Life of an Alert

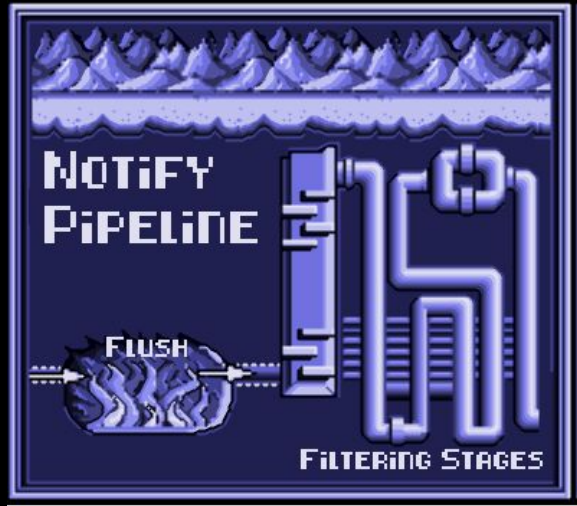
PromCon 2018 – 2018-08-09

Stuart Nelson

Why does the Alertmanager exist?


Alert Generator
Ingestion
API
Alert Provider

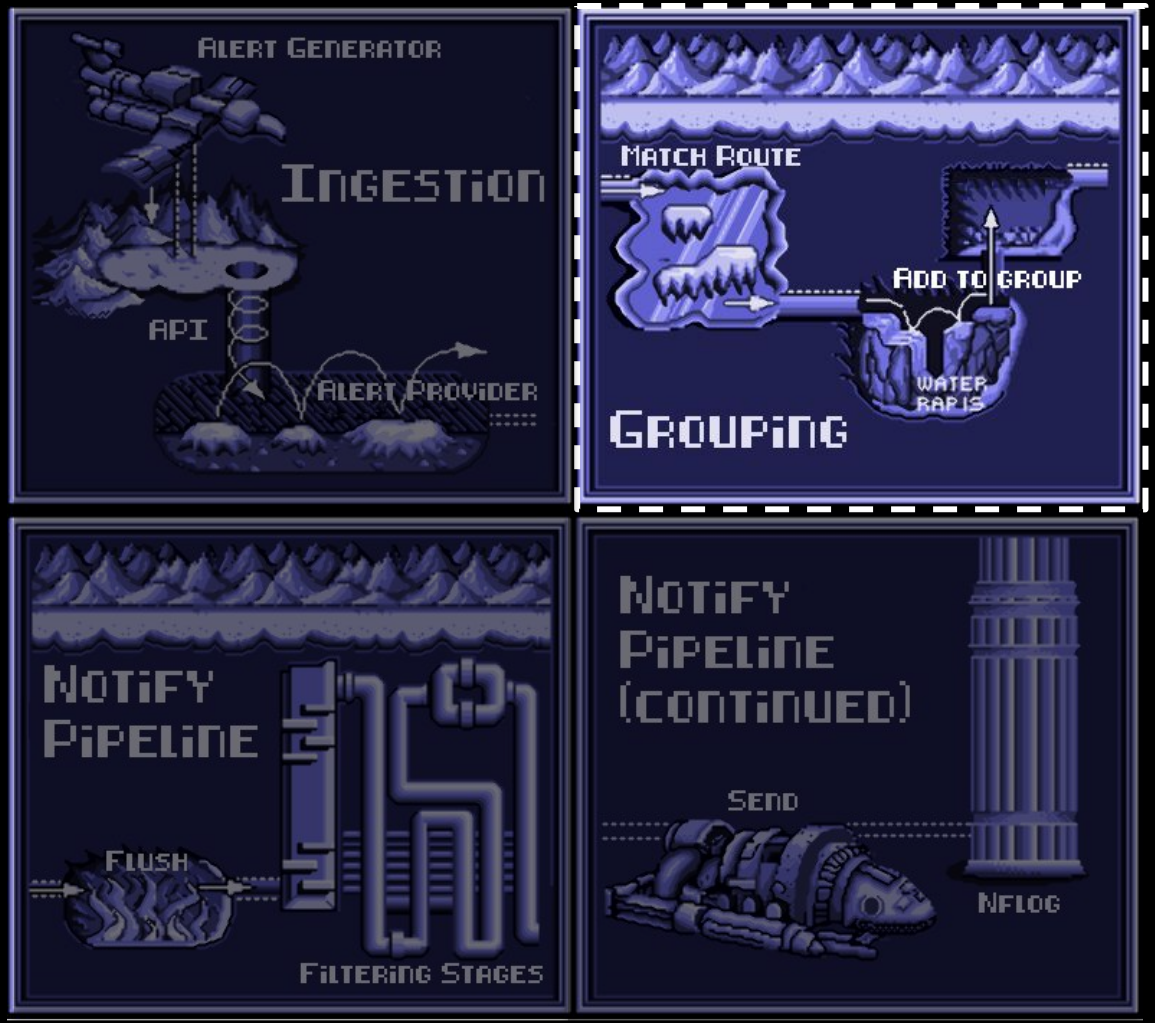

Match Route
Add to Group
Water Rapis
Grouping


Notify
Pipeline
Flush
Filtering Stages


Notify
Pipeline
(continued)
Send
Nflog

But …
What's actually happening?


Alert Generator
Ingestion
API
Alert Provider
Match Route
Add to Group
Water Rapis
Grouping
Notify Pipeline
Flush
Filtering Stages
Notify Pipeline (continued)
Send
Nflog


Alert Generator
Ingestion
API
Alert Provider
Match Route
Add to Group
Water Rapis
Grouping
Notify Pipeline
Flush
Filtering Stages
Notify Pipeline (continued)
Send
Nflog

Match Route

- ➔ Why do we match routes?
- ➔ `match`: Direct label match
- ➔ `match_re`: Regex label match
- ➔ Alerts are routed to most specific match
- ➔ Route visualizer helps!

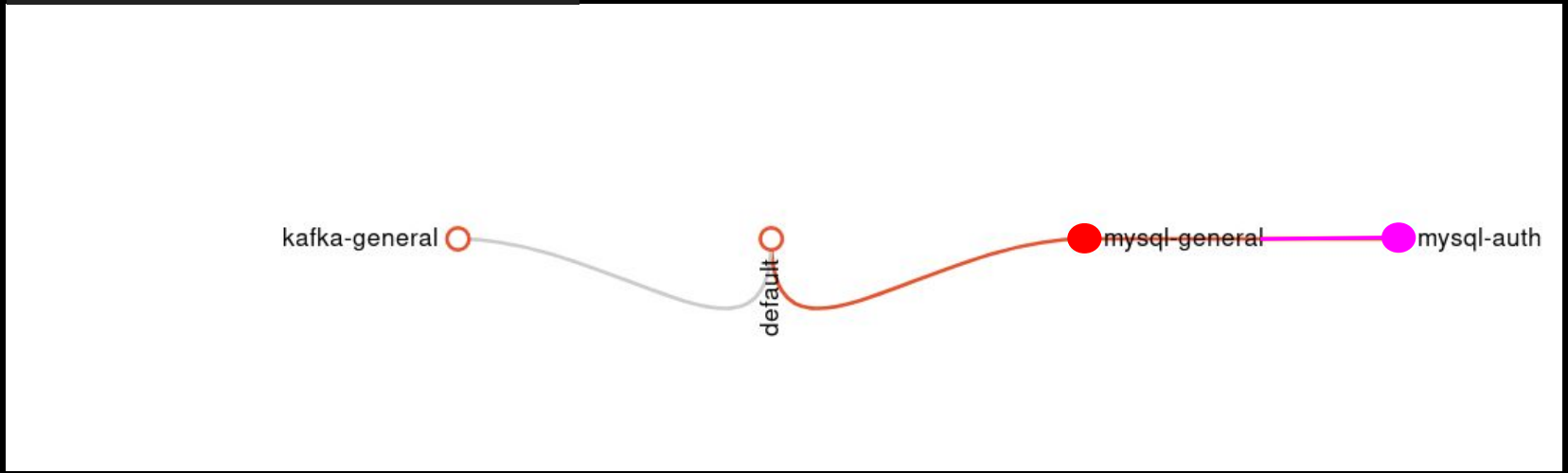
```
route:
  group_by: ['alertname', 'system']
  group_wait: 20s
  group_interval: 30m
  repeat_interval: 3h
  receiver: 'default'
  routes:
    - receiver: 'mysql-general'
      match:
        system: 'mysql'
      routes:
        - receiver: 'mysql-auth'
          match_re:
            cluster: 'user|api'
    - receiver: 'kafka-general'
      match_re:
        system: 'kafka'
```

SOUNDCLOUD

https://prometheus.io/webtools/alerting/routing-tree-editor/

```yaml
routes:
  - receiver: 'mysql-general'
    match:
      system: 'mysql'
    routes:
      - receiver: 'mysql-auth'
        match_re:
          cluster: 'user|api'
  - receiver: 'kafka-general'
    match:
      system: 'kafka'
```

```
{
 system="mysql",
 region="us-east-1",
 zone="ab",
 cluster="user"
}
```



Add to Group

- ➔ Why do we group?
- ➔ `group_wait`: bundle alerts for first notification
- ➔ `group_interval`: send notification for new or resolved alerts
- ➔ `repeat_interval`: remind users that alerts are still firing

```
route:
  group_by: ['alertname', 'system', 'dc']
  group_wait: 20s
  group_interval: 30m
  repeat_interval: 3h
  receiver: 'default'
```

SOUNDCLOUD


Alert Generator
Ingestion
API
Alert Provider


Match Route
Add to Group
Water Rapis
Grouping


Notify
Pipeline
Flush
Filtering Stages


Notify
Pipeline
(continued)
Send
Nflog

Inhibition

- ➔ Why do we inhibit?
- ➔ What should you inhibit?

```
inhibit_rules:
  - source_match:
      alertname: 'TORRouterDown'
    target_match_re:
      alertname: '.*Unreachable'
    equal: ['dc', 'rack']
```

Inhibiting Alert:
{ alertname="TorRouterDown", dc="MUC", rack="a01", team="networking" }

```
inhibit_rules:
  - source_match:
     alertname: 'TORRouterDown'
    target_match_re:
     alertname: '.*Unreachable'
    equal: ['dc', 'rack']
```

Inhibited Alert:
{ alertname="MysqlUnreachable", dc="MUC", rack="a01", team="backend" }


Alert Generator
Ingestion
API
Alert Provider

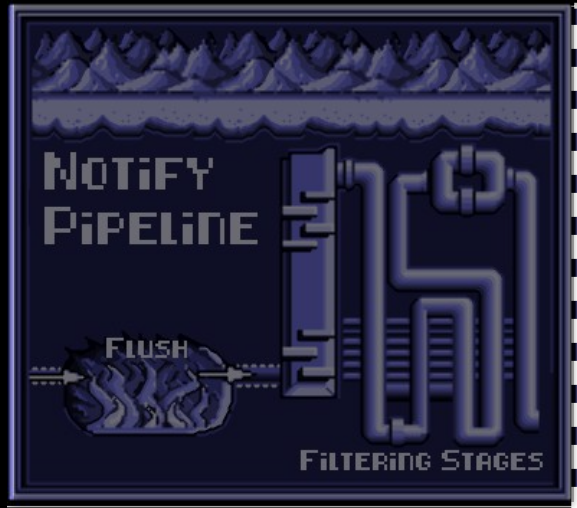

Match Route
Add to Group
Water Rapis
Grouping


Notify
Pipeline
Flush
Filtering Stages


Notify
Pipeline
(continued)
Send
Nflog


Alert Generator
Ingestion
API
Alert Provider

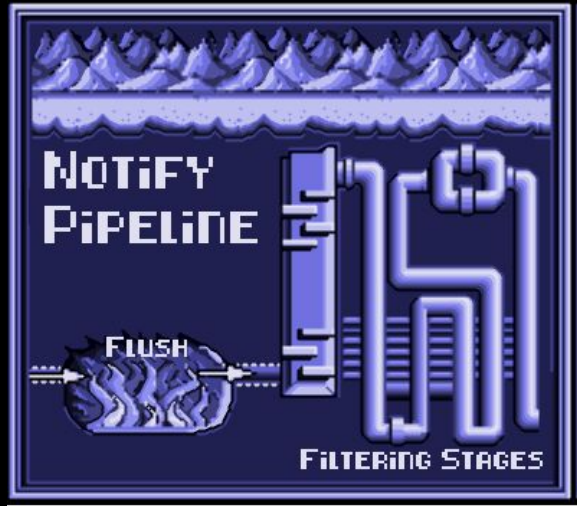

Match Route
Add to Group
Water Rapis
Grouping


Notify Pipeline
Flush
Filtering Stages


Notify Pipeline (continued)
Send
Nflog


Alert Generator
Ingestion
API
Alert Provider


Match Route
Add to Group
Water Rapis
Grouping


Notify
Pipeline
Flush
Filtering Stages


Notify
Pipeline
(continued)
Send
Nflog

(end)