RSA NetWitness Logs

Event Source Log Configuration Guide

BlueCat

Last Modified: Friday, May 05, 2017

Event Source Product Information:

Vendor: BlueCat
Event Source: BlueCat IPAM, DNS and DHCP
Version: Adonis 7.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: bluecat
Collection Method: Syslog
Event Source Class.Subclass: Network.System

Configure BlueCat

To configure Syslog collection for the BlueCat event source, you must:

I. Configure Syslog Output on BlueCat IPAM

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on BlueCat

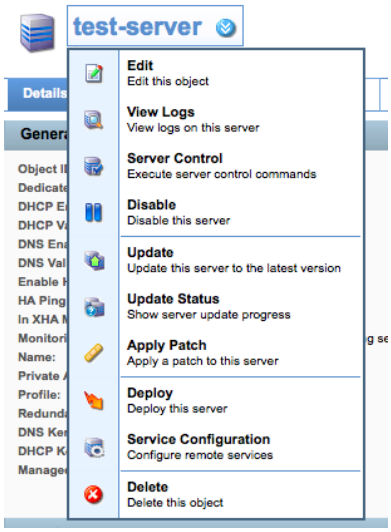
You can configure the BlueCat IPAM to send DNS and DHCP log messages to RSA NetWitness Suite.

To configure BlueCat:

1. Log onto the BlueCat Proteus™ URL, using administrator credentials.
2. Click the **Servers** tab.

   The **Servers** tab lists all available BlueCat DHCP servers.
3. Select the server for which you are configuring logging.
4. Click the server name, then select **Service Configuration** from the drop-down menu.

   In this screen shot, the server is named **test-server**:



5. From the **Service Type** field, select **Syslog**.
6. In the **SIEM Settings** section, do the following:

- Select the **Enable ArcSight Forwarding** check box.
- For the ArcSight Server, enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

7. Click **Update**.

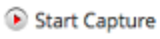
You have now enabled the collection of DNS and DHCP log messages for RSA NetWitness Suite.

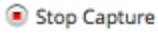
Configure RSA NetWitness Suite for Syslog Collection

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.

Trademarks