RSA NetWitness Logs

Event Source Log Configuration Guide

nCircle Configuration Compliance Manager

Last Modified: Tuesday, May 09, 2017

Event Source Product Information:

Vendor: nCircle
Event Source: Configuration Compliance Manager
Versions: 5.10

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ncircleccm
Collection Method: Syslog
Event Source Class.Subclass: Network.Configuration Management

To configure the nCircle Configuration Compliance Manager event source, you must:

I. Configure Syslog Output on nCircle Configuration Compliance Manager

II. Configure RSA NetWitness Suite for Syslog Collection

Configure nCircle Configuration Compliance Manager

To configure nCircle Configuration Compliance Manager, you must complete the following tasks:

I. Configure System Health Events

II. Configure nCircle CCM for Alerting

Configure System Health Events

To configure System Health Events:

1. Go to **Settings > System > System Health Maintenance > System Health Events**.
2. Click **Add** to add a System Health Event for monitoring.
3. Choose **Syslog** from the drop-down menu.
4. Choose all of the event types that you want to send through syslog.
5. Click **Settings** to configure the notification method. The notification configuration method is the same as configuring an Alert.
6. Click **OK** to save the System Health Event.
7. Click **OK** in the System Settings window.

Configure nCircle CCM for Alerting

To configure nCircle CCM for alerting:

1. Log on to the nCircle CCM console.
2. Navigate to the **Asset group** location.
3. For each asset that you want to configure, right-click, and select **Scan Configuration**.
4. Click **Add**.

5. In the Edit Scan Task window, from the **Task Type** drop-down list, select **Alert**.
6. In the **Task Name** field, assign a name for the alert.
7. Click **Use Custom**, and select **In Response to Events**.
8. Select all of the events, and click **OK**.
9. Click **Add**, and select **Add Syslog Alert**.
10. In the Syslog Action window, complete the fields as follows.

Field	Action
Host	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Transport Protocol	Select **UDP**.
Port	Type **514**.

11. Click **OK**.

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 parser is **ncircleccm**.

Configure Syslog Collection

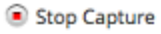
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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