

# **Laporan Praktikum 6**

## **Administrasi Sistem**

### **Manajemen Log**



Muhammad Azhar Rasyad  
0110217029  
Teknik Informatika 1

**Sekolah Tinggi Teknologi Terpadu Nurul Fikri**  
**2018**

# Manajemen Log

Manajemen Log berfungsi untuk memudahkan dalam manajemen file file log dan untuk membuat standar yang sama dalam penulisan format data log maka dibutuhkan sebuah sistem log.

Berikut merupakan **implementasi dari manajemen log** dan sistem operasi yang digunakan adalah **Ubuntu 16.04 LTS** :

## Lab 6.1 Memeriksa service rsyslog

1. Untuk memeriksa apakah service rsyslog sudah berjalan atau belum maka Anda dapat memeriksanya dengan menjalankan perintah berikut:

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ service rsyslog status  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset:  
   Active: active (running) since Rab 2018-11-21 12:27:10 WIB; 1h 8min ago  
     Docs: man:rsyslogd(8)  
           http://www.rsyslog.com/doc/  
   Main PID: 887 (rsyslogd)  
    CGroup: /system.slice/rsyslog.service  
            └─887 /usr/sbin/rsyslogd -n  
  
Nov 21 12:27:09 mazharrasyad systemd[1]: Starting System Logging Service...  
Nov 21 12:27:10 mazharrasyad systemd[1]: Started System Logging Service.  
lines 1-11/11 (END)
```

2. Jika service rsyslog belum berjalan , Anda dapat menjalankannya dengan perintah sebagai berikut:

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ sudo service rsyslog start  
[sudo] password for mazharrasyad:  
mazharrasyad@mazharrasyad:~$
```

## Lab 6.2 Konfigurasi rsyslog – mendefiniskan log spesifik

1. 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

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ ls /etc | grep rsyslog  
rsyslog.conf  
rsyslog.d  
mazharrasyad@mazharrasyad:~$
```

2. Buatlah file dengan nama 10-mylog.conf didalam direktori /etc/rsyslog.d/

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d  
mazharrasyad@mazharrasyad:~$ cd /etc/rsyslog.d/  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ ls  
20-ufw.conf 50-default.conf  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$
```

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ sudo nano 10-mylog.conf
```

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d  
GNU nano 2.5.3 File: 10-mylog.conf Modified  
daemon.info /var/log/mylog  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ ls  
10-mylog.conf 20-ufw.conf 50-default.conf  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$
```

3. Isi file 10-mylog.conf adalah sebagai berikut:

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ cat 10-mylog.conf  
daemon.info /var/log/mylog  
mazharrasyad@mazharrasyad:/etc/rsyslog.d$
```

4. Kemudian restart rsyslog dengan perintah berikut ini:

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ sudo service rsyslog restart
mazharrasyad@mazharrasyad:/etc/rsyslog.d$
```

5. Kemudian amati apakah file 'mylog' terbentuk atau ada pada direktori /var/log ?

```
mazharrasyad@mazharrasyad: /etc/rsyslog.d
mazharrasyad@mazharrasyad:/etc/rsyslog.d$ ls /var/log | grep mylog
mylog
mazharrasyad@mazharrasyad:/etc/rsyslog.d$
```

6. Selanjutnya uji penulisan pesan log seolah olah dari suatu fasilitas daemon tertentu dengan priority info, menggunakan perintah atau tool logger , seperti perintah berikut ini:
7. Amati isi dari file /var/log/mylog, dengan perintah :

### Lab 6.3 Konfigurasi rsyslog – mengesampingkan pesan log spesifik

1. Suatu pesan log dari suatu fasilitas dengan priority tertentu atau keseluruhan dapat dikesampingkan (discard)
2. Coba Anda ubah isi dari file /etc/rsyslog.d/10-mylog.conf, sehingga menjadi seperti berikut ini:
3. Kemudian restart rsyslog
4. 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:
5. 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

1. 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 memanfaatkan fitur yang tersedia dari syslog.
2. 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`
3. Buatlah file `/etc/rsyslog.d/05-sttnf.conf`, kemudian isi dengan baris berikut ini:
4. Restart rsyslog
5. Kemudian coba kirim pesan log seolah olah dari program STT-NF menggunakan tool logger seperti berikut ini:
6. Amati apa yang terjadi pada file `/var/log/sttnf-logout` ? Dan bagaimana pada file `/var/log/syslog` ?
7. Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:
8. Amati apa yang terjadi pada file `/var/log/sttnf-logout` ? Dan bagaimana pada file `/var/log/syslog` ?
9. Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:
10. Amati apa yang terjadi pada file `/var/log/sttnf-logout` ? Dan bagaimana pada file `/var/log/syslog` ?

## Lab 6.5 Konfigurasi rotasi log

1. Atur rotasi log dari file `/var/log/mylog` agar dilakukan rotasi perhari , dan file rotasi dijaga sampai 6 rotasi
2. Buatlah file dengan nama sttnf didalam direktori `/etc/logrotate.d`
3. Kemudian tuliskan bari berikut ini kedalam file tersebut:
4. Kemudian lakukan rotasi secara paksa dengan perintah berikut ini:
5. Lihat dalam direktori `/var/log` file dengan nama mylog dan mylog.1 ?
6. Amati juga pesan log di `/var/log/syslog` apakah ada pesan "Rotate starting" dan "Rotate done"

----- Selesai -----

# Referensi

- Modul praktikum Administrasi sistem dan jaringan – STT NF (Disusun oleh: Henry Saptono, S.Si, M.Kom)