

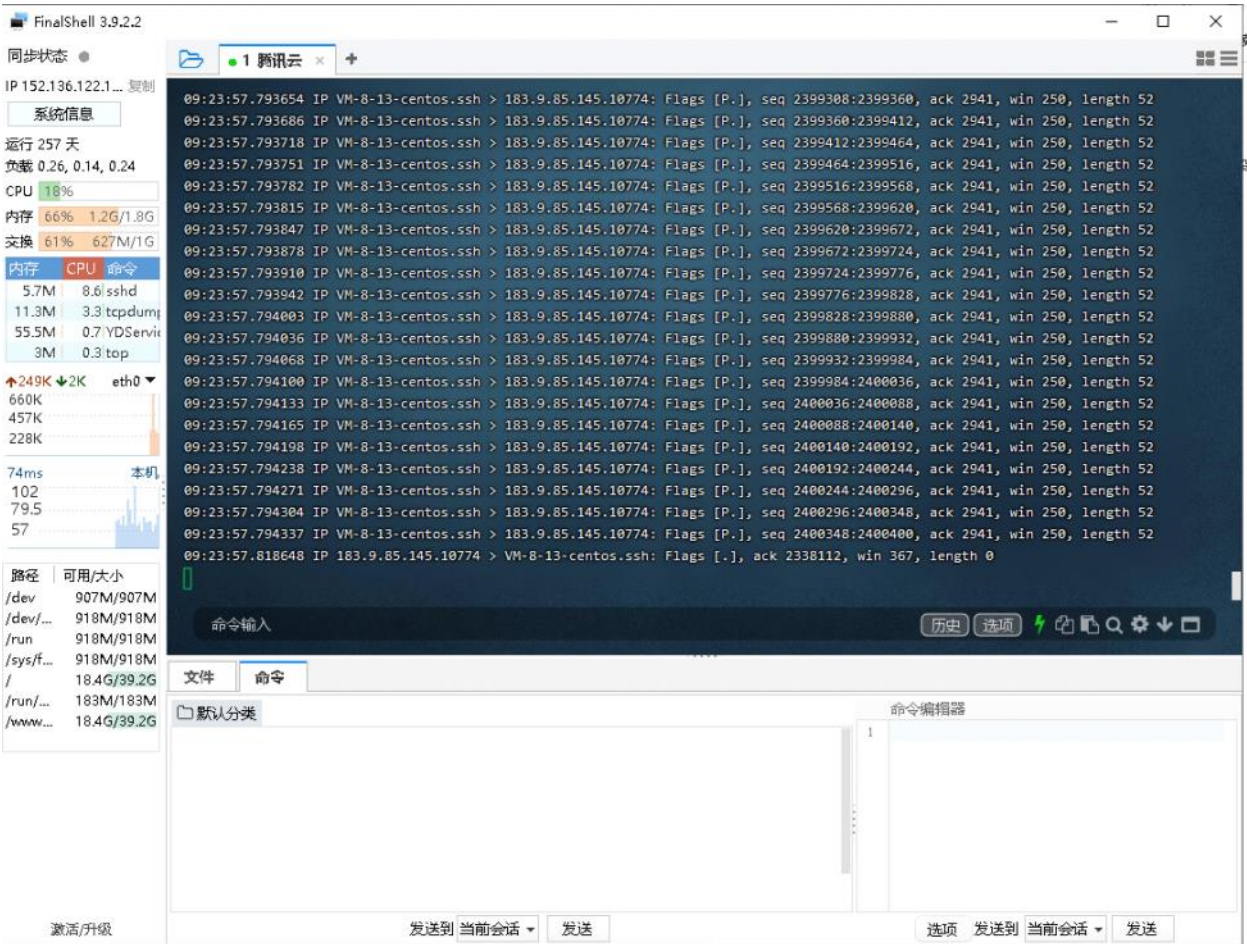
# tcpdump命令使用

2022年2月22日 9:19

## tcpdump命令使用

抓取指定网卡

1、使用tcpdump -i eth0命令，监视第一个网络接口eth0



抓取指定IP

1、使用tcpdump host 110.242.68.4命令，抓取指定IP网络报文





FinalShell 3.9.2.2

同步状态

IP 152.136.122.1... 复制

系统信息

运行 257 天

负载 0.08, 0.15, 0.16

CPU 9%

内存 66% 1.2G/1.8G

交换 61% 622M/1G

内存 CPU 命令

52.8M 0.7YDServ

41.9M 0.3BT-Pan

5.8M 0.3sshd

4.1M 0.3tat\_age

↑10K ↓2K eth0

14K

10K

5K

69ms

90

73.5

57

路径 可用/大小

/dev 907M/907M

/dev/... 918M/918M

/run 917M/918M

/sys/f... 918M/918M

/ 18.4G/39.2G

/run/... 183M/183M

/www/... 18.4G/39.2G

激活/升级

1 腾讯云

[root@VM-8-13-centos ~]# tcpdump -i any -XO -vvv -s0 -w /root/'hostname'\_anyport.cap

tcpdump: listening on any, link-type LINUX\_SLL (Linux cooked), capture size 262144 bytes

^Zt 13743

[2]+ 已停止 tcpdump -i any -XO -vvv -s0 -w /root/'hostname'\_anyport.cap

[root@VM-8-13-centos ~]#

VM-8-13-centos\_anyport.cap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.8.13	183.9.85.145	SSH	172	Server: Encrypted packet
2	0.068039	183.9.85.145	10.0.8.13	TCP	56	10576 → 22 [ACK] Seq=1 A
3	0.476064	183.9.85.145	10.0.8.13	ICMP	44	Echo (ping) request id=
4	0.476097	10.0.8.13	183.9.85.145	ICMP	44	Echo (ping) reply id=
5	0.476103	183.9.85.145	10.0.8.13	ICMP	44	Echo (ping) request id=
6	0.476107	10.0.8.13	183.9.85.145	ICMP	44	Echo (ping) reply id=
7	0.538143	183.9.85.145	10.0.8.13	ICMP	72	Destination unreachable

> Frame 1: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: 10.0.8.13, Dst: 183.9.85.145

> Transmission Control Protocol, Src Port: 22, Dst Port: 10576, Seq: 1, Ack: 1, Len: 116

> SSH Protocol

0000 00 04 00 01 00 06 52 54 00 86 e9 d1 00 08 00 .....RT.....

0010 45 10 00 9c 06 73 40 00 40 06 15 32 0a 00 0d E....s@. @..2....

0020 b7 09 55 91 00 16 29 50 b5 fb 76 e0 47 ac 48 e2 ..U....)P ..v.G.H.

0030 50 18 00 fa df f1 00 00 48 7a 46 f9 7b 9f fe db P.....HzF{...

0040 b7 61 83 83 6c 35 b3 91 e3 2b da 46 68 72 8f 4a -a..15...+Fhr-J

0050 54 9e af f8 0a cc cd 33 ef 01 6f c0 a1 39 ab 40 T.....3 ..o..9.@

0060 57 1a dd 94 3d 0a db 2d d5 5f 76 4d 8f 9b 42 d6 W.....\_vM..B.

0070 ac c1 06 37 27 77 37 40 5d 57 47 e1 e7 75 d2 a9 ...7'w7@ ]WG...u..

0080 a1 6a 57 74 75 29 24 91 79 2e e1 70 1f d6 3b d0 -jWtu)\$ .y.p...;

VM-8-13-centos\_anyport.cap

分组: 13733 · 已显示: 13733 (100.0%) 配置: Default

# yum命令使用

2022年2月22日 10:32

使用yum安装vim

yum install -y vim

```
[root@VM-8-13-centos ~]# yum install -y vim
已加载插件: fastestmirror, langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered with an entitlement server. You can use subscription-manager to register.

Repository epel is listed more than once in the configuration
Loading mirror speeds from cached hostfile
docker-ce-stable | 3.5 kB 00:00:00
epel | 4.7 kB 00:00:00
extras | 2.9 kB 00:00:00
os | 3.6 kB 00:00:00
updates | 2.9 kB 00:00:00
(1/2): epel/7/x86_64/updateinfo | 1.0 MB 00:00:00
(2/2): epel/7/x86_64/primary_db | 7.0 MB 00:00:00
软件包 2:vim-enhanced-7.4.629-8.el7_9.x86_64 已安装并且是最新版本
无须任何处理
[root@VM-8-13-centos ~]#
```

使用yum安装wget

yum install -y wget

```
[root@VM-8-13-centos ~]# yum install wget
已加载插件: fastestmirror, langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered with an entitlement server. You can use subscription-manager to register.

Repository epel is listed more than once in the configuration
Loading mirror speeds from cached hostfile
软件包 wget-1.14-18.el7_6.1.x86_64 已安装并且是最新版本
无须任何处理
[root@VM-8-13-centos ~]#
```

使用wget查询端口是否通

wget 110.242.68.3:80

```
[root@VM-8-13-centos ~]# wget 110.242.68.3:80
--2022-02-22 10:37:28-- http://110.242.68.3/
正在连接 110.242.68.3:80... 已连接。
已发出 HTTP 请求, 正在等待回应... 200 OK
长度: 2381 (2.3K) [text/html]
正在保存至: "index.html.5"

100%[=====] 2,381 --.-K/s 用时 0s

2022-02-22 10:37:28 (403 MB/s) - 已保存 "index.html.5" [2381/2381]

[root@VM-8-13-centos ~]#
```

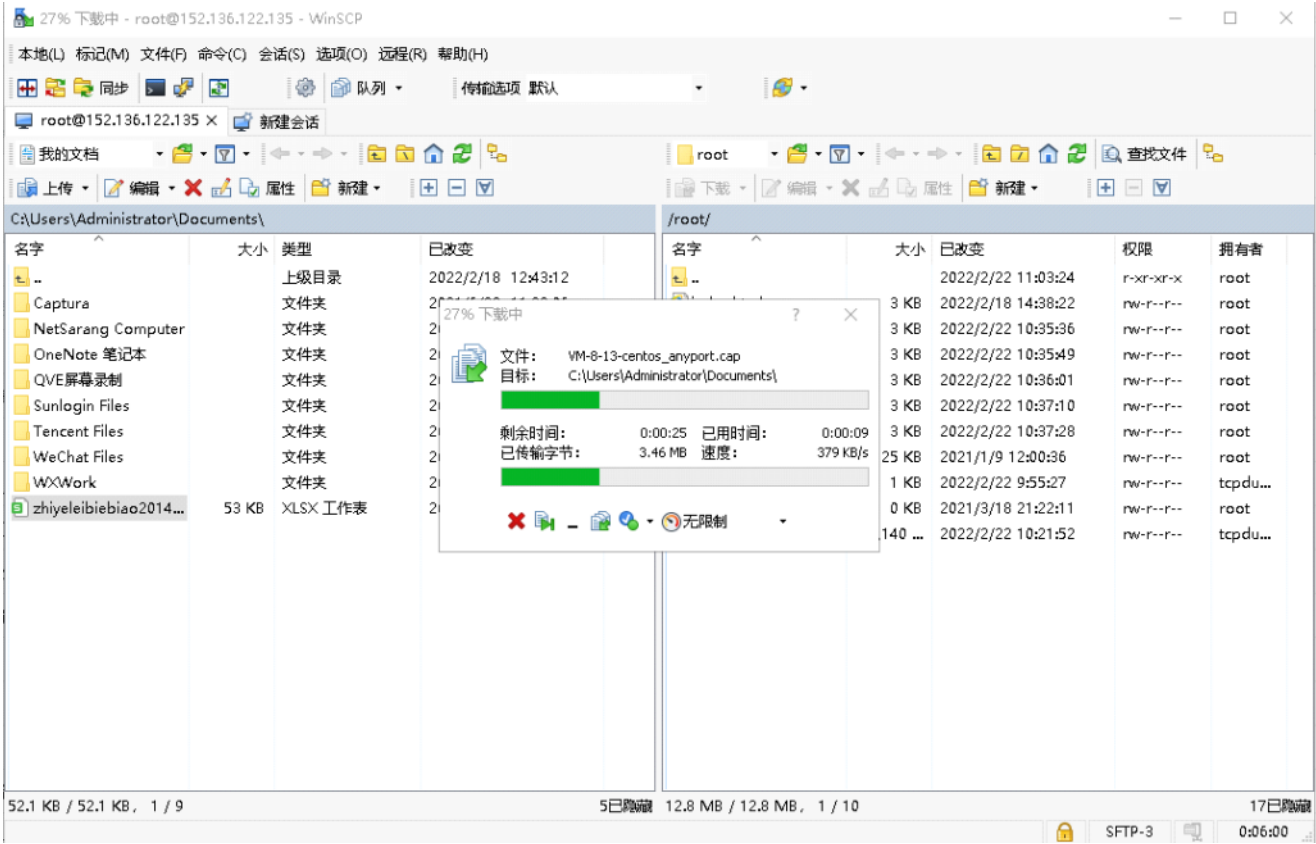




# 使用winscp工具

2022年2月22日 11:10

## 使用winscp工具实现windows和linux文件互传



# ps命令使用

2022年2月22日 11:14

根据ps命令参数使用，可查询当前服务器进程状态

使用命令ps au查询

```
root      25510  0.0  0.1 116864 3276 pts/0    Ss   11:04   0:00 -bash
root      25553  0.0  0.1 116864 3240 pts/1    Ss   11:04   0:00 -bash
root      25635  0.1  0.1 162816 3096 pts/1    S+   11:04   0:00 top

[root@VM-8-13-centos ~]# ps %cpu
error: garbage option

Usage:
ps [options]

Try 'ps --help <simple|list|output|threads|misc|all>'
or 'ps --help <s|l|o|t|m|a>'
for additional help text.

For more details see ps(1).
[root@VM-8-13-centos ~]# ps au
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1453  0.0  0.0 110208  644 ttyS0    Ss+   2021   0:00 /sbin/agetty --keep-baud 115200,38400,9600 ttyS0 vt220
root      5363  0.0  0.0 155452 1872 pts/0    R+    11:13   0:00 ps au
root     24120  0.0  0.0   5976    0 pts/0    Ss+   2021   0:00 /bin/bash
root      25510  0.0  0.1 116864 3276 pts/0    Ss   11:04   0:00 -bash
root      25553  0.0  0.1 116864 3240 pts/1    Ss   11:04   0:00 -bash
root      25635  0.1  0.1 162816 3096 pts/1    S+   11:04   0:00 top
[root@VM-8-13-centos ~]#
```

再根据进程信息pid查询关联的网络信息

使用命令lsof -i | grep pid

```
[root@VM-8-13-centos ~]# lsof -i | grep 3367
nginx      3367    www    51u  IPv4 154981537      0t0  TCP *:cddbp (LISTEN)
nginx      3367    www    52u  IPv4 154981538      0t0  TCP *:http (LISTEN)
nginx      3367    www    53u  IPv4 154981539      0t0  TCP *:https (LISTEN)
[root@VM-8-13-centos ~]# lsof -i | grep 3367
```

或使用命令netstat -nap | grep pid

```
[root@VM-8-13-centos ~]# netstat -nap | grep 3367
tcp        0      0 0.0.0.0:888      0.0.0.0:*        LISTEN      3367/nginx: worker
tcp        0      0 0.0.0.0:443      0.0.0.0:*        LISTEN      3367/nginx: worker
tcp        0      0 0.0.0.0:80       0.0.0.0:*        LISTEN      3367/nginx: worker
unix  3      [ ]          STREAM  CONNECTED  478916289 3367/nginx: worker
unix  3      [ ]          STREAM  CONNECTED  478916290 3367/nginx: worker
```

# cat命令使用

2022年2月22日 13:40

使用cat filename 命令，找到需要查询的api接口配置文件进行查询（json文件）

```
[root@VM-8-13-centos ~]# cd ./data
[root@VM-8-13-centos data]# ls
policy.json
[root@VM-8-13-centos data]# cat policy.json
{
  "default": [
    {
      "type": "insecureAcceptAnything"
    }
  ],
  "transports": {
    "docker-daemon": {
      "": [{"type": "insecureAcceptAnything"}]
    }
  }
}
```

命令输入

文件	命令				
/data					
文件名	大小	类型	修改时间	权限	用户/用户组
policy.json	256 B	JSON 文件	2020/07/01 22:56	-rw-r--r--	root/root

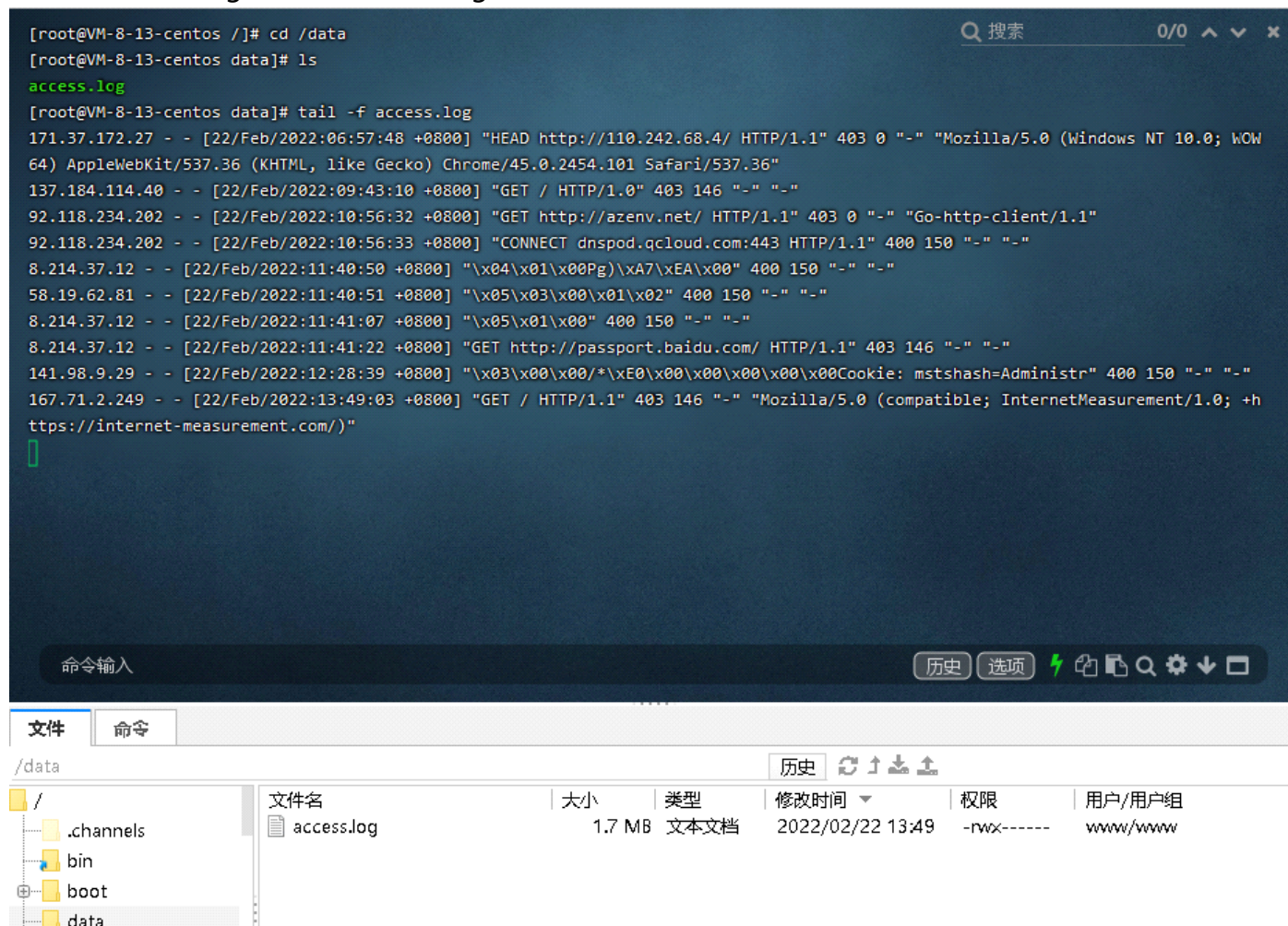


# tail&grep命令使用

2022年2月22日 11:21

使用tail命令，查询文件内容

例: tail -f access.log 循环查询access.log日志文件后10行内容



```
[root@VM-8-13-centos /]# cd /data
[root@VM-8-13-centos data]# ls
access.log
[root@VM-8-13-centos data]# tail -f access.log
171.37.172.27 - - [22/Feb/2022:06:57:48 +0800] "HEAD http://110.242.68.4/ HTTP/1.1" 403 0 "-" "Mozilla/5.0 (Windows NT 10.0; WOW
64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
137.184.114.40 - - [22/Feb/2022:09:43:10 +0800] "GET / HTTP/1.0" 403 146 "-" "-"
92.118.234.202 - - [22/Feb/2022:10:56:32 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [22/Feb/2022:10:56:33 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
8.214.37.12 - - [22/Feb/2022:11:40:50 +0800] "\x04\x01\x00Pg\xA7\xEA\x00" 400 150 "-" "-"
58.19.62.81 - - [22/Feb/2022:11:40:51 +0800] "\x05\x03\x00\x01\x02" 400 150 "-" "-"
8.214.37.12 - - [22/Feb/2022:11:41:07 +0800] "\x05\x01\x00" 400 150 "-" "-"
8.214.37.12 - - [22/Feb/2022:11:41:22 +0800] "GET http://passport.baidu.com/ HTTP/1.1" 403 146 "-" "-"
141.98.9.29 - - [22/Feb/2022:12:28:39 +0800] "\x03\x00\x00/*\xE0\x00\x00\x00\x00\x00Cookie: msthash=Administr" 400 150 "-" "-"
167.71.2.249 - - [22/Feb/2022:13:49:03 +0800] "GET / HTTP/1.1" 403 146 "-" "Mozilla/5.0 (compatible; InternetMeasurement/1.0; +h
tps://internet-measurement.com/)"
```

命令输入

历史 选项 闪电 打印 搜索 设置 窗口

文件 命令

/data

文件名	大小	类型	修改时间	权限	用户/用户组
access.log	1.7 MB	文本文件	2022/02/22 13:49	-rwx-----	www/www

同时，利用grep命令，查询该文件内所需要的字段

例: grep "92.118.234.202" access.log命令，查询关于IP 92.118.234.202有关的日志信息

```
^C 搜索 0/0 ^ v x
[root@VM-8-13-centos data]# grep "92.118.234.202" access.log
92.118.234.202 - - [27/Dec/2021:23:14:38 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:06:35:29 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:08:35:36 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:10:36:00 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:12:35:27 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:14:35:23 +0800] "GET http://azenv.net/ HTTP/1.1" 403 146 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:16:35:03 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:16:35:04 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [28/Dec/2021:18:35:03 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:18:35:03 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [28/Dec/2021:20:35:11 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:20:35:11 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [28/Dec/2021:22:35:15 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [28/Dec/2021:22:35:16 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [29/Dec/2021:04:39:01 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [29/Dec/2021:04:39:02 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [29/Dec/2021:07:33:38 +0800] "GET http://azenv.net/ HTTP/1.1" 403 0 "-" "Go-http-client/1.1"
92.118.234.202 - - [29/Dec/2021:07:33:40 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [29/Dec/2021:10:09:09 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [29/Dec/2021:11:53:28 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"
92.118.234.202 - - [29/Dec/2021:18:13:15 +0800] "CONNECT dnspod.qcloud.com:443 HTTP/1.1" 400 150 "-" "-"

命令输入 历史 选项 闪电 复制 粘贴 搜索 设置 下载 窗口
```



# sed&awk命令使用

2022年2月22日 14:06

## sed命令使用

1、使用命令 sed -e 4a\newline testfile 在第四行后添加新字符串

```
[root@VM-8-13-centos data]# ls
test.txt
[root@VM-8-13-centos data]# cat test.txt
HELLO LINUX!
Linux is a free unix-type operating system.
This is a linux testfile!
Linux test
[root@VM-8-13-centos data]# sed -e 4a\newline test.txt
HELLO LINUX!
Linux is a free unix-type operating system.
This is a linux testfile!
Linux test
newline
```

2、使用命令 nl testfile | sed '5d' 以行为单位的新增/删除

```
[root@VM-8-13-centos data]# nl test.txt | sed '5d'
 1 HELLO LINUX!
 2 Linux is a free unix-type operating system.
 3 This is a linux testfile!
 4 Linux test
```

3、使用命令 nl testfile | sed '4c No 4 number'以行为单位的替换与显示

```
[root@VM-8-13-centos data]# nl test.txt | sed '4c No 4 number'
 1 HELLO LINUX!
 2 Linux is a free unix-type operating system.
 3 This is a linux testfile!
No 4 number
```

## awk命令使用

1、使用命令 awk '[[pattern] action]' {filenames} 每行按空格或TAB分割，输出文本中的

1、3项



```
[root@VM-8-13-centos data]# ls
test.txt
[root@VM-8-13-centos data]# cat test.txt
HELLO LINUX!
Linux is a free unix-type operating system.
This is a linux testfile!
Linux test [root@VM-8-13-centos data]# awk '{print $1,$3}' test.txt
HELLO
Linux a
This a
Linux
[root@VM-8-13-centos data]#
```

## 2、使用命令awk -F, '{print \$1,\$2}' log.txt 使用","分割

```
[root@VM-8-13-centos data]# ls
test.txt
[root@VM-8-13-centos data]# cat test.txt
HELLO,LINUX!
Linux is a free unix-type operating system.
This,is,a,linux,testfile!
Linux test [root@VM-8-13-centos data]# awk -F, '{print $1,$2}' test.txt
HELLO LINUX!
Linux is a free unix-type operating system.
This is
Linux test
[root@VM-8-13-centos data]#
```