NetMeta

A scalable network observability toolkit optimized for performance

Tim Windelschmidt - 20.11.2023

Hi 👋

- Tim Windelschmidt
- Software Engineer at Monogon SE
- Co-Maintainer of NetMeta (https://github.com/monogon-dev/NetMeta)
- How you can reach me:
  - Github, Telegram, IRC: fionera
  - Matrix: @fionera:matrix.org

What is NetMeta?

And why should I care?

NetMeta is a scalable network observability toolkit optimized for performance

What does this mean?

- Sub-second resolution
- Efficient storage
- Blazingly fast queries (thanks to Clickhouse)
- Easy and simple usage
- Fully open-source and permissively licensed (Apache-2.0)

Why another flow-aggregator?

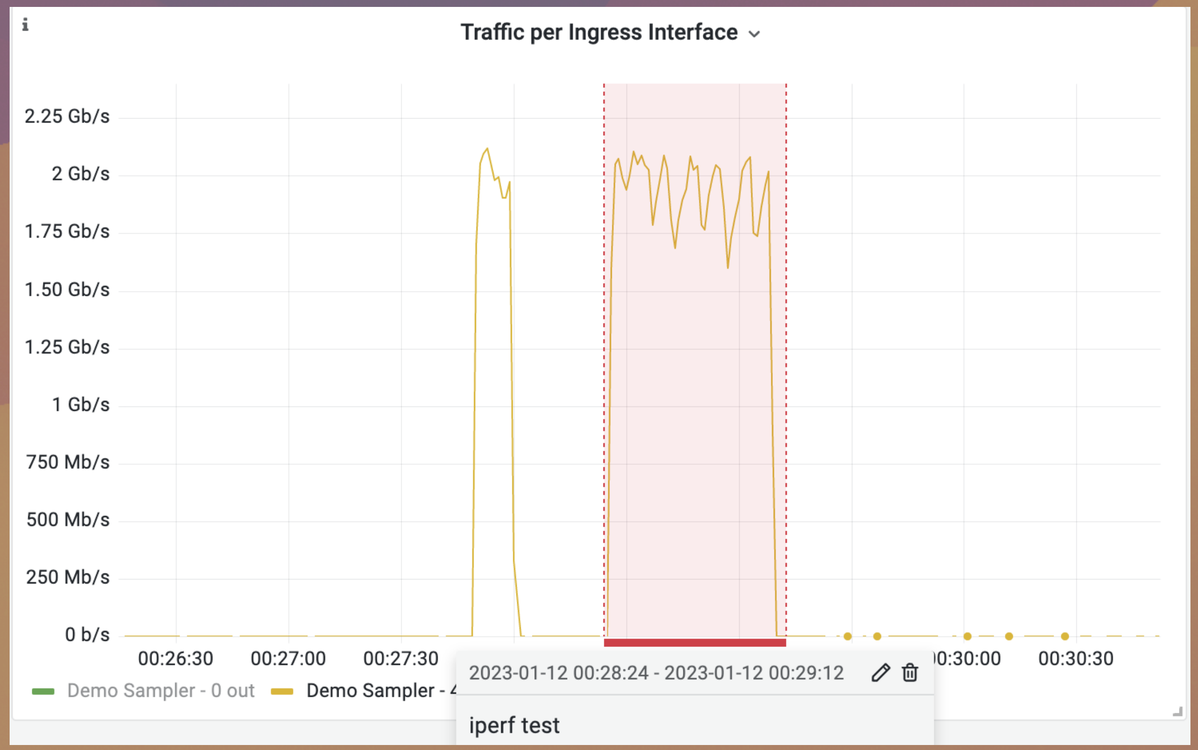
- Previous solutions got abandoned
- Didn’t had the same performance / granularity
- were just too expensive / not reachable

Alternatives

- Elastiflow / Elastiflow2
  - Archived / Closed source
- Kentik (kentik.com)
  - Closed source
- Akvorado (github.com/akvorado/akvorado)
  - AGPLv3
  - No support contracts possible

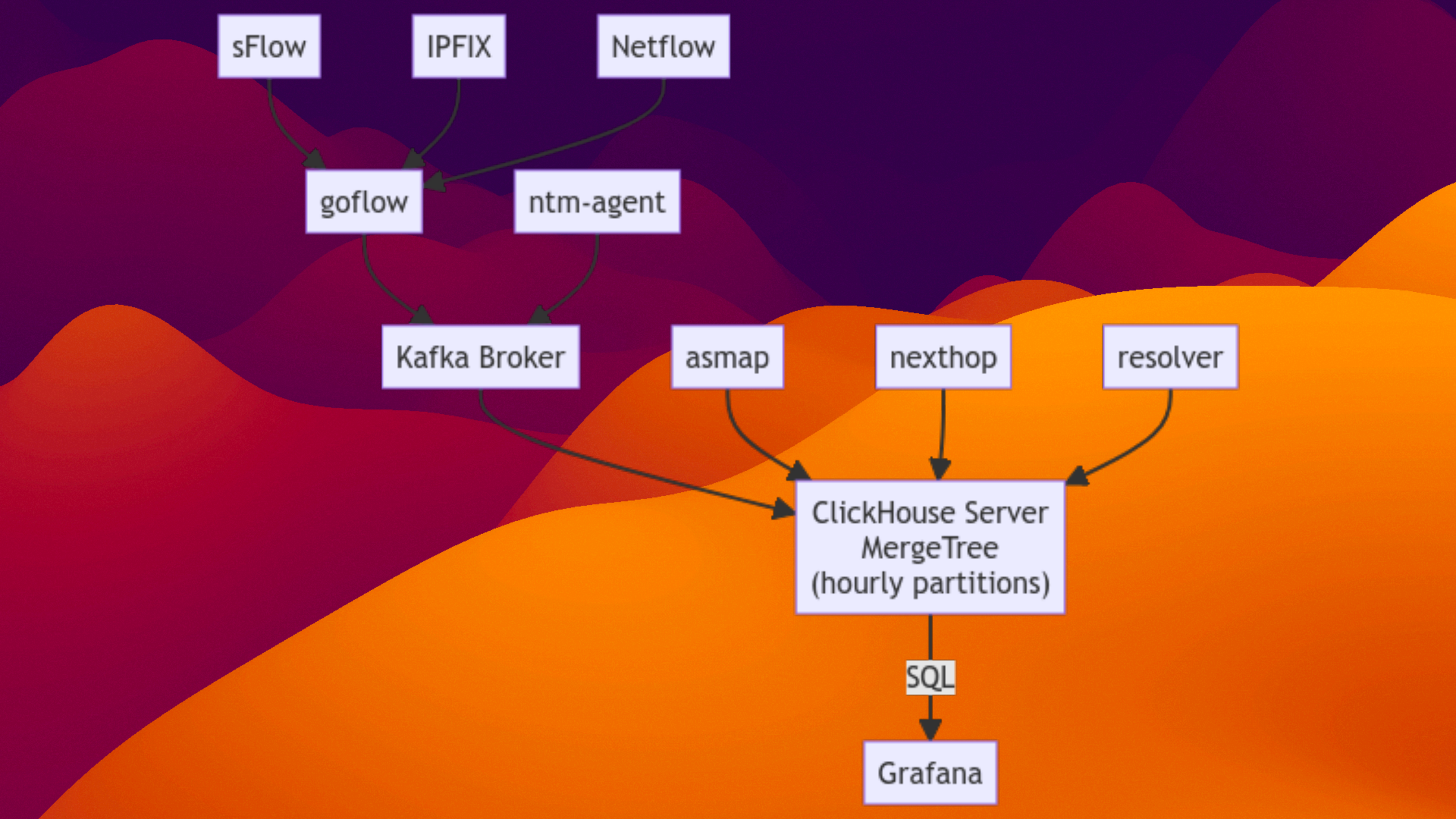
3rd Party integrations

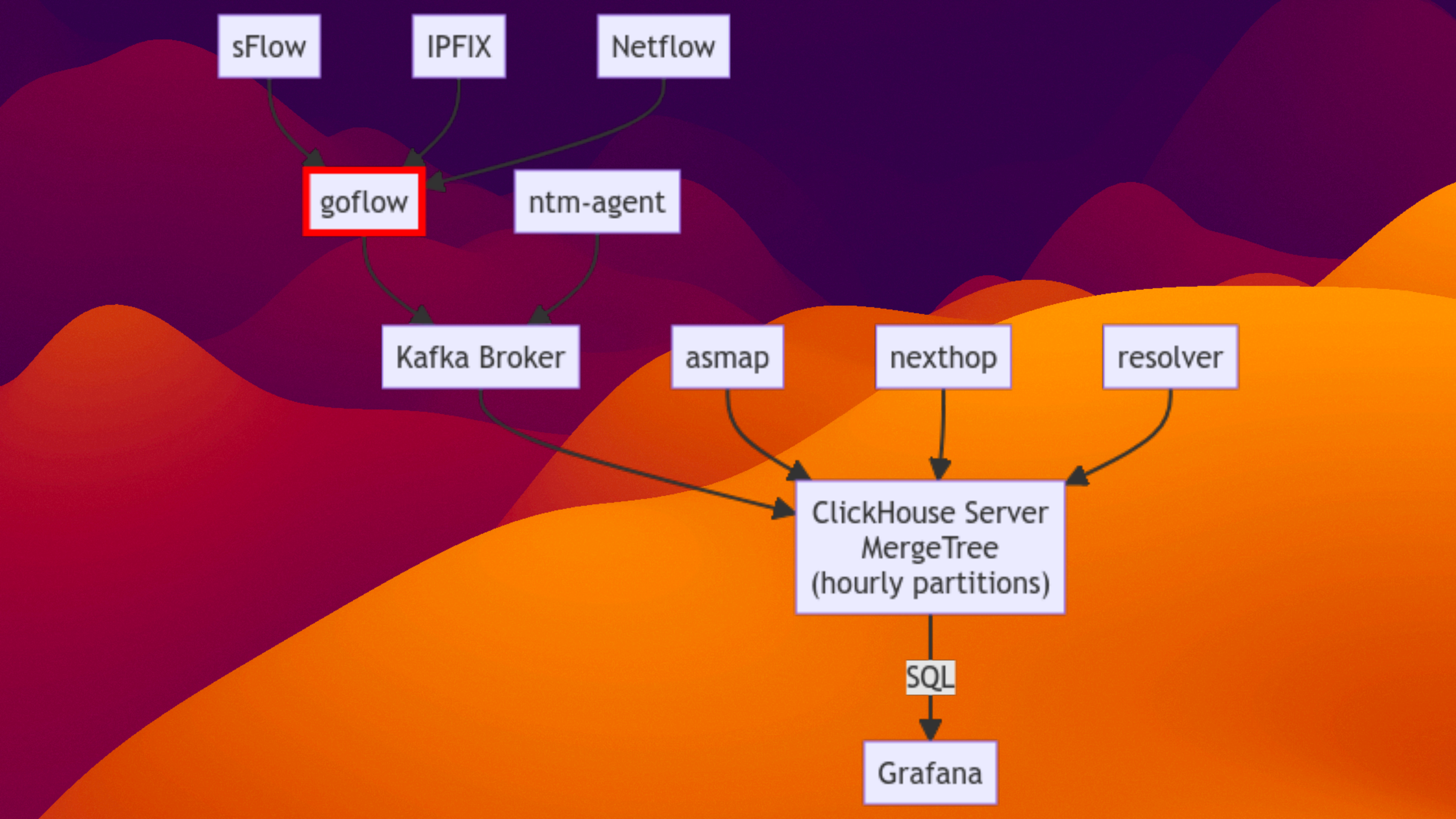
- Basic Grafana dashboards
  - Every annotation provider should just work ™
- FastNetMon attack notifications
- Raw-SQL on underlying Clickhouse DB
- Custom ingest via Kafka and Protobuf



Dataflow

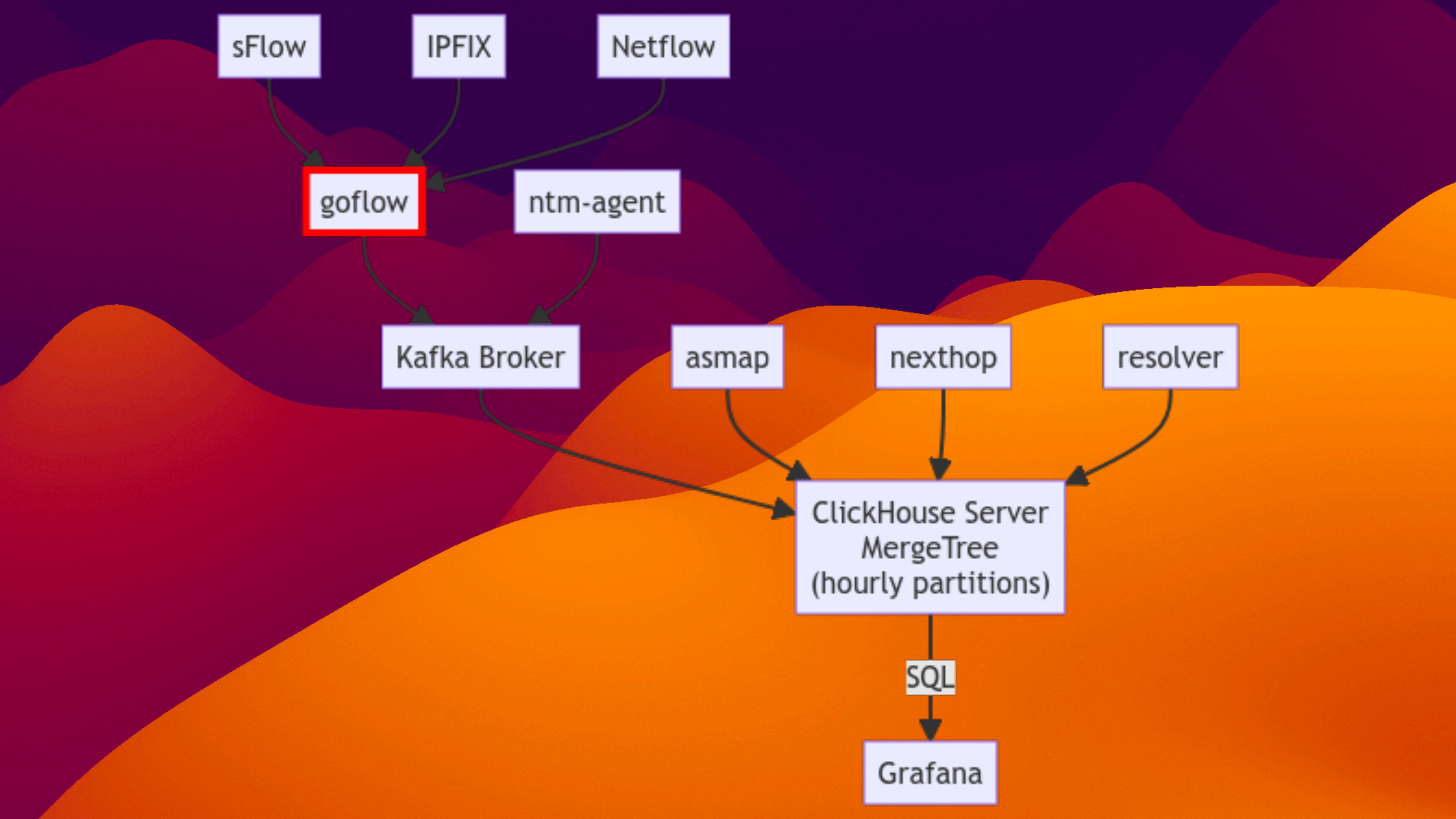
📦 goes brrrt

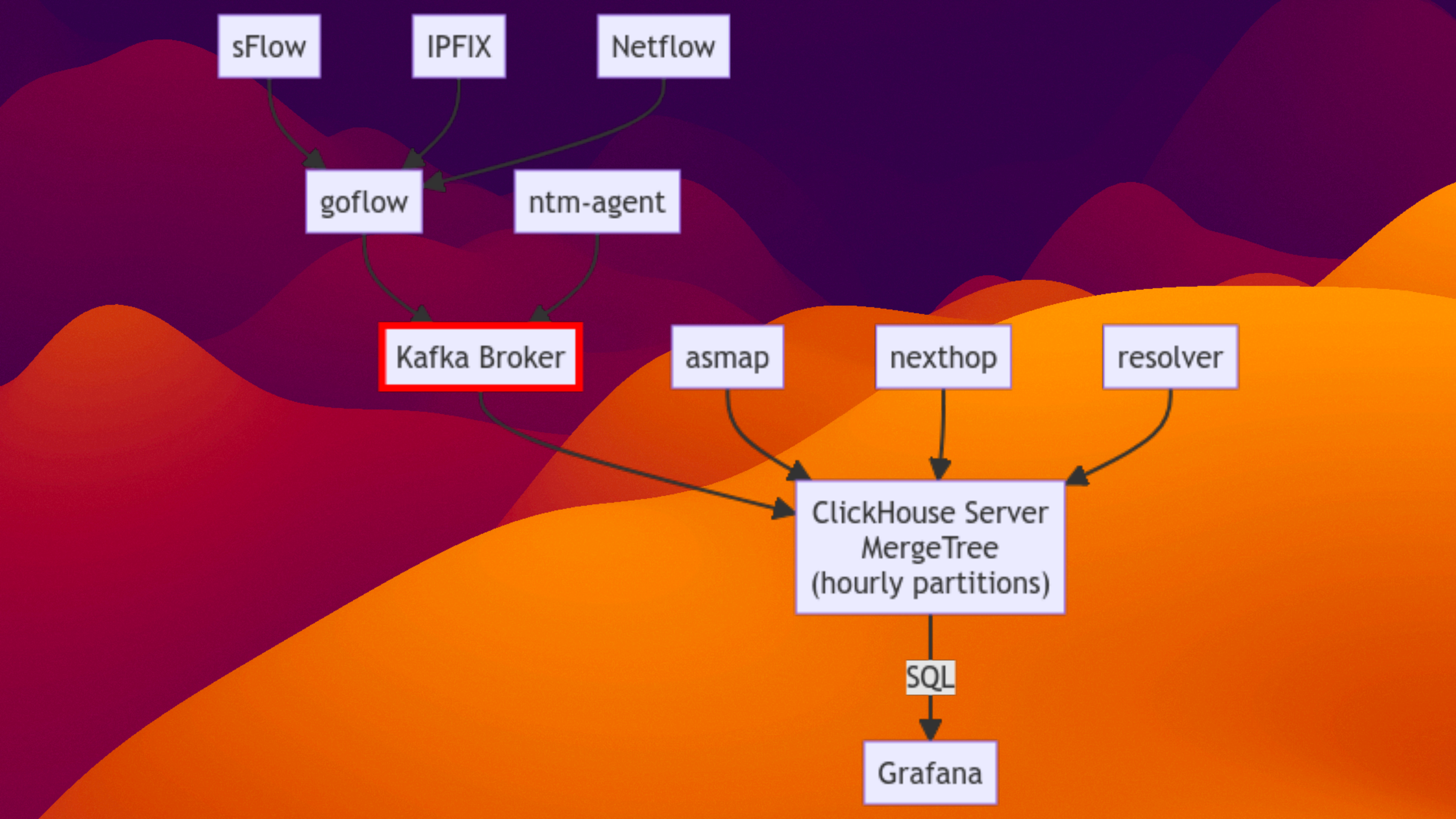

sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana

Where and how to collect samples

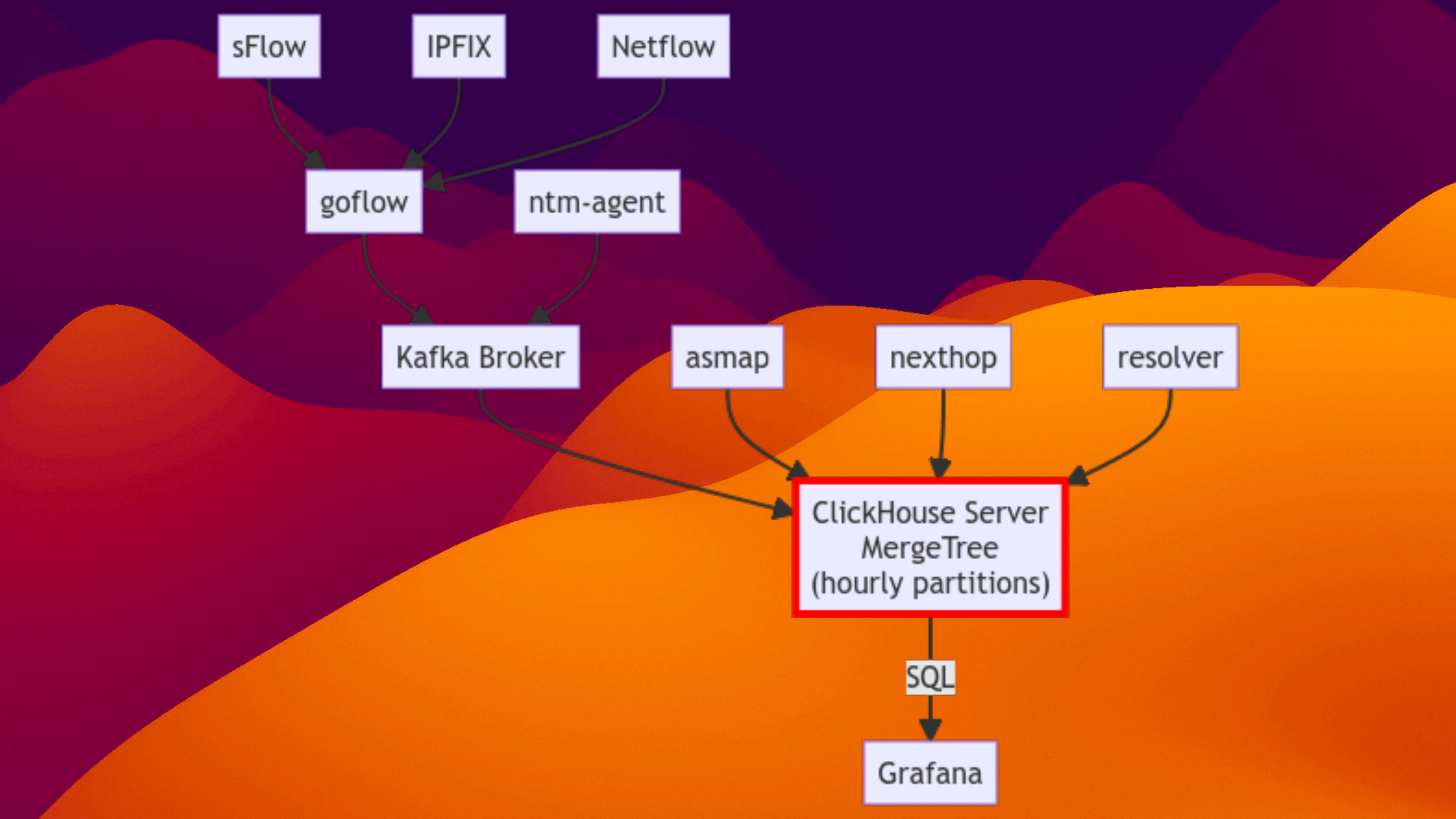
- goflow/goflow2 (https://github.com/netsampler/goflow2)
  - Open Source collector for sFlow/IPFIX/NetFlow
- Portmirror
  - Custom collector for fibertap/portmirror environments
- Agent
  - NetMeta Agent based on “tc” is planned…


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana

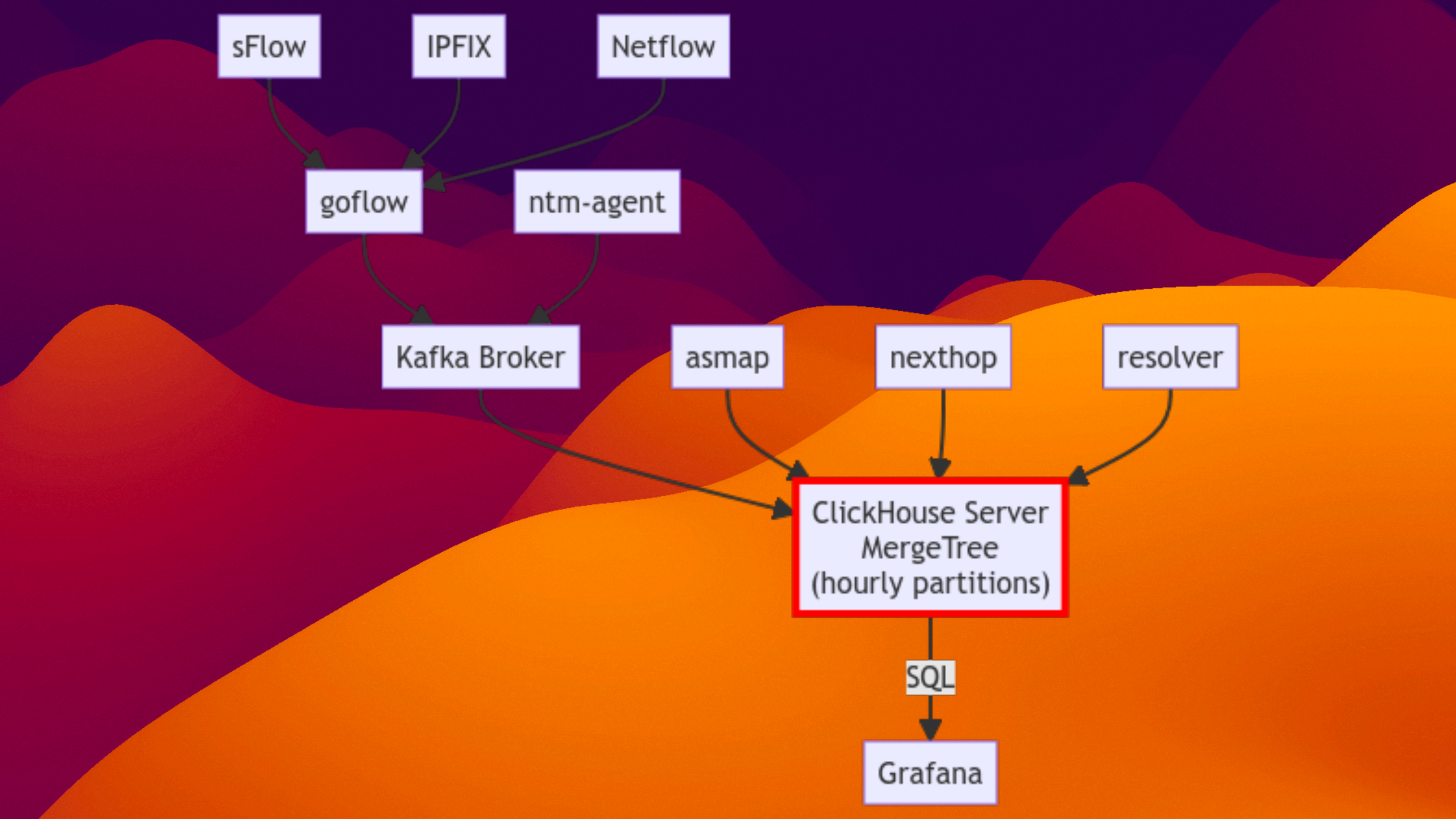
How to queue samples

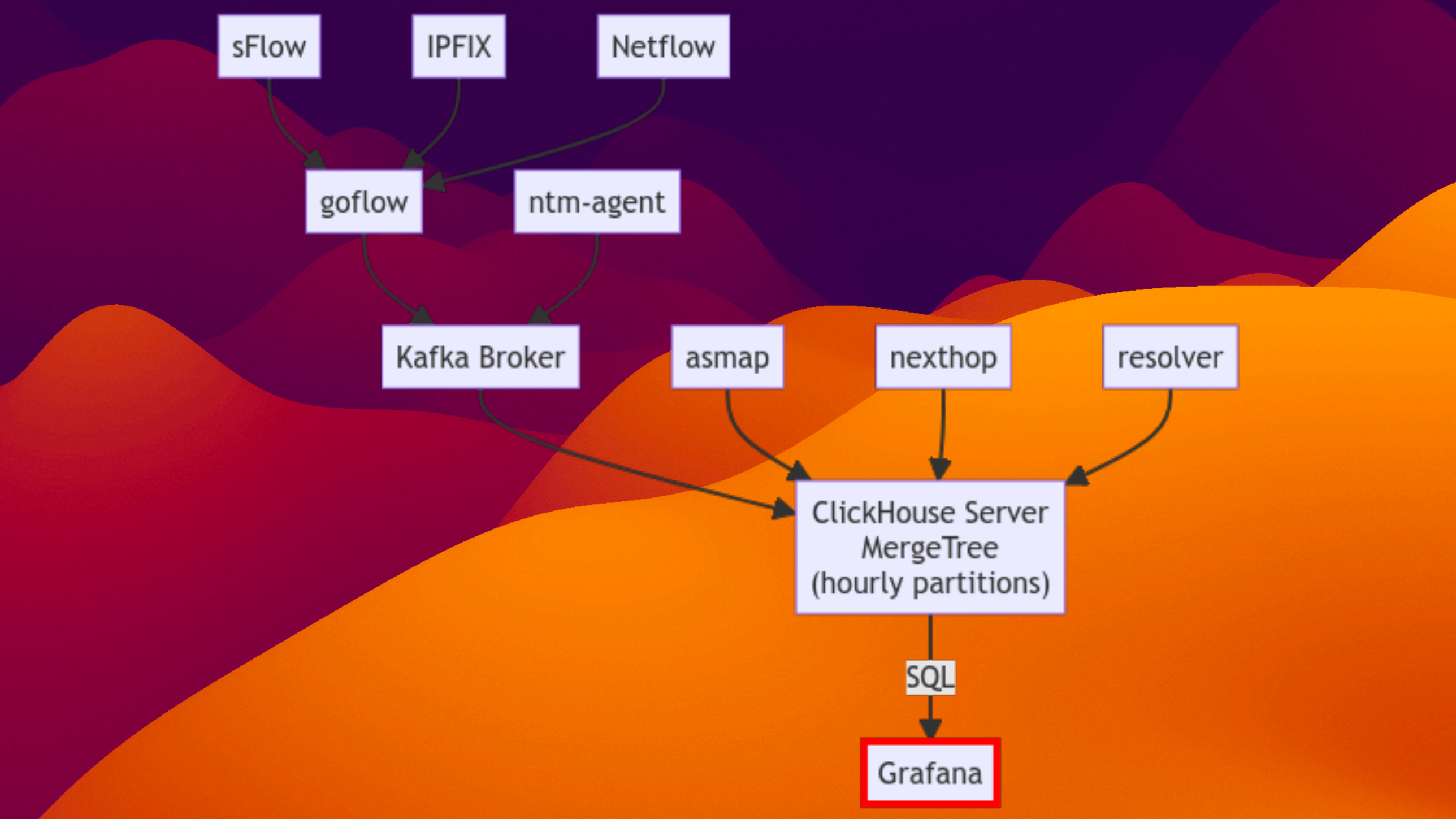
- Apache Kafka as message queue
  - Open-Source
  - Scales with easy to allow distributed deployments
  - Allows multiple consumers to receive the same message
- Managed via Strimzi-Operator
  - Allows easy management via CRDs


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana

Storing and querying of samples

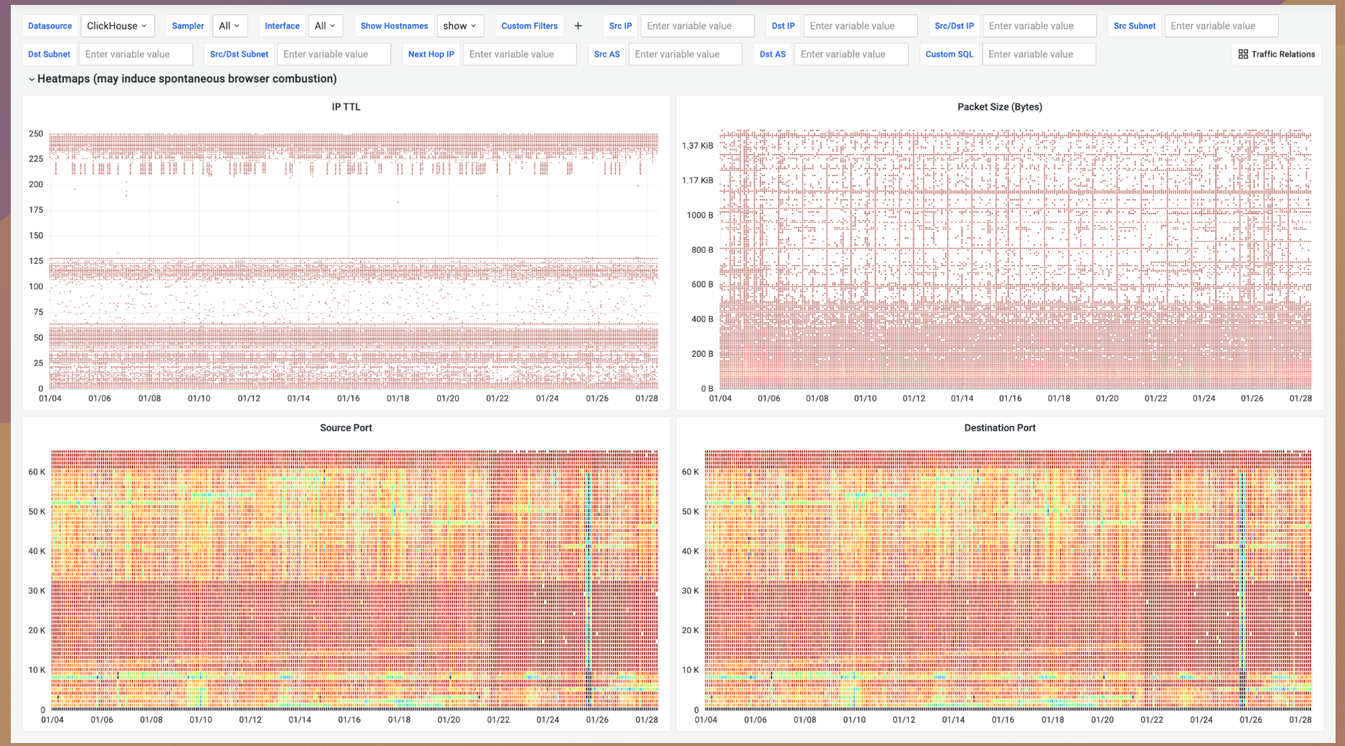
- Why Clickhouse?
  - Open-Source
  - Very *very* Fast
  - Supports the weirdest features
- Example Deployments
  - 423.6GiB - 17.4B Rows (Intel Xeon E3-1270 v5)
  - 30GiB - 700M Rows (7 Day retention for 60Gbit)


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana


sFlow
IPFIX
Netflow
goflow
ntm-agent
Kafka Broker
asmap
nexthop
resolver
ClickHouse Server
MergeTree
(hourly partitions)
SQL
Grafana

Visualization

- Grafana as base
- Known tooling
- Easy to extend
- Panels generated in CUE



Deployment

Can I use winget? 🤔

Configuration

- Based on CUE, …
  - Grafana Dashboards
  - K8s Manifests
- …, and Bazel
  - Tooling/Containers
- Tables generated based on Protobuf Files

Deployment

- K3s for Single-Node Environments
- Multi-Node possible but no official way yet
- Work on native NixOS deployment is being done

Roadmap

What else to come?

Roadmap

- NetMeta Agent for local collection
- Official Multi-node deployments
- AS Paths via BMP
- Reverse-DNS for IPs
- GeoIP Lookups/Map
- <your feature request here>

That’s it!

Thanks for your time and have a nice event 😊

P.S.: Try out the demo instance at https://netmeta.demo.monogon.dev/