



SECURITY ANALYTICS 10.6

EVENT SOURCE AUTOMATING MONITORING

RSA

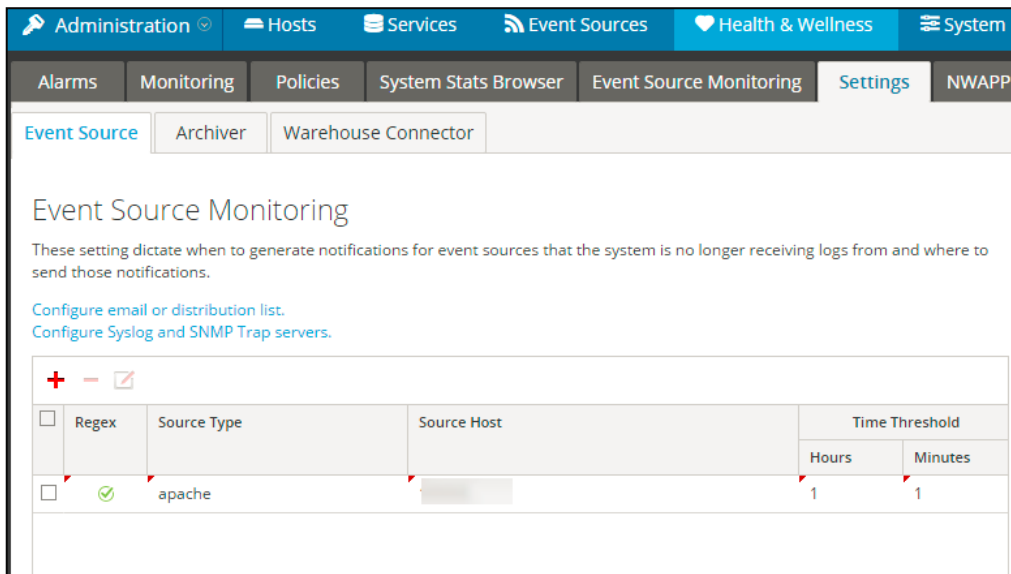
Monitoring event sources with 10.5

- ▶ Number of log messages and idle time for each event source / event type was recorded
- ▶ Admins could configure a time threshold and be notified when the event source stopped sending logs

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time
	ciscopix	0	NWAPPLIANCE28818	250	15 hours, 27 min	2015-03-23 07:33:08 ...
	unknown	0	NWAPPLIANCE28818	5	15 hours, 27 min	2015-03-23 07:33:10 ...
	aix	NWAPPLIANCE24887	NWAPPLIANCE24887	9	6 days, 6 hours, 45 min	2015-03-18 04:15:26 ...

Limitations

- ▶ Thresholds were static
- ▶ Thresholds had to be defined manually
- ▶ No alerts if the event source was generating too many / too few messages, but only if it was no more sending logs
- ▶ Not considering devices which for example might be quite during the night



The screenshot shows a management console interface for 'Event Source Monitoring'. The top navigation bar includes 'Administration', 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', and 'System'. Below this, a secondary navigation bar contains 'Alarms', 'Monitoring', 'Policies', 'System Stats Browser', 'Event Source Monitoring', 'Settings', and 'NWAPP'. The main content area is titled 'Event Source Monitoring' and includes a sub-header 'Event Source' with tabs for 'Archiver' and 'Warehouse Connector'. The page explains that these settings dictate when to generate notifications for event sources that the system is no longer receiving logs from. It provides links to 'Configure email or distribution list' and 'Configure Syslog and SNMP Trap servers'. A table below lists the configured event sources:

<input type="checkbox"/>	Regex	Source Type	Source Host	Time Threshold	
				Hours	Minutes
<input type="checkbox"/>	✓	apache		1	1

Automatic Monitoring with 10.6



- Receive automatic alerts based on deviations from the baseline behavior of your event sources
- No need to set up numerous group thresholds and policies
- For each event source, the number of logs generated every hour (e.g. 8am-9am) is compared with the baseline created the previous days during the same timeframe

The screenshot shows the Splunk Administration interface. The top navigation bar includes 'Administration', 'Hosts', 'Services', and 'Event Sources'. Below this, a secondary navigation bar has 'Manage', 'Monitoring Policies', 'Alarms', and 'Settings'. The 'Settings' tab is active, and the page title is 'Automatic Monitoring Settings (Beta)'. The main content area contains the following configuration options:

- Automatic Monitoring Settings (Beta)**
Automatic Monitoring keeps an hourly baseline of individual Event Source rates and alerts as configured on the Monitoring Policies tab.
- Monitoring Configuration**
 - Enable Automatic Monitoring:
 - Enable Notifications from Automatic Monitoring:
 - Low Standard Deviations: 2.5
 - High Standard Deviations: 2.5
 - Enable Aggregation Persistence:
 - Aggregation Persistence Interval in Days: 120
 - Enable Generation of Analytics:

At the bottom of the configuration area are 'Reset' and 'Apply' buttons.



EMC²

EMC, RSA, the EMC logo and the RSA logo are trademarks of EMC Corporation in the U.S. and other countries.