Lab #9: **Setup of Subscription-Level Logging**

Purpose:

- We're configuring subscription-level logging, which includes activity from our **Activity Log**. These logs will be sent to our Logs Analytics workspace.

> ***Note**: The **Activity Log** provides insight into the operations of each Azure resource. This log is used to determine the what, who, and when for any 'write' operations (PUT, POST, DELETE) taken on resources in our subscription.*

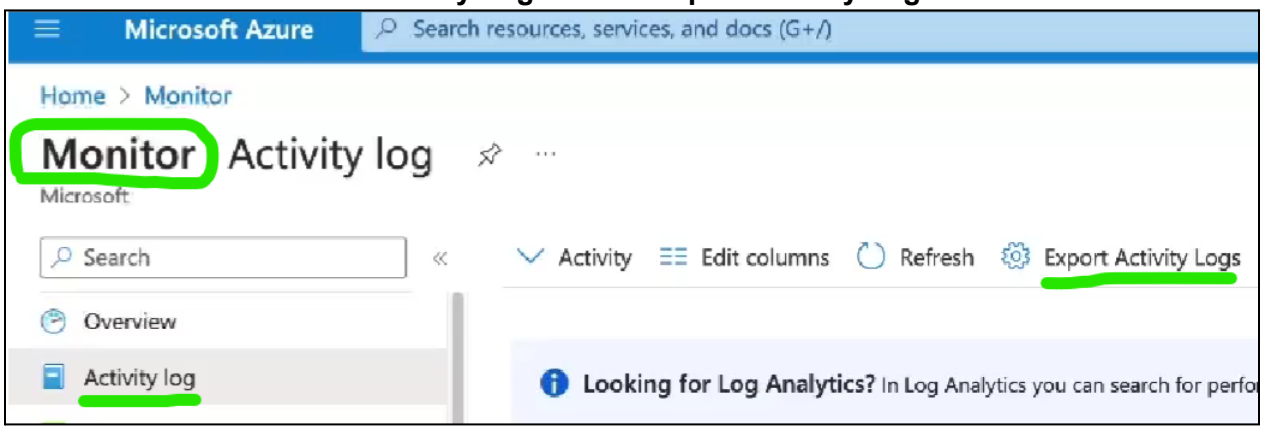
Tasks:

1. **Export the Activity Log to our Logs Analytics workspace**
    - Export Activity Logs
    - Verify that the Activity Logs are being sent to the workspace
2. **Generate audit logs (Resource Group creation)**
    - Create a new Resource Group ("Scratch-Resource-Group")
    - Create another new Resource Group ("Critical-Infrastructure-Wastewater")
    - Delete both of these Resource Groups
3. **Observe the "Activity Logs" logs in Log Analytics Workspace**
    - Querying for the deletion of critical Resource Groups
    - Querying for changes to Network Security Groups
    - Deletion activities within a certain timespan
    - From Microsoft Defender for Cloud Security Events
    - Querying activity on the Management Plane

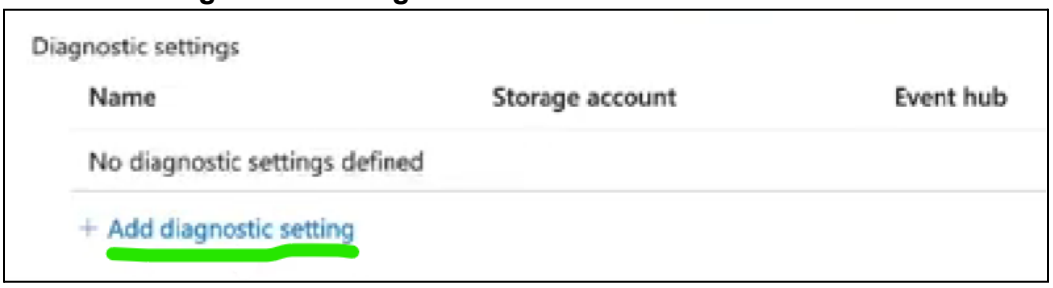
Task 1: **Export the Activity Log to our Logs Analytics workspace**

Export Activity Logs:

1. **Azure** account > **Monitor** > **Activity Log** > select **Export Activity Logs**



2. Select **Add Diagnostic Settings**:



   a. **Diagnostic setting name:** ds-azure-activity
   b. Logs > **Categories**: (select all checkboxes)
   c. **Destination**: (select the "Send to Log Analytics workspace" checkbox)
      i. Select our subscription and workspace.
   d. Select **Save**.

Verify that the Activity Logs are being sent to the workspace:

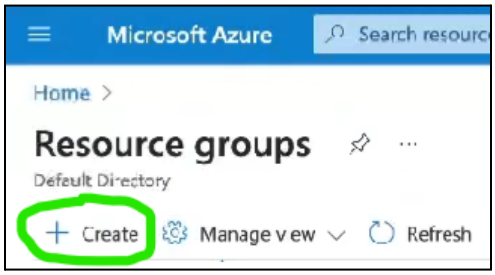
1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. In **New Query** terminal, run this command: **AzureActivity**

> ***Note***: *Though no results have appeared yet, it confirms that the logging is working!*

Task 2: Generate audit logs (Resource Group creation)

Create two new Resource Groups:

1. Create the first resource group.

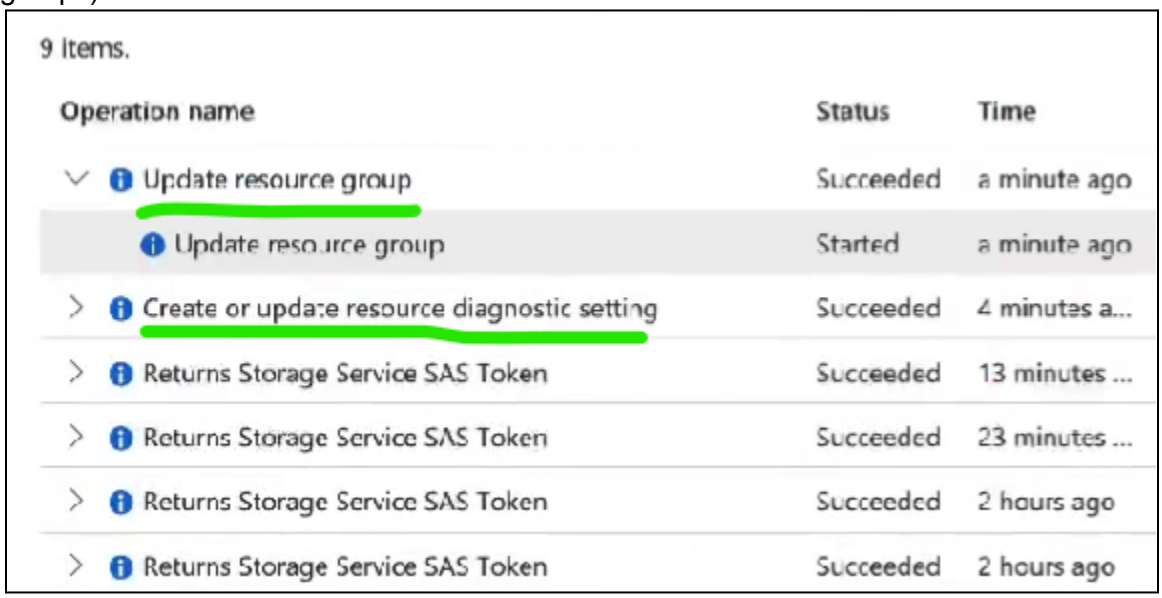


   a. **Azure** account > **Resource Groups** > **Create a resource group**
   Name it "Scratch-Resource-Group"
   b. Select **Review + Create**.
2. Create the second resource group.
   a. **Azure** account > **Resource Groups** > **Create a resource group**
   b. Name it "Critical-Infrastructure-Wastewater"
   c. Select **Review + Create**.

Verify that the Activity Logs are being sent to the workspace:

1. First, check the "Activity Logs" logs in **Azure Monitor**:

a. **Azure** account > **Monitor** > **Activity Log** > (we see the new logs from the created resource groups)



2. Second, check **Logs Analytics workspace**:
   a. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
   b. In **New Query** terminal, run **AzureActivity**

> ***Note***: *No "Activity Log" results have appeared yet in our Log Analytics workspace. This is understandable because the export mechanism takes time (may take 10-20 min).*

Delete both of these new Resource Groups:

1. **Azure** account > **Resource Groups** > (delete both of the new Resource Groups)

> ***Note***: *This should generate some more "Activity Log" logs.*

2. Re-run the **AzureActivity** command (results have appeared):

Task 3: Observe the “Activity Logs” logs in Logs Analytics workspace

Querying for the deletion of critical Resource Groups:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** > **New Query** terminal >
2. Run this command:
   AzureActivity | where ResourceGroup **startswith** "Critical-Infrastructure-" **| order by** TimeGenerated

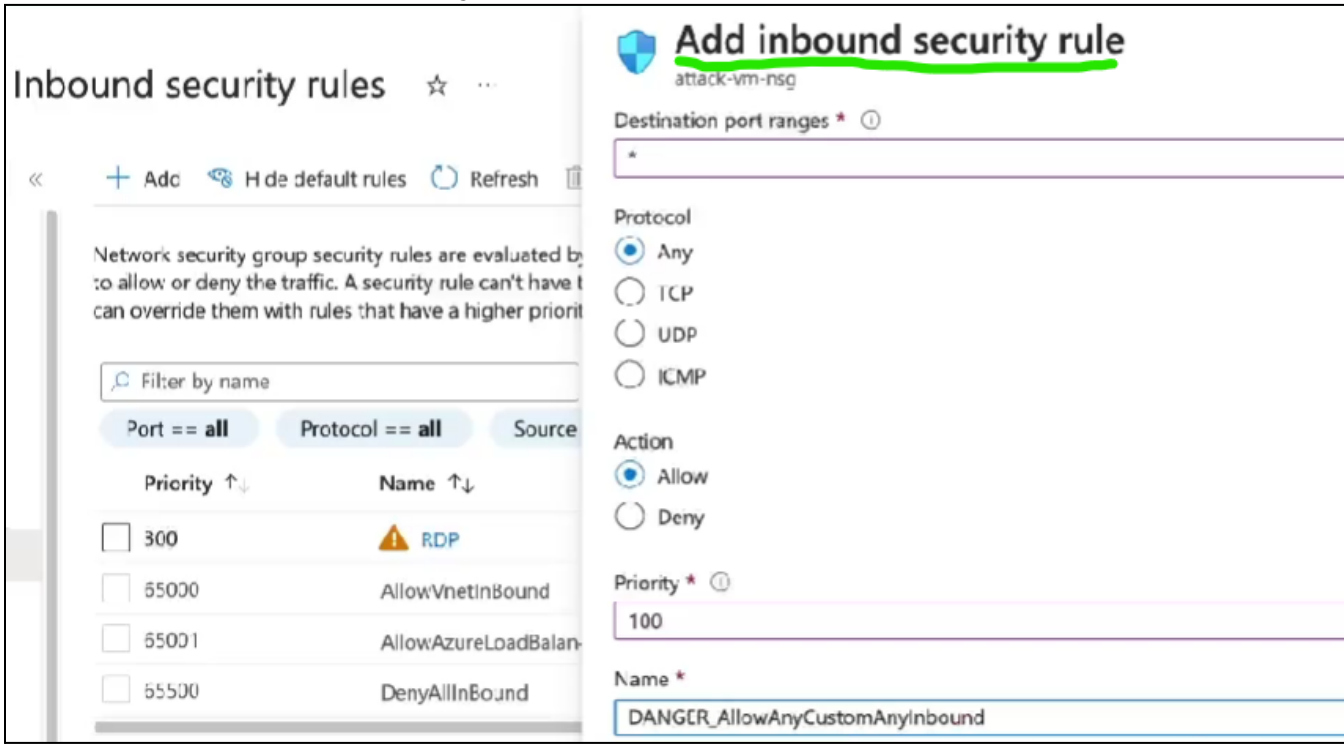
Results | Chart

TimeGenerated [Local Time]	OperationNameValue	Level	ActivityStatusValue
> 9/8/2023, 11:24:54.755 AM	MICROSOFT.RESOURCES/SU...	Information	Success
> 9/8/2023, 11:24:54.458 AM	MICROSOFT.RESOURCES/SU...	Information	Start

Note: *This command queries for log results where something was done in a Resource Group that starts with “Critical-Infrastructure-”. The commands in this section/task could ultimately be utilized for setting up activity alerts.*

Querying for changes to Network Security Groups:

1. Update an NSG (to generate logs):
   a. **Azure** account > **Network Security Groups** > (open the attack NSG)
   b. Add a new rule to **Inbound Security Rules** > (allows all inbound traffic)



2. View this newly created activity log:
   a. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
   b. **New Query** terminal > Ran this command:
   AzureActivity | where OperationNameValue **==**
   "MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/SECURITYRULES/WRITE"
   | order by TimeGenerated

Results | Chart

TimeGenerated [Local Time]	OperationNameValue	Level	Activi
9/6/2023, 11:33:10.397 AM	MICROSOFT.NETWORK/NETWORKSECURITYGROJPS/SECURITYRULES/WRITE	Information	Succe
9/6/2023, 11:33:05.319 AM	MICROSOFT.NETWORK/NETWORKSECURITYGROJPS/SECURITYRULES/WRITE	Information	Accep
9/6/2023, 11:33:04.319 AM	MICROSOFT.NETWORK/NETWORKSECURITYGROJPS/SECURITYRULES/WRITE	Information	Start

Deletion activities within a certain timespan:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. **New Query** terminal > Run this command:
   AzureActivity | where OperationNameValue **endswith** "DELETE" **| where** ActivityStatusValue **==** "Success" **| where** TimeGenerated **>** ago(30m) **| order by** TimeGenerated

From Microsoft Defender for Cloud Security Events:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. **New Query** terminal > Run this command:
   AzureActivity | where CategoryValue **==** "Security"

Querying activity on the Management Plane:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. **New Query** terminal > Run this command:
   AzureActivity | where CategoryValue **==** "Administrative"

End:

1. We configured the Azure Activity Log to be forwarded to our Log Analytics workspace.

   ***Note**: Soon, we'll set up a SIEM to query our Log Analytics workspace frequently (e.g., 1x/10min).*