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

Network Watcher - NSG flow log Microsoft	gs					* ×
Search (Ctrl+/)	🖏 Refresh					
Ø Overview	Subscription ® Microsoft Azure			Resource group Type to start fi	Resource type 0 selected	Resource @ Type to start fi ~
MONITORING						
👗 Topology	You can download flow	w logs from configured storage ac	counts.			
NETWORK DIAGNOSTIC TOOLS						
🕵 IP flow verify	NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS	STORA	GE ACCOUNT
🕺 Next hop	💗 webtestnsg-c3dxj32iloqq-	Network security group	ContosoAppGatewa	y 😑 Disabled		
Security group view	🔋 webtestnsg-h7tfrpjb4hd…	Network security group	ContosoAppGatewa	y 🥺 Enabled	webte	stvhdc3dxj32iloqqo
Packet capture	🏮 fabriakmvm1-nsg	Network security group	FabrikamRG	Disabled		
	🏮 fabrikamvm3-nsg	Network security group	FabrikamRG	Enabled	webte	stvhdc3dxj32iloqqo
METRICS	🏮 fabrikamvm4-nsg	Network security group	FabrikamRG	Disabled		
Network subscription limit	🔋 webtestnsg-r5wpjct4pltz	Network security group	testresourcegroup	Disabled		
1065	🌍 webtestnsg-xqpow6s7bp	Network security group	testresourcegroup	Disabled		
NSG flow logs						
Diagnostic logs						

Select a Network Security Group from the list by clicking it.

Network Watcher - NSG flow log	gs					* ×
C Search (Ctrl+/)	🕑 Refresh					
💙 Overview	Subscription Microsoft Azure		Resource group #	Resource type C selected	Resource Type to start filtering	
MONITORING	You can download flow logs	from configured storage accounts.				
NETWORK DIAGNOSTIC TOOLS	NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS	STORAGE ACCOUNT	
 IP flow verify Next hop 	🧊 webtestnisg-c3dxj32iloqqo	Network security group	ContosoAppGateway	Disabled		
Security group view	webtestnsg-h7tfrpjb4hdmk	Network security group	ContosoAppGateway	Crabled	webtestvhdc3dxj32iloqqo	
S Packet capture	fabrikamvm3-nsg	Network security group	FabrikamRG	e Disabled	webtestvhdc3dxjj32iloqqo	
METRICS	🏮 fabrikamvm4-nsg	Network security group	FabrikamRG	Disabled		
Network subscription limit	😻 webtestnsg-r5wpjct4pltzm	Network security group	testresourcegroup	Disabled		
NSC Brackage	🜍 webtestnsg-xapow6s7bpesg	Network security group	testresourcegroup	Disabled		
Diagnostic logs						

Navigate to the correct storage account and then Containers -> insights-logsnetworksecuritygroupflowevent

Storage accounts 💉 🗶	webtestvhdc3dxj32iloqqo -	- Containers				
+ Add III Columns ひRefresh	P Search (Ctrl+/)	+ Container 👌 Refresh				
Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories	- Ormina	Essentials 🗠				
Charles and		P Search containers by prefix				
Titler by name	Activity log					
Microsoft Azure Internal Consumption (1 🛩	Access control (JAM)	NAME	VAL			
7 items	/ Taos	insights-logs-networksecuritygroupflowevent	https://webtestvhdc3daj32iloqqo.blob.core.windows.net/insights-logs-r			
	X Diagnose and solve problems	network-watcher-logs	https://webtestvhdc3dsj32iloqqo.blob.core.windows.net/network-watch			
labrikamrgdiag668 •••		vhds	https://webtestvhdc3dsj32iloqqa.blob.core.windows.net/vhds			
fabrikamrgdisks247 •••	SETTINGS					
function27786903b938	📍 Access keys					
webtestvhdc3dxj32iloqqo ···	E Configuration					
webtestvhdh?tfrpjb4hdmk •••	Shared access signature					
webtestvhdr5wpjct4pltzm ***	Properties					
webtestvhdxqpow6s7bpesg •••	Locks					
	Automation script					
	BLOB SERVICE					
	Containers					
	COIS					
	Custom domain					

https://www.splunk.com/en_us/blog/tips-and-tricks/splunking-microsoft-azure-networkwatcher-data.html