NIC Chile
Secondary DNS Service
History and Evolution

Marco Díaz

OARC Buenos Aires 2016

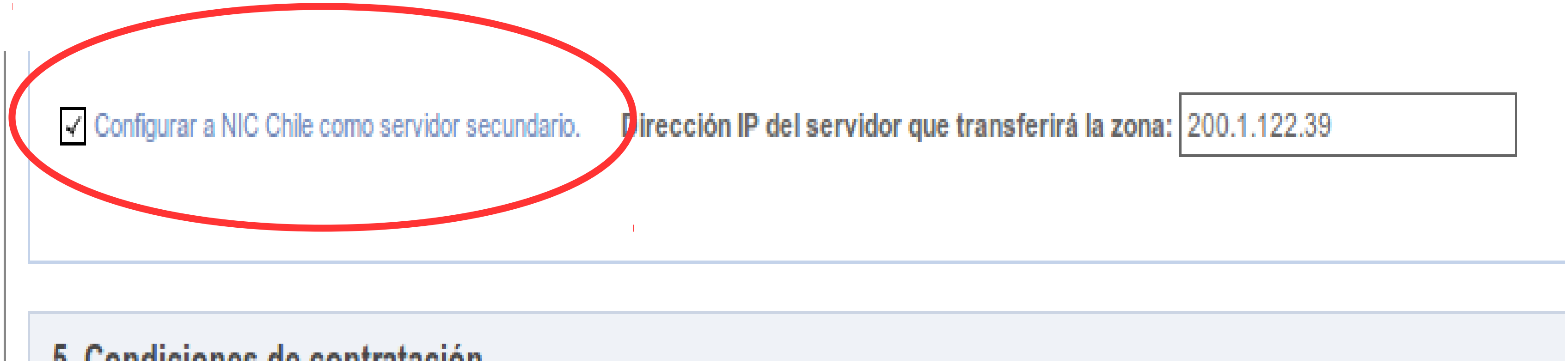
A little bit of history

- NIC Chile started to offer secondary service as a way to improve the local Internet.
- Launched in 2001.
- Since then it has been a service free of charge for our customers.

A little bit of history

- A unicast machine, BIND server over Linux OS.
- A new configuration generated every hour.
- A friendly interface for customers when choosing the service

A little bit of history



☑ Configurar a NIC Chile como servidor secundario.

Dirección IP del servidor que transferirá la zona: 200.1.122.39

5. Condiciones de contratación

Operations

- More than 32000 zones.
- Lots of zones transfer failed.
- Lame delegations.
- Customer calls to “touch” their file zone to keep it alive a little longer.

In 2008 we started to generate changes every 30 min.

Problems

- Due to the very frequent reconfig, a lot of TCP overhead between DNS servers.

```
[…]
transfers-in 4500;
transfers-out 1000;
tcp-clients 3500;
tcp-listen-queue 15;
serial-query-rate 4000;
transfers-per-ns 300;
transfer-source 200.1.123.7;
provide-ixfr no;
Max-transfer-time-in 20;
[...]
```

Problems

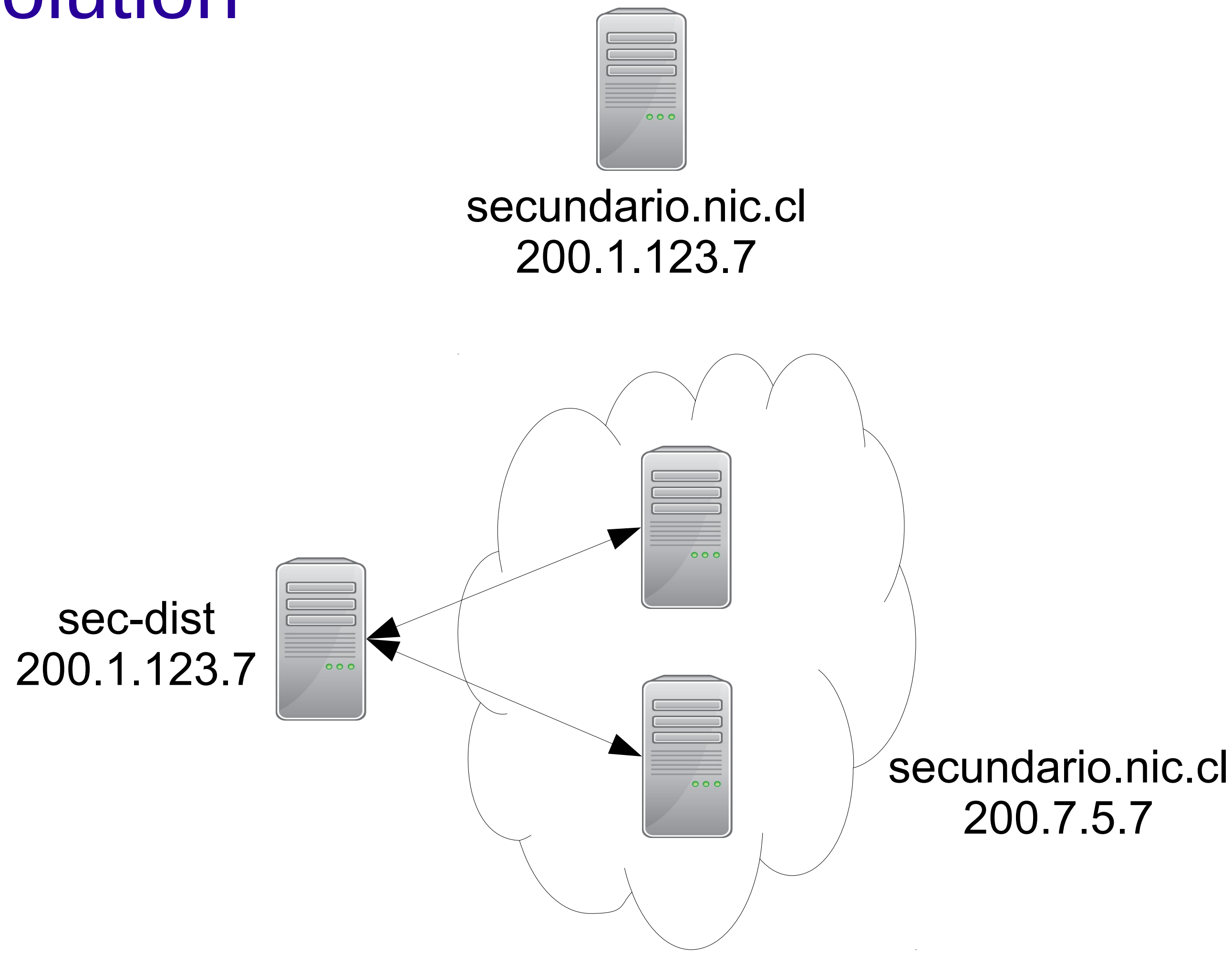
- Given the large amount of SOA queries and transfer attempts every 30 min, we started to have interruptions in the service.

- Interruptions due to scheduled maintenance.

Evolution

- We wanted a solution that did not involve changes for current customers.
- In October 2009, first major upgrade unicast to anycast
  - 2 nodes
  - 1 distributor

Evolution

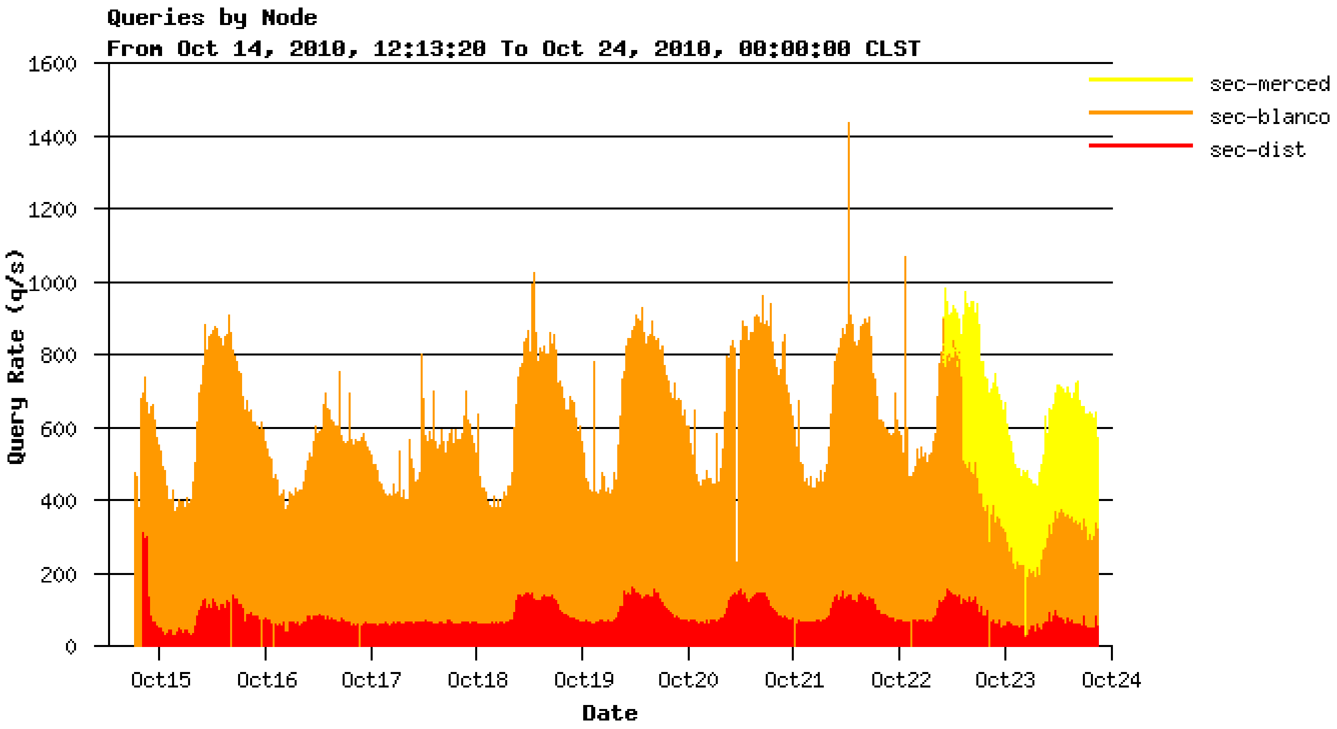


secundario.nic.cl
200.1.123.7

sec-dist
200.1.123.7

secundario.nic.cl
200.7.5.7

Anycast


Queries by Node
From Oct 14, 2010, 12:13:20 To Oct 24, 2010, 00:00:00 CLST
Query Rate (q/s)
0
200
400
600
800
1000
1200
1400
1600
Oct15
Oct16
Oct17
Oct18
Oct19
Oct20
Oct21
Oct22
Oct23
Oct24
Date
sec-merced
sec-blanco
sec-dist

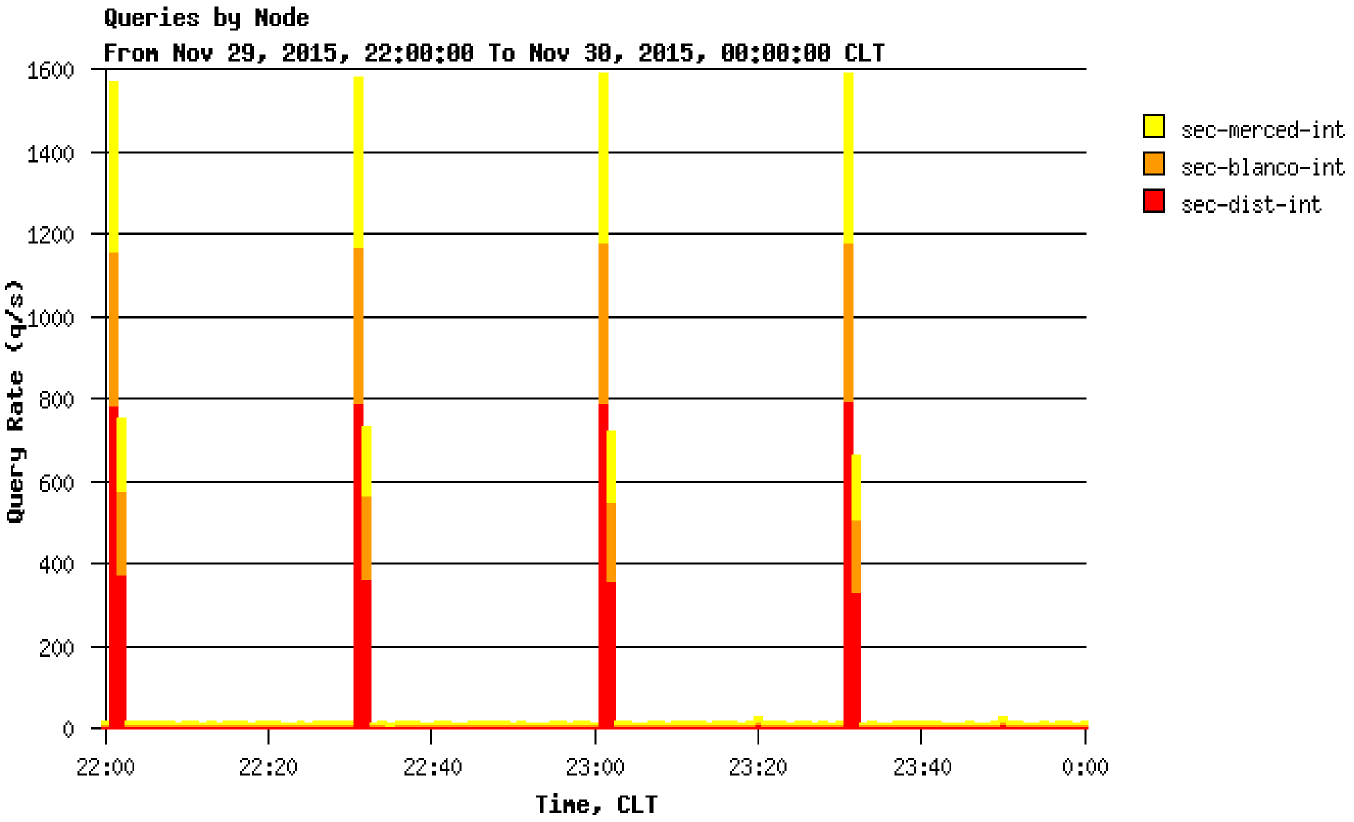
Advantages

- Redundancy
- Transfers between nodes and distributor are much faster.
- The service has less impact every 30 min.
- Scheduled maintenance without service interruptions.

Disadvantage

- Overhead *still* exist.

Overhead peaks



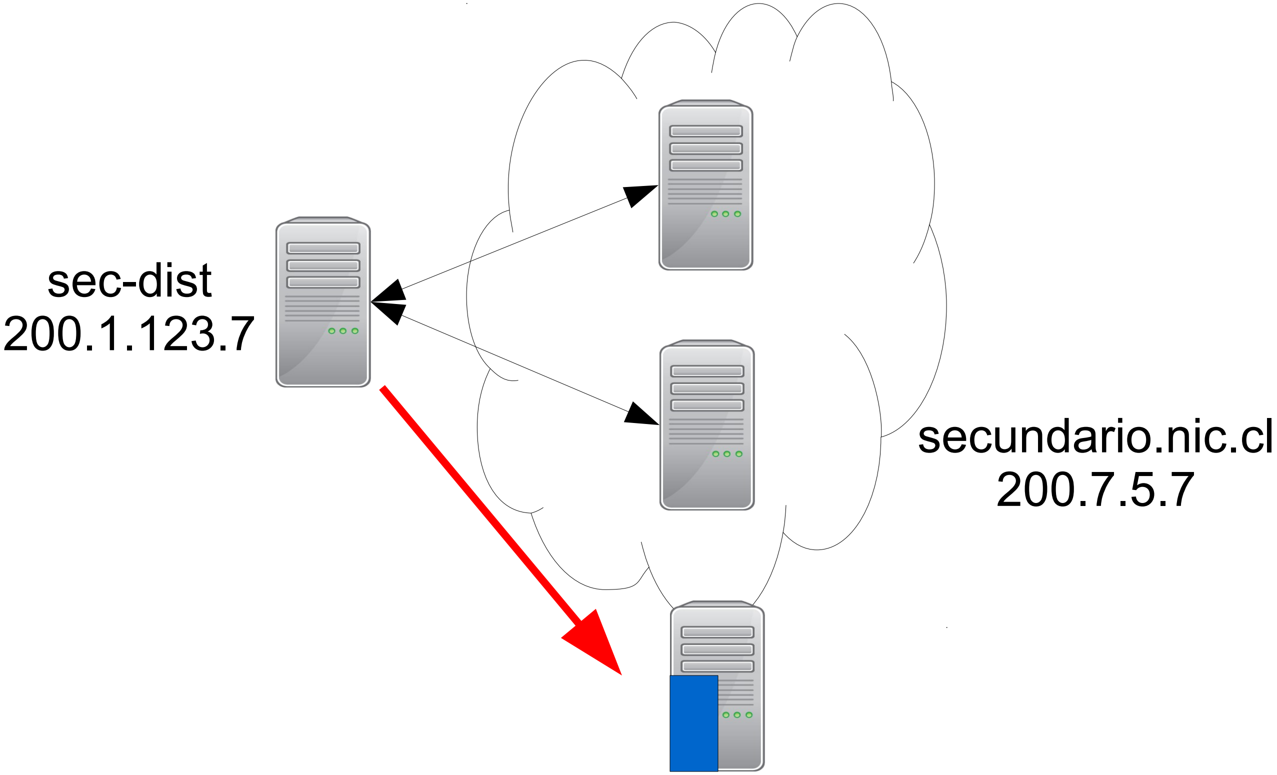
“MetaSlave” solution

- Small daemon that runs along the DNS server, on a different port, and listens for a notify query

- Based on work from Jan-Piet Mens of “Automatic provisioning of slave DNS servers”

- When the server receives a notify, triggers the addition of that zone to the server.

MetaSlave implementation



MetaSlave implementation

- Perl script
- TSIG-signed communication with the distributor
- Queue for commands when the server is not available.
- Invoke *addzone* commands.
  - Support Bind and NSD.

MetaSlave implementation

- Server side config

```
also-notify
 {
     172.30.21.67 port 54 key dist-nodo;
  };
```

MetaSlave implementation

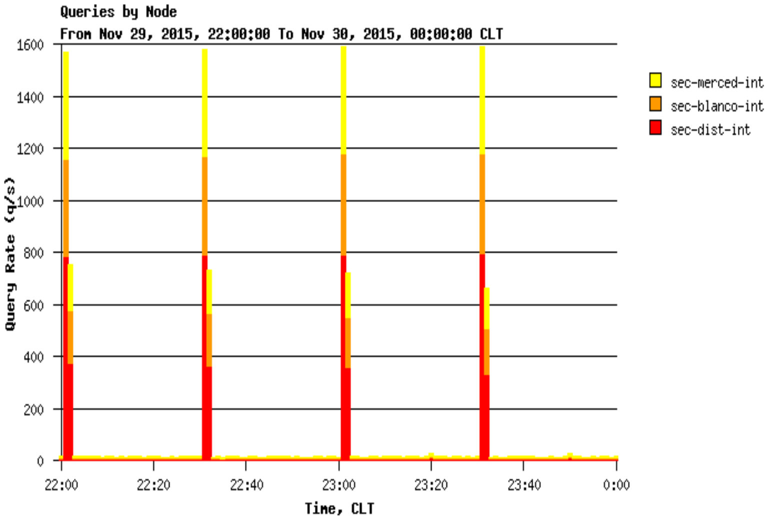
- Advantages
  - Adding only well configured zones.
  - Does not generate overhead traffic.

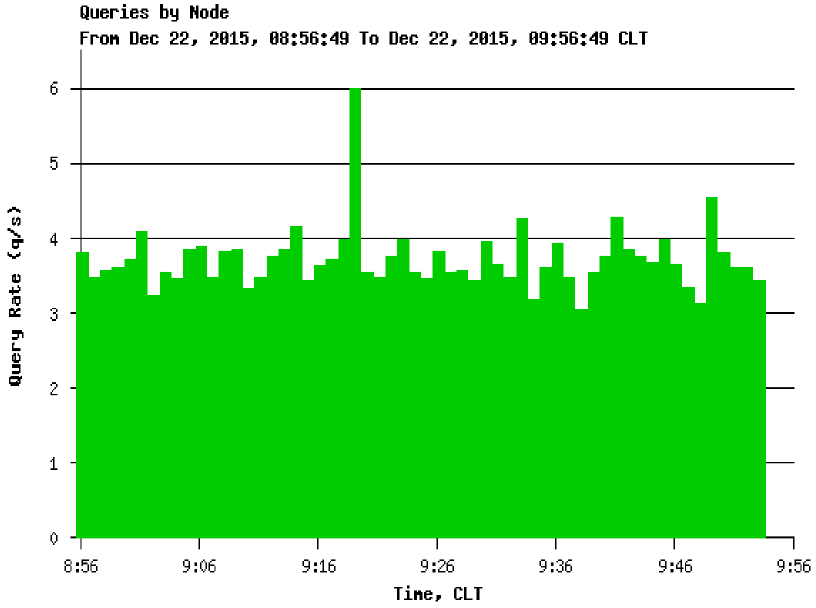
- Disadvantage
  - Does not manage change of states (elimination of a zone)

MetaSlave implementation

- Workaround
  - Another daemon, that runs on the distributor.
  - After every generation, generate a list of the zones eliminated, and invokes delete commands on the node.

Results


Queries by Node
From Nov 29, 2015, 22:00:00 To Nov 30, 2015, 00:00:00 CLT
Query Rate (q/s)
1600
1400
1200
1000
800
600
400
200
0
22:00
22:20
22:40
23:00
23:20
23:40
0:00
Time, CLT
🟨 sec-merced-int
🟧 sec-blanco-int
🟥 sec-dist-int


Queries by Node
From Dec 22, 2015, 08:56:49 To Dec 22, 2015, 09:56:49 CLT
Query Rate (q/s)
6
5
4
3
2
1
0
8:56
9:06
9:16
9:26
9:36
9:46
9:56
Time, CLT

Results

- BAD configured zones identified where almost 60%
- Well configured zones 40%

Total of zones using the service 32464

Added in the “metaslaved” node **13054**

Future work

- Improve policies for the use of service.
- Improve the scripts for fault tolerance.
- Using this to mitigate lame delegations.

Thanks!

mdiaz@nic.cl

Links

http://www.nic.cl

http://jpmens.net/2013/02/13/automatic-provisioning-of-slave-dns-servers/