### Overview

These steps will walk you through:

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

### 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 <u>Listen On Privileged</u> <u>Ports</u>

## Create Input UDP 514

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

www.nagios.com



Page 1 of 14

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

Home > Configure >	Global		Search logs		+ Add Log Source		• System
Configure Configure Configure Configure Configuration Config Snapshots A Add Log Source Config Config Snapshots A Add Log Source Config Config Config Config Config Per Instance (Advanced) Config Config Snapshots Config Snapsho	~ ~ ~	Global Config Docs of Manage logstash config opti data through the filters when Save & Apply Inputs Filters Outputs Inputs Privileged Ports (2 Sysilog (Default)	2 ons that will be added to all instances in creating global filters. Verify View efault)	<ul> <li>Note that all applie</li> <li>•     </li> </li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	d global filters will happen before the local filters Windows Event Log (Default) Import Files - JSON (Default)	. Keep in mind the flow of the log + Add Input	
Inputs Filters	Outputs						
Inputs Privileged Po	orts 🖸					+	Add Input
Syslog (D	efault)		/ ~ [ 11	w	indows Event Log (Default)	0.	~ D 0
Import Fil	les - Raw (Default)		/ ~ 🛛 🔟		port Files - JSON (Default)	1	~ 🛛 🗇
XI Audit Log		/ ~ [] []		Block Name		~ 🛛 🔟	

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.

Syslog (ESXi)	/ ^ 🛛 🔟
syslog { type => 'syslog-esxi' port => 514 }	

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.



- 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 <u>Advanced Config</u> <u>section</u>.

www.nagios.com



Page 4 of 14

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

Home > Configure > Global	Bearch logs		+ Add Log Source		• System
Configure  Configure Configuration Config Snapshots Add Log Source Global (All Instances) Config Global Config Config	Global Config Docs 2 Manage logstash config options that will data through the filters when creating glo Sawe & Apply V Ver Inputs Filters Outputs	be added to all instances. Note that ball filters.	all applied global filters will happen before the local filters. K	eep in mind the flow of the log	
Per Instance (Advanced)	Inputs Privileged Ports (2		U Windows Event Log (Default)	+ Add Input	
	Import Files - Raw (Default)	/ ~	Import Files - JSON (Default)	/ ~ 0 0	
	Xi Audit Log	1 ~			
Inputs Filters Outputs Inputs Privileged Ports [2]				(	+ Add Input
Syslog (Default)		/ ~ [] 1	Windows Event Log (Default)		/~00
Import Files - Raw (Defi	ault)	/ ~ [] 11	Import Files - JSON (Default)		∥ ∽ [ 0
XI Audit Log		/ ~ [] []	Block Name		~ [ 0

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 (ESXi)

$ yslog {
    type => 'syslog-esxi'
    port => 1514
    }

$ yslog {
```

```
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.

www.nagios.com



Page 7 of 14

### 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**.

Summary	Monitor	Configure	Permissions	VMs	Datas	stores	Networks	Updates
VMkernel	l adapters		Advanced S	ystem	Sett	ings		
Physical a	adapters	1	Kau			Value		
I CP/IP co	onfiguration	-			Ŧ	value		
Virtual Mac	chines	~	Syslog.global.logF	ilters				
VM Start	up/Shutdown	-	Syslog global logE	iltersEnab	le	false		
Agent VM	A Settings		Systeg.global.logi	last		Taibe		
Default V	M Compatibility	y .	Sysiog.global.logH	lost				
Swap File	Swap File Location		Syslog.global.logL	evel		error		
System		~	Syslog.global.msg	QueueDro	pMark	90		
Licensing	I		Syslog.global.rem RetryDelay	oteHost.co	onnect	180		
Host Prof	file	-	Syslog.global.rem	oteHost.m	axMsg	1024		
Time Con	figuration		Len					
Authentic	cation Services		Syslog.global.vsan	Backing		false		
Certificat	e	-	Syslog.loggers.api	Forwarde	r.rotat	8		
Power Ma	anagement	-	e					
Advance	d System Settir	ngs	Syslog.loggers.api	Forwarde	r.size	1024		
System R	esource Reser	vation	Syslog.loggers.att	estd.rotate	е	8		
Firewall		-	Syslog.loggers.att	estd.size		1024		
Sorvicos								

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

Advanced System Settings

EDIT...

www.nagios.com



Page 8 of 14

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved. Trademarks are the property of their respective owner.

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

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	





Page 9 of 14

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved. Trademarks are the property of their respective owner.

### Allow Outbound Syslog Port

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

Summary	Monitor	Configure	Permissions	VMs	Datastores	Networks	Updates	
Swap File <b>System</b> Licensing	e Location	~	Firewall Connections:	GOING				
Host Pro	file		Service name		TCP ports		UDP ports	
Authentication Services			DVSSync				8301, 8302	
Certificat	e		HBR		31031, 440	)46		
Power M	anagement		NFC		902			
Advance	d System Setti	ings	WOL				9	
System F	Resource Reser	rvation	DHCP Client				68	
Firewall			DNS Client		53		53	
Services			Equit Toloranco		80, 8200			
Security Profile			Fault Tolerance		80, 8300			
System S	Swap		httpClient		80, 443			
Package	S		NTP Client				123	
Hardware		~	syslog		514, 1514		514	

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

Firewall	EDIT
Connections:	
INCOMING OUTGOING	





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 automatical	access to a serviously when any of th	ce or client, check the con neir ports are opened, and	rresponding box. By default d stop when all of their port	, daemons will start s are closed.		
Groups						
UNGROUPED	SECURE SHELL	SIMPLE NETWORK MANAGEME	NT PROTOCOL			
Quick Filter	syslog					
	Service name	Incoming Ports	Outgoing Ports	D		
Z →   :	syslog		514, 1514 (TCP), 514 (U	IDP) N		
18				1 item		
				CANCEL		



### **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:

N	Home > Dashboard	Search logs + Add Log Source				System	
â	My Default Dashboard \$		+ Add Row	< Share	🗄 Last 24h		~
80 E	∧ Default Query Templates	L best into 25.2 15					
Ļ	404 500 SSH AD Errors	T INGUIDIOZOZIO					U
ŵ	Account Lockout Password Change	⊘ Nagios Logserver Search				+ ō	
0	Failed Login Sendmail						

You should see results appear in the All Events panel.

All Events			
Filter messages		Export as	CSV Columns V
Type ↑↓	@timestamp ↑↓	Message î↓	lp 1↓
system	2024-12-11T22:55:35.596Z	[api.call@6876 subject="vpxuser" object="vmodl.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	$\rightarrow$ [context]zKq7AVICAgAAAP////8Jc2FuZGJveGQAAANZQWxpYnZtYWN_	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.

www.nagios.com



Page 12 of 14

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

Global Config Docs 2							
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.							
Save	Save & Apply	✓ Verify	View				
Inputs Filters	Outputs						
Filters							+ Add Filter
Apache	9 (Default)			/ ~ 🛛 🔟	XI Audit Log		

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

ESXI	/ ^ 🛛 🔟
<pre>if [host] == '10.25.2.15' or [host] == '10.25.2.14' {     mutate {         replace =&gt; { 'type' =&gt; 'syslog-esxi' }     } }</pre>	

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' 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 <u>Configure ESXi</u> section.

### **Finishing Up**

This completes the documentation on How to Send ESXi Logs to Nagios Log Server 2024. If you have additional guestions or other support-related guestions, 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

www.nagios.com



Page 14 of 14