# 22. Turvaserveri monitooring

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 22. Turvaserveri monitooring
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.38

# Sisukord

# 22.1. Sissejuhatus

Selles õppetükis antakse ülevaade erinevatest võimalustest turvaserveri monitooringuks. Selle õppetüki läbimisel oskad turvaserveri monitoorimiseks kasutada käske „top“, „uptime“, „ps“, „free“, „df", „iostat“, „mpstat“, „netstat“, „iptrad“ ja „iftop“. Samuti tead, millal kasutada rakendusepõhiseid monitooringu tööriistu ja kuidas konfigureerida turvaserver kahe tööriista – Cacti ja Nagios – jaoks.

Õppetüki läbimiseks kulub aega umbes 30 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

X-TEE

Riigi Infosüsteemi Amet

# 22.2. Turvaserveri monitooringu vajadus

Teenuse kvaliteedi määrab muuhulgas nende kättesaadavus. Selleks, et teenused oleksid alati kättesaadavad, peab teenust osutavatel turvaserveritel olema piisavalt vabu ressursse.

Näiteks riiklikud infosüsteemid peavad järgima infosüsteemide kolmeastmelise etalonturbe (ISKE) süsteemi, mis määrab muuhulgas ka käideldavuse nõuded. ISKE neli taset käideldavuse kategoorias on:

- K0 – käideldavus väiksem kui 80% aastas, maksimaalne lubatud ühekordse katkestuse pikkus teenuse tööajal rohkem kui 24 tundi,
- K1 – käideldavus 80%-99% aastas, maksimaalne lubatud ühekordse katkestuse pikkus teenuse tööajal 4-24 tundi,
- K2 – käideldavus 99%-99,9% aastas, maksimaalne lubatud ühekordse katkestuse pikkus teenuse tööajal 1-4 tundi,
- K3 – käideldavus vähemalt 99,9% aastas, maksimaalne lubatud ühekordse katkestuse pikkus teenuse tööajal kuni 1 tund.

Käideldavusnõuded ja reageerimisajad on tavaliselt defineeritud teenustaseme lepingus (*Service Level Agreement, SLA*). Neid nõudeid defineerib üldjuhul äripool, kellelt sellist informatsiooni peaks ka küsima.

Teenuste toimimise tagamiseks vastavalt ISKE käideldavusastmele või teenustaseme lepingule on parim viis rakendada monitooringut. Sedasi saab olla kursis võimalike tõrgetega ja neile vajaliku kiirusega reageerida.

# 22.3. Turvaserveri monitooringu käsud

Järgmisena käsitletakse selles õppetükis turvaserveri monitooringuks kasutatavaid käske:

- „top“,
- „uptime“,
- „ps“,
- „free“,
- „df“,
- „iostat“,
- „mpstat“,
- „netstat“,
- „iptraf“ ja
- „iftop“.

# 22.4. Käsk „top“

Käsk „top“ on protsessitegevuse käsk.

Programm „top“ annab töötava süsteemi dünaamilise reaalajas vaate. See võib kuvada süsteemi koondteabe ning samuti protsesside või lõimede loendi, mida praegu haldab Linuxi tuum.

Kasutaja saab konfigureerida kuvatud süsteemi koondteabe tüüpe ja protsesside jaoks kuvatud teabe tüüpe, järjekorda ja mahtu ja selle konfiguratsioon saab muuta püsivaks kõigi taaskäivituste korral.

```
top - 10:17:27 up  2:39,  1 user,  load average: 0.00, 0.01, 0.05
Tasks: 166 total,   2 running, 164 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.3 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   2049104 total,  1595732 used,   453372 free,    69340 buffers
KiB Swap:  2095100 total,        0 used,  2095100 free.   375264 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1093 xroad     20   0 2091008 186356  30956 S  0.7  9.1   1:35.16 java
 1095 xroad     20   0 2242312 235192  31712 S  0.7 11.5   0:46.01 java
 1086 xroad     20   0 2266496 406224  32604 S  0.3 19.8   3:52.63 java
 1090 xroad     20   0 2102580 192612  31548 S  0.3  9.4   1:21.33 java
    1 root     20   0   33504   3924   2600 S  0.0  0.2   0:01.35 init
    2 root     20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root     20   0       0      0      0 S  0.0  0.0   0:00.02 ksoftirqd/0
    5 root      0 -20       0      0      0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root     20   0       0      0      0 S  0.0  0.0   0:00.34 rcu_sched
    8 root     20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_bh
    9 root     20   0       0      0      0 R  0.0  0.0   0:00.31 rcuos/0
   10 root     20   0       0      0      0 S  0.0  0.0   0:00.00 rcuob/0
   11 root     rt   0       0      0      0 S  0.0  0.0   0:00.00 migration/0
```

Käsk „top“ annab hea ülevaate serveri töövõimeajast, 1, 5 ja 15 minuti süsteemikoormuse keskmisest ja mälu ja CPU kasutusest üldiselt ja samuti ka iga üksiku protsessi kohta.

Käsk „top“ annab mitmeid kasulikke kiirklahve:

| | |
|---|---|
| t | Lülitab koondteabe sisse ja välja. |
| m | Lülitab mäluteabe sisse ja välja. |
| A | Sordib kuva eri süsteemiressursside tipptarbijate järgi<br>(kasulik süsteemi jõudlust vajavate ülesaanete tuvastamiseks). |
| f | Sisestab topi jaoks interaktiivse konfiguratsioonikuva<br>(kasulik „top“-i seadistamiseks konkreetse ülesande jaoks). |
| o | Võimaldab interaktiivselt valida topi sisese järjestamise. |
| 1 | Kuvab protsessori (CPU) koormuse. |
| k | Väljastab käsu “kill“. |

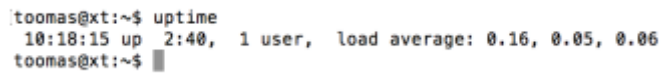
Rusikareegliks on see, et server ei tohiks saalida mälu ega koormus ei tohiks olla suurem kui 1 (1=100%) vastavalt saadaolevatele CPU-de mahule. Seega, kui sul on neli tuuma, ei tohi koormus olla suurem kui 4.

# 22.5. Käsk „uptime“

Käsku „uptime“ saab kasutada selleks, et vaadata, kui kaua server on töötanud.

Käsk aitab ka kontrollida:

- kellaaega,
- praegu sisselogitud kasutajate arvu ja
- keskmist süsteemikoormust viimase 1, 5 ja 15 minuti jooksul.



# 22.6. Käsk „ps“

Käsk „ps“ kuvab teavet aktiivsete protsesside valiku kohta.

Kõigi protsesside kuvamiseks kasuta käsku `ps -A`.

```
toomas@xt:~$ ps -A
  PID TTY          TIME CMD
    1 ?        00:00:01 init
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00 ksoftirqd/0
    5 ?        00:00:00 kworker/0:0H
    7 ?        00:00:00 rcu_sched
    8 ?        00:00:00 rcu_bh
    9 ?        00:00:00 rcuos/0
   10 ?        00:00:00 rcuob/0
   11 ?        00:00:00 migration/0
   12 ?        00:00:00 watchdog/0
   13 ?        00:00:00 khelper
   14 ?        00:00:00 kdevtmpfs
   15 ?        00:00:00 netns
   16 ?        00:00:00 perf
   17 ?        00:00:00 khungtaskd
   18 ?        00:00:00 writeback
```

Protsessipuu kuvamiseks kasuta käsku `ps axjf`.

```
    1  1086  1086  1086 ?           -1 Ssl    107   3:55 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -Djruby.co
    1  1088  1088  1088 ?           -1 Ss       0   0:00 /usr/sbin/sshd -D
 1088  2749  2749  2749 ?           -1 Ss       0   0:00  \_ sshd: toomas [priv]
 2749  2819  2749  2749 ?           -1 S     1000   0:00      \_ sshd: toomas@pts/0
 2819  2820  2820  2820 pts/0     2871 Ss    1000   0:00          \_ -bash
 2820  2871  2871  2820 pts/0     2871 R+    1000   0:00              \_ ps axjf
    1  1090  1090  1090 ?           -1 Ssl    107   1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlogback.co
    1  1091  1091  1091 ?           -1 Ssl    107   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlogback.co
    1  1093  1093  1093 ?           -1 Ssl    107   1:36 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlogback.co
    1  1094  1094  1094 ?           -1 Ss       0   0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
    1  1095  1095  1095 ?           -1 Ssl    107   0:46 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSize=70m -D
    1  1096  1096  1096 ?           -1 Ss       1   0:00 atd
    1  1097  1097  1097 ?           -1 Ss       0   0:00 cron
    1  1220  1217  1217 ?           -1 S      105   0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=/etc/pos
 1220  1222  1222  1222 ?           -1 Ss     105   0:00  \_ postgres: checkpointer process
 1220  1223  1223  1223 ?           -1 Ss     105   0:00  \_ postgres: writer process
 1220  1224  1224  1224 ?           -1 Ss     105   0:00  \_ postgres: wal writer process
 1220  1225  1225  1225 ?           -1 Ss     105   0:00  \_ postgres: autovacuum launcher process
 1220  1226  1226  1226 ?           -1 Ss     105   0:00  \_ postgres: stats collector process
 1220  2537  2537  2537 ?           -1 Ss     105   0:00  \_ postgres: serverconf serverconf 127.0.0.1(39750) idle
 1220  2539  2539  2539 ?           -1 Ss     105   0:00  \_ postgres: serverconf serverconf 127.0.0.1(39762) idle
 1220  2585  2585  2585 ?           -1 Ss     105   0:00  \_ postgres: serverconf serverconf 127.0.0.1(40112) idle
```

Kõigi käitamisvalikutega protsesside kuvamiseks kasuta käsku `ps auxw`.

```
root      1088  0.0  0.2  61380  5588 ?        Ss   07:38   0:00 /usr/sbin/sshd -D
xroad     1090  0.8  9.3 2102580 192092 ?      Ssl  07:38   1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
xroad     1091  0.1  6.0 2058060 124952 ?      Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
xroad     1093  0.9  9.1 2091008 186640 ?      Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlo
root      1094  0.0  0.0   4372  1560 ?        Ss   07:38   0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
xroad     1095  0.4 11.4 2242312 235232 ?      Ssl  07:38   0:47 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
daemon    1096  0.0  0.0  19140   160 ?        Ss   07:38   0:00 atd
root      1097  0.0  0.1  23656  2144 ?        Ss   07:38   0:00 cron
postgres  1220  0.0  1.0 247784 21076 ?        S    07:38   0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=
postgres  1222  0.0  0.2 247920  5516 ?        Ss   07:38   0:00 postgres: checkpointer process
postgres  1223  0.0  0.2 247784  4700 ?        Ss   07:38   0:00 postgres: writer process
postgres  1224  0.0  0.1 247784  3268 ?        Ss   07:38   0:00 postgres: wal writer process
postgres  1225  0.0  0.3 248644  6156 ?        Ss   07:38   0:00 postgres: autovacuum launcher process
postgres  1226  0.0  0.1 103596  3600 ?        Ss   07:38   0:00 postgres: stats collector process
ntp       1554  0.0  0.2  31452  4416 ?        Ss   07:38   0:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 106:114
root      1614  0.0  0.0  15820  2008 tty1     Ss+  07:39   0:00 /sbin/getty -8 38400 tty1
root      1940  0.0  0.0      0     0 ?        S    08:17   0:00 [kauditd]
postgres  2537  0.0  0.6 250344 12296 ?        Ss   09:46   0:00 postgres: serverconf serverconf 127.0.0.1(39750) idle
postgres  2539  0.0  0.5 249324 11972 ?        Ss   09:47   0:00 postgres: serverconf serverconf 127.0.0.1(39762) idle
postgres  2585  0.0  0.5 250328 12264 ?        Ss   09:54   0:00 postgres: serverconf serverconf 127.0.0.1(40112) idle
postgres  2588  0.0  0.5 249324 11972 ?        Ss   09:54   0:00 postgres: serverconf serverconf 127.0.0.1(40138) idle
postgres  2633  0.0  0.6 250344 12376 ?        Ss   10:01   0:00 postgres: serverconf serverconf 127.0.0.1(40490) idle
```

Esimese 10 protsessi kuvamiseks mälutarbimise põhjal kasuta järgmist käsku.

```
ps -auxf | sort -nr -k 4 | head -10
```

```
toomas@xt:~$ ps -auxf | sort -nr -k 4 | head -10
xroad     1086  2.4 19.8 2266496 406144 ?      Ssl  07:38   3:56 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -D
jruby.compile.mode=OFF -Djetty.admin.port=8083 -Djetty.public.port=8084 -Daddon.extraClasspath= -Dlogback.configurationFile=/etc/xroad/conf.d/jetty-l
ogback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/share/xroad/jetty9/start.jar org.eclipse.
jetty.start.Main jetty.home=/usr/share/xroad/jetty9
xroad     1095  0.4 11.4 2242312 235388 ?      Ssl  07:38   0:47 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
e=70m -Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml -Dxroad.proxy.clientHandlers=ee.ria.xroad.proxy.clientproxy.AsicContainerHandle
r,ee.ria.xroad.proxy.clientproxy.MetadataHandler -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/sha
re/xroad/jlib/proxy.jar:/usr/share/xroad/jlib/addon/proxy/messagelog-1.0.jar:/usr/share/xroad/jlib/addon/proxy/metaservice-1.0.jar -Dxroad.proxy.mess
ageLogManagerImpl=ee.ria.xroad.proxy.messagelog.LogManager -Dxroad.proxy.serverServiceHandlers=ee.ria.xroad.proxy.serverproxy.MetadataServiceHandlerI
mpl -Dxroad.monitoringagent.uri=akka.tcp://XRoadProxyMonitorAgent@127.0.0.1:2554/user/ProxyMonitorAgent ee.ria.xroad.proxy.ProxyMain
xroad     1090  0.8  9.3 2102580 192092 ?      Ssl  07:38   1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/addons/proxy-monitor-agent-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/u
sr/share/xroad/lib/ -cp /usr/share/xroad/jlib/monitoring-proxy-agent.jar ee.ria.xroad.proxymonitoragent.Main
xroad     1093  0.9  9.1 2091008 186644 ?      Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlo
gback.configurationFile=/etc/xroad/conf.d/signer-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/
-cp /usr/share/xroad/jlib/signer.jar ee.ria.xroad.signer.SignerMain
xroad     1091  0.1  6.0 2058060 124952 ?      Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/confclient-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/l
ib/ -cp /usr/share/xroad/jlib/configuration-client.jar ee.ria.xroad.common.conf.globalconf.ConfigurationClientMain
postgres  1220  0.0  1.0 247784 21076 ?        S    07:38   0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=
/etc/postgresql/9.3/main/postgresql.conf
postgres  2689  0.0  0.8 255452 16744 ?        Ss   10:09   0:00  \_ postgres: serverconf serverconf 127.0.0.1(40914) idle

postgres  2839  0.0  0.6 250192 12436 ?        Ss   10:16   0:00  \_ postgres: serverconf serverconf 127.0.0.1(41362) idle

postgres  2633  0.0  0.6 250344 12376 ?        Ss   10:01   0:00  \_ postgres: serverconf serverconf 127.0.0.1(40490) idle

postgres  2537  0.0  0.6 250344 12296 ?        Ss   09:46   0:00  \_ postgres: serverconf serverconf 127.0.0.1(39750) idle

toomas@xt:~$
```

Esimese 10 protsessi kuvamiseks CPU-tarbimise põhjal kasuta järgmist käsku.

```
ps -auxf | sort -nr -k 3 | head -10
```

```
toomas@xt:~$ ps -auxf | sort -nr -k 3 | head -10
xroad     1086  2.4 19.8 2266496 406240 ?      Ssl  07:38   3:57 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -D
jruby.compile.mode=OFF -Djetty.admin.port=8083 -Djetty.public.port=8084 -Daddon.extraClasspath= -Dlogback.configurationFile=/etc/xroad/conf.d/jetty-l
ogback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/share/xroad/jetty9/start.jar org.eclipse.
jetty.start.Main jetty.home=/usr/share/xroad/jetty9
xroad     1093  0.9  9.1 2091008 186636 ?      Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlo
gback.configurationFile=/etc/xroad/conf.d/signer-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/
-cp /usr/share/xroad/jlib/signer.jar ee.ria.xroad.signer.SignerMain
xroad     1090  0.8  9.3 2102580 192220 ?      Ssl  07:38   1:23 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/addons/proxy-monitor-agent-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/u
sr/share/xroad/lib/ -cp /usr/share/xroad/jlib/monitoring-proxy-agent.jar ee.ria.xroad.proxymonitoragent.Main
xroad     1095  0.4 11.6 2242312 238388 ?      Ssl  07:38   0:48 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
e=70m -Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml -Dxroad.proxy.clientHandlers=ee.ria.xroad.proxy.clientproxy.AsicContainerHandle
r,ee.ria.xroad.proxy.clientproxy.MetadataHandler -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/sha
re/xroad/jlib/proxy.jar:/usr/share/xroad/jlib/addon/proxy/messagelog-1.0.jar:/usr/share/xroad/jlib/addon/proxy/metaservice-1.0.jar -Dxroad.proxy.mess
ageLogManagerImpl=ee.ria.xroad.proxy.messagelog.LogManager -Dxroad.proxy.serverServiceHandlers=ee.ria.xroad.proxy.serverproxy.MetadataServiceHandlerI
mpl -Dxroad.monitoringagent.uri=akka.tcp://XRoadProxyMonitorAgent@127.0.0.1:2554/user/ProxyMonitorAgent ee.ria.xroad.proxy.ProxyMain
xroad     1091  0.1  6.0 2058060 124952 ?      Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/confclient-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/l
ib/ -cp /usr/share/xroad/jlib/configuration-client.jar ee.ria.xroad.common.conf.globalconf.ConfigurationClientMain
www-data   934  0.0  0.2  42372  5496 ?        S    07:38   0:00  \_ nginx: worker process
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
toomas    2899  0.0  0.0   7216  1756 pts/0    S+   10:22   0:00              \_ head -10
toomas    2898  0.0  0.0  15720  1972 pts/0    S+   10:22   0:00              \_ sort -nr -k 3
toomas    2897  0.0  0.1  18608  2724 pts/0    R+   10:22   0:00              \_ ps -auxf
toomas@xt:~$
```

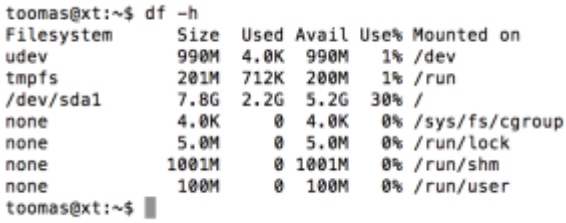
# 22.7. Käsk „free“

Käsk „free“ kuvab vaba ja kasutatud füüsilise ja swap-mälu kogumahtu süsteemis ning samuti tuuma poolt kasutatud puhvreid.

# 22.8. Käsk „df“

Käsk „df“ annab teavet failisüsteemi kettaruumi kasutuse kohta.

Inimloetava teabe kuvamiseks kasuta käsku `df -h`.



# 22.9. Käsk „iostat“

Käsk „iostat“ annab teavet seadmete ja sektsioonide CPU statistika ja sisendi/väljundi statistika kohta.

Käsku „iostat“ kasutatakse süsteeemi sisend-/väljundseadme koormuse monitoorimiseks. Selleks jälgitakse aega, mille jooksul seadmed on aktiivsed võrreldes nende tavalise edastuskiirusega. Käsk „iostat“ genereerib aruandeid, mida saab kasutada süsteemikonfiguratsiooni muutmiseks, et paremini tasakaalustada sisend-/väljundkoormust füüsiliste ketaste vahel.

```
toomas@xt:~$ iostat
Linux 4.2.0-27-generic (xt)     07/22/2016      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           4.02    0.00    0.46    0.10    0.00   95.42

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               3.88        49.09        38.62     488091     384016
scd0              0.00         0.00         0.00         44          0

toomas@xt:~$
```

See käsk aitab ka tuvastada, kas salvestusruum on kitsaskohaks mõned konkreetses serveris. See kuvab ketta jaoks laiendatud statistika kolm aruannet viiesekundiliste vahemikega.

```
toomas@xt:~$ iostat -d -x 5 3
Linux 4.2.0-27-generic (xt)     07/22/2016      _x86_64_        (1 CPU)

Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await w_await  svctm  %util
sda               0.42     3.47    1.38    2.50    48.83    38.55    45.08     0.02    5.25   14.41    0.20   0.43   0.17
scd0              0.00     0.00    0.00    0.00     0.00     0.00     8.00     0.00    5.09    5.09    0.00   5.09   0.00

Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await w_await  svctm  %util
sda               0.00     0.20    0.00    0.40     0.00     2.42    12.00     0.00    0.00    0.00    0.00   0.00   0.00
scd0              0.00     0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00    0.00    0.00   0.00   0.00

Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await w_await  svctm  %util
sda               0.00    13.16    0.00    3.85     0.00    68.02    35.37     0.00    0.00    0.00    0.00   0.00   0.00
scd0              0.00     0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00    0.00    0.00   0.00   0.00

toomas@xt:~$
```

Kõige olulise on see, et jälgiksite järgnevat.

- **svctm**: keskimine teenuseaeg (millisekundites) seadme jaoks väljastatud sisend-/väljundtaotluste jaoks,
- **%util**: CPU-aja protsent, mille jooksul seadmesse väljastati sisend-/väljuntaotlused (ribalaiuse kasutus seadme jaoks). Seadme küllastus ilmneb siis, kui väärtus läheneb sajale protsendile.

Kui need numbrid on kõrged, pead tegustema hakkama.

# 22.10. Käsk „mpstat“

Käsk „mpstat“ annab teavet protsessidega seotud statistika kohta.

Käsk „mpstat“ kirjtuab tavalised väljundtegevused iga saadaoleva protsessori jaoks. Esimene protsessor on 0. Teatatakse ka keskmistest globaalsetest tegevustest protsessori kohta.

```
toomas@xt:~$ mpstat -P ALL
Linux 4.2.0-27-generic (xt)     07/22/2016      _x86_64_        (1 CPU)

10:26:55 AM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
10:26:55 AM  all    4.01    0.00    0.42    0.10    0.00    0.04    0.00    0.00    0.00   95.44
10:26:55 AM    0    4.01    0.00    0.42    0.10    0.00    0.04    0.00    0.00    0.00   95.44
toomas@xt:~$
```

# 22.11. Käsk „netstat“

Käsk „netstat“ prindib võrguühendused, marsruutimistabelid, liidesestatistika, maskeraadühendused ja multisaate liikmesuse.

Kõigi võrguühenduste kuvamiseks saad kasutada käsku `netstat -a`. Numbriliste aadresside kuvamiseks selle asemel, et proovida määratleda sümboolset hosti ja porti, kasuta käsku `netstat -an`. Kuulamisportide linkimiseks ka programmidega saad kasutada käsku `netstat -anp`.

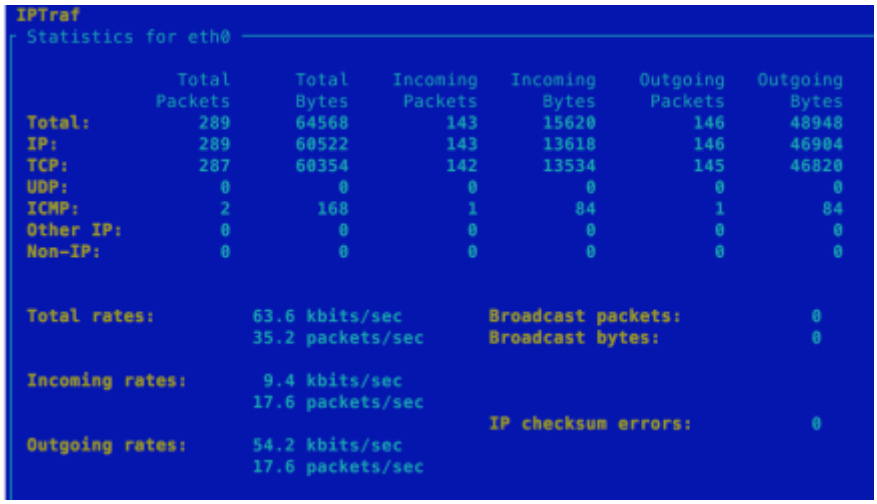
```
toomas@xt:~$ netstat -anp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4000            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41108         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40490         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41750         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40138         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41728         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40112         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41362         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40542         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40546         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40502         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40548         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40936         ESTABLISHED -
tcp        0      0 195.222.5.8:22          195.222.5.1:36574       ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40544         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41112         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:41114         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40540         ESTABLISHED -
```

# 22.12. Käsk „iptraf“

„iptraf“ on ncurses-põhine IP LAN monitor, mis genereerib erinevaid võrgustatistikaid (sh TCP teabe, UDP arvud, ICMP teabe, Etherneti koormusteabe, sõlmestatistika, IP kontrollsumma vead jm).

„ipftaf“ saab anda järgmist teavet hõlpsalt loetavas vormingus:

- võrguliikluse statistika TCP-ühenduse järgi,
- IP liikluse statistika võrguliidese järgi,
- võrguliikluse statistika protokolli järgi,
- võrguliikluse statistika TCP/UDP pordi ja paketi suuruse järgi,
- võrguliikluse statistika Layer2 aadressi järgi.

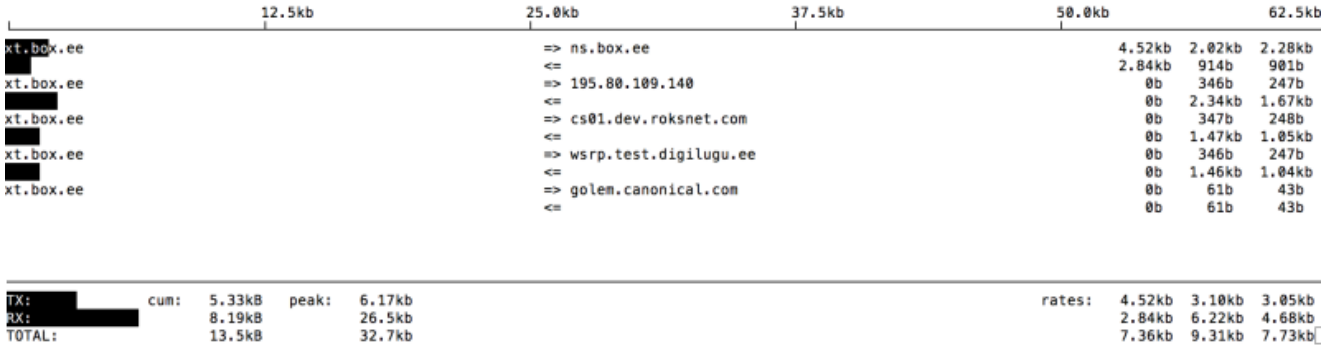


# 22.13. Käsk „iftop“

Käsk „iftop“ kuvab ribalaiuse reaalajas kasutuse liideses hosti järgi.

Käsk „iftop“ kuulab võrguliiklust nimetatud liideses või esimeses liideses, mille ta leiab ja mis näeb välja nagu väline liides, kui midagi pole määratud ja kuvab praeguse ribalaiuse kasutuse tabeli hostide paaride järgi.

Käsku „iftop“ peab käitama piisavate õigustega, et monitoorida liidese kogu võrguliiklust.



# 22.14. Monitooringurakendused

Loetletud tööriistad aitavad sul monitoorida turvaserverit, kui oled sisse logitud. Pikemas perspektiivis on mõistlik kasutada rakendusi, mis koguvad teavet aja jooksul ja esitavad selle näiteks graafiliselt. See annab parema arusaamise sellest, kuidas süsteem suure koormuse korral töötab.

Usaldusväärsete tulemuste saamiseks tuleks monitooringurakendused installida eraldi serverisse. Näiteks ei saa võrgutõrgete teateid meili teel saata, kui võrk ise ei tööta.

Järgmisena tutvustatakse selles õppetükis järgmisi monitooringutööriistu.

- Cacti
- Nagios

# 22.15. Cacti ja Nagios


Cacti on täielik võrgugraafika lahendus. See pakub kiireid pollimise, täiustatud diagrammimallide loomise, mitmeid andmete hankimismeetodite ja kasutajahaldusfunktsioonide valmislahendusi. See saab pakkuda andmeid võrgu, CPU, mälu, sisselogitud kasutajate, Apache'i, DNS-serverite ja palju muu kohta. See kõik on pakitud intuitiivsesse hõlpsalt kasutatavasse liidesesse.

Nagios on populaarne avatud lähtekoodiga arvutisüsteem ja võrgu monitooringu rakenduse tarkvara. See aitab monitoorida hoste, võrguseadmeid ja teenuseid. See saab saata teateid, kui midagi läheb valesti või muutub paremaks.

Monitooritavad süsteemiparameetrid/teenused:

- CPU koormus,
- mälu tarbimine.
- kettaruum,
- võrgu tarbitud ribalaius,
- X-tee teenuste teenusepordi saadavus,
- toimingute arv,
- Pingi latents,
- NTP aja sünkroniseerimine.

Lisateavet Cacti kohta leiate siit. Nagiose ametlik veebisait asub siin.

# 22.16. Turvaserveri konfigureerimine Cacti jaoks

X-tee turvaserveri konfigureerimiseks nii, et Cacti saaks seda monitoorida, on vajalikud järgmised toimingud.

Esmalt installige deemon `snmp`:

```
sudo apt-get install s
nmpd
```

Deemon `snmpd` peab olema konfigureeritud töötama Cactiga. Konfiguratsioonifaili asukoht: `/etc/snmp/snmpd.conf`. Veenduge, et redigeerite faili `snmpd.conf` ja mitte faili `snmp.conf`.

```
sudo nano /etc/snmp/sn
mpd.conf
```

Redigeerige „Agent Behavior“, mis peaks asuma faili ülaosas. Kommenteeri välja rida „ühendused ainult kohalikust süsteemist“ ja lisage rida konkreetse IP kuulamiseks olenevalt teie võrgu konfiguratsioonist.

```
# Kuula ainult kohalik
ust süsteemist pärit ü
hendusi
#agentAddress udp:127.
0.0.1:161
```

```
# Kuula konkreetse IP
 ühendusi
agentAddress udp:192.1
68.0.1:161
```

Järgmisena otsige üles jaotis Access Control Kommenteeri sisse ja redigeeri rida `rocommunity secret 10.0.0.0/16`. Muuda see viitekohaseks Cacti serveriks.

```
rocommunity secret <Ca
ctiServerIpAddress>
```

Kogukonna nimi võib olla erinev, kuid antud hosti lisamisel peab see Cacti serveri konfiguratsioonis olema sama.

Võimalik, et soovite redigeerida süsteemiteavet, mis seostatakse teie andmetega jaotises „System Information“. Saate lisada oma serveri füüsilise asukoha ja kontaktmeiliaadressi. See võib olla kasulik arvutite eristamiseks, kui monitoorid suurt hulka servereid.

```
sysLocation Teie süste
emi asukoht
sysContact contact@ema
il.com
```

Kui muudatused on tehtud, salvesta fail, välju ja taaskäivita teenus `snmpd`.

```
sudo service snmpd res
tart
```

# 22.17. Turvaserveri konfigureerimine Nagiose jaoks

X-tee turvaserveri konfigureerimiseks nii, et Nagios saaks seda monitoorida, on vajalikud järgmised toimingud.

Installi Nagiose kauglisandmooduli käiviti.

```
sudo apt install nagio
s-nrpe-server
```

See installib kogu nõutava tarkvara Nagiose kauglisandmooduli töötamiseks ning samuti käivitab deemoni pärast installimist.

Pärast installimist redigeeri Nagios NRPE konfiguratsioon:

```
sudo nano /etc/nagios/
nrpe.cfg
```

Muuda hosti kuulamise väärtusi tulenevalt oma võrgukonfiguratsioonist ja Nagiose monitooringuserverist. Kommenteeri sisse ja muuda järgmine IP:

```
#server_address=127.0.
0.1
```

Lisa Nagiose monitooringuserveri IP väärtuseks:

```
allowed_hosts=127.0.0.
1,<Nagios Monitoring s
erver IP>
```

# 22.18. Küsimus

**Selle õppetüki lõpetamiseks otsusta, milliseid käske all kirjeldatakse.**

A. Aruanded CPU statistika ja sisendi/väljundi statistika kohta seadmete ja sektsioonide jaoks
B. Protsessitegevuse käsk
C. Teavitab failisüsteemi kettaruumi kasutuse kohta
D. Saab kasutada selleks, et vaadata, kui kaua turvaserver on töötanud
E. Kuvab ribalaiuse reaalajas kasutuse liideses hosti järgi

Õigeid vastuseid vaata siit (avaneb uues aknas).