pfSense - Bug #5413

Incorrect Handling of Unbound Resolver [service restarts, cache loss, DNS service interruption]

11/10/2015 11:42 PM - ky41083 -

Status:	Confirmed	**Start date:**	11/10/2015
Priority:	High	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	0%
Category:	DNS Resolver	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	All	**Affected Architecture:**	

Description

The right way to handle local DNS changes, for Unbound at least, would basically be to do the opposite of what is being done now. Rather than write to the config files and bounce the service, you would use unbound-control to tell Unbound about the local DNS changes.

Discussion here: https://forum.pfsense.org/index.php?topic=89589.0
Full rough draft solution here: https://forum.pfsense.org/index.php?topic=89589.msg568043#msg568043

Quick and dirty rough draft summary... doubt code syntax is even completely right (if I had more time it would be, leave it up to who codes it), but this method is the only right one. The only other solution would be to remove Unbound completely and replace it with something else (please don't, it works very well when used correctly).

Functions like this:
$unbound_entries .= "local-data: \"{$host['fqdn']} {$type} {$host['ipaddr']}\"\n";

Should be changed to something like this:
$unbound_cmd .= "unbound-control local_data {$host['fqdn']} {$type} {$host['ipaddr']}";

And NEVER EVER bounce the Unbound service. Ever. It is completely unnecessary.

Initial service start / user initiated service restart should probably use the same unbound-control calls for managing all local DNS entries, to prevent both modifying Unbound config files and calling unbound-control to do the same exact thing. Plus it's cleaner, now we don't have 2 code paths to maintain (config files & unbound-control), and we don't use more RAM to store unneeded config file entries.

Additional implementation considerations can be found in the cited post above.

History

#1 - 11/11/2015 12:18 AM - Chris Buechler

- Category set to DNS Resolver

- Status changed from New to Confirmed

- Priority changed from Normal to High

#2 - 11/11/2015 01:58 AM - ky41083 -

Can someone please add "DNS service interruption" to the portion of the title in brackets? It is also a main symptom, but I spaced on it when I created the issue. TY

#3 - 12/24/2015 02:11 AM - David Wood

I know a bug report is not really the place for arguing about the merits of a solution, but I respectfully maintain some of my caution in https://forum.pfsense.org/index.php?topic=89589.msg568394#msg568394 , especially in relation to ky41083's assertion that there is no need ever to restart Unbound.

Changes in local-data can be handled via unbound-control as ky41083 says - though the inability to remove just the A or AAAA record will likely require some care, as both can exist for the same local host and there is no guaranteed temporal relationship between changes in A and AAAA. In particular, DHCP and DHCPv6 are entirely separate and not synchronous.

Unlike ky41083, I cannot see any alternative to restarting Unbound if there are configuration changes made to Unbound beyond changes to local data, as SIGHUP and unbound-control reload unfortunately amount to a reload at present (i.e. cache flush and re-read of the configuration files). unbound-control does not allow for on-the-fly reconfiguration of all aspects of Unbound. This is why I suggested a diff based approach on the forums as one possibility.

These are, of course, implementation points. I agree that Unbound should be reconfigured on-the-fly whenever possible. In time, I hope that Unbound will get saner SIGHUP handling, but this will likely be a lot of work.

Unfortunately, I have no time to work on this issue at present.

#4 - 01/26/2016 04:04 AM - Jim Thompson

- Subject changed from Incorrect Handling of Unbound Resolver [service restarts, cache loss] to Incorrect Handling of Unbound Resolver [service restarts, cache loss, DNS service interruption]

#5 - 01/26/2016 04:05 AM - Jim Thompson

- Assignee set to Renato Botelho

#6 - 02/23/2016 03:25 AM - robi robi

I had to go back to DNS Forwarder (dnsmasq) because of this.
In my case, unbound was restarting itself every 2 seconds, and clients were complaining about no internet access.

Please provide a quick fix, what lines should be modified on a running system to restore unbound functionality.
Thank God dnsmasq it's still inthere and only a checkbox away.

#7 - 02/23/2016 05:39 PM - Chris Buechler

robi: your issue is almost certainly a different root cause, this issue just exacerbates it. Post a new thread on the forum describing what you're seeing, with your system logs from the time.

#8 - 04/02/2016 10:53 PM - ky41083 -

No, arguing about the merits of a solution is not what Redmine bug reports are for, so I won't be, as it just makes more work for the people actually trying to fix the bug. I wouldn't normally even post the following here, but someone clearly felt the need to re-post issues here that are already posted and addressed in the forum.

Your concerns addressed, David:

https://forum.pfsense.org/index.php?topic=89589.msg568708#msg568708
https://forum.pfsense.org/index.php?topic=89589.msg607906#msg607906

I completely welcome any further discussion, in the forum. That place where people who "unfortunately, have no time to work on this issue at present" can constructively hash out finer implementation details.

#9 - 10/04/2016 11:04 AM - Anonymous

Is there any update on when this might get worked on? It has been almost a year now.

#10 - 10/10/2016 09:32 PM - ky41083 -

If the dev's won't / can't answer you, I will. Due to changes in 2.3 (I tested with 2.3.2p1), restarting of the Unbound service to pick up any live DNS changes has been rendered completely and wholly UNNECESSARY. My guess is nobody's figured this out yet because all the kill / restart Unbound code is still present and used.

All you have to do now (this didn't fully work on 2.2.6, requiring a reboot to pickup some live DNS changes, like static DHCP), is disable all the code points that restart Unbound, and poof, everything just works, without so much as poking Unbound itself. Yes, I have a patch. Yes, I will post it soon. I just updated from 2.2.6 a few days ago and am still getting things sorted...

#11 - 10/10/2016 11:50 PM - BBcan177 .

Some users have also reported issues with the Unbound Resolver and pfBlockerNG DNSBL. I am not able to reproduce, but some users are reporting that Unbound Fails to reload after IP Interface changes when DNSBL is enabled. I assume this is due to the fact that DNSBL adds an include file which might take a little longer to load:

```
server:include: /var/unbound/pfb_dnsbl.conf
```

The pfBlockerNG DNSBL Reload code here as reference:
https://github.com/pfsense/FreeBSD-ports/blob/devel/net/pfSense-pkg-pfBlockerNG/files/usr/local/pkg/pfblockerng/pfblockerng.inc#L1402

#12 - 10/11/2016 12:17 AM - ky41083 -

Patch Posted: https://forum.pfsense.org/index.php?topic=119467.0

#13 - 10/11/2016 12:40 AM - ky41083 -

BBcan177 . wrote:

> Some users have also reported issues with the Unbound Resolver and pfBlockerNG DNSBL. I am not able to reproduce, but some users are reporting that Unbound Fails to reload after IP Interface changes when DNSBL is enabled. I assume this is due to the fact that DNSBL adds an include file which might take a little longer to load:
>
> server:include: /var/unbound/pfb_dnsbl.conf
>
> The pfBlockerNG DNSBL Reload code here as reference:
> https://github.com/pfsense/FreeBSD-ports/blob/devel/net/pfSense-pkg-pfBlockerNG/files/usr/local/pkg/pfblockerng/pfblockerng.inc#L1402

I would guess, that the Unbound full cache dump / load process, adds FAR more delay, than the additional include file ever could. Just using the GUI options for Unbound, you can easily end up with a multi-gigabyte DNS cache. The pfSenseless dev's have discussed this as a way to keep the Unbound cache when reloading it, and even they know better than to do this.

pfBlockerNG DNSBL, should absolutely not be doing it either. You should open a bug citing the poor cache handling choice.

#14 - 10/16/2016 10:37 PM - Anonymous

The patch you posted only prevents Unbound from being restarted by performing GUI actions, not automatically when a new DHCP lease is granted. This is because Unbound is restarted directly by "dhcpleases" in that case. If the "dhcpleases" configuration is modified such that it does not restart Unbound, Unbound never picks up any changes to its configuration.

#15 - 11/30/2016 07:32 PM - ky41083 -

With the patch above applied, and "Register DHCP leases in the DNS Resolver" enabled, the Unbound service does not restart. Ever. Verified by following:

Via SSH:

unbound-control -c /var/unbound/unbound.conf stats_noreset

--- snip ---
time.now=1480555628.497528
time.up=683456.981686
time.elapsed=683456.981686
--- snip ---

Dashboard displays:
Uptime 7 Days 21 Hours 54 Minutes 12 Seconds

All DHCP leases are fully DNS resolvable via Unbound, regardless of if they are new as of 7 seconds or 7 days ago.

Any questions?

#16 - 11/30/2016 07:44 PM - ky41083 -

Michael Marley wrote:

> Unbound is restarted directly by "dhcpleases"

Please post a Github link to the file + line you are referring to.

Everything I've looked at, and all behavior I am seeing, says anything starting / stopping Unbound, works by calling functions in either services.inc or unbound.inc.

#17 - 05/30/2017 06:42 AM - Anonymous

Hi all

I'm facing same issue on our pfSense boxes.

We're using unbound and configured dhcp server to update unbound.
Each time a new devise, workstation, laptop, smartphone or tablet request an IP, unbound is restarted.
All our systems are using pfSense unbound and quite frequently Continuous Integration jobs failed when they try to resolv a name.

What about including ky41083 patch ?

#18 - 05/30/2017 03:31 PM - Dmitriy K

- File resolver.log added

Sadly, I've faced the same problem with Unbound. This issue forced me to use RAM disks. I hope there will be a fix in near future.

#19 - 12/25/2019 02:42 AM - Jason NA

Is there any update here? Apparently there has been a fix available for over 2 years?

#20 - 01/02/2020 10:28 AM - Nick B

This is a big problem when using pfblockerng and also registering DHCP leases in the resolver as it causes unbound to reload frequently and because of the large pfblockerng database unbound can take ~20 seconds to reload causing disruptions for all clients. Can this patch here get included?

#21 - 01/02/2020 10:38 AM - Jim Pingle

There is no patch here to apply. There are some general theories and wishes, but no code. If someone wants to take it on, we'd be more than happy to review a pull request to make the recommended changes.

#22 - 01/10/2020 06:17 PM - Alexander Berkes

Hi all,

I have been looking at this issue for the last few days, because I am affected by myself and would like this annoying bug to be fixed.

One of the biggest problems is dhcpleases sending a SIGHUP to the unbound process instead of using unbound-control to update the dhcp leases state.
This is especially noticed when unbound is used in conjunction with pfBlockerNG and huge dns-blocklists are in use.

Call me a google noob, but somehow I couldn't find anything else regarding source-code of dhcpleases than:
[[https://github.com/unexpectedBy/pfsense-tools/blob/master/pfPorts/dhcpleases/files/dhcpleases.c]]

Sadly, this is not the current version of dhcpleases.

Anyhow, I took the above mentioned code of dhcpleases as a basis and wrote a diff based solution with unbound-control.
First tests show me that it is basically doing what it should.

Could anybody toss me towards the right direction if there is any repository containing the latest version of dhcpleases?

Regards

#23 - 01/13/2020 05:36 AM - Renato Botelho

Alexander Berkes wrote:

> Hi all,
>
> I have been looking at this issue for the last few days, because I am affected by myself and would like this annoying bug to be fixed.
>
> One of the biggest problems is dhcpleases sending a SIGHUP to the unbound process instead of using unbound-control to update the dhcp leases state.
> This is especially noticed when unbound is used in conjunction with pfBlockerNG and huge dns-blocklists are in use.
>
> Call me a google noob, but somehow I couldn't find anything else regarding source-code of dhcpleases than:
> [[https://github.com/unexpectedBy/pfsense-tools/blob/master/pfPorts/dhcpleases/files/dhcpleases.c]]
>
> Sadly, this is not the current version of dhcpleases.
>
> Anyhow, I took the above mentioned code of dhcpleases as a basis and wrote a diff based solution with unbound-control.
> First tests show me that it is basically doing what it should.
>
> Could anybody toss me towards the right direction if there is any repository containing the latest version of dhcpleases?
>
> Regards

https://github.com/pfsense/FreeBSD-ports/blob/devel/sysutils/dhcpleases/files/dhcpleases.c

#24 - 01/14/2020 03:02 PM - Alexander Berkes

Renato Botelho wrote:

> https://github.com/pfsense/FreeBSD-ports/blob/devel/sysutils/dhcpleases/files/dhcpleases.c

Thanks for the link.

I made a fork and added my changes:
[[https://github.com/n3bul4/FreeBSD-ports/blob/devel/sysutils/dhcpleases/files/dhcpleases.c]]

First of all, this is just a proof of concept. I only made a few tests so far, which look good to me. Any help is appreciated.

The way this works is by making a diff (with the standard diff command) between the current dhcp.leases file and the corresponding unbound view (called dhcpleases).
Obsolete DNS entries get removed and new ones are added (via unbound-control).

For this to work, a few changes to unbound.conf are needed:

1.) unbound needs to be configured with a view named "dhcpleases"

```
view:
    name: dhcpleases
```

2.) every interface, where clients should "see" the hostnames needs to have an access-control-view directive:

```
server:
    access-control-view: 192.168.12.0/24 dhcpleases
    access-control-view: 192.168.13.0/24 dhcpleases
    access-control-view: 192.168.14.0/24 dhcpleases
    .
    .
    .
```

The above would add access for all clients in the networks 192.168.12.0-192.168.14.0 with a netmask 255.255.255.0.

3.) The include directive for dhcpleases_entries.conf in unbound.conf has to be removed / commented out

```
# dhcp lease entries
#include: /var/unbound/dhcpleases_entries.conf
```

For a quick shot, points 1 and 2 can be added to the "Custom options" section in the pfsense DNS Resolver configuration webgui.
For point 3 to work, one would have to edit /etc/inc/unbound.inc. Function unbound_generate_config_text.
Simply search for "# dhcp lease entries" and comment out the line below as shown in point 3.
Compile dhcpleases, copy it to your pfsense box.
Make a backup of /usr/local/sbin/dhcpleases.
Kill running dhcpleases process.
Move compiled dhcpleases version to /usr/local/sbin/dhcpleases.
Restart unbound.

Final notes:

The code creates 2 files in /tmp:
/tmp/dhcpleases.sort
/tmp/dhcpleases.diff

New DNS entries are added with a bulk operation (view_local_datas), whereas delete operations are done one by one.
This is due to lack of a bulk remove operation from views in unbound-control, which would be a nice feature request.
So keep in mind, that DNS delete operations will take longer than adding DNS entries.

dhcpleases logs information about addded / removed entries to system.log

Any thoughts and help are welcome!

#25 - 01/14/2020 03:42 PM - Renato Botelho

Alexander Berkes wrote:

> Renato Botelho wrote:
>
> > https://github.com/pfsense/FreeBSD-ports/blob/devel/sysutils/dhcpleases/files/dhcpleases.c
>
> Thanks for the link.
>
> I made a fork and added my changes:
> [[https://github.com/n3bul4/FreeBSD-ports/blob/devel/sysutils/dhcpleases/files/dhcpleases.c]]
>
> First of all, this is just a prove of concept. I only made a few tests so far, which look good to me. Any help is appreciated.
>
> The way this works is by making a diff (with the standard diff command) between the current dhcp.leases file and the corresponding unbound view (called dhcpleases).
> Obsolete DNS entries get removed and new ones are added (via unbound-control).
>
> For this to work, a few changes to unbound.conf are needed:
>
> 1.) unbound needs to be configured with a view named "dhcpleases"
>
> [...]
>
> 2.) every interface, where clients should "see" the hostnames needs to have an access-control-view directive:
>
> [...]
>
> The above would add access for all clients in the networks 192.168.12.0-192.168.14.0 with a netmask 255.255.255.0.
>
> 3.) The include directive for dhcpleases_entries.conf in unbound.conf has to be removed / commented out
> [...]
>
> For a quick shot, points 1 and 2 can be added to the "Custom options" section in the pfsense DNS Resolver configuration webgui.
> For point 3 to work, one would have to edit /etc/inc/unbound.inc. Function unbound_generate_config_text.
> Simply search for "# dhcp lease entries" and comment out the line below as shown in point 3.
> Compile dhcpleases, copy it to your pfsense box.
> Make a backup of /usr/local/sbin/dhcpleases.
> Kill running dhcpleases process.
> Move compiled dhcpleases version to /usr/local/sbin/dhcpleases.
> Restart unbound.
>
> Final notes:
>
> The code creates 2 files in /tmp:
> /tmp/dhcpleases.sort
> /tmp/dhcpleases.diff
>
> New DNS entries are added with a bulk operation (view_local_datas), whereas delete operations are done one by one.
> This is due to lack of a bulk remove operation from views in unbound-control, which would be a nice feature request.
> So keep in mind, that DNS delete operations will take longer than adding DNS entries.
>
> dhcpleases logs information about addded / removed entries to system.log
>
> Any thoughts and help are welcome!

please submit the proposed changes as a Pull Request against FreeBSD-ports repository -
https://docs.netgate.com/pfsense/en/latest/development/submitting-a-pull-request-via-github.html

This way developers can review what you have changed

#26 - 01/14/2020 04:45 PM - Alexander Berkes

[[https://github.com/pfsense/FreeBSD-ports/pull/751]]

#27 - 03/30/2020 04:26 PM - Brittney Lars

How are other people dealing with this issue or working around it? For me it's causing such frequent internet outages (dns outages are internet outages for clients) on my network that I am starting to consider looking for an alternative.

#28 - 03/30/2020 09:28 PM - Nick B

Brittney Lars wrote:

> How are other people dealing with this issue or working around it? For me it's causing such frequent internet outages (dns outages are internet outages for clients) on my network that I am starting to consider looking for an alternative.

I have disabled registering DHCP leases in the resolver. Even though I rely on that feature I'd rather not have frequent DNS interruptions than local hostname resolutions.

#29 - 04/01/2020 12:08 PM - Brittney Lars

Thanks @Nick B this workaround works well.

#30 - 12/02/2020 12:03 PM - Raffi T

Thanks for all the work on this. It seems like there is progress made on that git page, but the status of this bug is still 0%. Is that correct? What's the status of the code review?

Thanks,
Raffi

Files

resolver.log	500 KB	05/30/2017	Dmitriy K