BalaBit
IT Security

THE SYSLOG-NG STORE BOX

High Performance Log Management Appliance

Highlights

High performance collection and indexing

Filtering, parsing, rewriting, normalization

Rapid search through billions of messages

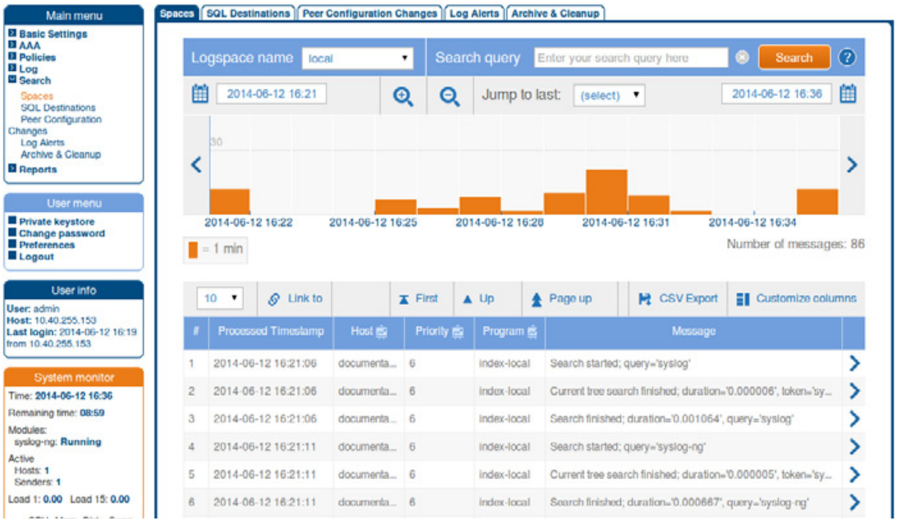
Customized reporting

Easy integration with 3rd party tools via REST API

Secure, encrypted transport and storage

Granular access control

The syslog-ng Store Box™ (SSB) is a high-performance, high-reliability log management appliance that builds on the strengths of the syslog-ng Premium Edition. With SSB, you can collect and index log data, perform complex searches, secure sensitive information with granular access policies, generate reports to demonstrate compliance, and forward log data to 3rd party analysis tools.



User: admin
Host: 10.40.255.153
Last login: 2014-06-12 16:19 from 10.40.255.153

Time: 2014-06-12 16:36
Remaining time: 08:59
Modules:
syslog-ng: Running
Active
Hosts: 1
Senders: 1
Load 1: 0.00 Load 15: 0.00

Logspace name: local
Search query: Enter your search query here
2014-06-12 16:21
Jump to last: (select)
2014-06-12 16:36

Number of messages: 86

10

#	Processed Timestamp	Host	Priority	Program	Message
1	2014-06-12 16:21:06	documenta...	6	index-local	Search started; query='syslog'
2	2014-06-12 16:21:06	documenta...	6	index-local	Current tree search finished; duration='0.000006', token='sy...
3	2014-06-12 16:21:06	documenta...	6	index-local	Search finished; duration='0.001064', query='syslog'
4	2014-06-12 16:21:11	documenta...	6	index-local	Search started; query='syslog-ng'
5	2014-06-12 16:21:11	documenta...	6	index-local	Current tree search finished; duration='0.000005', token='sy...
6	2014-06-12 16:21:11	documenta...	6	index-local	Search finished; duration='0.000667', query='syslog-ng'

Collect and index log data at unparalleled speeds

SSB uses the syslog-ng Premium Edition as log collection agents which provides reliable log collection and transfer with local disk buffering, client-side failover, and application level acknowledgement via the Reliable Log Transfer Protocol (RLTP™). Installers are available for 50+ platforms, including the most popular Linux distributions, commercial versions of UNIX and Windows.

The syslog-ng Store Box's indexing engine is optimized for performance. Depending on its exact configuration, one syslog-ng Store Box can collect and index up to 100,000 messages per second for sustained periods. A single SSB can collect log messages from more than 5,000 log sources.When deployed in a client-relay configuration, a single SSB can collect logs from tens of thousands of log sources.

Search, troubleshoot, and report

With SSB's full-text search, you can search through billions of logs in seconds via the intuitive web-based user interface. Wildcards and Boolean operators allow you to perform complex searches and drill down on the results. Users can gain a quick overview of their IT environment and identify problems. Users can easily create **customized reports** from the charts and statistics they create on the search interface to demonstrate compliance with standards and regulations such as PCI-DSS, ISO 27001, SOX and HIPAA.

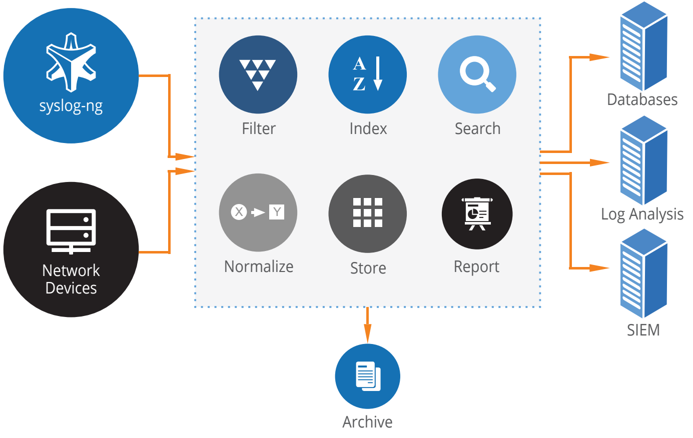
Filter and normalize

SSB offers flexible filtering capabilities based on message meta-data and message content to reduce the noise generated in high traffic environments and segment data for better search and analysis.

The **PatternDB™** can classify incoming logs in real-time based on message content, assign name/value pairs, and correlate messages to normalize logs, allowing you to aggregate disparate log formats to search and generate statistics.

Parsing and rewriting capabilities allow you to transform logs based on filters or PatternDB™ results to reduce the complexity of log data improving search and analysis performance.

SSB



Secure your log data

Logs can be transferred from syslog-ng Premium Edition clients to SSB using **Transport Layer Security (TLS)** encryption, protecting any sensitive data.TLS allows the mutual authentication of the host and the server using X.509 certificates.

SSB's **Logstore** stores log data in encrypted, compressed, and time-stamped binary files, restricting access to authorized personnel only.

Authentication, Authorization and Accounting settings provide **granular access control** restricting access to the SSB configuration and stored logs based on usergroup privileges. SSB can be integrated with LDAP and Radius databases.

Licensing and support

Licensing is based on the number of Log Source Hosts (LSH) that send logs to the SSB and its hardware configuration. There are no license limits on the amount or rate of data processed or stored, making project budgeting easy. Purchasing SSB entitles you to access binary installation files for syslog-ng Premium Edition for more than 50 server platforms. Product support – including 7x24 support – is available on an annual basis. Support subscriptions entitle customers to software upgrades and hardware replacement.

Store and forward

With SSB you can store large amounts of log data, create automated retention policies, and backup data to remote servers. The largest SSB appliance can store up to 10 terabytes of uncompressed data.

SSB provides **automatic data archiving** to remote servers.The data on the remote server remains accessible and searchable; several terabytes of log data can be accessed from the SSB web interface. SSB uses the remote server as a network drive via the NetworkFile System (NFS) or the Server Message Block (SMB/CIFS) protocol.

You can also forward logs to 3rd party analysis tools or fetch data from SSB via its **REST API**. You can access the API using a RESTful protocol over HTTPS, meaning that you can use any programming language that has access to a RESTful HTTPS client to integrate SSB into your environment, including popular languages such as Java and Python.

High Availability

SSB can be deployed in a high availability configuration. In this case, two SSB units (a master and a slave) having identical configurations operate simultaneously. The master shares all data with the slave node, and if the master unit stops functioning, the other one becomes active immediately, so the servers are continuously accessible. SSB T4 and larger versions are also equipped with dual power units.

Hardware Specifications

Product	Unit	Redundant PSU	Processor	Memory	Useful Capacity	RAID	IPMI
SSB T-1	1	No	Intel(R) Xeon(R) X3430 @ 2.40GHz (4 cores)	2 x 4 GB (DDR3)	1 TB	Software raid	Yes
SSB T-4	1	Yes	Intel(R) Xeon(R) E3-1275V2 @ 3.50GHz (4 cores)	2 x 4 GB (DDR3)	4 TB	LSI MegaRAID SAS 9271-4i	Yes
SSB T-10	2	Yes	2 x Intel(R) Xeon(R) E5-2630V2 @ 2.6GHz (6 cores)	8 x 4 GB (DDR3)	10 TB	LSI MegaRAID SAS 9271-4i	Yes

Virtual Appliances

SSB-VA	Virtual Appliance	VMWare ESXi/ESX	Microsoft Hyper-V

Read more about syslog-ng Store Box

Request an evaluation

Request a callback

ABOUT BALABIT

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring and log management to help protect customers against internal and external threats and meet security and compliance regulations. BalaBit is known for its open source log management application, syslog-ng, which has more than 1 million users worldwide.

www.balabit.com