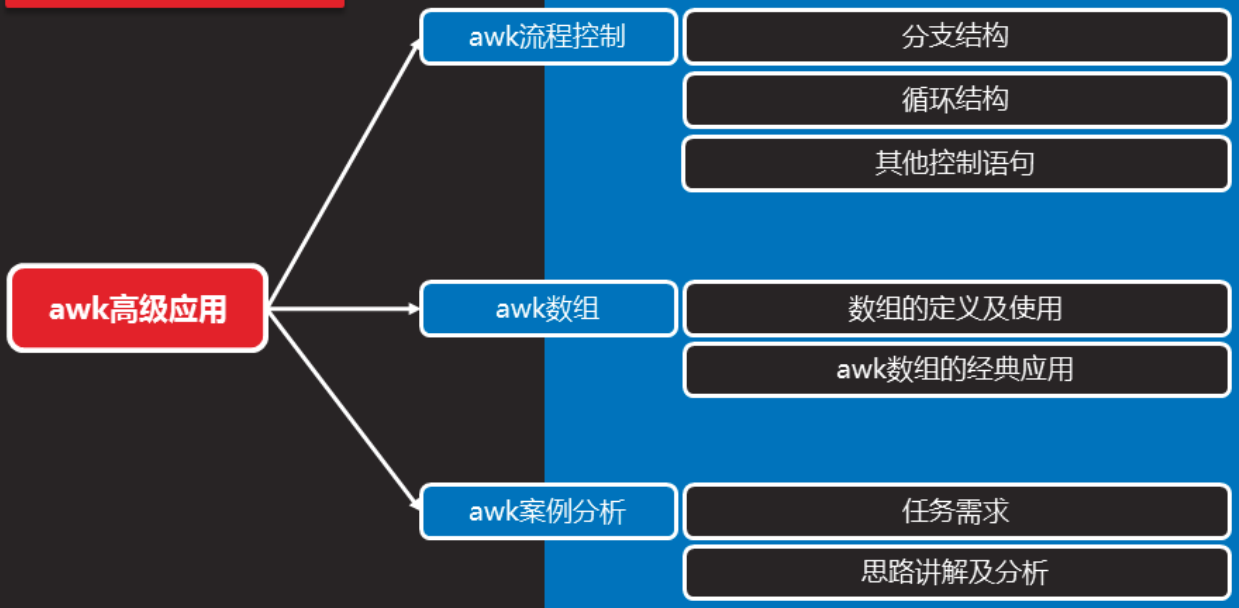

Tedu.cn
达内教育
Shell脚本编程
NSD SHELL
DAY06

内容

上午	09:00 ~ 09:30	作业讲解与回顾
	09:30 ~ 10:20	awk高级应用
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	综合案例
	15:00 ~ 15:50	
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

awk高级应用



awk流程控制

分支结构

知识讲解

- 单分支
  - if(条件){编辑指令}
- 双分支
  - if(条件){编辑指令1}else{编辑指令2}
- 多分支
  - if(条件){编辑指令1}else if(条件){编辑指令2}.. ..
    else{编辑指令N}

分支结构（续1）

Tedu.cn 达内教育

- 应用示例
  - 统计UID小于或等于500的用户个数
  - 统计UID大于500的用户个数

知识讲解

```
[root@svr5 ~]# awk  -F:  'BEGIN{i=0;j=0}{if($3<=500){i++} \
else{j++}}END{print i,j}'  /etc/passwd
37   22
```

Tedu.cn 达内教育

awk数组

数组的定义及使用

知识讲解

- 定义数组
  - 格式：数组名[下标]=元素值
- 调用数组
  - 格式：数组名[下标]
- 遍历数组
  - 用法：for(变量 in 数组名){print 数组名[变量]}

数组的定义及使用（续1）

知识讲解

- 用法示例：
  - 为数组name赋值两个元素，值分别为jim、tom

```
[root@svr5 ~]# awk 'BEGIN{name[0]="jim";name[1]="tom"; print
name[0],name[1]}'
jim tom
```

Tedu.cn 达内教育

案例1：awk流程控制

- if分支结构（双分支、多分支）
- 练习awk数组的使用

课堂练习

Tedu.cn 达内教育

awk案例分析

任务需求

Tedu.cn 达内教育

知识讲解

- 针对Web访问日志计算访问量排名
  - 获得结果：客户机的地址、访问次数
  - 按照访问次数排名

```
[root@svr5 ~]# less  /var/log/httpd/access_log
192.168.4.5 - - [08/May/2015:10:35:27 +0800] "GET /pxe/centos6
HTTP/1.1" 404 287 "-" "ELinks/0.12pre5 (textmode; Linux; 79x21-2)"
192.168.4.110 - - [08/May/2015:10:35:58 +0800] “GET / HTTP/1.1”
403 3985 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0;
rv:11.0) like Gecko LBBROWSER"
```

此Web日志中的第1个字段，即对应客户机的IP地址

思路讲解及分析

Tedu.cn 达内教育

知识讲解

- 利用awk提取客户机IP地址、计算访问次数
  - 以$1做下标，定义数组ip
  - 最后利用for循环输出数组下标、对应数组元素的值

```
awk  ' {ip[$1]++} END{for(i in ip) {print ip[i],i}}'  /var/log/httpd/access_log
```

思路讲解及分析（续1）

Tedu.cn 达内教育

知识讲解

- 利用sort对提取结果排序
  - -n：按数字升序排列
  - -k：针对指定的列进行排序
  - -r：反向排序

```
awk  '{ip[$1]++} END{for(i in ip) {print ip[i],i}}' .. .. | sort  -nr
```

案例2：awk扩展应用

Tedu.cn 达内教育

课堂练习

1. 分析Web日志的访问量排名，要求如下：
   - 获得结果：客户机的地址、访问次数
   - 按照访问次数排名

综合案例

Tedu.cn
达内教育

监控脚本

任务需求

Tedu.cn 达内教育

知识讲解

- 编写脚本监控本机各项数据指标：
  - CPU负载
  - 网卡流量
  - 内存剩余容量
  - 磁盘剩余容量
  - 计算机账户数量
  - 当前登录账户数量
  - 计算机当前开启的进程数量
  - 本机已安装的软件包数量

思路讲解及分析

Tedu.cn 达内教育

知识讲解

- 思路：
  - uptime
  - ifconfig
  - fee
  - df
  - cat /etc/passwd
  - ps aux
  - rpm -qa

案例3：编写监控脚本

- 编写监控脚本，监控如下数据项目：
  - CPU负载
  - 网卡流量
  - 内存剩余容量
  - 磁盘剩余容量
  - 计算机账户数量
  - 当前登录账户数量
  - 计算机当前开启的进程数量
  - 本机已安装的软件包数量

课堂练习

安全检测脚本

任务需求

Tedu.cn 达内教育

知识讲解

- 防止远程ssh暴力破解密码
  - 检测ssh登录日志，如果远程登陆账号名错误3次，则屏蔽远程主机的IP
  - 检测ssh登录日志，如果远程登陆密码错误3次，则屏蔽远程主机的IP

思路讲解及分析

Tedu.cn 达内教育

知识讲解

- 思路：
  - ssh登录日志为/var/log/secure
  - 分析日志文件格式
  - 找出用户名以及密码错误的规律，并提取有效数据
  - 对有效数据进行汇总统计，实现黑名单过滤功能

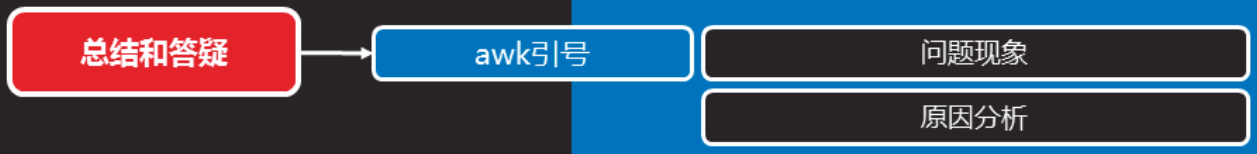
案例4：编写安全检测脚本

Tedu.cn 达内教育

课堂练习

- 防止远程ssh暴力破解密码
  - 检测ssh登录日志，如果远程登陆账号名错误3次，则屏蔽远程主机的IP
  - 检测ssh登录日志，如果远程登陆密码错误3次，则屏蔽远程主机的IP

总结和答疑



awk引号

问题现象

知识讲解

- 故障错误信息

```
[root@svr5 ~]# awk -F: "{print $1,$3}" /etc/passwd |head -2
awk: cmd. line:1: {print ,}
awk: cmd. line:1:        ^ syntax error
```

原因分析

Tedu.cn 达内教育

知识讲解

- 分析故障
  - 报错信息：awk: cmd. line:1:　　^ syntax error
- 分析故障原因
  - awk的条件和指令需要使用单引号