syslog

Linux日志机制的核心是rsyslog守护进程

该服务负责监听Linux下的日志信息，并把日志信息追加到对应的日志文件中，一般在/var/log目录下。

它还可以把日志信息通过网络协议发送到另一台Linux服务器上，或者将日志存储在MySQL或Oracle等数据库中。

配置文件

rsyslog的配置文件在 /etc/rsyslog.conf和 /etc/rsyslog.d/ 目录内的文件。 rsyslog.conf文件配置了rsyslog守护进程在哪里保存日志信息。

rsyslog.conf 配置文件主要包括以下几个部分：

全局配置

配置ryslog守护进程的全局属性，比如主信息队列大小（$MainMessageQueueSize），加载外部模块($ModLoad)等等。

规则（选择器+动作）

每个规则行由两部分组成，selector部分和action部分，这两部分由一个或多个空格或tab分隔，selector部分指定源和日志等级，action部分指定对应的操作。

选择器 SELECTORS

selector也由两部分组成，设施和优先级，由点号.分隔。第一部分为消息源或称为日志设施，第二部分为日志级别。

日志设施有：

auth(security), authpriv: 授权和安全相关的消息

kern: 来自Linux内核的消息

mail: 由mail子系统产生的消息

cron: cron守护进程相关的信息

daemon: 守护进程产生的信息

news: 网络消息子系统

lpr: 打印相关的日志信息

user: 用户进程相关的信息

local0 to local7: 保留，本地使用

日志级别有(升序)：

debug：包含详细的开发情报的信息，通常只在调试一个程序时使用。

info：情报信息，正常的系统消息，比如骚扰报告，带宽数据等，不需要处理。

notice： 不是错误情况，也不需要立即处理。

warning： 警告信息，不是错误，比如系统磁盘使用了85%等。

err：错误，不是非常紧急，在一定时间内修复即可。

crit：重要情况，如硬盘错误，备用连接丢失。

alert：应该被立即改正的问题，如系统数据库被破坏，ISP连接丢失。

emerg：紧急情况，需要立即通知技术人员。

日志设置样例:

cron.\* /var/log/cron

把所有来自cron守护进程的消息保存到/var/log/cron文件中。

mail.warn /var/log/mail.warn

当指定日志级别时，所有等于或大于该日志等级的信息都要被处理。比如上面的例子中，mail子系统所有warning及以上信息的日志都保存在/var/log/mail.warn文件中。

怎样指定一个日志的级别？

比如我们只想保留info信息，可以使用下面的写法：

mail.=info /var/log/mail.info

使用=可以指定日志等级

除了指定某一类的日志，还可以使用!排除这类信息，比如：

mail.!info /var/log/mail.info

动作 ACTION

action是规则描述的一部分，规则用于处理消息。总的来说，消息内容被写到一种日志文件上，但也可以执行其他动作，比如写到数据库表中或转发到其他主机。

action的配置：

保存到文件，cron.\* -/var/log/cron.log如果路径前有-则表示每次输出日志时不同步（fsync）指定日志文件。 （如果系统崩溃，会丢失日志，但是这样可以提高日志性能）文件路径既可以是静态文件也可以是动态文件。动态文件由模板前加 ? 定义。

通过网络发送日志 格式如下： @[()]:[] @ 表示使用 UDP 协议。@@ 表示使用 TCP 协议。 可以为： z 表示使用 zlib 压缩，NUMBER 表示压缩级别。多个选项 使用 , 分隔。 例如：

. @192.168.0.1 # 使用UDP 发送日志到 192.168.0.1

.@@example.com:18 # 使用 TCP 发送到 "example.com" 的 18 端口

. @(z9)[2001::1] # 使用 UDP 发送消息到 2001::1，启用 zlib 9 级压缩

cron.\* ~ 丢弃所有信息，即该配置之后的动作不会看到该日志。 随 rsyslog 版本不同，如果有如下警告信息，则将 ~ 修改为 stop。

模板

模板允许你指定日志信息的格式，可用于生成动态文件名，或在规则中使用。

$template myformat,"%$NOW% %TIMESTAMP:8:15% %hostname% %syslogtag% %msg%\n"

$ActionFileDefaultTemplate myformat

$template DynamicFile,"/var/log/info-%$NOW%.log"

local0.=info ?DynamicFile

转发到远程机器

传统方式的UDP传输，有损耗

基于TCP明文的传输，只在特定情况下丢失信息，并被广泛使用

UDP 在主机名前加"@"

TCP 在主机名前加"@@"

例： \*.\* @192.168.0.1 将所有日志信息通过UDP协议发送到192.168.0.1

日志文件

随着日志文件越来越大，这不仅会带来性能问题，同时对日志的管理也非常棘手。 当一个日志文件被rotated，会创建一个新的日志文件，同时旧的日志文件会被重命名。这些文件在一段时间内被保留，一旦产生一定数量的旧的日志，系统就会删除一部分旧的日志。

logrotate配置文件

logrotate的配置文件为/etc/logrotate.conf

默认情况下，每周对日志文件进行一次rotate，并且保留4份旧日志。 这里wtmp和btmp有些例外，wtmp记录系统登录日志，btmp记录错误的登录尝试。这两个日志文件每月进行一次rotate。 自定义的log rotation配置文件在/etc/logrotate.d目录下。

cat /etc/logrotate.d/rsyslog