What is new in syslog-ng Store Box 5 LTS

June 27, 2018

Abstract

Welcome to syslog-ng Store Box (SSB) version 5 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 5 LTS.

This document covers the syslog-ng Store Box 5 LTS product.

Table of Contents

1. Upgrade to the new release

This is a Long Term Supported or LTS release, which means that it will be supported for 3 years after the original publication date and for 1 year after the succeeding LTS Release is published (whichever date is later). It also means that if you are running a previous feature release, you have 2 months to upgrade to the latest LTS version if you want to keep running on a supported release.

For a full description of LTS and feature releases, see the *Balabit version policy*.

Who should upgrade

We recommend you to upgrade to SSB 5 LTS, if you are not running SSB on Pyramid hardware and any of the following is true:

- You wish to take advantage of any of the new features.
- You are running a previous feature release.

Pyramid hardware is not supported
SSB 5 LTS is not supported on the following hardware: SSB N1000, SSB N1000d, SSB N5000, SSB N10000.

In case you have SSB deployed on other, newer hardware or you have SSB 4 LTS, those will not be affected in any way. The *Balabit version policy* applies to those.

If you wish to take advantage of new features and remain supported beyond the end date of the Extended Support phase, you need to upgrade your hardware. For assistance with your hardware upgrade, *contact our Sales Team*. For further inquiries, *contact the One Identity Support Team*.

If you do not know the type of your hardware or when it was purchased, complete the following steps:

1. Login to SSB.
2. Navigate to **Basic Settings > Troubleshooting > System debug**, click **Collect and save current system state info**, and save the file.
3. Open *https://support.balabit.com/* and click **Submit a Ticket**.
4. In the **Type of request** field, select **Request for information**.
5. Into the **Subject** field, enter `Determining hardware type`.
6. Click **Add File**, and upload the file you downloaded from SSB in Step 1.
7. We will check the type of your hardware and notify you.

How to upgrade

For step-by-step instructions on upgrading to 5 LTS, see *How to upgrade to syslog-ng Store Box 5 LTS* at the *syslog-ng Documentation page*.

All questions, comments or inquiries should be directed to `<info@balabit.com>` or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*

2. Changes since between SSB 4 LTS and 4 F9

2.1. Virtualization

Deploying SSB on Microsoft Azure

You can now deploy SSB on Microsoft Azure using a bring-your-own license model.

Running SSB in Microsoft Azure brings you the obvious benefits of running an application in the cloud. The most notable of these is the ability to adapt to the capacity needs of your application. Azure Linux Virtual Machines provides on-demand, high-scale, secure, virtualized infrastructure. Microsoft Azure offers a range of SKU types suitable for different use cases, allowing you to pick various details of your instance(s) (for example, memory, CPU, storage).

For step-by-step instructions, see *Deploying syslog-ng Store Box 5 LTS on Microsoft Azure*

Deploying SSB on Amazon Web Services

You can now deploy SSB on Amazon Web Services (AWS) using a bring-your-own license.

Running SSB in AWS brings you the obvious benefits of running an application in the cloud. The most notable of these is the ability to dynamically adapt to the changing capacity needs of your application. AWS offers a range of instance types suitable for different use cases, allowing you to pick various details of your instance(s) (for example, memory, CPU, storage). Launching instances happens within a matter of minutes, and you only pay for what you use.

For details, see *Deploying syslog-ng Store Box 5 LTS on Amazon Web Services*.

New virtual appliance

The SSB Virtual Appliance is now officially supported on Microsoft Hyper-V. For details, see *Chapter 7, syslog-ng Store Box Hyper-V Installation Guide* in *The syslog-ng Store Box 5 LTS Installation Guide*.

Increasing the virtual disk size of SSB under a virtual machine

Increasing the virtual disk size of SSB under a virtual machine is now much easier. You only have to power down the virtual machine, increase the disk size, and start the machine again.

For step-by-step instructions on the procedure, see *Chapter 8, Increasing the virtual disk size of SSB under a virtual machine* in *The syslog-ng Store Box 5 LTS Installation Guide*.

Change in the use of the management interface in virtual environments

When deploying SSB in a virtual environment, it is sufficient to use only a single network interface. When only one network interface is defined, however, that interface will be the one used for management purposes.

2.2. Logspaces and multiple nodes

Remote logspaces

SSB can access and search logspaces (including filtered logspaces) on other SSB appliances. To configure SSB to access a logspace on another (remote) SSB, set up a remote logspace. Once configured, remote logspaces

can be searched like any other logspace on SSB. You can also create filtered logspaces that are based on the remote logspace.

For details on creating remote logspaces, see *Procedure 8.5, Creating remote logspaces* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Filtered logspaces

Filtered logspaces allow you to create a smaller, filtered subset of the logs contained in an existing local or remote logspace. Assigning a user group to a filtered logspace enables fine grained access control by creating a group which sees only a subset of the logs from a logspace. You can use the same search expressions and logic as on the Search interface to create a filtered logspace.

For details on creating filtered logspaces, see *Procedure 8.4, Creating filtered logspaces* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

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 5 LTS Administrator Guide*.

2.3. Search and indexer improvements

Search interface improvements

- Option to show full log message in the list of search results added to **Search** > **Logspaces** > **Customize columns**.
- You can add now dynamic columns to the list of log messages directly from the detailed view of a log message.
- You can also view statistics directly from the detailed view of a log message.
- Logspace view properties are now saved for each logspace (on client side).
- Usability improvements.
- The **Link** and **CSV** buttons have been moved to a new area, an action bar under the overview section with the calendar bars.
- The new action bar features an **Alert** button, which allows the creation of content-based alerts. For more information on such alerts, see *Section Content-based alerting (p. 7)*.

- When any user action results in an error condition, the action bar displays an error or warning notification.
  For further details, see *Action bar:* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Indexer improvements

- The number of indexed logs in a logspace can now exceed 4294967296 (2^32) per day.
- Vastly improved the shortest timeframe for searching and creating statistics: you can now search with one second precision (earlier, it was one minute).
- The string '`NOT`' can now be used as the first keyword in search expressions.
- The indexer service of SSB now has increased performance and requires less memory than in earlier releases.

2.4. Message handling, parsing, alerting

Reliable Log Transfer Protocol™

The SSB application can receive log messages in a reliable way over the TCP transport layer using the Reliable Log Transfer Protocol™ (RLTP™). RLTP™ is a proprietary transport protocol that prevents message loss during connection breaks. The transport is used between syslog-ng Premium Edition hosts and SSB (for example, a client and SSB, or a client-relay-SSB), and interoperates with the flow-control and reliable disk-buffer mechanisms of syslog-ng Premium Edition, thus providing the best way to prevent message loss. The sender detects which messages has the receiver successfully received. If messages are lost during the transfer, the sender resends the missing messages, starting from the last successfully received message. Therefore, messages are not duplicated at the receiving end in case of a connection break (however, in failover mode this is not completely ensured). RLTP™ also allows to receive encrypted connections.

For details on configuring SSB to receive messages using RLTP™, see *Procedure 7.3, Creating syslog message sources in SSB* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Parsing `key-value` pairs

SSB can separate a message consisting of whitespace or comma-separated `key-value` pairs (for example, firewall logs, Postfix log messages) into name-value pairs. You can specify the separator character to parse different log messages, for example, colon (`:`) to parse MySQL log messages, or the equal sign (`=`) for firewall logs. For details, see *Procedure 10.7, Parsing key-value pairs* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Parsing sudo log messages

SSB separates `sudo` log messages into name-value pairs. The sudo parser enables you to enrich your log message data with details of privilege escalation events, such as who initiated the event, what command was issued, and so on. Metadata generated from the parsed values is searchable and can be used in statistics and custom reports.

For further information, see *Procedure 10.6, Parsing sudo log messages* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Content-based alerting

SSB can create content-based alerts about log messages based on specific search expressions. Search queries are run every few seconds and an alert is triggered whenever a match between the contents of a log message and a search expression is found. Alerts are collected and sent to a pre-defined email address (or email addresses).

Some log messages might have particular significance for users and therefore getting notifications about those can often be more efficient than searching for them manually.

For more detailed information about content-based alerting, see *Section 12.4, Creating content-based alerts* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

2.5. Acessing SSB

Certificate chain support for web user interface and RPC API

SSB now supports certificate chains, that is, web server certificates that contain intermediate certificates in addition to the end-user subscriber or server certificate. Previously, at the start of an SSL or TLS session, SSB only presented the server certificate to the client machine. From version 5 LTS onwards, you can choose to upload a certificate chain, and SSB will send the client machine both the server certificate and any additional intermediate certificates.

For details, see *Procedure 3.2, Configuring SSB with the Welcome Wizard* in *The syslog-ng Store Box 5 LTS Administrator Guide*, *Procedure 6.7.2, Uploading external certificates to SSB* in *The syslog-ng Store Box 5 LTS Administrator Guide*, and *Procedure 11.4, Setting the certificates used in TLS-encrypted log transport* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

HTTP Strict Transport Security (HSTS) support when switching to a self-signed certificate or when CA-signed certificate expires for SSB's web interface

If you have successfully accessed the SSB web interface using HTTPS at least once, your browser will remember this and force you to access SSB using HTTPS. This can cause issues when you switch to a self-signed certificate from a trusted CA-signed certificate, or when the SSL certificate of the web interface expires.

The resolution to this issue is to remove HSTS settings from the browser or to upload a new certificate using a different browser on a different machine.

For further information, see *Section 4.1, Supported web browsers* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

2.6. Hardware and operating system

10Gbit interface support

SSB now supports a 10Gbit network interface to receive log messages. You can use the 10Gbit interface instead of, or together with the regular 1Gbit external (LAN 1) interface. That way, you can use SSB without any additional changes even if your network devices support only 10Gbit, and you must connect SSB to a 10Gbit-only network.

For details, see *Section Using a 10Gbit interface as external interface* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Operating system upgrade

In this release, we have upgraded the operating system underlying the SSB appliance. The upgrade brings you a more recent and thus, more secure version of the operating system, with longer support lifetime.

Pyramid hardware is not supported

SSB 5 LTS is not supported on the following hardware: SSB N1000, SSB N1000d, SSB N5000, SSB N10000.

In case you have SSB deployed on other, newer hardware or you have SSB 4 LTS, those will not be affected in any way. The *Balabit version policy* applies to those.

If you wish to take advantage of new features and remain supported beyond the end date of the Extended Support phase, you need to upgrade your hardware. For assistance with your hardware upgrade, *contact our Sales Team*. For further inquiries, *contact the One Identity Support Team*.

2.7. Security-related changes

Changes in SNMP v3 trap settings

The MD5 authentication method and the DES encryption method are no longer available as SNMP trap settings, when configuring SSB to:

- Send alerts to a central monitoring server via SNMP v3.
- Forward log messages to an SNMP destination using the SNMP v3 protocol.

Support for these has been removed due to concerns over the level of security provided by such methods.

For details, see *Procedure 4.5.2, Configuring SNMP alerts* in *The syslog-ng Store Box 5 LTS Administrator Guide*, and *Procedure 9.4, Forwarding log messages to SNMP destinations* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Note that when upgrading your SSB to version 4 F8, your SNMP trap **MD5** (authentication method) settings will be automatically set to **SHA1**, while your SNMP trap **DES** (encryption method) settings will be automatically set to **AES**. For more information, see *Section SNMP v3 trap settings* in *How to upgrade to syslog-ng Store Box 5 LTS*.

Note that these automatic changes may require you to reset the relevant configuration options at your end, following an upgrade to SSB 4 F8 or later.

SHA-256 replaces MD5 when creating key fingerprints

When calculating the fingerprint of private keys, the SHA-256 algorithm replaces the previously used MD5 hash function. The web user interface of SSB now displays the used hash function next to the fingerprint of a key. Look at the following example:

2.8. Monitoring SSB

Changes in the prevention of disk space fill-up

The default value and the possible values you can set at **Basic Settings** > **Management** > **Disk space fill up prevention** > **Disconnect clients when disks are** have changed.

The default value has changed from `0` to `90`, meaning that disk space fill-up prevention is now turned on by default.

Another change concerns the value `100`. Starting from version 4 F8, you are only allowed to set values between `1-99`. This means that if you had `100` specified before the upgrade, then that will change to `99` following the upgrade.

For more information, see *Section Changes in the prevention of disk space fill-up* in *How to upgrade to syslog-ng Store Box 5 LTS*.

Changes in SNMP high disk utilization trap

The SNMP trap that is related to maximum disk utilization has changed. For details on how the changes might affect you, see *Section SNMP high disk utilization trap* in *How to upgrade to syslog-ng Store Box 5 LTS*.

2.9. General improvements and changes

- The **Log** > **Sources** > **Do not parse messages** option has been renamed to **Do not parse**.
- SSB now uses a bind user to query information from LDAP.
- In SSB version 4 F5 and later, you cannot manually change the speed of network interfaces.
- The **Anonymous login** option has been removed from SMB/CIFS Archive and Backup policies. To continue to use anonymous login, enter `anonymous` as username, and leave the **Password** field empty. (If you had the **Anonymous login** option enabled, this change is automatic.)

New guides

To improve how information is organized in the documentation set and make it easier for users to find information relevant to their roles, two new guides have been added, a user guide and an installation guide. The contents of both guides have previously been included in the syslog-ng Store Box Administrator Guide.

For further details on the user guide, see *The syslog-ng Store Box 5 LTS User Guide*.

For more information on the installation guide, see *The syslog-ng Store Box 5 LTS Installation Guide*.