Linux服务器构建与运维管理

第8章：系统管理

阮晓龙

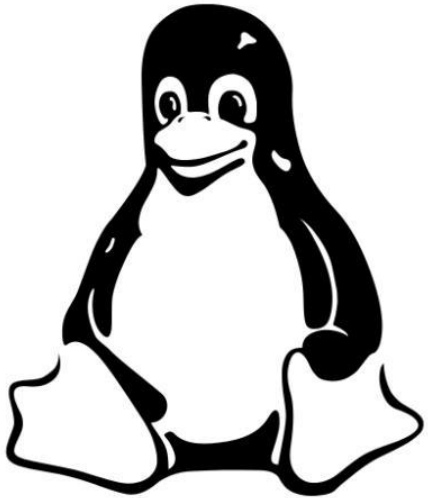
13938213680 / rxl@hactcm.edu.cn
http://linux.xg.hactcm.edu.cn
http://www.51xueweb.cn

河南中医药大学管理科学与工程学科

2018.5

提纲

- 系统管理概述
- 权限管理
  用户、用户组、PAM
- 存储管理
  磁盘处理、RAID、逻辑卷管理
- 文件系统管理
  文件系统、默认安装目录、文件系统修复
- 进程管理
  进程管理、任务计划、定时启动
- 日志管理
  syslogd、logrotate、LogAnalyzer



1.系统管理概述

- 从时间维度上看
  - 一般管理主要对管理对象的当前状况进行控制，使之与预期目标一致；
  - 系统管理不仅注重当前管理，而且还注重对管理对象过去行为特征的分析和发展趋势的预测，它在时间维度上坚持系统的整体观和联系观，强调任何一个系统都是过去、现在和未来的统一，把系统看成是时间的函数。
- 从空间维度上看
  - 一般管理往往只关注某个具体特定的管理对象；
  - 系统管理从整体、联系和开放的观点出发，关注具体对象控制的同时，还考虑该对象与其他事物的关联性以及对象与环境的相互作用。

1.系统管理概述

- 在Linux操作系统中，系统管理的内容就是系统管理员的基本任务或者日常维护，作为一名系统管理员日常需要操作的基本任务有以下方面。
  - 权限管理。
    - 系统管理员应负责为新用户增设账号，将不再活动的用户账号删除，还要处理在账号存在期间所有与该账号有关的事物（如忘记密码等）。当某个用户不应该再访问系统时，必须禁用该用户的账号，该账号拥有的所有文件必须备份后给予删除，以使系统不会随着时间的增长而积累无用信息。
  - 磁盘管理。
    - 如果新增硬件，必须配置系统，使之识别并使用该硬件。如添加磁盘阵列，需要配置系统从而能够识别到磁盘信息，从而更好地使用新存储资源。

1.系统管理概述

- 在Linux操作系统中，系统管理的内容就是系统管理员的基本任务或者日常维护，作为一名系统管理员日常需要操作的基本任务有以下方面。
  - 文件管理。
    - 维护系统的文件系统内容，保证系统文件内容清晰化，方便其他工作人员使用相应文件开展工作。
  - 内存管理。
    - 大型的部署环境需要时刻进行监视系统的运行状态，合理有效的利用系统计算资源，更好地为业务提供计算资源。

1.系统管理概述

- 在Linux操作系统中，系统管理的内容就是系统管理员的基本任务或者日常维护，作为一名系统管理员日常需要操作的基本任务有以下方面。
  - 进程管理。
    - 处理系统中的无用进程，降低系统负载压力。
  - 日志管理。
    - 日志管理也是系统中非常重要的管理工作，但也是经常被忽略或者不尽心做的工作，其工作内容主要为合理的记录相应日志并进行保存，以便于操作追溯和日志审查。

2.权限管理

- 用户标示符
  - 用户登录Linux系统，输入的是用户名（name）以及密码（password），但是Linux操作系统并不会直接识别登录时的用户信息，操作系统中只认识用户的ID标识（UID）。
  - UID（UserID）是用户的ID标识，每个用户的UID值是唯一的，确切的说每个用户都必须对应一个唯一的UID，UID的唯一性关系到系统安全。
  - 系统用户的UID值从0开始，是一个正整数，至于最大值可以在/etc/login.defs中查看到，一般Linux发行版约定最大值为60000。在Linux操作系统中，root的UID是0，拥有系统的最高权限。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/login.defs | grep -v "^#" | grep -v "^$"
MAIL_DIR        /var/spool/mail
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
UID_MIN                  1000
UID_MAX                 60000
SYS_UID_MIN               201
SYS_UID_MAX               999
GID_MIN                  1000
GID_MAX                 60000
SYS_GID_MIN               201
SYS_GID_MAX               999
CREATE_HOME     yes
UMASK           077
USERGROUPS_ENAB yes
ENCRYPT_METHOD SHA512
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 20,24 1 会话 CAP NUM

2.权限管理

- 用户标示符
  - UID是确认用户权限的标识，用户登录系统所属的角色是通过UID来实现的，而非用户名，因此把几个用户共用一个UID是非常危险的。
  - UID的唯一性是需要管理员人为保障的，管理员可以通过修改/etc/passwd文件来修改任何用户的UID值。通常情况下，Linux发行版都会预留一定的UID给系统虚拟用户使用。例如Fedora系统会把前499个UID预留，管理员添加新用户时UID需要从500开始。

- 讨论：创建一个用户demo，将其UID修改为0，会拥有root权限么？

2.权限管理

- 用户类型
  - Linux用户类型简单分为root用户、普通用户、系统用户、虚拟用户。
    - root用户：
      - 用户UID为0，拥有系统最高权限，类似于Windows系统中administrator用户，是整个系统唯一一个拥有最高权限的账户。
    - 普通用户：
      - 由root管理员创建供用户登录系统进行操作使用的账户，但这类用户只能操作个人目录下的内容。通常这类用户的UID在500以上，类似于Windows系统中users用户组中的账户。
    - 系统用户：
      - Linux为满足自身系统管理所内置的账号，通常在安装过程中自动创建，不能用于登录操作系统。通常系统用户的UID是在1-499之间，如系统中的“halt”、“mail”等。这类用户类似于Windows系统中的system用户，但是权限远没有system用户高。
    - 虚拟用户：
      - 在Linux系统中一些用户用来完成特定任务，且没有登录系统权限的用户。
      - 比如说人们使用“nobody”用户访问系统中的网页程序，使用“匿名”用户访问系统的FTP时，都是使用的是虚拟用户。
      - Linux系统中常见的虚拟用户有nobody、ftp、lp、adm、bin等。

2.权限管理

- 用户组标识符
  - GID（Group）是Linux操作系统中用户组的ID值，在系统中每个用户组的GID值是唯一的，管理员通过GID限制每个用户组的权限。
  - GID和UID类似，是一个正整数或0。GID从0开始，GID为0的组是系统赋予给root用户组使用。
  - Linux系统会预留一些较靠前的GID给系统虚拟用户使用，每个系统预留的GID都有所不同。
  - 系统添加用户组默认的GID范围是在/etc/login.def文件中通过GID_MIN和GID_MAX两个选项进行定义，

2.权限管理

- 用户组
  - 用户组（group）就是具有相同特性的用户（user）的集合体，用户组是权限的容器。
  - 在Linux操作系统运行操作过程中，管理员有时需要让多个用户具有相同的权限，比如查看、修改某一文件或执行某个命令，这时管理员把需要操作的用户定义到同一用户组下，通过修改文件或目录权限让定义的用户组具有一定的操作权限，这样同一用户组下的所有用户都具有对该文件或目录都具有相同的权限，这就是用户组的主要意义。

2.权限管理

- 用户组
  - 在Linux操作系统中，主要有三类用户组，分别为普通用户组、系统用户组以及私有组，具体如下所示。
    - 普通用户组：
      - 通常是由系统管理员创建的，可以指定加入多个用户，加入的用户将继承用户组的权限。
    - 系统用户组：
      - 该类用户组一般存放系统用户，用于执行系统中的某些应用软件。
    - 私有组，也称基本组：
      - 当创建用户时，如果没有为其指明所属用户组，则就为其定义一个私有的用户组，私有用户组的名称和用户名相同。
      - 私有组可以转变成普通用户组，当把其他用户加入到一个私有组中，私有组就变成了普通用户组。

2.权限管理

- 用户组
  - Linux操作系统中用户与用户组的对应关系有四种，分别是一对一、多对一、一对多或多对多。
    - 一对一：某个用户可以是某个用户组的唯一成员。
    - 多对一：多个用户可以是某个唯一用户组的成员，不归属其他用户组。
    - 一对多：某个用户可以是多个用户组的成员。
    - 多对多：多个用户对应多个用户组，并且几个用户可以是归属相同的组。

2.权限管理

- 与用户有关的配置文件
  - 与用户有关的信息保存在/etc/passwd和/etc/shadow两个文件中。
  - /etc/passwd
    - /etc/passwd是系统识别用户的一个文件，在实际中/etc/passwd就相当于操作系统的“花名册”，系统所有的用户都在这里有记载。
    - 如一个账户“zhangsan”登录操作系统，其账号在登录时需经过如下步骤。
      - 账号登录时，系统首先查阅/etc/passwd文件，判断是否有“zhangsan”账号；
      - 确定账号的UID值，根据UID值确认用户和身份；
      - 系统中如果存在“zhangsan”账号，则读取/etc/shadow文件中所对应的“zhangsan”账号的密码，如果密码核实无误则登录系统成功，并开始读取用户的配置文件。

2.权限管理

- 与用户有关的配置文件
  - 与用户有关的信息保存在/etc/passwd和/etc/shadow两个文件中。
  - /etc/passwd
    - /etc/passwd是系统识别用户的一个文件，在实际中/etc/passwd就相当于操作系统的“花名册”，系统所有的用户都在这里有记载。
    - 如一个账户“zhangsan”登录操作系统，其账号在登录时需经过如下步骤。
      - 账号登录时，系统首先查阅/etc/passwd文件，判断是否有“zhangsan”账号；
      - 确定账号的UID值，根据UID值确认用户和身份；
      - 系统中如果存在“zhangsan”账号，则读取/etc/shadow文件中所对应的“zhangsan”账号的密码，如果密码核实无误则登录系统成功，并开始读取用户的配置文件。
    - 在/etc/passwd配置文件中，每一行都表示的是一个用户的信息，每一行有7个字段，每个字段之间用“：”号分割。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:997:User for polkitd:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
arpwatch:x:77:77::/var/lib/arpwatch:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
webalizer:x:67:996:Webalizer:/var/www/usage:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 27,24 1 会话 CAP NUM

表 11-1 /etc/passwd 字段含义说明

字段	说明
第一字段	root，用户名（也被称为登录名）
第二字段	x，root 登录账户的密码，具体内容是一个字母，表明其密码已被映射到/etc/shadow 文件中
第三字段	0，表示用户（root）的 UID 值
第四字段	0，表示用户（root）所在组的 GID 值
第五字段	root，表示用户名全称，这是可选的，可以不设置
第六字段	/root，表示用户个人目录所在
第七字段	/bin/bash，表示用户所有 Shell 的类型

2.权限管理

- 与用户有关的配置文件
  - 与用户有关的信息保存在/etc/passwd和/etc/shadow两个文件中。
  - /etc/shadow
    - /etc/shadow文件是/etc/passwd的影子文件，但并不是由/etc/passwd产生的。
    - /etc/shadow和/etc/passwd是对应互补的。
    - /etc/shadow文件内容包括了用户名及被加密的密码以及其他在/etc/passwd中没有包括的用户信息。比如用户的有效期限、密码过期时间等。
    - /etc/shadow文件的读取和修改需要root权限。
    - 在/etc/shadow配置文件中，每一行都表示的是一个用户密码的映射信息，每一行有9个字段，每个字段之间用“：”号分割。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/shadow
root:$6$1gSkSpb9IUlEiIXW$oo04L5JbV33wICkt/wqHTcQJ0Syo6wECvqlwd.tCUCanAhFbQab0YtM
MXCD4ZRxGmfdpj30yFv0Axdi46kF8y1::0:99999:7:::
bin:*:17110:0:99999:7:::
daemon:*:17110:0:99999:7:::
adm:*:17110:0:99999:7:::
lp:*:17110:0:99999:7:::
sync:*:17110:0:99999:7:::
shutdown:*:17110:0:99999:7:::
halt:*:17110:0:99999:7:::
mail:*:17110:0:99999:7:::
operator:*:17110:0:99999:7:::
games:*:17110:0:99999:7:::
ftp:*:17110:0:99999:7:::
nobody:*:17110:0:99999:7:::
systemd-network:!!:17587::::::
dbus:!!:17587::::::
polkitd:!!:17587::::::
postfix:!!:17587::::::
sshd:!!:17587::::::
rpc:!!:17603:0:99999:7:::
arpwatch:!!:17611::::::
tcpdump:!!:17611::::::
apache:!!:17632::::::
mysql:!!:17644::::::
webalizer:!!:17645::::::
vuser:!!:17653:0:99999:7:::
rpcuser:!!:17655::::::
[root@Centos7Teach ~]#
```

表 11-2 /etc/shadow 字段含义说明

字段	说明
第一字段	用户名（也被称为登录名），在/etc/shadow 中，用户名和/etc/passwd 是相同的，这样就把 passwd 和 shadow 中用户的用户记录联系在一起，该字段为非空字段
第二字段	密码，已被加密的密码，如果在该字段显示的是“x”，表示这个用户不能登录到系统，该字段为非空字段
第三字段	上次修改口令的时间。这个时间是从 1970 年 01 月 01 日算起到最近一次修改口令的时间间隔（天数）
第四字段	两次修改口令间隔最少的天数，如果设置为 0，则表示禁用此功能，其默认值是通过/etc/login.defs 文件的 PASS_MIN_DAYS 选项进行定义
第五字段	两次修改口令间隔最多的天数，也就是所谓的口令有效期。其默认值是通过/etc/login.defs 文件的 PASS_MAS_DAYS 选项进行定义
第六字段	提前多少天警告用户口令即将过期。当用户登录系统后，系统登录程序将提醒用户口令将要在多少天内作废。其默认值是通过/etc/login.defs 文件的 PASS_WARN_AGE 选项进行定义
第七字段	在口令过期之后多少天禁用此用户。此字段表示用户口令作废多少天后，系统会禁用此用户。用户禁用后，将无法登录系统且无法进行口令修改
第八字段	用户过期日期。此字段制定了用户过期的天数（从 1970 年的 01 月 01 日开始的天数），如果这个字段的值为空，账号永远不过期
第九字段	保留字段，目前为空，以备将来 Linux 发展之用

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 29,24 1 会话 CAP NUM

2.权限管理

- 用户组有关的配置文件
  - 与用户组有关的信息保存在/etc/group和/etc/gshadow两个文件中。
  - /etc/group
    - /etc/group文件是用户组的配置文件，内容包括用户的用户组，并且能显示出用户是归属哪个用户组或哪几个用户组。
    - 用户组在系统管理中为系统管理员提供了极大的方便，但也存在一定的安全性问题。如某个用户对系统管理有重要的权限，建议最好让用户拥有独立的用户组，或者是把用户下的文件权限设置为完全私有，从而确保不会因为用户组的权限集成特性造成其他用户越权管理。
    - root用户组通常不要把普通用户加入进去，以防止普通用户拥有root权限。
    - 在/etc/group配置文件中包括用户组（Group）、用户组口令、GID以及该用户组所包含的用户（User），每个用户组一条记录，每一行有4个字段，每个字段之间用“：”号分割。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:30:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
ssh_keys:x:999:
input:x:998:
systemd-journal:x:190:
systemd-network:x:192:
dbus:x:81:
polkitd:x:997:
postdrop:x:90:
postfix:x:89:
sshd:x:74:
rpc:x:32:
arpwatch:x:77:
tcpdump:x:72:
apache:x:48:
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

表 11-3 /etc/group 字段含义说明

字段	说明
第一字段	用户组名称，该字段为非空字段
第二字段	密码，已被加密的密码，如果在该字段显示的是“x”，表示这个用户的密码为为空，该字段为非空字段
第三字段	GID 值，该字段为非空字段
第四字段	用户列表，每个用户之间用“,”分割。该字段可以为空，如果字段为空，则表示用户组为 GID 的用户名

2.权限管理

- 用户组有关的配置文件
  - 与用户组有关的信息保存在/etc/group和/etc/gshadow两个文件中。
  - /etc/gshadow
    - /etc/gshadow是/etc/group的加密文件，用户组（Group）管理的密码就是存放在这个文件中。
    - /etc/gshadow和/etc/group是互补的两个文件。
    - 在/etc/gshadow内容中每个用户组一条记录，每一行有4个字段，每个字段之间用“：”号分割。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/gshadow
root:::
bin:::
daemon:::
sys:::
adm:::
tty:::
disk:::
lp:::
mem:::
kmem:::
wheel:::
cdrom:::
mail:::postfix
man:::
dialout:::
floppy:::
games:::
tape:::
video:::
ftp:::
lock:::
audio:::
nobody:::
users:::
utmp:!::
utempter:!::
ssh_keys:!::
input:!::
systemd-journal:!::
systemd-network:!::
dbus:!::
polkitd:!::
postdrop:!::
postfix:!::
sshd:!::
rpc:!::
arpwatch:!::
tcpdump:!::
apache:!::
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

表 11-4 /etc/gshadow 字段含义说明

字段	说明
第一字段	用户组名称，该字段为非空字段
第二字段	用户组密码，该字段可以为空或者为“!”，如果为空或为“!”，表示没有密码
第三字段	用户组管理者，该字段可以为空，如果有多个用户组管理者，用“,”号分割
第四字段	组成员，如果有多个成员，用“,”分割

2.权限管理

- 用户规则文件
  - etc/login.defs
    - /etc/login.defs文件是当创建用户时的一些默认规划。
    - 对此文件的修改需要root权限。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/login.defs | grep -v "^#" | grep -v "^$"
MAIL_DIR        /var/spool/mail
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
UID_MIN                  1000
UID_MAX                 60000
SYS_UID_MIN               201
SYS_UID_MAX               999
GID_MIN                  1000
GID_MAX                 60000
SYS_GID_MIN               201
SYS_GID_MAX               999
CREATE_HOME     yes
UMASK           077
USERGROUPS_ENAB yes
ENCRYPT_METHOD SHA512
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 19,24 1 会话 CAP NUM

表 11-5 /etc/login.defs 主要配置选项说明

配置	初始值	说明
MAIL_DIR	/var/spool/mail	定义创建用户时，要在目录/var/spool/mail 中创建一个用户 mail 文件
PASS_MAX_DAYS	99999	定义用户的密码不过期最多的天数
PASS_MIN_DAYS	0	定义密码修改之间最小的天数
PASS_MIN_LEN	5	定义密码最小长度
PASS_WARN_AGE	7	定义密码过期告警天数
UID_MIN	1000	定义最小 UID 为 1000，添加用户时，UID 是从 1000 开始
UID_MAX	60000	定义最大 UID 值为 60000
SYS_UID_MIN	201	定义系统用户 UID 最小为 201，添加系统用户 UID 从 201 开始
SYS_UID_MAX	999	定义系统用户最大为 999
GID_MIN	1000	定义最小 GID 为 1000，添加用户组 GID 从 1000 开始
GID_MAX	60000	定义最大 GID 值为 60000
SYS_GID_MIN	201	定义系统用户组最小为 201，添加系统用户组 GID 从 201 开始
SYS_GID_MAX	999	定义系统用户组最大为 999
CREATE_HOME	yes	定义创建用户时，是否创建用户目录，初始要求创建
UMASK	077	定义创建用户后的权限掩码
USERGROUPS_ENAB	yes	定义创建用户时是否同时创建相同用户名的组
ENCRYPT_METHOD	SHA512	定义密码的加密方式为 SHA512

2.权限管理

- 用户规则文件
  - etc/default/useradd
    - /etc/default/userad定义了通过useradd命令添加用户时的规则。

2.权限管

2.1用户与用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/default/useradd | grep -v "^#" | grep -v "^$"
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 9,24 1 会话 CAP NUM

表 11-6 /etc/default/useradd 配置选项说明

配置	初始值	说明
GROUP	100	定义创建用户时，用户归属用户组为 100
HOME	/home	定义创建用户时，在/home 中创建用户名目录
INACTIVE	-1	定义启用账号过期权限，-1 表示不启用
EXPIRE	-	定义账号终止日期，不设置表示不启用
SHELL	/bin/bash	定义创建用户所具有的 SHELL 类型
SKEL	/etc/skel	定义账号使用默认文件内容，可以理解为添加用户的目录默认文件存放位置。 当用户用 useradd 添加用户时，用户主目录下的文件都是从这个目录中复制的
CREATE_MAIL_SPOOL	yes	定义是否创建邮箱缓存，yes 表示创建

2.权限管理

- 文件目录权限
  - 文件目录权限针对的角色
    - Linux操作系统中，文件权限是依据三种角色进行定义的，分别是文件所有者（属主）、文件属组用户和其他人。
    - 文件所有者是指创建文件的人，但是并不是一定的，因为文件创建后可以变更文件属主为指定用户。通俗的说，文件创建者是文件的所有者（属主），但是这个权限可以转让。转让文件属主权限的操作必须由root账户执行。
    - 在具体使用中，可以将文件交给一个用户组进行管理，那么这个用户组就是文件属组。文件属组不是一堆文件的组合，而是一堆用户的组合，也就是用户组的概念。在具体的文件权限管理上，可以指定一组用户文件的管理权限。
    - 其他人就是除了文件所有者、文件属组用户外的所有人。

2.权限管理

- 文件目录权限
  - 文件目录权限类型
    - 文件权限的定义有三种方式，分别是：读取（r）、写入（w）和执行（x）。
    - （1）对于单独的文件具有的权限如下所示。
      - 读取权限：指用户可以打开文件，并查看文件的内容；
      - 写入权限：指用户可以编辑文件，修改文件的内容，但是否可以删除文件或重命名文件，是由用户对该文件所在目录的权限决定；
      - 执行权限：指用户可以执行文件。Linux操作系统中，可以进行执行权限设置的文件有二进制代码文件和Shell脚本文件两种。
    - （2）对文件目录具有的权限如下所示。
      - 读取权限：指用户能否列出文件目录内的所有文件夹和文件信息；
      - 写入权限：指用户能否在文件目录内创建、删除和重命名文件；
      - 执行权限：指用户能否进入文件目录内。

2.权限管理

- 文件目录权限
  - 文件目录权限表示方法
    - 每一个文件有3种表示权限的方法，那么一个文件就有8种权限，Linux使用八进制来表示文件目录权限。
    - 在Linux操作系统中，每一个文件或文件目录都要针对三种角色进行授权，因此Linux使用9位二进制数来表示文件目录权限。
    - 由于3个二进制对应与1个八进制数，因此也可以使用3位八进制数来表示文件目录权限。

2.权限管理

- 文件目录权限
  - 文件目录权限表示方法

表 11-7 八进制、二进制、文件权限对应关系

八进制	二进制	文件目录权限	权限描述
0	000	---	无权限
1	001	--x	执行
2	010	-w-	写入
3	011	-wx	写入执行
4	100	r--	读取
5	101	r-x	读取执行
6	110	rw-	读取写入
7	111	rwx	读取写入执行

2.权限管理

- 用户权限掩码
  - 权限掩码
    - umask是chmod配套的，总共4位（GID/UID、属主、组权、其他用户权限），不过在实际应用过程中通常使用到的是后3个。
    - 默认情况创建用户后，用户的umask值是022（可以用umask命令查看）。

2.权限管理

- 用户权限掩码
  - 权限掩码计算
    - umask命令允许设定文件创建时的缺省模式，对应每一类用户（文件属主、同组用户、其他用户）存在一个相应的umask值中的数字。
    - 对于文件来说，这个数字最大值是6。系统不允许用户在创建文本文件时就赋予该文件执行权限，必须在创建后用“chmod”命令增加这一权限。
    - 目录运行执行权限，这样针对目录来说，umask中各个数字最大可以到7。
    - 计算umask值的方法，主要遵循umask是从权限中“拿去”相应的位即可。

2.权限管理

- 用户权限掩码
  - 权限掩码计算

表 11-8 umask 与文件、目录权限对应关系

umask 中某位值	文件		目录	
	权限值	描述	权限值	描述
0	6	读取写入	7	读取写入执行
1	6	读取执行	6	读取写入
2	4	读取	5	读取执行
3	4	读取	4	读取
4	2	写入	3	写入执行
5	2	写入	2	写入
6	0	无权限	1	执行
7	0	无权限	0	无权限

2.权限管理

用户管理常用命令

表 11-9 用户管理命令一览表

命令	说明
useradd	添加用户
adduser	添加用户
passwd	设置用户的密码
usermod	修改用户的配置参数，例如登录名、用户的个人目录等
pwconv	开启用户的投影密码。将用户密码从/etc/passwd 同步到/etc/shadow
pwck	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，该命令会把密码从 shadow 文件内，重新存入到 passwd 文件中
finger	查看用户信息工具
id	查看用户 UID、GID 及所归属的用户组
chfn	更改用户信息
su	用户切换工具
sudo	通过另一个用户来执行命令（execute a command as another user），su 用来切换用户，然后通过切换到用户来完成相应的任务
visudo	visudo 是编辑/etc/sudoers 的命令，相当于直接编辑/etc/sudoers
sudoedit	通过另一个用户来执行完成相应的命令

2.权限管理

查看用户信息：id

【功能】

id 命令用于查看用户信息和用户组信息；指定用户名时查看指定用户信息，不指定用户名时查看当前用户的信息，不指定参数时，显示所有信息。

【语法】

```
# id [选项] [用户名]
```

【选项说明】

id 命令选项及其说明如表 11-10 所示。

表 11-10 id 命令选项及其说明

选项	说明
-a	显示用户名、UID 和该用户所属的所有组
-Z 或--context	显示当前用户 SELinux 所对应的安全上下文信息
-g 或--group	显示所用所属群组的 ID
-G 或—groups	显示用户所属附加群组的 ID
-n 或—name	显示用户，所属群组或附件群组的名称
-r 或—real	显示实际 ID
-u 或—user	显示用户 ID
-z 或—zero	显示用户空字符，无空格
--help	显示 id 帮助信息
--version	显示版本信息

2.权限管

- 查看用户

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# id apache
uid=48(apache) gid=48(apache) groups=48(apache)
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# id -g
0
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# id -G
0
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 16,24 1 会话 CAP NUM

2.权限管理

- 查看登录用户信息：w、who、users

【功能】

w、who 和 users 命令都可查询已登录当前主机的用户，三者命令的作用相同，但是使用方式不同。

【语法】

w、who 和 users 命令其语法格式分别如下所示。

```
#查看登录用户信息-w 命令
# w [选项] [用户名]
#查看登录用户信息-who 命令
# who [选项] [查询文件]
#查看登录用户信息-users 命令
# users [选项]
```

三种命令都可不添加任何选项和参数进行查看当前登录用户的默认信息。

2.权限管理

- 查看登录用户信息

【选项说明】

①w 命令选项及其说明如表 11-11 所示。

表 11-11 w 命令选项及其说明

选项	说明
-h 或--no-header	不显示头信息
-u 或--no-current	显示当前进程和 CPU 时间时忽略用户名
-s 或--short	使用短输出格式
-f 或--from	显示用户从哪里进行登录，有主机名显示主机名，否则显示 IP 地址
-o 或--old-style	使用旧输出样式进行输出
-i 或--ip-addr	显示登录用户的 IP 地址
--help	显示 w 命令帮助信息
-V 或--version	显示版本信息

②who 命令选项及其说明如表 11-12 所示。

表 11-12 who 命令选项及其说明

选项	说明
-a 或--all	显示用户登录的所有信息
-b 或--boot	显示系统启动时间
-d 或--dead	显示系统中死进程
-H 或--heading	显示各栏位的标题信息列
-l 或—login	显示系统登录进程信息，只显示 1 条
--lookup	通过 DNS 获取登录用户的主机名
-m	此选项和指定"am i"字符串返回结果相同，显示登录主机名和用户
-p 或--process	显示当前由 init 生成的活动进程
-q 或--count	显示登录系统的账号名称和总人数
-r 或--runlevel	显示初始化进程的当前运行级别
-s 或--short	此参数将忽略不予处理，仅负责解决 who 指令其他版本的兼容性问题
-t 或--time	显示系统上次时间更改
-T 或-w 或—mesg 或—message 或--writable	显示用户的信息状态栏
-u 或--users	显示当前系统中登录的所有用户信息
--help	显示 who 命令帮助信息
-V 或--version	显示版本信息

2.权限管

- 查看登录

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# w
 14:01:39 up 6 days, 13:02,  2 users,  load average: 0.05, 0.03, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    10.10.0.1        11:09    2:50m  0.01s  0.01s -bash
root     pts/1    10.10.0.1        13:09    3.00s  0.08s  0.02s w
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 6,24 1 会话 CAP NUM

表 11-14 w 命令返回结果说明

字段	结果	说明
-	04:22:11	执行 w 命令的时间
-	up 2:30	表示当前系统运行 2 小时 30 分钟
-	1 user	表示当前登录系统用户总数
-	Load average	表示系统在最近 1、5、10 分钟内负载程度
USER	root	显示登录用户账号名
TTY	pts/0	显示用户登录所使用的终端
LOGIN@	01:52	表示用户登录系统进入的时长为 1 小时 52 分
IDLE	3.00s	用户空闲时间，从用户上一次任务结束后开始计时
JCPU	0.10s	以终端号来区分，表示在这段时间内，所有与该终端相关的进程任务所耗费的 CPU 时间
PCPU	0.00s	指 WHAT 域任务执行后消耗 CPU 时间
WHAT	w	表示当前用户执行的任务

2.权限管

- 查看登录

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# who
root     pts/0        May 16 11:09 (10.10.0.1)
root     pts/1        May 16 13:09 (10.10.0.1)
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# users
root root
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 8,24 1 会话 CAP NUM

表 11-15 who 命令返回结果说明

结果	说明
root	显示当前登录用户账号名
pts/0	显示用户登录所使用的终端
2017-12-20 06:30 （172.16.124.159）	显示登录用户登录时间以及 IP 地址

2.权限管理

新增用户：useradd

【功能】

useradd 命令用于 Linux 中创建新的系统用户。使用 useradd 命令创建账号完成之后，实际上是保存在/etc/passwd 文本文件中。

【语法】

```
# useradd [选项] [登录用户名]                    //useradd 常用语法格式
# useradd – D
# useradd – D [选项]
```

【选项说明】

useradd 命令选项及其说明如表 11-16 所示。

表 11-16 useradd 命令选项及其说明

选项	说明
-b 或--base-dir BASE_DIR	为创建的用户指定基础目录
-c 或--comment COMMENT	为用户加上备注文字，备注文字会保存在 passwd 的稳重栏位中
-d 或--home-dir HOME_DIR	指定用户登录时的起始目录
-D 或--defaults	变更预设值
-e 或--expiredate EXPIRE_DATE	指定账号的有效期限
-f 或--inactive INACTIVE	指定在密码过期后多少天关闭该账号
-g 或--gid GROUP	指定用户所属用户组

2.权限管理

- 新增用户：use

表 11-16 useradd 命令选项及其说明

选项	说明
-b 或--base-dir BASE_DIR	为创建的用户指定基础目录
-c 或--comment COMMENT	为用户加上备注文字，备注文字会保存在 passwd 的稳重栏位中
-d 或--home-dir HOME_DIR	指定用户登录时的起始目录
-D 或--defaults	变更预设值
-e 或--expiredate EXPIRE_DATE	指定账号的有效期限
-f 或--inactive INACTIVE	指定在密码过期后多少天关闭该账号
-g 或--gid GROUP	指定用户所属用户组
-G 或--groups GROUPS	指定用户所属的附加用户组
-h 或--help	显示 useradd 帮助命令信息
-k 或--skel SKEL_DIR	替换用户骨架目录，包括将被复制到用户家目录的文件和目录
-K 或--key KEY=VALUE	覆盖/etc/login.defs 默认的用户添加规则值
-l 或--no-log-init	不将用户添加到 lastlog 和 faillog 数据库
-m 或--create-home	自动创建用户的登入目录
-M 或--no-create-home	不自动创建用户的登入目录
-N 或--no-user-group	不创建与用户名相同的组名称
-o 或--non-unique	允许创建具有重复 UID（非唯一）的用户
-p 或--password PASSWORD	为新用户创建加密密码
-r 或--system	指定创建系统账号
-R 或--root CHROOT_DIR	指定用户的 CHROOT 目录
-s 或--shell SHELL	指定用户登入后所使用的 shell
-u 或--uid UID	指定用的 UID 值
-U 或--user-group	指定为该用户创建一个与用户名称相同的用户组
-Z 或--selinux-user SEUSER	使用一个特定的 seuser 的 SELinux 用户映射

2.权限管

- 新增用户

Teach-CentOS 7 - root@Centos7Teach:/var/mail - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# useradd user1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# useradd user2 -u 544
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# useradd user3 -g user2 -G user1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# cat /etc/passwd | grep user
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
user1:x:1000:1000::/home/user1:/bin/bash
user2:x:544:1001::/home/user2:/bin/bash
user3:x:1001:1001::/home/user3:/bin/bash
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# cd /home
[root@Centos7Teach home]# ls -l
total 0
drwx------. 2 user1 user2 62 May  3 11:32 ftpuser
drwx------. 2 user3  1002 62 May  3 22:33 tsuser
drwx------. 2 user1 user1 62 May 16 14:15 user1
drwx------. 2 user2 user2 62 May 16 14:15 user2
drwx------. 2 user3 user2 62 May 16 14:16 user3
drwx------. 2 user1 user1 62 May  2 11:35 vuser
drwx------. 2  1002  1002 62 May  3 22:34 wsuser
[root@Centos7Teach home]# cd /var/mail/
[root@Centos7Teach mail]# ls -l
total 208
-rw-rw----. 1 user1 mail      0 May  3 11:32 ftpuser
-rw-------. 1 root  mail 207089 May 16 03:18 root
-rw-rw----. 1 rpc   mail      0 Mar 13 23:04 rpc
-rw-rw----. 1 user1 mail      0 May 10 20:29 snort
-rw-rw----. 1 user3 mail      0 May  3 22:33 tsuser
-rw-rw----. 1 user1 mail      0 May 16 14:15 user1
-rw-rw----. 1 user2 mail      0 May 16 14:15 user2
-rw-rw----. 1 user3 mail      0 May 16 14:16 user3
-rw-rw----. 1 user1 mail      0 May  2 11:35 vuser
-rw-rw----. 1  1002 mail      0 May  3 22:34 wsuser
[root@Centos7Teach mail]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 36,27 1 会话 CAP NUM

2.权限管理

修改用户口令

【功能】

passwd 命令用于设置用户的认证信息，包括用户名密码、密码过期时间等。只有管理者可以指定用户名称，一般用户只能变更自己的密码。

【语法】

```
# passwd [选项] [用户名]
```

【选项说明】

passwd 命令选项及其说明如表 11-17 所示。

表 11-17 passwd 命令选项及其说明

选项	说明
-k 或--keep-tokens	保留即将过期的用户在期满后人能使用
-d 或--delete	删除用户密码，仅能通过 root 权限操作
-l 或--lock	锁住用户无权更改其密码，仅 root 权限操作
-u 或--unlock	解除用户锁定
-e 或--expire	终止对某用户进行密码更改，仅 root 权限操作
-f 或--force	强制操作，仅 root 权限操作
-x 或--maximum=DAYS	两次密码修改的最大天数，仅 root 权限操作
-n 或--minimum=DAYS	两次修改密码的最小天数，仅 root 权限操作
-w 或--warning=DAYS	在距多少天提醒用户修改密码，仅 root 权限操作
-i 或--inactive=DAYS	在密码过期后多少天，用户被禁用掉，仅 root 权限操作
-S 或--status	查询用户的密码状态，仅 root 权限操作
--stdin	用于批量修改用户密码操作，仅 root 权限操作
-?或--help	显示 passwd 命令帮助信息
--usage	显示简短使用信息

2.权限管理

- 修改用户信息

【语法】

```
# usermod [选项] [用户名]
```

【选项说明】

usermod 命令选项及其说明如表 11-18 所示。

表 11-18 usermod 命令选项及其说明

选项	说明
-c 或--comment COMMENT	修改用户账号的备注文字
-d 或--home HOME_DIR	修改用户登录时的目录
-e 或--expiredate EXPIRE_DATE	修改账号的有效期限
-f 或--inactive INACTIVE	修改在密码过期后多少天即关闭账号
-g 或--gid GROUP	修改用户所属的用户组
-G 或--groups GROUPS	修改用户所属的附加用户组
-a 或--append	修改用户追缴到附加组
-h 或--help	显示 usermod 命令帮助信息
-l 或--login NEW_LOGIN	修改登录用户账号名称
-L 或--lock	锁定用户密码，使密码无效
-m 或--move-home	将用户主目录的内容移动到新位置
-o 或--non-unique	允许修改具有重复 UID（非唯一）的用户
-p 或--password PASSWORD	为新用户修改加密密码
-R 或--root CHROOT_DIR	指定用户的 CHROOT 目录
-s 或--shell SHELL	指定用户登入后所使用的 shell
-u 或--uid UID	指定用的 UID 值
-U 或--unlock	指定为该用户创建一个与用户名称相同的用户组
-Z 或--selinux-user SEUSER	使用一个特定的 seuser 的 SELinux 用户映射

2.权限管

- 修改用户

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# usermod -G user1 user3
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# usermod -s /sbin/nologin user3
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# usermod -L user1,user2
usermod: user 'user1,user2' does not exist
[root@Centos7Teach ~]# usermod -L user1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# usermod -U user1
usermod: unlocking the user's password would result in a passwordless account.
You should set a password with usermod -p to unlock this user's password.
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/sys
tematic
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@Centos7Teach ~]# usermod -L user1
[root@Centos7Teach ~]# usermod -U user1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 26,24 1 会话 CAP NUM

2.权限管理

删除用户：userdel

【功能】

userdel 命令用户删除指定的用户，以及与用户相关的文件，如不加选项，则仅删除用户账号，而不删除相关文件。

【语法】

```
# userdel [选项] [用户名]
```

【选项说明】

userdel 命令选项及其说明如表 11-19 所示。

表 11-19 userdel 命令选项及其说明

选项	说明
-f 或--force	强制删除用户，即使用户当前已登录
-h 或--help	显示 userdel 帮助命令
-r 或--remove	删除用户的同时，删除与用户相关的所有文件
-R 或--root CHROOT_DIR	指定用户的 CHROOT 目录
-Z 或--selinux-user	移除 SELinux 用户映射

2.权限管

- 删除用户

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# userdel user1
userdel: group user1 not removed because it has other members.
[root@Centos7Teach ~]# userdel -r user2
userdel: group user2 is the primary group of another user and is not removed.
[root@Centos7Teach ~]# userdel -r user3
[root@Centos7Teach ~]# tree /home
/home
|-- ftpuser
|-- tsuser
|-- user1
|-- vuser
`-- wsuser

5 directories. 0 files



[root@Centos7Teach ~]# tree /var/mail/
/var/mail/
|-- ftpuser
|-- root
|-- rpc
|-- snort
|-- tsuser
|-- user1
|-- vuser
`-- wsuser

0 directories, 8 files
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 31,24 1 会话 CAP NUM

2.权限管理

- 用户组管理常用命令

表 11-20 用户管理命令一览表

命令	说明
groupadd	添加用户组
groupdel	删除用户组
groupmod	修改用户组信息
groups	显示用户所属的用户组信息
grpck	检查用户组及密码文件的完整性（/etc/group 和/etc/gshadow）
grpconv	开启用户组的投影密码。将用户组密码从/etc/group 同步到/etc/gshadow。如果/etc/gshadow 不存在则创建
grpunconv	执行 grpunconv 指令可以关闭用户组投影密码，它会把密码从 gshadow 文件内，重回存到 group 文件里，并删除 gshadow 文件

2.权限管理

创建用户组：groupadd

【功能】

groupadd 命令用于创建一个新的用户组，新用户组的信息将被添加到系统文件中。groupadd 命令可指定用户名称来建立新的用户组账号，需要时可从系统中取的新用户组值，在创建用户组时建议尽量简单，直接使用用户组名称就可以。

【语法】

```
# groupadd [选项] [组名]
```

【选项说明】

groupadd 命令选项及其说明如表 11-21 所示。

表 11-21 groupadd 命令选项及其说明

选项	说明
-f 或--force	强制执行，使用此参数可以创建相同 ID 的用户组，与-o 操作不相同
-g 或--gid GID	为创建的用户组指定 ID 号
-h 或--help	显示 groupadd 命令帮助信息
-K 或--key KEY=VALUE	覆盖/etc/login.defs 默认的用户组添加规则值
-o 或--non-unique	允许设置相同组 ID 的用户组
-p 或--password PASSWORD	为新用户组创建加密密码
-r 或--system	指定创建系统用户组
-R 或--root CHROOT_DIR	指定用户组的 CHROOT 目录

2.权限管

- 创建用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# groupadd usergroup1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# tail /etc/group
arpwatch:x:77:
tcpdump:x:72:
apache:x:48:
mysql:x:27:
webalizer:x:996:
rpcuser:x:29:
cgred:x:995:
user1:x:1000:
user2:x:1001:
usergroup1:x:1002:
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 15,24 1 会话 CAP NUM

2.权限管理

- 修改用户组：groupmod

【功能】

groupmod 命令用于修改用户组的基本信息。

【语法】

```
# groupmod [选项] [组名]
```

【选项说明】

groupmod 命令选项及其说明如表 11-22 所示。

表 11-22 groupmod 命令选项及其说明

选项	说明
-g 或--gid GID	更改用户组的 GID 值，如无其他选项指定 GID 在系统中唯一
--h 或--help	显示 groupmod 命令帮助信息
-n 或--new-name NEW_GROUP	修改用户组名称，如无其他选项指定 Name 在系统中唯一
-o 或--non-unique	修改用户组的 GID 可与其他用户组具有相同的 GID
-p 或--password PASSWORD	为新用户组创建加密密码
-R 或--root CHROOT_DIR	指定用户组的 CHROOT 目录

2.权限管

- 修改用户

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# groupadd usergroup1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# tail /etc/group
arpwatch:x:77:
tcpdump:x:72:
apache:x:48:
mysql:x:27:
webalizer:x:996:
rpcuser:x:29:
cgred:x:995:
user1:x:1000:
user2:x:1001:
usergroup1:x:1002:
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# groupmod -p usergroup1pwd usergroup1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# tail /etc/group
arpwatch:x:77:
tcpdump:x:72:
apache:x:48:
mysql:x:27:
webalizer:x:996:
rpcuser:x:29:
cgred:x:995:
user1:x:1000:
user2:x:1001:
usergroup1:x:1002:
[root@Centos7Teach ~]# tail /etc/gshadow
arpwatch:!::
tcpdump:!::
apache:!::
mysql:!::
webalizer:!::
rpcuser:!::
cgred:!::
user1:!::
user2:!::
usergroup1:usergroup1pwd::
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 39,24 1 会话 CAP NUM

2.权限管理

用户组管理：gpasswd

【功能】

gpasswd 命令是 Linux 下用户组/etc/group 和/etc/gshadow 的管理工具，可以对该组内的用户进行相应的管理。

【语法】

```
# gpasswd [选项] [组名]
```

【选项说明】

gpasswd 命令选项及其说明如表 11-23 所示。

表 11-23 gpasswd 命令选项及其说明

选项	说明
-a 或--add USER	添加用户到用户组
-d 或--delete USER	从用户组中删除用户
-h 或--help	显示 gpasswd 命令帮助信息
-Q 或--root CHROOT_DIR	指定用户组的 CHROOT 目录
-r 或--remove-password	删除用户组密码
-R 或--restrict	限制用户登入用户组，只有组中人员才可以用 newgrp 加入该组
-M 或--members USER,...	指定组成员
-A 或--administrators ADMIN,...	指定组内管理员

2.权限管

- 用户组管

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# tail /etc/passwd
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
arpwatch:x:77:77::/var/lib/arpwatch:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
webalizer:x:67:996:Webalizer:/var/www/usage:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
user1:x:1000:1000::/home/user1:/bin/bash
user2:x:1001:1001::/home/user2:/bin/bash
user3:x:1002:1003::/home/user3:/bin/bash
[root@Centos7Teach ~]# gpasswd -a user1 usergroup1
Adding user user1 to group usergroup1
[root@Centos7Teach ~]# gpasswd -a user2 usergroup1
Adding user user2 to group usergroup1
[root@Centos7Teach ~]# gpasswd -a user3 usergroup1
Adding user user3 to group usergroup1
[root@Centos7Teach ~]# tail /etc/passwd
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
arpwatch:x:77:77::/var/lib/arpwatch:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
webalizer:x:67:996:Webalizer:/var/www/usage:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
user1:x:1000:1000::/home/user1:/bin/bash
user2:x:1001:1001::/home/user2:/bin/bash
user3:x:1002:1003::/home/user3:/bin/bash
[root@Centos7Teach ~]# tail -n 5 /etc/group
cgred:x:995:
user1:x:1000:
user2:x:1001:
usergroup1:x:1002:user1,user2,user3
user3:x:1003:
[root@Centos7Teach ~]# gpasswd -d user1 usergroup1
Removing user user1 from group usergroup1
[root@Centos7Teach ~]# gpasswd -d user2 usergroup1
Removing user user2 from group usergroup1
[root@Centos7Teach ~]# gpasswd -d user3 usergroup1
Removing user user3 from group usergroup1
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

2.权限管理

- 删除用户组：groupdel

【功能】

groupdel 命令用于删除指定的用户组，本命令要修改/etc/group 和/etc/gshadow 两个系统文件。若该用户组中仍包含某些用户，则必须先删除这些用户后，方能删除用户组。

【语法】

```
# groupdel [组名]
```

2.权限管

- 删除用户组

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# userdel -r user1
[root@Centos7Teach ~]# userdel -r user2
[root@Centos7Teach ~]# userdel -r user3
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# groupdel usergroup1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# tail /etc/passwd
polkitd:x:999:997:User for polkitd:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
arpwatch:x:77:77::/var/lib/arpwatch:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
webalizer:x:67:996:Webalizer:/var/www/usage:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# tail /etc/group
postfix:x:89:
sshd:x:74:
rpc:x:32:
arpwatch:x:77:
tcpdump:x:72:
apache:x:48:
mysql:x:27:
webalizer:x:996:
rpcuser:x:29:
cgred:x:995:
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 30,24 1 会话 CAP NUM

2.权限管理

- 用户与用户组授权
  - 常用3种命令对系统中的文件/目录进行用户或用户组授权，分别是：chown、chgrp、chmod。
    - chown：该命令改变某个文件或目录的所有者和所属的组，该命令可以向某个用户授权，使该用户变成指定文件的所有者或者改变文件所属的组。
    - chgrp：该命令用来改变文件或目录所属的用户组。组名可以是用户组ID，文件名可以是由空格分开的要改变属组的文件列表，也可以是由通配符描述的文件集合。
    - chmod：该命令用来改变文件或目录的权限。文件或目录权限的控制分别以读取、写入、执行3种一般权限来区分，另有3种特殊权限可供运用。可使用chmod命令改变文件与目录的权限，设置方式采用文字或数字代号均可。
    - 第2章已经讲解过授权命令，具体内容参考第2章相关部分。

2.权限管理

- PAM简介
  - Linux-PAM（Pluggable Authentication Modules for Linux）可插拔认证模块。
  - Linux-PAM是一套适用于Linux的身份验证共享库系统，它为系统中的应用程序或服务提供动态身份验证模块支持。
  - 在Linux中，PAM是可动态配置的，本地系统管理员可以自由选择应用程序。
  - PAM应用在许多程序与服务上，比如登录程序（login、su）的PAM身份验证（口令认证、限制登录）、passwd强制密码、用户进程实时管理、向用户分配系统资源等。

2.权限管理

- PAM简介
  - PAM的主要特征是认证的性质是可动态配置的。
  - PAM的核心部分是库（libpam）和PAM模块的集合，它们是位于文件夹/lib/security中的动态链接库（.so）文件，以及位于/etc/pam.d/目录中（或者是/etc/pam.conf配置文件）的各个PAM模块配置文件。
  - /etc/pam.d/目录中定义了各种程序和服务的PAM配置文件，其中system-auth文件是PAM模块的重要配置文件，它主要负责用户登录系统的身份认证工作，不仅如此，其他的应用程序或服务可通过include接口来调用它（该文件是system-auth-ac的软链接）。此外password-auth配置文件也是与身份验证相关的重要配置文件，比如用户的远程登录验证（SSH登录）就是通过它调用。
  - 在Ubuntu、SUSE Linux等发行版中，PAM主要配置文件是common-auth、common-account、common-password、common-session这四个文件，所有的应用程序和服务的主要PAM配置都可以通过它们来调用。

2.权限管

安全身份验证模块

- PAM简介

Teach-CentOS 7 - root@Centos7Teach:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach /]# ldd /usr/bin/htpasswd | grep libpam
[root@Centos7Teach /]#
[root@Centos7Teach /]# ldd /usr/bin/ssh | grep libpam
[root@Centos7Teach /]#
[root@Centos7Teach /]# ldd /usr/bin/passwd | grep libpam
        libpam.so.0 => /lib64/libpam.so.0 (0x00007f832a171000)
        libpam_misc.so.0 => /lib64/libpam_misc.so.0 (0x00007f8329f6c000)
[root@Centos7Teach /]#
[root@Centos7Teach /]#ldd /usr/bin/login | grep pam
        libpam.so.0 => /lib64/libpam.so.0 (0x00007f81eeb4a000)
        libpam_misc.so.0 => /lib64/libpam_misc.so.0 (0x00007f81ee946000)
[root@Centos7Teach /]#
[root@Centos7Teach /]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 13,24 1 会话 CAP NUM

2.权限管理

- PAM简介
  - /etc/pam.d/目录中包含应用程序的PAM配置文件，例如，login程序将其程序/服务名称定义为login，与之对应的PAM配置文件为/etc/pam.d/login。
  - 每个配置文件都包含一组指令，用于定义模块以及控制标志和参数。每条指令都有一个简单的语法，用于标识模块的目的（接口）和模块的配置设置。
  - 语法格式如下所示。
    - module_interface　control_flag　module_name　module_arguments

2.权限管理

- PAM语法格式。
  - module_interface control_flag module_name module_arguments
  - PAM语法格式分成四个部分：模块接口、控制标志、模块名称、传递参数。
    - 模块接口也可称为模块管理组，PAM为认证任务提供四种类型可用的模块接口，它们分别提供不同的认证服务。
    - 控制标志是实现用户在对某一个特定的应用程序或服务身份验证的具体实现细节。所有的PAM模块被调用时都会返回成功或者失败的结果，每个PAM模块中由多个对应的控制标志决定结果是否通过或失败。每个控制标志对应一个处理结果，PAM库将这些通过/失败的结果整合为一个整体的通过/失败结果，然后将结果返回给应用程序。
    - 模块名称也包含模块对应程序文件的路径，如果没有给出路径，单独一个模块名称，则说明该模块默认在目录/usr/lib/security中。
    - 传递参数用来传递该模块的参数，一般来说每个模块的参数都不相同，可以由该模块的开发者自定义，但是也有几个共同的参数。

2.权限管理

- PAM语法格式

表 11-24 PAM 模块接口

接口名称	说明
auth	认证模块接口。如验证用户身份、检查密码是否可以通过并设置用户凭据
account	账户模块接口。检查指定账户是否满足当前验证条件，如用户是否有权访问所请求的服务、检查用户是否到期
password	密码模块接口。用户更改用户密码，以及强制使用强密码配置
session	会话模块接口。用于管理和配置用户会话，在用户成功认证之后启动生效

表 11-25 PAM 控制标志

选项	说明
required	模块测试必须成功才能继续认证，如果在此处测试失败，则继续测试引用在该模块接口下一个模块，直到所有的模块测试完成，才将结果通知给用户
requisite	模块结果必须成功才能继续认证，如果在此处测试失败，则会立即将失败结果通知给用户
sufficient	模块结果如果测试失败，将被忽略。如果 sufficient 模块测试成功，并且之前的 required 模块没有发生故障，PAM 会向应用程序返回通过的结果，不会再调用堆栈中其他模块
optional	该模块返回的通过/失败结果将被忽略。当没有其他模块被引用时，标记为 optional 模块并且成功验证时该模块才是必须的。该模块被调用来执行一些操作，并不影响模块堆栈的结果
include	与其他控制标志不同，include 与模块结果的处理方式无关。该标志用于直接引用其他 PAM 模块的配置参数

表 11-26 PAM 中常见的参数

参数	说明
debug	表明该模块应当用 syslog()函数将调试信息写入到系统日志文件中
no_warn	表明该模块不应把警告信息发送给应用程序
use_first_pass	表明该模块不能提示用户输入密码，应使用前一个模块从用户那里得到的密码
try_first_pass	表明该模块应首先使用前一个模块从用户那里得到的密码，如果该密码验证不通过，再提示用户输入新的密码
use_mapped_pass	表明该模块不能提示用户输入密码，而是使用映射过的密码
expose_account	表明该模块显示用户的账号名等信息，一般只能在安全的环境下使用，因为泄漏用户名会对安全造成一定程度的威胁

2.权限管理

- PAM常用模块

表 11-27 PAM 常用模块介绍

PAM 模块	接口管理类型	说明
pam_unix.so	auth	提示用户输入密码，并与/etc/shadow 文件相比对，匹配返回结果 0
	account	检测用户的账号信息（包括是否过期等），账号可用时，返回结果 0
	password	修改用户的密码，将用户输入的密码，作为用户的新密码更新 shadow 文件
pam_shells.so	auth	如果用户想登录系统，那么它的 shell 必须是在/etc/shells 文件中之一的 shell
	account	
pam_deny.so	auth	该模块可用于拒绝访问
	account	
	password	
	session	
pam_permit.so	auth	该模块任何时候都返回成功
	account	
	password	
	session	
pam_securetty.so	auth	如果用户要以 root 登录时，则登录的 tty 必须在/etc/securentty 之中
pam_listfile.so	auth	访问应用程序的控制开关
	account	
	password	
	session	
pam_cracklib.so	password	这个模块可以插入到一个程序的密码栈中，用于检查密码的强度
pam_limits.so	session	定义使用系统资源的上限，root 用户也会受此限制，可以通过 /etc/security/limits.conf 或/etc/security/limits.d/*.conf 来设定

2.权限管理

PAM案例：强制使用强密码

【配置文件】

在 Linux 中强制用户使用强密码，其配置文件及其路径为“/etc/pam.d/system-auth-ac”。

【模块与参数】

使用模块：pam_cracklib。该模块仅适用于 password 模块接口，主要用于在用户密码配置时的验证，该模块中常用的参数及其配置说明，如表 11-28 所示。

表 11-28 pam_cracklib 模块参数配置

参数	说明
minlen=N	密码字符长度不少于 N 位（默认为 9）
lcredit=-N	至少包含 N 个小写字母
ucredit=-N	至少包含 N 个大写字母
dcredit=-N	至少包含 N 个数字
ocredit=-N	至少包含 N 个特殊字符
retry=N	配置密码时，提示 N 次用户密码错误输入
difok=N	配置密码时，新密码至少 N 个字符与旧密码不同（默认为 5）
reject_username	新密码中不能包含与用户名称相同的字段
maxrepeat=N	拒绝包含超过 N 个连续字符的密码，默认值为 0 表示此检查已禁用
maxsequence=N	拒绝包含大于 N 的单调字符序列的密码，例如“1234”或“fedcb”，默认情况下即使没有这个参数配置，一般大多数这样的密码都不会通过，除非序列只是密码的一小部分
maxclassrepeat=N	拒绝包含相同类别的 N 个以上连续字符的密码。默认为 0 表示此检查已禁用
use_authtok	强制使用先前的密码，不提示用户输入新密码（不允许用户修改密码）

2.权限管

安全身份验证模块

- PAM案例

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# rpm -qa | grep cracklib
cracklib-2.9.0-11.el7.x86_64
cracklib-dicts-2.9.0-11.el7.x86_64
[root@Centos7Teach ~]# tree /etc/pam.d/
/etc/pam.d/
|-- atd
|-- chfn
|-- chsh
|-- config-util
|-- crond
|-- fingerprint-auth -> fingerprint-auth-ac
|-- fingerprint-auth-ac
|-- login
|-- other
|-- passwd
|-- password-auth -> password-auth-ac
|-- password-auth-ac
|-- polkit-1
|-- postlogin -> postlogin-ac
|-- postlogin-ac
|-- remote
|-- runuser
|-- runuser-l
|-- smartcard-auth -> smartcard-auth-ac
|-- smartcard-auth-ac
|-- smtp -> /etc/alternatives/mta-pam
|-- smtp.postfix
|-- sshd
|-- su
|-- su-l
|-- sudo
|-- sudo-i
|-- system-auth -> system-auth-ac
|-- system-auth-ac
|-- systemd-user
|-- vmtoolsd
|-- vsftpd.bak
|-- vsftpd.rpmsave
`-- vsftpdr
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

2.权限管

安全身份验证模块

- PAM案例

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/pam.d/passwd
#%PAM-1.0
auth        include      system-auth
account     include      system-auth
password    substack     system-auth
-password    optional    pam_gnome_keyring.so use_authtok
password    substack     postlogin
password    required      pam_cracklib.so minlen=15 lcredit=-1 ucredit=-1 ocredi
t=-1 dcredit=-1 difok=6
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# passwd user1
Changing password for user user1.
New password:
Retype new password:
BAD PASSWORD: is too simple
Retype new password:
Sorry, passwords do not match.
passwd: Failed preliminary check by password service
[root@Centos7Teach ~]# passwd user1
Changing password for user user1.
New password:
Retype new password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

minlen=12	最少12个字符
lcredit=-1	最少1个小写字母
ucredit=-1	最少1个大写字母
ocredit=-1	最少1个数字
dcredit=-1	最少1个特殊字符
difok=6	新密码和原有密码至少6个字符不相同

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 26,24 1 会话 CAP NUM

2.权限管理

PAM案例：多次失败登陆自动锁定

【配置文件】

在 Linux 中限制用户登录失败次数，其配置文件及其路径为“/etc/pam.d/sshd（或者/etc/pam.d/password-auth-ac）”。

【模块与参数】

使用“pam_tally2”模块可适用于 auth 模块接口，主要用于用户登录时的验证，该模块中常用的参数及其配置说明，如表 11-30 所示。

表 11-30 pam_tally2 模块参数配置

参数	参数说明	说明
onerr=[succeed|fail]	全局选项	配置该条参数是否执行
file=/path/to/log		失败登录日志文件，默认为/var/log/tallylog
audit		如果登录的用户没有找到，则将用户名信息记录到系统日志中
silent		不打印相关的信息
no_log_info		不通过 syslog 记录日志信息
deny=n	auth 选项	失败登录次数超过 n 次后拒绝访问
lock_time=n		失败登录后锁定的时间（秒数）
unlock_time=n		超出失败登录次数限制后，解锁的时间
no_lock_time		不在日志文件/var/log/faillog 中记录 fail_locktime 字段
magic_root		root 用户(uid=0)调用该模块时，计数器不会递增
even_deny_root		root 用户失败登录次数超过 deny=n 次后拒绝访问
root_unlock_time=n		与 even_deny_root 相对应的选项，如果配置该选项，则 root 用户在登录失败次数超出限制后被锁定指定时间

2.权限管

安全身份验证模块

- PAM案例

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
auth        required      pam_tally2.so  deny=3 unlock_time=120 file/var/log/tal
lylog

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
account     required      pam_tally2.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry
=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_au
thtok


password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet
use_uid
session     required      pam_unix.so
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# pam_tally2 --user=zhangsan
Login           Failures Latest failure     From
zhangsan            5    05/16/18 23:25:22  10.10.0.1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 38,24 1 会话 CAP NUM

2.权

验证模块

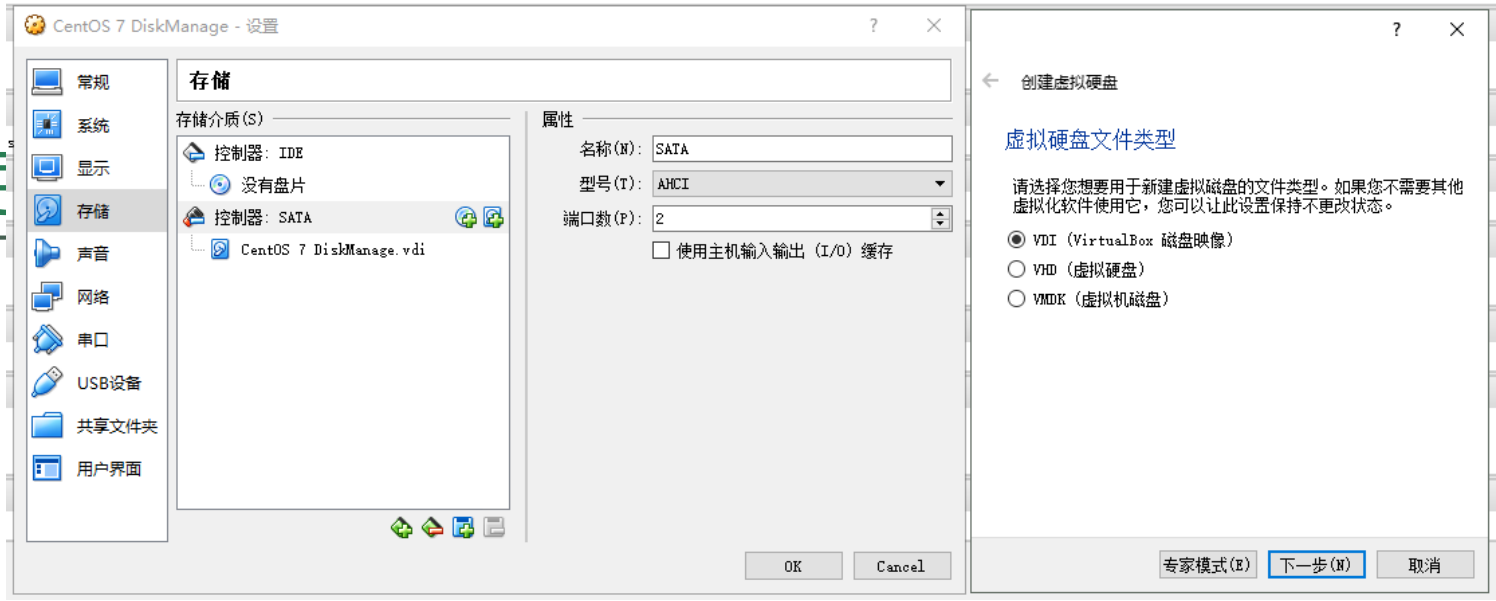
- PAM

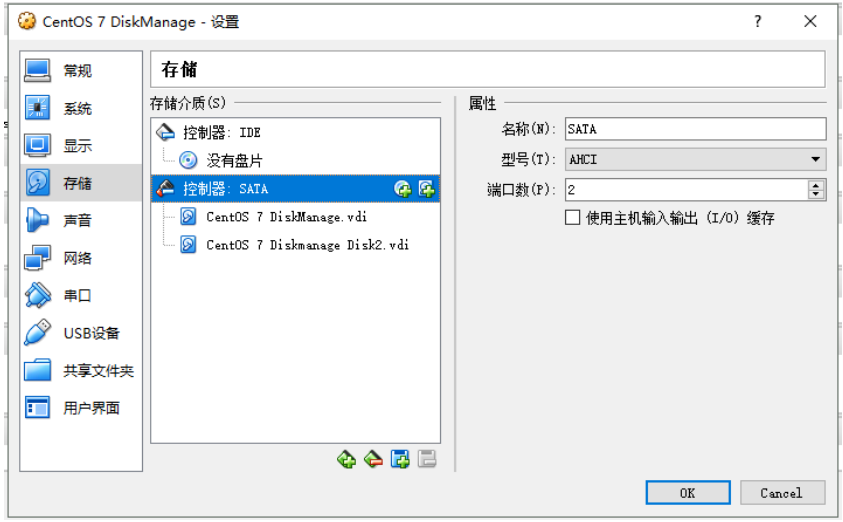
```
zhangsan@Centos7Teach:~
login as: zhangsan
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
login as: zhangsan
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
login as: zhangsan
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Access denied
zhangsan@211.69.35.213's password:
Account locked due to 4 failed logins
Account locked due to 5 failed logins
Last failed login: Wed May 16 23:25:24 CST 2018 from 10.10.0.1 on ssh:notty
There were 12 failed login attempts since the last successful login.
Last login: Wed May 16 23:19:34 2018 from 10.10.0.1
[zhangsan@Centos7Teach ~]$
```

3.存储管理

- 在Linux系统上增加新硬盘的操作有四个步骤：
  - 完成新增硬盘的操作
    - 在物理服务商增加一块物理硬盘
    - 在虚拟主机上增加一块虚拟磁盘
  - 查看新增磁盘的信息
  - 磁盘分区与格式化
  - 磁盘挂载

3.在 加硬盘


CentOS 7 DiskManage - 设置
常规
系统
显示
存储
声音
网络
串口
USB设备
共享文件夹
用户界面
存储
存储介质(S)
控制器: IDE
没有盘片
控制器: SATA
CentOS 7 DiskManage.vdi
属性
名称(N): SATA
型号(T): AHCI
端口数(P): 2
使用主机输入输出 (I/O) 缓存
OK
Cancel
创建虚拟硬盘
虚拟硬盘文件类型
请选择您想要用于新建虚拟磁盘的文件类型。如果您不需要其他虚拟化软件使用它，您可以让此设置保持不更改状态。
VDI (VirtualBox 磁盘映像)
VHD (虚拟硬盘)
VMDK (虚拟机磁盘)
专家模式(E)
下一步(N)
取消


CentOS 7 DiskManage - 设置
常规
系统
显示
存储
声音
网络
串口
USB设备
共享文件夹
用户界面
存储
存储介质(S)
控制器: IDE
没有盘片
控制器: SATA
CentOS 7 DiskManage.vdi
CentOS 7 Diskmanage Disk2.vdi
属性
名称(N): SATA
型号(T): AHCI
端口数(P): 2
使用主机输入输出 (I/O) 缓存
OK
Cancel

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000eeb9c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    16777215     7339008   8e  Linux LVM

Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-root: 6652 MB, 6652166144 bytes, 12992512 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 859 MB, 859832320 bytes, 1679360 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@CentOS7Base ~]#
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 31,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x6f4417cf.

Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   g   create a new empty GPT partition table
   G   create an IRIX (SGI) partition table
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-41943039, default 41943039):
Using default value 41943039
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-41943039, default 41943039):
Using default value 41943039
Partition 1 of type Linux and of size 20 GiB is set

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@CentOS7Base ~]# mkfs.ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1310720 inodes, 5242624 blocks
262131 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2153775104
160 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

[root@CentOS7Base ~]#
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:/newdisk - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000eeb9c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    16777215     7339008   8e  Linux LVM

Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x22653f47

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048    41943039    20970496   83  Linux

Disk /dev/mapper/centos-root: 6652 MB, 6652166144 bytes, 12992512 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 859 MB, 859832320 bytes, 1679360 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@CentOS7Base ~]# mkdir /newdisk
[root@CentOS7Base ~]# mount /dev/sdb1 /newdisk
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# cd /newdisk
[root@CentOS7Base newdisk]# mkdir demofolder
[root@CentOS7Base newdisk]#
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,29 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:/ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base /]# vi /etc/fstab
[root@CentOS7Base /]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Fri Apr  6 18:04:16 2018
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /                       xfs     defaults        0 0
UUID=62e32dd3-d222-4ffc-901b-4a1ab5933ea0 /boot                   xfs     defaults        0 0
/dev/mapper/centos-swap swap                    swap    defaults        0 0
/dev/sdb1               /newdisk                ext4    defaults        0 0
[root@CentOS7Base /]#
[root@CentOS7Base /]#
```

第一列是设备地址。

第二列是默认挂载点。

第三列是文件类型，可以为任意文件类型或者auto，如果是auto则表示有mount来判断类型。

第四列是设备或者分区所需要的挂载选项。取值很多，如果是defaults则表示所有选项全部使用默认配置，包括rw, suid, dev, exec, auto, nouser, 和 async。

第五列是表示dump选项：dump工具通过这个选项位置上的数字来决定文件系统是否需要备份。如果是0，dump就会被忽略，事实上，大多数的dump设置都是0。

第六列是fsck选项：fsck命令通过检测该字段来决定文件系统通过什么顺序来扫描检查，根文件系统/对应该字段的值应该为1，其他文件系统应该为2。若文件系统无需在启动时扫描检查，则设置该字段为0。

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 16,23 1 会话 CAP NUM

3.存储管理

- RAID是Redundant Array of Inexpensive Disks的缩写，直译为“廉价冗余磁盘阵列”，也简称为“磁盘阵列”。
- 后来RAID中的字母I改为Independent，RAID就成了“独立冗余磁盘阵列”，但这只是名称的变化，实质性的内容并没有改变。
- RAID可以理解成一种使用磁盘驱动的方法，将一组磁盘驱动器用某种逻辑方式联系起来，作为一个逻辑磁盘驱动器来使用。

3.存储管理

表 11-33 不同的 RAID 级别

级别	描述
RAID 0	级别 0 只是数据带。在级别 0 中，数据被拆分到多于一个的驱动器，如果是更高的数据吞吐量。这是 RAID 的最快和最有效的形式。但是，这个级别中没有数据镜像，所以在阵列中任何磁盘的失败将引起所有数据的丢失。软件 RAID 是级别 0，它使多个硬盘看起来像一个磁盘，但是速度比任何单个磁盘快得多。因为驱动器被并行访问。软件 RAID 可以用 IDE 或 SCSI 控制器，也可以使用任何磁盘组合
RAID 1	级别 1 是完全硬盘镜像。在独立的磁盘上创建和支持数据两份拷贝。级别 1 阵列与一个驱动器相比，读速度快、写速度慢，但是如果任意一个驱动器错误，不会有数据丢失。这是最昂贵的 RAID 级别，因为每个磁盘需要第二个磁盘做它的镜像。这个级别提供最好的数据安全
RAID 2	级别 2 设想用于没有内嵌错误检测的驱动器。因为所有的 SCSI 驱动器支持内嵌错误检测，这个级别已过时，基本上没有用了。Linux 不使用这个级别
RAID 3	级别 3 是一个有奇偶校验磁盘的磁盘带。存储奇偶校验信息到一个独立的驱动器上，允许恢复任何单个驱动器上的错误。Linux 不支持这个级别
RAID 4	级别 4 是拥有一个奇偶校验磁盘的大块带。奇偶校验信息意味着任何一个磁盘失败数据都可以被恢复。级别 4 阵列的读性能非常好，写速度比较慢，因为奇偶校验数据必须每次更新
RAID 5	级别 5 与级别 4 相似，但是它将奇偶校验信息分布列到多个驱动器中。这样提高了磁盘写速度，它每兆字节的花费与级别 4 相同，提高了高水平数据保护下的高速随机性能，是使用最广泛的 RAID 系统。

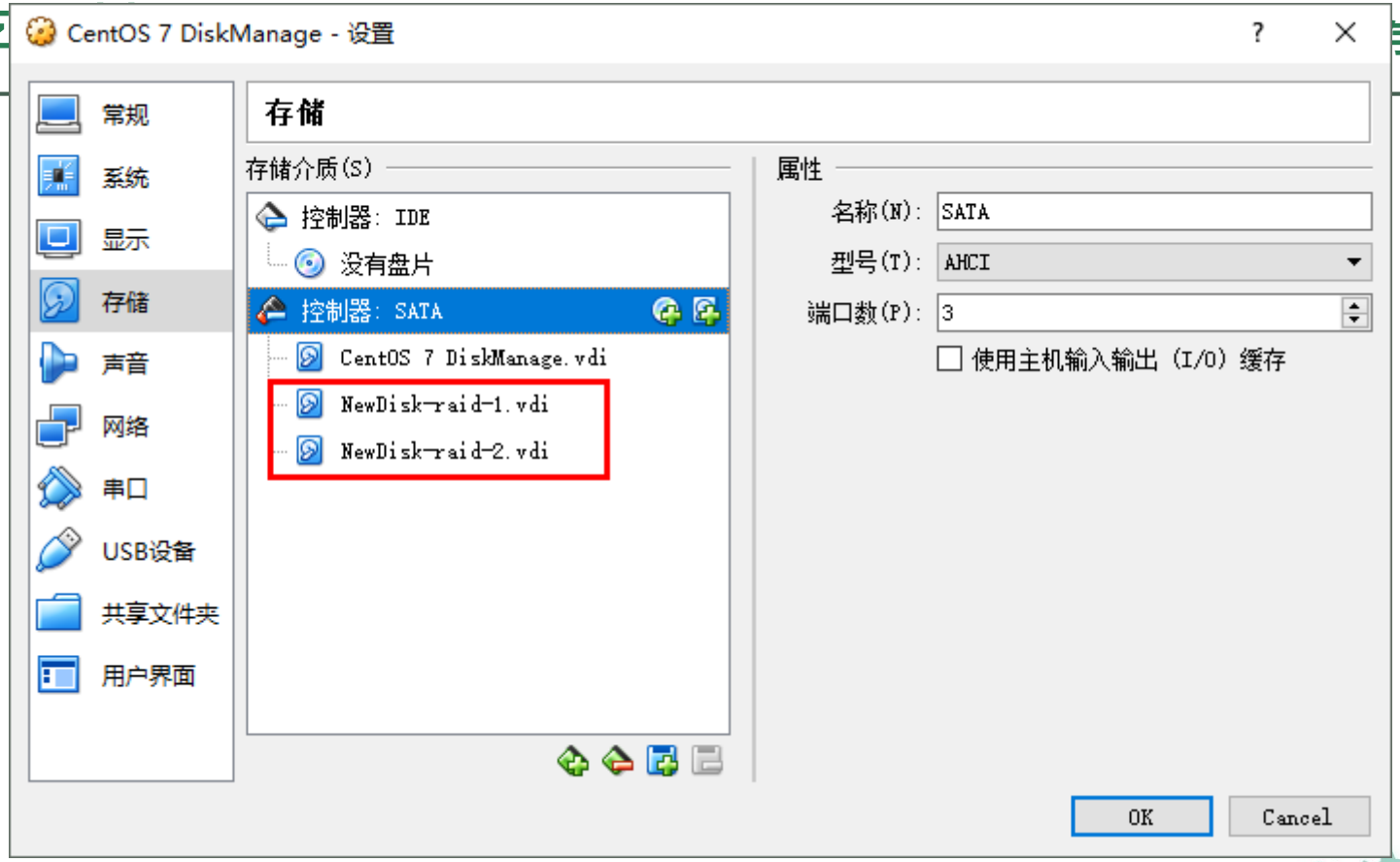
3.存储管理

- 软硬RAID对比
  - 因为硬盘本身始终是RAID实现里最突出的瓶颈，所以没有理由认为基于硬件实现的RAID一定会比基于软件或者基于操作系统的实现速度快。
  - 硬件RAID之所以在过去一直占优，主要有两个原因：缺乏替代它的软件，硬件能在某种非易失性存储器里实现写缓冲。
  - 写缓冲确实提供性能，因为它使得写操作似乎即刻就能完成。

3.存储管理

- 实例：Linux上配置软RAID
  - 在Linux上增加两块硬盘，用于实现RAID 1。
  - 创建磁盘阵列RAID 1。
  - 编辑阵列配置文件。
  - 创建文件系统。
  - 管理阵列存储服务。
  - 实现RAID管理。

3.存


CentOS 7 DiskManage - 设置
常规
系统
显示
存储
声音
网络
串口
USB设备
共享文件夹
用户界面
存储
存储介质(S)
控制器: IDE
没有盘片
控制器: SATA
CentOS 7 DiskManage.vdi
NewDisk-raid-1.vdi
NewDisk-raid-2.vdi
属性
名称(N): SATA
型号(T): AHCI
端口数(P): 3
使用主机输入输出 (I/O) 缓存
OK
Cancel

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000eeb9c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    16777215     7339008   8e  Linux LVM

Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sdc: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-root: 6652 MB, 6652166144 bytes, 12992512 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 859 MB, 859832320 bytes, 1679360 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@CentOS7Base ~]#
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 37,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000eeb9c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    16777215     7339008   8e  Linux LVM

Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x20db1d35

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048    41943039    20970496   83  Linux

Disk /dev/sdc: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2e3bbb03

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1            2048    41943039    20970496   83  Linux

Disk /dev/mapper/centos-root: 6652 MB, 6652166144 bytes, 12992512 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 859 MB, 859832320 bytes, 1679360 sectors
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# yum -y install mdadm
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.sjtu.edu.cn
 * extras: ftp.sjtu.edu.cn
 * updates: ftp.sjtu.edu.cn
Resolving Dependencies
--> Running transaction check
---> Package mdadm.x86_64 0:4.0-13.el7 will be installed
--> Processing Dependency: libreport-filesystem for package: mdadm-4.0-13.el7.x86_64
--> Running transaction check
---> Package libreport-filesystem.x86_64 0:2.1.11-40.el7.centos will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch          Version                  Repository   Size
================================================================================
Installing:
 mdadm                  x86_64        4.0-13.el7               base        431 k
Installing for dependencies:
 libreport-filesystem   x86_64        2.1.11-40.el7.centos     base         39 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 470 k
Installed size: 1.0 M
Downloading packages:
libreport-filesystem-2.1.11-40 FAILED
http://ftp.sjtu.edu.cn/centos/7.5.1804/os/x86_64/Packages/libreport-filesystem-2.1.11-40.el7.centos.x86_64.rpm: [Errno 1
4] curl#6 - "Could not resolve host: ftp.sjtu.edu.cn; Unknown error"
Trying other mirror.
mdadm-4.0-13.el7.x86_64.rpm    FAILED
http://ftp.sjtu.edu.cn/centos/7.5.1804/os/x86_64/Packages/mdadm-4.0-13.el7.x86_64.rpm: [Errno 14] curl#6 - "Could not re
solve host: ftp.sjtu.edu.cn; Unknown error"
Trying other mirror.
libreport-filesystem-2.1.11-40 FAILED
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

主机,IP地址或会话名称

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# mdadm -C /dev/md0 -ayes -l 1 -n 2 /dev/sd[b,c]1
mdadm: Note: this array has metadata at the start and
    may not be suitable as a boot device.  If you plan to
    store '/boot' on this device please ensure that
    your boot-loader understands md/v1.x metadata, or use
    --metadata=0.90
Continue creating array? y
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdc1[1] sdb1[0]
      20953088 blocks super 1.2 [2/2] [UU]
      [===>.................]  resync = 19.5% (4096768/20953088) finish=2.0min speed=136558K/sec

unused devices: <none>
[root@CentOS7Base ~]#
[root@CentOS7Base ~]#
```

mdadm参数说明：

-C --create 创建阵列。

-a --auto 同意创建设备，如不加此参数时必须先使用mknod命令来创建一个RAID设备，不过推荐使用-a yes参数一次性创建。

-l --level 阵列模式，支持的阵列模式有 linear, raid0, raid1, raid4, raid5, raid6, raid10, multipath, faulty, container。

-n --raid-devices 阵列中活动磁盘的数目，该数目加上备用磁盘的数目应该等于阵列中总的磁盘数目。

/dev/md0 阵列的设备名称。

/dev/sd[b,c]1 参与创建阵列的磁盘名称。

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 19,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
[root@CentOS7Base ~]# mdadm -D /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Thu May 17 23:50:55 2018
        Raid Level : raid1
        Array Size : 20953088 (19.98 GiB 21.46 GB)
     Used Dev Size : 20953088 (19.98 GiB 21.46 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Thu May 17 23:53:35 2018
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : CentOS7Base:0  (local to host CentOS7Base)
              UUID : a04ceb3b:d7e82c47:f663bf07:06fac39d
            Events : 17

    Number   Major   Minor   RaidDevice State
       0       8       17        0      active sync   /dev/sdb1
       1       8       33        1      active sync   /dev/sdc1
[root@CentOS7Base ~]#
[root@CentOS7Base ~]#
```

仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 29,23 1 会话 CAP NUM

192.168.10.101 - root@CentOS7Base:/newmddisk - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@192.168.10.101:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.10.101

```
       1       8       33        1      active sync   /dev/sdc1
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# echo DEVICE /dev/sd{b,c}1 >> /etc/mdadm.conf
[root@CentOS7Base ~]# mdadm -Evs >> /etc/mdadm.conf
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# mkfs.ext4 /dev/md0
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1310720 inodes, 5238272 blocks
261913 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2153775104
160 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

[root@CentOS7Base ~]# mkdir /newmddisk
[root@CentOS7Base ~]# mount /dev/md0 /newmddisk
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# echo "/dev/md0  /newmddisk  ext4  defaults  0 0" >> /etc/fstab
[root@CentOS7Base ~]#
[root@CentOS7Base ~]# cd /newmddisk
[root@CentOS7Base newmddisk]# mkdir folder1
[root@CentOS7Base newmddisk]# ls -l
total 20
drwxr-xr-x. 2 root root  4096 May 18 00:05 folder1
drwx------. 2 root root 16384 May 18 00:03 lost+found
[root@CentOS7Base newmddisk]#
```

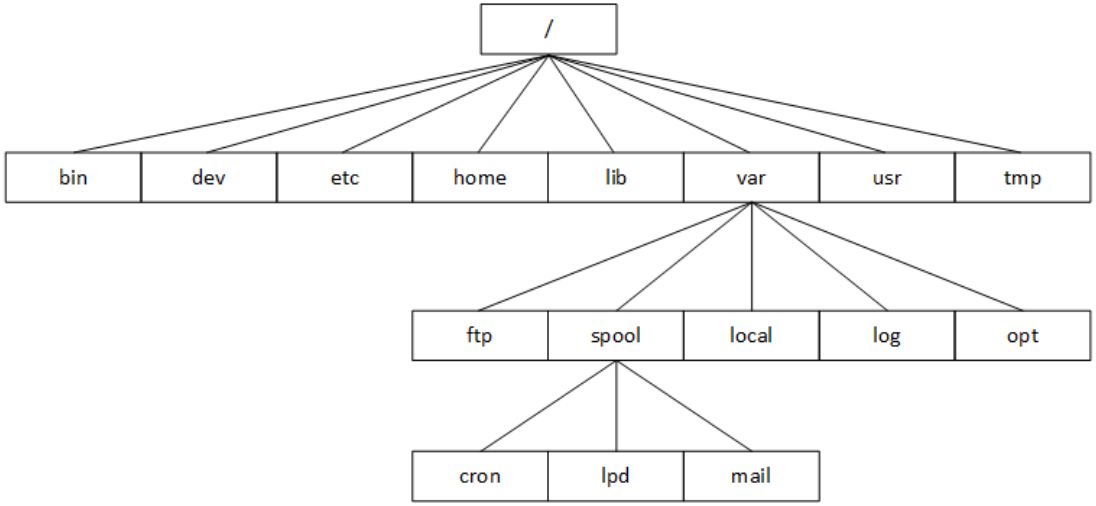
仅将文本发送到当前选项卡

ssh://root@192.168.10.101:22 SSH2 xterm 120x40 40,31 1 会话 CAP NUM

4.文件系统管理

- 在操作系统中，文件命令、存储和组织结构就称为文件系统（File System）。不同的操作系统对文件的组织方式会有所区别，其所支持的文件系统类型也会不一样。
  - 对于Linux操作系统，文件系统是指格式化后用于存储文件的设备（硬盘分区、光盘、软盘、闪盘及其他存储设备），其中包含有文件、目录以及定位和访问这些文件和目录所必须的信息。此外，文件系统还会对存储空间进行组织和分配，并对文件的访问进行保护和控制。这些文件和目录的命令、存储、组织和控制的总体结构就统称为文件系统。
  - 在Linux操作系统中，文件系统的组织方式是采用树状的层次式目录结构，在这个结构中处于最顶层的是根目录，用“/”代表，往下延伸就是其各级子目录。

4.文件系统管理


/
bin
dev
etc
home
lib
var
usr
tmp
ftp
spool
local
log
opt
cron
lpd
mail

4.文件系统管理

- Linux操作系统所能支持的文件系统类型很多，除了UNIX所能支持的各种常见文件系统类型外，还支持包括FAT16、FAT32、NTFS在内的各种Windows文件系统。
- Linux用户可以通过“加载”的方式把Windows操作系统的分区挂载到Linux的某个目录下进行访问。

4.文件系统管理

4.2文件系统类型

表 11-37 Linux 支持的文件系统类型

文件系统	说明
ext	第一个专门针对 Linux 的文件系统，为 Linux 的发展做出了重要贡献，但由于性能和兼容性上存在许多缺陷，现在已经很少使用
ext2	是为解决 ext 文件系统的缺陷而设计的高性能、可扩展的文件系统，在 1993 年发布，其特点是存取文件的性能好，在中小型的文件方面的优势尤其明显
ext3	日志文件系统，是 ext2 的升级版本，用户可以方便地从 ext2 文件系统迁移到 ext3 文件系统。ext3 在 ext2 的基础上加入了日志功能，即使系统因为故障导致宕机，ext3 文件系统也只需要数十秒中即可恢复，避免了意外宕机对数据的破坏
ext4	ext4 是 ext3 的改进版，修改了 ext3 中部分重要的数据结构，而不仅仅想 ext3 对 ext2 那样，只是增加了一个日志功能而已。ext4 提供了更佳的性能和可靠性，还有更为丰富的功能
swap	Swap 是 Linux 中一个专门用于交换分区的文件系统（类似与 Windows 上的虚拟内存）。Linux 使用这个分区作为交换空间。一般这个 swap 格式的交换分区是主内存的 2 倍。在内存不够时，Linux 会将部分数据写到交换分区上，当需要时在装进内存
NFS	NFS 是 Network File system 的缩写，即网络文件系统。有 SUN 公司于 1984 年开发并推出，可以支持不同的操作系统，实现不同系统间的文件共享，所以它的通信协议设计与主机及操作系统无关。用户可以通过 mount 命令把远程文件系统挂载在指定的目录下，像在本地一样对远程的文件进行操作
iso9660	CD-ROM 的标准文件系统，不仅能读取光盘和光盘 ISO 影像文件，而且还支持在 Linux 环境中刻录光盘
smb	支持 SMB 协议的网络文件系统，可用于实现 Linux 和 Windows 操作系统之间的文件共享
cifs	通用网际文件系统（CIFS）是微软服务器消息块协议（SMB）的增强版本，是计算机用户在企业内部和因特网上共享文件的标准方法
msdos	ms-dos 文件系统
umsdos	Linux 下扩展的 msdos 文件系统
vfat	这是一个与 Windows 系统兼容的 Linux 文件系统，可以作为 Windows 分区的 Linux 交换文件的文件系统类型
ntfs	Windows NT 所采用的独特文件系统结构
jsf	IBM 的 AIX 使用的日志文件系统，该文件系统是为面向事务的高性能系统而开发的
Xfs	有 SGI 开发的一个全 64 位、快速、安全的日志文件系统，用于 SGI 的 IRIX 操作系统，现在 SGI 已将文件系统的关键架构技术授权与 Linux
minix	是 Minix 操作系统使用的文件系统，也是 Linux 最初使用的文件系统
ramfs	内存文件系统，访问速度非常快
hpfs	IBM 的 LAN Server 和 OS/2 的文件系统
proc	是 Linux 操作系统中一种基于内存的伪文件系统
ufs	Sun Microsystem 操作系统（Solaris 和 SunOS）所用的文件系统
reiserfs	最早用于 Linux 的日志文件系统之一
hfs	苹果电脑所使用的文件系统
ncpfs	Novell NetWare 所使用的 NCP 协议的网络操作系统

4.文件系统管理

【功能】

fsck 命令能够修复因为非正常关机造成的文件系统损坏。

【语法】

```
# fsck [ -sAVRTNP] [-C [fd]] [-t fstype] [filesys…] [--] [ fd-specific-options]
```

【选项说明】

各选项说明如表 11-39 所示。

表 11-39 fsck 命令选项

命令选项	说明
-s	依次执行检查作业，而不是并行执行
-t fstype	知道检查的文件系统的类型
-A	检查/etc/fstab 中设置的所有文件系统
-C [fd]	显示检查任务的进度条
-N	不真正检查，只是显示会进行什么操作
-R	当使用-A 选项时，跳过对根文件系统的检测
-T	不显示标题
-V	限制指令执行过程
-a	不提示用户确认，自动修复文件系统
-n	不尝试修复文件系统，只把结果显示在标准输出中
-r	交互式修复文件系统（要求用户确认）
-y	自动尝试修复文件系统的任何错误

4.文件系

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# fdisk -l

Disk /dev/sda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000433e9

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200   125829119    61864960   8e  Linux LVM

Disk /dev/mapper/centos-root: 41.1 GB, 41120956416 bytes, 80314368 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 2147 MB, 2147483648 bytes, 4194304 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-home: 20.1 GB, 20073938944 bytes, 39206912 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@Centos7Teach ~]# fsck -y /dev/sda1
fsck from util-linux 2.23.2
/sbin/fsck.xfs: XFS file system.
[root@Centos7Teach ~]# fsck -y /dev/sda2
fsck from util-linux 2.23.2
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 36,24 1 会话 CAP NUM

5.进程管理

- Linux是一个多用户、多任务的操作系统。在这样的系统中，各种计算机资源（如文件、内存、CPU等）的分配和管理都以进程为单位。
- 为了协调多个进程对这些共享资源的访问，操作系统要跟踪所有进程的活动，以及它们对系统资源的使用情况从而实施对进程和资源的动态管理。
- 程序是存储在磁盘上包含可执行机器指令和数据的静态实体，而进程是在操作系统中执行的特定任务的动态实体。一个程序允许有多个进程，而每个运行中的程序至少由一个进程组成。

5.进程管理

- 作为一个多用户多任务操作系统，Linux每个进程与其他进程都是彼此独立的，都有自己独立的权限与职责。
  - 用户的应用程序不会干扰到其他用户的程序或操作系统本身。
  - 进程间有并列关系，还有父进程和子进程的关系。
  - 进程间的父子关系实际上是管理和被管理的关系。当父进程终止时，子进程也随之而终止。但子进程终止，父进程并不一定终止。

5.进程管理

- Linux操作系统包括如下3中不同类型的进程，每种进程都有其自己的特点和属性。
  - 交互进程：有Shell启动的进程。
    - 可在前台运行，也可以在后台运行。
  - 批处理进程：
    - 该进程和终端没有联系，是一个进程序列。
  - 守护进程：
    - Linux系统启动时的进程，并在后台运行。

5.进程管理

- 通常在操作系统中，进程至少要有3中基本状态，分别为：运行态、就绪态和封锁态（或阻塞态）。
  - 运行状态：
    - 指当前进程已分配到CPU，它的程序正在处理器上执行时的状态。处于这种状态的进程个数不能大于CPU的数目。
  - 就绪状态：
    - 指进程已具备运行条件，但因为其他进程正占用CPU，所以暂时不能运行而等待分配CPU的状态。一旦把CPU分给它，立即就可运行。
  - 封锁状态：
    - 指进程因等待某种事件发生（例如等待某一输入、输出操作完成，等到其他进程发来的信号等）而暂时不能运行的状态。也就是说，处于封锁状态的进程尚不具备运行条件，即使CPU空闲，它也无法使用。这种状态有时也称为不可运行状态或挂起状态。

5.进程管理

- Linux系统中，进程主要有以下几个状态。
  - 运行态（TASK_RUNNING）：
    - 此时进程正在运行（即系统的当前进程）或者准备运行（即就绪态）。
  - 等待态：
    - 此时进程在等待一个事件的发生或某种系统资源。Linux系统分为两种等待进程，分别为可中断的（TASK_INTERRUPTIBLE）和不可中断的（TASK_UNINTERRUPTIBLE）。可中断的等待进程可以被某一信号（Signal）中断；而不可中断的等待进程不受信号的打扰，将一直等待硬件状态的改变。
  - 停止态（TASK_STOPPED）：
    - 进程被停止，通常是通过接收一个信号。正在被调试的进程可能处于停止状态。
  - 僵死态（TASK_ZOMBIE）：
    - 由于某些原因被终止的进程，但是该进程的控制结构task_struct仍然保留着。

5.进程管理

- 查看进程：ps

【功能】

ps 命令是 Process Status 的缩写，它是 Linux 中查看进程信息最基本、最常用的命令。使用该命令可以确定有哪些进程正在运行和运行的状态、进程是否结束、进程有没有僵死、哪些进程占用了过多的资源等等，大部分信息都是可以通过执行该命令得到的。

【语法】

```
# ps [选项]
```

【选项说明】

ps 命令常用选项及其说明如表 11-48 所示。

表 11-48 ps 命令选项及其说明

选项	说明
-a	显示所有终端机下执行的程序，除了阶段作业领导者之外
a	显示现行终端机下的所有程序，包括其他用户的程序
-e	显示所有进程
-f	全格式输出
-h	不显示标题
-l	长格式输出
-w	宽格式输出
-A	显示所有进程，等同于-e 选项
-r	只显示正在运行的进程
-T	只显示当前终端中运行的进程
-x	显示没有控制终端的进程
k spec	按照-k 中设置的格式对输出结果进行排序。spec 的格式为：[+|-]key1[,[+|-]]key2[,...]。其中，key1、key2...为输出结果中的字段名；各字段间以逗号进行分隔；“+”表示升序，这时系统默认的；“-”表示降序

5.进程管

- 查看进程

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 May16 ?        00:00:02 /usr/lib/systemd/systemd --switc
root         2     0  0 May16 ?        00:00:00 [kthreadd]
root         3     2  0 May16 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 May16 ?        00:00:00 [kworker/0:0H]
root         7     2  0 May16 ?        00:00:00 [migration/0]
root         8     2  0 May16 ?        00:00:00 [rcu_bh]
root         9     2  0 May16 ?        00:00:00 [rcu_sched]
root        10     2  0 May16 ?        00:00:00 [watchdog/0]
root        11     2  0 May16 ?        00:00:00 [watchdog/1]
root        12     2  0 May16 ?        00:00:00 [migration/1]
root        13     2  0 May16 ?        00:00:00 [ksoftirqd/1]
root        15     2  0 May16 ?        00:00:00 [kworker/1:0H]
root        17     2  0 May16 ?        00:00:00 [kdevtmpfs]
root        18     2  0 May16 ?        00:00:00 [netns]
root        19     2  0 May16 ?        00:00:00 [khungtaskd]
root        20     2  0 May16 ?        00:00:00 [writeback]
root        21     2  0 May16 ?        00:00:00 [kintegrityd]
root        22     2  0 May16 ?        00:00:00 [bioset]
root        23     2  0 May16 ?        00:00:00 [kblockd]
root        24
root        28
root        29
root        30
root        31
root        39
root        40                                                  1]
root        41                                                  d]
root        42     2  0 May16 ?        00:00:00 [kpsmoused]
root        44     2  0 May16 ?        00:00:00 [ipv6_addrconf]
root        63     2  0 May16 ?        00:00:00 [deferwq]
root        97     2  0 May16 ?        00:00:00 [kauditd]
root       278     2  0 May16 ?        00:00:00 [mpt_poll_0]
root       279     2  0 May16 ?        00:00:00 [ata_sff]
root       280     2  0 May16 ?        00:00:00 [mpt/0]
root       287     2  0 May16 ?        00:00:00 [scsi_eh_0]
root       288     2  0 May16 ?        00:00:00 [scsi_tmf_0]
root       289     2  0 May16 ?        00:00:00 [scsi_eh_1]
root       290     2  0 May16 ?        00:00:00 [kworker/u4:2]
```

表 11-49 全格式输出结果说明

字段	说明	字段	说明
UID	运行进程用户	STIME	进程启动的时间
PID	进程的 ID	TTY	终端号
PPID	父进程 ID	TIME	进程使用的 CPU 时间
C	CPU 调度情况	CMD	启动进程的命令

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

5.进程管

- 查看进程

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# ps -ef | grep bash
root       788   784  0 May16 pts/0    00:00:00 -bash
root      1649   788  0 01:07 pts/0    00:00:00 grep --color=auto bash
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ps -T1
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:02 /usr/lib/systemd/systemd --switched-root --system --d
  788 pts/0    Ss     0:00 -bash
 1650 pts/0    R+     0:00 ps -T1
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ps -Af kuid,-pid
UID         PID  PPID  C STIME TTY          STAT   TIME CMD
root       1651   788  0 01:08 pts/0    R+     0:00 ps -Af kuid,-pid
root       1646     2  0 01:06 ?        S      0:00 [kworker/1:0]
root       1641     2  0 01:01 ?        S      0:00 [kworker/1:2]
root       1580     2  0 00:45 ?        S      0:00 [kworker/1:3]
root       1571     2  0 00:41 ?        S      0:00 [kworker/0:1]
root       1387     2  0 May16 ?        S      0:03 [kworker/0:0]
root        788   784  0 May16 pts/0    Ss     0:00 -bash
root        784   652  0 May16 ?        Ss     0:01 sshd: root@pts/0
root        775     1  0 May16 ?        Ss     0:00 /usr/libexec/postfix/master -
root        709     2  0 May16 ?        S<     0:00 [kworker/0:1H]
root        652     1  0 May16 ?        Ss     0:00 /usr/sbin/sshd -D
root        650     1  0 May16 ?        Ssl    0:01 /usr/bin/python -Es /usr/sbin
root        636     1  0 May16 ?        Ss     0:00 /usr/sbin/crond -n
root        633     1  0 May16 tty1     Ss+    0:00 /sbin/agetty --noclear tty1 l
root        631     1  0 May16 ?        Ss     0:00 /usr/sbin/atd -f
root        626     1  0 May16 ?        Ss     0:00 /usr/lib/systemd/systemd-logi
root        625     1  0 May16 ?        Ssl    0:00 /usr/sbin/NetworkManager --no
root        606     1  0 May16 ?        Ss     0:01 /usr/sbin/irqbalance --foregr
root        603     1  0 May16 ?        Ss     0:07 /usr/bin/vmtoolsd
root        602     1  0 May16 ?        Ssl    0:00 /usr/sbin/rsyslogd -n
root        597     1  0 May16 ?        Ss     0:00 /usr/bin/VGAuthService -s
root        574     1  0 May16 ?        S<sl   0:00 /sbin/auditd
root        569     2  0 May16 ?        S      0:00 [xfsaild/dm-2]
root        568     2  0 May16 ?        S<     0:00 [xfs-eofblocks/d]
root        567     2  0 May16 ?        S<     0:00 [xfs-log/dm-2]
root        566     2  0 May16 ?        S<     0:00 [xfs-reclaim/dm-]
root        565     2  0 May16 ?        S<     0:00 [xfs-cil/dm-2]
root        564     2  0 May16 ?        S<     0:00 [xfs-conv/dm-2]
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 80x40 40,24 1 会话 CAP NUM

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# ps -aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.1 128168  6732 ?        Ss   May16   0:02 /usr/lib/systemd/systemd --switched-root --system --des
root          2  0.0  0.0      0     0 ?        S    May16   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    May16   0:00 [ksoftirq
root          5  0.0  0.0      0     0 ?        S<   May16   0:00 [kworker/
root          7  0.0  0.0      0     0 ?        S    May16   0:00 [migratio
root          8  0.0  0.0      0     0 ?        S    May16   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    May16   0:00 [rcu_sche
root         10  0.0  0.0      0     0 ?        S    May16   0:00 [watchdog
root         11  0.0  0.0      0     0 ?        S    May16   0:00 [watchdog
root         12  0.0  0.0      0     0 ?        S    May16   0:00 [migratio
root         13  0.0  0.0      0     0 ?        S    May16   0:00 [ksoftirq
root         15  0.0  0.0      0     0 ?        S<   May16   0:00 [kworker/1:0H]
root         17  0.0  0.0      0     0 ?        S    May16   0:00 [kdevtmpfs]
root         18  0.0  0.0      0     0 ?        S<   May16   0:00 [netns]
root         19  0.0  0.0      0     0 ?        S    May16   0:00 [khungtas
root         20  0.0  0.0      0     0 ?        S<   May16   0:00 [writebac
root         21  0.0  0.0      0     0 ?        S<   May16   0:00 [kintegri
root         22  0.0  0.0      0     0 ?        S<   May16   0:00 [bioset]
root         23  0.0  0.0      0     0 ?        S<   May16   0:00 [kblockd]
root         24  0.0  0.0      0     0 ?        S<   May16   0:00 [md]
root         28  0.0  0.0      0     0 ?        S    May16   0:00 [kswapd0]
root         29  0.0  0.0      0     0 ?        SN   May16   0:00 [ksmd]
root         30  0.0  0.0      0     0 ?        SN   May16   0:00 [khugepag
root         31  0.0  0.0      0     0 ?        S<   May16   0:00 [crypto]
root         39  0.0  0.0      0     0 ?        S<   May16   0:00 [kthrotlo
root         40  0.0  0.0      0     0 ?        S    May16   0:00 [kworker/
root         41  0.0  0.0      0     0 ?        S<   May16   0:00 [kmpath_r
root         42  0.0  0.0      0     0 ?        S<   May16   0:00 [kpsmouse
root         44  0.0  0.0      0     0 ?        S<   May16   0:00 [ipv6_add
root         63  0.0  0.0      0     0 ?        S<   May16   0:00 [deferwq]
root         97  0.0  0.0      0     0 ?        S    May16   0:00 [kauditd]
root        278  0.0  0.0      0     0 ?        S<   May16   0:00 [mpt_poll_0]
root        279  0.0  0.0      0     0 ?        S<   May16   0:00 [ata_sff]
root        280  0.0  0.0      0     0 ?        S<   May16   0:00 [mpt/0]
root        287  0.0  0.0      0     0 ?        S    May16   0:00 [scsi_eh_0]
root        288  0.0  0.0      0     0 ?        S<   May16   0:00 [scsi_tmf_0]
root        289  0.0  0.0      0     0 ?        S    May16   0:00 [scsi_eh_1]
root        290  0.0  0.0      0     0 ?        S    May16   0:00 [kworker/u4:2]
```

表 11-50 输出结果说明

字段	说明	字段	说明
USER	运行进程用户	RSS	进程占用物理内存的大小
PID	进程的 ID	STAT	进程的状态
%CPU	进程的 CPU 使用率	START	进程启动的时间
%MEM	进程的内存使用率	TIME	进程使用 CPU 的时间
VSZ	进程占用虚拟内存的大小	COMMAND	启动进程的命令

通过-aux选项，可以查看系统中所有进程资源使用情况，包括：

- 运行进程的用户（USER）
- CPU使用率（%CPU）
- 内存使用率（%MEM）
- 驻留数据集大小（RSS）
- 终端号（TTY）
- 进程状态（STAT）
- 进程启动时间（START）
- 进程使用的CPU时间（TIME）
- 运行进程的命令（COMMAND）

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 40,24 1 会话 CAP NUM

5.进程管理

- 启动进程
  - 在Linux系统中，启动一个进程有两个主要途径：调度启动和手工启动。
    - 手工启动就是有用户输入命令或单击图形窗口启动一个程序。
    - 根据进程的类型来分，手工启动又可以分为前台启动和后台启动两种。
      - 前台启动：是手工启动一个进程的最常用方式。例如，用户输入一个ls命令，这就会启动一个前台进程。前台进程的特点就是会一直占据着终端窗口，除非前台进程运行完毕，否则用户无法在该终端窗口中在执行其他命令。前台启动进程的方式一般比较适合运行时间较短、需要与用户交互的程序。
      - 后台启动：进程运行后不管是否已经完成，都会立即返回到Shell提示符下，不会占用终端窗口。所以用户以后台方式启动进程后，可以继续运行其他程序，而后台进程会由系统继续调度执行。如果一个程序运行比较耗时，而且不需要与用户进行交互，那么可以考虑使用后台启动方式。例如用户启动一个复制大量数据文件的进程，为了不使当前的Shell在复制完成前都一直被cp命令占用，从后台启动这个进程将是一个明智的选择。

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# ps aux | grep bash
root       788  0.0  0.0  11908  1964 pts/0    Ss   May16   0:00 -bash
root      1687  0.0  0.0   9048   664 pts/0    S+   01:17   0:00 grep --color=auto bash
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ps aux | grep bash &
[1] 1689
[root@Centos7Teach ~]# root       788  0.0  0.0  11908  1964 pts/0    Ss+  May16   0:00 -bash
root      1689  0.0  0.0   9048   664 pts/0    S    01:17   0:00 grep --color=auto bash

[1]+  Done                    ps aux | grep --color=auto bash
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 12,24 1 会话 CAP NUM

5.进程管理

- 终止进程：kill

【功能】

如果要终止一个前台进程的运行，可以按下快捷键 Ctrl+C，如果是后台进程，那必须使用 kill 命令来终止。要终止一个后台进程，首先需要知道该进程的进程 ID，可以通过 ps 命令进行获取，然后把进程 ID 作为参数在 kill 命令中指定。对于普通用户来说，用户只能管理自己运行的进程，而 root 用户则可以管理系统中所有的进程。

【语法】

```
# kill [选项] [进程]
```

【选项说明】

kill 命令常用选项及其说明如表 11-51 所示。

表 11-51 kill 命令选项及其说明

选项	说明
-a	当处理当前进程时，不限制命令名和进程号的对应关系
-l [信息编号]	如果加[信息编号]选项，则-l 参数会列出全部的信息
-p	指定 kill 命令只打印相关进程的进程号，而不发送任何信号
-s [信息名称或编号]	指定要送出的信息
-u	指定用户

5.进程管理

- 终止进程：kill

表 11-52 信号列表说明

信号	取值	默认动作	含义（发出信号的原因）
SIGHUP	1	Term	终端的挂断或进程死亡
SIGINT	2	Term	来自键盘的中断信号
SIGQUIT	3	Core	来自键盘的离开信号
SIGILL	4	Core	非法指令
SIGABRT	6	Core	来自 abort 的异常信号
SIGFPE	8	Core	浮点例外
SIGKILL	9	Term	杀死
SIGSEGV	11	Core	段非法错误(内存引用无效)
SIGPIPE	13	Term	管道损坏：向一个没有读进程的管道写数据
SIGALRM	14	Term	来自 alarm 的计时器到时信号
SIGTERM	15	Term	终止
SIGUSR1	30,10,16	Term	用户自定义信号 1
SIGUSR2	31,12,17	Term	用户自定义信号 2
SIGCHLD	20,17,18	Ign	子进程停止或终止
SIGCONT	19,18,25	Cont	如果停止，继续执行
SIGSTOP	17,19,23	Stop	非来自终端的停止信号
SIGTSTP	18,20,24	Stop	来自终端的停止信号
SIGTTIN	21,21,26	Stop	后台进程读终端
SIGTTOU	22,22,27	Stop	后台进程写终端
SIGBUS	10,7,10	Core	总线错误（内存访问错误）
SIGPOLL	-	Term	Pollable 事件发生(Sys V)，与 SIGIO 同义
SIGPROF	27,27,29	Term	统计分布图用计时器
SIGSYS	12,-,12	Core	非法系统调用(SVr4)
SIGTRAP	5	Core	跟踪/断点自陷
SIGURG	16,23,21	Ign	socket 紧急信号(4.2BSD)
SIGVTALRM	26,26,28	Term	虚拟计时器到时(4.2BSD)
SIGXCPU	24,24,30	Core	超过 CPU 时限(4.2BSD)
SIGXFSZ	25,25,31	Core	超过文件长度限制(4.2BSD)
SIGIOT	6	Core	IOT 自陷，与 SIGABRT 同义
SIGEMT	7,-,7		Term
SIGSTKFLT	-,16,-	Term	协处理器堆栈错误(不使用)
SIGIO	23,29,22	Term	描述符上可以进行 I/O 操作
SIGCLD	-,-,18	Ign	与 SIGCHLD 同义
SIGPWR	29,30,19	Term	电力故障(System V)
SIGINFO	29,-,-		与 SIGPWR 同义
SIGLOST	-,-,-	Term	文件锁丢失
SIGWINCH	28,28,20	Ign	窗口大小改变(4.3BSD, Sun)
SIGUNUSED	-,31,-	Term	未使用信号(will be SIGSYS)

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# ps aux | grep httpd
root      1786  1.0  0.1 226304  5112 ?        Ss   01:23   0:00 /usr/sbin/httpd -DFOREGROUND
apache    1787  0.0  0.0 226304  3036 ?        S    01:23   0:00 /usr/sbin/httpd -DFOREGROUND
apache    1788  0.0  0.0 226304  3036 ?        S    01:23   0:00 /usr/sbin/httpd -DFOREGROUND
apache    1789  0.0  0.0 226304  3036 ?        S    01:23   0:00 /usr/sbin/httpd -DFOREGROUND
apache    1790  0.0  0.0 226304  3036 ?        S    01:23   0:00 /usr/sbin/httpd -DFOREGROUND
apache    1791  0.0  0.0 226304  3036 ?        S    01:23   0:00 /usr/sbin/httpd -DFOREGROUND
root      1794  0.0  0.0   9044   664 pts/0    S+   01:23   0:00 grep --color=auto httpd
[root@Centos7Teach ~]# kill 1786
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# ps aux | grep httpd
root      1802  0.0  0.0   9044   664 pts/0    S+   01:24   0:00 grep --color=auto httpd
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 14,24 1 会话 CAP NUM

5.进程管理

- 更改进程优先级：nice renice
  - 在Linux系统中，每个进程在执行时都会赋予一个优先等级，等级越高，进程获得CPU时间就会越多，所以级别越高的进程，运行的时间就会越短，反之则需要较长的运行时间。
  - 进程的优先等级范围为-20~19，其中，-20表示最高等级，而19则是最低。
  - 等级-1~-20只有root用户可以设置，进程运行的默认级别为0。

【功能】

nice 命令用于以指定的进程调度优先级启动其他的程序。

【语法】

```
# nice [选项] [命令]
```

【选项说明】

nice 命令常用选项及其说明如表 11-53 所示。

表 11-53 nice 命令选项及其说明

选项	说明
-n	指定进程的优先级（整数）

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# vi test1.php &
[1] 1857
[root@Centos7Teach ~]# nice vi test2.php &
[2] 1858

[1]+  Stopped                 vi test1.php
[root@Centos7Teach ~]# nice -19 vi test3.php &
[3] 1859

[2]+  Stopped                 nice vi test2.php
[root@Centos7Teach ~]# nice --19 vi test4.php &
[4] 1860

[3]+  Stopped                 nice -19 vi test3.php
[root@Centos7Teach ~]# nice -30 vi test5.php &
[5] 1861

[4]+  Stopped                 nice --19 vi test4.php
[root@Centos7Teach ~]#

[5]+  Stopped                 nice -30 vi test5.php
[root@Centos7Teach ~]# ps lax | grep test
0     0  1857   788  20   0  20420  1424 do_sig T    pts/0      0:00 vi test1.php
0     0  1858   788  30  10  20420  1420 do_sig TN   pts/0      0:00 vi test2.php
0     0  1859   788  39  19  20420  1428 do_sig TN   pts/0      0:00 vi test3.php
4     0  1860   788   1 -19  20420  1424 do_sig T<   pts/0      0:00 vi test4.php
0     0  1861   788  39  19  20420  1424 do_sig TN   pts/0      0:00 vi test5.php
0     0  1863   788  20   0   9044   664 pipe_w S+   pts/0      0:00 grep --color=auto test
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# renice 5 1861
1861 (process ID) old priority 19, new priority 5
[root@Centos7Teach ~]# ps lax | grep test
0     0  1857   788  20   0  20420  1424 do_sig T    pts/0      0:00 vi test1.php
0     0  1858   788  30  10  20420  1420 do_sig TN   pts/0      0:00 vi test2.php
0     0  1859   788  39  19  20420  1428 do_sig TN   pts/0      0:00 vi test3.php
4     0  1860   788   1 -19  20420  1424 do_sig T<   pts/0      0:00 vi test4.php
0     0  1861   788  25   5  20420  1424 do_sig TN   pts/0      0:00 vi test5.php
0     0  1867   788  20   0   9044   664 pipe_w S+   pts/0      0:00 grep --color=auto test
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 39,24 1 会话 CAP NUM

5.进程管理

周期性执行：crontab

【功能】

crontab 可以根据分钟、小时、日期、月份、星期的组合来调度任务的自动执行。用户只要在 crontab 中设置好任务启动的时间，到了相应的时间后系统就会自动启动该任务。

【语法】

```
# crontab [选项] [crontab 文件]
```

【选项说明】

crontab 命令常用选项及其说明如表 11-54 所示。

表 11-54 crontab 命令选项及其说明

选项	说明
-u user	指定更改是哪个用户自动任务。如果不设置，则默认会更改当前运行命令用户的自动任务列表。该选项只有 root 用户能使用，一般用户只能更改自己的任务列表
-l	输出当前的自动任务列表
-r	删除当前的自动任务列表
-e	更改用户的自动任务列表
-i	与-r 选项相同，但在删除任务列表前会提示用户确认

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed

  *  *  *  *  *  root  date > /root/cron-date.txt
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# cat /root/cron-date.txt
Thu May 17 01:51:01 CST 2018
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

文件中每一行的格式如下所示。

分钟 小时 日期 月份 星期 命令

其格式中每个字段的说明如表 11-55 所示。

表 11-55 定时任务文件格式字段说明

字段	说明
分钟	从 0~59 之间的任何整数
小时	从 0~23 之间的任何整数
日期	从 1~31 之间的任何整数（如果制定了月份，则必须是该月份的有效日期）
月份	从 1~12 之间的任何整数
星期	从 0~7 之间的任何整数，其中 0 或 7 表示星期天
命令	需要定制指定的命令

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 22,24 1 会话 CAP NUM

5.进程管理

- 周期性执行：crontab
  - 实例1：每1分钟执行一次同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - * * * * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例2：每小时的第3和第15分钟执行同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 3,15 * * * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例3：在上午8点到11点的第3和第15分钟执行同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 3,15 8-11 * * * command
  - 实例4：每隔两天的上午8点到11点的第3和第15分钟执行同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 3,15 8-11 /2 * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/

5.进程管理

- 周期性执行：crontab
  - 实例5：每个星期一的上午8点到11点的第3和第15分钟执行同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 3,15 8-11 * * 1 rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例6：每晚的21:30同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 30 21 * * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例7：每月1、10、22日的4 : 45同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 45 4 1,10,22 * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例8：每周六、周日的1 : 10同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 10 1 * * 6,0 rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/

5.进程管理

- 周期性执行：crontab
  - 实例9：每天18 : 00至23 : 00之间每隔30同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 0,30 18-23 * * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例10：每星期六的晚上11 : 00 pm同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 0 23 * * 6 rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例11：每一小时重启smb
  - * /1 * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例12：晚上11点到早上7点之间，每隔一小时同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - * 23-7/1 * * * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/

5.进程管理

- 周期性执行：crontab
  - 实例13：每月的4号与每周一到周三的11点同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 0 11 4 * mon-wed rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例14：一月一号的4点同步当前主机/mnt/下所有文件到192.168.1.88:/mnt/
  - 0 4 1 jan * rsync -vzopgrt –delete /mnt/ 192.168.1.88:/mnt/
  - 实例15：每小时执行/etc/cron.hourly目录内的脚本
  - 01 * * * * root run-parts /etc/cron.hourly

5.进程管理

- 定时执行：at

【功能】

使用 at 命令可以在指定的时间执行指定的命令。与 crontab 不同，通过 at 命令定义的任务只会运行一次，也就是说，运行一次后该任务就不在存在了。

【语法】

```
# at [选项] [日期时间]
```

【选项说明】

at 命令常用选项及其说明如表 11-56 所示。

表 11-56 at 命令选项及其说明

选项	说明
-f	指定包含具体指令的任务文件
-q	指定新任务的队列名称
-l	显示待执行任务的列表
-d	删除指定的待执行任务
-m	任务执行完成后巷用户发送邮件

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# at -f /root/backup.sh 2pm +3 days
job 4 at Sun May 20 14:00:00 2018
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# at -f /root/backup.sh now+30 minutes
job 5 at Thu May 17 02:30:00 2018
[root@Centos7Teach ~]#
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 7,24 1 会话 CAP NUM

5.进程管理

- 空闲时执行：batch

【功能】

batch 命令用于低优先级运行作业，该命令几乎和 at 命令的功能完全相同。唯一的区别在与 at 命令是在指定时间，很精确地执行指定命令，而 batch 却是在系统负载较低，资源比较空闲的时候执行命令。batch 的执行主要是由系统来控制的，因而用于的干预权利很小。该命令适合于执行占用资源较多的命令。

【语法】

```
# batch [选项] [日期时间]
```

【选项说明】

batch 命令常用选项及其说明如表 11-57 所示。

表 11-57 batch 命令选项及其说明

选项	说明
-f	指定包含具体指令的任务文件
-q	指定新任务的队列名称
-m	任务执行完成后向用户发送邮件

Teach-CentOS 7 - root@Centos7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@Centos7Teach ~]# at -f /root/backup.sh 2pm +3 days
job 4 at Sun May 20 14:00:00 2018
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# at -f /root/backup.sh now+30 minutes
job 5 at Thu May 17 02:30:00 2018
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# bash -f /root/backup.sh
[root@Centos7Teach ~]#
[root@Centos7Teach ~]# cat /root/
.bash_history           .lesshst                community-rules.tar.gz  samba.install.sh
.bash_logout            .mysql_history          cron-date.txt           samba.remove.sh
.bash_profile           .pki/                   demo.conf               vsftpd.install.sh
.bashrc                 .tcshrc                 firewalld               vsftpd.remove.sh
.cshrc                  backup.sh               runlog.txt
[root@Centos7Teach ~]# cat /root/runlog.txt
Thu May 17 02:05:46 CST 2018
[root@Centos7Teach ~]# bash -f /root/backup.sh
[root@Centos7Teach ~]# cat /root/runlog.txt
Thu May 17 02:06:32 CST 2018
[root@Centos7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 20,24 1 会话 CAP NUM

6.日志管理

- 系统日志
  - 详细而准确的分析以及备份系统日志是一个系统管理员应该要进行的任务之一。
  - 简单地说，就是记录系统活动信息的信息，例如：何时、何地（来源IP）、何人（什么服务名称）、做了什么操作。换句话说就是：记录系统在什么时候由哪个进程做了什么样的行为时，发生了何种的事件等。

6.日志管理

- 日志管理策略
  - Linux系统管理员应该建立一套与日志工作有关的规章制度。
  - 日志策略至少应解决一下几方面的问题。
    - 建立日志集中管理机制：集中管理日志的主要好处一是更便于其收集、整理合分析使用；二是可以防止敏感信息发生意外丢失或被人们蓄意篡改或删除。
    - 为日志提供备份：日志文件同样是重要的数据，同样需要备份和归档。如果需要备份的内容多到需要分批分组，应该定义一个专门的分组来备份应用程序和操作系统的日志文件。
    - 日志文件的保护：一定要严格限制无关人员访问操作系统的日志文件，这些文件往往包含各种口令字或其他敏感信息。
    - 日志文件的保存期：把日志文件压缩为文件永久地保存并非不现实，需要确定日志的保存期。

6.日志管理

常用日志文件

表 11-59 常用日志文件及其说明

日志文件	日志说明
/var/log/boot.log	记录系统在引导过程中发生的事件，就是 Linux 系统开机自检过程显示的信息
/var/log/cron	记录 crontab 守护进程 crond 所派生的子系统的动作，前面加上用户、登录时间和 PID 以及派生出的进程的动作
/var/log/maillog	记录每一个发送到系统或从系统发出的电子邮件的活动，可以查看用户使用哪个系统发送工具或把数据发送到哪个系统
/var/log/messages	该日志文件是许多进程日志文件的汇总，从该文件可以看出任何入侵启动或成功入侵的日志信息
/var/log/syslog	默认 Linux 不生成该日志文件，但可以配置/etc/syslog.conf 让系统生成该日志文件，该日志文件只记录警告信息
/var/log/secure	记录与安全有关的信息
/var/log/lastlog	记录最近成功登录的事件和最后一次不成功的登录事件，由 login 生成。该文件是二进制文件，需要使用 lastlog 命令查看，根据 UID 排序显示登录名、端口号和上次登录时间
/var/log/wtmp	记录每个用户登录、注销以及系统的启动、停机的事件
/var/log/utmp	记录有关当前登录的每个用户的信息
/var/log/xferlog	记录 FTP 会话，可以显示出用户向 FTP 服务器或从服务器拷贝了什么文件
/var/log/Xfree86.x.log	记录了 X-Window 启动的情况
/var/log/kernlog	默认 Linux 记录该日志文件，可以配置/etc/syslog.conf 生成该文件。该文件记录了系统启动时加载设备或使用设备的情况

6.日志管理

关于日志文件的国家要求

数据安全性	5	（1）依据《互联网安全保护技术措施规定》第十一、十二条 （2）罚则《计算机信息网络国际联网安全保护管理办法》第二十一条	安装并运行互联网公共上网服务场所安全管理系统，且具有符合公共安全行业技术标准的联网接口（非经营性公共上网服务场所需检查此项）	检查该单位是否安装了互联网公共上网服务场所安全管理系统，并与市局管理中心实时联网。	①互联网公共上网服务场所安全管理系统运行正常； ②互联网公共上网服务场所安全管理系统达到上述检查要求； ③与市局管理中心实时联网。
	6	（1）依据《互联网安全保护技术措施规定》第十三条 （2）罚则《计算机信息网络国际联网安全保护管理办法》第二十一条	大于六十天的记录备份	通过日志留存设备检查相关日志记录。	①应用会话记录和系统会话记录大于六十天； ②**告警记录大于六十天。**

6.日志管理

- 日志格式
  - 一般来说，系统产生的信息经过syslog记录之后，每条信息均会记录下面几个重要信息。
    - 事件发生的日期与时间；
    - 发生此事件的主机名；
    - 启动此事件的服务名称（如samba，xinetd等）或函数名称（如libpam）；
    - 该信息的实际数据内容。

Teach-CentOS 7 - root@CentOS7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

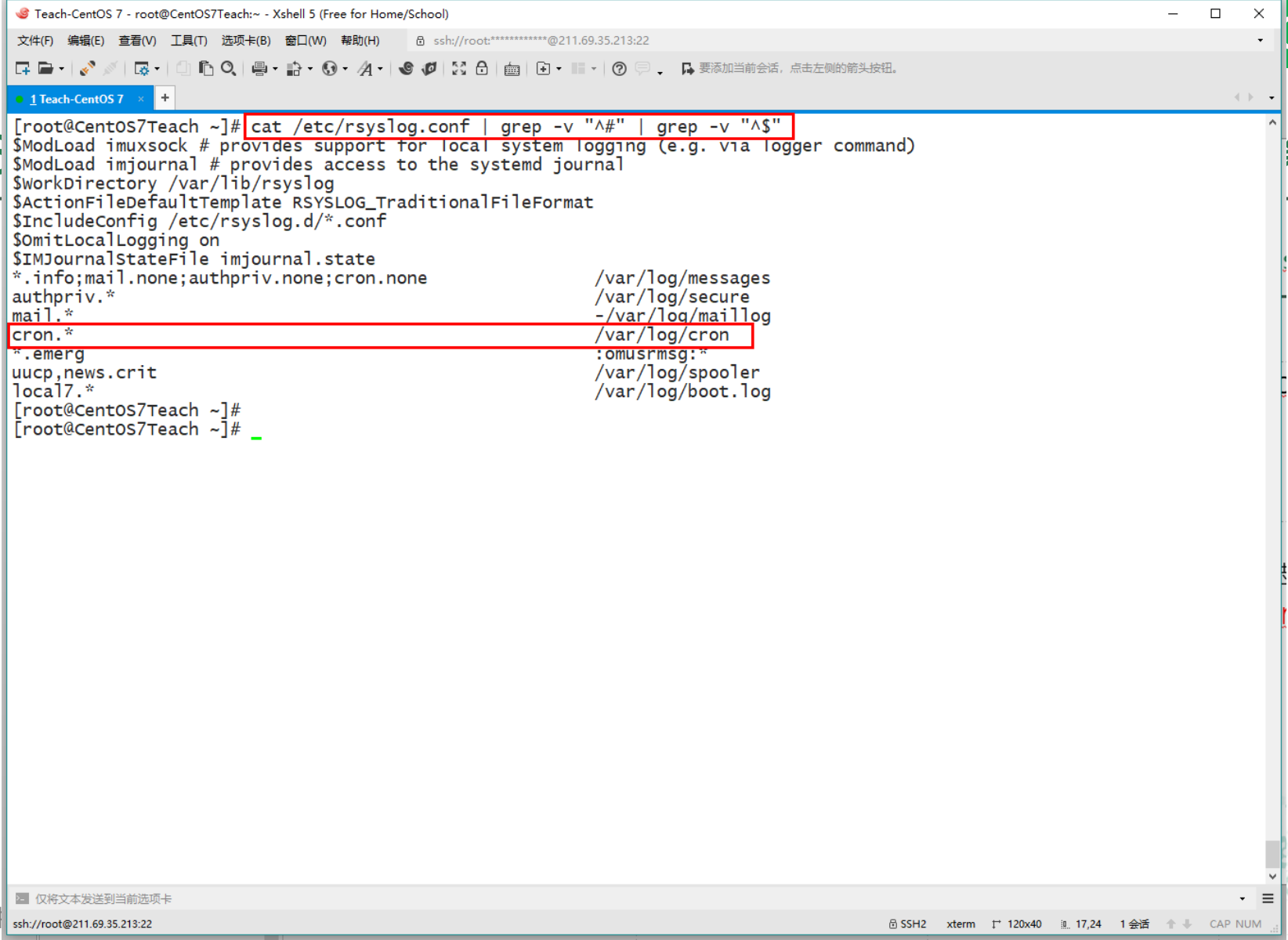
```
[root@CentOS7Teach ~]# tail /var/log/secure
May 18 00:32:32 CentOS7Teach login: pam_unix(login:session): session closed for user root
May 18 00:32:53 CentOS7Teach sshd[1300]: Accepted password for root from 10.10.0.1 port 54902 ssh2
May 18 00:32:53 CentOS7Teach sshd[1300]: pam_unix(sshd:session): session opened for user root by (uid=0)
May 18 00:33:13 CentOS7Teach sshd[1321]: Invalid user godep from 10.10.0.1 port 56918
May 18 00:33:13 CentOS7Teach sshd[1321]: input_userauth_request: invalid user godep [preauth]
May 18 00:33:13 CentOS7Teach sshd[1321]: pam_unix(sshd:auth): check pass; user unknown
May 18 00:33:13 CentOS7Teach sshd[1321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
r= rhost=10.10.0.1
May 18 00:33:15 CentOS7Teach sshd[1321]: Failed password for invalid user godep from 10.10.0.1 port 56918 ssh2
May 18 00:33:16 CentOS7Teach sshd[1321]: Received disconnect from 10.10.0.1 port 56918:11: Normal Shutdown, Thank you fo
r playing [preauth]
May 18 00:33:16 CentOS7Teach sshd[1321]: Disconnected from 10.10.0.1 port 56918 [preauth]
[root@CentOS7Teach ~]#
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 14,24 1 会话 CAP NUM

6.日志管理

- 日志配置文件
  - syslog针对各种服务与信息记录所对应的配置文件是/etc/syslog.conf。配置文件规定了什么服务的什么等级信息以及被记录在哪里。
  - 该文件中设置的语法格式如下所示（以authpriv服务为例）。
    - #服务名称[.=!]信息等级　　信息记录的文件名或设备或主机
    - authpriv.*　　/var/log/secure
      - authpriv服务产生的所有等级的信息，都被记录到/var/log/secure日志文件中。
  - 在CentOS 7操作系统中，syslog的配置文件为/etc/rsyslog.conf。


Teach-CentOS 7 - root@CentOS7Teach:~ - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://root:**********@211.69.35.213:22
要添加当前会话，点击左侧的箭头按钮。
1 Teach-CentOS 7
[root@CentOS7Teach ~]# cat /etc/rsyslog.conf | grep -v "^#" | grep -v "^$"
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
$WorkDirectory /var/lib/rsyslog
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
$IncludeConfig /etc/rsyslog.d/*.conf
$OmitLocalLogging on
$IMJournalStateFile imjournal.state
*.info;mail.none;authpriv.none;cron.none /var/log/messages
authpriv.* /var/log/secure
mail.* -/var/log/maillog
cron.* /var/log/cron
.emerg :omusrmsg:
uucp,news.crit /var/log/spooler
local7.* /var/log/boot.log
[root@CentOS7Teach ~]#
[root@CentOS7Teach ~]#
仅将文本发送到当前选项卡
ssh://root@211.69.35.213:22
SSH2 xterm 120x40 17,24 1 会话
CAP NUM

6.日志管理

- syslog的服务名称

表 11-60 常用的服务类型说明

服务类型	日志说明
auth（authpriv）	主要与认证有关的机制。例如 login，ssh，su 等需要账号/密码
cron	就是例行工作调度 crontab/at 等生成信息日志的地方
daemon	与各个 daemon 有关的信息
kern	就是内核（kernel）产生信息的地方
lpr	与打印机相关的信息
mail	与邮件收发有关的信息记录
news	与新闻组服务器有关的东西
syslog（rsyslog）	就是 syslogd 这个程序本身生成的信息
user,uucp,local0~local7	与 Unix Like 机器本身有关的一些信息

6.日志管理

- syslog的信息等级

表 11-61 信息等级信息描述

等级	等级名称	说明
1	info	仅是一些基本的信息说明而已
2	notice	除了 info 外还需要注意的一些信息内容
3	warning（warn）	警示的信息，可能有问题，但是还不至于影响到整个 daemon 运行的信息；基本上，info，notice，warn 这三个信息都是在告知一些基本信息而已，应该还不至于造成一些系统运行困扰
4	err（error）	一些重大的错误信息，例如配置文件的某些设置值造成该服务器无法启动的信息说明，通常通过 err 的错误告知，应该可以了解该服务无法启动的问题
5	crit	比 error 还要严重的错误信息，这个 crit 是临界点（critical）的缩写，这个错误已经很严重了
6	alert	警告，已经很有问题的等级，比 crit 还要严重
7	emerg（panic）	“疼痛”等级，意指系统已经几乎要死机的状态，这是很严重的错误信息了。通常大概只有硬件出问题导致整个内核无法顺利运行，就会出现该等级信息

6.日志管理

- 信息日志的安全性
  - 日志文件的重要性毋庸置疑，那怎么保证日志文件的安全性呢？如何保证日志文件不被删除或被root用户不小心更改？
  - 通过“chattr”命令将日志文件设置成为“只能增加数据但不能被删除的状态”从而保护日志文件。

6.日志管理

- 信息日志的安

【功能】

chattr 命令用来改变文件属性。这项指令可以改变存放在 ext2 文件系统上的文件或目录属性，这些属性共有 8 种属性，具体属性描述如表 11-62 所示。

表 11-62 chattr 命令属性

属性命令	描述
a	让文件或目录仅供附加用途
b	不更新文件或目录的最后存取时间
c	将文件或目录压缩后存放
d	将文件或目录排除在倾倒操作之外
i	不得任意改动文件或目录
s	保密性删除文件或目录
S	即时更新文件或目录
u	预防意外删除

【语法】

```
# chattr [选项]
```

【选项说明】

chattr 命令常用选项及其说明如表 11-63 所示。

表 11-63 chattr 命令选项及其说明

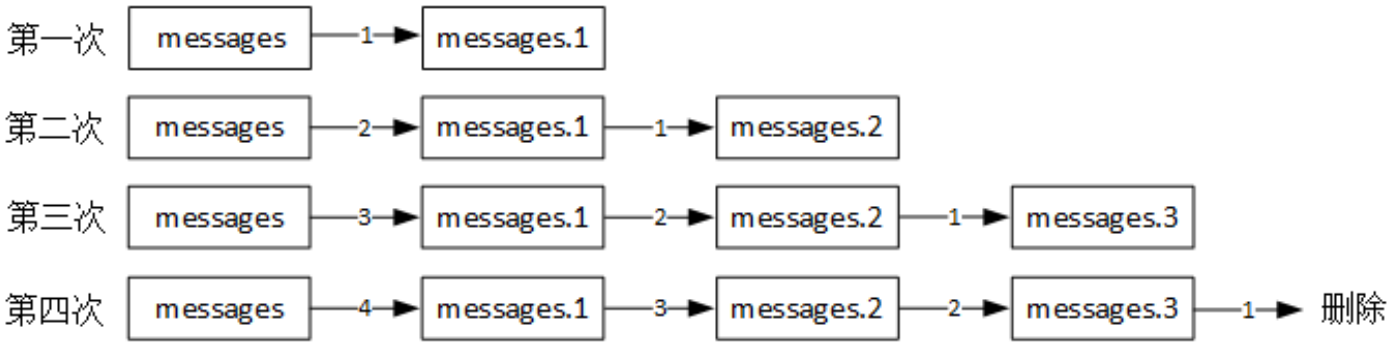
选项	说明
-R	递归处理，将指令目录下的所有文件及及子目录一并处理
-v [版本号码]	设置文件或目录版本
-V	显示指令执行过程
+[属性]	开启文件或目录的该选项属性
-[属性]	关闭文件或目录的该项属性
=[属性]	指定文件或目录的该项属性

6.日志管理

- logrotate程序是一个日志管理工具，主要用于对系统日志进行轮转、压缩和删除，也可以将日志发送到指定邮箱。
  - 使用该程序可使系统管理员轻松管理系统所产生的记录文件，每个记录文件都可以被设置成每日、每周或每月处理，也能在文件太大时立即处理，从而分割日志文件，删除旧的日志文件，并创建新的日志文件，起到"转储"作用，从而为系统节省磁盘空间。
  - logrotate将旧的日志文件移动成旧文件，并且重新新建一个空文件来记录。其工作原理为：
    - 第一次执行完rotate之后，原本的messages会变成messages.1而且会制造一个空的messages给系统来保存日志文件；
    - 第二次执行之后，则messages.1会变成messages.2，messages会变成messages.1，又造成一个空的messages来保存日志文件。
    - 如果设置仅保留3个日志文件的话，那么执行第四次时，则messages.3这个文件就会被删除，并由后面的较新的保存日志文件所替代。

6.日志管理

- logrotate



Teach-CentOS 7 - root@CentOS7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@CentOS7Teach ~]# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
        minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
[root@CentOS7Teach ~]#
```

针对wtmp日志的配置

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 37,24 1 会话 CAP NUM

6.日志管理

logrotate日志处理

【功能】

可使用 logrotate 命令，可单独对日志执行 rotate 操作，进行日志文件管理操作。

【语法】

```
# logrotate [选项] [配置文件]
```

【选项说明】

logrotate 命令常用选项及其说明如表 11-63 所示。

表 11-63 logrotate 命令选项及其说明

选项	说明
-d 或—debug	详细限制指令执行过程，便于排错或了解程序执行的情况
-f 或--force	强行启动文件维护操作，即使 logrotate 指令没有需要
-s 或--state [状态文件]	使用指定的状态文件
-v 或—version	显示指令执行过程
-usage	显示指令基本用户

Teach-CentOS 7 - root@CentOS7Teach:~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H) ssh://root:**********@211.69.35.213:22

要添加当前会话，点击左侧的箭头按钮。

1 Teach-CentOS 7

```
[root@CentOS7Teach ~]# logrotate -v /etc/logrotate.conf
reading config file /etc/logrotate.conf
including /etc/logrotate.d
reading config file bootlog
reading config file syslog
reading config file wpa_supplicant
reading config file yum
Allocating hash table for state file, size 15360 B

Handling 6 logs

rotating pattern: /var/log/boot.log
 after 1 days (7 rotations)
empty log files are rotated, old logs are removed
considering log /var/log/boot.log
  log needs rotating
rotating log /var/log/boot.log, log->rotateCount is 7
dateext suffix '-20180518'
glob pattern '-[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]'
glob finding old rotated logs failed
copying /var/log/boot.log to /var/log/boot.log-20180518
set default create context to system_u:object_r:plymouthd_var_log_t:s0
truncating /var/log/boot.log

rotating pattern: /var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
 weekly (4 rotations)
empty log files are rotated, old logs are removed
considering log /var/log/cron
  log needs rotating
considering log /var/log/maillog
  log needs rotating
considering log /var/log/messages
  log needs rotating
considering log /var/log/secure
  log needs rotating
considering log /var/log/spooler
```

仅将文本发送到当前选项卡

ssh://root@211.69.35.213:22 SSH2 xterm 120x40 40,24 1 会话 CAP NUM

6.日志管理

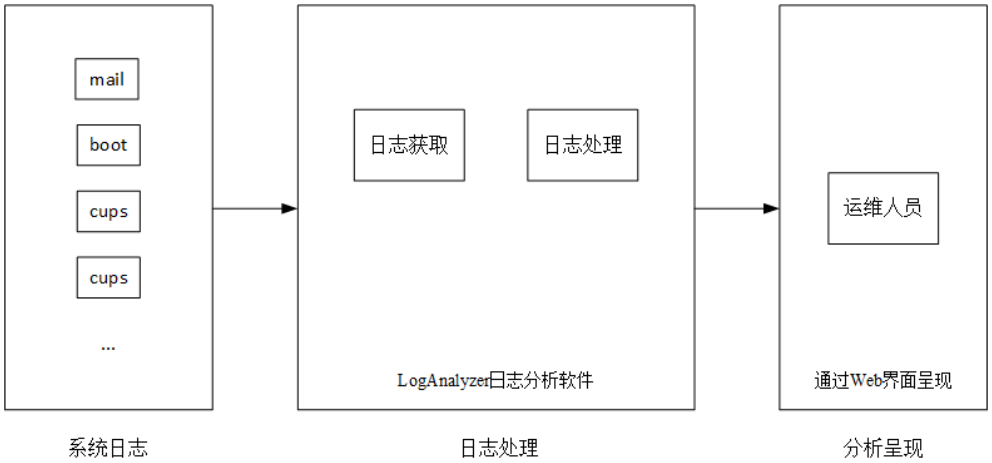
- 需求描述
  - 在系统日常维护过程中，仅仅通过查看日志文件，会有着以下的几方面问题。
    - 数据量大
      - 当系统中运行业务较多时，每天产生的数据量的数量是巨大的，如果仅靠系统运维人员以查看每个日志文件的方式进行系统检查是几乎不可能的。
    - 可读性差
      - 系统运行过程中会产生大量的日志信息，但是这些日志进行并不是宜读的格式。而日志分析可以将日志本身解析成多个可读字段信息，能够让普通用户都能看的懂，并可通过可视化的方式共同查看系统运行状态以及业务服务情况。

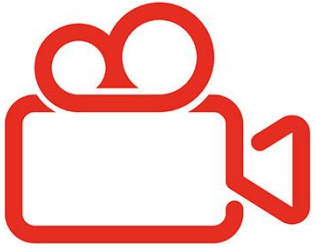
6.日志管理

- 需求描述
  - 在系统日常维护过程中，仅仅通过查看日志文件，会有着以下的几方面问题。
    - 等级不清晰
      - 系统产生的日志信息常有7种不同等级，但是这些等级的日志信息保存在不同的文件中，查看起来比较麻烦。
      - 通过日志审计分析，可将不同等级的日志信息进行不同颜色等级标注，使运维人员快速查看出危险等级高的日志信息，并快速解决危险问题。
    - 发现不及时
      - 当系统发生危险等级高的问题时，虽产生出相应的日志信息，但是运维人员不能及时发现.
      - 通过相应的日志审计分析工具，当发现危险等级高的日志后，可直接通过一定的技术手段将日志信息告知给相关运维人员，从而及时发现问题并快速解决问题。

6.日志管理

方案设计


mail
boot
cups
cups
...
日志获取
日志处理
LogAnalyzer日志分析软件
运维人员
通过Web界面呈现
系统日志
日志处理
分析呈现



- 示例：基于LogAnalyzer进行系统日志审计分析
  - 安装基础环境：LAMP
  - 安装数据库，并导入初始数据
  - 部署LogAnalyzer分析软件
  - 应用测试