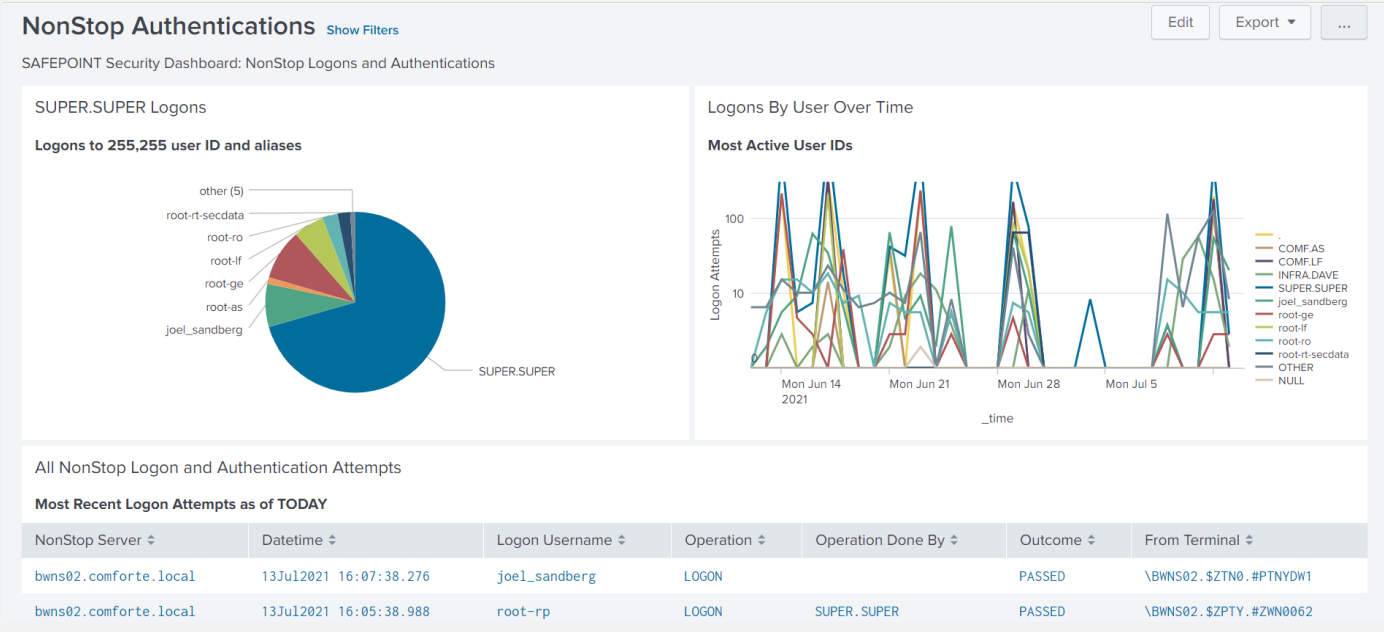
SAFEPOINT LOGSTREAM

(AND SAFEPOINT SPLUNK APP)

Fact Sheet

PURPOSE

The SafePoint Logstream product locates and collects NonStop log data, formats the log records into a standard format, and writes the target records to a SIEM processor or any audit collection server. It does this in a highly fault-tolerant manner. SafePoint Logstream streams large amounts of log data to a SIEM via SYSLOG. Currently SafePoint Logstream can stream Safeguard, NonStop SSH, iTP Webserver, EMS, SP sudo, and KSL (keystroke) log data. Future releases will provide support for other log sources. SafePoint Logstream helps achieve compliance of the various sections of PCI Requirement 10.



Sample SafePoint Splunk App Dashboard. NonStop data feed by SafePoint Logstream

FEATURES

High Volume Log Streaming

There can be massive amounts of NonStop log data, depending on how much auditing is taking place on the systems. NonStop subsystems like Safeguard, SSH, EMS -- and others -- can emit large quantities of audit log data which must be monitored and collected in an efficient manner. SafePoint Logstream handles extremely large quantities of audit data and reduces that data into reasonably sized, normalized output streams.

High Degree of Fault-Tolerance

The SafePoint Logstream software utilizes high-performance parallel processing of multiple audit trails. It relies on several mechanisms to maximize resiliency and fault tolerance. It is possible to restart the software so that it continues from the point where it left off. These mechanisms include a central component running as a NonStop process pair, as well as processes which run with kernel persistence. In addition, the software maintains a form of checkpointing so that if it needs to restart, it can reposition to the last remembered location in the input audit log files.

Broad integration with enterprise management infrastructures

The SafePoint Logstream product sends messages via SYSLOG to tier-two event collectors like Splunk, QRadar, and others. SafePoint Logstream's streaming messages can be viewed and analyzed using any SYSLOG-aware SIEM. Common Event Format (CEF) provides an industry-standard message format for the output log stream. Logstream is bundled with the SafePoint Splunk app, providing NonStop-oriented dashboards and alerts.

Extensible Architecture

Currently SafePoint Logstream can stream Safeguard, NonStop SSH, iTP Webserver, EMS, SP sudo, and KSL (keystroke) data. The software is readily expandable, and future releases will provide support for other log sources.

BENEFITS

> Boost security

SafePoint Logstream enables security organizations to fully leverage event information from their HPE NonStop environments. It enables security analysts to more effectively monitor their entire infrastructure, and more quickly identify and respond to potential threats. Logstream facilitates the analysis of event data, both forensically and in real time, for early detection of targeted attacks and security breaches

> Improve Big Data Analytics

Moving event data to a SIEM facilitates a detailed analysis of that data. SafePoint Logstream normalizes the data and parses it into discrete fields, providing for easy analysis. Once at the SIEM, event data and contextual information from multiple sources can be analyzed in terms of activity patterns, trends, user activity, and overall security compliance.

> Leverage infrastructure investments

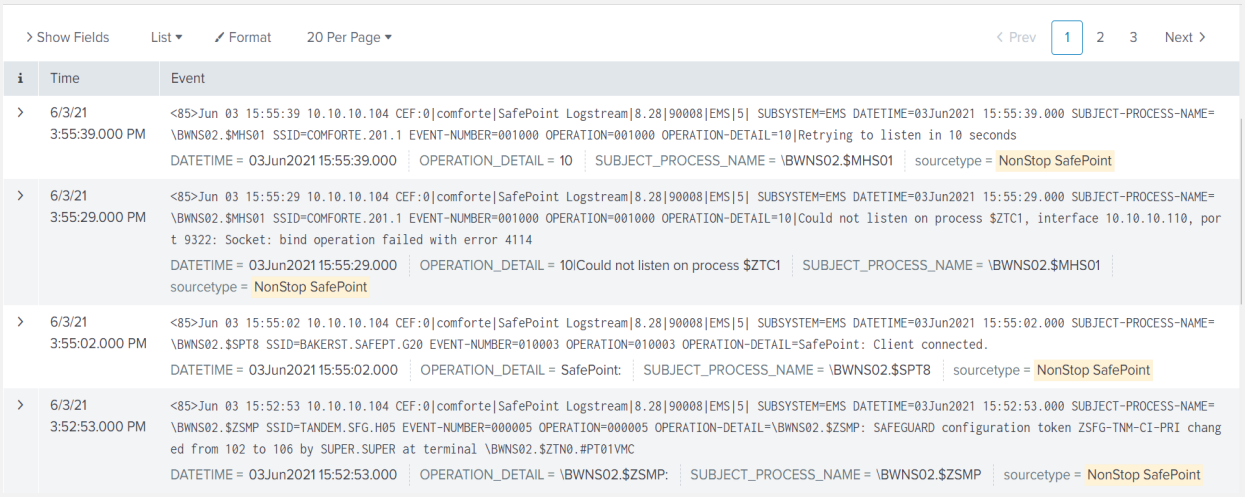
SafePoint Logstream enables organizations to work with their existing security infrastructure, while more fully leveraging HPE NonStop-related security information, whether generated by OSS, EMS, audit clients, or other sources.

> Integration with SIEM

SafePoint Logstream streams audit data directly to an enterprise SIEM system, providing security officers and auditors with access to NonStop audit data. The SafePoint Splunk App provides the final piece of this integration, simplifying the task of NonStop data analysis.

> Bonus: Command-level Security & Auditing

SafePoint sudo provides an HPE NonStop Guardian Guardian/TACL interface to sudo command-level security. Sudo is a standard Unix/Linux utility which allows a permitted user to execute a command as another user. SafePoint Sudo provides TACL definitions for sudo commands so that Guardian and OSS command-level security can be easily defined, implemented, and audited. SafePoint Logstream processes sudo log records.



Sample SafePoint Splunk App Dashboard. NonStop data feed by SafePoint Logstream