

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:

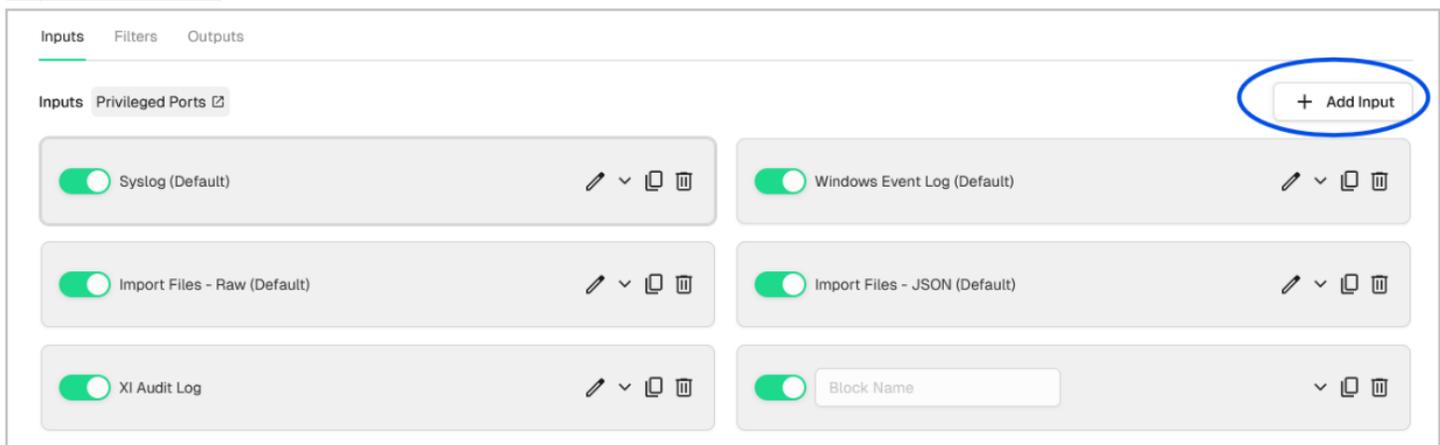
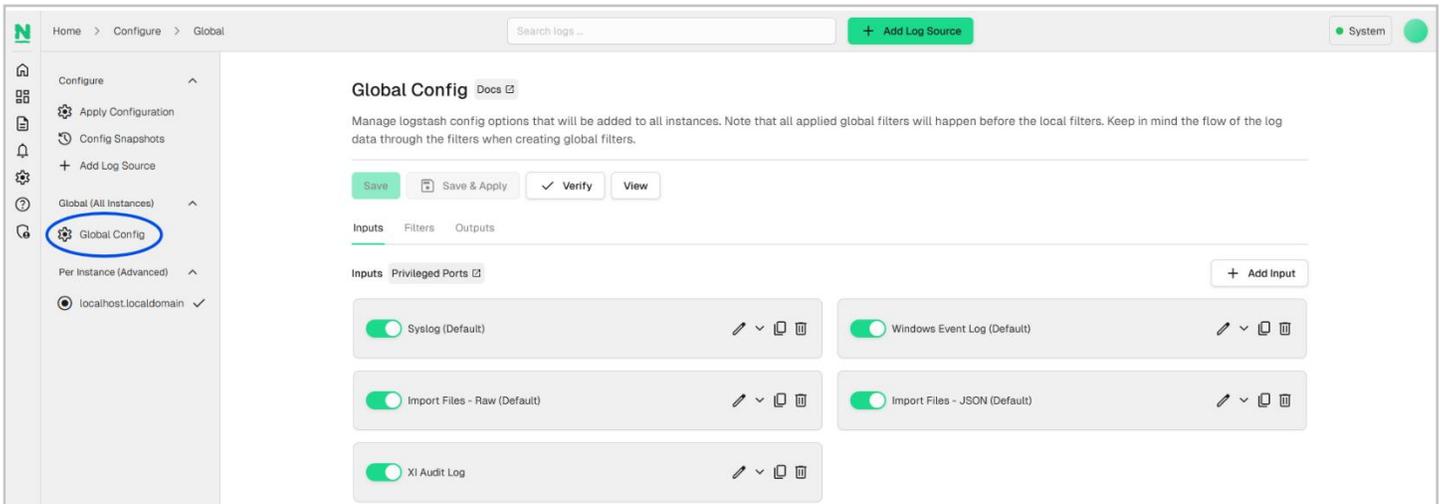
- UDP 514
- TCP 1514
- Customers have observed that the UDP 514 port is a better method to use. ESXi servers can sometimes stop sending logs using TCP 1514 when Nagios Log Server configuration is applied and does not automatically start sending them again.
- To use UDP 514 you will need to configure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

Create Input UDP 514

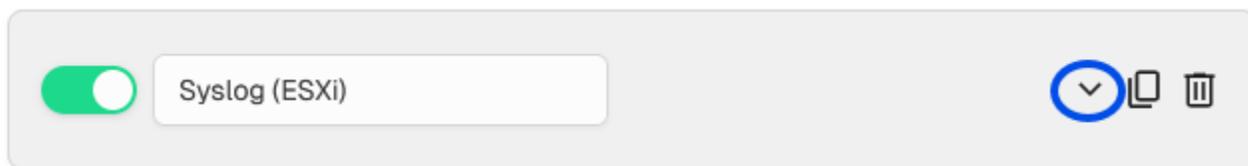
As previously stated, to use UDP 514 you will need to configure your Nagios Log Server to [Listen On Privileged Ports](#). If you already have an Input for UDP 514, skip this to the [Advanced Configuration](#) section.

How To Send ESXi Logs To Nagios Log Server 2024R2

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



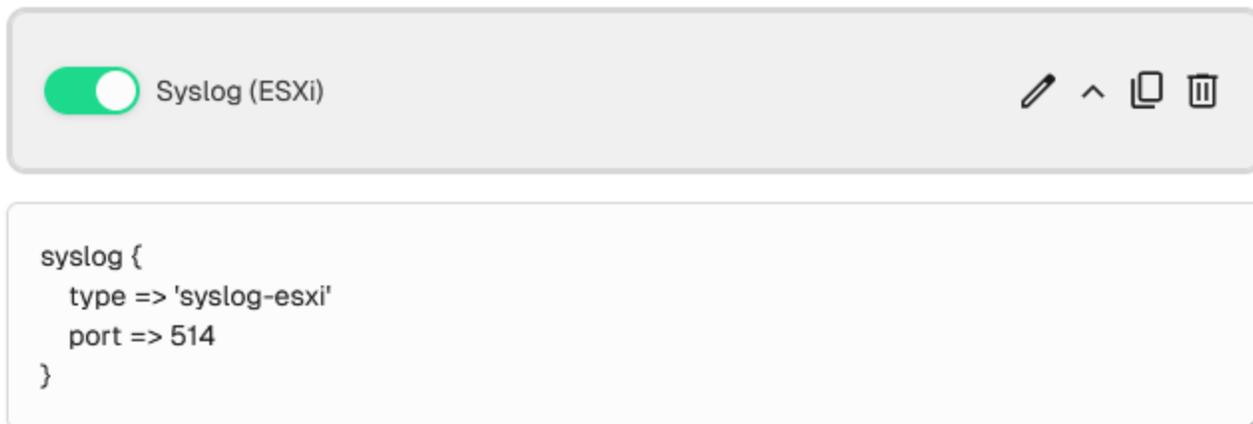
2. Click the **+ Add Input** button. A new block will appear at the bottom of the list of Inputs.



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

How To Send ESXi Logs To Nagios Log Server 2024R2

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.

How To Send ESXi Logs To Nagios Log Server 2024R2

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
```

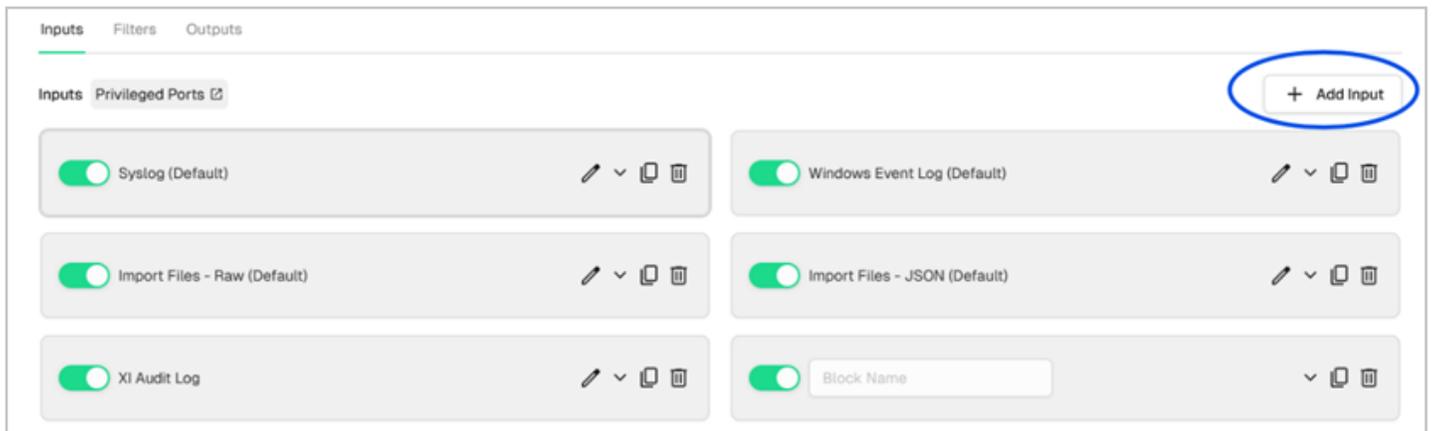
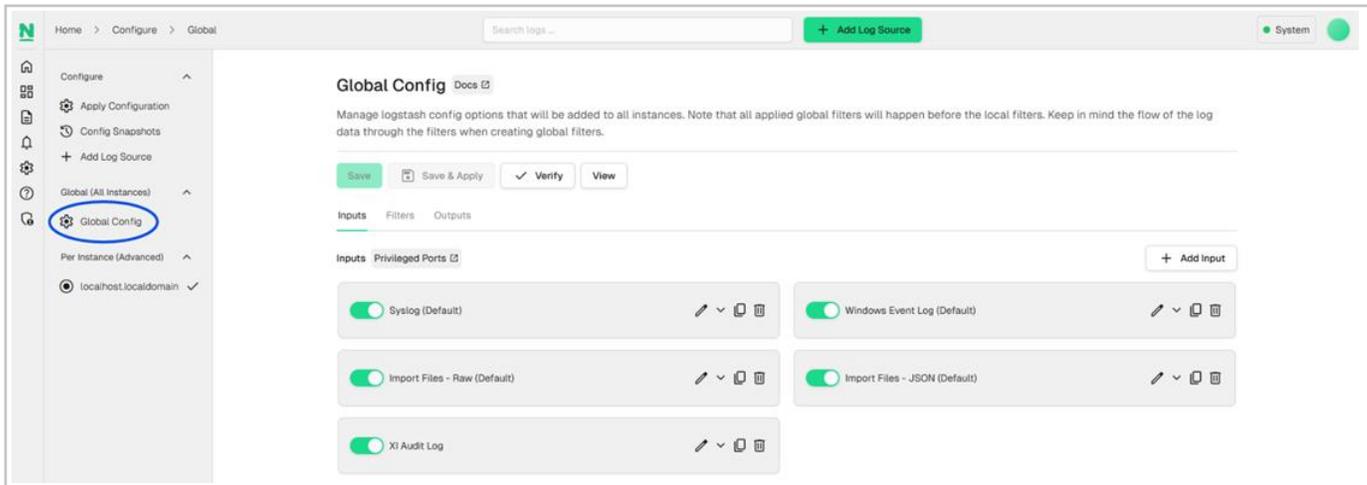
You can now proceed to the [Configure ESXi](#) section.

Create Input TCP 1514

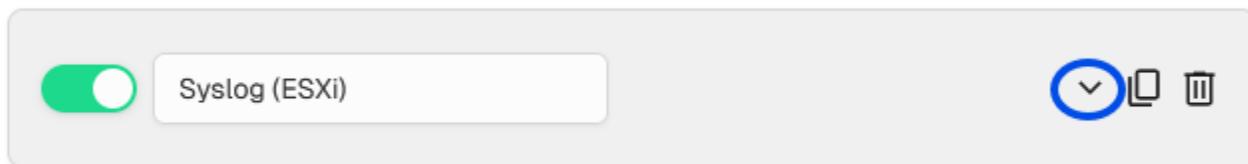
If you already have an Input for TCP 1514 then you will need skip this and read the [Advanced Config section](#).

How To Send ESXi Logs To Nagios Log Server 2024R2

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).

How To Send ESXi Logs To Nagios Log Server 2024R2

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 => 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
```

How To Send ESXi Logs To Nagios Log Server 2024R2

- 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.

How To Send ESXi Logs To Nagios Log Server 2024R2

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**.

Key	Value
Syslog.global.logFilters	
Syslog.global.logFiltersEnable	false
Syslog.global.logHost	
Syslog.global.logLevel	error
Syslog.global.msgQueueDropMark	90
Syslog.global.remoteHost.connectRetryDelay	180
Syslog.global.remoteHost.maxMsgLen	1024
Syslog.global.vsanBacking	false
Syslog.loggers.apiForwarder.rotate	8
Syslog.loggers.apiForwarder.size	1024
Syslog.loggers.attestd.rotate	8
Syslog.loggers.attestd.size	1024

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

Advanced System Settings

EDIT...

How To Send ESXi Logs To Nagios Log Server 2024R2

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

Edit Advanced System Settings | 10.25.2.11 ×

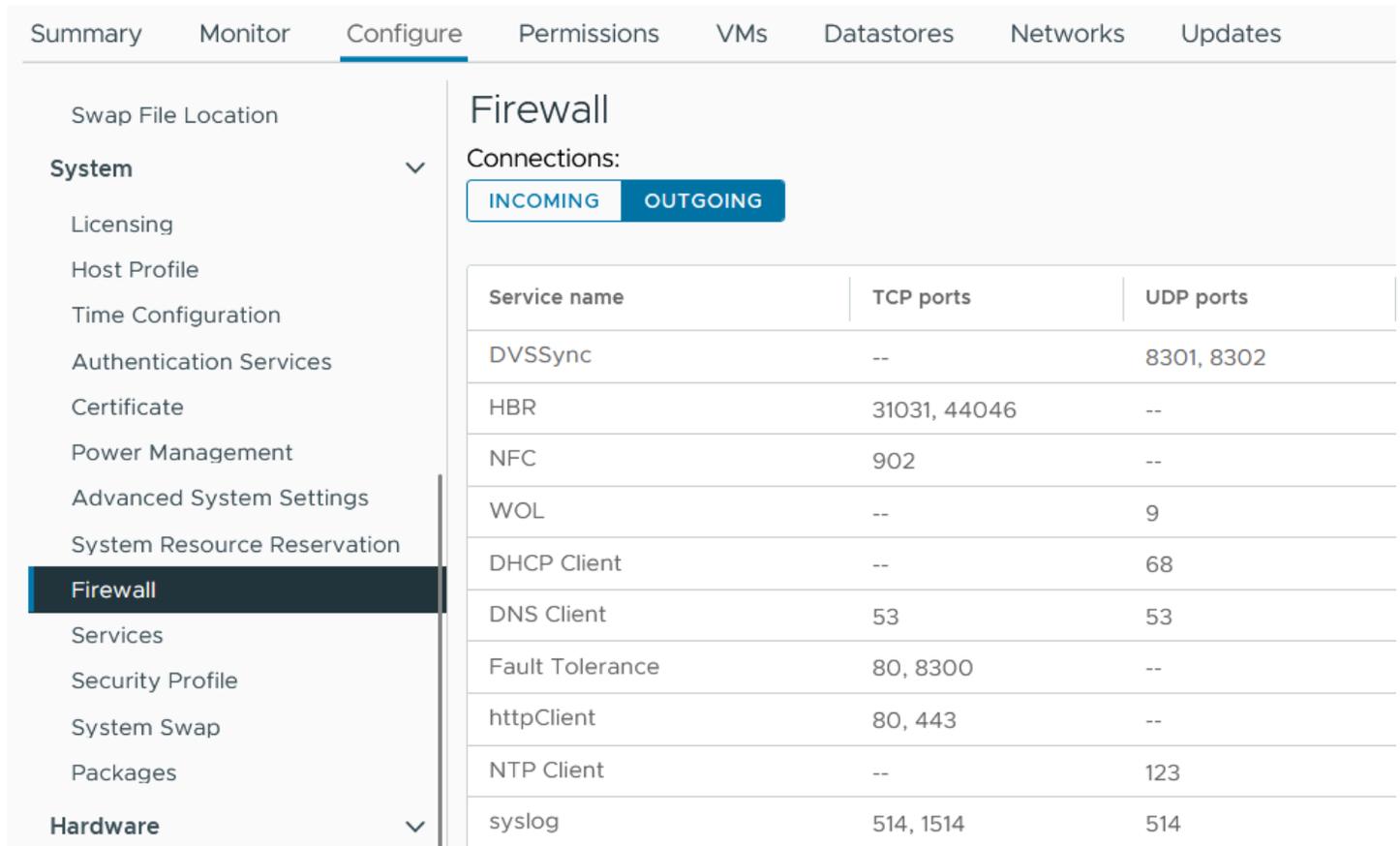
Syslog.global.logDirUnique	false
Syslog.global.logFilters	
Syslog.global.logFiltersEnable	false
Syslog.global.logHost	tcp://192.168.1.137:1514
Syslog.global.logLevel	error
Syslog.global.msgQueueDropMark	90
Syslog.global.remoteHost.connectRetryDelay	180
Syslog.global.remoteHost.maxMsgLen	1024
Syslog.global.vsanBacking	false
Syslog.loggers.apiForwarder.rotate	8
Syslog.loggers.apiForwarder.size	1024
Syslog.loggers.attestd.rotate	8
Syslog.loggers.attestd.size	1024
Syslog.loggers.auth.rotate	8
Syslog.loggers.auth.size	1024
Syslog.loggers.clomd.rotate	8
Syslog.loggers.clomd.size	1024

CANCEL OK

How To Send ESXi Logs To Nagios Log Server 2024R2

Allow Outbound Syslog Port

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



The screenshot shows the ESXi configuration interface for the Firewall. The 'Configure' tab is active, and the 'Firewall' section is selected in the left-hand navigation menu. The 'OUTGOING' tab is selected under 'Connections:'. A table lists various services and their associated ports.

Service name	TCP ports	UDP ports
DVSSync	--	8301, 8302
HBR	31031, 44046	--
NFC	902	--
WOL	--	9
DHCP Client	--	68
DNS Client	53	53
Fault Tolerance	80, 8300	--
httpClient	80, 443	--
NTP Client	--	123
syslog	514, 1514	514

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



This close-up screenshot shows the top right corner of the Firewall configuration page. The 'Firewall' title is visible, along with the 'Connections:' section where the 'OUTGOING' tab is selected. An 'EDIT...' button is located in the top right corner of the configuration area.

How To Send ESXi Logs To Nagios Log Server 2024R2

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

Edit Security Profile | 10.25.2.11



To provide access to a service or client, check the corresponding box. By default, daemons will start automatically when any of their ports are opened, and stop when all of their ports are closed.

Groups

UNGROUPED

SECURE SHELL

SIMPLE NETWORK MANAGEMENT PROTOCOL

Quick Filter

<input checked="" type="checkbox"/>	Service name	Incoming Ports	Outgoing Ports	D
<input checked="" type="checkbox"/>	> syslog	--	514, 1514 (TCP), 514 (UDP)	N

18 1 item

CANCEL

OK

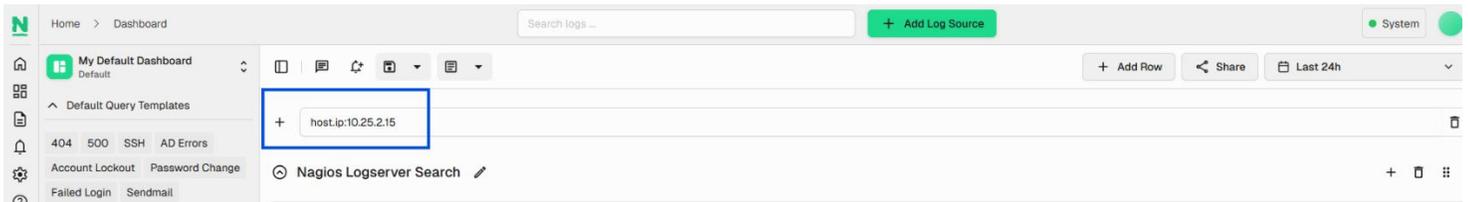
How To Send ESXi Logs To Nagios Log Server 2024R2

Check Nagios Log Server

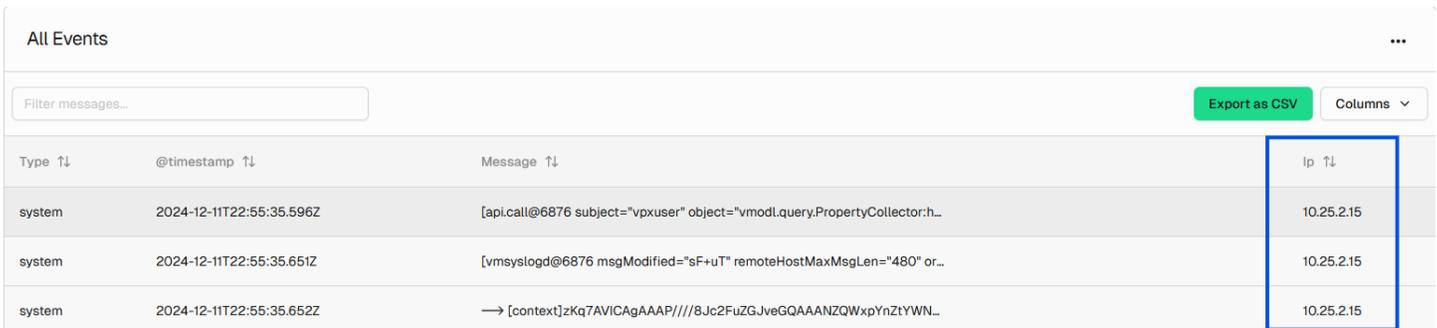
To confirm that Nagios Log Server is receiving data from the ESXi server navigate to the Dashboards page. Perform a Query on the host field using the IP Address of your ESXi host:

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

In our example this will look like this:



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

A screenshot of the 'All Events' panel in Nagios Log Server. It shows a table of search results for the query 'host.ip:10.25.2.15'. The table has columns for Type, @timestamp, Message, and Ip. The Ip column is highlighted with a blue box.

Type	@timestamp	Message	Ip
system	2024-12-11T22:55:35.596Z	[api.call@6876 subject="vpxuser" object="vmmodl.query.PropertyCollector:h...	10.25.2.15
system	2024-12-11T22:55:35.651Z	[vmsyslogd@6876 msgModified="sF+uT" remoteHostMaxMsgLen="480" or...	10.25.2.15
system	2024-12-11T22:55:35.652Z	→ [context]zKq7AVICAgAAAP/////8Jc2FuZGJveGQAAANZQWxpYnZlYWNL...	10.25.2.15

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

Advanced Configuration

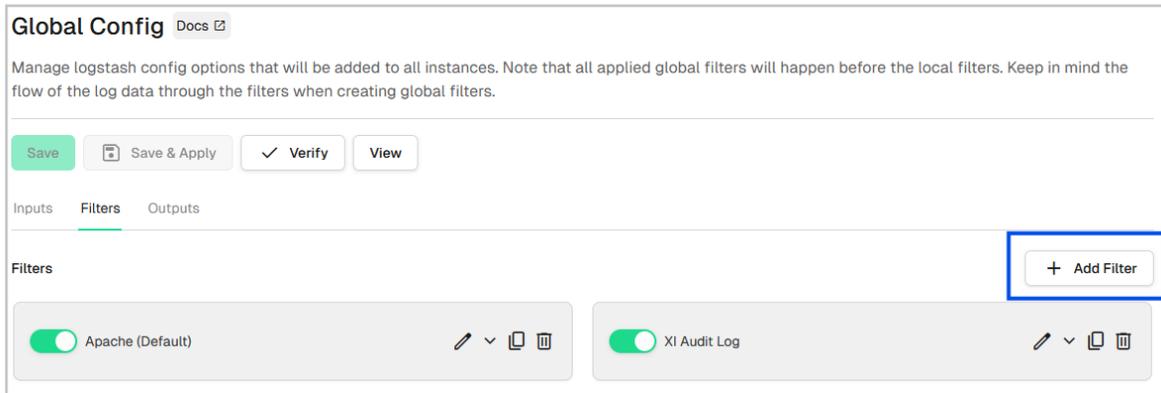
If you already have an existing SYSLOG input for UDP 514 or TCP 1514 then you will also need to define a filter that defines the type as syslog-esxi for the received ESXi logs.

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

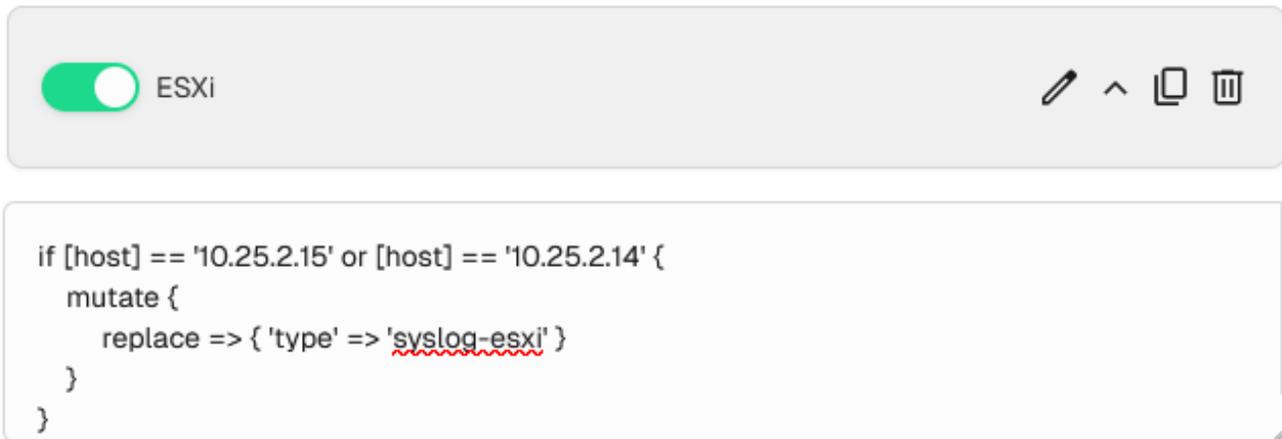
The filter you are going to create requires that the addresses of all ESXi hosts sending syslogs to Nagios Log Server be defined as part of the filter. This example will use the addresses 10.25.2.15 and 10.25.1.14. Replace these example IPs with the IP addresses of your own ESXi host.

How To Send ESXi Logs To Nagios Log Server 2024R2

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.



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

How To Send ESXi Logs To Nagios Log Server 2024R2

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](#)