

rdatadev dec. 2021

GRAFANA Loki / Promtail

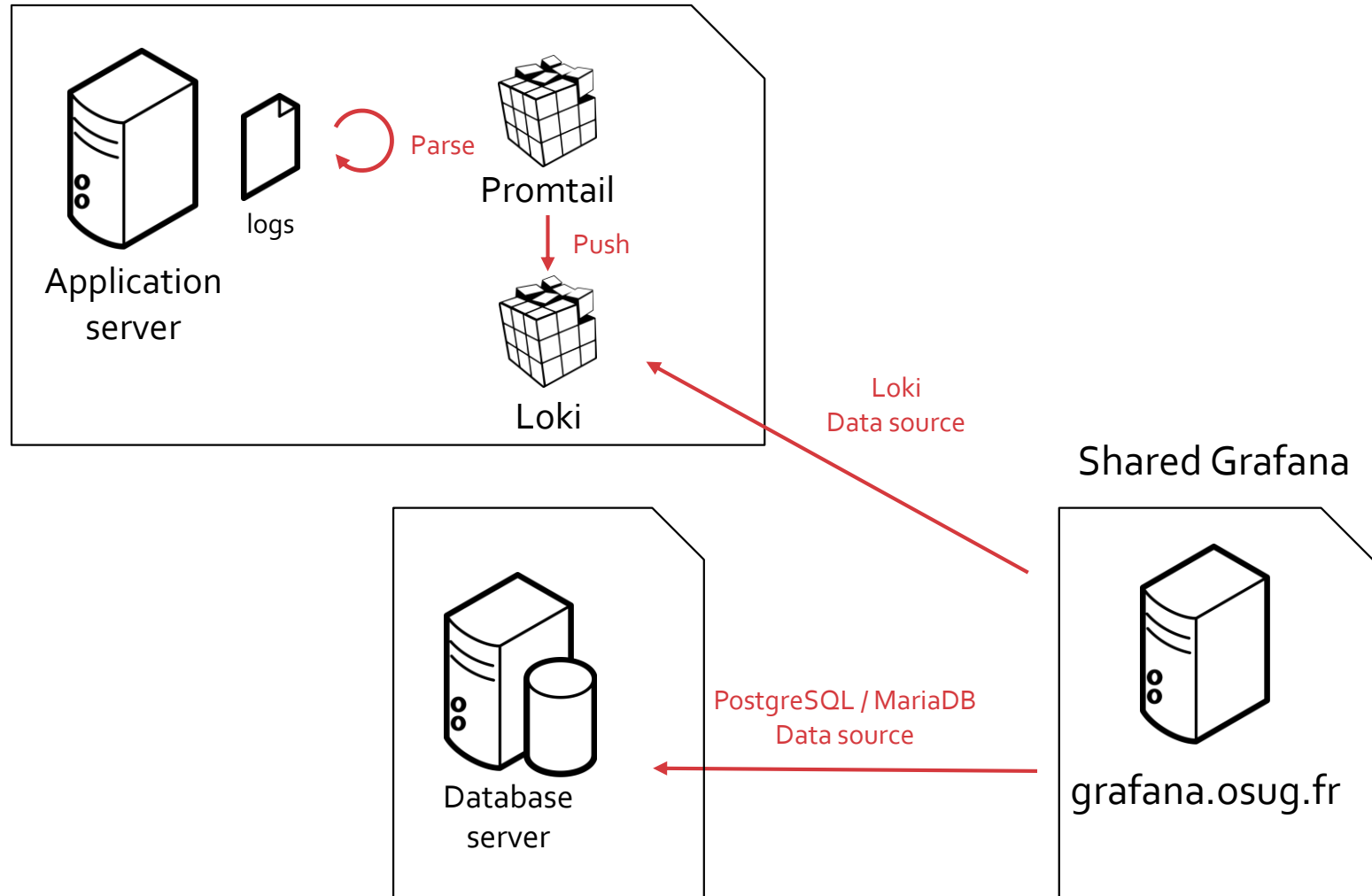
Use case in SPHERE & SSHADE

Loki

Promtail

- <https://grafana.com/oss/loki/>
- “Loki is a horizontally-scalable, highly-available, multi-tenant log aggregation system inspired by Prometheus. It is designed to be very cost effective and easy to operate. It does not index the contents of the logs, but rather a set of labels for each log stream.”
- <https://grafana.com/docs/loki/latest/clients/promtail/>
- “Promtail is an agent which ships the contents of local logs to a private Loki instance or Grafana Cloud. It is usually deployed to every machine that has applications needed to be monitored.”

Overview



Installation

- <https://grafana.com/docs/loki/latest/installation/docker/>
- Install Loki and Promtail on local machine
- Customized to deploy services configuration from Ansible

```
services:
  loki:
    image: grafana/loki:latest
    restart: unless-stopped
    ports:
      - "3100:3100"
    volumes:
      - /srv/docker/loki/config/loki:/etc/loki
    command: -config.file=/etc/loki/local-config.yaml
    networks:
      - loki

  promtail:
    image: grafana/promtail:latest
    restart: unless-stopped
    volumes:
      - /var/log:/var/log
      - /srv/docker/loki/config/promtail:/etc/promtail
    command: -config.file=/etc/promtail/config.yml
    networks:
      - loki
```

Loki retention policy

- <https://grafana.com/docs/loki/latest/operations/storage/retention/>
- 28 days retention

```
chunk_store_config:
  max_look_back_period: 672h

table_manager:
  retention_deletes_enabled: true
  retention_period: 672h
```

- Example of space usage on sphere-dc :

```
spherdwh@sphere-dc ~
$ docker ps --size
CONTAINER ID   IMAGE                                PORTS                NAMES                SIZE
a34f856829d0   grafana/promtail:latest             loki_promtail_1     546B (virtual 168MB)
26ffb818fc24   grafana/loki:latest                  0.0.0.0:3100->3100/tcp loki_loki_1         853MB (virtual 915MB)
```

Promtail

- targets

```
- job_name: tomcat
  static_configs:
    # Tomcat logs
    - targets:
      | - localhost
      labels:
      | job: tomcat
      | __path__: /var/log/tomcat8/catalina.out

    # DC application logs
    - targets:
      | - localhost
      labels:
      | job: application
      | __path__: /var/log/tomcat8/{sphere-server,sphere-server-dev,cobrex-server,cobrex-server-dev}.log

    # DB logs
    - targets:
      | - localhost
      labels:
      | job: db
      | __path__: /var/log/tomcat8/{sphere-server,sphere-server-dev,cobrex-server,cobrex-server-dev}-db.log

- job_name: sshade
  static_configs:
    # UWSGI logs
    - targets:
      | - localhost
      labels:
      | job: application
      | __path__: /var/log/uwsgi/{www,dev,sandbox}.sshade.eu/error.log
    - targets:
      | - localhost
      labels:
      | job: access
      | __path__: /var/log/uwsgi/{www,dev,sandbox}.sshade.eu/access.log
```

Promtail - parsing

```
pipeline_stages:
- match:
  selector: '{job="db"}'
  stages:
  - regex:
    expression: '^(?P<time>\S+ \S+) (?P<level>\S+) \[(?P<logger>\S+)\] - \[(?P<sql_type>[A-Z][A-Z]+) (?P<log>.*)*$'
  - labels:
    sql_type:
- match:
  selector: '{job="tomcat"}'
  stages:
  - multiline:
    firstline: '^[\S+][^a][^t]\S+'
    max_wait_time: 3s
  - replace:
    expression: '^(. *AssociationRuleOptimization)(?:Error|Exception)[:\n]'
    replace: '{{.Value}}ExcWarning (WARNING) '
  - replace:
    expression: '^(. *ProcessLauncher)(?:Error|Exception): Process output contains an error.'
    replace: '{{.Value}}ExcWarning (WARNING) '
  - replace:
    expression: '^(\s*(?:Internal Exception: |Caused by: |Exception in thread "[^"]+" )?[A-z._\d]*(?:Error|Exception)[A-z._\d]*)[:\n]'
    replace: '{{.Value}} (ERROR)'
  - regex:
    expression: '^(?P<time>\S+ \S+) (?P<level>\S+) - (?P<log>.*)*$'
  - regex:
    expression: '^(?P<time>\S+) \[(?P<thread>\S+)\] (?P<level>\S+) (?P<logger>\S+)? ?- (?P<log>.*)*$'
  - regex:
    expression: '^(?P<time>\S+ \S+) (?P<level>\S+) \[(?P<logger>\S+)\] (?P<log>.*)*$'
  - regex:
    expression: '^(?P<exception>\s*(?:Internal Exception: )?[A-z._\d]*(?:Error|Exception|ExcWarning)[A-z._\d]*) \((?P<level>\S+)\)[[:\n] ]'
  - labels:
    level:
- match:
  selector: '{job="application"}'
  stages:
  - multiline:
    firstline: '^[\S+][^a][^t]\S+'
    max_wait_time: 3s
  - replace:
    expression: '^(\s*(?:Internal Exception: |Caused by: )?[A-z._\d]*(?:Error|Exception)[A-z._\d]*)[:\n]'
    replace: '{{.Value}} (ERROR)'
  - regex:
    expression: '^(?P<time>\S+ \S+) (?P<level>\S+) \[(?P<logger>\S+)\] - (?P<log>.*)*$'
  - regex:
    expression: '^(?P<exception>\s*(?:Internal Exception: |Caused by: )?[A-z._\d]*(?:Error|Exception)[A-z._\d]*) \((?P<level>\S+)\)[[:\n] ]'
  - labels:
    level:
    logger:
```

Promtail

- parsing

```
- match:
  selector: '{job="access"}'
  stages:
  - replace:
    expression: '\((HTTP\S+ 200)\)'
    replace: '{{.Value}} INFO'
  - replace:
    expression: '\((HTTP\S+ (404|403|500))\)'
    replace: '{{.Value}} ERROR'
  - replace:
    expression: '\((HTTP\S+ (3\d\d))\)'
    replace: '{{.Value}} TRACE'
  - regex:
    expression: '^\[pid: (?P<pid>\S+)\|app: (?P<app>\d+)\|req: (?P<req_nb>\d+)\/(?P<req_total>\d+)\] (?P<ip>\S+) \(\) \{.*\}
    \[(?P<time>[^\]]+)\] (?P<method>\S+) (?P<ur\>\S+) => generated (?P<size>\S+) bytes in (?P<duration>\S+) .* \((?P<http_version>HTT
    P\S+) (?P<code>\S+) ?(?P<level>\S+)\) (?P<info>.*)$'
  - pack:
    labels: [size, duration]
  - labels:
    level:
    status:
    method:
    code:
```


Promtail - parsing

- Use named capturing groups (?P<name>...)

```
- regex:
  expression: '^(?P<time>\S+ \S+) (?P<level>\S+) - (?P<log>.*)$'
- regex:
  expression: '^(?P<time>\S+) \[(?P<thread>\S+)\] (?P<level>\S+) (?P<logger>\S+)? ?- (?P<log>.*)$'
- regex:
  expression: '^(?P<time>\S+ \S+) (?P<level>\S+) \[(?P<logger>\S+)\] (?P<log>.*)$'
```

- Pack captured groups as JSON with `pack`

```
- regex:
  expression: '^\[pid: (?P<pid>\S+)\|app: (?P<app>\d+)\|req: (?P<req_nb>\d+)\|(?P<req_total>\d+)\] (?P<ip>\S+) \(\) \{.*\} \[(?P<time>[^\]]+)\] (?P<method>\S+) (?P<url>\S+) => generated (?P<size>\S+) bytes in (?P<duration>\S+) .* \[(?P<http_version>HTT P\S+) (?P<code>\S+) ?(?P<level>\S+)?\] (?P<info>.*)$'
- pack:
  labels: [size, duration]
```

```
2021-12-14 13:21:08 [pid: 6777|app: 0|req: 34084/278083] 157.90.209.78 () {38 vars in 803 bytes}
(HTTP/1.1 200 INFO) 4 headers in 307 bytes (1 switches on core 0)
```

Log labels	
code	200
duration	628
filename	/var/log/uwsgi/www.sshade.eu/access.log
job	access
level	INFO
method	GET
size	28235

Detected fields	
ts	2021-12-14T12:21:08.642Z
tsNs	1639484468642518093

Promtail - parsing

- Use `replace` to inject a customized log level

```
- replace:
  expression: '^(*AssociationRuleOptimization)(?:Error|Exception)[:\n]'
  replace: '{{.Value}}ExcWarning (WARNING) '
- replace:
  expression: '^(*ProcessLauncher)(?:Error|Exception): Process output contains an error.'
  replace: '{{.Value}}ExcWarning (WARNING) '
- replace:
  expression: '^(\s*(?:Internal Exception: |Caused by: |Exception in thread "[^"]+" )?[A-z._\d]*(?:Error|Exception)[A-z._\d]*)[:\n]'
  replace: '{{.Value}} (ERROR) '
- regex:
  expression: '^(?P<time>\S+ \S+) (?P<level>\S+) - (?P<log>.*)$'

  - replace:
    expression: '\\((HTTP\S+ 200)\\)'
    replace: '{{.Value}} INFO'
  - replace:
    expression: '\\((HTTP\S+ (404|403|500))\\)'
    replace: '{{.Value}} ERROR'
  - replace:
    expression: '\\((HTTP\S+ (3\d\d))\\)'
    replace: '{{.Value}} TRACE'
- regex:
  expression: '^\[pid: (?P<pid>\S+)\\|app: (?P<app>\d+)\\|req: (?P<req_nb>\d+)\\/(?P<req_total>\d+)\\ (?:P<ip>\S+) \\(\\) \\. * \\(\\(P<http_version>HTT
P\S+) (?P<code>\S+) (?P<level>\S+)?\\) (?P<info>.*)$'
```

- Use `multiline` to group stack traces lines

```
selector: '{job="tomcat"}'
stages:
- multiline:
  firstline: '^\\S+[^a][^t]\\S'
  max_wait_time: 3s

selector: '{job="application"}'
stages:
- multiline:
  firstline: '^\\(Traceback|\\S+)'
  max_wait_time: 3s
```

```
> 2021-12-14 06:49:08 Traceback (ERROR) (most recent call last):
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 270, in __call__
    response = self.execution_policy(environ, self)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 276, in default_execution_policy
    return router.invoke_request(request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 245, in invoke_request
    response = handle_request(request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/tweens.py", line 43, in excview_tween
    response = _error_handler(request, exc)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/tweens.py", line 17, in _error_handler
```

Promtail

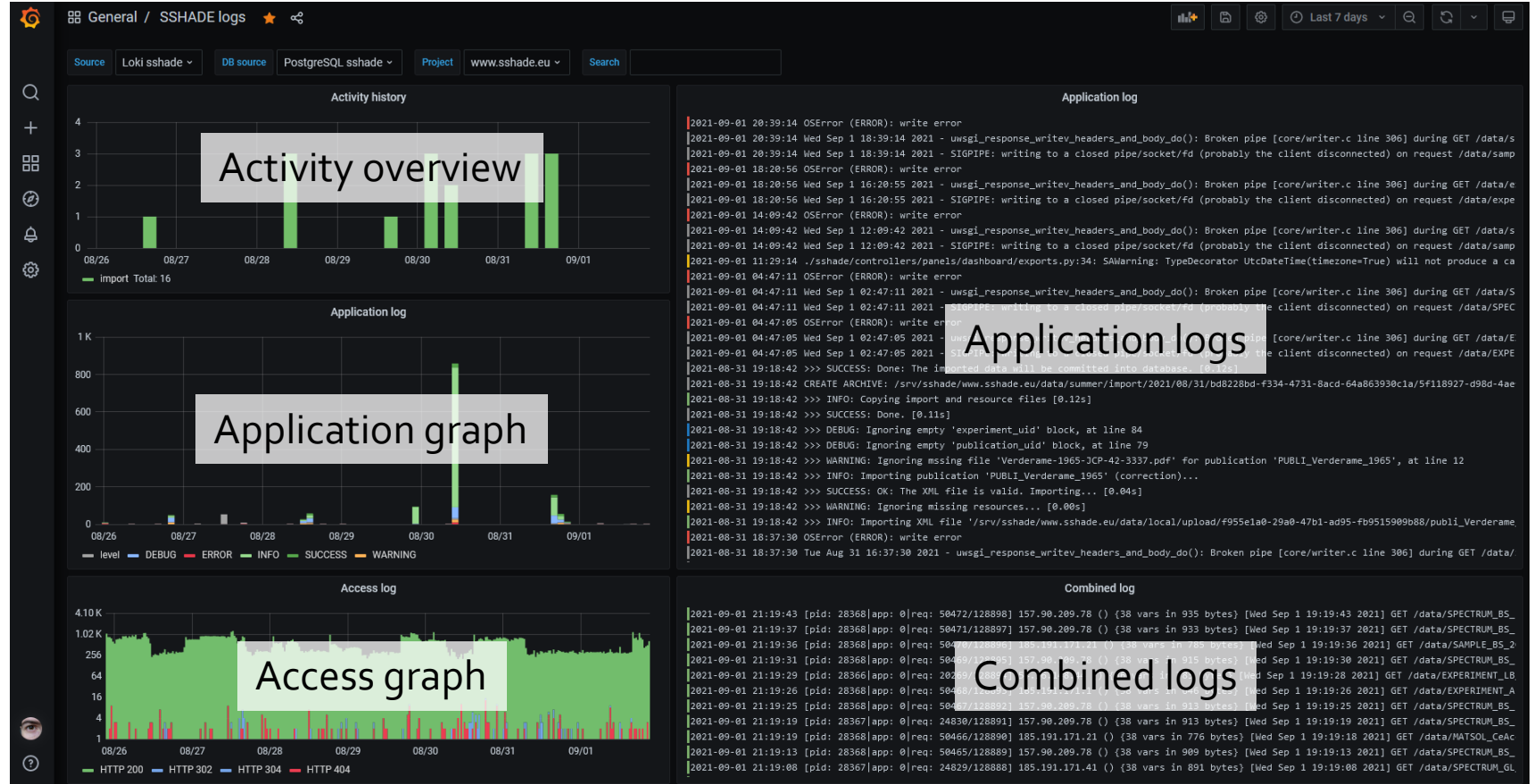
- parsing

Notes

- Grafana uses Go lang regular expressions, no negative/positive lookahead/lookbehind

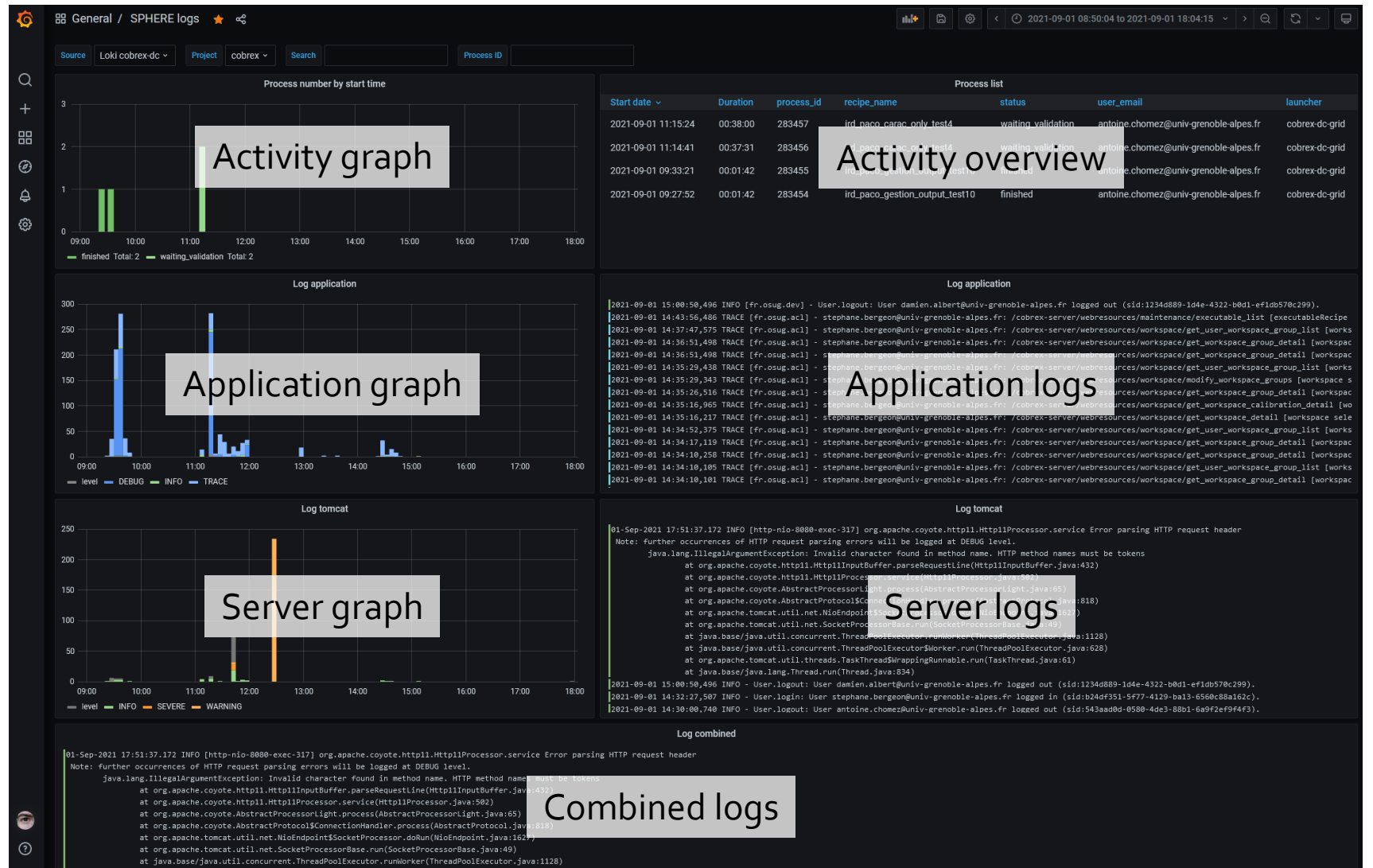
Grafana logs dashboard

SSHADe



Grafana logs dashboard

SPHERE



Grafana - logs

- Correlate activity/database requests to logs with combined logs
- Unpack JSON with `| unpack`, refine query with `| var = "value"`
- Explore labels, wrap, deduplication

The screenshot displays the Grafana Logs Explorer interface. At the top, the 'Explore' tab is active, showing the Loki data source 'sphere-dc'. Three log queries are defined:

- Query 1: `{job=~"tomcat"} |~ ""`
- Query 2: `{job=~"application", filename=~".*.*.*)" |~ ""`
- Query 3: `{job="db", filename=~".*.*.*", sql_type!=""} |~ ""`

Each query has a 'Range' query type and a 'Line limit' of 'auto'. Below the queries, a 'Logs' section shows a distribution chart with a legend for log levels: warning (yellow), info (green), unknown (grey), error (red), debug (blue), and trace (cyan). The chart shows a significant spike in debug logs at 12:00. Below the chart, there are controls for 'Time' (checked), 'Unique labels' (unchecked), 'Wrap lines' (checked), 'Dedup' (None), and 'Flip results order'. At the bottom, the log output is shown with a limit of 2000 (2000 returned) and a total bytes processed of 1.16 MB. The log entries are:

```
> 2021-12-14 13:30:01 2021-12-14 13:30:01,253 DEBUG [fr.osug.dev] - Grid api request /resources/3016: HTTP/1.1 200 OK
> 2021-12-14 13:30:01 2021-12-14 13:30:01,213 DEBUG [fr.osug.dev] - Grid api request /resources/nodes/luke63: HTTP/1.1 200 OK
> 2021-12-14 13:30:01 2021-12-14 13:30:01,166 DEBUG [fr.osug.dev] - Grid api request /resources/1377: HTTP/1.1 200 OK
> 2021-12-14 13:30:01 2021-12-14 13:30:01,123 DEBUG [fr.osug.dev] - Grid api request /resources/nodes/luke54: HTTP/1.1 200 OK
```

Grafana - logs

- Explore combined logs : split, link, show/hide



The image displays two side-by-side screenshots of the Grafana Explore interface, demonstrating log exploration capabilities.

Left Screenshot:

- Log browser:** Query: `{job="application", filename=~".*www.sshade.eu.*"} |~ ""`
- Log browser:** Query: `{job="access", filename=~".*www.sshade.eu.*"} | unpack |~ ""`
- Logs:** A bar chart showing log volume over time, with a legend for 'error' (red) and 'unknown' (grey).
- Common labels:** application Limit: 1000 (8 returned) Total bytes processed: 3.75 kB
- Log entries:**

```
> 2021-12-14 06:50:01 OSError (ERROR): write error
> 2021-12-14 06:50:01 Tue Dec 14 05:50:01 2021 - uwsgi_response_write_headers_and_body_do(): Broken pipe [core/writer.c line 306] during GET /data/SPECTRUM_OP_20180117_002/details (73.36.40.61)
> 2021-12-14 06:50:01 Tue Dec 14 05:50:01 2021 - SIGPIPE: writing to a closed pipe/socket/fd (probably the client disconnected) on request /data/SPECTRUM_OP_20180117_002/details (ip 73.36.40.61) !!!
> 2021-12-14 06:49:08 Exception (ERROR): ERROR: This account is already validated.
> 2021-12-14 06:49:08 Traceback (ERROR) (most recent call last):
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 270, in __call__
    response = self.execution_policy(environ, self)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 276, in default_execution_policy
    return router.invoke_request(request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 245, in invoke_request
    response = handle_request(request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/tweens.py", line 43, in excview_tween
    response = _error_handler(request, exc)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/tweens.py", line 17, in _error_handler
    reraise(*exc_info)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/util.py", line 733, in reraise
    raise value
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/tweens.py", line 41, in excview_tween
    response = handler(request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/router.py", line 144, in handle_request
    registry, request, context, context_iface, view_name
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/view.py", line 674, in __call_view
    response = view_callable(context, request)
  File "/srv/sshade/www.sshade.eu/sshade/.venv/lib/python3.7/site-packages/pyramid/config/views.py", line 151, in __call__
    return view(context, request)
```

Right Screenshot:

- Log browser:** Query: `{job="application", filename=~".*www.sshade.eu.*"} |~ ""`
- Log browser:** Query: `{job="access", filename=~".*www.sshade.eu.*"} | unpack |~ ""`
- Logs:** A bar chart showing log volume over time, with a legend for 'info' (green), 'trace' (blue), and 'error' (red).
- Common labels:** access Limit: 1000 (103 returned) Total bytes processed: 92.1 kB
- Log entries:**

```
> 2021-12-14 06:50:01 [pid: 74256]app: 0|req: 42335/274476| 73.36.40.61 () (58 vars in 1704 bytes) [Tue Dec 14 05:50:00 2021] GET /data/SPECTRUM_OP_20180117_002/details => generated 0 bytes in 833 msec (HTTP/1.1 200 INFO) 2 headers in 0 bytes (0 switches on core 0)
> 2021-12-14 06:49:59 [pid: 74256]app: 0|req: 42334/274475| 73.36.40.61 () (58 vars in 1666 bytes) [Tue Dec 14 05:49:59 2021] GET /user/register => generated 10825 bytes in 70 msec (HTTP/1.1 200 INFO) 2 headers in 82 bytes (1 switches on core 0)
> 2021-12-14 06:49:56 [pid: 104295]app: 0|req: 29815/274474| 54.36.149.70 () (36 vars in 643 bytes) [Tue Dec 14 05:49:56 2021] GET /data/MATNET_PCV05230_ID_20170721_005/MATERIAL_ID_20170721_005/CONST_ID_20170721_013/ATOM_O => generated 23940 bytes in 36 msec (HTTP/1.1 200 INFO) 4 headers in 307 bytes (1 switches on core 0)
> 2021-12-14 06:49:52 [pid: 107766]app: 0|req: 45151/274473| 73.36.40.61 () (58 vars in 1690 bytes) [Tue Dec 14 05:49:52 2021] GET /user/configure/identity => generated 11434 bytes in 14 msec (HTTP/1.1 200 INFO) 2 headers in 82 bytes (1 switches on core 0)
> 2021-12-14 06:49:50 [pid: 74256]app: 0|req: 42333/274472| 185.191.171.17 () (38 vars in 791 bytes) [Tue Dec 14 05:49:50 2021] GET /data/matter/MATSO_L_HuyGare-100-200_BS_20210401/MATERIAL_BS_20210401_230/CONST_BS_20200813_123/ATOM_Mn => generated 27897 bytes in 56 msec (HTTP/1.1 200 INFO) 4 headers in 307 bytes (1 switches on core 0)
> 2021-12-14 06:49:50 [pid: 107766]app: 0|req: 45150/274471| 73.36.40.61 () (58 vars in 1701 bytes) [Tue Dec 14 05:49:50 2021] GET /user/configure/agreement => generated 11510 bytes in 17 msec (HTTP/1.1 200 INFO) 2 headers in 82 bytes (1 switches on core 0)
> 2021-12-14 06:49:41 [pid: 42728]app: 0|req: 28315/274470| 185.191.171.38 () (38 vars in 951 bytes) [Tue Dec 14 05:49:41 2021] GET /data/EXPERIMENT_OP_20201104_001/SPECTRUM_OP_20200915_015/SAMPLE_OP_20200915_015/LAYER_1_OP_20200915_015/MATHIN_OP_20201103_002/MATERIAL_OP_20201103_100/CONST_OP_20201103_300/ATOM_Sc => generated 22707 bytes in 73 msec (HTTP/1.1 200 INFO) 4 headers in 307 bytes (2 switches on core 0)
> 2021-12-14 06:49:39 [pid: 107766]app: 0|req: 45149/274469| 73.36.40.61 () (62 vars in 1734 bytes) [Tue Dec 14 05:49:39 2021] GET /user/profile => generated 15522 bytes in 64 msec (HTTP/1.1 200 INFO) 2 headers in 82 bytes (1 switches on core 0)
> 2021-12-14 06:49:38 [pid: 104295]app: 0|req: 29814/274468| 73.36.40.61 () (68 vars in 1097 bytes) [Tue Dec 14 05:49:38 2021] POST /user/configure/agreement => generated 202 bytes in 13 msec (HTTP/1.1 302 TRACE) 3 headers in 129 bytes (1 switches on core 0)
> 2021-12-14 06:49:31 [pid: 74256]app: 0|req: 42332/274467| 73.36.40.61 () (62 vars in 1757 bytes) [Tue Dec 14 05:49:31 2021] GET /user/configure/agreement => generated 11510 bytes in 22 msec (HTTP/1.1 200 INFO) 2 headers in 82 bytes (2 switches on core 0)
> 2021-12-14 06:49:31 [pid: 107766]app: 0|req: 45148/274466| 73.36.40.61 () (68 vars in 1906 bytes) [Tue Dec 14 05:49:31 2021] POST /user/configure/identity => generated 214 bytes in 13 msec (HTTP/1.1 302 TRACE) 3 headers in 141 bytes (2 switches on core 0)
```

Variables

Variable	Definition
<code>datasource</code>	<code>loki</code>
<code>db_datasource</code>	<code>postgres</code>
<code>project</code>	<code>.*,www.sshade.eu,dev.sshade.eu,sandbox.sshade.eu</code>
<code>search</code>	

- Use variables for Loki and database sources
- Restrict logs to project : `filename=~".*$project.*"`
- Search field on all queries : `|~ "$search"`
- Exclude query, either :
 - exclude a non existing string by default (ie. `"_no_exclusion_"`)
 - hack the search field with `"!~ "value`

Variable from SQL

Query Options

Data source	<input type="text" value="{datasource}"/>	Refresh	<input type="text" value="Never"/>
Query	SELECT CONCAT(u.id, ':', u.email) FROM user u ORDER BY u.last_login_date DESC		
Regex	/(?<value>.+)ate DESC		
Sort	Disabled		

- Use correct datasource
- `CONCAT` multiple columns then split for value/text
- Fine-tune `ORDER` in the query instead of sort
- `All` used as `IN($variable)` can be slow for text, prefer numeric id if available

Selected (1)

All

IFS

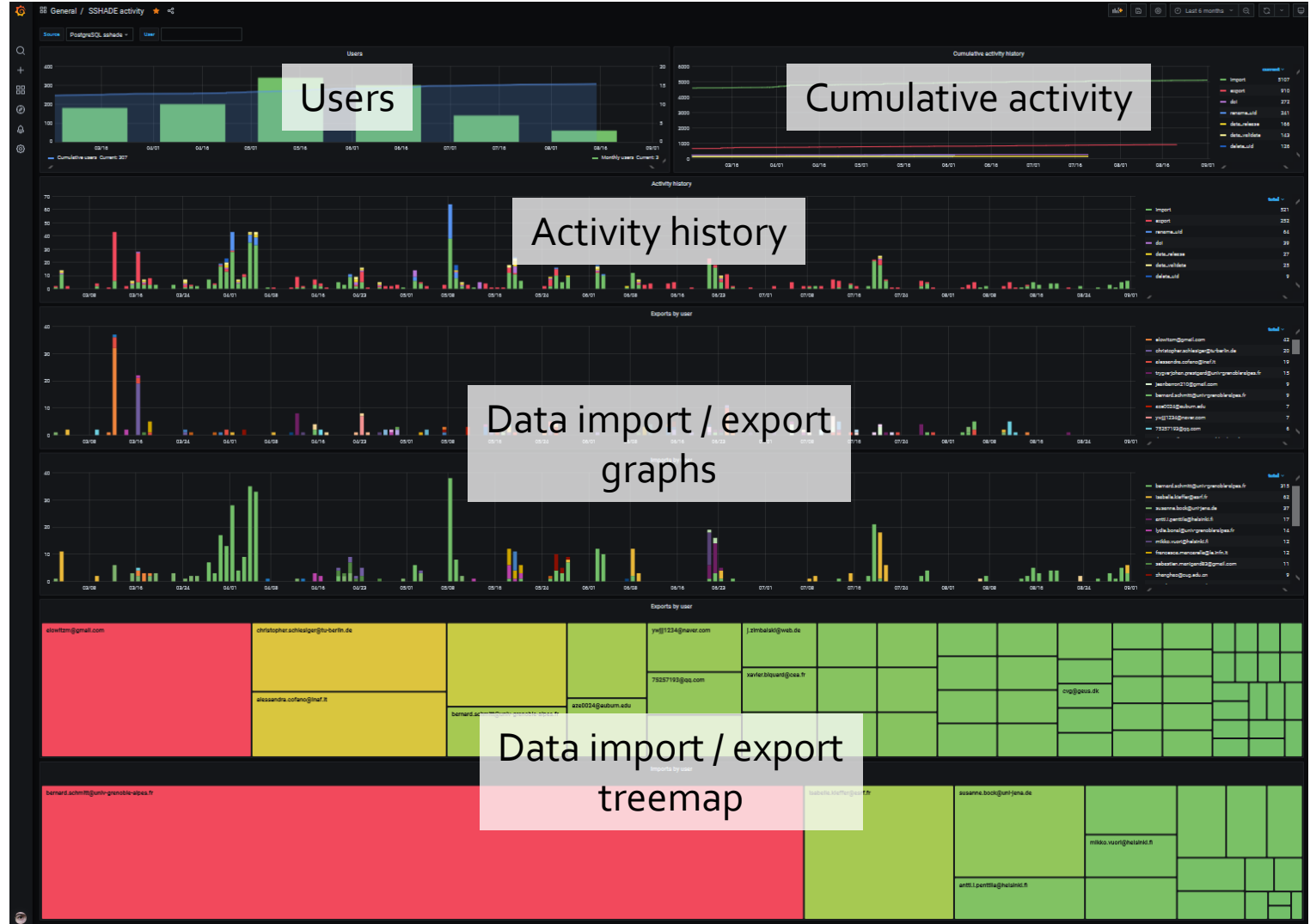
IRDIS

LSS

SPHERE

ZIMPOL

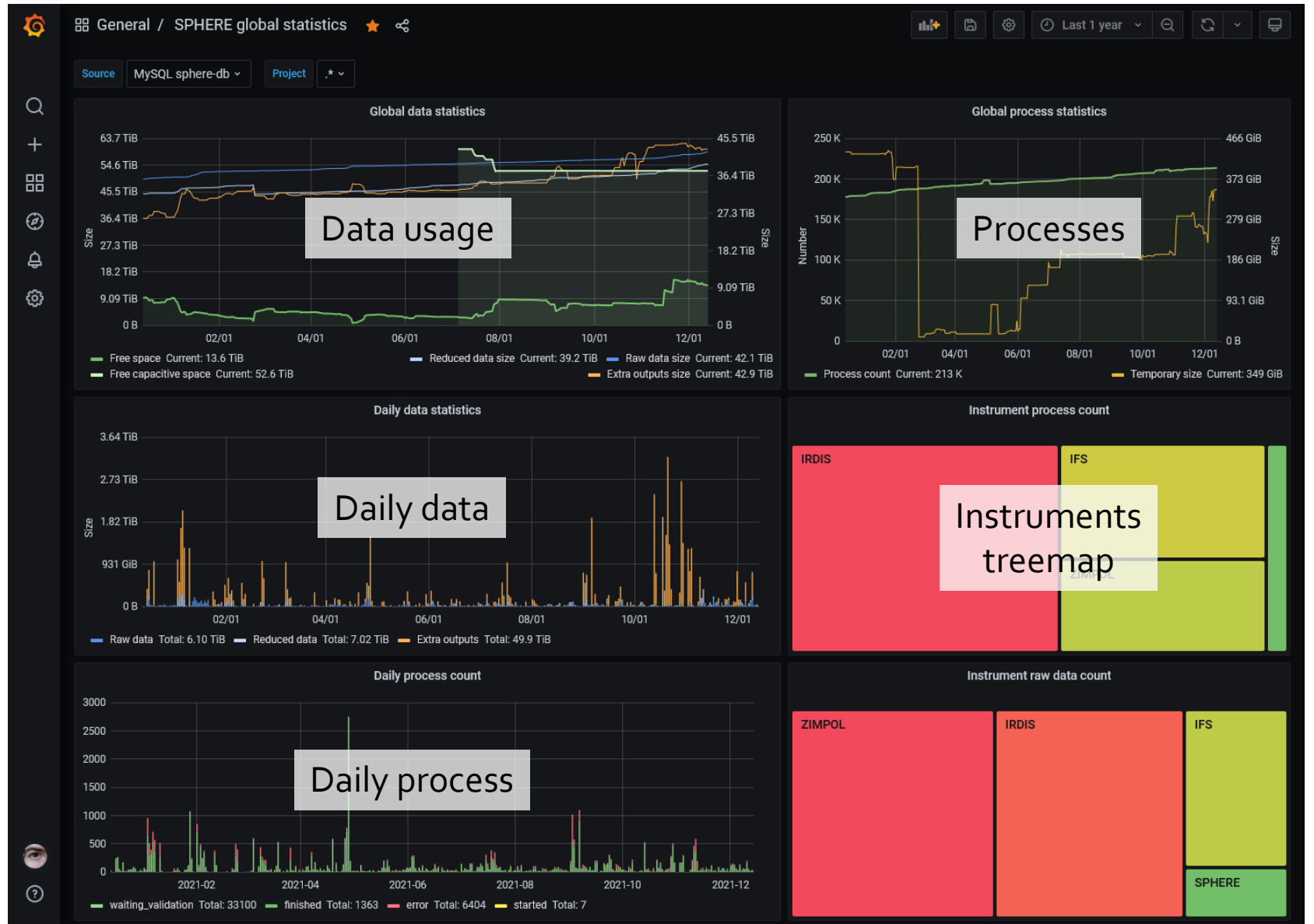
Grafana - activity SSHADE



Grafana

- global activity

SPHERE



Variables

Source MySQL sphere-db Project * User All Instrument All Recipe All Frame type All

Grafana
- detailed
activity

SPHERE



Timeline

Data usage

Treemaps

Tips

- Use query option Max data points, Min interval to improve readability
- Use SQL `sum(count(id)) OVER (ORDER BY date)` to display cumulative graphs
- Use Legend `{{field}}` to display a field value
- Use Inspect / Panel JSON `"aliasColors"` to override colors consistently