

BIND 9.11's new features (BIND 9.11 新機能)

Mukund Sivaraman

muks@isc.org

Internet Systems Consortium

New in BIND 9.11

- ▶ Provisioning
 - ▶ Catalog Zones
 - ▶ DynDB
 - ▶ `rndc showzone`, `modzone` and NZD backend
- ▶ DNSSEC
 - ▶ Negative trust anchors
 - ▶ Child CDS/CDNSKEY automatic generation
 - ▶ DNSSEC key manager
- ▶ Other
 - ▶ `dnstap` logging
 - ▶ EDNS CLIENT-SUBNET (authoritative)
 - ▶ Performance improvements

Provisioning

- ▶ Before Catalog Zones, operators didn't have any way to automatically create a new zone on a slave server to match a new zone on a master, other than accessing the slave's configuration file and executing a reconfig.
- ▶ Operators wanted **standardized provisioning** that didn't require maintaining custom scripts and methods for updating slaves.
- ▶ Some operators wanted ability to serve zone data from a shared database backend.
- ▶ BIND administrators found that deleting zones when using **NZF config files (rndc delzone)** was slow when the number of zones was large.

Catalog Zones

- ▶ A **DNS catalog** is a list of zones.
- ▶ A **catalog zone** is a regular DNS zone that contains the list of zones represented as regular RRs within the zone.
- ▶ Slaves transfer this zone from the master and **reconfigure automatically** to serve the list of zones within the catalog.
- ▶ When a zone name is added to the catalog zone on the master, the catalog zone update is transferred to the slaves. The slave then adds the new zone to its configuration automatically and transfers the new zone's contents from the master.
- ▶ We are trying to standardize the method as `draft-muks-dnsop-dns-catalog-zones-01`.

Catalog Zone Example

```
cat.isc.org. IN SOA . . 2016022901 900 600 86400 1
cat.isc.org. IN NS nsexample.
```

```
version.cat.isc.org. IN TXT "1"
```

```
5960775b5c.zones.cat.isc.org. IN PTR domain1.com.
0e2ffd0d66.zones.cat.isc.org. IN PTR domain2.net.
ab89bcd650.zones.cat.isc.org. IN PTR domain3.org.
```

DynDB - dynamic DB interface

- ▶ **dns_db** C API interface is used by **named** to store zone data, and access zone data when serving DNS queries.
- ▶ **RBTDB** is the default statically linked **dns_db** implementation within **named** that is used to store zone contents in memory.
- ▶ **DynDB** allows administrators to install other **dns_db** implementations as dynamically loadable **.so** modules that provide other backends such as SQL databases, customized answer generation, etc. Such modules are called **drivers**.
- ▶ Currently there are no drivers in BIND 9.11. We hope that some will be contributed for open source SQL databases.

Negative Trust Anchors

- ▶ **rndc nta** command can be used to **temporarily** disable DNSSEC validation for a domain for a specific duration.
- ▶ This is useful to a resolver operator in case a popular domain is failing DNSSEC validation temporarily and gets complaints from users that they are not able to resolve names within that zone.
- ▶ **named** will periodically test to see whether data below an NTA can now be validated.
- ▶ The negative trust anchor expires after the configured time.

Child CDS/CDNSKEY automatic generation

- ▶ BIND now automatically creates CDS and CDNSKEY records, signed by the KSK.
- ▶ The parent side of a delegation can poll the child zone for these CDS and CDNSKEY and automatically update DS records on the parent.
- ▶ This allows rolling the KSK without requiring a manual update of the DS record in the parent zone.
- ▶ Note that BIND does not currently implement parent-side behavior of automatically updating the DS records.

dnssec-keymgr - DNSSEC key manager

- ▶ Python wrapper tool to facilitate the key rollover process for zones handled by BIND. It calls BIND utilities.
- ▶ Reads a policy definition file (default: `/etc/dnssec.policy`) and creates or updates DNSSEC keys to ensure that a zone's keys match the policy for that zone.
- ▶ New keys are created when necessary.
- ▶ Existing keys' timing metadata is adjusted as needed to set the correct rollover, etc.
- ▶ If the policy changes, all applicable keys are corrected.
- ▶ It is expected that this tool will be run automatically and unattended (for example, using `cron`).

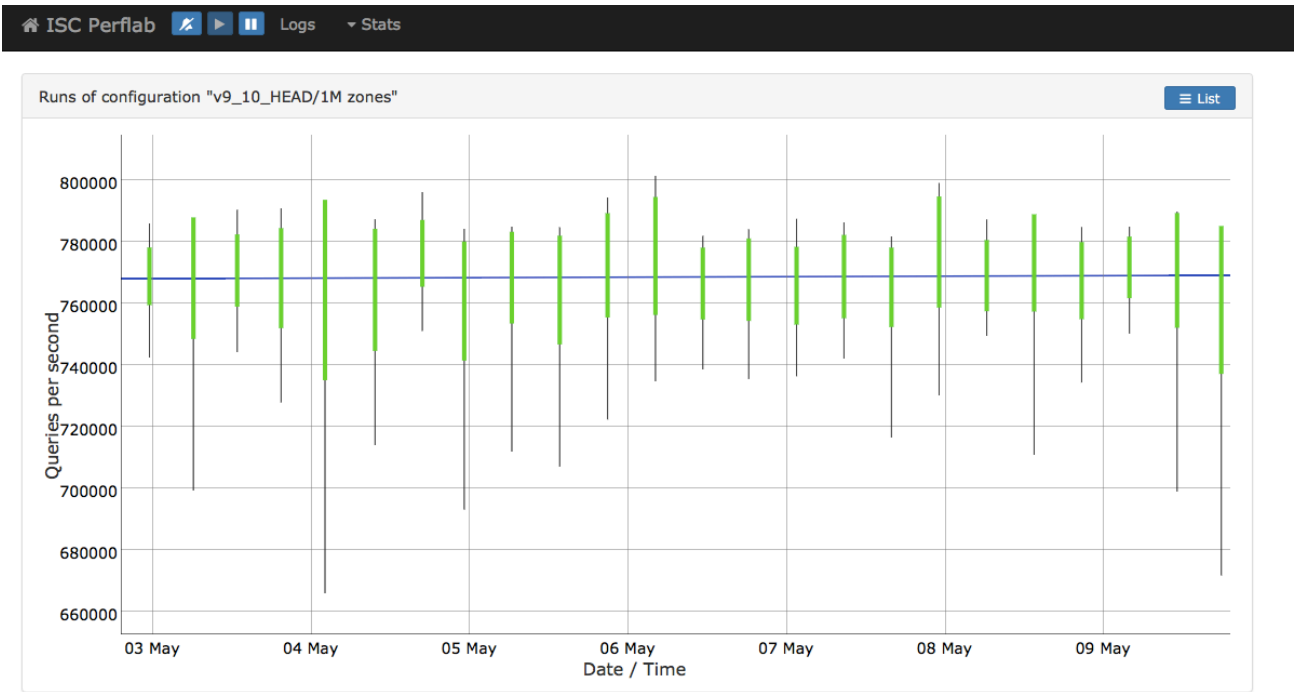
EDNS CLIENT-SUBNET

- ▶ A basic experimental implementation of authoritative CLIENT-SUBNET has been added in 9.11.
- ▶ During 9.11 development cycle, we also implemented resolver EDNS CLIENT-SUBNET support for BIND which is complete and ready for production use, but we cannot release it currently due to contractual reasons. We plan to make it available to subscription users, but it will not be released in public releases until some time in 2018.




Changes to BIND development process

- ▶ Performance lab.
- ▶ Fuzz testing.





























































Perflab - continuous benchmarking



Perflab - list of tests

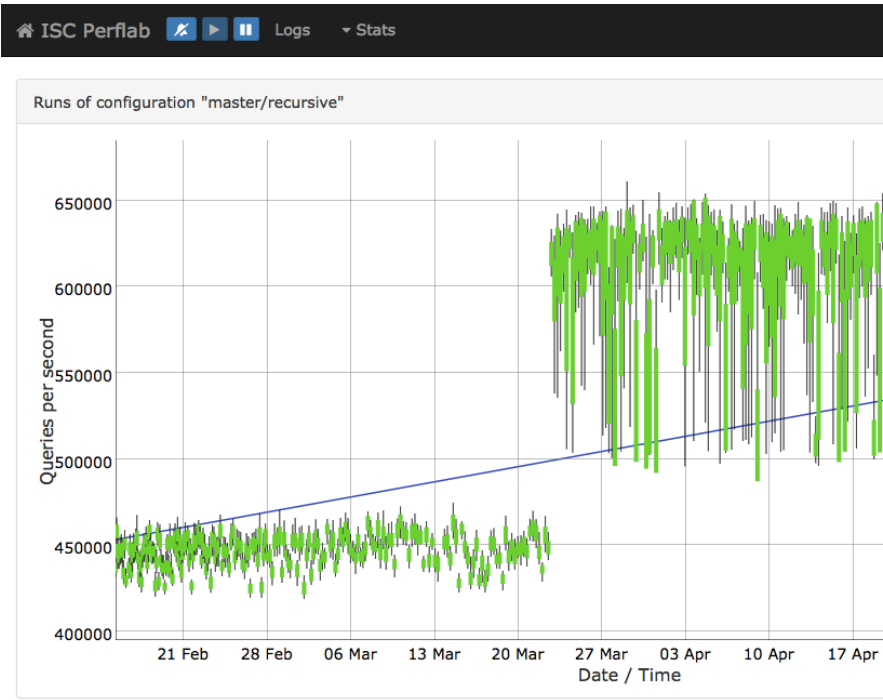
ISC Perflab    Logs ▼ Stats

Configurations View

master/1k zones	     Edit
master/1M RRs	     Edit
master/recursive	     Edit
master/root zone	     Edit
master/root/minimal	     Edit
rt42188_freebsd	     Edit
v9_10_HEAD/1M RRs	     Edit
v9_10_HEAD/1M zones	     Edit
v9_10_HEAD/recursive	     Edit
v9_9_HEAD/1M RRs	     Edit
v9_9_HEAD/1M zones	     Edit
v9_9_HEAD/recursive	     Edit

New

Perflab - noticing QPS changes



Fuzzing and CVE announcements

- ▶ ISC has been fuzz testing BIND to find defects pro-actively.
- ▶ Over the past year, CVEs have been issued for bugs found internally by fuzzing and code review.
- ▶ Patch is always available for users with a CVE announcement. JPRS makes Japanese translations of release announcements: <https://jprs.jp/tech/>
- ▶ OS distributions are given notice to prepare patched packages in advance so users can upgrade on announcement day.
- ▶ Most of these CVE bugs (crash-capable) were introduced many years ago. Quality of the codebase is increasing as we remove these bugs and refactor code.

End

- ▶ We want feedback from Japanese community. We see many issues discussed on Twitter in Japanese language.
- ▶ Discuss issues on bind-users mailing list:
<https://lists.isc.org/mailman/listinfo/bind-users>