

Fantastic DNS records and where to find them

Demystifying systemd-resolved and how it is integrated on Ubuntu

Dimitri John Ledkov <xnox@ubuntu.com>

What is systemd-resolved?

- Local, caching, DNS resolver
- Per-link nameserver configuration storage
- NSS-module, dbus API, command-line tool
- Networked daemon
- Resolvconf implementation

How to start using systemd-resolved?

Symlink /etc/resolv.conf to...

- /run/systemd/resolve/stub-resolv.conf
(stub with domains)
- /usr/lib/systemd/resolv.conf
(stub resolver, static)
- /run/systemd/resolve/resolv.conf
(underlying DNS servers)

How do these resolv.conf files look like?

/usr/lib/systemd/resolv.conf

```
nameserver 127.0.0.53
```

```
options edns0
```

How do these resolv.conf files look like?

`/run/systemd/resolve/stub-resolv.conf`

```
nameserver 127.0.0.53
```

```
options edns0
```

```
search buildd enablement external internal power ppa
```

How do these resolv.conf files look like?

`/run/systemd/resolve/resolv.conf`

```
nameserver 10.172.192.1
```

```
nameserver 192.168.1.1
```

```
search buildd enablement external internal power ppa
```

How to start using systemd-resolved? (cont)

... or don't mangle /etc/resolv.conf

- Enable NSS module
- Use command line tool
- Use dbus API
- Use the dynamic resolv.conf generated files
- Use dig

How to update resolved nameservers?

- Netplan.io / NetworkManager / Networkd
- DBus API
- resolvectl (systemd-resolved) command line tools
- /sbin/resolvconf -> /usr/bin/resolvectl interface
- Reads /etc/resolv.conf if managed by others
- Configuration file fallbacks
- Compile time fallbacks

Fun Stuff

Optional features one can enforce for the whole system

```
#LLMNR=no
```

```
#MulticastDNS=no
```

```
#DNSSEC=no
```

```
#DNSOverTLS=no
```

```
#Cache=yes
```

```
#DNSStubListener=yes
```

```
#ReadEtcHosts=yes
```

resolvctl command line

Global

LLMNR setting: no

MulticastDNS setting: no

DNSOverTLS setting: no

DNSSEC setting: no

DNSSEC supported: no

resolvctl command line

Link 2 (wlp2s0)

Current Scopes: DNS

DefaultRoute setting: yes

LLMNR setting: yes

MulticastDNS setting: no

DNSSEC setting: no

DNSOverTLS setting: no

DNSSEC supported: no

Current DNS Server: 10.0.0.1

DNS Servers: 10.0.0.1

DNS Domain: ~.

rieo.lan

resolvctl command line

<code>query HOSTNAME ADDRESS...</code>	Resolve domain names, IPv4 and IPv6 addresses
<code>service [[NAME] TYPE] DOMAIN</code>	Resolve service (SRV)
<code>openpgp EMAIL@DOMAIN...</code>	Query OpenPGP public key
<code>tlsa DOMAIN[:PORT]...</code>	Query TLS public key
<code>status [LINK...]</code>	Show link and server status
<code>statistics</code>	Show resolver statistics
<code>reset-statistics</code>	Reset resolver statistics
<code>flush-caches</code>	Flush all local DNS caches
<code>reset-server-features</code>	Forget learnt DNS server feature levels

resolvctl command line

<code>dns [LINK [SERVER...]]</code>	Get/set per-interface DNS server address
<code>domain [LINK [DOMAIN...]]</code>	Get/set per-interface search domain
<code>default-route [LINK [BOOL]]</code>	Get/set per-interface default route flag
<code>llmnr [LINK [MODE]]</code>	Get/set per-interface LLMNR mode
<code>mdns [LINK [MODE]]</code>	Get/set per-interface MulticastDNS mode
<code>dnsovertls [LINK [MODE]]</code>	Get/set per-interface DNS-over-TLS mode
<code>dnssec [LINK [MODE]]</code>	Get/set per-interface DNSSEC mode
<code>nta [LINK [DOMAIN...]]</code>	Get/set per-interface DNSSEC NTA
<code>revert LINK</code>	Revert per-interface configuration

Bugs

- Edns0 is sad
- Captive portals are sad
- Abuse of Option 15 for multiple domains
- MDNS taking too long
- Domain-less searches are not forwarded

Ubuntu Defaults

- UseDomains=true (dhcp acquired domains trusted)
- LMMNR, MDNS, DNSSEC, DnsOverTLS - **false**
- Listen on UDP and TCP port 53 on lo 127.0.0.53
- FallbackDNS none
- Resolv.conf stub-resolve.conf by default
- No NSS module by default
- Networkd, NetworkManager, ifupdown integration
- Resolvconf replacement (soon)