Configure a Storage Account in Microsoft Cloud Services

To gather data from Azure Storage Table, Azure Storage Blob, and Azure Virtual Machine Metrics, you need to create or configure a storage account in Microsoft Azure.

Create and Manage Storage Account

See Create Azure storage accounts for the instructions to create and manage the storage account.

Configure the Storage Account to get data

- The Splunk Add-on for Microsoft Cloud Services provides two methods for you to get Azure storage table and Azure virtual machine metrics data. You can use either an **Access Key** or **Account Token (SAS: Shared access signature)** with the following steps.
- If you want to get Azure storage blob data, you can also use **None Secret** to get the data without inputting key or token.

Get storage account access key

1. Log in to your Azure portal or Azure Government portal.
2. Select the storage account you want to use.
3. Copy either **Key1** or **Key2** of **Access Key** under **Settings**.

Get your storage account token (SAS)

1. Log in to your Azure portal or Azure Government portal.
2. Select the storage account you want to use.
3. In the **Shared access signature** menu, configure your shared access signature based on the data you want to collect, such as **allowed services**, **allowed resource types** and **start and expiry date/time** under **Settings**. In the **Allowed resource type** section, verify that the **Service** box is checked.
4. Generate your SAS and copy it to your clipboard.

Get storage blob data without key or token

1. Login to your Azure portal or Azure Government portal.
2. Click **All resources** in the menu, then select the storage account that that you want to use.
3. Click **Overview** and then select **Blobs** under **Services**.
4. Select the container you want to configure and then click **Access policy**.
5. Select **Container** for the **Access type**.

Configuring NSG Flow Logs in the Azure Portal

From the Azure Portal, navigate to a Network Watcher instance and select Flow Logs
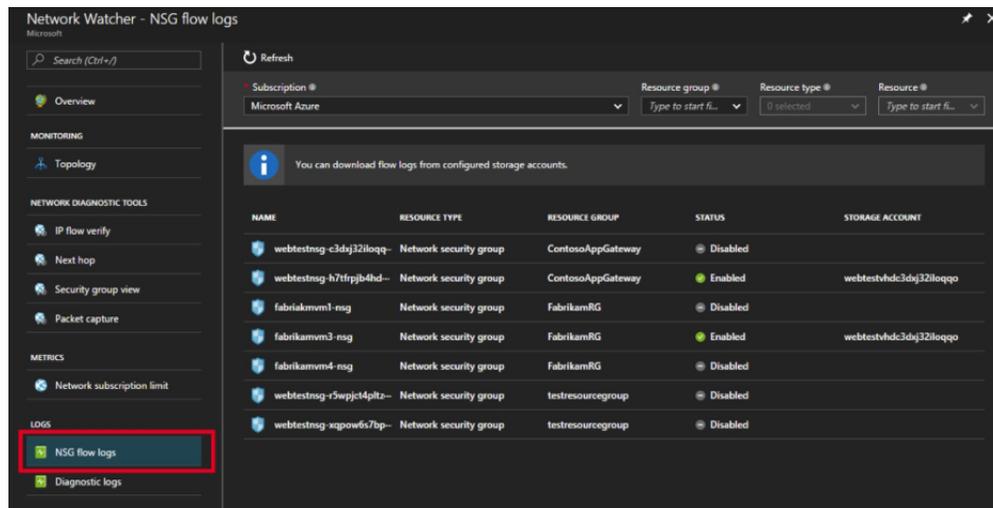
Select a Network Security Group from the list by clicking it.
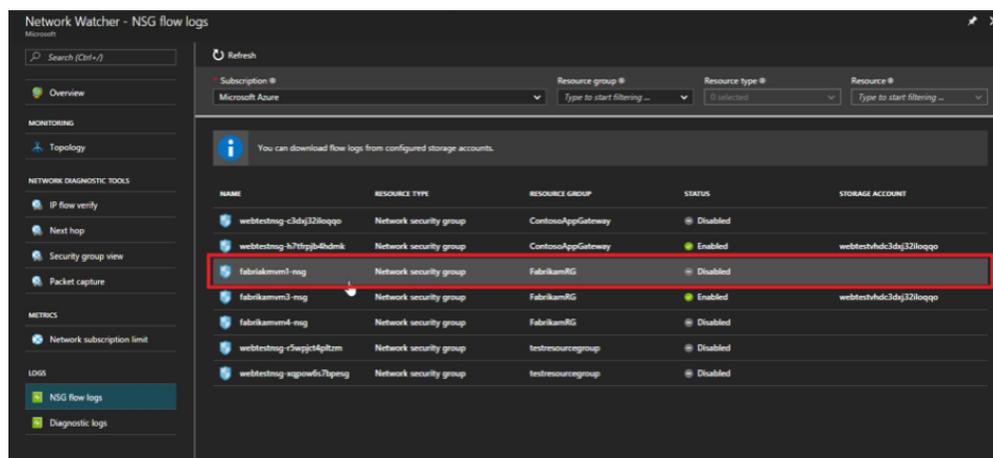
Navigate to the correct storage account and then Containers -> insights-logs-networksecuritygroupflowevent
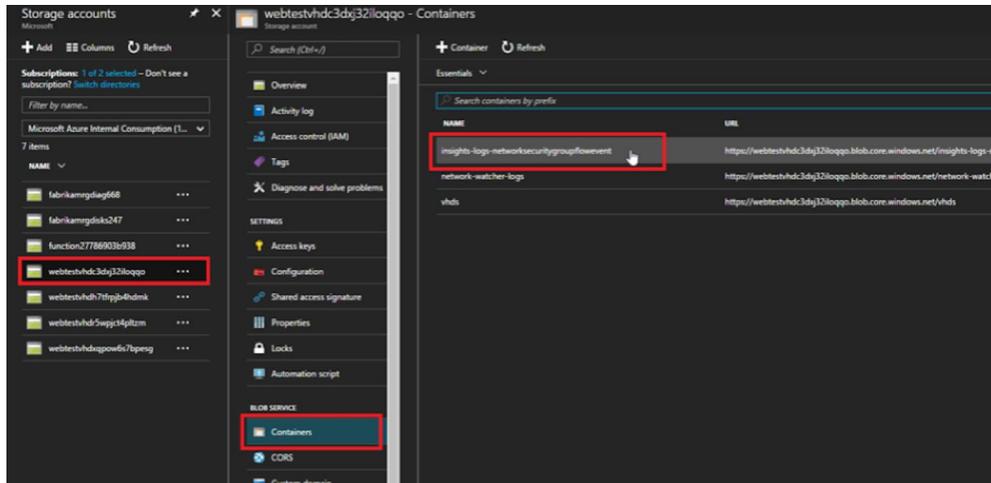
https://www.splunk.com/en_us/blog/tips-and-tricks/splunking-microsoft-azure-network-watcher-data.html