Administrasi Sistem Linux

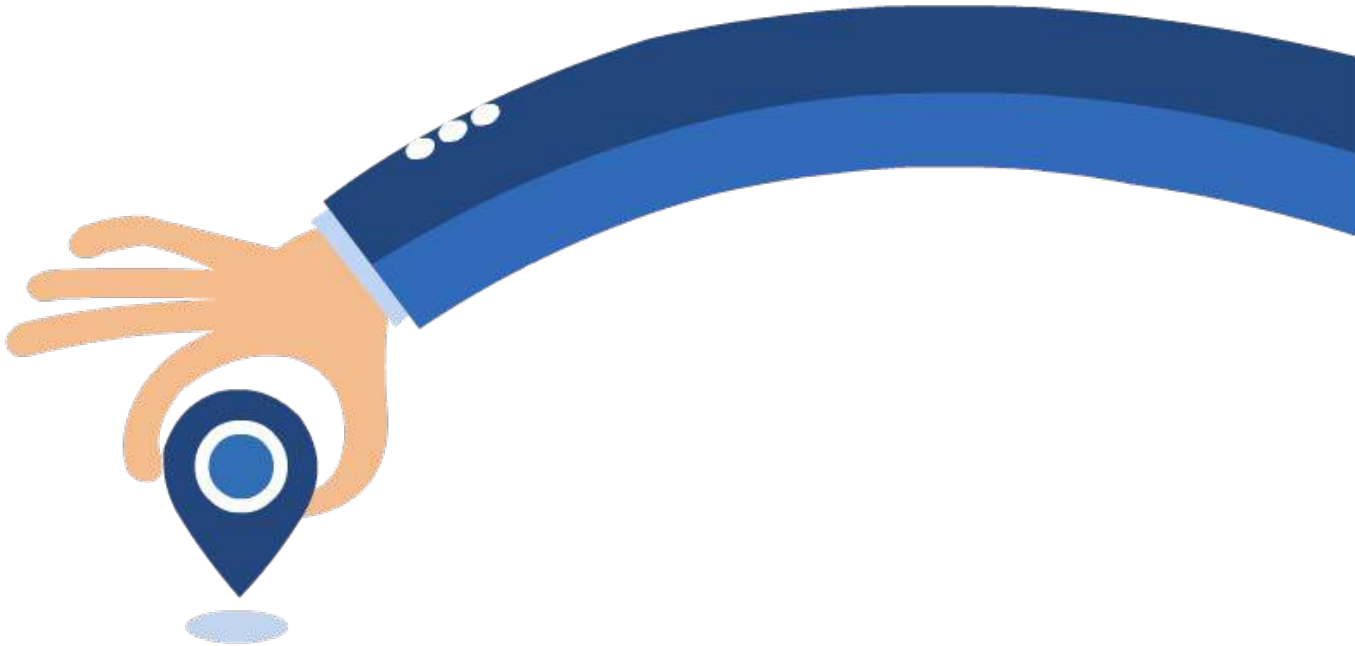
Pertemuan ke- 9

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id 021 7788 6691 info@petik.or.id

Materi

Mengelola Log

Apa itu Log?

- Dalam komputasi, log adalah sebuah file yang berisi daftar tindakan atau aksi yang telah terjadi.
- Sebagai contoh, web server memelihara file log 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

- Tren suatu peristiwa atau kejadian dapat dipresentasikan melalui suatu hasil analisis dan statistik dari data-data log sebuah sistem atau aplikasi. Sehingga diharapkan dapat memberikan gambaran tentang tindakan dan aksi yang terjadi dari suatu sistem atau aplikasi
- Untuk mengidentifikasi masalah dan untuk *troubleshooting* masalah membutuhkan pengamatan tindakan dan aksi atau kejadian-kejadian dari sistem dan aplikasi selama suatu periode waktu tertentu (*historical monitoring*).

Manfaat Log

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

Mengelola Log

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

Mengelola Log

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

rsyslog

- Mulanya sebagian besar layanan (service) 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.

rsyslog

- Beberapa file log dikendalikan oleh sebuah daemon yang disebut rsyslog.
- Daftar pesan-pesan log yang dipelihara oleh rsyslog dapat ditemukan dalam file konfigurasi rsyslog yaitu file /etc/rsyslog.conf dan dalam file-file konfigurasi yang terdapat dalam direktori /etc/rsyslog.d/
- Untuk melihat isi file /etc/rsyslog.conf, lakukan perintah berikut:

```
# cat /etc/rsyslog.conf
```

Lokasi file-file log

- File-file log di sistem Linux/Unix terletak di dalam 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 direktori /var/log, lakukan perintah berikut:

```
# ls -l /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:

```
# tail /var/log/syslog
```

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

```
# tail -f /var/log/syslog
```

Format Entri dalam File Log

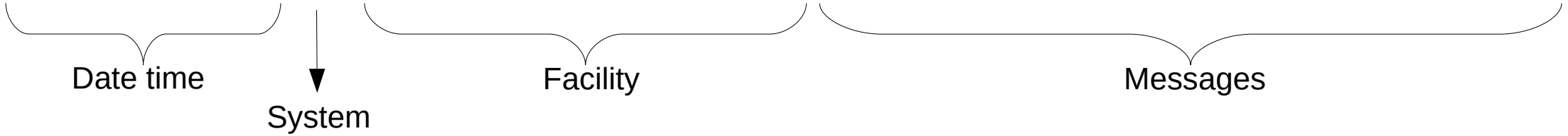
Standar format entri file log adalah terdiri dari informasi sebagai berikut:

- **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 sistem yang membangkitkan pesan. Facility ini bisa berupa kernel itu sendiri, sistem daemon, atau bahkan aplikasi-aplikasi.
- **Messages**, adalah teks pesan yang dihasilkan

Format Entri dalam File Log

Contoh entri dalam file log:

```
May 16 00:05:21 pc2 su: pam_unix(su-l:session): session opened for user root by dudi(uid=500)
```



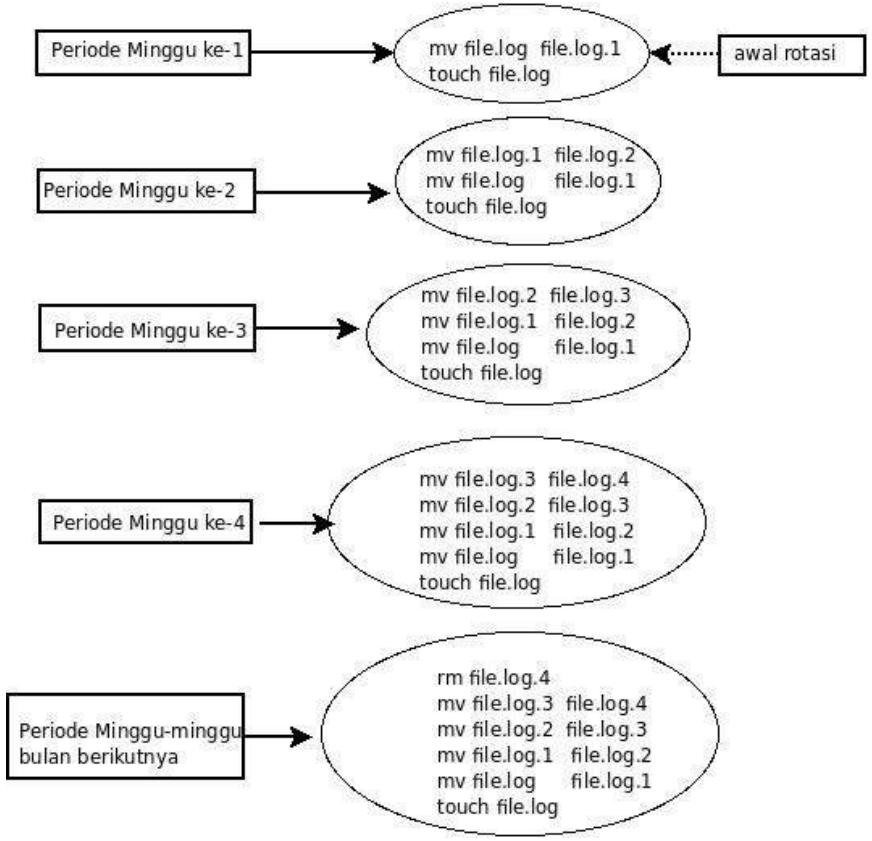
Rotasi File Log

- 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 adalah proses otomatis yang digunakan dalam sistem administrasi dimana file log dirotasi secara periodik (perhari, perminggu, atau perbulan)

Rotasi File Log

Cara kerja rotasi log dengan logrotate sangat sederhana yaitu memindahkan atau mengubah nama 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 di periode 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 File 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, logrotate dikonfigurasi untuk merotasi log setiap minggu dan tetap mempertahankan file-file log empat minggu sebelumnya. File konfigurasi utama logrotate adalah /etc/logrotate.conf.

Direktif pada file Konfigurasi Logrotate

- compress, file log yang lama akan dikompresi secara default menggunakan gzip.
- compresscmd, menentukan perintah yang digunakan untuk mengkompresi file log. Secara default menggunakan perintah gzip.
- compressext, menentukan ekstensi yang digunakan pada file log yang sudah dikompresi.
- create [mode] owner group, segera membuat file log setelah melakukan rotasi.

Direktif pada file Konfigurasi Logrotate

- daily, file log dirotasi setiap satu hari sekali.
- delaycompress, menunda kompresi file log ke rotasi berikutnya.
- hourly, file log dirotasi setiap satu jam sekali.
- maxsize size, file log akan dirotasi ketika ukurannya melebihi size bytes walaupun waktu yang ditentukan belum tercapai.
- minsize size, file log akan dirotasi ketika ukurannya melebihi size bytes, tetapi tidak akan dilakukan sebelum waktu yang ditentukan tercapai.

Direktif pada file Konfigurasi Logrotate

- missingok, jika file log tidak ada lanjutkan tanpa menampilkan pesan error.
- monthly, file log dirotasi setiap satu bulan sekali.
- postrotate/endscript, baris diantara postrotate dan endscript akan dieksekusi (menggunakan /bin/sh) setelah file log dirotasi.
- prerotate/endscript, baris diantara prerotate dan endscript akan dieksekusi (menggunakan /bin/sh) sebelum file log dirotasi dan hanya jika file log akan dirotasi.

Direktif pada file Konfigurasi Logrotate

- rotate count, file log akan dirotasi sebanyak count kali sebelum dihapus. Jika count sama dengan 0, file log akan langsung dihapus setelah dilakukan rotasi. Secara default count sama dengan 0.
- size size, file log akan dirotasi hanya jika ukurannya melebihi size bytes.
- sharedscripts, script prerotate dan postrotate hanya akan dieksekusi satu kali saja.
- su user *group*, rotasi file log akan dieksekusi menggunakan *privilege* user dan group.

Direktif pada file Konfigurasi Logrotate

- weekly, file log akan dirotasi setiap satu pekan sekali.
- yearly, file log akan dirotasi setiap satu tahun sekali.
- notifempty, file log tidak akan dirotasi jika kosong.

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id