

LogLogic ST Product Family

Reliable Log Archives for Security, Compliance and Availability

Increasingly stringent compliance requirements have prompted best practices groups to recommend more reliable log data archival strategies. Retaining secure log archives is critical to proving regulatory compliance and can be used as legal evidence in court proceedings. A complete record of access, activity, and configuration changes for network devices provides an audit trail for security policy validation.

In addition to compliance, log data archives can assist with network problem remediation and decision support, increasing network performance and improving availability.

IT managers can mine log data for root-cause analysis to aid in system recovery and damage cleanup after a security or performance incident. Due to its many uses, legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley, recommend retaining and protecting log data for up to seven years.

The LogLogic™ ST family of products simplifies, automates and reduces the cost of log data retention by eliminating the need for servers, tape libraries, and archival administrators. With a simple drop-in deployment, the ST appliance instantly begins collecting and securely archiving log data from any and all connected log sources at any message volume. It holds up to two terabytes of compressed data for up to two years and interfaces to NAS devices for longer term archiving. When used with LogLogic's LX appliances, the ST appliance also guarantees complete and accurate transmission of network equipment logs from anywhere on the enterprise WAN.

LogLogic Log Management Appliances

The LogLogic ST family of products provides network administrators:

- **Aggregation:** Centralizes raw log data storage from local and remote syslog-compatible log sources
- **Analysis:** Accelerates problem resolution and validates security policy enforcement through fast log data mining
- **Archives:** Stores unaltered log data for up to two years and connects to external storage networks for infinite scalability
- **Automation:** Automates the entire log data archival process, minimizing administration costs while providing more secure log data capture and retention

Key Benefits

Better

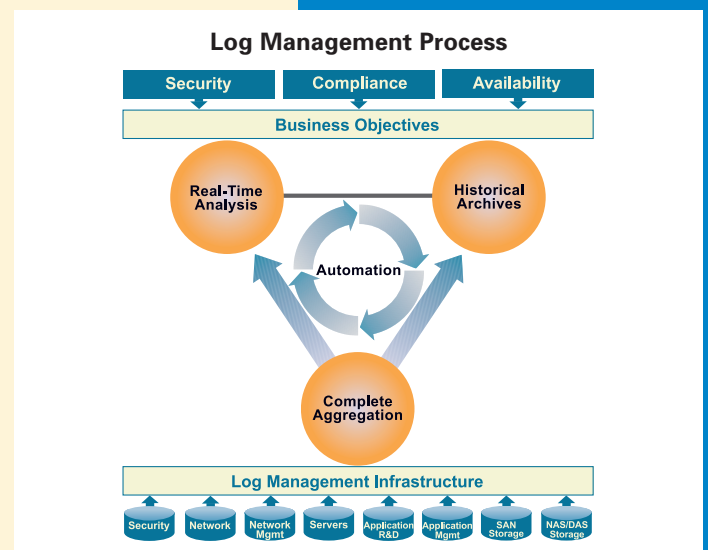
- **End-to-end:** Builds archives for any syslog devices
- **TCO:** Easy to install and maintain

Faster

- **High performance:** Centralizes long-term log data archives
- **Reliability:** Captures complete log data, even under duress

Smarter

- **More useful:** Retains complete, unfiltered records
- **Easier:** Frees up valuable IT resources



Features

Centralized, aggregated storage

The ST appliance provides high-speed log data capture of all remote and central network logs. The LogLogic LX appliance collects the data from all syslog-compatible log sources and sends it to the ST appliance for centralized data archives. Log data can be TCP encapsulated and scrambled to ensure safe data transmission to the ST appliance. In addition, automatic remote buffering of network logs can prevent any data from being lost in case of a WAN failure. To ensure maximum reliability of log data aggregation, the ST appliance offers RAID-5 storage, redundant fans and hot swappable power supplies, automated backup and hot standby/failover capabilities.

Fast analysis of archival data

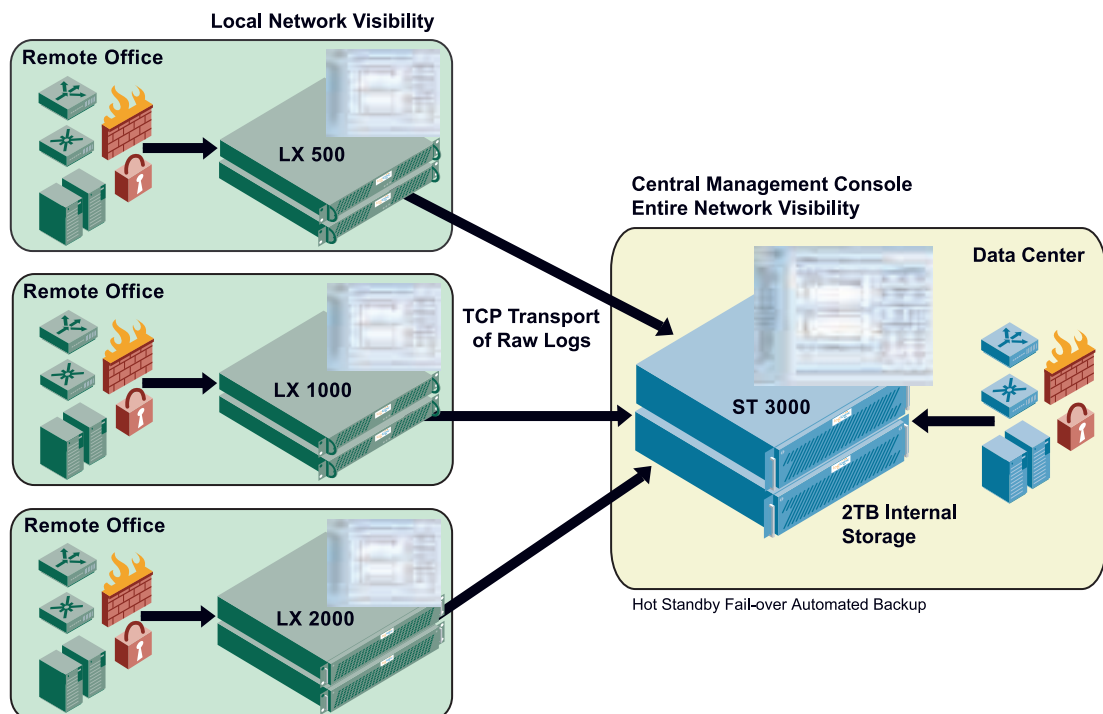
The ST appliance provides a flexible search interface so that network administrators can easily retrieve the information they need for investigating security, compliance or availability issues. The ST appliance is managed by a central, browser-based management console and benefits from LogLogic's new domain virtualization technology. Administrators can search through all log data sources, independent of their physical locations and the appliances to which they are attached.

Reliable, secure archives

The ST appliance provides centralized, secure log data archives that are physically separate from the metalogs used for real-time analysis. It retains up to two years of log data and connects to NAS storage networks for longer term archival. Because the data is archived without the intervention of software agents or proprietary database structures, it is more credible when used as evidence in court or to prove regulatory compliance. The LogLogic solution provides additional log data protection in the form of compression, and an MD5 key is stored in a separate location to make the log archives tamper-proof.

Automated data retention

By automating the entire log data archival process, the ST appliance minimizes administration costs while providing more secure log data capture and retention. The ST appliance is easy to use, requiring minimum installation, zero training, and no additional hardware or software. Its self-maintaining database eliminates the need for a database administrator. Additionally, the ST appliance auto-discovers new network log sources, further reducing the cost of maintenance and administration.



Applications

Log data protects intellectual property

According to the American Chamber of Commerce, enterprises lose an average of \$1,250,000 annually due to Intellectual Property (IP) theft. Using log data to monitor ongoing user activity deters IP theft. Furthermore, since the ST appliance saves all log data in its original form, without intervention from software agents or proprietary database structures, it is more credible as evidence and can serve as a valuable resource in compliance investigations and legal proceedings.

Log data access simplifies compliance efforts

Log data provides an independent third-party audit trail of all access and activity as well as configuration changes. Best practices groups recommend keeping two copies of logs - one for everyday monitoring and the other for long-term archiving. They also recommend retaining a complete, unaltered copy of all log data for up to seven years. However, with network equipment producing terabytes of log data every year, the process of collecting, securing, and providing access to log data is complex. Server, storage, tape library, and storage administration costs continue to escalate, making capturing complete log data from new network devices increasingly expensive. To add to the problem, data must be mined manually, a time-consuming and costly

process. With the ST appliance, all data required to prove compliance is securely archived, while remaining immediately searchable and retrievable. By eliminating manual data mining, the ST appliance helps enterprises reduce the costs and resources spent on regulatory compliance.

Rapid log data access increases network availability

When responding to security breaches or network performance issues, time is of the essence. Fast access to archival log data helps with root-cause analysis and accelerates problem remediation, improving network availability and performance. However most data archives are not easily searchable; data must be mined by hand with time-consuming scripts that push up labor costs and slow response times. Furthermore, data from disperse sources may be stored separately, making data correlation difficult. Without a centralized bank of accessible data, many organizations spend tremendous time and resources searching for the data they need to troubleshoot network problems. The resulting delays can decrease network availability, as problems go untreated. The ST appliance stores raw log data in flat text files of one-minute increments, which accelerates time-based searching through years of data. In addition, the ST appliance offers a flexible text-based search interface to make the process of hunting for the relevant data quick and efficient.

Features and Benefits

Better End-to-end <ul style="list-style-type: none">■ Unaltered, complete raw log data retention■ Up to 12:1 raw log data compression■ Raw logs for real-time and historical analysis	Faster High-performance <ul style="list-style-type: none">■ High-speed log data capture■ Automated backup and retrieval procedures■ Protected log data transfer and retention	Smarter More useful <ul style="list-style-type: none">■ Internal storage or external networked storage■ Supports any syslog device■ Provides raw logs for any application
TCO <ul style="list-style-type: none">■ Dedicated, plug-and-play appliance■ No installation or training required■ Automated log data archival procedures	Reliability <ul style="list-style-type: none">■ Three-tiered role-based access■ Secure S-HTTP access■ MD5 hash tamper protection	Easier <ul style="list-style-type: none">■ Flexible search interface■ Log aggregation from local and remote sources■ Collation into one central log data archive

Product Specifications



System Management

- Command Line Interface
- Web-based GUI (Internet Explorer, Netscape, Mozilla, Firefox)
- Built-in central management station
- SNMP support

High Availability

- Hot standby and fail-over for log message capture
- Hot swappable redundant power supplies
- Redundant fans
- RAID-5 storage (ST 3000)

Operating Environment

- Linux hardened and optimized kernel

Device Support

- All syslog protocol compliant devices including firewalls, VPNs, routers, switches, servers and other devices.
- OPSEC LEA including firewalls and VPN systems.

Safety and Emissions Certification

- **Safety:** UL-Safety, CB to IEC 60950: 1999, 3rd edition; TUV GS mark to EN60950: 2000; TUV C-US to UL60950: 2000; CAN/CSA-C22.2 No 60950: 2000
- **Emissions:** FCC Class B, VCCI Class B, CE class B, C-Tick, ICS, EN 60.950/IEC



Appliance Specifications	ST 2000	ST 3000
Sustained message per second (mps) rate	50,000 mps	50,000 mps
Compression ratio	up to 12:1	up to 12:1
Management station	available	available

Hardware Specifications	ST 2000	ST 3000
CPU	2x 2.8 GHz Xeon	2x 2.8 GHz Xeon
Memory	2 GB	2 GB
System storage	2x 80 GB SATA RAID	2x 80 GB SATA RAID
Data storage	NAS	10x 250 GB SATA RAID
Power	2x 350 W	2x 460 W
Chassis	2u	3u
Ethernet	1x 10/100 1x 10/100/1000	1x 10/100 1x 10/100/1000
Console port	9-pin serial	9-pin serial

LogLogic, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Product Specifications are subject to change without notice.



LogLogic, Inc.
1154 E. Arques Ave.
Sunnyvale, CA 94085
www.loglogic.com

US Toll Free: 888 347 3883
Tel: +1 408 215 5900
Fax: +1 408 774 1752
info@loglogic.com