

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*

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

[Save](#) [Verify](#) [Apply](#) [View](#)

Inputs

[+ Add Input](#)

Active	Syslog (Default)	+ - copy trash
Active	Windows Event Log (Default)	+ - copy trash
Active	Syslog (ESXi)	- copy trash

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

[Save](#)

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

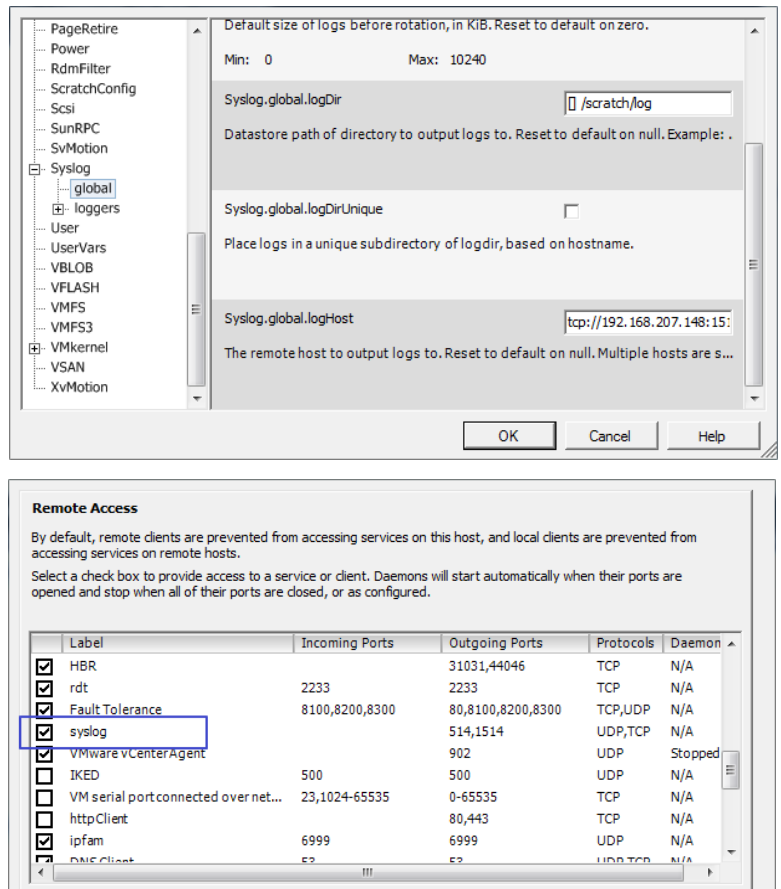
This completes the steps required on the Nagios Log Server.

Configure ESXi

Now we need to configure ESXi to send syslogs to this server:

- Open the vSphere Client to the ESXi server (can be done through vCenter)
- Select the **ESXi host** in the inventory pane
- Click the **Configuration** tab on the right
- Under **Software** click **Advanced Settings**
- Expand **Syslog** and click **global**
- Change **Syslog.global.logHost** to:
 - **tcp://192.168.207.148:1514**
 - *Where 192.168.207.148 is the IP Address of the Nagios Log Server*
 - Click **OK**
- Under **Software** click **Security Profile**
- For **Firewall** click **Properties**
- Find **syslog** and Tick the box
- Click **OK**

This completes the steps required on the ESXi server.

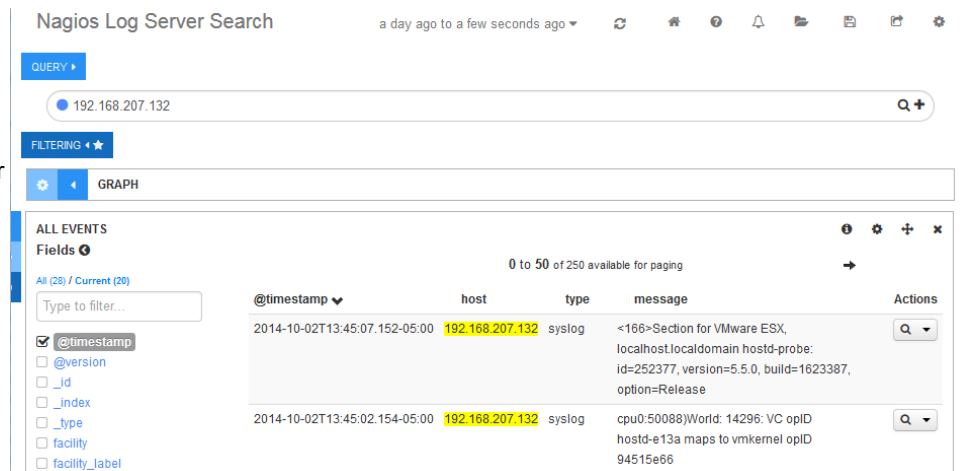


Check Nagios Log Server

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

Login to your Nagios Log Server

- Click **Dashboard** on the menu bar
- In the **Query** field type the **IP Address** of your **ESXi** host and press Enter
- You will now see the results appear



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>