Windows Event Log, Syslog, SNMP Trap Monitoring

Monitoring event data can be one of the most daunting tasks faced daily by IT staff. In many industries, legal and organizational directives require that vast amounts of event information be regularly collected and reviewed for potential security or operational breaches. In addition, event data holds performance clues essential for applications to run at maximum efficiency. With potentially hundreds of thousands of events to examine each day, many organizations turn to automation to help manage event volume.

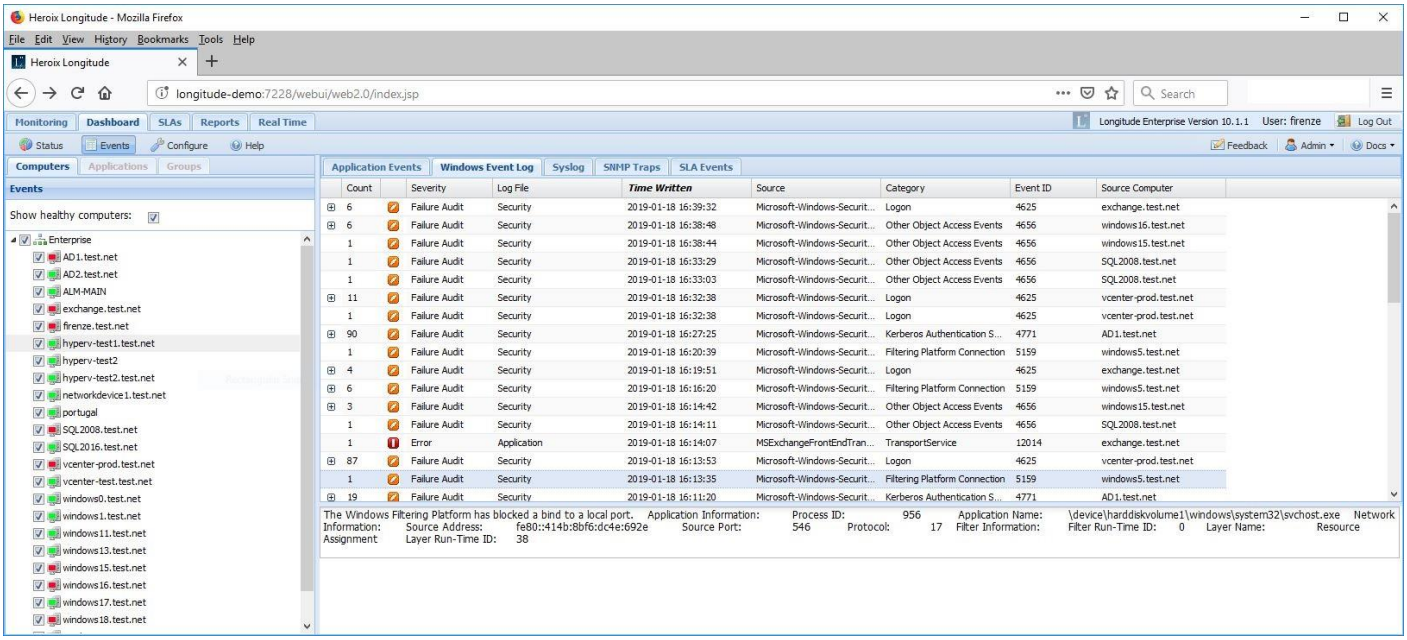
Longitude allows powerful, flexible automation for collecting and consolidating event information from Windows Event Logs, Syslog, and SNMP traps. Using Longitude's web-based interface, you can easily set up an appropriate event handling regimen without having to write scripts.

Events collected from the Windows Event Logs, Syslog, and SNMP traps can be consolidated to Longitude events, making them available for evaluation, analysis, display, reporting, and alerting by Longitude. Furthermore, you can leverage Longitude's correlated events capabilities to increase situational awareness by detecting patterns in consolidated events, or linking event data with information from other Longitude data sources.

Windows Event Log Monitoring

The WindowsEventLog solution enables Windows event log records to be collected for display and alerting. Specify events of interest based on event log file, event ID, event source, and event type.

- Event log records can be displayed in Longitude's Windows Event Log Viewer (shown below).
- Collected event log records can be consolidated into Longitude events for display with other Longitude events in the Applications view of the Longitude Event Monitor.
- Consolidated events can be used to trigger Longitude actions or correlated events.
- Event reports display statistics related to the number of event log records of each type, and include drill down for more detail on the events.



Syslog Monitoring

The Syslog solution enables Syslog records to be collected within Longitude for display and alerting. Specify events of interest based on IP address, facility, and severity.

- Syslog records can be displayed in Longitude's Syslog Viewer
- Collected Syslog records can be consolidated into Longitude events for display with other Longitude events in the Applications view of the Longitude Event Monitor.
- Consolidated events can be used to trigger Longitude actions or correlated events.
- Event reports display statistics related to the number of Syslog records of each type, and include drill down for more detail on the events.

SNMP Trap Monitoring

The SnmpTrap solution enables SNMP Traps to be collected within Longitude for display and alerting. Specify traps of interest based on trap name, number, IP address, and OID; Longitude can collect SNMP V1, V2, and V3 traps.

- SNMP traps can be displayed in Longitude's SNMP Trap Viewer (shown below).
- Collected SNMP traps can be consolidated into Longitude events for display with other Longitude events in the Applications view of the Longitude Event Monitor.
- Consolidated events can be used to trigger Longitude actions or correlated events.
- An SNMP trap report allows historical review of collected SNMP traps.

HEROIX
www.heroix.com

165 Bay State Drive
Braintree, MA 02184
Telephone: 781-848-1701
info@heroix.com