

Tulisan Seri UNIX SYSTEM ADMINISTRATOR dari INDOCISC

Mengelola catatan (log) dengan “syslog”

oleh: Budi Rahardjo <budi at indocisc.com>

Segala kegiatan di sistem UNIX (dan variannya seperti Linux, FreeBSD, Solaris, AIX, HP-UX dan sejenisnya) dapat dicatat. Pencatatan ini digunakan untuk kebutuhan audit, yaitu memeriksa sistem jika dibutuhkan. Misalnya, jika terjadi kesalahan (error) maka administrator dapat lebih mudah mencari sumber kesalahan karena informasinya tercatat dengan rapi. Demikian pula jika terjadi penyalahgunaan fasilitas, maka dapat diketahui siapa yang melakukannya dan apa saja yang dilakukannya.

Pencatatan kegiatan dilakukan dengan menuliskan data-data ke dalam berkas catatan yang sering disebut dengan nama “logfile” atau berkas log. Proses pencatatan ini sendiri sering disebut dengan istilah *logging*.

Pada mulanya pencatatan ini dilakukan sekehendak dari sang pembuat program. Berkas log dapat disimpan dimana saja dengan format yang berbeda-beda. Bayangkan sebuah sistem UNIX yang memiliki banyak fungsi misalnya sebagai server database, server web, server email, dan seterusnya. Pencatatan yang berbeda-beda ini tentunya akan membingungkan administrator sehingga akhirnya muncul standar logging yang menggunakan fasilitas atau program “syslog”.

Program syslog pada mulanya dikembangkan oleh Eric Allman (yang juga membuat program mail *sendmail*). Saat ini sudah ada beberapa variasi dari program syslog tersebut. Namun pada intinya fungsinya adalah sama. Program syslog ini mencatat kegiatan dalam sebuah format yang standar. Letak logfile dan apa saja yang dicatat dapat diatur oleh sebuah berkas konfigurasi (*syslog.conf*) yang biasanya berada di direktori */etc*. Sebagai contoh, di sistem Linux Debian yang saya gunakan, berkas konfigurasi ini berada di */etc/syslog.conf*. Informasi lebih lengkap tentang isi dan konfigurasi dari berkas ini dapat dilihat dengan menggunakan perintah “*man 5 syslog.conf*”. Untuk syslog nya sendiri dapat dilihat dengan melihat manual *syslogd* pada *section 8* dari manual.

```
debian# man 5 syslog.conf
debian# man 8 syslogd
```

Sebagai contoh, di server saya berkas */var/log/syslog* mencatat beberapa kejadian di sistem. Isi berkas ini antara lain:

```
Dec 9 09:06:15 mx tcplogd: www connection attempt from
kalasan.ntt.net.id [202.171.0.67]
```

contoh di atas menunjukkan koneksi web dari

```
Dec 9 09:08:25 mx tcplogd: ssh connection attempt from
research.indocisc.com [192.168.1.1]
```

contoh di atas menunjukkan adanya koneksi ssh dari mesin
research.indocisc.com

Masih banyak contoh-contoh isi dari berkas *syslog*. Silahkan lihat isi berkas ini untuk melihat apa saja yang dicatat. Perlu diingat bahwa berkas ini biasanya diset hanya dapat dibaca oleh superuser (root). Untuk itu anda harus menjadi superuser (root) untuk bisa membaca isi berkas tersebut.

Konfigurasi *syslog.conf*

Secara umum format dari isi berkas *syslog.conf* adalah sebagai berikut:

fasilitas <TAB> *action*

Perlu diperhatikan bahwa yang memisahkan antara “fasilitas” dan “action” adalah tab. Hal ini sering tidak terlihat dan dianggap sebagai spasi saja. Beberapa versi syslog tidak dapat jalan jika anda menggunakan spasi. Jadi perlu diperhatikan jika anda menggunakan fasilitas *cust-and-paste* yang sering mengubah tab menjadi spasi. Contoh isi berkas *syslog.conf*:

```
mail.info /var/log/mail.log
```

Contoh di atas mengatakan bahwa pesan dari sistem email disimpan dalam berkas */var/log/mail.log*. Secara umum, bagian fasilitas masih dapat dibagi menjadi bertingkat:

fasilitas.level

Dalam contoh di atas, level *info* dari sistem email saja yang disimpan dalam berkas log tersebut. Selain level *info* ada beberapa level lain seperti *emerg*, *alert*, *crit*, *err*, *warning*, *notice*, dan *debug*. Informasi lengkap mengenai level dan urutannya (dengan urutan prioritas yang menurun) dapat dilihat di pada tabel berikut.

Level	Arti
emerg	Situasi gawat (panik)
alert	Situasi urgent
crit	Situasi kritis (critical)
err	Kondisi error
warning	Peringatan (warning)
notice	Perlu diperhatikan
info	Sekedar informasi
debug	Untuk debugging

Berikut ini contoh informasi yang tertulis dalam berkas *mail.log*.

```
Dec 2 06:26:22 mx postfix/qmgr[280]: 25C881492C:  
from=<root@indocisc.com>, size=864, nrcpt=1 (queue active)  
Dec 2 06:26:22 mx postfix/cleanup[23364]: 66A0714921: message-  
id=<20011201232617.C0C4F14921@indocisc.com>  
Dec 2 06:26:22 mx postfix/local[23414]: 1AA621493A:  
to=<budi@indocisc.com>, relay=local, delay=0, status=sent (mailbox)
```

Action pun ada bermacam-macam, mulai dari menyimpan dalam berkas sampai ke mengarahkan logging ke server lain. Contoh di bawah ini menunjukkan bahwa informasi tentang mail dengan level *info* diteruskan ke host dengan nama “*loghost*”.

```
mail.info @loghost
```

Action	Arti
Filename	Tulis pesan di berkas bernama filename
@hostname	Teruskan pesan ke syslogd di server hostname
@ipaddress	Teruskan pesan ke host dengan nomor IP ipaddress
User1,user2	Write ke user1 dan user2 kalau mereka logged in
*	Write ke semua user yang logged in

Pada host *loghost* program *syslog* harus diberitahu untuk menerima logging ini. Pada sistem Linux debian yang saya gunakan hal ini dilakukan dengan menambahkan option “-r” pada *syslog*. Khusus untuk Linux debian hal ini dapat dilakukan dengan mudah dengan mengedit

berkas `/etc/init.d/syslog`. Setelah itu kedua syslog harus diberitahu bahwa ada perubahan pada konfigurasinya dengan mengirimkan sinyal HUP, yaitu dengan menggunakan perintah

```
debian# kill -HUP pid-syslog
```

dimana *pid-syslog* adalah *process identification* (PID) dari proses *syslogd*. Atau cara yang lebih mudah adalah dengan melakukan perintah

```
debian# sh /etc/init.d/syslog restart
```

Setelah dilakukan perintah di atas, maka kegiatan yang berhubungan dengan email dalam level info akan tercatat di host *loghost*. Keuntungan melakukan konsolidasi ini adalah untuk memudahkan administrasi yang tersentralisasi. Anda kemudian dapat menggunakan program untuk menganalisa log dari berbagai host, seperti program “swatch”.

Masih banyak hal lain yang dapat kita lakukan dengan syslog ini. Silahkan mencoba bereksperimen dengan fasilitas syslog ini. Jika anda membuat sebuah program (tools) dan membutuhkan fasilitas logging, jangan lupa gunakan fasilitas syslog ini.

NT Syslog

Syslog umumnya digunakan di sistem UNIX. Bagaimana jika anda mengelola sistem yang berbasis Windows NT? Ternyata ada program NTSyslog yang dapat digunakan untuk mengirimkan data-data (events) dari mesin NT ke sistem UNIX.

NTSyslog: <http://www.sabernet.net/software/ntsyslog.html>

atau sudah dipindahkan ke

<http://ntsyslog.sourceforge.net/>

Bahan Bacaan

Informasi mengenai syslog dapat diperoleh melalui manual pages (man pages) di sistem UNIX untuk *syslogd* (8), *syslog.conf* (5). Buku yang bagus untuk mempelajari administrasi sistem UNIX secara umum adalah buku karangan Evi Nemeth, Garth Snyder, Scott Seebas, dan Trent R. Hein yang berjudul “*UNIX System Administration Handbook*” terbitan Prentice Hall.

Versi 1.1 [9 Desember 2001]. Menambahkan detail tentang isi berkas syslog, tabel tingkat *severity* dari syslog, dan tabel action.