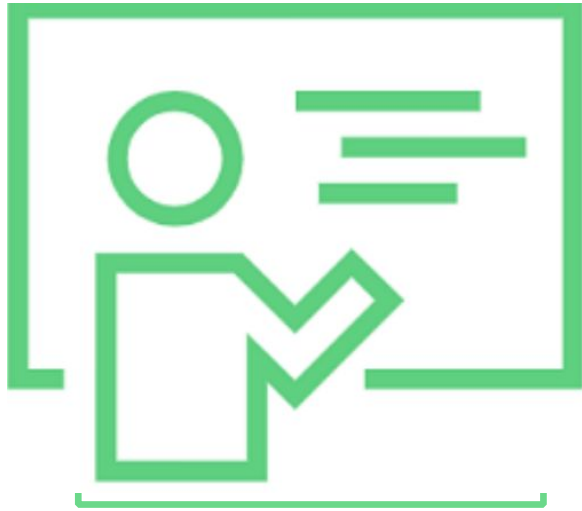




Loggning och övervakning

Joakim Englund, Systemmentor AB

Repetition från dag 8

- Flera tasks producerade händelser
- Timers bestämde när arbetet startade
- Kön skilde produktion från publicering
- Räknare och event visade återanslutning

Dagens mål

- Skriva sökbara, strukturerade loggar
- Definiera relevanta räknare och svarstider
- Knyta ihop klient och server med korrelations-ID
- Jämföra logg, dashboard och nätverkstrafik
- Skriva en reproducerbar felsökningsguide

Observerbarhet

"Det fungerar inte"



Vad? När? Var? Hur ofta? Hur långsamt?

- Ett distribuerat fel kan ligga i klient, nät, broker, API eller lagring
- Vi behöver synliga signaler från flera områden

Olika signaler

<i>Signal</i>	<i>Svarar främst på</i>
Logg	Vad hände i ett specifikt förlopp?
Mätetal	Hur mycket, hur ofta och hur långsamt?
Nätverksspår	Vad passerade gränssnittet?

Exempel på en bra logghändelse

I JSON:

```
{  
  "timestamp": "2026-09-22T08:21:04.123Z",  
  "level": "WARNING",  
  "event": "reading_rejected",  
  "request_id": "lab-invalid-1",  
  "status": 400,  
  "duration_ms": 0.42,  
  "reason": "value must be a positive number"  
}
```

Tidsstämpel och klocka

- Använd UTC och skriv tidszon
- Använd samma format i alla komponenter
- Synkronisera enheternas klockor
- Mät duration med monoton klocka (tänk tidtagarur)

En monoton klocka är en klocka som bara går framåt medan en vanlig klocka kan justeras pga tidssynkronisering, byte av tidszon, eller att man ställer om klockan (sommars-/vintertid).

Loggnivå är betydelse

<i>Nivå</i>	<i>Exempel</i>
DEBUG	Tillfällig diagnosdetalj
INFO	Mätning accepterad
WARNING	Ogiltig indata avvisad
ERROR	Begärt arbete misslyckades

Korrelations-ID

- Är en konsekvent meddelande-ID som följer ett meddelande genom systemet
- Klienten skickar ett ID eller servern skapar ett
- Samma ID returneras och loggas
- ID:t är inte ett lösenord och ska inte innehålla persondata

Logga inte hemligheter

Samma påminnelse vi drar typ varje tillfälle, men..

Logga inte:

- Lösenord eller access-token
- Privata nycklar
- Hela certifikat i varje händelse
- Onödig persondata
- Obegränsad sensordata utan syfte och retention

Fundera först, välj mätetal sedan

Fråga	Mätetal
Kommer data fram?	Accepterade mätningar
Avvisas indata?	Valideringsfel
Är tjänsten långsam?	Svarstid i ms
Tappar enheten kontakt?	Återanslutningar
Växer kön?	Aktuell/maximal ködjup

Undvik mätetal bara för att de är enkla att samla.

Räknare, mätare och duration

- Räknare: ökar, exempel ``requests_total``
- Mätare: kan gå upp och ned, exempel ``queue_depth``
- Duration: mäts mellan tydliga start- och slutpunkter

En omstart kan nollställa processens räknare. Dashboarden bör därför visa uptime eller starttid.

Total, takt och andel

feltakt = Δ valideringsfel / Δ tid

felandel = valideringsfel / alla relevanta anrop

- Totalen sedan start saknar tidskontext
- Nämnare och mätintervall måste framgå

Medelvärde kan dölja toppar

Svarstider: 10, 11, 12, 13, 500 ms

Medel: 109,2 ms

Max: 500 ms

- Visa minst antal mätningar och enhet
- Maxvärde visar topp men inte fördelning
- Percentiler är en fördjupning

Dashboarden är en vy

Tjänst → /api/metrics → Dashboard/metrics → Verktyg/människa

- Samma definitioner bakom alla vyer
- Uppdateringsintervall ska vara synligt
- En tom panel kan betyda mätfel, inte noll

Demons fysiska och logiska roller

- Terminal 1: Server/gateway med logg och mätetal
- Terminal 2: Simulerad sensorenhet
- Terminal 3, valfri: Passiv nätverksobservatör

Filtrera rätt trafik

Capture filter: tcp port 8090

Display filter: tcp.port == 8090 && http

- Capture filter begränsar vad som samlas in
- Display filter begränsar vad som visas
- Porten avgränsar demon från annan trafik

Vad ser vi med TLS?

<i>Kan normalt ses</i>	<i>Skyddas av TLS</i>
IP-adresser och portar	HTTP/MQTT-nyttolast
Tidpunkter och paketstorlekar	Headers och topic inne i tunneln
Att en anslutning upprättas	Sensorvärden och token

Ett reproducerbart fel

För labben och caset

1. Beskriv startläge och version
2. Ange exakta steg och testdata
3. Skriv förväntat resultat
4. Skriv observerat resultat
5. Bifoga minsta relevanta bevis
6. Återställ och upprepa

Laborationens definition av klar

- Minst en strukturerad logghändelse
- Minst ett definierat mätetal
- Normalfall och avsiktligt fel dokumenterade
- Samma scenario synligt i minst två beviskällor
- Extra, men bra om ni gör: Guide verifierad av annan grupp