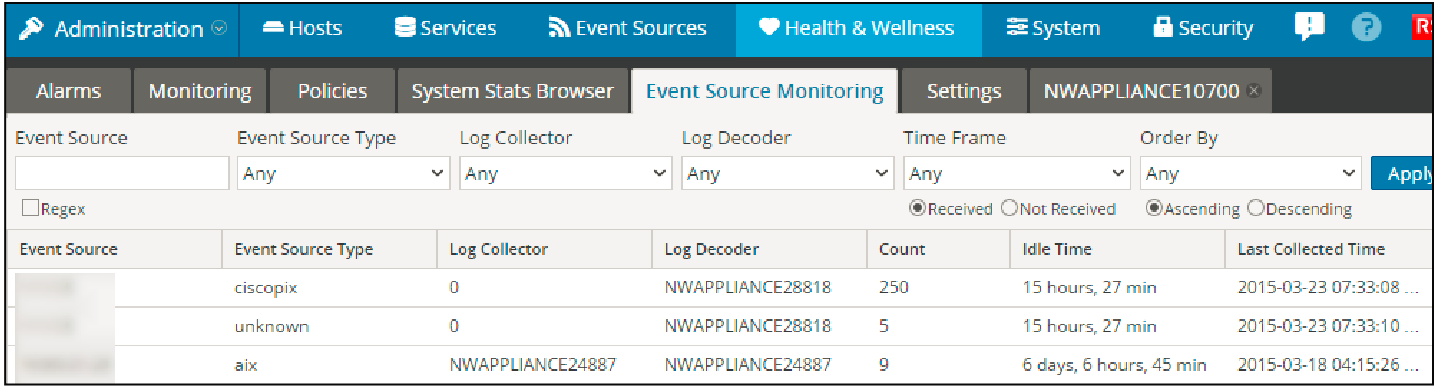
SECURITY ANALYTICS 10.6

EVENT SOURCE AUTOMATING MONITORING

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

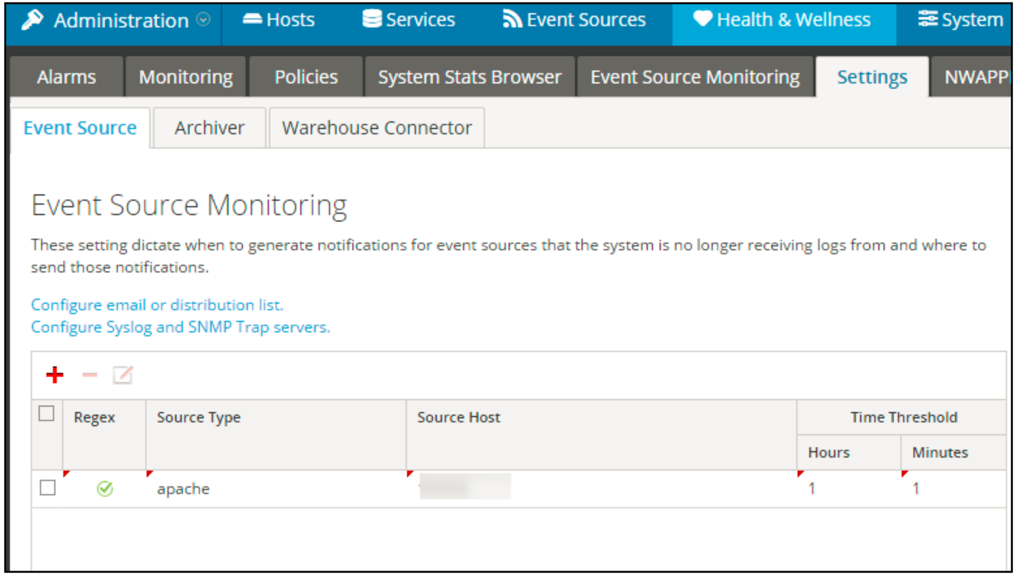


Event Source: □ Regex
Event Source Type: Any
Log Collector: Any
Log Decoder: Any
Time Frame: Any ● Received ○ Not Received
Order By: Any ● Ascending ○ Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time
[redacted]	ciscopix	0	NWAPPLIANCE28818	250	15 hours, 27 min	2015-03-23 07:33:08 ...
[redacted]	unknown	0	NWAPPLIANCE28818	5	15 hours, 27 min	2015-03-23 07:33:10 ...
[redacted]	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 was no more sending logs
- Not considering devices which for example might be quite during the night



Event Source Monitoring

These setting dictate when to generate notifications for event sources that the system is no longer receiving logs from and where to send those notifications.

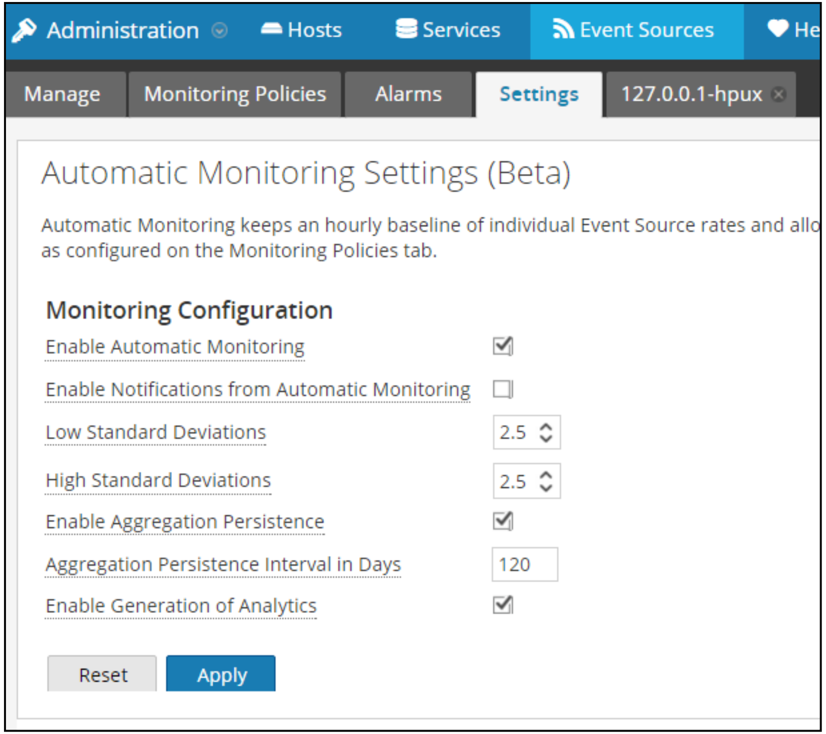
Configure email or distribution list.
Configure Syslog and SNMP Trap servers.

□	Regex	Source Type	Source Host	Time Threshold	
				Hours	Minutes
□	✓	apache	[redacted]	1	1

Automatic Monitoring with 10.6

NEW!

- 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



Automatic Monitoring Settings (Beta)

Automatic Monitoring keeps an hourly baseline of individual Event Source rates and allo
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	☑

RSA®

EMC²