

¿Qué estará haciendo el DNS en este momento? ©

Santiago Aggio
Conicet, UTN-FRBB

FTL 2022, LACNIC 37
Ciudad de Cali
Mayo de 2022

Objetivos

- DNS es un servicio de infraestructura crítica
 - ¿Por qué no corremos nuestra propia instancia?
 - ¿Tenemos plano de control?
 - ¿Qué infraestructura necesitamos?
 - ¿Recursivos, autoritativos y... DNS-over-HTTPS?
- ¿Y lo estamos monitoreando? ¿Cómo?
Veremos una forma de hacerlo en tiempo real

Tipos de DNS: Recursivos

- Proveedores usan en sus clientes recursivos públicos como implementación inicial y.... permanente!!!!.
 - “Tercerizamos” el servicio y perdemos captura de tráfico
 - Menor control y capacidad de monitoreo
 - Menor capacidad de resolución de problemas
- No recomendable en servidores de alta demanda de resolución (Ej: Mail server con mecanismos antispam)

Tipos de DNS: Recursivos Públicos

Google

8.8.8.8

8.8.4.4

2001:4860:4860::8888

2001:4860:4860::8844

OpenDNS

208.67.222.222

208.67.220.220

2620:0:ccc::2

2620:0:ccd::2

Cloudflare

1.1.1.1

1.0.0.1

2606:4700:4700::1111

2606:4700:4700::1001

Quad9

9.9.9.9

149.112.112.112

2620:fe::fe

2620:fe::9

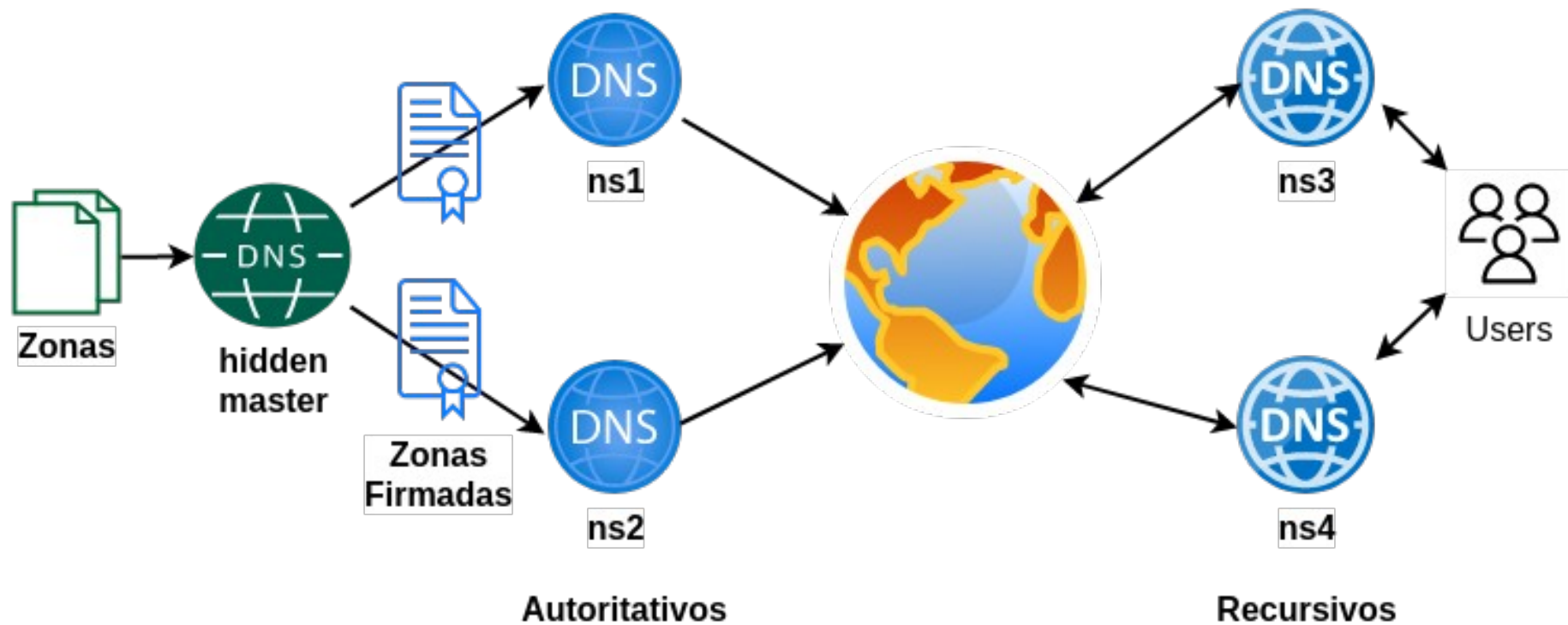
Tipos de DNS: Autoritativos

- Requerido por el RIR para los inversos de los bloques IP delegados (in-addr.arpa, ip6.arpa)
 - Contratamos el servicio
- Zonas propias en directa
- Registros especiales asociados a la zona y dominio
 - SPF, DKIM, DMARC, SIP, etc
- DNSSEC

Infraestructura requerida

- 2 servidores autoritativos
 - Zonas directas registradas e inversas delegadas
- 2 servidores recursivos (resolvers locales)
 - Accesible para las direcciones IP propias (usuarios/clientes)
- 1 servidor para firmar las zonas (DNSSEC)
 - Firma las zonas y las transfiere a los autoritativos
 - Sin acceso desde Internet para preservar claves

Infraestructura requerida



¿Cómo podemos medir?

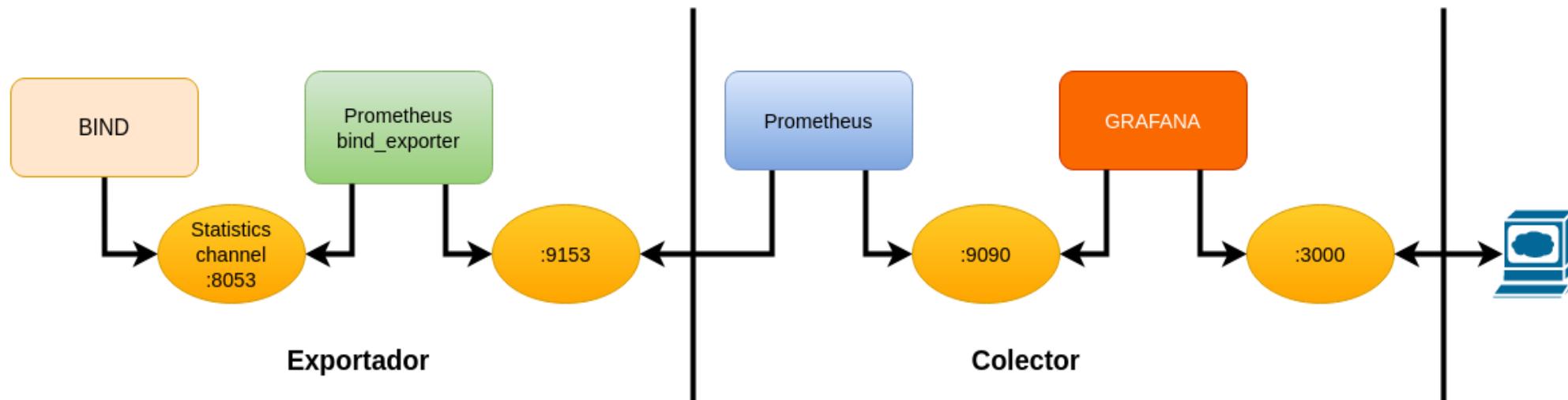
- Capturamos tráfico en una interfaz
 - Con tcpdump (port 53) generamos archivos pcap para posterior procesamiento (Investigación)
- IPFIX
 - Softflowd: flujos (Netflow / IPFIX) exportados a un colector
- Procesando logs con scripts o con herramientas de análisis
 - Fluentd / Logstash + Elasticsearch + Kibana
- RIPE Atlas DomainMON (<https://atlas.ripe.net/domainmon/>)

Implementación

- Bind
 - statistics channel enabled
- Prometheus
 - bind_exporter en cada DNS
- Prometheus
 - Colector Centralizado
- Grafana
 - Visualización con data source desde Prometheus



Implementación



BIND 9 Statistics



- 8 secciones de estadísticas en versión 9.16.25
 - Incoming Requests, Incoming Queries, Outgoing Queries, Name Server Statistics, Zone Maintenance Statistics, Resolver Statistics, Cache DB RRsets Statistics, Socket I/O Statistics
- Cada sección provee un gran número de contadores de estadísticas de diferente tipo
- Salida en formato xml y json
 - `curl http://localhost:8053/json`

BIND 9 Statistics



```
curl http://localhost:8053/json 2>/dev/null | jq '.zonestats'
```

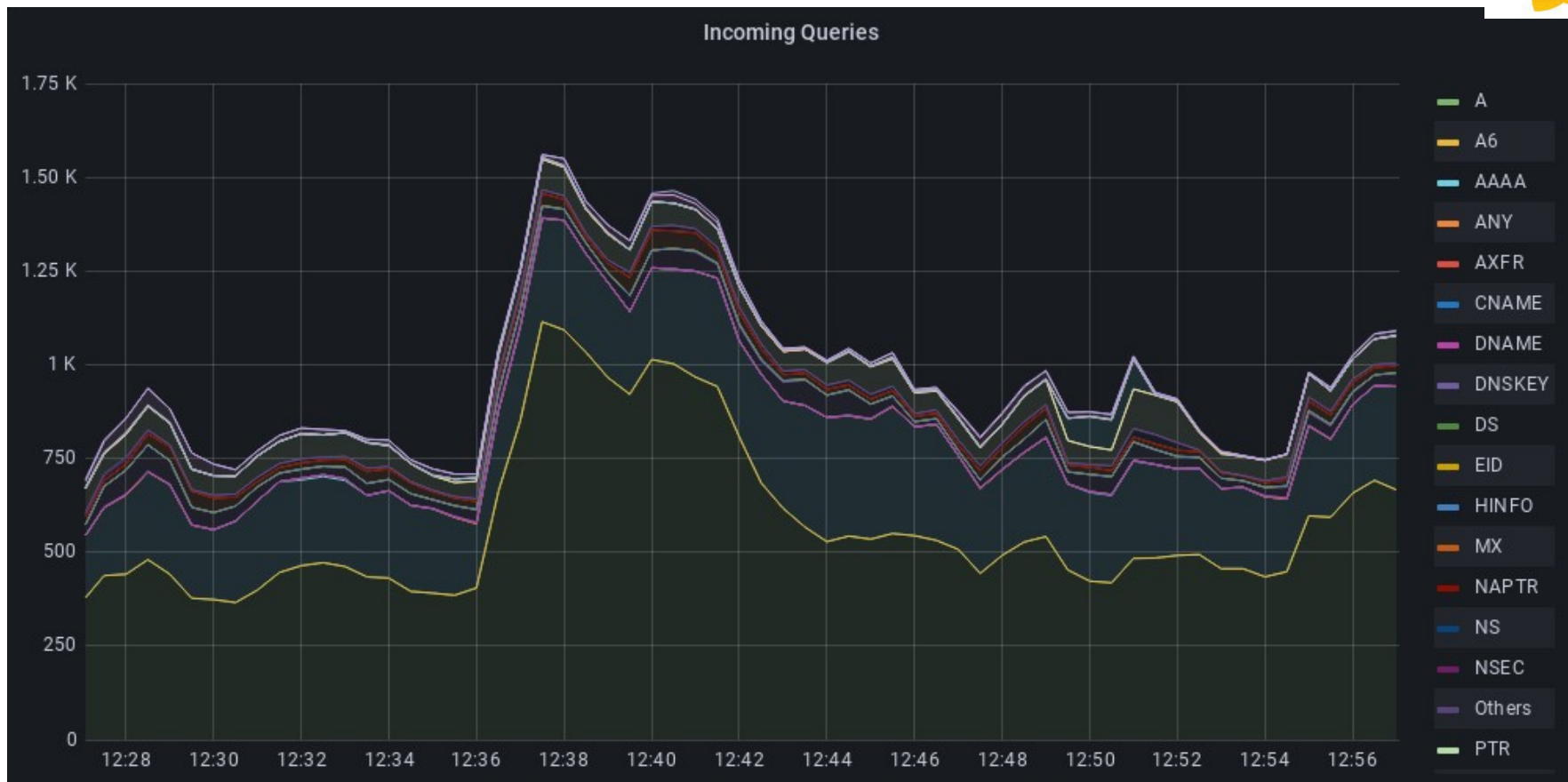
```
{  
  "NotifyInv4": 144,  
  "NotifyInv6": 144,  
  "NotifyRej": 30,  
  "SOAOutv4": 7861,  
  "SOAOutv6": 13029,  
  "AXFRReqv4": 20,  
  "AXFRReqv6": 73,  
  "IXFRReqv4": 128,  
  "IXFRReqv6": 4457,  
  "XfrSuccess": 4585,  
  "XfrFail": 93  
}
```



Vista en Grafana

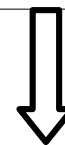


Vista en Grafana

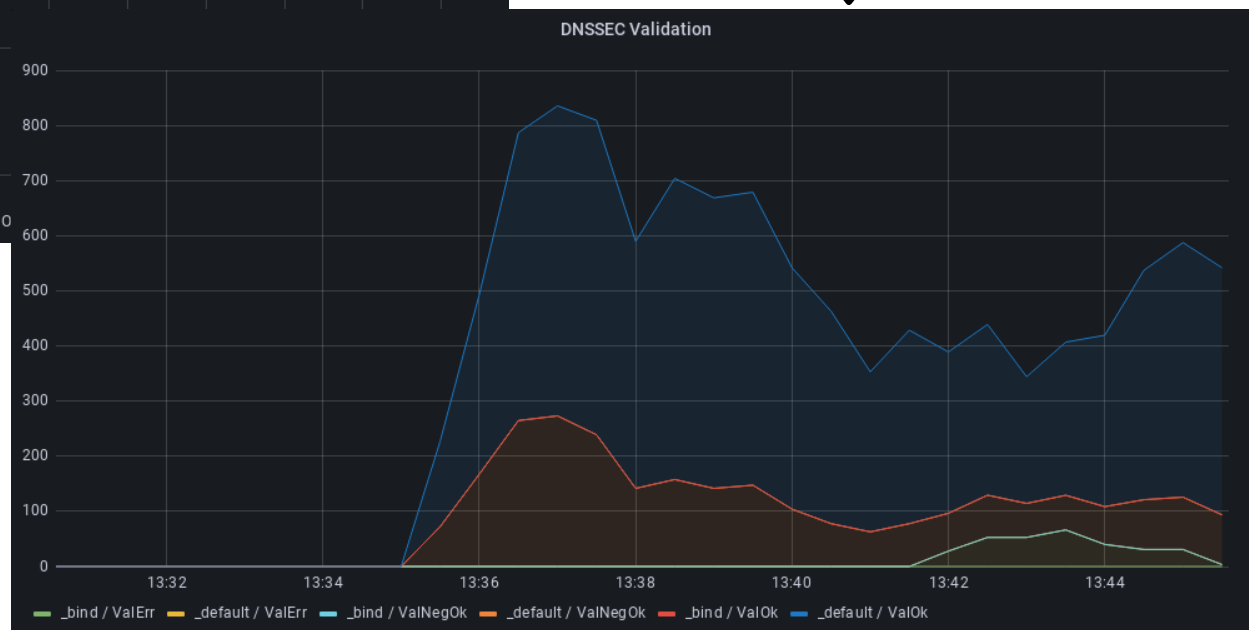
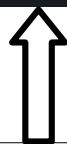




Con validación dnssec

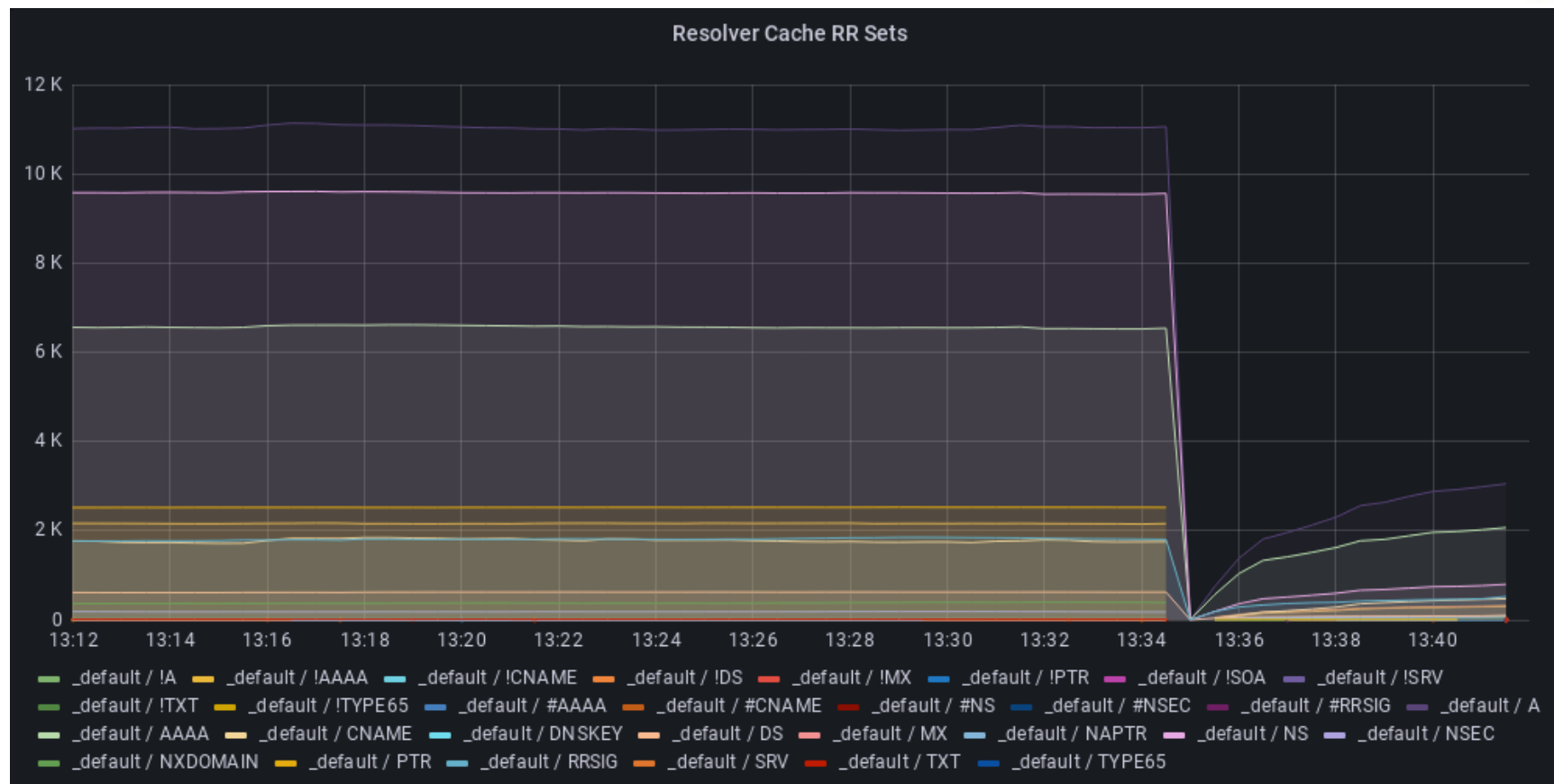


Sin validación dnssec






Vista en Grafana

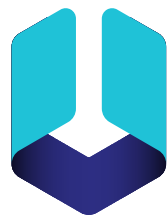




unbound

- Desarrollado por  **NLNETLABS**
- Recursivo “liviano” de alta prestación
- Configuración simple y amigable
- Utilitarios de control para administración remota
- Estadística mediante contadores
- Soporta DNS-over-HTTPS

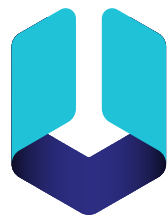




unbound



- Monitoreo por terceras partes: Cacti, Munin
- Monitoreo desde Prometheus
 - <https://github.com/svartalf/unbound-telemetry>
 - https://github.com/letsencrypt/unbound_exporter
- Grafana dashboard:
<https://grafana.com/grafana/dashboards/11705>



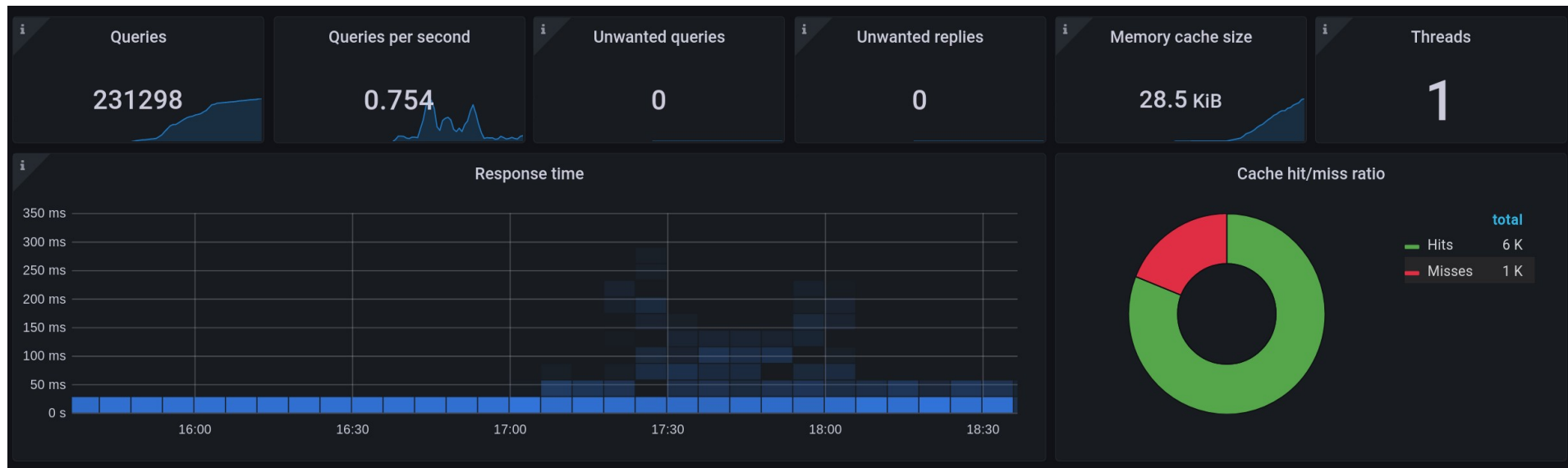
unbound



```
$ unbound-control stats_noreset | grep num.query.type  
num.query.type.A=5261  
num.query.type.PTR=2133  
num.query.type.MX=755  
num.query.type.TXT=4  
num.query.type.AAAA=2711  
num.query.type.SRV=3
```

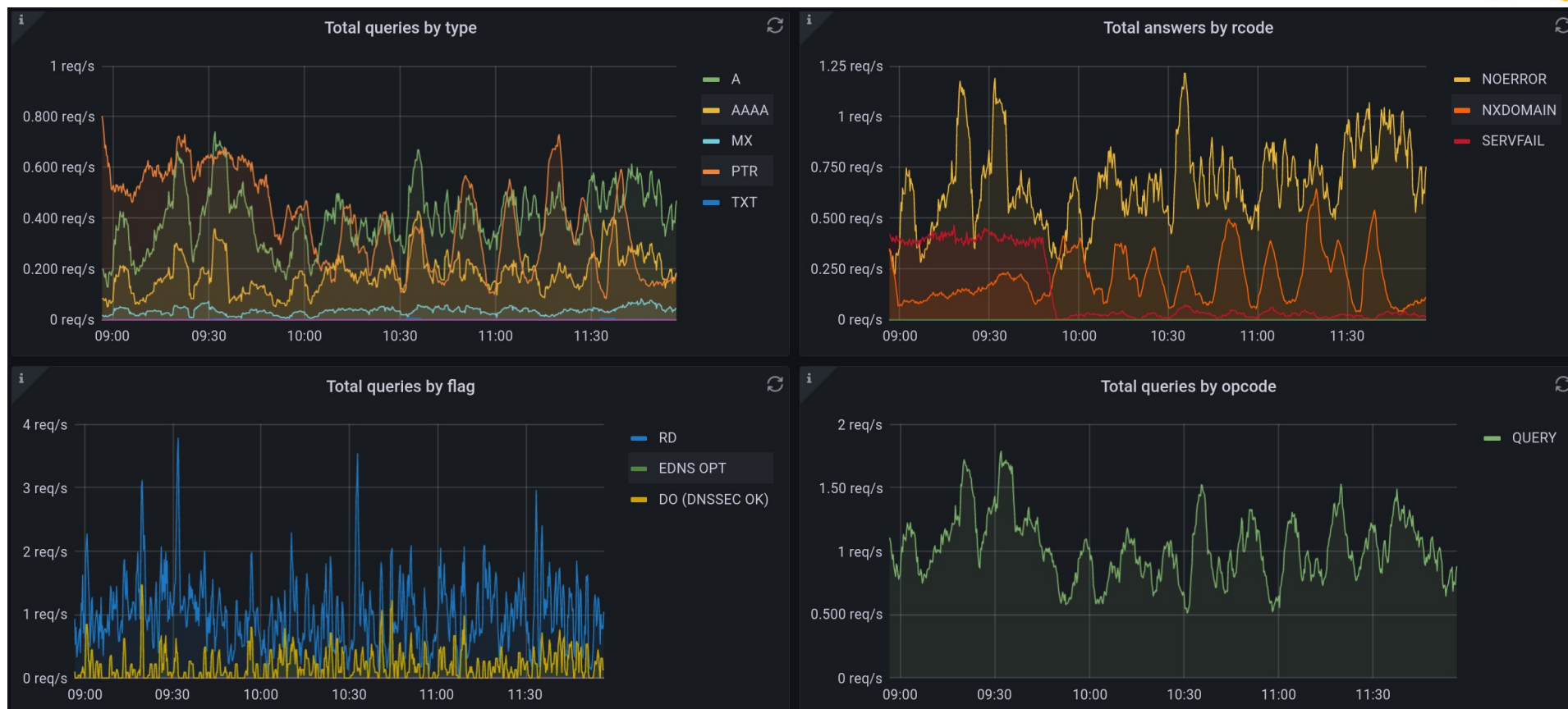


Vista en Grafana





Vista en Grafana



Conclusiones

- Es recomendable implementar servidores DNS recursivos y autoritativos en la propia infraestructura
- Aprovechamos el canal de estadística y contadores disponibles en Bind y Unbound para obtener más información
- Prometheus + Grafana proveen una vista de la métrica del servicio en tiempo real
- Es un complemento a las mediciones y detecciones obtenidas a partir del análisis de paquetes, flujos IP y logs

Referencias

- Bind9. <https://www.isc.org/bind/>
- Prometheus bind_exporter.
https://github.com/prometheus-community/bind_exporter
- Prometheus colector. <https://prometheus.io/>
- Grafana. <https://grafana.com/grafana/>
- Grafana Dashboard.
<https://grafana.com/dashboards/12309>

Referencias

- “¿Qué estará haciendo ‘X’ en este momento?”

©. CQC,

- [https://es.wikipedia.org/wiki/Caiga_quien_caiga_\(Argentina\)](https://es.wikipedia.org/wiki/Caiga_quien_caiga_(Argentina))



- <https://memegenerator.net/instance/51870466/homer-simpson-1-doh>

¿Preguntas?

Muchas Gracias

slaggio@criba.edu.ar

Especial agradecimiento a Lacnic!!!!