



Open source observability z OpenTelemetry i Elasticsearch

Andrzej Stencel

Zielona Góra JUG Meetup

Zielona Góra, 5 grudnia 2024

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/2024/12/05/jug-zg-meetup.html>

Observability? Znaczy co?



66

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](#)

66

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.

Obserwowalność to zdolność zrozumienia stanu wewnętrznego systemu poprzez badanie jego wyników. W kontekście oprogramowania oznacza to zdolność zrozumienia stanu wewnętrznego systemu poprzez badanie jego danych telemetrycznych, które obejmują ślady, metryki i logi.

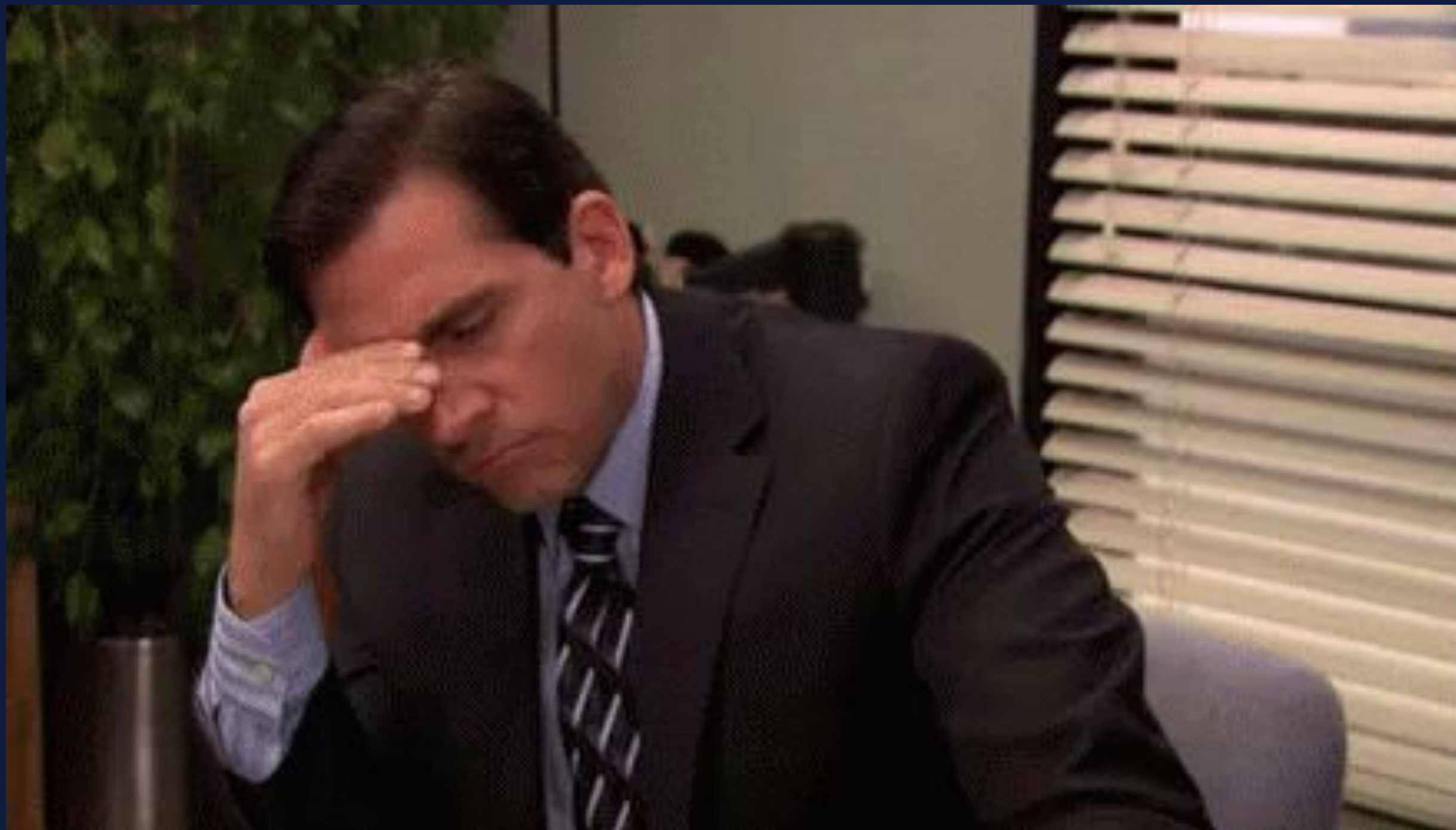
[OpenTelemetry docs](#)

[Google Translate](#)

Observability? A po co to komu?

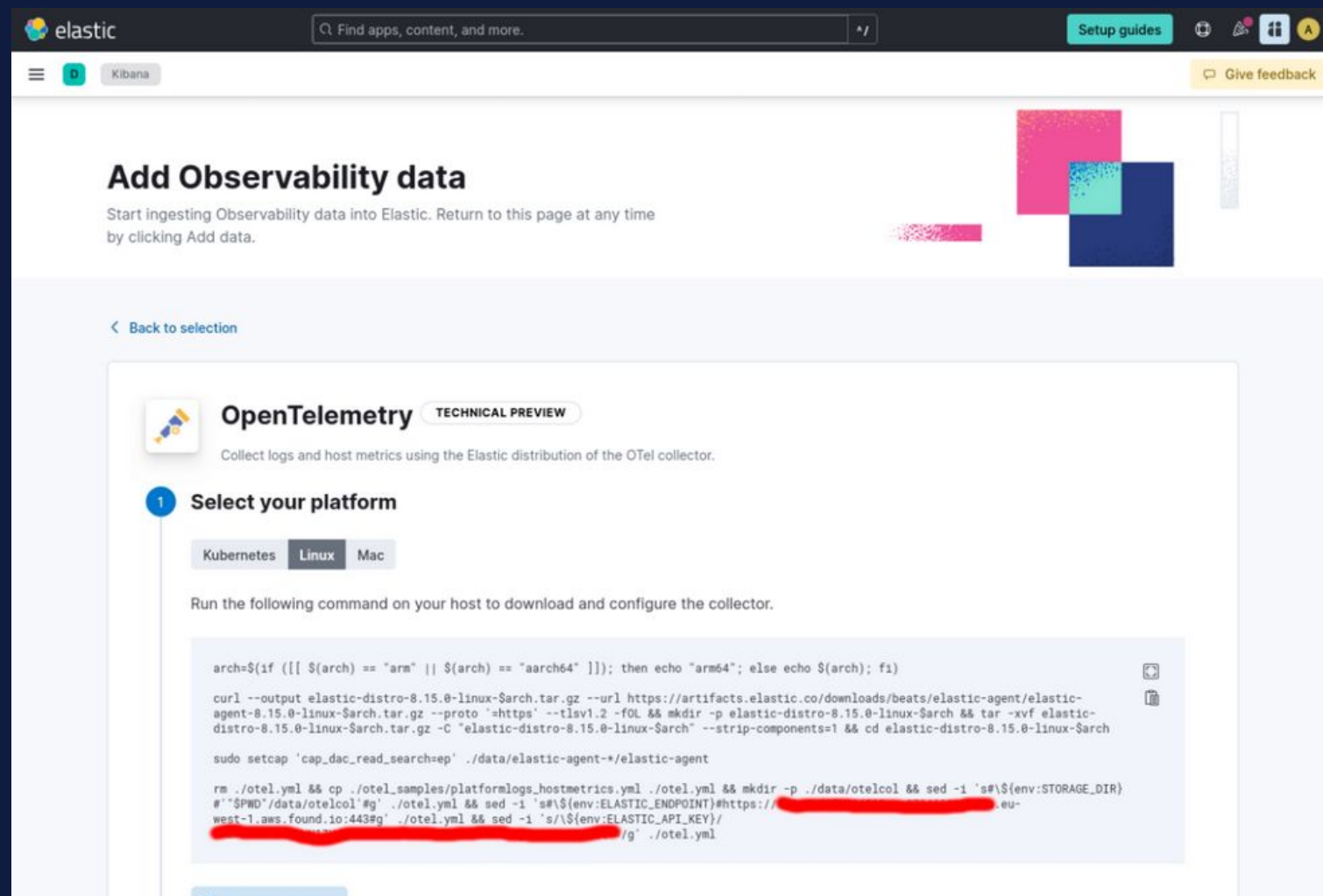


Observability? A jak to się robi?



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 TECHNICAL PREVIEW

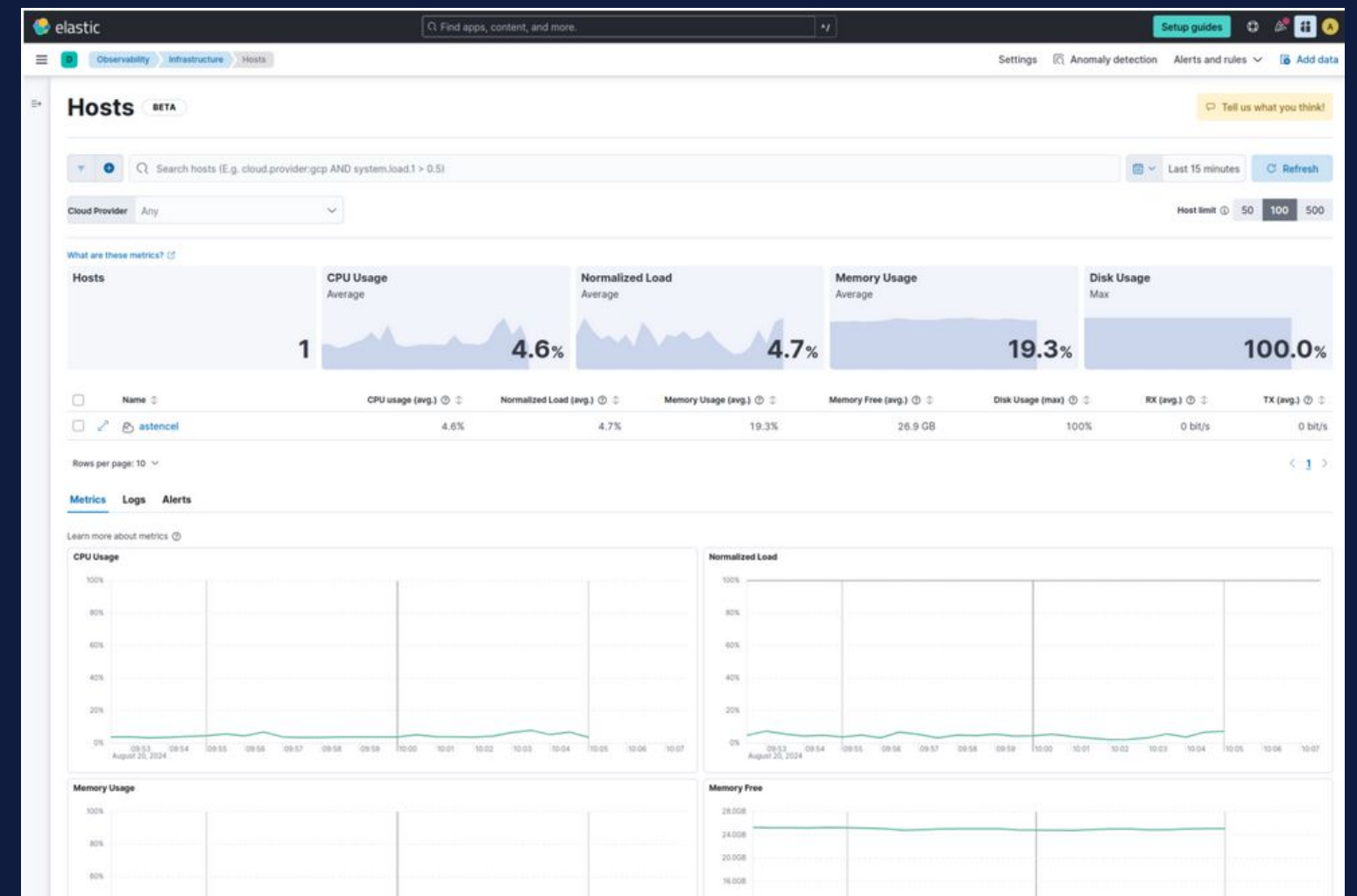
Collect logs and host metrics using the Elastic distribution of the OTel collector.

1 Select your platform

Kubernetes Linux Mac

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-$arch.tar.gz --proto https --tlsv1.2 -fL && mkdir -p elastic-distro-8.15.0-linux-$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-$arch
sudo setcap 'cap_dac_read_searchep' ./data/elastic-agent-*/elastic-agent
rm ./otel.yml && cp ./otel_samples/platformlogs_hostmetrics.yml ./otel.yml && mkdir -p ./data/otelcol && sed -i 's#$(env:STORAGE_DIR)#$(env:STORAGE_DIR)#g' ./otel.yml && sed -i 's#$(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
```



Hosts BETA

Search hosts (E.g. cloud.provider:gcp AND system.load1 > 0.5)

Cloud Provider: Any

Host limit: 50 100 500

Hosts	CPU Usage Average	Normalized Load Average	Memory Usage Average	Disk Usage Max
astencil	4.6%	4.7%	19.3%	100.0%

Rows per page: 10

Metrics Logs Alerts

Learn more about metrics

CPU Usage

Normalized Load

Memory Usage

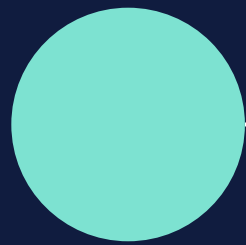
Memory Free

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>

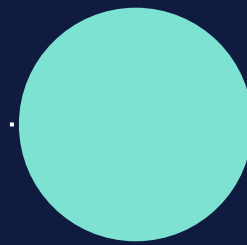
🎉 Elasticsearch is open source again 🎉

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



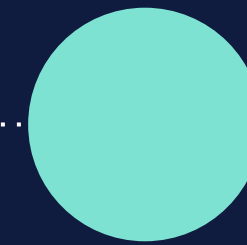
2010

Apache 2.0



Jan 2021

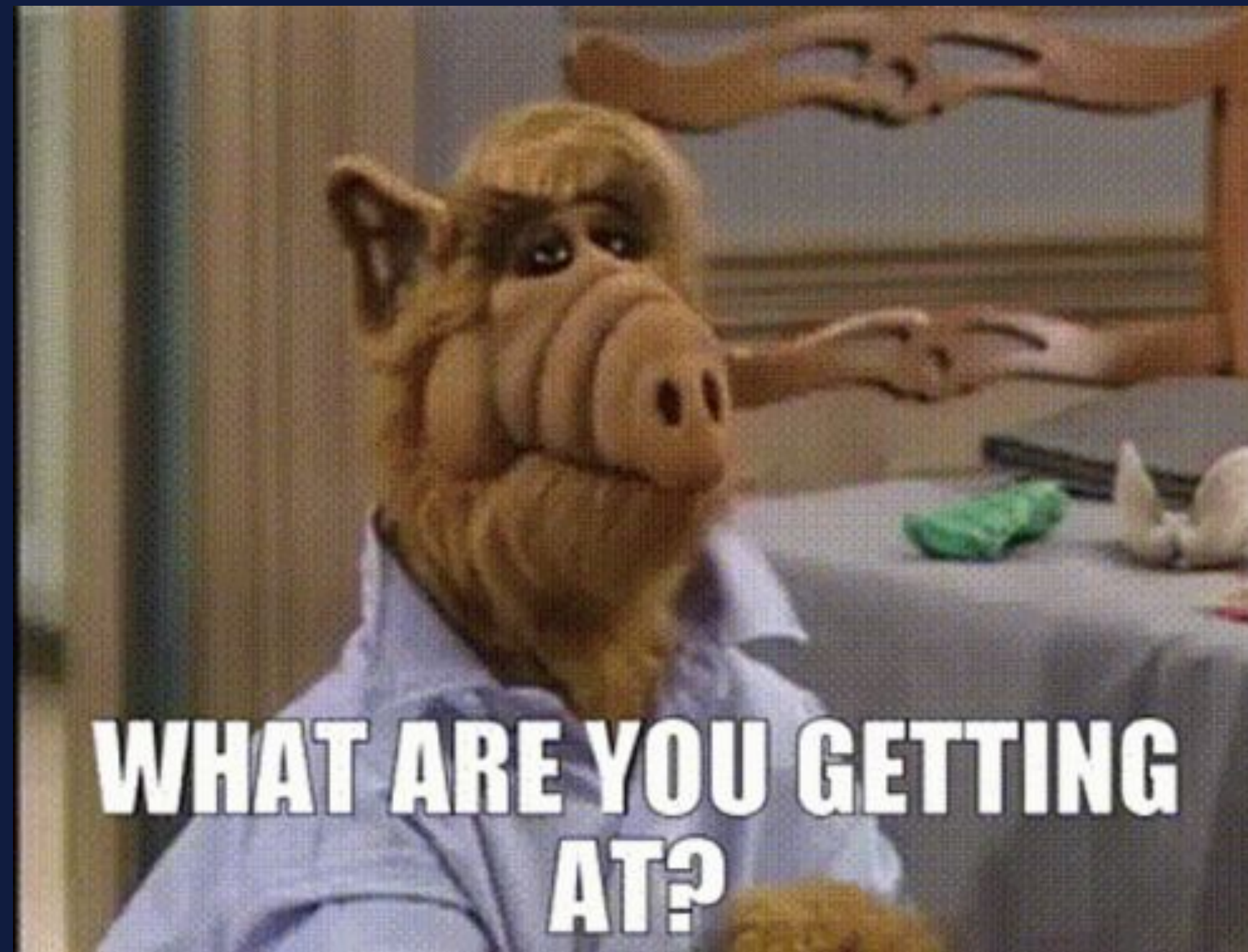
Elastic Licence
SSPL



Aug 2024

Elastic Licence
SSPL
AGPL

Co z tym OpenTelemetry?



Co z tym OpenTelemetry?

- Ograniczenia i limity nie interesują mnie!
- Projekt powstał w 2019 roku z połączenia projektów OpenTracing oraz OpenCensus
- Projekt zarządzany przez Cloud Native Computing Foundation, niezależny od żadnego konkretnego dostawcy.
- Wsparcie od największych dostawców rozwiązań observability

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

Co mi daje OpenTelemetry?

- Specyfikacja niezależna od dostawcy (np. logi)
- Konwencje nazewnnicze niezależne od dostawcy usługi - host.name, service.name itd.
- Korelacja - powiązanie logów, metryk, ~~trace'ów~~ śladów
- Rosnący ekosystem gotowych narzędzi
 - Biblioteki do (auto)instrumentacji (np. dla Javy)
 - OpenTelemetry Collector
 - Operator dla Kubernetes
 - Kolejny operator dla Kubernetes
 - <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 # domyślna wartość: "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: Transform processor

```
processors:  
  transform:  
    log_statements:  
      - context: log  
        statements:  
          - set(severity_text, "FAIL") where body == "request failed"
```


OpenTelemetry Collector:

Filter processor

```
processors:  
  filter:  
    metrics:  
      metric:  
        - 'name == "my.metric" and resource.attributes["my_label"] == "abc123"'
```

OpenTelemetry Collector: More processors

- Attributes processor
- Resource processor
- Kubernetes Attributes processor
- Tail Sampling processor (for traces)

- Other Contrib processors

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
 - Basic Authentication
 - Bearer Token Authentication
 - Health Check (for Kubernetes)

OpenTelemetry Collector: connectors

Connected Observability Pipelines in the OpenTelemetry Collector



OpenTelemetry Collector: Pipelines

```
service:  
  pipelines:  
    logs/my-logs:  
      receivers:  
        - filelog/my-files  
      processors:  
        - transform/do-this  
        - filter/remove-that  
      exporters:  
        - elasticsearch  
        - debug
```

```
metrics/from-host:  
  receivers:  
    - hostmetrics  
  processors:  
    - transform/another  
    - filter/yet-another  
  exporters:  
    - awss3  
    - debug
```

```
traces/from-apps:  
  receivers: [otlp]  
  processors: [tail_sampling]  
  exporters: [otlp]
```

OpenTelemetry Collector: Putting it all together

Przejrzymy konfigurację z pierwszego DEMO

OpenTelemetry: Czy to jest gotowe?



New: Free OpenTelemetry training from CNCF

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

THE **LINUX** FOUNDATION

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

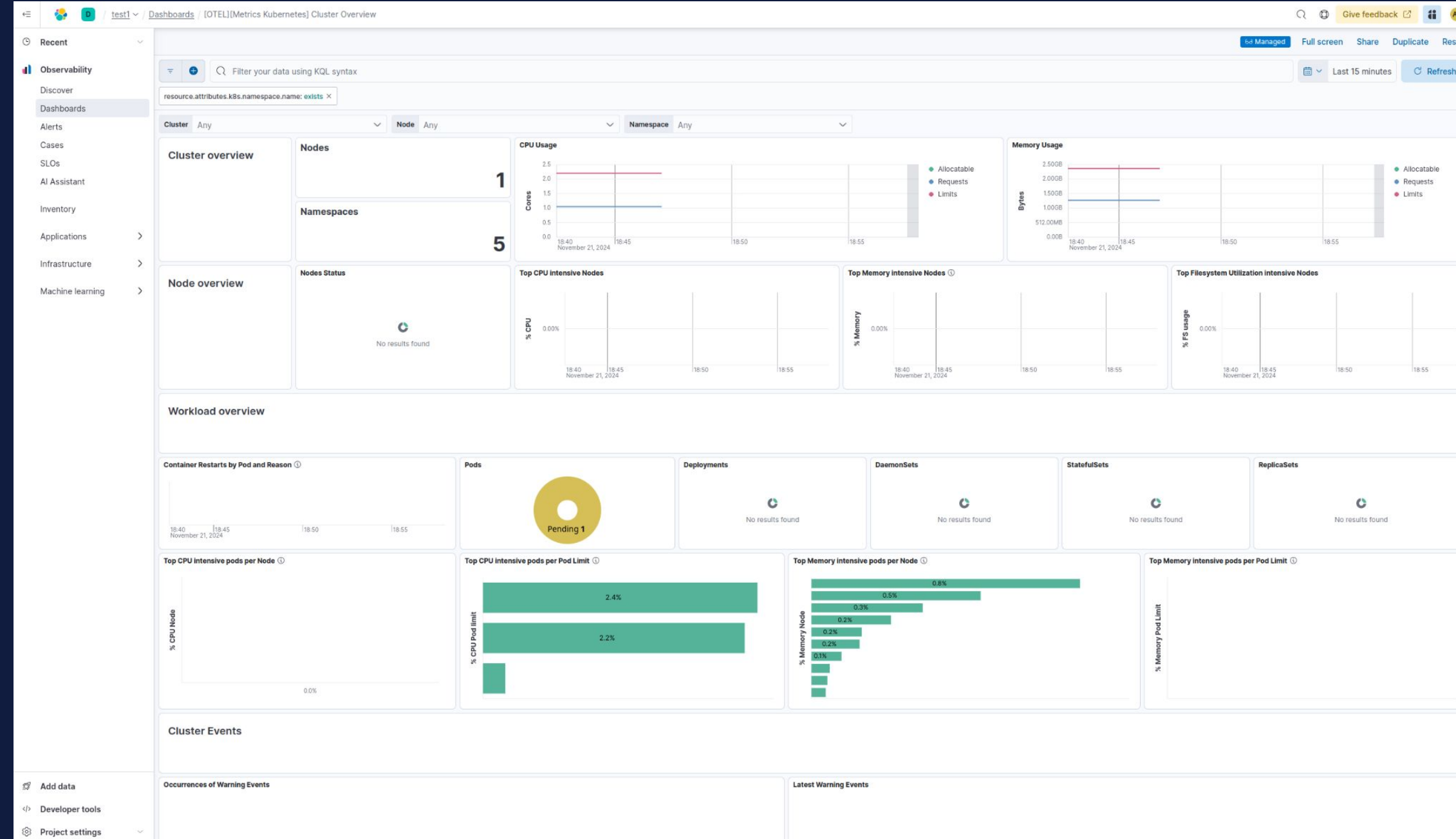
Enroll Today

Login Using My Portal Before Enrolling

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/2024/12/05/jug-zg-meetup.html>



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