How To Send ESXi Logs To Nagios Log Server 2024R2

Overview

These steps will walk you through:

- Creating an input for desired port to Nagios Log Server 2024R2
    - UDP 514
    - TCP 1514
- Configuring Firewall Rules on Nagios Log Server
- Configuring ESXi to send syslogs to Nagios Log Server

UDP 514 vs TCP 1514

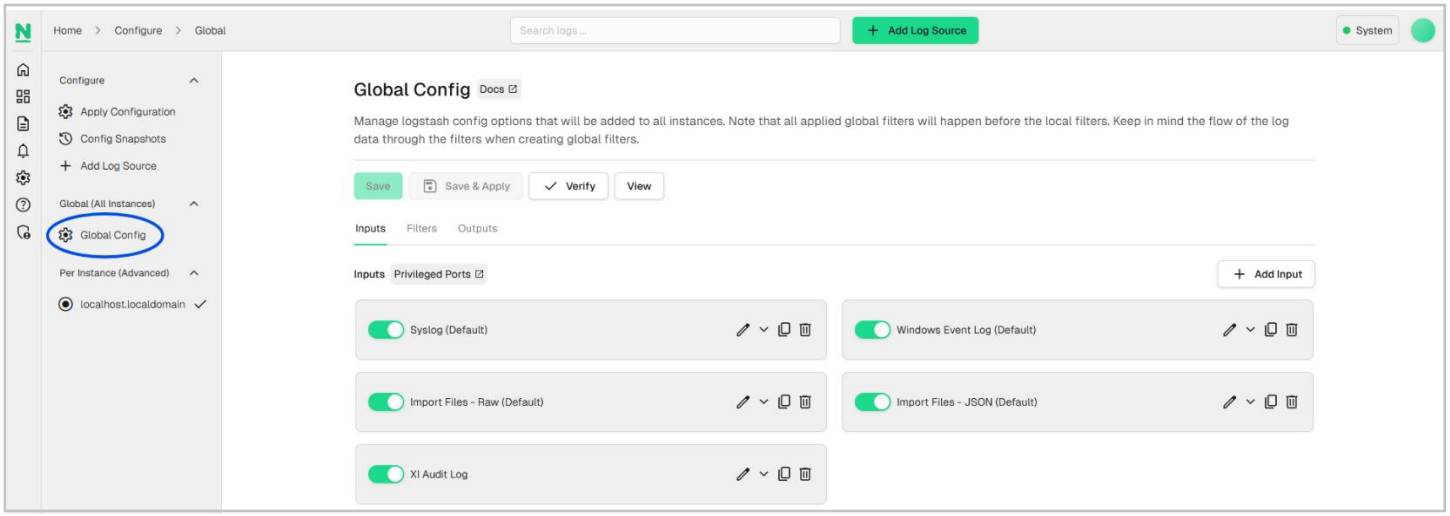
ESXi can send syslogs on two ports/protocols:

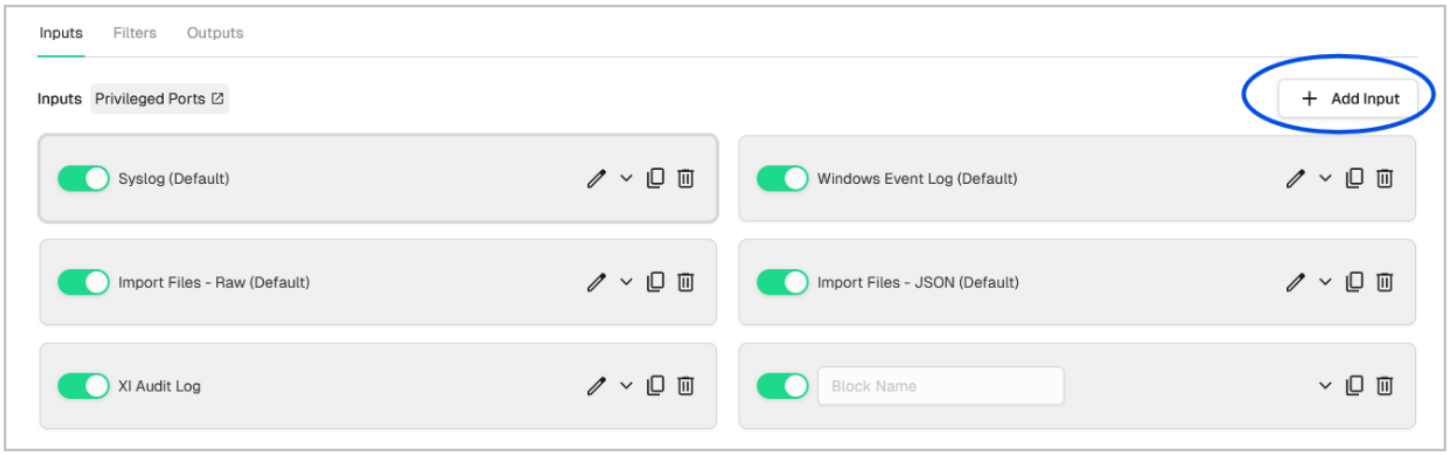
- UDP 514
- TCP 1514
- Customers have observed that the UDP 514 port is a better method to use. ESXi servers can sometimes stop sending logs using TCP 1514 when Nagios Log Server configuration is applied and does not automatically start sending them again.
- To use UDP 514 you will need to configure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

Create Input UDP 514

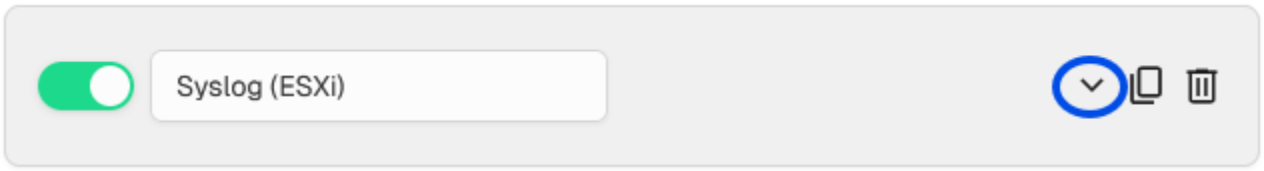
As previously stated, to use UDP 514 you will need to configure your Nagios Log Server to Listen On Privileged Ports. If you already have an Input for UDP 514, skip this to the Advanced Configuration section.

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





2. Click the **+ Add** Input button. A new block will appear at the bottom of the list of Inputs.



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

4. Click the down arrow, as shown in the screenshot above, to expand the input and reveal the text area.

5. In the text area field enter the following code, as seen in the screenshot above (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):
    a. **RHEL | CentOS | Oracle Linux**

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

    b. **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
```

    c. **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:

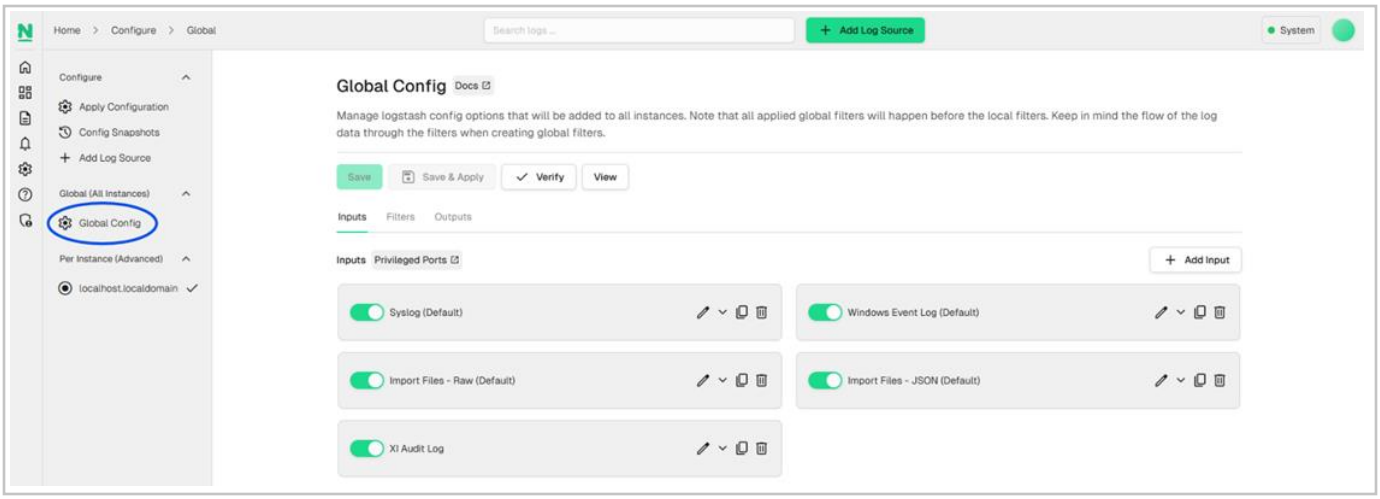
```
sudo ufw allow 514/udp
sudo ufw reload
```

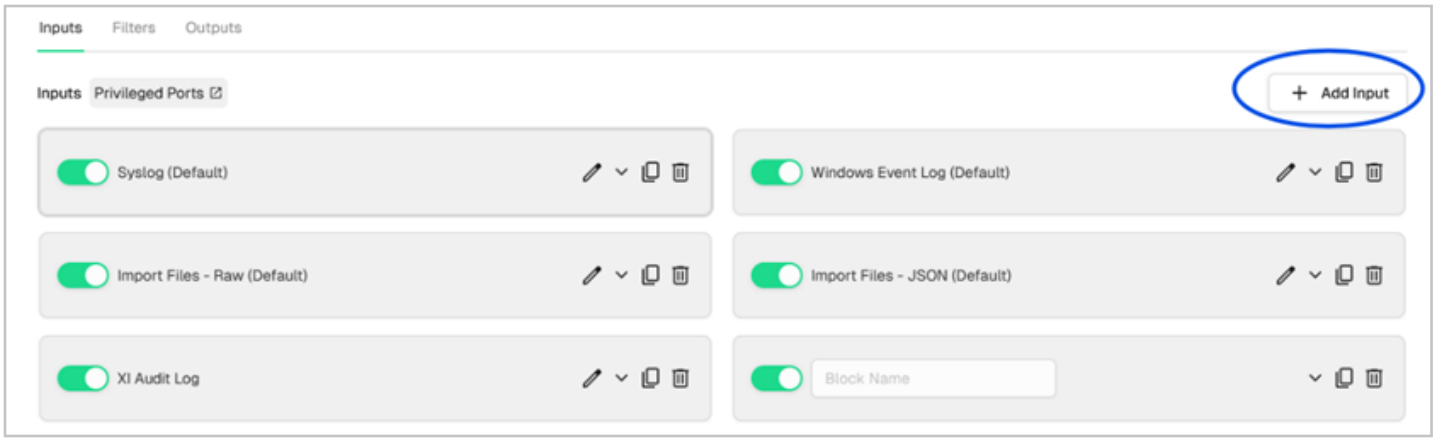
You can now proceed to the Configure ESXi section.

Create Input TCP 1514

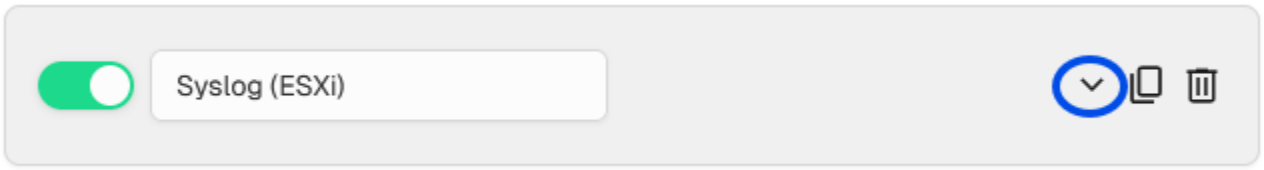
If you already have an Input for TCP 1514 then you will need skip this and read the Advanced Config section.

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





2. Click the **+ Add** Input button. A new block will appear at the bottom of the list of Inputs.



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

4. 4. Click the down arrow, as shown in the screenshot above, to expand the input and reveal the text area.
5. 5. In the text area field enter the following code, as seen in the screenshot above (you can copy and paste):


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

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 TCP traffic. Establish a terminal session to your Nagios Log Server and execute the following commands (depending on your operating system version):
    a. **RHEL | CentOS | Oracle Linux**

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

b. **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
```

c. **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.

ESXI Configuration

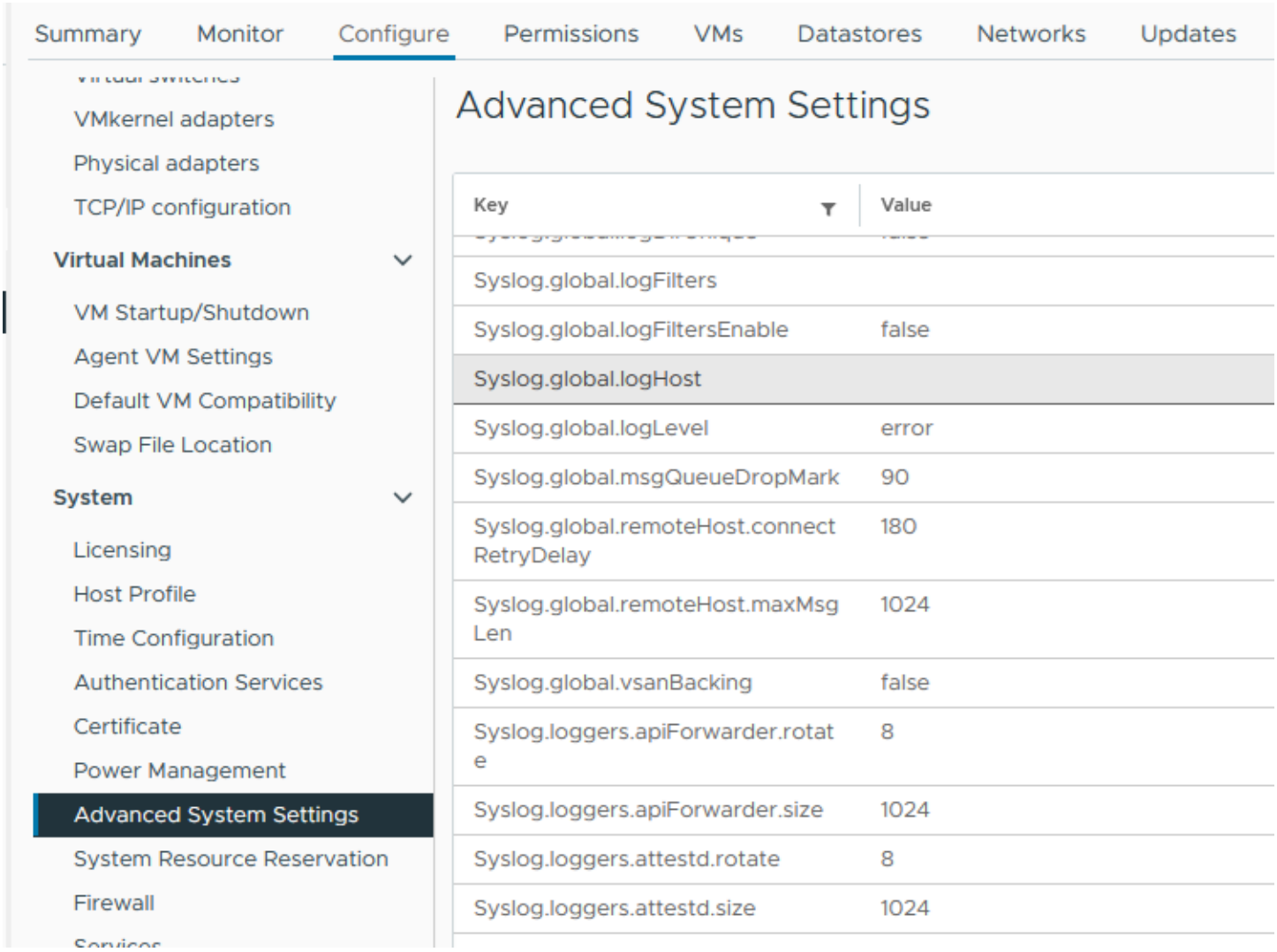
An ESXi host must be given the address of the Nagios Log Server, the port of the input, if the protocol(TCP or UDP) to use. These are in the ESXI host using a setting called **Syslog.global.logHost**.

The host must also allow outbound traffic to the remote machine.

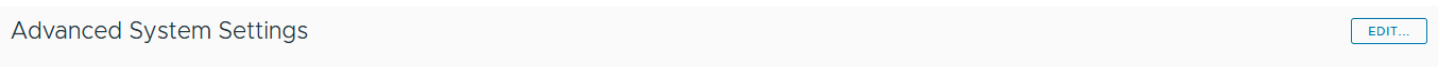
The sections below step through how to configure an ESXi host but note that these steps may vary depending on VMWare versions and VMWare documentation may need to be consulted.

Configure Syslog.global.logHost

1. Using the vSphere Client, locate the ESXI host that you wish to gather logs from, and go to **Configure > System > Advanced System Settings**.

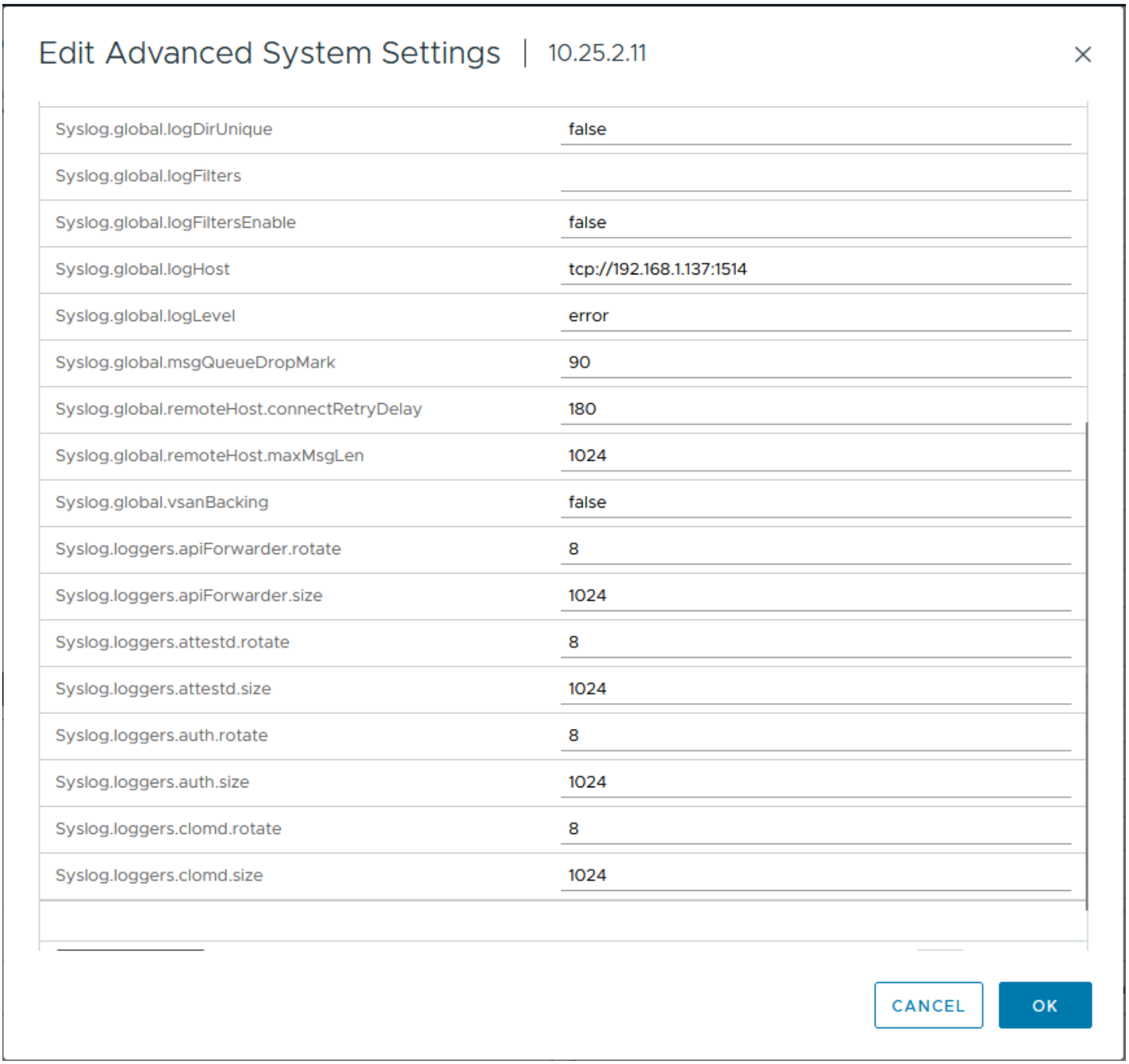


2. Click the **Edit**… button found toward the top right of the **Advanced System Settings** screen.



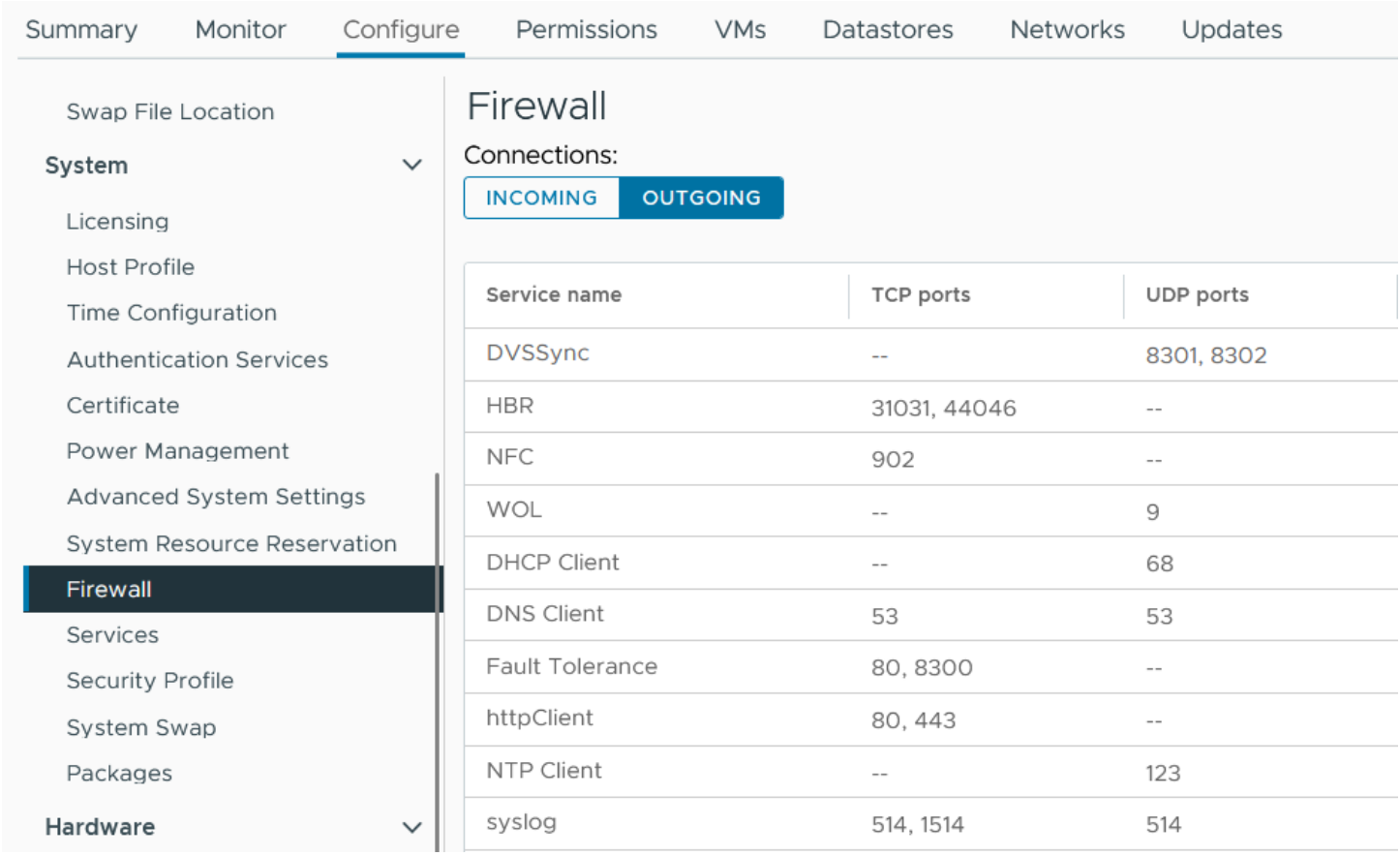
3. On the **Edit Advanced System Settings** window, locate the **Syslog.global.logHost** setting, and enter the information for the input that was configured on Nagios Log Server. The format is:

   ```
   protocol://address:port
   ```

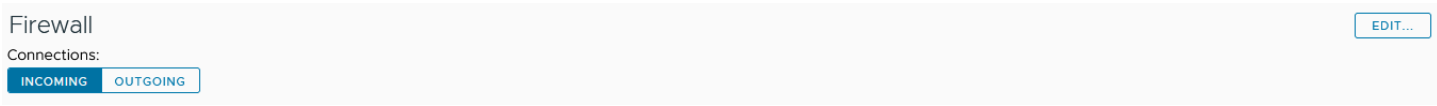


Allow Outbound Syslog Port

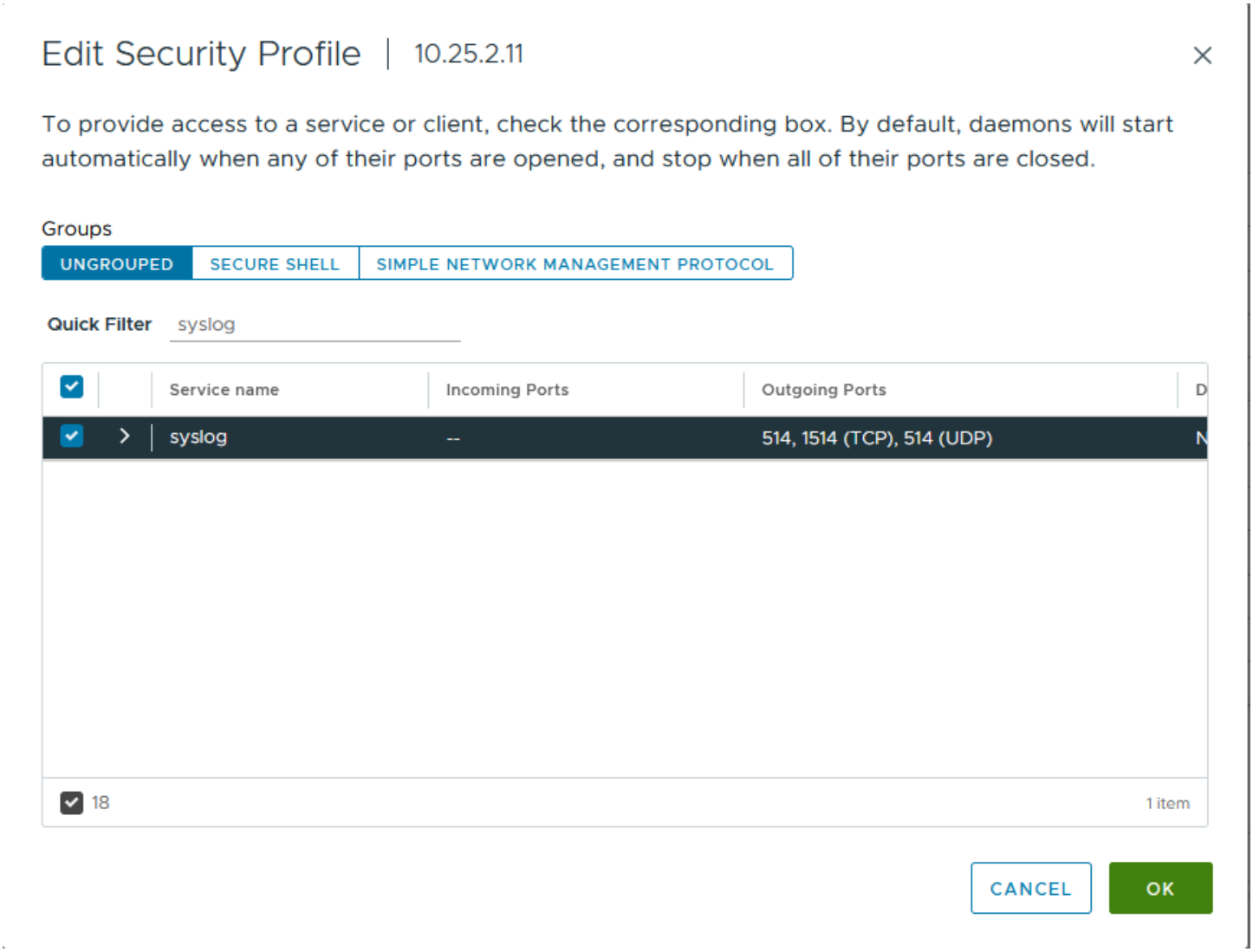
1. Navigate to **Configure > System > Firewall**, and click the **Edit…** button



2. Click the **Edit**… button found toward the top right of the **Firewall** screen.



3. Search for the syslog service on the **Edit Security Profile** window and click the checkbox to enable it.

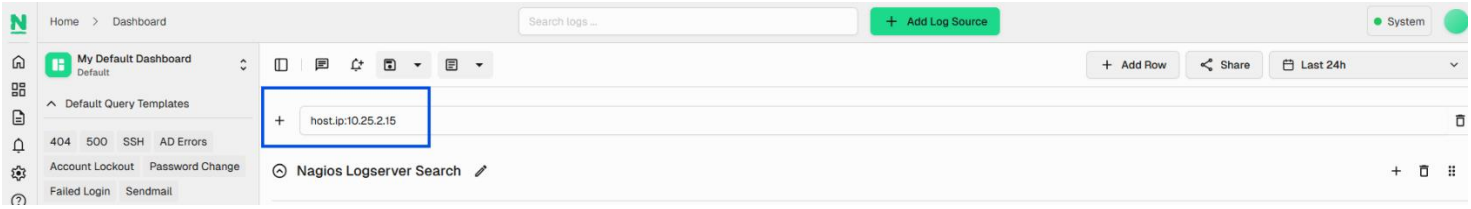


Check Nagios Log Server

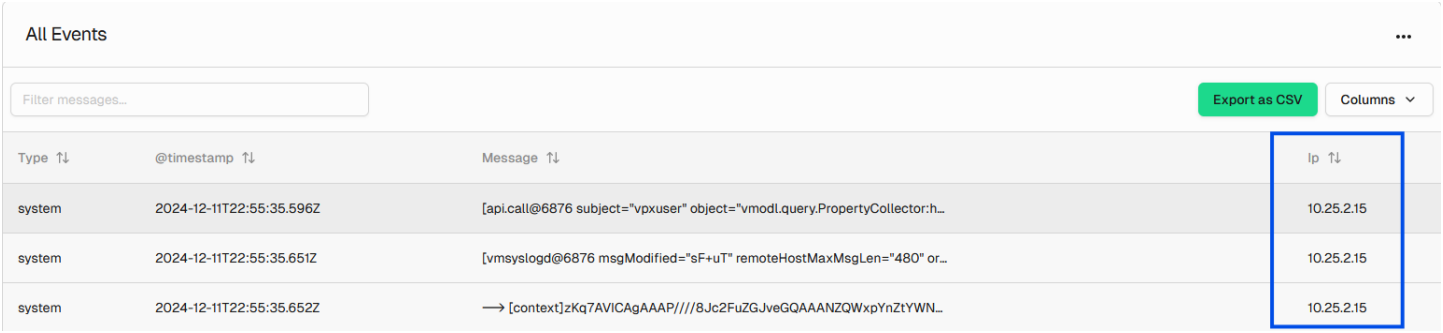
To confirm that Nagios Log Server is receiving data from the ESXi server navigate to the Dashboards page. Perform a Query on the host field using the IP Address of your ESXi host:

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

In our example this will look like this:



You should see results appear in the **All Events** panel.



If you see these results, everything should be working correctly.

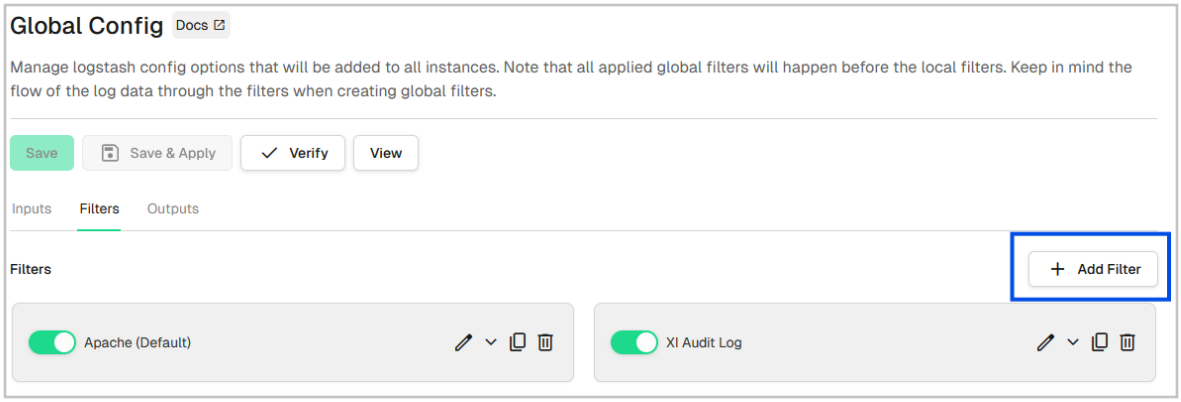
Advanced Configuration

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.

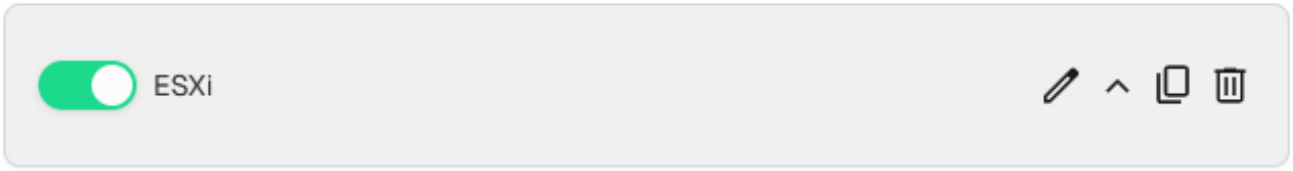
This is to ensure that the differences between ESXi syslog date formats match the format of other syslog data being stored in OpenSearch by Nagios Log Server

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 10.25.2.15 and 10.25.1.14. Replace these example IPs with the IP addresses of your own ESXi host.

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



2. Click the **+ Add Filter** button.
3. A new block will appear at the bottom of the list of filters.




```
if [host] == '10.25.2.15' or [host] == '10.25.2.14' {
   mutate {
      replace => { 'type' => 'syslog-esxi' }
   }
}
```

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, but be sure to replace the IP addresses with the actual IP addresses of your ESXI hosts):

```
if [host] == '10.25.2.15' or [host] == '10.25.2.14' {
     mutate {
          replace => { 'type' => 'syslog-esxi' }
     }
}
```

   Note: 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.

Finishing Up

This completes the documentation on How to Send ESXi Logs to Nagios Log Server 2024. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library