Lektion 12 – Laboration 1

Analysera loggfiler utan att skripta

- Skapa en Apache - loggfil med verktyget från Lektion 11, Laboration 2.
  - Det går bra att återanvända en tidigare fil!
- Använd **zcat**, **cut**, **sort**, **uniq**, **grep**, **head** och **tail** för att lösa uppgifterna nedan.
- Skriv inte ett skript där ni loopar et.c. Använd kommandoraden direkt.
- Använd inte **awk**, **perl**, etc, som vi inte använt i kursen.
  - (Du borde alltså inte behöva googla)

1: Hitta de mest aktiva ip-näten

Vi vill ta reda på vilka ”/16” – nät som varit mest aktiva på vår webbserver. Vi vill med andra ord hitta de rader i loggen med flest dubbletter i de två första oktetterna i ip-adressen.

Exempelvis för adressen ”10.20.30.40” vill vi bara titta på ”10.20” i vår jämförelse.

Exempelutskrift:

```
      4 57.18
      3 97.181
      3 96.153
      3 92.231
      3 80.129
      3 76.152
      3 68.172
```

2: Hitta antalet anrop för varje HTTP-metod

I en logg-rad som:

```
110.79.215.157 - - [20/Mar/2021:15:56:10 +0000] "GET /explore HTTP/1.0" 200 4972
```

är ”GET” metoden.

Vi vill nu räkna samman hur många gånger olika metoder anropats.

Exempelutskrift:

```
    969 DELETE
   6009 GET
   1003 POST
   2019 PUT
```

Tips: Du borde kunna lösa uppgiften med cut, cut, sort och uniq.

3: Hitta de tjänster som får flest HTTP 301 Moved Permanently

Vi har fått en förfrågan från utvecklingsteamet. De felsöker alla tjänster som returnerar redirect. och undrar följande:

- Hur stor del av alla serveranrop till ”/portals” blir ”redirectade”?
- Är det någon skillnad i storlek på svaren för anrop som besvaras med ”redirect” mot andra svar?

Tips:

- Eftersom förfrågan är en one-off är det ingen idé att börja skripta, men en fråga kanske kräver mer än en ”körning”, alltså flera olika kommandon för att få fram svaret.
- Det är ok att använda ”miniräknare” för att kombinera resultat och få fram ett svar.
- Vi räknar med alla anrop oavsett anrops-method (GET, HEAD, POST, PUT) om inget annat anges.
- Vi räknar alla svar med statuskod ”301” som ”redirects”.
- Det räcker inte att greppa hela loggrader efter ”301”, eftersom siffran förekommer på andra ställen än just status-fältet.
- Gå steg-för-steg och kontrollera resultatet i less med en pipe innan du går vidare.