Syslog UDP Source 认为整个 UDP 数据报文是一个 syslog 事件，并将其转换为一个 Flume 事件，而 Multiport Syslog Source 每次遇到一个换行符(\ *n*)字符创建一个新的消息。这些 Source 创建两个 header，Facility 和 Severity，在每个 Flume 事件的 header 中指明每个消息的 Facility 和 Severity。这可以用于分桶或多路复用 Channel 选择器（第 6 章中讨论）。

表 3-9 列出了两种 Source 的公共配置参数。

表3-9 Syslog Source配置

参数	默认值	描述
type	-	Syslog UDP Source 类型是 syslogudp，Multiport Syslog Source 类型是 multiport_syslogtcp
host	-	绑定的 IP 地址或主机名。使用 0.0.0.0 绑定机器上所有的接口
keepFields	false	如果设置为 true，syslog 消息的所有字段会保存在事件除了 header 之外的 body

Syslog UDP Source 可以使用 syslogudp 别名，而 Multiport Syslog Source 可以使用 multiport_syslogtcp 别名。两类 Source 都需要用户使用 host 参数的值来指定绑定的主机名。如果要绑定机器上所有的端口，将 host 参数的值设置为 0.0.0.0。如果 keepFields 参数设置为 true，syslog 消息的字段通常会移动到事件的 header（或整个移除），例如 Priority、Timestamp 和 Hostname 字段会保留在事件 body，同时也复制到事件的 header。Multiport Syslog Source 也允许 syslog 消息将每个端口接收的数据编码为不同的字符集。本质上这能使单类 Source 接收不同种类的 Source 的数据，并将消息编码为不同的字符集。

除了公共参数，Syslog UDP Source 只有一个另外的参数（见表 3-10）。

表3-10 Syslog UDP Source配置

参数	默认值	描述
port	-	绑定的端口号

Port 参数用来指定 Source 应该绑定的端口号。

60 Multiport Syslog Source 可以在主机上绑定多个端口。除了公共参数，Multiport Syslog Source 还定义了表 3-11 中的参数。