RSA Event Source Configuration Guide

Varonis DatAdvantage

Last Modified:Friday, October 31, 2014

Event Source (Device) Product Information	
Vendor	Varonis
Event Source (Device)	DatAdvantage
Supported Versions	5.5, 5.9.x
Additional Downloads	rsavaronis.sql
RSA Product Information	
Supported Version	RSA enVision 4.1
Event Source (Device) Type	varonisprobe, 187
Collection Method	• ODBC on version 5.5 • Syslog on version 5.9
Event Source (Device) Class.Subclass	Security.Access Control
Content 2.0 Table	Access

This document contains the following information for the Varonis DatAdvantage event source:

Varonis DatAdvantage Configuration Instructions

Depending on your version of Varonis DatAdvantage, integrate Varonis DatAdvantage the with the RSA enVision platform as follows:

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

Configure Syslog Collection for Varonis DatAdvantage 5.9

RSA enVision uses Syslog to collect messages from DatAdvantage version 5.9.

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 your RSA enVision appliance.
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 ODBC Collection for Varonis DatAdvantage 5.5

To configure Varonis DatAdvantage version 5.5 to work with RSA enVision, you must complete these tasks:

I. Set up Varonis DatAdvantage

II. Add a data source to the NIC Collector Service

III. Set up the NIC ODBC Service

Set up Varonis DatAdvantage 5.5.

The RSA enVision platform uses ODBC to collect messages from DatAdvantage version 5.5.

To set up Varonis DatAdvantage for ODBC:

1. Open Microsoft SQL Server Management Studio.
2. Select **varonis_serv** > **Databases** > **Varonis** > **Programmability** > **Stored Procedures**.
3. Right-click **Stored Procedures**, and select **New Stored Procedure**.
4. Copy all contents from the **rsavaronis.sql** file to the new text file.
5. Click **Execute**.

Add Data Source to the NIC Collector Service

To add the Varonis DatAdvantage data source to the NIC Collector:

1. Follow these steps to add an SQL Server System data source:
    a. In your RSA enVision appliance, click **Start** > **Programs** > **Administrative Tools** > **Data Sources (ODBC)**.

    Note: If both of the Data Sources ODBC-32 and ODBC-64 are listed, select Data Source ODBC-32.

    b. In the **System DSN** tab, click **Add**.
    c. Select **SQL Server**.

    Note: If the Microsoft driver that you want is not available, download the latest MDAC files from the Microsoft web site.

    d. Click **Finish**.
2. Follow these steps to configure the SQL Server data source:

a. In the Create a New Source to SQL Server window, complete the fields as follows.

Field	Action
Name	Type **vrns**
Description	(Optional) Enter a description of the data source.
Server	Select your SQL server from the drop-down list, or enter the server name or IP address.

b. Click **Next**.

c. Select **With SQL Server Authentication**.

d. Verify that **Connect to SQL server to obtain default settings for the additional configuration options** is selected.

e. Create a logon ID and password.

Note: You will need this logon information when you set up the NIC ODBC Service.

f. Click **Next**.

g. Select **Change the default database to**.

h. From the drop-down list, select the database name given by Varonis.

i. Click **Next** > **Finish**.

3. Follow these steps to test the SQL data source:

a. In the ODBC Microsoft SQL Server Setup window, click **Test Data Source**.

b. Click **OK** to close the Microsoft SQL Server Setup window.

c. Click **OK** to save settings and close the ODBC Data Source window.

Set Up the NIC ODBC Service

Note: Since Varonis is database-intensive software, RSA recommends using an ODBC Interval of 2 minutes or more.

To set up the NIC ODBC Service in RSA enVision:

1. Log on to RSA enVision with your administrator credentials.
2. Click **Overview** > **System Configuration** > **Services** > **Device Services** > **Manage ODBC Service**.
3. In the Manage ODBC Service window, click **Add**.

4. To add the Varonis DatAdvantage data source, complete the fields as follows.

Field	Action
Data source name	Type **vrns**
Type	Select **VaronisProbe**
IP address	Select **Use static IP address associated with the data source name**, and enter the IP address of the database location.
User name	Enter the database logon ID that you created when you added the data source.
Password	Enter the password that you created when you added the data source.
Verify Password	Enter the password again.
Start ODBC Service on Apply	Ensure that **Start ODBC Service on Apply** is selected.

5. Click **Apply**.

Varonis DatAdvantage Release Notes (20141031-154112)

What's New in This Release

RSA has added support for Varonis DatAdvantage version 5.9.x.

New and Updated Event Messages in Varonis DatAdvantage

For complete details on new and updated messages, see the Event Source Update Help.