

NetWitness® Platform XDR

Microsoft Azure Log Analytics Wokspace Event Source Log Configuration Guide

Microsoft Azure Log Analytics Wokspace

Event Source Product Information:

Vendor: [Microsoft](#)

Event Source: Azure Log Analytics Wokspace

Versions: All

NetWitness Product Information:

Supported On: Netwitness Platform XDR 11.7 and later

Note: Azure Log Analytics Wokspace is supported from NetWitness Platform XDR 11.5. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: azure

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

Contents

Introduction to Microsoft Azure Log Analytics Wokspace	5
Configure the Microsoft Azure Log Analytics Workspace Event Source	6
Add Reader Role to the Log Analytics Workspace for Your Application:	6
Set up Azure Kubernetes Service (AKS) to Send Azure Kubernetes Logs to Log Analytics Workspace ...	8
NetWitness Supported Event Sources	9
Configure the Microsoft Azure Log Analytics Plugin in NetWitness Platform XDR	10
Microsoft Azure Log Analytics Collection Configuration Parameters	12
Basic Parameters	12
Advanced Parameters	13
Getting Help with NetWitness Platform XDR	15
Self-Help Resources	15
Contact NetWitness Support	15
Feedback on Product Documentation	16

Introduction to Microsoft Azure Log Analytics

Wokspace

A Log Analytics workspace is a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration but might combine data from multiple services. This article provides an overview of concepts related to Log Analytics workspaces and provides links to other documentation for more details on each. For more information, please refer [Log Analytics Workspace](#).

IMPORTANT: Links to Microsoft website provided in this document are subject to change by Microsoft.

To configure Microsoft Azure Graph, you must complete the following tasks

- I. [Configure the Microsoft Azure Log Analytics Workspace Event Source](#)
- II. [Configure the Microsoft Azure Log Analytics Plugin in NetWitness Platform XDR](#)

Configure the Microsoft Azure Log Analytics Workspace Event Source

This section describes how to use the Azure Management Portal to register an application in Azure Active Directory (Azure AD).

To register an application in Azure AD:

1. Go to [Register a New Application Using the Azure Portal](#) and follow the instructions to register an application.
2. Locate the API Permissions section for your registered application, and under the API permissions, click **Add a permission**.
3. Under the **APIs my organization uses** section type, click **Log Analytics API**.
4. Click **Application permissions**. Select **Data.Read** and click **Add permission**.

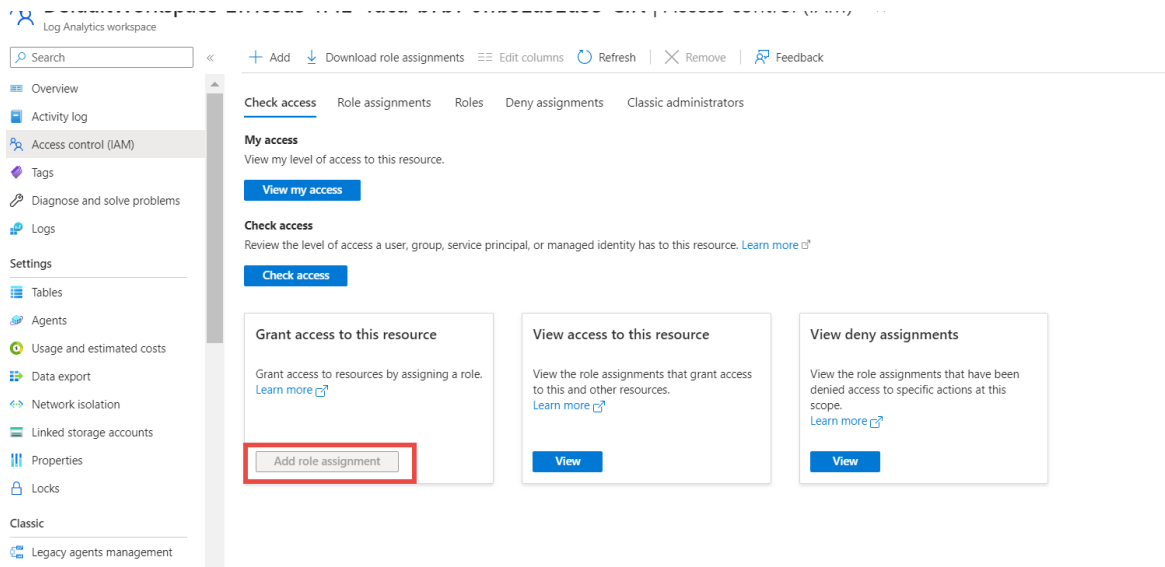
Note: Only Azure Admin can grant consent for **Data.Read**. If you are not an admin, consult the Azure Admin.

The screenshot shows the Azure Management Portal interface for configuring API permissions. The left sidebar contains navigation options like Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (selected), Expose an API, App roles, and Owners. The main content area shows the 'API permissions' section for the application 'test-message-trace'. A table lists the configured permissions:

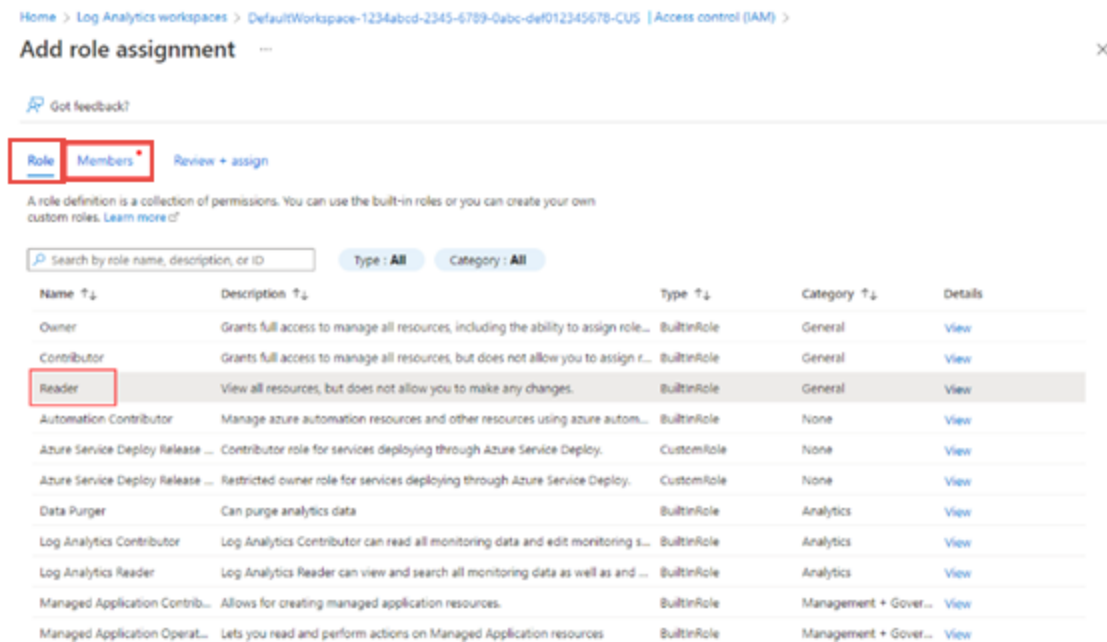
API / Permissions name	Type	Description	Admin consent requ...	Status
Log Analytics API (2)				
Data.Read	Delegated	Read Log Analytics data as user	No	...
Data.Read	Application	Read Log Analytics data	Yes	Granted for RSA Global ...

Add Reader Role to the Log Analytics Workspace for Your Application:

1. Go to your Log Analytics workspace and click **Add role assignment** in the Access control(IAM) tab.

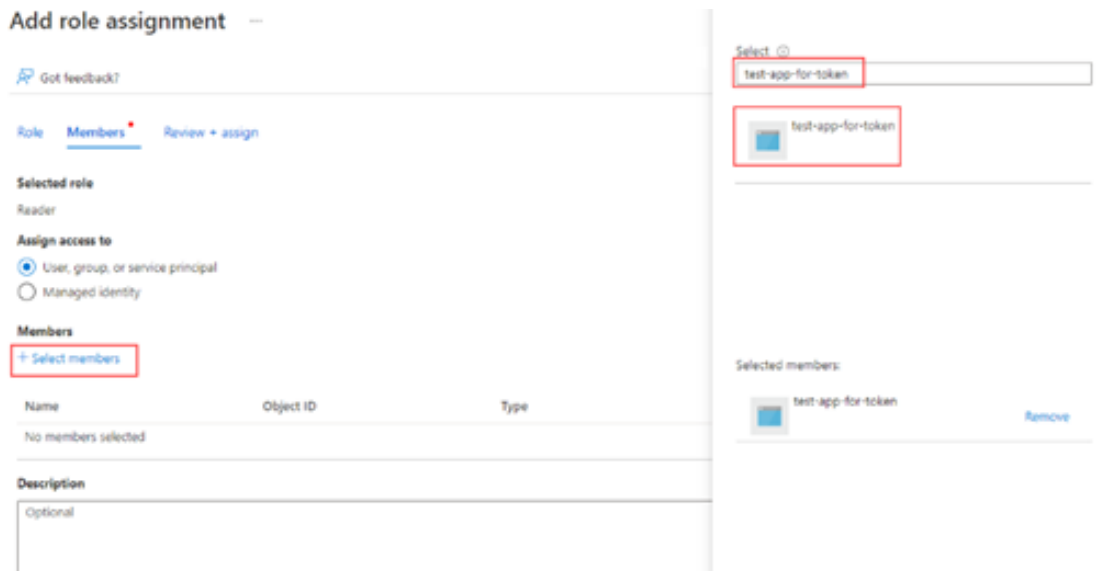


2. Under **Role** tab, select the *Reader* role then click **Members**.



3. In the **Members** tab, click **Select members**.

Select dialog appears on the right side.



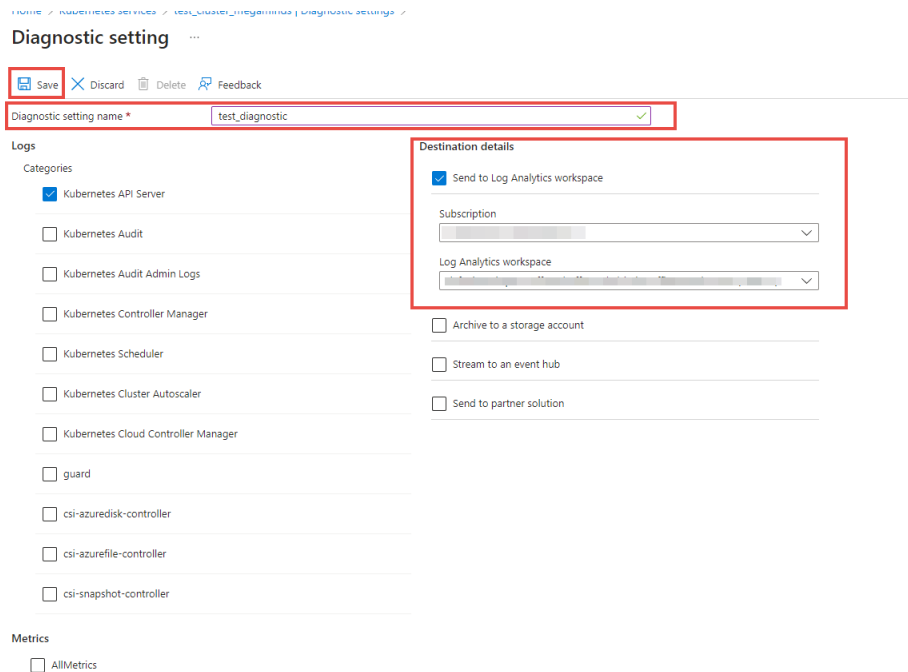
4. In the **Select** dialog, select your application name, Review the details and click **Assign**.

Set up Azure Kubernetes Service (AKS) to Send Azure Kubernetes Logs to Log Analytics Workspace

1. Go to the cluster in Azure Kubernetes Service and click on **Diagnostic setting**.
2. Click on **Add Diagnostic setting** and provide a **Diagnostic setting name**.
3. Select all the log categories which have to be captured in NetWitness Platform XDR.

The supported log categories are:

- Kubernetes API server
 - Kubernetes Audit
 - Kubernetes Audit Admin
 - Kubernetes Scheduler
 - Guard.
4. Select the **Destination details** as **Send to Log Analytics workspace**. Select the **Subscription** and **Log Analytics workspace** details in dialog.



5. Click **Save**.



NetWitness Supported Event Sources

The below table provides information about Microsoft Azure event sources and their permission details.

Microsoft Azure Event Sources	Parser Required	Configuration Steps
Azure Kubernetes	azure	<p>Table name AzureDiagnostics (case sensitive).</p> <p>Allowed log type = ["kube-apiserver", "kube-audit", "kube-audit-admin", "kube-scheduler", "guard"]. Enter the required log types from the list in Allowed log type above.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>IMPORTANT: Enter the logs types separated by comma without any space. Example : kube-apiserver, kube-audit.</p> </div>

Configure the Microsoft Azure Log Analytics Plugin in NetWitness Platform XDR

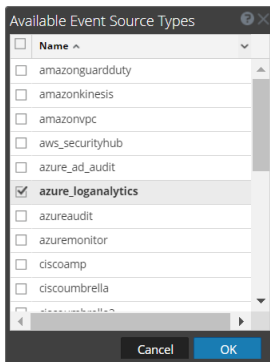
To configure the Microsoft Azure Log Analytics Event Source:

1. In the NetWitness Platform XDR menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Collector, and from the **Actions** () menu 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.

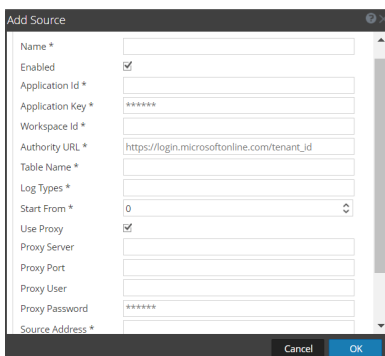


5. Select **azure_loganalytics** from the list, and click **OK**.

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.



7. Define parameter values, as described in [Microsoft Azure Log Analytics 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 NetWitness Platform XDR 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 Log Analytics plugin instance.

Microsoft Azure Log Analytics Collection

Configuration Parameters

The following table describes the configuration parameters for the Microsoft Azure Graph integration with NetWitness Platform XDR.

Note: Items that are followed by an asterisk (*) are 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	The box is selected by default. Select the box to enable the event source configuration to start collection.
Application ID*	The Application ID is found in the Azure Application Configure tab. Scroll down until you see it.
Application Key *	Enter the Client Secret or Private key.
Workspace ID*	Enter Log analytics workspace ID. The Workspace ID is found in the Azure Kubernetes Service, Application Log Analytics Service > Select specific Log Analytics Workspace > Overview .
Authority URL *	Enter <code>https://login.microsoftonline.com/<tenant-id></code> . Replace tenant-id with your tenant ID.
Table Name*	See NetWitness Supported Event Sources to find the correct Table Name.
Log Types*	Enter logs types separated by comma without any space. Example : kube-apiserver, kube-audit. For more information, see NetWitness Supported Event Sources .
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 collection.
	Note: Do not edit the Start Date value of a running graph plugin instance. This value is used for bookmarking purpose to avoid collection of duplicate logs. To start from a different start date, create a new plugin event source.
Use Proxy	Check to enable proxy.

Name	Description
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).
Source Address *	IP address that is provided to the Azure Graph plugin instance. Logs from this event source will be collected using 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	<p>Caution: Enable debugging (set this parameter to On or Verbose) only 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.</p> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed to debug and monitor isolated event source collection issues. After changing 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.</p>
SSL Enabled	<p>The check box is selected by default.</p> <p>Uncheck this box to disable SSL certificate verification.</p>

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases .
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.