

What is new in syslog-ng Store Box 4 F3

January 21, 2016



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Copyright © 1996-2016 Balabit SA

Table of Contents

1. Preface	3
2. Multiple logspaces	4
3. General improvements and changes	5

1. Preface

Welcome to syslog-ng Store Box (SSB) version 4 F3 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 F3.

This document covers the syslog-ng Store Box 4 F3 product.

**Note**

For step-by-step instructions on upgrading to 4 F3 see *How to upgrade to syslog-ng Store Box 4 F3* 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. Multiple logspaces

If you have several SSBs located at different sites, you can view and search the logs of these machines from the same web interface without having to log on to several different interfaces.

Creating multiple logspaces can also be useful if you want to pre-filter log messages based on different aspects and then share these filtered logs only with certain user groups.

The multiple logspace aggregates the messages that arrive from the member logspaces. The new log messages are listed below each other every second.

Once configured, multiple logspaces can be searched like any other logspace on SSB. You can also create filtered logspaces that are based on the multiple logspace.

For details on creating remote logspaces, see [*Procedure 8.6, Creating multiple logspaces*](#) in *The syslog-ng Store Box 4 F3 Administrator Guide*.



3. General improvements and changes

The indexer service of SSB now has increased performance and requires less memory than in earlier releases.