

HA OS DNS Setting - Configuration not respected?

le_top

Nov '21

I am surprised about the network address resolution in HA.

I have an OPNSense firewall that provides its own IP as the DNS server and when examining the DNS configuration using `ha dns info`, I get:

```
[core-ssh ~]$ ha dns info
host: 172.30.32.3
locals:
- dns://10.33.2.254
servers: []
update_available: false
version: 2021.06.0
version_latest: 2021.06.0
```

On my firewall, I override some DNS entries to point to the local network address (10.X.X.X) rather than the public (dynamic) network address.

So I want MYPUBLICDOMAIN to resolve to 10.33.2.X (which depends on the subdomain as well).

When I resolve my network address using `nslookup MYPUBLICDOMAIN`, I get my public address, and when I do `nslookup MYPUBLICDOMAIN 10.33.2.254`, I get 10.33.2.175 back. A ping to MYPUBLICDOMAIN resolves in a ping to the public network address.

The answer is more or less found in the dns log, which can be read using `ha dns log`:

```
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
[INFO] 127.0.0.1:52905 - 61064 "NS IN . udp 17 false 512" NOERROR - 0 30.00076.
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 172.30.32.2:36022 - 17994 "A IN version.home-assistant.io. udp 43 false
```



So the local dns service is checking addresses on cloudflare - WTH ?! That's not what I want - my firewall is acting as a DNS filter as well (it seems that I'll need to find a way to block those alternative DNS services).

The expected behavior is to use the configuration provided by the DHCP server first. I would also not use a third party service unless getting acceptance from the user. And maybe let him choose between Cloudflare, freenom.world, google, etc.

How to make this work properly?

To point to my local dns service first, I did this:

```
ha dns option --servers dns://10.33.2.254 --servers dns://80.80.80.80 --serve
```



But IMHO that's not something that should be required!

[Note: I am also adding a rule to my firewall: [HOWTO - Redirect all DNS Requests to Opnsense](#) - `nslookup MYPUBLICDOMAIN 1.0.0.1` now shows my local address as well]

[🔗 Installing Home Assistant OS using Proxmox 7](#)

[🔗 Improve Privacy, Stop using hardcoded DNS](#)

francisp Francis

Nov '21

There is a long thread about this on this forum. Short result: if you don't like this behavior, don't use HA OS or HA Supervised, but switch to HA Container or HA Core.

le_top

Nov '21

Well, were not really informed about it before installing it. AFAIK the general default behavior is to first check the DNS provided by the DHCP service

Anyway, my firewall now fixes it for whatever device tries to bypass the local DNS this way.

koying Chris B

Nov '21

TBH, Supervised installing a half-dozen containers (and now requiring an "OS agent") should be a big warning sign that it does more than it should 😞

le_top

Nov '21

I do not know how many hidden containers it installs, but having separate containers is a good thing to isolate services. So it's not an indicator that it does more than it should for me, but give a positive impression instead. My reported containers are: "Terminal & SSH", "Check Home Assistant configuration", "Mosquitto

broker", "File editor", "Custom deps deployment", "SQLite web", "Grafana". So that's half a dozen but I am sure that they are not all there.

koying Chris B Nov '21

My point is: Why does an application like HomeAssistant needs to install a DNS server of it's own in your/my LAN in the first place...

francisp Francis Nov '21

Look at the one's starting with Hassio:

<input type="checkbox"/>	Name	Status	File	Quick actions	Stack	Image
<input type="checkbox"/>	addon_docker2mqtt_portainer	running	3.0		-	ghcr.io/hassio-addons/portainer/sarchd4.2.0.0
<input type="checkbox"/>	homeassistant	running	3.0		-	ghcr.io/home-assistant/supbergyak-4k-homeassistant.2021.01
<input type="checkbox"/>	addon_3183ebd8_tatacloud	running	3.0		-	3183ebd8/sarchd4-addon-tatacloud.1.1
<input type="checkbox"/>	hassio_supervisor	running	3.0		-	homeassistant/sarchd4-hassio-supervisor
<input type="checkbox"/>	hassio_observer	running	3.0		-	ghcr.io/home-assistant/sarchd4-hassio-observer.2021.01.0
<input type="checkbox"/>	hassio_db	running	3.0		-	ghcr.io/home-assistant/sarchd4-hassio-db.2021.01.0
<input type="checkbox"/>	addon_0c070704_hassio_google...	running	3.0		-	suberchen/hassio-google-drive-backup-sarchd4.0.105.2
<input type="checkbox"/>	addon_crow_configuration	running	3.0		-	homeassistant/sarchd4-addon-configuration.5.5.5
<input type="checkbox"/>	addon_d0707014_influxdb	running	3.0		-	ghcr.io/hassio-addons/influxdb/sarchd4.2.2.0
<input type="checkbox"/>	addon_d0707014_grafana	running	3.0		-	ghcr.io/hassio-addons/grafana/sarchd4.2.2.0
<input type="checkbox"/>	hassio_audio	running	3.0		-	ghcr.io/home-assistant/sarchd4-hassio-audio.2021.01.0
<input type="checkbox"/>	hassio_multicast	running	3.0		-	ghcr.io/home-assistant/sarchd4-hassio-multicast.2021.04.0
<input type="checkbox"/>	hassio_dns	running	3.0		-	ghcr.io/home-assistant/sarchd4-hassio-dns.2021.04.0

le_top Nov '21

@francisp How did you get that list? I'd love to be able to intervene on the containers (I am running two systems: on on a Pi and another one on a Nuc).

@koying As far as I understand, the DNS server is an Add-on that can be added by choice - as I did not see any use for it, I did not add it.

The description says: "For example, you can have your Home Assistant domain resolve with an internal address inside your network."
So yes, that is what I did on my firewall - my publicdomain is resolved to a local IP inside my network.
That addon allows you to add static IPs, etc.

Then of course the DNS server would also require the DHCP server to be installed so that you can tell your clients that they should not use the internet router.

As long as those are choices, that's fine by me, sending of DNS queries to a party not "dictated" by my setup is another. I know that some information for usage statistics is sent to Nabu Casa in several ways which is pretty much unavoidable if you configure a system for automatic updates.

Base on the list provided by @francisp , I am in favor of this approach and I do not consider it to be excessive - it's almost not enough because there could be one container per integration - that might help avoid restarting my ZHA every time I make a change to the configuration that requires an HA restart which stops my ZHA for a moment, and puts some of the devices to a temporary sleep - I even have a few that do not recover all the time from such an interruption.

tmjpugh Nov '21

le_top:
How did you get that list?

Looks like Portainer

francisp Francis Nov '21

Indeed, Portainer.

koying Chris B Nov '21

le_top:
As far as I understand, the DNS server is an Add-on that can be added by choice - as I did not see any use for it, I did not add it.

Nope. hassio-dns is not optional, and you have it, whether you like it or not, as you noticed, basically.

k8gg Nov '21

le_top:
Anyway, my firewall now fixes it for whatever device tries to bypass the local DNS this way.

Sidebar, and I'm interested: what do the firewall rules look like around this?
I mean, blocking local devices from reaching out to 1.1.1.1 is only half of the fight, right?

Now back to the subject - With the levels of control you are looking for, the install method of HAOS might not be for you. Consider either Core or Container methods.

le_top

Nov '21

- Unfortunately, Portainer is discontinued - it would have been nice for monitoring/restarting only.
- hassio-dns is not optional- Ok, I can't check because I cant install portainer - while the configuration looks more like a "resolv.conf" than a DNS Server, there is a [full DNS server as far as information goes]
- @k8gg I provided the HOWTO in my initial post - basically you add a rule to the firewall matching all outbound requests to port 53 and route the to the firewall's local DNS server. So I did not add a rule to block 1.1.1.1 and 1.0.0.1 specifically, but this reroutes all historical DNS requests (it does not block *all* DNS request types). There is probably a list out there with all "public" DNS services so that you could block their IPs.
- Control: I am not looking for *full* control - there's stuff I like in HAOS - I do not have to care so much for the host os, etc.

koying Chris B

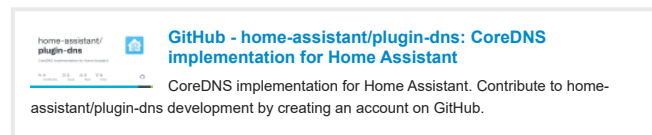
Nov '21

le_top:

while the configuration looks more like a "resolv.conf" than a DNS Server

I think you are confusing one of the addons and the actual plugin.

hassio-dns is a full CoreDNS server, and I don't remember any configuration options on the user side (I stopped using Supervised when a root os-agent was requested above all the stuff that was already installed).



francisp Francis

Nov '21

le_top:

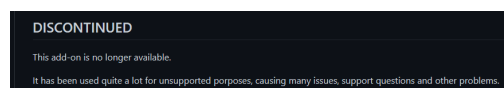
Unfortunately, Portainer is discontinued

Where did you get that idea ? Portainer has been replaced by Portainer-ce, but they are essentially the same.

koying Chris B

Nov '21

The portainer *addon* is discontinued. They *really* don't want you to install anything else...



francisp Francis

Nov '21

I did not know that. I still have it installed on my HA instances.

Tamsy

Nov '21

Luckily i installed Portainer as an Add-on ~2 weeks ago. But I noticed with core-2021.11.3 the icon has suddenly changed.

Well, it was used a lot for unsupported **purposes** ... 🤔

The noose tightens for HA supervised users.

koying Chris B

Nov '21

I've been a bit harsh with the DNS plugin: it basically mimic what docker is doing in bridge mode to resolve docker containers, specifically addons here, in host mode.

I've done some tests in a VM, and DNS resolution works fine: it *does* go to my internal DNS without tweakings.

Cloudflare is only a fallback if the default DNS cannot be reached.

OP, you didn't tell what kind of installation you have: HassOS on device? HassOS in VM? Supervised?

baz123 Brian

Nov '21

It was a toys out of the pram moment I think 🤔

Note the message "used for unsupported purposes"...