ONE IDENTITY™

syslog-ng Store Box 6.4

Upgrade Guide

SSB Upgrade Guide
Updated - May 2020
Version - 6.4

Contents

Preface

Welcome to syslog-ng Store Box (SSB) version 6.4 and thank you for choosing our product. This document describes the process to upgrade existing SSB installations to SSB 6.4. 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.

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 6.4

Upgrading to SSB 6.4 is tested and supported using the following upgrade path:

- *The latest SSB 6 LTS maintenance version (for example, 6.0) -> SSB 6.4*

  Always upgrade to the latest available maintenance version of SSB 6 LTS before upgrading to SSB 6.4.

- *The latest maintenance versions of the previous three feature releases (in this case, SSB 6.1 or 6.2) -> SSB 6.4*

From older releases, upgrade to 6 LTS first. For details, see How to upgrade to syslog-ng Store Box 5 LTS.

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 file, 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 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 (SSB) Appliance 3000 and 3500, see the Latest IPMI firmware for Syslog-ng Store Box 3000/3500 and One Identity Safeguard for Privileged Sessions 3000/3500 appliances.

  For syslog-ng Store Box (SSB) T1 and syslog-ng Store Box (SSB) T4, 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:

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

- 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 6.4

For details on upgrading your syslog-ng Store Box (SSB) installation to 6.4, see the following procedures.

Upgrading SSB

If you want to upgrade a SSB cluster, see Upgrading an SSB cluster on page 8.

Prerequisites

Read the following warnings before starting the upgrade process.

To upgrade a standalone SSB node to version 6.4

1. Stop SSB from accepting the incoming log traffic. Navigate to **Basic Settings > System > Service control** and click **Disable**.

2. 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. 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.

4. *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**.

5. 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 9.

6. 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. 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. 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 9.

4. 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.

5. 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.

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

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