

Foreman - Support #4435

only able to create PTR records in Foreman (dns is set in Domains)

02/24/2014 11:39 PM - TJ Walker

Status: Resolved	
Priority: Normal	
Assignee:	
Category:	
Target version:	
Triaged:	Found in Releases:
Fixed in Releases:	
Description	
HOSTNAME: puppet01.oadr OS: redhat RELEASE: CentOS release 6.4 (Final) FOREMAN: 1.3.1 RUBY: ruby 1.8.7 (2011-06-30 patchlevel 352) [x86_64-linux] PUPPET: 3.3.2	
<p>I have DNS running on a separate server and foreman can create PTR records but when I update domains to point to the DNS server I get the following error updating/adding hosts:</p> <pre>Net::Error execution expired lib/net/dns.rb:36:in `rescue in lookup' lib/net/dns.rb:15:in `lookup' lib/net/dns.rb:61:in `dns_lookup' lib/net/dns/a_record.rb:28:in `conflicts' lib/net.rb:27:in `conflicting?' app/models/concerns/orchestration/dns.rb:121:in `dns_conflict_detected?' app/models/concerns/orchestration.rb:47:in `valid?' app/models/concerns/foreman/sti.rb:29:in `save_with_type' app/controllers/hosts_controller.rb:85:in `create' app/models/concerns/foreman/thread_session.rb:33:in `clear_thread'</pre>	
<p>if I change the resolv.conf on the foreman server to the IP of the foreman server (it was set to the IP of the DNS server) I don't get the error but foreman also doesn't update the DNS (A or PTR).</p>	
<p>I can manually add records using the nsupdate command and using curl to pass through the foreman server (curl -i -d "fqdn=www02.oadr&value=10.199.200.13&type=A" http://10.199.202.64:8443/dns/).</p>	
<p>also none of the records exist in DNS (nslookup returns nothing from the DNS server)</p>	

History

#1 - 02/25/2014 08:41 AM - Dominic Cleal

- *Tracker changed from Bug to Support*
- *Status changed from New to Feedback*

A timeout is usually symptomatic of Foreman being unable to access one of your authoritative nameservers, assuming you still have query_local_nameservers set to the default of false. In particular, check your SOA for the zone being managed and that the Foreman host can query (e.g. with dig) the master listed in the SOA and others specified by NS records.

#2 - 02/25/2014 06:37 PM - TJ Walker

Here is the response of dig on the foreman host:

```
[root@puppet01 ~]# cat /etc/resolv.conf
search oadr
nameserver 10.199.202.64
[root@puppet01 ~]# dig oadr
```

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6 <<>> oadr
;; global options: +cmd
```

```
:: Got answer:
:: >>HEADER<< opcode: QUERY, status: NOERROR, id: 26121
:: flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

```
:: QUESTION SECTION:
;oadr.                IN      A
```

```
:: AUTHORITY SECTION:
oadr.                 3600 IN      SOA     ns01.oadr. root.oadr. 4 86400 3600 604800 3600
```

```
:: Query time: 1 msec
:: SERVER: 10.199.202.64#53(10.199.202.64)
:: WHEN: Tue Feb 25 13:25:16 2014
:: MSG SIZE rcvd: 68
```

I changed query_local_nameservers to true and still get the same error. If I remove the DNS server from More>Domains>oadr but keep it in Subnets then I can create a new host and in the foreman-proxy proxy.log I can see foreman issuing the command to create the PTR record:

```
D, [2014-02-25T18:28:19.208902 #5733] DEBUG -- : running /usr/bin/nsupdate k/etc/rndc.key
D, [2014-02-25T18:28:19.212599 #5733] DEBUG -- : nsupdate: executed - server 10.199.202.64
D, [2014-02-25T18:28:19.219492 #5733] DEBUG -- : nsupdate: executed - update add 22.200.199.10.in-addr.arpa. 86400 IN PTR test.oadr
```

db.oadr located in /var/named/dynamic/ has the same file permissions as the PTR zones:

```
rw-r--r. 1 named named 356 Feb 24 23:06 db.200.199.10.in-addr.arpa
rw-r--r. 1 named named 2106 Feb 25 18:28 db.200.199.10.in-addr.arpa.jnl
rw-r--r. 1 named named 336 Feb 24 21:47 db.202.199.10.in-addr.arpa
rw-r--r. 1 named named 777 Jan 23 12:57 db.202.199.10.in-addr.arpa.jnl
rw-r--r. 1 named named 542 Feb 24 22:12 db.204.199.10.in-addr.arpa
rw-r--r. 1 named named 542 Feb 24 22:13 db.206.199.10.in-addr.arpa
rw-r--r. 1 named named 1060 Feb 24 23:10 db.oadr
rw-r--r. 1 named named 1017 Feb 24 22:54 db.oadr.jnl
```

Here is the content of the zone file:

```
$TTL 10800
@ IN SOA ns01.oadr. root.oadr. (
1 ;Serial
86400 ;Refresh
3600 ;Retry
604800 ;Expire
3600 ;Negative caching TTL
)
```

```
@ IN NS ns01.oadr.
```

```
ns01.oadr. IN A 10.199.202.64
```

thanks for your help.

#3 - 02/25/2014 09:18 PM - TJ Walker

I found the problem. I needed to chown named:named /var/named/chroot/etc/* (it was owned by root)

One last question I have some hosts that were created while this was broken, can I use hammer to update DNS for hosts that are missing in DNS?

#4 - 02/26/2014 09:03 AM - Dominic Cleal

- Status changed from Feedback to Resolved

Ah interesting, glad you found it.

You can't trigger this at the moment unfortunately (#2799 + related bugs), but there's a thread with some nice code (in the fifth post) on foreman-users that can recreate DNS records via the proxy server:

<https://groups.google.com/forum/#!topic/foreman-users/86fEMd7sico>