Linux学习：第六天

目录

日志管理

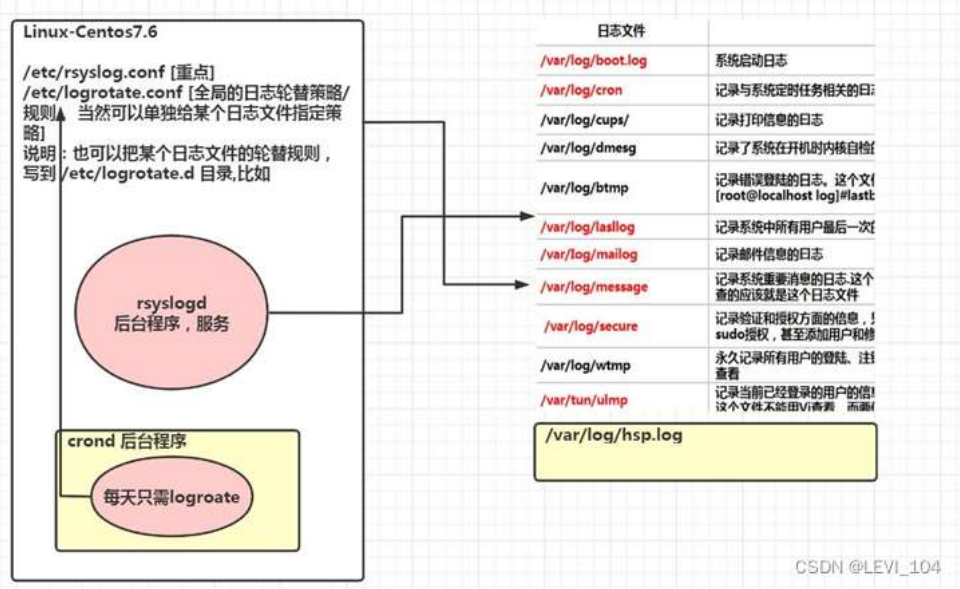
日志文件是重要的系统信息文件，其中记录了许多重要的系统事件，包括用户的登录信息、系统的启动信息、系统的安全信息、邮件相关信息、各种
息等。日志对于安全来说也很重要，它记录了系统每天发生的各种事情，通过日志来检查错误发生的原因，或者受到攻击时攻击者留下的痕迹。可以
日志是用来记录重大事件的工具

系统日志文件的保存位置：/var/log/

系统常用的日志如下：

日志文件	说 明
/var/log/boot.log	系统启动日志
/var/log/cron	记录与系统定时任务相关的日志
/var/log/cups/	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息。也可以使用dmesg命令直接查看内核自检信息
/var/log/btmp	记录错误登陆的日志。这个文件是二进制文件，不能直接用Vi查看，而要使用lastb命令查看。命令如下：[root@localhost log]#lastb
/var/log/lasllog	记录系统中所有用户最后一次的登录时间的日志。这个文件也是二进制文件.要使用lastlog命令查看
/var/log/mailog	记录邮件信息的日志
/var/log/message	记录系统重要消息的日志.这个日志文件中会记录Linux系统的绝大多数重要信息。如果系统出现问题，首先要检查的应该就是这个日志文件
/var/log/secure	记录验证和授权方面的倍息，只要涉及账户和密码的程序都会记录，比如系统的登录、ssh的登录、su切换用户，sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中
/var/log/wtmp	永久记录所有用户的登陆、注销信息，同时记录系统的后动、重启、关机事件。是二进制文件.而要使用last命令查看
/var/tun/ulmp	记录当前已经登录的用户的信息。这个文件会随着用户的登录和注销而不断变化，只记录当前登录用户的信息。这个文件不能用Vi查看，而要使用w、who、users等命令查看

日志管理服务rsyslogd



- 查询 Linux 中的 rsyslogd 服务是否启动：ps aux | grep "rsyslog" | grep -v "grep"
- 查询 rsyslogd 服务的自启动状态：systemctl list-unit-files | grep rsyslog
- 配置文件：/etc/rsyslog.conf

编辑文件时的格式为： *.* 。 存放日志文件其中第一个*代表日志类型，第二个*代表日志级别

日志类型如下：

> auth ##pam 产生的日志
>
> authpriv ##ssh、ftp 等登录信息的验证信息
>
> corn ##时间任务相关
>
> kern ##内核
>
> lpr ##打印
>
> mail ##邮件
>
> mark(syslog)-rsyslog##服务内部的信息，时间标识
>
> news 新闻组
>
> user 用户程序产生的相关信息
>
> uucp unix to nuix copy 主机之间的通信
>
> local 1-7 自定义的日志设备

日志级别分为

> debug ##有调试信息的，日志通信最多info ##一般信息日志，最常用notice ##最具有重要性的普通条件的信息warning ##警告级别
>
> err ##错误级别，阻止某个功能或者模块不能正常工作的信息
>
> crit ##严重级别，阻止整个系统或者整个软件不能正常工作的信息alert ##需要立刻修改的信息
>
> emerg ##内核崩溃等重要信息none ##什么都不记录
>
> 注意：从上到下，级别从低到高，记录信息越来越少

由日志服务 rsyslogd 记录的日志文件，日志文件的格式包含以下 4 列：

> 1. 事件产生的时间

2. 产生事件的服务器的主机名
3. 产生事件的服务名或程序名
4. 事件的具体信息

日志轮替

日志轮替就是把旧的日志文件移动并改名，同时建立新的空日志文件，当旧日志文件超出保存的范围之后，就会进行删除

日志轮替文件的命名：

1. centos7 使用 logrotate 进行日志轮替管理，要想改变日志轮替文件名字，通过 /etc/logrotate.conf 配置文件中“dateext” 参数：
2. 如果配置文件中有“dateext”参数，那么日志会用日期来作为日志文件的后缀，例如 “secure-20201010”。这样日志文件名不会重叠，也就不文件的改名， 只需要指定保存日志个数，删除多余的日志文件即可。
3. 如果配置文件中没有“dateext”参数，日志文件就需要进行改名了。当第一次进行日志轮替时，当前的“secure”日志会自动改名为“secure.1”，建“secure”日志， 用来保存新的日志。当第二次进行日志轮替时，“secure.1” 会自动改名为“secure.2”， 当前的“secure”日志会自动改名为“secure.1”，然后也会新建“secure”日志，用来保存新的日志，以此类推。

logrotate配置文件

- /etc/logrotate.conf 为 logrotate 的全局配置文件

```
# rotate log files weekly, 每周对日志文件进行一次轮替
weekly
# keep 4 weeks worth of backlogs, 共保存 4 份日志文件，当建立新的日志文件时，旧的将会被删除
rotate 4
# create new (empty) log files after rotating old ones, 创建新的空的日志文件，在日志轮替后
create
# use date as a suffix of the rotated file, 使用日期作为日志轮替文件的后缀
dateext
# uncomment this if you want your log files compressed, 日志文件是否压缩。如果取消注释，则日志会在转储的同时进行压缩
#compress
#RPM packages drop log rotation information into this directory include /etc/logrotate.d
# 包含 /etc/logrotate.d/ 目录中所有的子配置文件。也就 是说会把这个目录中所有子配置文件读取进来，
#下面是单独设置，优先级更高。
# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
monthly # 每月对日志文件进行一次轮替
create 0664 root utmp # 建立的新日志文件，权限是 0664 ， 所有者是 root ， 所属组是 utmp 组
minsize 1M    # 日志文件最小轮替大小是 1MB 。也就是日志一定要超过 1MB 才会轮替，否则就算时间达到一个月，也不进行日志转储
rotate 1 # 仅保留一个日志备份。也就是只有 wtmp 和 wtmp.1 日志保留而已
}
/var/log/btmp {
missingok # 如果日志不存在，则忽略该日志的警告信息
monthly
create 0600 root utmp rotate 1
```

```
}
```

上述配置文件的参数说明如下

daily 日志的轮替周期是每天

weekly 日志的轮替周期是每周

monthly 日志的轮替周期是每月

rotate 数字 保留的日志文件的个数。0 指没有备份

compress 日志轮替时，旧的日志进行压缩

create mode owner group 建立新日志，同时指定新日志的权限与所有者和所属组。 mail address 当日志轮替时，输出内容通过邮件
定的邮件地址。missingok 如果日志不存在，则忽略该日志的警告信息

notifempty 如果日志为空文件，则不进行日志轮替

minsize 大小 日志轮替的最小值。也就是日志一定要达到这个最小值才会轮替，否则就算时间达到也不轮替

size 大小 日志只有大于指定大小才进行日志轮替，而不是按照时间轮替。

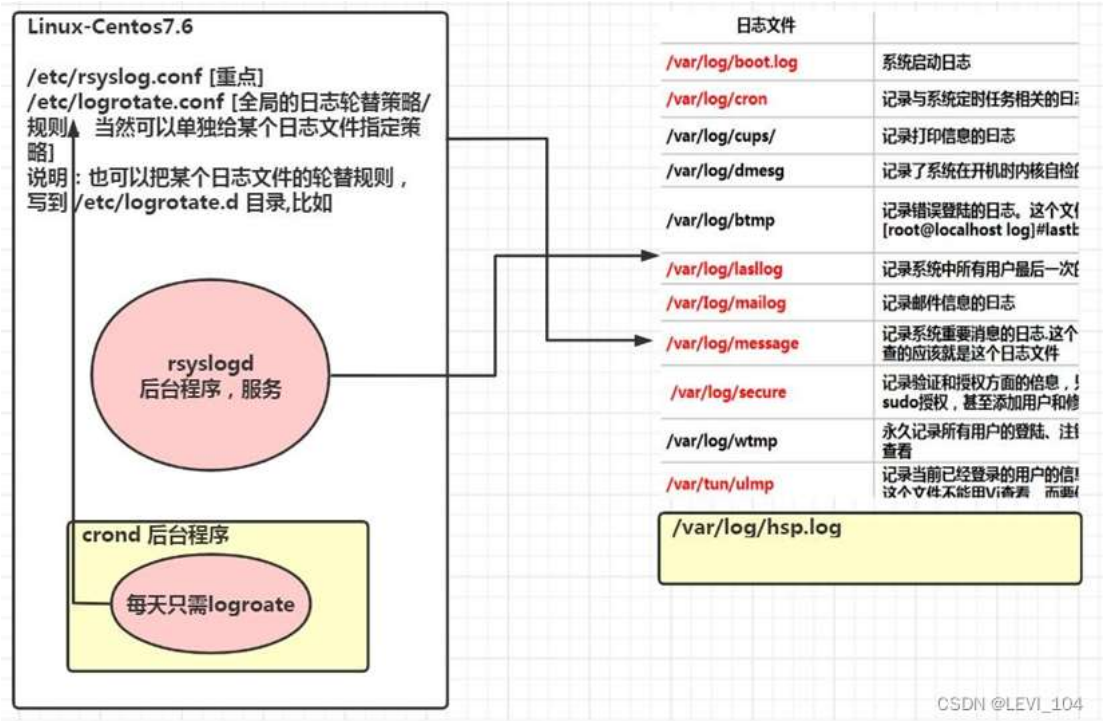
dateext 使用日期作为日志轮替文件的后缀。

sharedscripts 在此关键字之后的脚本只执行一次。prerotate/endscript 在日志轮替之前执行脚本命令。
postrotate/endscript 在日志轮替之后执行脚本命令。

把自己的日志加入日志轮替

1. 第一种方法是直接在/etc/logrotate.conf 配置文件中写入该日志的轮替策略
2. 第二种方法是在/etc/logrotate.d/目录中新建立该日志的轮替文件，在该轮替文件中写入正确的轮替策略，因为该目录中的文件都会被“include”
件中，所以也可以把日志加入轮替。
3. 推荐使用第二种方法，因为系统中需要轮替的日志非常多，如果全都直接写 入/etc/logrotate.conf 配置文件，那么这个文件的可管理性就会非
于此文件的维护。
4. 在/etc/logrotate.d/ 配置轮替文件一览

日志轮替原理图



查看内存日志

> journalctl 可以查看内存日志, 这里我们看看常用的指令
>
> journalctl ##查看全部journalctl -n 3 ##查看最新 3 条
>
> journalctl --since 19:00 --until 19:10:10 #查看起始时间到结束时间的日志可加日期journalctl -p err ##报错日志
>
> journalctl -o verbose ##日志详细内容
>
> journalctl _PID=1245 _COMM=sshd ##查看包含这些参数的日志（在详细日志查看） 或者 journalctl | grep
>
> 注意: journalctl 查看的是内存日志, 重启清空

定制自己的Linux系统

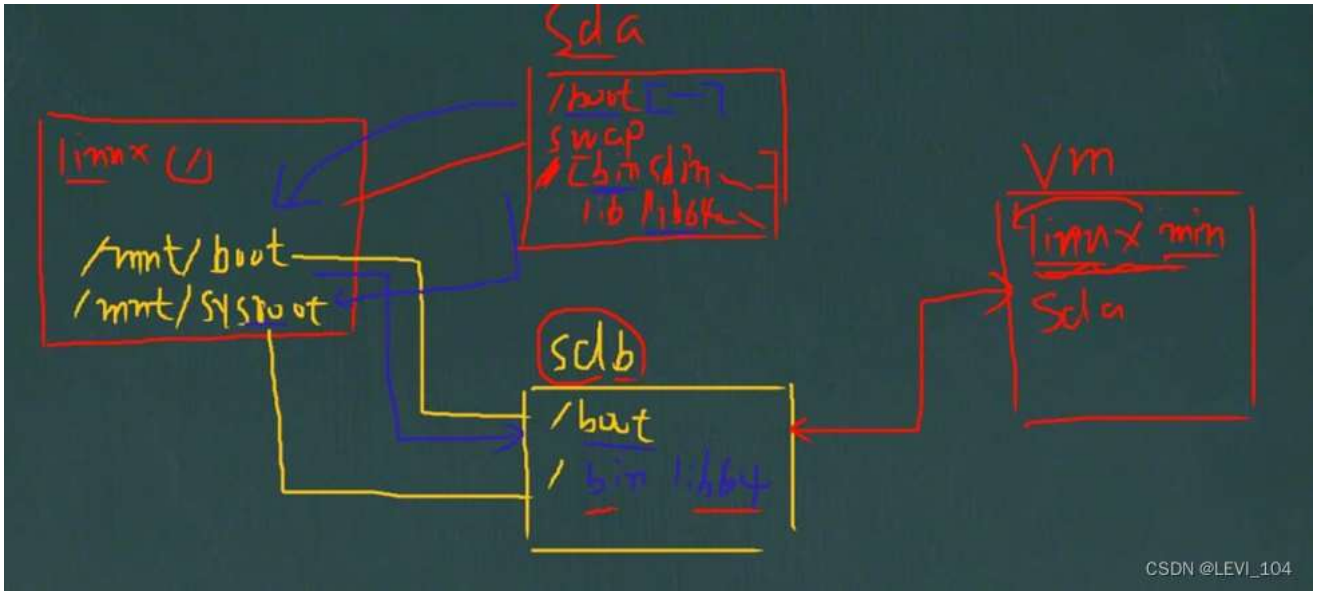
通过裁剪现有 Linux 系统(CentOS7.6)，创建属于自己的 min Linux 小系统

基本原理：

> 启动流程介绍：
>
> 制作 Linux 小系统之前，再了解一下 Linux 的启动流程：
>
> 1、首先 Linux 要通过自检，检查硬件设备有没有故障
>
> 2、如果有多块启动盘的话，需要在 BIOS 中选择启动磁盘
>
> 3、启动 MBR 中的 bootloader 引导程序
>
> 4、加载内核文件
>
> 5、执行所有进程的父进程、老祖宗 systemd 6、欢迎界面
>
> 在 Linux 的启动流程中，加载内核文件时关键文件： 1）kernel 文件: vmlinuz-3.10.0-957.el7.x86_64 2）initrd 文件: initramfs-3.10.0-957.el7.x86_64.img

制作min linux思路分析

1. 在现有的 Linux 系统(centos7.6)上加一块硬盘/dev/sdb，在硬盘上分两个分区，一个是/boot，一个是/，并将其格式化。需要明确的是，现在加在现有的 Linux 系统中是/dev/sdb，但是，当我们把东西全部设置好时，要把这个硬盘拔除，放在新系统上，此时，就是/dev/sda
2. 在/dev/sdb 硬盘上，将其打造成独立的 Linux 系统，里面的所有文件是需要拷贝进去的
3. 作为能独立运行的 Linux 系统，内核是一定不能少，要把内核文件和 initramfs 文件也一起拷到/dev/sdb 上
4. 以上步骤完成，我们的自制 Linux 就完成, 创建一个新的 linux 虚拟机，将其硬盘指向我们创建的硬盘，启动即可
5. 示意图

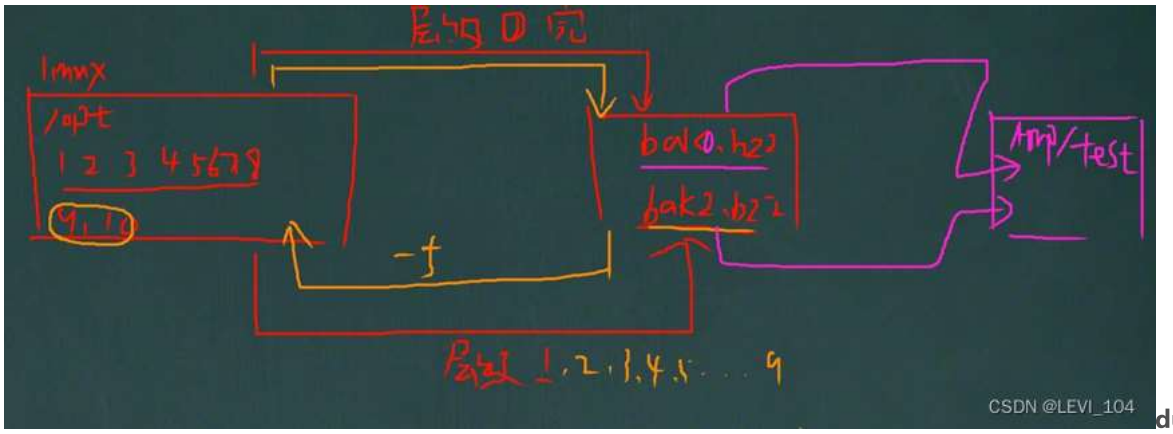


系统的备份与恢复

LEVI_104

实体机无法做快照，如果系统出现异常或者数据损坏，后果严重， 要重做系统，还会造成数据丢失。所以我们可以使用备份和恢复技术。linux 的备简单， 有两种方式：

1. 把需要的文件(或者分区)用 TAR 打包就行，下次需要恢复的时候，再解压开覆盖即可
2. 使用 dump 和 restore 命令。如果 linux 上没有 dump 和 restore 指令，需要先按照yum -y install dump和 yum -y install restore



dump备份

dump [-cu] [-0123456789] [-f<备份后的文件名>] [-T<日期>] [目录或文件系统]

dump [] -wW

> -c： 创建新的归档文件，并将由一个或多个文件参数所指定的内容写入归档文件的开头。
>
> -0123456789： 备份的层级。0 为最完整备份，会备份所有文件。若指定 0 以上的层级，则备份至上一次备份以来修改或新增的文件, 到 9 后，轮替.
>
> -f <备份后文件名>： 指定备份后文件名
>
> -j ：调用 bzlib 库压缩备份文件，也就是将备份后的文件压缩成 bz2 格式，让文件更小
>
> -T <日期>： 指定开始备份的时间与日期
>
> -u： 备份完毕后，在/etc/dumpdares 中记录备份的文件系统，层级，日期与时间等。
>
> -t： 指定文件名，若该文件已存在备份文件中，则列出名称
>
> -W： 显示需要备份的文件及其最后一次备份的层级，时间 ，日期。
>
> -w： 与-W 类似，但仅显示需要备份的文件。

dump备份文件或者目录

前面我们在备份分区时，是可以支持增量备份的，如果备份文件或者目录，不再支持增量备份, 即只能使用 0 级别备份

案例， 使用 dump 备份 /etc 整个目录

dump -0j -f /opt/etc.bak.bz2 /etc/

#下面这条语句会报错，提示 DUMP: Only level 0 dumps are allowed on a subdirectory dump -1j -f /opt/etc.bak.bz2 /etc/

restore备份

restore 命令用来恢复已备份的文件，可以从 dump 生成的备份文件中恢复原文件

格式：restore [模式选项] [选项]

> 说明下面四个模式， 不能混用，在一次命令中， 只能指定一种。
>
> -C： 使用对比模式，将备份的文件与已存在的文件相互对比。
>
> -i：使用交互模式，在进行还原操作时，restors 指令将依序询问用户
>
> -r：进行还原模式
>
> -t：查看模式，看备份文件有哪些文件
>
> 选项

> -f <备份设备>：从指定的文件中读取备份数据，进行还原操作

工具统计

宝塔bt，MySQL数据库，webmin

Linux的简单学习到此为止，接下来，可以继续学习以太坊了