

[Home](#)[Linux](#)[Windows](#)[Security](#)[Exam Guides](#)[Archives](#)[About](#)[Contact](#)

RootUsers

Guides, tutorials, reviews and news for System Administrators.

How To Configure Local DNS Query Cache In Linux With Dnsmasq

Posted by Jarrod on February 24, 2016

[Go to comments](#)[Leave a comment \(2\)](#)

In many Linux based distributions there does not appear to be any local DNS query caching performed by default on the client side like there is in Windows. This means that if a process on the system constantly needs to connect to some domain name it will perform a DNS lookup against the resolver defined to retrieve the IP every single time.

In this particular example instance there is a process that performs 30,000,000 DNS requests per day on average against the nameserver, we are going to significantly reduce this by configuring a local DNS cache on the server performing the excessive DNS queries.

Currently this Linux server is performing so many DNS queries that the DNS query log on the nameserver is hitting the default 20,000 messages within 10 minutes rsyslog rate limit ([see here on changing the rsyslog limit](#)) in less than a minute, resulting in logs being dropped and not recorded. Rather than increase the rate limits on the logging and use more system resources, I've checked the queries that are actually being logged and almost all of them are for the same domains over and over again. This means that implementing a local DNS query cache should be effective here.

Enable Dnsmasq

Dnsmasq can be used for many things, in this instance we're only making use of its local query caching functions. Note that the upstream nameserver will need to have recursive queries enabled for dnsmasq to correctly cache the records.

Rather than directly enabling the service and modifying the configuration file, here we're going to simply enable the plugin for Network Manager. Note that these tests are in CentOS 7 where the dnsmasq package was already installed, if you do not have this package install it now via yum.

To enable dnsmask in Network Manager, we need to edit the /etc/NetworkManager/NetworkManager.conf file and add the following configuration under the [main] section.

```
[main]
dns=dnsmasq
```

In order to apply this change we next need to restart Network Manager, which can be done with the command below, noting that this is case sensitive.

```
systemctl restart NetworkManager
```

That's it, we can now confirm that this has worked as expected by checking the `/etc/resolv.conf` file which should be specifying "nameserver 127.0.0.1" meaning that the Linux system will send DNS requests to itself.

Sure enough if we check, localhost should now be listening for DNS queries on port 53.

```
[root@centos7 ~]# netstat -antup | grep dnsmasq
tcp        0      0 127.0.0.1:53          0.0.0.0:*             LISTEN      31618
udp        0      0 127.0.0.1:53          0.0.0.0:*             31618
```

Next if we take a look in the `/var/run/NetworkManager/dnsmasq.conf` file we should see the IP address of the nameserver that was originally specified within `/etc/resolv.conf`.

```
[root@centos7 ~]# cat /var/run/NetworkManager/dnsmasq.conf
server=192.168.1.1
```

So all DNS requests first go through the instance of dnsmasq running on localhost, if the response is not in the cache then the request will be forwarded to the defined nameserver and then placed into the cache.

By default the most recent 150 DNS queries are cached in memory. The size of the cache can be modified by creating the `/etc/NetworkManager/dnsmasq.d/cache` as shown below.

```
[root@centos7 ~]# cat /etc/NetworkManager/dnsmasq.d/cache
cache-size=5000
```

This configuration allows for up to 5000 entries to be stored in the cache at once, to apply the change the NetworkManager service will need to be restarted again. Entries should be cached based on the TTL defined on the record.

There are plenty of other values that can be defined within files in the `/etc/NetworkManager/dnsmasq.d/` directory, to view these run the below command to open the manual page.

```
man 8 dnsmasq
```

Viewing Cache Statistics

Now that we have dnsmasq running via Network Manager, we want to get an idea of the amount of cache hits to determine if our cache is actually helping at all.

```
killall -sUSR1 dnsmasq
```

This will dump the current statistics to the /var/log/messages or /var/log/syslog file, depending on your operating system / configuration. We can then search the log file for 'dnsmasq' as shown below.

```
[root@centos7 ~]# grep dnsmasq /var/log/messages
Jan  8 05:29:40 centos7 dnsmasq[32618]: time 1452230980
Jan  8 05:29:40 centos7 dnsmasq[32618]: cache size 5000, 0/62 cache insertions re-use
Jan  8 05:29:40 centos7 dnsmasq[32618]: queries forwarded 64, queries answered locally
Jan  8 05:29:40 centos7 dnsmasq[32618]: server 192.168.72.1#53: queries sent 64, retr
```

In this example 148,924,680 DNS queries have been answered by the local dnsmasq cache, and just 64 queries were sent externally to the defined nameserver. I performed a dig on a random domain name that the server should not have had any reason to be accessing and confirmed that the queries forwarded externally increased by 1 to 65 as expected, indicating that the statistics were correctly working.

Summary

By simply enabling the dnsmasq plugin through NetworkManager in Linux, we have successfully enabled local DNS query caching which will increase performance for records that will be constantly looked up, as they will now be available on the local system rather than on an external nameserver.

Share this:



How To, Linux

DNS, Linux

[← How To Provide NFS Shares For Group Collaboration](#)

[How To Configure An iSCSI Target And Initiator In Linux](#) →

[Leave a comment ?](#)

2 Comments.

Gilbert Standen November 18, 2016 at 1:29 am

Reply

Hi Jarrod, Thanks for this great post. I did all the steps you posted, but dnsmasq is not listening on 127.0.0.1 and /etc/resolv.conf is not being updated. Oracle Linux 7.2.

Jarrod November 21, 2016 at 6:59 pm

Reply

I'm not too sure on that, while I've never specifically used Oracle Linux 7.2 myself I understand that it's another RHEL derivative like CentOS so I would think that the

steps here should also apply unless Oracle are doing something special in this area.

Leave a Comment

NOTE - You can use these HTML tags and attributes:

 <abbr title=""> <acronym title=""> <blockquote
cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike>

 NAME EMAIL Website URL

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

Subscribe

Receive new post notifications by email for free!
Unsubscribe any time.

 Email Address

Recent Posts

[How To Setup A LAMP Web Server With CentOS 7 Linux](#)
[Configure Storage Reports in Windows Server 2016](#)
[BSides Canberra 2017 CTF – Rekt Exfil Write-up](#)
[Configure File Screens for File Server Resource Manager \(FSRM\)](#)
[Where Is The Apache Configuration File In CentOS?](#)

Recent Comments

[Moritz](#) on [How To Install Cinnamon GUI In CentOS 7 Linux](#)
[Ørjan Nilsen](#) on [How To Fix MariaDB 10.0.29 SELinux Update Failure](#)
[Jarrod](#) on [How To Join CentOS Linux To An Active Directory Domain](#)
[Gaby](#) on [How To Join CentOS Linux To An Active Directory Domain](#)
[G123](#) on [How to Increase the size of a Linux LVM by adding a new disk](#)

Categories

[Command Examples](#)
[Exam Guides](#)
[How To](#)
[Linux](#)
[Security](#)
[Technology](#)
[Uncategorized](#)
[Windows](#)
[XenServer](#)



