How to upgrade to syslog-ng Store Box 5 LTS

June 27, 2018

Table of Contents

1. Preface

Welcome to syslog-ng Store Box (SSB) version 5 LTS and thank you for choosing our product. This document describes the process to upgrade existing SSB installations to SSB 5 LTS. The main aim of this paper is to aid system administrators in planning the migration to the new version of SSB.

Warning
Read the entire document thoroughly before starting the upgrade.

Upgrading to SSB 5 LTS is not supported if you have SSB deployed on any of the following Pyramid hardware: SSB N1000, SSB N1000d, SSB N5000, SSB N10000. For details, see *Section Pyramid hardware is not supported (p. 4)*.

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 features 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.

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. Prerequisites and Notes

Upgrade path to SSB 5 LTS

Upgrading to SSB 5 LTS is tested and supported using the following upgrade path:

- **The latest SSB 4 LTS maintenance version (for example, 4.0.7) -> SSB 5 LTS**
  Always upgrade to the latest available maintenance version of SSB 4 LTS before upgrading to SSB 5 LTS.

- **The latest maintenance version of the previous feature release (in this case, SSB 4 F9) -> SSB 5 LTS**

From older releases, upgrade to 4 LTS first. For details, see *How to upgrade to syslog-ng Store Box 4 LTS*.

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.

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.

Due to the removal of support for these authentication and encryption methods, certain configuration changes automatically take effect when you upgrade your SSB to version 5 LTS from 4.0. They are as follows:

- MD5 authentication method:

  - If you have **Basic Settings > Management > SNMP trap settings > SNMP v3 > Authentication method** set to **MD5**, that will automatically be set to **SHA1**.
  - If you have **Log > Destinations > SNMP destination > SNMP trap settings > SNMP v3 > Authentication method** set to **MD5**, that will automatically be set to **SHA1**.
- DES encryption method:
  - If you have **Basic Settings > Management > SNMP trap settings > SNMP v3 > Encryption method** set to **DES**, that will automatically be set to **AES**.
  - If you have **Log > Destinations > SNMP destination > SNMP trap settings > SNMP v3 > Encryption method** set to **DES**, that will automatically be set to **AES**.

Note that these automatic changes may require you to reset the relevant configuration options at your end, following an upgrade to version 5 LTS from 4.0.

Changes in the prevention of disk space fill-up

The following changes have been introduced in SSB 4 F8 regarding the prevention of disk space fill-up:

- The default value of **Basic Settings > Management > Disk space fill up prevention > Disconnect clients when disks are** has changed from *0* to *90*.
  If you had *0* specified, then following the upgrade, it will change to *90*. This means that disk fillup prevention will be turned on by default, with clients getting disconnected once disk utilization exceeds 90%.

- 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 on preventing disk space from filling up, see ????.

SNMP high disk utilization trap

The following changes have been introduced regarding the SNMP trap that is sent when disk utilization exceeds a pre-configured value:

- In the *dismanEventMIB* trap, the value of *dskDevice* has changed from *rootfs* to *none*. This only concerns the disk with index 1.
  In case you had some filters or alerts set on the value *rootfs*, then those will not work anymore.

- The *dismanEventMIB* trap sends out path information in a new field called *dskPath*.

Upgrade checklist

The following list applies to all configurations:

- You have backed up your configuration and your data.
  For more information on creating configuration and data backups, see *Section 4.7, Data and configuration backups* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

- For added safety, you have also exported the current configuration of SSB.

For detailed instructions, refer to *Procedure 6.3.6, Exporting the configuration of SSB* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

- You have a valid MyBalabit account.
  To download the required firmware files, you need a valid *MyDownloads* account. Note that the registration is not automatic, and might require up to two working days to process.

- You have downloaded the new 5 LTS license file from *MyDownloads*. As license files are specific to each long term release, upgrading to SSB 5 LTS removes any earlier license.

Warning
SSB now strictly checks if you have a High Availability license when running SSB in High Availability mode. You cannot upgrade to 5 LTS or later when using a single-node license in a HA environment. After upgrading to 5 LTS or later, an SSB node can be converted to HA only if a valid HA license is installed. HA licenses include the following line:

```
Licensed-Options: Highavailability
```

To buy a valid HA license, contact your sales representative or *contact our Sales Team*.

- You have downloaded the latest SSB core firmware and boot firmware from the *syslog-ng Downloads page*.
  For a detailed description of the different firmwares, see *Section 2.8, Firmware in SSB* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

- You have read the Release Notes (changelog) of the firmware(s) before updating. The Release Notes might include additional instructions specific to the firmware version.
  The Release Notes are available on the *syslog-ng Downloads page*.

If you have a high availability cluster:

- You have IPMI access to the slave node. You can find detailed information on using the IPMI interface in the following documents:
  - For SSB T1, see the *SMT IPMI User's Guide*.
  - For SSB T4 and T10, see the *X9 SMT IPMI User's Guide*.
- You have verified on the **Basic Settings > High Availability** page that the HA status is not degraded.
- *If you have a high availability cluster with geoclustering enabled:*
  Perform the firmware upload steps an hour before the actual upgrade. Geoclustering can introduce delays in master-slave synchronization, and the slave node might not be able to sync the new firmware from the master node on time.

If you are upgrading SSB in a virtual environment:

- You have created a snapshot of the virtual machine before starting the upgrade process.
- You have configured and enabled console redirection (if the virtual environment allows it).

During the upgrade, SSB displays information about the progress of the upgrade and any possible problems to the console, which you can monitor with IPMI (ILOM) or console access.

We recommend that you test the upgrade process in a non-productive (virtual, etc.) environment first.

Upgrading SSB requires a reboot. We strongly suggest that you perform the upgrade on the productive appliance during maintenance hours only, to avoid any potential data loss.

3. Upgrading to SSB 5 LTS

3.1. Procedure – Upgrading SSB (single node)

Purpose:

If you want to upgrade a SSB cluster, see *Procedure 3.2, Upgrading an SSB cluster (p. 8)*. To upgrade a standalone SSB node to version 5 LTS, complete the following steps.

Prerequisites:

Read the following warnings before starting the upgrade process.

Steps:

Step 1. Update the core firmware of SSB using the web interface.

Step a. Navigate to **Basic Settings** > **System** > **Core firmwares**.

Step b. Upload the new core firmware.

Step c. When the upload is finished, select the **After reboot** option for the new firmware.
Do not reboot SSB yet.

Step 2. Upload the boot firmware of SSB using the web interface.

Step a. Navigate to **Basic Settings** > **System** > **Boot firmwares**.

Step b. Upload the new boot firmware.

Step c. When the upload is finished, select the **After reboot** option for the new firmware.

Step 3. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.
Navigate to **Basic Settings** > **Troubleshooting** > **System debug** and choose **Collect and save current system state info**.

Step 4. Navigate to **Basic Settings** > **System** > **System Control** > **This node**, and choose **Reboot**.
SSB attempts to boot with the new firmware. Wait for the process to complete.

Step 5. Log in to the SSB web interface to verify that the upgrade was successful.
Navigate to **Basic Settings** > **System** > **Version details** and check the version numbers of SSB. In case you encounter problems, you can find common troubleshooting steps in *Section 4, Troubleshooting (p. 11)*.

Step 6. Upload the new license file. For details, see *Procedure 3.3, Updating the SSB license (p. 10)*.

3.2. Procedure – Upgrading an SSB cluster

Prerequisites:

Make sure that you have physically connected the IPMI interface to the network and that it is properly configured. This is important because you can only power the slave node on through the IPMI interface. For details on configuring the IPMI interface, see *Section 6.6, Out-of-band management of SSB* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

> **Warning**
> SSB now strictly checks if you have a High Availability license when running SSB in High Availability mode. You cannot upgrade to 5 LTS or later when using a single-node license in a HA environment. After upgrading to 5 LTS or later, an SSB node can be converted to HA only if a valid HA license is installed. HA licenses include the following line:
>
> ```
> Licensed-Options: Highavailability
> ```
>
> To buy a valid HA license, contact your sales representative or *contact our Sales Team*.

Steps:

Step 1. Update the core firmware of SSB using the web interface.

Step a. Navigate to **Basic Settings** > **System** > **Core firmwares**.

Step b. Upload the new core firmware.

Step c. When the upload is finished, select the **After reboot** option for the new firmware. *Do not reboot SSB yet.*

Step 2. Upload the boot firmware of SSB using the web interface.

Step a. Navigate to **Basic Settings** > **System** > **Boot firmwares**.

Step b. Upload the new boot firmware.

Step c. When the upload is finished, select the **After reboot** option for the new firmware. *Do not reboot SSB yet.*

Step 3. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.
Navigate to **Basic Settings** > **Troubleshooting** > **System debug** and choose **Collect and save current system state info**.

Step 4. Navigate to **Basic Settings** > **High availability**, and verify that the new firmware is displayed for the slave node. This might take a few minutes.
Note that at this stage, the slave node is not using the new firmware yet.

Step 5. Navigate to **Basic Settings** > **System** > **High availability** > **Other node** and click **Shutdown**.

Step 6. Restart the master node: choose **This node** > **Reboot**.
SSB attempts to boot with the new firmware. Wait for the process to complete.

Step 7. Log in to the SSB web interface to verify that the master node upgrade was successful.
Navigate to **Basic Settings** > **System** > **Version details** and check the version numbers of SSB. In case you encounter problems, you can find common troubleshooting steps in *Section 4, Troubleshooting (p. 11)*.

Step 8. Upload the new license file. For details, see *Procedure 3.3, Updating the SSB license (p. 10)*.

Step 9. Use the IPMI interface to reboot the slave node.

The slave node attempts to boot with the new firmware, and reconnects to the master node to sync data. During the sync process, certain services (including Heartbeat) are not available. Wait for the process to finish, and the slave node to boot fully.

Step 10. Navigate to **Basic Settings > System > High availability & Nodes** and verify that the slave node is connected, and has the same firmware versions as the master node.

> **Note**
> When upgrading an SSB cluster, the upgrade process on the slave node will only be completed once a takeover has been performed.

3.3. Procedure – Updating the SSB license

Steps:

Step 1. Download the new 5 LTS license file from *MyDownloads*.

Step 2. Navigate to **Basic Settings > System > License**.

Step 3. Click **Browse** and select the new license file.

You can upload compressed licenses (for example, `.zip` archives).

Step 4. Click **Upload**, then **Commit**.

4. Troubleshooting

If you experience any strange behavior of the web interface, first try to reload the page by holding the SHIFT key while clicking the Reload button of your browser to remove any cached version of the page.

In the unlikely case that SSB encounters a problem during the upgrade process and cannot revert to its original state, SSB performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH access to SSB, unless SSB is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the Support Team to diagnose and solve the problem. Note that SSH access will be enabled on every active interface, even if management access has not been enabled for the interface.

In case the web interface is not available within 30 minutes of rebooting SSB, check the information displayed on the local console and *contact the One Identity Support Team*.