RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC DNS Update

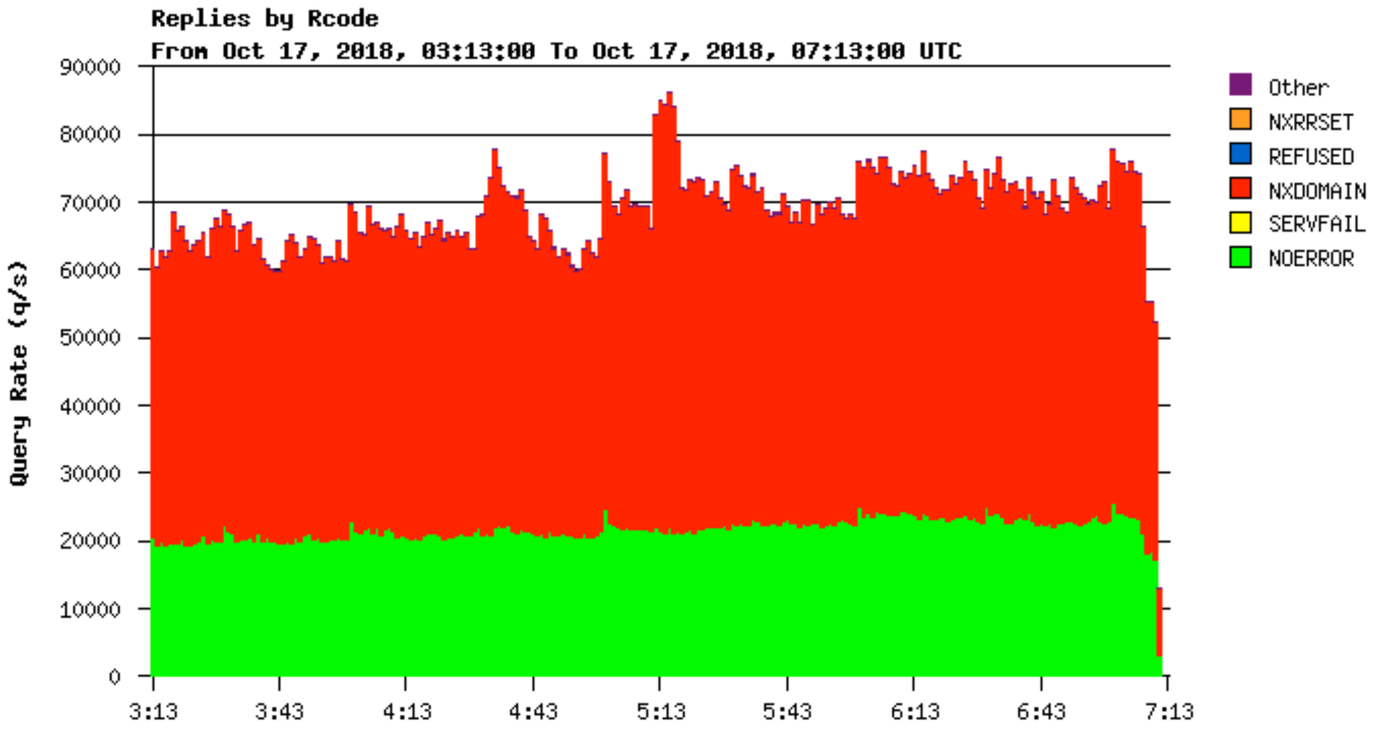
K-root and DNSSEC

Anand Buddhdev | October 2018 | RIPE 77

K-root

Status

- 63 instances (2 new since RIPE 76, in Vilnius and Lugansk)
- Response rate across all of K-root



Capacity and usage

- **About 100 Gbit/s**
  - Most instances connected at 1 Gbit/s, with some core sites at 10 Gbit/s
- **About 250 Mbit/s outbound on average**
- **Usage not evenly distributed**

Expansion

- **We are upgrading remaining core instances to 10 Gbit/s**
- **RIPE NCC executive board approved budget for a new 100 Gbit/s instance in 2018**
  - We plan to add a new instance, with 100 Gbit/s capable hardware
  - However we will not connect at 100 Gbit/s initially
  - 100 Gbit/s transit is expensive at small scale
  - Engineering challenges of handling traffic at such high speed
  - Once we have more instances with 100 Gbit/s capable hardware, we can connect them all at faster speeds

DNSSEC

Signer migration

DNSSEC history

- **2005-2010**
  - Perl tools wrapping **dnssec-signzone**
  - Despite automation with scripts and cron jobs, there was much manual work
- **2010-present**
  - Secure64 signer - proprietary solution
  - Very few choices (open source or otherwise)
  - Runs on HP Itanium servers (more security, courtesy of Itanium architecture)
  - Better automation

Reasons for migration

- **Old hardware - signers are over 8 years old now**
- **Cost - Secure64 solution isn’t cheap**
- **Open source has become better**
  - Many good solutions to choose from
  - Good support - bugs and feature requests are handled quickly
  - Great communities around each solution - more knowledge sharing

Important evaluation criteria

- Good and up to date documentation
- Bump-in-the-wire signing (XFR in, sign, XFR out)
- Support for modern algorithms and algorithm roll-over
- Automated ZSK and KSK roll-overs
- Safety during KSK roll-overs
- Clear and verbose logging
- Import foreign ZSKs to allow for seamless migration

The contenders

- BIND - good DNSSEC support, flexible
- OpenDNSSEC - dedicated signer, flexible
- PowerDNS - used by some large hosting companies for signing customer zones
- Knot DNS - relatively new DNSSEC support
- Secure64 - new x86_64 signer based on Knot DNS

The contenders

Nitpicking

BIND

- **BIND >= 9.11 has *dnssec-keymgr***
  - Only gets built and installed if the build server has the Python “ply” module installed
  - The manual has no information about it either; it’s only mentioned in the release notes
- **DNSSEC documentation on ISC’s website is outdated**

OpenDNSSEC

- **Not packaged for CentOS 7**
- **Documentation is outdated**
- **Configuration in XML**
  - Difficult to write, read and maintain
- **Requires PKCS#11 library and SoftHSM, even if no HSM is used**

PowerDNS

- “pdnsutil secure-zone ZONE”
- No automatic key roll-over
- Needs more config to work with non-PowerDNS slaves

And the winner is…

Secure64 x86_64 signer

- Based on Knot DNS
- Costs $$$
- May lag behind the official version released by CZ.NIC

Signing with Knot DNS

```
template:
  - id: default
    dnssec-signing: on
```

```
policy:
  - id: mypolicy
    algorithm: rsasha256
    zsk-size: 1024

template:
  - id: default
    dnssec-policy: mypolicy
    dnssec-signing: on
```

Migration plan

Private key export

- **Export private portions of KSKs and ZSKs from old signer**
  - Import keys into new signer
  - Sign zones with these keys
  - Switch XFR from old signer to the new signer
  - Done! :)
- **However… this isn’t possible**
  - The old signers do not allow exporting private keys

Migration with a key roll-over

- **Set up new signer, and configure zones**
- **Let it generate new KSKs and ZSKs for each zone**
- **Export public ZSKs from new signer into old signer**
  - Old signer signs the DNSKEY RRset (including new signer's ZSK) with its KSK
- **Export public ZSKs from old signer into new signer**
  - New signer signs the DNSKEY RRset (including old signer's ZSK) with its KSK
- **Add DS records of new signer's KSKs into relevant parent zones**

DNSKEY RRsets

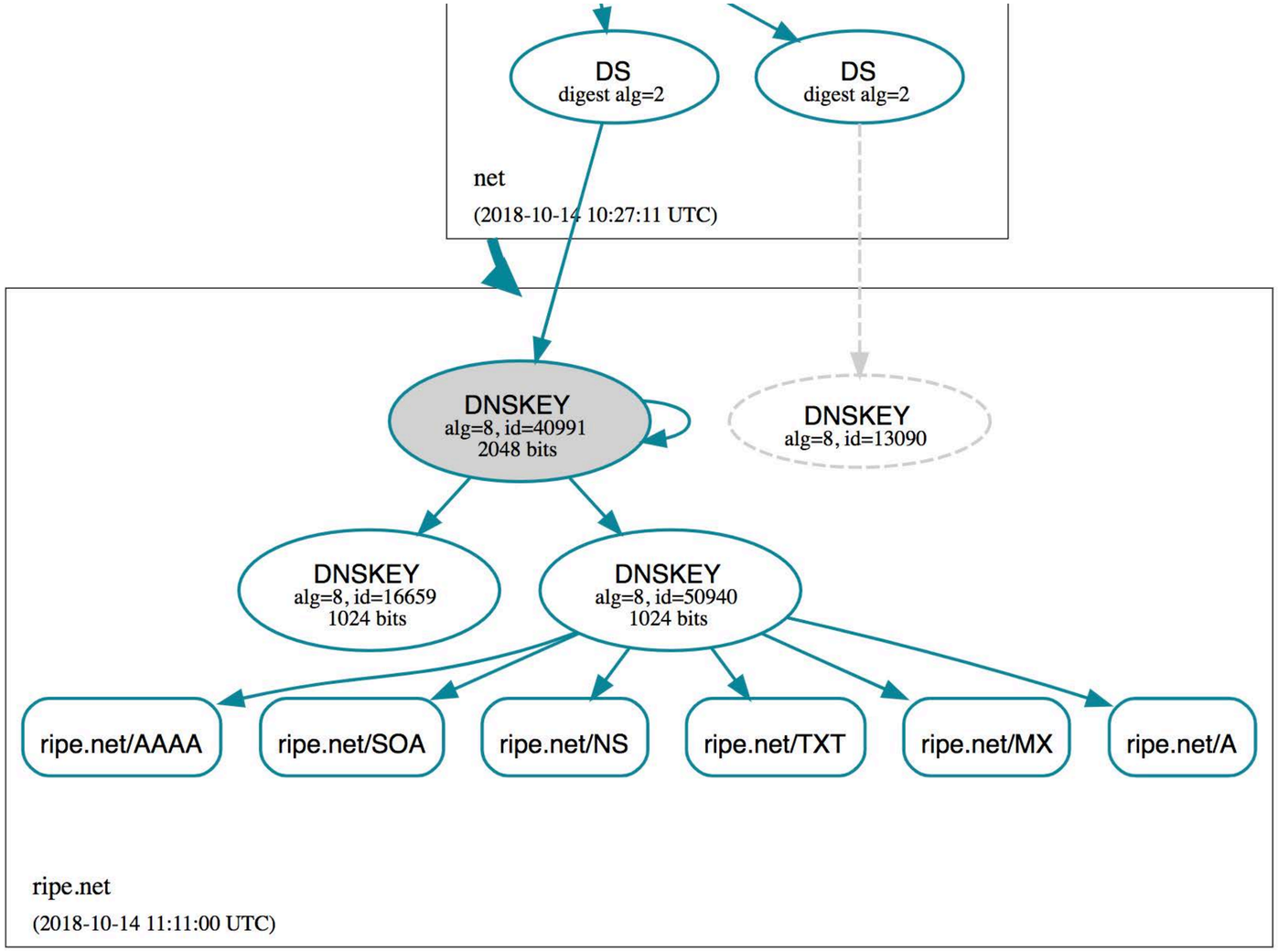
```
; <<>> DiG <<>> @oldsigner ripe.net any +norec +dnssec +multi
ripe.net. 3600 IN DNSKEY 256 3 8 AwEAAbLTfDP…; ZSK; alg = RSASHA256; key id = 16659
ripe.net. 3600 IN DNSKEY 256 3 8 AwEAAbLwKBk…; ZSK; alg = RSASHA256; key id = 50940
ripe.net. 3600 IN DNSKEY 257 3 8 AwEAAf9kY9W…; KSK; alg = RSASHA256; key id = 13090
ripe.net. 3600 IN RRSIG DNSKEY 8 2 3600 20181115100324 20181016090324 13090 ripe.net. …
ripe.net. 3600 IN RRSIG    SOA 8 2 3600 20181115100324 20181016090324 16659 ripe.net. …
```

```
; <<>> DiG <<>> @newsigner ripe.net any +norec +dnssec +multi
ripe.net. 3600 IN DNSKEY 256 3 8 AwEAAbLTfDP…; ZSK; alg = RSASHA256; key id = 16659
ripe.net. 3600 IN DNSKEY 256 3 8 AwEAAbLwKBk…; ZSK; alg = RSASHA256; key id = 50940
ripe.net. 3600 IN DNSKEY 257 3 8 AwEAAbziD7q…; KSK; alg = RSASHA256; key id = 40991
ripe.net. 3600 IN RRSIG DNSKEY 8 2 3600 20181026095159 20181012082159 40991 ripe.net. …
ripe.net. 3600 IN RRSIG    SOA 8 2 3600 20181030155802 20181016142802 50940 ripe.net. …
```

DS RRset

```
; <<>> DiG <<>> ripe.net ds +dnssec
ripe.net.  4187  IN  DS  13090 8 2 B4F2C7…
ripe.net.  4187  IN  DS  40991 8 2 D8D3C8…
```

DNSViz


DS
digest alg=2
DS
digest alg=2
net
(2018-10-14 10:27:11 UTC)
DNSKEY
alg=8, id=40991
2048 bits
DNSKEY
alg=8, id=13090
DNSKEY
alg=8, id=16659
1024 bits
DNSKEY
alg=8, id=50940
1024 bits
ripe.net/AAAA
ripe.net/SOA
ripe.net/NS
ripe.net/TXT
ripe.net/MX
ripe.net/A
ripe.net
(2018-10-14 11:11:00 UTC)

Signer security

- Minimal CentOS installation
- No HSM - keys on encrypted disk partition
- Only DNS and monitoring allowed into and out of the server
  - No SSH, SMTP, HTTP
- Operators can only login at the console, which they can only reach via the server's iDRAC
- SSH and HTTPS may be briefly opened to reconfigure or update the server

DNSSEC

CDS / CDNSKEY automation

Reverse DNS delegation

```
domain:          0.0.193.in-addr.arpa
descr:           RIPE NCC Internal Use
admin-c:         BRD-RIPE
tech-c:          OPS4-RIPE
zone-c:          GII-RIPE
mnt-by:          RIPE-GII-MNT
created:         2002-07-05T11:37:47Z
last-modified:   2018-09-25T09:19:40Z
source:          RIPE
nserver:         manus.authdns.ripe.net
nserver:         sns-pb.isc.org
nserver:         ns4.apnic.net
nserver:         tinnie.arin.net
nserver:         a1.verisigndns.com
nserver:         a2.verisigndns.com
nserver:         a3.verisigndns.com
ds-rdata:        62081 8 2 cc8cf3a7d515cdbd55ad83859249dc78c9b5b287e41745f37a40bf0860b6d06d
ds-rdata:        29132 8 2 bf17be59f139975d984792913f61469952599995f9d1b08e3c50d9006b7731ad
```

CDS/CDNSKEY for automation

- **RFC 8078 describes automation for DS record updates**
- **Two main issues for RIPE NCC**
  - Implementation - scan all delegations or only the secure ones
  - Updating domain objects - normally RIPE NCC does not update users' objects

Questions

anandb@ripe.net