RSA NetWitness Logs

Event Source Log Configuration Guide

Network Appliance Data ONTAP

Last Modified: Thursday, January 4, 2018

Event Source Product Information:

Vendor: Network Appliance
Event Source: Data ONTAP
Versions: 6.x, 7.0-7.3.1.1, 8.x, 9.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.

Additional Downloads: Adiscon EventReporter 8.1 or 12.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: netapp
Collection Method: Syslog, Windows Event Logs
Event Source Class.Subclass: Storage.Storage

To configure Network Appliance Data ONTAP to work with RSA NetWitness Suite, perform the following tasks:

I. Configure NetWitness Suite for Syslog Collection

II. To collect administration and system events, perform one of the following tasks, based on your ONTAP version:

  - Configure Network Appliance Data ONTAP version 8.1.1 and higher, or
  - Configure Network Appliance Data ONTAP versions up to 8.0.2

  > **Note:** NetApp version 8.2.4 P6 does not support advanced commands. If you are configuring this version,

III. Configure CIFS Auditing on NetApp ONTAP

IV. Perform one of the following tasks:

  - To collect access events via Adiscon Event Reporter follow Configure Adiscon Event Reporter for CIFS Auditing instructions.
  - To collect access events via Windows Legacy Collector in Sec Analytics 10.3 and above, follow Configure Windows Legacy Collector for CIFS Auditing instructions.

> **Note:** Network Appliance Data ONTAP provides administration, system, and access events.

Configure NetWitness Suite for Syslog collection

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 **netapp**.

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.

Configure Network Appliance Data ONTAP using Advanced Commands

If your NetApp version supports advanced commands (most versions 8.1.1 and higher ***do*** support this), use the instructions in this section.

> **Note:** You can perform this task any time the cluster is running by entering the commands on the Data ONTAP command line.

1. Create a syslog server destination for high-severity events:

   ```
   event destination create -name rsa_sa -syslog ip_address -
   syslog-facility default
   ```

   where *ip_address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

2. Configure all events of severity level Critical, Alert, and Emergency to forward notifications to the syslog server that you just created or to your existing syslog server:

   ```
   event route add-destinations {-severity
   CRITICAL|ALERT|EMERGENCY} -destinations rsa_sa
   ```

Configure Network Appliance Data ONTAP Using Manual File Editing

Use the instructions in this section to configure versions 6.x, 7.0-7.3.1.1, 8.0.2, ***and any other versions that do not support advanced commands***.

To configure Network Appliance Data ONTAP for syslog collection, complete one of the following tasks:

- Use a text editor to edit the **syslog.conf** file on the targeted filer.
- Use a web browser to add or modify the **syslog.conf** file.

Edit syslog.conf

To edit the syslog.conf file:

1. Using a text editor, open **/etc/syslog.conf**.
2. Insert the following string:

   ```
   *.* @ip_address
   ```

   where:

   - *.* represents all logging Properties and Facilities, and
   - *ip_address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
3. Save the file.
4. Log on to the filer with your administrative credentials.
5. Click **FilerView** > **Filer** > **Configure Syslog**.
6. Highlight the text box.
7. Click **Reset**.

Add or modify syslog.conf

To add or modify the syslog.conf file:

1. Open a web browser, and go to `http://filename/na_admin`, where *filename* is the name of the targeted NetApp filer.
2. Click **FilerView** > **Filer** > **Configure Syslog**.
3. Click in the text box.
4. Click **New Action**.
5. Type `@ip_address,` where *ip_address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
6. Click **OK**.
7. Highlight the ***   *** (asterisks) line.
8. Click **Modify**.
9. Under **Properties**, click **Set All**.
10. Under **Facilities**, click **Set All**.
11. Click **OK** > **Apply** > **Reset**.

Configure CIFS Auditing on NetApp ONTAP

To configure CIFS Auditing

1. Log on to the NetApp Filer with your administrative credentials.
2. Click **FileView** > **Filer** > **Use Command Line**.
3. Run the following commands in the order listed:

```
options cifs.audit.autosave.file.extension timestamp
options cifs.audit.autosave.ontime.interval Nsuffix
```

> **Note:** where ***N*** is a number and ***suffix*** is an abbreviation for a period of time. For example, enter `1h` for one hour.

```
options cifs.audit.autosave.ontime.enable on
options cifs.audit.autosave.onsize.threshold 90%
options cifs.audit.autosave.onsize.enable on
options cifs.audit.file_access_events.enable on
options cifs.audit.logon_events.enable on
options cifs.audit.account_mgmt_events.enable on
options cifs.audit.enable on
```

> **Note:** You must enable auditing for each file and folder on which you want to audit CIFS activity. For instructions, refer to the NetApp documentation on CIFS auditing.

These steps create the .evt files that contain access events. To send these events to RSA NetWitness Suite, use either Adiscon Event Reporter or the RSA NetWitness Suite Windows Legacy Collector. To complete the configuration, do either of the following:

- Configure Adiscon EventReporter, or
- Configure the Windows Legacy Collector.

Configure Adiscon Event Reporter for CIFS Auditing

> **Warning:** RSA has found that Adiscon EventReporter stops sending log data when an EVT log file rotation occurs due to the log file reaching maximum file capacity. To resolve the issue, the Adiscon EventReporter service must be restarted.

To Configure Adiscon EventReporter 8.1 or 12.1 for CIFS Auditing:

1. Download the latest version of Adiscon EventReporter from the EventReporter web site (http://www.eventreporter.com, and install it on a Windows client from which you can access NetApp Filer.
2. Open the EventReporter application and click **Configured Services** > **Default EventLog Monitor**. Change the following options in the Configuration Services window:
   a. Under **General Options > Preferred Language**, select **English (United States) - (ENU)**.
   b. Click the **Insert** button to add an Eventlogtype Name.
   c. Click the **Eventlogtype Name** drop-down list and select **Security**.
   d. Click **Advanced** to open the Configuration Application window.
3. In the Configuring Application window, complete the following steps:
   a. Select **Use Checksum to verify the last processed event**.
   b. Select **Read Eventlog from File**.
   c. In the **File&Path Name** field, type **\\*Filer IP or Name*\ETC$\log\adtlog.evt**.
   d. From the **Type of Eventlog** menu, select **Security**.
   e. In the **Event types to log** section, select all event types.
   f. Click **OK**.
   g. Click **Save**.
4. In the Configured Services > Default EventLog Monitor panel, click **Advanced Options**.
5. In the Advanced Options window, follow these steps:
   a. In the **Syslog Tag Value** field, type **NetApp**.
   b. Select **Use Legacy Format**, **Add Facilitystring**, **Add Username**, and **Add Logtype**.
   c. Click **OK**.
   d. Click **Save**.
6. In the Configured Services > Default EventLog Monitor panel, in the **General**

Options section, select a **Sleep Time** value, and click **Save**.

> **Important:** Do not select a Sleep Time interval greater than the automatic log save interval because this would cause a loss of data. Ideally, the Sleep Time interval should be half the automatic log save interval.

7. Click **RuleSets > Default RuleSet > Forward Syslog > Actions > Forward Syslog**.
8. In the Default RuleSet > ForwardSyslog > ForwardSyslog panel, follow these steps:
   a. Ensure that **Enable: ForwardSyslog** is selected.

   b. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

   c. In the **Syslog Processing** field, select **Use Legacy RFC 3164 processing** or **Use RFC 5424 processing (Recommended)**.

   > **Note:** RSA NetWitness Suite supports both Syslog processing options.

   d. Click **Save**.
9. Click the right-arrow Play button in the menu bar to start EventReporter.

> **Important:** Run the EventReporter service under a user name that has access to the **\ETC$\log** folder.

Configure Windows Legacy Collector for CIFS Auditing

Note: This method is supported only with the Windows Legacy Collector in RSA NetWitness Suite. It is not supported in the CentOS Log Collector.

Set Up Your Windows Legacy Event Source Domain

Important: You only need to perform this task if this the first time you are configuring Windows Legacy event collection for RSA NetWitness Suite and have not set up your event source domain for NetWitness Windows Legacy collection.

To set up your event source domain for Windows Legacy event source collection:

1. Download the **RSA Security Analytics Legacy Windows Collection Update and Installation Instructions** guide from RSA Link here: https://community.rsa.com/docs/DOC-41196
2. Follow the instructions in this document to set up your event source domain so that the RSA NetWitness Log Collector can collect events from Windows Legacy event sources.

Configure the Windows Legacy Event Source in RSA NetWitness Suite:

To configure the Windows Legacy Event Source in RSA NetWitness Suite:

1. Visit RSA Link for NetWitness and search for the help topic **Configure Windows Legacy and NetApp Event Sources**.
2. Complete the steps in this topic using the following value for the **Event Log Name**:

   Application

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.