DNS updates

what a lot of people don’t know about DNS

by Jens Kühnel

DNS RR

- Which DNS resource records do you know?
- According to Wikipedia:
  - 47 used
  - 43 obsolete or unused

Topics

- We will look into the following:
  - RFC9460: https RR in DNS
  - RFC9432: DNS catalog zone
  - RFC6762 App G: Internal TLDs
  - RFC2136: DNS update
  - RFC9364: DNSSEC (not discussed here)
- Using bind9 and powerdns

HTTPS RR in DNS

- RFC9460: released in Nov 2023
  - Powerdns > 4.4.0 (2020)
  - Bind9 > 9.16.21 (2021)
- Variant of SVCB Resource Record for https
- Allows additional info about a https server
  - Name TTL IN HTTPS SVCPriority TARGETNAME Params
  - Prio (0=Alias, else like MX)

Alias mode vs Service mode

- Alias mode (Prio = 0)
  - Allows to forward service to a other domain (at zone level no CNAME are allowed)
  - No parameters are possible
    - example.com. 3600 IN HTTPS 0 svc.example.net.
- Service mode (Prio != 0)
  - target name specifies an alternative name
  - special target name „.“
    - example.com 300 IN HTTPS 1 . PARAMS

Https parameters

- Alpn
  - Application Protocol Negotiation
  - H1,h2,h3 (http3 with quic/udp)
- Port
  - Use different port instead of 443
- Ipv4hint ipv6hint
  - Specify the ipv4 or ipv6 to avoid extra A/AAAA request
- ECH
  - Public key and metadata for encrypted Client hello

Limited possiblities

	Chrome	Firefox	Safari	Notes
AliasMode	❌	❌	✅	Firefox Bug Chromium issue
ALPN	✅	✅	✅	previously discussed
ECH	✅	✅	❌	
IP Hints (no A / AAAA)	❌	❌	✅	Firefox bug Chromium issue
IP Hints (with A / AAAA)	❌	✅	✅	Firefox / Safari race results
no-default-alpn	❌	❌	❌	Firefox Bug Chromium issue
Port	❌	✅	✅	Chromium issue

- Source: https://www.netmeister.org/blog/https-caniuse.html

Zonetransfer

- Is zone transfer known?
- Primary and secondaries?
- TSIG?

DNS catalog zone

- RFC9432 from 2023
- configures secondaries to accept Zones from primaries, without changing the secondaries.
- works with powerdns and bind
  - but only bind extends to support TSIG zone transfer

Parameter

$TTL 1

catalog.example.org. IN SOA . . 8 86400 3600 86400 3600

catalog.example.org. IN NS invalid.

version IN TXT "2"

8ad180f028330a84d6189427ae602490c7111137.zones IN PTR example.com.

label.primaries.ext.8ad180f028330a84d6189427ae602490c7111137.zones IN TXT "NAME-OF-SIG."

Private DNS Namespace

- Problems since beginning of DNS
  - .local (MDNS only)
  - Using „unused“ TLD is dangerous
  - RFC6762 Appendix G suggested:
    - .intranet
    - .internal
    - .private
    - .corp
    - .home
    - .lan
  - ICANN Board officially reserved **.internal** in 2024

nsupdate

- RFC2136 (1997) & RFC3007 (2000)
- Allows for dynamic DNS updates
- Uses dns and does not need http like 90% of all dynamic updates tools.
- Uses TSIG (like zone transfer) to authenticate, but is not encrypted.

TSIG on server

- Generate TSIG key with tsig-keygen
- Simple bind setup:
  - Add keyfile in bind config
  - Add Allow-update with keyname in zone
- Simple powerdns setup:
  - pdnsutil tsigkey generate test hmac-sha512
  - pdnsutil metadata add example.org TSIG-ALLOW-DNSUPDATE test
    - Source: https://doc.powerdns.com/authoritative/dnsupdate.html#tsig-allow-dnsupdate

Client

- Rfc2136 in a lot of tools available
- Needs the TSIG key
- Simple bash script:

```
nsupdate -k tsig-keys.txt -v << EOF
Server PRIMARY.example.org.
zone exmple.org
update delete example.org. A
update add    example.org. 600 A 127.0.0.1
show
send
EOF
```