6. MANAJEMEN LOG

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

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

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

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

Rsyslog

Mulanya sebagain besar layanan (services) mengelola file log nya sendiri sendiri melalui sistem log masing-masing. Tetapi kini kebanyakan layanan dapat menggunakan rsyslog 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.

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/

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

Lab 6.1. Memeriksa service rsyslog

- Untuk memeriksa apakah service rsyslog sudah berjalan atau belum maka Anda dapat memeriksanya dengan menjakankan perintah berikut:
  ```
  # service rsyslog status
  ```
  atau
  ```
  # /etc/init.d/rsyslog status
  ```
  atau
  ```
  # ps axf | grep rsyslog
  ```
- Jika service rsyslog belum berjalan , Anda dapat menjalankannya dengan perintah sebagai berikut:
  ```
  # service rsyslog start
  ```
  atau
  ```
  # /etc/init.d/rsyslog start
  ```

Lab 6.2. Konfigurasi rsyslog – mendefiniskan log spesifik

- Temukan file konfigurasi rsyslog di direktori /etc
  - File konfigurasi utama rsyslog adalah rsyslog.conf
  - File file dalam direktori /etc/rsyslog.d , merupakan file file konfigurasi spesifik
- Buatlah file dengan nama 10-mylog.conf didalam direktori /etc/rsyslog.d/
- Isi file 10-mylog.conf adalah sebagai berikut:
  `daemon.info /var/log/mylog`

- Kemudian restart rsyslog dengan perintah berikut ini:
  ```
  # service rsyslog restart
  ```
- Kemudian amati apakah file 'mylog' terbentuk atau ada pada direktori /var/log ?
- Selanjutnya uji penulisan pesan log seolah olah dari suatu fasilitas daemon tertentu dengan priority info, menggunakan perintah atau tool logger , seperti perintah berikut ini:
  ```
  # logger -p daemon.info -t 'STT-NF' "New user have been added to STT-NF App"
  ```
- Amati isi dari file /var/log/mylog, dengan perintah :
  ```
  # tail /var/log/mylog
  ```

Lab 6.3. Konfigurasi rsyslog – mengesampingkan pesan log spesifik

- Suatu pesan log dari suatu fasilitas dengan priority tertentu atau keseluruhan dapat dikesampingkan (discard)
- Coba Anda ubah isi dari file /etc/rsyslog.d/10-mylog.conf, sehingga menjadi seperti berikut ini:
  ```
  #daemon.info                /var/log/mylog
  daemon.info      ~
  ```
- Kemudian restart rsyslog
- Selanjutnya perhatikan isi dari file /var/log/mylog saat ini ketika suatu fasilitas daemon mencoba mengirimkan pesan info , apakah tercatat dalam file /var/log/mylog? Lakukan perintah berikut ini:

  ```
  # logger -p daemon.info -t 'STT-NF' "User Logout"
  ```

- Perhatikan juga apakah pesan tersebut tercatat dalam file log lainnya seperti dalam file /var/log/syslog ?

Lab 6.4. Konfigurasi rsyslog – menerima log dari suatu program spesifik dengan konten spesifik

- Suatu pesan log dari suatu program spesifik dengan konten pesan mengandung suatu kata tertentu atau spesifik dan kemudian dicatat kedalam suatu file tertentu oleh rsyslog, dapat Anda terapkan dengan memanfaat fitur yang tersedia dari syslog.
- Contoh Anda menginginkan rsyslog menerima pesan dari aplikasi atau program bernama 'STT-NF' dan dengan isi pesan mengandung kata 'logout', yang akan dicatat oleh rsyslog kedalam file /var/log/sttnf-logout
- Buatlah file /etc/rsyslog.d/05-sttnf.conf, kemudian isi dengan baris berikut ini:
  ```
  if $programname == 'STT-NF' and $msg contains 'logout' then /var/log/sttnf-logout
  ```
- Restart rsyslog
- Kemudian coba kirim pesan log seolah olah dari program STT-NF menggunakan tool logger seperti berikut ini:
  - ```
    # logger -p daemon.info -t 'STT' "user have been logout sir"
    ```
    ```

Amati apa yang terjadi pada file /var/log/sttnf-logout ? Dan bagaimana pada file /var/log/syslog ?

- Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:

```
# logger -p daemon.info -t 'STT-NF' "user have been login sir"
```

Amati apa yang terjadi pada file /var/log/sttnf-logout ? Dan bagaimana pada file /var/log/syslog ?

- Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:

```
# logger -p daemon.info -t 'STT-NF' "user have been logout sir"
```

Amati apa yang terjadi pada file /var/log/sttnf-logout ? Dan bagaimana pada file /var/log/syslog ?

Lab 6.5. Konfigurasi rotasi log

- Atur rotasi log dari file /var/log/mylog agar dilakukan rotasi perhari , dan file rotasi dijaga sampai 6 rotasi
- Buatlah file dengan nama **sttnf** didalam direktori /etc/logrotate.d
- Kemudian tuliskan bari berikut ini kedalam file tersebut:

```
/var/log/mylog {
      daily
      missingok
      rotate 6
      compress
      delaycompress
      notifempty
      create 640 root adm
      sharedscripts
      postrotate
            /usr/bin/logger -p mail.info 'ROTATE STTNF' “Rotate done”
      endscript
      prerotate
            /usr/bin/logger -p mail.info 'ROTATE STTNF' “Rotate starting”
      endscript
}
```

- Kemudian lakukan rotasi secara paksa dengan perintah berikut ini:

```
# logrotate -f /etc/logrotate.d/sttnf
```

- Lihat dalam direktori /var/log file dengan nama mylog dan mylog.1 ?
- Amati juga pesan log di /var/log/syslog apakah ada pesan `“Rotate starting”` dan `“Rotate done”`