Ze

ZEBRIUM

# Autonomous Log Monitoring

*USING MACHINE LEARNING*

Larry Lancaster
Founder and CTO
Zebrium

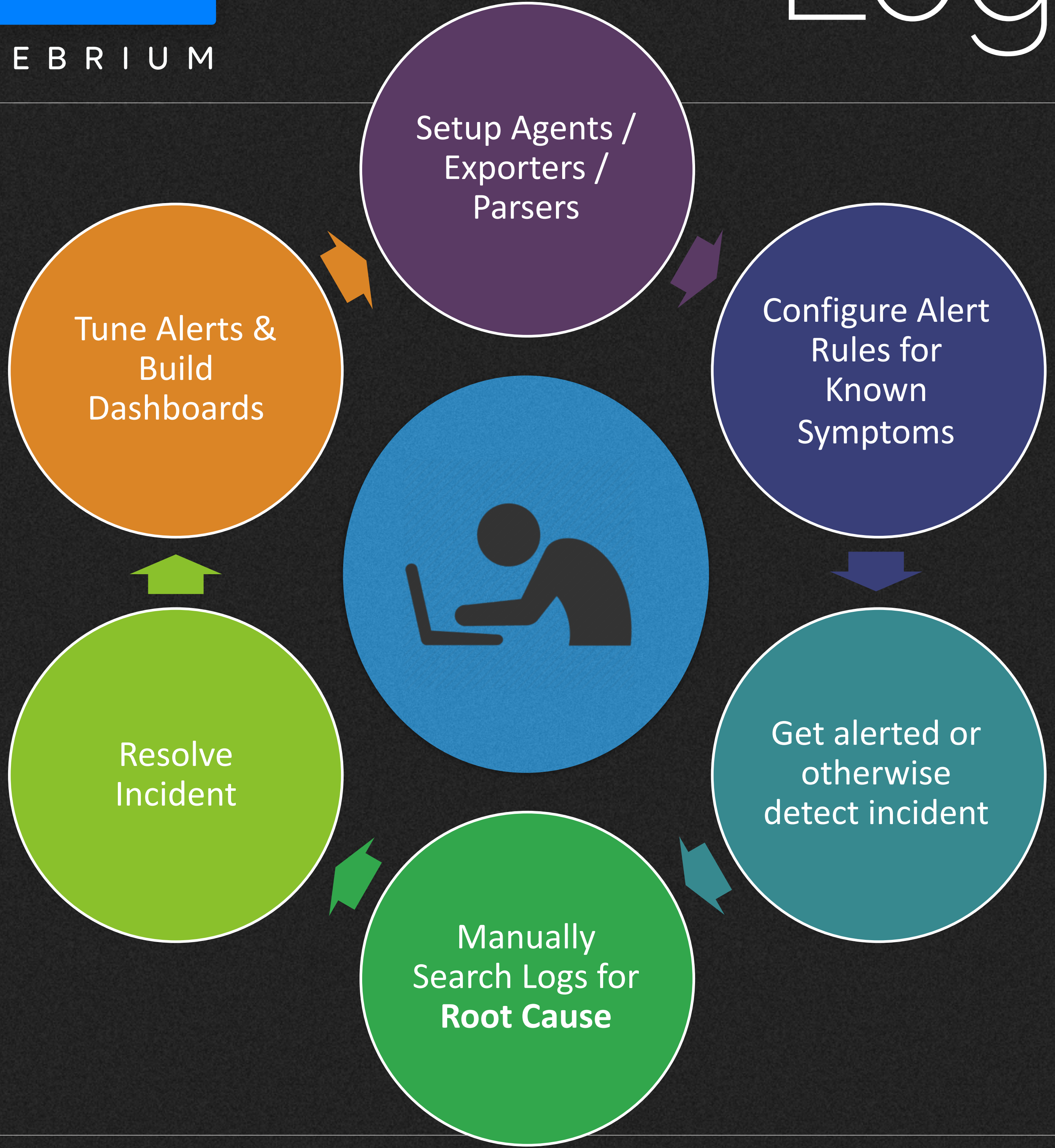
ZEBRIUM

# Machine data is my life

- NetApp - *Engineering Informatics*
- EMC / Data Domain - *Product Analytics*
- Glassbeam - *Chief Technology Officer*
- Nimble Storage - *Chief Data Scientist*
- Zebrium - *Founder and CTO*

ZEBRIUM

# Log monitoring today


Setup Agents / Exporters / Parsers
Configure Alert Rules for Known Symptoms
Get alerted or otherwise detect incident
Manually Search Logs for **Root Cause**
Resolve Incident
Tune Alerts & Build Dashboards

SLOW (MTTR)

FRAGILE (FORMATS CHG)

ANNOYING (ALERT FATIGUE)

HUMAN-DRIVEN

# Logs are used for RC

...so why aren't they better at helping us monitor?

# What keeps logs "dumb"?

Logs are stuck in "index + search"

# 20 YEARS AGO

Shrink-Wrap:

*1 incident 1 user*

*1 incident 1 monolith*

*1 incident 10 logfiles*

Log use for root-cause:

*index and search*

# 20 YEARS AGO

Shrink-Wrap:

*1 incident 1 user*

*1 incident 1 monolith*

*1 incident 10 logfiles*

Log use for root-cause:

*index and search*

# TODAY

SaaS:

*1 incident 100K users*

*1 incident 100 services*

*1 incident 1K logstreams*

Log use for root-cause:

***still index and search(!)***

# Our vision

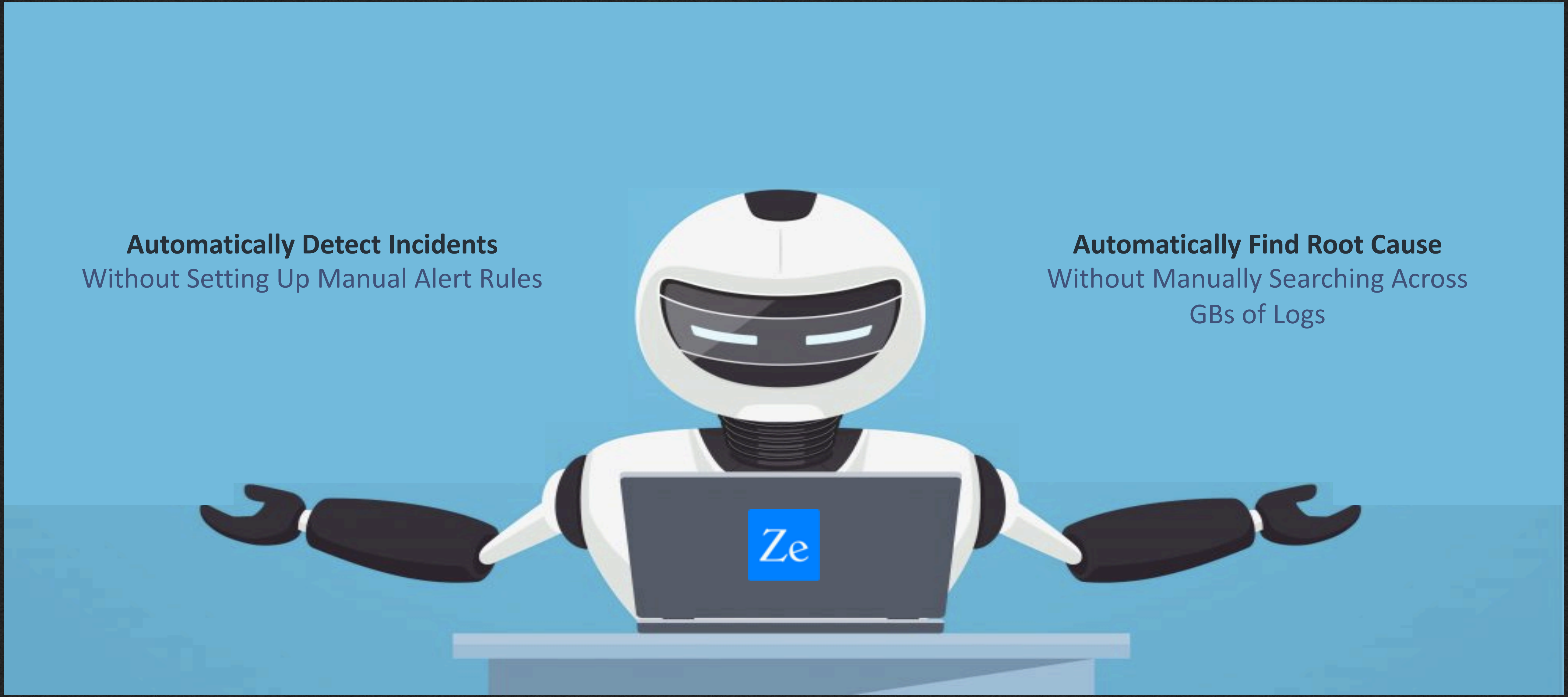
The future will not be "index + search".

# What I want from a tool

Characterize incidents before I notice

ZEBRIUM

# What I want from a tool



**Automatically Detect Incidents**
Without Setting Up Manual Alert Rules

**Automatically Find Root Cause**
Without Manually Searching Across GBs of Logs

# Why is it so hard?

Formats change

Parses are ambiguous

Experts are needed to interpret

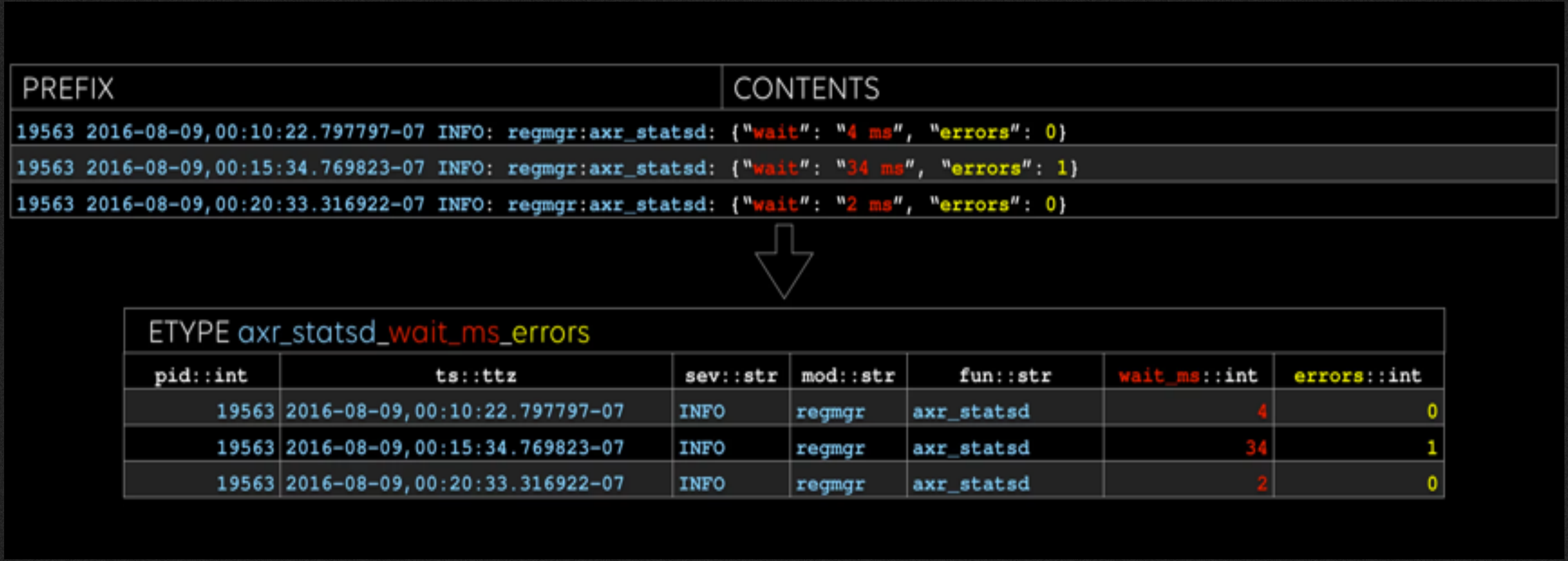
Apps are bespoke

ZEBRIUM

# Ze: How it works

Complete relational structuring of logs

# Ze: How it works



```
PREFIX                                                 CONTENTS
19563 2016-08-09,00:10:22.797797-07 INFO: regmgr:axr_statsd: {"wait": "4 ms", "errors": 0}
19563 2016-08-09,00:15:34.769823-07 INFO: regmgr:axr_statsd: {"wait": "34 ms", "errors": 1}
19563 2016-08-09,00:20:33.316922-07 INFO: regmgr:axr_statsd: {"wait": "2 ms", "errors": 0}
```

ETYPE axr_statsd_wait_ms_errors

| pid::int | ts::ttz | sev::str | mod::str | fun::str | wait_ms::int | errors::int |
|---|---|---|---|---|---|---|
| 19563 | 2016-08-09,00:10:22.797797-07 | INFO | regmgr | axr_statsd | 4 | 0 |
| 19563 | 2016-08-09,00:15:34.769823-07 | INFO | regmgr | axr_statsd | 34 | 1 |
| 19563 | 2016-08-09,00:20:33.316922-07 | INFO | regmgr | axr_statsd | 2 | 0 |

ZEBRIUM

# Ze: How it works

## No information included or required about:

- Known prefix formats
- Specific logtype keywords
- Event grammar / syntax

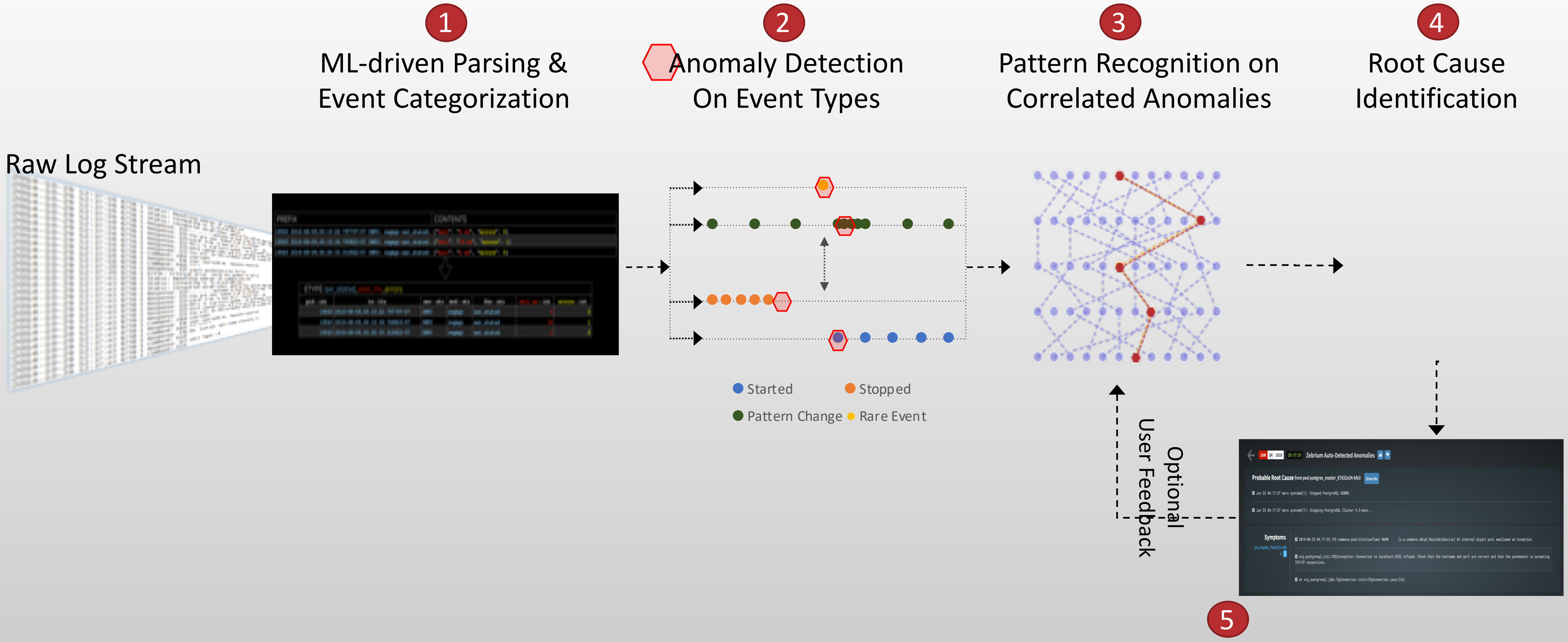
***We embrace free-text logs***

ZEBRIUM

# Ze: How it works

Anomaly detection on relationally structured data

# Ze: How it works



1 ML-driven Parsing & Event Categorization

2 Anomaly Detection On Event Types

3 Pattern Recognition on Correlated Anomalies

4 Root Cause Identification

5

Probable Root Cause from pod postgres_master_67d32e34-bfe3

```
Jun 25 04:17:37 mars systemd[1]: Stopped PostgreSQL RDBMS.
Jun 25 04:17:37 mars systemd[1]: Stopping PostgreSQL Cluster 9.5-main...
```

Symptoms

```
2019-06-25 04:17:39,129 commons-pool-EvictionTimer WARN    [o.a.commons.dbcp2.BasicDataSource] An internal object pool swallowed an Exception.
org.postgresql.util.PSQLException: Connection to localhost:5432 refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections.
at org.postgresql.jdbc.PgConnection.<init>(PgConnection.java:216)
```

# Ze: How it works

## No information included or required about:

- Connectors, knowledge bases
- Specific application behaviors
- Specific semantic keywords

***Works great on bespoke app or stack***

# Other ML attempts

Use deep learning

Use one algorithm

Work in batch

ZEBRIUM

# Ours: Swiss army knife

Respect Pareto

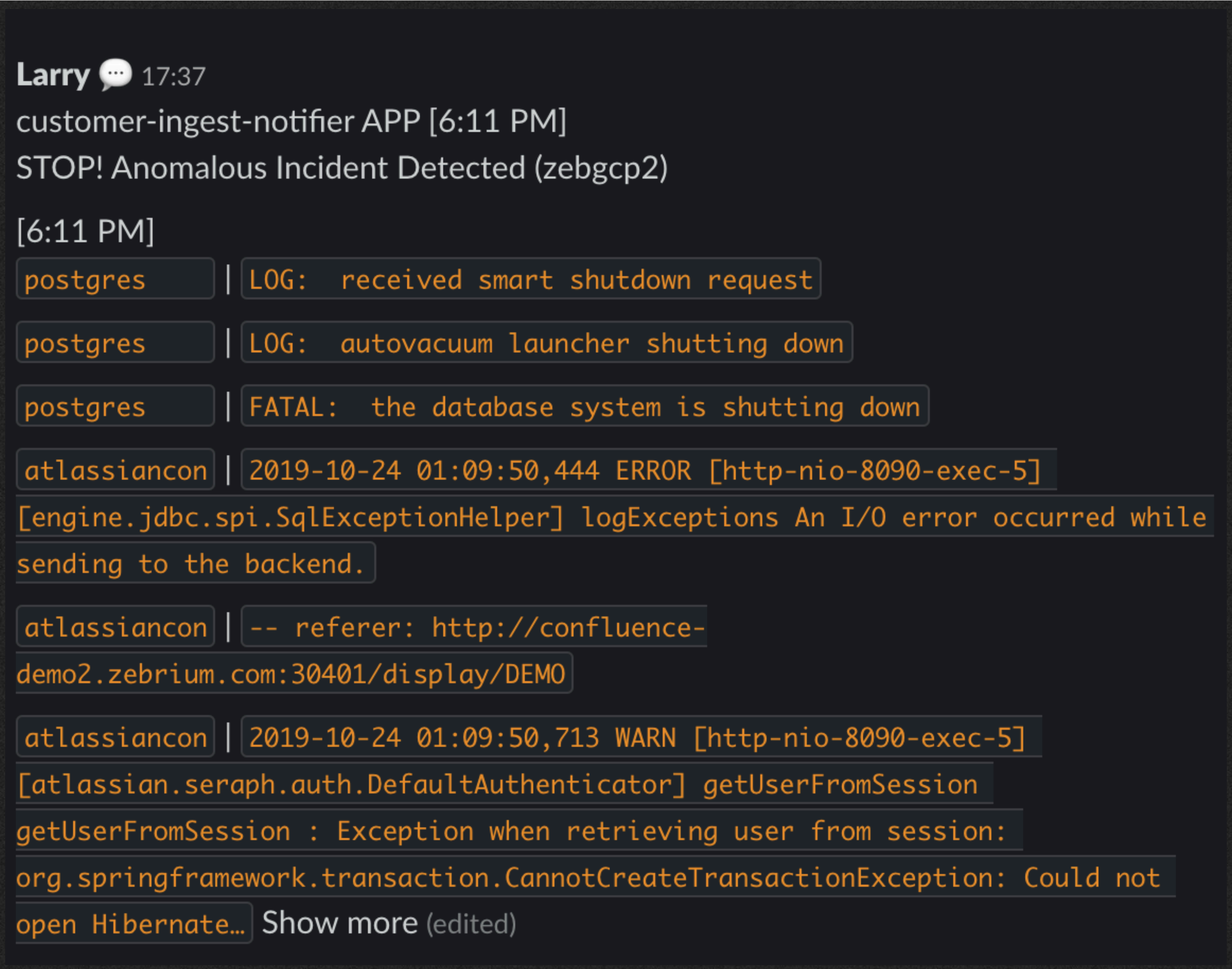
Structure First

AD gets better w / complexity!!!

# Demo

ZEBRIUM

# Demo: slack notification



**Larry** 17:37

customer-ingest-notifier APP [6:11 PM]

STOP! Anomalous Incident Detected (zebgcp2)

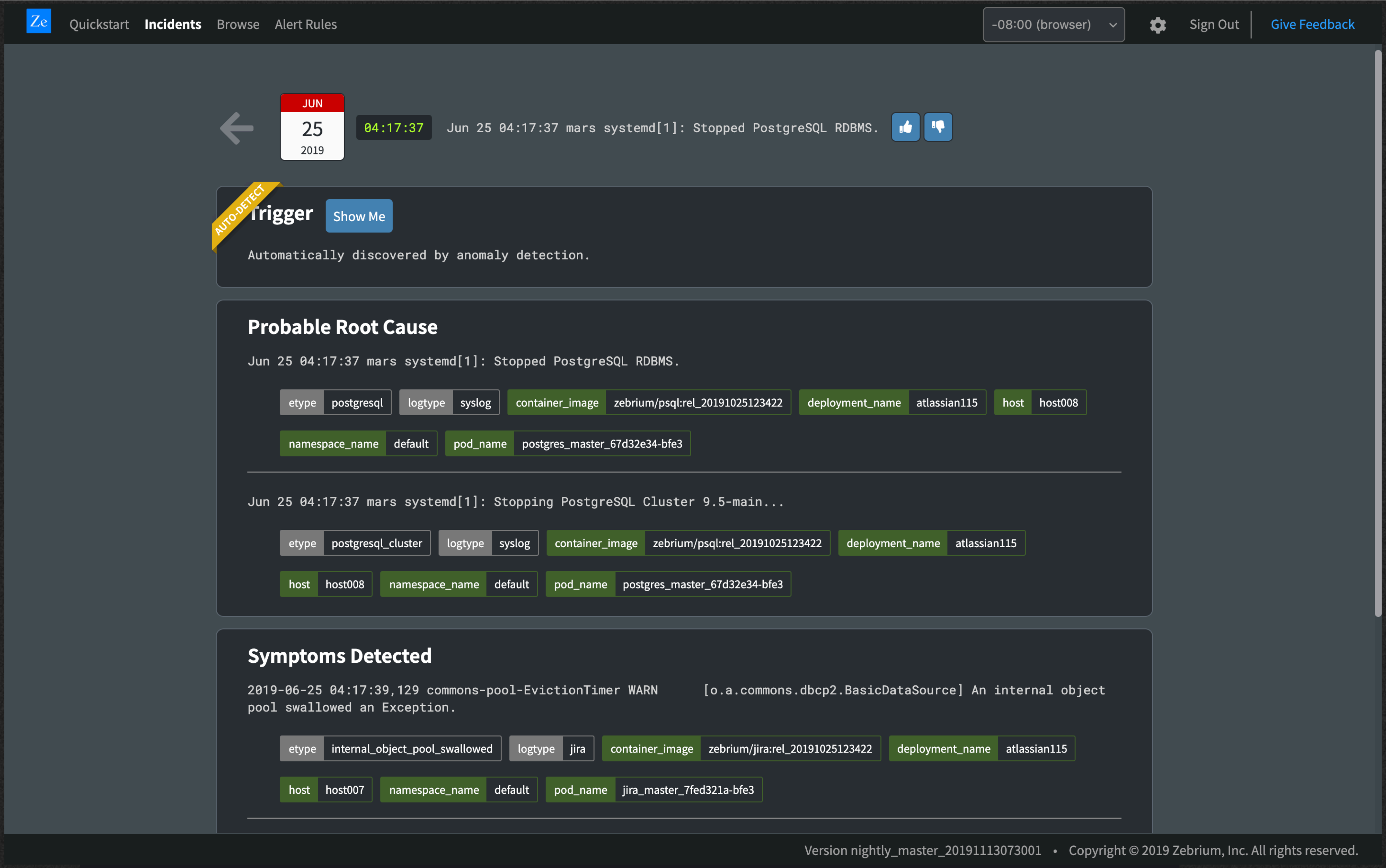
[6:11 PM]

```
postgres     | LOG:  received smart shutdown request
postgres     | LOG:  autovacuum launcher shutting down
postgres     | FATAL:  the database system is shutting down
atlassiancon | 2019-10-24 01:09:50,444 ERROR [http-nio-8090-exec-5]
[engine.jdbc.spi.SqlExceptionHelper] logExceptions An I/O error occurred while
sending to the backend.
atlassiancon | -- referer: http://confluence-
demo2.zebrium.com:30401/display/DEMO
atlassiancon | 2019-10-24 01:09:50,713 WARN [http-nio-8090-exec-5]
[atlassian.seraph.auth.DefaultAuthenticator] getUserFromSession
getUserFromSession : Exception when retrieving user from session:
org.springframework.transaction.CannotCreateTransactionException: Could not
open Hibernate…
```

Show more (edited)

ZEBRIUM

# Demo: incident detail



```
04:17:37  Jun 25 04:17:37 mars systemd[1]: Stopped PostgreSQL RDBMS.
```

## Trigger

Automatically discovered by anomaly detection.

## Probable Root Cause

```
Jun 25 04:17:37 mars systemd[1]: Stopped PostgreSQL RDBMS.
```

etype postgresql | logtype syslog | container_image zebrium/psql:rel_20191025123422 | deployment_name atlassian115 | host host008 | namespace_name default | pod_name postgres_master_67d32e34-bfe3

```
Jun 25 04:17:37 mars systemd[1]: Stopping PostgreSQL Cluster 9.5-main...
```

etype postgresql_cluster | logtype syslog | container_image zebrium/psql:rel_20191025123422 | deployment_name atlassian115 | host host008 | namespace_name default | pod_name postgres_master_67d32e34-bfe3

## Symptoms Detected

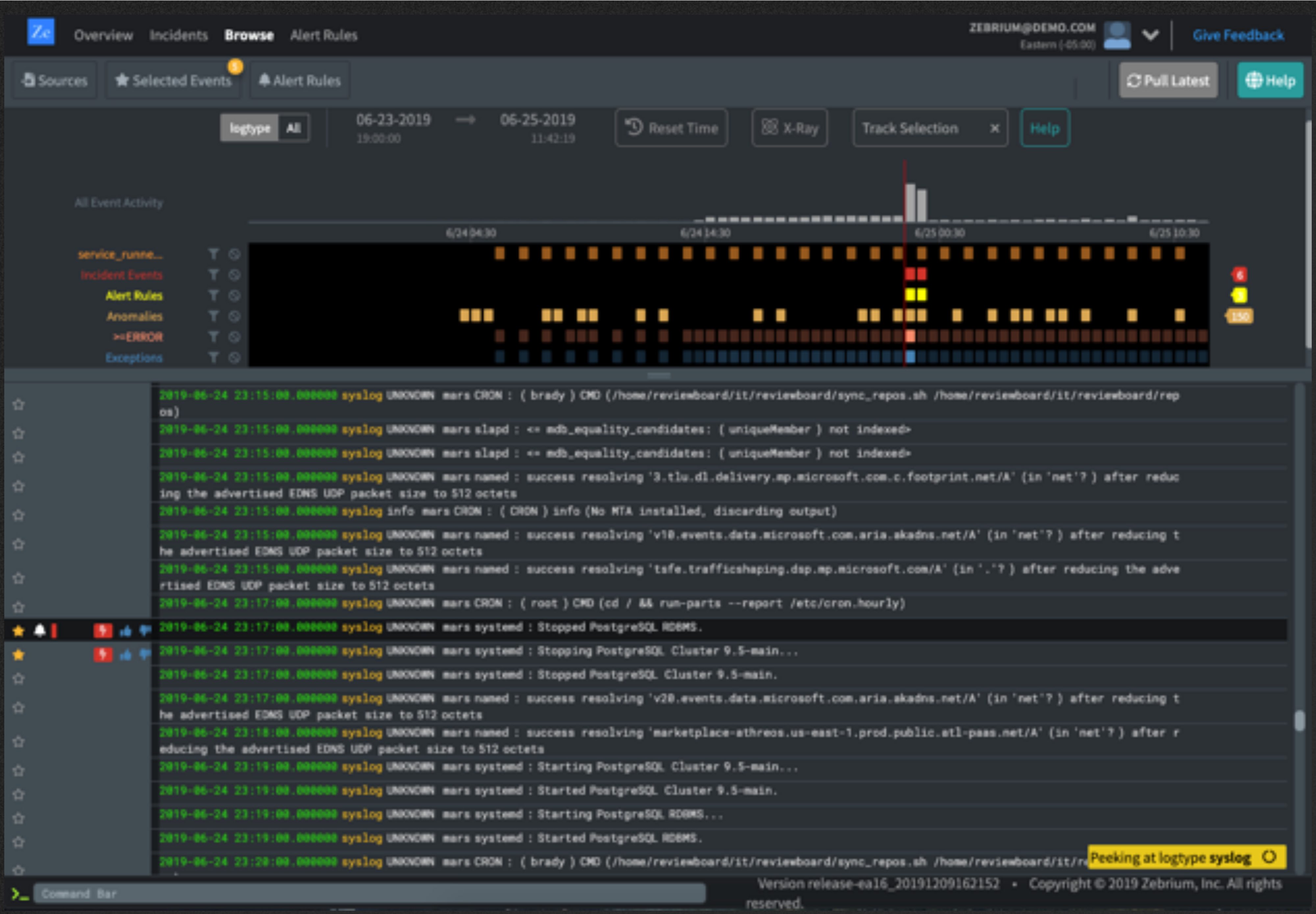
```
2019-06-25 04:17:39,129 commons-pool-EvictionTimer WARN      [o.a.commons.dbcp2.BasicDataSource] An internal object
pool swallowed an Exception.
```

etype internal_object_pool_swallowed | logtype jira | container_image zebrium/jira:rel_20191025123422 | deployment_name atlassian115 | host host007 | namespace_name default | pod_name jira_master_7fed321a-bfe3

Version nightly_master_20191113073001 • Copyright © 2019 Zebrium, Inc. All rights reserved.

ZEBRIUM

# Demo: Full-Featured UI

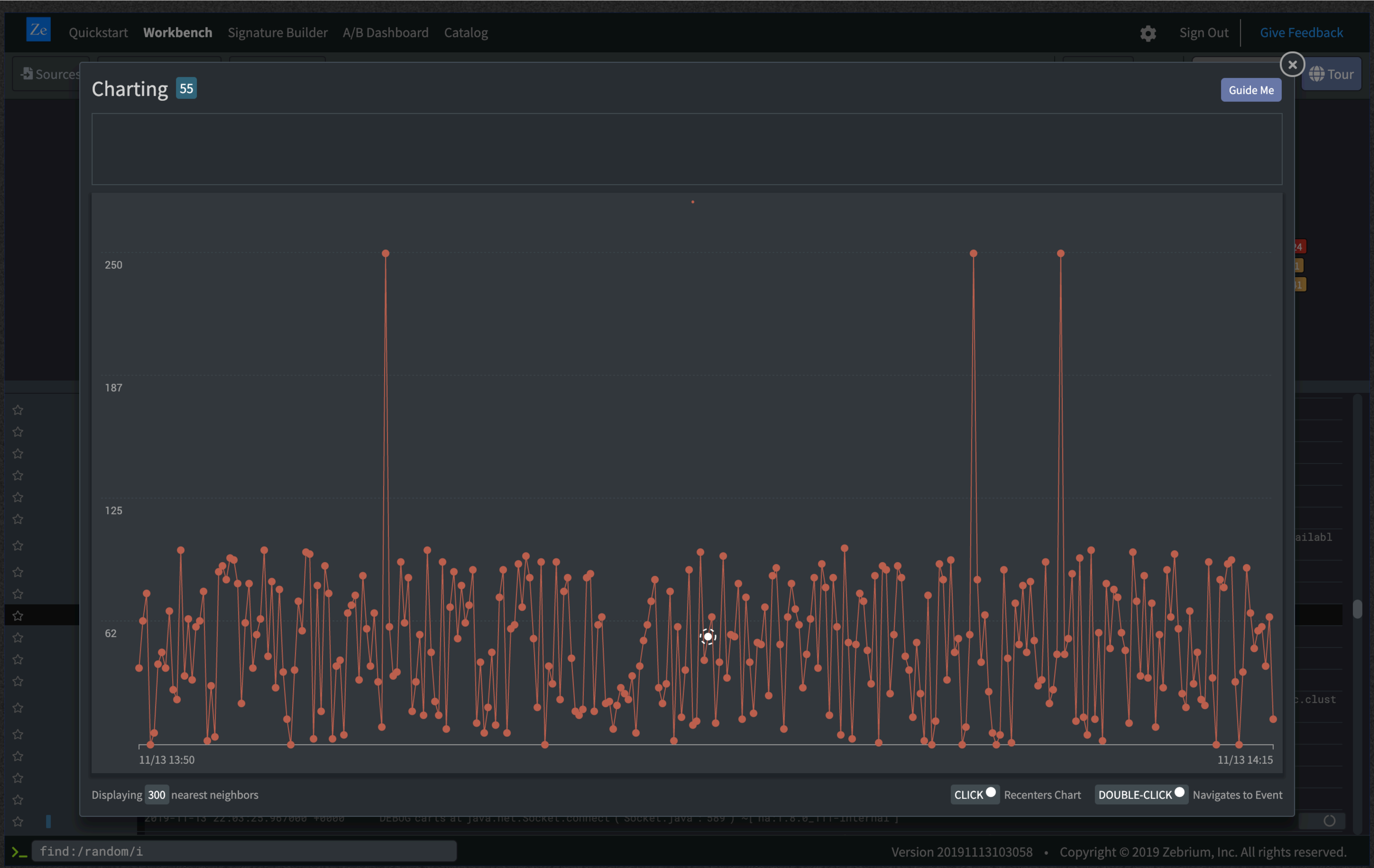


```
2019-06-24 23:15:00.000000 syslog UNKNOWN mars CRON : ( brady ) CMD (/home/reviewboard/it/reviewboard/sync_repos.sh /home/reviewboard/it/reviewboard/rep
os)
2019-06-24 23:15:00.000000 syslog UNKNOWN mars slapd : <= mdb_equality_candidates: ( uniqueMember ) not indexed>
2019-06-24 23:15:00.000000 syslog UNKNOWN mars slapd : <= mdb_equality_candidates: ( uniqueMember ) not indexed>
2019-06-24 23:15:00.000000 syslog UNKNOWN mars named : success resolving '3.tlu.dl.delivery.mp.microsoft.com.c.footprint.net/A' (in 'net'? ) after reduc
ing the advertised EDNS UDP packet size to 512 octets
2019-06-24 23:15:00.000000 syslog info mars CRON : ( CRON ) info (No MTA installed, discarding output)
2019-06-24 23:15:00.000000 syslog UNKNOWN mars named : success resolving 'v10.events.data.microsoft.com.aria.akadns.net/A' (in 'net'? ) after reducing t
he advertised EDNS UDP packet size to 512 octets
2019-06-24 23:15:00.000000 syslog UNKNOWN mars named : success resolving 'tsfe.trafficshaping.dsp.mp.microsoft.com/A' (in '.'? ) after reducing the adve
rtised EDNS UDP packet size to 512 octets
2019-06-24 23:17:00.000000 syslog UNKNOWN mars CRON : ( root ) CMD (cd / && run-parts --report /etc/cron.hourly)
2019-06-24 23:17:00.000000 syslog UNKNOWN mars systemd : Stopped PostgreSQL RDBMS.
2019-06-24 23:17:00.000000 syslog UNKNOWN mars systemd : Stopping PostgreSQL Cluster 9.5-main...
2019-06-24 23:17:00.000000 syslog UNKNOWN mars systemd : Stopped PostgreSQL Cluster 9.5-main.
2019-06-24 23:17:00.000000 syslog UNKNOWN mars named : success resolving 'v20.events.data.microsoft.com.aria.akadns.net/A' (in 'net'? ) after reducing t
he advertised EDNS UDP packet size to 512 octets
2019-06-24 23:18:00.000000 syslog UNKNOWN mars named : success resolving 'marketplace-athreos.us-east-1.prod.public.atl-paas.net/A' (in 'net'? ) after r
educing the advertised EDNS UDP packet size to 512 octets
2019-06-24 23:19:00.000000 syslog UNKNOWN mars systemd : Starting PostgreSQL Cluster 9.5-main...
2019-06-24 23:19:00.000000 syslog UNKNOWN mars systemd : Started PostgreSQL Cluster 9.5-main.
2019-06-24 23:19:00.000000 syslog UNKNOWN mars systemd : Starting PostgreSQL RDBMS...
2019-06-24 23:19:00.000000 syslog UNKNOWN mars systemd : Started PostgreSQL RDBMS.
2019-06-24 23:20:00.000000 syslog UNKNOWN mars CRON : ( brady ) CMD (/home/reviewboard/it/reviewboard/sync_repos.sh /home/reviewboard/it/re
```

Peeking at logtype **syslog**

Version release-ea16_20191209162152 • Copyright © 2019 Zebrium, Inc. All rights reserved.

# Demo: Chart from logs



Charting 55

Displaying 300 nearest neighbors

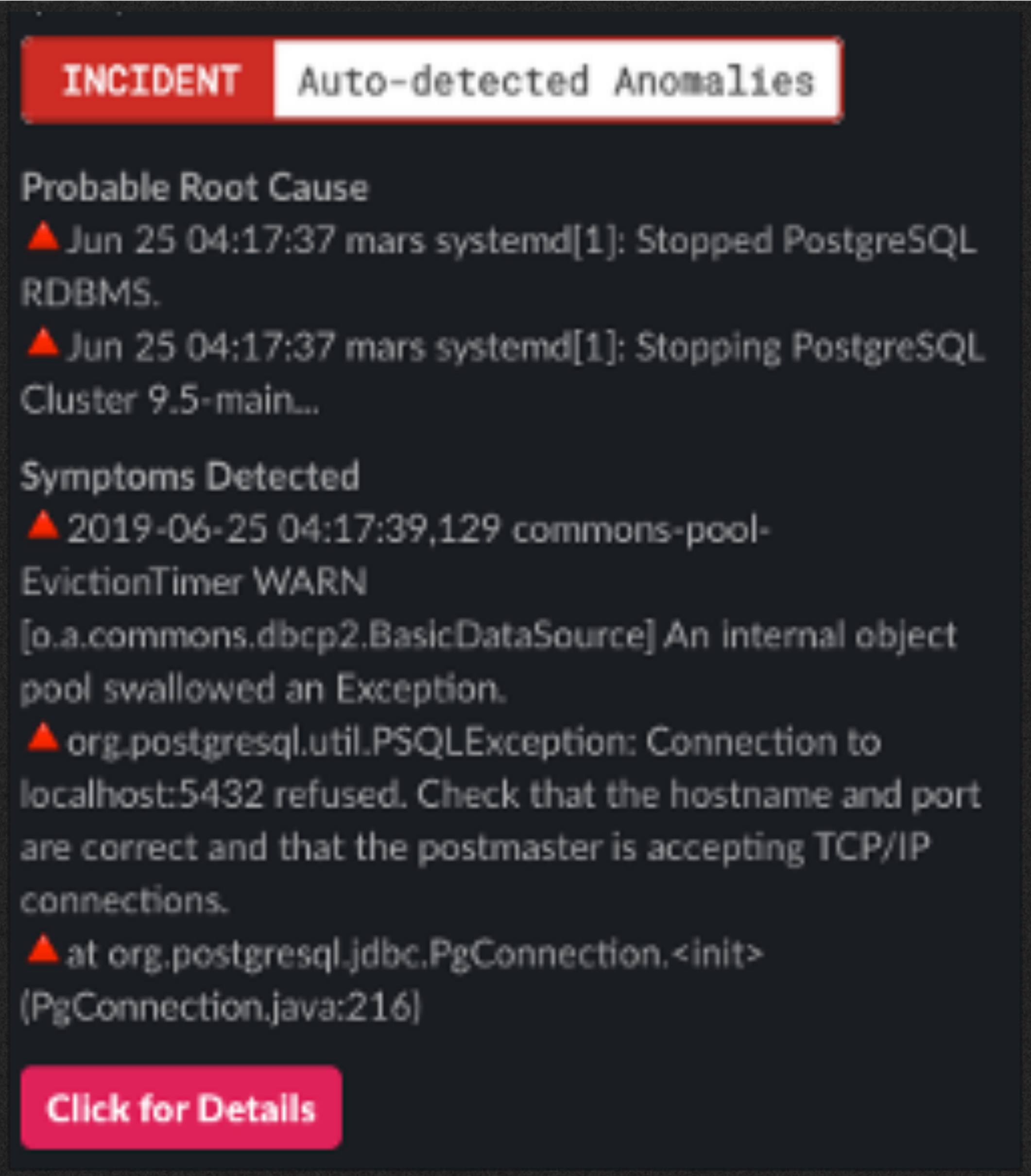
CLICK Recenters Chart DOUBLE-CLICK Navigates to Event

```
find:/random/i
```

Version 20191113103058 • Copyright © 2019 Zebrium, Inc. All rights reserved.

ZEBRIUM

# Where we're at



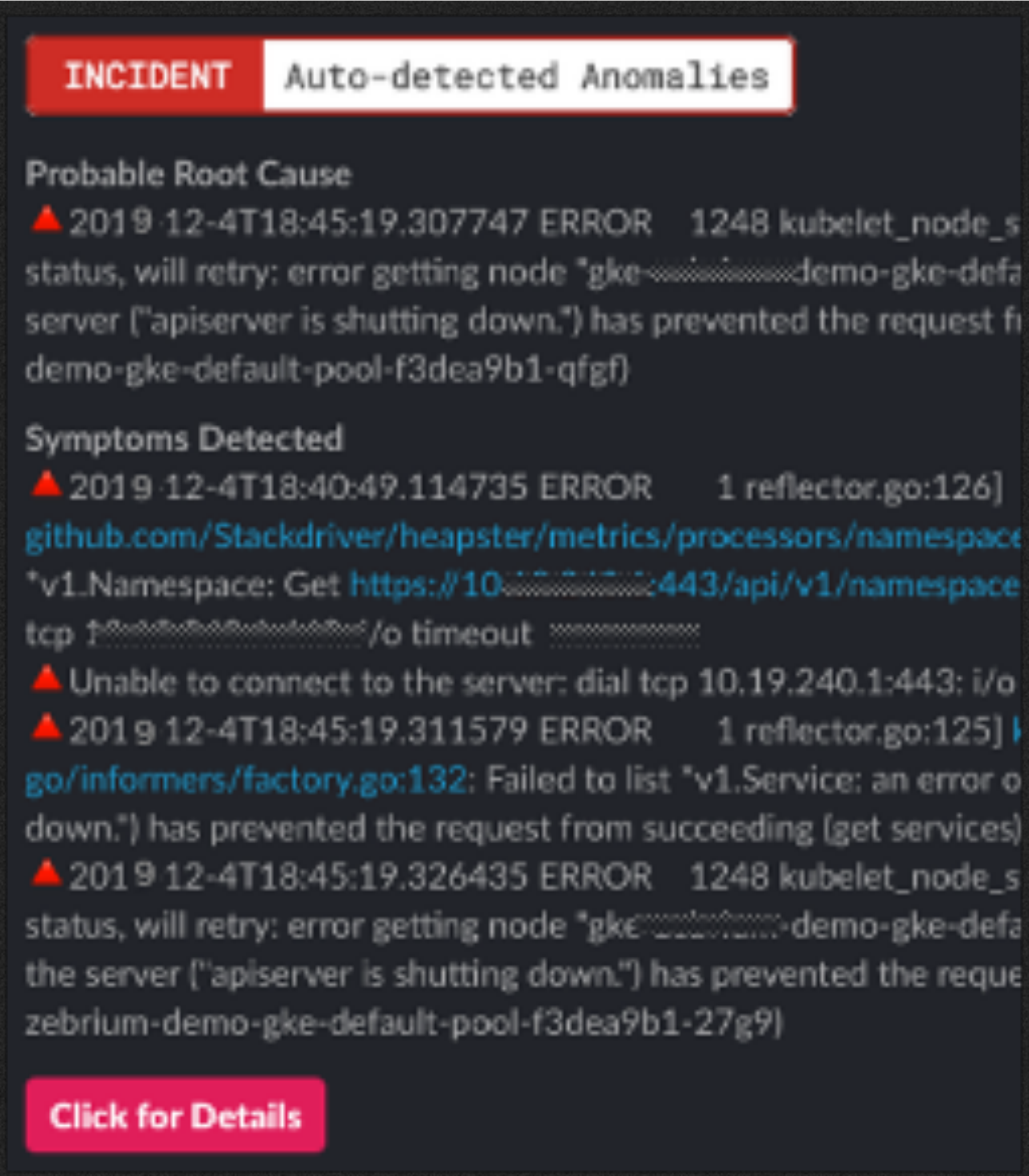
**Probable Root Cause**

```
▲Jun 25 04:17:37 mars systemd[1]: Stopped PostgreSQL RDBMS.
▲Jun 25 04:17:37 mars systemd[1]: Stopping PostgreSQL Cluster 9.5-main...
```

**Symptoms Detected**

```
▲2019-06-25 04:17:39,129 commons-pool-EvictionTimer WARN [o.a.commons.dbcp2.BasicDataSource] An internal object pool swallowed an Exception.
▲org.postgresql.util.PSQLException: Connection to localhost:5432 refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections.
▲at org.postgresql.jdbc.PgConnection.<init>(PgConnection.java:216)
```

## Application incidents



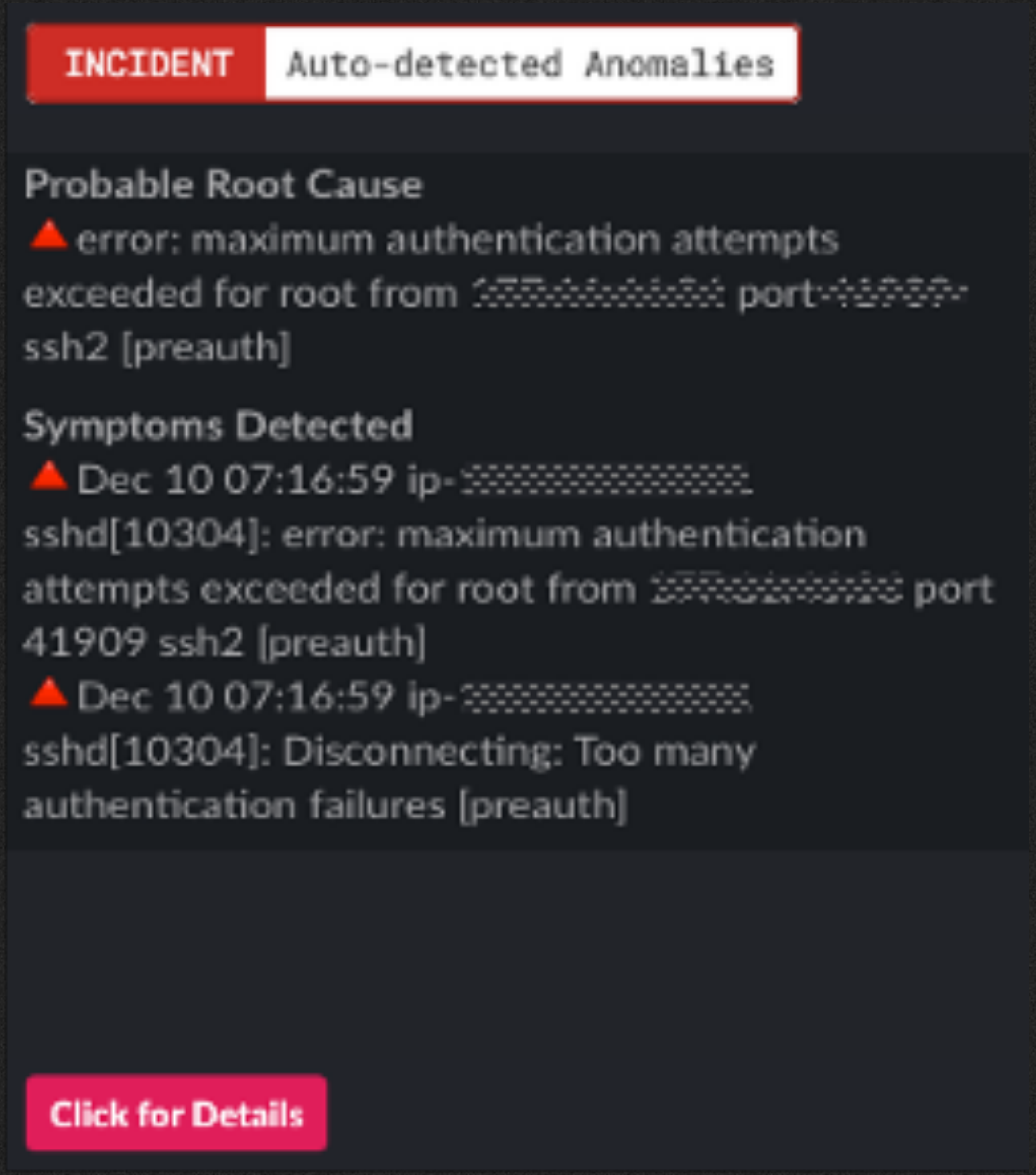
**Probable Root Cause**

```
▲2019-12-4T18:45:19.307747 ERROR    1248 kubelet_node_s
status, will retry: error getting node "gke-[redacted]demo-gke-defa
server ("apiserver is shutting down.") has prevented the request fr
demo-gke-default-pool-f3dea9b1-qfgf)
```

**Symptoms Detected**

```
▲2019-12-4T18:40:49.114735 ERROR      1 reflector.go:126]
github.com/Stackdriver/heapster/metrics/processors/namespace
*v1.Namespace: Get https://10[redacted]:443/api/v1/namespace
tcp 1[redacted]/o timeout  [redacted]
▲Unable to connect to the server: dial tcp 10.19.240.1:443: i/o
▲2019-12-4T18:45:19.311579 ERROR      1 reflector.go:125] k
go/informers/factory.go:132: Failed to list *v1.Service: an error o
down.") has prevented the request from succeeding (get services)
▲2019-12-4T18:45:19.326435 ERROR    1248 kubelet_node_s
status, will retry: error getting node "gke[redacted]-demo-gke-defa
the server ("apiserver is shutting down.") has prevented the reque
zebrium-demo-gke-default-pool-f3dea9b1-27g9)
```

## Kubernetes incidents



**Probable Root Cause**

```
▲error: maximum authentication attempts exceeded for root from [redacted] port[redacted] ssh2 [preauth]
```

**Symptoms Detected**

```
▲Dec 10 07:16:59 ip-[redacted] sshd[10304]: error: maximum authentication attempts exceeded for root from [redacted] port 41909 ssh2 [preauth]
▲Dec 10 07:16:59 ip-[redacted] sshd[10304]: Disconnecting: Too many authentication failures [preauth]
```

## Security Incidents

ZEBRIUM

# Recent validation

MAYADATA

OpenEBS

Containerized Storage for Containers

OpenEBS is an open source storage platform that provides persistent and containerized block storage for DevOps and container environments.

Mayadata reproduced a slew of real-world incidents from real Kubernetes clusters using Litmus.

Zebrium immediately detected and root-caused **100%** of these incidents… no training, config, metadata required.

# Next stop

- One-Stop Shop for Incident RC
  - Ingesting Prometheus metrics
  - Bringing in time series features
  - Cross-correlating metrics with log anomalies

Ze

ZEBRIUM

# Thanks!

email: larry@zebrium.com

twitter: stochastimus@twitter.com

URL: zebrium.com/private-beta-sign-up