ISC Support Subscriber News

2019 Q4

For ISC's BIND 9, ISC DHCP, and Kea DHCP support subscribers.

BIND/DNS News

BIND 9.16, due in early 2020, will replace BIND 9.11 as the next ESV

New Key and Signing Policy (KASP) Tool in BIND

The 9.16 release includes significant refactoring, particularly of the network socket handling, but there will be a few new features that have not yet appeared in the 9.15.x branch.

One of these is a new KASP feature, targeted for release in BIND 9.16.0. It will replace the dnssec-keymgr tool run from cron with a built-in state machine that both prevents zones from going bogus and is self-healing. We hope that this new tool will make it much easier to maintain DNSSEC-signed zones.

The BIND KASP tool allows users to apply the default policy or customize a policy for each zone, specifying the algorithm(s) to use and the signature validity and resigning intervals. For organizations for whom the default settings are adequate, establishing ongoing key maintenance is dramatically simplified to a statement like:

```
Zone "example.com"
{ ...
dnssec-policy "_default";
}
```

Restricted-access packages for subscribers

We have had a lot of questions about the status and our plans for producing binary packages for BIND 9 subscribers. We recommend ISC support subscribers use the restricted access packages on Cloudsmith, because, unlike the open source repositories, we can update those packages during the embargo period of a security vulnerability. For more information, see your support queue and this KB article on ISC packages for BIND 9.

Encrypted DNS - The Discussion Continues

DNS over HTTPS (DoH) was originally proposed to improve page loading times for web pages that had to fetch content from numerous external places in order to render the page. Since it is based on HTTPS, it also provides encryption, so it has gained support as a privacy-protecting protocol. Interest in deploying encrypted DNS had been somewhat limited until this year, when many providers began offering DoH-based open resolver services.

There is both excitement and serious concern about the impact of DoH. There are arguments about the pros and cons of the technology - moving DNS lookups into HTTPS will make them virtually useless as a control point, and will break DNS firewalls - and the impact of the deployment model. Since DNS over HTTPS is enabled by the browser, there is heated debate over whether the end-user has enough visibility or technical ability to agree to this change, which hands critical network control from their ISP to their browser vendor. Several big hosted DNS providers (Google, Cloudflare, Quad9) are providing DoH services to the general public, and this has further fueled concern about the consolidation and centralization of Internet control points in the hands of fewer, larger operators.

We have heard from service providers among you that you need to have a DoH offering, at least as a 'defense' against the open DoH providers that threaten to take some of our users. For the enterprises, the concern is mostly about how to block the use of DoH in the enterprise.

One BIND user and community contributor, Tony Finch at the University of Cambridge, has written a balanced and well-informed blog on the topic of DoH, explaining the University's plans to postpone the use of DoH and the reasons for the decision.

DNS over TLS (DoT) is the other leading DNS encryption option. For a review of the possible privacy threats and a comparison of the benefits and drawbacks of DoH and the competing DoT, we recommend another blog on DNS Security: Threat Modeling DNSSEC, DoT, and DoH, by Jan Schaumann. For users with a serious need for privacy a VPN is a better option than either DoH or DoT, because a VPN protects more than just the DNS traffic.

At ISC, we plan to *implement both* DoH *and* DoT in BIND 9. We feel it is our job to provide customers with options to evaluate and deploy in accordance with their policies and their users' requirements. Research on the comparative impact on user experience of both DoH and DoT is just beginning, and requires solid implementations.

ISC has joined the Encrypted DNS Deployment Initiative, which others may wish to consider joining as well. This is an open group for researching and sharing experience in use of encryption in the DNS, including both DoH and DoT. Subscribe to the mailing list here.

New Security Policy Now in Effect

In our July newsletter we alerted customers that we were considering changing our policy for handling security vulnerabilities. The new Software Defect and Security Vulnerability Disclosure Policy went into effect in September, and so far we have been able to avoid issuing CVEs for several medium-severity BIND vulnerabilities. All BIND subscribers have already received any ASN notifications, so all the information is available, but hopefully without the need to do an emergency update of ISC customers' systems.

Kea/DHCP News

- Kea 1.6 was released in August, featuring a new configuration backend database. This enables users to manage the configuration for multiple Kea servers via a single database. However, in the process of implementing this feature, we have apparently "broken" the ability to use a database cluster as a shared lease backend. Although this configuration is not explicitly supported, we know it is popular so we are looking into it. If you are using a database cluster as a shared lease backend, please do not update to Kea 1.6 without discussing with ISC's Support team first.
- Understanding Client Classification is a new Kea KB article that customers may find useful.
- Razvan Becheriu, who joined the ISC team earlier this year after contributing to the Cassandra backend, is leading the development of multi-threading in Kea to improve performance.

With the completion of Kea 1.6, we have changed our release model. We will continue producing Stable versions, which will now all be even-numbered, and we are adding Development versions, which will be odd-numbered. We plan to issue frequent Development versions, possibly as often as monthly, to make new features available more quickly for our users to try.

Updates from Support

Customers may find themselves in contact with our new technical support engineer, Peter Davies. Peter, a Welshman who lives in Denmark, has 20+ years experience in network applications administration. Peter starts November 1, joining Alan Clegg, Michael McNally, Brian Conry, and Cathy Almond.

Meet an ISC Engineer!

Michał Kępień of Warsaw, Poland, manages BIND 9 Quality Assurance at ISC. Before coming to ISC in June of 2017 as a BIND Developer, he worked as a network/system administrator at a small IT company and then as a DNS engineer at NASK, the registry for .pl (BIND support customers - shout out!).

To read more about Michał, please read our blog post.

CENTR & RIPE79 - Rotterdam, October 2019

Several ISC staff attended the most recent CENTR and RIPE meetings. Here are links to some talks of interest to our subscribers:

- There was a comprehensive analysis of the first-ever Root Key Rollover.
- Research on the effect of TTLs recommended (unsurprisingly) a TTL of ~ 1 day unless there is a good reason for a shorter one.
- Metrics on resolvers on the Internet, observed from RIPE probes. This is just raw data from NLNET labs, but it shows that the big public open resolver clouds are not taking over yet. Geoff Huston gave a presentation on Resolvers We Use which showed the same.
- Petr Špaček gave an excellent presentation on a new approach to benchmarking resolvers that uses a "Shotgun" tool he has published that we will be trying out at ISC.

Recent/Upcoming ISC Webinars

December 11th - Bert vs DoT
October 30th - BIND Logs of the Apocalypse
September - Unbound Commands and Extended
August - Using the Kea Configuration Backend

All our webinars are archived in ISC's YouTube channel and on our website.