linux 日常运维命令

1. 修改系统时间
   [root@localhost ~]# date -s "2012-11-16 10:16:00"
   [root@localhost ~]# clock -w
2. 查看系统的内核
   [root@localhost ~]# uname –a
3. 查看 linux 服务器物理 CPU 的个数
   [root@localhost ~]# cat /proc/cpuinfo | grep "physical id" | sort | uniq | wc –l
4. 查看 linux 服务器逻辑 CPU 的个数
   [root@localhost ~]# cat /proc/cpuinfo | grep "processor " | wc –l
5. 查看 linux 服务器的内存使用
   [root@localhost ~]# free –m
   已用内存：used-buffers-cached
   可用内存：free+buffers+cached
6. 查看服务器硬盘使用情况
   [root@localhost ~]# fdisk –l
7. 查看文件系统的磁盘空间占用情况
   [root@localhost ~]# df –h
8. 查看服务器 IO 使用情况，,（使用下面命令要先安装软件包 yum –y install sysstat）
   [root@localhost ~]# iostat
   Iostat –d –x –k 1(持续查看 IO 使用)
   如果%util 接近 100%说明产生的 I/O 请求太多，I/O 系统已经满负荷，该磁盘可能存在瓶颈。
   如果 idble 小于 70%，I/O 的压力就比较大，说明读取进程中有较多的等待，还可以结合 vmstat 查看 b 参数（等待资源的进程数）和 wa 参数（I/O 等待所占用的 CPU 时间的百分比，高于 30%时 I/O 的压力就比较高了）。
9. 查看目录的大小
   [root@localhost ~]# du -sh /root
10. Dd 命令的使用，在进行维护系统时也经常用到
    *制作交换文件的时候
    Dd if=/dev/zero of=/swapfile bs=1024 count=65536
    *制作驱动盘的时候
    Dd if=rhel40 .img of=/dev/fd0 bs=10k
    制作 ISO 镜像的时候
    Dd if=/dev/cdrom of=/root/cd1 .iso
11. 查看系统负载情况
    [root@localhost ~]# uptime 或者 top
    在使用 top 时，如果 r 经常大于 3 或 4，且 id 经常小于 50，则标示 CPU 的负荷很重
    如果每个 cpu 当前的活动进程数大于 5，则标示系统性能问题严重。
12. 使用 vmstat 命令查看 linux 系统的整体性能（进程、内存、虚拟内存、磁盘 IO、CPU 等）
    [root@localhost ~]# vmstat
13. 查看系统是 23 位的还是 64 位的
    [root@localhost ~]# ls -lF / | grep /$
    *或者用命令# file /sbin/init
    查看输出结果是否有/lib64 的目录，有则说明系统是 64 位的，没有说明是 32 位的。
14. 查看系统安装的模块
    [root@localhost ~]# lsmod
15. 查看服务器 PCI 设置（如：网卡、声卡、显卡等详细信息）
    [root@localhost ~]# lspci

16. 查看和设置用户密码策略

[root@localhost ~]# vim /etc/login.defs

*强制密码长度

[root@localhost ~]# vim /etc/pam.d/system-auth

password requisite pam_cracklib.so try_first_pass retry=3 minlen=12

17. 设置登录超时自动退出终端

[root@localhost ~]# vim /etc/profie

export TMOUT=600

18. 设置禁止 root 用户和空密码用户远程登录系统

[root@localhost ~]# vim /etc/ssh/sshd_config

PermitRootLogin no

PermitEmptyPasswords no

如果拒绝某个用户远程登录系统则：(不能 使用 deny 和 allow)

DenyUsers zhangfeng zhangxiao

-允许用户 zhang 远程登录系统，允许用户 wang 在某个主机登录，其它用户不允许。

AllowUsers zhang wang@192.168.12.1

限制登录失 败后的重试次数 MaxAuthTries 3

设置完后 SSH：使用命令是设置的生效：# /etc/init.d/sshd reload

19. 系统日志管理

[root@localhost ~]# vim /etc/syslog.conf （定义日志类型，输出路径）

[root@localhost ~]# vim /var/log/secure（查看系统登录安全日志：SSH/POP3/telnet、ftp 等）

[root@localhost ~]# last （产看登录用户的信息）

[root@localhost ~]# lastlog （查看所有用户登录的时间）

20. 设置用户在系统的权限；如只让用户使用 ifconfig 命令。

[root@localhost ~]# visudo （编辑 sudo 文件）

Zhang localhost=/sbin/ifconfig

定义别名格式如下：

User_Alias MING=zhang,wang,xiao (别名必须大写，这是定义一个用户组)

Host_Alias ZHU=smtp,pop

Cmnd_Alias MING=/bin/rpm , /usr/bin/yum (定义一组命令集合)

进行调用：

Cmnd_Alias MING=/bin/rpm ,/usr/bin/yum

Zhang localhost=MING

启用 sudo 后，进行日志设置

[root@localhost ~]# visudo

Default logfile = “/var/log/sudo”

[root@localhost ~]# vim /etc/syslog.conf

Local12.debug /var/log/sudo

[root@localhost ~]# /etc/init.d/syslog restart

[root@localhost ~]# sudo –l (查看当前用户被授权的 sudo 命令)

21. 锁定密码文件，运行增加和删除；

[root@localhost ~]# chattr +i /etc/passwd

[root@localhost ~]# chattr -I /etc/passwd(取消 i 权限)

22. 禁止用户执行控制台命令（poweroff、halt、reboot、eject）

在目录/etc/security/console.apps/下有以上命令，将其打包并移除到别的目录或者删除。

23. 禁止用户执行 Ctrl+Alt+Del 热键重启命令

[root@localhost ~]# vim /etc/inittab

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

[root@localhost ~]# init q （使用此命令使之生效）

24. 在 grub 之前设置密码，使用户在进入 grub 前输入密码

① [root@localhost ~]# grub-md5-crypt （设置 MD5 加密密码）

② [root@localhost ~]# vim /boot/grub/grub.conf (在 title 前加入 password --MD5)

25. 限制用户登录的 tty 终端

[root@localhost ~]# vim /etc/inittab （在 tty 终端前加#号，注释掉就可以）

26. 禁止 root 用户登录的终端

[root@localhost ~]# vim /etc/securetty （加#号注释）

27. 禁止除 root 外的用户从 tty1 终端登录系统

① [root@localhost ~]# vim /etc/pam.d/login

Account required pam_access.so (增加此认证)

② [root@localhost ~]# vim /etc/security/access.conf

-:ALL EXCEPT root:tty1 (去掉#号)

- : root : 192.168.12.0/24 172.16.0.0/8（禁止 root 用户从这两个网段远程登录）

26. 防火墙规则表

Filter 表：主要是对数据包进行过滤

Nat 表：主要用于修改数据包的 IP 地址、端口号等。

Mangle 表：此表应用并不广泛。

Raw 表：主要用于决定数据包是否被状态跟踪机制处理，在匹配时 raw 表优先于其它表。

Iptables -A（在末尾追加一条规则）

-D（删除指定链中的某条规则，按序号或内容）

-I（在指定的链中插入一条规则，没有指定位置，在开头插入）

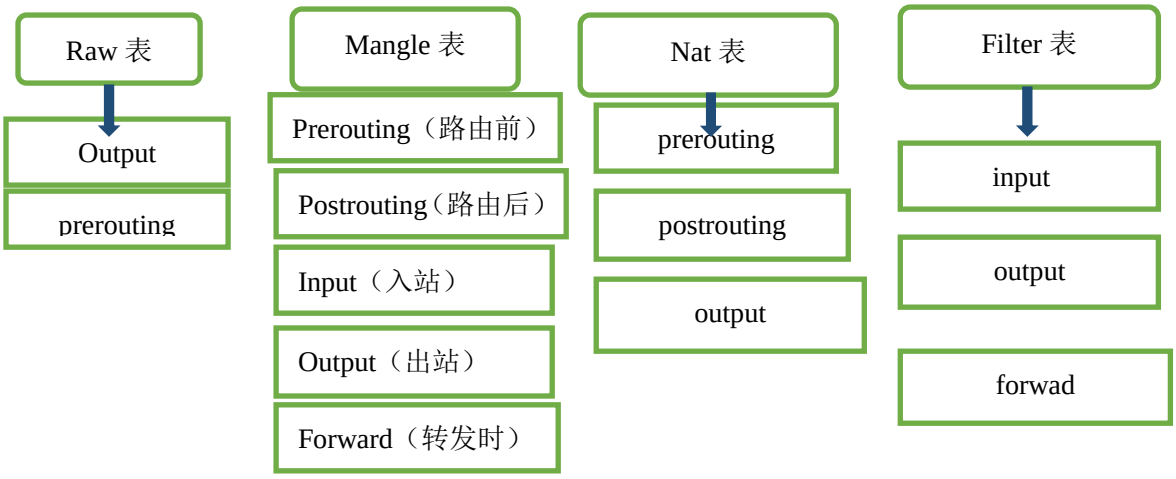
-L （显示防火墙规则）

-F （清除指定连中所有规则，没有指定则清楚表中所有链的规则）

-X（清除用户自定义的规则链）

-P （设置默认的策略）

Iptables （-t 表名） （-A 命令选项） （链名） （条件匹配 –p tcp） （-j 目标动作）



28. Linux 系统 SNAT（只能用在 nat 表的 POSTROUTING 链）和 DNAT（只能用在 nat 表的 prerouting 和 output 链）策略使用

* iptables -t nat -A POSTROUTING –s 192.168.1.0/24 -o etho -j SNAT --to-source 200.100.100.1 (有固定公网 IP 使用此策略)

* iptables -t nat -A POSTROUTING –s 192.168.1.0/24 -o ppp0 -j MASQUERADE (使用动态公网 IP 时使用次策略)

* Iptables -t nat -A PREROUTING -I eth0 -d 200.100.100.1 -p tcp --dport 80 -j DNAT --to-destination 192.68.12.1 (首先要开启路由转发功能，在使用 DNAT 策略)

27. 代理服务器 squid

配置文件：/etc/squid/squid.conf

http_port 3128 （这是 squid 的默认端口号）

cache_mem 64MB （用于设置缓存的内存空间大小）
maximum_object_size 4096 KB （允许保存的缓存的最大对象大小）
reply_body_max_size 1024 allow all （允许用户下载的最大文件大小）
access_log (用于指定日志文件的保存位置)
visible_hostname （用于设置代理服务器可用的完整主机名）
[root@localhost ~]# squid -z （初始化缓存目录）
[root@localhost ~]# squid -k reconfigure (重新加载配置文件)

脚本基础：

29. Sed 的基础用法

Sed 的格式如下：
Sed 【-nefr】【n1,n2】 action
其中：
-n ： 是安静模式，只有经过 sed 处理过的行才显示出来，其它的不显示。
-e ： 默认选项，表示直接在命令行模式进行 sed 操作。
-f ： 将 sed 的操作 写在一个文件里，如：-f filename
-r ： 表示使 sed 支持扩展正则表达式。
N1,n2 ： 选择要进行处理的行。如 10,20 表示在 10~20 行之间处理。
a : 表示添加，后接字符串，添加到当前行 的下一行。
c : 表示替换，后接字符串，用它替换 n1,n2 之间的行。
d : 表示删除字符模式的行，语法为 sed '/regexp/d' ,斜杠之间是正则表达式，模式在 d 前面，d 后面一般不接任何内容。
i : 表示插入，后接字符串，添加到当前行的上一行。
P : 表示打印，打印某个选择的数据，通常与 –n 一起使用。
S : 表示搜索，还可以替换，例如：1,20s/hao/zhang/g 表示替换 1~20 行的 hao 为 zhang。
实例如下：
① 显示 password 内容，将 2~5 行删除后显示
[root@node-rac1 ~]# cat -n /etc/passwd | sed '2,5d'
② 在文件第二行后面加上 hello 语句。
[root@node-rac1 ~]# cat -n /etc/passwd | sed '2a hello'
③ 在文件第二行后面加上两行字，
[root@node-rac1 ~]# cat -n /etc/passwd | sed '2a hello? \
zhangfneg ?'
④ 将 2~5 行的内容替换成“我是好人”
[root@node-rac1 ~]# cat -n /etc/passwd | sed '3,37c 我是好人'
⑤ 只显示文件 5~7 行
[root@node-rac1 ~]# cat -n /etc/passwd | sed -n '5,7p'
利用此表达方式也可以很轻松的分析日志：
[root@node-rac1 ~]# cat /var/log/secure | sed -n '/12:12:50/,/12:13:50/p'
⑥ 只显示 IP 地址和子网掩码
⑦ [root@node-rac1 ~]# ifconfig eth0 | grep "inet addr" | awk -F: '{print $2,$4}'|
> awk '{print $1,$3}'
192.168.12.231 255.255.255.0
[root@node-rac1 ~]#
⑧ 修改文件中第 3 行中的 while 为 root。
[root@node-rac1 ~]# sed -i '3s/root/while/g' zhang.sh

30. Sort 在 linux 中的用法

Sort –b : 忽略前导空格

Sort -f : 忽略大小写
Sort -M ： 按月排序
Sort -n ： 按数字排序
Sort -r ： 倒序排列
Sort -o ： 输入之文件
Sort -u 文件名 ：表示忽略重复，取单一
Sort a.txt | uniq -I 表示取消重复查看重复值有多少次。
例如：要查看服务器被多少 IP 访问过
[root@node-rac1 ~]# sort /var/log/httpd/access-log | awk '{print $1}' | uniq –c

31. Grep 在 linux 中的用法
Grep -a : 表示以文本文件方式搜索。
Grep -c : 表示计算找到符合行的次数
Grep -i : 忽略大小写。
Grep -n : 表示输出行号。
Grep -v : 表示反向选择。
正则表达式：
*修饰符：前一个字符出现零次或多次。
[ ] 通配符：任意单个字符在[ ]中
. 通配符：任意单个字符。
[^] 通配符：不在集合中的任意单个字符。
^ 定位点：行首，或以什么开头。
$ 定位点： 行尾。
[n1-n2]:列出截取的范围：grep ‘[a-z]’a.txt
[:ulnum:] 0-9,A-Z,a-z
[:digit:] 0-9
[:alpha:] A-Z,a-z
[:upper:] A-Z
[:lower:] a-z
[:punct:] 标点符号。

例如：搜索符合的单词的行。
[root@node-rac1 ~]# grep –n 't[ae]st' zhang.txt
取出 oo 前面不是 g 的行
[root@node-rac1 ~]# grep -n '[^g]oo' zhang.txt
查看文件开头不是以字母的行
[root@node-rac1 ~]# grep -n '^[^a-zA-Z]' zhang.sh
查询以 . 结尾的文件行
[root@node-rac1 ~]# grep -n '\.$' hao

扩展正则表达式 egrep 的使用：（grep 只支持基础表达式，而 egrep 支持扩展，其实 egrep 是 grep -E 的别名）
+ ：表示一个或多个重复字符。与.*作用类似
? ：表示 0 个或一个字符。与.*作用类似
| ：表示或的关系。比如’gd|good|dog’表示有 gd 和 good 和 dog 的字符串。
例如：查找文件，去除空白行和行首#的行
[root@node-rac1 ~]# egrep -v '^$|^#' hao
例如：-exec ok 的用法
查找文件并显示文件的属性
[root@node-rac1 ~]# find /root/ -name zhang.sh -exec ls -ld {} \;

32. Find 的常用参数
-name ： 按照文件名查找

-perm ：按照文件的权限查找文件。如：-777

-type ： 按照类型查找：d 目录；c 字符设备文件；p 管道文件；f 普通文件；l 符号链接文件

-user： 按照文件属主查找。

-group：按照文件属组查找文件。

-mtime –n +n ：按照文件的更改时间查找文件。

-nouser 和-nogroup：表示查找无效属组和属主的文件。

Xargs 参数的用法和 exec 差不多。

如:查看当前目录下文件权限是 777 的文件并同时将所有人执行的权限收回。

[root@node-rac1 ~]# find / -perm -777 -print | xargs chmod o-x

33. 脚本常用变量

Read 也可以设置变量如：

#read zhangfeng

Ni shi ge hao xue sheng!

#echo $zhangfneg

$# ：表示命令行中位置参数的数量。

$* ：表示所有位置参数的内容。

$? ：表示命令执行后返回的状态。返回值为 0 为正确。非 0 表示命令执行错误。

$$ ：表示当前的进程号

$! ：表示后台运行的最后一个进程的进程号。

$0 ：表示当前执行的进程的进程名。

数值比较：

-eq ：等于

-ne ：不等于

-gt ：大于

-lt ：小于

-le ：小于或等于

-ge ：大于或等于

逻辑测试：

&& ：逻辑与

|| ：逻辑或

！ ：逻辑否

34. 脚本结构

① ：单分支的 if 语句

```
If
  Then
fi
```

② ：双分支的 if 语句

```
If
  Then
Else
  fi
```

③ ：多分支的 if 语句

```
If
  Then
Elif
  Then
Else
fi
```

④ ：for 循环语句

For
Do
done

⑤：while 语句循环

While
Do
done

⑥：case 语句

Case 变量值 in
模式 1）
命令;;
模式 2）
命令;;
*）
默认命令 esac

选择题

1. 终止一个前台进程可能用到的命令或操作是

A .Kill B. Ctrl+c C. Shutdown D Halt

2. 命令工具 mkdir 在不存在父目录不存在的情况下使用哪个选项

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

3. 文件 exr 的访问权限为 rw-r--r--，现在要增加所有客户的执行权限和同组用户的写权限，下列命令正确的是( ):

A chmod a+xg+w exr B chmod 765 exr C chmod o+x exr D Chmod 777 exr

4. linux 文件权限一共 10 位长度，分成四段，第三段表示的内容是：

A.文件类型 B.文件所有者的权限 C.其他用户的权限 D.文件所有者所在组的权限

5. CentOS 系统中那条命令用于更改文件权限

A. Attrib B. Chmod C. Change D. file

6. 如何从当前系统中卸载一个已装载的文件系统

A. umount

B. dismount

C. mount 一 u

D 从/etc/fstab 中删除这个文件系统项

7. kickstart 的主要作用是

A.提供给客户端 IP 地址

B.提供客户端所需的引导文件

C.实现自动化的系统部署选项设置

D.提供系统镜像存储

8. 以下关于 DHCP 的描述中，正确的是（ ）

A.DHCP 客户机不可能跨越网段获取 IP 地址

B.DHCP 客户机只能收到一个 dhcpoffer

C.DHCP 服务器可以把一个 IP 地址同时租借给两个网络的不同主机

D.DHCP 服务器中可自行设定租约期

9. linux 文件权限一共 10 位长度，分成四段，第三段表示的内容是

A.文件类型 B.文件所有者的权限 C.其他用户的权限 D.又件所有者听在组的权限

10. 终止一个前台进程可能用到的命令或操作是

A .Kill B. Ctrl+c C. Shutdown D. Halt

11. 命令工具 mkdir 在不存在父目录不存在的情况下使用那个选项

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

12. 文件 exr 的访问权限为 rw-r--r--，现在要增加所有客户的执行权限和同组用户的写权限，下列命令正确的是

A. Chmod a+xg+w exr B. Chmod 765 exr C. Chmod o+x exr D. Chmod 777 exr

13. 下列不是 Linux 系统进程类型的是

A. 交互进程 B、批处理进程 C.守护进程 D.就绪进程

14. 配置 Apache 1.3.19 服务器需要修改的配置文件为

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

15. 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 (　　)命令

A.cat　　B.more　　C.less　　D.menu

16. 下列关于/etc/fstab 文件描述，正确的是

A. fstab 文件只能描述属于 linux 的文件系统

B. CD_ R0}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

17. Linux 将存储设备和输入/输出设备均看做文件来操作,( )不是以文件的形式出现。

A.目录　　B.软链接　　C.I 节点表　　D.网络适配器

18. 命令是在 VI 编辑器中执行存盘退出

A:q　　B ZZ　　C:q!　　D:WQ

19. 通过文件名存取文件时，文件系统内部的操作过程是通过

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工节点，通过工节点存取文件数据。

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

20. 目录存放着 Linux 的源代码(　　)

A /etc　　B/usr/src　　C /usr　　D /home

21. 关于文件系统的安装和卸载,下面描述正确的是( )

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是/mnt 下

C. 不管光驱中是否有光盘，系统都可以安装 CD-ROV 设备

D. Mount /dev/fd0 /floppy,此命令中目录/floppy 是自动生成的

22. 如果没有特殊声明,匿名 FTP 服务登录帐号为( )

A、 user B、anonymous C、guest D、用户自己的电子邮件地址

23. 哪个目录存放用户密码信息( )

A. /boot B. /etc C. /var D. /dev

24. 用”rm -i"，系统会提示什么来让你确认( )

A 命令行的每个选项 B.是否真的删除 C 是否有写的权限 D.文件的位置

25. 以下哪个命令可以终止一个用户的所有进程

A. skillall B skill C. kill D. killall

26. 选择正确的可以重启网卡的指令行

A. service network restart

B. ifdown eth0

C. ifup ethl

D. /etc/sysconfig/network — scripts restart

27. 列出包括以”．“开始的隐藏文件在内的所有文件的命令是（ ）

A.ls B.ls -a C.ls -l D. Ls

28. Linux 系统中表示用户主目录的符号是

A 、. B 、.. C、~ D、/

29. Linux 中为了将当前目录下所有.txt 文件打包并压缩归档到文件 this.tar.gz，我们可以使用

A. Tar -czvf this.tar.gz ./*.txt

B. Tar ./*.txt -zcvf this.tar.gz

C. Tar -zxvf this.tar.gz ./*.txt

D. Tar ./*.txt -zxvf this.tar.gz

30. 下列属于 linux 系统关机命令是：(多选)

A.shutdown B.Halt C.stop D.init 0

31. Linux 系统中，采用计划任务通常的命令为

A.cront B.ls C.smit D.sqlplus

32. Linux 最多 ( ) 各主分区

A.3 B.4 C.5 D.6

33. 使用 ( ) 命令更改一个文件的权限设置

A.check B.change C.chmod D.chown

34. 将光盘 CD-ROM (hdc>安装到文件系统的/m nt/cd rom 目录下的命令是

A. mount /mnt/cdrom

B. mount /mnt/cdrom /dev/hdc

C. mount /dev/hdc /mnt/cdrom

D. mount /dev/cdrom

35. 在 V1 编辑器里命令”dd”用来删除当前的

A.行

B.变量

C.字

D.字符

36. 在下列分区中，Linux 默认的分区是

A. FAT32 B. EXT3/ 4 C.FAT D.NTFS

37. 如果用户想对某一命令详细的了解，可用

A. is B. help C.man D.dir

38. 以长格式列目录时，若文件 test 的权限描述为:-rwxrw-r--则文件 test 的类型及文件组的权限是

A.目录文件、读写执行

B.目录文件、读写

C.普通文件、读写

D.普通文件、读

39. /etc/shadow 文件中存放

A.用户账号基本信息

B 用户口令的加密信息

C.用户组信息

D.文件系统信息

40. 为卸载一个软件包，应使用

A. rpm — i B. rpm — e C. rpm -q D. rpm -V

41. 在 LINUX 中，要查看文件内容，可使用

A. More B. cd C. Login D. Logout

42. LINUX 交换分区的格式为

A. ext2 B. ext3 C. FAT D. swap