RSA NetWitness Logs

Event Source Log Configuration Guide

VMware NSX

Last Modified: Thursday, November 30, 2017

Event Source Product Information:

Vendor: VMware
Event Source: VMware NSX
Version: 6.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Type: vmware_nsx, vmware_vshield

Note: VMware NSX Edge Firewall is supported with the **vmware_vshield** parser. VMware NSX Distributed Firewall is supported with the **vmware_nsx** parser.

Collection Method: Syslog
Event Source Class.Subclass: Hosts.Virtualization

To configure VMware NSX, you must complete these tasks:

- Configure VMware NSX to send Logs to NetWitness Suite
- Configure RSA NetWitness Suite

Configure VMware NSX to Send Logs to NetWitness Suite

VMware NSX is a software networking and security virtualization platform that delivers the operational model of a virtual machine for the network. Virtual networks reproduce the Layer2 - Layer7 network model in software, allowing complex multi-tier network topologies to be created and provisioned through programming in seconds. NSX includes a library of logical switches, logical routers, logical firewalls, logical load balancers, logical VPN, QOS and distributed security.

Configure VMware NSX to send Distributed Firewall Logs

You can configure VMware NSX to send the NSX Distributed Firewall logs (classified as **dfwpktlogs**) to RSA NetWitness Suite.

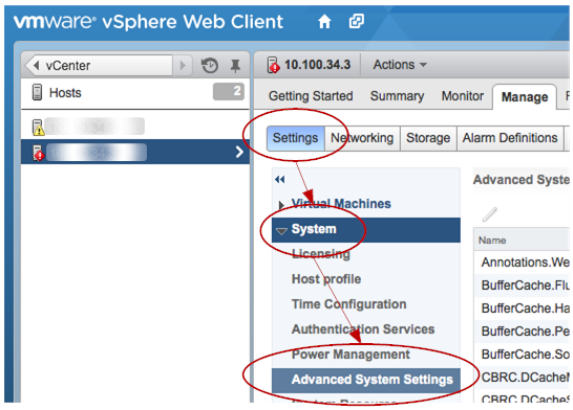
Note: All ESXi related logs will be received as well.

Since the Firewall event logs are packaged with the ESXi logs, you need to configure Syslog on your ESXi Hosts.

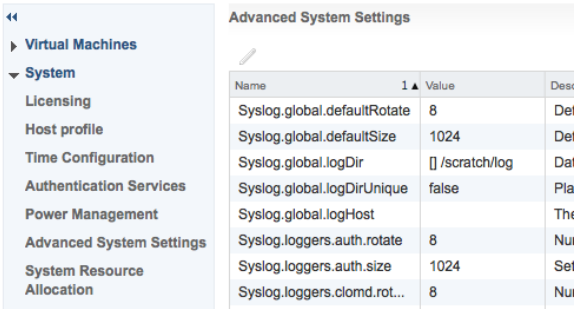
To configure Syslog on a VMware ESXi host:

Note: These instructions are reproduced from the VMware vSphere 5.5 Documentation Center.

1. Log on to the VMware vSphere Web Client.
2. In the left navigation pane, select **vCenter**.
3. In the vSphere Web Client inventory, select **Hosts**, and select the host that you want to configure.
4. Click the **Manage** tab.
5. In the System panel, click **Advanced System Settings**.



6. Locate the Syslog section of the Advanced System Settings list.



7. To set up logging globally, select the setting to change and click the Edit icon.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified as *[datastorename] path_to_file* where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path

Option	Description
	`/vmfs/volumes/storage1/systemlogs`
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:514`. UDP (default), TCP, and SSL are supported. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

8. (Optional) To overwrite the default log size and log rotation for any of the logs:
   a. Click the name of the log that you want to customize.
   b. Click the Edit Icon and enter the number of rotations and log size that you want.
9. Click **OK**.

Changes to the syslog options take effect immediately.

Configure VMware NSX to send Edge Firewall Logs

You can configure VMware NSX to send the NSX Edge Firewall logs to the RSA NetWitness Suite.

You can configure one or two remote syslog servers. NSX Edge events and logs related to firewall events that flow from NSX Edge appliances are sent to the syslog servers.

Note: These instructions are reproduced from the VMware NSX 6 Documentation Center.

To configure VMware NSX to send NSX Edge logs:

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Monitor** tab and then click the **Settings** tab.
5. In the **Details** panel, click **Change** next to Syslog servers.
6. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
7. Click **OK** to save the configuration.

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parsers are **vmware_nsx** and **vmware_vshield**.

Configure Syslog Collection

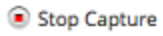
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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.

Trademarks