Windows 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.

syslog-ng Premium Edition on Windows:

The syslog-ng Premium Edition on Windows application has most of the features of its Linux/UNIX counterpart, and comes with the same text-based configuration. For limitations specific to the platform, see *Section 1.6.1, Limitations on Microsoft Windows platforms* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Three distinct operation scenarios are available:

- 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 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 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.

The application determines the mode of operation automatically, based on the license and the configuration file.

syslog-ng Agent for Windows:

A lightweight client alternative to syslog-ng Premium Edition for Windows, the syslog-ng Agent for Windows application can collect and forward log messages to a remote server. It comes with a graphical user interface, and it's easier to deploy to a large number of machines.

1.1. Scope

This guide contains instructions for setting up syslog-ng Premium Edition (PE) as server and syslog-ng Agent for Windows as client on Windows for evaluation.

In addition, basic configuration options are provided for reliable transfer protocol, macros in filenames, and storing messages in encrypted files.

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*.

1.2. Supported platforms

The list of supported platforms for syslog-ng PE for Windows and syslog-ng Agent for Windows is available here:

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

2. Installation

2.1. Procedure – Downloading the server installer

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 (5.0.2 is used as an example)

Step 3. Download the 32-bit or 64-bit installer, depending on your server's architecture:

- For the 32-bit installer, navigate to **Setups** > **win32** and download `syslog-ng-premium-edition-5.0.2-win32.exe`
- For the 64-bit installer, navigate to **Setups** > **win64** and download `syslog-ng-premium-edition-5.0.2-win64.exe`

The binaries include all required libraries and dependencies of syslog-ng. These components are installed in the `C:\Program Files\syslog-ng` directory by default.

The installer can reuse existing configuration and license files. Following installation, sample configuration files are also available in the `etc` subfolder.

2.2. Procedure – Downloading the client installer (Windows Agent)

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 (5.0.2 is used as an example)

Step 3. Navigate to **Setups** > **win32** and download `syslog-ng-agent-5.0.2-setup.exe`
Regardless of the path name, the installer contains both the 32-bit and the 64-bit binaries.

Step 4. **Installing the .NET framework.**

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 syslog-ng Premium Edition for Windows as server

Purpose:

To install syslog-ng Premium Edition for Windows as server, complete the following steps:

Prerequisites:

Running syslog-ng PE 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 installer

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

Step 4. Select **Install syslog-ng Premium Edition** and choose **Next** (the other option will simply unpack syslog-ng without registering it as a service)

Step 5. Keep the default installation path and choose **Next**

Step 6. Navigate to the license file (`license.txt`) and choose **Next**

Step 7. At this point, existing configurations could be loaded from backup. Skip this step by choosing **Next**

Step 8. Click **Install** to start the installation. Wait for the process to finish, then choose **Close**

Step 9. Configure the server using the sample configuration file:

Step a. Navigate to `C:\Program Files\syslog-ng\etc`

Step b. Copy `syslog-ng-eventlog-to-file-sample.conf` to `syslog-ng.conf`

Step c. The sample configuration file is configured to store logs in the `C:\tmp` temporary folder.
Create the `C:\tmp` temporary folder for storing logs.

Step 10. Start syslog-ng as an administrator:

Step a. In the Start menu, navigate to **All Programs** > **syslog-ng Premium Edition**

Step b. Right-click **Start syslog-ng**, and choose **Run as Administrator**
Expected outcome.

`syslog-ng PE is started, and logs appear in C:\tmp\eventlog_to_file_example.txt.`

2.4. Procedure – Preparing for the client installation

Purpose:

To verify the client installation, a new network source must be added to the syslog-ng PE configuration:

Steps:

Step 1. Open the `C:\Program Files\syslog-ng\etc\syslog-ng.conf` configuration file for editing

Step 2. Add the following snippet to the end of the file:

```
source s_network {
 syslog();
};

destination d_nettofile {
 file('C:\tmp\tcp_to_file_example.txt' flags(no-multi-line));
};

log {
 source(s_network);
 destination(d_nettofile);
 flags(flow-control);
};
```

Step 3. Save the configuration file

Step 4. Restart the syslog-ng service

2.5. Procedure – Installing the syslog-ng Agent for Windows client

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*.

Prerequisites:

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

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.
Expected outcome.

On the syslog-ng PE server, the logout and login events are displayed in the `C:\tmp\tcp_to_file_example.txt` logfile.

3. Configuring syslog-ng Premium Edition

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.

Note
The syslog-ng PE server for Windows can also be installed without a license file. In this case it will act as a client or relay (depending on configuration), but with some additional features compared to syslog-ng Agent for Windows. These features include disk buffer and relay.

Consult the documentation or a pre-sales engineer for further details.

3.1. 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*.

3.1.1. 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 C:\Program Files\syslog-ng\etc\syslog-ng.conf configuration file for editing

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.

3.1.2. Procedure – Configuring syslog-ng Agent for Windows clients for RLTP

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 2.2, Downloading the client installer (Windows Agent) (p. 5)*.

3.2. Procedure – Macros in file names

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 C:\Program Files\syslog-ng\etc\syslog-ng.conf configuration file for editing

Step 2. Locate the block starting with`destination d_nettofile`

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

```
destination d_nettofile {
 file('C:\tmp\tcp_to_file_example.txt' flags(no-multi-line));
 file('C:\tmp\$YEAR\$WEEK\$HOST-messages' flags(no-multi-line)
create-dirs(yes));
};
```

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

Step 4. Save the file and restart syslog-ng

Note
Collecting to `C:\tmp\tcp_to_file_example.txt` is left there for your convenience, it can be safely removed. If the related configuration item is removed, the file stays in the folder, but will not be updated.

3.3. 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 C:\Program Files\syslog-ng\etc\syslog-ng.conf configuration file for editing

Step 2. Locate the block starting with`destination d_nettofile`

Step 3. Add the following line right below:

```
destination d_logstore {
 logstore('C:\tmp\messages.lgs' compress(9) );
};
```

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

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:

```
"C:\Program Files\syslog-ng\bin\lgstool.exe” cat C:\tmp\messages.lgs
```

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/*