syslog-ng Store Box 6.0

Upgrade Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SSB Upgrade Guide
Updated - March 2020
Version - 6.0

Contents

1

Preface

Welcome to syslog-ng Store Box (SSB) version 6.0 and thank you for choosing our product. This document describes the process to upgrade existing SSB installations to SSB 6.0. The main aim of this paper is to aid system administrators in planning the migration to the new version of SSB.

CAUTION:

Read the entire document thoroughly before starting the upgrade.

Upgrading to SSB 6.0 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 Prerequisites and Notes on page 5.

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

- *Long Term Supported or LTS releases* (for example, SSB 5.0) 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 5.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SSB 5.1) 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).

CAUTION:

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

Prerequisites and Notes

Upgrade path to SSB 6.0.1

Upgrading to SSB 6.0.1 is tested and supported using the following upgrade path:

- *The latest SSB 5 LTS maintenance version (for example, 5.0.3) -> SSB 6.0.1*

  Always upgrade to the latest available maintenance version of SSB 5 LTS before upgrading to SSB 6.0.1.
- *The latest maintenance version of the previous feature release (in this case, SSB 5.3) -> SSB 6.0.1*

From older releases, upgrade to 5 LTS first. For details, see How to upgrade to syslog-ng Store Box 5 LTS.

Unsupported since SSB version 5.3

- Unsupported protocol: The sslv3 protocol is unsupported. Make sure that your clients support a newer protocol (at least tlsv1.0), otherwise SSB will not be able to receive log messages from them.
- Unsupported ciphers: The rc4 and 3des cipher suites are unsupported. Make sure that your clients support a cipher suite that contains more secure ciphers, otherwise SSB will not be able to receive log messages from them.
- Unsupported digest method: The sha-0 (sha) digest method cannot be used in logstores anymore. If you have a logstore that uses this digest method, you must configure the logstore to use a different method before upgrading to SSB 5.3. Note that SSB rotates the logstore files every midnight. After changing the digest method, you must wait for the next logrotation before upgrading to SSB 5.3. For details on changing the digest method, see "General syslog-ng settings" in the Administration Guide.

  CAUTION:

  After upgrading to SSB 5.3, you will not be able to access and search the logstore files that use the sha-0 digest method.
- The **Special > Firmware** user privilege has been removed. To upload a new firmware, the user now needs to have the **Basic Settings > System** privilege. Note

that users who had only the **Special > Firmware** privilege will not be able to login to SSB after upgrading to version 5.3. For details on managing user privileges, see "User management and access control" in the Administration Guide.

- Configuration changes of syslog-ng Premium Edition peers can be displayed only for peers running syslog-ng Premium Edition 3.0-6.0.x. Peers running syslog-ng Premium Edition version 7.0.x do not send such notifications. As a result, if you are forwarding the logs of an SSB node to another SSB node, such log messages will not be available. You can check the configuration changes of SSB on the **AAA > Accounting** page.

Unsupported since SSB version 5.2

CAUTION:

SNMP destinations and SQL sources have been removed in the SSB 5.2.0 release

Do not upgrade to SSB 5.2.0 if you are currently using and want to continue to use:

- **SNMP destinations**
- **SQL sources**

These functionalities have been removed from SSB starting with version 5.2.0. Upgrading from 5 LTS and its minor versions would mean that you would have to upgrade to 5.2.0 - to continue to receive support for the product.

Staying on 5 LTS and its minor versions means that you will not have access to the HDFS destination functionality available in SSB starting with version 5.1.0, however, you will continue to get support for 3 years after the original publication date of 5 LTS (December 2017) and for 1 year after the next LTS release is published (whichever date is later).

If you wish to carry on using SNMP destinations or SQL sources, contact zoltan.szasz@oneidentity.com.

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 version policy applies to those. For details, open the SSB product page on the Support Portal and navigate to **Product Life Cycle & Policies > Product Support Policies > Software Product Support Lifecycle Policy**.

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 our Support Team.

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

1. Log in to SSB.
2. Navigate to **Basic Settings > Troubleshooting > System debug**, click **COLLECT AND SAVE CURRENT SYSTEM STATE INFO**, and save the file.
3. Log in to the support portal and submit a ticket.
4. In the **Summary** field, enter `Determining hardware type`.
5. Upload the file you downloaded from SSB in Step 2.
6. We will check the type of your hardware and notify you.

Upgrade checklist

The following list applies to all configurations:

- The firmware of your SSB appliance is not tainted (that is, none of its files were modified locally). If the firmware is tainted, a warning is displayed on the **Basic Settings > System > Version details** page.

  Upgrading is not supported if the firmware is tainted. If your firmware is tainted, contact our Support Team.
- You have backed up your configuration and your data.

  For more information on creating configuration and data backups, see "Data and configuration backups" in the Administration Guide.
- For added safety, you have also exported the current configuration of SSB.

  For detailed instructions, refer to "Exporting the configuration of SSB" in the Administration Guide.
- You have a valid support portal account.

  To download the required firmware files and the license, you need a valid support portal account. To create an account, navigate to the support portal and follow the instructions on screen (you will need to enter your product's asset number, which is the license number or serial number you have been provided previously).
- You have downloaded the new 6.0 license file from support portal. As license files are specific to each long term release, upgrading to SSB 6.0 removes any earlier license.
- You have downloaded the latest SSB firmware file from the Downloads page.

  For a details about the firmware file, see "Firmware in SSB" in the Administration 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 Store Box Documentation 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 syslog-ng Store Box Appliance 3000 and 3500, see the 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 the synchronization between the primary and the secondary node, and the secondary node might not be able to sync the new firmware from the primary 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-production (virtual) environment first.

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

Upgrading to SSB 6.0.1

For details on upgrading your syslog-ng Store Box (SSB) installation to 6.0.1, see the following procedures.

Upgrading SSB

If you want to upgrade a SSB cluster, see Upgrading an SSB cluster on page 10.

Prerequisites:

Read the following warnings before starting the upgrade process.

To upgrade a standalone SSB node to version 6.0

1. Stop SSB from accepting the incoming log traffic. Navigate to **Basic Settings > System > Service control** and click **Disable**.
2. **If you are upgrading from SSB 5.3**: Update the firmware of SSB using the web interface.
    a. Navigate to **Basic Settings > System > Upgrade**.
    b. Upload the new ISO file.
    c. When the upload is finished, click **Upgrade and reboot node**.
3. **If you are upgrading from SSB 5.0**: Upload the boot firmware of SSB using the web interface.
    a. Navigate to **Basic Settings > System > Boot firmwares**.
    b. Upload the new boot firmware.
    c. When the upload is finished, select the **After reboot** option for the new firmware.
4. **If you are upgrading from SSB 5.0**: Update the core firmware of SSB using the web interface.

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

b. Upload the new core firmware.

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

Do not reboot SSB yet.

5. 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.

6. *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**.

7. 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 Troubleshooting on page 13.

8. Upload the new license file. For details, see Updating the SSB license on page 12.

9. Enable SSB to receive the incoming log traffic. Navigate to **Basic Settings > System > Service control** and click **Enable**.

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 secondary node on through the IPMI interface. For details on configuring the IPMI interface, see "Out-of-band management of SSB" in the Administration Guide.

To upgrade an SSB cluster

1. Stop SSB from accepting the incoming log traffic. Navigate to **Basic Settings > System > Service control** and click **Disable**.
2. **If you are upgrading from SSB 5.3**: Update the firmware of SSB using the web interface.

   a. Navigate to **Basic Settings > System > Upgrade**.

   b. Upload the new ISO file.

   c. When the upload is finished, click **Upgrade, reboot master, and shut down slave**.

3. **If you are upgrading from SSB 5.0**: Upload the boot firmware of SSB using the

web interface.

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

b. Upload the new boot firmware.

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

Do not reboot SSB yet.

4. **If you are upgrading from SSB 5.0**: Update the core firmware of SSB using the web interface.

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

b. Upload the new core firmware.

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

Do not reboot SSB yet.

d. *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**.

e. Navigate to **Basic Settings > High availability**, and verify that the new firmware is displayed for the secondary node. This might take a few minutes.

Note that at this stage, the secondary node is not using the new firmware yet.

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

g. Restart the primary node: choose **This node > Reboot**.

SSB attempts to boot with the new firmware. Wait for the process to complete.

5. Log in to the SSB web interface to verify that the primary 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 Troubleshooting on page 13.

6. Upload the new license file. For details, see Updating the SSB license on page 12.

7. Use the IPMI interface to start the secondary node.

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

8. Navigate to **Basic Settings > System > High availability & Nodes** and verify that the secondary node is connected, and has the same firmware versions as the primary node.

NOTE:

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

9. Enable SSB to receive the incoming log traffic. Navigate to **Basic Settings > System > Service control** and click **Enable**.

Updating the SSB license

To update the SSB license

1. Download the new 6.0 license file from support portal.

   You need a new license file for every long-term-supported release. If there is no license file for syslog-ng Store Box 6.0 under your account, contact our Licensing Team and **Request a license key for a new version**.
2. Navigate to **Basic Settings > System > License**.
3. Click **Browse** and select the new license file.

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

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product