# Quick Start Guide for syslog-ng Premium Edition 6 LTS

**June 19, 2018**

# Table of Contents

# 1. Introduction

The syslog-ng application is a flexible and highly scalable system logging application that is ideal for creating centralized and trusted logging solutions.

Typically, syslog-ng is used to manage log messages and implement centralized logging, where the aim is to collect the log messages of several devices on a single, central log server. The different devices — called syslog-ng clients — all run syslog-ng, and collect the log messages from the various applications, files, and other *sources*. The clients send all important log messages to the remote syslog-ng server, which sorts and stores them.

## 1.1. Modes of operation

The syslog-ng Premium Edition application has three distinct operation scenarios: *Client*, *Server*, and *Relay*. The syslog-ng PE application running on a host determines the mode of operation automatically based on the license and the configuration file.

In server mode, syslog-ng acts as a central log-collecting server. It receives messages from syslog-ng clients and relays over the network, and stores them locally in files, or passes them to other applications, for example log analyzers.

In client mode, syslog-ng collects the local logs generated by the host and forwards them through a network connection to the central syslog-ng server or to a relay. Clients often also log the messages locally into files.

In relay mode, syslog-ng receives logs through the network from syslog-ng clients and forwards them to the central syslog-ng server using a network connection. Relays also log the messages from the relay host into a local file, or forward these messages to the central syslog-ng server.

## 1.2. Scope

This guide contains instructions for setting up syslog-ng Premium Edition (PE) for evaluation. It covers server installation in Linux, and client installation on Linux and Windows.

In addition, basic configuration options are provided for disk buffering, reliable transfer protocol, macros in filenames, storing messages in encrypted files, and configuring syslog-ng to act as a relay.

This guide is intended as a quick introduction. For evaluating syslog-ng PE in scenarios which exceed the single client-to-server complexity (including, but not limited to usage in domain hosts, complex networks, productive environments, and load testing), refer to *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

## 1.3. Supported platforms

The list of supported platforms is available here:

*https://syslog-ng.com/log-management-software/supported-platforms*.

For Windows, the syslog-ng Agent for Windows application is available for all Windows releases starting with Windows XP, including the 64-bit versions of the operating system.

# 2. Installation

## 2.1. Procedure – Downloading the Linux installer (server and client)

**Purpose:**

To obtain the syslog-ng Premium Edition installer from MyBalaBit, complete the following steps:

**Prerequisites:**

The installers are available via *MyDownloads*. In addition to the installers, a *valid license* is required to install the syslog-ng PE server. Contact your sales representative for access and license files.

**Steps:**

Step 1. Navigate to **Downloads** > **All files** > **syslog-ng**> **premium edition**

Step 2. Choose the latest available version (4.2.4 is used as an example)

Step 3. Navigate to **Setups** > **linux-glibc2.3.6-amd64**

Step 4. Download `syslog-ng-premium-edition-4.2.4-linux-glibc2.3.6-amd64.run`
The binaries include all required libraries and dependencies of syslog-ng. These components are installed in the `/opt/syslog-ng` directory.

The installer can reuse existing configuration and license files, and also generate a simple configuration automatically into the `/opt/syslog-ng/etc/syslog-ng.conf` file.

**Note**
Existing syslog implementations on Linux systems are replaced during installation.

## 2.2. Procedure – Downloading the Windows installer (client only)

**Purpose:**

To obtain the syslog-ng Agent for Windows installer from MyBalaBit, complete the following steps:

**Prerequisites:**

The installers are available via *MyDownloads*. In addition to the installers, a *valid license* is required to install the syslog-ng PE server. Contact your sales representative for access and license files.

**Steps:**

Step 1. Navigate to **Downloads** > **All files** > **syslog-ng** > **syslog-ng-agent**

Step 2. Choose the latest available version (5.0.1a is used as an example)

Step 3. Navigate to **Setups** > **win32**

Step 4. Download `syslog-ng-agent-5.0.1a-setup.exe`
Regardless of the path name, the installer contains both the 32-bit and the 64-bit binaries.

Step 5. **Installing the .NET framework (Windows only).**
The installer requires Microsoft .NET framework version 3.5 or 4.0. For further details, see *Procedure 2.1, Installing the syslog-ng Agent in standalone mode* in *The syslog-ng Agent for Windows 6 LTS Administrator Guide*.

## 2.3. Procedure – Installing the syslog-ng PE server on Linux

**Purpose:**

To install syslog-ng Premium Edition in server mode, complete the following steps:

**Prerequisites:**

Running syslog-ng Premium Edition in server mode requires a license file. The license determines how many individual hosts can connect to the server. You can obtain the license from your sales representative.

**Steps:**

Step 1. Copy the installer and `license.txt` file to the server.

Step 2. Execute the following command as root:
```
sh syslog-ng-premium-edition-4.2.4-linux-glibc2.3.6-amd64.run
```

Step 3. Select **Continue** on the Welcome screen, and accept the EULA.

Step 4. Verify that the system summary is correct.
If false information is displayed, your platform might not be supported. Abort installation, and if necessary, contact BalaBit for support.

Step 5. Keep the default installation path and register your installation. Existing syslog implementations on the system are replaced.

Step 6. Provide the full path to the license file (`license.txt`).

Step 7. The installer generates a simple configuration. Make the following changes:

- Enable receiving remote log messages
- Skip entering a remote destination

**Expected outcome.**

The installer stops the previously installed syslog implementation, and starts the syslog-ng PE server.

Step 8. *Validating the installation*
Test local logging:

Step a. Issue the following commands as root:
```
logger test message
```

Step b. Verify local log with the following command:
```
tail /var/log/messages
```

**Expected outcome.**

The`test message`line is displayed in the log.

## 2.4. Procedure – Installing the syslog-ng PE client on Linux

**Purpose:**

To install syslog-ng Premium Edition in client mode, complete the following steps:

**Prerequisites:**

No license file is required to run syslog-ng PE in client mode.

**Steps:**

Step 1. Execute the following command as root:

```
sh syslog-ng-premium-edition-4.2.4-linux-glibc2.3.6-amd64.run
```

Step 2. Select **Continue** on the Welcome computeroutput, and accept the EULA.

Step 3. Verify that the system summary is correct.
If false information is displayed, your platform might not be supported. Abort installation, and if necessary, contact BalaBit for support.

Step 4. Keep the default installation path and register your installation. Existing syslog implementations on the system are replaced.

Step 5. The installer generates a simple configuration. Make the following changes:

- Disable receiving remote log messages
- Enter the IP address or host name of the syslog-ng PE server as remote destination

**Expected outcome.**

The installer stops the previously installed syslog implementation, and starts the syslog-ng PE client.

Step 6. *Validating the installation*

Step a. Test local logging. Issue the following commands as root:

```
logger test message
```

Step b. Verify local log with the following command:

```
tail /var/log/messages
```

**Expected outcome.**

The`test message`line is displayed in the log.

Step c. Test remote logging. On the client machine, enter the following command:

```
logger remote test message
```

Step d. Verify the server log. On the syslog-ng PE server, enter:

```
tail /var/log/messages
```

**Expected outcome.**

The host name of the client machine and the message text`remote test message`is displayed in the log.

**Troubleshooting.**

If messages are not forwarded from the client to the server, check if port 514 is blocked by a firewall (protected by default on most Linux servers).

## 2.5. Procedure – Installing on Windows

**Purpose:**

The following instructions describe the standalone installation, which is configured locally. For more advanced installation options (using domain group policies, installing by group policy), refer to *The syslog-ng Agent for Windows 6 LTS Administrator Guide*.

**Steps:**

Step 1. Execute the downloaded binary.

Step 2. Accept the EULA.

Step 3. Select the destination folder for syslog-ng Agent for Windows.

Step 4. Choose **Stand alone mode**.

Step 5. The installer generates a simple configuration. Enter the destination IP of the syslog-ng PE server:

- Step a. Select **Destinations**
- Step b. Double-click **Add new server**
- Step c. Enter the server's IP address
- Step d. Change the port number to *`601`*
- Step e. Click **OK**

Step 6. Close the configuration window to finish installation.

Step 7. *Validating the installation*
Test remote logging:

- Step a. Log out and back in on the Windows client
- Step b. Verify the server log. On the syslog-ng PE server, enter the following command:

```
tail /var/log/messages
```

**Expected outcome.**

The logout and login events are displayed in the log.

# 3. Configuring syslog-ng PE

The syslog-ng application reads incoming messages and forwards them to the selected *destinations*. The syslog-ng application can receive messages from files, remote hosts, and other *sources*.

Log messages enter syslog-ng in one of the defined sources, and are sent to one or more *destinations*.

Sources and destinations are independent objects: *log paths* define what syslog-ng does with a message, connecting the sources to the destinations. A log path consists of one or more sources and one or more destinations, messages arriving from a source are sent to every destination listed in the log path. A log path defined in syslog-ng is called a *log statement*.

There are many other optional elements, like filters, parsers, etc., but in this guide we focus on a core syslog-ng feature: reliable logging.

## 3.1. Procedure – Enabling disk buffer on the syslog-ng PE client on Linux

**Purpose:**

The Premium Edition of syslog-ng can store messages on the local hard disk if the central log server or the network connection to the server becomes unavailable. This feature is called the disk buffer and needs to be configured only on the client side.

**Note**
The log messages on Windows come from files – either eventlog containers or custom log files – which are already stored on the hard disk, so the agent does not use additional disk buffering.

To enable disk buffering on the syslog-ng PE client on Linux, modify its configuration:

**Steps:**

Step 1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor.

Step 2. Locate the line starting with`destination d_logserver`.

Step 3. Modify it to look like the following line:

```
destination d_logserver
     {
      tcp("<PEServerIP>" disk-buffer(disk-buf-size(2000000)));
     };
```

Replace *`<PEServerIP>`* with the hostname or IP address of the syslog-ng PE server.

For additional disk buffer options, refer to *Section 7.8.1, network() destination options* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Step 4. Save the configuration and restart syslog-ng.

## 3.2. Reliable Transfer Protocol™

The syslog-ng PE application can send and receive log messages in a reliable way over the TCP transport layer using the Reliable Log Transfer Protocol™ (RLTP™). RLTP™ is a proprietary transport protocol that prevents message loss during connection breaks. The transport is used between syslog-ng PE hosts (for example, a client and a server, or a client-relay-server), and interoperates with the flow-control and reliable disk-buffer mechanisms of syslog-ng PE, thus providing the best way to prevent message loss. The sender detects which messages has the receiver successfully received. If messages are lost during the transfer, the sender resends the missing messages, starting from the last successfully received message. Therefore, messages are not duplicated at the receiving end in case of a connection break (however, in failover mode this is not completely ensured). RLTP™ also allows to receive encrypted and non-encrypted connections on the same port, using a single source driver.

To make RLTP work, you have to enable it on the server and on all participating clients as well. In the following example, a minimum working configuration is provided. For additional options, including TLS configuration, refer to *Chapter 12, Reliable Log Transfer Protocol™* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

### 3.2.1. Procedure – Configuring the syslog-ng PE server for RLTP

**Purpose:**

To configure the syslog-ng Premium Edition server for RLTP, complete the following steps:

**Steps:**

Step 1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor

Step 2. Replace the line `syslog();` with the following:

```
syslog(port(601) transport(rltp(tls-required(no))));
```

Step 3. Save the file and restart syslog-ng
**Expected outcome.**

The syslog source now supports RLTP protocol as a transport, without TLS support. Declaring the port is necessary, as there is no default port number for RLTP transport.

### 3.2.2. Procedure – Configuring syslog-ng Windows clients for RLTP

**Purpose:**

To configure the syslog-ng Windows clients for RLTP, complete the following steps:

**Steps:**

Step 1. From the Start menu, launch the **Configure syslog-ng Agent for Windows** application

Step 2. Select **Destinations**

Step 3. Right-click the previously configured destination, and choose **Properties**

Step 4. Enable **RLTP**

Step 5. Choose **OK** to save your changes, and exit from the configuration interface

Step 6. Restart syslog-ng Agent for the new configuration settings to take effect

> **Note**
> To restart services, you need Administrator privileges. If you use the **Stop syslog-ng Agent** and **Start syslog-ng Agent** options from the Start Menu, remember to right-click and choose the **Run as Administrator** option.

Step 7. Remote logging can be tested the same way as described in *Procedure 2.5, Installing on Windows (p. 7)*.

### 3.2.3. Procedure – Configuring syslog-ng Linux clients for RLTP

**Purpose:**

To configure the syslog-ng Linux clients for RLTP, complete the following steps:

**Steps:**

Step 1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor.

Step 2. Replace the line starting with`destination d_logserver`with the following:

```
destination d_logserver
 {
  syslog("<PEServerIP>" transport(rltp())
  port("601")
  disk-buffer(disk-buf-size(2000000)));
 };
```

Replace <*PEServerIP*> with the hostname or IP address of the syslog-ng PE server.

Step 3. Save the file and restart syslog-ng.
Remote logging can be tested the same way as described in *Procedure 2.4, Installing the syslog-ng PE client on Linux (p. 6)*.

## 3.3. Procedure – Macros in filenames

**Purpose:**

On servers where logs of many clients are retained for extended periods of time, log files are usually stored under a directory hierarchy. To help sort incoming log messages to such hierarchies, syslog-ng supports the use of macros. Depending on the needs of your organization, date, source host, or combined solutions can be used.

In the following example, the file destination on the server is modified to also write messages into a directory structure under `/var/log`, where the first level is the year, the second level is the week of the year, followed by a file name based on the sending host.

**Steps:**

Step 1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor

Step 2. Locate the line starting with`destination d_messages`

Step 3. Modify it to look like the following line:

```
destination d_messages
 {
  file(“/var/log/messages”);
  file("/var/log/$YEAR/$WEEK/$HOST-messages" create-dirs(yes));
 };
```

Step 4. Save the file and restart syslog-ng

**Note**

Collecting to `/var/log/messages` is left there for your convenience, it can be safely removed. Even if the related configuration item is removed, the file stays there, but it is not updated anymore.

For more details on macros available in syslog-ng, refer to *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

## 3.4. Procedure – Storing messages in encrypted files

**Purpose:**

The syslog-ng PE application can store log messages securely in encrypted, compressed and timestamped binary files. Timestamps can be requested from an external Timestamping Authority (TSA).

Logstore files consist of individual chunks, every chunk can be encrypted, compressed, and timestamped separately. Chunks contain compressed log messages and header information needed for retrieving messages from the logstore file.

The syslog-ng PE application generates an SHA-1 hash for every chunk to verify the integrity of the chunk. The hashes of the chunks are chained together to prevent injecting chunks into the logstore file. The syslog-ng PE application can encrypt the logstore using various algorithms, using the aes128 encryption algorithm in CBC mode and the hmac-sha1 hashing (HMAC) algorithm as default.

In the following example, a simple logstore destination is added which stores logs with maximum compression.

**Steps:**

Step 1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor

Step 2. Locate the line starting with`destination d_messages`

Step 3. Add the following line right below:

```
destination d_logstore
 {
  logstore("/var/log/messages.lgs" compress(9) );
 };
```

Step 4. Locate the line containing`destination(d_messages)`

Step 5. Add the following line right below:

```
destination(d_logstore)
```

Step 6. Restart syslog-ng for the configuration changes to take effect

Step 7. *Validating the changes*
You can verify that logs are arriving to the logstore using the following command:

```
/opt/syslog-ng/bin/logcat /var/log/messages.lgs
```

## 3.5. Procedure – syslog-ng PE as a relay

**Purpose:**

As mentioned earlier, syslog-ng PE can be turned into a relay. This functionality is often used on larger networks, or when logs are collected from network devices using UDP and forwarded to a central location using the more reliable TCP or RLTP protocols. When used as a relay, syslog-ng PE does not store the logs locally, but forwards them immediately to the central syslog-ng PE server.

In this example, a syslog-ng PE Linux client is reconfigured as a relay.

**Steps:**

Step 1. Open `/opt/syslog-ng/etc/syslog-ng.conf` in a text editor

Step 2. Remove the current log statement: starting with line`log {`, delete everything until the end of the file

Step 3. Add a new UDP source for router logs:

```
source s_udp {udp();};
```

Step 4. Add a new log path for storing local logs locally:

```
log { source(s_local); destination(d_messages); };
```

Step 5. Add a new log path for sending both local messages and logs collected from the UDP source to the central server:

```
log
 {
  source(s_local);
  source(s_udp);
  destination(d_logserver);
 };
```

Step 6. *Validating the changes*
Test the relay by executing the following command on the relay machine:

```
/opt/syslog-ng/bin/loggen -i -D localhost 514
```

It generates about a thousand messages a second and sends to the UDP port of the local syslog-ng PE relay. Executing `tail /var/log/messages` should not show any of the generated messages on the relay, but doing the same on the server machine should show a large number of similar lines:

```
Sep 20 21:18:09 relayhost prg00000[1234]: seq: 0000009458, thread: 0000,
runid: 1379704679, stamp: 2013-09-20T21:18:09
PADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADD
```

# 4. Further information

## 4.1. About One Identity

One Identity LLC, is a leading provider of Privileged Access Management (PAM) and Log Management solutions. Founded in 2000, One Identity has a proven track record of helping businesses reduce the risk of data breaches associated with privileged accounts. With offices in the United States and Europe, and a global client list that includes 25 Fortune 100 companies, One Identity and its network of reseller partners serves more than 1,000,000 corporate users worldwide.

For more information, visit *syslog-ng.com*, read the *syslog-ng blog*, or follow us on Twitter via @balabit, LinkedIn or Facebook.

To learn more about commercial and open source One Identity products, request an evaluation version, or find a reseller, visit the following links:

- *The syslog-ng homepage*
- *syslog-ng Documentation page*
- *Contact us and request an evaluation version*

### About One Identity

One Identity helps organizations optimize identity and access management (IAM). Our combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, enables organizations to achieve their full potential — unimpeded by security, yet safeguarded against threats. For more information, visit *oneidentity.com*.

## 4.2. Sales contact

You can directly *contact our Sales Team* with sales related topics.

All questions, comments or inquiries should be directed to `<info@balabit.com>` or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*