



Dnstop - мониторинг запросов к DNS-серверу

Опубликовано muff в Пнд, 2013-09-30 02:12

При работе с **DNS**-сервером, может пригодится утилита **dnstop**, которой довольно удобно мониторить статистику запросов к **DNS**. Установка утилиты не вызывает проблем, поскольку она есть в портах. Выполним установку:

```
# cd /usr/ports/dns/dnstop && make install clean && rehash
```

После установки утилиты ознакомиться с ее возможностями можно на страницах руководства (**man**). Для знакомства с ключами запуска достаточно запустить утилиту без указания ключей:

```
# dnstop

usage: dnstop [opts] netdevice|savefile          -4      Count IPv4 packets          -6
      Count IPv6 packets          -Q      Count queries              -R      Count responses
      -a      Anonymize IP Addr     -b expr BPF program code   -i addr Ign
ore this source IP address      -n name Count only messages in this domain
-p      Don't put interface in promiscuous mode  -P      Print "progress" mess
ages in non-interactive mode    -r      Redraw interval, in seconds  -l N
      Enable domain stats up to N components    -X      Don't tabulate the "source
+ query name" stats            -f      filter-name

Available filters:      unknown-tlds      A-for-A      rfc1918-ptr      refu
sed      qtype-any
```

Чтобы просмотреть **top DNS**-запросов, достаточно в качестве аргумента указать интерфейс, на котором "ловить" запросы. Результат работы утилиты - ниже.

```
Queries: 5 new, 23 total                                     Mon Sep 30
01:53:10 2013

Sources      Count      %      cum%-----107.20.2
6.241      5      21.7      21.778.138.88.232      3      13.0      34.8202.43.32.21
      3      13.0      47.8184.105.224.2      2      8.7      56.562.24.128.253      2
      8.7      65.2123.151.39.143      1      4.3      69.672.52.104.6      1      4.3
      73.9203.80.96.9      1      4.3      78.3184.72.161.220      1      4.3      82.619
3.75.110.134      1      4.3      87.091.196.100.22      1      4.3      91.3173.193.11
8.4      1      4.3      95.7173.193.118.5      1      4.3      100.0
```

Можно фильтровать запросы по многим параметрам. Как вариант - по доменному имени. Для этого необходимо воспользоваться ключем **-n**, после которого в качестве аргумента необходимо передать доменное имя. Пример:

```
# dnstop -n muff.kiev.ua em0
```

На этом описание утилиты закончим, поскольку ничего сложного в ней нету. А вот полезным инструментом она может оказаться довольно часто...

Источник (получено 2025-03-27 01:30):

<http://muff.kiev.ua/content/dnstop-monitoring-zaprosov-k-dns-serveru>