Sending Mac OS X Logs to NLS 2024

Overview

The steps for receiving logs from Mac OS X are quite simple, you only need to add a line to a configuration file and restart a service. Nagios Log Server does not require any additional configuration, it is ready to receive logs from Max OS X out of the box.
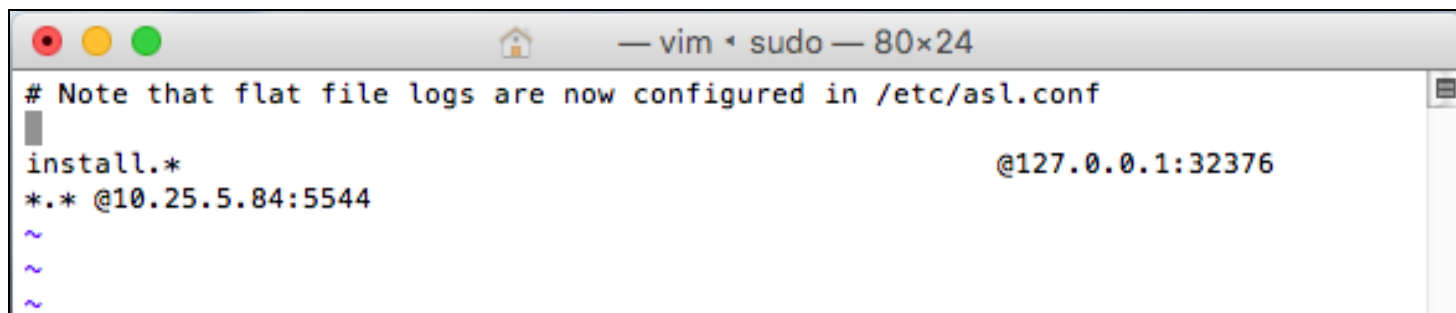
Configure Mac OS X

1. On your Mac OS X machine you will need to open the Terminal application (Utilities > Terminal).

2. Once in the terminal execute the following command to edit the /etc/syslog.conf file:

```
vi /etc/syslog.conf
```

3. You will be prompted to provide your password to edit this file.

4. When using the vi editor, to make changes press i on the keyboard first to enter insert mode. Press Esc to exit insert mode.

5. Add the following line to the end of the file, replacing xxx.xxx.xxx.xxx with the IP Address of your Nagios Log Server instance that will receive the logs:

. @xxx.xxx.xxx.xxx:5544

Here is an example of how it should look:

Nagios

```
# Note that flat file logs are now configured in /etc/asl.conf

install.*                                    @127.0.0.1:32376
*.* @10.25.5.84:5544
~
~
~
```

6. When you have finished, save the changes in vi by typing:

```
:wq
```

and press Enter.

7. The next step is to restart the syslogd daemon so the new configuration is applied and it starts sending logs to Nagios Log Server. Execute the following commands:

```
sudo launchctl stop com.apple.syslogd
```
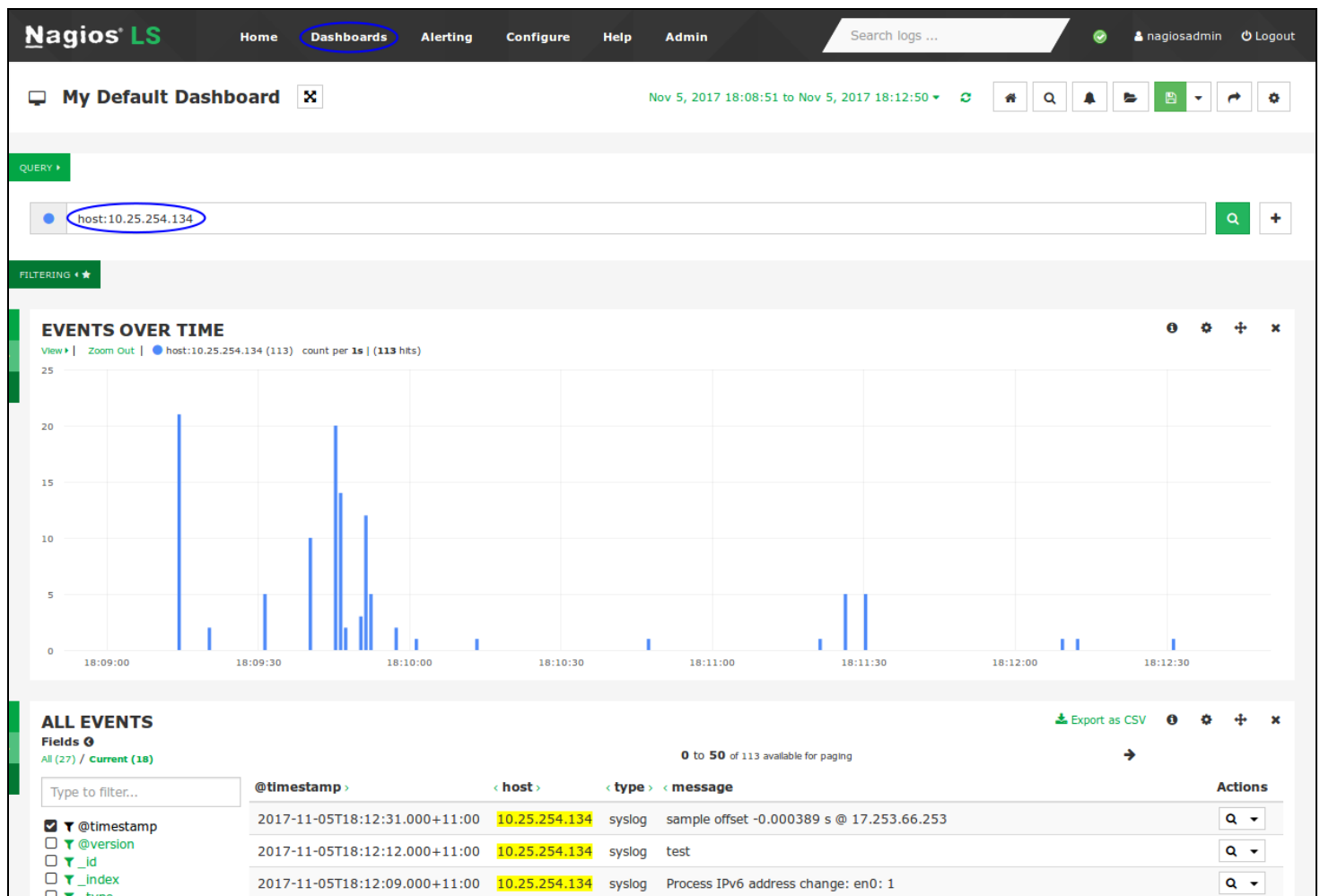
```
sudo launchctl start com.apple.syslogd
```

There should be no output on the screen from executing these commands. Execute the following command to force a log entry to be sent to Nagios Log Server:

```
logger test
```

Verify Logs

In Nagios Log Server navigate to Dashboards, open Advanced Search and perform a query using the IP address of the Mac OS X machine:

In the screenshot above you can see the test log entry, this confirms that Nagios Log Server is receiving logs from the Mac OS X machine.