

CUSTOMER STORY: OBSERVABILITY

Financial services · Payment gateway · Siloed logs → Elastic

Finding one failed payment among 1.4 billion daily log events

One of India's leading payment gateways processes 1.4 billion log events a day on Elastic, tracing any transaction across 25+ microservices by trace ID.

1.4 billion

Log events processed daily, no sampling

16,000/sec

Sustained indexing rate, searchable in real time

500 GB/day

25+ microservices, one Elastic cluster

Minutes, not hours

To trace a failed transaction end to end

The challenge

- ✗ 25+ microservices wrote logs around the clock with no shared context between them.
- ✗ A failed transaction's trace ID couldn't be searched across services.
- ✗ Latency wasn't monitored per service, and HTTP status codes weren't tracked centrally.
- ✗ A microservice could restart with nothing to alert the team.

The solution

- ✓ The team builds on a dedicated Elastic Stack sized for the platform's real transaction volume, not a reference architecture.
- ✓ Three Logstash nodes feed an Elasticsearch cluster of three master and nine data nodes.
- ✓ Engineers trace transactions and watch service health in Kibana dashboards.
- ✓ Per-service latency, HTTP status, and restart alerting run across the full estate.

How it works

1. Ingest

Logs from 25+ services into Elasticsearch

2. Trace

Search one trace ID across every hop

3. Monitor

Latency and status tracked per service

4. Alert

Restarts and anomalies surface instantly

Before

- Logs checked service by service, by hand
- No per-service latency or status visibility
- Service restarts passed silently

After

- One trace ID search, the full journey
- Per-service latency and status monitored
- Restarts trigger critical alerts

“Running at this volume under real production load is what **earned their trust**. Once a team sees the visibility hold, moving more critical workloads onto it stops being a risk conversation.”

— Ravi Papnoi, Deputy CEO, Ashnik, the customer's Elastic implementation partner

Why it matters beyond one estate

Sizing the platform around real transaction volume, rather than a reference architecture, is what let it hold at 16,000 events per second as a steady state rather than a spike. That same confidence is now extending to more of the business's critical workloads because the team has seen the visibility hold at scale and trusts it will keep holding as volume grows.