**已知：新奇科技公司的apache的访问日志存放在/data/log/httpd/access\_log文件中，要求每天凌晨0:30从日志文件中分析出以下内容并追加记录到/root/httpdlog/日期/result.txt文件中,并上传到远程服务器。**

**1.访问次数最多的前10个ip**

**2.访问次数最多的前10个页面**

**3.访问次数最多的前10个jpg页面**

**4.访问次数最多的10个时间段**

**5.传输字节超过10k的文件**

**6.包含baraja的行**

**前提：做ssh无密钥登录**

**步骤：1.ssh-keygen**

**2.scp /root/.ssh/id\_rsa.pub root@172.18.5.247:/root/.ssh/authorized\_keys**

**3.测试 ssh 172.18.5.247**

**脚本**

**#!/bin/bash**

**#定义日志文件**

**log=/data/log/httpd/access\_log**

**#log=/var/log/httpd/access\_log-20170109**

**#定义日期**

**date=`date +%Y%m%d`**

**#定义备份目录**

**bakdir=/root/httpdlog/$date**

**if [ ! -d $bakdir ];then**

**mkdir -p $bakdir**

**fi**

**#定义结果文件**

**file=$bakdir/result.txt**

**#将访问次数最多的前10个ip追加到结果文件中**

**echo "访问次数最多的前10个ip">>$file**

**cat $log|awk '{print $1}'|sort|uniq -c|sort -rn|head -10>>$file**

**#访问次数最多的前10个页面**

**echo "访问次数最多的前10个页面:">>$file**

**cat $log|awk '{print $7}'|sort|uniq -c|sort -rn|head -10>>$file**

**#包含baraja的行**

**echo "包含baraja的行:">>$file**

**cat $log|grep baraja>>$file**

**echo "传输字节超过10k的文件:"**

**cat $log|awk '$10>10000{print $7}'|sort|uniq -c>>$file**

**echo访问次数最多的前10个jpg页面>>$rfile**

**cat $log|awk '{print $7}'|grep jpg|sort|uniq -c|sort -rn|head -10>>$file**

**echo访问次数最多的10个时间段>>$rfile**

**cat $log|awk -F: '{print $2":"$3}'|sort|uniq -c|sort -rn|head -10>>$file**

**#上传到远程服务器**

**scp $file root@172.18.5.147:/root**

**#!/bin/bash**

**logfile=/data/log/httpd/access\_log**

**rfile=/root/httpdlog/result.txt**

**echo 访问次数最多的前10个ip>>$rfile**

**cat $logfile|awk '{print $1}'|sort|uniq -c|sort -rn|head -10>>$rfile**

**echo访问次数最多的前10个页面>>$rfile**

**cat $logfile|awk '{print $7}'|sort|uniq -c|sort -rn|head -10>>$rfile**

**echo传输字节超过10k的文件>>$rfile**

**cat $logfile|awk '$10>10000{print $7}'|sort|uniq>>$rfile**

**i**

**echo包含baraja的行>>$rfile**

**cat $logfile|grep "baraja">>$rfile**