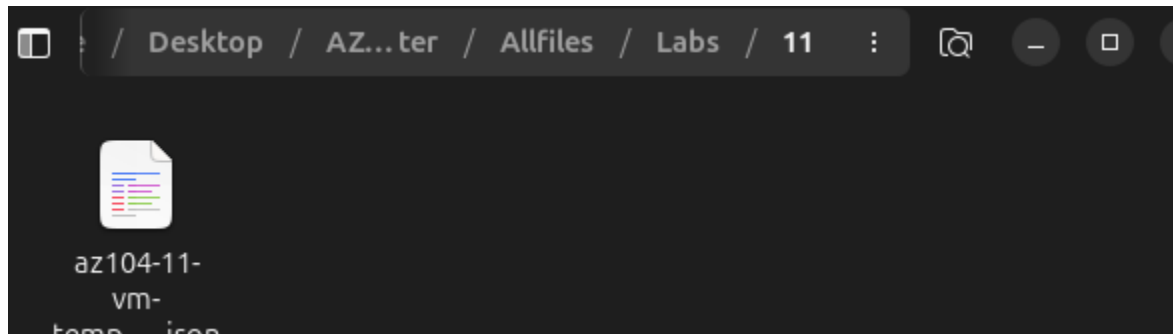


AZ-104-Microsoft Azure Administrator Kateryna Bakhmat

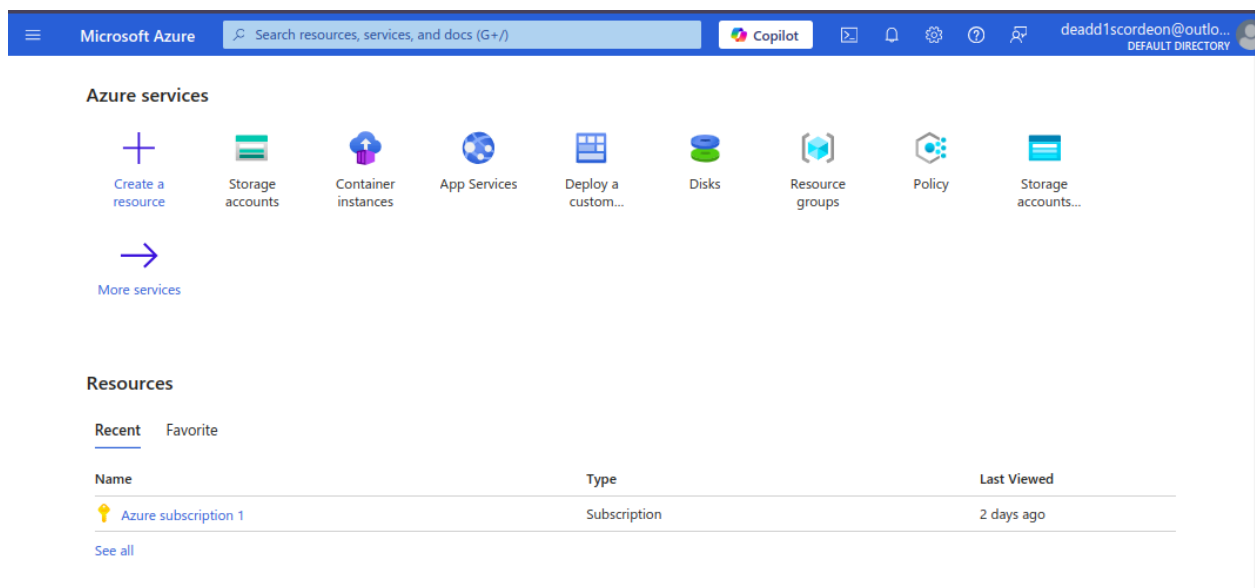
## Lab 11 - Implement Monitoring

Task 1: Use a template to provision an infrastructure

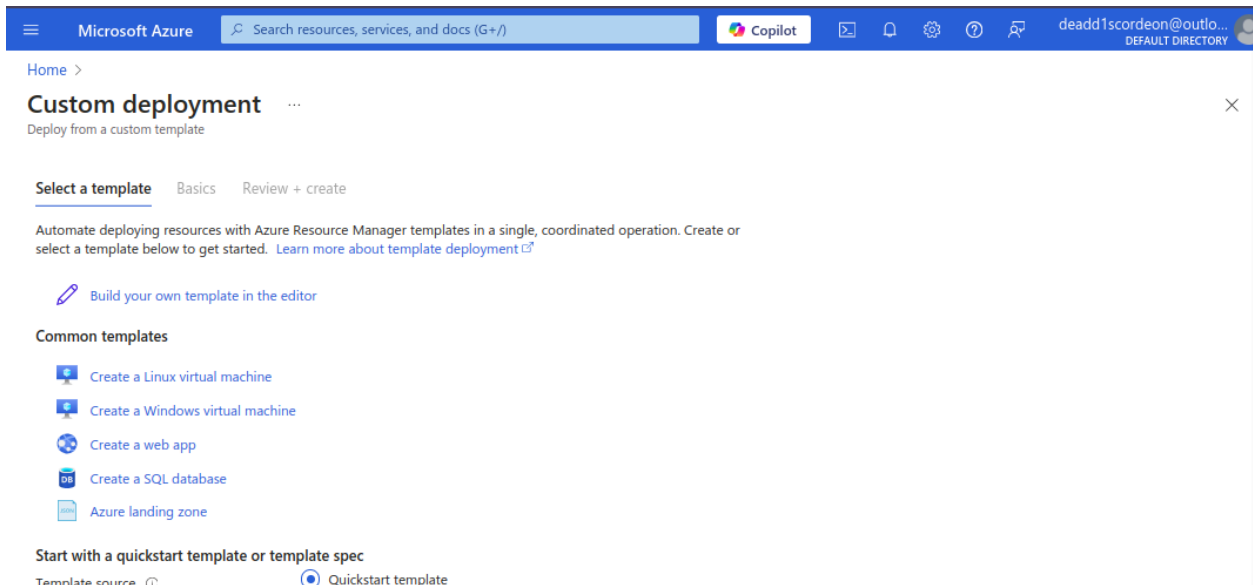
1.Download the \\Allfiles\\Lab11\\az104-11-vm-template.json lab files to your computer.



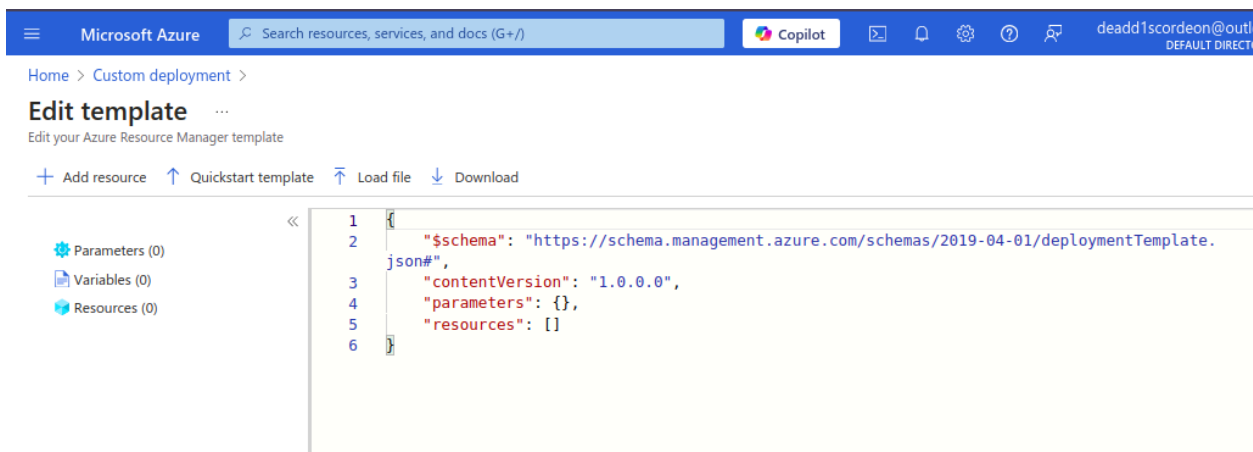
2.Sign in to the Azure portal - <https://portal.azure.com>.



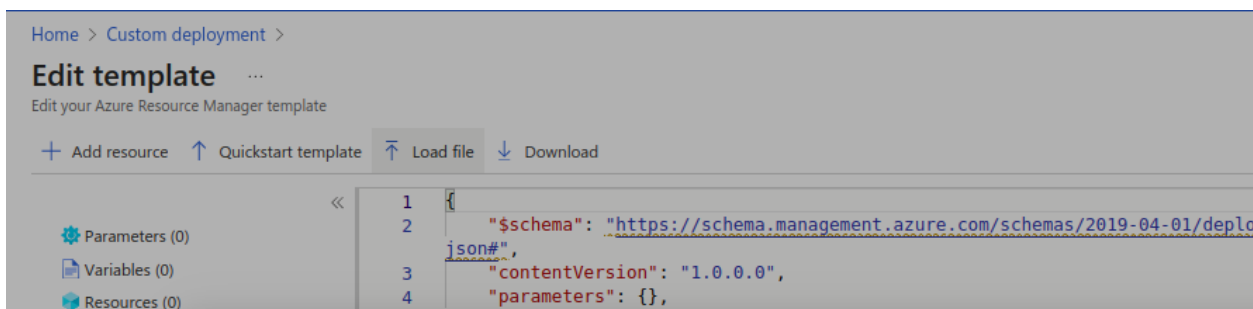
3.From the Azure portal, search for and select Deploy a custom template.



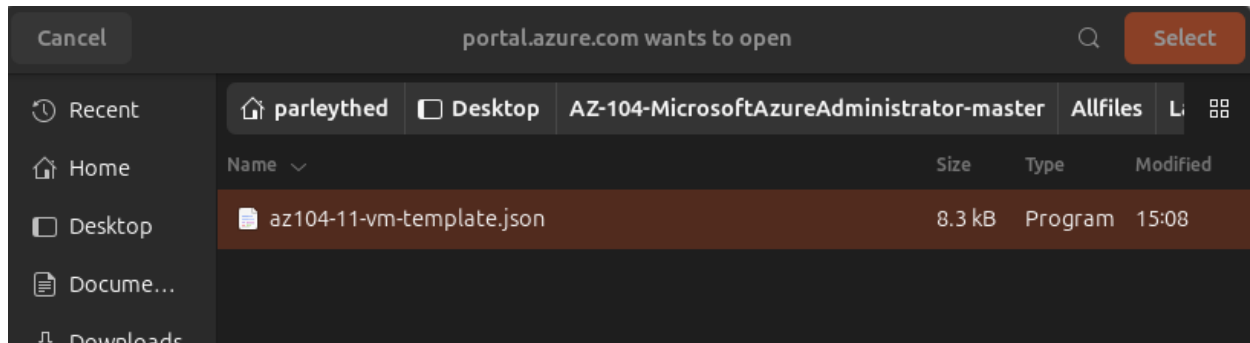
4. On the custom deployment page, select Build you own template in the editor.



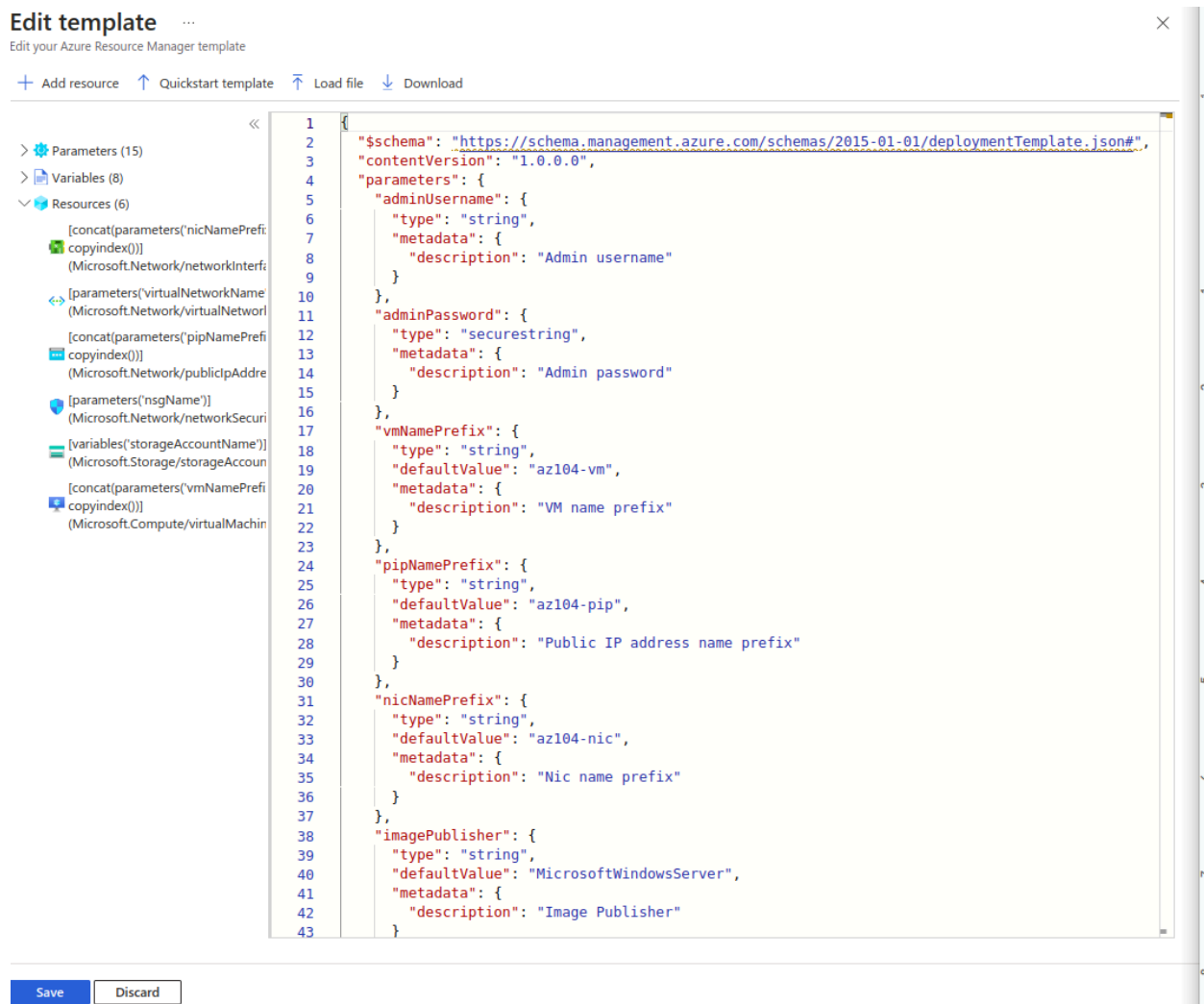
5. On the edit template page, select Load file.




6. Locate and select the \\Allfiles\\Labs11\\az104-11-vm-template.json file and select Open.



## 7. Select Save.



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

 New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template   **Basics**   Review + create

### Template



Customized template [↗](#)  
6 resources



Edit template



Edit parameters



Visualize

### Project details

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

Subscription \* ⓘ

Azure subscription 1



Resource group \* ⓘ

az104rg11



[Create new](#)

### Instance details

Region \* ⓘ

(Canada) Canada Central



Admin Username \* ⓘ

localadmin



Admin Password \* ⓘ

.....



Vm Name Prefix ⓘ

az104-vm



Pip Name Prefix ⓘ

az104-pip



Nic Name Prefix ⓘ

az104-nic



9. Select Review + Create, then select Create.

## Summary



Customized template  
6 resources

## Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

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	Azure subscription 1
Resource group	az104rg11
Region	Canada Central
Admin Username	localadmin
Admin Password	*****
Vm Name Prefix	az104-vm
Pip Name Prefix	az104-pip
Nic Name Prefix	az104-nic
Image Publisher	MicrosoftWindowsServer
Image Offer	WindowsServer

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

Microsoft Azure | Search resources, services, and users (0/7) | Copilot | DEFAULT DIRECTORY

Home >

## Microsoft.Template-20241024191514 | Overview

Deployment

Search x <<

Delete Cancel Redeploy Download Refresh

**Deployment succeeded** X  
Deployment 'Microsoft.Template-20241024191514' to resource group 'az104rg11' was successful.  
Pin to dashbo... Go to resource gr...

**Your deployment is complete**

Deployment name : Microsoft.Template-202... Start time : 10/24/2024, 7:15:23 PM  
Subscription : Azure subscription 1 Correlation ID : 08aaeeac-e761-48f7-81...  
Resource group : az104rg11

> Deployment details

> Next steps

Go to resource group

**Cost management**  
Get notified to stay within your budget and prevent unexpected charges on your bill.  
Set up cost alerts >

**Microsoft Defender for Cloud**

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

az104rg11 Resource group X

Search o <<

+ Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags ...

**Overview**

Activity log  
Access control (IAM)  
Tags  
Resource visualizer  
Events  
Settings  
Deployments  
Security  
Deployment stacks  
Policies  
Properties  
Locks  
Cost Management  
Monitoring  
Automation  
Help

**Essentials** JSON View

Subscription (move) Azure subscription 1  
Subscription ID f80303f7-6763-4988-a828-9a2836f89e14  
Deployments 1 Failed, 1 Succeeded  
Location Canada Central  
Tags (edit) Add tags

**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_55ba8b39d4eb400a94d446f5ca19041b	Disk	Canada Central
az104-vnet	Virtual network	Canada Central
az10411it6satpi4kup6	Storage account	Canada Central

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

1. In the portal, search for and select Monitor.

**Monitor | Overview** Microsoft

Search

**Overview**

- Activity log
- Alerts
- Metrics
- Logs
- Change Analysis
- Service health
- Workbooks
- Investigator (preview)
- > Insights
- > Managed Services
- > Settings
- > Support + Troubleshooting

**Overview** Tutorials

### Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

**Application insights**

Monitor your app's availability, performance, errors, and usage.

[View](#) [More](#)

**Container Insights**

Gain visibility into the performance and health of your controllers, nodes, and containers.

[View](#) [More](#)

**VM Insights**

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

[View](#) [More](#)

**Network Insights**

View the health and metrics for all deployed network resources.

[View](#) [More](#)

2. Take a minute to review all the insights, detection, triage, and diagnosis tools that are available.

### Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

**Application insights**

Monitor your app's availability, performance, errors, and usage.

[View](#) [More](#)

**Container Insights**

Gain visibility into the performance and health of your controllers, nodes, and containers.

[View](#) [More](#)

**VM Insights**

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

[View](#) [More](#)

**Network Insights**

View the health and metrics for all deployed network resources.

[View](#) [More](#)

### Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. [Learn more about monitoring](#)

**Metrics**

Create charts to monitor and investigate the usage and performance of your Azure resources.

[View](#) [More](#)

**Alerts**

Get notified and respond using alerts and actions.

[View](#) [More](#)

**Logs**

Analyze and diagnose issues with log queries.

[View](#) [More](#)

**Workbooks**

View, create and share interactive reports.

[View](#) [More](#)

**Change Analysis**

Investigate what changed to triage incidents.

[View](#) [More](#)

**Diagnostic Settings**

Route monitoring metrics and logs to selected locations.

[View](#) [More](#)

**Azure Monitor SCOM managed instance**

SCOM managed instance monitors workloads running on cloud and on-prem.


[View](#) [More](#)



**Managed Prometheus**


Collect Prometheus metrics from your containerized workloads to monitor their health and performance.

[View](#) [More](#)



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


**VM Insights**  
 Monitor the health, performance, and dependencies of your VMs and VM scale sets.

 View
  More


**VM Insights View**  
 Network Insights

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






 Refresh
  Provide Feedback

Get started
 **Overview**
 Performance
 Map

Subscription : **Azure subscription 1**
Resource group : **All resource groups**
Type : **All types**

Location : **All locations**
Group by : **Subscription, Resource group**

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

Name	Monitor Coverage	Workspace
  Azure subscription 1	1 of 1	
  az104rg11	1 of 1	
 az104-vm0	Not enabled	<div>Enable</div>



## 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.



**i** 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

5. 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 \*

Azure subscription 1

Data collection rule ⓘ

(new) MSVMI-DefaultWorkspace-f80303f7-6763-4988-a828-9a2836f89e14-EUS

[Create New](#)

**MSVMI-DefaultWorkspace-f80303f7-6763-4988-a828-9a2836f89e14-EUS**

Guest performance Enabled

Processes and dependencies (Map) Disabled

Log Analytics workspace DefaultWorkspace-f80303f7-6763-4988-a828-9a2836f89e14-EUS

**i** This will also enable System Assigned Managed Identity, in addition to existing User Assigned identities (if any).  
**Note:** Unless specified in the request, the machine will default to using System Assigned Identity. [Learn More](#)

Currently, only resources in certain regions are supported. [Learn More](#)

Configure

Cancel

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

\*\*\* Submitting deployment...

Submitting the deployment template for resource group 'az104rg11'.

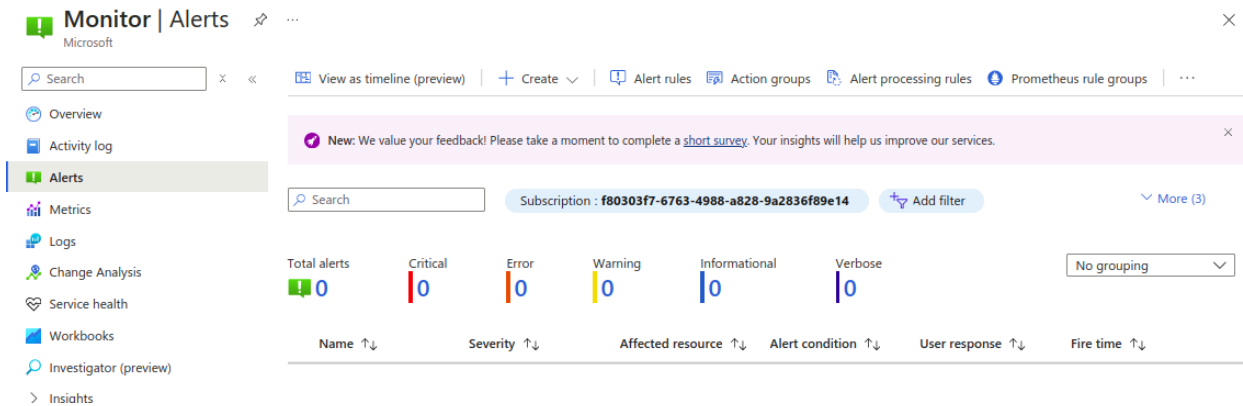
\*\*\* Initializing deployment...

Initializing template deployment to resource group 'az104rg11'.

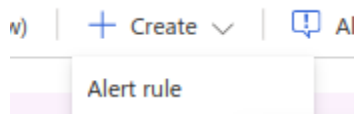
... of your virtual machine

## Task 2: Create an alert

1. Continue on the Monitor page, select Alerts.



2. Select Create + and select Alert rule.



3. 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 a resource

×

BrowseRecent

Resource types

All resource types

Locations

All locations

Search to filter items...

Resource	Resource type	Location
<input type="checkbox"/> Azure subscription 1	Subscription	-
<input type="checkbox"/> > az104-rg11	Resource group	-
<input type="checkbox"/> > az104-rg6	Resource group	-
<input checked="" type="checkbox"/> > az104rg11	Resource group	-
<input type="checkbox"/> > DefaultResourceGroup-EUS	Resource group	-

ⓘ

Metric and Log signals might not be available if the scope includes multiple resources.

Refine scope

Resource type

Select a resource type

Location

Select a location

^ Selected resources 1 scope

> az104rg11

Resource group

-

🗑️

Apply

Cancel

Clear all selections

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

Home > Monitor | Alerts >

Create an alert rule

Scope

Condition

Actions

Details

Tags

Review

Configure when the alert rule should trigger by selecting a signal and

Signal name \*

Select a signal

See all signals

Select a signal

Search by signal name

Signal type :

Signal name

Log search

Custom log search

Resource health

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

## Select a signal



Delete Virtual Machine (Virtual Machines) X

Signal type : All

Signal source : All

Signal name	Signal source
Activity log	
Delete Virtual Machine (Virtual Machines)	Administrative

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

Alert logic

Event Level ⓘ  
All selected ▼  
☒ Select all  
☒ Critical  
☒ Error  
☒ Warning  
☒ Informational  
☒ Verbose

Status ⓘ  
All selected ▼

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

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

Review + create

Previous

Next: Actions >

7. Review the Status selections. Leave the default of All selected.

Alert logic

Event Level ⓘ  
All selected ▼

Status ⓘ  
All selected ▼  
☒ Select all  
☒ Failed  
☒ Started  
☒ Succeeded

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 >

8. Leave the Create an alert rule pane open for the next task.

### Task 3: Configure action group notifications

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

The screenshot shows the 'Create an alert rule' page in the Azure portal. The 'Actions' tab is selected, and the 'Select action groups' dialog is open. The dialog prompts the user to 'Select up to five action groups to attach to this rule.' and includes a '+ Create action group' button. Below this, there is a search bar and a table with columns for 'Action group name', 'Resource group', and 'Contains actions'. The table currently shows 'No results to display'. On the left side of the dialog, there are radio buttons for 'Use quick actions (p)', 'Use action groups', and 'None'. The 'Use action groups' option is selected.

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

The screenshot shows the 'Basics' tab of the 'Create an alert rule' page. The 'Project details' section includes a 'Subscription' dropdown set to 'Azure subscription 1', a 'Resource group' dropdown set to 'az104rg11' with a 'Create new' link below it, and a 'Region' dropdown set to 'Global'. The 'Instance details' section includes an 'Action group name' field set to 'Alert the operations team' and a 'Display name' field set to 'AlertOpsTeam'. Both fields in the 'Instance details' section have a green checkmark icon to their right. A note at the bottom states 'The display name is limited to 12 characters'.

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

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	
Please configure the notification by clicking the edit button.		
▼		

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

### Email/SMS message/Push/Voice

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

☒ Email

Email \* ⓘ deadd1scordeon@outlook.com ✓

---

✔ Create action group ✕

Action group created successfully

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

Scope   Condition   Actions   Details   Tags   Review + create

#### Project details

Select the subscription and resource group in which to save the alert rule.

Subscription ⓘ	<div>Azure subscription 1</div>
Resource group * ⓘ	<div>az104rg11</div> <div><a href="#">Create new</a></div>
Region * ⓘ	<div>Global</div>

#### Alert rule details

Alert rule name * ⓘ	<div>VM was deleted</div>
Alert rule description ⓘ	<div>A VM in your resource group was deleted</div>

⌵ Advanced options

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



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

[Home](#) > [Monitor | Alerts](#) >

## Create an alert rule ...

Scope

Condition

Actions

Details

Tags

Review + create

### Scope

Resource

Azure subscription 1 > az104rg11

### 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	Azure subscription 1
Resource group	az104rg11
Region	global

Create

Previous

✓ Alert rule created

×

Alert rule VM was deleted successfully created. It might take a few minutes for changes to be shown.

Task 4: Trigger an alert and confirm it is working

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

## Virtual machines

Default Directory (deadd1scoredonoutlook.onmicrosoft.com)

[+](#) Create [↔](#) Switch to classic [🕒](#) Reservations [⚙️](#) Manage view [🔄](#) Refresh [↓](#) Export to CSV


Filter for any field...

Subscription equals all

Type equals all

Resource group equals all [✕](#)

Showing 1 to 1 of 1 records.

<input type="checkbox"/>	Name ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/>	 az104-vm0	Azure subscription 1	az104rg11	Canada Central

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

[Home](#) > [Virtual machines](#) >

 **az104-vm0** [🔖](#) [★](#) [⋮](#)  
Virtual machine

[🔗](#) Connect [▶](#) Start [🔄](#) Restart ☐ Stop [🕒](#) Hibernate [📦](#) Capture [🗑️](#) Delete [🔄](#) Re

[🖥️](#) Overview

[📋](#) Activity log

[^](#) Essentials

Delete

3. Select Delete from the menu bar.

[🕒](#) Hibernate [📦](#) Capture [🗑️](#) Delete [🔄](#) Re  
Delete

4. Check the box for Apply force delete. Enter delete to confirm and then select Delete.

## Delete az104-vm0






This action will permanently delete this virtual machine.

Resource to be deleted	Resource type
 az104-vm0	Virtual machine

☒ Apply force delete ⓘ

ⓘ This virtual machine can be safely force deleted because all of its associated resources are being deleted.

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 checked="" type="checkbox"/>
>  Network interfaces	1	<input checked="" type="checkbox"/>
>  Public IP addresses	1	<input checked="" type="checkbox"/>

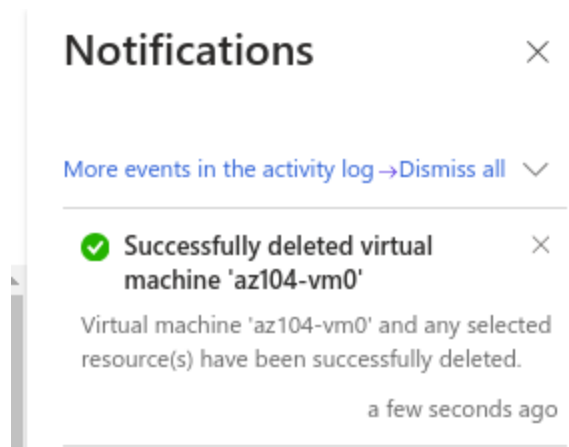
☒ I have read and understand that this virtual machine as well as any selected associated resources listed above will be deleted.

Delete

Cancel

 Feedback

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



6. 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](mailto:azure-noreply@microsoft.com).

## Azure Monitor alert 'VM was deleted' was activated for 'az104-vm0' at October 24, 2024 16:45 UTC

You're receiving this notification as a member of the AlertOpsTeam action group because an Azure Monitor alert was activated.

Activity log alert	VM was deleted
Time	October 24, 2024 16:45 UTC
Category	Administrative
Operation name	Microsoft.Compute/virtualMachines/delete
Correlation ID	052bb3be-0010-47c3-b4ce-5a9fd6270437
Level	Informational
Resource ID	/subscriptions/f80303f7-6763-4988-a828-9a2836f89e14/resourceGroups/az104rg11/providers/Microsoft.Compute/virtualMachines/az104-vm0
Caller	deadd1scoreon@outlook.com
Properties	<pre>{"statusCode": "Accepted", "serviceRequestId": null, "eventCategory": "Administrative", "entity": "/subscriptions/f80303f7-6763-4988-a828-9a2836f89e14/resourceGroups/az104rg11/providers/Microsoft.Compute/virtualMachines/az104-vm0", "message": "Microsoft.Compute/virtualMachines/delete", "hierarchy": "a91ad3f2-839c-4e1b-b0e8-0c2e83334265/f80303f7-6763-4988-a828-9a2836f89e14"}</pre>

[View in Azure portal >](#)[Investigate >](#)

7. On the Azure portal resource menu, select Monitor, and then select Alerts in the menu on the left.

[View as timeline \(preview\)](#) | [+ Create](#) | [Alert rules](#) | [Action groups](#) | [Alert processing rules](#) | [Prometheus rule groups](#) | ...

New: We value your feedback! Please take a moment to complete a [short survey](#). Your insights will help us improve our services.

Subscription : **f80303f7-6763-4988-a828-9a2836f89e14**

[Add filter](#)

[More \(3\)](#)

Total alerts  
**3**

Critical  
**0**

Error  
**0**

Warning  
**0**

Informational  
**0**

Verbose  
**3**

No grouping

Name ↑↓	Severity ↑↓	Affected resource ↑↓	Alert condition ↑↓	User response ↑↓	Fire time ↑↓	
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New	10/24/2024, 7:52 PM	***
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New	10/24/2024, 7:52 PM	***
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New	10/24/2024, 7:52 PM	***

8.You should have three verbose alerts that were generated by deleting vm0.

Total alerts  
**3**

Critical  
**0**

Error  
**0**

Warning  
**0**

Informational  
**0**

Verbose  
**3**

No grouping

Name ↑↓	Severity ↑↓	Affected resource ↑↓	Alert condition ↑↓	User response ↑↓
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New
<input type="checkbox"/> VM was deleted	4 - Verbose	az104-vm0	Fired	New

9.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.

...

View as timeline (preview) | + Create | Alert rules

New: We value your feedback! Please take a moment to complete a [short survey](#).

Search

Subscription: **Azure subscription**

Total alerts: 3 | Critical: 0 | Error: 0 | Warning: 0 | Info: 0

Name ↑↓	Severity ↑↓
<input type="checkbox"/> VM was deleted	4 - Verbose
<input type="checkbox"/> VM was deleted	4 - Verbose
<input type="checkbox"/> VM was deleted	4 - Verbose

### VM was deleted

Activity log alert details

Copy link | Go to alert rule | Investigate (preview)

Summary | History

General details

Severity	Fired time	Affected resource	Monitor service	Alert condition	User response
4 - Verbose	10/24/2024, 7:52 PM	az104-vm0	ActivityLog Administrative	Fired	New

Why did this alert fire?

The following event occurred: Microsoft.Compute/virtualMachines/delete

Event level	Category	Initiated by
Informational	Administrative	deadd1scoredeon@outlook.c

> Additional details

## Task 5: Configure an alert processing rule

1. Continue in the Alerts blade, select Alert processing rules and then + Create.

rules | Action groups | Alert processing rules | ...

Alert processing rules

te a [short survey](#). Your insights will help us improve our services.

Home > Monitor | Alerts >

### Alert processing rules

+ Create | Columns | Refresh | Open query | Delete | Enable | Disable

Search

Subscription: **Azure subscription 1** | Resource group: **all** | Target scope: **all** | Add tag filter

Name ↑↓	Scope	Filter	Rule type ↑↓	Scheduling	Status ↑
---------	-------	--------	--------------	------------	----------

2. Select your resource group, then select Apply.

## Select a scope

### Browse

Resource types

All resource types

Search to filter items...

Scope	Resource type	Location
<input type="checkbox"/> Azure subscription 1	Subscription	-
<input type="checkbox"/> > az104-rg11	Resource group	-
<input type="checkbox"/> > az104-rg6	Resource group	-
<input checked="" type="checkbox"/> > az104rg11	Resource group	-

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

Scope Rule settings Scheduling Details Tags Review + create

Rule type \*

- ☒ Suppress notifications  
The alert will still fire, but the action groups won't be invoked so you won't receive any notifications when it fires.
- ☐ Apply action group  
An action group invokes a defined set of notifications and actions when an alert is triggered.

4. Select Next: Scheduling.

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

5. 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:



Define when you'd like to apply this rule.

Apply the rule

- ☐ Always
- ☒ At a specific time
- ☐ Recurring

Start

End

Time zone

Preview From 10/24/2024 at 10:00 PM to 10/25/2024 at 7:00 AM (UTC+02:00 Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)

## 6. Select Next: Details and enter these settings:

Project details

Subscription

Resource group

[Create new](#)

Alert processing rule details

Rule name

Description

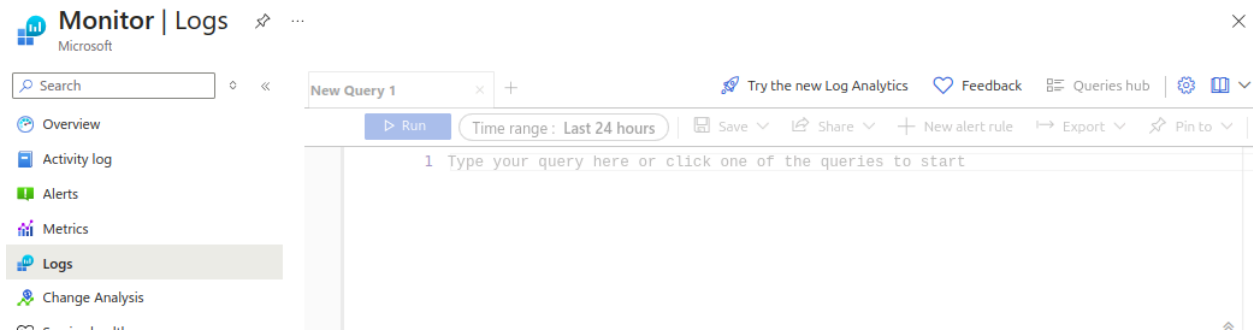
Enable rule upon creation ☒

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

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

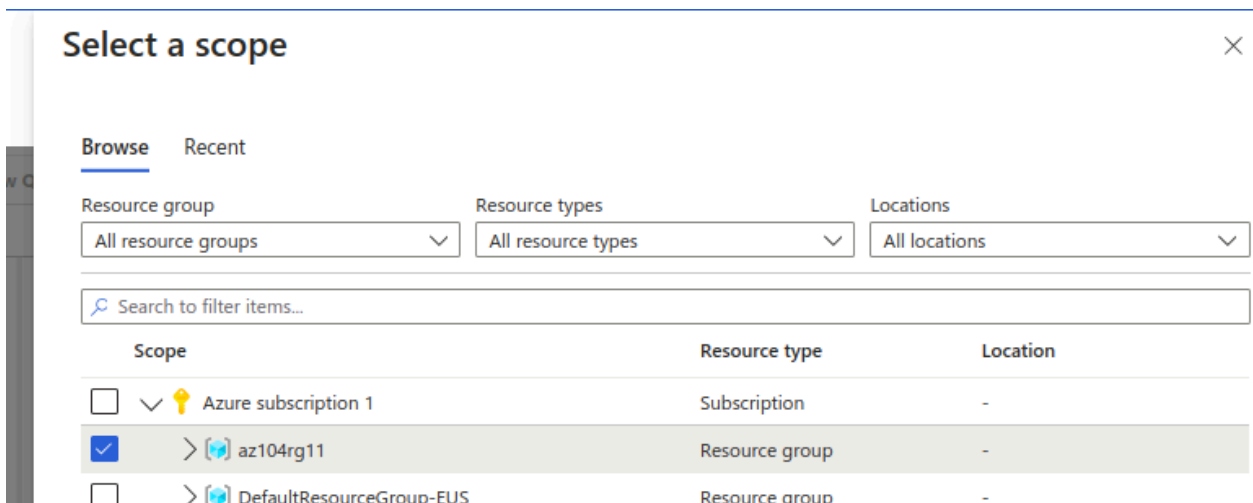
## Task 6: Use Azure Monitor log queries

### 1. In the Azure portal, search for and select Monitor blade, click Logs.

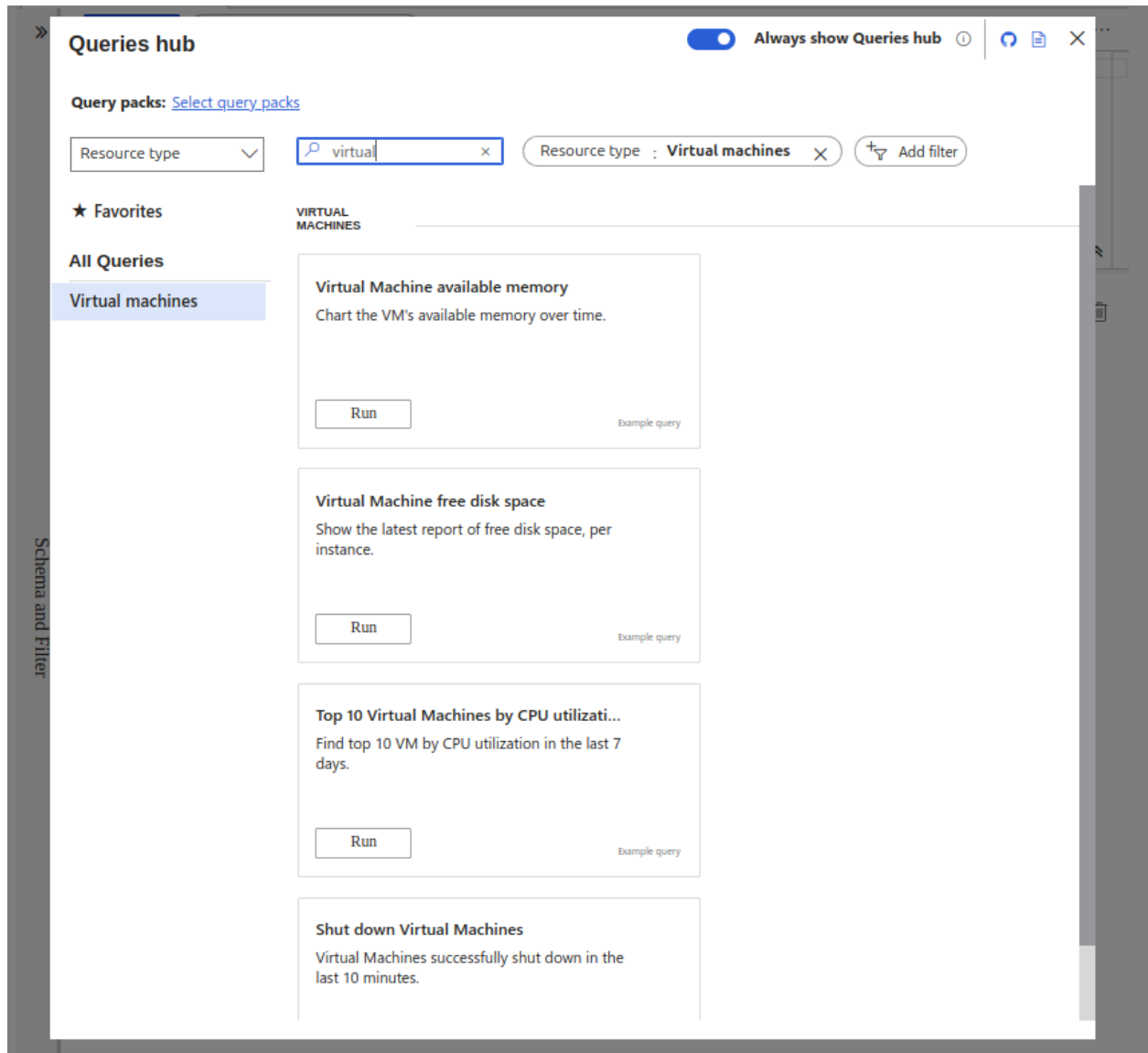


2.If necessary close the splash screen.

3.Select a scope, your resource group. Select Apply.



4.In the Queries tab, select Virtual machines (left pane).



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

**Queries hub** Always show Queries hub

Query packs: [Select query packs](#)

Resource type ▼ Search Resource type : Virtual machines × Add filter

★ Favorites

All Queries

Virtual machines

**VIRTUAL MACHINES**

**Count heartbeats**

Count all computers heartbeats from the last hour.

Run Example query

6. You should receive a heartbeat count for when the virtual machine was running.

Run Time range : Set in query Save Share New alert rule Export Pin to

```

1 // Count heartbeats
2 // Count all computers heartbeats from the last hour.
3 // Count computers heartbeats in the last hour.
4 // Normally, agents on VMs generate Heartbeat event every minute.
5 Heartbeat
6 | where TimeGenerated > ago(1h)
7 | summarize count() by Computer

```

Results Chart

Computer	count_
> az104-vm0	23

7. Review the query. This query uses the heartbeat table.

The screenshot displays the Azure Log Analytics query editor interface. At the top, there's a tab labeled "New Query 1\*" and a button to "Try the new Log Analytics". Below the tab, there's a "Run" button and a "Time range: Set in query" dropdown. The query editor contains the following Kusto query:

```
1 // Count heartbeats
2 // Count all computers heartbeats from the last hour.
3 // Count computers heartbeats in the last hour.
4 // Normally, agents on VMs generate Heartbeat event every m
5 Heartbeat
6 | where TimeGenerated > ago(1h)
7 | summarize count() by Computer
```

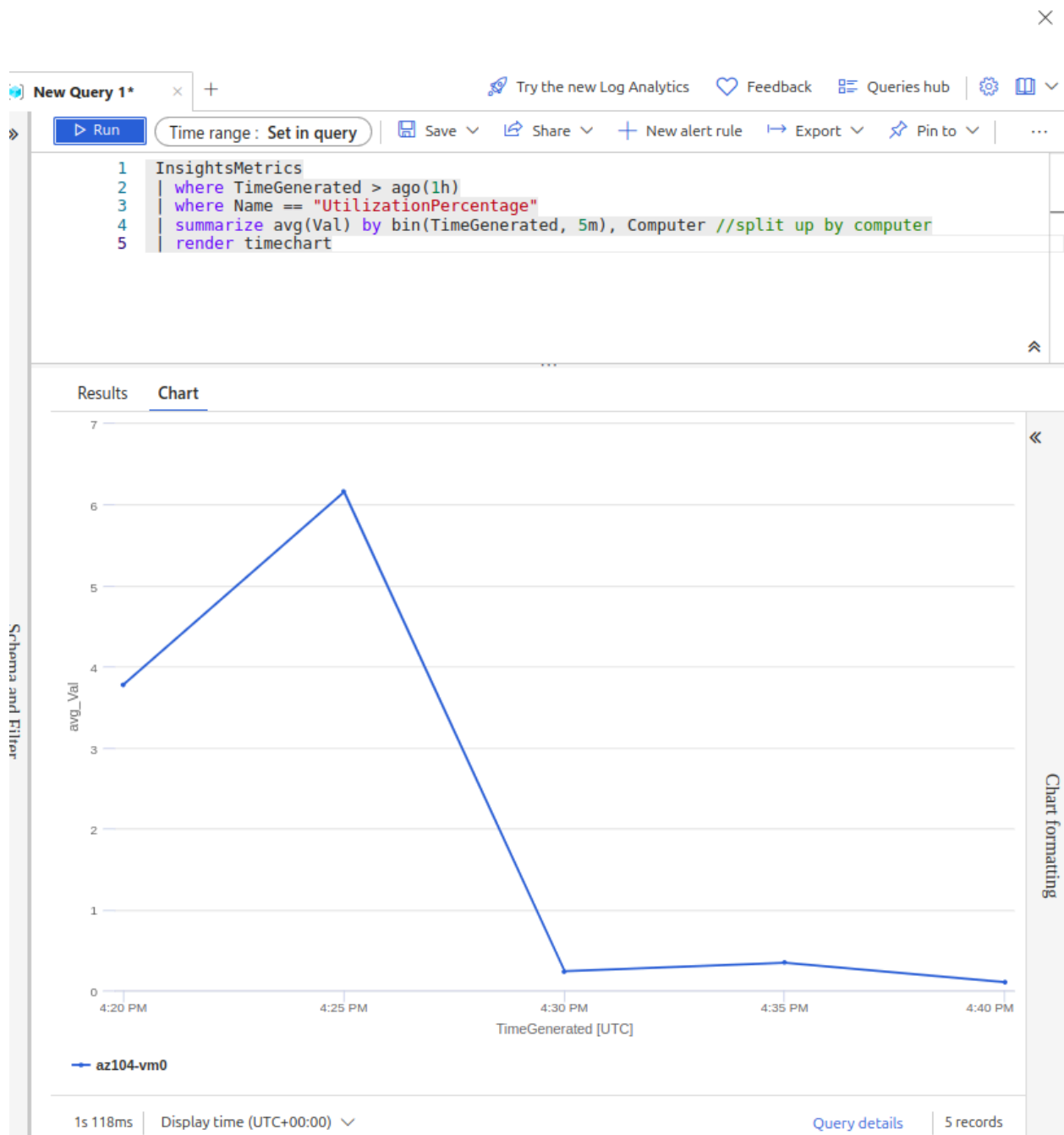
Below the query editor, there are two tabs: "Results" and "Chart". The "Results" tab is active, showing a table with two columns: "Computer" and "count\_". The table contains one row of data:

Computer	count_
> az104-vm0	23

On the right side of the interface, there's a sidebar with various metrics and settings:

- Total CPU: 187 Milliseconds
- Time span of the processed query: Less than a day
- Age of processed data: Less than a day
- Number of workspaces: 1
- Number of regions: 1
- Parallelism: N/A
- Request ID: 1083fbbb-5c29-4b1a-99a5-e4aec139b9...

8. Replace the query with this one, and then click Run. Review the resulting chart.



9.As you have time, review and run other queries.

Memory usage: 283 MB



New Query 1\* x +

Try the new Log Analytics Feedback Queries hub

Run Time range: Last 24 hours Save Share + New alert rule Export Pin to ...

```
1 // Virtual Machine free disk space
2 // Show the latest report of free disk space, per instance.
3 // To create an alert for this query, click '+ New alert rule'
4 Perf
5 | where ObjectName == "LogicalDisk" or // the object name used in Windows records
6   ObjectName == "Logical Disk" // the object name used in Linux records
7 | where CounterName == "Free Megabytes"
8 | summarize arg_max(TimeGenerated, *) by InstanceName // arg_max over TimeGenerated
   returns the latest record
9 | project TimeGenerated, InstanceName, CounterValue, Computer, _ResourceId
```

Results Chart

No results found from the last 24 hours  
Try [selecting another time range](#)