Module 15 - Lab 5B) - Log network traffic to and from a VM

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. In this tutorial, you learn how to:

- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data
- View logged data

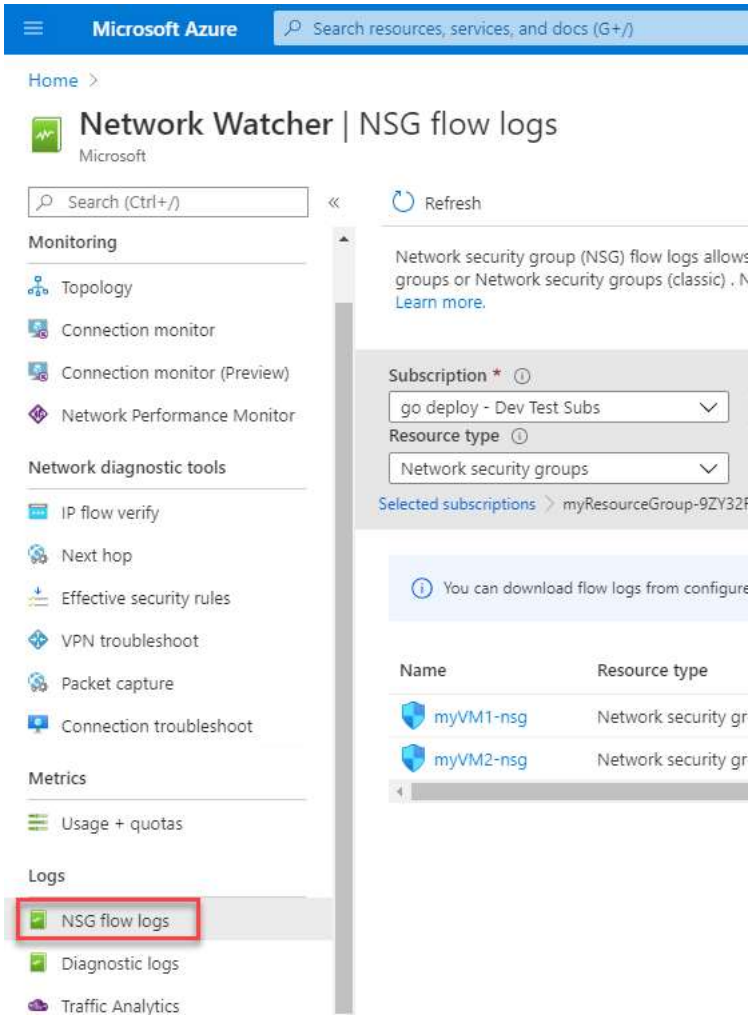
Task 1: Enable NSG flow log

- [ ] 1. NSG flow log data is written to an Azure Storage account. To create an Azure Storage account, select **+ Create a resource** at the top, left corner of the portal.
- [ ] 2. Select **Storage**, then select **Storage account - blob, file, table, queue**.
- [ ] 3. Enter, or select the following information, accept the remaining defaults, and then select **Create**.

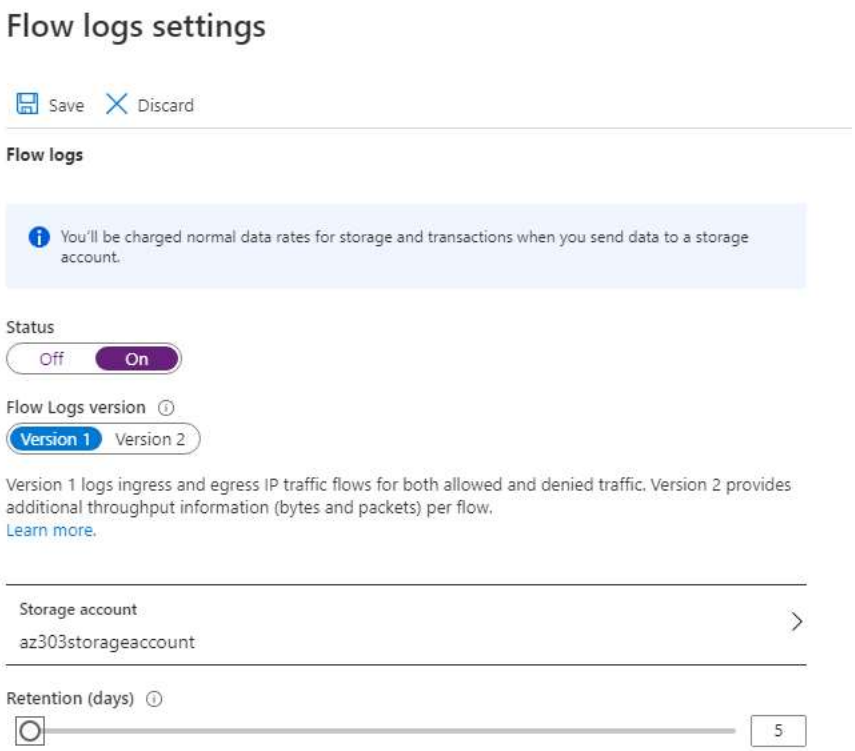
Setting	Value
Name	3-24 characters in length, can only contain lowercase letters and numbers, and must be unique across all Azure Storage accounts.
Location	Select **East US**
Resource group	Select **Use existing**, and then select **myResourceGroup**

The storage account may take around minute to create. Don't continue with remaining steps until the storage account is created. In all cases, the storage account must be in the same region as the NSG.

- [ ] 4. In the Azure Portal search for and select *Network Watcher*. When **Network Watcher** appears in the search results, select it.
- [ ] 5. Under **LOGS**, select **NSG flow logs**, as shown in the following picture:

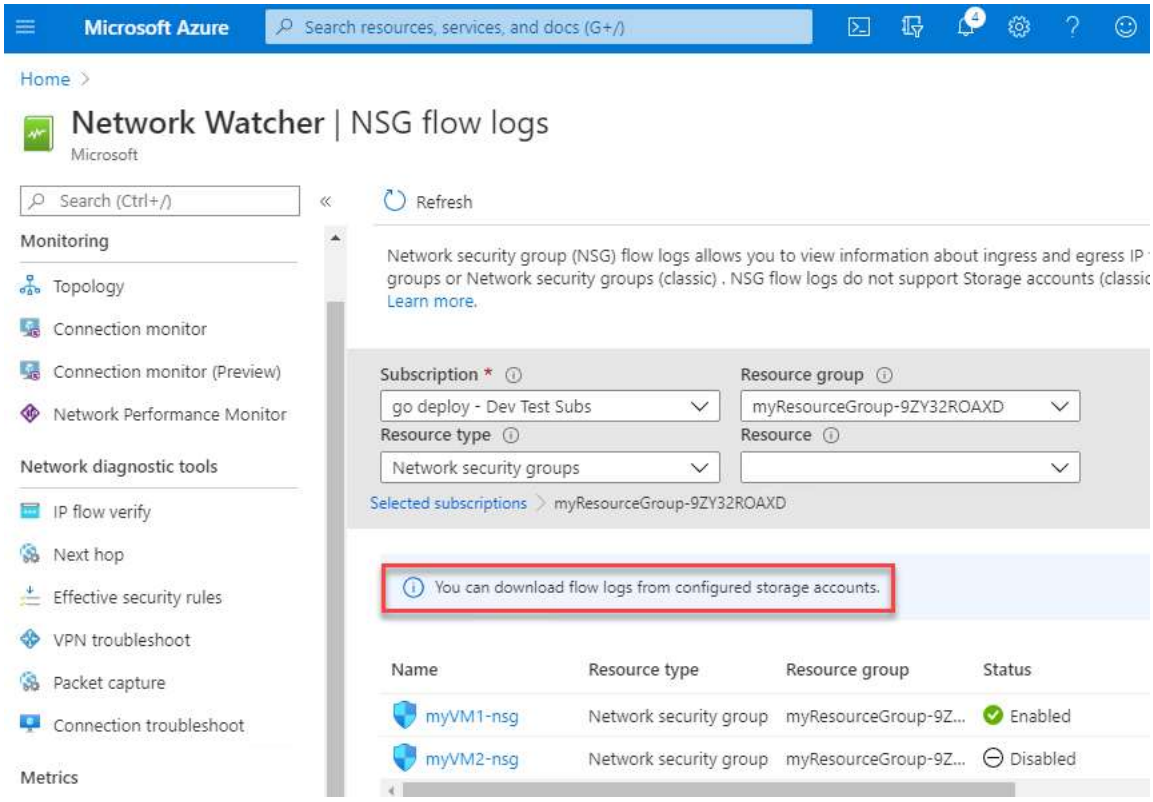


- [ ] 6. From the list of NSGs, select the NSG named **myVm1-nsg**.
- [ ] 7. Under **Flow logs settings**, select **On**.
- [ ] 8. Select the flow logging version. Version 2 contains flow-session statistics (Bytes and Packets)
- [ ] 9. Select the storage account that you created in the previous task.
- [ ] 10. Set **Retention (days)** to 5, and then select **Save**.



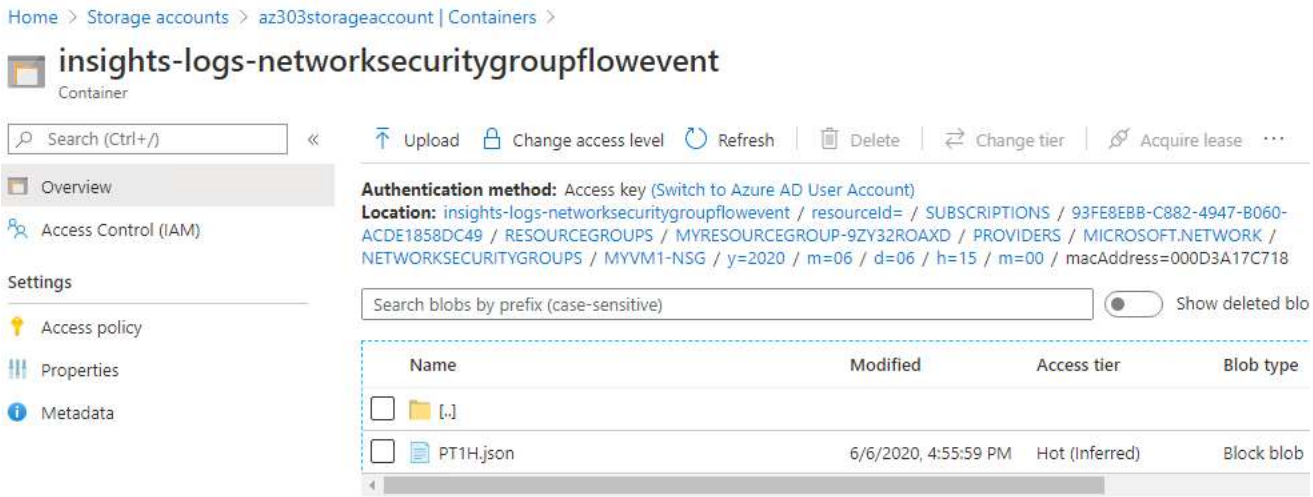
Task 2: Download flow log

- [ ] 1. From Network Watcher, in the portal, select **NSG flow logs** under **LOGS**.
- [ ] 2. Select **You can download flow logs from configured storage accounts**, as shown in the following picture:

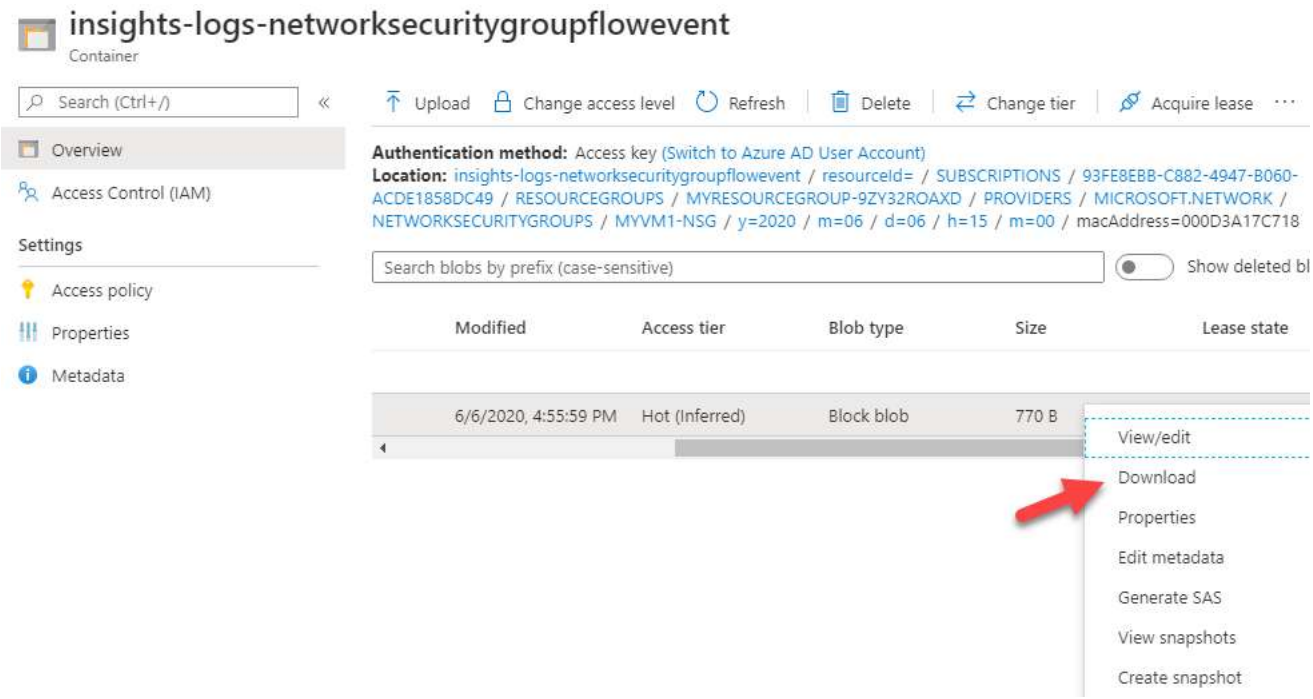


- [ ] 3. Select the storage account that you configured earlier.
- [ ] 4. Select **Containers**, and then select the **insights-logs-networksecuritygroupflowevent** container.
- [ ] 5. In the container, navigate the folder hierarchy until you get to a PT1H.json file, as shown in the picture that follows. Log files are written to a folder hierarchy that follows the following naming convention:

https://{storageAccountName}.blob.core.windows.net/insights-logs-networksecuritygroupflowevent/resourceId=/SUBSCRIPTIONS/{subscriptionID}/RESOURCEGROUPS/{resourceGroupName}/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/{nsgName}/y={year}/m={month}/d={day}/h={hour}/m=00/macAddress={macAddress}/PT1H.json



- [ ] 6. Select **...** to the right of the PT1H.json file and select **Download**.



Task 3: View flow log

The following json is an example of what you'll see in the PT1H.json file for each flow that data is logged for:

- [ ] 1. Version 1 flow log event

```
{
"time": "2018-05-01T15:00:02.1713710Z",
"systemId": "<Id>",
"category": "NetworkSecurityGroupFlowEvent",
"resourceId": "/SUBSCRIPTIONS/<Id>/RESOURCEGROUPS/MYRESOURCEGROUP/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/MYVM-NSG",
"operationName": "NetworkSecurityGroupFlowEvents",
"properties": {
    "Version": 1,
    "flows": [
        {
            "rule": "UserRule_default-allow-rdp",
            "flows": [
                {
                    "mac": "000D3A170C69",
                    "flowTuples": [
                        "1525186745,192.168.1.4,10.0.0.4,55960,3389,T,I,A"
                    ]
                }
            ]
        }
    ]
}
}
```

- [ ] 2. Version 2 flow log event


```
{
    "time": "2018-11-13T12:00:35.3899262Z",
    "systemId": "a0fca5ce-022c-47b1-9735-89943b42f2fa",
    "category": "NetworkSecurityGroupFlowEvent",
    "resourceId": "/SUBSCRIPTIONS/00000000-0000-0000-0000-000000000000/RESOURCEGROUPS/FABRIKAMRG/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITY
    "operationName": "NetworkSecurityGroupFlowEvents",
    "properties": {
        "Version": 2,
        "flows": [
            {
                "rule": "DefaultRule_DenyAllInBound",
                "flows": [
                    {
                        "mac": "000D3AF87856",
                        "flowTuples": [
                            "1542110402,94.102.49.190,10.5.16.4,28746,443,U,I,D,B,,,,",
                            "1542110424,176.119.4.10,10.5.16.4,56509,59336,T,I,D,B,,,,",
                            "1542110432,167.99.86.8,10.5.16.4,48495,8088,T,I,D,B,,,,"
                        ]
                    }
                ]
            },
            {
                "rule": "DefaultRule_AllowInternetOutBound",
                "flows": [
                    {
                        "mac": "000D3AF87856",
                        "flowTuples": [
                            "1542110377,10.5.16.4,13.67.143.118,59831,443,T,O,A,B,,,,",
                            "1542110379,10.5.16.4,13.67.143.117,59932,443,T,O,A,E,1,66,1,66",
                            "1542110379,10.5.16.4,13.67.143.115,44931,443,T,O,A,C,30,16978,24,14008",
                            "1542110406,10.5.16.4,40.71.12.225,59929,443,T,O,A,E,15,8489,12,7054"
                        ]
                    }
                ]
            }
        ]
    }
}
```


The value for **mac** in the previous output is the MAC address of the network interface that was created when the VM was created. The comma-separated information for **flowTuples**, is as follows:

Example data	What data represents	Explanation
1542110377	Time stamp	The time stamp of when the flow occurred, in UNIX EPOCH format. In the previous example, the date converts to May 1, 2018 at 2:59:05 PM GMT.
10.0.0.4	Source IP address	The source IP address that the flow originated from. 10.0.0.4 is the private IP address of the VM you created in Create a VM.
13.67.143.118	Destination IP address	The destination IP address that the flow was destined to.
44931	Source port	The source port that the flow originated from.
443	Destination port	The destination port that the flow was destined to. Since the traffic was destined to port 443, the rule named **UserRule_default-allow-rdp**, in the log file processed the flow.
T	Protocol	Whether the protocol of the flow was TCP (T) or UDP (U).
O	Direction	Whether the traffic was inbound (I) or outbound (O).
A	Action	Whether the traffic was allowed (A) or denied (D).
C	Flow State **Version 2 Only**	Captures the state of the flow. Possible states are **B**: Begin, when a flow is created. Statistics aren't provided. **C**: Continuing for an ongoing flow. Statistics are provided at 5-minute intervals. **E**: End, when a flow is terminated. Statistics are provided.
30	Packets sent - Source to destination **Version 2 Only**	The total number of TCP or UDP packets sent from source to destination since last update.
16978	Bytes sent - Source to destination **Version 2 Only**	The total number of TCP or UDP packet bytes sent from source to destination since last update. Packet bytes include the packet header and payload.
24	Packets sent - Destination to source **Version 2 Only**	The total number of TCP or UDP packets sent from destination to source since last update.

Example data	What data represents	Explanation
14008	Bytes sent - Destination to source **Version 2 Only**	The total number of TCP and UDP packet bytes sent from destination to source since last update. Packet bytes include packet header and payload.

✓ **Results**: In this lab, you learned how to enable NSG flow logging for an NSG. You also learned how to download and view data logged in a file. The raw data in the json file can be difficult to interpret. To visualize Flow Logs data, you can use **Azure Traffic Analytics**, **Microsoft Power BI**, and other tools.