Hosting your own DNS for *fun* and zero profit

@kevin@km6g.us (Fediverse)
@kevin:km6g.us (Matrix)

Kevin P. Fleming – FOSDEM 2023

What? Really?

- Yes, really.
- It’s easy (mostly).
- It can be done using 100% free and open source software.
- It’s fun (if you are a DNS geek – look around this room).
- It’s not zero cost, but isn’t expensive.

OK. Why, though?

- See previous slide referring to *fun*.
- Standards compliance – IPv6, DNSSEC, DNS **UPDATE**, new record types, etc.
- *Free* DNS hosting services usually include technical support of equal value.
- No limitations on number of zones, number of records, or anything else.
- Freedom from *big tech* decisions that the service you are using no longer fits in their business plans.

I’m convinced. What will I need?

- Some place (preferably not on a public network, but accessible over IPv6 or VPN) to host a **hidden primary** authoritative server.
- Two (or three, or more) public locations to host **public secondary** authoritative servers. Depending on the software you choose, these could be lightweight containers or tiny virtual machines.
- Well-supported and actively-developed DNS authoritative server software (hat tip to the PowerDNS team).
- A domain registrar which allows you to specify your own auth servers, which supports IPv4 and IPv6 glue records, and which supports **DS** records.

Is that really enough? I thought it was more...

- Assuming that you are not hosting thousands of domains for paying customers, that’s really enough.
- Internet users (end users) tend to use extremely large *public resolver* services (ISP-provided, or *big tech*-provided), which act as a caching layer for your zones.
- In the golden old days of the Internet, your auth servers would have been expected to handle queries from thousands (or millions) of sources… that is far less likely today.
- Inexpensive containers/VMs, in 2023, can handle DNS queries **quickly**.

Why did you do this?

In 2018, I wanted to find a DNS host which offered full IPv6 support, DNSSEC, and dynamic updates using a reliable (not web-scraping) protocol.

I found a small number of them, but their per-zone costs were outrageous. They were *enterprise service providers*, their offerings didn’t make sense for low-volume users like me.

What do you use today? (part 1)

- A *system container* on my home NAS, as the **hidden primary**.
- Two AWS EC2 t4g.nano virtual machines (one in Oregon, USA, the other in Dublin, Ireland) as **public secondaries**.
- A *system container* on an OVH dedicated server in Quebec, Canada as a **public secondary**.
- Two PCEngines APUs as network appliances in the home network, as **private secondaries** (hosting both public and private zones).

What do you use today? (part 2)

- PowerDNS Authoritative Server 4.7.3 on all machines.
- SQLite 3 databases populated using **NOTIFY+AXFR** replication.
- Ansible modules to manage zones and TSIG keys (which I wrote and published – details later).

What does that cost?

- Hidden primary on NAS – free.
- Public secondaries on AWS EC2 – €78.29 up-front (3 years), €1.53 for storage per month, net €3.70 per month.
- Public secondary on OVH server – free (as long as I still need it for things like Matrix, Mastodon, etc.)
- PowerDNS Authoritative Server 4.7.3 – free.
- SQLite 3 – free.
- Ansible modules to manage zones and TSIG keys – free.

What do you do with that?

- All of my network infrastructure, both public and private, uses auto-renewed Let’s Encrypt certificates (verified using DNS-01 challenges).
- **SSHFP** records (in DNSSEC-signed zones) for all of the SSH-accessible infrastructure, eliminating the need for ‘host key’ verification and caching.
- SVCB-based **HTTPS** records for all services used by browsers.
- Ansible-based management of all zones and most records.
- Online signing of DNSSEC zones, and automatic distribution of added/removed zones using **catalog zones**.

How much maintenance work is needed?

- When there are new PowerDNS releases, I build packages for the architectures I use and deploy them.
- When new zones are needed, or zones should be removed, the Ansible playbook makes the changes on the **hidden primary**; those changes replicate to the other authoritative servers automatically (the magic of **catalog zones**).

How can I get started?

- Verify that your domain registrar meets the requirements listed earlier; if not, move your domains to a better registrar.
- Decide which DNS authoritative server software you want to use.
- Decide where and how you want to deploy the two (or three) levels of authoritative servers, and how you will manage the software installation and upgrades on those systems.
- Decide how you will manage the zone list on the servers.
- If your answers above are “PowerDNS”, “Ansible”, and “catalog zones”, then you can use my Ansible modules to get started.

Bonus Content: What about recursive resolvers?

- Unsurprisingly, I use the PowerDNS Recursor in my infrastructure.
- Ansible manages this too, including private zones.
- There are recursors on the network appliances (for use inside the home network) and on the OVH server (for use by the services located there).
- The **hidden primary** sends NOTIFY messages to the recursors when zone contents change; the recursors flush any cached content for those zones, so users of the recursors don’t have to wait for TTL expiration.
- The LAN recursors are reached using anycast addresses advertised using OSPF… but that’s another talk.

Resources - Links

- PowerDNS Authoritative Server
- PowerDNS Recursor
- SQLite 3
- Ansible PowerDNS Authoritative Modules
- RFC 4255 - DNS SSHFP Records
- draft-ietf-dnsop-svcb-https-11 - DNS HTTPS Records

Questions Welcome!