日志审计与分析-日志筛选

实验目的：使用linux 下grep 命令筛选登录日志

1、练习使用grep命令

grep命令的作用？

Linux系统中grep命令是一种强大的文本搜索工具，它能使用正则表达式搜索文本，并把匹配的行打印出来。grep全称是Global Regular Expression Print，表示全局正则表达式版本，它的使用权限是所有用户。

grep命令的常用参数都有哪些？

grep [options]

主要参数:

[options]主要参数：

－c：只输出匹配行的计数。

－I：不区分大 小写(只适用于单字符)。

－h：查询多文件时不显示文件名。

－l：查询多文件时只输出包含匹配字符的文件名。

－n：显示匹配行及行号。

－s：不显示不存在或无匹配文本的错误信息。

－v：显示不包含匹配文本的所有行。

pattern正则表达式主要参数：

： 忽略正则表达式中特殊字符的原有含义。

^：匹配正则表达式的开始行。

$: 匹配正则表达式的结束行。

<：从匹配正则表达 式的行开始。

>：到匹配正则表达式的行结束。

[ ]：单个字符，如[A]即A符合要求 。

[ - ]：范围，如[A-Z]，即A、B、C一直到Z都符合要求 。

。：所有的单个字符。

- ：有字符，长度可以为0。

2、使用grep筛选出linux系统的成功和失败登录日志

主要日志有：

/var/log/btmp 记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看

/var/log/wtmp 永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看

登录失败记录：/var/log/btmp //lastb

最后一次登录：/var/log/lastlog //lastlog

登录成功记录: /var/log/wtmp //last

目前登录用户信息：/var/run/utmp //w、who、users

登录日志记录：/var/log/secure

文本

描述已自动生成

筛选登陆失败的日志：



无。因为我从未登录失败过。

筛选登录成功的日志：

文本

描述已自动生成

3、思考：如何定期备份日志？

可以编写一个备份脚本

4、查阅资料：什么是linux环境变量，设置环境变量的方法都有哪些？

在 Linux 系统中，环境变量是用来定义系统运行环境的一些参数，比如每个用户不同的家目录（HOME）、邮件存放位置（MAIL）等。

设置环境变量的方法：

Linux export 命令用于设置或显示环境变量。

export 　[-fnp][变量名称]=[变量设置值]

1. 修改.bashrc文件：vim ~.bashrc

在里面加入：export PATH="$PATH:/usr/local/arm/bin"

1. 修改 /etc/profile：vim /etc/profile

在里面加入：export PATH="$PATH:/usr/local/arm/bin"

以上两种方法需要重新注销系统才能生效，最后可以通过下面两个命令测试：

echo $PATH

arm-linux-gcc -v