**一、选择题**

1. Linux系统中DNS服务进程名为（**A**）

A．named  B.httpd  C.ftpd  D.SysLog

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

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

3. 在下列选项中，属于Linux系统日志服务的是（D）

A．named  B.httpd  C.ftpd  D.SysLog

4.Linux操作系统支持的文件系统类型是（A）

A、EXT3  B.NFT  C.TXT  D.FAT

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

A．这是一个文件，而不是目录

B．文件的拥有者可以对这个文件进行读、写和执行的操作

C．文件所有者可以读它，也可以执行它

D、其他所有用户只可以执行它

6.在大多数Linux发行版本中，以下哪个属于块设备（B）

A、串行口 B、硬盘 C、虚拟终端 D、打印机

7.怎样了解您在当前目录下还有多大空间（D）

A． df B. du / C. du .  D. df .

8.以下关于Linux超级权限的说明，不正确的是（C）

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

B.普通用户可以通过su和sudo来获得系统的超级权限

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

D．root是系统的超级用户，无论是否为文件和程序的所有者都具有访问权限

9.REDHAT 6.0的防火墙软件是哪个（B）

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

10．显示文件头部的命令是（C）

A．fidsk  B.mount  C.head  D.man

11.删除文件的命令是（B）

A．mkdir  B.rm  C. mv  D. remove

12.显示用户的ID，以及所属组的ID，要使用命令是（C）

A．su  B.who  C.id  D. man

13.Linux根分区的文件系统是（C）

A．FAT16  B.FAT32  C.EXT3  D.NTFS

14．Linux的DNS服务是下列哪个（C）

A．host  B.hosts  C. bind  D.vsftp

15.不能用来关机的命令是（D）

A.shutdown  B.halt  C.init  D.logout

16.以下哪个命令修改SAMBA口令（A）

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

17./dev/ethX表示（B）

A．系统回送接口 B.以太网接口设备 C.令牌环网设备 D.PPP设备

18.GRUB的配置文件是（C）

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

19.我们将逻辑分区建立在（B）上

A．从分区 B.扩展分区 C.主分区 D.第二分区

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

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

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

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

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

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

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

22.不是shell具有的功能特点是（C）

A.管道 B.输入输出重定向 C.监视系统 D.解释程序命令

23.如果你的umask设为022，则你创建文件的缺省权限是（D）

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

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

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

25.统计文件占用磁盘空间，我们可以使用命令（B）

A．df  B.du  C.mount  D. in

26在SHELL程序里，判断文件不存在的写法是（A）

A．if [ ! –f “$myfile”];then

B. if [-d “$myfile”];then

C. if [-f“$myfile”];then

D. if [! –d “$myfile”];then

27.使用tcpdump监听eth0的80端口网络数据的正确命令是（D）

A．tcpdump –n eth0 port! 80  B. tcpdump –ni eth0 port=80

C. tcpdump –i eth0 port ! 80  D. tcpdump–ni eth0 port 80

28.SQL中，下列操作有语法错误的是（D）

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

29.在Mysql中，下列关于创建数据库表的描述正确的是（C）

A．在创建表时必须设定列的约束

B．在删除表的时候通过列键的约束连接在一起的表会被一同删除

C．在创建表时必须设置列类型

D．通过CREATE TABLE new\_t SELECT \* FROM old\_t复制表的同时，表的约束能够一起被复制到新表中

30.SQL中，”AGE IN (20，22)”的语义是（D）

A.AGE<=22 AND AGE>=20  B. AGE<22 AND AGE>20

C.AGE=20 AND AGE=22  D.AGE=20 OR AGE=22

31.下列对跨站脚本攻击（XSS）的解释最准确的一项是：（D）

A.引诱用户点击虚假网络连接的一种攻击方法

B．构造精妙的关系数据库的结构化查询语言对数据库进行非法的访问

C．一种很强大的木马工具手段

D．将恶意代码嵌入到用户WEB网页中，从而达到恶意的目的

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

A．地址过滤      B.NAT      C.反转        D.IP欺骗

33.局域网的网络地址192.168.1.0/24，局域网络连接其他网络的网关地址是192.168.1.1。主机192.168.1.20访问172.16.1.0/24网络时，其路由设置正确的是（A）

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

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

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

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

34.取ls –l输出结果的第5列的值的正确写法是（B）

A．ls –l |awk “{print$5}”  B.  ls –l |awk‘{print$5}’

C. ls –l |awk {print$5}   D. ls–l |awk ‘print$5’

35.在vi编辑器的命令模式中，删除一行的命令是（B）

A.yy  B.dd  C.pp  D.xx

36.有一个中学获得了C类网段的一组IP192.168.1.0/24.要求你划分7个以上的子网，每个子网主机数不得少于25台，请问子网掩码该怎么写?（B）

A．255.255.255.128 B.255.255.255.224 C.255.255.255.240 D.255.255.240.0

37.在三层交换机和路由器上，启用路由功能的命令是:（D）

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

38.什么命令解压缩tar.gz文件（B）

A. tar –czcffilename.tar.gz  B. tar –xzvf  filename.tar.gz

C. tar –tzvf  filename.tar.gz  D. tar –dzvf filename.tar.gz

39.显示LINUX内核版本号的命令是(B)

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

**二．简答题**

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

答案：

**PHP: php  test.php**

**C: gcc  –o  test  test.c**

**Java: java  test**

2. ftp有几种模式，几种连接类型，有什么区别？

答案：

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

3. 两台Linux服务器都只开放了SSH服务，端口号均为999，你已使用user1登陆服务器1.1.1.1，需要将/home/user1/data.tar.gz文件传送至服务器2.2.2.2用户名为:userB 目的目录为/home/userB，并将文件更名为：dataB.tar.gz 请用一条命令完成上述任务（密码不考虑）

答案：

rsync -av -e “ssh -p999”  /home/user1/data.tar.gz  userB@2.2.2.2:/home/userB/dataB.tar.gz //这是一行命令

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

答案：

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

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

答案

:%s/192.168.0.111/192.168.0.112/g

:1000，1120s/aaa/bbb/g

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

答案：

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

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

防火墙四表五连:

四表：

filter：过滤，防火墙

nat ：network address translation 网络地址转换

mangle：拆解报文，作出修改，封装报文

raw： 关闭nat表上启用的链接追踪机制

五链：

PREROUTING 数据包进入路由之前

INPUT 目的地址为本机

FORWARD 实现转发

OUTPUT 原地址为本机，向外发送

POSTROUTING 发送到网卡之前