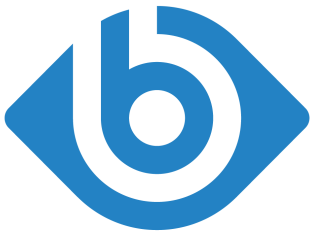
What is new in syslog-ng Premium Edition 5 LTS

November 19, 2015



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Table of Contents

1. Preface

Welcome to syslog-ng Premium Edition (syslog-ng PE) version 5 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 5 LTS.

This document covers the 5 LTS feature release of the syslog-ng Premium Edition product.

As of June 2011, the following release policy applies to syslog-ng Premium Edition:

- *Long Term Supported or LTS releases* (for example, syslog-ng PE 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 PE 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).

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.

2. Running syslog-ng Premium Edition on Windows platforms

Starting with version 5 LTS, syslog-ng Premium Edition is supported on Microsoft Windows platforms, allowing you to run a syslog-ng server on Windows. This is useful when collecting logs from Windows clients, as it does not require a separate Linux or UNIX host to run the syslog-ng server. It also allows you to collect the logs centrally from various networking devices (for example, routers, switches) and appliances that do not integrate their logging into Windows environments.

On Windows, you can configure syslog-ng PE similarly to other Linux and UNIX platforms using a configuration file.

Using the new eventlog() source, you can collect the native log messages of local Windows applications as well. As a result of making it possible to run syslog-ng PE on Microsoft Windows, several macros that were available only in syslog-ng Agent for Windows are now available in syslog-ng PE as well. For details, see *Section 13.1.5, Macros of syslog-ng PE* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

- For details on the limitations of running your syslog-ng PE logserver on Windows, see *Section 1.6.1, Limitations on Microsoft Windows platforms* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- For details on installing syslog-ng PE on Windows, see *Procedure 3.6, Installing syslog-ng PE on Windows platforms* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- For details on collecting logs from Eventlog containers, see *Section 6.2, Collecting messages from Windows eventlog sources* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

3. On-the-wire compression

When using the Reliable Log Transfer Protocol™ to transfer messages, syslog-ng PE can compress the log messages to save bandwidth. Using compression is especially useful to collect logs from low-bandwidth environments. For details, see *Section 12.2, RLTP™ options* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

4. Released in syslog-ng Premium Edition 4 F2

4.1. Reliable disk-based buffering

Reliable disk-based buffering is now available in syslog-ng PE. Use reliable disk-based buffering if you do not want to lose logs in case of reload/restart, unreachable destination or syslog-ng PE crash. This solution provides a slower, but reliable disk-buffer option. The disk-buffer file is created and initialized at startup and gradually grows as new messages arrive.

For details on reliable disk-based buffering, see *Section 8.3.1, Enabling reliable disk-based buffering* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

4.2. Collecting messages from SQL tables or relational databases

Starting with version 4 F2, the syslog-ng PE application is able to collect messages from SQL tables or relational databases, using the `sql()` driver. Currently the Microsoft SQL (MSSQL), MySQL, Oracle and PostgreSQL databases are supported. The syslog-ng PE application can connect to a database, collect records from a table, and then create a message from each record. Every query executed by the SQL source can be customized.

For details on messages from tables or relational database, see *Section 6.8, Collecting messages from tables or relational database* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

4.3. Reliable Log Transfer Protocol™

The syslog-ng 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 new transport protocol that prevents message loss during connection breaks. It detects the last received message on the receiving end and then starts resending messages from that point. Therefore, messages are not duplicated at the receiving end in case of a connection break. It also allows the negotiation of using TLS with a single source driver.

For details on Reliable Log Transfer Protocol™, see *Chapter 12, Reliable Log Transfer Protocol™* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

5. Released in syslog-ng Premium Edition 4 F1

5.1. New module architecture

syslog-ng PE became modular to increase its flexibility and also to simplify the development of additional modules. Most of the functionality of syslog-ng PE has been moved to separate modules. That way it becomes also possible to finetune the resource requirements of syslog-ng PE for example, by loading only the modules that are actually used in the configuration, or simply omitting modules that are not used but require large amount of memory.

For details on using modules, see *Section 5.6, Modules in syslog-ng PE* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

5.2. Multithreading, scaling, and performance improvements

Starting with version 4 F1, syslog-ng PE can be run in multithreaded mode to scale to multiple CPUs or cores for increased performance.

Depending on the exact syslog-ng PE configuration, environment, and other parameters, syslog-ng PE is capable of processing:

- over 150000 messages per second when receiving messages from a single connection and storing them in text files;
- over 150000 messages per second when receiving messages from a single connection and storing them in logstore files;
- over 500000 messages per second when receiving messages from multiple connections and storing them in text files;
- over 500000 messages per second when receiving messages from multiple connections and storing them in logstore files;
- over 100000 messages per second when receiving messages from secure (TLS-encrypted) connections and storing them in text files.

Note
By default, syslog-ng PE runs in single-thread mode. Multithreading must be explicitly enabled in the syslog-ng PE configuration file using the `threaded(yes)` option.

For details on using multithreading, see *Chapter 17, Multithreading and scaling in syslog-ng PE* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

5.3. Sending SNMP traps

The syslog-ng PE application can send SNMP traps using the Simple Network Management Protocol version 2c or version 3. Incoming log messages can be converted to SNMP traps, and the fields (such as the trap OID) of the SNMP messages can be customized using syslog-ng PE macros. Converting the syslog messages sent by Cisco devices to Cisco-specific SNMP traps defined by the CISCO-SYSLOG-MIB

(`enterprises.cisco.ciscoMgmt.ciscoCiscoMIB`) is also supported (such traps are also referred to as `clogMessageGenerated` notifications). That way, the incoming log messages can be forwarded to devices used to process and analyze Cisco-specific SNMP traps.

For details on using multithreading, see *Section 7.6, Sending SNMP traps* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*. For details on the Cisco-specific SNMP trap format, see *CISCO-SYSLOG-MIB* on the Cisco website.

5.4. Managing complex configurations

Version 4 F1 of syslog-ng PE offers several new features to simplify the maintenance of large configurations in heterogeneous environments.

- The syslog-ng PE application can automatically collect the system-specific log messages of the host on a number of platforms using the `system()` driver. For details, see *Section 6.11, Collecting the system-specific log messages of a platform* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- In syslog-ng PE version 4 F1, it is possible to define global variables in the configuration file. Global variables are actually `name-value` pairs; when syslog-ng processes the configuration file during startup, it automatically replaces `` `name` `` with `value`. The environmental variables of the host are automatically imported and can be used as global variables. For details, see *Section 5.4, Global and environmental variables* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- Parts (blocks) of a configuration file can be easily reused, you have to define the block (for example, a source) once, and you can reference it later. Any syslog-ng object can be a block, it is also possible to create blocks that contain multiple objects. Configuration blocks can receive arguments as well. Blocks are similar to C++ macros. For details, see *Section 5.7.2, Reusing configuration blocks* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

5.5. Improved decision making logic

Version 4 F1 of syslog-ng PE offers several new features that add new possibilities to processing messages and evaluating values only under certain conditions, improving the flexibility of syslog-ng PE.

- Macro values and templates can be compared as numerical and string values. String comparison is alphabetical: it determines if a string is alphabetically greater or equal to another string. You can also use boolean operators to combine comparison expressions. For details, see *Section 8.5.3, Comparing macro values in filters* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- Template functions allow you to modify the way macros or name-value pairs are expanded. Template functions can be used in template definitions, or when macros are used in the configuration of syslog-ng PE. For example, the `if` template function can include a different value in the log message based on its condition, while numerical template functions perform simple operations (like addition or multiplication) on integer numbers or macros containing integer numbers (for example, `$LEVEL_NUM` or `$YEAR`). For details, see *Section 13.1.6, Using template functions* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- Starting with 4 F1, it is possible to apply a rewrite rule to a message only if certain conditions are met. The `condition()` option effectively embeds a filter expression into the rewrite rule: the

message is modified only if the message passes the filter. For details, see *Section 13.2.4, Conditional rewrites* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

5.6. Message correlation, triggers, and other pattern database improvements

- Starting with version 4 F1, the syslog-ng PE application is able to correlate log messages identified using pattern databases.
  Log messages are supposed to describe events, but applications often separate information about a single event into different log messages. For example, the Postfix e-mail server logs the sender and recipient addresses into separate log messages, or in case of an unsuccessful login attempt, the OpenSSH server sends a log message about the authentication failure, and the reason of the failure in the next message.

  The syslog-ng PE application can correlate the identified messages and use all the information of the correlating messages, for example, to collect all important information about the event into a single log message. For details, see *Section 15.3, Correlating log messages* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

- The syslog-ng PE application is able to generate (trigger) messages automatically if certain events occur, for example, a specific log message is received, or the correlation timeout of a message expires. Basically, you can define messages for every pattern database rule that are emitted when a message matching the rule is received. Triggering messages is often used together with message correlation, but can also be used separately. For details, see *Section 15.4, Triggering actions for identified messages* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- It is now possible to specify multiple program patterns for a ruleset. For details, see the description of the `patterns` tag in *Section 15.5.3, The syslog-ng pattern database format* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.
- The <value> element of name-value pairs can include template functions. For details, see *Section 13.1.6, Using template functions* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*, for examples, see *Section if* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

6. Other changes

Released in syslog-ng Premium Edition 5.0.8:

- *New filter: netmask6()*
  Filter messages based on IPv6 addresses and subnets. For details, see *Section netmask6()* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

- *IPv6 not supported on Tru64*
  Starting from syslog-ng PE version 5.0.8, IPv6 is not supported on the Tru64 platform.

Released in syslog-ng Premium Edition 5 LTS:

- *New source option: use-syslog-ng-pid()*
  Override the PID value of the message with the PID of the running syslog-ng PE process.

- *New TLS option: cert-subject()*
  Use the specified certificate from the Windows Certificate Store. For details, see *Section 10.4, TLS options* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

- *New global option: custom-domain()*
  Use this option to specify a custom domain name that will be appended after the short hostname to receive the FQDN. For details, see *Section custom-domain()* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

- *New option for the udp() destination: spoof-interface()*
  On Microsoft Windows, use this option to specify the name of the interface that is used to send the spoofed messages.

- *New disk-buffer option: qout-size()*
  When using disk-based buffering, the number of messages stored in the output buffer of the destination can be specified.

- *New syslog-ng-ctl options: reload and stop*
  Reload and stop a running syslog-ng PE process.

- *Changes in template escaping*
  Escaping special characters used in templates has been changed and improved. For details, see *Section 13.1.2, Templates and macros* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

Released in syslog-ng Premium Edition 4 F2:

- *New hard macro: Unique receipt ID*
  A unique ID for messages generated at reception time on the receiving host. It facilitates defining relationships between messages that are potentially distributed to different files on the same host, or different hosts.

- *Installation path in .RUN installer*

The syslog-ng PE application can be installed to an alternative location. It can be useful if the user intends to install syslog-ng PE without registering it as a service, or if it cannot be installed to the default location because of policy compliance reasons.

- Starting with version 4 F2, the `lgstool cat` and `lgstool tail --filter` options are available.
- AIX 7.1 has been added to the list of supported platforms.
- *On-the-wire compression for TLS*
  Starting with version 4 F2 (4.2.2), on-the-wire compression can be enabled in TLS-encrypted communication to reduce the bandwidth usage of transporting log messages. For details, see the `allow-compress()` option in *Section 10.4, TLS options* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.

Released in syslog-ng Premium Edition 4 F1:

- The `log-fifo-size()` option can be set for logstore destinations as well. The default value of `log-fifo-size()` has been increased to 10000.
- The default value of `log-iw-size()` has been increased to 1000.
- New options called `ca-dir-layout()` and `cipher-suite()` options are available to specify the hash types and encryption parameters used in TLS connections. For details, see *Section 10.4, TLS options* in *The syslog-ng Premium Edition 5 LTS Administrator Guide*.