

Lab #7: Setup of VM & NSG Logging

Purpose:

- We'll configure logging for our VMs and NSGs, which will ultimately be sent to our Log Analytics workspace. We'll then query our Log Analytics workspace to ensure the logs are being forwarded to it.

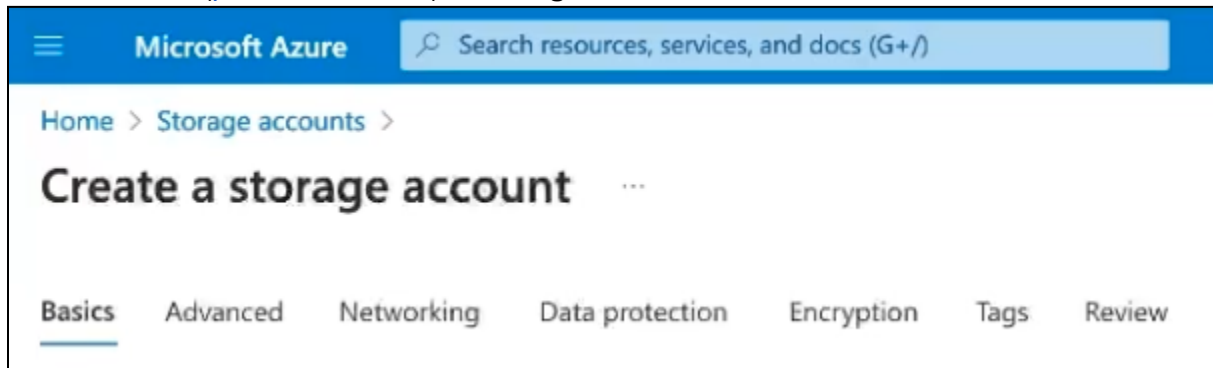
Tasks:

1. Create an Azure Storage Account
2. Enable Flow logs for both Network Security Groups
3. Configure Data Collection Rules within Log Analytics Workspace
4. Manually install the Log Analytics agent on "tester" VMs
5. Query Log Analytics for logs from the VMs and NSGs
6. Generate the failed logon attempts (Windows)

Task 1: Create an Azure Storage Account

Note: Azure requires this storage account to be created for our network security groups.

1. **Azure** account (portal.azure.com) > **Storage Accounts** > **Create**.

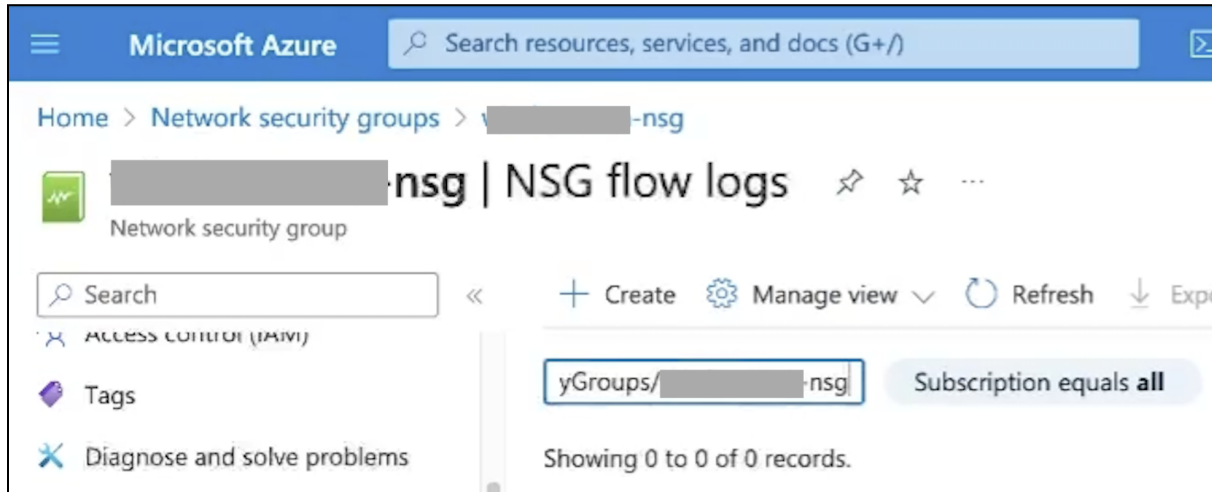


- a. **Subscription:** (select our Azure subscription)
- b. **Resource group:** ("Tester" resource group)
- c. **Instance Details > Storage account name:** (create a name), **Region:** (same as "Tester" VMs).
- d. Select **Review > Target workspace:** (select our workspace).
- e. Select **Review > select Create**.



Task 2: Enable Flow logs for both Network Security Groups

1. **Azure** account > go to **Network Security Groups (NSG)**
2. Select the Windows “Tester” NSG > **NSG flow logs** > **Create flow log**.



- a. **Select resource** > (select checkboxes for both windows-vm & linux-vm) > **confirm**.
- b. **Storage Accounts**: (select the newly-created storage account)
- c. **Retention**: 0
- d. Select **Analytics** > **Flow Logs Version**: Version 2, (select the **Enable Traffic Analytics** checkbox) > **Interval**: every 10min.
- e. Select **Review + Create** > **Create**.

Task 3: Configure Data Collection Rules w/in Log Analytics Workspace

Note: The data collection rule will help determine which logs will be forwarded to the Log Analytics workspace (you don't want to forward everything → \$\$\$).

1. **Azure** account > power on both “tester” VMs.
2. Go to **Log Analytics workspace** > select our workspace > **Agents** > **Data Collection Rules**.
 - a. Select **Create data collection rule**.
 - b. **Rule Name**: (create a name)
 - c. **Platform Type**: All
 - d. Select **Next (Resources)** > **Add resources** > (expand the “Tester” RG) select both “tester” VMs > **Apply**.
 - e. Select **Next (Collect)** > **Add data source** > **Linux Syslog** >
 - i. **LOG_AUTH** should be set to LOG_DEBUG. (All other logs should be set to **none**)

* Data source	Destination
Select which data source type and the data to collect for your resource(s).	
Data source type *	
Linux Syslog	
Facility	Minimum log level
LOG_ALERT	none
LOG_AUDIT	none
LOG_AUTH	LOG_DEBUG
LOG_AUTHPRIV	none
LOG_CLOCK	none
LOG_CRON	none

- ii. Select **Next > Add data source**.
- f. Select **Add data source** (again) > **Windows Event Logs** >
 - i. **Application**: Information; **Security**: Audit success, audit failure.
 - ii. Select **Next > Add data source**.
- g. Select **Review + Create > Create**.
- 3. Back at **Log Analytics workspace** > (select our workspace) > **Agents > Data Collection Rules** > (select the one data collection rule) > **Data Sources**.
 - a. Select **Windows Event Logs > Custom**.
 - i. Add the 2 log commands from this GitHub link: <https://github.com/erichmair/Azure-SOC-Honeynet-Project/blob/main/Special-Windows-Event-Data-Collection-Rules/Rules.txt> (paste one command > **Add**. Repeat).

None Basic Custom

Use XPath queries to filter event logs and limit data collection. [Learn more about event logs and XPath syntax](#)

Event logs

Application!*[System[(Level=4 or Level=0)]]	🗑️
Security!*[System[(band(Keywords,13510798882111488))]]	🗑️
Microsoft-Windows-Windows Defender/Operational!*[System[(EventID=1116 or EventID=1117)]]	🗑️
Microsoft-Windows-Windows Firewall With Advanced Security/Firewall!*[System[(EventID=2003)]]	🗑️

- ii. Select **Save**.

Task 4: Manually install the Log Analytics agent on “tester” VMs

Note: These agents will assist with picking and forwarding the logs to our Log Analytics workspace.

1. Open **windows-vm** > open **Notepad** app > (Done. We’ll come back to this VM soon)
2. **Azure** portal > **Log Analytics workspace** > select our workspace > **Agents**.
 - a. Select **Log Analytics agent instructions** (for the Windows servers tab) > paste the **Workspace ID** and **Primary Key** into the windows-vm Notepad app.
 - b. Copy the **Download Windows Agent (64 bit)** hyperlink into the windows-vm’s Edge browser > download the agent file:
 - i. Select **Agree/Next** for the initial few options > For **Agent Setup Options**, only select the Log Analytics checkbox.

Connect the agent to Azure Log Analytics (OMS)
Connects the agent to the Microsoft Azure Log Analytics (OMS) service and lets you to choose the workspace that the agent uses to register with. For more information, see <https://www.microsoft.com/oms>.

Connect the agent to System Center Operations Manager
This connects the agent to System Center Operations Manager and lets you specify the management group for which this agent will participate in monitoring.

< Back Next > Cancel

- ii. **Workspace ID:** (paste from Notepad)
- iii. **(Primary) Workspace Key:** (paste from Notepad)
- iv. Finish the last install steps.

Note: We now see **Microsoft Monitoring Agent** in the Control Panel. Logs should now be getting forwarded into our Log Analytics workspace.

- c. Close the windows-vm window.
- 3. Back at **Azure** portal > **Log Analytics workspace** > select our workspace > **Agents**.

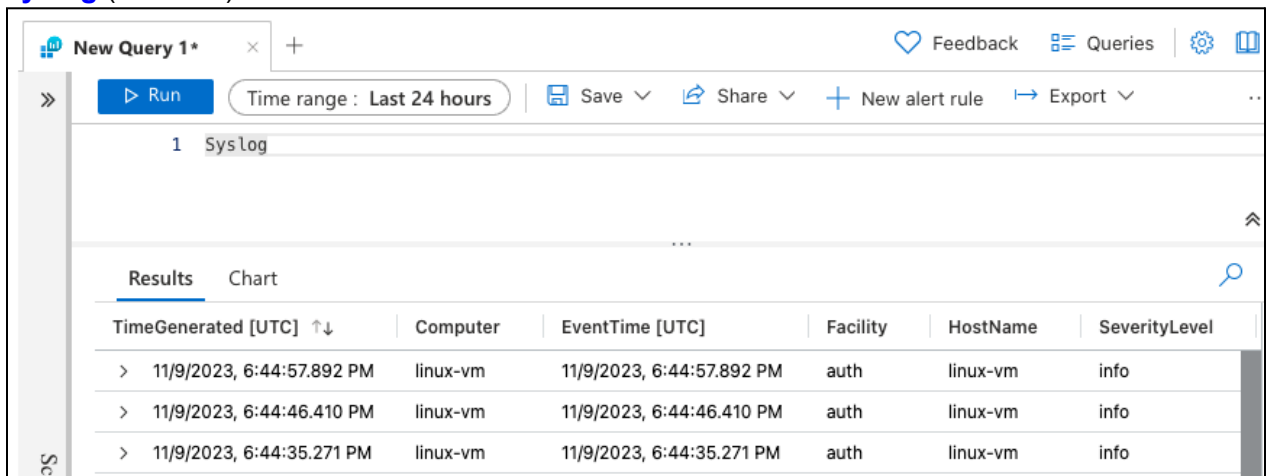
Note: We'll now be SSH-ing into the Linux "Tester" VM to perform our agent-install steps.

- a. Select **Log Analytics agent instructions** (for the Linux servers tab).
- b. Open our personal **terminal/PowerShell** application > **SSH** into the Linux VM (**ssh <username>@<VM public IP>**) > the prompt updated to the linux-vm.
- c. Paste the **Download and onboard agent for Linux** command into the SSH session ("**wget ...**").
- d. Exit the SSH session: **exit**

Note: We should now be able to start querying logs in our Log Analytics workspace!

Task 5: Query Log Analytics for logs from the VMs and NSGs

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs**.
2. In the query box, run these 3 commands [separately] to test each log source:
 - a. **Syslog** (linux-vm)



The screenshot shows the Azure Log Analytics query interface. The query box contains '1 SysLog'. The time range is set to 'Last 24 hours'. The results are displayed in a table with the following columns: TimeGenerated [UTC], Computer, EventTime [UTC], Facility, HostName, and SeverityLevel. The results show three entries for 'linux-vm' with 'auth' facility and 'info' severity level.

TimeGenerated [UTC]	Computer	EventTime [UTC]	Facility	HostName	SeverityLevel
> 11/9/2023, 6:44:57.892 PM	linux-vm	11/9/2023, 6:44:57.892 PM	auth	linux-vm	info
> 11/9/2023, 6:44:46.410 PM	linux-vm	11/9/2023, 6:44:46.410 PM	auth	linux-vm	info
> 11/9/2023, 6:44:35.271 PM	linux-vm	11/9/2023, 6:44:35.271 PM	auth	linux-vm	info

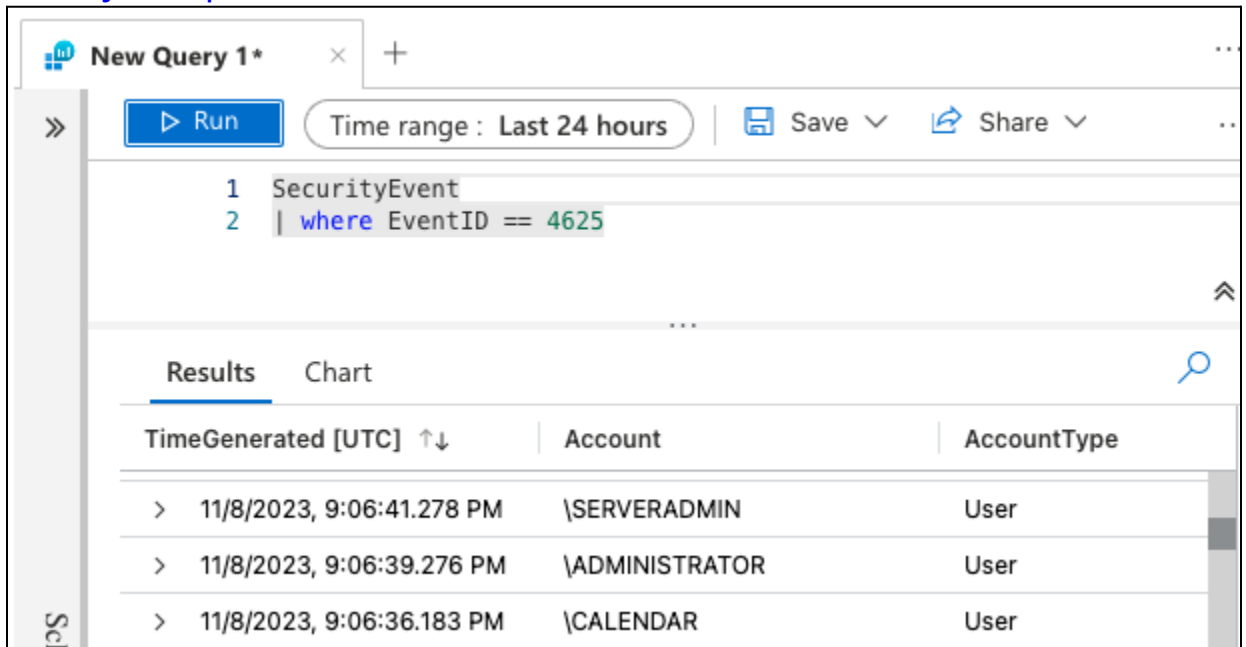
- b. **SecurityEvent** (windows-vm)
 - c. **AzureNetworkAnalytics_CL** (Network Security Groups/NSGs)
3. After running each command, we should see results. This has confirmed that logs are successfully being sent to the workspace.

Task 6: Generate the failedlogon attempts (Windows)

Note: After confirming that logs are coming in, generate the failed login attempts (Windows).

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs**.
2. In the query box, run these commands [separately] to view failed logon attempts:

- a. **SecurityEvent | where EventID == 4625**



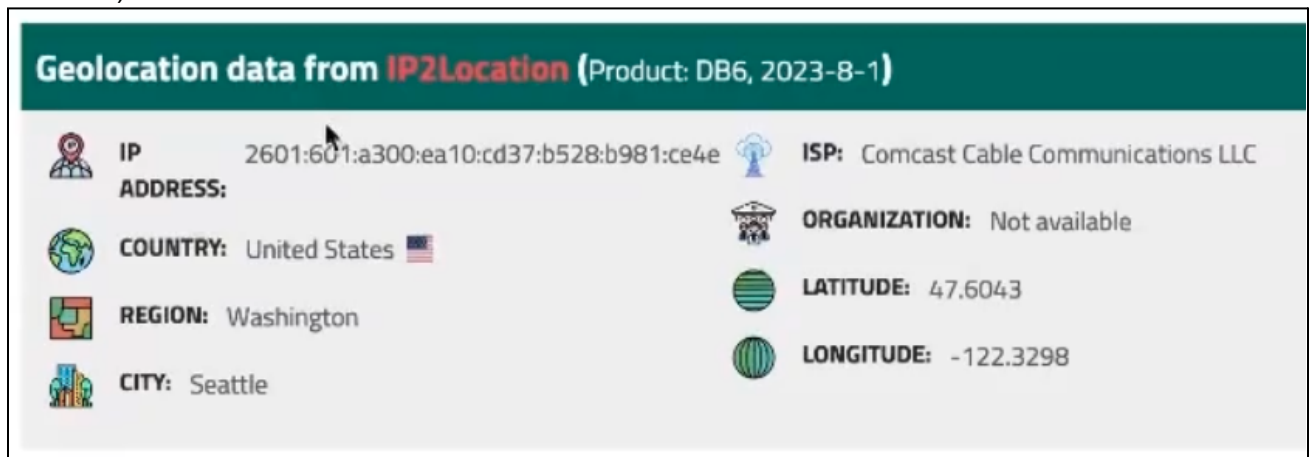
The screenshot shows a query editor window titled "New Query 1*" with a "Run" button and a "Time range: Last 24 hours" filter. The query text is:

```
1 SecurityEvent
2 | where EventID == 4625
```

Below the query, the "Results" tab is active, displaying a table with the following data:

TimeGenerated [UTC] ↑↓	Account	AccountType
> 11/8/2023, 9:06:41.278 PM	\SERVERADMIN	User
> 11/8/2023, 9:06:39.276 PM	\ADMINISTRATOR	User
> 11/8/2023, 9:06:36.183 PM	\CALENDAR	User

- b. We can analyze the attacker IPs using <https://iplocation.net> (or Google search for "geo locate IP address").



The screenshot shows geolocation data from IP2Location (Product: DB6, 2023-8-1) for the IP address 2601:601:a300:ea10:cd37:b528:b981:ce4e. The data is as follows:

IP ADDRESS: 2601:601:a300:ea10:cd37:b528:b981:ce4e	ISP: Comcast Cable Communications LLC
COUNTRY: United States 🇺🇸	ORGANIZATION: Not available
REGION: Washington	LATITUDE: 47.6043
CITY: Seattle	LONGITUDE: -122.3298

End:

- We've configured logging for our VMs and NSGs.