

NetWitness[®] Platform

Azure Monitor Event Source Log Configuration Guide

Azure Monitor

Event Source Product Information:

Vendor: [Microsoft](#)

Event Source: Azure Monitor Activity and Diagnostic Logs

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: azure

Note: NetWitness can now parse JSON event data directly on the Log Decoder and there is no need to transform logs into CEF. Previously, plugins had to be tailored to each JSON schema individually. Now, all of the raw JSON event data is sent straight to the Log Decoder. In v11.5, the plugin will collect logs in JSON event data and will pass them through to Log decoder directly in RFC 5424 format by adding a header, and it will be parsed by the JSON parser instead of the CEF parser. So to parse Azure monitor events, the azure parser needs to be deployed from Live.

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 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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2023

Contents

About Azure Monitor	5
Configure Azure Monitor to Export Activity and Diagnostic Logs to an EventHub	6
Set Up the Azure Monitor Event Source in NetWitness Platform	7
Deploy Azure Monitor Files from Live	7
Configure the Event Source	7
Azure Monitor Collection Configuration Parameters	10
Basic Parameters	10
Advanced Parameters	11
Getting Help with NetWitness Platform	12
Self-Help Resources	12
Contact NetWitness Support	12
Feedback on Product Documentation	13

About Azure Monitor

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources upon which they depend. Azure Monitor has the functionality to export Azure Activity, Diagnostic, Azure Active Directory Sign-in and Audit Logs.

The **Azure Activity Log** is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events. Using the Activity Log, you can determine the ‘what, who, and when’ for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties.

Azure Monitor Diagnostic Logs are logs emitted by an Azure service that provide rich, frequent data about the operation of that service.

Azure Active Directory Events consist of the following two type of Events:

- Sign-ins: Sign-in logs provides information about the usage of managed applications and user sign-in activities.
- Audit logs: Audit logs provide traceability through logs for all changes done by various features within Azure AD. Examples of audit log entries include changes made to any resources within Azure AD, such as adding or removing users, apps, groups, roles and policies.

For more information, see the following topics, available from Microsoft Docs website (docs.microsoft.com):

- Azure Activity Logs: [Monitor Subscription Activity with the Azure Activity Log](#)
- Azure Monitor Diagnostic Logs: [Collect and consume log data from your Azure Resources](#)
- Azure AD events: [Azure AD activity logs in Azure Monitor](#)

NetWitness can capture Azure Activity and Diagnostic logs through Azure EventHub. To set it up, complete the following tasks:

- I. [Configure Azure Monitor to Export Activity and Diagnostic Logs to an EventHub](#)
- II. [Set Up the Azure Monitor Event Source in NetWitness Platform.](#)

Configure Azure Monitor to Export Activity and Diagnostic Logs to an EventHub

Please refer to the following topics on Microsoft Docs website (docs.microsoft.com):

- To create an EventHub and forward Activity Logs to it, perform the steps described in [Stream the Azure Activity Log to Event Hubs](#)
- To export Diagnostic Logs to an EventHub, perform the steps described in the following link: [Stream Azure Diagnostic Logs to an event hub](#)
- To export Azure AD Sign-In and Audit logs to an EventHub, perform the steps described in the following link: [Azure AD activity logs in Azure Monitor](#).

Note: Ensure that the EventHub you are using has four partitions.


Set Up the Azure Monitor Event Source in NetWitness Platform

In NetWitness Platform, perform the following tasks:

- I. [Deploy Azure Monitor Files from Live](#)
- II. [Configure the Event Source](#).

Deploy Azure Monitor Files from Live

To deploy the parser from Live:



1. In the NetWitness Platform menu, select  (Configure) > **Live Content**.
The **Live Content** tab is displayed.
2. Browse Live Content for the **azure**, parser using **Log Device** as the **Resource Type**.
Select the **azure** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.
3. You also need to deploy the Azure Monitor package. Browse **Live Content** for Azure Monitor Event Logs content, typing "azuremonitor" into the Keywords text box, then click **Search**.
4. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

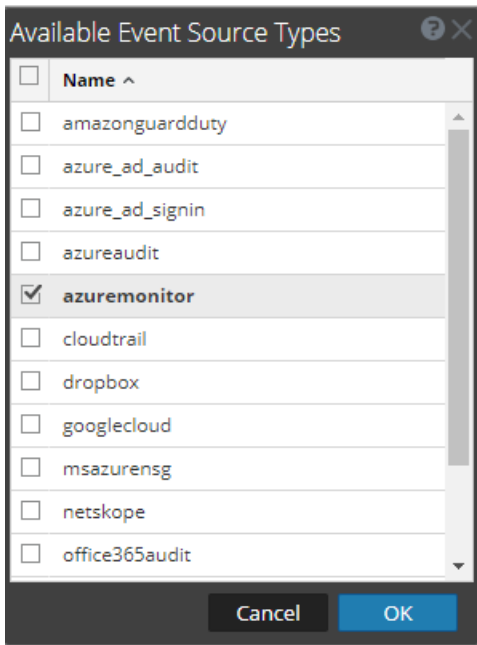
Note: On a hybrid installation, you need to deploy the package on both the Virtual Log Collector (vLC) and the Log Collector (LC).

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic.

Configure the Event Source

To configure the Azure Monitor Platform Event Source:

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

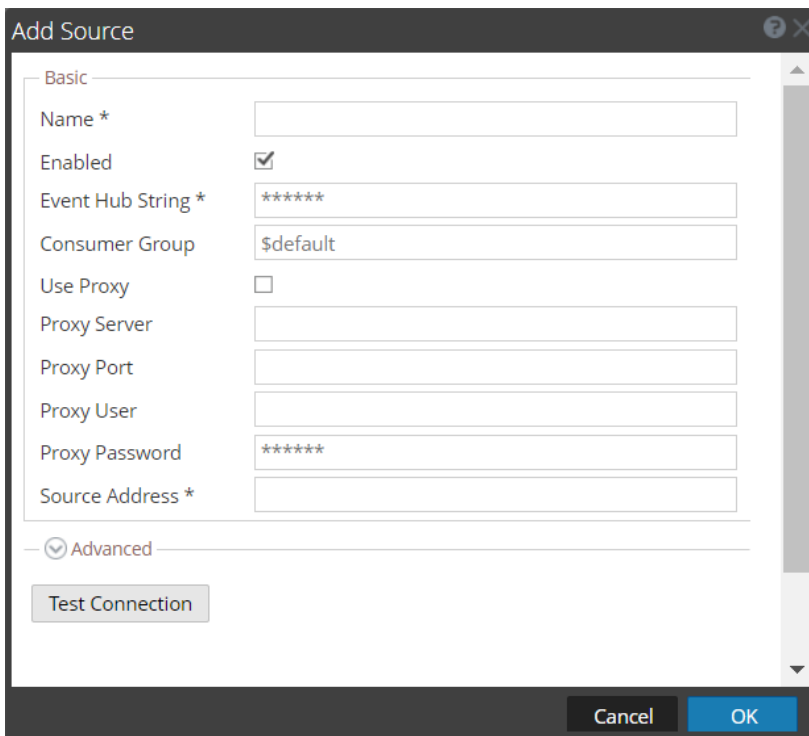


5. Select **azuremonitor** from the list, and click **OK**.

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 [Azure Monitor Collection Configuration Parameters](#).

8. Click **Test Connection**.

The test result 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 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 Azure Monitor plugin type.

Azure Monitor Collection Configuration Parameters

The following table describes the configuration parameters for the Azure Monitor Platform integration with NetWitness Platform.

Note the following:

- Fields marked with an asterisk (*) are required to successfully complete the configuration.
- If a proxy is being used, the proxy shall allow traffic through port 5671 (used for AMQPS).

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.
Event Hub String	You obtain the Event Hub connection string from the Access Policy tab of the Event Hub.
Consumer Group	Enter Consumer Group if any.
Use Proxy	Select the box to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	If proxy is being used, then the proxy shall allow traffic through port 5671, used for AMQPS.
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 to be provided to the Azure Monitor 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.

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	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit. > 300 is the default value.
Command Args	Optional arguments to be added to the script invocation.
Debug	<div> 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. </div> <p>Enables and disables debug logging for the event source.</p> <p>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. The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> <p>If you change this value, the change takes effect immediately (no restart required).</p>
SSL Enable	Uncheck this box to disable SSL certificate verification.

Getting Help with NetWitness Platform

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 the documentation for Logstash JDBC input plugin here:
<https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- 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 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 feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.