



**说明：** 这部分面试题是内部教材《面试宝典》的前 5 套，要想获取更多资料，请加阿铭老师微信号 [81677956](#)。或者关注公众号 [aming\\_linux](#)。加 QQ 群 [246401509](#) 讨论 Linux。

## 第 1 套

1. Linux 系统中 DNS 服务进程名为 ( A )

A . named    B.httpd    C.ftpd    D.SysLog

2.在 UINX/Linux 中，系统 Root 用户口令信息一半保存的文件夹是 ( D )

A . autobat    B.service.conf    C.inetd.conf    D.shadow

3. 在下列选项中，属于 Linux 系统日志服务的是 ( D )

A . named    B.httpd    C.ftpd    D.SysLog

4.Linux 操作系统支持的文件系统类型是 ( A )

A、 EX3    B.NFT    C.TXT    D.FAT

5.在 UINX 系统中输入命令 “ls-al test” 显示如下” -rwx--xr-x 1 root root 100 2013-12-20 23:51 test” 对它的含义解释错误的是 ( D )

A . 这是一个文件，而不是目录

B . 文件的拥有者可以对这个文件进行读、写和执行的操作

C . 文件所属成员有可以读它，也可以执行它

D、其他所有用户只可以执行它

6.在大多数 Linux 发版版本中，一下那个属于块设备 ( B )

A、 串行口 B、 硬盘 C、 虚拟终端 D、 打印机

7.怎样了解您在当前目录下还有多大空间 ( D )

A . use df    B. use du /    C. use du .    D. use df .



8.一下关于 Linux 超级权限的说明，不正确的是（ C ）

A.一般情况下，为了系统的安全，对于一般常规级别的应用，不需要 root 用户来操作完成

B.普通用户可以通过 su 和 sudo 来获得系统的超级权限

C.对于系统日志的管理，添加和删除用户等管理工作，必须以 root 用户登录才能进行

D . root 是系统的超级用户，无论是否为文件和程序的所有者都具有访问权限

9.REDHAT9.0 的防火墙软件是哪个（ B ）

A . ipchains   B.iptables   C.ISA   D.checkpoint

10 . 显示文件头部的命令是（ C ）

A . fidsk   B.mount   C.head   D.man

11.删除文件的命令是（ B ）

A . mkdir   B.rm   C. mv   D. remove

12.显示用户的 ID，以及所属组的 ID，要使用命令是（ C ）

A . su   B.who   C.id   D. man

13.Linux 根分区的文件系统是（ C ）

A . FAT16   B.FAT32   C.EXT3   D.NTFS

14 . Linux 的 DNS 服务是下列哪个（ C ）

A . host   B.hosts   C. bind   D.vsftp

15.不能用来关机的命令是（ D ）

A.shutdown   B.halt   C.init   D.logout

16.一下那个命令修改 SAMBA 口令（ A ）

A . smbpasswd   B.passwd   C.smbpassword   D.password



17./dev/ethX 表示 ( B )

A . 系统回送接口 B.以太网接口设备 C.令牌环网设备 D.PPP 设备

18.GRUB 的配置文件是 ( C )

A./etc/grub B./boot.ini C./etc/grub.conf D./etc/inittab

19.我们将逻辑分区建立在 ( B ) 分区上

A . 从分区 B.扩展分区 C.主分区 D.第二分区

20.使用 iptables 拒绝来自 10.10.10.1.访问的正确写法是 ( C )

A.iptables -I INPUT -s 10.10.10.1 -j ACCEPT

B. iptables -A INPUT -D 10.10.10.1 -j DROP

C. iptables -I INPUT -s 10.10.10.1 -j DROP

D. iptables -A INPUT -s 10.10.10.1 -j ACCEP

21.init 是 Linux 的第一个程序, 该程序是根据文件(B)来建立子进程的

A./etc B./etc/inittab C./etc/modules.conf D./etc/lilo.conf

22.不是 shell 具有的功能特点是 ( C )

A.管道 B.输入输出重定向 C.监视系统 D.解释程序命令

23.如果你的 umask 设为 022 , 则你创建文件的缺省权限是 ( D )

A.——w——w— B. —w——w—— C.r——xr—x—— D.rw—r——r——

24 . 为了修改文件 test 的许可模式, 使其文件属性具有读、写和运行的权限, 组和其他用户可以读和运行, 可以采用 ( A ) 方法

A . chmod 755 test B. chmod 700 test C. chmod +rwx test D.chmod g-w test

25.统计文件占用磁盘空间, 我们可以使用命令 ( B )

A . df B.du C.mount D. in



26 在 SHELL 程序里，判断文件不存在的写法是（ A ）

- A . if [ ! -f "\$myfile" ];then     B.if [-d "\$myfile" ];then  
C.if [-f "\$myfile" ];then     D. if [! -d "\$myfile" ];then

27.使用 tcpdump 监听 eth0 的 80 端口网络数据的正确命令是（ D ）

- A . tcpdump -n eth0 port! 80     B. tcpdump -ni eth0 port=80  
C. tcpdump -i eth0 port ! 80     D. tcpdump-ni eth0 port 80

28.SQL 中，下列操作有语法错误的是（ D ）

- A . AGE IS NOTNULL     B. NOT (AGE IS NULL)  
C. SNAME=' 王五'     D.SNAME=' 王%'

29.在 Mysql 中，下列关于创建数据库表的描述正确的是（ C ）

- A . 在创建表时必须设定列的约束  
B . 在删除表的时候通过列键的约束连接在一起的表会被一同删除  
C . 在创建表时必须设置列类型  
D . 通过 CREATE TABLE new\_t SELECT \* FROM old\_t 复制表的同时，表的约束能够一起被复制到新表中

30.SQL 中，“ AGE IN (20 , 22)” 的语义是（ A ）

- A.AGE<=22 AND AGE>=20     B. AGE<22 AND AGE>20  
C.AGE=20 AND AGE=22     D.AGE=20 OR AGE=22

31.下列对跨站脚本攻击（ XSS ）的解释最准确的一项是：（ D ）

- A.引诱用户点击虚假网络连接的一种攻击方法  
B . 构造精妙的关系数据库的结构化查询语言对数据库进行非法的访问  
C . 一种很强大的木马工具手段  
D . 将恶意代码嵌入到用户 WEB 网页中，从而达到恶意的目的



32.允许防火墙和某些路由器通过将地址引向不可信网络的方法来隐藏网络地址被称为？ B

A . 地址过滤    B.NAT    C.反转    D.IP 欺骗

33.局域网的网络地址 192.168.1.0/24 ,局域网络连接其他网络的网关地址是 192.168.1.1。

主机 192.168.1.20 访问 172.16.1.0/24 网络时，其路由设置正确的是 ( A )

A . route add -net 192.168.1.0 gw 192.168.1.1 netmask255.255.255.0 metric 1

B . route add -net 172.16.1.0 gw 192.168.1.1 netmask255.255.255.255 metric 1

C . route add -net 172.16.1.0 gw 172.16.1.1 netmask255.255.255.0 metric 1

D . route add default 192.168.1.0 gw 192.168.1.0 netmask172.168.1.1 metric 1

34.取 ls -l 输出结果的第 5 列的值的正确写法是 ( B )

A . ls -l |awk "{print\$5}"    B. . ls -l |awk '{print\$5}'

C.ls -l |awk {print\$5}    D.ls-l |awk 'print\$5'

35.在 vi 编辑器的命令模式中，删除一行的命令是 ( B )

A.yy    B.dd    C.pp    D.xx

36.有一个中学获得了 C 类网段的一组 IP192.168.1.0/24.要求你划分 7 个以上的子网，每

个子网主机数不得少于 25 台，请问子网掩码该怎么写？ B

A . 255.255.255.128    B.255.255.255.224

C.255.255.255.240    D.255.255.240.0

37.在三层交换机和路由器上，启用路由功能的命令是： D

A . ip router    B.enable route    C.start ip route    D.ip routing

38.什么命令解压缩 tar 文件 ( C )

A . tar -czcfilename.tar    B.tar -xzvffilename.tar

C.tar -tzvf filename.tar    D.tar -dzvf filename.tar



39.取 `ls -l` 输出结果的第 5 列的值的正确写法是 ( B )

A . `ls -l |awk "{print$5}"`      B. . `ls -l |awk '{print$5}'`

C.`ls -l |awk {print$5}`              D.`ls-l |awk 'print$5'`

40.显示 LINUX 内核版本号的命令是(B)

A.mkdir      B.uname -a      C.uname -e      D.linuxis

## 二 . 问答题

1.请分别详细写出如何在命令行下运行 PHP、C、java 程序的命令 , 程序名可用 test 代替 ?

答案 : PHP: `php test.php`

C: `gcc -o test test.c`

Java: `java test`

2. ftp 有几种模式 , 几种连接类型 , 有什么区别 ?

答案 : 分为主动模式与被动模式。主动为服务器发起 21 端口去访问客户端的随机端口 , 并通过服务器的 20 端口来传数据。被动模式正好相反 , 由客户端发起连接服务器的 21 端口 , 然后服务器随机开启一个数据连接端口来传数据。

3. 两台 Linux 服务器都只开放了 SSH 服务 , 端口号均为 999 , 你已使用 user1 登陆服务器

1.1.1.1 , 需要将 /home/user1/data.tar.gz 文件传送至服务器 2.2.2.2 用户名为: userB 目的目录为 /home/userB , 并将文件更名为 : dataB.tar.gz 请用一条命令完成上述任务 ( 密码不考虑 )

答 案 :    `rsync -av -e "ssh -p 999" /home/user1/data.tar.gz userB@2.2.2.2:/home/userB/dataB.tar.gz`



#### 4. 日志切分在运维中扮演着重要角色

现有 1 个 500G 的日志文件 A，时间跨度为 2013 年 1 月 25 日到 4 月 28 日。怎么获取其中 2 月某天时段的记录生成文件 B，注：操作服务器系统资源有限，请使用一条命令实现。

答案：假如日志每行都有时间标记，比如我们要获取的日期为 2013 年 2 月 10 日，日志中的日期表示是这样的“10/feb/2013:00:00:01”。那么答案为 `sed -rn '/10\feb\2013:/'`

`p A > B`

5. 现有 5000 行文本数据，用 vi 编辑器操作，需将文本中全部的 192.168.0.111 更改为 192.168.0.112，需将 1000 行至 1120 行的文本数据中的 aaa 更改为 bbb。请用两条命令实现

答案 `:1, $s/192.168.0.111/192.168.0.112/g`

`:1000, 1120s/aaa/bbb/g`

6. 一台 Linux 服务器 IP 为：192.168.0.8 只希望开放 TCP 80 端口，请写出 iptables 的设置命令

`iptables -A INPUT -p tcp -dport 80 -d 192.168.0.8 -j ACCEPT`

`iptables -A INPUT -p tcp -d 192.168.0.8 -j DROP`



## 第 2 套

1、用哪一个命令可以关机，而不重启 C

A、reboot    B、shutdown -r    C、halt    D、init 1

2、与磁盘无关的命令是？ A

A、free    B、du    C、df    D、mkfs

3、/etc/shadow 文件中存放？ B

A、用户账号基本信息    B、用户口令的加密信息

C、用户组信息    D、文件系统信息

4、配置 Apache 服务器需要修改的配置文件为？ A

A、httpd.conf    B、access.conf    C、srm.conf    D、named.conf

5、在 TCP/IP 模型中，应用层包含了所有的高层协议，在下列的一些应用协议中，——是能够实现本地与远程主机之间的文件传输工作。 B

A、telnet    B、FTP    C、SNMP    D、NFS

6、DNS 域名系统主要负责主机名和——之间的解析。 A

A、IP 地址    B、MAC 地址    C、网络地址    D、主机别名

7、建立一个新文件可以使用的命令为？ D

A、chmod    B、more    C、cp    D、touch

8、Apache 服务器默认的接听连接端口号是？ C

A、1024    B、800    C、80    D、8

9、设超级用户 root 当前所在目录为 /usr/local，键入 cd 命令后，用户当前所在目录为？

B

A、/home    B、/root    C、/home/root    D、/usr/local





10、将光盘 CD-ROM ( hdc ) 安装到文件系统的/mnt/cdrom 目录下的命令是？ C

A、mount /mnt/cdrom     B、mount /mnt/cdrom /dev/hdc

C、mount /dev/hdc /mnt/cdrom     D、mount /dev/hdc

11、一下哪个命令是 vi 编辑器中执行存盘退出的？ D

A、q     B、zz     C、:q!     D、:wq

12、下面选项中不属于 Linux 下常用的文件系统格式是哪个？ C

A、ext2     B、ext3     C、NTFS     D、xfs

13、mysql 的主从复制是通过什么方式完成数据同步的？ B

A、通过同步数据库表进行数据同步

B、通过同步日志文件回滚表数据

C、通过底层数据块同步进行同步

D、基于内存同步技术定时刷新数据到磁盘

14、在 ps 命令中什么参数使用来显示所有用户的进程的？ C

A、a     B、b     C、u     D、x

15、keepalived 是什么类型的集群软件？ B

A、负载均衡群集软件     B、高可用群集软件

C、高性能计算群集软件     D、存储群集软件

16、若一台服务器的内存为 16GB，则交换分区的大小通常是： A

A、32G     B、16G     C、0GB     D、4GB

17、Linux 操作系统中，cd ../..命令的作用是？ D

A、转到当前目录的上级     B、转到根目录

C、转到/root 目录     D、转到当前目录的上两级目录



18、按\_\_\_\_键能终止当前运行的命令 B

A、Ctrl-D    B、Ctrl-C    C、Ctrl-B    D、Ctrl-F

19、crontab 文件有 6 个域组成，每个域之间用空格分割，其排列如下： B

A、MIN HOUR DAY MONTH YEAR COMMAND

B、MIN HOUR DAY MONTH DAYOFWEEK COMMAND

C、COMMAND HOUR DAY MONTH DAYOFWEEK

D、COMMAND YEAR MONTH DAY HOUR MIN

20、在给定文件中查找与设定条件相符字符串的命令为？ A

A、grep B、gzip C、find D、sort

## 二、简答题

1、当一个一般文件权限为-rwxrwxrwx 则表示这个档案的意义为？我需要将一个文件的权限改为-rwxr-xr-- 请问该如何编写命令

答案：文件的权限为 777，所有用户拥有读写执行所有权限

```
chmod 754 file
```

2、如何用 mysqlq 命令进行备份和恢复？以 test 库为例。创建一个备份，并再用此备份进行恢复

答案：mysqldump -u root -p test > test.bak

```
mysql -u root -p < test.bak
```

3、写一个脚本查找最后创建时间是 3 天前，后缀是\*.log 的文件

答案：#!/bin/bash

```
find /var/log -name "*.log" -mtime +3
```



4、试简要的分析如下指令的区别 cat , tac、more、less、head、tail

答案：cat 正常显示文件

tac 按列逆向显示文件

more 分屏显示

less 分屏显示。支持查找，比 more 功能稍多

head 显示文件头。默认显示前 10 行

tail 显示文件尾。默认显示尾 10 行

5、有用户 manager、renshi、xingzheng，文件夹 renshi，xingzheng，要求 manager

用户可以查看并更改 renshi，xingzheng 文件夹下的文件，renshi 用户

答案：只能查看修改 renshi 文件夹，xingzheng 用户只能查看修改 xingzhengwenjian 加。

其他人不能访问改两个文件夹，问通过权限改如何实现

usermod -G renshi，xingzheng manager

chown renshi.renshi renshi；chmod 770 renshi

chown xingzheng.xingzheng xingzheng；chmod 770 xingzheng

6、什么是绝对路径和相对路径

答案：绝对路径：它从 / 根目录开始到目标文件和目录，比如/tmp/log/1.txt

相对路径：它以当前所在目录为参照物，到目标目录和文件，比如当前目录是/tmp/，

则 log/1.txt 为相对路径

7、简要叙述下列端口所运行的服务。

答案：21：[ftp](#)      22：[ssh](#)      23：telnet

25：smtp      110：pop3      3306：mysql



8、用 tar 命令归档并 gzip 压缩整个/test 目录，请写出完整压缩命令和解压命令

答案：tar -zcvf test.tar.gz /test

tar -zxvf test.tar.gz -C ./

9、有/mydata/scriptweb.sh 脚本文件，需要在每天 3:30 执行，请写出 crontab 参数

答案：30 3 \* \* \* /bin/bash /mydata/scriptweb.sh

10、描述下列指令的含义

答案：cd 切换目录

mkdir 创建目录

rm 删除目录或文件

chmod 更改目录和文件权限

chown 更改目录和文件所属主和组

mv 移动或重命名

ls 列出文件或目录

chgrp 更改目录所属组

free 查看内存



## 第 3 套

### 一、填空题：

1. linux 查看从本地到 218.56.57.58 的路由链路情况的命令是：route -eeFCn|grep 218.56.57.58

2. 检查硬盘 sda 读写速度的命令是：dd if=/dev/zero bs=1024 count=1000000 of=/1Gb.file

检查系统 IO 使用状态的命令是：iostat -d /dev/sda -k 1

3. 红帽操作系统版本号及内核版本的命令是：cat /etc/redhat-release; uname -a

4. CentOS6.3 操作系统日志是由 rsyslog 服务负责记录的，对应的配置文件为：cat /etc/rsyslog.conf

5. 常见的 MTA 有那些：sendmail、 postfix

6. 查看当前数据库的进程命令是：show full processlist;

7. Centos5.9 系统安装 anysetup-sec 的 rpm 包，如何查看该包包含那些文件：rpm -ql anysetup-sec

8. 查看当前系统加载的模块情况的命令是：lsmod；查看服务器各接口卡情况的命令是：lspci

9. 假设/a 目录不存在，建立如下目录结构的文件夹（/a/b/c/d）使用的命令是：mkdir -p /a/b/c/d

10. 假设文件 b.txt 含一些文件路径，使用的 tar 将 b.txt 文件中内容打包为 test.tar 的命令是：tar -cvf test.tar \$(cat b.txt|tr '\n' ' ')

11. 假设存在压缩包 any.tgz，查看此包的 tar 命令是：tar -tf /home 目录下解压，所使用的 tar 命令是：tar-zxf any.tgz -C /home

12. 修改 eth0 网卡为百兆全双工命令是：ethtool -s eth0 speed 100 duplex full autoneg



on

13.查看服务器内存容量的命令是：free 服务器 cpu 型号的命令是：awk -F: '/model name/{print \$2}' /proc/cpuinfo

14.Vi 编辑器中，向上翻页的组合键为 ctrl+f 要将 5-15 行间所有 hello 替换成 HELLO，vi 的命令为：5, 15s/hello/HELLO/g

15.Centos6.0 查看 mysqld 是否开机启动，执行那个命令：chkconfig --list|grep mysqld

16.用 find 命令清理系统/mail 分区下所有后缀为 “.lock” 文件，命令为：find /mail -type f -name “\*.lock” -exec rm -rf {} \;

17.Mysql 的 配 置 文 件 路 径 是：/etc/my.cnf httpd 的 配 置 文 件 路 径 是 /etc/httpd/conf/httpd.conf

18.查看一个文件类型使用那个命令 ls -l 换为 DOS 格式，命令是：unix2dos

## 二、简答题

19.linux 系统如果要对一个 5T 的存储阵列 sda 进行分区，应该使用什么命令分区，使用什么分区表？需要分配两个 100G 空间的，剩余空间给第三个分区，请提供命令：

答案：用 parted 来分区，yum install -y parted 安装。使用 gpt 分区表来分区。

分区步骤：parted /dev/sda 指定要分区的磁盘，进入后再继续执行下面的命令

mklabel gpt 指定分区表格式

mkpart primary 0 100G 第一个 100G 分区

mkpart primary 100G 200G 第二个 100G 分区

mkpart primary 200G -1 最后一个分区

exit 退出并保存



20.若要使我的程序/root/testsoft.sh 每年 1 月 1 日 ,5 月 1 日 ,10 月 1 日 0 点执行一次 ,  
请给出用法

答案 : `* 0 1 1 , 5 , 10 * /bin/bash /root/testsoft.sh`

21.vi 编辑器中 , 如何使其显示各行行号 ? 若要将文档中所有的 zhangsan , 替换成 lisi , 命令为 ?

答案 : 显示行号为: `set nu`      替换命令: `%s/zhangsan/lisi/g`

22.将文件 test 的权限赋为 743 , 语句为 ? 改权限的中文描述是 ?

答案 : `chmod 743 test`

把 test 文件的所有者权限设置为读写执行。所属组内成员权限设置为只读。其他用户的权限设置为写与执行。

23.一个分区的标签为 XXX 以标签形式挂在/tmp/mnt 下 , 命令格式为 ? 单机需要挂载 IP-SAN 设备时 , 需要在/etc/fstab 文件设置挂载点时需要注意什么参数 ?

答案 : `mount LABEL="XXX" /tmp/mnt`

要增加\_netdev 参数 , 这意思是挂载这个设置之前 , 先要开启网络服务 , 因为它依赖网络。

24.Linux 下将 211.154.203.84 的 8080 端口映射到内部 192.168.2.200 的 80 上 , 实现对内网机器的访问 , 请给出 NAT 转换命令行 ?

答案 : `iptables -t nat -A PREROUTING -d 211.154.203.84 -p tcp --dport 8080 -j DNAT --to 192.168.2.200:80`

25.假设存在 anymacro-4.8-txt-5.iso 已知/usr/bin/anysetup 是该 iso 的一个 rpm 包 , 请给找出到该文件所属 rpm 的方法 , 如何挂载 ISO 镜像并取出此 rpm 包放到/tmp 目录下 ?

答案 : `mount -t iso9660 -o loop anymacro-4.8-txt-5.iso /mnt/`

`find /mnt -type f -name "$(rpm -qf /usr/bin/anysetup)" -exec cp -rf {} /tmp/\;`



26.Cetnos6.0 系统默认语言是英文，我如何将操作系统的默认语言修改为简体中文（utf-8 格式）？

答案：LANG=zh\_CN.UTF-8

27.txt 为 utf8 编码的文件，如何操作能够终端使用 vi 工具正常显示文件内容

答案：set encoding=utf-8

28.查看 anymacro.com 的域名的 mx，ns，txt 记录的方法？说明这些记录的差别？如何确认某个 ip 地址是否已经做反向解析。

答案：nslookup -qt=mx anymacro.com

nslookup -qt=ns anymacro.com

nslookup -qt=txt anymacro.com

MX 记录主要用来做邮件服务器的域名记录，标明这是一台邮件服务器

NS 记录主要是用来做 DNS 服务器的记录，标明这是一台 DNS 服务器

TXT 记录主要用来做域名的说明。比如：域名所有者的信息。

nslookup -qa=ptr ip 地址，如果有返回正确的域名，就表示反解析正常。

29.现需要将邮件系统 A 的/mail 分区拷贝到邮件系统 B 的/mail 分区下，且必须保留 A 服务器/mail 分区的文件权限及属组，已知邮件服务器 A 的 ssh 端口为 31421，IP 地址为 192.168.1.1，邮件服务器 B 的 ssh 端口为 31422，IP 地址为 192.168.1.2，请提供远程拷贝命令

答案：A 服务器命令：rsync -avz -e "ssh -p 31422" /mail root@192.168.1.2:/mail

B 服务器命令：rsync -avz -e "ssh -p 31421" root@192.168.1.1:/mail /mail





30.CentOS6.0 安装系统时主机名和 DNS 服务器设置设错了，请给出具体要修改的文件：

答案： /etc/sysconfig/network 设置主机名

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

31.系统 MBR 引导丢失，我们如何利用系统光盘修复引导

答案：设置 bios，光驱启动，启动光盘进入 rescue mode，尝试重新安装 grub，命令：

grub-install /dev/sda，之后尝试重启

32.要以 user:zhangsan，password:6687 访问 test 数据库，语句为？

答案：mysql -uzhangsan -p6687 test



## 第 4 套

1.计划每天凌晨 1 点对 Mysql 数据库 letang 备份一次，备份后的文件要带有当天的日期。

请编写 shell 脚本并设定 crontab

答案：

```
vim /usr/local/sbin/backup.sh
```

```
#!/bin/bash
```

```
backup_dir=/root/mysql_bak
```

```
[ -d $backup_dir ] || mkdir $backup_dir
```

```
mysqldump -uroot --default-character-set=utf8 -p'****' letang >
```

```
/root/mysql_bak/$(date)_letang.sql
```

crontab:

```
0 1 * * * /bin/bash /usr/local/sbin/backup.sh
```

2.查询文件/logs/foo.log 以 “abc” 结尾的行。

答案：grep “abc\$” /logs/foo.log

3.如何将/usr/local/mysql/bin 添加到环境变量中

答案：vim /etc/profile.d/path.sh

写入 export PATH=\$PATH:/usr/local/mysql/bin

保存后执行: source /etc/profile

4.请描述一下如何查找并杀掉 letang.sh 进程

答案：ps aux|grep letang.sh 找出进程 ID,然后 kill 进程 ID

5.查找/logs 目录下前缀为 access 的文件并删除

答案：find /logs -type f -name “access\*” -exec rm -rf {} \;



6.通过 nginx 访问日志 access.log 统计 ip 和每个地址的访问次数，并列前 10 名

日志格式如下：

```
123.232.208.98 - [10/Sep/2016:16:33:13 +0800] "/thread-14858-1-1.html" 200
"http://www.lishiming.net/forum.php?mod=guide&view=my" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/31.0.1650.63 Safari/537.36 TheWorld 6"
```

答案：IP 前 10 名：`awk '{print $1}' access.log |sort|uniq -c|sort -rn|head`

网址前 10 名：`awk -F '"' '{print $2}' access.log|sort|uniq -c|head`

7.谈谈你对运维工程师的理解以及对工作的认识。

答案 运维工程师属于一个公司被人看不到 却很重要的职位 领导总是把运维排在最后面，和研发、产品、测试比起来，运维是默默服务在后面的。运维掌握着线上业务的命脉，一旦出现问题，所有技术人员都来找运维处理。所以，运维在日常工作中，需要做好监控和事故预案，当问题出现时，运维需要以最快的速度处理好问题。在平时，运维不仅仅要给研发、测试提供协助，还要自发性的去研究和分析服务器上的一些性能指标和日志，从而给研发同事提供一些数据和线索来优化业务。



## 第 5 套

### 一、SHELL 脚本部分：

#### 1.完成如下操作

- 1) 查询 file.txt 文件里第一列数据数值之和（字段以&符号分隔）
- 2) 查询 file.txt 在第 7 行之前添加一行，内容为“#注释”。
- 3) 打印出 file.txt 文件第 6 到第 10 行。

答案：

1) `awk -F' &' 'BEGIN{sum=0}{sum += $1}END{print sum}' file.txt`

2) `sed -i ' 7 i\ "#注释" ' file.txt`

3) `sed -n '6, 10' p file.txt`

#### 2.编写个 shell 脚本将/usr/local/test 目录下大于 100k 的文件转移到 /tmp 目录下。

答案：

```
find /usr/local/test -type f -size +100k -exec mv {} /tmp \;
```

#### 3.设计一个 shell 程序，添加一个新组为 class1，然后添加属于这个组的 30 个用户，用户名的形式为 stdxx，其中 xx 从 01 到 30

答案：

```
#!/bin/bash
```

```
for i in $(seq -w 01 30)
```

```
do
```

```
    useradd -g class1 std$i
```

```
done
```

说明：seq -w 可以让序列的数字都是两位数



4.通过 apache 访问 日志 access.log 统计 IP 和每个地址访问的次数 按访问 量列出前 10 名。

日志格式样例如下：

```
192.168.1.247 - - [02/Jul/2015:23:44:59 [0800] "GET /[HTTP/1.1 200
19"
```

答案： `awk '{print $1}' access.log|sort|uniq -c|sort -rn|head`

## 系统维护部分

1、Linux 系统怎么查找以普通用户 Galo 运行的所有进程？

答案： `ps aux|grep "^Galo"`

2、现用 vi 编辑了一个脚本 test.sh，在 linux 下执行时报错时，怎么进行调试脚本？

答案：用 `sh -x` 来查看脚本执行的过程 如果太多可以用 `&>` 定向执行过程到相应的日志里，再排查错误。

3、在 `/m_data/backup/scrip/` 目录下有一个数据库备份脚本 `mysql_bak.sh`，需要每周三凌晨 2:30 自动执行，使用 `crontab` 来完成此操作，请写下命令及 `crontab` 的内容？

答案： `30 2 * * 3 /bin/bash /m_data/backup/scrip/mysql_bak.sh`

4、Linux 服务器上的 tomcat 进程经常出现假死的情况，当你遇到这种问题时怎么处理该问题及采取怎样的预防措施？

答案：先排查假死时机器的负载，是否因为内存不足，cpu 使用过高，或者磁盘问题等导致。

临时解决办法是写个脚本监控 tomcat 进程状况和模拟用户访问 web 站点，当出现不正常时，重启 tomcat。另外还需要写一个监控系统各个硬件状态的脚本，比如 cpu、内存、磁盘、交换分区等，综合分析 tomcat 假死的原因，找问题是一个漫长和痛苦的事情，需要多



一些耐心，还需要我们敢去猜测，当然根据 tomcat、系统相关的日志来获取一些信息也是非常必要的。

5、如何使用命令查出 linux 系统 下某占用某个端口（如 8088）具体是哪个进程？

答案：netstat -lnp|awk -F'[ :/]+' '\$5~/8088/{print \$10}'

6、使用网络方式 kickstart 安装 linux 操作系统时，通常要在安装源服务器上配置并启动那些服务。

答案：dhcp ftp tftp

7、Apache 服务器的配置文件 httpd.conf 中有很多内容，请解释如下配置项：

答案：

- 1) MaxKeepAliveRequests 最大长连接请求数。
- 2) UserDir public\_html 用户的公用目录路径
- 3) DefaultType text/plain 默认网页格式为文本模式
- 4) AddLanguage en .en 加入英文字体
- 5) DocumentRoot "/var/www/html" 网站根目录
- 6) AddType application/x-httpd-php.php .php 增加对.php 文件的支持

8、Linux 现连接一个新的存储（如/dev/sdf，容量 2T）一个应用程序需要在/data 目录使用此存储的 500G 的存储空间（做成 LVM），需要哪些步骤，请描述。

答案：

fdisk /dev/sdf 分区

n, p, 1, 1 +500G w 分区步骤

pvcreeate /dev/sdf1 创建物理卷

vgcreate vg01 /dev/sdf1 创建卷组



`lvcreate -n lv01 -l 1000%free vg01` 创建逻辑卷

`mkfs.ext4 /dev/vg01/lv01` 格式化这个卷

`mount /dev/mapper/vg01-lv01 /data` 挂载这个卷

9、目前有一套 2 台 Linux 组成的 MySQL 双机热备系统，使用 heartbeat 或者你所熟悉的 HA 软件，进行双机切换测试，数据库版本为 MySQL5.5，写下双机切换的测试验证过程。

说明：这个题目考察的是大家对 HA 架构的熟练程度，遇上这样的题目多半是需要你上机操作的，如果是虚拟机实验，大家安装步骤是：1. 两台机器分别安装 mysql 2. 第一台部署 NFS，第二台挂载 NFS 3. 两台安装 heartbeat。当然，线上环境不建议做 NFS，因为 mysql 对磁盘 IO 有很高的要求，生产环境可以考虑 drbd，参考链接 <http://hypocritical.blog.51cto.com/3388028/1350251/>

10、基于 Linux 的系统监控或性能监控，写下你熟悉的一种监控软件（Nagios，Cacti，Nmon 或者其他工具或命令）能控制那些性能指标，报警有那些级别，有哪些报警方式。

答案：Zabbix 可以监控 cpu、内存、磁盘、进程、用户、文件、服务等基础项目，也可以自定义监控项目，通过 shell、python 等脚本实现。报警级别有 Information，Warning，Average，High，Disaster，可以通过邮件、短信、微信等方式告警

11、简述 raid0、raid1、raid5 三种工作模式的工作原理及特点。

答案：Raid0 最简单的模式，就是把 N 个物理磁盘合成一个总的虚拟磁盘。优点是：能够增加磁盘的 IO 性能。缺点是：只要有一个磁盘数据不正确，整个虚拟磁盘都会有影响。安全性最差。

Raid1 最安全的模式，raid1 也叫做镜像盘，一般都是以偶数形式出现。每个物理盘都有一块与它数据完全一致的磁盘搭配，优点是：在坏掉某一块磁盘时都不会造成数据的损坏。缺点是：磁盘的空间利用率只能达到 50%。



Raid5 最性价比的模式。raid5 是拿一块磁盘的空间来进行奇偶校验，容错能力平均分布所有硬盘上，当其中一块硬盘失效时，可以保证其它成员的硬盘数据正常，所以 RAID5 的总容量为“(N-1)\*最低容量硬盘容量”，对整体而言，raid5 容量效率比较高。优点是：在保证安全性的前提下最大化使用容量。缺点是：会影响整机的性能。

12、简述 Apache2.x 版本的两种工作模式，以及各自工作原理

答案：prefork 模式使用多个子进程，每个子进程只有一个线程。每个进程在某个确定的时间只能维持一个连接。在大多数平台上，Prefork MPM 在效率上要比 Worker MPM 要高，但是内存使用大得多。prefork 的无线程设计在某些情况下将比 worker 更有优势：它可以使用那些没有处理好线程安全的第三方模块，并且对于那些线程调试困难的平台而言，它也更容易调试一些。

worker 模式使用多个子进程，每个子进程有多个线程。每个线程在某个确定的时间只能维持一个连接。通常来说，在一个高流量的 HTTP 服务器上，Worker MPM 是个比较好的选择，因为 Worker MPM 的内存使用比 Prefork MPM 要低得多。但 worker MPM 也有不完善的地方，如果一个线程崩溃，整个进程就会连同其所有线程一起“死掉”。由于线程共享内存空间，所以一个程序在运行时必须被系统识别为“每个线程都是安全的”。

13、现有一套 Mysql 数据库，数据量 40G，应该如何对 Mysql 数据库进行备份和恢复？请写出三种备份方案，并标注你的最优方案。

答案：mysqldump 最常用的 mysql 备份工具，支持 myisam 或者 innodb 引擎，备份出来的数据是一个 sql 文件，它不仅要含有创建表的 sql 语句，还要包含表中每一条数据的插入 sql 语句。不管是备份还是恢复，效率都比较低，会锁表，如果数据量不大，使用 mysqldump 是很方便的。

xtrabackup 默认只支持 innodb 引擎的数据，备份的时候相当于直接把 mysql datadir





里面的所有文件拷贝一份，恢复也是直接把拷贝的文件放回去。所以，使用 xtrabackup 备份或者恢复速度都很快。它的变种工具 innobackupex 是对 xtrabackup 封装的 perl 脚本，提供了 myisam 表备份的能力。（能进行整库和数据表备份）。当数据量较大时，适合使用 innobackupex 来备份，效率很快。所以，本题中 40G 数据，适合使用这个工具。

binlog 就是大家熟知的主从了，它相当于是实时备份，在高可用架构中，通常使用主从或者主主，当一台宕机，另外一台可以马上替上去，数据可能会有少量丢失，但问题不大，我们可以通过查看 binlog 日志完全恢复。另外，做增量备份时，也可以只备份 binlog 文件，恢复时通过 binlog 文件可以恢复到指定某一时刻的数据状态。打开 binlog 意味着需要消耗额外的磁盘 I/O 资源。

14、在开启 iptables 防火墙的情况下，防火墙规则配置默认拒绝所有，请将 192.168.0.150 的 3306 端口映射到公网 58.206.99.105 的 1056 端口，能够正常访问数据库，写下详细的规则。

答案：

```
iptables -t nat -I PREROUTING -d 58.206.99.105 -p tcp --dport 1056 -j DNAT --to 192.168.0.150:3306
```

```
iptables -t filter -I FORWARD -d 58.206.99.105 -j ACCEPT
```

```
iptables -t filter -I FORWARD -s 192.168.0.150 -j ACCEPT
```

**说明：** 这部分面试题是内部教材《面试宝典》的前 5 套，要想获取更多资料，请加阿铭老师微信号 [81677956](#)。或者关注公众号 [aming\\_linux](#)。加 QQ 群 [246401509](#) 讨论 linux。