The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to configure your ESXi server to send syslog messages to the Nagios Log Server.

Target Audience

This document is intended for use by VMware Administrators who would like to send their ESXi syslog messages to Nagios Log Server for storage and analysis.

Overview

These steps will walk you through:

- Add syslog port 1514 to Nagios Log Server
- Configure ESXi to send syslogs to Nagios Log Server

Add Syslog Port 1514 to Nagios Log Server

Login to your Nagios Log Server

- Click Administration at the top right
- In the left pane click Global Configuration
- You will see the Inputs section
- Next to Syslog (Default) click the copy icon
- This creates a duplicate
- Change the name to Syslog (ESXi)
- Change the port to 1514
- Click the Save button underneath
- Click the **Apply** button above
- Wait for the Apply Configuration to finish

Open Firewall Ports on Nagios Log Server

Now establish an SSH session to your Nagios Syslog Server

- Type iptables -I INPUT -p tcp --destination-port 1514 -j ACCEPT and press Enter
- Type iptables -I INPUT -p udp --destination-port 1514 -j ACCEPT and press Enter
- Type service iptables save and press Enter

This completes the steps required on the Nagios Log Server.

Global Configuration

Manage logstash config options that will be added to all instances. N Keep in mind the flow of the log data through the filters when creating

outs	+ Add Input
Active Syslog (Default) 🖋	+ 🗠 🖻
Active Windows Event Log (Default) 🖋	+ 🕲 🖻
Active Syslog (ESXi) 🥜	- 4 🖻
<pre>syslog { type => 'syslog' port => 1514 }</pre>	



Nagios Enterprises, LLC US: 1-888-NAGIOS-1 Int'l: +1 651-204-9102 Fax: +1 651-204-9103 Web: www.nagios.com Email: sales@nagios.com

Nagios Log Server – ESXi Syslog Config

Nagios

Configure ESXi Default size of logs before rotation, in KiB. Reset to default on zero PageRetire Power Min: 0 Max: 10240 RdmFilter Now we need to configure ESXi to send syslogs to this server: ScratchConfig Syslog.global.logDir Π /scratch/log Scsi SunRPC Datastore path of directory to output logs to. Reset to default on null. Example: . Open the vSphere Client to the ESXi server (can be SyMotion done through vCenter) Syslog Ē٠ global Select the ESXi host in the inventory pane + loggers Syslog.global.logDirUnique Click the Configuration tab on the right User Place logs in a unique subdirectory of logdir, based on hostname. UserVars Under Software click Advanced Settings VBLOB Expand Syslog and click global VFLASH VMFS Change Syslog.global.logHost to: Syslog.global.logHost tcp://192.168.207.148:151 VMFS3 tcp://192.168.207.148:1514 + VMkernel 0 The remote host to output logs to. Reset to default on null. Multiple hosts are s... VSAN Where 192.168.207.148 is the IP Address of the 0 XvMotion

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.

OK

Cancel

Help

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	*
\Box	HBR		31031,44046	TCP	N/A	
\square	rdt	2233	2233	TCP	N/A	
	Fault Tolerance	8100,8200,8300	80,8100,8200,8300	TCP,UDP	N/A	
\square	syslog		514,1514	UDP,TCP	N/A	
⊻	VMware vCenterAgent		902	UDP	Stopped	h
	IKED	500	500	UDP	N/A	Ξ
	VM serial port connected over net	23,1024-65535	0-65535	TCP	N/A	
	http Client		80,443	TCP	N/A	
$\mathbf{\nabla}$	ipfam	6999	6999	UDP	N/A	
₹	DMCClient	E0	50	UDD TCD	NI/A	Ŧ

Check Nagios Log Server

Now we need to confirm that Nagios Log Server is receiving data from the ESXi server.

Login to your Nagios Log Server

•

0

Click OK

- Click Dashboard on the menu ba
- In the Query field type the IP Address of your ESXi host and press Enter

Nagios Log Server

For Firewall click Properties

Find syslog and Tick the box

Under Software click Security Profile

This completes the steps required on the ESXi server.

Click OK

You will now see the results appe

Nagios Log Server Sea	rch a day	ago to a few second	s ago 🔻	C	*	0	\$		B	0	đ	
QUERY >												
• 192.168.207.132											Q 1	•
FILTERING 4 ★												
🗢 🔺 GRAPH												
ALL EVENTS									0	٥	+	_
Fields ()	0 to 50 of 250 available for paging							→				
All (28) / Current (20)												
Type to filter	@timestamp 🗸	nost	type	mess	age						ACUC	ons
	2014-10-02T13:45:07.152-05	:00 192.168.207.13	syslog	<166>Se	ection f	or VMw	are ESX				Q	•
				localhost	tlocald	lomain	hostd-p	robe:				
				Id=25237	77, ver:	sion=5	.5.0, buil	d=16233	87,			
id id				and an D		-						
id index				option=R	leleas	e						
id index type	2014-10-02T13:45:02.154-05	:00 <mark>192.168.207.13</mark> :	syslog	option=R cpu0:500	teleas (088)Wo	e orld: 14	296: VC	opID			۹	•
id index type facility	2014-10-02T13:45:02.154-05	:00 <mark>192.168.207.13</mark> ;	2 syslog	option=R cpu0:500 hostd-e1	teleas)88)Wo 3a ma	e orld: 14 ips to v	296: VC mkernel	opID opID		(Q	Ŧ

Nagios Enterprises

Nagios Enterprises, LLC US: 1-888-NAGIOS-1 P.O. Box 8154 Saint Paul, MN 55108 USA

Int'l: +1 651-204-9102 Fax: +1 651-204-9103 Web: www.nagios.com Email: sales@nagios.com

Finishing Up

If you have any questions about querying or analyzing your log data on Nagios Log Server, contact our support team via our online forum at:

http://support.nagios.com/forum



USA

Nagios Enterprises, LLC US: 1-888-NAGIOS-1 P.O. Box 8154 Int'l: +1 651-204-9102 Saint Paul, MN 55108 Fax: +1 651-204-9103

Web: www.nagios.com Email: sales@nagios.com Page 3