

pfSense - Bug #5215

DHCP failover generates not working configuration.

09/30/2015 07:49 AM - Christopher Harbort

Status:	Rejected	Start date:	09/30/2015
Priority:	Low	Due date:	
Assignee:		% Done:	0%
Category:	DHCP (IPv4)	Estimated time:	0.00 hour
Target version:		Affected Version:	
Plus Target Version:		Affected Architecture:	
Release Notes:			
Description			
Using a CARP-Cluster of two nodes with DHCP Server in failover mode does not work, because the generated configuration is wrong. Setup: Node1: 172.23.136.131 Node2: 172.23.136.132 CARP: 172.23.136.130 Node2 is configuration master and the dhcpd settings got synchronized to Node1. As long as we do not use the "failover peer IP"-setting, both nodes just run the service without knowing each other. When we set the failover peer IP to Node1, both nodes hang in recover state. This is because the generated configuration(see attached files) for both nodes sets them to secondary and uses the wrong ports, so they can never reach the other node. I suggest following changes: Node1(secondary): failover peer "dhcp_opt6" { secondary; address 172.23.136.131; port 520; peer address 172.23.136.132; - peer port 519; + peer port 520; Node2(primary): failover peer "dhcp_opt6" { - secondary; + primary; + mclt 1800; + split 128; address 172.23.136.132; port 520; peer address 172.23.136.131; - peer port 519; + peer port 520; This fixed the issue on our systems.			

History

#1 - 09/30/2015 07:51 AM - Jim Pingle

- Status changed from New to Rejected

Configuration problem, please post on the forum for support assistance. I just set one up on 2.2.4 a day or two ago, it works fine when done correctly.

#2 - 09/30/2015 07:55 AM - Christopher Harbort

Hi Jim P,
please recheck this and do not reject it that fast. it just luck that sometimes the service report normal state, but they do not exchange lease information correctly, cause oft the ports.
we got version 2.2.4. if you read the generated configuration files, you will see the error with the peer and local port.
we reproduced this issue on multiple clusters.

#3 - 09/30/2015 07:57 AM - Jim Pingle

I did, and it works fine. You have a problem in your configuration if the DHCP configuration files are not correct as you have shown. Please discuss it in the forum before opening a ticket.

#4 - 09/30/2015 08:12 AM - Christopher Harbort

Ok, if you wish i will discuss the issue in the forum. But as you know the webui, there is no option to configure the ports and so the generated config is logically wrong and missing some needed options.(see also: <https://kb.isc.org/article/AA-00502/0/A-Basic-Guide-to-Configuring-DHCP-Failover.html>)

#5 - 09/30/2015 08:17 AM - Jim Pingle

Please leave the discussion for the forum.

When configured properly, it has a proper configuration:

Primary:

```
$ cat /var/dhcpd/etc/dhcpd.conf

option domain-name "dw.example.com";
option ldap-server code 95 = text;
option domain-search-list code 119 = text;
option arch code 93 = unsigned integer 16; # RFC4578

default-lease-time 7200;
max-lease-time 86400;
log-facility local7;
one-lease-per-client true;
deny duplicates;
ping-check true;
update-conflict-detection false;
authoritative;
failover peer "dhcp_lan" {
    primary;
    address 10.11.0.2;
    port 519;
    peer address 10.11.0.3;
    peer port 520;
    max-response-delay 10;
    max-unacked-updates 10;
    split 128;
    mclt 600;

    load balance max seconds 3;
}

subnet 10.11.0.0 netmask 255.255.255.0 {
    pool {
        option domain-name-servers 10.11.0.1;
        deny dynamic bootp clients;
        failover peer "dhcp_lan";
        range 10.11.0.11 10.11.0.245;
    }

    option routers 10.11.0.1;
    option domain-name-servers 10.11.0.1;
}
```

Secondary:

```
$ cat /var/dhcpd/etc/dhcpd.conf

option domain-name "dw.example.com";
```

```
option ldap-server code 95 = text;
option domain-search-list code 119 = text;
option arch code 93 = unsigned integer 16; # RFC4578

default-lease-time 7200;
max-lease-time 86400;
log-facility local7;
one-lease-per-client true;
deny duplicates;
ping-check true;
update-conflict-detection false;
authoritative;
failover peer "dhcp_lan" {
    secondary;
    address 10.11.0.3;
    port 520;
    peer address 10.11.0.2;
    peer port 519;
    max-response-delay 10;
    max-unacked-updates 10;

    load balance max seconds 3;
}

subnet 10.11.0.0 netmask 255.255.255.0 {
    pool {
        option domain-name-servers 10.11.0.1;
        deny dynamic bootp clients;
        failover peer "dhcp_lan";
        range 10.11.0.11 10.11.0.245;
    }

    option routers 10.11.0.1;
    option domain-name-servers 10.11.0.1;
}
```

Primary:
7gstfck.jpg

Secondary:
E2XiZwY.jpg

If yours does not match the above, you have a configuration problem, which can be discussed on the forum.

#6 - 09/30/2015 08:20 AM - Jim Pingle

- Affected Version deleted (2.2.4)

Files			
dhcpd-node1.conf	908 Bytes	09/30/2015	Christopher Harbort
dhcpd-node2.conf	908 Bytes	09/30/2015	Christopher Harbort