Streams - The Future of Solving Problems with Logs

Logs are back

Foundational

Logs are the bedrock of all investigations

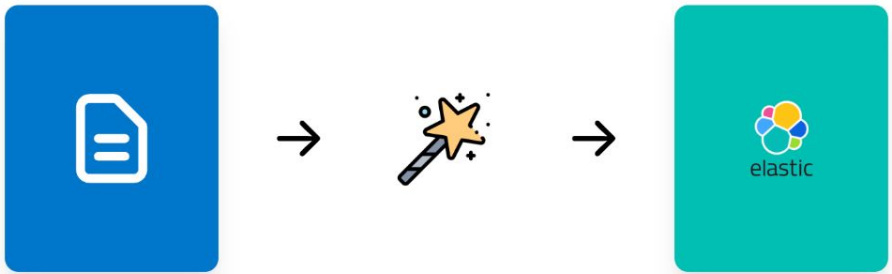
Reveals the 'Why'

Unstructured data tells the story

Structured Insights

Enable smarter analytics

Early days of ELK: Simple magic



The "Perceived" Challenge

What people think...

- Messy and unstructured
- Millions of noisy lines
- Context gaps everywhere

user_id=542 status_code=200

Server restarted host server_02

use_id=175 status_code=500

auth_method='oauth' status_code=401

The Reality of Logs

What's actually true...

- AI reads it like a book
- Rich context: users, devices, regions
- No instrumentation needed

```
user_id=542 status_code=200
Server restarted host server_02
user_id=175 status_code=500
auth_method='oauth' status_code=401
```

Logs are foundational to all investigations.

Industry searching for structure

Wide events, traces, and logs are all structured data

App Log | Trace Span | K8s Wide Event


```
{
  "timestamp": "2025-09-02T11:24:12Z",
  "level": "INFO",
  "service": "checkout-service",
  "message": "Checkout request processed",
  "user_id": "u123456",
  "cart_id": "c78910",
  "payment_provider": "stripe",
  "duration_ms": 182,
  "trace_id": "f84c8b9d12a64a94a2e9e7ab4f37cd01"
}
```


Wide events, traces == structured log

Industry searching for structure

Wide events, traces, and logs are all structured data

App Log | Trace Span | K8s Wide Event


```
{
  "trace_id": "f84c8b9d12a64a94a2e9e7ab4f37cd01",
  "span_id": "a32f67cd41eafc12",
  "parent_span_id": "root",
  "timestamp": "2025-09-02T11:24:12Z",
  "service": "checkout-service",
  "operation": "POST /checkout",
  "duration_ms": 182,
  "attributes": {
    "user_id": "u123456",
    "cart_id": "c78910",
    "payment_provider": "stripe"
  },
  "status": "OK"
}
```


Wide events, traces == structured log

Industry searching for structure

Wide events, traces, and logs are all structured data

App Log | Trace Span | K8s Wide Event


```
{
  "timestamp": "2025-09-02T11:23:45Z",
  "event_type": "pod_lifecycle",
  "cluster": "prod-cluster-1",
  "namespace": "payments",
  "pod_name": "checkout-7f5d4c6d8f-vx9bz",
  "reason": "OOMKilled",
  "restart_count": 3,
  "resource_requests": {
    "cpu": "500m",
    "memory": "512Mi"
  },
  "labels": {
    "app": "checkout",
    "team": "payments"
```


Wide events, traces == structured log

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 13%

Processing first stage...

Ingest → Store → Identify → Partition → Extract → Events → Assets → Investigate

Stage 1 of 8

Next stage >

Ingest

Bring log data in from agents, streams, and forwarders

RESULT

Log events arriving

Agents, forwarders, and streams feed the pipeline

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 25%

Processing first stage...

Ingest · **Store** · Identify · Partition · Extract · Events · Assets · Investigate

Stage 2 of 8

Next stage >

Store Efficiently

Logs ingested with LogsDB compression for cost-effective storage

RESULT

LogsDB Index Mode

Optimized sorting + compression for logs, so you store more without losing common O11y features.

OBSERVED **~72%** less storage

WITHOUT LOGSDB	WITH LOGSDB
1 TB	**286 GB**
Baseline footprint	Same data, smaller disk

Ingest once, store efficiently — then run the rest of the AI pipeline on top.

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 38%

Processing first stage...

Ingest — Store — **Identify** — Partition — Extract — Events — Assets — Investigate

Stage 3 of 8

Next stage >

System Identification

AI identifies the systems generating the logs

RESULT

Elasticsearch

`version 9.1.0, Java`

Nginx

`version 1.29.1`

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

AI DRIVEN ANALYSIS

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 50%

✓ Identify

Ingest → Store → Identify → **Partition** → Extract → Events → Assets → Investigate

Stage 4 of 8

Next stage ›

Data Partitioning

Route logs to appropriate streams based on source

RESULT

Elasticsearch

```
| WHERE service.name == elasticsearch
```

Nginx

```
| WHERE log.file.path LIKE '/var/log/nginx/*'
```

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

AI DRIVEN ANALYSIS

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 63%

✓ Identify ✓ Partition

✓ Ingest ✓ Store ✓ Identify ✓ Partition **Extract** Events Assets Investigate

Stage 5 of 8

Next stage >

Data Processing / Extract Information

Parse and extract structured fields from raw log lines

RESULT

Elasticsearch

```
\[%{TIMESTAMP_ISO8601:timestamp}\]\[%{LOGLEVEL:log.level}\s*\]...
```

Nginx

```
%{IPORHOST:client.ip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\]
...
```

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 75%

✓ Identify ✓ Partition ✓ Extract

Ingest ✓ — Store ✓ — Identify ✓ — Partition ✓ — Extract ✓ — Events — Assets — Investigate

Stage 6 of 8

Next stage ›

Find Significant Events

Identify important events and anomalies in the log data

RESULT

Elasticsearch

```
Query – "message: *OOMException*"
```

Nginx

```
Query – "http.status_code>=500"
```

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 88%

✓ Identify ✓ Partition ✓ Extract ✓ Events

✓ Ingest ✓ Store ✓ Identify ✓ Partition ✓ Extract ✓ Events **Assets** Investigate

Stage 7 of 8

Next stage ›

Generate Assets (Visualizations, Dashboards, SLOs)

Auto-generate relevant visualizations, SLOs, and dashboards

RESULT

Elasticsearch

```
SLO: 99.9% "NOT response.took>=300"
```

Nginx

```
SLO: 99.9% "NOT http.status_code>=500"
```

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost

AI DRIVEN ANALYSIS

Extracting Insights from Log Data

INPUT LOGS

Elasticsearch

[2025-09-09T23:17:58,854][ERROR][o.e.b.ElasticsearchUncaughtExceptionHandler] [main-node] fatal error in thread [elasticsearch[main-node][search][T#7]], exiting java.lang.OutOfMemoryError: Java heap space

Nginx

127.0.0.1 - - [01/Sep/2025:15:36:05 +0200] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"

CONTEXT

Accumulated Knowledge 100%

✓ Identify ✓ Partition ✓ Extract ✓ Events ✓ Assets

Stage 8 of 8

Investigate & Recommend

Use all accumulated context to explain what happened and recommend next actions

RESULT

Explanation

```
Using signals + events + extracted fields to explain what happened and
recommend next actions
```

- Reduce manual workflows
- Improve detection
- Simplified onboarding
- Lower cost