

[New issue](#)[Jump to bottom](#)

Prevent intermittent DNS failures when DNS server in local network is used. #55

gjdoornink wants to merge 1 commit into [home-assistant:master](#) from [gjdoornink:issue/issue-dns-forward-optional-external](#)

Conversation 8 Commits 1 Checks 0 Files changed 1



gjdoornink commented on Sep 23, 2021 • edited

Since the default forward policy is configured for sequential load balancing do not use `dns://127.0.0.1:5553` when a DNS server is specified either through DHCP (`.locals`) or the local configuration (`.servers`) since this will result in intermittent DNS lookup errors for hosts in the local network that are only known through the specified DNS servers.

To expand a bit, when a DNS server is specified either through DHCP (`.locals`) or the local configuration (`.servers`) the forward line will become something like: `forward . 'dns://192.168.0.1 dns://127.0.0.1:5553'`.

This means that DNS lookups for hosts in the local network (192.168.0.0/24) will, depending on the circumstances, be forwarded either 192.168.0.1 or 127.0.0.1:5553. When the DNS lookup for a host in the local network is forwarded to 127.0.0.1:5553, the lookup will fail.

edit: I had `.locals` and `.servers` the wrong way around, this is now fixed in the text above.



Since the policy is configured for sequential load balancing do not u...

ad16ddb

homeassistant commented on Sep 23, 2021

Hi @gjdoornink,

It seems you haven't yet signed a CLA. Please do so [here](#).

Once you do that we will be able to review and accept this pull request.

Thanks!

 homeassistant added `cla-needed` `cla-signed` and removed `cla-needed` labels on Sep 23, 2021

gjdoornink mentioned this pull request on Sep 23, 2021

Not resolving local host names #20



fenichelar commented on Sep 23, 2021

@gjdoornink @alexdelprete

I thought `.servers` was the list of manually configured DNS servers and `.locals` was the list of DHCP configured DNS servers? Do I have that backwards?

```
{{ join " " .servers }}
{{ if len .locals | eq 0 }}
  dns://127.0.0.11
{{ else }}
  {{ join " " .locals }}
{{ end }}
{{ if and (len .servers | eq 0) (len .locals | eq 0) }}
  dns://127.0.0.1:5553
{{ end }}
```

I am a bit confused by the 3rd line above. Why is `dns://127.0.0.11` being added if there are no local servers configured?

Correct me if I am wrong, but it looks like this will still result in the Cloudflare DNS servers being used if any of these errors are returned by the DHCP/locally configured DNS server: `REFUSED, SERVFAIL, NXDOMAIN`.

Maybe it makes sense to have the DNS `mode` configurable:

- `dhcp` - Use DHCP provided DNS servers only
- `manual` - Use manually configured DNS servers only
- `cloudflare` - Use Cloudflare DNS servers only
- `automatic` (default) - Use manually configured DNS servers, DHCP provided DNS servers, and Cloudflare DNS servers (current behavior before this PR)

I run my own DNS resolver and use DNS based blocking. DNS queries sent to external servers are blocked. Home Assistant constantly tries to connect to Cloudflare and fails. Even with the change in this PR, Home Assistant would still try to connect to Cloudflare if my DNS server returned `NXDOMAIN`. So I would run `dhcp` because my DHCP server returns my DNS server.

This would also benefit people who want the privacy benefits of using Cloudflare's DNS server instead of their ISP's DNS server. They could simply set the mode to `cloudflare` and all requests would be securely be sent to Cloudflare.

```
{{if .mode | eq "automatic"}}
forward . {{ join " " .servers }} {{ join " " .locals }} dns://127.0.0.1:5553 {
  except local.hass.io
  policy sequential
  health_check 1m
}
fallback REFUSED, SERVFAIL, NXDOMAIN . dns://127.0.0.1:5553
{{end}}
```

```
{{if .mode | eq "cloudflare"}}
forward . dns://127.0.0.1:5553 {
  except local.hass.io
  policy sequential
  health_check 1m
}
{{end}}

{{if .mode | eq "manual"}}
forward . {{ join " " .servers }} {
  except local.hass.io
  policy sequential
  health_check 1m
}
{{end}}

{{if .mode | eq "dhcp"}}
forward . {{ join " " .locals }} {
  except local.hass.io
  policy sequential
  health_check 1m
}
{{end}}
```

I removed the `dns://127.0.0.11` line from the `automatic` section because I don't see any reason for it to be there. But it could put back if it serves a purpose.

Thoughts?

gjdoornink commented on Sep 24, 2021 • edited

Author

@fenichelar

I thought `.servers` was the list of manually configured DNS servers and `.locals` was the list of DHCP configured DNS servers?
Do I have that backwards?

No, it seems I had it backwards, sorry about that :-)

I am a bit confused by the 3rd line above. Why is `dns://127.0.0.11` being added if there are no local servers configured?

Since I had it backwards, `dns://127.0.0.11` is only added if no DNS server is assigned through DHCP.

Maybe it makes sense to have the DNS mode configurable

It might, but the purpose of this patch is only to fix the intermittent failures of resolving hosts in the local network.
IMHO other changes are better served as a separate issue or pull request.

I removed the `dns://127.0.0.11` line from the `automatic` section because I don't see any reason for it to be there. But it could put back if it serves a purpose.

I do assume there was and is a reason and a purpose and, after going through a lot of the related discussions, I assume it has to do with ensuring a fallback is always present.

Kind regards,



gjdoornink commented on Sep 24, 2021

[View changes](#)

gjdoornink left a comment • edited

Author

The commit message has `(.locals)` and `(.servers)` the wrong way around.

fenichelar commented on Sep 24, 2021

I do assume there was and is a reason and a purpose and, after going through a lot of the related discussions, I assume it has to do with ensuring a fallback is always present.

I'm not sure. I believe `dns://127.0.0.11` would just point to the block the forward statement is already in. I feel like this might be a bug.

gjdoornink commented on Sep 24, 2021

Author

I'm not sure. I believe `dns://127.0.0.11` would just point to the block the forward statement is already in. I feel like this might be a bug.

I believe that `127.0.0.11` is the Embedded DNS Server of Docker.

gjdoornink mentioned this pull request on Sep 25, 2021

Remove hardcoded DNS servers #56

🔒 Closed

pvizeli commented on Sep 28, 2021

Member

See #56 ([review](#))

pvizeli closed this on Sep 28, 2021

gjdoornink commented on Sep 28, 2021

Author

@pvizeli

IMHO you are missing the point of this pull request.

This pull request is not about preventing Home Assistant from using external DNS resolvers.

This pull request is about the fact that using a local DNS resolver together with an external DNS resolver in the .forward statement will eventually result in DNS resolve errors of the hosts in the local network. This is caused due to the fact that .forward is not about defining fallback servers, but about defining a load-balancing pool.

Implementing the 'solution' you described in your comment in pull request #56 does not resolve the issue this PR aims to fix.

I would kindly ask you to reconsider your position



alexdelprete mentioned this pull request on Nov 9, 2021

HomeAssistant CoreDNS timeout settings bentasker/HomeAssistantAddons#3

Open

Reviewers

No reviews

Assignees

No one assigned

Labels

cla-signed

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants

