syslog-ng Store Box

PRODUCT DESCRIPTION

BalaBit
IT Security

Introduction

Log messages contain information about the events happening on the hosts. Monitoring system events is essential for security and system health monitoring reasons. A well-established log management solution offers several benefits to an organization. It ensures that computer security records are stored in sufficient detail, and provides a simple way to monitor and review these logs. Routine log reviews and continuous log analysis help to identify security incidents, policy violations, or other operational problems. Logs also often form the base of auditing and forensic analysis, product troubleshooting and support. There are also several laws, regulations and industrial standards that explicitly require the central collection, periodic review, and long-time archiving of log messages. Examples to such regulations are the Sarbanes-Oxley Act (SOX), the Basel II accord, the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI-DSS).

Built around the popular syslog-ng application used by thousands of organizations worldwide, the syslog-ng Store Box (SSB) brings you a powerful, easy to configure appliance to collect and store your logs. Using the features of the latest syslog-ng Premium Edition to their full power, SSB allows you to collect, process, and store log messages from a wide range of platforms and devices.

All data can be stored in encrypted, digitally signed, and optionally timestamped files, preventing any modification or manipulation, satisfying the highest security standards and policy compliance requirements.

Application areas

Central log collection and archiving

SSB offers a simple, reliable, and convenient way of collecting log messages centrally. It is essentially a high-capacity log server with high-availability support. Being able to collect logs from several different platforms makes it easy to integrate into any environment.

Secure log transfer and storage

Log messages often contain sensitive information and also form the base of audit trails for several applications. Preventing eavesdropping during message transfer and unauthorized access once the messages reach the logserver is essential for security and privacy reasons.

Automated log monitoring and log preprocessing

Monitoring log messages is an essential part of system-health monitoring and security incident detection and prevention. SSB offers a powerful platform that can classify tens of thousands of messages real-time to detect messages that deviate from regular messages, and promptly raise alerts. Although this classification does not offer as complete inspection as a log analyzing application, SSB can process much more messages than a regular log analyzing engine, and also filter out unimportant messages to decrease the load on the log analyzing application.

Policy compliance

Many organization must comply to regulations like the Sarbanes-Oxley Act (SOX), the Basel II accord, the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI-DSS). These regulations often have explicit or implicit requirements about log management, such as the central collection of log messages, the use of log analysis to prevent and detect security incidents, or guaranteeing the availability of log messages for an extended period of time – up to several years. SSB helps these organizations to comply with these regulations.

Typical end-users

The syslog-ng application is used worldwide by companies and institutions who collect and manage the logs of several hosts, and want to store them in a centralized, organized way. Using syslog-ng is particularly advantageous for:

- Internet Service Providers;
- Financial institutions and companies requiring policy compliance;
- Server, web, and application hosting companies;
- Data centers;
- Wide area network (WAN) operators;
- Server farm administrators.

Product features and benefits

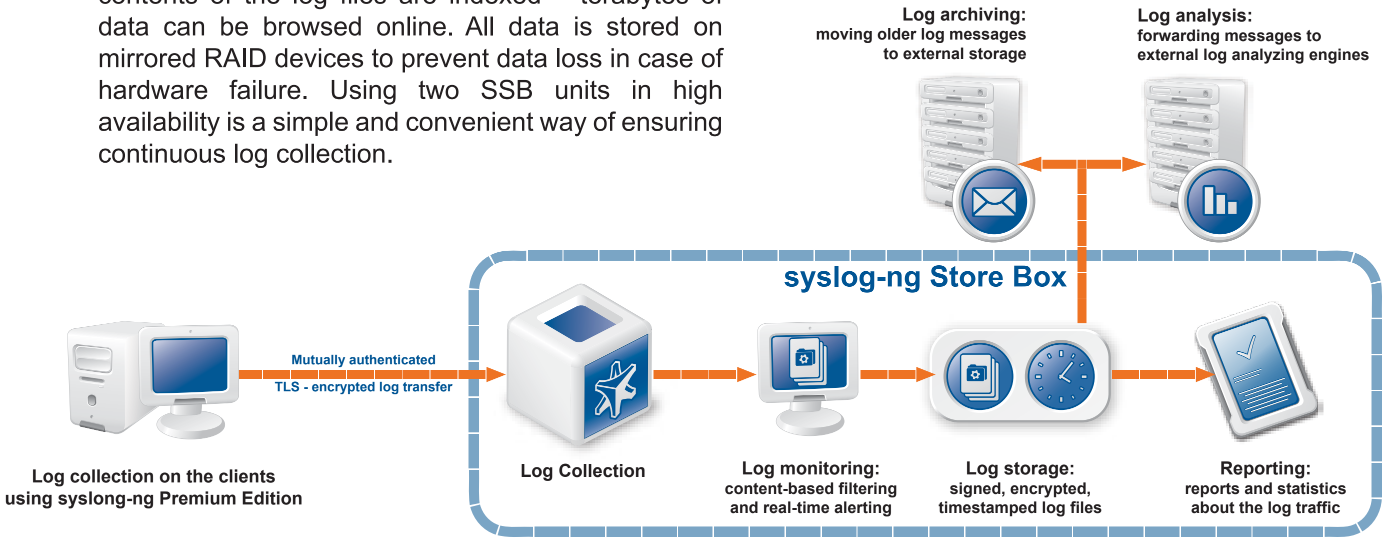
- Secure log collection using TLS
- Trusted, encrypted, signed, timestamped storage
- Log collectors for Unix and Windows platforms
- Forward messages to log analyzing engines
- Supports the latest IETF syslog protocol standard
- Fine-tuned access control to your logs
- Easy integration into your existing infrastructure
- Supports High Availability
- Built on reliable hardware from Sun Microsystems
- Manage easily from a web browser
- Automatic data archiving and backup
- One year support, warranty, and upgrades included in the base price

Secure, reliable log transfer

The syslog-ng Store Box can receive log messages sent using both the legacy BSD-syslog protocol, as well as the latest syslog protocol standards. Transferring messages to SSB is supported using the UDP, TCP, and TLS protocols. Mutual authentication of the TLS-encrypted channels maintains the integrity and confidentiality of the transferred information. Using syslog-ng to transfer the log messages helps you avoid losing messages even in case of network or hardware errors.

Trusted, timestamped log storage

The syslog-ng Store Box can store log messages securely in encrypted, compressed, and digitally signed binary files. That way any sensitive data is available only for authorized personnel who have the appropriate encryption key. Sections of the log files can be timestamped; timestamps can be requested from external Timestamping Authorities as well. The contents of the log files are indexed – terabytes of data can be browsed online. All data is stored on mirrored RAID devices to prevent data loss in case of hardware failure. Using two SSB units in high availability is a simple and convenient way of ensuring continuous log collection.



Direct database access

In addition to storing your log messages locally, SSB can also forward them directly to databases , or remote servers, including log analyzing applications. The following databases are supported: MySQL, Microsoft SQL (MSSQL), Oracle, and PostgreSQL.

Managing SSB

SSB is configured from a clean, intuitive web interface. The roles of each SSB administrator can be clearly defined using a set of privileges:

- manage SSB as a host;
- manage log collection, forwarding and storage;
- configure various alerts;
- browse the collected logs reports.

The web interface is accessible via a network interface dedicated to the management traffic. This management interface is also used for backups, sending alerts, and other administrative traffic. All configuration changes are automatically logged, simplifying the auditing of SSB.

Fine-tuned access control

The SSB web interface features highly customizable access control. Using this together with the powerful message-sorting capabilities of syslog-ng, you can exactly specify which log messages a user has access to. For example, it is possible to grant access only to the logs of a specific application to the support engineer of that application – it is even possible to narrow the time frame of the data only to the relevant period.

LDAP integration

SSB can connect to a remote LDAP database (e.g., a Microsoft Active Directory server) to resolve group memberships of the users who access the SSB web interface. Privileges to configure SSB or browse different logs can be defined based on group memberships.

Real-time log monitoring and alerting

Even though SSB is not a log analyzing engine, it is able to classify individual log messages using artificial ignorance, much like the popular logcheck application of the Unix world. SSB comes with a built-in database of log message patterns that are considered “normal”. Messages matching these patterns are produced during the legitimate use of the applications (e.g., sendmail, Postfix, MySQL, etc.), and are unimportant from the log monitoring perspective, while the remaining messages may contain something “interesting”. The administrators can define log patterns on the SSB interface, label matching messages (e.g., security event, etc.) and request alerts if a specific pattern is encountered. For thorough log analysis, SSB can also forward the incoming log messages to external log analyzing engines.

Log collector agent for several platforms

SSB uses the syslog-ng Premium Edition application to collect logs from different operating systems and hardware platforms, including Linux, Unix, BSD, Sun Solaris, HP-UX, IBM AIX, IBM System i, as well as Microsoft Windows XP, Server 2003, Vista, and Server 2008.

Agent for Microsoft Windows platforms

The syslog-ng Agent for Windows is a log collector and forwarder application for Microsoft Windows platforms, including Windows Vista and Windows Server 2008. It collects the log messages from eventlog groups and log files and forwards them to a syslog-ng server using regular or TLS-encrypted TCP connections. The syslog-ng Agent can be managed from a domain controller using group policies, or run as a standalone application.

Agent for IBM System i platforms

The syslog-ng agent for IBM System i is a system log collector and forwarder application for the IBM System i (formerly known as AS/400 and IBM iSeries) platform. It collects application and system messages, as well as messages from the System i security audit journal (QAUDJRN) and the operator message queue (QSYSOPR). The collected messages are forwarded to a syslog-ng server using regular or TLS-encrypted TCP connections. The syslog-ng server can run on a separate machine, or directly on IBM System i in the Portable Application Solutions Environment (PASE). The syslog-ng Agent for IBM System i is available as a standalone product and must be licensed independently from syslog-ng Store Box.

Automatic data and configuration backups

The recorded log messages and the configuration of SSB can be periodically transferred to a remote server using the following protocols:

- Network File System protocol (NFS);
- Rsync over SSH;
- Server Message Block protocol (SMB/CIFS).

The latest backup – including the data backup – can be easily restored via SSB's web interface.

Automatic data archiving

SSB's configuration and the recorded log messages are automatically archived to a remote server. The data on the remote server remains accessible and searchable; several terabytes of audit trails can be accessed from the SSB web interface. SSB uses the remote server as a network drive via the Network File System (NFS) or the Server Message Block (SMB/CIFS) protocol.

High Availability support

When log messages are sent to SSB and not stored locally, SSB becomes a single point of failure. If SSB fails, the collected logs are unavailable and might be lost forever. Since this is not acceptable for critical servers and services, SSB is available with HA support. In this case, two SSB units (a master and a slave) having identical configuration operate simultaneously. The master shares all data with the slave node, and if the master unit stops functioning, the other one becomes immediately active, so the servers are continuously accessible. SSB5000 and larger versions are also equipped with dual power units.

Handle extreme load

The syslog-ng Store Box is optimized for performance, and can handle enormous amount of messages. Depending on its exact configuration, it can process over 75,000 messages per second real-time, and over 24 GB raw logs per hour. Larger versions of the appliance (SSB5000 and SSB10000) include their own storage solutions capable of storing up to 10 Terabytes of data.

Software upgrades

Software upgrades are provided as firmware images – upgrading SSB using the SSB web interface is as simple as upgrading a network router. SSB stores up to five previous firmware versions; any one of them can be booted, allowing easy rollback in case of any problems. Upgrades for syslog-ng Premium Edition – the log collector agent of SSB – are available from the BalaBit website. Firmware upgrades for SSB and software updates of syslog-ng Premium Edition for one year are included in the base price of every SSB unit.

Support and warranty

The base price of all SSB units includes the following services:

- One-year online and phone support, available Monday-Friday from 9:00 to 18:00, CET.
- On-site hardware replacement warranty for one year. All hardware errors are corrected at your facility.
- Software updates for SSB and its log collector agents for one year.

Contact your local distributor for details on extended support and warranty.

Hardware specifications

SSB appliances are built on high performance, energy efficient, and reliable servers from Sun Microsystems that are easily mounted into standard rack mounts. Larger models include storage solutions.

syslog-ng Store Box SSB500

Sun Fire X2100 M2 (1xOpteron Dual Core CPU, 2 GB RAM, 500 GB SATA HDD, RAID1)
Software license for maximum 50 Log Source Hosts.

syslog-ng Store Box SSB5000

Sun Fire X4140 (1xOpteron Quad Core CPU, 4 GB RAM, redundant power supply, 5 TB SATA HDD in external storage, RAID6) Software license for unlimited Log Source Hosts. The high availability option applies only to the X4140 server, the external storage is not duplicated.

syslog-ng Store Box SANControl

Sun Fire X4140 (2xOpteron Quad Core CPU, 8 GB RAM, redundant power supply, iSCSI/FC SAN controller card) Software license for unlimited Log Source Hosts.

syslog-ng Store Box SSB1000

Sun Fire X2200 M2 (1xOpteron Quad Core CPU, 2 GB RAM, 1 TB SATA HDD, RAID1)
Software license for maximum 250 Log Source Hosts.

syslog-ng Store Box SSB10000

Sun Fire X4140 (2xOpteron Quad Core CPU, 8 GB RAM, redundant power supply, 10 TB SATA HDD in external storage, RAID 6) Software license for unlimited Log Source Hosts. The high availability option applies only to the X4140 server, the external storage is not duplicated.

syslog-ng Store Box SSB10000DS

Sun Fire X4540 (2xOpteron Quad Core CPU, 32 GB RAM, redundant power supply, 10 TB SATA HDD in internal storage, RAID 60) Software license for unlimited Log Source Hosts.

Free evaluation

A demo version of SSB is available as a VMware image upon request.

TO TEST THE SYSLOG-NG STORE BOX, REQUEST AN EVALUATION VERSION AT HTTP://WWW.BALABIT.COM/MYBALABIT/