

知识点1【netstat的帮助信息】

netstat的简介

netstat --help

知识点2【netstat的使用实例】

- 1)列出所有套接字的PID/程序名称
- 2)列出所有 tcp协议套接字的PID/程序名称
- 4)只显示所有监听套接字的PID/程序名称
- 5)只列出所有监听 tcp套接字的PID/程序名称
- 6)只列出所有监听 udp 套接字的PID/程序名称
- 7)只列出所有监听 UNIX 套接字的PID/程序名称
- 8)找出程序运行的套接字的PID/程序名称
- 10)找出运行在指定端口的进程
- 11)持续输出 netstat 信息(每隔一秒输出网络信息)
- 12)显示所有端口的统计信息
- 13) 显示核心路由信息 netstat -r
- 14) 显示网络接口列表

知识点1【netstat的帮助信息】

netstat的简介

netstat 是一个监控TCP/IP网络的非常有用的工具，用于显示各种网络相关信息，如网络连接，接口状态，路由表， (Interface Statistics)， masquerade 连接，多播成员 (Multicast Memberships) 等等。Netstat用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况

netstat --help

```
1 edu@edu:~/work/tmp/net$ netstat --help
```

```

2 usage: netstat [-vWeenNcCF] [<Af>] -r netstat {-V|--version|-h|--help}
3 netstat [-vWnNcaeol] [<Socket> ...]
4 netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }
5
6 -r, --route 显示路由表
7 -i, --interfaces display interface table
8 -g, --groups display multicast group memberships
9 -s, --statistics display networking statistics (like SNMP)
10 -M, --masquerade display masqueraded connections
11
12 -v, --verbose 显示详细信息
13 -W, --wide don't truncate IP addresses
14 -n, --numeric 不解析名称
15 --numeric-hosts 不解析主机名
16 --numeric-ports 忽略端口名称
17 --numeric-users 忽略用户名
18 -N, --symbolic resolve hardware names
19 -e, --extend 显示更多信息
20 -p, --programs display PID/Program name for sockets
21 -c, --continuous continuous listing
22
23 -l, --listening display listening server sockets
24 -a, --all, --listening display all sockets (default: connected)
25 -o, --timers display timers
26 -F, --fib display Forwarding Information Base (default)
27 -C, --cache display routing cache instead of FIB
28
29 <Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --ne
    trom
30 <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; 默认: inet
31 列出所有支持的协议:
32 inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
33 netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
34 x25 (CCITT X.25)
35

```

知识点2 【netstat的使用实例】

1)列出所有套接字的PID/程序名称

```
1 netstat -anp
```

2)列出所有 **tcp**协议套接字的PID/程序名称

```
1 netstat -antp
```

3)列出所有 **udp**协议套接字的PID/程序名称

```
1 netstat -anup
```

4)只显示所有**监听套接字**的PID/程序名称

```
1 netstat -lnp
```

5)只列出所有**监听 tcp**套接字的PID/程序名称

```
1 netstat -ltnp
```

6)只列出所有监听 **udp** 套接字的PID/程序名称

```
1 netstat -lunp
```

7)只列出所有监听 **UNIX** 套接字的PID/程序名称

```
1 netstat -lxnp
```

8)找出程序运行的套接字的PID/程序名称

```
1 netstat -anp | grep ssh
```

注意:并不是所有的进程都能找到,没有权限的会不显示,使用 root 权限查看所有的信息。

10)找出运行在指定端口的进程

```
1 netstat -anp | grep ':3306'
```

11)持续输出 **netstat** 信息(每隔一秒输出网络信息)

```
1 netstat -cnp
```

12)显示所有端口的统计信息

```
1 netstat -s
```

13) 显示核心路由信息 **netstat -r**

```
edu@edu:~/work/tmp/net$ netstat -r
内核 IP 路由表
Destination      Gateway           Genmask           Flags        MSS Window  irtt  Iface
default           localhost        0.0.0.0           UG           0 0        0     eth0
10.9.21.0         *                255.255.255.0     U            0 0        0     eth0
link-local        *                255.255.0.0       U            0 0        0     eth0
edu@edu:~/work/tmp/net$
```

14) 显示网络接口列表

```
1 edu@edu:~/work/tmp/net$ netstat -i
2 Kernel Interface table
3 Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
4 eth0 1500 0 2475463 0 5 0 837541 0 0 0 BMRU
5 lo 16436 0 33120 0 0 0 33120 0 0 0 LRU
```

```
6 edu@edu:~/work/tmp/net$
```