

**SYSLOG SERVER configuration guide**



**NOTE:** THIS DOCUMENT IS JUST A REFERENCE DOCUMENT TO SETUP SYSLOG SERVER IN WINDOWS/LINUX.

**THIS IS NOT A FEATURE OR SUPPORT DOCUMENT FOR SCM OR LINUX TC. HENCE FOR ANY ISSUES/DOUBTS, PLEASE REFER TO THE APPROPRIATE OFFICIAL SITES FOR MORE DETAILS.**

**Change History**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| 1.0 | 31-Mar-2020 | Initial Draft |
| 1.1 | 17-Apr-2020 | Logrotate section added |
| 1.2 | 23-Apr-2020 | QA reviewed and finalized |

Table of Contents

[**SYSLOG Server Configuration** 3](#_Toc38037490)

[**1.** **Syslog Server on a Linux System** 3](#_Toc38037491)

[**Setting up RSyslog Server** 3](#_Toc38037492)

[**2.** **Syslog Server on a Windows System** 6](#_Toc38037493)

[**Setting up Visual Syslog Server** 6](#_Toc38037494)

[**SnapVDI Configuration for Syslog Server** 13](#_Toc38037495)

[**Configuring remote syslog server for thin clients through SCM** 13](#_Toc38037496)

[**Steps to deploy the configuration file in SCM** 14](#_Toc38037497)

[**Log Rotation** 16](#_Toc38037498)

[**Log rotation for Visual Syslog Server** 16](#_Toc38037499)

[**Log rotation for Linux Syslog Server** 17](#_Toc38037500)

[**Configuring log rotation for Linux TC folder available in Syslog Server** 18](#_Toc38037501)

[**Setting Log size/archiving for Windows Event Log** 20](#_Toc38037502)

# **SYSLOG Server Configuration**

**Setup and configuration**

Logs are a critical component of any software or operating system. Logs usually record user’s actions, system events, network activity and more, depending on what they are intended for. Two of the most widely used logging systems on Linux systems are rsyslog and syslog-ng OSE. While windows mostly have syslog server implementations which are licensed and pricey. The one which we used here has a free license, Visual Syslog Server

This document describes the setup and configuration of remote syslog server in Linux and Windows systems. SnapVDI® software application utilizes the Syslog server to store and manage the logs from SnapVDI® Client Manager (SCM) and its Thin Clients. These logs can then be analyzed to generate a report and to debug issues without interfering in the customer environment.

Based on the customer requirement and familiarity of the platform, they can choose from following options:

1. Syslog Server on a Linux System
2. Syslog Server on a Windows System

## **Syslog Server on a Linux System**

Rsyslog is a powerful, secure and high-performance log processing system which accepts data from different types of source (systems/applications) and outputs it into multiple formats.

It has evolved from a regular syslog daemon to a fully featured, enterprise level logging system. It is designed in a client/server model; therefore, it can be configured as a client and/or as a central logging server for other servers, network devices, and remote applications.

### **Setting up RSyslog Server**

Most Linux distributions come with the rsyslog package preinstalled. In case it is not installed, you can install it using your Linux package manager tool as shown.

#CentOS 7  
$ sudo yum update && yum install rsyslog

#Ubuntu 16.04, 18.04  
$ sudo apt update && apt install rsyslog

Once rsyslog installed, you need to start the service for now, enable it to auto-start at boot and check it’s status with the [systemctl command](https://www.tecmint.com/manage-services-using-systemd-and-systemctl-in-linux/).

$ sudo systemctl start rsyslog

$ sudo systemctl enable rsyslog

$ sudo systemctl status rsyslog

The main rsyslog configuration file is located at /etc/rsyslog.conf, which loads modules, defines the global directives, contains rules for processing log messages and it also includes all config files in /etc/rsyslog.d/ for various applications/services.

$ sudo nano /etc/rsyslog.conf

You can use vim or vi or nano editor to open the rsyslog.conf file.

To configure rsyslog as a network/central logging server, you need to set the protocol (either UDP or TCP or both) it will use for remote syslog reception as well as the port it listens on.

If you want to use a UDP connection, which is faster but unreliable, search and uncomment the lines below (replace 514 with the port you want it to listen on, this should match the port address that the clients send messages to, we will look at this more when configuring a rsyslog client).

$ModLoad imudp

$UDPServerRun 514

To use TCP connection (which is slower but more reliable), search and uncomment the lines below.

$ModLoad imtcp

$InputTCPServerRun 514

Next, you need to define the ruleset for processing remote logs in the following format.

facility.severity\_level destination (where to store log)

Where:

* facility: is type of process/application generating message, they include auth, cron, daemon, kernel, local0..local7. Using \* means all facilities.
* severity\_level: is type of log message: emerg-0, alert-1, crit-2, err-3, warn-4, notice-5, info-6, debug-7. Using \* means all severity levels and none implies no severity level.
* destination: is either local file or remote rsyslog server (defined in the form IP:port).

We will use the following ruleset for collecting logs from remote hosts, using the RemoteLogs template.

Note that these rules must come before any rules for processing local messages, as shown below.

$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"

\*.\* ?RemoteLogs

& ~

Looking at the above ruleset, the first rule is,

*$template RemoteLogs,”/var/log/%HOSTNAME%/%PROGRAMNAME%.log”*

The directive $template tells rsyslog daemon to gather and write all of the received remote messages to distinct logs under /var/log, based on the hostname (client machine name) and remote client facility (program/application) that generated the messages as defined by the settings present in the template RemoteLogs.

The second line “\*.\* ?RemoteLogs” means record messages from all facilities at all severity levels using the RemoteLogs template configuration.

The final line “& ~” instructs rsyslog to stop processing the messages once it is written to a file. If you do not include “& ~”, messages will instead be written to the local files.

There are many other templates that you can use, for more information, see the rsyslog configuration man page (man rsyslog.conf) or refer to the [Rsyslog online documentation](https://www.rsyslog.com/doc/v8-stable/). Save and close the configuration file.

To apply the recent changes, restart rsyslog daemon with the following command.

$ sudo systemctl restart rsyslog

Note: User information and permission of the generated log files needs to be maintained while copying files. If the permission is changed, syslog server may not be able to update the logs inside the files.

## **Syslog Server on a Windows System**

Visual Syslog Server for Windows is a free open source program to receive and view syslog messages. Visual Syslog Server is a very straightforward and light-weight Syslog option that focuses on a real-time approach.

It does have some ability to handle and rotate logs automatically, to avoid bloat, and can also trigger scripts or programs based on thresholds that can be set.

### **Setting up Visual Syslog Server**

Download the latest stable release of Visual Syslog Server from the location specified below and follow the steps to install it.

<https://maxbelkov.github.io/visualsyslog/>

Click on [Latest stable release 1.6.4](https://github.com/MaxBelkov/visualsyslog/releases/latest) or whichever is the current version

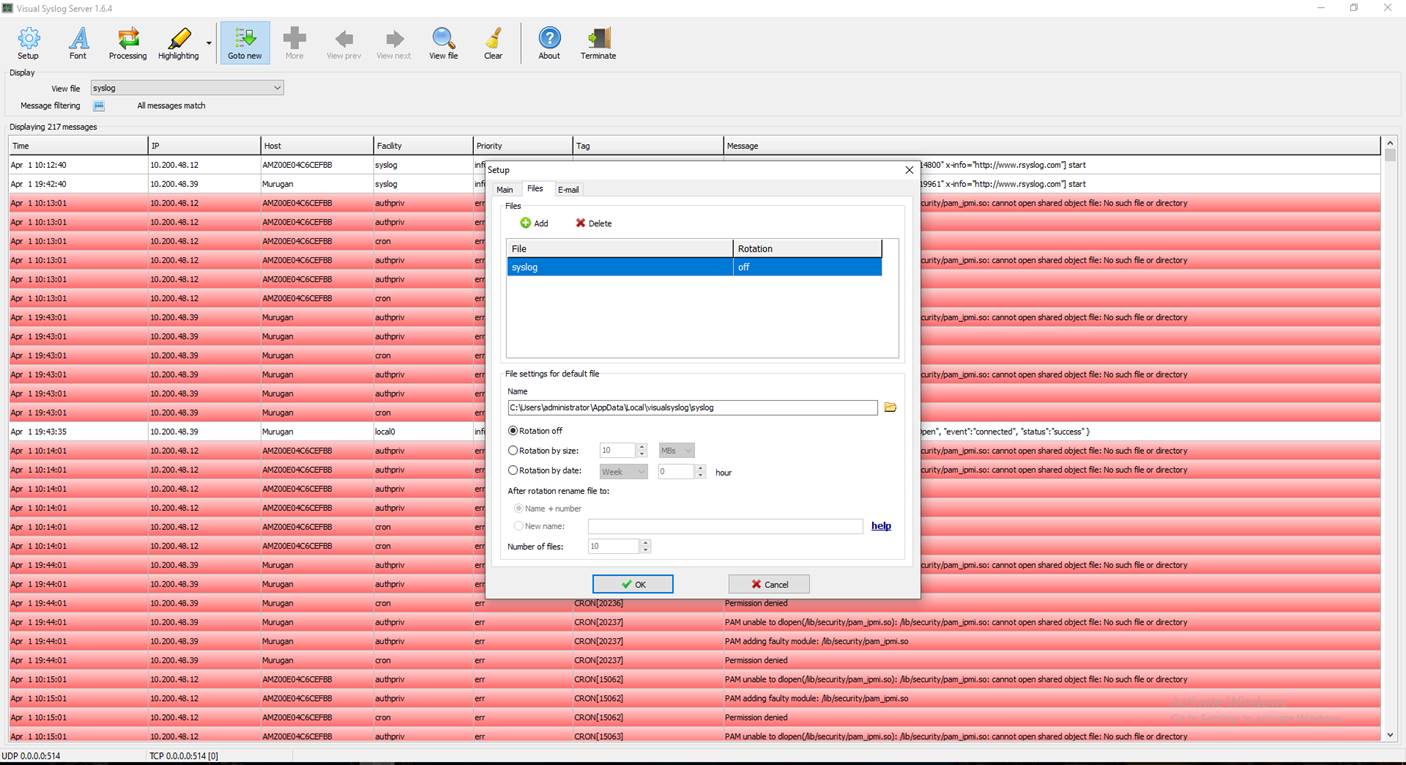
<https://github.com/MaxBelkov/visualsyslog/releases/tag/v1.6.4>

Download the [visualsyslog\_setup.zip](https://github.com/MaxBelkov/visualsyslog/releases/download/v1.6.4/visualsyslog_setup.zip)

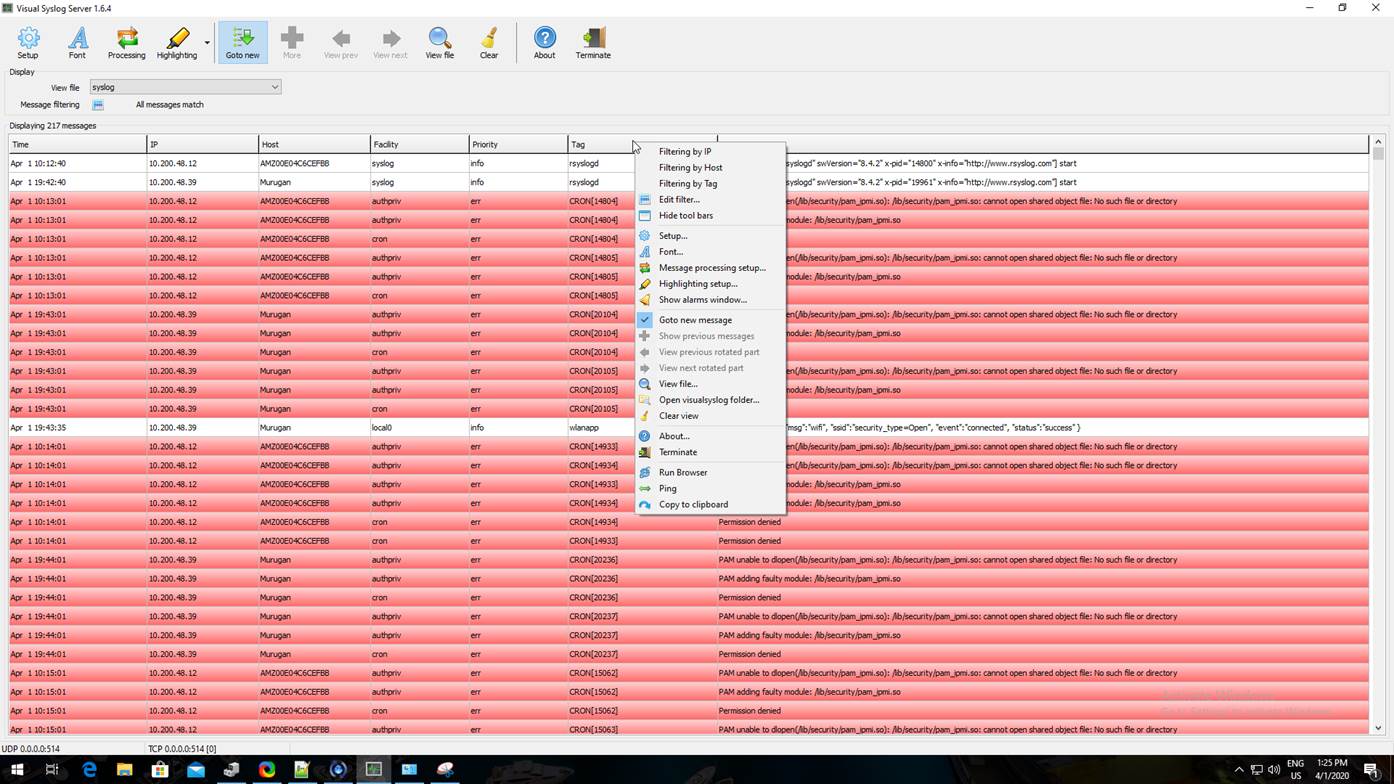
Extract it to a folder and click on the setup exe to start the installation. Make sure you are an Administrator of the system.

|  |  |
| --- | --- |
| 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |
| 5. |  |
| 6. |  |
| 7. | The server is now running on the default port and the logs can now be seen directly here. |

The log file location can be configured in the UI by clicking ‘Setup’ Icon on top -> ‘Files’ tab -> ‘File settings for default file’ option. Please refer to the screenshot below. You can get the log file from the configured location



All the logs include TC, SCM will be shown together. But we can apply filters at various level from the table. Right click on the column header -> select the desired option of filter or ‘edit filter’ to apply custom filter. Please refer to the screenshot below.



# **SnapVDI Configuration for Syslog Server**

As SnapVDI supports logging into Syslog server, following are the configurations that needs to be made on the SCM/TC side to send logs to the Syslog server.

## **Configuring remote syslog server for thin clients through SCM**

SCM will be used to push the configuration file to a group of thin clients which needs to be debugged or setting up remote syslog.

The Configuration file will be in INI format. The file can be up to 1KB. This section will have the following key values supported.

*REMOTE\_HOST - IP address of the server (in X.X.X.X format)*

*PORT - Can range from 1 – 65535, default is 514.*

*PROTOCOL - Can have one of the following values*

* *TCP*
* *UDP*

*LOG\_LEVEL - This can have any one of the following values*

* *ALL*
* *EMERGENCY*
* *ALERT*
* *CRITICAL*
* *ERROR*
* *WARNING*
* *NOTICE*
* *DEBUG*
* *INFO*

TC will use the above information to construct the remote server log entry in the below format.

<LOG\_LEVEL> <PROTOCOL><REMOTE\_HOST>:<PORT>

Sample content of the file is listed below, this file should be saved as .conf file which will be used by SCM to push to thin clients:

[syslog]

remote\_host=172.16.123.53

port=514

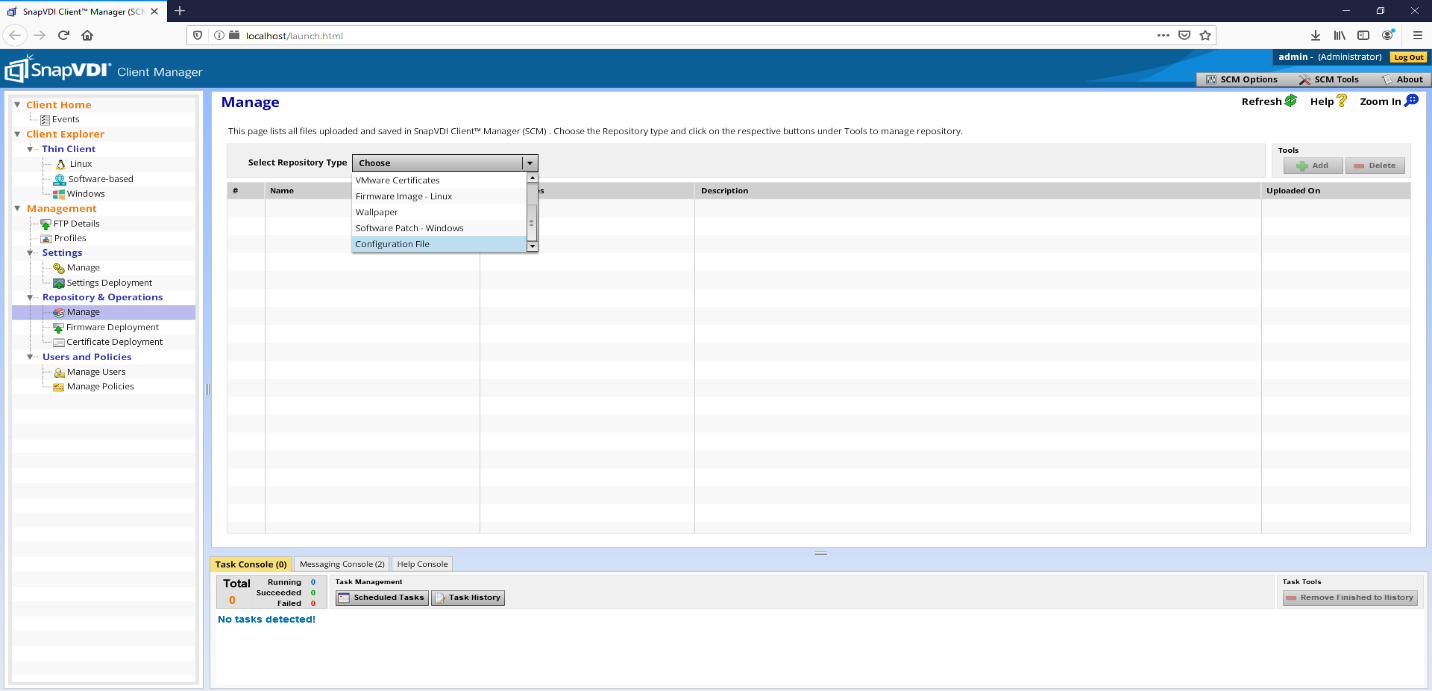
transport\_protocol=TCP

log\_level=ALL

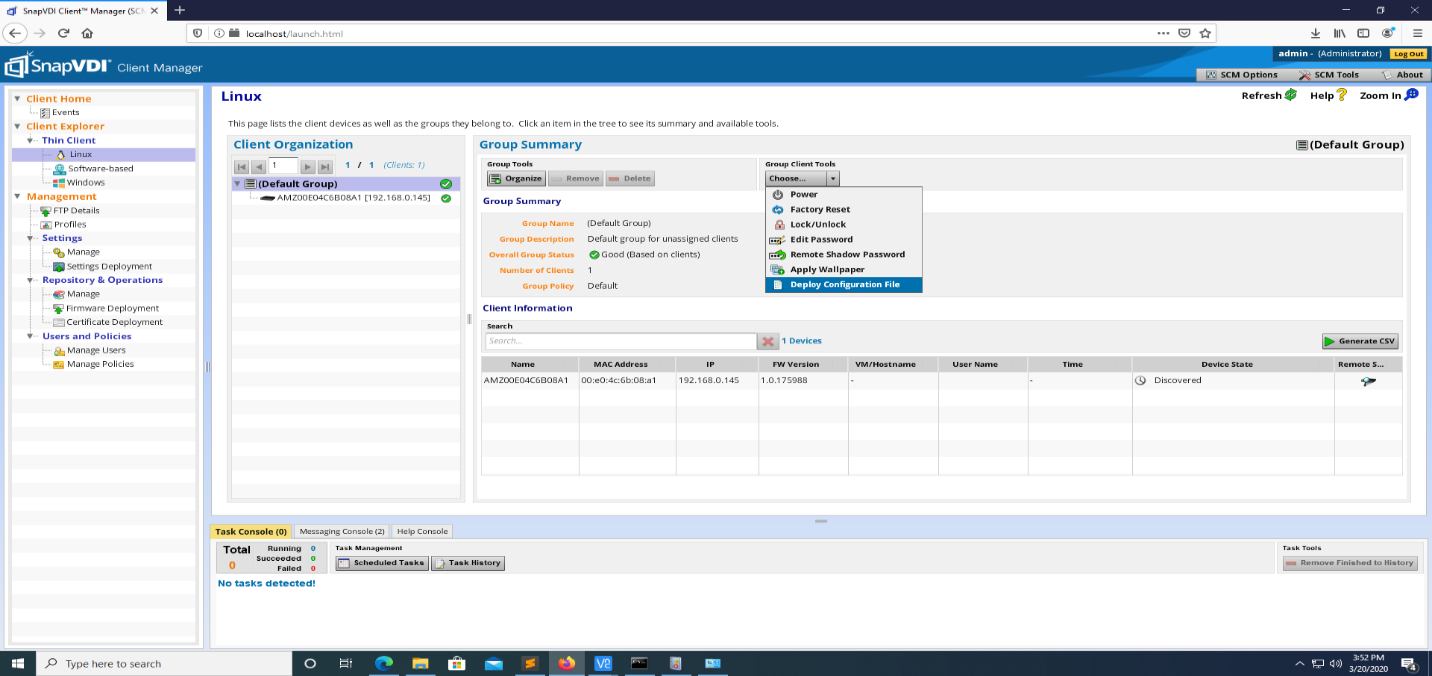
### **Steps to deploy the configuration file in SCM**

The following screen shows the option provided in SCM to push the syslog configuration file which has the ini format. Only \*.conf files are supported currently.

1. Add conf file to the repository



1. Push the conf file to the group of thin clients



# **Log Rotation**

A solution to this generic problem of log file growth is log rotation. This involves the regular (nightly or weekly, typically) moving of an existing log file to some other file name and starting fresh with an empty log file. Following are the brief instructions on how to *logrotate* for Visual Syslog Server (Windows) and Syslog Server (Linux),

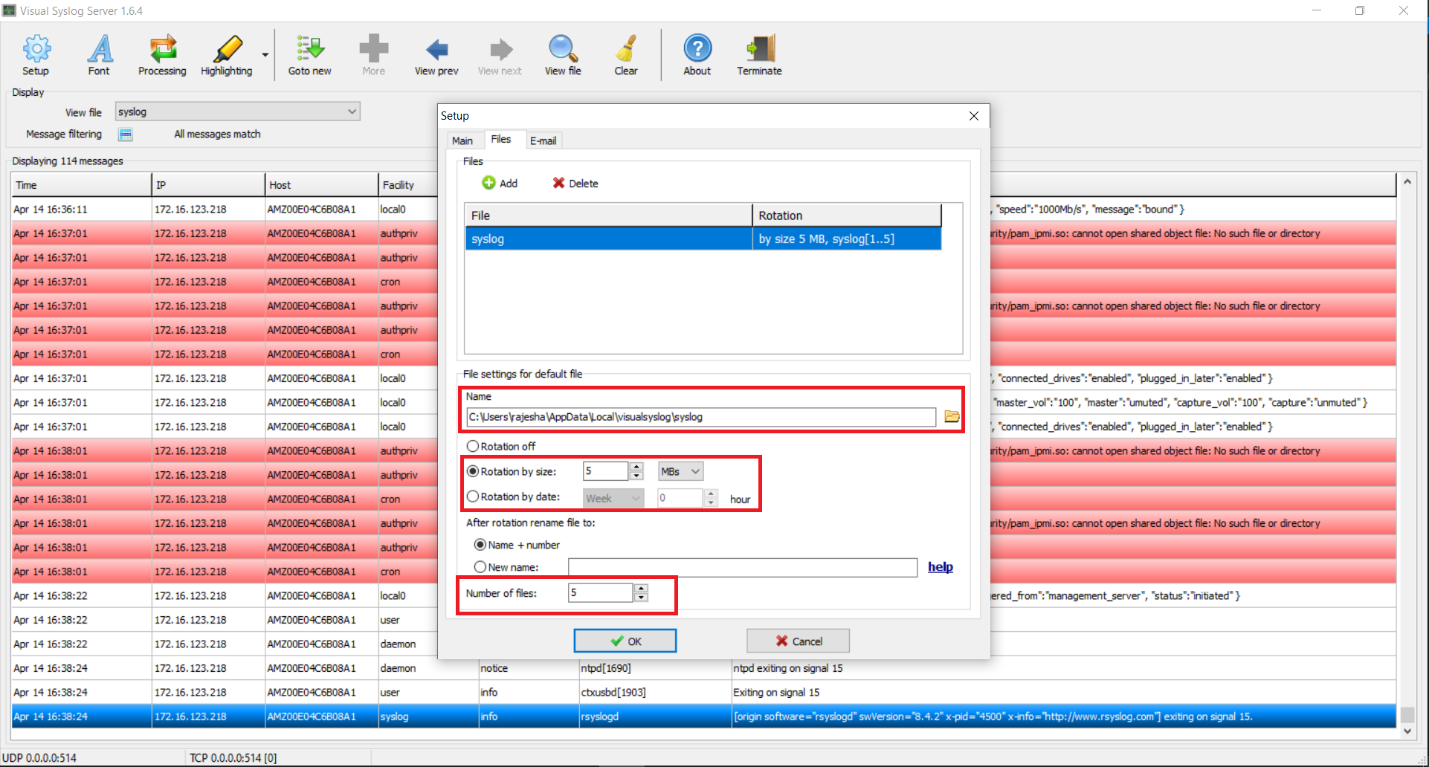
## **Log rotation for Visual Syslog Server**

Visual Syslog Server provides option to rotate logs. It can be done by doing the following,

*Click ‘Setup’ icon -> This will open ‘Setup’ window -> Navigate to ‘File’ tab.*

The name/path of the log file can be found in ‘Name’ section, which can be changed if need be. Rotation can be configured by size or date. Also, the total files to be maintained can be configured in the section ‘Number of files’.

*Please note, the screens are taken from Visual Syslog Server 1.6.4. The options and screens may vary based on different versions of the applications.*



Please refer to the following official link for more details, <http://maxbelkov.github.io/visualsyslog/>

## **Log rotation for Linux Syslog Server**

Linux Syslog server logs can be rotated using *logrotate* utility. This utility is generally available by default in Linux systems. If not, it can be installed using the following commands,

---------- **On Debian and Ubuntu** ----------

# aptitude update && aptitude install logrotate

---------- **On CentOS, RHEL and Fedora** ----------

# yum update && yum install logrotate

Any file that is created in the /etc/logrotate.d directory can be used to rotate logs. The files are usually created with root ownership and 644 permissions (rx-r--r--).

Sample content may look like below:

root@user:/etc/logrotate.d# cat rsyslog

/var/log/syslog

{

rotate 7

size 5M

missingok

delaycompress

compress

postrotate

reload rsyslog >/dev/null 2>&1 || true

endscript

}

* rotate: keep a log of 7 files.
* size: rotate once file size reaches 5MB
* missingok: don’t throw an error when the log file is not there
* delaycompress: Postpone compression of the previous log file to the next rotation cycle. This only has effect when used in combination with compress. It can be used when some program cannot be told to close its logfile and thus might continue writing to the previous log file for some time.
* compress: compress the log file
* postrottate – endscript: command to be executed once file is rotated. Normally reloading the syslog service.

### **Configuring log rotation for Linux TC folder available in Syslog Server**

Based on the template that was specified for the *rsyslog* configuration (refer page 4), the individual TCs logs are created in a separate folder in */var/log/<TC HOSTNAME>*. For eg, */var/log/AMZ00E04C6B08A1.* This folder will contain all the logs that are received from the specific TC. All the files inside that folder can be rotated by appending the following in the */etc/logrotate.d/rsyslog* file,

*Please note, these commands/files are applicable for Ubuntu 18.04 system. For other flavors/versions of Linux systems, the commands/files may vary.*

/var/log/AMZ00E04C6B08A1/\*.log

{

rotate 4

size 1M

missingok

notifempty

compress

}

***Note: Please use the corresponding TCs hostname which you wanted to do log rotate.***

After the log rotation is done, it will look something like this,

root@user:/var/log/AMZ00E04C6B08A1# ll

total 72

drwx------ 2 syslog syslog 4096 Apr 16 17:19 ./

drwxrwxr-x 14 root syslog 4096 Apr 16 15:56 ../

-rw-r--r-- 1 syslog syslog 2952 Apr 16 17:18 CRON.log

-rw-r--r-- 1 syslog syslog 332 Apr 16 17:14 CRON.log.1.gz

-rw-r--r-- 1 syslog syslog 345 Apr 16 17:09 CRON.log.2.gz

-rw-r--r-- 1 syslog syslog 338 Apr 16 17:04 CRON.log.3.gz

-rw-r--r-- 1 syslog syslog 336 Apr 16 16:59 CRON.log.4.gz

-rw-r--r-- 1 syslog syslog 557 Apr 16 16:10 kernel.log

-rw-r--r-- 1 syslog syslog 80 Apr 16 15:21 ntpd.log

-rw-r--r-- 1 syslog syslog 552 Apr 16 16:10 rsyslogd0.log

-rw-r--r-- 1 syslog syslog 580 Apr 16 16:10 rsyslogd-2359.log

-rw-r--r-- 1 syslog syslog 162 Apr 16 16:10 vue\_restservice.log

-rw-r--r-- 1 syslog syslog 195 Apr 16 16:09 vue\_restservice.log.1.gz

-rw-r--r-- 1 syslog syslog 634 Apr 16 16:10 vue\_restservice\_mgm.log

-rw-r--r-- 1 syslog syslog 327 Apr 16 16:09 vue\_restservice\_mgm.log.1.gz

-rw-r--r-- 1 syslog syslog 330 Apr 16 16:01 vue\_restservice\_mgm.log.2.gz

-rw-r--r-- 1 syslog syslog 348 Apr 16 15:53 vue\_restservice\_mgm.log.3.gz

-rw-r--r-- 1 syslog syslog 163 Apr 16 15:23 vue\_restservice\_mgm.log.4.gz

#### Multiple TC log rotation

It is possible to rotate logs of multiple TCs by adding single wildcard entry based on the TC folder name, **provided** all the TC hostname starts with same set of characters.

For e.g., the following configuration will rotate log files for all the TC log folders starting with name *AMZ,*

/var/log/AMZ\*/\*.log

{

size 1M

rotate 4

missingok

notifempty

compress

}

For complete documentation regarding *logrotate* and its parameters for Ubuntu 18.04 please refer to the link below:

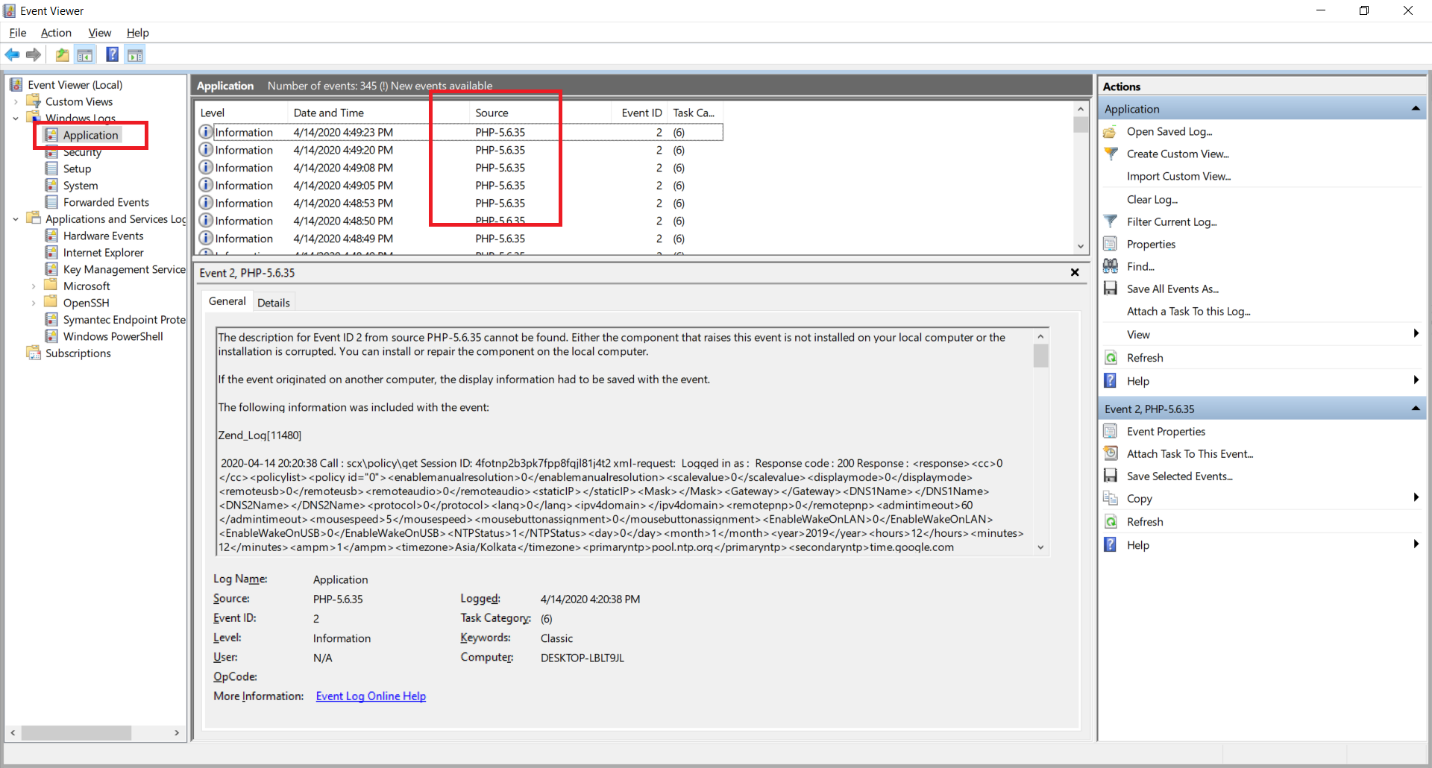
<http://manpages.ubuntu.com/manpages/bionic/en/man8/logrotate.8.html>

*logrotate* utility is dependent on *cron* for running the log rotation. By default, *logrotate* is configured to run in daily *cron* job. If need be, it can be changed to minutely, hourly, weekly & monthly. Please follow the below link to create a *cron* job in general,

<https://www.digitalocean.com/community/tutorials/how-to-use-cron-to-automate-tasks-ubuntu-1804>

## **Setting PHP Log size/archiving for Windows Event Log**

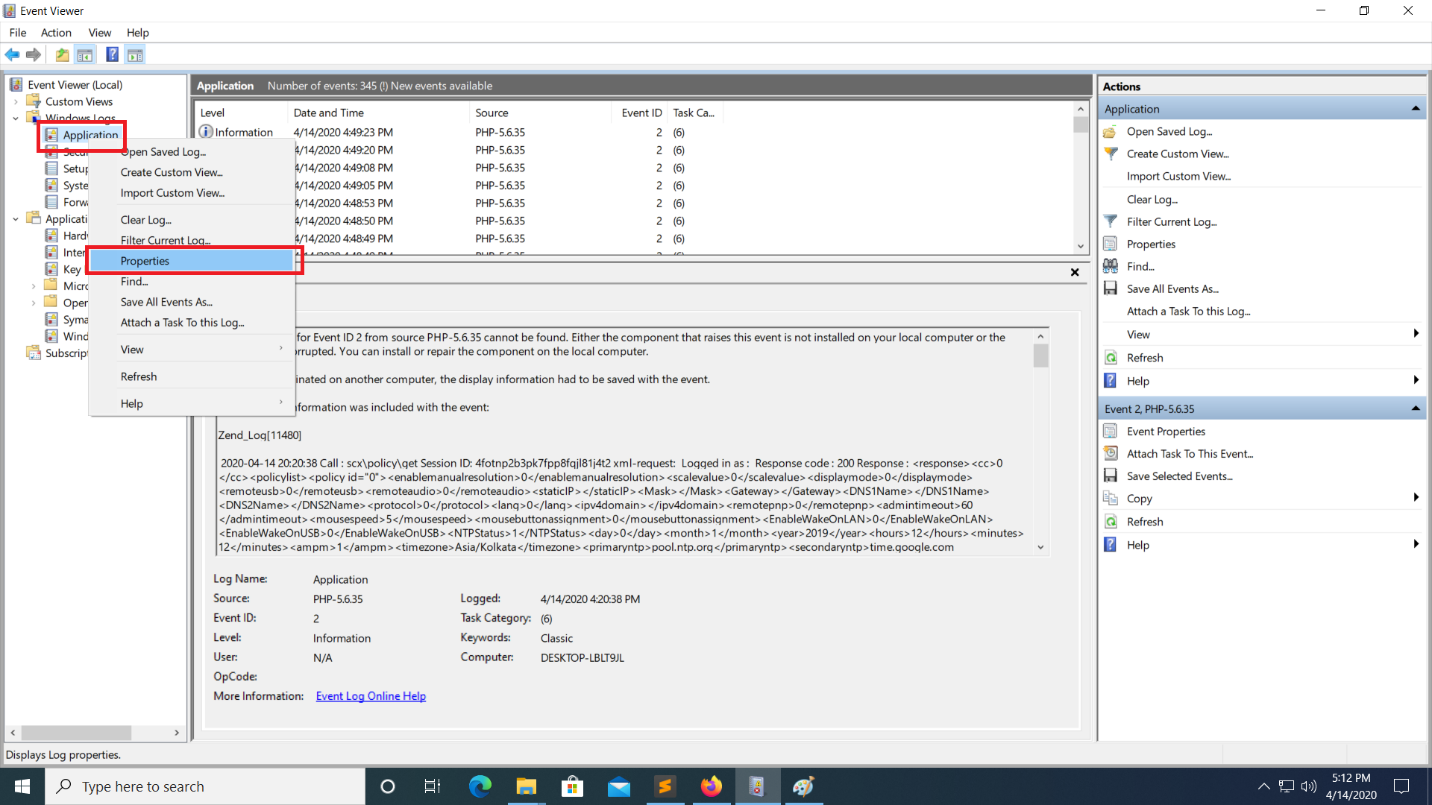
By default, SCM PHP Logs are written to Windows Event Log where SCM is installed. The SCM logs are written to Windows ‘Application’ log. The Source for the SCM event will be shown as ‘PHP-5.6.35’ as shown in the picture below,

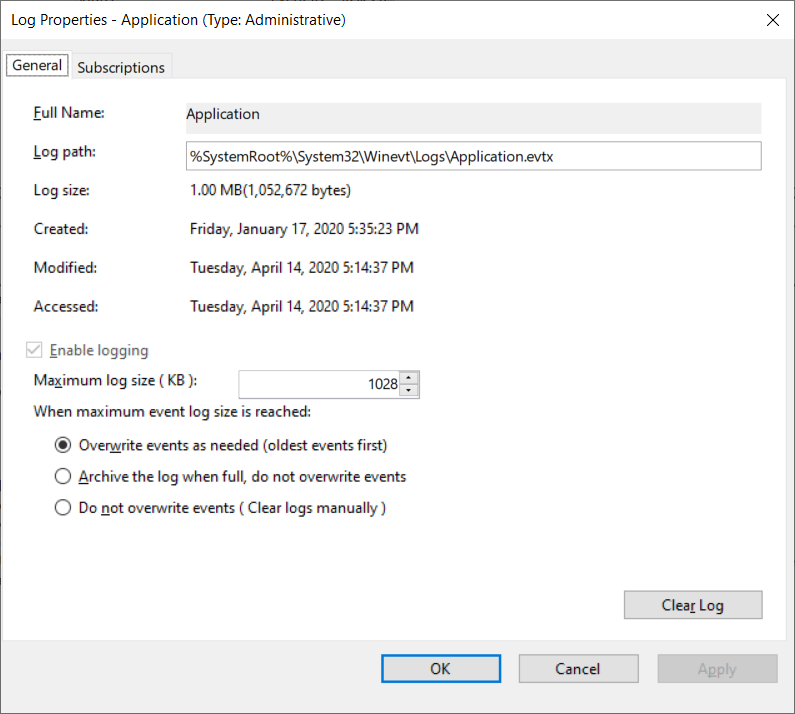


The application log size can be configured and archived from Windows Event Log. This can be done by doing the following,

*‘Application’ node -> right click -> Select ‘Properties’ from the context menu. This will open ‘Application’ log property window as shown below,*

*Please note, the screens are taken from Windows 10 Pro (64-bit) operating systems. The options and screens may vary based on different flavors of Windows.*





The log file can be found in ‘Log path’ mentioned in the ‘General’ tab. Please make changes based on the requirement. i.e., size, overwriting or archiving logs etc. and apply the settings.