

Secure Azure VM with RBAC, NSG, Backup & Monitoring

Objective

The objective of this project is to deploy a single-tier Azure Virtual Machine with complete governance, security, backup, and monitoring configurations aligned with AZ-104 core domains. This implementation focuses on establishing enterprise-grade practices for managing identity, networking, backup, and monitoring of Azure resources to ensure compliance, security, and high availability.

Tools & Technologies Used

- Microsoft Azure Portal (Azure pay as-you-go account)
- Windows Server Virtual Machine
- Azure Resource Manager (ARM)
- Network Security Group (NSG)
- Azure Backup Vault and Restore Points
- Azure Monitor, Log Analytics Workspace & Alerts
- Azure Role-Based Access Control (RBAC)
- Azure Locks and Tags for Governance

AZ-104 Domains Covered

- Identity & Governance – RBAC, Locks, Tags
- Compute – Virtual Machine, Disks
- Networking – Virtual Network (VNet), NSG, Public IP
- Storage – Backup Vault, Restore Point
- Monitoring – Log Analytics, Alerts

Deployment Steps

1. Resource Group Configuration

A new resource group named 'rg-securevm' was created to logically organize all resources related to this project. Tags were applied to help in cost tracking and categorization. Additionally, a 'CanNotDelete' lock was implemented to prevent accidental deletion of critical resources within the group, ensuring better governance and resource protection.

rg-securevm | Tags

Name	Value
environment	: production
owner	: asad

rg-securevm (Resource group)

owner : asad environment : production

No changes

rg-securevm | Locks

Lock name	Lock type	Scope	Notes
dont delete	Delete	rg-securevm	prevent accidental deletion

2.RBAC at the Resource Group Level

A resource based access control has assigned at the resource group level named 'rgsecurevm'. A contributor role has assigned to the user01 at a resource group level .A reader role has assigned to the user02 at a resource group level.

Resource Manager - Microsoft | rg-securevm - Microsoft Azure | Resource Manager - Microsoft | +

portal.azure.com/#@mohammedfarhaan0789@gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...

Microsoft Azure Search resources, services, and docs (G+) Copilot ? 🔍 Feedback

mohammedfarhaan.0789@gmail.onmicrosoft.com DEFAULT DIRECTORY (MOHAMM...)

Home > rg-securevm

rg-securevm | Access control (IAM)

Resource group

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

Add or remove favorites by pressing **Ctrl+L+Shift+F**

Search

Name Type Role Scope Condition

Owner (2)

- MA Mohammed Asad Farha... User Owner Subscription (Inherited) None
- MA Mohammed Asad Farha... User Owner Management group (Inhe... None

Contributor (1)

- user01 db7888eb-62d4-4ec9-... User Contributor This resource None

Reader (1)

- user02 d1a2dc7-e880-4d7a-b... User Reader This resource None

StorageCustomReader (1)

- Unknown fb901c72-d86e-4dbe-... Unknown StorageCustomReader Subscription (Inherited) None

User Access Administrator (1)

- MA Mohammed Asad Farha... User User Access Administrator Root (Inherited) None

ENG IN 07:56 AM 25-10-2025

This screenshot shows the Azure IAM access control interface for the 'rg-securevm' resource group. It lists various roles (Owner, Contributor, Reader, StorageCustomReader, User Access Administrator) and their assignments across different scopes (Subscription, Management group, This resource). The interface includes a search bar, a toolbar with common actions like Add, Download role assignments, Edit columns, Refresh, Delete, and Feedback, and a detailed table view.

securevm - Microsoft Azure | rg-securevm - Microsoft Azure | Resource Manager - Microsoft | +

portal.azure.com/#@mohammedfarhaan0789@gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...

Microsoft Azure Search resources, services, and docs (G+) Copilot ? 🔍 Feedback

user01@mohammedfar... DEFAULT DIRECTORY (MOHAMM...)

Home > Resource Manager | All resources >

securevm

Virtual machine

Search Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Connect Networking Network settings Load balancing Application security groups Network manager Settings

Add or remove favorites by pressing **Ctrl+L+Shift+F**

Help me copy this VM in any region Manage this VM with Azure CLI

Connect Start Restart Stop Hibernate Capture Delete Refresh Op

Help me copy this VM in any region

Failed to delete virtual machine 'securevm'

An error occurred while deleting virtual machine 'securevm' and/or any selected resource(s) associated with it. Error: 'The scope '/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/rg-securevm/providers/Microsoft.Compute/virtualMachin...' cannot perform delete operation because following scope(s) are locked: '/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/rg-securevm'. Please remove the lock and try again.'

Help me troubleshoot

Essentials

Resource group (move)	rg-securevm	Operating system	Windows
Status	Running	Size	Standard B2s (2 vcpus, 4 GiB memory)
Location	Central India	Primary NIC public IP	74.225.191.83 1 associated public IPs
Subscription (move)	Azure subscription 1	Virtual network/subnet	vnet-securevm/subnet_prod
Subscription ID	12e423fc-a819-4e80-b0c5-1b0dcc72b980	DNS name	Not configured
		Health state	-
		Time created	25/10/2025, 01:20 UTC

Tags (edit) : Add tags

Properties Monitoring (8 alerts) Capabilities (8) Recommendations Tutorials

Virtual machine Computer name: securevm

Networking Public IP address: 74.225.191.83 (Network Interface: securevm7051)

ENG IN 07:57 AM 25-10-2025

This screenshot shows the Azure Virtual Machine details page for 'securevm'. It displays basic information like status, location, and network configuration. A prominent error message indicates that deletion failed due to locks on the resource group. The interface includes a navigation bar, a left sidebar with various management options, and a main content area with tabs for Properties, Monitoring, Capabilities, Recommendations, and Tutorials.

Virtual Machine Overview

Essentials

- Resource group (move) : rg-securevm
- Status : Running
- Location : Central India
- Subscription (move) : Azure subscription 1
- Subscription ID : 12e423fc-a819-4e80-b0c5-1b0dcc72b980
- Operating system : Windows
- Size : Standard
- Primary NIC public IP : 74.225.191.83
1 associated public IPs
- Virtual network/subnet : vnet-securevm/subnet-prod
- DNS name : Not configured
- Health state : -
- Time created : 25/10/2025, 01:20 UTC

Tags (edit) : Add tags

Properties **Monitoring (8 alerts)** **Capabilities (8)** **Recommendations** **Tutorials**

Networking

Public IP address : 74.225.191.83 (Network interface securevm706)

3. Networking Setup

A secure virtual network (VNet) named 'vnet-securevm' was created with subnets for controlled resource communication. An NSG named 'nsg-securevm' was attached to the subnet to define traffic rules. A specific inbound rule for Remote Desktop (RDP) was added to allow administrative access, while other unnecessary ports remained closed. Public IP ('securevm-ip') was assigned to the network interface card (NIC) 'securevm706' to enable external connectivity for management tasks.

Virtual Network Overview

Essentials

- Resource group (move) : rg-securevm
- Location (move) : Central India
- Subscription (move) : Azure subscription 1
- Subscription ID : 12e423fc-a819-4e80-b0c5-1b0dcc72b980
- Address space : 10.0.0.0/16
- Subnets : 1 subnet
- DNS servers : Azure provided DNS service
- BGP community string : Configure
- Virtual network ID : 2895e9d0-fa73-421d-9129-b4e115abcc1b

Tags (edit) : Add tags

Capabilities (5)

- DDoS protection : Not configured
- Azure Firewall : Not configured
- Peering : Not configured

The image shows two screenshots of the Microsoft Azure portal interface.

Screenshot 1: Subnets

- Left Sidebar:** Shows navigation items like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for), and Add or remove favorites.
- Main Content:** Displays the 'Subnets' section for a virtual network named 'vnet-securevm'. It includes a search bar, a table with columns: Name, IPv4, IPv6, Available IPs, Delegated to, Security group, and Route table. A single entry 'subnet-prod' is listed with details: 10.0.1.0/24, - (IPv6), 250 (Available IPs), - (Delegated to), 'nsg-secure...' (Security group), and - (Route table). A note says 'Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.'
- Bottom:** Shows the Windows taskbar with various pinned icons and system status.

Screenshot 2: NSG Inbound Security Rules

- Left Sidebar:** Shows navigation items like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring), and a link to https://go.microsoft.com/fwlink/?linkid=2174617.
- Main Content:** Displays the 'Inbound security rules' section for a Network Security Group named 'nsg-securevm'. It includes a search bar, a table with columns: Priority, Name, Port, Protocol, Source, Destination, and Action. The table lists several rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	allowrdp	3389	TCP	Any	Any	Allow
110	allowhttp	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
- Bottom:** Shows the Windows taskbar with various pinned icons and system status.

4. Virtual Machine Deployment

A Windows Server-based virtual machine named 'securevm' was deployed with both OS and data disks configured. The VM was assigned a system-assigned managed identity to enable secure communication with other Azure services without using credentials. Boot diagnostics and monitoring were activated to observe the VM's health and performance.

The screenshot shows two side-by-side views of the Microsoft Azure portal.

Left View: Virtual Machine Overview

- Resource Group:** rg-securevm
- Status:** Running
- Location:** Central India
- Subscription:** Azure subscription 1
- Subscription ID:** 12e423fc-a819-4e80-b0c5-1b0dcc72b980
- Operating system:** Windows Server 2019 Datacenter
- Size:** Standard B2s (2 vcpus, 4 GiB memory)
- Primary NIC public IP:** 74.225.191.83 (1 associated public IP)
- Virtual network/subnet:** vnet-securevm/subnet-prod
- DNS name:** Not configured
- Health state:** -
- Time created:** 25/10/2025, 01:20 UTC

Right View: Disks Overview

- OS disk:**
 - Disk name: securevm_OsDisk_1_9b326f54f4aa4b3bb8d
 - Storage type: Premium SSD LRS
 - Size (GiB): 127
 - Max IOPS: 500
 - Max throughput: 100
 - Encryption: SSE with PMK
- Data disks:**
 - Filter by name: securevm_DataDisk_0
 - Showing 1 of 1 attached data disks
 - Create and attach a new disk
 - Attach existing disks
 - LUN: 0
 - Disk name: securevm_DataDisk_0
 - Storage type: Premium SSD LRS
 - Size (GiB): 4
 - Max IOPS: 120
 - Max throughput: 25
 - Encryption: SSE with PMK

5. Backup Configuration

A Recovery Services Vault named 'securevmvault' was set up to manage the backup and restore configurations. The VM was registered to the vault, and a manual backup job was triggered to create an initial restore point. This ensures that in case of system failure or data corruption, the VM can be restored to a previous healthy state.

securevm | Backup

Virtual machine

Back now Restore VM File Recovery Stop backup Resume backup Delete backup data Restore to Secondary Region Undelete ...

Security Microsoft Defender for Cloud

Backup + disaster recovery Backup

Operations Change tracking

Essentials

Recovery services vault : **securemvault** Backup Pre-Check : Passed

Subscription (move) : [Azure subscription 1](#) Last backup status : Success 01/01/2001, 05:30:00

Subscription ID : 12e423fc-a819-4e80-b0c5-1b0dcc72b980 Backup policy : [policyA \(Enhanced\)](#)

Alerts (in last 24 hours) : [View alerts](#) Oldest restore point : 25/10/2025, 07:05:48 (56 minute(s) ago)

Jobs (in last 24 hours) : [View jobs](#) Included disk(s) : All disks

JSON View

Recovery points

This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault-archive, click here.

Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.

Creation time ↑↓	Consistency	Recovery type
25/10/2025, 07:05:48	Application Consistent	Snapshot

<https://portal.azure.com/#> using Ctrl+Shift+F

Administrator: Windows PowerShell

```

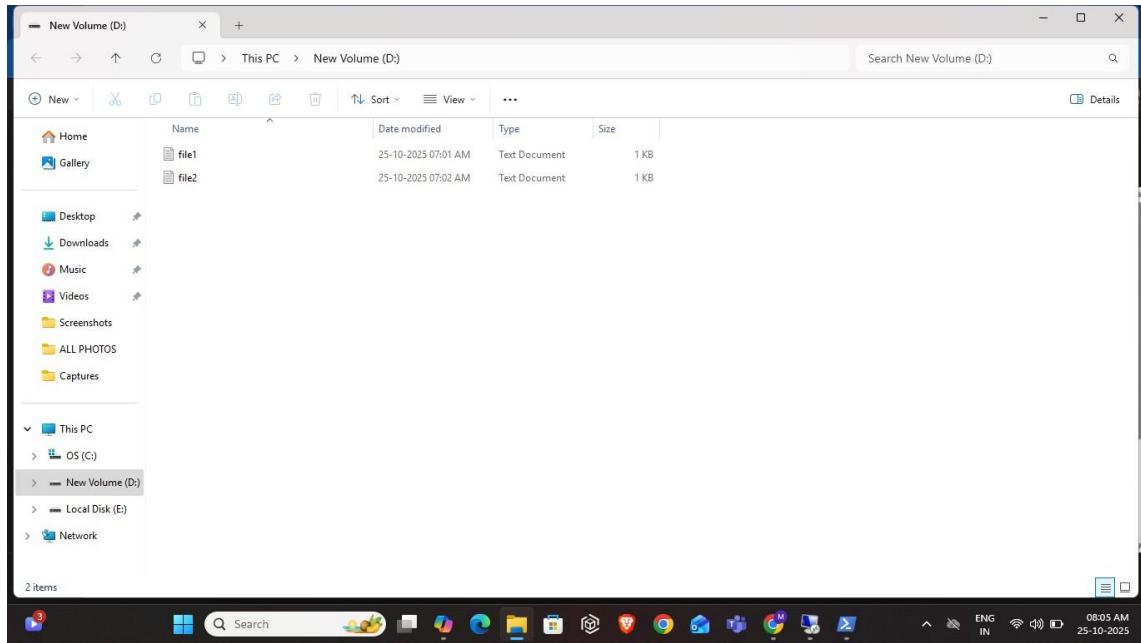
Checking for OS Compatibility: DONE
Ensuring that the machine meets the requirements to run the recovery script.
Checking for network connectivity: DONE
Checking for required cipher suite: DONE
Checking for Large Disks: DONE
Checking for Storage Pools: DONE
We detected a session already connected to a recovery point of the VM webvmwindows01 .
We need to unmount the volumes before connecting to the new recovery point of VM securevm,
Please enter 'Y' to proceed or 'N' to abort...
Please wait while we disconnect old session...
Older session disconnected. Establishing a new session for the new recovery point...
Connecting to recovery point using iSCSI service....
iSCSI target prepared
Connection succeeded!
Please wait while we attach volumes of the recovery point.
***** Open Explorer to browse for files *****
After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step 3 of the portal.

```

2 items

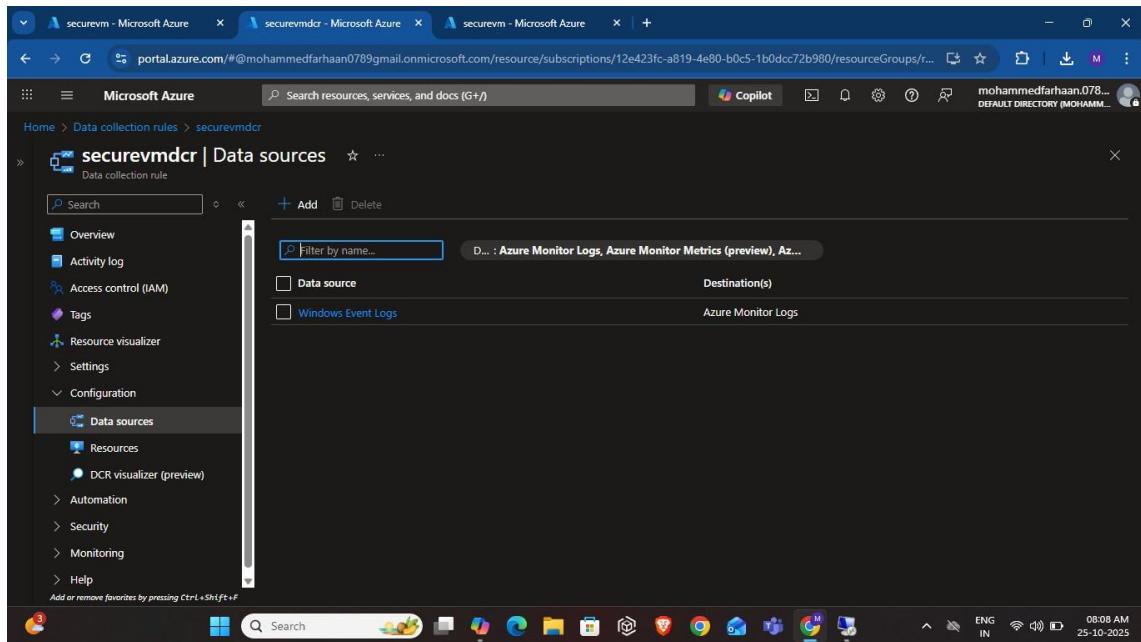
08:02 AM 25-10-2025

08:05 AM 25-10-2025



6. Monitoring and Alerts Setup

Monitoring was enabled by linking the VM to a Log Analytics Workspace named 'securevmlogsanalyticalworkspace'. The Azure Monitor Windows Agent was installed to collect telemetry data. A Data Collection Rule (DCR) named 'securevmmdcr' was configured to send performance metrics and logs to the workspace. Alerts were created using Activity Logs and an Action Group to notify administrators about critical changes or performance issues.



securevm - Microsoft Azure

securevm - Microsoft Azure

securevm - Microsoft Azure

portal.azure.com/#@mohammedfarhaan0789@gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

mohammedfarhaan.078...

DEFAULT DIRECTORY (MOHAMM...)

Home > Data collection rules > securevm

securevm | Resources

This is a preview version of the new data collection rule associated resources page. Your feedback is appreciated. View the classic experience.

+ Add Disassociate Refresh Edit Data Collection Endpoint

Preselect resources already associated with this data collection rule

Filter for any field... Subscription == Azure subscription 1 Add filter

Resource name	Type	Location	Data Collectio...	Resource Group	Subscription
securevm	Virtual machine	Central India	No endpoint co...	rg-securevm	Azure subscript...

Showing 1 - 1 of 1 results.

Add or remove favorites by pressing Ctrl+Shift+F

Search

ENG IN 08:08 AM 25-10-2025

Detailed description: This screenshot shows the 'Data collection rules' section in the Microsoft Azure portal. It displays a single resource named 'securevm' which is a virtual machine located in Central India. The resource is associated with the 'rg-securevm' resource group and the 'Azure subscription'. A note at the top indicates this is a preview version of the new data collection rule associated resources page.

securevm - Microsoft Azure

securevmlogsanalyticalworkspace - Microsoft Azure

securevm - Microsoft Azure

portal.azure.com/#@mohammedfarhaan0789@gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

mohammedfarhaan.078...

DEFAULT DIRECTORY (MOHAMM...)

Home > securevmlogsanalyticalworkspace

securevmlogsanalyticalworkspace | Logs

New Query 1+ ... x +

Run Time range : Last 30 minutes Show : 1000 results KQL mode

1 Event | where EventID == 4798

Save Share ... Queries hub

Results Chart

TimeGenerated [UTC]	Source	EventLog	Computer	EventCategory
25/10/2025, 02:23:18.567	Microsoft-Windows-Security-Audit	Security	securevm	13824
25/10/2025, 02:23:18.564	Microsoft-Windows-Security-Audit	Security	securevm	13824
25/10/2025, 02:23:16.278	Microsoft-Windows-Security-Audit	Security	securevm	13824
25/10/2025, 02:23:16.278	Microsoft-Windows-Security-Audit	Security	securevm	13824
25/10/2025, 02:23:16.278	Microsoft-Windows-Security-Audit	Security	securevm	13824

Add or remove favorites by pressing Ctrl+Shift+F

Search

ENG IN 08:12 AM 25-10-2025

Detailed description: This screenshot shows the 'Logs' section in the Microsoft Azure portal for a specific workspace. A query '1 Event | where EventID == 4798' is run, showing results from the last 30 minutes. The results table lists five events, all of which are Security logs from the Microsoft-Windows-Security-Audit source, generated on 25/10/2025 between 02:23:16.278 and 02:23:18.567 UTC, and categorized as 13824.

[securevm - Microsoft Azure](#) [windowseventactivitylogrule - Microsoft Azure](#) [securevm - Microsoft Azure](#)

Microsoft Azure Copilot

Home > Monitor | Alerts > Alert rules >

Alert rules

[Create](#) [Columns](#)

Search: windowseventactivitylogrule

Overview

Activity log alert rule

Scope

Resource: **SecureVM** Hierarchy: Azure subscription 1 > rg-securevm

Condition

Whenever the Activity Log has an event with Category='Administrative'

Actions

Name	Contains actions
windowseventactivitylogalert	1 Email

Give feedback

08:13 AM 25-10-2025

This screenshot shows the 'Alert rules' blade in the Azure portal. It displays a single alert rule named 'windowseventactivitylogrule'. The 'Scope' section shows it's applied to the 'SecureVM' resource. The 'Condition' section specifies that the alert triggers whenever an 'Administrative' category event is recorded in the activity log. The 'Actions' section shows that an email notification is configured for this alert. The bottom of the screen shows the Windows taskbar with various pinned icons.

[securevm - Microsoft Azure](#) [Action groups - Microsoft Azure](#) [securevm - Microsoft Azure](#)

Microsoft Azure Copilot

Home > Monitor | Alerts >

Action groups

[Create](#) [Columns](#) [Refresh](#) [Open query](#) [Delete](#) [Enable](#) [Disable](#) [Test action group](#)

Subscription: Azure subscription 1 Resource group: all Location: all Status: Enabled Add tag filter No grouping

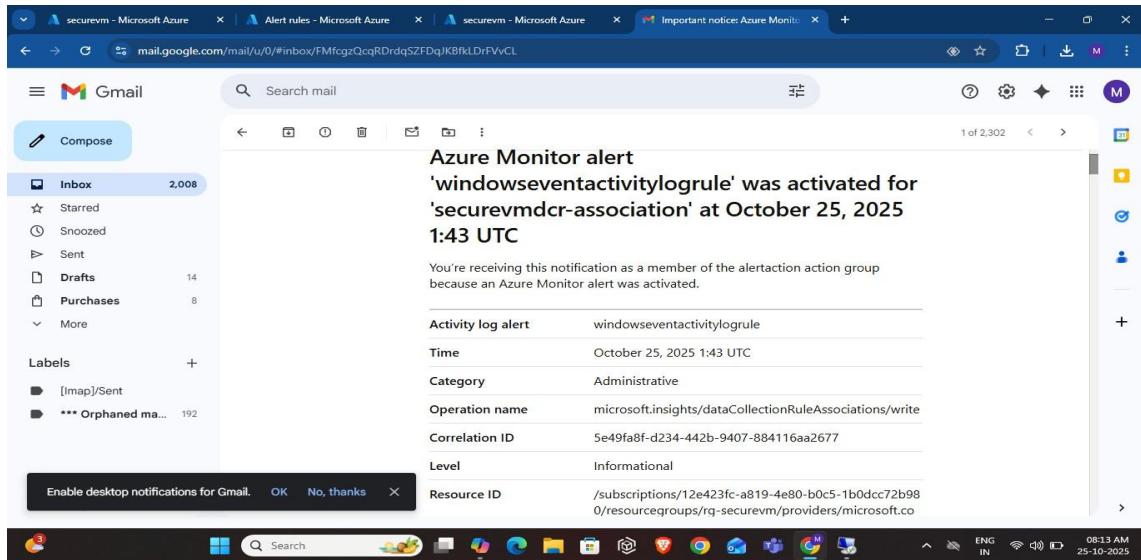
Name	Short name	Resource group	Subscription	Actions	Status
windowseventactivitylogalert	alertaction	rg-securevm	Azure subscription 1	1 Email	Enabled

Showing 1 - 1 of 1 results.

Give feedback

08:12 AM 25-10-2025

This screenshot shows the 'Action groups' blade in the Azure portal. It displays a single action group named 'alertaction', which is associated with the 'SecureVM' resource and configured to send an email notification. The action group is currently enabled. The bottom of the screen shows the Windows taskbar with various pinned icons.



7. Validation and Governance Review

After completing all configurations, validation was performed to ensure that NSG rules, RBAC roles, and backup jobs were functioning as expected. The resource locks were verified, and monitoring dashboards confirmed live data collection. This validation ensured that the VM met governance, security, and operational standards as per AZ-104 learning outcomes.

Outcome

The secure Azure VM was successfully deployed with a complete governance and protection model. The project demonstrated practical application of RBAC, NSG hardening, Azure Backup, and performance monitoring. The configuration proved resilient against accidental deletion, ensured system recoverability, and maintained continuous visibility through monitoring tools.

Skills Demonstrated

- Azure Resource Governance using Locks and Tags
- Role-Based Access Control (RBAC) Implementation
- Network Security using NSG Rules
- Azure Backup Vault Configuration and Restore Management
- Performance Monitoring and Log Analytics Setup
- Azure Alerting System using Action Groups

Subscription Used

Azure account (pay as-you-go).