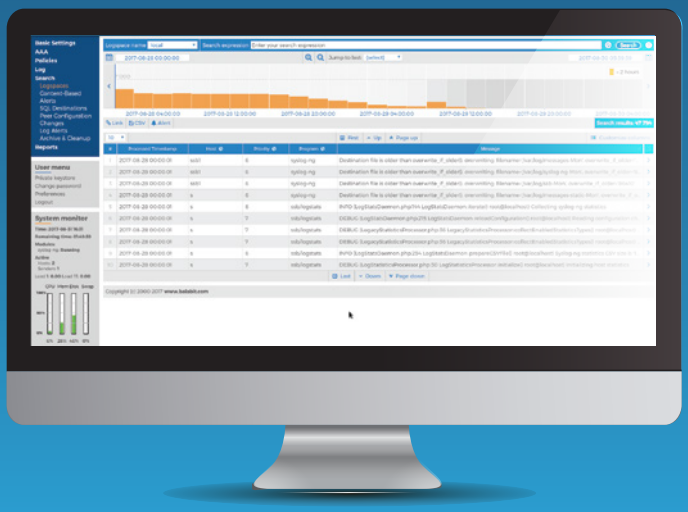
BALASYS

One Identity syslog-ng Store Box

High Performance Log Management Appliance

BENEFITS

- High performance collection and indexing
- Filtering, parsing, rewriting, normalization
- Rapid search through billions of messages
- Alerts based on automated search queries
- Easy integration with 3rd party tools via REST API
- Secure, encrypted transport and storage
- Granular role-based access control
- Multi-logspace searches



INTRODUCTION

syslog-ng™ Store Box (SSB) is a high performance, high reliability log management appliance that builds on the strengths of 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.

Collect and index log data at unparalleled speeds

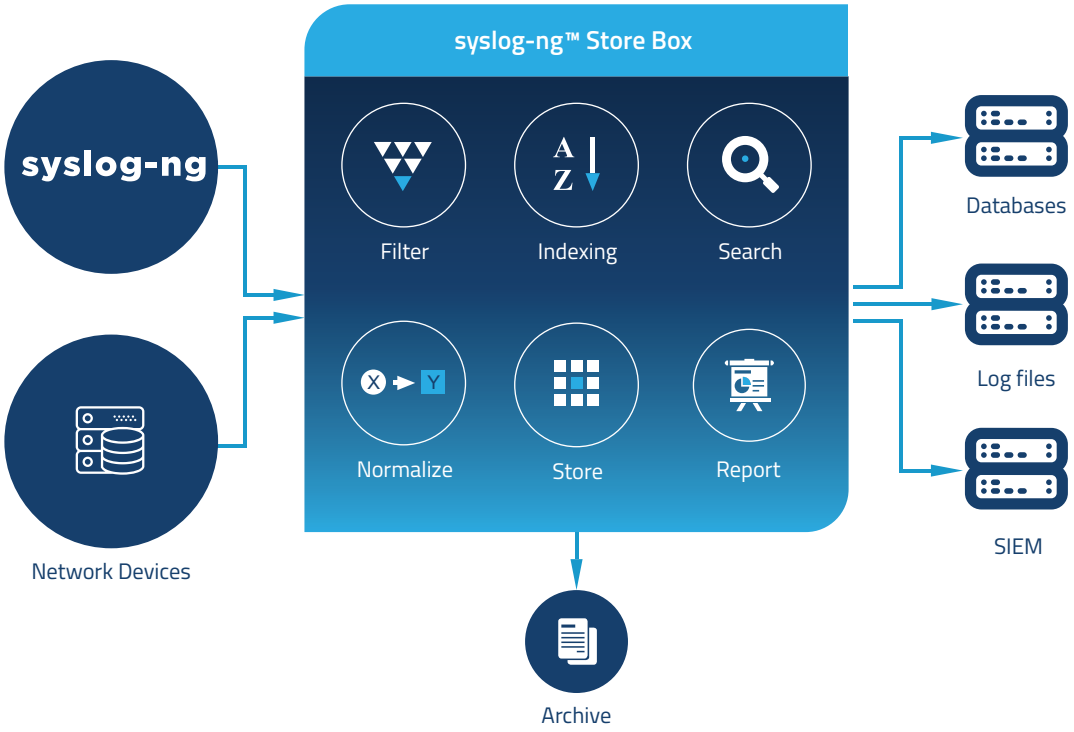
SSB uses the syslog-ng™ Premium Edition as log collection agents. Installers are available for 50+ platforms, including the most popular Linux distributions, commercial versions of UNIX and Windows. Depending on its configuration syslog-ng™ can collect up to 650,000 messages per second.

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 10,000 log sources when deployed in a client-relay configuration.

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. It offers an automatic search functionality for quicker detection of anomalies: SSB is able to search on the incoming log data and sends an alert when a critical event is detected.

Users can easily create customized reports to demonstrate compliance with standards and regulations such as PCI-DSS, ISO 27001, SOX and HIPAA.



Filter and normalize

The PatternDB™ can classify incoming logs in real-time based on message content, extract named information elements from unstructured log messages, allowing you to aggregate disparate log formats to search and generate statistics.

Parsing and rewriting capabilities allow you to transform and normalize logs based on filters and PatternDB™ results to enable effective search and analysis.

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 audit trails can be accessed from the SSB webinterface. SSB uses the remote server as a network drive via the Network File 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.

Search across multiple logspaces, appliances and locations

SSB collects and indexes logs in virtual containers called logspaces that enable organizations to segment their log data based on any number of criteria and restrict access to logs based on user profiles. With the multi-logspace search feature, you can search log data in multiple logspaces whether on the same SSB appliance or located on a different appliance even in a remote location. The ability to search across multiple appliances offers organizations the option to scale out their log management by adding additional appliances in a costs effective way.

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 timestamped 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 (PE) 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.

High Availability

SSB can be deployed in a high availability configuration. In this case, two SSB units (a master and a slave) having identical configuration operate simultaneously. The mastershares 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. 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 Appliance

SSB-VA	Virtual Appliance	VMWare ESXi/ESX	Microsoft Hyper-V	Amazon Web Services	Microsoft Azure

ONE IDENTITY™

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.