Afgangsprojekt for Informationsteknologi

Jakob Viggo Hansen – **Problemformulering** – 2022-09-13

I store virksomheder hvis virke er baseret på adskillige samarbejdende IT-systemer, er overvågning af drift og stabilitet en udfordring. Mange systemer kan udsende alarmer i tilfælde af driftsforstyrrelser eller stop. Men en enkeltstående alarm-melding vil ofte ikke afsløre det samlede billede af det påvirkede system. **Det er vanskeligt at udlede kontekst og underliggende drift status.**  
  
Desuden er diskrete systemer næsten altid blot komponenter i en længere kæde, et workflow eller data-flow. En fejl i et enkelt system skyldes ofte fejl i systemer som er placeret tidligere i kæden. Eller systemer senere i kæden kan lide under det aktuelle systems fejl.  
  
**Alle disse systemer genererer drifts-logs - ofte adskillige tusind linjer pr time.**Logs er indgangen til at udlede et billede af systemets tilstand, aktuelt og bagud i tiden.

**Men det kan være vanskeligt og tidskrævende at gennemlæse mange tusind loglinjer**, og vanskeligt at sammenstille de informationer som fremsøges, på tværs af tid og systemer. Overblikket kan drukne i mængden af data.

Jeg foreslår at udvikle en hjælpe-applikation, **LogWatcher**.

**LogWatcher er målrettet til personer som skal supportere og drifte virksomhedens system-park.**  
LogWatcher skal kunne hjælpe brugeren med at søge efter tekst-billeder på tværs af mange systemers logs. Baseret på søgeord og tidsgrænser skal LogWatcher hjælpe sin bruger med at danne sig et overblik over hændelser og deres tidslige distribution.  
  
LogWatcher skal have en **grafisk brugerflade** baseret på en HTML-side, tilgængelig via en standard web-browser. GUI'en skal facilitere **indsamling** af logs fra forbundne systemer, **gennemsøgning** af logs på basis af søge-termer og tidshorisonter, og **udstille** resultaterne fra søgningerne.  
  
Forud for selve søgningen skal de indsamlede logs persisteres til en **database**, som derefter vil udgøre det data-grundlag som LogWatcher skal traversere.  
  
**Søge-algoritmerne** skal være baseret på trie's og binære søgetræer, for at sikre god performance når brugeren potentielt skal søge over mange tusinde linjer rå log-data. Søge-komponenten bør udstille et \***eDSL** til at facilitere søgning i domænet.  
  
Søge-resultater kan udstilles som tekst-udsnit fra søge-hits. F.eks

* top-5 af systemer med søgeordene repræsenteret i deres logs.
* et grafisk billede af den tidslige distribution af et sæt søgeord (f.eks. over de seneste 48 timer)

**Ved hjælp fra LogWatcher kan brugerne altså hurtigere danne sig et overblik over begivenheder på tværs af systemer, og få hjælp til at danne en forståelse af hvor de underliggende problemer kan være opstået i den lange kæde af indbyrdes forbundne systemer.**

*\*Embedded Domain Specific Language*