syslog-ng Store Box 7.4.0

Security checklist for syslog-ng Store Box appliances

Copyright 2024 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

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 Security checklist for syslog-ng Store Box appliances
Updated - 16 April 2024, 16:38

For the most recent documents and product information, see Online product documentation.

Contents

Security checklist for configuring SSB **4**

About us **7**

Contacting us 7

Technical support resources 7

Security checklist for configuring SSB

The following checklist is a set of recommendations and configuration best practices to ensure that your syslog-ng Store Box (SSB) is configured securely.

General security recommendations

- As a general recommendation, use 2048-bit RSA keys (or stronger), `AES-256-CBC` cipher (or stronger), and `SHA-256` hash algorithm (or stronger). For more specific information, see the relevant sections of the *syslog-ng Store Box Administration Guide*.
- Use mutual authentication whenever possible, as detailed below, when configuring log sources, log destinations or LDAP user database.
- One Identity recommends that you generate certificates using your own public key infrastructure (PKI) solution and then upload them to SSB. Certificates generated by SSB cannot be revoked, therefore, they can become a security risk if compromised.
- When exporting the configuration of SSB, or creating configuration backups, always use encryption. Handle the exported data with care, as it contains sensitive information, including credentials. For more information on encrypting the configuration, see *Encrypting configuration backups with GPG* in the *Administration Guide*.
- Use every keypair or certificate only for one purpose. Do not reuse cryptographic keys or certificates, for example, do not use the same certificate for the SSB webserver and for encrypting logstores.
- For backward compatibility reasons, SSB does not enforce strict security configuration for backup, archive, and share - using SMB/CIFS and NFS - therefore, any security expectations need to be ensured by the joining peers and the underlying network architecture. For more information on backups and archiving, see *Data and configuration backups* in the *Administration Guide* and *Archiving and cleanup* in the *Administration Guide*.

Log traffic and storage specific security recommendations

- When creating logspaces on **Log** > **Logspaces**, use **LogStore** type rather than plain text files and apply encryption.
- When encrypting log files, One Identity recommends:
  - Using 2048-bit RSA keys (or stronger). For more information, see *Creating logstores* in the *Administration Guide*.
  - Using `AES-256-CBC` cipher (or stronger) and `SHA-256` hash algorithm (or stronger). For more information, see *General syslog-ng settings* in the *Administration Guide*.
- One Identity recommends using User Temporary private key store for decrypting and viewing encrypted logs on the **Search** > **Logspaces** interface. Avoid using User Permanent private key store or shared decryption private key uploaded on the **Log** > **Logspaces** interface. For more information, see *Browsing encrypted logspaces* in the *Administration Guide*.
- For the Server certificate and the Time Stamping Authority (TSA) certificate, upload the private key as well. One Identity recommends using 2048-bit RSA keys (or stronger). These two certificates must be issued by the same Certificate Authority. For more information on uploading certificates and keys created with an external PKI, see *Uploading external certificates to SSB* in the *Administration Guide*.
- When granting user privileges, make sure that only the intended users can access logspaces.

  By default, members of the `search` group can view the stored messages online. Use the **Access control** option to control which usergroups can access a logspace. For more information, see *Managing user rights and usergroups* in the *Administration Guide*.
- Configure each logsource in SSB at **Log** > **Sources** as follows:
  1. For **Transport**, select **TLS**.
  2. For **Incoming log protocol and message format**, select **Syslog (IETF-syslog, RFC 5452)**.
  3. For **Peer verification**, select **Required-trusted**.
  4. For **Cipher suite**, select **Secure**.

     By applying the **Secure** cipher suite, SSB will not allow permissive cipher suites to be used for remote connections.
- If log messages must be forwarded outside the box, configure log destinations at **Log** > **Destinations** in a similar way as the logsources described above (Steps 1-4). For more information, see *Forwarding log messages to remote servers* in the *syslog-ng Store Box Administration Guide*.

  NOTE: You cannot set cipher suites, as the TLS server is the remote side (Step 5).
- Consider that connections for log source or destination types UDP, TCP, SQL, and SNMP are not encrypted. Even though ALTP is encrypted, it can still be compromised.

- Enable flow-control to prevent message loss. For more information, see *Managing incoming and outgoing messages with flow-control* in the *Administration Guide*.

Accessing SSB

- Disallow permissive cipher suites for HTTPS connections towards the SSB webserver. When configuring the cipher suite capability for HTTPS connections, use the **Secure** cipher suite set under **Basic Settings** > **Management** > **Web interface and RPC API settings** > **Cipher suite**. For more information, see *Web interface and RPC API settings* in the *Administration Guide*.
- Use strong passwords, with at least 12 characters (including lower case letters, upper case letters, numbers, and special characters). For local SSB users, set the password policy strength to `strong` on **AAA** > **Settings** > **Minimal password strength**. For more information, see *Setting password policies for local users* in the *Administration Guide*.
- Accessing the SSB host directly using SSH is not recommended or supported, except for troubleshooting purposes. In such case, the One Identity Support Team will give you exact instructions on what to do to solve the problem.

  For security reasons, disable SSH access to SSB when it is not needed. For more information, see *Enabling SSH access to the SSB host* in the *Administration Guide*.
- Permit administrative access to SSB only from trusted networks. If possible, log messages from clients and administrative access to the SSB web interface should be originated from separate networks.
- Configure SSB to send an alert if a user fails to login to SSB. For more information, see the **Login failed** alert in *System related traps* in the *Administration Guide*.
- Configure **Disk space fill up prevention**, and configure SSB to send an alert if the free space on the disks of SSB is low. For more information, see *Preventing disk space fill up* in the *Administration Guide*.
- Prefer configuring SSB to use the local user database. If LDAP is needed, make sure to configure mutual authentication. For more information on local user management, see *Managing SSB users locally* in the *Administration Guide*.

Networking considerations

- SSB stores sensitive data. Use a firewall and other appropriate controls to ensure that unauthorized connections cannot access it.
- If possible, enable management access to SSB only from trusted networks.
- Make sure that the HA interface of SSB is connected to a trusted network.
- Make sure that for the communication between the peer nodes, for example, log sending, log receiving, or webserver interface communication, you have the properly secure configuration as described above.

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