RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Azure NSG (Flow Logs)

Last Modified: Monday, February 26, 2018

Event Source Product Information:

Vendor: Microsoft
Event Source: NSG (Flow Logs)
Versions: all

RSA Product Information:

Supported On: Security Analytics 10.6.2 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

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","resourceI
d":"/SUBSCRIPTIONS/2FF1C8D5-FF42-4DCD-B7B1-
0FFB52A31F33/RESOURCEGROUPS/LT-VPN-
RESGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/LT-NSG-
DEFAULT","operationName":"NetworkSecurityGroupFlowEvents","properti
es":{"Version":1,"flows":[{"rule":"UserRule_PontusAll","flows":
[{"mac":"000D3A103552","flowTuples":
["1514790906,xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,123,123,U,O,A","151479
0926,xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,61377,53,U,O,A","1514790926,xx
x.xxx.xxx.xxx,yyy.yyy.yyy.yyy,51258,443,T,O,A"]}]}]}}
```

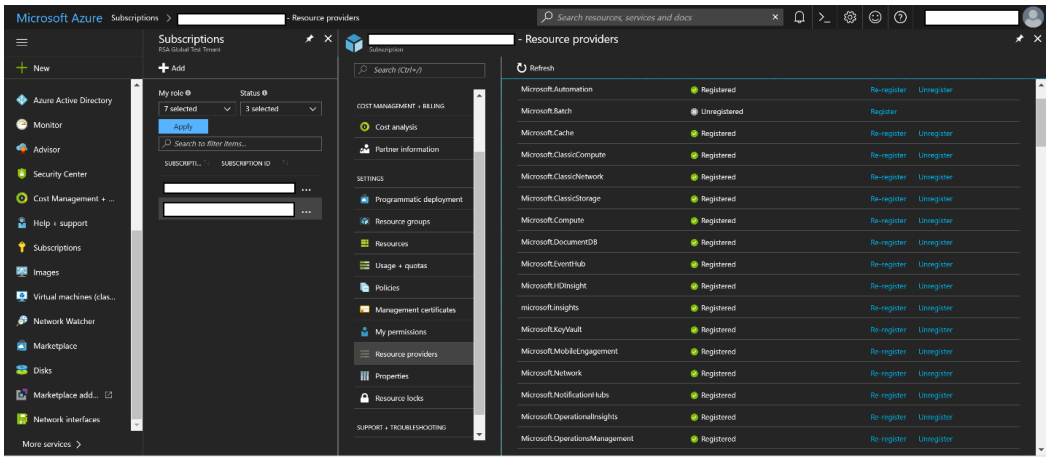
This message is converted into the following multiple sub-logs:

```
Jan 01 2018 08:19:50 cbdb1b39-ac02-4876-ad8e-c06761aebd13
CEF:0|Microsoft|Azure
NSG|1|NetworkSecurityGroupFlowEvents|NetworkSecurityGroupFlowEvent
s|5|category=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|NetworkSecurityGroupFlowEvent
s|5|category=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|NetworkSecurityGroupFlowEvent
s|5|category=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
```

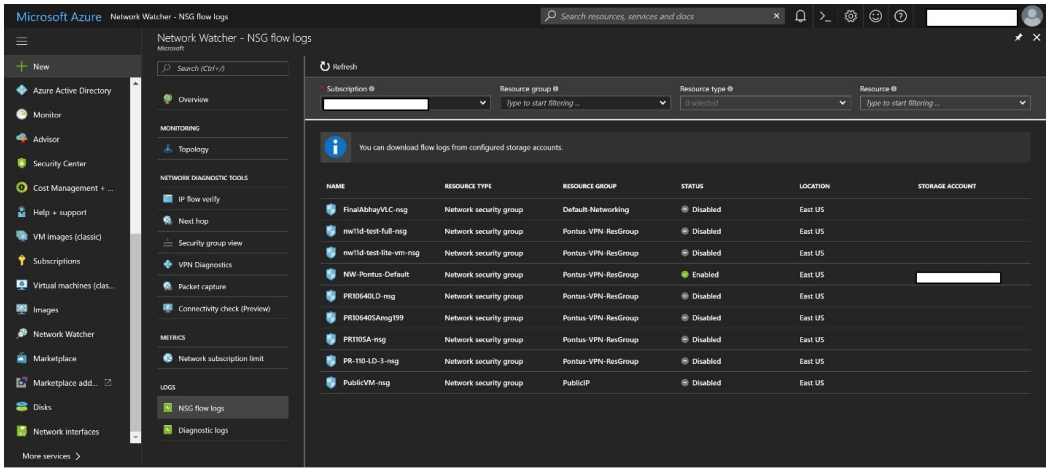
See network-watcher-nsg-flow-logging-overview for more details.

Configure NSG Flow Logs in Azure

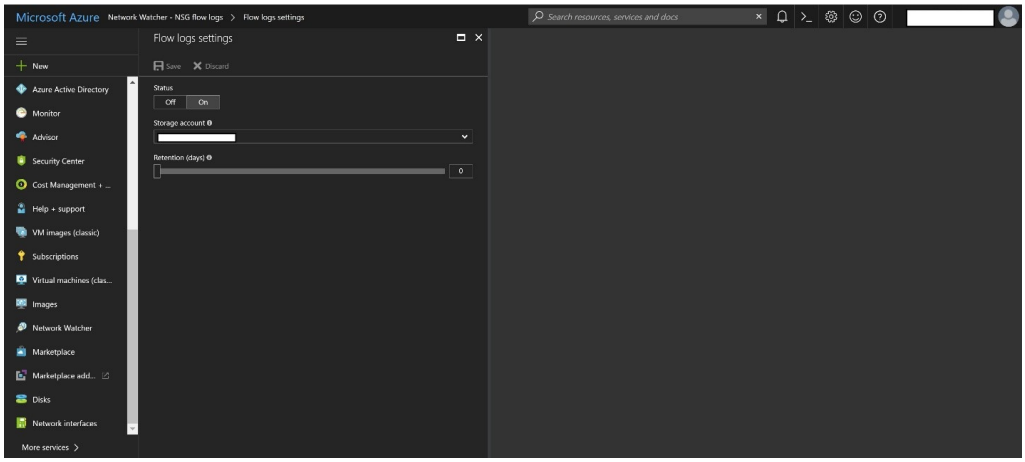
1. Log into the Azure portal at https://portal.azure.com.
2. Go to **Subscriptions**, and then select the subscription for which you want to enable flow logs.
3. On the **Subscription** blade, select **Resource Providers**.
4. 4. Look at the list of providers, and verify that the **microsoft.insights**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



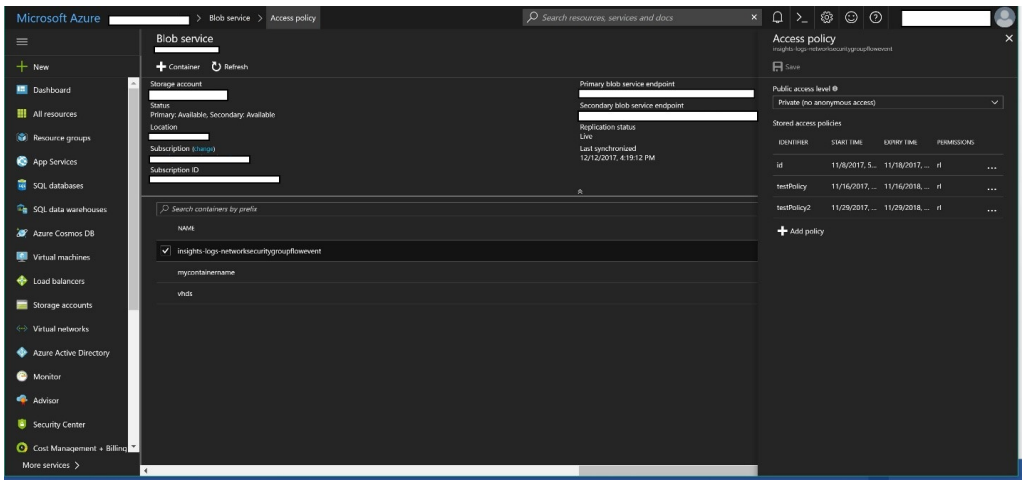
5. Go to **Network Watcher > NSG Flow logs**.



6. Select the Network Security Group and Resource group to enable logs.
7. Specify the storage account and duration for log retention.



8. Make sure to set the public access level to Private for **insights-logs-networksecuritygroupflowevent** container to block public anonymous access.



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

Create SAS Token with Access Policy

Note: This section provides example Powershell steps for creating an SAS token. Any other method can also be used.

These commands create an SAS token with an access policy having the following properties:

- **Validity** = 1 year
- **Protocol** = https only

- **Permissions** = list and read on the **insights-logs-networksecuritygroupflowevent** container

```
PS > Login-AzureRmAccount

PS > $accountKeys = Get-AzureRmStorageAccountKey -ResourceGroupName
"Pontus-VPN-ResGroup" -Name "pontusvpnresgroup167"

PS > $storageContext = New-AzureStorageContext -StorageAccountName
"pontusvpnresgroup167" -StorageAccountKey $accountKeys.value[0]

PS > $policyname = "testpolicy2"

PS > $starttime = $(Get-Date).ToUniversalTime().AddMinutes(-5)

PS > $expirytime = $(Get-Date).ToUniversalTime().AddYears(1)

PS > New-AzureStorageContainerStoredAccessPolicy -Container
"insights-logs-networksecuritygroupflowevent" -Policy $policyname -
Permission rl -StartTime $starttime -ExpiryTime $expirytime -
Context $storageContext

PS > New-AzureStorageContainerSASToken -name 'insights-logs-
networksecuritygroupflowevent' -Protocol HttpsOnly -Policy
$policyname -Context $storageContext

?
sv=2016-05-31&sr=c&si=testPolicy2&sig=CQWVu74sv50jI5SxqCMeDvwt1U3HUEZbOn
1ZuRsaxnU%3D&spr=https
```

The highlighted string represents the SAS token you need to provide when you instantiate the plugin.

See storage-dotnet-shared-access-signature-part-1 for more details.

Set Up Microsoft Azure NSG Event Source in RSA NetWitness

In RSA 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 RSA NetWitness Suite menu, select **Live**.
2. Browse Live for the **Common Event Format** (cef) parser, using **RSA 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

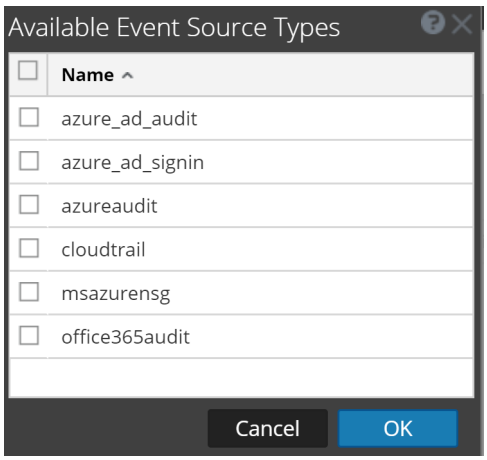
This section contains details on setting up the event source in RSA NetWitness Suite. In addition to the procedure, the Azure NSG Collection Configuration Parameters are described, as well as how to collect Azure NSG Flow Events in NetWitness Suite

To configure the Microsoft Azure NSG Event Source:

1. In the RSA NetWitness Suite 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.

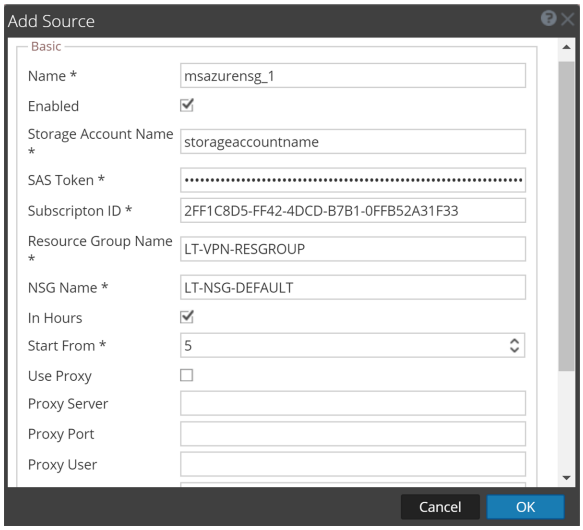


5. Select **msazurensg** from the list, and click **OK**.

   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 RSA NetWitness Suite 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 RSA NetWitness Suite. 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.

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 Create SAS Token with Access Policy 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).
Source Address	Input the IP address that needs to appear as the **device.ip**.

Trademarks

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