Centreon Syslog Server Documentation

Release 1.2.5

Laurent Pinsivy

December 09, 2016

centreon 12, avenue Raspail – 94250 Gentilly – France
tél +33 (0)1 49 69 97 12 fax +33 (0)1 78 12 00 28 mail contact@centreon.com
SAS au capital de 500 000 € – 483 494 589 RCS Créteil – TVA FR 02 483 494 589
www.centreon.com

The Centreon Syslog project consists of several parts:

- Centreon Syslog Frontend
- Centreon Syslog Server

The Centreon Syslog Frontend module is the graphic user interface of the project Centreon Syslog for Centreon local server. This interface allows to configure different Centreon Syslog Server modules as well as to view the syslog events collected by the latter modules. Besides viewing in real time syslog events of the collectors, the Centreon Syslog Frontend module also allows to make a search on past events.

The Centreon Syslog Server allows to manage syslog events stored into MySQL database by Syslog daemon (Rsyslog, Syslog-ng)

The Centreon Syslog CLAPI module allows you to extract recorded syslog events from databases to CSV, XML or ODT format. The extraction made from Centreon server is stored in command line format.

Note: It is important to note that this version no longer requires “php-syslog-ng” although it was required for the “Syslog 1.1” version.

This documentation will explain to you how to install and manage a Centreon Syslog Server:

CHAPTER 1

Installation

This documentation describes the installation using RPM for Centreon Enterprise Server (CES) and from sources:

1.1 Downloads

1.1.1 Formats

Generally speaking, Open Source softwares by Merethis are provided in three possible formats:

- binary RPM packages (recommended)
- tarballs with sources
- Subversion git/repository

RPM packages are the best format you can get as you would not have to worry about compilation and installation, everything is already made by Merethis' experts.

If your platform is not currently supported by RPMs you might consider using tarball sources which are always provided for stable release. However, compilation has to be done manually and it can be cumbersome in some situations.

The Git/Subversion repositories is for developers or beta-testers only. No official support is provided on them as they are most likely still under development.

For any help you can use the Centreon Syslog section from Centreon forum to have community support.

1.1.2 Centreon Syslog Server

Tarballs: http://forge.centreon.com/projects/centreon-syslog/files

Git: http://git.centreon.com/centreon-syslog

Old Subversion repository: http://svn.modules.centreon.com/centreon-syslog

1.2 Using packages

Merethis provides RPM for its products through Centreon Entreprise Server (CES). Open source products are available for free from our repository.

These packages have been successfully tested with CentOS 5 and RedHat 5.

1.2.1 Prerequisites

In order to use RPM from the CES repository, you have to install the appropriate repo file. Run the following command as privileged user:

```
$ wget http://yum.centreon.com/standard/ces-standard.repo -O /etc/yum.repos.d/ces-standard.repo
```

The repo file is now installed.

1.2.2 Installation

Use following documentation to install the module

Centreon Syslog Server

The centreon Syslog Server allows to store syslog event into MySQL database.

It can be install on the central server or as a distant collector.

Run the following command as privileged user:

```
$ yum install centreon-syslog-server
```

YUM suggests then installing the latest version of the package:

```
================================================================================================
 Package                    Arch          Version          Repository                        S
================================================================================================
Installing:
 centreon-syslog-server     noarch        1.2.3-1          ces-standard                      1

Transaction Summary
================================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 14 k
Is this ok [y/N]: y
```

Enter ‘y’ and press ENTER key to install package on your server.

YUM downloads the package and installs the latter:

```
Installed:
  centreon-syslog-server.noarch 0:1.2.3-1

Complete!
```

The package centreon-syslog-server is now installed on your server.

If you have install the package centreon-syslog-server in a distant poller it is necessary to create a MySQL account. Indeed the Centreon server must be able to reach the database MySQL of your poller. Run the following commands on your poller:

```
$ mysql -u root -p
mysql> GRANT SELECT ON centreon_syslog.* TO centreon@'<IP>' IDENTIFIED BY '<PASSWORD>';
mysql> FLUSH PRIVILEGES;
mysql> quit;
```

Notice: replace <IP> address by the Centreon main server IP address and <PASSWORD> by your password.

To configure the module, see *Configuration*

1.3 Using sources

Centreon Syslog Team provides sources package.

These packages have been successfully tested with CentOS/RedHat 5.x, Debian 5.x and Ubuntu 10.x.

1.3.1 Prerequisites

Before start to install Centreon Syslog Server module you need the follwing packages:

- Rsyslog >= v3.22.x
- Rsyslog-mysql >= 3.22.x
- MySQL >= v5.x running
- PHP & PHP-CLI >= 5.1.x
- PHP-MySQL module loaded
- Pear-DB >= 1.7.14

Get latest version from http://forge.centreon.com/projects/centreon-syslog/files or from http://svn.modules.centreon.com/centreon-syslog/tags

Warning: If all prerequires are not installed the installation process will failed.

1.3.2 Installation

Use following documentation to install the module:

Centreon Syslog Server

The centreon Syslog Server allows to store syslog event into MySQL database.

It can be install on the central server or as a distant collector.

Extract sources

Copy the tarball into '/tmp' directory and run the following commands:

```
$ tar xzf centreon-syslog-server-1.2.3.tar.gz
$ cd centreon-syslog-server-1.2.3
$ dos2unix install.sh libinstall/*
```

Install module

Start installation using following command:

```
$ bash install.sh -i

################################################################################
#                                                                              #
#           http://forge.centreon.com/projects/show/centreon-syslog            #
#                           Thanks for using Centreon                          #
#                                                                              #
#                                    v1.2.3                                    #
#                                                                              #
################################################################################
------------------------------------------------------------------------
        Checking all needed binaries
------------------------------------------------------------------------
rm                                                              OK
cp                                                              OK
mv                                                              OK
/bin/chmod                                                      OK
/bin/chown                                                      OK
echo                                                            OK
more                                                            OK
mkdir                                                           OK
find                                                            OK
/bin/grep                                                       OK
/bin/cat                                                        OK
/bin/sed                                                        OK
groupadd                                                        OK
useradd                                                         OK

You will now read Centreon Syslog module Licence.
        Press enter to continue.
```

Press ENTER key and accept GPL v2 licence:

```
Do you accept GPL license ?
[y/n], default to [n]:
> y
```

For the server module to function properly, a user is created. This user will be the user specified the cron jobs. The installation script will offer to create this user if it is not detected. The installation is aborted if the user is not created:

```
------------------------------------------------------------------------
        Checking syslog group and user
------------------------------------------------------------------------
Cannot find user: syslog                                        FAIL

Do you want to create this user
[y/n], default to [n]:
> y

Create user: syslog                                             OK
```

Notice: No password has been defined for the 'syslog' user. To work correctly, the Centreon Syslog Frontend module needs to connect to syslog server via SSH. This is true even if the client and the server are the same machine. That is why we must set a SHELL password for the new 'syslog' user.

The installation script checks prerequires:

```
------------------------------------------------------------------------
        Checking binaries and processus
------------------------------------------------------------------------
Mysql is running:                                                  OK
PHP version: 5.1.6                                                 OK
Pear-DB version: 1.7.14                                            OK
PHP MySQL module:                                                  OK
```

Define prefix directory for installation:

```
------------------------------------------------------------------------
        Get directories for installation
------------------------------------------------------------------------

Where do you want to install files ?
default to [/usr/bin/syslog]
> /usr/local/centreon-syslog

Do you want me to create this directory ? [/usr/local/centreon-syslog]
[y/n], default to [n]:
> y
```

Define location of logs files:

```
Where would you like to store your logs ?
default to [/usr/local/centreon-syslog/logs]
>

Do you want me to create this directory ? [/usr/local/centreon-syslog/logs]
[y/n], default to [n]:
> y
```

Define location of configuration files:

```
Where would you like to store configuration ?
default to [/usr/local/centreon-syslog/etc]
>

Do you want me to create this directory ? [/usr/local/centreon-syslog/etc]
[y/n], default to [n]:
> y
```

If you don't have MySQL root password press ENTER key:

```
------------------------------------------------------------------------
        Create syslog Database
------------------------------------------------------------------------
What is password for root user on MySQL ?
>
```

Define name of Centreon Syslog Server database:

```
What is the database name to record syslog message ? default to [syslog]
> centreon_syslog

Do you want me to create this database ? [centreon_syslog]
[y/n], default to [n]:
> y

Creating database centreon_syslog:                          OK
```

Define size of ‘program’ field for ‘logs’ table (30):

```
Which must be the size of the field "program", default to [15]:
> 30
```

Press ENTER key to create first ‘logs’ table:

```
Do you want me to create this table "logs" in "centreon_syslog" database ?
[y/n], default to [n]:
> y

Creating table logs:                                    OK
```

Create local MySQL account for the module:

```
Creation of local db user for cron

Do you want me to create user 'syslogadmin'@'localhost' ?
[y/n], default to [n]:
> y

Create user 'syslogadmin'@'localhost':                  OK
```

Add password for local MySQL account:

```
Do you want to add password for this user: 'syslogadmin'@'localhost'
[y/n], default to [y]:
> y

Enter password for dbuser
> syslogpasswd

Retype password for dbuser
> syslogpasswd

Add password for user 'syslogadmin'@'localhost':        OK
```

Create distant MySQL account for Centreon main server:

```
Creation of distant db user for cron

What is IP address of Centreon server ?
> 10.30.2.164

Do you want me to create user 'syslogadmin'@'10.30.2.164' ?
[y/n], default to [n]:
> y

Create user 'syslogadmin'@'10.30.2.164':                OK

Do you want to add password for this user: 'syslogadmin'@'10.30.2.164'
[y/n], default to [y]:
> y

Enter password for dbuser
> syslogpasswd

Retype password for dbuser
> syslogpasswd
```

```
Add password for user 'syslogadmin'@'10.30.2.164':          OK
```

Note: if the database is on the same server tha n Centreon main server, you must specify the external IP address of the server.

The installation script install the Centreon Syslog Server module on your plateform:

```
------------------------------------------------------------------------
        Install Syslog Cron
------------------------------------------------------------------------
Generation of the new Syslog cron:                          OK
Change of the macros in the files:                          OK
Application of the rights on the files:                     OK
Change of the owners on the files:                          OK
Removal of the old Syslog cron:                             OK
Copy php cron files:                                        OK
Copy cron in cron.d directory:                              OK
Erase temporay installation directory:                      OK

------------------------------------------------------------------------
        Create log rotation file
------------------------------------------------------------------------

Create log rotate file: /etc/logrotate.d//centreon-syslog  OK

------------------------------------------------------------------------
        Create syslog configuration files
------------------------------------------------------------------------

Create syslog configuration file: syslog_conf.pm            OK
Create php syslog configuration file: /usr/local/centreon-sOKlog/etc/syslog.conf.php
Set rigths on : /usr/local/centreon-syslog/etc/syslog.conf.OKp

------------------------------------------------------------------------
        Update database
------------------------------------------------------------------------

No update available:                                        PASSED

------------------------------------------------------------------------
        End of installation
------------------------------------------------------------------------

Installation is complete !                                  OK


################################################################################
#                                                                              #
#      Report bugs at                                                          #
#           http://forge.centreon.com/projects/centreon-syslog/issues/new      #
#                                                                              #
################################################################################
```

Your module is installed

Note: the installer creates a “syslog_conf.php” file in the “etc” directory. This file will be used for updates without asking any questions.

To configure the module, see *Configuration*

MERETHIS 12 AVENUE RASPAIL FR94290 GENTILLY

www.centreon.com

CHAPTER 2

Configuration

This chapter describes the functioning of the module as well as the configuration of the latter.

2.1 Configuration files

The configuration directory of Centreon Syslog Server is '/etc/centreon-syslog/'.

This directory includes:

- syslog.conf.php
- syslog.conf.pm

This files are used by a PHP cron scripts to manage "centreon_syslog" database.

The file /etc/centreon-syslog/syslog.conf.php can be generate from Centreon Syslog Frontend GUI. Please use frontend GUI to modify parameters and export those. If you modify manually this file, it can be overwrite by GUI.

2.2 Database functioning

The Centeon Syslog Server database generates every day two tables:

- cache
- logs

Every morning the PHP cron script '/usr/share/centreon-syslog/cron/tableLogRotate.php' moves tables 'cache' and 'logs' to 'cacheYYYMMDD' and 'logsYYYMMDD'. The 'logs' table includes only Syslog event of the actuel day. This table is used by Centreon Syslog Frontend real monitoring page to display events. The 'cache' table contains information generated by the PHP cron script '/usr/share/centreon-syslog/cron/reloadCache.php'.

This table is used by Centreon Syslog Frontend real monitoring page to display available filters for hosts, severity, facility, program, etc. A MySQL MERGE tables allow to group all 'cache' and 'logs' tables to 'all_cache' and 'all_logs'. These MySQL tables are used by Centreon Syslog Frontend search page.

Besides tables 'cache', ' logs ', ' all_cache ' and ' all_logs ' a table 'instance' allows to know the state of execution of cron.

2.3 Syslog events and database

The Centreon Syslog Server module uses dependences to 'rsyslog' and 'rsyslog-mysql' packages and modify original rsyslog configuration file ('/etc/rsyslog.conf') to insert Syslog events into 'centreon_syslog' database:

```
$ModLoad imtcp.so  # load module
$ModLoad imudp.so  # provides UDP syslog reception
$UDPServerRun 514 # start a UDP syslog server at standard port 514

...

$template sysMysql,"INSERT INTO logs (host,facility, priority,level,tag,datetime,program,msg) VALUES
*.* >127.0.0.1,centreon_syslog,centreon_syslog,mvh29123;sysMysql
```

The first three lines allow to accept Syslog evetns from TCP and UDP protocol on port 514. The last two lines describe how to insert events into database and parameters to connect to 'centreon_syslog' database (IP;database name;user;password;). Please sse http://www.rsyslog.com/doc/manual.html for more information.

2.4 Cron functioning

The definition of the PHP cron scripts is defined in the file '/etc/cron.d/centreon-syslog':

```
*/2 * * * * syslog php -q /usr/share/centreon-syslog/cron/reloadCache.php >> /var/log/centreon-syslog
59 23 * * * syslog php -q /usr/share/centreon-syslog/cron/tableLogRotate.php >> /var/log/centreon-sys
```

The script 'reloadCache.php' generates every 2 minutes real monotirring filters using information from 'logs' table.

The script 'tableLogRotate.php' rotates every night 'cache' and 'logs' tables to 'cacheYYYMMDD' and 'logsYYYMMDD'. Moreover this script delete old 'cacheYYYMMDD' and 'logsYYYMMDD' tables using retention day defined in '/etc/centreon-syslog/syslog.conf.php' file.

2.5 Retention of data

The '$syslogOpt["syslog_db_rotate"]' parameter defined in '/etc/centreon-syslog/syslog.conf.php' file describes the duration in days of retention of the Syslog events in 'centreon_syslog' database.

Notice: you must configure retention days fron Centreon Syslog Frontend GUI and export configuration to the Centreon Syslog Server.

2.6 Log of PHP scripts

The logs of the PHP scripts are available in the directory '/var/log/centreon-syslog'. A logrotate definition can be write into '/etc/logrotate.d/centreon-syslog' with following lines:

```
/var/log/centreon-syslog/*log {
      compress
      daily
      notifempty
      missingok
      rotate 7
      size 100M
}
```