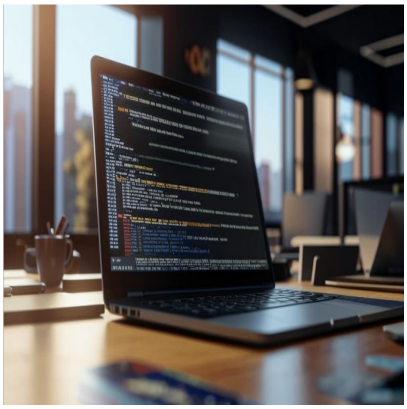

4 важных примера команд Dig, которые необходимо знать сисадмину или разработчику

Описание

Как системный администратор, все выглядит красиво только до тех пор, пока это не так. В такие кризисные моменты эти команды dig пригодятся. Следите за новостями. Системные администраторы всегда выполняют чертовски сложную работу. Даже самое элементарное требование к сисадмину – быть на связи 24 часа в сутки 7 дней в неделю – я ценю безгранично. Но мы здесь не для того, чтобы изучать их профессиональные характеристики; вместо этого проверьте, какое оружие они выбрали для устранения проблем с DNS.

Что такое команды Dig?

Сокращенно от Domain Information Groper, команды Dig – это один из самых быстрых методов опроса DNS-серверов на предмет того, что работает, а что нет. Вы можете проверить IP-адрес сервера, серверы имен, почтовый обмен, запрос TTL и т.д. с помощью легко запоминающихся текстов. Прежде чем приступить к рассмотрению нескольких основных команд dig, проверьте, установлены ли у вас утилиты dig:

```
$ dig -v
```

В результате должен быть получен результат, указывающий на версию dig, как показано ниже:

```
DiG 9.18.1-1ubuntu1-Ubuntu
```

Если вы не получили аналогичного ответа, значит, сначала нужно установить

утилиты Dig. Для тех, кто использует Ubuntu и Debian, введите:

```
$ sudo apt-get install dnsutils
```

И используйте:

```
$ sudo yum install bind-utils
```

...если вы работаете на CentOS или RHEL. Затем запустите `dig -v`, чтобы убедиться, что установка прошла гладко. Наконец, перейдите к следующим разделам, чтобы ознакомиться с несколькими командами Dig, которые помогут вам как системному администратору.

Проверьте IP-адрес

Это один из самых простых способов, когда мы проверяем IP-адрес сервера, лежащий в основе доменного имени.

`dig notissimus.com` – это та итерация, с которой мы начнем.

```
$ dig notissimus.com

; <<>> DiG 9.18.1-1ubuntu1-Ubuntu <<>> notissimus.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38635
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;geekflare.com.   IN A

;; ANSWER SECTION:
geekflare.com.  67 IN A 172.66.43.163
geekflare.com.  67 IN A 172.66.40.93

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 09 04:29:58 UTC 2022
```

Первое, что важно, – это ??????: `NOERROR` в разделе ” **Получили ответ** ” в верхней части. Это говорит о том, что все прошло успешно и без каких-либо проблем. Но информация, ради которой мы сделали этот запрос, – это IP-адрес сервера. Он указан в **разделе Answer** 172.66.40.93 (основной сервер) и 172.66.43.163 (отказоустойчивый). Кроме того, в **разделе “Вопрос**” находится ваш

первоначальный запрос. В последнем разделе приведены некоторые статистические данные о запросе. Но это очень много информации, которая не всегда нужна. Следовательно, вы можете получить более чистый ответ на этот запрос, введя:

```
$ dig notissimus.com +noall +answer notissimus.com. 53 IN A 172.66.43.163 geek
```

Здесь мы отрицаем все с помощью **+noall**, разрешая ожидаемый ответ с помощью **+answer**. Можно получить еще более краткий ответ, используя:

```
$ dig notissimus.com +short 172.66.43.163 172.66.40.93
```

Это был основной запрос, возвращающий запись **DNS A**; давайте посмотрим еще несколько.

Поиск определенных записей DNS

Серверы имен, авторитетный DNS-сервер для домена, можно найти по переменной ns.

```
$ dig notissimus.com ns +short olga.ns.notissimus.com. todd.ns.notissimus.com.
```

Аналогично, переменная mx отвечает на запросы почтовых серверов с указанием их приоритетов.

```
$ dig geekflare.com mx +noall +answer
geekflare.com.  300 IN MX 1 aspmx.l.google.com.
geekflare.com.  300 IN MX 10 alt3.aspmx.l.google.com.
geekflare.com.  300 IN MX 10 alt4.aspmx.l.google.com.
geekflare.com.  300 IN MX 5 alt1.aspmx.l.google.com.
geekflare.com.  300 IN MX 5 alt2.aspmx.l.google.com.
```

Аналогично, txt, aaaa, cname и т. д. можно использовать в качестве переменных команды dig для возврата различных записей DNS.

Трассировка DNS

Как видно из заголовка, Trace DNS проверяет путь от корневых серверов имен, авторитетных серверов имен, до IP-адреса домена.

```
$ dig geekflare.com +trace
```

```
; <<>> DiG 9.18.1-1ubuntu1-Ubuntu <<>> geekflare.com +trace
;; global options: +cmd
.   322660 IN NS a.root-servers.net.
```

```
.   322660 IN NS b.root-servers.net.
.   322660 IN NS c.root-servers.net.
.   322660 IN NS d.root-servers.net.
.   322660 IN NS e.root-servers.net.
.   322660 IN NS f.root-servers.net.
.   322660 IN NS g.root-servers.net.
.   322660 IN NS h.root-servers.net.
.   322660 IN NS i.root-servers.net.
.   322660 IN NS j.root-servers.net.
.   322660 IN NS k.root-servers.net.
.   322660 IN NS l.root-servers.net.
.   322660 IN NS m.root-servers.net.
;; Received 811 bytes from 127.0.0.53#53(127.0.0.53) in 16 ms

com.   172800 IN NS i.gtld-servers.net.
com.   172800 IN NS k.gtld-servers.net.
com.   172800 IN NS e.gtld-servers.net.
com.   172800 IN NS c.gtld-servers.net.
com.   172800 IN NS h.gtld-servers.net.
com.   172800 IN NS b.gtld-servers.net.
com.   172800 IN NS d.gtld-servers.net.
com.   172800 IN NS f.gtld-servers.net.
com.   172800 IN NS j.gtld-servers.net.
com.   172800 IN NS g.gtld-servers.net.
com.   172800 IN NS a.gtld-servers.net.
com.   172800 IN NS m.gtld-servers.net.
com.   172800 IN NS l.gtld-servers.net.
com.   86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4
com.   86400 IN RRSIG DS 8 1 86400 20221121170000 20221108160000 18733 . ZgW2d
;; Received 1201 bytes from 192.33.4.12#53(c.root-servers.net) in 148 ms

geekflare.com.  172800 IN NS olga.ns.cloudflare.com.
geekflare.com.  172800 IN NS todd.ns.cloudflare.com.
geekflare.com.  86400 IN DS 2371 13 2 CBAA2018F41B29985DAEDE7F127D4F9626ADA609
geekflare.com.  86400 IN RRSIG DS 8 2 86400 20221112051535 20221105030535 5392
;; Received 601 bytes from 2001:501:b1f9::30#53(m.gtld-servers.net) in 144 ms

geekflare.com.  300 IN A 172.66.43.163
geekflare.com.  300 IN A 172.66.40.93
geekflare.com.  300 IN RRSIG A 13 2 300 20221110051242 20221108031242 34505 ge
;; Received 183 bytes from 172.64.32.137#53(olga.ns.cloudflare.com) in 16 ms
```

Кроме того, вы можете получить короткий ответ, используя переменные `+short` или `+noall +answer`.

Обратный поиск DNS

Обратный поиск DNS позволяет обнаружить запись PTR, связанную с IP-адресом. Это противоположность записи DNS A и соответствие IP-адресов доменному имени. Однако раздел ответа будет отсутствовать, если у доменного имени нет записи

DNS PTR. Здесь используется команда `dig -x IP-?????`.

```
ubuntu@ubuntu:~$ dig yahoo.com +short
74.6.143.26
74.6.231.20
98.137.11.164
98.137.11.163
74.6.143.25
74.6.231.21
ubuntu@ubuntu:~$ dig -x 74.6.143.26

; <<>> DiG 9.18.1-1ubuntu1-Ubuntu <<>> -x 74.6.143.26
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32267
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;26.143.6.74.in-addr.arpa. IN PTR

;; ANSWER SECTION:
26.143.6.74.in-addr.arpa. 600 IN PTR media-router-fp74.prod.media.vip.bf1.yaho

;; AUTHORITY SECTION:
143.6.74.in-addr.arpa. 172800 IN NS ns3.yahoo.com.
143.6.74.in-addr.arpa. 172800 IN NS ns4.yahoo.com.
143.6.74.in-addr.arpa. 172800 IN NS ns5.yahoo.com.
143.6.74.in-addr.arpa. 172800 IN NS ns2.yahoo.com.
143.6.74.in-addr.arpa. 172800 IN NS ns1.yahoo.com.

;; Query time: 192 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 09 04:17:08 UTC 2022
;; MSG SIZE  rcvd: 203
```

Как вы можете видеть, доменное имя в разделе “Ответ”, media-router-fp74 `.prod.media.vip.bf1.yahoo.com/`, связано с основным IP-адресом 74.6.143.26. Посетив этот URL-адрес, вы попадете на домашнюю страницу поиска Yahoo. Однако это может быть справедливо не для всех хостингов: в некоторых случаях эти уродливые длинные URL ничего не разрешают.

Запрос определенных DNS-серверов

Иногда для DNS-запросов требуется пинговать определенный сервер. Этого можно легко добиться, добавив `@DNS server IP address`, выбрав любой DNS-сервер для конкретного запроса.

```
$ dig @1.1.1.1 geekflare.com +noall +answer +stats
geekflare.com.  300 IN A 172.66.40.93
```

```
geekflare.com.  300 IN A 172.66.43.163
;; Query time: 156 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Wed Nov 09 04:18:56 UTC 2022
;; MSG SIZE  rcvd: 74
```

Вы можете убедиться в этом в разделе статистики, где упоминается **Server: 1.1.1.1** , который принадлежит Cloudflare. Аналогичным образом можно запросить DNS-серверы Google (8.8.8.8):

```
$ dig @8.8.8.8 geekflare.com mx +noall +answer +stats
geekflare.com.  300 IN MX 1 aspmx.l.google.com.
geekflare.com.  300 IN MX 10 alt3.aspmx.l.google.com.
geekflare.com.  300 IN MX 10 alt4.aspmx.l.google.com.
geekflare.com.  300 IN MX 5 alt1.aspmx.l.google.com.
geekflare.com.  300 IN MX 5 alt2.aspmx.l.google.com.
;; Query time: 44 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Nov 09 04:23:16 UTC 2022
;; MSG SIZE  rcvd: 157
```

Давайте раскопаем его

Как видно из названия, они используются для выкапывания информации о DNS и выявления связанных с ней проблем. Команды Dig обычно работают быстро и легко запоминаются. Кроме того, утилиты для копания можно установить на Mac и Windows, что делает их универсальными в применении.

Дата Создания
22.05.2024