Adaptive DNS Resolver Discovery

draft-pauly-add-resolver-discovery

Tommy Pauly, Tommy Jensen, Eric Kinnear, Patrick McManus, Chris Wood
ADD
IETF 108, July 2020, Virtual
Motivating use cases

Discovery mechanism

Additional information mechanism
Use Cases

1. Upgrade a resolver from Do53 to DoH/DoT

2. Discover a designated DoH/DoT resolver for a set of domains
Use Cases
Resolver Upgrade

Move from Do53 to DoT/DoH for a resolver either locally provisioned or user-selected

Secure upgrade only

RFC 7858 (DoT) already has opportunistic

Validating resolver certificate and relationship to the original Do53 resolver is a minimum
Use Cases
Resolver Upgrade
Use Cases
Designated Discovery

Trusted designation for a zone hierarchy

Split DNS view solves many problems for both improved access and privacy
  Locally-hosted content
  Private names
  Identifying authorities for public content
Use Cases
Designated Discovery - Public Origins

Resolver

ISP Do53 Server

Other Traffic

Foo Traffic

Origin Foo DoH Server

Origin Foo Web Server
Use Cases
Designated Discovery - Enterprise Private Names

Enterprise DoH Server

Enterprise Private Traffic

Public DoH Server

Other Traffic
Discovery Mechanism
Requirements

Discovery based in the DNS

Common semantics for upgrade and designation

Upgrade should use a special-use query to resolver

Domain-based designation should occur along with normal name resolution queries
Discovery Mechanism

Why SVCB?

SVCB/HTTPS

• has a clear extension mechanism
• already will be sent for ECH, ALPN, etc.
• can address multi-DNS deployment concerns

CNAME and TXT aren’t already sent for every name, and don’t have strong semantics or extensibility

Using a hint in https:// headers is detached from the DNS, may run into multi-CDN issues
Additional Information Mechanism

Requirements

Some deterministic way to query properties of a DoH or DoT server

Properties should be an extensible dictionary

Something like JSON works
Additional Information Mechanism

Why PvD?

*Here there be bikesheds!*

PvD is one existing JSON media type + registry that describes properties for using networks and DNS

- Allows a local network to directly advertise the same JSON content about split-DNS using RAs

Using a .well-known is one way to have a deterministic GET request, easy to add alongside existing DoH servers
Takeaways

✓ Resolver discovery should use DNS records
✓ SVCB/HTTPS records seem cleanest
✓ JSON-style resolver information
Next steps

Currently being used in iOS/macOS betas

Refine and consolidate approach

Good approach to adopt as a starting place?