准确解决系统问题 做好Linux日志管理

http://www.sina.com.cn 2002/08/23 09:54 赛迪网--中国电脑教育报

文/范志超

为了保证Linux系统正常运行、准确解决遇到的各种各样的系统问题，认真地读取日志文件是系统管理员的一项非常重要的任务。本文将简单解释什么是日志文件、在哪里可以找到日志文件以及如何处理它们。

Linux内核由很多子系统组成，包括网络、文件访问、内存管理等。子系统需要给用户传送一些消息，这些消息内容包括消息的来源及其重要性等。所有的子系统都要把消息送到一个可以维护的公用消息区，于是，就有了一个叫Syslog的程序。

Syslog程序有什么用

系统核心和许多系统程序会产生错误信息、警告信息和其他信息。这些信息很重要的，所以它们应该被写到一个文件。执行这个过程的程序就是Syslog，它能设置成根据输出信息的程序或重要程度将信息排序到不同的文件。例如，由于核心信息更重要且需要有规律地阅读以确定问题出在哪里，所以要把核心信息与其他信息分开来，单独定向到一个分离的文件中。

日志文件通常存放在“/var/log”目录下。为了查看日志文件的内容必须要有“Root”权限。日志文件中的信息很重要，只能让超级用户有访问这些文件的权限。

查看日志文件

日志文件其实是纯文本的文件，每一行就是一个消息。只要是在Linux下能够处理纯文本的工具都能用来查看日志文件。日志文件总是很大的，因为从你第一次启动Linux开始，消息就都累积在日志文件中。看日志文件的一个比较好的方法是用像More或Less那样的分页显示程序，或者用Grep查找特定的消息。我们先用Less显示“/var/log/messages”，可以看到从日志文件中取出来的一些消息。每一行表示一个消息，而且都由四个域的固定格式组成：

*时间标签(Timestamp)，表示消息发出的日期和时间。

*主机名(Hostname)，表示生成消息的计算机的名字。如果只有一台计算机，主机名就可能没有必要了。但是，如果在网络环境中使用Syslog，那么就可能要把不同主机的消息发送到一台服务器上集中处理。在我们的例子中主机名为lcbj。

*生成消息的子系统的名字。可以是“Kernel”，表示消息来自内核或者是进程的名字，表示发出消息的程序的名字。在方括号里的是进程的PID。

*消息(Message)，即消息的内容。

```
Sep 18 11:03:44 lcbj sendmail[85]: starting daemon (8.9.3): SMTP+queueing@00:15:00 …
Sep 18 11:06:11 lcbj passwd[337]: password for 'progs' changed by 'root' …
Sep 18 11:17:12 lcbj -- MARK --
Sep 18 11:37:12 lcbj -- MARK -
【标注】 Some logs extracted from /var/log/messages
```

①

图1中，第一行是Sendmail发出的消息，Sendmail守护进程(Daemon)负责管理收到和发出的消息。这一行是守护进程正常启动的消息。

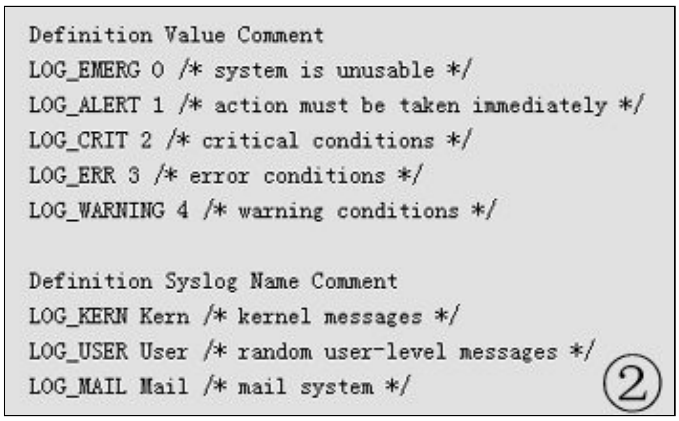
第二行是来自Passwd的消息，提醒用户“Progs”的口令被“Root”改变过。以后的其他消息，是向用户报告系统的运行情况。

实际上在“/var/log/message”文件中的消息都不是特别重要或紧急的。

有一个很有趣的消息是“MARK”消息，在默认情况下每隔20分钟就会生成一次表示系统还在正常运行的消息。“MARK”消息很像经常用来确认远程主机是否还在运行的“心跳信号”(Heartbeat)。“MARK”消息另外的一个用途是用于事后分析，能够帮助系统管理员确定系统死机发生的时间。

配置日志

让我们仔细地研究一下Syslog守护进程的运行情况吧。这个程序是在后台运行，从系统中获取新的消息，并把消息发送到合适的地方。每一个子系统发出日志消息的时候都会给消息指定一个类型。一个消息可以分成两个部分：“设备”和“优先级”。“设备”表示发出消息的子系统，“优先级”表示消息的重要性，其范围从0(最重要)到7(最不重要)。请见图2。



Syslog的基本配置是很简单的，而进行一些高级特性的配置需要一些经验。我们现在看看基本的配置，也就是根据“设备”和“优先级”确定哪些文件应该收到哪些消息。可以通过编辑文件(通常是“/etc/syslog.conf”)对任务进行定制。以“#”号开头的行都是注释行。其他的一些行也很容易理解，它们是由两个域组成，分别是“选择器(Selector)”和“动作(Action)”。“选择器”用相应的“设备”和“优先级”(都可以用“*”通配符表示“任何一个”)来表示消息的类型。“动作”表示一旦有一个新的消息和“选择器”相匹配的时候要采取什么行动。

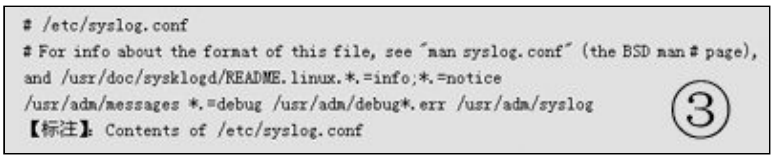


图3中，你会发现“优先级”等于“Info”和“Notice”的消息，无论它们的“设备”是什么，都发到“/usr/adm/messages”文件，因为在“选择器”中使用了通配符。同样“优先级”为“Debug”和“Err”的消息都分别送到“/usr/adm/debug”和“/usr/adm/syslog”文件。

编辑完“/etc/syslog”文件之后，还必须运行“Killall -HUP Syslogd”，这样所做的改变才会生效。这个命令发送“HUP”信号给Syslog守护进程，通知守护进程重新读取配置文件。

日志文件对于管理员来说很重要，通过对日志文件的管理，可以更好地维护系统，保障各种应用的正常进行。

【学园专题】自由奔放的Linux

相关链接

将Linux配置为代理防火墙用途(2002/08/23 09:45)
巧用Linux工作站通过校园网上互联网(2002/07/10 10:17)
免费的Linux在构建绿色校园网中的应用(2002/06/26 14:42)
配置红旗Linux使用ADSL上宽带网(2002/06/25 10:38)
