awk 搜索 过滤 文本

-F: {print $1 $3}

$0 $1 $2 $3 NR NF

awk 条件

正则 ~ !~

数字和字符

== != > >= < <=

&& ||

if(){}

for(i in $a){}

数组可以使用一个数组名称存储多个值

数组名[下标1]=值1

数组名[下标2]=值2

数组名[下标3]=值3

awk 'BEGIN{a[0]=10;a[1]=20;print a[1]}'

awk 'BEGIN{a[0]=10;a[1]=20;print a[0]}'

awk 'BEGIN{a["abc"]=10;a["xyz"]=20;print a["abc"]}'

awk 'BEGIN{a["abc"]=10;a["xyz"]=20;print a["xyz"]}'

awk 'BEGIN{a["abc"]="aabbcc";a["xyz"]="xxyyzz";print a["xyz"]}'

a[aaa]=4 a[192.168.0.1]=4

a[bbb]=2 a[192.168.0.2]=2

a[ccc]=1 a[192.168.0.3]=1

awk '{a[$1]++}END{for(i in a){print i,a[i]}}' txt4

192.168.0.1

192.168.0.1

192.168.0.2

192.168.0.3

192.168.0.1

192.168.0.2

192.168.0.1

准备测试环境:

yum -y install httpd //安装服务

netstat -ntulp | grep :80 //检查那个服务占用了80端口

/usr/local/nginx/sbin/nginx -s stop //如果是nginx需要关闭

killall nginx

systemc restart httpd //开启服务

echo 123 > /var/www/html/index.html //创建httpd的默认页面

curl http://172.25.0.10/index.html //测试

123

cat /var/log/httpd/access\_log //httpd的日志,每次被访问,都会添加新记录

yum -y install httpd-tools //ab工具安装包

ab -c 1 -n 50000 http://172.25.0.10/index.html //使用ab测试网站访问量,-c是用户数量, -n是访问次数

awk '{ip[$1]++}END{for(i in ip){print i,ip[i]}}' /var/log/httpd/access\_log //使用awk可以统计日志中的访问量

sort -r txt5 //sort排序 默认升序, -r降序

cpu负载,内存容量,硬盘空间,网卡流量,安装的软件包数量,账户数量,当前登录的账户数量

uptime | awk '{print "cpu平均负载是" $10,$11,$12}'

free -m | awk '/^Mem/{print "主机剩余内 存"$4"M"}'

df -h | awk '/vda1/{print "硬盘剩余空间 是"$4}'

ifconfig eth0 | awk '/RX p/{print "网卡eth0接收的数据量是"$5"字节"}'

p=`rpm -qa |wc -l`

echo "当前主机安装的软件包数量是$p"

awk '{x++}END{print "主机拥有账户总数是"x"个"}' /etc/passwd

x=`who |wc -l`

echo "当前登录账户数量是$x个"

psn=`ps aux |wc -l`

echo "主机运行的进程有$psn个"

================================

#!/bin/bash

while :

do

awk '{x++}END{print "主机拥有账户总数是"x"个"}' /etc/passwd

x=`who |wc -l`

echo "当前登录账户数量是$x个"

psn=`ps aux |wc -l`

echo "主机运行的进程有$psn个"

uptime | awk '{print "cpu平均负载是" $10,$11,$12}'

free -m | awk '/^Mem/{print "主机剩余内 存"$4"M"}'

df -h | awk '/vda1/{print "硬盘剩余空间 是"$4}'

ifconfig eth0 | awk '/RX p/{print "网卡eth0接收的数据量是"$5"字节"}'

p=`rpm -qa |wc -l`

echo "当前主机安装的软件包数量是$p"

sleep 2

clear

done

192.168.0.1 Failed /var/log/secure

192.168.0.1 Failed /var/log/secure

awk '/Failed/{ip[$11]++}END{for(i in ip){print i,ip[i]}}' /var/log/secure

编写监控脚本,如果查到有人访问本机密码输错超过三次则发邮件通知管理员

#!/bin/bash

x=`awk '/Failed/{ip[$11]++}END{for(i in ip){print i","ip[i]}}' /var/log/secure`

for i in $x

do

p=${i%,\*} //变量p内容是ip

s=${i#\*,} //变量s内容是输错密码的次数

[ $s -gt 3 ] && echo "报警! $p访问本机失败了$s次,赶紧处理

" | mail -s test root

done