How we un-scattered our DNS setup and unlocked new automation options



Dan Lüdtke
Technical Lead SRE @ eGym GmbH

eGYM

- *Make the gym work for everyone!*
- Digital strength machines
- "Fitness Cloud"
  - Unify training data across vendors
- Data Analysis
- Apps
- Research Projects
  - Improve Diabetes patients symptoms through special training program







A year ago...



team

foo.tu.ts.egym.com

artifact

team space

5 Registrars



Name Servers

#startuplife

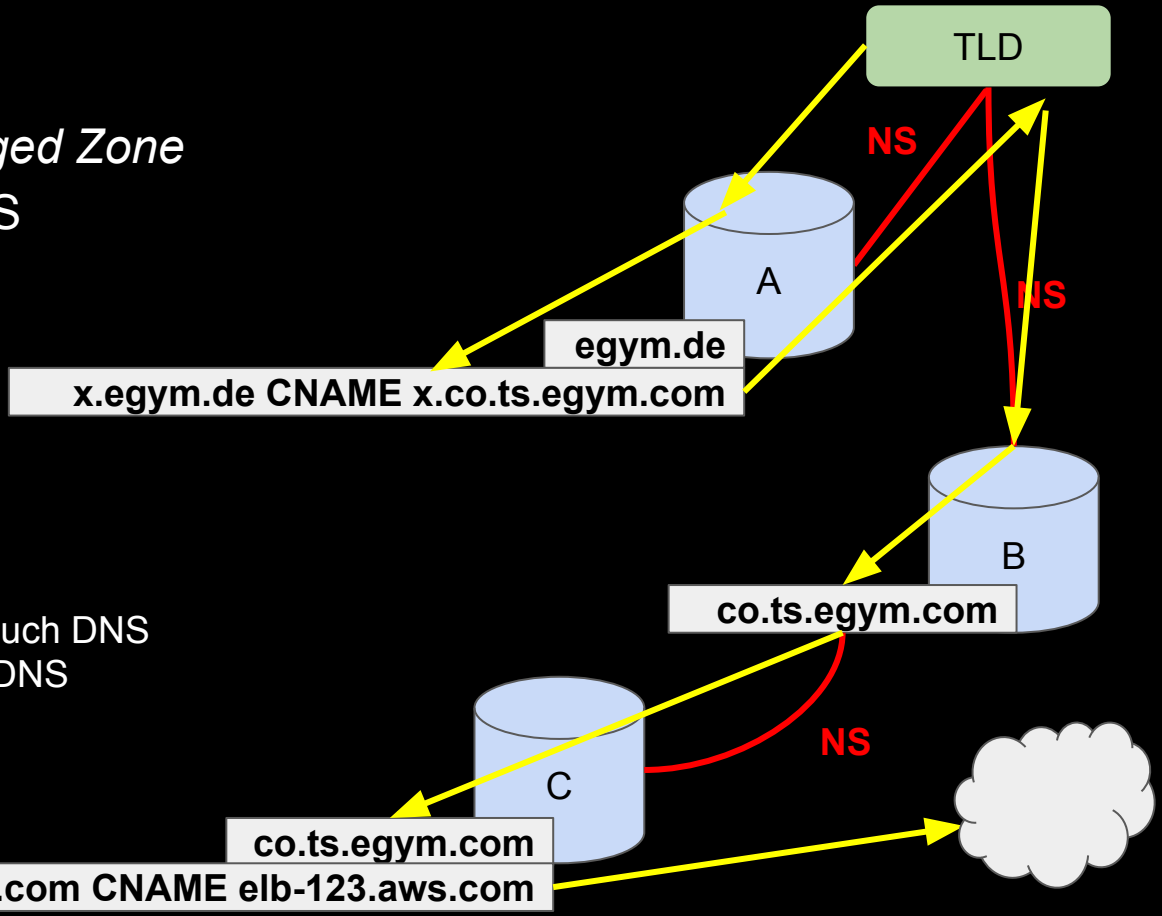
(do first, ask later)



Issues

- Ran into maximum *Managed Zone* limit on Google Cloud DNS
- Horrible lookups!
  - Slowing down customers
  - Hard to debug
- Deployment Strategy

  😜#YOLO
- "Haunted Graveyard"
  - Only few were allowed to touch DNS
  - Even fewer dared to touch DNS



Lessons Learned



Organizational structure and infrastructure evolve differently.

Don't force one onto the other.

Use company-wide unique artifact names in DNS.

Let's Improve!

What is the Problem here?

One does not simply *change* DNS

How to rollback?

Web interface does not provide atomicity!



Agility!

We build it, we run it!

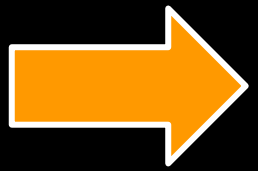
SRE is too slow changing DNS

SREs

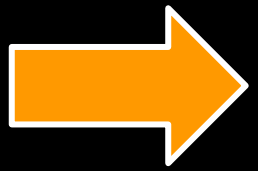
Devs

Divide and Conquer DNS Data

- Volatile
  - Special test domain
  - No availability guarantees
  - Everyone can change directly
  - No reviews
  - No tests
  - No atomicity (no changesets)
- Production
  - Version control
  - Reviewed changes
  - Tested for common mistakes
  - Tested for syntax, logic, deployment feasibility
  - Atomic deployment of whole changeset

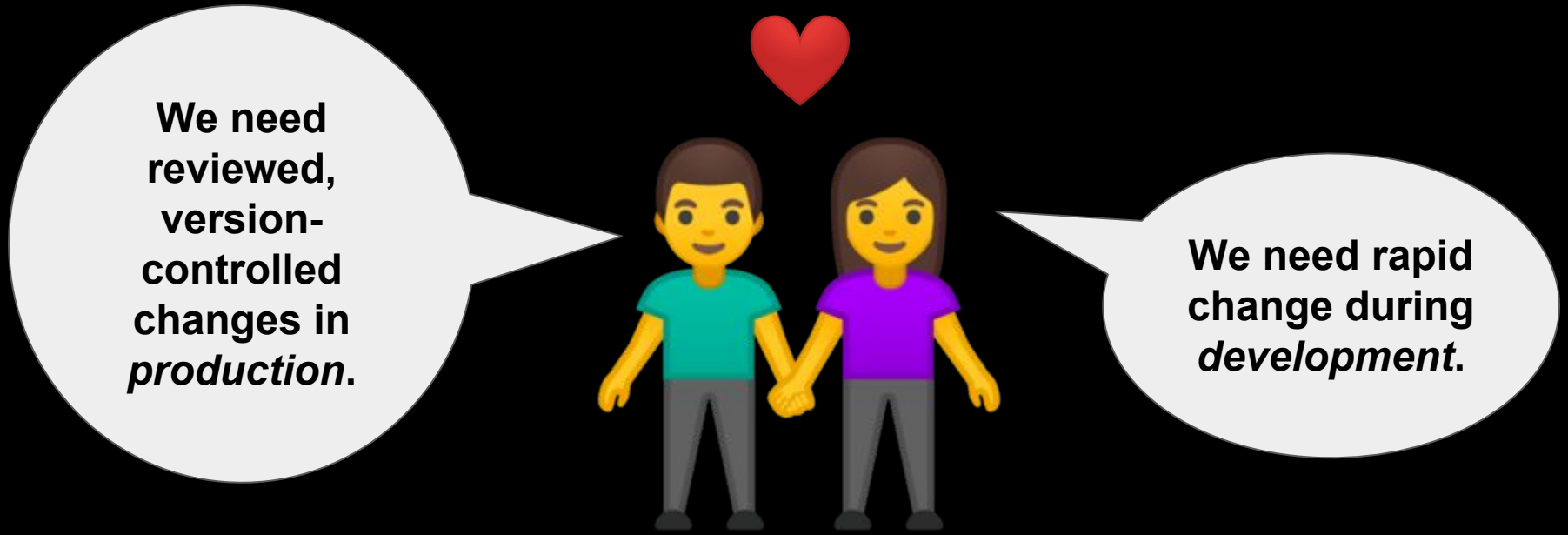


Agility



Reliability

Do we really have competing goals?



Storing DNS Data

Zone Data

- Version Control
  - Git repository
  - All developers have access
- YAML-based format
  - Developer love it
    - compared to zone files ;)
  - Easy to read and understand
- Templating functionality

coffee.egym.zone.yml

```
zones:
  - zone: egym.coffee
    description: Test zone.
    ttl: 300
    templates:
      - gmail
      - website
    names:
      - name: '@'
        texts:
          data:
            - foobar-site-verification-123456
      - name: paloalto
        forwarding:
          ttl: 60
          target: flaky.cloud.example.com.
      - name: losangeles
        addresses:
          literals:
            - 192.0.2.99
            - 2001:db8:200::99
```

Zone Data (Template)

- Tradeoff between
  - Principle of Least Surprise
  - Don't Repeat Yourself (DRY)
- Typical templates
  - Set of mail servers
  - Set of name servers (delegation)
  - Domain Parking
  - Redirect to commercial website

gmail.template.yml

```
templates:
  - template: gmail
    description: >
      This template adds Google
      mail servers to a zone.
    names:
      - name: '@'
        mail:
          ttl: 604800
          mailservers:
            - mailserver: aspmx.l.google.com.
              priority: 10
            - mailserver: alt1.aspmx.l.google.com.
              priority: 20
      - name: google._domainkey
        texts:
          data:
            - >
              v=DKIM1;
              k=rsa;
              p=foobar123456
```

Validating DNS Data

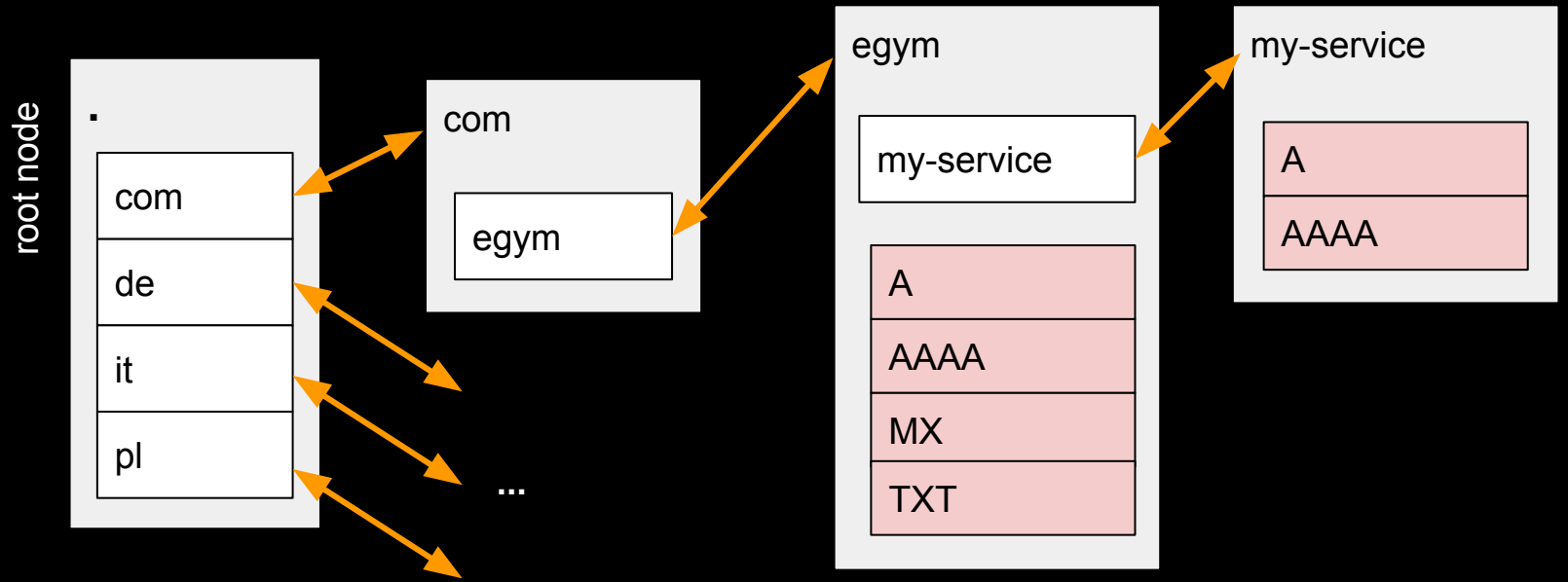
Resource Record Database (RRDB)

- Go package
- Limited dependencies
  - Go Standard Library
  - YAMLv2
- High test coverage
- Unfortunately: Battle-tested 

rrdb

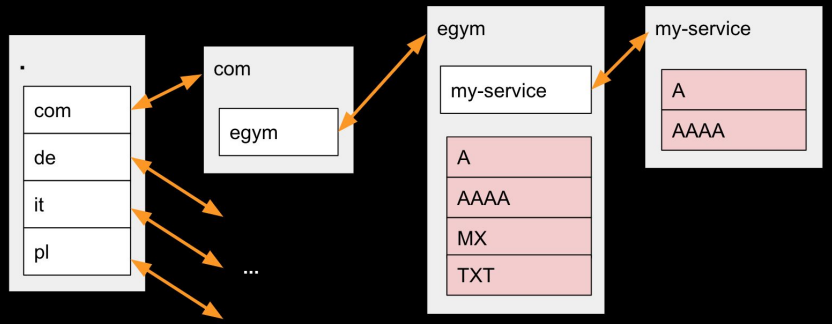
Files				Coverage
loader.go	115	111	2	2	96.52%
rrdb.go	332	332	0	0	100.00%
Folder Totals (2 files)	447	443	2	2	99.10%
Project Totals (7 files)	729	658	6	65	90.26%

RRDB Internals: Trie Data Structure

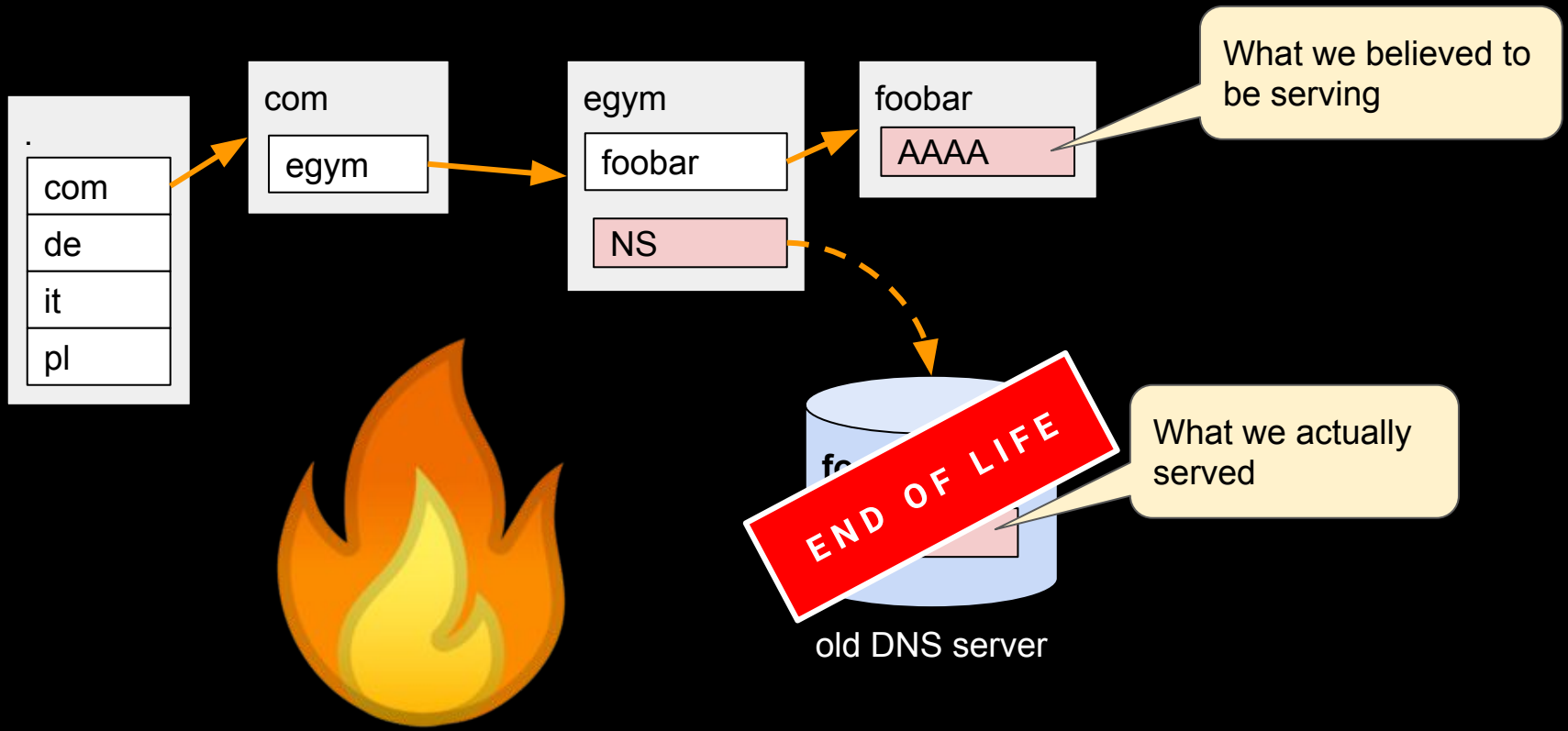


RRDB Internals: Today's Features

- Logic checks within nodes
  - E.g. CNAME and most other record types are mutually exclusive
- Back-and-forth traversal
  - Parent pointers
- Logic checks across nodes
  - E.g. Node with NS records should not have children
- Walk and query the Trie
- Idea: Inheritance of certain values (e.g. TTL)



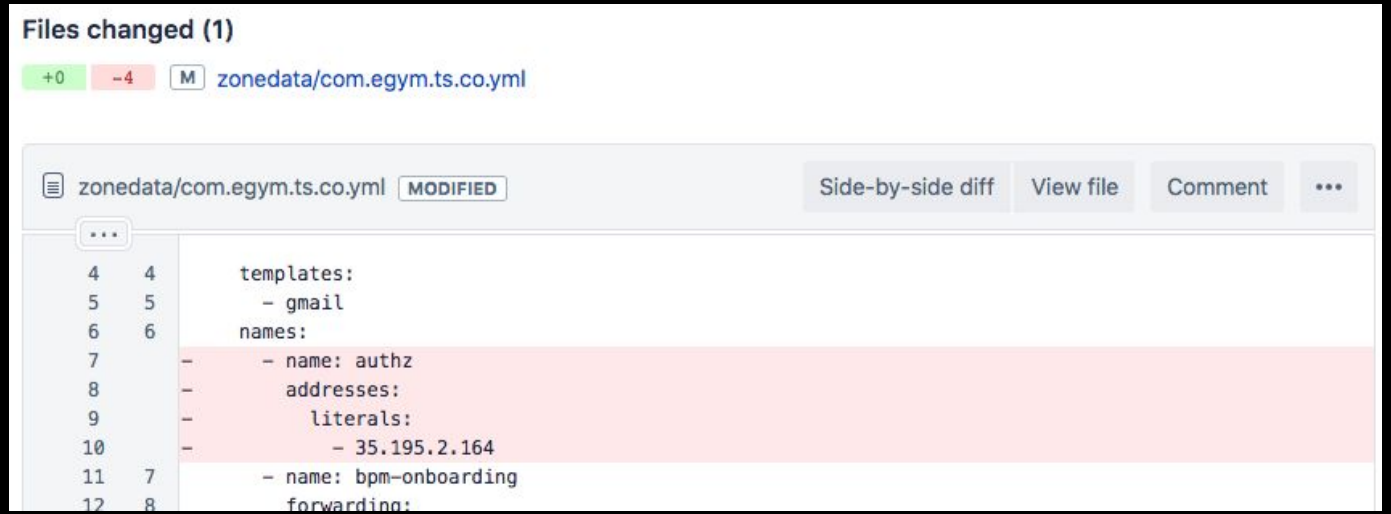
RRDB Internals: Past Disasters



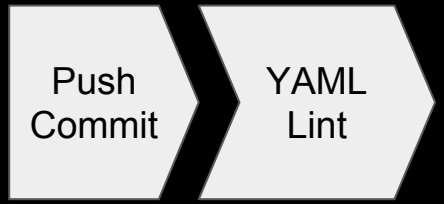
New Process

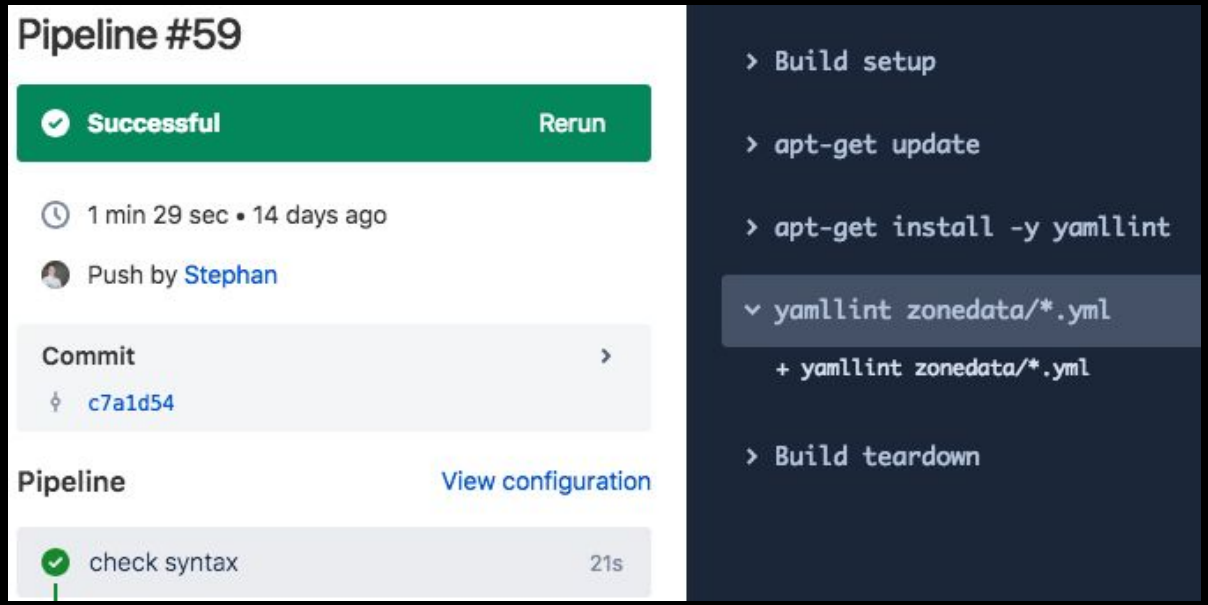
New Deployment Workflow

Push Commit

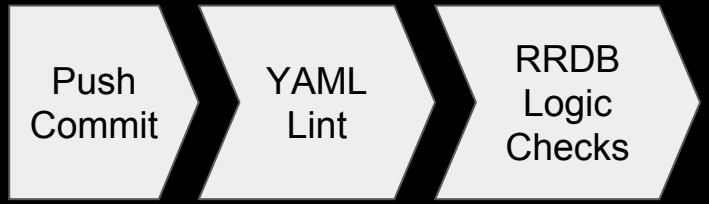


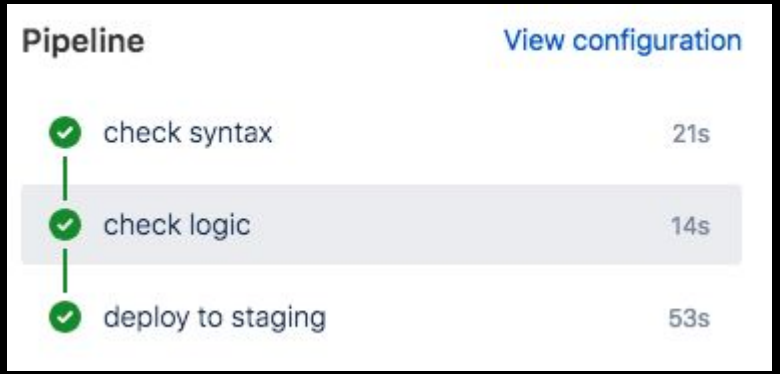
New Deployment Workflow

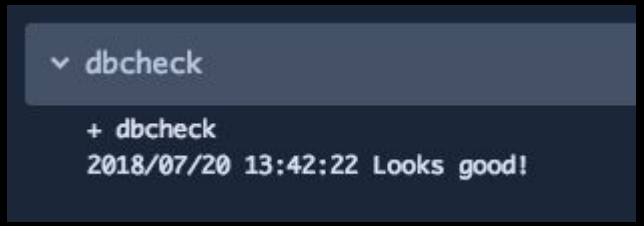




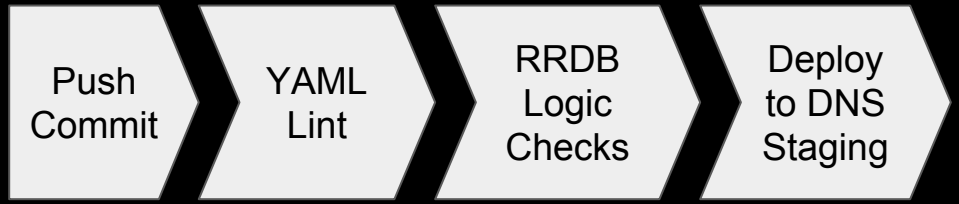
New Deployment Workflow

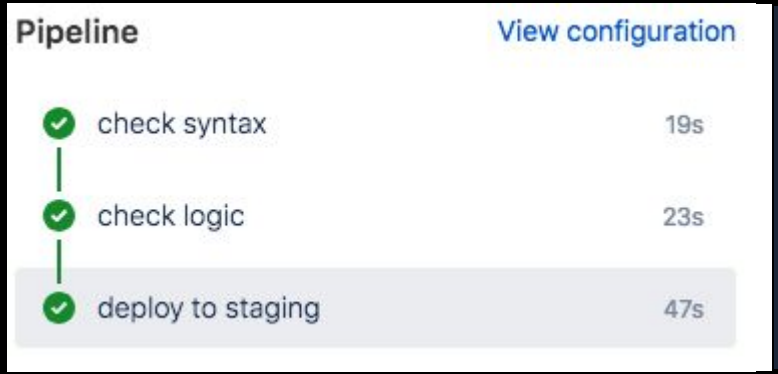






New Deployment Workflow

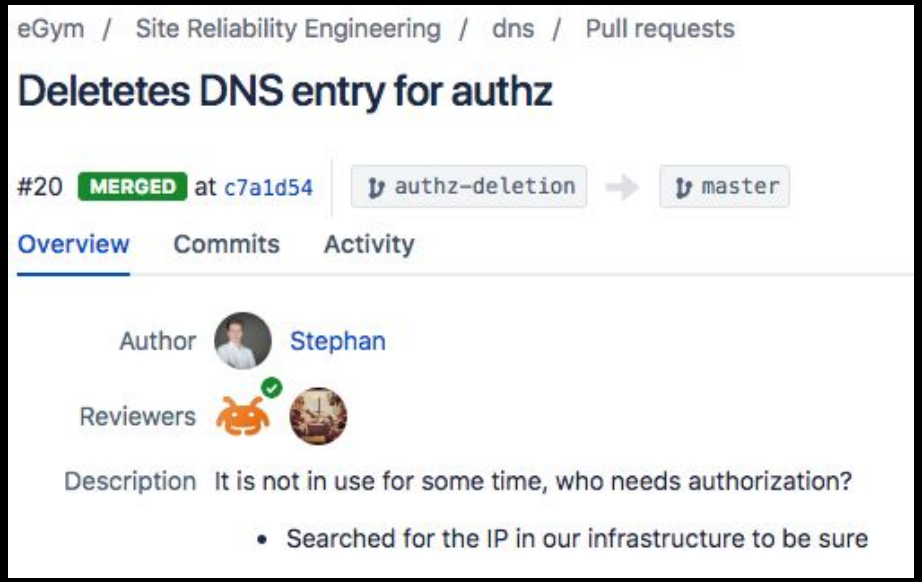




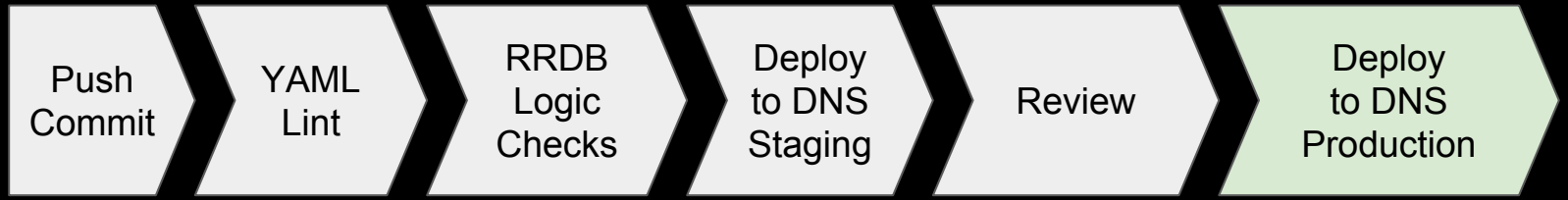

```
egym.at. 2018/07/20 08:50:23 nothing to change
egym.net. 2018/07/20 08:50:24 nothing to change
egym.com. 2018/07/20 08:50:24 1 record to be deleted
egym.com. 2018/07/20 08:50:24 *authz.co.ts.egym.com. A 300
egym.com. 2018/07/20 08:50:24  *35.195.2.164
egym.com. 2018/07/20 08:50:24 requesting change...
egym.com. 2018/07/20 08:50:24 request pending...
egym.com. 2018/07/20 08:50:25 request status: done
egym.directory. 2018/07/20 08:50:25 nothing to change
egym.bg. 2018/07/20 08:50:25 nothing to change
```

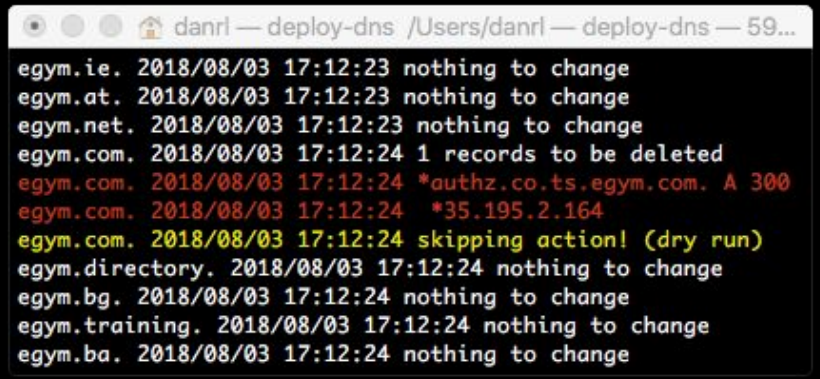
New Deployment Workflow

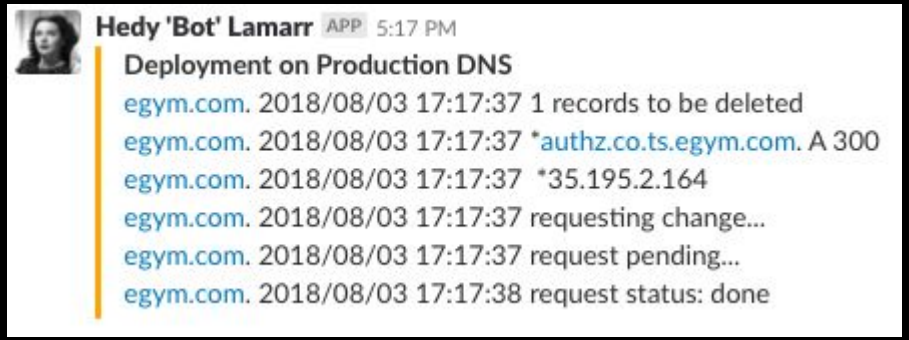
Push Commit → YAML Lint → RRDB Logic Checks → Deploy to DNS Staging → Review



New Deployment Workflow







Benefits of New Process

- DNS workflow and moving parts are out-of-band
  - Code and Pipeline on Bitbucket
  - Independent from the records we serve
- Pipeline run takes ~1.5 minutes
  - Before: review took hours or days
  - Including all checks
  - Including full staging deployment

Lessons Learned



Automated checks lower the entry barrier and empower developers.

Democratize critical infrastructure!

De-haunt the graveyards!

Battle-tested Existing Tools

- Record Store (Shopify)
  - No Cloud DNS support (added Jan '18)
  - We were just moving away from Ruby within SRE
- OctoDNS (Github)
  - No Cloud DNS support (added Oct '17)
- Denominator (Netflix)
  - No Cloud DNS support
- DNSControl (Stack Exchange)
  - Go
  - Uses Domain Specific Language
  - We did not know about it 😭





Lesson Learned

We may have fallen for Not-Invented-Here...?

Do proper research!

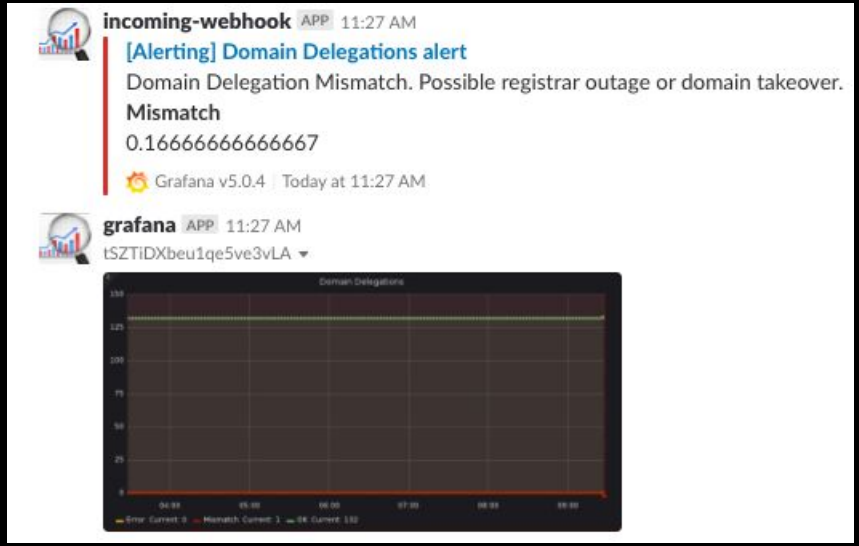


Use our tools if all of the following apply

- You love YAML
- You need a Go library (RRDB)
- Google Cloud DNS is your only DNS provider
- You need to walk & query the final dataset
  - Custom checks
  - Service Discovery
  - Special Needs
- Prefer a small binary
  - that fits into out-of-band pipelines



Achievements Unlocked



- DNS is finally out-of-band
- DNS is not scary anymore!
  - Spreads the review load from SRE to everyone
- Certificate Automation in Kubernetes
  - Cluster Issuer uses DNS-01 challenge
    - works for client certificate protected hostnames
  - Developers can request valid Let's Encrypt certificates via Certificate Resource
    - even before DNS is pointed to the corresponding Ingress Resource
- Configuration-less Delegation Monitoring
  - Automatically monitors all domains that appear on Cloud DNS
  - Alert on domain take-over
  - Alert on delegation errors



eGYM

Open Source *dns-tools* and *RRDB*

- https://bitbucket.org/egym-com/dns-tools/

Full story of our DNS Journey in our tech blog!

- https://code.egym.de/

Fitness and engineering careers: egym.com



Mostly non-political, tech-related, (re-)tweets: **@danrl_com**
I blog about SRE and technology: **https://danrl.com**

Join Munich SRE Meetup!

