Dnsmasq .lan domain while still using knot resolver

dpdrown 25d

Nov 2

I like dnsmasq's automatic *.lan automatic hostnames and I wanted to continue using them, but I didn't want to get rid of the knot resolver. dnsmasq automatically generates the hostnames based off the dhcp request hostname as well as any static hosts you've defined.

1 / 25

Nov 2

I set dnsmasq's DNS port to 54 in LuCI's *Network* > *DHCP and DNS* > *Advanced Settings* > *DNS Server Port*

I then changed kresd.conf generation in /etc/init.d/kresd, line 38:

```
init_header() {
   # ....
   echo "}" >> $CONFIGFILE
   # unchanged above this line, I added the line below
   echo "policy.add(policy.suffix(policy.FORWARD('127.0.0.1@54'),  policy.todnames({'lan'})))" >>$CONFIGFILE
}
```

Back

This forwards *.lan to port 54, which is handled by dnsmasq

End result:

9h ago

```
$ host turris.lan
turris.lan has address 192.168.1.1
$ host beaglebone.lan
beaglebone.lan has address 192.168.1.16
```

- How to configure local address DNS resoultion on Omnia
- Assign .LOCAL domain
- How do I get all my dhcp hostnames on a my house domain?
- Knot-resolver configuration improvement in omnia

danrl 25d

Thanks!
I am wondering why this isn't the default shipping config. (Although I prefer port 5353 over 54)

horada 22d

Is there a way to resolve also reverse DNS records?

I tried to add similar line with "domain" `168.192.in-addr.arpa` (both with and without closing . (dot), but it didn't work.

Dnsmasq on port 53535 properly resolve it:

```
$ dig +short -x 192.168.201.5 @192.168.201.1 -p 53535
pc.mydomain.cz.
```

But Knot not:

```
$ dig +short -x 192.168.201.5 @192.168.201.1
```

```
$
```

dpdrown 22d

Yes, this is possible but slightly harder.

The file /usr/lib/kdns_modules/policy.lua includes a list of reverse DNS to deny. You can comment out or delete the line for 168.192.in-addr.arpa

Then add that to your list of forwarded domains:

```
echo "policy.add(policy.suffix(policy.FORWARD('127.0.0.1@53535'), policy.todnames({'lan','201.168.192.in-addr.arp
echo "policy.add(policy.suffix(policy.DENY, policy.todnames({'168.192.in-addr.arpa'})))" >>$CONFIGFILE
```

horada 22d

Great! it works as expected 🙂, Thanks!

Just question about denying the rest of the `192.168.*` network for reverse DNS lookup, is it necessary?
I used just following part `168.192.in-addr.arpa` in the first command, because I have more networks that just the `201` and didn't used the second (`DENY`) command at all and it seems it works properly. So just want to know, if there is some reason for denying the unused part of the `192.168.*` network .

dpdrown 22d

It's considered nice to not forward those queries on to the general internet. You don't strictly have to filter it, but the people receiving all this junk DNS traffic would appreciate less of it.

horada 22d

Ah, ok ... so when I have forward to dnsmasq the whole private range (`168.192.in-addr.arpa`) it is ok, because it will not be forwarded outside, right?

dpdrown 22d

Yup, that's fine. dnsmasq's setting `Network > DHCP and DNS > Advanced Settings > Filter private (Do not forward reverse lookups for local networks)` is on by default

horada 22d

Thanks for explanation! 🙂

b00zuki 14d

Thanks alot for explaining how to fix the local name resolution. I was really wondering why something so basic like local DNS lookup wasn't working out of the box.

It's a basic feature and needs to be fixed fast. There should be definitly a way to configure it via web-ui and not only via shell.

npr 14d

Well, now I feel dumb, since I spent all night yesterday on disabling kresd and making dnsmasq be the default resolver. The problem is there seem to be a couple of custom scripts cz.nics ships that make sure kresd is the resolver that run periodically.

@dpdrown Do I need something special to make sure kresd forwards these queries for AAAA records as well? (if we take into account that dnsmasq will look at /tmp/hosts/odhcpd)

thessy 14d

Set the dnsmasq server port to 5353 and added the adapted line to /etc/init.d/kresd. Does not work for me, after that kresd does not start anymore. No message in /var/log/messages 😐

After swichting from openwrt router to turris omnia it would be fine, to have back local domain name resolving!

Hopefully cz.nic will bring update soon...

radekpribyl 14d

it is not adapted - it's additional line which needs to be inserted. Can you post the whole init_header() function?

thessy 14d

I know. I added after line 38 I following line:

echo "policy.add(policy.suffix(policy.FORWARD('127.0.0.1@5353'), policy.todnames({'pigdom'})))" >> $CONFIGFILE

For explanation, I changed my local domain from 'lan' to 'pigdom'. dnsmasq runs on port 5353

radekpribyl 14d

Not sure about the line number - I added it as line #40 and it works fine - see below

```
init_header() {
    echo "--Automatically generated file; DO NOT EDIT" > $CONFIGFILE
    echo "modules = {" >> $CONFIGFILE
    config_get_bool prefetch common prefetch 0
    echo "    'policy'" >> $CONFIGFILE
    if [ "$prefetch" \!= 0 ]; then
            echo "  , 'stats'" >> $CONFIGFILE
            echo "  , predict = {" >> $CONFIGFILE
            echo "        window = 30 -- 30 minutes sampling window" >> $CONFIGFILE
            echo "      , period = 24*(60/30) -- track last 24 hours" >> $CONFIGFILE
            echo "  }" >> $CONFIGFILE
    fi
    echo "}" >> $CONFIGFILE
    echo "policy.add(policy.suffix(policy.FORWARD('127.0.0.1@5353'),  policy.todnames({'home'})))" >>$CONFIGFILE
}
```

thessy 13d

Thanks! Added to line #41 and it works now

dpdrown 10d

> npr:

> Do I need something special to make sure kresd forwards these queries for AAAA records as well? (if we take into account that dnsmasq will look at /tmp/hosts/odhcpd)

kresd forwards AAAA records, but dnsmasq's automatic AAAA record creation (the ra-names flag on the dhcp-range option) isn't enabled.

Etz 6d

> radekpribyl:
>
> $CONFIGFILE

Any ideas where is that config file actually spawned?

---

radekpribyl 6d

check the /etc/init.d/kresd script and you can see:

```
CONFIGFILE=/tmp/kresd.config
```

Etz 6d

Yes, I could have checked it, but I'm currently away from my omnia... 😉

Mateusz_Czeladka 6d

This should be a default config that knotdns starts on port 53 and dnsmasq on 54 or 5353 and then that knotdns forwards to dnsmasq. Ok, Turris Omnia is for powerful users but still I vote for +1 on this as default config.

Ondrej_Caletka 6d

> Mateusz_Czeladka:
>
> but still I vote for +1 on this as default config.

I think appropriate *pull request* would work much better than voting 😉

Etz 6d

Well, Luci needs additional comment or tooltip as well then, because if regular user sees that config page, he would think that programmers were drunk to choose non standard DNS port, as all other OpenWRT routers use 53... (He changes it back to 53 and instantly breaks DNS) 😀

Jirka 1d

There is no way, how to configure .lan thing to the knot itself? Using dnsmasq for that is the only way to do that?

I dont care about luci, configuring via script is fine for me, but I dont know how. And it seems cleaner solution to me.