Systemd是Fedora自16版引入的新的init系统，与原有的OpenRC系统不同，引入了Unit概念，实现了并行启动。但由于其接管了太多的东西，导致了太多的变化。本文试讲解systemd中的log系统。

Systemd接管了原有的syslog，将日志系统设计成journal，所有的日志文件均保存在/var/log/journal目录下，并以加密形式保存，提高了安全性，也带来了不便，尤其是取证环节（然而在/run/log/journal目录下，仍保存着10分钟内未加密的原始log，，默认情况下）。因此，原有的/var/log/目录下经典的message等文件默认是不存在的。为此，我们需要使用journalctl来查看日志，并进行控制。

直接使用journalctl，即可日志。如图1，显示的是启动信息（顺便说一句，现在的dmesg命令将会显示自本次系统启动后所有的事件信息，而非仅仅启动信息）。

使用journalctl –f将显示 最后的10行log，同时等待新事件发生并显示（相当于曾经的tail –f /var/log/message）。

journalctl –b与dmesg等同，显示自本次启动后所发生的所有事件。

journalctl –p筛选信息严重性，与syslog相同，"emerg"(0), "alert"(1), "crit"(2), "err"(3), "warning"(4), "notice"(5), "info"(6), "debug"(7)，将显示指定等级及更严重等级的信息。

journalct –-since 与—until指定时间范围。可以指定日期或时间。

journalctl –u 指定信息来源。

jourlalctl后加涉及的对象，可筛选相关信息。如图2，journalctl /sbin/dhcpcd可查看dhcpcd发生的一系列事件。注意，\*ux中一切皆文件，因此journalctl 后可加任何文件，如磁盘/dev/sda等，但是要加绝对路径。可同时加多个文件，查看相关联的信息。

不仅如此，journalctl可以筛选更多的信息。Journalctl –o verbose 将显示每条信息的详细信息，如图3，所有列出的属性均可被筛选。直接在journalctl后加属性名匹配即可，实际上，这里可以使用正则表达式。

Journalctl –F 后加属性名，将显示日志中所有拥有此项属性的记录。如图4。同时，这里可以使用Tab自动补全。

！！！！！！！！！！！！！！！！！

以上所有的参数，是可以进行搭配的。

！！！！！！！！！！！！！！！！！

另外，并非所有的log都会在journalctl中看到，许多程序没有采用systemd的API，例如X，因此仍然需要查看/var/log/目录下的其他文件。