# Integrando Tests de Completitud y Conformidad en servicios DNS

LACNOG 2020

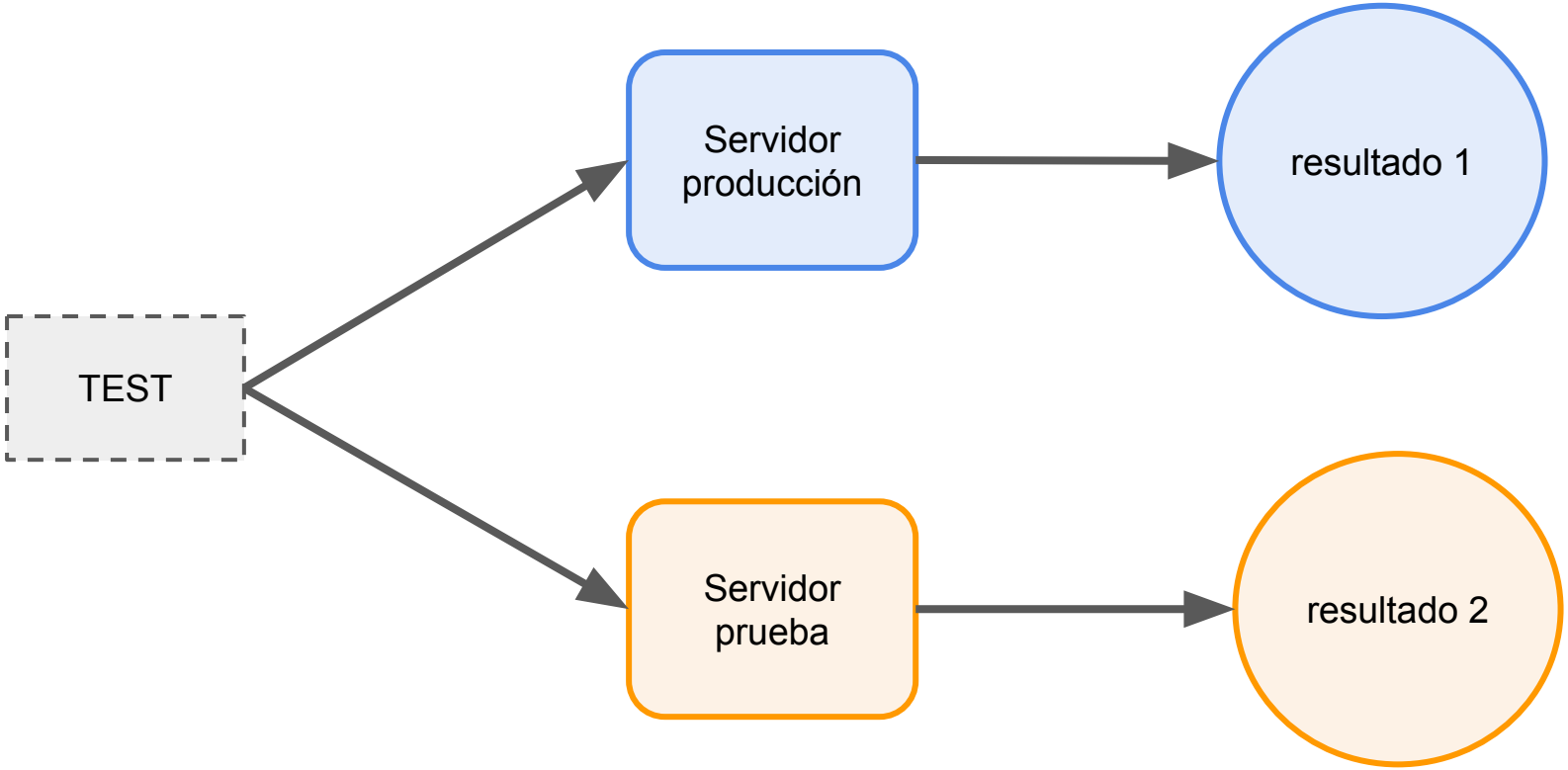
Mauricio Vergara Ereche
Hugo Salgado

# ¿Cuál es el problema?

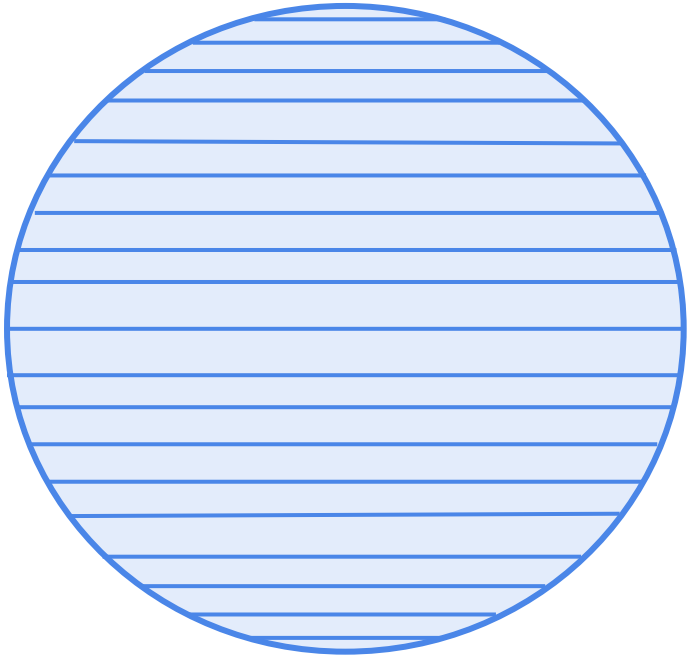
- Quiero actualizar mi servidores DNS
  - Estoy seguro que responderán correctamente?
  - ...y con el mismo comportamiento que tienen ahora mis actuales servidores?
  - Puedo tener un ambiente de **testing** antes de subirlo a producción?
    - QA
  - Automatizado?
    - Para integrar con mi pipeline CI/CD

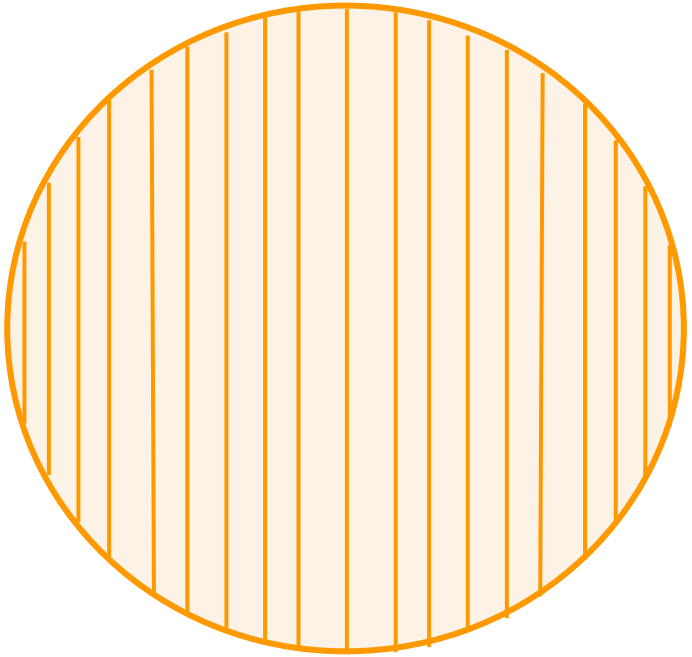
- Quiero probar un nuevo software DNS
  - Puedo ejecutar pruebas y ver si responde igual que mi actual DNS?
  - ...de manera automatizada?

# Idea general

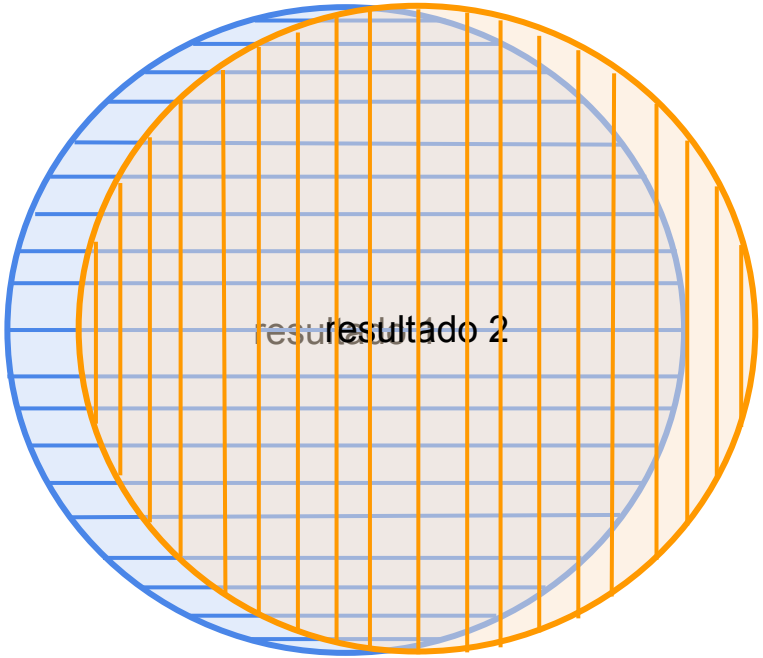


# Idea general: Comparando

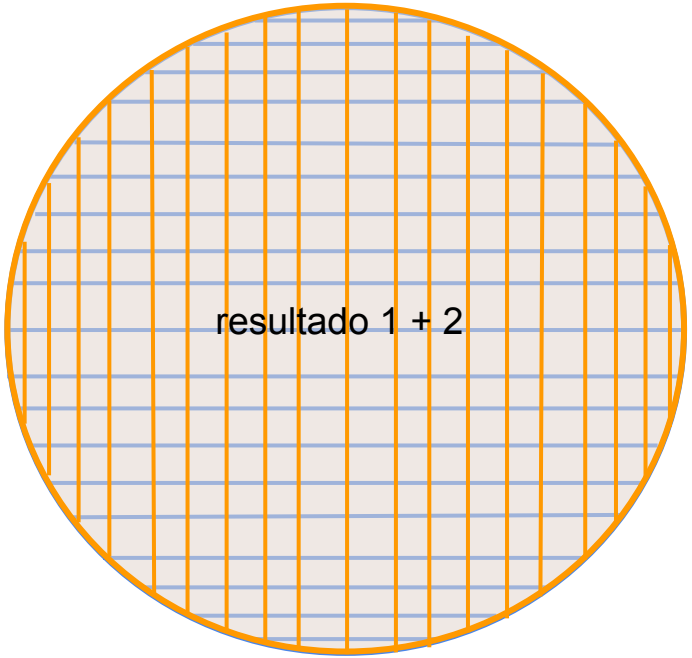




# Idea general: Comparando

# Idea general: Comparando

# Nuestra herramienta: **dns-comp**

- Escrita en Python 3
- Viene con un set de pruebas estándar de buen comportamiento
  - Basadas por ejemplo en DNS Flag Day 2018
- Envía queries DNS cuidadosamente construidas
- Compara los resultados
- Pruebas extensibles
  - Muy fácil de escribir una propia
  - y compartir en github
- Trabajo futuro: Integrable con su CI/CD favorito
  - Tal vez como unitest?

# Set de pruebas estándar

- Recomendaciones del “ICANN Root Server System Advisory Committee” (RSSAC047 (sección 5.3))
  - https://www.icann.org/en/system/files/files/rssac-047-12mar20-en.pdf

# Set de pruebas estándar

- Recomendaciones d n 5.3))
  - https://www.ica

Metrics for the DNS Root Servers and Root Server System

## 1 Introduction

In this report, the RSSAC:

- Defines measurements, metrics, and thresholds that root server operators (**RSOs**) meet to provide a minimum level of performance. The thresholds are based on technical metrics designed to assess the performance, availability, and quality of service that each root server identifier (**RSI**) provides. The thresholds and the metrics on which they are based are included as the RSSAC's input to a yet-to-be defined evaluation process for future RSOs.
- Defines system-wide, externally verifiable metrics and thresholds which demonstrate that the root server system (**RSS**) as a whole is online and serving correct and timely responses.

The report is organized as follows:

- Section 2 provides background and scope for the work.
- Section 3 defines some requirements for the vantage points.
- Section 4 discusses some general points about metrics and measurements, including some high-level requirements for the measurement system.
- Section 5 defines RSI-related metrics and thresholds on availability, response latency, correctness, and publication latency.
- Section 6 defines RSS-related metrics and thresholds on availability, response latency, correctness, and publication latency.

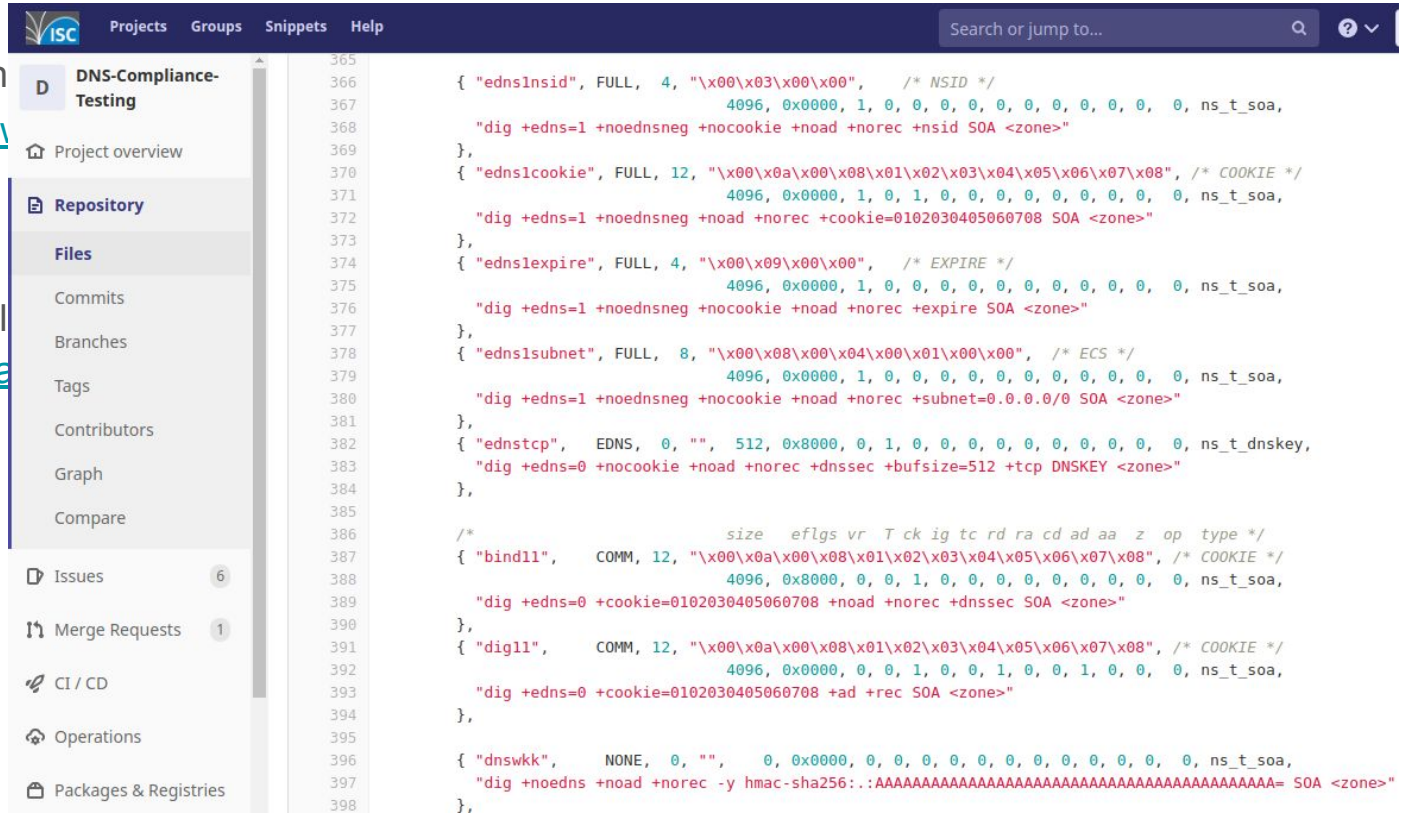
# Set de pruebas estándar

- Recomendaciones del “ICANN Root Server System Advisory Committee” (RSSAC047 (sección 5.3))
  - https://www.icann.org/en/system/files/files/rssac-047-12mar20-en.pdf

- ISC DNS Compliance Testing
  - https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing

# Set de pruebas estándar

- Recomendacion
  - https://ww
- ISC DNS Compl
  - https://gitla



# Ejemplo de caso de uso

- Tengo BIND 9.11 y quiero probar BIND 9.12
  - **Instalar** BIND 9.12 en alguna máquina de prueba.
  - **Configurar** BIND 9.12 con setup de producción de 9.12
  - Crear **tests** (o re-usar los que ya están hechos)
    - Cada test es creado con un comando **dig** y un **comentario** para identificarlo.
    - Sólo por orden, guardar el comando en un archivo con extensión **.cmd**
  - Crear el punto de comparación almacenando el resultado de los tests contra el servidor de producción actual (BIND 9.11)
    - Guardar en formato YAML con extensión **.yaml** (Usar: `dig @server +yaml`)
  - Para comparar el resultado contra el nuevo servidor
    - Sólo basta cambiar la IP del comando `dig @server`

```
$ dns-comp.py <test.yaml> <test.cmd>
```

# Ejemplo: Creación de test

Archivo **test-001.yaml**

```
# SOA record answer IPv4 UDP

dig cero32.cl. @ns.cero32.cl SOA
    +norec +time=1 +tries=1 +noignore
    +dnssec -4 +notcp +yaml
```

# Ejemplo: Resultado de comparación del test (1/2)

```yaml
-
  type: MESSAGE
  message:
     type: AUTH_RESPONSE
     query_time: !!timestamp 2020-09-23T01:23:19.043Z
     response_time: !!timestamp 2020-09-23T01:23:19.212Z
     message_size: 704b
     socket_family: INET
     socket_protocol: UDP
     response_address: 200.1.122.29
     response_port: 53
     query_address: 0.0.0.0
     query_port: 53553
     response_message_data:
          opcode: QUERY
          status: NOERROR
```

```yaml
id: 53187
flags: qr aa
QUESTION: 1
ANSWER: 2
AUTHORITY: 4
ADDITIONAL: 3
OPT_PSEUDOSECTION:
   EDNS:
     version: 0
     flags: do
     udp: 4096
     COOKIE: 006aed51d70b2e0b01000000
       5f6aa387de3c04595f361622 (good)
QUESTION_SECTION:
  - cero32.cl. IN SOA
```

# Ejemplo: Resultado de comparación del test (2/2)

```
ANSWER_SECTION:
   - cero32.cl. 43200 IN SOA ns.cero32.cl. mave.cero32.cl. 2020091701 21600 7200 2592000 1209600
   - cero32.cl. 43200 IN RRSIG SOA 7 2 43200 20210917202955 20200917202955 23807 cero32.cl.
                         NlW/yOnLZALhyErBh4SQRbEvmKL9mV7ZhQGbCwpEt7lU8xHWOnW2Q0mU
                         voJixYP2s4LUCmAoDufJkJlQWB5glEzoYUCYfIj4iMEcPRD09UGb9pBb
                         pL4yFHclg54b6TQPICsHzXbFSVAymM6rZfPOIL6Onz3ASzSW8MTj7ntr SbM=
AUTHORITY_SECTION:
   - cero32.cl. 43200 IN NS secundario.nic.cl.
   - cero32.cl. 43200 IN NS ns.cero32.cl.
   - cero32.cl. 43200 IN NS ns.niceto.cl.
   - cero32.cl. 43200 IN RRSIG NS 7 2 43200 20210917202955 20200917202955 23807 cero32.cl.
                         fuQ44U9nomjjUuoJp5+V/BVlBbbyt4R0KMq3ApuMJgIx5eNWyE9YG8HN
                         4CN8Z9UZYKgP+pAggG5EF8iUTUkVPrvp0mMq0O3wgCYiagJu4kaY9eMI
                         T2ij/pIkHUyxfddHM7iaERWJEnNrDLTh+RxNqEUYSdt35jNqYAQIK+Qa zpE=
ADDITIONAL_SECTION:
   - ns.cero32.cl. 43200 IN A 200.1.122.29
   - ns.cero32.cl. 43200 IN RRSIG A 7 3 43200 20210917202955 20200917202955 23807 cero32.cl.
                         lAebypa50nyV2ipUb1JX/6LrP2M98lc5QKoaQDzYy3eYjggRqJ2V5zMl
                         SpNzxeyJgcciTCMTMa3nl6AfOZqV8YMNFeKljkKlVHlkxF4jw0jpd+I6
                         GZ5vjX++0mZUoiqK5GtEdrsN3KUCnzu/sA9UkKQJZdpBdnJaZg2Q23tm cGk=
```

# Algunas pruebas

- “For positive responses where QNAME = and QTYPE = DS, a correct result requires all of the following:
  - The header AA bit is set.
  - The Answer section contains the signed DS RRset for the query name.
  - The Authority section is empty.
  - The Additional section is empty”

- “For negative responses, a correct result requires all of the following:
  - The header AA bit is set.
  - The Answer section is empty.
  - The Authority section contains the signed . / SOA record.
  - The Authority section contains a signed NSEC record covering the query name.
  - …”

# Ejemplo de salida (sin diferencias)

```
./run-all-tests.sh
```

```
## Running tests/tests-0001...  SOA record answer IPv4
 PASS
## Running tests/tests-0002...  SOA record answer IPv4 TCP
 PASS
## Running tests/tests-0003...  DNSKEY record answer IPv4 UDP
 PASS
## Running tests/tests-0004...  DNSKEY record answer IPv4 TCP
 PASS
## Running tests/tests-0005...  NS record answer IPv4 UDP
 PASS
[ … ]
```

# Ejemplo de salida (con diferencias)

```
./run-all-tests.sh
```

```
## Running tests/tests-0001...  SOA record answer IPv4
 PASS
## Running tests/tests-0002...  SOA record answer IPv4 TCP
 Item ['message']['response_message_data']['AUTHORITY_SECTION'] added to dictionary.
 Item ['message']['response_message_data']['ADDITIONAL_SECTION'] added to dictionary.
 Value of ['message']['response_message_data']['AUTHORITY'] changed from 0 to 14.
 Value of ['message']['response_message_data']['ADDITIONAL'] changed from 1 to 13.
 Value of ['message']['message_size'] changed from "389b" to "1204b".
 Item ['message']['response_message_data']['ANSWER_SECTION'][0] removed from iterable.
 Item ['message']['response_message_data']['ANSWER_SECTION'][1] removed from iterable.
## Running tests/tests-0003...  SOA record answer IPv6 UDP
 PASS
```

# Estado actual y próximos pasos

- En beta en:
  - https://github.com/mave007/dns_completitude_and_compliance

- Listo para utilizar (180 tests)!

- Próximos pasos
  - Agregar nuevos tests
  - Mejorar documentación
  - Pasarlo a v1.0
  - Su idea acá! (**issues** de Github)

# Gracias

LACNOG 2020

Mauricio Vergara Ereche
mave@cero32.cl

Hugo Salgado
hugo@salga.do