

Grafische Trafficanalyse mit MRTG

Autor: Sebastian Wolfgarten, sebastian@wolfgarten.com

Homepage: <http://www.wolfgarten.com>

Erstellungsdatum: 23. Februar 2002, 16:29 Uhr

Einleitung:

Dieser Artikel zeigt die Installation und Konfiguration von Mrtg, dem sogenannten "Multi Router Traffic Grapher". Damit kann man die Auslastung von Netzwerkverbindungen grafisch darstellen und überwachen. Das Programm ist in Perl und C geschrieben und für viele Unix/Linux Plattformen verfügbar.

Inhalt:

Mit MRTG (www.mrtg.org) ist es möglich, die Trafficauslastung von Netzwerkverbindungen grafisch darzustellen und zu überwachen. Das Programm liest SNMP Werte aus den zu überwachenden Geräten aus und erzeugt daraus HTML-Dateien mit einer grafischen Darstellung des aktuellen Netzwerktraffics. Beispielauswertungen findet man u. a. auf <http://www.stat.ee.ethz.ch/mrtg/>.

Die Installation gestaltet sich etwas schwieriger und Anfänger sollten eventuell auf bereits vorkompilierte Pakete der jeweiligen Distribution zurückgreifen. Unter SuSE findet sich der SNMP Daemon sowie Mrtg in der Serie "n", unter Debian reicht ein einfaches "apt-get install snmpd mrtg".

Wer dennoch die Installation per Hand durchführen möchte, der braucht zunächst ein Unix/Linux System mit Perl Interpreter und einem C-Compiler (z.B. gcc). Diese Programme sind in den gängigen Distributionen bereits enthalten und eigentlich unabdingbar. Wir brauchen neben den Quellen von Mrtg und den Snmpd auch die Bibliotheken "zlib", "libpng" und "gdlb".

Unter <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pub/mrtg-2.9.17.tar.gz> finden wir die aktuelle Version von MRTG. Die Bibliothek Zlib unter <ftp://sunsite.cnlab-switch.ch/mirror/infozip/zlib/zlib.tar.gz>, LibPNG gibt's auf <http://www.libpng.org/pub/png/src/libpng-1.0.12.tar.gz> und die GDLib finden Sie unter <http://www.boutell.com/gd/http/gd-1.8.3.tar.gz>! Schließlich besorgen wir uns von <http://prdownloads.sourceforge.net/net-snmp/ucd-snmp-4.2.3.tar.gz> den SNMP Daemon.

Danach entpacken wir die Zlib durch Eingabe des Befehls "tar xvzf zlib.tar.gz" und konfigurieren diese mit dem Befehl ".configure --prefix=/usr/local". Die Übersetzung des Programms sowie die eigentliche Installation erfolgt durch den Befehl "make" sowie "make install". Die nächste Bibliothek LibPNG entpacken wir ebenso und kopieren durch Eingabe des Befehls "cp scripts/makefile.linux ../libpng-1.0.12/makefile" das linux-optimierte Makefile in das entsprechende Verzeichnis und beginnen mit "make" den Kompilierungsvorgang. Wir schließen die Installation wie immer durch Eingabe des Befehls "make install" ab. Nun entpacken wir die GDLib und übersetzen diese durch Eingabe des Befehls "make"

und "make install". Somit sind die benötigten Bibliotheken installiert und wir können mit der Installation von Mrtg und dem Snmp Daemon fortfahren.

Nachdem wir Mrtg entpackt haben, konfigurieren wir es durch Eingabe des Befehls "./configure", übersetzen es mit "make" und führen die Installation mit "make install" durch. Last but not least müssen wir noch den SNMP Daemon installieren, der die eigentlichen Datentransferwerte sammelt. Dazu entpacken wir die Software und konfigurieren diese mit "./configure --prefix=/usr/local". Die Kompilierung startet mit dem Befehl "make" und die Installation wird mit "make install" abgeschlossen. Danach müssen wir noch die Perlmodule für SNMP installieren. Dazu wechseln wir mit "cd perl/SNMP/" in das entsprechende Verzeichnis und führen die Befehle "perl Makefile.PL", "make", "make test" sowie "make install" aus, um diese zu installieren.

Die Installation ist nun abgeschlossen und wir können mit der nicht weniger aufwendigen Konfiguration beginnen. Zuerst erzeugen wir die Konfigurationsdatei des SNMP Daemon durch Eingabe von "touch /etc/snmpd.conf". Im Downloadbereich unserer Seite befindet sich ein Beispiel für diese Datei sowie Startskripte für den SNMPPD und den Mrtg. Durch Eingabe von "/usr/local/sbin/snmpd -c /etc/snmpd.conf" kann der SNMP Daemon gestartet werden und der Befehl "/usr/local/bin/snmpwalk localhost test" überprüft das Vorhandensein des SNMP Daemons.

Endlich können wir uns der Konfigurationsdatei von Mrtg widmen. Dazu erstellen wir diese durch Eingabe von "touch /etc/mrtg.conf". Im Internet gibt es eine u.a. auf <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/reference.html> eine gute Referenz der zahlreichen Konfigurationsoptionen. Eine Beispielkonfiguration gibt es im Downloadbereich unserer Seite. Starten kann man Mrtg durch Eingabe von "/usr/local/mrtg-2/bin/mrtg /etc/mrtg.conf", wobei beim ersten und zweiten Start durchaus kleinere Fehlermeldungen erscheinen können. Mrtg erzeugt dabei die Netzwerkstatistiken einmalig und beendet sich wieder. Will man eine dauerhafte Statistik haben, so muss man beispielsweise einen Eintrag in die /etc/crontab machen, der Mrtg alle 5 Minuten startet. Dieser könnte so aussehen:

```
/5 * * * * root /usr/local/mrtg-2/bin/mrtg /etc/mrtg.conf 2>&1 > /dev/null
```

Schließlich sollte man diese statistischen Werte sowie den Zugang zum SNMP Daemon durch entsprechende Schutzmaßnahmen (Firewall und Verzeichnisschutz) gegen unauthorisierte Zugriffe schützen. Startskripte für Mrtg und den Snmpd liegen im Downloadbereich bereit, mit detaillierten Installationsanweisungen. Das war's :-)