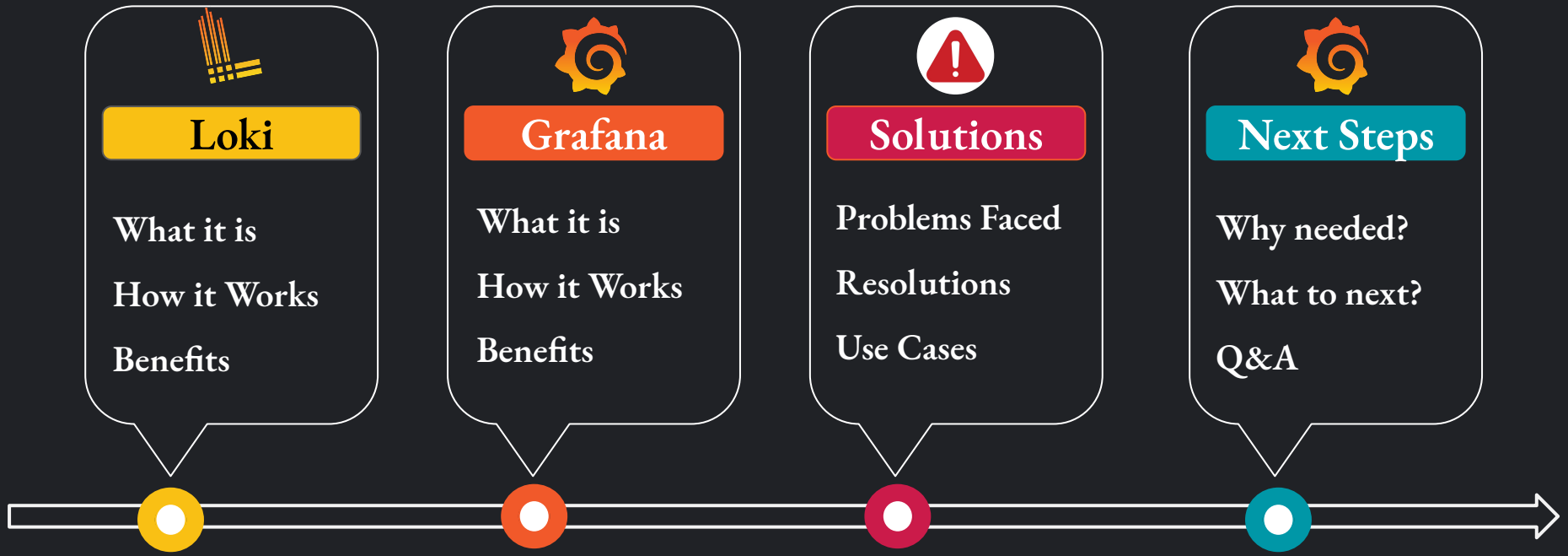
Centralized Log Aggregation & Analytics With Loki & Grafana

by ravin


Loki
What it is
How it Works
Benefits
Grafana
What it is
How it Works
Benefits
Solutions
Problems Faced
Resolutions
Use Cases
Next Steps
Why needed?
What to next?
Q&A

LOKI

- It is a horizontally scalable, highly available, multi-tenant log aggregation system inspired by prometheus
- Its Cost effective and easy to operate. Does not index contents of log
- **LogQL**

```
{ job=”frontend”, env=”dev”} => {
        time: “2020-01-23 15:56:01”.
        line: “POST /api/prom/push HTTP 1.1 502 0”
}
```

How it Works?

```
tecmint@TecMint ~ $ tailf /var/log/apache2/access.log
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozill
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 5
ox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "ht
0"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 4
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200
101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/compressed.gif HTTP/1.1"
) Gecko/20100101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/movie.gif HTTP/1.1" 200
o/20100101 Firefox/56.0"
```

Sys/App Logs

Application and system generated Logs

```
2012-08-26 15:50:46,907 - __main__ - INFO - Add wait request for demo-cpu.usage
2012-08-26 15:50:47,085 - __main__ - INFO - Handing write request msg_id=3130613
3643732656363643634373633613031383062643738636666663373939, qname=demo-log.update
, flush=None
2012-08-26 15:50:47,087 - __main__ - INFO - Write 78 byte, msg_id=31306133643732
656363643634373633613031383062643738636666663373939, qname=demo-log.update
2012-08-26 15:50:51,666 - __main__ - INFO - Handing write request msg_id=3231653
432386437616436623462646138353862373238623237616363306563, qname=demo-cpu.usage,
 flush=None
2012-08-26 15:50:51,668 - __main__ - INFO - Write 16 byte, msg_id=32316534323864
376164366234626461383538623732386232376163633065 63, qname=demo-cpu.usage
2012-08-26 15:50:51,669 - __main__ - INFO - Notify 1 requests waiting for demo-c
pu.usage
2012-08-26 15:50:51,839 - __main__ - INFO - Handing read request msg_id=32303430
336135323935643934636632626265653623339343762346363 3061, qname=demo-cpu.usage
2012-08-26 15:50:51,841 - __main__ - INFO - Read, msg_id=3230343033613532393564 3
934636632626265653623339343762346363 3061, qname=demo-cpu.usage
2012-08-26 15:50:51,844 - __main__ - INFO - Add wait request for demo-cpu.usage
2012-08-26 15:50:52,108 - __main__ - INFO - Handing write request msg_id=3864656
638656530636530333431396339343631343332306234663433363666, qname=demo-log.update
, flush=None
2012-08-26 15:50:52,110 - __main__ - INFO - Write 78 byte, msg_id=38646566386565
306365303334313963393436313433323062346634333636 66, qname=demo-log.update
```

How it Works?

Sys/App Logs

Application and system generated Logs

Promtail

Ships Logs to Loki

Discover Targets
Attaches Labels
Pushes To Loki

```
server:
  http_listen_port: 9080

clients:
  - url: http://localhost:3100/loki/api/v1/push

scrape_configs:
  - job_name: syslog
    syslog:
      json: false
      max_age: 12h
    static_configs:
      - targets:
          - localhost
        labels:
          job: syslog
          host: localhost
          __path__: /var/log/syslog
```

How it Works?

Sys/App Logs

Application and system generated Logs

Promtail

Ships Logs to Loki

Discover Targets
Attaches Labels
Pushes To Loki

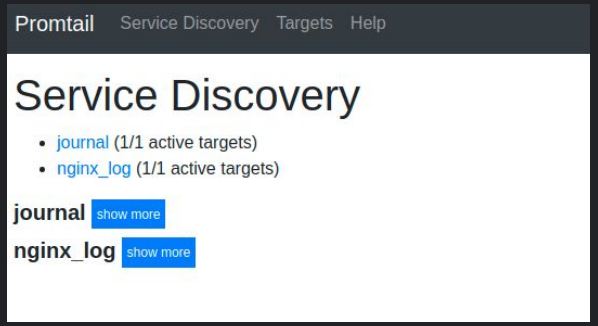
Loki Storage

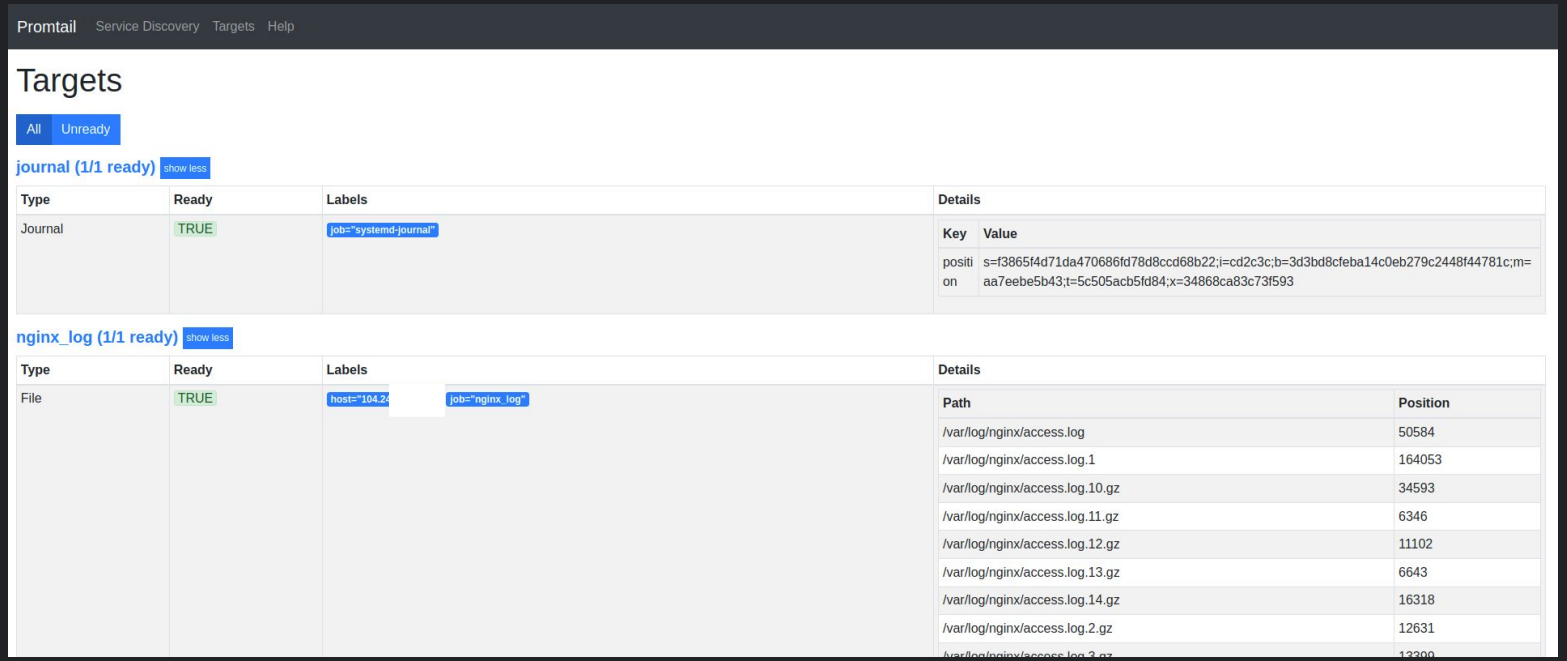
Log streams by ID & labels

Compressed chunks

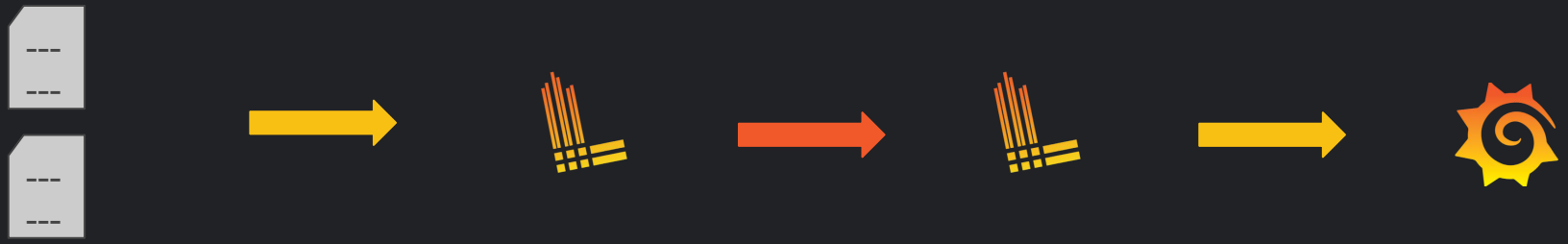
Index Stores streams/labels linking to chunk

How it Works?


Promtail
Service Discovery
Targets
Help
Service Discovery
journal (1/1 active targets)
nginx_log (1/1 active targets)
journal
show more
nginx_log
show more


Promtail
Service Discovery
Targets
Help
Targets
All
Unready
journal (1/1 ready)
show less
Type
Ready
Labels
Details
Journal
TRUE
job="systemd-journal"
Key
Value
position
s=f3865f4d71da470686fd78d8ccd68b22;i=cd2c3c;b=3d3bd8cfeba14c0eb279c2448f44781c;m=aa7eebe5b43;t=5c505acb5fd84;x=34868ca83c73f593
nginx_log (1/1 ready)
show less
Type
Ready
Labels
Details
File
TRUE
host="104.24
job="nginx_log"
Path
Position
/var/log/nginx/access.log
50584
/var/log/nginx/access.log.1
164053
/var/log/nginx/access.log.10.gz
34593
/var/log/nginx/access.log.11.gz
6346
/var/log/nginx/access.log.12.gz
11102
/var/log/nginx/access.log.13.gz
6643
/var/log/nginx/access.log.14.gz
16318
/var/log/nginx/access.log.2.gz
12631

How it Works?



Sys/App Logs

Application and system generated Logs

Promtail

Ships Logs to Loki

Discover Targets
Attaches Labels
Pushes To Loki

Loki Storage

Log streams by ID & labels

Compressed chunks

Index Stores streams/labels linking to chunk

Visualization

Create Visualizations

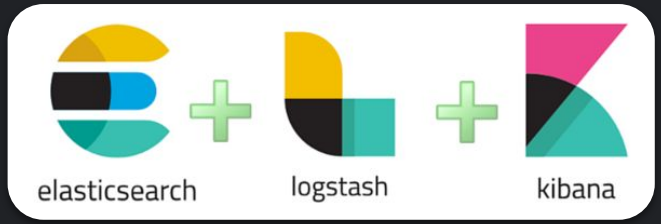
Transform Data

Create and manage Alerts

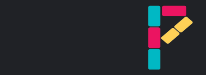
Benefits

- REST API
- Low Resource Footprint
- Near Real Time Search
- Perfect For K8s
- Fast Data Ingestion
- Why not SQL?  Promscale

Alternatives



Grafana



- Open-source visualization and Analytics software
- Query, Visualize, Alert On, Explore metrics - no matter where they are stored
- In Beautiful English, it provides you tools to turn your Time-series Database into beautiful graphs and visualization

Export Metrics & Logs

Annotations

Dashboard Variables

VC Config

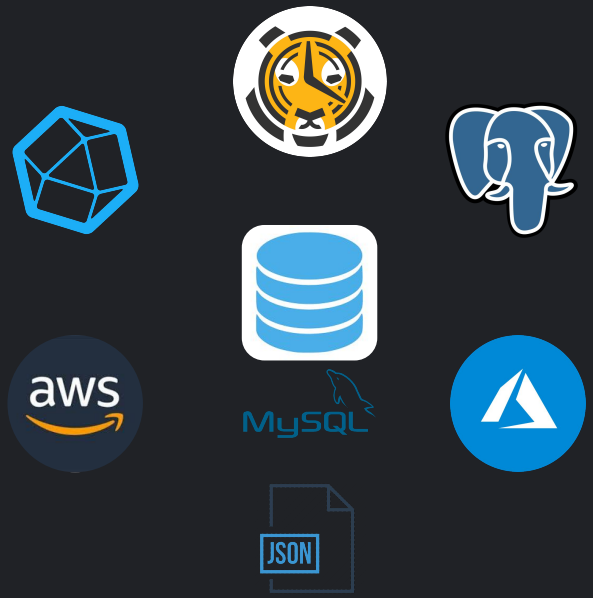
Manage Alerts

Import Dashboards & Plugins

Authentication & Permissions

Provisioning

How it Works



Data Sources

Grafana

API/Query

Dashboards/Alerts

Benefits

- Open-Source
- On Demand Dynamic Dashboards from Data Sources
- Customizable/interactive
- Real-Time Monitoring & Alerts
- Authentication & User Management
- Plugins

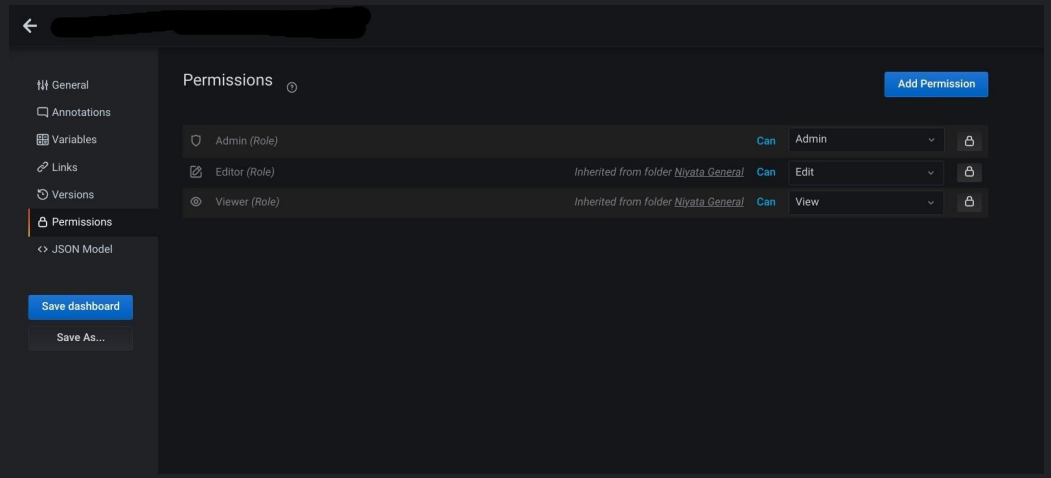
Alternatives

Problems Addressed & Resolved

Monitor Resource Usage

Centralized Control for monitoring events

Problems Addressed & Resolved



Monitor Resource Usage

Centralized Control for monitoring events

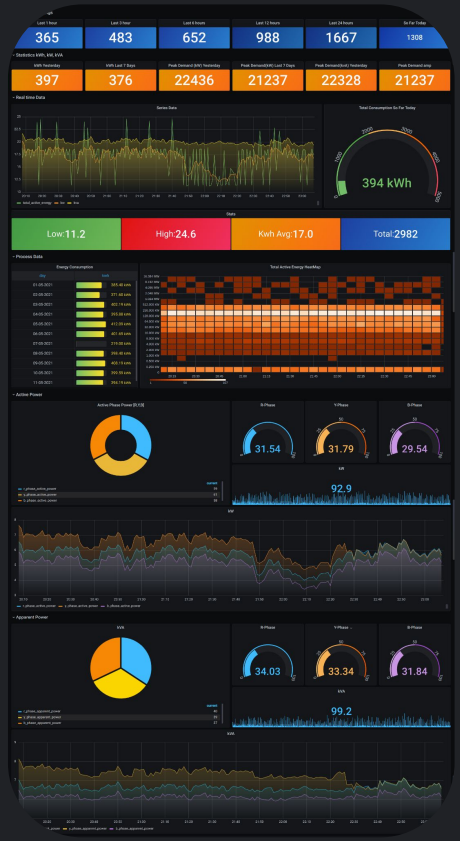
Manage Permissions

Monitor Kafka and Alert

Problems Addressed & Resolved

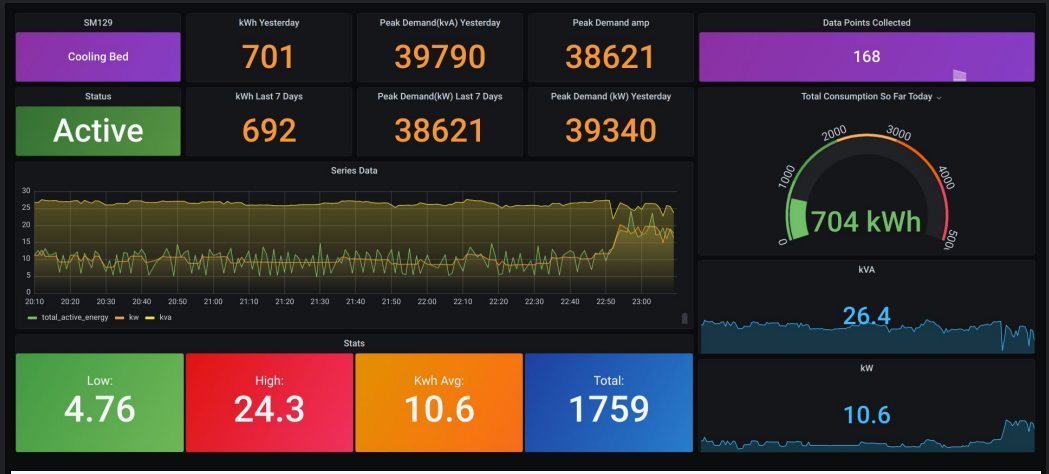
- Explore & Analyse logs
- Data inserted into database
- Correlate metrics
- Source of errors
- Resolve in minutes rather than hours/days

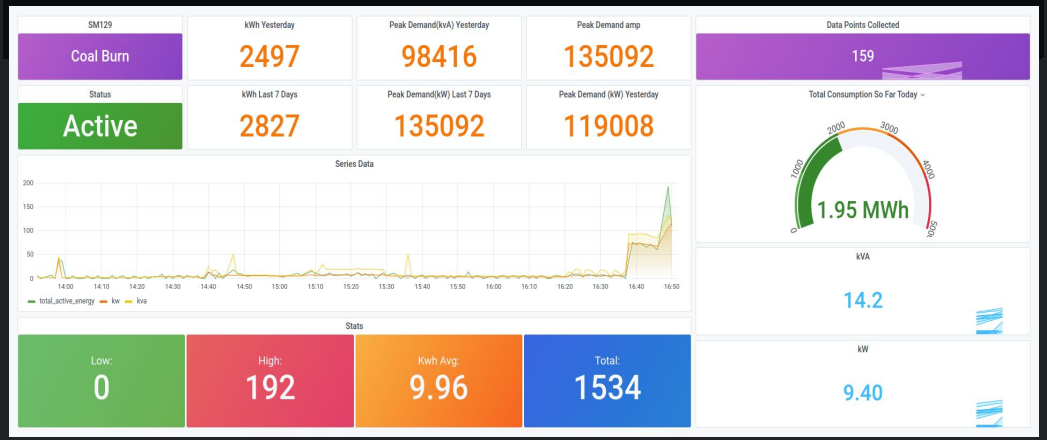
Didn’t stop us from exploring use cases



- Mimic the live dashboard for IoT
- Run a playlist of live dashboard in TV mode
- Admin and Financial dashboards
- Postgres, Redis and Nginx metrics

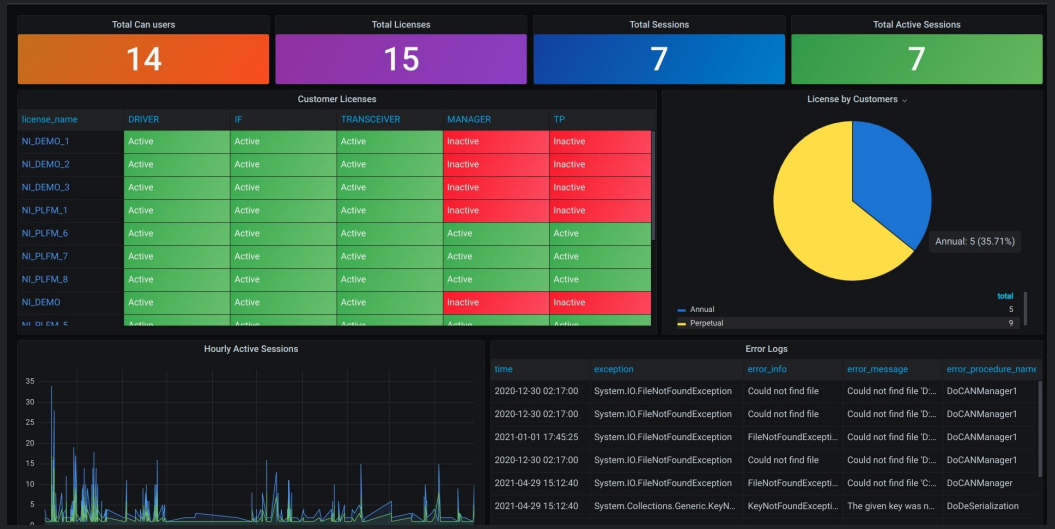
Didn't stop us from exploring use cases





- Mimic the live dashboard for IoT
- Run a playlist of live dashboard in TV mode
- Admin and Financial dashboards
- Postgres, Redis and Nginx metrics

Didn't stop us from exploring use cases



- Mimic the live dashboard for IoT
- Run a playlist of live dashboard in TV mode
- Admin and Financial dashboards
- Postgres, Redis and Nginx metrics

Didn’t stop us from exploring use cases

- Mimic the live dashboard for IoT
- Run a playlist of live dashboard in TV mode
- Admin and Financial dashboards
- Postgres, Redis and Nginx metrics

Why we need these?

- You can only improve something when you can measure it
- Faster MTTR by quickly narrowing down the issue
- Centralized visualization of your system, logs and application data
- On demand Analytics Dashboards with the Power of SQL and Grafana
- Audit Trail ~ The Journey of data at your fingertips

Continuous Monitoring

- ✓ Improved Quality
- ✓ Faster Response
- ✓ MTTR
- ✓ Shift Left
- ✓ Incident Management
- ✓ Improved UX
- ✓ You've Got Data
- ✓ Analytics and Decision
- ✓ Derive Business value


Surrounded By data, ~Jay Baer
Starved of Insights
Torture the data and it will confess to anything ~Ronal.H.Caose
No great marketing decisions have ever been made on qualitative data ~Ronal.H.Caose
With data collections, 'the sooner the better' is always the best answer ~Marissa Mayer
A Tool to enhance intuition
We are entering a new world in which data may be more important than software ~Tim O'Reilly
Information is the oil of 21st century and analytics is the combustion engine ~ Mr.Sondergaard
Its capital mistake to theorize before one has data ~Conan Doyle
There were 5 exabytes if information created between dawn of civilization through 2003, but that much information is now created in every 2 days ~Eric Schmidt
Data beats emotions ~Sean Rad
No matter where you are headed, your journey starts with great data
THANK YOU
Every company has big data in its future and every company will eventually be in data business ~Thomas H
The Goal is turn data into information and information into insight ~Carly Fiorina
Where there is data smoke, there is business fire ~ Thomas Redman
Above all else, show the data
And Don't just show data
Visualize It
Data are summaries of thousands of stories-tell a few of those stories to help make the data meaningful ~Dan Heath
You can have data without information, but you cannot have information without data ~Daniel Keys Moran
Don't just keep data
Analyze It
No great marketing decisions have ever been made on qualitative data ~John Sculley
If we have data, let's look at data. If all we have are opinions, let's go with mine ~Jim Barksdate
Don't just keep analysing
Derive Insights