Sending ESXi Logs to NLS 2024

Sending ESXi Logs to NLS 2024

Overview

These steps will walk you through:

- Create input for desired port to Nagios Log Server
 - <u>UDP 514</u>
 - <u>TCP 1514</u>
- 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 <u>Listen On Priv</u>ileged 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.

<u>N</u>agios

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

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

<u>N</u> agios LS	Home Dashboards Alerting Configure Help Adm	in Search logs	් 🔗 🛓 nagiosadmin 😃 Logout
Configure			
 Apply Configuration Config Snapshots Add Log Source 	GIODAL CONTIG Manage logstash config options that will be added to all instances. Note that a through the filters when creating global filters. View Logstash config language	ll applied global filters will happen before the local filters. Kee documentation C	ep in mind the flow of the log data
Global (All Instances)	Save Save & Apply & Verify View -		Show Outputs
Global Config	Inputs + Add	^{Input} ▼ Filters	+ Add Filter -
 Per Instance (Advanced) 			
● ✓ nls-c6x- x64.box293.local	Active Syslog (Default) / + 6	Active Apache (Default)	+ (2) 🖮
	Active Windows Event Log (Default) 🖌 🕇	1 🛱	
	Active Import Files - Raw (Default) 🖌 🕂) ŵ	
	Active Import Files - JSON (Default) 🖊 + 🤤	18	

Inputs	+ Add Input -
	Custom
Active Syslog (Default)	+ 4 <u>3</u> 🖻

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

<u>N</u>agios

www.nagios.com

© 2024 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Sending ESXi Logs to NLS 2024

Active	Syslog (ESXi)	一 42 前
syslog {	[
type	=> 'syslog-esxi'	
port	: => 514	
}		

- 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):

<u>N</u>agios

Sending ESXi Logs to NLS 2024

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

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

Nagios

Sending ESXi Logs to NLS 2024

<u>N</u>agios

<u>N</u> agios [,] LS	Home	Dashboards	Alerting	Configure	Help	Admin	Search logs	🥏 🛓 nagiosadmin 🙂 Logout
Configure Apply Configuration O Config Snapshots Add Log Source	Glob Manage k through t	al Config	ns that will be ting global filt	added to all in ers. View Logst	stances. N ash config	ote that all applied language documen	global filters will happen before the local filters. Keep lation ${\cal C}$	in mind the flow of the log data
Global (All Instances) Global Config Per Instance (Advanced)	Inputs	G Save & Apply	S verity	View +		+ Add Input →	Filters	Add Filter ✓
● ✓ nls-c6x- x64.box293.local	Ac	tive Syslog (Defa	ault) 🖍	fault) 🖋		+ 42 m + 42 m	Active Apache (Default)	+ 役 前
	Ac	tive Import Files	s - Raw (Defa	ult) 🖊		+ @ @		
	Ac	tive Import Files	: - JSON (Def	ault) 🖉		+ 4 面		

Inputs	+ Add Input →
Active Syslog (Default)	+ 🐴 🖮

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):

<u>N</u>agios

Sending ESXi Logs to NLS 2024

Active	Syslog (ESXi)	- 41 🖻
syslog -	[
type	e => 'syslog-esxi'	
port	t => 1514	
}		

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

Nagios

Sending ESXi Logs to NLS 2024

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.

<u>N</u>agios

Sending ESXi Logs to NLS 2024

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.

<u>N</u>agios

Sending ESXi Logs to NLS 2024

🕝 Advanced Settings			×
FSS FT HBR Irq ISCSI LPage Mem Migrate Misc NFS NFS41 Nmp Numa	^	Syslog.global.defaultRotate Default number of rotated logs to keep. Reset to default on zero. Min: 0 Max: 100 Syslog.global.defaultSize Default size of logs before rotation, in KiB. Reset to default on zero. Min: 0 Max: 10240 Syslog.global.logDir Datastore path of directory to output logs to. Reset to default on null. Example	8 1024 [] /scratch/log
 Power RdmFilter ScratchConfig Scsi Security SunRPC SvMotion 		Syslog.global.logDirUnique Place logs in a unique subdirectory of logdir, based on hostname.	
global j toggers User UserVars VBLOB VFLASH Virsto VMFS VMFS3 VMkernel VSAN	~	Syslog.global.logHost The remote host to output logs to. Reset to default on null. Multiple hosts a	udp://10.25.5.99:514 re supported and must be s
			OK Cancel

- 5. Expand Syslog and click global.
- 6. For UDP 514 change Syslog.global.logHost to:

udp://xxx.xxx.xxx.514

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

tcp://xxx .xxx.xxx.1514

<u>N</u>agios

Sending ESXi Logs to NLS 2024

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

8. Click OK.

Hardware	Security Profile			
Processors	Services		Refresh	Properties
Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings	SNMP Server PC/SC Smart Card Daemon Load-Based Teaming Daemon ESXi Shell X.Org Server VMware vCenter Agent NTP Daemon			
Power Management	Active Directory Service			
Software	SSH Syslog Server			
Licensed Features Time Configuration	Direct Console UI CIM Server Firewall		Refresh	Properties
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	Incoming Connections CIM Secure Server Fault Tolerance vSphere Web Access vSphere Web Client vsanvp SSH Server DHCPv6 CIM SLP Virtual SAN Clustering Service	5989 (TCP) 8100,8200,8300 (TCP,UDP) 80 (TCP) 902,443 (TCP) 8080 (TCP) 22 (TCP) 546 (TCP,UDP) 427 (UDP,TCP) 12345,23451,12321 (UDP) 902 (TCP)	All All All All All All All All All	

Under Software click Security Profile.

For Firewall click Properties.

<u>N</u>agios

<u>N</u>agios

Sending ESXi Logs to NLS 2024

, ch	note Access	m accepting populated of	a this bast, and local clients		d from	
cces	ssing services on remote hosts.	in accessing services of	Turis nost, and local clients	are prevente	uirom	
elec	t a check box to provide access to a se	rvice or client. Daemon	s will start automatically wh	en their ports	are	
ben	ed and stop when all of their ports are	closed, or as configure	d.			
	Label	Incoming Ports	Outgoing Ports	Protocols	Daemon	~
٦	DVFilter	2222		ТСР	N/A	-
Ŧ.	vprobeServer	57007		TCP	Stopped	
3	HBR		31031,44046	TCP	N/A	
7	Virtual SAN Transport	2233	2233	TCP	N/A	
2	Fault Tolerance	8100,8200,8300	80,8100,8200,8300	TCP,UDP	N/A	
2	syslog		514,1514	UDP,TCP	N/A	1
2	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	~
<					>	
Ser	vice Properties					
_						
Ge	neral					
Se	ervice: SSH Client					
P;	ackage Information:					
- 23						
E.	ewaii Settings					
Fire						
Fin	llowed IP Addresses: All					
Fire	llowed IP Addresses: All					
A	lowed IP Addresses: All					
A	lowed IP Addresses: All		Fir	ewall	Options]
A	lowed IP Addresses: All		Fin	ewall	Options	

<u>N</u>agios

www.nagios.com

© 2024 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the prop- Page: 11 erty of their respective owner.

Sending ESXi Logs to NLS 2024

<u>N</u>agios

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>

QUERY	
• host:10.25.6.146	Q +

You should see results appear in the ALL EVENTS panel.

ALL EVENTS				🛓 Export as CSV 🛛 🗿	• 4	i+ ×	¢
Fields () All (30) / Current (20)				0 to 50 of 250 available for paging			
Type to filter	@timestamp >	< host >	< type >	< message	Acti	ions	
✓ ▼ @timestamp	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):	۹	•	
□ ▼_id □ ▼_index □ ▼_type	2017-12-05T13:26:47.179+11:00	<mark>10.25.6.145</mark>	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	Q	•	
 T facility T facility_label T highlight ▼ host 	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	Q	•	

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

Nagios

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.

Active	ESXi	- 4 1 🖻
if [ho mu	<pre>st] == '10.25.6.145' or [host] == '10.25.6.146' { tate { replace => { 'type' => '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):

Nagios

www.nagios.com

© 2024 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Sending ESXi Logs to NLS 2024

```
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' 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.

