sabrina的专栏

linux的syslog机制 【syslog编程和设置】

2009-08-24 13:52 744人阅读 评论(0) 收藏 举报

linux 编程 服务器 socket cron unix

1. 前言

syslog是UNIX系统中提供的一种日志记录方法(RFC3164)，syslog本身是个服务器，程式中凡是使用syslog记录的信息都会发送到该服务器，服务器根据设置决定此信息是否记录，是记录到磁盘文件还是其他地方，这样使系统内所有应用程式都能以统一的方式记录日志，为系统日志的统一审计提供了方便。

2. 日志格式

syslog记录的日志格式为：
月 日 时:分:秒 主机名 标志 日志内容

3. syslog编程

为记录日志，通常用到3个函数，openlog(3)，syslog(3)和closelog(3)，openlog(3)和closelog(3)不是必须的，没有openlog(3)的话将用系统缺省的方式记录日志。

```
#include
void openlog( char *ident, int option, int  facility)
void syslog( int priority, char *format, ...)
void closelog( void )
```

openlog(3)有三个参数，第一个参数是标志字符串，也就是日志中的第5个字段，不设的话缺省取程式名称；
第二个参数是选项，是下面一些标志位的组合：

- LOG_CONS：日志信息在写给日志服务器的同时打印到终端
- LOG_NDELAY：即时记录日志
- LOG_PERROR：把日志信息也输出到标准错误流
- LOG_PID：在标志字段中记录进程的PID值

第三个参数是说明日志类型的，定义了以下类型(各类型啥意思就自己看或猜吧，俺就不多说了)：

- LOG_AUTH
- LOG_AUTHPRIV
- LOG_CRON
- LOG_DAEMON
- LOG_KERN
- LOG_LOCAL0 through LOG_LOCAL7
- LOG_LPR
- LOG_MAIL
- LOG_NEWS
- LOG_SYSLOG
- LOG_USER(default)

利用条件变量控制子线程 (0)
C语言中变长参数表print (0)
基于ath5k驱动的wireles (0)
linux的syslog机制 【sys (0)
Linux Kernel开发进展的 (0)
Wrt54gs v2+Kamikaze 7 (0)
WRT54GS+Kamikaze 7 (0)
Linux下共享库路径配置 (0)

推荐文章

* Android SQLite性能分析
* Android-自定义图像资源的使用（2）
* Cocos2dx 小技巧（十一） 小人虽短，但可以旋转
* C++ Primer 学习笔记_57_类与数据抽象 --管理指针成员
* 机器学习中的范数规则化之（二）核范数与规则项参数选择
* android 高仿 频道管理----网易、今日头条、腾讯视频（可以拖动的GridView）附源码DEMO

最新评论

linux SMP机器下查看每个CPU的
fantasy666666: 这个方法不错，分隔的很清楚

LOG_UUCP

syslog(3)函数主要的是第一个参数priority，后面那些参数就是和printf(3)函数用法相同了，priority值表示该条日志的级别，日志级别分8级，由高到低的顺序为：

LOG_EMERG
LOG_ALERT
LOG_CRIT
LOG_ERR
LOG_WARNING
LOG_NOTICE
LOG_INFO
LOG_DEBUG

如果openlog(3)时没有指定facility，是能把facility的值或到priority中的，如(LOG_AUTH | LOG_INFO)，已设置了就能不用或了。

closelog(3)这个没啥好说的了，关闭日志记录。

4. syslog服务器设置

syslog服务器的设置文件为/etc/syslog.conf，syslog(3)函数把想记录的日志信息都发送给日志服务器，但此日志最终是否记录到文件或发送给远程服务器，则是由此设置文件来决定的，该设置文件就是告诉日志服务器要记录那些类型和级别的日志，怎么记录等信息。

设置文件是文本文件，每行设置分两个字段，第一字段是说明要记录哪类日志，第二字段是说明日志存放位置，能是本地文件，也能是远程服务器。

第一字段：
第一字段基本格式是“facility.priority”，能同时定义多个，中间用逗号“,”或分号“;”分隔。
facility名称就是上面说的facility值的后半部的小写，如news, mail，kern, cron等，也能用“*”表示所有facility类型；
priority名称就是上面说的priority值的后半部的小写，如emerg, alert，err, info等，也能用“*”表示所有priority类型，比此级别高的日志都会自动记录，用none表示不记录；
举例：
kern.* : 所有级别的内核类型日志
mail.err: 错误及错误级别以上的mail类型日志
如果不记录某级别的日志，在级别前加“!”，如：
auth.info;auth.!err ： info及info级别以上但不包括err级别的auth类型日志
第二字段：
第二字段分两类，本地文件和远程服务器
本地文件：直接就是写本地文件的文件名，如 /var/log/messages。一般来说日志信息会即时写到文件中，但会降低系统效率，能在文件名前加减号“-”表示先将信息缓存，到一定量后再一次性写入文件，这样能提高效率；
远程服务器：格式是
[email=%E2%80%9C@address]“@address[/email]
”，“@”表示进行远程记录，将日志发送到远程的日志服务器，日志服务器的端口是UDP514，address能是IP地址，也能是域名

举例：

```
# 将所有级别的内核日志发送到终端
kern.*  /dev/console

# 将所有类型所有级别的日志记录到/var/log/messages文件
*.* /var/log/messages

# 所有info级别以上的信息，不包括mail类型所有级别和authpriv类型的err级别信息，
# 记录到/var/log/messages文件，不即时写入
*.info;mail.none;authpriv.!err       -/var/log/messages
```

#将所有级别的内核日志发送到远程syslog服务器
kern.* @1.1.1.1

5. syslog服务器

在linux下提供了sysklogd的syslog服务器的实现，能记录本机日志也能接收(syslogd的-r选项)和转发(syslogd的-h选项)来自外部的日志。

sysklogd包括两个程式，klogd和syslogd，klogd用于接收内核日志，再发送到syslogd，syslogd则能直接接收应用程式和远程的日志，syslogd是通过一个域socket(AF_UNIX)来接收数据的，syslog()函数记录的日志都发送到此域socket，socket文件是/dev/log。

syslog(3)函数发送给syslogd服务器的日志信息前都加上了类型和级别信息，具体格式是“”，“x”是个 0 ~ 255的数，8位，低3位表示日志级别，所以共8级，高五位表示日志类型，最多32种，不过目前没用到那么多，能看看/usr/include/sys/syslog.h中的定义就知道了。

要生成日志信息时，syslogd是先生成日志前部信息：月 日 时:分:秒 主机名 标志，再和日志内容信息拼接起来的，日期用ctime(3)函数获取，隐去了前4个表示星期的字节和后面年的信息，最终生成你所看到的日期格式，老实说那段代码及其丑陋。

6. 结论

syslog方便了程式信息的记录，由于使用了统一的格式记录使得审计也能比较方便。要记录日志，除了在应用程式中用syslog(3)函数记录外，还要正确设置/etc/syslog.conf文件，使服务器能正确记录那些想记录的日志。

另外还有一篇syslog协议

http://blog.csdn.net/xcj0535/archive/2009/05/07/4158624.aspx

更多 0

上一篇 Linux Kernel开发进展的总结

下一篇 linux SMP机器下查看每个CPU的利用率