**Linux日志管理**

Linux系统内核和许多程序会产生各种错误信息、警告信息和其他的提示信息，这些信息对管理员了解系统的运行状态是非常有用的，所以应该把它们写到日志文件中去。完成这个过程的程序就是syslog。syslog可以根据日志的类别和优先级将日志保存到不同的文件中。例如，为了方便查阅，可以把内核信息与其他信息分开，单独保存到一个独立的日志文件中。默认配置下，日志文件通常都保存在“/var/log”目录下。

日志相关服务

CentOS 6.X 以后日志的管理服务从syslog 升级成为了 rsyslog ，增强了部分功能。

基于TCP网络协议传输日志信息

更安全的网络传输方式

有日志消息的及时分析框架

后台数据库

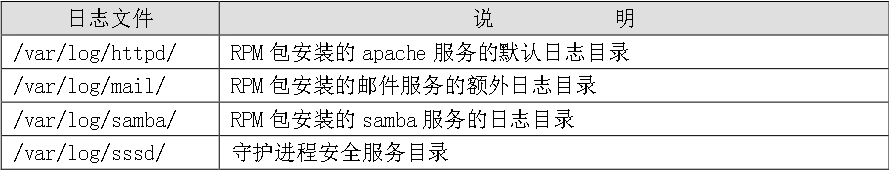
配置文件可以写一些简单的逻辑判断

兼容syslog配置文件

常见的日志文件



这些都是系统默认的日志，以及存放位置，那么除此之外我们还有一些RPM或者源码的软件安装产生的日志。



那么源码的日志则存放在了指定安装的位置下。

rsyslog 服务

日志的格式：

只要是通过rsyslog记录的日志，格式是相同的，包含以下内容：

发生时间

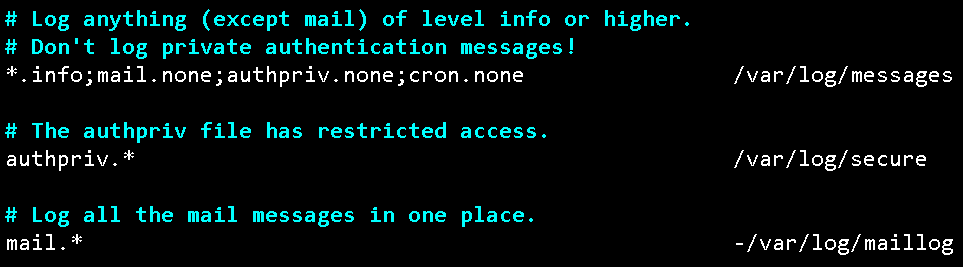
服务器的主机名

服务名或者程序名

事件具体信息

rsyslog 配置文件：

/etc/rsyslog.conf



第一列为日志类型和日志优先级的组合，每个类型和优先级的组合称为一个选择器；后面一列为保存日志的文件、服务器，或输出日志的终端。syslog 进程根据选择器决定如何操作日志。

对配置文件的几点说明：

* + - 日志类型和优先级由点号(.)分开，例如 kern.debug 表示由内核产生的调试信息。
    - kern.debug 的优先级大于 debug。
    - 星号(\*)表示所有，例如 \*.debug 表示所有类型的调试信息， kern.\*表示由内核产生的所有消息。
    - 可以使用逗号(,)分隔多个日志类型，使用分号(;)分隔多个选择器。

对日志的操作包括：

* + - 将日志输出到文件，例如 /var/log/maillog 或 /dev/console。
    - 将消息发送给用户，多个用户用逗号(,)分隔，例如 root, amrood。
    - 通过管道将消息发送给用户程序，注意程序要放在管道符(|)后面。
    - 将消息发送给其他主机上的 syslog 进程，这时 /etc/syslog.conf文件后面一列为以@开头的主机名(IP) 例：@192.168.88.30

rsyslog 识别的服务才能写到配置文件中



连接符号：

日志服务 [连接符号] 日志等级 日志记录位置

“.” ：代表只要比后面的等级高的（包含该等级）日志都记录下来。比如：“cron.info”代 表cron服务产生的日志，只要日志等级大于等于info级别，就记录

“.=”代表只记录所需等级的日志，其他等级的都不记录。比如：“\*.=emerg”代表人和日志服务产生的日志，只要等级是emerg等级就记录。这种用法及少见，了解就好

“.!”代表不等于，也就是除了该等级的日志外，其他等级的日志都记录。

日志等级：



特殊等级：none 不记录任何等级，相当于忽略该服务

日记记录位置：

日志文件的绝对路径。这是最常见的日志保存方法，如“/var/log/secure”就是保存系统验证和授权信息日志的。

系统设备文件。如“/dev/lp0”代表第一台打印机，如果日志保存位置是打印机设备的话，当有日志时就会在打印机打印（不太符合可持续发展战略哦-\_-!）。

转发给远程主机。因为可以选择使用TCP协议和UDP协议传输日志信息，所以有两种发送格式。如使用“@192.168.0.210:514”，就会把日志内容使用UDP协议发送到192.168.0.210的UDP 514端口上；如果使用“@@192.168.0.210:514”就会把日志内容使用TCP协议发送192.168.0.210的TCP 514端口上，其中514是日志服务默认端口。当然只要192.168.0.210同意接收此日志，就可以把日志内容保存在日志服务器上。

用户名。如“root”，就会把日志发送给root用户，当然root要在在线，否则就收不到日志信息了。发送日志给用户时，可以使用“\*”代表发送给所有在线用户，如“mail.\* \*”就会把mail服务产生的所有级别的日志发送给所

有在线用户。如果需要把日志发送给多个在线用户，用户名之间用“，”分隔。忽略或丢弃日志。如果接受日志的对象是“”，代表这个日志不会记录，而被直接丢弃。如“local3.\* ~”代表忽略local3服务类型所有的日志都不记录。

自定义日志记录：

vi /etc/rsyslog.conf

\*.crit /var/log/alert.log

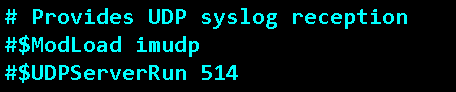
将所有临界点以上的错误都记录到alert日志中

修改完成，重启rsyslog服务，检查下有没有生成文件。

日志服务器搭建：

接收端：

配置文件：（有UDP和TCP）



取消注释，让接受端口生效。

重启服务，然后查看端口是否生成

发送端：

修改配置文件：

添加：

\*.\* @192.168.110.111:514

注意：可以使用UDP 用一个@ ； 也可以使用TCP 要用两个@@

重启服务，OK

测试：

在发送端，创建用户，然后检查接收端，查看日志/var/log/secure

注意事项：都知道Linux不依靠主机名识别，但是日志服务器需要根据主机 来识别，so。。。我们如果一台记录多台的日志信息，需要修改主机名。

日志轮替

主要目的防止单个日志文件过大，按照我们的规则对日志进行相应处理

主要依赖/etc/logrotate.conf配置文件中的dateext参数实现日志的处理。

主要参数解释：

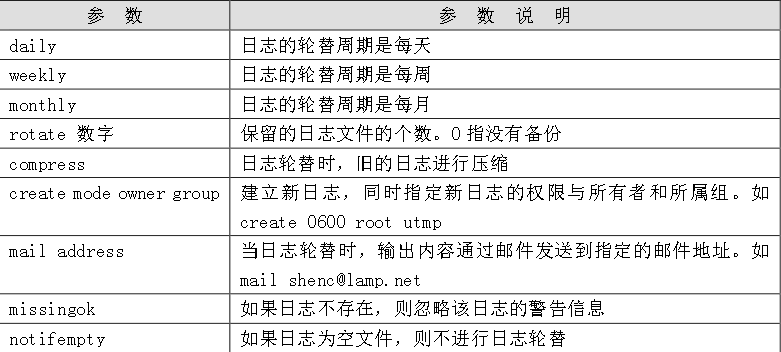
weekly 每周对日志进行依次轮替

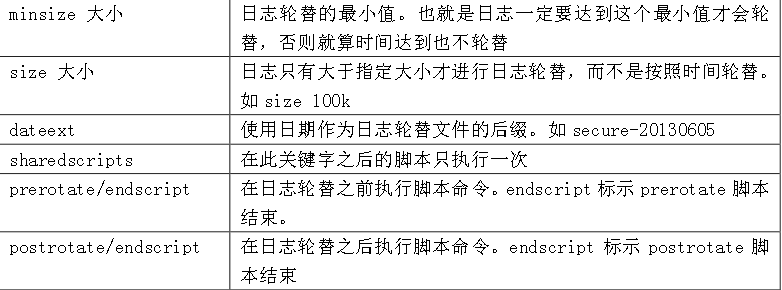
rotate 保存日志的数量

create 在轮替过程中，自动创建新的文件

dateext 使用日期作为日志文件的后缀

compress 是否压缩进行轮替的日志





系统自动定期进行日志轮替的原因：

/etc/cron.daily/ 有一个脚本，每天都会运行，查看是否有符合轮替的日志，然后进行相应处理

我们尝试在rsyslog配置文件中添加自己的日志记录，然后并且强制执行轮替，看会不会产生轮替文件

1. 先在配置文件中写入自己的日志轮替规则（参照原文中的）

2. 强制执行日志轮替（不管符不符合规定时间）

logrotate –vf /etc/logrotate.conf