

Lab 7 Report

CST8912_011

ZheZhang

041109657

March 9, 2025

Submitted to: Prof. Tanishq Bansal

Title

Azure Monitor: Configuring Alerts, Action Groups, and Log Queries

Introduction or Purpose

The purpose of this lab is to explore Azure's monitoring capabilities, specifically **Azure Monitor** and **Log Analytics**, to gain insight into the performance and configuration of Azure resources. The objectives include:

- Deploying a virtual machine using an ARM template.
- Configuring Azure Monitor to track resource performance.
- Creating alerts and configuring action group notifications.
- Testing alert triggers and validating notifications.
- Using Log Analytics to query performance metrics.

Steps Covered in the Lab

Task 1: Use a Template to Provision an Infrastructure

1. Downloaded the lab file az104-11-vm-template.json.
2. Logged into the Azure Portal (<https://portal.azure.com>).
3. Navigated to **Deploy a custom template** and selected **Build your own template in the editor**.
4. Loaded the az104-11-vm-template.json file and saved it.
5. Entered deployment details:
 - **Resource Group:** CST8912
 - **Region:** Canada Central
 - **Username:** localadmin
 - **Password:** 200530Zz!

6. Clicked **Review + Create**, then **Create**.
7. Verified that the deployment created:

- One virtual network.
- One virtual machine.

1. Configured **Azure Monitor for Virtual Machines**:

- Opened **Monitor** from the Azure Portal.
- Selected **View in the VM Insights**.
- Enabled monitoring for the deployed virtual machine.
- Used default subscription and data collection rules.

Monitor | Virtual Machines

Search x Refresh Provide Feedback

Overview Activity log Alerts Metrics Logs Change Analysis Service health Workbooks Investigator (preview) Insights Applications

Virtual Machines Storage accounts Containers Networks Azure Cosmos DB Key Vaults Azure Cache for Redis Azure Data Explorer Clusters Log Analytics workspaces Azure Local Service Bus (preview) Insights Hub Managed Services Settings Support + Troubleshooting

Get started Overview Performance Map

Filter by name... Subscription : 2 subscriptions Resource group : All resource groups Type : All types

Location : All locations Group by : Subscription, Resource group

Monitored (1) Not monitored (0) Workspace configuration Other onboarding options

Name	Monitor Coverage	Data collection rule
✓ Azure for Students	1 of 1	
✓ cst8912	1 of 1	
az104-vm0	Enabled	MSVMI-DefaultWorkspace-913a8401-361d-...

Task 2: Create an Alert

1. Opened **Monitor > Alerts**.
2. Clicked **Create +** and selected **Alert rule**.
3. Selected the resource group CST8912 and applied the setting.
4. Configured the condition:

- Clicked **See all signals**.
- Selected **Delete Virtual Machine (Virtual Machines)**.
- Applied default settings for event level and status.

Home > Monitor | Alerts >

Create an alert rule ...

Scope **Condition** Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * ⓘ Delete Virtual Machine (Virtual Machines) ▼
[See all signals](#)

Chart period
 Over the last 6 hours ▼

No data available

activityLogHistoryBarSeries
 7 PM

[View events in Azure Monitor - Activity Log](#)

Alert logic

Event Level ⓘ All selected ▼ Status ⓘ All selected ▼ Event initiated by ⓘ * (All services and users) ▼
[Add event initiator](#)

Condition preview

Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Virtual Machine (Virtual Machines)'

Task 3: Configure Action Group Notifications

1. Continued setting up the alert.
2. Clicked **Next: Actions**, then **Create action group**.
3. Configured the action group:
 - **Action Group Name:** Alert the operations team
 - **Display Name:** AlertOpsTeam
 - **Notification Type:** Email
 - **Notification Name:** VM was deleted
 - **Email Address:** (provided email)
4. Clicked **Review + Create**, then **Create**.

Create an alert rule

×

Scope

Condition

Actions

Details

Tags

Review + create

Scope

Resource

Azure for Students > CST8912

Condition

Condition preview

Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Virtual Machine (Virtual Machines)'

Actions

Action group name

Contain actions

Alert the operations team

1 Email

Details

Project details

Subscription

Resource group

Region

Azure for Students

CST8912

global

Alert rule details

Alert rule name

Alert rule description

Enable upon creation

VM was deleted

A VM in your resource group was deleted

☒

Task 4: Trigger an Alert and Confirm Notification

1. Navigated to **Virtual Machines**.
2. Selected az104-vm0, clicked **Delete**.
3. Checked **Apply force delete**, typed "delete" to confirm.
4. Verified deletion in **Notifications**.
5. Checked email for an alert from Azure Monitor.



You've been added to an Azure Monitor action group

You are now in the AlertOpsTeam action group and will receive notifications sent to the group.

[View details on Azure Monitor action groups >](#)

Account information

Subscription ID: 913A8401-361D-4F42-8D7D-E2FF44F75DA2

Resource group name: CST8912

Action group name: Alert the operations team

To unsubscribe from this action group, [click here](#).



[Privacy Statement](#)

Microsoft Corporation, One [Microsoft Way](#), [Redmond, WA 98052](#)



Task 5: Configure an Alert Processing Rule

1. Opened **Monitor > Alerts > Alert Processing Rules**.
2. Clicked + **Create**.
3. Selected the resource group CST8912.
4. Chose **Suppress notifications**.
5. Scheduled maintenance period:
 - **Start:** Today at 10 PM
 - **End:** Tomorrow at 7 AM
 - **Time Zone:** Local

6. Clicked **Review + Create**, then **Create**.

Create an alert rule

ScopeConditionActionsDetailsTagsReview + create

Scope

Resource

Azure for Students > CST8912

Condition

Condition preview

Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Virtual Machine (Virtual Machines)'

Actions

Action group name

Alert the operations team

Contain actions

1 Email

Details

Project details

Subscription

Resource group

Region

Azure for Students

CST8912

global

Alert rule details

Alert rule name

Alert rule description

Enable upon creation

VM was deleted

A VM in your resource group was deleted

☒

Task 6: Use Azure Monitor Log Queries

1.Opened **Monitor** > **Logs**.

2.Selected the scope as **CST8912 Resource Group**.

3.Ran **Count heartbeats** query:

Heartbeat

| summarize count() by Computer

- o Verified VM heartbeat was detected.

1. Replaced the query with:

InsightsMetrics

| where TimeGenerated > ago(1h)

```
| where Name == "UtilizationPercentage"
| summarize avg(Val) by bin(TimeGenerated, 5m), Computer
| render timechart
```

2.

- Ran the query and observed the CPU utilization chart.



Results

The lab successfully demonstrated:

- Deploying a virtual machine using an ARM template.
- Enabling Azure Monitor to track VM performance.
- Setting up alerts for VM deletion.
- Configuring an action group to send email notifications.
- Testing alert functionality by deleting a VM.
- Using Azure Monitor logs to analyze system metrics.

References

1. Microsoft Azure Documentation - <https://docs.microsoft.com/en-us/azure/>
2. Algonquin College Cloud Architecture Course Material