Sysevent

This plugin utilizes a network socket to listen for incoming rsyslog messages. Current configuration options include:

1. Listen: An IP and port on which to listen for incoming messages.
2. BufferSize: Size of the buffer used for receiving messages.
3. BufferLength: Length of ring buffer used to store messages.
4. RegexFilter: A regular expression to match against stored messages (all messages are always stored – see below). If no filters are provided, all messages will be dispatched by the plugin.

While running, two threads are used:

1. The main read thread, to read semaphore-protected shared memory.
2. A blocking listening thread that waits for rsyslog messages on a socket and writes them to shared memory (a ring buffer).

The listening thread waits for incoming messages and writes them into the ring buffer. All messages are stored. The read thread then wakes at plugin interval and steps through new messages in the ring buffer. What happens next depends on configuration and message content:

1. The plugin will try to parse the whole message as JSON data. If the parsing succeeds, the plugin breaks the message into its constituent elements for filtering and dispatching.
2. If any RegexFilters are configured, the "message" portion of the message must match at least one of these filters. The "message" portion is only available if JSON parsing succeeded in step 1. If JSON parsing failed, the whole of the message content is considered for filtering purposes.
3. Using data available from the message (individual key/value pairs of data, if JSON parsing succeeded), a notification is constructed and dispatched.