title	date	categories	tags
nc 命令常用用法	Fri Aug 05 2016 04:24:11 GMT+0800 (CST)	Linux	Linux 命令

man 手册介绍

> The nc (or netcat) utility is used for just about anything under the sun involving TCP or UDP. It can open TCP connections, sendUDP packets, listen on arbitrary TCP and UDP ports, do port scanning, and deal with both IPv4 and IPv6. Unlike telnet(1), nc scripts nicely, and separates error messages onto standard error instead of sending them to standard output, as telnet(1) does with some.

nc 功能简介

nc是网络界的“瑞士军刀”, 提供以下功能：

- 监听特定的端口,这时候 `nc` 可以作为一个服务器,不过仅仅是一个echo服务器
- 链接特定的端口,这时候 `nc` 就成为一个客户端,也是一个简单的客户端,只能起echo作用
- 扫描端口,这可以查询某个机器上是否开启了某个端口

语法格式

`nc` 语法格式过长，具体的可以查阅man手册，本文只介绍常用的几个选项

- -l Listen mode, for inbound connects 监听模式，接收链接

- -p port Specify local port for remote connects 指定一个本地端口去链接远端服务器
- -w secs Timeout for connects and final net reads 接收一个连接到第一个消息到来的超时时间

例子说明

监听端口

语法格式：nc -l [addr] port
说明：如果不指定`addr`,则绑定地址0.0.0.0，即该机器所绑定的所有网卡ip都能链接上指定的`port`

不指定IP

> [root@localhost103 ~]$ nc -l 1234
> [root@localhost103 ~]$netstat -tunlp | grep 1234
> tcp 0 0 0.0.0.0:1234 0.0.0.0:* LISTEN 22304/nc

指定IP

> [root@localhost103 ~]$ nc -l 127.0.0.1 1234
> [root@localhost103 ~]$netstat -tunlp | grep 1234
> tcp 0 0 127.0.0.1:1234 0.0.0.0:* LISTEN 23805/nc

链接指定IP PORT

语法格式：nc IP PORT [-p port]
说明：`IP` `PORT` 为目的机器的地址，可选项 -p port 为以本机指定的端口`port`链接目的地址

目标机器地址为：127.0.0.1 1234

> nc 127.0.0.1 1234 #直接则链接上目标机器

扫描端口

语法格式：nc -v -z port1-prot2
说明：`-v`是打印出详细信息 `-z`是指定端口区间

> [root@localhost103 ~]$ nc -v 192.168.201.75 -z 7000-7010
> nc: connect to 192.168.201.75 port 7000 (tcp) failed: Connection refused
> Connection to 192.168.201.75 7001 port [tcp/afs3-callback] succeeded!
> Connection to 192.168.201.75 7002 port [tcp/afs3-prserver] succeeded!
> nc: connect to 192.168.201.75 port 7003 (tcp) failed: Connection refused
> Connection to 192.168.201.75 7004 port [tcp/afs3-kaserver] succeeded!
> Connection to 192.168.201.75 7005 port [tcp/afs3-volser] succeeded!
> Connection to 192.168.201.75 7006 port [tcp/afs3-errors] succeeded!
> Connection to 192.168.201.75 7007 port [tcp/afs3-bos] succeeded!
> Connection to 192.168.201.75 7008 port [tcp/afs3-update] succeeded!
> Connection to 192.168.201.75 7009 port [tcp/afs3-rmtsys] succeeded!
> Connection to 192.168.201.75 7010 port [tcp/ups-onlinet] succeeded!

总结

`nc` 功能实则很强大,还可以做简单的代理服务器、传送文件等等功能,号称网络中的瑞士军刀,也不是浪得虚名,工具虽然强大,但还在乎于使用的人。关于该命令,还将持续学习中,以此做记录。