RSA NetWitness Platform

Event Source Log Configuration Guide

Microsoft Azure Security Alerts

Last Modified: Tuesday, June 16, 2020

Event Source Product Information:

Vendor: Microsoft
Event Source: Azure Security Alerts
Versions: API v1.0

RSA Product Information:

Supported On: Netwitness Platform 11.2.1 and later
Event Source Log Parser: cef

Note: The CEF parser parses this event source as **device.type=msazuregraph_security**.

Collection Method: Plugin Framework
Event Source Class.Subclass: Host.Cloud

To configure Microsoft Azure Security, you must complete these tasks:

I. Configure the Microsoft Azure Security event source

II. Set Up Microsoft Azure Security Event Source in RSA NetWitness

About Microsoft Graph Security

The Microsoft Graph Security ecosystem provides a unified interface to integrate with security solutions from Microsoft and other integrated solutions. Microsoft Graph Security Alerts are potential security issues within a customer's tenant that Microsoft or partner security solutions have identified and flagged for action or notification.

RSA Netwitness captures these alerts from Microsoft Azure through the Microsoft Graph API. Alerts via Microsoft Graph Security API from different providers can be found in the Microsoft Graph REST API documentation. The current link is here:

https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0#alerts

For more information, see https://docs.microsoft.com/en-us/graph/use-the-api.

> **Note:** Links to Microsoft web sites provided in this document are subject to change by Microsoft.

Configure the Microsoft Azure Security event source

This section describes how to use the Azure Management Portal to register your application in Azure AD, and to create a key.

To register your application:

1. Refer to the instructions in the Microsoft website for Register a New Application Using the Azure Portal to register the application.
2. Locate the API Permissions section for your registered application, and within the API permissions click **Add a permission**.
3. Assign the following Application Permissions to your registered application:
   - SecurityEvents.Read.All
   - SecurityEvents.ReadWrite.All

4. Navigate to the **Certificates and secrets** tab and create a new secret. The Application ID and secret key just created are required as inputs in Netwitness UI.

> **Important:** Azure only displays the client secret at the time you initially generate it. You cannot navigate back to this page and retrieve the client secret later. Make sure to copy and save this key, as it is needed for further configuration.

Set Up the Microsoft Azure Security Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

I. Deploy the CEF parser from Live

II. Configure the Microsoft Azure Security Event Source in NetWitness Platform.

Deploy Microsoft Azure Security Files from Live

Microsoft Azure Security plugin requires resources available in Live in order to collect logs.

To deploy the required content from Live:

1. In the RSA NetWitness Platform menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live Content for the **Common Event Format (cef)** parser, using **Log Device** as the **Resource Type**.

3. Select the **cef** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.

4. You also need to deploy the Microsoft Azure Security package. Browse Live for Microsoft Azure Security content, typing "msazuregraph_security" into the Keywords text box, then click **Search**.

5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

   > **Note:** If a remote VLC is being used for collection, then you need to deploy the plugin to the remote VLC as well as the Decoder

6. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Services Management Guide*.

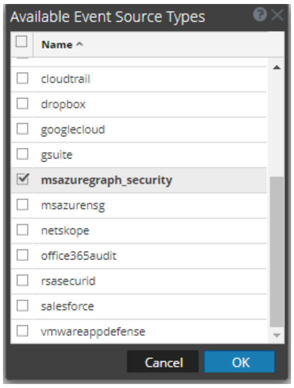
Configure the Microsoft Azure Security Event Source in NetWitness Platform

To configure the Microsoft Azure Security Event Source:

1. In the RSA NetWitness Platform menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.



□ **Name ^**

□ cloudtrail

□ dropbox

□ googlecloud

□ gsuite

☑ **msazuregraph_security**

□ msazurensg

□ netskope

□ office365audit

□ rsasecurid

□ salesforce

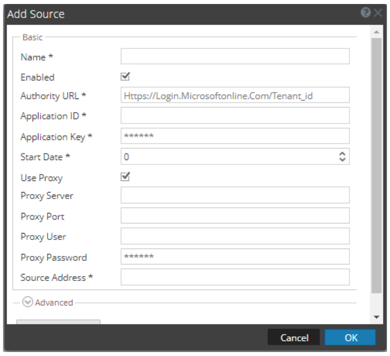
□ vmwareappdefense

5. Select **msazuregraph_security** from the list, and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

Name *	
Enabled	☑
Authority URL *	Https://Login.Microsoftonline.Com/Tenant_id
Application ID *	
Application Key *	******
Start Date *	0
Use Proxy	☑
Proxy Server	
Proxy Port	
Proxy User	
Proxy Password	******
Source Address *	

7. Define parameter values, as described in Microsoft Azure Security Collection Configuration Parameters.

8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   > **Note:** The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

10. Repeat steps 4–9 to add another Microsoft Azure Security plugin instance.

Microsoft Azure Security Collection Configuration Parameters

The following table describes the configuration parameters for the Microsoft Azure Security integration with RSA NetWitness Platform. Fields marked with an asterisk (*) are required.

Note: Items that are followed by an asterisk (*) required.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Authority URL *	Enter **https://login.microsoftonline.com/*<tenant-id>***
Application ID *	The Client ID is found the Azure Application Configure tab. Scroll down until you see it.
Application Key *	When you are configuring the event source, the client secret is displayed when you are creating a key, and you select duration of validation. Make sure to save this value, because you will only be able to see it once, and it cannot be retrieved later.
Start Date*	Choose the date from which to start collecting. This parameter defaults to the current date. Enter a value from 0 to 7, indicating how many days in the past from which to start.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).

Name	Description
Source Address *	IP address that is to be provided to the Azure Security plugin instance: logs from this event source will be collected with this device IP. **Note:** This is an arbitrary IP address chosen by the user. This value has no bearing on the collection of logs: its value is captured by the device.ip meta key, and can help you to query or group events collected by a particular instance of the plugin.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Note: Please avoid using special characters in the **Proxy User** and **Proxy Password** sections.

Advanced Parameters

Parameter	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.
Filter Query	Use the Filter Query parameter to retrieve subset of alerts. For details, see https://docs.microsoft.com/en-us/graph/query-parameters#filter-parameter.
CreatedDateTime	This setting determines which time value is used: • Select this box to pull alerts based on **CreatedDateTime**. • Clear this box to pull the alerts based on **LastModifiedTime**.

Trademarks

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