Opgave 13 - rsyslog og konfigurationsfiler

Information

Formålet med følgende øvelse er at introducere **Standard rsyslog-konfigurationsfilen**, hvor konfigurationer for Rsyslog kan ændres.

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

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

Instruktioner

Opsætning af `locate` til søgning

Kommandoen `find` er god til søgning af filer, men `locate` kan også med fordel anvendes.

1. Installer `locate` med kommandoen:

   ```
   sudo apt install locate
   ```

2. Opdater "Files on disk"-databasen:

   ```
   sudo updatedb
   ```

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

Skab et overblik over Rsyslog-logfilerne på operativsystemet

1. Brug `locate` til at finde alle filer med ordet `rsyslog`:

   ```
   locate rsyslog
   ```

2. Skab et generelt overblik over filerne:
3. Er der mange tilknyttede filer?
4. Kan du se, hvilke mapper de primært befinder sig i?

Rsyslog-konfigurationsfilen

Rsyslog-konfigurationsfilen indeholder den generelle opsætning af **rsyslog-daemonen**, herunder hvem der ejer logfilerne, og hvilken gruppe der er tilknyttet logfilerne. Herudover har den en **modulopsætning**. Moduler er ekstra funktionaliteter, som man kan tilføje til rsyslog.

1. Brug `locate` til at finde rsyslog-konfigurationsfilen `rsyslog.conf`:

   ```
   locate rsyslog.conf
   ```

2. Åbn filen med `nano`.
3. Find afsnittet "**Set the default permissions for all log files**".
4. Notér:
   - Hvem der er filens **ejer**.
   - Hvilken **gruppe** logfilerne er tilknyttet.
5. Udforsk de andre områder af filen. Særligt interessante sektioner:
   - **Moduler** (`module(load="imudp")`) – hvilke moduler er aktiveret?
   - **Andre konfigurationer** - Hvilken andre konfigurationer kan ændres inde i filen?
   - **File til regel ændring** - Er der information om hvilken file der ændres til at ændre Rsyslog regler?

Sikkerhed & fejlfinding

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

Refleksion

 Refleksionsopgaver:

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

Links

- rsyslog Documentation

2025-04-03 05:55:59