Opgave 14 - Logging regler for rsyslog kan ændres

Information

Formålet med denne øvelse, er at introducer Rsyslog filen `50-default.conf`, og hvordan man kan lave ændringer i Rsyslog konfigurationen. Typisk når der laves konfigurations ændringer i RSyslog anvendes denne file (Hvilket bliver beskrevet senere i opgaven).

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 og sikkerhedslogging**. Ved at ændre konfigurationsreglerne kan man: - **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 en **bedre praksis** at håndtere konfigurationer via separate filer i **`/etc/rsyslog.d/`** i stedet for at redigere `rsyslog.conf` direkte. Der er flere grunde til dette:

1. **Modularitet og Overblik** – Hver tjeneste eller funktion kan have sin egen konfigurationsfil, hvilket gør det lettere at vedligeholde og fejlfinde.
2. **Opdateringssikkerhed** – `rsyslog.conf` kan blive overskrevet ved en systemopdatering, mens filer i `/etc/rsyslog.d/` forbliver intakte.
3. **Bedre Fejlhåndtering** – Hvis en ændring i en separat fil laver fejl, kan du nemt deaktivere eller rette den uden at påvirke resten af systemet.
4. **Standardisering** – Mange systemer følger best practice ved at holde `rsyslog.conf` generisk og kun bruge den til at inkludere andre konfigurationsfiler.
5. **Lettere Rollback & Versionsstyring** – Ændringer i separate filer kan nemt testes, rulles tilbage eller deaktiveres uden at påvirke hele logsystemet.

Instruktioner

1. Find og analyser Rsyslog-konfigurationsfilen

1. Find filen `50-default.conf` i Rsyslog-konfigurationsmappen:

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

Hvis `locate` ikke finder filen, brug:

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

2. Åbn filen med:

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

3. Skab et overblik over alle logfiler, som der bliver sendt beskeder til.
4. Notér, hvilke filer `mail`-applikationen sender logbeskeder til, ved prioriteringerne:
   - **info**
   - **warning**
   - **err**

Tip: Brug følgende kommando for hurtigt at finde `mail`-logregler:

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

2. Ændring af Rsyslog-konfiguration

For at gøre øvelsen mere praktisk, skal du nu ændre Rsyslog-konfigurationen, så **SSH-loginforsøg** logges til en separat fil.

Dette kan være nyttigt til **sikkerhedsovervågning**, da det gør det lettere at opdage uautoriserede loginforsøg.

1. Opret en Rsyslog-konfigurationsfil

Opret en ny konfigurationsfil i `/etc/rsyslog.d/`:

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

2. Tilføj følgende linje for at gemme SSH-loginforsøg i en ny logfil

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

Bemærk: - Brug `authpriv.*` i stedet for `auth.info`, da SSH-autentificeringslogs normalt gemmes under `authpriv`.
- `*` betyder, at **alle logniveauer** (info, notice, warning osv.) inkluderes.

3. Opret logfilen med korrekte tilladelser

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

- **`chown syslog:adm`** sikrer, at `rsyslog` har adgang til at skrive til filen.

4. Sikre, at SSH sender logs til syslog

Åbn SSH-konfigurationsfilen:

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

Find (eller tilføj) følgende linje:

```
SyslogFacility AUTHPRIV
```

- **Dette sikrer, at SSH-logningen sendes til `authpriv`.**

5. Genstart nødvendige tjenester

Efter ændringerne skal vi genstarte `rsyslog` og `ssh`:

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

6. Test ændringen

Åbn en ny terminal og log ind på serveren via SSH:

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

Derefter, på serveren, tjek om der er nye logs:

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

7. Fejlsøgning (hvis logs ikke vises)

- **Tjek om rsyslog kører korrekt:**

  ```
  sudo systemctl status rsyslog
  ```

- **Valider rsyslog-konfigurationen for fejl:**

  ```
  sudo rsyslogd -N1
  ```

- **Test manuelt, om logs kan skrives til filen:**

```
logger -p authpriv.info "Test SSH logging"
tail -f /var/log/ssh.log
```

- **Sørg for, at systemet faktisk genererer SSH-logindgange:**

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

3. 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? Kan det have negative konsekvenser?

4. Refleksion

 Refleksionsopgaver:

- 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 på systemet?

Links

- rsyslog Documentation

2025-04-03 05:55:59