Øvelse 14 – Ændring af logging-regler i rsyslog

Information

Formålet med denne øvelse er at introducere rsyslog-filen **50-default.conf**, og hvordan man kan ændre rsyslog-konfigurationen.

Typisk når der laves konfigurationsændringer i rsyslog, anvendes filer i mappen **/etc/rsyslog.d/**. En af de vigtigste standardfiler er **50-default.conf**, som indeholder mange af systemets standardregler for logning.

Reglerne for, hvad rsyslog skal logge, findes i konfigurationsfilen:

```
/etc/rsyslog.d/50-default.conf
```

Rsyslog bruges til at styre, hvor systemets logbeskeder gemmes, og hvilke typer beskeder der logges. Dette er afgørende for:

- **fejlfinding**
- **overvågning af systemaktivitet**
- **sikkerhedslogging**

Ved at ændre konfigurationsreglerne kan man eksempelvis:

- **separere logs fra forskellige tjenester** for at gøre fejlfinding lettere
- **bestemme logniveauer** for at fokusere på relevante beskeder
- **opbevare sikkerhedsrelaterede logs** separat for bedre beskyttelse

---

Hvorfor ændrer vi ikke direkte i `rsyslog.conf`?

Det er **bedre praksis** at håndtere konfigurationer via separate filer i **/etc/rsyslog.d/** i stedet for at redigere `rsyslog.conf` direkte.

Fordele ved denne metode:

1. **Modularitet og overblik**
   Hver tjeneste eller funktion kan have sin egen konfigurationsfil.
2. **Opdateringssikkerhed**
   `rsyslog.conf` kan blive overskrevet ved systemopdateringer.

3. **Bedre fejlhåndtering**
   Fejl i en konfigurationsfil påvirker ikke nødvendigvis hele systemet.
4. **Standardisering**
   `rsyslog.conf` fungerer primært som en hovedfil, der inkluderer andre konfigurationsfiler.
5. **Lettere rollback og versionsstyring**
   Ændringer kan testes og rulles tilbage.

Instruktioner

1 Find og analyser rsyslog-konfigurationsfilen

1. Find filen **50-default.conf**:

   ```
   locate 50-default.conf
   ```

   Hvis `locate` ikke finder filen, brug:

   ```
   find /etc/rsyslog.d/ -name "50-default.conf"
   ```

2. Åbn filen:

   ```
   sudo nano /etc/rsyslog.d/50-default.conf
   ```

3. Skab et overblik over de logfiler, som systemets beskeder sendes til.
4. Notér, hvilke filer **mail-applikationen** sender logbeskeder til ved prioriteringerne:
   - info
   - warning
   - err

Tip: Brug følgende kommando til at filtrere konfigurationen:

```
grep "^mail." /etc/rsyslog.d/50-default.conf
```

Nu burde du have et overblik over, hvordan rsyslogs standardregler bestemmer, hvor logbeskeder gemmes.

---

2 Ændring af rsyslog-konfiguration

I denne del skal **SSH-loginforsøg logges til en separat fil** for bedre sikkerhedsovervågning.

---

1. Opret en ny rsyslog-konfigurationsfil

```
sudo nano /etc/rsyslog.d/50-ssh.conf
```

---

2. Tilføj følgende linje

```
authpriv.*    /var/log/ssh.log
```

Bemærk

- `authpriv` anvendes til autentificeringsrelaterede logs (bl.a. SSH)
- `*` betyder alle logniveauer

---

3. Opret logfilen og sæt korrekte tilladelser

```
sudo touch /var/log/ssh.log
sudo chown syslog:adm /var/log/ssh.log
sudo chmod 640 /var/log/ssh.log
```

Dette sikrer, at logfilen kun kan læses af autoriserede brugere.

---

4. Kontroller at SSH sender logs til syslog

Åbn SSH-konfigurationen:

```
sudo nano /etc/ssh/sshd_config
```

Find eller tilføj følgende linje:

```
SyslogFacility AUTHPRIV
```

---

5. Genstart tjenester

```
sudo systemctl restart rsyslog
sudo systemctl restart ssh
```

---

6. Test ændringen

Start et SSH-login:

```
ssh brugernavn@server-ip
```

Se derefter logfilen:

```
tail -f /var/log/ssh.log
```

---

7. Fejlsøgning

Tjek rsyslog-status:

```
sudo systemctl status rsyslog
```

Valider rsyslog-konfigurationen:

```
sudo rsyslogd -N1
```

Test manuel logbesked:

```
logger -p authpriv.info "Test SSH logging"
```

Se resultatet:

```
tail -f /var/log/ssh.log
```

Undersøg også auth.log:

```
sudo grep sshd /var/log/auth.log | tail -n 10
```

Sikkerhed & fejlfinding

- Hvorfor er det vigtigt, at kun bestemte brugere har adgang til logfiler?
- Hvordan kan man beskytte logfiler mod manipulation?
- Hvad sker der, hvis systemet logger for mange detaljer?

Refleksion

- Hvordan kunne du ændre logging-reglerne, så mail-logs sendes til en separat fil?

- Hvorfor er det vigtigt at kontrollere tilladelser på logfiler?
- Hvordan kan du bruge logs til at overvåge sikkerhedsrelaterede hændelser?
- Hvilke logs ville være kritiske at bevare ved kompromittering?

Links

rsyslog Documentation

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