【1-12】linux网络操作命令、工具

笔记本：	备课_linux		
创建时间：	2022/4/17 8:54	更新时间：	2022/4/29 15:46
作者：	兰鸣人花道	位置：	30°46'37 N 103°56'14 E

1、网络接口查看

- 为什么要查看ip？
- ifconfig
  - ifconfig eth0, 查看指定网卡的ip地址
  - ifconfig -a，查看所有网卡的ip地址
  - [root@localhost ~]# yum install -y net-tools   #如果这个命令不能使用，就安装net-tool这个工具
- ip addr
- 子网掩码
  - 255.255.255.0， 24
- 网关
  - x.x.x.1
- 端口
  - 服务器上给不同的应用开的访问的门

```
#    关闭防火墙
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]#

#    查看防火墙的状态
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor
preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)
[root@localhost ~]#

#    开机不启动防火墙的配置
[root@localhost ~]# systemctl disable firewalld
[root@localhost ~]#

#    配置静态ip的方法， 一般来说，你首先得在windows上通过cmd查看你自己电脑的ip

#    windows查看自己的ip, ping 192.168.4.XXX   这个ip有没有人用，如果没有人用，你就可
以配这个ip作为你的centos的静态ip
以太网适配器 以太网 2:
   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::2432:784f:49bf:6b7c%42
   IPv4 地址 . . . . . . . . . . . . : 192.168.4.208     # 确认自己的网段，
192.168.4.xxx
   子网掩码  . . . . . . . . . . . . : 255.255.255.0     # 子网掩码
   默认网关. . . . . . . . . . . . . : 192.168.4.1       #  网关

[root@localhost ~]# cd /etc/sysconfig/network-scripts/
[root@localhost network-scripts]# pwd
/etc/sysconfig/network-scripts
[root@localhost network-scripts]# ls
ifcfg-ens33  ifdown-isdn      ifdown-tunnel  ifup-isdn    ifup-Team
ifcfg-lo     ifdown-post      ifup           ifup-plip    ifup-TeamPort
ifdown       ifdown-ppp       ifup-aliases   ifup-plusb   ifup-tunnel
ifdown-bnep  ifdown-routes    ifup-bnep      ifup-post    ifup-wireless
ifdown-eth   ifdown-sit       ifup-eth       ifup-ppp     init.ipv6-global
```

```
ifdown-ippp  ifdown-Team      ifup-ippp      ifup-routes  network-functions
ifdown-ipv6  ifdown-TeamPort  ifup-ipv6      ifup-sit     network-functions-ipv6
[root@localhost network-scripts]# vi ifcfg-ens33
[root@localhost network-scripts]#
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
#BOOTPROTO="dhcp"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens33"
DEVICE="ens33"
ONBOOT="yes"
IPADDR=192.168.4.102
NETMASK=255.255.255.0
GATEWAY=192.168.4.1
DNS1=114.114.114.114
#DNS1=8.8.8.8

#    保存退出之后，要重启网卡，如果还不行，就reboot服务器试下
[root@localhost network-scripts]# systemctl restart network
[root@localhost network-scripts]#

#    要使用route命令，使用yum install -y net-tools进行安装

[root@localhost log]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.249.2   0.0.0.0         UG    100    0        0 ens32
192.168.249.0   0.0.0.0         255.255.255.0   U     100    0        0 ens32
[root@localhost log]#
```

  - 广播地址
    - x.x.x.255
  - lo
    - loopback，回环
    - 表示环回网卡，127.0.0.1一般表示本机
  - DHCP
    - 动态主机控制协议，是用来实现ip地址自动分配的协议
    - 配置主机IP的两种方法：
      - 动态分配
      - 配置静态IP

2、启用、禁用网络接口

- ifconfig eth0 down，禁用eth0接口
- ifconfig eth0 up，启用eth0接口
- service network start   #   servcie一般是centos6 上的系统管理命令，centos7 一般都是systemctl
- systemctl start network
- systemctl restart network
- systemctl status network
- systemct stop network

3、free

- free -m   查看内存使用

4、top

- top， 可以实时的监控服务器的cpu和内存使用情况

5、ping

- windows上的ping
- linux上的ping
    - ping -c 5 www.baidu.com

```
#    指定ping几次，用-c  几次
[root@localhost ~]# ping -c 3 www.baidu.com
PING www.baidu.com (39.156.66.18) 56(84) bytes of data.
64 bytes from 39.156.66.18 (39.156.66.18): icmp_seq=1 ttl=52 time=37.0 ms
64 bytes from 39.156.66.18 (39.156.66.18): icmp_seq=2 ttl=52 time=38.8 ms
64 bytes from 39.156.66.18 (39.156.66.18): icmp_seq=3 ttl=52 time=37.3 ms

--- www.baidu.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 37.094/37.753/38.855/0.784 ms
[root@localhost ~]#
```

6、lsof

- lsof
    - ssh, 默认22
    - ftp, 默认21
    - tomcat, 默认8080
    - nginx, 默认80
    - mysql, 默认3306

    - lsof -i:端口 ，作用是查看端口是否被占用，只要查询有结果就证明端口被占用了
        - **yum install -y lsof**
        - lsof -i:80
- **netstat**
    - **netstat -tnl**
        - 查看应用程序的，可以看到端口，可以直观的展示当前运行着的**tcp**程序

```
[root@localhost ~]# netstat -tnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:25                  :::*                    LISTEN
tcp6       0      0 :::3306                 :::*                    LISTEN
[root@localhost ~]#
```

- **ss -tnl**
    - **ss命令比netstat要快些**

```
[root@localhost ~]# ss -tnl
State      Recv-Q Send-Q Local Address:Port               Peer
Address:Port
LISTEN     0      128                *:22                          *:*
LISTEN     0      100     127.0.0.1:25                          *:*
LISTEN     0      128                *:80                          *:*
LISTEN     0      128             [::]:22                       [::]:*
LISTEN     0      100         [::1]:25                       [::]:*
LISTEN     0      80           [::]:3306                     [::]:*
[root@localhost ~]#
```

- ifconfig -s
    - 显示网络数据包统计详细

```
#    lsof 查看80端口是否被占用
[root@localhost ~]# lsof -i:80
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
nginx   12386   root    6u  IPv4 266134      0t0  TCP *:http (LISTEN)
nginx   12387 nobody    6u  IPv4 266134      0t0  TCP *:http (LISTEN)
[root@localhost ~]#
```

7、配置静态ip

- 配置不同的ip临时方案
    - ifconfig eth0 192.168.1.100 netmask 255.255.255.0 up
    - ifconfig eth0:1 192.168.1.101 netmask 255.255.255.0 up
    - ifconfig eth0:2 192.168.1.102 netmask 255.255.255.0 up
    - 一块网卡配置多个ip地址
- 临时方案重启失效

```
[root@localhost ~]# ifconfig ens33:2 192.168.4.104 netmask 255.255.255.0 up
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.102  netmask 255.255.255.0  broadcast 192.168.4.255
        inet6 fe80::298f:a30f:c5f9:1de5  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:66:56:d2  txqueuelen 1000  (Ethernet)
        RX packets 540865  bytes 388303869 (370.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 184544  bytes 29174033 (27.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


ens33:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.103  netmask 255.255.255.0  broadcast 192.168.4.255
        ether 00:0c:29:66:56:d2  txqueuelen 1000  (Ethernet)


ens33:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.104  netmask 255.255.255.0  broadcast 192.168.4.255
        ether 00:0c:29:66:56:d2  txqueuelen 1000  (Ethernet)


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 433  bytes 43517 (42.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 433  bytes 43517 (42.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]#
```

8、linux抓包与分析

- tcpdump
    - 一般不会用这个去抓包，借助抓包软件比如fiddler，wireshark，charles等

    - 渗透测试工具，burpsuite

9、远程工具

- xshell、putty、secureCRT、finalShell
    - ssh命令
        - ssh root@192.168.0.200
        - exit

```
[root@localhost ~]# ssh root@192.168.4.102
The authenticity of host '192.168.4.102 (192.168.4.102)' can't be established.
ECDSA key fingerprint is SHA256:wIDBUJluIzwWTGcH+UDbHXGBbj8kAHtB642FJBICl5Q.
ECDSA key fingerprint is MD5:4d:f9:22:7e:7b:98:45:37:fb:0c:c1:9c:ef:c4:b1:33.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.4.102' (ECDSA) to the list of known hosts.
root@192.168.4.102's password:输入密码
Last login: Fri Apr 29 14:46:36 2022 from 192.168.4.208
i'm coming...........
[root@localhost ~]# pwd
/root
[root@localhost ~]# exit
logout
Connection to 192.168.4.102 closed.
[root@localhost ~]#
```

- winscp、filezilla、xftp
- scp
    - scp xxx root@192.168.0.100:/root/xxx
    - scp root@192.168.0.100:/root/xxx xxx

```
#    拷贝本地文件到远程服务器
[root@localhost ~]# scp dos2unix-7.4.0-3.2.al8.x86_64.rpm
root@192.168.4.102:/tmp/
root@192.168.4.102's password:
dos2unix-7.4.0-
3.2.al8.x86_64.rpm                    100%  241KB  35.0MB/s   00:00
[root@localhost ~]# cd /tmp/
[root@localhost tmp]# ls
dos2unix-7.4.0-3.2.al8.x86_64.rpm
ks-script-5YqHE8
systemd-private-446139cdc96648c6b6bf2d9db3379db1-chronyd.service-YgBsvR
test
vmware-root_666-2731021219
vmware-root_668-2731152292
vmware-root_673-3988556249
vmware-root_675-3980232795
vmware-root_677-3980363868
vmware-root_689-4021587913
yum.log
yum_save_tx.2022-04-29.10-38.R0phhu.yumtx
[root@localhost tmp]#

#    反方向的传输，就是我要从别的服务器拷贝文件到我本地
[root@localhost ~]# scp root@192.168.4.102:/tmp/dos2unix-7.4.0-3.2.al8.x86_64.rpm
/test/
root@192.168.4.102's password:
dos2unix-7.4.0-
3.2.al8.x86_64.rpm                    100%  241KB  24.4MB/s   00:00
[root@localhost ~]# cd /test/
[root@localhost test]# ls
aaa.zip                            file_by_jerry  functions_m1.zip  root.zip
dos2unix-7.4.0-3.2.al8.x86_64.rpm  file_by_tom    jerry1            var.zip
file1.gz                           functions      jerry_file
file2                              functions.gz   root
[root@localhost test]# ll
total 69424
```

```
-rw-r--r--. 1 root root        474 Apr 28 17:22 aaa.zip
-rw-r--r--. 1 root root     247180 Apr 29 15:44 dos2unix-7.4.0-3.2.al8.x86_64.rpm
-rw----r--. 1 tom  root         38 Apr 28 16:07 file1.gz
-rw-r--r--. 1 tom  root          0 Apr 28 16:02 file2
-rw-rw-r--. 1 tom  root          0 Apr 28 16:13 file_by_jerry
-rw-r--r--. 1 tom  root          0 Apr 28 16:36 file_by_tom
-rw-r--r--. 1 root root      18281 Apr 28 17:17 functions
-rw-r--r--. 1 root root       5112 Apr 28 17:04 functions.gz
-rw-r--r--. 1 root root       5252 Apr 28 17:20 functions_m1.zip
drwxrwxr-x. 3 tom  group1       56 Apr 28 17:10 jerry1
-rw-rw-r--. 1 tom  root          0 Apr 28 16:46 jerry_file
dr-xr-x---. 3 root root       4096 Apr 28 17:28 root
-rw-r--r--. 1 root root       7947 Apr 28 17:24 root.zip
-rw-r--r--. 1 root root   70782438 Apr 28 17:23 var.zip
[root@localhost test]#
```