Øvelse 18 – Applikationslogs i Linux (Apache2)

Information

Formålet med denne øvelse er at introducere **applikationslogs** og demonstrere, hvordan en webserver som **Apache2** logger adgang til serveren.

I modsætning til systemlogs (fx `/var/log/syslog`), som indeholder generelle systemhændelser, er **applikationslogs** specifikke for den enkelte applikation og kan indeholde vigtige oplysninger om systemets brug, drift og sikkerhed.

I denne øvelse installerer du Apache2, tester webserverens funktionalitet og analyserer **adgangsloggen (`access.log`)**. Dette giver indsigt i:

- hvordan applikationslogs oprettes
- hvor de gemmes
- hvordan de kan bruges til fejlfinding og sikkerhedsanalyse

Baggrund

Applikationslogs er de logfiler, som en applikation genererer under drift.

I Apache2 registrerer **access.log** blandt andet:

- klientens IP-adresse
- tidspunkt for anmodningen
- HTTP-metode og ressource
- HTTP-statuskode
- størrelsen på svaret

En typisk Apache loglinje kan se sådan ud:

```
192.168.1.25 - - [12/Mar/2026:10:15:23 +0000] "GET /index.html HTTP/1.1" 200
10945
```

Denne linje fortæller blandt andet:

- hvilken klient der tilgik serveren
- hvilken ressource der blev anmodet om

- om anmodningen lykkedes (statuskode 200)

Formålet med øvelsen er ikke at lave en avanceret Apache-konfiguration, men at opnå en **praktisk forståelse af applikationslogning**.

Instruktioner

Husk at notere observationer og kommandoer i dit Linux cheat sheet.

---

1 Opsætning af Apache2-webserver

I dette trin installerer du Apache2 og verificerer, at webserveren fungerer.

1. Følg installationsguiden til Apache2: https://ubuntu.com/tutorials/install-and-configure-apache#1-overview
2. Verificér at Apache kører korrekt:

```
sudo systemctl status apache2
```

Hvis output viser **active (running)**, kører Apache korrekt.

---

2 Verificering af adgangslog (access.log)

I dette trin undersøger du Apache's adgangslog.

1. Udskriv indholdet af Apache's adgangslog:

```
cat /var/log/apache2/access.log
```

2. Tilgå webserveren fra en anden maskine ved at åbne en browser og indtaste:

```
http://[serverens-IP]
```

Alternativt kan du bruge `curl`:

```
curl [serverens-IP]
```

Apache kører som standard på **port 80**.

3. Udskriv de seneste loglinjer igen:

```
tail -n 10 /var/log/apache2/access.log
```

4. Verificér at IP-adressen fra den klient, du brugte, nu fremgår i loggen.

Nu burde du kunne se, hvordan en HTTP-anmodning registreres i Apache's adgangslog.

---

3 Overvågning af access.log i realtid

I dette trin overvåger du logfilen i realtid.

1. Overvåg logfilen:

```
sudo tail -f /var/log/apache2/access.log
```

2. Genindlæs websiden fra en browser eller kør `curl` flere gange.
3. Observer hvordan der tilføjes en ny loglinje for hver adgang til webserveren.

Dette viser, hvordan logfiler opdateres løbende under drift.

---

4 Undersøg andre Apache-logfiler

Apache genererer flere forskellige logfiler.

1. Undersøg hvilke logfiler der findes:

```
ls /var/log/apache2/
```

2. Identificér især følgende filer:
   - `access.log`
   - `error.log`
3. Undersøg indholdet af error-loggen:

```
tail -n 10 /var/log/apache2/error.log
```

Nu burde du have et overblik over, hvilke logfiler Apache bruger til henholdsvis **adgangsregistrering** og **fejlhåndtering**.

Sikkerhedsperspektiv

Applikationslogs spiller en vigtig rolle i sikkerhedsarbejde.

Access-logs kan blandt andet bruges til at:

- identificere mistænkelig trafik
- opdage scanning eller brute force-angreb
- analysere adgangsmønstre
- efterforske sikkerhedshændelser

Derfor er det vigtigt, at logfiler:

- beskyttes mod manipulation
- opbevares korrekt
- analyseres løbende.

Refleksionsøvelser

- Hvad er forskellen på systemlogs og applikationslogs?
- Hvorfor er adgangsloggen vigtig i forhold til sikkerhed?
- Hvilke andre logfiler findes i Apache2-mappen (`/var/log/apache2/`)?

Links

Apache logging basics

Linux log files

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