Practical Metazones

Shawn Instenes

I speak only for me (there, that’s done)

Vixie's Metazones

Vixie, Paul. (2006) "Federated Domain Name Service Using DNS Metazones"

Basically- put the information you need to do secondary-layer management in another DNS zone, and distribute THAT

Insures only the protocols/ports you need to be a DNS server anyway are used

A modern draft RFC is in progress (draft-muks-dnsop-dns-catalog-zones-03); I'll describe a backwards-compatible extension to those ideas

Catalog zones are nice… but

This is really just a zone list. What if you have several disjoint lists?

How do you describe ACL-like properties of zones (allow-query, allow-transfer, allow-recursion, also-notify…)?

Can we describe what we need without tying it too closely to BIND (or NSD or PowerDNS or…)?

We need more than zone lists…. so

While still being compatible with the existing draft, we also:

- Define a set of Name Server Groups (NSGs) which share defaults that override the global default properties
- Support per-zone overrides of those properties
- Support zone lists defined independently of a single catalog zone or NSG so that each NSG may refer to one or more zone lists to secondary/forward
- Existing code generates metazone from a single YAML describing query and external proxy DNS layers
- Changes are validated on a special host (the zonemaster) before commit

DNS server management, summarized

1) Source of truth (handwave)
2) Distribution methods to production datacenters (serious handwave)
3) **Query/cache layer**
4) **External proxy layer**

Name Server Groups and bootstrap

How does a new nameserver know where to get data?

dig masters.<my-ip>.metazone. IN APL +short # (**RFC 3123**)

This works because:

$ORIGIN metazone.
<nameserver-ip> IN DNAME <nsg-id>.metazone.
version.<nsg-id> IN TXT “1”
masters.<nsg-id> IN APL 1:10.9.8.7/32

; quick note: metazone uses APL, CNAME, DNAME, PTR, and TXT RRs only

Properties

Global defaults, lookup <prop>.metazone.

Name server group overrides: <prop>.<my-ip>.metazone.

Zone override: <prop>.<sha1-hash>.<zonelist>.metazone.

A PTR called “supported-attr” contains the full list of supported property names.

$ORIGIN metazone.
supported-attr IN PTR masters
supported-attr IN PTR version
supported-attr IN PTR also-notify-list …

Example metazone, part 1 (defaults)

; define properties and their defaults
version IN TXT “1”
supported-attr IN PTR masters
masters IN APL 1:10.2.3.4/32
supported-attr IN PTR zone-list
zone-list IN TXT “zones”
supported-attr IN PTR allow-query
allow-query IN APL 1:10.0.0.0/8 1:192.168.0.0/24

Example metazone, part 2 (zone lists)

zonecount.zones IN TXT “2”
digits.zones IN TXT “5”
<sha1-hash1>.zones IN PTR dev.example.com.
forward-list.<sha1-hash1>.zones IN APL 1:192.168.100.100/32 ; override!
00001.zonelist.zones IN CNAME <sha1-hash1>.zones
<sha1-hash2>.zones IN PTR prod.example.com.
00002.zonelist.zones IN CNAME <sha1-hash2>.zones
zonecount.edge_zones IN TXT “1”
digits.edge_zones IN TXT “5”
<sha1-hash3>.edge_zones IN PTR rpz.example.com.
00001.zonelist.edge_zones IN CNAME <sha1-hash3>.edge_zones

Example metazone, part 3 (name server groups)

; NSG “west”
version.west IN TXT “1”
masters.west IN APL 1:10.9.219.253/32
allow-query.west IN APL 1:10.1.0.0/16
default-forward-list.west IN APL 1:10.3.4.5/32 1:10.3.5.6/32 1:10.4.5.7/32
; NSG “east”
masters.east IN APL 1:10.11.12.13/32
allow-query.east IN APL 1:10.2.0.0/16
default-forward-list IN APL 1:10.5.6.7/32 1:10.6.7.8/32 1:10.7.8.9/32

What this looks like (BIND example)

```
; for readability, some ACLs are generated with known names
zone “prod.example.com.” {
    masters { “local-upstream”; };
    file “db.prod.example.com.”;
    allow-query { “query-3c44ab83”; };
    allow-transfer { “all-dns-servers”; };
    also-notify { “local-downstream”; };
};
zone “dev.example.com.” {
    forward { 192.168.100.100; };
};
```

Future directions

I want to help update the draft (we've been talking but I've been busy)

View support?

Updates based on operational experience!

I have code- can't share yet (working on it)