DNS Monitoring

Hands-on look at observability for authoritative DNS operators

Mark Price
mprice@netactuate.com

Craig Jackson
cjackson@netactuate.com

ICANN79 March 2024

Introduction

What will cover. . .

- Monitoring tools for DNS operators
- Specific hands-on demo with real data
- Github repo with playbooks and dashboards

About NetActuate

NetActuate is an edge infrastructure provider, also known as Anycast.com

ICANN79
March 2024

AS112

DNS-OARC
Domain Name System Operations Analysis and Research Center

- globally distributed sink for reverse DNS queries for private IP ranges
- RFC1918 / RFC3927 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16)
- reduces the load on root name servers by handling queries that should not be answered by the global Internet

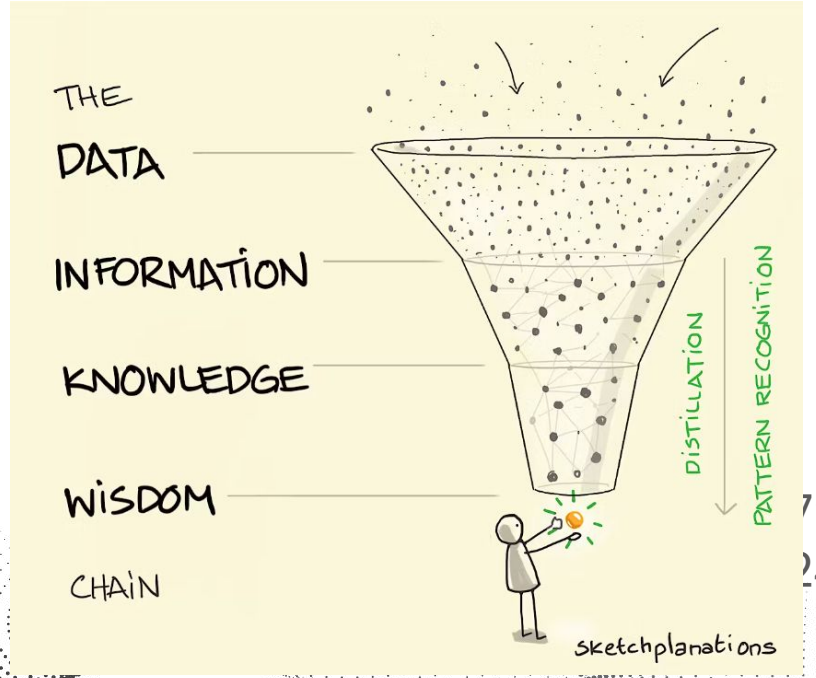
```
; Empty zone for Direct Delegation AS112 service.
;
$TTL 1W
@       IN      SOA     prisoner.iana.org. hostmaster.root-servers.org. (
                                1           ; serial number
                                1W          ; refresh
                                1M          ; retry
                                1W          ; expire
                                1W          ) ; negative caching TTL
;
        NS      blackhole-1.iana.org.
        NS      blackhole-2.iana.org.
;
; There should be no other resource records included in this zone.
;
```

ICANN79
March 2024

What is Observability

classic definition of: logs, metrics and traces

- Visibility of the infrastructure
- Collect + aggregate data
- Understandable and actionable view



Monitoring

Internal

Collect all data from our fleet, centralize and report

External

Monitoring from outside our perimeter to assess real-world response & availability

NN79
2024

External Monitoring of the DNS service

Commercial Options (Catchpoint, ThousandEyes, many others)

Perfops

Freemium

300+ nodes

Globalping

Free

simple & easy

900+ nodes

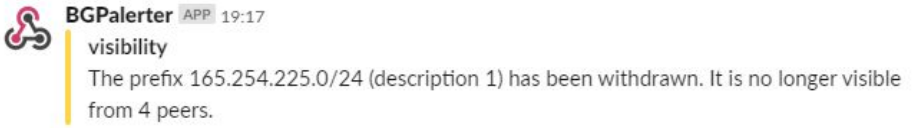
RIPE Atlas

slightly more complex

Earn credits to use

11,000+ nodes

External monitoring of BGP
(announcements, AS adjacencies, hijacks, IRR, RPKI ROAs)



DNS incidents are often the result of a network issue

https://github.com/nttgin/BGPalerter (OSS)

https://packetvis.com/ (Freemium)

https://bgp.tools/ (£25 monthly for commercial use)

Cisco Crosswork (f/k/a BGPMon.net)

ThousandEyes

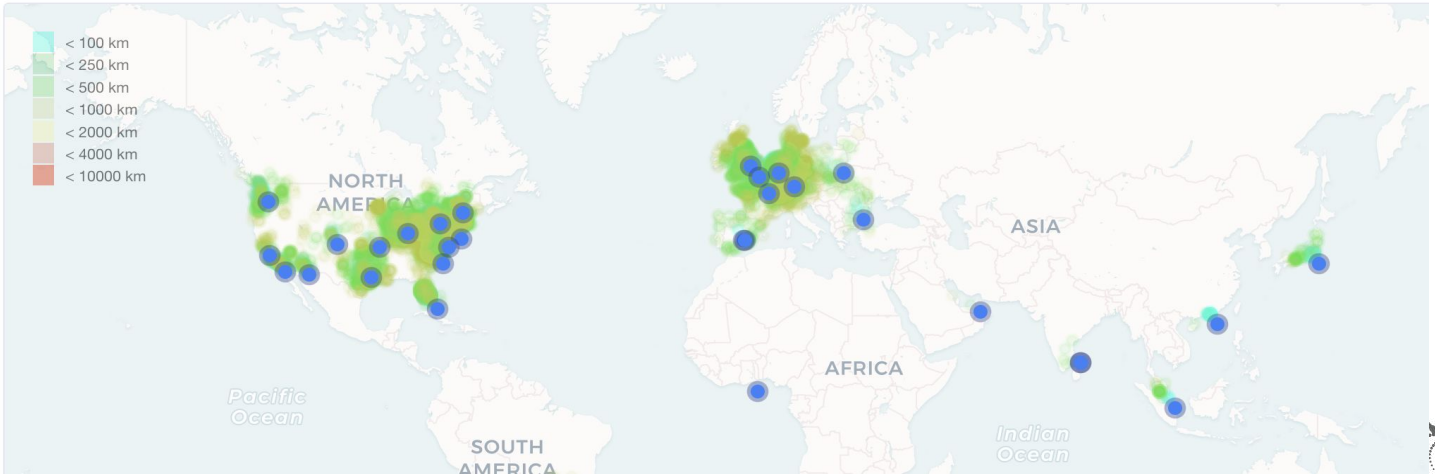
Internal Monitoring: Why and How

- Lots of noise and weird stuff
- Usually not practical to log _every_ query
- Understand if an anomaly is odd or serious (attack)
- Understand norms and baselines
  - from many points of view
- Dashboards available to analyze and correlate events
- Capacity planning

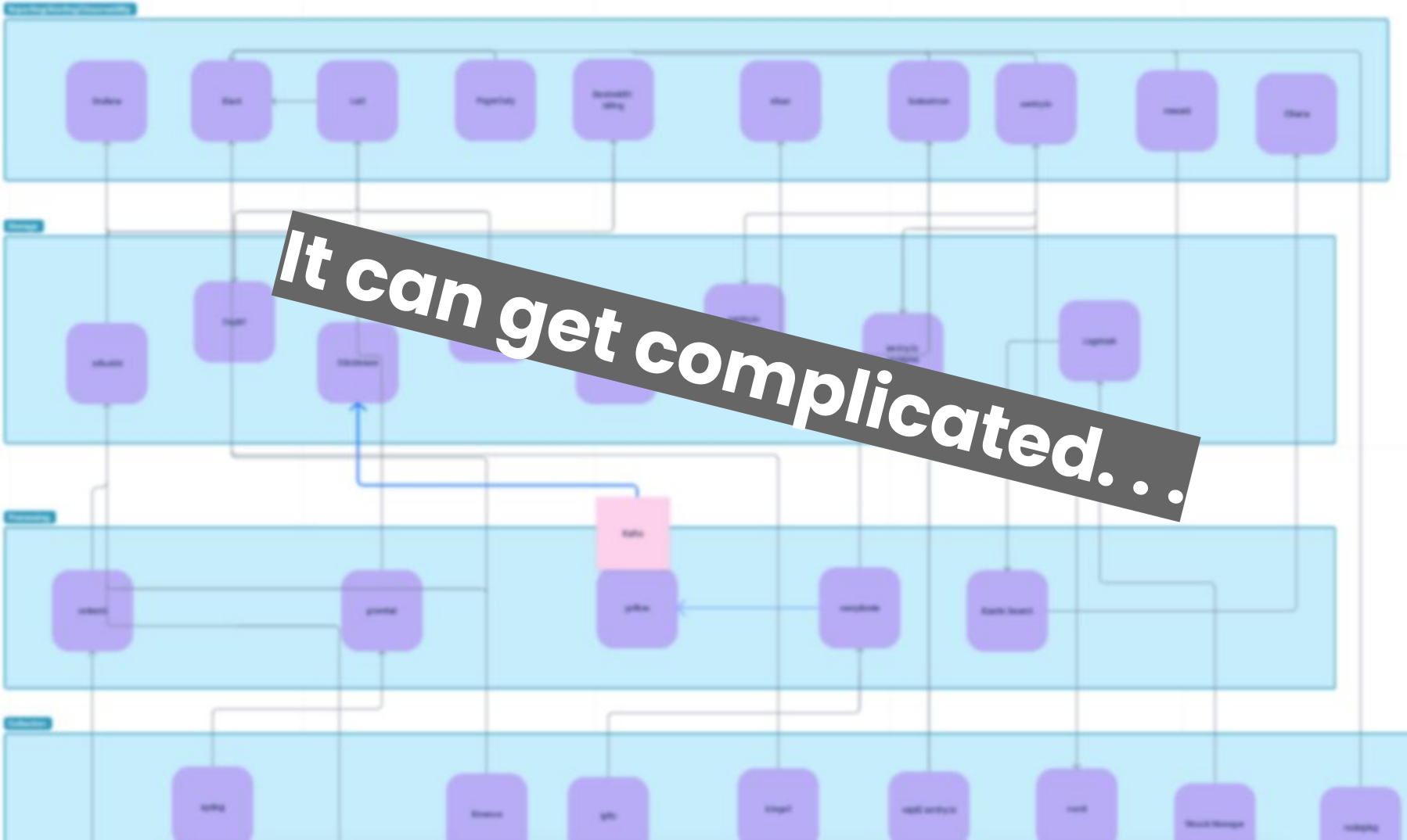
Internal Monitoring: Our Environment & Goals

Global deployment of Linux VMs + KnotDNS, orchestrated by Ansible
Objectives

- deploy a monitoring layer
- open source software
- simple (install / operate / maintain)



ICANN79
March 2024


It can get complicated. . .

Data Stack

Data Collection Agent	Time Series DB	Visualization
Telegraf →	InfluxDB →	Grafana
collectd	Graphite	Kibana (ELK)
statsd	Prometheus	
Prometheus Exporter	TimescaleDB	
Filebeat / Logstash	RRD files	
	Elastisearch	

Alerting ! !

Alerts can come from parts of our proposed data stack

InfluxDB (v2)

Grafana

Or a separate alert-focused tool such as Icinga or Nagios

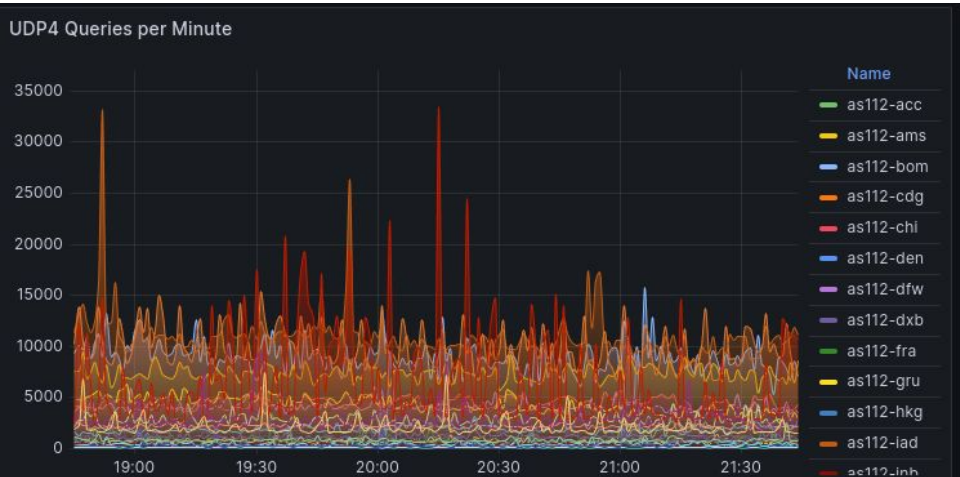
What It Looks Like

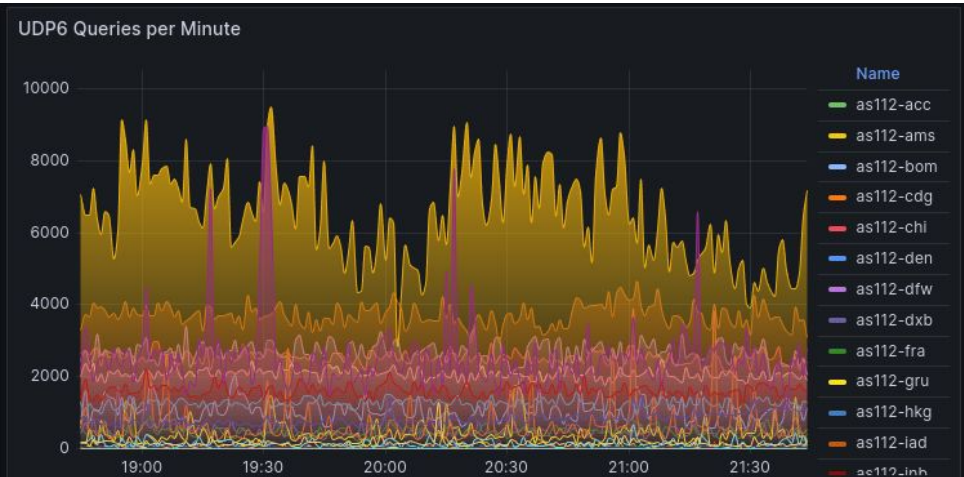
Live look at the dashboards

https://as112.anycast.com

user guest

- AS112 KnotDNS Stats (Global overview)
- Node Diagnostic (Deep dive per node)
- Regional QPS (View within each region)
- Region Comparison
- Resource Usage Top5 (Hardware resources)





How to build it

1. Install Influx
2. Install Grafana
3. Set some variables & run playbook

knotinstall.yaml 6.51 KiB

Blame | Edit | Replace | Delete

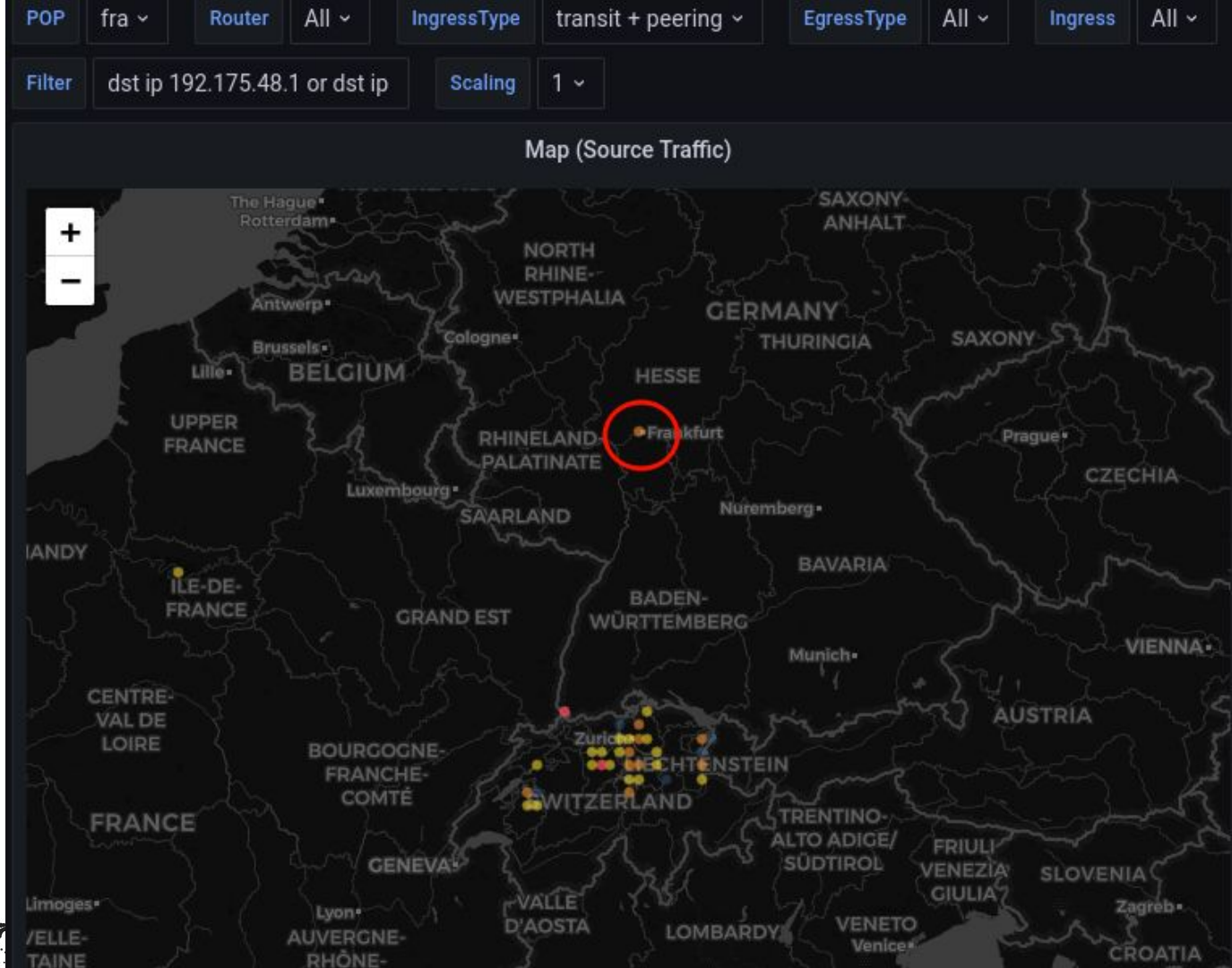
```yaml
---
- name: Install KNOT DNS Auth, Telegraf, and configure Telegraf for knot
  hosts: nodes
  become: yes
  vars:
    telegraf_version: "latest"  # Replace with the desired version or leave it as 'latest'
    local_folder_path: "./templates"  # Replace with the path to your db files on the Ansible control node
    influx_url: "http://[redacted]:8086" # Replace with your InfluxDB2 URL
    influx_token: '[redacted]' # Replace with your telegraf data sou
  tasks:
    - name: Add KNOT DNS repository
      ansible.builtin.apt_repository:
        repo: 'ppa:cz.nic-labs/knot-dns-latest'
```

Netflow / sflow consideration

- More work, but worth considering a flow monitoring stack as well for network-centric view
- Netflow data can be collected if you have routers, or an agent can run in the Linux servers
- Telegraf has sflow collector plugin
- Collects source IPs which is currently missing from our data stack
- Common choice for DDoS detection

Netflow example

Netflow
goflow
MaxMind GeoIP
Clickhouse db
Grafana



Further Reading

- our playbook: https://github.com/netactuate/as112-knotdns-data/
- Telegraf
- InfluxDB2 & Grafana Getting Started: https://medium.com/@nanditasahu031/integration-of-influxdb2-with-grafana-28b4aebb3368

Questions?

email: mp@netactuate.com