syslog

系统默认的日志守护进程

补充说明

syslog 是Linux系统默认的日志守护进程。默认的syslog配置文件是/etc/syslog.conf文件。程序，守护进程和内核提供了访问系统的日志信息。因此，任何希望生成日志信息的程序都可以向 syslog 接口呼叫生成该信息。

几乎所有的网络设备都可以通过syslog协议，将日志信息以用户数据报协议(UDP)方式传送到远端服务器，远端接收日志服务器必须通过syslogd监听UDP 端口514，并根据 syslog.conf配置文件中的配置处理本机，接收访问系统的日志信息，把指定的事件写入特定文件中，供后台数据库管理和响应之用。意味着可以让任何事件都登录到一台或多台服务器上，以备后台数据库用off-line(离线) 方法分析远端设备的事件。

通常syslog 接受来自系统的各种功能的信息，每个信息都包括重要级/etc/syslog.conf 文件通知 syslogd 如何根据设备和信息重要级别来报告信息。

使用方法

在/var/log中创建并写入日志信息是由syslog协议处理的，是由守护进程sylogd负责执行。每个标准的进程都可以用syslog记录日志。可以使用logger命令通过syslogd记录日志。

要向syslog文件/var/log/messages中记录日志信息：

```
logger this is a test log line

输出：
tail -n 1 messages
Jan  5 10:07:03 localhost root: this is a test log line
```

如果要记录特定的标记tag可以使用：

```
logger -t TAG this is a test log line

输出：
tail -n 1 messages
Jan  5 10:37:14 localhost TAG: this is a test log line
```