Quick intro to catalog zones

Wilhelm Wijkander
2023-06-22

Catalog zones

- DNS zone that describes other DNS zones
- Not a new concept
  - Current draft dates back to 2005 work by Paul Vixie("metazones") and a 2015 draft by ISC
  - PowerDNS has "autoprimary"
- (Currently) known as draft-ietf-dnsop-dns-catalog-zones-09
  - two versions, with v2 gaining traction
- Allows disseminating zone metadata "in-band" by AXFR
  - From "consumers" to "producers"
  - As opposed to setting up "out-of-band" configuration management
  - Interoperable, it's all DNS zones

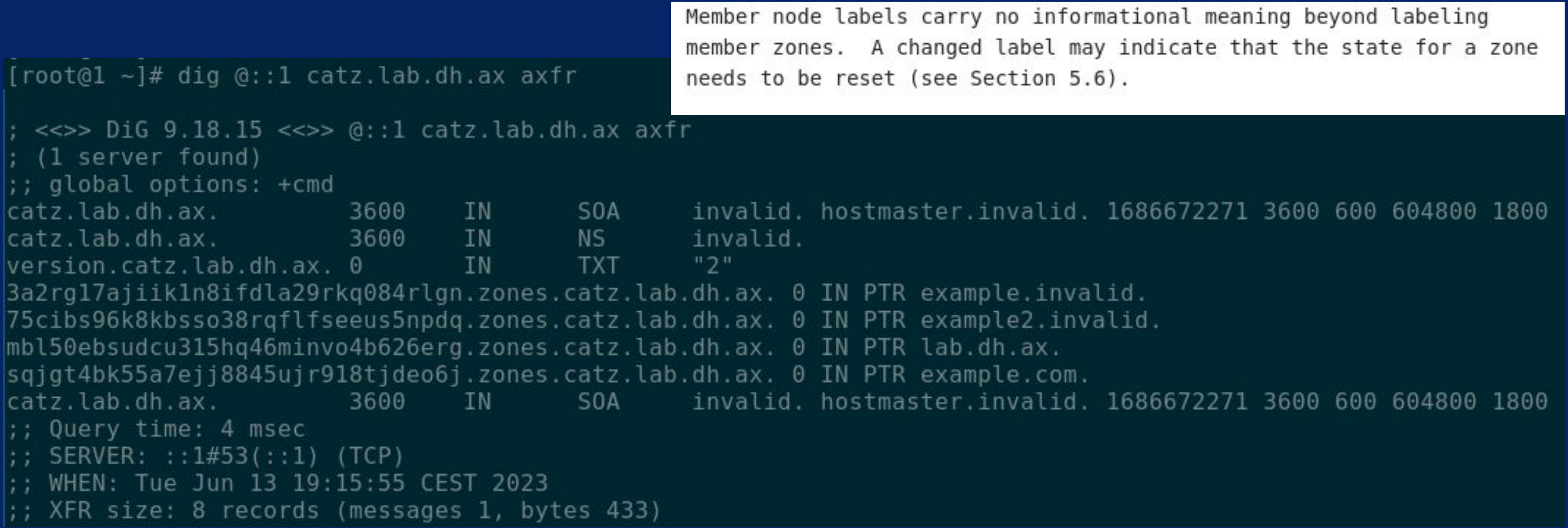
Usecase: decentralized DNS hosting

- Lowers the bar for sharing and exchanging DNS secondaries between people significantly
  - … and by extension making it easier to self-host DNS in a robust way as an alternative to centralized big DNS providers
  - Standardized interface - one TSIG key and catalog zone enables an unlimited number of secondary zones
  - All you need is one authoritative DNS server that understands catalog zones and some friends :)

Usecase: regular old primary-secondary setup

- But with less automation needed for secondaries
  - All changes happen on the primary, except for TSIG key rotation

Example catalog zone



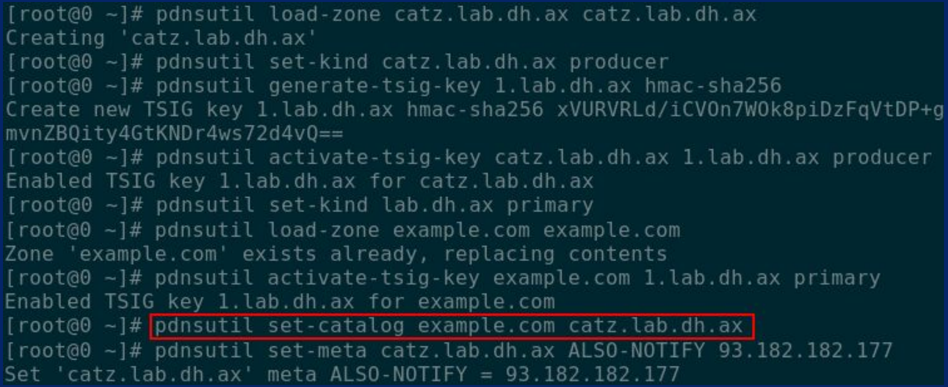
Member node labels carry no informational meaning beyond labeling
member zones. A changed label may indicate that the state for a zone
needs to be reset (see Section 5.6).

```
[root@1 ~]# dig @::1 catz.lab.dh.ax axfr

; <<>> DiG 9.18.15 <<>> @::1 catz.lab.dh.ax axfr
; (1 server found)
;; global options: +cmd
catz.lab.dh.ax.         3600    IN      SOA     invalid. hostmaster.invalid. 1686672271 3600 600 604800 1800
catz.lab.dh.ax.         3600    IN      NS      invalid.
version.catz.lab.dh.ax. 0       IN      TXT     "2"
3a2rg17ajiikln8ifdla29rkq084rlgn.zones.catz.lab.dh.ax. 0 IN PTR example.invalid.
75cibs96k8kbsso38rqflfseeus5npdq.zones.catz.lab.dh.ax. 0 IN PTR example2.invalid.
mbl50ebsudcu315hq46minvo4b626erg.zones.catz.lab.dh.ax. 0 IN PTR lab.dh.ax.
sqjgt4bk55a7ejj8845ujr918tjdeo6j.zones.catz.lab.dh.ax. 0 IN PTR example.com.
catz.lab.dh.ax.         3600    IN      SOA     invalid. hostmaster.invalid. 1686672271 3600 600 604800 1800
;; Query time: 4 msec
;; SERVER: ::1#53(::1) (TCP)
;; WHEN: Tue Jun 13 19:15:55 CEST 2023
;; XFR size: 8 records (messages 1, bytes 433)
```

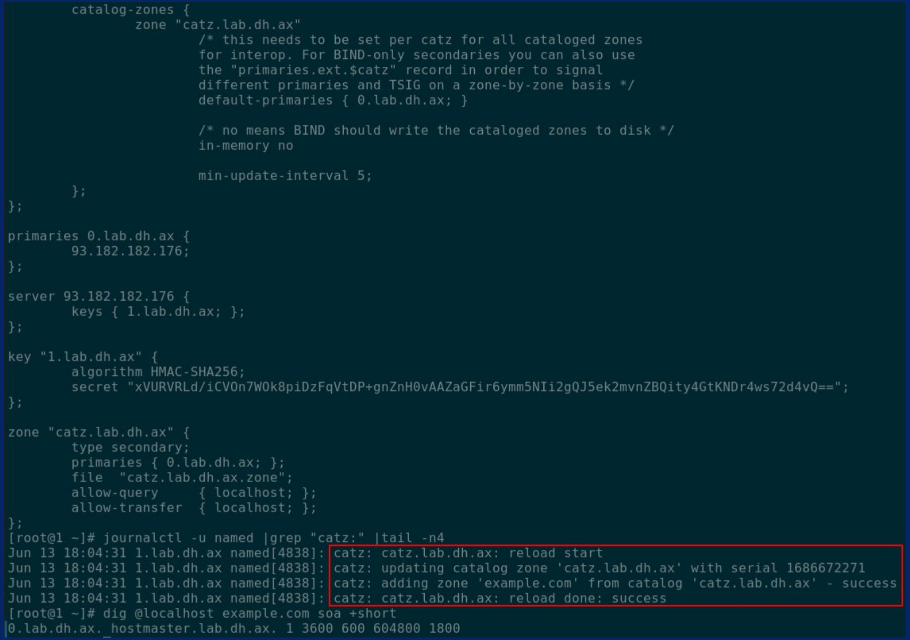
Example setup

PowerDNS primary



```
[root@0 ~]# pdnsutil load-zone catz.lab.dh.ax catz.lab.dh.ax
Creating 'catz.lab.dh.ax'
[root@0 ~]# pdnsutil set-kind catz.lab.dh.ax producer
[root@0 ~]# pdnsutil generate-tsig-key 1.lab.dh.ax hmac-sha256
Create new TSIG key 1.lab.dh.ax hmac-sha256 xVURVRLd/iCVOn7WOk8piDzFqVtDP+g
mvnZBQity4GtKNDr4ws72d4vQ==
[root@0 ~]# pdnsutil activate-tsig-key catz.lab.dh.ax 1.lab.dh.ax producer
Enabled TSIG key 1.lab.dh.ax for catz.lab.dh.ax
[root@0 ~]# pdnsutil set-kind lab.dh.ax primary
[root@0 ~]# pdnsutil load-zone example.com example.com
Zone 'example.com' exists already, replacing contents
[root@0 ~]# pdnsutil activate-tsig-key example.com 1.lab.dh.ax primary
Enabled TSIG key 1.lab.dh.ax for example.com
[root@0 ~]# pdnsutil set-catalog example.com catz.lab.dh.ax
[root@0 ~]# pdnsutil set-meta catz.lab.dh.ax ALSO-NOTIFY 93.182.182.177
Set 'catz.lab.dh.ax' meta ALSO-NOTIFY = 93.182.182.177
```

BIND9 secondary



```
        catalog-zones {
                zone "catz.lab.dh.ax"
                        /* this needs to be set per catz for all cataloged zones
                        for interop. For BIND-only secondaries you can also use
                        the "primaries.ext.$catz" record in order to signal
                        different primaries and TSIG on a zone-by-zone basis */
                        default-primaries { 0.lab.dh.ax; }

                        /* no means BIND should write the cataloged zones to disk */
                        in-memory no

                        min-update-interval 5;
        };
};

primaries 0.lab.dh.ax {
        93.182.182.176;
};

server 93.182.182.176 {
        keys { 1.lab.dh.ax; };
};

key "1.lab.dh.ax" {
        algorithm HMAC-SHA256;
        secret "xVURVRLd/iCVOn7WOk8piDzFqVtDP+gnZnH0vAAZaGFir6ymm5NIi2gQJ5ek2mvnZBQity4GtKNDr4ws72d4vQ==";
};

zone "catz.lab.dh.ax" {
        type secondary;
        primaries { 0.lab.dh.ax; };
        file  "catz.lab.dh.ax.zone";
        allow-query     { localhost; };
        allow-transfer  { localhost; };
};
[root@1 ~]# journalctl -u named |grep "catz:" |tail -n4
Jun 13 18:04:31 1.lab.dh.ax named[4838]: catz: catz.lab.dh.ax: reload start
Jun 13 18:04:31 1.lab.dh.ax named[4838]: catz: updating catalog zone 'catz.lab.dh.ax' with serial 1686672271
Jun 13 18:04:31 1.lab.dh.ax named[4838]: catz: adding zone 'example.com' from catalog 'catz.lab.dh.ax' - success
Jun 13 18:04:31 1.lab.dh.ax named[4838]: catz: catz.lab.dh.ax: reload done: success
[root@1 ~]# dig @localhost example.com soa +short
0.lab.dh.ax. hostmaster.lab.dh.ax. 1 3600 600 604800 1800
```

Security considerations

- No filtering on zones supplied from the primary currently supported
    - A zone can only be added from one catalog zone at a time, first come
    - TODO: might be achievable in PowerDNS with Lua axfrfilter?

Usual DNS hygiene:

- Use TSIG in order to authorize the transfer, and authenticate the contents of your zone.
    - ...consider limiting blast radius by using one TSIG secret per secondary
- Your zone in its entirety will be visible to your secondaries
- Consider signing your zones with DNSSEC so they can’t be tampered with
- Future: XFR-over-TLS (RFC9103)?

Implementation status

Current draft v2 supported in:

Primary:

- Almost any auth DNS server or service
  - (you might have to generate the catalog zone yourself)

Secondary:

- BIND9
  - (but make sure you set up a v2 zone)
- PowerDNS
- Knot

Thanks!

Questions? Want to exchange catalog zones?

- wilhelm@0x5e.se
- Libre___/libre on the usual IRC networks