification_interval   120
        notification_period     24x7
        notification_options    c,r
        check_command           check_ping!100.0,20%!500.0,60%
        }
```

Nadzor servisa
Nagios – Konfiguracija (4)

- **/etc/nagios/contacts.cfg**

```
define contact{
        contact_name                    pero
        alias                           Pero Peric
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,u,r
        service_notification_commands   notify-by-email,notify-by-epager
        host_notification_commands      host-notify-by-email,host-notify-by-
          epager
        email                           zskiljan@srce.hr
        }
```

Nadzor servisa
Nagios – Konfiguracija (5)

- **/etc/nagios/contactsgroup.cfg**

```
define contactgroup{
        contactgroup_name       jagor-admins
        alias                   Administratori jagora
        members                 pero
        }
```

Nadzor servisa
Nagios – Konfiguracija (6)

- **/etc/nagios/contactsgroup.cfg**

```
define contactgroup{
        contactgroup_name       jagor-admins
        alias                   Administratori jagora
        members                 pero
        }
```

Nadzor servisa
Nagios – Zaključak

- Nagios je trenutno najzaokruženiji sustav za nadzor servisa i sustava
- Ima izvrsno web sučelje kako korisničko, tako i administratorsko
- Proširljiv je i vrlo konfigurabilan, prikladan je i za distribuirane sustave
- Sve preporuke

Nadzor servisa
Nagios – Preporučeno štivo

- http://www.nagios.org/
- http://sourceforge.net/projects/nagat/
- http://www.webmin.com/
- http://nagmin.sourceforge.net/

Nadzor operacijskog sustava
Uvod

- U ovoj skupini alata za nadzor obradit ćemo nekoliko alata čija je karakteristika “pasivan” nadzor – prikupljanje podataka o sistemu i servisima, te izrada grafova
- Između brojnih alata obradit ćemo Orcu i Gangliu

Nadzor operacijskog sustava
Orca (1)

- Sustav Orca je idealan za praćenje stanja sustava, trendova na sustavu te ekscesa kroz grafove u dužem vremenskom razdoblju.
- Sastoji se od dva modula
  - jedan koji sakuplja podatke o sustavu (Orcallator – Solaris, Procallator – Linux, Orca Services - Servisi) i
  - drugi (Orca) koji analizira podatke i izrađuje grafove i web stranicu.

Nadzor operacijskog sustava
Orca (2)

- Orcallator sustav je razvijen za Solaris i iskorištava snagu SE toolkita, jezika koji ima snažne rutine za izvlačenje podataka iz sustava bez dodatnog opterećenja sustava.
- Kasnije je napravljen Procallator koji crpe informacije iz /proc file sistema pomoću Perla.
- Orca_services pak sakuplja podatke iz logova servisa i isto tako je pisan u perlu.

Nadzor operacijskog sustava Orca (3)

- Skripta Orca iz sakupljenih podataka rabeći orcallator.cfg, procallator.cfg i orca_services.cfg izrađuje grafove i web stranicu.
- Obzirom da je ta operacija vrlo procesorski zahtjevna pametno je to raditi na nekom centralnom poslužitelju koji nije previše opterećen. Podatke na centralni poslužitelj je moguće prenijeti na razne načine (ftp,rsync, netcat itd.).

Nadzor operacijskog sustava Orca (4)

- Kroz konfiguracijske datoteke (orcallator.cfg, procallator.cfg i orca_services.cfg) koje se moraju nalaziti sam ona hostu koji radi grafove, definiraju se lokacije podataka, grafova, itd.
- Sami grafovi se rade kroz RRDtool, tako da se podaci zbog toga moraju prebaciti u RRDtool bazu.

Nadzor operacijskog sustava
Orca (5)

- **Orca_services** se nalazi u contrib dijelu distribucije i nešto je drugačija od Orcallatora i Procallatora.
- To je Perl skripta koja slično Logchecku, promatra logove i broji pojavljivanje različitih događaja kao np. broj poslanih poruka, broj smtp grešaka, broj ftp konekcija, broj ftp grešaka itd.
- Skripta se dade nadograditi s novim servisima (ako znate Perl)

Nadzor operacijskog sustava Orca (6)

- Prednosti:
  - S instalacijom Orce, dolazi velik broj monitora
  - Daje izuzetan pregled svih aspekata sistema
- Nedostaci
  - Nema mehanizama za slanje obavijesti
  - Složena instalacija i konfiguracija
  - Nije lako proširljiv

Nadzor operacijskog sustava Orca (7)

- **Sakupljeni podaci** za se spremaju u datoteku:

/usr/local/var/orca/procallator/regoc/
proccol-GODINA-MJESEC-DAN

/usr/local/var/orca/orcallator/jagor/
orcallator-GODINA-MJESEC-DAN-BROJ

Nadzor operacijskog sustava Orca (8)

- i imaju oblik:

 # zaglavlja

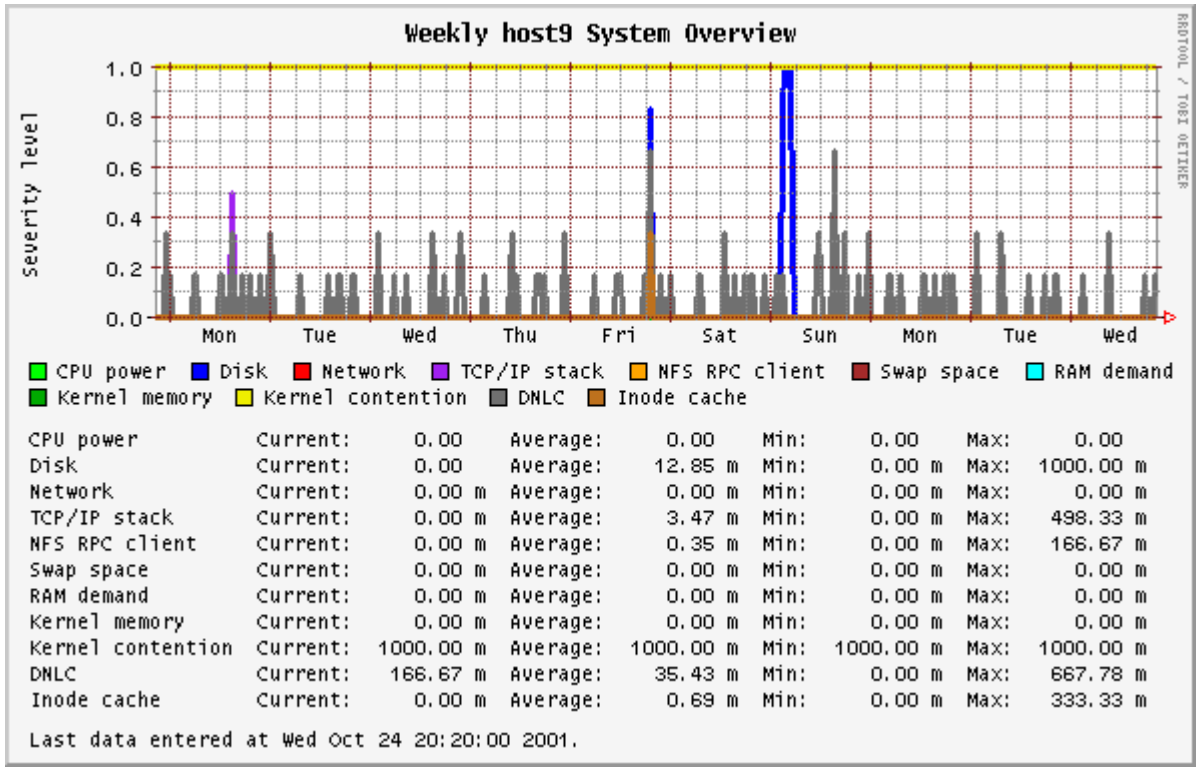
timestamp locltime uptime 1runq 5runq 15runq
#proc_oncpu #proc #proc/s ncpus usr%
nice% sys% wait% usr_%_1 …

1113516000 00:00:00 6818259.85 1.50 1.63
1.32 3 498 0.075 2 3.38 4.96 2.59 89.07

Nadzor operacijskog sustava
Orca (9)

- Sakupljeni podaci su Orci izvor za izradu grafova kroz RRDTool
- Kako je izrada grafova zahtjevan posao koji znatno može opteretiti sustav, najbolje rješenje je podatke prenositi na centralni poslužitelj na kojem će se podaci i prikazivati

Nadzor operacijskog sustava Orca (10)



Nadzor operacijskog sustava
Orca – Preporučeno štivo

- http://www.orcaware.com/orca/

Nadzor operacijskog sustava
Orca – Zaključak

- Sustav za sveobuhvatan nadzor sustava koji nam pruža izuzetno mnogo informacija o stanju sustava
- Jedinstven alat,
- Nije lagano proširljiv, ali
- Se preporuča za nadzor svakog poslužitelja

Nadzor operacijskog sustava
Ganglia – Uvod (1)

- Ganglia je distribuirani sustav za nadzor grida, klastera ili bilo koje skupine poslužitelja. Pisana je u Javi i sastoji se od tri komponente:
  - Gmond – lokalni sustav za nadzor
  - Gmeta – globalni sustav
  - Mrežno sučelje (Web Front End)

Nadzor operacijskog sustava
Ganglia - Uvod (2)

- Za crtanje grafova Ganglia također rabi RRDTool.
- Nema ugrađen sustav za odašiljanje obavijesti.
- Podatke o sustavu crpe iz /proc file sistema.
- Unaprijed je definiran pristojan broj veličina koje se mjere, no veličine koje su zadane se lako dadu nadopuniti novima kroz alat gmetric.

Nadzor operacijskog sustava
Ganglia – Gmond

- Gmond radi na svakom pojedinom čvoru klastera gdje prihvaća podatke o susjednim čvorovima kroz multicast protokol.
- Zahvaljujući takvom konceptu, vrlo je lagano uključiti nove čvorove u sustav nadzora (automatika)
- Po zahtjevu, Gmond predaje podatke centralnom nadzornom sustavu, a to je Gmeta.
- Gmeta pak sakuplja podatke sa čvorova, obrađuje ih i prikazuje.

Nadzor operacijskog sustava
Ganglia – Gmetad

- Ganglia Meta Daemon (gmetad) sakuplja podatke o nadzoru s više gmond ili gmetad izvora, te
- sprema informacije u RRD formatu i eksportira XML, koji je spoj svih izvora podataka

Nadzor operacijskog sustava
Ganglia – Multicast

- **Multicast tehnologija** je najučinkovitiji način isporuke datoteka ili toka podataka (data stream) s jednog poslužitelja na više klijenata. Multicast štedi poslužiteljske resurse i mrežnu propusnost, ali nije u širokoj uporabi zbog nekoliko razloga:
  - Prije svega, svi mrežni uređaji na putu od poslužitelja do klijenata moraju podržavati multicast
  - IP multicast standard je baziran na UDP protokolu, što znači da nije prikladan za sustave gdje je važna visoka pouzdanost
- Multicast se najčešće rabi u zatvorenim mrežama

Nadzor operacijskog sustava
Ganglia – Instalacija (1)

- Instalacija

```
% wget
  http://nchc.dl.sourceforge.net
  /sourceforge/ganglia/ganglia-
  3.0.1.tar.gz
% gunzip -c ganglia-3.0.1.tar.gz
  | tar xvf -
% cd ganglia
```

Nadzor operacijskog sustava
Ganglia – Instalacija (2)

- Ako na istom poslužitelju želite instalirati i gmetad, obavezno morate instalirati i RRDTool s pripadajućim bibliotekama te pri kompajliranju napraviti:

```
% ./configure --with-gmetad
```

Inače je dovoljno:

```
% ./configure  && make && make
  install
```

Nadzor operacijskog sustava
Ganglia – Instalacija (3)

- Debian:

```
% apt-get install ganglia-
   monitor
% apt-get install gmetad
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (1)

- Glavna konfiguracijska datoteka je `/etc/gmond.conf`.
- U njoj se određuju opće postavke, opis klastera koji se nadziru, definicija kanala na koji se šalje multikast, i metrika
- Opće postavke određuju ponašanje gmond-a. Npr. Da li se on pokreće kao daemon, pod kojim korisnikom se pokreće, s kojom razinom debugging informacija,

Nadzor operacijskog sustava
Ganglia – Konfiguracija (2)

```
globals {
  mute = "no"
/* Hoće li gmond slati informacije susjednim
   čvorovima? */
  deaf = "no"
/* Hoće li gmond primati informacije o
   susjednim čvorovima? *
  debug_level = "0"
  host_dmax = "0"
/* Hoće li gmond brisati info o hostu ako se
   on ne javlja - 0 = NE*/
}
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (3)

- Opis atributa klastera koji se nadzire:

```
cluster {
  name = "intranet"
  owner = "SRCE"
  latlong = "N45.82 E16.03"
  url="unspecified"
}
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (4)

Definicija kanala na koji se šalje multikast:

```
udp_send_channel {
/*mcast_join = "239.2.11.71" */
  host = mokos.srce.hr
/* Ako se definira host i port     */
  port = "8649"
/* gmond salje unikast poruke na */
/*  ttl="1" */
}
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (5)

Definicija kanala na koji se prima multikast:

```
udp_recv_channel {
/*  mcast_join = "239.2.11.71" */
  port = "8649"
/*  bind = "239.2.11.71" */
}
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (6)

Definicija kanala na koji se eksportira xml:

```
tcp_accept_channel {
  port = "8649"
}
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (7)

Skupi CPU svakih 20s, :

```
collection_group {
  collect_every = 20
  time_threshold = 90
metric {
    name = "cpu_user"
    value_threshold = "1.0"
  }
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (8)

Nastavak:

```
 metric {
    name = "cpu_system"
    value_threshold = "1.0"
  }
 metric {
    name = "cpu_idle"
    value_threshold = "5.0"
  }  }
```

Nadzor operacijskog sustava
Ganglia – Konfiguracija (9)

- Konfiguracijska datoteka gmetad je /etc/gmetad.conf

```
data_source "intranet" localhost
# Where gmetad stores its round-
   robin databases
#default:"/var/lib/ganglia/rrds"
#rrd_rootdir "/some/other/place"
```

Nadzor operacijskog sustava
Ganglia – Web Front End (1)

- Skup PHP skripti koje se smještaju na standardno ili neko posebno mjesto na webu
- Nalazi se u standardnoj distribuciji Ganglie
- Instalacija:

```
% cp ~/ganglia-3.X.X/web /var/www/ganglia
```

- Konfiguracija se radi kroz skriptu **conf.php**.

```
/var/www/ganglia/conf.php
```

Nadzor operacijskog sustava
Ganglia – Web Front End (2)

Primjer konfiguracije weba:

```
$gmetad_root =
   "/var/lib/ganglia";
$rrds = "$gmetad_root/rrds";
$ganglia_ip = "127.0.0.1";
$ganglia_port = 8652;
$cpu_user_color = "3333bb";
$cpu_nice_color = "ffea00";
```

Nadzor operacijskog sustava
Ganglia – Web Front End (3)

Nadzor operacijskog sustava
Ganglia – Gmetric (1)

- Aplikacija za proširivanje vrijednosti koje se nadziru.
- Npr. nredba:

```
gmetric --name temperature --value
    `cputemp` --type int16 --units
    Celcius
```

obznanjuje svim gmon daemonima koji slušaju na multicast kanalu vrijednost metrike **cputmp**.

Nadzor operacijskog sustava
Ganglia – Gmetric (2)

- Skripta za nadzor temperature kroz lm-sensors i gangliu – /usr/sbin/getcputmp.pl

```
#!/usr/bin/perl –w
use strict;
my $interface="lo";
my $sensors="/usr/local/bin/sensors";
my $gmetric="/usr/bin/gmetric";
my @temps = split "\n", `$sensors | grep emp | cut -b 13-16`;
my $count=0;
my $temp;
```

Nadzor operacijskog sustava
Ganglia – Gmetric (3)

```
foreach $temp (@temps){
 `$gmetric -i $interface -t float -n "cpu$count\_temp" -u "C" –v
$temp`;
  $count++;
}
$count=0;
my @fans=split "\n", `$sensors |grep Fan |cut -b 10-15`;
foreach my $fan(@fans){
  `$gmetric -i $interface -t float -n "fan$count\_Speed" -u "C" –v
$fan`;
  $count++}
```

Nadzor operacijskog sustava
Ganglia – Gmetric (4)

- Tipično, vrijednost bi dohvaćamo kroz skriptu koja se izvršava iz cron-a, a onda ovakvom naredbom vrijednost obznanjujemo svim hostovima u klasteru:

```
*/2 * * * * root /usr/sbin/getcputmp.pl \
>> /var/log/gmetric-lmsensors/gmetric-\
   lmsensors.log 2>&1
```

Nadzor operacijskog sustava
Ganglia – Preporučeno štivo

http://ganglia.sourceforge.net/

http://www.gridpp.rl.ac.uk/viewcvs/viewcvs.cgi/ganglia/gmetric-lmsensors/

http://www.irvined.co.uk/ganglia.shtml

Nadzor operacijskog sustava
Ganglia – Zaključak

- Izuzetan alat za nadzor velikog broja poslužitelja
- Pojeduje elegantan način za proširivanje vrijednosti koje se nadziru
- Zanimljiv jer je dostupan i za Windows platformu
- No ozbiljan nedostatak mu je to što nema ugrađene mehanizme za obavještavanje

NADZOR LINUX/UNIX POSLUŽITELJA - Zaključak (1)

- Postoji velik broj alata za nadzor, različitih mogućnosti i namjena
- Kroz ovu prezentaciju prikazali su najistaknutije predstavnike alata iz pojedinih područja – nadzor sklopovlja, nadzor logova, nadzor integriteta sistemskih datoteka, nadzor servisa, nadzor operacijskog sustava

NADZOR LINUX/UNIX POSLUŽITELJA - Zaključak (2)

- Na nama je da zavisno od potreba izaberemo prave alate
- Neki od njih su, prije svega alati za nadzor logova i IDS neizbježni i jedinstveni (AIDE, Logcheck, itd.)

Pitanja

?