RSA NetWitness Logs

Event Source Log Configuration Guide

VMware vShield and vShield Manager

Last Modified: Friday, June 02, 2017

Event Source Product Information:

Vendor: VMware
Event Source: vShield
Versions: 4.1, 5.0, 5.1.4

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: vmware_vshield
Collection Method: Syslog
Event Source Class.Subclass: Security.Firewall

To configure Syslog collection for the vShield and vShield Manager, complete the following tasks:

I. Configure NetWitness Suite for Syslog Collection

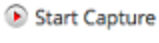
II. Configure Syslog Output on vShield and vShield Manager

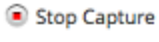
Configure NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see 

, click the icon to start capturing Syslog.
   - If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure Syslog Output on vShield and vShield Manager

You must complete the following tasks to configure Syslog output on VMware vShield:

I. Configure Syslog Output on vShield App

II. Configure Syslog Output on vShield Edge

III. Configure Syslog Output on vShield Manager

Configure Syslog Output on vShield App

To configure Syslog output on vShield App:

1. Log on to the vShield Manager user interface.
2. Select the server on which vShield App is installed.
3. Click the **Summary** tab.
4. Under **Service Virtual Machines**, click the arrow next to the vShield App machine.
5. Under **Syslog Servers**, enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
6. From the **Log Level** drop-down menu, select **INFO**.
7. Click **Add** to save the settings.

Configure Syslog Output on vShield Edge

To configure Syslog output on vShield Edge:

1. In the vSphere Client, click **Inventory** > **Networking**.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the **vShield Edge** tab.
4. Under **Remote Syslog Servers**, in the top text box, enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
5. Click **Commit** to save the configuration.

Configure Syslog Output on vShield Manager

To configure Syslog output on vShield Manager:

1. Log onto the vShield Manager Web UI, using administrator credentials.
2. In the left navigation pane, click **Settings and Reports**.
3. Select **Configuration** > **Syslog Server**, and click **Edit**.

   The Syslog Server Information dialog box appears.
4. Enter the following information:
   - IP address: the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector
   - Port: **514**
5. Click **OK** to save the configuration.

Trademarks