EDNS Client Subnet Identifier in BIND Subscription Edition

Evan Hunt, BIND9 Engineer
Eddy Winstead, Sr. Sales Engineer

May 20, 2020

https://www.isc.org

Webinar will be recorded

Recording will be posted ~ couple days, on ISC’s Youtube channel and on https://www.isc.org/presentations/

Questions - enter in Q&A or Chat panel, we will address these at the end

Webinar agenda

- Subscription edition, why & what
- ECS explained
- Use Cases
- Configuration details
- Implementation discussion with Evan
- Q&A

BIND9 Subscription Edition, Why?

- Balance of doing good for the Internet while maintaining a sustainable organization
- Historically, Support & Professional Services
- Pattern of commercial requests for features with primarily a commercial purpose
- Opportunity to trial an experimental feature and get feedback

BIND9 Subscription Edition, What?

- Known by many names:
  - -S version (i.e. BIND-9.11.18-S)
  - Stable Preview
- Features have included:
  - RRL → open source
  - Negative Trust Anchor → open source
  - Client query limits → open source
  - Umbrella support
  - ECS

EDNS Client Subnet (ECS)

- defined in RFC 7871
- defines an EDNS0 option to convey network information
- allows authoritative servers to return differing answers to recursive servers based on perceived topology
- can be safely ignored

ECS implementation in BIND9 -S

- recursive only
- prior versions of BIND included an experimental authoritative ECS implementation. This has since been deprecated.

ECS implementation in BIND9 -S

- defaults to /24 and /56 (which are the maximum allowed)

- intended to be configured per zone

Primary concerns with ECS

- Privacy. More specific network ranges decrease client privacy (i.e., /24 vs. /22)

- Cache size. ECS answers are cached for use by future clients. The more specific you configure, the larger the cache will be.

More on Caching with ECS

- negative answers (e.g. NXDOMAIN) are cached globally

- DNS infrastructure like delegations and dnssec keys are also cached globally

BIND9 ECS use cases

- large majority of customers just want to pass ECS data to the large content providers
- interesting internal network use
  - control of both recursive & authoritative, providing differing location-based answers
  - filtering internally before external recursion

BIND9 -S ECS configuration options

ecs-bits

This option takes exactly two arguments, representing the default SOURCE PREFIX-LENGTH to use in ECS queries for IPv4 and IPv6 addresses respectively. These values can be overridden on a per-domain basis by specifying bits-v4 and bits-v6 values in ecs- zones. The default values are 24 and 56 respectively for IPv4 and IPv6 addresses, which are also the maximum allowed. Higher values are not permitted, and will be capped to 24 and 56 respectively.

BIND9 -S ECS configuration options

ecs-zones

```
ecs-zones {
   example.com bits-v4 20;
   ! excluded.example.org;
   example.org bits-v4 22 bits-v6 48;
   example.net;
};
```

It is assumed that ECS will be configured at the zone level, not using individual domain names within a zone. Consequently, ECS options are only sent when the name being queried and the apex of the zone being queried both match ecs-zones.

management of ecs-zones

- CDNs usually work by having the domain name they serve return a CNAME that points into their namespace

- if the CDN domains are in ecs-zones, you can get ECS tailored responses

BIND9 -S ECS configuration options

ecs-forward

Specifies an ACL of client addresses from which ECS-tagged queries may be forwarded. The default is **none**.

If a client is not allowed in this ACL, then recursive queries which contain the ECS option with non-zero source prefix-length will be answered with REFUSED. (This does not apply to ECS options with zero source prefix-lengths; all clients are permitted to send those.)

If the client *is* allowed, and if the query would normally be processed using ECS (i.e., because the query name is covered by **ecs-zones**), then the ECS option that was sent by the client may be forwarded.

Discussion with Evan Hunt

Evan was a primary ISC developer for our ECS implementation

Planning, implementation gotchas, testing, etc

Any surprises in user behavior…?

Q&A

Interested in ECS in BIND9?

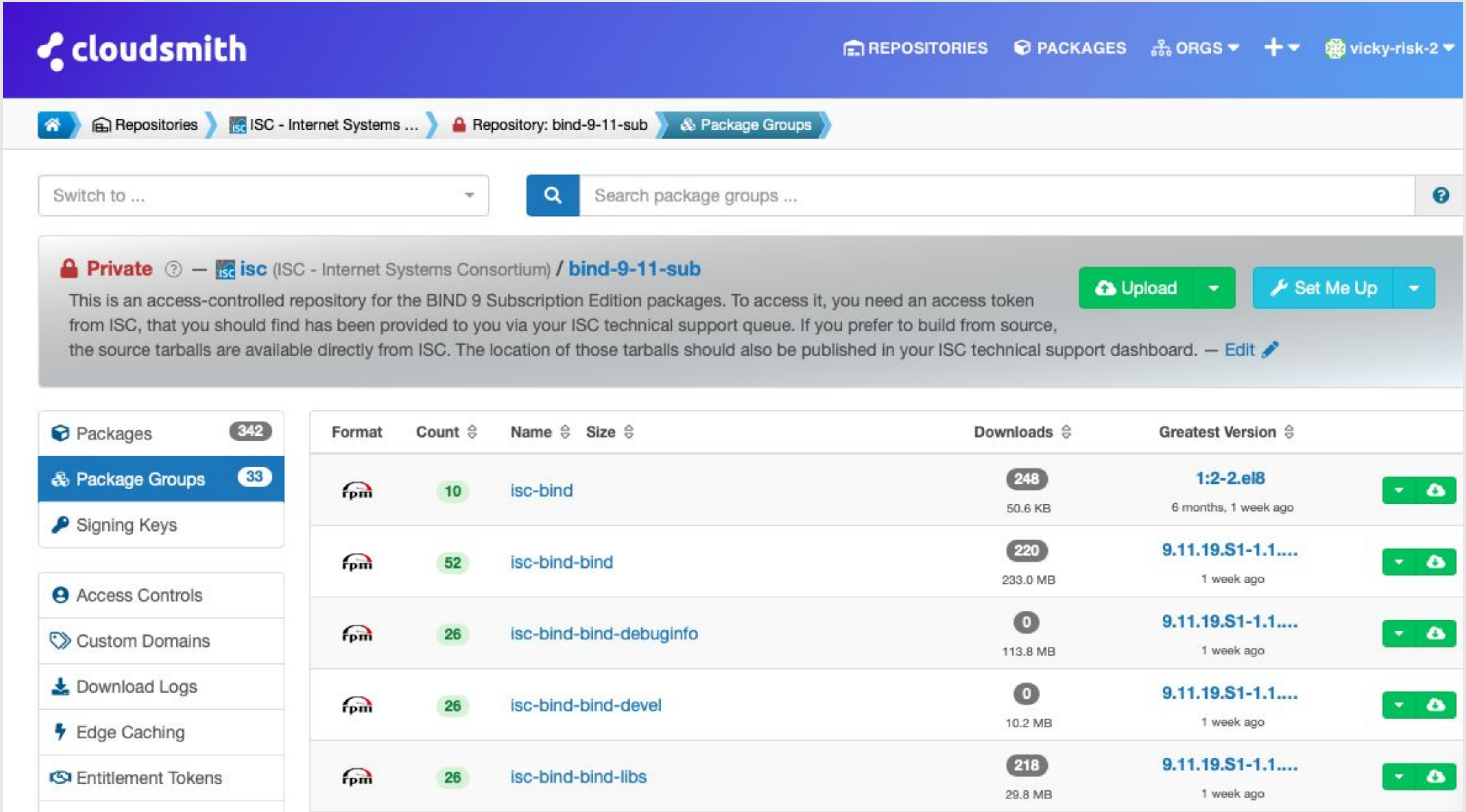
Contact:

https://www.isc.org/contact/

info@isc.org

Thank you!

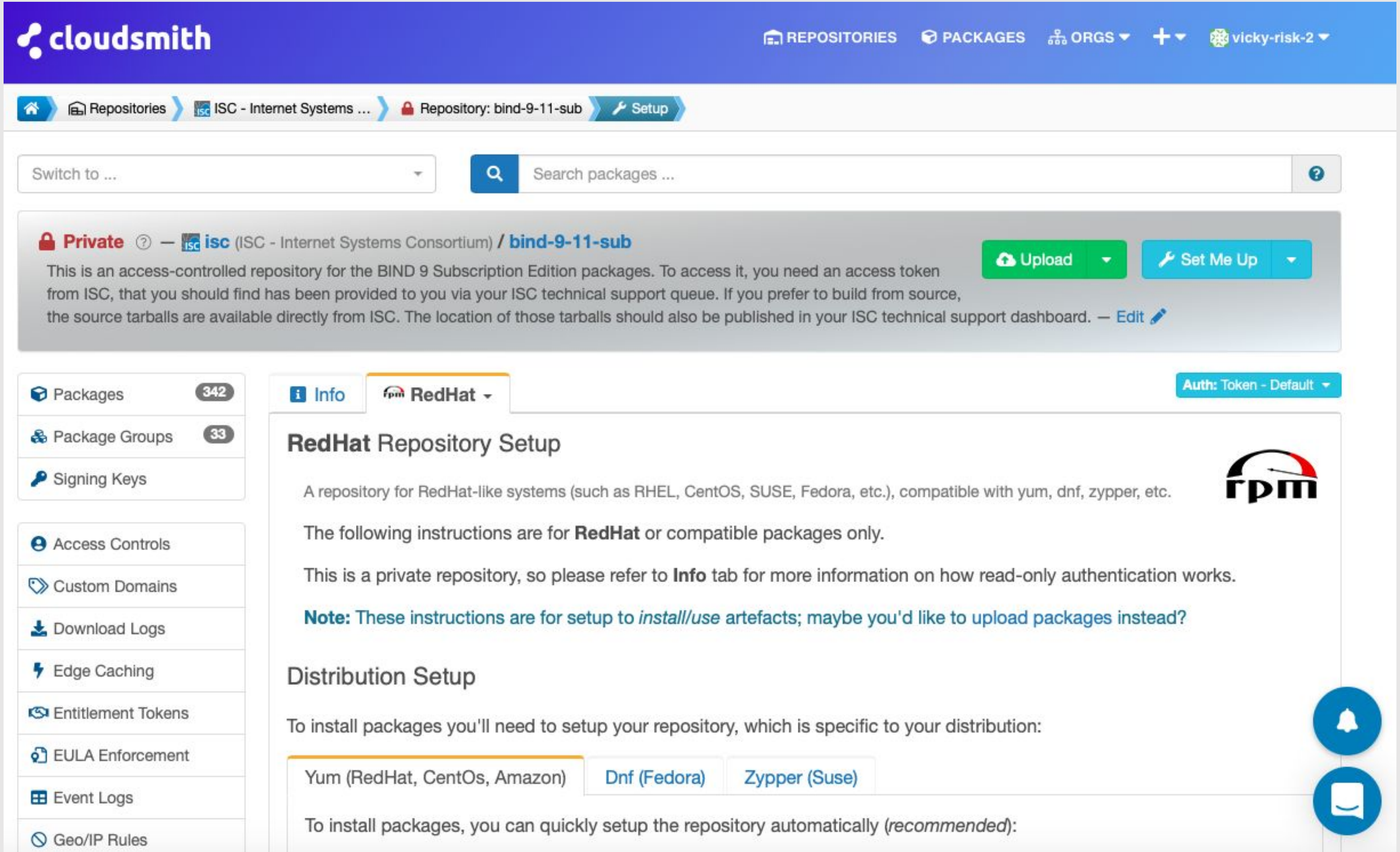
- BIND9 -S edition: https://www.isc.org/docs/BIND-9-S-Edition.pdf
- RFC 7871 https://tools.ietf.org/html/rfc7871
- Presentations: https://www.isc.org/presentations



Private — isc (ISC - Internet Systems Consortium) / bind-9-11-sub

This is an access-controlled repository for the BIND 9 Subscription Edition packages. To access it, you need an access token from ISC, that you should find has been provided to you via your ISC technical support queue. If you prefer to build from source, the source tarballs are available directly from ISC. The location of those tarballs should also be published in your ISC technical support dashboard. — Edit

Format	Count	Name	Size	Downloads	Greatest Version
rpm	10	isc-bind	50.6 KB	248	1:2-2.el8 6 months, 1 week ago
rpm	52	isc-bind-bind	233.0 MB	220	9.11.19.S1-1.1.... 1 week ago
rpm	26	isc-bind-bind-debuginfo	113.8 MB	0	9.11.19.S1-1.1.... 1 week ago
rpm	26	isc-bind-bind-devel	10.2 MB	0	9.11.19.S1-1.1.... 1 week ago
rpm	26	isc-bind-bind-libs	29.8 MB	218	9.11.19.S1-1.1.... 1 week ago



Private — isc (ISC - Internet Systems Consortium) / bind-9-11-sub

This is an access-controlled repository for the BIND 9 Subscription Edition packages. To access it, you need an access token from ISC, that you should find has been provided to you via your ISC technical support queue. If you prefer to build from source, the source tarballs are available directly from ISC. The location of those tarballs should also be published in your ISC technical support dashboard. — Edit

RedHat Repository Setup

A repository for RedHat-like systems (such as RHEL, CentOS, SUSE, Fedora, etc.), compatible with yum, dnf, zypper, etc.

The following instructions are for **RedHat** or compatible packages only.

This is a private repository, so please refer to **Info** tab for more information on how read-only authentication works.

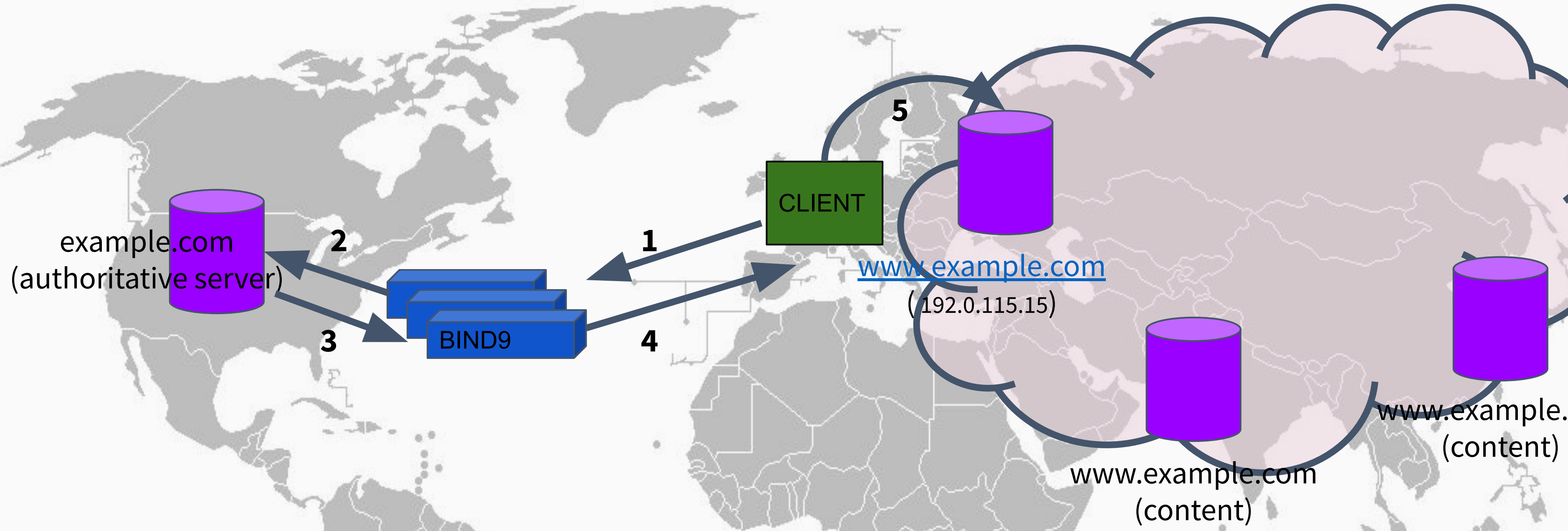
Note: These instructions are for setup to *install/use* artefacts; maybe you'd like to upload packages instead?

Distribution Setup

To install packages you'll need to setup your repository, which is specific to your distribution:

Yum (RedHat, CentOs, Amazon) | Dnf (Fedora) | Zypper (Suse)

To install packages, you can quickly setup the repository automatically (*recommended*):



1) www.example.com, A?
2) www.example.com, A? (and here subnet of requestor))
3) www.example.com, A = 192.0.115.15 (ADD TO CACHE)
4) www.example.com, A = 192.0.115.15
5) fetch content from geo-local server