



SECURELOG SYSTEM

Secure and Reliable Log Centralization Platform

INTRODUCING SECURELOG

SecureLog is a complete last generation suite for Log management. It is based upon encrypted transfer protocols and data memorization technologies which allow to centralize, store and analyze logs in an intuitive effortless way, always guaranteeing data integrity and availability.

WHY LOG MANAGEMENT

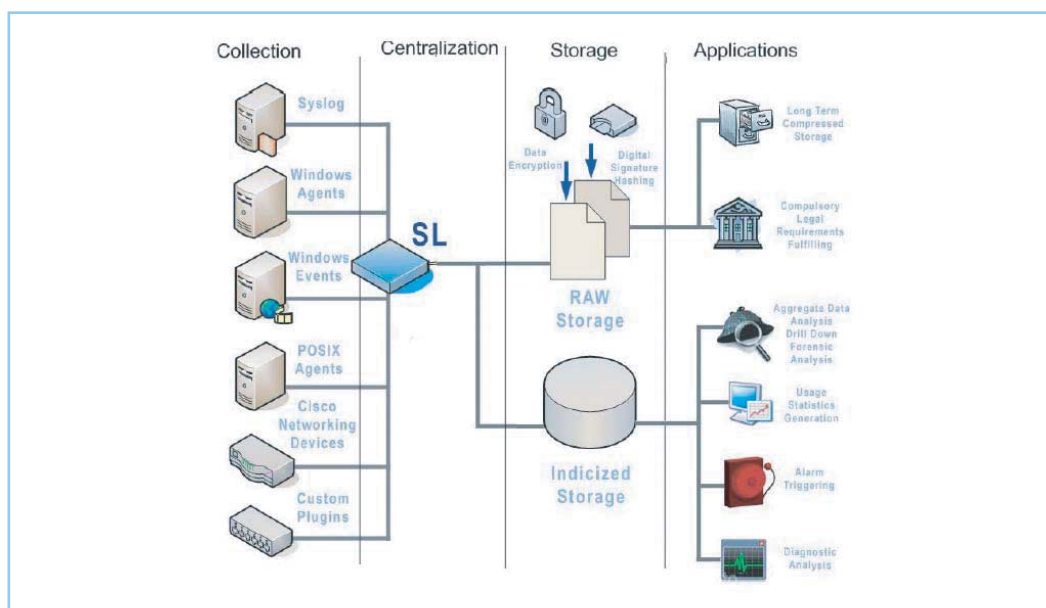
During the last two decades information technology has been meeting a large amount of success, meaning among other things that networks have been continuously growing in size and that the number of computing devices, physical or virtual has also been rapidly rising virtually in every company worldwide. One of the consequences of this trend is that computer attacks and threats have also become more common. In order to face these new dangers, the good system administrator must not only secure the systems under his control, but also keep track of all system activity, in the case an intruder manages to break through system defenses or simply something goes wrong at both hardware or software levels. No matter what is the cause for the downtime of a certain resource, it is fundamental to be able to track what has gone wrong, in order not only to perform a quick system restore but also to avoid the re-occurrence of the problem. Such tracking can be achieved by log analysis, since such files constitute indeed the black box of each

modern computer system. Of course, once collected and centralized, log data can also be exploited to draw reports of system usage (web server statistics, for instance).

Through the use of a log server, system administrators can have an immediate snapshot of all system status, monitoring at the same time all of the activities going on inside of a network. It then becomes much easier to detect irregular behaviors and also to isolate significant elements, which allow to further identify and trace intrusion attempts or failures. Moreover a system administrator can effortlessly obtain regular updated information about normal operational status of network devices or hosts.

When log are remotely kept moreover, even in the case an attacker is able to modify local logs in order to try to hide his intrusion, a secured, not alterable copy of these log files is preserved elsewhere, so that he won't be able to completely erase all traces of his activity.

Logs allows therefore to recreate happened events and also have probative validity in case of debate in most countries. At the moment log management is a problem that companies face only when problems have already turned up, which actually is actually too late in most of the cases.



SecureLog Data Path



SECURELOG SYSTEM

Secure and Reliable Log Centralization Platform

SECURELOG OVERVIEW

SecureLog has been designed to address all of the issues depicted in the paragraph above. It aims to be an invaluable instrument for system administrators, but not only. Its analysis features allow the instrument to be used also by marketing departments and IT managers to obtain quick statistics, reports and snapshots of systems usage.

SecureLog allows a significant reduction in terms of log management and overall IT security costs; the scalability of the product moreover allows deployments to be made in different steps, by purchasing hardware and software upgrades only when more data has to be handled and therefore more computational power is needed.

Data can be collected both by peripherals which are Syslog or Syslog-NG standard compliant and by SecureLog collectors (available for different flavors of Microsoft Windows, Linux and Unix Operating Systems). Such collectors allow encrypted data transmission and provide additional data security and integrity checks, guaranteeing that data isn't altered during transmission and that the complete source file content is entirely transmitted.

An intuitive web based GUI allows the operator to easily manage and configure all transport and centralization features, providing the system administrator with a single integrated environment, through which he can handle operations that would otherwise need a lot of time consuming efforts, if they were to be carried on one by one, without proper tools and instruments.

Such GUI integrates an advanced indexing and analysis engine also (such feature is powered by SATA H.T.S. partner Sawmill Technologies, an international level authority in the field of log analysis: <http://www.sawmill.net/>). The results of SATA H.T.S. and Sawmill integrated technologies is an environment which offers the user powerful log management, analysis, statistical and reporting tools, combined together into a single interface, allowing easy handling of large quantities of data and immediate interaction and therefore comprehension of Log information.

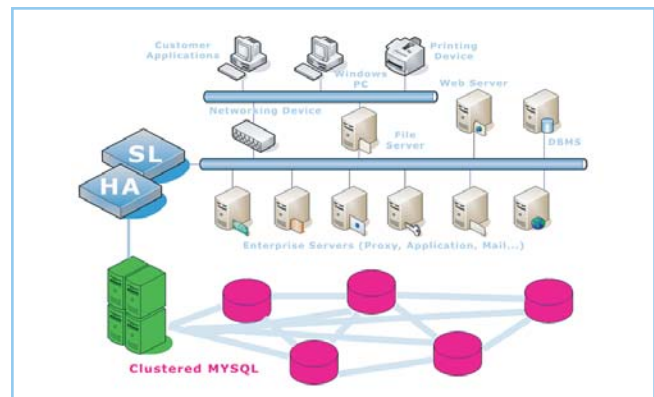
SecureLog already supports over 600 log format parsing templates and the possibility of modifying existent templates

or creating new ones allows the system to index and analyze logs produced virtually by any software or hardware source.

The integrated digital signature feature allows a user to be certain of data integrity even after log files have been extracted from the device. Such feature coupled with data encryption (both during data collection and at the filesystem level) guarantees data integrity through all of the log data life cycle, a feature which is of course fundamental.

SecureLog can be configured with local storing devices or coupled with remote devices, in order to keep virtually any amount of data, therefore satisfying those laws and regulations which require even years of data retention.

Example 3: Enterprise environment



SECURELOG STRENGTHS

SecureLog main advantages are:

- * Logs from different systems can be effortlessly centralized;
- * Data integrity is preserved through all Log File life cycle;
- * Analysis and reporting on collected data can be easily achieved;
- * Security management overall costs can be reduced;
- * SecureLog operates in compliance with Pisanu Law;
- * SecureLog fulfills Basel II, ISO27001 certification, Sarbanes-Oxley Act (SOX), HIPAA (Health), GLBA (finance), Visa Cisp and NIST recommendations in terms of Log retention.



SECURELOG SYSTEM

Secure and Reliable Log Centralization Platform

A Log management system has to be reliable, secure and scalable. SecureLog has been conceived to address such requirements and the outcome is a platform which is able to manage Log Files during their entire life cycles in great security and reliability. Acquisition, transmission, centralization and memorization all take place in a secured, reliable and performing environment.

SECURELOG MAIN FEATURES

- Collector based or standard compatible (Syslog, Syslog-NG) event collection;
- Encrypted data transmission - Rijndael (AES) algorithm;
- Buffered collector transmission;
- Sequence and authenticity controls both at the network and application levels;
- Burst performances on encrypted data: 40.000 - 60.000 events collected per second;
- E-mail alarms in the case of agent malfunction or special events happening;
- Encrypted data storage (Rijndael or Serpent at the filesystem level);
- Data storage possibility on both local disks or other external storage devices (SAN, NAS);
- Ready analysis support for more than 600 types of log formats;
- Possibility of creating new analysis templates;
- Option to define customized reporting filters, with support of regular expression;
- Support for "drill down" analysis operations;
- Original log files are kept and can be easily downloaded in RAW unaltered format;
- Support for digital signature with access to certificates through smart card readers with ISO7816 standard support;
- Virtually unlimited storage scalability;
- Maximum Data Compression: About 10:1;
- Management Interfaces: Web Based GUI on https protocol;
- User ACL: Different management profiles each with different privileges on clients and/or files;
- Hardened Linux operative system.



SECURELOG SYSTEM

Secure and Reliable Log Centralization Platform

REFERENCE HARDWARE PLATFORMS

Model	Hardware	Internal Storage	Events/Sec*
Tower	2 x Dual Xeon 5130 2.0 Ghz - 12 Gb Ram	SAS 2.1 Tb - RAID 5	40.000+
Standard 2U	2 x Dual Xeon 5140 2.33 Ghz - 12 Gb Ram	SAS 1.5 Tb - RAID 5	40.000+
Enterprise 7U	2 x Dual Xeon 3.0 Ghz - 32 Gb Ram	SAS 3.0 Tb - RAID 5	60.000+
Standard Diskless 2U	2 x Dual Xeon 5140 2.33 Ghz - 12 Gb Ram	NA	40.000+
Enterprise Diskless 7U	2 x Dual Xeon 3.0 Ghz - 32 Gb Ram	NA	60.000+

* reference data obtained on events of average size 80bytes, in optimal temperature (22°) and networking conditions

The herein models serve as an example only and SATA HTS reserves the right to replace them with similar or more performing alternatives, depending on the customer requirements and networking structure. Reliable and market leader vendors such as IBM, DELL or HP will only be considered by SATA H.T.S when considering such alternatives. Specific hardware models will be cited in offer sheets.

In order to meet large environments requirements or specific customer needs, additional features or performance enhancing upgrades can be provided. In such cases please feel free to directly contact us.



SATA HTS HI-TECH SERVICES
Palazzo delle Professioni- via Cjavecis, 3 / 33100 Udine , Italy
tel. + 39 0432 499860 fax +39 0432 499831
www.sata-hts.com info@sata-hts.com

Analysis technologies powered by

