pfSense - Bug #7413

status_dhcpv6_leases.php: Some DHCPv6 leases are not displayed in the GUI

03/20/2017 01:31 PM - Jim Pingle

Status:	Resolved	**Start date:**	03/20/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	DHCP (IPv6)	**Estimated time:**	0.00 hour
Target version:	2.4.3		
Plus Target Version:		**Affected Version:**	2.4
Release Notes:		**Affected Architecture:**	All

Description

On status_dhcpv6_leases.php, only about half the leases in my /var/dhcpd/var/db/dhcpd6.leases file are displayed in the GUI (ia-na blocks) and none of my local prefix delegations are displayed (ia-pd blocks)

Lease that DOES display:

```
ia-na "\000\000\000\000\000\001\000\001\037\372}\255\000\014)xnO" {
  cltt 1 2017/03/20 17:48:38;
  iaaddr 2001:db8::ffff:f236 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 19:48:38;
  }
}
```

The PD for that same lease which does NOT display:

```
ia-pd "\000\000\000\000\000\001\000\001\037\372}\255\000\014)xnO" {
  cltt 1 2017/03/20 17:48:38;
  iaprefix 2001:db8:1:ee70::/60 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 19:48:38;
  }
}
```

Some leases/PD that DO NOT display:

```
ia-na "\000\000\000\000\000\001\000\001\026(\314\301\210\306c\235\351\203" {
  cltt 1 2017/03/20 18:21:26;
  iaaddr 2001:470:1f11:e1c::ff9c {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 20:21:26;
  }
}

ia-na "\000\000\000\000\000\001\000\001\035\212\343x\000@H\262\202\026" {
  cltt 1 2017/03/20 18:00:51;
  iaaddr 2001:db8::ffff:9f51 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
```

```
      ends 1 2017/03/20 20:00:51;
  }
}

ia-pd "\000\000\000\000\000\001\000\001\035\212\343x\000@H\262\202\026" {
  cltt 1 2017/03/20 18:01:06;
  iaprefix 2001:db8:1:eef0::/60 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 20:01:06;
  }
}

ia-na "\000\000\000\000\000\001\000\001\036\220/\231\000\015\2713\017p" {
  cltt 1 2017/03/20 17:57:31;
  iaaddr 2001:db8::ffff:8e10 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 19:57:31;
  }
}

ia-pd "\000\000\000\000\000\001\000\001\036\220/\231\000\015\2713\017p" {
  cltt 1 2017/03/20 17:58:08;
  iaprefix 2001:db8:1:ef00::/60 {
    binding state active;
    preferred-life 4500;
    max-life 7200;
    ends 1 2017/03/20 19:58:08;
  }
}
```

Associated revisions

Revision c56471a7 - 12/17/2017 12:44 AM - Anders Lind

Fixes #7413: Some DHCPv6 leases are not displayed in the GUI

. Better handling/parsing of ISC dhcpv6 leases file and removal of unnecessary properties.
. Experimental Pools/failover handling in the parsing of DHCPv6.
. Cleanup on the Status DHCVPv6 Leases page.
. Correction re. Mac address sent to 'Services' - 'Wake-on-LAN' - 'Edit' page when clicking the + button for 'Add WOL mapping' on the Status DHCPv6 Leases page.
. IPv6 matcher/parser and unit testing of it.
. Small debugging tool for inspecting lease file content.

This corresponds to this commit
https://github.com/al-right/pfSense-dhcpv6-gui-leases-patch/tree/5501616d5b9fc7bcad855b0dadd9d2fef8b4fa43

Please read parser/README.md and https://redmine.pfsense.org/issues/7413#note-11 for more notes about the changes.

History

#1 - 04/06/2017 09:13 PM - Anonymous

Yeah, my DHCPv6 status page is only showing one lease, which happens to be a static reservation. None of the rest of my address leases show up. I don't have any PD going on since the interface is tracking another.

#2 - 05/06/2017 08:50 PM - Anders Lind

I think I found out what the problem is!

This commit changed how the lease file is handled:
https://github.com/pfsense/pfsense/commit/8f867225f4c2d3e61863f8d87d4ddb4143d5dda6#diff-b48bdab1db8f78638fbf6c7d98a01172

Likely it was tested with GNU awk, because here the lease file is parsed without trouble.

The lease file can be found in: /var/dhcpd/var/db

So the line discussed here is line 164 in

:

```
    exec("{$sed} {$cleanpattern} {$leasesfile} | {$awk} {$splitpattern}", $leases_content);
```

To be more specific take the lease file and run in Linux/bash:

```
cat dhcpd6.leases | sed '/^ia-.. /, /^}/ !d; s,;$,,; s,  *, ,g' | awk '{printf $0); $0 ~ /^\}/ {printf "\n"}'
```

It should work fine. You might want while testing to switch history expansion off:
set +o histexpand

In pfSense where tsch is used I do not know how to switch history expansion off, but anyway to make sed run you will have to escape !d with a backslash.
The commands are then:

```
cat dhcpd6.leases | sed '/^ia-.. /, /^}/ \!d; s,;$,,; s,  *, ,g' | awk '{printf $0); $0 ~ /^\}/ {printf "\n"}'
```

Now, when awk gets the output of sed and that output contains a percent character % awk will print out an error message like the below and stop executing - that is the reason why a lot of leases do not show up in the GUI:

```
awk: weird printf conversion %" {
 input record number 58, file
 source line number 1
awk: not enough args in printf(ia-na "+\256\264\003\000\001\000\001\033\226Pg\264\256+\031\273%" {)
 input record number 58, file
 source line number 1
```

Now, there might be other characters than just % that makes awk throw an error so maybe you will get other results as well.
I do not see any % listed in the initial bug description, but it might be located somewhere earlier in the lease file unless as mentioned other characters make awk stop and throw error messages.

I do not know if the percent sign % needs to be escaped e.g. via
sed so that it says %% before being served to awk, but I am looking forward
to hear your results!

Thanks!

#3 - 05/07/2017 08:17 AM - Anders Lind

I can confirm adding an extra sed substitution for % to %% works!

Meaning changing

```
$cleanpattern = "'/^ia-.. /, /^}/ !d; s,;$,,; s,  *, ,g'";
```

to:

```
$cleanpattern = "'/^ia-.. /, /^}/ !d; s,;$,,; s,  *, ,g; s/%/%%/'";
```

, makes it work.

But there is a huge but.

Currently the regular expression matching here
has a problem:

```
    preg_match('/ia-.. "(.*)" { (.*)/ ', $leases_content[$i], $duid_split);
```

Main problem is that new lines have already been removed from the input when we reach here.

This means that it is not deterministic when the 1st group matching of
"(.*)" will end. Why?
Because space character and curly braces {} all are legal characters in the lease file.
Why is that so?
Because quotify_buf
checks for isascii() and isprint().

Now isprint allows characters from 0x20 – 0x7E to become printed directly in the lease file.
So here we go - that breaks the regular expression e.g. should it happen someone has a IAID+DUID that looks like
'" { '
(single quotes are boundaries)

Therefore the idea about that newlines should not be removed too soon.

Now if that problem gets solved and newlines are not removed too soon (by rewriting the code)
we can also avoid having the redundant code with a FIXME in lines 238 - 256 (we could remove all of these lines completely)
https://github.com/pfsense/pfsense/blob/1a8b65541c3a3185792f41ed293aaf763a4caf01/src/usr/local/www/status_dhcpv6_leases.php#L238 :

```
            case "ia-pd":
                $is_prefix = true;
            case "ia-na":
                $entry['iaid'] = $tmp_iaid;
                $entry['duid'] = $tmp_duid;
                if ($data[$f+1][0] == '"') {
                    $duid = "";
                    /* FIXME: This needs a safety belt to prevent an infinite loop */
                    while ($data[$f][strlen($data[$f])-1] != '"') {
                        $duid .= " " . $data[$f+1];
                        $f++;
                    }
                    $entry['duid'] = $duid;
                } else {
                    $entry['duid'] = $data[$f+1];
                }
                $entry['type'] = $dynamic_string;
                $f = $f+2;
                break;
```

, which would make the code more clean and less error prone. :)
That would mean lines 208 - 216 needs to be rewritten.

Eager to hear your comments on this!

#4 - 08/11/2017 12:52 PM - Renato Botelho

- Assignee set to Renato Botelho

#5 - 09/11/2017 03:58 PM - Renato Botelho

- Target version changed from 2.4.0 to 2.4.1

#6 - 10/08/2017 02:04 PM - Kill Bill

Am I the only one thinking that this absolutely unreadable regex madness needs to go to /dev/null and ISC DHCP server needs an API to show leases instead?

#7 - 10/08/2017 02:17 PM - Jim Pingle

I agree, but last I looked OMAPI didn't quite do everything we need, plus it required making a program in C to interface with it since there wasn't any PHP interface that we could find. That may have changed recently, but it'll need more investigation.

#8 - 10/08/2017 03:36 PM - Kill Bill

Jim Pingle wrote:

> I agree, but last I looked OMAPI didn't quite do everything we need. ... That may have changed recently, but it'll need more investigation.

After a quick search, afraid this is a waste of time as far as ISC DHCP is concerned, perhaps time to look into Kea instead.

http://isc-dhcp-users.2343191.n4.nabble.com/DHCPv6-omshell-OMAPI-tp2072p2078.html

#9 - 10/12/2017 09:51 AM - Jim Pingle

- Target version changed from 2.4.1 to 2.4.2

Moving target to 2.4.2 as we need 2.4.1 sooner than anticipated.

#10 - 10/23/2017 12:20 PM - Jim Pingle

- Target version changed from 2.4.2 to 2.4.3

#11 - 12/03/2017 03:06 PM - Anders Lind

I have made a patch that addresses the issue, but it is
also a rewrite of a large part of the status leases
page, that does the following:

- Proper handling of the lease file for
  getting leases, prefixes and the mapping (between
  the delegated network and the routed ip address.)
  Everything has been tested. Regarding the Pools/failover
  part: It has been deduced from looking at the source code
  and other ISC documentation and not from a live configured
  system, but some made up 'failover' lease content was
  used and tested on a live system. E.g. this was pasted
  into the dhcpv6 leases file:

```
failover peer "Failover-Pair-Name" state {
  my state recover-wait at 1 2017/03/03 20:20:12;
  partner state communications-interrupted at 1 2017/03/03 20:20:12;
  mclt 123;
}

failover peer "Failover-2GETHER" state {
  my state recover-done at 1 2017/03/03 21:24:12;
  partner state unknown-state at 1 2017/03/03 21:44:12;
  mclt 456;
}
```

  , but I welcome you to try verifying this on an actual
  'failover' configured system to see the result.
  (Feel free to upload/send me a lease file with
  content from a real 'failover' configured system.)
  Re. making proper retrieval of failover content I found the
  relevant places in source (more is mentioned in detail within the patch
  as well), but part of it can be seen here:
  https://source.isc.org/cgi-bin/gitweb.cgi?p=dhcp.git;a=blob;f=server/db.c
  int write_failover_state (dhcp_failover_state_t *state)
  and https://deepthought.isc.org/article/AA-00252/31/Putting-the-working-server-in-a-failover-pair-into-partner-down-state.html (although it lacks
  the time and MCLT info.)

- An IPv6 address matcher/parser that is used.
  It can be skipped if one trusts the lease content
  and that noone manually edits the lease file.

- Unit tests of the IPv6 matching/parsing.
  Run with: php -f parser_ipv6_tester.php

- A small debugging tool for testing lease file content
  both on a pfSense router machine (with live content
  from ndp) as well as offline (e.g. if you copy a lease
  file over to a desktop computer.)
  All in all made to make sure that the stuff works.
  Run with: php -f parser_dhcpv6_lease_tester.php

- Also there is a small correction to wake on lan
  on the status lease page that did not transfer
  the mac address to the Services - Wake-on-LAN - Edit page.

- Also this patch cleans up the code and verifies
  the content of the lease file to some extent.
  During the cleaning up I have found, by looking
  at the ISC source code, that these properties
  are not used at all in DHCPv6 land.
  They are only used by IPv4 DHCP:

```
starts
tstp
tsfp
atsfp
hardware
uid
client-hostname
next (binding state)
```

, because DHCPv6 server uses the method write_ia
https://source.isc.org/cgi-bin/gitweb.cgi?p=dhcp.git;a=blob;f=server/db.c (referred to in
https://source.isc.org/cgi-bin/gitweb.cgi?p=dhcp.git;a=blob;f=server/dhcpv6.c):
DHCPv6: int write_ia(const struct ia_xx *ia)
vs
DHCPv4: int write_lease (lease)
So therefore they are thrown away in this patch.

For now I would just like to ask for some feedback
e.g. do you like what you see
before I submit a pull request?

The files can be found here:
https://github.com/al-right/pfSense-dhcpv6-gui-leases-patch

Thanks

#12 - 12/16/2017 07:41 PM - Anders Lind

I have added a PR here: https://github.com/pfsense/pfsense/pull/3892
and updated https://forum.pfsense.org/index.php?topic=132791 , because
some people in the forum are willing to test.

Thanks

#13 - 01/15/2018 03:13 PM - Anders Lind

The PR has been updated with a second patch addressing the
requested changes and includes further amends e.g. visual changes.
Please see https://github.com/pfsense/pfsense/pull/3892

Thanks

#14 - 02/01/2018 12:02 PM - Anonymous

- Assignee changed from Renato Botelho to Anonymous

Re-assigned for testing

#15 - 02/07/2018 12:14 PM - Jim Pingle

PR looks good to me. I had a number of leases on my edge firewall that were not showing before, and now they all show up with this patch applied.
Before, it showed me 8 leases and 0 delegated. Now it shows 18 leases and 4 delegations, which matches what is in the leases file.

#16 - 02/22/2018 06:52 AM - Renato Botelho

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

PR has been merged

#17 - 03/02/2018 03:55 PM - Jim Pingle

- Status changed from Feedback to Resolved

Works fine now