KubeCon | CloudNativeCon

Europe 2023

KubeCon | CloudNativeCon

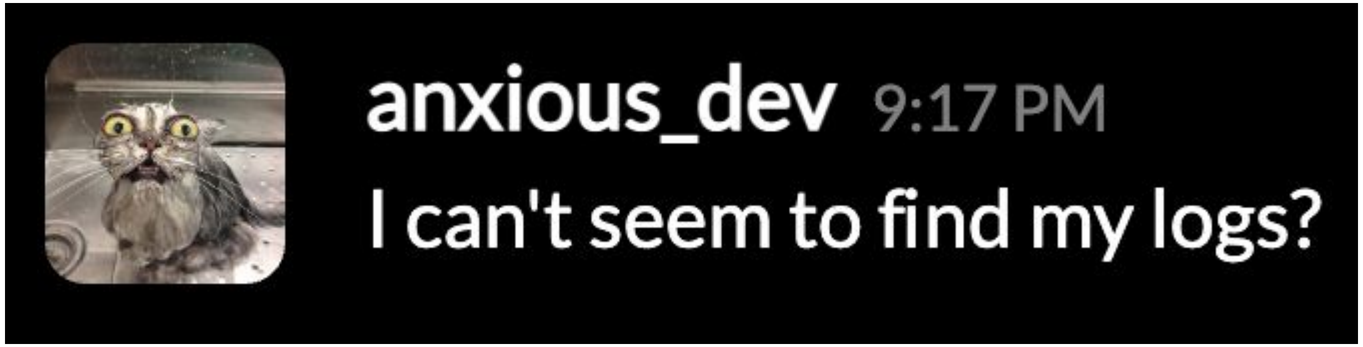
Europe 2023

Managing Cardinality and Performance for Your Logging Stack

Derek Cavanaugh, Sara Moore

RECURSION pharmaceuticals

The Crime Scene

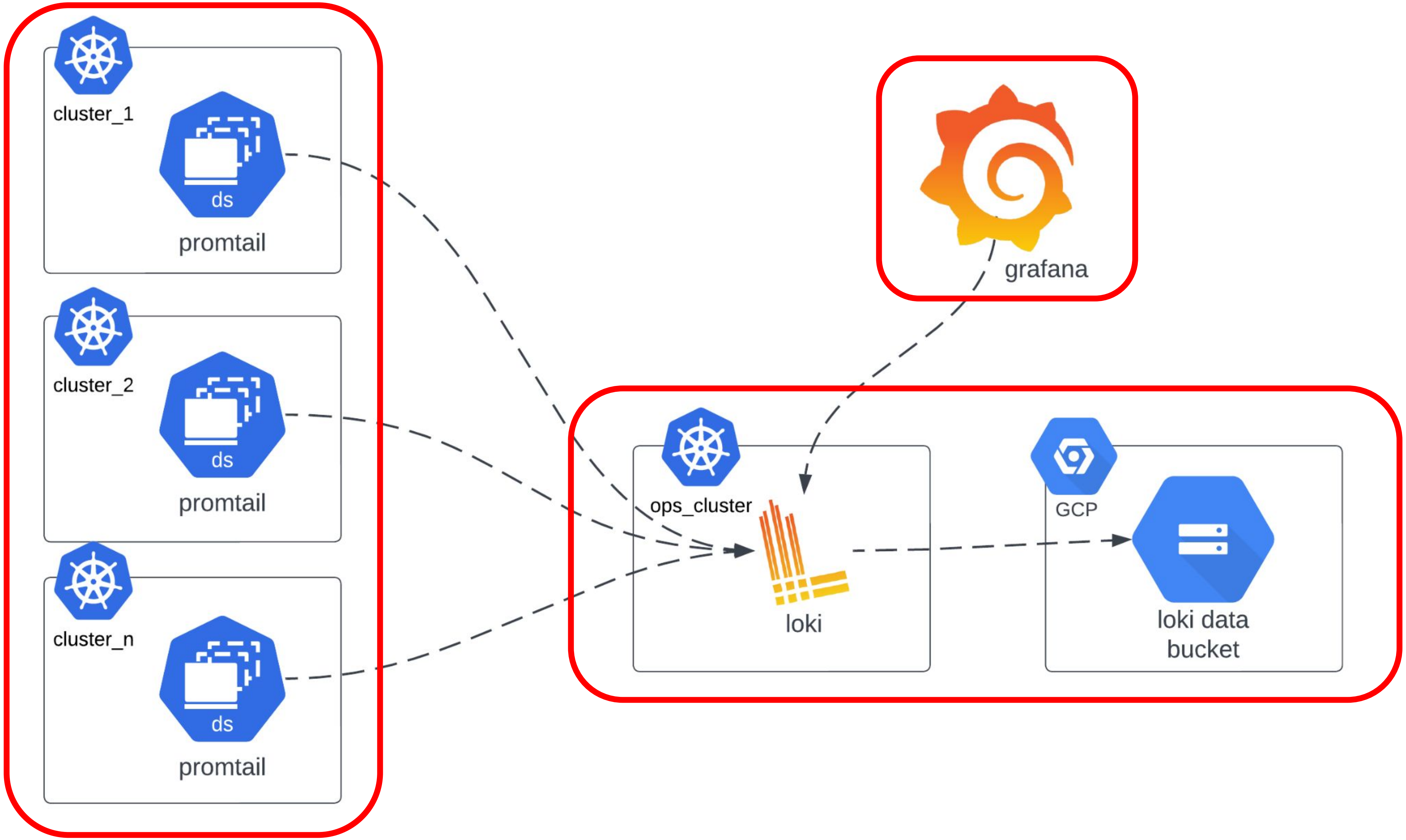


anxious_dev 9:17 PM

I can't seem to find my logs?

The case of missing logs… 🔎

PLG Architecture



The Case of the Missing Logs

"Maximum active stream limit exceeded, reduce the number of active streams (reduce labels or reduce label values), or contact your Loki administrator to see if the limit can be increased"

The Case of the Missing Logs

"**Maximum active stream limit exceeded,** reduce the number of active streams (reduce labels or reduce label values), or contact your Loki administrator to see if the limit can be increased"

Let's raise the limit.

PLG Basics

Indexes

Cardinality

Active Streams

Chunks

PLG Basics

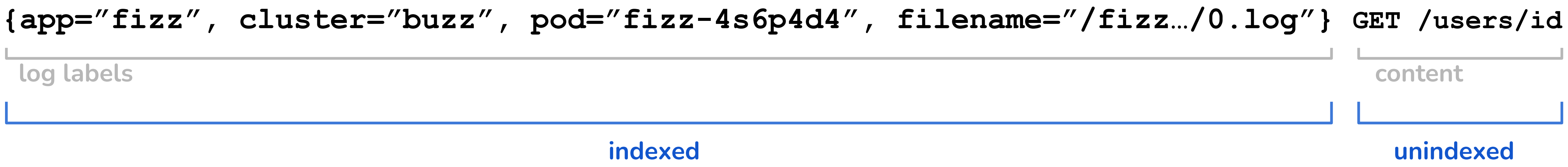
Indexes

Cardinality

Active Streams

Chunks

Indexes



```
{app="fizz", cluster="buzz", pod="fizz-4s6p4d4", filename="/fizz…/0.log"} GET /users/id
```

PLG Basics

Indexes - created from log labels

Cardinality

Active Streams

Chunks

PLG Basics

Indexes - created from log labels

Cardinality

Active Streams

Chunks

Cardinality

```
{app=”foo”, pod=”foo-a”}...
{app=”foo”, pod=”foo-b”}...
{app=”foo”, pod=”foo-c”}...
{app=”foo”, pod=”foo-d”}...
{app=”foo”, pod=”foo-e”}...

{app=”bar”, pod=”bar-a”}...
{app=”bar”, pod=”bar-b”}...
```

PLG Basics

Indexes - created from log labels

Cardinality - measured by uniqueness of labels

Active Streams

Chunks

PLG Basics

Indexes - created from log labels

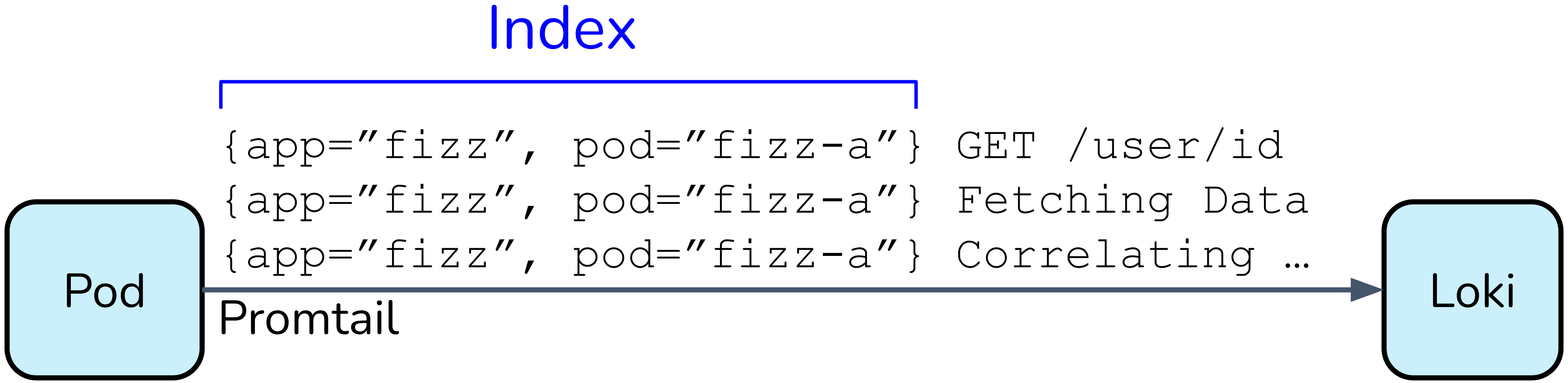
Cardinality - measured by uniqueness of labels

Active Streams

Chunks

Active Streams

Log lines being received with the same index (matching label set)



Index

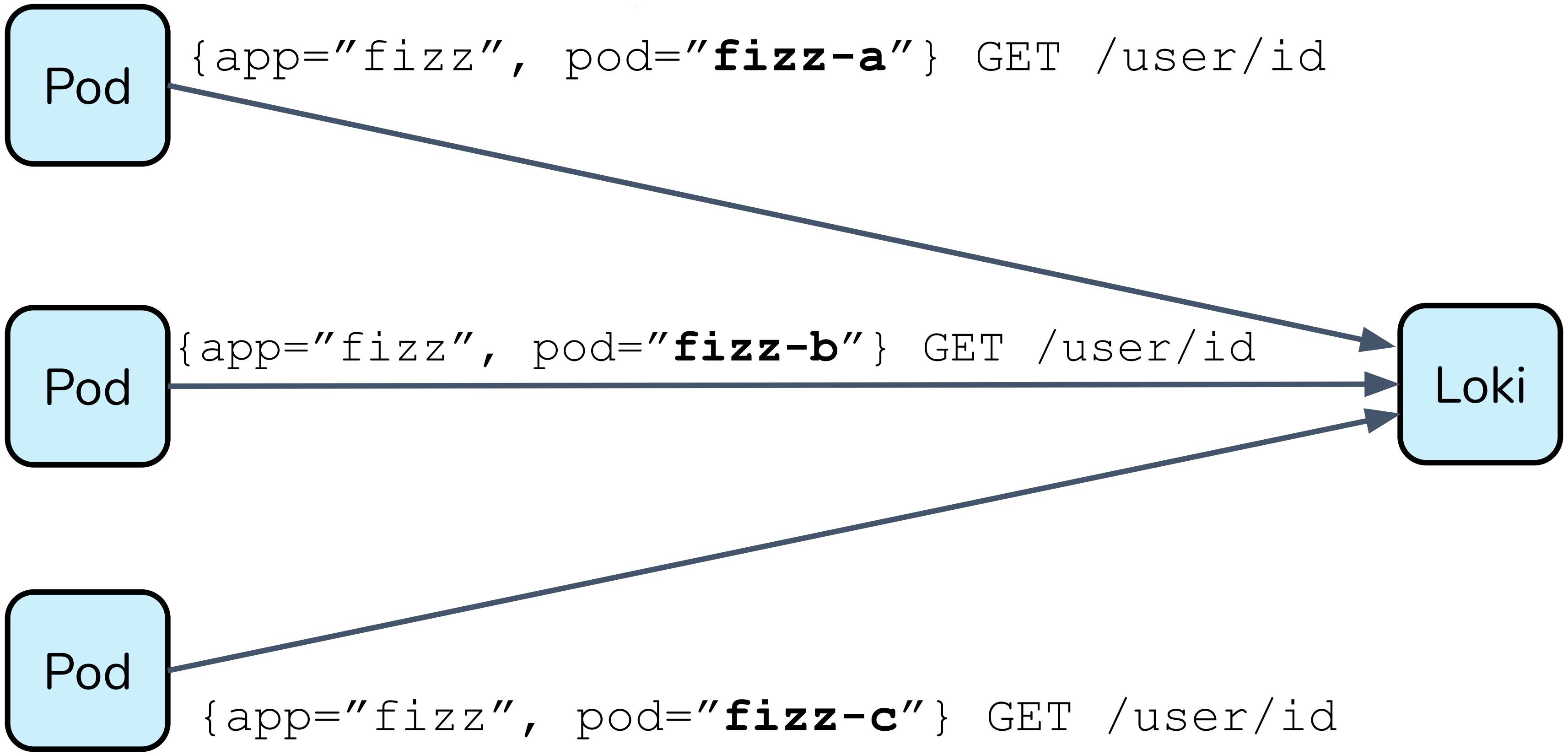
```
{app="fizz", pod="fizz-a"} GET /user/id
{app="fizz", pod="fizz-a"} Fetching Data
{app="fizz", pod="fizz-a"} Correlating …
```

Pod

Promtail

Loki

Active Streams


Pod
{app="fizz", pod="**fizz-a**"} GET /user/id
Pod
{app="fizz", pod="**fizz-b**"} GET /user/id
Loki
Pod
{app="fizz", pod="**fizz-c**"} GET /user/id

PLG Basics

Indexes - created from log labels

Cardinality - measured by uniqueness of labels

Active Streams - logs with the same index actively shipping to Loki

Chunks

PLG Basics

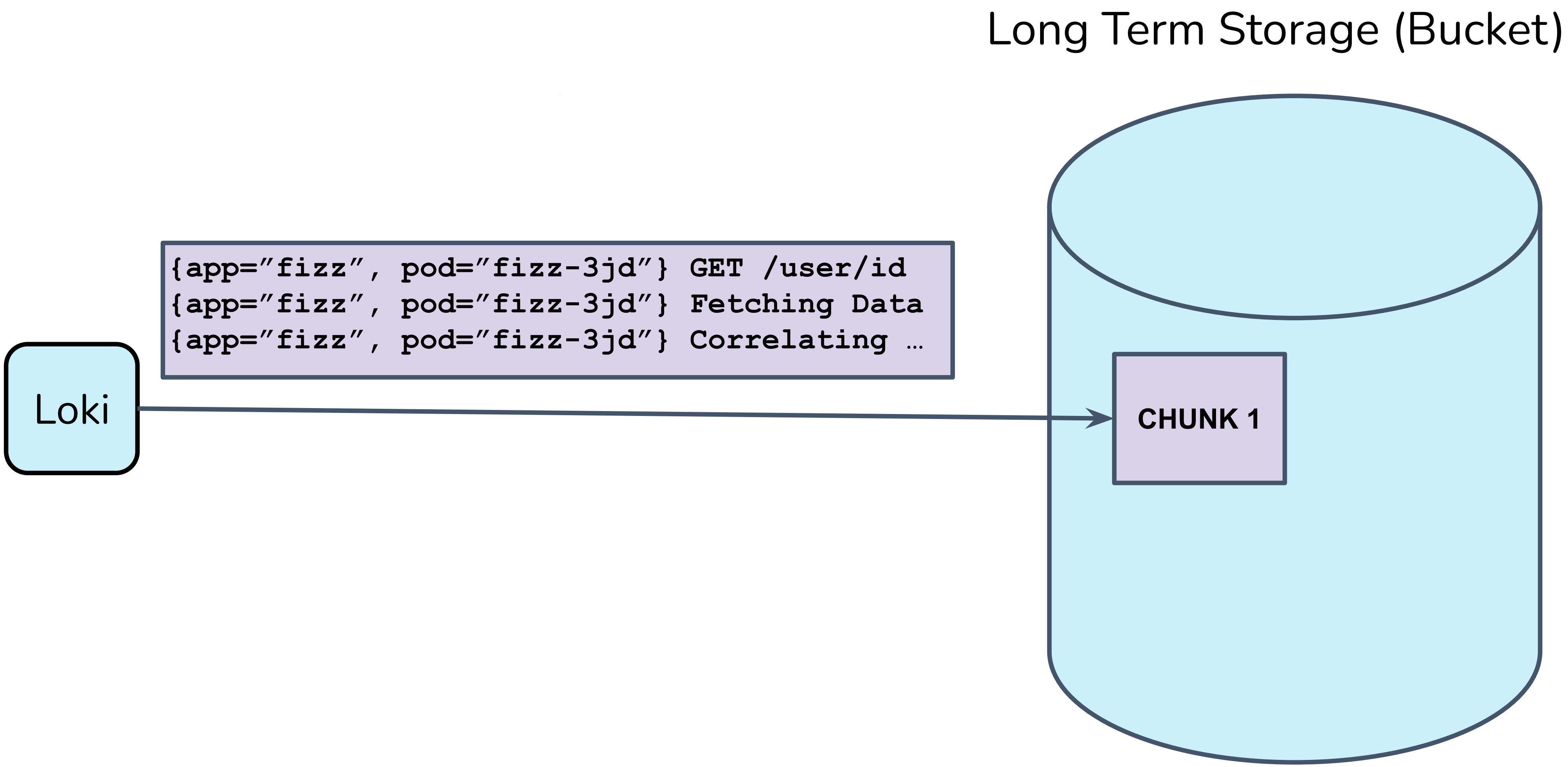
Indexes - created from log labels

Cardinality - measured by uniqueness of labels

Active Streams - logs with the same index actively shipping to Loki

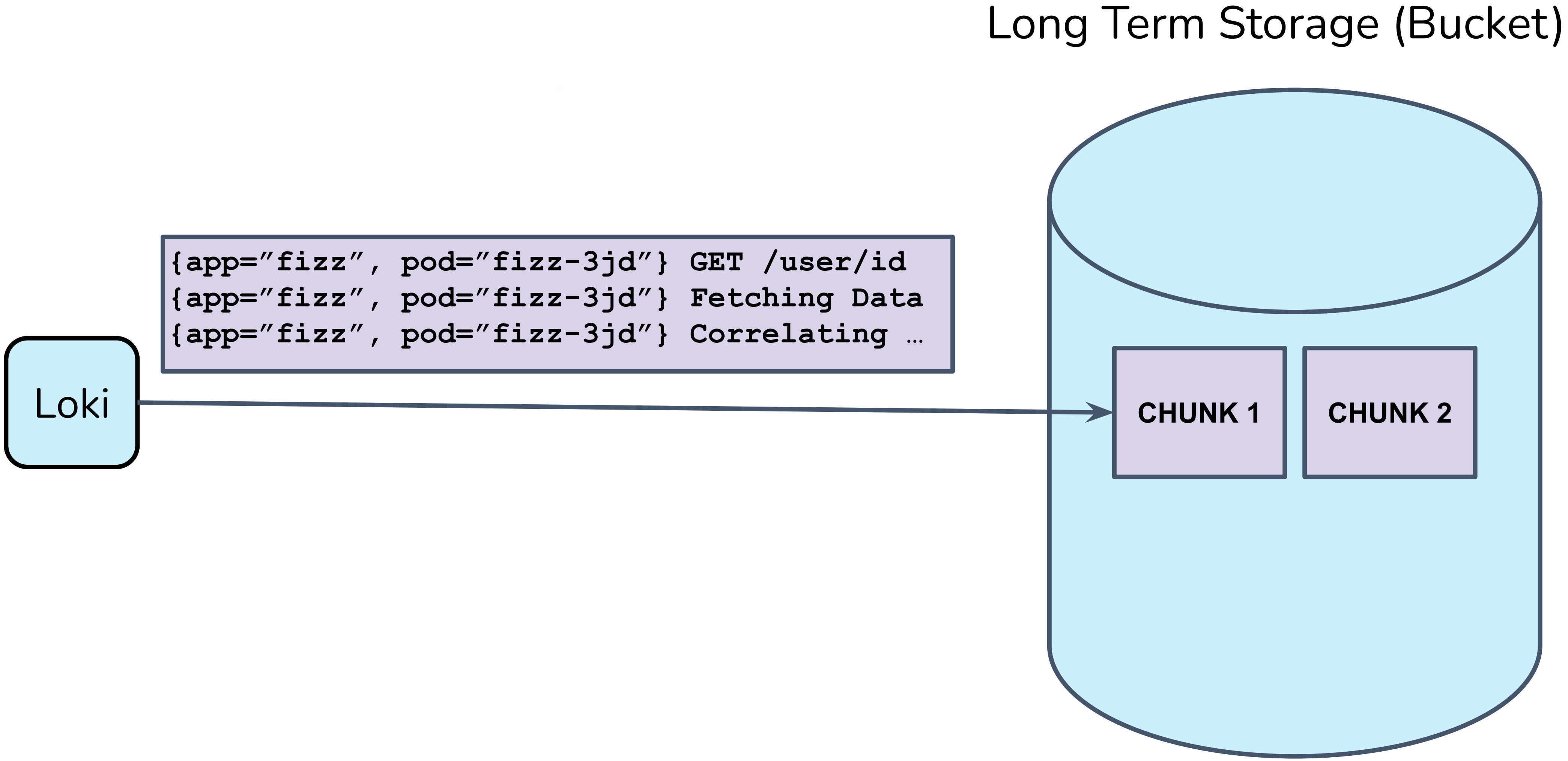
Chunks

Chunks



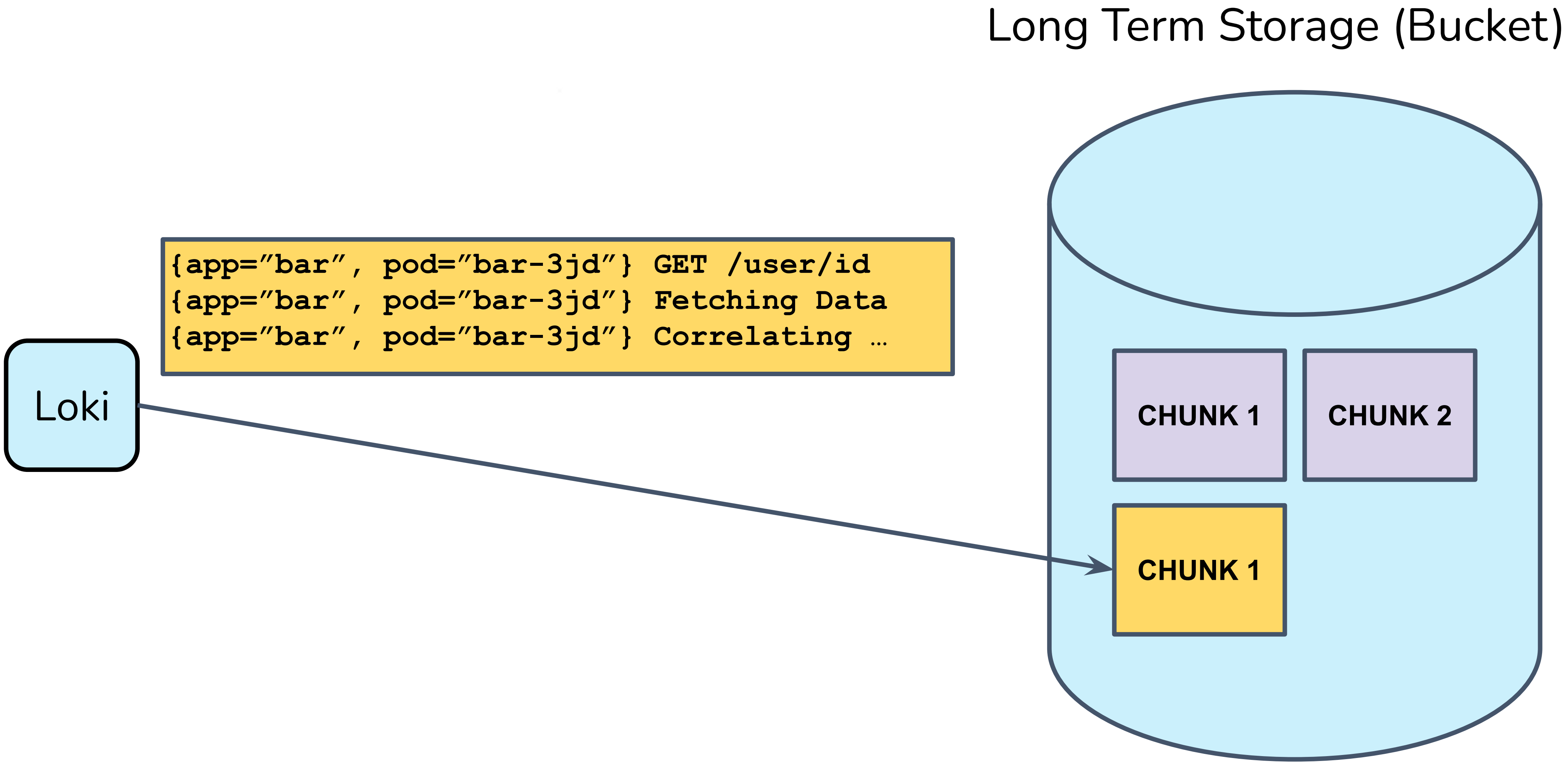
```
{app=”fizz”, pod=”fizz-3jd”} GET /user/id
{app=”fizz”, pod=”fizz-3jd”} Fetching Data
{app=”fizz”, pod=”fizz-3jd”} Correlating …
```

Chunks



```
{app="fizz", pod="fizz-3jd"} GET /user/id
{app="fizz", pod="fizz-3jd"} Fetching Data
{app="fizz", pod="fizz-3jd"} Correlating …
```

Chunks



```
{app="bar", pod="bar-3jd"} GET /user/id
{app="bar", pod="bar-3jd"} Fetching Data
{app="bar", pod="bar-3jd"} Correlating …
```

PLG Basics

Indexes - created from log labels

Cardinality - measured by uniqueness of labels

Active Streams - logs with the same index actively shipping to Loki

Chunks - blocks of log data with matching indexes

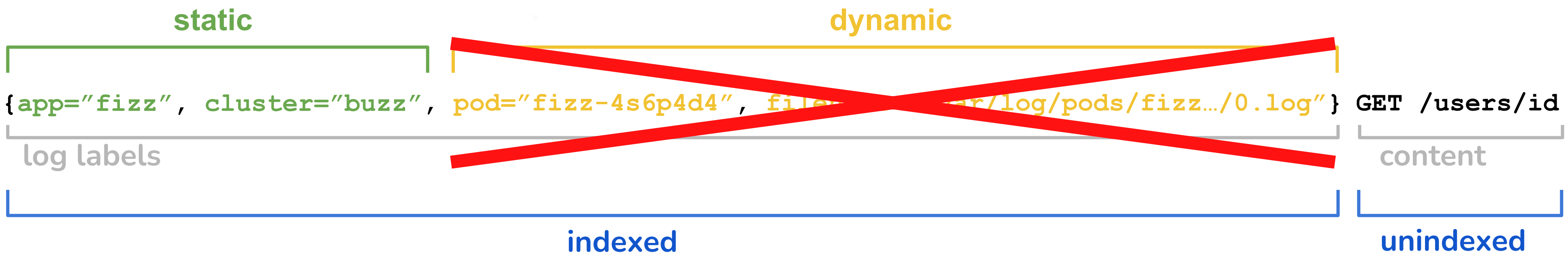
The Case of the Missing Logs

`“Maximum active stream limit exceeded,` **`reduce the number of active streams (reduce labels or reduce label values)`**`, or contact your Loki administrator to see if the limit can be increased”`

```
{app=”fizz”, pod=”fizz-3jd”} GET /user/id
```

Our log labels have high cardinality

Config Changes



```
{app="fizz", cluster="buzz", pod="fizz-4s6p4d4", filename="/var/log/pods/fizz…/0.log"} GET /users/id
```

Config Changes

Promtail Pipelines - Transform logs before shipping to Loki

Stage Types

- **Parsing** - parse and extract data from the current log line
- **Transform** - transform extracted data
- **Action** - modify extracted data
- **Filtering** - run custom stages or drop log entries based on a specified filter

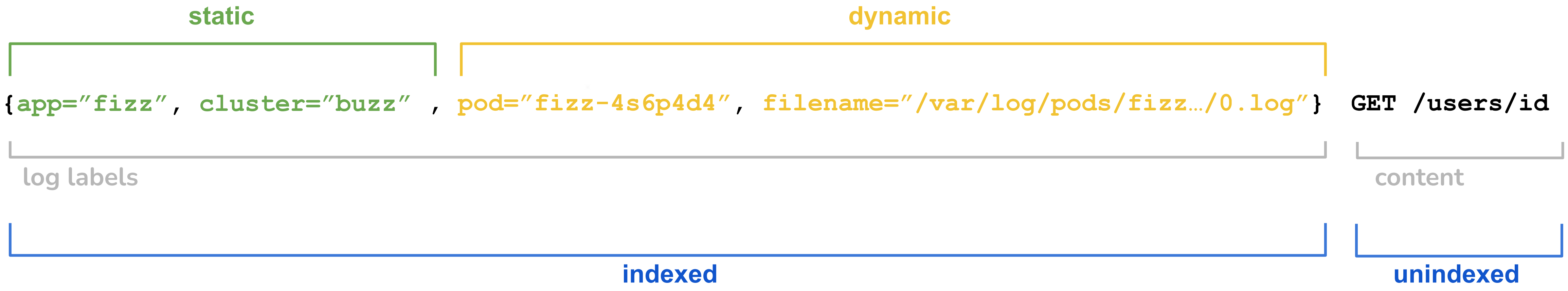
`labeldrop` **- Action** type that drops labels from the label set before sending the log to Loki

Let’s write some config!

Config Changes

```
scrape_configs:
  - job_name: kubernetes-pods
    kubernetes_sd_configs:
      - role: pod
    pipeline_stages:
      - cri: {}
      - labeldrop:
        - filename
        - pod
```

Config Changes


static

dynamic

{app=″fizz″, cluster=″buzz″ , pod=″fizz-4s6p4d4″, filename=″/var/log/pods/fizz…/0.log″} GET /users/id

log labels

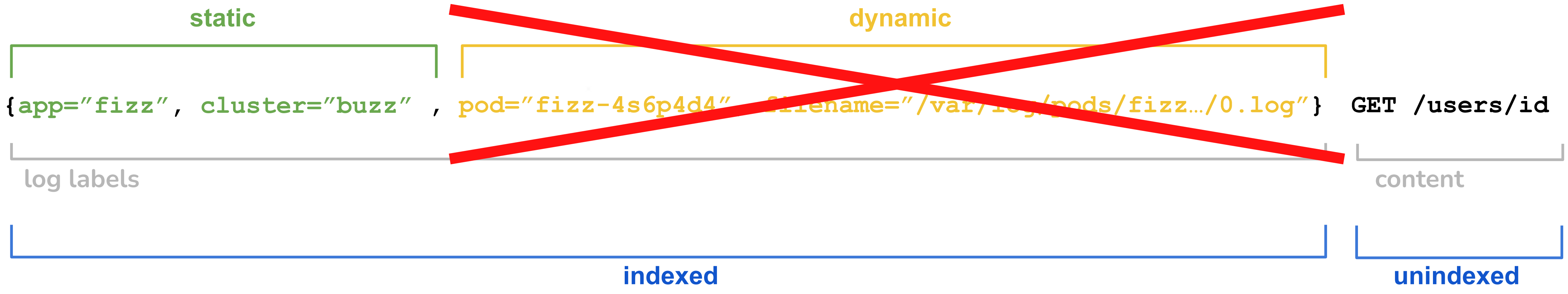
content

indexed

unindexed

```
scrape_configs:
  - job_name: kubernetes-pods
    pipeline_stages:
      - cri: {}
      - labeldrop:
        - filename
        - pod
```

Config Changes



static

dynamic

{app="fizz", cluster="buzz" , ~~pod="fizz-4s6p4d4", filename="/var/log/pods/fizz…/0.log"~~} GET /users/id

log labels

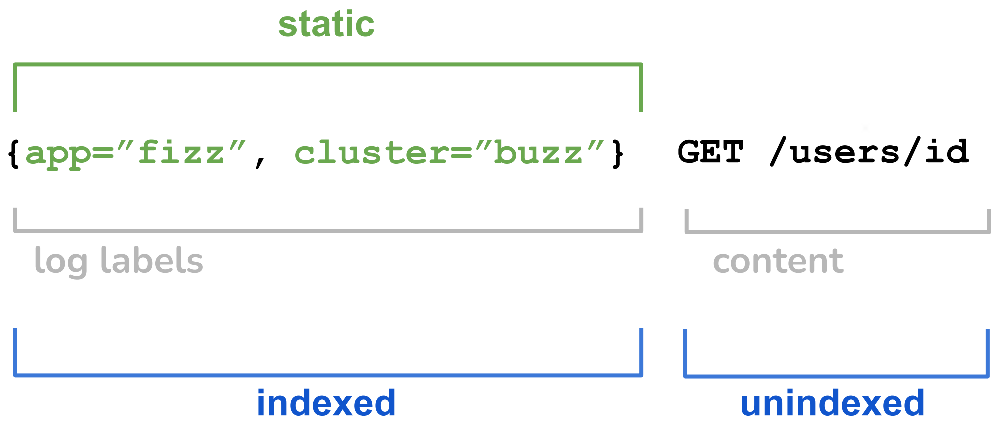
content

indexed

unindexed

```
scrape_configs:
  - job_name: kubernetes-pods
    pipeline_stages:
      - cri: {}
      - labeldrop:
        - filename
        - pod
```

Config Changes



static

{app="fizz", cluster="buzz"} GET /users/id

log labels

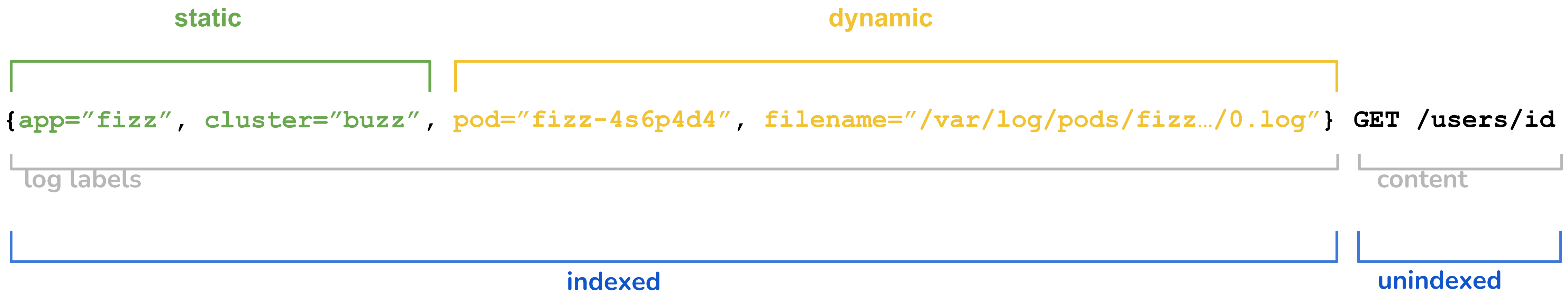
content

indexed

unindexed

```
scrape_configs:
  - job_name: kubernetes-pods
    pipeline_stages:
      - cri: {}
      - labeldrop:
        - filename
        - pod
```

Config Changes



static

dynamic

```
{app=”fizz”, cluster=”buzz”, pod=”fizz-4s6p4d4”, filename=”/var/log/pods/fizz…/0.log”} GET /users/id
```

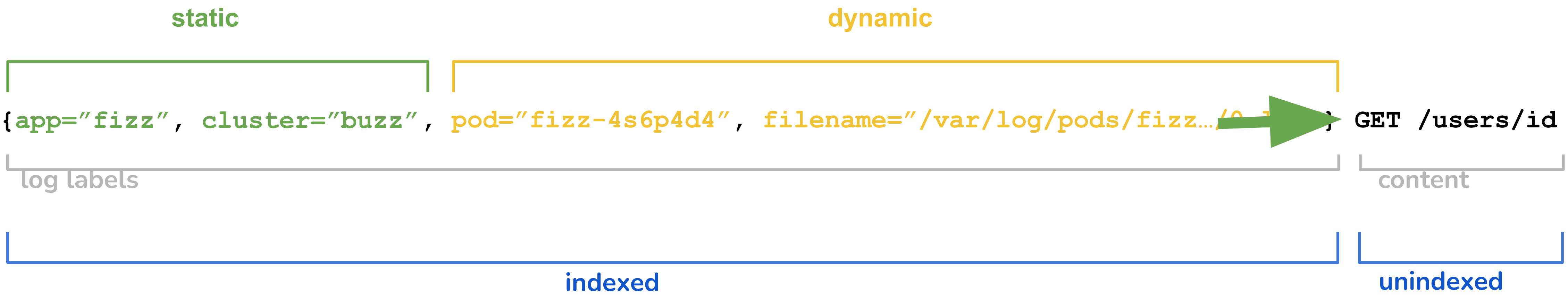
log labels

content

indexed

unindexed

Config Changes



static

dynamic

{app=”fizz”, cluster=”buzz”, pod=”fizz-4s6p4d4”, filename=”/var/log/pods/fizz…/0.l [illegible]} GET /users/id

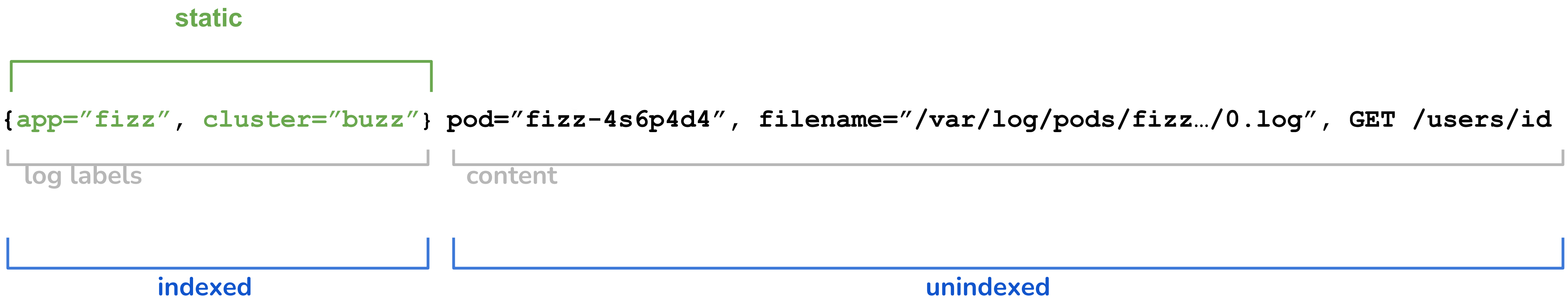
log labels

content

indexed

unindexed

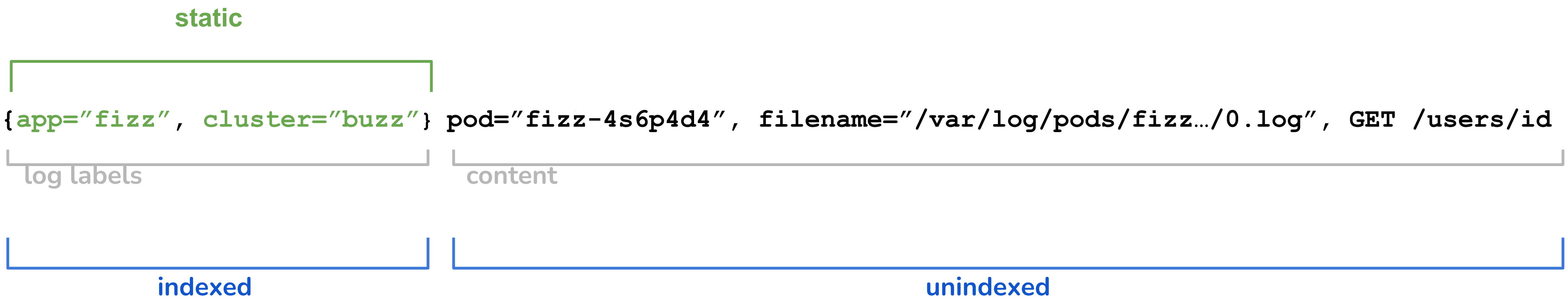
Config Changes



static

```
{app="fizz", cluster="buzz"} pod="fizz-4s6p4d4", filename="/var/log/pods/fizz…/0.log", GET /users/id
```

Config Changes



static

```
{app="fizz", cluster="buzz"} pod="fizz-4s6p4d4", filename="/var/log/pods/fizz…/0.log", GET /users/id
```

log labels

content

indexed

unindexed

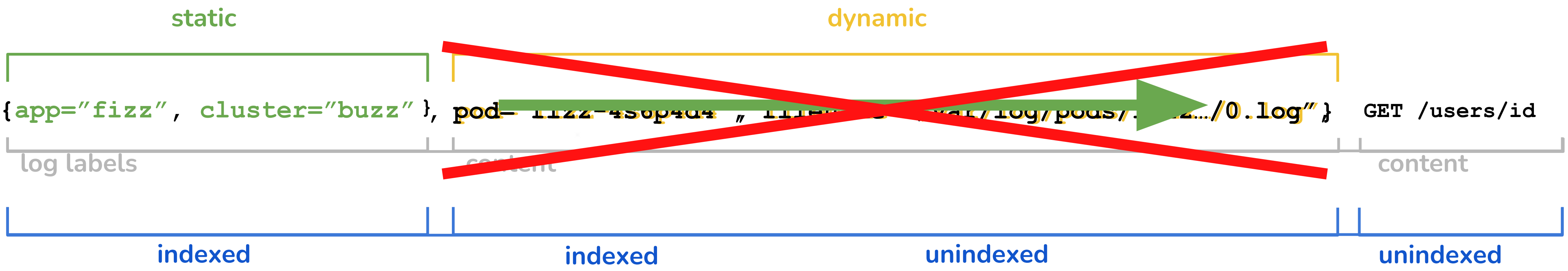
`replace` - **Parser** type that parses a log line using a regular expression and replaces the log line

Back to the config!

Config Changes

```
scrape_configs:
  - job_name: kubernetes-pods
    kubernetes_sd_configs:
      - role: pod
    pipeline_stages:
      - cri: {}
      - replace:
          expression: "(.*)"
          replace: "pod=\"{{ .pod }}\" filename=\"{{ .filename }}\" {{ .Value }}"
      - labeldrop:
        - filename
        - pod
```

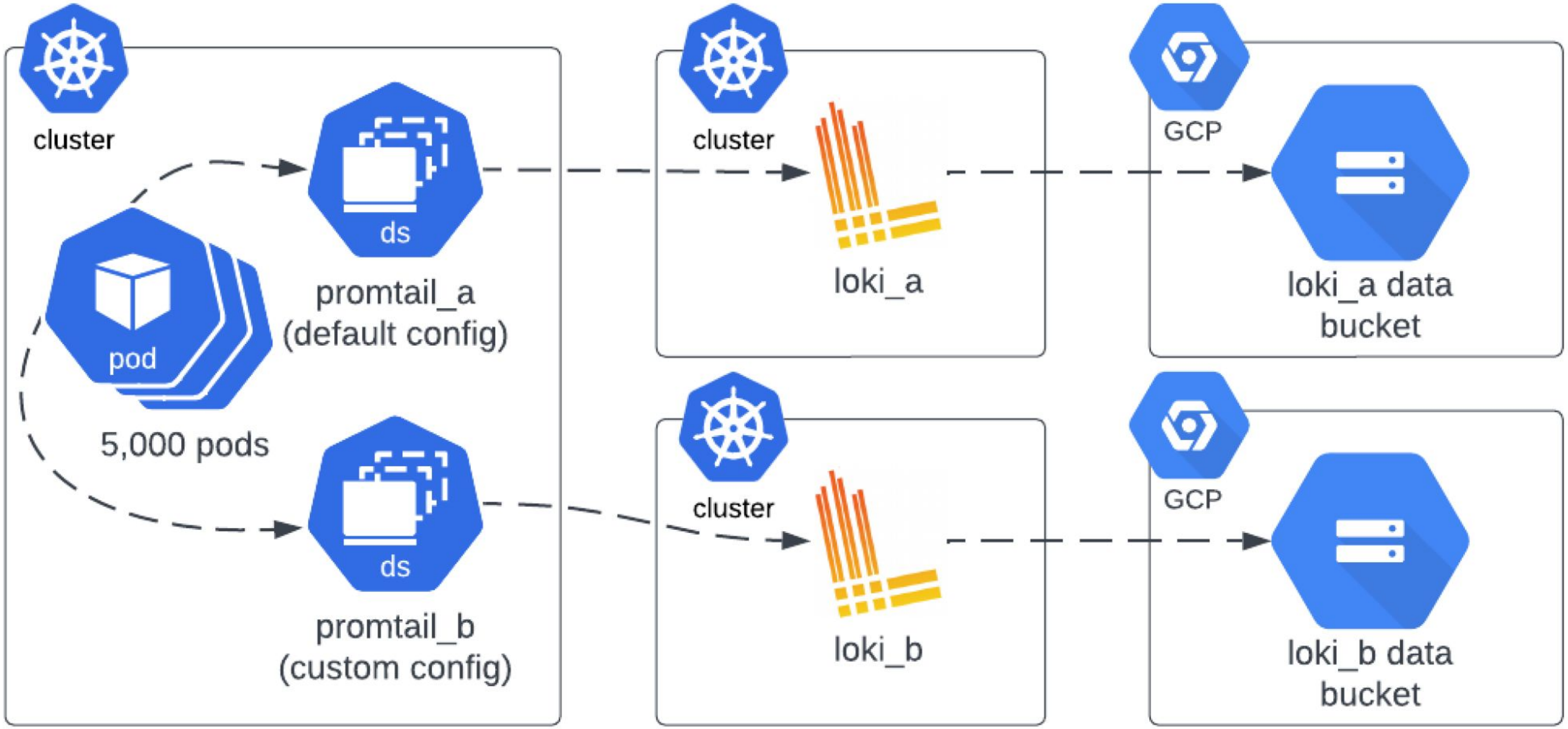
Config Changes


static
dynamic
{app=”fizz”, cluster=”buzz” }, pod=”fizz-4s6p4d4”, filename=”/var/log/pods/…z…/0.log”}
GET /users/id
log labels
content
content
indexed
indexed
unindexed
unindexed

```
scrape_configs:
  - job_name: kubernetes-pods
    kubernetes_sd_configs:
      - role: pod
    pipeline_stages:
      - cri: {}
      - replace:
          expression: "(.*)"
          replace: "pod=\"{{ .pod }}\" filename=\"{{ .filename }}\" {{ .Value }}"
      - labeldrop:
        - filename
        - pod
```

Measuring The Impact

Test Cluster



Measuring The Impact

`logcli` - command line tool to interface with Loki API

`--analyze-labels` - logcli argument to audit labels and stream count

```
logcli series {} --analyze-labels --addr="https://loki-a.com" --since=1h
```

Measuring The Impact

DEFAULT

```
❯ logcli series {} --analyze-labels --addr="https://loki-a.com" --since=1h
Total Streams:  5040
Unique Labels:  9

Label Name   Unique Values  Found In Streams
filename     5031           5040
pod          4893           5040
container    43             5040
job          35             5040
app          32             5040
node_name    29             5040
namespace    16             5040
component    14             159
stream       2              5040
```

100x Improvement

OPTIMIZED

```
❯ logcli series {} --analyze-labels --addr="https://loki-b.com" --since=1h
Total Streams:  54
Unique Labels:  7

Label Name   Unique Values  Found In Streams
container    42             54
job          33             54
app          30             54
node_name    29             54
namespace    16             54
component    12             19
stream       2              54
```

Measuring The Impact

DEFAULT

```
❯ logcli query '{app="random-logger"}' --addr="https://loki-a.com" --limit=1000
--since=721h --stats
...
Querier.TotalChunksDownloaded 730
Querier.ChunksDownloadTime    317.754626m[illegible]
...
Summary.TotalBytesProcessed   20 MB
Summary.TotalLinesProcessed   15[illegible]73[illegible]
Summary.ExecTime              1.941192303s
...
```

OPTIMIZED

```
❯ logcli query '{app="random-logger"}' --addr="https://loki-b.com" --limit=1000
--since=721h --stats
...
Querier.TotalChunksDownloaded 4
Querier.ChunksDownloadTime    [illegible]28646ms
...
Summary.TotalBytesProcessed   576 kB
Summary.TotalLinesProcessed   2469
Summary.ExecTime              43.567752ms
...
```

40x faster

97% less data

The Case of the Missing Logs

“Maximum active stream limit exceeded, **reduce the number of active streams** (**reduce labels or reduce label values**), or contact your Loki administrator to see if the limit can be increased”

The fix: Reduce the cardinality of our logs.

CLOSED

Key Takeaways

Every cluster is unique, test your cardinality before making any changes.

Upping your max active stream count isn't always the right solution. Try looking at cardinality first.

Observability is the lifeblood of your systems, it's your ability to diagnose and fix problems. It's worth spending time to tune your configuration for your use-case.

The PLG Stack is Awesome.

Thank you to grafana labs and the incredible community around them for developing and maintaining this tooling.

```
“Maximum active stream limit exceeded, reduce the number
of active streams (reduce labels or reduce label
values), or contact your Loki administrator to see if
the limit can be increased”
```

Best error log ever?

Session Feedback

Please scan the QR Code above
to leave feedback on this session