# Sending ESXi Logs To Nagios Log Server

## Purpose

This document describes how to configure your VMware ESXi server to send syslog messages to Nagios Log Server.

## Target Audience

This document is intended for use by VMware Administrators who would like to send their ESXi syslog messages to Nagios Log Server for storage and analysis.

## Overview

These steps will walk you through:

- Create input for desired port to Nagios Log Server
  - UDP 514
  - TCP 1514
- Configure Firewall Rules on Nagios Log Server
- Configure ESXi to send syslogs to Nagios Log Server

## UDP 514 vs TCP 1514

ESXi can send syslogs on two ports/protocols:

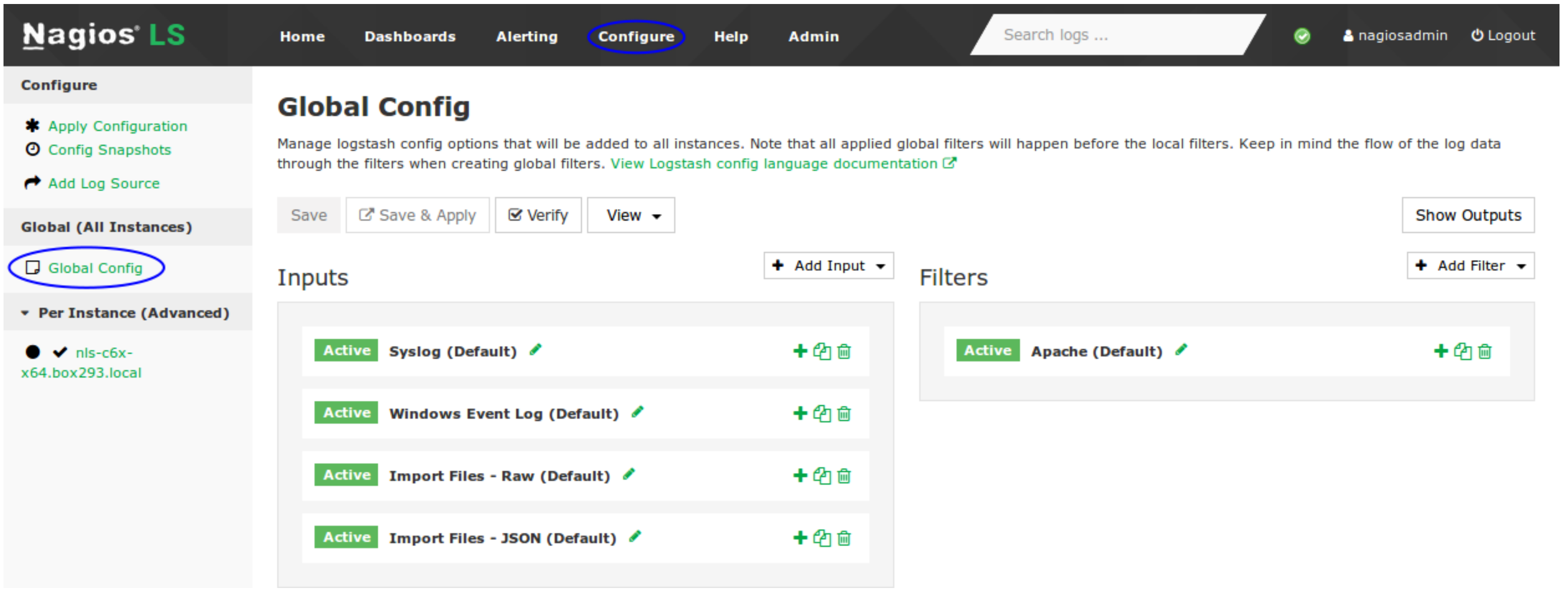
- UDP 514
- TCP 1514
- It has been observed by customers that the UDP 514 port is a better method to use. It was found that ESXi servers can stop sending logs using TCP 1514 when Nagios Log Server configuration is applied and does not automatically start sending them again.
- To use UDP 514 you will need to configure your Nagios Log Server to Listen On Privileged Ports

## Create Input UDP 514

As previously stated, to use UDP 514 you will need to configure your Nagios Log Server to Listen On Privileged Ports.

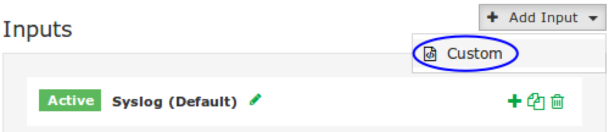
If you already have an Input for UDP 514 then you will need skip this and read the Advanced Config section.

Login to Nagios Log Server and navigate to **Configure** > **Global (All Instances)** > **Global Config**.



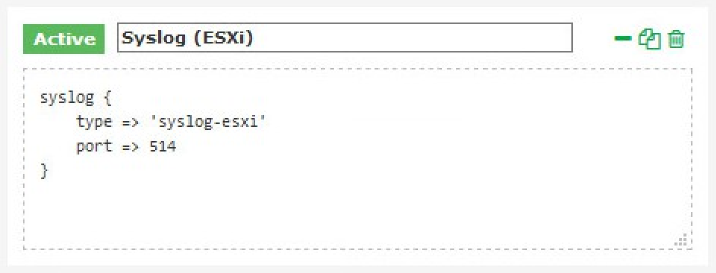
Manage logstash config options that will be added to all instances. Note that all applied global filters will happen before the local filters. Keep in mind the flow of the log data through the filters when creating global filters. View Logstash config language documentation

Click the **+ Add Input** button and select **Custom**.



## Sending ESXi Logs To Nagios Log Server

A new block will appear at the bottom of the list of Inputs.



Active Syslog (ESXi)

```
syslog {
    type => 'syslog-esxi'
    port => 514
}
```

Type a unique **name** for the input which will be **`Syslog (ESXi)`**.

In the text area field enter the following code (you can copy and paste):

```
syslog {
     type => 'syslog-esxi'
     port => 514
}
```

Click the **Save & Apply** button to create this input and apply the configuration.

You also need to create a firewall rule to allow the incoming UDP traffic. Establish a terminal session to your Nagios Log Server and execute the following commands (depending on your operating system version):

### RHEL | CentOS | CentOS Stream | Oracle Linux

```
firewall-cmd --zone=public --add-port=514/udp
firewall-cmd --zone=public --add-port=514/udp --permanent
```

**Debian:**

The local firewall is not enabled on Debian by default and no steps are required here. **IF** it is enabled then the commands are:

```
iptables -I INPUT -p udp --destination-port 514 -j ACCEPT
```

**Ubuntu:**

The local firewall is not enabled on Ubuntu by default and no steps are required here. **IF** it is enabled then the commands are:

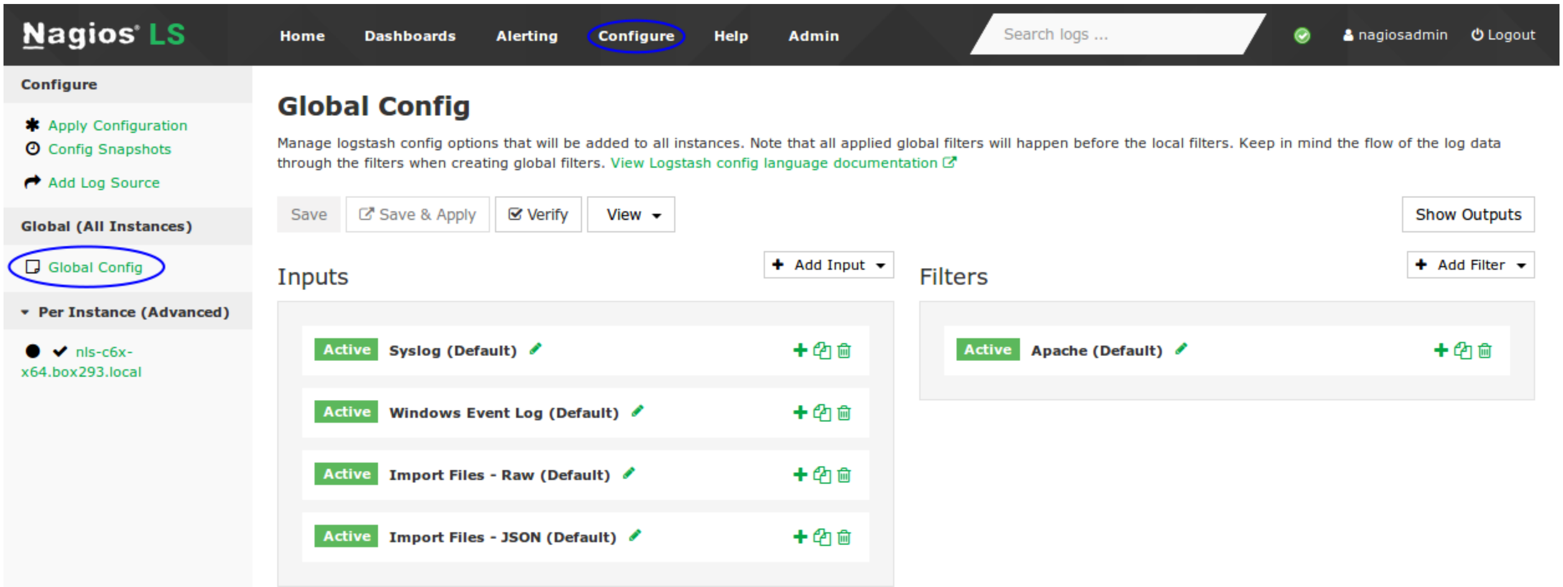
```
sudo ufw allow 514/udp
sudo ufw reload
```

You can now proceed to the Configure ESXi section.

## Create Input TCP 1514

If you already have an Input for TCP 1514 then you will need skip this and read the Advanced Config section.

Login to Nagios Log Server and navigate to **Configure** > **Global (All Instances)** > **Global Config**.

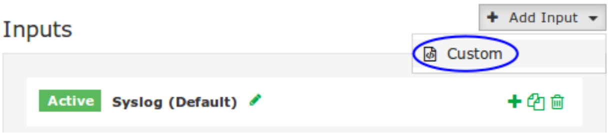


Global Config

Manage logstash config options that will be added to all instances. Note that all applied global filters will happen before the local filters. Keep in mind the flow of the log data through the filters when creating global filters. View Logstash config language documentation

Inputs:
- Active Syslog (Default)
- Active Windows Event Log (Default)
- Active Import Files - Raw (Default)
- Active Import Files - JSON (Default)

Filters:
- Active Apache (Default)

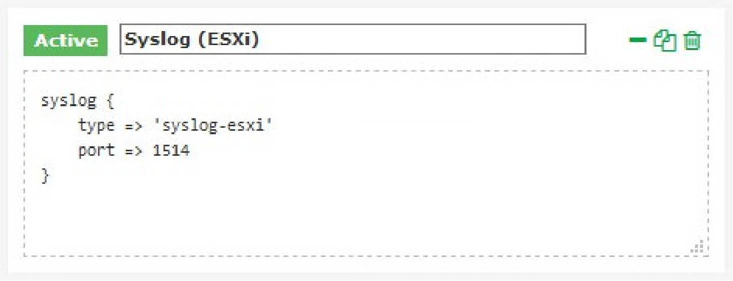


Click the **+ Add Input** button and select **Custom**.

A new block will appear at the bottom of the list of Inputs.

Type a unique **name** for the input which will be `Syslog (ESXi)`. In the text area field enter the following code (you can copy and paste):

```
syslog {
     type => 'syslog-esxi'
     port => 1514
}
```



```
syslog {
    type => 'syslog-esxi'
    port => 1514
}
```

Click the **Save & Apply** button to create this input and apply the configuration.

You also need to create a firewall rule to allow the incoming TCP traffic. Establish a terminal session to your Nagios Log Server and execute the following commands (depending on your operating system version):

### RHEL | CentOS | CentOS Stream | Oracle Linux

```
firewall-cmd --zone=public --add-port=1514/tcp
firewall-cmd --zone=public --add-port=1514/tcp --permanent
```

**Debian:**

The local firewall is not enabled on Debian by default and no steps are required here. **IF** it is enabled then the commands are:

```
iptables -I INPUT -p udp --destination-port 1514 -j ACCEPT
```

**Ubuntu:**

The local firewall is not enabled on Ubuntu by default and no steps are required here. **IF** it is enabled then the commands are:

```
sudo ufw allow 1514/udp
sudo ufw reload
```

You can now proceed to the Configure ESXi section.

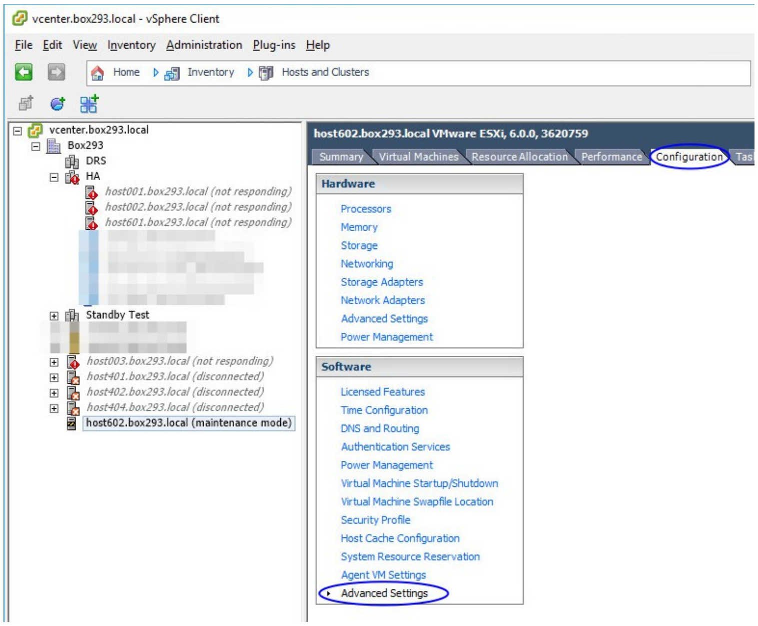
## Configure ESXi

Open the vSphere Client to the ESXi server (can be done through vCenter).

Select the **ESXi host** in the inventory pane.

Click the **Configuration** tab on the right.

Under **Software** click **Advanced Settings**.


vcenter.box293.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Hosts and Clusters
vcenter.box293.local
Box293
DRS
HA
host001.box293.local (not responding)
host002.box293.local (not responding)
host601.box293.local (not responding)
[redacted]
Standby Test
[redacted]
host003.box293.local (not responding)
host401.box293.local (disconnected)
host402.box293.local (disconnected)
host404.box293.local (disconnected)
host602.box293.local (maintenance mode)
host602.box293.local VMware ESXi, 6.0.0, 3620759
Summary
Virtual Machines
Resource Allocation
Performance
Configuration
Tas
Hardware
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Power Management
Virtual Machine Startup/Shutdown
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
System Resource Reservation
Agent VM Settings
Advanced Settings

Expand **Syslog** and click **global**.

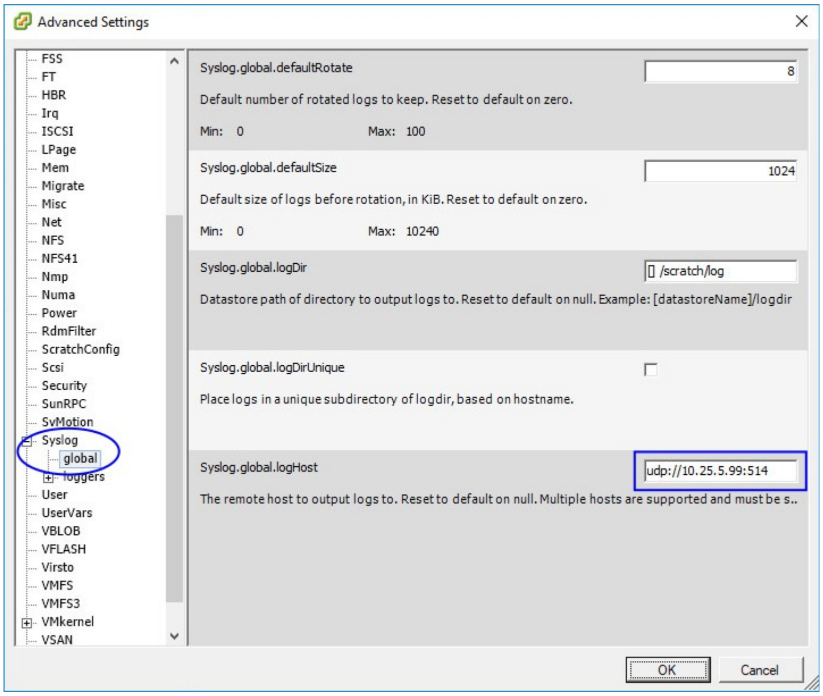
For UDP 514 change **Syslog.global.logHost** to:

```
udp://xxx.xxx.xxx.xxx:514
```

For TCP 1514 change **Syslog.global.logHost** to:

```
tcp://xxx .xxx.xxx.xxx:1514
```

Where `xxx.xxx.xxx.xxx` is the IP Address of your Nagios Log Server.



Syslog.global.defaultRotate: 8
Default number of rotated logs to keep. Reset to default on zero.
Min: 0 Max: 100

Syslog.global.defaultSize: 1024
Default size of logs before rotation, in KiB. Reset to default on zero.
Min: 0 Max: 10240

Syslog.global.logDir: [] /scratch/log
Datastore path of directory to output logs to. Reset to default on null. Example: [datastoreName]/logdir

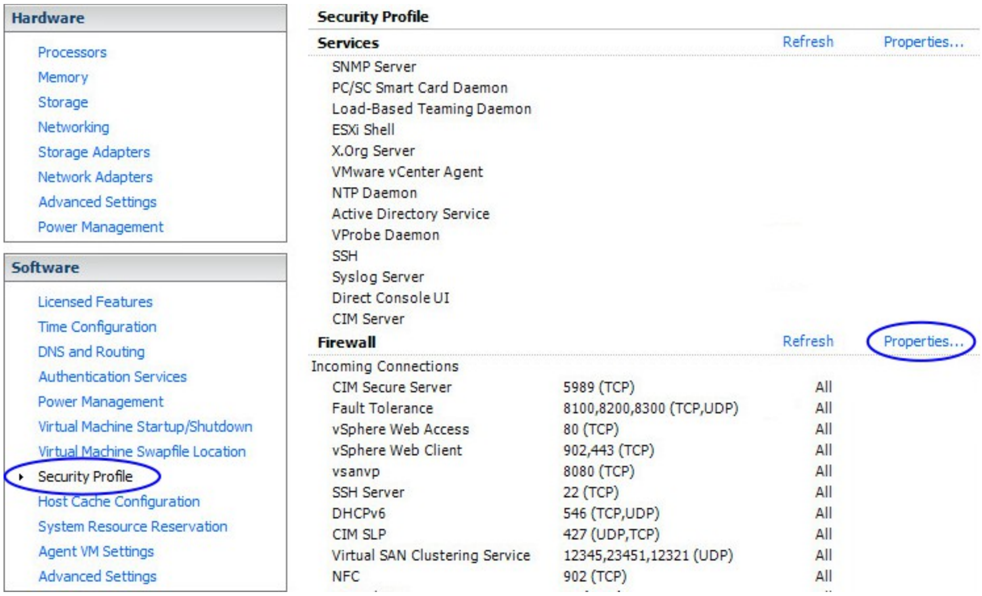
Syslog.global.logDirUnique: □
Place logs in a unique subdirectory of logdir, based on hostname.

Syslog.global.logHost: udp://10.25.5.99:514
The remote host to output logs to. Reset to default on null. Multiple hosts are supported and must be s..

Click **OK**.

Under **Software** click **Security Profile**.

For **Firewall** click **Properties**.



Services:
SNMP Server
PC/SC Smart Card Daemon
Load-Based Teaming Daemon
ESXi Shell
X.Org Server
VMware vCenter Agent
NTP Daemon
Active Directory Service
VProbe Daemon
SSH
Syslog Server
Direct Console UI
CIM Server

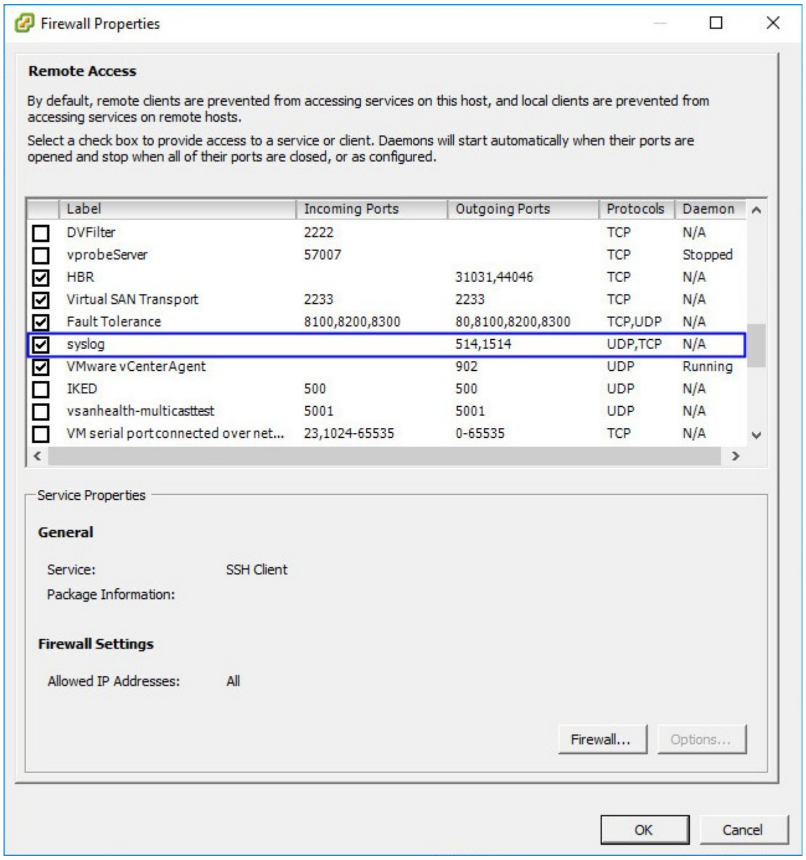
Incoming Connections

| | | |
|---|---|---|
| CIM Secure Server | 5989 (TCP) | All |
| Fault Tolerance | 8100,8200,8300 (TCP,UDP) | All |
| vSphere Web Access | 80 (TCP) | All |
| vSphere Web Client | 902,443 (TCP) | All |
| vsanvp | 8080 (TCP) | All |
| SSH Server | 22 (TCP) | All |
| DHCPv6 | 546 (TCP,UDP) | All |
| CIM SLP | 427 (UDP,TCP) | All |
| Virtual SAN Clustering Service | 12345,23451,12321 (UDP) | All |
| NFC | 902 (TCP) | All |

Find **syslog** and **Tick** the box.

Click **OK**.

This completes the steps required on the ESXi server.



Firewall Properties

**Remote Access**

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

Select a check box to provide access to a service or client. Daemons will start automatically when their ports are opened and stop when all of their ports are closed, or as configured.

| | Label | Incoming Ports | Outgoing Ports | Protocols | Daemon |
|---|---|---|---|---|---|
| ☐ | DVFilter | 2222 | | TCP | N/A |
| ☐ | vprobeServer | 57007 | | TCP | Stopped |
| ☑ | HBR | | 31031,44046 | TCP | N/A |
| ☑ | Virtual SAN Transport | 2233 | 2233 | TCP | N/A |
| ☑ | Fault Tolerance | 8100,8200,8300 | 80,8100,8200,8300 | TCP,UDP | N/A |
| ☑ | syslog | | 514,1514 | UDP,TCP | N/A |
| ☑ | VMware vCenterAgent | | 902 | UDP | Running |
| ☐ | IKED | 500 | 500 | UDP | N/A |
| ☐ | vsanhealth-multicasttest | 5001 | 5001 | UDP | N/A |
| ☐ | VM serial port connected over net... | 23,1024-65535 | 0-65535 | TCP | N/A |

Service Properties

**General**

Service: SSH Client

Package Information:

**Firewall Settings**

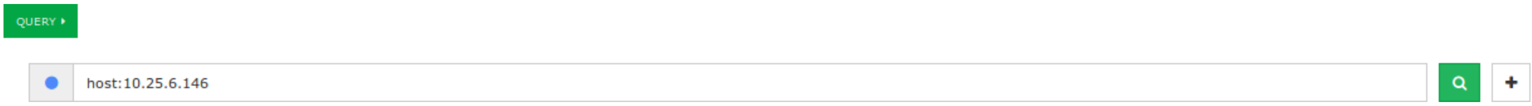
Allowed IP Addresses: All

## Check Nagios Log Server

To confirm that Nagios Log Server is receiving data from the ESXi server navigate to the **Dashboards** page.

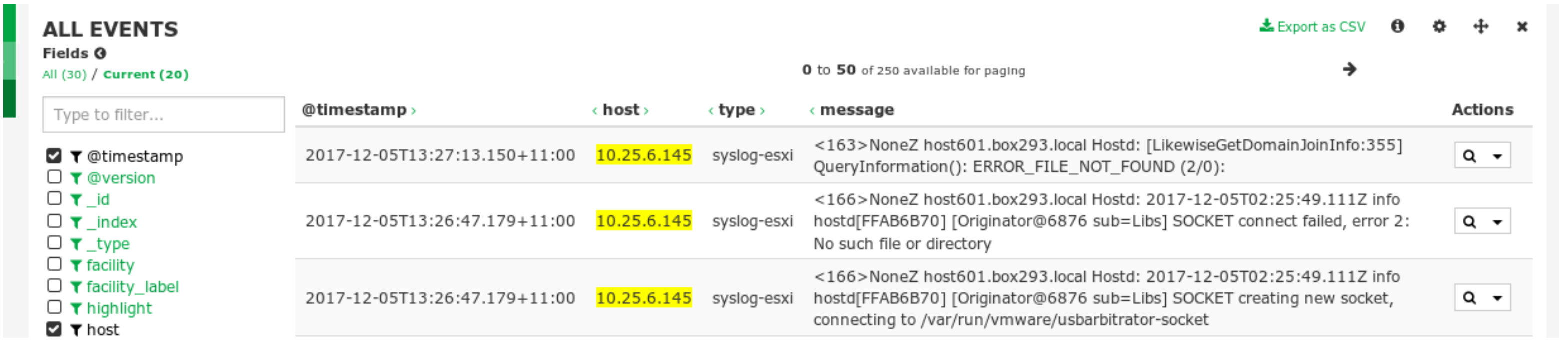
Perform a **Query** on the host field using the **IP Address** of your **ESXi** host:

```
host:<ESXi Host Address>
```



host:10.25.6.146

You should see results appear in the ALL EVENTS panel.



ALL EVENTS

Fields

All (30) / Current (20)

Type to filter...

- ☑ @timestamp
- ☐ @version
- ☐ _id
- ☐ _index
- ☐ _type
- ☐ facility
- ☐ facility_label
- ☐ highlight
- ☑ host

0 to 50 of 250 available for paging

| @timestamp | host | type | message | Actions |
|---|---|---|---|---|
| 2017-12-05T13:27:13.150+11:00 | 10.25.6.145 | syslog-esxi | <163>NoneZ host601.box293.local Hostd: [LikewiseGetDomainJoinInfo:355] QueryInformation(): ERROR_FILE_NOT_FOUND (2/0): | |
| 2017-12-05T13:26:47.179+11:00 | 10.25.6.145 | syslog-esxi | <166>NoneZ host601.box293.local Hostd: 2017-12-05T02:25:49.111Z info hostd[FFAB6B70] [Originator@6876 sub=Libs] SOCKET connect failed, error 2: No such file or directory | |
| 2017-12-05T13:26:47.179+11:00 | 10.25.6.145 | syslog-esxi | <166>NoneZ host601.box293.local Hostd: 2017-12-05T02:25:49.111Z info hostd[FFAB6B70] [Originator@6876 sub=Libs] SOCKET creating new socket, connecting to /var/run/vmware/usbarbitrator-socket | |

If you are seeing these results then everything should be working correctly.

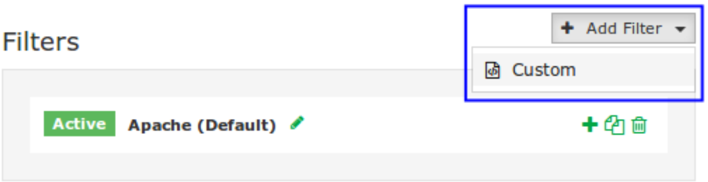
## Advanced Configuration

If you already have an existing SYSLOG input for UDP 514 or TCP 1514 then you will also need to define a filter that defines the `type` as `syslog-esxi` for the received ESXi logs. The reason behind this is because the ESXi syslog date format may be slightly different to that of other syslog data received. This causes problems with the indices created every day by Elasticsearch, ultimately resulting in Elasticsearch dropping the log data and not storing it in the database.

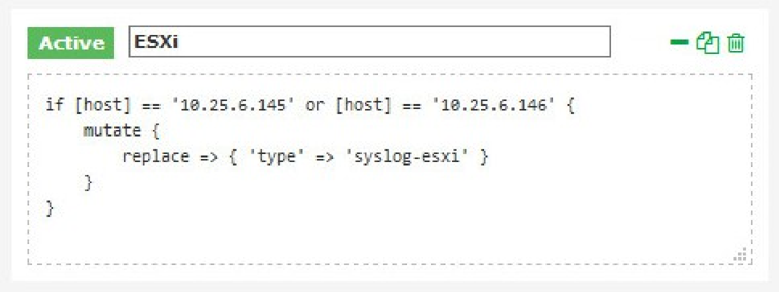
The filter you are going to create requires that the addresses of all ESXi hosts sending syslogs to Nagios Log Server be defined as part of the filter. This example will use the addresses `10.25.6.145` and `10.25.6.146`.

In Nagios Log Server and navigate to **Configure** > **Global (All Instances)** > **Global Config**.

Click the **+ Add Filter** button and select **Custom**.



A new block will appear at the bottom of the list of filters.



ESXi

```
if [host] == '10.25.6.145' or [host] == '10.25.6.146' {
    mutate {
        replace => { 'type' => 'syslog-esxi' }
    }
}
```

Type a unique **name** for the filter which will be **`ESXi`**.

In the text area field enter the following code (you can copy and paste):

```
if [host] == '10.25.6.145' or [host] == '10.25.6.146' {
    mutate {
        replace => { 'type' => 'syslog-esxi' }
    }
}
```

For every ESXi host you will be receiving logs from you will need to add an additional `or [host] == 'xxx.xxx.xxx.xxx'` condition.

Click the **Save & Apply** button to create this filter and apply the configuration. Once the configuration has been applied you should proceed to the Configure ESXi section.

## Finishing Up

This completes the documentation on how sending ESXi logs to Nagios Log Server.
If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb