Sending ESXi Logs to NLS 2024

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:

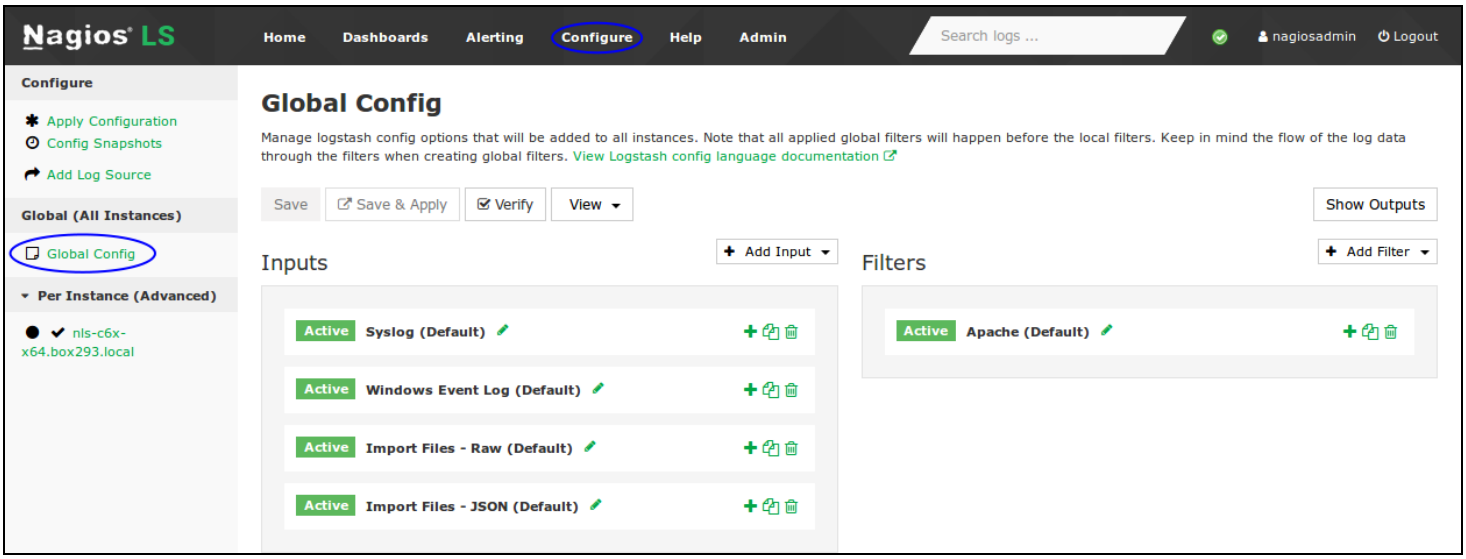
- UDP 514
- TCP 1514
- It has been observed by customers that the UDP 514 port is a better method to use. It was found that ESXi servers can stop sending logs using TCP 1514 when Nagios Log Server configuration is applied and does not automatically start sending them again.
- To use UDP 514 you will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

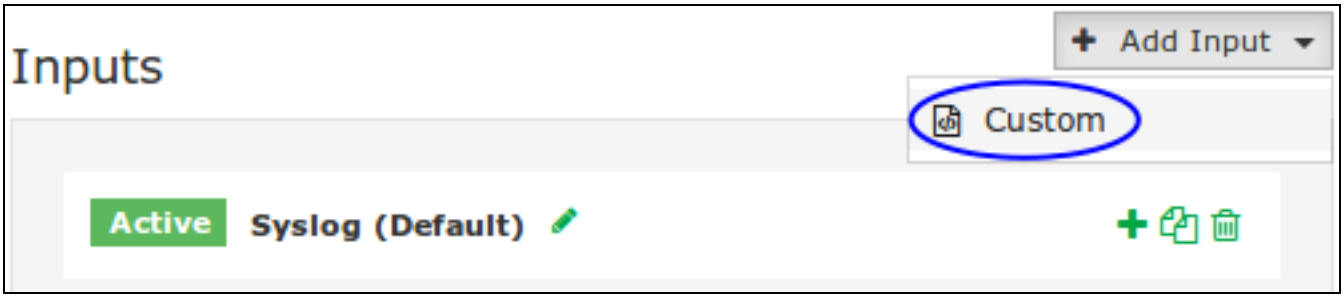
Create Input UDP 514

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

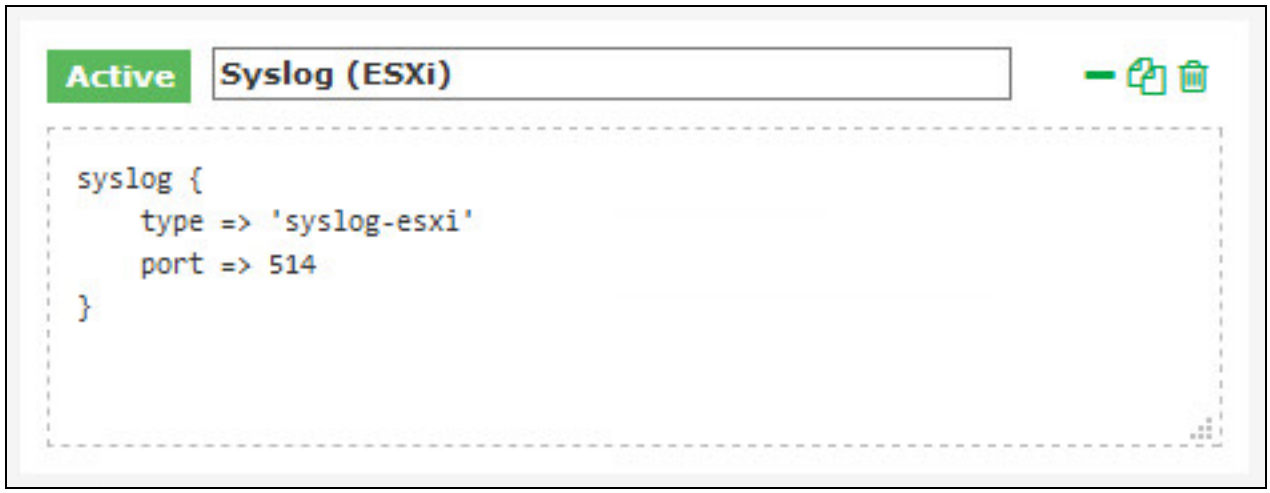
If you already have an Input for UDP 514 then you will need skip this and read the Advanced Config section.

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





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



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

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

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

```
syslog {
```

```
type => 'syslog-esxi'
```

```
port => 514
```

```
}
```

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

7. 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 | 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
```

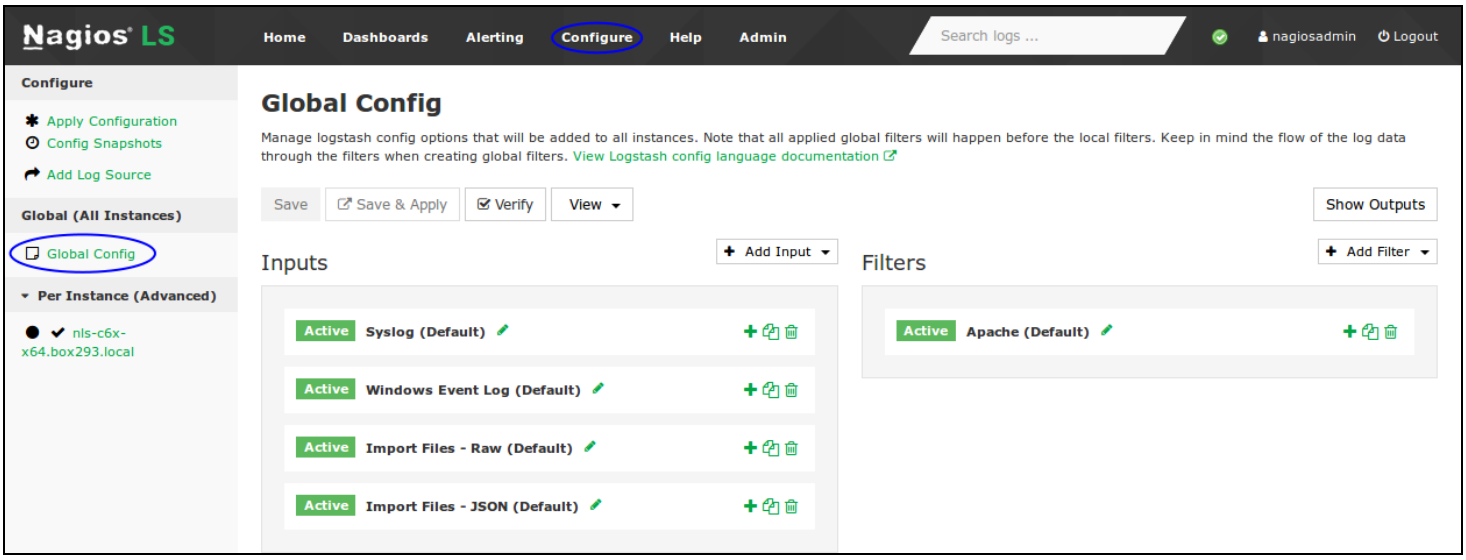
```
sudo ufw reload
```

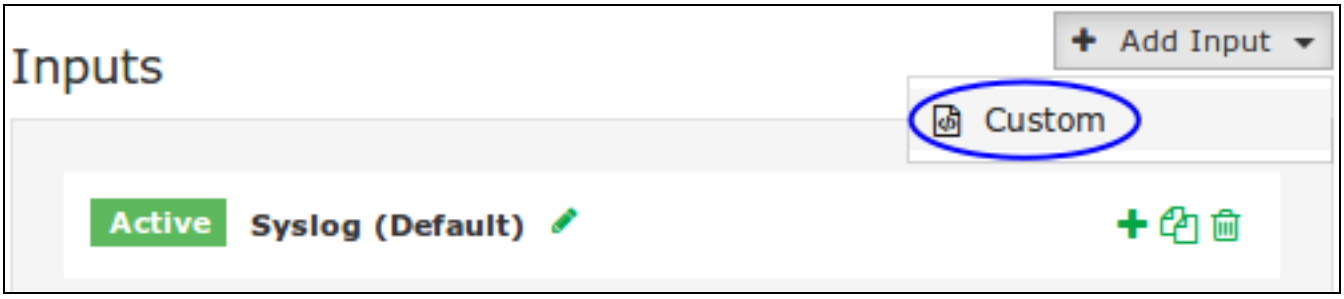
You can now proceed to the Configure ESXi section.

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.

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

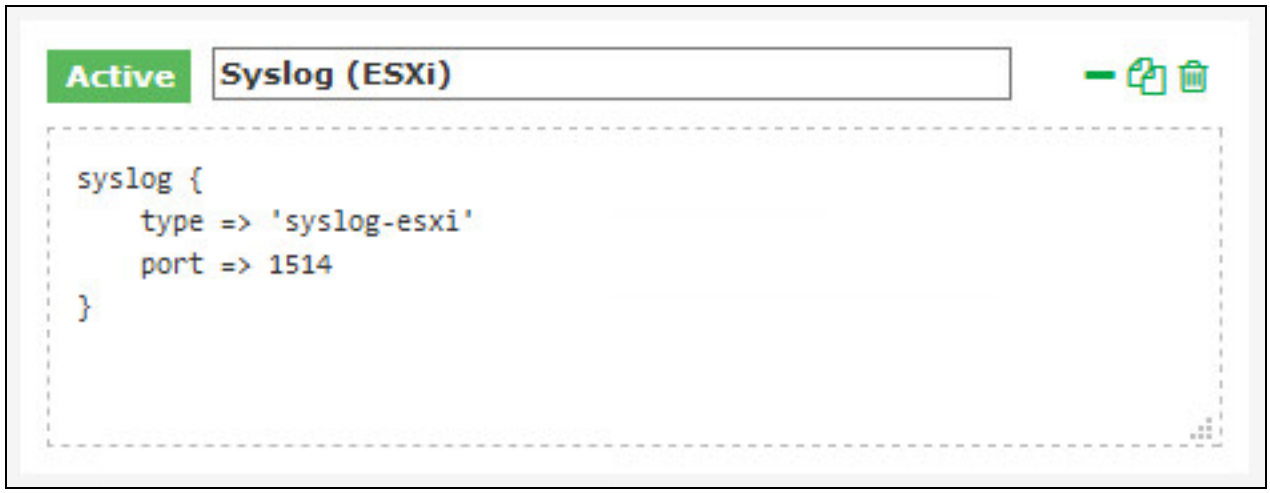




2. Click the + Add Input button and select Custom.

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

4. 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
```

```
}
```

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

6. 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 | 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:

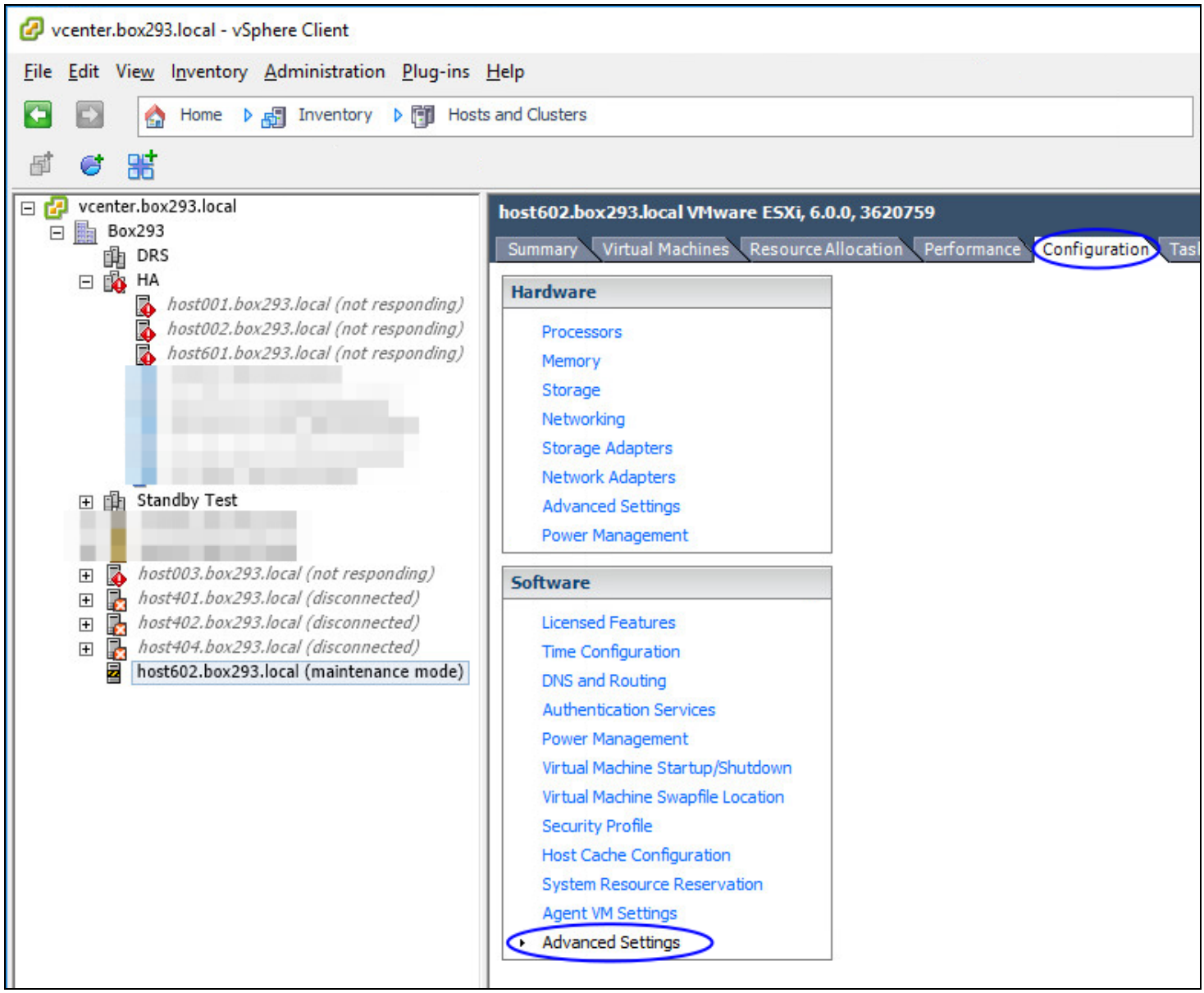
The local firewall is not enabled on Ubuntu by default and no steps are required here. IF it is enabled then the commands are:

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

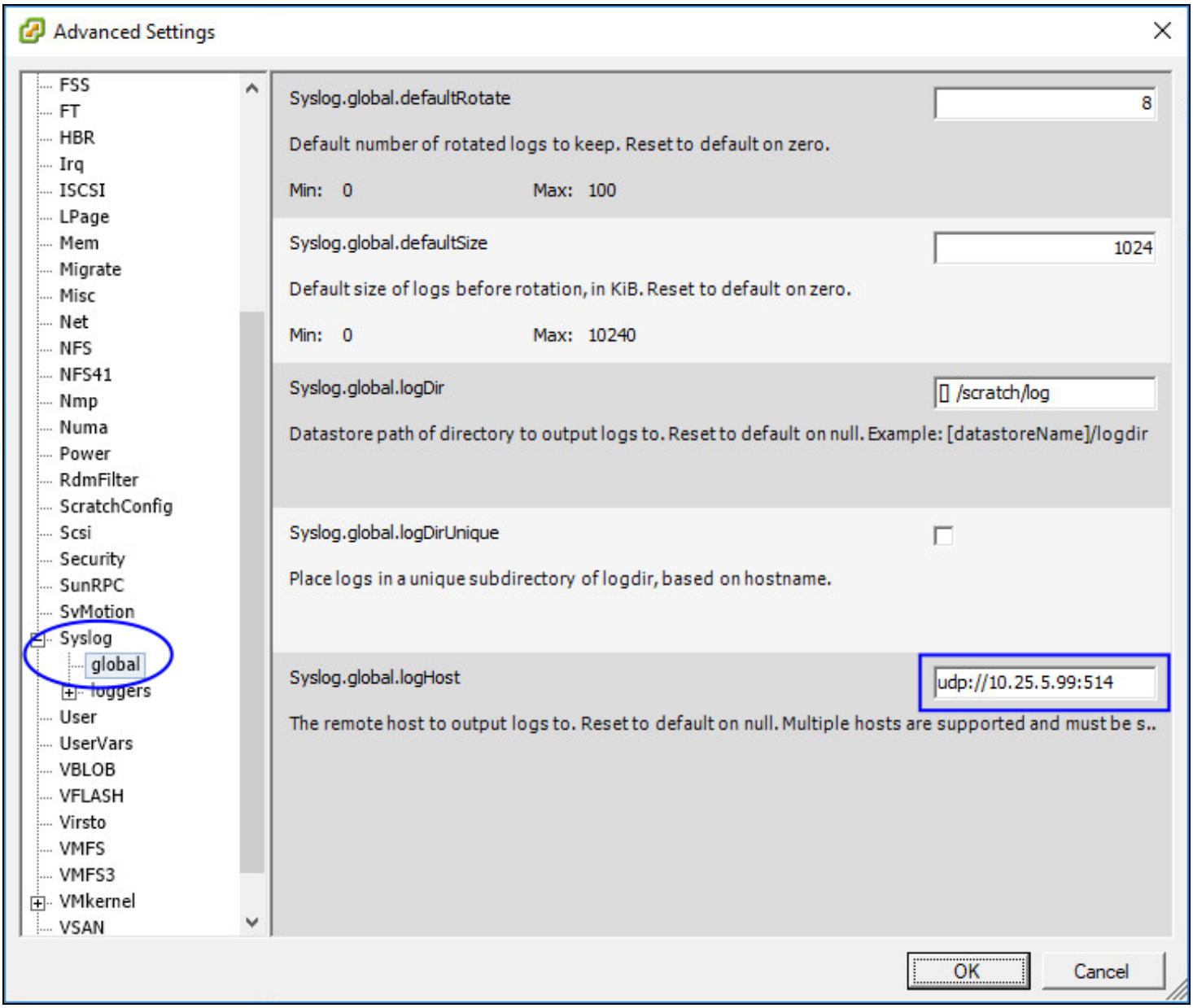
```
sudo ufw reload
```

You can now proceed to the Configure ESXi section.

Configure ESXi



1. Open the vSphere Client to the ESXi server (can be done through vCenter).
2. Select the ESXi host in the inventory pane.
3. Click the Configuration tab on the right.
4. Under Software click Advanced Settings.



5. Expand Syslog and click global.

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

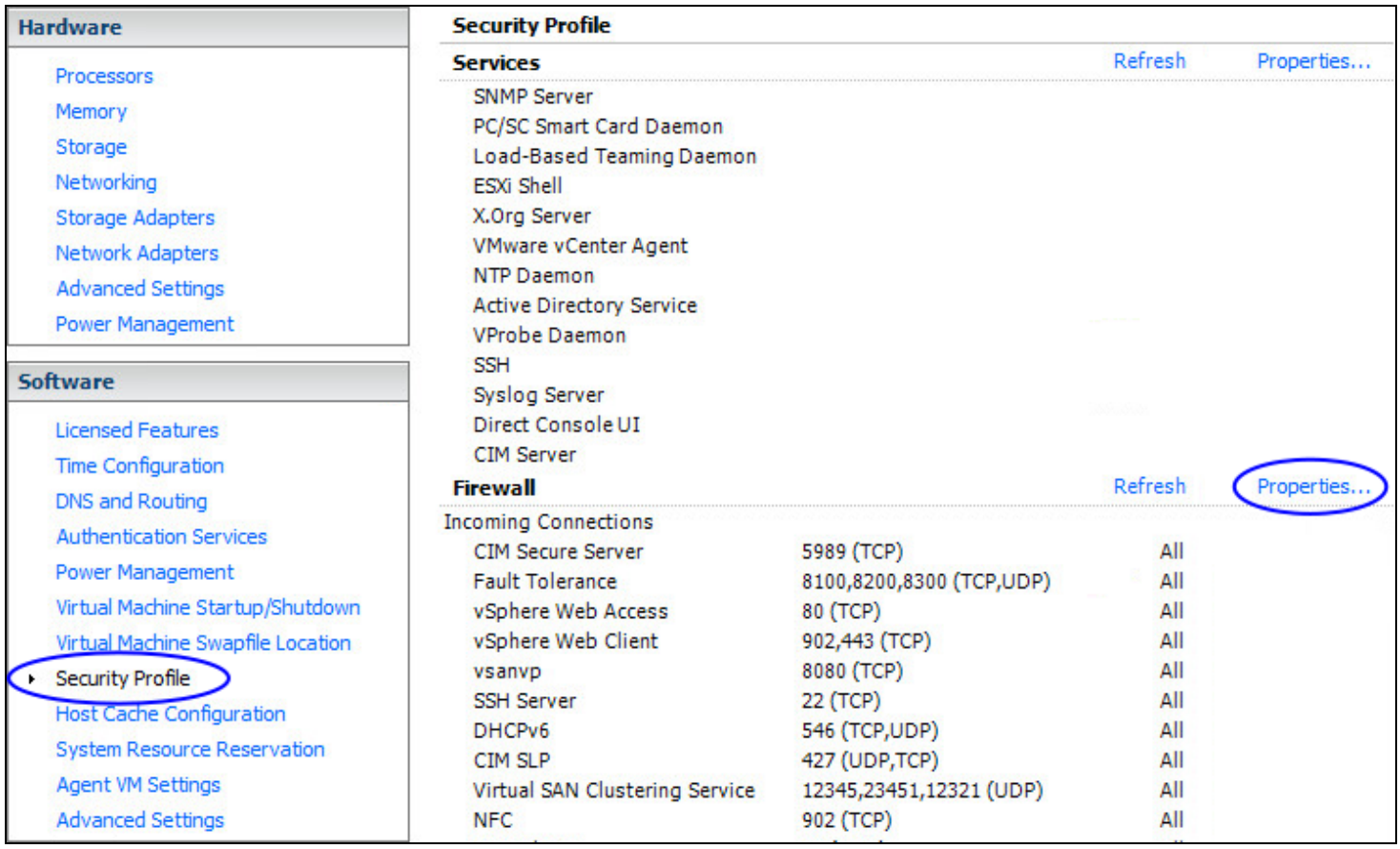
udp://xxx.xxx.xxx.xxx:514

7. 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.

8. Click OK.



Under Software click Security Profile.

For Firewall click Properties.

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 vCenter Agent		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

Firewall... Options...

OK Cancel

9. Find syslog and Tick the box.

10. Click OK.

This completes the steps required on the ESXi server.

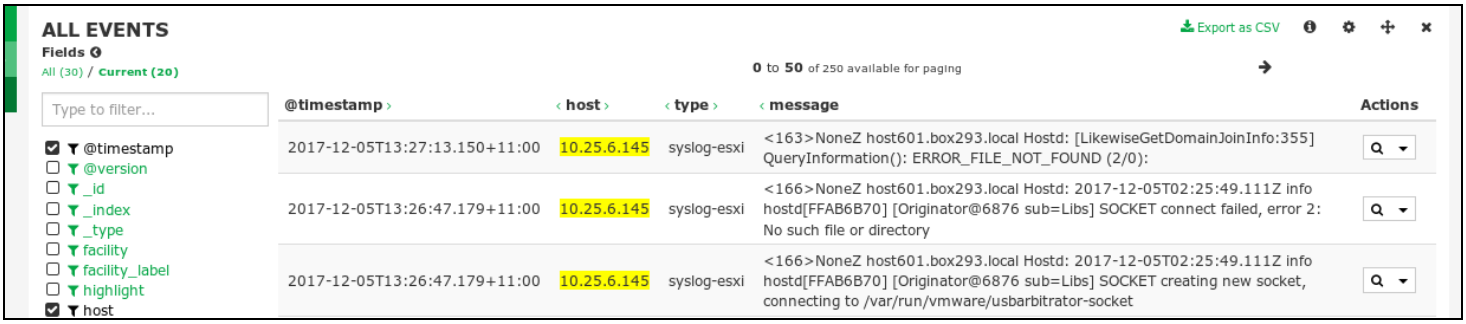
Check Nagios Log Server

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>

You should see results appear in the ALL EVENTS panel.



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

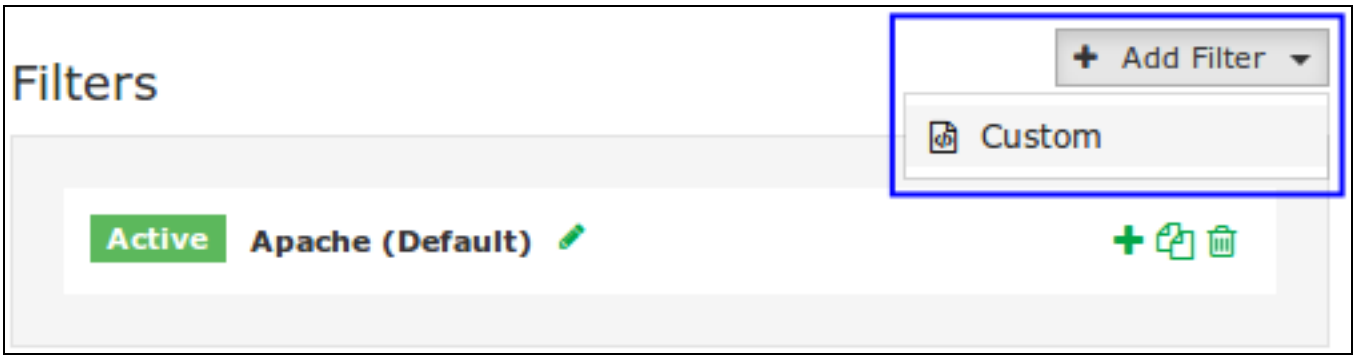
Advanced Configuration

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.

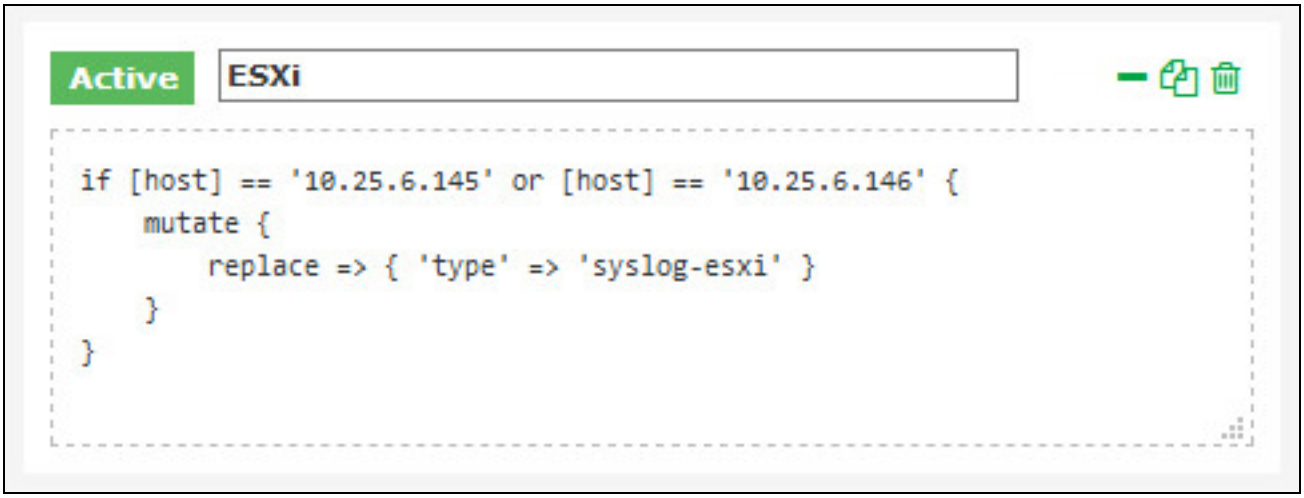
The filter you are going to create requires that the addresses of all ESXi hosts sending syslogs to Nagios Log Server be defined as part of the filter. This example will use the addresses 10.25.6.145 and 10.25.6.146.

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



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

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



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

5. 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.

6. 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.