

MRTG – nem csak a hálózat figyelésére!

Az MRTG eredetileg egy hálózati forgalmat figyelő program, ami a hálózat terheltségének függvényében, png formátumban grafikonokat hoz létre.

Egyszerűségének köszönhetően bárminek a megfigyelésére használható, amit két számmal ki lehet fejezni. Az MTRG (Multi Router Traffic Grapher) első változatát *Tobias Oetiker* Perl nyelven írta meg, majd egyes részeit a jobb teljesítmény érdekében C-kóddal helyettesítette (2.0). Linux és Windows NT rendszereken egyaránt fut; a weblapon részletes lista található arról, hogy mely operációs rendszereken próbálták már ki. A GPL keretein belül szabadon használható. Aki csak pár hálózati kapcsolatot, illetve a processzorterheltséget szeretné figyelgetni, annak figyelmébe ajánlom *trey* nagyon jó, magyar nyelvű leírását a <http://www.szabilinux.hu/mrtg/> címen.

Telepítés

Az MRTG 2.9.17-es változatát próbáltam ki; Debian Woody GNU/Linux-rendszerre telepítettem, miként azt már megszokhattuk:

```
apt-get install mrtg
```

Más népszerű terjesztéseknek szintén része. Függőségként az `snmp`, illetve a PNG kezeléséhez szükséges könyvtárakat rak fel. Támogatja a SNMPv1-et és az SNMPv2-t, a cikk írása idején azonban az SNMPv3-at még nem.

Az SNMP (Simple Network Management Protokoll) lényege röviden összefoglalva az, hogy a hálózati eszközök és a nyomtatók kezelését leegyszerűsítse. Az SNMP-t alapvetően egyszerűre tervezték, teljes megvalósítása mégis 500–600 oldal terjedelmű. Az elgondolás lényege: léteznek ügynökök és felügyeleti állomások, amelyek kapcsolatot tartanak egymással. A felügyeleti állomás általában egy általános célú számítógép, ami az ügynökök állapotát tudja lekérdezni, illetve beállítani. Ha valakit részletesebben érdekel a téma, *Andrew S. Tanenbaum* Számítógéphálózatok című könyvét ajánlom. Annak ellenére, hogy az MRTG is tartalmaz SNMP-megvalósítást, érdemes feltenni az `snmpd`-t (`apt-get install snmpd`). Alapbeállításokkal biztonsági okokból nem használható, ezért hogy működésre bírjuk, nyissuk meg kedvenc szövegszerkesztőnkkel a beállítófájlját (Debian: `/etc/snmp/snmpd.conf`), és írjuk át a vonatkozó részt az 1. listának megfelelően. Alapértelmezett kapuja az UDP161, 162. Ha szükséges, engedélyezzük a tűzfalunkon.

Könnyen is lehet: a cfmaker

Telepítés után egy példa beállítófájl: `/etc/mrtg.cfg` található, amit alapértelmezés szerint ötperceként le is futtat (`/etc/cron.d/mrtg`). A következő paranccsal nagyon egyszerűen létrehozhatjuk a saját gépünkre szabott beállítófájl, aminek több hálózati kapcsolata is lehet:

```
cfmaker 127.0.0.1 --output /etc/mrtg.cfg
```

Bármelyik hálózati kártya IP-címét megadhatjuk, természetesen a `localhost`-ot is, ahogyan a példában látni lehet. Ezzel el is készült egy beállítófájl, ami minden hálózati csatoló

```
# sec.name source
community
#com2sec paranoid default public
com2sec readonly default public
#com2sec readwrite default private
```

```
#!/bin/sh
case "$1" in
  start)
    /usr/bin/mrtg /etc/mrtg.cfg --logging
    ↪ /var/log/mrtg.log
    ;;
  stop)
    kill `cat /etc/mrtg.cfg.pid`
    ;;
  *)
    echo "Usage: /etc/init.d/mrtg
    ↪ {start|stop}" >&2
    exit 1
    ;;
esac
exit 0
```

(interface) szükséges beállításait tartalmazza.

Az MRTG-t általában `cron`-ból érdemes futtatni, illetve következő paranccsal:

```
mrtg/etc/mrtg.cfg
```

Az utóbbi a kipróbálás során hasznos, hogy az eredmény létrehozását megsürgesse. Démonként is futtatható, csak be kell szúrnia következő sorokat a beállítófájlba:

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

Hogy rendszerinduláskor elinduljon, készítsünk egy a 2. listán láthatóhoz hasonló parancsfájl, és Debian esetén helyezzük a `/etc/init.d/` könyvtárba; majd egy közvetett hivatkozást (symlink) a `/etc/rc2.d/` könyvtárba, vagy más `rc*.d` könyvtárba – a kedvenc futási szintnek (runlevel) megfelelően. Ha démonként fut, jobb, ha mindezt nem rendszergazdaként teszi. Az alábbi kapcsolókkal állítható be, hogy milyen felhasználóként, illetve csoportként fusson:

```
--user=user_name and --group=group_name
```

Ha a beállítófájl megváltozott, a démon újra kell indítani, hogy észlelje a változásokat. Az alapértelmezett könyvtár, ahová az

```
#R0szlet az mrtg.cfg fajlb l

Target[smart]:
↳ '/etc/mrtg/scripts/smart.stat'
MaxBytes[smart]: 100
Options[smart]: gauge, nopercnt, transparent
Unscaled[smart]: dwym
XSize[ezwf]: 600
YSize[ezwf]: 200
YLegend[smart]: Number of test
↳ PreFailure/Advisory
ShortLegend[smart]: %
#LegendI[smart]: Threshold:
LegendO[smart]: Prefailure:
LegendI[smart]: Advisory:
Title[smart]: S.M.A.R.T test on
↳ coolczus.sysconfig.hu
PageTop[smart]: <H1>SMART usage on
↳ coolczus.sysconfig.hu</H1>
```

```
#!/usr/bin/perl
print " ".(int(`ide-smart /dev/hda | grep
↳ Prefailure | wc -l` / 30 * 100) . "\n");
print " ".(int(`ide-smart /dev/hda | grep
↳ Advisory | wc -l` / 30 * 100) . "\n");
print " ".(int(`ide-smart /dev/hda | grep
↳ Advisory | wc -l` / 30 * 100) . "\n");
print " ".(int(`ide-smart /dev/hda | grep
↳ Advisory | wc -l` / 30 * 100) . "\n");
$uptime = `usr/bin/uptime | sed 's/\ \ * /
↳ /g'`;
@uptime = split(/,/, $uptime);
@uptime = split(/up/, @uptime[0]);
$server = `bin/uname -n`;
printf "@uptime[1]\n";
printf $server;
```

elkészített weblapot rakja, a `/var/www/mrtg`, ami felülbíráható, ha a `cfm` programot a

```
--global "WorkDir: /home/mrtg/public_html"
```

beállításal indítjuk. Az elkészült fájlban a *System*, *Maintainer* stb. részek nyugodtan átírhatók. A `cfm` program sűgőoldalán ahhoz is elegendő tájékoztatást találunk, hogy saját beállítófájl-készítőt hozzunk létre.

Ha mindezzel megvagyunk, kell 5–10 perc, amíg az MRTG „bemelegszik”, és használható adatokkal lát el minket a hálózat forgalmáról. Ha a weblap egyszerűnek tűnik, tetszés szerint tovább alakítható: háttér, cím – mondhatni szinte minden megváltoztatható; vagy a kifejezetten MRTG-hez írt programmal, az `indexmaker`-rel is lehet próbálkozni. Mi mindent figyelhetünk MRTG segítségével? A cikk további részéből ez is kiderül.

Más lehetőségek

Mielőtt meg jobban belevetnénk magunkat, néhány szót ejtek a beállítófájl írásmódjáról. Minden kulcsszónak a sor elején kell kezdődnie. Az üres sorokat figyelmen kívül hagyja. A megjegy-

```
coolczus@COOLCZUS:~/ $
/mrtg/scripts/smart.stat
23
76
10 days
COOLCZUS
coolczus@COOLCZUS:~/ $
```

zés jele a kettős kereszt (#). Ha a kulcsszó utáni sor fehér karakterrel (TAB>>, SPACE) kezdődik, akkor azt az előző sor végéhez fűzi. Ez áttekinthetőbb beállításokat eredményez, ami akkor érdekes, ha a beállítófájlba HTML-kódot is írunk. Most nézzük végig a lehetőségeket! Miként a bevezetőben olvasható, mindenre alkalmas, ami két számmal vagy többel kifejezhető. A 3. listának megfelelően a *Target* részénél meg lehet adni egy programot (általában egy egyszerű héjprogramot vagy Perl-parancsfájlt lásd a 4. listát), ami a standard kimenetére az 5. listán látható formában írja ki az adatokat. Szögletes zárójelben egy tetszőleges nevet kell megadni, amire az adott beállítás vonatkozik. A példában a Perl-parancsfájl az `ide-smart` programkimenetet dolgozza fel (Debian esetén: `apt-get install ide-smart`), és a *Prefailure/Advisory* százalékos eloszlását számolja ki. További kulcsszavak a teljesség igénye nélkül: *MaxBytes*: – a beosztás legnagyobb értékét állítja be. *Options*: – néhány beállításnál eldönthetjük, engedélyezzük-e vagy sem. A *gauge*: az átadott értékeket megjeleníti a grafikonon. Alaphelyzetben a két érték különbségét veszi, és elosztja a köztük eltelt idővel; a *nopercnt*: százalékban kifejezve nem írja ki; *transparent*: az elkészített képnek átlátszó háttére lesz. *Unscaled*: megadható, hogy melyik grafikont rajzolja ki (d=day w=week m=month y=year), a példa szerint mind a négyet kirajzolja. Xsize, YSize: a grafikon méretét lehet megadni, pixelben. *Ylegend*: a mértékegység megadható, szavakban. A *Short-Legend[smart]*: előző szolgáltatás rövidítve. *Legend[1234IO]*: hatféle magyarázat az értékekhez. A többi beállítás és jelentése megtalálható a hivatalos weblapon. Például *XZoom*, *XScale*, *PageFoot*, *Options[]: nobanner, Background, Timezone* és még sok más is.

Összefoglalva

Az MRTG-t alapvetően a hálózati eszközökön folyó forgalom ellenőrzésére fejlesztették ki, amire bonyolult hálózatok esetén is tökéletesen megfelel. Csak a képzelet szabhat határt annak, hogy mit figyelünk meg.

Kolcza Péter

(kpeter@sysconfig.hu) imádja a South Parkot. A Miskolci Egyetem informatika szakos hallgatója. Elvakult GNU/Linux-rajongó. Ha egyetemi elfoglaltságai engedik, rendszeréptéssel foglalkozik. A cikkel kapcsolatban minden észrevételt szívesen fogad.

Kapcsolódó címek

- <http://www.snmp.com>
- <http://people.ethz.ch/~oetiker/webtools/mrtg/>
- <http://faq.mrtg.org/howto.html>
- <http://www.david-guerrero.com/papers/snmp/>
- <http://bodq.vstu.edu.ua/activity/>