

RSA NetWitness Platform

Event Source Log Configuration Guide



Varonis DatAdvantage

Last Modified: Wednesday, June 27, 2018

Event Source Product Information:

Vendor: [Varonis](#)

Event Source: DatAdvantage

Versions: 5.5, 5.9.x, 6.x (6.x for Syslog only)

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 Download: rsavaronis.sql

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: varonisprobe

Collection Methods:

- ODBC for version 5.5
- Syslog for version 5.9 and newer

Event Source Class.Subclass: Security.Access Control

Depending on your version of Varonis DatAdvantage, integrate Varonis DatAdvantage the with RSA NetWitness Platform as follows:

- Configure Syslog collection for version 5.9 and newer, or
- Configure ODBC collection for version 5.5.

Configure Varonis DatAdvantage Version 5.9 and Newer

Perform the following tasks to configure Varonis DatAdvantage 5.9 and newer:

- Configure Varonis DatAdvantage to send Syslog
- Configure RSA NetWitness Platform for Syslog collection

Configure Varonis DatAdvantage to send Syslog to RSA NetWitness Platform

RSA NetWitness Platform uses Syslog to collect messages from DatAdvantage version 5.9 and newer.

To configure Varonis DatAdvantage to send Syslog:

1. Log onto Varonis DatAdvantage.
2. Select **Tools > DatAlert**.
3. Select the **Configuration** tab and fill in fields in the **Syslog Message Forwarding** section:

Field	Action
Syslog server IP address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	514
Facility name	Choose a value based on your environment.
Identity	Enter Varonis-Alert or use the default value.

4. Select the **Alert Templates** tab, and choose the **Varonis default template**.
5. In the **Apply to alert methods** field, select **Syslog message**.
6. Click **OK**, then **Apply** to save your changes.
7. Create and configure rules based on your environment.

Note: For each rule, ensure that **Syslog Message** is selected in the **Alert Method** tab.

Configure RSA NetWitness Platform for Syslog Collection

Perform the following steps in RSA NetWitness Platform:

- 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 Platform 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 **varonisprobe**.



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 Varonis DatAdvantage version 5.5

To configure Varonis DatAdvantage for ODBC collection, perform the following tasks:

- Configure a Microsoft SQL Server stored procedure
- Configure RSA NetWitness Platform for ODBC Collection

Configure a Microsoft SQL Server stored procedure

To set up Varonis DatAdvantage for ODBC:

1. Open Microsoft SQL Server Management Studio.
2. Select *varonis_server* > **Databases** > **Varonis** > **Programmability** > **Stored Procedures**.
3. Right-click **Stored Procedures**, and select **New Stored Procedure**.
4. Copy all contents from **rsavaronis.sql** to the new text file. The **rsavaronis.sql** file is available as an additional download from RSA Link here:
<https://community.rsa.com/docs/DOC-73478>
5. Click **Execute**.

Configure RSA NetWitness Platform for ODBC Collection

Perform the following procedures to configure RSA NetWitness Platform for ODBC collection:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

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 from RSA NetWitness Platform 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 **varonisprobe**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click **+** to open the **Add DSN** dialog.

Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).


7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Varonis
PortNumber	Specify the Port Number. The default port number is 1433

Field	Description
HostName	Specify the hostname or IP Address of Varonis
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

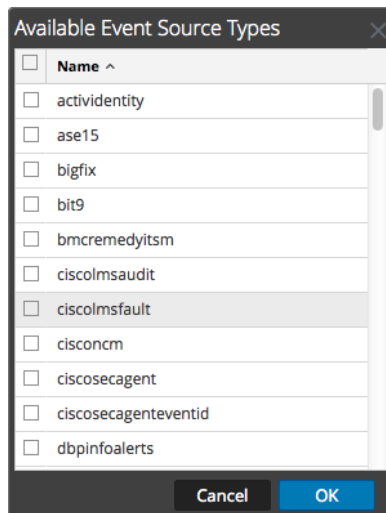
Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

The Event Categories panel is displayed with the existing sources, if any.

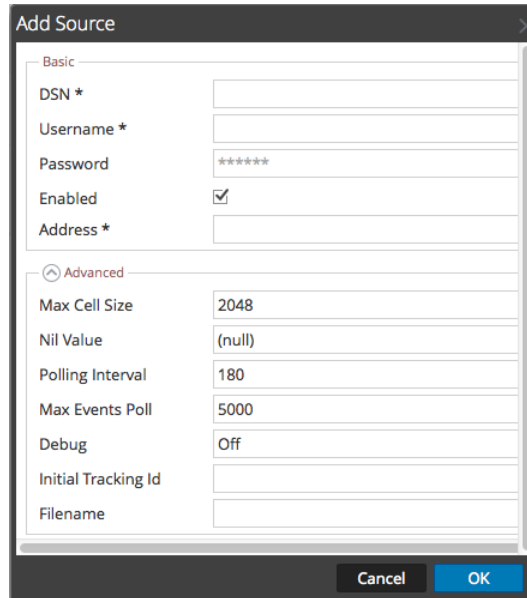
5. Click **+** to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

Select **varonisprobe** from the **Available Event Source Types** dialog.

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click **+** to open the **Add Source** dialog.



The screenshot shows the 'Add Source' dialog box with the following fields and values:

Section	Field	Value
Basic	DSN *	
	Username *	
	Password	*****
	Enabled	<input checked="" type="checkbox"/>
	Address *	
Advanced	Max Cell Size	2048
	Nil Value	(null)
	Polling Interval	180
	Max Events Poll	5000
	Debug	Off
	Initial Tracking Id	
	Filename	

9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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