Module 4: Log Server 2.0 and alerting in Nagios

Demo Document 2

Demo: Demo on Setting up Log Server.

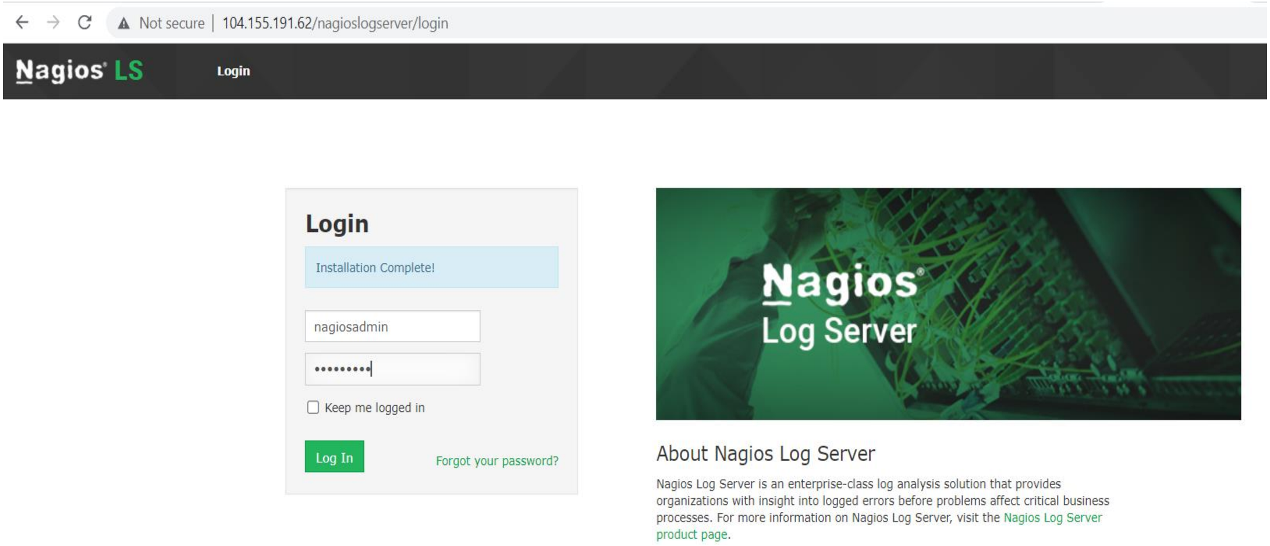
Problem Statement:

In this demo you will learn how to setup the Log Server.

Solution Steps:

NOTE – **Refer Module 4 Demo 1 to INSTALL and CONFIGURE NAGIOS LOG SERVER.**

1. Login with **username** and **password** to **NAGIOS LOG SERVER**.



Login

Installation Complete!

nagiosadmin

•••••••••

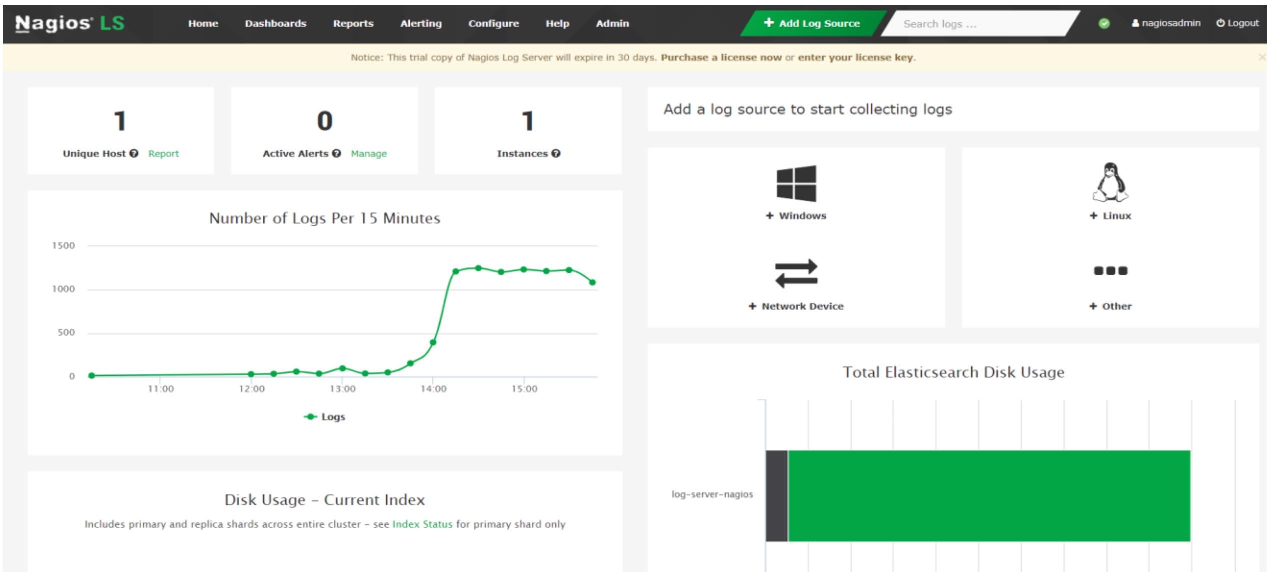
☐ Keep me logged in

Log In   Forgot your password?

About Nagios Log Server

Nagios Log Server is an enterprise-class log analysis solution that provides organizations with insight into logged errors before problems affect critical business processes. For more information on Nagios Log Server, visit the Nagios Log Server product page.

2. Now you are navigated to **Nagios Log Server** homepage as shown in the below screenshot.



Notice: This trial copy of Nagios Log Server will expire in 30 days. Purchase a license now or enter your license key.

1 Unique Host Report

0 Active Alerts Manage

1 Instances

Add a log source to start collecting logs

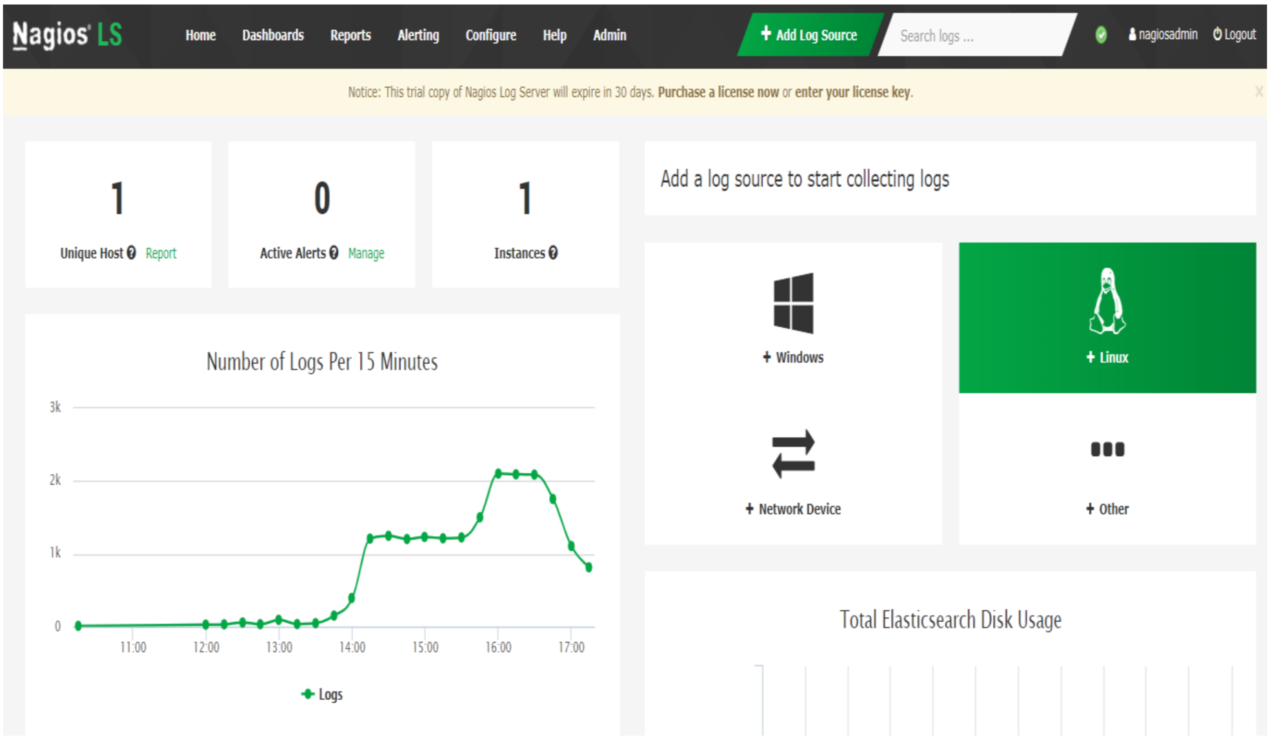
Number of Logs Per 15 Minutes

Total Elasticsearch Disk Usage

Disk Usage – Current Index

Includes primary and replica shards across entire cluster – see Index Status for primary shard only

3. Let us add **LINUX** server system logs. So, select **LINUX** from **Nagios Log Server** homepage as shown in the below screenshot.

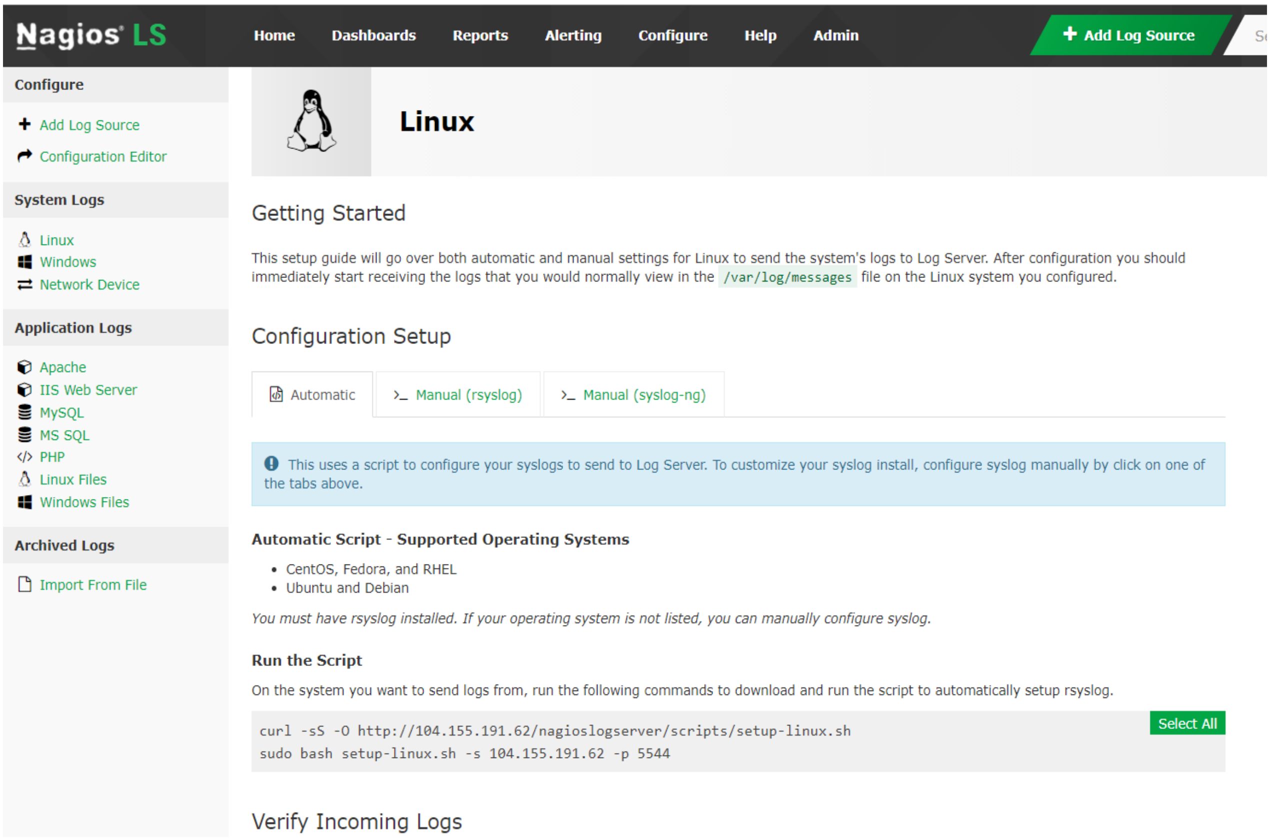


Notice: This trial copy of Nagios Log Server will expire in 30 days. **Purchase a license now** or **enter your license key**.

1	0	1
Unique Host Report	Active Alerts Manage	Instances

Add a log source to start collecting logs

4. Now you can see the Configuration setup for **LINUX**.



Linux

Getting Started

This setup guide will go over both automatic and manual settings for Linux to send the system's logs to Log Server. After configuration you should immediately start receiving the logs that you would normally view in the `/var/log/messages` file on the Linux system you configured.

Configuration Setup

This uses a script to configure your syslogs to send to Log Server. To customize your syslog install, configure syslog manually by click on one of the tabs above.

Automatic Script - Supported Operating Systems

- CentOS, Fedora, and RHEL
- Ubuntu and Debian

You must have rsyslog installed. If your operating system is not listed, you can manually configure syslog.

Run the Script

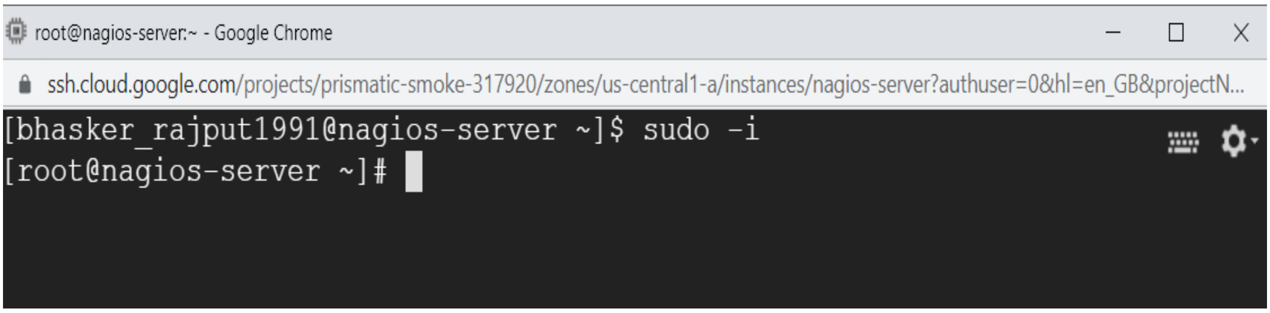
On the system you want to send logs from, run the following commands to download and run the script to automatically setup rsyslog.

```
curl -sS -O http://104.155.191.62/nagioslogserver/scripts/setup-linux.sh
sudo bash setup-linux.sh -s 104.155.191.62 -p 5544
```

Verify Incoming Logs

5. Now create another machine (**UBUNTU/CENTOS**) using **VIRTUAL BOX** or **AWS**, that is required to post logs on **NAGIOS LOG SERVER** and the connect to the machine.
NOTE – **In my case I have created CENTOS machine, so I have logged into the CENTOS**

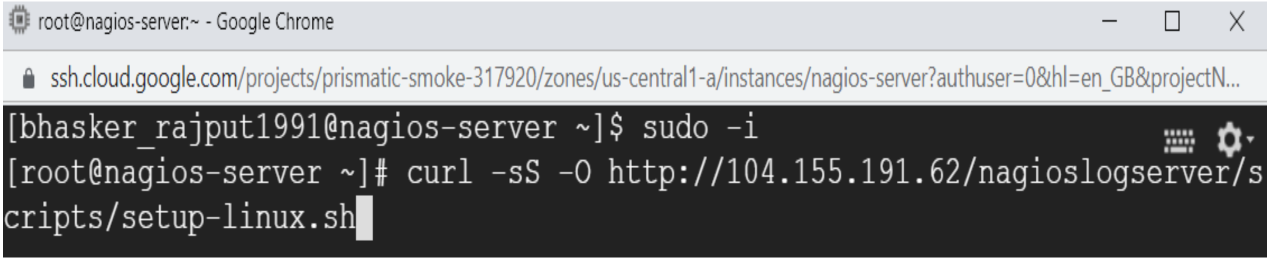
machine but if you creating UBUNTU machine then you have to login to UBUNTU machine.



```
[bhasker_rajput1991@nagios-server ~]$ sudo -i
[root@nagios-server ~]#
```

root@nagios-server:~ - Google Chrome
ssh.cloud.google.com/projects/prismatic-smoke-317920/zones/us-central1-a/instances/nagios-server?authuser=0&hl=en_GB&projectN...

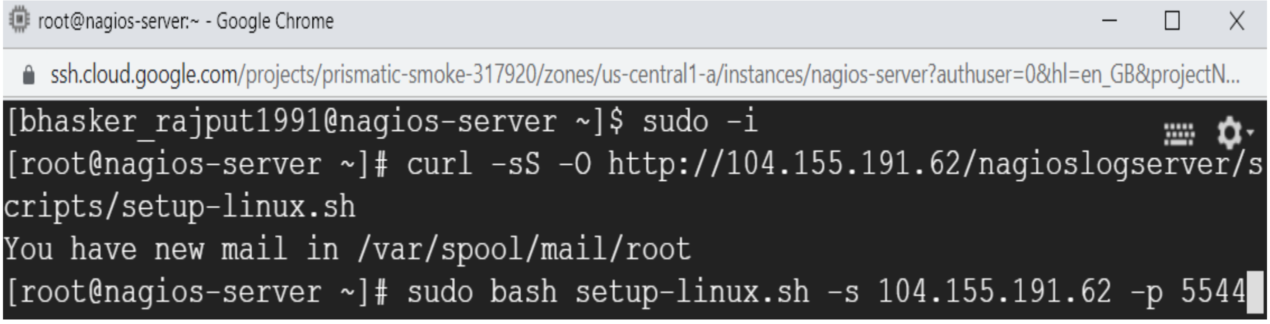
6. Change your privileges to **ROOT** using command:
   sudo -i
   Now use the below command to **download** the script to automatically set up **rsyslog**.
   curl -sS -O http://35.188.106.171/nagioslogserver/scripts/setup-linux.sh



```
[bhasker_rajput1991@nagios-server ~]$ sudo -i
[root@nagios-server ~]# curl -sS -O http://104.155.191.62/nagioslogserver/s
cripts/setup-linux.sh
```

root@nagios-server:~ - Google Chrome
ssh.cloud.google.com/projects/prismatic-smoke-317920/zones/us-central1-a/instances/nagios-server?authuser=0&hl=en_GB&projectN...

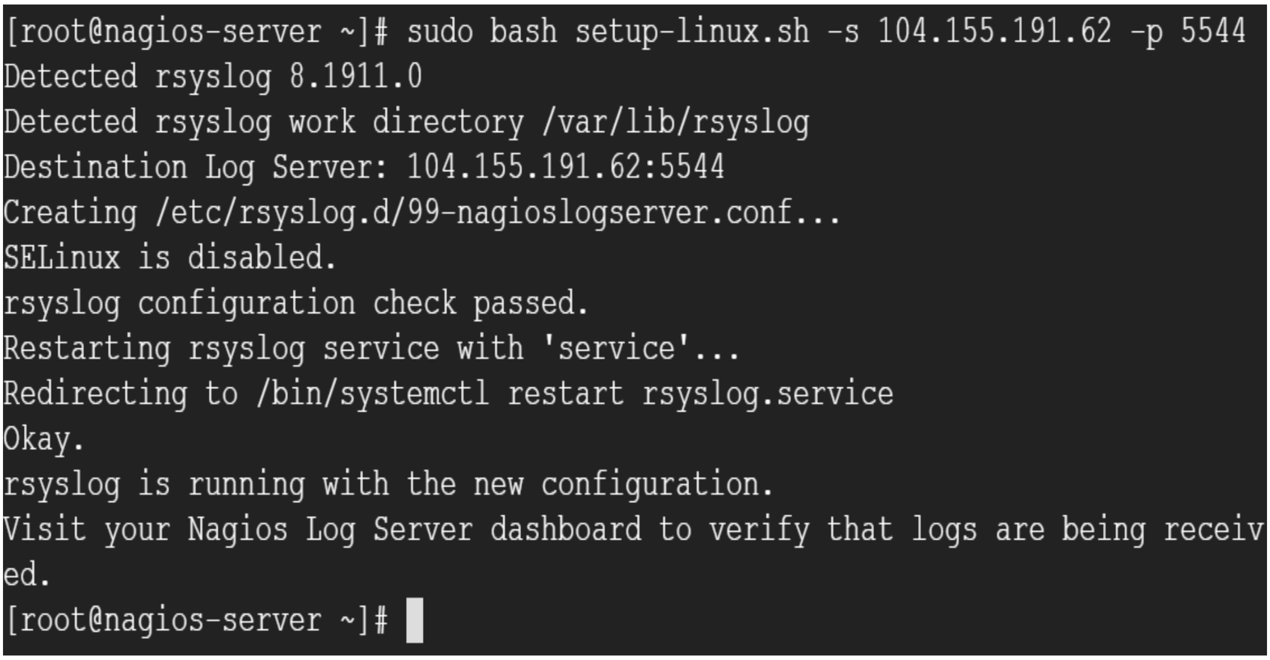
7. Now use the below command to **run** the script.
   sudo bash setup-linux.sh -s 35.188.106.171 -p 5544



```
[bhasker_rajput1991@nagios-server ~]$ sudo -i
[root@nagios-server ~]# curl -sS -O http://104.155.191.62/nagioslogserver/s
cripts/setup-linux.sh
You have new mail in /var/spool/mail/root
[root@nagios-server ~]# sudo bash setup-linux.sh -s 104.155.191.62 -p 5544
```

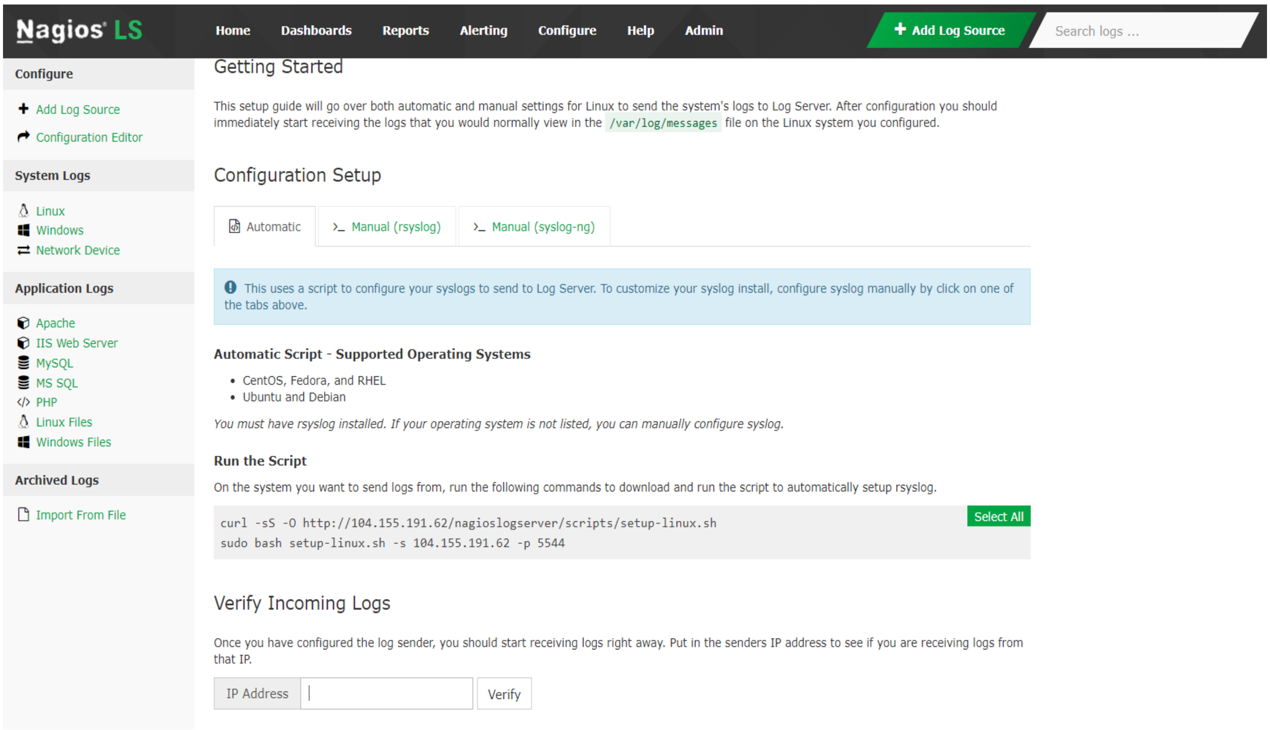
root@nagios-server:~ - Google Chrome
ssh.cloud.google.com/projects/prismatic-smoke-317920/zones/us-central1-a/instances/nagios-server?authuser=0&hl=en_GB&projectN...

8. Now **rsyslog** is configured successfully as shown in the below screenshot.



```
[root@nagios-server ~]# sudo bash setup-linux.sh -s 104.155.191.62 -p 5544
Detected rsyslog 8.1911.0
Detected rsyslog work directory /var/lib/rsyslog
Destination Log Server: 104.155.191.62:5544
Creating /etc/rsyslog.d/99-nagioslogserver.conf...
SELinux is disabled.
rsyslog configuration check passed.
Restarting rsyslog service with 'service'...
Redirecting to /bin/systemctl restart rsyslog.service
Okay.
rsyslog is running with the new configuration.
Visit your Nagios Log Server dashboard to verify that logs are being receiv
ed.
[root@nagios-server ~]# 
```

9. COPY your newly created (**UBUNTU/CENTOS**) machine **Server External IP** and navigate back to **Nagios Log Server** LINUX configuration page and scroll down.



Getting Started

This setup guide will go over both automatic and manual settings for Linux to send the system's logs to Log Server. After configuration you should immediately start receiving the logs that you would normally view in the `/var/log/messages` file on the Linux system you configured.

Configuration Setup

This uses a script to configure your syslogs to send to Log Server. To customize your syslog install, configure syslog manually by click on one of the tabs above.

Automatic Script - Supported Operating Systems

- CentOS, Fedora, and RHEL
- Ubuntu and Debian

You must have rsyslog installed. If your operating system is not listed, you can manually configure syslog.

Run the Script

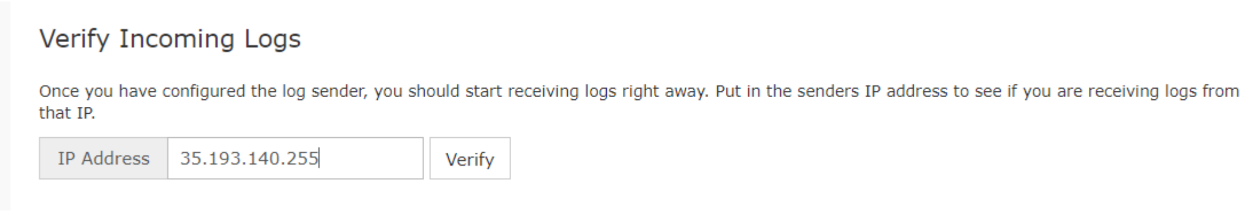
On the system you want to send logs from, run the following commands to download and run the script to automatically setup rsyslog.

```
curl -sS -O http://104.155.191.62/nagioslogserver/scripts/setup-linux.sh
sudo bash setup-linux.sh -s 104.155.191.62 -p 5544
```

Verify Incoming Logs

Once you have configured the log sender, you should start receiving logs right away. Put in the senders IP address to see if you are receiving logs from that IP.

10. Now to validate you need to provide **SERVER External IP** and click on **VERIFY**.

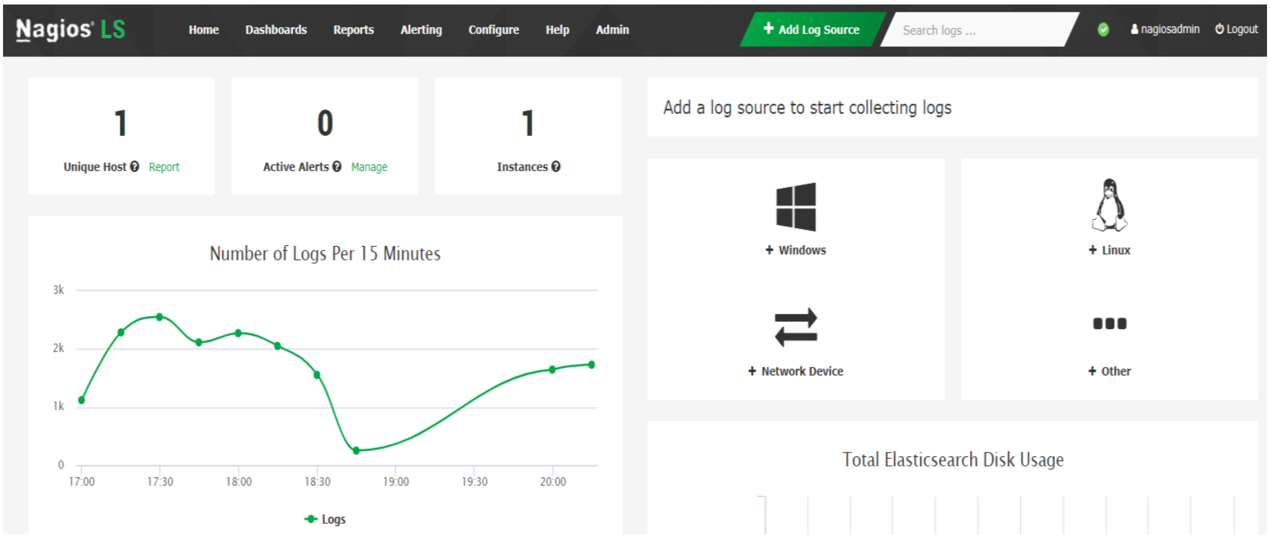


Verify Incoming Logs

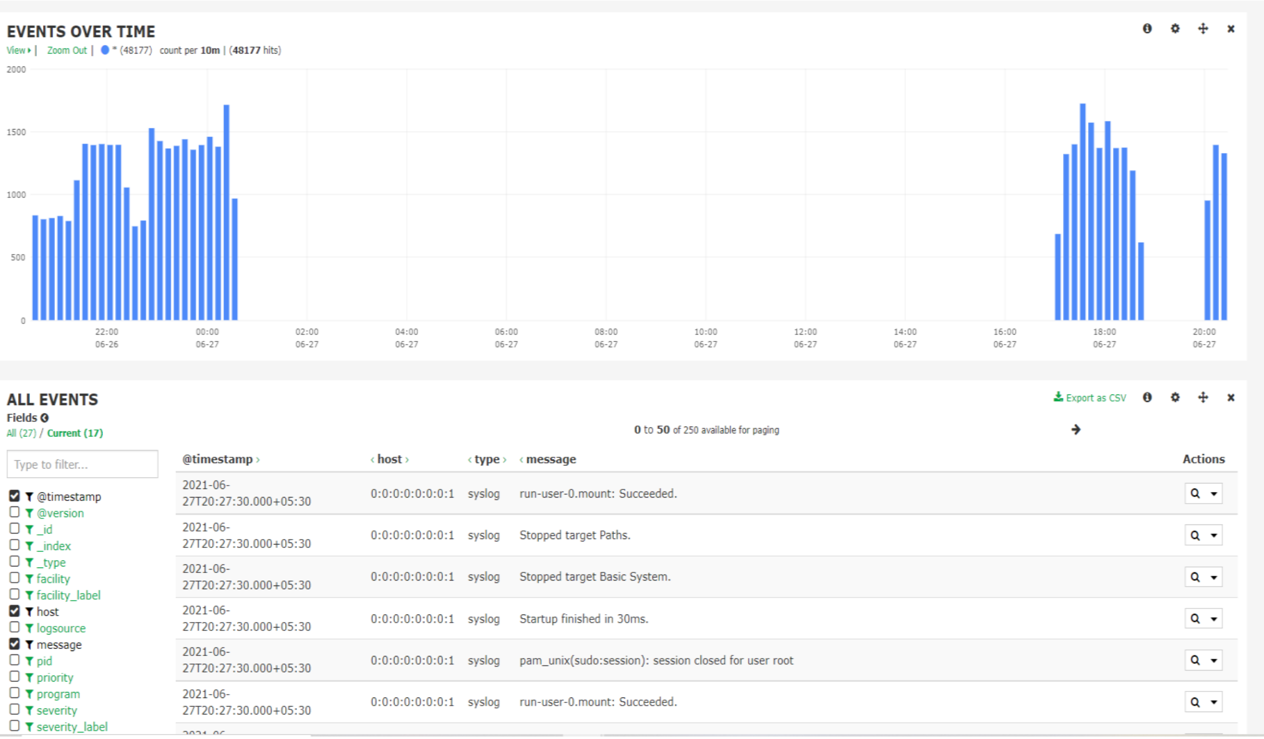
Once you have configured the log sender, you should start receiving logs right away. Put in the senders IP address to see if you are receiving logs from that IP.

IP Address: 35.193.140.255

11. Now on **NAGIOS LOG SERVER** HOME page click on **Dashboards**.



12. Now you can see **syslogs** populating on **NAGIOS LOG SERVER.**



0 to 50 of 250 available for paging

☑ @timestamp
☐ @version
☐ _id
☐ _index
☐ _type
☐ facility
☐ facility_label
☑ host
☐ logsource
☑ message
☐ pid
☐ priority
☐ program
☐ severity
☐ severity_label

@timestamp	host	type	message	Actions
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	run-user-0.mount: Succeeded.	
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	Stopped target Paths.	
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	Stopped target Basic System.	
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	Startup finished in 30ms.	
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	pam_unix(sudo:session): session closed for user root	
2021-06-27T20:27:30.000+05:30	0:0:0:0:0:0:0:1	syslog	run-user-0.mount: Succeeded.	