

CANTON WEKE OTIENO

SECURITY ENGINEER TRACK

STUDENT TRACKING NUMBER; ADC-SE01-24010

CYBER SHUJAA

INSTRUCTOR: Dr. Paula

LAB 11 - IMPLEMENT MONITORING

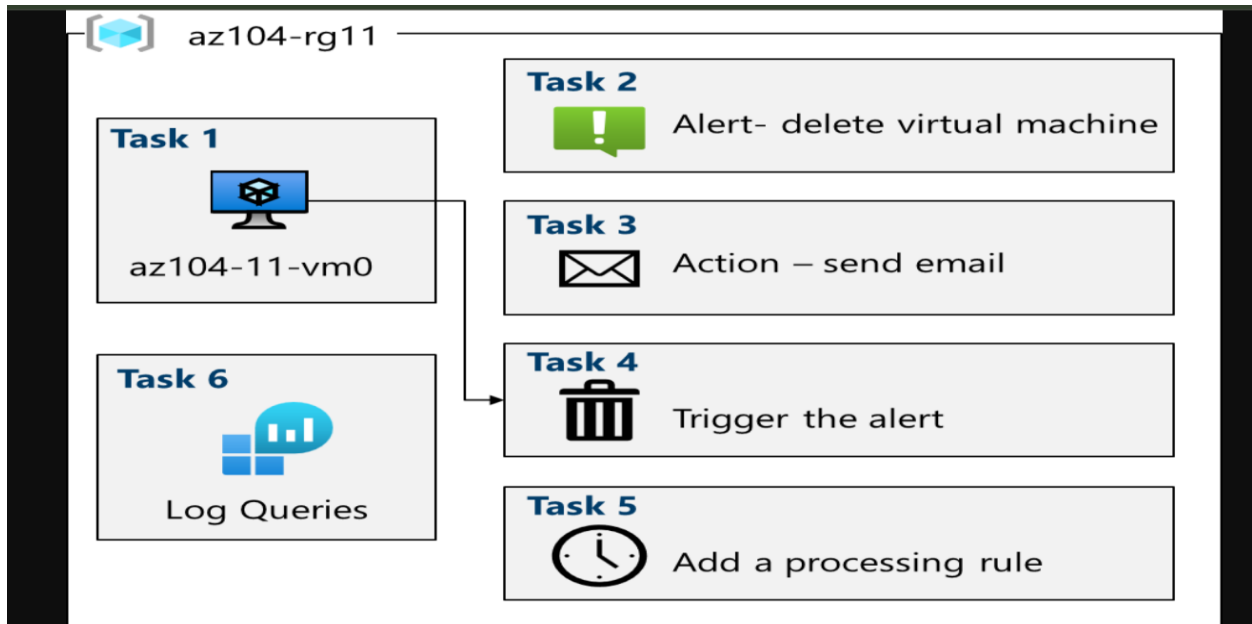
Introduction

In today's rapidly evolving digital landscape, cloud infrastructure management has become a cornerstone of IT operations. This lab delves into the practical aspects of using Microsoft Azure to provision and monitor cloud infrastructure, emphasizing the importance of efficient deployment, proactive monitoring, and data-driven decision-making.

This lab, involves how to do configuration of Azure Monitor, creating an alert and send it to an action group. triggering and testing the alert and check the activity log.

The report contains five activities and task that give guidance on how to the configurations, this task includes, using a template to provision an infrastructure, Creating an alert. Configuring action group notifications, triggering an alert and confirming its functionality, configuring an alert processing rule. and finally use Azure Monitor log queries.

Architecture diagram



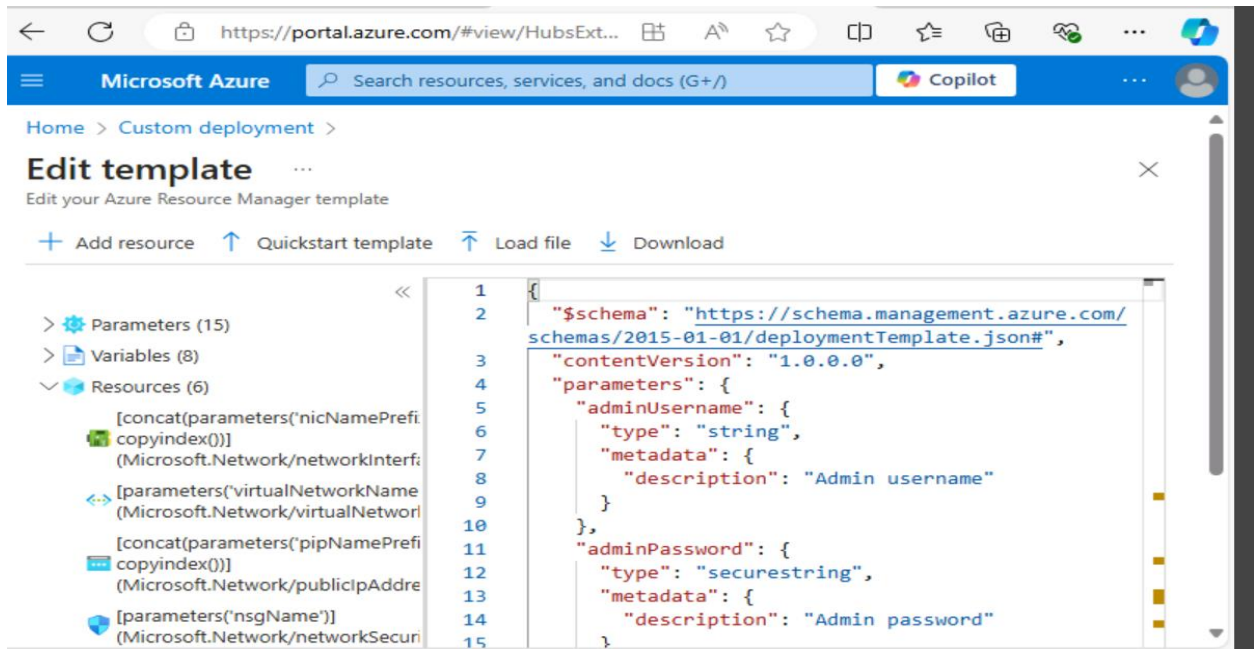
Task 1: Use a template to provision an infrastructure

In this task, involves deployment of a virtual machine that will be used to test monitoring scenarios.

Instruction and steps for conducting configuration

- Download the \Allfiles\Lab11\az104-11-vm-template.json lab files to your computer.
- Sign in to the Azure portal - <https://portal.azure.com>.
- From the Azure portal, search for and select Deploy a custom template.

- On the custom deployment page, select Build you own template in the editor.
- On the edit template page, select Load file.
- Locate and select the \\Allfiles\\Labs11\\az104-11-vm-template.json file and select Open.
- Select Save.



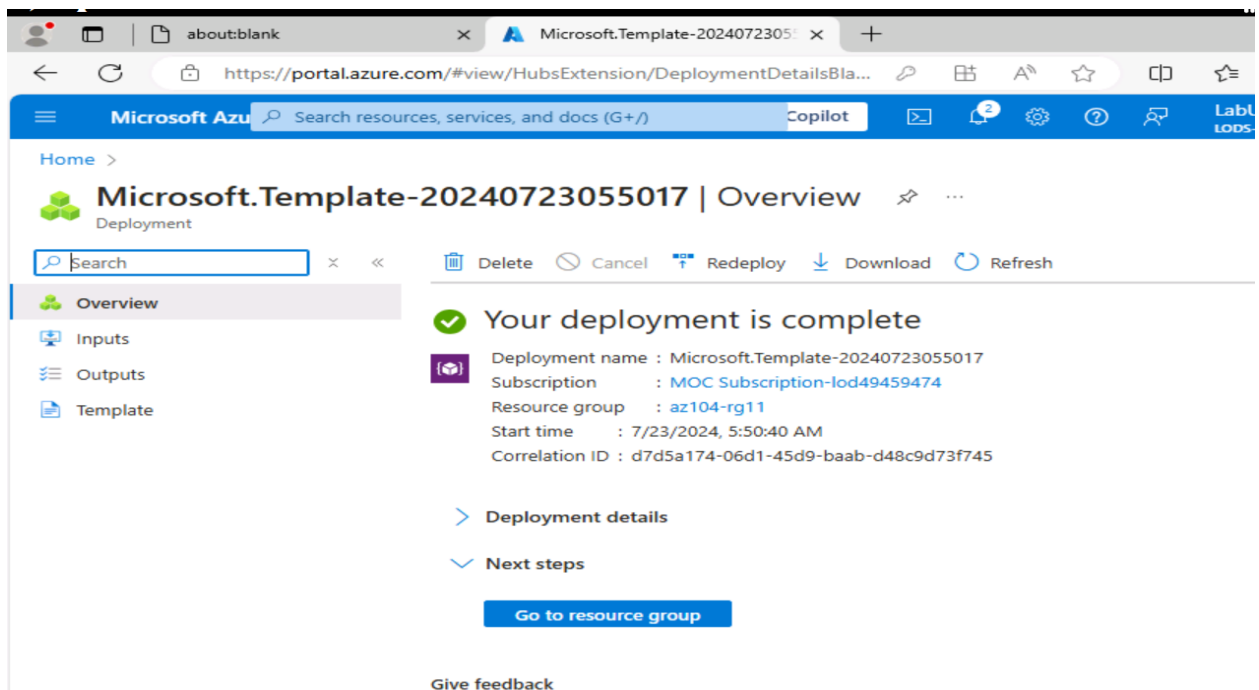
- Use the following information to complete the custom deployment fields, leaving all other fields with their default values:

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. The page title is 'Custom deployment' with a subtitle 'Deploy from a custom template'. Below the title, there is a message about 'New! Deployment Stacks' and a link to 'Try it now'. The main area contains a form with the following fields:

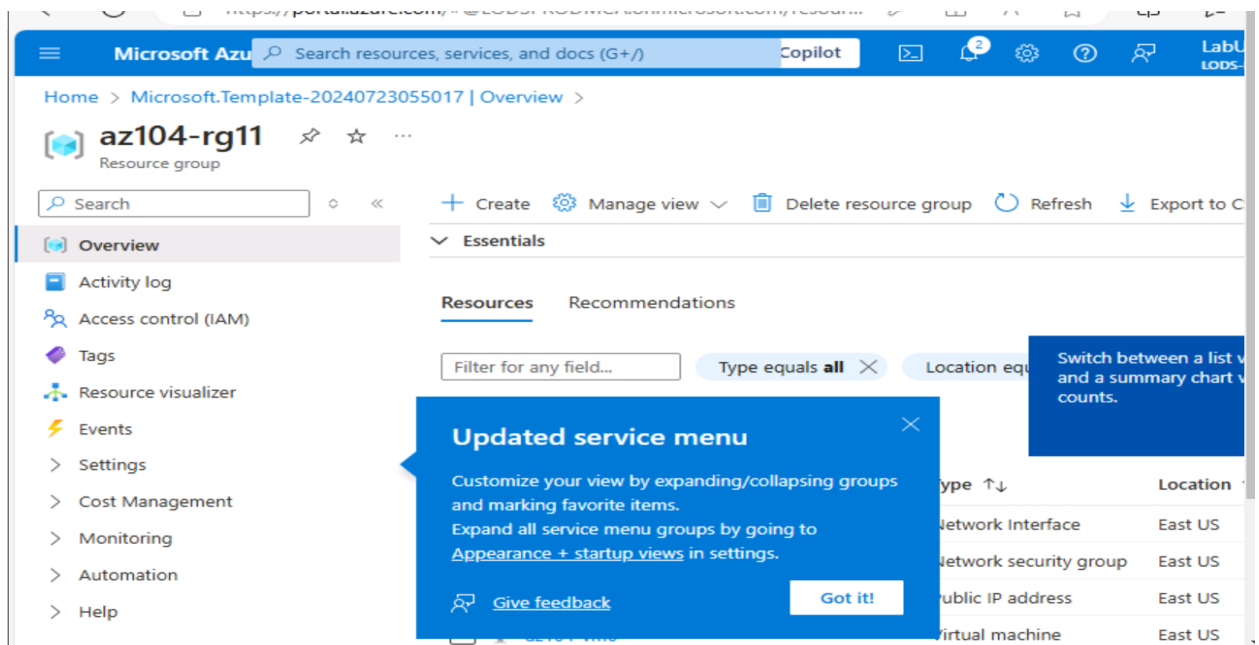
- Subscription: MOC Subscription-lod49459474
- Resource group: (New) az104-rg11
- Region: East US
- Admin Username: localadmin
- Admin Password: [masked]
- Vm Name Prefix: az104-vm
- Pip Name Prefix: az104-s
- Nic Name Prefix: az104-nic

At the bottom of the form, there are buttons for 'Previous', 'Next', and 'Review + create'.

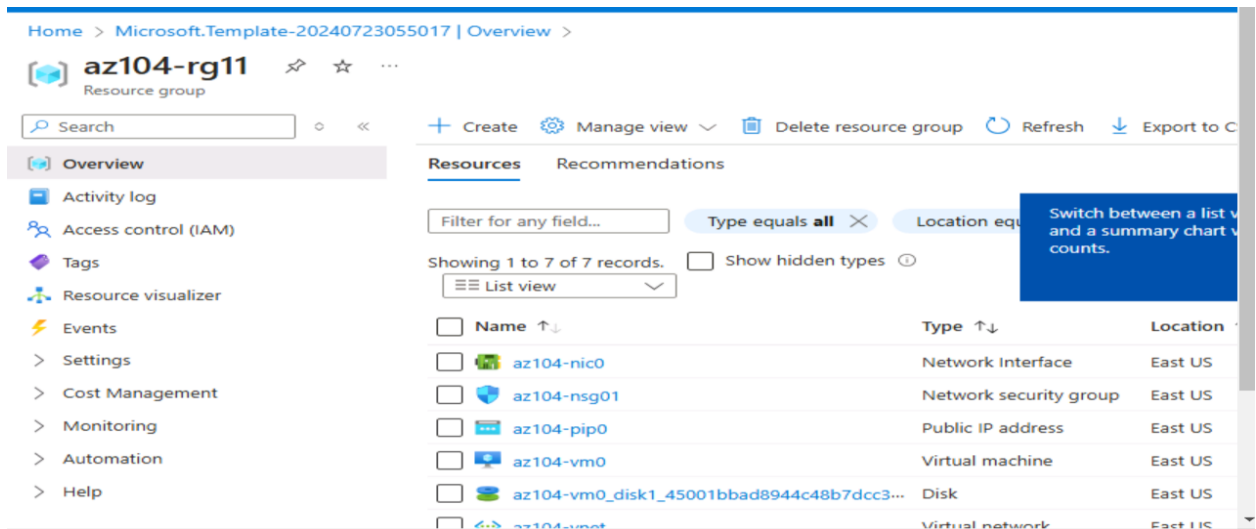
- Select Review + Create, then select Create.



- Wait for the deployment to finish, then click Go to resource group.

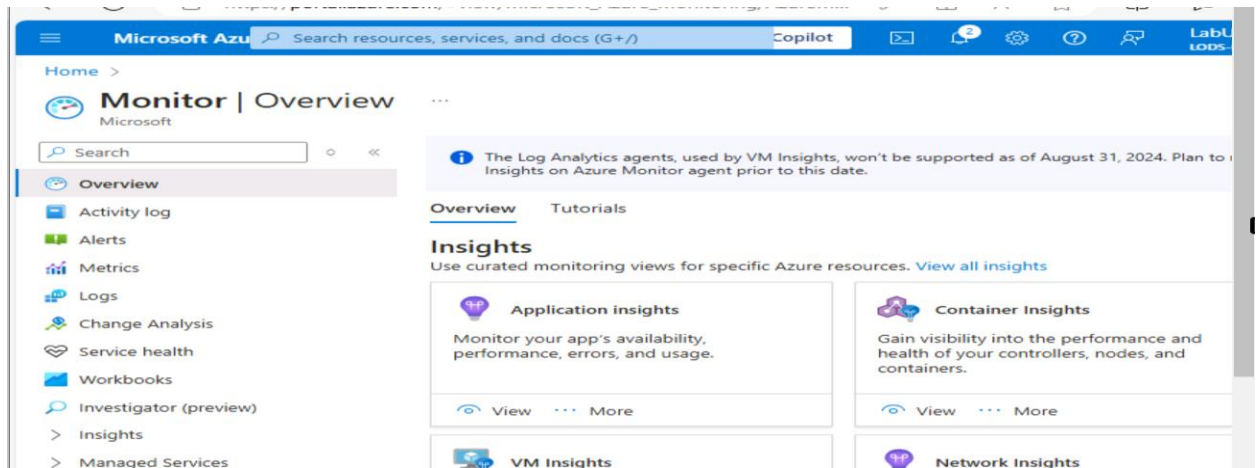


- Review what resources were deployed. There should be one virtual network with one virtual machine.

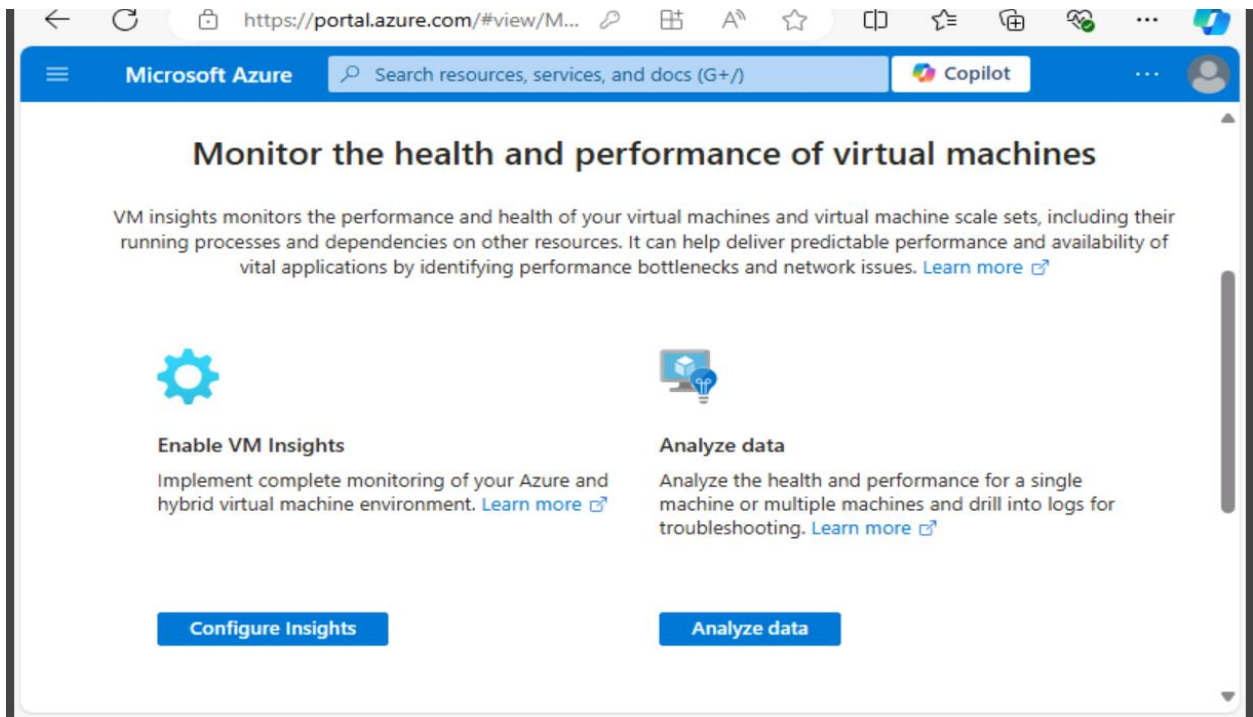


Configure Azure Monitor for virtual machines (this will be used in the last task)

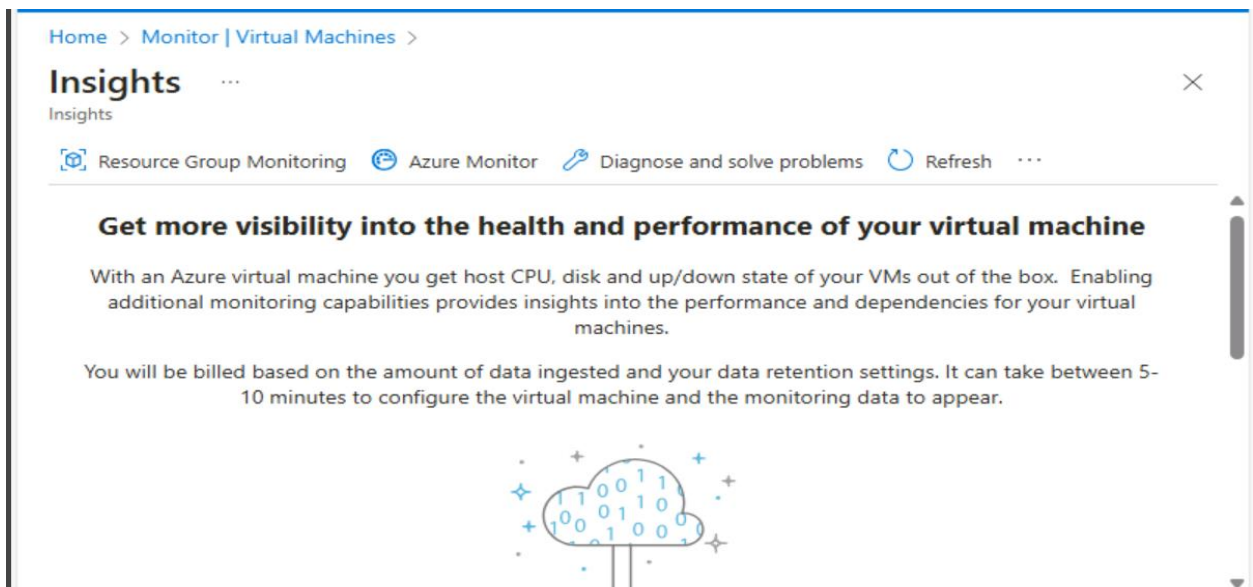
- In the portal, search for and select Monitor.
- Take a minute to review all the insights, detection, triage, and diagnosis tools that are available.



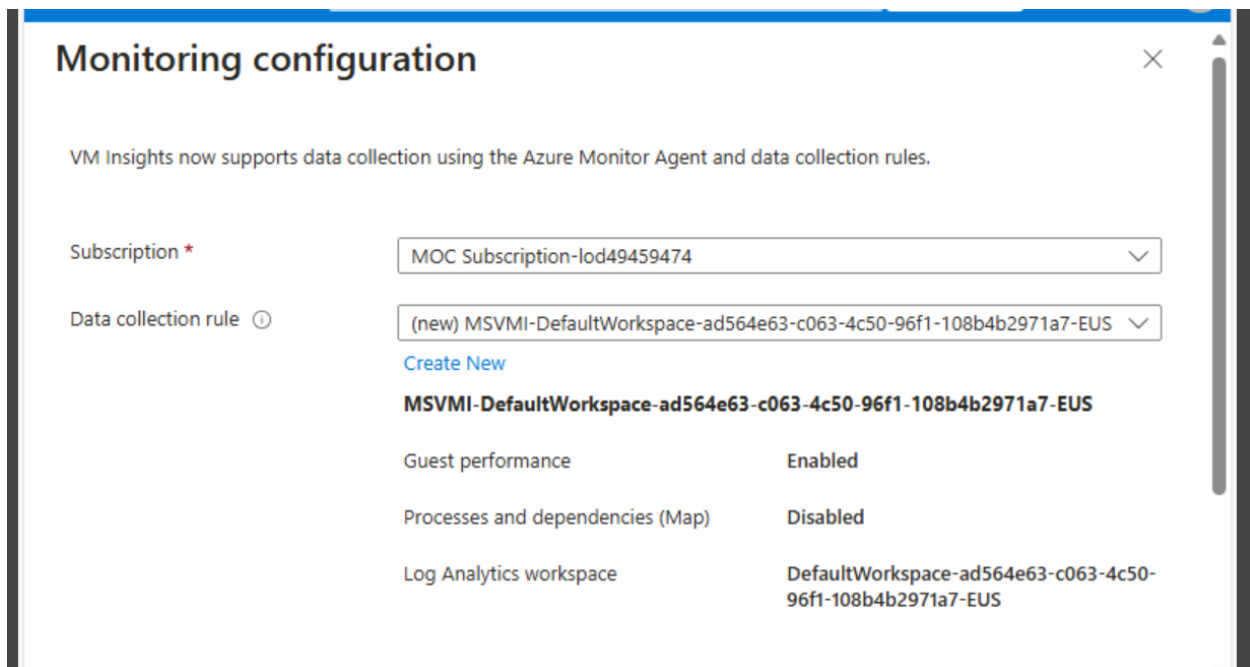
- Select View in the VM Insights box, and then select Configure Insights.



- Select your virtual machine, and then Enable (twice).



- Take the defaults for subscription and data collection rules, then select Configure.



Monitoring configuration

VM Insights now supports data collection using the Azure Monitor Agent and data collection rules.

Subscription * MOC Subscription-lod49459474

Data collection rule ⓘ (new) MSVM-DefaultWorkspace-ad564e63-c063-4c50-96f1-108b4b2971a7-EUS

[Create New](#)

MSVM-DefaultWorkspace-ad564e63-c063-4c50-96f1-108b4b2971a7-EUS

Guest performance	Enabled
Processes and dependencies (Map)	Disabled
Log Analytics workspace	DefaultWorkspace-ad564e63-c063-4c50-96f1-108b4b2971a7-EUS

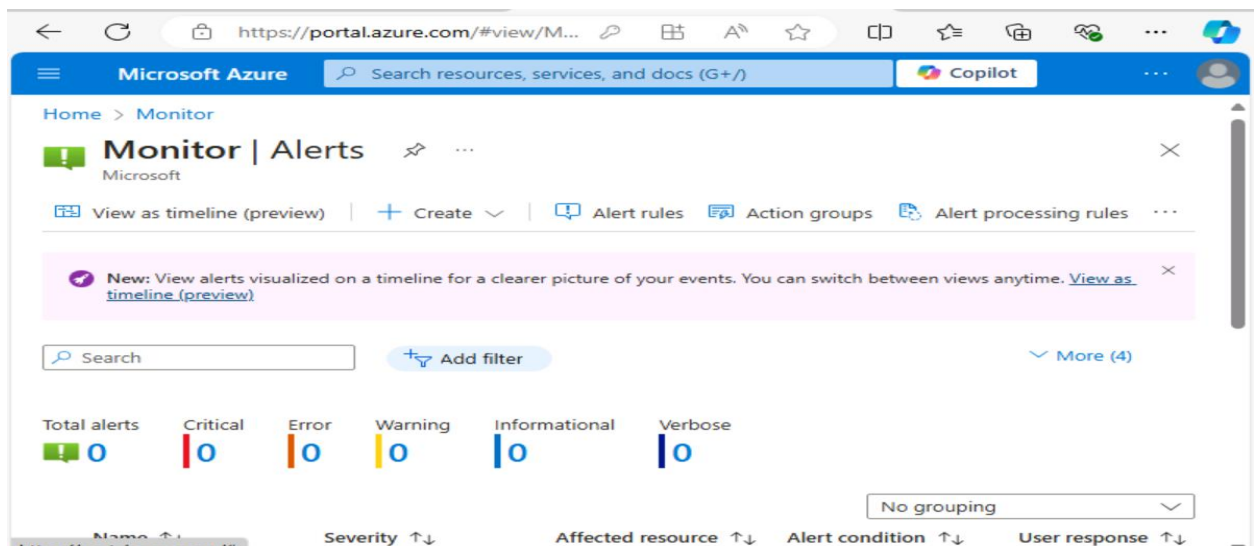
- It will take a few minutes for the virtual machine agent to install and configure, proceed to the next step.

Task 2: Create an alert

This task involves creating of an alert when virtual machine is deleted

Instruction and steps for configuration

- Continue the Monitor page, select Alerts.



Microsoft Azure

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

Copilot

Home > Monitor

Monitor | Alerts

Microsoft

View as timeline (preview) | Create | Alert rules | Action groups | Alert processing rules

New: View alerts visualized on a timeline for a clearer picture of your events. You can switch between views anytime. [View as timeline \(preview\)](#)

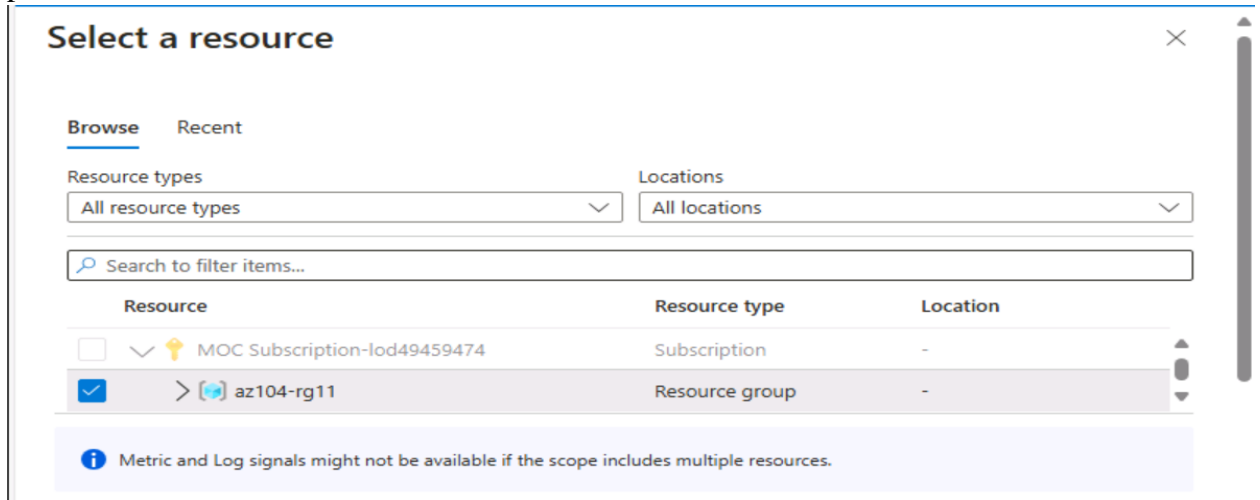
Search Add filter More (4)

Total alerts 0 Critical 0 Error 0 Warning 0 Informational 0 Verbose 0

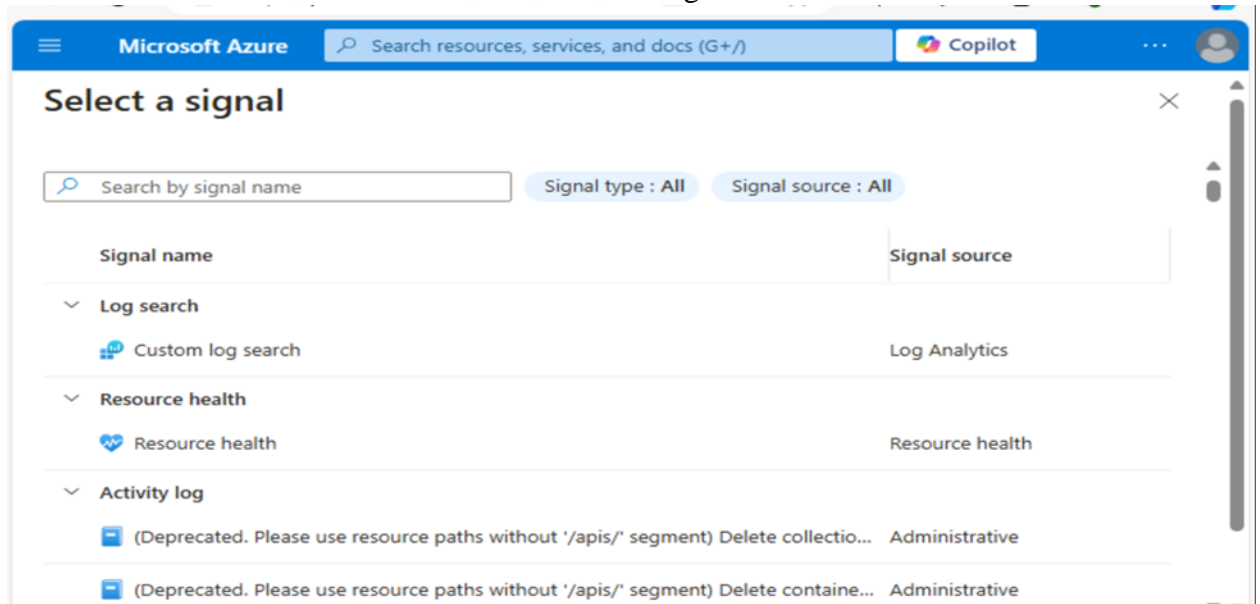
No grouping

Name ↑↓ Severity ↑↓ Affected resource ↑↓ Alert condition ↑↓ User response ↑↓

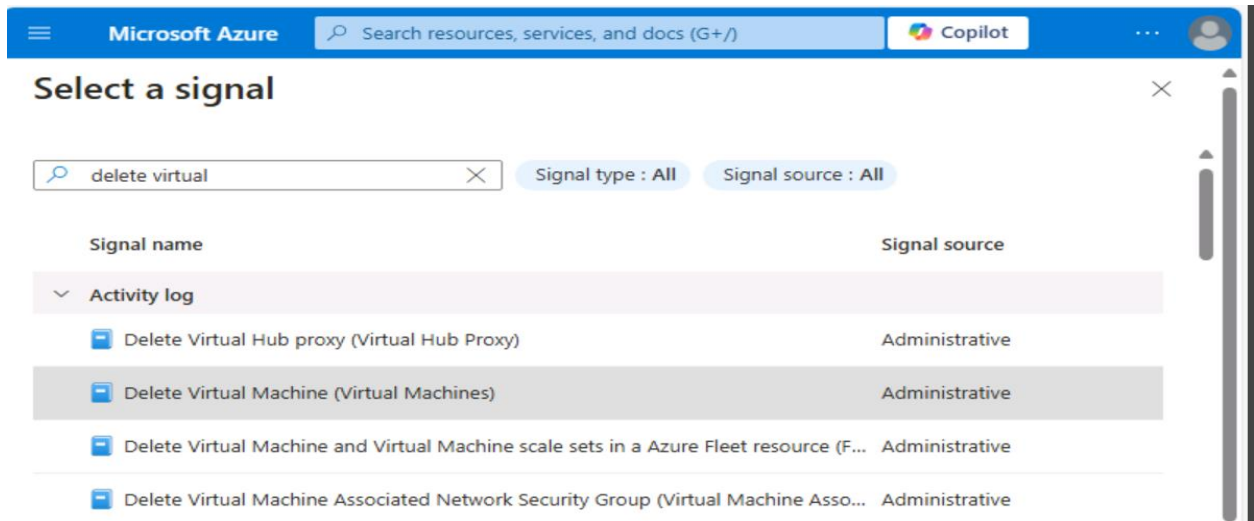
- Select Create + and select Alert rule.
- Select the box for the resource group, then select Apply. This alert will apply to any virtual machines in the resource group. Alternatively, you could just specify one particular machine.



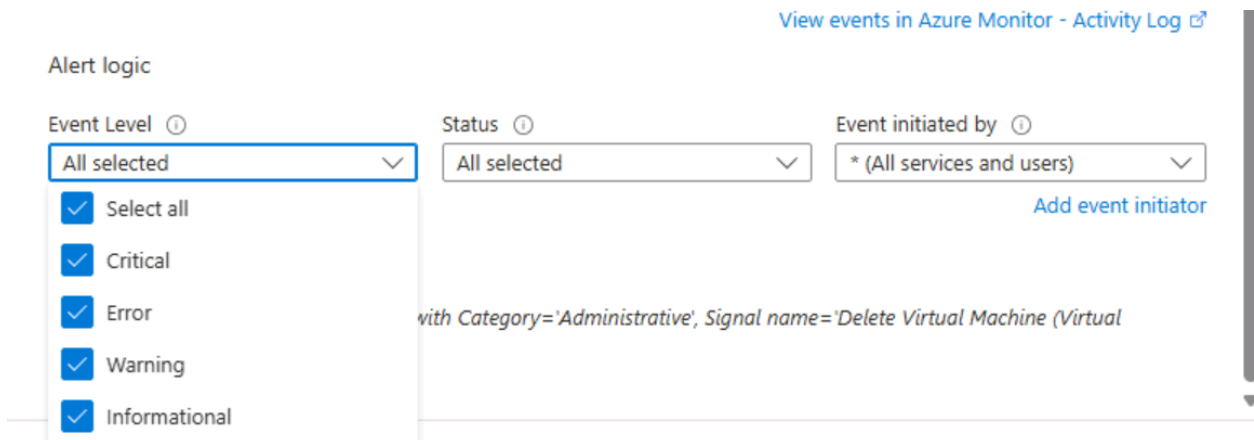
- Select the Condition tab and then select the See all signals link.



- Search for and select Delete Virtual Machine (Virtual Machines). Notice the other built-in signals. Select Apply



- In the Alert logic area (scroll down), review the Event level selections. Leave the default of All selected.



- Review the Status selections. Leave the default of All selected.
- Leave the Create an alert rule pane open for the next task.

Task 3: Configure action group notifications

In this task, if the alert is triggered send an email notification to the operations team.

- Continue working on your alert. Select Next: Actions, and then select Create action group.

Select action groups

Select up to five action groups to attach to this rule.

[+ Create action group](#)

Subscription ⓘ
MOC Subscription-lod49459474

[Search](#)

Action group name ↑↓	Resource group ↑↓	Contains actions	Location ↑↓
No results to display			

- On the Basics tab, enter the following values for each setting.

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ MOC Subscription-lod49459474

Resource group * ⓘ az104-rg11
[Create new](#)

Region * Global

Instance details

Action group name * ⓘ Alert the operations team ✓

Display name * ⓘ AlertOpsTeam ✓
The display name is limited to 12 characters

[Review + create](#) [Previous](#) [Next: Notifications](#)

- Select Next: Notifications and enter the following values for each setting.

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

- Select Email, and in the Email box, enter your email address, and then select OK.

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

Home > Monitor | Alerts >

Email/SMS message/Push/Voice

Add or edit Email/SMS message/Push/Voice action

Basics **Notifications**

Choose how to get notified

Notification type

Email/SMS message/Push/Voice

☒ Email

Email *

☐ SMS (Carrier charges may apply)

Country code

Phone number

☐ Azure mobile app notification

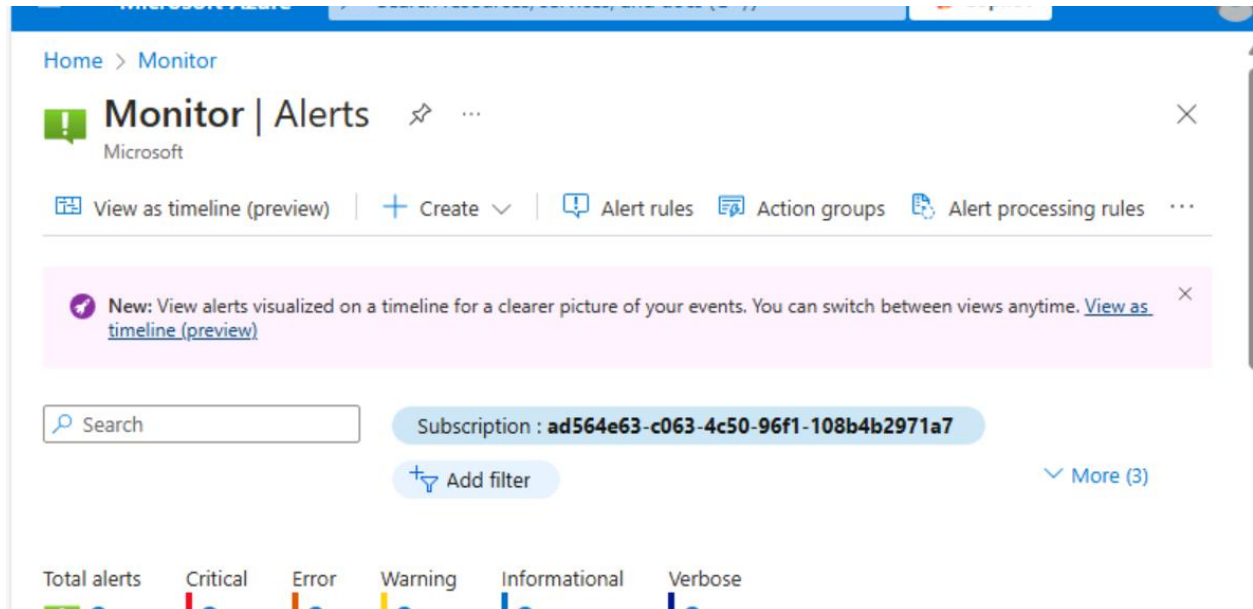
Azure account email

☐ Voice

Review + create

- Once the action group is created move to the Next: Details tab and enter the following values for each setting.

- Select Review + create to validate your input, then select Create.

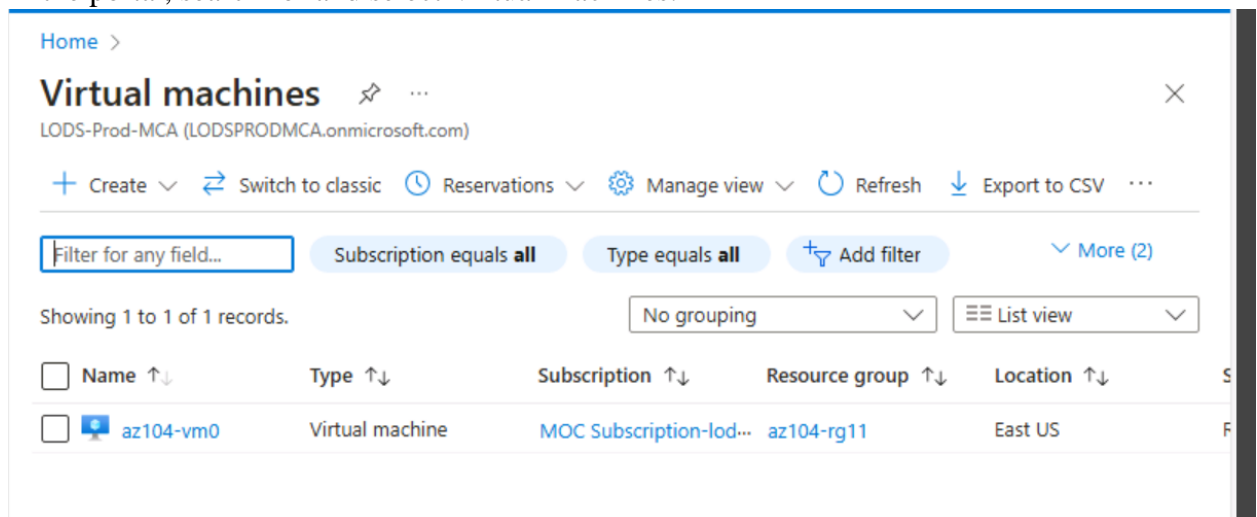


Task 4: Trigger an alert and confirm it is working

In this task, involves triggering the alert and confirming that a notification is sent .

Instructions

- In the portal, search for and select Virtual machines.



- Check the box for the az104-vm0 virtual machine.

<input checked="" type="checkbox"/>	Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	
<input checked="" type="checkbox"/>	az104-vm0	Virtual machine	MOC Subscription-lod...	az104-rg11	East US	F

- Select Delete from the menu bar.
- Check the box for Apply force delete. Enter delete to confirm and then select Delete.

Delete Resources

The selected resources along with their related resources and contents will be permanently deleted. If you are unsure of the selected resource dependencies, navigate to the individual resource page to perform the delete operation. More details of the resource dependencies are available in the manage experience.

Resources to be deleted (1)

Name	Resource type	
az104-vm0	Virtual machine	Remove

☒ Apply force delete for selected Virtual machines and Virtual machine scale sets ⓘ

Enter "delete" to confirm deletion *

delete

- In the title bar, select the Notifications icon and wait until vm0 is successfully deleted.

Virtual machines

LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.com)

[Create](#) [Switch to classic](#) [Reservations](#)

Subscription equals **all** [Add filter](#) [More \(3\)](#)

Showing 0 to 0 of 0 records. [No grouping](#)

Notifications

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

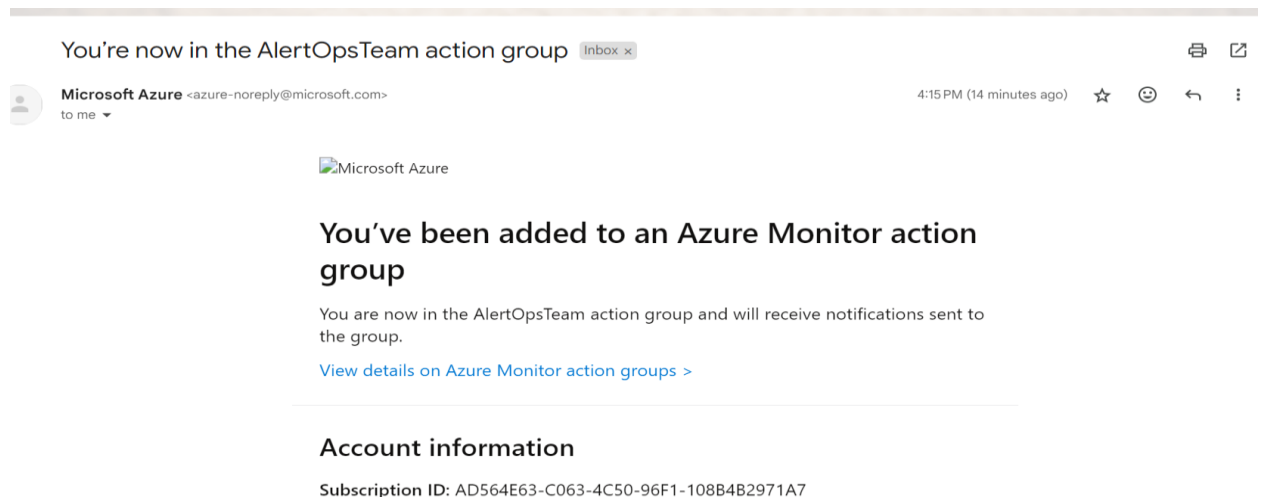
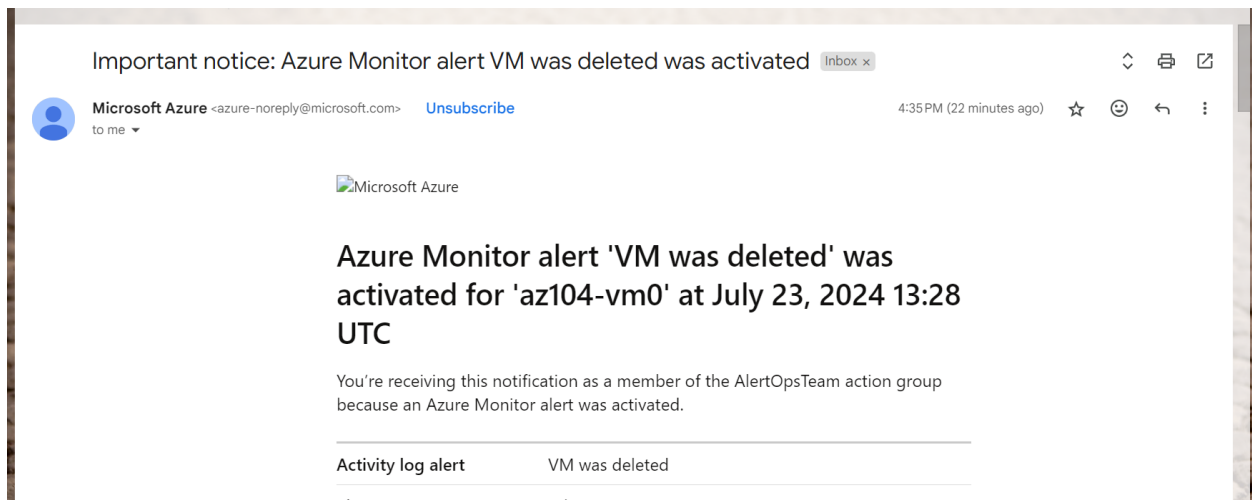
✓ Executed delete command on 1 selected items

Succeeded: 1, Failed: 0, Canceled: 0

a few seconds ago

Alert rule created

- You should receive a notification email that reads, Important notice: Azure Monitor alert VM was deleted was activated... If not, open your email program and look for an email from azure-noreply@microsoft.com



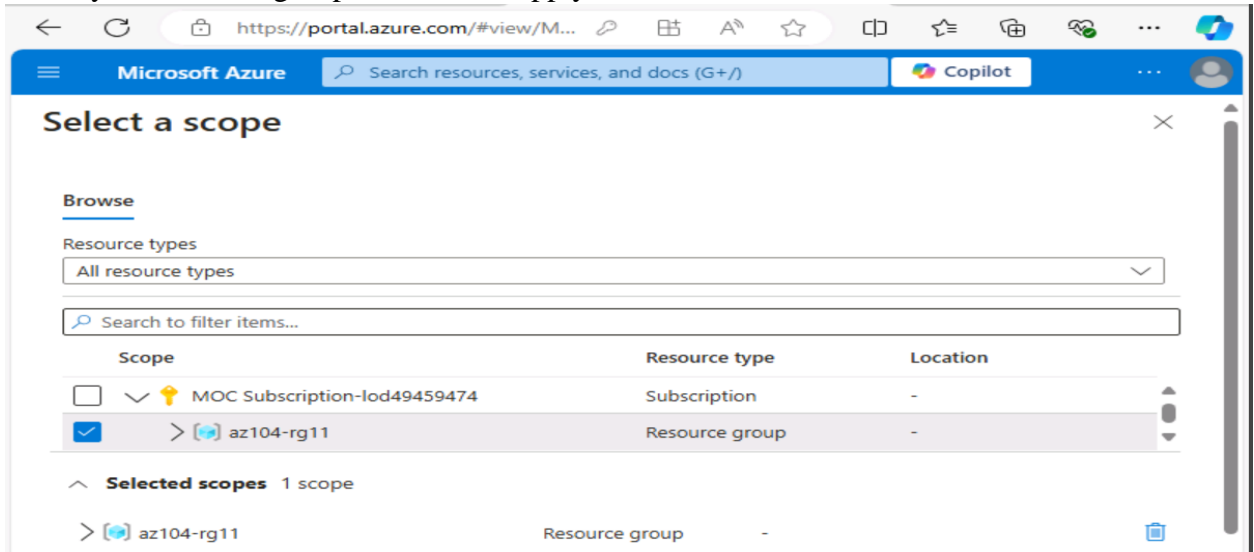
- On the Azure portal resource menu, select Monitor, and then select Alerts in the menu on the left.
- You should have three verbose alerts that were generated by deleting vm0.
- Select the name of one of the alerts (For example, VM was deleted). An Alert details pane appears that shows more details about the event.

Task 5: Configure an alert processing rule

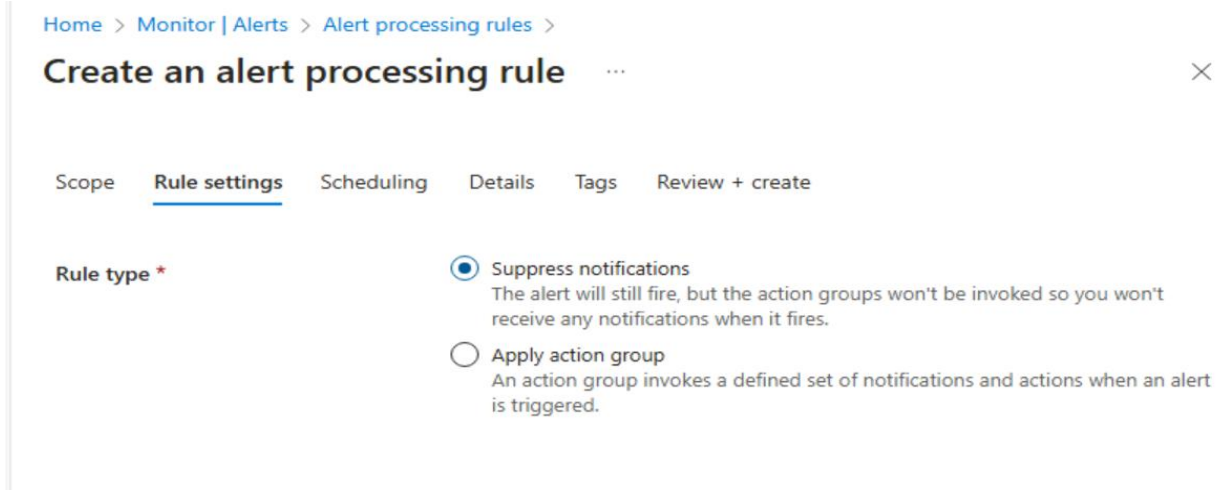
In this task, you create an alert rule to suppress notifications during a maintenance period.

Instructions

- Continue in the Alerts blade, select Alert processing rules and then + Create.
- Select your resource group, then select Apply.



- Select Next: Rule settings, then select Suppress notifications.



- Select Next: Scheduling.
- By default, the rule works all the time, unless you disable it or configure a schedule. You are going to define a rule to suppress notifications during overnight maintenance. Enter these settings for the scheduling of the alert processing rule:

Home > Monitor | Alerts > Alert processing rules >

Create an alert processing rule

Scope Rule settings **Scheduling** Details Tags Review + create

Define when you'd like to apply this rule.

Apply the rule

☐ Always
☒ At a specific time
☐ Recurring

Start
 End
 Time zone

Preview From 07/23/2024 at 10:00 PM to 07/24/2024 at 12:00 AM (UTC-08:00 Pacific Time)

- Select Next: Details and enter these settings:

Project details

Subscription
 Resource group [Create new](#)

Alert processing rule details

Rule name ☒
 Description
 Enable rule upon creation ☒

- Select Review + create to validate your input, then select Create.

Alert processing rules

[+ Create](#)
[Columns](#)
[Refresh](#)
[Open query](#)

[Add tag filter](#)

[More \(5\)](#)

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

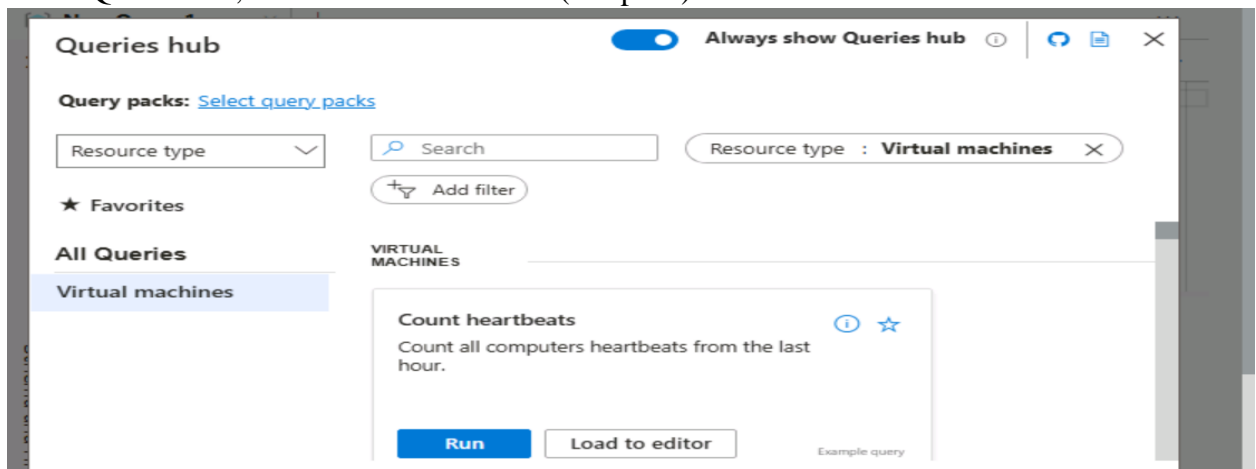
☒ **Create alert processing rule**
 Alert processing rule created successfully
 a few seconds ago

Task 6: Use Azure Monitor log queries

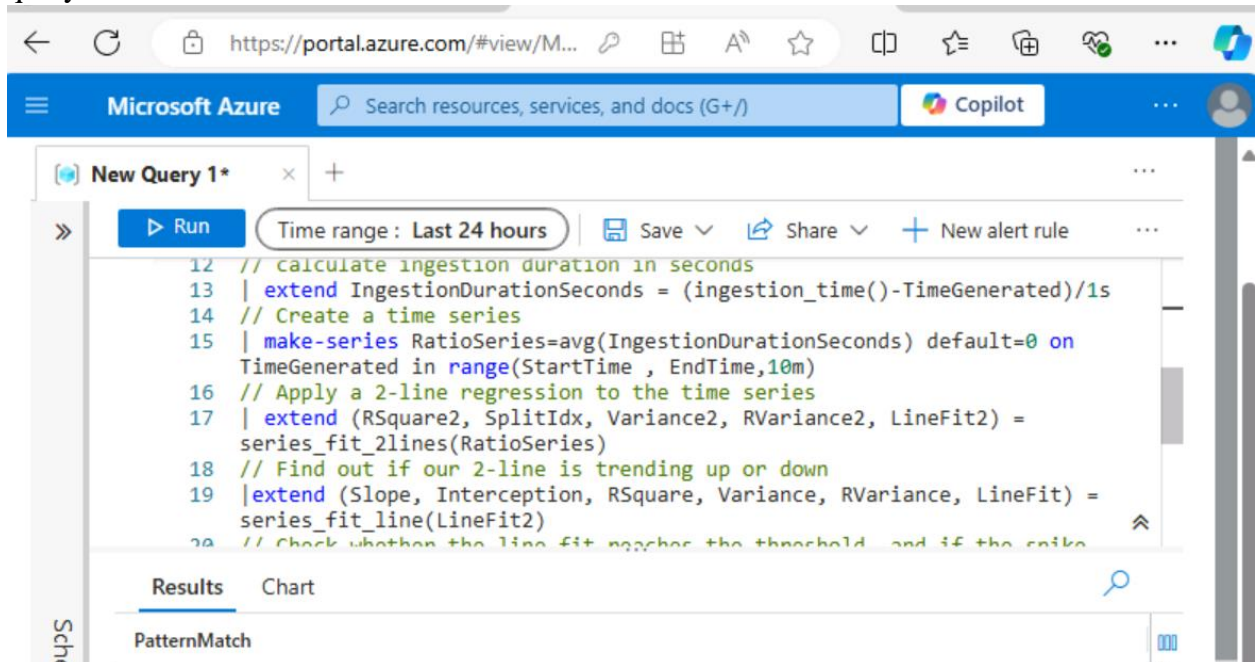
In this task, it involves using Azure Monitor to query the data captured from the virtual machine.

Instructions and steps to the configuration

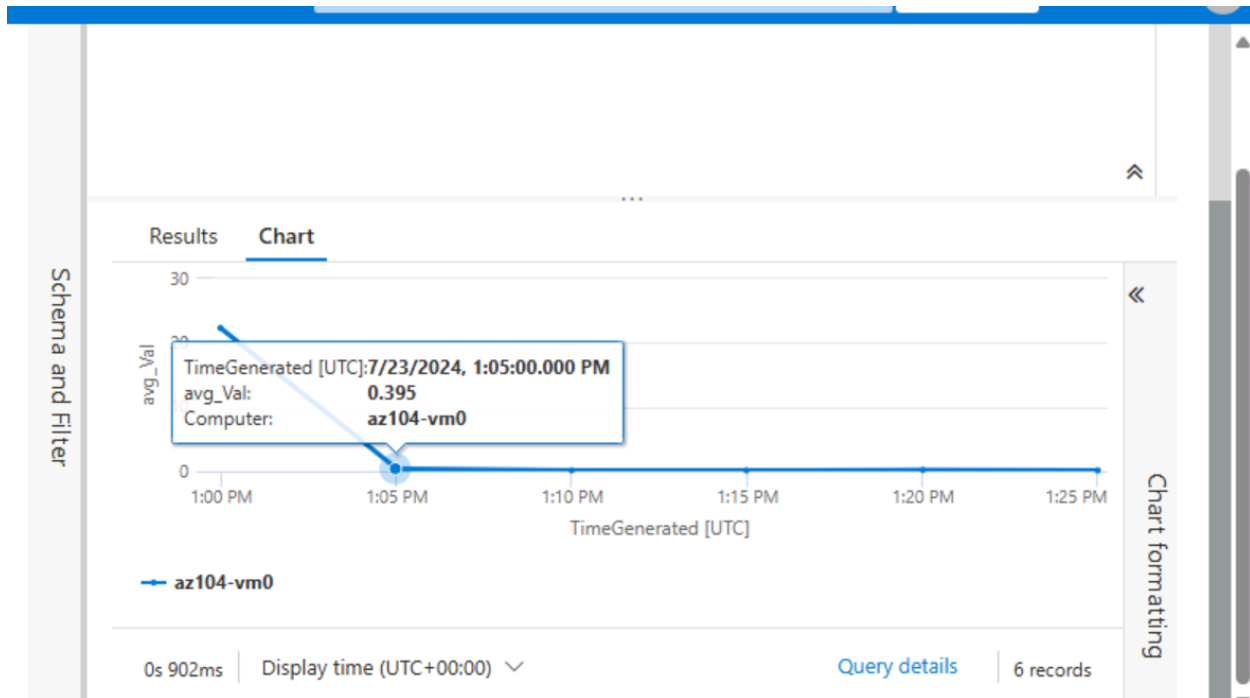
- In the Azure portal, search for and select Monitor blade, click Logs.
- If necessary close the splash screen.
- Select a scope, your resource group. Select Apply.
- In the Queries tab, select Virtual machines (left pane).



- Review the queries that are available. Run (hover over the query) the Count heartbeats query.



- You should receive a heartbeat count for when the virtual machine was running.
- Review the query. This query uses the heartbeat table.
- Replace the query with this one, and then click Run. Review the resulting chart.
- As you have time, review and run other queries.



Conclusion

In this lab assignment, I explored the capabilities of Azure for provisioning and managing cloud infrastructure through a series of practical tasks. Beginning with the use of templates, I efficiently deployed and configured infrastructure, which demonstrated the power of Infrastructure as Code (IaC) in creating repeatable and consistent environments. Creating alerts and configuring action group notifications allowed me to understand how Azure can proactively monitor resources and services, ensuring any issues are immediately flagged and addressed. By triggering alerts and confirming their functionality, I gained insights into how Azure's monitoring and alerting system can be effectively used to maintain the health and performance of applications.

Furthermore, configuring an alert processing rule provided hands-on experience with Azure's ability to automate responses to specific alerts, enhancing operational efficiency and reducing manual intervention. Finally, utilizing Azure Monitor log queries showcased the platform's capability in gathering and analyzing data, which is crucial for diagnosing problems, optimizing performance, and making informed decisions. Overall, these tasks provided a comprehensive overview of Azure's monitoring and alerting features, reinforcing the importance of effective cloud infrastructure management.

From these tasks, I learned several valuable lessons applicable to real-world scenarios. First, leveraging templates for infrastructure provisioning significantly enhances efficiency and accuracy, reducing the potential for human error and ensuring that environments are set up according to best practices. This skill is essential for any organization aiming to scale its operations in the cloud. Second, the importance of proactive monitoring and alerting cannot be overstated. By setting up alerts and configuring action groups, organizations can quickly identify and respond to potential issues, minimizing downtime and maintaining service reliability.

Additionally, the exercise of configuring alert processing rules highlighted the benefits of automating repetitive tasks and streamlining workflows, freeing up time for more strategic activities. Finally, the ability to effectively query and analyze logs is a critical skill for diagnosing issues and optimizing performance, enabling data-driven decision-making. Overall, these lessons underscore the significance of adopting robust cloud management practices and leveraging Azure's tools to ensure optimal performance and reliability in a dynamic and ever-evolving IT landscape.