netstat 命令介绍

技术|netstat 的10个基本用法 (linux.cn)

netstat 是一款命令行工具，可用于列出系统上所有的网络套接字连接情况，包括 tcp, udp 以及 unix 套接字，另外它还能列出处于监听状态（即等待接入请求）的套接字。

- -a, --all
- --tcp|-t
- --udp|-u
- **--numeric , -n**
- **-l, --listening**
- **-p, --program**
- **-e, --extend**
- --route , -r
- --interfaces=iface , -I=iface , -i

```
sudo netstat -anlpe | head -20
```

1. 列出所有连接

列出所有当前的连接。使用 -a 选项即可。

```
[lcc@localhost ~]$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State
tcp        0      0 localhost.locald:domain 0.0.0.0:*
           LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*
           LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*
           LISTEN
tcp        0      0 localhost:smtp          0.0.0.0:*
           LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*
           LISTEN
tcp        0     36 localhost.localdoma:ssh
10.10.10.1:55190        ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*
             LISTEN
......
```

2. 只列出 TCP 或 UDP 协议的连接

使用 **-t** 选项列出 TCP 协议的连接:

使用 **-u** 选项列出 UDP 协议的连接:

```
[lcc@localhost ~]$ netstat -t | head -10
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State
tcp        0      0 localhost.localdoma:ssh
10.10.10.1:55190        ESTABLISHED
```

3. 禁用反向域名解析，加快查询速度

默认情况下 netstat 会通过反向域名解析技术查找每个 IP 地址对应的主机名。就使用 **-n** 选项禁用域名解析功能。

```
[lcc@localhost ~]$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State
tcp        0      0 192.168.122.1:53        0.0.0.0:*
            LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*
            LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*
            LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*
            LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*
            LISTEN
tcp        0     36 10.10.10.10:22
10.10.10.1:55190        ESTABLISHED
tcp6       0      0 :::22                   :::*
             LISTEN
tcp6       0      0 ::1:631                 :::*
             LISTEN
tcp6       0      0 ::1:25                  :::*
             LISTEN
tcp6       0      0 :::111                  :::*
             LISTEN
```

4. 只列出监听中的连接

使用 **-l** 选项列出正在监听的套接字。

```
[lcc@localhost ~]$ netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State
tcp        0      0 192.168.122.1:53        0.0.0.0:*
            LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*
            LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*
            LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*
            LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*
            LISTEN
tcp6       0      0 :::22                   :::*
             LISTEN
tcp6       0      0 ::1:631                 :::*
             LISTEN
tcp6       0      0 ::1:25                  :::*
             LISTEN
tcp6       0      0 :::111                  :::*
             LISTEN
```

5. 获取进程名、进程号以及用户 ID

使用 **-p** 选项查看进程信息。

使用 **-p** 选项时，netstat 必须运行在 root 权限之下，不然它就不能得到运行在 root 权限下的进程名，而很多服务包括 http 和 ftp 都运行在 root 权限之下。

```
[lcc@localhost ~]$ sudo netstat -nlpt
[sudo] password for lcc:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State       PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*
           LISTEN      1467/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*
           LISTEN      1083/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*
           LISTEN      1081/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*
           LISTEN      1497/master
tcp        0      0 0.0.0.0:111             0.0.0.0:*
           LISTEN      590/rpcbind
tcp6       0      0 :::22                   :::*
             LISTEN      1083/sshd
tcp6       0      0 ::1:631                 :::*
             LISTEN      1081/cupsd
tcp6       0      0 ::1:25                  :::*
             LISTEN      1497/master
tcp6       0      0 :::111                  :::*
             LISTEN      590/rpcbind
```

相比进程名和进程号而言，查看进程的拥有者会更有用。使用 **-ep** 选项可以同时查看进程名和用户名。

```
[lcc@localhost ~]$ sudo netstat -nlpet
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State       User       Inode
PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*
           LISTEN      0          29265
1467/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*
           LISTEN      0          27631      1083/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*
           LISTEN      0          26210
1081/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*
           LISTEN      0          29355
1497/master
tcp        0      0 0.0.0.0:111             0.0.0.0:*
           LISTEN      0          19518
590/rpcbind
tcp6       0      0 :::22                   :::*
           LISTEN      0          27633
1083/sshd
tcp6       0      0 ::1:631                 :::*
           LISTEN      0          26209
1081/cupsd
tcp6       0      0 ::1:25                  :::*
           LISTEN      0          29356
1497/master
tcp6       0      0 :::111                  :::*
           LISTEN      0          19521
590/rpcbind
```

> *假如你将* **-n** *和* **-e** *选项一起使用，User 列的属性就是用户的 ID 号，而不是用户名。*

6. 打印统计数据

netstat 可以打印出网络统计数据，包括某个协议下的收发包数量。

```
[lcc@localhost ~]$ netstat -s
Ip:
    86175 total packets received
    0 forwarded
    0 incoming packets discarded
    85850 incoming packets delivered
    35108 requests sent out
    16 outgoing packets dropped
    1044 dropped because of missing route
Icmp:
    37 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 36
        echo requests: 1
    40 ICMP messages sent
    ......
```

7. 显示内核路由信息

使用 **-r** 选项打印内核路由信息。打印出来的信息与 route 命令输出的信息一样。我们也可以使用 **-n** 选项禁止域名解析。

```
[lcc@localhost ~]$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags
MSS Window  irtt Iface
0.0.0.0         10.10.10.2      0.0.0.0         UG
   0 0          0 ens33
10.10.10.0      0.0.0.0         255.255.255.0   U
  0 0          0 ens33
192.168.122.0   0.0.0.0         255.255.255.0   U
  0 0          0 virbr0
```

8. 打印网络接口

netstat 也能打印网络接口信息，**-i** 选项就是为这个功能而生。

```
[lcc@localhost ~]$ netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR
TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33            1500   182015      0      0 0
35440      0      0      0 BMRU
lo              65536       72      0      0 0
   72      0      0      0 LRU
virbr0           1500        0      0      0 0
    0      0      0      0 BMU
```

将 **-e** 选项和 **-i** 选项搭配使用，可以输出用户友好的信息。

```
[lcc@localhost ~]$ netstat -ie
Kernel Interface table
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu
1500
        inet 10.10.10.10  netmask 255.255.255.0
broadcast 10.10.10.255
        inet6 fe80::5ddc:ac63:20bb:df92  prefixlen 64
scopeid 0x20<link>
        ether 00:0c:29:29:02:a6  txqueuelen 1000
(Ethernet)
        RX packets 182026  bytes 266933392 (254.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35447  bytes 3308136 (3.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0
collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 72  bytes 6116 (5.9 KiB)
```

```
.....
```

9. netstat 持续输出

我们可以使用 netstat 的 **-c** 选项持续输出信息。