sanfoundry.com

5 "nslookup" Command Usage Examples in Linux

by linuxcmd2

7-9 minutes

This tutorial explains Linux “nslookup” command, options and its usage with examples.

nslookup – query Internet name servers interactively

DESCRIPTION

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”.

Authoritative Answer vs Non-Authoritative Answer

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”.

SYNOPSIS

nslookup [– option] … host [server]

OPTIONS

all
List the current settings

d2
Set exhaustive debug mode on

nod2
Set exhaustive debug mode off

debug
Set debug mode on

nodebug
Set debug mode off

defname
Set domain-appending mode on

nodefname
Set domain-appending mode off

domain=string

Establish the appendable domain

ignoretc

Set it to ignore packet truncation errors

noignoretc

Set it to acknowledge packet truncation errors

host

Inquires about the specified host. In this non-interactive command format, nslookup Does not prompt for additional commands.

–

Causes nslookup to prompt for more information, such as host names, before sending one or more queries.

server

Directs inquiries to the name server specified here in the command line rather than the one read from the /etc/resolv.conf file. server can be either a name or an Internet address. If the specified host cannot be reached, nslookup resorts to using the name server specified in /etc/resolv.conf.

EXAMPLES

1. Simple Example

Looking up google.com

```
$ nslookup google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   google.com
```

```
Address: 74.125.200.138
Name:   google.com
Address: 74.125.200.113
Name:   google.com
Address: 74.125.200.102
Name:   google.com
Address: 74.125.200.100
Name:   google.com
Address: 74.125.200.101
Name:   google.com
Address: 74.125.200.139
```

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.

```
$ nslookup -query=mx google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
google.com      mail exchanger = 10
aspmx.l.google.com.
google.com      mail exchanger = 50
alt4.aspmx.l.google.com.
google.com      mail exchanger = 40
alt3.aspmx.l.google.com.
google.com      mail exchanger = 30
alt2.aspmx.l.google.com.
google.com      mail exchanger = 20
alt1.aspmx.l.google.com.
```

```
Authoritative answers can be found from:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
alt2.aspmx.l.google.com internet address =
74.125.137.27
alt1.aspmx.l.google.com internet address =
74.125.142.26
aspmx.l.google.com      internet address =
74.125.129.27
alt4.aspmx.l.google.com internet address =
173.194.75.27
alt3.aspmx.l.google.com internet address =
173.194.68.26
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  internet address = 216.239.32.10
```

3. View available DNS records using -query=any

Using -query=any, we can get all records

```
$ nslookup -query=any google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
```

```
        mail addr = dns-admin.google.com
        serial = 2013121300
        refresh = 7200
        retry = 1800
        expire = 1209600
        minimum = 300
google.com      mail exchanger = 10
aspmx.l.google.com.
google.com      mail exchanger = 40
alt3.aspmx.l.google.com.
google.com      mail exchanger = 30
alt2.aspmx.l.google.com.
google.com      mail exchanger = 50
alt4.aspmx.l.google.com.
google.com      mail exchanger = 20
alt1.aspmx.l.google.com.
google.com      has AAAA address
2404:6800:4003:c00::65
Name:   google.com
Address: 74.125.200.139
Name:   google.com
Address: 74.125.200.102
Name:   google.com
Address: 74.125.200.138
Name:   google.com
Address: 74.125.200.113
Name:   google.com
Address: 74.125.200.100
Name:   google.com
Address: 74.125.200.101
```

```
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
alt3.aspmx.l.google.com internet address =
173.194.68.27
alt2.aspmx.l.google.com internet address =
74.125.137.26
alt4.aspmx.l.google.com internet address =
173.194.75.27
alt1.aspmx.l.google.com internet address =
74.125.142.26
```

4. Reverse DNS lookup

Looking up IP address to get the domainname.

```
$ nslookup 173.194.68.27
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
27.68.194.173.in-addr.arpa      name = qa-in-
f27.1e100.net.

Authoritative answers can be found from:
```

```
194.173.in-addr.arpa    nameserver =
NS2.GOOGLE.COM.
194.173.in-addr.arpa    nameserver =
NS4.GOOGLE.COM.
194.173.in-addr.arpa    nameserver =
NS3.GOOGLE.COM.
194.173.in-addr.arpa    nameserver =
NS1.GOOGLE.COM.
NS3.GOOGLE.COM  internet address = 216.239.36.10
NS4.GOOGLE.COM  internet address = 216.239.38.10
NS2.GOOGLE.COM  internet address = 216.239.34.10
NS1.GOOGLE.COM  internet address = 216.239.32.10
```

5. Using Specific DNS server

In the following wxample ns1.google.com is the specific name server which is being looked up.

```
$ nslookup google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.com
Address: 173.194.36.0
Name:   google.com
Address: 173.194.36.5
Name:   google.com
Address: 173.194.36.7
Name:   google.com
Address: 173.194.36.9
Name:   google.com
Address: 173.194.36.2
```

```
Name:   google.com
Address: 173.194.36.1
Name:   google.com
Address: 173.194.36.8
Name:   google.com
Address: 173.194.36.14
Name:   google.com
Address: 173.194.36.3
Name:   google.com
Address: 173.194.36.4
Name:   google.com
Address: 173.194.36.6
```

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

Sanfoundry Global Education & Learning Series – 1000 Linux Tutorials.