“DNS Flag day”

El fin de los parches provisorios para EDNS

Hugo Salgado, .CL
Sebastián Castro, .NZ

LACNOG 2018, Rosario, Argentina

nic chile
SOMOS EL PUNTO CL

InternetNZ

¿De qué se trata?

“El próximo 1° de febrero de 2019, los cuatro principales proveedores de software para DNS recursivos -Bind, Unbound, PowerDNS y Knot- realizarán un lanzamiento conjunto de nuevas versiones de sus sistemas con una característica en común: el fin de parches provisorios históricos que perdonaban ciertas conductas desviadas del estándar en los servidores DNS autoritativos.”

De http://blog.nic.cl/2018/06/dns-flag-day-el-fin-de-los-parches.html

¿Qué es EDNS?

- RFC 6891: Extension Mechanisms for DNS (EDNS(0))
  - Define un mecanismo compatible con DNS para indicar soporte para nuevas opciones
  - Especificación original incluye soporte para paquetes más grandes (sobre 512 bytes), más códigos de respuesta, etc.

¿Para qué sirve?

Extensiones:

- **NSID** -- RFC 5001: identificación de instancia del servidor
- **DNSSEC** -- bit DO: por favor, responda con registros DNSSEC
- **Client-subnet**, RFC 7871: desde qué red viene esta consulta?
- **Keep-alive**, RFC 7828: timeout variable para DNS sobre TCP.
- **Cookies**, RFC 7873: mecanismo liviano de seguridad.
- Y más en el futuro...

¿Cuál es el problema actual?

- DNS autoritativos que bloquean respuestas
- Malas implementaciones de DNS que no siguen los estándares.
- Firewalls mal implementados o malas políticas que bloquean tráfico que sigue los estándares.

DNS resolvers tienen que esperar timeout y reintentar con TCP o sin EDNS

=> DELAYs y dificultad en innovación

¿Cuál es la solución?

1. Campaña “DNS flag day” para corregir los DNS con problemas.
2. Eliminar workarounds en forma coordinada.
3. ¡Que el dolor lo sienta el que lo causa!
    a. algunos dominios podrían dejar de funcionar

Mediciones del impacto

¿Cómo se hace la medición?

- Herramienta “DNS Compliance Testing” escrita por ISC https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing

- Dada una lista de dominios y sus servidores de nombre, verifica por conformidad con los estándares de DNS
  - Nosotros ejecutamos el subset de pruebas de EDNS

- Herramienta “EDNS Compliance scanner for DNS zones” de CZ.NIC para preprocesar la zona de cada TLD y reducir el número de pruebas
  - Si un servidor tiene mil dominios, no es necesario probar mil veces.

Estadísticas generales

	CL	NZ
Número de dominios	420918 (solo activos)	690807
Número de servidores de nombre únicos	22567	21296
Direcciones IPv4 únicas	22612	21374
Direcciones IPv6 únicas	4007	3294
Servidores dual-stack	3862	4527
Servidores solo con IPv4	18572	16532
Servidores solo con IPv6	133	237

¿Cómo se interpretan los resultados?

- En un ccTLD, es factible encontrar dominios mal configurados, lame delegations, servidores que no responden a tiempo, etc.

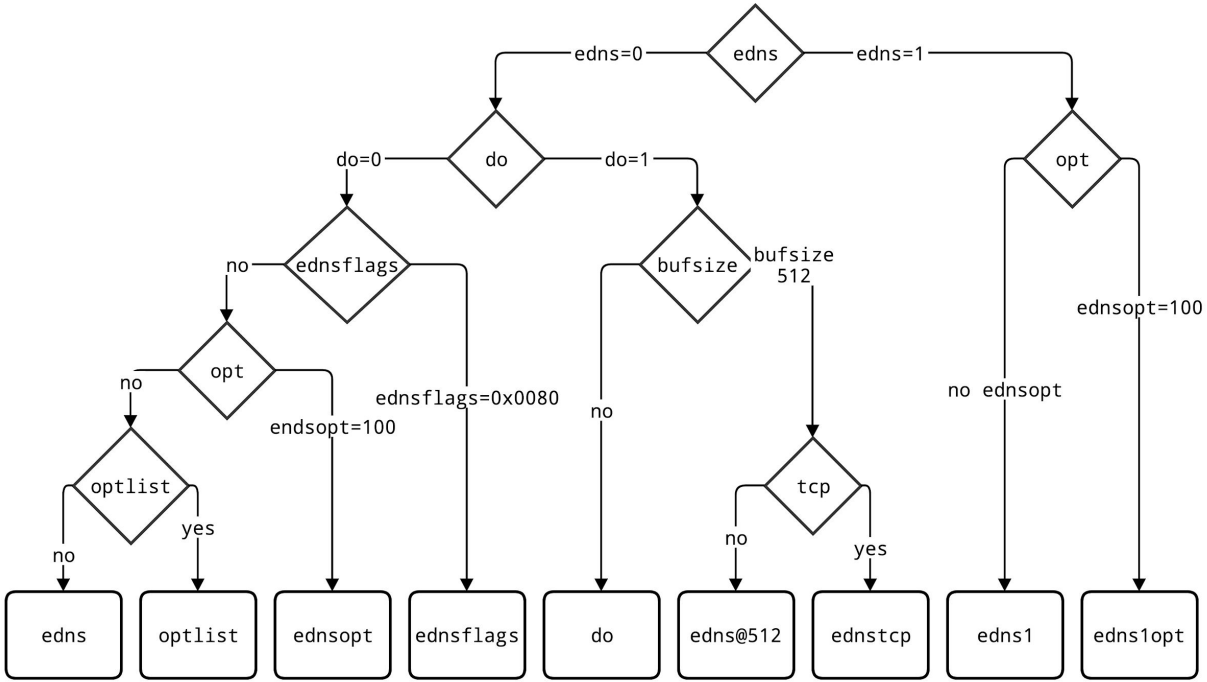
- No todos los tests funcionan

- Existe una jerarquía de tests
  - Si el test de DNS básico falla, es muy probable que el test de EDNS básico falle también

Jerarquía de pruebas

Diferentes valores de la consulta se alteran para probar diferentes componentes

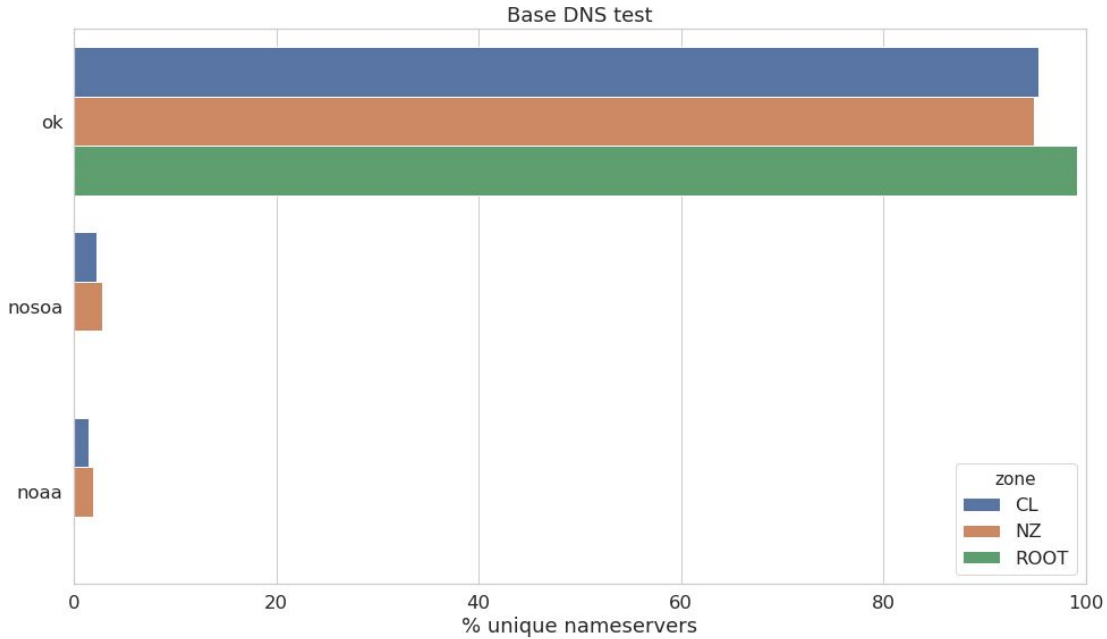
Existen dependencias, ciertos tests son más complejos.



Resultados de prueba de DNS

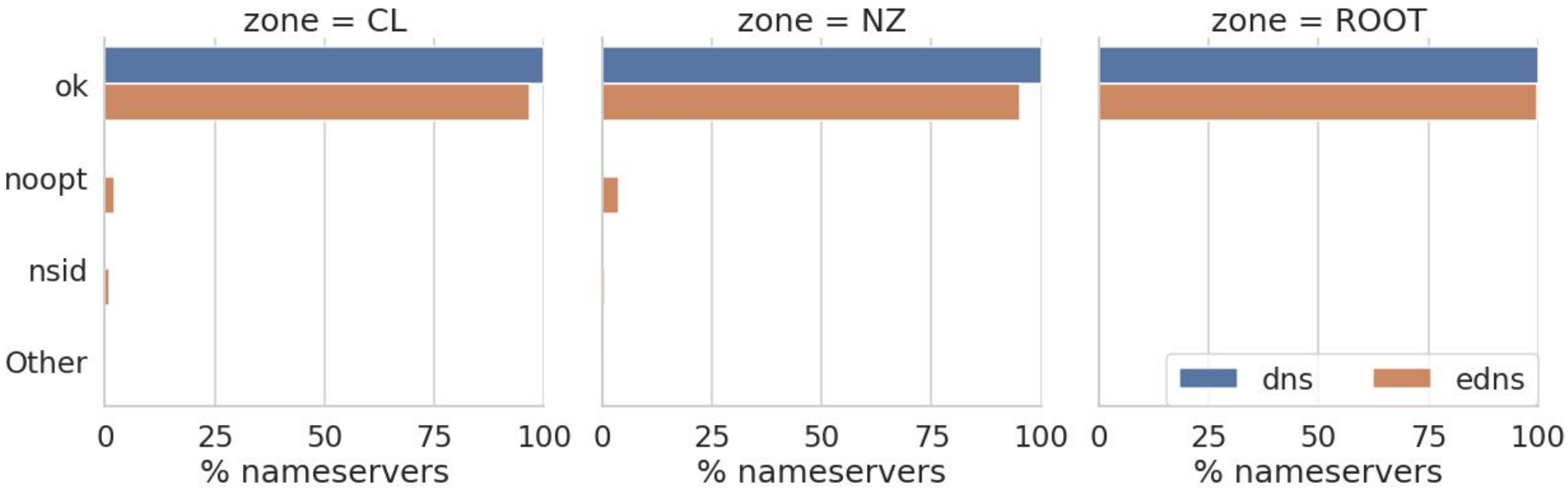
dig +noedns +noad +norec SOA <ZONA>

- ok: Llegó respuesta satisfactoria
- refused: Código de respuesta REFUSED
- timeout: Respuesta no llegó a tiempo
- nosoa: Respuesta sin registro SOA
- noaa: Respuesta sin bit AA
- servfail: Código de respuesta SERVFAIL
- other: Otros errores



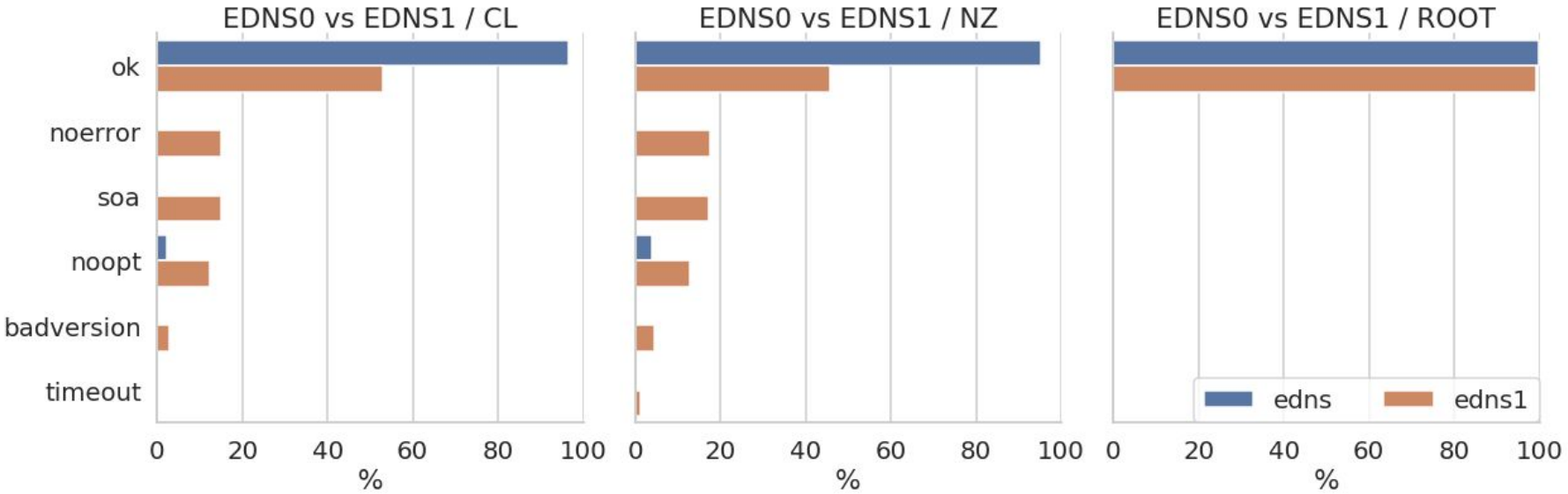
DNS vs EDNS

- DNS: dig **+noedns** +noad +norec SOA <zone>
- EDNS: dig **+edns=0 +nocookie** +noad +norec SOA <zone>



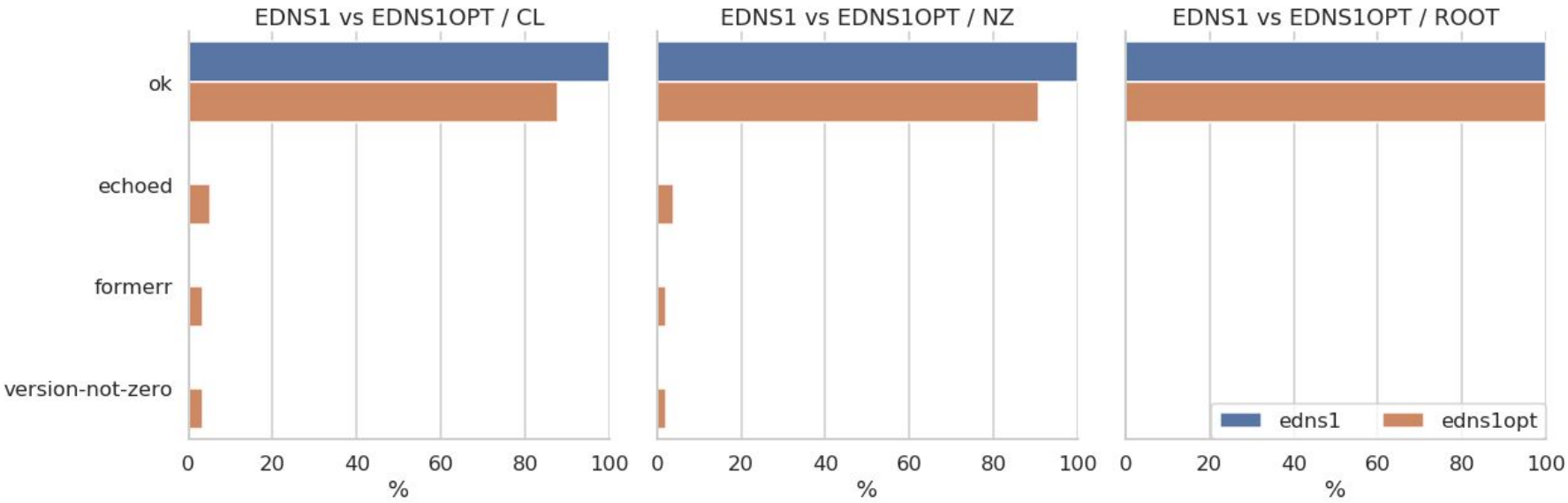
EDNS0 vs EDNS1

- EDNS0: dig **+edns=0** +nocookie +noad +norec SOA <zone>
- EDNS1: dig **+edns=1 +noednsneg** +nocookie +noad +norec SOA <zone>



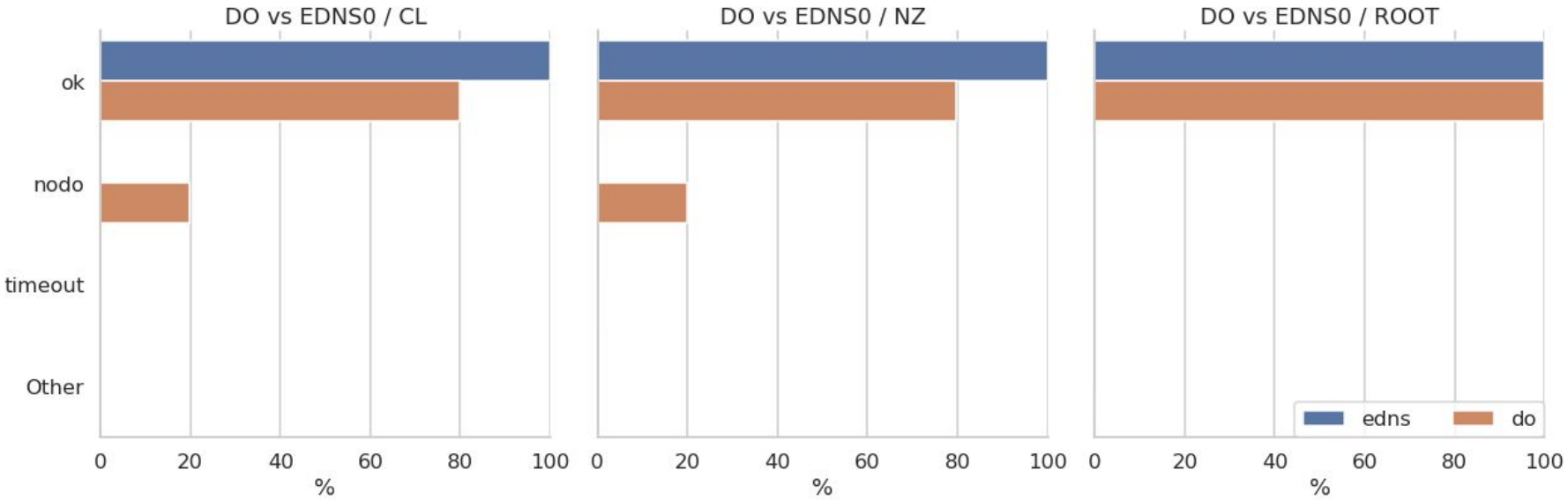
EDNS1 vs EDNS1OPT

- EDNS1: dig +edns=1 +noednsneg +nocookie +noad +norec SOA <zone>
- EDNS1OPT: dig +edns=1 +noednsneg +nocookie +noad +norec **+ednsopt=100** SOA <zone>



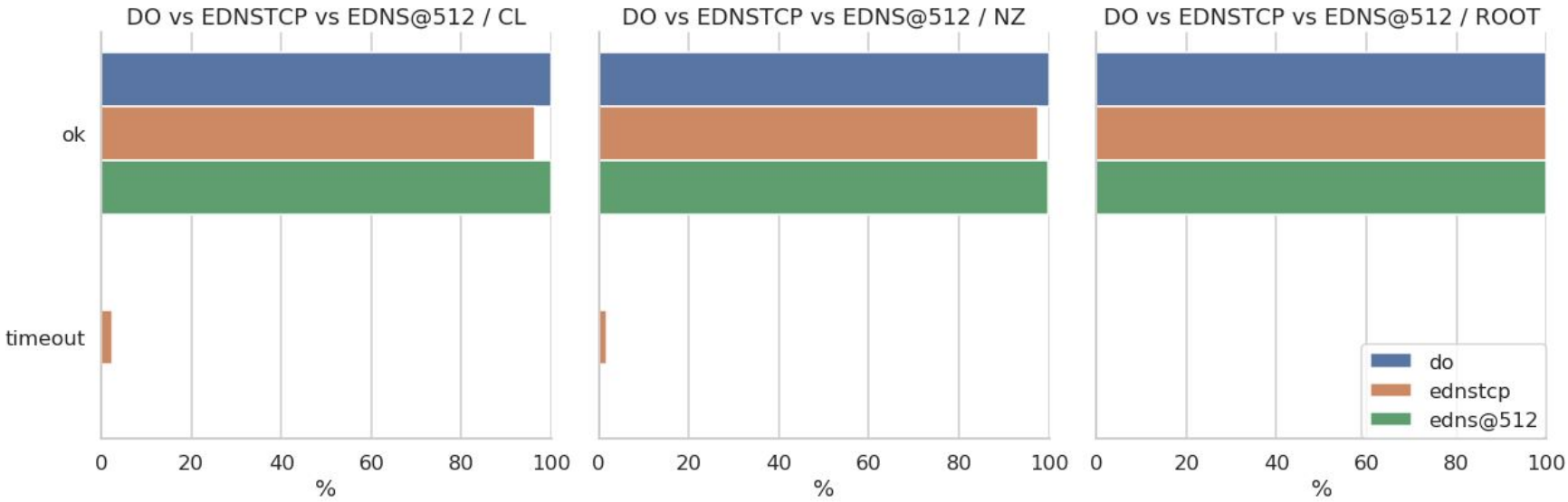
DO vs EDNS

- DO: dig +edns=0 +nocookie +noad +norec **+dnssec** SOA <zone>
- EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>



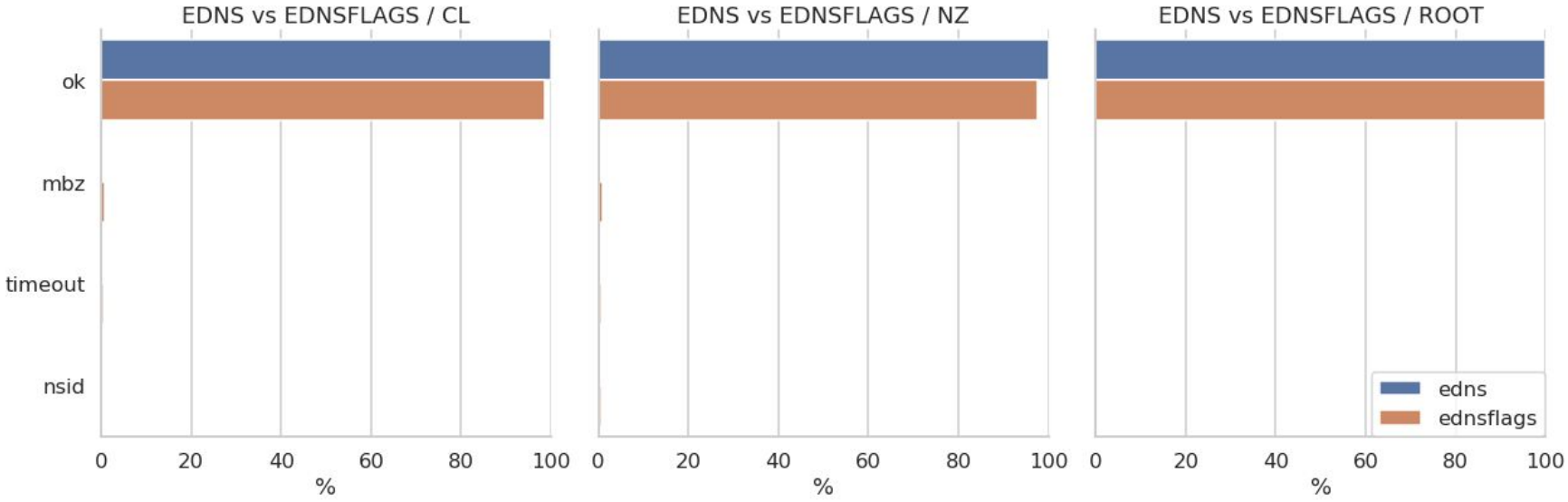
DO vs EDNSTCP vs EDNS@512

- DO: dig +edns=0 +nocookie +noad +norec +dnssec SOA <zone>
- EDNSTCP: dig +edns=0 +nocookie +noad +norec +dnssec **+bufsize=512 +tcp** DNSKEY <zone>
- EDNS@512: dig +edns=0 +nocookie +noad +norec +dnssec **+ignoretc +bufsize=512** DNSKEY <zone>



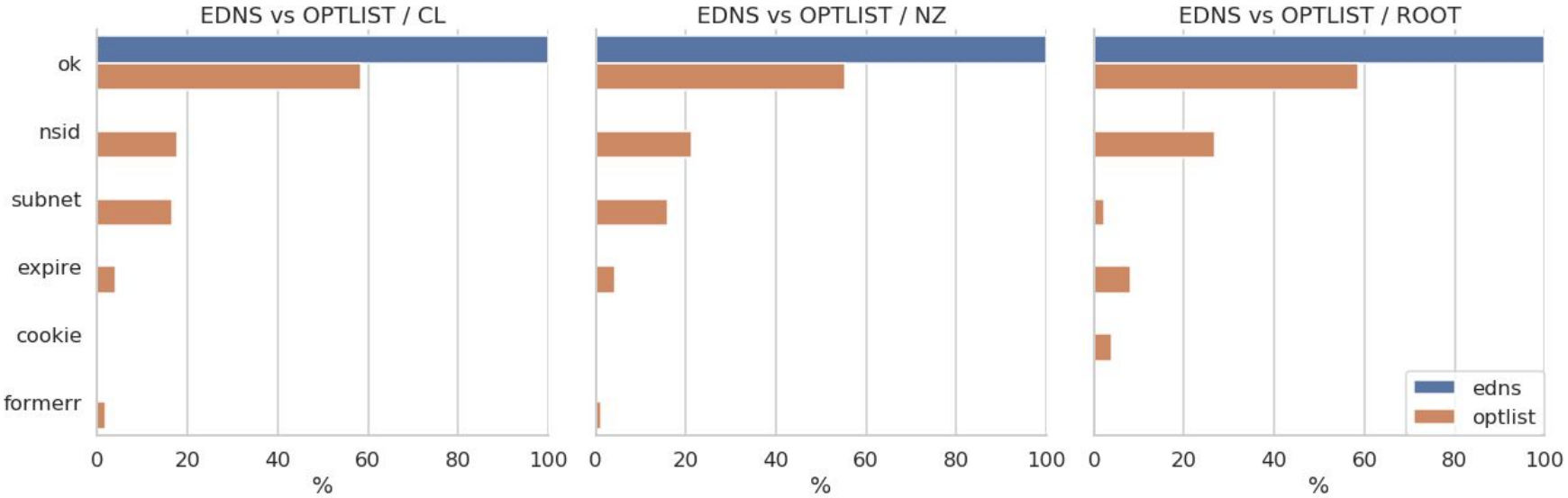
EDNS vs EDNSFLAGS

- EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>
- EDNSFLAGS: dig +edns=0 +nocookie +noad +norec **+ednsflags=0x0080** SOA <zone>



EDNS vs OPTLIST

- EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>
- OPTLIST: dig +edns=0 +noad +norec **+nsid +subnet=0.0.0.0/0 +expire +cookie=0102030405060708** SOA <zone>



Comportamiento por servidor

Cada servidor de nombre debería tener un comportamiento estable

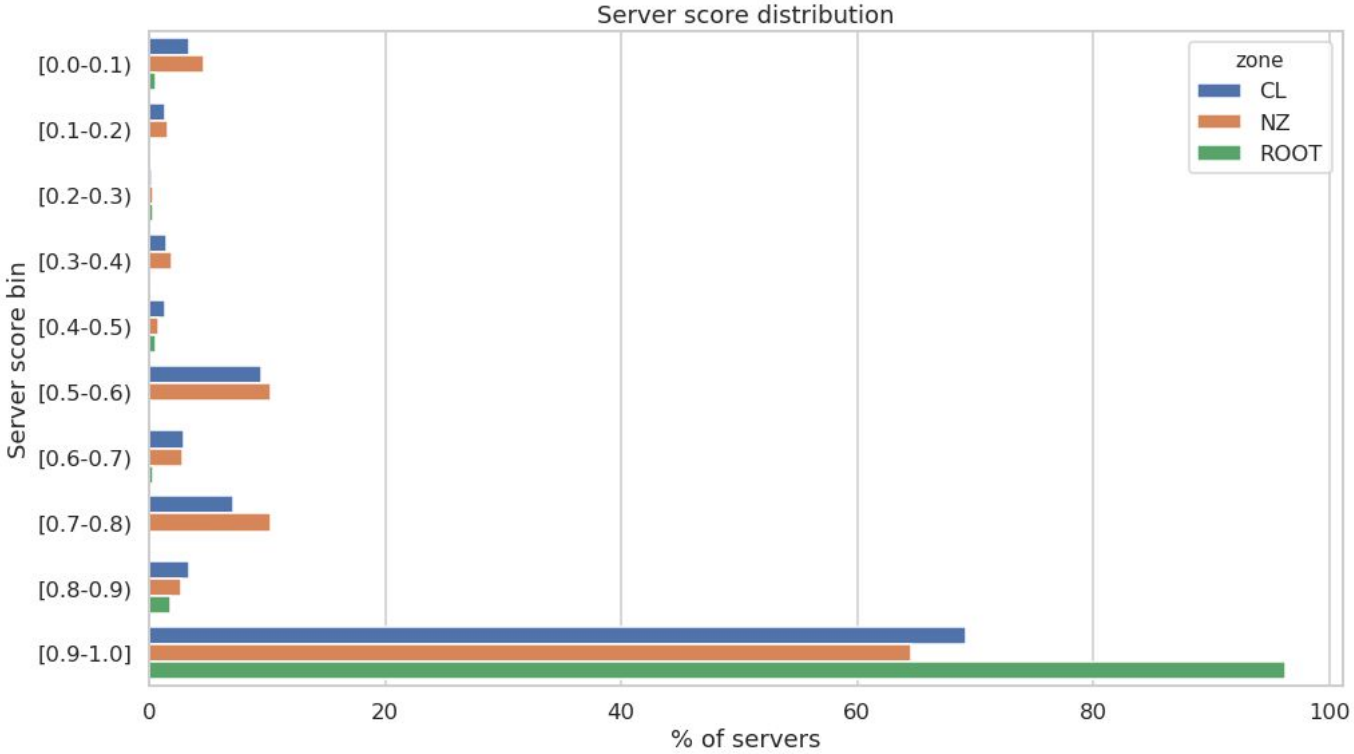
¿Qué pasa si analizamos el comportamiento por servidor, asignándoles un puntaje?

- Cada prueba recibe un puntaje: 0.0 si falló, 0.8 si casi funciona, 1.0 si funciona
- El puntaje de un servidor es el promedio de sus pruebas

Comportamiento por servidor

En general los servidores tienen puntaje sobre 0.5

Los TLDs tienen en general servidores con buena salud.



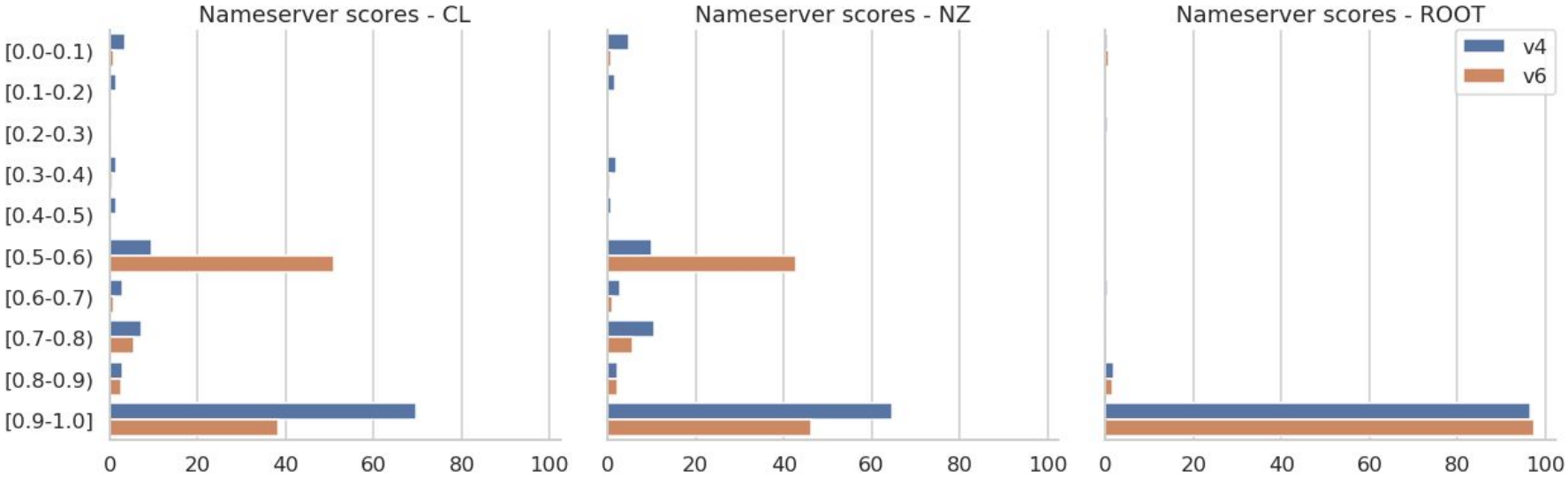
IPv4 vs IPv6

Un servidor de nombres puede tener un comportamiento diferente dependiendo si se consulta su dirección IPv4 o IPv6.

Comparemos en general IPv4 e IPv6

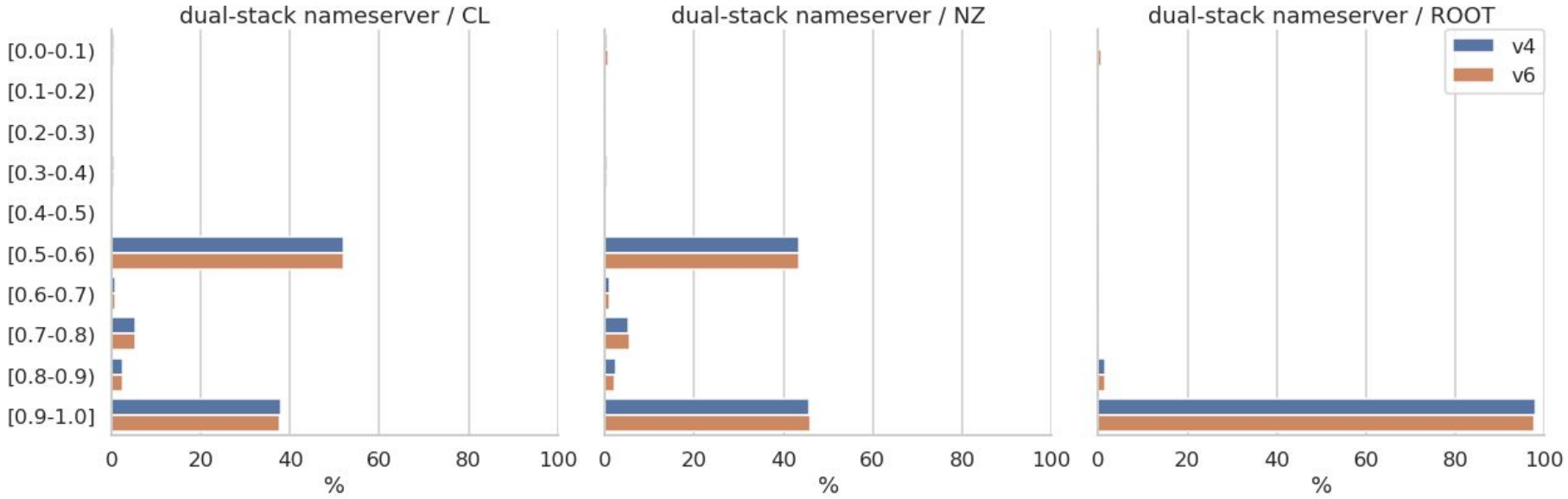
Luego miramos para servidores con ambas direcciones si hay diferencias mayores.

IPv4 vs IPv6: Comparación general



Servidores con IPv6 se comportan peor, alrededor de 20% menos no alcanza el máximo puntaje. ¿Es un problema de IPv6?

IPv4 vs IPv6: servidores dual-stack



Si sólo dejamos servidores que tienen dirección IPv4 e IPv6. No hay diferencia.

Los culpables son los servidores sólo con dirección IPv6.

¿Cómo puedo saber si afecta a mi dominio?

- Hay un sitio web con información y prueba en línea.
  - https://dnsflagday.net

- Colección por parte de ISC
  - https://ednscomp.isc.org
  - Cubre servidores raíz y TLDs

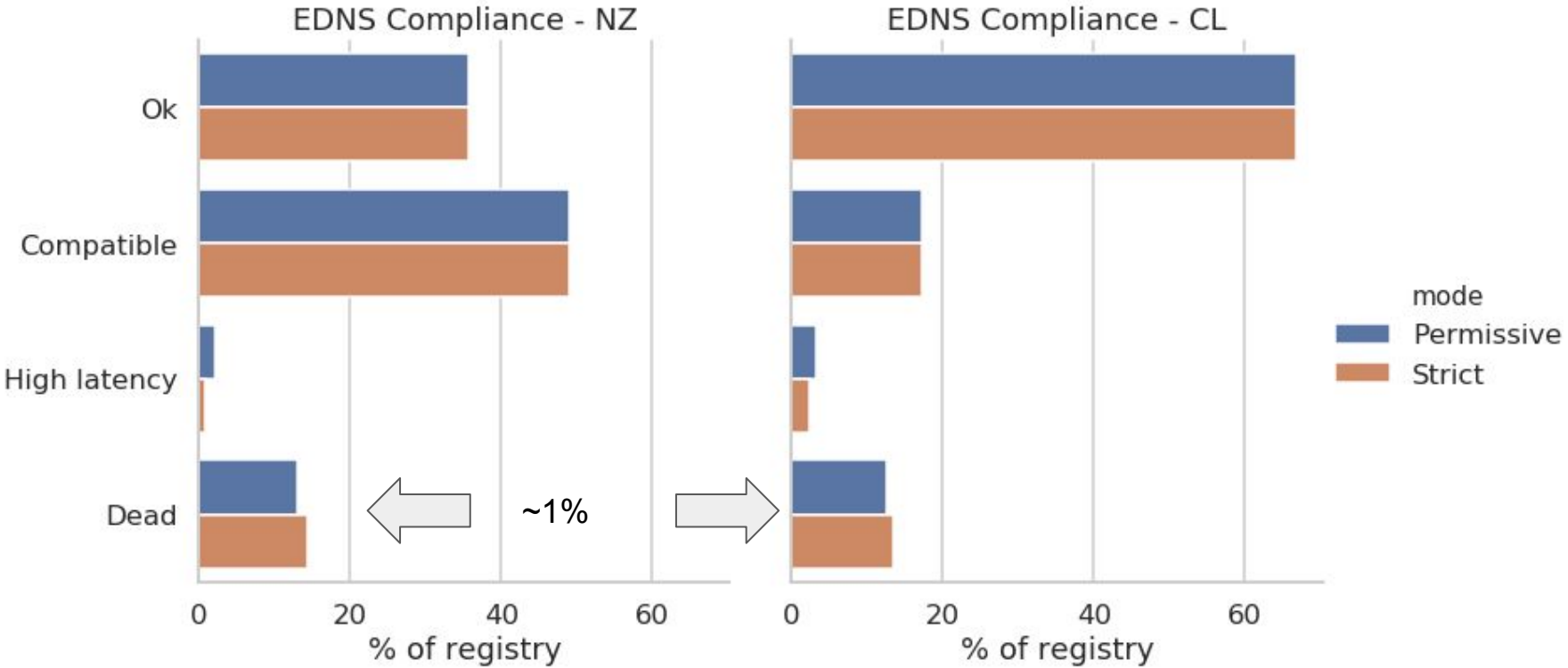
- Estoy encargado de un TLD, ¿cómo repito este análisis?
  - EDNS Compliance Scanner de CZ.NIC
  - https://gitlab.labs.nic.cz/knot/edns-zone-scanner/

¿Cuántos dominios estarían afectados?

- **EDNS Compliance scanner** propone 4 estados para un dominio:
  - OK: El dominio no está afectado
  - Compatible: El dominio tiene algunos problemas pero no se verá afectado el DNS Flag Day
  - High Latency: El dominio sufrirá de timeouts al tratar de resolverlo
  - Dead: El dominio no funcionará

- Además define 2 modos: Permissive (como en éstos momentos) y Strict (después de Flag day)

¿Cuántos dominios estarían afectados?



Mi dominio está afectado, ¿cómo corrijo los errores?

- Actualizar tu software de DNS a una versión moderna
- Utilizar software que adhiera a los estándares
- Corregir reglas de firewall, especialmente inspección profunda de paquetes DNS
- Re-testear

Trabajo futuro

- Campaña de concientización.

- Seguir ejecutando la colección consistentemente cada mes, para identificar si los errores desaparecen.
  - Invitar a otros ccTLDs a revisar sus dominios
  - Se puede obtener un listado de dominios que pasarán a “dead” en modo “strict” -> dar aviso

- Ver el mundo arder el día 1 de Febrero de 2019

Preguntas

dnsflagday.net/es/

Hugo Salgado, hsalgado@nic.cl
Sebastián Castro, sebastian@internetnz.net.nz

nic chile
SOMOS EL PUNTO CL

InternetNZ