Centreon Syslog Frontend Documentation

Release 1.5.0

Laurent Pinsivy

December 09, 2016

The Centreon Syslog project consists of several parts:

- Centreon Syslog Frontend
- Centreon Syslog Server
- Centreon Syslog CLAPI

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, use and manage a Centreon Syslog Frontend:

CHAPTER 1

Installation

This documentation describes 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 Git/Subversion repositories

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.

CES 2.2

Run the following command as privileged user:

```
$ wget http://yum.centreon.com/standard/2.2/ces-standard.repo -O /etc/yum.repos.d/ces-standard.repo
```

The repo file is now installed.

CES 3.0

Run the following command as privileged user:

```
$ wget http://yum.centreon.com/standard/3.0/stable/ces-standard.repo -O /etc/yum.repos.d/ces-standard
```

The repo file is now installed.

1.2.2 Installation

Use following documentation to install the module

Centreon Syslog Frontend

The centreon Syslog Frontend is the graphical user interface for Centreon main server.

Run the following command as privileged user:

```
$ yum install centreon-syslog-frontend
```

YUM suggests the installation of the latest version of the packages:

```
================================================================================================
 Package                        Arch        Version               Repository
================================================================================================
Installing:
 centreon-syslog-frontend       noarch      1.5.0-1               ces-standard-noarch
Installing for dependencies:
 libssh2                        x86_64      1.2.9-1.el5.rf        rpmforge
 ssh2                           x86_64      0.11.0-3              ces-standard-deps

Transaction Summary
================================================================================================
Install       3 Package(s)
Upgrade       0 Package(s)

Total download size: 494 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-frontend.noarch 0:1.5.0-1

Dependency Installed:
  libssh2.x86_64 0:1.2.9-1.el5.rf                          ssh2.x86_64 0:0.11.0-3

Complete!
```

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

Note: To conclude installation, see *Web installation*

1.3 Using sources

Centreon Syslog Team provides source packages.

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

1.3.1 Prerequisites

Before starting to install Centreon Syslog Frontend module you need the follwing packages:

- Centreon 2.2.x, 2.3.x, 2.4.x
- libssh2 >= 1.2.1
- ssh2 >= 0.11.0

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

---

Note: See *Installation of prerequisites* to install libssh2 and ssh2

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

1.3.2 Installation

Use following documentation to install the module:

Installation of prerequisites

This section describes how to install prerequisites for Centreon Syslog Frontend from sources.

Installation for Debian / Ubuntu

This section describes the installation of libssh2 for Debian / Ubuntu operating system.

Prerequisites Here is the list of packages to be pre-installed:

- php5-dev
- openssl
- libssl-dev
- gcc
- make

Also, update the packages:

```
$ apt-get update
$ apt-get upgrade
```

Create the working directory Create the working directory:

```
$ cd /tmp
$ mkdir libssh2
$ cd libssh2
```

Download the packages:

```
$ wget http://www.libssh2.org/download/libssh2-1.2.1.tar.gz
$ wget http://pecl.php.net/get/ssh2-0.11.0.tgz
```

Installation of libssh2 Run the following commands:

```
$ tar -xzvf libssh2-1.2.1.tar.gz
$ cd libssh2-1.2.1
$ ./configure && make all install
```

The installation of libssh2 is finished.

Installation of ssh2 Run the following commands:

```
$ tar -xzvf ssh2-0.11.0.tgz
$ cd ssh2-0.11.0
$ phpize && ./configure --with-ssh2 && make
```

To finish the installation, copy the ssh2.so file to the directory for the PHP extensions. This directory can be different depending on your Linux distribution and PHP build:

```
$ cp modules/ssh2.so /usr/lib/php5/20060613+lfs
```

The installation of ssh2 is finished.

Note: if your version of PHP is 5.3 you can have a bug, please see http://pecl.php.net/bugs/bug.php?id=16727

Integration of the extension SSH into Apache Run the following commands:

```
$ echo "extension=ssh2.so" > /etc/php5/cli/conf.d/ssh2.ini
$ echo "extension=ssh2.so" > /etc/php5/apache2/conf.d/ssh2.ini
```

Then restart Apache to apply modification:

```
$ /etc/init.d/apache2 restart
```

To check if SSH2 library is correctly installed you can run the following command:

```
$ php -i |grep ssh
Registered PHP Streams => php, file, http, ftp, compress.bzip2, compress.zlib, https, ftps, ssh2.shel
ssh2
libssh2 version => 1.1
banner => SSH-2.0-libssh2_1.1
```

Installation for Redhat / CentOS

This section describes the installation of libssh2 for Redhat / CentOS operating system.

Prerequisites Here is the list of packages to be pre-installed:

- php5-dev
- php-devel
- openssl
- openssl-devel
- libssl-dev
- gcc
- make

Also, update the packages:

```
$ yum update
$ yum upgrade
```

Create the working directory Create the working directory:

```
$ cd /tmp
$ mkdir libssh2
$ cd libssh2
```

Download the packages:

```
$ wget http://www.libssh2.org/download/libssh2-1.2.1.tar.gz
$ wget http://pecl.php.net/get/ssh2-0.11.0.tgz
```

Installation of libssh2 Run the following commands:

```
$ tar -xzvf libssh2-1.2.1.tar.gz
$ cd libssh2-1.2.1
$ ./configure && make all install
```

The installation of libssh2 is finished.

Installation of ssh2 Run the following commands:

```
$ tar -xzvf ssh2-0.11.0.tgz
$ cd ssh2-0.11.0
$ phpize && ./configure --with-ssh2 && make
```

To finish the installation, copy the ssh2.so file to the directory for the PHP extensions. This directory can be different depending on your Linux distribution:

```
$ cd modules
```

For 32 bits operating system:

```
$ cp -R ssh2.so /usr/lib/php/modules
```

For 64 bits operating system:

```
$ cp -R ssh2.so /usr/lib64/php/modules
```

The installation of ssh2 is finished.

Integration of the extension SSH into Apache Run the following command:

```
$ echo "extension=ssh2.so" >> /etc/php.ini
```

Then restart Apache to apply modification:

```
$ /etc/init.d/httpd restart
```

To control if SSH2 library is correctly installed you can run the following command:

```
$ php -i |grep ssh
Registered PHP Streams => php, file, http, ftp, compress.bzip2, compress.zlib, https, ftps, ssh2.shel
ssh2
libssh2 version => 1.1
banner => SSH-2.0-libssh2_1.1
```

Centreon Syslog Frontend

The centreon Syslog Frontend is the graphical user interface for Centreon main server.

> **Warning:** If one of the following action failed the installation failed too. You must correct failed before restart installation process.

Extract sources

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

```
$ tar xzf centreon-syslog-frontend-1.5.0.tar.gz
$ cd centreon-syslog-frontend-1.5.0
$ dos2unix install.sh libinstall/*
```

Install module

Start installation using following command:

```
$ bash install.sh -u /etc/centreon

################################################################################
#                                                                              #
#                  Thanks for using Centreon Syslog Frontend                   #
#                                  v 1.5.0                                     #
#                                                                              #
################################################################################
------------------------------------------------------------------------
        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
Parameters was loaded with success                              OK

------------------------------------------------------------------------
        Update Module Name
------------------------------------------------------------------------
Update module name "Syslog" to "centreon-syslog":               OK

------------------------------------------------------------------------
        Checking php extension
------------------------------------------------------------------------
SSH2 extension for PHP:                                         OK
XML-Writer extension for PHP:                                   OK

------------------------------------------------------------------------
        Install Centreon Syslog Frontend web interface
------------------------------------------------------------------------
Changing macros                                                 OK
Setting right                                                   OK
Setting owner/group                                             OK
```

Todo

finir capture shell

Your module is installed

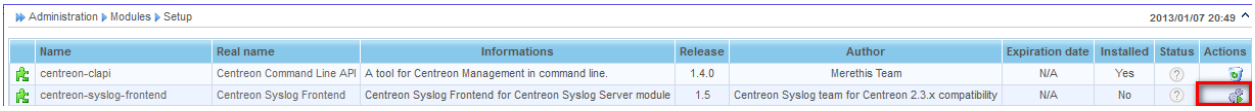
Notice: replace "/etc/centreon" directory by the "etc" directy of Centreon of your installation. The installation will use parameters of Centreon installation to install this module.

Note: To finish installation, see *Web installation*

1.4 Web installation

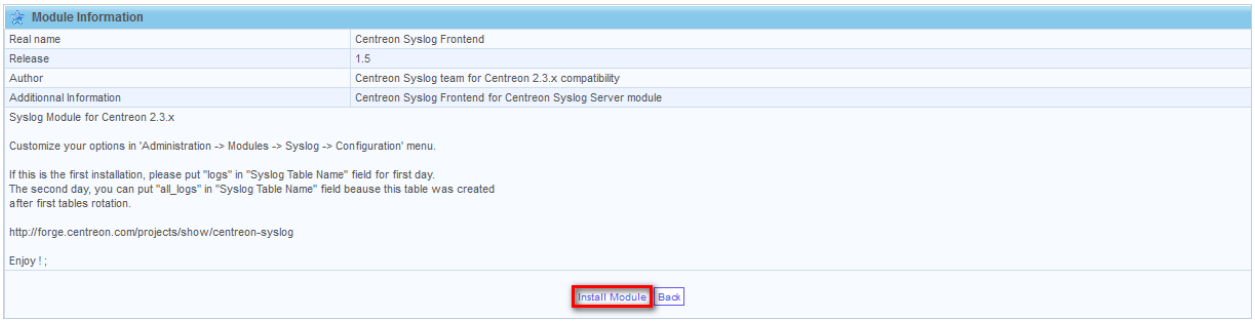
Go to web interface of Centreon then navigate to the menu “Administration -> Modules -> Setup”.

A line should reference the Centreon Syslog Frontend module but it is not installed yet. To complete the installation, click on the icon located right on the line as shown by the red box:

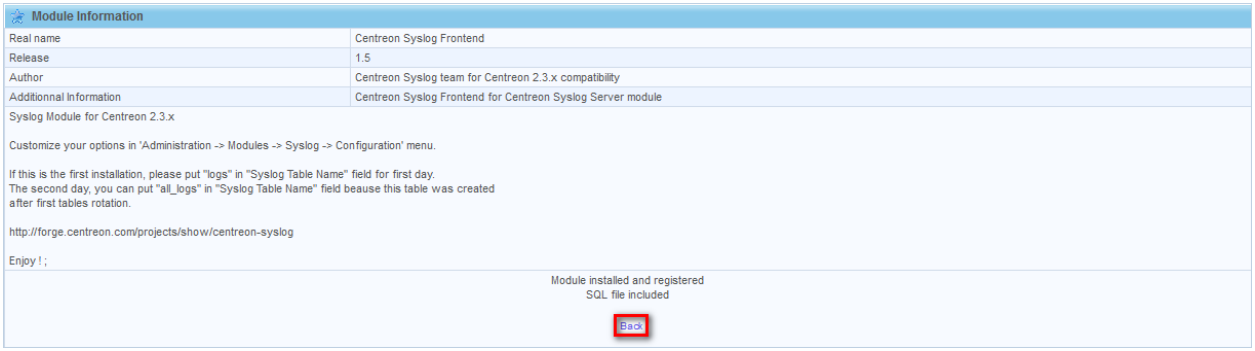


	Name	Real name	Informations	Release	Author	Expiration date	Installed	Status	Actions
	centreon-clapi	Centreon Command Line API	A tool for Centreon Management in command line.	1.4.0	Merethis Team	N/A	Yes		
	centreon-syslog-frontend	Centreon Syslog Frontend	Centreon Syslog Frontend for Centreon Syslog Server module	1.5	Centreon Syslog team for Centreon 2.3.x compatibility	N/A	No		

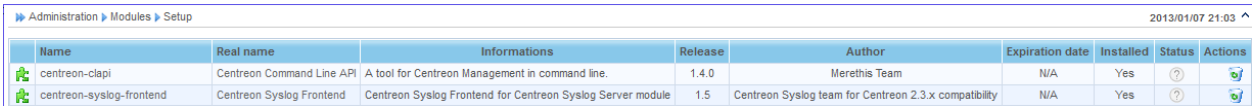
The module information will appear. Click on the “Install Module” button to add the menus in Centreon interface:



Click on “Back” to finish installation:



The installation is now finished:



	Name	Real name	Informations	Release	Author	Expiration date	Installed	Status	Actions
	centreon-clapi	Centreon Command Line API	A tool for Centreon Management in command line.	1.4.0	Merethis Team	N/A	Yes		
	centreon-syslog-frontend	Centreon Syslog Frontend	Centreon Syslog Frontend for Centreon Syslog Server module	1.5	Centreon Syslog team for Centreon 2.3.x compatibility	N/A	Yes		

Note: To configure the module, see *Configuration*

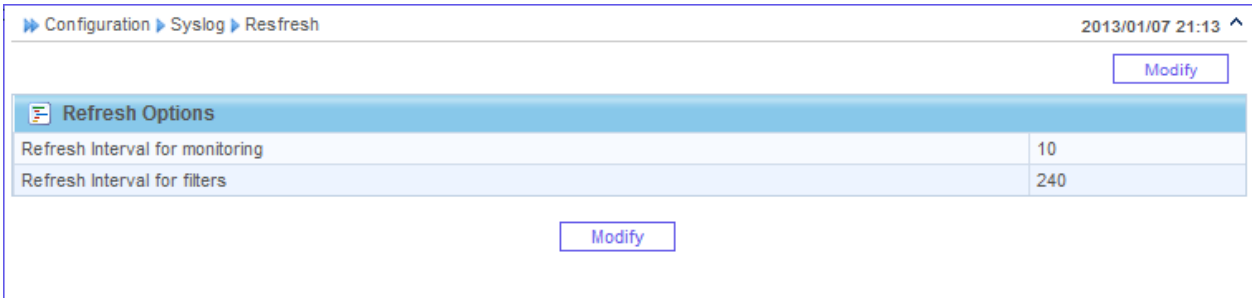
Configuration

This chapter describes the configuration of the module as well as how to add a Centreon Syslog Server.

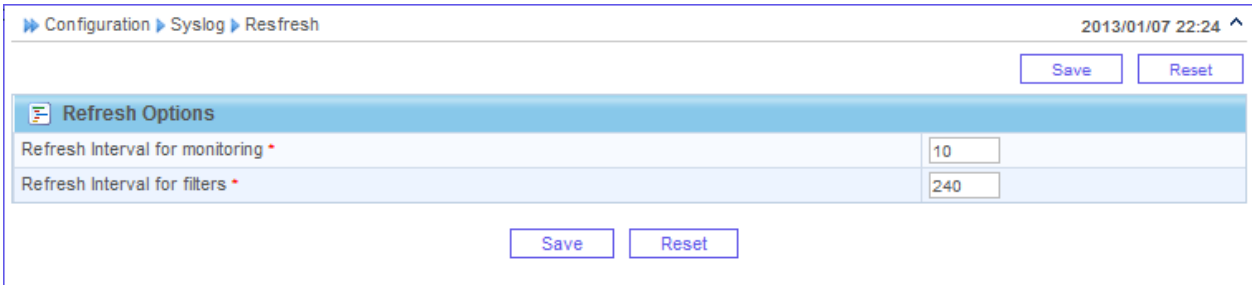
2.1 General configuration

2.1.1 General options

Connect to Centreon GUI on main server and go to the menu “Configuration -> Syslog -> Refresh”:



Click on “Modify” button to edit information:



Modify configuration and click on the “Save” button to save your modification.

Fields description are the following :

Name	Description
Refresh interval for monitoring	Interval in seconds to refresh monitoring syslog events
Refresh interval for filters	Interval in seconds to refresh filters for monitoring pages

2.1.2 Language of the interface

The interface of monitroing, search and administration of this module can be available in several languages. This depends of following both points:

- Language defined of Centreon user
- The availability of the translation file of the module

Translate the file "messages.pot" from module sources located "www/modules/centreon-syslog-frontend" directory.

Note: you can use poedit to make translation.

Create your locale language directory using the following command:

```
$ mkdir -p /usr/share/centreon/www/modules/centreon-syslog-frontend/locale/`locale | grep LC_MESSAGES
```

Warning: change Centreon installation directory '/usr/share/centreon' by your.

Compile your translated language file using command:

```
$ msgfmt messages.pot -o /usr/share/centreon/www/modules/centreon-syslog-frontend/locale/`locale | gr
```

Warning: change Centreon installation directory '/usr/share/centreon' by your.

Set Apache user rights on the file:

```
$ chown -R www-data.www-data /usr/share/centreon/www/modules/centreon-syslog-frontend/locale
```

Restart Apache server:

```
$ /etc/init.d/apache2 reload
```

Todo

change user language

2.1.3 ACL configuration

The management of access rights is identical to that besides of the interface Centreon. For it it is necessary to use:

- Access groups
- Menus Access

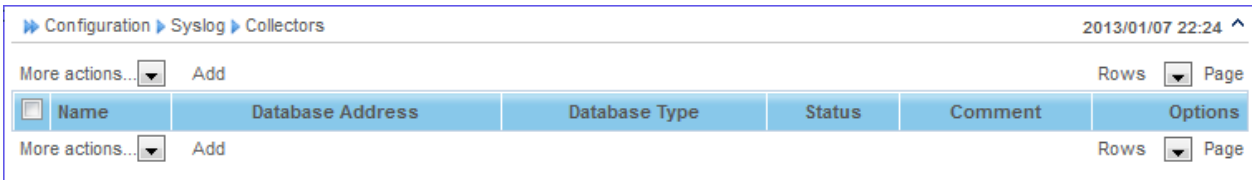
An access group is a container to group users who can have access to Centreon GUI. Once this group was created, it is possible to link an access restriction to the menus at this group. So all the users included in this group can see only what was allowed them.

To modify ACL for users of Centreon connect to Centreon and go to the menu "Administration -> ACL".

Warning: It is not possible to create ACL on syslog object. If a user can have access to Centreon Syslog Frontend module pages, this user can see all syslog events.

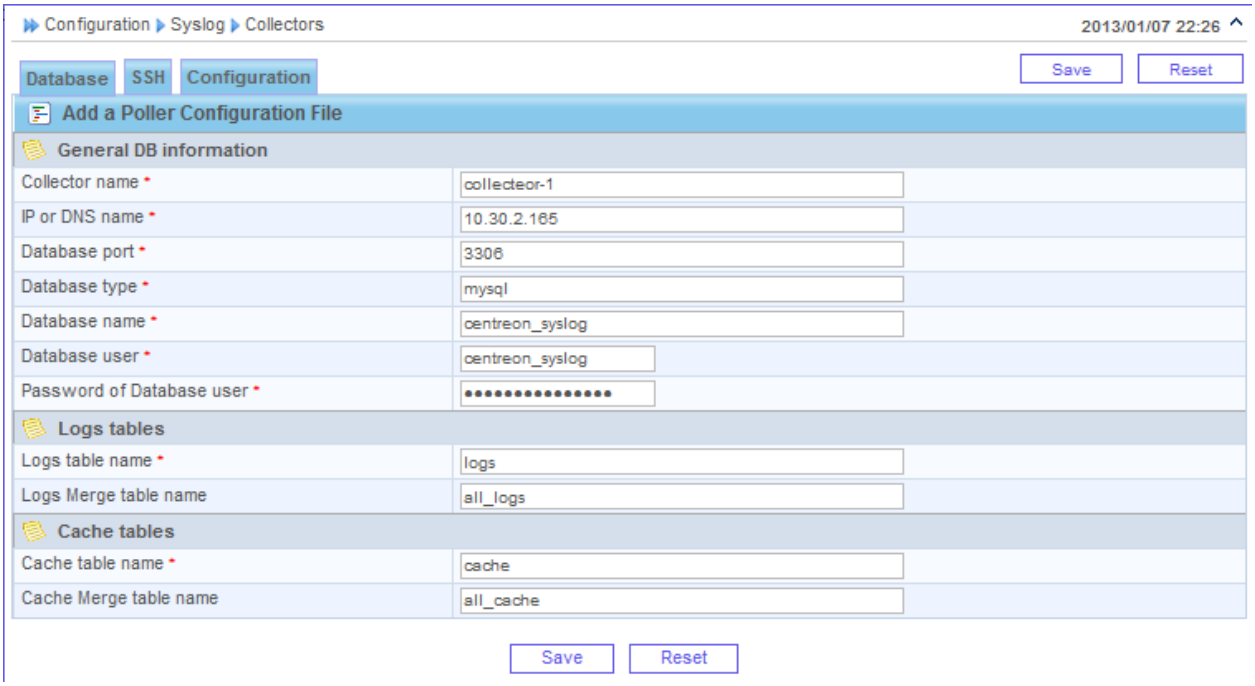
2.2 Add a collector

Connect to Centreon GUI on main server and go to the menu “Configuration -> Syslog -> Collectors” and click on “Add”:



2.2.1 Database configuration

Define information of your Centreon Syslog Server:

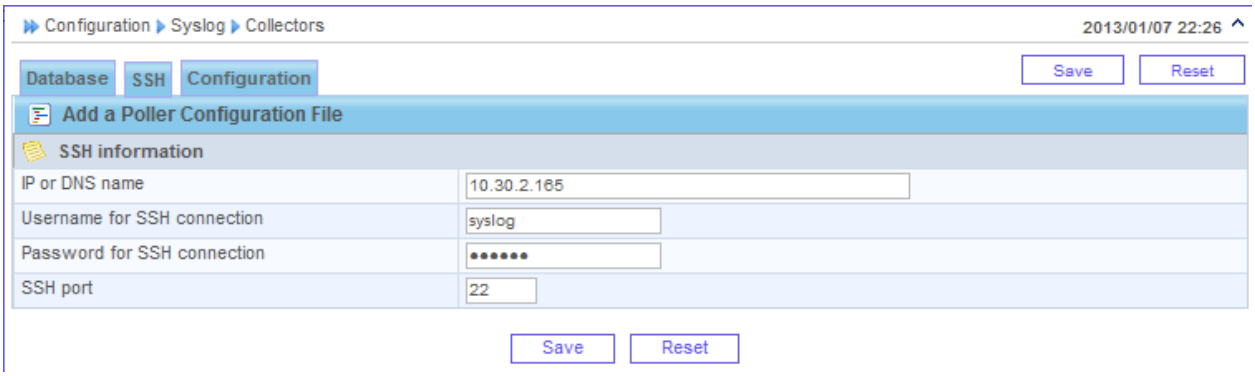


Fields description are the following:

Name	Description
Collector Name	Name of your Syslog collector
IP or DNS name	IP address or DNS of your Syslog server
Database port	Port number of MySQL database on your collector
Database type	Use ‘mysql’
Database name	Name of your database (‘centreon_syslog’ by default)
Database user	Name of user can connect to MySQL server
Password of Database user	Password of MySQL user
Logs table name	Name of daily table to store syslog events (‘logs’ by default)
Logs Merge table name	Name of MySQL merge table of daily syslog events tables (‘all_logs’ by default)
Cache table name	Name of cache for filters for real time syslog pages (‘cache’ by default)
Cache Mere table name	Name of MySQL merge table of daily cache tables (‘all_cache’ by default)

2.2.2 SSH configuration

Go to “SSH” tab:

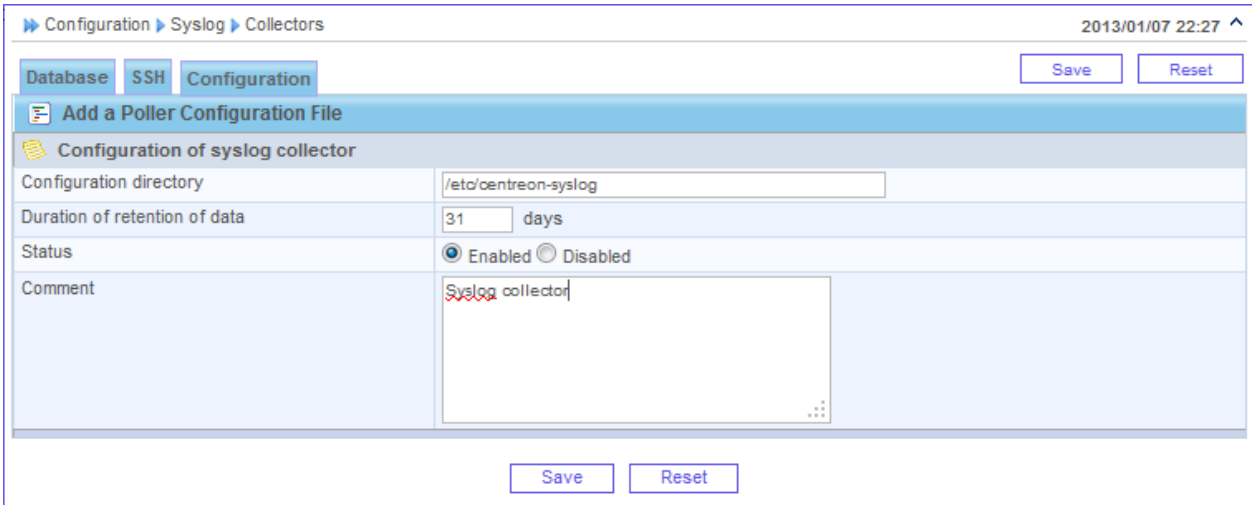


Fields description are the following:

Name	Description
IP or DNS name	IP address or DNS of your Syslog server
Username for SSH connection	‘Syslog’ by default. Created during Centreon Syslog Server installation process
Password for SSH connection	Password created during installation of Centreon Syslog Server
SSH port	Port number of SSH on your collector (‘22’ by default)

2.2.3 General configuration

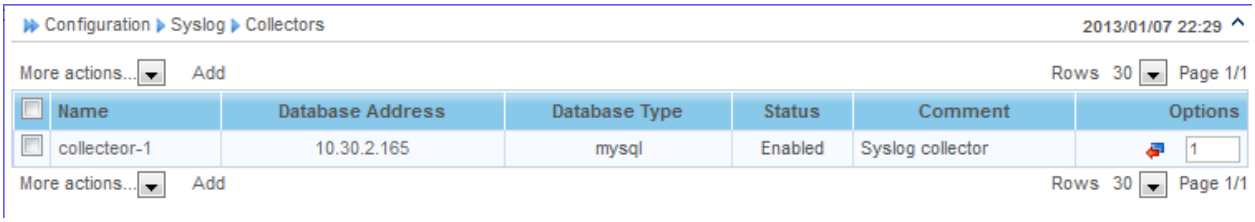
Go to “Configuration” tab:



Fields description are the following:

Name	Description
Configuration directory	Centreon Syslog Server “etc” directory (‘/etc/centreon-syslog’ by default)
Duration of retention of data	Number of days to store syslog events in database before deletion
Status	Enable/Disable display of syslog events from this collector in monitoring pages
Comment	Add description of this collector

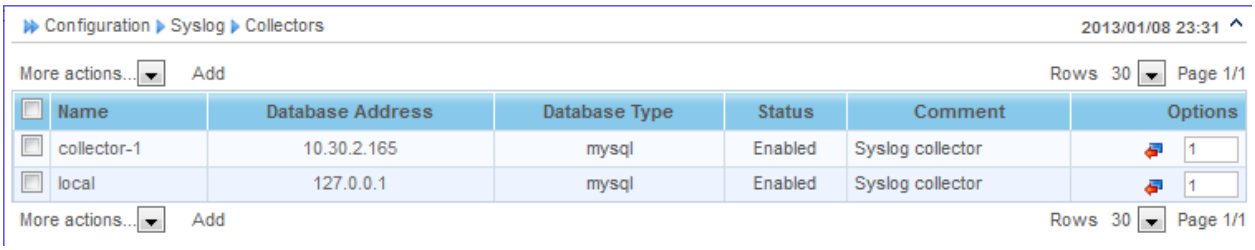
Click on “Save” button to save your configuration:



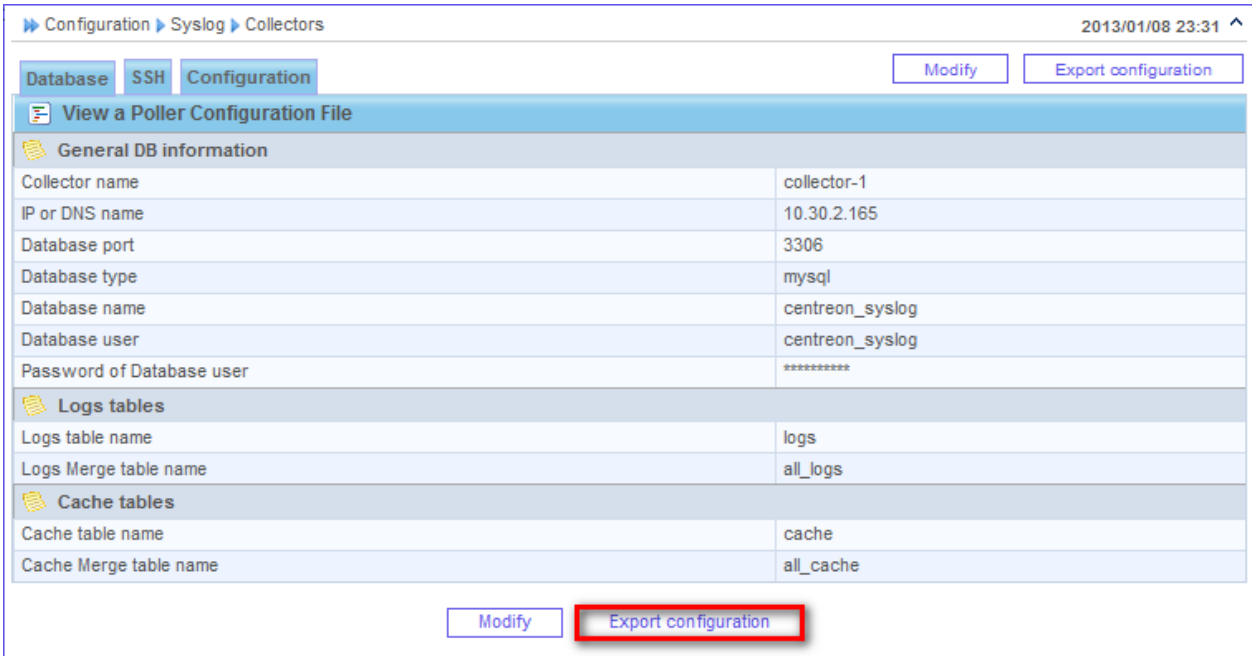
The configuration of your syslog collector is now complete!

2.2.4 Export of configuration

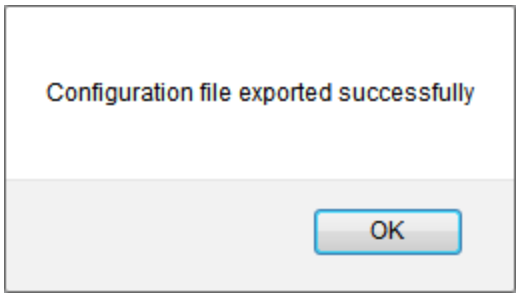
If you modifiy the duration of retention of data you must export configuration to the Centreon Syslog Server. Log on Centreon and go to the menu “Configuration -> Syslog -> Collectors” and click on your collector definition:



Click on the “Export configuration” button to transfer ‘syslog.conf.php’ to the collector:



If the export is successful, this popup appears:

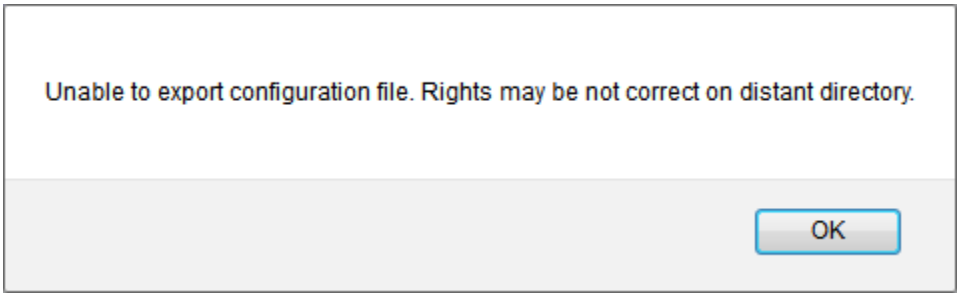


Else you may have an error of configuration.

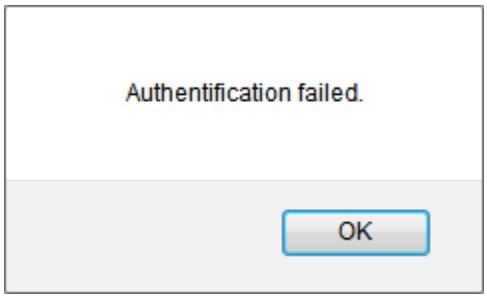
Type of errors

The following messages can be returned:

- the “etc” directory of Centreon Syslog Server in configuration of the collector is not correct
- the ‘syslog ‘user’ have incorrect rights on the “etc” directory of Centreon Syslog Server on distant server



The following messages mean that the authentication failed, the specified password for ‘syslog’ user in configuration of the collector is probably incorrect:



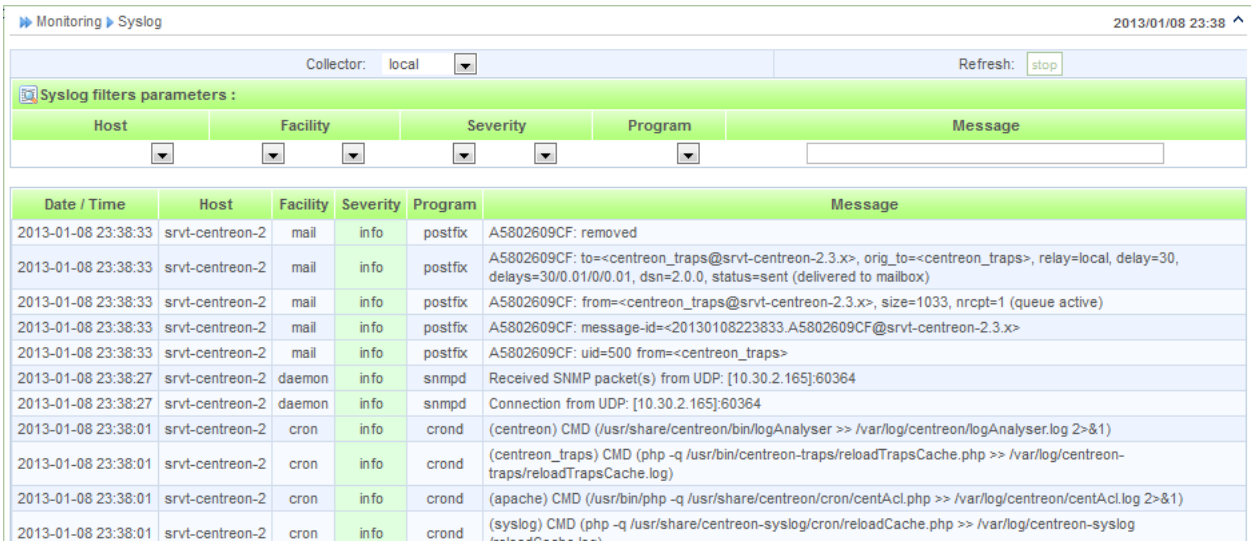
See also:

User manual to run at best this module.

This chapter describes how to use this module

3.1 Real time monitoring

Connect to Centreon GUI on main server and go to the menu “Monitoring -> Syslog -> Monitoring”. First you have to select the collector (Centreon Syslog Server) defined in *Configuration*:



Date / Time	Host	Facility	Severity	Program	Message
2013-01-08 23:38:33	srvt-centreon-2	mail	info	postfix	A5802609CF: removed
2013-01-08 23:38:33	srvt-centreon-2	mail	info	postfix	A5802609CF: to=<centreon_traps@srvt-centreon-2.3.x>, orig_to=<centreon_traps>, relay=local, delay=30, delays=30/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
2013-01-08 23:38:33	srvt-centreon-2	mail	info	postfix	A5802609CF: from=<centreon_traps@srvt-centreon-2.3.x>, size=1033, nrcpt=1 (queue active)
2013-01-08 23:38:33	srvt-centreon-2	mail	info	postfix	A5802609CF: message-id=<20130108223833.A5802609CF@srvt-centreon-2.3.x>
2013-01-08 23:38:33	srvt-centreon-2	mail	info	postfix	A5802609CF: uid=500 from=<centreon_traps>
2013-01-08 23:38:27	srvt-centreon-2	daemon	info	snmpd	Received SNMP packet(s) from UDP: [10.30.2.165]:60364
2013-01-08 23:38:27	srvt-centreon-2	daemon	info	snmpd	Connection from UDP: [10.30.2.165]:60364
2013-01-08 23:38:01	srvt-centreon-2	cron	info	crond	(centreon) CMD (/usr/share/centreon/bin/logAnalyser >> /var/log/centreon/logAnalyser.log 2>&1)
2013-01-08 23:38:01	srvt-centreon-2	cron	info	crond	(centreon_traps) CMD (php -q /usr/bin/centreon-traps/reloadTrapsCache.php >> /var/log/centreon-traps/reloadTrapsCache.log)
2013-01-08 23:38:01	srvt-centreon-2	cron	info	crond	(apache) CMD (/usr/bin/php -q /usr/share/centreon/cron/centAcl.php >> /var/log/centreon/centAcl.log 2>&1)
2013-01-08 23:38:01	srvt-centreon-2	cron	info	crond	(syslog) CMD (php -q /usr/share/centreon-syslog/cron/reloadCache.php >> /var/log/centreon-syslog

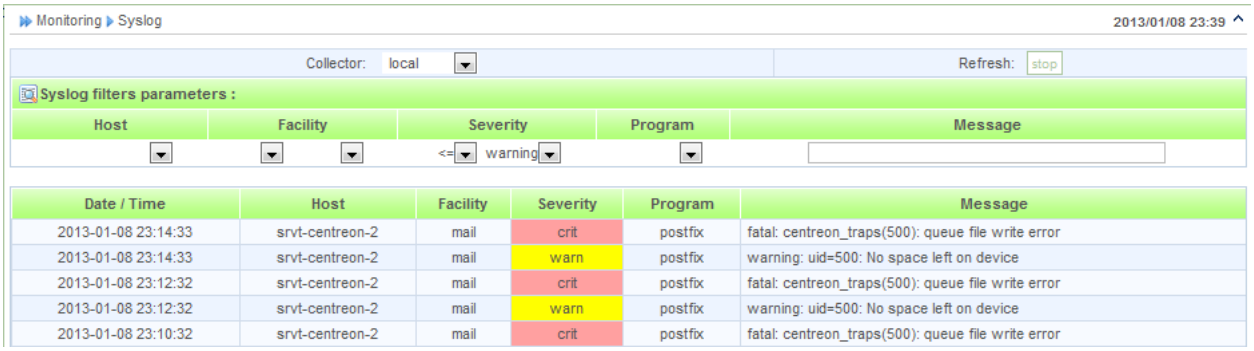
Note: Only the last 50 events are shown. This page is updated every 15 seconds. You can change the interval of refreshment from general *Configuration*:

During the first access to the page of “monitoring”, all the filters are not selected by default. The display thus presents the last fifty elements stored into database. Then in regular interval the page is automatically refreshed.

It is possible to filter the display following the criteria below:

Name	Description
Collectors	Name of the Centreon Syslog Server collector
Host	DNS or IP address who generated the event
Facility	Facility of the event
Severity	Severity of the event
Program	Name of program which generated the event
Message	Description of the event

Here a example of events filtered by severity more important or equal to 'warning':



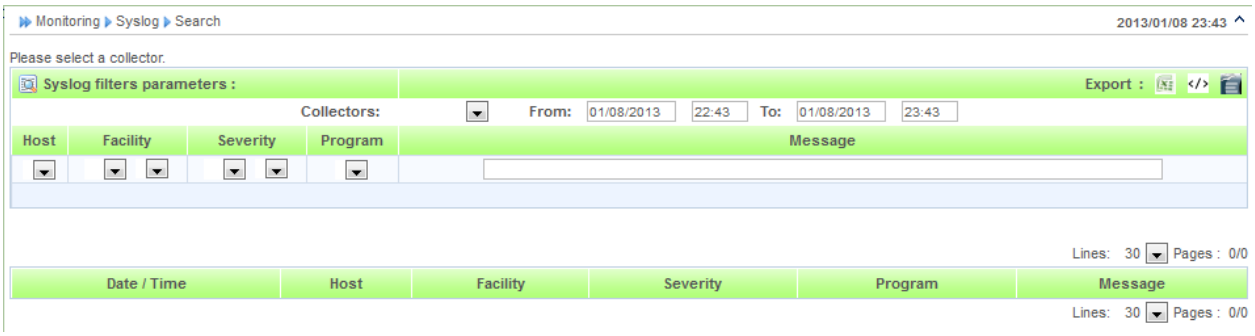
You can use different filters in same time. If any events are shown it means that any event matches with your criteria. The 'facility' and 'severity' filters can be used with mathematical operator. It is possible to select all the events "inferiors or equals" to severity "warn". In this case, will be selected the events corresponding to the severities: emerg, panic, alert, critic, to error, err, warning and warn.

Each severity and facility is linked to a number defined in *Severities and facilities correspondences*.

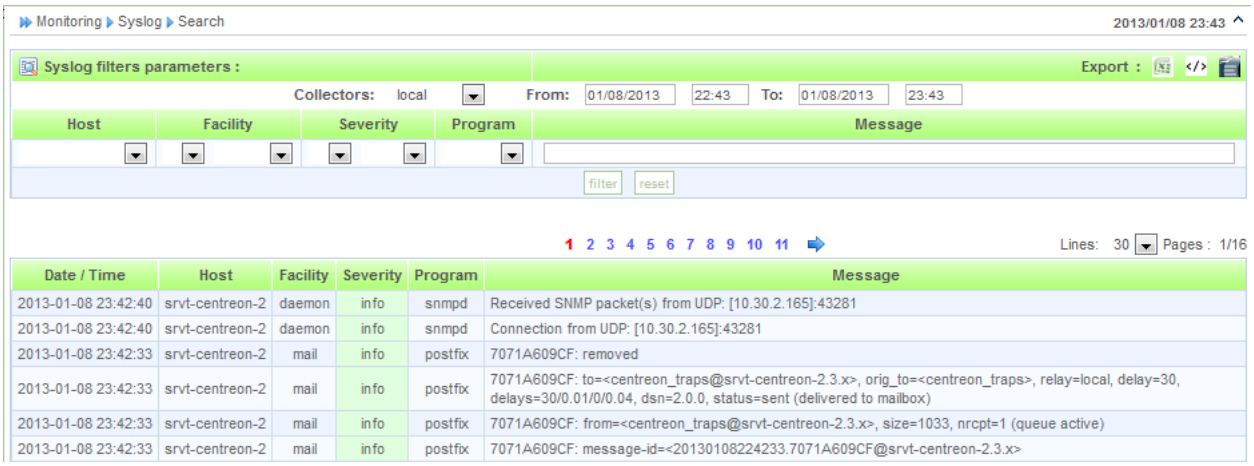
Note: You can stop the refresh of the page using the "stop" button and restart the refresh using the "start" button.

3.2 Search and extract past events

Connect to Centreon GUI on main server and go to the menu "Monitoring -> Syslog -> Search". First you have to select the collector (Centreon Syslog Server) defined in *Configuration*:



Having selected the collector, the events of last hour are shown:



It is possible to filter the display following the criteria below:

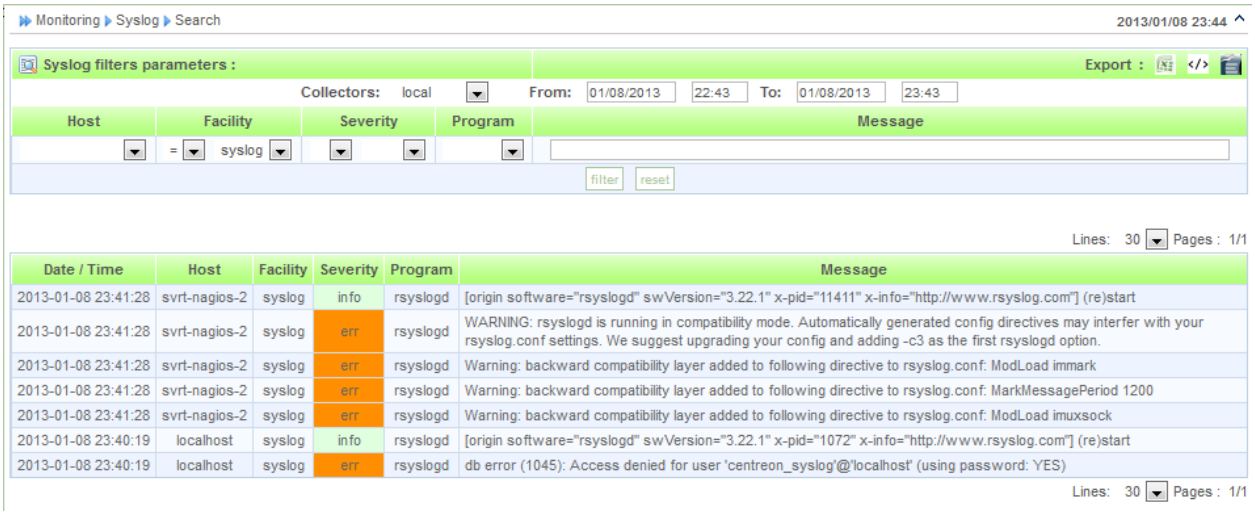
Name	Description
Collectors	Name of the Centreon Syslog Server collector
From	Date and time of the beginning of search
To	Date and time of the end of search
Host	DNS or IP address who generated the event
Facility	Facility of the event
Severity	Severity of the event
Program	Name of program which generated the event
Message	Description of the event

Note: The use of "message" filter is based on MySQL LIKE type search.

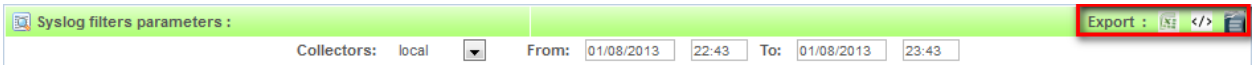
Once the criteria of search selected, click the "filter" button to launch the search.

Note: It is possible that the search takes one certain time. Indeed, this one is realized on the totality of the recording in database on selected period.

Here is an example of events filtered by facility equal to 'syslog':



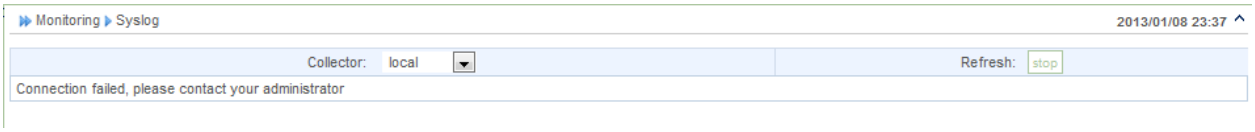
You can export the result to CSV, XML or ODT file using the following icons:



3.3 Appendices

3.3.1 Type of errors

If you have the following message, it means that parameters to access to database on Centreon Syslog Server are incorrect:

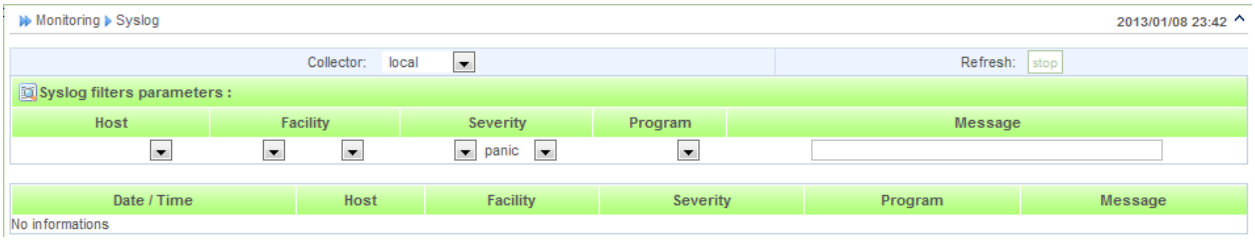


Modify your *Configuration*:

If you have the following message, it means that you have a problem with merge cache table on Centreon Syslog Server

Connect to your distant MySQL database and repear merge cache table.

The following message can be a problem. It can mean that that the insertion in database is stopped:



Check Syslog daemon paramters using documentation of Centreon Syslog Server.

3.3.2 Severities and facilities correspondences

Facility

Name	Value
emerg, panic	0
alert	1
crit	2
error,err	3
warning, warn	4
notice	5
info	6
debug	7

Severity

Name	Value
kern	0
user	1
mail	2
daemon	3
auth	4
severity	5
syslog	6
lpr	7
news	8
uucp	9
cron	10
authpriv	11
ftp	12
local0	16
local1	17
local2	18
local3	19
local4	20
local5	21
local6	22
local7	23