10 Linux nslookup Command Examples for DNS Lookup

nslookup is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.

It is also used to troubleshoot DNS related problems. This article provides few examples on using the nslookup command.

nslookup can operate on both “Interactive mode” and “Non-Interactive mode”. Interactive mode allows the user to query the DNS-Server about various host, and domains. Non-Interactive mode allows the user to query the information for a host or domain. In this article, all the commands explained are “Non-Interactive mode”.

1. nslookup – Simple Example

nslookup followed by the domain name will display the “A Record” (IP Address) of the domain.

```
$ nslookup redhat.com

Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
Name:   redhat.com
Address: 209.132.183.181
```

In the above output, server refers to the IP address of the DNS server. Then the below section provides the “A Record” (IP Address) of the domain “redhat.com”.

2. Query the MX Record using -query=mx

MX (Mail Exchange) record maps a domain name to a list of mail exchange servers for that domain. The MX record tells that all the mails sent to “@redhat.com” should be routed to the Mail server in that domain.

```
$ nslookup -query=mx redhat.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
redhat.com      mail exchanger = 10 mx2.redhat.com.
redhat.com      mail exchanger = 5 mx1.redhat.com.

Authoritative answers can be found from:
mx2.redhat.com  internet address = 66.187.233.33
mx1.redhat.com  internet address = 209.132.183.28
```

In the above example, we have 2 MX records for the domain “redhat.com”. The number (5, 10), associated with the MX records tells the preference of mail server. Lower the number, higher the preference. So when a mail is sent to “@redhat.com”, first preference will be “mx1.redhat.com”, then “mx2.redhat.com”.

Authoritative Answer vs Non-Authoritative Answer

You may also noticed the keyword “Authoritative Answer” and “Non-Authoritative Answer” in the above output.

Any answer that originates from the DNS Server which has the complete zone file information available for the domain is said to be authoritative answer.

In many cases, DNS servers will not have the complete zone file information available for a given domain. Instead, it maintains a cache file which has the results of all queries performed in the past for which it has gotten authoritative response. When a DNS query is given, it searches the cache file, and return the information available as “Non-Authoritative Answer”.

3. Query the NS Record using -query=ns

NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain. It will output the name serves which are associated with the given domain.

```
nslookup -type=ns redhat.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
redhat.com      nameserver = ns4.redhat.com.
redhat.com      nameserver = ns2.redhat.com.
redhat.com      nameserver = ns1.redhat.com.
redhat.com      nameserver = ns3.redhat.com.

Authoritative answers can be found from:
ns4.redhat.com  internet address = 209.132.188.218
ns2.redhat.com  internet address = 209.132.183.2
ns1.redhat.com  internet address = 209.132.186.218
ns3.redhat.com  internet address = 209.132.176.100
```

4. Query the SOA Record using -query=soa

SOA record (start of authority), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc…

```
$ nslookup -type=soa redhat.com
Server:         192.168.19.2
```

```
Address:        192.168.19.2#53

Non-authoritative answer:
redhat.com
        origin = ns1.redhat.com
        mail addr = noc.redhat.com
        serial = 2012071601
        refresh = 300
        retry = 180
        expire = 604800
        minimum = 14400

Authoritative answers can be found from:
ns1.redhat.com  internet address = 209.132.186.218
```

- mail addr – specifies the mail address of the domain admin (noc@redhat.com)
- serial – sort of revision numbering system. The standard convention is to use "YYYYMMYYNN" format. (2012-07-16. 01 will be incremented, if more than one edit has taken place on a same day)
- refresh – specifies (in seconds), when the secondary DNS will poll the primary to see if the serial number has been increased. If increased, secondary will make a new request to copy the new zone file.
- retry – specifies the interval to re-connect with the Primary DNS
- expire – specifies the time that the secondary DNS will keep the cached zone file as valid
- minimum – specifies the time that the secondary DNS should cache the zone file

5. View available DNS records using -query=any

We can also view all the available DNS records using -query=any option.

```
$ nslookup -type=any google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
Name:   google.com
Address: 173.194.35.7
Name:   google.com
Address: 173.194.35.8

google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 2012071701
        refresh = 7200
        retry = 1800
        expire = 1209600
        minimum = 300
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
```

```
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx-v4v6.l.google.com.
google.com      has AAAA address 2a00:1450:4002:801::1004

Authoritative answers can be found from:
ns4.google.com internet address = 216.239.38.10
ns3.google.com internet address = 216.239.36.10
```

6. Reverse DNS lookup

You can also do the reverse DNS look-up by providing the IP Address as argument to nslookup.

```
$ nslookup 209.132.183.181
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
181.183.132.209.in-addr.arpa   name = origin-www2.redhat.com.
```

7. Using Specific DNS server

Instead of using default DNS server's for querying, you can also specify a particular name server to resolve the domain name.

```
$ nslookup redhat.com ns1.redhat.com

Server:         209.132.186.218
Address:        209.132.186.218#53

Name:   redhat.com
Address: 209.132.183.181
```

In the above command, we have used the ns1.redhat.com as the DNS server. Here you may notice that, we don't get any "Non-authoritative answer:" header, since ns1.redhat.com has all the zone information of redhat.com

8. Change the port number to connect with

By default DNS servers uses the port number 53. If for any reasons, the port number got changed, then we can specify the port number using -port option

```
$ nslookup -port 56 redhat.com
```

9. Change timeout interval to wait for a reply

You can change the default timeout to wait for a reply using -timeout option.

```
$ nslookup -timeout=10 redhat.com
```

10. Enabling debug mode using -debug

You can turn on/off the debugging using -debug option in the command line

```
$ nslookup -debug redhat.com
Server:         192.168.19.2
Address:        192.168.19.2#53

------------
    QUESTIONS:
        redhat.com, type = A, class = IN
    ANSWERS:
    ->  redhat.com
        internet address = 209.132.183.181
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   redhat.com
Address: 209.132.183.181
```