syslog-ng Store Box 5.2.0

Security checklist for syslog-ng Store Box appliances

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SSB Security checklist for syslog-ng Store Box appliances
Updated - October 2018
Version - 5.2.0

Contents

3

Security checklist for configuring SSB

The following checklist is a set of recommendations and configuration best practices to ensure that your 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 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 or cleaning up the collected data" 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 Timestamping 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 **Strong**.

     By applying the **Strong** 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). Note that you cannot set cipher suites since the TLS server is the remote side (Step 5). For more information, see "Forwarding log messages to remote servers" in the Administration Guide.

- 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. For more information, see "Creating syslog message sources in SSB" in the Administration Guide.
- 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 **Strong** cipher suite set under **Basic Settings > Management > Web interface and RPC API > Cipher suite**. For more information, see "Web interface and RPC API" in the Administration Guide.
- Use strong passwords, which have 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 "Setting password policies for local users" 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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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