DATA SHEET

LT AUDITOR+

SYSLOG SERVER

Real Time Auditing for Network Devices

THE CHALLENGE

Presenting information in easy to read, meaningful reports of critical syslog messages, imbedded in a sea of unintelligible hard to decipher messages, is a huge challenge to meet auditing and compliance requirements.

The application can handle

- Inconsistent log content - Each type of log source represents values differently. For example, date may be represented in MMDDYYYY format while another in MM-DD-YYYY format and sometimes you receive logs with no datetime stamps.
- Inconsistent log formats – There are absolutely no standards followed and users are left to the mercy of the device manufacture's developers to figure out how to interpret messages generated by any device. Typically, there is no common structure and the message is difficult to normalize making it difficult to report and alert on critical information.
- High volume of redundant or useless data – The sheer volume of noise data generated by network devices is a problem because it makes it far more difficult to pinpoint vital events when dealing with a firehose of messages. In most cases noise constitutes 80 to 85% of the total volume of messages generated.

THE SOLUTION

LT Auditor+ Syslog Server is a high-performance log management application that can process in excess of 2 million messages / hour. The application is highly scalable and can be customized to support any syslog device.

LT Auditor+ Syslog Server at a glance:

- Content-based real time alerting - Configure the application to alert you about important and critical events.
- Seamless integration into the LT Auditor+ infrastructure enabling scheduling and generation of superior reports for audit and compliance.
- High throughput centralized collection of syslog messages, from any device on the network with the ability to normalize logs into a consistent format.
- A mechanism to set rules with advanced filtering to retrieve critical information required by an organization and store this information for quick analysis and further processing.
- Exclusion filtering to reduce noise events to improve the quality of logs collected.
- Robust normalization technology to split messages into key-value pairs using parsing techniques and Regular Expressions (RegEx). Splitting messages into Who What Where and When formats.
- Handles all types of messages including JSON messages.
- Installs in minutes and easy to configure.

AUDITED DEVICES

Routers
Switches
Firewalls
VPNs
Wireless Access Points
Other Syslog enabled devices

AUDITED OPERATIONS

Login Activity
Failed Login Activity
Configuration Updates
Connection Opened
Connection Closed
Broadcast Packet Dropped
DNS Packet Allowed
ICMP Packet Dropped
Website Access Denied
TCP Connection Dropped
Website Accessed

DATA SHEET

LT AUDITOR+

SYSLOG SERVER

Real Time Auditing for Network Devices

BLUE LANCE

BENEFITS

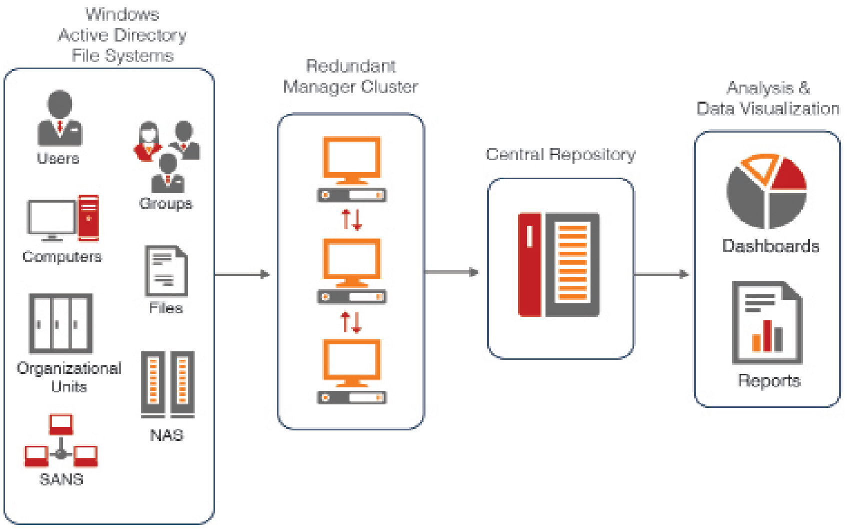
LT Auditor+ Syslog Server is a vital addition to any organization's security arsenal. LT Auditor+ Syslog Server benefits an organization in many ways namely:

- Provides a mechanism for routine reviews and analysis to identify security incidents, policy violations and malicious activity.
- Provides functionality for auditing and forensic analysis.
- Supports an organization's internal investigations and helps to identify operational trends and long-term problems.
- Provides the capability for review, protection, and retention of audit records.

Besides these benefits, LT Auditor+ Syslog Server can be leveraged to meet a number of laws and regulations that compel organizations to store and review certain logs such as

- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability (HIPAA)
- Sarbanes-Oxley Act (SOX) - SOX

Information Flow



ABOUT BLUE LANCE

Blue Lance is a global provider of cybersecurity governance solutions helping organizations protect their digitally managed assets for over 25 years. Blue Lance solutions allow organizations to minimize risk from sophisticated Cyber thieves, complex industry and government regulations. Blue Lance stands with customers as a trusted partner offering cybersecurity governance solutions that enable expanded oversight and validation of audit readiness for internal policies, industry or government regulations; and the safe keeping of confidential information, trade secrets, intellectual property, critical infrastructure, and other digitally managed assets. Blue Lance is headquartered in Houston, Texas.

FEATURES

24x7 Monitoring with real-time alerts

Management Summary reports with drill-down capability

Over 100 security and compliance report templates

Translation and correlation of user activity into plain English reports and alerts

Automatic report scheduling and delivery

Audit access to files, folders

Enterprise-wide data consolidation

Comprehensive Auditing with Granular filtering

Audit the Auditor

Robust, fault tolerant and load balanced architecture

Multi-Manager-Agent architecture

Automatic audit policy deployment