CSNB113: System Administration
-
14th Topic: Logging

Logging

With our servers up, we need to know in which state they are. This is done by **examining** the ***logs*** (we have seen some examples in the lab exercise), but that is kind of cumbersome. So we have some utilities that do the examination on their own, they have been programmed (written) to extract all relevant information. There are many different such utilities, sometimes with overlapping tasks.

As an example only, here we will look at the output of three utilities:

- Logwatch (http://sourceforge.net/projects/logwatch/files/
- Daily out (OpenBSD)
- Daily Insecurity Output (OpenBSD)

Forgetting?? - Cron!

We are all humans. We tend to forget. We tend to forget regular tasks. We would tend to forget to run all those utilities.

We have cron. cron helps us by running our tasks regularly: we can instruct it to run a repeated task, once per minute, once (or more often) per hour, once (or more often) per day, once (or more often) per week, once (or more often) per month.

This method is a very old method, from the 1970, with a 'newer' version from 1987. It allows all users, including the system administrator, to have a ***crontab*** of their own, into which they can place the timing information and the program(s) to run. It contains information about

minute hour dom month dow cmd

minute	This controls what minute of the hour the command will run on, and is between '0' and '59'
hour	This controls what hour the command will run on, values must be between 0 and 23 (0 is midnight)
dom	This is the Day of Month, that you want the command run on
month	This is the month a specified command will run on
dow	This is the Day of Week that you want a command to be run on
cmd	This is the command that you want run

Examples:

```
min hour dom month dow cmd
59  11   *   *     1-5 backup    ← runs at 11:59 on Monday, Tuesday, Wednesday, Thurday, Friday
30   8   17   1,6   *   whoami    ← runs at 8:30 on each 17th of January (1) and June (6)
21  3    *   *     *   logwatch  ← runs at 3:21 any day
```

Daily log(watch) - postfix

```
 ##################### Logwatch 7.3.6 (05/19/07) ####################
       Processing Initiated: Mon Nov 15 04:22:08 2010
       Date Range Processed: yesterday
                             ( 2010-Nov-14 )
                             Period is day.
     Detail Level of Output: 0
           Type of Output: unformatted
         Logfiles for Host: metalab.uniten.edu.my
 ##################################################################

 ---------- Postfix Begin ------------------------

  60.079K  Bytes accepted                      61,521
  60.079K  Bytes delivered                     61,521
 ========  ==================================================

     16   Accepted                            94.12%
      1   Rejected                            5.88%
 --------  --------------------------------------------------
     17   Total                              100.00%
 ========  ==================================================

      1   Reject unknown user                100.00%
 --------  --------------------------------------------------
      1   Total Rejects                      100.00%
 ========  ==================================================

      4   Connections made
      1   Connections lost
      4   Disconnections
     16   Removed from queue
      2   Delivered
      7   Sent via SMTP
      7   Forwarded



 ---------- Postfix End ------------------------
```

Daily log(watch) - sshd

---------- SSHD Begin ----------

Failed logins from:
  114.251.37.16: 89 times
  115.168.35.215: 11 times
  187.9.92.122 (187-9-92-122.customer.tdatabrasil.net.br): 566 times
  210.169.222.100: 13 times

Illegal users from:
  115.168.35.215: 760 times
  187.9.92.122 (187-9-92-122.customer.tdatabrasil.net.br): 2062 times
  190.220.21.227 (host227.190-220-21.telmex.net.ar): 4 times
  210.169.222.100: 2 times
  211.154.254.173: 724 times

Login attempted when shell does not exist:
  uucp : 3 Time(s)

Received disconnect:
  11: Bye Bye : 4230 Time(s)

Unmatched Entries
reverse mapping checking getaddrinfo for 187-9-92-122.customer.tdatabrasil.net.br [187.9.92.122] failed - POSSIBLE BREAK-IN ATTEMPT! : 2628 time(s)
reverse mapping checking getaddrinfo for host227.190-220-21.telmex.net.ar [190.220.21.227] failed - POSSIBLE BREAK-IN ATTEMPT! : 4 time(s)

---------- SSHD End ----------

Daily log(watch) - disk

---------- Disk Space Begin ----------

Filesystem 512-blocks   Used   Avail Capacity Mounted on
/dev/sd0a   402252   145316   236824   38%   /
/dev/sd0j   117928640 51481456 60550752   46%   /home
/dev/sd0d   4334900   28   4118128   0%   /tmp
/dev/sd0h   16509196   7357272   8326468   47%   /usr
/dev/sd0e   6193704   1615612   4268408   27%   /var
/dev/sd0g   8252052   37168   7802284   0%   /var/mail
/dev/sd0f   123841944 106698524 10951324   91%   /var/www

/dev/sd0f => 91% Used. Warning. Disk Filling up.

---------- Disk Space End ----------

---------- Fortune Begin ----------

Everything is controlled by a small evil group to which, unfortunately,
no one we know belongs.

---------- Fortune End ----------

########## Logwatch End ##########

Daily output Intro

OpenBSD 4.8 (GENERIC.MP) #335: Mon Aug 16 09:09:20 MDT 2010
deraadt@amd64.openbsd.org:/usr/src/sys/arch/amd64/compile/GENERIC.MP

3:33AM up 22 days, 19:25, 0 users, load averages: 1.55, 2.30, 1.53

Running daily.local:
Skipping bad record (1)
[new_snode] Warning: String exceeds storage size (187)
[new_snode] Warning: String exceeds storage size (138)
/usr/sbin/apachectl stop: httpd stopped
/usr/sbin/apachectl graceful: httpd not running, trying to start
/usr/sbin/apachectl graceful: httpd started
hw.sensors.softraid0.drive0=online (sd3), OK

Volume	Status	Size	Device	
softraid0	0 Online	153179181056	sd3	RAID1
0	Online	153179181056	0:0.0	noencl <sd1k>
1	Online	153179181056	0:1.0	noencl <sd2k>

Daily output - / backup

Backing up root=/dev/rsd0a to /dev/rsd1a:
25570+1 records in
25570+1 records out
209469952 bytes transferred in 104.351 secs (2007357 bytes/sec)
** /dev/rsd1a
** Last Mounted on /
** Phase 1 - Check Blocks and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check Reference Counts
** Phase 5 - Check Cyl groups
3956 files, 36468 used, 64095 free (671 frags, 7928 blocks, 0.7% fragmentation)

MARK FILE SYSTEM CLEAN? yes

***** FILE SYSTEM WAS MODIFIED ****

Daily output - / file system

Checking subsystem status:

disks:

```
Filesystem  1K-blocks     Used     Avail Capacity  Mounted on
/dev/sd0a     201126    72936    118134    38%    /
/dev/sd0j   58964320  23751118  32264986    42%    /home
/dev/sd0d    2167450        6   2059072     0%    /tmp
/dev/sd0h    8254598   3708074   4133796    47%    /usr
/dev/sd0e    3096852    107190   2834820     4%    /var
/dev/sd0g    4126026     33112   3886614     1%    /var/mail
/dev/sd3a   148394556  57447456  83527376    41%    /var/www
```

Last dump(s) done (Dump '>' file systems):

```
> /dev/rsd0a    (     /) Last dump: Level 0, Date Sat Feb 19 05:43
> /dev/rsd0e    (  /var) Last dump: Level 0, Date Sat Feb 19 05:43
> /dev/rsd0g    (/var/mail) Last dump: Level 0, Date Sat Feb 19 05:44
> /dev/rsd0h    (  /usr) Last dump: Level 0, Date Sat Feb 19 05:44
```

Daily output - / network

network:

```
Name    Mtu   Network     Address           Ipkts Ierrs    Opkts Oerrs Colls
lo0     33160 <Link>                      455     0      455     0     0
lo0     33160 127/8       127.0.0.1         455     0      455     0     0
lo0     33160 ::1/128     ::1               455     0      455     0     0
lo0     33160 fe80::%lo0/64 fe80::1%lo0       455     0      455     0     0
bge0    1500  <Link>      00:13:21:ae:65:65 114116347  1220 187353883     0     0
bge0    1500  172.16.0/24 172.16.0.2        114116347  1220 187353883     0     0
bge0    1500  fe80::%bge0/64 fe80::213:21ff:feae:6565%bge0 114116347  1220
187353883     0     0
enc0*   0     <Link>                      0     0       0     0     0
pflog0  33160 <Link>                        0     0   688668     0     0
```

Daily output - / insecurity

```
======
/etc/group diffs (-OLD  +NEW)
======
--- /var/backups/etc_group.current      Mon May 31 18:18:50 2010
+++ /etc/group  Sat Jun 19 14:57:32 2010
@@ -82,3 +82,4 @@
 _rwalld:*:96:_rwalld
 _nsd:*:97:_nsd
 _ldpd:*:98:_ldpd
+mailthru:*:1009:

======
/etc/passwd diffs (-OLD  +NEW)
======
--- /var/backups/etc_passwd.current     Mon May 31 18:18:50 2010
+++ /etc/passwd Sat Jun 19 14:57:32 2010
@@ -57,3 +57,4 @@
 _rwalld:*:96:96:rpc.rwalld:/var/empty:/sbin/nologin
 _nsd:*:97:97:NSD Daemon:/var/empty:/sbin/nologin
 _ldpd:*:98:98:LDP Daemon:/var/empty:/sbin/nologin
+mailthru:*:1009:1009:Tunnel to mail SMTP through this box:/home/mailthru:/bin/ksh
```

Web-Server

It is interesting to see the statistics for a webserver. For the users, but also for the system administrator. We want to know the numbers of visits and the volume of data transferred. This allows us to see some cracking, breakage and / or abuse.

There are a number of programs available for this purpose.

Only as an example, we look at *webalizer*. The following examples are taken from metalab.

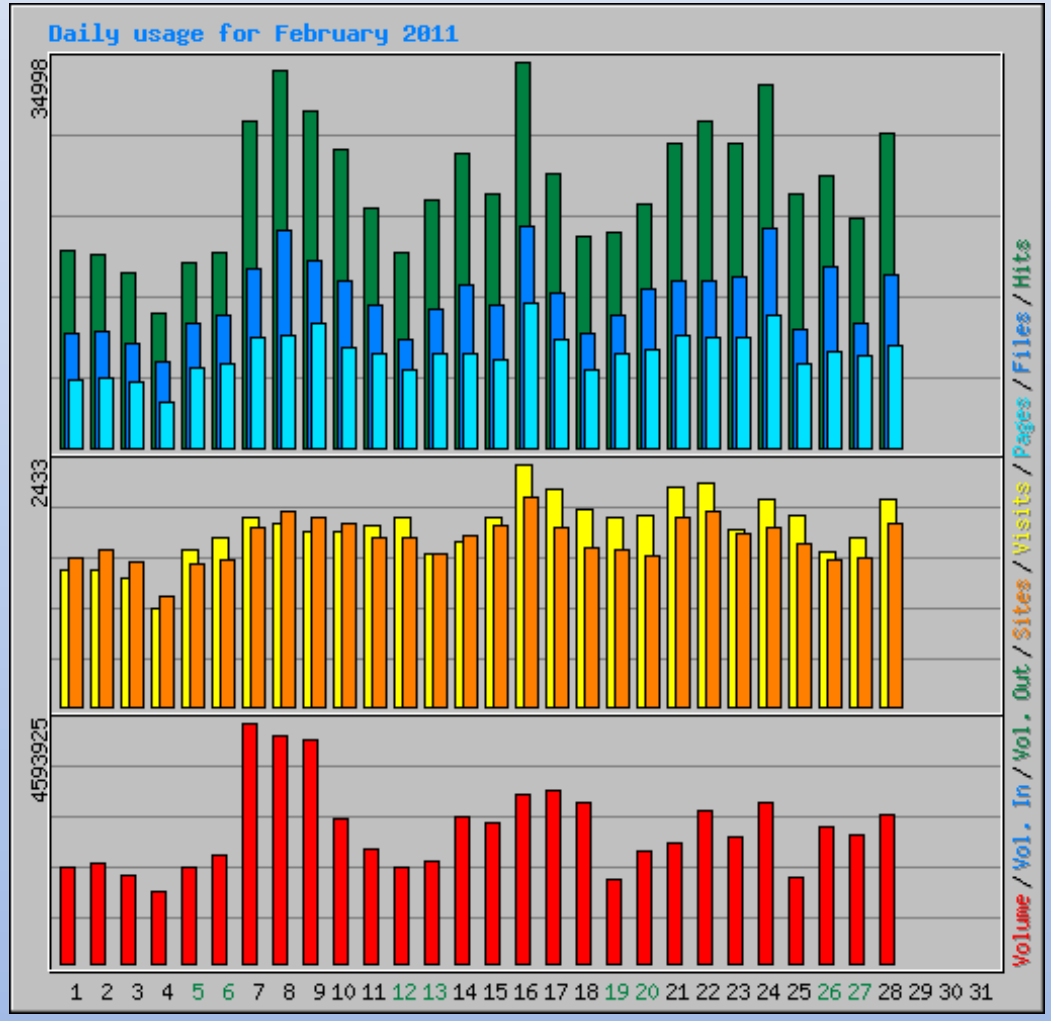
Webalizer gives us information about

- Overall usage
- Code 404 [URL not found]
- Daily Statistics
- Hourly Statistics
- URLs
- Entry [from which sites users came]
- Exit [from which pages user exit]
- Sites [IP-address of visitors]
- Referrers [where hyperlinks to our site were found and used]
- Search [search terms used]
- Users [names of users]
- Agents [browser brands and types used]
- Countries
-

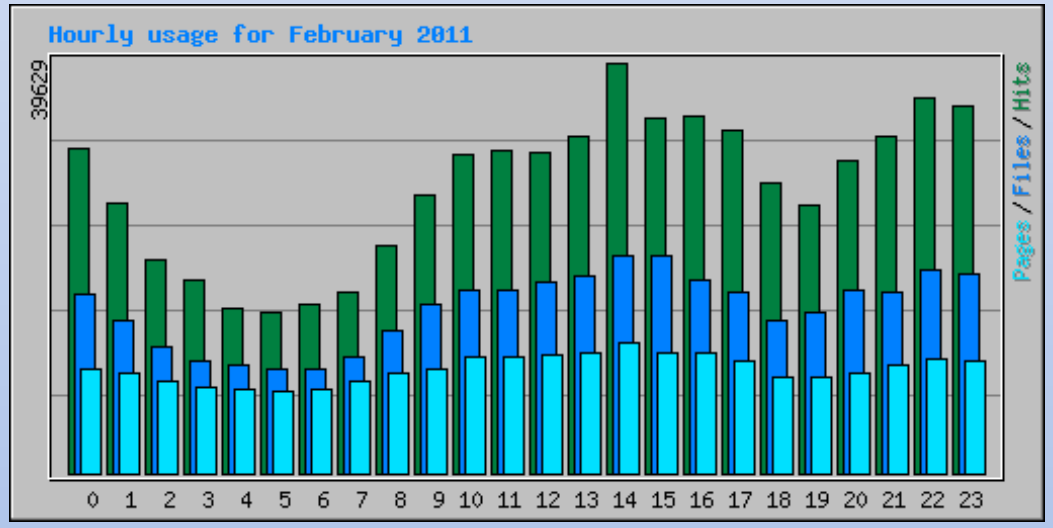
Web-Server - Numbers

Monthly Statistics for February 2011		
Total Hits		665561
Total Files		382671
Total Pages		242004
Total Visits		49927
Total Volume		68.36 GB
Total Vol. In		0 bytes
Total Vol. Out		0 bytes
Total Unique Sites		27341
Total Unique URLs		32741
Total Unique Referrers		18711
Total Unique Usernames		8
Total Unique User Agents		414
	Avg	Max
Hits per Hour	990	3150
Hits per Day	23770	34998
Files per Day	13666	20084
Pages per Day	8643	13158
Visits per Day	1783	2433
Volume per Day	2.44 GB	4.38 GB
Vol. In per Day	0 bytes	0 bytes
Vol. Out per Day	0 bytes	0 bytes

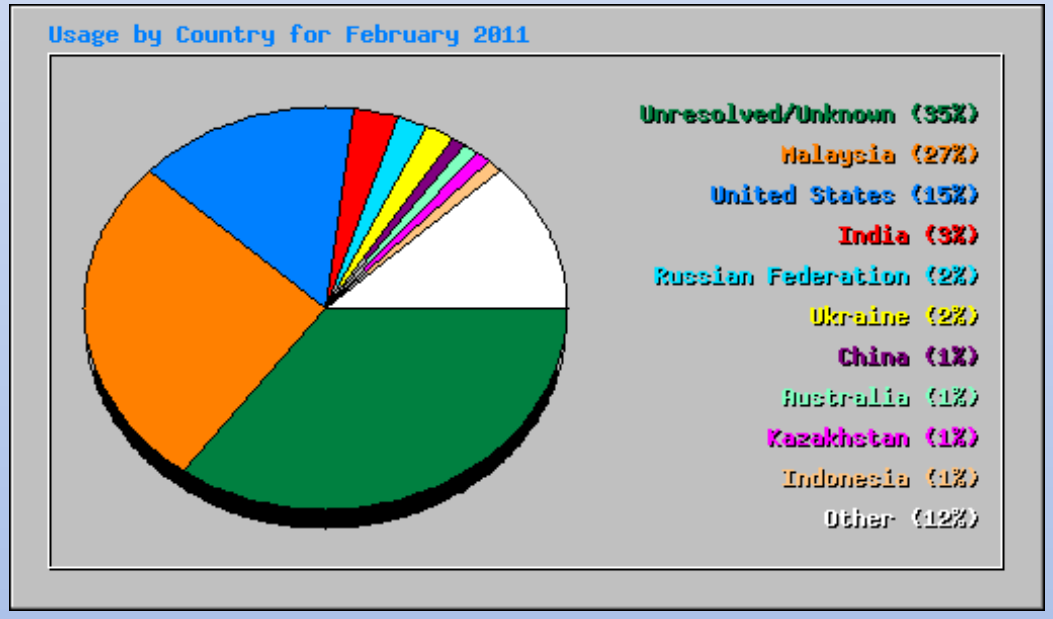
Web-Server - Days



Web-Server - Hours



Web-Server - Countries



References

- http://sourceforge.net/projects/logwatch/files/
- http://www.unixgeeks.org/security/newbie/unix/cron-1.html
- http://www.patrickfrei.ch/webalizer/