参考博客：https://www.cnblogs.com/liuwei-xd/p/11022230.html

日志管理基础

处理日志的进程

`rsyslogd`：绝大部分日志记录，和系统操作有关，安全，认证`sshd,su`，计划任务`at,cron`

`httpd/nginx/mysql`等等应用可以以自己的方式记录日志

```
[root@localhost ~]# ps aux |grep rsyslogd
root       6789  0.2  0.2 216416  4068 ?        Ssl  14:17   0:00
/usr/sbin/rsyslogd -n
```

日志可以存放在本地

日志可以存放在远程服务器

常见的日志文件(系统、进程、应用程序)

日志文件	作用描述
tail /var/log/messages	系统主日志文件
tail -20 /var/log/messages	
tail -f /var/log/messages	动态查看日志文件的尾部
tailf /var/log/secure	认证、安全
tail /var/log/maillog	和邮件postfix相关
tail /var/log/cron	crond、at进程产生的日志
tail /var/log/dmesg	和系统启动相关
tail /var/log/audit/audit.log	系统审计日志
tail /var/log/yum.log	yum
tail /var/log/mysqld.log	MySQL
tail /var/log/xferlog	访问FTP服务器相关
w	当前登录的用户 /var/log/wtmp
last	最近登录的用户 /var/log/btmp
lastlog	所有用户的登录情况 /var/log/lastlog

案例1:统计登录失败top5

```
[root@localhost ~]# grep 'Fail' /var/log/secure |awk '{print $11}' |sort |uniq -c |sort -k1 -n -r |head -5
    779 hadoop
    501 test
    261 183.240.132.21
    224 user
    21 195.54.160.183
```

案例2：统计登录成功

```
[root@localhost ~]# grep 'Accepted' /var/log/secure |awk '{print $(NF-3)}' |sort |uniq -c
      4 117.90.214.165
      2 122.194.35.187
```

案例3：查看网卡是否已被驱动

```
[root@localhost ~]# grep -i eth /var/log/dmesg
[    2.090634] e1000 0000:02:01.0 eth0: (PCI:66MHz:32-bit) 00:0c:29:bb:9a:bb
[    2.090642] e1000 0000:02:01.0 eth0: Intel(R) PRO/1000 Network Connection
```

rsyslogd子系统

```
[root@localhost ~]# rpm -qc rsyslog
/etc/logrotate.d/syslog     # 日志轮转(切割)相关
/etc/rsyslog.conf           # rsyslogd的主配置文件
/etc/sysconfig/rsyslog      # rsyslogd相关文件
```

```
[root@localhost ~]# vim /etc/rsyslog.conf
# 告诉rsyslogd进程 哪个设备(facility)，关于哪个级别的信息，以及如何处理
authpriv.*                                              /var/log/secure
mail.*                                                  -/var/log/maillog
cron.*                                                  /var/log/cron
*.emerg                                                 :omusrmsg:*
authpriv.*                                              *                       # 所有终端
authpriv.*                                              @192.168.1.123          # UDP
authpriv.*                                              @@192.168.1.123         # TCP
```

设备facility相关内容，查看man手册https://man7.org/linux/man-pages/man3/syslog.3.html

设备类型(表示日志类型)	解释
LOG_AUTHPRIV	安全认证
LOG_CRON	cron 和 at
LOG_DAEMON	后台进程
LOG_FTP	ftp进程
LOG_KERN	内核信息
LOG_LOCAL0 through LOG_LOCAL7	用户自定义设备
LOG_LPR	打印机子系统
LOG_MAIL	邮件系统
LOG_NEWS	新闻子系统
LOG_SYSLOG	syslogd自身产生的日志

级别(日志重要级别)	解释
LOG_EMERG	紧急，致命，服务无法继续运行，如配置文件丢失
LOG_ALERT	报警，需要立即处理，如磁盘空间使用95%
LOG_CRIT	致命行为
LOG_ERR	错误行为
LOG_WARNING	警告信息
LOG_NOTICE	普通
LOG_INFO	标准信息
LOG_DEBUG	调试信息，排错才开，一般不建议使用

- 案例1
  - 将authpriv设备日志记录到/var/log/auth.log
- 案例2
  - 改变应用程序sshd的日志设备为local5,并定义local5设备日志记录到/var/log/local5.local
- 案例3
  - 使用logger程序写日志到指定的设备及级别

```
logger "run....."
logger -p emerg "run......"
logger -p authpriv.info "run......"
```

案例， rsyslog远程管理日志

- 修改server1的rsyslog.conf配置文件，打开tcp、udp监听端口

```
[root@server1 httpd]# vim /etc/rsyslog.conf
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

- 重启rsyslog，检查端口是否在监听

```
[root@server1 ~]# yum install net-tools -y
[root@server1 ~]# netstat -nltup |grep 514
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
   1342/rsyslogd
tcp6       0      0 :::514                  :::*                    LISTEN
   1342/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*
  1342/rsyslogd
udp6       0      0 :::514                  :::*
   1342/rsyslogd
```

- 修改server2的ssh配置文件，将日志发送到local0中

```
[root@server2 ~]# vim /etc/ssh/sshd_config
SyslogFacility LOCAL0
```

- 修改server2的rsyslog.conf

```
[root@server2 ~]# vim /etc/rsyslog.conf
local0.*                                                @192.168.80.193
[root@server2 ~]# systemctl restart rsyslog.service
```