RSA NetWitness Logs

Event Source Log Configuration Guide

NFR NIDS

Last Modified: Wednesday, April 26, 2017

Event Source Product Information:

Vendor: NFR
Event Source: NIDS
Versions: 3.x, 4.x, 5.x
Additional Downloads: mappriorities.pl, nic.pl

RSA Product Information:

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

To configure the NFR NIDS event source, you must:

I. Configure Syslog Output on NFR NIDS

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on NFR NIDS

To configure NFR NIDS, you must download the **nic.pl** and **mappriorities.pl** Perl scripts from the RSA NetWitness Event Source Additional Downloads space on RSA Link here: NFR NIDS Additional Downloads.

The configuration instructions are dependent on the your version of NFR NIDS. See the procedure that matches your version of NFR NIDS:

- Configure NFR NIDS Version 5.x
- Configure NFR NIDS Version 4.x
- Configure NFR NIDS Version 3.x

Configure NFR NIDS Version 5.x

To configure NFR Security NIDS version 5.x:

1. Place the **nic.pl** and **mappriorities.pl** Perl scripts into the NFR home directory on the Sentivist server (**/usr/local/nfr**).
2. Change the permissions on these files to make them executable:

   ```
   #chmod 755 nic.pl
   #chmod 755 mappriorities.pl
   ```

3. Edit the **nic.pl** Perl script as follows:
   - Set the value of **$ENVISION_HOST** to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
   - If you set **$DISCOVER_BY_SENSOR_IP** to **yes**, ensure the following:
     - Ensure the path is correct: **open CENTRAL, "<$NFRHOME/server/etc/central.cfg";**
     - The **central.cfg** file has the correct sensor **name\ip** mappings.
4. Edit the **mappriorities.pl** Perl script to update the following:

   ```
   $NFRHOME = "/usr/local/nfr/server";
   $nfrpassword = "nfrdemo"; #change to your DB password
   $nfruser = "nfr";
   $nfrdbhost = "127.0.0.1";
   $nfrversion = "5.0";
   ```

5. Edit the **\etc\crontab** file to schedule the **mappriorites.pl** Perl script to run at an interval according to how often you change alert priority values in the Sentivist UI.

   For example, to run once per day at 1 AM:

   a. From the command line, type the following:

   ```
   #crontab -e
   ```

   b. Insert `* 1 * * * /usr/local/nfr/mappriorities.pl` into the **crontab** file.

6. Log on to the Sentivist Protection Center with administrative Credentials.
7. In the Sentivist Protection Center, select **Management** > **Policies** from the menu to open the Sentivist Policy Manager.
8. Select **Alert Configuration** tab. Browse to alert group you want to monitor.
9. Select the rule and click **Edit Rules**.
10. In the Edit Rules window, click **New Rule**.
11. In the Rule Template window, select **Generic** and click **OK**.
12. In the New Generic Rule Window, type the following values:

Field	Value
Rule Name	**Nfralert**
Executable	**/usr/local/nfr/nic.pl**
Arguments	leave this field blank
Interval	**10**
Alert Count	**30**

13. Click **OK**.
14. In the Edit Rules window, select the new rule you created and click the right arrow button to move the rule into the **Applied Rules** column.
15. Click **OK**.
16. Click **Apply**, then **Close** in the **Alert Configuration** section of the Sentivist Policy Manager window.

Note: When message ID priorities are changed, the **crontab** runs and creates or updates the **/usr/local/nfr/log/nfrmappriorities.map** file.

Configure NFR NIDS Version 4.x

To configure NFR Security NIDS version 4.x:

1. Place the **nic.pl** and **mappriorities.pl** Perl scripts into the NFR home directory on the Sentivist server (**/usr/local/nfr**).
2. Change the permissions on these files to make them executable:

   ```
   #chmod 755 nic.pl
   #chmod 755 mappriorities.pl
   ```
3. Edit the **nic.pl** Perl script as follows:
   - Set the value of **$ENVISION_HOST** to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
   - If you set **$DISCOVER_BY_SENSOR_IP** to **yes**, ensure the following:
     - Ensure the path is correct: **open CENTRAL, "<$NFRHOME/server/etc/central.cfg";**
     - The **central.cfg** file has the correct sensor **name\ip** mappings.
4. Edit the **mappriorities.pl** perl script to update the following:

   ```
   $NFRHOME = "/usr/local/nfr/server";
   $nfrpassword = "nfrdemo"; #change to your DB password
   $nfruser = "nfr";
   $nfrdbhost = "127.0.0.1";
   $nfrversion = "4.1";
   ```
5. Edit the **\etc\crontab** file to schedule the **mappriorites.pl** Perl script to run at an interval according to how often you change alert priority values in the Sentivist UI.

   For example, to run once per day at 1 AM:

   a. From the command line, type the following:

      ```
      #crontab -e
      ```

   b. Insert `* 1 * * * /usr/local/nfr/mappriorities.pl` into the **crontab** file.
6. Create a rule in the NFR Administration Interface:

   a. Open the NFR Administration Interface and click the **Administration** tab.

   b. Select **Alert Configuration**.

c. Select the **Rules** option from the Alert Configuration Menu.

d. In the Rules for All window, click **New**, select **Generic**, then click **OK**.

e. From the New Generic Rule window, type a rule name. For example, **nfralert**.

f. Enter the full path to the **nic.pl** script in the **Executable** field. For example, **/usr/local/nfr/bin/nic.pl**.

g. Leave the **Arguments** field blank.

h. Set **Interval** and **Alert Count** to **10** and **30** respectively.

i. Click **OK**.

j. In the Rules for All window, select the new rule you created (**nfralert**) and click **Add**.

k. Click **OK**.

This rule is available to all groups and alerts on all IDS and System Events.

Configure NFR NIDS Version 3.x

To configure NFR Security NIDS version 3.x:

1. Place the **nic.pl** Perl script into the **NFR** home directory on the Sentivist server (**/usr/local/nfr**).
2. Make the **nic.pl** file executable by entering the following command:

   ```
   #chmod 755 nic.pl
   ```
3. Edit **nic.pl** to set the value of **$ENVISION_HOST** to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
4. Create a rule in the NFR Administration Interface:

   a. Open the NFR Administration Interface and click the **Administration** tab.

   b. Select **Alert Configuration**.

   c. Select the **Rules** option from the Alert Configuration Menu.

   d. In the Rules for All window, click **New**, select **Generic**, then click **OK**.

   e. From the New Generic Rule window, type a rule name. For example, **nfralert**.

   f. Enter the full path to the **nic.pl** script in the **Executable** field. For example, **/usr/local/nfr/bin/nic.pl**.

g. Leave the **Arguments** field blank.

h. Set **Interval** and **Alert Count** to **10** and **30** respectively.

i. Click **OK**.

j. In the Rules for All window, select the new rule you created (**nfralert**) and click **Add**.

k. Click **OK**.

This rule is available to all groups and alerts on all IDS and System Events.

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 **nfrnids**.

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