How Orb powers DNS Insights … and can power your analytics too

Shannon Weyrick

Head of Technology

- Quick History on Orb & DNS Insights
- Architecture & Building DNS Insights
- Appendix: A Practical Application

netbox labs

sweyrick@netboxlabs.com

https://orb.community

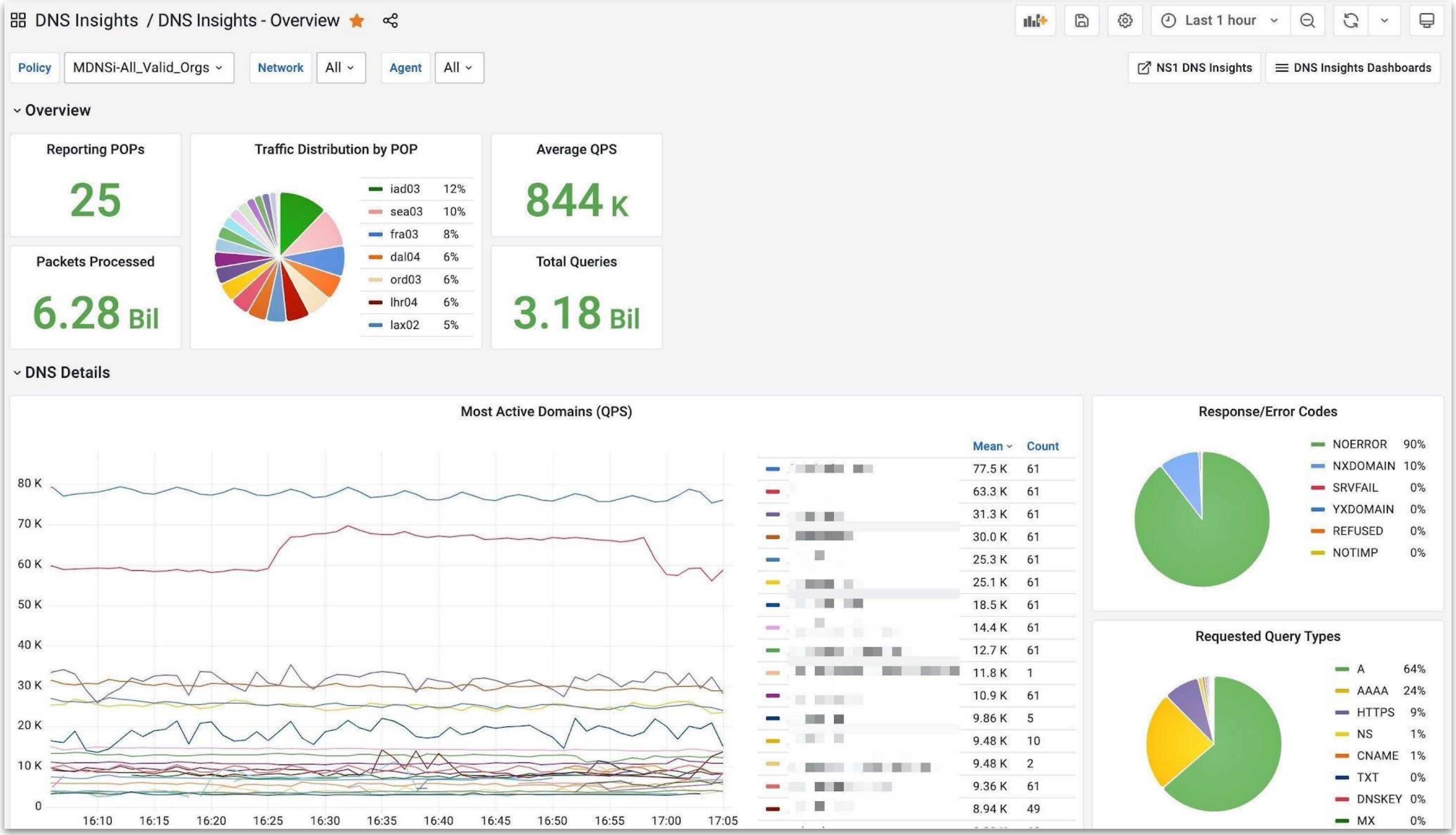
Quick History on Orb & DNS Insights

What is Orb?

- An open source network observability platform created at NS1 Labs, now at NetBox Labs (see OARC 38)
- Uses pktvisor for packet and DNS analysis (see OARC 33)

Who is NS1, what is DNS Insights?

- NS1 is a managed authoritative DNS provider
- DNS Insights is an NS1 product powered by Orb
- Allows NS1 customers to receive a stream of the same detailed metrics that NS1 operators use to manage and protect NS1's network



DNS Insights / DNS Insights - Overview ★

Last 1 hour

Policy: MDNSi-All_Valid_Orgs | Network: All | Agent: All

NS1 DNS Insights | DNS Insights Dashboards

Overview

Reporting POPs: 25

Packets Processed: 6.28 Bil

Average QPS: 844 K

Total Queries: 3.18 Bil

Traffic Distribution by POP

iad03	12%
sea03	10%
fra03	8%
dal04	6%
ord03	6%
lhr04	6%
lax02	5%

DNS Details

Most Active Domains (QPS)

	Mean	Count
[redacted]	77.5 K	61
[redacted]	63.3 K	61
[redacted]	31.3 K	61
[redacted]	30.0 K	61
[redacted]	25.3 K	61
[redacted]	25.1 K	61
[redacted]	18.5 K	61
[redacted]	14.4 K	61
[redacted]	12.7 K	61
[redacted]	11.8 K	1
[redacted]	10.9 K	61
[redacted]	9.86 K	5
[redacted]	9.48 K	10
[redacted]	9.48 K	2
[redacted]	9.36 K	61
[redacted]	8.94 K	49

Response/Error Codes

NOERROR	90%
NXDOMAIN	10%
SRVFAIL	0%
YXDOMAIN	0%
REFUSED	0%
NOTIMP	0%

Requested Query Types

A	64%
AAAA	24%
HTTPS	9%
NS	1%
CNAME	1%
TXT	0%
DNSKEY	0%
MX	0%

netbox labs

sweyrick@netboxlabs.com

https://orb.community

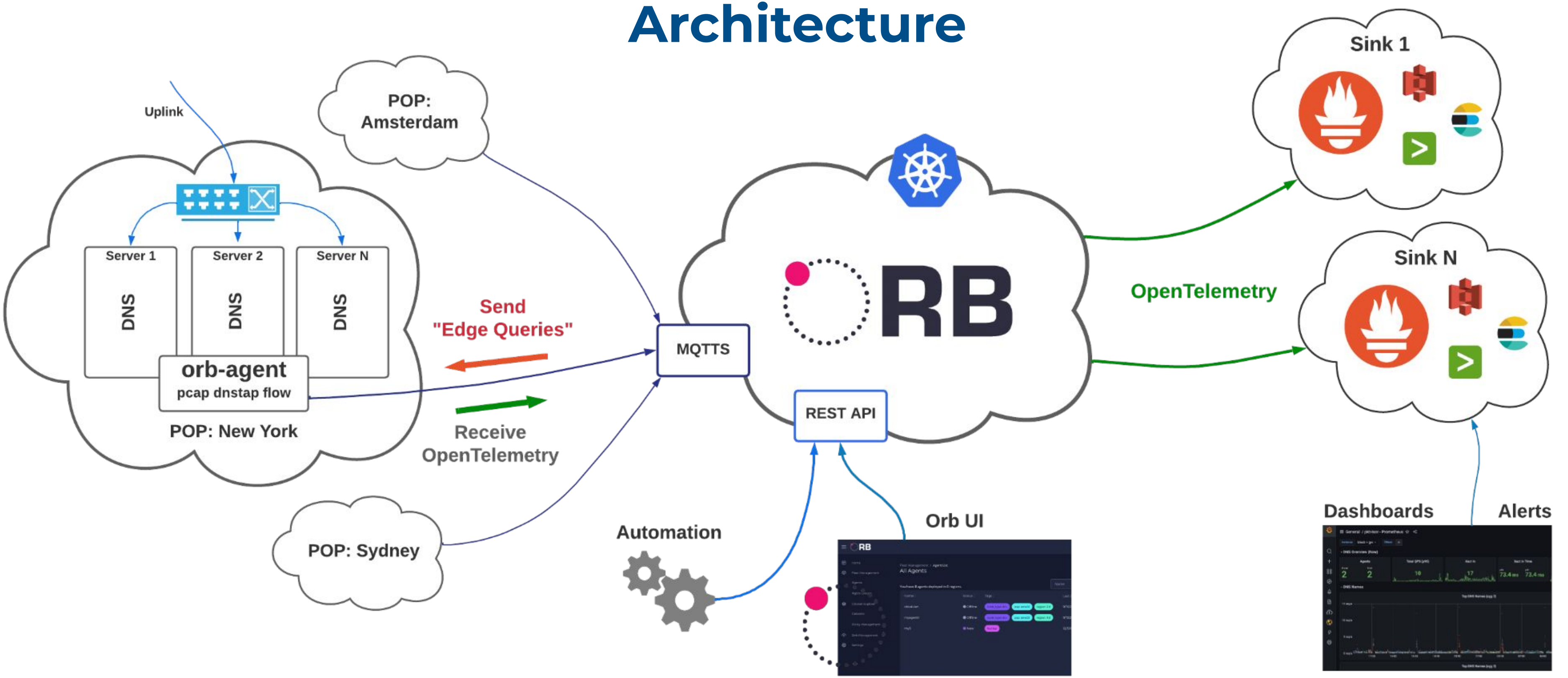
How is Orb different?

- Analysis in real-time at the edge
- Manages a set of custom policies across a whole fleet of agents
- Modern, flexible data pipelines based on OpenTelemetry
- Telemetry data can be streamed directly to operators & customers
- Fleet configuration via central REST API
- Free Open Source Software

Why DNS Insights?

- NS1's anycast network offers a unique viewpoint to which customers don't normally have access
- Far greater range of relevant DNS information than traffic levels
- Debug issues, spot misconfiguration, identify malicious traffic
- Can create their own dashboards and view NS1 DNS telemetry alongside their other observability data
- Provides same depth of information that NS1 operators get

Orb Architecture



netbox labs

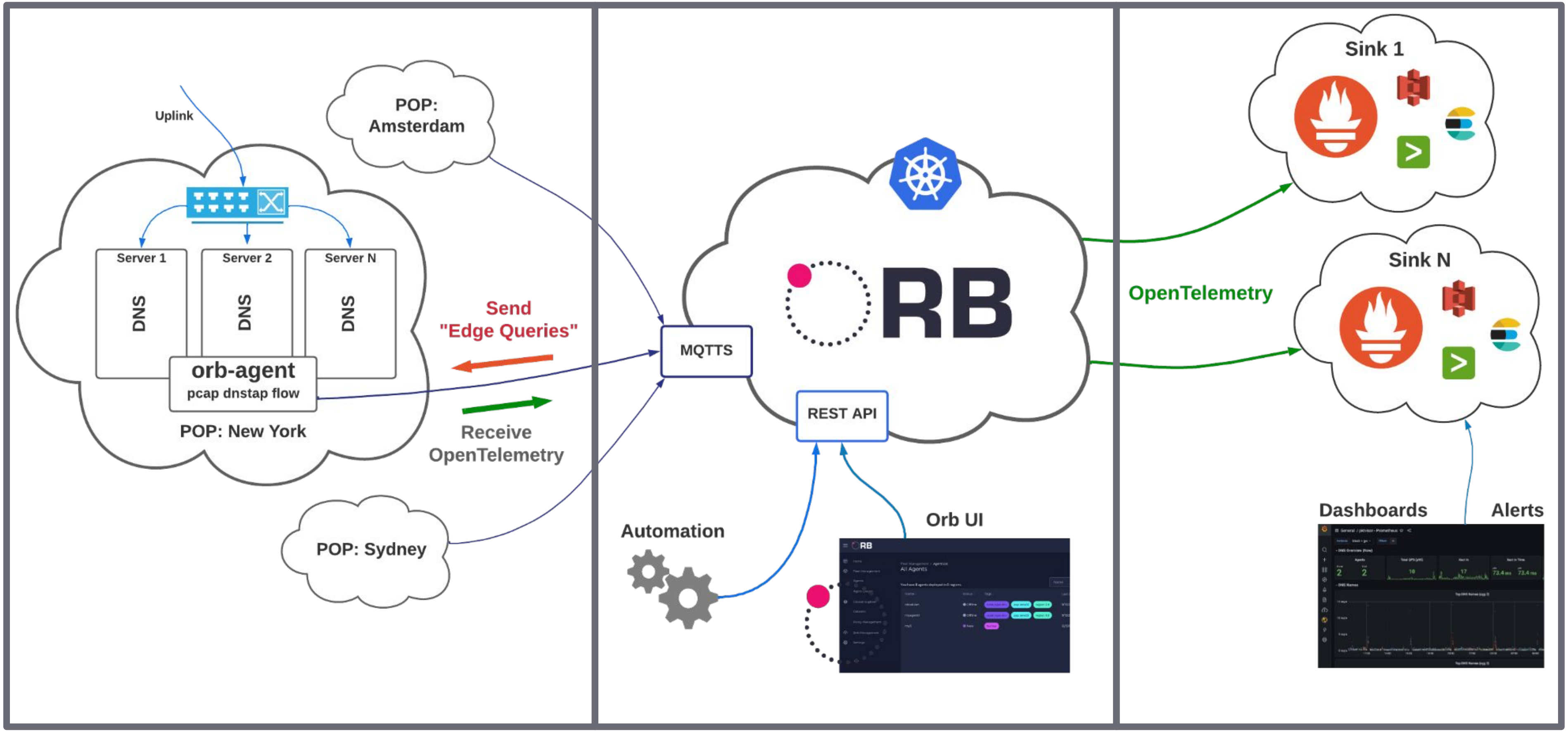
sweyrick@netboxlabs.com

https://orb.community

Edge

Control Plane

Sinks



Uplink

Server 1

Server 2

Server N

DNS

DNS

DNS

orb-agent

pcap dnstap flow

POP: New York

POP: Amsterdam

POP: Sydney

Send "Edge Queries"

Receive OpenTelemetry

MQTTS

RB

REST API

Automation

Orb UI

OpenTelemetry

Sink 1

Sink N

Dashboards

Alerts

Building DNS Insights: Edge Architecture

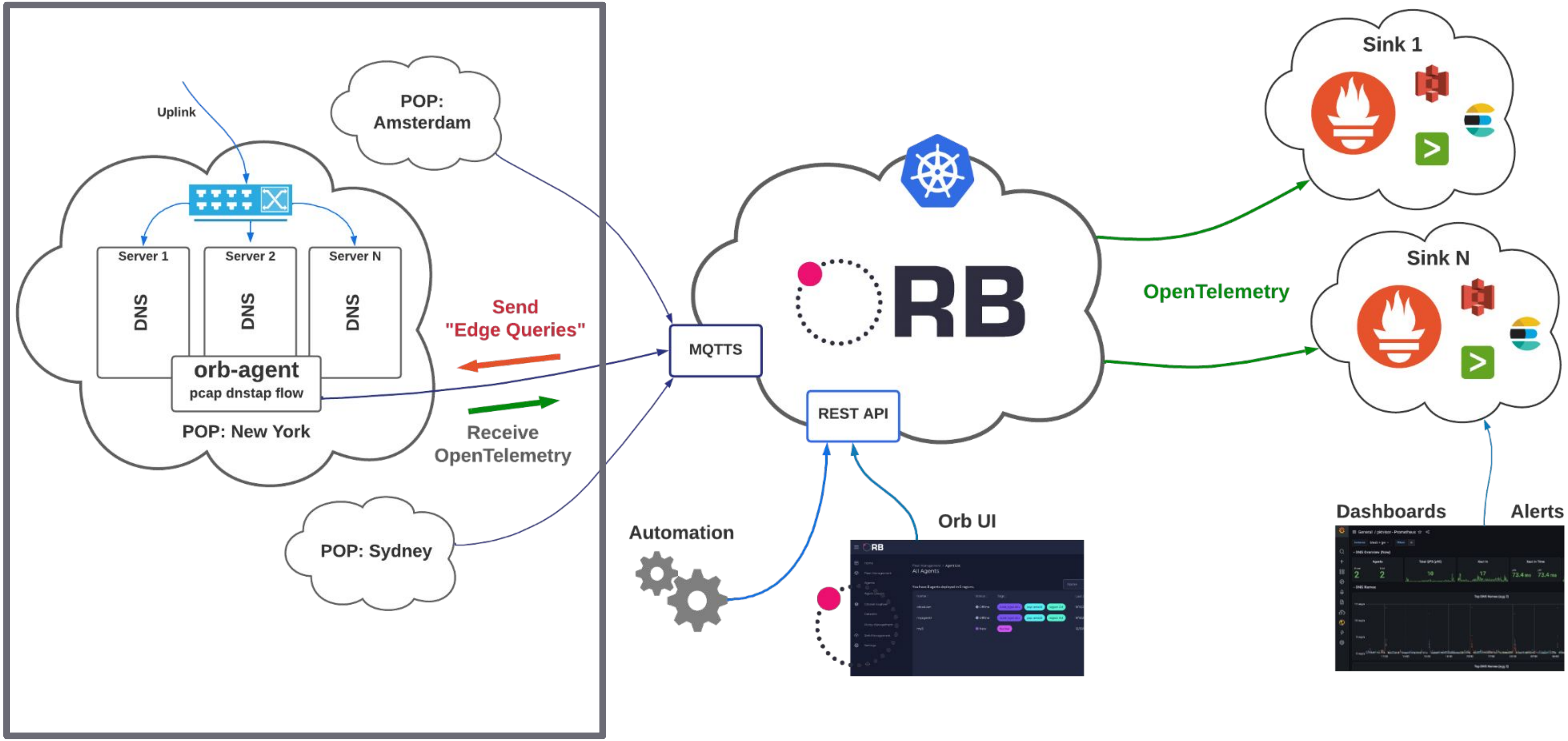
Analyzing 1 million global queries per second in real-time

netbox labs

sweyrick@netboxlabs.com

https://orb.community

Edge



netbox labs

sweyrick@netboxlabs.com

https://orb.community

Working With Agents

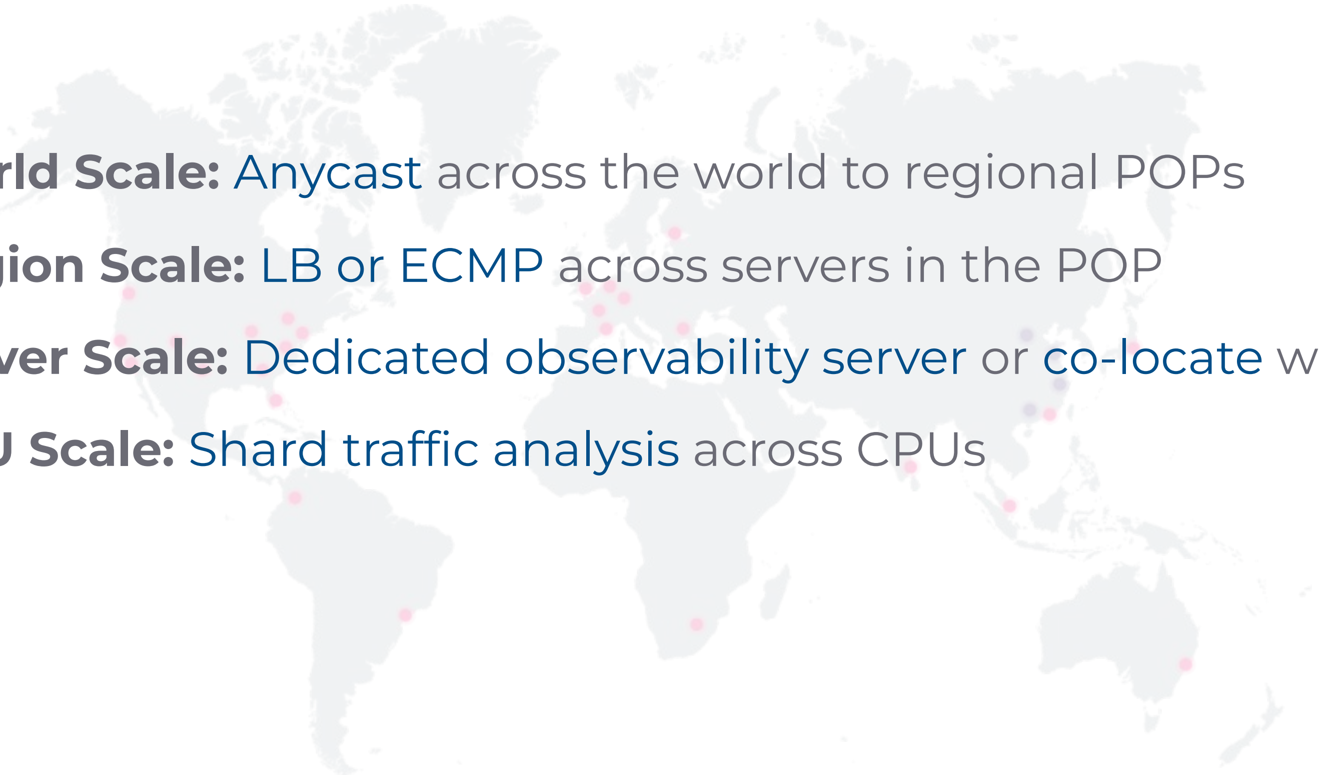
agent.yaml

```
visor:
  taps:
    default_flow:
      input_type: pcap
      config:
        iface: eth0
```

- Lightweight docker containers
- To install/upgrade, pull and restart
- Egress only, MQTT over TLS

```
docker run -d --net=host \
-e ORB_CLOUD_MQTT_ID=a4715b19-1a6e-4ecb-9f87-9908c7b5c9cf \
-e ORB_CLOUD_MQTT_CHANNEL_ID=11bd1e66-dc05-442c-93ee-73a7cc6611ff \
-e ORB_CLOUD_MQTT_KEY=88463219-f829-43f6-925a-04b3790c1bca \
-v ${PWD}/agent.yaml:/opt/orb/agent.yaml \
ns1labs/orb-agent
```

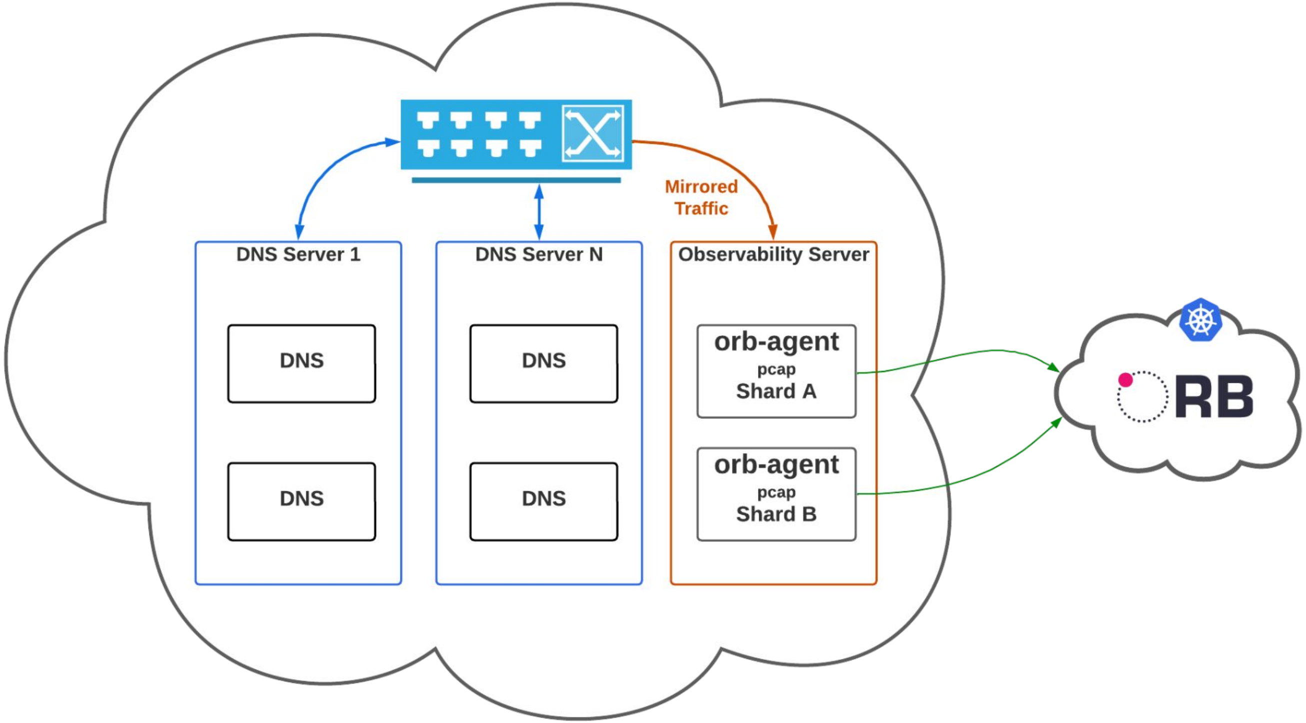
How do you real-time analyze 1m QPS?



- **World Scale:** Anycast across the world to regional POPs
- **Region Scale:** LB or ECMP across servers in the POP
- **Server Scale:** Dedicated observability server or co-locate with DNS
- **CPU Scale:** Shard traffic analysis across CPUs

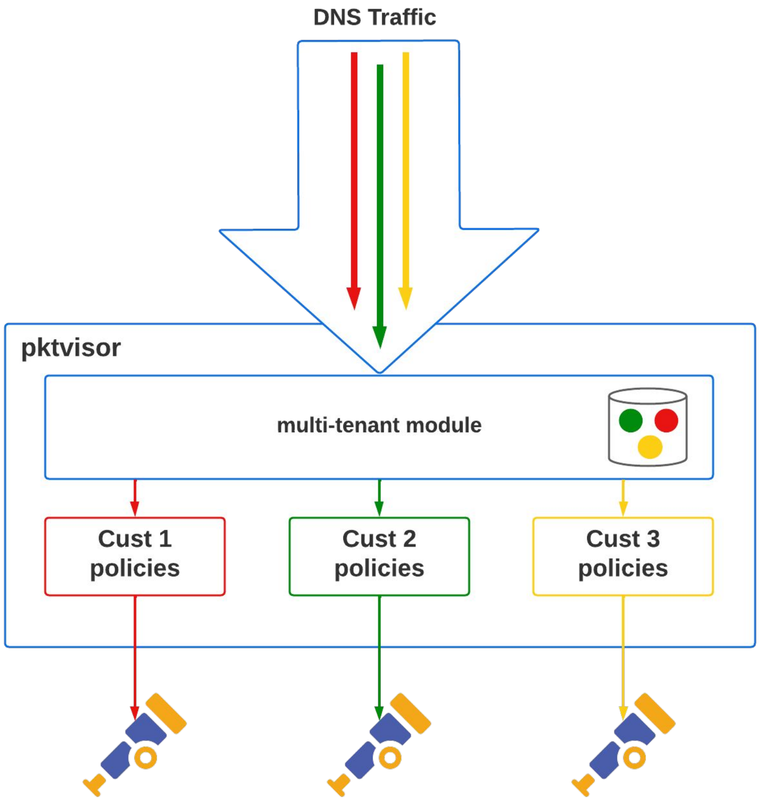
NS1 Example: Traffic Mirroring in a POP

- Dedicated observability server
- Two agents for fault isolation
- Split traffic by port ranges across multiple CPUs
- Agent shards and recombines the analysis



Solving NS1 Edge Multi-tenancy

- Policies must be able to filter by customer
- Requires use of a custom pktvisor module
- Each customer transits to a separate data pipeline



Building DNS Insights: Control Plane

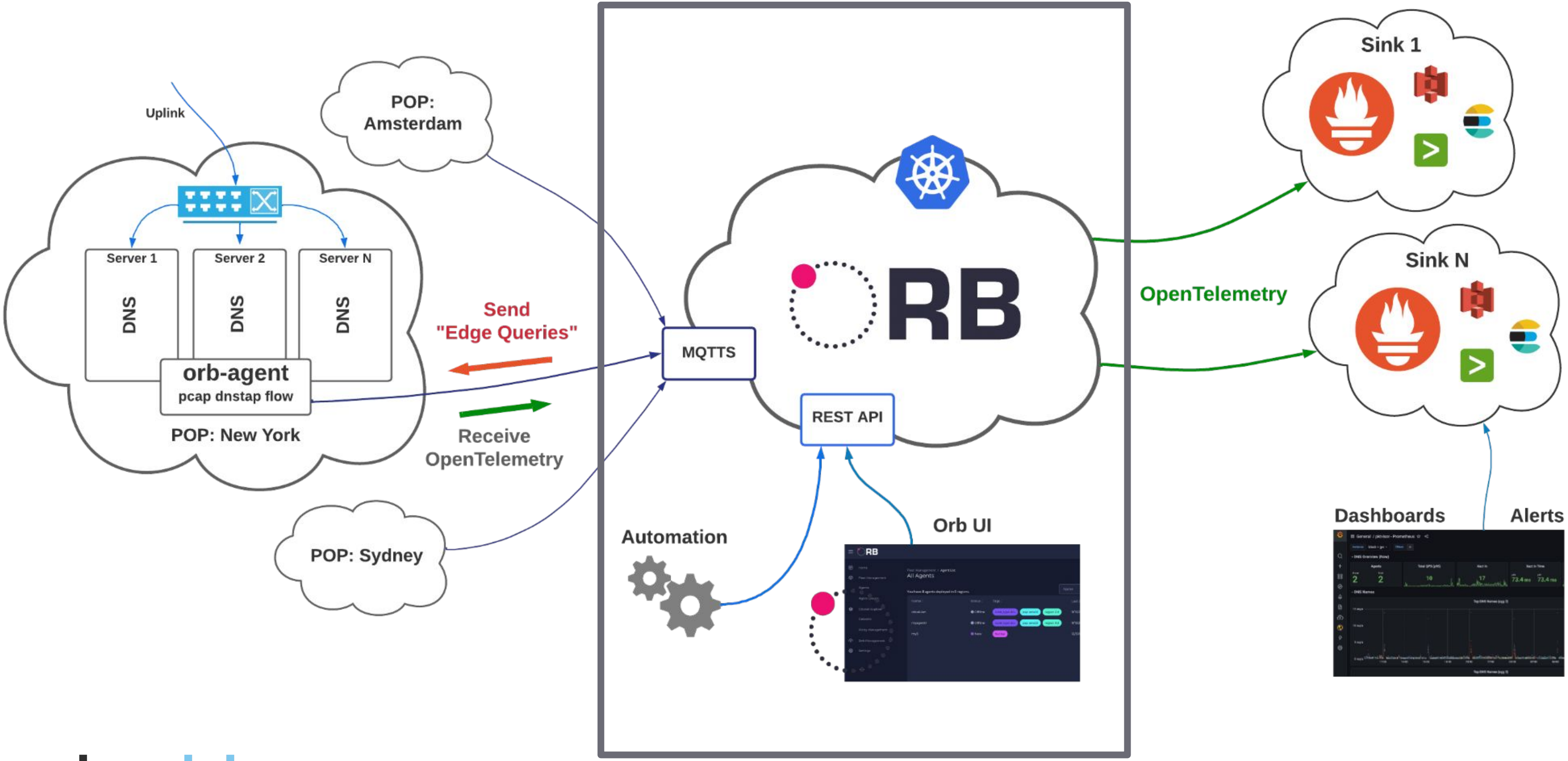
Centralized fleet configuration management

netbox labs

sweyrick@netboxlabs.com

https://orb.community

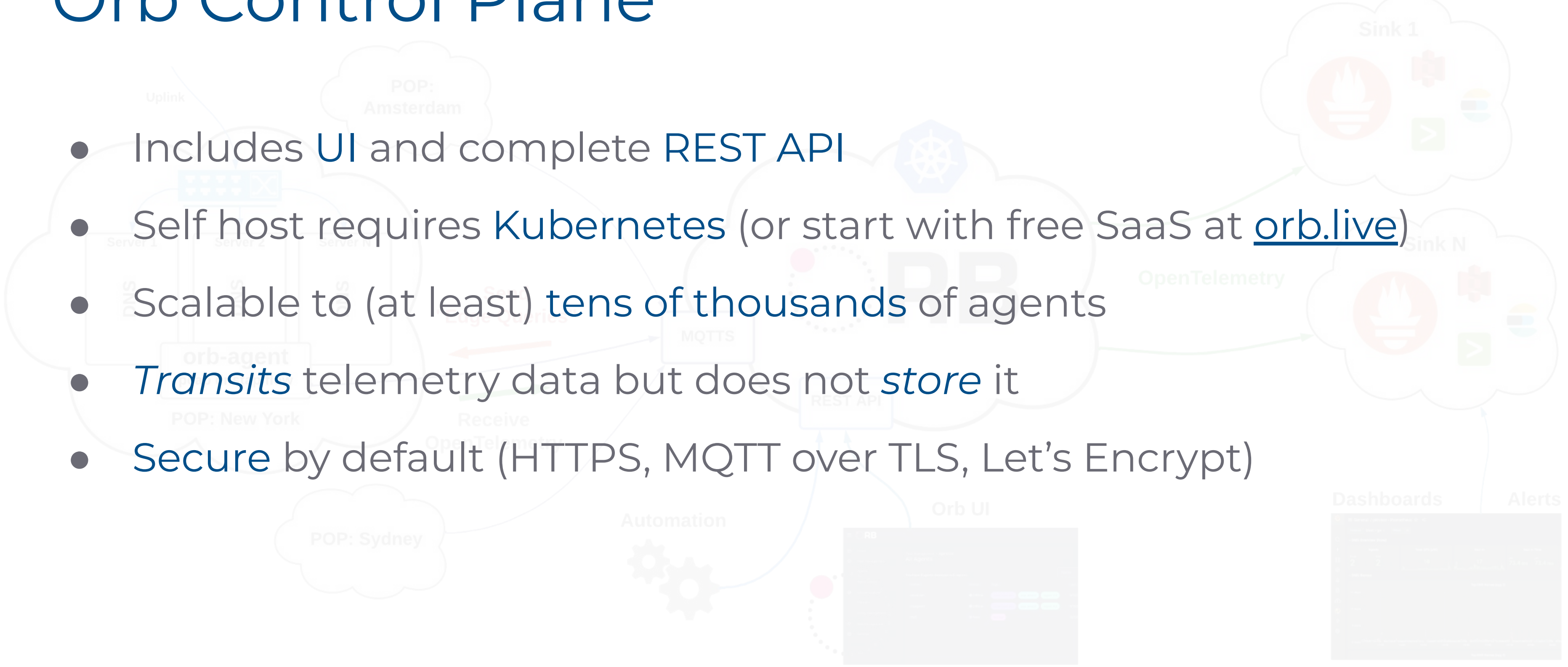
Control Plane



sweyrick@netboxlabs.com

https://orb.community

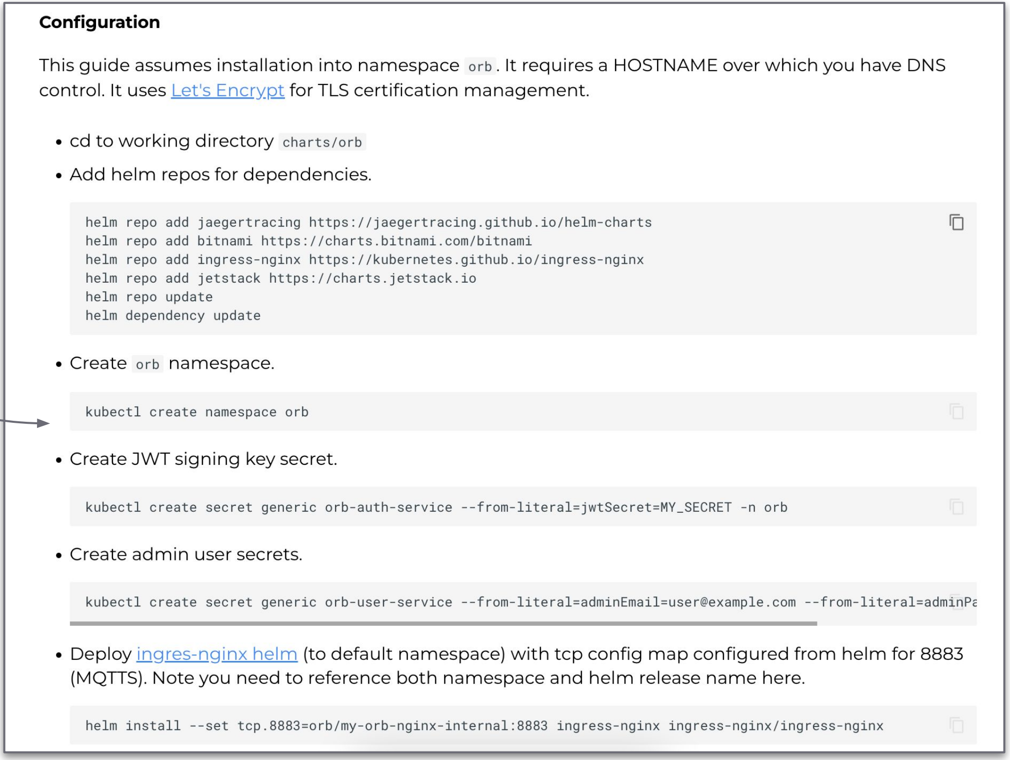
Orb Control Plane



- Includes UI and complete REST API
- Self host requires Kubernetes (or start with free SaaS at orb.live)
- Scalable to (at least) tens of thousands of agents
- *Transits* telemetry data but does not *store* it
- Secure by default (HTTPS, MQTT over TLS, Let’s Encrypt)

Installing Into Kubernetes

- Helm chart is provided
- NS1 and orb.live use EKS
- Follow the helm install instructions



Configuration

This guide assumes installation into namespace `orb`. It requires a HOSTNAME over which you have DNS control. It uses Let's Encrypt for TLS certification management.

- cd to working directory `charts/orb`
- Add helm repos for dependencies.

```
helm repo add jaegertracing https://jaegertracing.github.io/helm-charts
helm repo add bitnami https://charts.bitnami.com/bitnami
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
helm repo add jetstack https://charts.jetstack.io
helm repo update
helm dependency update
```

- Create `orb` namespace.

```
kubectl create namespace orb
```

- Create JWT signing key secret.

```
kubectl create secret generic orb-auth-service --from-literal=jwtSecret=MY_SECRET -n orb
```

- Create admin user secrets.

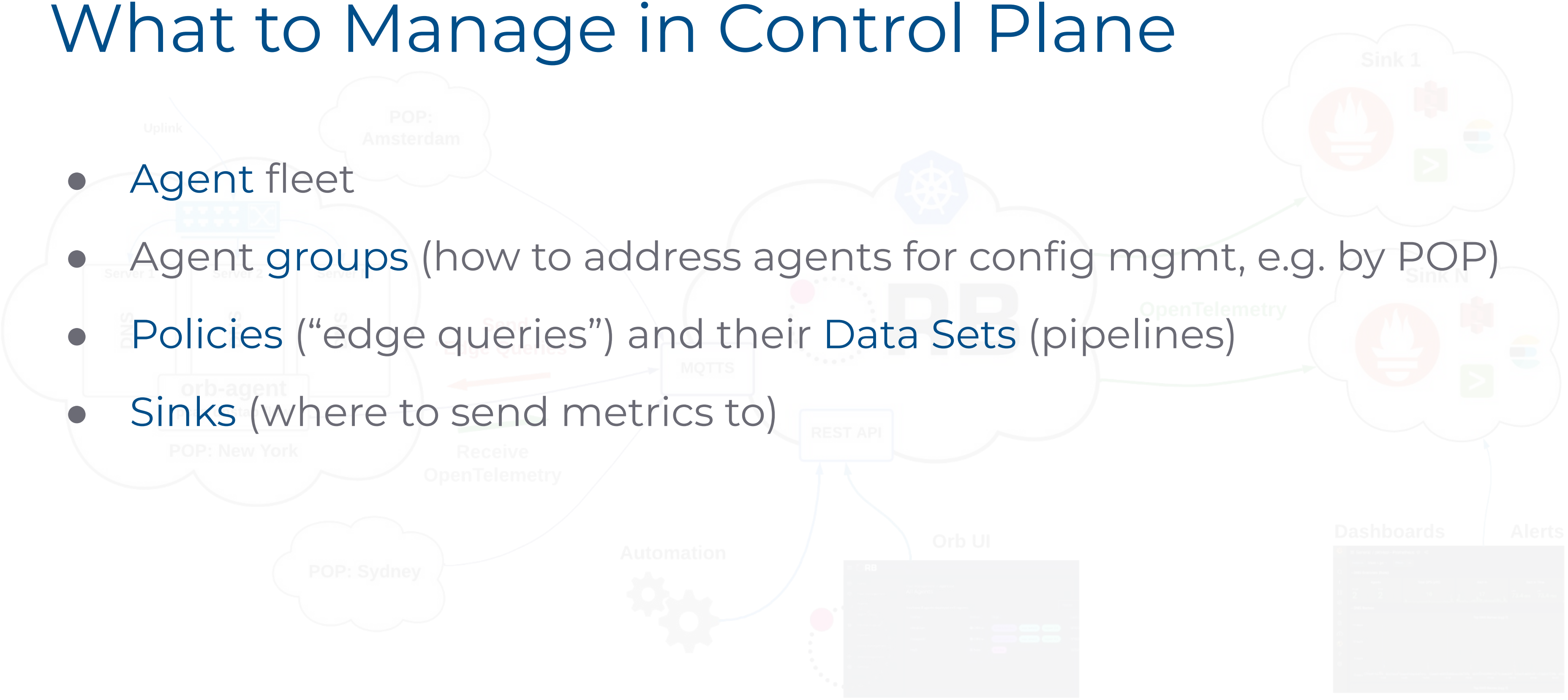
```
kubectl create secret generic orb-user-service --from-literal=adminEmail=user@example.com --from-literal=adminPa
```

- Deploy ingres-nginx helm (to default namespace) with tcp config map configured from helm for 8883 (MQTTS). Note you need to reference both namespace and helm release name here.

```
helm install --set tcp.8883=orb/my-orb-nginx-internal:8883 ingress-nginx ingress-nginx/ingress-nginx
```

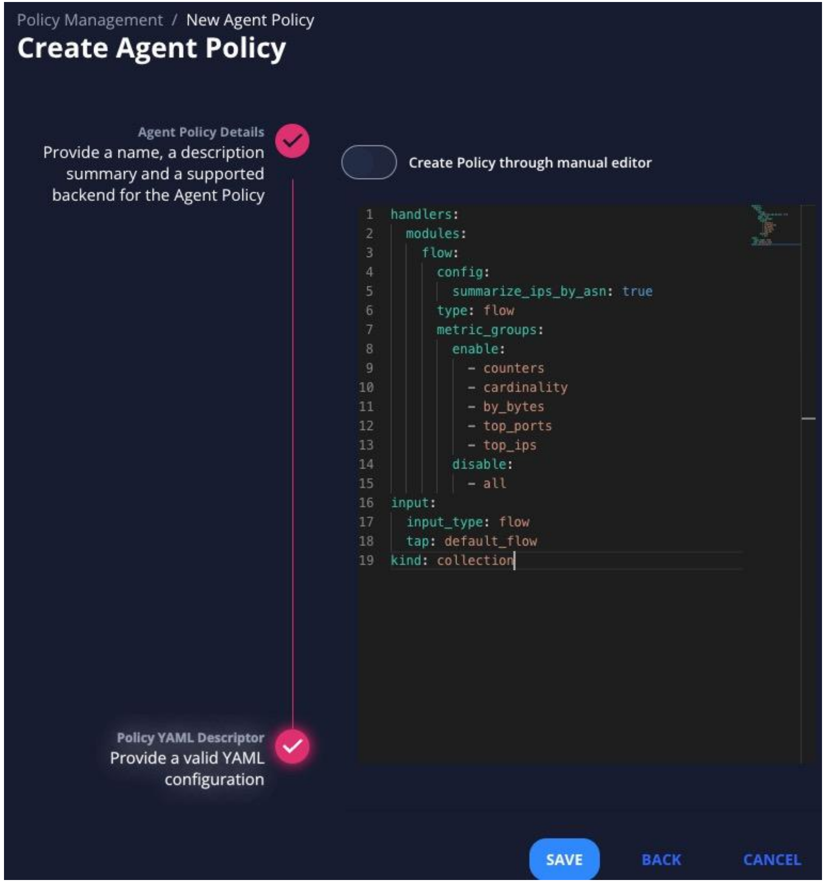
What to Manage in Control Plane

- Agent fleet
- Agent groups (how to address agents for config mgmt, e.g. by POP)
- Policies (“edge queries”) and their Data Sets (pipelines)
- Sinks (where to send metrics to)



Policies

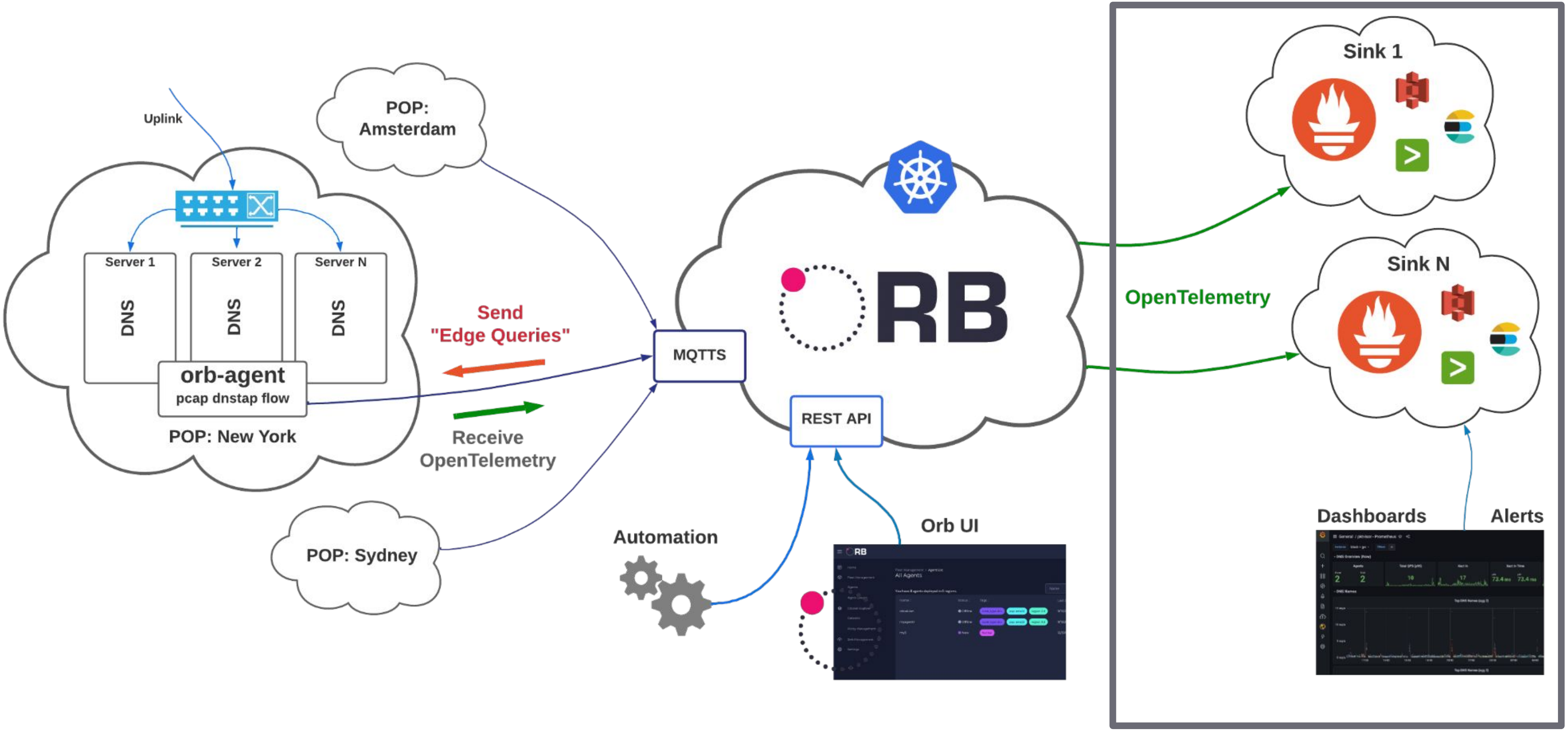
- Act as “edge queries” to observe precisely
- Create, update, remove in real-time
- Composable and granular
- NS1 manages multiple, concurrent policies per customer using tags



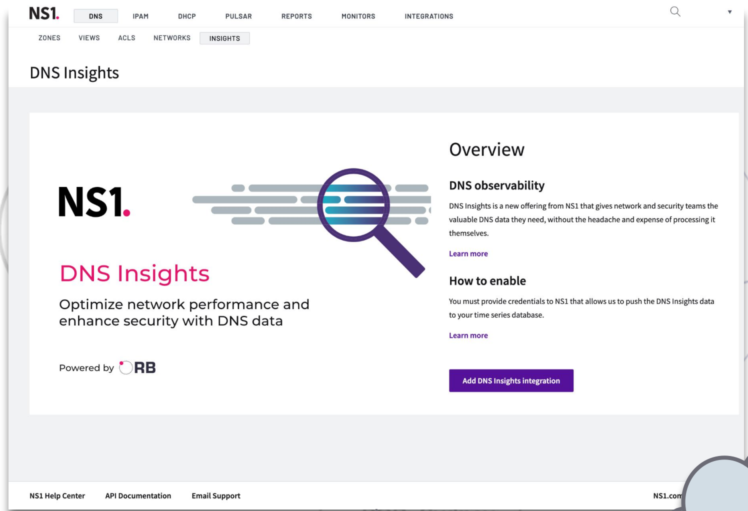
Policy Management / New Agent Policy
Create Agent Policy
Agent Policy Details
Provide a name, a description summary and a supported backend for the Agent Policy
Create Policy through manual editor
Policy YAML Descriptor
Provide a valid YAML configuration
SAVE
BACK
CANCEL

```yaml
handlers:
  modules:
    flow:
      config:
        summarize_ips_by_asn: true
      type: flow
      metric_groups:
        enable:
          - counters
          - cardinality
          - by_bytes
          - top_ports
          - top_ips
        disable:
          - all
input:
  input_type: flow
  tap: default_flow
kind: collection
```

Sinks


Uplink
Server 1
Server 2
Server N
DNS
DNS
DNS
orb-agent
pcap dnstap flow
POP: New York
POP: Amsterdam
POP: Sydney
Send
"Edge Queries"
Receive
OpenTelemetry
MQTTS
RB
REST API
Automation
Orb UI
RB
All Agents
OpenTelemetry
Sink 1
Sink N
Dashboards
Alerts

How Insights Manages Sinks



DNS Insights

NS1.

DNS Insights

Optimize network performance and enhance security with DNS data

Powered by ORB

Overview

DNS observability

DNS Insights is a new offering from NS1 that gives network and security teams the valuable DNS data they need, without the headache and expense of processing it themselves.

Learn more

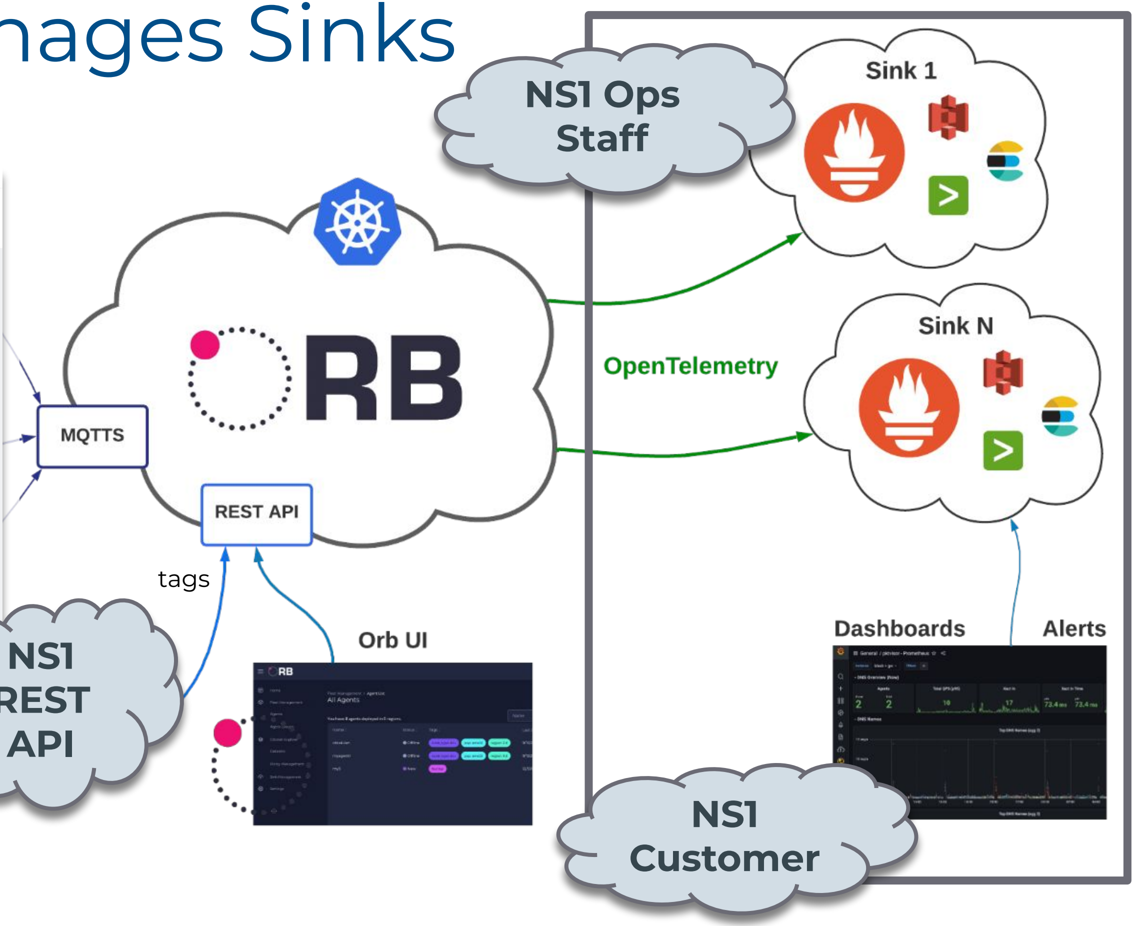
How to enable

You must provide credentials to NS1 that allows us to push the DNS Insights data to your time series database.

Learn more

Add DNS Insights integration

NS1 Help Center API Documentation Email Support NS1.com



netbox labs

sweyrick@netboxlabs.com

https://orb.community

Conclusion

Key Takeaways

- Orb is a network observability platform with exceptional support for large scale DNS analysis
- Orb powers NS1’s DNS Insights product at scale, in production today
- Orb is free, open source software and can power your analytics too!

Next Steps

- Join the community: https://orb.community
- Try Orb SaaS for free: https://orb.live
- Star the project: github.com/orb-community/orb
- Watch the OARC 33 talk on pktvisor
- Watch the OARC 38 talk Orb: On the Edge of Small Data

Thank you

netbox labs

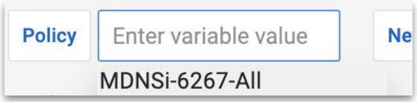
sweyrick@netboxlabs.com

https://orb.community

Appendix: Dynamic Debugging

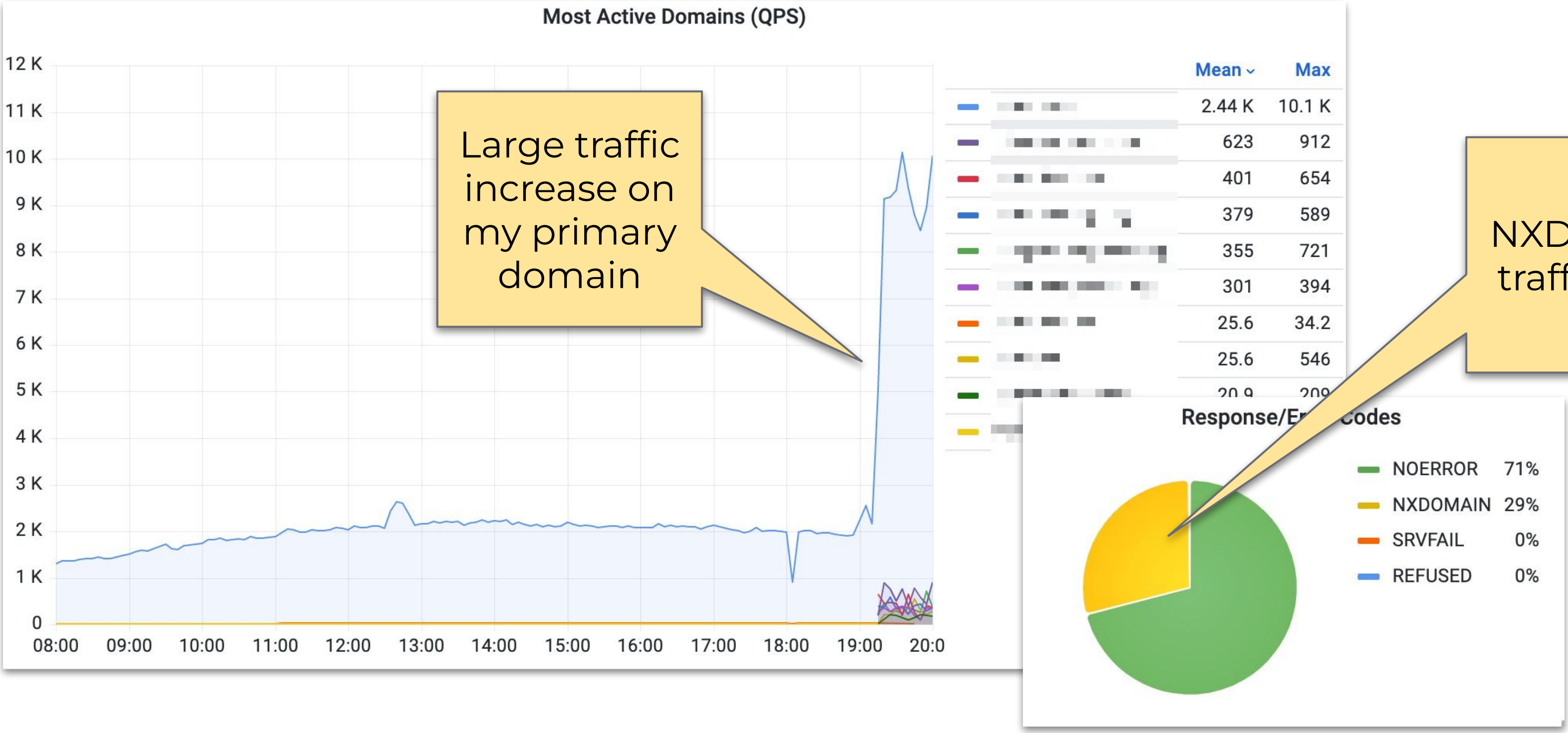
A practical application of applying dynamic policies in real time

Identify Questionable Traffic



Policy: Enter variable value

MDNSi-6267-All



Most Active Domains (QPS)

		Mean ⌄	Max
🟦	[redacted]	2.44 K	10.1 K
🟪	[redacted]	623	912
🟥	[redacted]	401	654
🟦	[redacted]	379	589
🟩	[redacted]	355	721
🟪	[redacted]	301	394
🟧	[redacted]	25.6	34.2
🟨	[redacted]	25.6	546
🟩	[redacted]	20.9	209
🟨	[redacted]		

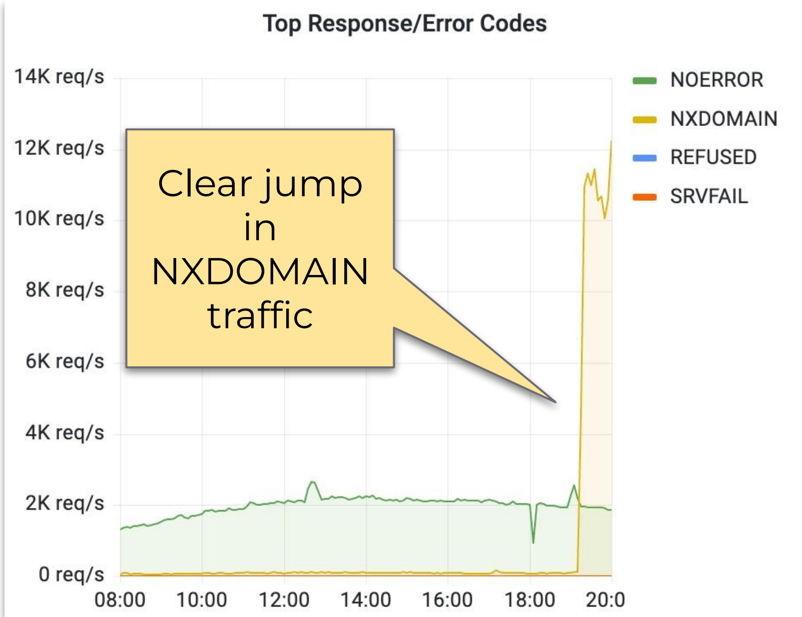
Response/Error Codes

🟩	NOERROR	71%
🟨	NXDOMAIN	29%
🟧	SRVFAIL	0%
🟦	REFUSED	0%

Large traffic increase on my primary domain

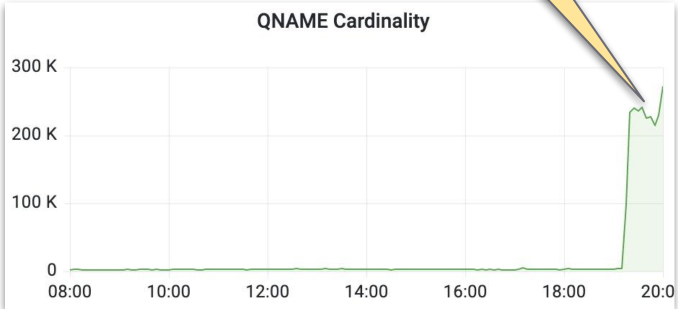
NXDOMAIN traffic is up

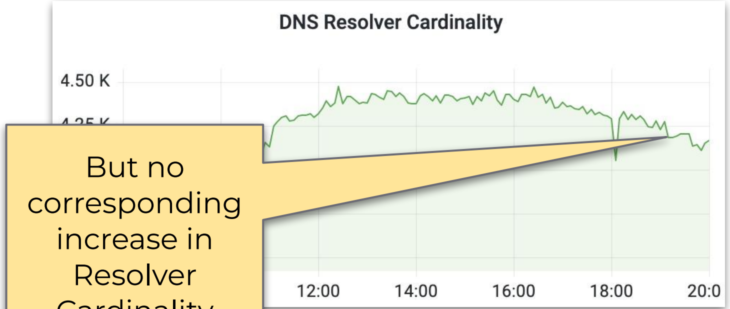
Suspicious... now what?



Clear jump in NXDOMAIN traffic

Dramatic increase in QNAME Cardinality



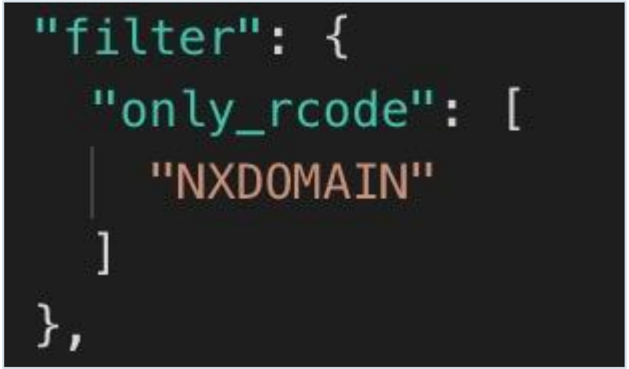


But no corresponding increase in Resolver Cardinality

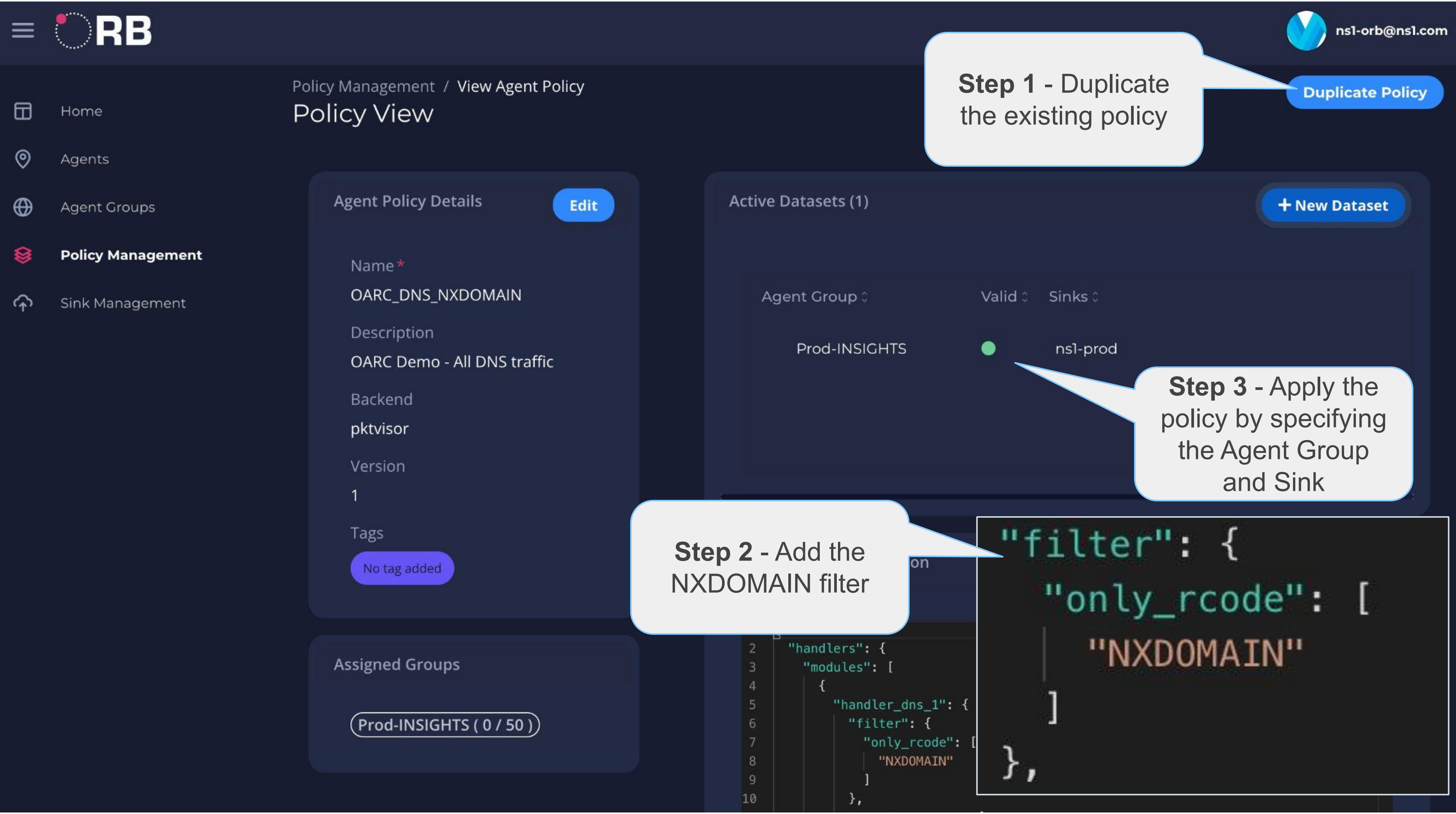
Dive Deep With a New Policy in Real-time

- Policies are YAML/JSON based
- Easy to duplicate and filter down

Let’s **create** and **push** a policy to show only NXDOMAIN traffic:



```
"filter": {
  "only_rcode": [
    "NXDOMAIN"
  ]
},
```



Policy Management / View Agent Policy

Policy View

Step 1 - Duplicate the existing policy

Agent Policy Details

Name*

OARC_DNS_NXDOMAIN

Description

OARC Demo - All DNS traffic

Backend

pktvisor

Version

1

Tags

No tag added

Assigned Groups

Prod-INSIGHTS (0 / 50)

Active Datasets (1)

Agent Group	Valid	Sinks
Prod-INSIGHTS	●	ns1-prod

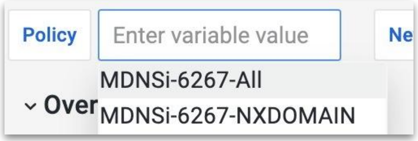
Step 3 - Apply the policy by specifying the Agent Group and Sink

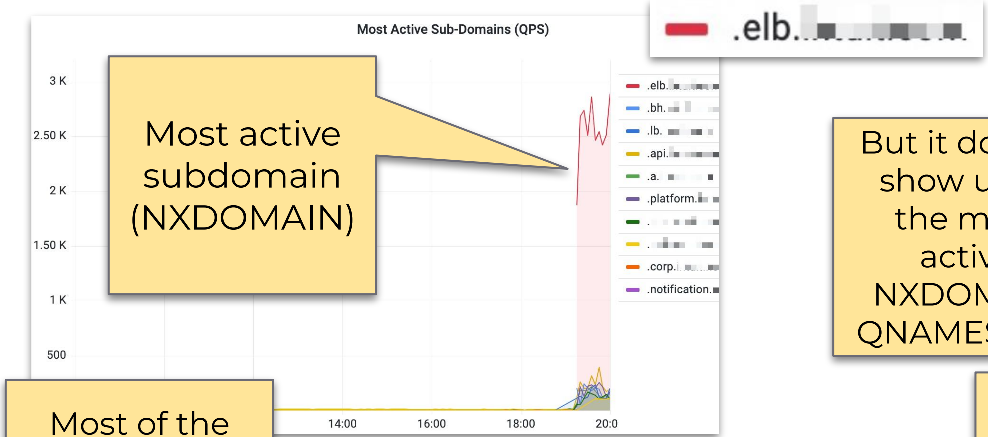
Step 2 - Add the NXDOMAIN filter

```
  "handlers": {
    "modules": [
      {
        "handler_dns_1": {
          "filter": {
            "only_rcode": [
              "NXDOMAIN"
            ]
          },
```

```
"filter": {
  "only_rcode": [
    "NXDOMAIN"
  ]
},
```

Review new Policy data

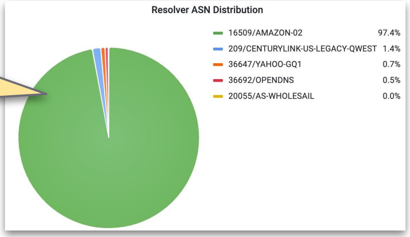


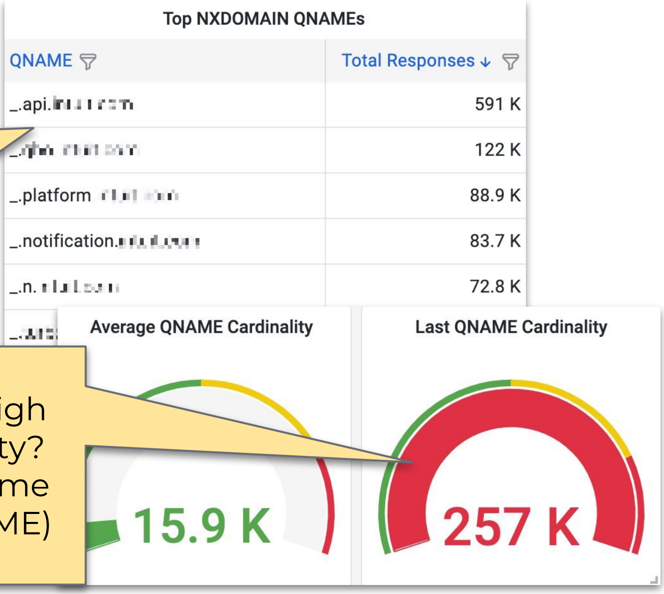


Most active subdomain (NXDOMAIN)

But it doesn't show up in the most active NXDOMAIN QNAMES (?!?)

Most of the NXDOMAIN traffic is coming from the same ASN

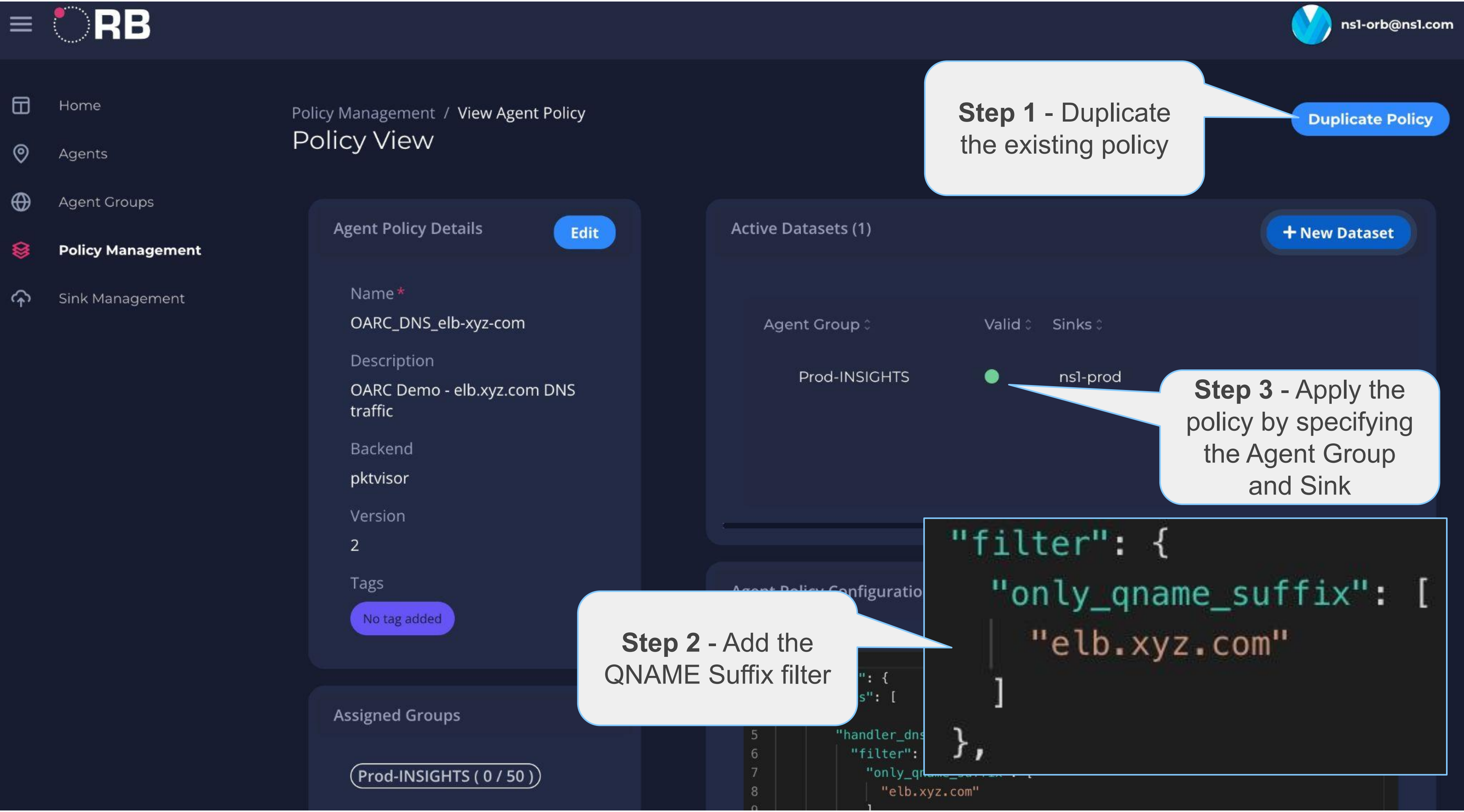




Top NXDOMAIN QNAMEs

QNAME	Total Responses ↓
_.api.[redacted]	591 K
_.[redacted]	122 K
_.platform [redacted]	88.9 K
_.notification.[redacted]	83.7 K
_.n.[redacted]	72.8 K
_.[redacted]	

Due to high cardinality? (low volume per QNAME)



Policy Management / View Agent Policy

Policy View

Step 1 - Duplicate the existing policy

Agent Policy Details

Name*
OARC_DNS_elb-xyz-com

Description
OARC Demo - elb.xyz.com DNS traffic

Backend
pktvisor

Version
2

Tags
No tag added

Assigned Groups

Prod-INSIGHTS (0 / 50)

Active Datasets (1)

Agent Group	Valid	Sinks
Prod-INSIGHTS	●	ns1-prod

Step 3 - Apply the policy by specifying the Agent Group and Sink

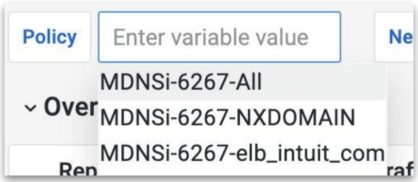
Agent Policy Configuratio

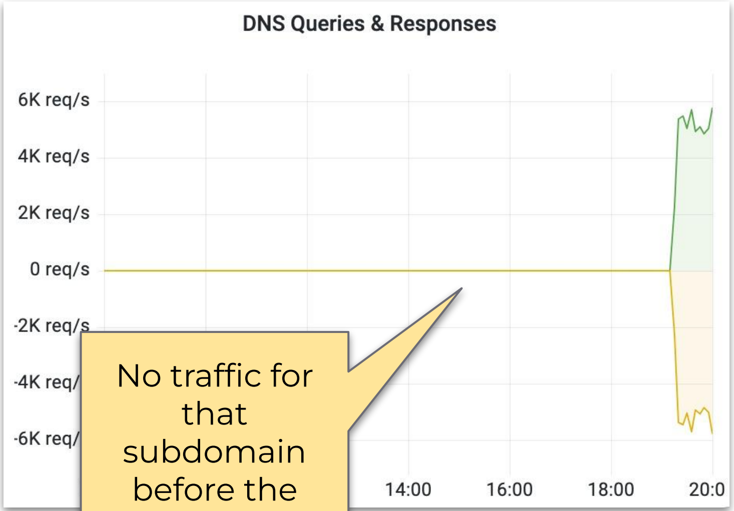
Step 2 - Add the QNAME Suffix filter

```
"filter": {
  "only_qname_suffix": [
    "elb.xyz.com"
  ]
},
```

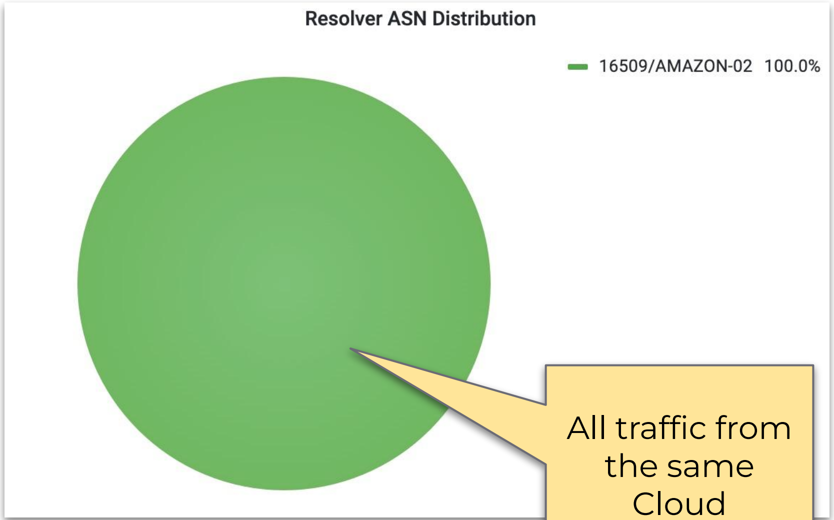
```
": {
s": [
"handler_dns
  "filter":
    "only_q
      "elb.xyz.com"
```

Review Deepest Policy data





No traffic for that subdomain before the event



All traffic from the same Cloud Provider

Conclusion: Misconfiguration? Automated QA Testing? Contact vendor.

Thank you

netbox labs

sweyrick@netboxlabs.com

https://orb.community