Centreon

# CENTREON SYSLOG SERVER MODULE

# INSTALLATION MANUAL

*Author: Laurent Pinsivy*
*Translation by: Michael Joyner (Centreon Community)*

MERETHIS COMPAGNY

12 Avenue Raspail – 94250 Gentilly - France

Phone: 01.49.69.97.12 - Fax: 01.78.12.00.28

Merethis

# Table of contents

# 1. DESCRIPTION

The Centreon Syslog module consists of two parts :

- The server ,
- The presentation, or viewing the Syslog events .

The Centreon module, « Centreon-syslog-frontend » not only allows you to view the syslog but it is also an interface to search and filter syslog events. Syslog events is saved into a database and this is managed by the module « centreon-syslog-server ».

The "centreon-syslog-server" module allows you to maintain the events recorded in the database. These events are inserted by syslog-ng, rsyslog or other syslog daemon.

It is important to note that this version no longer requires "php-syslog-ng". The was previously required for the "Syslog 1.1" version and is no longer necessary.

## 1.1. PREREQUISITES

The list of requirements necessary for the « centreon-syslog-server » installation script is: :

- MySQL-Server ;
- PHP4 or superior ;
- PEAR-DB.

## 1.2. INSTALLATION

There are two parts to installing the « centreon-syslog-server » module :

- Installing the module ;
- Configuring the syslog daemon .

The first step described first time installations as well as version updating. The second chapter covers installation and configuration of the syslog daemon.

# 2. INSTALLATION

## 2.1. FIRST TIME INSTALLATION

Installation of the « centreon-syslog-server » is ran from the shell script : « install.sh ». It must be installed as the root user to run. The script will ask for confirmation before it installs any files.

You can obtain the latest version from the « Centreon-Syslog » module on the http://forge.centreon.com site download page. You will need to create a forge account to access the site.

Unzip the archive and move in the folder :

```
$> tar xzf centreon-syslog-server-1.2.1.tgz
$> cd  centreon-syslog-server-1.2.1
```

### 2.1.1. ACCEPTING THE GPL V2 LICENCE

Start the installation and accept the GPL v2 :

```
$> bash install.sh -i

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

### 2.1.2. CHECKING « SYSLOG » USER

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.

**Note :** No password has been defined for the user « syslog ». To work correctly, the « centreon-syslog-frontend » 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.

```
------------------------------------------------------------------------
        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
```

### 2.1.3. CHECKING FOR DEPENDENCIES

If at least one of the dependencies is not present the installer will finish and show the missing dependency. We must then install this dependency and then restart the installation script over again.

```
------------------------------------------------------------------------
        Checking binaries and processus
------------------------------------------------------------------------
Mysql is running:                                          OK
PHP version: 5.1.6                                         OK
PEAR-DB version: 1.7.13                                    OK
```

### 2.1.4. CREATION OF THE INSTALLATION DIRECTORIES

The installer provides default directories that you can change them to meet your needs. If these directories are missing, the installer will ask to create them with appropriate rights to the directories. If you answer no, the installation process will be aborted.

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

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

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

Where would you like to store your logs ?
default to [/usr/bin/syslog/logs]
>

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

Where would you like to store configuration ?
default to [/usr/bin/syslog/etc]
>

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

Once the directories are defined, the installer copies will copy the files.

```
------------------------------------------------------------------------
        Install Syslog Cron
------------------------------------------------------------------------
Removal of the old Syslog cron:                            OK
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
Directory /usr/bin/syslog/logs already exists
Creation of the repertory for the logs:                    PASSED
Removal of the old Syslog cron:                            OK
Copy php cron files:                                       OK
Copy cron in cron.d directory:                             OK
Erase temporay installation directory:                     OK
```

### 2.1.5. DATABASE CREATION FOR « SYSLOG »

The installer checks whether the « syslog » database is already on your machine, if it is found then the installation is complete. Otherwise, the installer will ask to create the associated database tables as well as the users.

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

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

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

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

Creating table logs:                                      OK

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

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

Enter password for dbuser
> your_password

Retype password for dbuser
> your_password

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

Creation of distant db user for cron
```

**Note :** If the database server is on the same server then the Centreon server, you must specify the external IP address of server.

```
What is IP address of Centreon server ?
> 192.168.1.51

Do you want me to create user 'syslogadmin'@'192.168.1.51' ?

[y/n], default to [n]:
> y

Create user 'syslogadmin'@'192.168.1.51':                  OK

Do you want to add password for this user: 'syslogadmin'@'192.168.1.51'
[y/n], default to [y]:
> y

Enter password for dbuser
> syslogadmin

Retype password for dbuser
> syslogadmin

Add password for user 'syslogadmin'@'192.168.1.51':        OK
```

After creating the database and entering the user information, the installer creates a « syslog_conf.pm » file in the directory « /etc ». This file updates without asking any questions.

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

Create syslog configuration file: syslog_conf.pm           OK
Create php syslog configuration file: /usr/bin/syslog/etc/sOKlog.conf.php

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

Update from 1.0 to 1.1:                                    OK

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

Installation is complete !                                 OK


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

## 2.2. UPGRADING FROM A PREVIOUS VERSION

### 2.2.1. UPGRADING FROM « SYSLOG 1.0 »

Upgrading from "Syslog" version 1.0 is not supported directly. You must download the « Syslog 1.1 »version and then update.

### 2.2.2. UPGRADING FROM « SYSLOG 1.1 »

There have been many changes made to the « syslog » database structure.

Previously only the « logs » table was getting a daily rotation. However, for those who were using the « search_cache_syslog » table, it was cached every 2 minutes by cron job. This cache was calculated on the « all_logs » table ( i.e., on all « log »" tables on the « syslog » database ).

This consumed too many CPU and memory resources. In order to decrease CPU resources during this calculation, the table « cache » (formerly « search_cache_syslog ») is made a daily cron job as to rotate the data. The table « cache » will therefore be calculated on the current « logs » table and the interface will go seek this information on the new table « all_cache » which includes the « cache » tables.

To make your old database compatible with the new module, an additional script needs to be run. It creates daily « cache » tables from then daily table « logs ». Then a « all_cache » table is created.

To allow this to happen it is essential to stop the « crond » service used by the module « centreon-syslog-server ». You will need to comment out two rows in the « /etc/cron.d/centreon-syslog » file by adding the symbol « # » at the beginning of line and then restart the service « crond ».

Editing the file :

```
$> vim /etc/cron.d/centreon-syslog
```

Comment out the required lines :

```
#*/2 * * * * syslog php -q /usr/bin/syslog/reloadcache.php >> /usr/bin/syslog/logs/reloadcache.log
#59 23 * * * syslog php -q /usr/bin/syslog/tableLogRotate.php >> /usr/bin/syslog/logs/SyslogRotation.log
```

Restart the « crond » service :

```
$> /etc/init.d/crond restart
```

Modify the « syslog » database update script :

```
$> cd  DB_UPGRADE
$> vim upgrade_syslog_database.php
```

Update the database connection information :

```
$syslogDB = array(
                    'phptype'  => 'mysql',
                    'username' => "syslog_server_db_user",
                    'password' => "syslog_server_db_password",
                    'hostspec' => "syslog_server",
                    'database' => "syslog_db",
                );
```

Once you update your changes run the script. The operation may take some time depending on the number of records in table « logsxxxxxxxx ». It might consume some CPU and Memory during process.

Run the script :

```
$> php upgrade_syslog_database.php
```

After the script executes we will want to :

- Remove comments « # » in file « /etc/cron.d/syslog-centreon » previously inserted ;
- Restart the « crond » service .

The script will display its progress in this way :

```
BEGIN UPGRADE FOR SYSLOG DATABASE AT 2009-07-27 13:13:40
Try to connect to syslog database at2009-07-27 13:13:40
Connection successful
Get names of all logs table
Get names of all logs tables complete
Table cache20090711 created
Create table cache20090712 at 2009-07-27 13:19:46
Table cache20090712 created
Create table cache20090713 at 2009-07-27 13:19:53
Table cache20090713 created
Create table cache20090714 at 2009-07-27 13:20:01
Table cache20090714 created
Create table cache20090715 at 2009-07-27 13:20:11
Table cache20090715 created
Drop table all_cache
Table all_cache created
FINISH UPGRADE FOR SYSLOG DATABASE AT 2009-07-27 13:20:18
```

The following error is encountered, to change allowed for the execution of PHP memory space :

```
PHP Fatal error:  Allowed memory size of 134217728 bytes exhausted (tried to allocate 76 bytes) in
/usr/share/pear/PEAR.php on line 872
```

To fix this edit the php.ini file and change the block next to the « memory_limit » filed :

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

max_execution_time = 30     ; Maximum execution time of each script, in seconds
max_input_time = 60 ; Maximum amount of time each script may spend parsing request data
memory_limit = 128M      ; Maximum amount of memory a script may consume
```

**Note** : For a table of about 950,000 records, the PHP memory limit must be 256M.

# 3. INSTALLATION AND CONFIGURATION OF SYSLOG DAEMON

## 3.1. SYSLOG-NG

Install the following package.

```
$> apt-get install syslog-ng
```

Edit the configuration file syslog-ng.conf :

```
$> emacs /etc/syslog-ng/syslog-ng.conf
```

And paste these lines to the end of the file :

```
source s_everything { internal(); pipe("/proc/kmsg"); unix-stream("/dev/log"); udp(); };

destination d_mysql {
      program("/usr/bin/mysql --user=DB_USER --password=DB_PASSWORD DATABASE"
      template("INSERT INTO logs (host, facility, priority, level, tag, datetime, program, msg)
      VALUES ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG', '$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC',
'$PROGRAM', '$MSG' );\n")
       template-escape(yes));
};

log {source(s_everything); destination(d_mysql);};
```

Please change username and password for MySQL database :

```
/usr/bin/mysql --user=DB_USER --password=DB_PASSWORD DATABASE
```

### 3.2. RSYSLOG

Install the following package :

```
$> apt-get install rsyslog rsyslog-mysql
```

Edit the configuration file rsyslog.conf :

```
$> vim /etc/rsyslog.conf
```

And paste these lines at the beginning of the file :

```
$ModLoad MySQL

$AllowedSender UDP, 127.0.0.1, 192.168.1.0/24
$AllowedSender TCP, 127.0.0.1, 192.168.1.0/24
```

Change network 1**92.168.1.0/24** to your network.

And then paste these lines at the end of the file:

```
# Configuration changes for Windows/Snare/Centreon-E2S logs
$EscapeControlCharactersOnReceive off


$template sysMysql,"INSERT INTO logs (host,facility, priority,level,tag,datetime,program,msg) VALUES
('%HOSTNAME%','%syslogfacility%','%syslogpriority%','%syslogseverity%','%syslogtag%',
'%timereported:::date-mysql%','%programname%', '%msg:::space-cc%')", SQL

*.* >IP_SERVEUR_DB,DB_NAME,BD_USER,DB_PASSWORD;sysMysql
```

The following bloc is just **one line**:

```
$template sysMysql,"INSERT INTO logs (host,facility, priority,level,tag,datetime,program,msg) VALUES
('%HOSTNAME%','%syslogfacility%','%syslogpriority%','%syslogseverity%','%syslogtag%',
'%timereported:::date-mysql%','%programname%', '%msg:::space-cc%')", SQL
```

Change **IP_SERVEUR_DB, DB_NAME, BD_USER et DB_PASSWORD** to your information.

For more clarity in the « centreon-syslog-frontend » module it is possible to replace the macro %syslogpriority% and %syslogseverity% respectively by %syslogpriority-text% and %syslogseverity-text%. For example you can replace the numbers 1,2, or 3 with the text instead like « Emergency », « Critical » or « Warning ».

Edit the file "rsyslog" to receive syslog events, also listen on UDP TCP on port 514 :

```
$> vim /etc/sysconfig/rsyslog
```

Replace the line:

```
SYSLOGD_OPTIONS="-m 0"
```

By this line:

```
SYSLOGD_OPTIONS="-r514 -t514 -m 0"
```

Restart the syslog daemon :

```
$> /etc/init.d/rsyslog start
```