

# Opgave 18 - Applikationslogs

## Formål

Formålet med denne øvelse er at introducere applikationslogs og demonstrere, hvordan en webserver som Apache2 logger adgang til serveren. I modsætning til systemlogs, som f.eks. `/var/log/syslog`, er applikationslogs specifikke for den enkelte applikation og kan indeholde vigtige oplysninger om systemets drift og brug.

I denne opgave vil du installere og konfigurere Apache2, teste webserverens funktionalitet og analysere adgangsdagbogen (`access.log`). Dette giver indsigt i, hvordan applikationslogs lagres, og hvordan de kan bruges til fejlfinding og sikkerhedsanalyse.

## Information

Applikationslogs er de logfiler, som en applikation genererer, mens den kører på værten. I denne opgave skal du analysere logs fra webserveren Apache2. Vi fokuserer på adgangsdagbogen (`access.log`), der registrerer IP-adresser på klienter, der har tilgået serveren.

Dagens opsætning er en relativt simpel konfiguration. Formålet er at vise, hvordan applikationslogs fungerer, og hvordan de lagres som tekstfiler på værten.

Du kan få et fuldt overblik over Apache2-logning [her](#), og du kan se lokationen af Apache2-logfiler på Ubuntu i afsnittet [Application logs, her](#).

## Instruktioner

### 1. Opsætning af Apache2-webserver

1. Følg guiden til installation af Apache2-webserver [her](#).
2. Efter installationen skal du verificere, at Apache kører korrekt ved at eksekvere:

```
sudo systemctl status apache2
```

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

### 2. Verificering af adgangsdagbog

1. Udskriv indholdet af Apache's adgangsdagbog, som findes i:

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

2. Besøg serverens IP-adresse fra en anden enhed ved at åbne en browser og indtaste:

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

eller anvend *curl*:

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

Apache kører som standard på port 80, så du behøver ikke angive portnummeret i URL'en eller ip.

3. Verificer, at den seneste linje i `access.log` indeholder IP-adressen på den enhed, du brugte til at tilgå webserveren.

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

### 3. Overvågning af access.log i realtid

For at overvåge logfilen i realtid, kørs:

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

Mens denne kommando kører, kan du genindlæse websiden fra en anden maskine. Du bør se en ny linje tilføjet i loggen for hver adgang.

### 4. Refleksion over applikationslogs

Mange af de tidligere opgaver har fokuseret på systemlogs, men det er vigtigt at huske, at applikationer ofte har deres egne logfiler.

- Applikationer har ofte deres egne **adgangsrettigheder**, hvilket påvirker, hvordan logs genereres og tilgås.
- Applikationslogs kan bruges til **fejlfinding** og **sikkerhedsovervågning**, da de indeholder oplysninger om systemets brug.

## Refleksion

### ▮ Refleksionsopgaver:

- Hvad er forskellen mellem systemlogs og applikationslogs?
- Hvorfor kan adgangsløgen være vigtig for både fejlfinding og sikkerhed?
- Hvilke andre logfiler findes i Apache2? (Tjek indholdet af `/var/log/apache2/`)

- Hvem har adgang til Apache-logfilerne, og hvordan kan de beskyttes?

## Links

- [Apache logging basics](#)
- [Linux log files](#)

🕒 2025-04-03 05:55:59