## 常用命令和技巧

### Scp

将本机文件复制到远程服务器上

scp /usr/local/kafka\_2.11-0.11.0.0/config/server.properties [app@172.25.6.11:/haha](mailto:app@172.25.6.11:/haha)

将远程服务器上的文件复制到本机

scp app@172.25.6.12:/usr/local/kafka\_2.11-0.11.0.0/config/server.properties /haha

可能会存在Scp 目录没有操作权限的问题

先将远程 复制到 /tmp目录，在从/tmp复制到目标目录

ssh dk@alidev10 切换节点

层级目录显示

tree -L 1 -L后面显示目录的层数

## 常用目录

### 修改dns

/etc/resolve.conf

### 网卡配置

Centos 6

/etc/sysconfig/network-scripts/ifcfg-eth0

Centos 7

vim /etc/sysconfig/network-scripts/ifcfg-ens33

IPADDR="168.33.222.123"

GATEWAY="168.33.222.2"

DNS1="202.96.134.133"

### 设置环境变量

修改/etc/profile

在末尾添加

export PATH=$PATH:/home/xyz/Tesseract/bin

然后执行source /etc/profile 使之立即生效

### 端口相关

添加

firewall-cmd --zone=public --add-port=80/tcp --permanent （--permanent永久生效，没有此参数重启后失效）

重新载入

firewall-cmd --reload

查看

firewall-cmd --zone= public --query-port=80/tcp

删除

firewall-cmd --zone= public --remove-port=80/tcp --permanent

### 防火墙相关

1、关闭firewall：

systemctl stop firewalld.service #停止firewall

systemctl disable firewalld.service #禁止firewall开机启动

firewall-cmd --state #查看默认防火墙状态（关闭后显示notrunning，开启后显示running）

2、iptables防火墙（这里iptables已经安装，下面进行配置）

vi/etc/sysconfig/iptables #编辑防火墙配置文件

# sampleconfiguration for iptables service

# you can edit thismanually or use system-config-firewall

# please do not askus to add additional ports/services to this default configuration

\*filter

:INPUT ACCEPT [0:0]

:FORWARD ACCEPT[0:0]

:OUTPUT ACCEPT[0:0]

-A INPUT -m state--state RELATED,ESTABLISHED -j ACCEPT

-A INPUT -p icmp -jACCEPT

-A INPUT -i lo -jACCEPT

-A INPUT -p tcp -mstate --state NEW -m tcp --dport 22 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -jACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 8080-j ACCEPT

-A INPUT -j REJECT--reject-with icmp-host-prohibited

-A FORWARD -jREJECT --reject-with icmp-host-prohibited

COMMIT

:wq! #保存退出

备注：这里使用80和8080端口为例。\*\*\*部分一般添加到“-A INPUT -p tcp -m state --state NEW -m tcp--dport 22 -j ACCEPT”行的上面或者下面，切记不要添加到最后一行，否则防火墙重启后不生效。

Systemctl restart iptables.service #最后重启防火墙使配置生效

Systemctl enable iptables.service #设置防火墙开机启动

### 获取命令执行的结果

用‘’号获取。``为tab键上面那个键

result=`echo “123”`

echo $result

执行结果

123

### 正则截取字符串

echo $url |sed 's#url=\(.\*\)#\1#g'

--使用子表达式（）时需要转意’\(\)’

--s表示替换

--g表示全局

### Sed打印文件第二行到N行

sed -n "2,1p" $file

sed -n ‘行号或行号描述p’ $file 打印文件第N行

sed -n ‘2，$p’ $file 打印文件第2行到最后行

### 获取文件行数

### cat $file | wc -l

### 字符串转数组和数组的遍历

**for((i=1;i<=10;i++))**

**for i in $(seq 1 10)**

**for i in {1..10}**

**${#argsParamArr[\*]}获取数组长度**

OLD\_IFS="$IFS"

IFS=","

arr=($a)

IFS="$OLD\_IFS"

for s in ${arr[@]}

do

echo "$s"

done

arr=($a)用于将字符串$a分割到数组$arr ${arr[0]} ${arr[1]} ... 分别存储分割后的数组第1 2 ... 项 ，${arr[@]}存储整个数组。变量$IFS存储着分隔符，这里我们将其设为逗号 "," OLD\_IFS用于备份默认的分隔符，使用完后将之恢复默认。

### 字符截取

# 号截取，从左边起开始匹配,匹配到字符的位置，删除左边字符，保留右边字符。

## 号截取，从左边起开始匹配,匹配到字符的位置，删除左边字符，保留右边字符

%号截取，从右边起开始匹配,匹配到字符的位置，删除左边字符，保留左边字符

%% 号截取，从右边起开始匹配,匹配到字符的位置，删除左边字符，保留左边字符

Eg：

假设有变量 var=http://www.aaa.com/123.htm

echo ${var#\*//}

即删除 http://

结果是 ：www.aaa.com/123.htm

### 单引号与双引号的区别