Kris Buytaert @krisbuytaert

Bow for me, for I am coroot

OSMC 2024

Who am I ?

- I used to be a developer
- Then I became an Ops person
- Chief Trolling/Travel/Technical Officer @ Inuits.eu
- Chief Yak Shaver @ o11y.eu
- Organiser of #devopsdays, #cfgmgmtcamp, #loadays, …
- Cofounder of all of the above
- Everything is a Freaking DNS Problem
- DNS : devops needs sushi
- @krisbuytaert on twitter/github/
- @mastodon.social/@krisbuytaert

Why this title ?

Observability is the new Hype

- Docker, Docker, Docker, Docker, Docker, Docker…
- Kubernetes, Kubernetes, Kubernetes, Kubernetes, Kubernetes, Kubernetes,
- O11y, o11y, o11y, o11y, o11y, o11y, o11y,
- We’re all doing this, right ?
- This is the new default, right . ?

What is monitoring?

- High level overview of the state of a service/component
- Availability
- Technical components
- Performance ?

What is going on?

What's observability?

- Understand how your services behave
- Like you are at their place
- Without incident specific code

Why is this going on?

What's observability - in Practice?

Are there Three pillars:

- Metrics
- Logs
- Traces

The Fourth Pillar

Maybe it’s not Pillars, but layers.

How do monitoring and observability connect?

- Monitoring is required
- If lucky, monitoring is enough
- Observability is removing luck <- @roidelapluie
- It’s the next layer up …

It’s not new

Remember Packetbeat ?

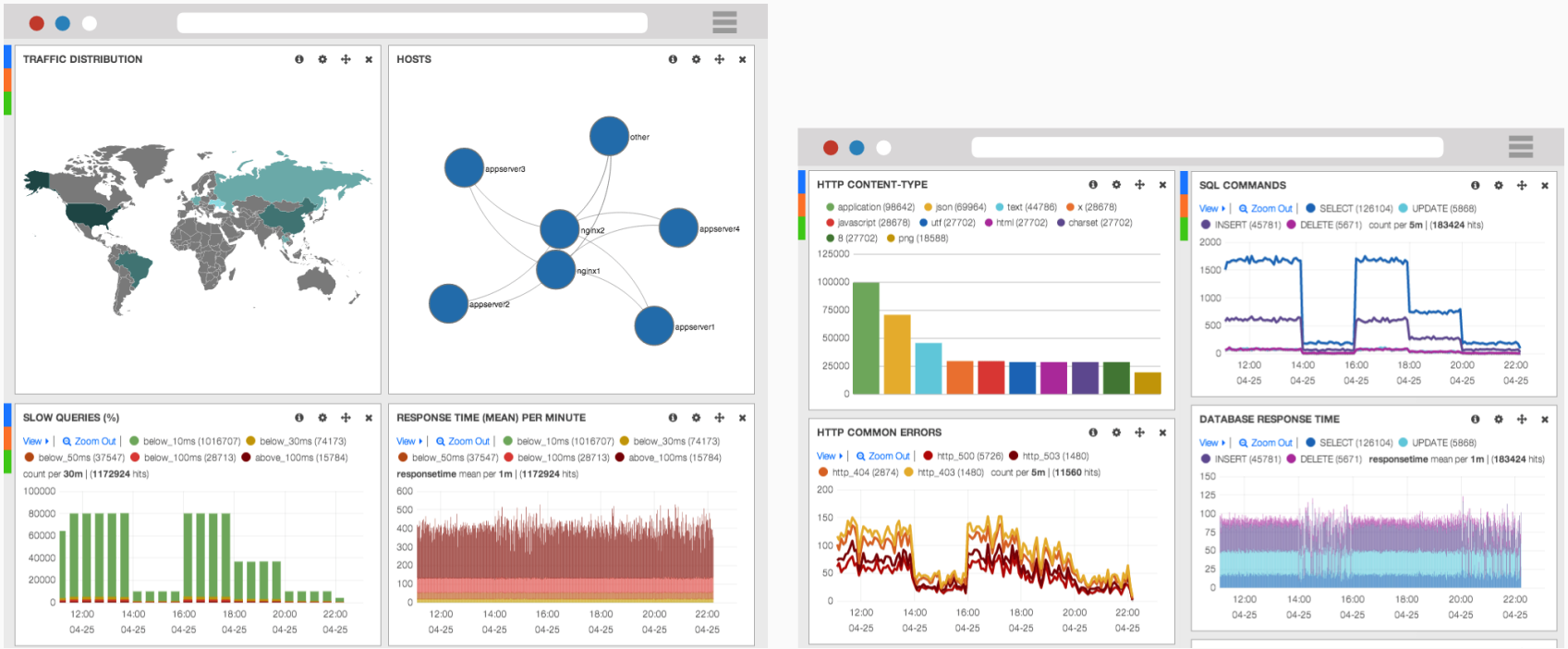


Figure 2: Nostalgia

Where is the real observability ?

- Often we have metrics
- But only for a month
- Often we lost our long term metrics
- Often we have logs
- But no derived metrics
- We are only alerting on those metrics
- We are not learning from our metrics
- We've regressed

Please Fix your Monitoring first …

- SSOT , 100% automated monitoring
- No manual configuration tolerated
- Fix your metrics
- I bet you have regression on shipping your Metrics
- Fix your log shipping
- I bet you logshipping is partially broken
- I bet you have broken dashboards

OpenTelemetry

- Protocol
- SDK's
- Signals
  - Traces (stable)
  - Metrics (stable)
  - Logs (stable)
  - Profiles (wip Q1 2025)
  - RUM (wip)
- OtelCollector

OpenTelemetry

- Top CNCF Project
- “Vendor Driven Standardisation”
- Protocol, not implementation
- Claims AutoInstrumentation,
- Different components have different maturity levels
- Different languages have different maturity levels (11)

There is no magic

Paul Johnston - current focus: moving electrons
@PaulDJohnston

This.

Cannot believe how many people think that generalised instrumentation is somehow the "best" solution.

"What do I need to know? It would be good to instrument exactly that wouldn't it!"

Getting data and querying is hard.

Producing the data you need in the first place? 👍

Luc van Donkersgoed @donkersgood · Sep 10

Replying to @dfrasca80 and @honeycombio

Not a silly question at all! OpenTelemetry supports auto instrumentation, but I'm a strong proponent for manual instrumentation. This allows me to add business context which makes the output WAY more valuable.

Is eBPF the magic ?

- Linux Kernel level
- extended Berkeley Packet filter
- “A marriage of strace + tcpdump on steriods”
- Framework to attach to low level functions
- Framework used to collect statistics
- Framework to build a monitoring tool

Open Source ebpf Tools

- ebpf_exporter
- opentelemetry-network
- Falco (security)
- Coroot
- Pixie (k8s)
- Odigos (k8s)
- Tracee (docker/k8s)
- Caretta (maps your dependencies) (k8s)
- Keppler (power usage / k8s)

The eBPF tooling landscape

- K8s only ..
- Reality is mixed ..

So most of the tools are not useful for the majority of our industry

Coroot

- Open source (Apache 2.0)
- Cloud-agnostic : bare metal, k8s …
- ebpf based exporter
- Ships : metrics, logs and traces
- zero instrumentation
- application AND ebpf based tracing
- SLO Driven alerting
- Fast insight in problems
- Root Cause Detection

Coroot requirements

- Prom Compatible datastore for Metrics
  - e.g Prometheus, Thanos, Mimir, Cortex, Victoria …
  - per project
  - label value too long for metric (actual: 3741, limit: 2048) , configure it large enough
  - used to store metrics
- Clickhouse
  - schema per project
  - Recently added support for clustered tables (still need to test)
  - used to store logs, traces, …
- pgsql (for prod)
  - used to store project information

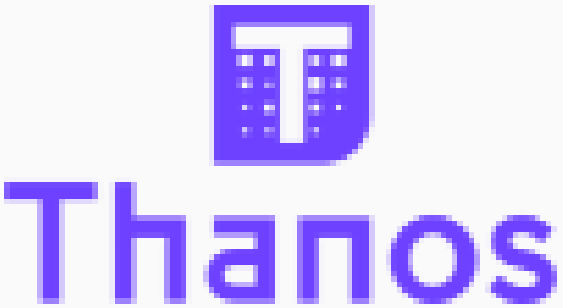
Prometheus

Prometheus

- Prometheus is an Open Source CNCF Project
- Collects and stores metrics - Pull-based
- Framework , not integrated solution
- Exporters for every piece of the infra
- Long-Term Support release (powered by o11y.eu)

Prometheus Compatible MultiTenant Backends

- Thanos



- Cortex

- Mimir

- …

Clickhouse

“ClickHouse is an open-source column-oriented DBMS (columnar database management system) for online analytical processing (OLAP) that allows users to generate analytical reports using SQL queries in real-time.”

- Apache 2.0
- SQL all the things

Clickhouse & Otel

```
clickhouse01.o11ylab.o11y.eu :) show tables;

SHOW TABLES

Query id: 6376d37a-a6b4-4052-92ab-dc1d66713e03

    ┌─name──────────────────────┐
1.  │ otel_logs                 │
2.  │ otel_traces               │
3.  │ otel_traces_trace_id_ts   │
4.  │ otel_traces_trace_id_ts_mv│
5.  │ profiling_profiles        │
6.  │ profiling_profiles_mv     │
7.  │ profiling_samples         │
8.  │ profiling_stacks          │
    └───────────────────────────┘

8 rows in set. Elapsed: 0.003 sec.
```

Clickhouse TTL

```
clickhouse01.o11ylab.o11y.eu :) show create table otel_logs;

SHOW CREATE TABLE otel_logs

Query id: 0badcedc-776f-4d06-b0e7-4f9b8a6e4685

   ┌─statement──────────────────────────────────────────────────────────────
1. │ CREATE TABLE coroot_o11ylab.otel_logs
(
    `Timestamp` DateTime64(9) CODEC(Delta(8), ZSTD(1)),
    `TraceId` String CODEC(ZSTD(1)),
    `SpanId` String CODEC(ZSTD(1)),
    `TraceFlags` UInt32 CODEC(ZSTD(1)),
    `SeverityText` LowCardinality(String) CODEC(ZSTD(1)),
    `SeverityNumber` Int32 CODEC(ZSTD(1)),
    `ServiceName` LowCardinality(String) CODEC(ZSTD(1)),
    `Body` String CODEC(ZSTD(1)),
    `ResourceAttributes` Map(LowCardinality(String), String) CODEC(ZSTD(1)),
    `LogAttributes` Map(LowCardinality(String), String) CODEC(ZSTD(1)),
    INDEX idx_trace_id TraceId TYPE bloom_filter(0.001) GRANULARITY 1,
    INDEX idx_res_attr_key mapKeys(ResourceAttributes) TYPE bloom_filter(0.01) GRANULARITY 1,
    INDEX idx_res_attr_value mapValues(ResourceAttributes) TYPE bloom_filter(0.01) GRANULARITY 1,
    INDEX idx_log_attr_key mapKeys(LogAttributes) TYPE bloom_filter(0.01) GRANULARITY 1,
    INDEX idx_log_attr_value mapValues(LogAttributes) TYPE bloom_filter(0.01) GRANULARITY 1,
    INDEX idx_body Body TYPE tokenbf_v1(32768, 3, 0) GRANULARITY 1
)
ENGINE = MergeTree
PARTITION BY toDate(Timestamp)
ORDER BY (ServiceName, SeverityText, toUnixTimestamp(Timestamp), TraceId)
TTL toDateTime(Timestamp) + toIntervalDay(1)
SETTINGS index_granularity = 8192, ttl_only_drop_parts = 1 │
   └────────────────────────────────────────────────────────────────────────

1 row in set. Elapsed: 0.002 sec.

clickhouse01.o11ylab.o11y.eu :)
```

Coroot deployment options

- helm (k8s)
- puppet
- docker
- docker swarm
- (curl scripts)
- (manually)
- (ping me if you want rpms)

Deploying Coroot

- Install the server,
- Initial connection for default project to prometheus / clickhouse
- Create more individual projects,
- Configure their prometheus / clickhouse backends

Coroot-node-agent

- Install the agent
- configure it to connect to the server with the APIkey for your project
- ships ebpf based metrics / logs / traces to the server
- is an actual prometheus exporter (:10300/metrics)

Coroot-cluster-agent

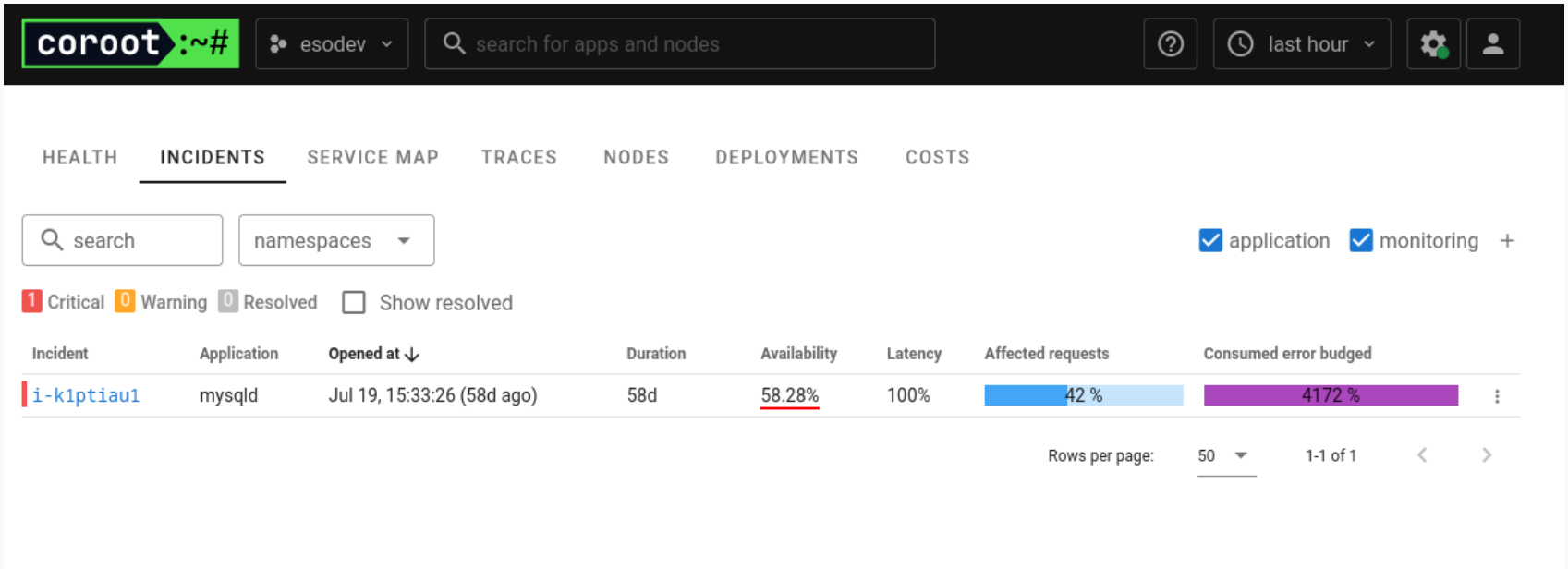
Additional support for instrumentation of

- MySQL
- PgSQL
- Redis
- Mongo

requires coroot-cluster-agent (per project)

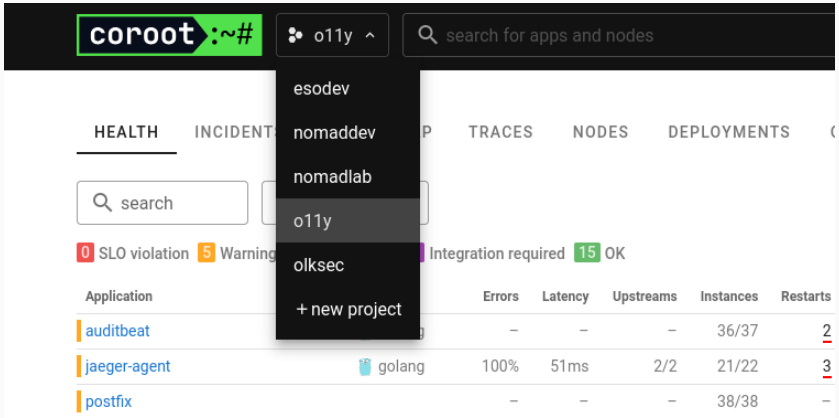
Database Integration Use case

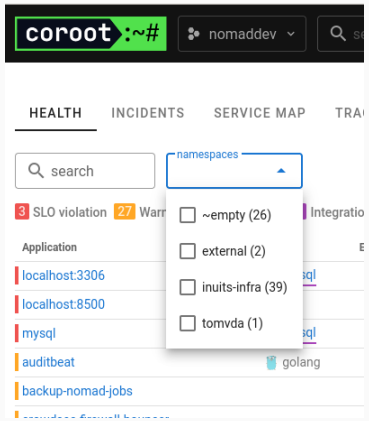
- More in depth details about database
- (more on this incident later)



Projects & Namespaces

- projects map to agents with api-key
- isolated views
- namespaces for k8s / nomad





General Environment Health

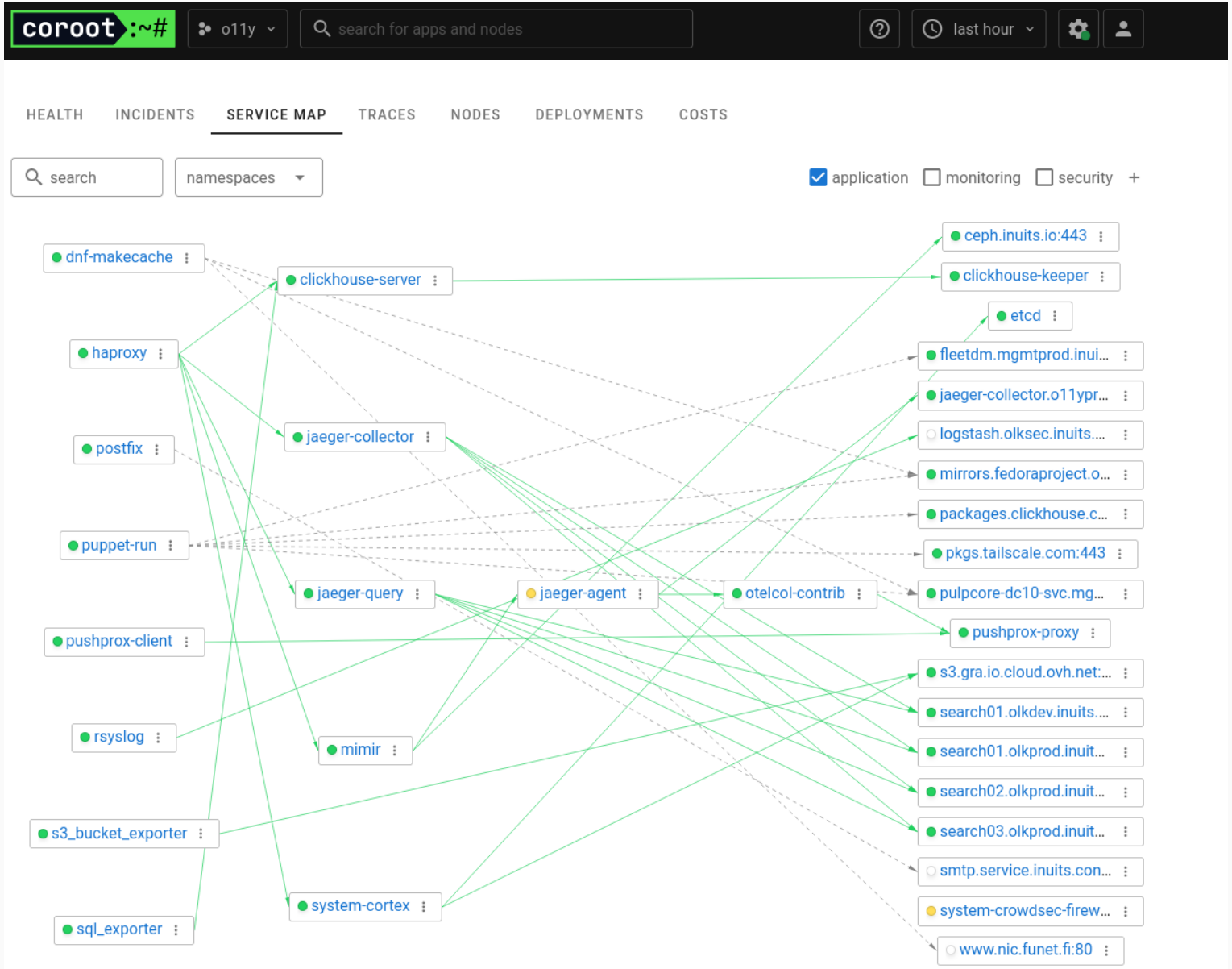
HEALTH | SERVICE MAP | TRACES | NODES | DEPLOYMENTS

search | namespaces | application | monitoring | +

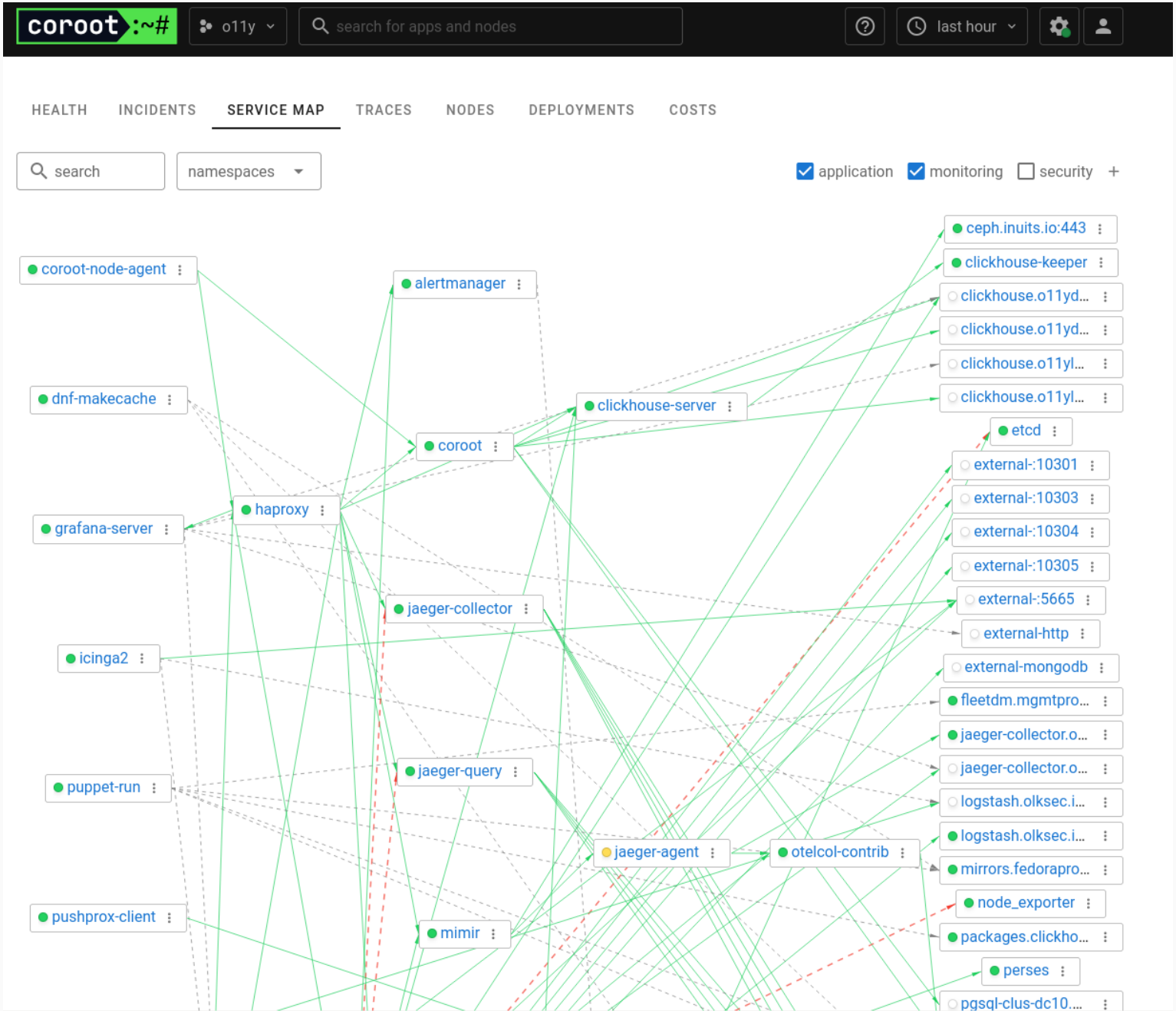
5 SLO violation | 53 Warning | 5 Errors in logs | 44 OK

Application	Errors	Latency	Upstreams	Instances	Restarts	CPU	Mem	I/O	Disk	Net	L
consul	–	10s	55/55	6/6	–	–	–	2%	90%	25ms	
mysql	12%	25ms	–	3/3	–	–	–	<1%	82%	10ms	
mysql-06ebec06-c4ff-902f-80e6-36a...	13%	192ms	0/1	1/1	–	–	–	<1%	3%	failed conns	
mysql-45f329ab-2ef3-29d1-5538-cc...	9%	74ms	0/2	1/1	–	–	–	<1%	3%	25ms	
mysql-4fcfd407-cf7e-8810-a205-05f...	8%	92ms	0/1	1/1	–	–	–	<1%	2%	failed conns	
auditbeat	–	–	–	7/7	–	–	–	2%	93%	26ms	1 uniq
backup-nomad-jobs-5b60a0b5-3b73...	–	–	1/1	0/1	–	–	–	–	–	–	
compactor-160cd7ab-9630-3164-ef...	–	5ms	0/1	1/1	–	–	–	–	–	failed conns	
compactor-6491125d-0e18-7c9e-70...	–	5ms	–	1/1	–	–	–	–	–	failed conns	1 uniq
crowdsec-firewall-bouncer	–	–	1/1	10/10	2158	–	–	<1%	82%	44ms	
distributor-048a9392-dbcd-de17-db...	–	49ms	3/4	1/1	–	–	–	–	–	failed conns	
distributor-62235234-e70b-f793-a09...	–	49ms	1/2	1/1	–	–	–	–	–	failed conns	
distributor-772c1fa9-10e2-1d37-b22...	<1%	49ms	3/4	1/1	–	–	–	–	–	failed conns	
distributor-7a93fd91-f783-d893-b60...	<1%	50ms	3/4	1/1	–	–	–	–	–	failed conns	
distributor-daf5993e-f588-a13a-580...	–	49ms	3/4	1/1	–	–	–	–	–	failed conns	
distributor-e26a2c2d-bf29-6c41-95b...	<1%	49ms	3/4	1/1	–	–	–	–	–	failed conns	
dnf-makecache	–	–	1/1	0/11	–	–	–	–	–	–	
icinga2	–	–	3/4	17/17	–	–	–	2%	93%	failed conns	
ingester-559935ea-58f0-4786-f529-...	–	5ms	0/1	1/1	–	–	–	<1%	2%	failed conns	
ingester-ac391338-00fa-f51b-a3bc-...	–	50ms	0/1	1/1	–	–	–	<1%	3%	failed conns	

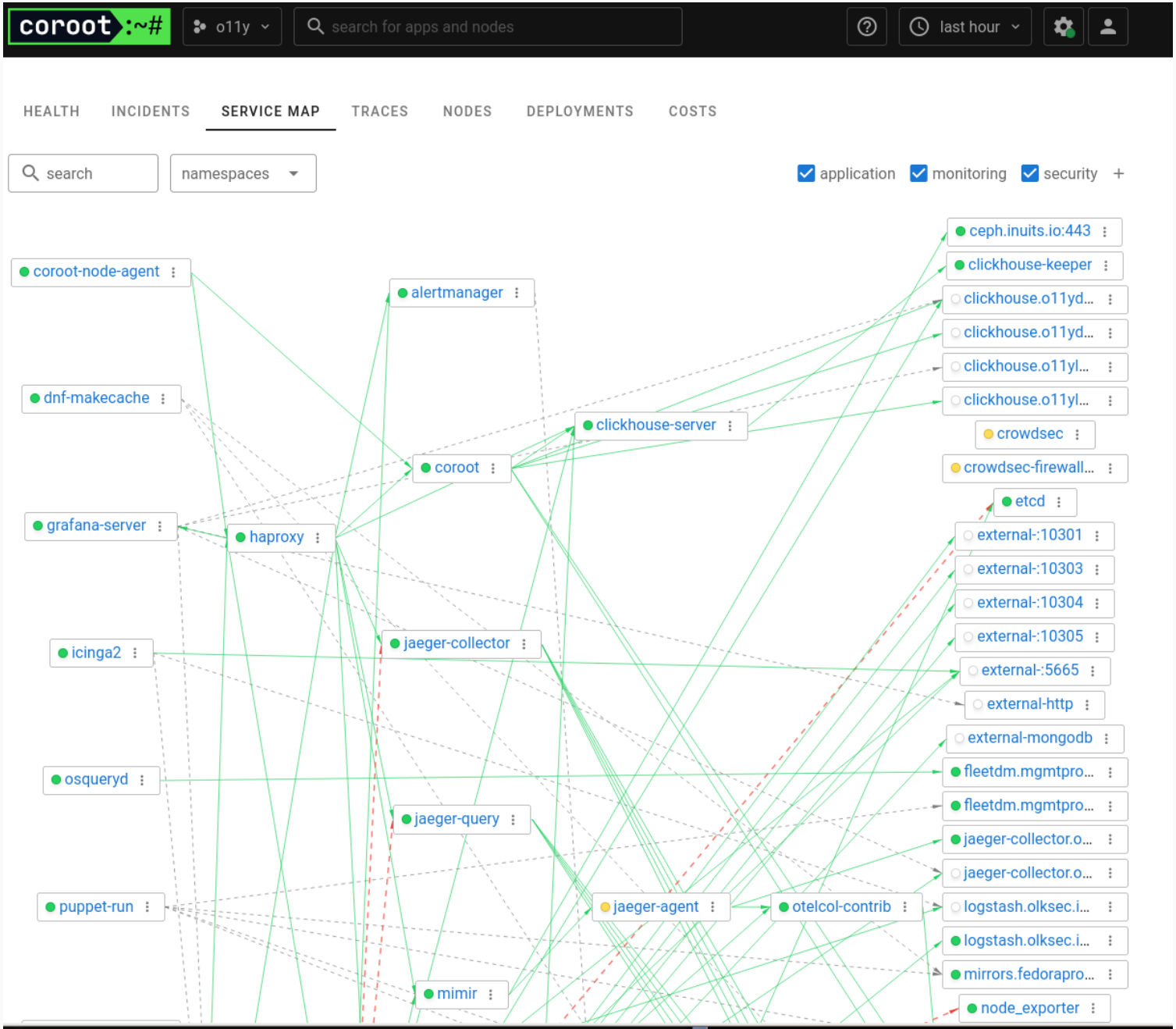
Service Map (Application)



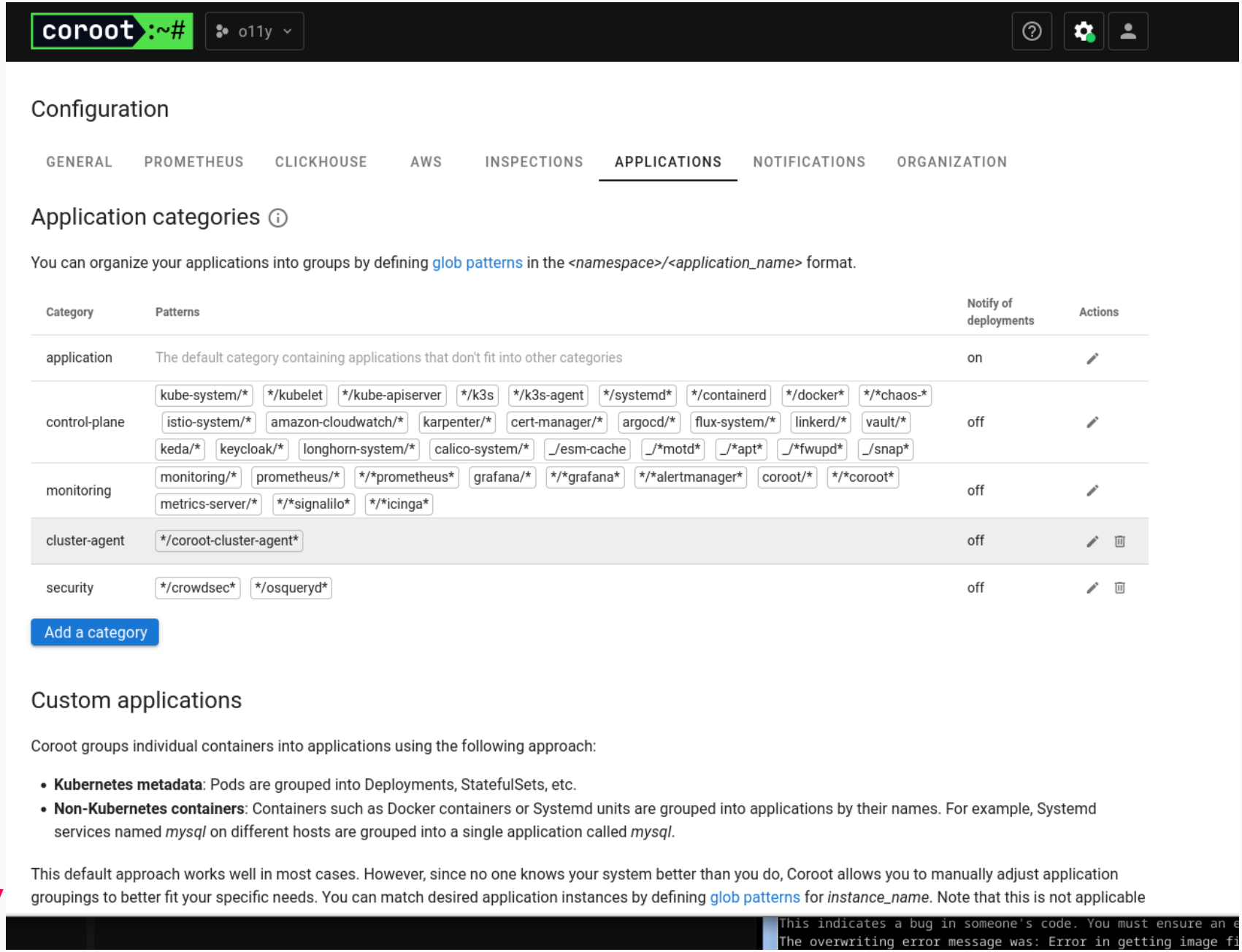
Service Map (App + Monitoring)



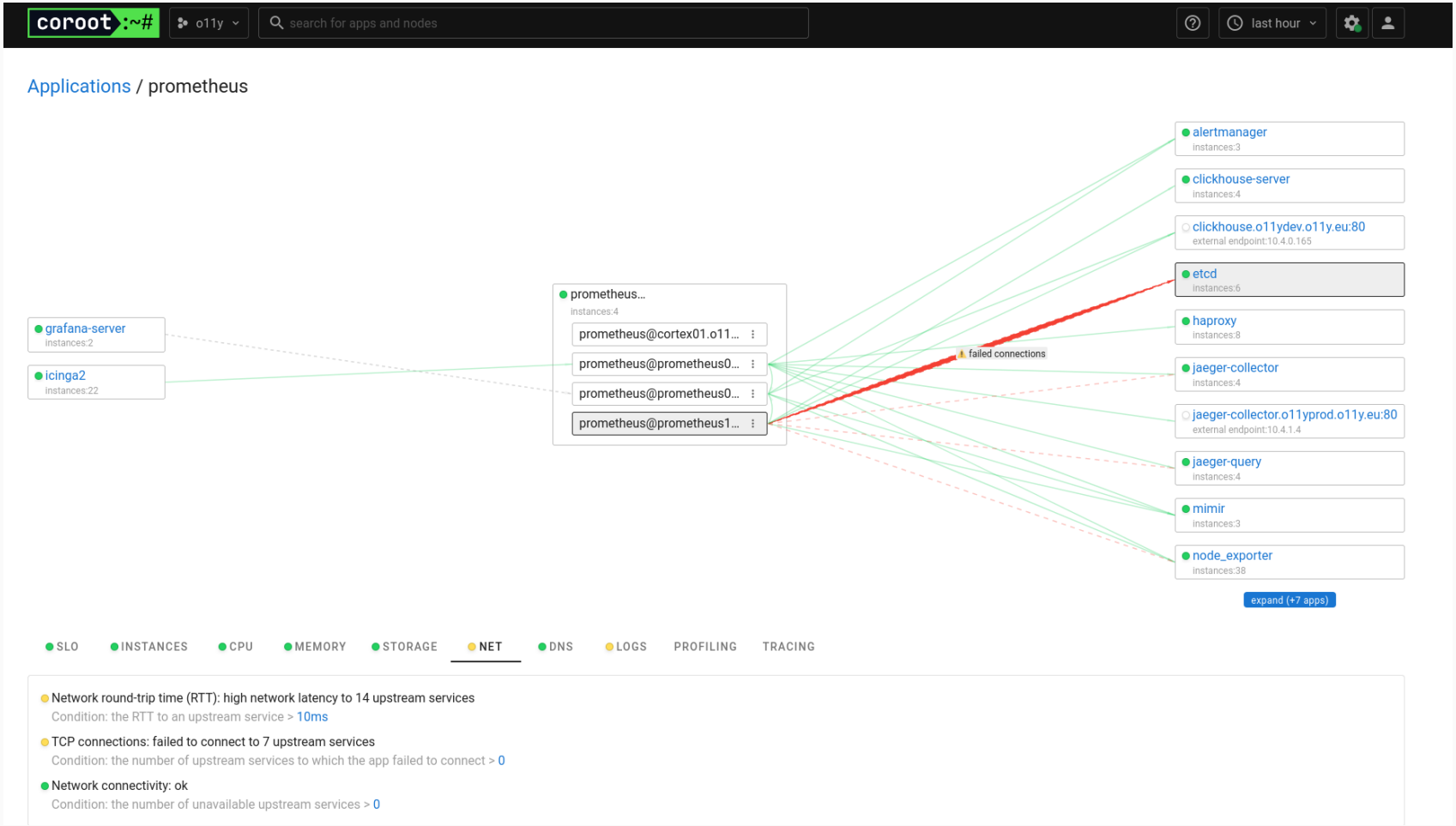
Service Map (App + Monitoring + Security)



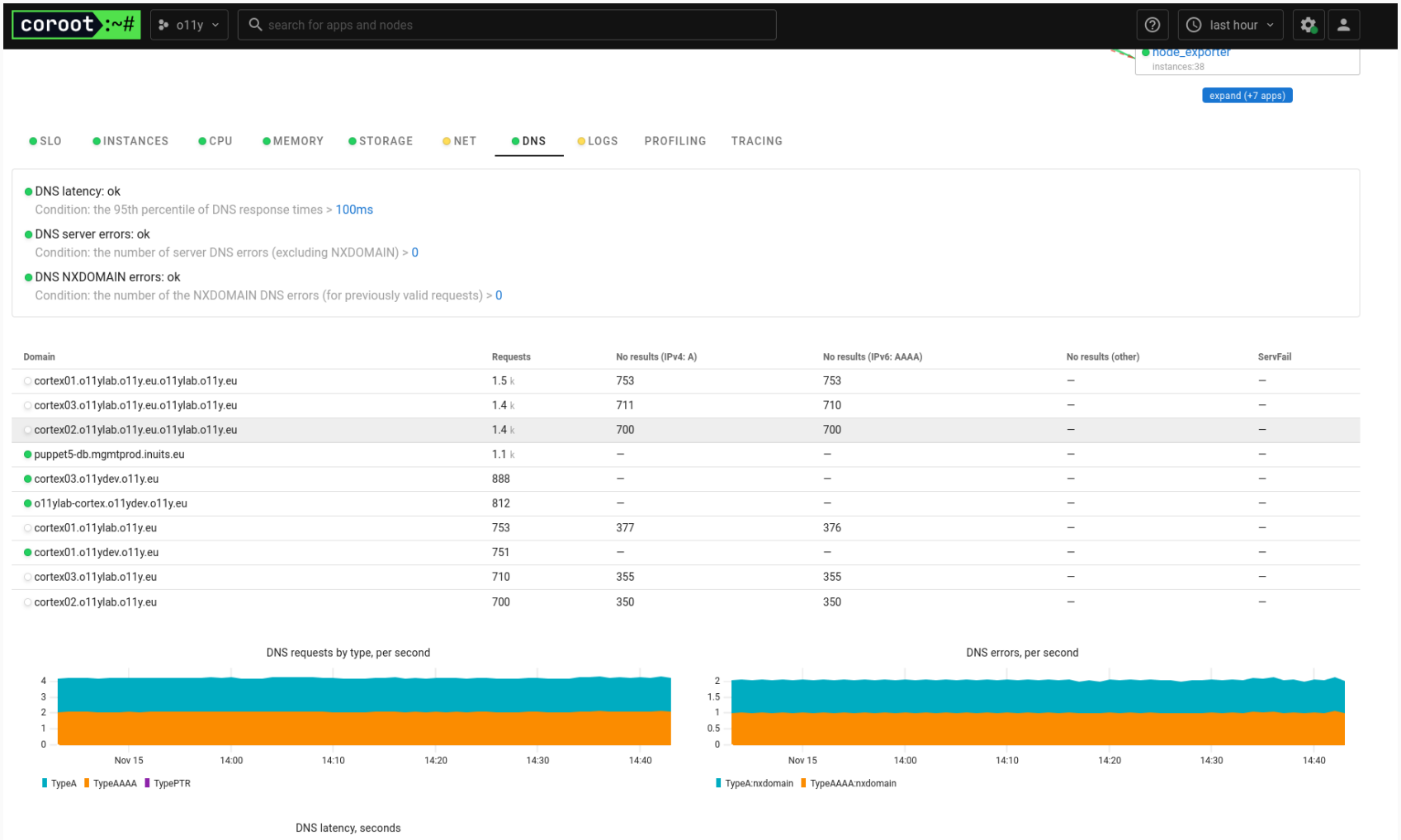
Filter and Define Categories



Service Map Etcd Error

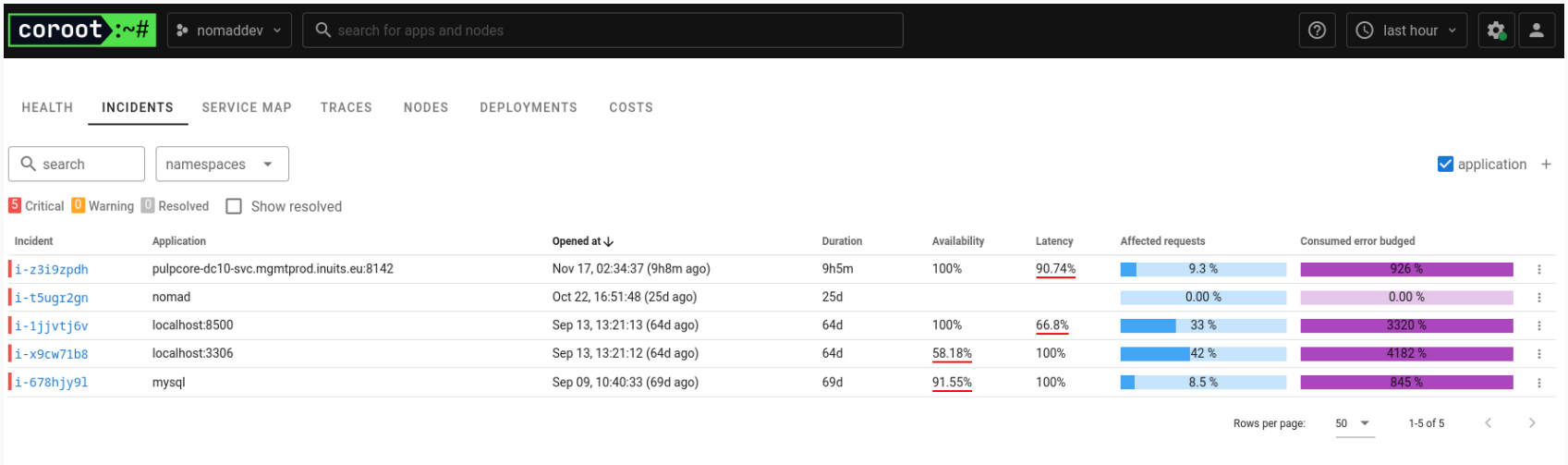


DNS


coroot :~#
o11y
search for apps and nodes
last hour
node_exporter
instances:38
expand (+7 apps)
SLO
INSTANCES
CPU
MEMORY
STORAGE
NET
DNS
LOGS
PROFILING
TRACING
DNS latency: ok
Condition: the 95th percentile of DNS response times > 100ms
DNS server errors: ok
Condition: the number of server DNS errors (excluding NXDOMAIN) > 0
DNS NXDOMAIN errors: ok
Condition: the number of the NXDOMAIN DNS errors (for previously valid requests) > 0
Domain
Requests
No results (IPv4: A)
No results (IPv6: AAAA)
No results (other)
ServFail
cortex01.o11ylab.o11y.eu.o11ylab.o11y.eu 1.5 k 753 753 – –
cortex03.o11ylab.o11y.eu.o11ylab.o11y.eu 1.4 k 711 710 – –
cortex02.o11ylab.o11y.eu.o11ylab.o11y.eu 1.4 k 700 700 – –
puppet5-db.mgmtprod.inuits.eu 1.1 k – – – –
cortex03.o11ydev.o11y.eu 888 – – – –
o11ylab-cortex.o11ydev.o11y.eu 812 – – – –
cortex01.o11ylab.o11y.eu 753 377 376 – –
cortex01.o11ydev.o11y.eu 751 – – – –
cortex03.o11ylab.o11y.eu 710 355 355 – –
cortex02.o11ylab.o11y.eu 700 350 350 – –
DNS requests by type, per second
4
3
2
1
0
Nov 15
14:00
14:10
14:20
14:30
14:40
TypeA
TypeAAAA
TypePTR
DNS errors, per second
2
1.5
1
0.5
0
Nov 15
14:00
14:10
14:20
14:30
14:40
TypeA:nxdomain
TypeAAAA:nxdomain
DNS latency, seconds

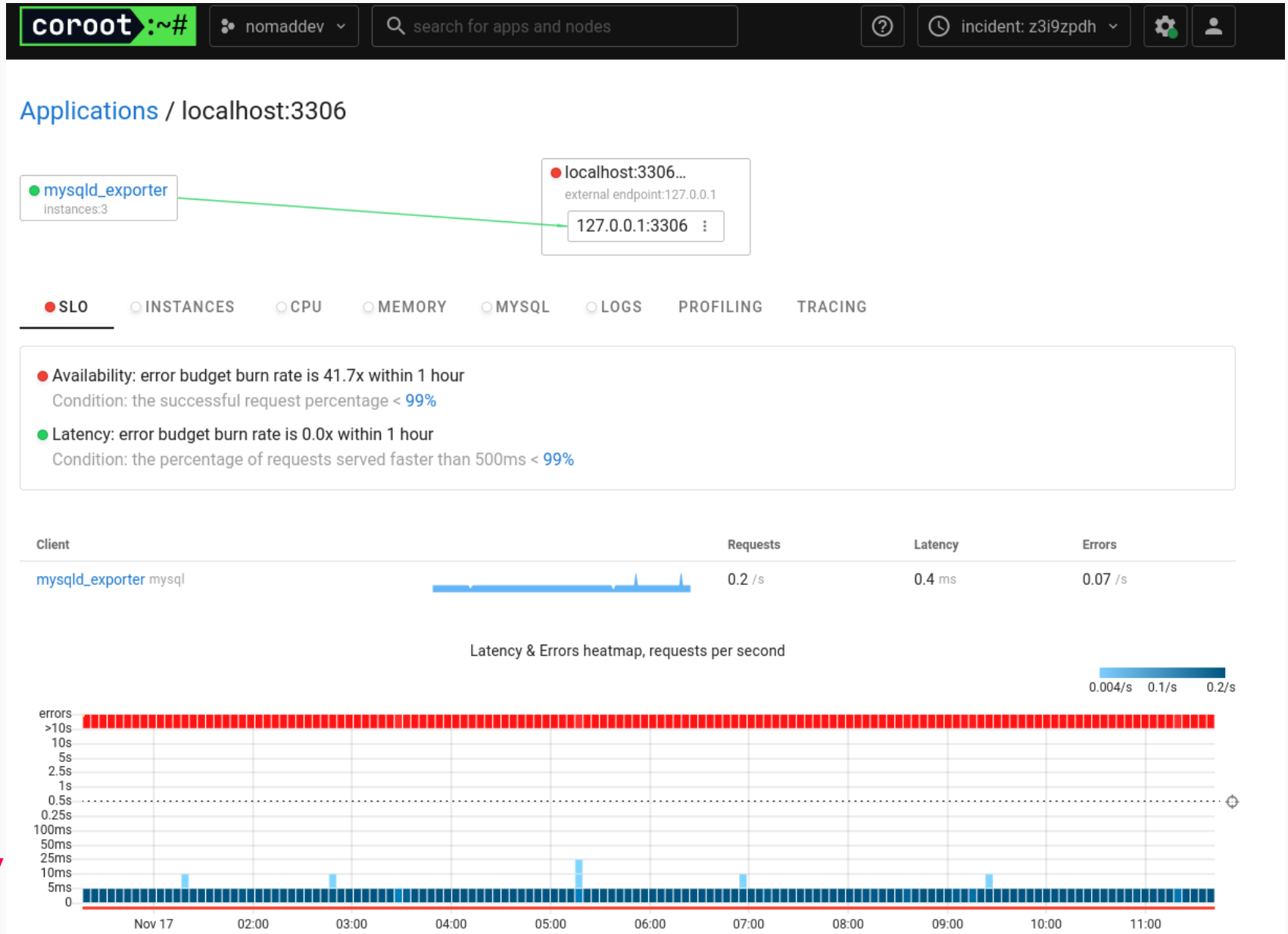
Incidents

- All in one space ..



- Incident timeframe.

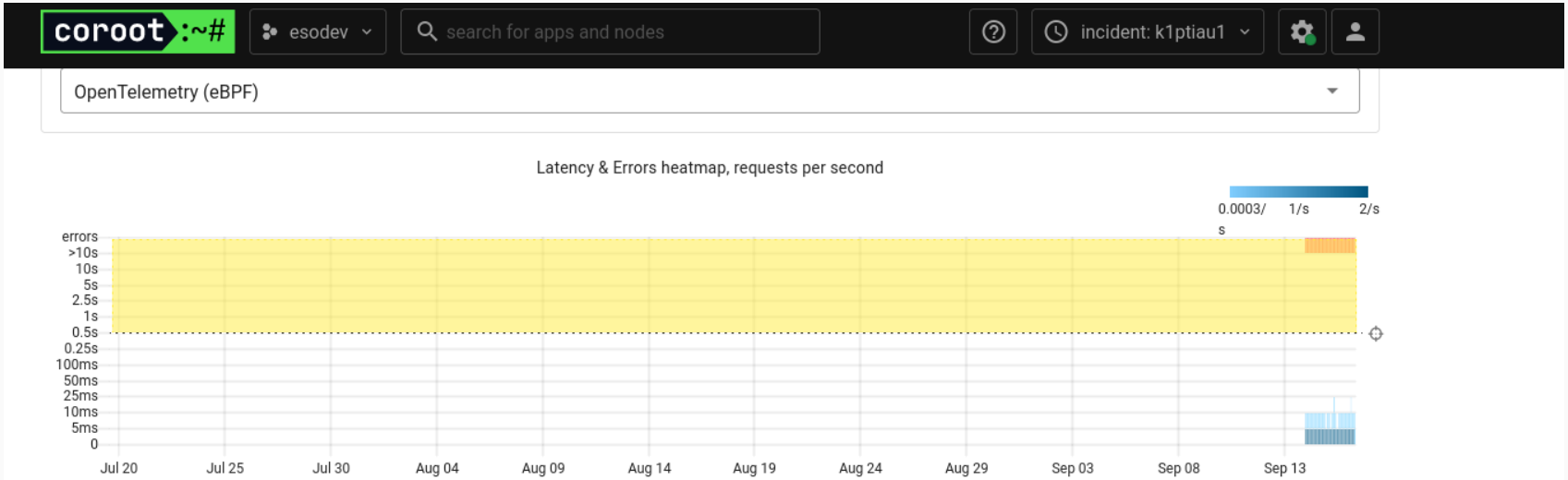
MySQL Incident



Tracing

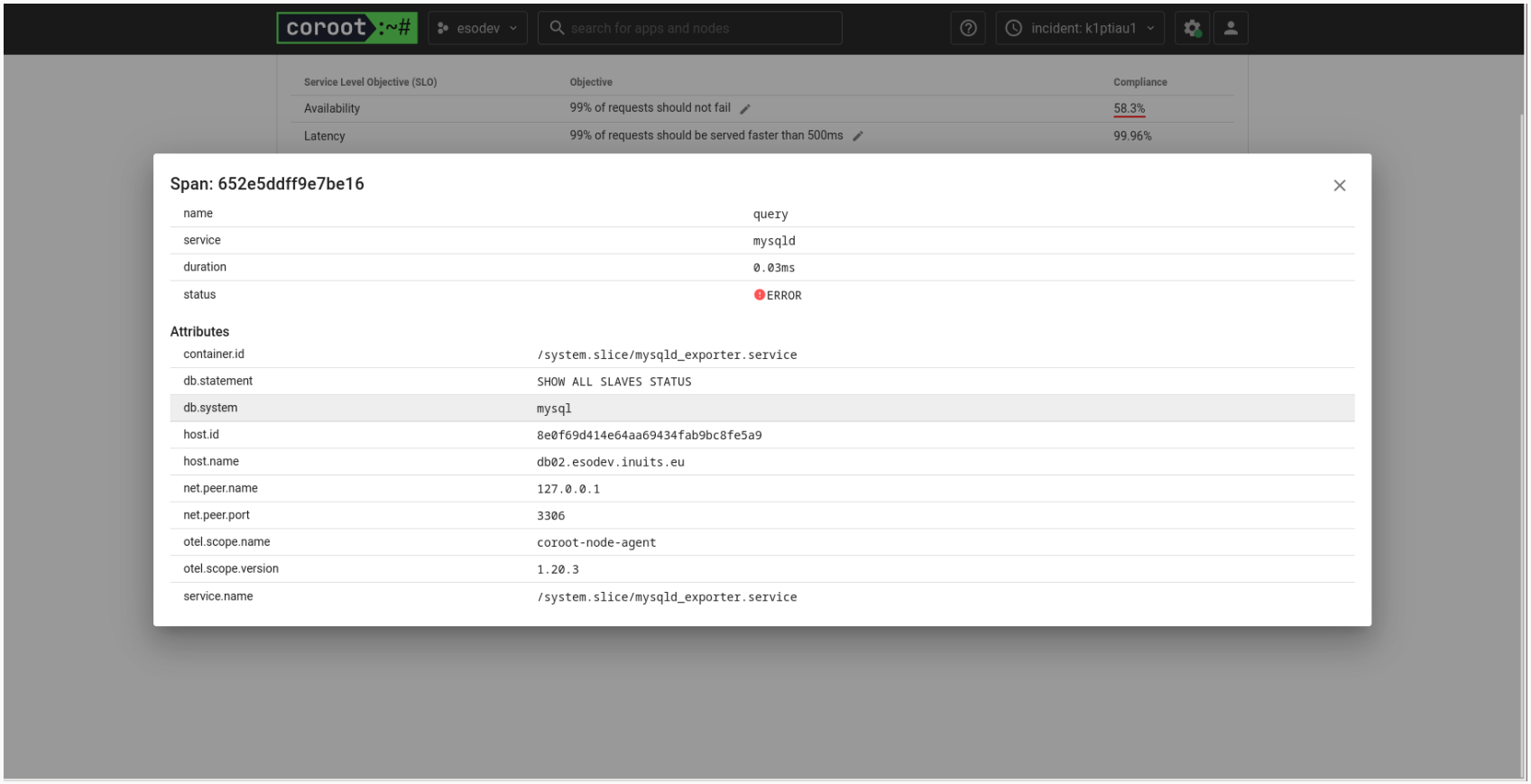
- ebpf
- otel endpoint

MySQL Traces

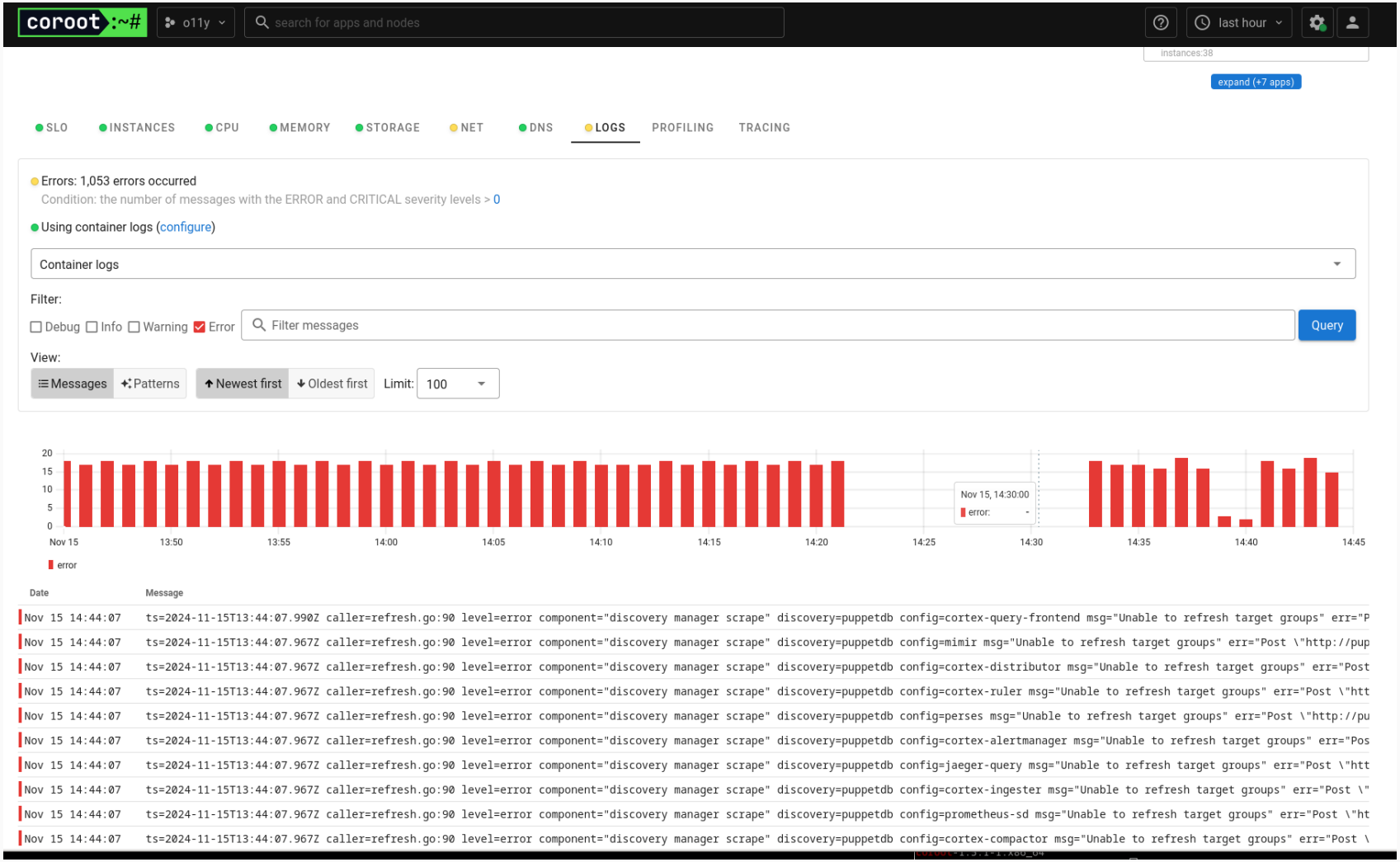


Trace ID	Client	Status	Duration	Name	Details
9fb4877e	mysqld_exporter	ERROR	0.0 ms	query	SHOW ALL SLAVES STATUS
af0e7c60	mysqld_exporter	ERROR	0.0 ms	query	SHOW ALL SLAVES STATUS NOLOCK
f7362ff1	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS NONBLOCKING
44ebec51	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS
b738acf8	mysqld_exporter	ERROR	0.0 ms	query	SELECT @@query_response_time_stats
4a3cdafc	mysqld_exporter	ERROR	0.0 ms	query	SHOW ALL SLAVES STATUS
c653dc19	mysqld_exporter	ERROR	0.0 ms	query	SHOW ALL SLAVES STATUS NOLOCK
9ad7216f	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS NONBLOCKING
6662d783	mysqld_exporter	ERROR	0.0 ms	query	SELECT @@query_response_time_stats
32d588c2	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS
60c83d66	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS
dc7b8743	mysqld_exporter	ERROR	0.0 ms	query	SHOW ALL SLAVES STATUS NOLOCK
bbe6a85e	mysqld_exporter	ERROR	0.1 ms	query	SHOW ALL SLAVES STATUS NONBLOCKING

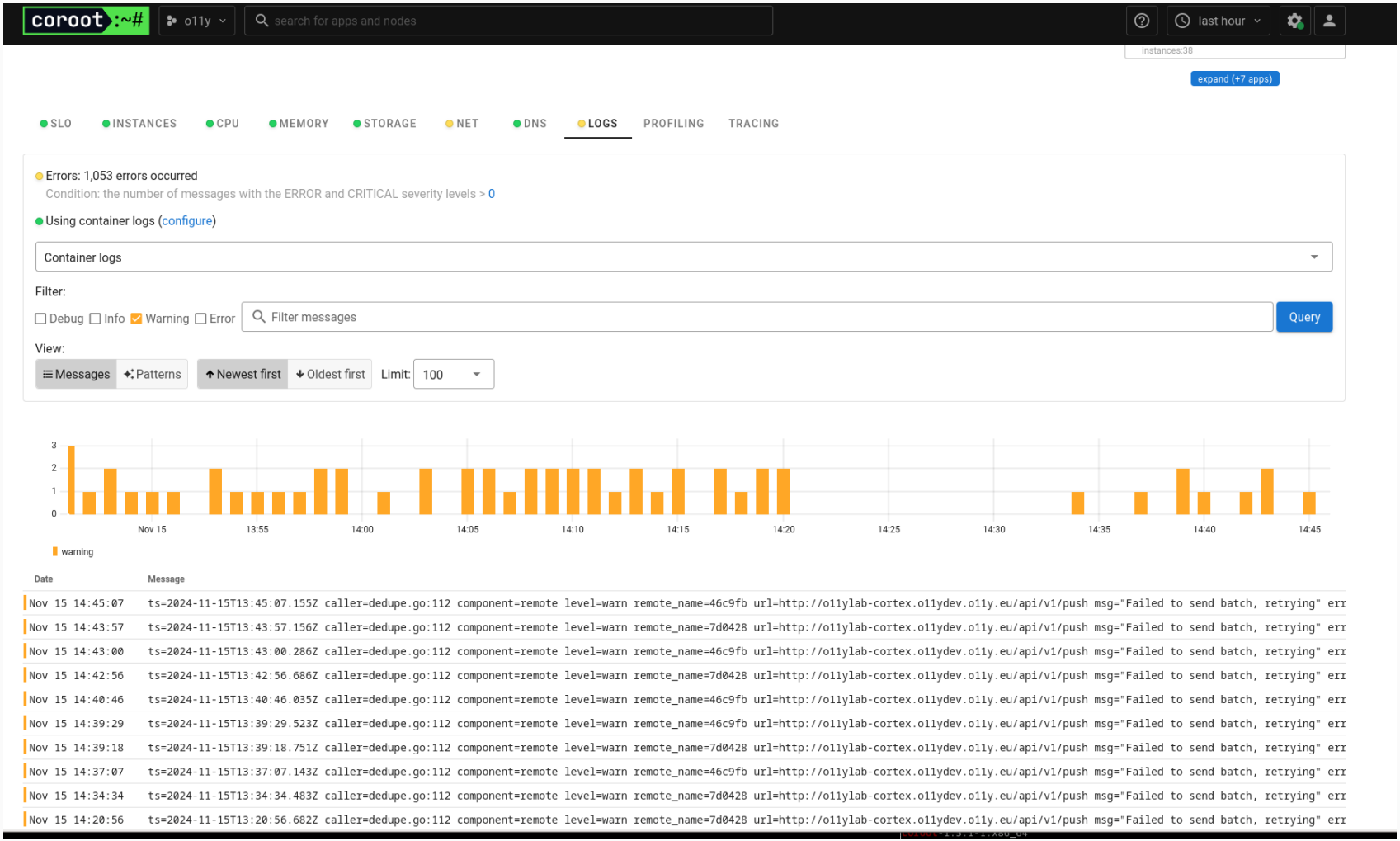
MySQL trace detail



Log Errors

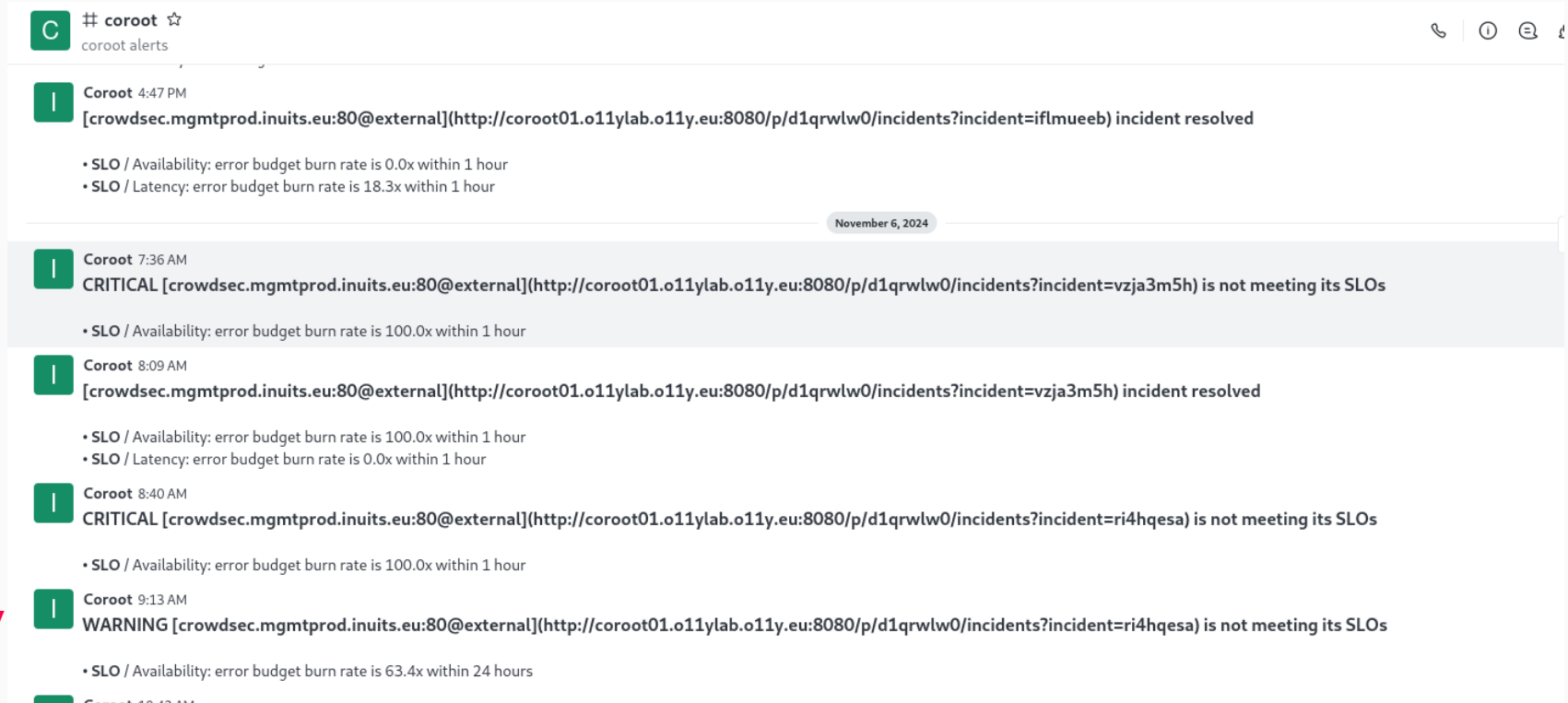

coroot :~#
o11y
search for apps and nodes
last hour
instances:38
expand (+7 apps)
SLO
INSTANCES
CPU
MEMORY
STORAGE
NET
DNS
LOGS
PROFILING
TRACING
Errors: 1,053 errors occurred
Condition: the number of messages with the ERROR and CRITICAL severity levels > 0
Using container logs (configure)
Container logs
Filter:
Debug
Info
Warning
Error
Filter messages
Query
View:
Messages
Patterns
Newest first
Oldest first
Limit: 100
20
15
10
5
0
Nov 15
13:50
13:55
14:00
14:05
14:10
14:15
14:20
14:25
14:30
14:35
14:40
14:45
Nov 15, 14:30:00
error: -
error
Date
Message
Nov 15 14:44:07 ts=2024-11-15T13:44:07.990Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-query-frontend msg="Unable to refresh target groups" err="P
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=mimir msg="Unable to refresh target groups" err="Post \"http://pup
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-distributor msg="Unable to refresh target groups" err="Post
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-ruler msg="Unable to refresh target groups" err="Post \"htt
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=perses msg="Unable to refresh target groups" err="Post \"http://pu
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-alertmanager msg="Unable to refresh target groups" err="Pos
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=jaeger-query msg="Unable to refresh target groups" err="Post \"htt
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-ingester msg="Unable to refresh target groups" err="Post \"
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=prometheus-sd msg="Unable to refresh target groups" err="Post \"ht
Nov 15 14:44:07 ts=2024-11-15T13:44:07.967Z caller=refresh.go:90 level=error component="discovery manager scrape" discovery=puppetdb config=cortex-compactor msg="Unable to refresh target groups" err="Post \

Log Warning


coroot :~#
o11y
search for apps and nodes
last hour
instances:38
expand (+7 apps)
SLO
INSTANCES
CPU
MEMORY
STORAGE
NET
DNS
LOGS
PROFILING
TRACING
Errors: 1,053 errors occurred
Condition: the number of messages with the ERROR and CRITICAL severity levels > 0
Using container logs (configure)
Container logs
Filter:
Debug
Info
Warning
Error
Filter messages
Query
View:
Messages
Patterns
Newest first
Oldest first
Limit:
100
3
2
1
0
Nov 15
13:55
14:00
14:05
14:10
14:15
14:20
14:25
14:30
14:35
14:40
14:45
warning
Date
Message
Nov 15 14:45:07 ts=2024-11-15T13:45:07.155Z caller=dedupe.go:112 component=remote level=warn remote_name=46c9fb url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:43:57 ts=2024-11-15T13:43:57.156Z caller=dedupe.go:112 component=remote level=warn remote_name=7d0428 url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:43:00 ts=2024-11-15T13:43:00.286Z caller=dedupe.go:112 component=remote level=warn remote_name=46c9fb url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:42:56 ts=2024-11-15T13:42:56.686Z caller=dedupe.go:112 component=remote level=warn remote_name=7d0428 url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:40:46 ts=2024-11-15T13:40:46.035Z caller=dedupe.go:112 component=remote level=warn remote_name=46c9fb url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:39:29 ts=2024-11-15T13:39:29.523Z caller=dedupe.go:112 component=remote level=warn remote_name=46c9fb url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:39:18 ts=2024-11-15T13:39:18.751Z caller=dedupe.go:112 component=remote level=warn remote_name=7d0428 url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:37:07 ts=2024-11-15T13:37:07.143Z caller=dedupe.go:112 component=remote level=warn remote_name=46c9fb url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:34:34 ts=2024-11-15T13:34:34.483Z caller=dedupe.go:112 component=remote level=warn remote_name=7d0428 url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err
Nov 15 14:20:56 ts=2024-11-15T13:20:56.682Z caller=dedupe.go:112 component=remote level=warn remote_name=7d0428 url=http://o11ylab-cortex.o11ydev.o11y.eu/api/v1/push msg="Failed to send batch, retrying" err

Alerting

- Per project configuration
- SLO Driven
- Configureable
- Alert integrations
  Slack,Teams,PagerDuty,OpsGenie,WebHooks (e.g RocketChat)

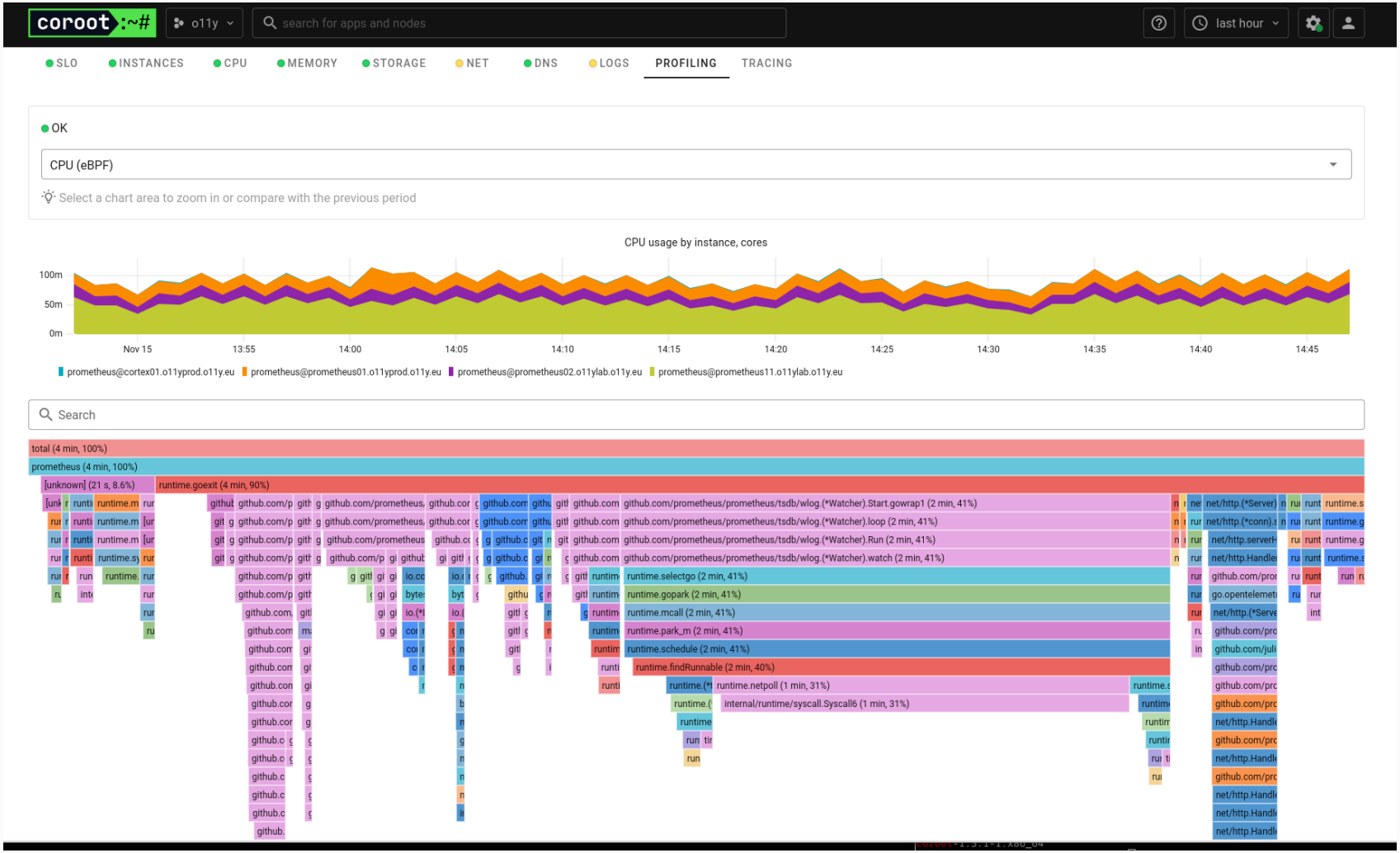


A word on SLO ..

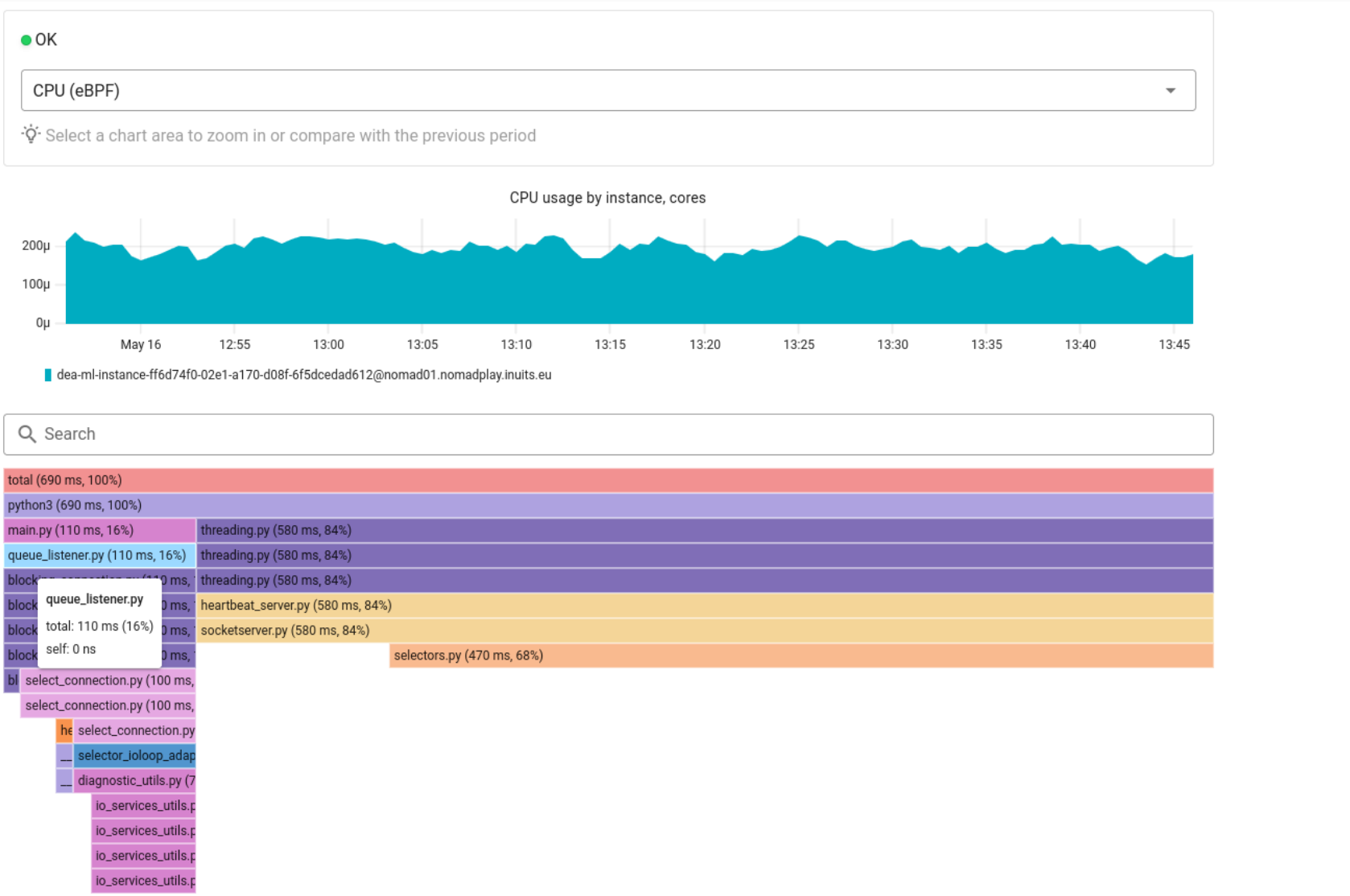
- 100% Fail vs vs 85% available
- Configurable
- Non intrusive alerts are helpful for debugging
- Don’t wake people up unless your business is critical
- What if you don’t meet them ?
- Are they actionable ?
- Most orgs don’t have the right culture
- They don’t have their teams empowered

Profiling

- Pyroscope based



Profiling


OK
CPU (eBPF)
Select a chart area to zoom in or compare with the previous period
CPU usage by instance, cores
200µ
100µ
0µ
May 16
12:55
13:00
13:05
13:10
13:15
13:20
13:25
13:30
13:35
13:40
13:45
dea-ml-instance-ff6d74f0-02e1-a170-d08f-6f5dcedad612@nomad01.nomadplay.inuits.eu
Search
total (690 ms, 100%)
python3 (690 ms, 100%)
main.py (110 ms, 16%)
threading.py (580 ms, 84%)
queue_listener.py (110 ms, 16%)
threading.py (580 ms, 84%)
threading.py (580 ms, 84%)
heartbeat_server.py (580 ms, 84%)
socketserver.py (580 ms, 84%)
selectors.py (470 ms, 68%)
queue_listener.py
total: 110 ms (16%)
self: 0 ns
select_connection.py (100 ms,
select_connection.py (100 ms,
select_connection.py
selector_ioloop_adap
diagnostic_utils.py (7
io_services_utils.p
io_services_utils.p
io_services_utils.p
io_services_utils.p

There is more ..

- Cost calculations
- Deployments
- Otel gateway
- Root Cause Analysis

My personal Use cases today

- Debug Tool
- Informing me where to look
- Fully enabled in dev environments and some prod
- Feature flagged and enabled on demand in others
- Future : enabled everywhere

#o11ylove

I always loved monitoring, done right,

But coroot gave me #o11ylove

Kris Buytaert

@krisbuytaert

kris@o11y.eu

Essensteenweg 31

2930 Brasschaat

Belgium

Contact: info@o11y.eu