虽说年前就有很多人在修改简历、刷新简历，但是为了大家心中所谓的年终奖，99.9999%的人都会选择沉默，有一种「明修栈道，暗度陈仓」意味。

拿完了年终奖，过完了春节，老子早 TMD 的不想干了，终于不用在你「对象是种扣嗖的老板或领导」这里受你这等鸟气了。于是乎，吭哧吭哧的埋头苦写简历，狂撒网，做梦都想有朝一日能出任 CEO，迎娶白富美，走上人生的巅峰。

理想是丰满的，现实是残酷的，搞不好，美梦没有做完，就会吃上一记当头一棒，将你打入「绝情谷」谷底。所以，跳槽找工作一定要慎重，慎重，再慎重。

之前也写过类似的一篇文章「与努力同样重要的是，学会做好这 6 点！」，混职场的读者可以参考参考。但今天，我不们不讲混职场，只讨论求职找工作中如何避坑，否则，又像网友调侃那样：这是跳出一坑，又入一坑啊，总之坑不完啊。

那么，跳槽找工作到底会有哪些坑呢？

这篇文章来自我经常查阅的公众号

民工哥技术之路（ID：jishuroad）

扫描二维码，回复**"避坑"**查看全文

▼

在这个信息大爆炸的时代，互联网技术更新迭代如此之快，经常会听到一些同行们说："快学不动了，年纪大了"。的确，近些年来，对于技术人学习的强度与深度是呈现不断的加深的形态，一门新技术从出生、再到学习、再到企业应用，无疑对 IT 技术从业人员来说，无形当中的学习成本（时间、精力）也是不断的增加。所以，如何快速学习是一个很严肃的话题，我关注了近 400+个公众号，每天从不同的号中获取不同的知识点，然后通过自己的总结、整理，形成自己的一个有效的知识体系，久而久之发现这种获取、学习的方法非常好。

民工哥技术之路也是我关注的众多公众号之一，坚持**每天 10:00 分享不一样的干货**，专注高并发、大流量、高负载、高可用、MySQL 数据库、系统架构等开源技术。而且号主还比较细心，专注于给读者提供有价值、便利的阅读体验，把往期的精华文章定整理成一个目录的形式

关注**"民工哥技术之路"**回复**"目录"**可获最新版本

用号主的原话对民工哥技术之路的总结：热爱开源，拥抱开源。一个 IT 民工的技术之路经验分享。一个喜欢折腾、对技术有执着追求的公众号。

号主还有一段十年的杭漂经历 ,用号主的原话说 :本人文笔很烂 ,但愿用心写出来的故事，能够一同奔跑在技术道路上的伙伴们一点借鉴、一点思考、一点鼓励。

不管你才踏出社会，还是已久经沙场，**请相信，这个世界上，岁月对每个人都是公平的，**1 天都是 24 个小时，一分钟都是 60 秒。也许你要花久一点的时间才能找到你真正想做的事情，也许你要花长一点的时间才能改变现在的状况，但是**不管早还是晚，请你一定要出发，不管是早还是晚，请记得一定要努力去做、去改变！！！**

十年杭漂，今撤霸都

对了，号主还是《运维工程师进阶成神之路》系列文章的作者，文章从最基础的网络基础开篇，涉及系统基础、新手必备命令与 Shell 脚本编写、Linux 服务部署与配置、面试题讲解；再到提高篇：MySQL 数据库、企业生产项目实战案例、云计算、Docker 容器、虚拟化技术、企业架构实战；最后还提高一些实际职场中的踩坑经验总。总结成一句话：干货满满的，无论开发、运维、测试都值得学习一波。

关注**“民工哥技术之路”**回复**“成神之路”**可获最新版本

此系列 Github 地址：https://github.com/mingongge/BestOPS

关注**民工哥技术之路**回复**“备份”**获取生产数据备份方案

看了这么多民工哥技术之路的文章之后，是不感觉还阔以呢？其实民工哥技术之路有很多干货文章，这里篇幅有限就不能一一列举了，大家可以扫下方二维码关注后，慢慢仔细认真的逐一阅读。告诉大家一个小秘密：民工哥技术之路还不定期举行读者福利活动哦，比如说：赠送技术书籍、技术课程等。

民工哥技术之路（ID：jishuroad）

扫描二维码关注查看更多精彩内容

▼

1、请描述下 linux 系统的开机启动过程

开机加电 BIOS 自检---------->MBR 引导---------->grub 引导菜单---------->加载内核---------->启动 init 进程---------->读取 inittab 文件---------->启动 mingetty 进程---------->登录系统

2、权威 DNS 和递归 DNS 含义，智能 DNS 的实现原理

权威 DNS

是经上一级授权对域名进行解析的 DNS 服务器，同时它可以把解析授权转授给其他服务器，递归 DNS

负责接受用户对任何域名的查询，并返回结果给用户，它可以缓存结果避免用户再向上查询

智能 DNS

就是将对用户发起的查询进行判断出是哪个运营商的用户查询，然后将请求转发给相应的运

营商 IP 处理，减少跨运营访问的时间，提高访问速度

3、通过 APACHE 访问日志 access.log 统计 IP 和每个地址访问的次数，列出访问量前 10 名的 IP 地址，写出具体命令

awk '{print $1}' access.log|uniq -c|sort -rn |head -10

4、编写脚本实现将/usr/local/test 目录下大于 100K 文件，将它拷贝到/tmp 目录下

```
#!/bin/bash
for file in `ls /usr/local/test`
do
if [ -f $file ];then
    if [ `ls -l $file`|awk '｛print $5｝' -gt 10000];then
       mv $file /tmp/
    fi
fi
done
```

5、将本地的 80 端口的请求转发到 8080 端口，本机地址 10.0.0.254，写出命令

iptables -t nat -A PRETOUTING -d 10.0.0.254 -p tcp --dprot 80 -j NDAT --to-destination 10.0.0.254:8080

6、如何实现 nginx 代理的节点访问日志记录的是真实访客的 IP，不是代理的 IP

配置 nginx.conf 配置文件增加下同的标记内容

```
server{
            listen 80;
            server_name blog.text.com;
            location / {
            proxy_pass http://test_servers;
            proxy_set_header Host $host;
                  proxy_set_headerX-Forwarded-For $remote_addr;
        }
```

修改完成后，重新加载 nginx 即可，/application/nginx/sbin/nginx -s reload

7、MYSQL 一主多从，主库宕机，如何合理切换到从库，其它从库如何处理？

1：登陆所有从库查看 post 信息，使用 POST 最大的做为新的主库，然后将从为提升为新的主库，登陆从库（新的主库）执行 stop slave，

2：修改 my.cnf 配置文件，开启 log-bin 并重新启动数据库服务，登陆数据库执行 restet master ,show master status\G;查看主库信息，最后创建授权同步用户与权限和网站使用数据库的用户与权限，同步所有机器的/etc/hosts 文件（这时就体现了之前全网用域名则不是用 IP 的作用了，不然还得修改网站程序切换到新主库服务器 IP 上，否则无法连接到数据库）

3：登陆其它从库，执行 change master 操作，查看同步状态

8、误操作 drop 语句导致数据库数据破坏，请给出恢复的实际大体步骤

所有数据恢复的基础都在于备份，必须要有完整的备份，否则恢复无从谈起

误操作导致的数据库破坏需要使用增量恢复的方法进行恢复数据库，具体步骤如下

1、查看备份与 binlog 文件
2、刷新并备份 binlog 文件

```
mysqladmin -uroot -pmysql123 -S /data/mysql.sockflush-logs
```

3、将 binlog 文件恢复成 sql 语句

```
mysqlbinlog --no-defaults mysql-bin.000061 mysql-bin.000062 >bin.sql
```

4、将其中误操作的语句删除（就是 drop 的动作）
5、解压全备文件，恢复全备文件

```
gzip -d mysql_backup_2016-10-12.sql.gz
mysql -uroot -pmysql123 -S/data/3306/mysql.sock < mysql_backup_2016-10-12.sql
```

如果有对表的操作，恢复数据时需要接表名
6、恢复误操作前的 binlog 文件记录的 sql 语句

```
mysql -uroot -pmysql123 -S/data/3306/mysql.sock < bin.sql
```

最后登陆数据库，查看数据是否恢复成功，如果有确定的误操作时间，就直接恢复这段时间的数据即可

9、列举一个实际生产的例子，网站访问速度慢是因为数据库访问慢导致的

问题情况描述：
突然有一天，有同事反应，网站访问速度很慢，有时候会出现打不开网站的情况，刷新等待好长时间后又正常打开
解决步骤：
登陆数据库执行 show full processlist 看到有很多相同的查询动作且征对同一张表，因此确定网站打不开的原因是这个，故将此 IP 禁止访问。日常工作中避免此类问题发生解决方法如下：可以将数据库读写分离；安装数据缓存服务器，尽量将大部分的请求不直接对接数据库；

10、一个 shell 脚本手工可以执行，放入定时任务后不能执行，可能的原因？

手工可以执行，表明脚本本身不存在逻辑上的问题，可能原因有以下几点
1：定时任务书写有错误导致，执行的脚本没有写绝对路径，找不到脚本
2：环境变量问题导致

11、利用 shell 开发 rsync 服务启动、停止脚本，并通过 chkconfig 进行开关机管理

```
[root@mysql-1 download]# vi RSstart.sh
#!/bin/sh
##create by mingongge at 2017-01-10
. /etc/init.d/functions
case "$1" in
start)
     rsync --daemon
     if [ $? -eq 0 ];then
       action "rsync is started" /bin/true
     else
       action "rsync is started" /bin/false
     fi
;;
stop)
```

```
      pkill rsync
      sleep 2
      if [ `ps -ef|grep rsync|grep -v grep |wc -l` -eq 0 ];then
         action "rsync is stoped " /bin/true
      else
         action "rsync is stoped " /bin/false
      fi
;;
restart)
     pkill rsync
     sleep 2
     if [ `ps -ef|grep rsync|grep -v grep |wc -l` -eq 0 ];then
        rsync --daemon
        if [ $? -eq 0 ];then
           action "rsync is restarted" /bin/true
        fi
     fi
;;
*)
    echo "USAGE :{start|stop|restart}"
;;
esac
```

```
 “RSstart.sh" [New] 36L, 731C written
[root@mysql-1 download]# chmod +x RSstart.sh
[root@mysql-1 download]# sh RSstart.sh
USAGE :{start|stop|restart}
[root@mysql-1 download]# sh RSstart.sh   start
rsync is started                                [   OK   ]
[root@mysql-1 download]# ps -ef|grep rsync
root       1088       1   0 Jan09 ?        00:00:00 rsync --daemon
root       3527    2869   0 03:54 pts/0    00:00:00 grep rsync
[root@mysql-1 download]# sh RSstart.sh   stop
rsync is stoped                                 [   OK   ]
[root@mysql-1 download]# ps -ef|grep rsync
root       3540    2869   0 03:54 pts/0    00:00:00 grep rsync
[root@mysql-1 download]# sh RSstart.sh   start
rsync is started                                [   OK   ]
[root@mysql-1 download]# sh RSstart.sh   restart
rsync is restarted                               [   OK   ]
[root@mysql-1 download]# ps -ef|grep rsync
root       3558       1   0 03:54 ?        00:00:00 rsync --daemon
```

root 3564 2869 0 03:55 pts/0 00:00:00 grep rsync
配置开关机管理
然后在脚本最前面加上以下内容
chkconfig: 2345 21 99
description: chkconfig rsync service
具体自己测试下，也有可能这个启动，关闭序号有冲突，需要修改

12、请描述 OSI7 层模型各层名字及功能，并举例在不同层对应的协议
第一层：物理层，利用传输介质为数据提供物理连接， 对应的协议：ARP
第二层：数据链路层：建立和管理各节点间的链接链路 对应的协议：PPTP、CDP
第三层：网络层，是控制数据链路层与上传输层之间的信息转发、建立与维持对应的协议：IP、路由协议
第四层：传输层，提供会话传输服务，确保数据正确传送对应的协议：TCP UDP
第五层：会话层，提供建立会话管理，支持数据交换
第六层：表示层，处理数据（数据格式、编码、加密等），按一定的格式传送至会话层
第七层：应用层，为用户提供各类应用服务（文件、打印、邮件等服务）对应协议：HTTP、FTP、SMTP、POP3

13、linux 系统环境下如何查看系统运行了多长时间
[root@mysql-1 download]#uptime
02:05:22 up 2:32, 2 users, load average: 0.00, 0.00, 0.00
[root@mysql-1 download]#top
top -02:07:34 up 2:34, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 73total, 1 running, 72 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 0.0%sy, 0.0%ni,100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 486284k total, 174664kused, 311620k free, 6424k buffers
Swap: 1048568k total, 0kused, 1048568k free, 63548k cached
02:05:22 up 2:32, 2 users, load average: 0.00,0.00, 0.00
服务器运行多长时间 登陆用户数 上一分钟、5 分钟、15 分钟的负载

14、linux 系统中添加路由的方法
主机路由
route add -host 192.168.197.100 dev eth0
网关路由
route add default gw 192.168.197.1
网络路由
route ad -net 192.168.1.0 netmask 255.255.255.0 deveth1
route ad -net 192.168.1.0 netmask 255.255.255.0 gw192.168.197.1

15、已知 test.txt 文件内容如下，请取出文件的 5-15 行内容
[root@i ~]# cat test.txt
1
2
3

4
5bbb
6xxxxxxxxxx
7123i4i44
8
9
10
11
12
13ffffff
14fffff
15bbbbbb
16
17nnnnnn
方法一：[root@i ~]# grep 15bbbbbb -B 10 test.txt
5bbb
6xxxxxxxxxx
7123i4i44
8
9
10
11
12
13ffffff
14fffff
15bbbbbb
方法二：[root@i ~]# sed -n '5,15p' test.txt
5bbb
6xxxxxxxxxx
7123i4i44
8
9
10
11
12
13ffffff
14fffff
15bbbbbb
方法三：[root@i~]# awk '{if(NR<16 && NR>4) print $1}' test.txt
5bbb
6xxxxxxxxxx
7123i4i44
8
9

10
11
12
13ffffff
14fffff
15bbbbbb

16、/var/log/messages 日志出现 kernel:nf_conntrack:tablefull,dropping packet,请问是什么原因导致的，如何解决？

此报错为 iptables 报错信息，连接跟踪表已满，开始丢包，可能的原因是由于频繁的连接、关闭，或者网络的一些 TCP 的连接导致的

解决方法：

1、加大跟踪表的大小

2、禁用一些不必跟踪的连接状态

3、禁用模块 ip_vs nf_conntect

17、linux 系统 nginx 与 Php 环境，发现 PHP-FPM 进程高，请说出可能的原因以及如何解决

1：php 的插件程序与现有的 PHP 版本存在不兼容情况，解决方法从 php.ini 中禁止相关插件

2：软件本身存在问题，需要开发协同运维一同处理，查找原因

3：php 程序存在死循环现象，使用服务器负载过高，解决方法使用 top 命令查看

18、磁盘报错：nospace left on device，但是 df-h 查看空间没有满，为什么？

原因：系统 inode 满了，因为所有的文件的文件名信息都是存放在 inode 里面的，文件内容是存放在 block 里面

可以使用 df -i 来查看 inode 的使用情况

```
[root@mysql-1 download]# df -i
Filesystem     Inodes   IUsed    IFree IUse% Mounted on
/dev/sda2     1234576 138303 1096273    12% /
tmpfs           60785       1    60784   1% /dev/shm
/dev/sda1       51200      38    51162   1% /boot
```

19、 磁盘空间满了，删除一部分 nginx 日志后，但是磁盘空间还是满的，为什么？

删除的日志信息，一部分可能还是被进程调用，因此，需要重启 nginx 服务来释放进程；或者实际生产环境中使用>/log/access.log 清空文件

20、查看 apache 进程数

perfork 模式

```
ps -ef|grep http|grep -v grep|wc -l
```

worker 模式

```
pstree -a|grep httpd|wc -l
```

21、提取文件 test.log 中 FAILD 与 SUCCESSFUL 的字符但不包括 DONE 的行，然后以:为隔符，提取第三列

```
[root@mysql-1]# cat test.log
FAILD:SUCCESSFUL:DONE:CRITICAL
FAILD:SUCCESSFUL:NO:GOOD
FAILD:NO:DO:QINGYUN
SUCCESSFUL:DONE:CRITICAL::CRITICAL
```
方法一：
```
[root@mysql-1]# egrep "FAILD|SUCCESSFUL"test.log |grep -v DONE|awk -F ':' '{print $3}'
NO
DO
```
方法二：
```
[root@mysql-1]# egrep "FAILD|SUCCESSFUL"test.log |grep -v DONE|cut -d: -f3
NO
DO
```

22、公司机房的服务器接近 254 台了，请你设计一个解决方案，如何划分网段，并实现业务平滑迁移。

第一种方案：变长子网掩码的方法，加大 IP 地址的可使用范围，全网分发/etc/hosts 文件

第二种方案：增加核心交换机，在核心交换机划分 VLAN，将新增的服务器加入新的 VLAN 中，全网分发/etc/hosts 文件

23、Nginx 反向代理如何实现代理 RS 节点上的不同虚拟主机，请说出原理和配置方法或思路。

客户端向反向代理发送请求，反向代理按一定的规则转发至目标服务器，并将返回的内容返回给客户端，可分为以下两种：

配置内部不同服务器转发：

```
  upstream app1 {
        server 192.168.1.10:80 weight=5;
       server 192.168.1.11:80 weight=5;
       }
   upstream app2 {
        server 192.168.1.20:80 weight=5;
       server 192.168.1.21:80 weight=5;
       }
   配置 server
     server{
      listern 80;
      server_name app.abc.com
       }
配置匹配转发规则
    location /app1/ {
     proxy_pass http://example.com/app1;
proxy_set_header Host $host;
    }
   location/app2/ {
```

proxy_passhttp://example.com/app2;
proxy_set_header Host $host;
}
做为负载均衡
配置负载均衡服务器池，也就是调度规则
upstream test_servers {
server 192.168.1.2:80 weight=5;
server 192.168.1.4:80 weight=5;
server 192.168.1.6:82 weight=15;
}
然后配置 server 标签，
server {
listen 80;
server_name www.abc.com;
proxy_pass http://test_servers;
proxy_set_header Host $host
}
配置完成后，重新加载 nginx 服务

24、说出 netstat -an 命令结果中最后一列 status 对应的不同网络连接状态含义

[root@ ~]# netstat -an
Active Internet connections (servers andestablished)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 139.24.65.45:54296 10.11.68.13:80 ESTABLISHED
tcp 0 52 39.24.65.145:22 36.32.8.85:546 ESTABLISHED
tcp 0 0 139.24.165.45:586 10.11.8.13:80 CLOSE_WAIT

- ✓ listen 服务启动后首先处于的状态（监听状态）
- ✓ established 建立连接，表示建立连接的两端可以正常通信了
- ✓ close_wait 对方主动关闭连接或网络异常而中断，因此状态会变成
- ✓ time_wait 主动断开连接，收到对方确认后的状态，相当于释放资源，可以设置些种状态的参数，也就是主动断开后，下一次再连接的时间间隔
- ✓ syn_sent 请求连接的状态，需要访问其它机器时首先发出的同步信号

25、binlog 是什么？binlog 记录的是什么？有几种模式及优缺点，企业中选择哪种模式做同步？

blnlog：是用于记录所有更新了数据的操作语句，语句以事件的形式保存，它描述数据的更改过程
作用：用于实时备份数据，数据库的主从复制
log_bin 打开记录 binlog 功能
binlog 的查看
mysqlbinlog /home/mysql/binlog/binlog.000003

binlog 的删除：可分为自动与手动删除

自动删除
能过 binlog 参数 expire_logs_days 来实现
show binary logs;
show variables like "expire_logs_days;"
set gloable expire_logs_days=3;

手工删除
reset master 删除主的 binlog
reset slave 删除从的中继日志

三种模式：
Row level 模式 :日志会记录每一行数据被修改的形式，然后在从端对相同的数据进行修改
优点：可以不记录执行 SQL 语句上下文相关的信息，只记录哪一条数据被修改，修改成什么样了
缺点：所有执行的语句都当记录到日志文件中，而且都会以每行记录的修改来记录，会产生大量的日志内容
statement 模式：每一条修改数据的 SQL 都会记录 master 的 bin-log 中，slave 在复制的时候 SQL 进程会解析成和原来 master 端执行过的相同的 SQL 来执行
优点：解决了上 row level 模式的缺点，不需要记录每一行数据的变化，减少日志量，可以得高性能
缺点：由于记录的是执行语句，在此模式下会有主从无法复制的问题出现
mixed 自动模式：MYSQL 会根据执行的每一条具体 SQL 语句来区分对待记录的日志格式，

企业使用场景：
1、如果不会用到 mysql 特殊的功能，基本都是默认的模式 statement 模式
2、如果会到 mysql 的一些特殊功能，基本都是会使用 row level 模式

26、请详细描述 http 协议原理
http 协议：是客户端与服务端之间通信传输数据的基础，HTTP 协议是基于 TCP/IP 协议之上的协议
原理包括四个过程：
连接：浏览器与服务器建立连接，打开一个 socket 的虚拟文件，表明连接建立成功
请求：浏览器通过 socket 向服务器提交请求（一般是 GET 或 POST 请示命令）
应答：浏览器请求提交后，通过 HTTP 协议传送给服务器，服务器收到后进行处理将结果又通过 HTTP 回传给客户端，从而在客户端显示出所请求的页面
关闭连接：当应答结束后，浏览器与服务器之间就断开连接

27、请详细描述 MySQL 主从复制原理。
原理：主库开启 binlog 功能并授权从库连接主库同步的用户权限 ,将数据库的修改或变化生成 bin-log 日志，从库通过 change mster 的语句得到主库的相关信息，从库开启 slave 并连接主加进行相关验证，验证通过后，主库的 IO 线程根据从库的请求将相关位置点信息，与最新的 blnlog 信息发送给从库的 IO 线程，从库的 IO 线程将 SQL 语句的信息放在 relay-log 中，最后从库的 SQL 线程将 relay-log 中的 SQL 语句应用到从库中，实现主库与从库之间的数据同步，然后不断重新上述动作

28、用一条命令将除了 sshd、crond、network、rsyslog 几个服务之外的服务全部关闭（无需开机自动）

方法一：

```
[root@centos6~]# for name in `chkconfig --list|grep 3:on|awk '{print $1}'|grep -Ev
"sshd|crond|rsyslog|network"`;dochkconfig $name off;done
[root@centos6~]# chkconfig --list|grep 3:on
crond       0:off  1:off    2:on    3:on   4:on    5:on    6:off
network     0:off  1:off    2:on    3:on   4:on    5:on    6:off
rsyslog     0:off  1:off    2:on    3:on   4:on    5:on    6:off
sshd    0:off  1:off    2:on    3:on   4:on    5:on    6:off
```

方法二：

```
[root@centos6 ~]# chkconfig--list|grep 3:on|awk '{print $1}'|grep
-Ev"sshd|crond|rsyslog|network"|sed -r "s#(.*)#chkconfig \1off#g"|bash
[root@centos6~]# chkconfig --list|grep 3:on
crond       0:off  1:off    2:on    3:on   4:on    5:on    6:off
network     0:off  1:off    2:on    3:on   4:on    5:on    6:off
rsyslog     0:off  1:off    2:on    3:on   4:on    5:on    6:off
sshd        0:off  1:off    2:on    3:on   4:on    5:on    6:off
```

29、说明系统/etc/inittab 中各个启动级别的含意

```
[root@centos6~]# tail /etc/inittab
#Default runlevel. The runlevels used are:
#    0 - halt (Do NOT set initdefault to this)  关机
#    1 - Single user mode          单用户模式
#    2 - Multiuser, without NFS (The same as 3,if you do not have
networking)                       多用户，没有 NFS
#    3 - Full multiuser mode   完整多用户模式
#    4 - unused
#    5 - X11                       桌面模式
#    6 - reboot (Do NOT set initdefault to this)  重启
#
id:3:initdefault:    默认
```

30、写一个 sed 命令，修改/tmp/input.txt 文件的内容，要求：(1) 删除所有空行；(2) 一行中，如果包含"11111"，则在"11111"前面插入"AAA"，在"11111"后面插入"BBB"，比如：将内容为 0000111112222 的一行改为：0000AAA11111BBB2222

```
[root@~]# cat -n /tmp/input.txt
    1   000011111222
    2
    3   000011111222222
    4   11111000000222
    5
```

```
     6
     7  11111111111122222222222
     8  2211111111
     9  112222222
    10   1122
    11
```
删除所有空行命令

```
[root@~]# sed '/^$/d' /tmp/input.txt
000011111222
000011111222222
11111000000222
11111111111122222222222
2211111111
112222222
1122
```
插入指定的字符

```
[root@~]# sed 's#\(11111\)#AAA\1BBB#g' /tmp/input.txt
0000AAA11111BBB222
0000AAA11111BBB222222
AAA11111BBB000000222
AAA11111BBBAAA11111BBB11122222222222
22AAA11111BBB111
112222222
1122
```

31、每周一下午三点将/tmp/logs 目录下面的后缀为*.log 的所有文件 rsync 同步到备份服务器 192.168.1.100 中同样的目录下面，crontab 配置项该如何写：

```
00 15 * * 1 rsync -avzP /tmp/logs/*.log root@192.168.1.100:/tmp/logs
```

32、找到/tmp/目录下面的所有名称以"_s1.jpg"结尾的普通文件，如果其修改日期在一天内，则将其打包到/tmp/back.tar.gz 文件中

```
find /tmp -type f -name ".*_sj.jpg" -mtime 1|xarges tar zxf /tmp/back.tar.gz
```

33、写出如何给 apache 增加 virtualhost，让访问 http://www.test.com 和 http://www.test.cn 的时候，都打开/var/www/html 目录下面的文件：

```
<VirtualHost *:80>
    ServerAdmin admini@abc.com
    DocumentRoot "/var/www/html"
   ServerName www.test.com
    ServerAlias   test.cn
    ErrorLog "logs/bbs-error_log"
    CustomLog "logs/bbs-access_log" common
</VirtualHost>
```

34、配置 mysql 服务器的时候，配置了 auto_increment_increment=3，请问这里的 3 意味着

什么？
auto_increment 是用于主键自动增长的，从 3 开始增长，3 表示自增的起始值

35、用一条命令显示本机 eth0 网卡的 IP 地址，不显示其它字符
方法一：
[root@apache ~]# ifconfig eth0|grep "inet addr"|awk -F '[:]+' '{print $4}'
192.168.1.22
方法二：
[root@apache ~]# ifconfig eth0|awk -F '[:]+' 'NR==2 {print $4}'
192.168.1.22
方法三：
[root@apache ~]# ifconfig eth0|sed -n '2p'|sed 's#^.*addr:##g'|sed 's# Bc.*$##g'
192.168.1.22
方法四：
[root@apache ~]# ifconfig eth0|sed -n '2p'|sed -r 's#^.*addr:(.*) Bc.*$#\1#g'
192.168.1.22

36、请详细说明 keepalived 的故障切换工作原理
这种故障切换是通过 VRRP 协议来实现的，主节点会按一定的时间间隔发送心跳信息的广播包，告诉备节点自己的存活状态信息，当主节点发生故障时，备节点在一段时间内就收到广播包，从而判断主节点出现故障，因此会调用自身的接管程序来接管主节点的 IP 资源及服务，当主节点恢复时，备节点会主动释放资源，恢复到接管前的状态，从而来实现主备故障切换

37、写出一个 curl 命令，访问指定服务器 61.135.169.121 上的如下 URL：
http://www.baidu.com/s?wd=test，访问的超时时间是 20 秒：
curl --connect-timeout 20 http://61.135.169.121/s?wd=test

38、用 netstat 命令配合其他 shell 命令，按照源 IP 统计所有到 80 端口的 ESTABLISHED 状态链接的个数，输出结果类似（第一列为连接数，第二列为 IP）：
[root@~]# netstat -an|grep ESTABLISHED
tcp 0 52 139.224.199.85:22 101.47.33.86:51763 ESTABLISHED
tcp 0 0 139.224.199.85:45368 106.11.68.13:80 ESTABLISHED
[root@ ~]# netstat -an|grep ESTABLISHED|grep ":80"
tcp 0 0 139.224.199.85:45368 106.11.68.13:80 ESTABLISHED
[root@ ~]# netstat -an|grep ESTABLISHED|grep ":80"|awk 'BEGIN{FS="[[:space:]:]+"}{print $4}'
139.224.199.85
说明：FS 是字段分隔符
如果需要进行整理并排序的话，完整命令如下
[root@ ~]# netstat -an|grep ESTABLISHED|grep ":80"|awk 'BEGIN{FS="[[:space:]:]+"}{print $4}'|sort|uniq -c|sort -nr

39、请简要说明 Linux 系统在目标板上的启动过程?
该问题是 Linux 运维面试最常见的问题之一，问题答案如下：

1.用户打开 PC 的电源，BIOS 开机自检，按 BIOS 中设置的启动设备(通常是硬盘)启动；
2.启动设备上安装的引导程序 lilo 或 grub 开始引导 Linux；
3.首先进行内核的引导，接下来执行 init 程序，init 程序调用了 rc.sysinit 和 rc 等程序，rc.sysinit 和 rc；
4.当完成系统初始化和运行服务的任务后，返回 init；
5.init 启动了 mingetty 后，打开了终端供用户登录系统；
6.用户登录成功后进入了 Shell，这样就完成了从开机到登录的整个启动过程。

40、解释下什么是 GPL,GNU,自由软件？

GPL：（通用公共许可证）：一种授权，任何人有权取得、修改、重新发布自由软件的权力。
GNU:(革奴计划)：目标是创建一套完全自由、开放的的操作系统。
自由软件：是一种可以不受限制地自由使用、复制、研究、修改和分发的软件。主要许可证有 GPL 和 BSD 许可证两种。

41、如何选择 Linux 操作系统版本?

一般来讲，桌面用户首选 Ubuntu；服务器首选 RHEL 或 CentOS，两者中首选 CentOS。
根据具体要求：
①安全性要求较高，则选择 Debian 或者 FreeBSD。
②需要使用数据库高级服务和电子邮件网络应用的用户可以选择 SUSE。
③想要新技术新功能功能可以选择 Feddora，Feddora 是 RHEL 和 CentOS 的一个测试版和预发布版本。
④根据现有状况，绝大多数互联网公司选择 CentOS。现在比较常用的是 6 系列，现在市场占有大概一半左右。另外的原因是 CentOS 更侧重服务器领域，并且无版权约束。

42、初学者在 Linux 系统的开机启动项如何选择？

建议选择五个开机启动项：
①.crond： 该服务用于周期地执行系统及用户配置的计划任务。有要周期性执行的任务计划需要开启，此服务是生产场景必须要用的一个软件。
②.iptables： iptables 包过滤防火墙，有外网 IP 时，考虑开启。
③.network： 启动系统时，若想激活/关闭启动时的各个网络接口，则应（必须）考虑开启。
④.sshd： 远程连接 Linux 服务器时需要用到这个服务程序，所以必须要开启，否则将无法远程连接到 Linux 服务器。
⑤.rsyslog： 是操作系统提供的一种机制，系统的守护程序通常会使用 rsyslog 将各种信息收集写入到系统日志文件中，CentOS6 以前此服务的名字为 syslog。
⑥.sysstat: 是一个软件包，包含监测系统性能及效率的一组工具，这些工具对于 Linux 系统性能数据很有帮助，比如 CPU 使用率、硬盘和网络吞吐数据等，这些数据的分析，有利于判断系统运行是否正常，所以它是提高系统运行效率、安全运行服务的助手。

43、请描述 Linux 系统优化的 12 个步骤。

⑴登录系统:不使用 root 登录，通过 sudo 授权管理，使用普通用户登录。
⑵禁止 SSH 远程：更改默认的远程连接 SSH 服务及禁止 root 远程连接。
⑶时间同步：定时自动更新服务器时间。
⑷配置 yum 更新源，从国内更新下载安装 rpm 包。
⑸关闭 selinux 及 iptables（iptables 工作场景如有 wan ip，一般要打开，高并发除外）

⑹调整文件描述符数量，进程及文件的打开都会消耗文件描述符。
⑺定时自动清理/var/spool/clientmquene/目录垃圾文件，防止节点被占满（c6.4 默认没有sendmail，因此可以不配。）
⑻精简开机启动服务（crond、sshd、network、rsyslog）
⑼Linux 内核参数优化/etc/sysctl.conf，执行 sysct -p 生效。
更改字符集，支持中文，但是还是建议使用英文，防止乱码问题出现。
⑾锁定关键系统文件（chattr +i /etc/passwd /etc/shadow /etc/group /etc/gshadow /etc/inittab 处理以上内容后，把 chatter 改名，就更安全了。）
⑿清空/etc/issue，去除系统及内核版本登陆前的屏幕显示。

44、描述 Linux 运行级别 0-6 的各自含义
0：关机模式
1：单用户模式<==破解 root 密码
2：无网络支持的多用户模式
3：有网络支持的多用户模式（文本模式，工作中最常用的模式）
4：保留，未使用
5：有网络支持的 X-windows 支持多用户模式（桌面）
6: 重新引导系统，即重启

45、描述 Linux 系统从开机到登陆界面的启动过程
⑴开机 BIOS 自检，加载硬盘。
⑵读取 MBR,MBR 引导。
⑶grub 引导菜单(Boot Loader)。
⑷加载内核 kernel。
⑸启动 init 进程，依据 inittab 文件设定运行级别
⑹init 进程，执行 rc.sysinit 文件。
⑺启动内核模块，执行不同级别的脚本程序。
⑻执行/etc/rc.d/rc.local
⑼启动 mingetty，进入系统登陆界面。

46、描述 Linux 下软链接和硬链接的区别
在 Linux 系统中，链接分为两种，一种是硬链接（Hard link），另一种称为符号链接或软链接（Symbolic Link）。
①默认不带参数的情况下，ln 创建的是硬链接，带-s 参数的 ln 命令创建的是软链接。
②硬链接文件与源文件的 inode 节点号相同，而软链接文件的 inode 节点号，与源文件不同，
③ln 命令不能对目录创建硬链接，但可以创建软链接。对目录的软链接会经常使用到。
④删除软链接文件，对源文件和硬链接文件无任何影响。
⑤删除文件的硬链接文件，对源文件及软链接文件无任何影响。
⑥删除链接文件的源文件，对硬链接文件无影响，会导致其软链接失效（红底白字闪烁状）。
⑦同时删除源文件及其硬链接文件，整个文件才会被真正的删除。
⑧很多硬件设备的快照功能，使用的就是类似硬链接的原理。
⑨软链接可以跨文件系统，硬链接不可以跨文件系统。

47、生产场景如何对 linux 系统进行合理规划分区？

分区的根本原则是简单、易用、方便批量管理。根据服务器角色定位建议如下：
①单机服务器：如 8G 内存，300G 硬盘
分区： /boot 100-200M，swap 16G，内存大小 8G*2，/ 80G，/var 20G（也可不分），/data 180G（存放 web 及 db 数据）
优点：数据盘和系统盘分开，有利于出问题时维护。
RAID 方案：视数据及性能要求，一般可采用 raid5 折中。

②负载均衡器（如 LVS 等）
分区：/boot 100-200M，swap 内存的 1-2 倍，/ ，
优点：简单方便，只做转发数据量很少。
RAID 方案：数据量小，重要性高，可采用 RAID1

③负载均衡下的 RS server
分区： /boot 100-200M，swap 内存的 1-2 倍，/
优点：简单方便，因为有多机，对数据要求低。
RAID 方案：数据量大，重要性不高，有性能要求，数据要求低，可采用 RAID0

④数据库服务器 mysql 及 oracle 如 16/32G 内存
分区：/boot 100-200M，swap 16G，内存的 1 倍，/ 100G，/data 剩余（存放 db 数据）
优点：数据盘和系统盘分开，有利于出问题时维护,及保持数据完整。
RAID 方案：视数据及性能要求主库可采取 raid10/raid5，从库可采用 raid0 提高性能（读写分离的情况下。）

⑤存储服务器
分区：/boot 100-200M，swap 内存的 1-2 倍，/ 100G，/data(存放数据)
优点：此服务器不要分区太多。只做备份，性能要求低。容量要大。
RAID 方案：可采取 sata 盘，raid5

⑥共享存储服务器（如 NFS）
分区：/boot 100-200M，swap 内存的 1-2 倍，/ 100G，/data(存放数据)
优点：此服务器不要分区太多。NFS 共享比存储多的要求就是性能要求。
RAID 方案：视性能及访问要求可以 raid5,raid10,甚至 raid0（要有高可用或双写方案）
⑦监控服务器 cacti,nagios
分区：/boot 100-200M，swap 内存的 1-2 倍，/
优点：重要性一般，数据要求也一般。
RAID 方案：单盘或双盘 raid1 即可。三盘就 RAID5，看容量要求加盘即可。

49、描述 Linux 下文件删除的原理
Linux 系统是通过 link 的数量来控制文件删除的，只有当一个文件不存在任何 link 的时候，这个文件才会被删除。一般来说每个文件两个 link 计数器来控制 i_count 和 i_nlink。当一个文件被一个程序占用的时候 i_count 就加 1。当文件的硬链接多一个的时候 i_nlink 也加 1。删除一个文件，就是让这个文件，没有进程占用，同时 i_link 数量为 0。

50、请简单描述 VI 编辑器的使用

①vi 编辑器是 linux 系统下最最基本和最常用的标准文本编辑器。
②vi 编辑器有三种工作模式：普通模式、编辑模式、命令模式。
③普通模式下的键盘输入任何字符都是当作命令来执行的，也可以输入命令进行光标的移动，字符、单词、行的复制、粘帖以及删除等操作。
④编辑模式主要用于文本的输入。在该模式下，用户输入的任何字符都被作为文件的内容保存起来。
⑤命令模式下，用户可以对文件进行一些如字符串查找、替换、显示行号等操作还是必须要进入命令模式的。
⑥在普通模式下输入冒号即可进入命令模式，此时 vi 窗口的状态行会显示出冒号，等待用户输入命令。“i”插入模式，即可以进行编辑。用户输入完成后，按【Esc】之后编辑器又返回到普通模式下，在命令模式下，保存退出，可以使用的命令为 wq 和 x。前面加！表示强制退出，强制保存等。

51、请简单说出用户管理的相关命令及用途

#组管理命令
groupadd #添加组
groupdel #删除用户组
groupmod #修改用户组
groups #显示当前用户所属的用户组
grpck #检查用户组及密码文件的完整性（etc/group 以及/etc/gshadow 文件）
grpconv #通过/etc/group 和/etc/gshadow 的文件内容来同步或创建/etc/gshadow，如果/etc/gshadow 不存在则创建；
grpunconv #通过/etc/group 和/etc/gshadow 文件内容来同步或创建/etc/group，然后删除 gshadow 文件。

#用户管理命令
useradd #添加用户
adduser #添加用户
passwd #为用户设置密码
usermod #修改用户命令，可以通过 usermod 来修改登录名、用户的家目录等等
pwcov #同步用户从/etc/passwd 到/etc/shadow
pwck #pwck 是校验用户配置文件/etc/passwd 和/etc/shadow 文件内容是否合法或完整
pwunconv #执行 pwunconv 指令可以关闭用户投影密码，它会把密码从 shadow 文件内，重回存到 passwd 文件里。
finger #查看用户信息工具（危险命令，一般不用）
id #查看用户的 UID、GID 及所归属的用户组
chfn #更改用户信息工具
su #用户切换工具

52、请简述基础正则表达式 grep 高级参数的使用

常用参数：
-v 排除匹配内容，
-e 支持扩展的正则表达式，
-i 忽略大小写，

-o 输出匹配的内容（只是一块，不是行），
–color=auto 匹配内容显示颜色，
-n 在行首显示行号。
特殊字符注意事项：
^(尖括号)word ：表示搜索以 word 开头的内容。
word$ 表示搜索以 word 结尾的内容。
^$ 表示的是空行，不是空格。
. 代表且只能代表任意一个字符。非正则表达式其他功能（当前目录，加载文件）
\ 转义字符，让有着特殊身份意义的字符，脱掉马甲，还原原型。例如\.只表示原始小数点意义。
* 表示重复 0 个或多个前面的一个字符。不代表所有。
.* 表示匹配所有的字符。^.*表示以任意字符开头。
[任意字符如 abc] 匹配字符集内任意一个字符[a-z]。
[^abc] ^在中括号里面是非的意思，不包含之意。意思就是不包含 a 或 b 或 c 的行。
{n，m} 表示重复 n 到 m 次前一个字符。{n} 至少 n 次，多了不限。{n} N 次，{，m} 至多 m 次，少了不限。
注：使用 grep 或 sed 要对 { } 转义。即\ {\} .egrep 就不需要转义了。

53、请简述基础正则表达式 sed 高级参数的使用
解答：
-n 取消默认输出
-p 打印
-d 删除
-e 允许多项编辑
sed 取行，要特别注意 sed -n 's###g' filename 的使用，sed 的\(\)的功能可以记住正则表达式的一部分，其中，\1 为第一个记住的模式即第一个小括号中的匹配内容，\2 第二记住的模式，即第二个小括号中的匹配内容，sed 最多可以记住 9 个。
实际字符的选取最好要唯一，正则表达式是贪婪的，总是尽可能的匹配更远的符合匹配的内容。另外注意字符串中的空格。

54、请给出查看当前哪些用户在线的 Linux 命令
w #显示目前系统登录用户
who #显示目前已登录用户信息
last #列出目前与过去登入系统的用户相关信息
lastlog #检查某特定用户上次登录时间
whoami #打印与当前生效的用户 ID 关联的用户名
finger #用户信息查找程序
id #显示指定用户或当前用户的用户与组信息

55、请你描述下 crontab 的作用和语法，以及书写定时任务注意的要点。
设置 crontab 后我们可以使得 Linux 主动执行的在固定的间隔时间，执行指定的系统指令或 shell script 脚本。生产环境可以用来日志分析或生产备份等。
语法格式：
crontab [-u user] file ===》-u 的意思就是指定用户

crontab [-u user] { -l 显示文件内容| -r 全部删除 crontab 文件 | -e 编辑 crontab 文件| -i 删除 crontab 文件前确认提示}
举例：
*/5 10，12 * 3-8 * * /usr/sbin/ntpdate 10.0.0.155 >/dev/null 2>&1
前五段是时间间隔的设定，单位分别是分钟、小时、日、月、周（尽量避免使用日月和周同时出现，以免造成系统误判）。
第一个时间段 分钟 范围 0-59
第二个时间段 小时 范围 0-23
第三个世间段 日 范围 1-31
第四个时间段 月 范围 1-12
第五个时间段 周 范围 0-7

*星号代表任何时间都接受命令
，逗号，表示隔开。代表分隔的时间都适用此命令。
– 减号，两个时间段之间，代表在此时间段内执行定时任务。
/n 斜线和 n（数字）表示每隔 n 段时间执行一次。

注意要点分为：书写基本要领与书写注意事项
7 个基本要领：
第一、为定时任务规则加必要的注释
第二、定时任务命令或程序最好写到脚本里执行
第三、定时任务执行的脚本要规范路径，如：/server/scripts
第四、执行 shell 脚本任务时前加/bin/sh
执行定时任务时，如果是执行脚本，尽量在脚本前面带上/bin/sh 命名
第五、定时任务结尾加 >/dev/null 2>&1
第六、/dev/null 为特殊的字符设备文件，表示黑洞设备或空设备。
第七、有关重定向的说明
>或 1> 输出重定向：把前面输出的东西输入到后边的文件中，会删除文件原有内容。
>>或 1>> 追加重定向：把前面输出的东西追加到后边的文件中，不会删除文件原有内容。
<或<0 输入重定向：输入重定向用于改变命令的输入，指定输入内容，后跟文件名。
<<或<<0 输入重定向：后跟字符串，用来表示“输入结束”，也可用 ctrl+d 来结束输入。
2> 错误重定向：把错误信息输入到后边的文件中，会删除文件原有内容。
2>> 错误追加重定向：把错误信息追加到后边的文件中，不会删除文件原有内容。
标准输入（stdin）：代码为 0，使用<或<<。
标准输出（stdout）:代码为 1，使用>或>>。正常的输出。
标准错误输出（sederr）：代码为 2，使用 2>或 2>>。
特殊：
2>&1 就是把标准错误重定向到标准输出（>&）。
>/dev/null 2>&1 等价于 1>/dev/null 2>/dev/null

56、请列出 Linux 中你认为重要的文件夹及包含内容
① /目录下的文件夹里面分别是以下内容：
/usr 包含所有的命令和程序库、文档和其他文件及当前 linux 发行版的主要应用程序
/var 包含正在操作的文件，还有记录文件、加密文件、临时文件等

/home 除了 root 用户外的所有用户的配置文件，个性化文件和主目录，即家目录
/proc 虚拟目录，该目录实际上指向内存而不是硬盘
/bin　系统执行文件（二进制文件）普通用户可以使用
/sbin 系统执行文件（二进制文件）不能被普通用户使用，通常由 root 用户使用
/etc 操作系统的配置文件
/root root 用户的家目录
/dev 系统设备文件，linux 所有设备都是以文件的形式被处理，该目录不包含驱动程序
/lib 程序和核心模块共享库（仅限于/下的程序）
/boot 系统引导、启动文件，通常 grub 也在这里
/opt 可选应用程序目录
/tmp 临时文件，系统会自动清理
/lost+found 恢复文件（类似回收站）
/media 所有的磁盘（有时有光盘）将以文件夹的形式挂载，光盘镜像也可以挂载
/cd-rom 挂载光盘的地方

② /usr 目录下的文件比较重要，其作用下面分类列出：
/usr/X11 X-windows 桌面环境
/usr/doc linux 系统的文档资料
/usr/share 独立于当前计算机的数据结构，如字典中的词
/usr/bin 类似/bin 但是不参与启动，大部分命令都在这里
/usr/local 本地管理员安装的应用程序
/usr/local/bin 用户安装的应用程序（部分）

③ /proc 目录的内容
/proc/cpuinfo 处理器的信息
/proc/devices 当前运行内核的所有设备清单
/proc/dma 当前正在使用中的 DMA 通道
/proc/filesystem 当前运行内核所配置的文件系统
/proc/interrupts 当前使用的中断和曾经有多少个中断
/proc/ioports 正在使用的 I/O 端口

57、给出正确的关机和重启服务器的命令
⑴shutdown
[-t] 指定在多长时间之后关闭系统
[-r] 重启系统
[-k] 并不真正关机，只是给每个登录用户发送警告信号
[-h] 关闭系统（halt）
⑵halt
halt 是最简单的关机命令，其实际上是调用 shutdown -h 命令。halt 执行时，杀死应用进程，文件系统写操作完成后就会停止内核。
halt 命令的部分参数如下：
[-f] 没有调用 shutdown 而强制关机或重启
[-i] 关机或重新启动之前，关掉所有的网络接口
[-p] 关机时调用 poweroff，此选项为缺省选项

⑶reboot
reboot 工作过程与 halt 类似，作用是重新启动，而 halt 是关机。其参数与 halt 类似。
⑷init
init 是所有进程的祖先，其进程号始终为 1。init 用于切换系统的运行级别，切换的工作是立即完成的。init 0 命令用于立即将系统运行级别切换为 0，即关机；init 6 命令用于将系统运行级别切换为 6，即重新启动。

58、请简述修改/etc/sudoers 配置文件的注意事项
①别名的名称可以包含大写字母。数字、下划线。如果是字母必须要大写，（别名为一群拥有相同属性的集合）。
②一个别名下面可以有多个成员，成员间通过半角(,)逗号隔开。成员必须有效实际存在。别名成员受别名类型 Host_Alias、User_Alias、Runas_Alias、Cmnd_Alias 制约，定义什么类型的别名，就要有相什么类型的成员匹配。
③用户组前面必须加%号。命令别名下的成员必须是文件或目录的绝对路径。
④指定切换用户要用（）括号括起来，如果省略，则默认 root 用户，如果括号里是 ALL，则代表能切换到所有用户。
⑤命令路径要使用全路径。
⑥别名规则每行算一个规则，一行容不下时用\续行。另外超过一行，用反斜线换行。
⑦一般不建议先给 all 权限，后面排除。用什么权限，就给什么权限。（注意权限，语法）。如果不需要密码直接运行命令的应该加 NOPASSWD 参数。
⑧禁止某类程序或命令执行，要在命令动作前面加上“！”号，并放在允许执行命令之后。

59、请描述如何实现 linux 系统集权分治的权限分级精细管理？
① 收集以及制定用户和权限的匹配信息，原则是给于最小权限，但是又能完成所承担的工作职责。
② 各个用户组设置对应权限，用什么给什么，精细到每一条指令上根据分组情况。
③ 创建规划权限分组的用户.添加相关用户组。并修改 etc/sudoers 配置文件。
④ 增加 sudo 的权限开放，确定相关用户加入如 soduers 权限列表，并详细设置所开放权限内容，并选择是否需要密码的相关执行权限开放。(注意 ALL 权限,以及密码修改权限设置)。
⑤ 不建议先给 all 权限，后面排除。建议使用白名单。
⑥实战调试测试相关权限是否正确配置完成。
⑦编写操作说明，及相关注意事项。
⑧调试完毕，邮件周知所有相关人员系统权限设置生效，并附带操作说明及相关注意事项。

60、请写出下面 Linux SecureCRT 命令行快捷键命令的功能？
Ctrl + a 光标到开头
Ctrl + c 中断当前程序
Ctrl + d 退出当前窗口或当前用户
Ctrl + e 光标到结尾
Ctrl + l 清屏 相当与 clear
Ctrl + u 剪切、删除（光标以前的）内容
Ctrl + k 剪切、删除（光标以后的）内容
Ctrl + r 查找（最近用过的命令）
tab 所有路径以及补全命令

Ctrl+shift+c 命令行复制内容
Ctrl+shift+v 命令行粘贴内容
Ctrl + q 取消屏幕锁定
Ctrl + s 执行屏幕锁定

61、请描述服务器账户日志审计的 5 种解决方案。
⑴通过环境变量 syslog 对全部全部日志进行审计（信息量太大，不推荐）
⑵sudo 配合 syslog 服务，进行 sudo 操作日志进行审计（信息较少，效果不错）
⑶在 bash 解释器嵌入一个监视器，让所有用户使用修改过的 bash 程序，作为解释程序。
⑷齐治的堡垒机（商业产品）。

62、如果一台办公室内主机无法上网（打不开网站），请给出你的排查步骤？
①首先确定物理链路是否联通正常。
②查看本机 IP，路由，DNS 的设置情况是否达标。
③telnet 检查服务器的 WEB 有没有开启以及防火墙是否阻拦。
④ping 一下网关，进行最基础的检查，通了，表示能够到达服务器。
⑤测试到网关或路由器的通常情况，先测网关，然后再测路由器一级一级的测试。
⑥测试 ping 公网 ip 的通常情况（记住几个外部 IP），
⑦测试 DNS 的通畅。ping 出对应 IP。
⑧通过以上检查后，还在网管的路由器上进行检查。

63、描述 Linux shell 中单引号、双引号及不加引号的简单区别
单引号：所见即所得，即将单引号内的内容原样输出，或者描述为单引号里面看到的是什么就输出什么。
双引号：把双引号里面的内容给输出出来，如果内容中有命令、变量等，会先把，变来那个、命令解析出结果，然后输出最终内容。
双引号内的命令或者变量写法'命令或变量'或$(命令或变量)

无引号：把内容输出出来，可能不会键含有空格的字符串，视为一个整体输出，如果内容中有命令、变量等，会先把变量、命令解析出来，然后输出最终内容，如果字符串中带有空格等特殊字符，则不能完整输出，需要改加双引号。一般连续的字符串，数字，路径等可以用，不过最好用双引号，替代之 **64、请简述 Linux 启动过程中几个重要配置文件的执行过程**
Linux 登录后，配置执行顺序为(Debian Serials Capable)：
/etc/environment -> /etc/profile -> (~/.bash_profile | ~/.bash_login | ~/.profile) -> ~/.bashrc -> /etc/bashrc -> ~/.bash_logout
关于各个文件的作用说明：
（1）/etc/environment：此配置文件设置基本的 PATH 变量，及系统当前语言变量，虽然比较短，但却在系统启动中占据举足轻重的作用，比如如下是我的系统中的内容：
（2）/etc/profile：此文件为系统的每个用户设置环境信息,当用户第一次登录时,该文件被执行. 并从/etc/profile.d 目录的配置文件中搜集 shell 的设置。
（3）/etc/bash.bashrc: 为每一个运行 bash shell 的用户执行此文件.当 bash shell 被打开时,该文件被读取。
（4）~/.bash_profile: 每个用户都可使用该文件输入专用于自己使用的 shell 信息,当用户登录时,该文件仅仅执行一次!默认情况下,他设置一些环境变量,执行用户的.bashrc 文件。

（5）~/.bashrc: 该文件包含专用于你的 bash shell 的 bash 信息,当登录时以及每次打开新的 shell 时,该该文件被读取。
（6）~/.bash_logout: 当每次退出系统(退出 bash shell)时,执行该文件. 另外,/etc/profile 中设定的变量(全局)的可以作用于任何用户,而~/.bashrc 等中设定的变量(局部)只能继承 /etc/profile 中的变量,他们是"父子"关系。
（7）~/.bash_profile 是交互式、login 方式进入 bash 运行的~/.bashrc 是交互式 non-login 方式进入 bash 运行的通常二者设置大致相同，所以通常前者会调用后者。

65、请描述下列路径的内容是做什么的？
/var/log/messages 系统日志文件
/var/log/secure 系统安全文件（显示登录信息的文件）
/var/spool/clientmqueue 例行性任务回执邮件存放文件
/proc/interrupts 当前系统中断报告文件
/etc/fstab 开机自动挂载磁盘的配置文件
/etc/profile 环境变量存放的文件

66、请给出 Linux 中 eth0 的 IP 地址和广播地址的指令，需使用 cut、awk、grep、sed 指令。
第一种方法：使用 grep 和 cut 取值
第二种方法：使用 grep 和 awk（默认分隔符为空格）取值
第三种方法：使用 grep 和 awk（多分隔符）
第四种方法：使用 sed 和 awk
第五种方法：使用 grep 和 awk（多分隔符与加号+）
第六种方法：awk （分隔符及取行）
第七种方法：grep 网卡文件
第八种方法：head 取行 awk 分割

67、请输出你知道的 20 个 LINUX 命令及作用
cp 复制 -a(drp),
-r 拷贝目录
-p 保持属性
mv 移动文件或目录
mkdir 创建目录
-p 递归创建目录 mkdir /a/b/c
touch 创建文件，
cd 切换目录（~当前用户家目录，-上一次的目录）
cat 查看文件内容
-n 显示行号
ls 查看目录下文件，
-l 长格式
-d 查看目录
rm 删除文件或目录
-r 目录 -f 强制删除（慎用，mv,find）
find 查找文件或目录 -type 类型（f,d,l,c,b），-name 名字 -exec 执行动作*****
alias 查看及设置别名

unalias 取消别名
seq 打印序列 -s 指定分割符 -w 数字前面加 0 补齐位数
head 查看文件前 N 行，默认 10 行，-n 指定行数
tail 查看文件后 N 行，默认 10 行，-n 指定行数,-f 实时跟踪文件结尾的变化
sed linux 三剑客老二，文件增删改查，*****
pwd 打印当前工作目录
rmdir 删除空目录
echo 显示输出
xargs (配合 find,ls)等查找到的内容处理,-n 分组
tree -L 层数 -d 目录
rpm -q query 查询 -a all
uname -r 内核 -m32 位还是 64 位 -a 所有信息, -n 主机名（hostname）
hostname 主机名
whoami 查看当前用户
useradd 添加用户
passwd 改密码，–stdin 非交互设置密码
su 切换用户角色，-切换环境变量

68、写一个脚本查找最后创建时间是 3 天前，后缀是*.log 的文件并删除。
find / -name “*.log” -ctime +3 -exec rm -f {} \;

69、写一个脚本将某目录下大于 100k 的文件移动至/tmp 下。
for i in `find /test -type f -size +100k`;do cd /test && mv $i /tmp;done

70、写一个脚本将数据库备份并打包至远程服务器 192.168.1.1 /backup 目录下。
mount 192.168.1.1:/backup /mnt
cd /mnt
/usr/local/mysql/bin/mysqldump -hlocalhost -uroot test >test.sql
tar czf test.sql.tar.gz test.sql
rm -f test.sql

71、写一个防火墙配置脚本，只允许远程主机访问本机的 80 端口。
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
iptables -X
iptables -A INPUT -i eth0 -p tcp –dport 80 -j ACCEPT
iptables -P INPUT DROP

72、写一个脚本进行 nginx 日志统计，得到访问 ip 最多的前 10 个(nginx 日志路径：
/home/logs/nginx/default/access.log
awk ‘{a[$1]++}END{for (j in a) print a[j],j}’ /home/logs/nginx/default/access.log|sort -nr|head -10

73、写出下列配置的含义

（1）MaxKeepAliveRequests 100

（2）Options FollowSymLinks

Order Deny Allow

Deny from all

Allow from 192.168.1.1

（1）MaxKeepAliveRequests — 100 连接的最大请求数

（2）Options FollowSymLinks — 允许 192.168.1.1 可以列目录

Order Deny Allow

Deny from all

Allow from 192.168.1.1

74、写一个脚本把指定文件里的/usr/local 替换为别的目录。

sed 's:/user/local:/tmp:g' filename

75、简要描述 Linux 的启动过程？

BIOS 启动引导(从 mbr 中装载启动管理器 grub)—-GRUB 启动引导(装载 kernel 和 initrd 到内存)——内核启动参数-sys init 初始化..

76、简要叙述下列端口所运行的服务

21、22、23、25、110、143、873、3306 对应的服务是 ftp ssh telnet snmp pop3 IMAP rsync

77、TCP 断头最小长度是多少字节？

64 字节

78、让某普通用户能进行 cp /dir1/file1 /dir2 的命令时，请说明 dir1 file1 最小具有什么权限？

读取和执行权限 rx

79、简述 TCP 三次握手的过程？

客户端发送请求 SYN,服务器端接收请求确认并回应 SYN+ACK,客户端发回 ACK 回应….

80、如何查看当前的 Linux 服务器的运行级别？

答: 'who -r' 和 'runlevel' 命令可以用来查看当前的 Linux 服务器的运行级别。

81、如何查看 Linux 的默认网关？

答: 用 "route -n" 和 "netstat -nr" 命令，我们可以查看默认网关。

除了默认的网关信息，这两个命令还可以显示当前的路由表。

82、如何在 Linux 上重建初始化内存盘镜像文件？

答: 在 CentOS 5.X / RHEL 5.X 中，可以用 mkinitrd 命令来创建初始化内存盘文件。

举例如下：

```
1. # mkinitrd -f -v /boot/initrd-$(uname -r).img $(uname -r)
```

如果你想要给特定的内核版本创建初始化内存盘，你就用所需的内核名替换掉‘uname -r’。
在 CentOS 6.X / RHEL 6.X 中，则用 dracut 命令来创建初始化内存盘文件，举例如下：

```
# dracut -f
```

给特定的内核版本重建初始化内存盘文件则使用以下命令：

```
# dracut -f initramfs-2.x.xx-xx.el6.x86_64.img 2.x.xx-xx.el6.x86_64
```

83、cpio 命令是什么？

答: cpio 就是复制入和复制出的意思。
cpio 可以向一个归档文件（或单个文件）复制文件、列表，还可以从中提取文件。

84、patch 命令是什么？如何使用？

答: 顾名思义，patch 命令就是用来将修改（或补丁）写进文本文件里。
patch 命令通常是接收 diff 的输出并把文件的旧版本转换为新版本。
举个例子，Linux 内核源代码由百万行代码文件构成，所以无论何时，任何代码贡献者贡献出代码，只需发送改动的部分而不是整个源代码，然后接收者用 patch 命令将改动写进原始的源代码里。
创建一个 diff 文件给 patch 使用，

```
# diff -Naur old_file new_file > diff_file
```

旧文件和新文件要么都是单个的文件要么都是包含文件的目录，-r 参数支持目录树递归。
一旦 diff 文件创建好，我们就能在旧的文件上打上补丁，把它变成新文件：

```
# patch < diff_file
```

85、aspell 有什么用 ？

答: 顾名思义，aspell 就是 Linux 操作系统上的一款交互式拼写检查器。
aspell 命令继任了更早的一个名为 ispell 的程序，并且作为一款免费替代品 ，最重要的是它非常好用。
当 aspell 程序主要被其它一些需要拼写检查能力的程序所使用的时候，在命令行中作为一个独立运行的工具的它也能十分有效。

86、如何从命令行查看域 SPF 记录？

答: 我们可以用 dig 命令来查看域 SPF 记录。举例如下：

```
linuxtechi@localhost:~$ dig -t TXT google.com
```

87、如何识别 Linux 系统中指定文件(/etc/fstab)的关联包？

答:

```
# rpm -qf /etc/fstab
```

以上命令能列出提供”/etc/fstab”这个文件的包。

88、哪条命令用来查看 bond0 的状态？

答:

```
cat /proc/net/bonding/bond0
```

89、Linux 系统中的/proc 文件系统有什么用？

答: /proc 文件系统是一个基于内存的文件系统，其维护着关于当前正在运行的内核状态信息，其中包括 CPU、内存、分区划分、I/O 地址、直接内存访问通道和正在运行的进程。

这个文件系统所代表的并不是各种实际存储信息的文件，它们指向的是内存里的信息。/proc 文件系统是由系统自动维护的。

90、如何在/usr 目录下找出大小超过 10MB 的文件？

答:

```
# find /usr -size +10M
```

91、如何在/home 目录下找出 120 天之前被修改过的文件？

答:

```
# find /home -mtime +120
```

92、如何在/var 目录下找出 90 天之内未被访问过的文件？

答:

```
# find /var \! -atime -90
```

93、在整个目录树下查找文件”core”，如发现则无需提示直接删除它们。

答:

```
# find / -name core -exec rm {} \;
```

94、strings 命令有什么作用？

答: strings 命令用来提取和显示非文本文件中的文本字符串。

当用来分析你系统上莫名其妙出现的二进制程序时，可以从中找到可疑的文件访问，对于追查入侵有用处。

95、tee 过滤器有什么作用 ？

答: tee 过滤器用来向多个目标发送输出内容。

如果用于管道的话，它可以将输出复制一份到一个文件，并复制另外一份到屏幕上（或一些其它程序）。

```
1. linuxtechi@localhost:~$ ll /etc | nl | tee /tmp/ll.out
```

在以上例子中，从 ll 输出可以捕获到 /tmp/ll.out 文件中，并且同样在屏幕上显示了出来。

96、export PS1 = "$LOGNAME@hostname:\$PWD:" 这条命令是在做什么？

答: 这条 export 命令会更改登录提示符来显示用户名、本机名和当前工作目录。

97、ll | awk '{print $3,"owns",$9}' 这条命令是在做什么？

答: 这条 ll 命令会显示这些文件的文件名和它们的拥有者。

98、Linux 中的 at 命令有什么用？

答: at 命令用来安排一个程序在未来的做一次一次性执行。

所有提交的任务都被放在 /var/spool/at 目录下并且到了执行时间的时候通过 atd 守护进程来执行。

99、linux 中 lspci 命令的作用是什么？

答: lspci 命令用来显示你的系统上 PCI 总线和附加设备的信息。

指定-v，-vv 或-vvv 来获取越来越详细的输出，加上-r 参数的话，命令的输出则会更具有易读性。

100、什么是运维？什么是游戏运维？

1）运维是指大型组织已经建立好的网络软硬件的维护，就是要保证业务的上线与运作的正常，

在他运转的过程中，对他进行维护，他集合了网络、系统、数据库、开发、安全、监控于一身的技术

运维又包括很多种，有 DBA 运维、网站运维、虚拟化运维、监控运维、游戏运维等等

2）游戏运维又有分工，分为开发运维、应用运维（业务运维）和系统运维

开发运维：是给应用运维开发运维工具和运维平台的

应用运维：是给业务上线、维护和做故障排除的，用开发运维开发出来的工具给业务上线、维护、做故障排查

系统运维：是给应用运维提供业务上的基础设施，比如：系统、网络、监控、硬件等等

总结：开发运维和系统运维给应用运维提供了"工具"和"基础设施"上的支撑

开发运维、应用运维和系统运维他们的工作是环环相扣的

101、在工作中，运维人员经常需要跟运营人员打交道，请问运营人员是做什么工作的？

游戏运营要做的一个事情除了协调工作以外

还需要与各平台沟通，做好开服的时间、开服数、用户导量、活动等计划

102、现在给你三百台服务器，你怎么对他们进行管理？

管理 3 百台服务器的方式：

1）设定跳板机，使用统一账号登录，便于安全与登录的考量。

2）使用 salt、ansiable、puppet 进行系统的统一调度与配置的统一管理。

3）建立简单的服务器的系统、配置、应用的 cmdb 信息管理。便于查阅每台服务器上的各种信息记录。

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

RAID，可以把硬盘整合成一个大磁盘，还可以在大磁盘上再分区，放数据

还有一个大功能，多块盘放在一起可以有冗余（备份）

RAID 整合方式有很多，常用的：0 1 5 10

RAID 0，可以是一块盘和 N 个盘组合

其优点读写快，是 RAID 中最好的

缺点：没有冗余，一块坏了数据就全没有了

RAID 1，只能 2 块盘，盘的大小可以不一样，以小的为准

10G+10G 只有 10G，另一个做备份。它有 100%的冗余，缺点：浪费资源，成本高

RAID 5 ，3 块盘，容量计算 10*（n-1）,损失一块盘

特点，读写性能一般，读还好一点，写不好

冗余从好到坏：RAID1 RAID10 RAID 5 RAID0

性能从好到坏：RAID0 RAID10 RAID5 RAID1

成本从低到高：RAID0 RAID5 RAID1 RAID10

单台服务器：很重要盘不多，系统盘，RAID1

数据库服务器：主库：RAID10 从库 RAID5RAID0（为了维护成本，RAID10）

WEB 服务器，如果没有太多的数据的话，RAID5,RAID0（单盘）

有多台，监控、应用服务器，RAID0 RAID5

我们会根据数据的存储和访问的需求，去匹配对应的 RAID 级别

104、LVS、Nginx、HAproxy 有什么区别？工作中你怎么选择？

LVS： 是基于四层的转发

HAproxy： 是基于四层和七层的转发，是专业的代理服务器

Nginx： 是 WEB 服务器，缓存服务器，又是反向代理服务器，可以做七层的转发

区别： LVS 由于是基于四层的转发所以只能做端口的转发

而基于 URL 的、基于目录的这种转发 LVS 就做不了

工作选择：

HAproxy 和 Nginx 由于可以做七层的转发，所以 URL 和目录的转发都可以做

在很大并发量的时候我们就要选择 LVS，像中小型公司的话并发量没那么大

选择 HAproxy 或者 Nginx 足已，由于 HAproxy 由是专业的代理服务器

配置简单，所以中小型企业推荐使用 HAproxy

105、Squid、Varinsh 和 Nginx 有什么区别，工作中你怎么选择？

Squid、Varinsh 和 Nginx 都是代理服务器

什么是代理服务器：

能当替用户去访问公网，并且能把访问到的数据缓存到服务器本地，等用户下次再访问相同的资源的时候，代理服务器直接从本地回应给用户，当本地没有的时候，我代替你去访问公网，我接收你的请求，我先在我自己的本地缓存找，如果我本地缓存有，我直接从我本地的缓存里回复你，如果我在我本地没有找到你要访问的缓存的数据，那么代理服务器就会代替你去访问公网

区别：
1）Nginx 本来是反向代理/web 服务器，用了插件可以做做这个副业
但是本身不支持特性挺多，只能缓存静态文件
2）从这些功能上。varnish 和 squid 是专业的 cache 服务，而 nginx 这些是第三方模块完成
3）varnish 本身的技术上优势要高于 squid，它采用了可视化页面缓存技术在内存的利用上，Varnish 比 Squid 具有优势，性能要比 Squid 高。还有强大的通过 Varnish 管理端口，可以使用正则表达式快速、批量地清除部分缓存，它是内存缓存，速度一流，但是内存缓存也限制了其容量，缓存页面和图片一般是挺好的
4）squid 的优势在于完整的庞大的 cache 技术资料，和很多的应用生产环境
工作中选择：
要做 cache 服务的话，我们肯定是要选择专业的 cache 服务，优先选择 squid 或者 varnish。

106、Tomcat 和 Resin 有什么区别，工作中你怎么选择？
区别：Tomcat 用户数多，可参考文档多，Resin 用户数少，可考虑文档少
最主要区别则是 Tomcat 是标准的 java 容器，不过性能方面比 resin 的要差一些
但稳定性和 java 程序的兼容性，应该是比 resin 的要好
工作中选择：现在大公司都是用 resin，追求性能；而中小型公司都是用 Tomcat，追求稳定和程序的兼容

107、什么是中间件？什么是 jdk？
中间件介绍：
中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源
中间件位于客户机/ 服务器的操作系统之上，管理计算机资源和网络通讯
是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口
但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递
通过中间件，应用程序可以工作于多平台或 OS 环境。
jdk：jdk 是 Java 的开发工具包
它是一种用于构建在 Java 平台上发布的应用程序、applet 和组件的开发环境

108、讲述一下 Tomcat8005、8009、8080 三个端口的含义？
8005==》 关闭时使用
8009==》 为 AJP 端口，即容器使用，如 Apache 能通过 AJP 协议访问 Tomcat 的 8009 端口
8080==》 一般应用使用
109、什么叫 CDN？
即内容分发网络
其目的是通过在现有的 Internet 中增加一层新的网络架构，将网站的内容发布到
最接近用户的网络边缘，使用户可就近取得所需的内容，提高用户访问网站的速度

110、什么叫网站灰度发布？

灰度发布是指在黑与白之间，能够平滑过渡的一种发布方式

AB test 就是一种灰度发布方式，让一部用户继续用 A，一部分用户开始用 B

如果用户对 B 没有什么反对意见，那么逐步扩大范围，把所有用户都迁移到 B 上面 来

灰度发布可以保证整体系统的稳定，在初始灰度的时候就可以发现、调整问题，以保证其影响度

111、简述 DNS 进行域名解析的过程？

用户要访问 www.baidu.com，会先找本机的 host 文件，再找本地设置的 DNS 服务器，如果也没有的话，就去网络中找根服务器，根服务器反馈结果，说只能提供一级域名服务器.cn，就去找一级域名服务器，一级域名服务器说只能提供二级域名服务器.com.cn,就去找二级域名服务器，二级域服务器只能提供三级域名服务器.baidu.com.cn，就去找三级域名服务器，三级域名服务器正好有这个网站 www.baidu.com，然后发给请求的服务器，保存一份之后，再发给客户端

112、RabbitMQ 是什么东西？

RabbitMQ 也就是消息队列中间件，消息中间件是在消息的传息过程中保存消息的容器

消息中间件再将消息从它的源中到它的目标中标时充当中间人的作用

队列的主要目的是提供路由并保证消息的传递；如果发送消息时接收者不可用

消息队列不会保留消息，直到可以成功地传递为止，当然，消息队列保存消息也是有期限地

113、讲一下 Keepalived 的工作原理？

在一个虚拟路由器中，只有作为 MASTER 的 VRRP 路由器会一直发送 VRRP 通告信息,

BACKUP 不会抢占 MASTER，除非它的优先级更高。当 MASTER 不可用时(BACKUP 收不到通告信息)

多台 BACKUP 中优先级最高的这台会被抢占为 MASTER。这种抢占是非常快速的(<1s)，以保证服务的连续性

由于安全性考虑，VRRP 包使用了加密协议进行加密。BACKUP 不会发送通告信息，只会接收通告信息

114、讲述一下 LVS 三种模式的工作过程？

LVS 有三种负载均衡的模式，分别是 VS/NAT（nat 模式） VS/DR(路由模式) VS/TUN（隧道模式）

一、NAT 模式（VS-NAT）

原理：就是把客户端发来的数据包的 IP 头的目的地址，在负载均衡器上换成其中一台 RS 的 IP 地址并发至此 RS 来处理,RS 处理完后把数据交给负载均衡器,负载均衡器再把数据包原 IP 地址改为自己的 IP 将目的地址改为客户端 IP 地址即可期间,无论是进来的流量,还是出去的流量,都必须经过负载均衡器

优点：集群中的物理服务器可以使用任何支持 TCP/IP 操作系统，只有负载均衡器需要一个合法的 IP 地址

缺点：扩展性有限。当服务器节点（普通 PC 服务器）增长过多时,负载均衡器将成为整个系

统的瓶颈
因为所有的请求包和应答包的流向都经过负载均衡器。当服务器节点过多时
大量的数据包都交汇在负载均衡器那，速度就会变慢！

二、IP 隧道模式（VS-TUN）
原理：首先要知道，互联网上的大多 Internet 服务的请求包很短小，而应答包通常很大
那么隧道模式就是，把客户端发来的数据包，封装一个新的 IP 头标记(仅目的 IP)发给 RS
RS 收到后,先把数据包的头解开,还原数据包,处理后,直接返回给客户端,不需要再经过负载均衡器。注意,由于 RS 需要对负载均衡器发过来的数据包进行还原,所以说必须支持 IPTUNNEL 协议，所以,在 RS 的内核中,必须编译支持 IPTUNNEL 这个选项

优点：负载均衡器只负责将请求包分发给后端节点服务器，而 RS 将应答包直接发给用户
所以，减少了负载均衡器的大量数据流动，负载均衡器不再是系统的瓶颈，就能处理很巨大的请求量，这种方式，一台负载均衡器能够为很多 RS 进行分发。而且跑在公网上就能进行不同地域的分发。

缺点：隧道模式的 RS 节点需要合法 IP，这种方式需要所有的服务器支持”IP Tunneling”
(IP Encapsulation)协议，服务器可能只局限在部分 Linux 系统上

三、直接路由模式（VS-DR）
原理：负载均衡器和 RS 都使用同一个 IP 对外服务但只有 DR 对 ARP 请求进行响应
所有 RS 对本身这个 IP 的 ARP 请求保持静默也就是说,网关会把对这个服务 IP 的请求全部定向给 DR，而 DR 收到数据包后根据调度算法,找出对应的 RS,把目的 MAC 地址改为 RS 的 MAC（因为 IP 一致）并将请求分发给这台 RS 这时 RS 收到这个数据包,处理完成之后，由于 IP 一致，可以直接将数据返给客户，则等于直接从客户端收到这个数据包无异,处理后直接返回给客户端，由于负载均衡器要对二层包头进行改换,所以负载均衡器和 RS 之间必须在一个广播域，也可以简单的理解为在同一台交换机上

优点：和 TUN（隧道模式）一样，负载均衡器也只是分发请求，应答包通过单独的路由方法返回给客户端
与 VS-TUN 相比，VS-DR 这种实现方式不需要隧道结构，因此可以使用大多数操作系统做为物理服务器。
缺点：（不能说缺点，只能说是不足）要求负载均衡器的网卡必须与物理网卡在一个物理段上。

115、mysql 的 innodb 如何定位锁问题，mysql 如何减少主从复制延迟？
mysql 的 innodb 如何定位锁问题:
在使用 show engine innodb status 检查引擎状态时，发现了死锁问题
在 5.5 中，information_schema 库中增加了三个关于锁的表（MEMORY 引擎）
innodb_trx ## 当前运行的所有事务
innodb_locks ## 当前出现的锁
innodb_lock_waits ## 锁等待的对应关系

mysql 如何减少主从复制延迟:

如果延迟比较大，就先确认以下几个因素：
从库硬件比主库差，导致复制延迟
主从复制单线程，如果主库写并发太大，来不及传送到从库
就会导致延迟。更高版本的 mysql 可以支持多线程复制
慢 SQL 语句过多
网络延迟
master 负载
主库读写压力大，导致复制延迟，架构的前端要加 buffer 及缓存层
slave 负载
一般的做法是，使用多台 slave 来分摊读请求，再从这些 slave 中取一台专用的服务器
只作为备份用，不进行其他任何操作.另外， 2 个可以减少延迟的参数:
–slave-net-timeout=seconds 单位为秒 默认设置为 3600 秒
参数含义：当 slave 从主数据库读取 log 数据失败后，等待多久重新建立连接并获取数据
–master-connect-retry=seconds 单位为秒 默认设置为 60 秒
参数含义：当重新建立主从连接时，如果连接建立失败，间隔多久后重试
通常配置以上 2 个参数可以减少网络问题导致的主从数据同步延迟
MySQL 数据库主从同步延迟解决方案
最简单的减少 slave 同步延时的方案就是在架构上做优化，尽量让主库的 DDL 快速执行
还有就是主库是写，对数据安全性较高，比如 sync_binlog=1，innodb_flush_log_at_trx_commit = 1 之类的设置，而 slave 则不需要这么高的数据安全，完全可以讲 sync_binlog 设置为 0 或者关闭 binlog
innodb_flushlog 也可以设置为 0 来提高 sql 的执行效率。另外就是使用比主库更好的硬件设备作为 slave

116、如何重置 mysql root 密码？

一、 在已知 MYSQL 数据库的 ROOT 用户密码的情况下，修改密码的方法：
1、 在 SHELL 环境下，使用 mysqladmin 命令设置：
mysqladmin –u root –p password “新密码” 回车后要求输入旧密码
2、 在 mysql>环境中,使用 update 命令，直接更新 mysql 库 user 表的数据：
Update mysql.user set password=password(‘新密码’) where user=’root’;
flush privileges;
注意：mysql 语句要以分号”；”结束
3、 在 mysql>环境中，使用 grant 命令，修改 root 用户的授权权限。
grant all on . to root@’localhost’ identified by ‘新密码’;

二、 如查忘记了 mysql 数据库的 ROOT 用户的密码，又如何做呢？方法如下：
1、关闭当前运行的 mysqld 服务程序：service mysqld stop（要先将 mysqld 添加为系统服务）
2、 使用 mysqld_safe 脚本以安全模式（不加载授权表）启动 mysqld 服务
/usr/local/mysql/bin/mysqld_safe –skip-grant-table &
3、 使用空密码的 root 用户登录数据库，重新设置 ROOT 用户的密码
＃mysql -u root
Mysql> Update mysql.user set password=password(‘新密码’) where user=’root’;
Mysql> flush privileges;

117、lvs/nginx/haproxy 优缺点

Nginx 的优点是：

1、工作在网络的 7 层之上，可以针对 http 应用做一些分流的策略，比如针对域名、目录结构

它的正则规则比 HAProxy 更为强大和灵活，这也是它目前广泛流行的主要原因之一

Nginx 单凭这点可利用的场合就远多于 LVS 了。

2、Nginx 对网络稳定性的依赖非常小，理论上能 ping 通就就能进行负载功能，这个也是它的优势之一

相反 LVS 对网络稳定性依赖比较大，这点本人深有体会；

3、Nginx 安装和配置比较简单，测试起来比较方便，它基本能把错误用日志打印出来

LVS 的配置、测试就要花比较长的时间了，LVS 对网络依赖比较大。

4、可以承担高负载压力且稳定，在硬件不差的情况下一般能支撑几万次的并发量，负载度比 LVS 相对小些。

5、Nginx 可以通过端口检测到服务器内部的故障，比如根据服务器处理网页返回的状态码、超时等等，并且会把返回错误的请求重新提交到另一个节点，不过其中缺点就是不支持 url 来检测。比如用户正在上传一个文件，而处理该上传的节点刚好在上传过程中出现故障，Nginx 会把上传切到另一台服务器重新处理，而 LVS 就直接断掉了

如果是上传一个很大的文件或者很重要的文件的话，用户可能会因此而不满。

6、Nginx 不仅仅是一款优秀的负载均衡器/反向代理软件，它同时也是功能强大的 Web 应用服务器

LNMP 也是近几年非常流行的 web 架构，在高流量的环境中稳定性也很好。

7、Nginx 现在作为 Web 反向加速缓存越来越成熟了，速度比传统的 Squid 服务器更快，可考虑用其作为反向代理加速器

8、Nginx 可作为中层反向代理使用，这一层面 Nginx 基本上无对手，唯一可以对比 Nginx 的就只有 lighttpd 了

不过 lighttpd 目前还没有做到 Nginx 完全的功能，配置也不那么清晰易读，社区资料也远远没 Nginx 活跃

9、Nginx 也可作为静态网页和图片服务器，这方面的性能也无对手。还有 Nginx 社区非常活跃，第三方模块也很多

Nginx 的缺点是：

1、Nginx 仅能支持 http、https 和 Email 协议，这样就在适用范围上面小些，这个是它的缺点

2、对后端服务器的健康检查，只支持通过端口来检测，不支持通过 url 来检测

不支持 Session 的直接保持，但能通过 ip_hash 来解决

LVS：使用 Linux 内核集群实现一个高性能、高可用的负载均衡服务器

它具有很好的可伸缩性（Scalability)、可靠性（Reliability)和可管理性（Manageability)

LVS 的优点是：

1、抗负载能力强、是工作在网络 4 层之上仅作分发之用，没有流量的产生

这个特点也决定了它在负载均衡软件里的性能最强的，对内存和 cpu 资源消耗比较低

2、配置性比较低，这是一个缺点也是一个优点，因为没有可太多配置的东西

所以并不需要太多接触，大大减少了人为出错的几率

3、工作稳定，因为其本身抗负载能力很强，自身有完整的双机热备方案
如 LVS+Keepalived，不过我们在项目实施中用得最多的还是 LVS/DR+Keepalived
4、无流量，LVS 只分发请求，而流量并不从它本身出去，这点保证了均衡器 IO 的性能不会收到大流量的影响。
5、应用范围较广，因为 LVS 工作在 4 层，所以它几乎可对所有应用做负载均衡，包括 http、数据库、在线聊天室等

LVS 的缺点是：
1、软件本身不支持正则表达式处理，不能做动静分离
而现在许多网站在这方面都有较强的需求，这个是 Nginx/HAProxy+Keepalived 的优势所在
2、如果是网站应用比较庞大的话，LVS/DR+Keepalived 实施起来就比较复杂了
特别后面有 Windows Server 的机器的话，如果实施及配置还有维护过程就比较复杂了
相对而言，Nginx/HAProxy+Keepalived 就简单多了。

HAProxy 的特点是：
1、HAProxy 也是支持虚拟主机的。
2、HAProxy 的优点能够补充 Nginx 的一些缺点，比如支持 Session 的保持，Cookie 的引导
同时支持通过获取指定的 url 来检测后端服务器的状态
3、HAProxy 跟 LVS 类似，本身就只是一款负载均衡软件
单纯从效率上来讲 HAProxy 会比 Nginx 有更出色的负载均衡速度，在并发处理上也是优于 Nginx 的
4、HAProxy 支持 TCP 协议的负载均衡转发，可以对 MySQL 读进行负载均衡
对后端的 MySQL 节点进行检测和负载均衡，大家可以用 LVS+Keepalived 对 MySQL 主从做负载均衡
5、HAProxy 负载均衡策略非常多，HAProxy 的负载均衡算法现在具体有如下 8 种：
①roundrobin，表示简单的轮询，这个不多说，这个是负载均衡基本都具备的；
② static-rr，表示根据权重，建议关注；
③leastconn，表示最少连接者先处理，建议关注；
④ source，表示根据请求源 IP，这个跟 Nginx 的 IP_hash 机制类似
我们用其作为解决 session 问题的一种方法，建议关注；
⑤ri，表示根据请求的 URI；
⑥rl_param，表示根据请求的 URl 参数'balance url_param' requires an URL parameter name；
⑦hdr(name)，表示根据 HTTP 请求头来锁定每一次 HTTP 请求；
⑧rdp-cookie(name)，表示根据据 cookie(name)来锁定并哈希每一次 TCP 请求。

118、mysql 数据备份工具
mysqldump 工具
mysqldump 是 mysql 自带的备份工具，目录在 bin 目录下面：/usr/local/mysql/bin/mysqldump
支持基于 innodb 的热备份，但是由于是逻辑备份，所以速度不是很快，适合备份数据比较小的场景
Mysqldump 完全备份+二进制日志可以实现基于时间点的恢复。

基于 LVM 快照备份
在物理备份中，有基于文件系统的物理备份（LVM 的快照），也可以直接用 tar 之类的命令

对整个数据库目录
进行打包备份，但是这些只能进行冷备份，不同的存储引擎备份的也不一样，myisam 自动备份到表级别
而 innodb 不开启独立表空间的话只能备份整个数据库。

tar 包备份
percona 提供的 xtrabackup 工具
支持 innodb 的物理热备份，支持完全备份，增量备份，而且速度非常快，支持 innodb 存储引起的数据在不同
数据库之间迁移，支持复制模式下的从机备份恢复备份恢复，为了让 xtrabackup 支持更多的功能扩展
可以设立独立表空间，打开 innodb_file_per_table 功能，启用之后可以支持单独的表备份

119、keepalive 的工作原理和如何做到健康检查
keepalived 是以 VRRP 协议为实现基础的，VRRP 全称 Virtual Router Redundancy Protocol，即虚拟路由冗余协议。
虚拟路由冗余协议，可以认为是实现路由器高可用的协议，即将 N 台提供相同功能的路由器组成一个路由器组
这个组里面有一个 master 和多个 backup，master 上面有一个对外提供服务的 vip（该路由器所在局域网内
其他机器的默认路由为该 vip），master 会发组播，当 backup 收不到 vrrp 包时就认为 master 宕掉了
这时就需要根据 VRRP 的优先级来选举一个 backup 当 master。这样就可以保证路由器的高可用了
keepalived 主要有三个模块，分别是 core、check 和 vrrp。core 模块为 keepalived 的核心，负责主进程的启动、维护
及全局配置文件的加载和解析。check 负责健康检查，包括常见的各种检查方式，vrrp 模块是来实现 VRRP 协议的
Keepalived 健康检查方式配置
HTTP_GET|SSL_GET
HTTP_GET | SSL_GET
{
url {
path /# HTTP/SSL 检查的 url 可以是多个
digest # HTTP/SSL 检查后的摘要信息用工具 genhash 生成
status_code 200# HTTP/SSL 检查返回的状态码
}
connect_port 80 # 连接端口
bindto
connect_timeout 3 # 连接超时时间
nb_get_retry 3 # 重连次数
delay_before_retry 2 #连接间隔时间
}

120、统计 ip 访问情况，要求分析 nginx 访问日志，找出访问页面数量在前十位的 ip

cat access.log | awk '{print $1}' | uniq -c | sort -rn | head -10

121、使用 tcpdump 监听主机为 192.168.1.1，tcp 端口为 80 的数据，同时将输出结果保存输出到 tcpdump.log

tcpdump 'host 192.168.1.1 and port 80' > tcpdump.log

122、如何将本地 80 端口的请求转发到 8080 端口，当前主机 IP 为 192.168.2.1

iptables -A PREROUTING -d 192.168.2.1 -p tcp -m tcp -dport 80 -j DNAT-to-destination 192.168.2.1:8080

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

RAID 0：带区卷，连续以位或字节为单位分割数据，并行读/写于多个磁盘上，因此具有很高的数据传输率

但它没有数据冗余，RAID 0 只是单纯地提高性能，并没有为数据的可靠性提供保证

而且其中的一个磁盘失效将影响到所有数据。因此，RAID 0 不能应用于数据安全性要求高的场合

RAID 1：镜像卷，它是通过磁盘数据镜像实现数据冗余，在成对的独立磁盘上产生互为备份的数据

不能提升写数据效率。当原始数据繁忙时，可直接从镜像拷贝中读取数据，因此 RAID1 可以提高读取性能

RAID 1 是磁盘阵列中单位成本最高的，镜像卷可用容量为总容量的 1/2，但提供了很高的数据安全性和可用性

当一个磁盘失效时，系统可以自动切换到镜像磁盘上读写，而不需要重组失效的数据

RAID5：至少由 3 块硬盘组成，分布式奇偶校验的独立磁盘结构，它的奇偶校验码存在于所有磁盘上

任何一个硬盘损坏，都可以根据其它硬盘上的校验位来重建损坏的数据（最多允许 1 块硬盘损坏）

所以 raid5 可以实现数据冗余，确保数据的安全性，同时 raid5 也可以提升数据的读写性能

124、你对现在运维工程师的理解和以及对其工作的认识

运维工程师在公司当中责任重大，需要保证时刻为公司及客户提供最高、最快、最稳定、最安全的服务

运维工程师的一个小小的失误，很有可能会对公司及客户造成重大损失

因此运维工程师的工作需要严谨及富有创新精神

125、实时抓取并显示当前系统中 tcp 80 端口的网络数据信息，请写出完整操作命令

tcpdump -nn tcp port 80

126、服务器开不了机怎么解决一步步的排查

A、造成服务器故障的原因可能有以下几点：

1：服务器电源有问题(断电，电源线松动，人为原因)。

2：服务器系统文件丢失，硬件问题，散热不良造成蓝屏和死机。

3：服务器网络参数配置错误，物理链路原因等。

B、如何排查服务器故障的处理步骤如下：

1：1、先看服务器的电源指示灯是否亮，如果电源灯不亮,先检查并确认电源没问题时,试着按开机键是否能点亮服务器.如果不能点亮,和数据确认后先更换备用服务器以便快速恢复业务.

2： 2 如果服务器电源灯亮,接上显示器和键盘,如果服务器系统有异常(比如蓝屏…)不能正常登录系统,先和数据确认,是否执行能重启服务器或是更换备用服务器，以便快速恢复业务.

3： 3 如果正确输入用户名和密码情况下能登录系统,查看网卡指示灯是否正常,并用 ifconfig 命令查看网卡接口状态。用 ping 对 端 ip 测试网络是否连通,

4：4、如果 ping 不通，先和数据人员确认并检查网卡配置文件参数是否配置正确，是否正确配置网关(不正确则修正后)用“ifdown ; ifup 网卡名“命令重启单个网卡，网卡接口(灯)状态正常后，再用 ping 命令测试,

5：5、还 ping 不通，及时排查并确保本地尾纤，模块等物理设备接入正常，收发光在规定范围内，和数据人员确认是否可以重启服务器，并确认数据方面没有网络配置和数据方面的变化。

6：6、能 ping 通则告知数据人员，并让数据人员帮忙确认链路是否正常，有没有丢包现象等，没有丢包就 OK,有丢包就继续排查尾纤，模块等，直到链路正常没有丢包,数据人员能及时的从远程登录服务器做数据配置能快速恢复业务为 OK。

7 、7、如果不能接入服务器，与数据确认是否可以重启，重启后登陆正常，继续 3.4.5.6 步骤，如果还是不行，权衡利弊，有没有必要更换新的服务器上去，恢复业务要紧。

127、Linux 系统中病毒怎么解决

1）最简单有效的方法就是重装系统

2）要查的话就是找到病毒文件然后删除

中毒之后一般机器 cpu、内存使用率会比较高

机器向外发包等异常情况，排查方法简单介绍下

top 命令找到 cpu 使用率最高的进程

一般病毒文件命名都比较乱，可以用 ps aux 找到病毒文件位置

rm -f 命令删除病毒文件

检查计划任务、开机启动项和病毒文件目录有无其他可以文件等

3）由于即使删除病毒文件不排除有潜伏病毒，所以最好是把机器备份数据之后重装一下

128、发现一个病毒文件你删了他又自动创建怎么解决

公司的内网某台 linux 服务器流量莫名其妙的剧增,用 iftop 查看有连接外网的情况
针对这种情况一般重点查看 netstat 连接的外网 ip 和端口。
用 lsof -p pid 可以查看到具体是那些进程，哪些文件
经查勘发现/root 下有相关的配置 conf.n hhe 两个可疑文件，rm -rf 后不到一分钟就自动生成了
由此推断是某个母进程产生的这些文件。所以找到母进程就是找到罪魁祸首
查杀病毒最好断掉外网访问，还好是内网服务器，可以通过内网访问
断了内网，病毒就失去外联的能力，杀掉它就容易的多
怎么找到呢，找了半天也没有看到蛛丝马迹，没办法只有 ps axu 一个个排查
方法是查看可以的用户和和系统相似而又不是的冒牌货，果然，看到了如下进程可疑
看不到图片就是/usr/bin/.sshd
于是我杀掉所有.sshd 相关的进程，然后直接删掉.sshd 这个可执行文件
然后才删掉了文章开头提到的自动复活的文件
总结一下，遇到这种问题，如果不是太严重，尽量不要重装系统
一般就是先断外网，然后利用 iftop,ps,netstat,chattr,lsof,pstree 这些工具顺藤摸瓜
一般都能找到元凶。但是如果遇到诸如此类的问题
/boot/efi/EFI/redhat/grub.efi: Heuristics.Broken.Executable FOUND，个人觉得就要重装系统了

129、说说 TCP/IP 的七层模型

应用层 (Application)：
网络服务与最终用户的一个接口。
协议有：HTTP FTP TFTP SMTP SNMP DNS TELNET HTTPS POP3 DHCP
表示层（Presentation Layer）：
数据的表示、安全、压缩。（在五层模型里面已经合并到了应用层）
格式有，JPEG、ASCll、DECOIC、加密格式等
会话层（Session Layer）：
建立、管理、终止会话。（在五层模型里面已经合并到了应用层）
对应主机进程，指本地主机与远程主机正在进行的会话
传输层 (Transport)：
定义传输数据的协议端口号，以及流控和差错校验。
协议有：TCP UDP，数据包一旦离开网卡即进入网络传输层
网络层 (Network)：
进行逻辑地址寻址，实现不同网络之间的路径选择。
协议有：ICMP IGMP IP（IPV4 IPV6） ARP RARP
数据链路层 (Link)：
建立逻辑连接、进行硬件地址寻址、差错校验等功能。（由底层网络定义协议）
将比特组合成字节进而组合成帧，用 MAC 地址访问介质，错误发现但不能纠正
物理层（Physical Layer）：
是计算机网络 OSI 模型中最低的一层
物理层规定:为传输数据所需要的物理链路创建、维持、拆除
而提供具有机械的，电子的，功能的和规范的特性
简单的说，物理层确保原始的数据可在各种物理媒体上传输。局域网与广域网皆属第 1、2 层

物理层是 OSI 的第一层，它虽然处于最底层，却是整个开放系统的基础
物理层为设备之间的数据通信提供传输媒体及互连设备，为数据传输提供可靠的环境
如果您想要用尽量少的词来记住这个第一层，那就是“信号和介质”

130、你常用的 Nginx 模块，用来做什么
rewrite 模块，实现重写功能
access 模块：来源控制
ssl 模块：安全加密
ngx_http_gzip_module：网络传输压缩模块
ngx_http_proxy_module 模块实现代理
ngx_http_upstream_module 模块实现定义后端服务器列表
ngx_cache_purge 实现缓存清除功能

131、请列出你了解的 web 服务器负载架构
Nginx
Haproxy
Keepalived
LVS

132、查看 http 的并发请求数与其 TCP 连接状态
netstat -n | awk ‘/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}’
还有 ulimit -n 查看 linux 系统打开最大的文件描述符，这里默认 1024
不修改这里 web 服务器修改再大也没用，若要用就修改很几个办法，这里说其中一个：
修改/etc/security/limits.conf
soft nofile 10240
hard nofile 10240
重启后生效

133、用 tcpdump 嗅探 80 端口的访问看看谁最高
tcpdump -i eth0 -tnn dst port 80 -c 1000 | awk -F”.” ‘{print $1”.”$2”.”$3”.”$4}’| sort | uniq -c | sort -nr |head -20

134、写一个脚本，实现判断 192.168.1.0/24 网络里，当前在线的 IP 有哪些，能 ping 通则认为在线
```
!/bin/bash
for ip in seq 1 255
do
{
ping -c 1 192.168.1.$ip > /dev/null 2>&1
if [ $? -eq 0 ]; then
echo 192.168.1.$ip UP
else
echo 192.168.1.$ip DOWN
fi
```

}&
done
wait

135、已知 apache 服务的访问日志按天记录在服务器本地目录/app/logs 下，由于磁盘空间紧张现在要求只能保留最近 7 天的访问日志！请问如何解决？ 请给出解决办法或配置或处理命令

创建文件脚本：

!/bin/bash
for n in seq 14
do
date -s “11/0$n/14”
touch access_www_(date +%F).log
done

解决方法：

pwd/application/logs
ll
-rw-r–r–. 1 root root 0 Jan 1 00:00 access_www_2015-01-01.log
-rw-r–r–. 1 root root 0 Jan 2 00:00 access_www_2015-01-02.log
-rw-r–r–. 1 root root 0 Jan 3 00:00 access_www_2015-01-03.log
-rw-r–r–. 1 root root 0 Jan 4 00:00 access_www_2015-01-04.log
-rw-r–r–. 1 root root 0 Jan 5 00:00 access_www_2015-01-05.log
-rw-r–r–. 1 root root 0 Jan 6 00:00 access_www_2015-01-06.log
-rw-r–r–. 1 root root 0 Jan 7 00:00 access_www_2015-01-07.log
-rw-r–r–. 1 root root 0 Jan 8 00:00 access_www_2015-01-08.log
-rw-r–r–. 1 root root 0 Jan 9 00:00 access_www_2015-01-09.log
-rw-r–r–. 1 root root 0 Jan 10 00:00 access_www_2015-01-10.log
-rw-r–r–. 1 root root 0 Jan 11 00:00 access_www_2015-01-11.log
-rw-r–r–. 1 root root 0 Jan 12 00:00 access_www_2015-01-12.log
-rw-r–r–. 1 root root 0 Jan 13 00:00 access_www_2015-01-13.log
-rw-r–r–. 1 root root 0 Jan 14 00:00 access_www_2015-01-14.log
find /application/logs/ -type f -mtime +7 -name “*.log” |xargs rm –f
也可以使用-exec rm -f {} ;进行删除
ll
-rw-r–r–. 1 root root 0 Jan 7 00:00 access_www_2015-01-07.log
-rw-r–r–. 1 root root 0 Jan 8 00:00 access_www_2015-01-08.log
-rw-r–r–. 1 root root 0 Jan 9 00:00 access_www_2015-01-09.log
-rw-r–r–. 1 root root 0 Jan 10 00:00 access_www_2015-01-10.log
-rw-r–r–. 1 root root 0 Jan 11 00:00 access_www_2015-01-11.log
-rw-r–r–. 1 root root 0 Jan 12 00:00 access_www_2015-01-12.log
-rw-r–r–. 1 root root 0 Jan 13 00:00 access_www_2015-01-13.log
-rw-r–r–. 1 root root 0 Jan 14 00:00 access_www_2015-01-14.log

136、如何优化 Linux 系统（可以不说太具体）？

不用 root，添加普通用户，通过 sudo 授权管理
更改默认的远程连接 SSH 服务端口及禁止 root 用户远程连接
定时自动更新服务器时间
配置国内 yum 源
关闭 selinux 及 iptables（iptables 工作场景如果有外网 IP 一定要打开，高并发除外）
调整文件描述符的数量
精简开机启动服务（crond rsyslog network sshd）
内核参数优化（/etc/sysctl.conf）
更改字符集，支持中文，但建议还是用英文字符集，防止乱码
锁定关键系统文件
清空/etc/issue，去除系统及内核版本登录前的屏幕显示

137、请执行命令取出 linux 中 eth0 的 IP 地址(请用 cut，有能力者也可分别用 awk,sed 命令答)

cut 方法 1：
ifconfig eth0|sed -n '2p'|cut -d ":" -f2|cut -d " " -f1
192.168.20.130
awk 方法 2：
ifconfig eth0|awk 'NR==2'|awk -F ":" '{print $2}'|awk '{print $1}'
192.168.20.130
awk 多分隔符方法 3：
ifconfig eth0|awk 'NR==2'|awk -F "[:]+" '{print $4}'
192.168.20.130
sed 方法 4：
ifconfig eth0|sed -n '/inet addr/p'|sed -r 's#^.ddr:(.)Bc.*$##g'
192.168.20.130

138、请写出下面 linux SecureCRT 命令行快捷键命令的功能？

Ctrl + a
Ctrl + c
Ctrl + d
Ctrl + e
Ctrl + l
Ctrl + u
Ctrl + k
tab
Ctrl+shift+c
Ctrl+shift+v
解答：
Ctrl + a —->光标移动到行首
Ctrl + e —->光标移动到行尾
Ctrl + c —->终止当前程序
Ctrl + d —->如果光标前有字符则删除，没有则退出当前中断
Ctrl + l —->清屏

Ctrl + u —->剪切光标以前的字符
Ctrl + k —->剪切光标以后的字符
Ctrl + y —->复制 u/k 的内容
Ctrl + r —->查找最近用过的命令
tab —->命令或路径补全
Ctrl+shift+c —->复制
Ctrl+shift+v —->粘贴

139、每天晚上 12 点，打包站点目录/var/www/html 备份到/data 目录下（最好每次备份按时间生成不同的备份包）

cat a.sh
/bin/bash
cd /var/www/ && /bin/tar zcf /data/html-date +%m-%d%H.tar.gz html/
crontab –e
00 00 * * * /bin/sh /root/a.sh

140、数据库索引可以明显提高哪一操作的效率？

正确答案: A
A SELECT
B INSERT INTO … VALUES …
C UPDATE
D DELETE

141、数据库：以下哪种锁定方式能提供最佳的并行访问性能？

正确答案: D
A 列锁定
B 表锁定
C 块锁定
D 行锁定

142、从 DELETE 语句中省略 WHERE 子句，将产生什么结果？

正确答案: B
A DELETE 语句将失败因为没有记录可删除
B DELETE 语句将从表中删除所有的记录
C DELETE 语句将提示用户进入删除的标准
D DELETE 语句将失败，因为语法错误

143、raceroute 一般使用的是哪种网络层协议？

正确答案: D
A vrrp
B udp
C arp
D icmp

144、ospf 协议中哪种 lsa 只能在本区域内传播？
正确答案: A
A 2
B 3
C 5
D 7

145、在 linux 系统中，下列哪些信号无法捕获？
正确答案: B
A SIGHUP
B SIGKILL
C SIGQUIT
D SIGUSR1

146、Linux 下，如何查看一个端口被什么进程占用？
正确答案: B
A netstat -an|grep 端口号
B netstat -tnlp | grep 端口号
C iostat -an | grep 端口号
D iostat -dxt | grep 端口号

147、列表如何去掉重复元素？
正确答案: B
A 列表无法去重
B 先把 list 转换为一个去重的集合，然后在 list 化
C 先把 list 转换为一个去重的元组，然后在 list 化
D 列表不会有重复

148、Python 的列表(List)和元组(Tuple)区别是什么？
正确答案: A
A 列表可变，元组不可变
B 没有区别
C 限度限制不一样
D 列表可以被迭代，元组无法迭代
149、关于 Python 类的继承正确的说法是？
正确答案: C
A python 类无法继承
B 可以继承但是，无法执行父类的构建函数
C 可以有多个父类
D 只能有一个父类

150、以下关于端口的描述哪些是正确的？
正确答案: A B C D
A FTP 使用 TCP 20 端口

B FTP 使用 TCP 21 端口
C DNS 使用 TCP 53 端口
D DNS 使用 UDP 53 端口

151、下面关于 http 协议中的 GET 和 POST 方式的区别，哪些是错误的？
正确答案: A C
A 他们都可以被收藏，以及缓存
B GET 请求参数放在 URL 中
C GET 只用于查询请求，不能用于请求数据
D GET 不应该处理敏感数据的请求

152、从哪几个方面评价一个 hash 函数的好坏？列举几种常见的 hash 函数？
参考答案：hash 函数好坏的评判标准 1.高效，节省 cpu，才能提高并发，作为中间层，需要高效的根据 key 来计算 hash 2.冲突尽可能的小，小到可以建立唯一索引 3.尽可能的节省空间。例如，要把这个结果存储到数据库中，在给这个 hash 后的结果建立索引，那么我们希望这个列越小越好，以便节省数据存储空间。特别是数据库中建立索引的时候，被索引的字段自然是越小越好 4.要均匀，特别是有多个节点的时候，保证每个 key 分布的均匀，比较重要，否则负载没法均衡 5.rehash 的时候，保证 key 的重新分布尽可能的小，避免给后端带来较大的冲击 常见 hash 函数 比如，md5，sha-1，crc16，crc32 等

153、数据库：以下哪项不是 HASH 索引的特征？
正确答案: C
A MySQL 不能确定在两个值之间大约有多少行
B 不能使用 hash 索引来加速 ORDER BY 操作
C 只用于使用“>”或“<”操作符的比较
D 只能使用整个关键字来搜索一行

154、用户 JANKO 想在有三个列: empid, lastname, 和 salary. 的 employee 表中插入一行，该用户想输入数据 empid 59694, lastname Harris, 但没有 salary. 哪一个语句最适合这项工作？
正确答案: A
A INSERT INTO employee VALUES(59694,’harris’, null)
B INSERT INTO employee VALUES(59694,’harris’)
C INSERT INTO employee (empid, lastname, salary) VALUES(59694,’harris’)
D INSERT INTO employee (SELECT 59694 FROM ‘harris’)

155、数据库：以下哪项是在视图上不能进行的操作？
正确答案: C
A 更新视图
B 查询视图
C 在视图上定义新的表
D 在视图上定义新的视图

156、以下哪项不是 DNS 记录类型？

正确答案: C
A AAAA
B TXT
C TTL
D PTR

157、在 linux 环境下，查看日志文件的最后 100 行数据的正确方式是？
正确答案: D
A mv -100 a.log
B grep -100 a.log
C cat -100 a.log
D tail -100 a.log

158、假设用 4 个同样大小的硬盘来做 RAID，以下哪种 raid 模式获得的可用磁盘空间最少？
正确答案: B
A no-raid
B raid5
C raid1
D raid6

159、关于 linux 文件系统软连接和硬连接的区别，如下哪条是错误的？
正确答案: A
A 硬连接指通过文件复制来进行连接, 类似文件别名。
B 硬连接的作用是允许一个文件拥有多个有效路径名，删除源文件不影响硬连接
C 软连接又被称为符号连接，类似于快捷方程式
D 软连接包含另一文件的位置信息，删除源文件软件连也无法访问了

160、下面关于网络七层和四层的描述，哪条是错误的？
正确答案: A
A SNMP 工作在四层
B 四层是指网络的传输层，主要包括 IP 和端口信息
C 七层是指网络的应用层(协议层)，比如 http 协议就工作在七层
D 四层主要应用于 TCP 和 UDP 的代理，七层主要应用于 HTTP 等协议的代理

161、以下代码输出什么？
list = [‘a’, ‘b’, ‘c’, ‘d’, ‘e’]
print list[10:]
正确答案: A
A [ ]
B 程序异常
C [‘a’, ‘b’, ‘c’, ‘d’, ‘e’]
D 输出空

162、Python 语言什么那些类型的数据才能作为字典的 key？

正确答案: D
A 没有限制
B 字母，数字，下划线
C 字母
D 可被 hash 的的类型

163、以下哪些是常见的 TCP Flags？
正确答案: A B C D
A SYN
B RST
C ACK
D URG

164、Linux 操作系统具备以下哪些特性？
正确答案: A B C
A Multi User
B Multi Tasking
C Multi Process
D None of the above

165、编写 shell 脚本，能够生成 32 位随机密码
一种可能的方法：cat /dev/urandom | head -1 | md5sum | head -c 32

166、假设你是一个小型网站的管理员。周末的时候，你在自己家里发现网站打不开了，请问你能做哪些操作或方法，来确定是什么问题？
参考答案：1. 用自己的电脑访问百度网站，以检查是否自己电脑问题；
2. 联系自己朋友，看看其他人能否打开网站；
3. 使用 ping 命令 ping 网站服务器地址，检查服务器是否正常;
4. 登陆服务器，使用 netstat 命令检查 80 端口是否打开；
5. 登陆服务器，使用 ps 命令检查 http 进程是否存在；
6. 登陆服务器，检查网站日志；

167、当前云计算技术发展迅速，主流云计算平台大多数都以 Linux 为基础。请问以下哪个技术是 Linux 内核提供的可以限制、记录、隔离进程组所使用的物理资源（如：cpu,memory,IO 等等）的机制
正确答案: B
A KVM
B cgroup
C cgroup
D namespace

168、某 IP 地址为 160.55.115.24/20，它的子网划分出来的网络 ID 地址？
正确答案: A
A 160.55.112.0

B 160.55.115.0
C 160.55.112.24
D 其他答案都不对

169、TCP 协议在建立连接的过程中可能处于不同的状态，用 netstat 命令显示出 TCP 连接的状态为 SYN_SEND，则这个连接正处于
正确答案: B
A 监听对方的建立连接请求
B 已主动发出连接建立请求
C 等待对方的连接释放请求
D 收到对方的连接建立请求

170、以下网络协议使用加密传输的是
正确答案: D
A FTP
B TELNET
C DNS
D HTTPS

171、以下 WEB 漏洞类型是在客户端执行的是
正确答案: B
A SQL 注入
B XSS
C 命令注入
D 解析漏洞

172、用户程序发出磁盘 I/O 请求后，系统的正确处理流程是
正确答案: B
A 用户程序→系统调用处理程序→中断处理程序→设备驱动程序
B 用户程序→系统调用处理程序→设备驱动程序→中断处理程序
C 用户程序→设备驱动程序→系统调用处理程序→中断处理程序
D 用户程序→设备驱动程序→中断处理程序→系统调用处理程序

173、下列选项中，满足短任务优先且不会发生饥饿现象的调度算法是
正确答案: B
A 先来先服务
B 高响应比优先
C 时间片轮转
D 非抢占式短任务优先

174、下列选项中，降低进程优先权的合理时机是
正确答案: A
A 进程的时间片用完
B 进程刚完成 I/O，进入就绪队列

C 进程长期处于就绪队列中
D 进程从就绪状态转为运行态

175、一个袋子里装了 100 个苹果，100 个香蕉，100 个桔子，100 个梨，如果每分钟从里面随机抽取一个水果，那么最多过多少分钟时间能肯定至少拿到一打相同种类的水果？（1 打=12 个）
正确答案: D
A 40
B 12
C 24
D 45

176、6 块 300G 的硬盘做 raid5，新的设备容量是多大
正确答案: C
A 900G
B 1800G
C 1500G
D 300G

177、QQ 客户端通过什么协议，将消息发送至服务端？
正确答案: A
A UDP
B TCP
C SMTP
D 以上都不是

178、开发前端 js 时，如何给数组 list 增加元素 element?
正确答案: B
A list.add(element)
B list.push(element)
C list.append(element)
D 以上答案都不对

179、静态变量通常存储在进程的什么位置？
正确答案: C
A 堆
B 栈
C 全局区
D 代码区

180、IP 协议没有使用以下哪一层？
正确答案: D
A 链路层
B 物理层

C 网络层
D 传输层

181、在编译的过程中，语法分析器的任务是？
正确答案: B
A 分析单词的构成逻辑
B 分析单词串构成语言和说明的逻辑
C 分析语句和说明如何构成程序
D 分析程序的结构

182、下列排序算法中，哪个的时间复杂度不超过 nlogn？
正确答案: C
A 快速排序
B 冒泡排序
C 堆排序
D 归并排序

183、在数据库管理中，当我们某一个字段的查询量突然变大，我们应该如何提高查询性能？
正确答案: A
A 基于该字段添加索引
B 基于该字段添加主键
C 为该表创建外键
D 为该表添加索引

184、链表不具备的特点有：
正确答案: A
A 可随机立刻访问任何一个元素
B 插入、删除操作不需要移动元素
C 无需事先估计存储空间大小
D 存储空间大小与链表长度成正比

185、对名为 file 的文件使用 chmod 551 file 命令后，显示的权限为：
正确答案: D
A -rwxr-xr-x
B -rwxr–r–
C -r–r–r-x
D -r-xr-x–x

186、找出 IO 重定向执行结果与其他三个不同的：
正确答案: C
A ./run.sh >run.log 2>&1;
B./run.sh 2>&1 >run.log;
C ./run.sh &>run.log;
D ./run.sh 2>run.log >&2

187、TCP 协议在建立连接的过程中可能处于不同的状态，用 netstat 命令显示出 TCP 连接的状态为 SYN_SEND，则这个连接正处于

正确答案: B

A 监听对方的建立连接请求

B 已主动发出连接建立请求

C 等待对方的连接释放请求

D 收到对方的连接建立请求

188、6 块 300G 的硬盘做 raid5，新的设备容量是多大

正确答案: C

A 900G

B 1800G

C 1500G

D 300G

189、crontab 中每个域的含义？

正确答案: D

A 秒 分 周 日 月 命令

B 秒 分 时 日 周 命令

C 分 时 周 月 日 命令

D 分 时 日 月 周 命令

190、指令：ls | grep “[ad]*\.conf” 命令解释正确的是：

正确答案: A

A 显示包含 a 或者 d 为开头，后接任何字符，再后面是.conf 字符的文件（或目录）

B 显示包含 a 或者 d 出现 0 次或无数次，后面是.conf 字符的文件（或目录）

C 显示包含字母 a 或者 d 出现 0 次或 1 次，后面是.conf 字符的文件（或目录）

D 显示从字母 a 到 d ，后接任何字符，再后面是.conf 字符的文件（或目录）

191、以下密码学算法需要使用秘钥的是

正确答案: D

A SHA256

B SHA1

C MD5

D HMAC

192、以下不属于漏洞扫描工具的是

正确答案: C

A NMAP

B AWVS

C nc

D Nessus

193、以下不是用来进行认证的协议的是

正确答案: D

A Kerberos

B Outh2

C RADIUS

D SNMP

194、如下哪些 linux 命令可以查看文件内容（多选题）：

正确答案: A B C D

A less

B cat

C more

D vim

195、如下 sql 语句，会执行错误的是？

正确答案: A D

A UPDATE db1.table1 column1=”valu1”

B SELECT distinct(*) FROM table1 GROUP BY column1

C SET NAMES ‘utf8’

D DROP DATABASE table1

196、在前后端交互过程中，Cookie 是一个很重要、敏感的存储介质。如何防止 Cookie 内容被黑客篡改？

正确答案: A C D

A 服务端对 Cookie 内容加密

B 浏览器对 Cookie 内容加密

C 设置 HttpOnly

D 对 Cookie 设置有效时间

197、提供一个二叉树的子树查找函数，完成如下的功能：

输入参数：root， node

输出：1.node 所在的深度（0 表示不存在，最小深度为 1）；2.node 对应的路径（从 root 开始，左为 L,右为 R，按逗号分隔）；

说明：1.node 所在位置相同，左右子树和 name 都必须相同；

请用熟悉的语言，用两种方式（递归和栈）完成此函数

198、找出数组（至少包含一个数字）中的一个连续子数组、该子数组拥有最大和。

例如：给定一个数组[－2,1,－3,4,－1,2,1,－5,4],连续子数组［4,－1,2,1］的和是 6，比其它子数组的和都大。

```
int maxSubArray(int *nums, int arrLen){
}
```

199、给出一个非空的整数数组，返回其中前 k 个出现最频繁的元素。

比如 [1,1,1,2,2,3]，k = 2，输出[1,2]。

如果 n 是数组的大小，要求给出时间复杂度小于 O(n log n)的算法。

200、给出一个从小到大排好序的整数数组 nums 和一个整数 n，在数组中添加若干个补丁（元素）使得[1,n]的区间内的所有数都可以表示成 nums 中若干个数的和。返回最少需要添加的补丁个数。

样例 1：nums = [1, 3], n = 6

返回 1，表示至少需要添加 1 个数｛2｝，才可以表示 1 到 6 之间所有数。

样例 2：nums = [1, 5, 10], n = 20

返回 2，表示至少需要添加两个数｛2，4｝，才可以表示 1 到 20 之间所有数。

201、在 shell 中变量的赋值有四种方法，其中，采用 name=12 的方法称 A 。

A 直接赋值

B 使用 read 命令

C 使用命令行参数

D 使用命令的输出

202、D 命令可以从文本文件的每一行中截取指定内容的数据。

A cp

B dd

C fmt

D cut

203、在 Shell 脚本中，用来读取文件内各个域的内容并将其赋值给 Shell 变量的命令是 D 。

A fold

B join

C tr

D read

204、退出交互模式的 shell，应键入 C 。

A ;

B ^q

C exit

D quit

205、下列变量名中有效的 shell 变量名是： C 。

A -2-time

B _2$3

C trust_no_1

D 2004file

206 是 shell 具有的功能和特点的是 C 。

A 管道　　B 输入输出重定向

C 执行后台进程　　D 处理程序命令

207、下列对 shell 变量 FRUIT 操作，正确的是： C 。

A 为变量赋值：$FRUIT=apple
B 显示变量的值：fruit=apple
C 显示变量的值：echo $FRUIT
D 判断变量是否有值：[-f —$FRUIT]

208、下面的网络协议中，面向连接的的协议是： A 。
A 传输控制协议
B 用户数据报协议
C 网际协议
D 网际控制报文协议

209、一台主机要实现通过局域网与另一个局域网通信，需要做的工作是 C 。
A 配置域名服务器
B 定义一条本机指向所在网络的路由
C 定义一条本机指向所在网络网关的路由
D 定义一条本机指向目标网络网关的路由

210、在/etc/fstab 文件中指定的文件系统加载参数中，D 参数一般用于 CD-ROM 等移动设备。
A defaults
B sw
C rw 和 ro
D noauto
#noauto 只在命令下挂载

211、Linux 文件权限一共 10 位长度，分成四段，第三段表示的内容是 C 。
A 文件类型
B 文件所有者的权限
C 文件所有者所在组的权限
D 其他用户的权限

212、终止一个前台进程可能用到的命令和操作 B 。
A kill
B ;+C
C shut down
D halt

213、在使用 mkdir 命令创建新的目录时，在其父目录不存在时先创建父目录的选项是 D 。
A -m
B -d
C -f
D –p

214、下面关于 i 节点描述错误的是 A 。（inode 是一种数据结构，vfs 中描述文件的相关参

数？？）

A i 节点和文件是一一对应的

B i 节点能描述文件占用的块数

C i 节点描述了文件大小和指向数据块的指针

D 通过 i 节点实现文件的逻辑结构和物理结构的转换

215、具有很多 C 语言的功能，又称过滤器的是 C 。

A csh

B tcsh

C awk （awk 详解 ）

D sed

216、建立动态路由需要用到的文件有 D 。

A /etc/hosts

B /etc/HOSTNAME

C /etc/resolv.conf

D /etc/gateways

217、局域网的网络地址 192.168.1.0/24，局域网络连接其它网络的网关地址是 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 B 。

A route add –net 192.168.1.0 gw 192.168.1.1 netmask 255.255.255.0 metric1

B route add –net 172.16.1.0 gw 192.168.1.1 netmask 255.255.255.255 metric1

C route add –net 172.16.1.0 gw 172.16.1.1 netmask 255.255.255.0 metric 1

D route add default 192.168.1.0 netmask 172.168.1.1 metric 1

218、下列提法中，不属于 ifconfig 命令作用范围的是 D 。

A 配置本地回环地址

B 配置网卡的 IP 地址

C 激活网络适配器

D 加载网卡到内核中

219、下列关于链接描述，错误的是 B 。

A 硬链接就是让链接文件的 i 节点号指向被链接文件的 i 节点

B 硬链接和符号连接都是产生一个新的 i 节点

C 链接分为硬链接和符号链接

D 硬连接不能链接目录文件

220、在局域网络内的某台主机用 ping 命令测试网络连接时发现网络内部的主机都可以连同，而不能与公网连通，问题可能是 C。

A 主机 IP 设置有误

B 没有设置连接局域网的网关

C 局域网的网关或主机的网关设置有误

D 局域网 DNS 服务器设置有误

221、下列文件中，包含了主机名到 IP 地址的映射关系的文件是： B 。

A /etc/HOSTNAME

B /etc/hosts

C /etc/resolv.conf

D /etc/networks

222、不需要编译内核的情况是 D 。

A 删除系统不用的设备驱动程序时

B 升级内核时

C 添加新硬件时

D 将网卡激活

223、下列不是 Linux 系统进程类型的是 D 。

A 交互进程

B 批处理进程

C 守护进程

D 就绪进程（进程状态）

224、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

225、内核不包括的子系统是 D 。

A 进程管理系统

B 内存管理系统

C I/O 管理系统

D 硬件管理系统

226、在日常管理中，通常 CPU 会影响系统性能的情况是： A 。

A CPU 已满负荷地运转

B CPU 的运行效率为 30%

C CPU 的运行效率为 50%

D CPU 的运行效率为 80%

227、若一台计算机的内存为 128GB，则交换分区的大小通常是 A。

A 4GB

B 16GB

C 64GB

D 256GB

228、Linux 查看文件的命令，若希望在查看文件内容过程中可以用光标上下移动来查看文件内容，应使用 C 命令。

A cat
B more
C less
D head

229、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， B 是能够实现本地与远程主机之间的文件传输工作。
A telnet
B FTP
C SNMP
D NFS

230、当我们与某远程网络连接不上时，就需要跟踪路由查看，以便了解在网络的什么位置出现了问题，满足该目的的命令是 C 。
A ping
B ifconfig
C traceroute
D netstat

231、对名为 fido 的文件用 chmod 551 fido 进行了修改，则它的许可权是 D 。
A -rwxr-xr-x
B -rwxr–r–
C -r–r–r–
D -r-xr-x—x

232、用 ls –al 命令列出下面的文件列表， D 文件是符号连接文件。
A -rw-rw-rw- 2 hel-s users 56 Sep 09 11:05 hello
B -rwxrwxrwx 2 hel-s users 56 Sep 09 11:05 goodbey
C drwxr–r– 1 hel users 1024 Sep 10 08:10 zhang
Dl rwxr–r– 1 hel users 2024 Sep 12 08:12 cheng

233、DNS 域名系统主要负责主机名和 A 之间的解析。
A I P 地址
B MAC 地址
C 网络地址
D 主机别名

234、WWW 服务器是在 Internet 上使用最为广泛，它采用的是 B 结构。
A 服务器/工作站
B B/S
C 集中式
D 分布式

235、Linux 系统通过 C 命令给其他用户发消息。

A less
B mesg y
C write
D echo to
[注：mesg [y|n] 所有使用者 决定是否允许其他人传讯息到自己的终端机介面]

236、NFS 是 C 系统。
A 文件
B 磁盘
C 网络文件
D 操作

237、B 命令可以在 Linux 的安全系统中完成文件向磁带备份的工作。
A cp
B tr
C dir
D cpio
[注：如果用 echo $PATH 或者 echo $LD_LIBRARY_PATH 等类似的命令来显示路径信息的话，我们看到的将会是一大堆用冒号连接在一起的路径， tr 命令可以把这些冒号转换为回车，这样，这些路径就具有很好的可读性了：echo $PATH | tr ":" "\n"]

238、Linux 文件系统的文件都按其作用分门别类地放在相关的目录中，对于外部设备文件，一般应将其放在 C 目录中。
A /bin
B /etc
C /dev
D /lib

239、在重新启动 Linux 系统的同时把内存中的信息写入硬盘，应使用 D 命令实现。
A # reboot
B # halt
C # reboot
D # shutdown –r now

240、网络管理具备以下几大功能：配置管理、 A 、性能管理、安全管理和计费管理等。
A 故障 管理
B 日常备份管理
C 升级管理
D 发送邮件

241、关于代理服务器的论述，正确的是 A 。
A 使用 internet 上已有的公开代理服务器，只需配置客户端。
B 代理服务器只能代理客户端 http 的请求。
C 设置好的代理服务器可以被网络上任何主机使用。

D 使用代理服务器的客户端没有自己的 ip 地址。

242、关闭 linux 系统（不重新启动）可使用命令 B 。

A Ctrl+Alt+Del

B halt

C shutdown -r now

D reboot

243、实现从 IP 地址到以太网 MAC 地址转换的命令为： C 。

A ping

B ifconfig

C arp

D traceroute

244、在 vi 编辑器中的命令模式下，键入 B 可在光标当前所在行下添加一新行。

A ;

B ;

C ;

D A

245、在 vi 编辑器中的命令模式下，删除当前光标处的字符使用 A 命令。

A ;

B ;;

C ;

D ;;

246、在 vi 编辑器中的命令模式下，重复上一次对编辑的文本进行的操作，可使用 C 命令。

A 上箭头

B 下箭头

C ;

D <*>;

247、用命令 ls -al 显示出文件 ff 的描述如下所示，由此可知文件 ff 的类型为 A 。-rwxr-xr–1 root root 599 Cec 10 17:12 ff

A 普通文件

B 硬链接

C 目录

D 符号链接

248、删除文件命令为： D

A mkdir

B rmdir

C mv

D rm

249、在下列的名称中，不属于 DNS 服务器类型的是：C

A Primary Master Server

B Secondary Master Server

C samba

D Cache_only Server

250、 邮件转发代理也称邮件转发服务器，它可以使用 SMTP 协议，也可以使用 C 协议。

A FTP

B TCP

C UUCP

D POP

251、启动 samba 服务器进程，可以有两种方式：独立启动方式和父进程启动方式，其中前者是在 C 文件中以独立进程方式启动。

A /usr/sbin/smbd

B /usr/sbin/nmbd

Crc.samba

D /etc/inetd.conf

252、DHCP 是动态主机配置协议的简称，其作用是可以使网络管理员通过一台服务器来管理一个网络系统，自动地为一个网络中的主机分配 D 地址。

A 网络

B MAC

C TCP

D IP

253、对文件进行归档的命令为 D 。

A dd

B cpio

C gzip

D tar

254、改变文件所有者的命令为 C 。

A chmod

B touch

C chown

D cat

255、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

256、建立一个新文件可以使用的命令为 D 。

A chmod

B more

C cp

D touch (指令改变档案的时间记录。)

257、下列命令中，不能显示文本文件内容的命令是： D 。

A more

B less

C tail

D join

258、在使用匿名登录 ftp 时，用户名为 B 。

A users

B anonymous

C root

D guest

259、在实际操作中，想了解命令 logname 的用法，可以键入 D 得到帮助。

A logname –man

B logname/?

C help logname

D logname –help

260、文件权限读、写、执行的三种标志符号依次是 A 。

A rwx

B xrw

C rdx

D srw

261、Linux 文件名的长度不得超过 C 个字符。

A 64

B 128

C 256

D 512

262、从后台启动进程，应在命令的结尾加上符号 A 。

A &

B @

C #

D $

263、crontab 文件由六个域组成 ，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
crontab 命令：实现程序定时运行

264、用 ftp 进行文件传输时，有两种模式： C 。
A Word 和 binary
B .txt 和 Word Document
C ASCII 和 binary
D ASCII 和 Rich Text Format

265、某文件的组外成员的权限为只读；所有者有全部权限；组内的权限为读与写，则该文件的权限为 D 。
A 467
B 674
C 476
D 764

266、在 DNS 系统测试时，设 named 进程号是 53，命令 D 通知进程重读配置文件。
A kill –USR2 53
B kill –USR1 53
C kill -INT 63
D kill –HUP 53

267、Apache 服务器默认的接听连接端口号是 C 。
A 1024
B 800
C 80 (http)
D 8

268、PHP 和 MySQL 的联合使用 解决 了 C 。
A 在 Proxy 上处理数据库的访问问题
B 在 WWW 服务器上处理黑客的非法访问问题
C 在 WWW 服务器上处理数据库的访问问题
D 在 Sendmail 邮件系统上处理数据库的访问问题

269、OpenSSL 是一个 A 。
A 加密软件
B 邮件系统
C 数据库管理系统
D 嵌入式脚本编程语言

270、将 Windows C:盘(hda1)安装在 Linux 文件系统的/winsys 目录下，命令是 B 。

Aroot@l04.edu.cn:~#mount dev/had1 /winsys
Broot@l04.edu.cn:~#mount /dev/had1 /winsys
Croot@l04.edu.cn:~#mount /dev/had1 winsys
Droot@l04.edu.cn:~#mount dev/had1 winsys

271、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

272、字符设备文件类型的标志是 B 。
A p
B c
C s
D l

273、在/home/stud1/wang 目录下有一文件 file，使用 D 可实现在后台执行命令，此命令将 file 文件中的内容输出到 file.copy 文件中。
A cat file >;file.copy
B cat >;file.copy
C cat file file.copy &
D cat file >;file.copy &

274、在 DNS 配置文件中，用于表示某主机别名的是： B 。
A NS
B CNAME
C NAME
D CN

275、qmail 是 B 。
A 收取邮件的协议
B 邮件服务器的一种
C 发送邮件的协议
D 邮件队列

276、已知某用户 stud1，其用户目录为/home/stud1。分页显示当前目录下的所有文件的文件或目录名、用户组、用户、文件大小、文件或目录权限、文件创建时间等信息的命令是 D 。
A more ls –al
B more –al ls
C more < ls –al
D ls –al | more

277、关于进程调度命令， B 是不正确的。at–定期执行程序的调度命令

A 当日晚 11 点执行 clear 命令，使用 at 命令：at 23:00 today clear

B 每年 1 月 1 日早上 6 点执行 date 命令，使用 at 命令：at 6am Jan 1 date

C 每日晚 11 点执行 date 命令，crontab 文件中应为：0 23 * * * date

D 每小时执行一次 clear 命令，crontab 文件中应为：0 */1 * * * clear

278、系统中有用户 user1 和 user2，同属于 users 组。在 user1 用户目录下有一文件 file1，它拥有 644 的权限，如果 user2 用户想修改 user1 用户目录下的 file1 文件，应拥有 B 权限。

A 744

B 664

C 646

D 746

279、如果想配置一台匿名 ftp 服务器，应修改 C 文件。

A /etc/gateway

B /etc/ftpservers

C /etc/ftpusers

D /etc/inetd.conf

280、Samba 服务器的进程由 B 两部分组成 。

A named 和 sendmail

Bsmbd 和 nmbd

C bootp 和 dhcpd

D httpd 和 squid

281、要配置 NFS 服务器，在服务器端主要配置 C 文件。

A /etc/rc.d/rc.inet1

B /etc/rc.d/rc.M

C /etc/exports

D /etc/rc.d/rc.S

282、为保证在启动服务器时自动启动 DHCP 进程，应对 B 文件进行编辑。

A /etc/rc.d/rc.inet2

B /etc/rc.d/rc.inet1

C /etc/dhcpd.conf

D /etc/rc.d/rc.S

283、在配置代理服务器时，若设置代理服务器的工作缓存为 64MB，配置行应为 D 。

A cache 64MB

B cache_dir ufs /usr/local/squid/cache 10000 16 256

C cache_ mgr 64MB

Dcache_ mem 64MB

284、安全管理涉及的问题包括保证网络管理工作可靠进行的安全问题和保护网络用户及网络管理对象问题。 C 属于安全管理的内容。

A 配置设备的工作参数

B 收集与网络性能有关的数据

C 控制和维护访问权限

D 监测故障

285、以下命令对中，正确的是： B 。

A ls 和 sl

B cat 和 tac

C more 和 erom

D exit 和 tixe

cat 是显示文件夹的命令，这个大家都知道，tac 是 cat 的倒写，意思也和它是相反的。cat 是从第一行显示到最后一行，而 tac 是从最后一行显示到第一行，而 rev 则是从最后一个字符显示到第一个字符

286、B 命令是在 vi 编辑器中执行存盘退出。

A :q

B ZZ

C :q!

D :WQ

287、B 不是进程和程序的区别。

A 程序是一组有序的静态指令，进程是一次程序的执行过程

B 程序只能在前台运行，而进程可以在前台或后台运行

C 程序可以长期保存，进程是暂时的

D 程序没有状态，而进程是有状态的

288、在 php + mysql + apache 架构的 web 服务中输入 GET 参数 index.php?a=1&a=2&a=3 服务器端脚本 index.php 中$GET[a] 的值是？

正确答案: C

A 1

B 2

C 3

D 1,2,3

289、以下哪些不是 CSRF 漏洞的防御方案？

正确答案: D

A 检测 HTTPreferer

B 使用随机 token

C 使用验证码

D html 编码

290、以下程序存在何种安全漏洞？

```
<tr>
  <td class="font_content" align="right">交易状态：</td>
  <td class="font_content" align="left"><?php echo $_GET['trade_status'];?></td>
</tr>
```

正确答案: A

A XSS

B sql 注入

C 命令执行

D 代码执行

291、下列哪些工具可以作为离线破解密码使用？

正确答案: D

A hydra

B Medusa

C Hscan

D OclHashcat

292、下列命令中不能用于 Android 应用程序反调试的是？

正确答案: C

A ps

B cat/proc/self/status

C cat/proc/self/cmdline

D cat/proc/self/stat

293、用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？

正确答案: B

A 缓存溢出攻击

B 钓鱼攻击

C 暗门攻击

D DDOS 攻击

294、下列关于各类恶意代码说法错误的是？

正确答案: C

A 蠕虫的特点是其可以利用网络进行自行传播和复制

B 木马可以对远程主机实施控制

C Rootkit 即是可以取得 Root 权限的一类恶意工具的统称

D pcshare 一种远程控制木马

295、关于 XcodeGhost 事件的正确说法是？

正确答案: B

A 部分 Android 产品 也受到了影响

B 应用程序开发使用了包含后门插件的 IDE
C 当手机被盗时才有风险
D 苹果官方回应 APPSTORE 上的应用程序不受影响

296、下列关于各类恶意代码说法错误的是？
正确答案: C
A 蠕虫的特点是其可以利用网络进行自行传播和复制
B 木马可以对远程主机实施控制
C Rootkit 即是可以取得 Root 权限的一类恶意工具的统称
D 通常类型的病毒都只能破坏主机上的各类软件，而无法破坏计算机硬件

297、Unix 系统日志文件通常是存放在？
正确答案: A
A /var/log
B /usr/adm
C /etc/
D /var/run

298、防止系统对 ping 请求做出回应，正确的命令是？
正确答案: C
A echo 0>/proc/sys/net/ipv4/icmp_ehco_ignore_all
B echo 0>/proc/sys/net/ipv4/tcp_syncookies
C echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all
D echo 1>/proc/sys/net/ipv4/tcp_syncookies

299、文件名为 webshell.php.phpp1.php02 的文件可能会被那个服务器当做 php 文件进行解析？
正确答案: A
A Apache
B IIS
C nginx
D squid

300、cookie 安全机制，cookie 有哪些设置可以提高安全性？（多选题）
正确答案: A B C
A 指定 cookie domain 的子域名
B httponly 设置
C cookie secure 设置，保证 cookie 在 https 层面传输
D 以上都不对

301、下列哪些方式对解决 xss 漏洞有帮助？
正确答案: B C
A csp
B html 编码

C url 编码
D 验证码

302、可以抓取 Windows 登录密码的安全工具有？
正确答案: A C
A mimikatz
B sqlmap
C pwdump7
D hashcat

303、关于对称加密以下说法不正确的是？
正确答案: B D
A DES 属于对称加密
B 对称加密算法需要两个密钥来进行加密和解密
C 对称加密也叫单密钥加密
D RSA 属于对称加密

304、以下哪些命令可以查看 windows 安全日志？
正确答案: A B
A wevtutil
B eventquery.vbs
C systeminfo
D dsquery

305、以下 PHP 代码经过 mysql_real_escape_string 过滤还存在漏洞？为什么？
$id = $_GET[‘id’];
$id = mysql_real_escape_string($id);
$getid = “SELECT first_name, last_name FROM users WHERE user_id = $id”;
$result = mysql_query($getid) or die(‘
' . mysql_error() . '
‘);
$num = mysql_numrows($result);
参考答案：
这里$id 变量没有经过任何的过滤，直接传入了 sql 语句，造成数字型注入，mysql_real_escape_string 只对’ “ \ null 字符做转义，而数字型注入不需要’闭合，所以仍存在注入漏洞。

306、以下哪种上传处理方式相对安全？
正确答案: C
A 检查 Content-Type,非 image 格式一律禁止上传
B 黑名单检测方式
C 白名单检测方式
D javascript 判断是否允许上传

307、正则表达式语法中 \D 匹配的是？

正确答案: B

A 数字

B 非数字

C 字母

D 空白字符

308、以下哪种方式可以开启 socket 端口？

正确答案: C

A ssh -L lport:DHost:Dport root@ip

B ssh -R lport:DHost:Dport root@ip

C ssh -D lport root@ip

309、sql server2005 注入点那种权限可以使用 xp_cmdshell 执行命令？

正确答案: C

A public 权限

B db_owner 权限

C SA 权限

D 其他都正确

310、如下 Activity 代码：

```
Intent i = getIntent();
 try{
     String action = i.getAction();
     if(action.equalsIgnoreCase("mSec")){
         String s = (String) i.getSerializableExtra("serializable_key");
         ArrayListintArray = intent.getIntegerArrayListExtra("user_id");
         if (intArray != null) {
             for (int j = 0; j < 2; j++) {
                 intArray.get(j);
             }
         }
     }else{
     }
  }catch(ClassCastException e){
}
```

并定义如下变量：

ArrayListuser_id = new ArrayList(); user_id.add(1); user_id.add(2);

ArrayListuser_id1 = new ArrayList();

BigInteger bi = BigInteger.valueOf(1);

下面哪个 Intent 传入会造成应用崩溃：

正确答案: A

A

Intent i = new Intent();

i.setAction(“mSec”);
i.putExtra(“serializable_key”, bi);
i.putExtra(“user_id”, user_id1);
B
Intent i = new Intent();
i.setAction(“Msec”);
i.putExtra(“serializable_key”, bi);
i.putExtra(“user_id”, user_id);
C
Intent i = new Intent();
i.setAction(“Msec”);
i.putExtra(“serializable_key”, “str”);
i.putExtra(“user_id”, user_id);

311、默认端口 11211 上开放的服务是？
正确答案: D
A Docker
B pop3
C mongodb
D memcached

312、关于 XcodeGhost 事件的正确说法是？
正确答案: B
A 部分 Android 产品 也受到了影响
B 应用程序开发使用了包含后门插件的 IDE
C 当手机被盗时才有风险
D 苹果官方回应 APPSTORE 上的应用程序不受影响

313、下列关于各类恶意代码说法错误的是？
正确答案: C
A 蠕虫的特点是其可以利用网络进行自行传播和复制
B 木马可以对远程主机实施控制
C Rootkit 即是可以取得 Root 权限的一类恶意工具的统称
D 通常类型的病毒都只能破坏主机上的各类软件，而无法破坏计算机硬件

314、unix 系统日志文件通常是存放在？
正确答案: A
A /var/log
B /usr/adm
C /etc/
D /var/run

315、以下哪种 sql 注入支持多语句执行？
正确答案: A

A sql server
B oracle
C mysql
D db2

316、sql 注入（mysql 数据库）中常用的延时函数是？
正确答案: A C
A sleep()
B pthread_join
C benchmark
D postpone

317、以下哪些工具可以抓取 HTTP 数据包？
正确答案: A C
A Burpsuite
B hackbar
C Fiddler
D Nmap

318、应急响应中常用查看信息的命令有哪些？
正确答案: A B C D
A ps -aux
B last
C w
D more .bash_history

319、恶意攻击行为中，属于被动攻击的有？
正确答案: A B
A 窃听
B 流量分析
C SQL 注入攻击
D 暴力破解

320、下面的网络协议中，面向连接的的协议是： A 。
A 传输控制协议 B 用户数据报协议
C 网际协议 D 网际控制报文协议

321、在/etc/fstab 文件中指定的文件系统加载参数中， D 参数一般用于 CD-ROM 等移动设备。
A defaults B sw C rw 和 ro D noauto

323.、Linux 文件权限一共 10 位长度，分成四段，第三段表示的内容是 C 。
A 文件类型 B 文件所有者的权限
C 文件所有者所在组的权限 D 其他用户的权限

324、终止一个前台进程可能用到的命令和操作 B 。

A kill B <CTRL>;+C C shut down D halt

325、在使用 mkdir 命令创建新的目录时，在其父目录不存在时先创建父目录的选项是 D 。

A -m B -d C -f D -p

326、下面关于 i 节点描述错误的是 A 。（inode 是一种数据结构，vfs 中描述文件的相关参数？？）

A i 节点和文件是一一对应的

B i 节点能描述文件占用的块数

C i 节点描述了文件大小和指向数据块的指针

D 通过 i 节点实现文件的逻辑结构和物理结构的转换

327、一个文件名字为 rr.Z，可以用来解压缩的命令是： D 。

A tar B gzip C compress D uncompress

328、具有很多 C 语言的功能，又称过滤器的是 C 。

A csh

B tcsh

C awk （awk 详解）

D sed

329、 一台主机要实现通过局域网与另一个局域网通信，需要做的工作是 C 。

A 配置域名服务器

B 定义一条本机指向所在网络的路由

C 定义一条本机指向所在网络网关的路由

D 定义一条本机指向目标网络网关的路由

330、动态路由需要用到的文件有 D 。

A /etc/hosts B /etc/HOSTNAME C /etc/resolv.conf D /etc/gateways

331、局域网的网络地址 192.168.1.0/24，局域网络连接其它网络的网关地址是 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 B 。

A route add –net 192.168.1.0 gw 192.168.1.1 netmask 255.255.255.0 metric 1

B route add –net 172.16.1.0 gw 192.168.1.1 netmask 255.255.255.255 metric 1

C route add –net 172.16.1.0 gw 172.16.1.1 netmask 255.255.255.0 metric 1

D route add default 192.168.1.0 netmask 172.168.1.1 metric 1

332、下列提法中，不属于 ifconfig 命令作用范围的是 D 。

A 配置本地回环地址 B 配置网卡的 IP 地址

C 激活网络适配器 D 加载网卡到内核中

333、下列关于链接描述，错误的是 B 。

A 硬链接就是让链接文件的 i 节点号指向被链接文件的 i 节点
B 硬链接和符号连接都是产生一个新的 i 节点
C 链接分为硬链接和符号链接 D 硬连接不能链接目录文件

334、在局域网络内的某台主机用 ping 命令测试网络连接时发现网络内部的主机都可以连同，而不能与公网连通，问题可能是 C。
A 主机 IP 设置有误
B 没有设置连接局域网的网关
C 局域网的网关或主机的网关设置有误
D 局域网 DNS 服务器设置有误

335、下列文件中，包含了主机名到 IP 地址的映射关系的文件是： B 。
A /etc/HOSTNAME B /etc/hosts C /etc/resolv.conf D /etc/networks

336、不需要编译内核的情况是 D 。
A 删除系统不用的设备驱动程序时 B 升级内核时
C 添加新硬件时 D 将网卡激活

337、在 shell 中变量的赋值有四种方法，其中，采用 name=12 的方法称 A 。
A 直接赋值 B 使用 read 命令
C 使用命令行参数 D 使用命令的输出

338、D 命令可以从文本文件的每一行中截取指定内容的数据。
A cp B dd C fmt D cut

339、下列不是 Linux 系统进程类型的是 D 。
A 交互进程 B 批处理进程 C 守护进程 D 就绪进程（进程状态）

340、配置 Apache 1.3.19 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

341、内核不包括的子系统是 D 。
A 进程管理系统 B 内存管理系统 C I/O 管理系统 D 硬件管理系统

342、在日常管理中，通常 CPU 会影响系统性能的情况是： A 。
A CPU 已满负荷地运转 B CPU 的运行效率为 30%
C CPU 的运行效率为 50% D CPU 的运行效率为 80%

343、若一台计算机的内存为 128MB，则交换分区的大小通常是 C 。
A 64MB B 128MB C 256MB D 512MB

344、在安装 Linux 的过程中的第五步是让用户选择安装方式，如果用户希望安装部分组件（软件程序），并在选择好后让系统自动安装，应该选择的选项是 D 。
A full B expert C newbie D menu

345、Linux 有三个查看文件的命令，若希望在查看文件内容过程中可以用光标上下移动来查看文件内容，应使用 C 命令。

A cat B more C less D menu

346、下列信息是某系统用 ps –ef 命令列出的正在运行的进程， D 进程是运行 Internet 超级服务器，它负责监听 Internet sockets 上的连接，并调用合适的服务器来处理接收的信息。

A root 1 4.0 0.0 344 204? S 17:09 0:00 init

B root 2 0.0 0.1 2916 1520? S 17:09 0:00 /sbin/getty

C root 3 0.0 0.2 1364 632? S 17:09 0:00 /usr/sbin/syslogd

D root 4 0.0 1344 1204? S 17:09 0:10 /usr/sbin/inetd

347、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， B 是能够实现本地与远程主机之间的文件传输工作。

A telnet B FTP C SNMP D NFS

348、当我们与某远程网络连接不上时，就需要跟踪路由查看，以便了解在网络的什么位置出现了问题，满足该目的的命令是 C 。

A ping B ifconfig C traceroute D netstat

349、对名为 fido 的文件用 chmod 551 fido 进行了修改，则它的许可权是 D 。

A -rwxr-xr-x B -rwxr–r– C -r–r–r– D -r-xr-x—x

350、在 i 节点表中的磁盘地址表中，若一个文件的长度是从磁盘地址表的第 1 块到第 11 块，则该文件共占有 B 块号。

A 256 B 266 C 11 D 256×10

351、用 ls –al 命令列出下面的文件列表， D 文件是符号连接文件。

A -rw-rw-rw- 2 hel-s users 56 Sep 09 11:05 hello

B -rwxrwxrwx 2 hel-s users 56 Sep 09 11:05 goodbey

C drwxr–r– 1 hel users 1024 Sep 10 08:10 zhang

D lrwxr–r– 1 hel users 2024 Sep 12 08:12 cheng

352、DNS 域名系统主要负责主机名和 A 之间的解析。

A IP 地址 B MAC 地址 C 网络地址 D 主机别名

353、WWW 服务器是在 Internet 上使用最为广泛，它采用的是 B 结构。

A 服务器/工作站 B B/S C 集中式 D 分布式

354、Linux 系统通过 C 命令给其他用户发消息。

A less B mesg y C write D echo to

[注：mesg [y|n] 所有使用者 决定是否允许其他人传讯息到自己的终端机介面]

355、NFS 是 C 系统。

A 文件 B 磁盘 C 网络文件 D 操作

356、B 命令可以在 Linux 的安全系统中完成文件向磁带备份的工作。

A cp B tr C dir D cpio

[注：如果用 echo $PATH 或者 echo $LD_LIBRARY_PATH 等类似的命令来显示路径信息的话，我们看到的将会是一大堆用冒号连接在一起的路径， tr 命令可以把这些冒号转换为回车，这样，这些路径就具有很好的可读性了：

echo $PATH | tr ":" "\n"]

357、Linux 文件系统的文件都按其作用分门别类地放在相关的目录中，对于外部设备文件，一般应将其放在 C 目录中。

A /bin B /etc C /dev D /lib

358、在重新启动 Linux 系统的同时把内存中的信息写入硬盘，应使用 D 命令实现。

A # reboot B # halt C # reboot D # shutdown –r now

359、网络管理具备以下几大功能：配置管理、 A 、性能管理、安全管理和计费管理等。

A 故障管理 B 日常备份管理 C 升级管理 D 发送邮件

360、关于代理服务器的论述，正确的是 A 。

A 使用 internet 上已有的公开代理服务器，只需配置客户端。

B 代理服务器只能代理客户端 http 的请求。

C 设置好的代理服务器可以被网络上任何主机使用。

D 使用代理服务器的客户端没有自己的 ip 地址。

361、关闭 linux 系统（不重新启动）可使用命令 B 。

A Ctrl+Alt+Del B halt C shutdown -r now D reboot

262、实现从 IP 地址到以太网 MAC 地址转换的命令为： C 。

A ping B ifconfig C arp D traceroute

363、在 vi 编辑器中的命令模式下，键入 B 可在光标当前所在行下添加一新行。

A <a>; B <o>; C <I>; D A

364、在 vi 编辑器中的命令模式下，删除当前光标处的字符使用 A 命令。

A <x>; B <d>;<w>; C <D>; D <d>;<d>;

365、在 vi 编辑器中的命令模式下，重复上一次对编辑的文本进行的操作，可使用 C 命令。

A 上箭头 B 下箭头 C <.>; D <*>;

366、用命令 ls -al 显示出文件 ff 的描述如下所示，由此可知文件 ff 的类型为 A 。

-rwxr-xr– 1 root root 599 Cec 10 17:12 ff

A 普通文件 B 硬链接 C 目录 D 符号链接

367、删除文件命令为： D 。

A mkdir
B rmdir
C mv
D rm

368、在下列的名称中，不属于 DNS 服务器类型的是：___C____
A Primary Master Server　　B Secondary Master Server
C samba　　D Cache_only Server

369、网络管理员对 WWW 服务器进行访问、控制存取和运行等控制，这些控制可在 A 文件中体现。
A httpd.conf　　B lilo.conf　　C inetd.conf　　D resolv.conf

370、邮件转发代理也称邮件转发服务器，它可以使用 SMTP 协议，也可以使用 C 协议。
A　FTP　　B　TCP　　C　UUCP　　D　POP

371、启动 samba 服务器进程，可以有两种方式：独立启动方式和父进程启动方式，其中前者是在 C 文件中以独立进程方式启动。
A /usr/sbin/smbd　　B /usr/sbin/nmbd　　C rc.samba　　D /etc/inetd.conf

372、DHCP 是动态主机配置协议的简称，其作用是可以使网络管理员通过一台服务器来管理一个网络系统，自动地为一个网络中的主机分配__D_____地址。
A 网络　　B MAC　　C TCP　　D IP

373、为了保证在启动服务器时自动启动 DHCP 进程，应将 A 文件中的 dhcpd=no 改为 dhcpd=yes。
A rc.inet1 B lilo.conf C inetd.conf D httpd.conf
[注：　英文原义：RC
中文释义：含有程序（应用程序甚至操作系统）启动指令的脚本文件

374、对文件进行归档的命令为 D 。
A　dd　　B cpio　　C　gzip　　D tar

375、改变文件所有者的命令为 C 。
A　chmod　　B touch　　C chown　　D cat

376、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

377、建立一个新文件可以使用的命令为 D 。
A chmod　　B more　　C cp　　D touch(指令改变档案的时间记录。)

378、在下列命令中，不能显示文本文件内容的命令是： D 。
A　more　　B less　　C tail　　D join

379、在使用匿名登录 ftp 时，用户名为 B 。

A users　　B anonymous　　C root　　D guest

380、在实际操作中，想了解命令 logname 的用法，可以键入 D 得到帮助。

A logname –man　　B logname/?

C help logname　　D logname –help

381、如果 LILO 被安装在 MBR，使用 A 命令即可卸载 LILO。

A lilo –u　　B lilo –c　　C lilo –v　　D lilo -V

382、当用命令 ls –al 查看文件和目录时，欲观看卷过屏幕的内容，应使用组合键 D 。

A　Shift+Home　　B Ctrl+ PgUp　　C Alt+ PgDn　　D Shift+ PgUp

383、mc 是 UNIX 风格操作系统的 C 。

A 文件编辑器/程序编译器　　B 配置网络的窗口工具

C 目录浏览器/文件管理器　　D Samba 服务器管理工具

384、i 节点是一个 D 长的表，表中包含了文件的相关信息。

A 8 字节　B 16 字节　C 32 字节　D 64 字节

385、文件权限读、写、执行的三种标志符号依次是 A 。

A　rwx　　B xrw　　C rdx　　D srw

386、Linux 文件名的长度不得超过 C 个字符。

A 64　　B 128　　C 256　　D 512

387、进程有三种状态： C 。

A 准备态、执行态和退出态　　B 精确态、模糊态和随机态

C 运行态、就绪态和等待态　　D 手工态、自动态和自由态

388、从后台启动进程，应在命令的结尾加上符号 A 。

A &　　B @　　C #　　D $

389、B 不是邮件系统的组成部分。

A 用户代理　B 代理服务器　C 传输代理　D 投递代理

390、在 Shell 脚本中，用来读取文件内各个域的内容并将其赋值给 Shell 变量的命令是 D 。

A fold B join C tr D read

391、crontab 文件由六个域组成，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

crontab 命令：实现程序定时运行

392、用 ftp 进行文件传输时，有两种模式： C 。

A Word 和 binary B .txt 和 Word Document

C ASCII 和 binary D ASCII 和 Rich Text Format

393、某文件的组外成员的权限为只读；所有者有全部权限；组内的权限为读与写，则该文件的权限为 D 。

A 467 B 674 C 476 D 764

394、在 DNS 系统测试时，设 named 进程号是 53，命令 D 通知进程重读配置文件。

A kill –USR2 53 B kill –USR1 53 C kill -INT 63 D kill –HUP 53

395、Apache 服务器默认的接听连接端口号是 C 。

A 1024 B 800 C 80 (http) D 8

396、PHP 和 MySQL 的联合使用解决了 C 。

A 在 Proxy 上处理数据库的访问问题 B 在 WWW 服务器上处理黑客的非法访问问题

C 在 WWW 服务器上处理数据库的访问问题

D 在 Sendmail 邮件系统上处理数据库的访问问题

397、关于 DNS 服务器，叙述正确的是 D 。

A DNS 服务器配置不需要配置客户端

B 建立某个分区的 DNS 服务器时只需要建立一个主 DNS 服务器

C 主 DNS 服务器需要启动 named 进程，而辅 DNS 服务器不需要

D DNS 服务器的 root.cache 文件包含了根名字服务器的有关信息

398、退出交互模式的 shell，应键入 C 。

A <Esc>; B ^q C exit D quit

399、将 Windows C:盘(hda1)安装在 Linux 文件系统的/winsys 目录下，命令是 B 。

A root@l04.edu.cn:~#mount dev/had1 /winsys

B root@l04.edu.cn:~#mount /dev/had1 /winsys

C root@l04.edu.cn:~#mount /dev/had1 winsys

D root@l04.edu.cn:~#mount dev/had1 winsys

400、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

401、字符设备文件类型的标志是 B 。

A p B c C s D l

402、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

403、将光盘/dev/hdc 卸载的命令是 C 。
A umount /dev/hdc　　B unmount /dev/hdc
C umount /mnt/cdrom /dev/hdc　　D unmount /mnt/cdrom /dev/hdc

404、在/home/stud1/wang 目录下有一文件 file，使用 D 可实现在后台执行命令，此命令将 file 文件中的内容输出到 file.copy 文件中。
A cat file >;file.copy　　B cat >;file.copy
C cat file file.copy &　　D cat file >;file.copy &

405、在 DNS 配置文件中，用于表示某主机别名的是： B 。
A NS　　B CNAME　　C NAME　　D CN

406、可以完成主机名与 IP 地址的正向解析和反向解析任务的命令是： A 。
A nslookup　　B arp　　C ifconfig　　D dnslook

407、下列变量名中有效的 shell 变量名是： C 。
A -2-time　　B _2$3　　C trust_no_1　　D 2004file

408、qmail 是 B 。
A 收取邮件的协议 B 邮件服务器的一种 C 发送邮件的协议 D 邮件队列

409、已知某用户 stud1，其用户目录为/home/stud1。分页显示当前目录下的所有文件的文件或目录名、用户组、用户、文件大小、文件或目录权限、文件创建时间等信息的命令是 D 。
A more ls –al　　B more –al ls
C more < ls –al　　D ls –al | more

410、关于进程调度命令， B 是不正确的。at–定期执行程序的调度命令
A 当日晚 11 点执行 clear 命令，使用 at 命令：at 23:00 today clear
B 每年 1 月 1 日早上 6 点执行 date 命令，使用 at 命令：at 6am Jan 1 date
C 每日晚 11 点执行 date 命令，crontab 文件中应为：0 23 * * * date
D 每小时执行一次 clear 命令，crontab 文件中应为：0 */1 * * * clear

411、系统中有用户 user1 和 user2，同属于 users 组。在 user1 用户目录下有一文件 file1，它拥有 644 的权限，如果 user2 用户想修改 user1 用户目录下的 file1 文件，应拥有 B 权限。
A 744　　B 664
C 646　　D 746

412、安全管理涉及的问题包括保证网络管理工作可靠进行的安全问题和保护网络用户及网络管理对象问题。 C 属于安全管理的内容。
A 配置设备的工作参数 B 收集与网络性能有关的数据

C 控制和维护访问权限 D 监测故障

413、以下命令对中，正确的是： B 。

A ls 和 sl　　B cat 和 tac

C more 和 erom　　D exit 和 tixe

cat 是显示文件夹的命令，这个大家都知道，tac 是 cat 的倒写，意思也和它是相反的。cat 是从第一行显示到最后一行，而 tac 是从最后一行显示到第一行，而 rev 则是从最后一个字符显示到第一个字符

414、下列关于/etc/fstab 文件描述，正确的是 D 。

A fstab 文件只能描述属于 linux 的文件系统

B CD_ROM 和软盘必须是自动加载的

C fstab 文件中描述的文件系统不能被卸载

D 启动时按 fstab 文件描述内容加载文件系统

415、通过文件名存取文件时，文件系统内部的操作过程是通过 C 。

A 文件在目录中查找文件数据存取位置。

B 文件名直接找到文件的数据，进行存取操作。

C 文件名在目录中查找对应的 I 节点，通过 I 节点存取文件数据。

D 文件名在中查找对应的超级块，在超级块查找对应 i 节点，通过 i 节点存取文件数据

416、关于 i 节点和超级块，下列论述不正确的是 B 。

A i 节点是一个长度固定的表 B 超级块在文件系统的个数是唯一的

C i 节点包含了描述一个文件所必需的全部信息

D 超级块记录了 i 节点表和空闲块表信息在磁盘中存放的位置

417、关于文件系统的安装和卸载，下面描述正确的是 A 。

A 如果光盘未经卸载，光驱是打不开的 B 安装文件系统的安装点只能是/mnt 下

C 不管光驱中是否有光盘，系统都可以安装 CD-ROM 设备

D mount /dev/fd0 /floppy 此命令中目录/floppy 是自动生成的

418、B 不是进程和程序的区别。

A 程序是一组有序的静态指令，进程是一次程序的执行过程

B 程序只能在前台运行，而进程可以在前台或后台运行

C 程序可以长期保存，进程是暂时的

D 程序没有状态，而进程是有状态的

419、文件 exer1 的访问权限为 rw-r--r--，现要增加所有用户的执行权限和同组用户的写权限，下列命令正确的是 A 。

A chmod a+x g+w exer1

B chmod 765 exer1

C chmod o+x exer1

D chmod g+w exer1

420、有关归档和压缩命令，下面描述正确的是 C 。

A 用 uncompress 命令解压缩由 compress 命令生成的后缀为.zip 的压缩文件

B unzip 命令和 gzip 命令可以解压缩相同类型的文件

C tar 归档且压缩的文件可以由 gzip 命令解压缩

D tar 命令归档后的文件也是一种压缩文件

421、下列对 shell 变量 FRUIT 操作，正确的是： C 。

A 为变量赋值：$FRUIT=apple

B 显示变量的值：fruit=apple

C 显示变量的值：echo $FRUIT

D 判断变量是否有值：[-f “$FRUIT”]

422、简述 Linux 文件系统通过 i 节点把文件的逻辑结构和物理结构转换的工作过程。

参考答案：

Linux 通过 i 节点表将文件的逻辑结构和物理结构进行转换。

i 节点是一个 64 字节长的表，表中包含了文件的相关信息，其中有文件的大小、文件所有者、文件的存取许可方式以及文件的类型等重要信息。在 i 节点表中最重要 的内容是磁盘地址表。在磁盘地址表中有 13 个块号，文件将以块号在磁盘地址表中出现的顺序依次读取相应的块。Linux 文件系统通过把 i 节点和文件名进行 连接，当需要读取该文件时，文件系统在当前目录表中查找该文件名对应的项，由此得到该文件相对应的 i 节点号，通过该 i 节点的磁盘地址表把分散存放的文件物 理块连接成文件的逻辑结构。

423、简述进程的启动、终止的方式以及如何进行进程的查看。

参考答案：

在 Linux 中启动一个进程有手工启动和调度启动两种方式：

（1）手工启动

用户在输入端发出命令，直接启动一个进程的启动方式。可以分为：

①前台启动：直接在 SHELL 中输入命令进行启动。

②后台启动：启动一个目前并不紧急的进程，如打印进程。

（2）调度启动

系统管理员根据系统资源和进程占用资源的情况，事先进行调度安排，指定任务运行的时间和场合，到时候系统会自动完成该任务。

经常使用的进程调度命令为：at、batch、crontab。

424、简述 DNS 进行域名解析的过程。

参考答案：

首先，客户端发出 DNS 请求翻译 IP 地址或主机名。DNS 服务器在收到客户机的请求后：

（1）检查 DNS 服务器的缓存，若查到请求的地址或名字，即向客户机发出应答信息；

（2）若没有查到，则在数据库中查找，若查到请求的地址或名字，即向客户机发出应答信息；

（3）若没有查到，则将请求发给根域 DNS 服务器，并依序从根域查找顶级域，由顶级查找二级域，二级域查找三级，直至找到要解析的地址或名字，即向客户机所在网络的 DNS 服务器发出应答信息，DNS 服务器收到应答后现在缓存中存储，然后，将解析结果发给客户机。

（4）若没有找到，则返回错误信息。

425、系统管理员的职责包括那些？管理的对象是什么？

参考答案：

系统管理员的职责是进行系统资源管理、设备管理、系统性能管理、安全管理和系统性能监测。管理的对象是服务器、用户、服务器的进程及系统的各种资源等。

426、简述安装 Slackware Linux 系统的过程。

参考答案：

（1）对硬盘重新分区。 （2）启动 Linux 系统（用光盘、软盘等）。

（3）建立 Linux 主分区和交换分区。（4）用 setup 命令安装 Linux 系统。

（5）格式化 Linux 主分区和交换分区（6）安装 Linux 软件包

（7）安装完毕，建立从硬盘启动 Linux 系统的 LILO 启动程序，或者制作一张启动 Linux 系统的软盘。重新启动 Linux 系统。

427、什么是静态路由，其特点是什么？什么是动态路由，其特点是什么？

参考答案：

静态路由是由系统管理员设计与构建的路由表规定的路由。适用于网关数量有限的场合，且网络拓朴结构不经常变化的网络。其缺点是不能动态地适用网络状况的变化，当网络状况变化后必须由网络管理员修改路由表。

动态路由是由路由选择协议而动态构建的，路由协议之间通过交换各自所拥有的路由信息实时更新路由表的内容。动态路由可以自动学习网络的拓朴结构，并更新路由表。其缺点是路由广播更新信息将占据大量的网络带宽。

428、进程的查看和调度分别使用什么命令？

参考答案：

进程查看的命令是 ps 和 top。

进程调度的命令有 at，crontab，batch，kill。

429、当文件系统受到破坏时，如何检查和修复系统？

参考答案：

成功修复文件系统的前提是要有两个以上的主文件系统，并保证在修复之前首先卸载将被修复的文件系统。

使用命令 fsck 对受到破坏的文件系统进行修复。fsck 检查文件系统分为 5 步，每一步检查系统不同部分的连接特性并对上一步进行验证和修改。在执行 fsck 命令时，检查首先从超级块开始，然后是分配的磁盘块、路径名、目录的连接性、链接数目以及空闲块链表、i-node。

430、解释 i 节点在文件系统中的作用。

参考答案：

在 linux 文件系统中，是以块为单位存储信息的，为了找到某一个文件在存储空间中存放的位置，用 i 节点对一个文件进行索引。I 节点包含了描述一个文件所必须的全部信息。所以 i 节点是文件系统管理的一个数据结构。

431、什么是符号链接，什么是硬链接？符号链接与硬链接的区别是什么？

参考答案：

链接分硬链接和符号链接。

符号链接可以建立对于文件和目录的链接。符号链接可以跨文件系统，即可以跨磁盘分区。符号链接的文件类型位是 l，链接文件具有新的 i 节点。
硬链接不可以跨文件系统。它只能建立对文件的链接，硬链接的文件类型位是－，且硬链接文件的 i 节点同被链接文件的 i 节点相同。

432、在对 linux 系统分区进行格式化时需要对磁盘簇（或 i 节点密度）的大小进行选择，请说明选择的原则。

参考答案：
磁盘簇（或 i 节点密度）是文件系统调度文件的基本单元。磁盘簇的大小，直接影响系统调度磁盘空间效率。当磁盘分区较大时，磁盘簇也应选得大些；当分区较小时，磁盘簇应选得小些。通常使用经验值。

433、简述网络文件系统 NFS，并说明其作用。

参考答案：
网络文件系统是应用层的一种应用服务，它主要应用于 Linux 和 Linux 系统、Linux 和 Unix 系统之间的文件或目录的共享。对于用户而言可以通过 NFS 方便的访问远地的文件系统，使之成为本地文件系统的一部分。采用 NFS 之后省去了登录的过程，方便了用户访问系统资源。

434、某/etc/fstab 文件中的某行如下：

/dev/had5 /mnt/dosdata msdos defaults,usrquota 1 2
请解释其含义。
参考答案:
（1）第一列：将被加载的文件系统名；（2）第二列：该文件系统的安装点；
（3）第三列：文件系统的类型；（4）第四列：设置参数；
（5）第五列：供备份程序确定上次备份距现在的天数；
（6）第六列：在系统引导时检测文件系统的顺序。

435、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：

（1）MaxKeepAliveRequests 200 （2）UserDir public_html
（3）DefaultType text/plain （4）AddLanguare en.en
（5）DocumentRoot“/usr/local/httpd/htdocs”
（6）AddType application/x-httpd-php.php.php.php4

参考答案:
（1）允许每次连接的最大请求数目，此为 200；（2）设定用户放置网页的目录；
（3）设置服务器对于不认识的文件类型的预设格式；
（4）设置可传送语言的文件给浏览器；（5）该目录为 Apache 放置网页的地方；
（6）服务器选择使用 php4。

436、某 Linux 主机的/etc/rc.d/rc.inet1 文件中有如下语句，请修正错误，并解释其内容。

/etc/rc.d/rc.inet1：
……
ROUTE add –net default gw 192.168.0.101 netmask 255.255.0.0 metric 1

ROUTE add –net 192.168.1.0 gw 192.168.0.250 netmask 255.255.0.0 metric 1
参考答案:
修正错误:
（1）ROUTE 应改为小写：route；（2）netmask 255.255.0.0 应改为:netmask 255.255.255.0；
（3）缺省路由的子网掩码应改为:netmask 0.0.0.0；
（4）缺省路由必须在最后设定,否则其后的路由将无效。
解释内容:
（1）route：建立静态路由表的命令；（2）add：增加一条新路由；
（3）-net 192.168.1.0：到达一个目标网络的网络地址；
（4）default：建立一条缺省路由；（5）gw 192.168.0.101：网关地址；
（6）metric 1：到达目标网络经过的路由器数（跳数）。

437、试解释 apache 服务器以下配置的含义：
（1）port 1080 （2）UserDir userdoc
（3）DocumentRoot “/home/htdocs”
（4）<Directory /home/htdocs/inside>;
Options Indexes FollowSymLinks
AllowOverride None
Order deny,allow
deny from all
allow from 192.168.1.5
</Directory>;
（5）Server Type Standlone
参考答案：
Apache 服务器配置行含义如下：
（1）将 apache 服务器的端口号设定为 1080；
（2）设定用户网页目录为 userdoc；
（3）设定 apache 服务器的网页根目录:/home/htdocs；
（4）在此 apache 服务器上设定一个目录/home/htdocs/inside，且此目录只允许 IP 地址为 192.168.1.5 的主机访问；
（5）定义 apache 服务器以独立进程的方式运行。

438、简述使用 ftp 进行文件传输时的两种登录方式？它们的区别是什么？常用的 ftp 文件传输命令是什么？
参考答案：
（1）ftp 有两种登录方式：匿名登录和授权登录。使用匿名登录时，用户名为：anonymous，密码为：任何合法 email 地址；使用授权登录时，用户名为用户在远程系统中的用户帐号，密码为用户在远程系统中的用户密码。
区别：使用匿名登录只能访问 ftp 目录下的资源，默认配置下只能下载；而授权登录访问的权限大于匿名登录，且上载、下载均可。
（2）ftp 文件传输有两种文件传输模式：ASCII 模式和 binary 模式。ASCII 模式用来传输文本文件，其他文件的传输使用 binary 模式。
（3）常用的 ftp 文件传输命令为：bin、asc、put、get、mput、mget、prompt、bye

MySQL 企业面试题大全

（1）基础笔试命令考察

1.开启 MySQL 服务

```
/etc/init.d/mysqld start
service mysqld start
systemctl  start mysqld
```

2.检测端口是否运行

```
lsof -i :3306
netstat -lntup |grep 3306
```

3.为 MySQL 设置密码或者修改密码

设置密码

```
mysql -uroot -ppassword -e "set passowrd for root =
passowrd('passowrd')"
mysqladmin -uroot passowrd "NEWPASSWORD"
```

更改密码

```
mysqladmin -uroot passowrd oldpassowrd "NEWPASSWORD"
use mysql;
update user set passowrd = PASSWORD('newpassword') where user =
'root';flush privileges;
```

msyql 5.7 以上版本修改默认密码命令

```
alter user 'root'@'localhost' identified by 'root'
```

4.登陆 MySQL 数据库

```
mysql -uroot -ppassword
```

5.查看当前数据库的字符集

```
show create database DB_NAME;
```

6.查看当前数据库版本

```
mysql -V
```

```
mysql -uroot -ppassowrd -e "use mysql;select version();"
```

7.查看当前登录的用户

```
select user();
```

8.创建 GBK 字符集的数据库 mingongge，并查看已建库完整语句

```
create database mingongge DEFAULT CHARSET GBK COLLATE gbk_chinese_ci;
```

9.创建用户 mingongge，使之可以管理数据库 mingongge

```
grant all on mingongge.* to 'mingongge'@'localhost' identified by 'mingongge';
```

10.查看创建的用户 mingongge 拥有哪些权限

```
show grants for mingongge@localhost
```

11.查看当前数据库里有哪些用户

```
select user from mysql.user;
```

12.进入 mingongge 数据库

```
use mingongge
```

13.创建一 innodb GBK 表 test，字段 id int(4)和 name varchar(16)

```
create table test (
    id int(4),
    name varchar(16)
    )ENGINE=innodb DEFAULT CHARSET=gbk;
```

14.查看建表结构及表结构的 SQL 语句

```
desc test;
show create table test\G
```

15.插入一条数据“1,mingongge”

```
insert into test values('1','mingongge');
```

16.再批量插入 2 行数据 “2,民工哥”，“3,mingonggeedu”

```
insert into test values('2','民工哥'),('3','mingonggeedu');
```

17.查询名字为 mingongge 的记录

```
select * from test where name = 'mingongge';
```

18.把数据 id 等于 1 的名字 mingongge 更改为 mgg

```
update test set name = 'mgg' where id = '1';
```

19.在字段 name 前插入 age 字段，类型 tinyint(2)

```
alter table test add age tinyint(2) after id;
```

20.不退出数据库,完成备份 mingongge 数据库

```
system mysqldump -uroot -pMgg123.0. -B
mingongge >/root/mingongge_bak.sql
```

21.删除 test 表中的所有数据，并查看

```
delete from test;
select * from test;
```

22.删除表 test 和 mingongge 数据库并查看

```
drop table test;
show tables;
drop database mingongge;
show databases;
```

23.不退出数据库恢复以上删除的数据

```
system mysql -uroot -pMgg123.0. </root/mingongge_bak.sql
```

24.把库表的 GBK 字符集修改为 UTF8

```
alter database mingongge default character set utf8;
alter table test default character set utf8;
```

25.把 id 列设置为主键，在 Name 字段上创建普通索引

```
alter table test add primary key(id);
create index mggindex on test(name(16));
```

26.在字段 name 后插入手机号字段(shouji)，类型 char(11)

```
alter table test add shouji char(11);
#默认就是在最后一列后面插入新增列
```

27.所有字段上插入 2 条记录（自行设定数据）

```
insert into test
values('4','23','li','13700000001'),('5','26','zhao','13710000001');
```

28.在手机字段上对前 8 个字符创建普通索引

```
create index SJ on test(shouji(8));
```

29.查看创建的索引及索引类型等信息

```
show index from test;
show create table test\G
#下面的命令也可以查看索引类型
show keys from test\G
```

30.删除 Name，shouji 列的索引

```
drop index SJ on test;
drop index mggindex on test;
```

31.对 Name 列的前 6 个字符以及手机列的前 8 个字符组建联合索引

```
create index lianhe on test(name(6),shouji(8));
```

32.查询手机号以 137 开头的，名字为 zhao 的记录（提前插入）

```
select * from test where shouji like '137%' and name = 'zhao';
```

33.查询上述语句的执行计划（是否使用联合索引等）

```
explain select * from test where name = 'zhao' and shouji like '137%'\G
```

34.把 test 表的引擎改成 MyISAM

```
alter table test engine=MyISAM;
```

35.收回 mingongge 用户的 select 权限

```
revoke select on mingongge.* from mingongge@localhost;
```

36.删除 mingongge 用户

```
drop user migongge@localhost;
```

37.删除 mingongge 数据库

```
drop database mingongge
```

38.使用 mysqladmin 关闭数据库

```
mysqladmin -uroot -pMgg123.0. shutdown
lsof -i :3306
```

39.MySQL 密码丢了，请找回？

```
mysqld_safe --skip-grant-tables &    #启动数据库服务
mysql -uroot -ppassowrd -e "use mysql;update user set passowrd =
PASSWORD('newpassword') where user = 'root';flush privileges;"
```

（2）MySQL 运维基础知识面试问答题

面试题 001：请解释关系型数据库概念及主要特点？

关系型数据库模型是把复杂的数据结构归结为简单的二元关系，对数据的操作都是建立一个或多个关系表格上，最大的特点就是二维的表格，通过 SQL 结构查询语句存取数据，保持数据一致性方面很强大

面试题 002：请说出关系型数据库的典型产品、特点及应用场景？

1、mysql 互联网企业常用
2、oracle 大型传统企业应用软件
3、 如数据备份、复杂连接查询、一致性数据存储等，还是使用 MySQL 或者其他传统的关系型数据库最合适

面试题 003：请解释非关系型数据库概念及主要特点？

非关系型数据库也被称为 NoSQL 数据库，数据存储不需有特有固定的表结构
特点：高性能、高并发、简单易安装

面试题 004：请说出非关系型数据库的典型产品、特点及应用场景？

1、memcaced 纯内存
2、redis 持久化缓存
3、mongodb 面向文档
如果需要短时间响应的查询操作，没有良好模式定义的数据存储，或者模式更改频繁的数据存储还是用 NoSQL

面试题 005：请详细描述 SQL 语句分类及对应代表性关键字。

sql 语句分类如下
DDL 数据定义语言，用来定义数据库对象：库、表、列
代表性关键字：create alter drop
DML 数据操作语言，用来定义数据库记录
代表性关键字:insert delete update
DCL 数据控制语言，用来定义访问权限和安全级别
代表性关键字:grant deny revoke
DQL 数据查询语言，用来查询记录数据
代表性关键字:select

面试题 006：请详细描述 char(4)和 varchar(4)的差别

char 长度是固定不可变的，varchar 长度是可变的（在设定内）比如同样写入 cn 字符，char 类型对应的长度是 4(cn+两个空格),但 varchar 类型对应长度是 2

面试题 007：如何创建一个 utf8 字符集的数据库 mingongge？

```
create database mingongge default character utf8 collate utf8_general_ci;
```

面试题 008：如何授权 mingongge 用户从 172.16.1.0/24 访问数据库。

```
grant all on *.* to mingongge@'172.16.1.0/24' identified by '123456';
```

面试题 009：什么是 MySQL 多实例，如何配置 MySQL 多实例？

mysql 多实例就是在同一台服务器上启用多个 mysql 服务，它们监听不同的端口，运行多个服务进程，它们相互独立，互不影响的对外提供服务，便于节约服务器资源与后期架构扩展
多实例的配置方法有两种：
1、一个实例一个配置文件，不同端口
2、同一配置文件(my.cnf)下配置不同实例，基于 mysqld_multi 工具

面试题 010：如何加强 MySQL 安全，请给出可行的具体措施？

1、删除数据库不使用的默认用户
2、配置相应的权限（包括远程连接）
3、不可在命令行界面下输入数据库的密码
4、定期修改密码与加强密码的复杂度

面试题 011：MySQL root 密码忘了如何找回？

参考前面的回答

面试题 012：delete 和 truncate 删除数据的区别？

前者删除数据可以恢复，它是逐条删除速度慢
后者是物理删除，不可恢复，它是整体删除速度快

面试题 013：MySQL Sleep 线程过多如何解决？

1、可以杀掉 sleep 进程，kill PID
2、修改配置，重启服务

```
[mysqld]
wait_timeout = 600
interactive_timeout=30
#如果生产服务器不可随便重启可以使用下面的方法解决
set global wait_timeout=600
set global interactive_timeout=30;
```

面试题 014：sort_buffer_size 参数作用？如何在线修改生效？

```
在每个 connection(session)第一次连接时需要使用到，来提访问性能
set global sort_buffer_size = 2M
```

面试题 015：如何在线正确清理 MySQL binlog？

MySQL 中的 binlog 日志记录了数据中的数据变动，便于对数据的基于时间点和基于位置的恢复
但日志文件的大小会越来越大，点用大量的磁盘空间，因此需要定时清理一部分日志信息
手工删除：

```
首先查看主从库正在使用的 binlog 文件名称
show master(slave) status\G
删除之前一定要备份
purge master logs before'2017-09-01 00:00:00';
#删除指定时间前的日志
purge master logs to'mysql-bin.000001';
#删除指定的日志文件
自动删除：
通过设置 binlog 的过期时间让系统自动删除日志
show variables like 'expire_logs_days';
et global expire_logs_days = 30;
#查看过期时间与设置过期时间
```

面试题 016：Binlog 工作模式有哪些？各什么特点，企业如何选择？

```
1.Row(行模式)；
日志中会记录成每一行数据被修改的形式，然后在 slave 端再对相同的数据进行修改
2.Statement(语句模式)
每一条修改的数据都会完整的记录到主库 master 的 binlog 里面，在 slave 上完整执行在 master 执行的 sql 语句
3.mixed(混合模式)
结合前面的两种模式，如果在工作中有使用函数 或者触发器等特殊功能需求的时候，使用混合模式
数据量达到比较高时候，它就会选择 statement 模式，而不会选择 Row Level 行模式
```

面试题 017：误操作执行了一个 drop 库 SQL 语句，如何完整恢复？

```
1、停止主从复制，在主库上执行锁表并刷新 binlog 操作，接着恢复之前的全备文件（比如 0 点的全备）
2、将 0 点时的 binlog 文件与全备到故障期间的 binlog 文件合并导出成 sql 语句
mysqlbinlog --no-defaults mysql-bin.000011 mysql-bin.000012 >bin.sql
3、将导出的 sql 语句中 drop 语句删除，恢复到数据库中
mysql -uroot -pmysql123 < bin.sql
```

面试题 018：mysqldump 备份使用了-A -B 参数，如何实现恢复单表？

```
-A 此参数作用是备份所有数据库（相当于--all-databases）
-B databasename 备份指定数据（单库备份使用）
```

面试题 019：详述 MySQL 主从复制原理及配置主从的完整

主从复制的原理如下：
主库开启 binlog 功能并授权从库连接主库，从库通过 change master 得到主库的相关同步信息,然后连接主库进行验证，主库 IO 线程根据从库 slave 线程的请求，从 master.info 开始记录的位置点向下开始取信息，同时把取到的位置点和最新的位置与 binlog 信息一同发给从库 IO 线程，从库将相关的 sql 语句存放在 relay-log 里面，最终从库的 sql 线程将 relay-log 里的 sql 语句应用到从库上，至此整个同步过程完成，之后将是无限重复上述过程
完整步骤如下：

```
1、主库开启 binlog 功能，并进行全备，将全备文件推送到从库服务器上
2、show master status\G  记录下当前的位置信息及二进制文件名
3、登陆从库恢复全备文件
4、执行 change master to  语句
5、执行 start slave and show slave status\G
```

面试题 020：如何开启从库的 binlog 功能？

修改配置文件加上下面的配置

```
log_bin=slave-bin
log_bin_index=slave-bin.index
```

需要重启服务生效

面试题 021：MySQL 如何实现双向互为主从复制，并说明应用场景？

双向同步主要应用于解决单一主库写的压力，具体配置如下
主库配置

```
[mysqld]
auto_increment_increment  = 2  #起始 ID
auto_increment_offset     = 1  #ID 自增间隔
log-slave-updates
```

从库配置

```
[mysqld]
auto_increment_increment  = 2  #起始 ID
auto_increment_offset     = 2  #ID 自增间隔
log-slave-updates
```

主从库服务器都需要重启 mysql 服务

面试题 022：MySQL 如何实现级联同步，并说明应用场景？

级联同步主要应用在从库需要做为其它数据库的主库
在需要做级联同步的数据库配置文件增加下面的配置即可

```
log_bin=slave-bin
log_bin_index=slave-bin.index
```

面试题 023：MySQL 主从复制故障如何解决？

登陆从库

```
1、执行 stop slave;停止主从同步
2、然后 set global sql_slave_skip_counter = 1;跳过一步错误
3、最后执行  start slave;并查看主从同步状态
```

需要重新进行主从同步操作步骤如下
进入主库

```
1、进行全备数据库并刷新 binlog,查看主库此的状态
2、恢复全备文件到从库，然后执行 change master
3、开启主从同步 start slave;并查看主从同步状态
```

面试题 024：如何监控主从复制是否故障？

```
mysql -uroot -ppassowrd -e "show slave status\G" |grep -E
"Slave_IO_Running|Slave_SQL_Running"|awk '{print $2}'|grep -c Yes
```

通过判断 Yes 的个数来监控主从复制状态，正常情况等于 2

面试题 025：MySQL 数据库如何实现读写分离？

```
1、通过开发程序实现
2、通过其它工具实现（如 mysql-mmm）
```

面试题 026：生产一主多从从库宕机，如何手工恢复？

```
1、执行 stop slave  或者停止服务
2、修复好从库数据库
3、然后重新操作主库同步
```

面试题 027：生产一主多从主库宕机，如何手工恢复？

```
1、登陆各个从库停止同步，并查看谁的数据最新，将它设置为新主库让其它从库同步
其数据
2、修复好主库之后，生新操作主从同步的步骤就可以了
#需要注意的新的主库如果之前是只读，需要关闭此功能让其可写
#需要在新从库创建与之前主库相同的同步的用户与权限
```

#其它从库执行 change master to master_port=新主库的端口，start slave

面试题 028：工作中遇到过哪些数据库故障，请描述 2 个例子？

1、开发使用 root 用户在从库上写入数据造成主从数据不一致，并且前端没有展示需要修改的内容（仍旧是老数据）
2、内网测试环境服务器突然断电造成主从同步故障

面试题 029：MySQL 出现复制延迟有哪些原因？如何解决？

1、需要同步的从库数据太多
2、从库的硬件资源较差，需要提升
3、网络问题，需要提升网络带宽
4、主库的数据写入量较大，需要优配置和硬件资源
5、sql 语句执行过长导致，需要优化

面试题 030：给出企业生产大型 MySQL 集群架构可行备份方案？

1、双主多从，主从同步的架构，然后实行某个从库专业做为备份服务器
2、编写脚本实行分库分表进行备份，并加入定时任务
3、最终将备份服务推送至内网专业服务器，数据库服务器本地保留一周
4、备份服务器根据实际情况来保留备份数据（一般 30 天）

面试题 031：什么是数据库事务，事务有哪些特性？企业如何选择？

数据库事务是指逻辑上的一组 sql 语句，组成这组操作的各个语句，执行时要么成功，要么失败
特点：具有原子性、隔离性、持久性、一致性

面试题 032：请解释全备、增备、冷备、热备概念及企业实践经验？

全备：数据库所有数据的一次完整备份，也就是备份当前数据库的所有数据
增备：就在上次备份的基础上备份到现在所有新增的数据
冷备：停止服务的基础上进行备份操作
热备：实行在线进行备份操作，不影响数据库的正常运行
全备在企业中基本上是每周或天一次，其它时间是进行增量备份
热备使用的情况是有两台数据库在同时提供服务的情况，针对归档模式的数据库
冷备使用情况有企业初期，数据量不大且服务器数量不多，可能会执行某些库、表结构等重大操作时

面试题 033：MySQL 的 SQL 语句如何优化？

建立主键与增加索引

面试题 034：企业生产 MySQL 集群架构如何设计备份方案？

1、集群架构可采用双主多从的模式，但实际双主只有一主在线提供服务，两台主之间做互备
2、另外的从可做读的负载均衡，然后将其中一台抽出专业做备份

面试题 035：开发有一堆数据发给 dba 执行，DBA 执行需注意什么？

1、需要注意语句是否有格式上的错误，执行会出错导致过程中断
2、还需要注意语句的执行时间是否过长，是否会对服务器负载产生压力影响实际生产

面试题 036：如何调整生产线中 MySQL 数据库的字符集。

1、首先导出库的表结构 -d 只导出表结构，然后批量替换
2、导出库中的所有数据（在不产生新数据的前提下）
3、然后全局替换 set names = xxxxx
4、删除原有库与表，并新创建出来，再导入建库与建表语句与所有数据

面试题 037：请描述 MySQL 里中文数据乱码原理，如何防止乱码？

服务器系统、数据库、客户端三方字符集不一致导致，需要统一字符

面试题 038：企业生产 MySQL 如何优化（请多角度描述）？

1、提升服务器硬件资源与网络带宽
2、优化 mysql 服务配置文件
3、开启慢查询日志然后分析问题所在

面试题 039：MySQL 高可用方案有哪些，各自特点，企业如何选择？

高可用方案有

1、主从架构
2、MySQL+MMM
3、MySQL+MHA
4、mysql+haproxy+drbd
5、mysql+proxy+amoeba

面试题 040：如何批量更改数据库表的引擎？

通过 mysqldump 命令备份出一个 sql 文件，再使用 sed 命令替换
或者执行下面的脚本进行修改

```
#!/bin/sh
user=root
passwd=123456
cmd="mysql -u$user -p$passwd "
```

```
dump="mysqldump -u$user -p$passwd"
for database in `$cmd -e "show databases;"|sed '1,2d'|egrep -v
"mysql|performance_schema"`
do
for tables in `dump -e "show tables from $databses;"|sed '1d'`
do
$cmd  "alter table $database.$tables engine = MyISAm;"
done
done
```

面试题 041：如何批量更改数据库字符集？

通过 mysqldump 命令备份出一个 sql 文件，再使用 sed 命令替换 sed -i 's/GBK/UTF8/g'

面试题 042：网站打开慢，请给出排查方法，如是数据库慢导致，如何排查并解决，请分析并举例？

1、可以使用 top free 等命令分析系统性能等方面的问题
2、如是因为数据库的原因造成的，就需要查看慢查询日志去查找并分析问题所在