

Henry Saptono, S.Si, M.Kom



Manajemen Log

Apa itu log ?

Dalam komputasi, log adalah sebuah file yang berisi daftar tindakan atau aksi yang telah terjadi.

Sebagai contoh, Web server memelihara log file yang berisi daftar setiap permintaan yang dibuat oleh web client untuk web server



Manfaat log

- Data log dapat digunakan untuk :
 - Statistik
 - Informasi Debug



Manfaat log (cont)

Tren suatu peristiwa atau kejadian dapat dipresentasikan melalui suatu hasil analisis dan statistika dari data-data log sebuah sistem atau aplikasi. Sehingga diharapkan dapat memberikan gambaran tentang tindakan dan aksi yang terjadi dari suatu sistem atau aplikasi



Manfaat log (cont)

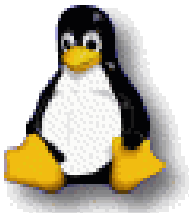
Untuk mengidentifikasi masalah, dan untuk trouble-shooting masalah, membutuhkan pengamatan tindakan dan aksi atau kejadian kejadian dari sistem dan aplikasi selama suatu periode waktu tertentu (*historical monitoring*).

Karena biasanya tidak mungkin untuk mengamati semua peristiwa saat terjadi, sehingga kebanyakan sistem(*daemon*) dan aplikasi merekam peristiwa-peristiwa penting kedalam suatu file yang dikenal sebagai file-file log.



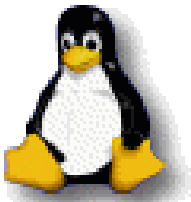
Manajemen Log

- Beberapa aplikasi yang berjalan dalam sebuah sistem memiliki caranya masing masing dalam menuliskan pesan pesan aktifitas atau tindakan dari aplikasi tersebut kedalam file log
- Tidak ada format log yang standar
- Hal ini menyebabkan kerumitan dalam pengelolaan file log atau data log



Manajemen Log (cont)

- Untuk memudahkan dalam manajemen file file log dan untuk membuat standar yang sama dalam penulisan format data log maka dibutuhkan sebuah **sistem log**. Pada system linux terdapat sebuah perangkat lunak sistem log yang dikenal dengan nama syslog (rsyslog) untuk mendukung manajemen log pada sistem linux.



Sistem log - rsyslog

- ♦ Mulanya sebagian besar layanan (services) mengelola file log nya sendiri sendiri melalui sistem log masing-masing. Tetapi kini kebanyakan layanan dapat menggunakan rsyslog *logging daemon* untuk mengumpulkan, menyaring, menyimpan, dan mem-forward log.
- ♦ rsyslog memiliki manfaat tambahan yaitu standarisasi format file log, sehingga lebih mudah untuk memeriksa data log dengan berbagai tool standar.



Sistem log - rsyslog

Beberapa file log dikendalikan oleh sebuah daemon yang disebut rsyslogd.

Daftar pesan-pesan log yang dipelihara oleh rsyslogd dapat ditemukan dalam file konfigurasi rsyslogd yaitu file `/etc/rsyslog.conf` dan dalam file file konfigurasi yang terdapat dalam direktori `/etc/rsyslog.d/`



Lokasi file file log

File file log di sistem linux/unix terletak didalam direktori `/var/log/` . Beberapa aplikasi seperti httpd dan samba memiliki direktori di dalam `/var/log/` untuk menyimpan file-file log masing masing.

Untuk melihat isi dari direktri `/var/log`, lakukan perintah berikut:

```
$ ls /var/log
```



Mengamati File log

Untuk membaca atau menampilkan file log pada sistem linux/unix umumnya digunakan perintah 'tail' , hal ini dikarenakan biasanya yang ingin dibaca atau diamati user adalah pesan log yang terkini (pesan terkini tercatat pada akhir baris dalam file log).

Berikut ini contoh membaca pesan file log yang terkini menggunakan perintah tail:

```
$sudo tail /var/log/daemon.log
```

Untuk membaca file log secara real time gunakan opsi -f pada perintah tail.

```
$sudo tail -f /var/log/daemon.log
```



Format entri dalam File Log

Standar format entri file log adalah terdiri dari informasi sebagai berikut:

Date time, menunjukkan tanggal dan waktu kejadian atau peristiwa

System, menunjukkan nama komputer atau hostname yang membangkitkan pesan (messages).

Facility, menunjukkan nama dari sebuah komponen system yang membangkitkan pesan. Facility ini bisa berupa kernel itu sendiri, sistem daemon, atau bahkan aplikasi-aplikasi.

Messages, adalah teks pesan yang dihasilkan

Standard format of syslog log entry

Oct 13 20:22:06	similikiti	sshd[16877]:	pam_unix(sshd:session): session closed for user henry
-----------------	------------	--------------	---

↑
date time

↑
System

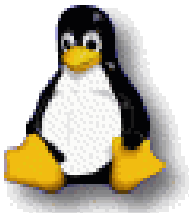
↑
Facility

↑
messages



Rotasi Log

- File log adalah file data, yang akan terus bertambah (tumbuh). Tentunya ini akan membutuhkan kapasitas penyimpanan.
- Dibutuhkan suatu metode untuk mengefisienkan penggunaan kapasitas penyimpanan oleh pertumbuhan file log, yaitu dengan cara :
 - Kompresi
 - **Rotasi log**



Rotasi Log (cont)

Rotasi log adalah proses otomatis yang digunakan dalam sistem administrasi di mana file log di rotasi secara periodik (perhari, perminggu, atau perbulan)

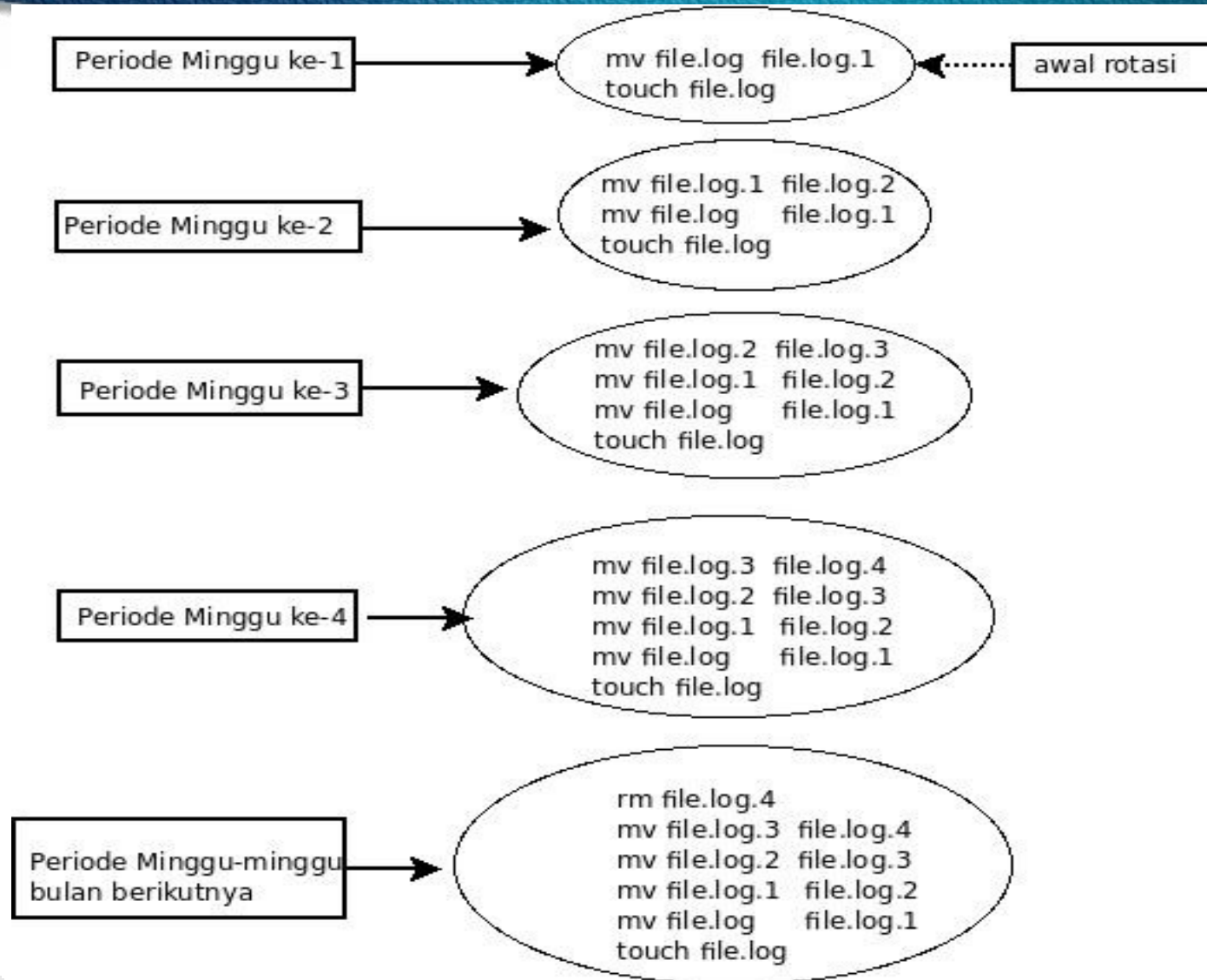


Rotasi Log (cont)

Cara kerja rotasi log dengan logrotate sangat sederhana yaitu memindahkan atau merename file log lama menjadi nama lain (misalnya : dari file.log menjadi file.log.1) selanjutnya membuat file log yang baru. Proses ini dilakukan lagi pada periode waktu tertentu yang kemudian diulangi kembali diperiode berikutnya (misalnya: file.log.1 → file.log.2 , file.log → file.log.1, create new file.log) dan seterusnya sampai batas jumlah rotasi yang ditetapkan.



Ilustrasi Rotasi Log



Logrotate

- Logrotate adalah aplikasi atau perangkat lunak rotasi log yang umum digunakan pada sistem linux untuk memudahkan mekanisme rotasi file file log
- Logrotate berisi tugas cron yang secara otomatis akan merotasi file-file log sesuai dengan konfigurasi pada file `/etc/logrotate.conf` dan file-file konfigurasi di direktori `/etc/logrotate.d/`. Secara default, ini dikonfigurasi untuk merotasi log setiap minggu dan tetap mempertahankan file-file log empat minggu sebelumnya. File konfigurasi utama logrotate adalah `/etc/logrotate.conf`.

