

# **Laporan Praktikum 6**

## **Administrasi Sistem**

### **Manajemen Log**



Muhammad Azhar Rasyad  
0110217029  
Teknik Informatika 1

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

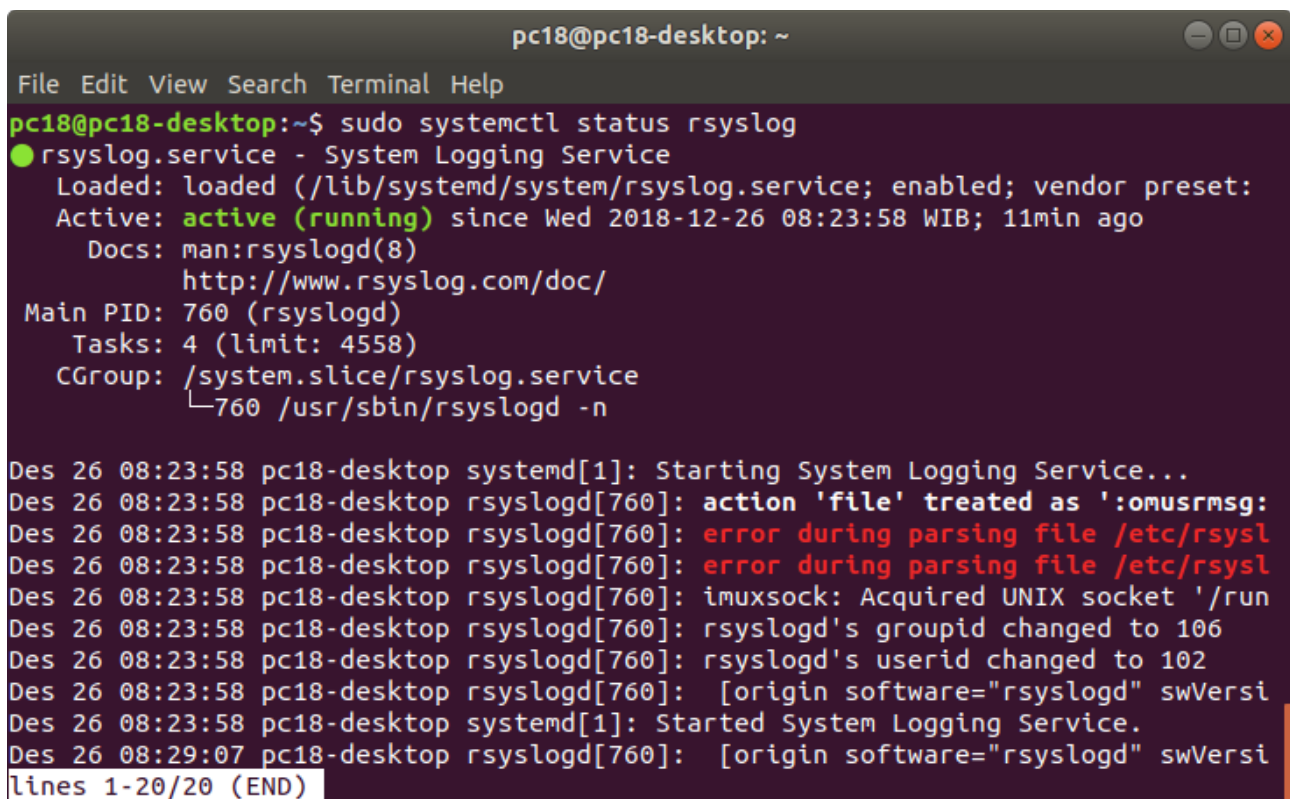
# Manajemen Log

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** :

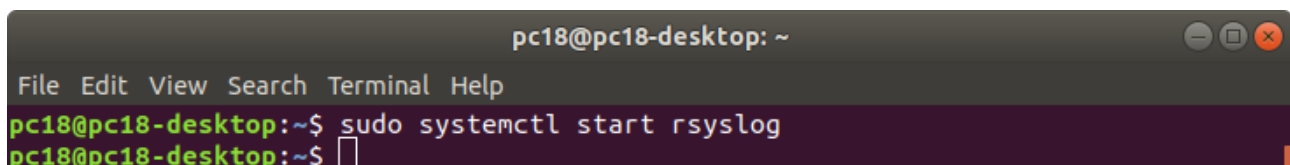
## Lab 6.1 Memeriksa service rsyslog

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



```
pc18@pc18-desktop: ~  
File Edit View Search Terminal Help  
pc18@pc18-desktop:~$ sudo systemctl status rsyslog  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset:  
   Active: active (running) since Wed 2018-12-26 08:23:58 WIB; 11min ago  
     Docs: man:rsyslogd(8)  
           http://www.rsyslog.com/doc/  
   Main PID: 760 (rsyslogd)  
     Tasks: 4 (limit: 4558)  
    CGroup: /system.slice/rsyslog.service  
            └─760 /usr/sbin/rsyslogd -n  
  
Des 26 08:23:58 pc18-desktop systemd[1]: Starting System Logging Service...  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: action 'file' treated as ':omusrmsg:  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: error during parsing file /etc/rsysl  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: error during parsing file /etc/rsysl  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: imuxsock: Acquired UNIX socket '/run  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: rsyslogd's groupid changed to 106  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: rsyslogd's userid changed to 102  
Des 26 08:23:58 pc18-desktop rsyslogd[760]: [origin software="rsyslogd" swVersi  
Des 26 08:23:58 pc18-desktop systemd[1]: Started System Logging Service.  
Des 26 08:29:07 pc18-desktop rsyslogd[760]: [origin software="rsyslogd" swVersi  
lines 1-20/20 (END)
```

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



```
pc18@pc18-desktop: ~  
File Edit View Search Terminal Help  
pc18@pc18-desktop:~$ sudo systemctl start rsyslog  
pc18@pc18-desktop:~$
```

## Lab 6.2 Konfigurasi rsyslog – mendefinisikan log spesifik

1. Temukan file konfigurasi rsyslog di direktori /etc
  - o File konfigurasi utama rsyslog adalah rsyslog.conf
  - o File file dalam direktori /etc/rsyslog.d , merupakan file file konfigurasi spesifik

```
pc18@pc18-desktop: ~  
File Edit View Search Terminal Help  
pc18@pc18-desktop:~$ ls /etc | grep rsyslog  
rsyslog.conf  
rsyslog.d  
pc18@pc18-desktop:~$
```

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

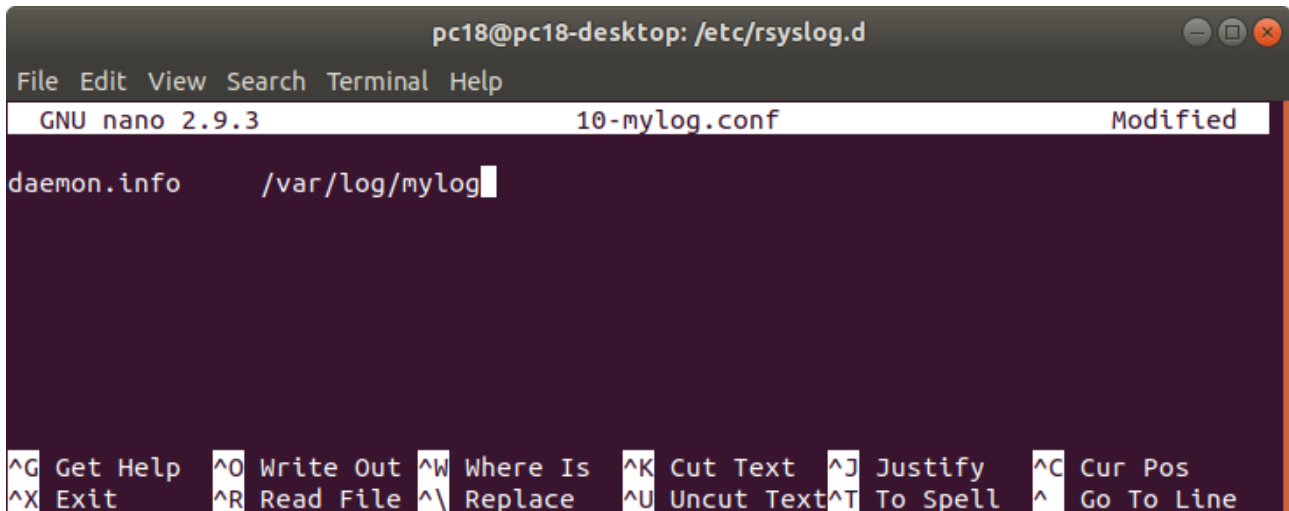
```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:~$ cd /etc/rsyslog.d
pc18@pc18-desktop:/etc/rsyslog.d$ ls
20-ufw.conf  50-default.conf
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Ketikkan `sudo nano 10-mylog.conf` maka akan seperti gambar berikut

The screenshot shows a terminal window with the nano text editor open. The title bar indicates the user is 'pc18' on a 'pc18-desktop' machine, editing the file '/etc/rsyslog.d'. The editor's status bar shows 'GNU nano 2.9.3', the filename '10-mylog.conf', and the state 'Modified'. The main editing area is currently empty. At the bottom, a help menu lists various keyboard shortcuts for navigating and editing the file.

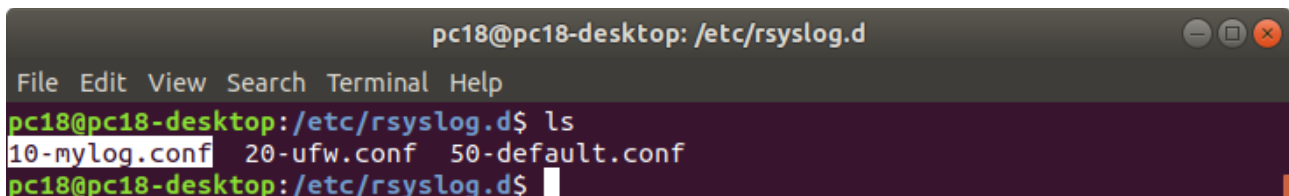
Shortcut	Action
^G	Get Help
^O	Write Out
^W	Where Is
^K	Cut Text
^J	Justify
^C	Cur Pos
^X	Exit
^R	Read File
^_	Replace
^U	Uncut Text
^T	To Spell
^_	Go To Line

- Kemudian isi seperti pada gambar dibawah



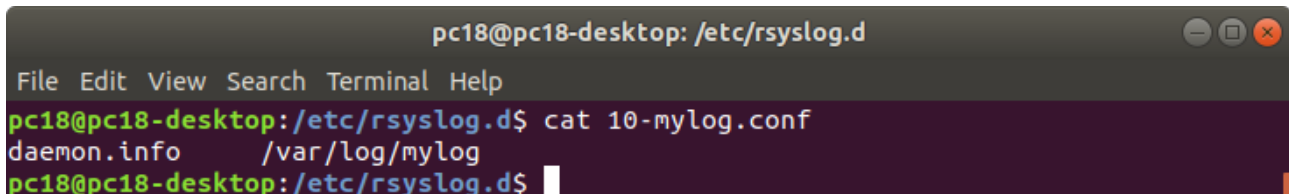
```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 10-mylog.conf Modified
daemon.info /var/log/mylog
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

- Periksa kembali apakah file 10-mylog.conf sudah terbuat atau belum



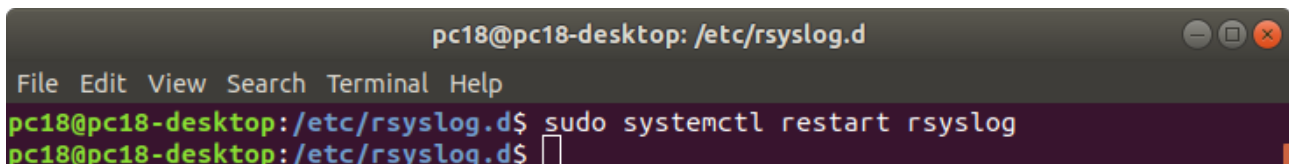
```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ ls
10-mylog.conf 20-ufw.conf 50-default.conf
pc18@pc18-desktop:/etc/rsyslog.d$
```

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



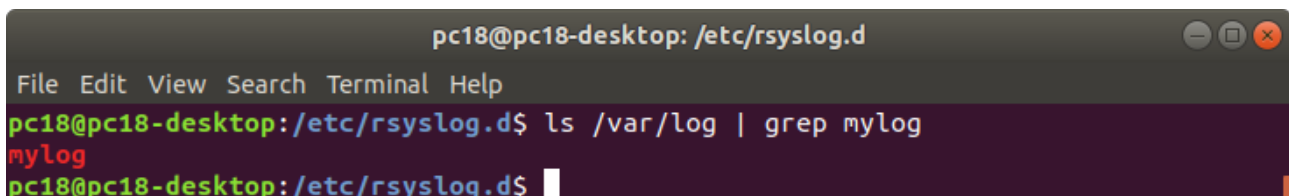
```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ cat 10-mylog.conf
daemon.info /var/log/mylog
pc18@pc18-desktop:/etc/rsyslog.d$
```

4. Kemudian restart rsyslog dengan perintah berikut ini:



```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo systemctl restart rsyslog
pc18@pc18-desktop:/etc/rsyslog.d$
```

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



```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ ls /var/log | grep mylog
mylog
pc18@pc18-desktop:/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:

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logger -p daemon.info -t 'STT-NF' "User B
aru Berhasil diBuat Ke STT-NF APPS !!"
sudo logger -p daemon.info -t 'STT-NF' "User Baru Berhasil diBuat Ke STT-NF APPS
ls /var/log | grep mylog"
pc18@pc18-desktop:/etc/rsyslog.d$
```

7. Amati isi dari file /var/log/mylog, dengan perintah :

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo tail /var/log/mylog
Dec 26 08:36:47 pc18-desktop ntfs-3g[4815]: Unmounting /dev/sdb (azhar)
Dec 26 08:38:45 pc18-desktop systemd[1]: Starting Cleanup of Temporary Directori
es...
Dec 26 08:38:45 pc18-desktop systemd[1]: Started Cleanup of Temporary Directorie
s.
Dec 26 08:39:01 pc18-desktop systemd[1]: Starting Clean php session files...
Dec 26 08:39:02 pc18-desktop systemd[1]: Started Clean php session files.
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopping System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopped System Logging Service.
Dec 26 08:41:36 pc18-desktop systemd[1]: Starting System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Started System Logging Service.
Dec 26 08:42:30 pc18-desktop STT-NF: User Baru Berhasil diBuat Ke STT-NF APPS ls
/var/log | grep mylog
pc18@pc18-desktop:/etc/rsyslog.d$
```

## 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:
  - Ketikkan perintah seperti berikut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo nano /etc/rsyslog.d/10-mylog.conf
```

- Jika perintah benar maka akan muncul isi file tersebut seperti berikut

```

pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.d/10-mylog.conf
daemon.info /var/log/mylog

[ Read 1 line ]
^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

```

- Kemudian ubah isinya seperti berikut

```

pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.d/10-mylog.conf Modified
#daemon.info /var/log/mylog
daemon.info ~

[ Read 1 line ]
^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

```

### 3. Kemudian restart rsyslog

```

pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo systemctl restart rsyslog
pc18@pc18-desktop:/etc/rsyslog.d$

```

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:

```

pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logger -p daemon.info -t 'STT-NF' "User L
ogout"
pc18@pc18-desktop:/etc/rsyslog.d$

```

- Pada file `/var/log/mylog` tidak tercatat pesan info diatas

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo tail /var/log/mylog
Dec 26 08:36:47 pc18-desktop ntfs-3g[4815]: Unmounting /dev/sdb (azhar)
Dec 26 08:38:45 pc18-desktop systemd[1]: Starting Cleanup of Temporary Directori
es...
Dec 26 08:38:45 pc18-desktop systemd[1]: Started Cleanup of Temporary Directorie
s.
Dec 26 08:39:01 pc18-desktop systemd[1]: Starting Clean php session files...
Dec 26 08:39:02 pc18-desktop systemd[1]: Started Clean php session files.
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopping System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopped System Logging Service.
Dec 26 08:41:36 pc18-desktop systemd[1]: Starting System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Started System Logging Service.
Dec 26 08:42:30 pc18-desktop STT-NF: User Baru Berhasil diBuat Ke STT-NF APPS ls
/var/log | grep mylog
pc18@pc18-desktop:/etc/rsyslog.d$
```

5. Perhatikan juga apakah pesan tersebut tercatat dalam file log lainnya seperti dalam file `/var/log/syslog` ?

- Pada file `/var/log/syslog` juga tidak terdapat pesan info tersebut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/syslog | grep "User Logout"
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Namun pada file `/var/log/auth.log` terdapat pesan info tersebut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/auth.log | grep "User Logout"
Dec 26 08:46:06 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout
Dec 26 08:48:18 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout
Dec 26 08:54:00 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout
Dec 26 08:55:51 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout
pc18@pc18-desktop:/etc/rsyslog.d$
```



## 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:
  - Ketikkan perintah berikut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo nano /etc/rsyslog.d/05-sttnf.conf
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Jika file baru maka akan seperti berikut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.d/05-sttnf.conf
[ New File ]
^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
```

- Kemudian isi perintah **if \$programname == 'STT-NF' and \$msg contains 'logout' then file=/var/log/sttnf-logout**

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.d/05-sttnf.conf Modified
if $programname == 'STT-NF' and $msg contains 'logout' then file=/var/log/sttnf$
^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
```



#### 4. Restart rsyslog

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo systemctl restart rsyslog
pc18@pc18-desktop:/etc/rsyslog.d$
```

5. Kemudian coba kirim pesan log seolah olah dari program STT-NF menggunakan tool logger seperti berikut ini:

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logger -p daemon.info -t 'STT-NF' "User Logout By Admin"
pc18@pc18-desktop:/etc/rsyslog.d$
```

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

- Yang terjadi pada file /var/log/sttnf-logout, terdapat pesan tersebut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/sttnf-logout | grep Logout
Dec 26 09:03:30 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout By Admin
Dec 26 09:03:30 pc18-desktop STT-NF: User Logout By Admin
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Yang terjadi pada file /var/log/syslog, tidak ada pesan tersebut

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/syslog | grep Logout
pc18@pc18-desktop:/etc/rsyslog.d$
```

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

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logger -p daemon.info -t 'STT-NF' "User Login By Admin"
pc18@pc18-desktop:/etc/rsyslog.d$
```

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

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo tail /var/log/sttnf-logout
Dec 26 09:10:51 pc18-desktop sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 26 09:10:51 pc18-desktop STT-NF: User Login By Admin
Dec 26 09:10:51 pc18-desktop sudo: pam_unix(sudo:session): session closed for user root
Dec 26 09:10:52 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/cat /var/log/sttnf-logout
Dec 26 09:10:52 pc18-desktop sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 26 09:10:52 pc18-desktop sudo: pam_unix(sudo:session): session closed for user root
Dec 26 09:11:01 pc18-desktop CRON[6208]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:11:01 pc18-desktop CRON[6209]: (root) CMD (cp -rf /home/guest /tmp)
Dec 26 09:11:01 pc18-desktop CRON[6208]: pam_unix(cron:session): session closed for user root
Dec 26 09:11:22 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/usr/bin/tail /var/log/sttnf-logout
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Yang terjadi pada file `/var/log/syslog`

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/syslog | grep Login
pc18@pc18-desktop:/etc/rsyslog.d$
```

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

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logger -p daemon.info -t 'STT-NF' "User Logout By Admin"
pc18@pc18-desktop:/etc/rsyslog.d$
```

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

- Yang terjadi pada file `/var/log/sttnf-logout`, pesan tersebut ada

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/sttnf-logout | grep Logout
Dec 26 09:03:30 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout By Admin
Dec 26 09:03:30 pc18-desktop STT-NF: User Logout By Admin
Dec 26 09:06:43 pc18-desktop sudo:      pc18 : TTY=pts/0 ; PWD=/etc/rsyslog.d ; U
SER=root ; COMMAND=/usr/bin/logger -p daemon.info -t STT-NF User Logout By Admin
Dec 26 09:06:43 pc18-desktop STT-NF: User Logout By Admin
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Yang terjadi pada file `/var/log/syslog`, pesan tersebut tidak ada

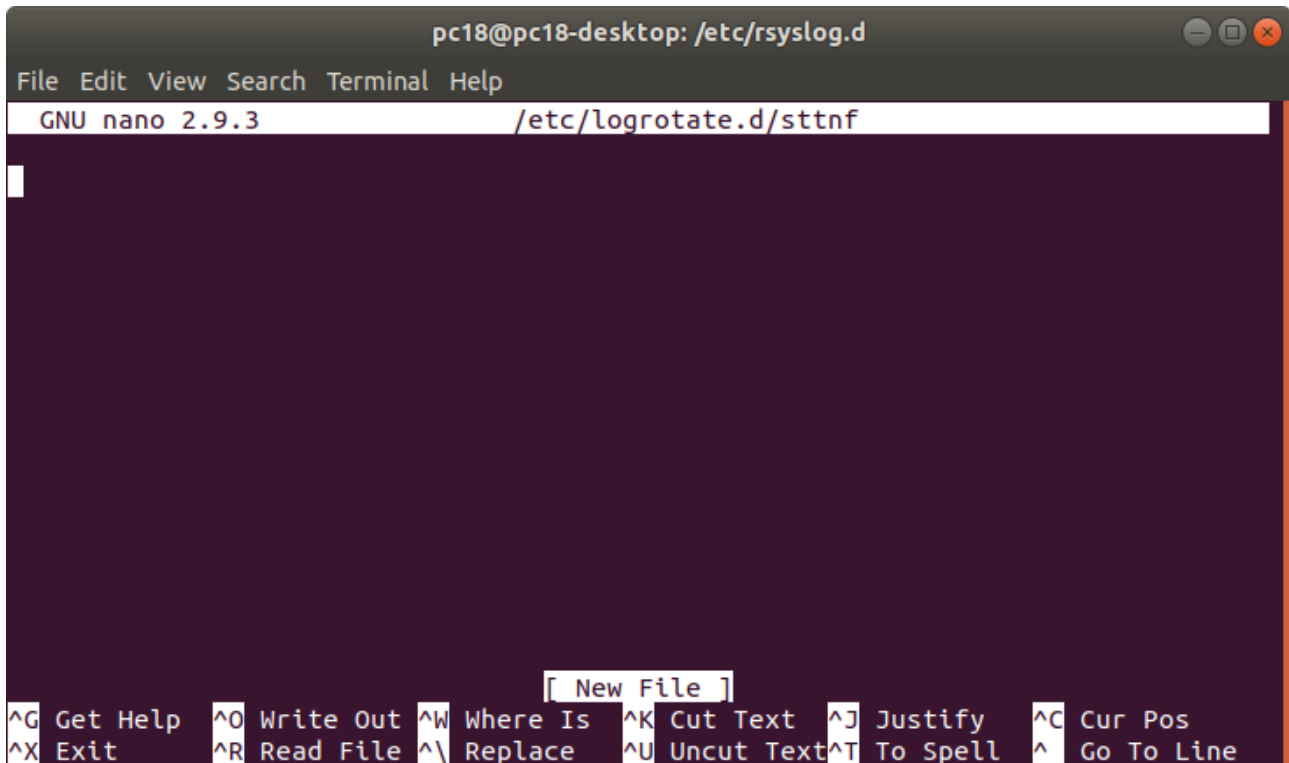
```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/syslog | grep Logout
pc18@pc18-desktop:/etc/rsyslog.d$
```

## 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`
- Ketikkan perintah berikut untuk membuat file

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo nano /etc/logrotate.d/sttnf
```

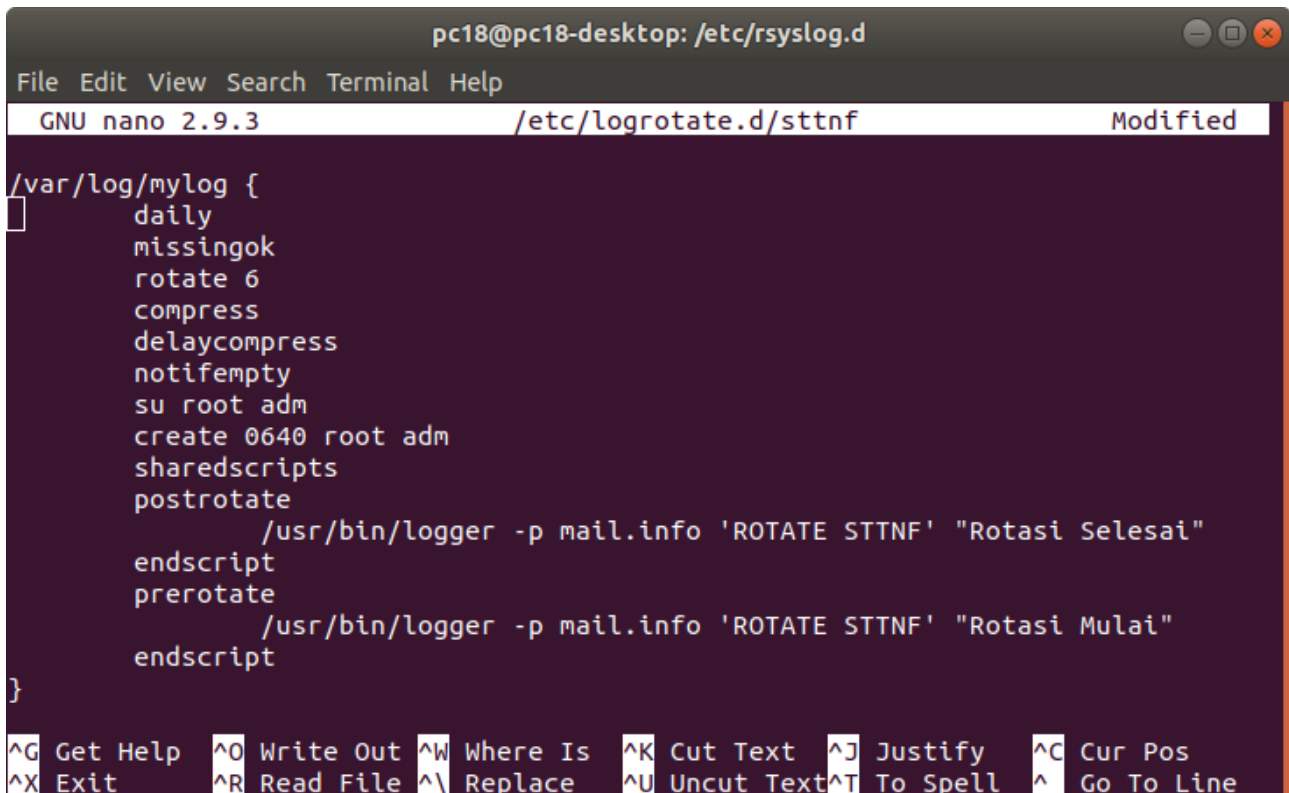
- Jika filenya masih baru maka akan kosong



```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/logrotate.d/sttnf

[ New File ]
^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
```

3. Kemudian tuliskan baris berikut ini kedalam file tersebut:



```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/logrotate.d/sttnf Modified

/var/log/mylog {
    daily
    missingok
    rotate 6
    compress
    delaycompress
    notifempty
    su root adm
    create 0640 root adm
    sharedscripts
    postrotate
        /usr/bin/logger -p mail.info 'ROTATE STTNF' "Rotasi Selesai"
    endscript
    prerotate
        /usr/bin/logger -p mail.info 'ROTATE STTNF' "Rotasi Mulai"
    endscript
}

^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
```

4. Kemudian lakukan rotasi secara paksa dengan perintah berikut ini:

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo logrotate -f /etc/logrotate.d/sttnf
pc18@pc18-desktop:/etc/rsyslog.d$
```

5. Lihat dalam direktori /var/log file dengan nama mylog dan mylog.1

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo ls -l /var/log | grep mylog
-rw-r----- 1 root      adm          0 Des 26 09:17 mylog
-rw-r----- 1 syslog    adm      8483839 Des 26 08:42 mylog.1
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Isi file /var/log/mylog

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo cat /var/log/mylog
pc18@pc18-desktop:/etc/rsyslog.d$
```

- Isi file /var/log/mylog.1

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo tail /var/log/mylog.1
Dec 26 08:36:47 pc18-desktop ntfs-3g[4815]: Unmounting /dev/sdb (azhar)
Dec 26 08:38:45 pc18-desktop systemd[1]: Starting Cleanup of Temporary Directories...
Dec 26 08:38:45 pc18-desktop systemd[1]: Started Cleanup of Temporary Directories.
Dec 26 08:39:01 pc18-desktop systemd[1]: Starting Clean php session files...
Dec 26 08:39:02 pc18-desktop systemd[1]: Started Clean php session files.
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopping System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Stopped System Logging Service.
Dec 26 08:41:36 pc18-desktop systemd[1]: Starting System Logging Service...
Dec 26 08:41:36 pc18-desktop systemd[1]: Started System Logging Service.
Dec 26 08:42:30 pc18-desktop STT-NF: User Baru Berhasil diBuat Ke STT-NF APPS
ls /var/log | grep mylog
pc18@pc18-desktop:/etc/rsyslog.d$
```

6. Amati juga pesan log di `/var/log/syslog` apakah ada pesan "Rotasi Mulai" dan "Rotate Selesai" jika ada maka rotasi berhasil dilakukan

```
pc18@pc18-desktop: /etc/rsyslog.d
File Edit View Search Terminal Help
pc18@pc18-desktop:/etc/rsyslog.d$ sudo tail /var/log/syslog
Dec 26 09:17:01 pc18-desktop CRON[6383]: (root) CMD ( cd / && run-parts --repo
rt /etc/cron.hourly)
Dec 26 09:17:01 pc18-desktop CRON[6384]: (root) CMD (cp -rf /home/guest /tmp)
Dec 26 09:17:17 pc18-desktop pc18: ROTATE STTNF Rotasi Mulai
Dec 26 09:17:17 pc18-desktop pc18: ROTATE STTNF Rotasi Selesai
Dec 26 09:18:01 pc18-desktop CRON[6413]: (root) CMD (cp -rf /home/guest /tmp)
Dec 26 09:18:01 pc18-desktop CRON[6411]: (root) CMD (cp /var/log/auth.log /tmp)
Dec 26 09:18:01 pc18-desktop CRON[6412]: (root) CMD (cp /etc/passwd /tmp)
Dec 26 09:18:01 pc18-desktop CRON[6417]: (root) CMD (/usr/bin/wget -O /tmp/xyz1.
html https://www.nurulfikri.ac.id)
Dec 26 09:18:01 pc18-desktop CRON[6410]: (CRON) info (No MTA installed, discardi
ng output)
Dec 26 09:19:01 pc18-desktop CRON[6428]: (root) CMD (cp -rf /home/guest /tmp)
pc18@pc18-desktop:/etc/rsyslog.d$
```

-----Selesai-----

## Referensi

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