PromCon
North America 2021

pktvisor.dev

Deep network traffic observability with pktvisor and Prometheus

Shannon Weyrick ◦ VP Research ◦ Office of CTO

sweyrick@ns1.com

The Big Picture

pktvisor and **Orb** supplement modern observability stacks by facilitating **edge network observability**

The projects are **free** and **open source** backed by **NS1.**

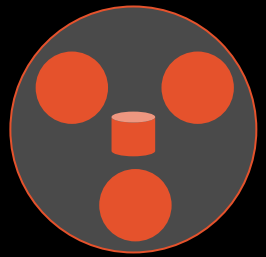
The ultimate goal is **dynamic orchestration** of **business intelligence** at the **edge**

Shannon Weyrick · sweyrick@ns1.com

1. Deep Network Observability

2.  pktvisor 

3.  pktvisor + Prometheus 

4.  Orb 

Deep Network Observability

Deep Network Observability

- Unwrapping and inspecting network traffic and activity can provide insight useful for **operations, debugging** and **security**
- But **analysis** and **collection** of traffic across a distributed and often ephemeral set of end points is **hard**
- How do we orchestrate and **extract insights** from these flows?

Shannon Weyrick · sweyrick@ns1.com

Context From NS1.

- At **NS1.** we run Managed DNS and other critical network services across many globe spanning networks
- We need to **tune** our global anycast networks for the **best delivery time**
- We are often subject to **malicious traffic** which we need to understand to be able to **protect against**
- We need to **debug individual delivery** nodes at high resolution
- We need a **global view** of all nodes and to drill in to **different dimensions of network traffic data** over time

Shannon Weyrick · sweyrick@ns1.com

What Do We Want To Know?

- What are the **counters**, **rates** and **frequent items** across common network traffic dimensions?
- How many **unique** IP addresses and query names (**cardinality**) are there?
- What are the important **quantiles** of transaction timings? What's the **histogram** of response payloads?
- What is the **amplification factor** from Query to Response size?
- What is **still querying** that DNS record that was **deleted**?
- From what **ASN** and **Geo** regions is traffic coming from?
- Is this traffic spike **malicious** or **legitimate**? Is this a random label attack? Is it widely distributed? IPv4? UDP? Against what zone?

Shannon Weyrick · sweyrick@ns1.com

pktvisor

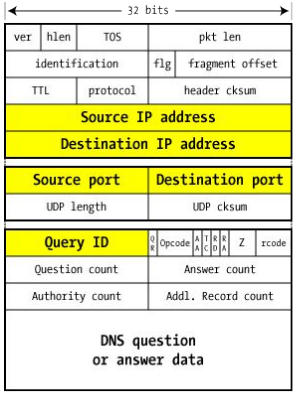
“packet visor”

The Big Picture: pktvisor

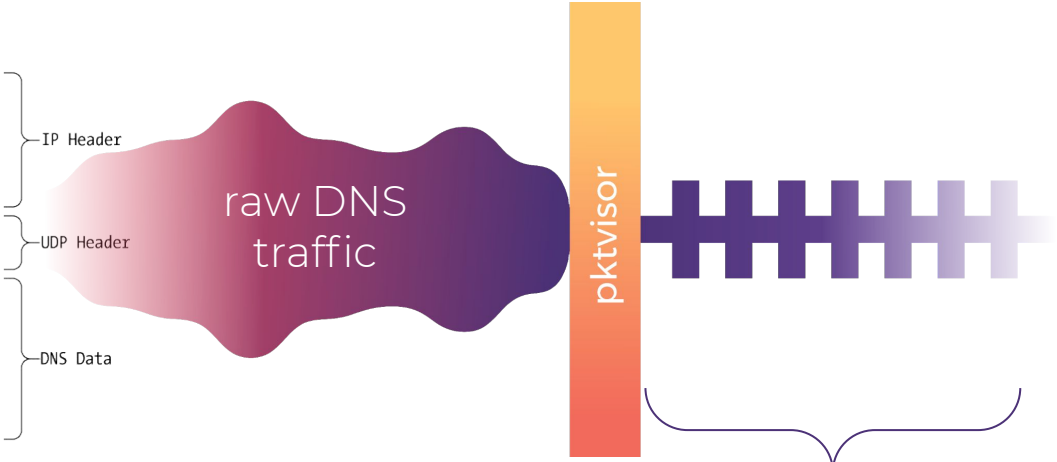
- **Free** and **open source** observability **agent** backed by NS1
- Cut its teeth **observing critical infrastructure** for the past 7 years
- Currently packet capture focused, more **input sources** on tap
- Goals
  - Support **pluggable input sources** and **analyzers** (contributors!)
  - Drive observability via **dynamic policies** over **REST API**
  - Support **modern** observability stacks

Shannon Weyrick · sweyrick@ns1.com

pktvisor.



DNS packet on the wire



1 minute summaries

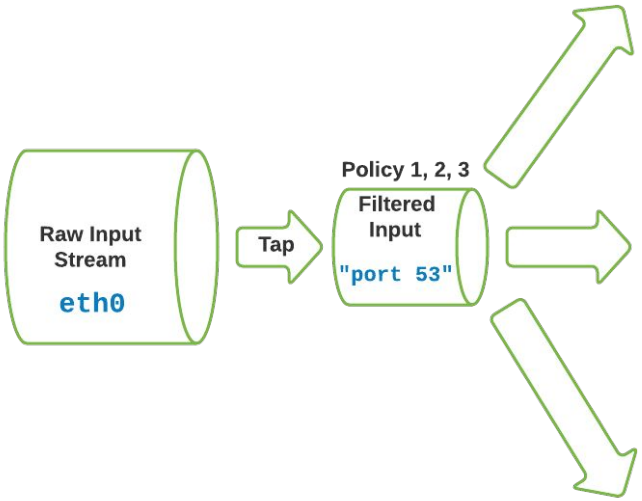
L7 Dissection

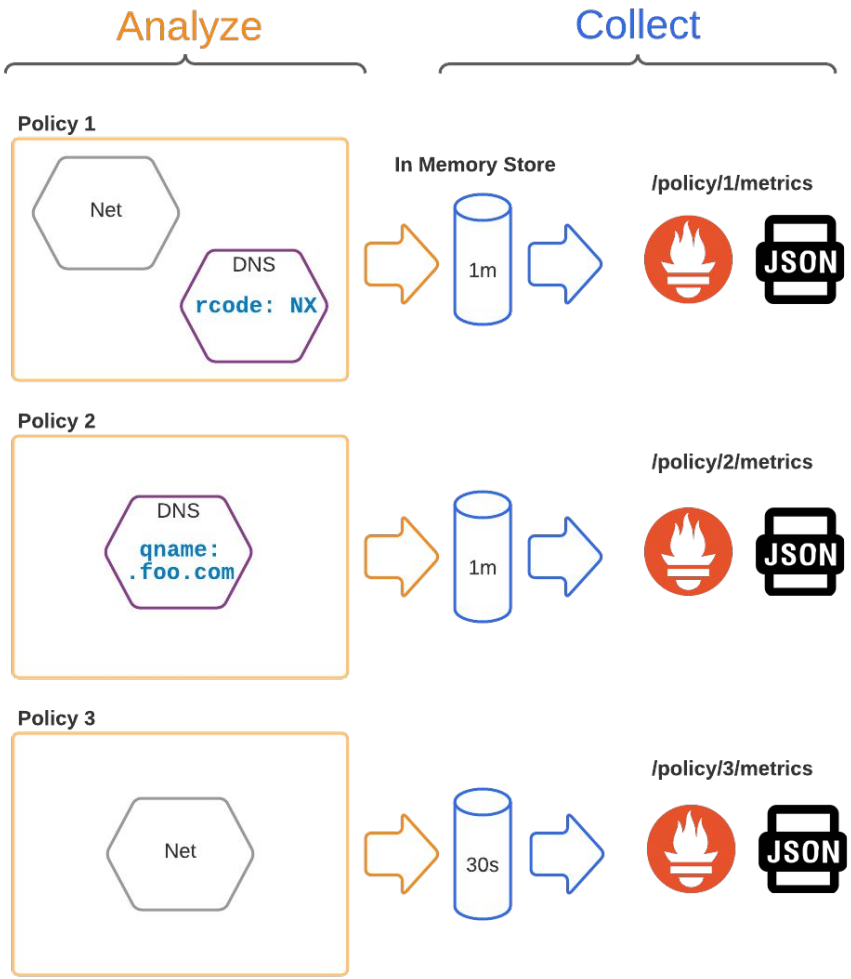
```
Top Queries
Top Query Types
Top Result Codes
Rate Percentiles
Top Sources
Counters
...
```

flow

Shannon Weyrick · sweyrick@ns1.com

pktvisor.





Shannon Weyrick · sweyrick@ns1.com

```
sweyrick@blesk:~$ curl -w "\n" -s localhost:10853/api/v1/policies/default/metrics/bu
cket/1 | jq . -C | head -39
{
  "default-default_dns": {
    "dns": {
      "cardinality": {
        "qname": 40
      },
      "period": {
        "length": 60,
        "start_ts": 1633445201
      },
      "rates": {
        "total": {
          "p50": 0,
          "p90": 14,
          "p95": 24,
          "p99": 52
        }
      },
      "top_nxdomain": [
        {
          "estimate": 1,
          "name": "ns-1022.awsdns-63.ne"
        },
        {
          "estimate": 1,
          "name": "lb._dns-sd._udp.0.1.168.192.in-addr.arpa"
        }
      ],
      "top_qname2": [
        {
          "estimate": 20,
          "name": ".malwarebytes.com"
        },
        {
          "estimate": 20,
          "name": ".apple.com"
        },
        {
          "estimate": 18,
sweyrick@blesk:~$ curl -w "\n" -s localhost:10853/api/v1/policies/default/metrics/bu
cket/1 | jq . -C | head -39
```

```
sweyrick@blesk:~$ curl -s localhost:10853/api/v1/policies/default/metrics/prometheus
| highlight -O xterm256 -S bash | head -22
# HELP packets_rates_pps_in Rate of ingress in packets per second
# TYPE packets_rates_pps_in summary
packets_rates_pps_in{instance="blesk",module="default-default_net",policy="default",q
uantile="0.5"} 4
packets_rates_pps_in{instance="blesk",module="default-default_net",policy="default",q
uantile="0.9"} 13
packets_rates_pps_in{instance="blesk",module="default-default_net",policy="default",q
uantile="0.95"} 14
packets_rates_pps_in{instance="blesk",module="default-default_net",policy="default",q
uantile="0.99"} 26
packets_rates_pps_in_sum{instance="blesk",module="default-default_net",policy="defaul
t"} 26
packets_rates_pps_in_count{instance="blesk",module="default-default_net",policy="defa
ult"} 59
# HELP packets_rates_pps_out Rate of egress in packets per second
# TYPE packets_rates_pps_out summary
packets_rates_pps_out{instance="blesk",module="default-default_net",policy="default",
quantile="0.5"} 3
packets_rates_pps_out{instance="blesk",module="default-default_net",policy="default",
quantile="0.9"} 16
packets_rates_pps_out{instance="blesk",module="default-default_net",policy="default",
quantile="0.95"} 22
packets_rates_pps_out{instance="blesk",module="default-default_net",policy="default",
quantile="0.99"} 31
packets_rates_pps_out_sum{instance="blesk",module="default-default_net",policy="defau
lt"} 31
packets_rates_pps_out_count{instance="blesk",module="default-default_net",policy="def
ault"} 59
# HELP packets_rates_pps_total Rate of all packets (combined ingress and egress) in p
ackets per second
# TYPE packets_rates_pps_total summary
packets_rates_pps_total{instance="blesk",module="default-default_net",policy="default
",quantile="0.5"} 6
packets_rates_pps_total{instance="blesk",module="default-default_net",policy="default
",quantile="0.9"} 29
packets_rates_pps_total{instance="blesk",module="default-default_net",policy="default
",quantile="0.95"} 34
packets_rates_pps_total{instance="blesk",module="default-default_net",policy="default
",quantile="0.99"} 57
sweyrick@blesk:~$ curl -s localhost:10853/api/v1/policies/default/metrics/prometheus
| highlight -O xterm256 -S bash | head -22
```

```
pktvisor-cli (client: 3.3.0-develop | server: 3.3.0-develop)
Pkts  3249 | UDP 1126 (34.7%) | TCP 2073 (63.8%) | Other 50 (1.5%) | IPv4 3196 (98.4%) | IPv6 3 (0.1%) | In 1629 (50.9%) | Out 1570 (49.1%) | Deep Samples 3249 (100.0%)
Pkt Rates Total 5/s 6/20/24/114 pps | In 3/s 3/9/12/59 pps | Out 2/s 3/10/14/61 pps | IP Card. In: 272 | Out: 284 | TCP Errors 0 | OS Drops 0 | IF Drops 0

DNS Wire Pkts 1112 (34.2%) | Rates Total 0/s 0/0/0/0 | UDP 1112 (100.0%) | TCP 0 (0.0%) | IPv4 1112 (100.0%) | IPv6 0 (0.0%) | Query 566 (50.9%) | Response 546 (49.1%)
DNS Xacts 546 | Timed Out 20 | In 176 (32.2%) | Out 370 (67.8%) | In 30.5/1627.4/1815.9/3220.9 ms | Out 21.7/82.4/94.1/260.3 ms | Qname Card. 252
DNS NOERROR 542 (99.3%) | SRVFAIL 0 (0.0%) | NXDOMAIN 4 (0.7%) | REFUSED 0 (0.0%) | Time Window 5:43PM to 5:48PM, Period 297s
```

```
Top QName 2
.amazon.com                 118 (10.6%)
.cloudfront.net              68 ( 6.1%)
.roku.com                    56 ( 5.0%)
.co.uk                           48
.google.com                      40
.amazonaws.com                   39
.awsstatic.com                   22
```

```
Top QName 3
.logs.roku.com               56 ( 5.0%)
.us-east-1.amazonaws.com     27 ( 2.4%)
.dscg.akamaiedge.net         16 ( 1.4%)
www.shopbop.com                  13
.shortbread.aws.dev              12
.amazon-blogs.psdops.com         12
www.imdb.com                     10
```

```
Top NX
lb._dns-sd._udp.0.1.168.192.in-addr.arpa 2
rns-779.awsdns-33.net             1 ( 0.2%)
us-east-1.console.aws.amazon.com 1 ( 0.2%)
```

```
Slow In
p3epspumangb5dvijf52er7wdi.appsync-api.us-
www.imdb.com                      3 ( 0.5%)
d23tl967axkois.cloudfront.net     2 ( 0.4%)
player.live-video.net                     2
sparrow.wondershare.com                   2
d2in0p32vp1pij.cloudfront.net             2
blog.aboutamazon.com                      2
```

```
Top QTypes
A                        1060 (95.3%)
HTTPS                      38 ( 3.4%)
AAAA                       10 ( 0.9%)
PTR                             4
```

```
Top RCodes
NOERROR                   542 (99.3%)
NXDOMAIN                    4 ( 0.7%)
```

```
Top SRVFAILS
```

```
Slow Out
ns10.tmobileus.net                3 ( 0.5%)
gtm-cn-v64163wlk09.gtm-a2b4.com   2 ( 0.4%)
cache.prod.amazon-blogs.psdops.com 2 ( 0.4
prod.log.shortbread.aws.dev               2
www.shopbop.com                           2
www.zappos.com                            2
filmstock-api-eus.wondershare.cc          2
```

```
Top REFUSED
```

```
IPv4
192.168.0.217            2132 (65.6%)
34.102.140.197            242 ( 7.4%)
34.122.121.32              35 ( 1.1%)
192.43.172.30                      20
192.42.93.30                       18
172.253.122.188                    16
208.78.70.31                       14
```

```
IPv6
ff02::1:2                   3 ( 0.1%)
```

```
Top DNS UDP Ports
10139                     4 ( 0.4%)
7096                      4 ( 0.4%)
28397                     4 ( 0.4%)
13766                             4
10702                             2
37127                             2
14127                             2
```

```
Top GeoLoc
Unknown                  2146 (66.1%)
NA/United States          931 (28.7%)
NA/United States/CA/Mountain View 32 ( 1.0
EU                                   14
NA/United States/CA/San Jose          9
EU/Ireland/L/Dublin                   8
AS/China                              6
```

```
Top ASN
Unknown                  2150 (66.2%)
16509/AMAZON-02           361 (11.1%)
15169/GOOGLE              325 (10.0%)
397213/ULTRADNS                    47
10515/CLT-NIC                      36
397215/ULTRADNS                    35
33517/DYNDNS                       32
```

Command Line UI

Easy Docker Install

ns1labs/pktvisor

PromCon
North America 2021

pull the image

```
root@host:~$ docker pull ns1labs/pktvisor
```

start the agent with a default collection policy

```
root@host:~$ docker run --net=host -d ns1labs/pktvisor pktvisord --prometheus eth0
```

scrape prometheus metrics

```
root@host:~$ curl localhost:10853/metrics
```

run the command line UI (ctrl-c to quit)

```
root@host:~$ docker run -it --rm --net=host ns1labs/pktvisor pktvisor-cli
```


Shannon Weyrick · sweyrick@ns1.com

pktvisor.

GitHub

https://pktvisor.dev

- FOSS
- Contributors welcome
- Please star!

ns1labs / pktvisor Public

Unwatch 42 | Unstar 357 | Fork 25

Code | Issues 28 | Pull requests 1 | Discussions | Actions | Projects 2 | Wiki | Security | Insights | Settings

develop | 5 branches | 10 tags | Go to file | Add file | Code

weyrick feature/cli refactor (#120) ... cd0fed1 10 days ago 281 commits

.github/workflows	no automatic build for master	5 months ago
3rd	switch random number generators used by sampling (#110)	3 months ago
RFCs	require a new key 'kind' to specify policy type, in preparation for f...	13 days ago
appimage	require binary arg to appimage to be consistent with docker image.	6 months ago
centralized_collection	run-pktvisor.sh IFS fix for args with spaces (#111)	2 months ago
cmake	feature/deps (#36)	7 months ago
cmd	require a new key 'kind' to specify policy type, in preparation for f...	13 days ago
docker	require binary arg to appimage to be consistent with docker image.	6 months ago
docs	rfcs	5 months ago
golang	feature/cli refactor (#120)	10 days ago
integration_tests	implement #78 dns filters (#105)	3 months ago
src	require a new key 'kind' to specify policy type, in preparation for f...	13 days ago
.clang-format	import	2 years ago
.dockerignore	issue #94 add TLS support to web server	4 months ago
.gitignore	Merge branch 'release' into feature/3.2.1-merge	4 months ago
.gitmodules	Modularize #23 (#27)	7 months ago
CMakeLists.txt	merge 3.2.0 release, go 3.3.0-develop	5 months ago
CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md	last month
CONTRIBUTING.md	Improve READMEs, other minor improvements (#25)	9 months ago

About

pktvisor is an observability agent that summarizes deep network data streams in real time, enabling on-node and centralized data visibility and analysis

pktvisor.dev

agent | monitoring | grafana | prometheus | observability | packet-capture | api-first | data-streams | collector-agent | datasketches | stream-processors | stream-summarization

Readme

MPL-2.0 License

Releases 10

3.2.1 Latest
on Jun 13

+ 9 releases

Contributors 8

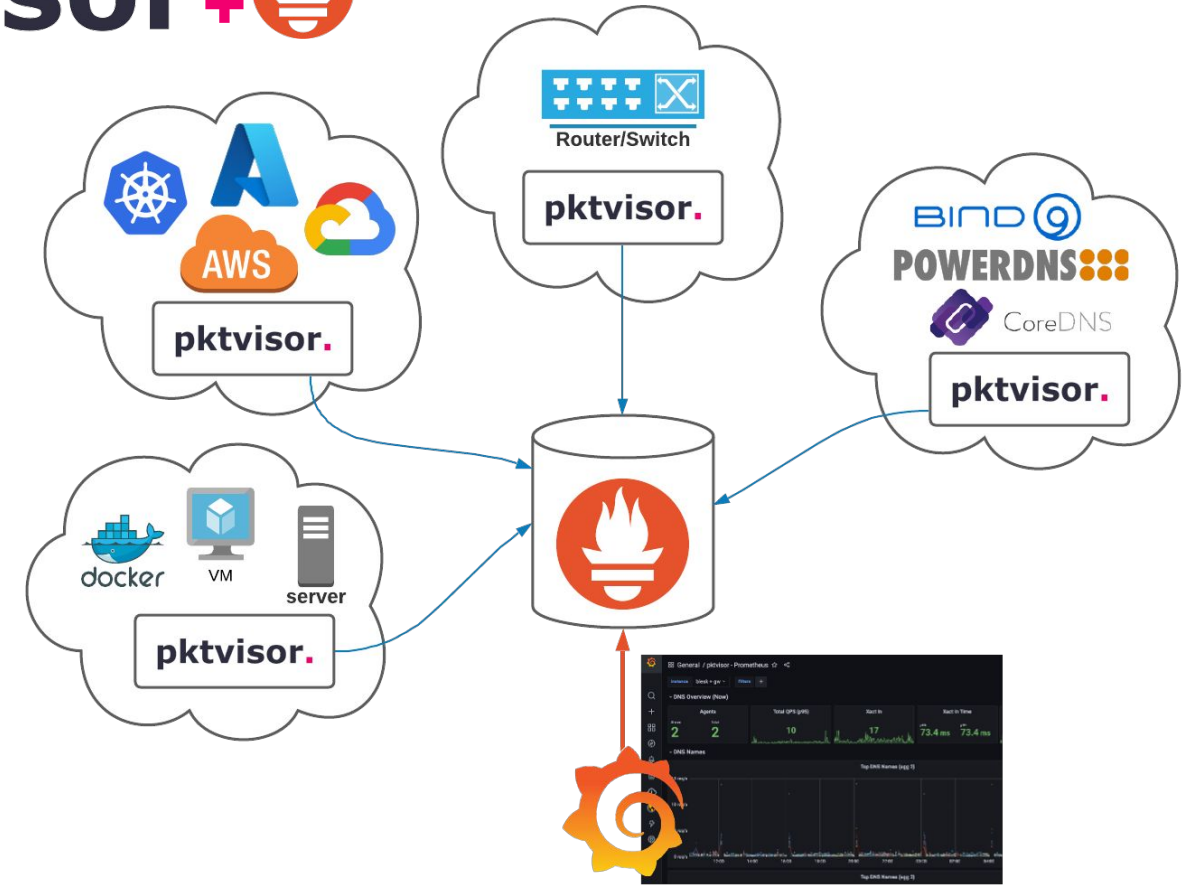
pktvisor+Prometheus

The Big Picture: pktvisor+Prometheus

- pktvisor exposes **Prometheus** metrics **per policy**
- Provides a **global view** of distributed pktvisor agents
- May be **scraped** or push with **remote write**
- Grafana and other tools for exploring, **visualizing** and **alerting**

Shannon Weyrick · sweyrick@ns1.com

pktvisor +



Shannon Weyrick · sweyrick@ns1.com

Easy Remote Write

pktvisor

docker

Prometheus

Grafana Agent

ns1labs/pktvisor-prom-write

Pulls 436

By ns1labs • Updated 17 hours ago

pktvisor with native ability to send metrics to Prometheus through remote write

Container

Overview Tags

pktvisor + centralized Prometheus collection

This container combines pktvisord with the Grafana Agent for collecting and sending metrics to Prometheus through remote write, including to cloud providers like Grafana Cloud.

There is a sample Grafana dashboard which provides a good starting point for visualizing pktvisor metrics. You can also find it online via the Grafana community dashboards, allowing you to import easily into any Grafana installation (ID 14221).

Example:

```
docker pull ns1labs/pktvisor-prom-write
docker run -d --net=host --env PKTVISORD_ARGS="--prom-instance <INSTANCE> <INTERFACE>" \
--env REMOTE_URL="https://<REMOTEHOST>/api/prom/push" --env USERNAME="<USERNAME>" \
--env PASSWORD="<PASSWORD>" ns1labs/pktvisor-prom-write
```

Grafana Dashboard

Grafana Labs | Grafana | Products | Open Source | Learn | Downloads | Contact us | Login

All dashboards » pktvisor - prometheus

pktvisor - prometheus by ns1labs

DASHBOARD

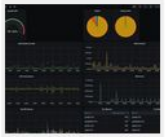
A dashboard for pktvisor observability tool (https://github.com/ns1labs/pktvisor), showcasing Network and DNS metrics.
Last updated: a month ago

Start with Grafana Cloud and the new FREE tier. Includes 10K series Prometheus or Graphite Metrics and 50gb Loki Logs

Downloads:
Reviews:

Add your review!

Overview | Revisions | Reviews




pktvisor summarizes network data streams in real time. It can capture Network, DNS, and other metrics via packet capture, dnstap, sflow, and other input methods.

This dashboard can be used as a starting point to visualize pktvisor metrics. See the Github page for information on how to deploy and collect these metrics.

Get this dashboard:

14221

Copy ID to Clipboard

Download JSON
How do I import this dashboard?

Dependencies:

Explore grafanacloud-ns1rd81-prom

Split | Last 1 hour | Clear all | Run query

Metrics browser ›

Enter a PromQL query (run with Shift+Enter)

0.2s

Query type: Range | Instant | Both

Step: auto

Exemplars

Help ›

+ Add query | Query history | Inspector

General / pktvisor - Prometheus

Last 24 hours | 1m

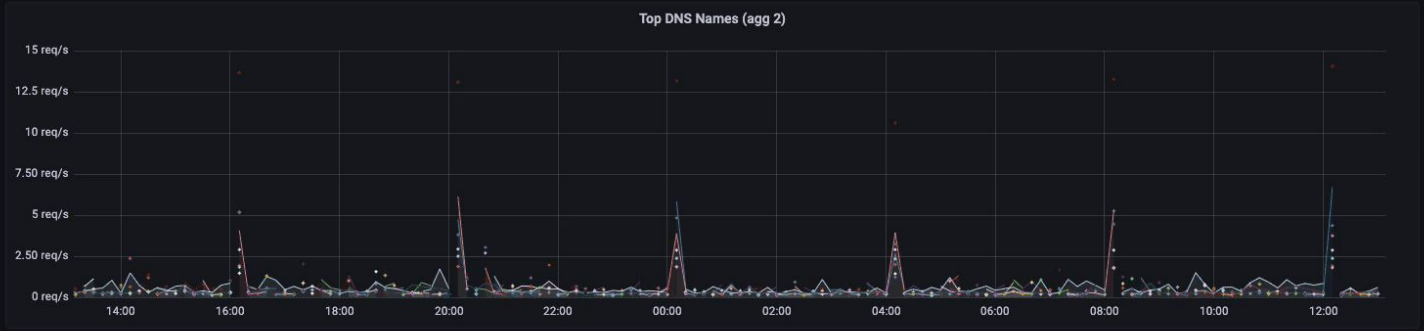
Instance | blesk + gw | Filters | +

pktvisor docs

DNS Overview (Now)

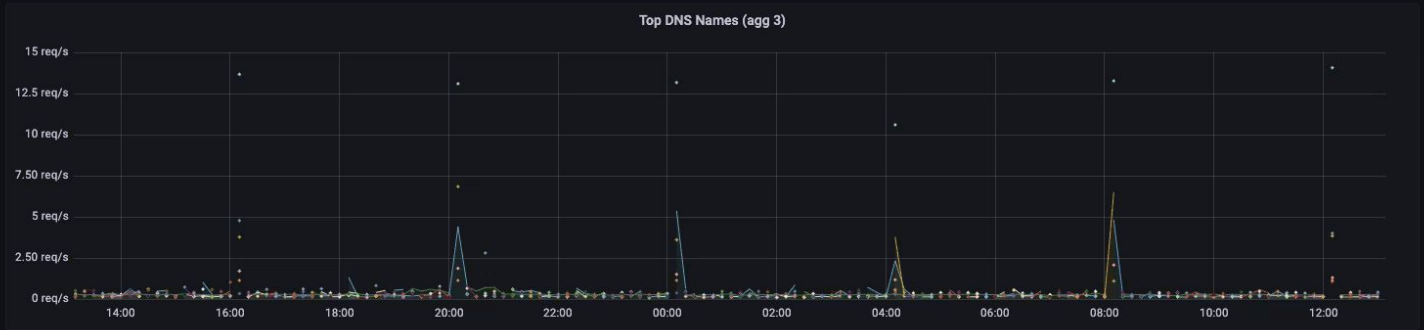
Agents		Total QPS (p95)	Xact In	Xact In Time		Xact Out	Xact Out Time		Unique QNames
Shown	Total			p95	p99		p95	p99	
2	2	19	27	71.6 ms	71.6 ms	50	85.3 ms	85.3 ms	45

DNS Names



Names (agg 2)

QName	Requsts (sum)
.google.com	20.9 K
.roku.com	19.5 K
.googleapis.com	7.23 K
.grafana.net	6.95 K
.akadns.net	6.43 K
.apple.com	5.22 K
.akamaiedge.net	5.18 K



Names (agg 3)

QName	Requsts (sum)
.logs.roku.com	18.7 K
.com.akadns.net	6.07 K
ns1rd81.grafana.net	5.42 K
.clients6.google.com	4.68 K
.oca.nflxvideo.net	4.67 K
.l.google.com	3.65 K
play.google.com	2.77 K

DNS

DNS Packets (In+Out) | QTypes | Result Codes | Transport


Orb

The Big Picture: Orb

- Nascent **free** and **open source** observability **platform** backed by NS1
- Based on **IoT** principals, provides **UI**, **API** and **agent communication**
- Solves challenges
  - **orchestrating** agents and their **policies**
  - **collecting** and **sinking** agent output

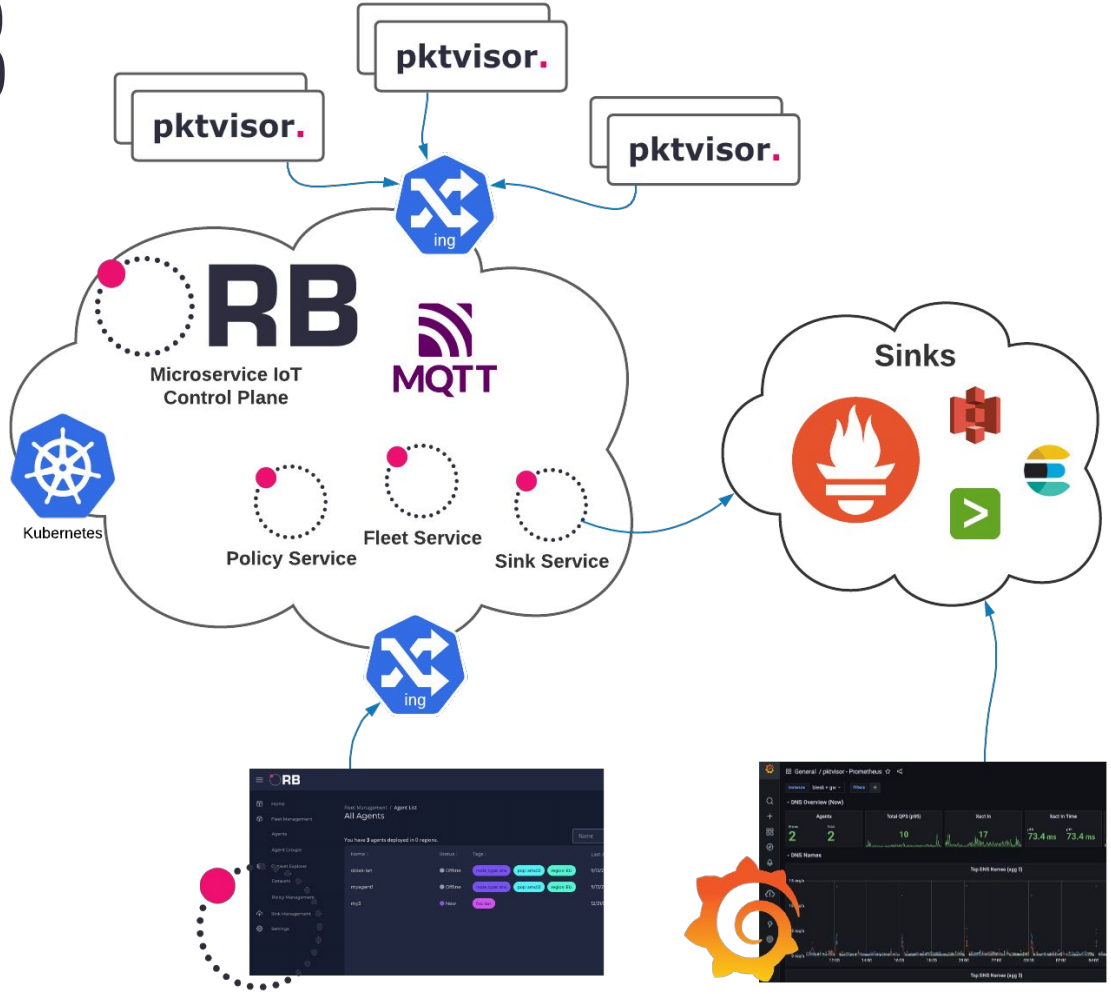
Shannon Weyrick · sweyrick@ns1.com

Orb Features

- **Multi-tenant fleet management** for agents
- Dynamic **agent grouping** (based on tagging) for assigning policies
- Definition and **orchestration of policies**, updating fleet in real time
- Centralized **metric collection** and **sinking** to **multiple destinations** per policy
- Helm chart for self-host **k8s deploy, free SaaS** coming soon at http://orb.live
- **Modular** support for observability agents (contributors!)

Shannon Weyrick · sweyrick@ns1.com

RB


pktvisor.
pktvisor.
pktvisor.
ing
RB
Microservice IoT
Control Plane
MQTT
Kubernetes
Policy Service
Fleet Service
Sink Service
Sinks
ing
RB
All Agents

ORB

sweyrick@ns1.com

- Home
- Fleet Management
  - Agents
  - Agent Groups
- Dataset Explorer
  - Datasets
  - Policy Management
- Sink Management
- Settings

Fleet Management / Agent List

All Agents

You have **3** agents deployed in 0 regions.

Name | Search by name

+ NEW AGENT

Name	Status	Tags	Last Activity
oblak-lan	Offline	node_type: dns, pop: ams02, region: EU	9/13/21, 1:32 PM
myagent1	Offline	node_type: dns, pop: ams02, region: EU	9/13/21, 1:38 PM
my3	New	foo: bar	12/31/01, 7:03 PM

ORB

GitHub

https://getorb.io

- FOSS
- Contributors welcome
- Please star!

ns1labs / orb Public

Unwatch 8 | Unstar 39 | Fork 3

Code | Issues 53 | Pull requests 6 | Discussions | Actions | Projects 3 | Wiki | Security | Insights | Settings

develop | 20 branches | 0 tags | Go to file | Add file | Code

dscabral Merge pull request #335 from ns1labs/feature/ORB-edit-dataset ... 42c81d0 1 hour ago 822 commits

.github	feature/sinker (#307)	6 days ago
.idea/runConfigurations	hotfix(orb_policies): add ide fleet config for main flux sdk	4 days ago
RFCs	separate policies from datasets, add to repo. and policy repo tests.	3 months ago
agent	feature/sinker (#307)	6 days ago
cmd	feature/sinker (#307)	6 days ago
docker	feature/sinker (#307)	6 days ago
docs/images	update arch diagrams	6 days ago
fleet	Merge pull request #335 from ns1labs/feature/ORB-edit-dataset	1 hour ago
grafana/api	Postman updated orb-grafana 1.0.0	3 months ago
internal/httputil	feat(agent_group): add feature to filter agent groups by tags	last month
pkg	feature/sinker (#307)	6 days ago
policies	Merge pull request #335 from ns1labs/feature/ORB-edit-dataset	1 hour ago
sinker	feature/sinker (#307)	6 days ago
sinks	feature/sinker (#307)	6 days ago
ui	Merge branch 'develop' into fix/orb-ui-update-cache-upon-deleting	3 days ago
.dockerignore	chore(boilerplate): added mainflux/ui boilerplate to Orb	3 months ago
.gitignore	feat(mock-server): adjusted settings	2 months ago
CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md	last month

About

Orb is a cloud native orchestration platform for dynamic edge observability

getorb.io

kubernetes | iot | ui | docker-compose | metrics | self-hosted | cloud-native | control-plane | observability | fleet-management | edge-computing

Readme

MPL-2.0 License

Releases

No releases published
Create a new release

Contributors 11

Languages

Summary

The Big Picture

pktvisor and **Orb** supplement modern observability stacks by facilitating **edge network observability**

The projects are **free** and **open source** backed by **NS1.**

The ultimate goal is **dynamic orchestration** of **business intelligence** at the **edge**

Shannon Weyrick · sweyrick@ns1.com

Thank You!

https://pktvisor.dev/ **https://getorb.io/**

PromCon
North America 2021

- sweyrick@ns1.com
- Orb Announcement List
- NS1 Labs Slack
- In person demos at NS1 booth Wed - Fri
- Or contact me on Virtual Platform or CNCF Slack!