SLA Breach Detector

Microservizio che monitora metriche (esposte dai microservizi via Prometheus) e rileva violazioni di soglie SLA definite per ciascuna metrica di tipo GAUGE definita nel progetto.

Requisiti funzionali

1. **Caricamento configurazione all'avvio**
   All'avvio legge un file di configurazione SLA (YAML o JSON) che contiene, per ogni metrica GAUGE monitorata: nome metrica, query PromQL, min, max

2. **Campionamento periodico e calcolo min/max**
   - Il servizio esegue un job periodico ogni T_check secondi.
   - Vincolo: T_check ≥ 5 × T_scrape (dove T_scrape è l'intervallo di scraping di Prometheus).
   - Ad ogni esecuzione, il servizio:
     - interroga Prometheus (HTTP API /api/v1/query) per ottenere il valore corrente della metrica (o della query PromQL associata),
     - aggiorna lo storico interno degli ultimi campioni (vedi sotto),
     - calcola il numero di campioni fuori soglia.

3. **Regola di SLA breach**
   - Per ogni metrica:
     - se almeno 3 campioni risultano < min oppure almeno 3 campioni risultano > max, genera un evento di SLA breach.

4. **Notifica breach**
   Il servizio deve supportare almeno un canale di notifica (Kafka, Telegram, email)
   Quando c'è breach, emette un evento con:
   - timestamp
   - metrica / query
   - valore osservato e soglia violata
   - contatore violazioni (sotto-min / sopra-max)

5. **API REST minime**
   - Update SLA config: aggiorna le soglie/metriche
   - Read SLA config: legge configurazione corrente

- Breach stats: restituisce quali metriche hanno avuto breach e quanti, dall’avvio del servizio