

DoT

Nach dieser Anleitung: <https://askubuntu.com/questions/1092498/dns-over-tls-with-systemd-resolved>

Use DNS Over TLS (DoT) on generic Linux systems

So for generic Linux distro with relative close-to-upstream kernel, systemd, glibc, toolchain, GNU utils, etc

1. edit `/etc/systemd/resolved.conf`

```
[Resolve]
DNS=1.1.1.1 1.0.0.1 8.8.8.8
#FallbackDNS=1.1.1.1 9.9.9.10 8.8.8.8 2606:4700:4700::1111 2620:fe::10 2001:4860:4860::8888
#Domains=
#LLMNR=yes
#MulticastDNS=yes
#DNSSEC=allow-downgrade
#DNSOverTLS=opportunistic
DNSSEC=yes
DNSOverTLS=yes
#Cache=yes
#DNSStubListener=yes
#ReadEtcHosts=yes
```

- Ubuntu 20.04 specific `resolved.conf`

```
[Resolve]
DNS=1.1.1.1 1.0.0.1 8.8.8.8
FallbackDNS=1.1.1.1 8.8.8.10 8.8.8.8
#Domains=
#LLMNR=no
```

```
#MulticastDNS=no
DNSSEC=yes
DNSOverTLS=yes
#Cache=yes
#DNSStubListener=yes
#ReadEtcHosts=yes
```

2. Assume `systemd-resolved` is enabled, restart the service

```
systemctl restart systemd-resolved.service
```

3. Use local stub resolver

`systemd-resolved` provides a local DNS stub listener on IP address 127.0.0.53 on the local loopback interface, so to use the DNS over TLS capable stub resolver, we'll need to somehow manage `/etc/resolv.conf` and make sure `127.0.0.53` is used as nameserver.

NOTE: systemd maintains `/run/systemd/resolve/stub-resolv.conf` for compatibility with traditional Linux programs. We can simply symlink to this file ;-)

```
ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
```

NOTE: For Arch Linux, I have to replace `openresolvconf` with `systemd-resolvconf`.

Done.

Revision #1

Created 24 January 2024 09:24:02 by Till

Updated 24 January 2024 09:24:45 by Till