elastic | The Search AI Company

# Open source observability z OpenTelemetry i Elasticsearch

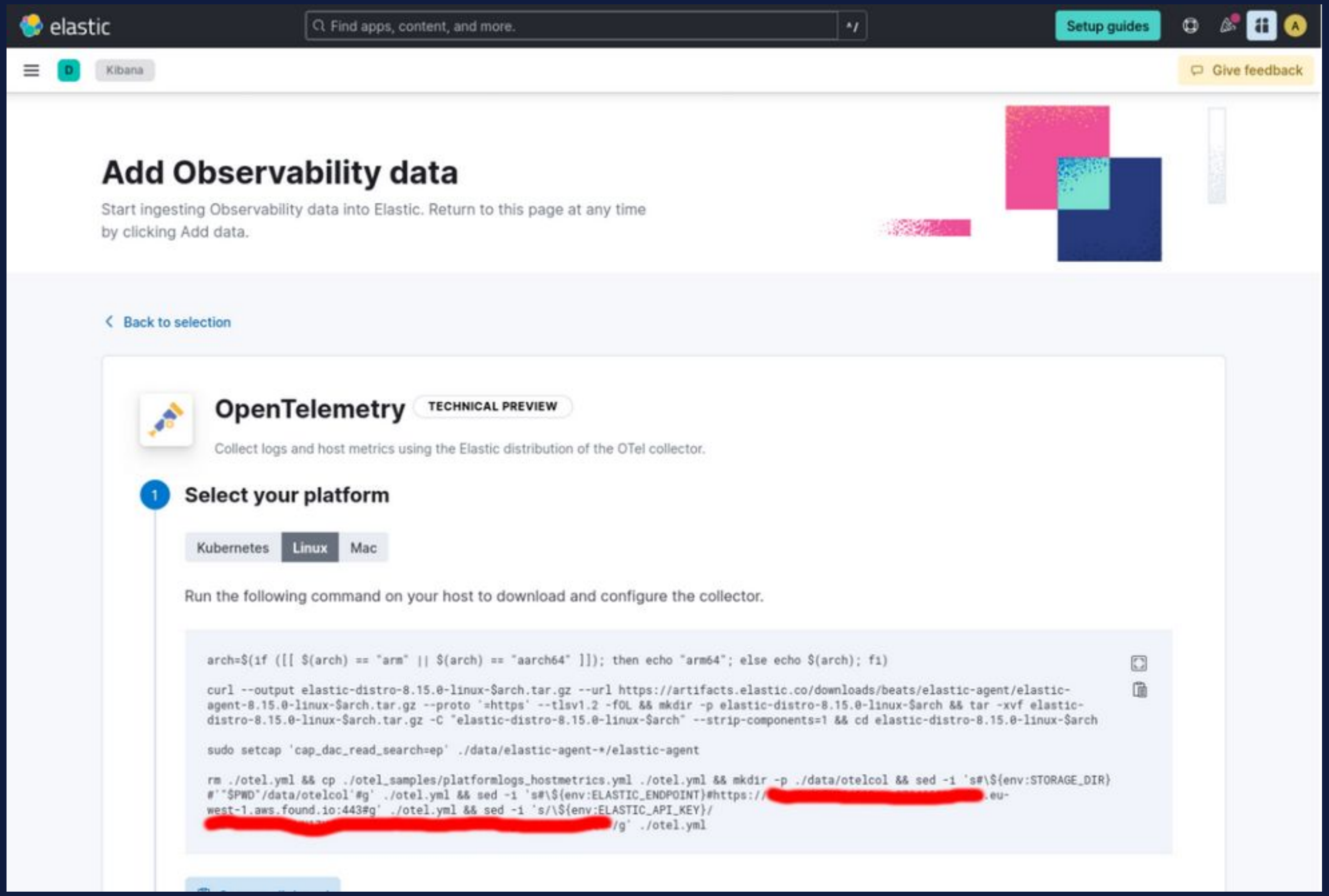
Andrzej Stencel

SysOps/DevOps Meetup

Poznań, 21 listopada 2024

# DEMO:

## Infrastructure monitoring with OpenTelemetry and Elasticsearch



### Add Observability data

Start ingesting Observability data into Elastic. Return to this page at any time by clicking Add data.

### OpenTelemetry

Collect logs and host metrics using the Elastic distribution of the OTel collector.

1 Select your platform

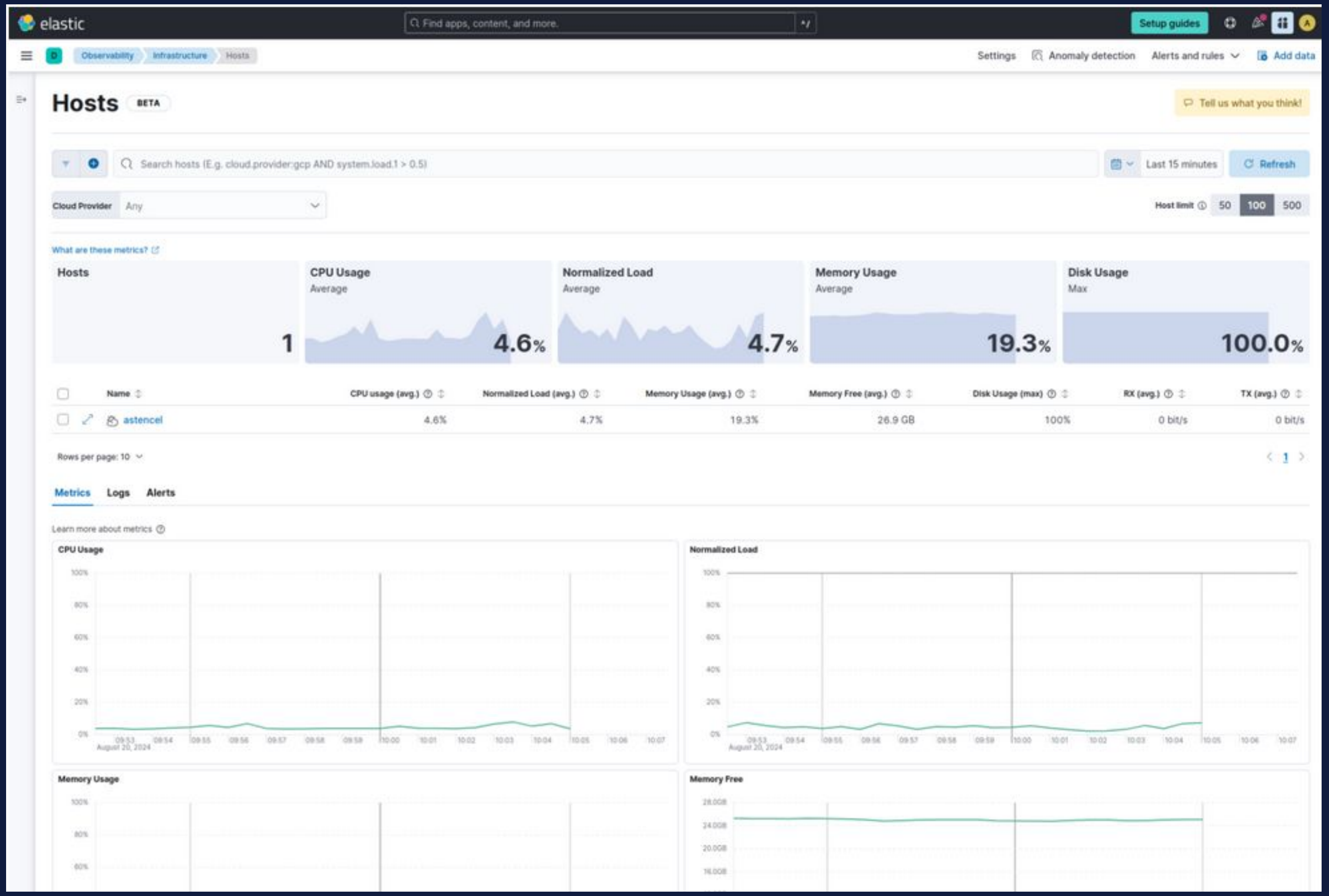
Run the following command on your host to download and configure the collector.

```
arch=$(if ([[ $(arch) == "arm" || $(arch) == "aarch64" ]]); then echo "arm64"; else echo $(arch); fi)

curl --output elastic-distro-8.15.0-linux-$arch.tar.gz --url https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-
agent-8.15.0-linux-$arch.tar.gz --proto '=https' --tlsv1.2 -fOL && mkdir -p elastic-distro-8.15.0-linux-$arch && tar -xvf elastic-
distro-8.15.0-linux-$arch.tar.gz -C "elastic-distro-8.15.0-linux-$arch" --strip-components=1 && cd elastic-distro-8.15.0-linux-$arch

sudo setcap 'cap_dac_read_search=ep' ./data/elastic-agent-*/elastic-agent

rm ./otel.yml && cp ./otel_samples/platformlogs_hostmetrics.yml ./otel.yml && mkdir -p ./data/otelcol && sed -i 's#\${env:STORAGE_DIR}
#'"$PWD"/data/otelcol'#g' ./otel.yml && sed -i 's#\${env:ELASTIC_ENDPOINT}#https://[redacted].eu-
west-1.aws.found.io:443#g' ./otel.yml && sed -i 's/\${env:ELASTIC_API_KEY}/
[redacted]/g' ./otel.yml
```



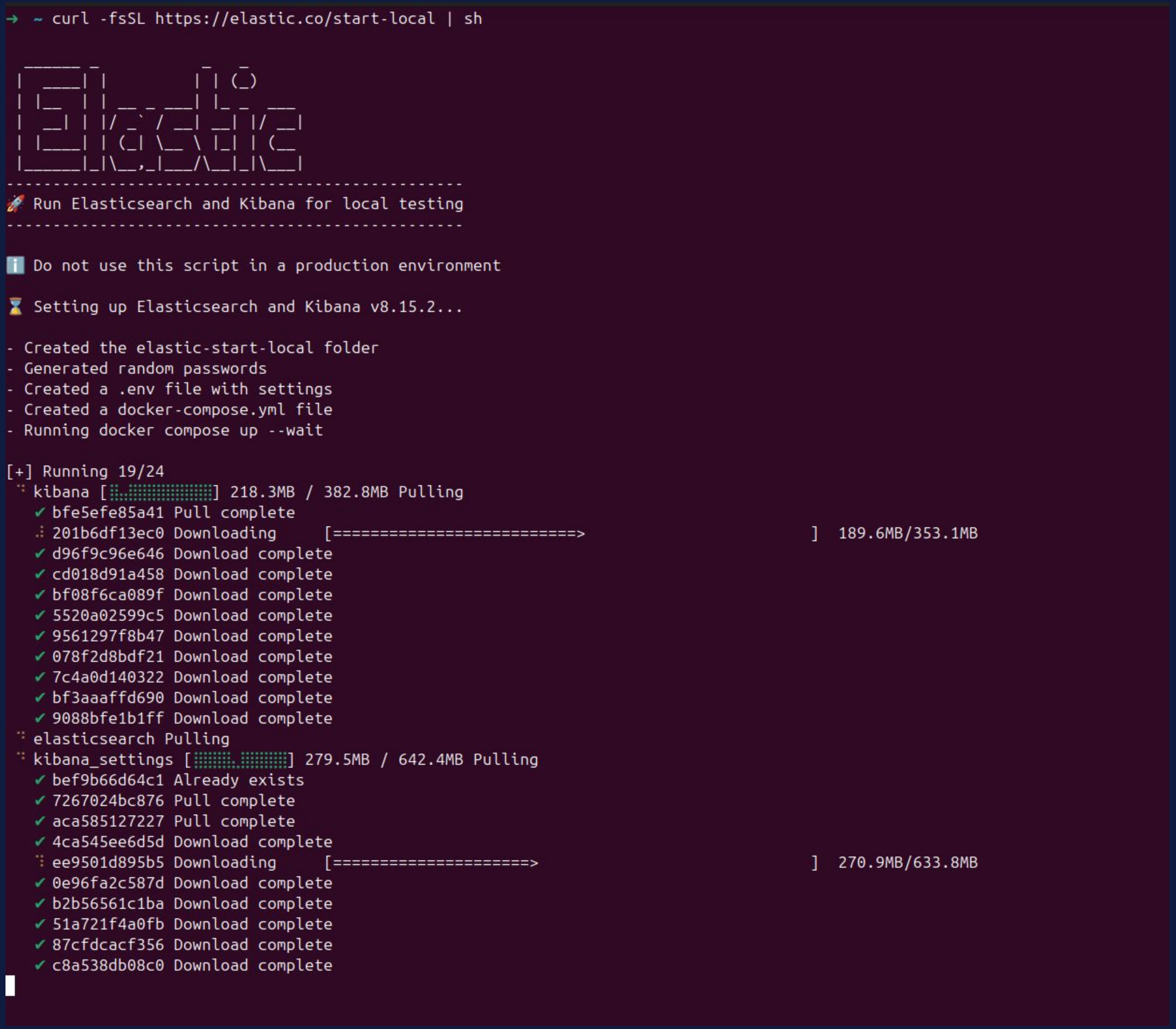
| Name | CPU usage (avg.) | Normalized Load (avg.) | Memory Usage (avg.) | Memory Free (avg.) | Disk Usage (max) | RX (avg.) | TX (avg.) |
|---|---|---|---|---|---|---|---|
| astencel | 4.6% | 4.7% | 19.3% | 26.9 GB | 100% | 0 bit/s | 0 bit/s |

Announcement: https://www.elastic.co/blog/whats-new-elastic-observability-8-15-0#introducing-the-elastic-distro-for-opentelemetry-collector

Walkthrough: https://andrzej-stencel.github.io/2024/08/28/elastic-distro-with-elastic-cloud.html

# Start Elasticsearch and Kibana locally

$ curl -fsSL https://elastic.co/start-local | sh



```
➜  ~ curl -fsSL https://elastic.co/start-local | sh

  ______ _           _   _
 |  ____| |         | | (_)
 | |__  | | __ _ ___| |_ _  ___
 |  __| | |/ _` / __| __| |/ __|
 | |____| | (_| \__ \ |_| | (__
 |______|_|\__,_|___/\__|_|\___|
-------------------------------------------------
🚀 Run Elasticsearch and Kibana for local testing
-------------------------------------------------

ℹ️ Do not use this script in a production environment

⌛ Setting up Elasticsearch and Kibana v8.15.2...

- Created the elastic-start-local folder
- Generated random passwords
- Created a .env file with settings
- Created a docker-compose.yml file
- Running docker compose up --wait

[+] Running 19/24
 ⠹ kibana [⣿⣀⣿⣿⣿⣿⣿⣿⣿⣿⣿] 218.3MB / 382.8MB Pulling
   ✔ bfe5efe85a41 Pull complete
   ⠼ 201b6df13ec0 Downloading     [==========================>                         ]  189.6MB/353.1MB
   ✔ d96f9c96e646 Download complete
   ✔ cd018d91a458 Download complete
   ✔ bf08f6ca089f Download complete
   ✔ 5520a02599c5 Download complete
   ✔ 9561297f8b47 Download complete
   ✔ 078f2d8bdf21 Download complete
   ✔ 7c4a0d140322 Download complete
   ✔ bf3aaaffd690 Download complete
   ✔ 9088bfe1b1ff Download complete
 ⠹ elasticsearch Pulling
 ⠹ kibana_settings [⣿⣿⣿⣿⣀⣿⣿⣿⣿⣿] 279.5MB / 642.4MB Pulling
   ✔ bef9b66d64c1 Already exists
   ✔ 7267024bc876 Pull complete
   ✔ aca585127227 Pull complete
   ✔ 4ca545ee6d5d Download complete
   ⠹ ee9501d895b5 Downloading     [=====================>                              ]  270.9MB/633.8MB
   ✔ 0e96fa2c587d Download complete
   ✔ b2b56561c1ba Download complete
   ✔ 51a721f4a0fb Download complete
   ✔ 87cfdcacf356 Download complete
   ✔ c8a538db08c0 Download complete
█
```

Run Elasticsearch locally | Elasticsearch Guide

# Pozwólcie, że się przedstawię

## Andrzej Stencel

Senior Software Engineer at Elastic

Maintainer w projekcie OpenTelemetry Collector Contrib

Link do slajdów:

https://andrzej-stencel.github.io/2024/11/21/sysops-devops-meetup.html

# Ręce do góry:

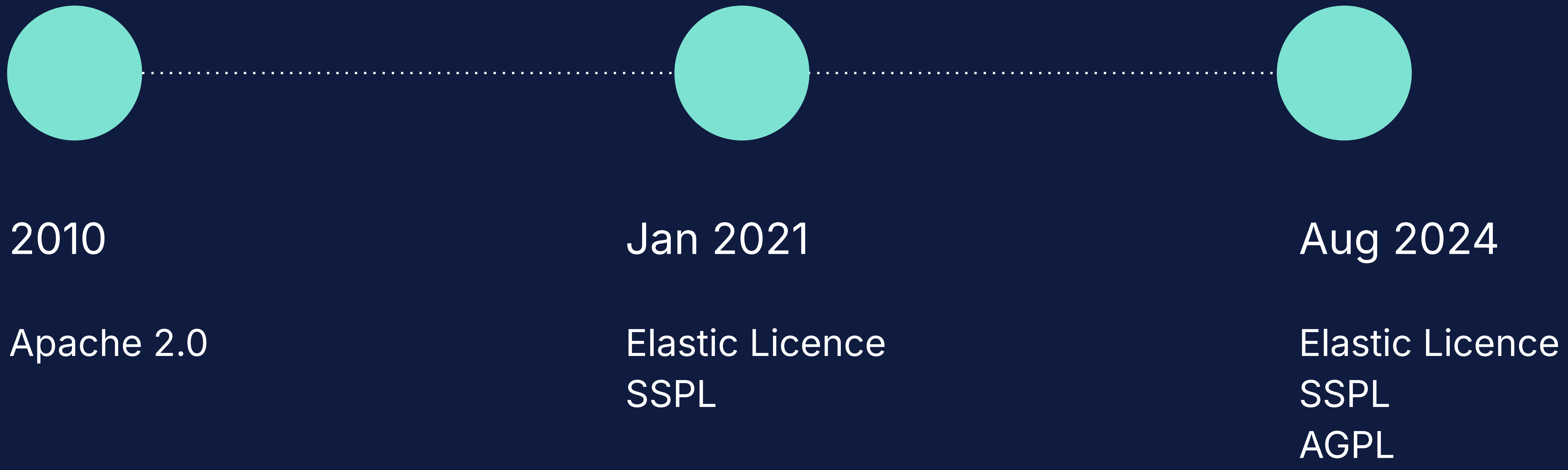
Czy słyszałeś o OpenTelemetry?

Czy używałeś OpenTelemetry w pracy?

Czy używałeś OpenTelemetry na produkcji?

# 🎉 Elasticsearch is open source again 🎉

https://www.elastic.co/blog/elasticsearch-is-open-source-again



2010

Apache 2.0

Jan 2021

Elastic Licence
SSPL

Aug 2024

Elastic Licence
SSPL
AGPL

# Observability? Znaczy co?

> Observability is the ability to understand the internal state of a system by examining its outputs. In the context of software, this means being able to understand the internal state of a system by examining its telemetry data, which includes traces, metrics, and logs.

OpenTelemetry docs

# OpenTelemetry - dlaczego?

- Vendor neutral specification, implementation
- Interoperability thanks to a standard protocol - OTLP
- Vendor-neutral telemetry with OTel semantic conventions
- Already rich, growing ecosystem
  - (auto-)instrumentation libraries
  - OpenTelemetry Operator
  - OpenTelemetry Kube Stack
  -

https://opentelemetry.io/docs/what-is-opentelemetry/#why-opentelemetry

# OpenTelemetry Collector:
## File Log receiver

```
receivers:
  filelog:
    include:
      - /var/log/*.log
    exclude:
      - /var/log/kern.log
    start_at: beginning     # the default is “end”
    storage: file_storage
```

# OpenTelemetry Collector:
## Host Metrics receiver

```
receivers:
  hostmetrics:
    collection_interval: 10s
    scrapers:
      cpu:
        metrics:
          system.cpu.time:
            enabled: false
          system.cpu.utilization:
            enabled: true
```

# OpenTelemetry Collector: More receivers

- Core receivers: OTLP, Nop
- Contrib receivers

# OpenTelemetry Collector:
# Elasticsearch exporter

```
exporters:
  elasticsearch:
    endpoint: "http://localhost:9200"
    api_key: ${env:ES_API_KEY}
    flush:
      interval: 1s
    mapping:
      mode: ecs
    logs_dynamic_index:
      enabled: true
    metrics_dynamic_index:
      enabled: true
    traces_dynamic_index:
      enabled: true
```

# OpenTelemetry Collector:
# Debug exporter

```
exporters:
  debug:
    use_internal_logger: true
    verbosity: normal            # basic, detailed
```

Use `use_internal_logger: false` to:

- prevent sampling of exporter's output
- prevent output from disappearing when `service::telemetry::log::level` is set to `warn` or `error`
- separate output from collector logs and redirect to a file with `> debug-output.txt`

# OpenTelemetry Collector: More exporters

- Core: OTLP, OTLP/HTTP, Nop

- Contrib exporters

# OpenTelemetry Collector:
## File Storage extension

```
extensions:
  file_storage:
    create_directory: true
    directory: ./otel-data
```

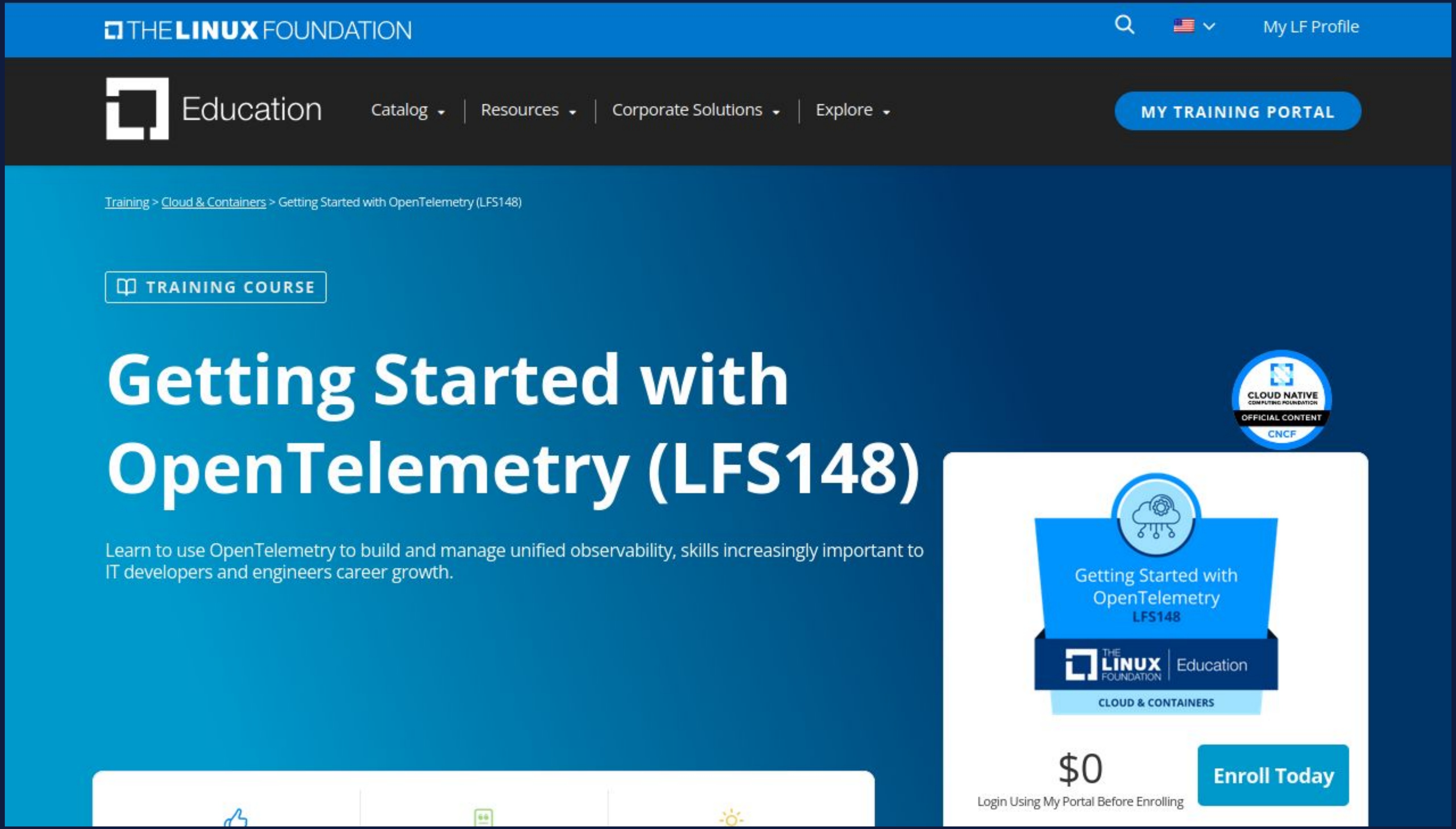
# OpenTelemetry Collector: More extensions

- Core: zPages

- Contrib extensions

# New: Free OpenTelemetry training from CNCF

https://training.linuxfoundation.org/training/getting-started-with-opentelemetry-lfs148/



THE LINUX FOUNDATION

My LF Profile

Education

Catalog | Resources | Corporate Solutions | Explore

MY TRAINING PORTAL

Training > Cloud & Containers > Getting Started with OpenTelemetry (LFS148)

TRAINING COURSE

Getting Started with OpenTelemetry (LFS148)

Learn to use OpenTelemetry to build and manage unified observability, skills increasingly important to IT developers and engineers career growth.

CLOUD NATIVE COMPUTING FOUNDATION
OFFICIAL CONTENT
CNCF
Getting Started with OpenTelemetry
LFS148
THE LINUX FOUNDATION | Education
CLOUD & CONTAINERS

$0

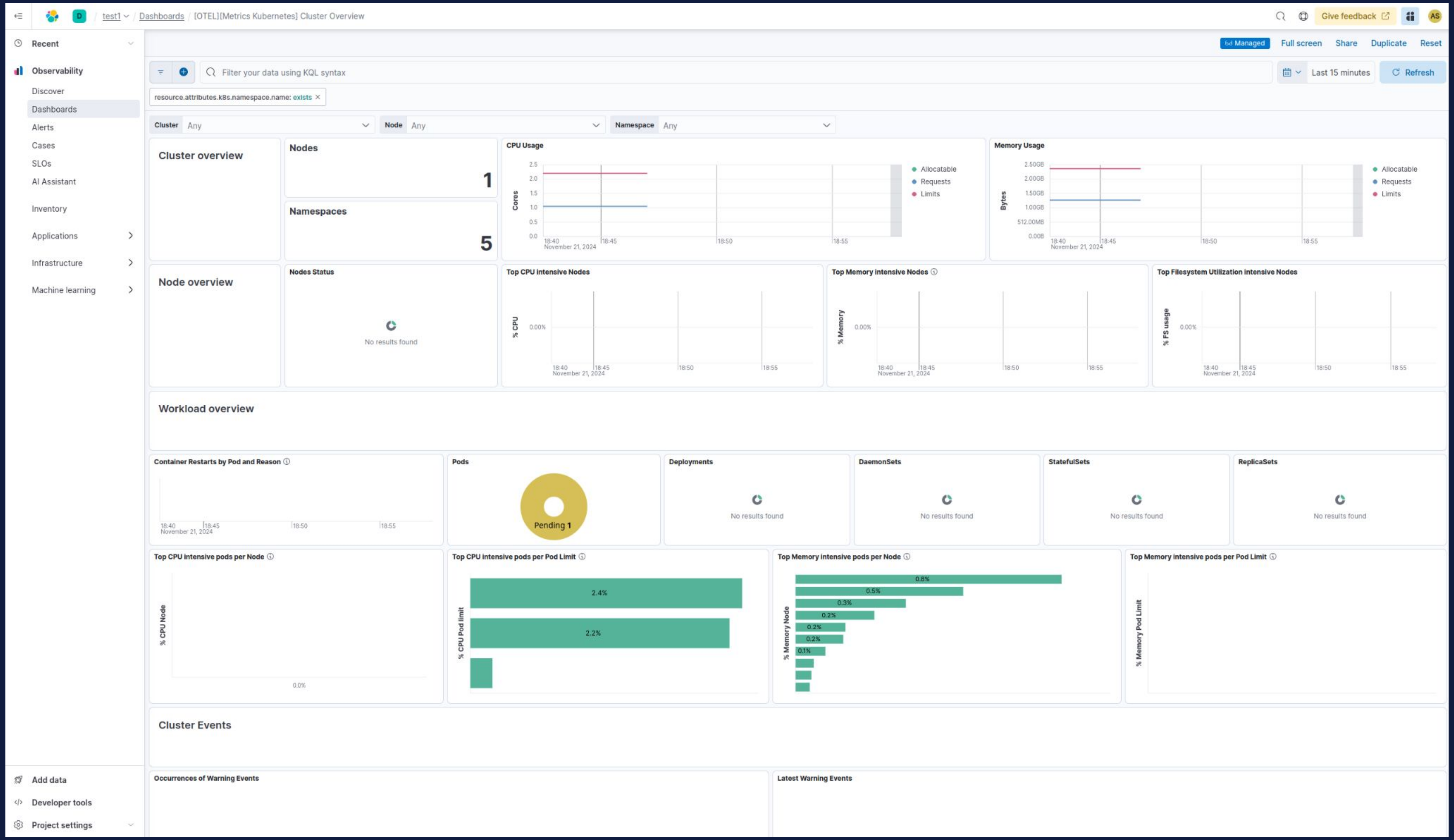
Login Using My Portal Before Enrolling

Enroll Today

# Bonus DEMO

## Collecting telemetry from workloads in Kubernetes with OpenTelemetry Operator

https://www.elastic.co/observability-labs/blog/elastic-opentelemetry-otel-operator



# Pytania?

Slides: https://andrzej-stencel.github.io/2024/11/21/sysops-devops-meetup.html

elastic | The Search AI Company

Feedback: https://freesuggestionbox.com/pub/whqnnke