What is new in syslog-ng Premium Edition 5 F5

January 22, 2016

Table of Contents

1. Preface

Welcome to syslog-ng Premium Edition (syslog-ng PE) version 5 F5 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 F5.

This document covers the 5 F5 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 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. 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 ????.

3. Performance improvements for the Elasticsearch destination

The default values of the syslog-ng PE Elasticsearch destination have been optimized to increase performance. As a result, performance using the default values has increased, up to 100%.

- By default, syslog-ng PE now sends log messages to the Elasticsearch server in batches: the default value of the *`flush-limit()`* option has been increased from 1 to 5000.
- You can now send messages to the Elasticsearch server in multiple concurrent batches, significantly improve the performance. By default, syslog-ng PE uses two batches. For details, see *Section concurrent_requests()* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

Also, the `message-template()` option has been renamed to *`template()`* to be consistent with the syntax of other destinations. For details on sending log messages to Elasticsearch, see *Section 7.2, Sending messages directly to Elasticsearch* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

4. Simplified configuration syntax for Java-based destinations

The configuration syntax of the Elasticsearch, HDFS, and Apache Kafka destinations has been simplified, and now these destinations use the `option-name(option-value)` format, like other destinations of syslog-ng PE. If you are using these destinations, we recommend that you manually update your syslog-ng PE configuration file to use the new format. You can keep using the old format without any problems, but the documentation of syslog-ng PE will only include the new format from now on. For details, see *Section 7.2, Sending messages directly to Elasticsearch* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*, *Section 7.3, Storing messages on the Hadoop Distributed File System (HDFS)* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*, and *Section 7.4, Publishing messages to Apache Kafka* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

To illustrate the change, here is an old configuration of the Elasticsearch destination:

```
java(

class-path("/opt/syslog-ng/lib/syslog-ng/java-modules/*.jar:<path-to-preinstalled-elasticsearch-libraries>")

    class-name("org.syslog_ng.elasticsearch.ElasticSearchDestination")

    option("index", "syslog-ng_${YEAR}.${MONTH}.${DAY}")
    option("type", "test")
    option("cluster", "syslog-ng")
```

And here is a new one:

```
elasticsearch(
    index("syslog-ng_${YEAR}.${MONTH}.${DAY}")
    type("test")
    cluster("syslog-ng")
);
```

5. 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.

6. 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 5 F5 Administrator Guide*.

7. Support for new platforms

Version 5 F5 of syslog-ng Premium Edition supports the following new platforms:

- Debian 8 "jessie" (x86_64)
- SUSE Linux Enterprise Server (SLES) 12 (x86_64)

For a complete list of supported platforms, see *Section 1.6, Supported platforms* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

8. Unsupported platforms

Starting with syslog-ng Premium Edition version 5 F5, the following platforms are not officially supported:

- Windows 2003 Server

For a complete list of supported platforms, see *Section 1.6, Supported platforms* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

9. Upgrade notes

If you are using custom configuration blocks that have arguments, you have to manually update your configuration file before upgrading syslog-ng PE. When you reference the received argument in the block, make sure that the referenced argument is enclosed only between backticks, and not between quotes or double-quotes. For example, this is correct: `` host(`host`) ``, but this is incorrect: `` host("`host`") port('`port`') ``. Remove the quotes before upgrading, otherwise syslog-ng PE will not start (syntax error in the cofiguration file).

For details on configuration blocks, see *Section 5.7.2.1, Passing arguments to configuration blocks* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.

10. Other changes

- 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 5 F5 Administrator Guide*.
- To simplify debugging and troubleshooting, the `syslog-debun` utility now supports the FreeBSD and HP-UX platforms. For details, see *syslog-debun(1)* in *The syslog-ng Premium Edition 5 F5 Administrator Guide*.