[**每天一个linux命令（56）：netstat命令**](http://www.cnblogs.com/peida/archive/2013/03/08/2949194.html)

netstat命令用于显示与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是在内核中访问网络及相关信息的程序，它能提供TCP连接，TCP和UDP监听，进程内存管理的相关报告。

如果你的计算机有时候接收到的数据报导致出错数据或故障，你不必感到奇怪，TCP/IP可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的IP数据报相当大的百分比，或者它的数目正迅速增加，那么你就应该使用netstat查一查为什么会出现这些情况了。

**1．命令格式：**

netstat [-acCeFghilMnNoprstuvVwx][-A<网络类型>][--ip]

**2．命令功能：**

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。

**3．命令参数：**

-a或–all 显示所有连线中的Socket。

-A<网络类型>或–<网络类型> 列出该网络类型连线中的相关地址。

-c或–continuous 持续列出网络状态。

-C或–cache 显示路由器配置的快取信息。

-e或–extend 显示网络其他相关信息。

-F或–fib 显示FIB。

-g或–groups 显示多重广播功能群组组员名单。

-h或–help 在线帮助。

-i或–interfaces 显示网络界面信息表单。

-l或–listening 显示监控中的服务器的Socket。

-M或–masquerade 显示伪装的网络连线。

-n或–numeric 直接使用IP地址，而不通过域名服务器。

-N或–netlink或–symbolic 显示网络硬件外围设备的符号连接名称。

-o或–timers 显示计时器。

-p或–programs 显示正在使用Socket的程序识别码和程序名称。

-r或–route 显示Routing Table。

-s或–statistice 显示网络工作信息统计表。

-t或–tcp 显示TCP传输协议的连线状况。

-u或–udp 显示UDP传输协议的连线状况。

-v或–verbose 显示指令执行过程。

-V或–version 显示版本信息。

-w或–raw 显示RAW传输协议的连线状况。

-x或–unix 此参数的效果和指定”-A unix”参数相同。

–ip或–inet 此参数的效果和指定”-A inet”参数相同。

**4．使用实例：**

**实例1：无参数使用**

**命令：**

netstat

**输出：**

[root@localhost ~]# netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
tcp        0    268 192.168.120.204:ssh         10.2.0.68:62420             ESTABLISHED   
udp        0      0 192.168.120.204:4371        10.58.119.119:domain        ESTABLISHED   
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags       Type       State         I-Node Path  
unix  2      [ ]         DGRAM                    1491   @/org/kernel/udev/udevd  
unix  4      [ ]         DGRAM                    7337   /dev/log  
unix  2      [ ]         DGRAM                    708823   
unix  2      [ ]         DGRAM                    7539     
unix  3      [ ]         STREAM     CONNECTED     7287     
unix  3      [ ]         STREAM     CONNECTED     7286     
[root@localhost ~]#

**说明：**

从整体上看，netstat的输出结果可以分为两个部分：

一个是Active Internet connections，称为有源TCP连接，其中"Recv-Q"和"Send-Q"指的是接收队列和发送队列。这些数字一般都应该是0。如果不是则表示软件包正在队列中堆积。这种情况只能在非常少的情况见到。

另一个是Active UNIX domain sockets，称为有源Unix域套接口(和网络套接字一样，但是只能用于本机通信，性能可以提高一倍)。

Proto显示连接使用的协议,RefCnt表示连接到本套接口上的进程号,Types显示套接口的类型,State显示套接口当前的状态,Path表示连接到套接口的其它进程使用的路径名。

**套接口类型：**

-t ：TCP

-u ：UDP

-raw ：RAW类型

--unix ：UNIX域类型

--ax25 ：AX25类型

--ipx ：ipx类型

--netrom ：netrom类型

**状态说明：**

LISTEN：侦听来自远方的TCP端口的连接请求

SYN-SENT：再发送连接请求后等待匹配的连接请求（如果有大量这样的状态包，检查是否中招了）

SYN-RECEIVED：再收到和发送一个连接请求后等待对方对连接请求的确认（如有大量此状态，估计被flood攻击了）

ESTABLISHED：代表一个打开的连接

FIN-WAIT-1：等待远程TCP连接中断请求，或先前的连接中断请求的确认

FIN-WAIT-2：从远程TCP等待连接中断请求

CLOSE-WAIT：等待从本地用户发来的连接中断请求

CLOSING：等待远程TCP对连接中断的确认

LAST-ACK：等待原来的发向远程TCP的连接中断请求的确认（不是什么好东西，此项出现，检查是否被攻击）

TIME-WAIT：等待足够的时间以确保远程TCP接收到连接中断请求的确认

CLOSED：没有任何连接状态

**实例2：列出所有端口**

**命令：**

netstat -a

**输出：**

[root@localhost ~]# netstat -a  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
tcp        0      0 localhost:smux              \*:\*                         LISTEN        
tcp        0      0 \*:svn                       \*:\*                         LISTEN        
tcp        0      0 \*:ssh                       \*:\*                         LISTEN        
tcp        0    284 192.168.120.204:ssh         10.2.0.68:62420             ESTABLISHED   
udp        0      0 localhost:syslog            \*:\*                                       
udp        0      0 \*:snmp                      \*:\*                                       
Active UNIX domain sockets (servers and established)  
Proto RefCnt Flags       Type       State         I-Node Path  
unix  2      [ ACC ]     STREAM     LISTENING     708833 /tmp/ssh-yKnDB15725/agent.15725  
unix  2      [ ACC ]     STREAM     LISTENING     7296   /var/run/audispd\_events  
unix  2      [ ]         DGRAM                    1491   @/org/kernel/udev/udevd  
unix  4      [ ]         DGRAM                    7337   /dev/log  
unix  2      [ ]         DGRAM                    708823   
unix  2      [ ]         DGRAM                    7539     
unix  3      [ ]         STREAM     CONNECTED     7287     
unix  3      [ ]         STREAM     CONNECTED     7286     
[root@localhost ~]#

**说明：**

显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请（LISTENING）的那些连接。

**实例3：显示当前UDP连接状况**

**命令：**

netstat -nu

**输出：**

[root@andy ~]# netstat -nu  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
udp        0      0 ::ffff:192.168.12:53392     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:56723     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:56480     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:58154     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:44227     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:36954     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:53984     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:57703     ::ffff:192.168.9.120:10000  ESTABLISHED   
udp        0      0 ::ffff:192.168.12:53613     ::ffff:192.168.9.120:10000  ESTABLISHED   
[root@andy ~]#

**说明：**

**实例4：显示UDP端口号的使用情况**

**命令：**

netstat -apu

**输出：**

[root@andy ~]# netstat -apu  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name     
udp        0      0 \*:57604                     \*:\*                                     28094/java            
udp        0      0 \*:40583                     \*:\*                                     21220/java            
udp        0      0 \*:45451                     \*:\*                                     14583/java            
udp        0      0 ::ffff:192.168.12:53392     ::ffff:192.168.9.120:ndmp   ESTABLISHED 19327/java            
udp        0      0 \*:52370                     \*:\*                                     15841/java            
udp        0      0 ::ffff:192.168.12:56723     ::ffff:192.168.9.120:ndmp   ESTABLISHED 15841/java            
udp        0      0 \*:44182                     \*:\*                                     31757/java            
udp        0      0 \*:48155                     \*:\*                                     5476/java             
udp        0      0 \*:59808                     \*:\*                                     17333/java            
udp        0      0 ::ffff:192.168.12:56480     ::ffff:192.168.9.120:ndmp   ESTABLISHED 28094/java            
udp        0      0 ::ffff:192.168.12:58154     ::ffff:192.168.9.120:ndmp   ESTABLISHED 15429/java            
udp        0      0 \*:36780                     \*:\*                                     10091/java            
udp        0      0 \*:36795                     \*:\*                                     24594/java            
udp        0      0 \*:41922                     \*:\*                                     20506/java            
udp        0      0 ::ffff:192.168.12:44227     ::ffff:192.168.9.120:ndmp   ESTABLISHED 17333/java            
udp        0      0 \*:34258                     \*:\*                                     8866/java             
udp        0      0 \*:55508                     \*:\*                                     11667/java            
udp        0      0 \*:36055                     \*:\*                                     12425/java            
udp        0      0 ::ffff:192.168.12:36954     ::ffff:192.168.9.120:ndmp   ESTABLISHED 16532/java            
udp        0      0 ::ffff:192.168.12:53984     ::ffff:192.168.9.120:ndmp   ESTABLISHED 20506/java            
udp        0      0 ::ffff:192.168.12:57703     ::ffff:192.168.9.120:ndmp   ESTABLISHED 31757/java            
udp        0      0 ::ffff:192.168.12:53613     ::ffff:192.168.9.120:ndmp   ESTABLISHED 3199/java             
udp        0      0 \*:56309                     \*:\*                                     15429/java            
udp        0      0 \*:54007                     \*:\*                                     16532/java            
udp        0      0 \*:39544                     \*:\*                                     3199/java             
udp        0      0 \*:43900                     \*:\*                                     19327/java            
[root@andy ~]#

**说明：**

**实例5：显示网卡列表**

**命令：**

netstat -i

**输出：**

[root@andy ~]# netstat -i  
Kernel Interface table  
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg  
eth0       1500   0 151818887      0      0      0 198928403      0      0      0 BMRU  
lo        16436   0   107235      0      0      0   107235      0      0      0 LRU  
[root@andy ~]#

**说明：**

**实例6：显示组播组的关系**

**命令：**

netstat -g

**输出：**

[root@andy ~]# netstat -g  
IPv6/IPv4 Group Memberships  
Interface       RefCnt Group  
--------------- ------ ---------------------  
lo              1      all-systems.mcast.net  
eth0            1      all-systems.mcast.net  
lo              1      ff02::1  
eth0            1      ff02::1:ffff:9b0c  
eth0            1      ff02::1  
[root@andy ~]#

**说明：**

**实例7：显示网络统计信息**

**命令：**

netstat -s

**输出：**

[root@localhost ~]# netstat -s  
Ip:  
    530999 total packets received  
    0 forwarded  
    0 incoming packets discarded  
    530999 incoming packets delivered  
    8258 requests sent out  
    1 dropped because of missing route  
Icmp:  
    90 ICMP messages received  
    0 input ICMP message failed.  
    ICMP input histogram:  
        destination unreachable: 17  
        echo requests: 1  
        echo replies: 72  
    106 ICMP messages sent  
    0 ICMP messages failed  
    ICMP output histogram:  
        destination unreachable: 8  
        echo request: 97  
        echo replies: 1  
IcmpMsg:  
        InType0: 72  
        InType3: 17  
        InType8: 1  
        OutType0: 1  
        OutType3: 8  
        OutType8: 97  
Tcp:  
    8 active connections openings  
    15 passive connection openings  
    8 failed connection attempts  
    3 connection resets received  
    1 connections established  
    3132 segments received  
    2617 segments send out  
    53 segments retransmited  
    0 bad segments received.  
    252 resets sent  
Udp:  
    0 packets received  
    0 packets to unknown port received.  
    0 packet receive errors  
    5482 packets sent  
TcpExt:  
    1 invalid SYN cookies received  
    1 TCP sockets finished time wait in fast timer  
    57 delayed acks sent  
    Quick ack mode was activated 50 times  
    60 packets directly queued to recvmsg prequeue.  
    68 packets directly received from backlog  
    4399 packets directly received from prequeue  
    520 packets header predicted  
    51 packets header predicted and directly queued to user  
    1194 acknowledgments not containing data received  
    21 predicted acknowledgments  
    0 TCP data loss events  
    1 timeouts after reno fast retransmit  
    9 retransmits in slow start  
    42 other TCP timeouts  
    3 connections aborted due to timeout  
IpExt:  
    InBcastPkts: 527777

**说明：**

按照各个协议分别显示其统计数据。如果我们的应用程序（如Web浏览器）运行速度比较慢，或者不能显示Web页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

**实例8：显示监听的套接口**

**命令：**

netstat -l

**输出：**

[root@localhost ~]# netstat -l  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
tcp        0      0 localhost:smux              \*:\*                         LISTEN        
tcp        0      0 \*:svn                       \*:\*                         LISTEN        
tcp        0      0 \*:ssh                       \*:\*                         LISTEN        
udp        0      0 localhost:syslog            \*:\*                                       
udp        0      0 \*:snmp                      \*:\*                                       
Active UNIX domain sockets (only servers)  
Proto RefCnt Flags       Type       State         I-Node Path  
unix  2      [ ACC ]     STREAM     LISTENING     708833 /tmp/ssh-yKnDB15725/agent.15725  
unix  2      [ ACC ]     STREAM     LISTENING     7296   /var/run/audispd\_events  
[root@localhost ~]#

**说明：**

**实例9：显示所有已建立的有效连接**

**命令：**

netstat -n

**输出：**

[root@localhost ~]# netstat -n  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
tcp        0    268 192.168.120.204:22          10.2.0.68:62420             ESTABLISHED   
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags       Type       State         I-Node Path  
unix  2      [ ]         DGRAM                    1491   @/org/kernel/udev/udevd  
unix  4      [ ]         DGRAM                    7337   /dev/log  
unix  2      [ ]         DGRAM                    708823   
unix  2      [ ]         DGRAM                    7539     
unix  3      [ ]         STREAM     CONNECTED     7287     
unix  3      [ ]         STREAM     CONNECTED     7286     
[root@localhost ~]#

**说明：**

**实例10：显示关于以太网的统计数据**

**命令：**

netstat -e

**输出：**

[root@localhost ~]# netstat -e  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State       User       Inode       
tcp        0    248 192.168.120.204:ssh         10.2.0.68:62420             ESTABLISHED root       708795       
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags       Type       State         I-Node Path  
unix  2      [ ]         DGRAM                    1491   @/org/kernel/udev/udevd  
unix  4      [ ]         DGRAM                    7337   /dev/log  
unix  2      [ ]         DGRAM                    708823   
unix  2      [ ]         DGRAM                    7539     
unix  3      [ ]         STREAM     CONNECTED     7287     
unix  3      [ ]         STREAM     CONNECTED     7286     
[root@localhost ~]#

**说明：**

用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量）

**实例11：显示关于路由表的信息**

**命令：**

netstat -r

**输出：**

[root@localhost ~]# netstat -r  
Kernel IP routing table  
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface  
192.168.120.0   \*               255.255.255.0   U         0 0          0 eth0  
192.168.0.0     192.168.120.1   255.255.0.0     UG        0 0          0 eth0  
10.0.0.0        192.168.120.1   255.0.0.0       UG        0 0          0 eth0  
default         192.168.120.240 0.0.0.0         UG        0 0          0 eth0  
[root@localhost ~]#

**说明：**

**实例12：列出所有 tcp 端口**

**命令：**

netstat -at

**输出：**

[root@localhost ~]# netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State        
tcp        0      0 localhost:smux              \*:\*                         LISTEN        
tcp        0      0 \*:svn                       \*:\*                         LISTEN        
tcp        0      0 \*:ssh                       \*:\*                         LISTEN        
tcp        0    284 192.168.120.204:ssh         10.2.0.68:62420             ESTABLISHED   
[root@localhost ~]#

**说明：**

**实例13：统计机器中网络连接各个状态个数**

**命令：**

netstat -a | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'

**输出：**

[root@localhost ~]# netstat -a | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'  
ESTABLISHED 1  
LISTEN 3  
[root@localhost ~]#

**说明：**

**实例14：**把状态全都取出来后使用uniq -c统计后再进行排序

**命令：**

netstat -nat |awk '{print $6}'|sort|uniq -c

**输出：**

[root@andy ~]# netstat -nat |awk '{print $6}'|sort|uniq -c  
     14 CLOSE\_WAIT  
      1 established)  
    578 ESTABLISHED  
      1 Foreign  
     43 LISTEN  
      5 TIME\_WAIT  
[root@andy ~]# netstat -nat |awk '{print $6}'|sort|uniq -c|sort -rn  
    576 ESTABLISHED  
     43 LISTEN  
     14 CLOSE\_WAIT  
      5 TIME\_WAIT  
      1 Foreign  
      1 established)  
[root@andy ~]#

**说明：**

**实例15：查看连接某服务端口最多的的IP地址**

**命令：**

netstat -nat | grep "192.168.120.20:16067" |awk '{print $5}'|awk -F: '{print $4}'|sort|uniq -c|sort -nr|head -20

**输出：**

[root@andy ~]# netstat -nat | grep "192.168.120.20:16067" |awk '{print $5}'|awk -F: '{print $4}'|sort|uniq -c|sort -nr|head -20  
      8 10.2.1.68  
      7 192.168.119.13  
      6 192.168.119.201  
      6 192.168.119.20  
      6 192.168.119.10  
      4 10.2.1.199  
      3 10.2.1.207  
      2 192.168.120.20  
      2 192.168.120.15  
      2 192.168.119.197  
      2 192.168.119.11  
      2 10.2.1.206  
      2 10.2.1.203  
      2 10.2.1.189  
      2 10.2.1.173  
      1 192.168.120.18  
      1 192.168.119.19  
      1 10.2.2.227  
      1 10.2.2.138  
      1 10.2.1.208  
[root@andy ~]#

**说明：**

**实例16：找出程序运行的端口**

**命令：**

netstat -ap | grep ssh

**输出：**

[root@andy ~]# netstat -ap | grep ssh  
tcp        0      0 \*:ssh                       \*:\*                         LISTEN      2570/sshd             
tcp        0      0 ::ffff:192.168.120.206:ssh  ::ffff:10.2.1.205:54508     ESTABLISHED 13883/14              
tcp        0      0 ::ffff:192.168.120.206:ssh  ::ffff:10.2.0.68:62886      ESTABLISHED 20900/6               
tcp        0      0 ::ffff:192.168.120.206:ssh  ::ffff:10.2.2.131:52730     ESTABLISHED 20285/sshd: root@no   
unix  2      [ ACC ]     STREAM     LISTENING     194494461 20900/6             /tmp/ssh-cXIJj20900/agent.20900  
unix  3      [ ]         STREAM     CONNECTED     194307443 20285/sshd: root@no   
unix  3      [ ]         STREAM     CONNECTED     194307441 20285/sshd: root@no   
[root@andy ~]#

**说明：**

**实例17：在 netstat 输出中显示 PID 和进程名称**

**命令：**

netstat -pt

**输出：**

[root@localhost ~]# netstat -pt  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name     
tcp        0    248 192.168.120.204:ssh         10.2.0.68:62420             ESTABLISHED 15725/0               
[root@localhost ~]#

**说明：**

netstat -p 可以与其它开关一起使用，就可以添加 “PID/进程名称” 到 netstat 输出中，这样 debugging 的时候可以很方便的发现特定端口运行的程序。

**实例18：找出运行在指定端口的进程**

**命令：**

netstat -anpt | grep ':16064'

**输出：**

[root@andy ~]# netstat -anpt | grep ':16064'  
tcp        0      0 :::16064                    :::\*                        LISTEN      24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:192.168.119.201:6462 ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:192.168.119.20:26341 ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:192.168.119.20:32208 ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:192.168.119.20:32207 ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:51303      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:51302      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:50020      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:50019      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:56155      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:50681      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:50680      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:52136      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:56989      ESTABLISHED 24594/java            
tcp        0      0 ::ffff:192.168.120.20:16064 ::ffff:10.2.1.68:56988      ESTABLISHED 24594/java            
[root@andy ~]#

**说明：**

运行在端口16064的进程id为24596，再通过ps命令就可以找到具体的应用程序了。