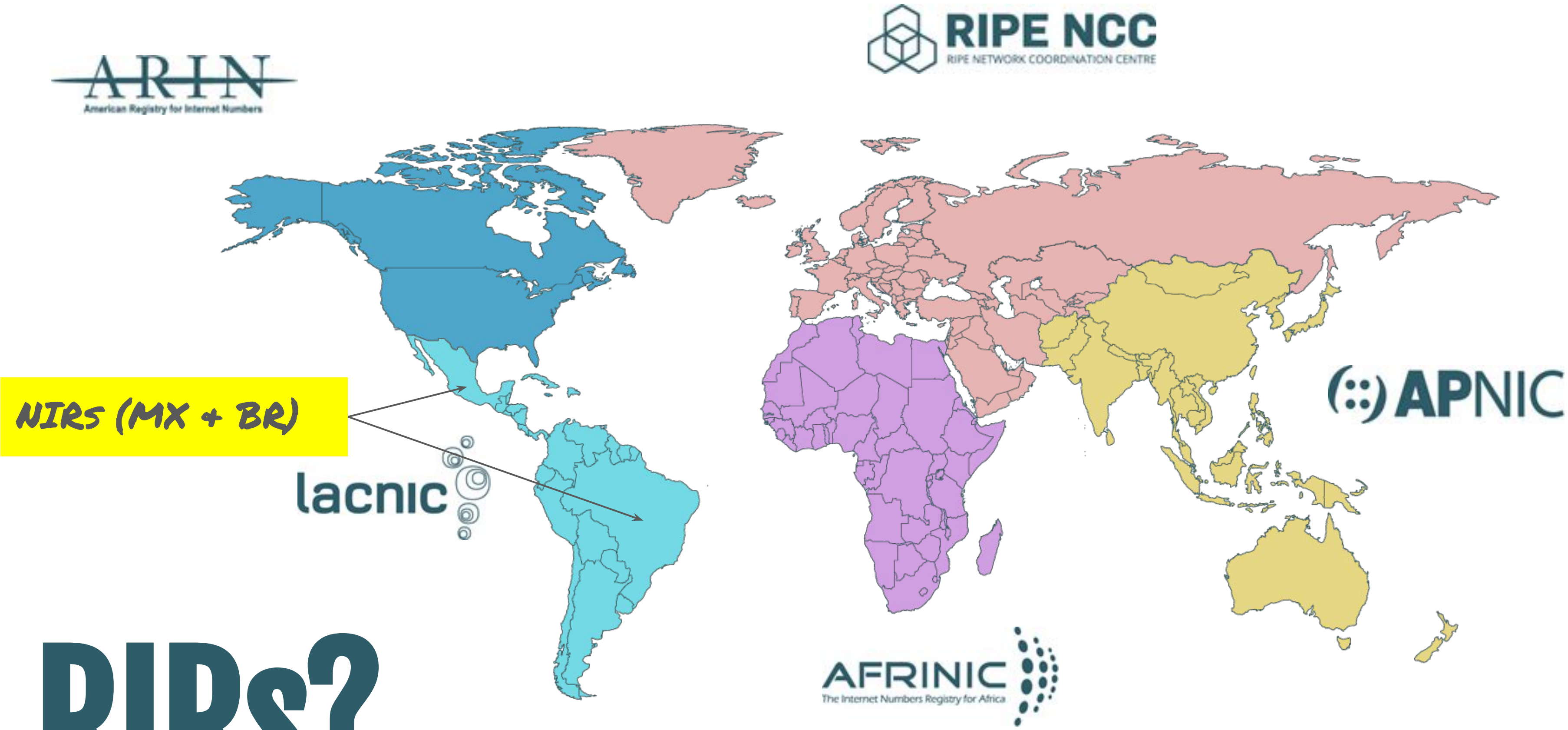
Migrating a Large RPKI CA

Carlos Martinez
LACNIC
IEPG @IETF120

Who are you ? Why are you here?

- I’m Carlos, working for LACNIC, one of the five RIRs

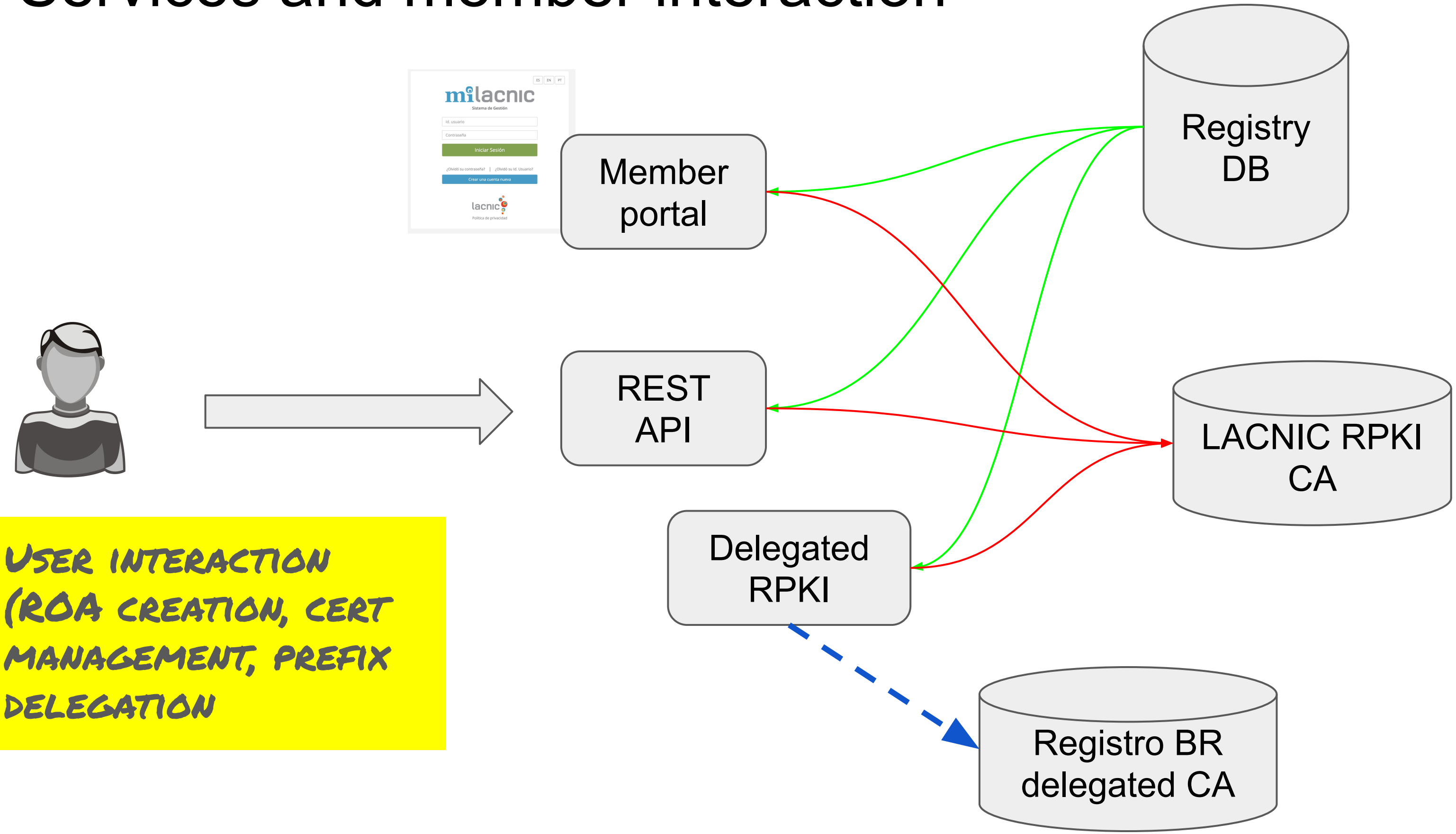
- I would like to share with you all a few things we learnt while migrating from our old RPKI software to a new architecture and to a new RPKI CA


ARIN
American Registry for Internet Numbers
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
lacnic
APNIC
AFRINIC
The Internet Numbers Registry for Africa

NIRs (MX + BR)

RIRs?

Services and member interaction

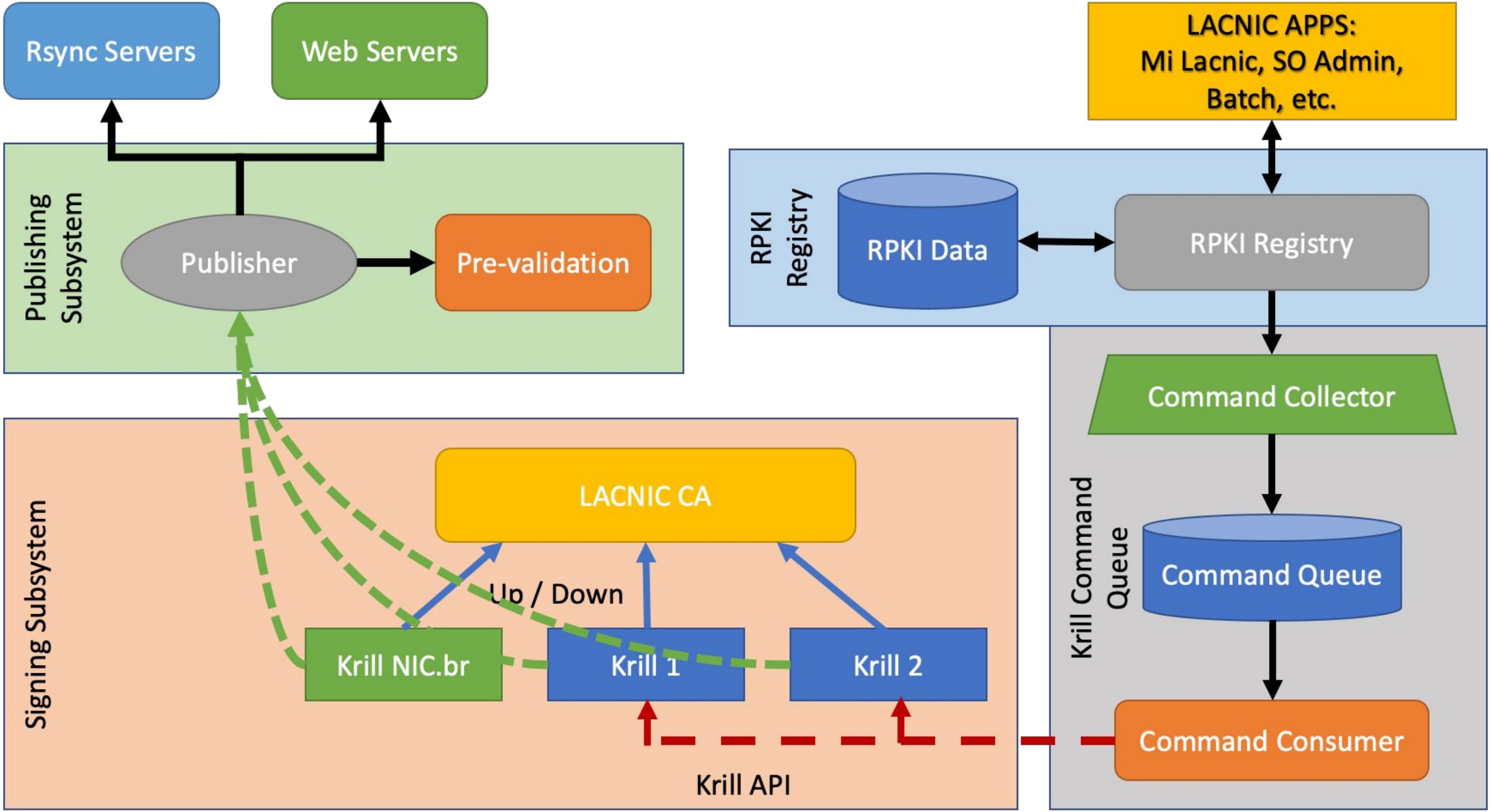


USER INTERACTION (ROA CREATION, CERT MANAGEMENT, PREFIX DELEGATION

Migration to a new architecture

For <reasons> we decided to migrate to a new architecture looking for:

- Looser coupling among components
- System modularity
- Stability
- Ability to follow new features coming out of the IETF quicker


Rsync Servers
Web Servers
LACNIC APPS:
Mi Lacnic, SO Admin,
Batch, etc.
Publishing Subsystem
Publisher
Pre-validation
RPKI Registry
RPKI Data
RPKI Registry
Command Collector
Krill Command Queue
Command Queue
Command Consumer
Signing Subsystem
LACNIC CA
Up / Down
Krill NIC.br
Krill 1
Krill 2
Krill API

Letting go…

Avoid “not invented here”.

What if there was an already available RPKI CA that we could use / adapt ?

Well…

Krill

https://nlnetlabs.nl/projects/routing/krill/

"PEOPLE DON'T WRITE
THEIR OWN DNS
SERVERS ANYMORE"

Migration “non negotiables”

- Keep the same TAL file
    - Key and URL
- Long running relying parties with initialized local caches should not notice anything except for a new RRDP session being issued
- Zero-downtime migration of Registro.BR delegated tree

Challenges

System validation and testing during development

- Integration with the current portal (production vs non-yet-production)

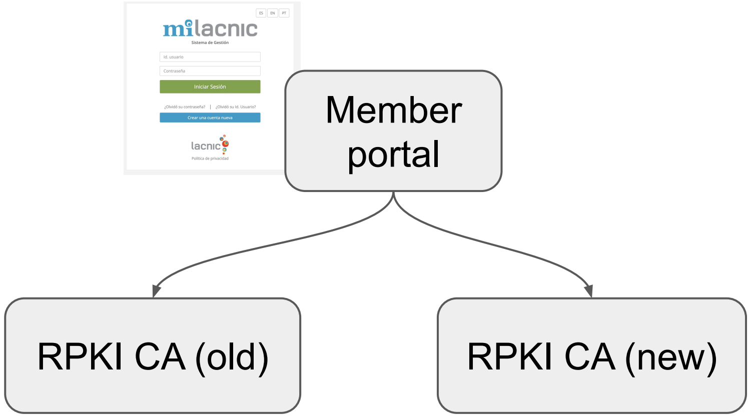
How to:

- Migrate transparently* both LACNIC hosted members and Registro.BR delegated CA

Migration strategy validation

Validation and testing during development

- When loosing the current coupling, we implemented an internal API for Portal communication with the RPKI CA and implemented the ability of the Portal to publish to *multiple endpoints at the same time* using the same internal API



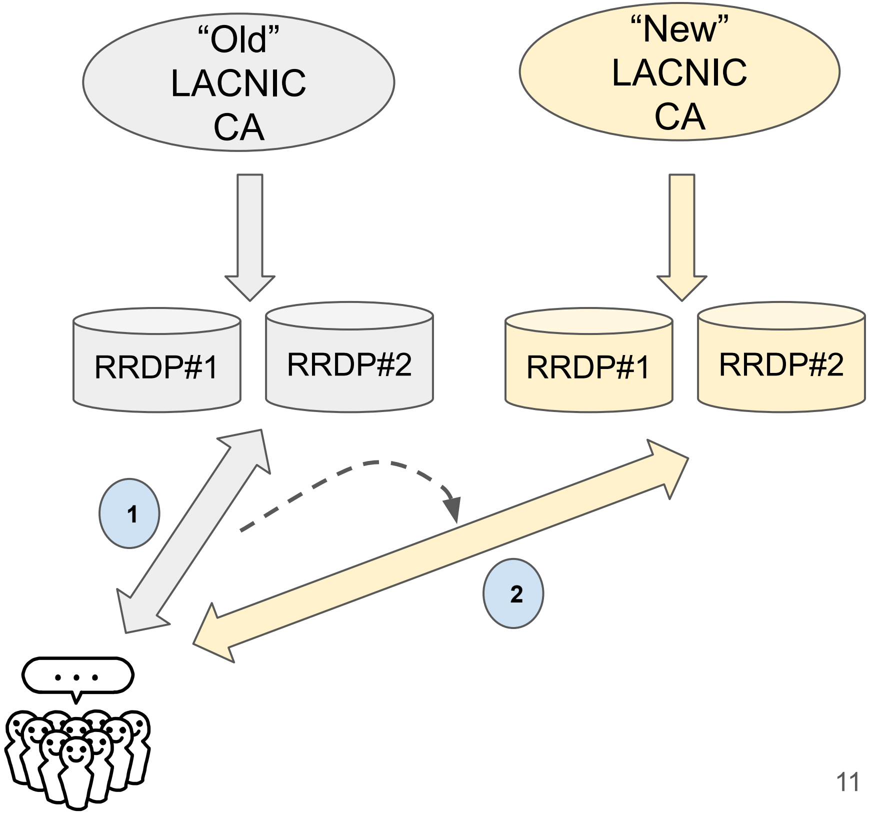
Member portal

RPKI CA (old)

RPKI CA (new)

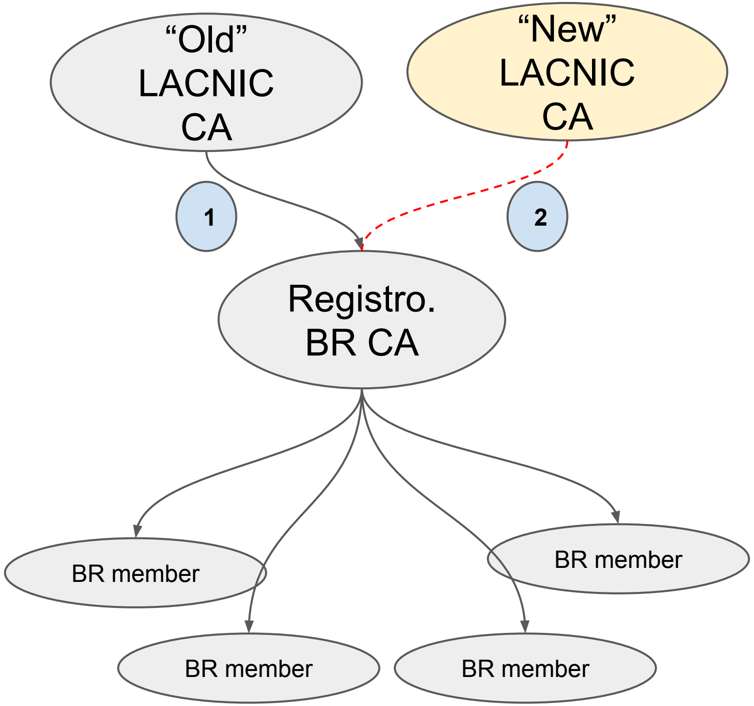
Migration Strategy: LACNIC CA

- Run old and new CAs in parallel for a few months and compare outputs
- New CA publishes to a different set of servers
  - *This went on for 6 months*
- Once comfortable with the outputs of both CAs , it would be time to actually migrate
- Change DNS records !



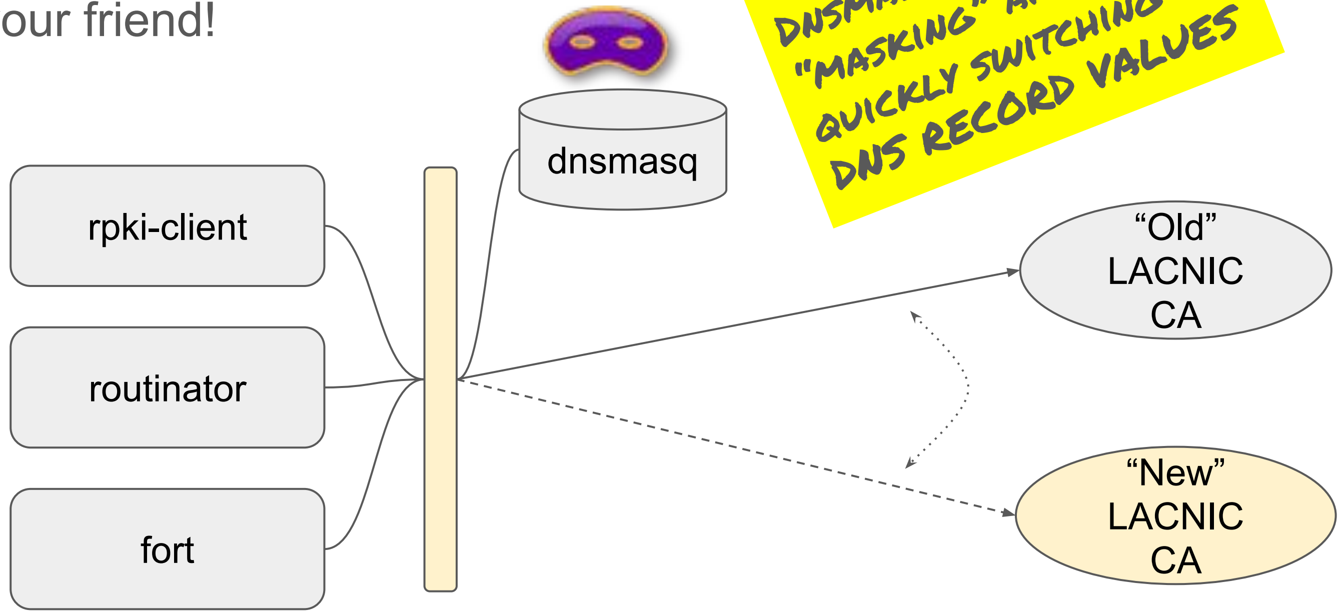
Migration Strategy: Registro.BR Delegated Tree

- Registro.BR offers only delegated RPKI service to Brazilian members
  - *Just moving the "hanging point" is not enough*
  - *Why? BR members would "dissapear" until each krill instance re-signs their own repo*
  - *This could take hours or even days*
- Krill supports *multiple parents*
  - The "new" CA was added as a second parent two weeks before the actual migration 💡
  - Doubles repository sizes
    - Most are quite small so no biggie



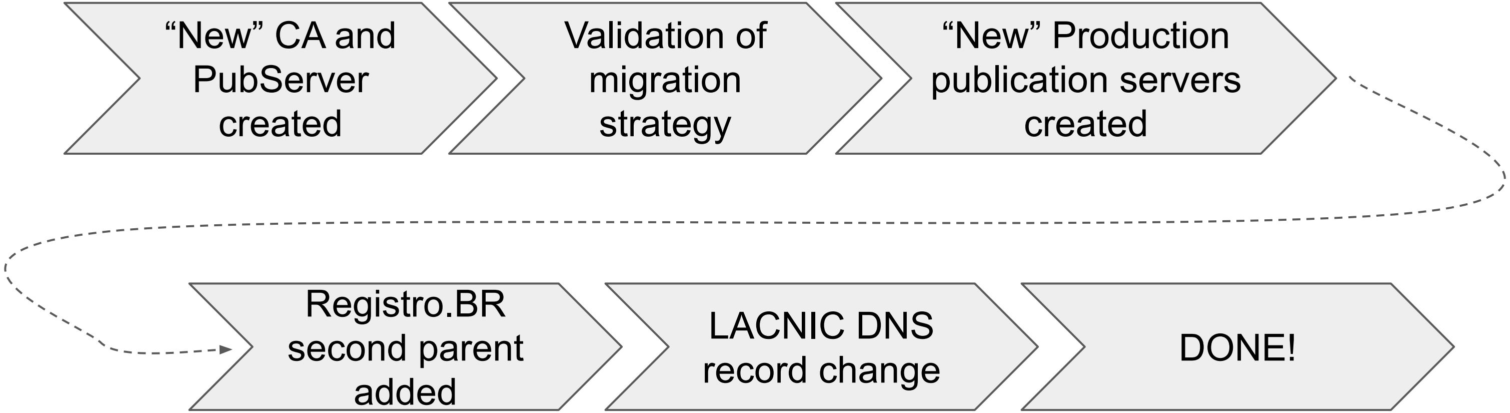
Validating the Strategy

Docker is your friend!



DNSMASQ ALLOWS FOR "MASKING" AND QUICKLY SWITCHING DNS RECORD VALUES

Migration Timeline



"New" CA and PubServer created

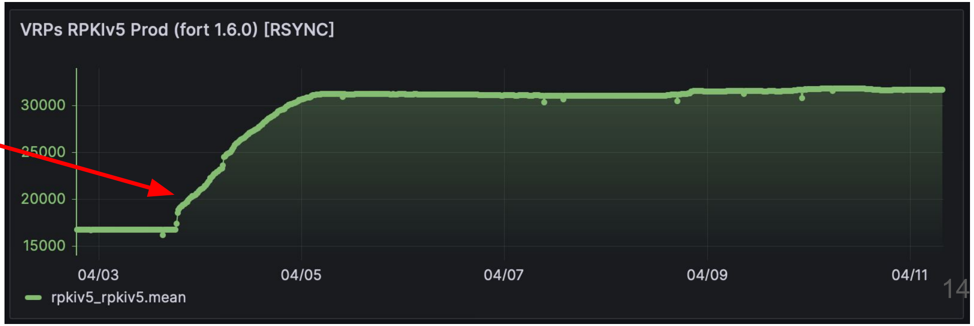
Validation of migration strategy

"New" Production publication servers created

Registro.BR second parent added

LACNIC DNS record change

DONE!



REGISTRO.BR SECOND PARENT ADDED

Communication During the Process

We tried to engage all stakeholders and ask for their opinions on these ideas

- RP developers (FORT, Routinator, rpki-client, rpki prover)
- Other RIRs
- Our NIRs

We kept the general community informed on next steps

- NANOG / LACNOG
- SIDROPS

THANK YOU ALL !!!

Thank You!