syslog——日志管理

syslog 已被许多日志函数采纳，用在许多保护措施中，任何程序都可以通过 syslog 记录事件。syslog 可以记录系统事件，可以写到一个文件或设备中，或给用户发送一个信息。它能记录本地事件或通过网络记录另一个主机上的事件。

1、syslog 组成：

1）syslogd：主要记录系统和网络等服务的日志信息;

2）klogd：主要记录内核产生的各项信息;

3）logretate：主要用来对日志文件进行切割循环记录等.

2、syslog 特点：

1）多线程工作;

2）支持以 TCP、UDP、SSL、TSL、RELP 协议和加密完成远程日志的记录;

3）支持在开源的关系型数据库 MYSQL、PGSQL 等之上记录日志信息;

4）它还是一个强大的系统过滤器，可实现过滤系统信息的任意部分;

5）自定义的输出格式.

3、syslog 中的术语

(1) facility，消息类型

kern	内核产生的日志信息
lpr	与打印系统相关的信息
mail	与邮件系统相关的信息
security	security 与安全相关的信息
syslog	syslogd 程序自身产生信息
user, uucp, local[0-7]	系统本身产生的信息，以及服务自定义使用

(2)priority，常用的优先级

等级	等级名称	描　　述
1	info	仅仅是一些基本信息的说明
2	notice	比 info 更需要注意的一些说明
3	warning、warm	警告信息，但不至于影响应用程序的运行
4	err、error	一些重大的错误日志，已经影响了应用程序的运行
5	crit	比 error 还要重要的错误信息
6	alert	已经是有严重级别的错误信息，比 crit 更严重
7	emerg、panic	内核已出现了恐慌
8	debug	调试信息，通常用于应用程序的调试过程

注：不同的服务类型有不同的优先级，**数值较大的优先级涵盖数值较小的优先级**

syslog 允许使用三种限定符对优先级进行修饰：星号(*)、等号(=)、叹号(!)：

星号(*)：把本项服务生成的所有日志消息都发送到操作动作指定的地点。“mail.*”将把所有优先级的消息都发送到操作动作指定的/var/log/mail 文件里。使用“*”限定符与使用“debug”优先级的效果完全一样，后者也将把所有类型的消息发送到指定地点。

等号(=)：只把本项服务生成的本优先级的日志消息都发送到操作动作指定的地点。例：可以用“=”限定符只发送调试消息而不发送其他更紧急的消息(这将为应用程序减轻很多负担)。当你只需要发送特定优先级别的消息时，就要使用等号限定符。

叹号(!)：把本项服务生成的所有日志消息都发送到操作动作指定的地点，但本优先级的消息不包括在内。

3、target，动作

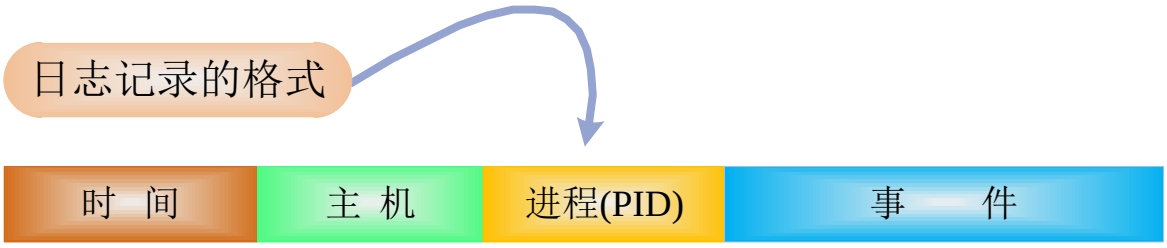
记录日志后的处理方式：

(1)保存到本地文件：在文件路径之前使用“-”，表示异步写入；

(2)通知用户：将日志信息通知指定用户，*表示所有用户；

(3)发送到远程日志服务器：日志服务器地址 @SERVER，此时服务器开启 rsyslog 服务且必须要监听在 tvp 或 udp 协议的 514 端口上；

(4)管道二次处理：可以通过管道命令送给某个命令进行处理|COMMAND。



4、系统自带的查看日志命令：

(1)成功登陆系统的记录日志：/var/log/wtmp，查看命令：last

(2)登陆系统失败的记录日志：/var/log/btmp，查看命令：lastb

(3)当前系统上每个用户各自最近一次登陆系统信息，查看命令：lastlog

5、logrotate，循环切割日志：

可配合 cron 定期的对日志文件进行处理，只要通过/etc/cron.daily/logrotate 程序来处理，配置文件：/etc/logrotate.conf（主配置文件）、/etc/logrotate.d/*

```
[root@node1 ~]#vim /etc/logrotate.conf
weekly                                  #默认每周对登录文件进行一次切割
```

```
rotate 4                                #保留多少个登录文件，默认是四个
dateext                                 #以日期作为文件的后缀名
create                                  #由于登录文件被更名，因此创建一个新的来继续记录
include /etc/logrotate.d                #将这个目录下的所有文件都读过来。许多服务的主配置文件里都有这个
/var/log/wtmp {
        monthly                         #每月一次
        create 0664 root utmp           #指定新建文件的权限与所属账号/群组
        minsize 1M                      #文件容量超过 1M 后才切割
        rotate 1                        #仅保留一个，即仅有 wtmp.1 保留
}
/var/log/btmp {
        missingok                       #表示如果找不到 log 文件也 OK
        monthly                         #每月一次
        create 0600 root utmp           #文件容量超过 1M 后才切割
        rotate 1                        #仅保留一个，即仅有 wtmp.1 保留
}
```

6、日志服务器的设置：

设置为日志服务器，需要在服务器端加载 syslog 中两个模块，以及监听 UDP 的 514 端口，重启服务：

```
[root@node1 ~]#vim /etc/rsyslog.conf
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514
[root@node1 ~]#service rsyslog restart
```

日志服务器客户端如下配置：

```
[root@node2 ~]#vim /etc/rsyslog.conf
*.info                                  @log_server
[root@node1 ~]#service rsyslog restart
```

7、/etc/rsyslog.conf 配置文件介绍：

```
[root@node2 ~]#vim /etc/rsyslog.conf
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat       #使用默认的时间戳
$IncludeConfig /etc/rsyslog.d/*.conf                           #包含进所有文件
##       Usage: facility(日志类型).priority(日志优先级)          target(保存方式)
# 表示将所有 facility 的 info 级别,但不包括 mail,authpriv,cron 相关的信息,记录到/var/log/messages 文件
```

```
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
# 表示将权限,授权相关的所有基本的信息,记录到/var/log/secure 文件中.这个文件的权限是 600
authpriv.*                                              /var/log/secure
# 表示将 mail 相关的所有基本的信息记录到/var/log/maillog 文件中,"-" 表示异步写入磁盘,
mail.*                                                  -/var/log/maillog
# 表示将任务计划相关的所有级别的信息记录到/var/log/cron 文件中
cron.*                                                  /var/log/cron
# 表示将所有 facility 的 emerg 级别的信息,发送给登录到系统上的所有用户
*.emerg                                                 *
# 表示将 uucp 及 news 的 crit 级别的信息记录到/var/log/spooler 文件中
uucp,news.crit                                          /var/log/spooler
# 表示将 local7 的所有级别的信息记录到/var/log/boot.log 文件中,
# local0 到 local7 这 8 个是用户自定义使用的,这里的 local7 记录的是系统启动相关的信息
local7.*                                                /var/log/boot.log
[root@node1 ~]#service rsyslog restart
## 注：修改完/etc/rsyslog.conf 后切记重启服务
```

附录：

常见日志文件及作用

/var/log/cron 记录了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，可使用 dmesg 命令查看内核自检信息。

/var/log/btmp 记录错误登录的日志，是二进制文件，不能直接 vi 查看，要用 lastb 命令查看；

/var/log/lastlog 记录系统中所有用户最后一次的登录时间的日志。用 lastlog 命令查看。

/var/log/mailog 记录邮件信息；

/var/log/message 记录系统重要信息的日志，记录 Linux 系统的绝大多数重要信息，如果系统出现问题，首先要检查的就是应该是这个日志文件；

/var/log/secure 记录验证和授权方面的信息，只要涉及账户和密码的程序都会记录。比如说系统的登录，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；

/var/log/wtmp 永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。使用 last 命令来查看；

/var/run/utmp 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，文件不能直接 vi，要使用 w，who，users 等命令；

参考链接：http://www.178linux.com/52733