ONE IDENTITY

by Quest

syslog-ng Store Box 6.0.3

Packaging Checklist

SSB Packaging Checklist
Updated - 23 August 2021, 09:53
Version - 6.0.3

Contents

Package contents inventory

Carefully unpack all server components from the packing cartons. The following items should be packaged with the syslog-ng Store Box:

- A syslog-ng Store Box appliance, pre-installed with the latest syslog-ng Store Box firmware.

- syslog-ng Store Box accessory kit, including the following:

  - syslog-ng Store Box 6.0 Packaging Checklist (this document).
  - GPL v2.0 license.

- Rack mount hardware.

- Power cable.

The default BIOS and IPMI passwords are in the documentation.

syslog-ng Store Box Hardware Installation Guide

This section describes how to set up the syslog-ng Store Box (SSB) hardware. Refer to the following documents for step-by-step instructions:

- *syslog-ng Store Box Appliance 3000*: see the *SC113 Chassis Series User's Manual, Chapter 6: Rack Installation*, available online at https://www.supermicro.com/manuals/chassis/1U/SC113.pdf.

- *syslog-ng Store Box Appliance 3500*: see the *SuperServer 1029U-T Series User's Manual, Chapter 2: Server Installation*, available online at https://www.supermicro.com/manuals/superserver/1U/MNL-1973.pdf.

The manuals are also available online at the syslog-ng Store Box Documentation page. Note that SSB hardware is built to custom specifications: CPU, memory, network card, and storage options differ from the stock chassis. You can find the hardware specifications in Hardware specifications

- For details on how to install a single SSB unit, see Installing the SSB hardware.

- For details on how to install two SSB units in high availability mode, see Installing two SSB units in HA mode.

Installing the SSB hardware

This section describes how to install a single syslog-ng Store Box (SSB) unit.

For further information about installing the syslog-ng Store Box Appliance hardware units, see section syslog-ng Store Box Hardware Installation Guide.

To install a single SSB unit

1. Unpack SSB.

2. *Optional step*: Install SSB into a rack with the slide rails. Slide rails are available for all SSB appliances.

3. Connect the cables.

   a. **For general networks**

   Connect the Ethernet cable facing your LAN to the Ethernet connector labeled 1. This is the external interface of SSB. This interface is used for the initial configuration of SSB, and for communication between SSB and the clients. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

   For 10Gbit-only networks

   Connect the cable facing your LAN to the SFP+ connector labeled 5. This is the external interface of SSB. This interface is used for the initial configuration of SSB, and for communication between SSB and the clients. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

   > ⓘ NOTE:
   >
   > Only Intel-based SFP+ transceivers are compatible with the Intel 82599EB host chipset found in SSB.
   >
   > The following Intel-based optical and Direct Attached Copper (DAC) SFP+ transceivers have been tested successfully with SSB, but in the future, their compatibility with SSB is not guaranteed:
   >
   > - AOC-E10GSFPSR (optical)
   > - SFP-10GE-SR (DAC)
   > - FTLX8571D3BCVIT1 (DAC)
   >
   > For a list of Intel-based connectors that may be compatible with the Intel 82599EB host chipset found in SSB, see 82599-BASED ADAPTERS/Linux* Base Driver for the Intel(R) Ethernet 10 Gigabit PCI Express Adapters.

   > ⚠ CAUTION:
   >
   > **Do not leave any unused SFP/SFP+ transceiver in the 10Gbit interface. It may cause network outage.**

b. Connect an Ethernet cable that you can use to remotely support the SSB hardware to the `IPMI` interface of SSB. For details, see the following documents:

For syslog-ng Store Box Appliance 3000 and 3500, see the IPMI User's Guide.

> ⚠ **CAUTION:**
>
> **Connect the IPMI before plugging in the power cord. Failing to do so will result in IPMI failure.**

> ⚠ **CAUTION: SECURITY HAZARD!**
>
> **The IPMI interface, like all out-of-band management interfaces, has known vulnerabilities that One Identity cannot fix or have an effect on. To avoid security hazards, One Identity recommends that you only connect the IPMI interface to well-protected, separated management networks with restricted accessibility. Failing to do so may result in an unauthorized access to all data stored on the SSB appliance. Data on the appliance can be unencrypted or encrypted, and can include sensitive information, for example, passwords, decryption keys, private keys, and so on.**
>
> **For more information, see Best Practices for managing servers with IPMI features enabled in Datacenters.**

> ⓘ NOTE:
>
> The administrator of SSB must be authorized and able to access the IPMI interface for support and troubleshooting purposes in case vendor support is needed.

The following ports are used by the IPMI interface:

- Port 623 (UDP): IPMI (cannot be changed)
- Port 5123 (UDP): floppy (cannot be changed)
- Port 5901 (TCP): video display (configurable)
- Port 5900 (TCP): HID (configurable)
- Port 5120 (TCP): CD (configurable)
- Port 80 (TCP): HTTP (configurable)

c. *Optional step*: Connect the Ethernet cable to be used for managing SSB after its initial configuration to the Ethernet connector labeled 2. This is the management interface of SSB. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

d. *Optional step*: Connect the Ethernet cable connecting SSB to another SSB node to the Ethernet connector labeled 4. This is the high availability (HA) interface of SSB. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

4. Power on the hardware.

5. Change the BIOS password on the syslog-ng Store Box. The default password is `ADMIN` or `changeme`, depending on your hardware.

6. Change the IPMI password on the syslog-ng Store Box. The default password is `ADMIN` or `changeme`, depending on your hardware.

   > **ⓘ NOTE:**
   >
   > Ensure that you have the latest version of IPMI firmware installed. You can download the relevant firmware from the One Identity Knowledge Base:
   >
   > - IPMI firmware for syslog-ng Store Box Appliance 3000
   > - IPMI firmware for syslog-ng Store Box Appliance 3500
   > - IPMI firmware for syslog-ng Store Box T1
   > - IPMI firmware for IPMI firmware for syslog-ng Store Box T4
   > - IPMI firmware for IPMI firmware for syslog-ng Store Box T10

   To change the IPMI password, connect to the IPMI remote console.

   > **ⓘ NOTE:**
   >
   > If you encounter issues when connecting to the IPMI remote console, add the DNS name or the IP address of the IPMI interface to the exception list (whitelist) of the Java console. For details on how to do this, see the Java FAQ entry titled How can I configure the Exception Site List?.

7. Following boot, SSB attempts to receive an IP address automatically via DHCP. If it fails to obtain an automatic IP address, it starts listening for HTTPS connections on the `192.168.1.1` IP address.

   To configure SSB to listen for connections on a custom IP address, complete the following steps:

   a. Access SSB from the local console, and log in with username `root` and password `default`.

   b. In the Console Menu, select **Shells > Core shell**.

   c. Change the IP address of SSB:

   ```
   ip addr add <IP-address>/24 dev eth0
   ```

   Replace `<IP-address>` with an IPv4 address suitable for your environment.

   d. Set the default gateway using the following command:

   ```
   ip route add default via <IP-of-default-gateway>
   ```

   Replace `<IP-of-default-gateway>` with the IP address of the default gateway.

   e. Type `exit`, then select **Logout** from the Console Menu.

8. Connect to the SSB web interface from a client machine and complete the Welcome Wizard as described in "The Welcome Wizard and the first login" in the Administration Guide.

   🛈 | NOTE:

   The syslog-ng Store Box Administrator Guide is available on the syslog-ng Store Box Documentation page.

Installing two SSB units in HA mode

This section describes how to install SSB with high availability support.

To install SSB with high availability support

1. For the first SSB unit, complete Installing the SSB hardware on page 6.

2. For the second SSB unit, complete Steps 1-3 of Installing the SSB hardware on page 6.

3. Connect the two units with an Ethernet cable via the Ethernet connectors labeled as 4.

4. Power on the second unit.

5. Change the BIOS and IPMI passwords on the second unit. The default password is ADMIN or changeme, depending on your hardware.

6. Connect to the SSB web interface of the first unit from a client machine and enable high availability mode. Navigate to **Basic Settings > High Availability** . Click **Convert to Cluster**, then reload the page in your browser.

7. Click **Reboot Cluster**.

8. Wait until the slave unit synchronizes its disk to the master unit. Depending on the size of the hard disks, this may take several hours. You can increase the speed of the synchronization via the SSB web interface at **Basic Settings > High Availability > DRBD sync rate limit**.

Hardware specifications

The syslog-ng Store Box (SSB) appliances are built on high performance, energy efficient, and reliable hardware that are easily mounted into standard rack mounts.

For detailed hardware specifications of your appliance, see "Hardware specifications" in the Installation Guide.

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