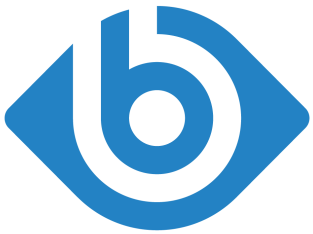
What is new in syslog-ng Premium Edition 6 LTS

May 10, 2017



BALABIT

Table of Contents

1. Preface

Welcome to syslog-ng Premium Edition (syslog-ng PE) version 6 LTS and thank you for choosing our product. This document describes the new features and most important changes since the latest release of syslog-ng PE. The main aim of this paper is to aid system administrators in planning the migration to the new version of syslog-ng PE. The following sections describe the news and highlights of syslog-ng PE 6 LTS.

This document covers the 6 LTS feature release of the syslog-ng Premium Edition product.

The following release policy applies to syslog-ng Premium Edition:

- *Long Term Supported or LTS releases* (for example, syslog-ng Agent 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, syslog-ng PE 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, syslog-ng Agent 4 F1) are supported for 6 months after their original publication date and for 2 months after succeeding Feature or LTS Release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new feature per release. Only the last of the feature releases is supported (for example when a new feature release comes out, the last one becomes unsupported).
  For a full description on stable and feature releases, see *Stable and feature releases*.

Warning
Downgrading from a feature release to an earlier (and thus unsupported) feature release, or to the previous LTS release is officially not supported, but usually works as long as your syslog-ng PE configuration file is appropriate for the old syslog-ng PE version. However, persistent data like the position of the last processed message in a file source will be probably lost.

Logstore files created with a newer version of syslog-ng PE might not be readable with an older version of syslog-ng PE.

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

2. Changes since syslog-ng PE 5 F6

Parsing `key=value` pairs

The syslog-ng PE application can separate a message consisting of whitespace or comma-separated `key=value` pairs (for example, Postfix log messages) into name-value pairs. You can also specify other separator character instead of the equal sign, for example, colon (`:`) to parse MySQL log messages. For details, see *Section 14.2, Parsing `key=value` pairs* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Updated TLS ciphers, new parameters

The OpenSSL application used in syslog-ng PE has been updated to version 1.0.2, so you can use new, stronger ciphers to protect the communication between your syslog-ng PE clients and servers. For an updated list of supported ciphers, see *Section cipher-suite()* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Also, you can now specify the curves that are permitted in the connection using the *`list-curves()`* option, and also import Diffie-Hellman parameters from a file using the *`dhparam-file()`* option. For details, see *Section 10.4, TLS options* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Other changes

- Starting from version 6 LTS, the syslog-ng PE installer packages (earlier called `client` and `server` package) are renamed. From now on, the package with the `compact` suffix does not include SQL support. If you do not use the *`sql()`* source or destination on the host, use the `compact` binaries. That way no unnecessary components are installed to your system. Earlier, the names of packages containing *`sql()`* support included the `server` suffix, this suffix has been removed from the package names.

Changes in syslog-ng Agent for Windows

- The graphical interface of the syslog-ng Agent for Windows application now supports version 4.0 of the Microsoft .NET Framework.
- Group Policies can be configured directly from the syslog-ng Agent for Windows interface.
- When creating a filter based on Event Source names, the Windows Agent interface displayed a list of possible sources. However, the names of this list did not always match the actual name of the Event Source (as displayed in the Event Viewer). From now on, the Windows Agent does not list the possible Event Source names. To create a filter using Event Source names, first find the "Source:" field as shown on the General tab of the Event Viewer, and enter its value in the filter.

Platform changes in syslog-ng PE 6 LTS

New platforms in syslog-ng PE 6 LTS:

- Ubuntu 16.04 LTS (Xenial Xerus)
- Windows Server 2016 (in syslog-ng PE version 6.0.4)

Platforms not supported in syslog-ng PE 6 LTS:

- AIX 6.1
- FreeBSD 9

- HP-UX 11i v2

For a complete list of supported platforms, see *Section 1.6, Supported platforms* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Platform changes in syslog-ng Agent for Windows 6 LTS

New platforms in syslog-ng Agent for Windows 6 LTS:

- Windows 10
- Windows Server 2012
- Windows Server 2016 (in syslog-ng PE version 6.0.4)

Platforms not supported in syslog-ng Agent for Windows 6 LTS:

- Microsoft Windows Server 2003
- Microsoft Windows XP SP3

For a complete list of supported platforms, see *Section 1.1, Supported operating systems* in *The syslog-ng Agent for Windows 6 LTS Administrator Guide*.

3. Changes between syslog-ng PE 5 LTS and 5 F6

3.1. New destinations

Elasticsearch 2.x and Shield support

Version 5 F6 of syslog-ng PE supports Elasticsearch version 2.0 and newer. Because of compatibility reasons, syslog-ng PE has a separate destination (`elasticsearch2()`) that you can use with Elasticsearch version 2.0 and newer.

X-Pack security (Elasticsearch Shield) is supported for both Elasticsearch 1.x and 2.x destinations, allowing you to authenticate your syslog-ng PE clients on the Elasticsearch server.

For details, see *Section 7.2, Sending messages directly to Elasticsearch version 2.0 or higher* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Send messages directly to Elasticsearch

Version 5.4 of syslog-ng PE can directly send log messages to *Elasticsearch*, allowing you to search and analyze your data in real time, and visualize it with *Kibana*. For details, see *Section 7.1, Sending messages directly to Elasticsearch version 1.x* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Publish messages to Apache Kafka

The syslog-ng PE application allows you to publish your log data to your Apache Kafka message bus, where subscribers can access them, making it easy to integrate your log data into a big data solution. For details, see *Section 7.5, Publishing messages to Apache Kafka* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Hadoop Distributed File System (HDFS) support

Version 5.3 of syslog-ng PE can send plain-text log files to the *Hadoop Distributed File System (HDFS)*, allowing you to store your log data on a distributed, scalable file system. This is especially useful if you have huge amount of log messages that would be difficult to store otherwise, or if you want to process your messages using Hadoop tools (for example, Apache Pig). For details, see *Section 7.4, Storing messages on the Hadoop Distributed File System (HDFS)* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Storing messages in MongoDB database

MongoDB is a schema-free, document-oriented database, ideal to collect log messages. Since it does not require a predetermined schema, it gives you much more flexibility than the SQL databases, making it it easy to store name-value pairs extracted from log messages. That way, you can conveniently store metadata received in a log message (for example, in the SDATA part of RFC5424-formatted log messages), or other data parsed from the body of the log messages (for example, usernames parsed from login/logout messages). For details, see *Section 7.7, Storing messages in a MongoDB database* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Sending e-mail alerts

An important aspect of logging is alerting on important but rare events. A common way to do that is via e-mail, sent either to people or to services which process them further. The SMTP destination driver allows you to send

e-mails based on incoming log messages to one or more addresses. For details, see *Section 7.11, Generating SMTP messages (e-mail) from logs* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

3.2. Processing incoming messages

Parsing JSON messages

JavaScript Object Notation (JSON) is a text-based open standard designed for human-readable data interchange. It is used primarily to transmit data between a server and web application, serving as an alternative to XML. The syslog-ng PE application can separate parts of JSON-encoded log messages to name-value pairs, allowing you to receive structured log messages from such applications, store them, and convert them to other format if needed. For details, see *Section 14.3, The JSON parser* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Reading messages from the systemd journal

The systemd journal is a new type of system log storage. This is used, or will be used on most Linux distributions, such as RHEL (from RHEL7), Fedora, CentOS, and so on. The journal can store name-value pairs instead of the traditional system log entries. syslog-ng PE 6 LTS can directly read log messages from the journal file of platforms using systemd. For details, see *Section 6.12, Collecting messages from the systemd-journal system log storage* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

3.3. Formatting messages

Formatting messages as Common Event Format extensions

syslog-ng PE version 5 F6 includes a new template function (`format-cef-extension`) to format name-value pairs as ArcSight Common Event Format extensions. Note that the template function only formats the selected name-value pairs, it does not provide any mapping. There is no special support for creating the prefix part of a Common Event Format message.

For details, see *Section format-cef-extension* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*

Converting messages into JSON format

The syslog-ng PE application can convert messages or selected value-pairs into JavaScript Object Notation (JSON) format. Including the template function in a message template allows you to store selected information about a log message (that is, its content, macros, or other metadata) in JSON format, or to forward JSON messages to external applications. For details, see *Section format-json* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Selecting and using name-value pairs

The syslog-ng PE application allows you to select and construct name-value pairs from any information already available about the log message, or extracted from the message itself. You can directly use this structured information, for example, in the following places:

- `mongodb()` destination (for details, see *Section 7.7, Storing messages in a MongoDB database* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*)
- `format-welf()` template function (for details, see *Section format-welf* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*)

- or in other destinations using the `format-json()` template function (for details, see *Section format-json* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*).

For details about value-pairs, see *Section 2.12, Structuring macros, metadata, and other value-pairs* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Rewriting multiple macros

Using the `groupset` rewrite rule, you can rewrite multiple macros at the same time, making it easy to modify the values of fields parsed using patterndb or from JSON. You can specify the list of macros manually, or also as a glob pattern. For details, see *Section 13.2.4, Setting multiple message fields to specific values* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Comparing macro values to a list

The syslog-ng PE application can compare the value of a macro to a list of strings. Earlier, if a specific macro had several different values, filtering on the macro values required several filter statements. Now you can specify every expected value in a file, and use the contents of that file in a filter. For details, see *Section 13.2.4, Setting multiple message fields to specific values* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Creating hashes from macro values

With the `hash` template function, you can create message digests from parts of the log message. For details, see *Section hash* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Adding a unique ID to log messages

HOSTID is a 32-bit number generated by a cryptographically secure pseudorandom number generator. Its purpose is to identify the syslog-ng PE host, thus it is the same for every message of the host. It can be accessed via the $HOSTID macro (which cannot be rewritten).

When the global option `use-uniqid(yes)` is set, syslog-ng PE generates this practically unique id for every received or locally generated message. You can add this ID to your messages using the $UNIQID macro. For details, see *Section use-uniqid()* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

3.4. Managing syslog-ng PE

Displaying license-related information

The syslog-ng PE application uses a license in server mode to determine the maximum number of hosts that are allowed to connect. Use the `syslog-ng-ctl show-license-info` command to display license-related information the number of hosts currently logging to your server. This helps you to plan your capacity, to check your license usage, and to detect client misconfiguration that can result in a license miscount anomaly. Note that in client or relay mode, syslog-ng PE does not require a license. For details, see *the section called "Displaying license-related information"* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Managing syslog-ng PE from Puppet

To simplify the management of large-scale syslog-ng PE deployments, you can now centrally manage your syslog-ng PE hosts from *Puppet*. The syslog-ng Premium Edition Puppet module allows you to perform the following tasks.

- Install syslog-ng PE from a package repository.

- Upgrade syslog-ng PE to a newer version.
- Delete syslog-ng PE from a host.
- Update the syslog-ng PE configuration file of your hosts from a central repository.
- Create backup of your syslog-ng PE configuration files. You can redistribute these backups to your hosts if a rollback is needed.

The Puppet module supports the following platforms: Red Hat Enterprise Linux (RHEL), Oracle Linux, CentOS, Ubuntu, and Debian. Other Linux platforms based on `.deb` and `.rpm` packages might also work, but are not tested. For details, see *Procedure 3.10, Managing syslog-ng PE from Puppet* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

New statistics framework

So far, you could access statistics only in unstructured format, using the `syslog-ng-ctl stats` command. Now you can query information from a running syslog-ng PE instance using the new `syslog-ng-query` utility. This tool allows you to access selected statistics in a controlled way, making it easy to process or monitor the results. This is a first step in a new statistics framework that aims to improve the how syslog-ng PE instances can be monitored.

Note that this new framework might decrease the performance of syslog-ng PE under very high load. If you experience any issues, contact the Balabit Support Team and let us know the details of your use case, so we can correct the problem.

Improved SELinux support

In addition to Red Hat Enterprise Linux 6.5, syslog-ng PE now supports SELinux on Red Hat Enterprise Linux 5, as well as on 6.0-6.4. The CentOS platforms corresponding to the supported RHEL versions are supported as well. For details, see *Procedure 3.5, Using syslog-ng PE on SELinux* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

Supported platforms

For a complete list of supported platforms, see *Section 1.6, Supported platforms* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.

3.5. Other changes

- You can now specify the location where syslog-ng PE stores the disk-buffer files using the *`dir()`* option of *`disk-buffer()`*. Note that the *`dir()`* option overrides the settings of the `--qdisk-dir` command-line option.
- Value-pairs now have a new option to select every value-pair that has a name beginning with a specified prefix, but remove the prefix when formatting the message. For details, see *Section value-pairs()* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.
- The syslog-ng Agent on Windows application now searches for CA certificates also in the Intermediate Certification Authorities Store.
- So far, the largest message syslog-ng PE could handle was 64kbyte, because internally syslog-ng PE represented the messages in a 16-bit nvtable. From now on, syslog-ng PE uses a 32-bit nvtable, allowing you to receive and manipulate messages much larger than 64kbyte.

- The *sql()* source and destination driver on the HP-UX platform does not support the Oracle SQL database anymore.
- On other platforms where Oracle SQL database is supported, the *sql()* source and destination driver supports version 12 of the Oracle SQL database.
- CSV-parsers can use strings as delimiters. For details, see *Section delimiters()* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.
- Multithreading is enabled by default (`threaded(yes)`).
- The `persist-tool` utility has a new `--rename-key` option to help solve troubleshooting the persist file.
- The `syslog-ng-ctl` utility has a new `stats --reset` option that resets all statistics counters to zero.
- A new utility called `syslog-debun` is available in syslog-ng PE 6 LTS. This tool can be used to collect information about your syslog-ng PE environment into a debug bundle to simplify troubleshooting and increase the speed of solving support tickets.
- When using the *program()* destination, the external application keeps on running when syslog-ng PE exits if the *keep-alive()* option is set.
- So far, you could create custom configuration blocks that had a fixed number of arguments. You can now create custom configuration blocks that can receive variable number of arguments, making the configuration of syslog-ng PE even more flexible. For example, this can be useful when passing arguments to a template, or optional arguments to an underlying driver. For details, see *Section 5.7.2.1, Passing arguments to configuration blocks* in *The syslog-ng Premium Edition 6 LTS Administrator Guide*.