RSA NetWitness Platform

Event Source Log Configuration Guide

Citrix NetScaler

Last Modified: Wednesday, July 15, 2020

Event Source Product Information:

Vendor: Citrix
Event Source: NetScaler
Versions: 9.x, 10.x, 11.x, 13.x

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: citrixns, CEF
Collection Method: Syslog
Event Source Class.Subclass: Security.Application Firewall

To configure Citrix NetScaler to work with RSA NetWitness Platform, perform the following tasks:

- Configure Syslog Output on Citrix NetScaler
- Configure NetWitness Platform, for either of the following:
  - Collection using Syslog, or
  - Collection using the CEF parser

> **Note:** If you are using the **cef** parser, make sure to disable the **citrixns** parser. For details, see Use the CEF Parser for Collection.

Configure Syslog Output on Citrix NetScaler

Please follow the instructions to support your version of Citrix NetScaler:

- Configure Citrix NetScaler for version 10.x, 11.x or 13.x
- Configure Citrix NetScaler for version 9.x

Configure Citrix NetScaler for version 10.x, 11.x or 13.x

To configure Citrix NetScaler version 10.x or 11.x:

1. Log on to the Citrix NetScaler web console with administrator credentials.
2. From the top menu, click **Configuration**.
3. In the left-hand navigation pane, expand the **System** folder.
4. Expand the **Auditing** folder, then click **Syslog**.
5. On the right-hand window, click **Servers**.
6. Click the **Add** button.
7. In the Configure Auditing Server window, complete the fields as follows.

Field	Action
Auditing Type	From the drop-down list, select **SYSLOG**.
Name	Enter the name of your RSA NetWitness Platform server.
IP Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type **514**.

Field	Action
Log Levels	Select **All**.
Log Facility	Select the appropriate log facility from the drop-down list.
Date Format	Select **MMDDYYYY**.
Time Zone	Select **GMT**.
TCP Logging	Select **TCP Logging**.
ACL Logging	Select **ACL Logging**.

8. Above the top menu, click **Create**.
9. Click the **Save the running configuration** icon near the top-right of the window.
10. Click **Yes** to confirm.
11. You also need to set the CEF logging flag:
    a. In the left-hand navigation pane, select **Security** > **Application Firewall**.
    b. In the **Settings** area, click **Change Engine settings**.
    c. Select the **CEF logging** field.
    d. Click **OK** to save.

Configure Citrix NetScaler for version 9.x

To configure Citrix NetScaler for version 9.x:

1. Log on to the Citrix NetScaler web console with administrator credentials.
2. From the top menu, click **Configuration**.
3. In the System Configuration window, select a configuration utility.
4. In the navigation pane, expand the **System** folder.
5. Click the **Auditing** folder.
6. In the **Settings** section of the Auditing window, click **Change global auditing settings**.
7. In the Configure Auditing Parameters window, complete the fields as follows.

Field	Action
Auditing Type	From the drop-down list, select **SYSLOG**.
IP Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type **514**.
Log Levels	Select **All**.
Log Facility	Select the appropriate log facility from the drop-down list.
Date Format	Select **MMDDYYYY**.
Time Zone	Select **GMT**.
TCP Logging	Select **TCP Logging**.
ACL Logging	Select **ACL Logging**.

8. Above the top menu, click **Save**.
9. When prompted, click **Yes**.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

You can either use Syslog collection or the CEF parser:

- To configure Syslog collection:
  - Ensure the required parser is enabled
  - Configure Syslog Collection
- To configure the CEF parser for collection, see Use the CEF Parser for 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select  **(Admin)** > **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.

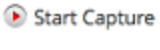
Note: The required parser is **citrixns**.

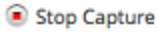
Configure Syslog Collection

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 **ADMIN** > **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 **ADMIN** > **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.

After 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.

Use the CEF Parser for Collection

If you want to collect using the CEF parser, you must disable the **citrixns** parser.

To ensure that the CEF parser is enabled and the citrixns parser is disabled:

1. In the RSA NetWitness Platform menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. Enable CEF and disable **citrixns**:
   - **Enable CEF**: In the Service Parsers Configuration panel, search for **cef**, and ensure that the Config Value field for this parser is selected.
   - **Disable citrixns**: In the Service Parsers Configuration panel, search for **citrixns**, and ensure that the Config Value field for this parser is not selected.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.