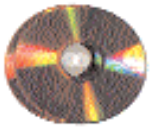
Naplófájl színezése



Gaelyne bemutatja, hogy az Apache httpd.conf fájljának megbűvölésével miként színezhetjük ki webes naplófájljainkat.

A weboldalak tárolásával foglalkozó cégeknek a legtöbbször életbevágóan fontos, hogy Apache-kiszolgálóik mit tesznek elérhetővé a világ számára, és ezt a lehető leggyorsabban szeretnék megtudni.

A rendszergazdának állandóan figyelnie kell a rendszer naplófájljait, ugyanígy a webes rendszergazdának is ellenőriznie kell a webes naplófájlokat. A valós idejű rendszerelemző programok nagy számát tekintve biztos voltam benne, hogy webes naplófájlok figyelésére több ilyen programot is találok majd. A ➲ http://freshmeat.net és más internetes lelőhelyek átbogarászása után megállapítottam, hogy igényeimet egyik program sem elégíti ki. Néhány ugyan éppen elérte a megfelelő színvonalat, a legtöbb azonban csak egy fájl figyelésére alkalmas; az a néhány pedig, amelyik több fájlt is elemez, olyan reménytelenül kezelhetetlen volt, hogy inkább más megoldás után néztem.

Végül nem programot használtam a feladatra, csupán végrehajtottam néhány módosítást az Apache httpd.conf fájljában. Az az ötletem támadt, hogy a gépekről származó adatokat egy „eldobható” naplófájlban összegyűjtöm, amit a `colortail` segítségével egy külső monitoron jelenítek meg. Így azonnal láthatom, melyik gép végez webes tevékenységet, honnan jön a forgalom, illetve éppen mely oldalakat hívják le. Sőt, ezáltal a parancsfájlokkal ügyeskedő srácokat és a nagy keresőmotorokat is megfelelően „kezelhetjük”. A rendszer olyan jól bevált, hogy később a rendszernaplózást is ennek használatával oldottuk meg.

A httpd.conf módosításai

Az általános naplózás formátuma (LogFormat) mellett egy „webmonitor” nevűt is létrehoztam:

1. lista A colortail.conf

```
# Az elérhető színek listája. Ezek bármelyikét
# használhatjuk, ha az alábbi formátumot betartjuk.
# COLOR magenta
# COLOR cyan
# COLOR green
# COLOR yellow
# COLOR brightred
# COLOR blue
# COLOR brightblue
# COLOR brightwhite

COLOR magenta
{
^.*(\[valami.com\]).*$
^.*(HEAD /).*$
}

COLOR cyan
{
^.*(\[masvalami.com.au\]).*$
^.*(GET /naplok/).*$
^.*(GET /konyvtar/).*$
^.*(GET /masikkonyvtar/).*$
}

COLOR brightyellow
{
# minden IP-címre illeszkedik
^.*([0-9]{3}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
^.*([0-9]{2}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
^.*([0-9]{1}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
# egy sorban két IP-címre illeszkedik
^.*([0-9]{3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]
➥{1,3}).*([0-9]{3}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
^.*([0-9]{2}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*([0-9]{2}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
^.*([0-9]{1}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*([0-9]{1}\.[0-9]{1,3}\.[0-9]{1,3}\.
➥[0-9]{1,3}).*$
}

COLOR brightred
{
# a root szóra illeszkedik
^.*(root).*$
# a DENY szóra illeszkedik
^.*(ppp-in DENY ppp0).*$
^.*(eth-in DENY eth0).*$
# Rendszernaplózás
^.*(authentication failure).*$
^.*(PAM_pwdb).*$
^.*(ftpd).*$
^.*(ssh).*$
^.*(ipop3d).*$
^.*(\[error\]).*$
^.*(LOGIN).*$
# CGI-BIN és PHP elemek
^.*(cgi-bin).*$
^.*(php).*$
^.*(php3).*$
}
```

2. lista A cron

```
#/bin/sh
#
# Napló-visszaállítás.
# Ez a fájl naponta egyszer fut le a cronból.
# Megforgatja a webmonitor_log fájlt és
# újraindítja a színes megjelenítést.

# PPP-kapcsolatunk a csatlakoztatott számítógép
# nevét "C128.valami.com"-ra állítja.

pty=`w | grep C128 | cut -c 10-15`

# Leállítja a colortailt, megforgatja
# a naplófájlt, újraindítja az Apache-és
# a rendszernaplózó démonokat.

/usr/bin/killall colortail;
cp /var/log/httpd/webmonitor_log
➥/var/log/httpd/webmonitor_log.old;
rm /var/log/httpd/webmonitor_log;
kill -1 `cat /var/run/httpd.pid`;
/usr/bin/killall -HUP syslogd;

# Ha a C128 csatlakoztatott, akkor
# az alábbi sorok a colortail kimenetét
# küldik át.

if [ "$pty" != "" ]
then
colortail -f -k
➥/etc/colortail.conf/var/log/httpd/
➥webmonitor_log> /dev/$pty &
fi
```

```
LogFormat "[%v] %h %u \"%r\" %>s %b\n\"%{Referrer}i
➥\" \"%{User-Agent}i\" %t" webmonitor
```

Ez a naplóadatot a hivatkozóval (Referrer) és a böngésző nevével (User-Agent) együtt egy második sorban jeleníti meg, megkönnyítve az olvasást. A naplófájl bármilyen formátumú lehet, akár a „megszokott” is, amilyet a hagyományos naplózáshoz használunk. Azért döntöttem a megváltoztatása mellett, mert az Apache elég rugalmas ahhoz, hogy megtehessük vele.

Mivel a GIF, JPEG és PNG grafikus fájlok a megjelenítést elronthatják, az alábbi sorokat illesztettem a *httpd.conf* fájl általános naplórészébe, amellyel kizártam e három fájltípust:

```
SetEnvIf Request_URI \.gif$ unwanted
SetEnvIf Request_URI \.jpg$ unwanted
SetEnvIf Request_URI \.png$ unwanted
```

Névalapú virtuális gépeket használtam, és mindegyikhez saját `<VirtualHost>` és `</VirtualHost>` tagok tartoznak. Állandó naplófájljaik mellett „webmonitor” fájlunkhoz minden egyes gépnél egy `CustomLog` parancsot adunk ki, például:

```
<VirtualHost valami.com>
...
CustomLog /var/log/httpd/someisp.com-access_log
➥combined
CustomLog /var/log/httpd/webmonitor_log
➥webmonitor env=!unwanted
...
</VirtualHost>
```

Bővítésem a következőképpen nézett ki:

```
CustomLog /var/log/httpd/webmonitor_log webmonitor
➥env=!unwanted
```

A `/var/log/httpd/webmonitor_log` a naplófájl elérési útvonala, amelyet az Apache azonnal el is készít, ha induláskor még nem létezett. Az egyéni formátumot használó naplófájl neve webmonitor, ezt a fenti `LogFormat` szakaszban határoztuk meg. Az `env=!unwanted` hatására a `SetEnvIf` sorokban megadott elemeket nem naplózza, így a grafikus fájlokra irányuló kérelmekről nem kapunk jelentést.

A fentiekben ábrázolt felügyeleti módszer olyannyira hasznosnak bizonyult, hogy a rendszernaplófájlokra is kiterjesztettük. Ehhez az alábbi sorokat illesztettük a `/etc/syslog.conf` fájlba:

```
kern.*;authpriv.*;*.crit;*.error;*.warning;*.emerg
➥/var/log/httpd/webmonitor_log*
```

A Colortail

A Colortail *Joakim Andersson* (➲ pt98jan@student.hk-r.se) programja, amit a ➲ http://www.student.hk-r.se/~pt98jan/colortail.html címről tölthetünk le, és a GNU felhasználási szerződésének feltételei érvényesek rá. A naplófájlok kiszínezése szebbé varázsolja a megjelenítést, továbbá óriási előnye, hogy a labor másik sarkából egyetlen pillantással meg tudjuk állapítani, éppen melyik gép bonyolít le forgalmat.

A Colortail mellett néhány példajellegű beállításfájlt is találunk, melyek egyike sem igazán felel meg a webes naplózáshoz (talán a *conf.xferlog* jó valamire). Némi bűvészkedés után az alábbiakban ismertetett formátumot alakítottuk ki. Ez egy keresztezés, mely webes és rendszerre vonatkozó események figyelésével egyaránt foglalkozik.

A színezés bekapcsolása

Ha a színezést helyileg szeretnénk bekapcsolni, akkor a

```
colortail -f -k /etc/colortail
➥/var/log/httpd/webmonitor_log &
```

parancsot használjuk. Egyetlen hátránya, hogy nem lehet állandóan a képernyőn, mindig a konzolról vagy az X-ablakról kell rá átváltani. A tevékenységek tökéletesebb megfigyeléséhez a színes kimenetet a rendszerhez kötött Commodore 128D típusú számítógépen jelenítjük meg. Az általunk használt felépítésben a C128 egy belső kiszolgálóra csatlakozik nullmodemmel és PPP-kapcsolattal. Innen lépünk be a naplófájlokat tartalmazó kiszolgálóra. Erre a célra bármilyen régi számítógép megfelel, amely képes ANSI vagy VT100-as megjelenítésre, valamint 80 oszlopos képernyővel rendelkezik. A PPP nem követelmény.

A `colortailt` nem a Commodore-ról indítjuk el, hanem az éjjelente lefutó cronra bízzuk a naplófájlok megforgatásának és a színes kimenet átküldésének feladatát. A *2. listán* az ezt végrehajtó fájl látható.

Összegzés

A naplófájlok figyelésének annyiféle módja létezik, mint égen a csillag, éppen ezért találtam érdekesnek ezt a feladatot. Bár a színezett naplófájlokban nincs semmi forradalmian új, még sehol nem láttam ilyesmit, és ez a megvalósítás tökéletesen megfelelt az igényeimnek. Remnyeim szerint ez a cikk felkeltette a webes események valós idejű megfigyelésére áhítozó rendszergazdák érdeklődését.

Gaelyne R. Gasson (gaelyne@videocam.net.au) webes rendszergazda Dél-Ausztráliában. A cikkben vázolt módszerrel egy szempillantás alatt meg tudja állapítani, honnan nézik webkaméráját ➲ http://gaelyne.com/webcam/.