

# 日志服务以及配置

## 一、rsyslog系统日志管理

什么程序 → 产生的什么日志 → 放到什么地方

### 1.处理日志的进程

- rsyslogd进程：系统的专职日志程序

处理绝大部分日志记录，系统操作有关的信息，如登录信息，程序启动关闭信息，错误信息等

```
[root@xnha rsyslog.d]# ps aux |grep rsyslog
root      1203  0.0  0.1 217256 7048 ?        Ssl  04:13   0:00 /usr/sbin/rsyslogd -n
root      5149  0.0  0.0 12320   968 pts/0    S+   08:21   0:00 grep --color=auto rsyslog
[root@xnha rsyslog.d]#
```

- httpd/nginx/mysql: 各类应用程序，可以以自己的方式记录日志

httpd的日志文件 /var/log/httpd 下的 access\_log和error\_log

```
[root@xnha httpd]# ll
总用量 12
-rw-r--r--. 1 root root    0 3月  11 11:16 access_log
-rw-r--r--. 1 root root 1033 3月  16 09:01 error_log
-rw-r--r--. 1 root root 6104 3月  12 21:49 error_log-20250316
[root@xnha httpd]# cat error_log
[Sun Mar 16 09:01:06.592820 2025] [core:notice] [pid 5828:tid 140275104102656] SELinux policy enabled; httpd
:system_r:httpd.t:s0
[Sun Mar 16 09:01:06.594840 2025] [suexec:notice] [pid 5828:tid 140275104102656] AH01232: suEXEC mechanism en
uexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::20c:29ff:f
me' directive globally to suppress this message
[Sun Mar 16 09:01:06.603977 2025] [lbmethod:heartbeat:notice] [pid 5828:tid 140275104102656] AH02282: No slot
[Sun Mar 16 09:01:06.604437 2025] [http2:warn] [pid 5828:tid 140275104102656] AH02951: mod_ssl does not seem
[Sun Mar 16 09:01:06.611781 2025] [mpm_event:notice] [pid 5828:tid 140275104102656] AH00489: Apache/2.4.37 (c
ng normal operations
[Sun Mar 16 09:01:06.611802 2025] [core:notice] [pid 5828:tid 140275104102656] AH00094: Command line: '/usr/s
[root@xnha httpd]#
```

### 2.常见的日志文件(系统、进程、应用程序)

- 各种日志的存放位置 /var/log
- /etc/rsyslog.d/: 目录下为各服务/应用的专用配置 (如 ssh.conf)。

```
[root@xnha rsyslog.d]# ls /var/log
anaconda      cron-20250316      maillog          spooler          vmware-network.8.log
audit         cups               maillog-20250309 spooler-20250309 vmware-network.9.log
boot.log      dnf.librepo.log   maillog-20250316 spooler-20250316 vmware-network.log
boot.log-20250306 dnf.log           messages         sssd             vmware-vgauthsvc.log.0
boot.log-20250309 dnf.rpm.log       messages-20250309 swtpm            vmware-vmvsvc.log
boot.log-20250310 firewallld         messages-20250316 test.txt         vmware-vmusr.log
boot.log-20250311 gdm               private          tuned            wtmp
boot.log-20250312 glusterfs         qemu-ga          vmware-network.1.log Xorg.0.log
boot.log-20250314 hawkey.log        README           vmware-network.2.log Xorg.0.log.old
boot.log-20250316 hawkey.log-20250309 samba            vmware-network.3.log Xorg.9.log
btmtp         hawkey.log-20250316 secure           vmware-network.4.log
chrony        httpd              secure-20250309  vmware-network.5.log
cron          lastlog            secure-20250316  vmware-network.6.log
cron-20250309 libvirt            speech-dispatcher vmware-network.7.log
```

- 系统的主日志文件 /var/log/messages

```
[root@xnha rsyslog.d]# cd /var/log
[root@xnha log]# tail -f messages
Mar 16 07:29:05 xnha org.gnome.Terminal.desktop[4572]: # unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
Mar 16 07:29:05 xnha org.gnome.Terminal.desktop[4572]: # watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
Mar 16 08:07:09 xnha cupsd[1079]: REQUEST localhost - - "POST / HTTP/1.1" 200 183 Renew-Subscription successful-ok
Mar 16 08:21:07 xnha journal[2413]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Mar 16 08:21:15 xnha journal[2413]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Mar 16 08:21:21 xnha journal[2413]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Mar 16 08:24:46 xnha kernel: hrtimer: interrupt took 9308800 ns
Mar 16 08:27:24 xnha systemd[1]: Starting dnf makecache...
Mar 16 08:27:24 xnha dnf[5221]: 元数据缓存近期已刷新。
Mar 16 08:27:24 xnha systemd[1]: Started dnf makecache.
Mar 16 08:28:37 xnha journal[2413]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
```

时间 主机名 应用程序: 日志内容

- 系统中记录认证、安全的日志 /var/log/secure

- 和邮件Postfix相关的日志 `/var/log/maillog`
- 计划任务相关的日志 `/var/log/cron`
- 系统审计日志 `/var/log/audit/audit.log`
- 当前登录的用户 `/var/log/wtmp`，使用last命令进行查看

#### 基本用法：

```
last -f /var/log/wtmp      # 查看所有登录记录（按文件格式解析）
last -t 2023-10-01       # 查看指定日期的记录
last -u username          # 过滤特定用户的登录记录
```

- 最近登录的用户 `/var/log/btmp`
- 所有用户的登录情况 `/var/log/lastlog`

## 3、rsyslogd配置

### 1.相关程序

- `yum install rsyslog logrotate`
- 默认已安装

### 2.启动程序

- `systemctl start rsyslog.service`

### 3.相关文件

```
[root@xnha etc]# rpm -qc rsyslog
/etc/logrotate.d/syslog
/etc/rsyslog.conf
/etc/sysconfig/rsyslog
```

```
[root@xnha etc]# rpm -qc rsyslog
/etc/logrotate.d/syslog
/etc/rsyslog.conf
/etc/sysconfig/rsyslog
[root@xnha etc]#
```

- `/etc/rsyslog.conf`
  - rsyslogd的主配置文件（关键）
- `/etc/sysconfig/rsyslog`
  - rsyslogd相关文件，定义级别（了解一下）
- `/etc/logrotate.d/syslog`
  - 和日志轮转（切割）相关

#### //观察日志程序的配置文件

## 4. 主配置文件

告诉rsyslogd进程什么日志，应该存到哪里。

```
vim /etc/rsyslog.conf
```

### RULES

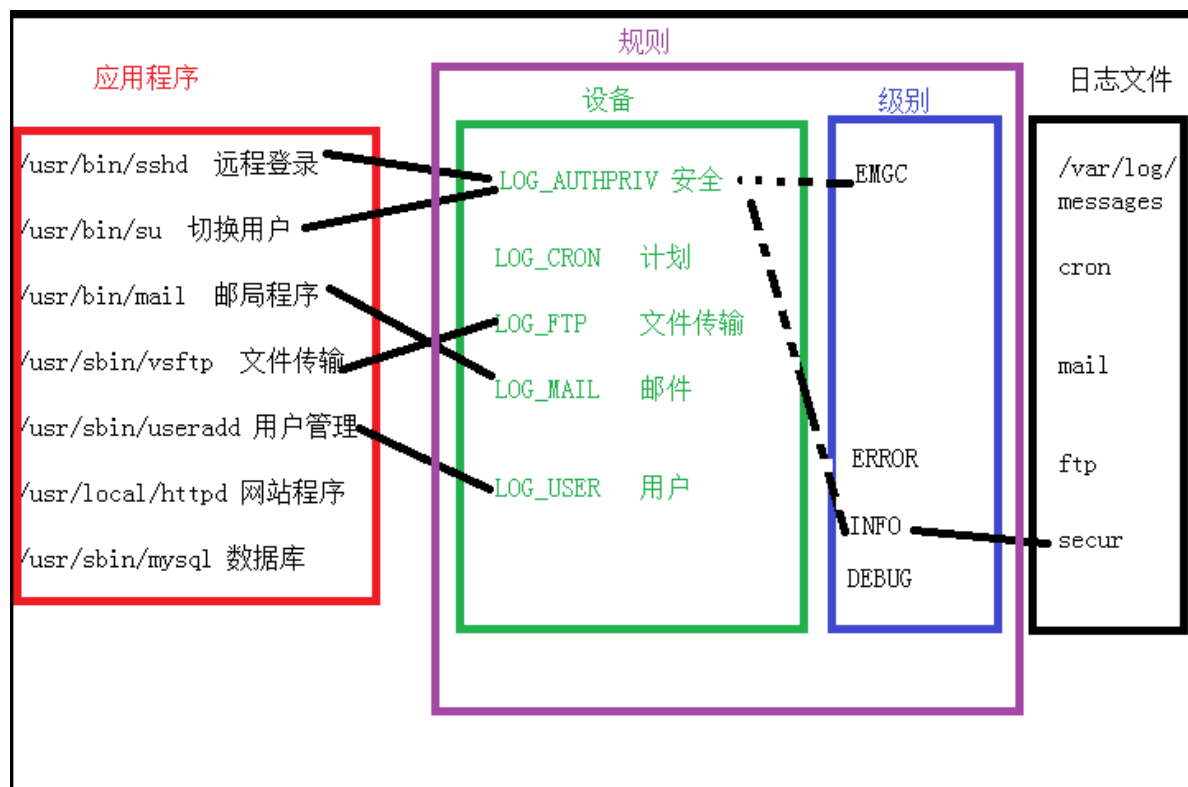
- RULES：即规则，是一套生成日志，以及存储日志的策略。
- RULES由三部分组成（FACILITY+LEVEL+FILE）
  - 设备+级别+存放位置
- authpriv.\* /var/log/secure (SSH信息)
- mail.\* -/var/log/maillog (发邮件)
- cron.\* /var/log/cron (创建任务)
  - 这里有一个-符号, 表示是使用异步的方式记录, 因为日志一般会比较大会比较大
- \*.info;mail.none;authpriv.none;cron.none /var/log/messages
- 系统日志排除了邮件，认证，计划日志。

### FACILITY和LEVEL

- facility设备
  - 是系统对某种类型APP事件的定义。如AUTHPRIV是安全事件，CRON是计划任务事件。用来收集同类程序日志。
  - 设备类型，使用 `man 3 syslog` 查看； 3：手册
    - LOG\_SYSLOG
      - syslogd自身产生的日志
    - LOG\_AUTHPRIV
      - 安全认证
    - LOG\_CRON
      - 调度程序(cron and at)
    - LOG\_MAIL
      - 邮件系统mail subsystem
    - LOG\_USER (default)
      - 用户相关
    - LOG\_DAEMON
      - 后台进程
    - LOG\_FTP
      - 文件服务器ftp daemon
    - LOG\_KERN
      - 内核设备kernel messages
    - LOG\_LPR
      - 打印机设备
      - printer subsystem
    - LOG\_LOCAL0 through LOG\_LOCAL7
      - 用户自定义设备
- level级别（从下到上，级别从低到高，记录的信息越来越少）

- 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，重要的标准信息
- LOG\_INFO 标准信息
- LOG\_DEBUG 调试信息，排错所需，一般不建议使用

规则示意图



## 5.实验1

关于程序和设备的联系问题，程序自身会决定将日志交给哪类设备。

如SSH程序会选择安全类设备。这一点由开发者定义。

### 1.修改ssh程序的设备类型

```
vim /etc/ssh/sshd_config
```

将原本要记录到认证日志中的内容修改为记录到Local5中；local自定义

```
# For more information, see manual page for

# Logging
#SyslogFacility AUTH
#SyslogFacility AUTHPRIV
SyslogFacility LOCAL5
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

## 2.修改rsyslog程序的规则

```
vim /etc/rsyslog.conf
```

```
local5.*      /var/log/serverzz
```

```
# Save boot messages also to boot.log
local7.*      /var/log/boot.log

local5.*      /var/log/mysshlog
```

## 3.重启rsyslog程序和ssh程序

```
[root@xnha etc]# systemctl restart sshd rsyslog.service
```

## 4.使用其他终端登录服务器，观察新日志文件。

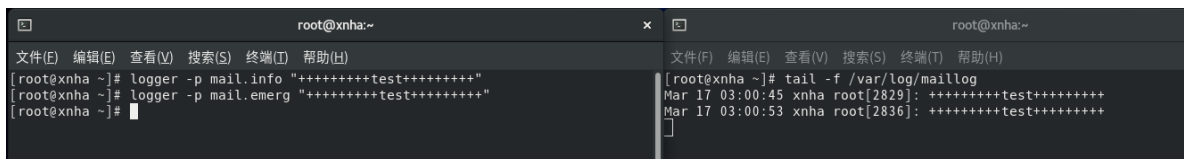
- 登陆后

```
[root@xnha log]# cat mysshlog
Mar 16 09:35:51 xnha sshd[6632]: Received signal 15; terminating.
Mar 16 09:35:51 xnha sshd[6671]: Server listening on 0.0.0.0 port 22.
Mar 16 09:35:51 xnha sshd[6671]: Server listening on :: port 22.
[root@xnha log]#
```

## 6.实验2

手动触发日志

```
[root@xnha ~]# logger -p mail.info "+++++++test++++++"
```



```
root@xnha:~
文件(E) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[root@xnha ~]# logger -p mail.info "+++++++test++++++"
[root@xnha ~]# logger -p mail.emerg "+++++++test++++++"
[root@xnha ~]#

root@xnha:~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[root@xnha ~]# tail -f /var/log/maillog
Mar 17 03:00:45 xnha root[2829]: ++++++test++++++
Mar 17 03:00:53 xnha root[2836]: ++++++test++++++
```

# 二、logrotate日志轮转

## 1. 简介

日志 记录了程序运行时各种信息。

通过日志可以分析用户行为，记录运行轨迹，查找程序问题。

可惜磁盘的空间是有限的

日志轮转就像飞机里的黑匣子，记录的信息再重要也只能记录最后一段时间发生的事。

为了节省空间和整理方便，日志文件经常需要按时间或大小等维度分成多份，删除时间久远的日志文件。

## 2. 工作原理

### 按照配置进行轮转

- 配置文件种类
  - 主配置文件: /etc/logrotate.conf
    - (决定每个日志文件如何轮转)
  - 子配置文件夹: /etc/logrotate.d/\*
    - 自定义配置
    - 便于管理
- 观察主文件和子文件

主文件 /etc/logrotate.conf

```
[root@xnha log]# cat -n /etc/logrotate.conf
 1 # see "man logrotate" for details
 2 # rotate log files weekly
 3 weekly
 4
 5 # keep 4 weeks worth of backlogs
 6 rotate 4
 7
 8 # create new (empty) log files after rotating old ones
 9 create
10
11 # use date as a suffix of the rotated file
12 dateext
13
14 # uncomment this if you want your log files compressed
15 #compress
16
17 # RPM packages drop log rotation information into this directory
18 include /etc/logrotate.d
19
20 # system-specific logs may be also be configured here.
```

子文件 /etc/logrotate.d

```
[root@xnha log]# ls /etc/logrotate.d/
bootlog  chrony  dnf      iscsiuiolog  libvirtd.qemu  psacct  sssd     up2date      wtmp
btmtp    cups    httpd    libvirtd     numad          samba   syslog   wpa_supplicant
```

## 3. 主配置文件介绍

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

## 全局设置

```
weekly      //轮转的周期，一周轮转
rotate 4     //保留4份
create      //轮转后创建新文件          把旧文件按照轮转要求改名字，eg:boot.log-20250316
dateext     //使用日期作为后缀
include /etc/logrotate.d    //包含该目录下的子配置文件
```

## 独立设置

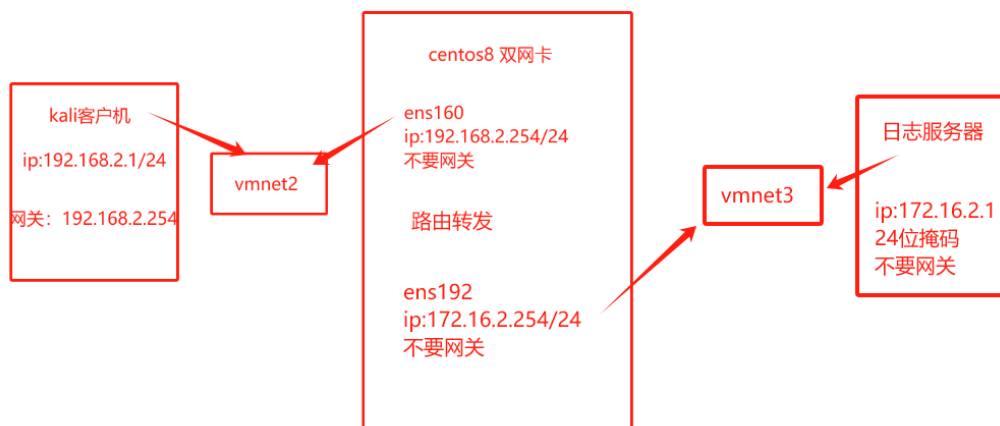
```
[root@xnha logrotate.d]# cat wtmp
# no packages own wtmp -- we'll rotate it here
/var/log/wtmp {
    missingok          #在日志轮转时，如果目标文件不存在，跳过报错并继续执行轮转。
    monthly            #设置轮转频率为每月一次
    create 0664 root utmp
    minsize 1M         #当wtmp文件大小达到1MB时触发轮转（即使未到每月周期）
    rotate 1           #仅保留最近一次轮转的备份文件，旧备份自动删除（每月轮转一次，最多保
留1个月的历史日志）
}

[root@xnha logrotate.d]# cat btmp
# no packages own btmp -- we'll rotate it here
/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}
```

## 三、异地备份

### 1.拓扑说明

按照图示配置网络，其中日志服务器位centos8 的克隆机即可



## 2.实验目标

模拟黑客暴力破解攻击，攻击成功后可能会登录到目标服务器中清除攻击日志，为方便审计，将centos8中的日志备份至日志服务器。

## 3. 操作

### 1、配置日志客户机

- 修改日志服务的配置文件

```
77 # ### begin forwarding rule ###          转发规则
78 # The statement between the begin ... end define a SINGLE forwarding
79 # rule. They belong together, do NOT split them. If you create multiple
80 # forwarding rules, duplicate the whole block!
81 # Remote Logging (we use TCP for reliable delivery)
82 #
83 # An on-disk queue is created for this action. If the remote host is
84 # down, messages are spooled to disk and sent when it is up again.
85 # $ActionQueueFileName fwdRule1 # unique name prefix for spool files
86 # $ActionQueueMaxDiskSpace 1g    # 1gb space limit (use as much as possible)
87 # $ActionQueueSaveOnShutdown on  # save messages to disk on shutdown
88 # $ActionQueueType LinkedList    # run asynchronously
89 # $ActionResumeRetryCount -1     # infinite retries if host is down
90 # remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
91 #*. * @remote-host:514           登录验证进程的info级别日志 用tcp协议发送给172.16.2.1 514
92 authpriv.info @172.16.2.1:514   端口 @@TCP 协议 @UDP协议
93 # ### end of the forwarding rule ###
```

- 一定要重启服务才能生效

```
systemctl restart rsyslog
```

### 2、配置日志服务器

```
1 # rsyslog configuration file
2
3 # For more information see /usr/share/doc/rsyslog-*/rsyslog
4 # If you experience problems, see http://www.rsyslog.com/do
5
6 ##### MODULES #####
7
8 # The imjournal module bellow is now used as a message sour
9 $ModLoad imuxsock # provides support for local system loggi
10 $ModLoad imjournal # provides access to the systemd journal
11 # $ModLoad imklog # reads kernel messages (the same are read
12 # $ModLoad immark # provides --MARK-- message capability
13
14 # Provides UDP syslog reception
15 # $ModLoad imudp
16 # $UDPServerRun 514
17
18 # Provides TCP syslog reception
19 $ModLoad imtcp
20 $InputTCPServerRun 514          开启tcp协议以及514端口
21
:set nu
```

- 同时添加规则



```

90 # ## end of the forwarding rule ##
91 # ### end of the forwarding rule ###
92 #fromhost-ip, isequal, "172.16.2.254" /var/log/nz2002log/172.16.2.254.log

```

根据ip地址接收      等于      "值"      保存位置

- 重启服务验证

```

[root@localhost ~]# systemctl restart rsyslog
[root@localhost ~]# ss -antpl
State      Recv-Q  Send-Q  Local Address:Port  Peer Address:Port
LISTEN     0       25      *:514               *:
users: ( ("rsyslogd",pid=57321,fd=3))
LISTEN     0       128     *:111               *:
users: ( ("rpcbind",pid=699,fd=8))
LISTEN     0       128     *:22                *:
users: ( ("sshd",pid=1010,fd=3))

```

### 3、验证日志是否会被发送过来

- 使用kail进行ssh爆破



```

Xshell 4 (Build 0129)
Copyright (c) 2002-2013 NetSarang Computer, Inc. All rights reserved.

```

```

Type `help` to learn how to use Xshell prompt.
xshell:\>

```



```

Connecting to 192.168.2.254:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

```

```

Last login: Thu Jun 18 11:31:03 2020
[root@localhost ~]#

```

win主机触发登录

### 4、日志服务器验证日志接收