Áskálva egy kicst a DIG-gel

PCLinuxOS Magazine – 2014. július

Írta: Professor Tux J. Penguin

9 parancs a DNS lekérdezésére DIG-gel

A **Dig** a **Domain Information Groper** (**gazdanév információ letapogató**) rövidítése. Ez egy hálózati admin parancssori eszköz, DNS-szerverek lekérdezésére. Hasznos **DNS**-problémák ellenőrzésére és hibakeresésre, de **DNS** keresés is végezhető vele, és a lekérdezett névkiszolgáló válaszát megjeleníti. A DIG a BING domain name server szoftvercsomag része. A DIG parancs az olyan régebbi parancsokat váltja le, mint az nslookup. A DIG a nagyobb Linux disztribúciókban elérhető.

1. Domén (gazdanév) lekérdezése “A” record

```
[youcantoo@localhost ~]$ dig yahoo.com

; <<>> DiG 9.9.3-P2 <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43271
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com. IN A

;; ANSWER SECTION:
yahoo.com. 1342 IN A 98.139.183.24
yahoo.com. 1342 IN A 206.190.36.45
yahoo.com. 1342 IN A 98.138.253.109
;; Query time: 27 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Mon Jun 16 15:20:59 PDT 2014
;; MSG SIZE rcvd: 86
```

Az előbbi parancs hatására a dig megnézi az „**A**” record-ot, a **yahoo.com**-ot keresve. A dig parancs elolvassa az **/etc/resolv.conf** fájlt és lekérdezi az ott található **DNS** szervereket. A dig a **DNS**-szerver válaszát jeleníti meg.

Most értelmezzük a parancs kimenetét:

1. a ;-vel kezdődő sorok a megjegyzések és nem részei az információnak;

2. az első sor megadja a dig parancs verziószámát (**9.8.2**);

3. a következő a **DNS**-szervertől kapott válasz fejlécét mutatja;

4. ezt követi a kérdező rész, ami egyszerűen közli velünk a kérdést, ami ez esetben egy, a **yahoo.com** „**A**” record-jára vonatkozik. Az **IN** jelenti, hogy ez egy Internet-keresés (az Internet osztályban);

5. a válasz rész azt mondja nekünk, hogy a **yahoo.com** a **98.139.183.24**-es **IP**-címmel rendelkezik;

6. végül néhány statisztika a kereséssel kapcsolatban. A statisztika kikapcsolható a **+nostats** opcióval.

2. Gazdanév-lekérdezés “A” record +short-tal

Alapbeállításban a dig elég bőbeszédű. Egyik módszer a kimenet korlátozására a +short opció használata. Ez drasztikusan levágja a kimenetet, ahogy az a következőkben látható.

```
[youcantoo@localhost ~]$ dig yahoo.com +short
206.190.36.45
98.139.183.24
98.138.253.109
```

3. MX (Mail eXchange rövidítése) record lelárdezése doménre

Csak különféle DNS forrás rekordok típusainak lekérdezésére.

```
[youcantoo@localhost ~]$ dig yahoo.com MX
; <<>> DiG 9.9.3-P2 <<>> yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58791
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com. IN MX
;; ANSWER SECTION:
yahoo.com. 1080 IN MX 1 mta5.am0.yahoodns.net.
yahoo.com. 1080 IN MX 1 mta6.am0.yahoodns.net.
yahoo.com. 1080 IN MX 1 mta7.am0.yahoodns.net.
```

4. SOA (Service of authority rövidítése) record lekérdezése doménre

```
[youcantoo@localhost ~]$ dig yahoo.com soa

; <<>> DiG 9.9.3-P2 <<>> yahoo.com soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49302
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com. IN SOA

;; ANSWER SECTION:
yahoo.com. 595 IN SOA
ns1.yahoo.com. hostmaster.yahoo-inc.com. 2014061609 3600 300
1814400 600
```

5. TTL (Time To Live rövidítése)record lekérdezése doménre

```
[youcantoo@localhost ~]$ dig yahoo.com ttl

; <<>> DiG 9.9.3-P2 <<>> yahoo.com ttl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26925
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com. IN A

;; ANSWER SECTION:
yahoo.com. 1342 IN A 206.190.36.45
yahoo.com. 1342 IN A 98.139.183.24
yahoo.com. 1342 IN A 98.138.253.109
```

6. Csak a válasz szekció (answer section) lekérdezése

```
[youcantoo@localhost ~]$ dig yahoo.com +nocomments
+noquestion +noauthority
+noadditional +nostats

; <<>> DiG 9.9.3-P2 <<>> yahoo.com +nocomments +noquestion
+noauthority +noadditional +nostats
;; global options: +cmd
yahoo.com. 1237 IN A 98.138.253.109
yahoo.com. 1237 IN A 206.190.36.45
yahoo.com. 1237 IN A 98.139.183.24
```

7. Az összes DNS record típus lekérdezése

```
[youcantoo@localhost ~]$ dig yahoo.com ANY +noall +answer

; <<>> DiG 9.9.3-P2 <<>> yahoo.com ANY +noall +answer
;; global options: +cmd
yahoo.com. 1164 IN A 206.190.36.45
yahoo.com. 1164 IN A 98.139.183.24
yahoo.com. 1164 IN A 98.138.253.109
yahoo.com. 690 IN MX 1 mta5.am0.yahoodns.net.
yahoo.com. 690 IN MX 1 mta6.am0.yahoodns.net.
yahoo.com. 690 IN MX 1 mta7.am0.yahoodns.net.
yahoo.com. 172689 IN NS ns5.yahoo.com.
yahoo.com. 172689 IN NS ns1.yahoo.com.
yahoo.com. 172689 IN NS ns6.yahoo.com.
yahoo.com. 172689 IN NS ns2.yahoo.com.
yahoo.com. 172689 IN NS ns3.yahoo.com.
yahoo.com. 172689 IN NS ns4.yahoo.com.
yahoo.com. 558 IN SOA ns1.yahoo.com.
hostmaster.yahoo-inc.com. 2014061609 3600 300 1814400 600
```

8. DNS-tartalék keresése

```
DNS Reverse Lookup lekérdezés. Csak a +short-tal kapott
válasz megjelenítése.

[youcantoo@localhost ~]$ dig -x 98.139.183.24 +short
ir2.fp.vip.bf1.yahoo.com.
```

9. Többszörös DNS Records lekérdezés.

Többszörös weblap DNS lekérdezés, pontosabban **MX**, **NS** (nameserver rövidítése) stb. rekordokra.

```
[youcantoo@localhost ~]$ dig yahoo.com mx +noall +answer redhat.com ns
+noall +answer

; <<>> DiG 9.9.3-P2 <<>> yahoo.com mx +noall +answer redhat.com ns
+noall
+answer
;; global options: +cmd
yahoo.com. 332 IN MX 1 mta7.am0.yahoodns.net.
yahoo.com. 332 IN MX 1 mta5.am0.yahoodns.net.
yahoo.com. 332 IN MX 1 mta6.am0.yahoodns.net.
redhat.com. 467 IN NS ns4.redhat.com.
redhat.com. 467 IN NS ns2.redhat.com.
redhat.com. 467 IN NS ns3.redhat.com.
redhat.com. 467 IN NS ns1.redhat.com.
```

Donate To PCLinuxOS

Community Supported.
No Billionaires/Millionaires.
No Corporate Backing Or Funding.

Click here to make a one-time donation through Google Checkout.

Or, click one of the amounts down below to make a monthly, recurring donation.