NetWitness® Platform

Microsoft Azure NSG (Flow Logs) Event Source Log Configuration Guide

NETWITNESS
Platform

Microsoft Azure NSG (Flow Logs)

Last Modified: Thursday, November 14, 2024

Event Source Product Information:

Vendor: Microsoft

Event Source: NSG (Flow Logs)

Versions: all

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: cef

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

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

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

November 2024

Contents

This document contains the following sections:

- NSG Flow Logs in Azure
- Set Up Microsoft Azure NSG Event Source in RSA NetWitness

NSG Flow Logs in Azure

Network Security Group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through a Network Security Group. These flow logs are written in JSON format and show outbound and inbound flows on a per rule basis, the NIC the flow applies to, 5-tuple information about the flow (Source and Destination IP, Source and Destination Port, and Protocol), and if the traffic was allowed or denied.

While flow logs target Network Security Groups, they are not displayed in the same manner as the other logs. Flow logs are stored only within a storage account and follow the logging path as shown in the following example:

```
https://{storageAccountName}.blob.core.windows.net/insights-logs-
networksecuritygroupflowevent/resourceId%3D/subscriptions/
{subscriptionId}/resourcegroups/
{resourceGroupName}/providers/microsoft.network/networksecuritygroups/
{nsgName}/{year}/{month}/{day}/PT1H.json
```

Event Format

Flow log messages have the following format:

- **time**: The time when the event was logged
- **systemId**: Network Security Group resource ID
- **category**: The category of the event; this is be **NetworkSecurityGroupFlowEvent**
- **resourceid**: The resource ID of the NSG
- **operationName**: Always **NetworkSecurityGroupFlowEvents**
- **properties**: A collection of properties of the flow, as follows:
  - **Version**: Version number of the Flow Log event schema
  - **flows**: A collection of flows. This property has multiple entries for different rules:
    - **rule**: Rule for which the flows are listed.
      - **flows**: a collection of flows
        - **mac**: The MAC address of the NIC for the VM where the flow was collected
        - **flowTuples**: A string that contains multiple properties for the flow tuple in comma-separated format
          - **Time Stamp** - This value is the time stamp of when the flow occurred in UNIX EPOCH format
          - **Source IP** - The source IP
          - **Destination IP** - The destination IP
          - **Source Port** - The source port

- **Destination Port** - The destination Port
- **Protocol** - The protocol of the flow. Valid values are T for TCP and U for UDP
- **Traffic Flow** - The direction of the traffic flow. Valid values are **I** for inbound and **O** for outbound.
- **Traffic** - Whether traffic was allowed or denied. Valid values are A for allowed and D for denied.

Log Format Example

Assume a log message as follows:


```
{"time":"2018-01-01T07:15:49.5426087Z","systemId":"cbdb1b39-ac02-4876-ad8e-
c06761aebd13","category":"NetworkSecurityGroupFlowEvent","resourceId":"/SUBSC
RIPTIONS/2FF1C8D5-FF42-4DCD-B7B1-0FFB52A31F33/RESOURCEGROUPS/LT-VPN-
RESGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/LT-NSG-
DEFAULT","operationName":"NetworkSecurityGroupFlowEvents","properties":
{"Version":1,"flows":[{"rule":"UserRule_PontusAll","flows":
[{"mac":"000D3A103552","flowTuples":
["1514790906,xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,123,123,U,O,A","1514790926,xxx.x
xx.xxx.xxx,yyy.yyy.yyy.yyy,61377,53,U,O,A","1514790926,xxx.xxx.xxx.xxx,yyy.yy
y.yyy.yyy,51258,443,T,O,A"]}]}]}}
```


This message is converted into the following multiple sub-logs:

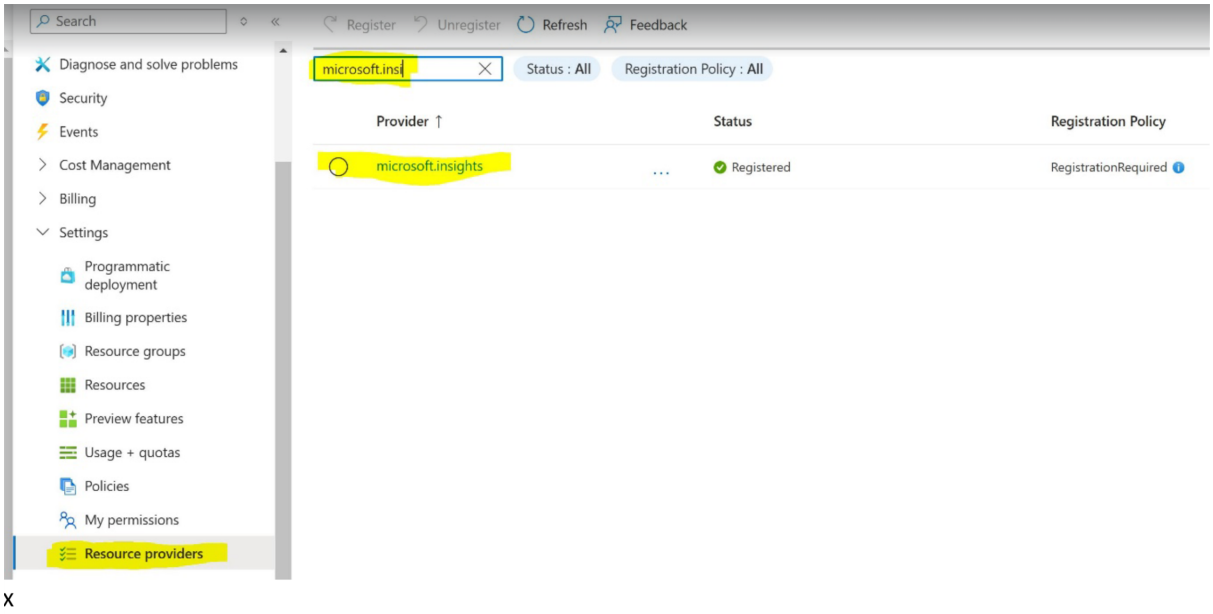

```
Jan 01 2018 08:19:50 cbdb1b39-ac02-4876-ad8e-c06761aebd13
CEF:0|Microsoft|Azure
NSG|1|NetworkSecurityGroupFlowEvents|NetworkSecurityGroupFlowEvents|5|categor
y=NetworkSecurityGroupFlowEvent src=xxx.xxx.xxx.xxx proto=UDP
deviceDirection=outbound resourceId=/SUBSCRIPTIONS/2FF1C8D5-FF42-4DCD-B7B1-
0FFB52A31F33/RESOURCEGROUPS/LT-VPN-
RESGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/LT-NSG-DEFAULT
operationName=NetworkSecurityGroupFlowEvents rulename=UserRule_PontusAll
timestamp=1514790906 macaddr=000D3A103552 version=1 systemId=cbdb1b39-ac02-
4876-ad8e-c06761aebd13 eventtime=2018-01-01T07:15:49.5426087Z dpt=123
action=allowed spt=123 dst=yyy.yyy.yyy.yyy


Jan 01 2018 08:19:50 cbdb1b39-ac02-4876-ad8e-c06761aebd13
CEF:0|Microsoft|Azure
NSG|1|NetworkSecurityGroupFlowEvents|NetworkSecurityGroupFlowEvents|5|categor
y=NetworkSecurityGroupFlowEvent src=xxx.xxx.xxx.xxx proto=UDP
deviceDirection=outbound resourceId=/SUBSCRIPTIONS/2FF1C8D5-FF42-4DCD-B7B1-
0FFB52A31F33/RESOURCEGROUPS/LT-VPN-
RESGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/LT-NSG-DEFAULT
operationName=NetworkSecurityGroupFlowEvents rulename=UserRule_PontusAll
timestamp=1514790926 macaddr=000D3A103552 version=1 systemId=cbdb1b39-ac02-
4876-ad8e-c06761aebd13 eventtime=2018-01-01T07:15:49.5426087Z dpt=53
action=allowed spt=61377 dst=yyy.yyy.yyy.yyy
```

```
Jan 01 2018 08:19:50 cbdb1b39-ac02-4876-ad8e-c06761aebd13
CEF:0|Microsoft|Azure
NSG|1|NetworkSecurityGroupFlowEvents|NetworkSecurityGroupFlowEvents|5|categor
y=NetworkSecurityGroupFlowEvent src=xxx.xxx.xxx.xxx proto=TCP
deviceDirection=outbound resourceId=/SUBSCRIPTIONS/2FF1C8D5-FF42-4DCD-B7B1-
0FFB52A31F33/RESOURCEGROUPS/LT-VPN-
RESGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/LT-NSG-DEFAULT
operationName=NetworkSecurityGroupFlowEvents rulename=UserRule_PontusAll
timestamp=1514790926 macaddr=000D3A103552 version=1 systemId=cbdb1b39-ac02-
4876-ad8e-c06761aebd13 eventtime=2018-01-01T07:15:49.5426087Z dpt=443
action=allowed spt=51258 dst=yyy.yyy.yyy.yyy
```

See network-watcher-nsg-flow-logging-overview for more details.

Configure NSG Flow Logs in Azure

1. Log into the Azure portal at https://portal.azure.com.
2. Go to **Subscriptions**, and then select the subscription for which you want to enable flow logs.
3. On the **Subscription** blade, select **Resource Providers**.
4. Look at the list of providers, and verify that the **microsoft.insights** provider is registered. If not, then select **Register**.



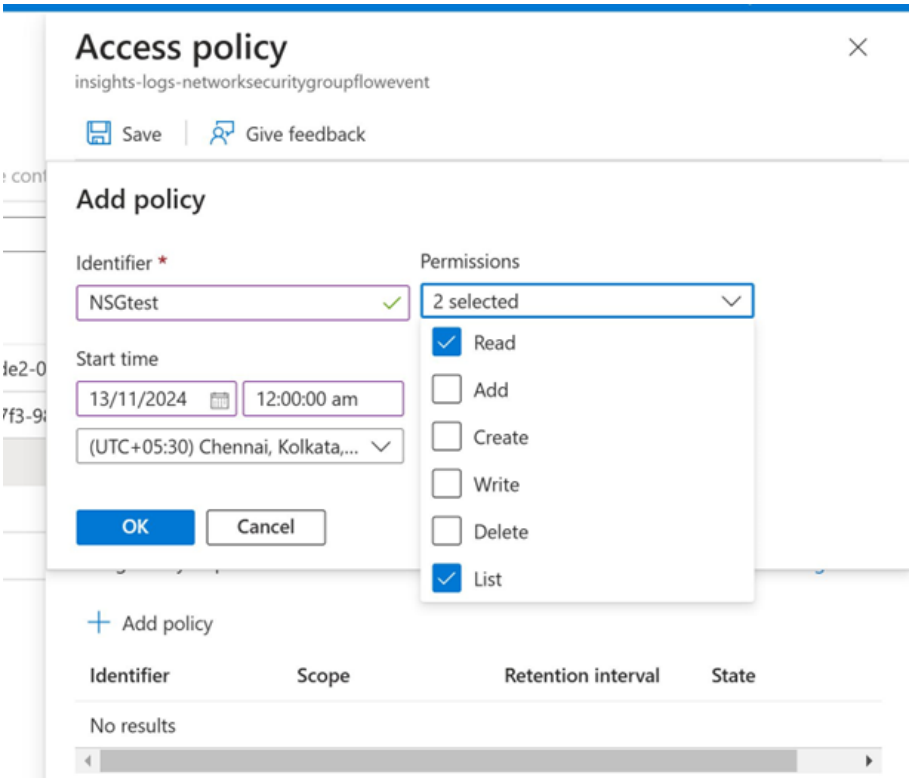
Screenshot 1: Azure Resource Provider Page

5. Go to **Network Watcher > NSG Flow logs**.
   - Select the **Network Security Group** and **Resource group** to enable logs.
   - Specify the **storage account**.
   - Make sure to set the public access level to Private for **insights-logs-networksecuritygroupflowevent** container to block public anonymous access.

- Make sure that the VMs are linked to the same NSG as the storage account which stored the flow logs.
- For more information see network-watcher-nsg-flow-logging-portal for more details.

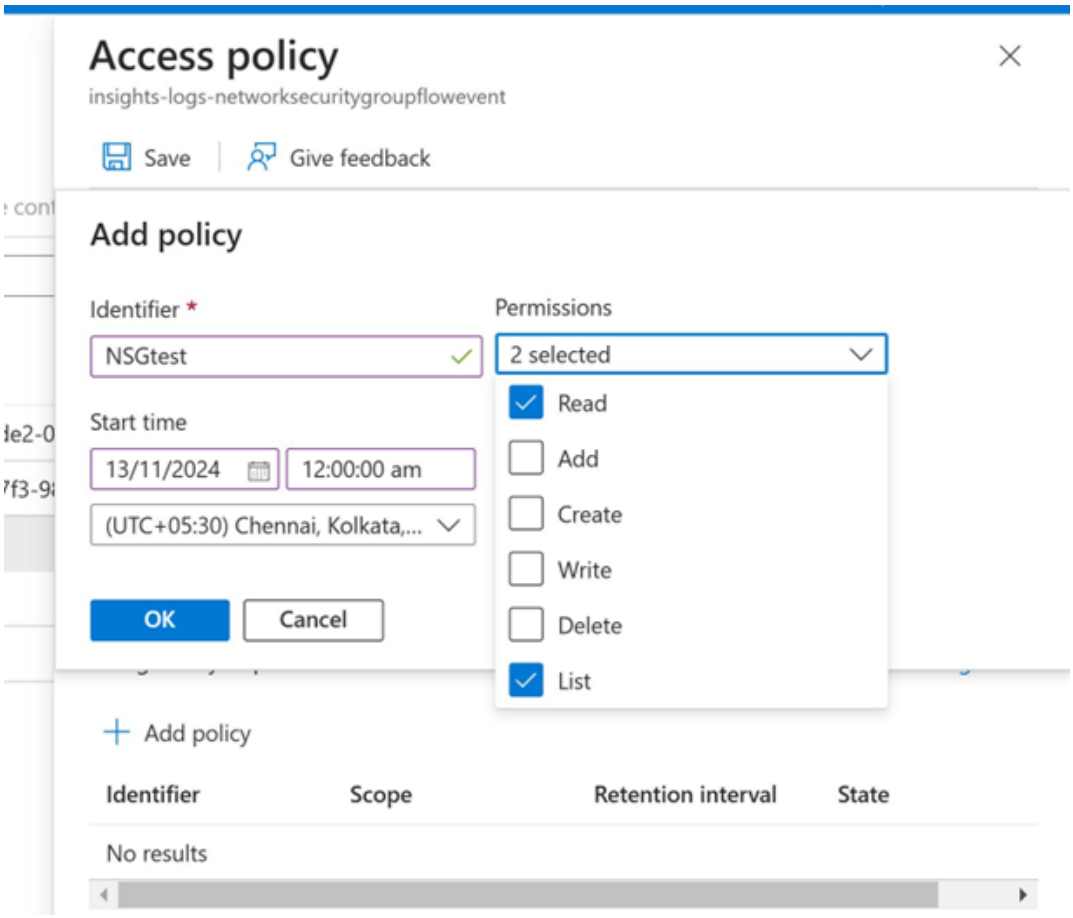
6. **Create SAS Token with Access Policy**.

- **Create an Access Policy**:
  - Go to a Storage Account → Containers → Select Insights-logs-networksecuritygroupflowevent → Click the three dots → Select the Access policy.



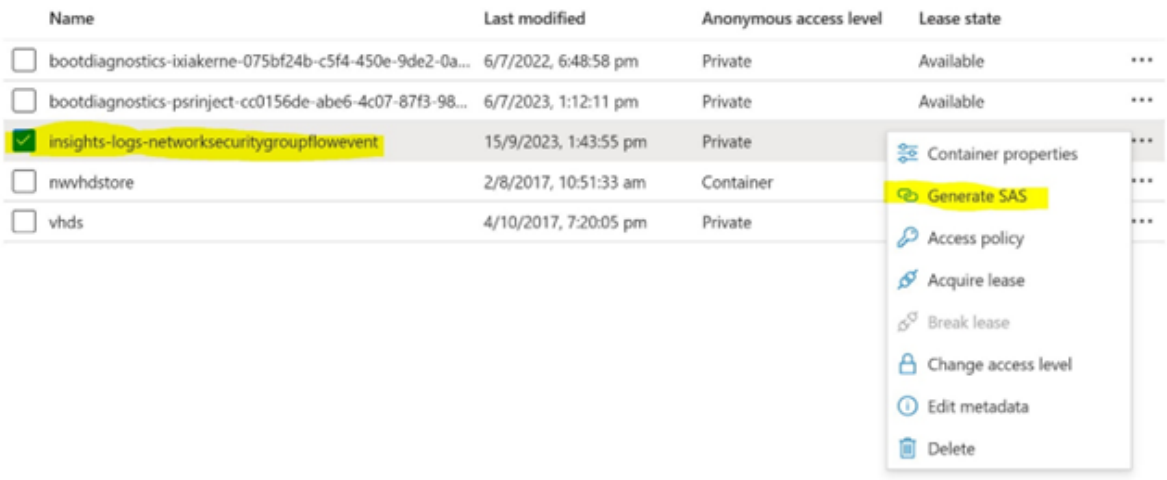
Screenshot 2: Create an access policy.

- Please fill in the following details
  - **Identifier**: Your preferred name for the access policy.
  - **Permission:** Select "Read" and "List"
  - **Start Time and End Time**: Specify your desired time range.



Screenshot 3: Inside an access policy page.

- **Generate a SAS Token**
  - Select the Insights-logs-networksecuritygroupflowevent and click the **three dots (...)**:



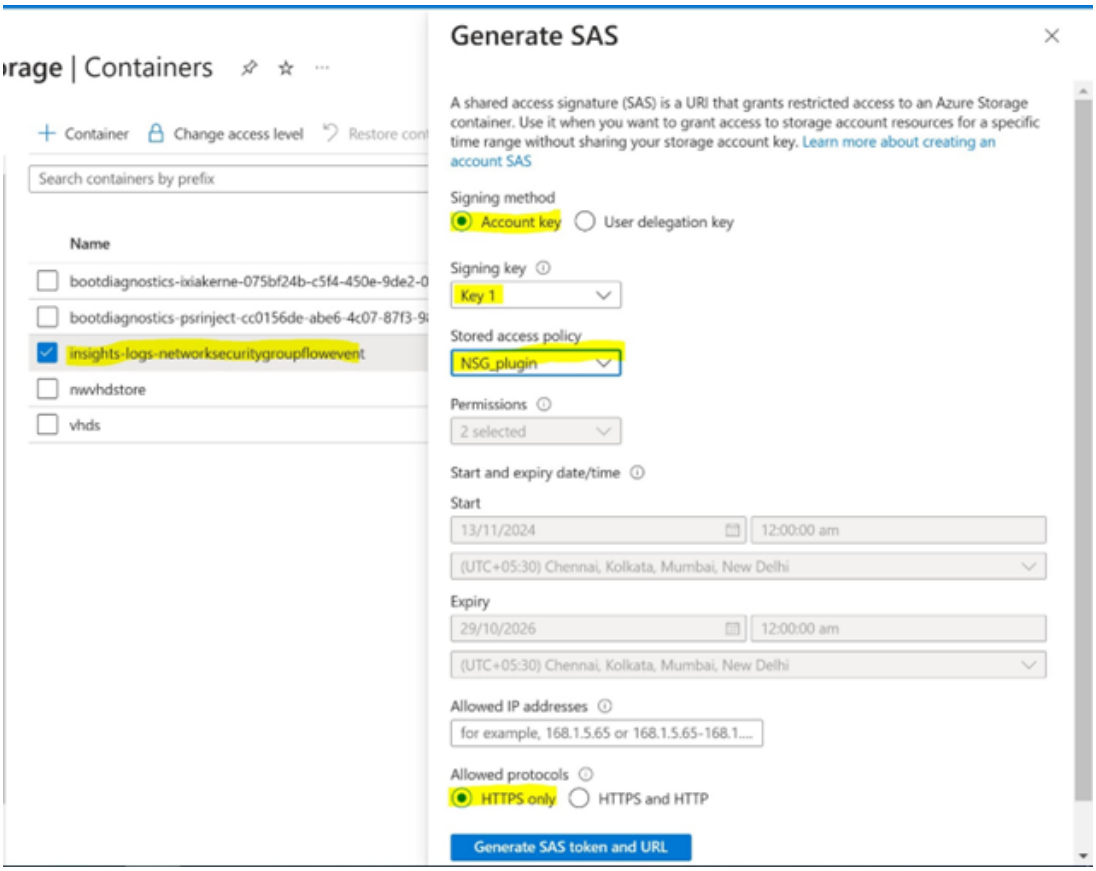
Screenshot 4: Generate a SAS Token.

Please provide the following details:

- **Signing Method**: Account key
- **Signing Key**: Choose a name for your key (e.g., in the example below, I created "Key 1").
- **Stored Access Policy**: Select the access policy created earlier.
- **Allowed Protocols**: HTTPS only.

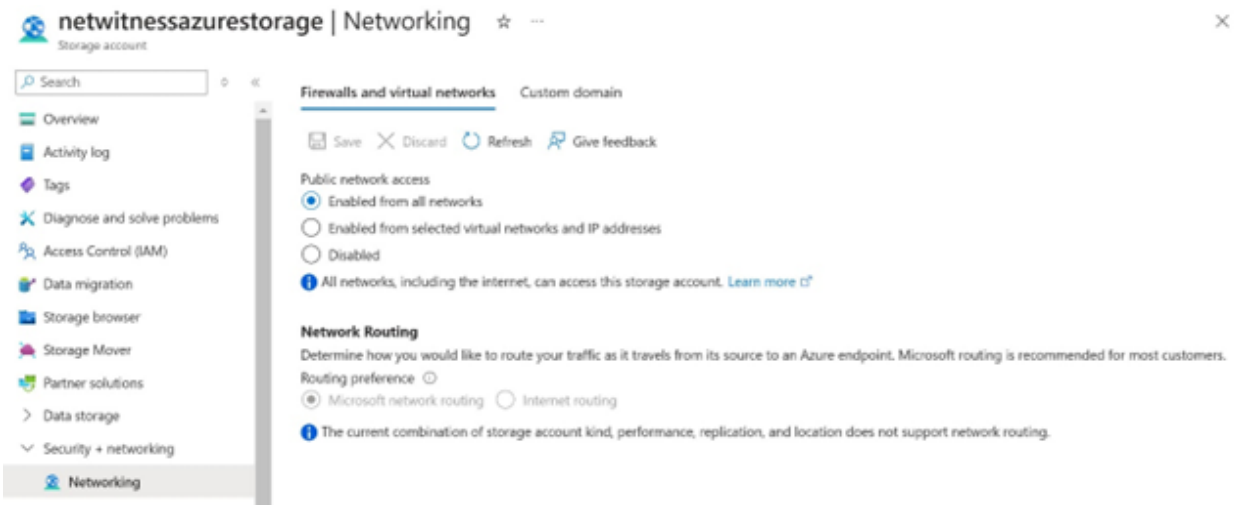
Once you've entered the details, click the Generate SAS Token and URL button.

Finally, copy the generated SAS Token, which is the primary string to be used in the Netwitness configuration.



Screenshot 5: Generate a SAS Token.

Lastly, ensure that your network settings, such as **firewalls and virtual networks**, are configured to allow connections between the storage account and the NetWitness remote/local log collector. Adjust your policy as needed to avoid blocking this connection.



Screenshot 6: Networking

Set Up Microsoft Azure NSG Event Source in NetWitness

In NetWitness Suite, perform the following tasks:

1. Deploy **msazurensg** package and CEF parser from Live
2. Configure the event source

Deploy the Azure NSG Files from Live

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

To deploy the Azure NSG content from Live:

1. In the NetWitness Platform menu, select **Live**.
2. Browse Live 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 the Log Decoders.
4. You also need to deploy the Azure NSG package. Browse Live for Azure NSG content, typing "Azure NSG" into the Keywords text box, then click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

   Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.

6. Restart the **nwlogcollector** service.

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

Configure the Azure NSG Event Source

This section contains details on setting up the event source in NetWitness Suite. In addition to the procedure, the Azure NSG Collection Configuration Parameters are described, as well as how to collect Azure NSG Flow Events in NetWitness Suite

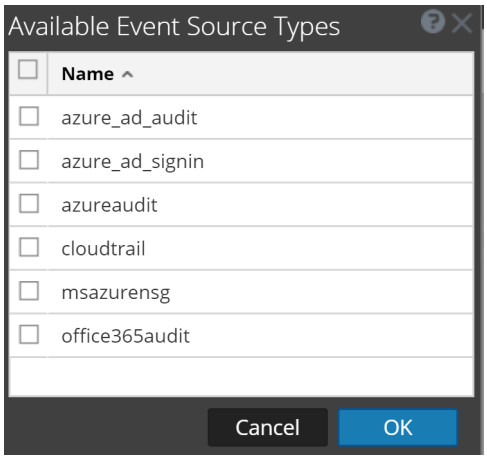
To configure the Microsoft Azure NSG Event Source:

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.

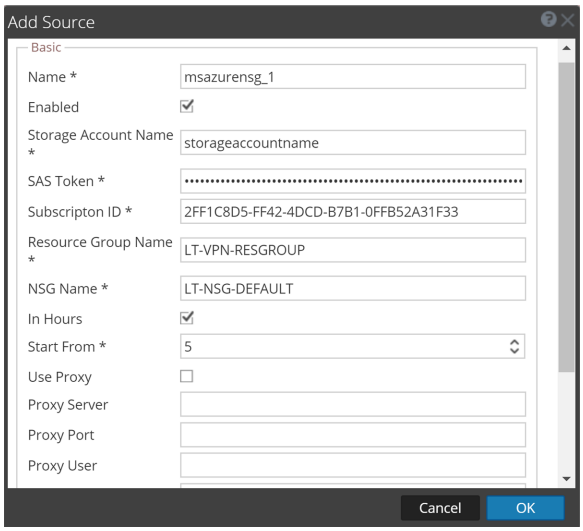


5. Select **msazurensg** from the list, and click **OK**.

   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 NSG 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.

Note: the API calls to the storage account are charged, as described here: https://azure.microsoft.com/en-in/pricing/details/storage/blobs/. Increasing the Polling Interval time will help in reducing the number of API calls made.

Microsoft Azure NSG Collection Configuration Parameters

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

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the **Advanced** section.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source.
Storage Account Name *	Name of the storage account used to store NSG flow logs.
SAS Token *	SAS token created, as described in the NSG Flow Logs in Azure section.
Subscription ID *	Subscription for which the NSG Flow logs were enabled.
Resource Group Name *	Name of the resource group to which the NSG belongs.
NSG Name *	Network Security Group name.
In Hours	Specifies whether **Start From** represents number of hours or days. • Selected (default): if selected, **Start From** represents number of hours. • Cleared: if not checked, indicates **Start From** represents number of days.
Start From *	Specifies the number of hours or days (see the **In Hours** parameter above) prior to the current time, from which log collection should start.
Use Proxy	Select to enable a 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	Input the IP address that needs to appear as the **device.ip**.

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.
Use Classic Path	Check this box if you want to use Azure Classic path in collection.
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	**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 and 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. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
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.