BIND 9 SUBSCRIPTION EDITION

The original, classic, full-featured DNS software system.

BIND 9 Open Source

- Standards-compliant, universally interoperable
- Professionally maintained by a full-time team of skilled engineers
- Supports authoritative or recursive resolver operations
- Complete DNSSEC support for both authoritative (signing) and resolver (validating)
- Modern cryptographic standards via OpenSSL
- Load traditional static zone files, add zones dynamically, or use dynDB LDAP interface
- RNDC management protocol, suitable for automated provisioning operations, with read and read/write controls, Python library

Subscription Edition Features

- EDNS0 Client-Subnet Identifier for resolver operations*
- Serve-stale enhancement for authoritative systems extends the availability of zones under DDoS attack
- Cisco Umbrella integration *
- DNSTAP log file rolling
- Multiple DNS Cookie secrets
- EDNS0 - RFCs 7828, 7830
- Refactored Response Policy Zones (RPZ) - faster loading

* Subscriber-only

Stable preview of upcoming releases

ISC support subscribers can deploy the most high-value features sooner than they will be generally available to open source users.

As a benefit to our support subscription customers we have created a special unpublished branch of BIND. We create this branch by carefully back-porting selected new features from our development branch, integrating them with an older stable base version of BIND.

EDNS Client-Subnet Identifier (subscriber-only)

This feature, also known as 'ECS,' is a very significant change from the open source. The client-subnet identifier is additional information about the client that the resolver provides to the authority when asking a question. With this information, the authority can provide a response that is specifically tailored for clients on that subnet. The premise is that the address the client is using to contact the resolver is a good indicator of the physical location of the client.

The BIND 9 -S edition includes **resolver-side** ECS. You can implement this in your resolvers, and configure them to include the client information with queries to Content Data Networks (CDNs). CDNs rely on this information to optimize the location the client connects to, particularly for large, media-rich content. In fact, the use of the EDNS Client Subnet Identifier was first implemented by a number of CDNs (see afasterinternet.com).

ECS has not been standardized by the IETF. There is concern about the privacy implication of providing additional information about the client to unrelated authorities all over the Internet. ISC has minimized the privacy risk by limiting the specificity of the subnet to a /24 and by implementing a feature that respects the client configuration if the client does not want to use ECS.

ECS should be deployed only if the benefit outweighs the cost. Once you enable ECS in your BIND 9 resolver, the resolver will cache the different responses for each subnet, significantly inflating cache size.

The most important aspect of the ECS implementation in BIND 9 is that the resolver administrator can decide whom to send the client-subnet identifier to (specifying the IP addresses to expose this information to in a white list), and the resolver administrator can indicate how specific the subnet should be (e.g. /24).

EDNS Client Subnet Identifier, continued

For a list of CDNs that use the ECS tag to direct clients to a local data source, see the web site, afasterinternet.com. Currently listed are; Google, Amazon Web Services, Cisco Umbrella (OpenDNS), Verizon (Edgecast), Cloudflare and several others.

Serve-Stale (Resolver)

This feature was designed to enable a well-provisioned resolver to be able to continue answering for a popular domain that was temporarily unresponsive, such as during a massive DDoS attack. Resolver systems that had this feature deployed were able to continue providing access to Twitter and other popular sites during the massive attack on Dyn in October 2016. These massive attacks have not ended.

Serve stale enables the returning of "stale" cached answers when the name servers for a zone are not answering. The default is not to return stale answers. Stale answers can be enabled or disabled via named configuration, or at runtime via **rndc.** If stale answers are enabled, **max-stale-ttl** sets the maximum time for which the server will retain records past their normal expiry to return them as stale records when the servers for those records are not reachable. The default is 1 week. Information about stale answers is logged under the **serve-stale** log category.

Cisco Umbrella Integration (subscriber-only feature)

This subscriber-only feature adds appliance and device IDs to DNS queries forwarded to Umbrella for resolution. For more about Umbrella see umbrella.cisco.com.

dnstap Logging

dnstap is a fast, flexible method for capturing and logging DNS traffic. Developed by Robert Edmonds at Farsight Security, Inc., it is supported with BIND 9 as well as Knot DNS, the Knot Resolver and Unbound. **dnstap** uses libfstrm (a lightweight high-speed framing library to send event payloads which are encoded using Protocol Buffers. To enable **dnstap** at compile time, the fstrm and protobuf-c libraries must be available, and BIND must be configured with **--enable-dnstap**.

dnstap can log either queries or responses. You may configure what message types (client, auth, resolver, forwarder) to log for each view. The **dnstap** frame stream can be directed to either a local file or a UNIX socket. If you elect to log to a file, you can rotate the files based on size, indicate how many versions to keep, and add a suffix for each file (timestamp or increment). (The log file rotation feature is the difference between the -S edition and the open source).

This list of features in the Subscription Edition is current as of December 4, 2018. For a current matrix showing the significant differences between BIND 9 versions, please see https://kb.isc.org/docs/aa-01310.

SUBSCRIPTION EDITION

FREQUENTLY ASKED QUESTIONS

Is the Subscription Edition open source? How is it licensed?

The BIND 9 -S releases are distributed to subscribers in source code form. ISC does not place any restrictions on how our support subscribers use the software in their own networks. However, the -S edition is for ISC support subscriber use only. There is a clause in ISC's standard support contract that requires that you treat the -S edition as ISC Confidential Information and not post, share, or redistribute it outside your organization.

Will the features in the Subscription Edition appear in the open source?

Most of the features in the Subscription Edition are a preview of features coming to the open source. However, we do occasionally put experimental features into the -S branch. These features may or may not ever appear in the open source, and we may even withdraw them in the future from the -S edition if they do not meet expectations in production.

How long does ISC support the current -S version for?

The purpose of the -S edition is to provide early access to new features. We will periodically rebase the -edition on a newer release to provide new features or needed bug fixes. When we do that, we will support the prior -S edition for 6 months, to provide an upgrade window. We do not plan to support more than two -S versions at once, so users adopting the -S edition should be prepared to update as often as twice a year.

The current -S edition is based on 9.11, which is an Extended Support Version. This branch will be supported through the end of 2021.

What documentation is available?

The features in the Subscription Edition are documented in the regular BIND Administrative Reference Manual (ARM). Release notes are provided in the -S tarball.

How can I get the Subscription Edition?

Support Subscribers at the Silver and above levels are eligible to use the BIND 9 -S edition. When you first sign up for support and we set up your support queue, we will include information on getting the -S version if you are eligible. When ISC releases a new -S edition, you will receive email and a ticket in your ISC support queue, with download instructions for the new version.

What support is available?

Annual support contracts are available at different levels, depending on the SLA you require. We have a dedicated support engineering staff and can provide 24 x 7 support for critical issues. The BIND 9 Subscription Edition is supported under all ISC BIND 9 support contracts at Silver level and above.