Mengamati Log Sistem

Hampir semua dari apa yang terjadi ketika komputer beroperasi, umumnya akan dicatat ke *log file*. Dengan demikian, administrator sistem dapat mengamati log untuk melihat apa saja yang sedang terjadi pada sistem, untuk kemudian dapat menindaklanjutinya sesuai dengan kebijakan yang diterapkan. Di artikel kali ini, kita akan membahas beberapa log di sistem yang mungkin akan sangat berguna dalam memecahkan masalah.

Tugas sistem operasi sangatlah berat. Selain bertugas dari sisi *low level* untuk berbicara dengan *hardware* dan mengatur proses sistem, sistem operasi juga harus bertindak layaknya seorang mata-mata tangguh yang mencatat hampir semua hal yang terjadi pada komputer.

Apa yang dicatat tersebut umumnya dimulai dari proses *booting*, kemudian *event-event* yang terjadi pada sistem ketika beroperasi, dan catatan-catatan lainnya. Tentu saja, karena sistem bisa berkembang menjadi begitu kompleks, sistem operasi tidak dapat mencatat semuanya sendiri. Oleh karena beberapa program yang berfungsi menyediakan service kemudian membantu sistem operasi untuk turut mencatat ke log sistem sesuai dengan tugas yang diembannya. Dengan demikian, log untuk hampir keseluruhan sistem pun dapat dicapai.

Sebenarnya, apa saja yang bisa kita lakukan dengan log-log tersebut? Berikut ini adalah beberapa di antaranya:

- *Troubleshooting*. Tidaklah mudah untuk melakukan troubleshooting. Apalagi pada sistem yang kompleks. Namun setidaknya, dengan adanya log file, kita bisa mendapatkan sedikit catatan tentang apa yang terjadi sebelumnya. Ini diharapkan bisa membantu kita untuk memecahkan masalah.
- *Audit keamanan*. Umumnya, bicara masalah keamanan, sistem operasi *multiuser* seperti halnya Linux akan sangat peduli. Segala yang berhubungan dengan tindakan mengganggu hardware, mengganggu user lain, mengganggu sistem, mengganggu jaringan umumnya akan dicatat. Administrator dapat membuat *script* sederhana untuk melihat percobaan gangguan pada sistem. Hanya, tentu saja kita tidak bisa selalu mengandalkan log file untuk setiap percobaan gangguan. User yang nakal (dan hebat pula) selalu ada.
- *Audit service*. Apabila kita mengelola server yang menjalankan service SAMBA, SQUID, HTTPD, dan lainnya, bantuan log file akan terasa sangat berguna. Umumnya, apa yang dilakukan oleh user untuk meminta service memang tidak akan dapat dicatat oleh server. Namun, penyedia service semacam SAMBA, SQUID dan HTTPD akan membantu sistem dengan menyediakan catatan yang lebih detail, sekaligus melengkapi log sistem (tidak semua service menyediakan fitur ini).

Umumnya, satu masalah besar yang menghambat log adalah tidak terintegrasinya log file. Di Linux, log general untuk sistem memang tersedia (syslog), namun, tidak semua proses lantas memiliki hak untuk mengubah file tersebut begitu saja. Dengan demikian, beberapa aplikasi akan memilih untuk membuat log file sendiri di lokasi yang bervariasi: mulai dari home directory user saja (akan sangat menyebalkan) sampai lokasi temporary lain. Proses-proses semacam ini membuat log yang bahkan dapat dihapus oleh user.

Sayangnya, kita tidak bisa memaksa semua aplikasi untuk dapat mencatat ke log sistem. Apa yang bisa dilakukan adalah menjaga sebaik-baiknya, sekaligus memanfaatkan log file semaksimal mungkin untuk menjaga sistem.

Setelah ini, kita akan mulai membahas beberapa log file yang dapat membantu kita untuk melakukan troubleshooting, audit keamanan dan audit service. Hampir semua file log akan disimpan di direktori /var/log. Anda akan membutuhkan hak akses root untuk dapat membaca semua log yang dibahas di artikel ini. Sebagai catatan, beberapa log file disimpan di lokasi yang terpisah atau bahkan tidak tersedia, tergantung pada kebijakan distro. Distro yang menuruti standar Linux seharusnya tidak akan menghapus atau menggabungkan atau menyimpan ke tempat lain log file tertentu. Tulisan ini dibuat pada distro SUSE 9.3 Pro, namun seharusnya bisa diterapkan pada distro-distro lain.

/var/log/messages

Ini adalah file log yang sangat sangat berguna. Hampir semua kejadian sistem akan didokumentasikan di sini. Karena file ini merupakan catatan hampir semua aktivitas sistem, maka hanya user root dan group root yang bisa membacanya (namun beberapa distro mengubahnya menjadi lebih ketat atau lebih longgar).

File ini akan mencatat mulai proses booting sampai service. Umumnya, beberapa service besar juga akan mencatat ke file log ini, jadi, boleh dikatakan, file log ini memiliki hampir semua informasi.

Berikut ini adalah baris-baris acak dari messages.

```
Jun 14 11:44:29 tbiserv0 kernel:
klogd 1.4.1, log source = /proc/
kmsg started.
Jun 14 11:44:29 tbiserv0 kernel:
ieee1394: Host added: ID:BUS
[0-00:1023]
GUID[000fea0000f64305]
Jun 14 11:44:29 tbiserv0 kernel:
hw_random hardware driver 1.0.0
loaded
Jun 14 11:44:29 tbiserv0 kernel:
```

```
Linux agpgart interface v0.100
(c) Dave Jones
Jun 14 11:44:29 tbiserv0 kernel:
agpgart: Detected an Intel 865
Chipset.
Jun 14 11:44:29 tbiserv0 kernel:
agpgart: Maximum main memory to
use for agp memory: 941M
Jun 14 11:44:29 tbiserv0 kernel:
agpgart: AGP aperture is 128M
@ 0xe8000000
Jun 14 11:44:29 tbiserv0 kernel:
usbcore: registered new driver
usbfs
Jun 14 11:44:29 tbiserv0 kernel:
usbcore: registered new driver
hub
Jun 14 11:44:29 tbiserv0
kernel: ACPI: PCI interrupt
0000:00:1d.7[D] -> GSI 23
(level, low) -> IRQ 185
Jun 14 11:44:29 tbiserv0 kernel:
ehci_hcd 0000:00:1d.7: EHCI Host
Controller
...
...
Jun 14 13:07:09 tbiserv0
squid[8307]: Accepting HTTP
connections at 0.0.0.0, port
8888, FD 12.
Jun 14 13:07:09 tbiserv0
squid[8307]: Accepting ICP
messages at 0.0.0.0, port 3130,
FD 13.
Jun 14 13:07:09 tbiserv0
squid[8307]: HTCP Disabled.
Jun 14 13:07:09 tbiserv0
squid[8307]: Accepting SNMP
messages on port 3401, FD 14.
Jun 14 13:07:09 tbiserv0
squid[8307]: WCCP Disabled.
Jun 14 13:07:09 tbiserv0
squid[8307]: Ready to serve
requests.
Jun 14 13:07:09 tbiserv0
squid[8307]: Done scanning /var/
cache/squid swaplog (0 entries)
Jun 14 13:07:09 tbiserv0
squid[8307]: Finished rebuilding
storage from disk.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Entries
scanned
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Invalid
entries.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 With invalid
flags.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Objects
loaded.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Objects
expired.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Objects
cancelled.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Duplicate URLs
purged.
Jun 14 13:07:09 tbiserv0
squid[8307]:    0 Swapfile
clashes avoided.
Jun 14 13:07:09 tbiserv0
squid[8307]:   Took 0.6 seconds
(   0.0 objects/sec).

...
...
Jun 14 17:32:05 tbiserv0
nmbd[5939]: [2005/06/14
17:32:05, 0] nmbd/nmbd_become_
dmb.c:become_domain_master_
browser_bcast(282)
Jun 14 17:32:05 tbiserv0
nmbd[5939]:   become_domain_
master_browser_bcast:
Jun 14 17:32:05 tbiserv0
nmbd[5939]:   Attempting to
become domain master browser
on workgroup TBI-CKG on subnet
192.168.0.1
Jun 14 17:32:05 tbiserv0
nmbd[5939]: [2005/06/14
17:32:05, 0] nmbd/nmbd_become_
dmb.c:become_domain_master_
browser_bcast(295)
Jun 14 17:32:05 tbiserv0
nmbd[5939]:   become_domain_
master_browser_bcast: querying
subnet 192.168.0.1 for domain
master brow
ser on workgroup TBI-CKG

...
...
Jun 14 17:33:38 tbiserv0 dhcpd:
DHCPREQUEST for 192.168.0.99
from 00:0f:ea:e5:6b:22 (tbi03)
via eth0
Jun 14 17:33:38 tbiserv0 dhcpd:
DHCPACK on 192.168.0.99 to
00:0f:ea:e5:6b:22 (tbi03) via
eth0
```

Dari baris-baris yang ditampilkan tersebut, bisa kita lihat bahwa messages mencatat apa yang terjadi pada kernel (umumnya pada saat booting atau ada perubahan di sistem), mencatat apa yang terjadi pada SQUID, dan mencatat yang terjadi pada SAMBA, dan mencatat permintaan IP dari workstation kepada DHCPD.

File ini juga mencatat yang yang terjadi ketika Anda mengutak-atik perangkat keras yang berpengaruh pada sistem, sebagai contoh, ketika kita mencabut kabel dari kartu jaringan dan memasangnya kembali:

```
Jun 14 17:34:00 tbiserv0 kernel:
eth0: network connection down
Jun 14 17:34:02 tbiserv0 kernel:
eth0: network connection up
using port A
Jun 14 17:34:02 tbiserv0 kernel:
speed:           100
Jun 14 17:34:02 tbiserv0 kernel:
autonegotiation: yes
Jun 14 17:34:02 tbiserv0 kernel:
duplex mode:     full
Jun 14 17:34:02 tbiserv0 kernel:
flowctrl:        symmetric
Jun 14 17:34:02 tbiserv0 kernel:
irq moderation:  disabled
Jun 14 17:34:02 tbiserv0 kernel:
scatter-gather:  enabled
Jun 14 17:34:02 tbiserv0 kernel:
tx-checksum:     enabled
Jun 14 17:34:02 tbiserv0 kernel:
rx-checksum:     enabled
```

Dengan banyaknya kejadian yang dicatat oleh file ini, ukuran file akan membesar dengan cepat. Namun, beberapa distro telah menerapkan log rotator yang akan merotasi log sehingga ukurannya tetap masuk akal.

Memanfaatkan log ini, Anda bisa mengetahui apa yang diinginkan dengan bantuan program grep dan menyaringnya dengan kata kunci yang telah didefinisikan (grep bertingkat bisa diterapkan untuk pencarian yang lebih akurat). Atau, Anda dapat lang-

sung membuka file log ini dan mencari dengan kata kunci tersebut. Anda yang senang membangun shell script tentunya bisa membangun shell script sederhana untuk membuat log ini lebih mudah dibaca.

/var/log/apache2/*

Untuk Anda yang menyalakan web server apache2, maka patut bergembira. Apache HTTPD merupakan salah satu service yang sangat senang mencatat kegiatan yang dilakukan selama melayani koneksi. Log yang dicatat mencakup kegiatan selama melayani ataupun ketika terjadi kegagalan. Lokasi file log akan sangat tergantung pada distro yang Anda gunakan (cobalah /var/log/httpd apabila apache2 tidak ditemukan).

Yang menarik dari web server ini adalah level log yang jelas dan sangat mudah untuk diatur di file konfigurasi utamanya. Bahkan, format log juga bisa diatur dengan sangat mudah. Selain itu, tersedia banyak sekali log analyser untuk apache web server di pasaran open source.

Berikut ini adalah beberapa contoh log kegiatan:

```
192.168.0.99 - - [21/Jun/2005:
12:39:27 +0700] “OPTIONS /
HTTP/1.1” 200 - “-” “Microsoft-
WebDAV-MiniRedir/5.1.2600”
192.168.0.99 - - [21/Jun/2005:
12:39:27 +0700] “PROPFIND /
NETLOGON HTTP/1.1” 405 972
“-” “Microsoft-WebDAV-
MiniRedir/5.1.2600”
192.168.0.99 - - [21/Jun/2005:
12:40:13 +0700] “OPTIONS /
HTTP/1.1” 200 - “-” “Microsoft-
WebDAV-MiniRedir/5.1.2600”
192.168.0.99 - - [21/Jun/2005:
12:40:13 +0700] “PROPFIND /
dos HTTP/1.1” 405 972
“-” “Microsoft-WebDAV-
MiniRedir/5.1.2600”
192.168.0.1 - - [21/Jun/2005:
13:16:36 +0700] “GET /favicon.
ico HTTP/1.0” 404 1044
“-” “Mozilla/5.0 (Windows; U;
Windows NT 5.
1; en-US; rv:1.7.6)
Gecko/20050225 Firefox/1.0.1”
```

Sementara, berikut ini adalah beberapa contoh log entry ketika terjadi kesalahan:

```
[Tue Jun 21 11:50:11 2005]
[warn] Init: Session Cache
is not configured [hint:
SSLSessionCache]
[Tue Jun 21 11:50:11 2005]
[notice] suEXEC mechanism
enabled (wrapper: /usr/sbin/
suexec2)
[Tue Jun 21 11:50:11 2005]
[notice] Apache/2.0.53 (Linux/
SUSE) configured -- resuming
normal operations
[Tue Jun 21 11:57:18 2005]
[error] [client 192.168.0.1]
File does not exist: /srv/www/
htdocs/favicon.ico
```

Bisa kita lihat bahwa level-level log dituliskan dengan sangat mudah dibaca. Mulai dari notice, warn, dan error.

/var/log/samba/log.*

Bagi Anda yang menyalakan service SAMBA, Anda juga patut berbahagia. SAMBA termasuk salah satu proyek open source terbaik dari sisi dokumentasi dan pencatatan. Di dalam direktori /var/log/samba lah terdapat catatan dari segala aktivitas yang terjadi selama melayani.

Umumnya, Anda akan memiliki dua file yaitu log.smbd dan log.nmbd. Apabila Anda menggunakan winbind, maka sebuah log tambahan, log.winbindd akan dapat Anda temukan.

Di file-file log tersebut, dengan mudah Anda bisa melihat apa yang sedang terjadi, termasuk catatan berguna untuk menyelesaikan masalah.

Contoh log.smbd:

```
[2005/06/21 13:07:12, 1] smbd/
service.c:make_connection_
snum(642)
  tbi04 (192.168.0.98) connect
to service dos initially as user
dos (uid=1002, gid=100) (pid
6914)
[2005/06/21 13:07:14, 1] smbd/
service.c:make_connection_
snum(642)
  tbi04 (192.168.0.98) connect
to service netlogon initially
as user dos (uid=1002, gid=100)
(pid 6914)
[2005/06/21 13:12:24, 1] smbd/
service.c:make_connection_
snum(642)
  tbi04 (192.168.0.98) connect
to service dos initially as user
dos (uid=1002, gid=100) (pid
6914)
[2005/06/21 13:12:39, 1] smbd/
service.c:close_cnum(830)
  tbi04 (192.168.0.98) closed
connection to service netlogon
```

Di file log.smbd tersebut, Anda bisa melihat setiap detil koneksi SAMBA. Dalam contoh tersebut, kita bisa melihat bagaimana proses *logout* sedang dilakukan (*closed connection*).

Contoh file log.nmbd:

```
[2005/06/21 11:50:09, 0] nmbd/
nmbd_become_dmb.c:become_domain_
master_browser_bcast(282)
  become_domain_master_browser_
bcast:
  Attempting to become domain
master browser on workgroup TBI-
CKG on subnet 192.168.0.1
[2005/06/21 11:50:09, 0] nmbd/
nmbd_become_dmb.c:become_domain_
master_browser_bcast(295)
  become_domain_master_browser_
bcast: querying subnet
192.168.0.1 for domain master
browser on workgroup TBI-CKG
[2005/06/21 11:50:13, 0] nmbd/
nmbd_logonnames.c:become_logon_
server_success(124)
  become_logon_server_success:
Samba is now a logon server for
workgroup TBI-CKG on subnet
192.168.0.1
[2005/06/21 11:50:17, 0] nmbd/
nmbd_become_dmb.c:become_domain_
master_stage2(113)
  *****

  Samba server TBISERV0 is now
a domain master browser for
workgroup TBI-CKG on subnet
192.168.0.1
  *****
[2005/06/21 11:50:32, 0] nmbd/
nmbd_become_lmb.c:become_local_
master_stage2(396)
```

```
  *****

  Samba name server TBISERV0
is now a local master browser
for workgroup TBI-CKG on subnet
192.168.0.1

  *****
```

Di file log.nmbd tersebut, Anda bisa melihat setiap detil SAMBA yang berhubungan dengan kegiatan *name resolution*. Pada contoh tersebut, terlihat proses bagaiman SAMBA server bernegosiasi menjadi LMB.

/var/log/squid/*.log

Squid juga merupakan salah satu service yang sangat menyenangkan penggunanya. Di log yang dimiliki, squid mencatat hampir segalanya, mulai dari kegiatan melayani sebagai proxy sampai detail akses per komputer dan tujuan yang diakses.

Berikut ini adalah beberapa baris dari cache.log, yang mencatat kegiatan selama melayani:

```
2005/06/21 11:50:18| Beginning
Validation Procedure
2005/06/21 11:50:18|   Completed
Validation Procedure
2005/06/21 11:50:18|   Validated
44 Entries
```

Sementara, berikut ini adalah catatan detil akses dari komputer client dan alamat yang dituju. Contoh berikut ini juga mempertunjukkan porn filter yang menolak user ketika mengunjungi 17tahun.com.

```
1119334601.378    785
192.168.0.98 TCP_DENIED/403 1285
GET http://17tahun.com/
- NONE/- text/html
1119334601.471     92
192.168.0.98 TCP_DENIED/403 1307
GET http://17tahun.com/favicon.
ico - NONE/- text/html
1119334681.184     19
192.168.0.98 TCP_IMS_HIT/304 274
GET http://192.168.0.1/
- NONE/- text/html
1119334685.190     13
192.168.0.98 TCP_MISS/200 934
GET http://192.168.0.1/pub/
- DIRECT/192.168.0.1 text/html
```

/var/log/boot*

Di file log ini, Anda bisa mengamati beberapa hal yang terjadi pada saat booting. Tidak semua memang, tapi cukup banyak yang bisa diamati. Anda juga mungkin bisa melihat tambahannya di *messages*.

Beberapa service seperti DHCPD memang tidak memiliki sendiri. Namun, kerjasamanya cukup baik dengan menuliskan informasi yang sangat detil di messages. Melihat log DCHCP di messages akan sangat membantu. Dengan tetap memperhatikan file log, banyak hal yang mengganggu sistem mungkin dapat dicegah atau dihentikan. Tentunya, termasuk bagaimana menjaga sistem agar tetap handal melayani. Sampai di sini dulu pembahasan kita tentang file log. Tetaplah mengawasi!

Noprianto *(noprianto@infolinux.co.id)*