OARC31

Software Report

Jerry Lundström

Oct 10, 2019

Table of Contents

1 Development platforms

The development server (sponsored by Netnod) runs a bunch of VMs to do continuous building and testing which is managed by Buildbot.

> https://dev.dns-oarc.net/

Our platforms, which we keep to the latest stable/LTS release, are:

- Debian 10
- Ubuntu 18.04.3
- CentOS 7.7.1908
- FreeBSD 12.0-RELEASE-p10
- OpenBSD 6.5

1.1 Automated package building

As announced at OARC30, package building is now triggered automatically when building develop and master branches of all our projects!

For Debian, Ubuntu and SLE/openSUSE, this is triggered by buildbot after a successful build of the main branches. For EPEL/Fedora we use COPR's own webhooks to trigger this directly from GitHub.

All platforms use my personal `dist-tools` scripts to create tarballs, deb-files etc.

All packages built from develop branch will have an additional version added to them as ".<seconds since 1970–01–01 00:00:00 UTC>", which makes it simple for all package managers to update to the latest development version once built.

For Debian we build and publish packages ourselves, using `cowdancer-dist` and `reprepro`. For Ubuntu we build on LaunchPad. For SLE/openSUSE we build on SUSE's Open Build System. And for CentOS/EPEL/Fedora we build on COPR.

In early September I received a pull request for dnsperf by Petr Menšík (Red Hat) for enhancement of the COPR Makefile to better check prerequirements, reuse the rpmbuild directory and checked out dist-tools, and to be able to obtain the source with spectool. These changes have been applied to all projects.

You can find more information, instructions and links at:

> https://dev.dns-oarc.net/packages

Today we build packages for:

- Debian: Stretch (stable), Buster (testing), Sid (unstable)
- Ubuntu: Xenial (16.04), Bionic (18.04), Disco (19.04), Eoan (19.10)
- CentOS/RHEL: EPEL 7
- Fedora: 29, 30, 31, rawhide

- SUSE Linux Enterprise: 12 SP3, 12 SP4, 15, 15 SP1
- openSUSE: Leap 15.0, Leap 15.1, Tumbleweed

2 Software Updates

A key part of DNS-OARC's mission is to develop, maintain and host various software tools for DNS data collection, measurement and analysis. OARC can develop new, or enhance features of existing, tools via a custom for-hire development contract. OARC Members will receive priority for such work, and at a discounted rate depending on their membership tier.

You can find a list of all our software and information about funded development here:

> https://www.dns-oarc.net/oarc/software

2.1 dnsperf

dnsperf and resperf (part of dnsperf) are tools that makes it simple to gather accurate latency and throughput metrics for DNS services. These tools are easy-to-use and can simulate typical Internet usage, so network operators can benchmark their naming and addressing infrastructure and plan for upgrades.

v2.3.0

With the release of v2.3.0 we added TCP and TLS support to dnsperf and resperf. The transport mode can now be selected at runtime using `-m <mode>` for dnsperf and `-M <mode>` for resperf, and the default server port is determined by the transport mode, UDP/TCP port 53 and TLS port 853.

v2.3.1

During the development of these new modes I mostly use docker containers and I noticed a huge performance increase if I added a `poll()` for the stream sockets, so it was added to v2.3.0 release.

Quite soon after the release I got an issue from Brian Wellington (Akamai/Nominum) that TCP performance was 1/12th of what was expected. With his help and help from Jan Hák (CZ.NIC) we tracked it down to this `poll()` and with the removal of it the performance was back up at expected levels. This fix was released with v2.3.1.

Thanks Brian Wellington (Akamai/Nominum) for the initial report and testing, and Jan Hák (CZ.NIC) for testing and confirming the results.

v2.3.2

Release v2.3.2 fixes a buffer overflow when using TSIG and algorithms with digests larger then SHA256 (reported by Mukund Sivaraman).

2.2 dnscap

dnscap is a network capture utility designed specifically for DNS traffic. It produces binary data in pcap(3) and other format. This utility is similar to tcpdump(1), but has a number of features tailored to DNS transactions and protocol options. DNS-OARC uses dnscap for DITL data collections.

v1.10.1

Fix various issues found by code analysis tools, a few compiler warnings removed, undefined bit shift behavior fixed, parameter memory leaks plugged and documentation updates.

v1.10.2

Fixed bug in the handling of defragmentation configuration which lead to the use of a local scope variable later on and caused unexpected behavior.

v1.10.3

This release fix the inclusion of all plugins for the Debian and Ubuntu packages, they (especially the new anonymization plugins) were missed due to being specified one by one in the control files. The package will now include any plugin built.

2.3 dnsjit

dnsjit is a combination of parts taken from dsc, dnscap, drool, and put together around Lua to create a script-based engine for easy capturing, parsing and statistics gathering of DNS messages while also providing facilities for replaying DNS traffic.

dnsjit is available as package in the pre-release channels.

The develop branch of drool (DNS Replay Tool) is now written in Lua and can replay DNS traffic from packet capture (PCAP) files and send it to a specified server, with options such as to manipulate the timing between packets, as well as loop packets infinitely or for a set number of iterations.

v0.9.8

This new alpha release of dnsjit fixes a few issues with the PCAP link type and the processing of the network stack in `filter.layer`. It also adds a new DNS client output `output.dnscli` which can use UDP, TCP and TLS.

Query/response matching across PCAPs

Along with v0.9.8 there is a new example script for matching queries with responses, outputting statistics about them such as response time and with the option to save state (in-flight queries) between runs.

2.4 dnsmeter

dnsmeter is a tool for testing performance of a nameserver and the infrastructure around it which DENIC uses to do reliable performance measurements by configuring dnsmeter to issue queries from a wide range of IP-addresses. This allows DENIC to simulate a query pattern which is close to their production environment.

dnsmeter was moved to OARC in September (announcement) and you can read the Development Update #1910 for a technical description of the tool which also showcases some example runs.

v1.0.0

The first release of dnsmeter was made after reworking the repository and including all things necessary for making packages.

v1.0.1

While making the Development Update #1910 I wanted to include screenshots of running dnsmeter and of course ran into a few issues which got fixed in release v1.0.1.

The first issue was a dependency problem which caused dnsmeter to throw an exception when using it, others included missing the first 8 bytes in a text payload due to how it detects PCAPs and then various display bugs, such as RTT calculations.

2.5 dsc

DNS Statistics Collector (dsc) is a tool used for collecting and exploring statistics from busy DNS servers. It uses a distributed architecture with collectors running on or near nameservers sending their data to one or more central presenters for display and archiving.

v2.8.1

I managed to totally miss to add the configuration glue for the new response time indexer and everyone that tested this before the v2.8.0 release were happy with the default. Release v2.8.1 fixed that so you can now configure it.

2.6 dsc-datatool

dsc-datatool is a tool for converting, exporting, merging and transforming dsc data using a plugin architecture. It can be used to convert dsc XML data into InfluxDB which can be used by Grafana to display DNS statistics.

v0.05

I got a report that importing to InfluxDB failed because of empty values which can happen in some indexers, apparently this worked with older InfluxDB but changed in v0.90.

With release v0.05 the InfluxDB output will now quote empty values as two double quotes (`””`).

DSC + Grafana — ** Feedback wanted! **

I created dsc-datatool back in June 17 2016 as an experiment to export DSC data into Graphite. This later evolved into using InfluxDB and Grafana, and I made a wiki about how to set this up yourself.

It's now almost 3 years later(!) and I would love to hear how it's working, or not, from anyone using it, even if there are no issues!

Please drop me an email and let me know how you're using it, what platforms and if you did any modifications. I would also happily accept any Grafana dashboards you've created!

2.7 dsp

The DNS Statistics Presenter is the older graphing system that can present DSC data.

v2.0.1

This release is mostly about building and packaging the software, by adding DESTDIR support and fixing automake issues, there are no new features or changes.

3 Member software updates

3.1 Flamethrower (by NS1)

Flamethrower is a small, fast, configurable tool for functional testing, benchmark, and stress testing DNS servers and networks. It supports IPv4, IPv6, UDP, TCP and DNS-over-TLS, and has a modular system for generating queries used in the tests.

Since OARC30, Flamethrower received primarily bug and stability fixes. Overall performance was improved by avoiding full DNS response message parsing and instead processing the message header only. The query output rate limiter was improved not to cause packet burst on start and to distribute more evenly among concurrent senders. This results in more accurate measurements, especially for short test runs.

3.2 ENTRADA (by SIDN)

SIDN recently released ENTRADA 2, an open source DNS big data tool. This new version contains many new features such as support for AWS (S3 and Athena) allowing for a serverless deployment. This is a great way to get started with DNS analytics without having to invest in hardware.

Another new feature is the ability to analyze TCP handshakes (using captured DNS data) to determine the Round Trip Time (RTT) between a resolver and authoritative name server. The RTT can be used as a metric in a quality of service monitoring tool, the cool thing is that the measurements are performed using actual resolvers in the wild.

For more details see the ENTRADA website: https://entrada.sidnlabs.nl

3.3 DNS shotgun (by CZ.NIC)

DNS shotgun is a dnsjit-based project to simulate real clients from captured DNS traffic.

We are currently working on support for various connection-oriented features like DNS-over-TCP and DNS-over-TLS, and connection-oriented configuration like keep-alive and timeouts. Ultimately, the tool can be used to answer questions like “What performance will we get from this DNS server if 25% of its clients switch to DNS-over-TLS?”

Any help with the development, being collaboration or sponsorship, is greatly appreciated! Please contact Tomáš Křížek <tomas.krizek@nic.cz> if you wish to discuss this further.

As of October 2019, the shotgun prototype scales to one million UDP clients at ~450,000 QPS on commodity hardware (Xeon E5-2630, 8 cores @ 2.4 GHz).