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

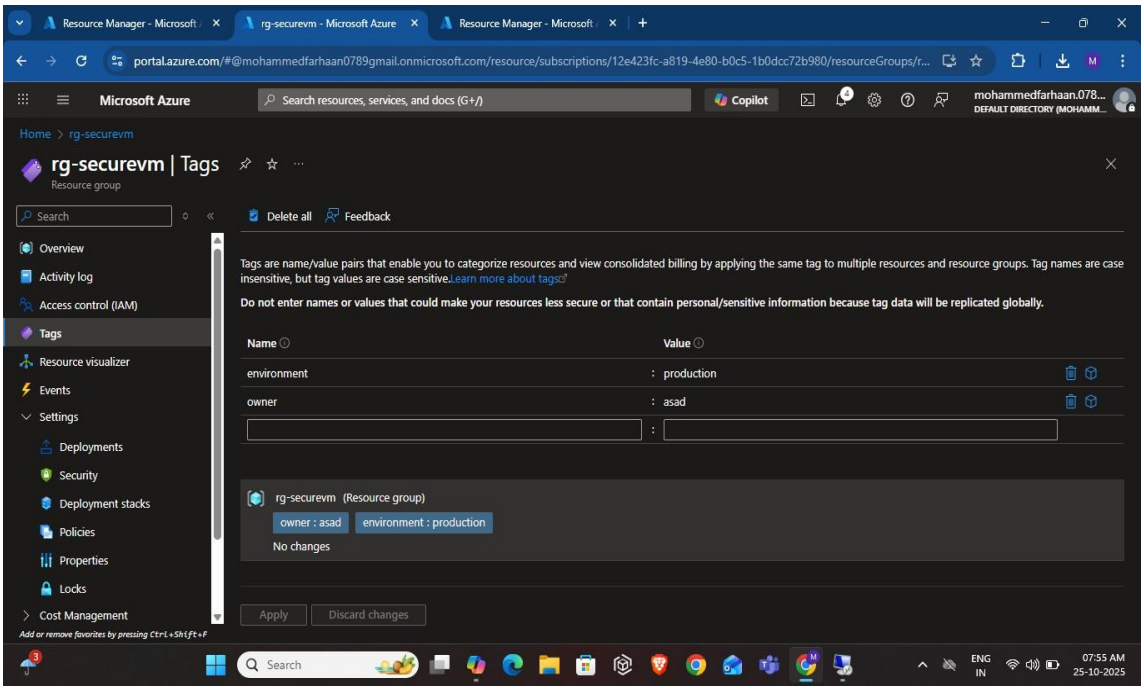
AZ-104 Domains Covered

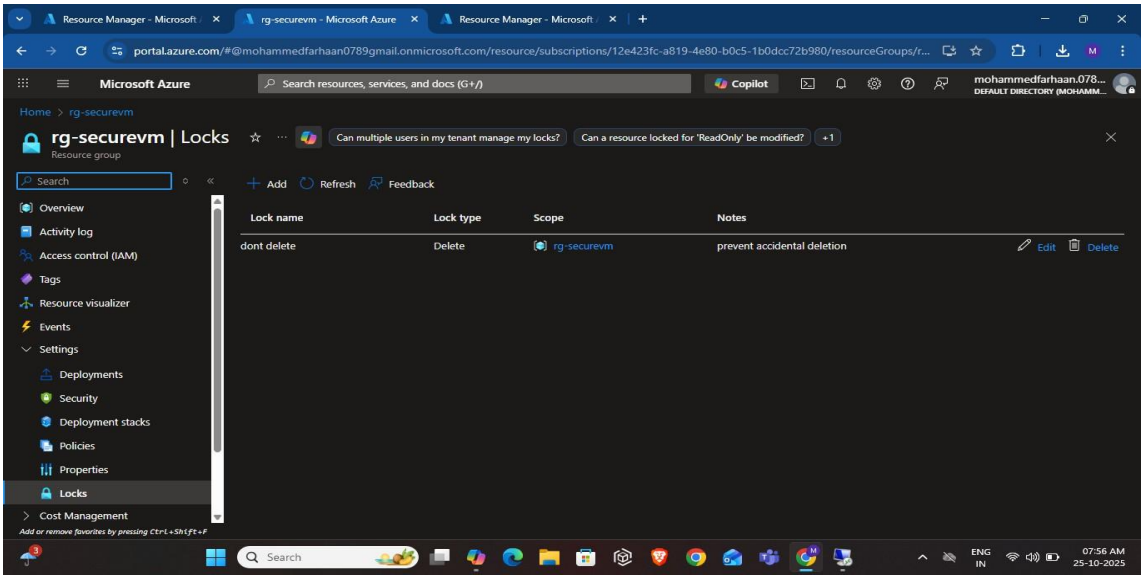
- Identity & Governance – RBAC, Locks, Tags
- Compute – Virtual Machine, Disks
- Networking – Virtual Network (VNet), NSG, Public IP
- Storage – Backup Vault, Restore Point
- Monitoring – Log Analytics, Alerts

Deployment Steps

1. Resource Group Configuration

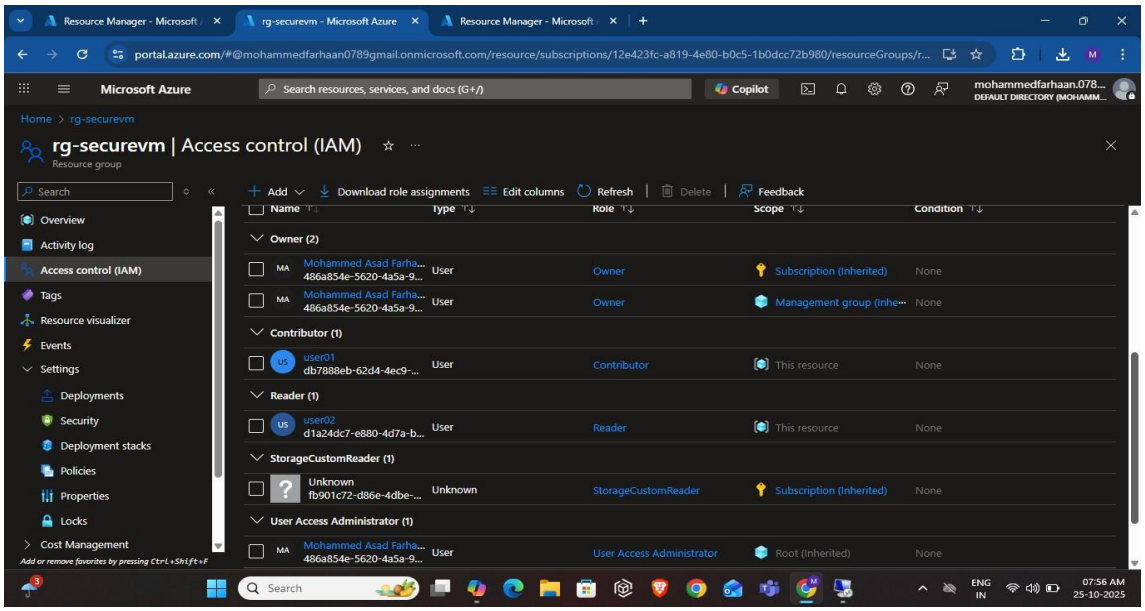
A new resource group named 'rg-securevm' was created to logically organize all resources related to this project. Tags were applied to help in cost tracking and categorization. Additionally, a 'CanNotDelete' lock was implemented to prevent accidental deletion of critical resources within the group, ensuring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

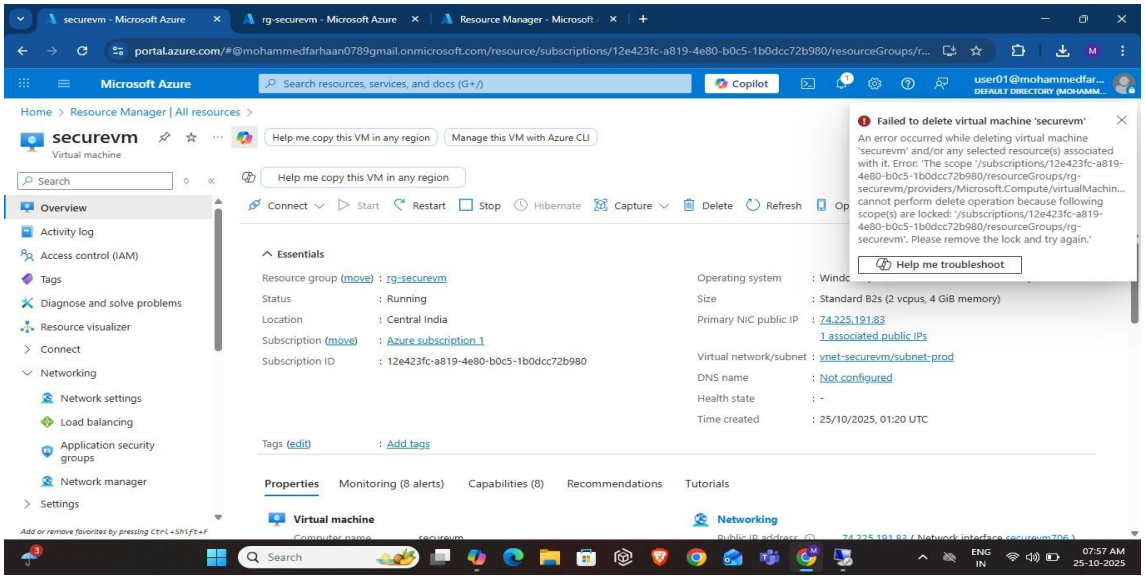


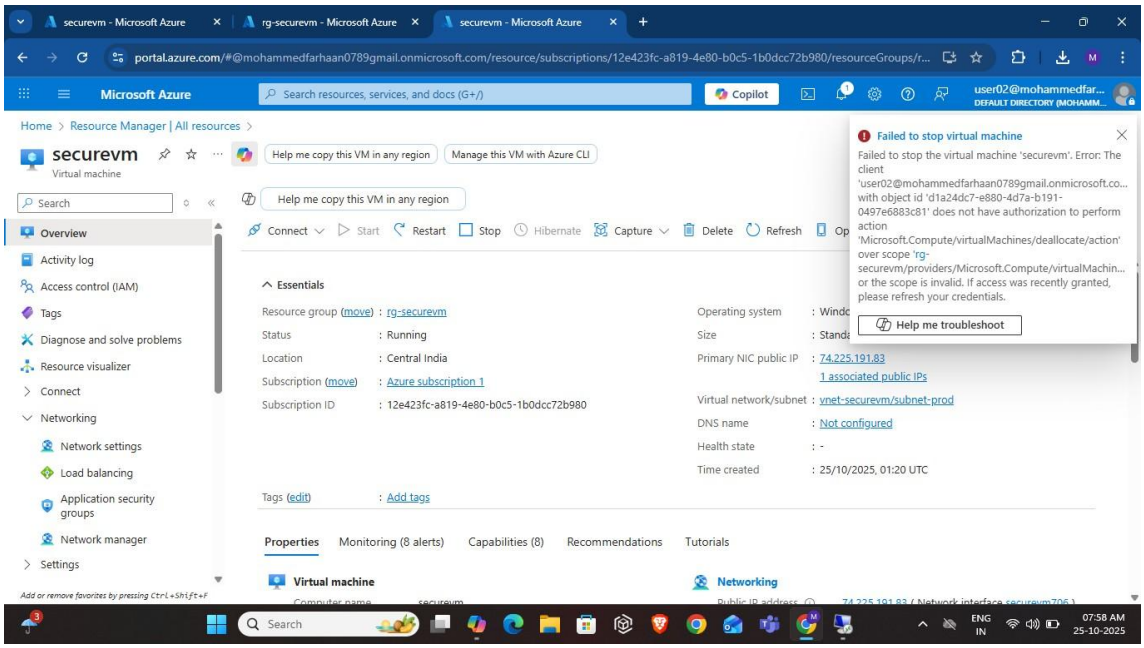


2.RBAC at the Resource Group Level

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.

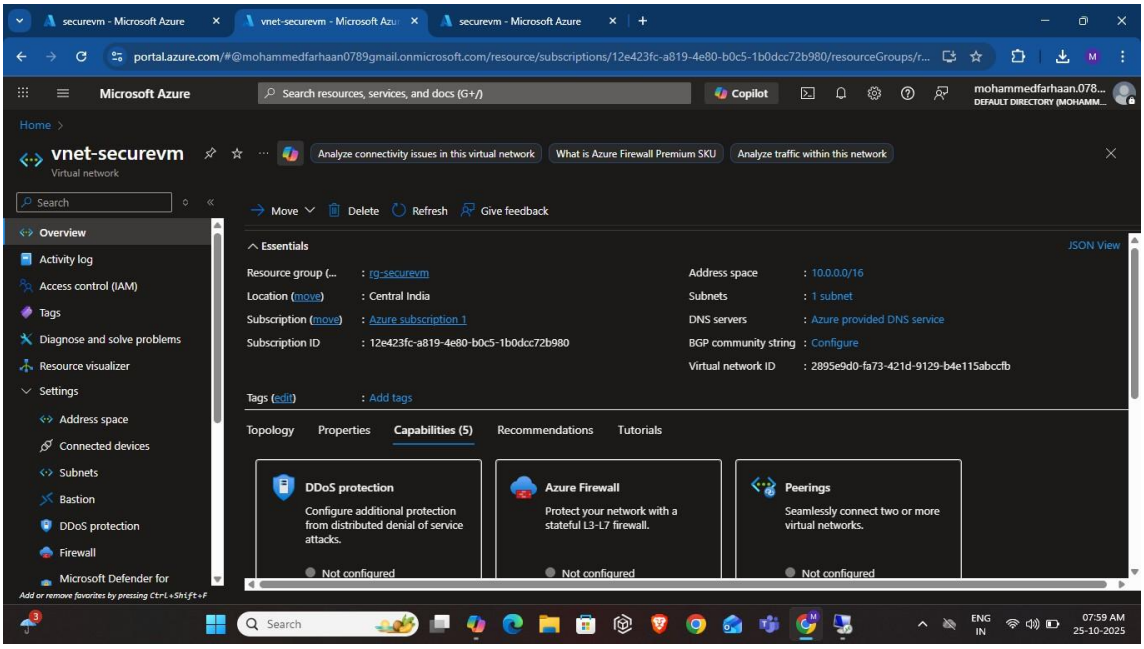

Resource Manager - Microsoft
rg-securevm - Microsoft Azure
Resource Manager - Microsoft
portal.azure.com/#@mohammedfarhaan0789gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mohammedfarhaan.078...
DEFAULT DIRECTORY (MOHAMM...
Home > 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+Shift+F
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
Name
Type
Role
Scope
Condition
Owner (2)
Mohammed Asad Farha... 486a854e-5620-4a5a-9...
User
Owner
Subscription (Inherited)
None
Mohammed Asad Farha... 486a854e-5620-4a5a-9...
User
Owner
Management group (Inhe...
None
Contributor (1)
user01 db7888eb-62d4-4ec9-...
User
Contributor
This resource
None
Reader (1)
user02 d1a24dc7-e880-4d7a-b...
User
Reader
This resource
None
StorageCustomReader (1)
Unknown fb901c72-d86e-4dbe-...
Unknown
StorageCustomReader
Subscription (Inherited)
None
User Access Administrator (1)
Mohammed Asad Farha... 486a854e-5620-4a5a-9...
User
User Access Administrator
Root (Inherited)
None
Search
ENG
IN
07:56 AM
25-10-2025

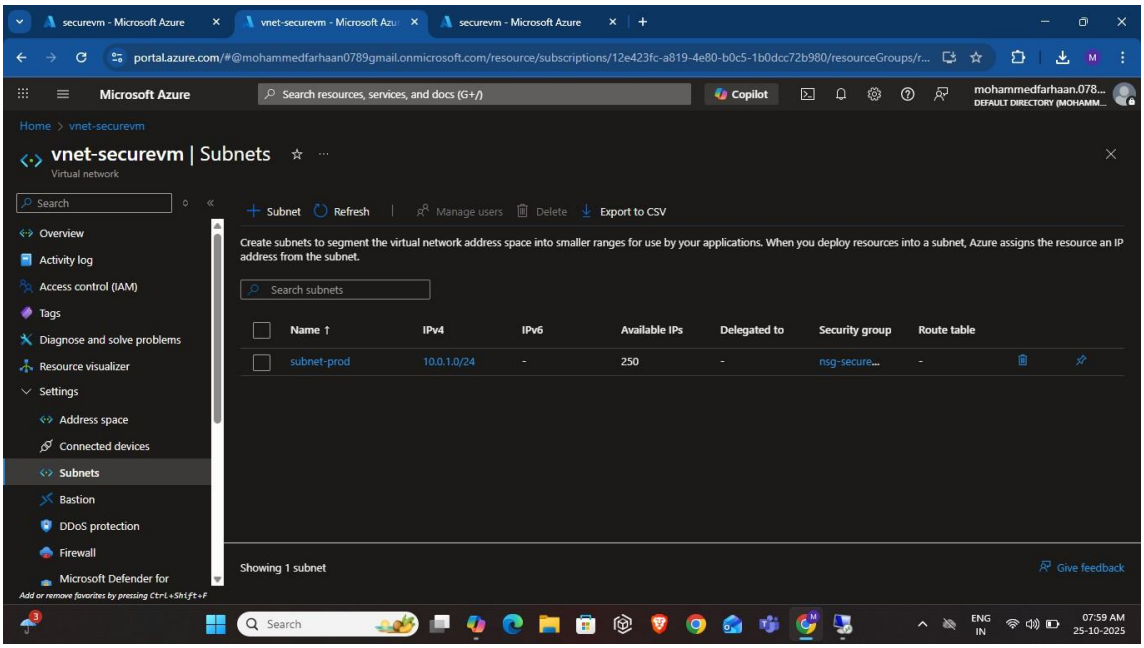

securevm - Microsoft Azure
rg-securevm - Microsoft Azure
Resource Manager - Microsoft
portal.azure.com/#@mohammedfarhaan0789gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
user01@mohammedfar...
DEFAULT DIRECTORY (MOHAMM...
Home > Resource Manager | All resources >
securevm
Virtual machine
Help me copy this VM in any region
Manage this VM with Azure CLI
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+Shift+F
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
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 : Windo
Size : Standard B2s (2 vcpus, 4 GiB memory)
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
Virtual machine
Networking
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
Search
ENG
IN
07:57 AM
25-10-2025

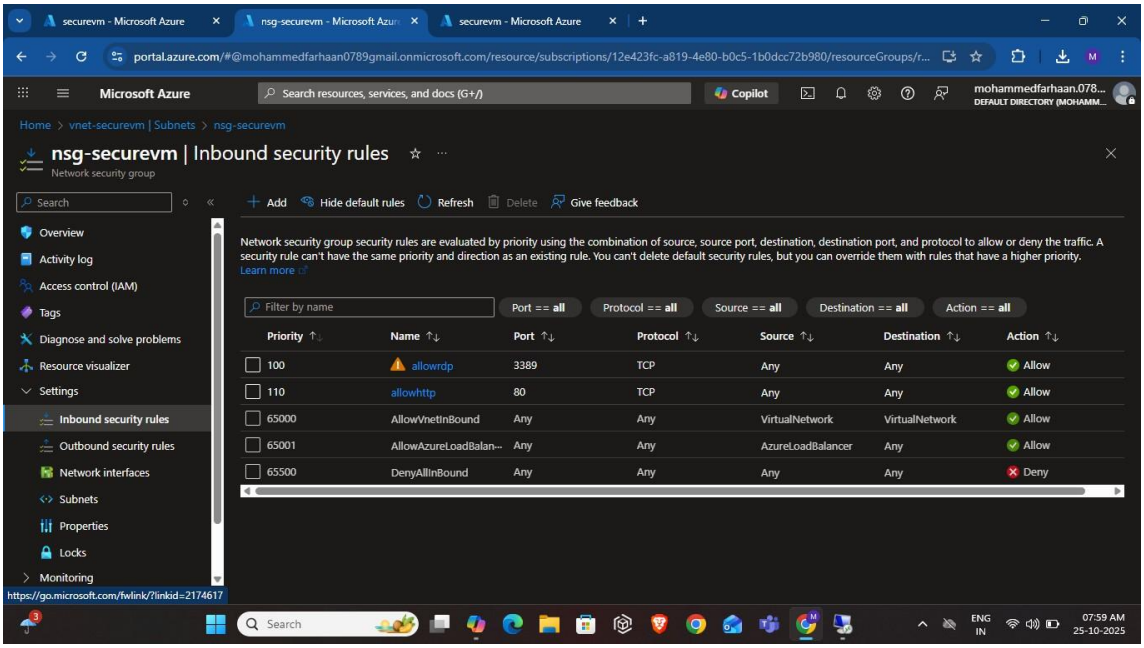


3. Networking Setup

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.

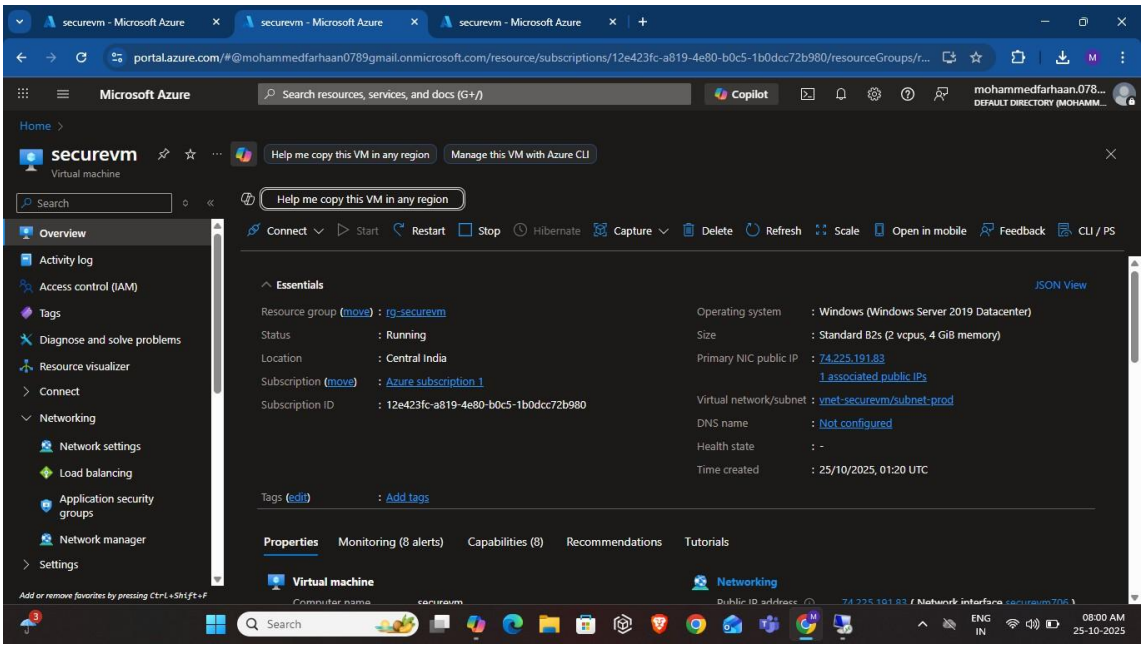


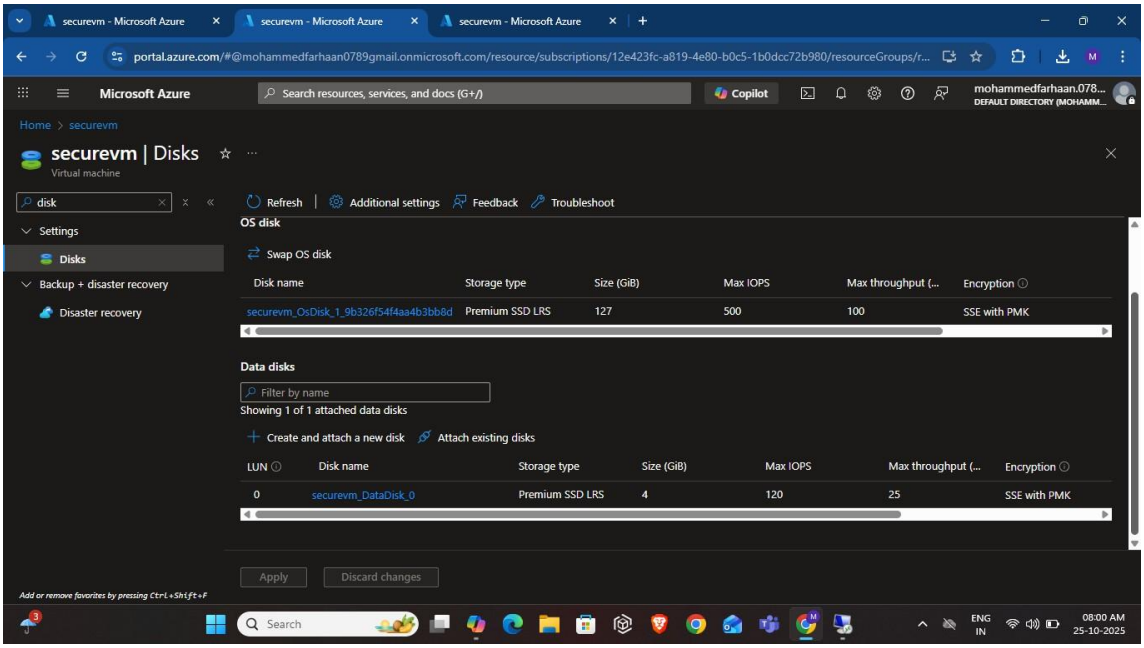




4. Virtual Machine Deployment

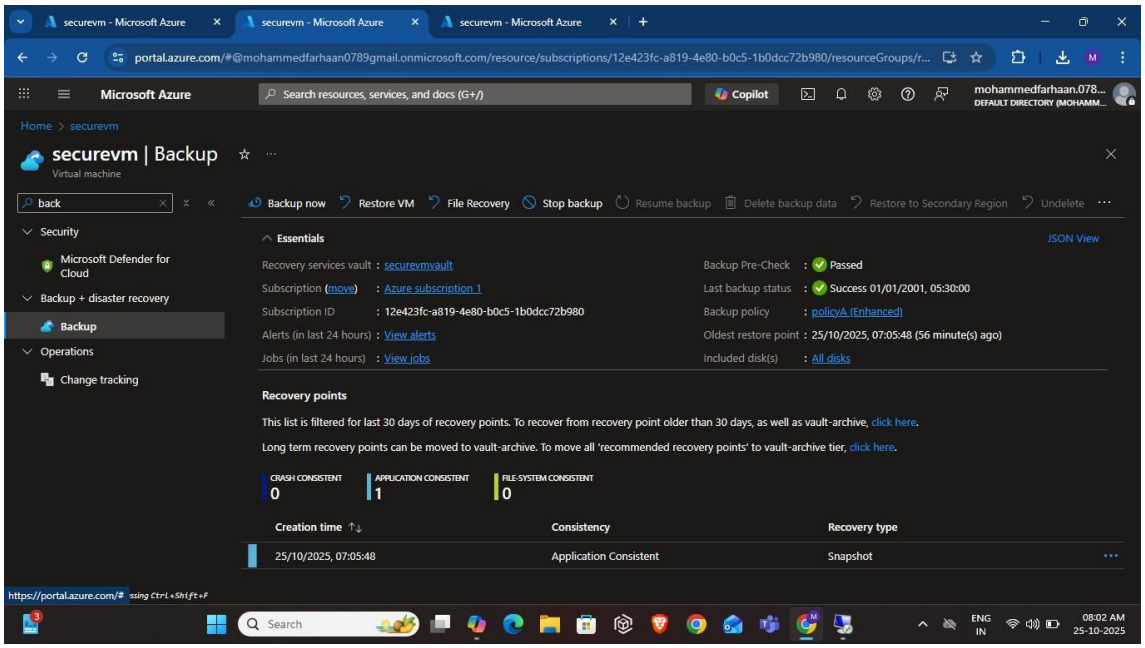
A Windows Server-based virtual machine named 'securevm' was deployed with both OS and data disks configured. The VM was assigned a system-assigned managed identity to enable secure communication with other Azure services without using credentials. Boot diagnostics and monitoring were activated to observe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

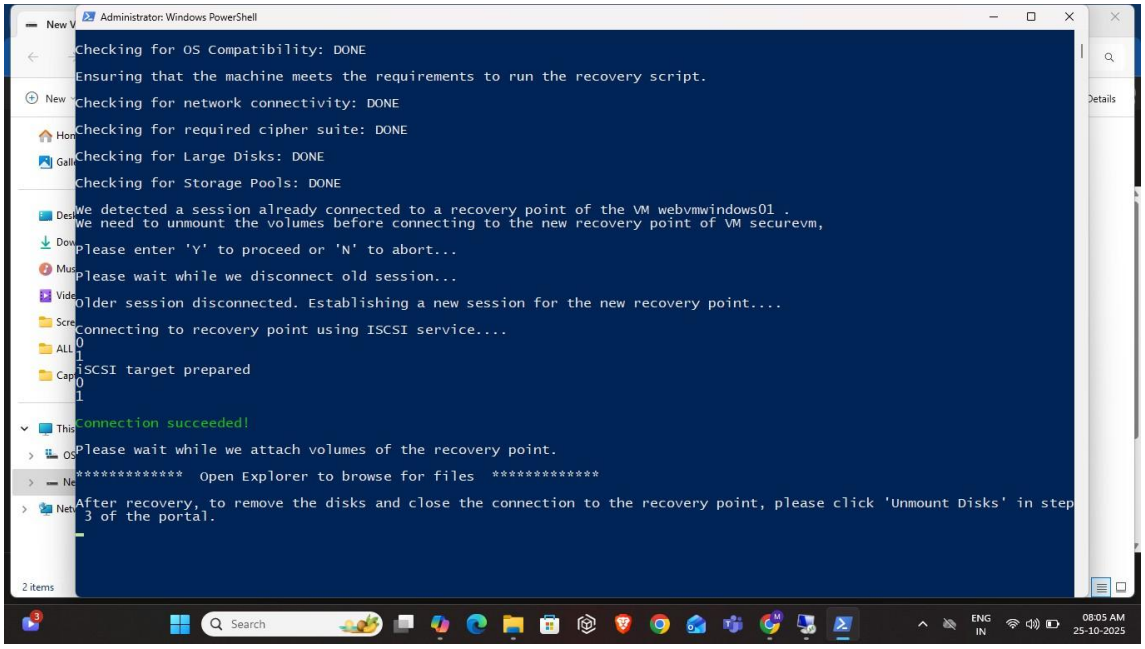


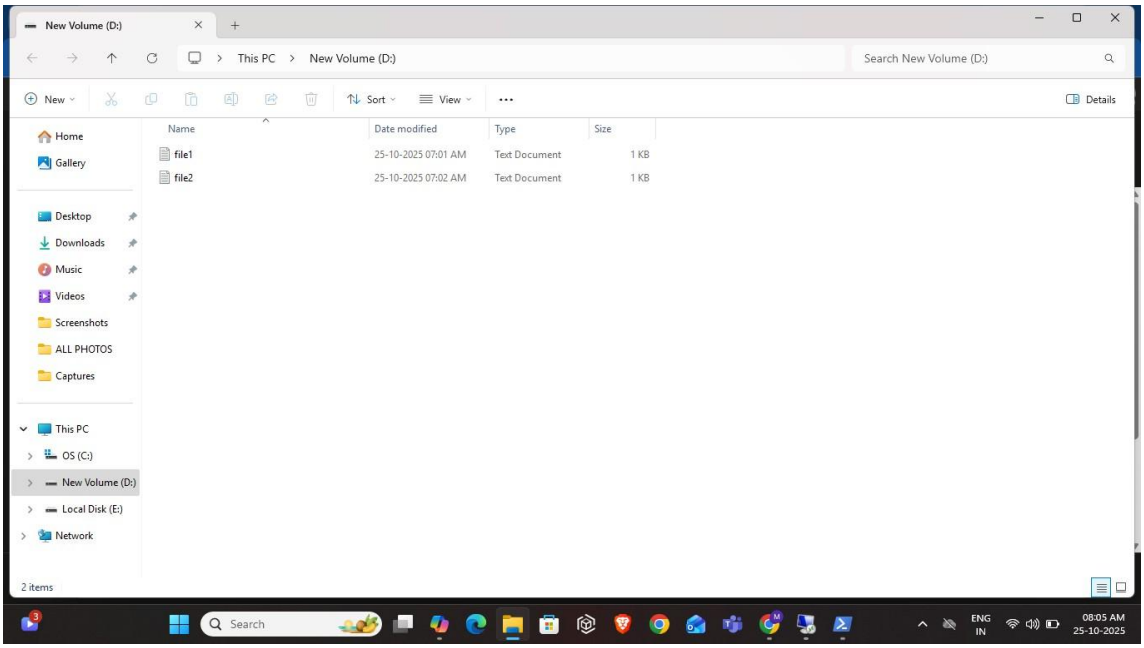


5. Backup Configuration

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.

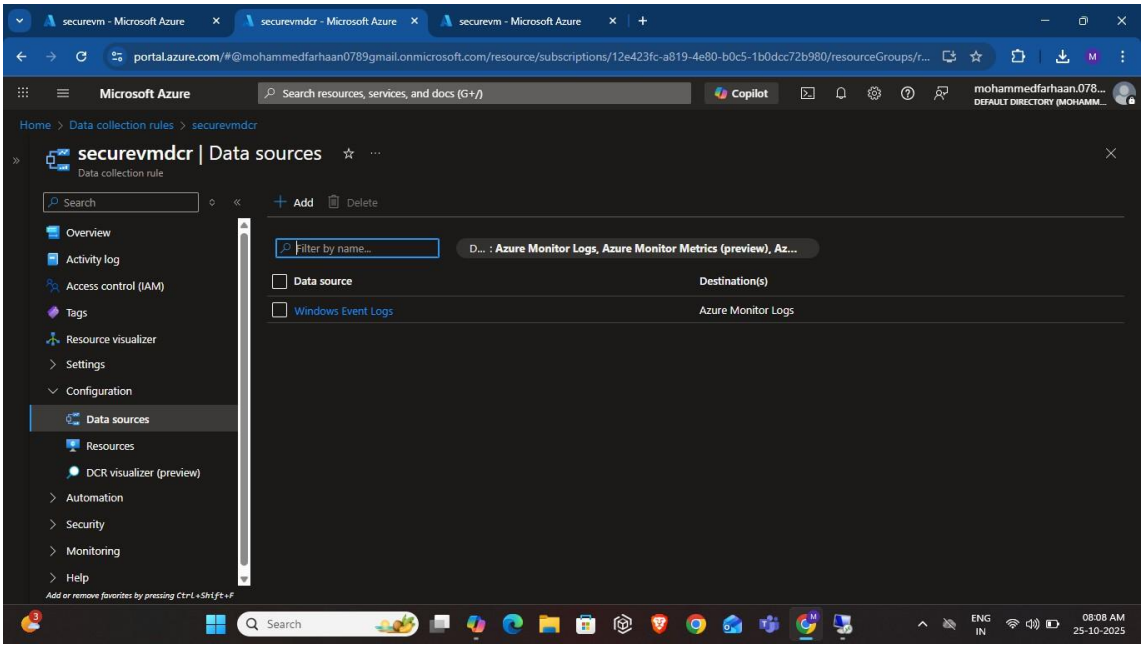

securevm - Microsoft Azure
portal.azure.com/#@mohammedfarhaan0789gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mohammedfarhaan.078...
DEFAULT DIRECTORY (MOHAMM...
Home > securevm
securevm | Backup
Virtual machine
back
Security
Microsoft Defender for Cloud
Backup + disaster recovery
Backup
Operations
Change tracking
Backup now
Restore VM
File Recovery
Stop backup
Resume backup
Delete backup data
Restore to Secondary Region
Undelete
Essentials
JSON View
Recovery services vault : securevmvault
Subscription (move) : Azure subscription 1
Subscription ID : 12e423fc-a819-4e80-b0c5-1b0dcc72b980
Alerts (in last 24 hours) : View alerts
Jobs (in last 24 hours) : View jobs
Backup Pre-Check : Passed
Last backup status : Success 01/01/2001, 05:30:00
Backup policy : policyA (Enhanced)
Oldest restore point : 25/10/2025, 07:05:48 (56 minute(s) ago)
Included disk(s) : All disks
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.
CRASH CONSISTENT 0
APPLICATION CONSISTENT 1
FILE-SYSTEM CONSISTENT 0
Creation time
Consistency
Recovery type
25/10/2025, 07:05:48
Application Consistent
Snapshot
https://portal.azure.com/#
Search
ENG IN
08:02 AM 25-10-2025

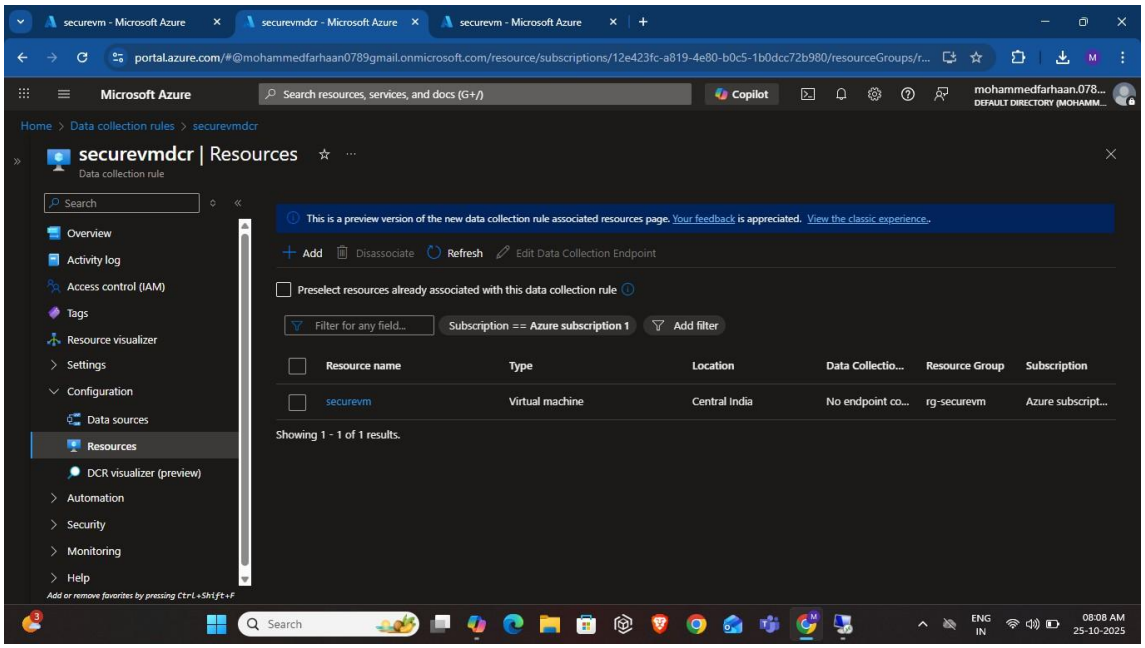

Administrator: Windows PowerShell
Checking for OS Compatibility: DONE
Ensuring that the machine meets the requirements to run the recovery script.
Checking for network connectivity: DONE
Checking for required cipher suite: DONE
Checking for Large Disks: DONE
Checking for Storage Pools: DONE
We detected 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....
0
1
iSCSI target prepared
0
1
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
Search
ENG IN
08:05 AM 25-10-2025

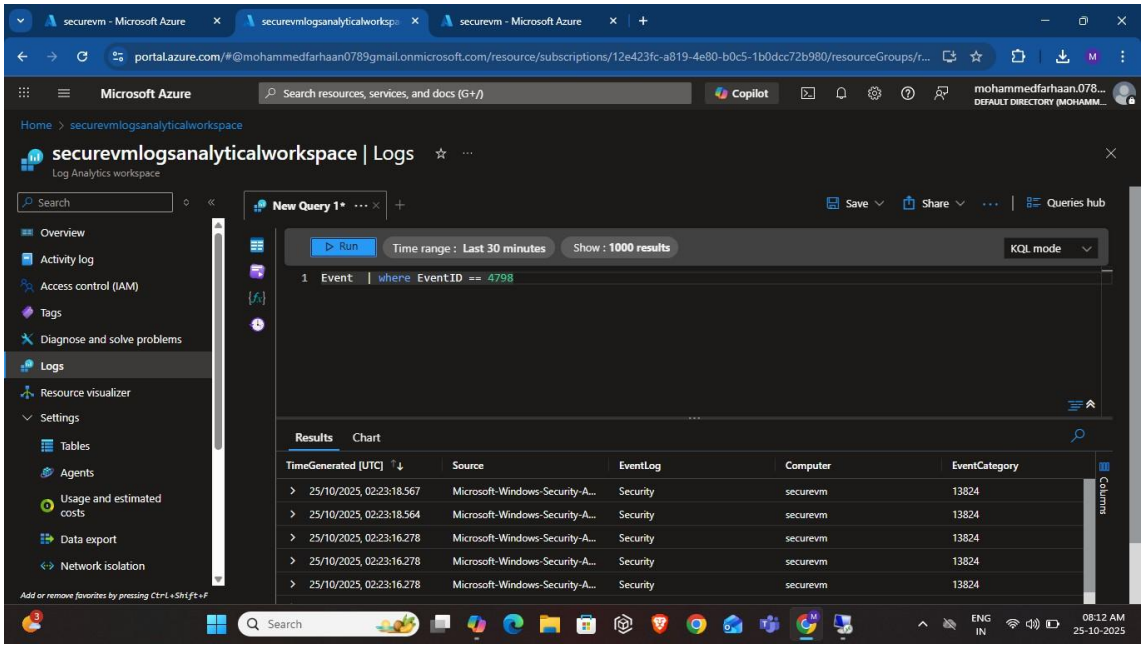


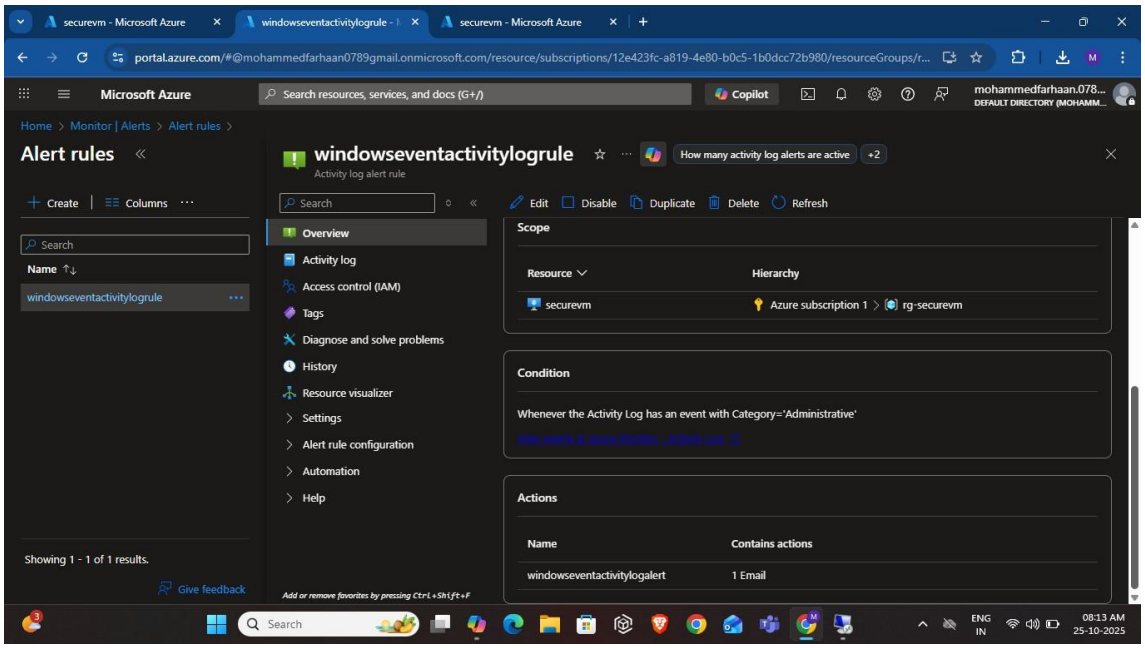
6. Monitoring and Alerts Setup

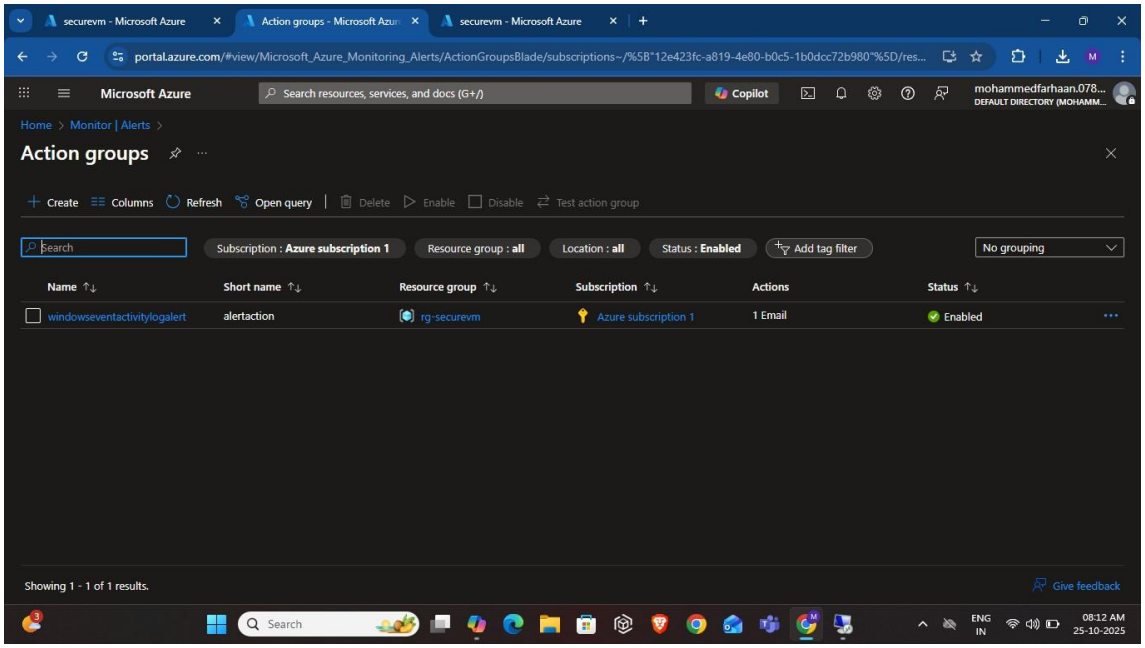
Monitoring was enabled by linking the VM to a Log Analytics Workspace named 'securevmlogsanalyticalworkspace'. The Azure Monitor Windows Agent was installed to collect telemetry data. A Data Collection Rule (DCR) named 'securevmdcr' was configured to send performance metrics and logs to the workspace.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

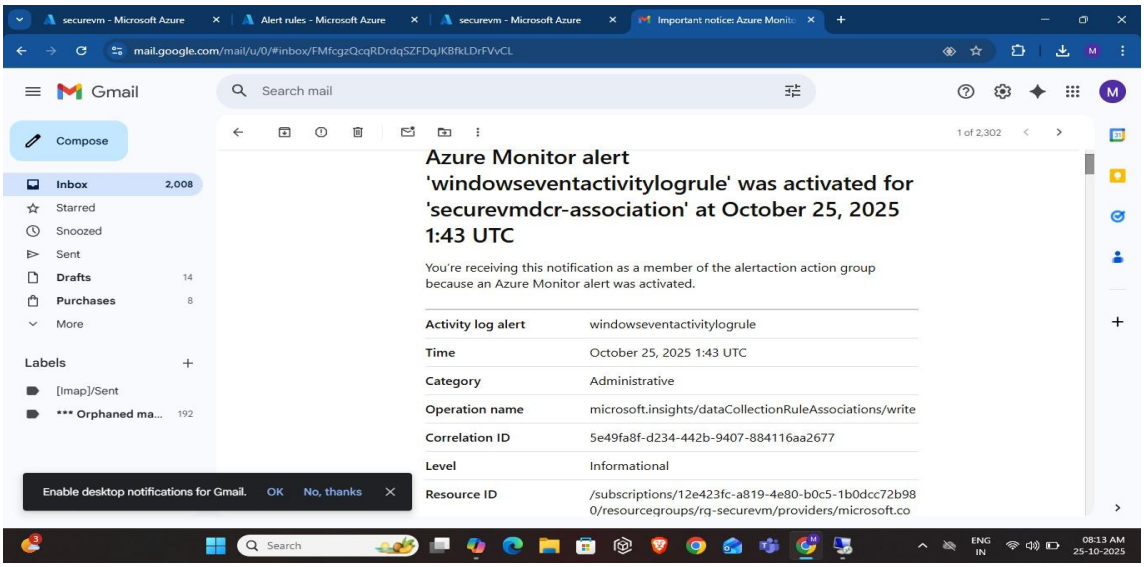



securevm - Microsoft Azure
securevmdcr - Microsoft Azure
securevm - Microsoft Azure
portal.azure.com/#@mohammedfarhaan0789gmail.onmicrosoft.com/resource/subscriptions/12e423fc-a819-4e80-b0c5-1b0dcc72b980/resourceGroups/r...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mohammedfarhaan.078...
DEFAULT DIRECTORY (MOHAMM...
Home > Data collection rules > securevmdcr
securevmdcr | Resources
Data collection rule
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
Configuration
Data sources
Resources
DCR visualizer (preview)
Automation
Security
Monitoring
Help
Add or remove favorites by pressing Ctrl+Shift+F
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.
Search
ENG
IN
08:08 AM
25-10-2025


securevm - Microsoft Azure
securevmlogsanalyticalworkspa
securevm - Microsoft Azure
portal.azure.com/#@mohammedfarhaan0789gmail.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
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Tables
Agents
Usage and estimated costs
Data export
Network isolation
Add or remove favorites by pressing Ctrl+Shift+F
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 30 minutes
Show : 1000 results
KQL mode
1 Event | where EventID == 4798
Results
Chart
TimeGenerated [UTC]
Source
EventLog
Computer
EventCategory
25/10/2025, 02:23:18.567 Microsoft-Windows-Security-A... Security securevm 13824
25/10/2025, 02:23:18.564 Microsoft-Windows-Security-A... Security securevm 13824
25/10/2025, 02:23:16.278 Microsoft-Windows-Security-A... Security securevm 13824
25/10/2025, 02:23:16.278 Microsoft-Windows-Security-A... Security securevm 13824
25/10/2025, 02:23:16.278 Microsoft-Windows-Security-A... Security securevm 13824
Columns
Search
ENG
IN
08:12 AM
25-10-2025


securevm - Microsoft Azure
windowseventactivitylogrule - I
securevm - Microsoft Azure
portal.azure.com/#@mohammedfarhaan0789gmail.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 > Monitor | Alerts > Alert rules >
Alert rules
Create
Columns
Search
Name
windowseventactivitylogrule
Showing 1 - 1 of 1 results.
Give feedback
windowseventactivitylogrule
Activity log alert rule
How many activity log alerts are active
+2
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
History
Resource visualizer
Settings
Alert rule configuration
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
Edit
Disable
Duplicate
Delete
Refresh
Scope
Resource
Hierarchy
securevm
Azure subscription 1 > rg-securevm
Condition
Whenever the Activity Log has an event with Category='Administrative'
Actions
Name
Contains actions
windowseventactivitylogalert
1 Email
Search
ENG
IN
08:13 AM
25-10-2025


securevm - Microsoft Azure
Action groups - Microsoft Azur
securevm - Microsoft Azure
portal.azure.com/#view/Microsoft_Azure_Monitoring_Alerts/ActionGroupsBlade/subscriptions~/%5B"12e423fc-a819-4e80-b0c5-1b0dcc72b980"%5D/res...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
mohammedfarhaan.078...
DEFAULT DIRECTORY (MOHAMM...
Home > Monitor | Alerts >
Action groups
Create
Columns
Refresh
Open query
Delete
Enable
Disable
Test action group
Search
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
Search
ENG
IN
08:12 AM
25-10-2025



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).