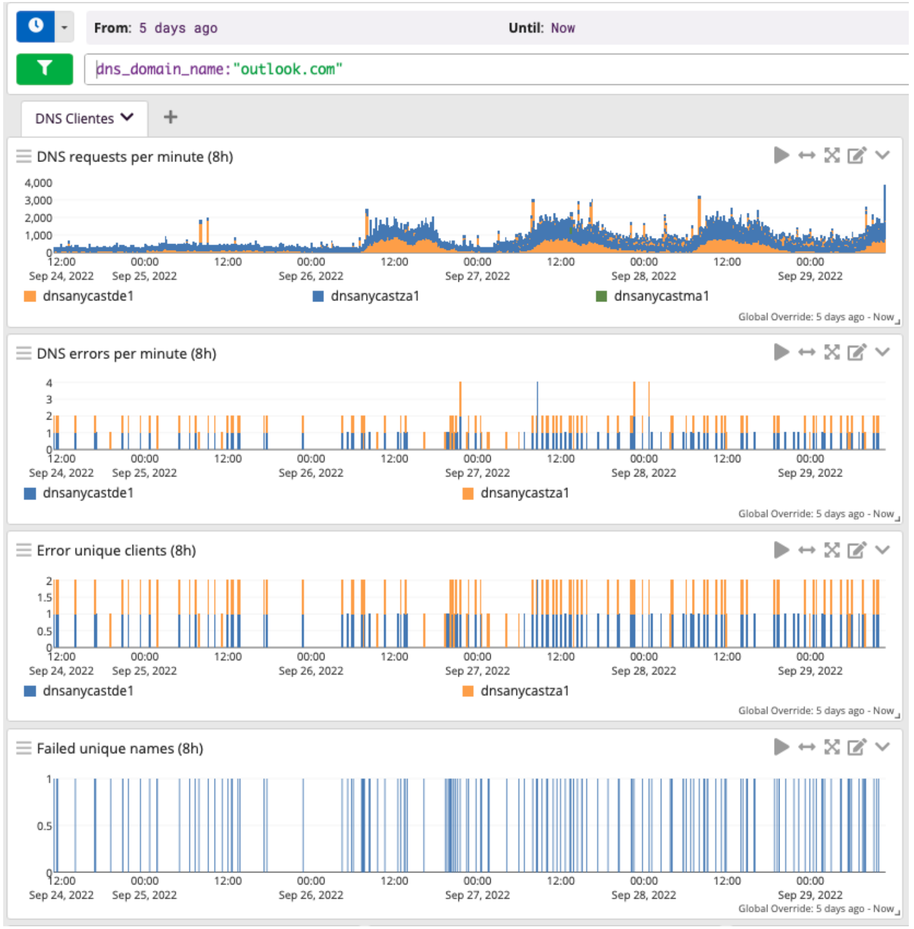
DNSTAP

Borja Marcos.
borjam@sarenet.es

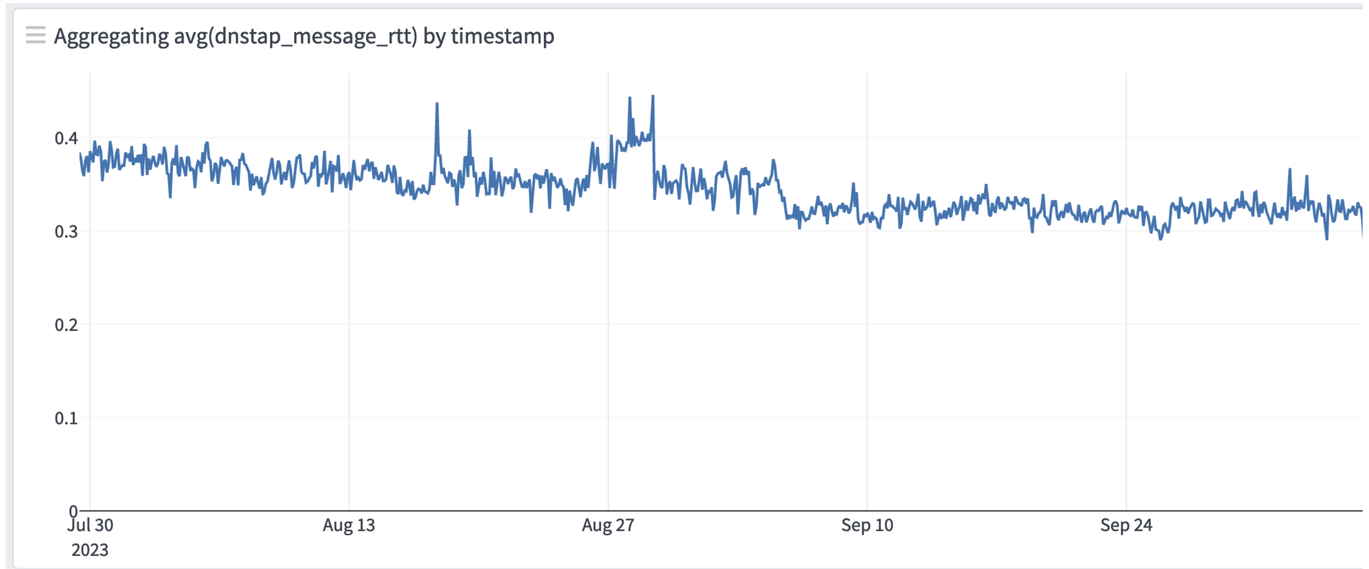
¿Por qué monitorizar el DNS?

- It’s always DNS!
- DNS pasivo
- Seguimiento de experiencia de usuario
- Radar más allá del horizonte

Monitorizando un dominio



¿Cómo funciona mi caché?



Syslog

Grok pattern

Pattern

```
%{WORD:dns_log_category}: client @%{DATA}
%{IP:dns_client_addr}#%{BASE10NUM:dns_client_port} \(%{DATA}\):
(view: %{USERNAME:view_name} )?query:
%{USERNAME:dns_req_name} %{WORD:dns_query_family}
%{WORD:dns_rrtype} %{DATA} \(%{IP:dns_server_addr}\)
```

Pcap

- Decodificar paquetes
- Deducir información de estado
- Complejidad

DNSTAP

https://dnstap.info

- Información emitida por el propio servidor DNS -> Tenemos información de estado
- Mecanismo independiente de versión/autor de DNS
- Basado en protobuf
- Desglose de actividad (todos los modos de diálogo)

Ejemplo de mensaje: RR

dnstap_message_query_family
IN

dnstap_message_query_id
17272

dnstap_message_query_name
194.251.205.origin.asn.cymru.com.

dnstap_message_query_port
41174

dnstap_message_query_rcode
NOERROR

dnstap_message_query_rrtype
NS

dnstap_message_query_time
2023-10-06 21:15:01.580

dnstap_message_query_zone
asn.cymru.com.

dnstap_message_response_address
216.31.12.17

dnstap_message_response_message

```
;; opcode: QUERY, status: NOERROR, id: 17272
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;194.251.205.origin.asn.cymru.com.      IN       NS

;; AUTHORITY SECTION:
asn.cymru.com.  900     IN      SOA     ns1.asn.cymru.com. noc.cymru.com. 1696616400 1800 900 86400 900
```

dnstap_message_response_port
53

dnstap_message_response_time
2023-10-06 21:15:01.680

dnstap_message_rtt
99.866196

dnstap_message_socket_family
INET

dnstap_message_socket_protocol
UDP

dnstap_message_type
RESOLVER_RESPONSE

dnstap_type
MESSAGE

Algunas limitaciones

- Exige adopción por parte de desarrolladores de software de DNS
- Relación 1:1 entre paquetes de red y paquetes Dnstap
- Exige ser cuidadoso con la privacidad

Disponibilidad

- Bind 9.17/9.18: Implementación completa excepto tiempo de respuesta en CR
- Unbound: Marcas de tiempo menos precisas (pone marca de tiempo al enviar paquete Dnstap) y no calcula tiempos de respuesta
- Disponible en Knot, PowerDNS y otros pero no lo he probado.
- Código de referencia en Go disponible: https://github.com/dnstap/golang-dnstap