Øvelse 13 – rsyslog og konfigurationsfiler

Information

Formålet med følgende øvelse er at introducere **rsyslogs primære konfigurationsfil**, hvor konfigurationer for rsyslog kan ændres.

De fleste Linux-distributioner i dag har to log-daemons (applikationsprocesser), som logger parallelt med hinanden: **rsyslogd** og **journald**. Den praktiske forskel mellem de to log-daemons er, at **rsyslogd** logger i tekstfiler, hvorimod **journald** logger i binære filer.

I faget **systemsikkerhed** arbejdes der primært med **rsyslog** i Ubuntu Linux.

Logfiler indeholder ofte følsomme oplysninger om systemets aktivitet. Derfor er det vigtigt, at kun autoriserede brugere har adgang til dem, og at logsystemet er korrekt konfigureret.

Instruktioner

1 Opsætning af locate til søgning

Kommandoen `find` er god til at søge efter filer på systemet, men værktøjet `locate` kan også anvendes.

Kommandoen `locate` bruges til hurtigt at finde filer på systemet.
I modsætning til `find` søger `locate` i en database over filer på systemet, hvilket gør søgningen meget hurtigere.

1. Installer `locate` med kommandoen `apt install locate`
2. Opdater "Files on disk"-databasen med kommandoen: `sudo updatedb`

> **Bemærk:**
> `locate` benytter en database, der ikke opdateres automatisk. Derfor skal du køre `sudo updatedb`, før nye filer vises i søgeresultaterne.

---

2 Skab et overblik over rsyslog-filerne på operativsystemet

I dette trin skal du finde filer relateret til **rsyslog** for at få et overblik over, hvor logsystemets konfiguration og komponenter befinder sig.

1. Brug `locate` til at finde alle filer med ordet *rsyslog*: `locate rsyslog`
2. Undersøg resultatet og overvej følgende:
   - Er der mange tilknyttede filer?
   - Kan du se, hvilke mapper de primært befinder sig i?

Nu burde du have et overblik over, hvor på systemet rsyslog-filer og konfigurationer typisk er placeret.

---

3 Rsyslog-konfigurationsfilen

Rsyslog-konfigurationsfilen indeholder den generelle opsætning af **rsyslog-daemonen**, herunder hvem der ejer logfilerne, og hvilken gruppe der er tilknyttet dem.

Filen indeholder også en **modulopsætning**. Moduler er ekstra funktionaliteter, som kan tilføjes til rsyslog, f.eks. netværkslogning eller integration med andre systemer.

1. Brug `locate` til at finde konfigurationsfilen:

   ```
   locate rsyslog.conf
   ```

2. Åbn konfigurationsfilen:

   ```
   nano /etc/rsyslog.conf
   ```

3. I konfigurations filen, Find afsnittet "**Set the default permissions for all log files**".
4. Notér:
   - Hvem der er filernes **ejer**
   - Hvilken **gruppe** logfilerne er tilknyttet
5. Udforsk andre områder af konfigurationsfilen. Særligt interessante sektioner:
   - **Moduler**
     Eksempel: `module(load="imudp")` – hvilke moduler er aktiveret?
   - **Andre konfigurationer**
     Hvilke andre indstillinger kan ændres i filen?
   - **Logregler**
     Er der information om, hvilken mappe eller fil der bruges til at definere **rsyslog-regler**?

Nu burde du have fået et overblik over, hvordan rsyslog konfigureres, samt hvor regler og moduler for logning defineres i systemet.

---

4 Kontroller rsyslog-servicen

Rsyslog kører som en systemservice på Linux-systemet.

I dette trin skal du kontrollere, om rsyslog-servicen kører korrekt.

1. Kontroller status for rsyslog-servicen:

```
sudo systemctl status rsyslog
```

2. Undersøg outputtet og noter:
   - Om servicen **kører**
   - Hvornår den sidst blev startet
   - Eventuelle fejlmeddelelser

Nu burde du kunne verificere, at rsyslog-servicen kører korrekt på systemet.

Sikkerhed & fejlfinding

- Hvorfor er det vigtigt, at kun bestemte brugere har adgang til logfiler?
- Hvordan kan man beskytte logfiler mod manipulation?

Refleksion

- Hvorfor er det vigtigt at have korrekte tilladelser på logfiler?
- Hvordan kan du bruge logs til at overvåge sikkerhedsrelaterede hændelser på systemet?

Links

- rsyslog Documentation
- systemctl manual

Last update: 2026-03-20 13:58:28