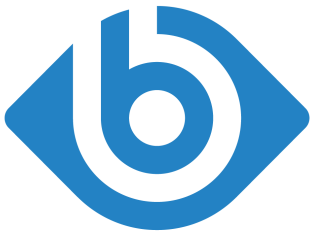
# What is new in syslog-ng Store Box 4 LTS

**January 21, 2016**



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

# Table of Contents

1. Preface ..... 3
2. New hardware appliance ..... 4
3. General improvements and changes ..... 5
4. Improvements and changes from feature releases ..... 6

# 1. Preface

Welcome to syslog-ng Store Box (SSB) version 4 LTS and thank you for choosing our product. This document describes the new features and most important changes since the latest release of SSB. The main aim of this paper is to aid system administrators in planning the migration to the new version of SSB. The following sections describe the news and highlights of SSB 4 LTS.

This document covers the syslog-ng Store Box 4 LTS product.

**Note**
For step-by-step instructions on upgrading to 4 LTS see *How to upgrade to syslog-ng Store Box 4 LTS* at *https://www.balabit.com/support/documentation/*.

As of June 2011, the following release policy applies to syslog-ng Store Box:

- *Long Term Supported or LTS releases* (for example, SSB 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, SSB 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SSB 4 F1) are supported for 6 months after their original publication date and for 2 months after succeeding Feature or LTS Release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new feature per release. Only the last of the feature releases is supported (for example when a new feature release comes out, the last one becomes unsupported).

**Warning**
Downgrading from a feature release to an earlier (and thus unsupported) feature release, or to the previous LTS release is not supported.

## 2. New hardware appliance

syslog-ng Store Box 4 LTS supports new, improved hardware appliances that provide more computing power and increased I/O speed to meet your increasing auditing and processing needs. Every SSB delivered after September 30, 2014 is shipped on the new hardware. If you have bought SSB earlier and would like to buy a new appliance, contact your local BalaBit distributor, or directly <sales@balabit.com>. The following table summarizes the specification of the new appliances.

| Product | SSB T-1 | SSB T-4 | SSB T-10 |
|---|---|---|---|
| Redundant PSU | No | Yes | Yes |
| Processor | Intel(R) Xeon(R) X3430 @ 2.40GHz | Intel(R) Xeon(R) E3-1275V2 @ 3.50GHz | 2 x Intel(R) Xeon(R) E5-2630V2 @ 2.6GHz |
| Memory | 2 x 4 GB | 2 x 4 GB | 8 x 4 GB |
| Capacity | 2 x 1 TB | 4 x 2 TB | 13 x 1 TB |
| RAID | Software RAID | LSI MegaRAID SAS 9271-4i SGL | LSI 2208 (1GB cache) |
| IPMI | Yes | Yes | Yes |
| NIC | 2x Intel® 82574L Gigabit Ethernet Controllers (Label 1, 2)<br><br>Supermicro AOC-SG-i2 Dual GbE PCI-E x4 (Label 3, 4) | 2x Intel® 82574L Gigabit Ethernet Controllers (Label 1, 2)<br><br>Supermicro AOC-SG-i2 Dual GbE PCI-E x4 (Label 3, 4) | Intel® i350 Dual Port Gigabit Ethernet (Label 1, 2)<br><br>Supermicro AOC-SG-i2 Dual GbE PCI-E x4 (Label 3, 4) |

*Table 1. Hardware specifications*

## 3. General improvements and changes

- Security changes from version 4.0.1:
  For accessing the web interface, SSLv3 and medium or weak ciphers are no longer supported. This renders Internet Explorer 7 incompatible.

  For SSH access, the list of supported SSH ciphers and HMAC algorithms has also changed. Only the following ciphers are supported SSH connections:

  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - arcfour
  - arcfour128
  - arcfour256

  Only the following HMAC algorithms are supported for SSH connections:

  - hmac-sha1
  - hmac-ripemd160
- Redundant high availability (HA) gateways can no longer be configured from version 4.0.1. To avoid HA status warnings, move all SSB appliances in the HA cluster to the same network domain.
- The SAN support is discontinued from version 3 F1. If you have SANConnect, do not upgrade to version 4 LTS.
- Support for Sun hardware is discontinued from version 3 F1. If you have Sun hardware, do not upgrade to this release.
- It is not required to manually decompress the license file. Compressed licenses (for example `.zip` archives) can also be uploaded.
- For details on the fixed issues see *our issue tracking page*.

# 4. Improvements and changes from feature releases

**Changes in SSB 3 F1:**

- *Collecting messages from relational databases (SQL):* SSB can collect messages from the following relational databases: Microsoft SQL (MSSQL), MySQL, Oracle and PostgreSQL. SSB can connect to a database, collect records from a table and then create a message from each record. Every query executed by the SQL source can be customized. For details, see *Section 7.4, Creating SQL message sources in SSB* in *The syslog-ng Store Box 4 LTS Administrator Guide*.
- *Multithreaded mode:* The syslog-ng application inside SSB is running in multithreaded mode to scale to multiple CPUs or cores for increased performance.
- *Performance improvements:* The measurements were conducted under the following conditions: from 10 sources, 140 bytes long normal UNIX logs sent to an indexed logstore, with empty PatternDB, on SSB10000.
  - The message rate has been improved from 24 Gb/h in version 3 LTS to 37 Gb/h in version 3 F1.
  - The average collecting and indexing rate has been improved from more than 45,000 msg/sec in version 3 LTS to more than 70,000 msg/sec in version 3 F1.
- The period after idle sessions of the SSB web interface time out can be customized. For details, see *Section 4.2.3, Web interface timeout* in *The syslog-ng Store Box 4 LTS Administrator Guide*.
- The sender address of the e-mails sent by SSB can be customized. For details, see *Procedure 4.5.1, Configuring e-mail alerts* in *The syslog-ng Store Box 4 LTS Administrator Guide*.
- It is now possible to configure HA clusters stretched across long distances, such as nodes across buildings, cities or even continents. For details, see *Section 6.2.2, Asynchronous data replication* in *The syslog-ng Store Box 4 LTS Administrator Guide*.
- It is now possible to configure patterns for multiline messages in the Pattern Database. For details, see *Section 14.7, Using pattern parsers* in *The syslog-ng Store Box 4 LTS Administrator Guide*.
- For details on the fixed issues see *our issue tracking page*.

**Changes in SSB 3 F2:**

- *RPC API:* Access and query the log messages stored on SSB from remote applications. 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 to your environment.
  Accessing SSB with the RPC API offers several advantages:
  - Integration into custom applications and environments.
  - Flexible, dynamic search queries.
  - Search in multiple logstores: execute multiple search-queries and merge the results.
  - Include search results and statistics directly in customized reports created using a custom or third-party application.
  - Correlate the log messages with a custom application.

  For details, see *Chapter 15, The SSB RPC API* in *The syslog-ng Store Box 4 LTS Administrator Guide*.

- *New log message search interface:* The new, more intuitive interface adds the following functionalities:

- You can search across all log messages using a single search field.
- You can set the beginning and ending date and time of the examined period manually.
- The list of results can now be scrolled, and navigated using the cursor, and the Page Down + Page Up keys.
- Clicking keywords in the list of log messages adds them to the search query.
- You can display all known details of an individual log item.
- When viewing statistics, the pie chart and the list view are now displayed together.

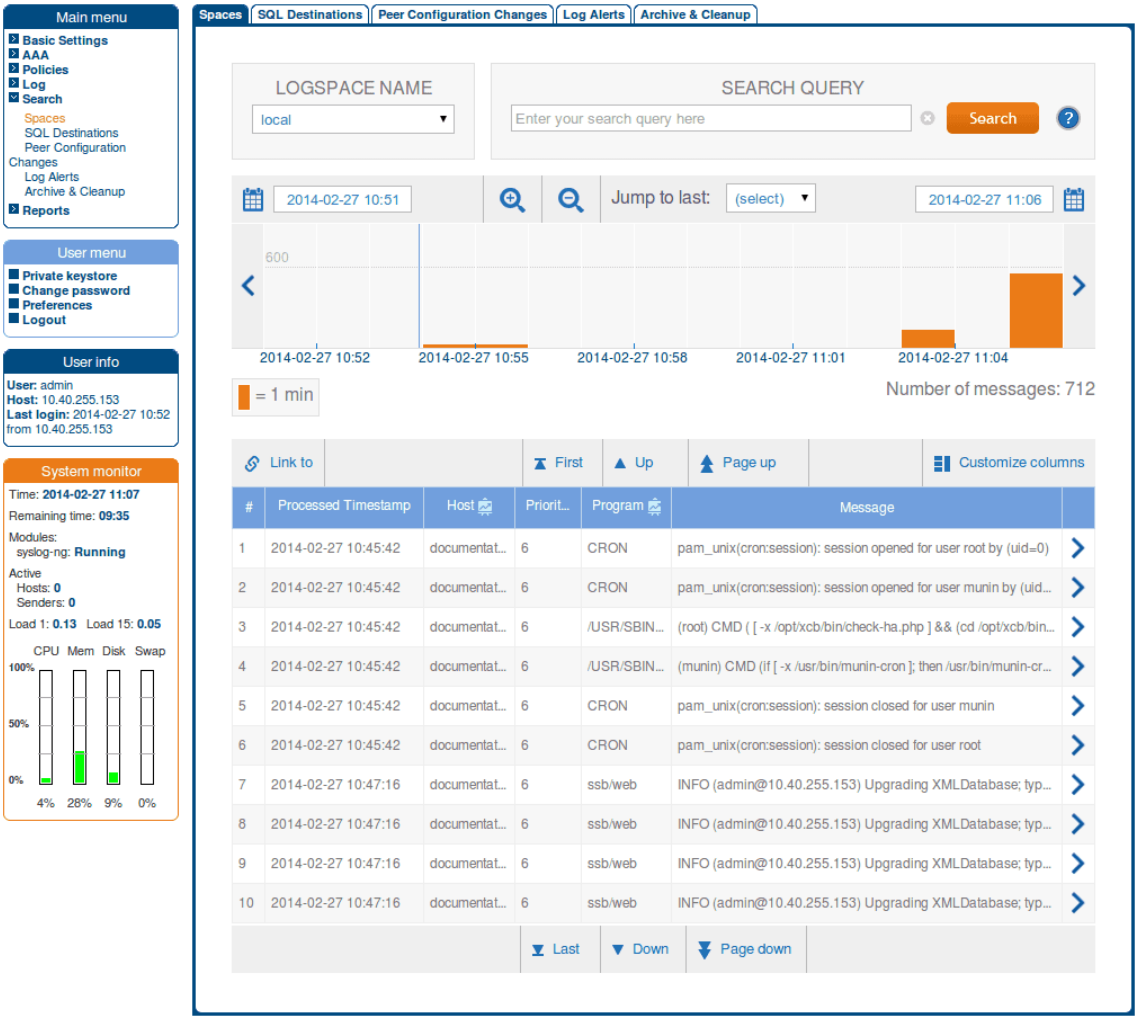



*Figure 1. The log message search interface*

For details, see *Chapter 12, Browsing log messages* in *The syslog-ng Store Box 4 LTS Administrator Guide*.

- *Nested groups can be disabled:* By default, SSB uses nested groups when querying LDAP servers. Nested groups are mostly useful when authenticating the users to Microsoft Active Directory, but can slow down the query and cause the connection to timeout if the LDAP tree is very large.

- The SSB Virtual Appliance is now officially supported on VMWare ESX 4.0 and later and ESXi 5.0 and later as well.
- For technical reasons, the internal timestamp handling of SSB has been changed. This change improves indexing and search performance.
- *New multi-page HTML documentation:*
  - Improved navigation: use the Contents tab on the new sidebar to move between sections, and the Search tab to find and highlight keywords in the document.
  - Shortcuts to download the PDF version of the document, or share the section you're reading.
  - Syntax-highlighting for code examples.
  - You can comment on every page to provide us feedback, ask questions about the documentation, or get in touch with us with your syslog-ng Store Box related questions.

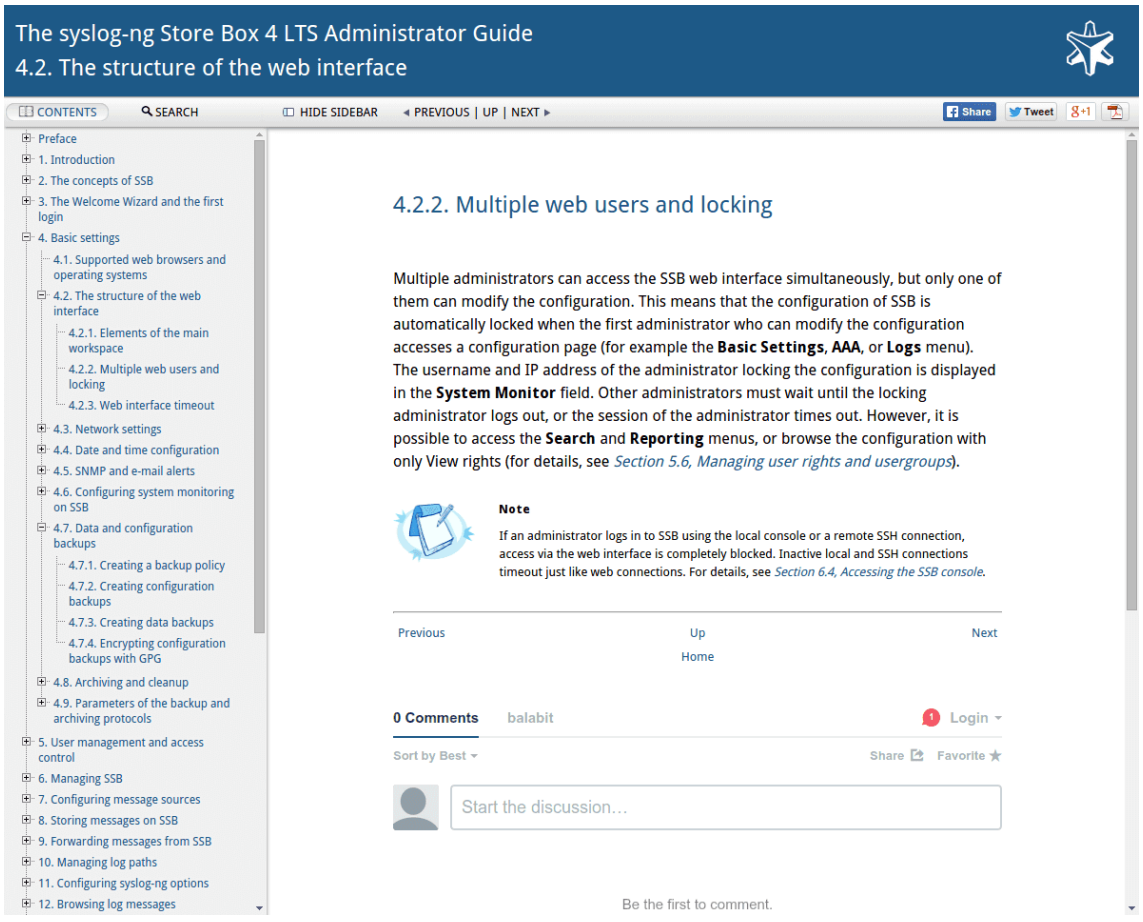



*Figure 2. The new documentation format*