需求：

1、保留 kern.log、messages、syslog

2、每过 10M 做一次压缩，保留两个压缩文件

3、每 24 小时判断一次大小

4、并且把 systemd 的日志管理关掉

所有服务的登录的文件或错误信息文件都在/var/log 下：

内核日志:/var/log/kern.log

包含内核产生的日志，有助于在定制内核时解决问题

系统报错日志:/var/log/messages

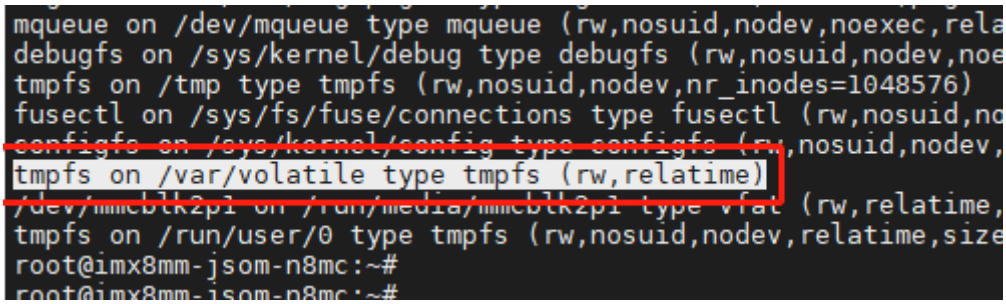
messages 日志是核心系统日志文件。它包含了系统启动时的引导消息，以及系统运行时的其他状态消息。IO 错误、网络错误和其他系统错误都会记录到这个文件中。

系统警告日志: /var/log/syslog

只记录警告信息，常常是系统出问题的信息，使用 lastlog 查看

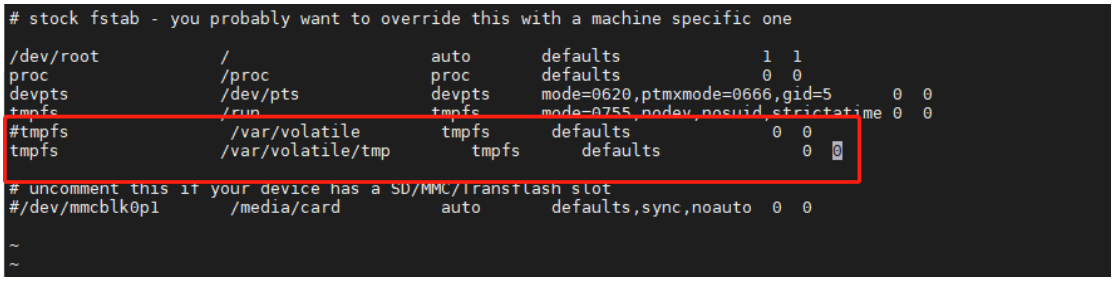
功能实现：

/var/log 本身是一个软链接，链接到了/var/volatile/log ；但是/var/volatile 目录本身是一个临时目录，每当关机时，里面的内容就会消失，所以导致默认情况下 log 目录里面只能存放当前开机的相关日志。



所以如果要保存多次的相关日志，首先要把 log 目录取消挂载在临时节点。这就需要修改文件：/etc/fstab

将挂载目录/var/volatile 修改为/var/volatile/tmp



logrotate 程序用来管理系统中的最新的事件，我们可以用它来备份日志文件。logrotate 的配置文件是 /etc/logrotate.conf。主要（部分）参数如下表：

参数	功能
compress	通过 gzip 压缩转储以后的日志
nocompress	不需要压缩时，用这个参数
copytruncate	用于还在打开中的日志文件，把当前日志备份并截断
nocopytruncate	备份日志文件但是不截断
create mode owner group	转储文件，使用指定的文件模式创建新的日志文件
delaycompress	和 compress 一起使用时，转储的日志文件到下一次转储时才压缩
nodelaycompress	覆盖 delaycompress 选项，转储同时压缩
errors address	转储时的错误信息发送到指定的 Email 地址
ifempty	即使是空文件也转储，这个是 logrotate 的缺省选项
notifempty	如果是空文件的话，不转储
mail address	把转储的日志文件发送到指定的 E-mail 地址
olddir directory	转储后的日志文件放入指定的目录，必须和当前日志文件在同一个文件系统
noolddir	转储后的日志文件和当前日志文件放在同一个目录下
prerotate/endscript	在转储以前需要执行的命令可以放入这个对，这两个关键字必须单独成行
postrotate/endscript	在转储以后需要执行的命令可以放入这个对，这两个关键字必须单独成行
daily/ weekly/ monthly	指定转储周期为每天/每周/每月
rotate n	指定日志文件删除之前转储的次数，0 指没有备份，5 指保留 5 个备份
dateext	指定转储后的日志文件以当前日期为格式结尾
dateformat	配合 dateext 使用，紧跟在下一行出现，定义日期格式，只支持%Y %m %d %s 这 4 个参数，如:dateformat -%Y%m%d%s
size size	当日志文件到达指定的大小时才转储，Size 可以指定 bytes (缺省)以及 KB (sizek)或者 MB (sizem)

编辑/etc/logrotate.conf 文件

```
# system-specific logs may also be configured here.

/var/log/kern.log
/var/log/messages
/var/log/syslog
{
        rotate 2      #保存 2 个备份
        daily         #每天转储
        missingok  #忽略错误

        notifempty #空文件不转储
        compress   #压缩
        nodelaycompress     #转储同时压缩
        sharedscripts       #所有的日志文件都转储完毕后统一执行一次脚本
        create              #建立新的日志文件
        size 10M            #文件到达 10M 才能转储
        dateext             #指定转储后的文件名以当前日期结尾
        dateformat -%Y%m%d%s    #日期格式
        postrotate          #转储后执行的命令放到该行下面
        echo "store-log ok" > /dev/ttymxc1    #转储后执行的命令
        endscript           #转储后执行的命令放到该行上面
}
```

至此，日志转储设置已经设置完毕。但是需要每天检查，日志文件是否达到转储条件，所以需要引入 crontab 定时任务。

crontab，用于设置周期性被执行的指令。该命令从标准输入设备读取指令，并将其存放于“crontab”文件中，以供之后读取和执行。通常，crontab 储存的指令被守护进程激活。“crontab -e”是每个用户都可以执行的命令，也就是说，不同的用户身份可以执行自己的定时任务。但是有些定时任务需要系统执行，这时就需要编辑 /etc/crontab 这个配置文件了。

crontab 的命令构成为 时间+动作，其时间有分、时、日、月、周五种，操作符有：

* 取值范围内的所有数字

/ 每过多少个数字

- 从 X 到 Z

，散列数字

关于文件/etc/crontab 的更多具体使用方法，可以自行百度

Linux Crontab 定时任务 | 菜鸟教程 (runoob.com)

编辑/etc/crontab

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

#  m   h   dom   mon   dow   user          command
   0   0    */1    *     *    root           logrotate   /etc/logrotate.conf
```

翻译过来就是：

每天的 0 时 0 分，以 root 身份运行命令：logrotate /etc/logrotate.conf

综上：每隔 1 天，就会执行一次转储命令，如果 log 文件达到 10M，就会进行压缩转储；并累计保留两个备份。

另：关闭 systemd 的日志管理

方法一：

关闭服务：`$ systemctl disable systemd-journald`

方法二：

打开/etc/systemd/journald.conf 文件，屏蔽所有内容

另，选择性保存日志文件：

打开/etc/syslog.conf 文件，不需要生成的 log 文件，屏蔽即可

```
# /etc/syslog.conf - Configuration file for syslogd(8)
#
# For information about the format of this file, see syslog.conf(5)
#


#
# First some standard log files.  Log by facility.
#
#auth,authpriv.*                         /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog

#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
kern.*                          -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
#mail.*                         -/var/log/mail.log
#user.*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
#mail.warn                      -/var/log/mail.warn
#mail.err                        /var/log/mail.err
#mail.*;mail.!=info             -/var/log/mail
#mail,news.=info                -/var/log/info
```