PRAKTIKUM MENGELOLA LOG

Lab 1. Memeriksa paket rsyslog

- Untuk memeriksa apakah paket rsyslog sudah terinstal atau belum, Anda dapat menjalankan perintah berikut:
  ```
  $ dpkg -l rsyslog atau
  $ apt list rsyslog
  ```
- Apabila paket rsyslog belum diinstal, jalankan perintah berikut untuk menginstalnya:
  ```
  $ sudo apt install rsyslog
  ```

Lab 2. Memeriksa service rsyslog

- Untuk memeriksa apakah service rsyslog sudah berjalan atau belum maka Anda dapat memeriksanya dengan menjalankan perintah berikut:
  ```
  $ systemctl status rsyslog
  ```
- Jika service rsyslog belum berjalan, Anda dapat menjalankannya dengan perintah sebagai berikut:
  ```
  $ sudo systemctl start rsyslog
  ```

Lab 3. Konfigurasi rsyslog - mendefiniskan log spesifik

- Temukan file konfigurasi rsyslog di direktori /etc
  - File konfigurasi utama rsyslog adalah /etc/rsyslog.conf
  - File-file dalam direktori /etc/rsyslog.d, merupakan file-file konfigurasi spesifik
- Buatlah file dengan nama 10-mylog.conf di dalam direktori /etc/rsyslog.d/
- Isi file 10-mylog.conf adalah sebagai berikut:
  ```
  daemon.info           /var/log/mylog
  ```
- Kemudian restart service rsyslog dengan perintah berikut ini:
  ```
  $ sudo systemctl restart rsyslog
  ```
- 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 'Pesantren PeTIK' "New user have been added to PeTIK App"
  ```
- Amati isi dari file /var/log/mylog, dengan perintah :
  ```
  # tail /var/log/mylog
  ```
- Perhatikan juga apakah pesan tersebut tercatat dalam file log lainnya seperti dalam file /var/log/syslog?

Lab 4. Konfigurasi rsyslog – mengirimkan pesan ke user yang login

- Suatu pesan log dari suatu fasilitas dengan priority tertentu atau keseluruhan dapat dikirimkan ke *console* dimana user tersebut login
- Coba Anda ubah isi dari file /etc/rsyslog.d/10-mylog.conf, sehingga menjadi seperti berikut ini:
  ```
  daemon.info     /var/log/mylog
  daemon.info     action(type="omusrmsg" users="dudi")
  ```
- Kemudian restart service rsyslog
  ```
  $ sudo systemctl restart rsyslog
  ```
- Jangan lupa untuk mengaktifkan akses untuk menulis ke console demgan perintah berikut:
  ```
  $ mesg y
  ```
- 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 'PeTIK' "User Logout"
  ```

- Perhatikan juga apakah pesan tersebut tampil di console dimana user dudi login?

Lab 5. 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 ke dalam suatu file tertentu oleh rsyslog, dapat Anda terapkan dengan memanfaatkan fitur yang tersedia dari rsyslog.
- Contoh Anda menginginkan rsyslog menerima pesan dari aplikasi atau program bernama 'PeTIK' dan dengan isi pesan mengandung kata 'logout', yang akan dicatat oleh rsyslog ke dalam file /var/log/petik-logout .
- Buatlah file /etc/rsyslog.d/05-petik.conf, kemudian isi dengan baris berikut ini:
```
if $programname == 'PeTIK' and $msg contains 'logout' then
/var/log/petik-logout
```
- Restart service rsyslog
```
$ sudo systemctl restart rsyslog
```
- Kemudian coba kirim pesan log seolah-olah dari program PeTIK menggunakan tool logger seperti berikut ini:
```
# logger -p daemon.info -t 'petik' "user have been logout sir"
```
- Amati apa yang terjadi pada file /var/log/petik-logout? Dan bagaimana pada file /var/log/syslog?
- Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:
```
# logger -p daemon.info -t 'PeTIK' "user have been login sir"
```
- Amati apa yang terjadi pada file /var/log/petik-logout? Dan bagaimana pada file /var/log/syslog?
- Kemudian coba lakukan lagi pengiriman pesan log dengan perintah berikut ini:
```
# logger -p daemon.info -t 'PeTIK' "user have been logout sir"
```
- Amati apa yang terjadi pada file /var/log/petik-logout? Dan bagaimana pada file /var/log/syslog?

Lab 6. Konfigurasi rotasi log

- Atur rotasi log dari file /var/log/mylog agar dilakukan rotasi per hari, dan file rotasi dijaga sampai 6 rotasi
- Buatlah file dengan nama petik di dalam direktori /etc/logrotate.d
- Kemudian tuliskan baris berikut ini ke dalam file tersebut:

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

- Kemudian lakukan rotasi secara paksa dengan perintah berikut ini:
```
# logrotate -f /etc/logrotate.d/petik
```
- Lihat dalam direktori /var/log file dengan nama mylog dan mylog.1?
- Amati juga pesan log di /var/log/maillog apakah ada pesan "Rotate starting" dan "Rotate done"