NetWitness® Platform

Microsoft Azure Event Source Log Configuration Guide

NETWITNESS
Platform

Microsoft Azure

Last Modified: Tuesday, September 17, 2024

Event Source Product Information:

Vendor: Microsoft

Event Source: Azure

Versions: all

RSA Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: cef

Collection Method: azureaudit

Event Source Class.Subclass: Host.Cloud

Note: Azure AD Graph API is now deprecated. For more information, see https://docs.microsoft.com/en-us/previous-versions/azure/ad/graph/api/api-catalog. Customers using NetWitness Platform version 12.2 or later can use either the Azure Monitor or MS Azure Graph plugin to capture Azure events.

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

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

August 2024

Contents

Collecting Azure Events in NetWitness Platform

Microsoft Azure is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

The following topics describe how to configure Azure as an event source:

1. Configure the Azure Event Source
2. Set Up the Azure Event Source in NetWitness Platform
3. Azure Collection Configuration Parameters
4. Troubleshooting Collection From the Azure Event Source

Azure Collection Plugins

There are 3 plugins associated with Azure collection:

- **azureaudit**: collects management logs

Note: You may need to have Microsoft Azure premium access to collect the audit logs.

Azureaudit

This plugin collects Azure resource management events:

- What, who, and when information for any write operations (PUT, POST, DELETE) taken on the resources in your subscription.
- **Administrative**: for example, "create virtual machine" and "delete network security group“
- **Service Health**: for example, "SQL Azure in East US is experiencing downtime.“
- **Alert**: for example, "CPU % on myVM has been over 80 for the past 5 minutes."
- **Autoscale**: for example, "Autoscale scale up action failed."
- BaseURL: https://management.azure.com
- Microsoft documentation: Monitor Subscription Activity with the Azure Activity Log

Configuration in Azure

These are the Azure configuration procedures for all of the plugins:

1. Create an Active directory application and create a secret key.
2. Set APIs and permissions for the created App.
   - If you are collecting using **azureaudit**, use the **Azure service management API**.
3. Assign a Role to created App.

Note: Azure AD Graph API is now deprecated. For more information, see https://docs.microsoft.com/en-us/previous-versions/azure/ad/graph/api/api-catalog. Customers using NetWitness Platform version 12.2 or later can use either the AzureMonitor or MS Azure Graph plugin to capture Azure events.

Azure Configuration Goals

The Microsoft Azure interface is subject to change at any time. Thus, it is difficult for this documentation to provide accurate steps for the procedures that the configuration of Azure with NetWitness requires. The following list describes what you need to accomplish, rather than the exact steps to perform in Microsoft Azure.

- The NetWitness plugins and scripts need to authenticate to the Azure APIs
- To accomplish this, you must create a "client application" within Azure Active Directory (AD).
- This client app functions as a common authentication point for our scripts to each of the Azure APIs
- As you create your client app, you need to obtain some IDs and parameters that you need to provide during the event source configuration in NetWitness.
- Finally, you need to assign your client app a "role" (typically with **Reader** or **Security Reader** permissions) in Azure, for access to subscriptions within a tenant.

  Note: To collect **azureaudit** events, the **Reader** role is sufficient.

Later in this guide, we provide steps to configure the client app. However, as noted, the steps may vary based on updates and changes by Microsoft. In addition to following these steps, you must also:

1. Add APIs for the NetWitness provided scripts to access.
2. Grant permissions to use them for this client app.
3. Create a secret key and gather other configuration settings and IDs for use in our Event Source Configuration.

Configure the Azure Event Source

Configuration Procedures

To configure Azure, you must complete these tasks:

I. Create an Active Directory Application

II. Get Client ID and Authentication Key

III. Get the Federation Metadata Endpoint

IV. Set Permissions

V. Assign a Role to the AD Application

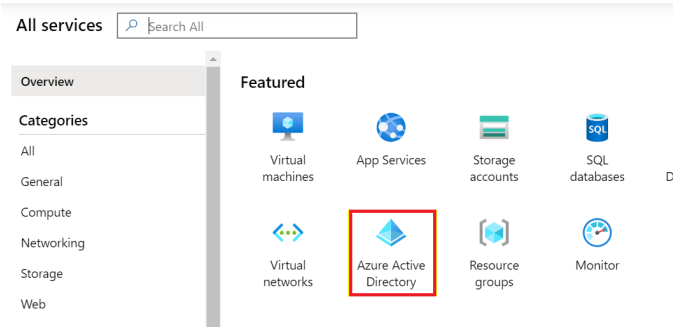
Create an Active Directory Application

You can currently view the Microsoft Azure Prerequisites to access the Azure AD reporting API topic for more details. Note, however, that Microsoft can move or delete that link whenever it chooses.

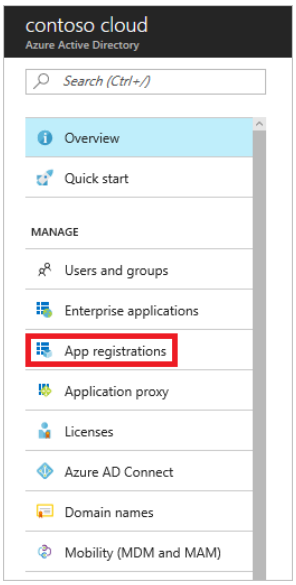
To create an Active Directory application:

Note: These instructions are available on the Microsoft Azure page Prerequisites to access the Azure AD reporting API.

1. Log in to your Azure account through the Microsoft Azure portal (https://portal.azure.com).
2. Make sure you know the default Active Directory for your subscription, as you can only grant access for applications in the same directory as your subscription.
3. Select **Active Directory** from the left pane.



4. On the **Azure Active Directory** blade, click **App registrations**.



5. On the **App registrations** blade, in the toolbar on the top, click **New application registration**.

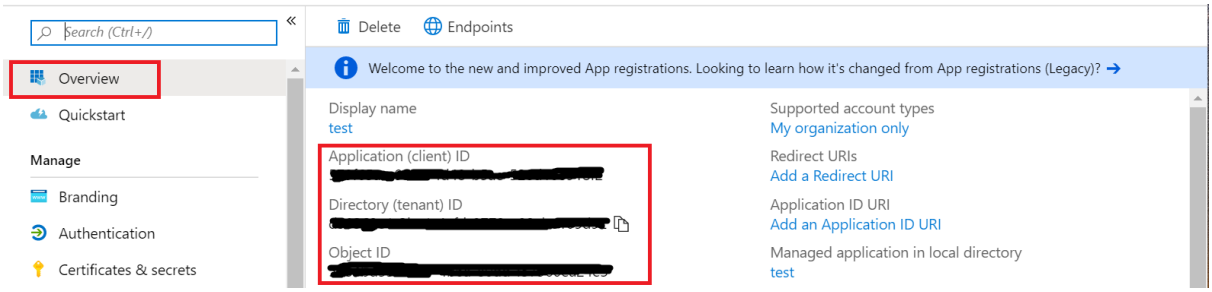
6. On the **Create** blade, perform the following steps:
   a. Provide a name for the application.
   b. Select the **Application type** from the drop-down menu.
   c. For **SIGN-ON URL**, enter `http://localhost`
   d. Click **Create**.

Get Client ID and Authentication Key

When programmatically logging in, you need the client ID for your application. To use with RSA NetWitness Platform, you also need an authentication key.

To get your client ID and key:

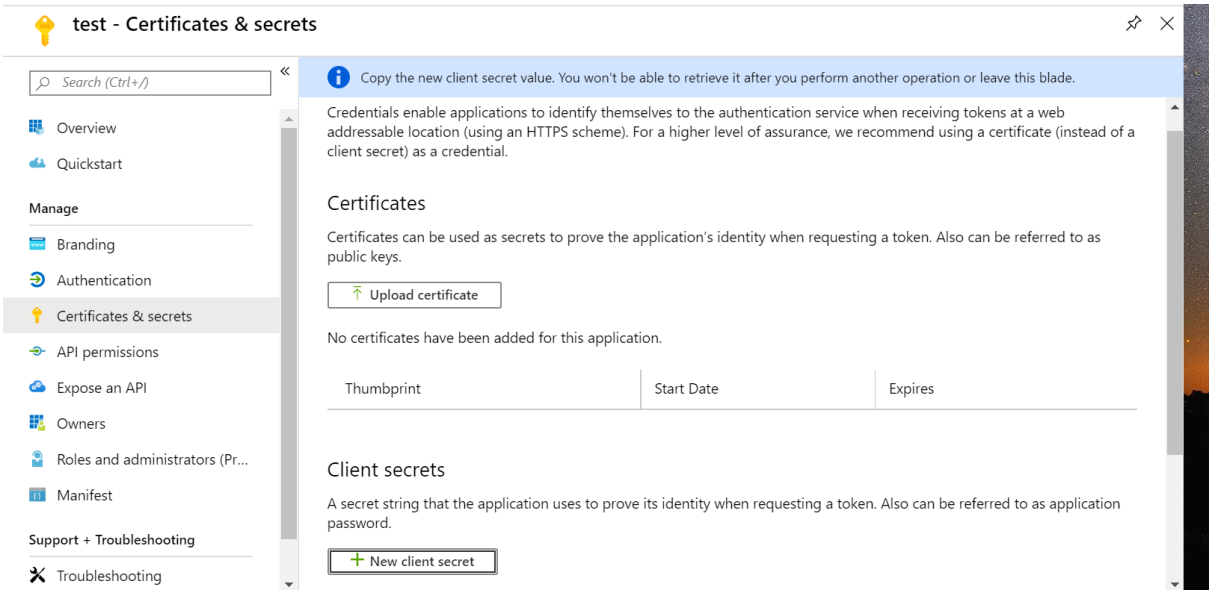
1. The Object ID and Application (client) ID can be found on the Overview page.



2. Copy the Application (client) ID.

Note: You will need this later, when configuring the event source in RSA NetWitness Platform.

3. In the left navigation panel, select new **Certificates and Secrets**.
4. In the **Client secrets** section, click **New Client secret** to create a key.



5. Add a description for the key and add an expiration date.
6. Click **Add** to create your key.

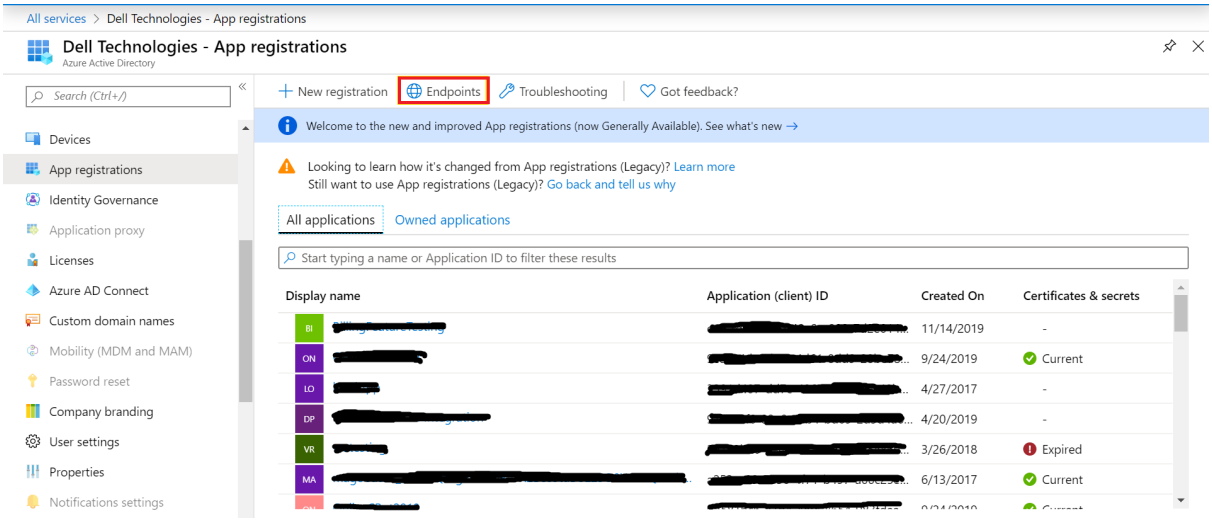
Warning: The saved key is displayed and you **must** copy it now. You will not be able to retrieve the key later.

Get the Federation Metadata Endpoint

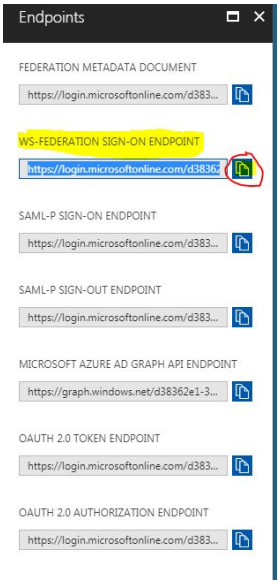
You will need to pass the Federation Metadata Endpoint with authentication requests to RSA NetWitness Platform.

To retrieve the Federation Metadata Endpoint:

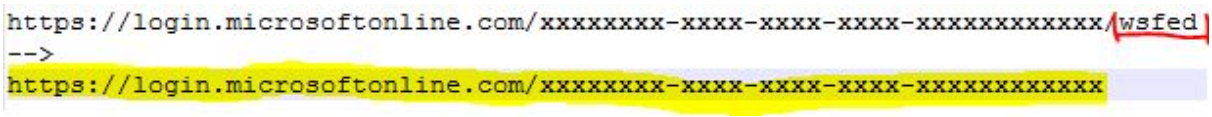
1. Navigate to **Active Directory > App Registrations > Endpoints**.



2. Copy the URL in the WS-FEDERATION SIGN-ON ENDPOINT field.



3. Remove the trailing **/wsfed** characters from the end of the listed URL.



Set Permissions

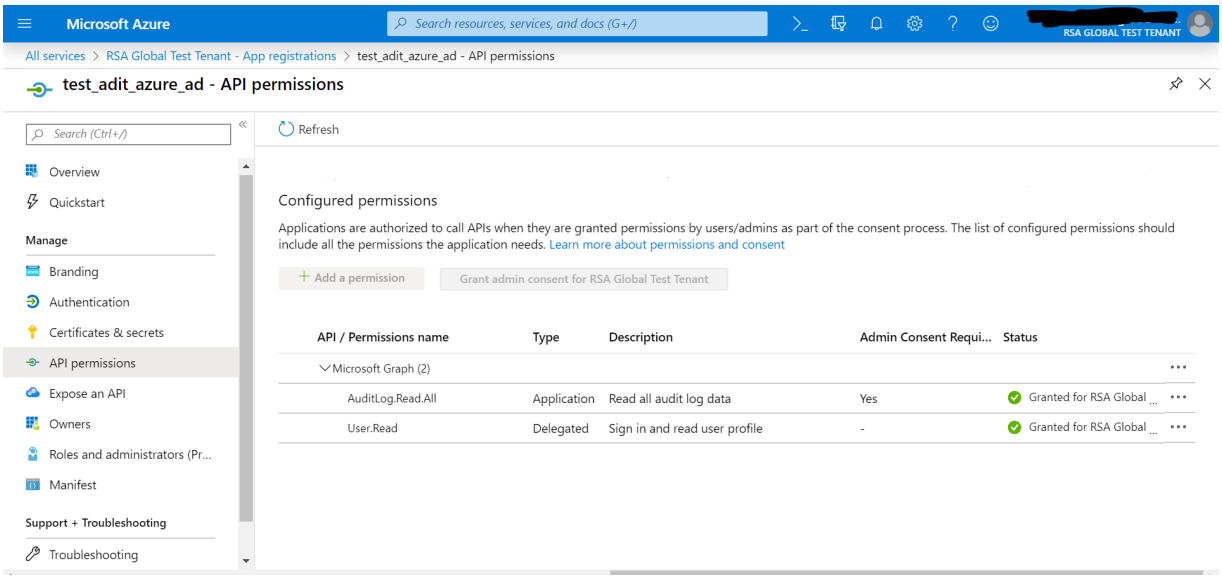
If your application accesses resources on behalf of a signed-in user, you must grant your application the permission to access other applications. You do this in the **API permissions** section. By default, a delegated permission is already enabled for the Azure Active Directory. Leave this delegated permission unchanged.

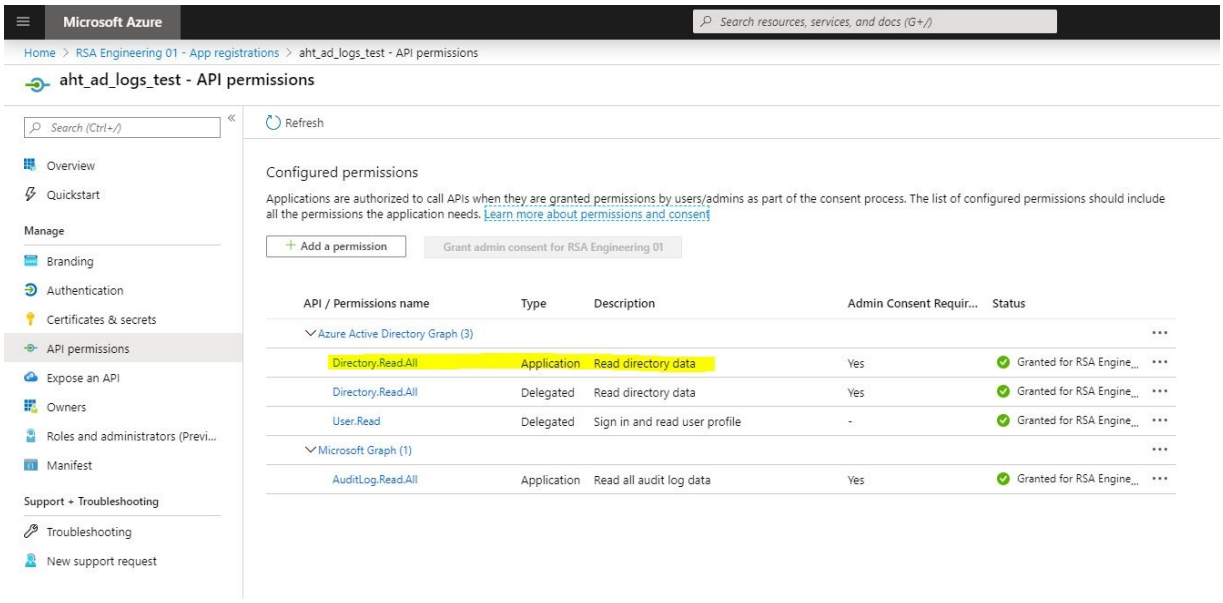
1. In the API permissions section, click **Add a permission**.
2. Under the Microsoft APIs, select **Azure Service Management** and click on **Application permission**.
3. Add the permissions you require:
   - To configure **azure_audit** logs alone, the required application permission is **AuditLog.Read.All**.
4. After you select the required permissions, click **Add permissions**.

Note: To set the permissions above, you might need administrator access.

After you add permissions, the API permissions window looks like the following:

- For azure_audit:





Assign a Role to the AD Application

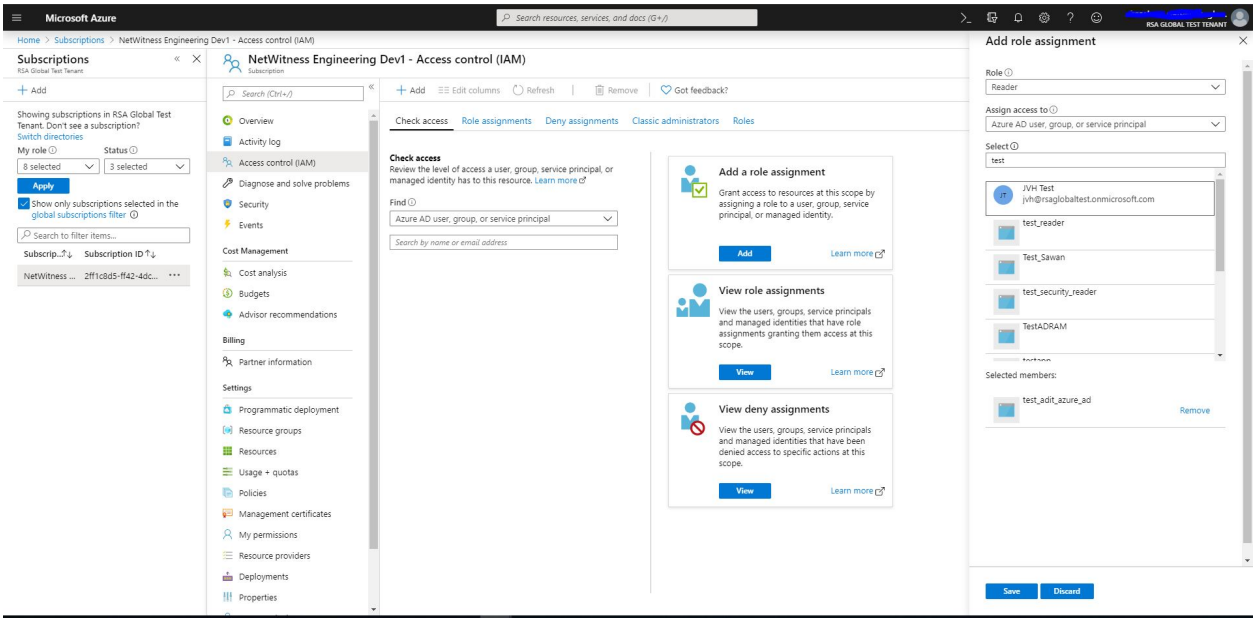
Note: Instructions in this section were adapted from the following Microsoft Azure documentation topic: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure#add-access.

This section describes how to set permissions for the entire subscription. You can also grant permissions on a more restrictive level, for example, for each "resource group." The steps do this are similar: see the Microsoft Azure documentation (linked in the previous note) for details.

To add a *Reader* role for the client application:

1. Navigate to **Subscriptions** in the Azure portal.
2. Select the subscription that you want to read from and click **Access Control(IAM)**.
3. Under **Add a role assignment**, click **Add**.
4. Under the **Role** heading, select **Reader**, and under **SELECT**, choose your application name.
5. Click **Save**.

The following screen shows an example subscription and Reader role.



Set Up the Azure Event Source in NetWitness Platform

In NetWitness Platform, perform the following tasks:

- Deploy the Azure plugins and cef parser from Live.
- Configure the event source.

Deploy the Azure Files from Live

Azure requires resources available in Live in order to collect Azure logs.

To deploy the Azure content from Live:

1. In the NetWitness Platform menu, select **Live**.
2. Browse Live for **Azure** content, typing **azure** into the **Keywords** text box and click **Search**.
3. Select the items returned from the Search
   - MS Azure Active Directory Audit Log Collector Configuration
4. Click Deploy to deploy the parsers to the appropriate Log Collectors, using the Deployment Wizard.
5. Repeat steps 2–4 to find and deploy the **cef** parser.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Resource Guide* on NetWitness Link.

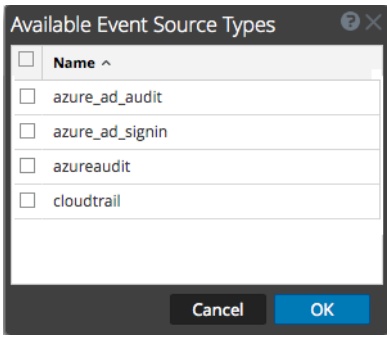
Configure the Azure Event Source

To configure the Azure Event Source:

1. In the NetWitness Platform menu, select **Administration** > **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.

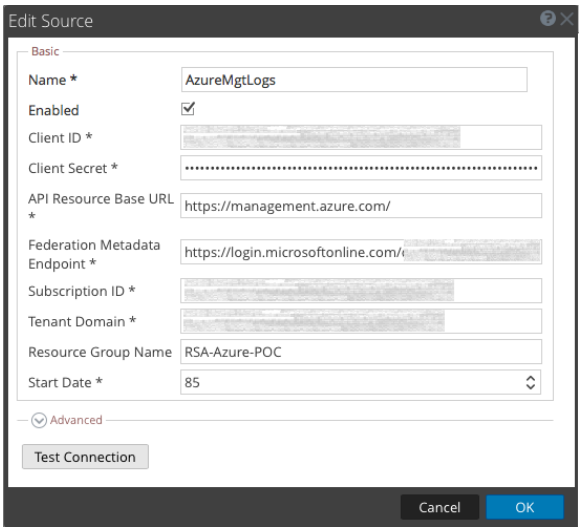


5. Select one of the Azure entries from the list, and click **OK**.

   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.



Note: This dialog box is for the **azureaudit** plugin. The available parameters for the other Azure plugins are slightly different.

7. Define parameter values, as described in Azure 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.

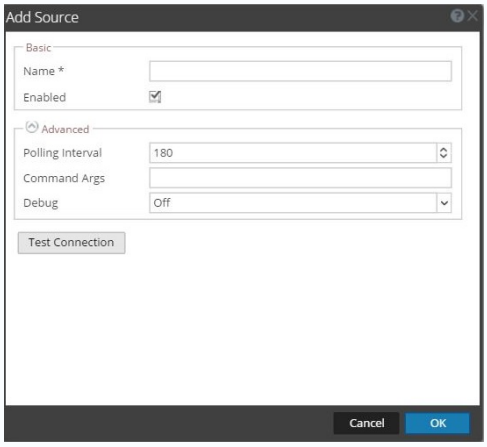
Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform displays an error message.

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 plugin type.

Troubleshooting Collection From the Azure Event Source

Issue	Details
Category azureaudit visible but not usable	Users that have a Log Collector at a version older than 10.6.2 will see the plugin for Azure, but cannot add a source. This is visible if you have pulled down new content from Live after the release of Security Analytics 10.6.2. If you navigate to your **LC > View | Config > Event Sources > Plugins | Config**, you can add the **azureaudit** Event Category. However, if you attempt to add a source, the Add Source dialog box will not contain any of the Azure parameters: 
Content overwritten after an upgrade to 10.6.2	If you pulled down new content from Live before you upgraded to 10.6.2, RSA strongly recommends that you pull down the content **again**, after you upgrade. Note that the Logcollector service will need to be restarted after you pull down the new content.

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.