

Split DNS/DNSSEC setup using unbound and dnssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Linux Plumbers 2014, Dusseldorf

<http://data.pavlix.net/mikroexpo/2014/>

Classic setup using `/etc/resolv.conf`

Classic setup

- Static or from DHCP/VPN
- A single set of nameservers
- List of search domains
- DNS done via a single network
- Leaking DNS queries to VPN

Classic resolv.conf setup

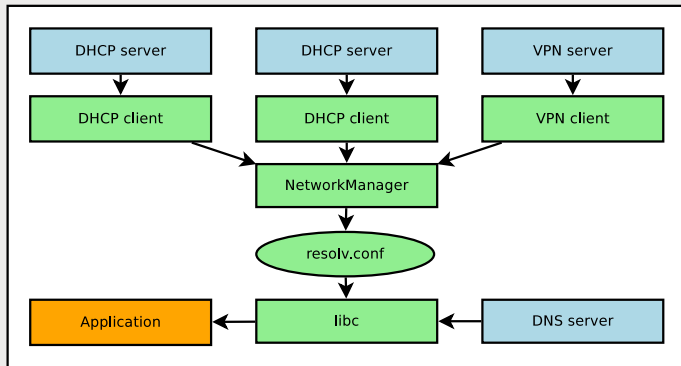
Split DNS/DNSSEC
setup using unbound
and dnssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



Manual resolv.conf setup

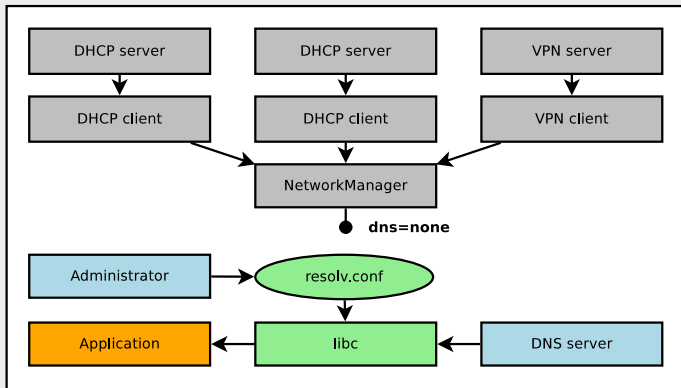
Split DNS/DNSSEC
setup using unbound
and dnssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



Split DNS client setup

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion

- Split view from different sites
- Accessing internal view via VPN
- Global name servers and DNSSEC
- Nameservers per domain subtree
- Per domain DNSSEC configuration

- Some support in dnsmasq
- Forward zones in unbound
- Manual configuration
- Information from NetworkManager
- DNS probing by dnssec-trigger
- And hotspot signon probing

Manual unbound setup

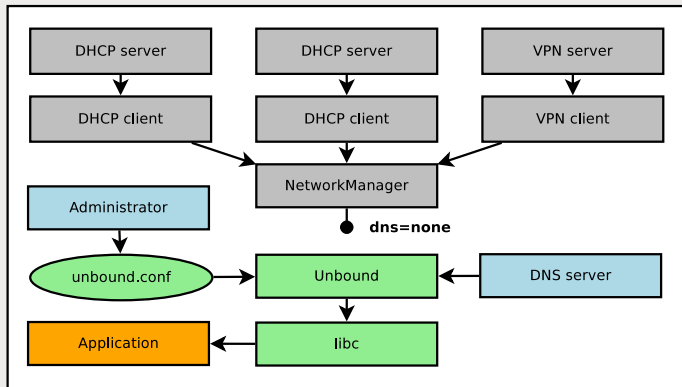
Split DNS/DNSSEC
setup using unbound
and dnssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



NetworkManager talks to unbound

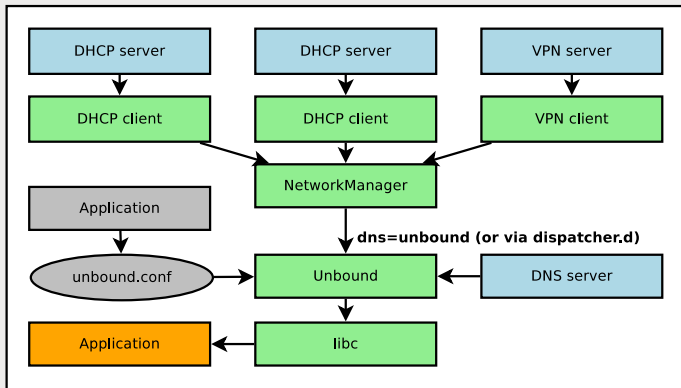
Split DNS/DNSSEC
setup using unbound
and dnssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



NetworkManager talks to dnsssec-trigger

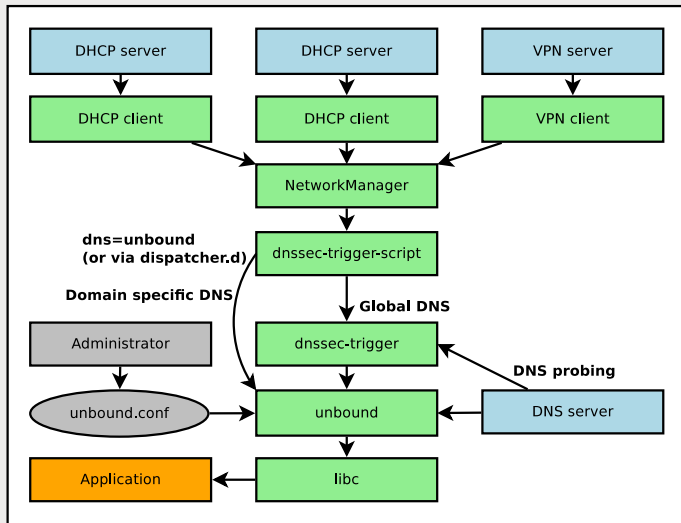
Split DNS/DNSSEC
setup using unbound
and dnsssec-trigger

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



systemd-resolved considerations

- We still need unbound
- And dnssec-trigger
- Another cache to be flushed
- Will provide LLMNR
- And hopefully more

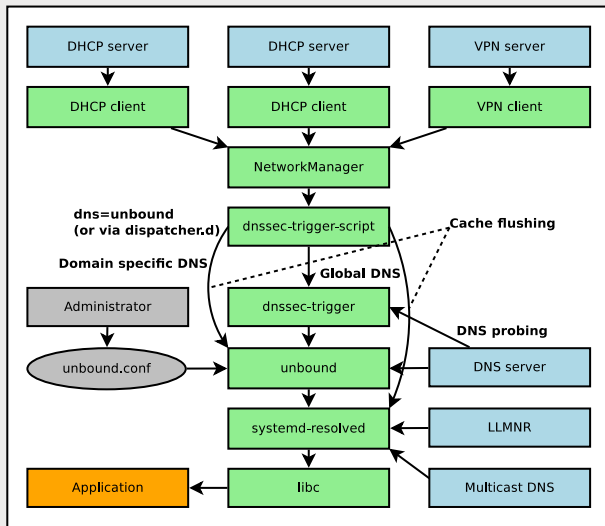
systemd-resolved comes into play

Pavel Šimerda
pavlix@pavlix.net

Classic setup

Split DNS

Discussion



Main issues

- DNS detection issues
 - Wildcard specific issues
 - EDNS replied with NXDOMAIN
- Cache flushing
 - Application caching
 - nscd
- Ensuring trusted validator
 - resolv.conf and glibc
- Split DNS/DNSSEC view
- Access to internal zones
 - Lack of zone lists

Discussion...

<http://data.pavlix.net/mikroexpo/2014/>

pavlix@pavlix.net
psimerda@redhat.com

<http://fedoraproject.org/wiki/User:Pavlix>

<http://fedoraproject.org/wiki/Networking>