RIPE NCC
RIPE NETWORK COORDINATION CENTRE

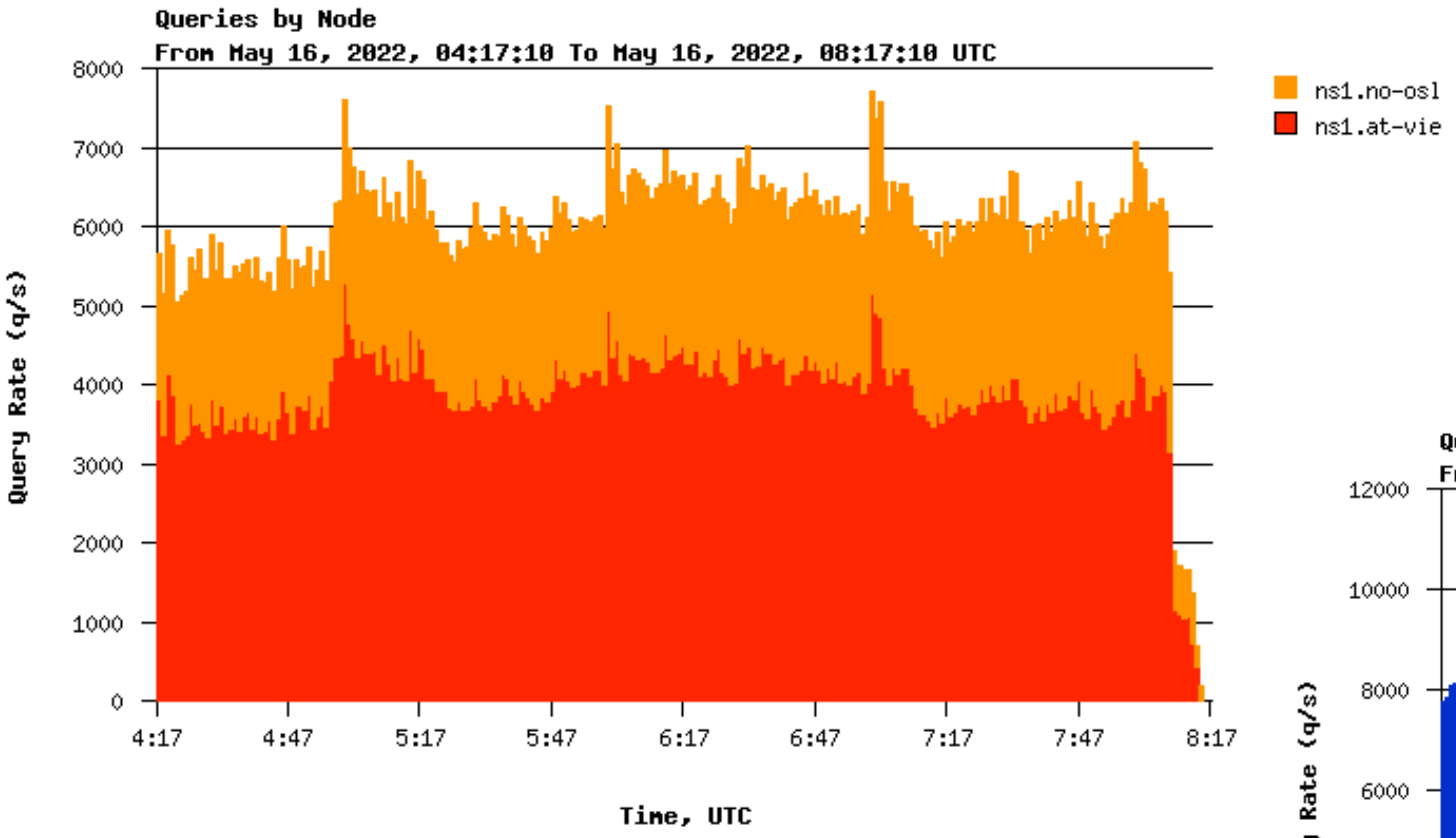
RIPE NCC DNS Update

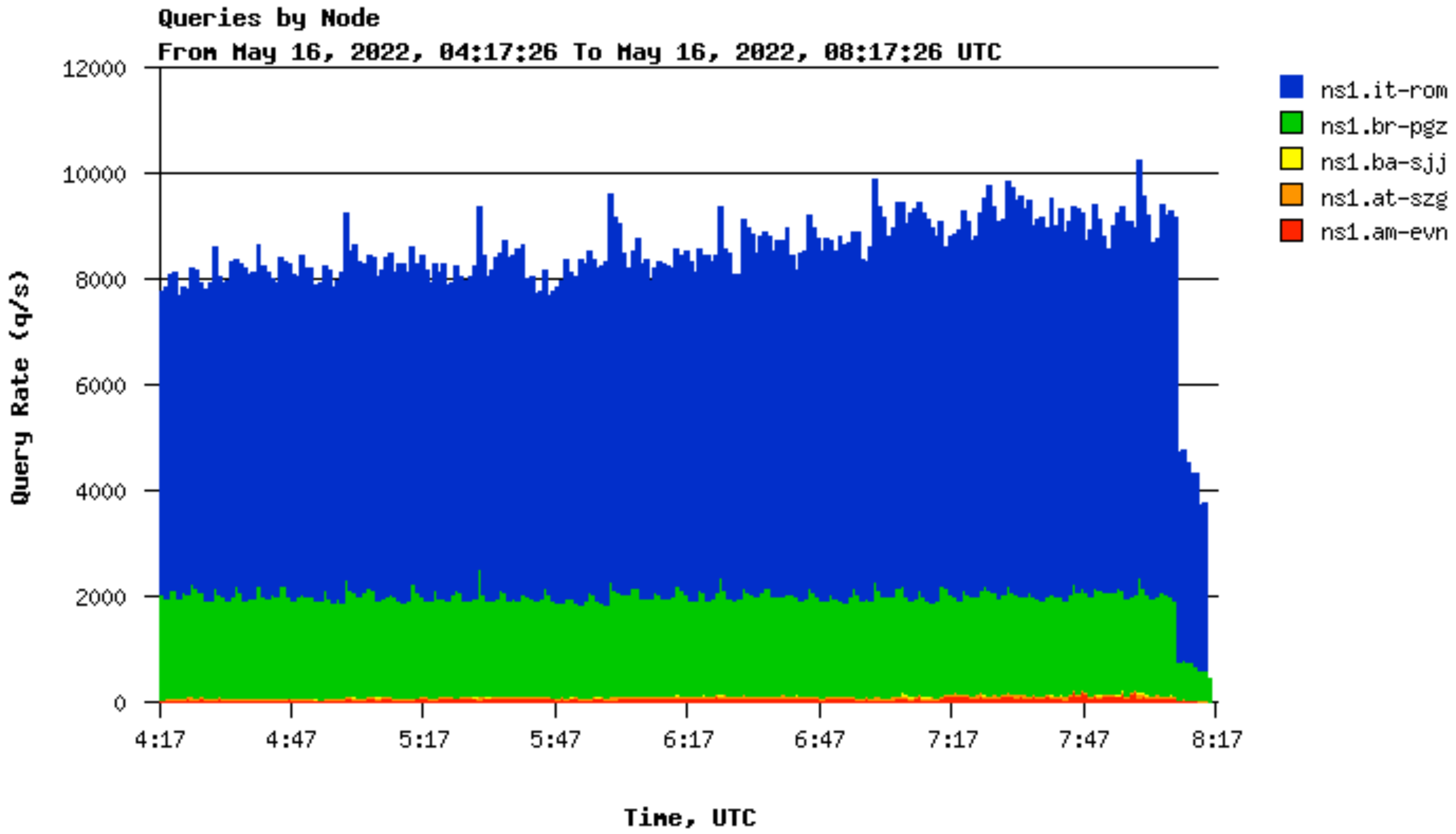
Florian Obser | 19 May 2022 | RIPE 84

Hosted DNS

- Community-supported expansion of RIPE NCC's Anycast DNS services: K-root and AuthDNS
- K-root is widely covered, with 87 hosted instances worldwide
- AuthDNS has just 7 hosted instances, 3 new since RIPE 83
  - Salzburg
  - Sarajevo
  - Yerevan

Hosted AuthDNS Query Rate





About 10% of total query rate

Switch to Combined Signing Key

- Our KSKs and ZSKs were stored together on the signer
- Our algorithm 13 keys are of the same size
- Algorithm 13 keys offer stronger security, avoiding the need for frequent ZSK roll-overs
- In the first week of May 2022, we switched to CSKs for all our zones, by performing a KSK roll-over
  - In our Knot DNS signer configuration, we enabled the “single-type-signing” option
  - Knot DNS waited for DS record updates, and then gracefully withdrew old keys
  - No outages seen or reported

Effect of Using a CSK

```
ripe.net.  3600  DNSKEY   257 3 13 l90y… ; id = 60427
ripe.net.  3600  RRSIG DNSKEY 13 2 3600 20220526120652 20220512103652 60427 ripe.net. B9+3…

ripe.net.  3600  SOA     manus.authdns.ripe.net. dns.ripe.net. 1652691582 3600 600 864000 3600
ripe.net.  3600  RRSIG SOA 13 2 3600 20220530085942 20220516072942 60427 ripe.net. emf0…

ripe.net.  3600  A    193.0.6.139
ripe.net.  3600  RRSIG A 13 2 300 20220525110652 20220511093652 60427 ripe.net. D1+0…
```

Lower TTLs for NS and DS records

- Proposal to DNS Working Group in November 2021, about lowering TTLs on NS and DS records
  - There was support from various people, and no objections
- We lowered the TTLs on Wednesday, 20 April 2022
  - NS records: 86400
  - DS records: 3600
- There was NO increase in query rates at RIPE NCC's servers
- Lower TTLs on DS records help operators complete their KSK roll-overs more quickly

Zonemaster

- We use Zonemaster to perform pre-delegation checks when domain object updates are submitted to the RIPE Database
  - Test results are emitted at INFO, NOTICE, WARNING, ERROR and CRITICAL levels
  - A domain object update is rejected if any result is at ERROR or CRITICAL levels
- On 9 May 2022, we switched to a newer version of Zonemaster
  - Bug fixes
  - Additional checks
  - Support for newer DNSSEC algorithms such as ED25519 and ED448

IPv6-only for Management Interfaces

- We have switched to IPv6-only for the management interfaces of our Anycast DNS servers:
  - K-root: Amsterdam, London, Ponta Grossa, Salzburg, Tokyo
  - AuthDNS: Amsterdam, London, Ponta Grossa, Salzburg, Stockholm
- All management services (e.g. monitoring, SSH, zone transfers) run over IPv6
- We plan to keep switching more sites to IPv6-only
- Some networks are still problematic - their management traffic will remain dual-stacked or IPv4-only for the time being

Hardware Replacement

- The hardware of the K-root sites in Frankfurt and Miami is old and needs to be refreshed
- Delays in hardware delivery, caused by the ripple effect of the global pandemic
- We hope to have the hardware replaced in the latter half of 2022

New Core Site for AuthDNS

- The AuthDNS anycast cluster is composed of 3 core sites in Europe, and 7 hosted sites
- Increase capacity and resilience by adding a fourth core site, ideally outside of Europe
- Aim to deploy by the end of 2022
    - Hardware delivery delays may be an issue

Software Stuff

- We continue to run a mix of BIND, Knot DNS and NSD
- For BGP, we recently introduced FRRouting next to BIRD
  - Needed to roll our own packages with a small patch to work with multiple routing tables in Linux
- We run CentOS 7, but will soon update to a distribution derived from a newer version of RedHat Enterprise Linux

Questions ?

fobser@ripe.net