Centralizirana analiza računalnih zapisa u distribuiranim sustavima

Maja Dabčević, Željko Kovačević,
Aleksandar Stojanović, Damir Maleković

CASE 2026

Uvod

- Distribuirani sustavi sastoje se od više komponenti koje međusobno komuniciraju tijekom poslovnih procesa
- Olakšano skaliranje i održavanje sustava
- Otežan nadzor sustava, praćenje događaja i identifikacija propusta
- Računalni zapisi pružaju uvid u stanje sustava, ali su raspršeni po pojedinim komponentama što otežava korelaciju složenih procesa koji obuhvaćaju zapise iz više izvora
- **Rješenje: centralizirana jedinica za obradu i pohranu zapisa**

```
"timestamp": "2026-02-25T15:21:03.428Z",
  "severity": "INFO",
    "body": "Narudžba rezervnih dijelova uspješno kreirana.",
  "traceId": "012a6b5f8671d623",
  "spanId": "84f9f038b6d3a5aa",
  "attributes": {
    "http.method": "POST",
    "http.status_code": 201,
    "user.id": "a7630ab7",
    "order.id": "342bb94e",
    "app.name": "orders-api"
  },
  "resource": {
    "service.name": "orders-api",
    "service.version": "1.4.3",
    "host.name": "api-server-1"
  }
```


Računalni zapisi

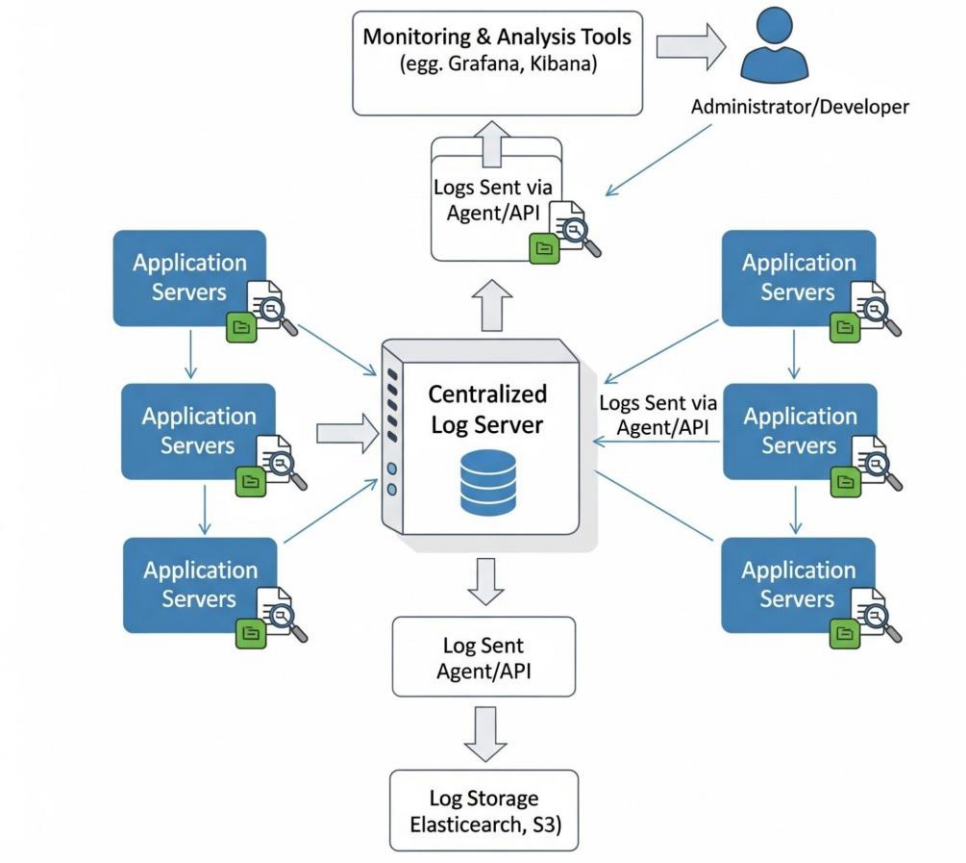
- Bilježe događaje unutar sustava – tko je, kada i gdje, što napravio
- Služe za rekonstrukciju događaja, revizorske procese, nadzor sustava, forenzičke istrage...
- Mogu sadržavati osjetljive podatke, što zahtjeva pažljivu obradu i pohranu te usklađenost s normama
- Različiti izvori (poslužitelj, aplikacija, baza...) i formati
- Često je potrebno sagledati zapise iz više izvora za razumijevanje sustava
- U slučaju kvara ili kompromitacije čvora lokalni zapisi mogu postati nedostupni ili izgubljeni

Strukturiranje računalnih zapisa

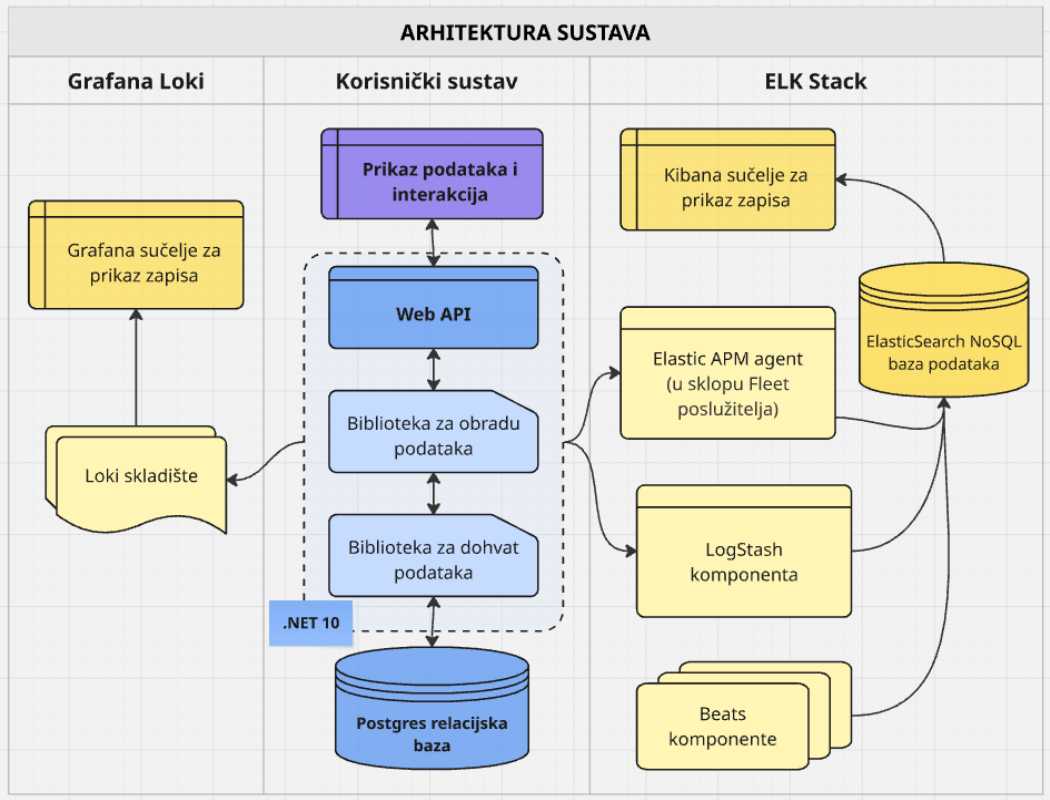
Polje	Opis
timestamp	Precizna vremenska oznaka zapisa
level	Razina zapisa. Moguće kategorije: razvojni, informacija, upozorenje, greška, kritično stanje
message	Srž zapisa; tekst koji opisuje događaj u sklopu kojeg je stvoren zapis.
correlationId	Jedinstveni identifikator zahtjeva. Može se unaprijediti u TraceID i SpanIDs
sourceContext	Podaci o klasi, modulu i metodi unutar koje je zapis kreiran.
exception	U slučaju grešaka, tekst iznimaka se sprema u posebno polje u odnosu na opis (message)
userId	Sažetak korisničkog identifikatora koji omogućuje praćenje analizu događaja po korisniku bez odavanja povjerljivih podataka.

Centralizirano zapisivanje

- Posebna komponenta za obradu i pohranu zapisa iz više izvora
- Obogaćivanja zapisa metapodacima
- Normalizacija ulaznih podataka
- Indeksiranje prilikom pohrane
- Pohranjene zapise je zatim moguće pretraživati, filtrirati i korelirati
- Vizualizacija putem prilagođenih nadzornih ploča i sustava obavijesti



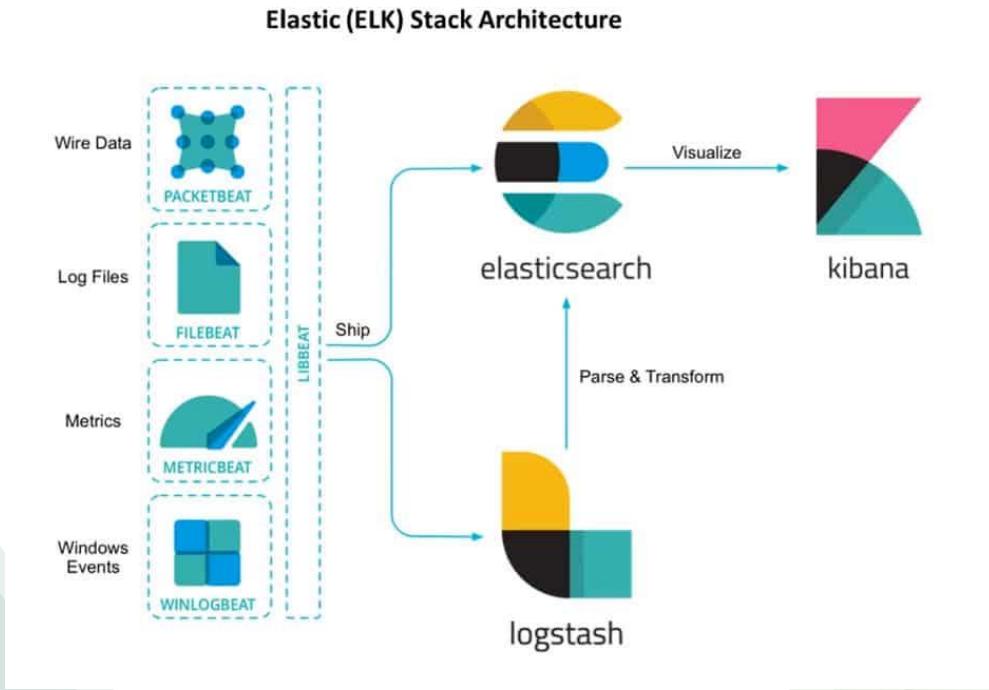
Primjer implementacije centralizirane obrade



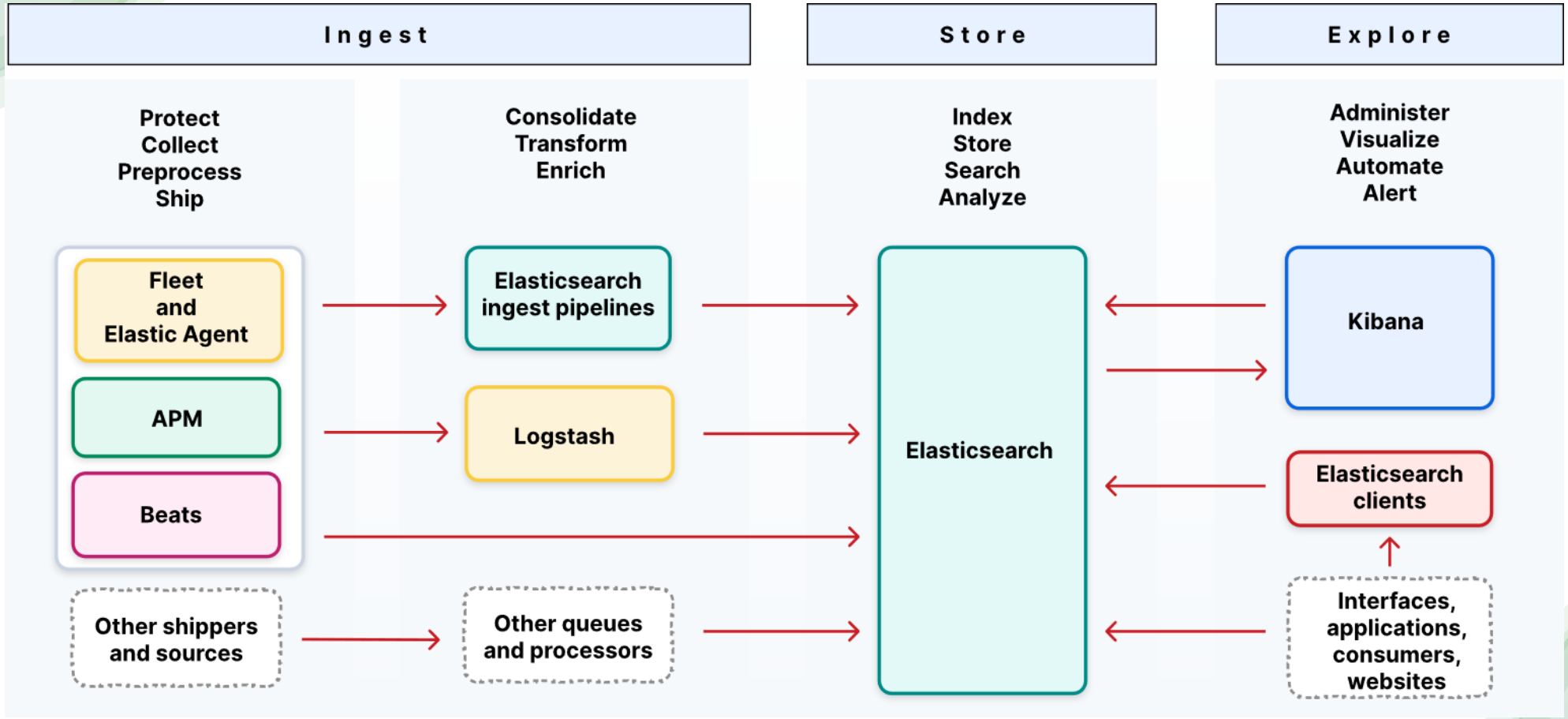
- Višeslojna web aplikacija
- Obogaćeni Serilog zapisi u JSON formatu
- Slanje genernih zapisa na dva nadzorna sustava istovremeno:
  - **ELK Stack**
  - **Grafana Loki**
- Distribuiranost je simulirana Docker kontejnerima

ELK Stack

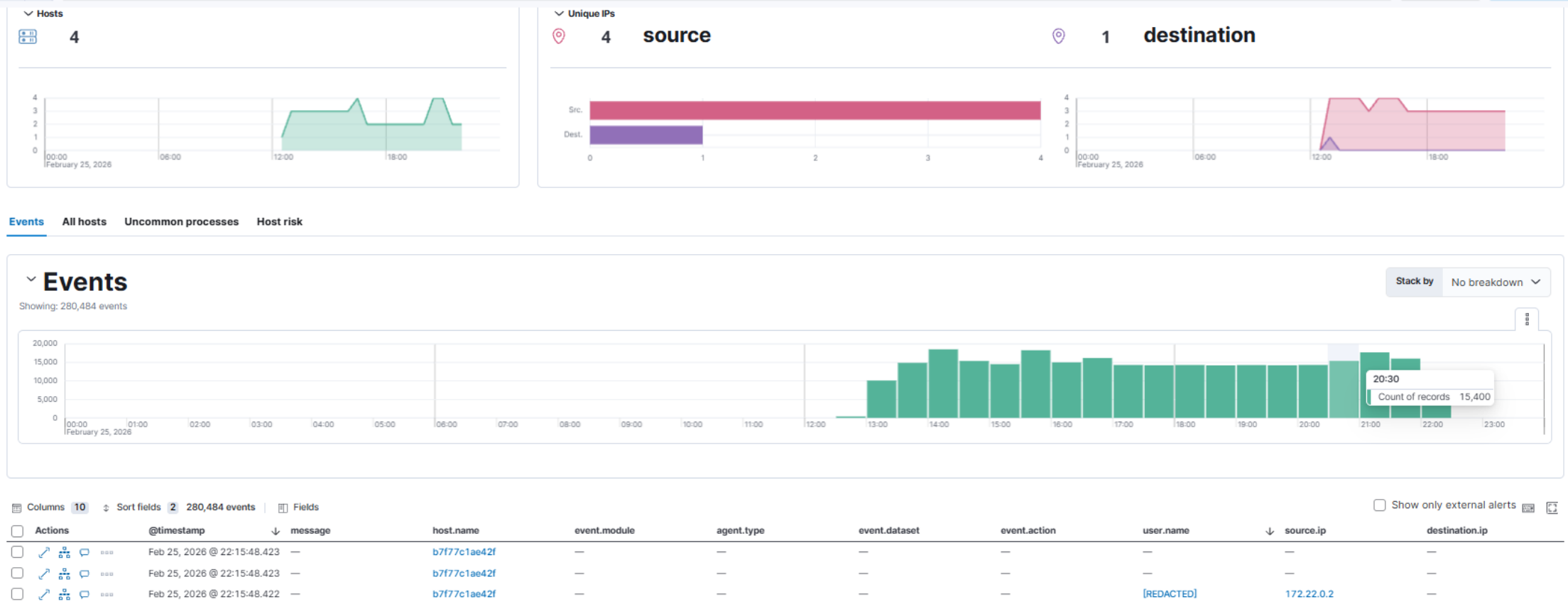
- Modularno rješenje koje se sastoji od 3 osnovne i mnoštva dodatnih komponenti za obradu zapisa
- **Elasticsearch** – dokumentno orijentirana baza podataka za obradu, indeksiranje i pohranu JSON zapisa
- **Logstash / Beats** – specijalizirane komponente za prikupljanje zapisa i metrika unutar sustava
- **Kibana** – web sučelje za vizualizaciju podataka iz ES baze
- Omogućava naprednu analitiku i obradu po poljima te složene upite, agregacije i obavijesti



ELK Stack


Ingest
Store
Explore
Protect
Collect
Preprocess
Ship
Consolidate
Transform
Enrich
Index
Store
Search
Analyze
Administer
Visualize
Automate
Alert
Fleet and Elastic Agent
APM
Beats
Other shippers and sources
Elasticsearch ingest pipelines
Logstash
Other queues and processors
Elasticsearch
Kibana
Elasticsearch clients
Interfaces, applications, consumers, websites

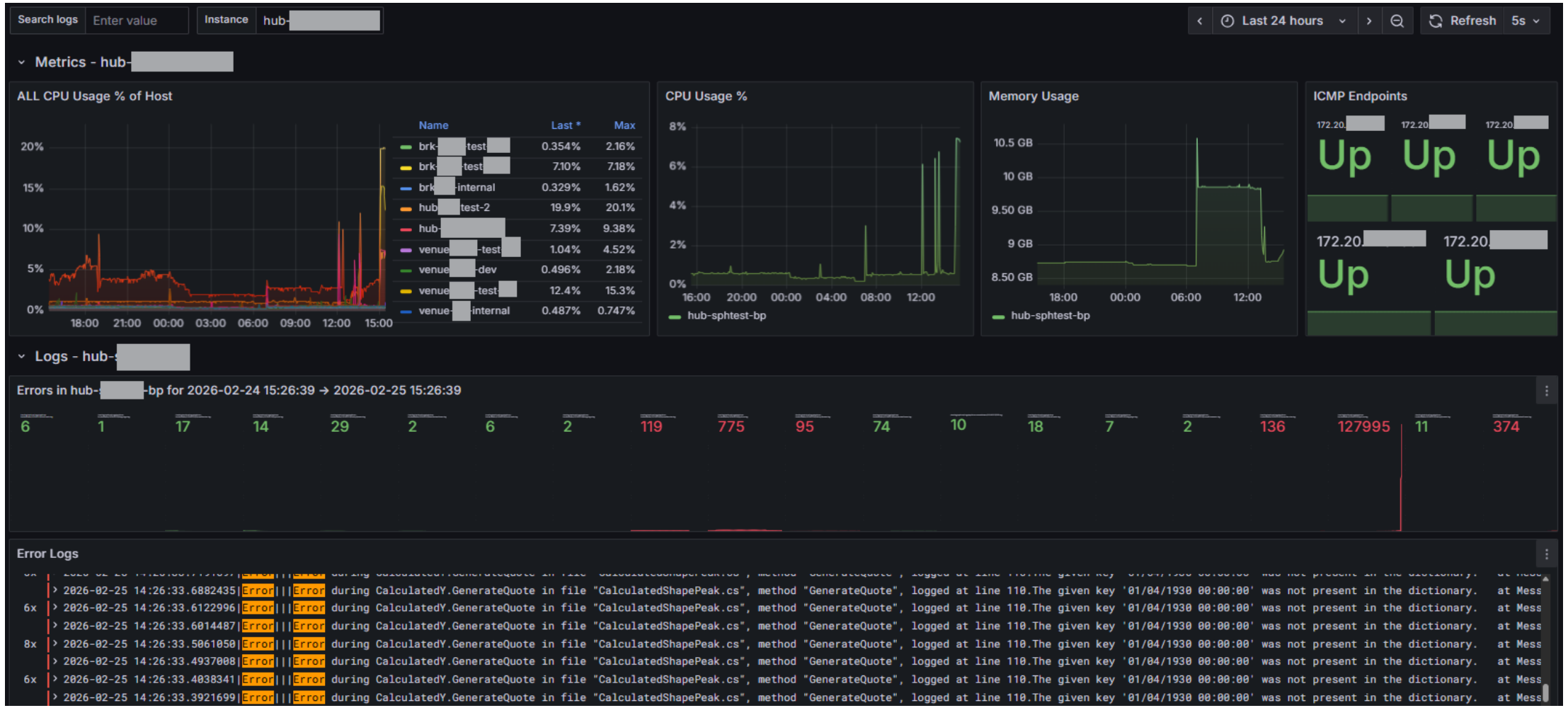
ELK Stack


Hosts
4
Unique IPs
4
source
1
destination
Src.
Dest.
Events
All hosts
Uncommon processes
Host risk
Events
Showing: 280,484 events
Stack by
No breakdown
20:30
Count of records 15,400
Columns 10
Sort fields 2
280,484 events
Fields
Show only external alerts
Actions
@timestamp
message
host.name
event.module
agent.type
event.dataset
event.action
user.name
source.ip
destination.ip
Feb 25, 2026 @ 22:15:48.423
b7f77c1ae42f
Feb 25, 2026 @ 22:15:48.423
b7f77c1ae42f
Feb 25, 2026 @ 22:15:48.422
b7f77c1ae42f
[REDACTED]
172.22.0.2

Grafana Loki

- Za razliku od ELK, Loki indeksira samo unaprijed definirane oznake poput naziva servisa i okruženja
- Sadržaj se sprema u komadima (chunks) što se najčešće kombinira s vanjskim servisima za pohranu podataka (npr. Amazon S3)
- Grafana web sučelje dolazi bez unaprijed konfiguriranih ploča, ali je moguće preuzeti gotove predloške s weba
- Jednostavnija i manje zahtjevna inačica u odnosu na ELK

Grafana Loki



Rezultati usporedbe

ELK Stack

- snažna analitika
- napredne nadzorne ploče
- korelacija događaja
- veća potrošnja resursa
- složenija konfiguracija

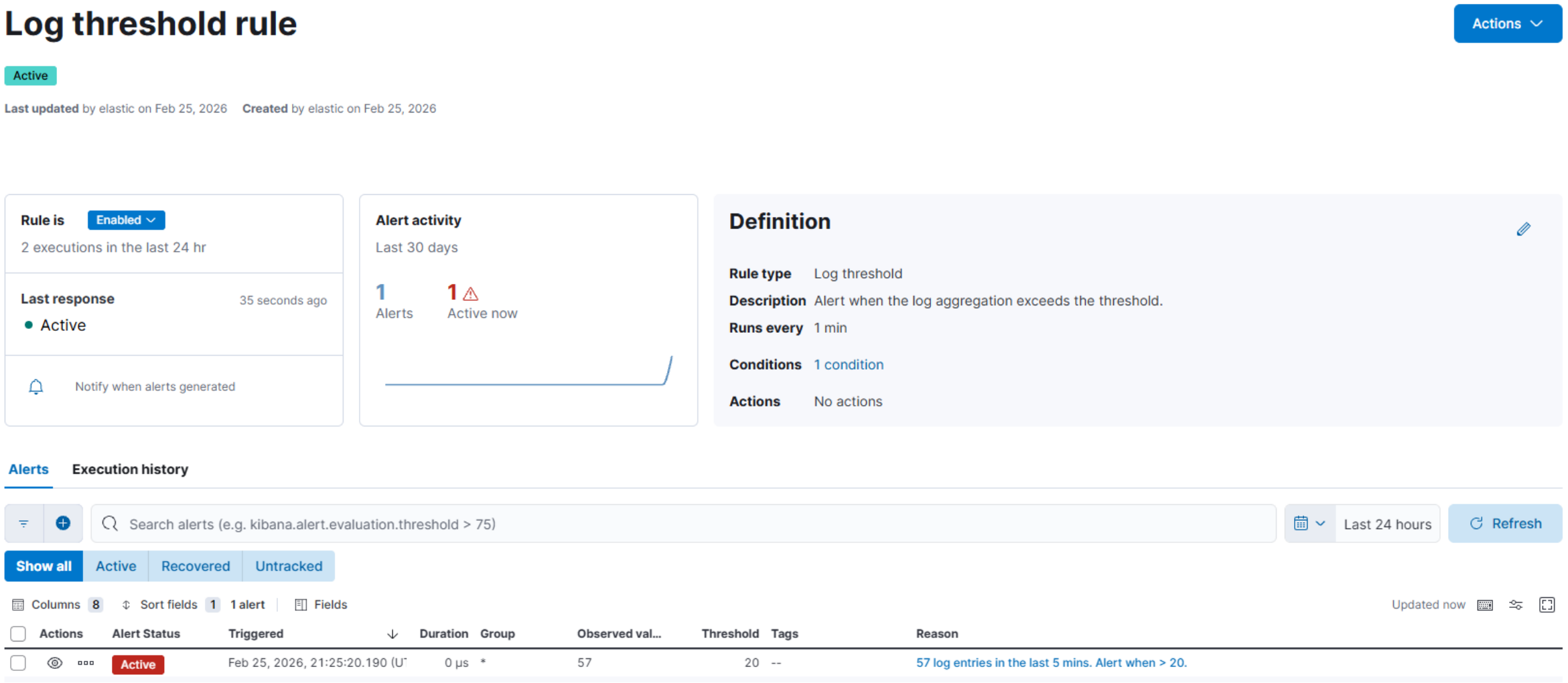
Grafana Loki

- jednostavna implementacija
- manji infrastrukturni zahtjevi
- brze vremenske pretrage
- ograničena analitika nad sadržajem zapisa

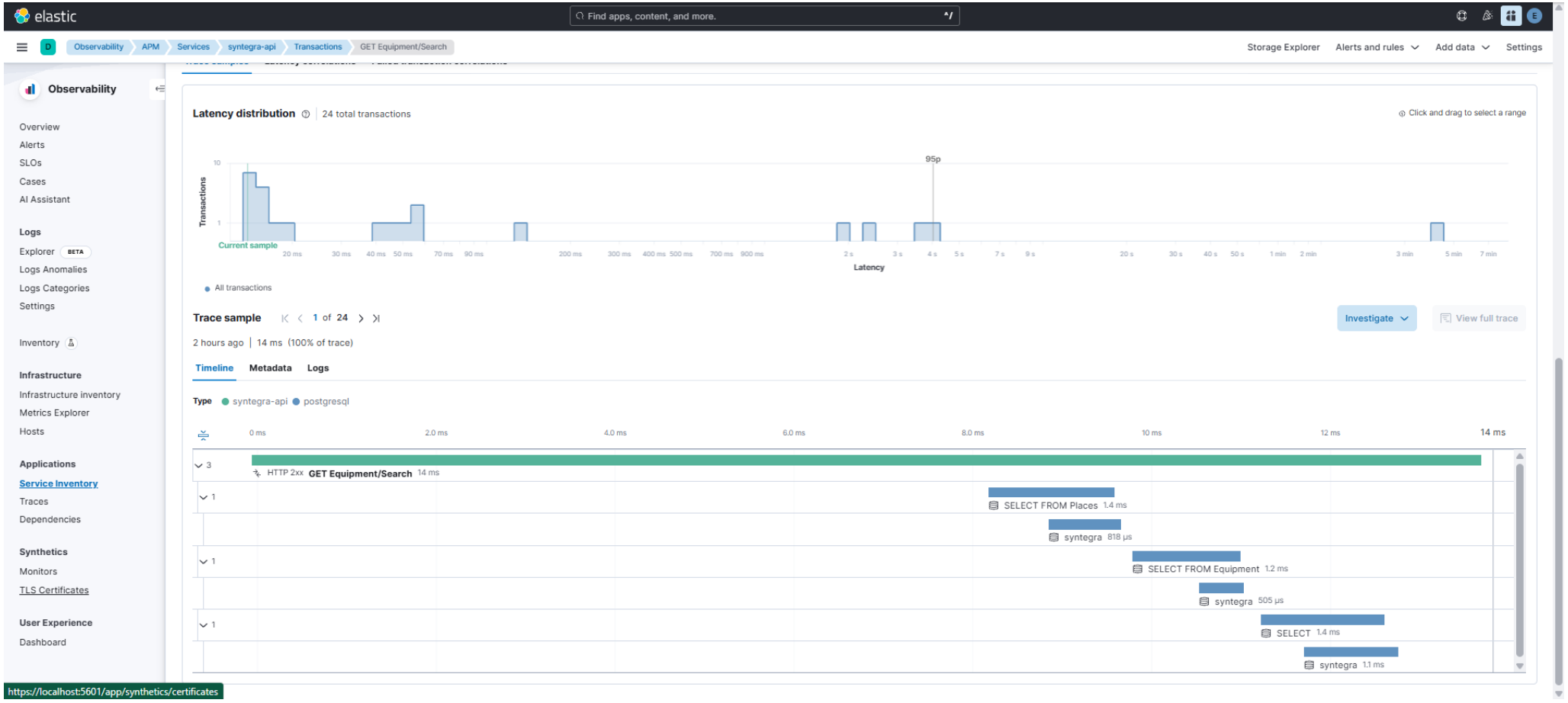
Rezultati

- Oba rješenja nude osnovne funkcionalnosti za centraliziranu obradu zapisa iz distribuiranih sustava i postavljanje sigurnosnih alarma
- ELK rješenje je osjetno zahtjevnije i teže za postaviti, međutim, daje znatno detaljniji uvid u stanje sustava radi više desetaka unaprijed definiranih nadzornih ploča
- Grafana Loki rješenje je brže i lakše za postaviti, pogotovo za manje kompliciranе slučajeve, ali poteškoće se pojavljuju pri velikim količinama zapisa koje je potrebno indeksirati po prilagođenim poljima

Prilagođena upozorenja



Nadogradnja: praćenje metrika



Zaključak

- Centralizirana analiza zapisa omogućuje bolji nadzor distribuiranih sustava, bržu detekciju incidenata i lakšu forenzičku analizu
- Ispravno strukturirani zapisi olakšavaju obradu i daljnju analitiku
- Odabir rješenja ovisi ponajviše o krajnjim potrebama:
- **ELK** je pogodniji za dubinsku analizu poslovnih procesa i povezanih metrika te za sigurnosne istrage; unapijed definirane nadzorne ploče pokrivaju velik broj čestih scenarija
- **Grafana Loki** je učinkovit za operativni nadzor i jednostavne upite te je bolji odabir za izradu prilagođenih ploča za podatkovne tokove

HVALA NA PAŽNJI