

Lab 7 CST8912_011

Tarang Savaj

Sava0207

March 10, 2025

Submitted to:
Prof. Tanishq Bansal

Lab-7

Title

- Optimizing Cloud Costs with Azure Monitor and Log Analytics

Introduction

- An efficient cloud system operation requires effective management of cloud expenses as a fundamental aspect. Businesses must track their cloud costs while transitioning infrastructure to the cloud and simultaneously maximize value through performance and reliability. This laboratory demonstrates the Azure platform's capabilities for cloud cost monitoring using built-in management services that enable effective budget control.
- During this laboratory work, I will investigate Azure Monitor and Log Analytics solutions, as they track cloud resource performance and configuration details. These analytical tools help businesses monitor expenses by tracking infrastructure changes and providing notifications about critical incidents. My system implements automated alert systems alongside log queries to monitor critical events, such as virtual machine deletions, and to send instant notifications to the operations team.
- I will perform several tasks during the lab, including deploying virtual machines using a customized template system and designing alerts and notification functions within action group capabilities. To analyze resource usage, I will use Azure Monitor log queries to track performance data while working with the platform. The practical application of Azure services during this workshop will enhance my understanding of cloud resource monitoring, cost management, and efficient responses to infrastructure changes.

Steps

- To complete this lab, start by deploying a virtual machine using a custom template in the Azure portal. Once the VM is set up, enable **Azure Monitor** and configure VM Insights to track its performance. Next, create an alert to notify the operations team if a virtual machine is deleted. Set up an action group to send an email notification when the alert is triggered. To test this, delete the virtual machine and check your email for the alert notification. You can also verify the alert in the Azure portal under the **Monitor** section. After that, create an alert processing rule to pause notifications during scheduled maintenance by setting a time range. Finally, use **Azure Monitor log queries** to analyze the virtual machine's activity, run built-in queries like "Count heartbeats," and try a custom query to track CPU usage over time. Once everything is done, clean up the resources and document the steps.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Custom deployment >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↑ Load file ↓ Download

> Parameters (15)

> Variables (8)

▼ Resources (6)

- [concat(parameters('nicNamePrefix'), copyIndex())] (Microsoft.Network/networkInterface)
- [parameters('virtualNetworkName')] (Microsoft.Network/virtualNetwork)
- [concat(parameters('pipNamePrefix'), copyIndex())] (Microsoft.Network/publicIpAddress)
- [parameters('nsgName')] (Microsoft.Network/networkSecurityGroup)
- [variables('storageAccountName')] (Microsoft.Storage/storageAccount)
- [concat(parameters('vmNamePrefix'), copyIndex())] (Microsoft.Compute/virtualMachines)

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "adminUsername": {
6       "type": "string",
7       "metadata": {
8         "description": "Admin username"
9       }
10    },
11    "adminPassword": {
12      "type": "securestring",
13      "metadata": {
14        "description": "Admin password"
15      }
16    },
17    "vmNamePrefix": {
18      "type": "string",
19      "defaultValue": "az104-vm",
20      "metadata": {
21        "description": "VM name prefix"
22      }
23    },
24    "pipNamePrefix": {
25      "type": "string",
26      "defaultValue": "az104-pip",
27      "metadata": {
28        "description": "Public IP address name prefix"
29      }
30    },
31    "nicNamePrefix": {
32      "type": "string",
33      "defaultValue": "az104-nic",
34      "metadata": {
```

Save Discard

1.1 Showing uploaded JSON file

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home >

Custom deployment

Deploy from a custom template

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription

Resource group

Region

Admin Username

Admin Password

Vm Name Prefix

Pip Name Prefix

Nic Name Prefix

Image Publisher

Image Offer

Image SKU

Vm Size

Virtual Network Name

Address Prefix

Virtual Network Resource Group

Subnet0Name

Subnet0Prefix

Nsg Name

Azure for Students

CST8912

Canada Central

localadmin

az104-vm

az104-pip

az104-nic

MicrosoftWindowsServer

WindowsServer

2019-Datacenter

Standard_D2s_v3

az104-vnet

10.0.0.0/24

az104-rg11

subnet0

10.0.0.0/26

az104-nsg01

Previous

Next

Create

1.2 Overview of Custom deployment

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home > Microsoft.Template-20250309212355 | Overview >

CST8912

Resource group

Search

Create

Manage view

Delete resource group

Refresh

Export to CSV

Open query

Assign tags

Move

Delete

Export template

Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

Essentials

Subscriptions

Deployments

1 Succeeded

Location

Canada Central

Resources

Recommendations

Filter for any field...

Type equals all

Location equals all

Add filter

Showing 1 to 7 of 7 records.

Show hidden types

No grouping

List view

Name	Type	Location
az104-nic0	Network interface	Canada Central
az104-nsg01	Network security group	Canada Central
az104-pip0	Public IP address	Canada Central
az104-vm0	Virtual machine	Canada Central
az104-vm0_disk1_0b08e9dd80144ad7b05780bd7c490614	Disk	Canada Central
az104-vnet	Virtual network	Canada Central
az10411n68205ghcadde	Storage account	Canada Central

Previous

Page 1 of 1

Next

Give feedback

1.3 Overview of Resource group

Microsoft Azure | Monitor | Virtual Machines

Get started: Overview, Performance, Map

Filter by name... | Subscription: 2 subscriptions | Resource group: cs10912 | Type: Virtual

Name	Monitor Coverage
Azure for Students	1 of 1
cs10912	1 of 1
cs104-vm0	Not enabled Enable

Azure Monitor
Insights Onboarding

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the monitoring data to appear.

The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

[Enable](#)

Having difficulties enabling Azure Monitors for VM? [Troubleshoot](#)

Have more questions?
[Learn more about virtual machine monitoring](#)
[What is VM Insights?](#)
[Learn more about pricing](#)
[Support Matrix](#)
[FAQ](#)
[Update Azure Agent](#)

1.4 Enabling VM twice

Microsoft Azure | Monitor | Alerts

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 * [Select a signal](#) [See all signals](#)

Select a signal

Signal type: All | Signal source: All

Signal name	Signal source
Activity log	
Delete Virtual Machine (Virtual Machines)	Administrative
Deletes PreservedOSDisk on the Virtual Machine (Virtual Machines)	Administrative

[Review + create](#) [Previous](#) [Next: Actions >](#) [Apply](#) [Cancel](#)

2.1 showing delete virtual machine in the alerts

Microsoft Azure Search resources, services, and docs (G+)

Home > Monitor | Alerts >

Create an alert rule

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

Chart period
Over the last 6 hours ⌵

No data available

activityLogHistoryBarSeries

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)

[Review + create](#) [Previous](#) [Next: Actions >](#)

2.2 Showing all selected in Event level and Status

Microsoft Azure Search resources, services, and docs (G+)

Home > Monitor | Alerts > Create an alert rule >

Create action group

Basics **Notifications** Actions Tags Review + create

Choose how to get notified when the action group is triggered. This step is optional.

Notification type ⌵	Name ⌵	Selected ⌵
Email/SMS message/Push/Voice ⌵	VM was deleted ⌵	Email ⌵
⌵	⌵	⌵

[Review + create](#) [Previous](#) [Next: Actions >](#)

3.1 Showing notification in action group

Delete az104-vm0

This action will permanently delete this virtual machine.

Resource to be deleted	Resource type
az104-vm0	Virtual machine

☒ **Apply force delete**

You can also choose to delete associated resources at the same time. Resources that aren't deleted will be orphaned. Associated resources that are in use by other resources are not shown here.

Associated resource type	Quantity	Delete with VM
OS disk	1	<input type="checkbox"/>
Network interfaces	1	<input type="checkbox"/>
Public IP addresses	1	<input type="checkbox"/>

☒ I have read and understand that this virtual machine as well as any selected associated resources listed above will be deleted.

Delete **Cancel**

4.1 deleting virtual machine with apply force delete

Notifications

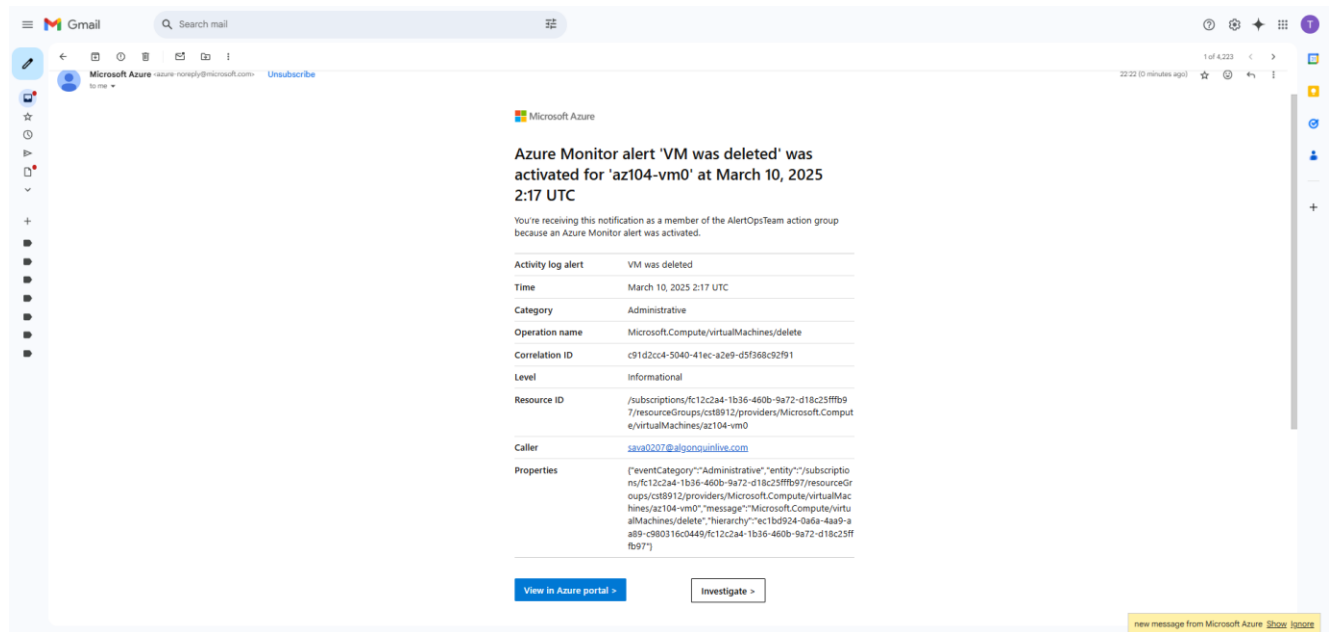
More events in the activity log → [Dismiss all](#)

Successfully deleted virtual machine 'az104-vm0'

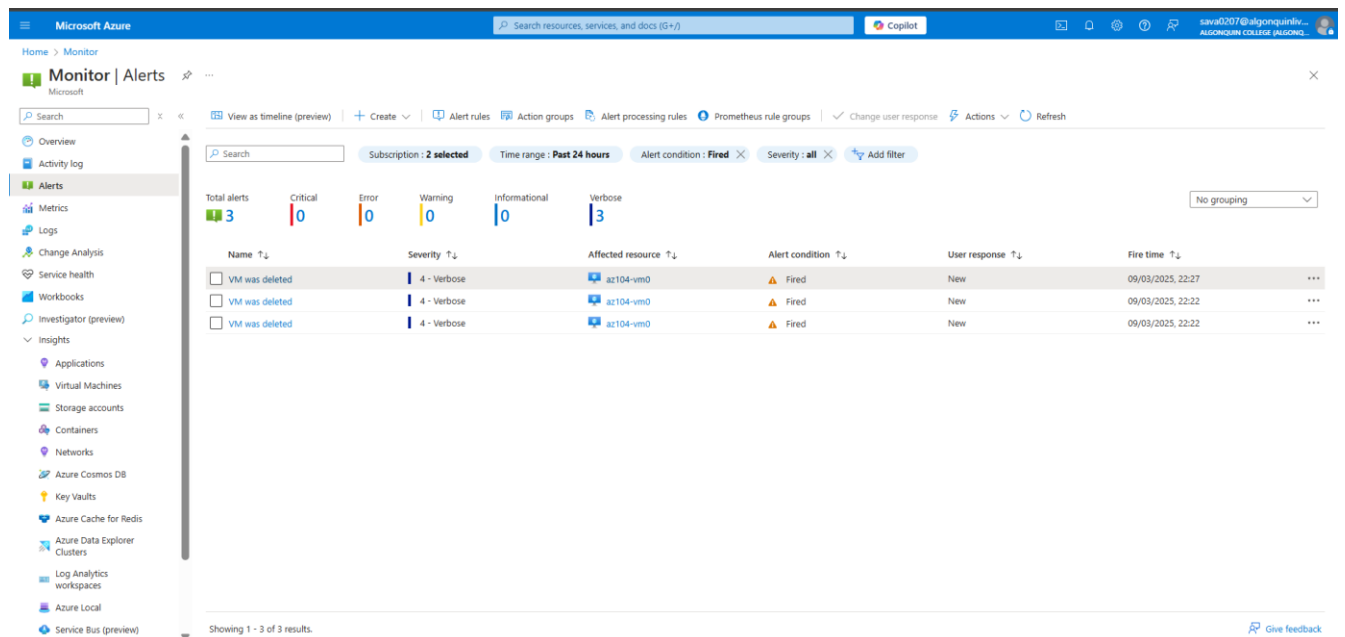
Virtual machine 'az104-vm0' and any selected resource(s) have been successfully deleted.

a few seconds ago

4.2 notification of virtual machine deleted



4.3 Mail showing deleted VM notification



4.4 Showing alert notification

The screenshot displays the 'Planned Maintenance' alert processing rule in the Microsoft Azure portal. The interface includes a left-hand navigation pane with options like 'Create', 'Columns', and 'Name'. The main content area shows the rule's configuration, including its name, description, and various settings.

Planned Maintenance
Alert processing rule

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Automation
- Help

Essentials

- Resource group: CST8912
- Location: Global
- Subscription: Azure for Students
- Subscription ID: fc12c2d4-1b36-460b-9a72-d18c25fffb97
- Tags: Add tags

Scope

- Resource: cst8912
- Hierarchy: Azure for Students

Scheduling

- Apply the rule: At a specific time
- Schedule: From 03/09/2025 at 10:00 PM to 03/10/2025 at 7:00 AM (Ea...

Rule settings

- Rule type: Suppress notifications

Showing 1 - 1 of 1 results.

5.1 Overview of alert processing rules

The screenshot displays the 'Monitor | Logs' section in the Microsoft Azure portal. It shows a new query being run, with the results displayed in a table format. The query is a KQL (Kusto Query Language) query that filters for heartbeat events and summarizes the count by bin of time generated and computer.

Monitor | Logs

New Query 1*

Time range: Set in query | Show: 1000 results

Run

```

1 heartbeat
2 | where TimeGenerated > ago(24h)
3 | summarize count() by bin(TimeGenerated, 5m), Computer
4 | order by TimeGenerated desc
5

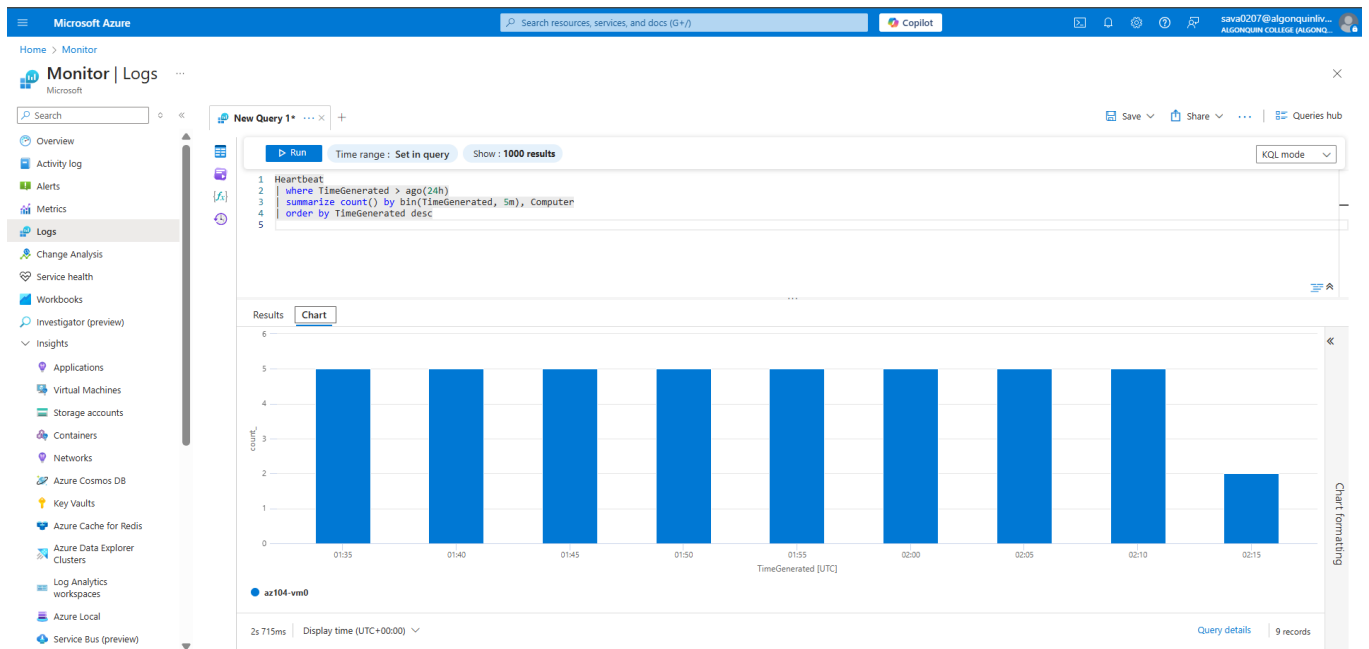
```

Results

TimeGenerated [UTC]	Computer	count_
> 10/03/2025, 02:15:00.000	az104-vm0	2
> 10/03/2025, 02:10:00.000	az104-vm0	5
> 10/03/2025, 02:05:00.000	az104-vm0	5
> 10/03/2025, 02:00:00.000	az104-vm0	5
> 10/03/2025, 01:55:00.000	az104-vm0	5
> 10/03/2025, 01:50:00.000	az104-vm0	5
> 10/03/2025, 01:45:00.000	az104-vm0	5
> 10/03/2025, 01:40:00.000	az104-vm0	5
> 10/03/2025, 01:35:00.000	az104-vm0	5

2s 715ms | Display time (UTC+00:00) | Query details | 1 - 9 of 9

6.1 Run the given query and showing result



6.2 Charts of the query

The screenshot shows the Microsoft Azure portal. At the top, there's a 'Delete alert rule' notification: 'Alert rule deleted successfully'. Below this, the 'Azure services' section shows icons for various services. The 'Resources' section is expanded, showing a table of resources:

Name	Type	Last Viewed
VM was deleted	Activity log alert rule	a few seconds ago
CST8912	Resource group	a few seconds ago
DefaultWorkspace-fc12c2a4-1b36-460b-9a72-d18c25fbb97-EUS	Log Analytics workspace	18 minutes ago
Planned Maintenance	Alert processing rule	41 minutes ago
vault-mde5ovd6	Recovery Services vault	3 weeks ago
savajtarangr	Resource group	3 weeks ago
Azure for Students	Subscription	4 weeks ago
AVD-Prod	Subscription	4 weeks ago

Below the table, there's a 'Navigate' section with icons for Subscriptions, Resource groups, All resources, and Dashboard. At the bottom, there's a 'Tools' section with icons for Microsoft Learn, Azure Portal, Microsoft Defender for Cloud, and Microsoft Defender for Endpoint.

7.1 Delete alert rule

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home >

CST8912 Resource group

Deleting resource group CST8912
Deleting resource group CST8912

Search

Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

Essentials

Subscription (moyd) : Azure for Students

Subscriptions ID : fct2c2a4-1b36-460b-9a72-d18c25ffb97

Tags (edit) : Add tags

Deployments : 3 Succeeded

Location : Canada Central

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 7 of 7 records. Show hidden types

No grouping List view

Name	Type	Location
Alert the operations team	Action group	Global
az104-nic0	Network interface	Canada Central
az104-nsg01	Network security group	Canada Central
az104-pip0	Public IP address	Canada Central
az104-vm0_disk1_ob08e9dd0144ad7b057808d7c496814	Disk	Canada Central
az104-vnet	Virtual network	Canada Central
az10411n662o5ghcaddie	Storage account	Canada Central

< Previous Page 1 of 1 Next >

Give feedback

7.2 Deleting Resource group

References

- References for this task are taken from the provided lab file.